Soluções da FlexPod

FlexPod

NetApp
November 22, 2024

Índice

Soluções da FlexPod

Definição de FlexPod

Especificações técnicas do FlexPod Express

TR-4293: Especificações técnicas do FlexPod Express

Mais informações sobre Karthick Radhakrishnan, NetApp

O FlexPod Express é uma arquitetura pré-projetada e de práticas recomendadas, desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS) e na família de switches Cisco Nexus, e a camada de storage foi criada com o uso do NetApp FAS ou do storage NetApp e-Series. O FlexPod Express é uma plataforma adequada para executar vários hipervisores de virtualização e sistemas operacionais (SO) bare metal e cargas de trabalho empresariais.

O FlexPod Express oferece não apenas uma configuração de linha de base, mas também a flexibilidade de ser dimensionada e otimizada para acomodar vários casos de uso e requisitos diferentes. Este documento categoriza as configurações do FlexPod Express com base no sistema de storage usado, no FlexPod Express com NetApp FAS e no FlexPod Express com e-Series.

Plataformas FlexPod

Existem três plataformas FlexPod:

- **Centro de dados FlexPod.** Essa plataforma é uma infraestrutura de data center virtual altamente dimensionável, adequada para aplicações empresariais de workload, virtualização, VDI e nuvem pública e privada. O data center FlexPod tem suas próprias especificações, que estão documentadas no "TR-4036: Especificações técnicas do FlexPod Datacenter".
- **FlexPod Express.** Essa plataforma é uma infraestrutura convergente compacta destinada a casos de uso de borda e escritório remoto.

Este documento fornece as especificações técnicas da plataforma FlexPod Express.

Regras do FlexPod

O design do FlexPod permite uma infraestrutura flexível que abrange muitos componentes e versões de software diferentes.

Use os conjuntos de regras como guia para criar ou montar uma configuração válida do FlexPod. Os números e regras listados neste documento são os requisitos mínimos para o FlexPod; eles podem ser expandidos nas famílias de produtos incluídas, conforme necessário para diferentes ambientes e casos de uso.

Configurações de FlexPod validadas em comparação com compatíveis

A arquitetura FlexPod é definida pelo conjunto de regras descritas neste documento. Os componentes de hardware e as configurações de software devem ser suportados pela Lista de Compatibilidade de hardware (HCL) da Cisco e pela "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

Cada Cisco Validated Design (CVD) ou NetApp Verified Architecture (NVA) é uma possível configuração de FlexPod. O Cisco e o NetApp documentam essas combinações de configuração e as validam com testes completos. As implantações do FlexPod que se desviam dessas configurações são totalmente suportadas se seguirem as diretrizes deste documento e todos os componentes estiverem listados como compatíveis nas HCL e NetApp do Cisco "IMT" .

Por exemplo, a adição de controladores de storage adicionais ou servidores Cisco UCS e a atualização de software para versões mais recentes é totalmente suportada se o software, o hardware e as configurações atenderem às diretrizes definidas neste documento.

Software de storage

O FlexPod Express é compatível com sistemas de storage que executam sistemas operacionais NetApp ONTAP ou SANtricity.

NetApp ONTAP

O software NetApp ONTAP é o sistema operacional executado em sistemas de storage AFF e FAS. O ONTAP fornece uma arquitetura de storage altamente dimensionável que permite operações ininterruptas, upgrades sem interrupções e uma infraestrutura de dados ágil.

Para obter mais informações sobre o ONTAP, consulte "Página do produto ONTAP".

Software e-Series SANtricity

O software e-Series SANtricity é o sistema operacional executado em sistemas de storage e-Series. O SANtricity oferece um sistema altamente flexível que atende a diferentes necessidades de aplicativos e oferece alta disponibilidade integrada e uma ampla variedade de recursos de proteção de dados.

Para obter mais informações, consulte "Página do produto SANtricity" .

Requisitos mínimos de hardware

Esta seção descreve os requisitos mínimos de hardware para as diferentes versões do FlexPod Express.

FlexPod Express com NetApp FAS

Os requisitos de hardware para soluções FlexPod Express que usam controladores NetApp FAS para storage subjacente incluem as configurações descritas nesta seção.

Configuração baseada em CIMC (servidores de rack independentes)

A configuração do controlador de gerenciamento integrado (CIMC) da Cisco inclui os seguintes componentes de hardware:

- Dois switches Ethernet padrão 10Gbps em uma configuração redundante (recomenda-se o Cisco Nexus 31108, com suporte para os modelos Cisco Nexus 3000 e 9000)
- Servidores de rack autônomos do Cisco UCS C-Series
- Duas controladoras das séries AFF C190, AFF A250, FAS2600 ou FAS 2700 em uma configuração de par de alta disponibilidade (HA) implantada como um cluster de dois nós

Configuração gerenciada pelo Cisco UCS

A confirmação gerenciada pelo Cisco UCS inclui os seguintes componentes de hardware:

- Dois switches Ethernet padrão 10Gbps em uma configuração redundante (recomenda-se o Cisco Nexus 3524)
- Um chassi do servidor blade de corrente alternada (AC) Cisco UCS 5108
- Duas interconexões de tecido Cisco UCS 6324
- Servidores Cisco UCS B-Series (pelo menos quatro servidores blade Cisco UCS B200 M5)
- Duas controladoras AFF C190, AFF A250, FAS2750 ou FAS2720 em uma configuração de par de HA (exigem duas portas 2 [UTA2] de adaptador de destino unificado disponíveis por controladora)

FlexPod Express com e-Series

Os requisitos de hardware para a configuração inicial do FlexPod Express com e-Series incluem:

- Duas interconexões de tecido Cisco UCS 6324
- Um chassi Cisco UCS Mini 5108 AC2 ou DC2 (as interconexões de malha Cisco UCS 6324 são suportadas apenas no chassi AC2 e DC2)
- Servidores Cisco UCS B-Series (pelo menos dois servidores blade Cisco UCS B200 M4)
- Uma configuração de par de HA de um sistema de storage e-Series E2824 carregado com um mínimo de 12 unidades de disco
- Dois switches Ethernet padrão 10Gbps em uma configuração redundante (switches existentes no data center podem ser usados)

Esses componentes de hardware são necessários para criar uma configuração inicial da solução; servidores blade adicionais e unidades de disco podem ser adicionados conforme necessário. O sistema de storage e-Series E2824 pode ser substituído por uma plataforma superior e também pode ser executado como um sistema all-flash.

Requisitos mínimos de software

Esta seção descreve os requisitos mínimos de software para as diferentes versões do FlexPod Express.

Requisitos de software para o FlexPod Express com NetApp AFF ou FAS

Os requisitos de software do FlexPod Express com NetApp FAS incluem:

- ONTAP 9,1 ou posterior
- Cisco NX-os versão 7,0(3)I6(1) ou posterior
- Na configuração gerenciada pelo Cisco UCS, o Cisco UCS Manager UCS 4,0(1b)

Todos os softwares devem ser listados e suportados no "NetApp IMT". Alguns recursos de software podem exigir versões mais recentes de código do que os mínimos listados em arquiteturas anteriores.

Requisitos de software para FlexPod Express com e-Series

Os requisitos de software do FlexPod Express com e-Series incluem:

- Software e-Series SANtricity 11,30 ou superior
- Cisco UCS Manager 4,0(1b).

Todos os softwares devem ser listados e suportados no "NetApp IMT".

Requisitos de conetividade

Esta seção descreve os requisitos de conetividade para as diferentes versões do FlexPod Express.

Requisitos de conectividade do FlexPod Express com NetApp FAS

Os requisitos de conectividade do FlexPod Express com NetApp FAS incluem:

- Os controladores de storage do NetApp FAS devem ser conectados diretamente aos switches Cisco Nexus, com exceção da configuração gerenciada pelo Cisco UCS, na qual os controladores de storage são conectados às interconexões da malha.
- Nenhum equipamento adicional pode ser colocado em linha entre os componentes principais do FlexPod.
- Os canais de porta virtual (VPCs) são necessários para conetar os switches da série Cisco Nexus 3000/9000 aos controladores de armazenamento NetApp.
- Embora não seja necessário, a ativação do suporte de quadros jumbo é recomendada em todo o ambiente.

Requisitos de conectividade do FlexPod Express com o NetApp e-Series

Os requisitos de conectividade do FlexPod Express com e-Series incluem:

- Os controladores de storage do e-Series devem ser diretamente conectados às interconexões de malha.
- Nenhum equipamento adicional deve ser colocado em linha entre os componentes principais do FlexPod.
- VPCs são necessários entre as interconexões de malha e os switches Ethernet.

Requisitos de conectividade do FlexPod Express com NetApp AFF

Os requisitos de conectividade do FlexPod Express com NetApp AFF incluem:

- Os controladores de storage do NetApp AFF devem ser conectados diretamente aos switches do Cisco Nexus, com exceção da configuração gerenciada por Cisco UCS, na qual os controladores de storage são conectados à malha.
- Nenhum equipamento adicional pode ser colocado em linha entre os componentes principais do FlexPod.
- Os canais de porta virtual (VPCs) são necessários para conetar os switches da série Cisco Nexus 3000/9000 aos controladores de armazenamento NetApp.
- Embora não seja necessário, a ativação do suporte de quadros jumbo é recomendada em todo o ambiente.

Outros requisitos

Os requisitos adicionais para o FlexPod Express incluem o seguinte:

- São necessários contratos de suporte válidos para todos os equipamentos, incluindo:

    - Suporte SMARTnet para equipamentos Cisco
    - Suporte SupportEdge Advisor ou SupportEdge Premium para equipamentos NetApp
- Todos os componentes de software devem ser listados e suportados no "NetApp IMT".
- Todos os componentes de hardware do NetApp devem ser listados e suportados no "NetApp Hardware Universe".
- Todos os componentes de hardware do Cisco devem ser listados e suportados no "HCL do Cisco".

Recursos opcionais

Esta seção descreve os recursos opcionais do FlexPod Express.

Opção de inicialização iSCSI

A arquitetura FlexPod Express utiliza o arranque iSCSI. Os requisitos mínimos para a opção de inicialização iSCSI incluem:

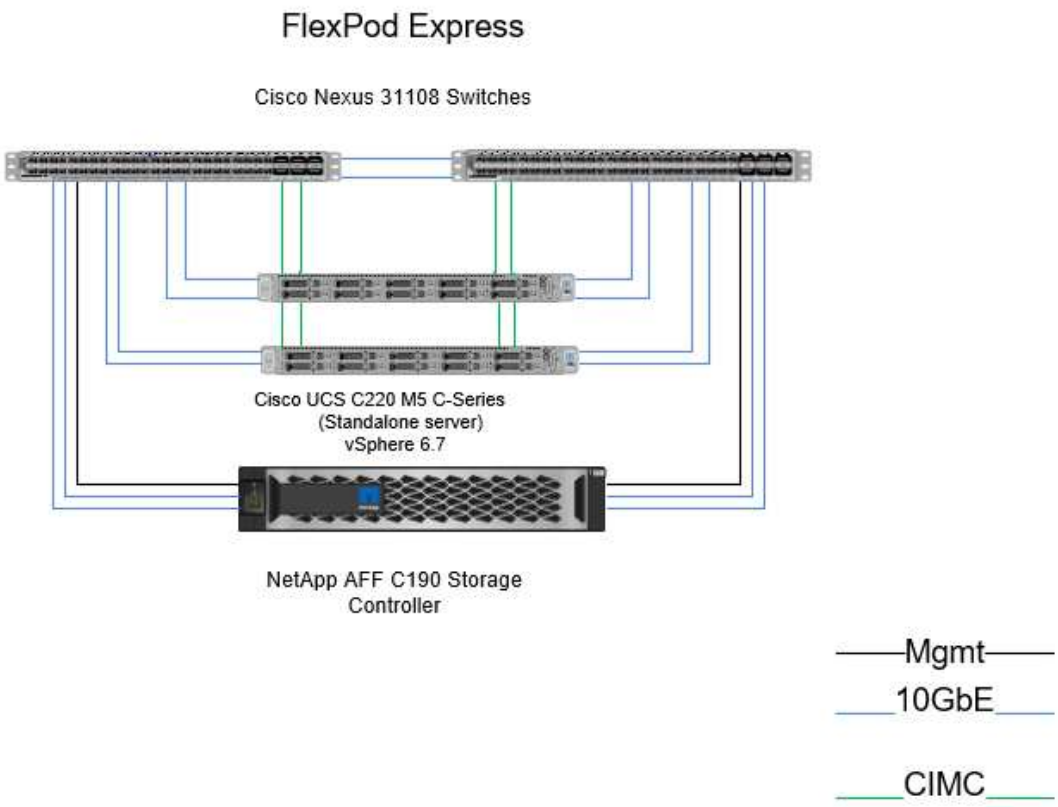
- Uma licença/funcionalidade iSCSI ativada no controlador de armazenamento NetApp
- Um adaptador Ethernet 10Gbps de duas portas em cada nó no par de HA do controlador de storage NetApp
- Um adaptador no servidor Cisco UCS que é capaz de inicializar iSCSI

Opções de configuração

Esta seção fornece mais informações sobre a configuração necessária e validada na arquitetura do FlexPod Express.

FlexPod Express com Cisco UCS C-Series e AFF C190 Series

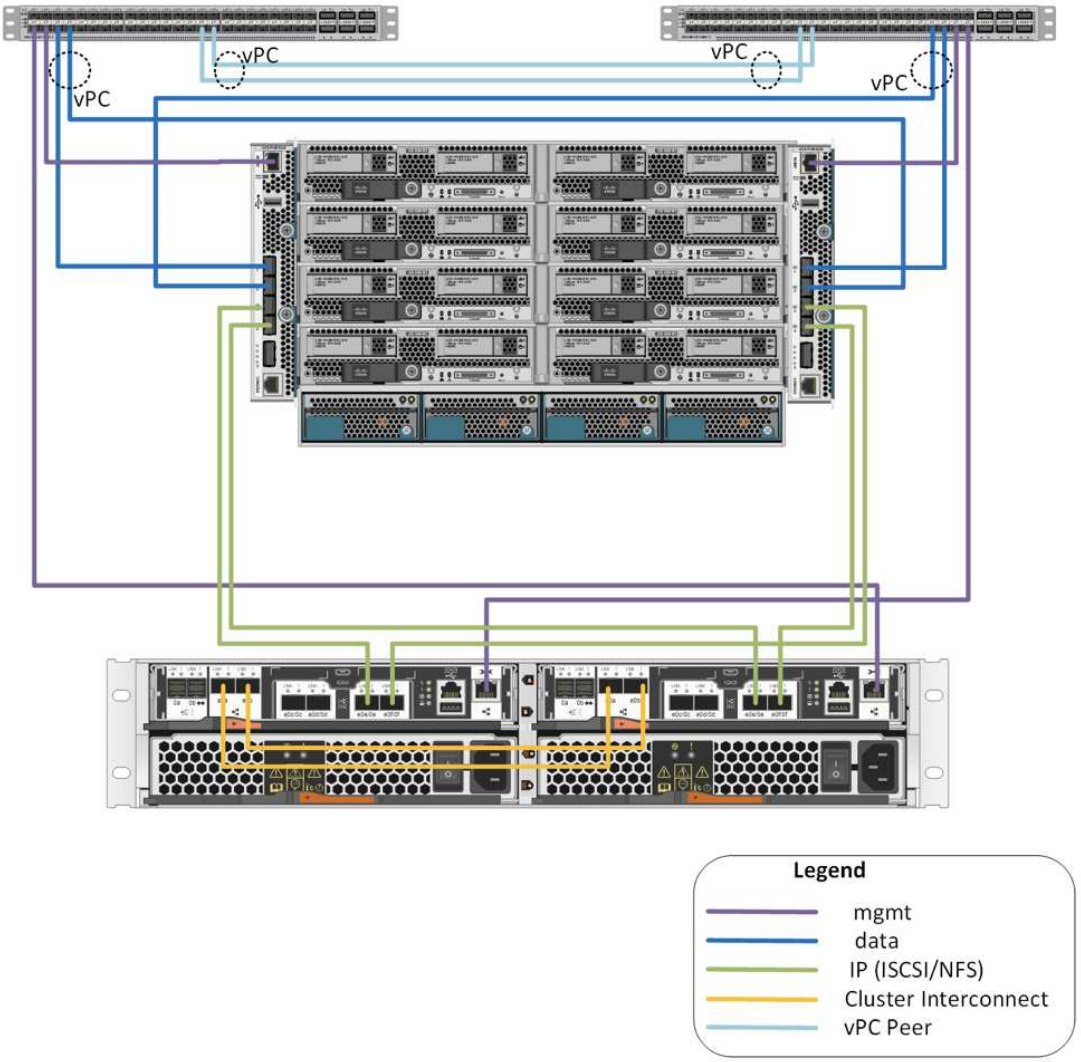
A figura a seguir ilustra o FlexPod Express com a solução Cisco UCS C-Series e AFF C190 series. Esta solução suporta ambos os uplinks 10GbE.



Para obter mais informações sobre essa configuração, consulte o Guia de implantação do FlexPod Express com VMware vSphere 6,7 e NetApp AFF C190 NVA (em andamento).

FlexPod Express com Cisco UCS Mini e AFF A220 e FAS 2750/2720

A figura a seguir ilustra o FlexPod Express com a configuração gerenciada pelo Cisco UCS.



Para obter mais informações sobre essa configuração, "FlexPod Express com VMware vSphere 6.7U1 e NetApp AFF A220 com armazenamento direto - anexado IP - baseado"consulte .

Componentes do Cisco

O Cisco contribui substancialmente para o design e a arquitetura do FlexPod Express; ele contribui com as camadas de computação e rede da solução. Esta seção descreve os componentes do Cisco UCS e do Cisco Nexus que estão disponíveis para o FlexPod Express.

Opções de servidor blade Cisco UCS B-Series

Os blades da série B do Cisco UCS atualmente suportados na plataforma Cisco UCS Mini são B200 M5 e B420 M4. Outros blades serão listados na tabela a seguir à medida que forem suportados na plataforma Cisco UCS Mini.

Servidor Cisco UCS B-Series	Número de peça	Especificações técnicas
Cisco UCS B200 M5	UCSB-B200-M5	https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-b200-m5-blade-server/model.html
Cisco UCS B200 M4	UCSB-B200-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b200m4-specsheet.pdf
Cisco UCS B420 M4	UCSB-B420-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b420m4-spec-sheet.pdf

Opções de servidor de rack Cisco UCS C-Series

Os blades da série C do Cisco UCS estão disponíveis nas variedades de unidade de um rack e dois rack (RU), com várias opções de CPU, memória e e e/S. Os números de peça listados na tabela a seguir são para o servidor base; eles não incluem CPUs, memória, unidades de disco, placas PCIe ou Cisco FEX. Várias opções de configuração estão disponíveis e suportadas no FlexPod.

Servidor de rack Cisco UCS C-Series	Número de peça	Especificações técnicas
Cisco UCS C220 M4	UCSC-C220-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
Cisco UCS C240 M4	UCSC-C240-M4S	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c240m4-sff-spec-sheet.pdf
Cisco UCS C460 M4	UCSC-C460-M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c460m4_specsheet.pdf

Switches Cisco Nexus

Switches redundantes são necessários para todas as arquiteturas FlexPod Express.

O FlexPod Express com a arquitetura NetApp AFF ou FAS foi desenvolvido com o switch Cisco Nexus 31108. O FlexPod Express com a arquitetura Cisco UCS Mini (Cisco UCS- Managed) é validado usando o switch Cisco Nexus 3524. Essa configuração também pode ser implantada com um switch padrão.

O FlexPod Express com e-Series pode ser implantado com um switch padrão.

A tabela a seguir lista os números de peça para o chassi da série Cisco Nexus; eles não incluem módulos adicionais SFP ou adicionais.

Switch Cisco Nexus Series	Número de peça	Especificações técnicas
Cisco Nexus 3048	N3K-C3048TP-1GE	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-685363.html
Cisco Nexus 31108	N3K-C31108PC-V	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 9396	N9K-C9396PX	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-729405.html
Cisco Nexus 3172	N3K-C3172	https://www.cisco.com/c/en/us/products/collateral/switches/nexus-3000-series-switches/data_sheet_c78-729483.html

Opções de licenciamento do suporte da Cisco

Contratos de suporte válidos SMARTnet são necessários em todos os equipamentos Cisco na arquitetura FlexPod Express.

> As licenças necessárias e os números de peça dessas licenças devem ser verificados pelo seu representante de vendas, pois podem diferir para diferentes produtos.

A tabela a seguir lista as opções de licenciamento de suporte do Cisco.

Licenciamento do suporte da Cisco	Guia de licença
SMARTnet 24x7x4	http://www.cisco.com/web/services/portfolio/product-technical-support/smartnet/index.html

Componentes do NetApp

Os controladores de storage do NetApp fornecem a base de storage na arquitetura do FlexPod Express para inicialização e storage de dados de aplicações. Esta seção lista as diferentes opções do NetApp na arquitetura do FlexPod Express.

Opções do controlador de storage NetApp

NetApp FAS

Controladores redundantes da série AFF C190, AFF A220 ou FAS2750 são necessários na arquitetura do FlexPod Express. Os controladores executam o software ONTAP. Ao encomendar os controladores de armazenamento, a versão de software preferida pode ser pré-carregada nos controladores. Para o ONTAP, o cluster pode ser implantado com um par de switches de interconexão de cluster ou em uma configuração de cluster sem switch.

Os números de peça listados na tabela a seguir são para um controlador vazio. Diferentes opções e configurações estão disponíveis com base na plataforma de storage selecionada. Consulte o seu

representante de vendas para obter detalhes sobre estes componentes adicionais.

Controlador de storage	Número de peça FAS	Especificações técnicas
FAS2750	Com base nas opções individuais escolhidas	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
FAS2720	Com base nas opções individuais escolhidas	https://www.netapp.com/us/products/storage-systems/hybrid-flash-array/fas2700.aspx
AFF C190	Com base nas opções individuais escolhidas	https://www.netapp.com/us/products/entry-level-aff.aspx
AFF A220	Com base nas opções individuais escolhidas	https://www.netapp.com/us/documentation/all-flash-fas.aspx
FAS2620	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
FAS2650	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx

Storage e-Series

Na arquitetura do FlexPod Express, é necessário um par de HA de controladores da série NetApp E2800. Os controladores executam o SANtricity os.

Os números de peça listados na tabela a seguir são para um controlador vazio. Diferentes opções e configurações estão disponíveis com base na plataforma de storage selecionada. Consulte o seu representante de vendas para obter detalhes sobre estes componentes adicionais.

Controlador de storage	Número de peça	Especificações técnicas
E2800	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/e2800/e2800-tech-specs.aspx

Módulos de expansão Ethernet NetApp

NetApp FAS

A tabela a seguir lista as opções do adaptador NetApp FAS10GbE.

Componente	Número de peça	Especificações técnicas
NetApp X1117A	X1117A-R6	https://library.netapp.com/ecm/ecm_download_file/ECMM1280307

Os sistemas de storage das séries FAS2500 e 2600 têm portas integradas de 10GbE GbE.

O adaptador NetApp X1117A destina-se a sistemas de armazenamento FAS8020.

Storage e-Series

A tabela a seguir lista as opções do adaptador e-Series 10GbE.

Componente	Número de peça
10GbE portas iSCSI/16GB FC de 4 GB	X-56025-00-0E-C
10GbE portas iSCSI/16GB FC de 2 GB	X-56024-00-0E-C

> Os sistemas de storage da série E2824 têm portas integradas de 10GbE GbE.
>
> A placa de interface de host (HIC) de 4 portas iSCSI/16GB FC de 10GbE GB pode ser usada para densidade de porta adicional.

As portas integradas e o HIC podem funcionar como adaptadores iSCSI ou adaptadores FC, dependendo do recurso ativado no SANtricity os.

Para obter mais informações sobre as opções de adaptadores suportados, consulte a seção adaptador "NetApp Hardware Universe" de .

Discos e compartimentos de disco NetApp

NetApp FAS

É necessário um mínimo de um compartimento de disco NetApp para os controladores de storage. O tipo de compartimento NetApp selecionado determina quais tipos de unidade estão disponíveis nesse compartimento.

As séries FAS2700 e FAS2600 de controladores são oferecidas como uma configuração que inclui controladores de armazenamento duplo e discos alojados dentro do mesmo chassi. Essa configuração é oferecida com unidades SATA ou SAS; portanto, não são necessários compartimentos de disco externos adicionais, a menos que os requisitos de desempenho ou capacidade ditem mais fusos.

> Todos os números de peça do compartimento de disco são para o compartimento vazio com duas PSUs CA. Consulte o seu representante de vendas para obter números de peça adicionais.
>
> Os números de peça da unidade de disco variam de acordo com o tamanho e o fator de forma do disco que você pretende comprar. Consulte o seu representante de vendas para obter números de peça adicionais.

A tabela a seguir lista as opções do compartimento de disco NetApp, juntamente com as unidades compatíveis com cada tipo de compartimento, que podem ser encontradas no NetApp Hardware Universe. Siga o link Hardware Universe, selecione a versão do ONTAP que você está usando e, em seguida, selecione o tipo de prateleira. Na imagem do compartimento, clique em unidades compatíveis para ver as unidades compatíveis com versões específicas do ONTAP e das gavetas de disco.

Compartimento de disco	Número de peça	Especificações técnicas
DS212C	DS212C-0-12	"Especificações técnicas dos compartimentos de disco e Mídia de armazenamento unidades compatíveis no NetApp Hardware Universe"

Compartimento de disco	Número de peça	Especificações técnicas
DS224C	DS224C-0-24	"Especificações técnicas dos compartimentos de disco e Mídia de armazenamento unidades compatíveis no NetApp Hardware Universe"
DS460C	DS460C-0-60	"Especificações técnicas dos compartimentos de disco e Mídia de armazenamento unidades compatíveis no NetApp Hardware Universe"
DS2246	X559A-R6	"Especificações técnicas dos compartimentos de disco e Mídia de armazenamento unidades compatíveis no NetApp Hardware Universe"
DS4246	X24M-R6	"Especificações técnicas dos compartimentos de disco e Mídia de armazenamento unidades compatíveis no NetApp Hardware Universe"
DS4486	DS4486-144TB-R5-C	"Especificações técnicas dos compartimentos de disco e Mídia de armazenamento unidades compatíveis no NetApp Hardware Universe"

Storage e-Series

É necessário no mínimo um compartimento de disco NetApp para controladores de storage que não hospedam nenhuma unidade em seu chassi. O tipo de compartimento NetApp selecionado determina quais tipos de unidade estão disponíveis nesse compartimento.

A série E2800 de controladores é oferecida como uma configuração que inclui controladores de storage duplos e discos alojados em um compartimento de disco compatível. Essa configuração é oferecida com unidades SSD ou SAS.

Os números de peça da unidade de disco variam de acordo com o tamanho e o fator de forma do disco que você pretende comprar. Consulte o seu representante de vendas para obter números de peça adicionais.

A tabela a seguir lista as opções do compartimento de disco NetApp e as unidades compatíveis com cada tipo de compartimento, que podem ser encontradas no NetApp Hardware Universe. Siga o link Hardware Universe, selecione a versão do ONTAP que você está usando e, em seguida, selecione o tipo de prateleira. Na imagem do compartimento, clique em unidades compatíveis para ver as unidades compatíveis com versões específicas do ONTAP e das gavetas de disco.

Compartimento de disco	Número de peça	Especificações técnicas
DE460C	E-X5730A-DM-0E-C	"Especificações técnicas dos compartimentos de disco unidades compatíveis no NetApp Hardware Universe"
DE224C	E-X5721A-DM-0E-C	"Especificações técnicas dos compartimentos de disco unidades compatíveis no NetApp Hardware Universe"
DE212C	E-X5723A-DM-0E-C	"Especificações técnicas dos compartimentos de disco unidades compatíveis no NetApp Hardware Universe"

Opções de licenciamento do software NetApp

NetApp FAS

A tabela a seguir lista as opções de licenciamento do software NetApp FAS.

Licenciamento de software da NetApp	Número de peça	Especificações técnicas
Licença de cluster de base	Consulte sua equipe de vendas da NetApp para obter mais informações sobre licenciamento.	

Storage e-Series

A tabela a seguir lista as opções de licenciamento do software e-Series.

Licenciamento do software NetApp	Número de peça	Especificações técnicas
Caraterísticas padrão	Consulte sua equipe de vendas da NetApp para obter mais informações sobre licenciamento.	
Funcionalidades premium		

Opções de licenciamento do suporte da NetApp

As licenças SupportEdge Premium são necessárias e os números de peça dessas licenças variam de acordo com as opções selecionadas no design do FlexPod Express.

NetApp FAS

A tabela a seguir lista as opções de licenciamento de suporte do NetApp para o NetApp FAS.

Licenciamento do suporte da NetApp	Número de peça	Especificações técnicas
SupportEdge Premium4 horas no local; meses: 36	CS-O2-4HR	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf

Storage e-Series

A tabela a seguir lista as opções de licenciamento de suporte do NetApp para storage e-Series.

Licenciamento do suporte da NetApp	Número de peça	Especificações técnicas
Suporte a hardware Premium 4 horas no local; meses: 36	SVC-O2-4HR-E	https://www.netapp.com/pdf.html?item=/media/19784-ds-3873.pdf
Suporte de software	SW-SSP-O2-4HR-E	
Instalação inicial	SVC-INST-O2-4HR-E	

Requisitos de alimentação e cabeamento

Esta seção descreve os requisitos mínimos de energia e cabeamento para um design do FlexPod Express.

Requisitos de energia

Os requisitos de energia são baseados nas especificações dos EUA e assumem o uso de energia CA. Outros países podem ter diferentes requisitos de energia. As opções de alimentação de corrente contínua (DC) também estão disponíveis para a maioria dos componentes. Para obter dados adicionais sobre a potência máxima necessária, bem como outras informações detalhadas sobre a energia, consulte as especificações técnicas detalhadas para cada componente de hardware.

Para obter dados de energia detalhados do Cisco UCS, consulte "Calculadora de energia Cisco UCS".

A tabela a seguir lista as portas de alimentação necessárias por dispositivo.

Switches Cisco Nexus	São necessários cabos de alimentação
Cisco Nexus 3048	Cabos de alimentação de 2x C13 V/C14 V para cada switch da série Cisco Nexus 3000
Cisco Nexus 3524	Cabos de alimentação de 2x C13 V/C14 V para cada switch da série Cisco Nexus 3000
Cisco Nexus 9396	Cabos de alimentação de 2x C13 V/C14 V para cada switch da série Cisco Nexus 9000

Chassi do Cisco UCS	São necessários cabos de alimentação
Cisco UCS 5108	2 CAB-US515P-C19-US/CAB-US520-C19-US para cada chassi Cisco UCS

Servidores Cisco UCS B-Series	São necessários cabos de alimentação
Cisco UCS B200 M4	N/A; o servidor blade é alimentado pelo chassi
Cisco UCS B420 M4	N/A; o servidor blade é alimentado pelo chassi
Cisco UCS B200 M5	N/A; o servidor blade é alimentado pelo chassi
Cisco UCS B480 M5	N/A; o servidor blade é alimentado pelo chassi

Servidores Cisco UCS C-Series	Portas de alimentação necessárias
Cisco UCS C220 M4	2 cabos de alimentação C13/C14 para cada servidor Cisco UCS
Cisco UCS C240 M4	
Cisco UCS C460 M4 Cisco UCS C220 M5 Cisco UCS C240 M5 Cisco UCS C480 M5	

Controladores NetApp FAS	Portas de alimentação necessárias (por par de HA)
FAS2554	2 x C13/C14
FAS2552	2 x C13/C14
FAS2520	2 x C13/C14
FAS8020	2 x C13/C14

Controladores e-Series	Portas de alimentação necessárias (por par de HA)
E2824	2 x C14/C20

Compartimentos de disco NetApp FAS	Portas de alimentação necessárias
DS212C	2 x C13/C14
DS224C	2 x C13/C14
DS460C	2 x C13/C14
DS2246	2 x C13/C14
DS4246	4 x C13/C14

Compartimentos de disco e-Series	Portas de alimentação necessárias
DE460C	2 x C14/C20
DE224C	2 x C14/C20
DE212C	2 x C14/C20

Requisitos mínimos de cabos

Esta seção descreve os requisitos mínimos de cabo para um design FlexPod Express. A maioria das implementações do FlexPod requer cabos adicionais, mas o número varia de acordo com o tamanho e o escopo da implantação.

A tabela a seguir lista o número mínimo de cabos necessários para cada dispositivo.

Switches Cisco Nexus 3000 Series	Cabos necessários
Cisco Nexus 31108	Pelo menos dois cabos de fibra 10GbE ou Twinax por switch
Cisco Nexus 3172PQ	
Cisco Nexus 3048	
Cisco Nexus 3524	
Cisco Nexus 9396	
DS212C	
DS2246	O número de cabos SAS depende da configuração específica das gavetas de disco
DS460C	
DS224C	
DS4246	
E2800	• Pelo menos um cabo Gigabit Ethernet (1GbE) para gerenciamento por controlador • Pelo menos dois cabos 10GbE por controladora (para iSCSI) ou dois cabos FC que atendem aos requisitos de velocidade
DE460C	2 cabos mini-SAS HD por prateleira de disco
DE224C	2 cabos mini-SAS HD por prateleira de disco
DE212C	2 cabos mini-SAS HD por prateleira de disco

Especificações técnicas e Referências

Esta seção descreve especificações técnicas importantes adicionais para cada um dos componentes do FlexPod Express.

Servidores blade Cisco UCS B-Series

A tabela a seguir lista as opções do servidor blade da série B do Cisco UCS.

Componente	Cisco UCS B200 M4	Cisco UCS B420 M4	Cisco UCS B200 M5
Suporte do processador	Intel Xeon E5-2600	Intel Xeon E5-4600	Processadores escaláveis Intel Xeon
Capacidade máxima de memória	DIMMs de 24 GB para um máximo de 768GB GB	DIMMs de 48 GB para um máximo de 3TB GB	DIMMs de 24 GB para um máximo de 3072GB GB
Tamanho e velocidade da memória	32GB DDR4; 2133MHz	64GB DDR4; 2400MHz	16GB, 32GB, 64GB e 128GB DDR4; 2666MHz
Suporte de inicialização SAN	Sim	Sim	Sim
Slots de adaptador de e/S mezzanine	2	3	2, frontal e traseiro, incluindo suporte de GPU

Componente	Cisco UCS B200 M4	Cisco UCS B420 M4	Cisco UCS B200 M5
Taxa de transferência máxima de e/S.	80Gbps	160Gbps	80Gbps

Servidores de rack Cisco UCS C-Series

A tabela a seguir lista as opções do servidor de rack Cisco UCS C-Series.

Componente	Cisco UCS C220 M4	Cisco UCS C240 M4	Cisco UCS C460 M4	Cisco UCS C220 M5
Suporte do processador	1 ou 2 Intel E5-2600 series	1 ou 2 Intel Xeon série E5-2600	2 ou 4 Intel Xeon série E7-4800/8800	Processadores escaláveis Intel Xeon (1 ou 2)
Capacidade máxima de memória	1,5 GB	1,5 TB	6 TB	3072 GB
Slots PCIe	2	6	10	2
Fator forma	1RU	2RU	4RU	1 RU

A tabela a seguir lista as fichas técnicas das opções do servidor de rack Cisco UCS C-Series.

Componente	Datasheet do Cisco UCS
Cisco UCS C220 M4	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m4-sff-spec-sheet.pdf
Cisco UCS C240 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m4-rack-server/datasheet-c78-732455.html
Cisco UCS C460 M4	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c460-m4-rack-server/datasheet-c78-730907.html
Cisco UCS C220 M5	https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/c220m5-sff-specsheet.pdf

Switches Cisco Nexus 3000 Series

A tabela a seguir lista as opções de switch da série Cisco Nexus 3000.

Componente	Cisco Nexus 3048	Cisco Nexus 3524	Cisco Nexus 31108	Cisco Nexus 3172PQ
Fator forma	1RU	1RU	1RU	1 RU

Componente	Cisco Nexus 3048	Cisco Nexus 3524	Cisco Nexus 31108	Cisco Nexus 3172PQ
Máximo de 1Gbps portas	48	24	48 (10/40/100Gbps)	Portas de 72 1 GbE/10GbE GbE, ou 48 1 GbE/10GbE GbE mais seis portas de 40GbE GbE
Taxa de encaminhamento	132Mbps	360Mbps	1.2Bpps	1Bpps
Suporte a quadro jumbo	Sim	Sim	Sim	Sim

A tabela a seguir lista as fichas técnicas das opções de switch da série Cisco Nexus 3000.

Componente	Detalhes completos do Cisco Nexus
Cisco Nexus 31108	http://www.cisco.com/c/en/us/products/switches/nexus-31108pc-v-switch/index.html
Cisco Nexus 3172PQ	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3048	https://www.cisco.com/c/en/us/products/switches/nexus-3048-switch/index.html
Cisco Nexus 3172PQ-XL	https://www.cisco.com/c/en/us/products/switches/nexus-3172pq-switch/index.html
Cisco Nexus 3548 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524 XL	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html
Cisco Nexus 3548	https://www.cisco.com/c/en/us/products/switches/nexus-3548-x-switch/index.html
Cisco Nexus 3524	https://www.cisco.com/c/en/us/products/switches/nexus-3524-x-switch/index.html

A tabela a seguir lista as opções de switch da série Cisco Nexus 9000.

Componente	Cisco Nexus 9396	Cisco Nexus 9372
Fator forma	2RU	1RU
Máximo de portas	60	54
10Gbps portas de uplink SFP	48	48

A tabela a seguir lista as fichas técnicas das opções de switch da série Cisco Nexus 9000.

Componente	Datasheet do Cisco Nexus
Cisco Nexus 9396	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Cisco Nexus 9372	http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/datasheet-c78-736967.html
Nexus 9396X	https://www.cisco.com/c/en/us/products/switches/nexus-9396px-switch/index.html?dtid=osscdc000283

Controladores de storage NetApp FAS

A tabela a seguir lista as opções atuais do controlador de armazenamento NetApp FAS.

Componente atual	FAS2620	FAS2650
Configuração	2 controladoras em um chassi de 2U U.	2 controladoras em um chassi de 4U U.
Capacidade bruta máxima	1440 TB	1243 TB
Unidades internas	12	24
Número máximo de unidades (internas e externas)	144	144
Tamanho máximo do volume	100 TB	
Tamanho máximo de agregado	4 TB	
Número máximo de LUNs	2.048 gb por controlador	
Rede de armazenamento suportada	ISCSI, FC, FCoE, NFS e CIFS	
Número máximo de volumes NetApp FlexVol	1.000 gb por controlador.	
Número máximo de cópias Snapshot do NetApp	255.000 gb por controlador	
Armazenamento em cache inteligente máximo de flash NetApp Pool	24 TB	

Para obter detalhes sobre a opção de controlador de armazenamento FAS, consulte "Modelos FAS" a seção do Hardware Universe. Para AFF, "Modelos AFF" consulte a secção.

A tabela a seguir lista as caraterísticas de um sistema de controlador FAS8020.

Componente	FAS8020
Configuração	2 controladoras em um chassi de 3U U.
Capacidade bruta máxima	2880 TB

Componente	FAS8020
Número máximo de unidades	480
Tamanho máximo do volume	70 TB
Tamanho máximo de agregado	324 TB
Número máximo de LUNs	8.192 gb por controlador
Rede de armazenamento suportada	ISCSI, FC, NFS e CIFS
Número máximo de volumes FlexVol	1.000 gb por controlador
Número máximo de cópias Snapshot	255.000 gb por controlador
Armazenamento em cache inteligente máximo de NetApp Flash Cache	3 TB
Armazenamento máximo de dados em cache do Flash Pool	24 TB

A tabela a seguir lista as fichas técnicas das controladoras de storage NetApp.

Componente	Datasheet do controlador de storage
Série FAS2600	http://www.netapp.com/us/products/storage-systems/fas2600/fas2600-tech-specs.aspx
Série FAS2500	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
Série FAS8000	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

Adaptadores Ethernet NetApp FAS

A tabela a seguir lista os adaptadores NetApp FAS 10GbE.

Componente	X1117A-R6
Contagem de portas	2
Tipo de adaptador	SFP com fibra

O adaptador SFP X1117A-R6 é suportado em controladores da série FAS8000.

Os sistemas de storage das séries FAS2600 e FAS2500 têm portas integradas de 10GbE GbE. Para obter mais informações, consulte "Folha de dados do adaptador NetApp 10GbE" .

Para obter mais detalhes do adaptador com base no modelo AFF ou FAS, consulte "Secção do adaptador" no Hardware Universe.

Compartimentos de disco NetApp FAS

A tabela a seguir lista as opções atuais do compartimento de disco do NetApp FAS.

Componente	DS460C	DS224C	DS212C	DS2246	DS4246
Fator forma	4RU	2RU	2RU	2RU	4RU
Unidades por compartimento	60	24	12	24	24
Fator forma da unidade	fator forma grande de 3,5"	fator forma pequeno de 2,5"	fator forma grande de 3,5"	fator forma pequeno de 2,5"	fator forma grande de 3,5"
Módulos de e/S de gaveta	Dois módulos IOM12	Dois módulos IOM12	Dois módulos IOM12	Dois módulos IOM6	Dois módulos IOM6

Para obter mais informações, consulte o datasheet do shelves de disco do NetApp.

Para obter mais informações sobre os compartimentos de disco, consulte o NetApp Hardware Universe "Seção compartimentos de disco" .

Unidades de disco NetApp FAS

As especificações técnicas dos discos NetApp incluem tamanho do fator forma, capacidade do disco, RPM do disco, controladores de suporte e requisitos de versão do Data ONTAP e estão localizadas na seção unidades no "NetApp Hardware Universe".

Controladores de storage e-Series

A tabela a seguir lista as opções atuais do controlador de storage do e-Series.

Componente atual	E2812	E2824	E2860
Configuração	2 controladoras em um chassi de 2U U.	2 controladoras em um chassi de 2U U.	2 controladoras em um chassi de 4U U.
Capacidade bruta máxima	1800 TB	1756,8 TB	1800 TB
Unidades internas	12	24	60
Número máximo de unidades (internas e externas)	180		
SSD máximo	120		
Tamanho máximo de volume para o volume do pool de discos	1024 TB		
Máximo de pools de discos	20		
Rede de armazenamento suportada	ISCSI e FC		
Número máximo de volumes	512		

A tabela a seguir lista as fichas técnicas do controlador de storage e-Series atual.

Componente	Datasheet do controlador de storage
E2800	https://www.netapp.com/pdf.html?item=/media/7573-ds-3805.pdf

Adaptadores e-Series

A tabela a seguir lista os adaptadores e-Series.

Componente	X-56023-00-0E-C	X-56025-00-0E-C	X-56027-00-0E-C	X-56024-00-0E-C	X-56026-00-0E-C
Contagem de portas	2	4	4	2	2
Tipo de adaptador	10Gb base-T	FC de 16G GB e iSCSI de 10GbE GB	SAS	FC de 16G GB e iSCSI de 10GbE GB	SAS

Compartimentos de disco e-Series

A tabela a seguir lista as opções do compartimento de disco e-Series.

Componente	DE212C	DE224C	DE460C
Fator forma	2RU	2RU	4RU
Unidades por compartimento	12	24	60
Fator forma da unidade	fator forma pequeno de 2,5" 3,5"	2,5"	fator forma pequeno de 2,5" 3,5"
Módulos de e/S de gaveta	IOM12	IOM12	IOM12

Unidades de disco e-Series

As especificações técnicas das unidades de disco NetApp incluem tamanho do fator forma, capacidade do disco, RPM do disco, controladores de suporte e requisitos de versão do SANtricity e estão localizadas na seção unidades em "NetApp Hardware Universe".

Arquiteturas e equipamentos anteriores

O FlexPod é uma solução flexível que permite aos clientes utilizar equipamentos novos e existentes atualmente à venda pela Cisco e pela NetApp. Ocasionalmente, certos modelos de equipamentos da Cisco e da NetApp são designados como fim de vida útil.

Mesmo que esses modelos de equipamentos não estejam mais disponíveis, os clientes que compraram um desses modelos antes da data de fim de venda podem usar esse equipamento em uma configuração FlexPod.

Além disso, as arquiteturas FlexPod Express são atualizadas periodicamente para introduzir o hardware e o software mais recentes da Cisco e da NetApp à solução FlexPod Express. Esta seção lista as arquiteturas e hardware anteriores do FlexPod Express usados dentro delas.

Arquiteturas FlexPod Express anteriores

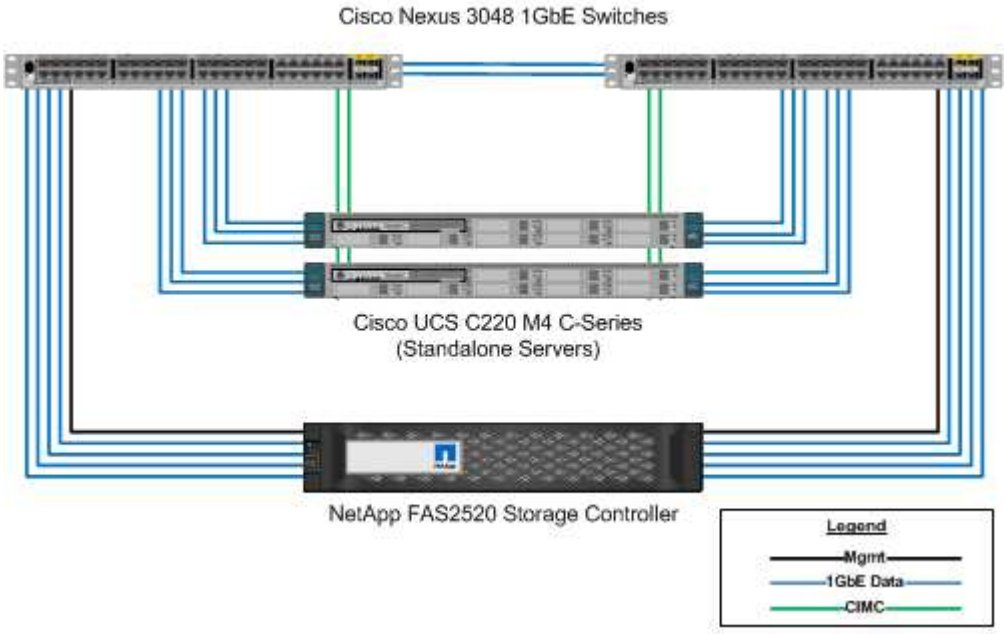
Esta seção descreve as arquiteturas FlexPod Express anteriores.

Configurações pequenas e médias do FlexPod Express

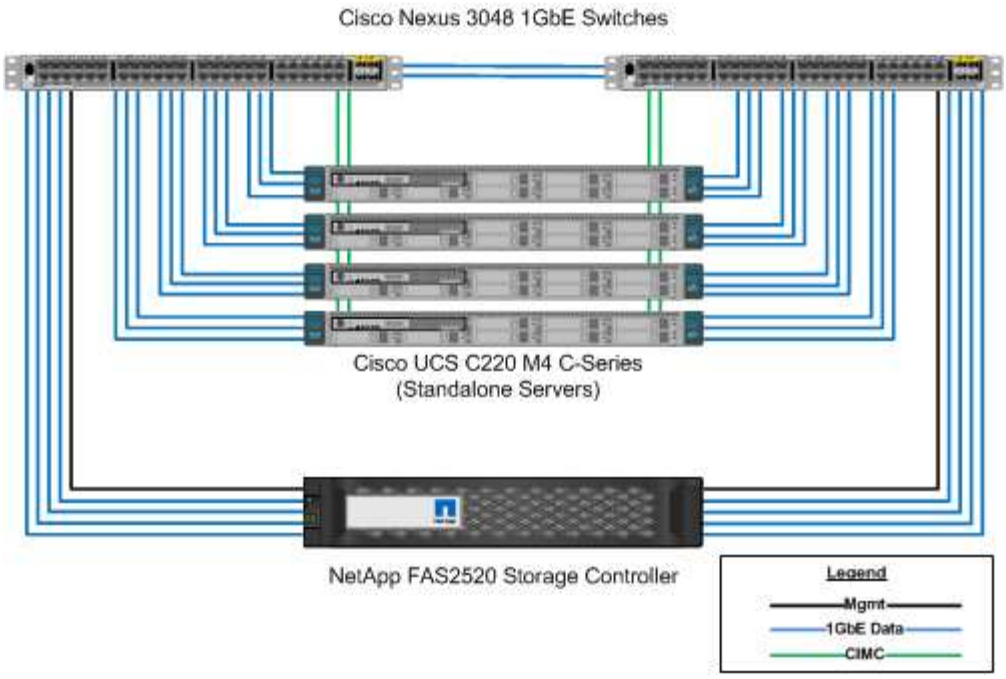
As configurações pequenas e médias do FlexPod Express incluem os seguintes componentes:

- Dois switches Cisco Nexus 3048 em uma configuração redundante
- Pelo menos dois servidores de montagem em rack Cisco UCS C-Series
- Dois controladores das séries FAS2200 ou FAS2500 em uma configuração de par de HA

A figura a seguir ilustra a configuração pequena do FlexPod Express.



A figura a seguir ilustra a configuração média do FlexPod Express.

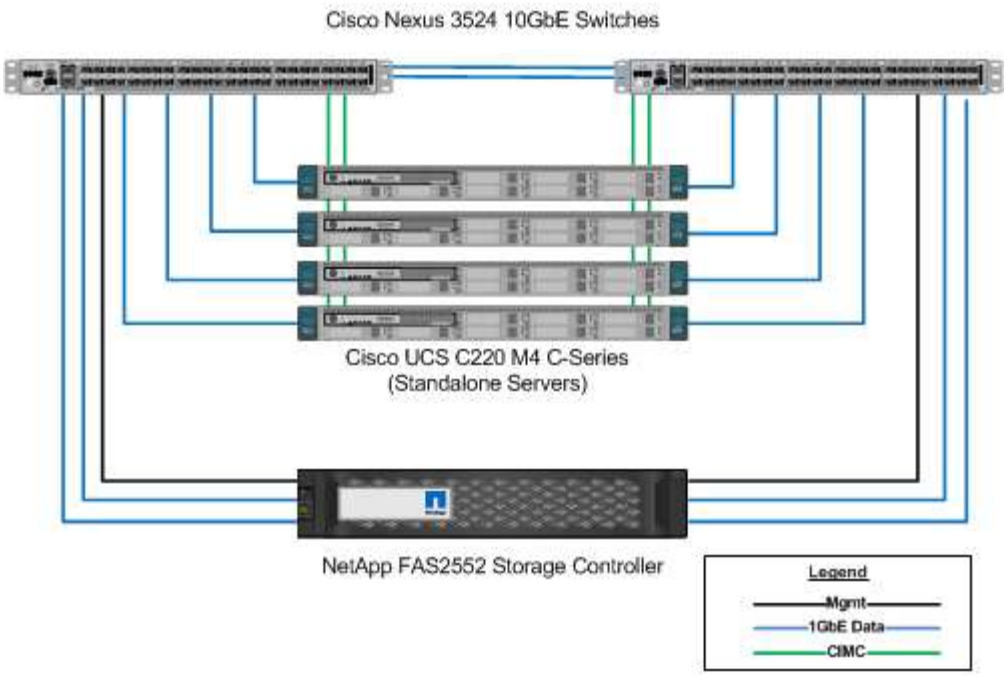


Configuração grande do FlexPod Express

A configuração do FlexPod Express Large inclui os seguintes componentes:

- Dois switches da série Cisco Nexus 3500 ou Cisco Nexus 9300 em uma configuração redundante
- Pelo menos dois servidores de montagem em rack Cisco UCS C-Series
- Duas controladoras FAS2552, FAS2554 ou FAS8020 em uma configuração de par de HA (requer duas portas de 10GbE GbE por controladora)
- Um compartimento de disco NetApp com qualquer tipo de disco suportado (quando o FAS8020 é usado)

A figura a seguir ilustra a configuração grande do FlexPod Express.



Arquiteturas verificadas anteriores do FlexPod Express

As arquiteturas verificadas anteriores do FlexPod Express ainda são suportadas. Os documentos de arquitetura e implantação incluem:

- "FlexPod Express com Cisco UCS C-Series e NetApp FAS2500 Series"
- "FlexPod Express com VMware vSphere 6,0: Configurações pequenas e médias"
- "FlexPod Express com VMware vSphere 6,0: Configuração grande"
- "FlexPod Express com Microsoft Windows Server 2012 R2 Hyper-V: Configurações pequenas e médias"
- "FlexPod Express com Microsoft Windows Server 2012 R2 Hyper-V: Configuração grande"

Hardware anterior

A tabela a seguir lista o hardware usado em arquiteturas FlexPod Express anteriores.

Hardware usado em arquiteturas anteriores	Especificações técnicas (se disponíveis)
Cisco UCS C220 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c220-m3-rack-server/data_sheet_c78-700626.html
Cisco UCS C24 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706103.html
Cisco UCS C22 M3	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/data_sheet_c78-706101.html
Cisco UCS C240 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c240-m3-rack-server/data_sheet_c78-700629.html
Cisco UCS C260 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/c260m2_specsheet.pdf

Hardware usado em arquiteturas anteriores	Especificações técnicas (se disponíveis)
Cisco UCS C420 M3	http://www.cisco.com/en/US/products/ps12770/index.html
Cisco UCS C460 M2	http://www.cisco.com/en/US/prod/collateral/ps10265/ps10493/ps11587/spec_sheet_c17-662220.pdf
Cisco UCS B200 M3	http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b200-m3-blade-server/data_sheet_c78-700625.html
Cisco UCS B420 M3	N/A.
Cisco UCS B22 M3	http://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/b22m3_specsheet.pdf
Cisco Nexus 3524	http://www.cisco.com/c/en/us/products/switches/nexus-3524-switch/index.html
FAS2240	
FAS2220	http://www.netapp.com/us/products/storage-systems/fas2200/fas2200-tech-specs.aspx
DS4243	N/A.

Equipamento legado

A tabela a seguir lista as opções do controlador de storage herdado do NetApp.

Controlador de storage	Número de peça FAS	Especificações técnicas
FAS2520	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2552	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS2554	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/fas2500/fas2500-tech-specs.aspx
FAS8020	Com base nas opções individuais escolhidas	http://www.netapp.com/us/products/storage-systems/fas8000/fas8000-tech-specs.aspx

A tabela a seguir lista as opções do compartimento de disco herdado do NetApp para o NetApp FAS.

Compartimento de disco	Número de peça	Especificações técnicas
DE1600	E-X5682A-DM-0E-R6-C	"Especificações técnicas dos compartimentos de disco unidades compatíveis no NetApp Hardware Universe"

Compartimento de disco	Número de peça	Especificações técnicas
DE5600	E-X4041A-12-R6	"Especificações técnicas dos compartimentos de disco unidades compatíveis no NetApp Hardware Universe"
DE6600	X-48564-00-R6	"Especificações técnicas dos compartimentos de disco unidades compatíveis no NetApp Hardware Universe"

Controladores FAS legados NetApp

A tabela a seguir lista as opções legadas do controlador NetApp FAS.

Componente atual	FAS2554	FAS2552	FAS2520
Configuração	2 controladoras em um chassi de 4U U.	2 controladoras em um chassi de 2U U.	2 controladoras em um chassi de 2U U.
Capacidade bruta máxima	576 TB	509 TB	336 TB
Unidades internas	24	24	12
Número máximo de unidades (internas e externas)	144	144	84
Tamanho máximo do volume	60 TB		
Tamanho máximo de agregado	120 TB		
Número máximo de LUNs	2.048 gb por controlador		
Rede de armazenamento suportada	ISCSI, FC, FCoE, NFS e CIFS		ISCSI, NFS e CIFS
Número máximo de volumes NetApp FlexVol	1.000 gb por controlador		
Número máximo de cópias Snapshot do NetApp	255.000 gb por controlador		

Para mais modelos NetApp FAS, consulte o "Secção de modelos FAS" no Hardware Universe.

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- Centro de Documentação do sistema AFF e FAS

  "https://docs.netapp.com/platstor/index.jsp"

- Página de recursos da documentação do AFF

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- Página de recursos de documentação dos sistemas de armazenamento FAS

  "https://www.netapp.com/us/documentation/fas-storage-systems.aspx"

- FlexPod

  "https://flexpod.com/"

- Documentação do NetApp

  "https://docs.netapp.com"

Especificações técnicas do data center FlexPod

TR-4036: Especificações técnicas do FlexPod Datacenter

Arvind Ramakrishnan, e Jyh-shing Chen, NetApp

A plataforma FlexPod é uma arquitetura de data center pré-projetada e com práticas recomendadas desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e nas controladoras de storage da NetApp (sistemas AFF, ASA ou FAS).

O FlexPod é uma plataforma adequada para executar uma variedade de hipervisores de virtualização, bem como sistemas operacionais bare-metal e workloads empresariais. O FlexPod oferece não apenas uma configuração de linha de base, mas também a flexibilidade de ser dimensionada e otimizada para acomodar vários casos de uso e requisitos diferentes.

> Antes de encomendar uma configuração completa do FlexPod, consulte "Infraestrutura convergente da FlexPod" a página em NetApp.com para obter a versão mais recente destas especificações técnicas.

"Próximo: Plataformas FlexPod."

Plataformas FlexPod

Existem duas plataformas FlexPod:

- **Centro de dados FlexPod.** Essa plataforma é uma infraestrutura de data center virtual altamente dimensionável que é adequada para aplicações empresariais de workload, virtualização, infraestrutura de desktop virtual (VDI) e workloads de nuvem pública, privada e híbrida.
- **FlexPod Express.** Essa plataforma é uma infraestrutura convergente compacta destinada a casos de uso de borda e escritório remoto. O FlexPod Express tem suas próprias especificações documentadas no "Especificações técnicas do FlexPod Express."

Este documento fornece as especificações técnicas da plataforma de datacenter FlexPod.

Regras do FlexPod

O design do FlexPod permite uma infraestrutura flexível que abrange muitos componentes e versões de software diferentes.

Use os conjuntos de regras como guia para criar ou montar uma configuração válida do FlexPod. Os números e regras listados neste documento são os requisitos mínimos para uma configuração do FlexPod. Eles podem ser expandidos nas famílias de produtos incluídas, conforme necessário para diferentes ambientes e casos de uso.

Configurações de FlexPod validadas em comparação com compatíveis

A arquitetura FlexPod é definida pelo conjunto de regras descritas neste documento. Os componentes de hardware e as configurações de software devem ser suportados pelo "Lista de compatibilidade de hardware e software do Cisco UCS" e pelo "Ferramenta de Matriz de interoperabilidade NetApp (IMT)".

Cada Cisco Validated Design (CVD) ou NetApp Verified Architecture (NVA) é uma possível configuração de FlexPod. O Cisco e o NetApp documentam essas combinações de configuração e as validam com testes completos. As implantações do FlexPod que se desviam dessas configurações são totalmente suportadas se seguirem as diretrizes deste documento e se todos os componentes estiverem listados como compatíveis na Lista de compatibilidade de hardware e software do Cisco UCS e no NetApp "IMT" .

Por exemplo, a adição de mais controladores de storage ou servidores Cisco UCS e a atualização de software para versões mais recentes serão totalmente compatíveis se o software, o hardware e as configurações atenderem às diretrizes definidas neste documento.

NetApp ONTAP

O software NetApp ONTAP é instalado em todos os sistemas NetApp FAS, AFF e AFF All SAN Array (ASA). O FlexPod é validado com o software ONTAP, fornecendo uma arquitetura de storage altamente dimensionável que habilita operações ininterruptas, upgrades sem interrupções e uma infraestrutura de dados ágil.

Para obter mais informações sobre o ONTAP, consulte "Software de gerenciamento de dados ONTAP" a página do produto.

Modos de comutação Cisco Nexus de operação

Uma variedade de produtos Cisco Nexus podem ser usados como o componente de comutação de uma determinada implantação do FlexPod. A maioria dessas opções aproveita o tradicional software Cisco Nexus os ou NX-os. A família de switches Cisco Nexus oferece vários recursos em suas linhas de produtos. Esses recursos são detalhados posteriormente neste documento.

A oferta da Cisco no espaço de rede definido por software é chamada de infraestrutura centrada em aplicativos (ACI). A linha de produtos Cisco Nexus que suporta o modo ACI, também chamado de modo de tecido, é a série Cisco Nexus 9300. Esses switches também podem ser implantados no modo NX-os ou autônomo.

O Cisco ACI destina-se a implantações de data center que se concentram nos requisitos de uma aplicação

específica. Os aplicativos são instanciados por meio de uma série de perfis e contratos que permitem a conetividade do host ou da máquina virtual (VM) até o armazenamento.

O FlexPod é validado com ambos os modos de operação dos switches Cisco Nexus. Para obter mais informações sobre os modos ACI e NX-os, consulte as seguintes páginas do Cisco:

- "Infraestrutura centrada em aplicações da Cisco"
- "Software Cisco NX-os"

Requisitos mínimos de hardware

Uma configuração de data center do FlexPod tem requisitos mínimos de hardware, incluindo, entre outros, switches, interconexões de malha, servidores e controladores de storage NetApp.

Você deve usar servidores Cisco UCS. Os servidores C-Series e B-Series foram usados nos designs validados. Os Extenders de malha Cisco Nexus (FEXs) são opcionais nos servidores da série C.

Uma configuração do FlexPod tem os seguintes requisitos mínimos de hardware:

- Dois switches Cisco Nexus em uma configuração redundante. Esta configuração pode consistir em dois switches redundantes do Cisco Nexus 5000, 7000 ou 9000 Series. Os dois interrutores devem ser do mesmo modelo e devem ser configurados no mesmo modo de operação.

  Se você estiver implantando uma arquitetura ACI, deverá observar os seguintes requisitos adicionais:

  - Implante os switches Cisco Nexus 9000 Series em uma topologia de coluna vertebral.
  - Use três Controladores de infraestrutura de políticas de aplicativos da Cisco (APICS).
- Duas interconexões de malha Cisco UCS 6200, 6300 ou 6400 Series em uma configuração redundante.
- Servidores Cisco UCS:
  - Se a solução usar servidores da série B, um chassi de servidor blade da série B do Cisco UCS 5108 mais dois servidores blade da série B do Cisco UCS e dois módulos de e/S (IOMs) de 2104, 2204/8, 2408 ou 2304.
  - Se a solução usar servidores C-Series, dois servidores em rack Cisco UCS C-Series.

    Para implantações maiores de servidores de rack Cisco UCS C-Series, você pode escolher um par de módulos FEX 2232PP. No entanto, o 2232PP não é um requisito de hardware.
- Duas controladoras de storage NetApp em uma configuração de par de alta disponibilidade (HA):

  Essa configuração pode consistir em controladores de storage compatíveis da série NetApp FAS, AFF ou ASA. Consulte o "NetApp Hardware Universe" aplicativo para obter uma lista atual de modelos de controlador FAS, AFF e ASA compatíveis.

  - A configuração de HA requer duas interfaces redundantes por controladora para acesso aos dados. As interfaces podem ser FCoE, FC ou Ethernet (GbE) de 10/25/100GB GbE.
  - Se a solução usar o NetApp ONTAP, será necessária uma topologia de interconexão de cluster aprovada pelo NetApp. Para obter mais informações, consulte a "Interrutores" guia do NetApp Hardware Universe.
  - Se a solução usar o ONTAP, pelo menos duas portas adicionais 10/25/100GbE por controladora serão necessárias para acesso aos dados.

    - Para clusters do ONTAP com dois nós, é possível configurar um cluster sem switch de dois nós.
    - Para clusters ONTAP com mais de dois nós, é necessário um par de switches de interconexão de cluster.
- Um compartimento de disco NetApp com qualquer tipo de disco compatível. Consulte a guia prateleiras do "NetApp Hardware Universe" para obter uma lista atual de modelos de compartimentos de disco compatíveis.

Requisitos mínimos de software

Uma configuração do FlexPod tem os seguintes requisitos mínimos de software:

- NetApp ONTAP -
    - A versão do software ONTAP requer o ONTAP 9.1 ou posterior
- O Cisco UCS Manager lança:
    - Interconexão de malha da série Cisco UCS 6200 – 2,2 (8a)
    - Interconexão de malha da série Cisco UCS 6300 – 3,1 (1e)
    - Interconexão de malha da série Cisco UCS 6400 – 4,0 (1)
- Modo gerenciado de Intersight do Cisco:
    - Interconexão de malha da série Cisco UCS 6400 – 4,1(2)
- Para switches Cisco Nexus 5000 Series, o software Cisco NX-os versão 5,0(3)N1(1c) ou posterior, incluindo NX-os 5,1.x
- Para switches Cisco Nexus 7000 Series:
    - O chassi de 4 slots requer o software Cisco NX-os versão 6,1 (2) ou posterior
    - O chassi de 9 slots requer o software Cisco NX-os versão 5,2 ou posterior
    - O chassi de 10 slots requer o software Cisco NX-os versão 4,0 ou posterior
    - O chassi de 18 slots requer o software Cisco NX-os versão 4,1 ou posterior
- Para switches Cisco Nexus 9000 Series, o software Cisco NX-os versão 6,1 (2) ou posterior

O software usado em uma configuração do FlexPod deve ser listado e suportado no NetApp "IMT" . Alguns recursos podem exigir versões mais recentes do software do que os listados.

Requisitos de conetividade

Uma configuração do FlexPod tem os seguintes requisitos de conetividade:

- Uma rede de gerenciamento fora da banda Ethernet 100Mbps/1GB Ethernet separada é necessária para todos os componentes.
- A NetApp recomenda que você habilite o suporte a quadros jumbo em todo o ambiente, mas isso não é necessário.
- As portas do dispositivo de interconexão de malha Cisco UCS são recomendadas apenas para conexões iSCSI e nas.
- Nenhum equipamento adicional pode ser colocado em linha entre os componentes principais do FlexPod.

Ligações uplink:

- As portas nos controladores de armazenamento NetApp devem ser conetadas aos switches Cisco Nexus 5000, 7000 ou série 9000 para habilitar o suporte a canais de portas virtuais (VPCs).
- Os VPCs são necessários dos switches Cisco Nexus 5000, 7000 ou 9000 Series para os controladores de armazenamento NetApp.
- Os VPCs são necessários dos switches Cisco Nexus 5000, 7000 ou 9000 Series para as interconexões de malha.
- Um mínimo de duas conexões são necessárias para uma VPC. O número de conexões em uma VPC pode ser aumentado com base na carga do aplicativo e nos requisitos de desempenho.

Ligações diretas:

- As portas do controlador de storage do NetApp que estão diretamente conectadas às interconexões de malha podem ser agrupadas para habilitar um canal de porta. A VPC não é compatível com esta configuração.
- Os canais de porta FCoE são recomendados para designs FCoE de ponta a ponta.

Inicialização SAN:

- As soluções FlexPod são projetadas em torno de uma arquitetura de inicialização SAN usando protocolos iSCSI, FC ou FCoE. O uso das tecnologias boot-from-SAN fornece a configuração mais flexível para a infraestrutura do data center e permite os recursos avançados disponíveis em cada componente da infraestrutura. Embora a inicialização a partir de SAN seja a configuração mais eficiente, a inicialização a partir de armazenamento de servidor local é uma configuração válida e suportada.
- A inicialização DE SAN em FC-NVME não é compatível.

Outros requisitos

Uma arquitetura FlexPod tem os seguintes requisitos adicionais de interoperabilidade e suporte:

- Todos os componentes de hardware e software devem ser listados e suportados no NetApp "IMT" , no "Lista de compatibilidade de hardware e software do Cisco UCS" e na ferramenta de Matriz de interoperabilidade de hardware e software do Cisco UCS.
- São necessários contratos de suporte válidos para todos os equipamentos, incluindo:
  - Suporte Smart Net Total Care (SMARTnet) para equipamentos Cisco
  - Suporte SupportEdge Advisor ou SupportEdge Premium para equipamentos NetApp

Para obter mais informações, consulte o NetApp "IMT" .

Recursos opcionais

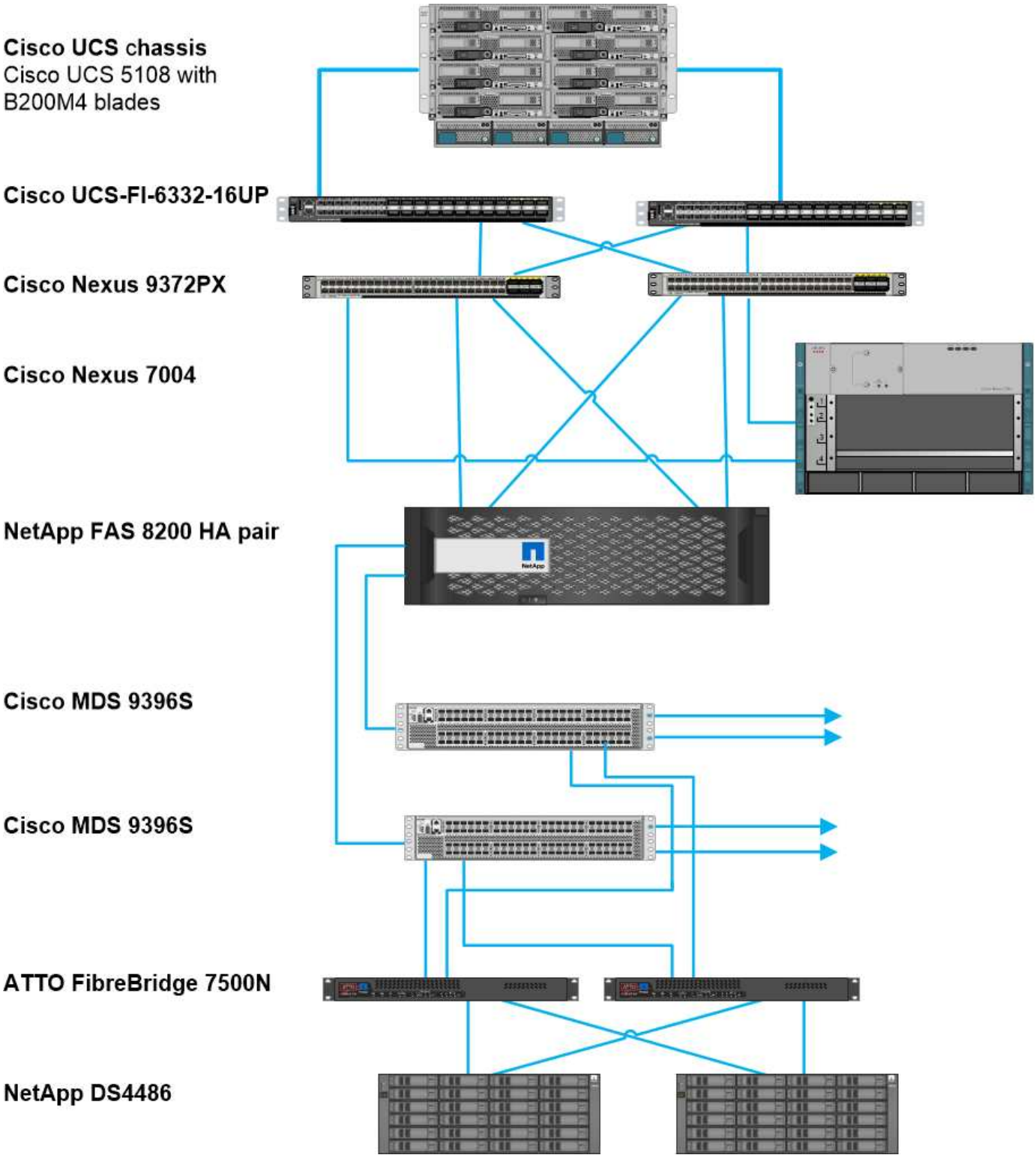
O NetApp oferece suporte a vários componentes opcionais para aprimorar ainda mais as arquiteturas de data center do FlexPod. Os componentes opcionais estão descritos nas subseções a seguir.

MetroCluster

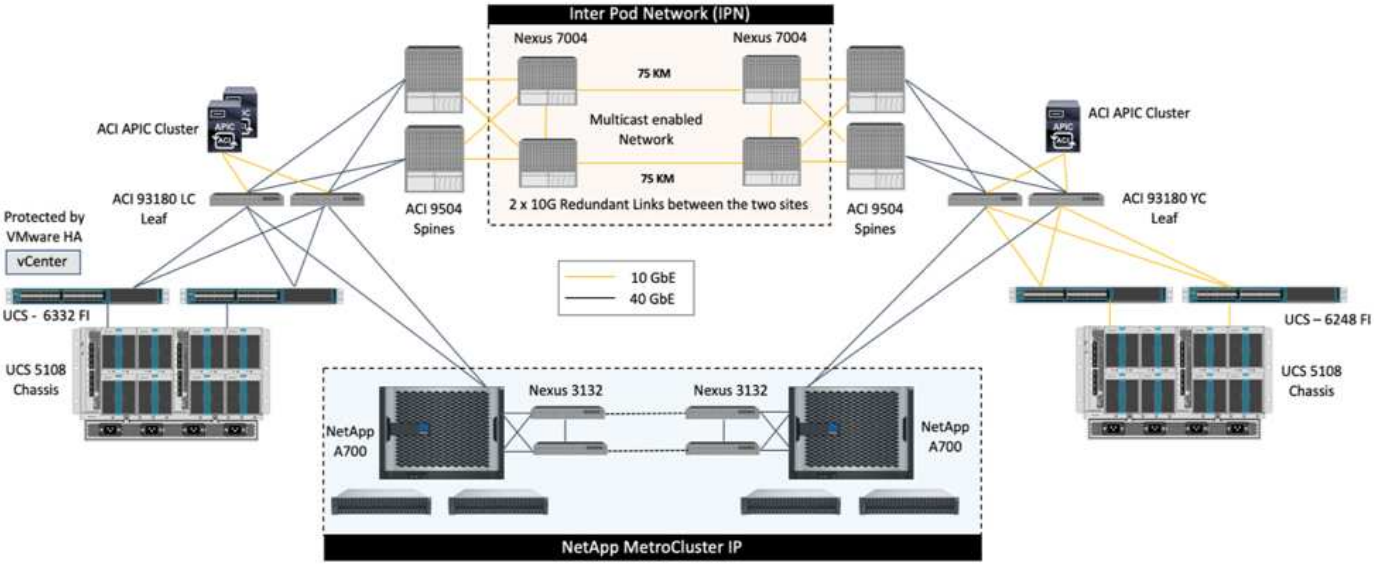
O FlexPod dá suporte às duas variantes do software NetApp MetroCluster para disponibilidade contínua em configurações de cluster de dois ou quatro nós. O MetroCluster fornece replicação síncrona para workloads

essenciais. Ele requer uma configuração de site duplo que esteja conetada com a comutação Cisco. A distância máxima suportada entre os locais é de aproximadamente 300km km (186 milhas) para o MetroCluster FC e aumenta para aproximadamente 435 milhas (700km km) para o MetroCluster IP. As figuras a seguir ilustram um data center FlexPod com arquitetura NetApp MetroCluster e um data center FlexPod com arquitetura IP NetApp MetroCluster, respetivamente.

A figura a seguir mostra o data center FlexPod com arquitetura NetApp MetroCluster.

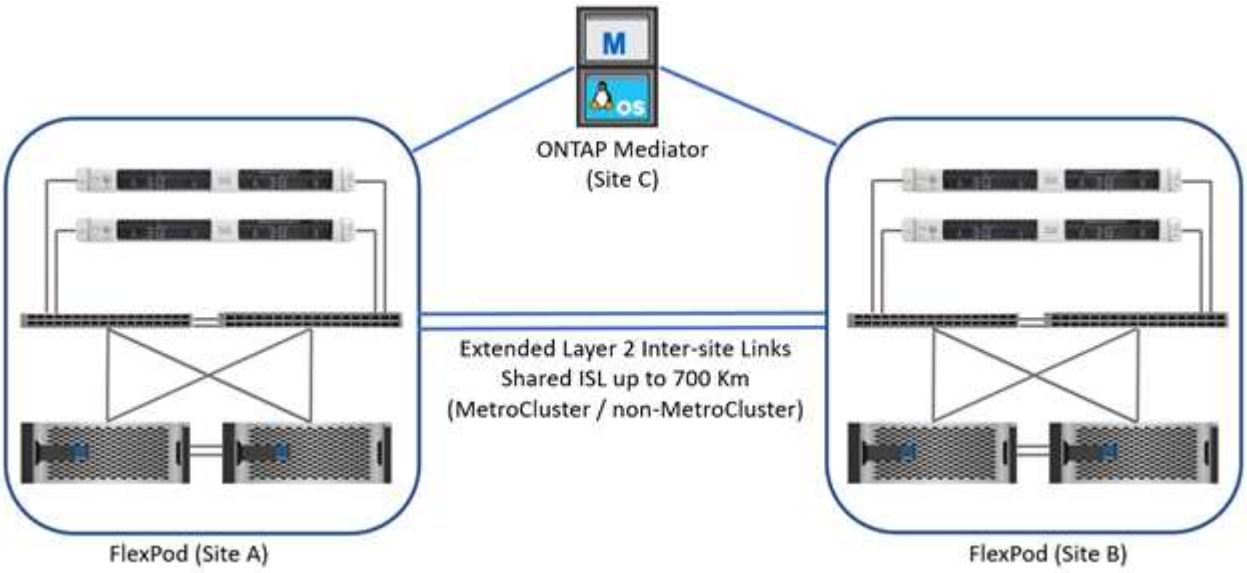


A figura a seguir mostra o datacenter FlexPod com arquitetura NetApp MetroCluster IP.



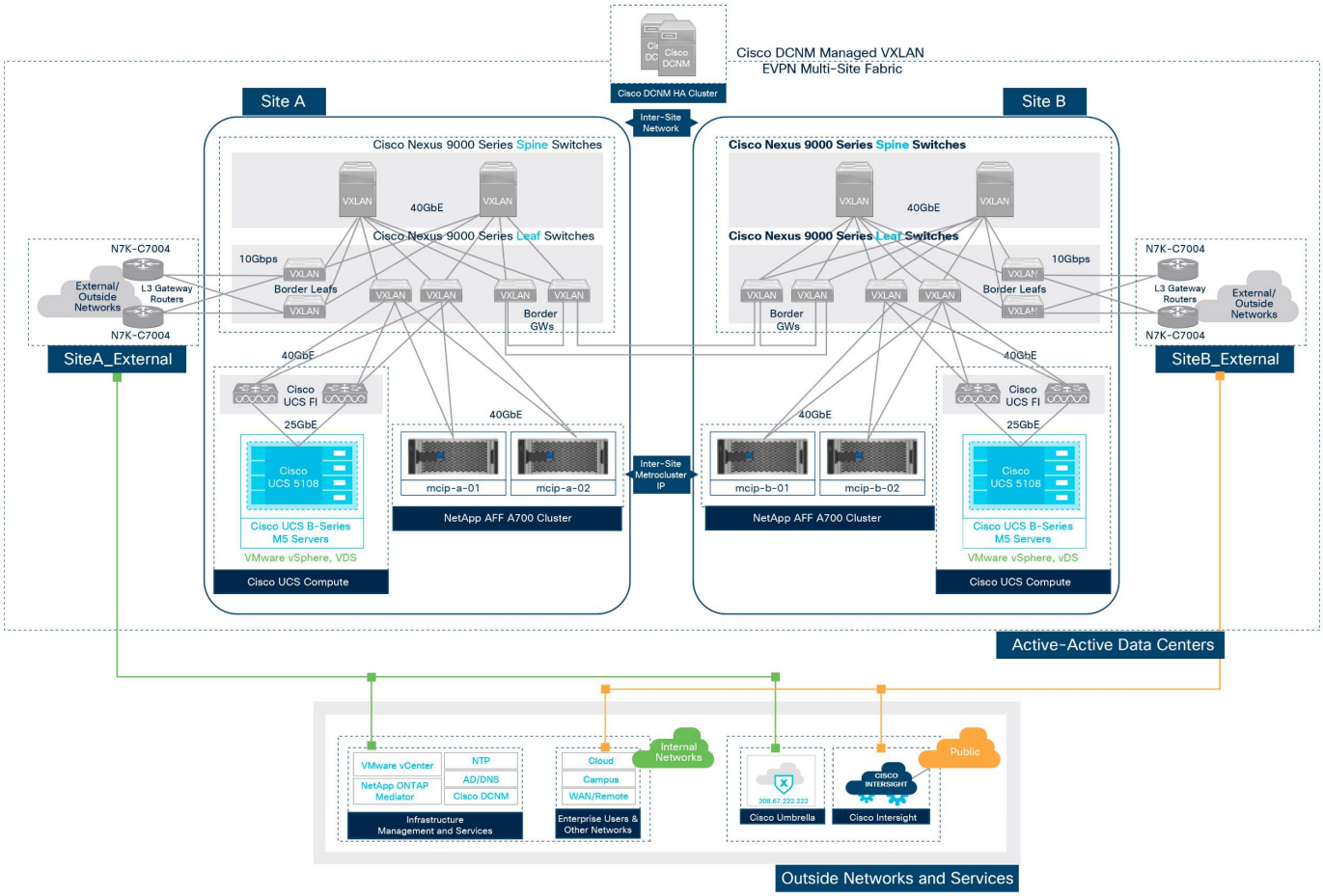
A partir do ONTAP 9.8, o Mediador ONTAP pode ser implantado em um terceiro local para monitorar a solução IP MetroCluster e facilitar o switchover automatizado não planejado quando ocorre um desastre no local.

Para uma implantação de solução IP FlexPod MetroCluster com conetividade local a local de camada 2 estendida, você pode obter economia de custos compartilhando ISL e usando switches FlexPod como switches IP MetroCluster compatíveis se a largura de banda da rede e os switches atenderem aos requisitos, conforme ilustrado na figura a seguir, que mostra a solução IP FlexPod MetroCluster com compartilhamento ISL e switches compatíveis.

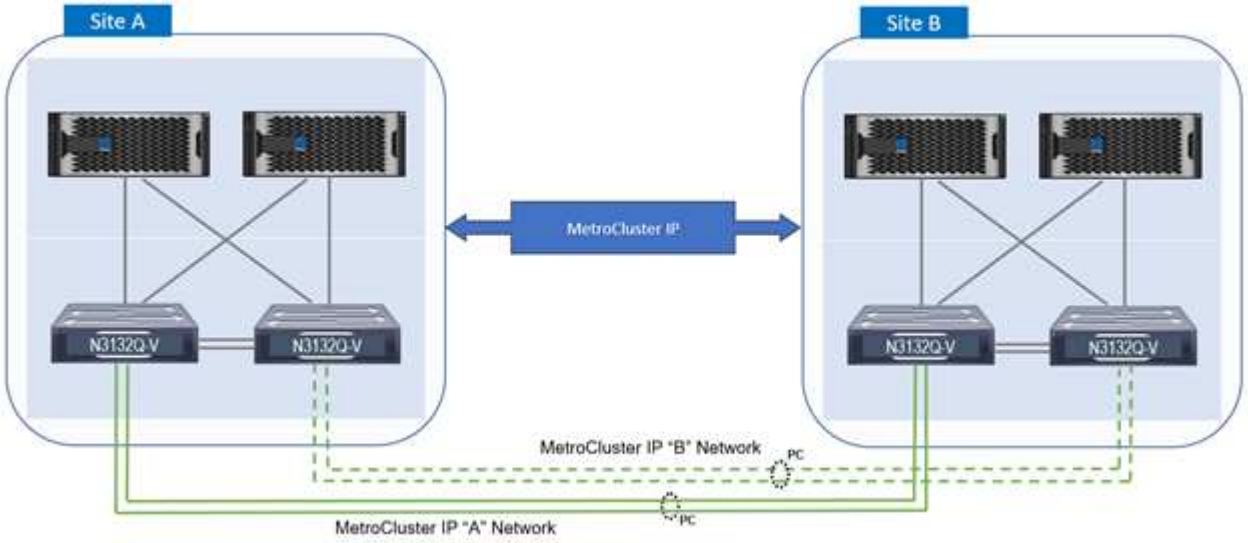


As duas figuras a seguir descrevem a malha de vários locais VXLAN e a malha de armazenamento IP MetroCluster para uma solução IP FlexPod MetroCluster com implantação de malha multi-local VXLAN.

- Estrutura multi-local VXLAN para solução IP FlexPod MetroCluster



- Malha de storage IP MetroCluster para solução FlexPod MetroCluster IP



FC-NVMe completo

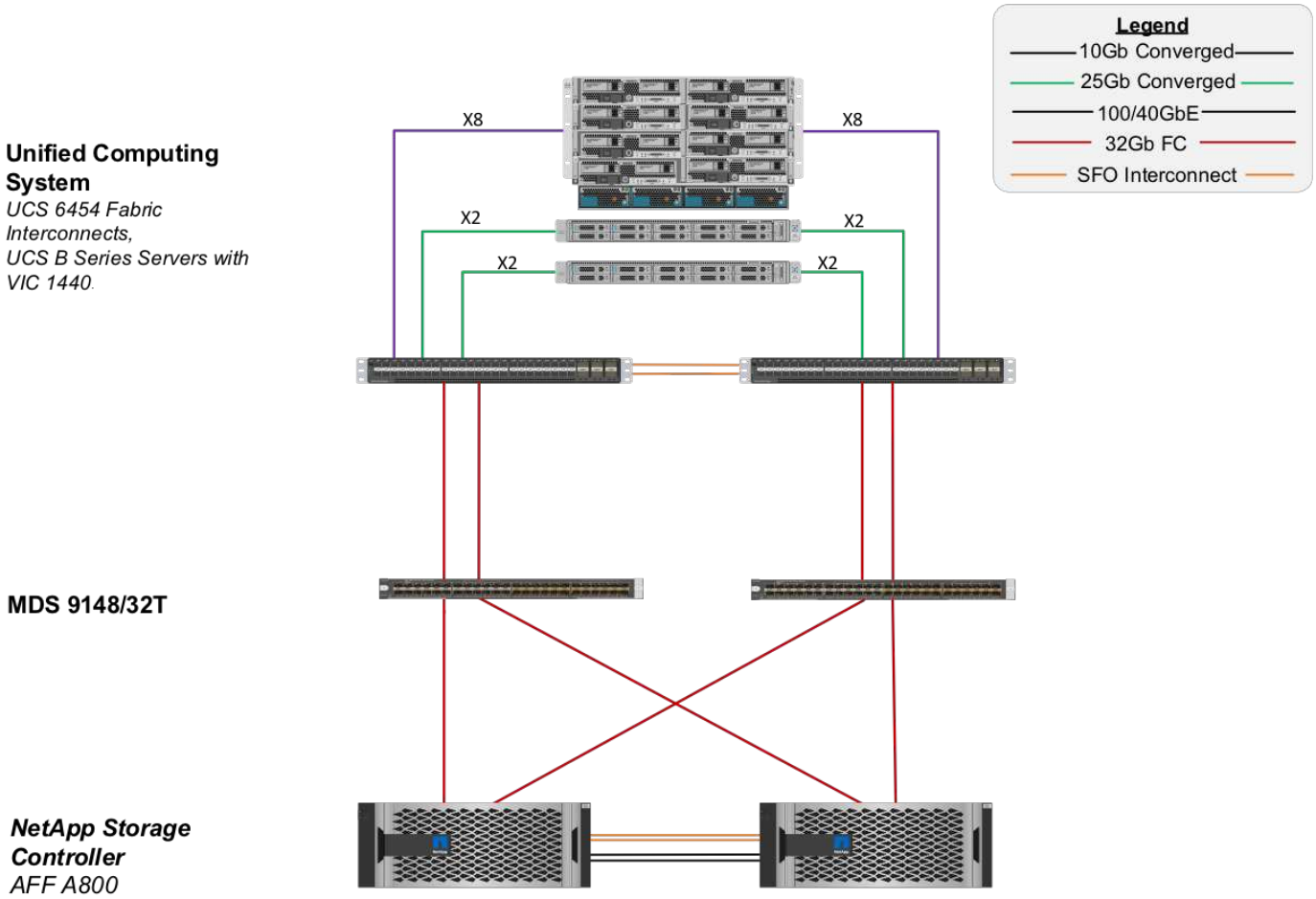
Um FC-NVMe completo estende de forma otimizada a infraestrutura de SAN existente do cliente para aplicações em tempo real, além de fornecer IOPS e taxa de transferência aprimorados com latência reduzida.

Um transporte SAN FC de 32G GB existente pode ser usado para transportar simultaneamente workloads NVMe e SCSI.

A figura a seguir ilustra o data center FlexPod para FC com Cisco MDS.

Mais detalhes sobre as configurações do FlexPod e os benefícios de desempenho, consulte "Apresentação do white paper NVMe completo para FlexPod."

Para obter mais informações sobre a implementação do ONTAP, "TR-4684: Implementando e configurando SANs modernas com NVMe" consulte .



Inicialização FC SAN por meio do Cisco MDS

Para aumentar a escalabilidade usando uma rede SAN dedicada, o FlexPod oferece suporte ao FC por meio de switches MDS Cisco e switches Nexus com suporte a FC, como o Cisco Nexus 93108TC-FX. A opção de inicialização SAN FC por meio do Cisco MDS tem os seguintes requisitos de licenciamento e hardware:

- Um mínimo de duas portas FC por controlador de storage NetApp; uma porta para cada malha SAN
- Uma licença de FC em cada controlador de storage NetApp
- Switches MDS Cisco e versões de firmware compatíveis com o NetApp "IMT"

Para obter mais orientações sobre um design baseado em MDS, consulte o CVD "FlexPod Datacenter com VMware vSphere 6.7U1 Fibre Channel e guia de implantação iSCSI".

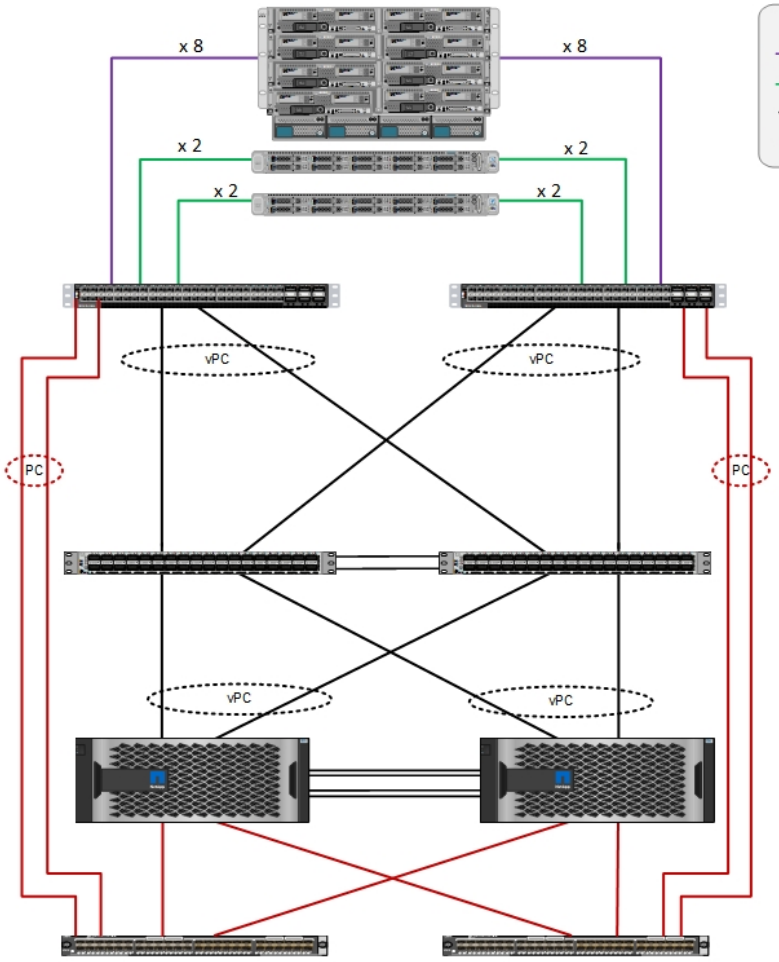
As figuras a seguir mostram um exemplo de FlexPod Datacenter para FC com conetividade MDS e FlexPod Datacenter para FC com Cisco Nexus 93180YC-FX, respetivamente.

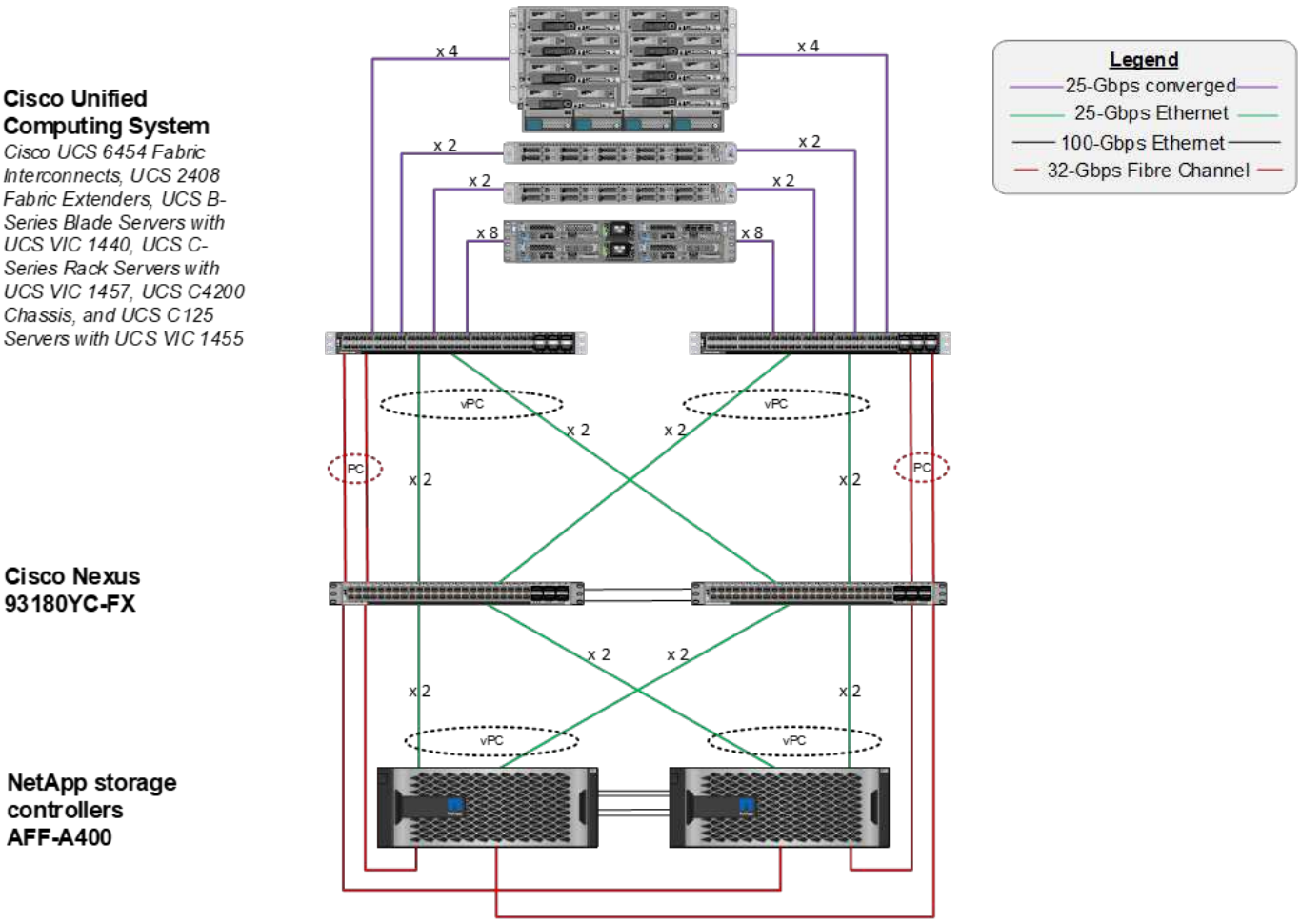
Cisco Unified Computing System
Cisco UCS 6454 Fabric Interconnects, UCS B-Series Blade Servers with UCS VIC 1440, and UCS C-Series Rack Servers with UCS VIC 1457

Cisco Nexus 9336C-FX2

NetApp storage controllers AFF-A800

Cisco MDS 9148T or 9132T switch





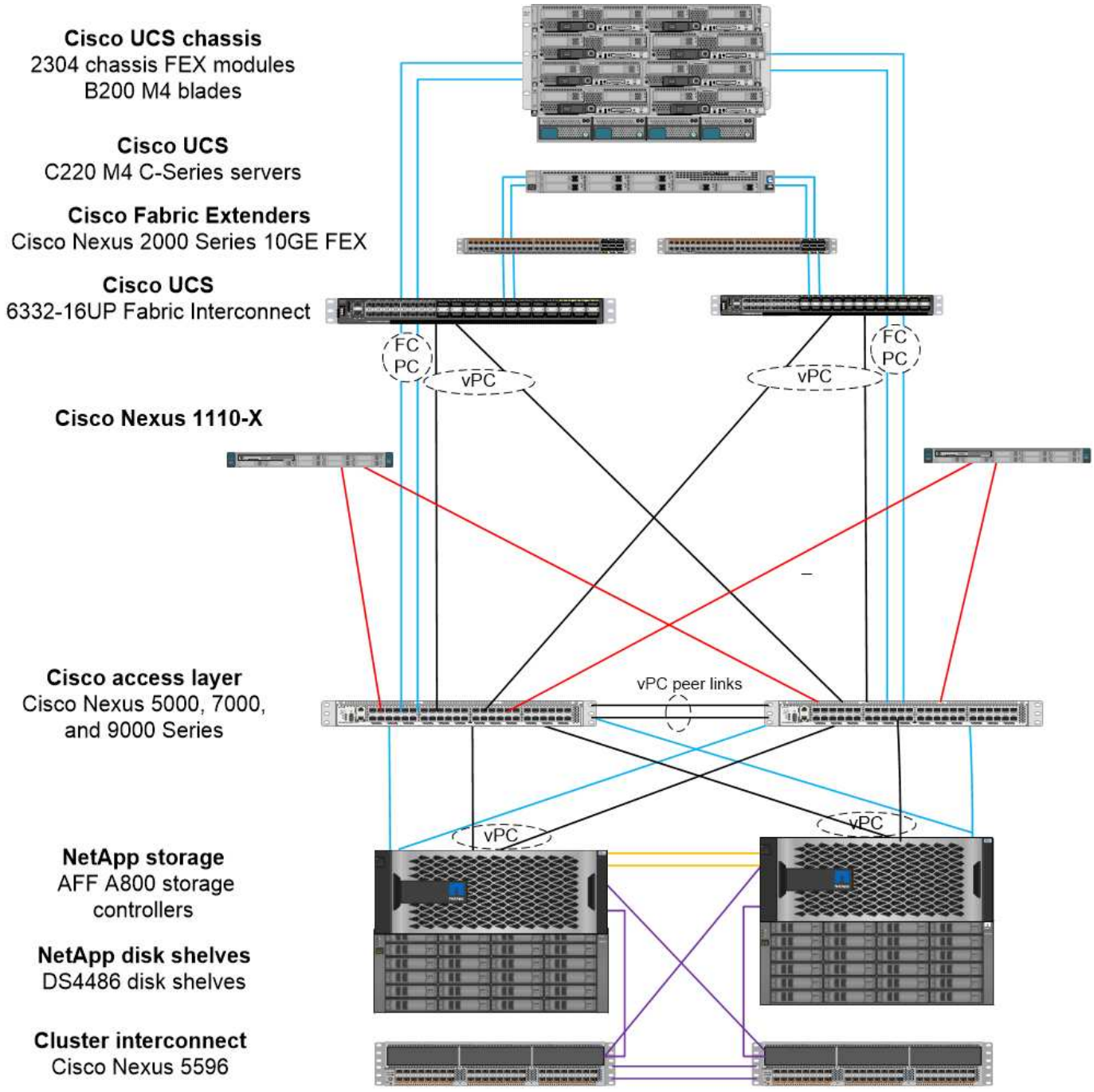
Inicialização FC SAN com Cisco Nexus

A opção clássica de inicialização FC SAN tem os seguintes requisitos de licenciamento e hardware:

- Quando o zoneamento FC é executado no switch Cisco Série Nexus 5000, uma licença de pacote de serviço de protocolos de armazenamento para os switches Cisco série Nexus 5000 (FC_FEATURES_PKG) é necessária.
- Quando o zoneamento FC é executado no switch Cisco Nexus 5000 Series, os links SAN são necessários entre a interconexão de malha e o switch Cisco Nexus 5000 Series. Para redundância adicional, os canais de porta SAN são recomendados entre os links.
- Os switches Cisco Nexus 5010, 5020 e 5548P exigem um módulo de FC ou porta universal (UP) separado para conectividade à interconexão da malha do Cisco UCS e ao controlador de storage da NetApp.
- O Cisco Nexus 93180YCX-FX requer uma licença de recurso FC para recursos para habilitar o FC.
- Cada controlador de storage NetApp requer, no mínimo, duas portas FC de 8 GB/16 GB/32GB GB para conectividade.
- É necessária uma licença FC no controlador de storage NetApp.

> O uso da família de switches Cisco Nexus 7000 ou 9000 impede o uso de FC tradicional, a menos que o zoneamento FC seja realizado na interconexão de malha. Nesse caso, os uplinks SAN para o switch não são suportados.

A figura a seguir mostra uma configuração de conectividade FC.



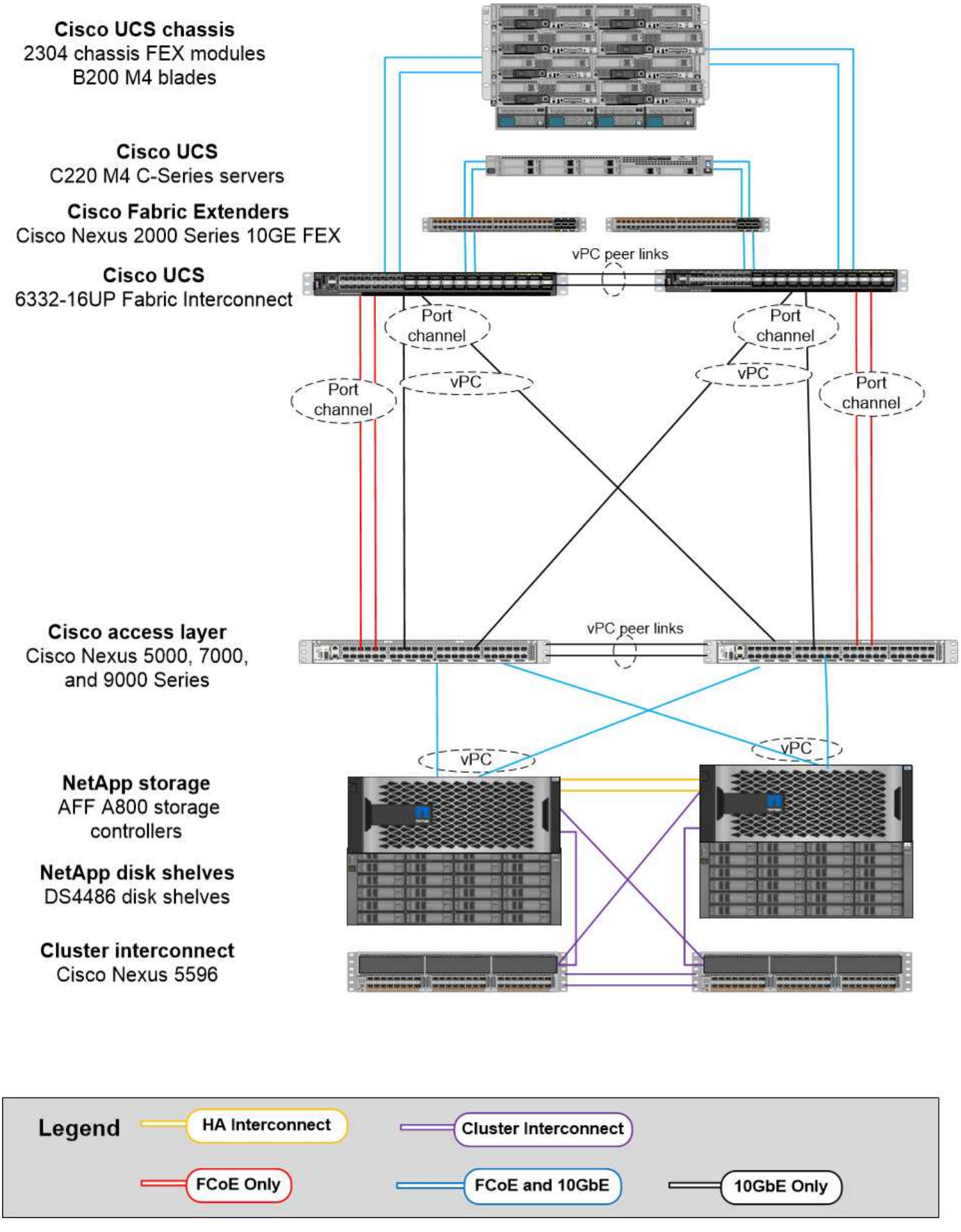
Opção de inicialização FCoE SAN

A opção de inicialização FCoE SAN tem os seguintes requisitos de licenciamento e hardware:

- Quando o zoneamento FC é executado no switch, uma licença de pacote de serviço de protocolos de storage para os switches Cisco Nexus 5000 ou 7000 Series (`FC_FEATURES_PKG`) é necessária.
- Quando o zoneamento FC é executado no switch, uplinks FCoE são necessários entre a interconexão de malha e os switches Cisco Nexus 5000 ou 7000 Series. Para redundância adicional, os canais de porta FCoE também são recomendados entre os links.
- Cada controlador de storage NetApp requer pelo menos uma placa complementar de adaptador de destino unificado (UTA) de porta dupla para conectividade FCoE, a menos que estejam presentes portas integradas de adaptador de destino unificado 2 (UTA2).
- Essa opção requer uma licença FC no controlador de storage NetApp.
- Se você usar os switches da série Cisco Nexus 7000 e o zoneamento FC for executado no switch, uma placa de linha capaz de suportar FCoE é necessária.

> O uso dos switches Cisco Nexus 9000 Series impede o uso do FCoE, a menos que o zoneamento FC seja executado na interconexão de malha e o armazenamento seja conetado às interconexões de malha com as portas do dispositivo. Nesse caso, uplinks FCoE para o switch não são suportados.

A figura a seguir mostra um cenário de inicialização FCoE.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
Port channel
Port channel
Port channel
vPC
vPC
Port channel
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FCoE Only
FCoE and 10GbE
10GbE Only

Opção de inicialização iSCSI

A opção de inicialização iSCSI tem os seguintes requisitos de licenciamento e hardware:

- É necessária uma licença iSCSI no controlador de armazenamento NetApp.
- É necessário um adaptador no servidor Cisco UCS que seja capaz de inicializar iSCSI.
- É necessário um adaptador Ethernet 10Gbps de duas portas no controlador de armazenamento NetApp.

A figura a seguir mostra uma configuração somente Ethernet que é inicializada usando iSCSI.

Cisco UCS chassis
2304 Chassis FEX modules
B200 M4 blades

Cisco UCS
C220 M4 C-Series servers

Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX

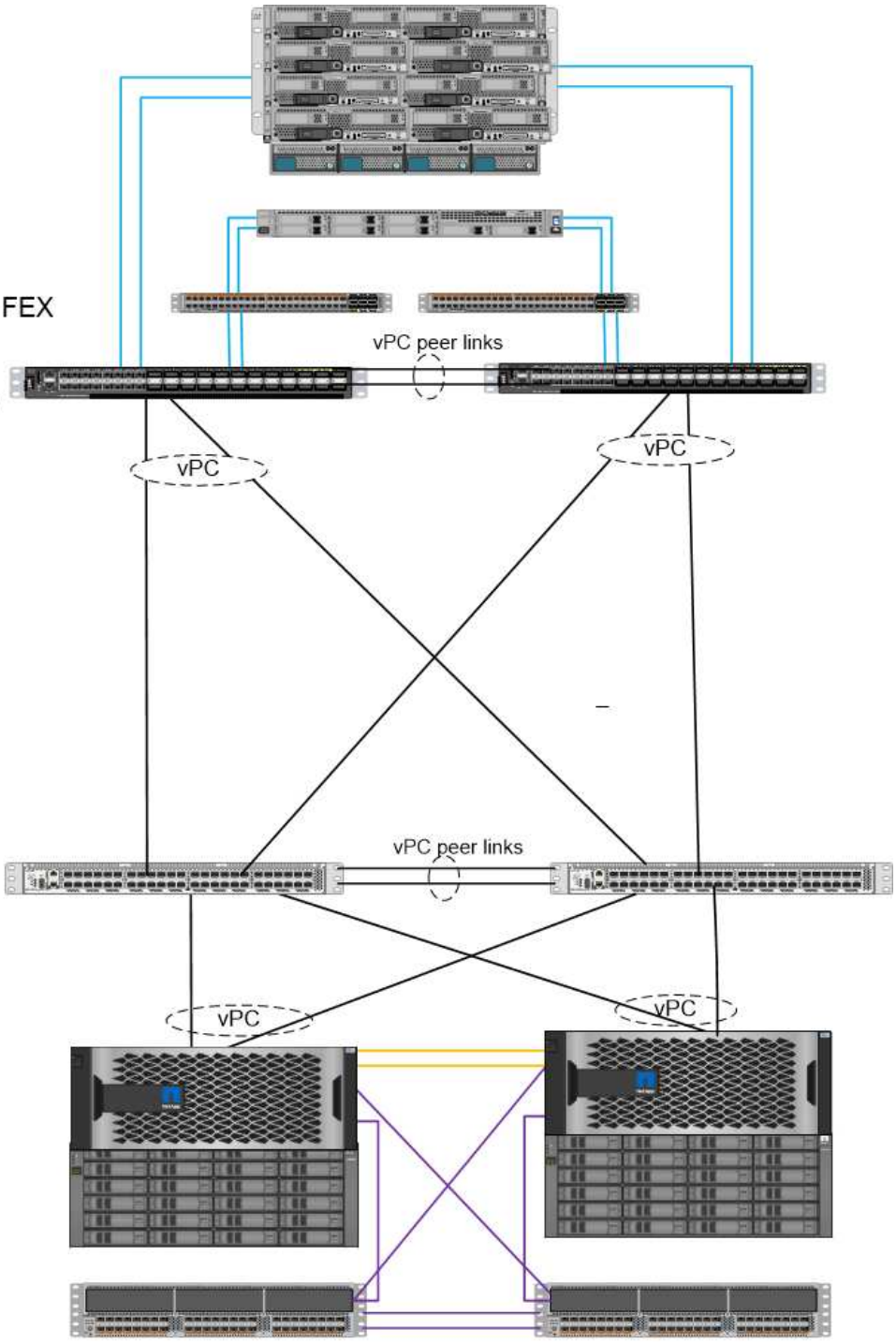
Cisco UCS
6332-16UP Fabric Interconnect

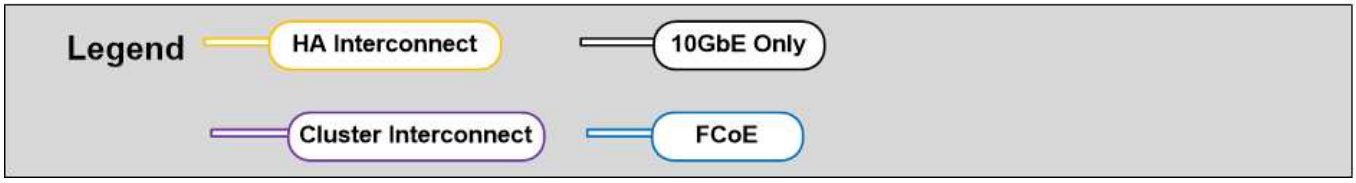
Cisco access layer
Cisco Nexus 5000, 7000, and 9000 Series

NetApp storage
AFF A800 storage controllers

NetApp disk shelves
DS4486 Disk shelves

Cluster Interconnect
Cisco Nexus 5596





Conexão direta do Cisco UCS com o storage NetApp

Os controladores NetApp AFF e FAS podem ser diretamente conectados aos interconectores da malha do Cisco UCS sem qualquer switch SAN upstream.

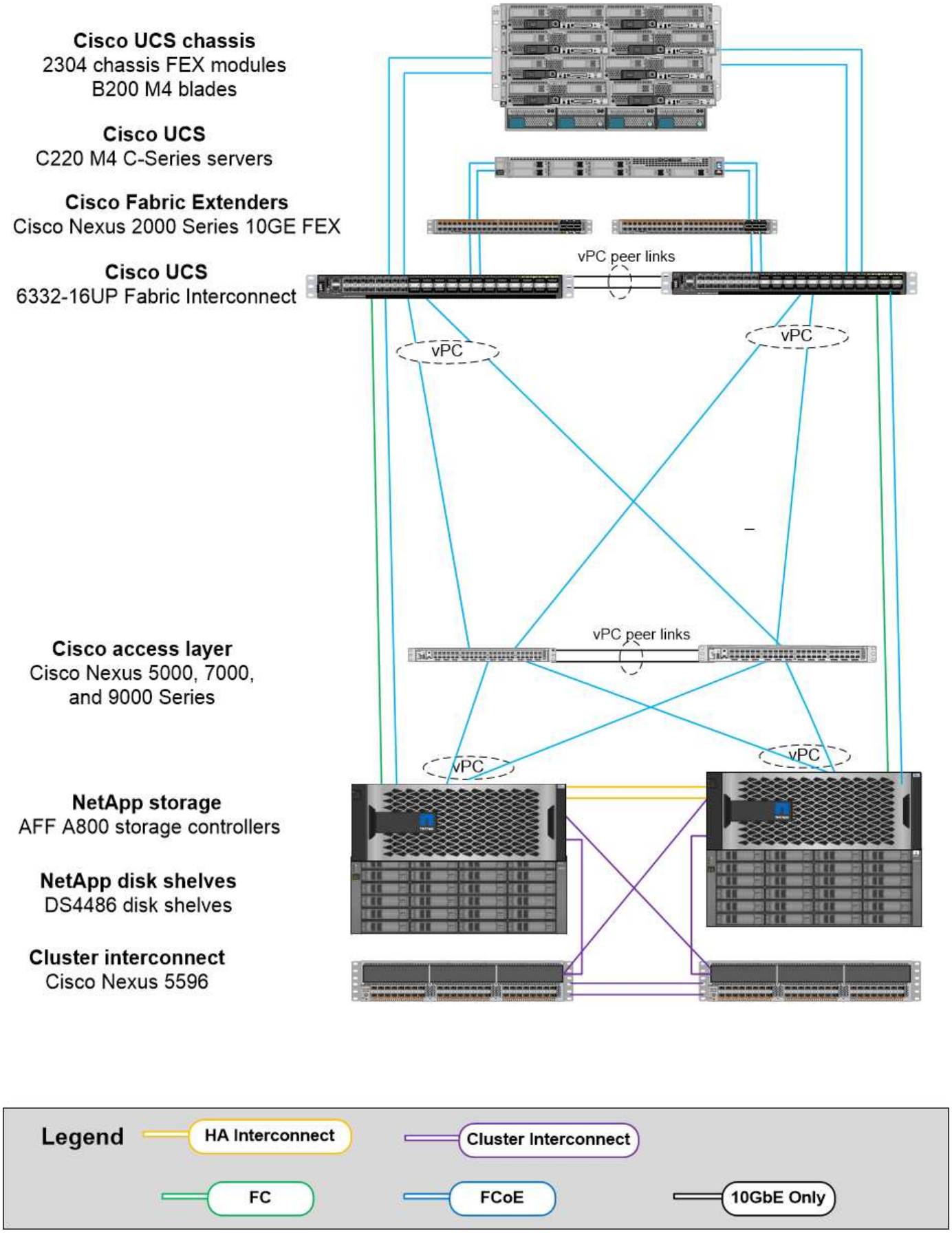
Quatro tipos de portas Cisco UCS podem ser usados para se conetar diretamente ao armazenamento NetApp:

- **Porta FC de armazenamento.** Conectar diretamente essa porta a uma porta FC no storage NetApp.
- **Porta FCoE de armazenamento.** Conete diretamente essa porta a uma porta FCoE no armazenamento NetApp.
- **Porta do aparelho.** Conete diretamente essa porta a uma porta 10GbE no armazenamento NetApp.
- **Porta de armazenamento unificada.** Ligue diretamente esta porta a um UTA NetApp.

Os requisitos de licenciamento e hardware são os seguintes:

- É necessária uma licença de protocolo no controlador de storage NetApp.
- Um adaptador Cisco UCS (iniciador) é necessário no servidor. Para obter uma lista de adaptadores Cisco UCS suportados, consulte o NetApp "IMT" .
- É necessário um adaptador de destino no controlador de armazenamento NetApp.

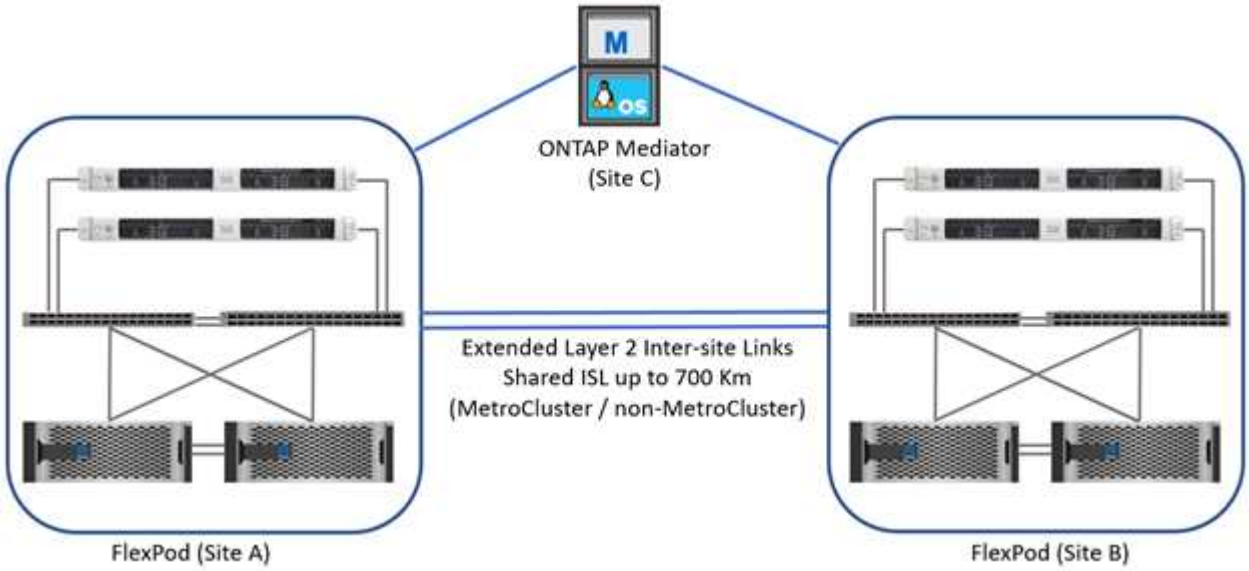
A figura a seguir mostra uma configuração de conexão direta FC.


Cisco UCS chassis
2304 chassis FEX modules
B200 M4 blades
Cisco UCS
C220 M4 C-Series servers
Cisco Fabric Extenders
Cisco Nexus 2000 Series 10GE FEX
Cisco UCS
6332-16UP Fabric Interconnect
vPC peer links
vPC
vPC
Cisco access layer
Cisco Nexus 5000, 7000,
and 9000 Series
vPC peer links
vPC
vPC
NetApp storage
AFF A800 storage controllers
NetApp disk shelves
DS4486 disk shelves
Cluster interconnect
Cisco Nexus 5596
Legend
HA Interconnect
Cluster Interconnect
FC
FCoE
10GbE Only

Notas:

- O Cisco UCS é configurado no modo de comutação FC.
- As portas FCoE do destino para a malha interconexões são configuradas como portas de storage FCoE.
- As portas FC do destino para a malha, as interconexões são configuradas como portas de storage FC.

A figura a seguir mostra uma configuração de conexão direta iSCSI/Unified IP.



Notas:

- O Cisco UCS está configurado no modo de comutação Ethernet.
- As interconexões de portas iSCSI do destino para a malha são configuradas como portas de storage Ethernet para dados iSCSI.
- As portas Ethernet do destino para a malha, as interconexões são configuradas como portas de storage Ethernet para dados CIFS/NFS.

Componentes do Cisco

O Cisco contribuiu substancialmente para o design e a arquitetura do FlexPod, abrangendo as camadas de computação e rede da solução. Esta seção descreve as opções Cisco UCS e Cisco Nexus que estão disponíveis para o FlexPod. O FlexPod suporta servidores Cisco UCS B-Series e C-Series.

Opções de interconexão de malha do Cisco UCS

Interconexões de malha redundantes são necessárias na arquitetura do FlexPod. Ao adicionar vários chassis Cisco UCS a um par de interconexões de malha, lembre-se de que o número máximo de chassis em um ambiente é determinado por um limite de arquitetura e de porta.

Os números de peça que são mostrados na tabela a seguir são para as interconexões de tecido base. Eles não incluem a unidade de fonte de alimentação (PSU) ou SFP, QSFP ou módulos de expansão. Há suporte para interconexões de malha adicionais; consulte a "NetApp IMT" para obter uma lista completa.

Interconexão de malha Cisco UCS	Número de peça	Especificações técnicas
Cisco UCS 6332UP	UCS-FI-6332-UP	"Interconexão de malha Cisco UCS 6332"
Cisco UCS 6454	UCS-FI-6454-U	"Interconexão de malha Cisco UCS 6454"

Cisco UCS 6454

A série Cisco UCS 6454 oferece conetividade FCoE e Ethernet de 10/25/40/100GbE com taxa de linha, baixa latência e sem perdas, bem como portas unificadas capazes de operação Ethernet ou FC. As portas 44 10/25Gbps podem operar como Ethernet convergente de 10Gbps GbE ou 25Gbps GbE, das quais oito são portas unificadas capazes de operar a 8 GbE/16 GbE/32Gbps GbE para FC. Quatro portas operam a 1/10/25Gbps para conetividade legada, e seis portas QSFP servem como portas uplink 40/100Gbps ou portas breakout. Você pode estabelecer conectividade de rede 100Gbps de ponta a ponta com controladores de storage NetApp compatíveis com adaptadores 100Gbps. Para obter adaptadores e suporte à plataforma, consulte o "NetApp Hardware Universe".

Para obter detalhes sobre portas, consulte a "Interconexão de malha Cisco UCS 6454" Folha de dados.

Para obter especificações técnicas sobre os módulos de dados QSFP 100GB, consulte "Folha de dados dos módulos Cisco 100GBASE QSFP".

Opção de chassi do Cisco UCS B-Series

Para usar os blades da série B do Cisco UCS, é necessário ter um chassi da série B do Cisco UCS. A tabela abaixo descreve a opção de chassi do Cisco UCS BSeries.

Chassi da série B do Cisco UCS	Número de peça	Especificações técnicas
Cisco UCS 5108	N20-C6508	"Chassi do servidor blade da série Cisco UCS 5100"

Cada chassi blade Cisco UCS 5108 deve ter dois IOMs da série Cisco UCS 2200/2300/2400 para fornecer conectividade redundante às interconexões de malha.

Opções de servidor blade Cisco UCS B-Series

Os servidores blade da série B Cisco UCS estão disponíveis em variedades de meia largura e largura total, com várias opções de CPU, memória e e e/S. Os números de peça listados na tabela a seguir são para o servidor base. Eles não incluem CPU, memória, unidades ou placas adaptadoras mezzanine. Várias opções de configuração estão disponíveis e são compatíveis com a arquitetura FlexPod.

Lâmina da série B Cisco UCS	Número de peça	Especificações técnicas
Cisco UCS B200 M6	UCSB-B200-M6	"Servidor blade Cisco UCS B200 M6"

As gerações anteriores de blades da série B do Cisco UCS podem ser usadas na arquitetura do FlexPod, se forem suportadas no "Lista de compatibilidade de hardware e software do Cisco UCS". Os servidores tipo lâmina da série B Cisco UCS também devem ter um contrato de suporte SMARTnet válido.

Opção de chassi do Cisco UCS X-Series

Para usar os nós de computação do Cisco UCS X-Series, você precisa ter um chassi do Cisco UCS X-Series. A tabela a seguir descreve a opção de chassi do Cisco UCS X-Series.

Lâmina da série X Cisco UCS	Número de peça	Especificações técnicas
Cisco UCS 9508 M6	UCSX-9508	"Chassis da série X Cisco UCX9508"

Cada chassi do Cisco UCS 9508 deve ter dois módulos de malha inteligentes (IFMs) Cisco UCS 9108 para fornecer conetividade redundante às interconexões de malha.

Opções de dispositivo Cisco UCS X-Series

Os nós de computação do Cisco UCS X-Series estão disponíveis com várias opções de CPU, memória e e/S. Os números de peça listados na tabela a seguir são para o nó base. Eles não incluem CPU, memória, unidades ou placas adaptadoras mezzanine. Várias opções de configuração estão disponíveis e são compatíveis com a arquitetura FlexPod.

Nós de computação do Cisco UCS X-Series	Número de peça	Especificações técnicas
Cisco UCS X210c M6	UCSX-210C-M6	"Nó de computação do Cisco UCS X210c M6"

Opções de servidor de rack Cisco UCS C-Series

Os servidores em rack da série C Cisco UCS estão disponíveis em uma e duas variedades de unidades de rack (RU), com várias opções de CPU, memória e e e/S. Os números de peça listados na segunda tabela abaixo são para o servidor base. Eles não incluem CPUs, memória, unidades, placas PCIe (Peripheral Component Interconnect Express) ou o extensor de malha Cisco. Várias opções de configuração estão disponíveis e são compatíveis com a arquitetura FlexPod.

A tabela a seguir lista as opções do servidor de rack Cisco UCS C-Series.

Servidor de rack Cisco UCS C-Series	Número de peça	Especificações técnicas
Cisco UCS C220 M6	UCSC-C220-M6	"Servidor de rack Cisco UCS C220 M6"
Cisco UCS C225 M6	UCSC-C225-M6	"Servidor de rack Cisco UCS C225 M6"
Cisco UCS C240 M6	UCSC-C240-M6	"Servidor de rack Cisco UCS C240 M6"
Cisco UCS C245 M6	UCSC-C245-M6	"Servidor de rack Cisco UCS C245 M6"

As gerações anteriores de servidores da série C do Cisco UCS podem ser usadas na arquitetura do FlexPod, se forem compatíveis com o "Lista de compatibilidade de hardware e software do Cisco UCS". Os servidores Cisco UCS C-Series também devem ter um contrato de suporte SMARTnet válido.

Opções de switch da série Cisco Nexus 5000

Switches redundantes da série Cisco Nexus 5000, 7000 ou 9000 são necessários na arquitetura do FlexPod. Os números de peça listados na tabela abaixo são para o chassi do Cisco Nexus 5000 Series; eles não incluem módulos SFP, FC complementar ou módulos Ethernet.

Switch Cisco Nexus 5000 Series	Número de peça	Especificações técnicas
Cisco Nexus 56128P	N5K-C56128P	"Switches da plataforma Cisco Nexus 5600"
Cisco Nexus 5672UP-16G	N5K-C5672UP-16G	
Cisco Nexus 5596UP	N5K-C5596UP-FA	"Switches Cisco Nexus 5548 e 5596"
Cisco Nexus 5548UP	N5K-C5548UP-FA	

Opções de switch da série Cisco Nexus 7000

Switches redundantes da série Cisco Nexus 5000, 7000 ou 9000 são necessários na arquitetura do FlexPod. Os números de peça listados na tabela abaixo são para o chassi da série Cisco Nexus 7000; eles não incluem módulos SFP, placas de linha ou fontes de alimentação, mas incluem bandejas de ventilador.

Switch Cisco Série Nexus 7000	Número de peça	Especificações técnicas
Cisco Nexus 7004	N7K-C7004	"Switch Cisco Nexus de 7000 4 slots"
Cisco Nexus 7009	N7K-C7009	"Switch Cisco Nexus de 7000 9 slots"
Cisco Nexus 7702	N7K-C7702	"Switch Cisco Nexus de 7700 2 slots"
Cisco Nexus 7706	N77-C7706	"Switch Cisco Nexus de 7700 6 slots"

Opções de switch da série Cisco Nexus 9000

Switches redundantes da série Cisco Nexus 5000, 7000 ou 9000 são necessários na arquitetura do FlexPod. Os números de peça listados na tabela abaixo são para o chassi Cisco Nexus 9000 Series; eles não incluem módulos SFP ou módulos Ethernet.

Switch Cisco Série Nexus 9000	Número de peça	Especificações técnicas
Cisco Nexus 93180YC-FX	N9K-C93180YC-FX	"Switches Cisco Nexus 9300 Series"
Cisco Nexus 93180YC-EX	N9K-93180YC-EX	
Cisco Nexus 9336PQ em suspensão	N9K-C9336PQ	
Cisco Nexus 9332PQ	N9K-C9332PQ	
Cisco Nexus 9336C-FX2	N9K-C9336C-FX2	
Cisco Nexus 92304QC	N9K-C92304QC	"Switches Cisco Nexus 9200 Series"
Cisco Nexus 9236C	N9K-9236C	

Alguns switches Cisco Nexus 9000 Series têm variantes adicionais. Estas variantes são suportadas como parte da solução FlexPod. Para obter a lista completa de switches Cisco Nexus 9000 Series, "Switches Cisco Nexus 9000 Series" consulte no site da Cisco.

Opções Cisco APIC

Ao implantar o Cisco ACI, você deve configurar os três APICS do Cisco além dos itens na "Switches Cisco Nexus 9000 Series"seção . Para obter mais informações sobre os tamanhos APIC da Cisco, consulte a. "Datasheet da infraestrutura centrada em aplicações da Cisco."

Para obter mais informações sobre as especificações do produto APIC, consulte a Tabela 1 a Tabela 3 no "Folha de dados do controlador de infraestrutura de políticas de aplicações da Cisco".

Opções de extensão de tecido Cisco Nexus

Os FEXs redundantes de montagem em rack Cisco Nexus 2000 são recomendados para grandes arquiteturas FlexPod que usam servidores série C. A tabela abaixo descreve algumas opções do Cisco Nexus FEX. Também são suportados modelos FEX alternativos. Para obter mais informações, consulte "Lista de compatibilidade de hardware e software do Cisco UCS" .

Cisco Nexus montado em rack FEX	Número de peça	Especificações técnicas
Cisco Nexus 2232PP	N2K-C2232PP	"Extensores de tecido da série Cisco Nexus 2000"
Cisco Nexus 2232TM-E	N2K-C2232TM-E	
Cisco Nexus 2348UPQ	N2K-C2348UPQ	"Extensores de malha de plataforma Cisco Nexus 2300"
Cisco Nexus 2348TQCiscoP 2348TQ-e	N2K-C2348TQN2K-C2348TQ-E	

Opções do Cisco MDS

Os switches Cisco MDS são um componente opcional na arquitetura do FlexPod. Malhas de switch SAN redundantes são necessárias quando você implementa o switch Cisco MDS para FC SAN. A tabela abaixo lista os números de peça e os detalhes de um subconjunto dos switches MDS Cisco suportados. Consulte "NetApp IMT" e "Lista de compatibilidade de hardware e software do Cisco" para obter uma lista completa dos switches SAN suportados.

Switch Cisco MDS série 9000	Número de peça	Descrição
Cisco MDS 9148T	DS-C9148T-24IK	"Switches Cisco MDS série 9100"
Cisco MDS 9132T	DS-C9132T-MEK9	
Cisco MDS 9396S	DS-C9396S-K9	"Switches Cisco MDS série 9300"

Opções de licenciamento do software Cisco

As licenças são necessárias para habilitar protocolos de storage nos switches Cisco Nexus. Todos os switches das séries Cisco Nexus 5000 e 7000 exigem uma licença de serviços de storage para habilitar o protocolo FC ou FCoE para implementações de inicialização de SAN. Atualmente, os switches Cisco Nexus 9000 não são compatíveis com FC ou FCoE.

As licenças necessárias e os números de peça dessas licenças variam dependendo das opções selecionadas

para cada componente da solução FlexPod. Por exemplo, os números de peça de licença de software variam dependendo do número de portas e quais switches da série Cisco Nexus 5000 ou 7000 você escolher. Consulte o seu representante de vendas para obter os números de peça exatos. A tabela abaixo lista as opções de licenciamento do software Cisco.

Licenciamento do software Cisco	Número de peça	Informações da licença
Licença de armazenamento Cisco Nexus 5500, 8, 48 e 96 portas	N55-8P-SSK9/N55-48P-SSK9/N55-96P-SSK9	"Licenciamento de recursos do software Cisco NX-os"
Licença de protocolos de storage do Cisco Nexus 5010/5020	N5010-SSK9/N5020-SSK9	
Licença de protocolos de storage do Cisco Nexus 5600	N56-16P-SSK9/N5672-72P-SSK9/N56128-128P-SSK9	
Licença empresarial de storage do Cisco Nexus 7000	N7K-SAN1K9	
Licença de serviços empresariais Cisco Nexus 9000	N95-LAN1K9/N93-LAN1K9	

Opções de licenciamento de suporte do Cisco

Contratos de suporte válidos SMARTnet são necessários em todos os equipamentos Cisco na arquitetura FlexPod.

As licenças necessárias e os números de peça dessas licenças devem ser verificados pelo seu representante de vendas, pois podem variar para diferentes produtos. A tabela abaixo lista as opções de licenciamento de suporte do Cisco.

Licenciamento do suporte da Cisco	Guia de licença
Smart Net Total Care Onsite Premium	"Serviço de cuidados totais de rede inteligente Cisco"

Componentes do NetApp

Os controladores de storage do NetApp fornecem a base de storage na arquitetura FlexPod para inicialização e storage de dados de aplicações. Os componentes do NetApp incluem controladores de storage, switches de interconexão de cluster, unidades e compartimentos de disco e opções de licenciamento.

Opções do controlador de storage NetApp

Controladores redundantes NetApp FAS, AFF ou AFF ASA são necessários na arquitetura do FlexPod. Os controladores executam o software ONTAP. Quando os controladores de armazenamento são encomendados, a versão de software preferida pode ser pré-carregada nos controladores. Para o ONTAP, é encomendado um cluster completo. Um cluster completo inclui um par de controladores de storage e uma interconexão de cluster (switch ou sem switch).

Diferentes opções e configurações estão disponíveis, dependendo da plataforma de armazenamento selecionada. Consulte o seu representante de vendas para obter detalhes sobre estes componentes adicionais.

As famílias de controladores listadas na tabela abaixo são apropriadas para uso em uma solução de data

center FlexPod, pois sua conexão com os switches Cisco Nexus é perfeita. Consulte a "NetApp Hardware Universe" para obter detalhes de compatibilidade específicos em cada modelo de controlador.

Família de controladores de storage	Especificações técnicas
AFF Série A.	"Documentação da série A do AFF"
AFF ASA Série A.	"Documentação da série A do AFF ASA"
Série FAS	"Documentação da série FAS"

Opções de switch de interconexão de cluster

A tabela a seguir lista os switches de interconexão de cluster Nexus que estão disponíveis para arquiteturas FlexPod. Além disso, o FlexPod oferece suporte a todos os switches de cluster compatíveis com ONTAP, incluindo switches não Cisco, desde que sejam compatíveis com a versão do ONTAP que está sendo implantada. Consulte a "NetApp Hardware Universe" para obter detalhes de compatibilidade adicionais para modelos de interrutores específicos.

Switch de interconexão de cluster	Especificações técnicas
Cisco Nexus 3132Q-V	"Documentação do NetApp: Switches Cisco Nexus 3132Q-V."
Cisco Nexus 9336C-FX2	"Documentação do NetApp: Switches Cisco Nexus 9336C-FX2"

Opções de compartimento de disco e unidade NetApp

É necessário no mínimo um compartimento de disco NetApp para todos os controladores de storage.

O tipo de compartimento NetApp selecionado determina quais tipos de unidade estão disponíveis nesse compartimento.

Para todos os compartimentos de disco e números de peça de disco, consulte o seu representante de vendas.

Para obter mais informações sobre as unidades suportadas, clique no link NetApp Hardware Universe na tabela a seguir e selecione unidades suportadas.

Compartimento de disco	Especificações técnicas
DS224C	"Compartimentos de disco e Mídia de armazenamento unidades com suporte no NetApp Hardware Universe"
DS212C	
DS460C	
NS224	

Opções de licenciamento do software NetApp

A tabela a seguir lista as opções de licenciamento do software NetApp que estão disponíveis para a arquitetura do datacenter do FlexPod. O software NetApp é licenciado no nível do controlador FAS e AFF.

Licenciamento do software NetApp	Número de peça	Especificações técnicas
SW, BNDL completo (controlador), -C.	SW-8XXX-COMP-BNDL-C	"Biblioteca de produtos De A A Z"
SW, princípios Básicos da ONTAP (controlador), -C	SW-8XXX-ONTAP9-C	

Opções de licenciamento de suporte do NetApp

As licenças do NetApp SupportEdge Premium são necessárias para a arquitetura do FlexPod, mas os números de peça dessas licenças variam de acordo com as opções selecionadas no design do FlexPod. Por exemplo, os números de peça de licença de software são diferentes dependendo do controlador FAS que você escolher. Consulte o seu representante de vendas para obter informações sobre os números de peça exatos para licenças de suporte individuais. A tabela abaixo mostra um exemplo de uma licença SupportEdge.

Licenciamento de suporte do NetApp	Número de peça	Especificações técnicas
SupportEdge Premium 4 horas no local - meses: 36	CS-O2-4HR	"NetApp SupportEdge Premium"

Requisitos de alimentação e cabeamento

Um design FlexPod tem requisitos mínimos de energia e cabeamento.

Requisitos de energia

Os requisitos de energia para o data center FlexPod diferem com base no local onde a configuração do data center FlexPod está instalada.

Para obter mais dados sobre a potência máxima necessária e para obter outras informações detalhadas sobre a energia, consulte as especificações técnicas de cada componente de hardware listado na "Especificações técnicas e Referências: Componentes de hardware"seção .

Para obter dados de energia detalhados do Cisco UCS, consulte "Calculadora de energia Cisco UCS".

Para obter os dados de alimentação do controlador de armazenamento NetApp, consulte "NetApp Hardware Universe". Em plataformas, selecione a plataforma de storage que deseja usar na configuração (FAS/V-Series ou AFF). Selecione a versão do ONTAP e o controlador de armazenamento e, em seguida, clique no botão Mostrar resultados.

Requisitos mínimos de cabos

O número e o tipo de cabos e adaptadores necessários variam de acordo com a implantação do FlexPod Datacenter. O tipo de cabo, o tipo de transcetor e o número são determinados durante o processo de projeto com base em seus requisitos. A tabela abaixo lista o número mínimo de cabos necessários.

Hardware	Número do modelo	Cabos necessários
Chassi do Cisco UCS	Cisco UCS 5108	Pelo menos dois cabos twinaxiais por módulo Cisco UCS 2104XP, 2204XP ou 2208XP

Hardware	Número do modelo	Cabos necessários
O Cisco UCS Fabric interconecta-se	Cisco UCS 6248UP	• Dois cabos Cat5e para portas de gerenciamento • Dois cabos Cat5e para as interconexões L1, L2, por par de interconexões de tecido • Pelo menos quatro cabos twinaxiais por interconexão de tecido • Pelo menos quatro cabos FC por interconexão de malha
	Cisco UCS 6296UP	Cisco UCS 6332-16UP
	Cisco UCS 6454	Cisco UCS 6332
	• Dois cabos Cat5e para portas de gerenciamento • Dois cabos Cat5e para as interconexões L1, L2, por par de interconexões de tecido • Pelo menos quatro cabos twinaxiais por interconexão de tecido	Cisco UCS 6324
	• Duas portas de gerenciamento 10/100/1000Mbps • Pelo menos dois cabos twinaxiais por interconexão de tecido	Switches Cisco Nexus 5000 e 7000 Series
	Cisco Série Nexus 5000	
• Pelo menos dois cabos de fibra 10GbE ou twinaxial por interrutor • Pelo menos dois cabos FC por switch (se for necessária conectividade FC/FCoE)	Cisco Série Nexus 7000	Switches Cisco Nexus 9000 Series

Hardware	Número do modelo	Cabos necessários
Cisco Série Nexus 9000	Pelo menos dois cabos 10GbE por interrutor	Controladores NetApp FAS
AFF Série A.	• Um par de cabos SAS ou SATA por controlador de armazenamento • Pelo menos dois cabos FC por controladora, se estiver usando FC legado • Pelo menos dois cabos 10GbE por controlador • Pelo menos um cabo GbE para gerenciamento por controladora • Para o ONTAP, são necessários oito cabos twinaxiais curtos por par de comutadores de interconexão de cluster	
Série FAS	Compartimentos de disco NetApp	DS212C
Dois cabos SAS, SATA ou FC por compartimento de disco		DS224C
		DS460C
		NS224

Especificações técnicas e referências

As especificações técnicas fornecem detalhes sobre os componentes de hardware em uma solução FlexPod, como chassi, FEXs, servidores, switches e controladores de armazenamento.

Chassi do servidor blade da série B do Cisco UCS

As especificações técnicas do chassi do servidor blade da série B do Cisco UCS, como mostrado na tabela abaixo, incluem os seguintes componentes:

- Número de unidades de rack
- Número máximo de lâminas
- Funcionalidade de malha unificada
- Largura de banda de e/S midplane por servidor
- Número de compartimentos de e/S para FEXs

Componente	Chassi do servidor blade da série Cisco UCS 5100
Unidades de rack	6

Componente	Chassi do servidor blade da série Cisco UCS 5100
Lâminas de largura total máxima	4
Lâminas de meia largura máxima	8
Capazes de malha unificada	Sim
E/S midplane (e/S)	Até 80Gbps Gbps de largura de banda de e/S por servidor
Compartimentos de e/S para FEXs	Dois compartimentos para Cisco UCS 2104XP, 2204/8XP, 2408XP e 2304 FEXs

Para obter mais informações, consulte "Folha de dados do chassi do servidor blade da série Cisco UCS 5100" .

Servidores blade Cisco UCS B-Series

As especificações técnicas dos servidores blade da série B do Cisco UCS, como mostrado na tabela abaixo, incluem os seguintes componentes:

- Número de soquetes do processador
- Suporte do processador
- Capacidade de memória
- Tamanho e velocidade
- Suporte de inicialização SAN
- Número de slots de adaptador mezzanine
- Taxa de transferência máxima de e/S.
- Fator forma
- Número máximo de servidores por chassi

Componente	Datasheet do Cisco UCS
Cisco UCS B200 M6	"Servidor blade Cisco UCS B200 M6"

Servidores de rack Cisco UCS C-Series

As especificações técnicas dos servidores de rack Cisco UCS C-Series incluem suporte ao processador, capacidade máxima de memória, número de slots PCIe e tamanho do formato. Para obter detalhes adicionais sobre modelos de servidor UCS compatíveis, consulte a "Compatibilidade de hardware do Cisco" lista. As tabelas a seguir ilustram as folhas de dados do servidor de rack C-Series e a opção de chassi do Cisco UCS C-Series, respetivamente.

Componente	Datasheet do Cisco UCS
Cisco UCS C220 M6	"Servidor de rack Cisco UCS C220 M6"
Cisco UCS C225 M6	"Servidor de rack Cisco UCS C225 M6"
Cisco UCS C240 M6	"Servidor de rack Cisco UCS C240 M6"
Cisco UCS C245 M6	"Servidor de rack Cisco UCS C245 M6"

Chassi Cisco UCS X-Series

As especificações técnicas do chassi da série X do Cisco UCS, como mostrado na tabela abaixo, incluem os seguintes componentes:

- Número de unidades de rack
- Número máximo de nós
- Funcionalidade de malha unificada
- Número de compartimentos de e/S para IFMs

Componente	Chassi de nó de computação do Cisco UCS 9508 X.
Unidades de rack	7
Número máximo de nós	8
Capazes de malha unificada	Sim
Compartimentos de e/S para IFMs	Dois compartimentos para módulos inteligentes de tecido Cisco UCS 9108 (IFMs)

Para obter mais informações, consulte "Folha de dados do chassi da série X do Cisco UCS X9508".

Nó de computação do Cisco UCS X-Series

As especificações técnicas do nó de computação do Cisco UCS X-Series, como mostrado na tabela a seguir, incluem os seguintes componentes:

- Número de soquetes do processador
- Suporte do processador
- Capacidade de memória
- Tamanho e velocidade
- Suporte de inicialização SAN
- Número de slots de adaptador mezzanine
- Taxa de transferência máxima de e/S.
- Fator forma
- Número máximo de nós de computação por chassi

Componente	Datasheet do Cisco UCS
Cisco UCS X210c M6	"Nó de computação do Cisco UCS X210c M6"

Recomendação de GPU para FlexPod AI, ML e DL

Os servidores em rack Cisco UCS C-Series listados na tabela abaixo podem ser usados em uma arquitetura FlexPod para hospedar workloads de AI, ML e DL. Os servidores Cisco UCS C480 ml M5 foram criados especificamente para cargas de trabalho de IA, ML e DL e usam GPUs baseadas em SXM2 da NVIDIA, enquanto os outros servidores usam GPUs baseadas em PCIe.

A tabela abaixo também lista as GPUs recomendadas que podem ser usadas com esses servidores.

Servidor	GPUs
Cisco UCS C220 M6	NVIDIA T4
Cisco UCS C225 M6	NVIDIA T4
Cisco UCS C240 M6	NVIDIA TESLA A10, A100
Cisco UCS C245 M6	NVIDIA TESLA A10, A100

Adaptadores Cisco UCS VIC para servidores blade Cisco UCS B-Series

As especificações técnicas dos adaptadores de placa de interface virtual (VIC) do Cisco UCS para servidores tipo lâmina da série B do Cisco incluem os seguintes componentes:

- Número de portas uplink
- Desempenho por porta (IOPS)
- Potência
- Número de portas blade
- Descarga de hardware
- Suporte para virtualização de entrada/saída única (SR-IOV)

Todas as arquiteturas FlexPod validadas atualmente usam um Cisco UCS VIC. Outros adaptadores são suportados se estiverem listados no NetApp "IMT" e forem compatíveis com a implantação do FlexPod, mas talvez não forneçam todos os recursos descritos nas arquiteturas de referência correspondentes. A tabela a seguir ilustra as folhas de dados do adaptador Cisco UCS VIC.

Componente	Datasheet do Cisco UCS
Adaptadores de interface virtual Cisco UCS	"Folhas de dados do Cisco UCS VIC"

O Cisco UCS Fabric interconecta-se

As especificações técnicas das interconexões de malha do Cisco UCS incluem o tamanho do fator forma, o número total de portas e slots de expansão e a capacidade de taxa de transferência. A tabela a seguir ilustra as folhas de dados da interconexão de malha do Cisco UCS.

Componente	Datasheet do Cisco UCS
Cisco UCS 6248UP	"Interconexões de malha da série Cisco UCS 6200"
Cisco UCS 6296UP	
Cisco UCS 6324	"Interconexão de malha Cisco UCS 6324"
Cisco UCS 6300	"Interconexões de malha da série Cisco UCS 6300"
Cisco UCS 6454	"Interconexões de malha da série Cisco UCS 6400"

Switches Cisco Nexus 5000 Series

As especificações técnicas para os switches Cisco Nexus 5000 Series, incluindo o tamanho do fator forma, o número total de portas e o suporte de módulo e placa filha camada 3, estão contidas na folha de dados de cada família de modelos. Estas fichas técnicas podem ser encontradas na seguinte tabela.

Componente	Datasheet do Cisco Nexus
Cisco Nexus 5548UP	"Switch Cisco Nexus 5548UP"
Cisco Nexus 5596UP (2U)	"Switch Cisco Nexus 5596UP"
Cisco Nexus 56128P	"Switch Cisco Nexus 56128P"
Cisco Nexus 5672UP	"Switch Cisco Nexus 5672UP"

Switches Cisco Nexus 7000 Series

As especificações técnicas dos switches Cisco Nexus 7000 Series, incluindo o tamanho do fator forma e o número máximo de portas, estão contidas no datasheet para cada família de modelos. Estas fichas técnicas podem ser encontradas na seguinte tabela.

Componente	Datasheet do Cisco Nexus
Cisco Nexus 7004	"Switches Cisco Nexus 7000 Series"
Cisco Nexus 7009	
Cisco Nexus 7010	
Cisco Nexus 7018	
Cisco Nexus 7702	"Switches Cisco Nexus 7700 Series"
Cisco Nexus 7706	
Cisco Nexus 7710	
Cisco Nexus 7718	

Switches Cisco Nexus 9000 Series

As especificações técnicas dos switches Cisco Nexus 9000 estão contidas na folha de dados para cada modelo. As especificações incluem o tamanho do fator de forma, o número de supervisores, o módulo de malha e os slots de placa de linha e o número máximo de portas. Estas fichas técnicas podem ser encontradas na seguinte tabela.

Componente	Datasheet do Cisco Nexus
Cisco Série Nexus 9000	"Switches Cisco Nexus 9000 Series"
Cisco Série Nexus 9500	"Switches Cisco Nexus 9500 Series"
Cisco Série Nexus 9300	"Switches Cisco Nexus 9300 Series"
Cisco Nexus 9336PQP chave de fenda	"Cisco Nexus 9336PQP chave de fenda"
Cisco Série Nexus 9200	"Switches da plataforma Cisco Nexus 9200"

Controlador de infraestrutura de políticas de aplicações da Cisco

Ao implantar o Cisco ACI, além dos itens na "Switches Cisco Nexus 9000 Series"seção , você deve configurar três APICS Cisco. A tabela a seguir lista a folha de dados do Cisco APIC.

Componente	Datasheet do Cisco Application Policy Infrastructure
Controlador de infraestrutura de políticas de aplicações da Cisco	"Folha de dados Cisco APIC"

Detalhes do extensor de tecido Cisco Nexus

As especificações técnicas do Cisco Nexus FEX incluem velocidade, número de portas e links fixos e tamanho do fator de forma.

A tabela a seguir lista a folha de dados do Cisco Nexus 2000 Series FEX.

Componente	Folha de dados do extensor de tecido Cisco Nexus
Extensores de tecido da série Cisco Nexus 2000	"Folha de dados do Nexus 2000 Series FEX"

Módulos SFP

Para obter informações sobre os módulos SFP, consulte os seguintes recursos:

- Para obter informações sobre o Cisco 10Gb SFP, "Módulos Gigabit Cisco 10" consulte .
- Para obter informações sobre o Cisco 25GB SFP, "Módulos Gigabit Cisco 25" consulte .
- Para obter informações sobre o módulo QSFP do Cisco, consulte "Folha de dados dos módulos Cisco 40GBASE QSFP".
- Para obter informações sobre o Cisco 100GB SFP, "Módulos Gigabit Cisco 100" consulte .
- Para obter informações sobre o módulo Cisco FC SFP, consulte "Folha de dados dos transcetores conetáveis da família Cisco MDS 9000".
- Para obter informações sobre todos os módulos Cisco SFP e transcetor suportados, "Notas de instalação do módulo transcetor Cisco SFP e SFP" consulte e "Módulos transceiver Cisco".

Controladores de storage NetApp

As especificações técnicas dos controladores de storage NetApp incluem os seguintes componentes:

- Configuração do chassi
- Número de unidades de rack
- Quantidade de memória
- Armazenamento em cache NetApp FlashCache
- Tamanho agregado
- Tamanho do volume
- Número de LUNs
- Armazenamento de rede suportado
- Número máximo de volumes NetApp FlexVol
- Número máximo de hosts SAN suportados
- Número máximo de cópias Snapshot

Série FAS

Todos os modelos disponíveis de controladores de storage FAS são compatíveis para uso em um data center FlexPod. Especificações detalhadas para todos os controladores de storage da série FAS estão disponíveis no "NetApp Hardware Universe". Consulte a documentação específica da plataforma listada na tabela a seguir para obter informações detalhadas sobre um modelo FAS específico.

Componente	Documentação da plataforma do controlador da série FAS
Série FAS9000	"Folha de dados da série FAS9000"
Série FAS8700	"Folha de dados da série FAS8700"
Série FAS8300	"Folha de dados da série FAS8300"
Série FAS500f	"Folha de dados da série FAS500f"
Série FAS2700	"Folha de dados da série FAS2700"

AFF Série A.

Todos os modelos atuais de controladores de storage NetApp AFF A-Series são compatíveis para uso no FlexPod. Informações adicionais podem ser encontradas na "Especificações técnicas da AFF" folha de dados e na "NetApp Hardware Universe". Consulte a documentação específica da plataforma listada na tabela a seguir para obter informações detalhadas sobre um modelo AFF específico.

Componente	Documentação da plataforma de controlador AFF A-Series
NetApp AFF A800	"Documentação da Plataforma AFF A800"
NetApp AFF A700	"Documentação da Plataforma AFF A700"
NetApp AFF A700s	"Documentação da Plataforma AFF A700s"
NetApp AFF A400	"Documentação da Plataforma AFF A400"
NetApp AFF A250	"Documentação da Plataforma AFF A250"

AFF ASA Série A.

Todos os modelos atuais de controladores de storage NetApp AFF ASA A-Series são compatíveis para uso no FlexPod. Informações adicionais podem ser encontradas nos recursos de documentação de todos os Arrays SAN, no relatório técnico do ONTAP AFF All SAN Array System e no NetApp Hardware Universe. Consulte a documentação específica da plataforma listada na tabela a seguir para obter informações detalhadas sobre um modelo AFF específico.

Componente	Documentação da plataforma de controlador AFF A-Series
NetApp AFF ASA A800	"Documentação da Plataforma AFF ASA A800"
NetApp AFF ASA A700	"Documentação da plataforma AFF ASA A700"
NetApp AFF ASA A400	"Documentação da Plataforma AFF ASA A400"
NetApp AFF ASA A250	"Documentação da Plataforma AFF ASA A250"
NetApp AFF ASA A220	"Documentação da plataforma AFF ASA A220"

Compartimentos de disco NetApp

As especificações técnicas dos compartimentos de disco NetApp incluem o tamanho do fator forma, o número de unidades por compartimento e os módulos de e/S de gaveta. Essa documentação pode ser encontrada na tabela a seguir. Para obter mais informações, consulte "Especificações técnicas dos compartimentos de disco e Mídia de storage da NetApp" e "NetApp Hardware Universe" .

Componente	Documentação do compartimento de disco NetApp FAS/AFF
Compartimento de disco NetApp DS212C	"DS212C Documentação do compartimento de disco"
Compartimento de disco NetApp DS224C	"DS224C Documentação do compartimento de disco"
Compartimento de disco NetApp DS460C	"DS460C Documentação do compartimento de disco"
Compartimento de disco SSD NVMe-SSD NetApp NS224	"NS224 Documentação do compartimento de disco"

Unidades NetApp

As especificações técnicas das unidades NetApp incluem o tamanho do fator forma, a capacidade do disco, as RPM do disco, as controladoras compatíveis e os requisitos de versão do ONTAP. Essas especificações podem ser encontradas na seção unidades do "NetApp Hardware Universe".

Equipamento legado

O FlexPod é uma solução flexível que permite utilizar os equipamentos existentes e os novos equipamentos atualmente à venda pela Cisco e NetApp. Ocasionalmente, certos modelos de equipamentos da Cisco e da NetApp são designados como fim de vida útil (EOL).

Mesmo que esses modelos de equipamentos não estejam mais disponíveis, se você comprou um desses modelos antes da data de fim de disponibilidade (EOA), você pode usar esse equipamento em uma configuração do FlexPod. Uma lista completa dos modelos de equipamentos antigos suportados no FlexPod que não estão mais à venda pode ser referenciada no "Índice de término da disponibilidade dos programas de produtos de suporte e Serviço NetApp".

Para obter mais informações sobre equipamentos Cisco legados, consulte os avisos EOL e EOA do Cisco para "Servidores em rack Cisco UCS C-Series", "Servidores blade Cisco UCS B-Series" e "Switches Nexus".

O suporte à malha FC legada inclui o seguinte:

- 2GB tecido
- 4GB tecido

O software legado inclui o seguinte:

- NetApp Data ONTAP operando no modo 7D, 7.3.5D e posterior
- ONTAP 8,1.x a 9,0.x
- Cisco UCS Manager 1,3 e posterior
- Cisco UCS Manager 2,1 a 2.2.7

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- Documentação do produto NetApp

  "https://docs.netapp.com/"

- Comunicações de suporte da NetApp

  "https://mysupport.netapp.com/info/communications/index.html"

- Ferramenta de Matriz de interoperabilidade NetApp (IMT)

  "https://mysupport.netapp.com/matrix/#welcome"

- NetApp Hardware Universe

  "https://hwu.netapp.com/"

- Suporte à NetApp

  "https://mysupport.netapp.com/"

Data center FlexPod

Data center FlexPod com NetApp SnapMirror Business Continuity e ONTAP 9.10

TR-4920: Centro de dados FlexPod com continuidade de Negócios NetApp SnapMirror e ONTAP 9.10

Jyh-shing Chen, NetApp

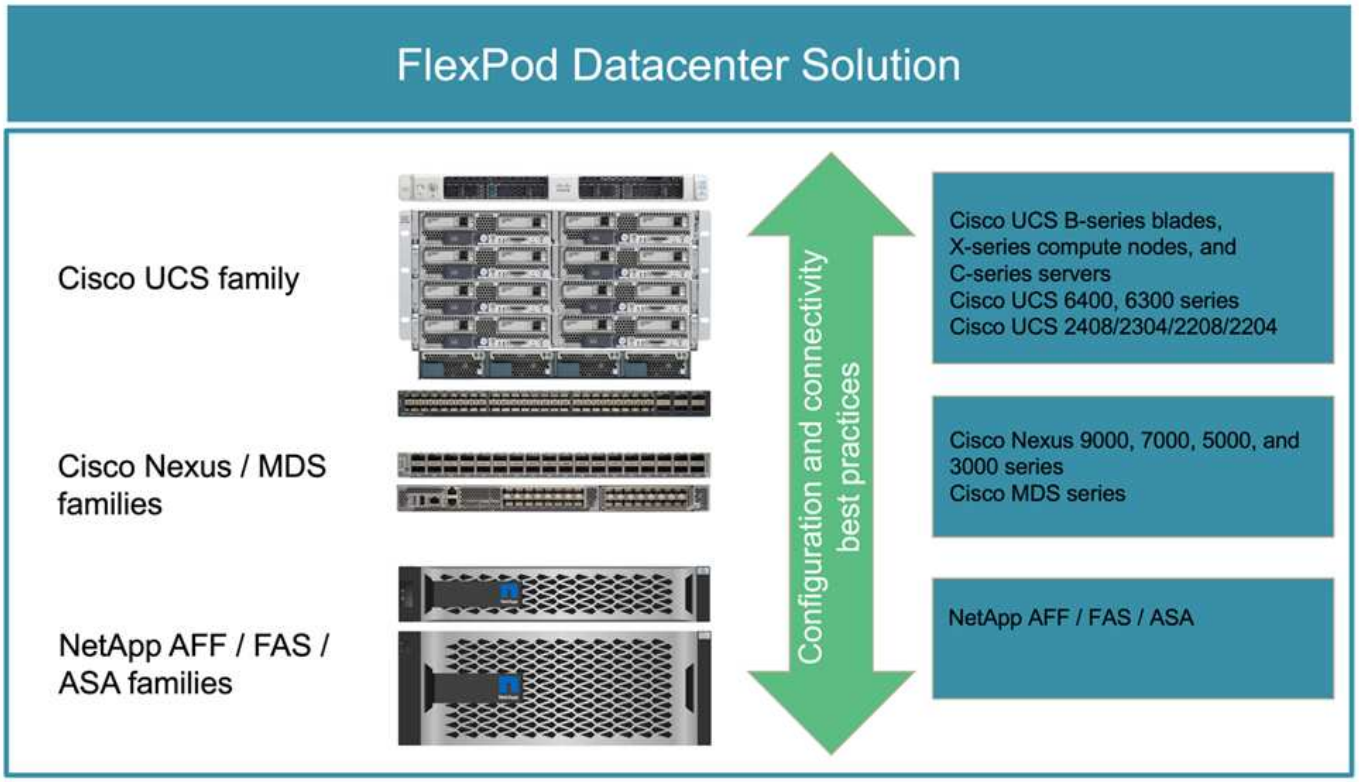
Introdução

Solução FlexPod

O FlexPod é uma arquitetura de data center de infraestrutura convergente prática recomendada que inclui os seguintes componentes do Cisco e do NetApp:

- Sistema de computação unificada da Cisco (Cisco UCS)
- Famílias de switches Cisco Nexus e MDS
- Sistemas NetApp FAS, NetApp AFF e NetApp All SAN Array (ASA)

A figura a seguir mostra alguns dos componentes usados para criar soluções FlexPod. Esses componentes são conectados e configurados de acordo com as práticas recomendadas do Cisco e do NetApp para fornecer uma plataforma ideal para executar uma variedade de workloads empresariais com confiança.



Um grande portfólio de Cisco Validated designs (CVDs) e NetApp Verified Architectures (NVAs) estão disponíveis. Esses CVDs e NVAs cobrem todas as principais cargas de trabalho de data center e são o

resultado de colaborações e inovações contínuas entre a NetApp e a Cisco em soluções FlexPod.

Incorporando testes e validações extensivos em seu processo de criação, os CVDs e NVAs da FlexPod fornecem designs de arquitetura de solução de referência e guias de implantação passo a passo para ajudar parceiros e clientes a implantar e adotar soluções da FlexPod. Ao usar esses CVDs e NVAs como guias de projeto e implementação, as empresas podem reduzir riscos, reduzir o tempo de inatividade da solução e aumentar a disponibilidade, escalabilidade, flexibilidade e segurança das soluções FlexPod que implantam.

Cada uma das famílias de componentes do FlexPod mostradas (Cisco UCS, switches Cisco Nexus/MDS e storage NetApp) oferece opções de plataforma e recursos para escalar a infraestrutura para cima ou para baixo, oferecendo suporte aos recursos e funcionalidades necessários nas práticas recomendadas de configuração e conectividade do FlexPod. O FlexPod também pode fazer escalabilidade horizontal para ambientes que exigem várias implantações consistentes com a implementação de stacks FlexPod adicionais.

Recuperação de desastres e continuidade dos negócios

Existem vários métodos que as empresas podem adotar para garantir que possam recuperar rapidamente seus aplicativos e serviços de dados de desastres. Ter um plano de recuperação de desastres (DR) e continuidade dos negócios (BC), implementar uma solução que atenda aos objetivos de negócios e realizar testes regulares dos cenários de desastre permite que as empresas se recuperem de um desastre e continuem serviços comerciais críticos após uma situação de desastre.

As empresas podem ter diferentes requisitos de DR e BC para diferentes tipos de aplicativos e serviços de dados. Alguns aplicativos e dados podem não ser necessários durante uma situação de emergência ou desastre, enquanto outros podem precisar estar continuamente disponíveis para atender aos requisitos empresariais.

Para aplicativos de missão crítica e serviços de dados que possam interromper seus negócios quando não estiverem disponíveis, uma avaliação cuidadosa é necessária para responder a perguntas como o tipo de cenários de manutenção e desastre que a empresa precisa considerar, a quantidade de dados que a empresa pode perder em caso de desastre e a rapidez com que a recuperação pode e deve ocorrer.

Para empresas que dependem de serviços de dados para geração de receita, os serviços de dados podem precisar ser protegidos por uma solução que pode suportar não apenas vários cenários de ponto único de falha, mas também um cenário de desastre de interrupção no local para fornecer operações de negócios contínuas.

Objetivo do ponto de restauração e objetivo de tempo de recuperação

O objetivo do ponto de restauração (RPO) mede a quantidade de dados que você pode perder em termos de tempo ou o ponto em que pode recuperar os dados. Com um plano de backup diário, uma empresa pode perder um dia de dados, porque as alterações feitas nos dados desde o último backup podem ser perdidas em um desastre. Para serviços de dados essenciais aos negócios e essenciais, é possível que você precise de um RPO zero e de um plano e infraestruturas associados para proteger os dados sem perda de dados.

O objetivo de tempo de recuperação (rto) mede quanto tempo você pode se dar ao luxo de não ter os dados disponíveis ou a rapidez com que os serviços de dados precisam ser restaurados. Por exemplo, uma empresa pode ter uma implementação de backup e recuperação que usa fitas tradicionais para certos conjuntos de dados devido ao seu tamanho. Como resultado, para restaurar os dados das fitas de backup, pode levar várias horas ou até dias se houver uma falha de infraestrutura. As considerações de tempo também devem incluir tempo para fazer backup da infraestrutura, além de restaurar dados. Para serviços de dados essenciais, você pode exigir um rto muito baixo e, assim, só pode tolerar um tempo de failover de segundos ou minutos para colocar os serviços de dados on-line de volta para continuidade dos negócios com rapidez.

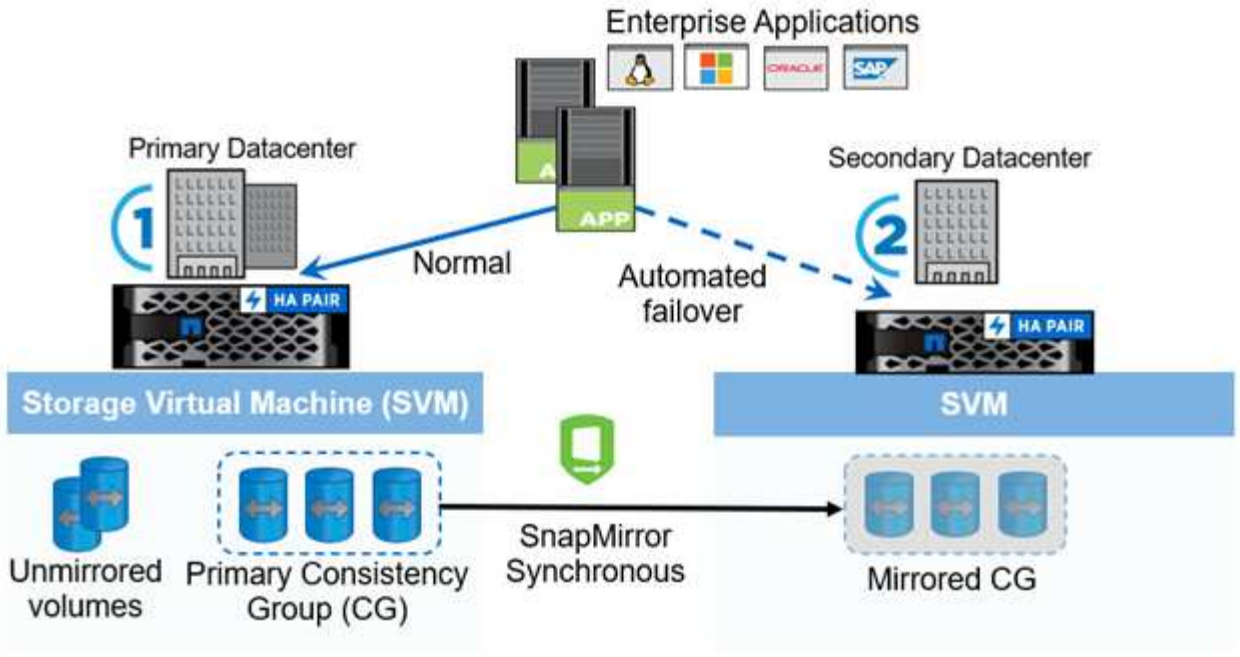
SM-BC

A partir do ONTAP 9.8, você pode proteger workloads SAN para failover transparente de aplicações com o NetApp SM-BC. Você pode criar relacionamentos de grupo de consistência entre dois clusters AFF ou dois clusters ASA para replicação de dados a fim de alcançar RPO zero e rto quase zero.

A solução SM-BC replica dados usando a tecnologia SnapMirror Synchronous em uma rede IP. Ele fornece granularidade no nível da aplicação e failover automático para proteger seus serviços de dados essenciais aos negócios, como Microsoft SQL Server, Oracle, etc., com LUNs SAN baseados em protocolo iSCSI ou FC. Um Mediador ONTAP implantado em um terceiro local monitora a solução SM-BC e permite o failover automático em caso de desastre no local.

Um grupo de consistência (CG) é uma coleção de volumes FlexVol que oferece uma garantia de consistência de ordem de gravação para o workload do aplicativo que precisa ser protegido para manter a continuidade dos negócios. Ele permite cópias Snapshot simultâneas de uma coleção de volumes consistentes com falhas. Uma relação SnapMirror, também conhecida como relação CG, é estabelecida entre um CG de origem e um CG de destino. O grupo de volumes escolhidos para fazer parte de um CG pode ser mapeado para uma instância de aplicativo, um grupo de instâncias de aplicativos ou para uma solução completa. Além disso, os relacionamentos de grupo de consistência SM-BC podem ser criados ou excluídos sob demanda com base em requisitos e mudanças de negócios.

Conforme ilustrado na figura a seguir, os dados no grupo de consistência são replicados para um segundo cluster do ONTAP para recuperação de desastres e continuidade dos negócios. As aplicações têm conectividade com os LUNs nos dois clusters do ONTAP. A e/S normalmente é servida pelo cluster primário e é retomada automaticamente do cluster secundário se um desastre ocorrer no primário. Ao projetar uma solução SM-BC, as contagens de objetos suportados para as relações CG (por exemplo, um máximo de 20 CGS e máximo de 200 endpoints) devem ser observadas para evitar exceder os limites suportados.



"Próximo: Solução FlexPod SM-BC."

Solução FlexPod SM-BC

"Anterior: Introdução."

Visão geral da solução

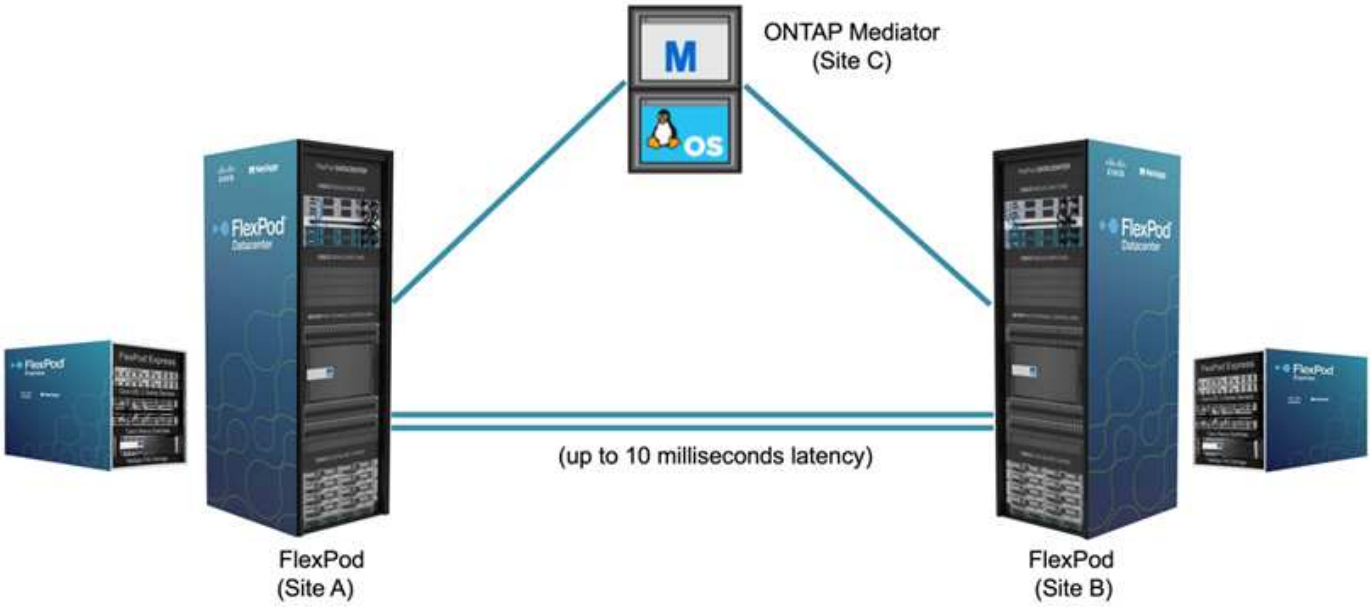
Em um alto nível, uma solução FlexPod SM-BC consiste em dois sistemas FlexPod, localizados em dois locais separados por alguma distância, conetados e emparelhados juntos para fornecer uma solução de data center altamente disponível, altamente flexível e altamente confiável que pode fornecer continuidade dos negócios apesar de uma falha no local.

Além de implantar duas novas infraestruturas FlexPod para criar uma solução FlexPod SM-BC, a solução também pode ser implementada em duas infraestruturas FlexPod existentes que são compatíveis com SM-BC ou adicionando um novo FlexPod ao ponto com um FlexPod existente.

Os dois sistemas FlexPod em uma solução FlexPod SM-BC não precisam ser idênticos nas configurações. No entanto, os dois clusters ONTAP precisam ser das mesmas famílias de storage, dois sistemas AFF ou dois ASA, mas não necessariamente o mesmo modelo de hardware. A solução SM-BC não suporta sistemas FAS.

Os dois locais FlexPod exigem conetividade de rede que atenda aos requisitos de largura de banda e qualidade do serviço da solução e tenha latência de ida e volta de menos de 10 milissegundos (10ms ms) entre locais, conforme exigido pela solução ONTAP SM-BC. Para esta validação da solução FlexPod SM-BC, os dois locais FlexPod são interconetados através de uma rede de camada 2 estendida no mesmo laboratório.

A solução NetApp ONTAP SM-BC oferece replicação síncrona entre os dois clusters de storage do NetApp para alta disponibilidade e recuperação de desastres em um campus ou área metropolitana. O Mediador ONTAP implantado em um terceiro local monitora a solução e permite o failover automatizado em caso de desastre no local. A figura a seguir fornece uma visão de alto nível dos componentes da solução.



Com a solução FlexPod SM-BC, você pode implantar uma nuvem privada baseada no VMware vSphere em uma infraestrutura distribuída e integrada. A solução integrada permite que vários locais sejam coordenados como uma única infraestrutura de solução para proteger os serviços de dados de uma variedade de cenários de ponto único de falha e uma falha completa no local.

Este relatório técnico destaca algumas das considerações de design de ponta a ponta da solução FlexPod SM-BC. Os profissionais são encorajados a consultar informações disponíveis nos vários CVDs e AVDs FlexPod para obter detalhes adicionais de implementação da solução FlexPod.

Embora a solução tenha sido validada com a implantação de dois sistemas FlexPod baseados nas práticas recomendadas do FlexPod, conforme documentado em CVDs, ela leva em consideração os requisitos da

solução SM-BC. A solução FlexPod SM-BC implementada discutida neste relatório foi validada para resiliência e tolerância a falhas durante vários cenários de falha, bem como um cenário simulado de falha do local.

Requisitos da solução

A solução FlexPod SM-BC foi projetada para atender aos seguintes requisitos principais:

- Continuidade dos negócios de aplicações essenciais aos negócios e serviços de dados em caso de falha completa do data center (local)
- Disposição flexível e distribuída do workload com mobilidade de workload entre data centers
- Afinidade do local onde os dados da máquina virtual são acessados localmente, a partir do mesmo local do data center, durante as operações normais
- Recuperação rápida sem perda de dados quando ocorre uma falha no local

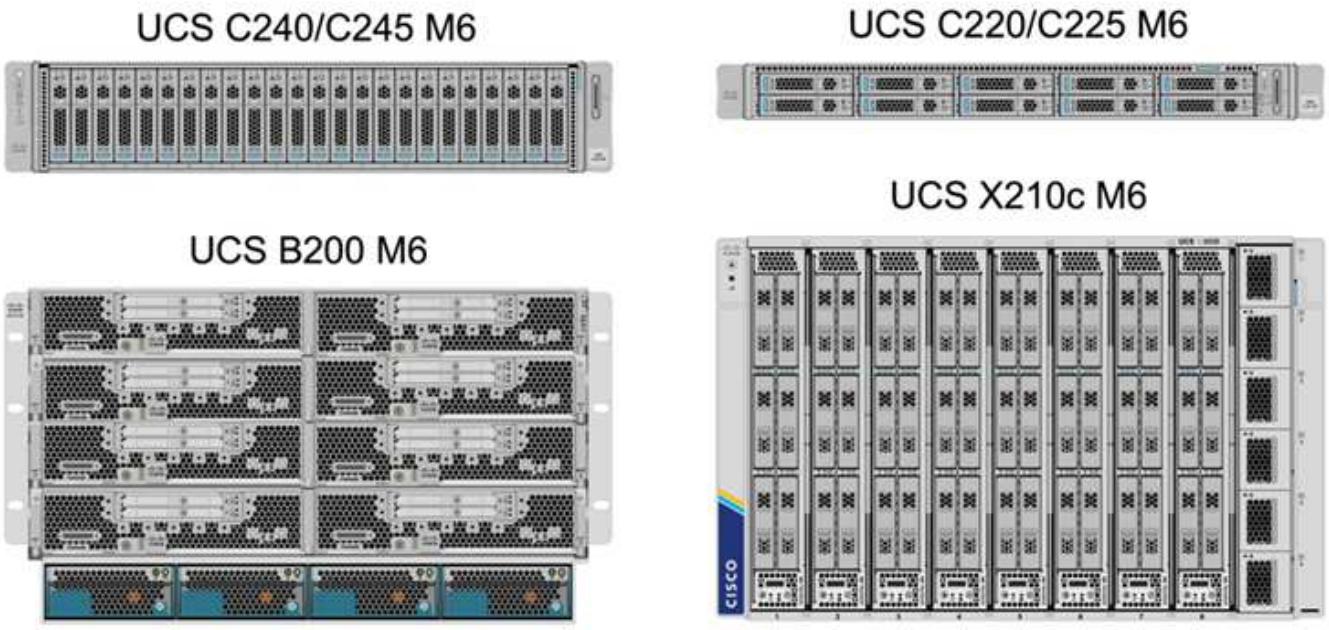
Componentes da solução

Componentes de computação do Cisco

O Cisco UCS é uma infraestrutura de computação integrada que fornece recursos de computação unificados, malha unificada e gerenciamento unificado. Ele permite que as empresas automatizem e acelerem a implantação de aplicativos, incluindo workloads de virtualização e bare-metal. O Cisco UCS dá suporte a uma ampla variedade de casos de uso de implantação, incluindo locais remotos e filiais, data centers e casos de uso de nuvem híbrida. Dependendo dos requisitos específicos da solução, a implementação de computação do FlexPod Cisco pode utilizar vários componentes em diferentes escalas. As subseções a seguir fornecem informações adicionais sobre alguns dos componentes do UCS.

Nó de computação e servidor UCS

A figura a seguir mostra alguns exemplos dos componentes do servidor UCS, incluindo servidores em rack UCS C- Series, chassi UCS 5108 com servidores blade B-Series e o novo chassi UCS X9508 com nós de computação X-Series. Os servidores de rack da série C Cisco UCS estão disponíveis em um fator de forma de unidade de rack (RU), modelos baseados em CPU Intel e AMD e com várias velocidades e núcleos de CPU, memória e opções de e/S. Os servidores blade da série B do Cisco UCS e os novos nós de computação da série X também estão disponíveis com várias opções de CPU, memória e e e/S, e todos eles têm suporte na arquitetura FlexPod para atender aos diversos requisitos empresariais.



Além da última geração de servidores em rack C220/C225/C240/C245 M6U, B200 M6 servidores blade e X210c nós de computação mostrados nesta figura, gerações anteriores de servidores em rack e blade também podem ser usadas se ainda forem compatíveis.

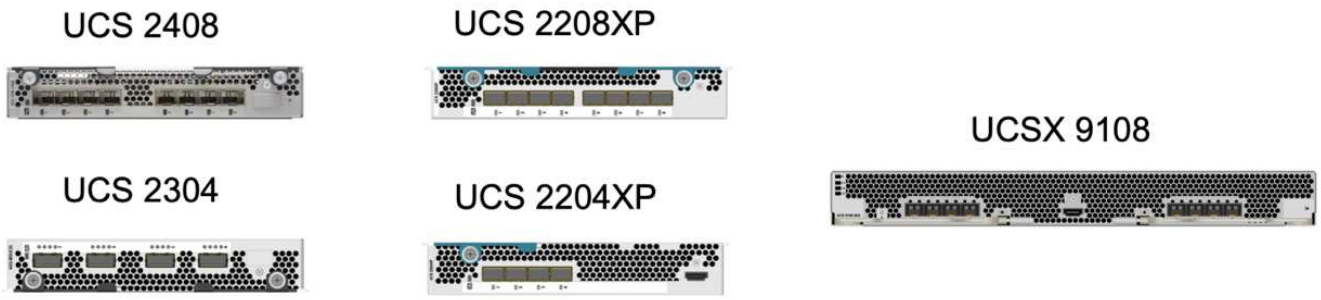
Módulo de e/S e módulo de tecido inteligente

O módulo de e/S (IOM)/extensor de malha e o módulo de malha inteligente (IFM) fornecem conetividade de malha unificada para o chassi do servidor blade Cisco UCS 5108 e o chassi da série X do Cisco UCS X9508, respetivamente.

A quarta geração do UCS IOM 2408 tem oito portas Ethernet unificadas de 25 G para conetar o chassi do UCS 5108 com o Fabric Interconnect (FI). Cada 2408 tem quatro conetividade Ethernet de backplane 10-G através do midplane para cada servidor blade no chassi.

O UCSX 9108 25G IFM tem oito portas Ethernet unificadas de 25 G para conetar os servidores blade no chassi UCS X9508 com interconexões de malha. Cada 9108 tem quatro conexões 25-G em direção a cada nó de computação UCS X210c no chassi X9108. O 9108 IFM também funciona em conjunto com a interconexão de tecido para gerenciar o ambiente do chassi.

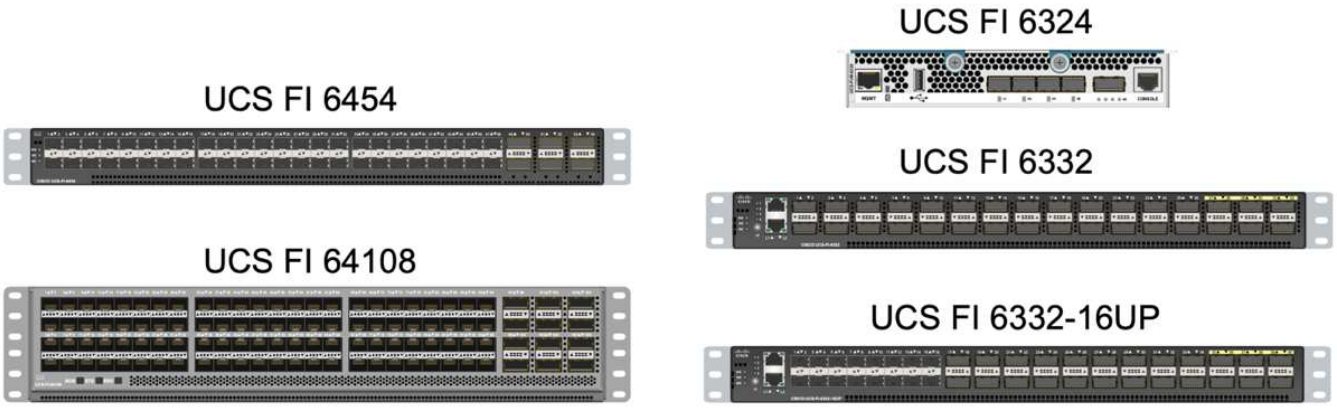
A figura a seguir mostra as gerações UCS 2408 e IOM anteriores para o chassi UCS 5108 e o IFM 9108 para o chassi X9508.



O tecido UCS interconecta-se

As interconexões de malha do Cisco UCS (FIs) fornecem conectividade e gerenciamento para todo o Cisco UCS. Normalmente implantadas como um par ativo/ativo, as FIs do sistema integram todos os componentes em um único domínio de gerenciamento altamente disponível, controlado pelo Cisco UCS Manager ou pelo Cisco Intersight. As FIs Cisco UCS fornecem uma única malha unificada para o sistema com comutação de corte e baixa latência e sem perdas que dá suporte ao tráfego de LAN, SAN e gerenciamento usando um único conjunto de cabos.

Existem duas variantes para as FIs Cisco UCS de quarta geração: UCS FI 6454 e 64108. Eles incluem suporte para portas Ethernet de 10/25 Gbps, portas Ethernet de 1/10/25 Gbps, portas Ethernet de ligação ascendente de 40/100 Gbps e portas unificadas que podem suportar Ethernet de 10/25 Gigabit ou Fibre Channel de 8/16/32 Gbps. A figura a seguir mostra as FIs Cisco UCS de quarta geração, juntamente com os modelos de terceira geração que também são compatíveis.

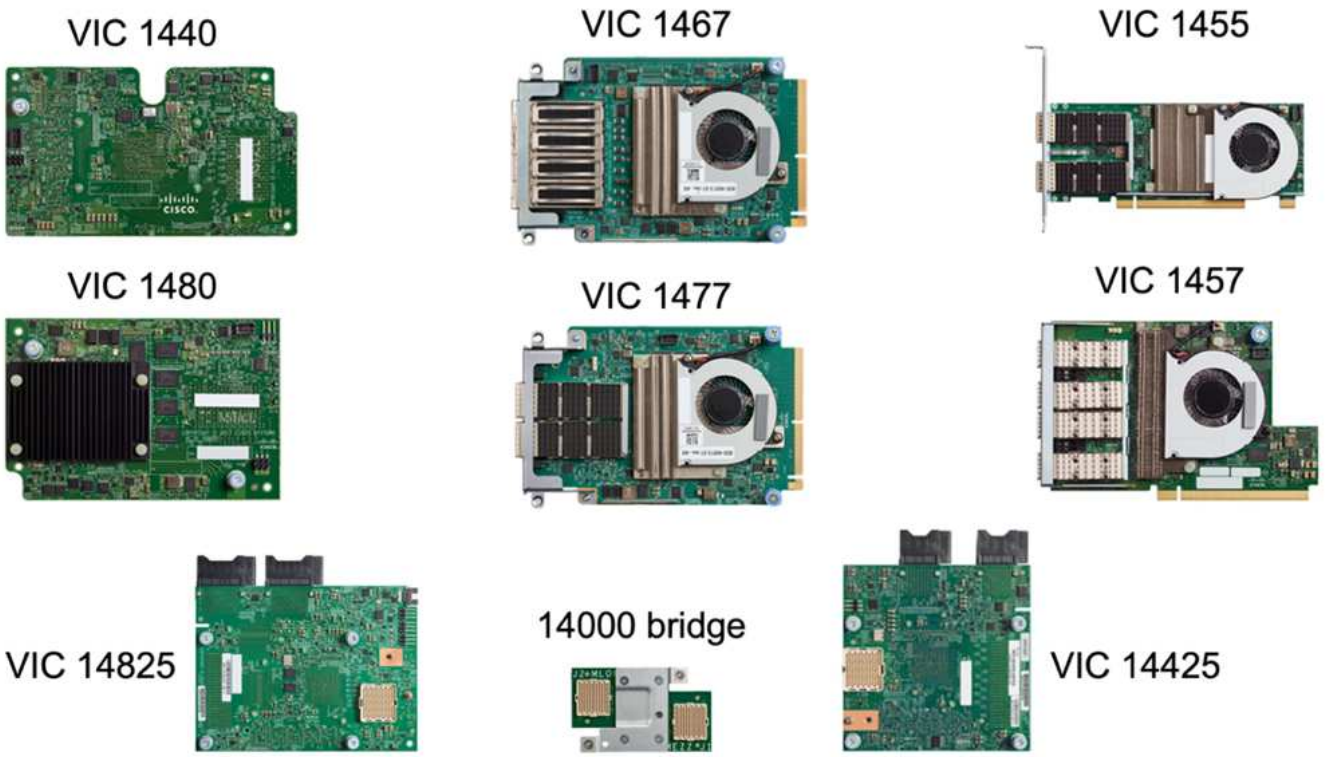


Para dar suporte ao chassi do Cisco UCS X-Series, são necessárias interconexões de malha de quarta geração configuradas no modo gerenciado de Intersight (IMM). No entanto, o chassi da série B do Cisco UCS 5108 pode ser suportado tanto no modo IMM quanto no modo gerenciado do UCSM.

O UCS Fi 6324 usa o fator de forma IOM e é incorporado em um chassi UCS Mini para implantações que exigem apenas um pequeno domínio UCS.

Cartões de interface virtual UCS

As placas de interface virtual Cisco UCS (VICS) unificam o gerenciamento do sistema e a conetividade LAN e SAN para servidores de rack e blade. Ele suporta até 256 dispositivos virtuais, seja como placas de interface de rede virtual (vNICs) ou como adaptadores de barramento de host virtual (vHBAs) usando a tecnologia Cisco SingleConnect. Como resultado da virtualização, as placas VIC simplificam muito a conetividade de rede e reduzem o número de adaptadores de rede, cabos e portas de switch necessários para a implantação da solução. A figura a seguir mostra alguns dos VICS do Cisco UCS disponíveis para os servidores série B e série C e os nós de computação da série X.



Os diferentes modelos de adaptadores suportam servidores blade e rack diferentes com diferentes contagens de portas, velocidades de portas e fatores de forma de LAN modular na placa-mãe (mLOM), placas mezzanine e interfaces PCIe. Os adaptadores podem suportar algumas combinações de Ethernet 10/25/40/100-G e Fibre Channel over Ethernet (FCoE). Eles incorporam a tecnologia de adaptador de rede convergente (CNA) da Cisco, suportam um conjunto abrangente de recursos e simplificam o gerenciamento de adaptadores e a implantação de aplicativos. Por exemplo, o VIC suporta a tecnologia de Extensor de malha de máquina virtual de data center (VM-FEX) da Cisco, que estende as portas de interconexão de malha Cisco UCS para máquinas virtuais, simplificando assim a implantação da virtualização do servidor.

Com uma combinação de Cisco VIC em mLOM, mezzanine e configurações de expansores de portas e placas de ponte, você pode aproveitar ao máximo a largura de banda e a conetividade disponíveis para os servidores blade. Por exemplo, usando os dois links 25-G no VIC 14825 (mLOM) e 14425 (mezzanine) e 14000 (bridge card) para o nó de computação X210c, a largura de banda combinada do VIC é de 2 x 50-G e 2 x 50-G, ou 100g por Fabric/IFM e 200g total por servidor com a configuração dupla IFM.

Para obter detalhes sobre as famílias de produtos Cisco UCS, especificações técnicas e documentações, consulte o "UCS do Cisco" site para obter informações.

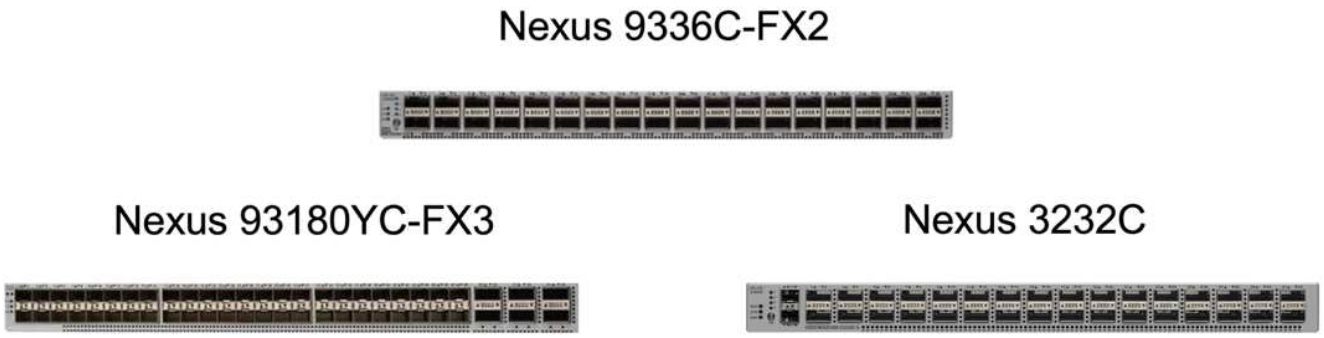
Componentes de comutação Cisco

Switches Nexus

A FlexPod usa os switches da série Cisco Nexus para fornecer malha de comutação Ethernet para comunicações entre os controladores de storage Cisco UCS e NetApp. Todos os modelos de switch Cisco Nexus com suporte atual, incluindo o Cisco Nexus 3000, 5000, 7000 e 9000 Series, são compatíveis com a implantação do FlexPod.

Ao selecionar um modelo de switch para implantação do FlexPod, há muitos fatores a serem considerados, como desempenho, velocidade da porta, densidade da porta, latência de comutação e protocolos como suporte a ACI e VXLAN, para seus objetivos de projeto, bem como o tempo de suporte dos switches.

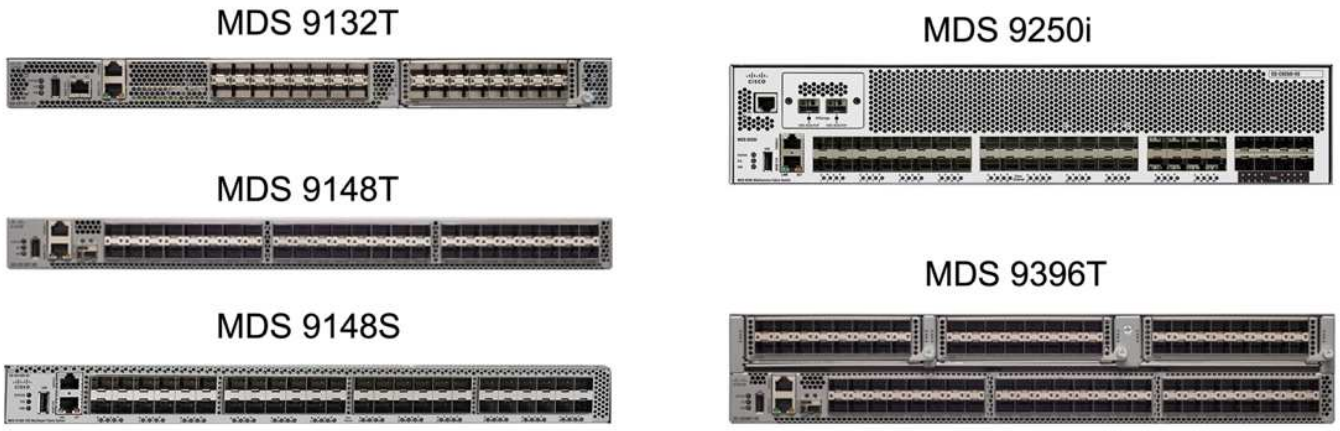
A validação de muitos CVDs FlexPod recentes usa switches Cisco Nexus 9000 da série, como o Nexus 9336C-FX2 e o Nexus 93180YC-FX3, que oferecem portas 40/100g e 10//25G de alto desempenho, baixa latência e eficiência de energia excecional em um formato compacto de 1UU. As velocidades adicionais são suportadas através de portas uplink e cabos de arranque. A figura a seguir mostra alguns switches Cisco Nexus 9k e 3k, incluindo o Nexus 9336C-FX2 e o Nexus 3232C usados para essa validação.



Consulte "Switches de data center Cisco" para obter mais informações sobre os switches Nexus disponíveis e suas especificações e documentações.

Switches MDS

Os switches de malha Cisco MDS 9100/9200/9300 Series são um componente opcional na arquitetura do FlexPod. Esses switches são altamente confiáveis, altamente flexíveis, seguros e podem fornecer visibilidade do fluxo de tráfego na malha. A figura a seguir mostra alguns exemplos de switches MDS que podem ser usados para criar malhas SAN FC redundantes para uma solução FlexPod que atenda aos requisitos de aplicativos e negócios.



Os switches de malha multicamadas 32G de alto desempenho do Cisco MDS 9132T/9148T/9396T são econômicos e altamente confiáveis, flexíveis e dimensionáveis. Os recursos e funções avançados de rede de storage vêm com facilidade de gerenciamento e são compatíveis com todo o portfólio da família Cisco MDS 9000 para uma implementação de SAN confiável.

Os recursos de telemetria e análise de SAN de última geração estão integrados a essa plataforma de hardware de última geração. Os dados de telemetria extraídos da inspeção dos cabeçalhos de quadros podem ser transmitidos para uma plataforma de visualização de análise, incluindo o Gerenciador de rede do Centro de dados Cisco. Os switches MDS com suporte a FC de 16G GB, como o MDS 9148S, também são compatíveis com o FlexPod. Além disso, os switches MDS de vários serviços, como o MDS 9250i, que oferece suporte aos protocolos FCoE e FCIP, além do protocolo FC, também fazem parte do portfólio de

soluções da FlexPod.

Em switches MDS semi-modulares, como 9132T e 9396T, módulos de expansão de porta adicionais e licenças de porta podem ser adicionados para oferecer suporte à conetividade de dispositivos adicionais. Nos switches fixos, como 9148T, licenças de porta adicionais podem ser adicionadas conforme necessário. Essa flexibilidade de pagamento conforme o uso fornece um componente de despesas operacionais para ajudar a reduzir as despesas de capital para a implementação e operação da infraestrutura de SAN baseada em switch MDS.

Consulte "Switches de malha Cisco MDS" para obter mais informações sobre os switches de malha MDS disponíveis e consulte "NetApp IMT" e "Lista de compatibilidade de hardware e software do Cisco" para obter uma lista completa de switches SAN compatíveis.

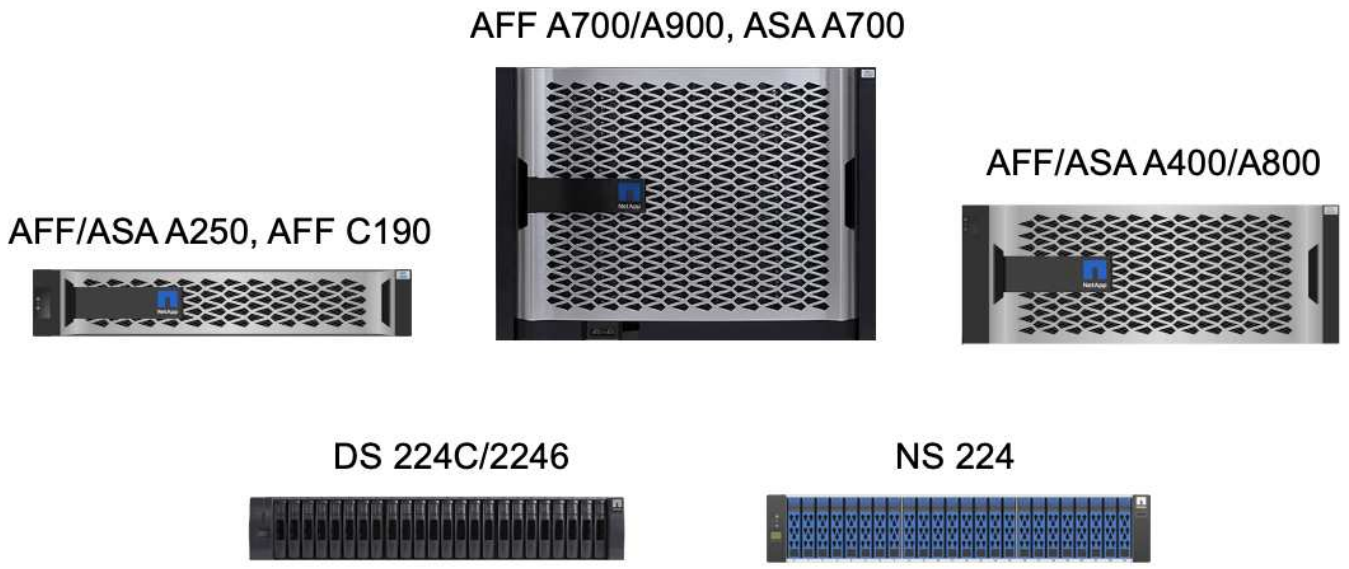
Componentes do NetApp

Controladores NetApp AFF ou ASA redundantes que executam o software ONTAP 9,8 ou versões posteriores são necessários para criar uma solução FlexPod SM-BC. A versão mais recente do ONTAP, atualmente 9.10.1, é recomendada para a implantação do SM-BC para aproveitar as inovações contínuas do ONTAP, o desempenho e as melhorias de qualidade e a maior contagem máxima de objetos para o suporte ao SM-BC.

Os controladores NetApp AFF e ASA com inovações e performance líderes do setor fornecem recursos de gerenciamento de dados empresariais e proteção de dados com muitos recursos. Os sistemas AFF e ASA dão suporte a tecnologias NVMe completas, incluindo SSDs conectados a NVMe e conectividade de host front-end NVMe sobre Fibre Channel (NVMe/FC). Você pode melhorar a taxa de transferência de workload e reduzir a latência de I/o com a adoção da infraestrutura SAN baseada em NVMe/FC. Entretanto, armazenamentos de dados baseados em NVMe/FC podem ser usados atualmente apenas para workloads não protegidos pelo SM-BC, pois a solução SM-BC atualmente oferece suporte apenas aos protocolos iSCSI e FC.

Os controladores de storage NetApp AFF e ASA também fornecem uma base de nuvem híbrida para os clientes aproveitarem a mobilidade de dados otimizada habilitada pelo NetApp Data Fabric. Com o Data Fabric, é fácil obter dados da borda onde são gerados para o centro onde são usados e para a nuvem. Assim, é possível aproveitar os recursos de AI e ML flexíveis sob demanda para obter insights de negócios úteis.

Como mostrado na figura a seguir, o NetApp oferece uma variedade de controladoras de storage e gavetas de disco para atender aos seus requisitos de performance e capacidade. Consulte a tabela a seguir para obter links para páginas de produtos para obter informações sobre os recursos e especificações do controlador NetApp AFF e ASA.

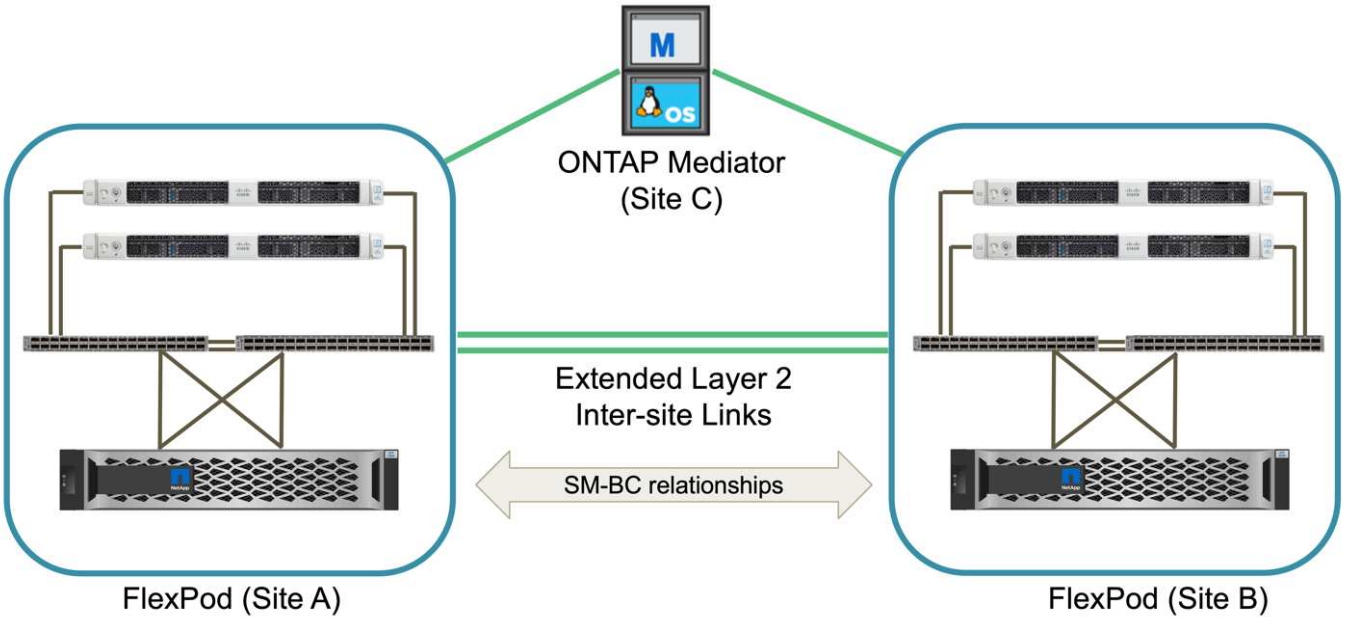


Família de produtos	Especificações técnicas
Série AFF	"Documentação da série AFF"
Série ASA	"Documentação da série ASA"

Consulte "Compartimentos de disco NetApp e documentação de Mídia de storage" a e "NetApp Hardware Universe" para obter detalhes sobre as gavetas de disco e os compartimentos de disco com suporte para cada modelo de controladora de storage.

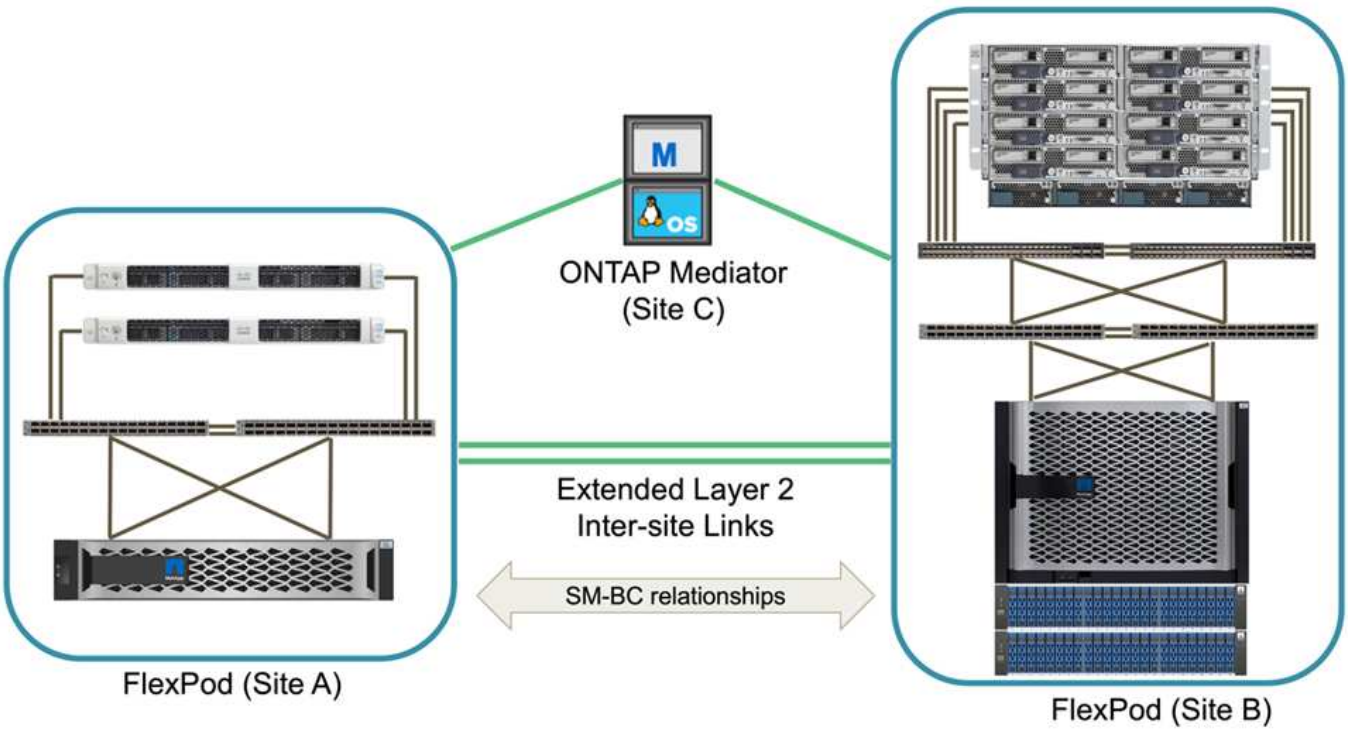
Topologias de soluções

As soluções da FlexPod são flexíveis em topologia e podem ser ampliadas ou ampliadas para atender a diferentes requisitos de solução. Uma solução que requer proteção da continuidade dos negócios e apenas recursos mínimos de computação e storage pode usar uma topologia de solução simples, conforme ilustrado na figura a seguir. Essa topologia simples usa os servidores em rack UCS C-Series e as controladoras AFF/ASA com SSDs na controladora sem compartimentos de disco adicionais.



Os componentes redundantes de computação, rede e armazenamento são interconetados com conetividade redundante entre os componentes. Esse design altamente disponível oferece resiliência da solução e permite que a TI resista a cenários de ponto único de falha. O design de vários locais e as relações de replicação de dados síncrona ONTAP SM-BC fornecem serviços de dados essenciais aos negócios, apesar do potencial de falha de storage em um único local.

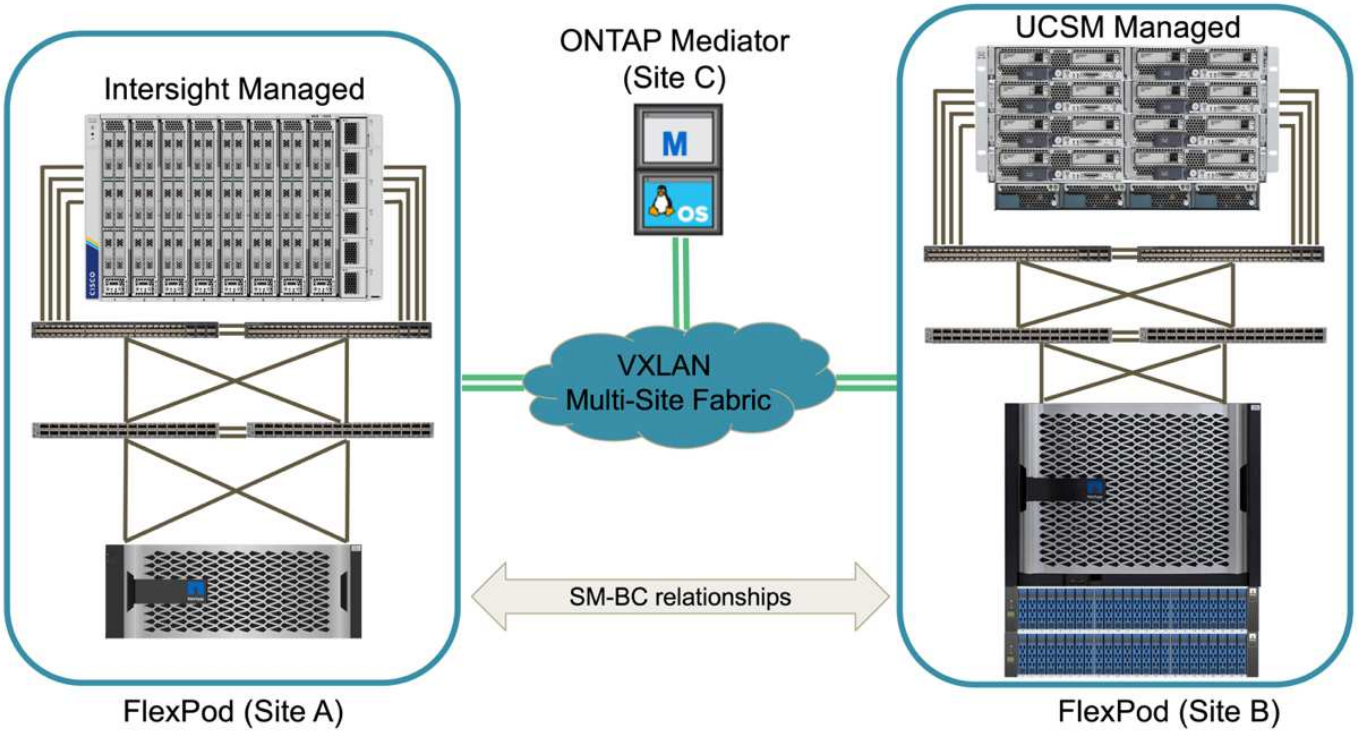
Uma topologia de implantação assimétrica que pode ser usada por empresas entre um data center e uma filial em uma área metropolitana pode parecer com a figura a seguir. Para esse design assimétrico, o data center precisa de um FlexPod de alta performance com mais recursos de computação e storage. No entanto, o requisito da filial é menor e pode ser atendido por um FlexPod muito menor.



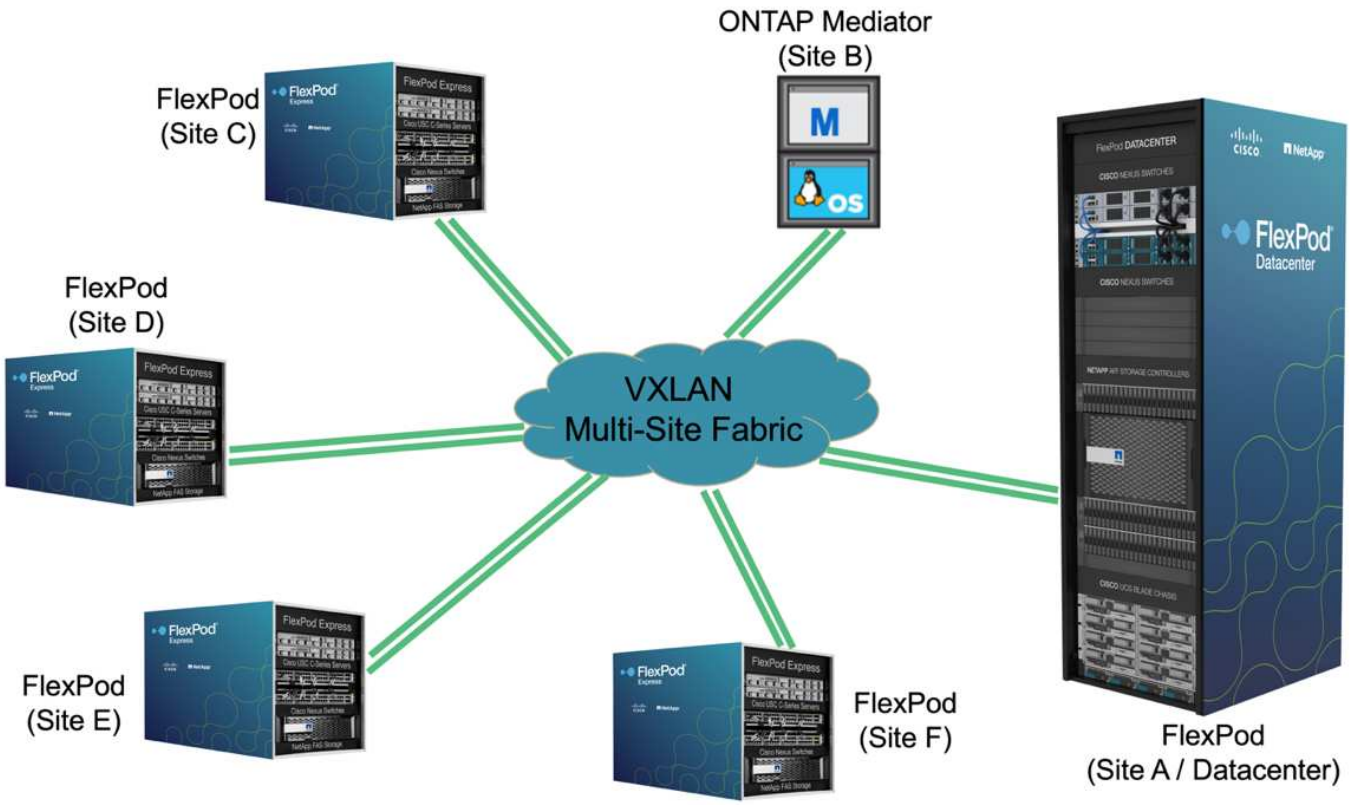
Para empresas com maiores requisitos de recursos de computação e armazenamento e vários locais, uma

malha de vários locais baseada em VXLAN permite que vários locais tenham uma malha de rede perfeita para facilitar a mobilidade de aplicativos para que um aplicativo possa ser servido de qualquer local.

Pode haver uma solução FlexPod existente usando o chassi do Cisco UCS 5108 e os servidores blade da série B que devem ser protegidos por uma nova instância do FlexPod. A nova instância do FlexPod pode usar o mais recente chassi do UCS X9508 com X210c nós de computação gerenciados pelo Cisco Intersight, conforme mostrado na figura a seguir. Nesse caso, os sistemas FlexPod em cada local são conectados a uma malha de data center maior e os locais são conectados por meio de uma rede de interconexão para formar uma malha de vários locais VXLAN.



Para empresas que têm um data center e várias filiais em uma área metropolitana que precisam ser protegidas para fornecer continuidade de negócios, a topologia de implantação do FlexPod SM-BC mostrada na figura a seguir pode ser implementada para proteger aplicativos e serviços de dados críticos para alcançar objetivos de RPO zero e rto quase zero para todos os locais.



Para esse modelo de implantação, cada filial estabelece as relações SM-BC e os grupos de consistência necessários com o data center. Você deve levar em conta os limites de objetos SM-BC suportados, para que as relações de grupo de consistência geral e as contagens de endpoints não excedam os máximos suportados no data center.

"Próximo: Visão geral da validação da solução."

Validação da solução

Validação da solução - Visão geral

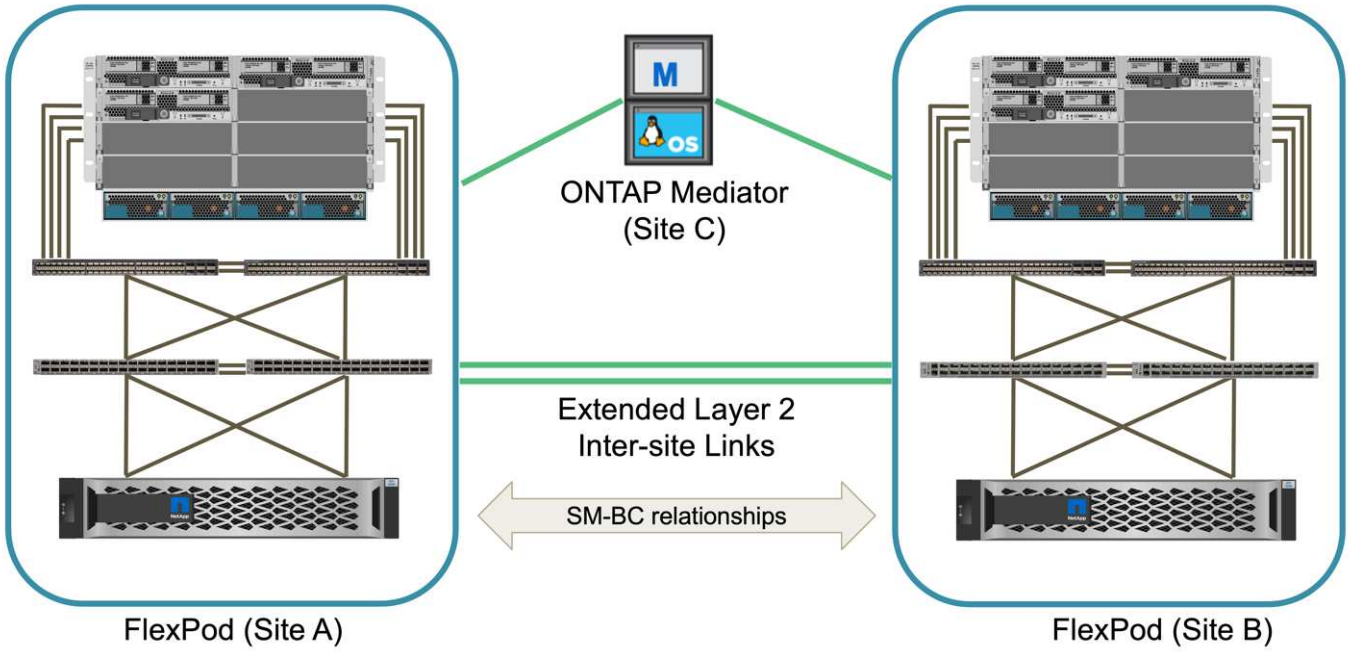
"Anterior: Solução FlexPod SM-BC."

Os detalhes de projeto e implementação da solução FlexPod SM-BC dependem da configuração e dos objetivos específicos da solução da FlexPod. Após a definição dos requisitos gerais de continuidade dos negócios, a solução FlexPod SM-BC pode ser criada implementando uma solução completamente nova com dois novos sistemas FlexPod, adicionando um novo FlexPod em outro local para emparelhar com um FlexPod existente ou emparelhando dois sistemas FlexPod existentes.

Como as soluções FlexPod são de natureza flexível em suas configurações, todas as configurações e componentes FlexPod compatíveis podem ser usados. O restante desta seção fornece informações sobre as validações de implementação executadas para uma solução de infraestrutura virtual baseada em VMware. Exceto para os aspetos relacionados ao SM-BC, a implementação segue os processos de implantação padrão do FlexPod. Consulte os CVDs e NVAs FlexPod disponíveis apropriados para suas configurações específicas para obter detalhes gerais de implementação do FlexPod.

Topologia de validação

Para validação da solução FlexPod SM-BC, são usados componentes de tecnologia compatíveis da NetApp, Cisco e VMware. A solução conta com pares de HA do NetApp AFF A250 executando o ONTAP 9.10,1, switches duplos Cisco Nexus 9336C-FX2 no local A e switches duplos Cisco Nexus 3232C no local B, Cisco UCS 6454 FIs em ambos os locais e três servidores Cisco UCS B200 M5 em cada local que executa o VMware vSphere 7.0u2 e gerenciados pelo UCS Manager e pelo VMware vCenter Server. A figura a seguir mostra a topologia de validação da solução em nível de componente com dois sistemas FlexPod executados no local A e no local B conetados por links intersites estendidos da camada 2 e Mediador ONTAP em execução no local C.



Hardware e software

A tabela a seguir lista o hardware e o software usados para a validação da solução. É importante observar que o Cisco, o NetApp e a VMware têm matrizes de interoperabilidade usadas para determinar o suporte para qualquer implementação específica do FlexPod:

- "http://support.netapp.com/matrix/"
- "Ferramenta de interoperabilidade de hardware e software Cisco UCS"
- "http://www.vmware.com/resources/compatibility/search.php"

Categoria	Componente	Versão do software	Quantidade
Computação	Interconexão de malha Cisco UCS 6454	4,2 mm (1f mm)	4 (2 por local)
	Servidores Cisco UCS B200 M5	4,2 mm (1f mm)	6 (3 por local)
	Cisco UCS IOM 2204XP	4,2 mm (1f mm)	4 (2 por local)
	Cisco VIC 1440 (PID: UCSB-MLOM-40G-04)	5,2 mm (1a mm)	2 (1 por local)

Categoria	Componente	Versão do software	Quantidade
	Cisco VIC 1340 (PID: UCSB-MLOM-40G-03)	4,5 mm (1a mm)	4 (2 por local)
Rede	Cisco Nexus 9336C-FX2	9,3 mm (6 mm)	2 (local A)
	Cisco Nexus 3232C	9,3 mm (6 mm)	2 (local B)
Armazenamento	NetApp AFF A250	9.10.1	4 (2 por local)
	Gerente do sistema da NetApp	9.10.1	2 (1 por local)
	NetApp Active IQ Unified Manager	9,10	1
	Ferramentas do NetApp ONTAP para VMware vSphere	9,10	1
	Plug-in do NetApp SnapCenter para VMware vSphere	4,6	1
	NetApp ONTAP Mediador	1,3	1
	NAbox	3.0.2	1
	Colheita de NetApp	21,11.1-1	1
Virtualização	VMware ESXi	7.0U2	6 (3 por local)
	Driver Ethernet nenic do VMware ESXi	1.0.35.0	6 (3 por local)
	VMware vCenter	7.0U2	1
	Plug-in NFS do NetApp para VMware VAAI	2,0	6 (3 por local)
Teste	Microsoft Windows	2022	1
	Microsoft SQL Server	2019	1
	Microsoft SQL Server Management Studio	18,10	1
	HammerDB	4,3	1
	Microsoft Windows	10	6 (3 por local)
	Iómetro	1.1.0	6 (3 por local)

"Próximo: Validação da solução - Compute."

Validação da solução - Compute

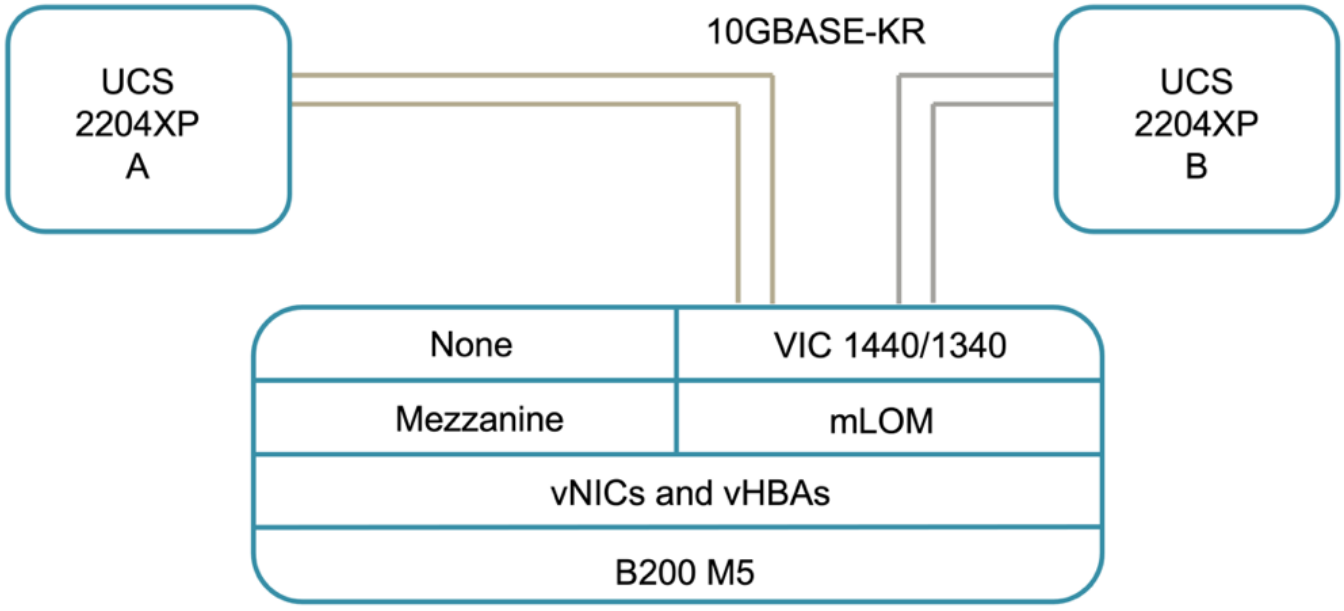
"Preívous: Validação da solução - Visão geral."

A configuração de computação da solução FlexPod SM-BC segue as práticas recomendadas típicas de soluções FlexPod. As seções a seguir destacam algumas das

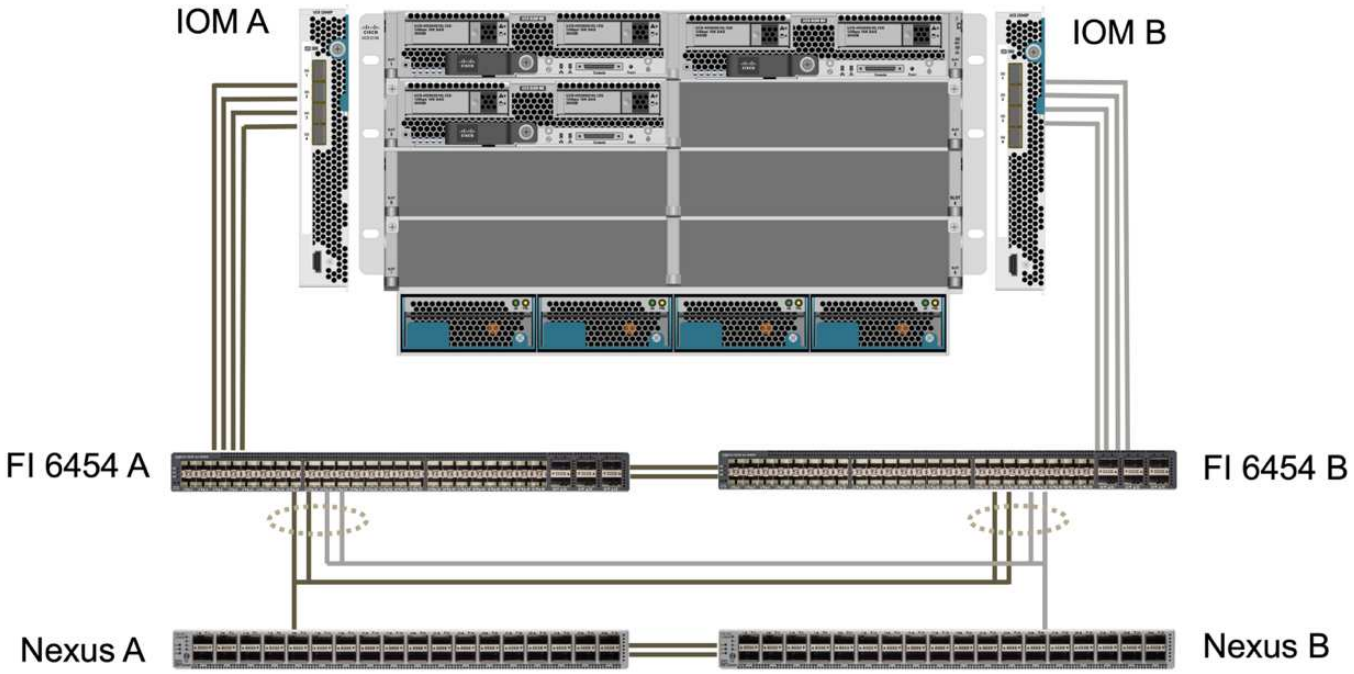
configurações e conetividade usadas para a validação. Algumas das considerações relacionadas ao SM-BC também são destacadas para fornecer referências e orientações de implementação.

Conetividade

A conetividade entre os servidores blade UCS B200 e os IOMs é fornecida pela placa UCS VIC através das conexões do backplane do chassi UCS 5108. Os extensores de malha UCS 2204XP usados para a validação têm dezesseis portas 10G cada para se conetar aos oito servidores blade de meia largura, por exemplo, duas para cada servidor. Para aumentar a largura de banda da conetividade do servidor, um VIC adicional baseado no mezanino pode ser adicionado para conetar o servidor à alternativa UCS 2408 IOM, que fornece quatro conexões 10G para cada servidor.



A conetividade entre o chassi do UCS 5108 e as FIs do UCS 6454 usadas para a validação é fornecida pela IOM 2204XP que usa quatro conexões 10G. As PORTAS FI 1 a 4 são configuradas como portas de servidor para essas conexões. As portas FI 25 a 28 são configuradas como portas uplink de rede para o switch Nexus A e B no local. A figura e a tabela a seguir fornecem o diagrama de conetividade e os detalhes de conexão de porta para que as unidades UCS 6454 se conetem ao chassi UCS 5108 e aos switches Nexus.



Dispositivo local	Porta local	Dispositivo remoto	Porta remota
UCS 6454 FI A	1	IOM A.	1
	2		2
	3		3
	4		4
	25	Nexus A.	1/13/1
	26		1/13/2
	27	Nexus B	1/13/3
	28		1/13/4
	L1	UCS 6454 FI B	L1
	L2		L2
UCS 6454 FI B	1	IOM B	1
	2		2
	3		3
	4		4
	25	Nexus A.	1/13/3
	26		1/13/4
	27	Nexus B	1/13/1
	28		1/13/2
	L1	UCS 6454 FI A	L1

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
	L2		L2

As conexões acima são semelhantes para ambos os sites A e B, apesar do site A usar o Nexus 9336C-FX2switches e o site B usando switches Nexus 3232C. Os cabos de arranque 40g a 4x10G são utilizados para as ligações Nexus to FI. As conexões FI ao Nexus utilizam canal de porta e os canais de porta virtual são configurados nos switches Nexus para agregar as conexões a cada FI.

Ao usar uma combinação diferente de componentes de switch IOM, FI e Nexus, certifique-se de usar cabos apropriados e velocidade de porta para a combinação de ambiente.

Largura de banda adicional pode ser obtida usando componentes que suportam conexões de velocidade mais alta ou mais conexões. Redundância adicional pode ser obtida adicionando conexões adicionais com componentes que os suportam.

Perfis de serviço

Um chassi de servidor blade com interconexões de malha gerenciadas pelo UCS Manager (UCSM) ou Cisco Intersight pode abstrair os servidores usando perfis de serviço disponíveis no UCSM e perfis de servidor no Intersight. Essa validação usa UCSM e perfis de serviço para simplificar o gerenciamento do servidor. Com perfis de serviço, substituir ou atualizar um servidor pode ser feito simplesmente associando o perfil de serviço original com o novo hardware.

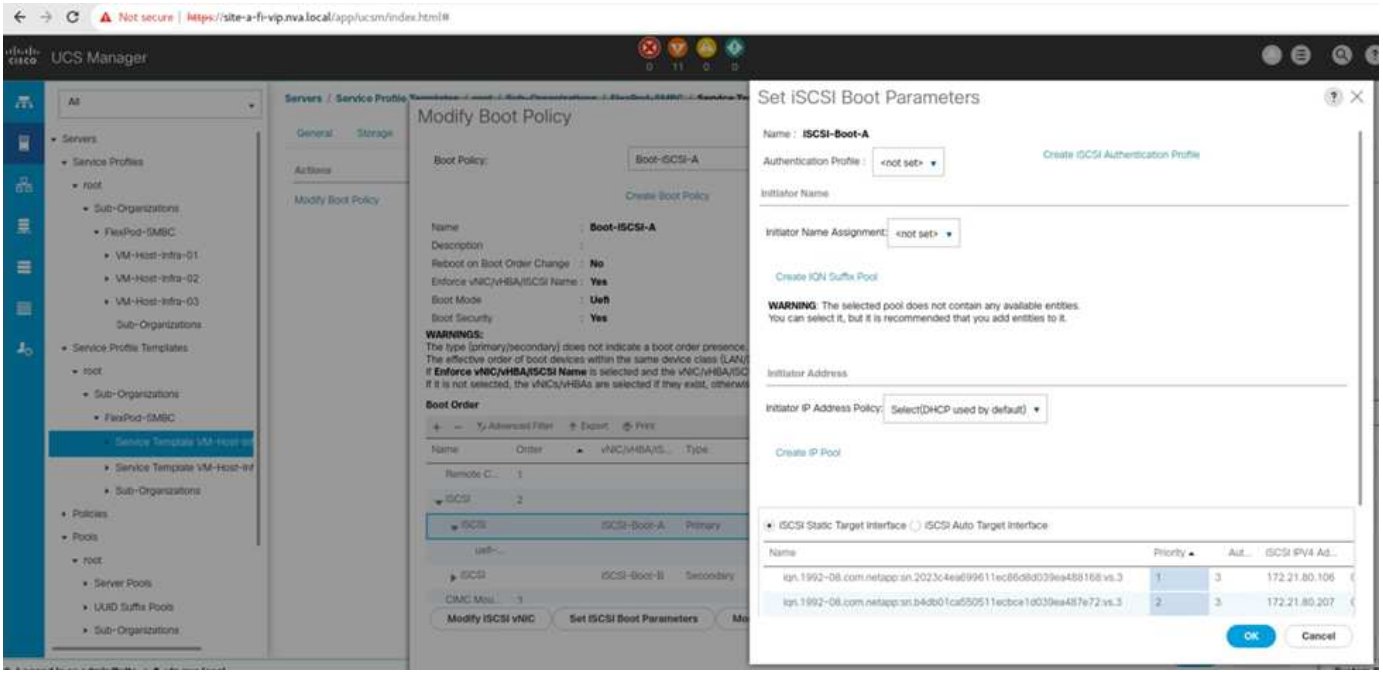
Os perfis de serviço criados suportam o seguinte para os hosts do VMware ESXi:

- ARRANQUE SAN a partir do armazenamento AFF A250 em qualquer local utilizando o protocolo iSCSI.
- Seis vNICs são criados para os servidores onde:
  - Dois vNICs redundantes (vSwitch0-A e vSwitch0-B) transportam tráfego de gerenciamento na banda. Opcionalmente, esses vNICs também podem ser usados por dados de protocolo NFS que não são protegidos pelo SM-BC.
  - Dois vNICs redundantes (vDS-A e vDS-B) são usados pelo comutador distribuído vSphere para transportar o VMware vMotion e outro tráfego de aplicativos.
  - ISCSI-A vNIC usado pelo iSCSI-A vSwitch para fornecer acesso ao caminho iSCSI-A.
  - ISCSI-B vNIC usado pelo vSwitch iSCSI-B para fornecer acesso ao caminho iSCSI-B.

Inicialização de SAN

Para a configuração de arranque SAN iSCSI, os parâmetros de arranque iSCSI são definidos para permitir o arranque iSCSI a partir de ambas as estruturas iSCSI. Para acomodar o cenário de failover SM-BC no qual um LUN de inicialização iSCSI SAN é servido a partir do cluster secundário quando o cluster primário não está disponível, a configuração de destino estático iSCSI deve incluir destinos do local A e do local B. além disso, para maximizar a disponibilidade de LUN de inicialização, configure as configurações de parâmetro de inicialização iSCSI para inicializar a partir de todos os controladores de armazenamento.

O destino estático iSCSI pode ser configurado na política de inicialização dos modelos de perfil de serviço sob a caixa de diálogo Definir parâmetro de inicialização iSCSI, conforme mostrado na figura a seguir. A configuração recomendada do parâmetro de inicialização iSCSI é mostrada na tabela a seguir, que implementa a estratégia de inicialização discutida acima para obter alta disponibilidade.



Malha iSCSI	Prioridade	Destino iSCSI	LIF iSCSI
ISCSI A	1	Local Um destino iSCSI	Site A Controller 1 Iscsi A LIF
	2	Local B destino iSCSI	Site B Controller 2 Iscsi A LIF
ISCSI B	1	Local B destino iSCSI	Local B controlador 1 iSCSI B LIF
	2	Local Um destino iSCSI	Local A controlador 2 iSCSI B LIF

"Próximo: Validação da solução - rede."

Validação da solução - rede

"Anterior: Validação da solução - Compute."

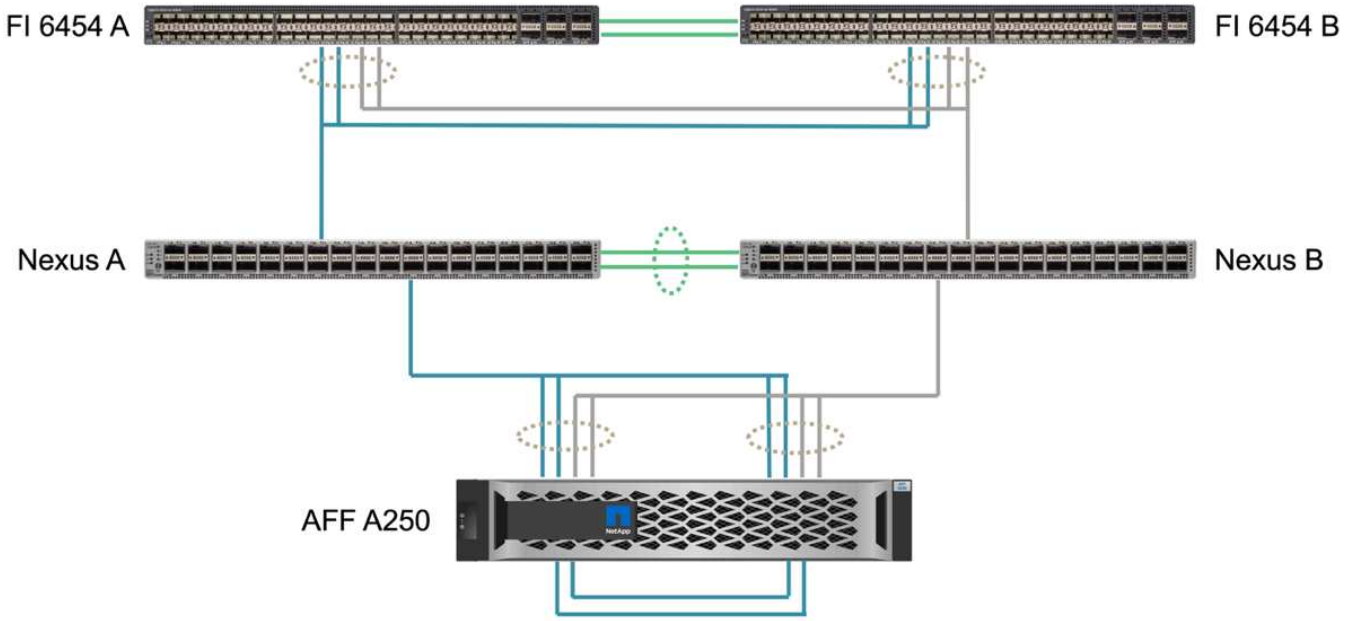
A configuração de rede para a solução FlexPod SM-BC segue as práticas recomendadas típicas da solução FlexPod em cada local. Para conetividade entre locais, a configuração de validação da solução coneta os switches FlexPod Nexus nos dois locais para fornecer conetividade entre locais que estende VLANs entre os dois locais. As seções a seguir destacam algumas das configurações e conetividade usadas para a validação.

Conetividade

Os switches FlexPod Nexus em cada local fornecem conectividade local entre a computação UCS e o storage ONTAP em uma configuração altamente disponível. Os componentes redundantes e a conetividade redundante fornecem resiliência em cenários de ponto único de falha.

O diagrama a seguir mostra a conetividade local do switch Nexus em cada local. Além do que é mostrado no diagrama, há também conexões de rede de console e gerenciamento para cada componente que não são

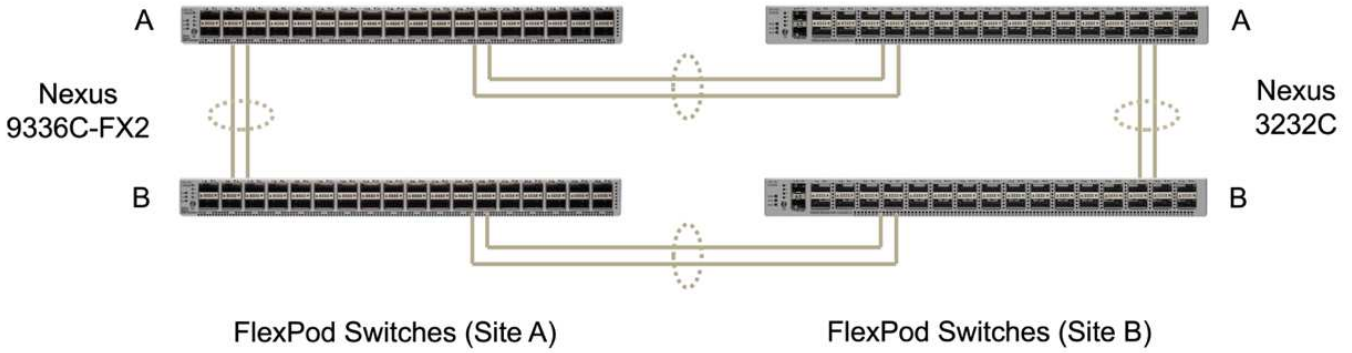
mostrados. Os cabos multiconexões de 40G a 4 x 10G são usados para conetar os switches Nexus às FIs UCS e aos controladores de armazenamento ONTAP AFF A250. Como alternativa, os cabos multiconexões 100g a 4 x 25G podem ser usados para aumentar a velocidade de comunicação entre os switches Nexus e os controladores de armazenamento AFF A250. Para simplificar, os dois controladores AFF A250 são mostrados logicamente como lado a lado para ilustração de cabeamento. As duas conexões entre os dois controladores de armazenamento permitem que o armazenamento forme um cluster sem switch.



A tabela a seguir mostra a conectividade entre switches Nexus e controladoras de storage AFF A250 em cada local.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Nexus A.	1/10/1	AFF A250 A.	e1a
	1/10/2		e1b
	1/10/3	AFF A250 B	e1a
	1/10/4		e1b
Nexus B	1/10/1	AFF A250 A.	e1c
	1/10/2		e1d
	1/10/3	AFF A250 B	e1c
	1/10/4		e1d

A conectividade entre os switches FlexPod no local A e o local B é mostrada na figura a seguir, com os detalhes do cabeamento listados na tabela a seguir. As conexões entre os dois switches em cada local são para os links de ponto de VPC. Por outro lado, as conexões entre os switches entre os sites fornecem os links entre os sites. Os links estendem as VLANs entre locais para comunicação entre clusters, replicação de dados SM-BC, gerenciamento na banda e acesso a dados para os recursos do local remoto.



Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Coloque Um interrutor A	33	Interrutor A do local B.	31
	34		32
	25	Interrutor B do local A	25
	26		26
Interrutor B do local A	33	Interrutor B do local B.	31
	34		32
	25	Coloque Um interrutor A	25
	26		26
Interrutor A do local B.	31	Coloque Um interrutor A	33
	32		34
	25	Interrutor B do local B.	25
	26		26
Interrutor B do local B.	31	Interrutor B do local A	33
	32		34
	25	Interrutor A do local B.	25
	26		26

A tabela acima lista a conetividade a partir das perspetivas de cada switch FlexPod. Como resultado, a tabela contém informações duplicadas para legibilidade.

Canal de porta e canal de porta virtual

O canal de porta permite a agregação de links usando o Link Aggregation Control Protocol (LACP) para agregação de largura de banda e resiliência de falha de link. O canal de porta virtual (VPC) permite que as conexões de canal de porta entre dois switches Nexus apareçam logicamente como um. Isso aumenta ainda mais a resiliência de falhas em cenários como uma falha de link único ou uma falha única de switch.

O tráfego do servidor UCS para armazenamento assume os caminhos da IOM A para FI A e IOM B para FI B antes de chegar aos switches Nexus. Como as CONEXÕES FI aos switches Nexus utilizam canal de porta no lado FI e canal de porta virtual no lado do switch Nexus, o servidor UCS pode efetivamente usar caminhos

através de ambos os switches Nexus e pode sobreviver a cenários de ponto único de falha. Entre os dois locais, os switches Nexus são interconetados como ilustrado na figura anterior. Há dois links cada um para conetar os pares de switches entre os sites e eles também usam uma configuração de canal de porta.

A conetividade do protocolo de storage de dados iSCSI/NFS, entre clusters e gerenciamento na banda é fornecida pela interconexão dos controladores de storage em cada local com os switches locais Nexus em uma configuração redundante. Cada controlador de storage é conetado a dois switches Nexus. As quatro conexões são configuradas como parte de um grupo de interfaces no storage para aumentar a resiliência. No lado do switch Nexus, essas portas também fazem parte de uma VPC entre os switches.

A tabela a seguir lista o ID do canal da porta e o uso em cada local.

ID do canal da porta	Utilização
10	Link local Nexus peer
15	Interconexão de malha A links
16	Links B de interconexão de malha
27	Links A do controlador de armazenamento
28	Ligações B do controlador de armazenamento
100	Alternar entre sites A links
200	Ligações B do interrutor inter-local

VLANs

A tabela a seguir lista as VLANs configuradas para configurar o ambiente de validação da solução FlexPod SM-BC juntamente com seu uso.

Nome	ID DA VLAN	Utilização
VLAN nativa	2	VLAN 2 usado como VLAN nativa em vez de VLAN padrão (1)
OOB-MGMT-VLAN	3333	VLAN de gerenciamento fora da banda para dispositivos
IB-MGMT-VLAN	3334	VLAN de gerenciamento na banda para hosts ESXi, gerenciamento de VM, etc.
NFS-VLAN	3335	VLAN NFS opcional para tráfego NFS
ISCSI-A-VLAN	3336	VLAN de malha iSCSI-A para tráfego iSCSI
ISCSI-B-VLAN	3337	VLAN de malha iSCSI-B para tráfego iSCSI
VMotion-VLAN	3338	VLAN de tráfego VMware vMotion
VM-tráfego-VLAN	3339	VLAN de tráfego VMware VM

Nome	ID DA VLAN	Utilização
VLAN entre clusters	3340	VLAN entre clusters para comunicações peer de cluster ONTAP

Embora o SM-BC não ofereça suporte a protocolos NFS ou CIFS para continuidade dos negócios, você ainda pode usá-los para workloads que não precisam ser protegidos para manter a continuidade dos negócios. Armazenamentos de dados NFS não foram criados para essa validação.

"Próximo: Validação da solução - armazenamento."

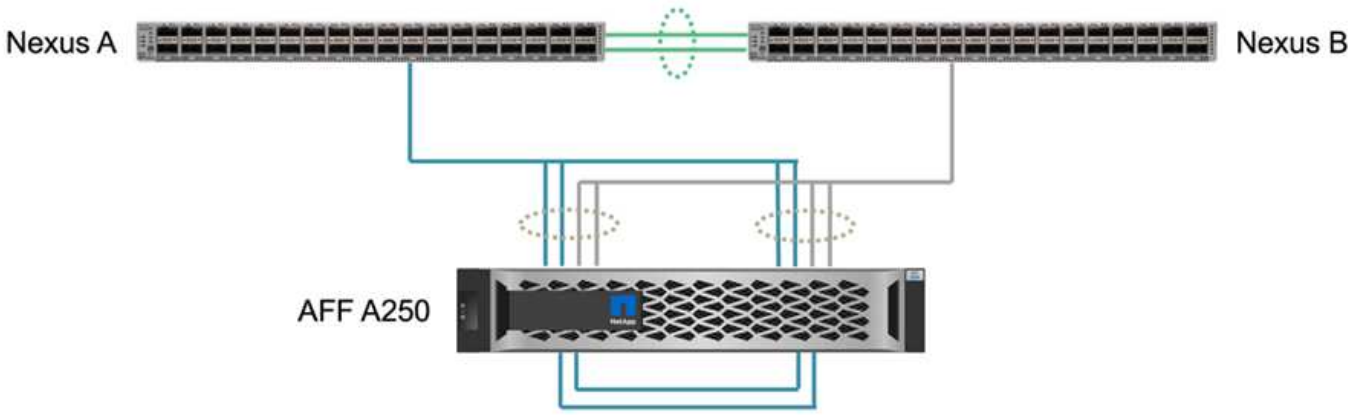
Validação da solução - armazenamento

"Anterior: Validação da solução - rede."

A configuração de storage da solução FlexPod SM-BC segue as práticas recomendadas típicas de soluções FlexPod em cada local. Para peering de cluster SM-BC e replicação de dados, eles usam os links entre locais estabelecidos entre os switches FlexPod em ambos os locais. As seções a seguir destacam algumas das configurações e conetividade usadas para a validação.

Conetividade

A conetividade de armazenamento para as FIs UCS locais e servidores blade é fornecida pelos switches Nexus no local. Por meio da conetividade do switch Nexus entre locais, o storage também pode ser acessado pelos servidores blade UCS remotos. A figura e a tabela a seguir mostram o diagrama de conectividade de storage e uma lista de conexões para os controladores de storage em cada local.



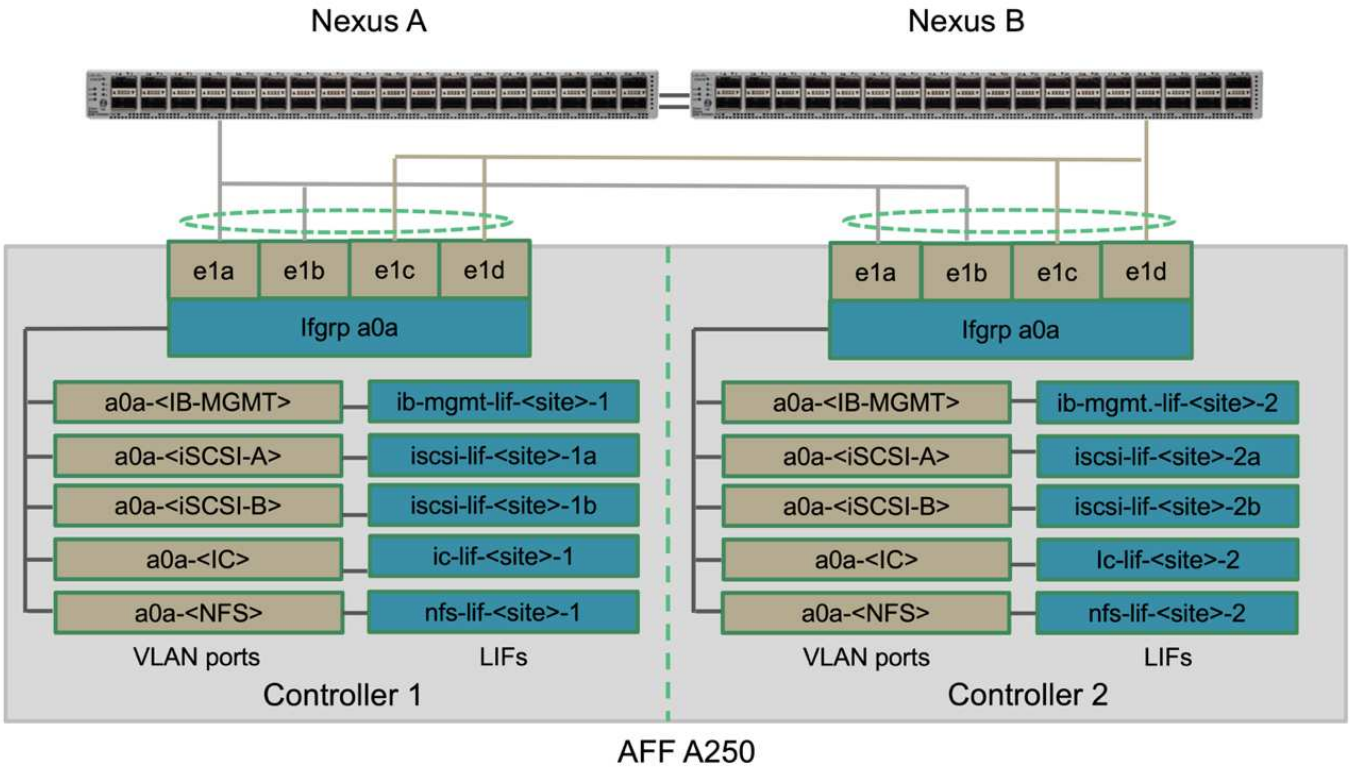
Dispositivo local	Porta local	Dispositivo remoto	Porta remota
AFF A250 A.	e0c	AFF A250 B	e0c
	e0d		e0d
	e1a	Nexus A.	1/10/1
	e1b		1/10/2

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
	e1c	Nexus B	1/10/1
	e1d		1/10/2
AFF A250 B	e0c	AFF A250 A.	e0c
	e0d		e0d
	e1a	Nexus A.	1/10/3
	e1b		1/10/4
	e1c	Nexus B	1/10/3
	e1d		1/10/4

Conexões e interfaces

Duas portas físicas em cada controlador de storage são conetadas a cada switch Nexus para agregação de largura de banda e redundância para essa validação. Essas quatro conexões participam de uma configuração de grupo de interfaces no storage. As portas correspondentes nos switches Nexus participam de uma VPC para agregação de links e resiliência.

Os protocolos de gerenciamento na banda, entre clusters e armazenamento de dados NFS/iSCSI usam VLANs. As portas VLAN são criadas no grupo de interfaces para segregar os diferentes tipos de tráfego. Interfaces lógicas (LIFs) para as respetivas funções são criadas em cima das portas VLAN correspondentes. A figura a seguir mostra a relação entre as conexões físicas, grupos de interfaces, portas VLAN e interfaces lógicas.

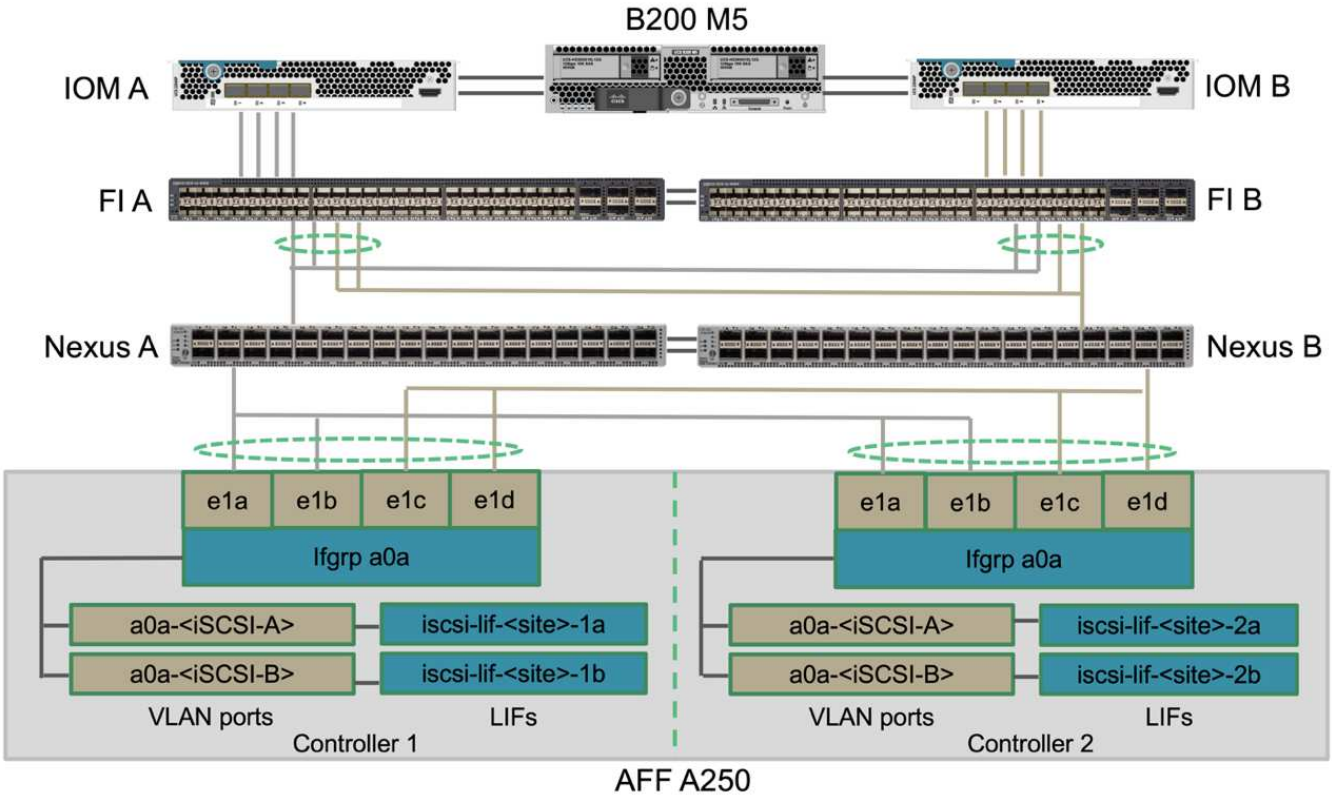


Inicialização de SAN

A NetApp recomenda a implementação de inicialização SAN para os servidores Cisco UCS na solução FlexPod. A implementação da inicialização SAN permite proteger o sistema operacional com segurança no sistema de storage NetApp, proporcionando melhor desempenho e flexibilidade. Para esta solução, a inicialização iSCSI SAN foi validada.

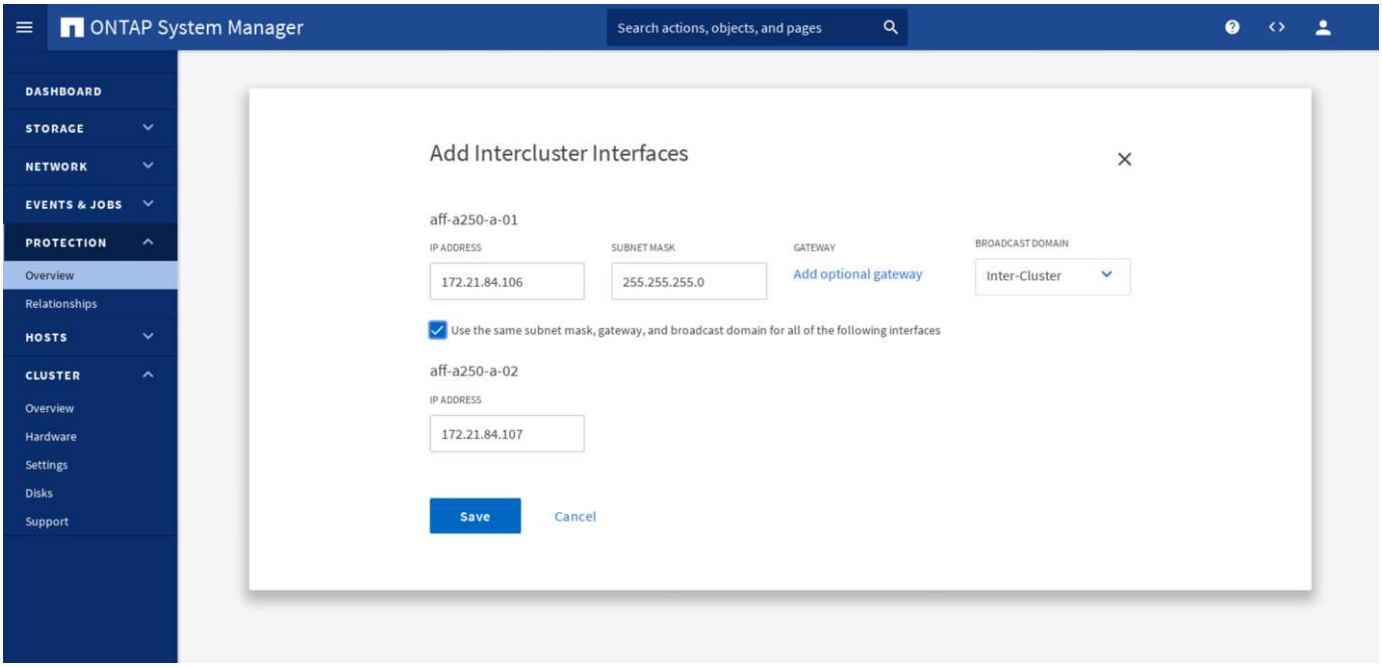
A figura a seguir mostra a conetividade para inicialização de SAN iSCSI do servidor Cisco UCS do armazenamento NetApp. Na inicialização de SAN iSCSI, cada servidor Cisco UCS recebe dois vNICs iSCSI (um para cada malha SAN) que fornecem conetividade redundante do servidor até o armazenamento. As portas de armazenamento Ethernet 10/25-G conetadas aos switches Nexus (neste exemplo, e1a, e1b, E1C e e1d) são agrupadas para formar um grupo de interfaces (ifgrp) (neste exemplo, a0a). As portas iSCSI VLAN são criadas no ifgrp e as iSCSI LIFs são criadas nas portas iSCSI VLAN.

Cada LUN de inicialização iSCSI é mapeado para o servidor que é inicializado através dos iSCSI LIFs associando o LUN de inicialização com os nomes qualificados iSCSI do servidor (IQNs) em seu grupo de inicialização. O igrop de inicialização do servidor contém dois IQNs, um para cada malha vNIC/SAN. Esse recurso permite que somente o servidor autorizado tenha acesso ao LUN de inicialização criado especificamente para esse servidor.



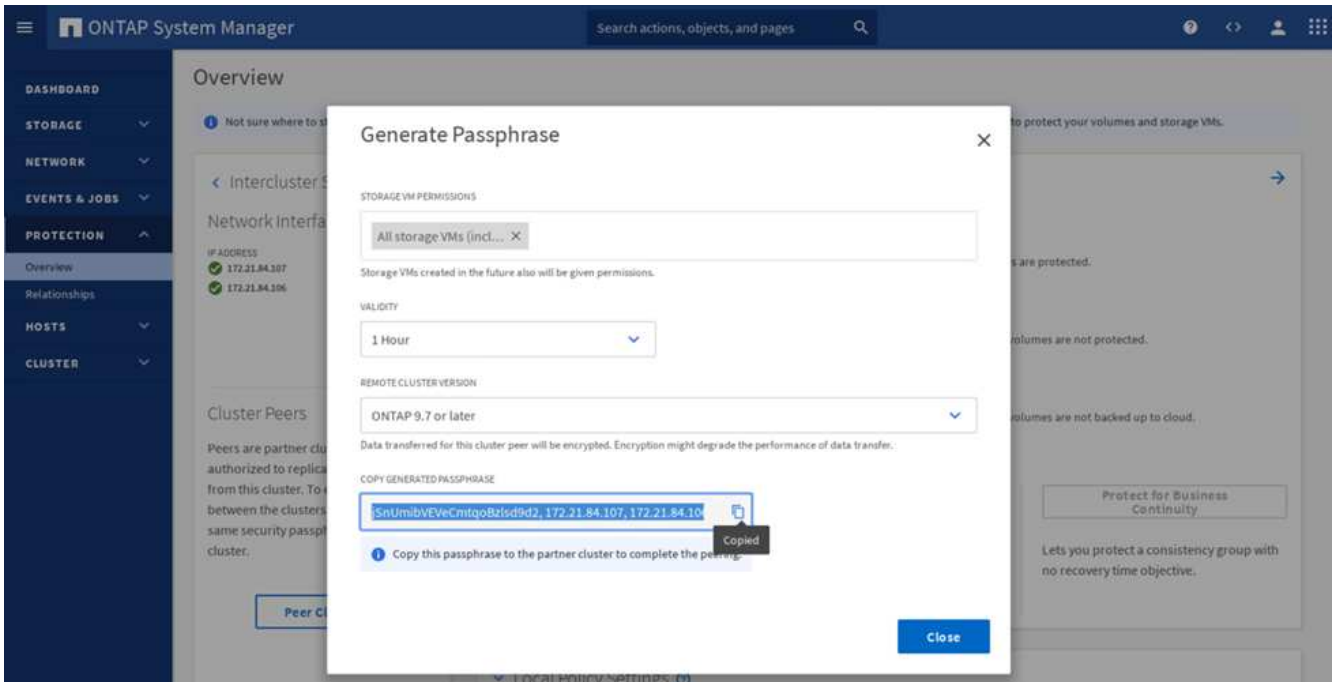
Peering de clusters

Os pares de cluster do ONTAP comunicam-se através dos LIFs entre clusters. Usando o Gerenciador de sistemas do ONTAP para os dois clusters, você pode criar as LIFs de clusters necessárias no painel proteção > Visão geral.

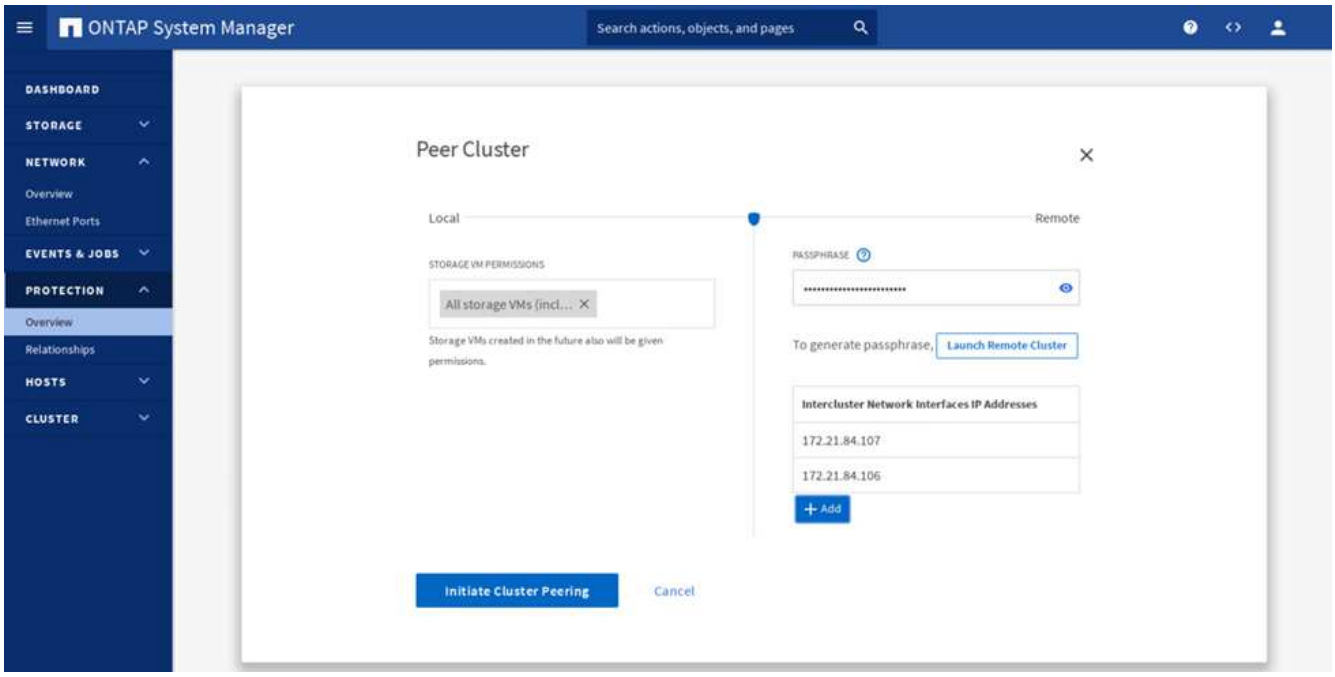


Para analisar os dois clusters juntos, execute as seguintes etapas:

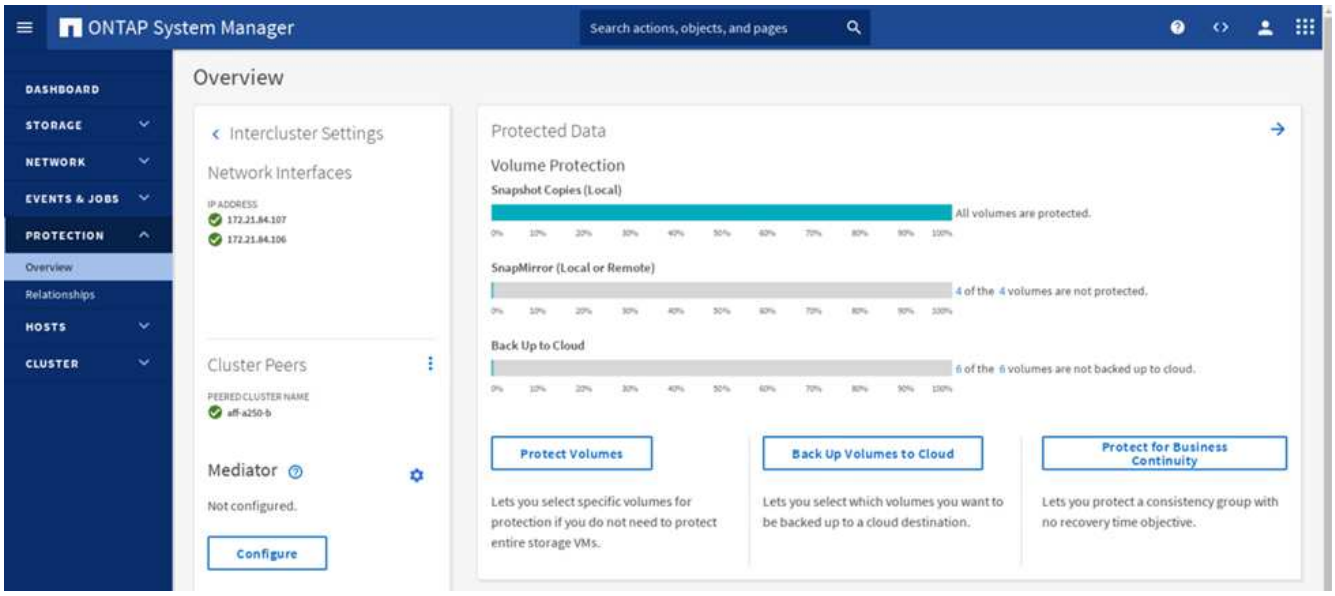
1. Gere a senha de peering de cluster no primeiro cluster.



2. Invoque a opção Peer Cluster no segundo cluster e forneça as informações de senha e LIF entre clusters.



3. O painel System Manager Protection > Overview (proteção do gestor do sistema > Visão geral) mostra as informações de pares do cluster.



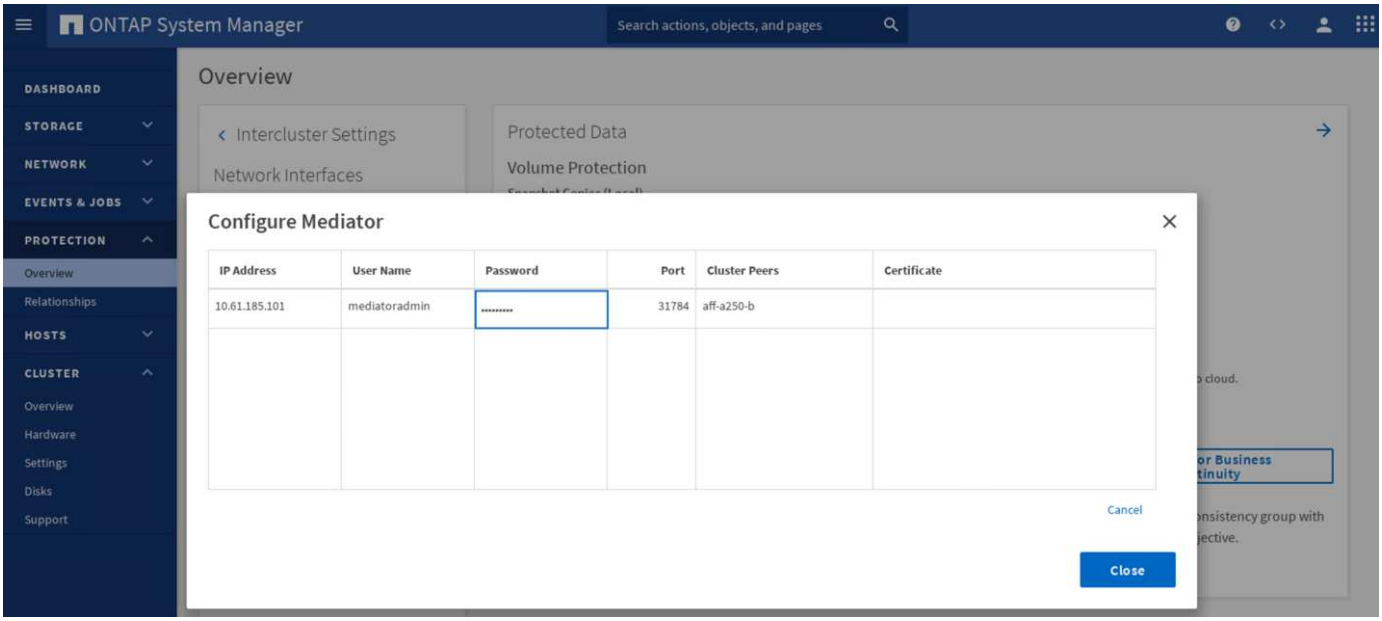
Instalação e configuração do Mediador ONTAP

O Mediador ONTAP estabelece um quórum para os clusters ONTAP em um relacionamento SM-BC. Ele coordena o failover automatizado quando uma falha é detetada e ajuda a evitar cenários de split-brain quando cada cluster tenta simultaneamente estabelecer o controle como o cluster primário.

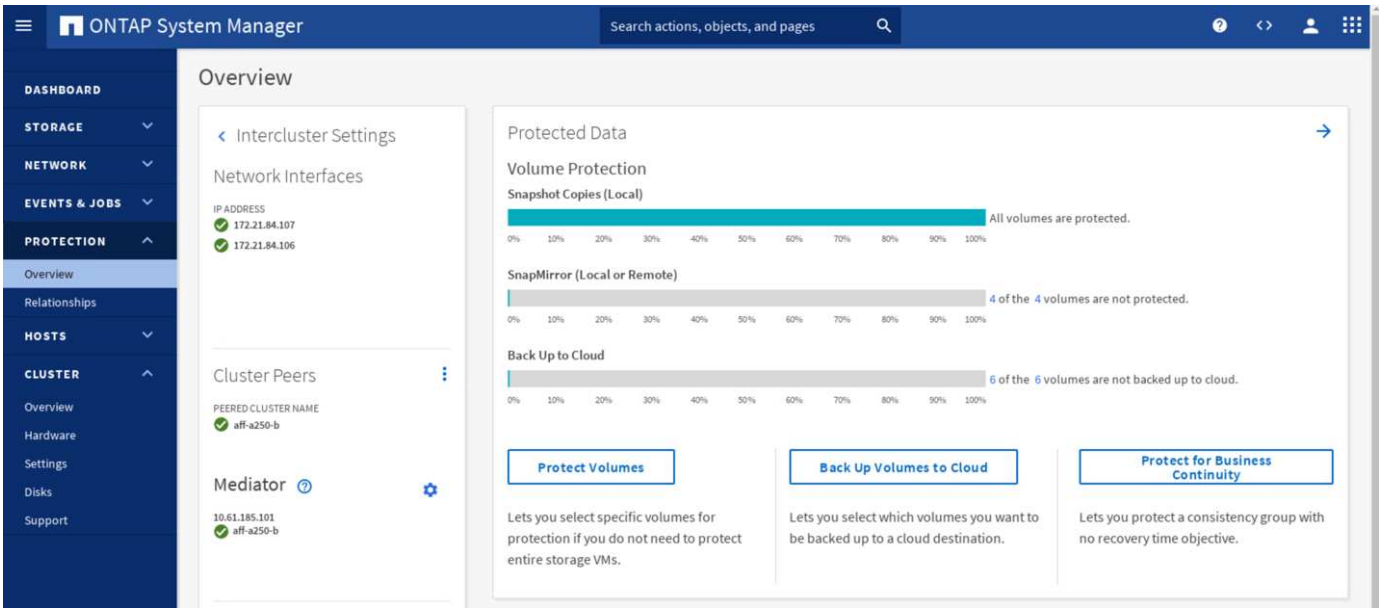
Antes de instalar o Mediador ONTAP, confira "Instale ou atualize o serviço do Mediador ONTAP" a página para pré-requisitos, versões Linux suportadas e os procedimentos para instalá-los nos vários sistemas operacionais Linux suportados.

Depois que o Mediador ONTAP for instalado, você poderá adicionar o certificado de segurança do Mediador ONTAP aos clusters do ONTAP e, em seguida, configurar o Mediador ONTAP no painel proteção do Gerenciador do sistema > Visão geral. A captura de tela a seguir mostra a GUI de configuração do ONTAP

Mediator.



Depois de fornecer as informações necessárias, o Mediador ONTAP configurado aparece no painel proteção do Gerenciador de sistema > Visão geral.



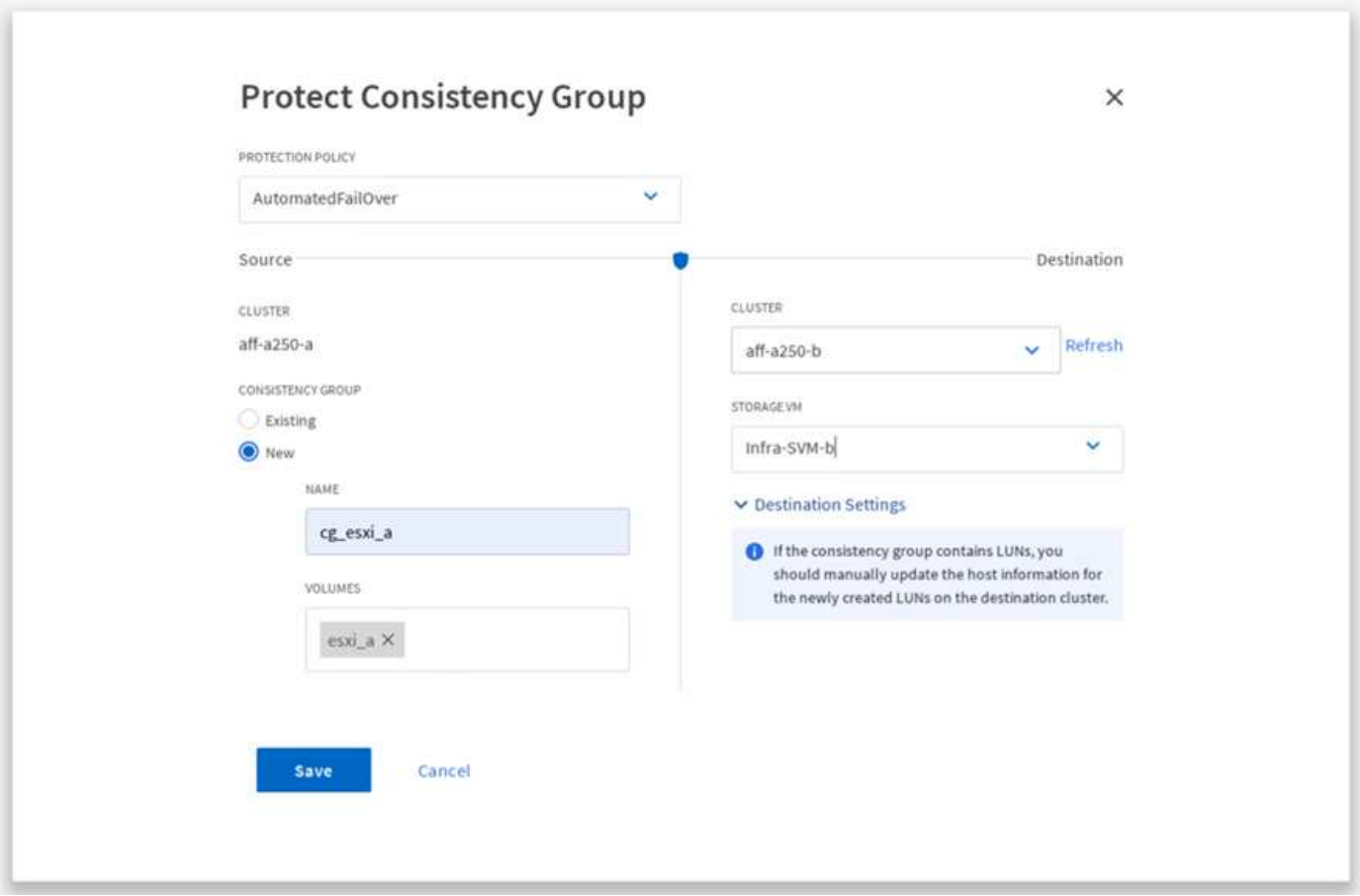
Grupo de consistência SM-BC

Um grupo de consistência fornece uma garantia de consistência de ordem de gravação para um workload de aplicações que abrange uma coleção de volumes especificados. Para o ONTAP 9.10,1, aqui estão algumas das restrições e limitações importantes.

- O número máximo de relações de grupo de consistência SM-BC em um cluster é 20.
- O número máximo de volumes suportados por relação SM-BC é 16.
- O número máximo de endpoints totais de origem e destino em um cluster é 200.

Para obter detalhes adicionais, consulte a documentação do ONTAP SM-BC no "restrições e limitações".

Para a configuração de validação, o Gerenciador de sistema do ONTAP foi usado para criar os grupos de consistência para proteger os LUNs de inicialização do ESXi e os LUNs de armazenamento de dados compartilhados para ambos os sites. A caixa de diálogo de criação do grupo de consistência é acessível acedendo a proteção > Visão geral > proteger para continuidade de negócios > proteger Grupo de consistência. Para criar um grupo de consistência, forneça os volumes de origem, o cluster de destino e as informações de máquina virtual de armazenamento de destino necessários para a criação.

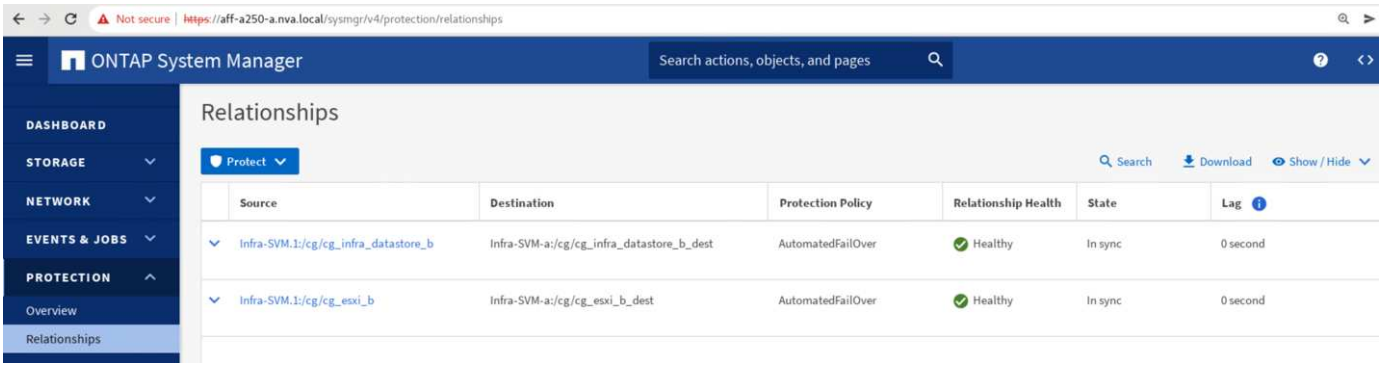


A tabela a seguir lista os quatro grupos de consistência que são criados e os volumes que são incluídos em cada grupo de consistência para o teste de validação.

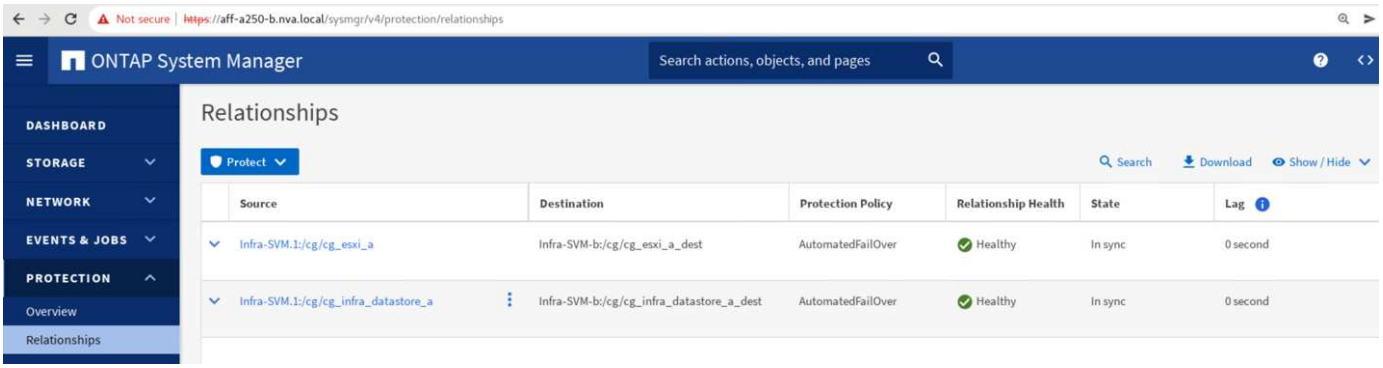
System Manager	Grupo de consistência	Volumes
Local A	cg_esxi_a	esxi_a
Local A	cg_infra_datastore_a	infra_datastore_a_01 infra_datastore_a_02
Local B	cg_esxi_b	esxi_b
Local B	cg_infra_datastore_b	infra_datastore_b_01 infra_datastore_b_02

Depois que os grupos de consistência são criados, eles aparecem sob as respetivas relações de proteção no local A e no local B.

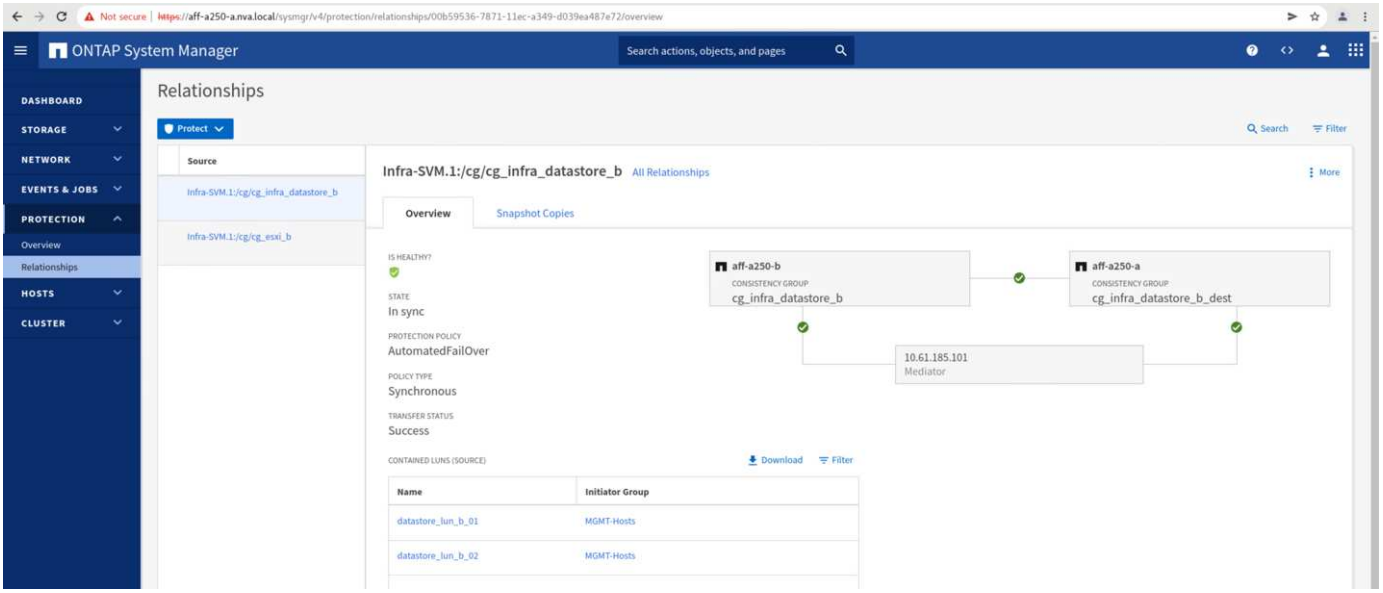
Esta captura de tela mostra as relações de grupo de consistência no site A..



Esta captura de tela mostra as relações de grupo de consistência no site B..



Esta captura de tela mostra os detalhes da relação do grupo de consistência para o grupo cg_infra_datastore_B.



Volumes, LUNs e mapeamentos de host

Depois que os grupos de consistência são criados, o SnapMirror sincroniza os volumes de origem e destino para que os dados possam estar sempre sincronizados. Os volumes de destino no local remoto carregam os nomes de volume com o final _dest. Por exemplo, para o volume esxi_a no Site Um cluster, há um volume de proteção de dados esxi_a_dest (DP) correspondente no site B.

Esta captura de tela mostra as informações de volume para o site A..

```
aff-a250-a::> vol show -vserver Infra-SVM-a
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-a esxi_a     aggr1_aff_a250_a_01 online RW     320GB    315.9GB    1%
Infra-SVM-a esxi_b_dest aggr1_aff_a250_a_02 online DP   3.86GB    638.4MB   83%
Infra-SVM-a infra_datastore_a_01 aggr1_aff_a250_a_01 online RW 1TB 717.6GB  29%
Infra-SVM-a infra_datastore_a_02 aggr1_aff_a250_a_02 online RW 1TB 828.4GB  19%
Infra-SVM-a infra_svm_root aggr1_aff_a250_a_01 online RW   1GB    966.5MB    0%
Infra-SVM-a infra_svm_root_m01 aggr1_aff_a250_a_01 online LS 1GB  966.6MB    0%
Infra-SVM-a infra_svm_root_m02 aggr1_aff_a250_a_02 online LS 1GB  966.6MB    0%
Infra-SVM-a vol_infra_datastore_b_01_dest aggr1_aff_a250_a_01 online DP 138.7GB 31.52GB  76%
Infra-SVM-a vol_infra_datastore_b_02_dest aggr1_aff_a250_a_01 online DP 49.37GB 9.03GB  80%
9 entries were displayed.
```

Esta captura de tela mostra as informações de volume para o site B.

```
aff-a250-b::> vol show -vserver Infra-SVM-b
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
Infra-SVM-b esxi_a_dest aggr1_aff_a250_b_02 online DP   4.10GB    768.2MB   80%
Infra-SVM-b esxi_b     aggr1_aff_a250_b_01 online RW     320GB    315.8GB    1%
Infra-SVM-b infra_datastore_b_01 aggr1_aff_a250_b_01 online RW 1TB 911.9GB  10%
Infra-SVM-b infra_datastore_b_02 aggr1_aff_a250_b_02 online RW 1TB 964.0GB   5%
Infra-SVM-b infra_svm_root aggr1_aff_a250_b_01 online RW   1GB    966.9MB    0%
Infra-SVM-b infra_svm_root_m01 aggr1_aff_a250_b_01 online LS 1GB  967.0MB    0%
Infra-SVM-b infra_svm_root_m02 aggr1_aff_a250_b_02 online LS 1GB  967.0MB    0%
Infra-SVM-b vol_infra_datastore_a_01_dest aggr1_aff_a250_b_02 online DP 270.0GB 27.39GB  89%
Infra-SVM-b vol_infra_datastore_a_02_dest aggr1_aff_a250_b_02 online DP 202.8GB 28.20GB  85%
9 entries were displayed.
```

Para facilitar o failover transparente de aplicações, os LUNs SM-BC espelhados também precisam ser mapeados para os hosts do cluster de destino. Isso permite que os hosts vejam caminhos adequados para as LUNs dos clusters de origem e destino. As `igroup show` saídas e `lun show` para ambos os sites A e B são capturadas nas duas capturas de tela A seguir. Com os mapeamentos criados, cada host ESXi no cluster vê seu próprio LUN de inicialização SAN como ID 0 e todos os quatro LUNs compartilhados do armazenamento de dados iSCSI.

Esta captura de tela mostra os grupos de host e o mapeamento LUN para o Site Um cluster.

```
aff-a250-a::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-a MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
Infra-SVM-a VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-a VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-a VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-a VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-a VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-a VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-a::> lun show -m
Vserver    Path                                        Igroup   LUN ID  Protocol
---------- ------------------------------------------  -------  ------  --------
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-01          VM-Host-Infra-a-01  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-02          VM-Host-Infra-a-02  0  iscsi
Infra-SVM-a /vol/esxi_a/VM-Host-Infra-a-03          VM-Host-Infra-a-03  0  iscsi
Infra-SVM-a /vol/esxi_a/swap_lun_a                  MGMT-Hosts   13  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-01     VM-Host-Infra-b-01  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-02     VM-Host-Infra-b-02  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/VM-Host-Infra-b-03     VM-Host-Infra-b-03  0  iscsi
Infra-SVM-a /vol/esxi_b_dest/swap_lun_b             MGMT-Hosts   23  iscsi
Infra-SVM-a /vol/infra_datastore_a_01/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-a /vol/infra_datastore_a_02/datastore_lun_a_02  MGMT-Hosts  12  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_01_dest/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-a /vol/vol_infra_datastore_b_02_dest/datastore_lun_b_02  MGMT-Hosts  22  iscsi
12 entries were displayed.
```

Esta captura de tela mostra os grupos de host e o mapeamento LUN para o cluster do site B.

```
aff-a250-b::> igroup show
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
Infra-SVM-b MGMT-Hosts iscsi    vmware   iqn.2010-11.com.flexpod:ucs-smbc-b:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-b:3
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:1
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:2
                                         iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-a-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:1
Infra-SVM-b VM-Host-Infra-a-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:2
Infra-SVM-b VM-Host-Infra-a-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-a:3
Infra-SVM-b VM-Host-Infra-b-01 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:1
Infra-SVM-b VM-Host-Infra-b-02 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:2
Infra-SVM-b VM-Host-Infra-b-03 iscsi vmware iqn.2010-11.com.flexpod:ucs-smbc-b:3
7 entries were displayed.

aff-a250-b::> lun show -m
Vserver    Path                                      Igroup   LUN ID  Protocol
---------- ----------------------------------------  -------  ------  --------
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-01      VM-Host-Infra-a-01  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-02      VM-Host-Infra-a-02  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/VM-Host-Infra-a-03      VM-Host-Infra-a-03  0  iscsi
Infra-SVM-b /vol/esxi_a_dest/swap_lun_a              MGMT-Hosts   13  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-01           VM-Host-Infra-b-01  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-02           VM-Host-Infra-b-02  0  iscsi
Infra-SVM-b /vol/esxi_b/VM-Host-Infra-b-03           VM-Host-Infra-b-03  0  iscsi
Infra-SVM-b /vol/esxi_b/swap_lun_b                   MGMT-Hosts   23  iscsi
Infra-SVM-b /vol/infra_datastore_b_01/datastore_lun_b_01  MGMT-Hosts  21  iscsi
Infra-SVM-b /vol/infra_datastore_b_02/datastore_lun_b_02  MGMT-Hosts  22  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_01_dest/datastore_lun_a_01  MGMT-Hosts  11  iscsi
Infra-SVM-b /vol/vol_infra_datastore_a_02_dest/datastore_lun_a_02  MGMT-Hosts  12  iscsi
12 entries were displayed.
```

"Próximo: Validação da solução - virtualização."

Validação da solução - virtualização

"Anterior: Validação da solução - armazenamento."

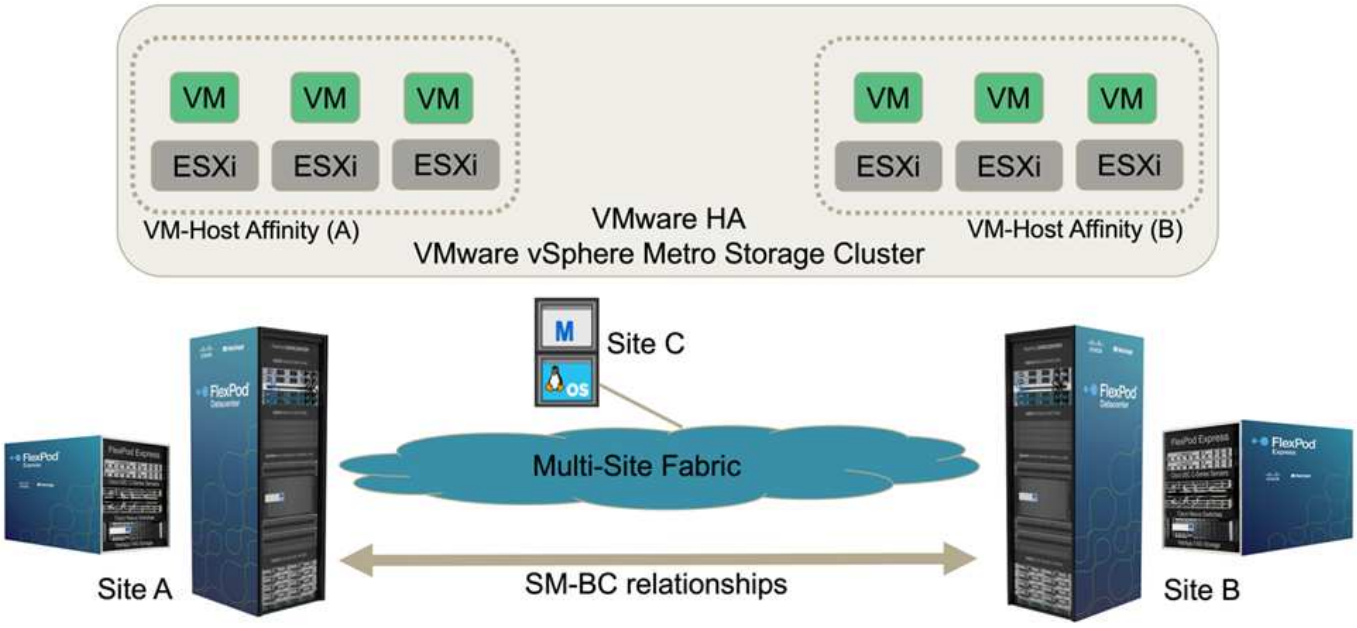
Na solução FlexPod SM-BC para vários locais, um único VMware vCenter gerencia os recursos de infraestrutura virtual para toda a solução. Os hosts de ambos os data centers participam do único cluster VMware HA que abrange ambos os data centers. Os hosts têm acesso à solução NetApp SM-BC, onde o storage com relações SM-BC definidas pode ser acessado de ambos os locais.

O storage da solução SM-BC está em conformidade com o modelo de acesso uniforme no recurso vMSC (VMware vSphere Metro Storage Cluster) para evitar desastres e tempo de inatividade. Para um desempenho ideal da máquina virtual, os discos da máquina virtual devem ser hospedados nos sistemas NetApp AFF A250 locais para minimizar a latência e o tráfego nos links WAN em operação normal.

Como parte da implementação do projeto, a distribuição das máquinas virtuais nos dois locais deve ser determinada. Você pode determinar a afinidade do site da máquina virtual e a distribuição de aplicativos entre os dois sites de acordo com as preferências do site e os requisitos do aplicativo. Os grupos VM/Host do cluster VMware e as regras VM/Host são usados para configurar afinidade VM/Host para garantir que as VMs estejam sendo executadas em hosts no local desejado.

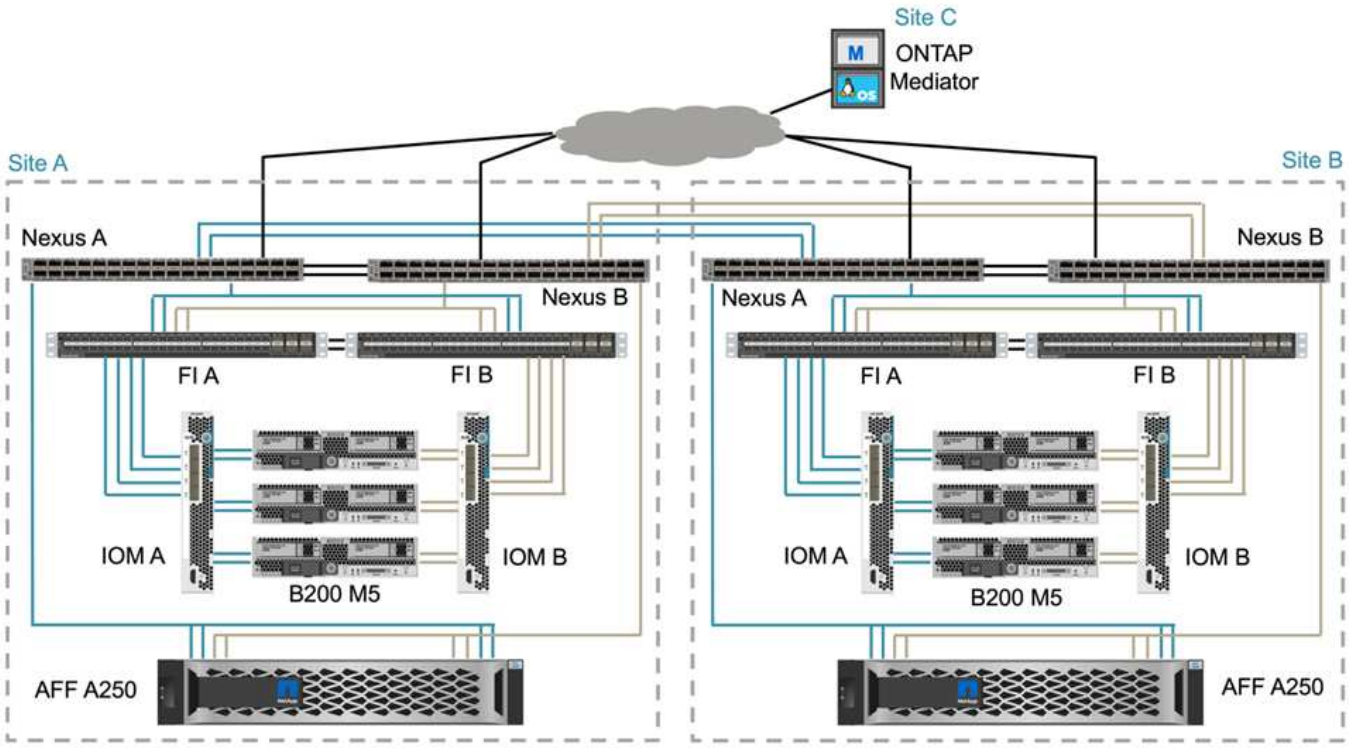
No entanto, as configurações que permitem que as VMs sejam executadas em ambos os locais garantirão que as VMs possam ser reiniciadas pelo VMware HA em hosts remotos para fornecer resiliência da solução. Para acomodar máquinas virtuais para serem executadas em ambos os locais, todos os armazenamentos de dados compartilhados iSCSI devem ser montados em todos os hosts ESXi para garantir uma operação suave do vMotion de máquinas virtuais entre locais.

A figura a seguir mostra uma visualização de virtualização de solução FlexPod SM-BC de alto nível, que inclui recursos VMware HA e vMSC para fornecer alta disponibilidade para serviços de computação e storage. A arquitetura da solução de data center ativo-ativo permite a mobilidade da carga de trabalho entre locais e fornece proteção de DR/BC.



Conetividade de rede de ponta a ponta

A solução FlexPod SM-BC inclui infraestruturas FlexPod em cada local, conectividade de rede entre locais e o mediador ONTAP implantado em um terceiro local para atender aos objetivos de RPO e rto necessários. A figura a seguir mostra a conetividade de rede de ponta a ponta entre os servidores Cisco UCS B200M5 em cada local e o armazenamento NetApp com recursos SM-BC em um local e em vários locais.



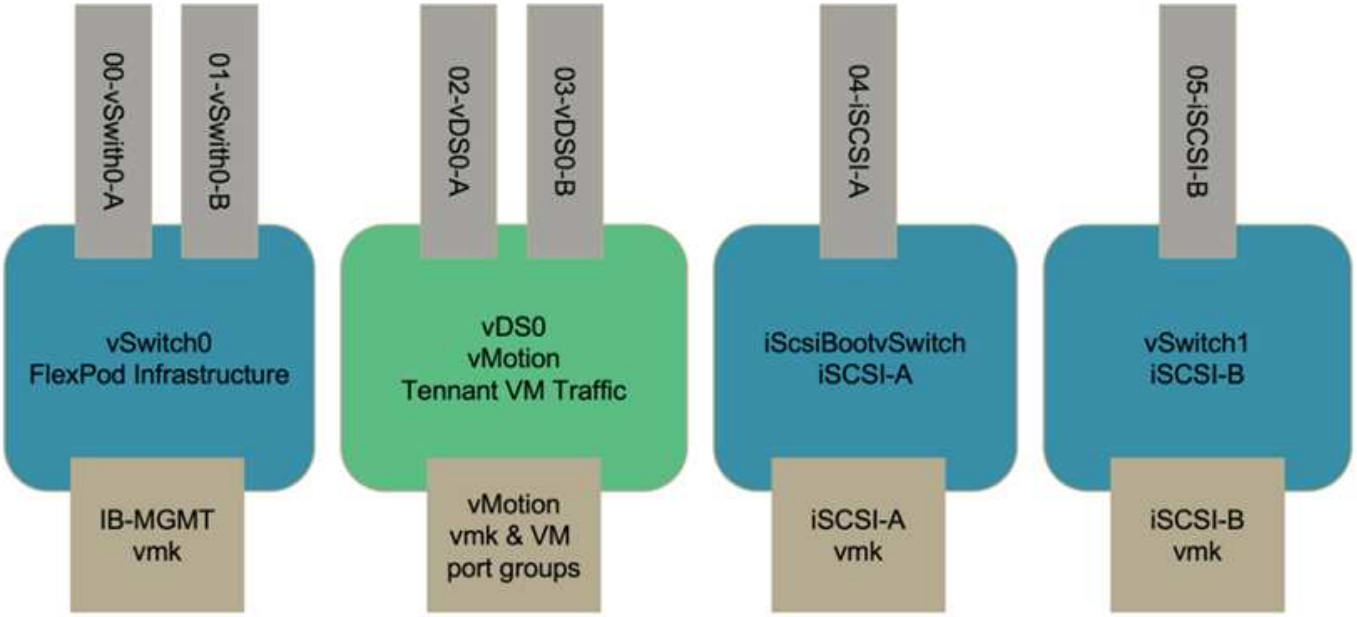
A arquitetura de implantação do FlexPod é idêntica em cada local para validação dessa solução. No entanto, a solução dá suporte a implantações assimétricas e também pode ser adicionada a soluções FlexPod existentes se elas atenderem aos requisitos.

A arquitetura de camada 2 estendida é usada para um Data Fabric otimizado em vários locais que fornece conectividade entre a computação Cisco UCS canalizada por porta e o storage NetApp em cada data center, bem como conectividade entre data centers. A configuração do canal de porta e a configuração do canal de porta virtual, quando apropriado, são usadas para agregação de largura de banda e tolerância a falhas entre as camadas de computação, rede e armazenamento, bem como para os links entre sites. Como resultado, os servidores blade UCS têm conetividade e acesso multipath ao storage NetApp local e remoto.

Rede virtual

Cada host no cluster é implantado usando redes virtuais idênticas, independentemente de sua localização. O design separa os diferentes tipos de tráfego usando os switches virtuais VMware (vSwitch) e os switches distribuídos virtuais VMware (vDS). O VMware vSwitch é usado principalmente para as redes de infraestrutura FlexPod e vDS para redes de aplicativos, mas não é necessário.

Os switches virtuais (vSwitch, vDS) são implantados com dois uplinks por switch virtual; os uplinks no nível do hypervisor ESXi são referidos como vmnics e NICs virtuais (vNICs) no software Cisco UCS. Os vNICs são criados no adaptador Cisco UCS VIC em cada servidor usando perfis de serviço Cisco UCS. São definidos seis vNICs, dois para vSwitch0, dois para vDS0, dois para vSwitch1 e dois para uplinks iSCSI, como mostrado na figura a seguir.



O vSwitch0 é definido durante a configuração do host VMware ESXi e contém a VLAN de gerenciamento da infraestrutura do FlexPod e as portas VMK (host ESXi) para gerenciamento. Um grupo de portas de máquinas virtuais de gerenciamento de infraestrutura também é colocado no vSwitch0 para qualquer máquina virtual de gerenciamento de infraestrutura crítica que seja necessária.

É importante colocar essas máquinas virtuais de infraestrutura de gerenciamento no vSwitch0 em vez do vDS, porque se a infraestrutura do FlexPod for desligada ou desligada e você tentar ativar essa máquina virtual de gerenciamento em um host diferente do host no qual estava sendo executado originalmente, ele inicializa bem na rede no vSwitch0. Esse processo é particularmente importante se o VMware vCenter for a máquina virtual de gerenciamento. Se o vCenter estivesse no vDS e fosse movido para outro host e então iniciasse, ele não seria conetado à rede após a inicialização.

Dois vSwitches de inicialização iSCSI são usados neste projeto. A inicialização iSCSI do Cisco UCS requer vNICs separados para inicialização iSCSI. Esses vNICs usam VLAN iSCSI da malha apropriada como VLAN nativa e são conetados ao vSwitch de inicialização iSCSI apropriado. Opcionalmente, você também pode implantar redes iSCSI no vDS implantando um novo vDS ou usando um existente.

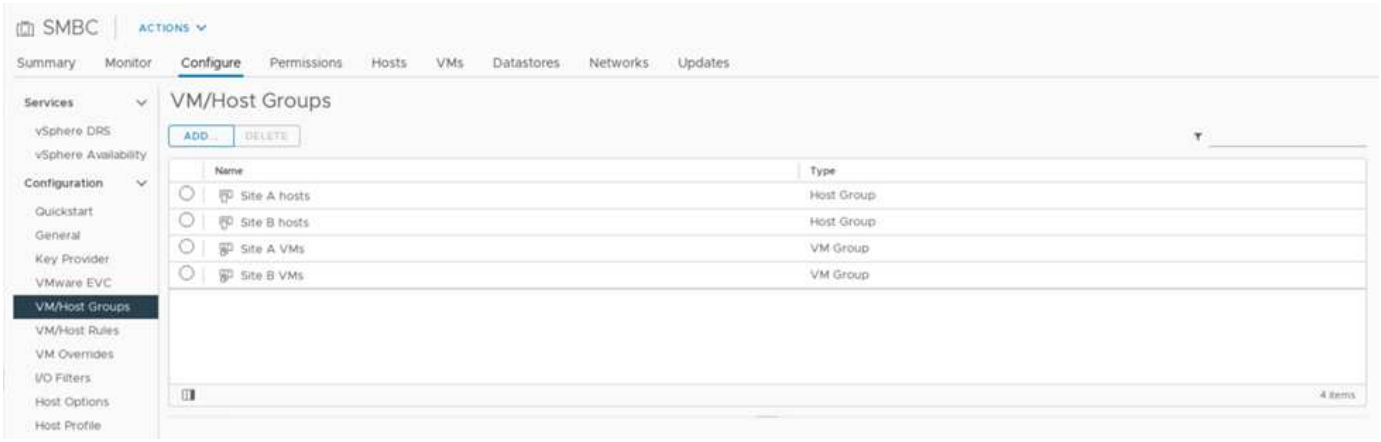
Grupos e regras de afinidade do VM-Host

Para permitir que as máquinas virtuais sejam executadas em qualquer host ESXi em ambos os sites SM-BC, todos os hosts ESXi devem montar os datastores iSCSI de ambos os sites. Se os armazenamentos de dados de ambos os sites forem corretamente montados por todos os hosts ESXi, você poderá migrar uma máquina virtual entre todos os hosts com vMotion e a VM ainda mantém acesso a todos os discos virtuais criados a partir desses datastores.

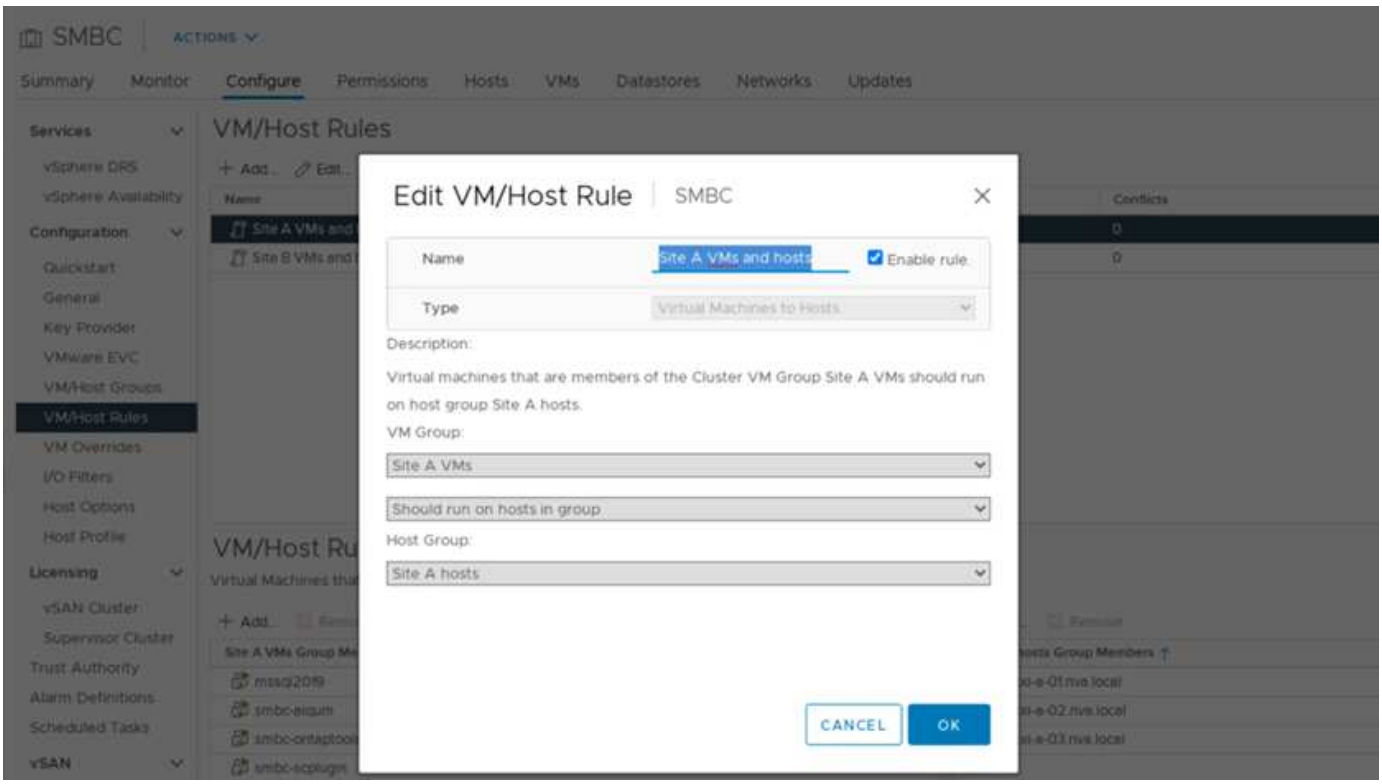
Para uma máquina virtual que usa datastores locais, seu acesso a discos virtuais se torna remoto se for migrado para um host no local remoto e, assim, aumentando a latência da operação de leitura devido à distância física entre os sites. Portanto, é uma prática recomendada manter as máquinas virtuais nos hosts locais e utilizar o armazenamento local no local.

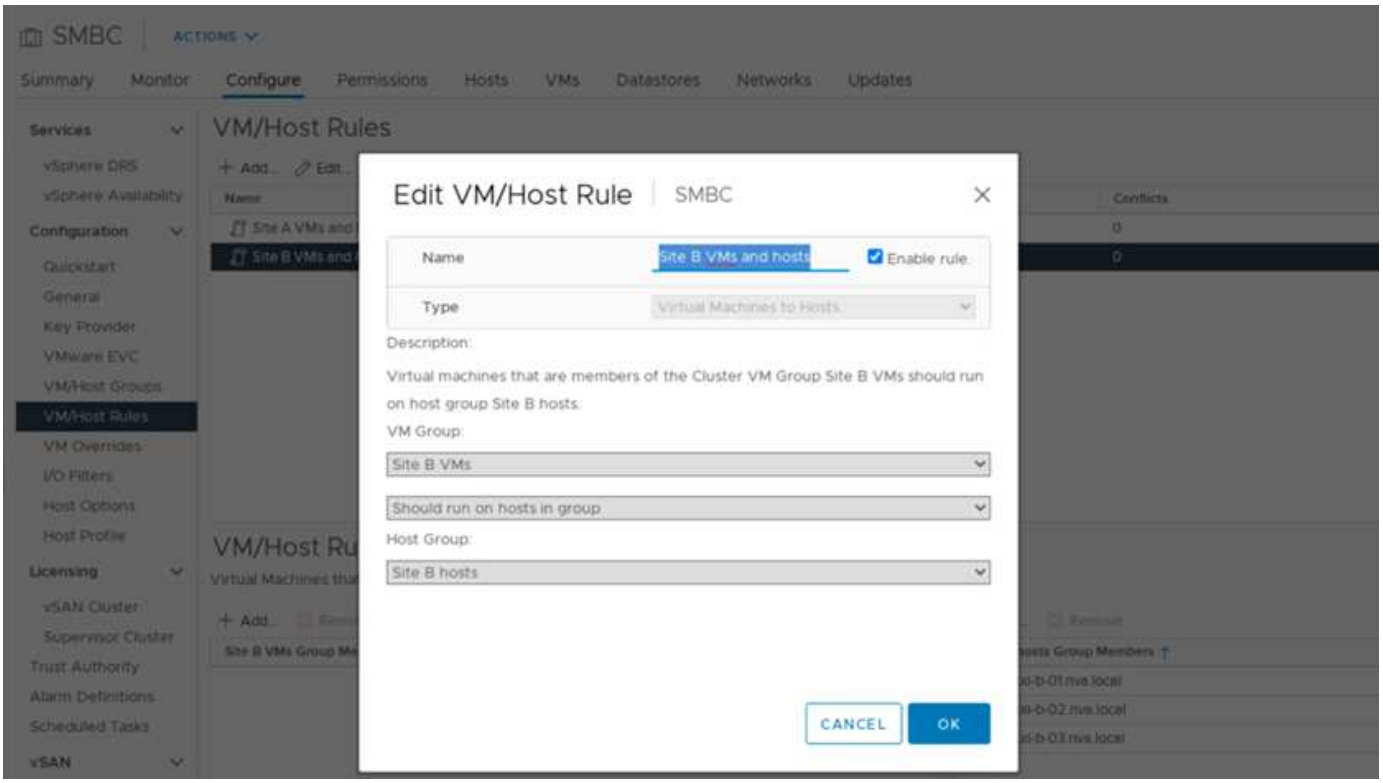
Usando um mecanismo de afinidade de VM/host, você pode usar grupos de VM/host para criar um grupo de VM e um grupo de hosts para máquinas virtuais e hosts localizados em um determinado site. Usando regras de VM/host, você pode especificar a política para as VMs e hosts a seguir. Para permitir a migração de máquina virtual em locais durante um cenário de manutenção ou desastre, use a especificação de política "deve ser executada em hosts em grupo" para essa flexibilidade.

A captura de tela a seguir mostra que dois grupos de hosts e dois grupos de VM são criados para hosts e VMs do local A e do local B.



Além disso, as duas figuras a seguir mostram as regras de VM/host criadas para as VMs do local A e do local B para serem executadas nos hosts em seus respetivos sites usando a política "deve ser executada em hosts no grupo".

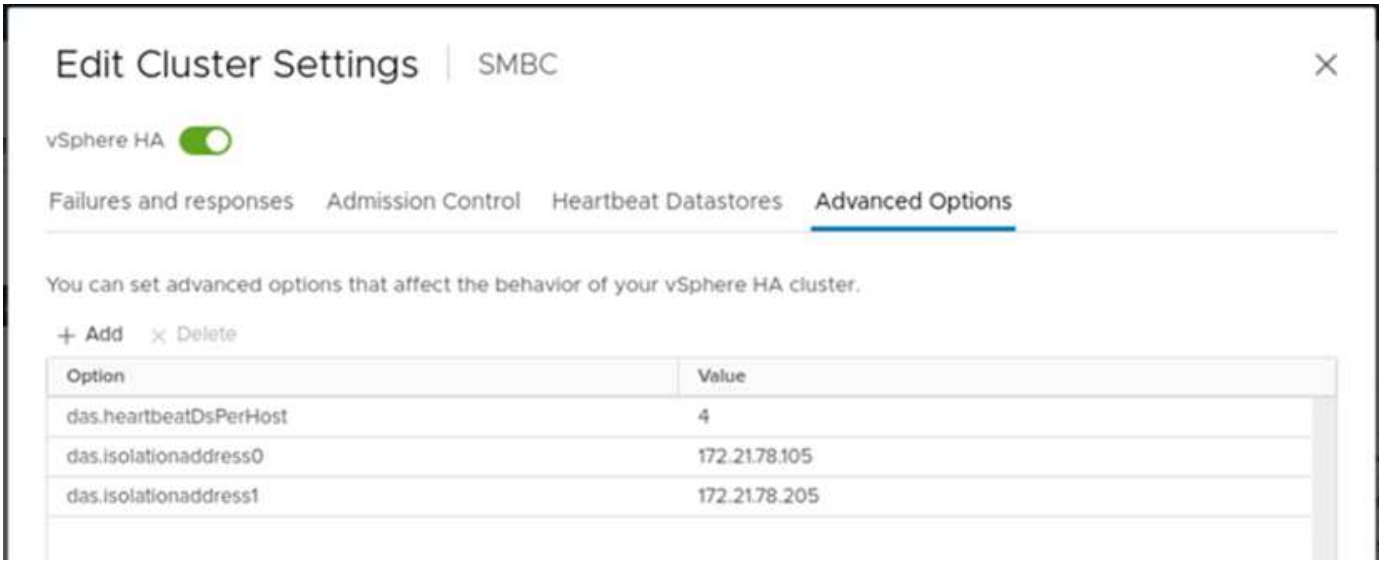




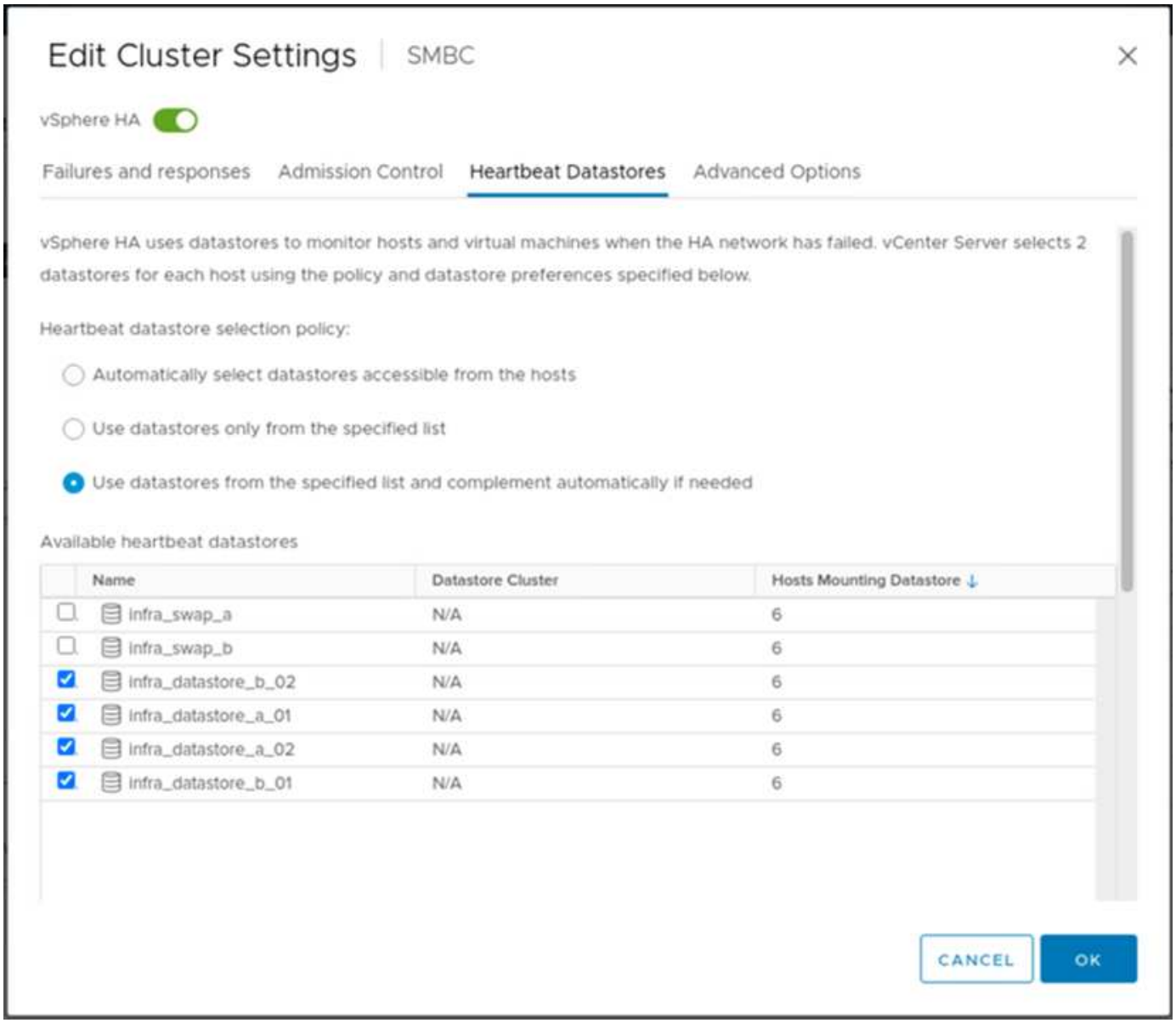
Heartbeat do vSphere HA

O VMware vSphere HA tem um mecanismo de heartbeat para validação do estado do host. O mecanismo de heartbeat primário é através da rede, e o mecanismo de heartbeat secundário é através do datastore. Se os heartbeats não forem recebidos, ele decide se ele é isolado da rede fazendo ping no gateway padrão ou nos endereços de isolamento configurados manualmente. Para o heartbeat do datastore, a VMware recomenda aumentar os datastores de heartbeat do mínimo de dois para quatro para um cluster estendido.

Para a validação da solução, os dois endereços IP de gerenciamento de cluster ONTAP são usados como endereço de isolamento. Além disso, a opção avançada recomendada do vSphere HA `ds.heartbeatDsPerHost` com um valor de 4 foi adicionada, conforme mostrado na figura a seguir.



Para o datastore heartbeat, especifique os quatro datastores compartilhados do cluster e complemente automaticamente, como mostrado na figura a seguir.



Para obter práticas recomendadas e configurações adicionais para o cluster de armazenamento VMware HA Cluster e VMware vSphere Metro, consulte "Criação e uso de clusters de HA do vSphere" "VMware vSphere Metro Storage Cluster (vMSC)" e o KB da VMware para "NetApp ONTAP com NetApp SnapMirror Business Continuity (SM-BC) e VMware vSphere Metro Storage Cluster (vMSC)".

"Próximo: Validação da solução - cenários validados."

Validação da solução - cenários validados

"Anterior: Validação da solução - virtualização."

A solução FlexPod Datacenter SM-BC protege os serviços de dados para uma variedade de cenários de ponto único de falha, bem como para um desastre no local. O design redundante implementado em cada local fornece alta disponibilidade, e a implementação SM-BC com replicação síncrona de dados entre locais protege os serviços de dados de um desastre em todo o site de um local. A solução implantada é validada para as funções de solução desejadas e vários cenários de falha para os quais a solução foi

projetada para proteger.

Validação das funções da solução

Uma variedade de casos de teste são usados para verificar as funções da solução e simular cenários de falha parcial e completa do local. Para minimizar a duplicação com os testes já realizados nas soluções de datacenter FlexPod existentes no Programa de Design validado da Cisco, o foco deste relatório é nos aspetos relacionados à SM-BC da solução. Algumas validações gerais do FlexPod são incluídas para que os profissionais passem por suas validações de implementação.

Para a validação da solução, uma máquina virtual do Windows 10 por host ESXi foi criada em todos os hosts ESXi em ambos os sites. A ferramenta Iometer foi instalada e usada para gerar e/S para dois discos de dados virtuais que são mapeados a partir dos armazenamentos de dados iSCSI locais compartilhados. Os parâmetros de carga de trabalho do Iometer configurados foram I/o de 8 KB, 75% leitura e 50% aleatória, com 8 comandos de e/S pendentes para cada disco de dados. Para a maioria dos cenários de teste realizados, a continuação do Iometer I/o serve como uma indicação de que o cenário não causou uma interrupção do serviço de dados.

Como o SM-BC é essencial para aplicativos empresariais, como servidores de banco de dados, a instância do Microsoft SQL Server 2019 em uma máquina virtual do Windows Server 2022 também foi incluída como parte do teste para confirmar que o aplicativo continua a ser executado quando o armazenamento em seu local local não está disponível e o serviço de dados é retomado no armazenamento do local remoto sem interrupções do aplicativo.

Teste de inicialização da SAN iSCSI do host ESXi

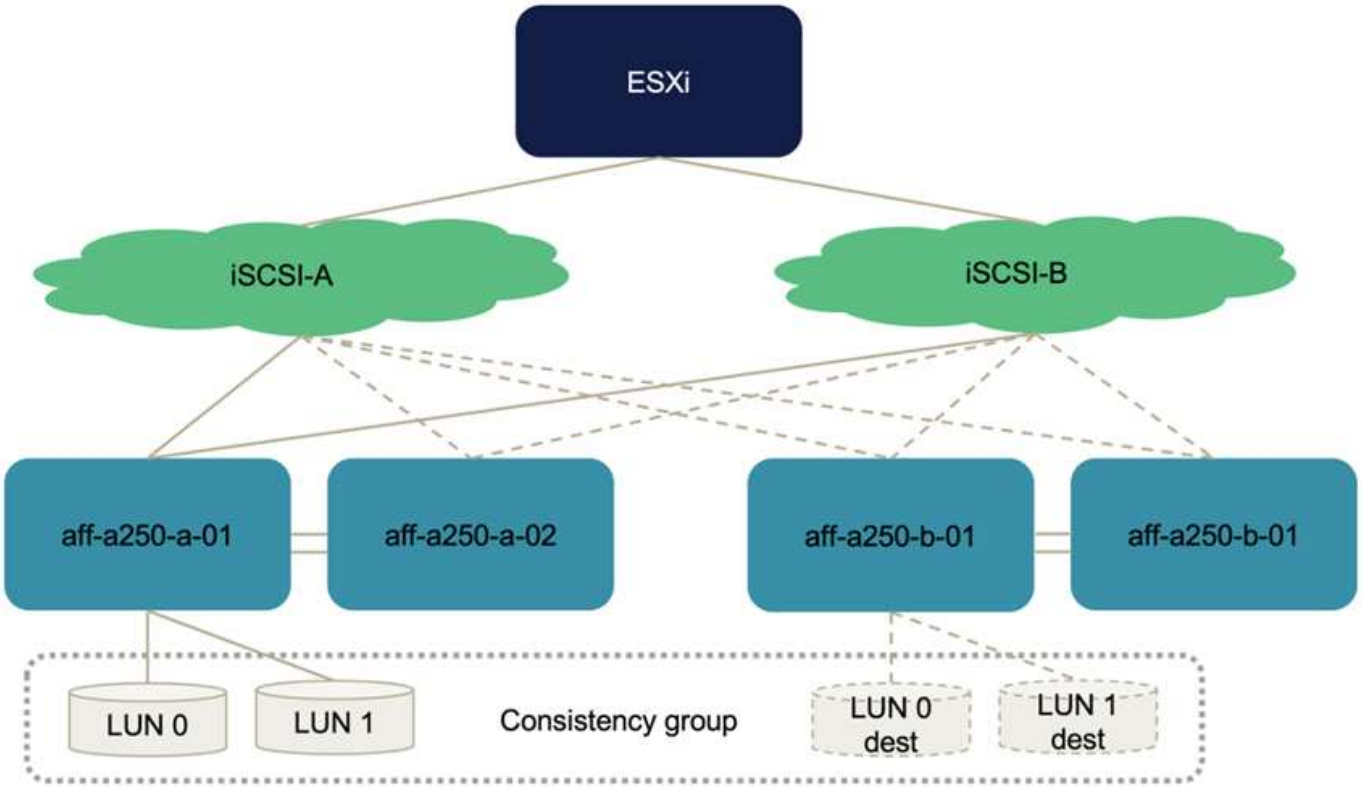
Os hosts ESXi na solução são configurados para inicializar a partir de SAN iSCSI. O uso da inicialização SAN simplifica o gerenciamento do servidor ao substituir um servidor, pois o perfil de serviço do servidor pode ser associado a um novo servidor para que ele seja inicializado sem fazer alterações adicionais de configuração.

Além de inicializar um host ESXi localizado em um local a partir de seu LUN de inicialização iSCSI local, testes também foram realizados para inicializar o host ESXi quando seu controlador de armazenamento local estiver em um estado de aquisição ou quando seu cluster de armazenamento local estiver completamente indisponível. Esses cenários de validação garantem que os hosts ESXi estejam configurados adequadamente por design e possam ser inicializados durante um cenário de manutenção de armazenamento ou desastre para recuperação de desastres para fornecer continuidade de negócios.

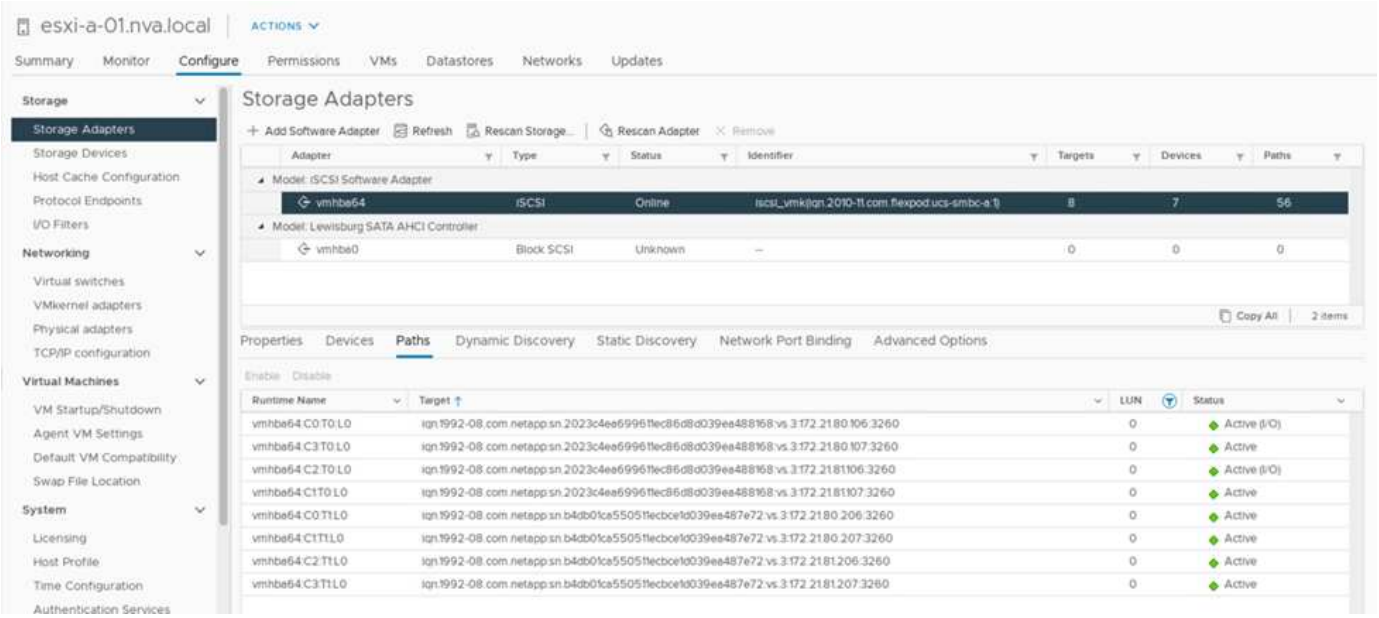
Antes de configurar a relação de grupo de consistência SM-BC, um iSCSI LUN hospedado por um par de HA de controladora de storage tem quatro caminhos, dois por cada malha iSCSI, com base na implementação de práticas recomendadas. Um host pode chegar ao LUN através das duas VLANs/malhas iSCSI para o controlador de hospedagem LUN, bem como através do parceiro de alta disponibilidade do controlador.

Depois que a relação de grupo de consistência SM-BC é configurada e os LUNs espelhados são mapeados adequadamente para os iniciadores, a contagem de caminho para o LUN dobra. Para essa implementação, passa de ter dois caminhos ativos/otimizados e dois caminhos ativos/não otimizados para ter dois caminhos ativos/otimizados e seis caminhos ativos/não otimizados.

A figura a seguir ilustra os caminhos que um host ESXi pode levar para acessar um LUN, por exemplo, LUN 0. Como o LUN é anexado ao site Um controlador 01, apenas os dois caminhos que acessam diretamente o LUN por meio desse controlador são ativos/otimizados e todos os seis caminhos restantes são ativos/não otimizados.



A captura de tela a seguir das informações de caminho do dispositivo de armazenamento mostra como o host ESXi vê os dois tipos de caminhos de dispositivo. Os dois caminhos ativos/otimizados são mostrados como tendo `active (I/O)` o status do caminho, enquanto os seis caminhos ativos/não otimizados são mostrados apenas `active` como . Observe também que a coluna destino mostra os dois destinos iSCSI e os respetivos endereços IP iSCSI LIF para chegar aos destinos.



Quando um dos controladores de storage está inativo para manutenção ou atualização, os dois caminhos que alcançam o controlador inativo não estão mais disponíveis e aparecem com o status do caminho `dead`.

Se um failover do grupo de consistência ocorrer no cluster de storage primário, seja devido a testes de failover manual ou failover automático, o cluster de storage secundário continuará a fornecer serviços de dados para

as LUNs no grupo de consistência SM-BC. Como as identidades LUN são preservadas e os dados foram replicados de forma síncrona, todos os LUNs de inicialização do host ESXi protegidos por grupos de consistência SM-BC permanecem disponíveis no cluster de armazenamento remoto.

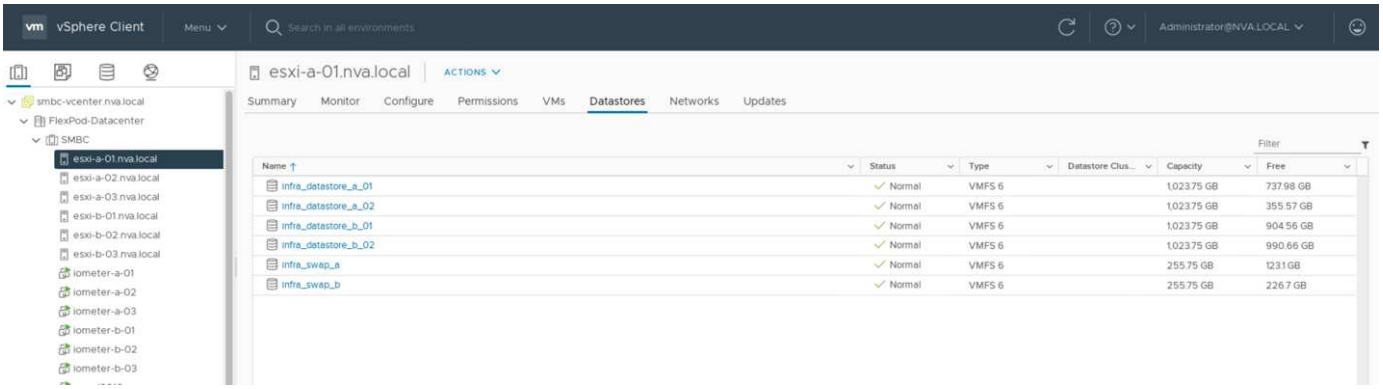
Teste de afinidade de VM/host e VMware vMotion

Embora uma solução genérica de data center VMware FlexPod ofereça suporte a vários protocolos, como FC, iSCSI, NVMe e NFS, o recurso da solução FlexPod SM-BC oferece suporte a protocolos SAN FC e iSCSI, normalmente usados para soluções essenciais aos negócios. Esta validação utiliza apenas armazenamentos de dados baseados em protocolo iSCSI e arranque SAN iSCSI.

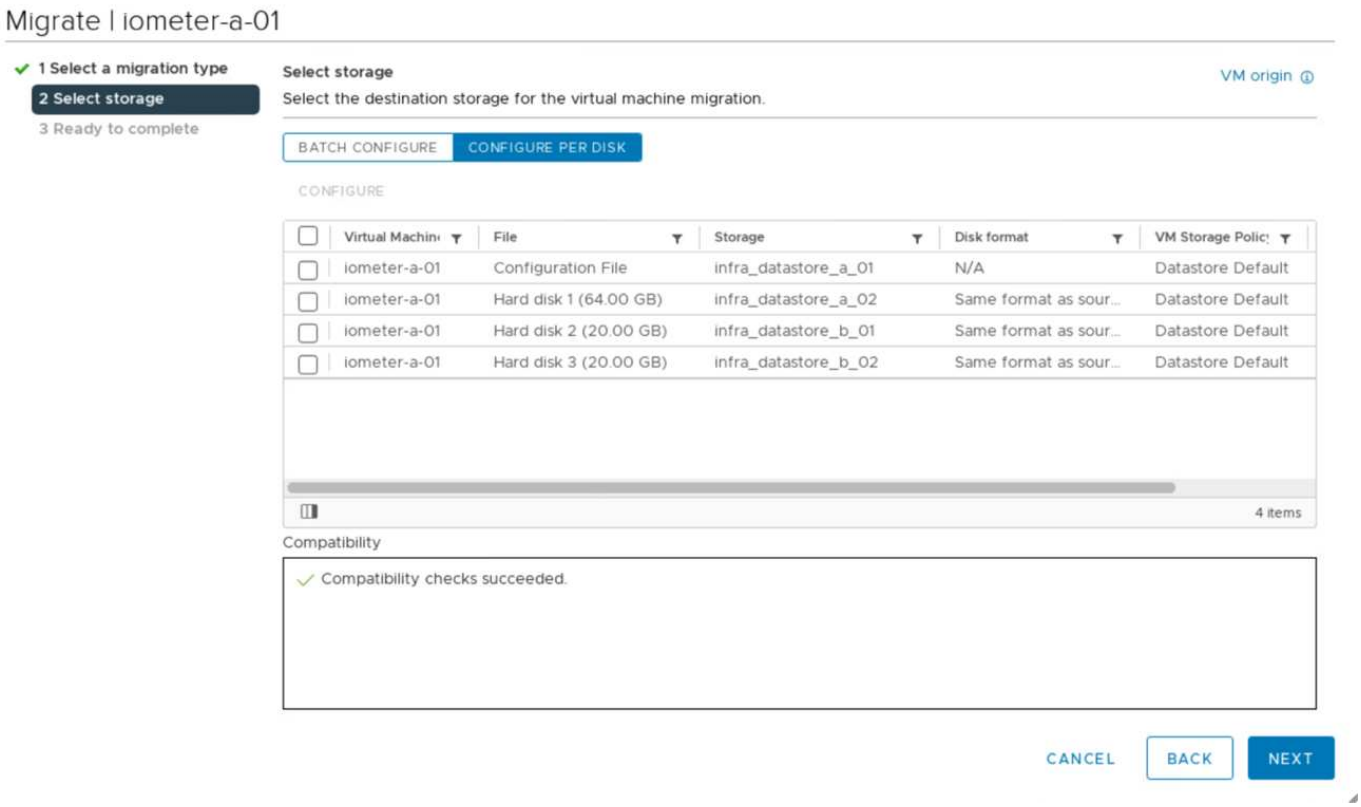
Para permitir que máquinas virtuais usem serviços de armazenamento de qualquer local SM-BC, os armazenamentos de dados iSCSI de ambos os locais devem ser montados por todos os hosts do cluster para permitir a migração de máquinas virtuais entre os dois locais e para cenários de failover de desastres.

Para aplicações executadas na infraestrutura virtual que não exigem a proteção do grupo de consistência SM-BC nos locais, o protocolo NFS e os datastores NFS também podem ser usados. Nesse caso, deve ser observado cuidado ao alocar o storage para VMs para que as aplicações essenciais aos negócios estejam usando adequadamente os datastores SAN protegidos pelo grupo de consistência SM-BC para fornecer continuidade dos negócios.

A captura de tela a seguir mostra que os hosts estão configurados para montar armazenamentos de dados iSCSI de ambos os sites.



Você tem a opção de migrar discos de máquina virtual entre armazenamentos de dados iSCSI disponíveis de ambos os sites, como mostrado na figura a seguir. Para considerações de desempenho, é ótimo ter máquinas virtuais que usam storage de seu cluster de storage local para reduzir as latências de e/S de disco. Isto é especialmente verdadeiro quando os dois locais estão localizados a algumas distâncias distante devido à latência física da distância de ida e volta de aproximadamente 1msm por 100kmm de distância.



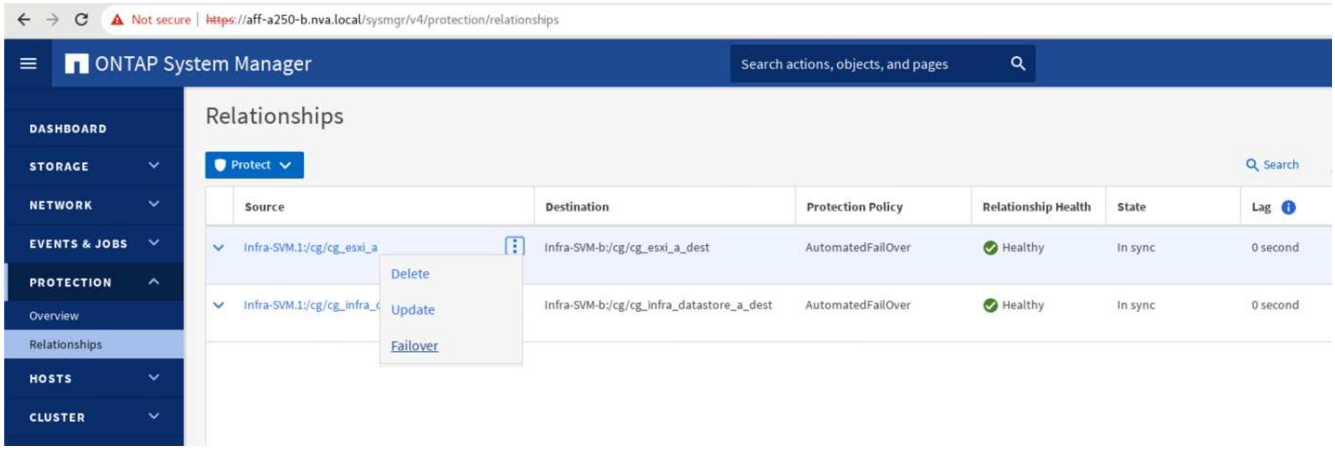
Testes de vMotion de máquinas virtuais para um host diferente no mesmo site, bem como em todos os sites foram realizados e foram bem-sucedidos. Depois de migrar manualmente uma máquina virtual entre sites, a regra de afinidade VM/Host ativa e migra a máquina virtual de volta para o grupo onde ela pertence sob a condição normal.

Failover de storage planejado

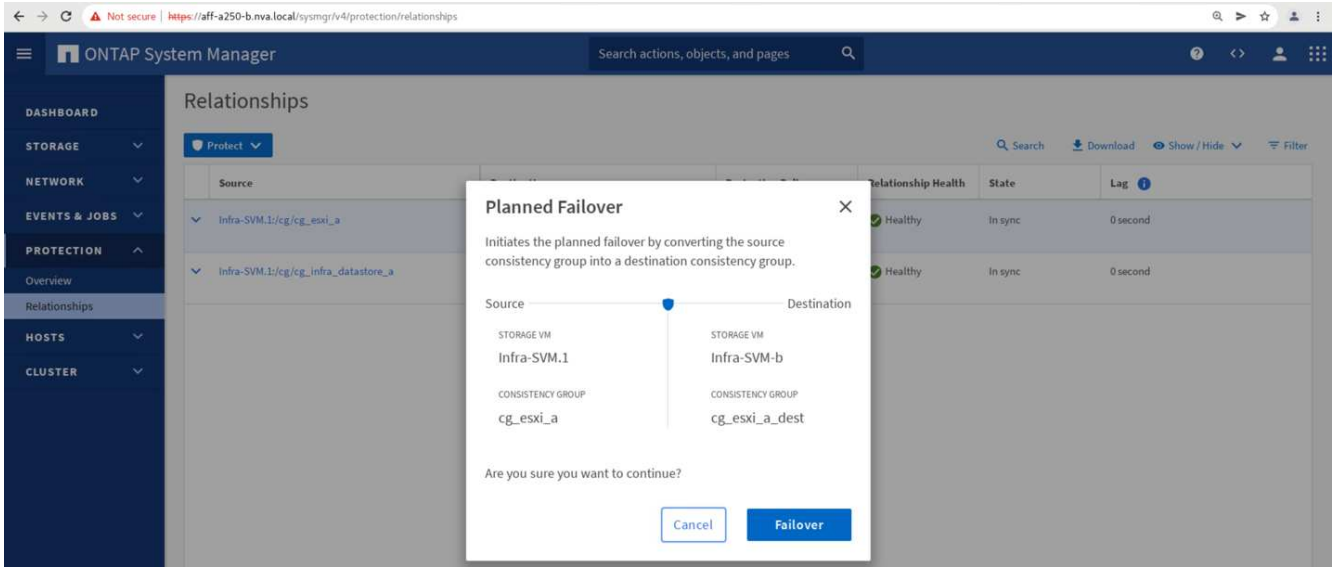
As operações de failover de armazenamento planejadas devem ser executadas na solução após a configuração inicial para determinar se a solução está funcionando corretamente após o failover de armazenamento. Os testes podem ajudar a identificar quaisquer problemas de conetividade ou configuração que possam levar a interrupções de e/S. Testar e resolver regularmente quaisquer problemas de conetividade ou configuração ajuda a fornecer serviços de dados ininterruptos quando ocorre um desastre no local real. O failover de armazenamento planejado também pode ser usado antes de uma atividade de manutenção de armazenamento agendada para que os serviços de dados possam ser atendidos a partir do local não afetado.

Para iniciar um failover manual dos serviços de dados de armazenamento do local A para o local B, você pode usar o local B ONTAP System Manager para executar a ação.

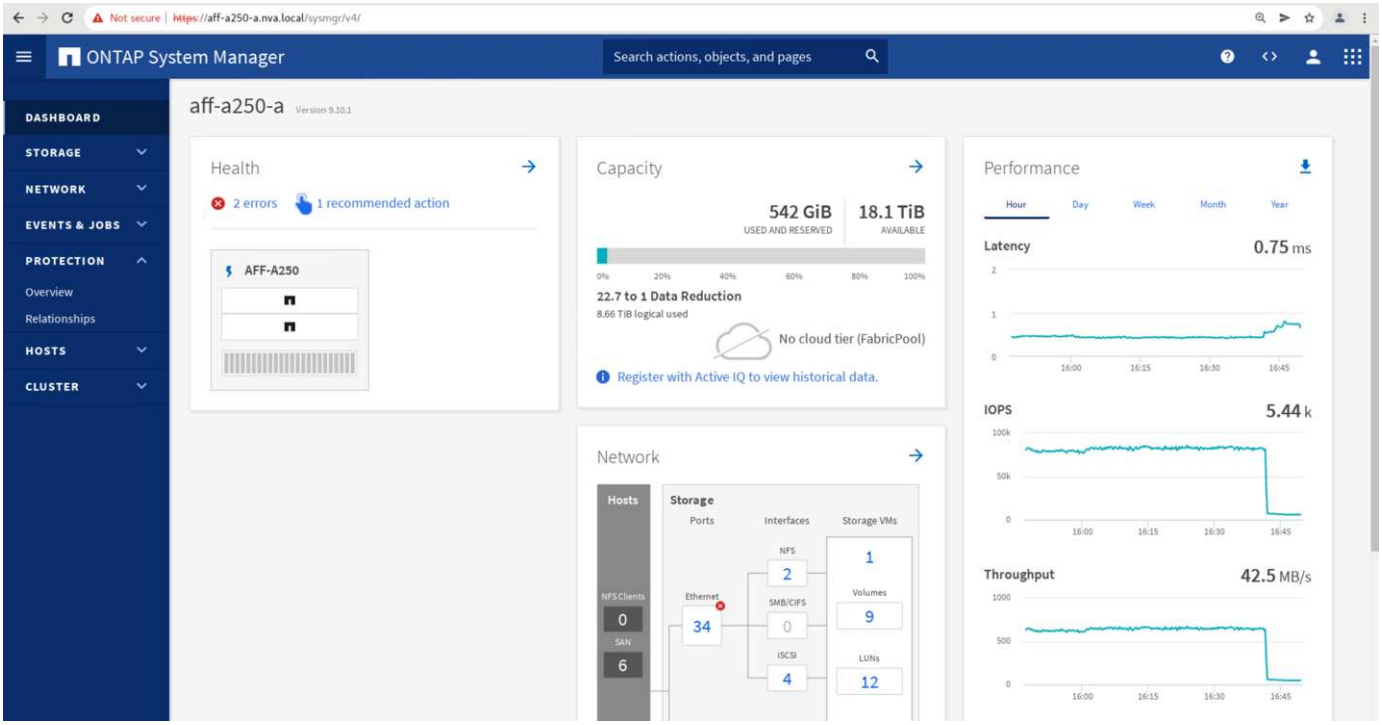
1. Navegue até a tela proteção > relacionamentos para confirmar se o estado da relação do grupo de consistência é `In Sync`. Se ele ainda estiver `Synchronizing` no estado, aguarde até que o estado se torne `In Sync` antes de executar um failover.
2. Expanda os pontos ao lado do nome da fonte e clique em failover.



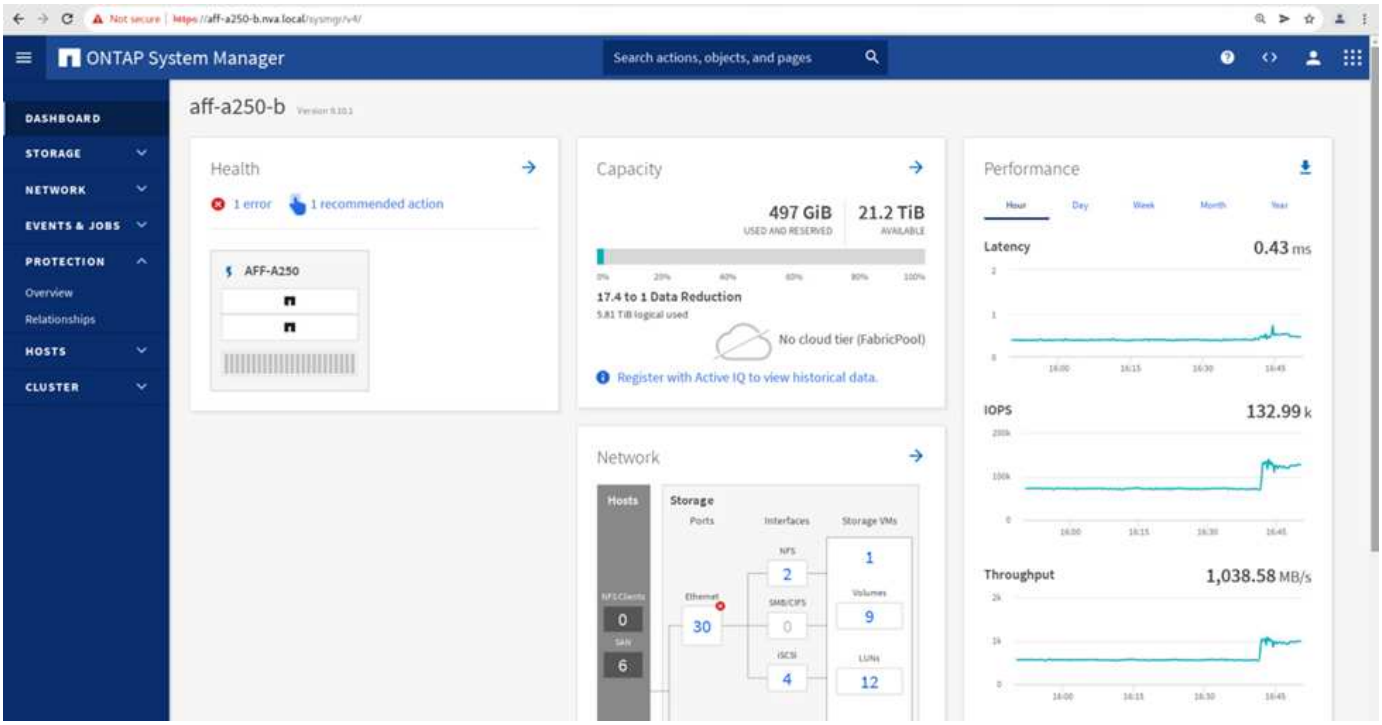
3. Confirme o failover para que a ação seja iniciada.



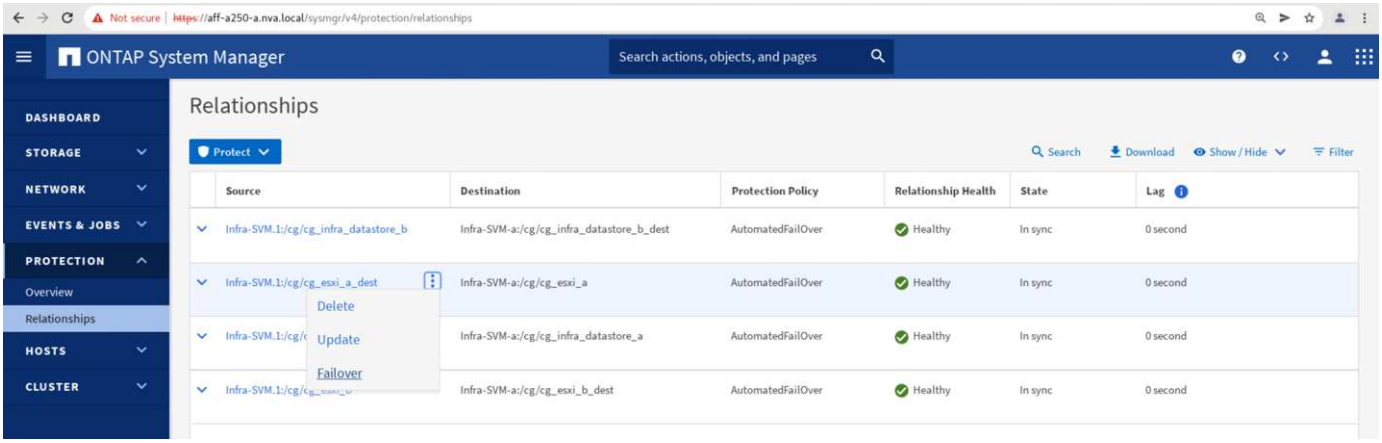
Pouco depois de iniciar o failover dos dois grupos de consistência `cg_esxi_a` e `cg_infra_datastore_a`, no local B System Manager GUI, o Site A I/o que atende esses dois grupos de consistência passou para o local B. como resultado, a I/o no local A reduziu significativamente, conforme mostrado no site A Painel De desempenho do System Manager.



Por outro lado, o painel desempenho do painel do site B System Manager mostra um aumento significativo de IOPs, devido ao fornecimento de e/S adicionais transferidas do local A para cerca DE 130k IOPs e a uma taxa de transferência de aproximadamente 1GB GB/s, mantendo uma latência de e/S inferior a 1 milissegundos.

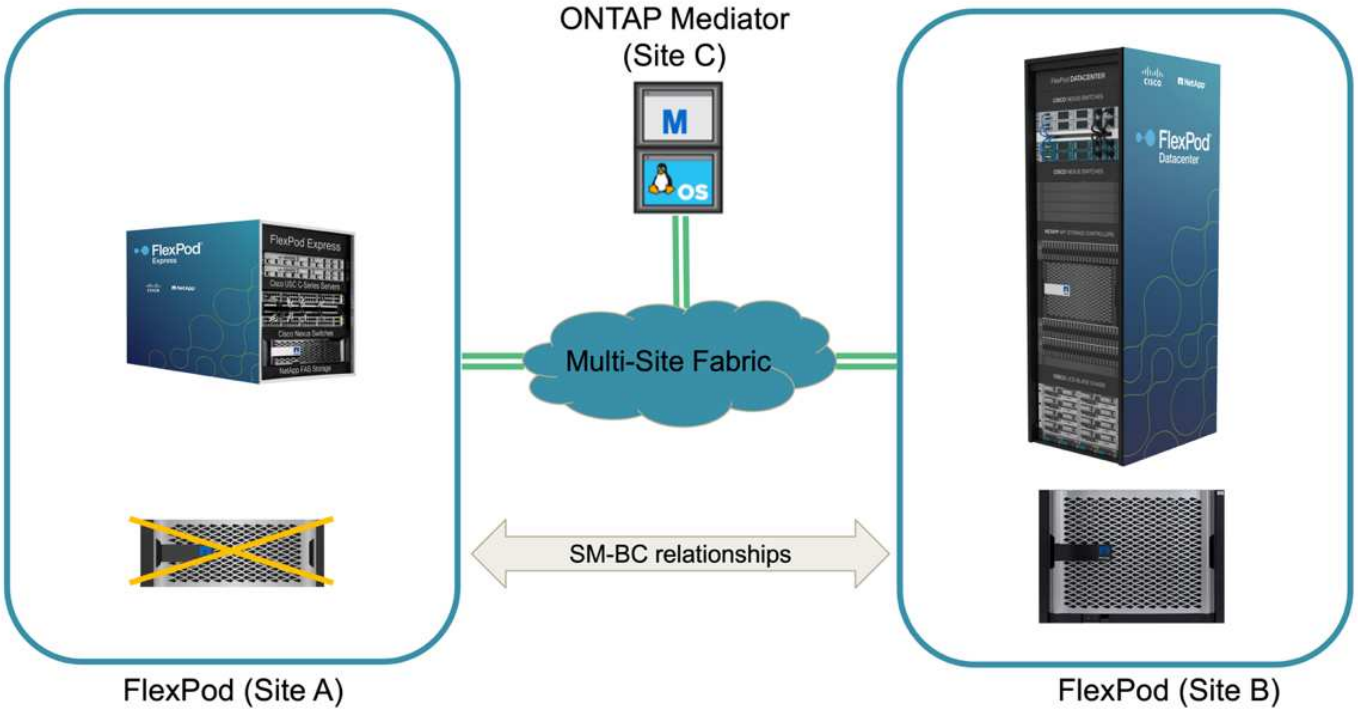


Com a e/S migrada de forma transparente do local A para o local B, os controladores de armazenamento do local A podem agora ser suspensos para manutenção programada. Depois que o trabalho de manutenção ou teste for concluído e o local Um cluster de armazenamento for colocado de volta e operacional, verifique e aguarde que o estado de proteção do grupo de consistência mude para `In sync` antes de executar um failover para retornar a e/S do local B ao local A. tenha em atenção que quanto mais tempo um local for retirado para manutenção ou teste, mais tempo demora antes de os dados serem sincronizados e o grupo de consistência for devolvido ao `In sync` estado.



Failover de storage não planejado

Um failover de storage não planejado pode ocorrer quando um desastre real acontece ou durante uma simulação de desastre. Por exemplo, veja a figura a seguir em que o sistema de storage no local A experimenta uma falha de energia, um failover de storage não planejado é acionado e os serviços de dados para LUNs do local A, protegidos pelas relações SM-BC, continuam do local B.

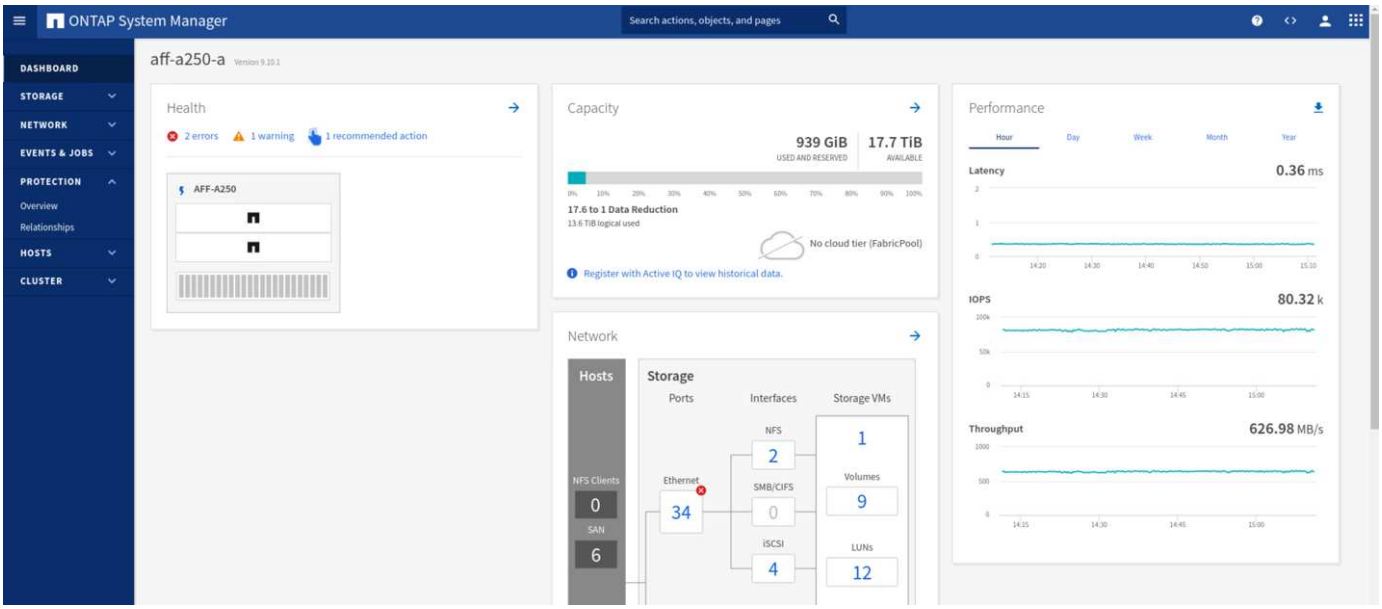


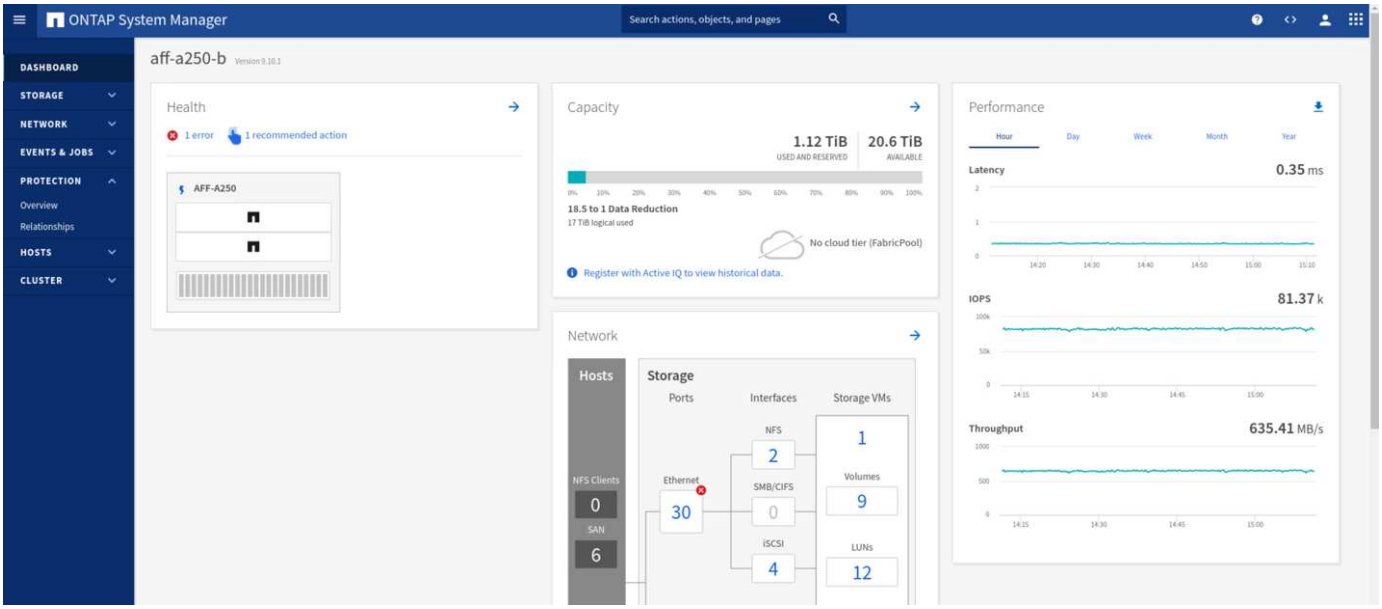
Para simular um desastre de armazenamento no local A, ambos os controladores de armazenamento no local A podem ser desligados desligando fisicamente o interrutor de alimentação para interromper o fornecimento de energia para os controladores, ou usando o comando de gerenciamento de energia do sistema dos processadores de serviços de armazenamento para desligar os controladores.

Quando o cluster de armazenamento no local perde energia, há uma parada repentina dos serviços de dados fornecidos pelo local Um cluster de armazenamento. Em seguida, o Mediador ONTAP, que monitora a solução SM-BC de um terceiro local, deteta Uma condição de falha de armazenamento do local e permite que a solução SM-BC execute um failover automatizado não planejado. Isso permite que os controladores de storage do local B continuem os serviços de dados para as LUNs configuradas nas relações de grupo de consistência SM-BC com o local A.

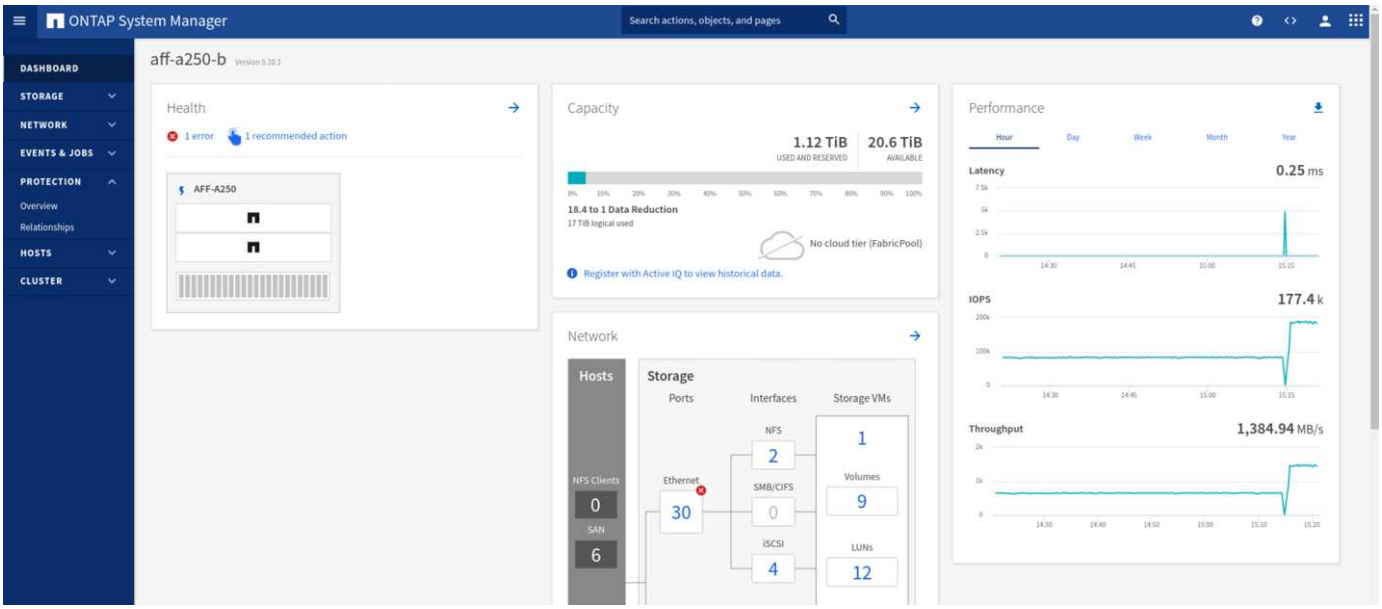
Do ponto de vista do aplicativo, os serviços de dados param brevemente enquanto o sistema operacional verifica o status do caminho para os LUNs e, em seguida, recomeça a e/S nos caminhos disponíveis para os controladores de storage do local B sobreviventes.

Durante os testes de validação, a ferramenta Iometer nas VMs em ambos os locais gera e/S para seus datastores locais. Após o local Um cluster foi desligado, e/S parou brevemente e, em seguida, retomou posteriormente. Veja as duas figuras a seguir para os painéis do cluster de armazenamento no local A e no local B, respetivamente, antes do desastre, que mostram aproximadamente 80k IOPS e 600 MB/s de taxa de transferência em cada local.

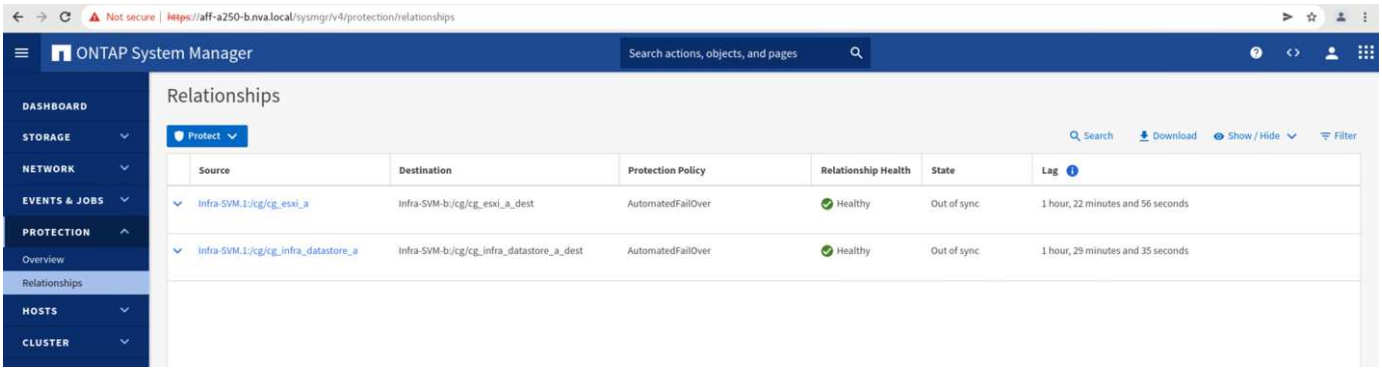




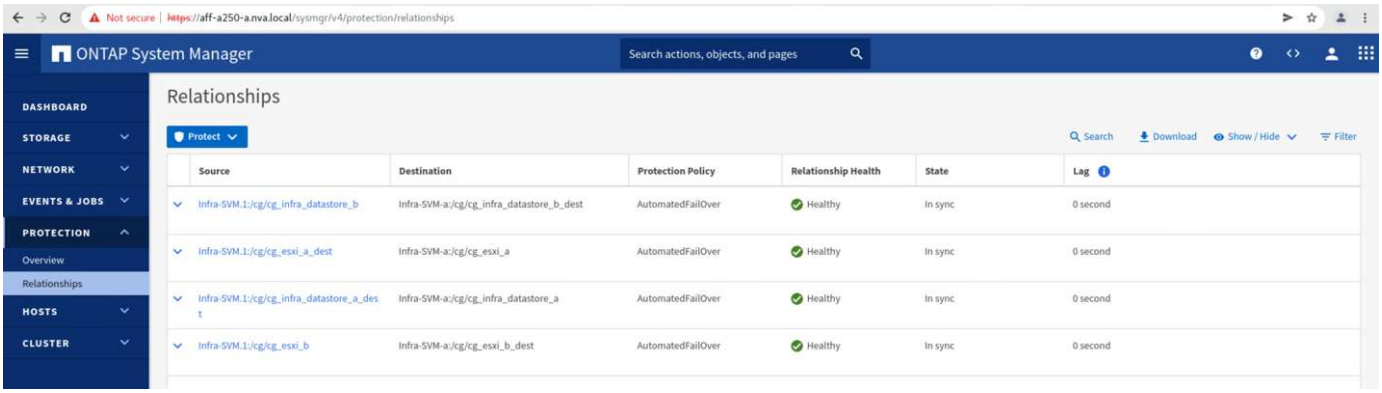
Depois de desligar os controladores de armazenamento no local A, podemos validar visualmente que a e/S do controlador de armazenamento local B aumentou drasticamente para fornecer serviços de dados adicionais em nome do local A (veja a figura a seguir). Além disso, a GUI das VMs do Iometer também mostrou que a e/S continuou apesar da interrupção do cluster de storage no local. Observe que, se houver datastores adicionais com suporte de LUNs não protegidos por relacionamentos SM-BC, esses datastores não estarão mais acessíveis quando o desastre do storage ocorrer. Portanto, é importante avaliar as necessidades de negócios dos vários dados de aplicativos e colocá-los adequadamente em datastores protegidos por relacionamentos SM-BC para fornecer continuidade de negócios.



Enquanto o Site Um cluster está inativo, as relações dos grupos consistentes mostram `Out of sync` o status como mostrado na figura a seguir. Depois que a energia é ligada novamente para os controladores de armazenamento no local A, o cluster de armazenamento é inicializado e a sincronização de dados entre o local A e o local B acontece automaticamente.



Antes de retornar os serviços de dados do site B de volta ao site A, você deve verificar o site A System Manager e garantir que as relações SM-BC sejam alcançadas e o status estejam de volta em sincronia. Depois de confirmar que os grupos de consistência estão sincronizados, uma operação de failover manual pode ser iniciada para retornar serviços de dados nos relacionamentos do grupo de consistência de volta ao local A.



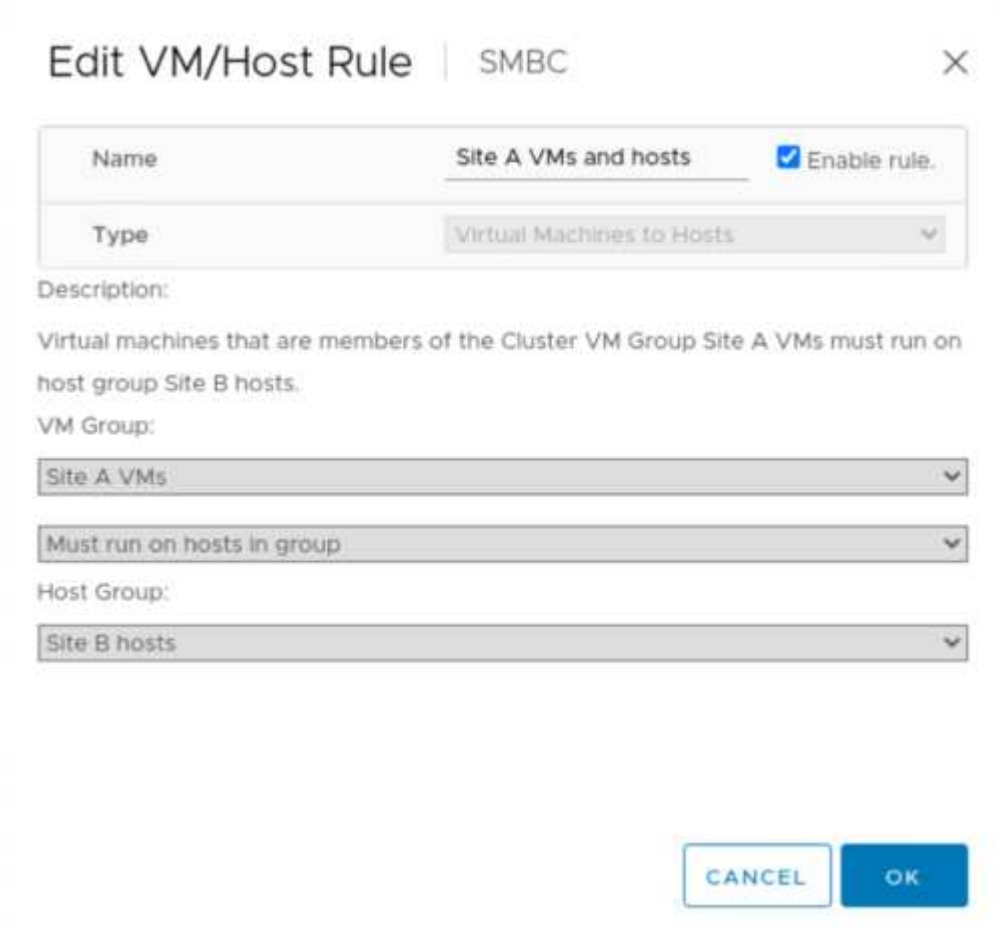
Manutenção completa do local ou falha do local

Um local pode precisar de manutenção do local, experimentar perda de energia ou pode ser afetado por um desastre natural, como um furacão ou um Terremoto. Portanto, é crucial que você exerça cenários planejados e não planejados de falha do local para ajudar a garantir que sua solução FlexPod SM-BC esteja configurada adequadamente para sobreviver a essas falhas em todos os seus aplicativos e serviços de dados essenciais aos negócios. Os seguintes cenários relacionados ao local foram validados.

- Cenário de manutenção do local planejado migrando máquinas virtuais e serviços de dados críticos para o outro site
- Cenário de falha não planejada no local desligando servidores e controladores de storage para simulação de desastres

Para preparar um local para a manutenção planejada do local, é necessária uma combinação de migração de máquinas virtuais afetadas fora do local com o vMotion e um failover manual das relações do grupo de consistência SM-BC para migrar máquinas virtuais e serviços de dados críticos para o site alternativo. Os testes foram realizados em duas ordens diferentes: O VMotion primeiro seguido pelo failover SM-BC e o failover SM-BC primeiro seguido pelo vMotion, para confirmar que as máquinas virtuais continuam sendo executadas e os serviços de dados não são interrompidos.

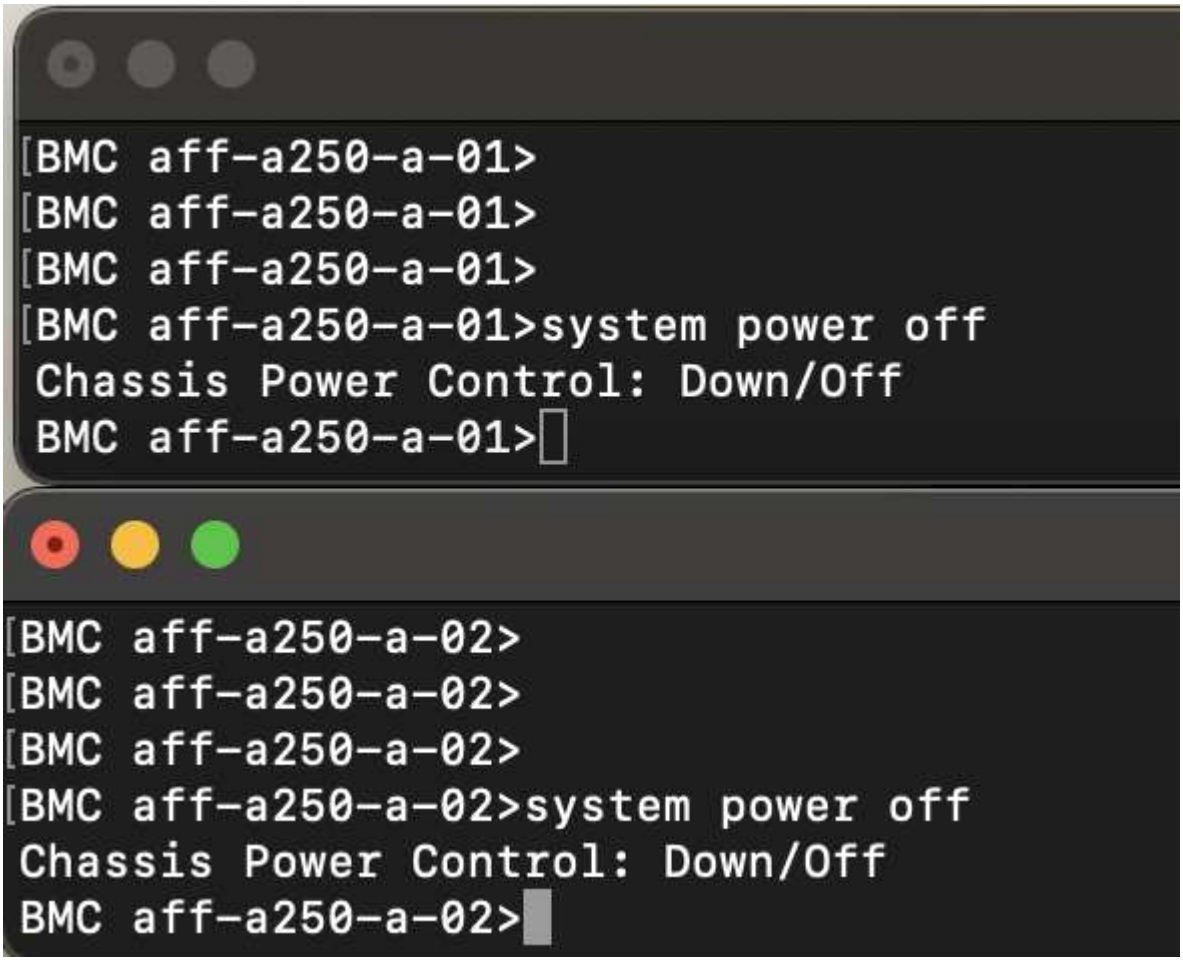
Antes de executar a migração planejada, atualize a regra de afinidade VM/host para que as VMs que estão sendo executadas no site sejam migradas automaticamente para fora do site que está sendo submetido a manutenção. A captura de tela a seguir mostra um exemplo de modificação do site De Uma regra de afinidade de VM/host para que as VMs migrem do local A para o local B automaticamente. Em vez de especificar que as VMs agora precisam ser executadas no local B, você também pode optar por desativar a regra de afinidade temporariamente para que as VMs possam ser migradas manualmente.



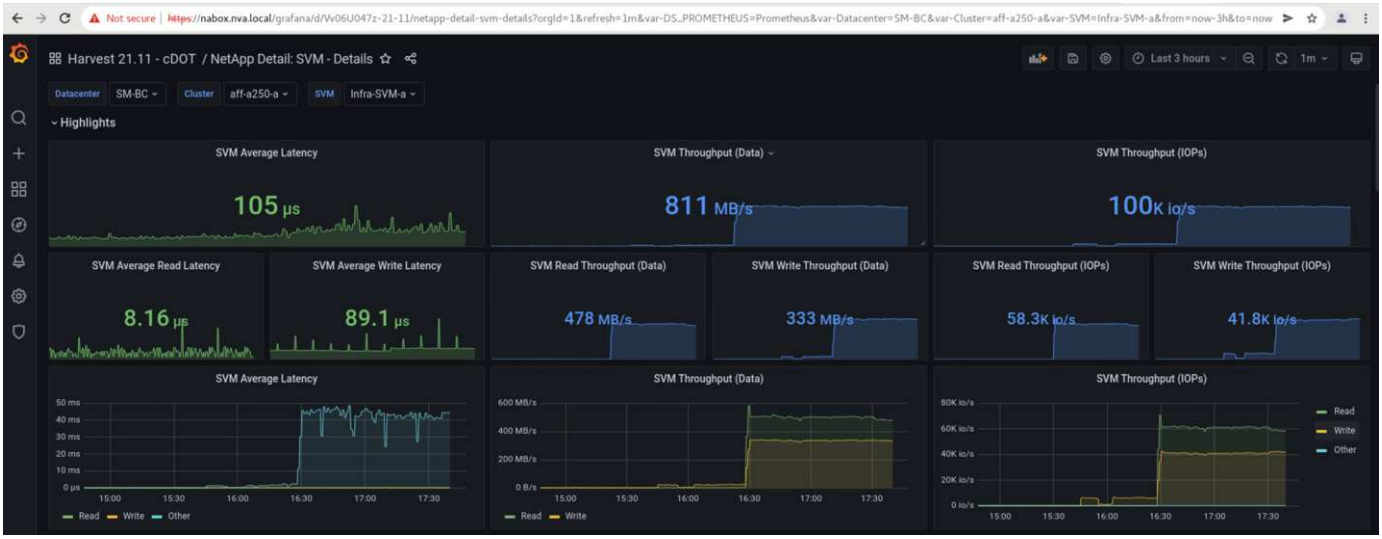
Depois que as máquinas virtuais e os serviços de armazenamento tiverem sido migrados, você poderá desligar servidores, controladores de armazenamento, compartimentos de discos e switches e executar as atividades de manutenção necessárias do local. Quando a manutenção do site for concluída e a instância do FlexPod for reativada, você poderá alterar a afinidade do grupo de hosts para que as VMs voltem ao site original. Depois disso, você deve alterar a regra de afinidade do site VM/Host "deve ser executada em hosts no grupo" para "deve ser executada em hosts no grupo" para que as máquinas virtuais possam ser executadas em hosts no outro local caso ocorra um desastre. Para os testes de validação, todas as máquinas virtuais foram migradas com sucesso para o outro site e os serviços de dados continuaram sem problemas após a execução de um failover para as relações SM-BC.

Para a simulação não planejada de desastre no local, os servidores e os controladores de storage foram desligados para simular um desastre no local. O recurso VMware HA deteta as máquinas virtuais descarregadas e reinicia essas máquinas virtuais no site sobrevivente. Além disso, o Mediador ONTAP em execução em um terceiro local deteta a falha do local e o local sobrevivente inicia um failover e começa a fornecer serviços de dados para o local inativo conforme esperado.

A captura de tela a seguir mostra que a CLI do processador de serviços dos controladores Storge foi usada para desligar o site De Um cluster abruptamente para simular um desastre de armazenamento no local.



Os dashboards de máquina virtual de armazenamento dos clusters de armazenamento, conforme capturados pela ferramenta de coleta de dados NetApp Harvest e exibidos no painel Grafana na ferramenta de monitoramento NAbox, são mostrados nas duas capturas de tela a seguir. Como pode ser visto no lado direito dos gráficos IOPS e throughputs, o cluster do local B pega o Cluster De Uma carga de trabalho de armazenamento imediatamente depois que o local Em Que Um cluster cai.

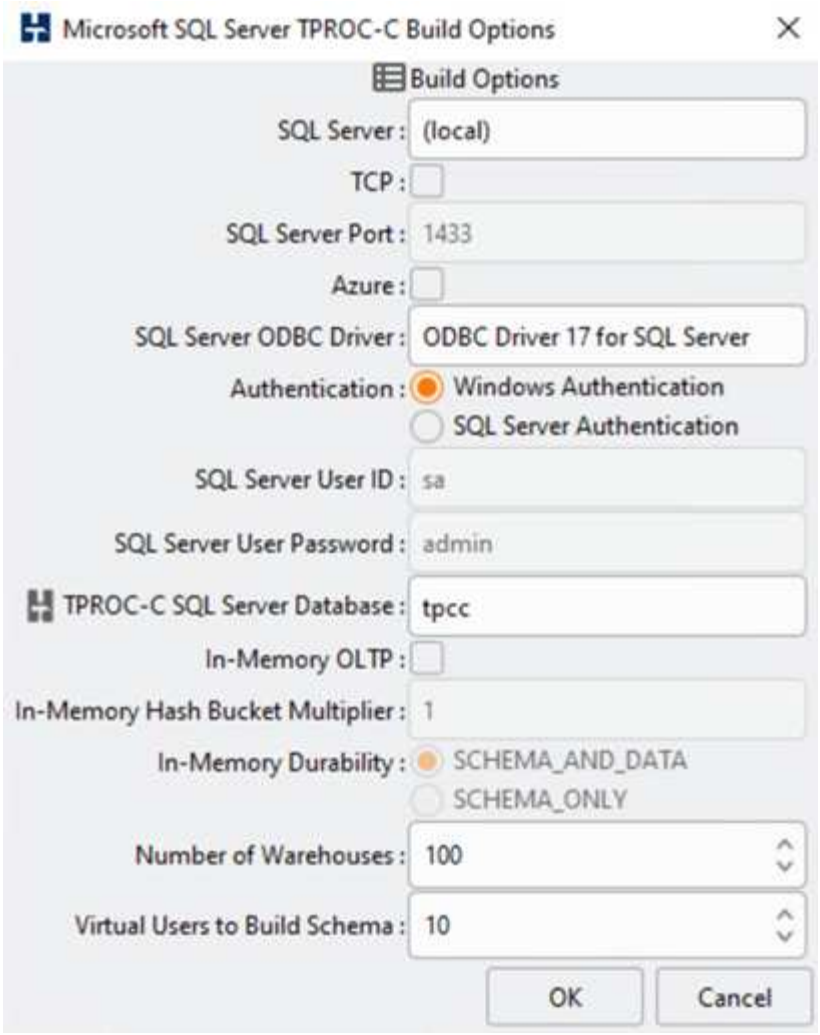


Microsoft SQL Server

O Microsoft SQL Server é uma plataforma de banco de dados amplamente adotada e implantada para TI corporativa. A versão do Microsoft SQL Server 2019 traz muitos novos recursos e melhorias para seus mecanismos relacionais e analíticos. Ele dá suporte a workloads com aplicações executadas no local, na nuvem e híbridas podem usar uma combinação das duas. Além disso, ele pode ser implantado em várias plataformas, incluindo Windows, Linux e containers.

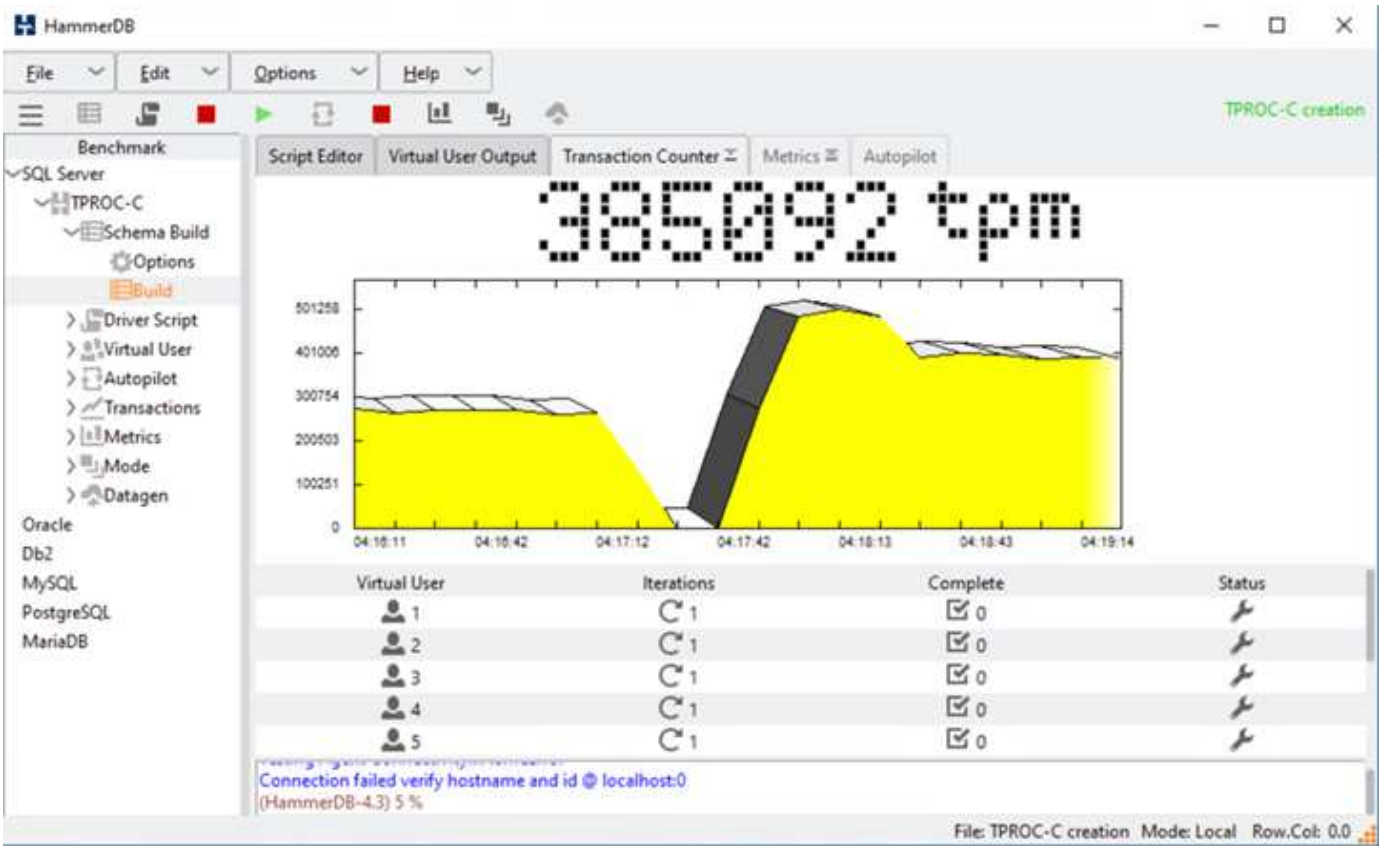
Como parte da validação de carga de trabalho crítica para os negócios da solução FlexPod SM-BC, o Microsoft SQL Server 2019 instalado em uma VM do Windows Server 2022 está incluído junto com as VMs Iometer para testes de failover de armazenamento planejados e não planejados do SM-BC. Na VM do Windows Server 2022, o SQL Server Management Studio é instalado para gerenciar o servidor SQL. Para testes, a ferramenta de banco de dados HammerDB é usada para gerar transações de banco de dados.

A ferramenta de teste de banco de dados HammerDB foi configurada para teste com a carga de trabalho Microsoft SQL Server TPROC-C. Para as configurações de compilação do esquema, as opções foram atualizadas para usar 100 armazéns com 10 usuários virtuais, como mostrado na captura de tela a seguir.



Depois que as opções de compilação do esquema foram atualizadas, o processo de compilação do esquema foi iniciado. Alguns minutos depois, uma falha não planejada simulada do cluster de armazenamento local B foi introduzida desligando ambos os nós do cluster de armazenamento AFF A250 de dois nós ao mesmo tempo usando comandos CLI do processador do sistema.

Após uma breve pausa das transações de banco de dados, o failover automatizado para a correção de desastres foi iniciado e as transações foram retomadas. A captura de tela a seguir mostra a captura de tela do HammerDB Transaction Counter naquela época. Como o banco de dados do Microsoft SQL Server normalmente reside no cluster de armazenamento do site B, a transação parou brevemente quando o armazenamento no local B foi desativado e, em seguida, retomado após o failover automatizado aconteceu.



As métricas de cluster de armazenamento foram capturadas usando a ferramenta NAbox com a ferramenta de monitoramento de colheita NetApp instalada. Os resultados são exibidos nos painéis Grafana predefinidos para a máquina virtual de armazenamento e outros objetos de armazenamento. O dashboard fornece metrics para latência, taxa de transferência, IOPS e detalhes adicionais com estatísticas de leitura e gravação separadas para o local B e o local A.

Esta captura de tela mostra o painel de desempenho do NAbox Grafana para o cluster de armazenamento local B.

O IOPS do cluster de storage do local B era de cerca de 100K mil IOPS antes da introdução do desastre. Em seguida, as métricas de desempenho mostraram uma queda acentuada para zero no lado direito dos gráficos devido ao desastre. Como o cluster de armazenamento do local B estava inativo, nada poderia ser coletado

do cluster do local B após a introdução do desastre.

Por outro lado, o IOPS do local Um cluster de storage pegou os workloads adicionais do local B após o failover automatizado. A carga de trabalho adicional pode ser facilmente vista no lado direito dos gráficos de IOPS e throughput na captura de tela a seguir, que mostra o painel de desempenho do NAbox Grafana para o local De Um cluster de armazenamento.

O cenário de teste de desastre de storage acima confirmou que o workload do Microsoft SQL Server pode sobreviver a uma interrupção completa do cluster de storage no local B, onde o banco de dados reside. A aplicação usou de forma transparente os serviços de dados fornecidos pelo local Um cluster de storage após a deteção do desastre e o failover.

Na camada de computação, quando as VMs em execução em um determinado local sofrem uma falha de host, as VMs são projetadas para serem reiniciadas automaticamente pelo recurso VMware HA. Para uma interrupção completa da computação no local, as regras de afinidade de VM/host permitem que as VMs sejam reiniciadas no local sobrevivente. No entanto, para que uma aplicação essencial aos negócios forneça serviços ininterruptos, é necessário um clustering baseado em aplicações, como o cluster de failover Microsoft ou a arquitetura de aplicações baseada em contêiner do Kubernetes, para evitar o tempo de inatividade da aplicação. Consulte o documento relevante para a implementação do clustering baseado em aplicações, que está além do âmbito deste relatório técnico.

"Próximo: Conclusão."

Conclusão

"Anterior: Validação da solução - cenários validados."

O data center FlexPod com SM-BC usa um design de data center ativo-ativo para fornecer continuidade dos negócios e recuperação de desastres para workloads essenciais aos negócios. A solução normalmente interconeta dois data centers implantados em locais separados e geograficamente dispersos em uma área metropolitana. A solução NetApp SM-BC usa replicação síncrona para proteger serviços de dados essenciais aos negócios contra falhas no local. A solução exige que os dois locais de implantação do FlexPod tenham uma latência de rede de ida e volta inferior a 10 milissegundos.

O Mediador NetApp ONTAP implantado em um terceiro local monitora a solução SM-BC e permite o failover automatizado quando um desastre no local é detetado. O VMware vCenter com VMware HA e a configuração estendida do cluster de storage VMware vSphere Metro funcionam perfeitamente com o NetApp SM-BC para permitir que a solução atenda aos objetivos de RPO zero e rto quase zero desejados.

A solução FlexPod SM-BC também pode ser implantada em infraestruturas FlexPod existentes se elas atenderem aos requisitos ou adicionando uma solução FlexPod adicional a um FlexPod existente para atingir os objetivos de continuidade dos negócios. Ferramentas adicionais de gerenciamento, monitoramento e automação, como o Cisco Intersight, Ansible e HashiCorp baseadas em Terraform, estão disponíveis no NetApp e no Cisco. Assim, você pode monitorar a solução com facilidade, obter insights sobre suas operações e automatizar a implantação e as operações.

Das perspetivas de uma aplicação essencial aos negócios, como o Microsoft SQL Server, um banco de dados que reside em um armazenamento de dados VMware protegido por uma relação CG do ONTAP SM-BC continua disponível apesar de uma interrupção no storage no local. Conforme verificado durante o teste de validação, após uma interrupção de energia do cluster de storage em que o banco de dados reside, ocorre um failover da relação CG SM-BC e as transações do Microsoft SQL Server são retomadas sem interrupção do aplicativo.

Com proteção granular de dados da aplicação, os relacionamentos de CG do ONTAP SM-BC podem ser criados para suas aplicações essenciais aos negócios a fim de atender a requisitos de RPO zero e rto quase zero. Para que o cluster VMware no qual o aplicativo Microsoft SQL Server está sendo executado possa sobreviver a uma falha no armazenamento no local, os LUNs de inicialização dos hosts ESXi em cada local também são protegidos por um relacionamento CG SM-BC.

A flexibilidade e a escalabilidade do FlexPod permitem que você comece com uma infraestrutura de tamanho certo que pode crescer e evoluir à medida que seus requisitos empresariais mudam. Esse design validado permite que você implante de forma confiável a nuvem privada baseada no VMware vSphere em uma infraestrutura distribuída e integrada, fornecendo assim uma solução resiliente a muitos cenários de ponto único de falha, bem como a falha do local para proteger serviços de dados empresariais críticos.

"Próximo: Onde encontrar informações adicionais e histórico de versões."

Onde encontrar informações adicionais e histórico de versões

"Anterior: Conclusão."

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

FlexPod

- Página inicial do FlexPod

  "https://www.flexpod.com"

- Cisco validou guias de design e implantação para FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Servidores Cisco - sistema de computação unificada (UCS)

  "https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html"

- Documentação do produto NetApp

  "https://www.netapp.com/support-and-training/documentation/"

- FlexPod Datacenter com Cisco UCS 4,2(1) no modo gerenciado UCS, VMware vSphere 7,0 U2 e NetApp ONTAP 9.9 Guia de Design

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2_design.html"

- FlexPod Datacenter com Cisco UCS 4,2(1) no modo gerenciado do UCS, VMware vSphere 7,0 U2 e Guia de implantação do NetApp ONTAP 9.9

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html"

- FlexPod Datacenter com Cisco UCS X-Series, VMware 7,0 U2 e NetApp ONTAP 9.9 Guia de Design

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

- FlexPod Datacenter com Cisco UCS X-Series, VMware 7,0 U2 e NetApp ONTAP 9.9 Guia de implantação

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmware_7u2.html"

- FlexPod Express para VMware vSphere 7,0 com o Cisco UCS Mini e o Guia de design NetApp AFF/FAS NVA

  https://www.netapp.com/pdf.html?item=/media/22621-nva-1154-DESIGN.pdf

- FlexPod Express para VMware vSphere 7,0 com o Cisco UCS Mini e o Guia de implantação do NetApp AFF/FAS NVA

  https://www.netapp.com/pdf.html?item=/media/21938-nva-1154-DEPLOY.pdf

- FlexPod MetroCluster IP com malha frontal multi-local VXLAN

  "https://www.cisco.com/c/dam/en/us/products/collateral/servers-unified-computing/flexpod-metrocluster-ip-vxlan-multi-site-wp.pdf"

- NAbox

  "https://nabox.org"

- Colheita de NetApp

  "https://github.com/NetApp/harvest/releases"

SM-BC

- SM-BC

  "https://docs.netapp.com/us-en/ontap/smbc/index.html"

- TR-4878: Continuidade de Negócios SnapMirror (SM-BC) ONTAP 9.8

https://www.netapp.com/pdf.html?item=/media/21888-tr-4878.pdf

- Como excluir corretamente um SnapMirror Relationship ONTAP 9

  "https://kb.netapp.com/Advice_and_Troubleshooting/Data_Protection_and_Security/SnapMirror/How_to_correctly_delete_a_SnapMirror_relationship_ONTAP_9"

- Noções básicas de recuperação de desastres síncronas do SnapMirror

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-synchronous-disaster-recovery-basics-concept.html"

- Noções básicas de recuperação de desastres do SnapMirror assíncrono

  "https://docs.netapp.com/us-en/ontap/data-protection/snapmirror-disaster-recovery-concept.html#data-protection-relationships"

- Proteção de dados e recuperação de desastres

  "https://docs.netapp.com/us-en/ontap/data-protection-disaster-recovery/index.html"

- Instale ou atualize o serviço do Mediador ONTAP

  "https://docs.netapp.com/us-en/ontap/mediator/index.html"

VMware vSphere HA e vSphere Metro Storage Cluster

- Criação e uso de clusters de HA do vSphere

  "https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.avail.doc/GUID-5432CA24-14F1-44E3-87FB-61D937831CF6.html"

- VMware vSphere Metro Storage Cluster (vMSC)

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-vmsc"

- Práticas recomendadas do VMware vSphere Metro Storage Cluster

  "https://core.vmware.com/resource/vmware-vsphere-metro-storage-cluster-recommended-practices"

- NetApp ONTAP com NetApp SnapMirror Business Continuity (SM-BC) com VMware vSphere Metro Storage Cluster (vMSC). (83370)

  "https://kb.vmware.com/s/article/83370"

- Proteja aplicativos e bancos de dados de camada 1 com o VMware vSphere Metro Storage Cluster e o ONTAP

  "https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-tier-1-applications-and-databases-with-VMware-vSphere-Metro-Storage/ba-p/171636"

Microsoft SQL e HammerDB

- Microsoft SQL Server 2019

"https://www.microsoft.com/en-us/sql-server/sql-server-2019"

- Arquitetando o Microsoft SQL Server no Guia de práticas recomendadas do VMware vSphere

  "https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/solutions/sql-server-on-vmware-best-practices-guide.pdf"

- HammerDB website

  "https://www.hammerdb.com"

Matriz de compatibilidade

- Matriz de compatibilidade de hardware Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Ferramenta de Matriz de interoperabilidade do NetApp

  "https://support.netapp.com/matrix/"

- NetApp Hardware Universe

  "https://hwu.netapp.com"

- Guia de compatibilidade da VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Abril de 2022	Lançamento inicial.

Data center do FlexPod com VMware vSphere 7,0, Cisco VXLAN Single-Site Fabric e NetApp ONTAP 9.7 - Desenho

Ramesh Isaac, Cisco Abhinav Singh, NetApp

Os Cisco Validated designs (CVDs) consistem em sistemas e soluções projetados, testados e documentados para facilitar e melhorar as implantações dos clientes. Esses designs incorporam uma ampla gama de tecnologias e produtos em um portfólio de soluções que foram desenvolvidas para atender às necessidades de negócios dos clientes. A Cisco e a NetApp fizeram uma parceria para fornecer o FlexPod, que serve de base para uma variedade de workloads e fornecem designs de arquitetura robustos, eficientes e dimensionáveis para atender aos requisitos do cliente. Uma solução FlexPod é uma abordagem validada para implantar tecnologias e produtos Cisco e NetApp para criar uma infraestrutura compartilhada de nuvem pública e privada.

"Data center do FlexPod com VMware vSphere 7,0, Cisco VXLAN Single-Site Fabric e NetApp ONTAP 9.7 - Desenho"

FlexPod Datacenter com VMware vSphere 7,0 e NetApp ONTAP 9 .7 - implantação

João Jorge, Cisco Sree Lakshmi Lanca, NetApp

Este documento descreve o data center Cisco e NetApp FlexPod com o NetApp ONTAP 9.7 no sistema de armazenamento all-flash NetApp AFF A400, o software unificado do Cisco UCS Manager versão 4,1(2) com processadores escaláveis Intel Xeon de segunda geração e VMware vSphere 7,0. O Cisco UCS Manager (UCSM) 4,1(2) fornece suporte consolidado do seguinte:

- Todos os modelos atuais de interconexão de tecido Cisco UCS: 6200, 6300, 6324 (Cisco UCS Mini)
- 6400
- Série 2200/2300/2400 IOM
- Cisco UCS B-Series
- Cisco UCS C-Series

Também estão incluídas as plataformas de gerenciamento Cisco Intersight e NetApp Active IQ SaaS.

O FlexPod Datacenter com NetApp ONTAP 9.7, o software unificado Cisco UCS versão(2) e o VMware vSphere 7,0 incluem uma arquitetura de data center pré-projetada e de práticas recomendadas, desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), a família de switches Cisco Nexus 9000, switches de malha multicamadas MDS 9000 e arrays de storage NetApp AFF A-Series que executam o software de gerenciamento de dados ONTAP 9.4,1.

"FlexPod Datacenter com VMware vSphere 7,0 e NetApp ONTAP 9 .7 - implantação"

Centro de dados FlexPod com Cisco Intersight e NetApp ONTAP 9 .7 - Design

John George, Cisco Scott Kovacs, NetApp

Este documento descreve a solução Cisco e NetApp FlexPod, que é uma abordagem validada para implantar as tecnologias Cisco e NetApp como infraestrutura de nuvem compartilhada. Esse design validado fornece uma estrutura para implantar o VMware vSphere, a plataforma de virtualização mais popular em data centers de classe empresarial, no FlexPod.

"Centro de dados FlexPod com Cisco Intersight e NetApp ONTAP 9 .7 - Design"

Data center FlexPod com Cisco Intersight e NetApp ONTAP 9.7 - implantação

John George, Cisco Scott Kovacs, NetApp

A tendência atual do setor no design de data center é para infraestruturas compartilhadas. Ao usar a virtualização e plataformas DE TI pré-validadas, os clientes empresariais embarcaram na jornada para a nuvem, afastando-se dos silos de aplicativos e em direção a uma infraestrutura compartilhada que pode ser implantada rapidamente, aumentando assim a agilidade e reduzindo custos. A Cisco e a NetApp fizeram uma parceria para fornecer o FlexPod, que usa os melhores componentes de rede, servidor e storage para servir de base para uma variedade de workloads, possibilitando designs de arquitetura eficientes que podem ser implantados de forma rápida e confiável.

"Data center FlexPod com Cisco Intersight e NetApp ONTAP 9.7 - implantação"

Centro de dados FlexPod com Cisco Intersight e NetApp ONTAP 9 .7 - Design

John George, Cisco Scott Kovacs, NetApp

Este documento descreve uma solução validada para implantar as tecnologias Cisco e NetApp como uma infraestrutura de nuvem compartilhada. Esse design validado fornece uma estrutura para implantar o VMware vSphere, a plataforma de virtualização mais popular em data centers de classe empresarial, no FlexPod.

O FlexPod é uma infraestrutura integrada líder que dá suporte a uma ampla variedade de workloads e casos de uso empresariais. Essa solução permite que os clientes implantem de forma rápida e confiável uma nuvem privada baseada no VMware vSphere em uma infraestrutura integrada.

"Centro de dados FlexPod com Cisco Intersight e NetApp ONTAP 9 .7 - Design"

FlexPod Datacenter com VMware vSphere 6,7 U2, Cisco UCS Fouth-Generation Fabric e NetApp ONTAP 9.6

João Jorge, Cisco Sree Lakshmi Lanca, NetApp

Este documento descreve o data center Cisco e NetApp FlexPod com o NetApp ONTAP 9.6, o software unificado do Cisco UCS Manager versão 4,0(4) com processadores escaláveis Intel Xeon de segunda geração e o VMware vSphere 6,7 U2. O Cisco UCS Manager (UCSM) 4,0(4) fornece suporte consolidado do seguinte:

- Todos os modelos atuais de interconexão de tecido Cisco UCS: 6200, 6300, 6324 (Cisco UCS Mini)
- 6454
- Série 2200/2300/2400 IOM
- Cisco UCS B-Series
- Cisco UCS C-Series.

O FlexPod Datacenter com NetApp ONTAP 9.6, o software unificado Cisco UCS versão 4,0(4) e o VMware vSphere 6,7 U2 é uma arquitetura de data center pré-projetada e de práticas recomendadas, desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), a família de switches Cisco Nexus

9000, switches de malha multicamadas MDS 9000 e arrays de storage NetApp AFF A-Series que executam o ONTAP 9.

"FlexPod Datacenter com VMware vSphere 6,7 U2, Cisco UCS quarta geração Fabric e NetApp ONTAP 9.6"

Data center FlexPod com VMware vSphere 6,7 U1, malha de quarta geração Cisco UCS e NetApp AFF A-Series - Design

João Jorge, Cisco Sree Lakshmi Lanca, NetApp

Este documento descreve a solução Cisco e NetApp FlexPod, que é uma abordagem validada para implantar as tecnologias Cisco e NetApp como infraestrutura de nuvem compartilhada. Esse design validado fornece uma estrutura para implantar o VMware vSphere, a plataforma de virtualização mais popular em data centers de classe empresarial, no FlexPod.

O FlexPod é uma infraestrutura integrada líder que dá suporte a uma ampla variedade de workloads e casos de uso empresariais. Essa solução permite que os clientes implantem de forma rápida e confiável a nuvem privada baseada no VMware vSphere em uma infraestrutura integrada.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), usando a versão unificada de software para oferecer suporte às plataformas de hardware Cisco UCS, incluindo servidores blade Cisco UCS da série B e servidores de rack da série C, interconexões de malha Cisco UCS 6454, switches Cisco da série 9000, switches de canal de fibra Cisco MDS e arrays de storage NetApp All Flash. Além disso, ele inclui o VMware vSphere 6,7 Update 1, que fornece vários novos recursos para otimizar a utilização do storage e facilitar uma nuvem privada.

"Data center FlexPod com VMware vSphere 6,7 U1, malha de quarta geração Cisco UCS e NetApp AFF A-Series - Design"

FlexPod Datacenter com VMware vSphere 6,7 U1, Cisco UCS de quarta geração e NetApp AFF A-Series

John George, Cisco Scott Kovacs, NetApp

Este documento descreve o data center Cisco e NetApp FlexPod com o software unificado do Cisco UCS Manager versão 4,0(2) e o VMware vSphere 6,7 U1. O Cisco UCS Manager (UCSM) 4,0(2) fornece suporte consolidado de todos os modelos atuais de interconexão de malha do Cisco UCS (6200, 6300, 6324 (Cisco UCS Mini)), IOM da série 6454,2200/2300, Cisco UCS B-Series e Cisco UCS C-Series. O FlexPod Datacenter com o software unificado Cisco UCS versão 4,0(2) e o VMware vSphere 6,7 U1 é uma arquitetura de data center pré-projetada e com práticas recomendadas, desenvolvida com base no sistema de computação unificada (UCS) da Cisco, a família de switches Cisco Nexus 9000, switches de malha multicamadas MDS 9000 e arrays de storage NetApp AFF A-Series que executam o sistema operacional de storage ONTAP 9.

"FlexPod Datacenter com VMware vSphere 6,7 U1, Cisco UCS de quarta geração e NetApp AFF A-Series"

FlexPod Datacenter com Cisco ACI multipod, NetApp MetroCluster IP e VMware vSphere 6,7 - Projeto

Arvind Ramakrishnan, Cisco, NetApp

Este documento descreve a integração da solução Cisco ACI Multi-Pod e NetApp MetroCluster IP no datacenter FlexPod para fornecer uma solução de multi-data center altamente disponível. A arquitetura de vários data centers oferece a capacidade de equilibrar workloads entre dois data centers que utilizam mobilidade ininterrupta de workload, permitindo assim a migração de serviços entre locais sem a necessidade de manter uma interrupção.

A solução FlexPod com multipod ACI e NetApp MetroCluster IP oferece os seguintes benefícios:

- Mobilidade otimizada de workload entre data centers
- Políticas consistentes em todos os sites
- Extensão da camada 2 em data centers geograficamente dispersos
- Evitar tempo de inatividade melhorado durante a manutenção
- Prevenção e recuperação de desastres

"FlexPod Datacenter com Cisco ACI multipod, NetApp MetroCluster IP e VMware vSphere 6,7 - Projeto"

FlexPod Datacenter com Cisco ACI multipod com NetApp MetroCluster IP e VMware vSphere 6,7 - implantação

Cisco, Cisco Ramesh Issac, Ramesh Issac, Ramakrishnan, NetApp

A Cisco e a NetApp fizeram uma parceria para fornecer uma série de soluções FlexPod que permitem plataformas estratégicas de data center. A solução FlexPod oferece uma arquitetura integrada que incorpora as melhores práticas de design para computação, armazenamento e rede, minimizando assim os riscos DE TI validando a arquitetura integrada para garantir a compatibilidade entre vários componentes. A solução também aborda os pontos problemáticos DA TI, fornecendo orientação de projeto documentada, orientação de implantação e suporte que podem ser usados em várias etapas (Planejamento, projeto e implementação) de uma implantação.

"FlexPod Datacenter com Cisco ACI multipod com NetApp MetroCluster IP e VMware vSphere 6,7 - implantação"

Nuvem híbrida

Nuvem híbrida da FlexPod com Cloud Volumes ONTAP para Epic

TR-4960: Nuvem híbrida da FlexPod com Cloud Volumes ONTAP para Epic

Em parceria com: 

Kamini Singh, NetApp

A chave para fazer uma transformação digital é simplesmente fazer mais com os dados. Os hospitais geram e exigem grandes quantidades de dados para executar sua organização e atender seus pacientes com eficiência. As informações são coletadas e processadas ao tratar pacientes e gerenciar horários e recursos médicos da equipe.

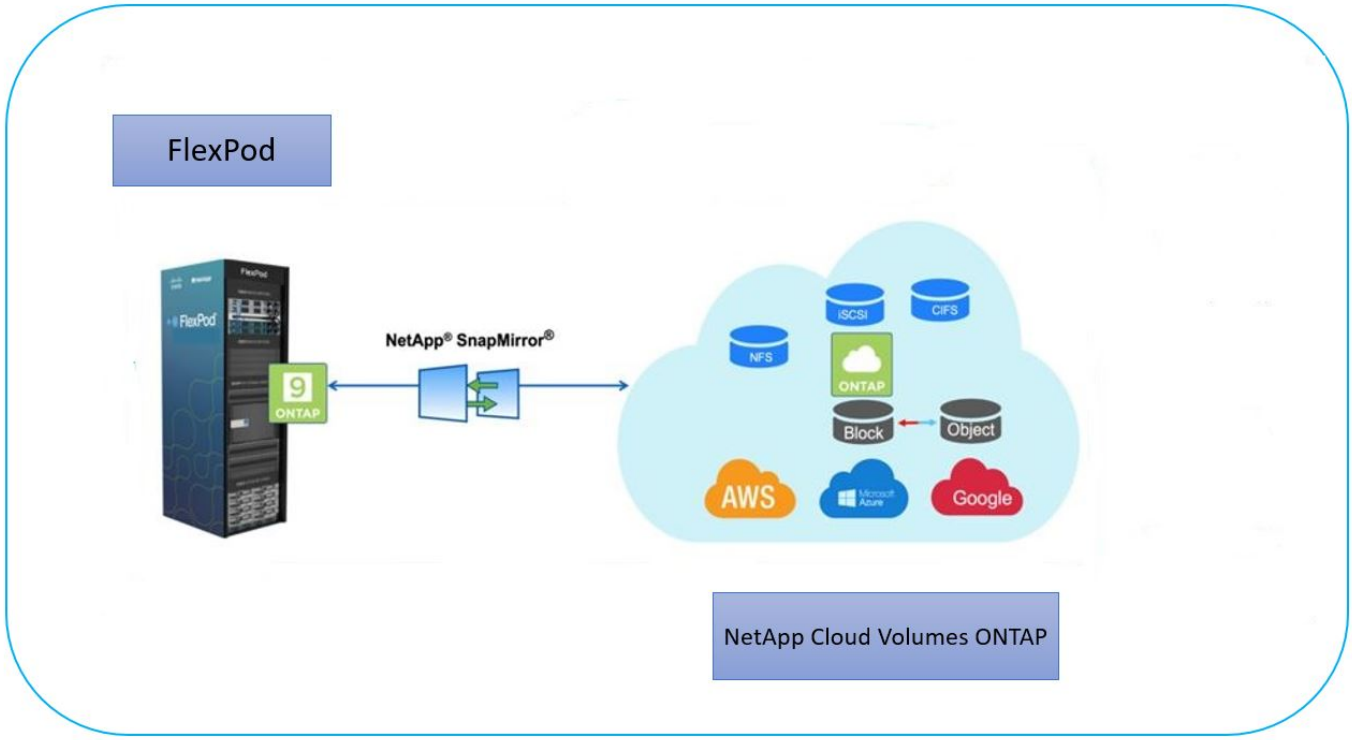
O tamanho cada vez maior dos dados de saúde e os insights valiosos que esses dados podem fornecer tornam os serviços de dados de saúde e a proteção de dados críticos e desafiadores. Primeiro, os dados de serviços de saúde precisam estar disponíveis e protegidos para atender aos requisitos de recuperação, continuidade dos negócios médicos ou conformidade.

Em segundo lugar, os dados de saúde devem estar prontamente disponíveis para análise. Muitas vezes, essa análise usa abordagens baseadas em inteligência artificial (IA) e aprendizado de máquina (ML) para ajudar as empresas médicas a melhorar suas soluções e criar valores de negócios.

Terceiro, as infraestruturas de serviço de dados e as metodologias de proteção de dados precisam acomodar o crescimento dos dados de saúde à medida que os negócios médicos crescem. Além disso, a mobilidade de dados está se tornando cada vez mais crítica devido à necessidade de migrar dados da borda para o centro e a nuvem para usar os recursos disponíveis lá para análise ou arquivamento de dados.

A NetApp oferece uma solução única de gerenciamento de dados para aplicações empresariais, incluindo saúde, e podemos orientar hospitais em sua jornada rumo à transformação digital. O NetApp Cloud Volumes ONTAP oferece uma solução para gerenciamento de dados de saúde no qual os dados podem ser replicados com eficiência de um data center FlexPod para o Cloud Volumes ONTAP implantado em nuvem pública, como a AWS.

Ao utilizar recursos de nuvem pública seguros e econômicos, o Cloud Volumes ONTAP aprimora a recuperação de desastres (DR) baseada na nuvem com replicação de dados altamente eficiente, eficiência de storage incorporada e testes simples de recuperação de desastres. Esses sistemas são gerenciados com controle unificado e simplicidade de arrastar e soltar, o que fornece proteção econômica e à prova de balas contra qualquer tipo de erro, falha ou desastre. A Cloud Volumes ONTAP fornece a tecnologia NetApp SnapMirror como solução para replicação de dados em nível de bloco que mantém o destino atualizado por meio de atualizações incrementais.



Público-alvo

Este documento destina-se aos engenheiros de soluções de parceiros (ses) e da NetApp e ao pessoal de serviços profissionais. O NetApp assume que o leitor tem os seguintes conhecimentos:

- Uma sólida compreensão dos conceitos de SAN e nas
- Familiaridade técnica com os sistemas de storage da NetApp ONTAP
- Familiaridade técnica com a configuração e administração do software ONTAP

Benefícios da solução

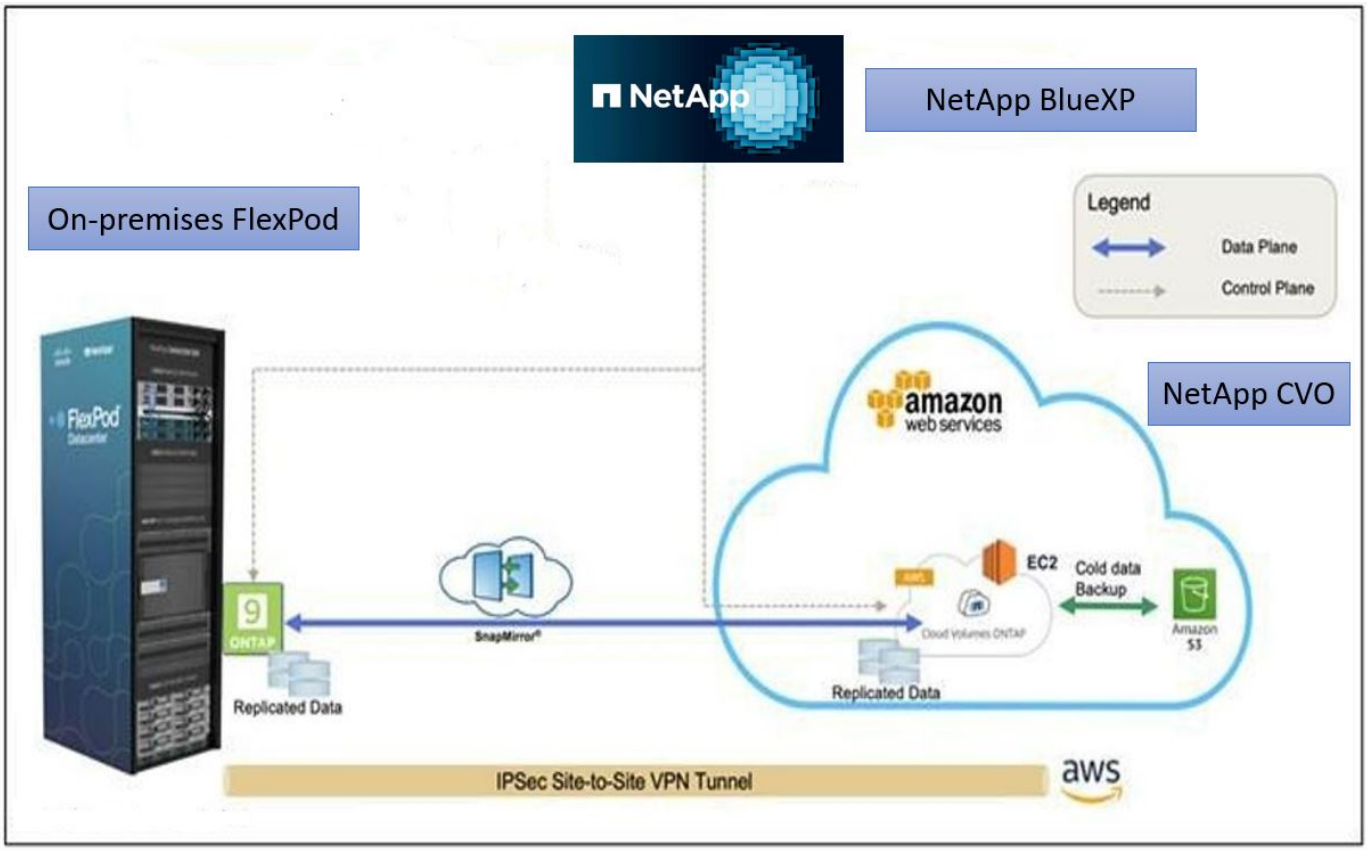
O data center FlexPod integrado ao NetApp Cloud Volumes ONTAP oferece os seguintes benefícios para os workloads do setor de saúde:

- * Proteção personalizada. * O Cloud Volumes ONTAP fornece replicação de dados em nível de bloco da ONTAP para a nuvem, o que mantém o destino atualizado por meio de atualizações incrementais. Os usuários podem especificar uma programação de sincronização para determinar quando as alterações na origem são transferidas. Isso fornece proteção personalizada para todos os tipos de dados de saúde.
- **Failover e failback.** Quando ocorre um desastre, os administradores de storage podem definir rapidamente o failover para os volumes de nuvem. Quando o local principal é recuperado, os novos dados criados no ambiente de DR são sincronizados de volta para os volumes de origem, permitindo que a replicação de dados secundários seja restabelecida. Dessa forma, os dados de saúde podem ser facilmente recuperados sem interrupções.
- **Eficiência.** O espaço de storage e os custos da cópia de nuvem secundária são otimizados usando compressão de dados, thin Provisioning e deduplicação. Os dados de saúde são transferidos no nível do bloco de forma comprimida e desduplicada, melhorando a velocidade das transferências. Os dados também são automaticamente dispostos em camadas em storage de objetos de baixo custo e somente retornados ao storage de alto desempenho quando acessados, como em um cenário de DR. Isso reduz significativamente os custos contínuos de storage.

- **Proteção contra ransomware.** A proteção contra ransomware do NetApp BlueXP verifica fontes de dados em ambientes locais e na nuvem, detecta vulnerabilidades de segurança e fornece seu status de segurança atual e sua pontuação de riscos. Em seguida, ele fornece recomendações práticas que você pode investigar e seguir para corrigir. Dessa forma, você pode proteger os dados essenciais de saúde contra ataques de ransomware.

Topologia da solução

Esta seção descreve a topologia lógica da solução. A figura a seguir representa a topologia da solução composta pelo ambiente FlexPod on-premises, pelo NetApp Cloud Volumes ONTAP (CVO) executado no Amazon Web Services (AWS) e pela plataforma SaaS NetApp BlueXP .



Os planos de controlo e os planos de dados são claramente indicados entre os pontos finais. O plano de dados é executado entre a instância do ONTAP em execução no FAS all-flash no FlexPod e a instância do NetApp CVO na AWS, aproveitando uma conexão VPN local a local segura. A replicação dos dados de workloads do setor de saúde do data center FlexPod no local para o NetApp Cloud Volumes ONTAP é gerenciada pela replicação do NetApp SnapMirror. Essa solução também oferece suporte a essa solução para fazer backup e disposição em camadas opcionais dos dados inativos que residem na instância do NetApp CVO no AWS S3.

"Próximo: Componentes da solução."

Componentes da solução

"Anterior: Visão geral da solução."

FlexPod

O FlexPod é um conjunto definido de hardware e software que forma uma base integrada para soluções virtualizadas e não virtualizadas. O FlexPod inclui storage NetApp ONTAP, rede Cisco Nexus, rede de storage Cisco MDS e o sistema de computação unificada da Cisco (Cisco UCS).

As organizações de saúde estão procurando uma solução para facilitar a transformação digital e melhorar as experiências e os resultados dos pacientes. Com o FlexPod, você tem uma plataforma segura e dimensionável que impulsiona a eficiência e capacita sua equipe a tomar decisões mais informadas com mais rapidez, para que possam fornecer um melhor atendimento ao paciente.

O FlexPod é a plataforma ideal para as necessidades de workload do setor de saúde, pois oferece os seguintes benefícios:

- Otimização das operações para obter insights mais rápidos e melhores resultados para os pacientes.
- Simplificação de aplicativos de geração de imagens com infraestrutura dimensionável e confiável.
- Implantação rápida e eficiente com uma abordagem comprovada para aplicativos específicos de saúde, como EHR.

EHR

O Electronic Health Records (EHRs) faz software para grupos médicos de médio e grande porte, hospitais e organizações de saúde integradas. Os clientes também incluem hospitais comunitários, instalações acadêmicas, organizações infantis, provedores de redes de segurança e sistemas multi-hospitalares. O software integrado à EHR abrange funções clínicas, de acesso e de receita e estende-se para a casa.

As organizações de provedores de saúde permanecem sob pressão para maximizar os benefícios de seus investimentos substanciais em EHRs líderes do setor. Quando os clientes projetam seus data centers para soluções EHR e aplicações de missão crítica, eles geralmente identificam os seguintes objetivos para a arquitetura do data center:

- Alta disponibilidade das aplicações EHR
- Alto desempenho
- Facilidade de implementação de EHR no data center
- Agilidade e escalabilidade para permitir o crescimento com novas versões ou aplicações de EHR
- Custo-benefício
- Capacidade de gerenciamento, estabilidade e facilidade de suporte
- Proteção de dados, backup, recuperação e continuidade dos negócios robustos

O FlexPod é validado pela EHR e oferece suporte a uma plataforma que contém Cisco Cisco UCS com processadores Intel Xeon, Red Hat Enterprise Linux (RHEL) e virtualização com o VMware ESXi. Essa plataforma, combinada à classificação de alto nível de conforto da EHR para storage NetApp executando ONTAP, dá aos clientes a confiança de executar suas aplicações de saúde em uma nuvem privada totalmente gerenciada por meio do FlexPod, que também pode ser conectada a qualquer um dos fornecedores de nuvem pública.

NetApp BlueXP

O BlueXP (anteriormente NetApp Cloud Manager) é uma plataforma de gerenciamento baseada em SaaS de classe empresarial que permite que especialistas DE TI e arquitetos de nuvem gerenciem centralmente sua infraestrutura híbrida de várias nuvens usando as soluções de nuvem da NetApp. Ele fornece um sistema

centralizado para visualização e gerenciamento do storage de nuvem e no local, com suporte a contas e fornecedores de nuvem híbrida. Para obter mais informações, "BlueXP"consulte .

Conetor

Uma instância do Connector permite que o BlueXP gerencie recursos e processos em um ambiente de nuvem pública. O conetor é necessário para muitos dos recursos fornecidos pelo BlueXP e pode ser implantado na nuvem ou na rede local.

O conetor é suportado nos seguintes locais:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- No local

Para saber mais sobre o conetor, consulte o "Página do conetor".

NetApp Cloud Volumes ONTAP

O NetApp Cloud Volumes ONTAP é uma oferta de storage definido por software que executa o software de gerenciamento de dados ONTAP na nuvem para fornecer gerenciamento avançado de dados para workloads de arquivo e bloco. Com o Cloud Volumes ONTAP, você pode otimizar seus custos de storage de nuvem e aumentar a performance das aplicações, além de aprimorar a proteção, a segurança e a conformidade dos dados.

Os principais benefícios incluem o seguinte:

- * Eficiências de armazenamento.* Utilize deduplicação de dados incorporada, compressão, thin Provisioning e clonagem instantânea para minimizar custos de storage.
- **Alta disponibilidade.** Fornecer confiabilidade empresarial e operações contínuas em caso de falhas no seu ambiente de nuvem.
- **Proteção de dados.** A Cloud Volumes ONTAP usa o SnapMirror, a tecnologia de replicação NetApp líder do setor, para replicar dados no local para a nuvem, facilitando a disponibilização de cópias secundárias para vários casos de uso. O Cloud Volumes ONTAP também se integra ao Cloud Backup para fornecer recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de nuvem.
- **Disposição em camadas de dados.** Alterne entre pools de armazenamento de alto e baixo desempenho sob demanda sem colocar os aplicativos offline.
- **Consistência da aplicação.** Fornecer a consistência das cópias NetApp Snapshot usando a tecnologia NetApp SnapCenter.
- **Segurança de dados.** O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.
- **Controles de conformidade de privacidade.** A integração com o Cloud Data Sense ajuda você a entender o contexto dos dados e identificar dados confidenciais.

Para obter informações mais detalhadas, "Cloud Volumes ONTAP"consulte .

NetApp Active IQ Unified Manager

O NetApp Active IQ Unified Manager permite o monitoramento dos clusters de storage do ONTAP a partir de uma interface única, reprojetada e intuitiva que fornece inteligência do conhecimento da comunidade e

análises de AI. Ele fornece insights abrangentes operacionais, de performance e proativos sobre o ambiente de storage e as máquinas virtuais que nele são executadas. Quando ocorre um problema com a infraestrutura de storage, o Unified Manager pode notificá-lo sobre os detalhes do problema para ajudar a identificar a causa raiz. O painel da máquina virtual fornece uma visão das estatísticas de desempenho da VM para que você possa investigar todo o caminho de e/S do host vSphere até a rede e, finalmente, até o armazenamento.

Alguns eventos também fornecem ações corretivas que podem ser tomadas para corrigir o problema. Você pode configurar alertas personalizados para eventos para que, quando os problemas ocorrem, você seja notificado por meio de traps de e-mail e SNMP. O Active IQ Unified Manager permite que você se Planeje para os requisitos de storage de seus usuários prevendo tendências de capacidade e uso para que você possa agir antes que surjam problemas, evitando decisões reativas a curto prazo que podem levar a problemas adicionais a longo prazo.

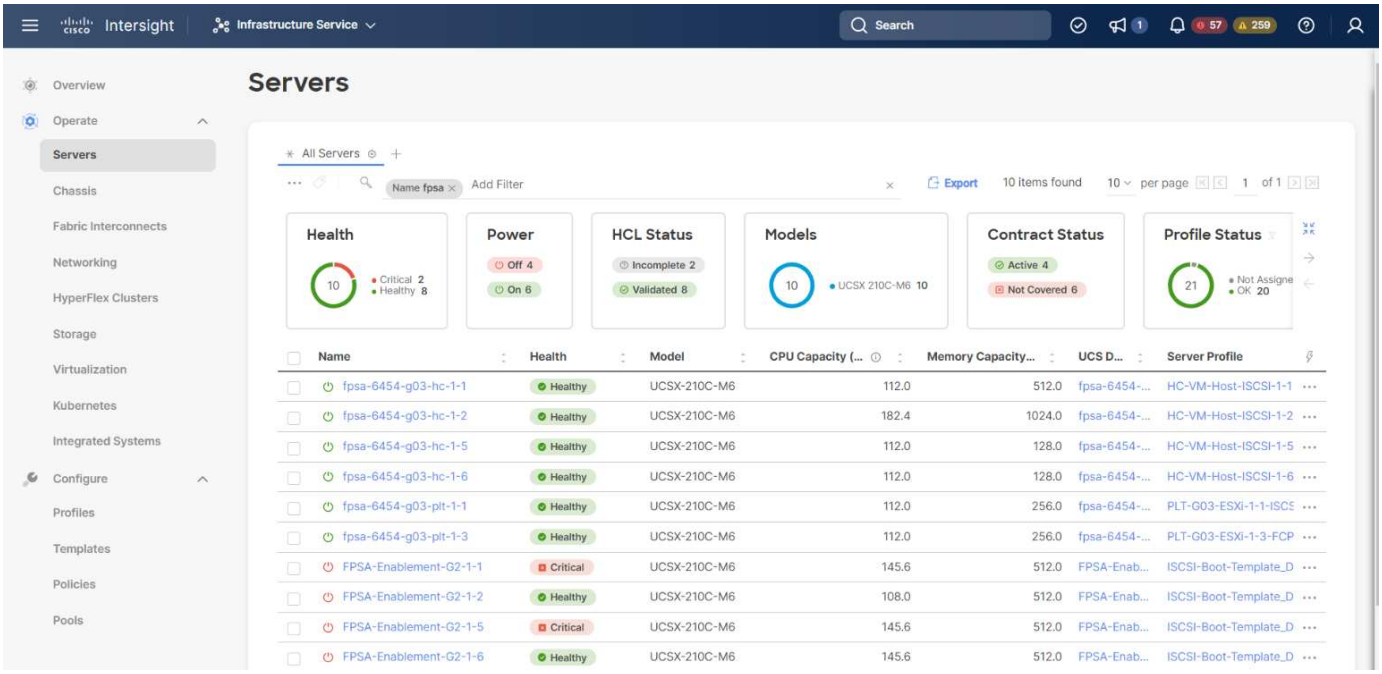
Para obter mais informações, "Active IQ Unified Manager"consulte .

Cisco Intersight

O Cisco Intersight é uma plataforma SaaS que oferece automação, observabilidade e otimização inteligentes para aplicações e infraestrutura tradicionais e nativas da nuvem. A plataforma ajuda a impulsionar a mudança com as equipes DE TI e fornece um modelo operacional projetado para a nuvem híbrida. O Cisco Intersight oferece os seguintes benefícios:

- * Entrega mais rápida. * O Intersight é fornecido como um serviço da nuvem ou no data center do cliente com atualizações frequentes e inovação contínua, devido a um modelo de desenvolvimento de software baseado em agilidade. Dessa forma, o cliente pode se concentrar no suporte às necessidades críticas dos negócios.
- **Operações simplificadas.** O Intersight simplifica as operações usando uma única ferramenta segura fornecida por SaaS com inventário, autenticação e APIs comuns para trabalhar em toda a stack e em todos os locais, eliminando silos entre as equipes. Isso permite gerenciar servidores físicos e hipervisores no local, para VMs, K8s, sem servidor, automação, otimização e controle de custos tanto no local quanto em nuvens públicas.
- **Otimização contínua.** Você pode otimizar seu ambiente continuamente usando a inteligência fornecida pelo Cisco Intersight em todas as camadas, bem como pelo Cisco TAC. Essa inteligência é convertida em ações recomendadas e automatizáveis para que você possa se adaptar em tempo real a qualquer alteração: Da movimentação de cargas de trabalho e monitoramento da integridade dos servidores físicos até recomendações de redução de custos para as nuvens públicas com as quais você trabalha.

Existem dois modos de operações de gerenciamento possíveis com o Cisco Intersight: O modo gerenciado de UMM e o modo gerenciado de Intersight (IMM). Você pode selecionar o modo gerenciado UCSM nativo (UMM) ou o modo gerenciado Intersight (IMM) para sistemas Cisco UCS conectados à malha durante a configuração inicial das interconexões de malha. Nesta solução, IMM nativo é usado. A figura a seguir mostra o Painel de Controle Intersight do Cisco.



VMware vSphere 7,0

O VMware vSphere é uma plataforma de virtualização para gerenciar holisticamente grandes coleções de infraestrutura (incluindo CPUs, armazenamento e rede) como um ambiente operacional otimizado, versátil e dinâmico. Ao contrário dos sistemas operacionais tradicionais que gerenciam uma máquina individual, o VMware vSphere agrega a infraestrutura de um datacenter inteiro para criar uma única potência com recursos que podem ser alocados de forma rápida e dinâmica para qualquer aplicativo necessário.

Para obter mais informações sobre o VMware vSphere e seus componentes, "VMware vSphere" consulte .

VMware vCenter Server

O VMware vCenter Server fornece gerenciamento unificado de todos os hosts e VMs a partir de um único console e agrega o monitoramento de desempenho de clusters, hosts e VMs. O VMware vCenter Server oferece aos administradores uma visão profunda sobre o status e a configuração de clusters de computação, hosts, VMs, armazenamento, SO convidado e outros componentes críticos de uma infraestrutura virtual. O VMware vCenter gerencia o rico conjunto de recursos disponíveis em um ambiente VMware vSphere.

Para obter informações detalhadas, "VMware vCenter"consulte .

Revisões de hardware e software

Essa solução de nuvem híbrida pode ser estendida a qualquer ambiente FlexPod que esteja executando versões compatíveis de software, firmware e hardware, conforme definido nas "Ferramenta de Matriz de interoperabilidade do NetApp" , "Compatibilidade de hardware e software do UCS" e "Guia de compatibilidade da VMware".

A tabela a seguir mostra as revisões de hardware e software do FlexPod no local.

Componente	Produto	Versão
Computação	Cisco UCS X210c M6	5,0 mm (1b mm)

Componente	Produto	Versão
	O tecido Cisco UCS interconeta 6454	4,2 mm (2a mm)
Rede	Cisco Nexus 9336C-FX2P NX-os	9,3 mm (9 mm)
Armazenamento	NetApp AFF A400	ONTAP 9.11.1P2
	Ferramentas do NetApp ONTAP para VMware vSphere	9,11
	Plug-in NFS do NetApp para VMware VAAI	2,0
	NetApp Active IQ Unified Manager	9.11P1
Software	VMware vSphere	7,0 MM (U3 MM)
	Driver Ethernet nenic do VMware ESXi	1.0.35.0
	Dispositivo VMware vCenter	7.0.3
	Dispositivo virtual de assistência à monitorização da distância da Cisco	1,0.9-342

A tabela a seguir mostra as versões NetApp BlueXP e Cloud Volumes ONTAP.

Fornecedor	Produto	Versão
NetApp	BlueXP	3.9.24
	Cloud Volumes ONTAP	ONTAP 9,11

"Próximo: Instalação e configuração."

Instalação e configuração

"Anterior: Componentes da solução."

Implantação de NetApp Cloud Volumes ONTAP

Execute as seguintes etapas para configurar sua instância do Cloud Volumes ONTAP:

1. Preparar o ambiente do fornecedor de serviços de nuvem pública.

   Você precisa capturar os detalhes do ambiente do seu provedor de serviços de nuvem pública para a configuração da solução. Por exemplo, para a preparação de ambiente do Amazon Web Services (AWS), você precisa da chave de acesso da AWS, da chave secreta da AWS e de outros detalhes de rede, como região, VPC, sub-rede, etc.

2. Configure o gateway de endpoint da VPC.

   Um gateway de endpoint VPC é necessário para habilitar a conexão entre a VPC e o serviço AWS S3. Isso é usado para ativar o backup no CVO, um endpoint com o tipo Gateway.

3. Acesse o NetApp BlueXP .

   Para acessar o NetApp BlueXP e outros serviços de nuvem, você precisa se inscrever "NetApp BlueXP" no . Para configurar espaços de trabalho e usuários na conta do BlueXP , clique "aqui"em . Você precisa de uma conta que tenha permissão para implantar o conetor no seu provedor de nuvem diretamente da BlueXP . Pode transferir a política BlueXP a partir de "aqui".

4. Implante o conetor.

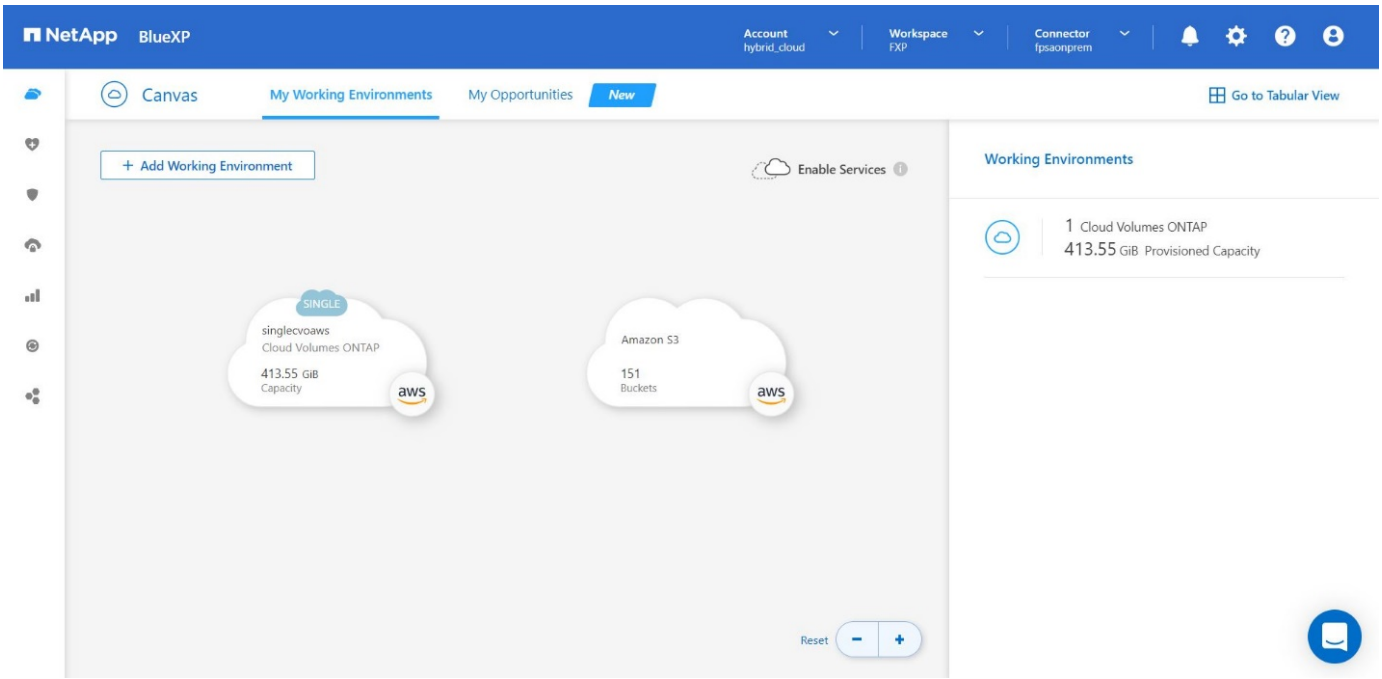
   Antes de adicionar um ambiente de trabalho Cloud volume ONTAP, você deve implantar o Connector. O BlueXP solicita se você tentar criar seu primeiro ambiente de trabalho do Cloud Volumes ONTAP sem o conetor no lugar. Para implantar o Connector no AWS a partir do BlueXP , consulte "link"este .

5. Inicie o Cloud Volumes ONTAP na AWS.

   É possível iniciar o Cloud Volumes ONTAP em uma configuração de sistema único ou como par de HA na AWS. "Leia as instruções passo a passo".

   Para obter informações detalhadas sobre essas etapas, consulte o "Guia de início rápido para Cloud Volumes ONTAP na AWS".

   Nessa solução, implantamos um sistema Cloud Volumes ONTAP de nó único na AWS. A figura a seguir mostra o Dashboard do NetApp BlueXP com instância CVO de nó único.



Implantação do FlexPod no local

Para entender os detalhes de design do FlexPod com UCS X-Series, VMware e NetApp ONTAP, consulte o "Data center FlexPod com Cisco UCS X-Series" guia de design. Este documento fornece orientações de design para incorporar a plataforma UCS X-Series gerenciada pelo Cisco Intersight na infraestrutura de datacenter do FlexPod.

Para implantar a instância do FlexPod no local, "este guia de implantação" consulte .

Este documento fornece orientações de implantação para incorporar a plataforma UCS X-Series gerenciada

pelo Cisco Intersight em uma infraestrutura de datacenter do FlexPod. O documento abrange as configurações e as práticas recomendadas para uma implantação bem-sucedida.

O FlexPod pode ser implantado no modo gerenciado UCS e no modo gerenciado de Intersight Cisco (IMM). Se você estiver implantando o FlexPod no modo gerenciado do UCS, consulte este "guia de design" e "guia de implantação" este .

A implantação do FlexPod pode ser automatizada com o uso do Ansible. Abaixo estão os links para os repositórios do GitHub para implantação do FlexPod de ponta a ponta:

- É possível ver a configuração do FlexPod com o Cisco UCS no modo gerenciado UCS, no NetApp ONTAP e no VMware vSphere "aqui".
- É possível ver a configuração do FlexPod com o Cisco UCS no IMM, NetApp ONTAP e VMware vSphere "aqui" .

Configuração de storage ONTAP no local

Esta seção descreve algumas das etapas importantes de configuração do ONTAP que são específicas a esta solução.

1. Configurar um SVM com o serviço iSCSI em execução.

```
1. vserver create -vserver Healthcare_SVM -rootvolume
Healthcare_SVM_root -aggregate aggr1_A400_G0312_01 -rootvolume-security-
style unix
2. vserver add-protocols -vserver Healthcare_SVM -protocols iscsi
3. vserver iscsi create -vserver Healthcare_SVM

   To verify:

   A400-G0312::> vserver iscsi show -vserver Healthcare_SVM
   Vserver: Healthcare_SVM
   Target Name:
   iqn.1992-08.com.netapp:sn.1fbf00f438c111ed866cd039ea91fb56:vs.3
   Target Alias: Healthcare_SVM
   Administrative Status: up
```

   Se a licença iSCSI não tiver sido instalada durante a configuração do cluster, certifique-se de que instala a licença antes de criar o serviço iSCSI.

2. Crie um FlexVol volume.

```
1. volume create -vserver Healthcare_SVM -volume hc_iscsi_vol -aggregate
aggr1_A400_G0312_01 -size 500GB -state online -policy default -space
guarantee none
```

3. Adicione interfaces para acesso iSCSI.

```
1. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01a
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node01-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> -status-admin up
2. network interface create -vserver Healthcare_SVM -lif iscsi-lif-01b
-service-policy default-data-iscsi -home-node <st-node01> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node01-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
3. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02a
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-a-vlan-id> -address <st-node02-infra-iscsi-a-ip>
-netmask <infra-iscsi-a-mask> –status-admin up
4. network interface create -vserver Healthcare_SVM -lif iscsi-lif-02b
-service-policy default-data-iscsi -home-node <st-node02> -home-port
a0a-<infra-iscsi-b-vlan-id> -address <st-node02-infra-iscsi-b-ip>
-netmask <infra-iscsi-b-mask> –status-admin up
```

Nesta solução, criamos quatro interfaces lógicas iSCSI (LIFs), duas em cada nó.

Depois que a instância do FlexPod estiver ativa e em execução com o vCenter implantado e todos os hosts ESXi adicionados a ela, precisamos implantar uma VM Linux que funcione como um servidor que se coneta e acessa o armazenamento do NetApp ONTAP. Nesta solução, instalamos uma instância do CentOS 8 no vCenter.

4. Crie um LUN.

```
1. lun create -vserver Healthcare_SVM -path /vol/hc_iscsi_vol/iscsi_lun1
-size 200GB -ostype linux -space-reserve disabled
```

Para um banco de dados operacional EHR (ODB), um diário e cargas de trabalho de aplicações, a EHR recomenda apresentar o storage aos servidores como iSCSI LUNs. O NetApp também é compatível com o uso de FCP e NVMe/FC se você tiver versões do AIX e dos sistemas operacionais RHEL capazes, o que aumenta a performance. FCP e NVMe/FC podem coexistir na mesma malha.

5. Crie um grupo.

```
1. igroup create –vserver Healthcare_SVM –igroup ehr –protocol iscsi
–ostype linux –initiator iqn.1994-05.com.redhat:8e91e9769336
```

Igroups são usados para permitir o acesso do servidor a LUNs. Para o host Linux, o servidor IQN pode ser encontrado no arquivo `/etc/iscsi/initiatorname.iscsi`.

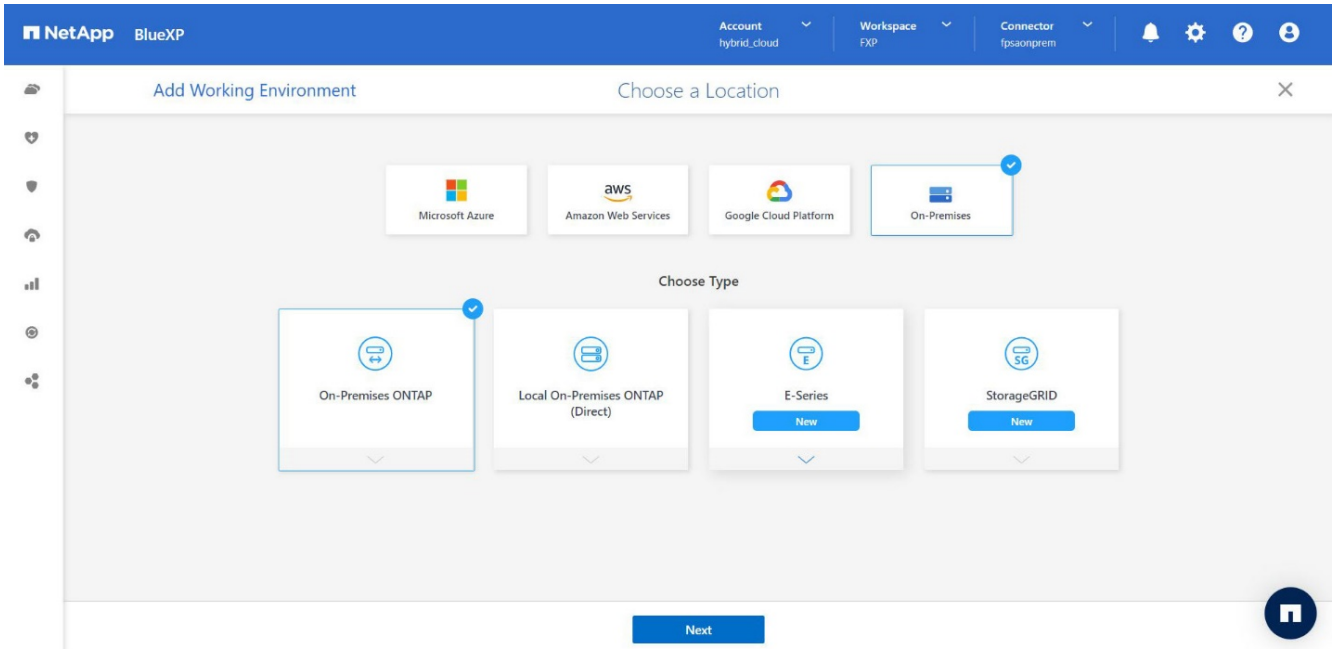
6. Mapeie o LUN para o grupo.

```
1. lun mapping create -vserver Healthcare_SVM -path
/vol/hc_iscsi_vol/iscsi_lun1 -igroup ehr -lun-id 0
```

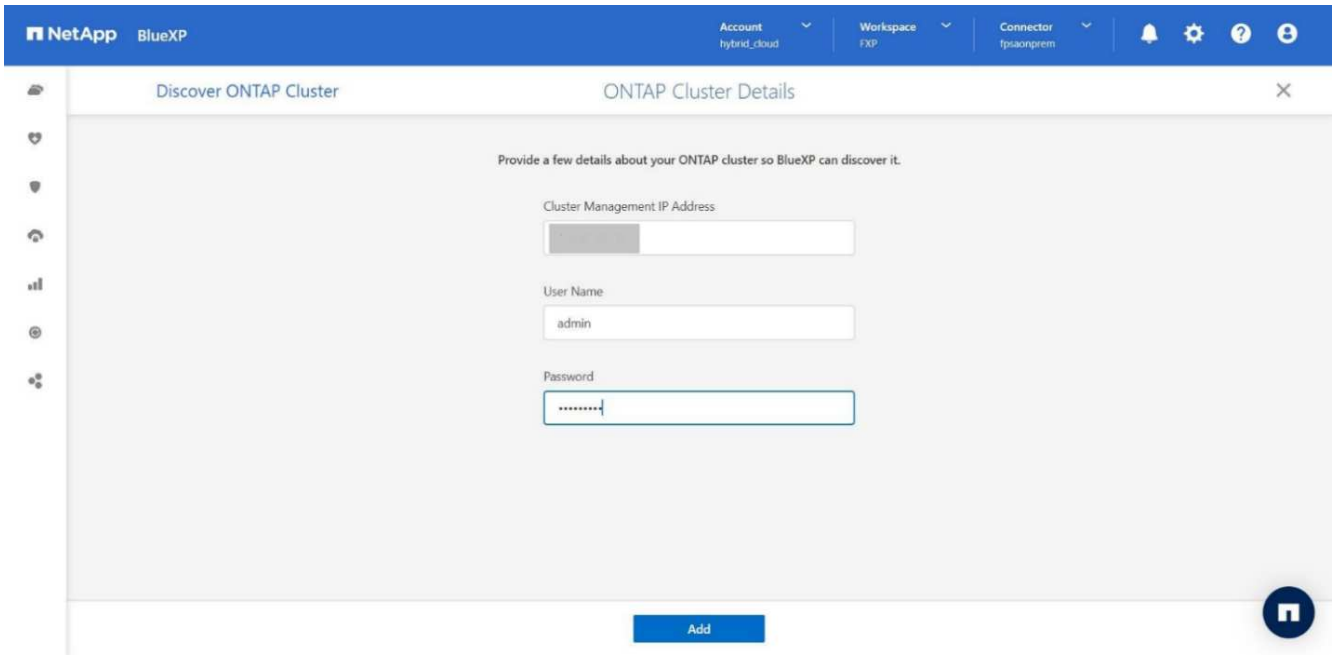
Adicione storage FlexPod no local ao BlueXP

Siga as etapas a seguir para adicionar seu storage FlexPod ao ambiente de trabalho usando o NetApp BlueXP .

1. No menu de navegação, selecione **Storage** > **Canvas**.
2. Na página Canvas, clique em **Adicionar ambiente de trabalho** e selecione **no local**.
3. Selecione **ONTAP on-premises**. Clique em **seguinte**.

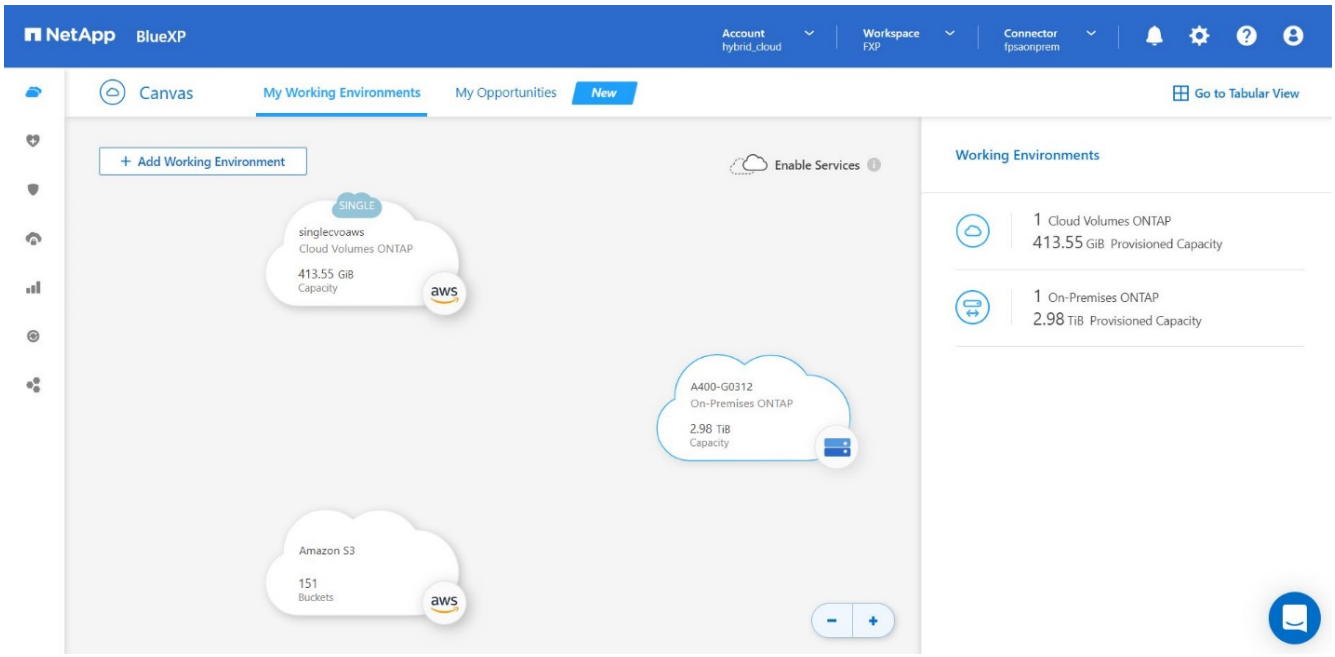


4. Na página Detalhes do cluster do ONTAP, insira o endereço IP de gerenciamento do cluster e a senha da conta de usuário do administrador. Em seguida, clique em **Add**.



5. Na página Detalhes e credenciais, insira um nome e uma descrição para o ambiente de trabalho e clique em **Go**.

   BlueXP descobre o cluster do ONTAP e o adiciona como um ambiente de trabalho no Canvas.



Para obter informações detalhadas, consulte a página "Descubra clusters ONTAP no local".

"Próximo: Configuração DE SAN."

Configuração SAN

"Anterior: Instalação e configuração."

Esta seção descreve a configuração do lado do host necessária pela EHR para permitir

que o software se integre melhor com o armazenamento NetApp. Neste segmento, discutimos especificamente a integração de host para sistemas operacionais Linux. Utilize o "Ferramenta de Matriz de interoperabilidade NetApp (IMT)" para validar todas as versões de software e firmware.

As etapas de configuração a seguir são específicas para o host CentOS 8 que foi usado nesta solução.

Kit de utilitário de host NetApp

A NetApp recomenda a instalação do kit de utilitário de host NetApp (Utilitários de host) nos sistemas operacionais de hosts que estão conetados e acessando sistemas de storage da NetApp. O MPIO (Microsoft Multipath I/o) nativo é suportado. O sistema operacional deve ser capaz de acesso a unidade lógica assimétrica (ALUA) para multipathing. A instalação dos Utilitários do host configura as configurações do adaptador de barramento do host (HBA) para armazenamento NetApp.

Os utilitários de host do NetApp podem ser baixados "aqui". Nesta solução, instalamos o Linux Host Utilities 7,1 no host.

```
[root@hc-cloud-secure-1 ~]# rpm -ivh netapp_linux_unified_host_utilities-
7-1.x86_64.rpm
```

Descubra o armazenamento ONTAP

Certifique-se de que o serviço iSCSI está em execução quando os logs devem ocorrer. Para definir o modo de login para um portal específico em um destino ou para todos os portais em um destino, use o `iscsiadm` comando.

```
[root@hc-cloud-secure-1 ~]# rescan-scsi-bus.sh
[root@hc-cloud-secure-1 ~]# iscsiadm -m discovery -t sendtargets -p
<iscsi-lif-ip>
[root@hc-cloud-secure-1 ~]# iscsiadm -m node -L all
```

Agora você pode usar `sanlun` para exibir informações sobre os LUNs conetados ao host. Certifique-se de que você está logado como root no host.

```
[root@hc-cloud-secure-1 ~]# sanlun lun show
controller(7mode/E-Series)/
                                      device    host              lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
---
Healthcare_SVM                        /dev/sdb host33  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1

Healthcare_SVM                        /dev/sdc host34  iSCSI    200g
cDOT
                       /vol/hc_iscsi_vol/iscsi_lun1
```

Configurar multipathing

O Mapper Multipathing (DM-Multipath) é um utilitário nativo de multipathing no Linux. Pode ser usado para redundância e para melhorar o desempenho. Ele agrega ou combina vários caminhos de e/S entre servidores e storage, criando um único dispositivo no nível do sistema operacional.

1. Antes de configurar o DM-Multipath no seu sistema, certifique-se de que o seu sistema foi atualizado e inclui o `device-mapper-multipath` pacote.

```
[root@hc-cloud-secure-1 ~]# rpm -qa|grep multipath
device-mapper-multipath-libs-0.8.4-31.el8.x86_64
device-mapper-multipath-0.8.4-31.el8.x86_64
```

2. O arquivo de configuração é o `/etc/multipath.conf` arquivo. Atualize o ficheiro de configuração conforme ilustrado abaixo.

```
[root@hc-cloud-secure-1 ~]# cat /etc/multipath.conf
defaults {
   path_checker      readsector0
   no_path_retry      fail
}
devices {
   device {
      vendor         "NETAPP  "
      product         "LUN.*"
      no_path_retry     queue
      path_checker      tur
   }
}
```

3. Ative e inicie os serviços multipath.

```
[root@hc-cloud-secure-1 ~]# systemctl enable multipathd.service
[root@hc-cloud-secure-1 ~]# systemctl start  multipathd.service
```

4. Adicione o módulo do kernel carregável `dm-multipath` e reinicie o serviço multipath. Finalmente, verifique o status de multipathing.

```
[root@hc-cloud-secure-1 ~]# modprobe -v dm-multipath
insmod /lib/modules/4.18.0-408.el8.x86_64/kernel/drivers/md/dm-
multipath.ko.xz

[root@hc-cloud-secure-1 ~]# systemctl restart multipathd.service

[root@hc-cloud-secure-1 ~]# multipath -ll
3600a09803831494c372b545a4d786278 dm-2 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1
alua' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| `- 33:0:0:0 sdb 8:16 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
`- 34:0:0:0 sdc 8:32 active ready running
```

Para obter informações detalhadas sobre essas etapas, "aqui" consulte .

Criar volume físico

Use o `pvcreate` comando para inicializar um dispositivo de bloco a ser usado como um volume físico. A inicialização é análoga à formatação de um sistema de arquivos.

```
[root@hc-cloud-secure-1 ~]# pvcreate /dev/sdb
Physical volume "/dev/sdb" successfully created.
```

Criar grupo de volume

Para criar um grupo de volumes a partir de um ou mais volumes físicos, use o `vgcreate` comando. Este comando cria um novo grupo de volumes por nome e adiciona ao menos um volume físico.

```
[root@hc-cloud-secure-1 ~]# vgcreate datavg /dev/sdb
Volume group "datavg" successfully created.
```

O `vgdisplay` comando pode ser usado para exibir propriedades do grupo de volume (como tamanho, extensões, número de volumes físicos, etc.) em um formulário fixo.

```
[root@hc-cloud-secure-1 ~]# vgdisplay datavg
  --- Volume group ---
  VG Name               datavg
  System ID
  Format                lvm2
  Metadata Areas        1
  Metadata Sequence No  1
  VG Access             read/write
  VG Status             resizable
  MAX LV                0
  Cur LV                0
  Open LV               0
  Max PV                0
  Cur PV                1
  Act PV                1
  VG Size               <200.00 GiB
  PE Size               4.00 MiB
  Total PE              51199
  Alloc PE / Size       0 / 0
  Free  PE / Size       51199 / <200.00 GiB
  VG UUID               C7jmI0-J0SS-Cq91-t6b4-A9xw-nTfi-RXcy28
```

Criar volume lógico

Quando você cria um volume lógico, o volume lógico é gravado a partir de um grupo de volumes usando as extensões livres nos volumes físicos que compõem o grupo de volumes.

```
[root@hc-cloud-secure-1 ~]# lvcreate - l 100%FREE -n datalv datavg
Logical volume "datalv" created.
```

Este comando cria um volume lógico chamado `datalv` que usa todo o espaço não alocado no grupo de volumes `datavg` .

Criar sistema de arquivos

```
[root@hc-cloud-secure-1 ~]# mkfs.xfs -K /dev/datavg/datalv
meta-data=/dev/datavg/datalv     isize=512    agcount=4, agsize=13106944
blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=1, sparse=1, rmapbt=0
         =                       reflink=1    bigtime=0 inobtcount=0
data     =                       bsize=4096   blocks=52427776, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0, ftype=1
log      =internal log           bsize=4096   blocks=25599, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

Faça a pasta para montar

```
[root@hc-cloud-secure-1 ~]# mkdir /file1
```

Monte o sistema de ficheiros

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1

[root@hc-cloud-secure-1 ~]# df -k
Filesystem                 1K-blocks    Used Available Use% Mounted on
devtmpfs                     8072804       0   8072804   0% /dev
tmpfs                        8103272       0   8103272   0% /dev/shm
tmpfs                        8103272    9404   8093868   1% /run
tmpfs                        8103272       0   8103272   0% /sys/fs/cgroup
/dev/mapper/cs-root         45496624 5642104  39854520  13% /
/dev/sda2                    1038336  258712    779624  25% /boot
/dev/sda1                     613184    7416    605768   2% /boot/efi
tmpfs                        1620652      12   1620640   1% /run/user/42
tmpfs                        1620652       0   1620652   0% /run/user/0
/dev/mapper/datavg-datalv 209608708 1494520 208114188   1% /file1
```

Para obter informações detalhadas sobre essas tarefas, consulte a página "Administração LVM com comandos CLI".

Geração de dados

`Dgen.pl` É um gerador de dados de script perl para o simulador de e/S da EHR (GenerateIO). Os dados dentro dos LUNs são gerados com o script EHR `Dgen.pl`. O script foi projetado para criar dados semelhantes ao que seria encontrado dentro de um banco de dados EHR.

```
[root@hc-cloud-secure-1 ~]# cd GenerateIO-1.17.3/

[root@hc-cloud-secure-1 GenerateIO-1.17.3]# ./dgen.pl --directory /file1
--jobs 80

[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37
dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38
dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39
dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40
dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80

[root@hc-cloud-secure-1 file1]# df -k .
Filesystem                1K-blocks  Used       Available  Use%  Mounted
on
/dev/mapper/datavg-datalv  209608708  178167156  31441552   85%   /file1
```

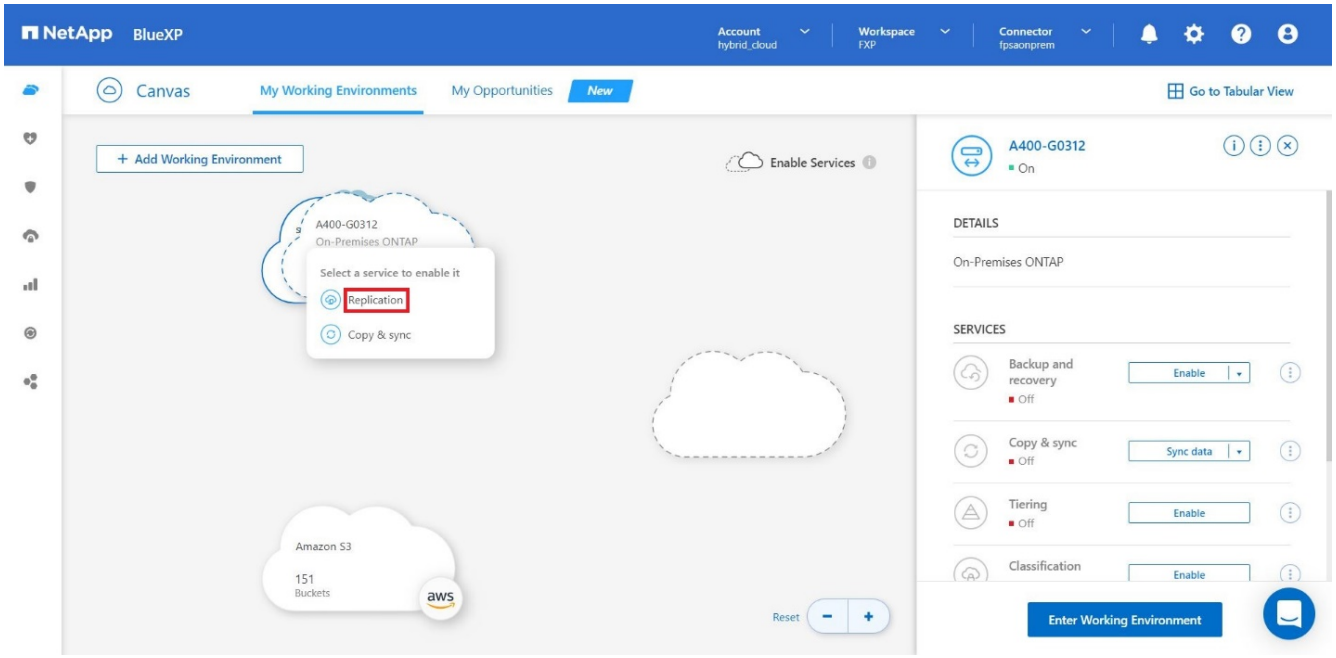
Durante a execução, o `Dgen.pl` script usa 85% do sistema de arquivos para geração de dados por padrão.

Configurar a replicação do SnapMirror entre o ONTAP no local e o Cloud Volumes ONTAP

O NetApp SnapMirror replica dados em alta velocidade em LAN ou WAN, para que você tenha alta disponibilidade e rápida replicação de dados em ambientes virtuais e tradicionais. Ao replicar dados para os sistemas de storage da NetApp e atualizar continuamente os dados secundários, os dados permanecem atuais e disponíveis sempre que for necessário. Não são necessários servidores de replicação externos.

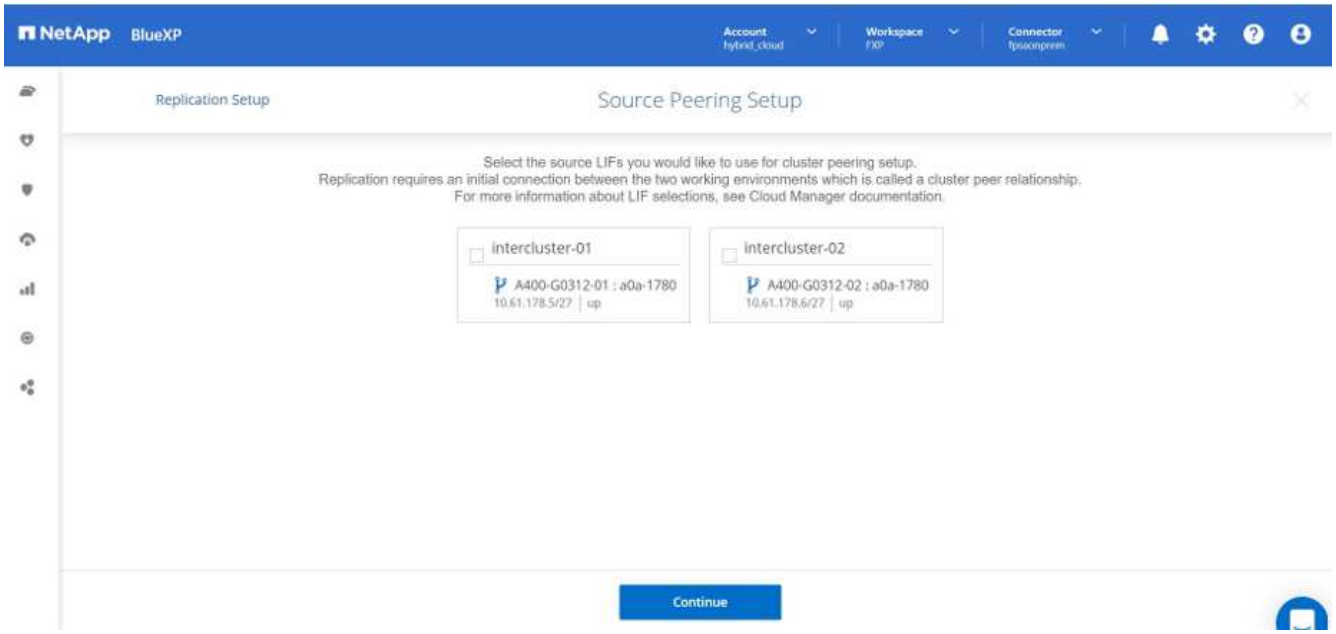
Siga as etapas a seguir para configurar a replicação do SnapMirror entre o sistema ONTAP local e o CVO.

1. No menu de navegação, selecione **Storage** > **Canvas**.
2. No Canvas, selecione o ambiente de trabalho que contém o volume de origem, arraste-o para o ambiente de trabalho para o qual deseja replicar o volume e selecione **replicação**.

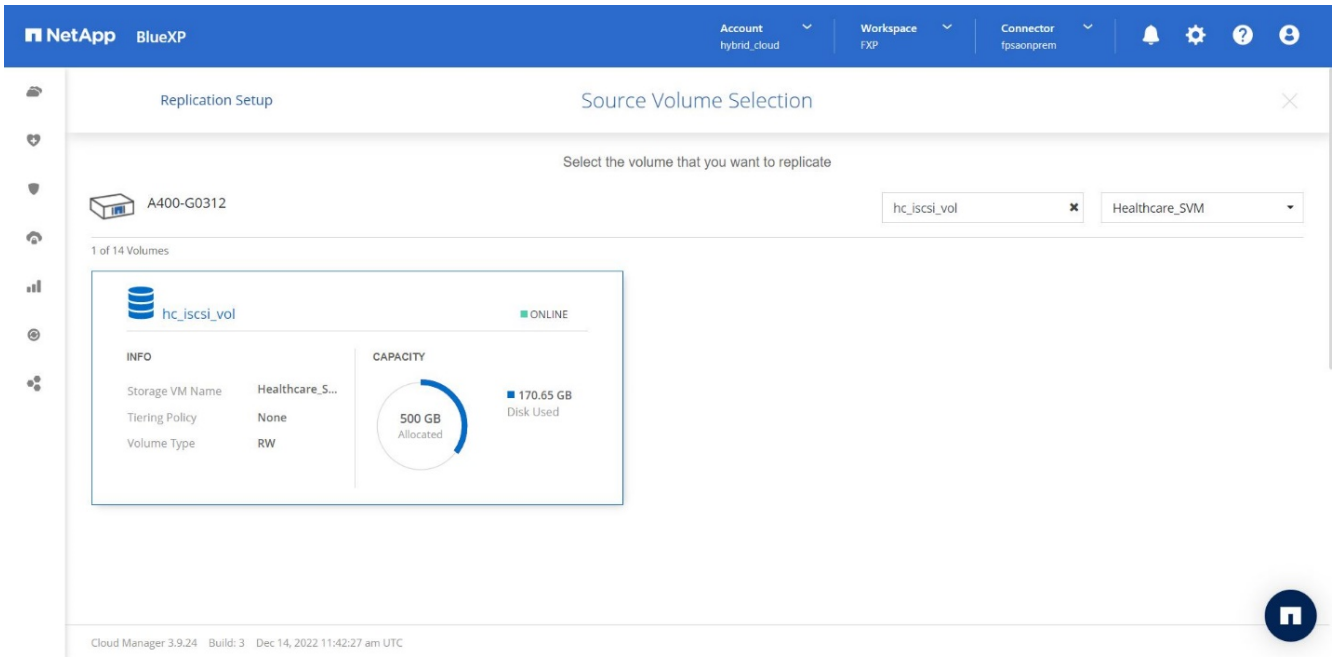


As etapas restantes explicam como criar uma relação síncrona entre o Cloud Volumes ONTAP e os clusters do ONTAP no local.

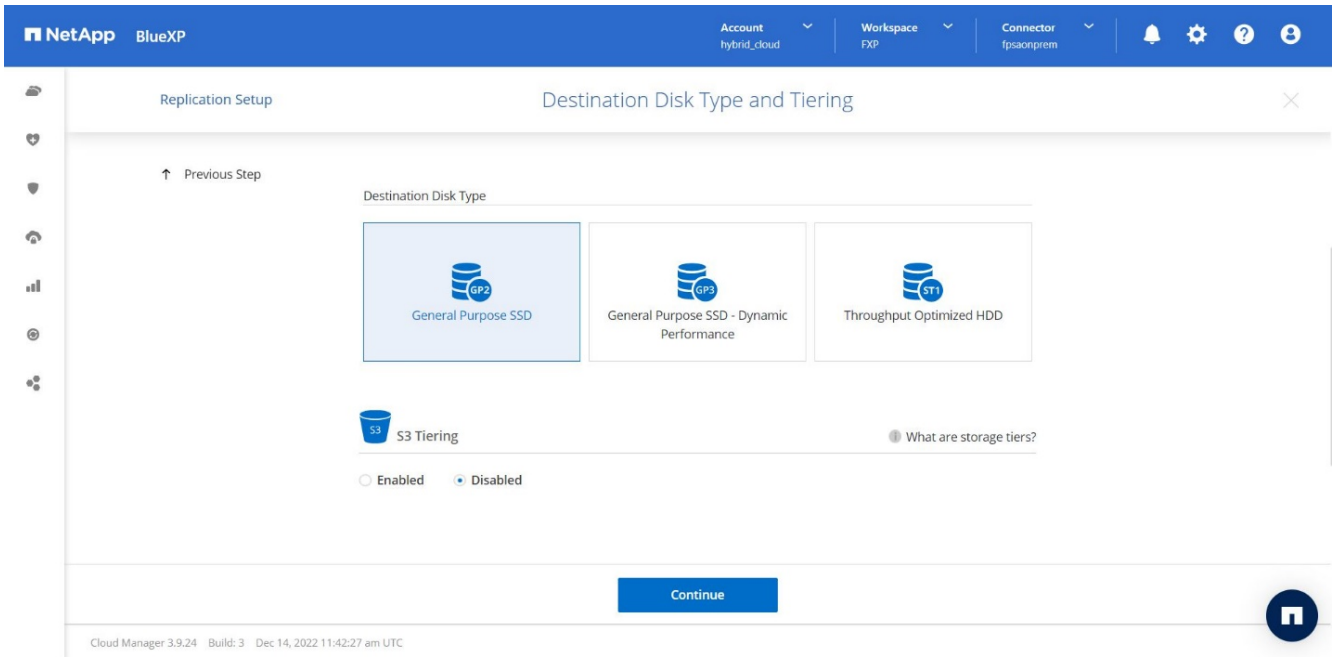
3. * Configuração de peering de origem e destino.* Se esta página for exibida, selecione todas as LIFs entre clusters para o relacionamento de pares de cluster.



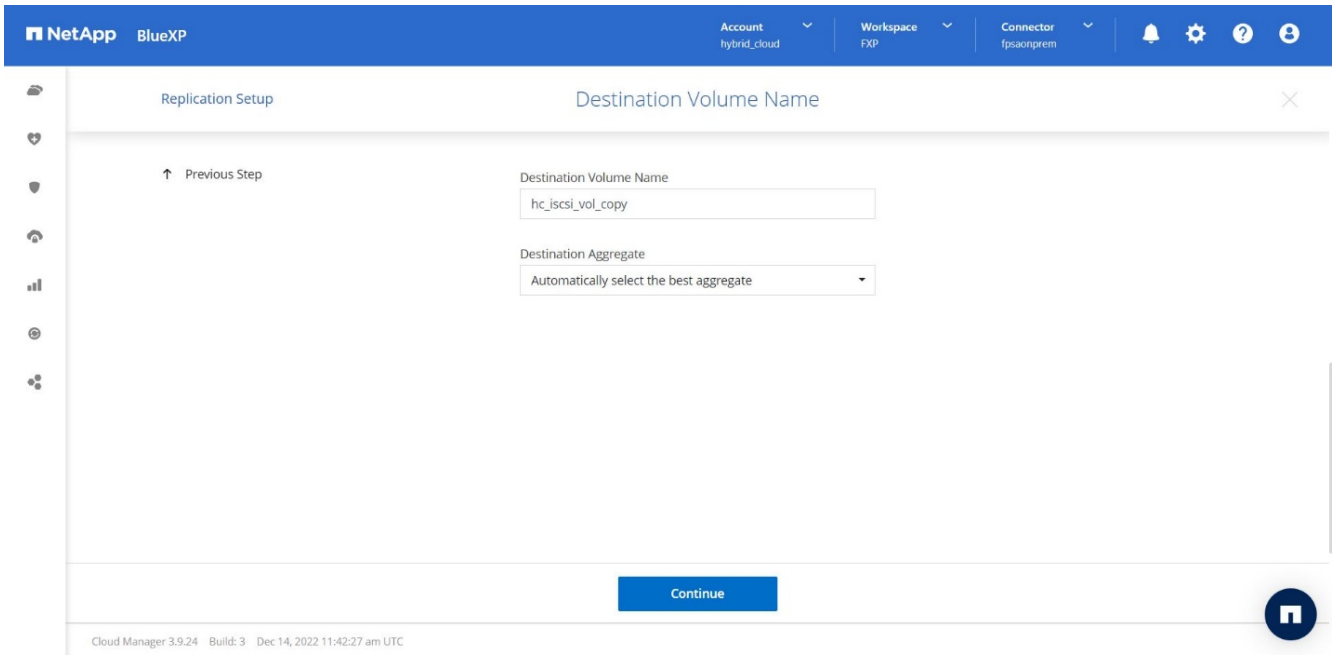
4. **Seleção de volume de origem.** Selecione o volume que pretende replicar.



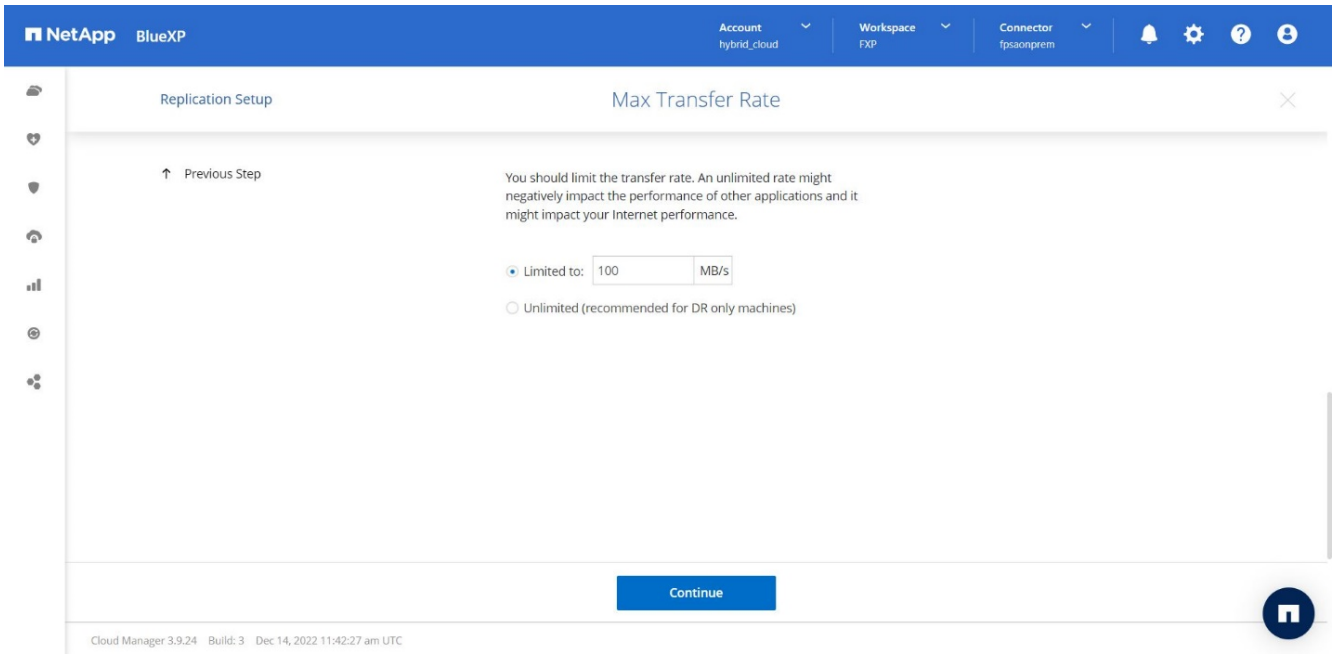
5. **Tipo de disco de destino e disposição em camadas.** Se o destino for um sistema Cloud Volumes ONTAP, selecione o tipo de disco de destino e escolha se deseja habilitar a disposição em camadas de dados.



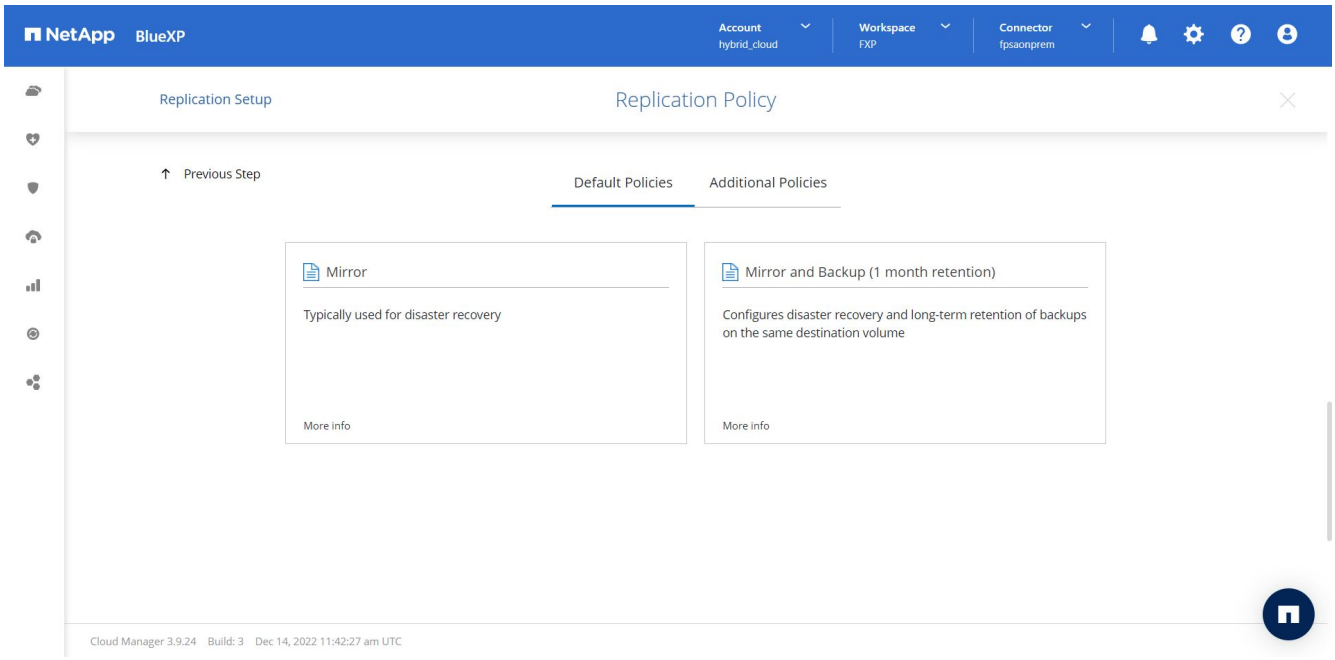
6. **Nome do volume de destino:** Especifique o nome do volume de destino e escolha o agregado de destino. Se o destino for um cluster do ONTAP, você também deverá especificar a VM de armazenamento de destino.



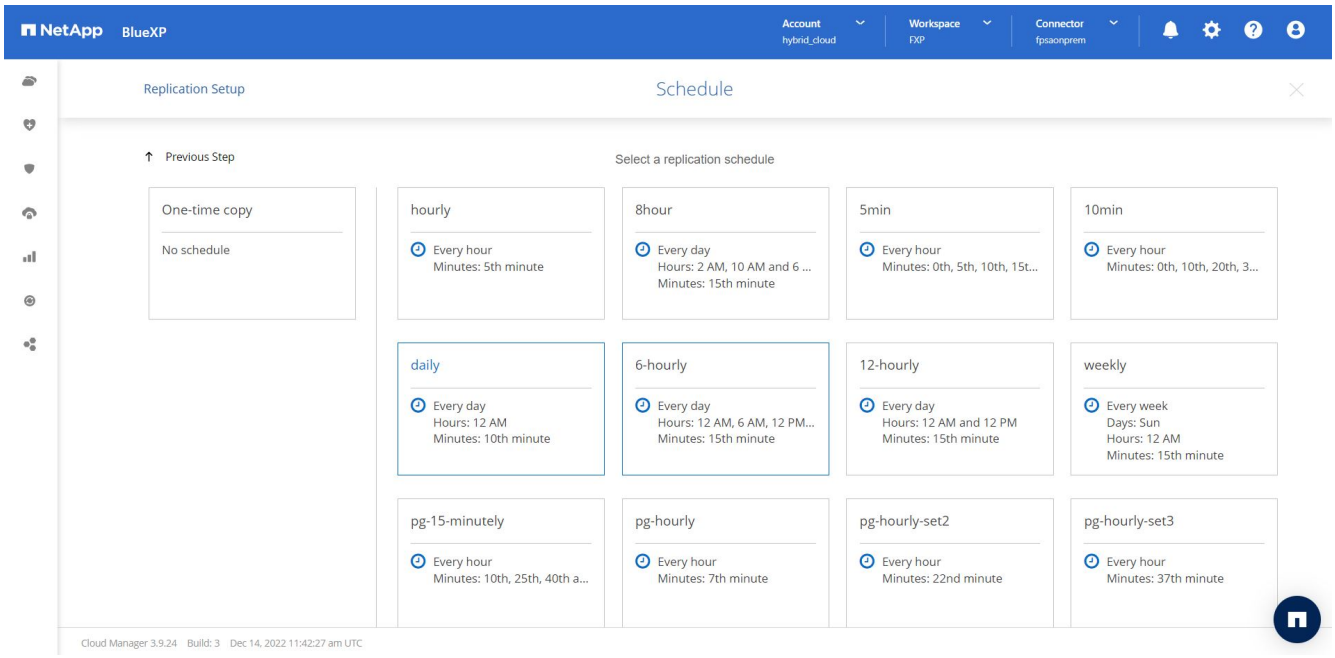
7. * Taxa máxima de transferência.* Especifique a taxa máxima (em megabytes por segundo) na qual os dados podem ser transferidos.



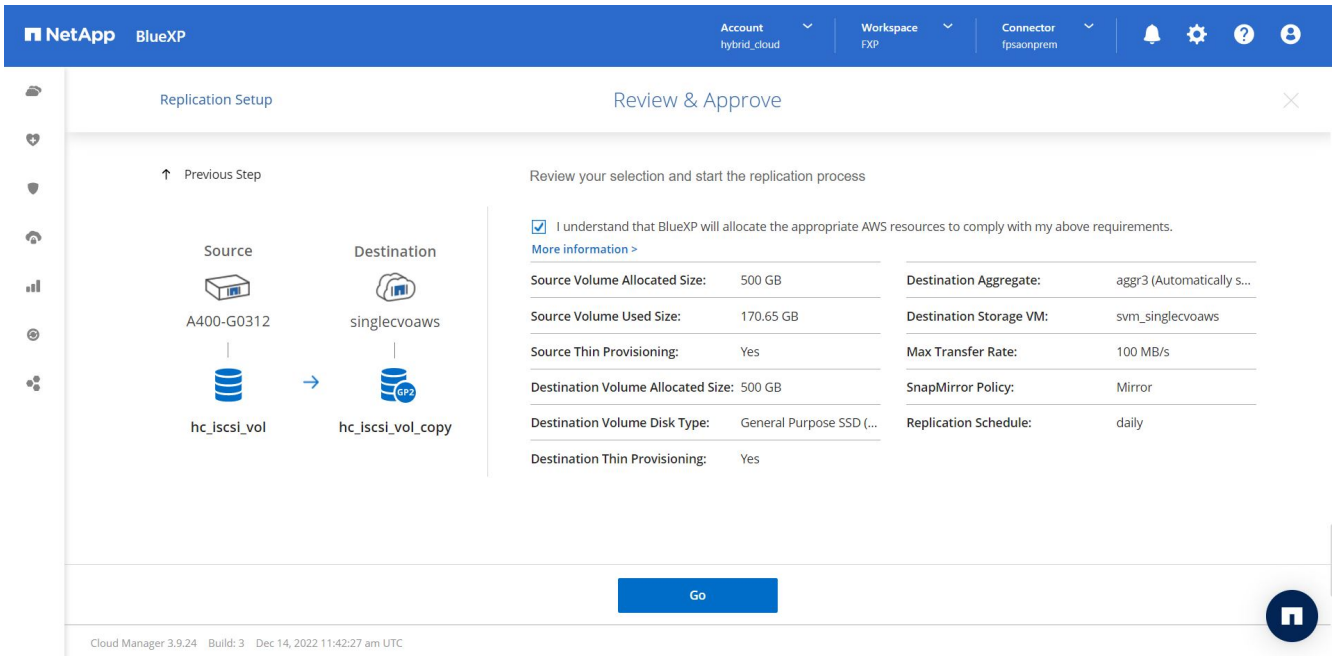
8. **Política de replicação.** Escolha uma política padrão ou clique em **políticas adicionais** e selecione uma das políticas avançadas. Para obter ajuda, "saiba mais sobre políticas de replicação".



9. **Programação.** Escolha uma cópia única ou uma programação recorrente. Várias programações padrão estão disponíveis. Se você quiser uma programação diferente, você deve criar uma nova programação no `destination cluster` usando o System Manager.

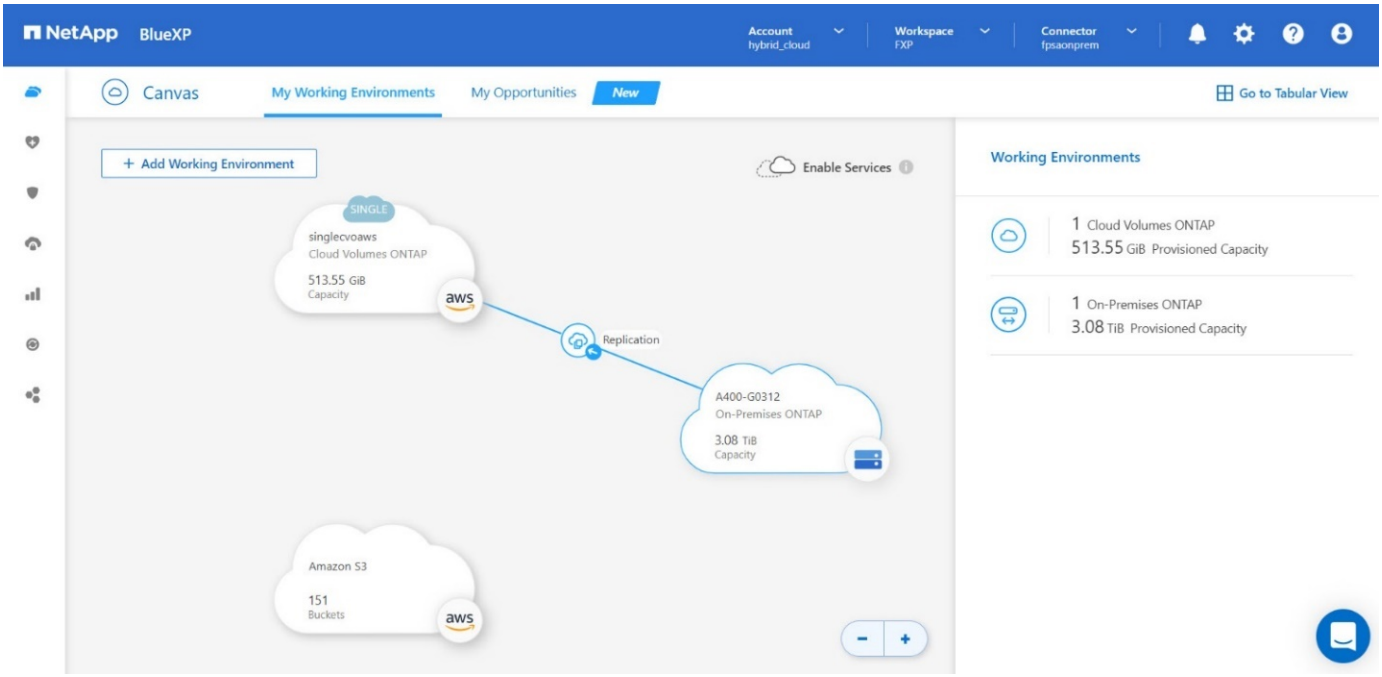


10. **Revisão.** Reveja as suas seleções e clique em **Go**.

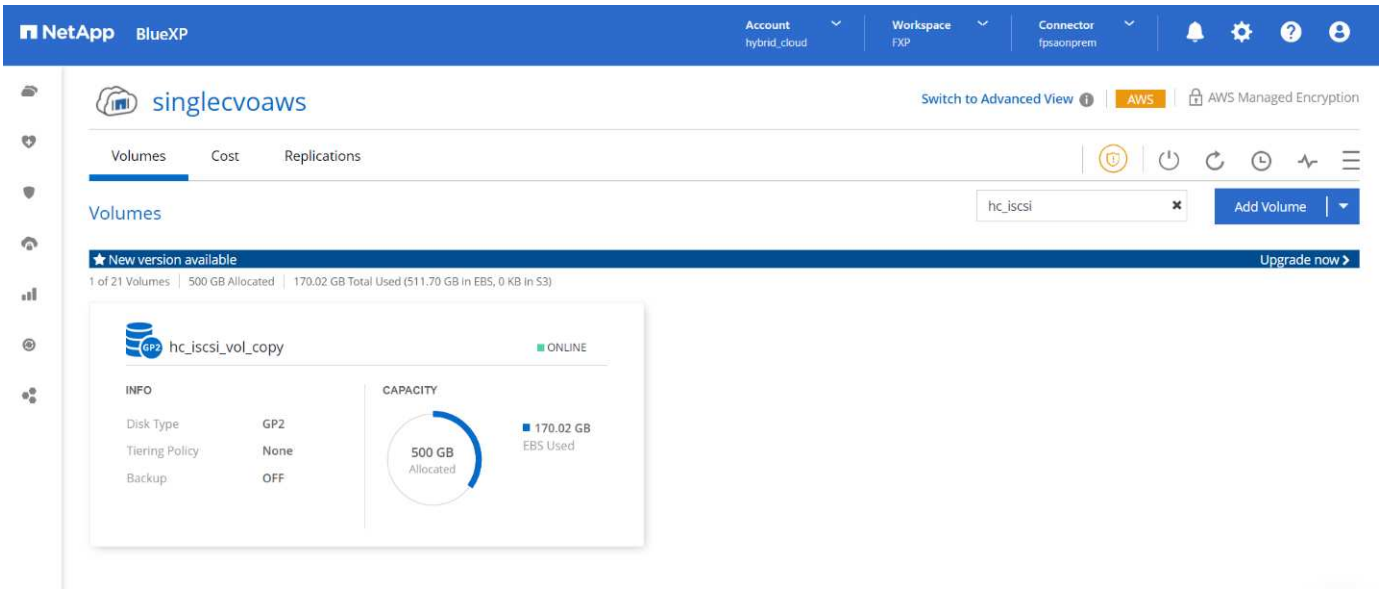


Para obter informações detalhadas sobre essas etapas de configuração, "aqui"consulte .

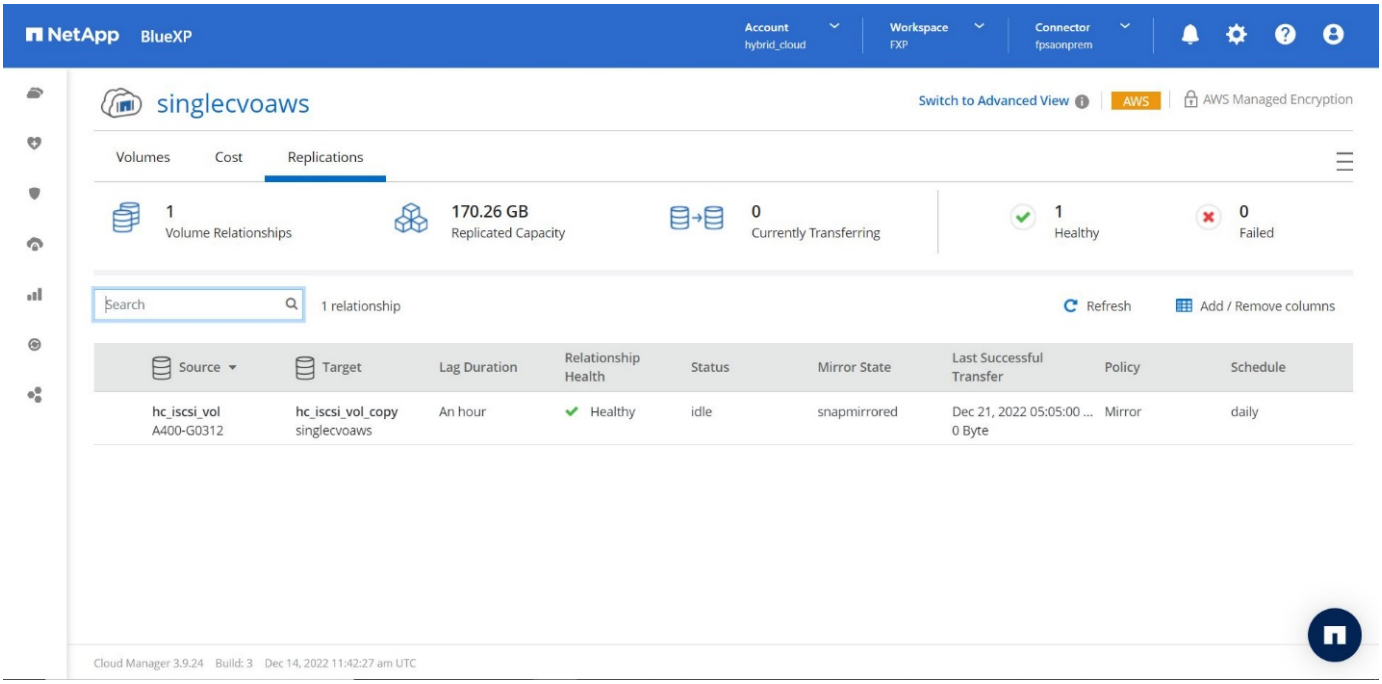
O BlueXP inicia o processo de replicação de dados. Agora, você pode ver o serviço **replicação** estabelecido entre o sistema ONTAP local e o Cloud Volumes ONTAP.



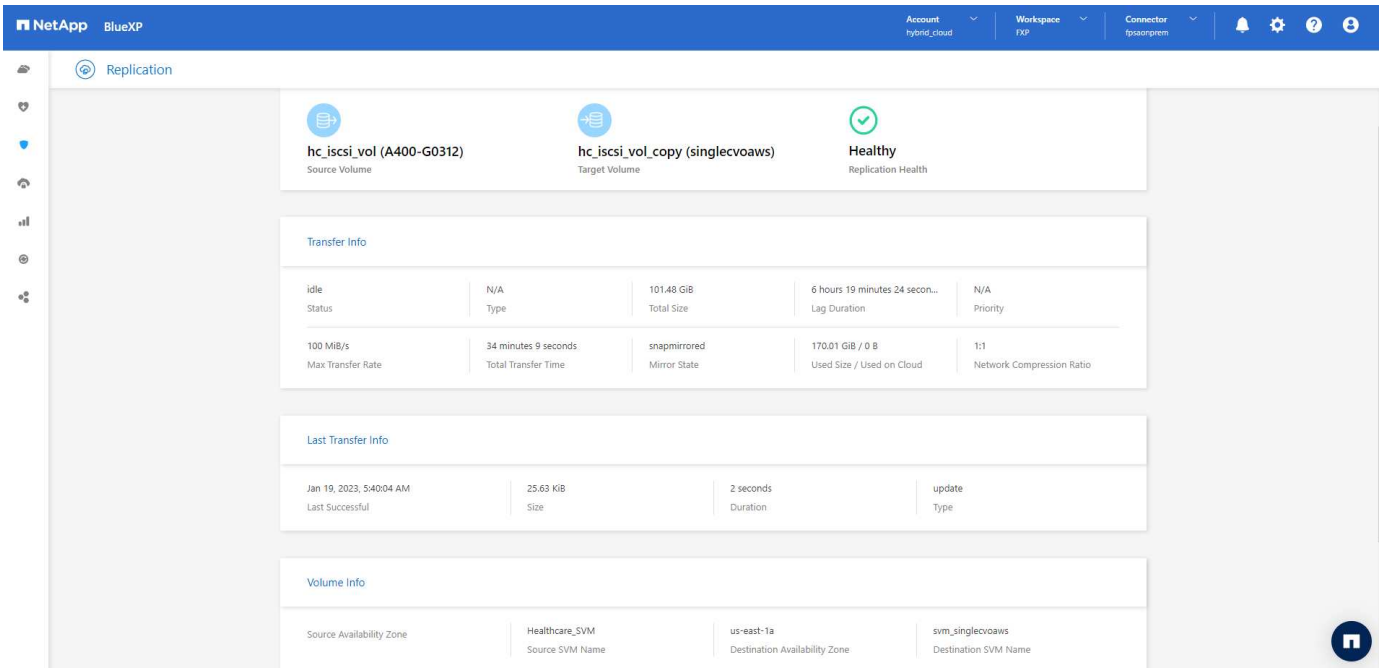
No cluster Cloud Volumes ONTAP, você pode ver o volume recém-criado.



Você também pode verificar se a relação do SnapMirror está estabelecida entre o volume no local e o volume de nuvem.



Mais informações sobre a tarefa de replicação podem ser encontradas na guia **replicação**.



"Próximo: Validação da solução."

Validação da solução

"Anterior: Configuração SAN."

Nesta seção, revisamos alguns casos de uso da solução.

- Um dos principais casos de uso do SnapMirror é o backup de dados. O SnapMirror pode ser usado como uma ferramenta de backup principal replicando dados no mesmo cluster ou em destinos remotos.
- Uso do ambiente DR para executar o teste de desenvolvimento de aplicações (desenvolvimento/teste).
- DR em caso de desastre na produção.
- Distribuição de dados e acesso remoto a dados.

Notavelmente, os relativamente poucos casos de uso validados nesta solução não representam toda a funcionalidade da replicação do SnapMirror.

Desenvolvimento e teste de aplicativos (desenvolvimento/teste)

Para acelerar o desenvolvimento de aplicações, você pode clonar rapidamente os dados replicados no local de recuperação de desastres e usá-los para aplicações de desenvolvimento/teste. O colocation dos ambientes de DR e desenvolvimento/teste pode melhorar significativamente a utilização de instalações de backup ou DR. Os clones de desenvolvimento/teste sob demanda fornecem quantas cópias de dados você precisa para chegar à produção com mais rapidez.

A tecnologia NetApp FlexClone pode ser usada para criar rapidamente uma cópia de leitura e gravação de um FlexVol volume de destino do SnapMirror caso você queira ter acesso de leitura e gravação da cópia secundária para confirmar se todos os dados de produção estão disponíveis.

Siga as etapas a seguir para usar o ambiente de DR para executar o desenvolvimento/teste de aplicações:

1. Faça uma cópia dos dados de produção. Para fazer isso, execute um snapshot de aplicação de um volume no local. A criação de instantâneos de aplicativos consiste em três etapas: `Lock`, `Snap` E `Unlock`.

a. Quiesce o sistema de arquivos para que a e/S seja suspensa e os aplicativos mantenham a consistência. Qualquer aplicativo escreve atingindo o sistema de arquivos permanece em um estado de espera até que o comando unquiesce seja emitido na etapa c. os passos a, b e c são executados por meio de um processo ou um fluxo de trabalho que é transparente e não afeta o SLA do aplicativo.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -f /file1
```

Esta opção solicita que o sistema de arquivos especificado seja congelado de novas modificações. Qualquer processo tentando gravar no sistema de arquivos congelado é bloqueado até que o sistema de arquivos seja descongelado.

b. Criar um snapshot do volume local.

```
A400-G0312::> snapshot create -vserver Healthcare_SVM -volume
hc_iscsi_vol -snapshot kamini
```

c. Desmarque o sistema de arquivos para reiniciar o e/S.

```
[root@hc-cloud-secure-1 ~]# fsfreeze -u /file1
```

Esta opção é usada para descongelar o sistema de arquivos e permitir que as operações continuem. Todas as modificações do sistema de arquivos que foram bloqueadas pelo congelamento são desbloqueadas e podem ser concluídas.

O snapshot consistente com a aplicação também pode ser realizado usando o NetApp SnapCenter, que tem a orquestração completa do fluxo de trabalho descrito acima como parte do SnapCenter. Para obter informações detalhadas, "aqui"consulte .

2. Execute uma operação de atualização do SnapMirror para manter os sistemas de produção e DR sincronizados.

```
singlecvoaws::> snapmirror update -destination-path
svm_singlecvoaws:hc_iscsi_vol_copy -source-path
Healthcare_SVM:hc_iscsi_vol

Operation is queued: snapmirror update of destination
“svm_singlecvoaws:hc_iscsi_vol_copy”.
```

Uma atualização do SnapMirror também pode ser executada através da GUI do BlueXP na guia **replicação**.

3. Crie uma instância do FlexClone com base no snapshot do aplicativo que foi feito anteriormente.

```
singlecvoaws::> volume clone create -flexclone kamini_clone -type RW
-parent-vserver svm_singlecvoaws -parent-volume hc_iscsi_vol_copy
-junction-active true -foreground true -parent-snapshot kamini

[Job 996] Job succeeded: Successful
```

Para a tarefa anterior, um novo snapshot também pode ser criado, mas você deve seguir as mesmas etapas acima para garantir a consistência do aplicativo.

4. Ative um volume de FlexClone para abrir a instância de EHR na nuvem.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/kamini_clone/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup    LUN ID
Protocol
---------- -------------- --------------- -----  --------   ------
---------
svm_singlecvoaws
                /vol/kamini_clone/iscsi_lun1    ehr-igroup   0    iscsi
```

5. Execute os seguintes comandos na instância EHR na nuvem para acessar os dados ou o sistema de arquivos.
   a. Descubra o armazenamento ONTAP. Verifique o status de multipathing.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show

Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                    /vol/kamini_clone/iscsi_lun1
sudo multipath -ll

Output:
3600a09806631755a452b543041313053 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

b. Ative o grupo de volume.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

c. Monte o sistema de arquivos e exiba o resumo das informações do sistema de arquivos.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                1K-blocks  Used     Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708 183987096  25621612  88%
/file1
```

Isso valida que você pode usar o ambiente DR para desenvolvimento/teste de aplicativos. A execução de desenvolvimento/teste de aplicações no storage de recuperação de desastres permite que você use mais recursos que, de outra forma, podem ficar ociosos na maior parte do tempo.

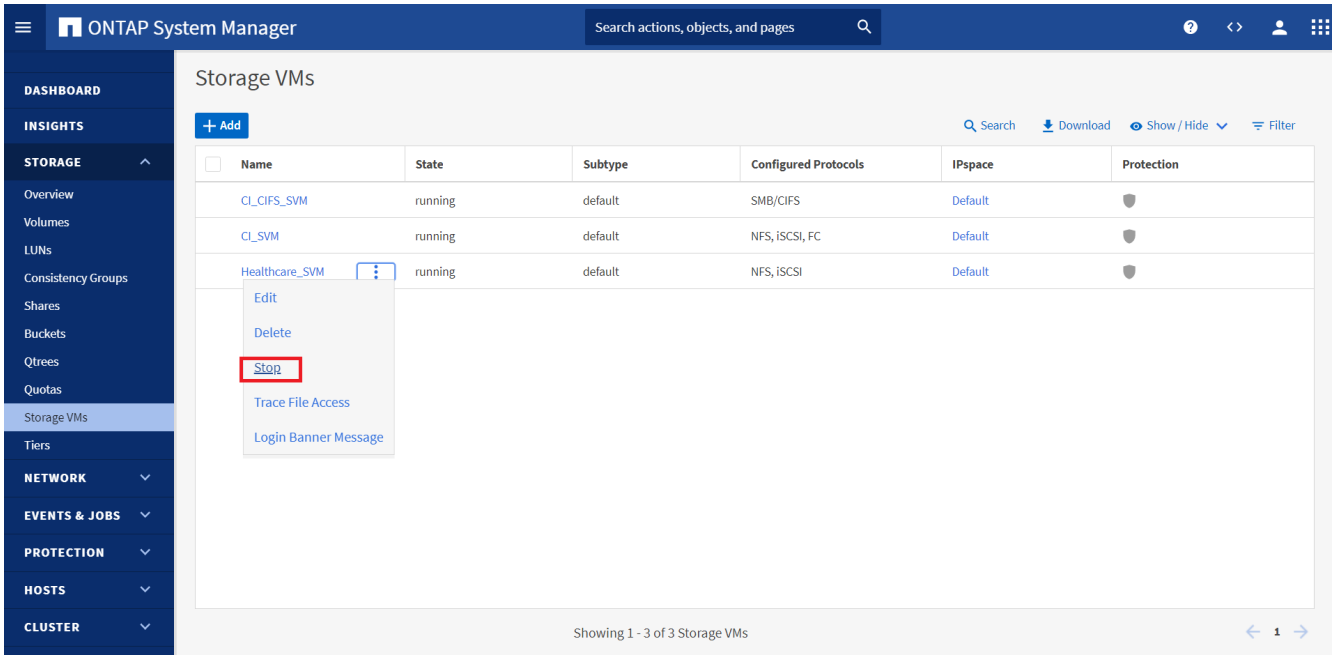
Recuperação de desastres

A tecnologia SnapMirror também é usada como parte dos planos de DR. Se os dados essenciais forem replicados para um local físico diferente, um desastre grave não precisa causar períodos prolongados de indisponibilidade de dados para aplicações essenciais aos negócios. Os clientes podem acessar dados replicados na rede até a recuperação do local de produção de corrupção, exclusão acidental, desastre natural e assim por diante.

No caso de failback para o local principal, o SnapMirror fornece um meio eficiente de ressincronizar o local de DR com o local principal, transferindo apenas dados alterados ou novos de volta para o local principal a partir do local de DR simplesmente invertendo a relação do SnapMirror. Depois que o local de produção primário retomar as operações normais da aplicação, o SnapMirror continuará a transferência para o local de DR sem precisar de outra transferência de linha de base.

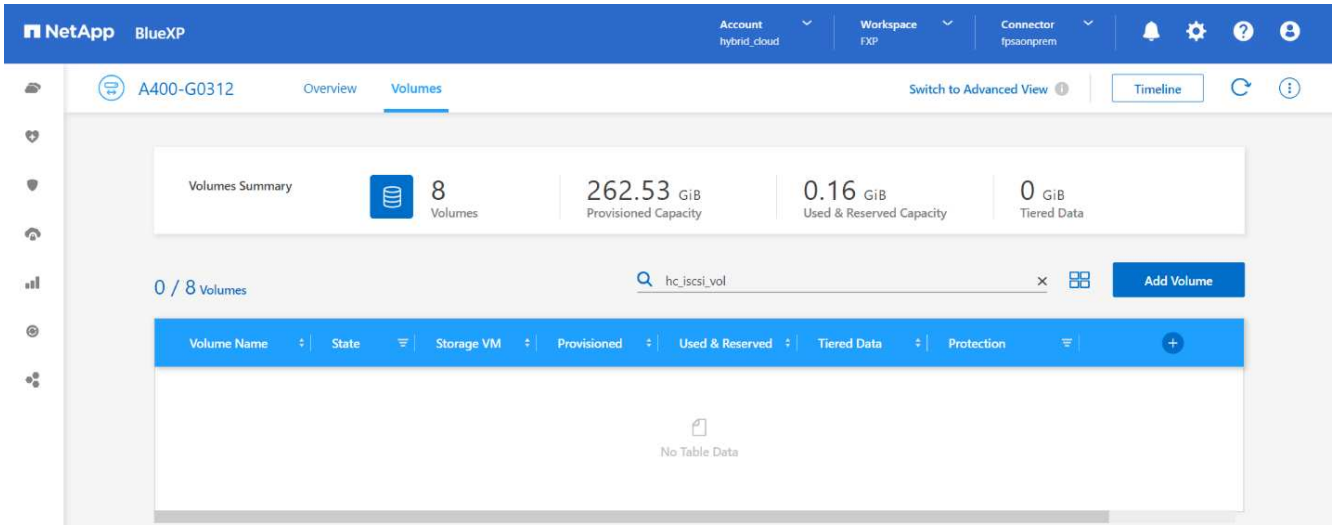
Para executar a validação de um cenário de DR bem-sucedido, execute as seguintes etapas:

1. Simule um desastre no lado da origem (produção) parando o SVM que hospeda o volume ONTAP no local (`hc_iscsi_vol`).



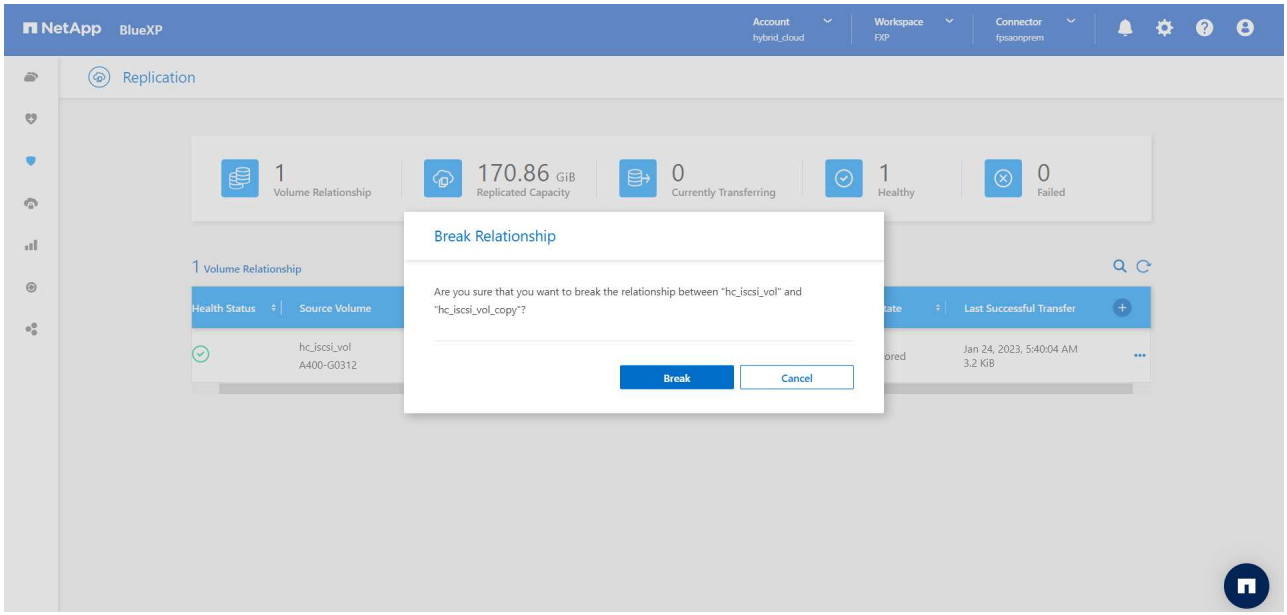
Verifique se a replicação do SnapMirror já está configurada entre o ONTAP no local na instância do FlexPod e o Cloud Volumes ONTAP na AWS, para que você possa criar snapshots de aplicações frequentes.

Depois que o SVM tiver sido interrompido, o `hc_iscsi_vol` volume não será visível no BlueXP .



2. Ative o DR no CVO.

   a. Quebre a relação de replicação do SnapMirror entre o ONTAP local e o Cloud Volumes ONTAP e promova o volume de destino do CVO (`hc_iscsi_vol_copy`) para produção.



   Depois que a relação SnapMirror é interrompida, o tipo de volume de destino muda de proteção de dados (DP) para leitura/gravação (RW).

```
singlecvoaws::> volume show -volume hc_iscsi_vol_copy -fields typev
server          volume              type
--------------- ------------------- ----
svm_singlecvoaws hc_iscsi_vol_copy RW
```

   b. Ative o volume de destino no Cloud Volumes ONTAP para abrir a instância de EHR em uma instância do EC2 na nuvem.

```
singlecvoaws::> lun mapping create –vserver svm_singlecvoaws –path
/vol/hc_iscsi_vol_copy/iscsi_lun1 -igroup ehr-igroup –lun-id 0

singlecvoaws::> lun mapping show
Vserver     Path                                  Igroup   LUN ID
Protocol
---------- ----------------------------------  --------  ------
---------
svm_singlecvoaws
            /vol/hc_iscsi_vol_copy/iscsi_lun1  ehr-igroup  0    iscsi
```

c. Para acessar os dados e o sistema de arquivos na instância EHR na nuvem, primeiro descubra o armazenamento ONTAP e verifique o status de multipathing.

```
sudo rescan-scsi-bus.sh
sudo iscsiadm -m discovery -t sendtargets -p <iscsi-lif-ip>
sudo iscsiadm -m node -L all
sudo sanlun lun show
Output:
controller(7mode/E-Series)/         device    host             lun
vserver(cDOT/FlashRay) lun-pathname filename  adapter protocol size
product
------------------------------------------------------------------------
--------
svm_singlecvoaws                    /dev/sda  host2   iSCSI    200g
cDOT
                  /vol/hc_iscsi_vol_copy/iscsi_lun1
sudo multipath -ll
Output:
3600a09806631755a452b543041313051 dm-0 NETAPP,LUN C-Mode
size=200G features='3 queue_if_no_path pg_init_retries 50'
hwhandler='1 alua' wp=rw
`-+- policy='service-time 0' prio=50 status=active
`- 2:0:0:0 sda 8:0 active ready running
```

d. Em seguida, ative o grupo de volume.

```
sudo vgchange -ay datavg
Output:
1 logical volume(s) in volume group "datavg" now active
```

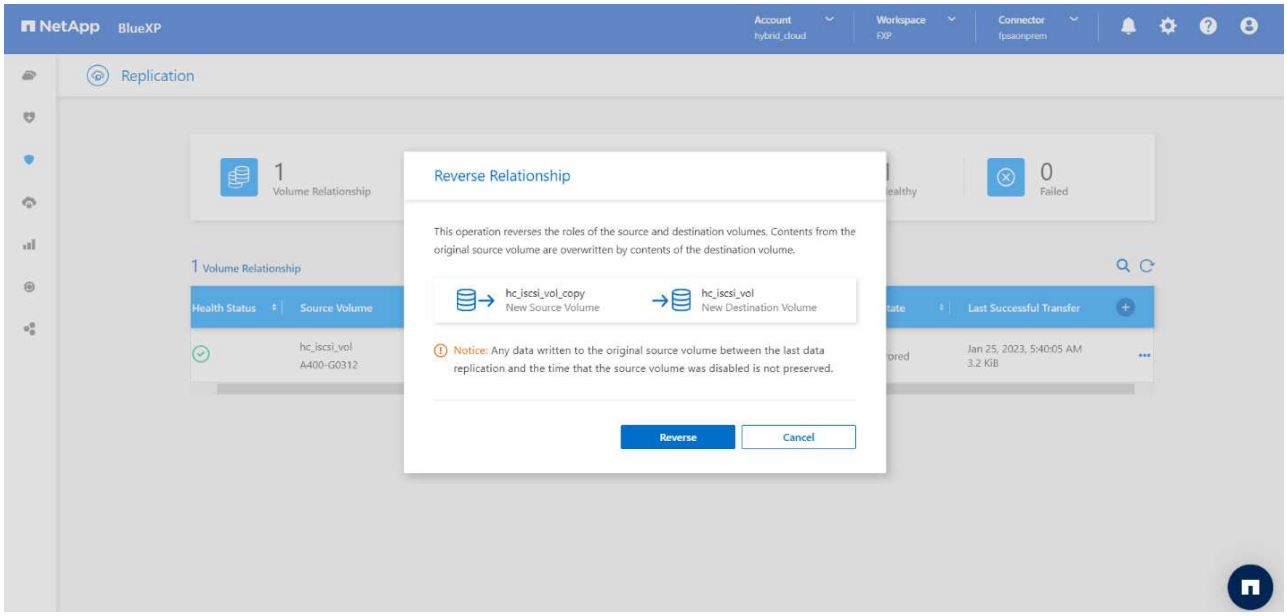
e. Finalmente, monte o sistema de arquivos e exiba as informações do sistema de arquivos.

```
sudo mount -t xfs /dev/datavg/datalv /file1

cd /file1
df -k .
Output:
Filesystem                 1K-blocks  Used      Available  Use%
Mounted on
/dev/mapper/datavg-datalv  209608708  183987096  25621612  88%
/file1
```

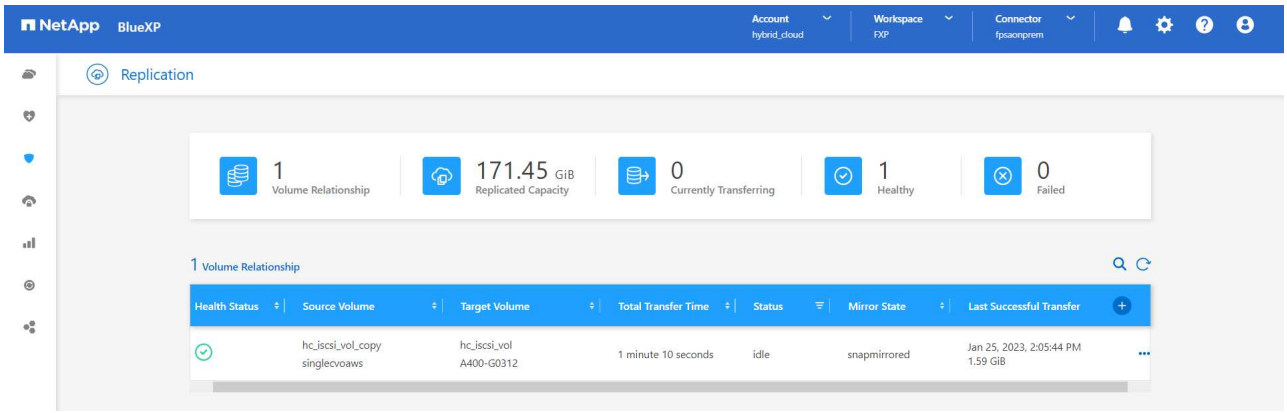
Essa saída mostra que os usuários podem acessar dados replicados na rede até a recuperação do local de produção em caso de desastre.

f. Inverta a relação SnapMirror. Esta operação inverte as funções dos volumes de origem e destino.



Quando esta operação é executada, o conteúdo do volume de origem original é substituído pelo conteúdo do volume de destino. Isso é útil quando você deseja reativar um volume de origem que ficou offline.

Agora, o volume CVO (`hc_iscsi_vol_copy`) torna-se o volume de origem e o volume no local (`hc_iscsi_vol`) torna-se o volume de destino.



Quaisquer dados gravados no volume de origem original entre a última replicação de dados e a hora em que o volume de origem foi desativado não são preservados.

a. Para verificar o acesso de gravação ao volume CVO, crie um novo arquivo na instância EHR na nuvem.

```
cd /file1/
sudo touch newfile
```

Quando o local de produção está inativo, os clientes ainda podem acessar os dados e também executar gravações no volume Cloud Volumes ONTAP, que agora é o volume de origem.

No caso de failback para o local principal, o SnapMirror fornece um meio eficiente de ressincronizar o local de DR com o local principal, transferindo apenas dados alterados ou novos de volta para o local principal a partir do local de DR simplesmente invertendo a relação do SnapMirror. Depois que o local de produção primário retomar as operações normais da aplicação, o SnapMirror continuará a transferência para o local de DR sem precisar de outra transferência de linha de base.

Esta seção ilustra a resolução bem-sucedida de um cenário de DR quando o local de produção é atingido por um desastre. Os dados agora podem ser consumidos com segurança por aplicativos que agora podem atender os clientes enquanto o site de origem passa por restauração.

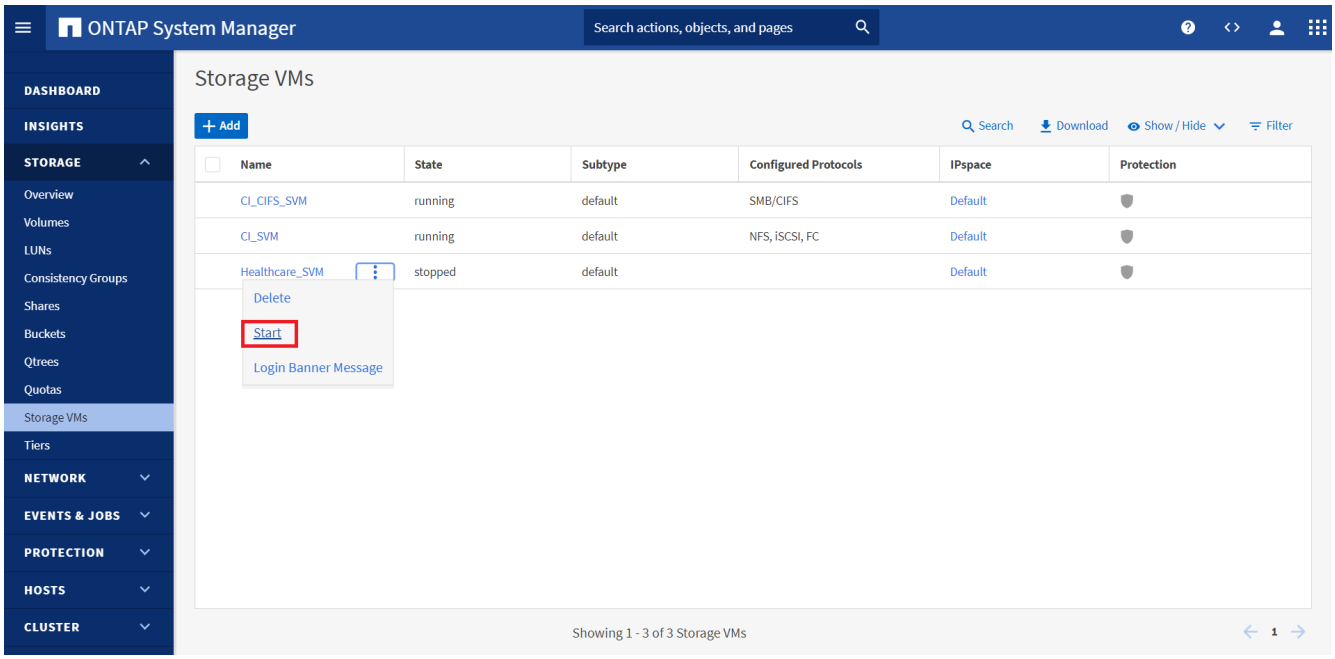
Verificação de dados no local de produção

Depois que o local de produção for restaurado, você deve garantir que a configuração original seja restaurada e que os clientes possam acessar os dados do site de origem.

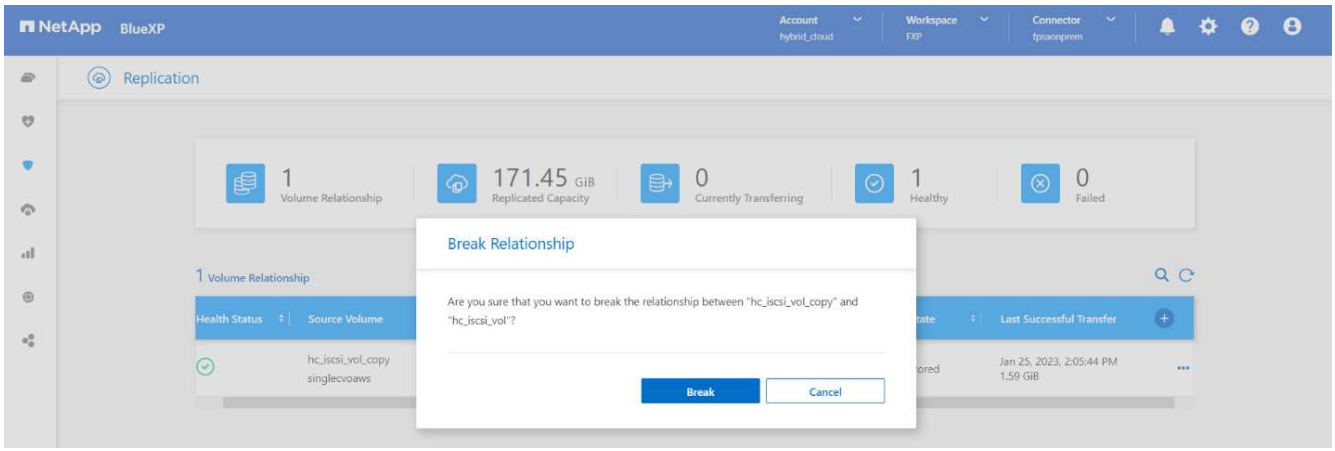
Nesta seção, falamos sobre como criar o site de origem, restaurar a relação SnapMirror entre ONTAP on-premises e Cloud Volumes ONTAP e, finalmente, realizar uma verificação de integridade de dados no fim da fonte

O seguinte procedimento pode ser utilizado para a verificação dos dados no local de produção:

1. Certifique-se de que o site de origem está agora disponível. Para fazer isso, inicie o SVM que hospeda o volume ONTAP no local (`hc_iscsi_vol`).



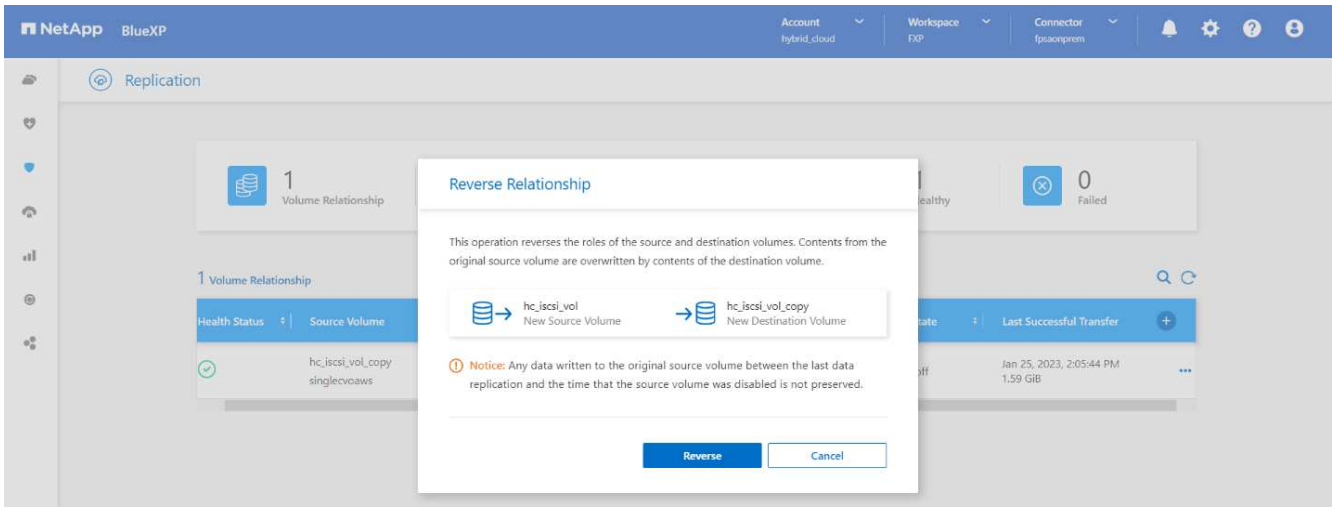
2. Quebre a relação de replicação do SnapMirror entre o Cloud Volumes ONTAP e o ONTAP no local e promova o volume on-(`hc_iscsi_vol`premises) de volta à produção.



Depois que a relação do SnapMirror é interrompida, o tipo de volume local muda de proteção de dados (DP) para leitura/gravação (RW).

```
A400-G0312::> volume show -volume hc_iscsi_vol -fields type
vserver        volume       type
-------------- ------------ ----
Healthcare_SVM hc_iscsi_vol RW
```

3. Inverta a relação SnapMirror. Agora, o volume ONTAP no local (`hc_iscsi_vol`) se torna o volume de origem como era antes e o volume Cloud Volumes ONTAP (`hc_iscsi_vol_copy`) se torna o volume de destino.



Seguindo estes passos, restauramos com sucesso a configuração original.

4. Reinicie a instância EHR no local. Monte o sistema de arquivos e verifique se o `newfile` que você criou na instância EHR na nuvem quando a produção estava inativa agora também existe aqui.

```
[root@hc-cloud-secure-1 ~]# mount -t xfs /dev/datavg/datalv /file1
[root@hc-cloud-secure-1 ~]# cd /file1/
[root@hc-cloud-secure-1 file1]# ls
dir01  dir05  dir09  dir13  dir17  dir21  dir25  dir29  dir33  dir37  dir41  dir45  dir49  dir53  dir57  dir61  dir65  dir69  dir73  dir77  kamini
dir02  dir06  dir10  dir14  dir18  dir22  dir26  dir30  dir34  dir38  dir42  dir46  dir50  dir54  dir58  dir62  dir66  dir70  dir74  dir78  latest_file
dir03  dir07  dir11  dir15  dir19  dir23  dir27  dir31  dir35  dir39  dir43  dir47  dir51  dir55  dir59  dir63  dir67  dir71  dir75  dir79  newfile
dir04  dir08  dir12  dir16  dir20  dir24  dir28  dir32  dir36  dir40  dir44  dir48  dir52  dir56  dir60  dir64  dir68  dir72  dir76  dir80
```

Podemos inferir que a replicação de dados da origem para o destino foi concluída com sucesso e que a integridade dos dados foi mantida. Isto conclui a verificação dos dados no local de produção.

"Próximo: Conclusão."

Conclusão

"Anterior: Validação da solução."

Criar uma nuvem híbrida é o objetivo que a maioria das organizações de saúde forneça disponibilidade de dados a qualquer momento. Nessa solução, implementamos uma solução de nuvem híbrida da FlexPod com o Cloud Volumes ONTAP, utilizando a tecnologia de replicação NetApp SnapMirror para validar alguns casos de uso para fazer backup e recuperar aplicações e workloads do setor de saúde.

O FlexPod, uma infraestrutura convergente pré-validada e rigorosamente testada da parceria estratégica da Cisco e do NetApp, foi projetada para fornecer alta disponibilidade e performance previsível do sistema de baixa latência. Esta abordagem resulta em elevados níveis de conforto da EHR e, em última análise, o melhor tempo de resposta para os utilizadores do sistema EHR.

Com o NetApp, você pode executar produção de EHR, recuperação de desastres, backup ou disposição em camadas na nuvem, como faria com que os recursos de storage do NetApp fossem executados em um data center local. Com o NetApp Cloud Volumes ONTAP, o NetApp fornece os recursos de classe empresarial e o desempenho necessário para executar eficazmente as EHR na nuvem. As opções de nuvem da NetApp fornecem bloco sobre iSCSI e arquivo sobre NFS ou SMB.

Essa solução atende à necessidade das organizações de saúde e permite que elas deem um passo em direção à transformação digital. Ele também pode ajudá-los a gerenciar suas aplicações e workloads de

maneira eficiente.

"Próximo: Onde encontrar informações adicionais."

Onde encontrar informações adicionais

"Anterior: Conclusão."

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Página inicial do FlexPod

  "https://www.flexpod.com"

- Cisco validou guias de design e implantação para FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- NetApp BlueXP

  "https://bluexp.netapp.com/"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/concept-overview-cvo.html"

- Início rápido do Cloud Volumes ONTAP na AWS

  "https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-aws.html"

- Replicação do SnapMirror

  "https://docs.netapp.com/us-en/cloud-manager-replication/concept-replication.html"

- TR-3928: Práticas recomendadas da NetApp para a Epic

  https://www.netapp.com/pdf.html?item=/media/17137-tr3928pdf.pdf

- TR-4693: Guia de implantação do FlexPod Datacenter para EPIC EHR

  "https://www.netapp.com/media/10658-tr-4693.pdf"

- FlexPod para Epic

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_vmw_epic.html"

- Ferramenta de Matriz de interoperabilidade do NetApp

  "http://support.netapp.com/matrix/"

- Ferramenta de interoperabilidade de hardware e software Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guia de compatibilidade da VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Março de 2023	Versão inicial

Nuvem híbrida da FlexPod para Google Cloud Platform com NetApp Cloud Volumes ONTAP e Cisco Intersight

TR-4939: Nuvem híbrida da FlexPod para Google Cloud Platform com NetApp Cloud Volumes ONTAP e Cisco Intersight

Ruchika Lahoti, NetApp

Introdução

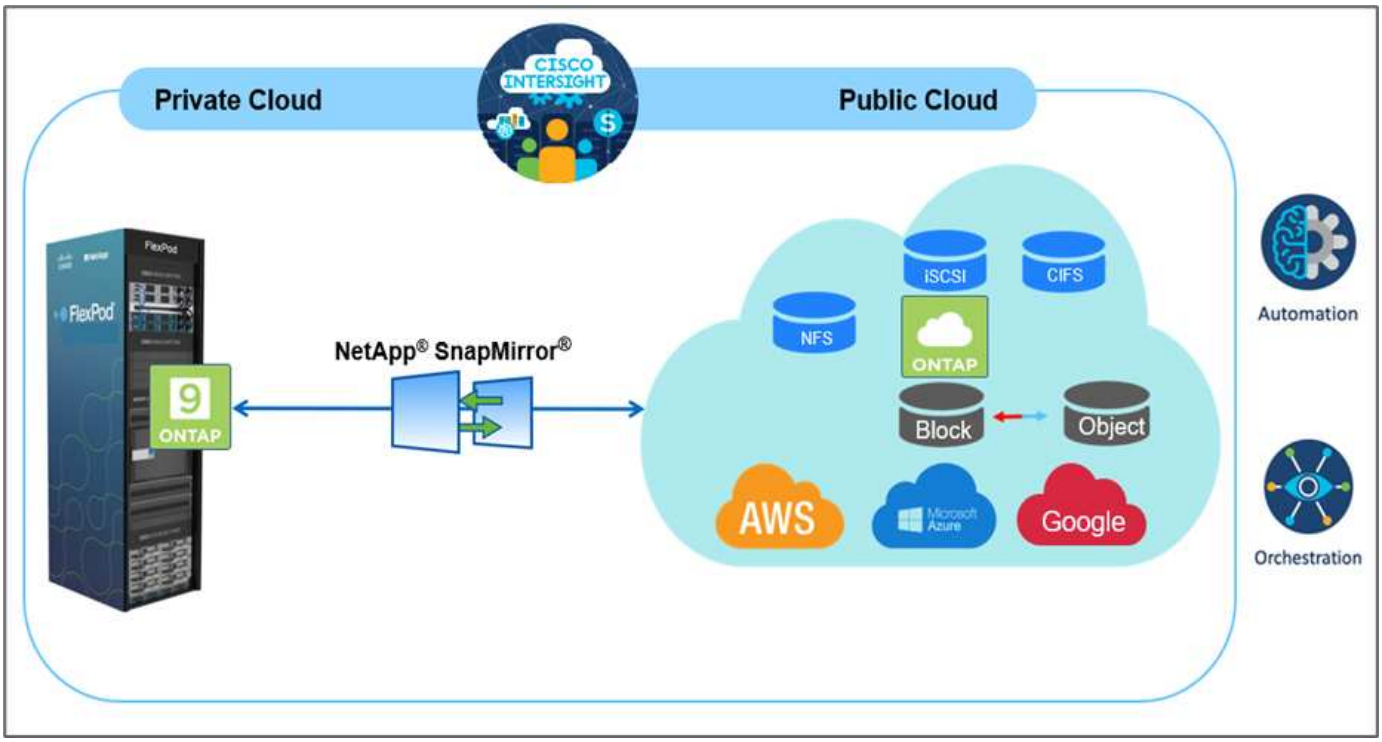
Proteger dados com recuperação de desastres (DR) é um objetivo essencial para a continuidade dos negócios. O DR permite que as organizações façam failover de suas operações de negócios em um local secundário e, posteriormente, recuperem e façam failback para o local primário de forma eficiente e confiável. Várias preocupações, como desastres naturais, falhas de rede, vulnerabilidades de software e erro humano, tornam o desenvolvimento de uma estratégia de DR uma prioridade DE TI principal.

Para a recuperação de desastres, todos os workloads executados no local principal precisam ser fielmente reproduzidos no local de recuperação de desastres. Uma organização também precisa ter uma cópia atualizada de todos os dados empresariais, incluindo banco de dados, serviços de arquivos, storage NFS e iSCSI, etc. Como os dados no ambiente de produção são constantemente atualizados, as alterações precisam ser transferidas regularmente para o local de DR.

A implantação de ambientes de DR é um desafio para a maioria das organizações devido ao requisito de independência de infraestrutura e local. O número de recursos necessários e os custos de configuração, teste e manutenção de um data center secundário podem ser muito altos, geralmente se aproximando do custo de todo o ambiente de produção. É difícil manter um espaço físico mínimo dos dados com proteção adequada, sincronizando os dados continuamente e estabelecendo failover e failback aprimorados. Depois de criar o local de DR, o desafio passa a ser replicar dados do ambiente de produção e mantê-los sincronizados no futuro.

Esse relatório técnico reúne a solução de infraestrutura convergente da FlexPod, o NetApp Cloud Volumes ONTAP no Google Cloud e o Cisco Intersight para formar um data center de nuvem híbrida para recuperação de desastres. Nesta solução, discutimos o design e a execução de um fluxo de trabalho ONTAP no local usando o Cisco Intersight Cloud Orchestrator. Também discutimos a implantação do NetApp Cloud Volumes ONTAP e a orquestração e automação da replicação de dados e DR entre o FlexPod e o Cloud Volumes ONTAP usando o Serviço de Intersight Cisco para o HashiCorp Terraform.

A figura a seguir fornece uma visão geral da solução.



Essa solução oferece várias vantagens, incluindo:

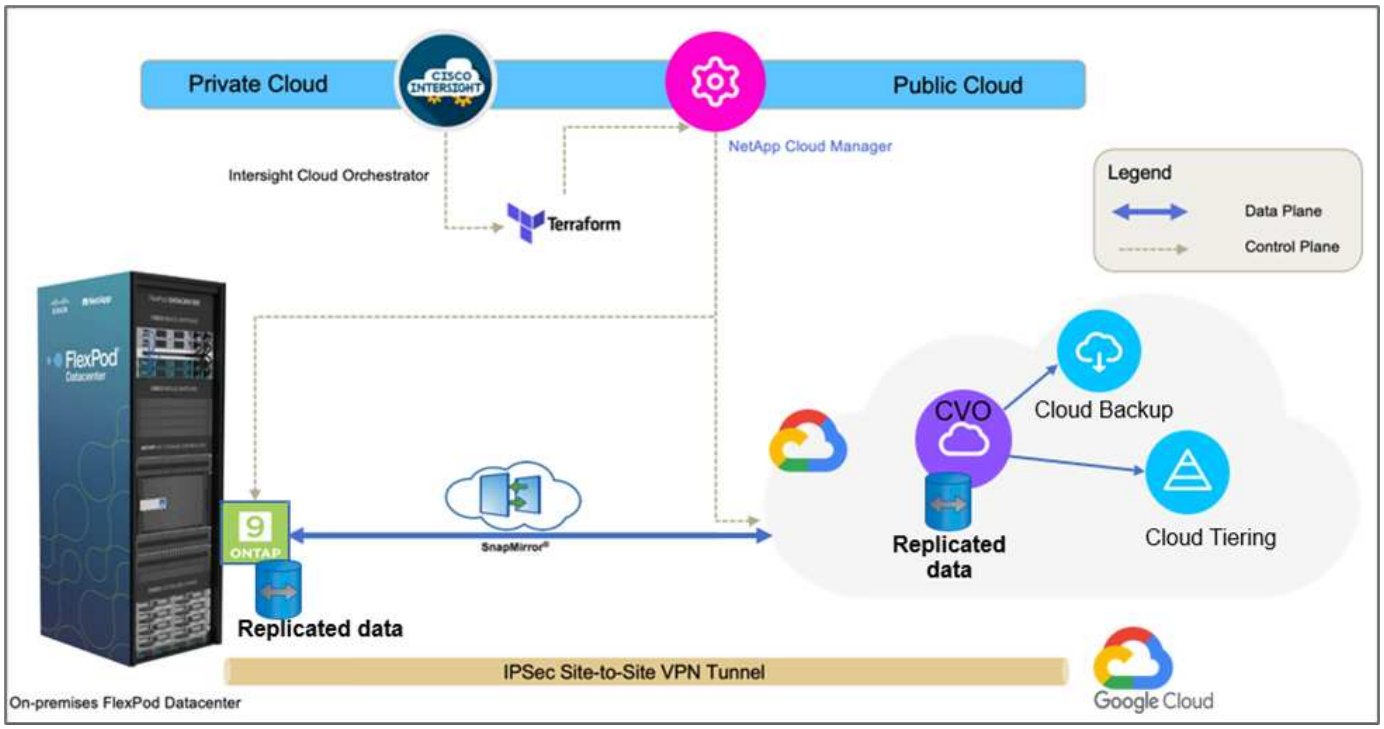
- **Orquestração e automação.** O Cisco Intersight simplifica as operações diárias da infraestrutura de nuvem híbrida da FlexPod com estruturas de orquestração consistentes fornecidas por meio de automação.
- * Proteção personalizada. * O Cloud Volumes ONTAP fornece replicação de dados em nível de bloco da ONTAP para a nuvem, o que mantém o destino atualizado por meio de atualizações incrementais. Os usuários podem especificar uma programação de sincronização a cada 5 minutos ou a cada hora, por exemplo, com base nas alterações na origem que são transferidas.
- * Failover contínuo e failback.* Quando ocorre um desastre, os administradores de storage podem fazer failover rapidamente para os volumes de nuvem. Quando o local principal é recuperado, os novos dados criados no ambiente de DR são sincronizados de volta para os volumes de origem, restabelecendo a replicação de dados secundários.
- **Eficiência:** o espaço de armazenamento e os custos da cópia de nuvem secundária são otimizados por meio do uso de compactação de dados, thin Provisioning e deduplicação. Os dados são transferidos no nível do bloco de forma comprimida e desduplicada, melhorando a velocidade de transferência. Os dados também são automaticamente dispostos em camadas em storage de objetos de baixo custo e somente retornados ao storage de alto desempenho quando acessados, como em um cenário de DR. Isso reduz significativamente os custos contínuos de storage.
- **Aumento da produtividade DE TI.** O uso do Intersight como a única plataforma segura de nível empresarial para gerenciamento do ciclo de vida da infraestrutura e do aplicativo simplifica o gerenciamento de configuração e a automação de tarefas manuais em escala para a solução.

Público-alvo

O público-alvo deste documento inclui, entre outros, engenheiros de vendas, consultores de campo, serviços profissionais, gerentes DE TI, engenheiros de parceiros, engenheiros de confiabilidade do site, arquitetos de nuvem, engenheiros de nuvem e clientes que desejam aproveitar uma infraestrutura criada para fornecer eficiência DE TI e permitir inovação DE TI.

Topologia da solução

Esta seção descreve a topologia lógica da solução. A figura a seguir representa a topologia da solução do ambiente FlexPod no local, do NetApp Cloud Volumes ONTAP executado no Google Cloud, do Cisco Intersight e do NetApp Cloud Manager.



Os planos de controlo e os planos de dados são claramente indicados entre os pontos finais. O plano de dados usa uma conexão VPN site a site segura para conetar a instância do ONTAP em execução no FlexPod All Flash FAS à instância do NetApp Cloud Volumes ONTAP no Google Cloud.

A replicação dos dados de workload do FlexPod para o NetApp Cloud Volumes ONTAP é gerenciada pelo NetApp SnapMirror, e o processo geral é orquestrado por meio do Cisco Intersight Cloud Orchestrator para ambientes locais e de nuvem. O Cisco Intersight Cloud Orchestrator consome os provedores de recursos Terraform para que o NetApp execute operações relacionadas à implantação do NetApp Cloud Volumes ONTAP e estabeleça relacionamentos de replicação de dados.

Essa solução também oferece suporte ao backup e à disposição em camadas opcionais de dados inativos que residem na instância do NetApp Cloud Volumes ONTAP no Google Cloud Storage.

"Próximo: Componentes da solução."

Componentes da solução

"Anterior: Visão geral da solução."

FlexPod

O FlexPod é um conjunto definido de hardware e software que forma uma base integrada para soluções virtualizadas e não virtualizadas. O FlexPod inclui storage NetApp ONTAP, rede Cisco Nexus, rede de storage Cisco MDS e sistema de computação unificada da Cisco (Cisco UCS). O design é flexível o suficiente para que a rede, a computação e o storage possam se encaixar em um rack de data center ou possa ser

implantado de acordo com o design do data center do cliente. A densidade da porta permite que os componentes de rede acomodem várias configurações.

Cisco Intersight

O Cisco Intersight é uma plataforma SaaS que oferece automação, observabilidade e otimização inteligentes para aplicações e infraestrutura tradicionais e nativas da nuvem. A plataforma ajuda a impulsionar a mudança com as equipes DE TI e fornece um modelo operacional projetado para a nuvem híbrida. O Cisco Intersight oferece os seguintes benefícios:

- * Entrega mais rápida. * Fornecido como um serviço a partir da nuvem ou no data center do cliente com atualizações frequentes e inovação contínua, devido a um modelo de desenvolvimento de software baseado em agilidade. Dessa forma, o cliente pode se concentrar em acelerar a entrega para a linha de negócios.
- **Operações simplificadas.** Simplifique as operações usando uma única ferramenta segura fornecida por SaaS com inventário, autenticação e APIs comuns para trabalhar em toda a stack e em todos os locais, eliminando silos entre as equipes. Desde o gerenciamento de servidores físicos e hipervisores no local, até VMs, K8s, sem servidor, automação, otimização e controle de custos nas nuvens locais e públicas.
- **Otimização contínua.** Otimize seu ambiente continuamente usando a inteligência fornecida pelo Cisco Intersight em todas as camadas, bem como o Cisco TAC. Essa inteligência é convertida em ações recomendadas e automatizáveis para que você possa adaptar em tempo real a cada mudança: Da movimentação de cargas de trabalho e monitoramento de integridade dos servidores físicos às recomendações de redução de custos das nuvens públicas com as quais você trabalha.

Existem dois modos de operações de gerenciamento possíveis com o Cisco Intersight: O modo gerenciado de UMM e o modo gerenciado de Intersight (IMM). Você pode selecionar UMM ou IMM nativos para sistemas Cisco UCS conetados à malha durante a configuração inicial das interconexões de malha. Nesta solução, IMM nativo é usado.

Licenciamento do Cisco Intersight

O Cisco Intersight usa uma licença baseada em subscrição com vários níveis.

Os níveis de licença do Cisco Intersight são os seguintes:

- **Cisco Intersight Essentials.** Inclui todas as funcionalidades básicas e os seguintes recursos:
  - Cisco Rio de Janeiro
  - Direito ao supervisor do IMC do Cisco
  - Configuração baseada em políticas com perfis de servidor
  - Gerenciamento de firmware
  - Avaliação da compatibilidade com a Lista de Compatibilidade de hardware (HCL)
- **Vantagem do Cisco Intersight.** Inclui os recursos e funcionalidades do nível Essentials, além dos seguintes recursos:
  - Widgets, inventário, capacidade, recursos de utilização e correlação de inventário entre domínios em computação física, rede, armazenamento, virtualização de VMware e nuvem pública da AWS.
  - O serviço de aconselhamento de segurança da Cisco, onde os clientes podem receber alertas de segurança importantes e avisos de campo sobre dispositivos endpoint afetados.
- **Cisco Intersight Premier.** Além dos recursos fornecidos no nível Advantage, o Cisco Intersight Premier oferece o seguinte:

- Intersight Cloud Orchestrator (ICO) para Cisco e plataformas de computação, rede, storage, sistemas integrados, virtualização, contêiner e nuvem pública de terceiros
- Direito de assinatura completo para o Cisco UCS diretor sem custo adicional.

Pode encontrar mais informações sobre o Licenciamento Intersight e os recursos suportados em cada licenciamento "aqui" .

> Nesta solução, usamos o Intersight Cloud Orchestrator e o Intersight Service for HashiCorp Terraform. Esses recursos estão disponíveis para usuários com a licença Intersight Premier, portanto, esse nível de licenciamento deve estar habilitado.

Integração da nuvem do Terraform com o ICO

Use o ICO (Cisco Intersight Cloud Orchestrator) para criar e executar fluxos de trabalho que chamam APIs do Terraform Cloud (TFC). A tarefa Invoke Web API Request oferece suporte ao Terraform Cloud como destino e pode ser configurada com APIs do Terraform Cloud usando métodos HTTP. Assim, o fluxo de trabalho pode ter uma combinação de tarefas que chama várias APIs do Terraform Cloud usando tarefas genéricas de API e outras operações. Você precisa de uma licença Premier para usar o recurso ICO.

Assistência de Intersight da Cisco

O Cisco Intersight Assist ajuda você a adicionar dispositivos de endpoint ao Cisco Intersight. Um data center pode ter vários dispositivos que não se conetam diretamente ao Cisco Intersight. Qualquer dispositivo que seja suportado pelo Cisco Intersight, mas não se conete diretamente a ele, requer um mecanismo de conexão. O Cisco Intersight Assist fornece esse mecanismo de conexão e ajuda você a adicionar dispositivos ao Cisco Intersight.

O Cisco Intersight Assist está disponível no dispositivo virtual Cisco Intersight, que é distribuído como uma máquina virtual implantável contida em um formato de arquivo Open Virtual Appliance (OVA). Você pode instalar o dispositivo em um servidor ESXi. Para obter mais informações, consulte "Guia de introdução ao dispositivo virtual Cisco Intersight" .

Depois de reivindicar o Intersight Assist no Intersight, você pode reivindicar dispositivos de endpoint usando a opção de solicitação através do Intersight Assist. Para obter mais informações, "Como começar"consulte .

NetApp Cloud Volumes ONTAP

- Utilização de deduplicação de dados incorporada, compressão, thin Provisioning e clonagem para minimizar os custos de storage.
- Fornecer confiabilidade empresarial e operações contínuas em caso de falhas no seu ambiente de nuvem.
- A Cloud Volumes ONTAP usa o NetApp SnapMirror, tecnologia de replicação líder do setor, para replicar dados no local para a nuvem, facilitando a disponibilização de cópias secundárias para vários casos de uso.
- O Cloud Volumes ONTAP também se integra ao Cloud Backup Service para fornecer recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de nuvem.
- Alternar entre pools de armazenamento de alto e baixo desempenho sob demanda sem colocar os aplicativos offline.
- Fornecendo consistência de cópias Snapshot usando o NetApp SnapCenter.
- O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.

- A integração com o Cloud Data Sense ajuda você a entender o contexto dos dados e identificar dados confidenciais.

Cloud Central

O Cloud Central fornece um local centralizado para acessar e gerenciar os serviços de dados de nuvem da NetApp. Com esses serviços, você executa aplicações críticas na nuvem, cria locais de recuperação de desastres automatizados, faz backup de seus dados SaaS e migra e controla dados com eficiência em várias nuvens. Para obter mais informações, "Cloud Central"consulte .

Cloud Manager

O Cloud Manager é uma plataforma de gerenciamento baseada em SaaS de classe empresarial que permite que especialistas DE TI e arquitetos de nuvem gerenciem centralmente sua infraestrutura multicloud híbrida usando as soluções de nuvem da NetApp. Ele fornece um sistema centralizado para visualização e gerenciamento do storage no local e na nuvem para dar suporte a vários provedores e contas de nuvem híbrida. Para obter mais informações, "Cloud Manager"consulte .

Conetor

O Connector permite que o Cloud Manager gerencie recursos e processos em um ambiente de nuvem pública. Uma instância do Connector é necessária para usar muitos recursos fornecidos pelo Cloud Manager e pode ser implantada na nuvem ou na rede local. O conetor é suportado nos seguintes locais:

- AWS
- Microsoft Azure
- Google Cloud
- No local

NetApp Active IQ Unified Manager

Com o NetApp Active IQ Unified Manager, você monitora seus clusters de storage do ONTAP a partir de uma interface única, redesenhada e intuitiva que fornece inteligência do conhecimento comunitário e análises de AI. Ele fornece insights operacionais, de desempenho e proativos abrangentes sobre o ambiente de storage e as máquinas virtuais que estão sendo executadas nele. Quando ocorre um problema com a infraestrutura de storage, o Unified Manager pode notificá-lo sobre os detalhes do problema para ajudar a identificar a causa raiz. O painel da máquina virtual fornece uma visão das estatísticas de desempenho da VM para que você possa investigar todo o caminho de e/S do host vSphere até a rede e, finalmente, até o armazenamento.

Alguns eventos também fornecem ações corretivas que você pode tomar para corrigir o problema. Você pode configurar alertas personalizados para eventos para que, quando os problemas ocorrem, você seja notificado por meio de traps de e-mail e SNMP. O Active IQ Unified Manager permite Planejar os requisitos de storage de seus usuários prevendo as tendências de capacidade e uso para agir proativamente antes que surjam problemas, evitando decisões reativas a curto prazo que podem levar a problemas adicionais a longo prazo.

VMware vSphere

O VMware vSphere é uma plataforma de virtualização para gerenciar holisticamente grandes coleções de infraestruturas (recursos incluindo CPUs, armazenamento e rede) como um ambiente operacional otimizado, versátil e dinâmico. Ao contrário dos sistemas operacionais tradicionais que gerenciam uma máquina individual, o VMware vSphere agrega a infraestrutura de um data center inteiro para criar uma única potência com recursos que podem ser alocados de forma rápida e dinâmica para qualquer aplicativo necessário.

Para obter mais informações sobre o VMware vSphere, siga "este link".

VMware vSphere vCenter

O VMware vCenter Server fornece gerenciamento unificado de todos os hosts e VMs a partir de um único console e agrega o monitoramento de desempenho de clusters, hosts e VMs. O VMware vCenter Server oferece aos administradores uma visão profunda sobre o status e a configuração de clusters de computação, hosts, VMs, armazenamento, SO convidado e outros componentes críticos de uma infraestrutura virtual. O VMware vCenter gerencia o rico conjunto de recursos disponíveis em um ambiente VMware vSphere.

Versões de hardware e software

Essa solução de nuvem híbrida pode ser estendida a qualquer ambiente FlexPod que esteja executando versões compatíveis de software, firmware e hardware, conforme definido na ferramenta de Matriz de interoperabilidade do NetApp e na Lista de Compatibilidade de hardware do Cisco UCS.

A solução FlexPod usada como plataforma de linha de base em nosso ambiente local foi implantada de acordo com as diretrizes e especificações descritas "aqui".

A rede dentro deste ambiente é baseada em ACI. Para obter mais informações, "aqui"consulte .

- Consulte os links a seguir para obter mais informações:
- "Ferramenta de Matriz de interoperabilidade do NetApp"
- "Guia de compatibilidade da VMware"
- "Ferramenta de interoperabilidade de hardware e software Cisco UCS"

A tabela a seguir mostra as revisões de hardware e software do FlexPod.

Componente	Produto	Versão
Computação	Cisco UCS X210C-M6	5,0 mm (1b mm)
	O tecido Cisco UCS interconeta 6454	4,2 mm (2a mm)
Rede	Cisco Nexus 9332C (coluna)	14,2 mm (7s mm)
	Cisco Nexus 9336C-FX2 (Folha)	14,2 mm (7s mm)
	ACI do Cisco	4,2 mm (7s mm)
Armazenamento	NetApp AFF A220	9.11.1
	Ferramentas do NetApp ONTAP para VMware vSphere	9,10
	Plug-in NFS NetApp para VMware VAAI	2,0-15
	Active IQ Unified Manager	9,11
Software	VSphere ESXi	7,0 MM (U3 MM)
	Dispositivo VMware vCenter	7.0.3
	Dispositivo virtual de assistência à monitorização da distância da Cisco	1,0.11-306

A execução das configurações do Terraform acontece na conta do Terraform Cloud for Business. A configuração do Terraform usa o provedor Terraform para o NetApp Cloud Manager.

A tabela a seguir lista os fornecedores, produtos e versões.

Componente	Produto	Versão
HashiCorp	Terraform	1.2.7

A tabela a seguir mostra as versões do Cloud Manager e do Cloud Volumes ONTAP.

Componente	Produto	Versão
NetApp	Cloud Volumes ONTAP	9,11
	Cloud Manager	3.9.21

"Próximo: Instalação e configuração - implantar FlexPod."

Instalação e configuração

Implante o FlexPod

"Anterior: Componentes da solução."

Para entender os detalhes de projeto e implantação do FlexPod, incluindo a configuração de vários elementos do design e as práticas recomendadas associadas, "Cisco Validated designs para FlexPod" consulte .

O FlexPod pode ser implantado no modo gerenciado UCS e no modo gerenciado pelo Cisco Intersight. Se você estiver implantando o FlexPod no modo gerenciado do UCS, o projeto validado do Cisco mais recente pode ser "aqui"encontrado .

O sistema de computação unificado (Cisco UCS) da Cisco X-Series é um novo sistema de computação modular, configurado e gerenciado a partir da nuvem. Ele foi projetado para atender às necessidades de aplicações modernas e para melhorar a eficiência operacional, agilidade e escala por meio de um design modular adaptável e pronto para o futuro. Encontre as orientações de design sobre a incorporação da plataforma UCS X-Series gerenciada pelo Cisco Intersight na infraestrutura do FlexPod "aqui" .

FlexPod com implantação ACI Cisco pode ser encontrado "aqui".

"Próximo: Configuração do Cisco Intersight."

Configuração do Cisco Intersight

"Anterior: Implantar FlexPod."

Para configurar o Cisco Intersight e o Intersight Assist, consulte os Cisco Validated designs for FlexPod Found . "aqui"

"Próximo: Pré-requisito da integração da nuvem do Terraform com ICO."

Pré-requisito do Terraform Cloud Integration com ICO

"Anterior: Configuração do Cisco Intersight."

Procedimento 1: Conete o Cisco Intersight e o Terraform Cloud

1. Solicite ou crie um destino de nuvem do Terraform fornecendo os detalhes relevantes da conta do Terraform Cloud.
2. Crie um destino do Terraform Cloud Agent para nuvens privadas para que os clientes possam instalar o agente no data center e ativar a comunicação com o Terraform Cloud.

   Para obter mais informações, siga "este link".

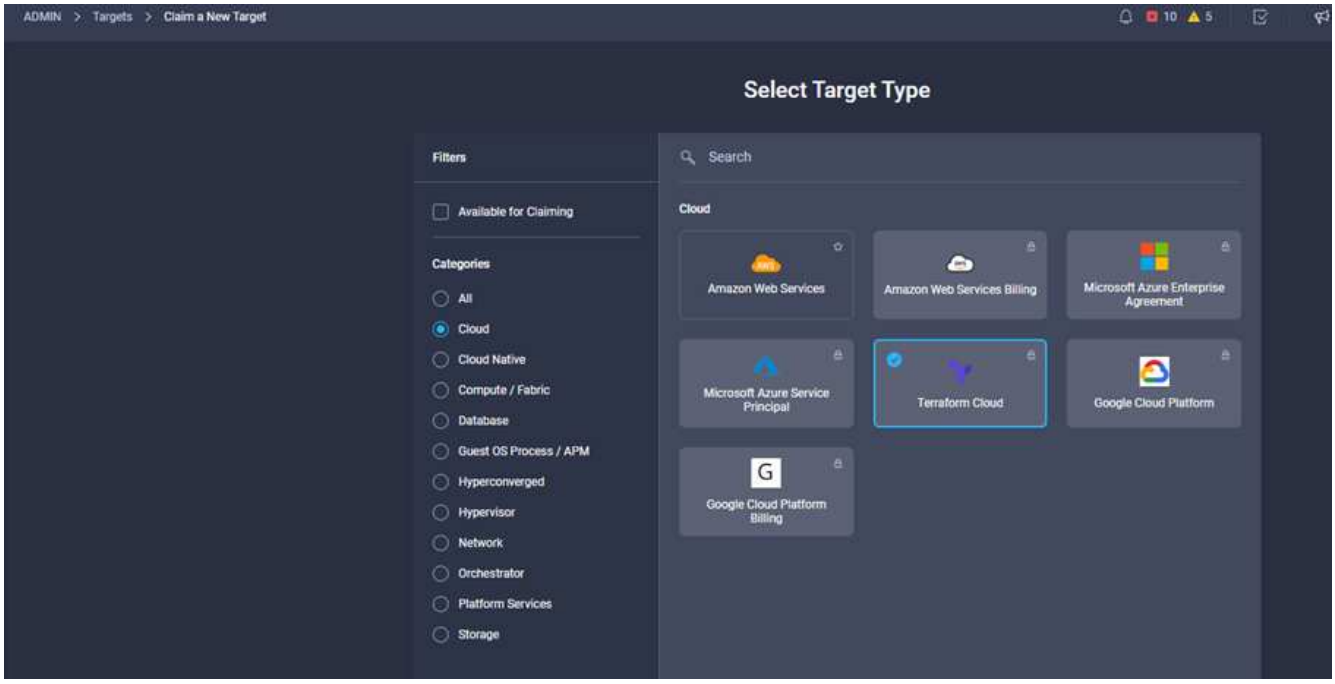
Procedimento 2: Gerar token de usuário

Como parte da adição de um destino para o Terraform Cloud, você deve fornecer o nome de usuário e o token da API na página de configurações do Terraform Cloud.

1. Faça login no Terraform Cloud e vá para **tokens de usuário**: "https://app.terraform.io/app/settings/tokens".
2. Clique em **criar um novo token de API**.
3. Atribua um nome para lembrar e salve o token em um local seguro.

Procedimento 3: Solicite o Terraform Cloud Target

1. Inicie sessão no Intersight com o Administrador de conta, o Administrador de dispositivo ou o Técnico de dispositivos Privileges.
2. Navegue até **ADMIN > Targets > reivindicar um novo alvo**.
3. Em **categorias**, clique em **nuvem**.
4. Clique em **Terraform Cloud** e clique em **Iniciar**.



5. Insira um nome para o destino, seu nome de usuário para o Terraform Cloud, o token da API e uma

organização padrão no Terraform Cloud, conforme exibido na imagem a seguir.

6. No campo **Default Managed hosts**, certifique-se de adicionar os seguintes links junto com outros hosts gerenciados:
   - github.com
   - github-releases.githubusercontent.com

Se tudo for inserido corretamente, você verá o destino do Terraform Cloud exibido na seção **Intersight Targets**.

Procedimento 4: Adicionar agentes Terraform Cloud

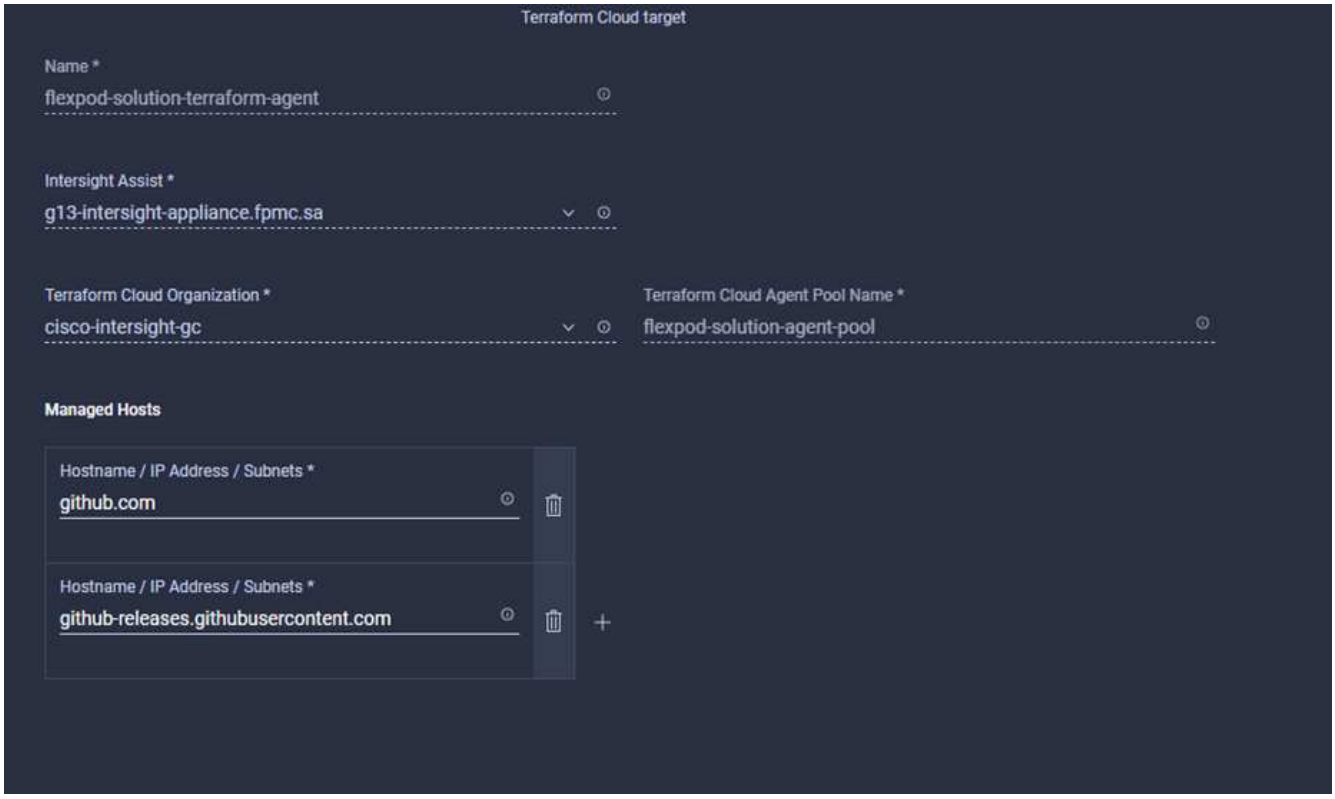
Pré-requisitos:

- Destino do Terraform Cloud.
- Reivindicou o Intersight Assist no Intersight antes de implantar o Terraform Cloud Agent.

Só é possível solicitar cinco agentes para cada assistência.

Depois de criar a conexão com o Terraform, é necessário ativar um Terraform Agent para executar o código Terraform.

1. Clique em **solicitar o Terraform Cloud Agent** na lista suspensa do destino do Terraform Cloud.
2. Insira os detalhes do agente Terraform Cloud. A captura de tela a seguir mostra os detalhes de configuração do agente Terraform.



Você pode atualizar qualquer propriedade do Terraform Agent. Se o destino estiver no estado **não conetado** e nunca estiver no estado **conetado**, um token não foi gerado para o agente Terraform.

Depois que a validação do agente for bem-sucedida e um token de agente for gerado, você não poderá reconfigurar a Organização e/ou o pool de agentes. A implantação bem-sucedida de um agente Terraform é indicada por um status **conectado**.

Depois de ativar e reivindicar a integração do Terraform Cloud, você pode implantar um ou mais agentes do Terraform Cloud no Cisco Intersight Assist. O agente Terraform Cloud é modelado como um destino filho do destino Terraform Cloud. Ao reivindicar o destino do agente, você verá uma mensagem indicando que o pedido de destino está em andamento.

Após alguns segundos, o destino é movido para o estado **conectado** e a plataforma Intersight roteia pacotes HTTPS do agente para o gateway Terraform Cloud.

Seu Terraform Agent deve ser reivindicado corretamente e deve aparecer em alvos como **conectado**.

"Próximo: Configurar provedor de serviços de nuvem pública."

Configure o provedor de serviços de nuvem pública

"Anterior: Integração da nuvem Terraform com o pré-requisito da ICO."

Procedimento 1: Acesse o Gerenciador de nuvem do NetApp

Para acessar o NetApp Cloud Manager e outros serviços de nuvem, você precisa se inscrever "Centro de nuvem da NetApp" no .

Para configurar espaços de trabalho e usuários na conta do Cloud Central, clique "aqui"em .

Procedimento 2: Conetor de ativação

Para implantar o conetor no Google Cloud, consulte este "link".

"Próximo: Implantação automatizada do storage NetApp de nuvem híbrida."

Implantação automatizada de storage de nuvem híbrida NetApp

"Anterior: Configurar provedor de serviços de nuvem pública."

Google Cloud

Primeiro, é necessário habilitar APIs e criar uma conta de serviço que forneça ao Cloud Manager permissões para implantar e gerenciar sistemas Cloud Volumes ONTAP que estejam no mesmo projeto que o conetor ou em projetos diferentes.

Antes de implantar um conetor em um projeto do Google Cloud, verifique se o conetor não está sendo executado no local ou em um provedor de nuvem diferente.

Dois conjuntos de permissões devem estar em vigor antes de implantar um conetor diretamente do Cloud Manager:

- Você precisa implantar o Connector usando uma conta do Google que tenha permissões para iniciar a instância de VM do Connector do Cloud Manager.
- Ao implantar o Connector, você será solicitado a selecionar a instância de VM. O Cloud Manager obtém permissões da conta de serviço para criar e gerenciar sistemas Cloud Volumes ONTAP em seu nome. As permissões são fornecidas anexando uma função personalizada à conta de serviço. Você precisa configurar dois arquivos YAML que incluem as permissões necessárias para o usuário e a conta de serviço. Saiba como usar "Os arquivos YAML para configurar permissões" aqui.

```
https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6["este vídeo detalhado"^]Consulte para obter todos os pré-requisitos necessários.
```

Modos de implantação e arquitetura do Cloud Volumes ONTAP

O Cloud Volumes ONTAP está disponível no Google Cloud como um sistema de nó único e como um par de nós de alta disponibilidade (HA). Com base nos requisitos, podemos escolher o modo de implantação do Cloud Volumes ONTAP. A atualização de um único sistema de nós para um par de HA não é compatível. Para alternar entre um sistema de nó único e um par de HA, você precisa implantar um novo sistema e replicar dados do sistema existente para o novo sistema.

Cloud Volumes ONTAP altamente disponível no Google Cloud

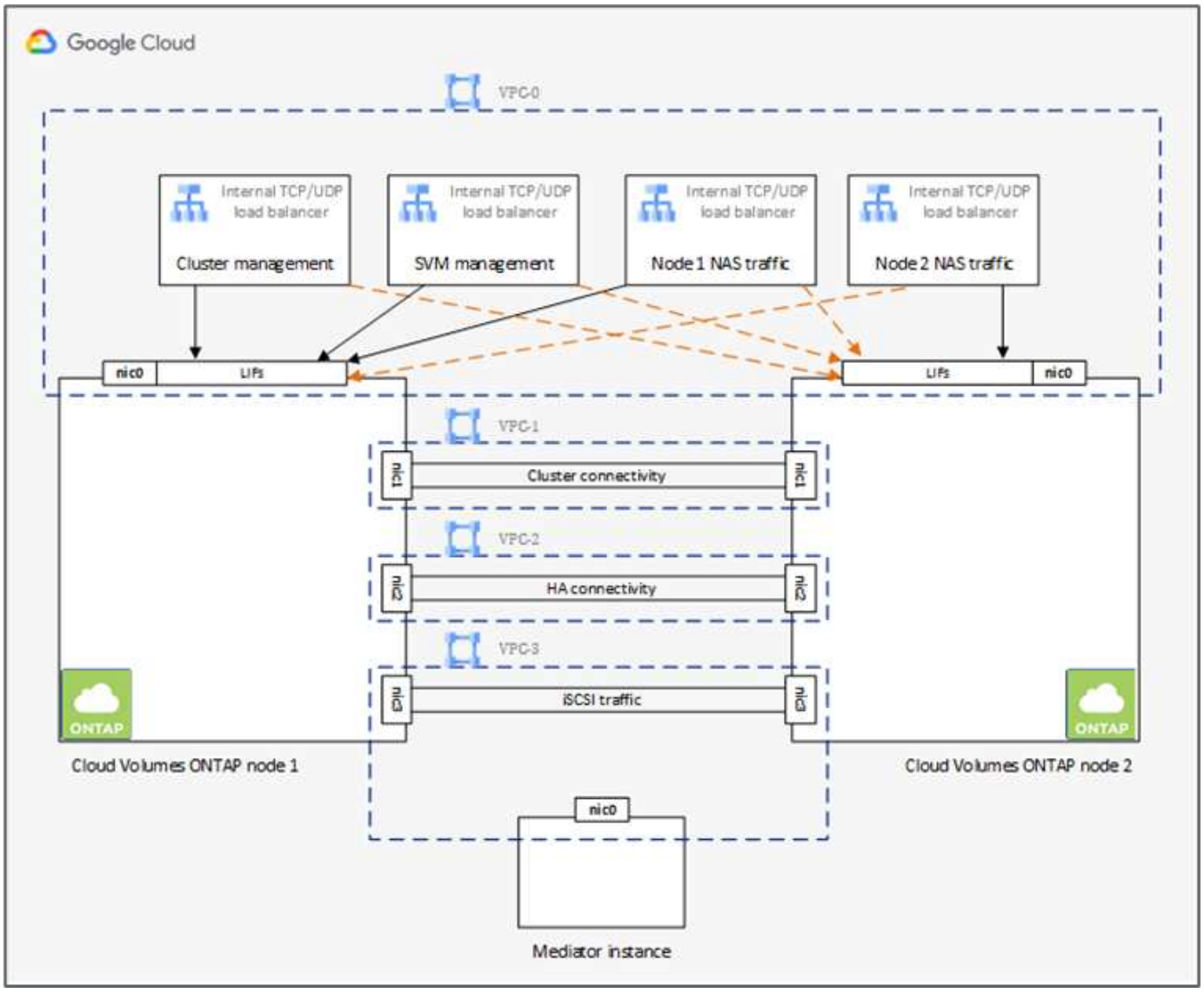
O Google Cloud é compatível com a implantação de recursos em várias regiões geográficas e várias zonas dentro de uma região. A implantação de HA consiste em dois nós de ONTAP que usam poderosos tipos de máquina padrão n1 ou n2, disponíveis no Google Cloud. Os dados são replicados em sincronia entre os dois nós do Cloud Volumes ONTAP para fornecer disponibilidade em caso de falha. A implantação DE HA do Cloud Volumes ONTAP requer quatro VPCs e uma sub-rede privada em cada VPC. As sub-redes nos quatro

VPCs devem ser provisionadas com intervalos CIDR não sobrepostos.

Os quatro VPCs são usados para os seguintes fins:

- O VPC 0 permite a comunicação de entrada para os nós de dados e Cloud Volumes ONTAP.
- O VPC 1 fornece conectividade de cluster entre nós do Cloud Volumes ONTAP.
- A VPC 2 permite replicação de RAM (NVRAM) não volátil entre nós.
- O VPC 3 é usado para conetividade com a instância do mediador de HA e o tráfego de replicação de disco para reconstruções de nós.

A imagem a seguir mostra um Cloud Volumes ONTAP altamente disponível na nuvem Goggle.



Para obter detalhes, "este link" consulte .

Para obter os requisitos de rede do Cloud Volumes ONTAP no Google Cloud, "este link" consulte .

Para obter detalhes sobre a disposição de dados em camadas, "este link"consulte .

Configurar pré-requisitos de ambiente

A criação automatizada de clusters do Cloud Volumes ONTAP, a configuração do SnapMirror entre um volume local e um volume de nuvem, a criação de um volume de nuvem etc. são realizadas com a configuração do Terraform. Essas configurações do Terraform são hospedadas em uma conta do Terraform Cloud for Business. Com o Intersight Cloud Orchestrator, você pode orquestrar tarefas como criar uma área de trabalho em uma conta do Terraform Cloud for Business, adicionar todas as variáveis necessárias à área de trabalho, executar um plano Terraform etc.

Para essas tarefas de automação e orquestração, há alguns requisitos e dados necessários, conforme descrito nas seções a seguir.

Repositório do GitHub

Você precisa de uma conta do GitHub para hospedar seu código Terraform. O Intersight Orchestrator cria um novo espaço de trabalho na conta Terraform Cloud for Business. Esta área de trabalho é configurada com um fluxo de trabalho de controle de versão. Para isso, você precisa manter a configuração do Terraform em um repositório do GitHub e fornecê-la como uma entrada ao criar o workspace.

"Este link do GitHub" Fornece a configuração do Terraform com vários recursos. Você pode fazer um fork deste repositório e fazer uma cópia na sua conta do GitHub.

Neste repositório, `provider.tf` tem a definição para o provedor Terraform necessário. O provedor Terraform para o Gerenciador de nuvem do NetApp é usado.

`variables.tf` tem todas as declarações variáveis. O valor para essas variáveis é inserido como entrada de fluxo de trabalho do Intersight Cloud Orchestrator. Isso fornece uma maneira conveniente de passar valores para uma área de trabalho e executar a configuração do Terraform.

`resources.tf` Define os vários recursos necessários para adicionar um ONTAP no local ao ambiente de trabalho, criar um cluster de nó único do Cloud Volumes ONTAP no Google Cloud, estabelecer uma relação do SnapMirror entre o local e o Cloud Volumes ONTAP, criar um volume de nuvem no Cloud Volumes ONTAP etc.

Neste repositório:

- `provider.tf` Tem o NetApp Cloud Manager como uma definição para o provedor Terraform necessário.
- `variables.tf` Tem as declarações de variável que são usadas como entrada para o fluxo de trabalho do Intersight Cloud Orchestrator. Isso fornece uma maneira conveniente de passar valores para a área de trabalho e executar a configuração do Terraform.
- `resources.tf` Define vários recursos para adicionar um ONTAP local ao ambiente de trabalho, criar um cluster Cloud Volumes ONTAP de nó único no Google Cloud, estabelecer uma relação SnapMirror entre o local e o Cloud Volumes ONTAP, criar um volume de nuvem no Cloud Volumes ONTAP etc.

Você pode adicionar um bloco de recursos adicional para criar vários volumes no Cloud Volumes ONTAP ou usar construções Count ou `for_each` Terraform.

Para conetar espaços de trabalho, módulos e conjuntos de políticas do Terraform aos repositórios git que contêm configurações do Terraform, o Terraform Cloud precisa de acesso ao repositório do GitHub.

Adicione um cliente e o ID do token OAuth do cliente é usado como uma das entradas de fluxo de trabalho do Intersight Cloud Orchestrator.

1. Faça login na sua conta do Terraform Cloud for Business. Navegue até **Definições > fornecedores**.

2. Clique em **Adicionar um provedor VCS**.
3. Selecione a sua versão.
4. Siga as etapas em **Configurar provedor**.
5. Você vê o cliente adicionado em **provedores VCS**. Anote o ID do token OAuth.

Atualizar token para operações da API do NetApp Cloud Manager

Além da interface do navegador da Web, o Cloud Manager tem uma API REST que fornece aos desenvolvedores de software acesso direto à funcionalidade do Cloud Manager por meio da interface SaaS. O serviço Cloud Manager consiste em vários componentes distintos que formam coletivamente uma plataforma de desenvolvimento extensível. O token de atualização permite gerar tokens de acesso que você adiciona ao cabeçalho de autorização para cada chamada de API.

Sem chamar uma API diretamente, o provedor NetApp-cloudmanager usa um token de atualização e traduz os recursos do Terraform em chamadas de API correspondentes. Você precisa gerar um token de atualização para as operações da API do NetApp Cloud Manager a partir "Centro de nuvem da NetApp"do .

Você precisa da ID do cliente do conetor do Cloud Manager para criar recursos no Cloud Manager, como criar um cluster Cloud Volumes ONTAP, configurar o SnapMirror, etc.

1. Entre no Cloud Manager: "https://cloudmanager.netapp.com/".
2. Clique em **Connector**.
3. Clique em **Gerenciar conetores**.
4. Clique nas elipses e copie a ID do conetor.

Desenvolva o fluxo de trabalho do Cisco Intersight Cloud Orchestrator

O Cisco Intersight Cloud Orchestrator está disponível no Cisco Intersight se:

- Você instalou a licença Intersight Premier.
- Você é um administrador de conta, administrador de armazenamento, administrador de virtualização ou administrador de servidor e tem um mínimo de um servidor atribuído a você.

Designer de fluxo de trabalho

O Designer de fluxo de trabalho ajuda você a criar novos fluxos de trabalho (bem como tarefas e tipos de dados) e editar fluxos de trabalho existentes para gerenciar destinos no Cisco Intersight.

Para iniciar o Workflow Designer, vá para **Orchestration > workflows**. Um painel exibe os seguintes detalhes nas guias **Meus fluxos de trabalho**, **fluxos de trabalho de amostra** e **todos os fluxos de trabalho**:

- Estado de validação
- Estado da última execução
- Principais fluxos de trabalho por contagem de execução
- Principais categorias de fluxo de trabalho
- Número de fluxos de trabalho definidos pelo sistema
- Principais fluxos de trabalho por destinos

Usando o painel, você pode criar, editar, clonar ou excluir uma guia. Para criar sua própria guia de exibição

personalizada, clique em ***, especifique um nome e selecione os parâmetros necessários que precisam ser exibidos nas colunas, colunas de tag e widgets. Você pode renomear uma guia se ela não tiver um ícone *Lock**.

No painel, há uma lista tabular de fluxos de trabalho que exibe as seguintes informações:

- Nome de exibição
- Descrição
- Definido pelo sistema
- Versão padrão
- Execuções
- Estado da última execução
- Estado de validação
- Última atualização
- Organização

A coluna ações permite executar as seguintes ações:

- **Execute.** Executa o fluxo de trabalho.
- **História.** Exibe o histórico de execução do fluxo de trabalho.
- **Gerenciar versões.** Crie e gerencie versões para fluxos de trabalho.
- **Excluir.** Eliminar um fluxo de trabalho.
- **Repetir.** Tente novamente um fluxo de trabalho com falha.

Fluxo de trabalho

Crie um fluxo de trabalho que consiste nos seguintes passos:

- **Definindo um fluxo de trabalho.** Especifique o nome de exibição, a descrição e outros atributos importantes.
- **Definir entradas de fluxo de trabalho e saídas de fluxo de trabalho.** Especifique quais parâmetros de entrada são obrigatórios para a execução do fluxo de trabalho e as saídas geradas na execução bem-sucedida
- **Adicionar tarefas de fluxo de trabalho.** Adicione uma ou mais tarefas de fluxo de trabalho no Designer de fluxo de trabalho necessárias para que o fluxo de trabalho execute sua função.
- *Validar o fluxo de trabalho. *Validar um fluxo de trabalho para garantir que não haja erros na conexão de entradas e saídas de tarefas.

Criar fluxos de trabalho para storage FlexPod no local

Para configurar um fluxo de trabalho para o storage FlexPod no local, "este link"consulte .

"Próximo: Fluxo de trabalho de DR."

Fluxo de trabalho da DR

"Anterior: Implantação automatizada de storage NetApp de nuvem híbrida."

A sequência de passos é a seguinte:

1. Defina o fluxo de trabalho.
   - Crie um nome curto e fácil de usar para o fluxo de trabalho, como o Disaster Recovery Workflow.
2. Defina a entrada de fluxo de trabalho. As entradas que tomamos para este fluxo de trabalho incluem o seguinte:
   - Opções de volume (nome do volume, caminho de montagem)
   - Capacidade de volume
   - Data center associado ao novo datastore
   - Cluster no qual o datastore está hospedado
   - Nome do novo datastore a ser criado no vCenter
   - Tipo e versão do novo datastore
   - Nome da organização do Terraform
   - Área de trabalho do Terraform
   - Descrição da área de trabalho do Terraform
   - Variáveis (sensíveis e não sensíveis) necessárias para executar a configuração do Terraform
   - Motivo para iniciar o plano
3. Adicione as tarefas de fluxo de trabalho.

   As tarefas relacionadas a operações no FlexPod incluem o seguinte:

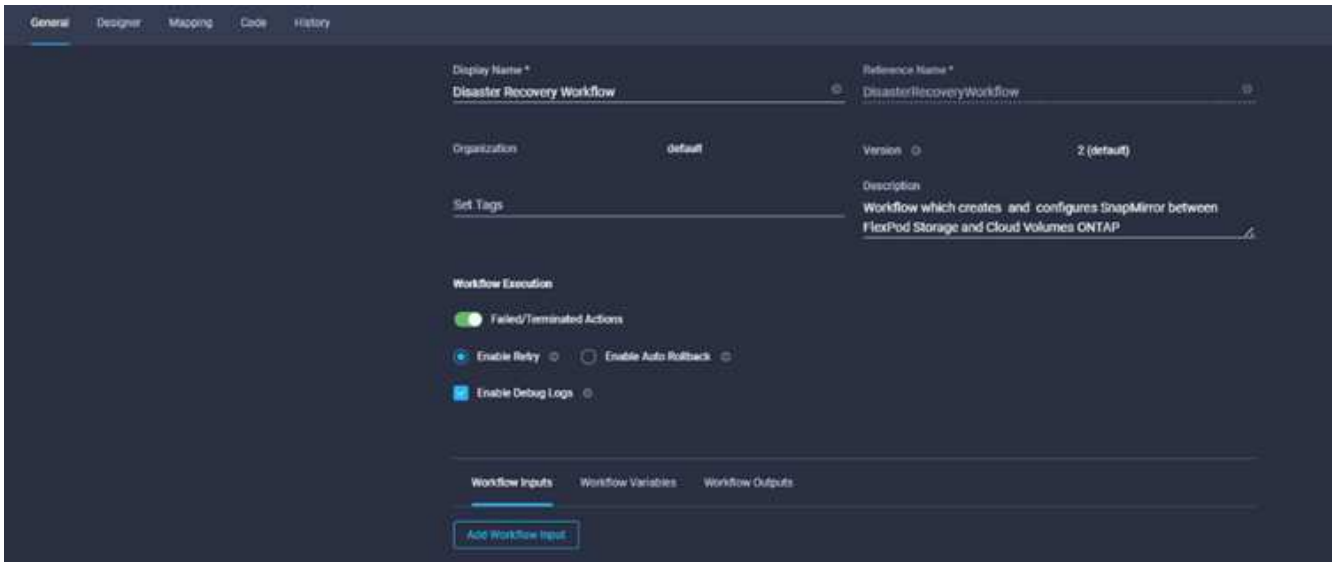
   - Criar volume no FlexPod.
   - Adicionar política de exportação de armazenamento ao volume criado.
   - Mapeie o volume recém-criado para um datastore no VMware vCenter.

     As tarefas relacionadas à criação do cluster Cloud Volumes ONTAP:

   - Adicione o espaço de trabalho do Terraform
   - Adicione variáveis Terraform
   - Adicione variáveis sensíveis ao Terraform
   - Inicie o novo plano Terraform
   - Confirme a execução do Terraform
4. Valide o fluxo de trabalho.

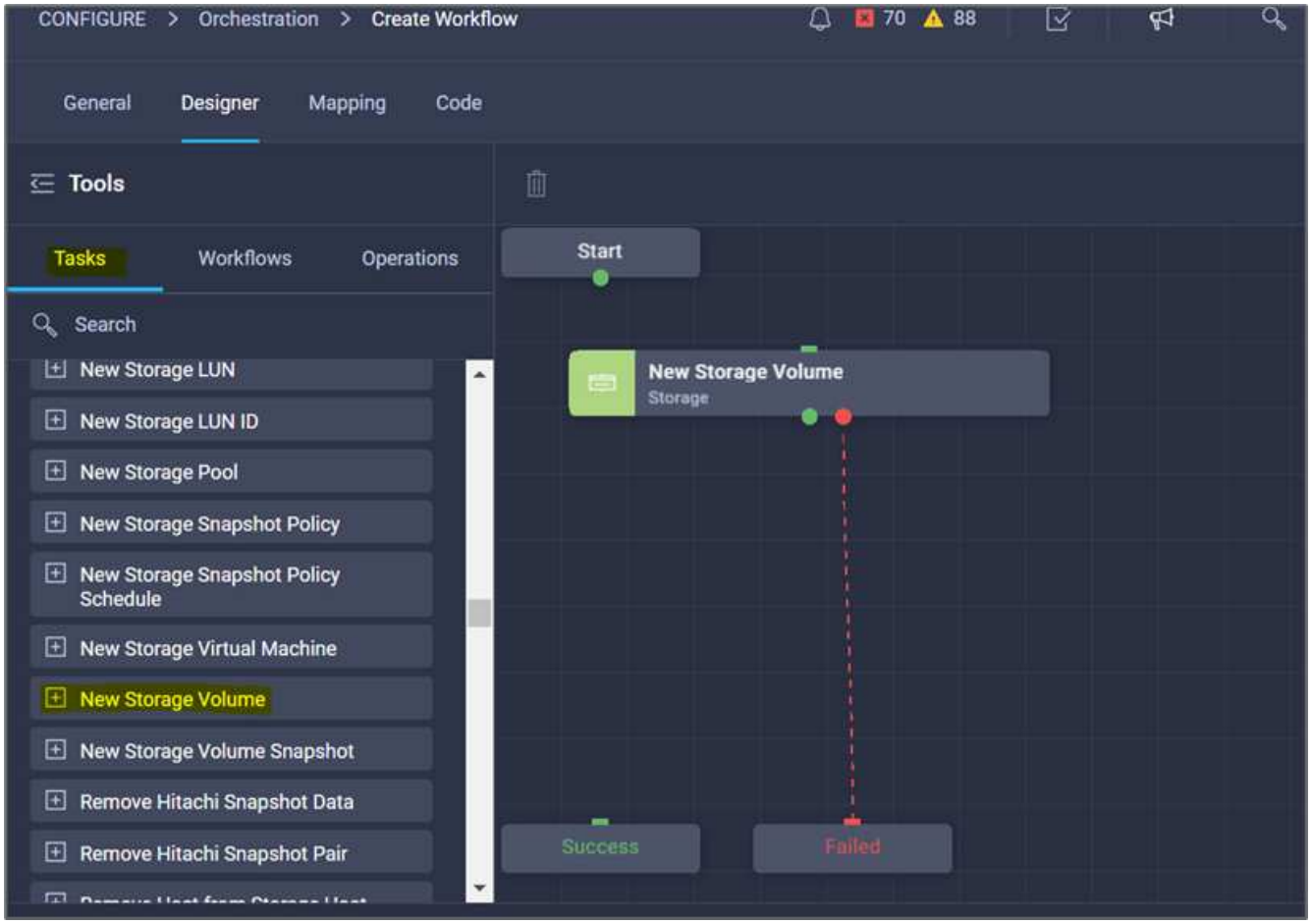
Procedimento 1: Crie o fluxo de trabalho

1. Clique em **Orchestration** no painel de navegação esquerdo e clique em **Create Workflow**.
2. No separador **Geral**:
   a. Forneça o nome de exibição (Disaster Recovery Workflow).
   b. Selecione a organização, defina tags e forneça uma descrição.
3. Clique em Guardar.

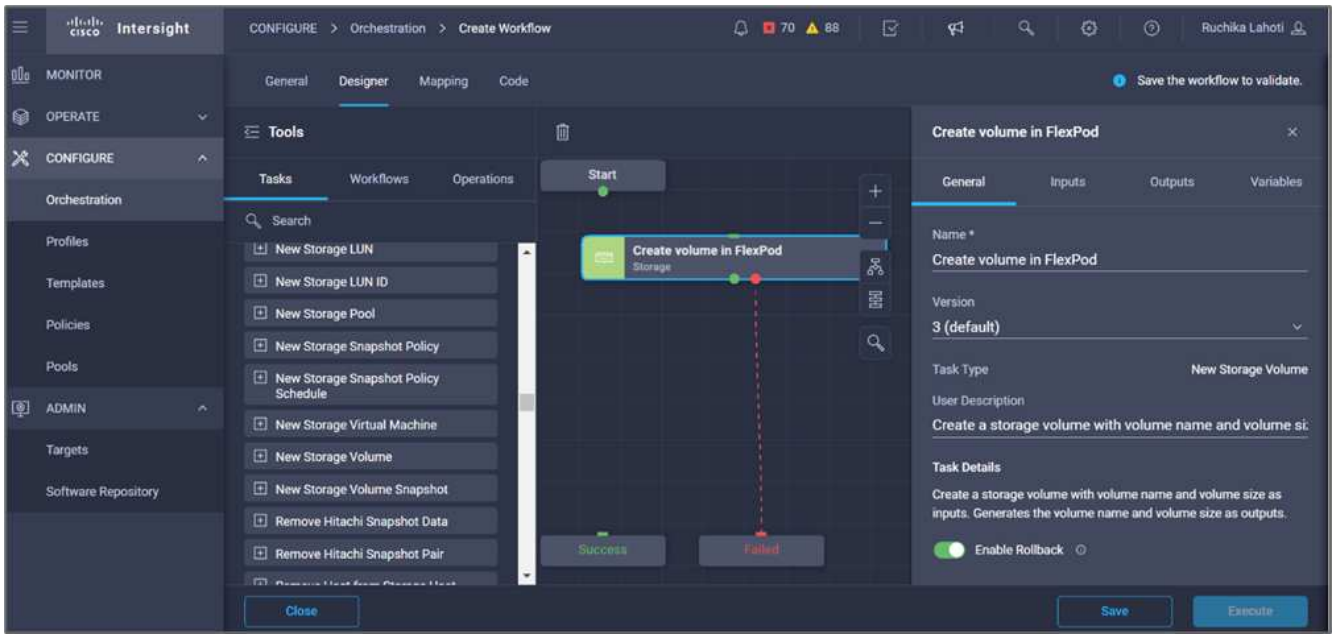


Procedimento 2. Crie um novo volume no FlexPod

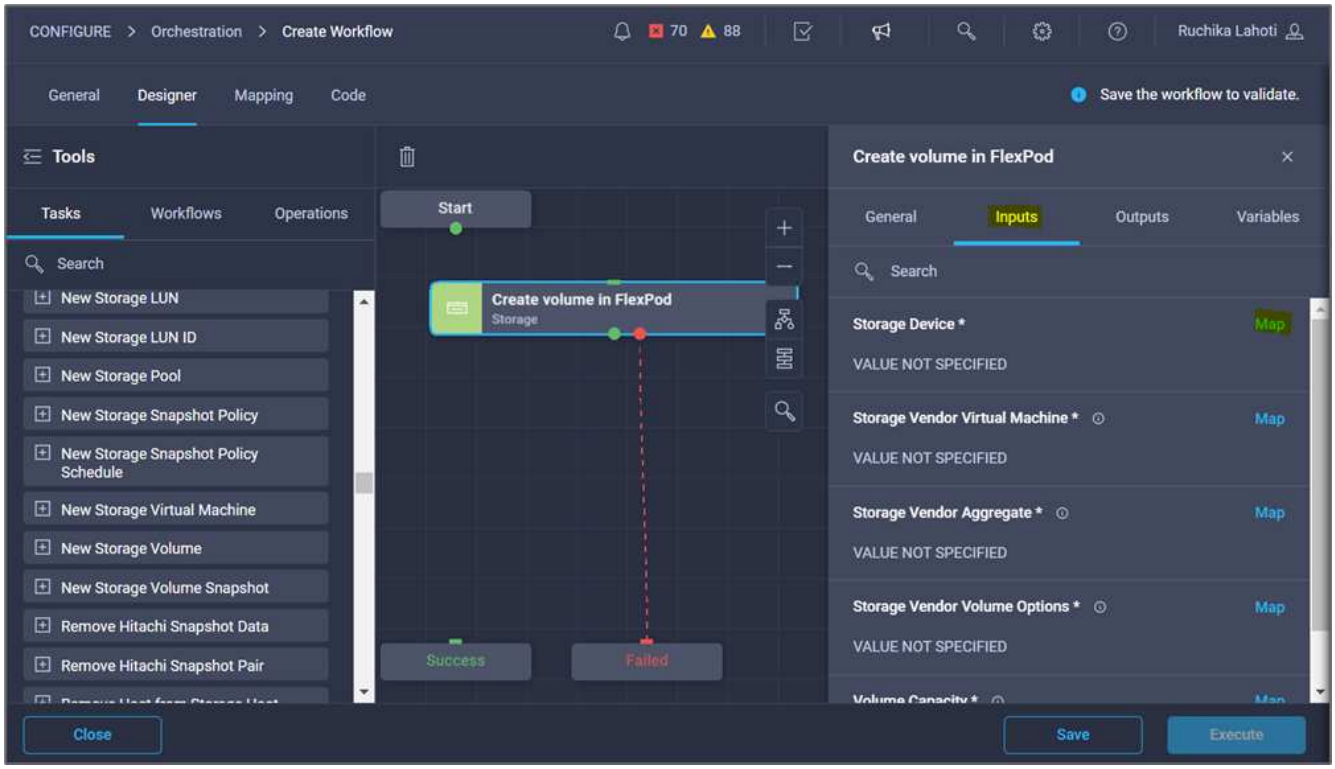
1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte a tarefa **armazenamento > novo volume de armazenamento** da seção **Ferramentas** na área **Design**.
3. Clique em **novo volume de armazenamento**.



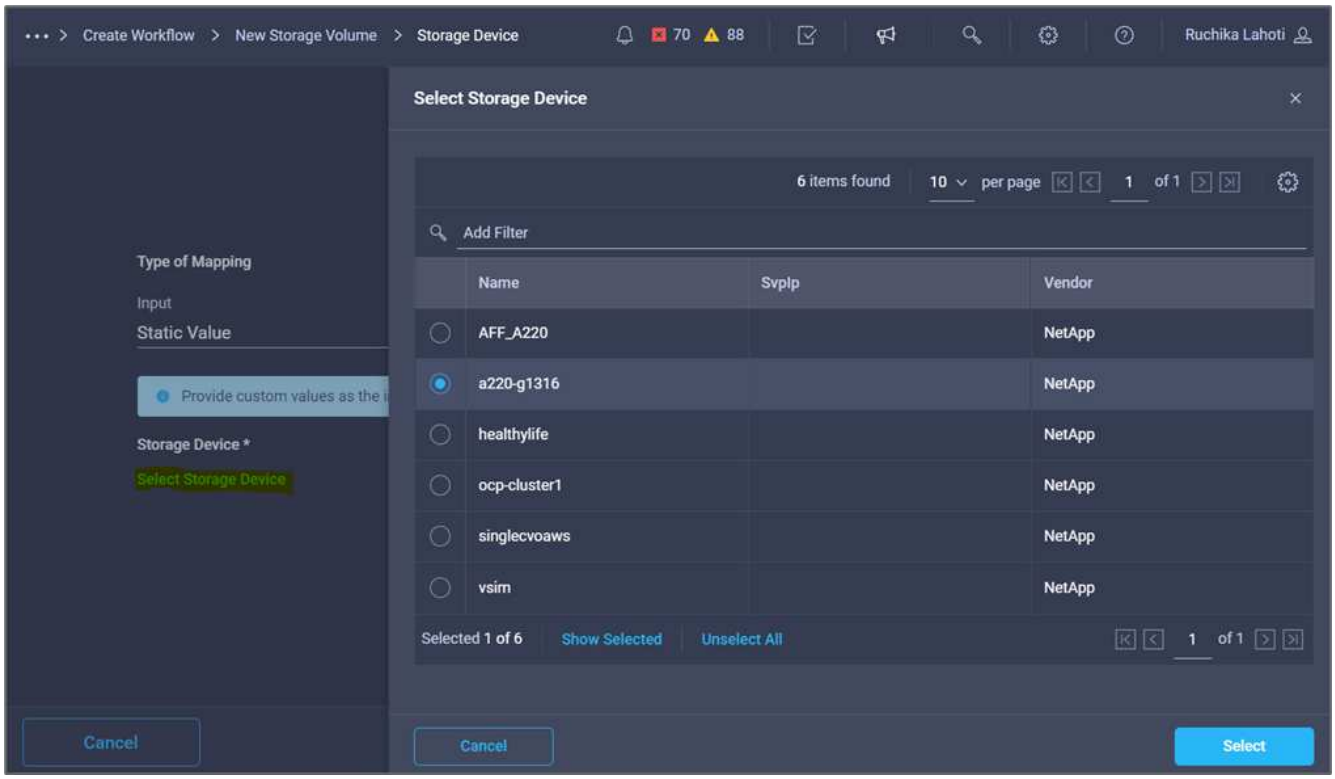
4. Na área **Propriedades da tarefa**, clique na guia **Geral**. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa. Neste exemplo, o nome da tarefa é **criar volume no FlexPod**.



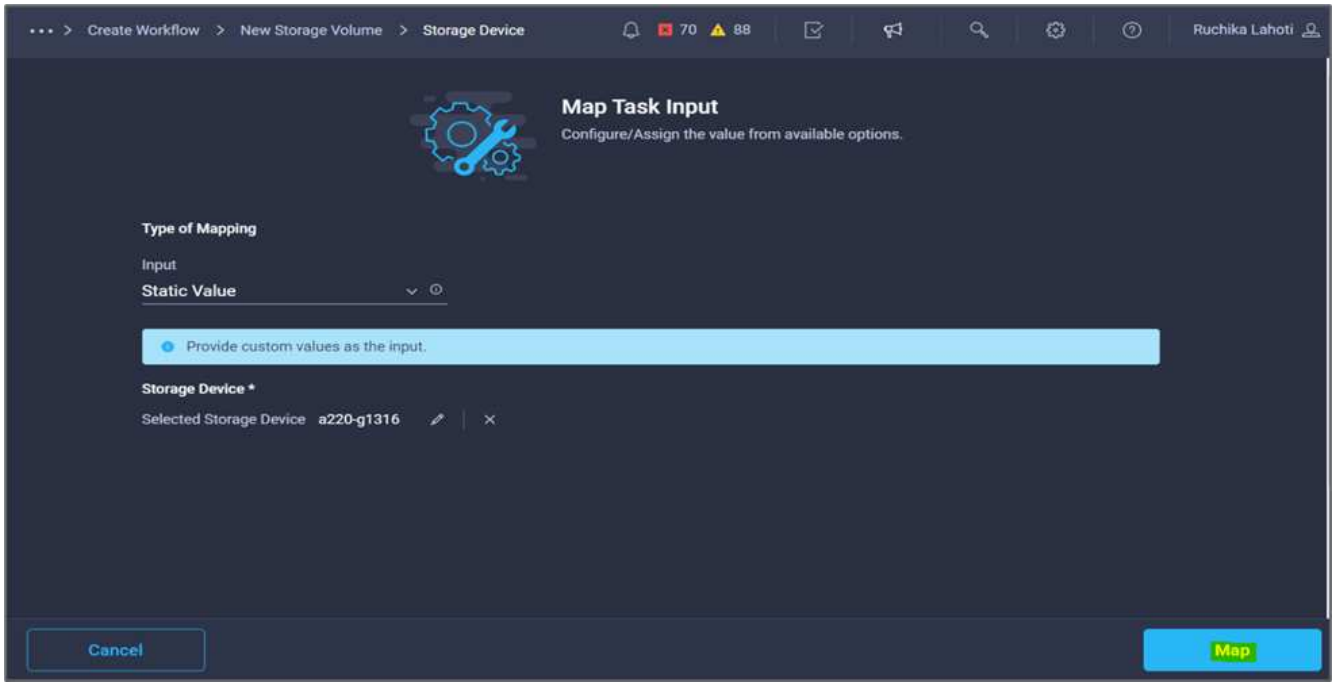
5. Na área **Task Properties**, clique em **Inputs**.
6. Clique em **Map** no campo **Storage Device** (dispositivo de armazenamento).



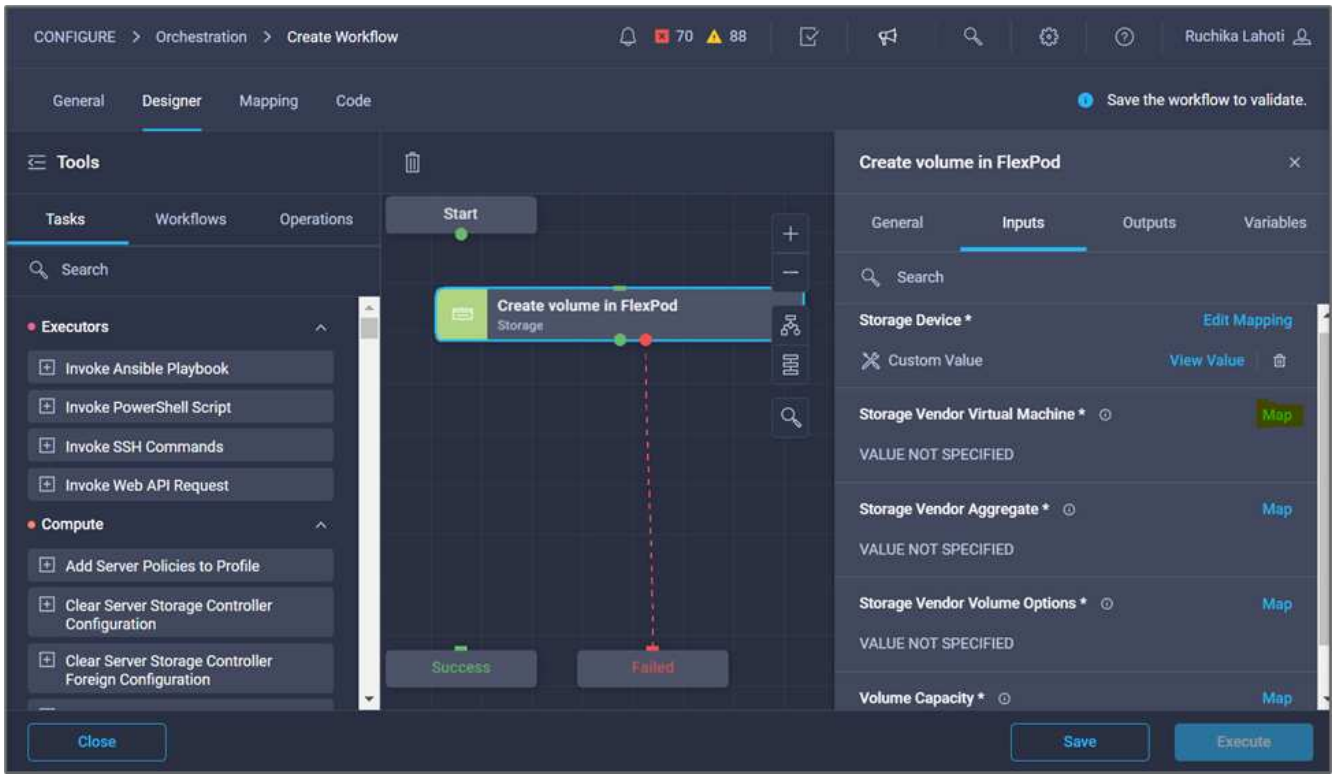
7. Escolha **valor estático** e clique em **Selecionar dispositivo de armazenamento**.
8. Clique no destino de armazenamento adicionado e clique em **Select**.



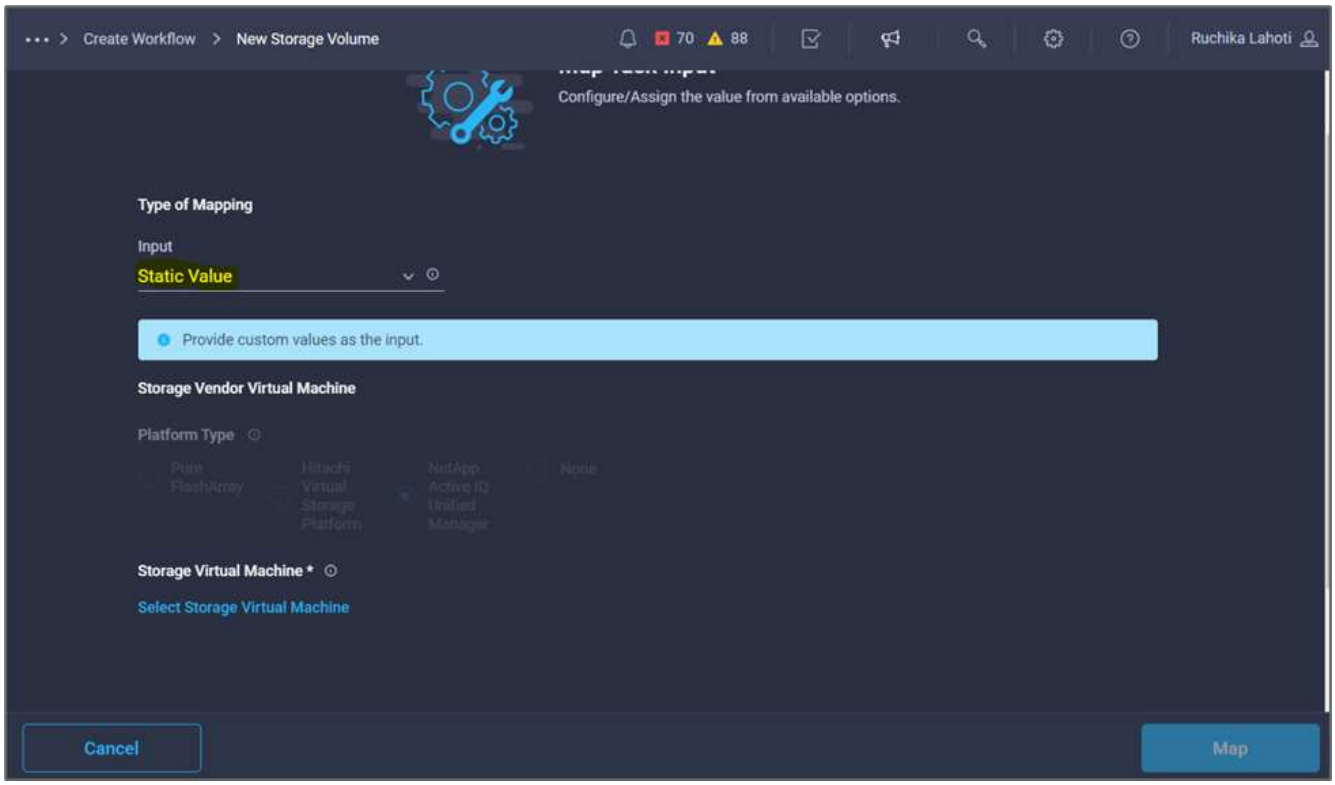
9. Clique em **mapa**.



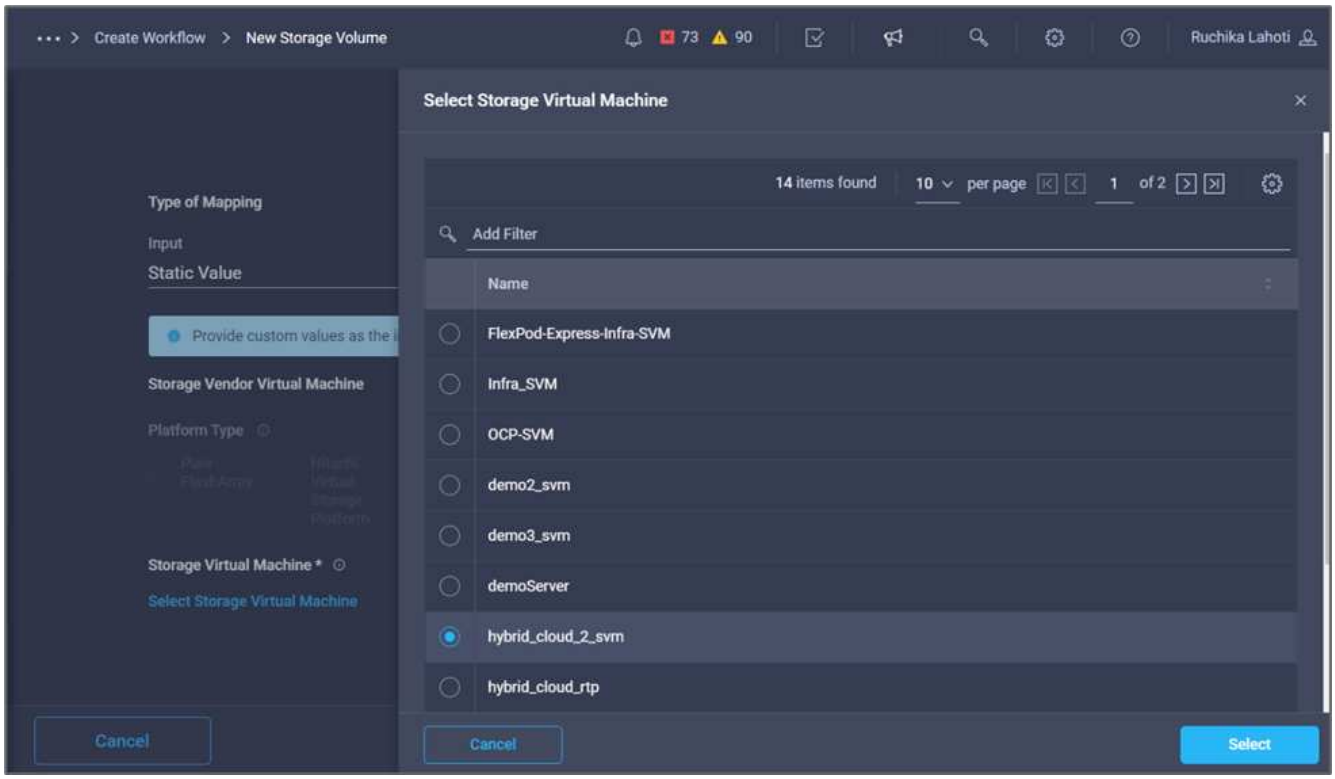
10. Clique em **Map** no campo **Storage Vendor Virtual Machine**.



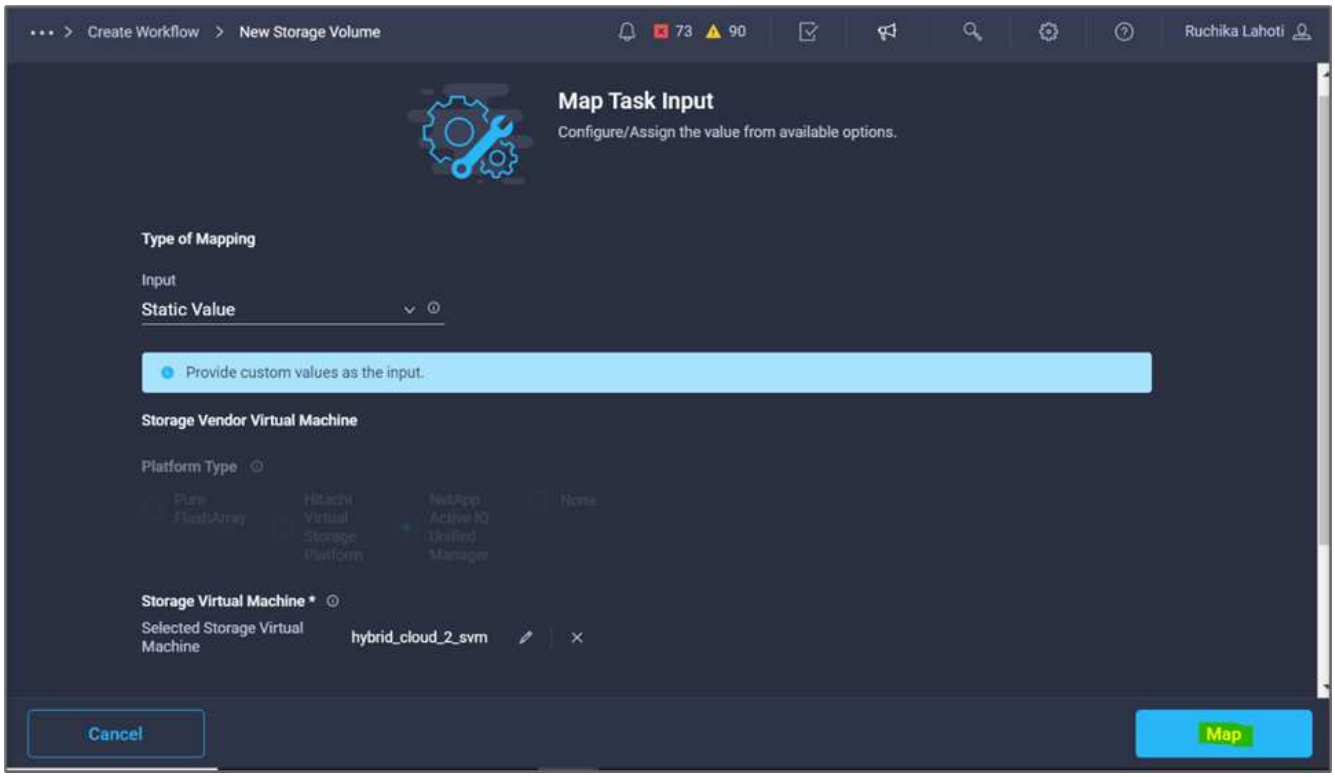
11. Escolha **Static Value** e clique em **Select Storage Virtual Machine**.



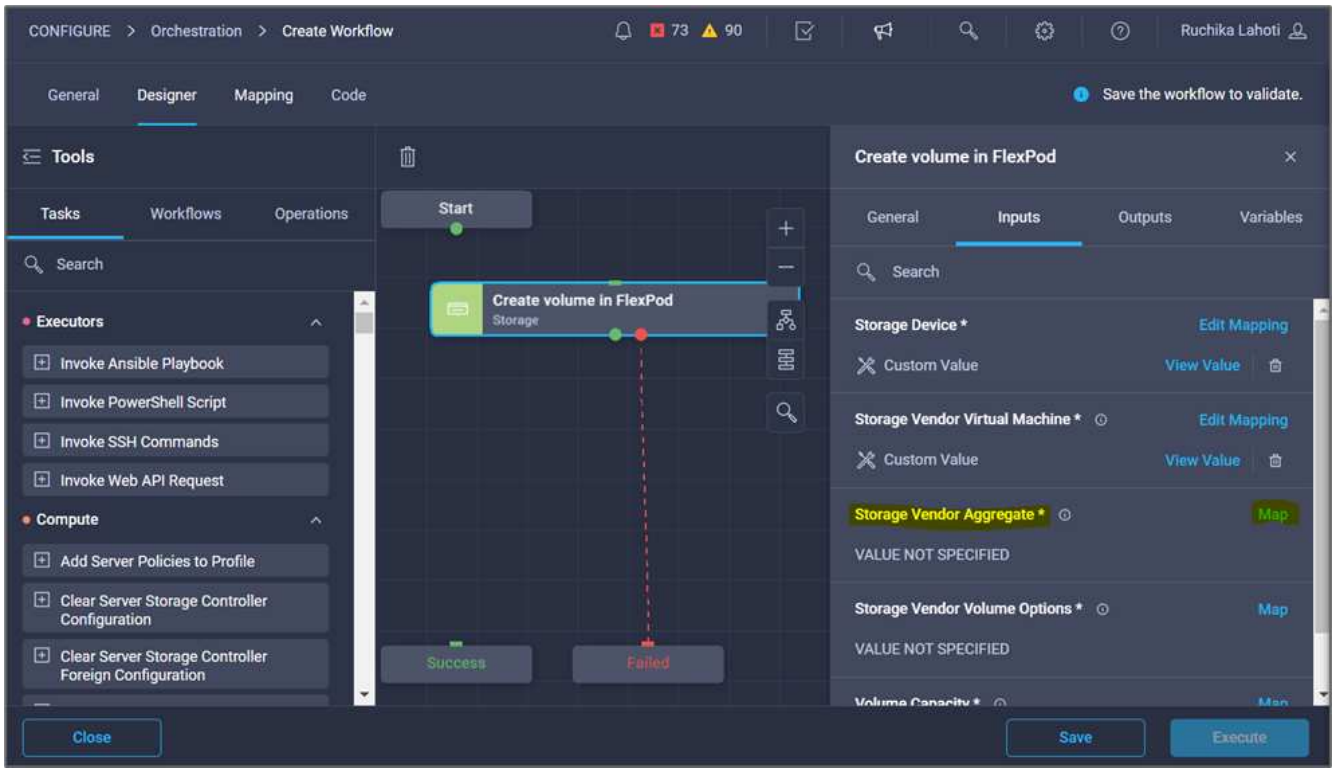
12. Selecione a máquina virtual de armazenamento onde o volume precisa ser criado e clique em **Select**.



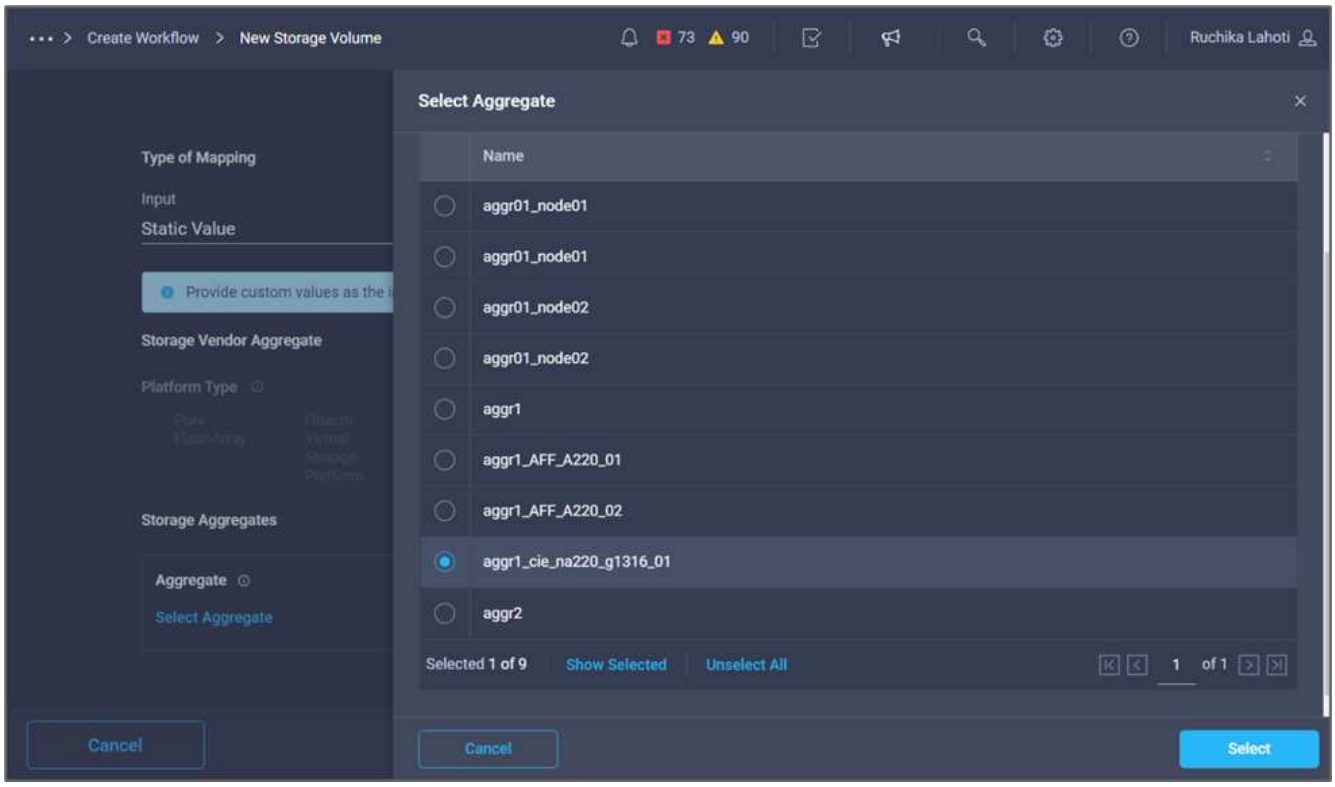
13. Clique em **mapa**.



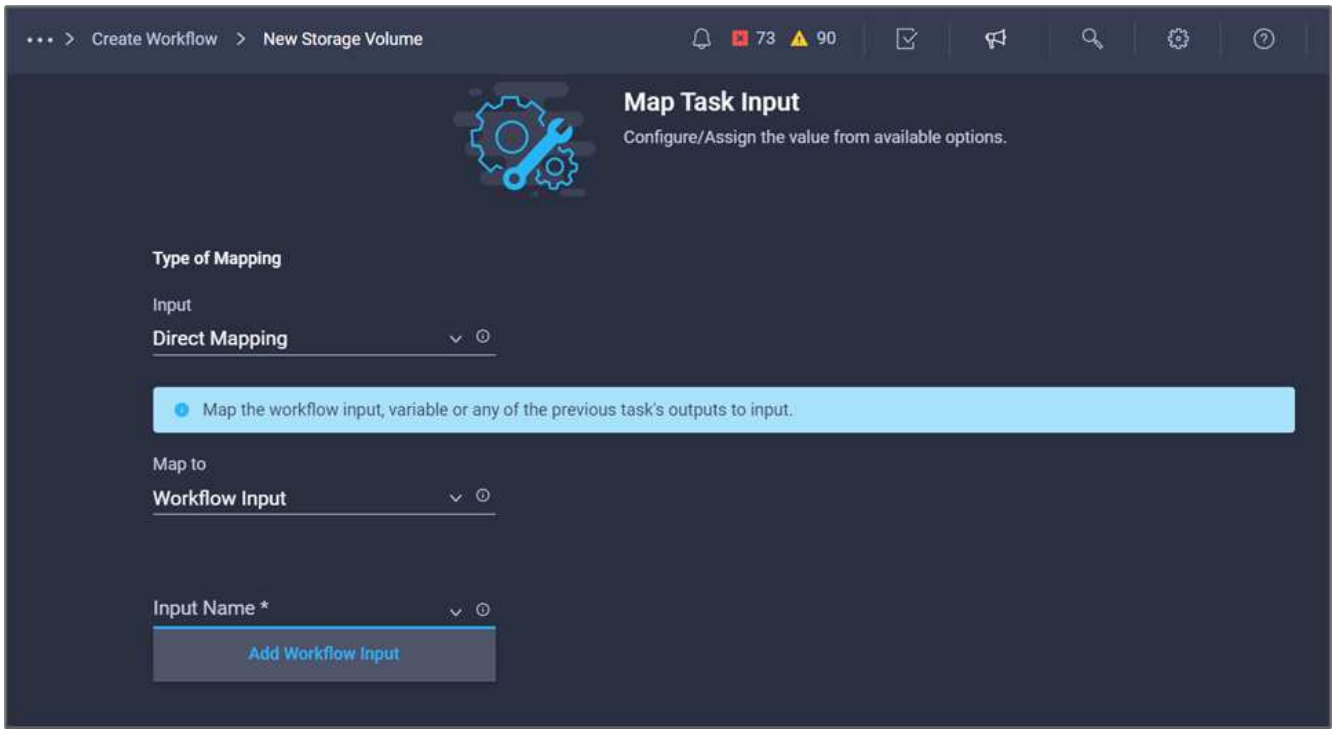
14. Clique em **Map** no campo **Storage Vendor Aggregate**.



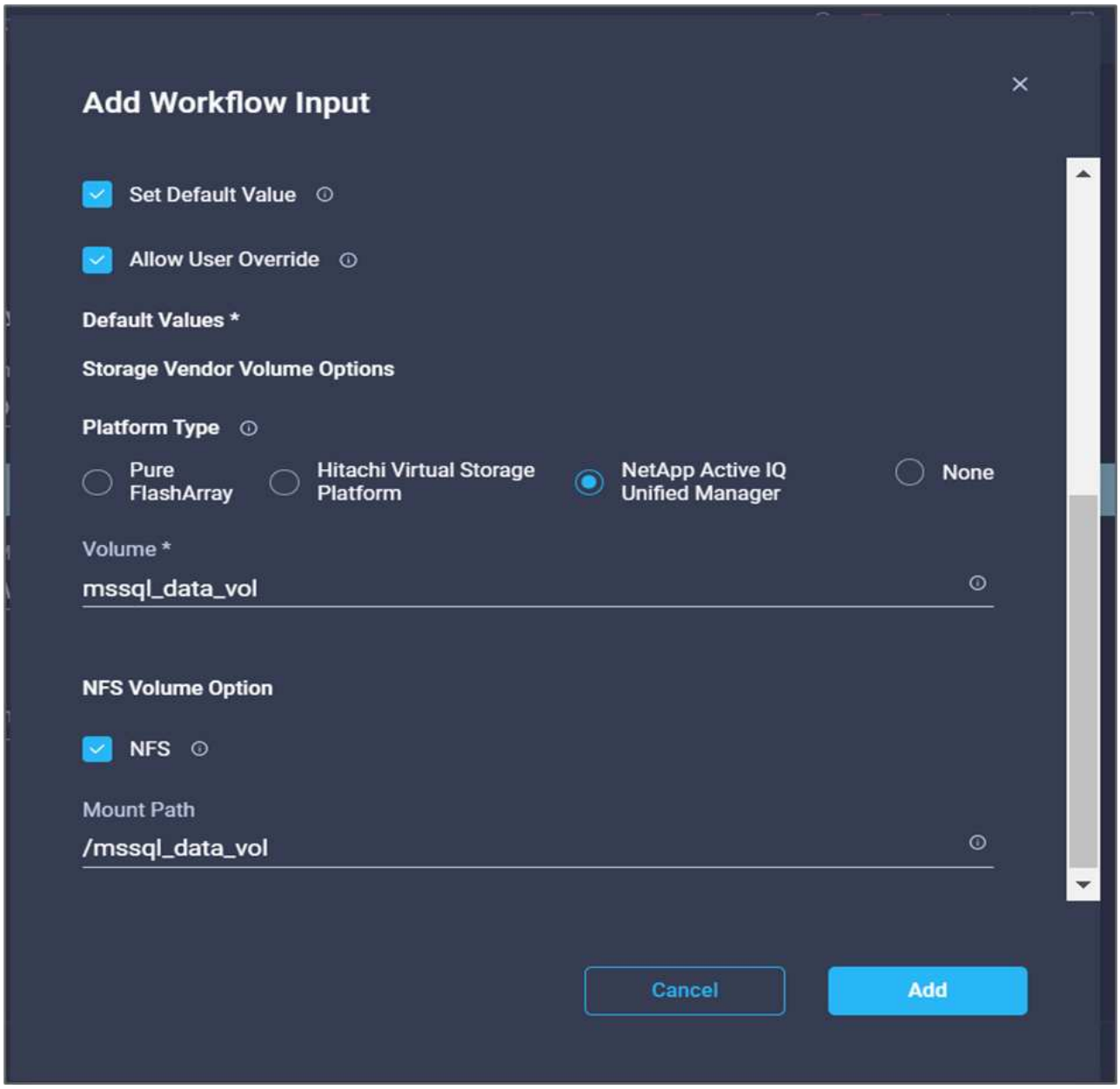
15. Escolha **Static Value** e clique em **Select Storage Aggregate**. Escolha o agregado e clique em **Select**.



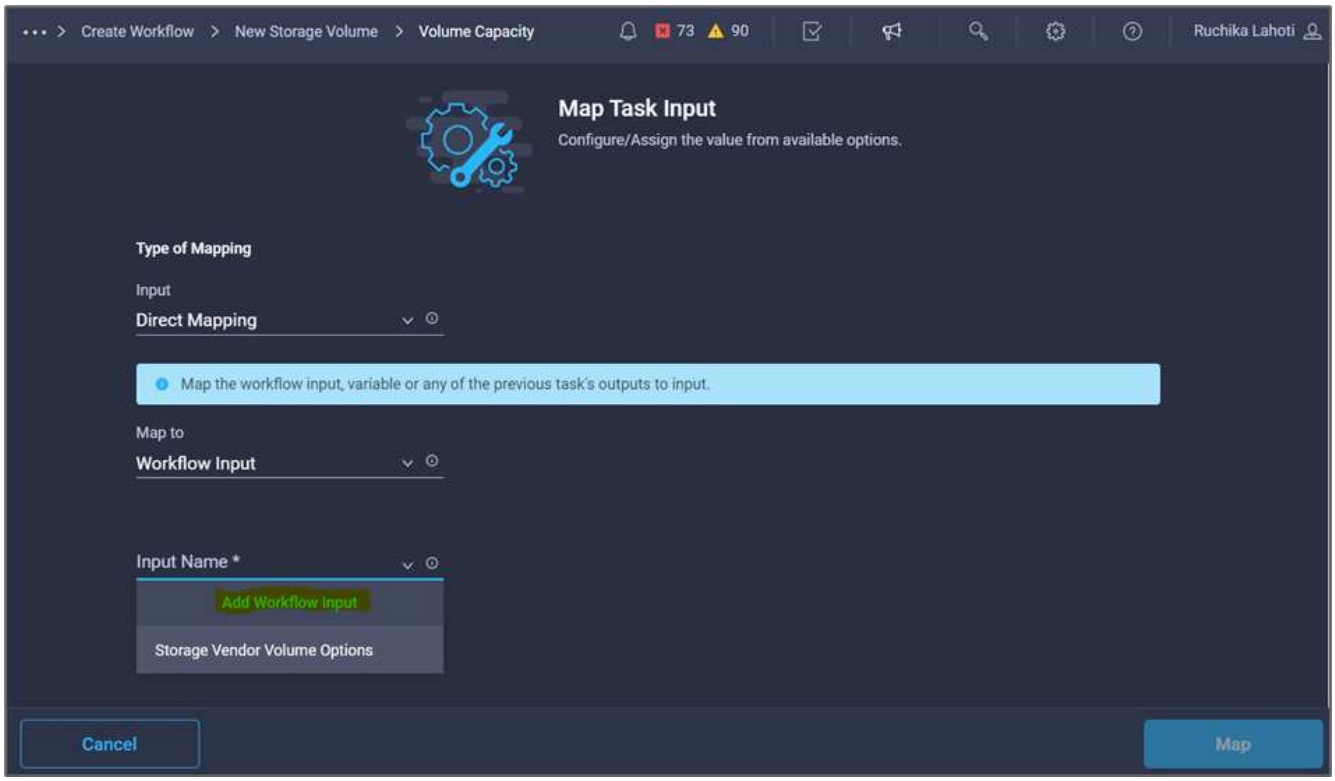
16. Clique em **mapa**.
17. Clique em **Map** no campo **Storage Vendor volume Options** (Opções de volume do fornecedor de armazenamento).
18. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.



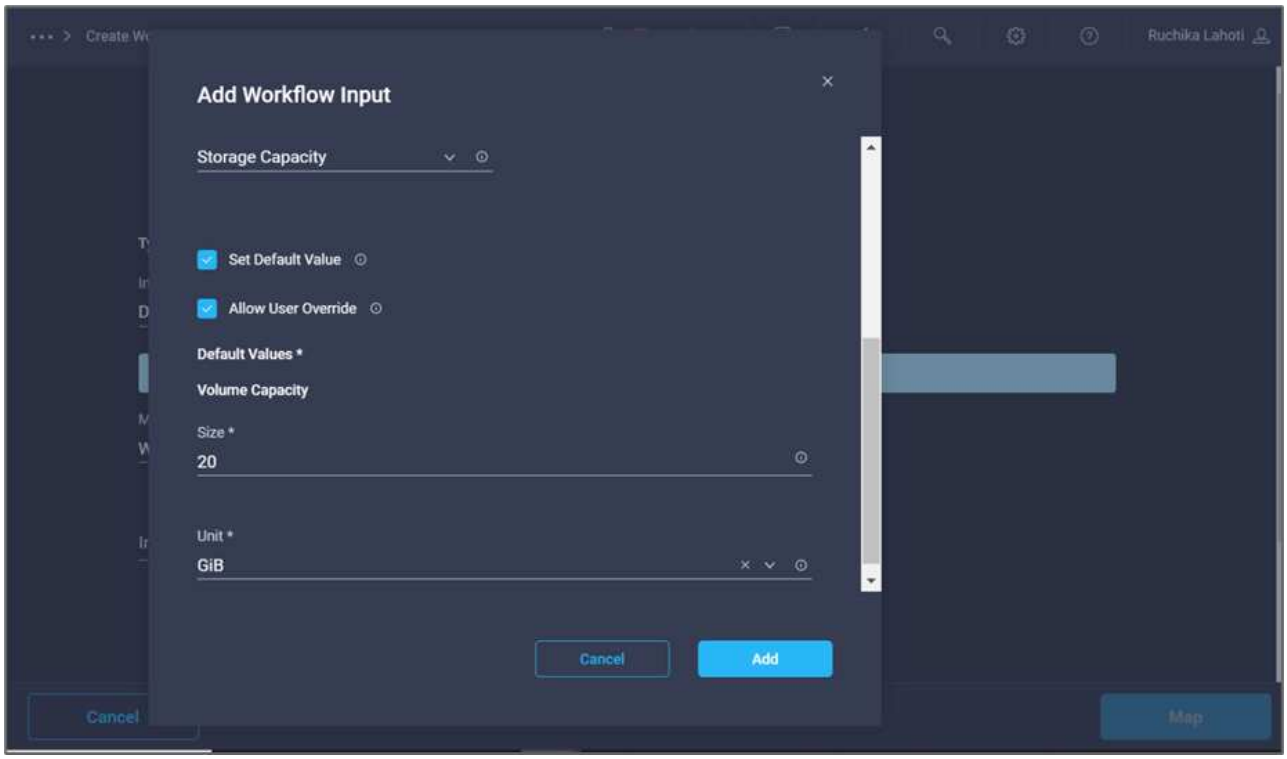
19. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Certifique-se de que **Opções de volume do fornecedor de armazenamento** está selecionado para **tipo**.
    c. Clique em **Definir valor padrão e Substituir**.
    d. Clique em **obrigatório**.
    e. Defina o **tipo de plataforma** como **NetApp Active IQ Unified Manager**.
    f. Forneça um valor padrão para o volume criado em **volume**.
    g. Clique em **NFS**. Se NFS for definido, um volume NFS será criado. Se esse valor for definido como false, um volume SAN será criado.
    h. Forneça um caminho de montagem e clique em **Add**.



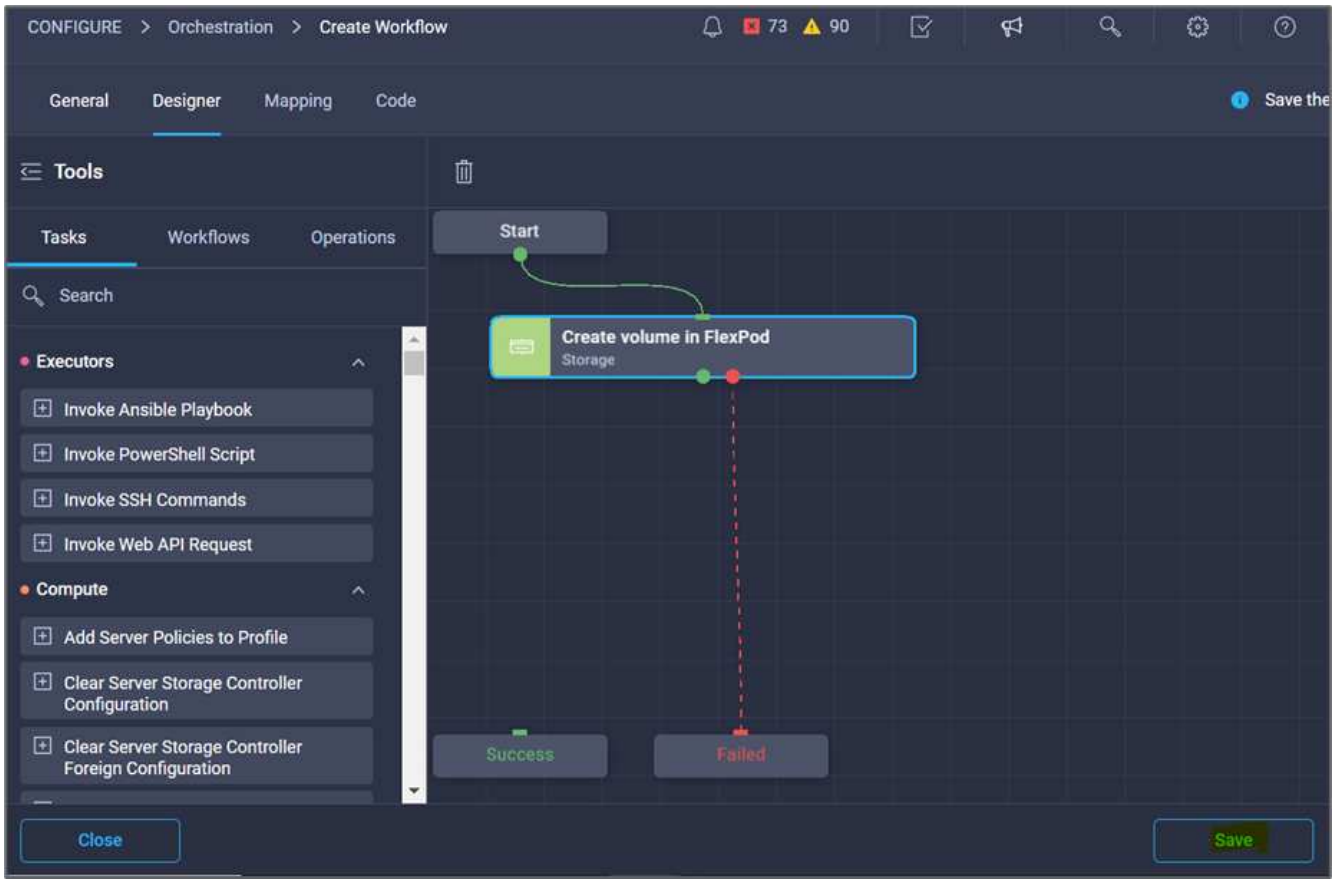
20. Clique em **mapa**.
21. Clique em **Map** no campo **volume Capacity**.
22. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
23. Clique em **Input Name** e **Create Workflow Input**.



24. No assistente Adicionar entrada:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Clique em **obrigatório**.
    c. Para **tipo**, selecione **capacidade de armazenamento**.
    d. Clique em **Definir valor padrão e Substituir**.
    e. Forneça um valor padrão para o tamanho do volume e a unidade.
    f. Clique em **Add**.



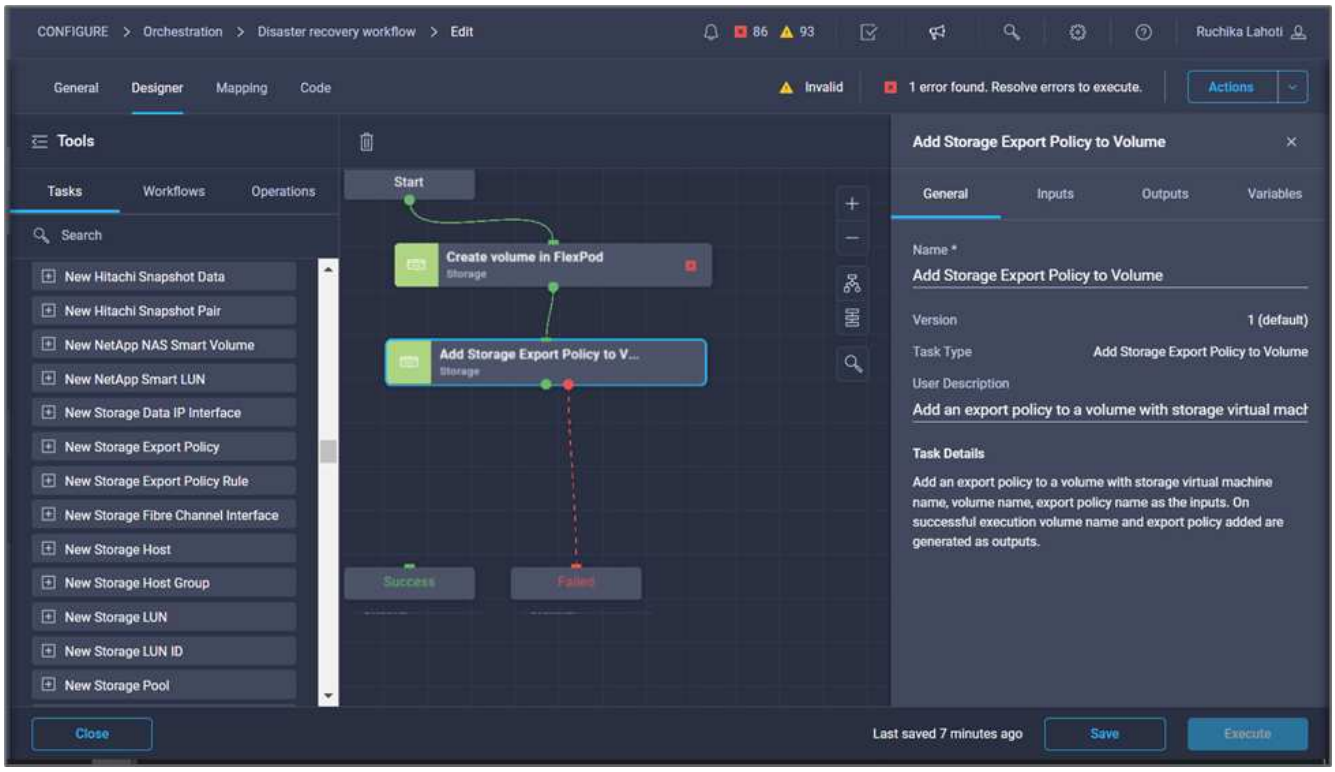
25. Clique em **mapa**.
26. Com o Connector, crie uma conexão entre as tarefas **Iniciar** e **criar volume no FlexPod** e clique em **Salvar**.



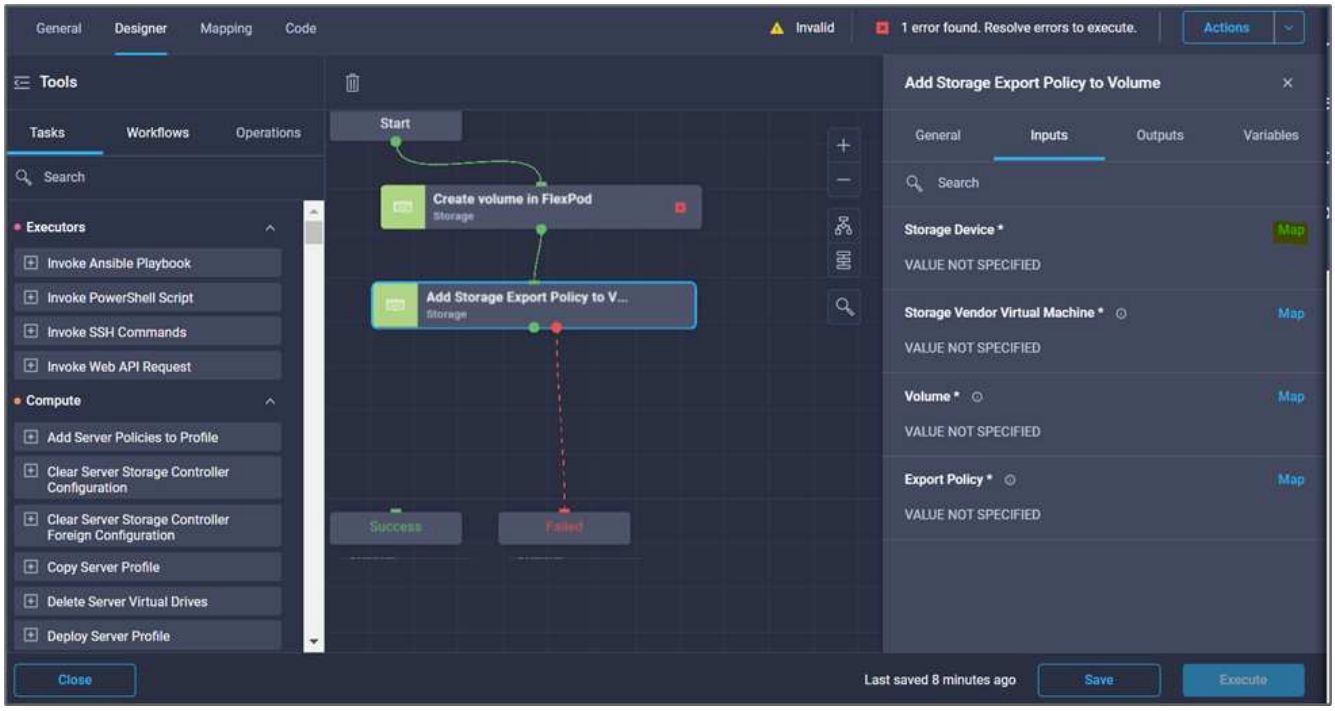
Ignore o erro por enquanto. Esse erro é exibido porque não há conetividade entre as tarefas **criar volume no FlexPod** e **sucesso** que é necessário para especificar a transição bem-sucedida.

Procedimento 3: Adicionar política de exportação de armazenamento

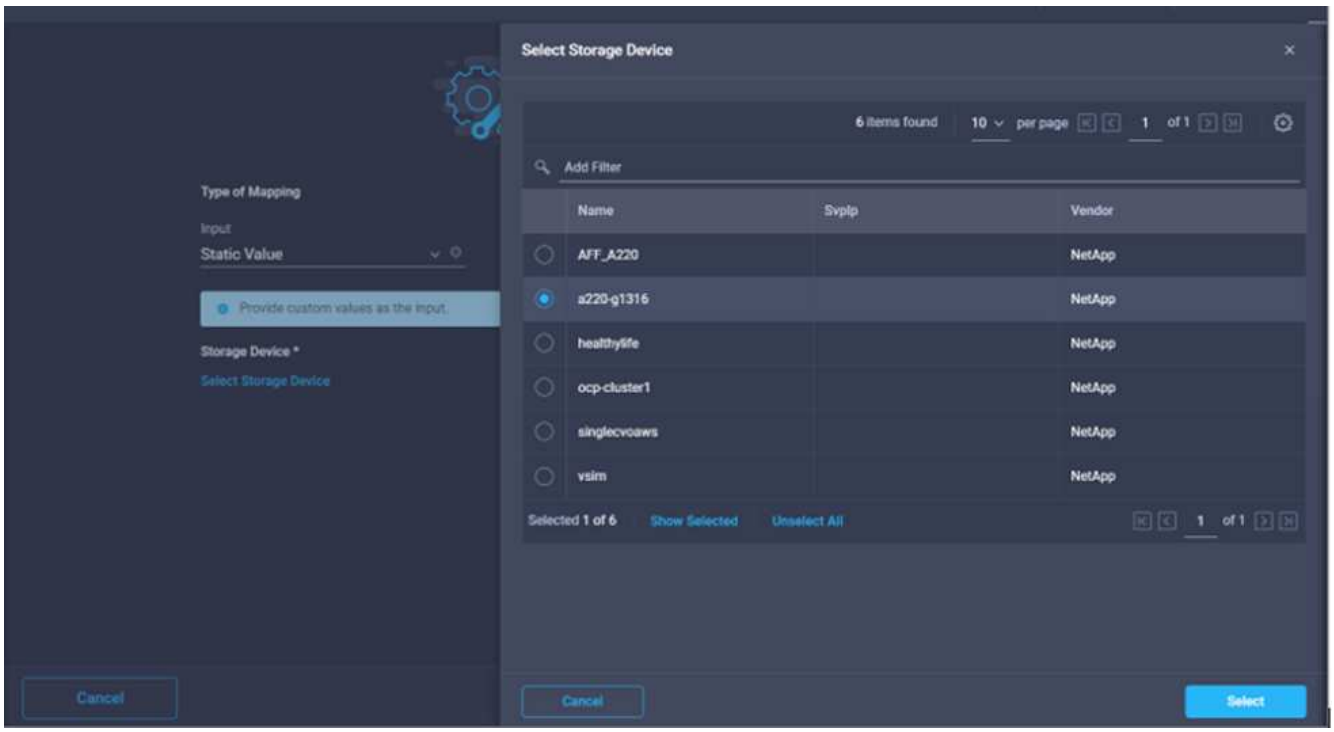
1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte a tarefa **armazenamento > Adicionar política de exportação de armazenamento para volume** na seção **Ferramentas** na área **Design**.
3. Clique em **Adicionar política de exportação de armazenamento ao volume**. Na área **Propriedades da tarefa**, clique na guia **Geral**. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa. Neste exemplo, o nome da tarefa é Adicionar política de exportação de armazenamento.
4. Use o conetor para fazer uma conexão entre as tarefas **criar volume no FlexPod** e **Adicionar política de exportação de armazenamento**. Clique em **Salvar**.



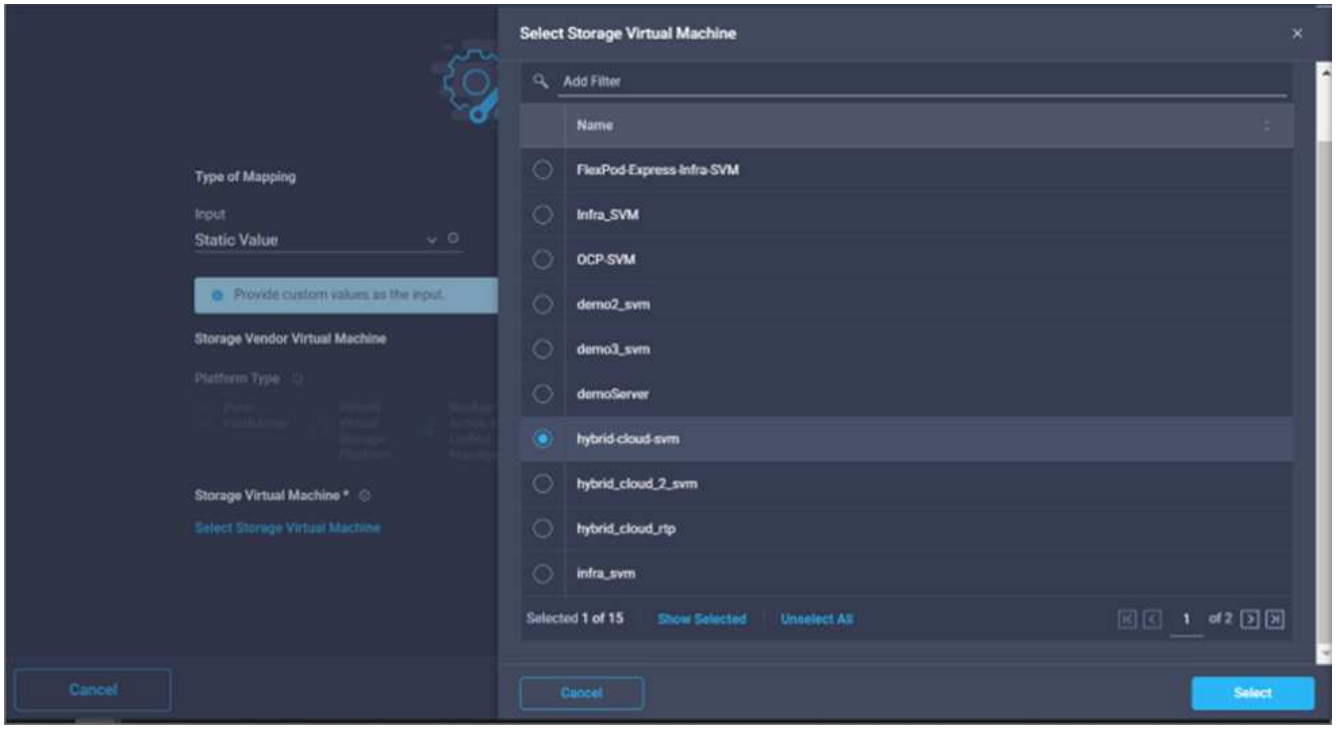
5. Na área **Task Properties**, clique em **Inputs**.
6. Clique em **Map** no campo **Storage Device** (dispositivo de armazenamento).



7. Escolha **valor estático** e clique em **Selecionar dispositivo de armazenamento**. Selecione o mesmo destino de armazenamento adicionado ao criar a tarefa anterior de criar um novo volume de armazenamento.
8. Clique em **mapa**.

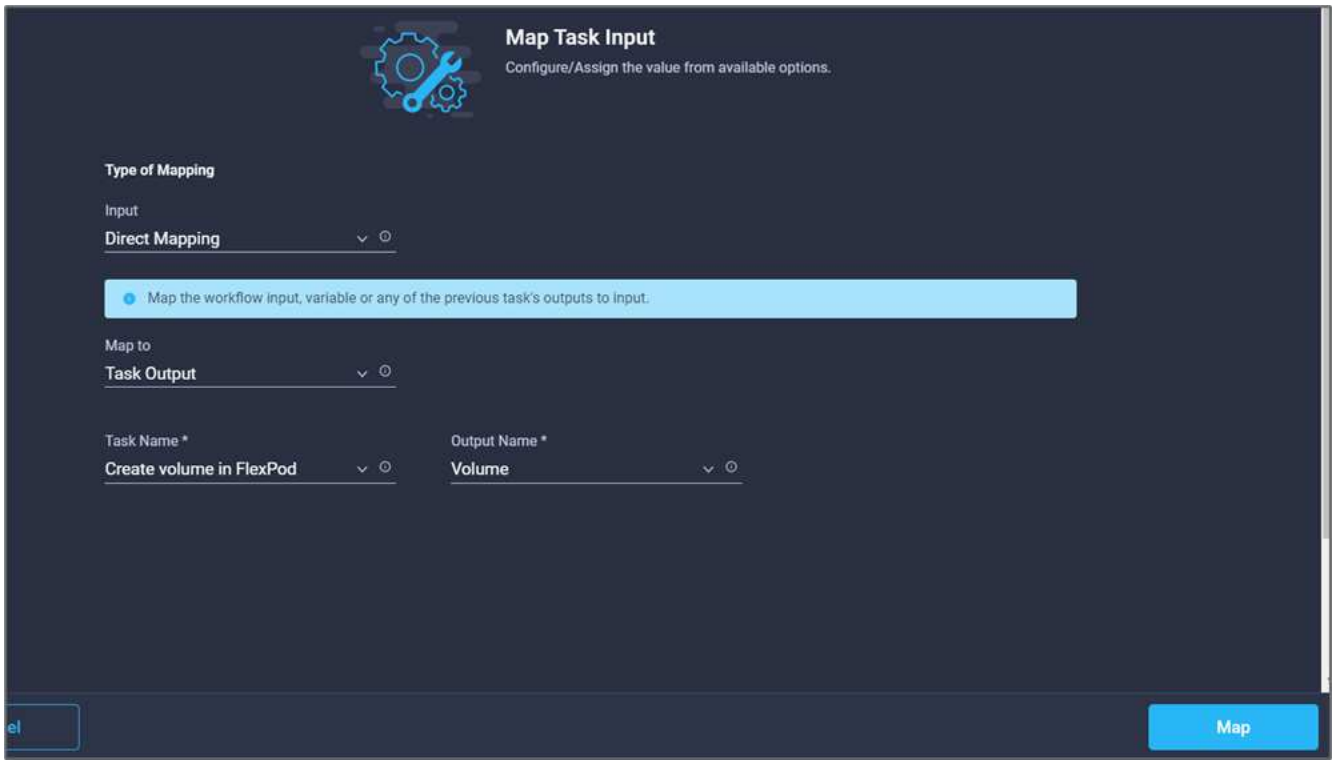


9. Clique em **Map** no campo **Storage Vendor Virtual Machine**.
10. Escolha **Static Value** e clique em **Select Storage Virtual Machine**. Selecione a mesma máquina virtual de armazenamento adicionada ao criar a tarefa anterior de criar um novo volume de armazenamento.

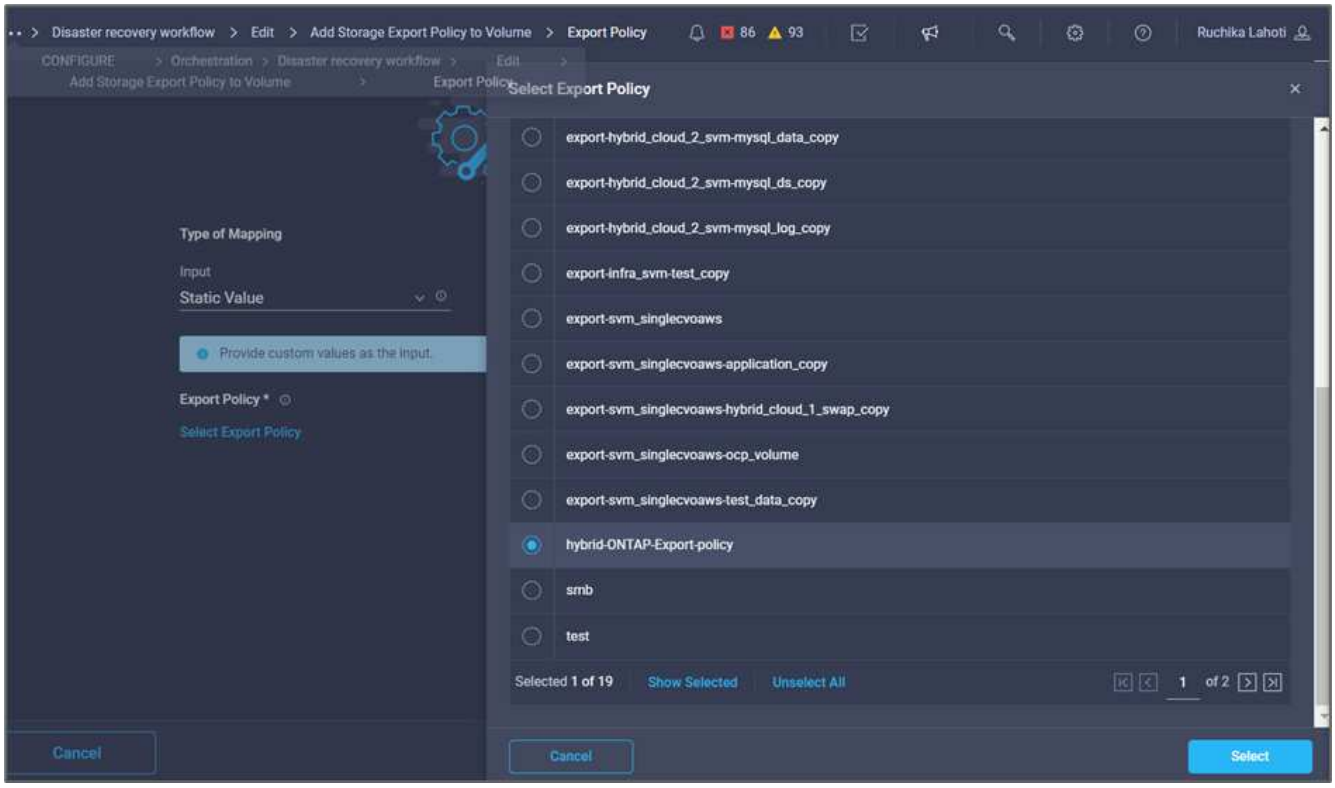


11. Clique em **mapa**.
12. Clique em **Map** no campo **volume**.
13. Clique em **Nome da tarefa** e, em seguida, clique em **criar volume no FlexPod**. Clique em **Nome de saída** e depois em **volume**.

> No Cisco Intersight Cloud Orchestrator, você pode fornecer a saída de uma tarefa anterior como entrada para uma nova tarefa. Neste exemplo, os detalhes **volume** foram fornecidos da tarefa **criar volume no FlexPod** como entrada para a tarefa **Adicionar política de exportação de armazenamento**.



14. Clique em **mapa**.
15. Clique em **mapa** no campo **Política de exportação**.
16. Escolha **valor estático** e clique em **Selecionar política de exportação**. Selecione a política de exportação criada.

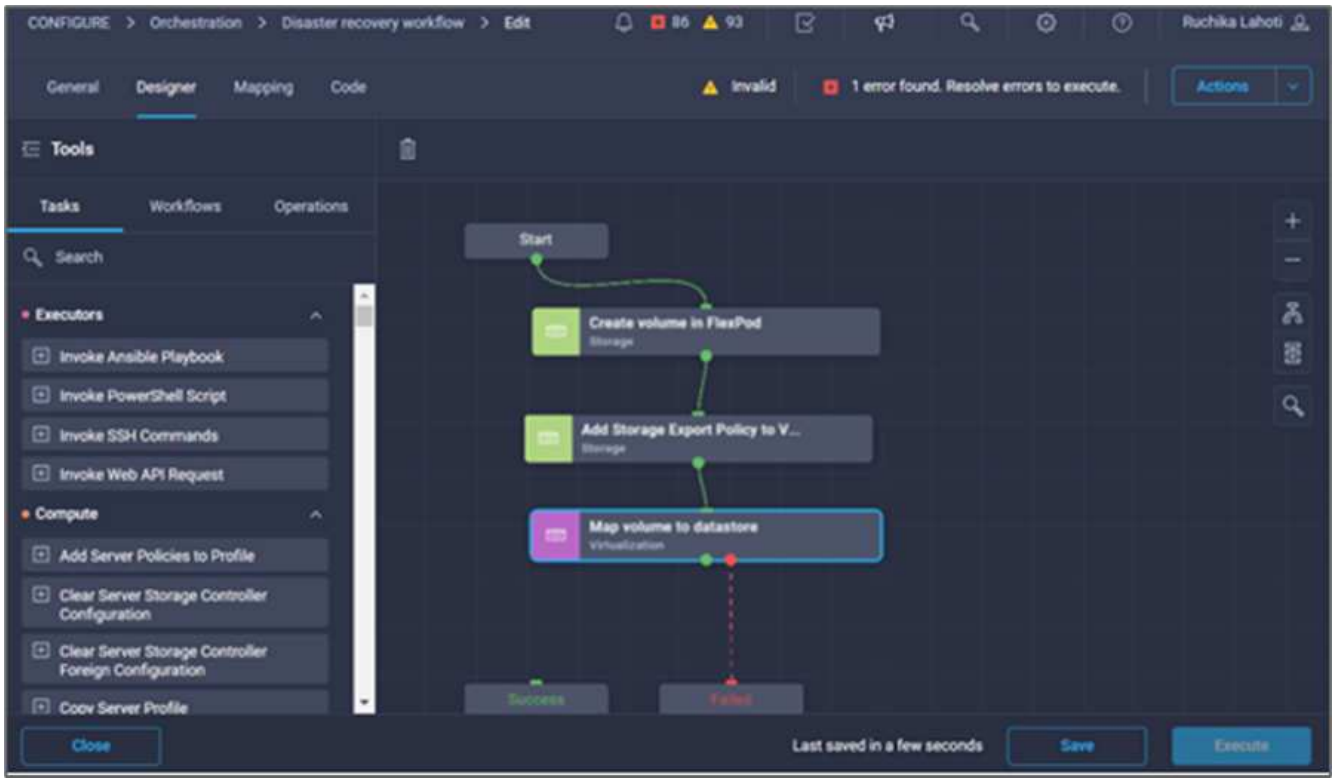


17. Clique em **Map** e depois em **Save**.

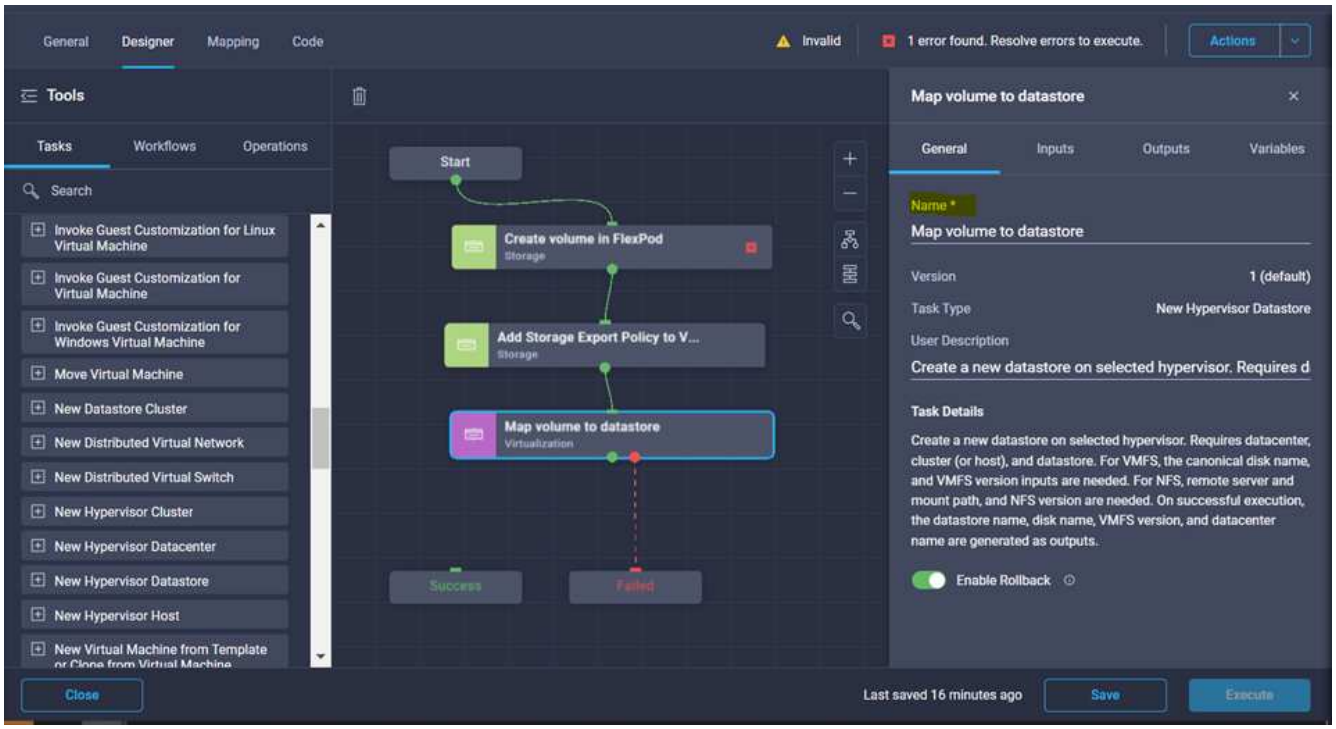
Isso conclui a adição de uma política de exportação ao volume. Em seguida, você cria um novo mapeamento do datastore do volume criado.

Procedimento 4: Mapear o volume FlexPod para o datastore

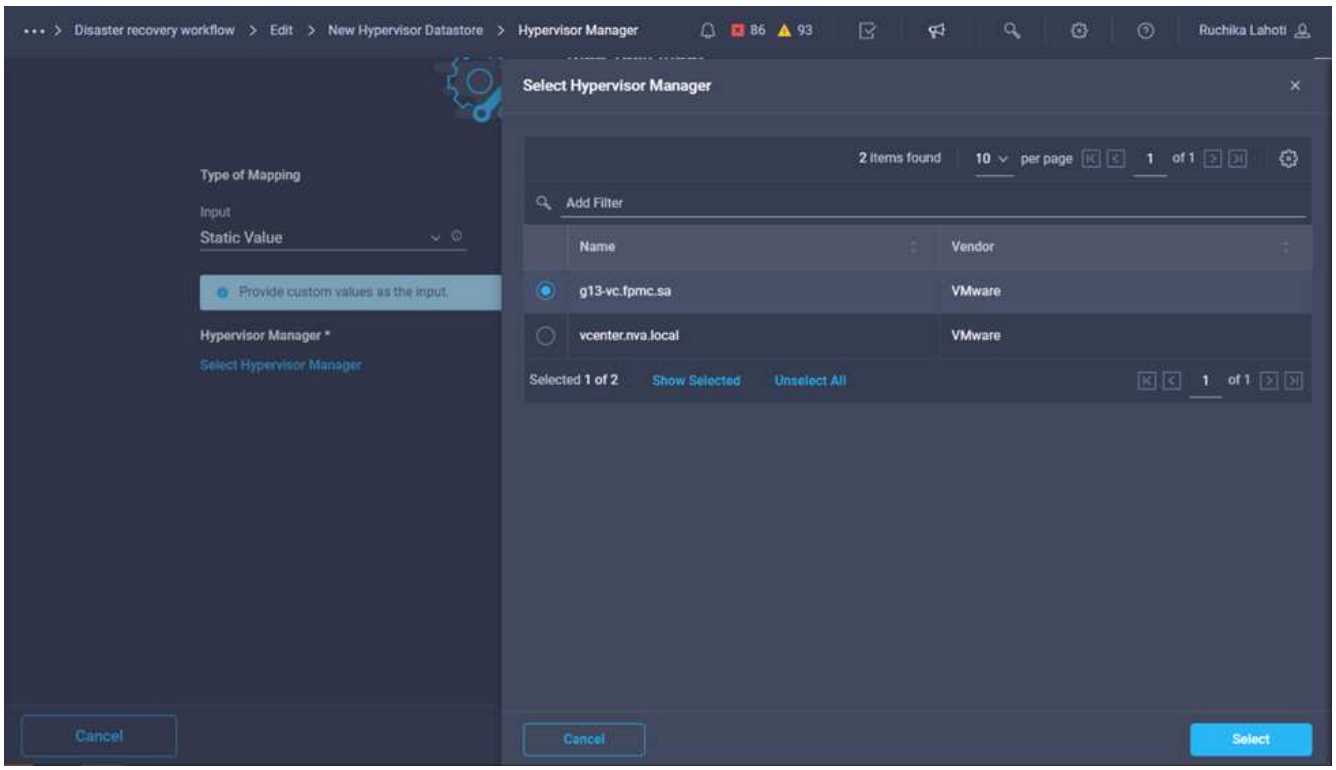
1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte a tarefa **Virtualization > New Hypervisor datastore** na seção **Tools** na área **Design**.
3. Use o conetor para fazer uma conexão entre as tarefas **Add Storage Export Policy** e **New Hypervisor datastore**. Clique em **Salvar**.



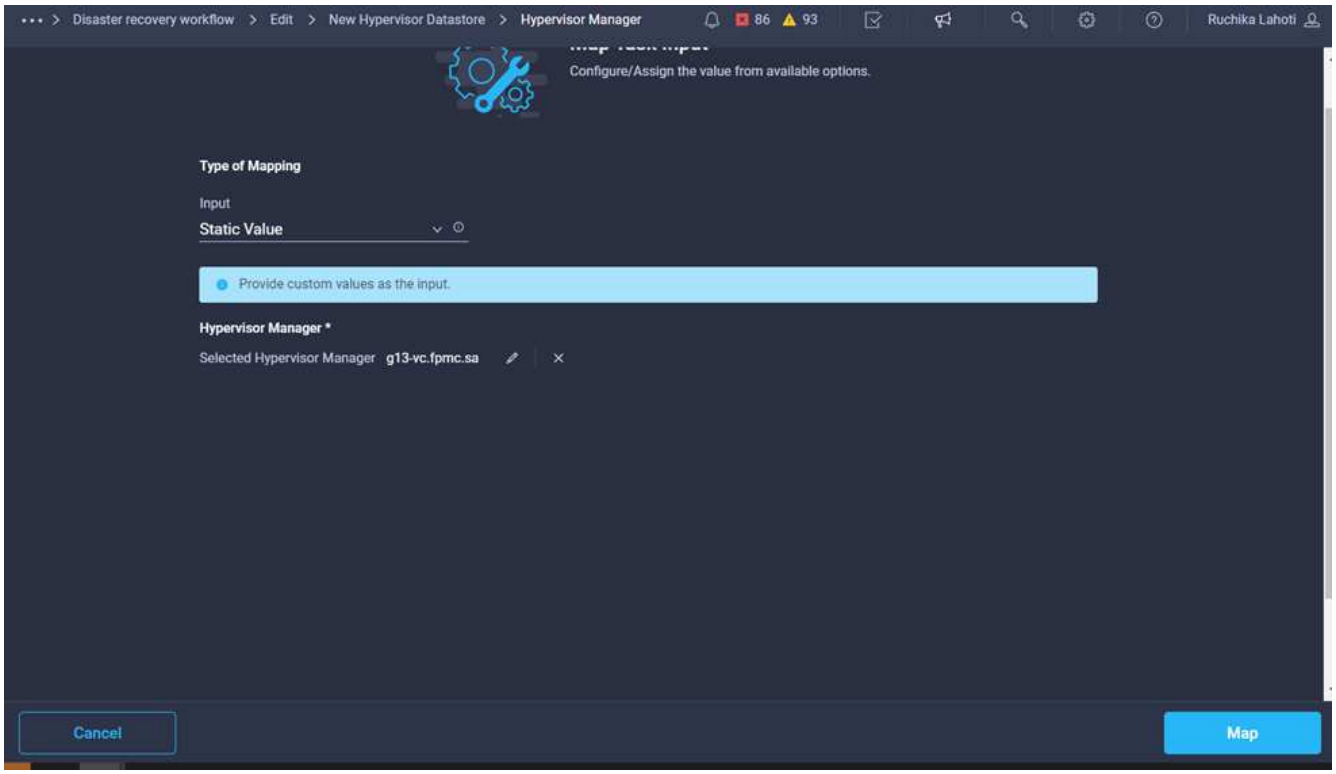
4. Clique em **New Hypervisor datastore**. Na área **Propriedades da tarefa**, clique na guia **Geral**. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa. Neste exemplo, o nome da tarefa é **Map volume to datastore**.



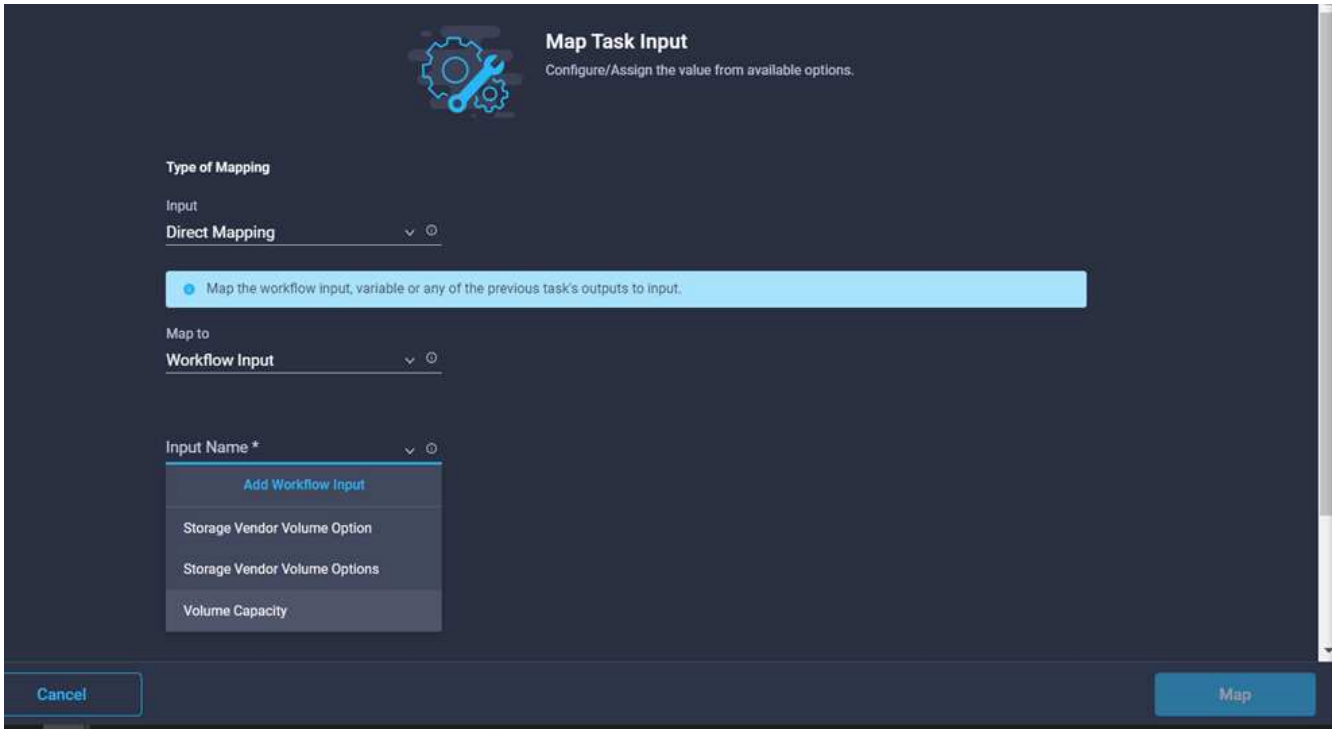
5. Na área **Task Properties**, clique em **Inputs**.
6. Clique em **Map** no campo **Hypervisor Manager**.
7. Escolha **Static Value** e clique em **Select Hypervisor Manager**. Clique no destino do VMware vCenter.



8. Clique em **mapa**.



9. Clique em **Map** no campo **Data Center**. Esse é o data center associado ao novo datastore.
10. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
11. Clique em **Input Name** e em **Create Workflow Input**.

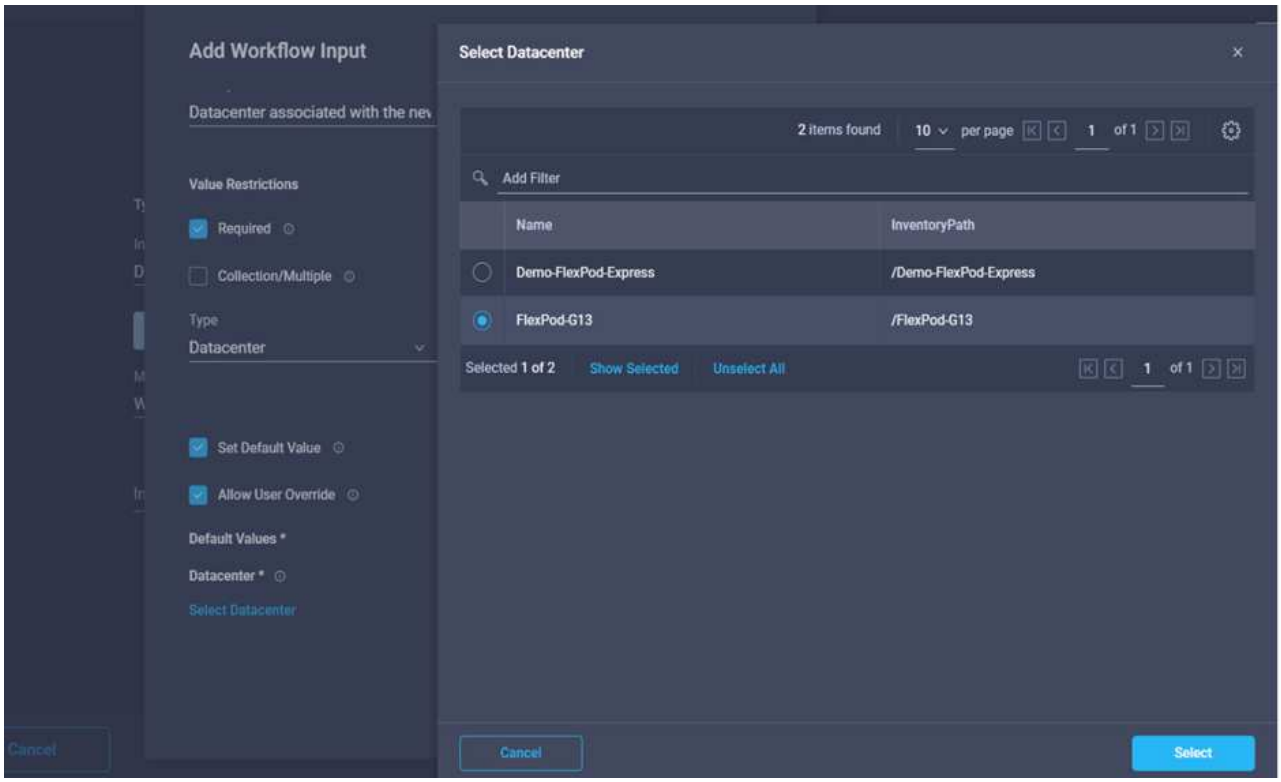


12. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Selecione **Datacenter** como o tipo.

c. Clique em **Definir valor padrão e Substituir**.

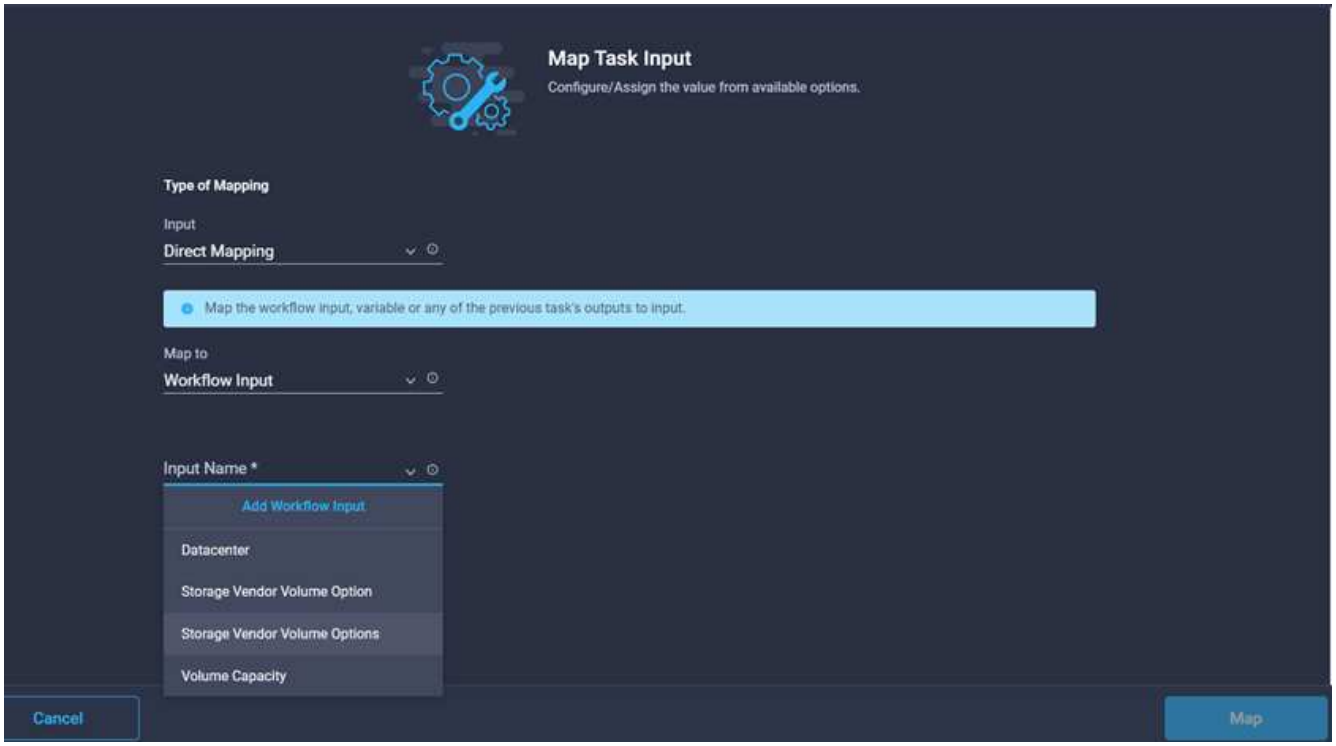
d. Clique em **Select Datacenter**.

e. Clique no data center associado ao novo datastore e clique em **Select**.

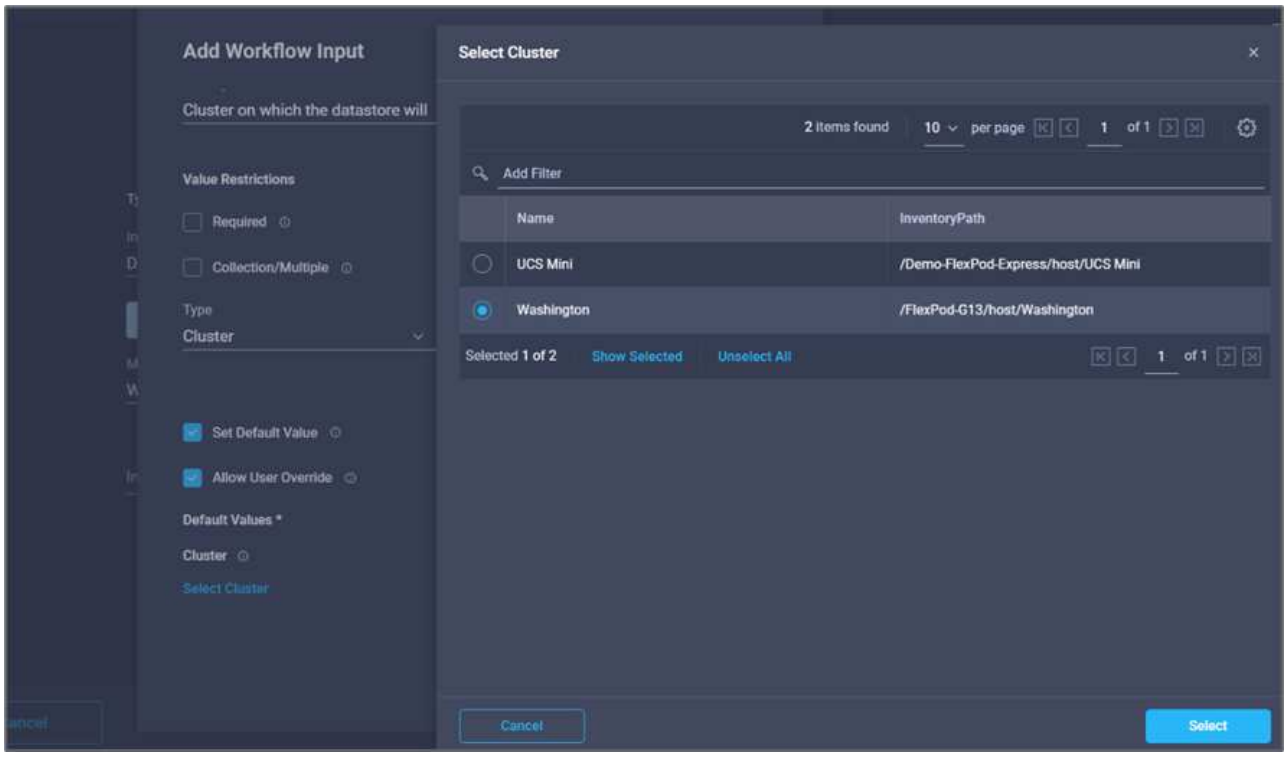


- Clique em **Add**.

13. Clique em **mapa**.
14. Clique em **Map** no campo **Cluster**.
15. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.

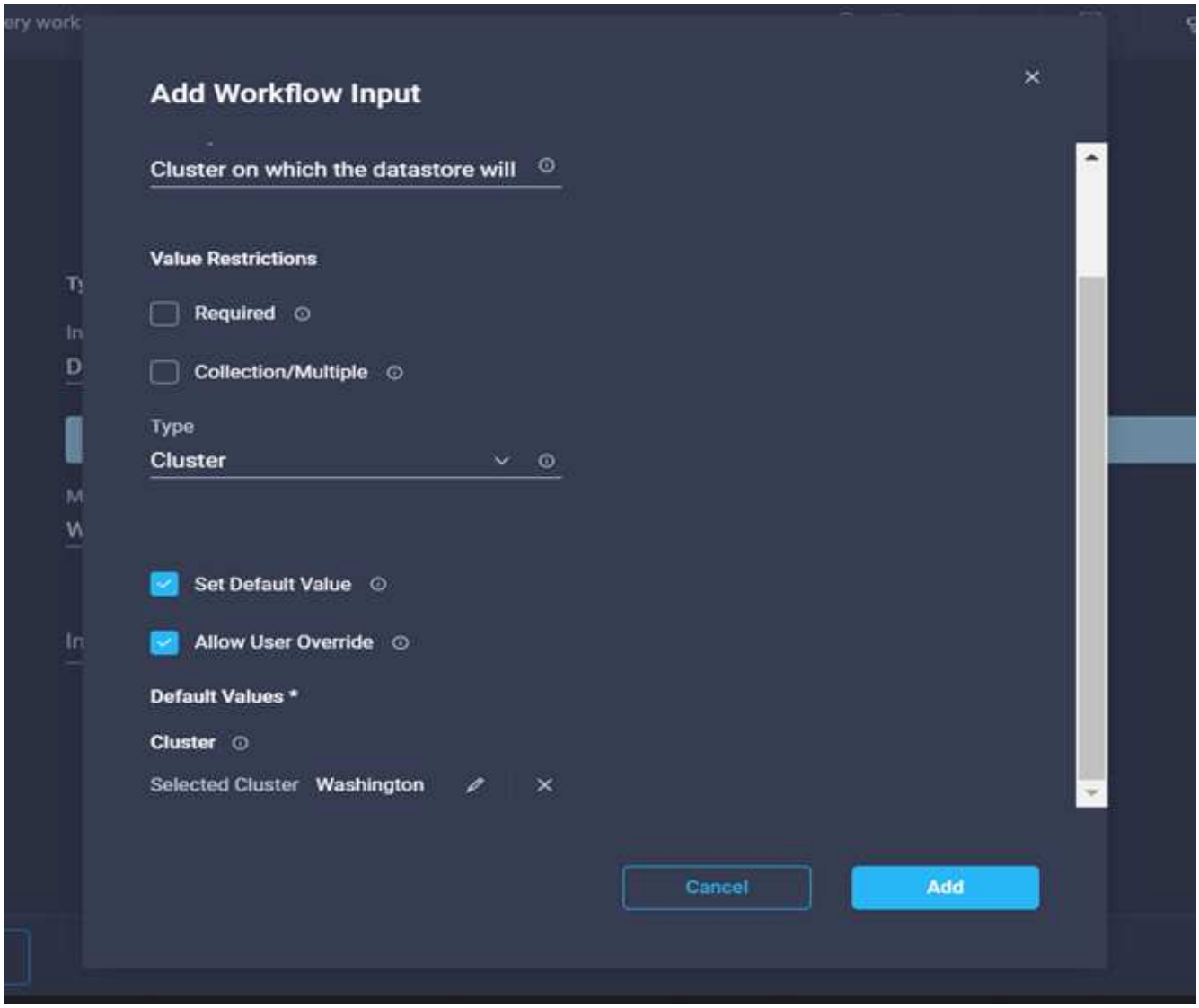


16. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Clique em **obrigatório**.
    c. Selecione Cluster como o tipo.
    d. Clique em **Definir valor padrão e Substituir**.
    e. Clique em **Select Cluster**.
    f. Clique no cluster associado ao novo datastore.
    g. Clique em **Select**.

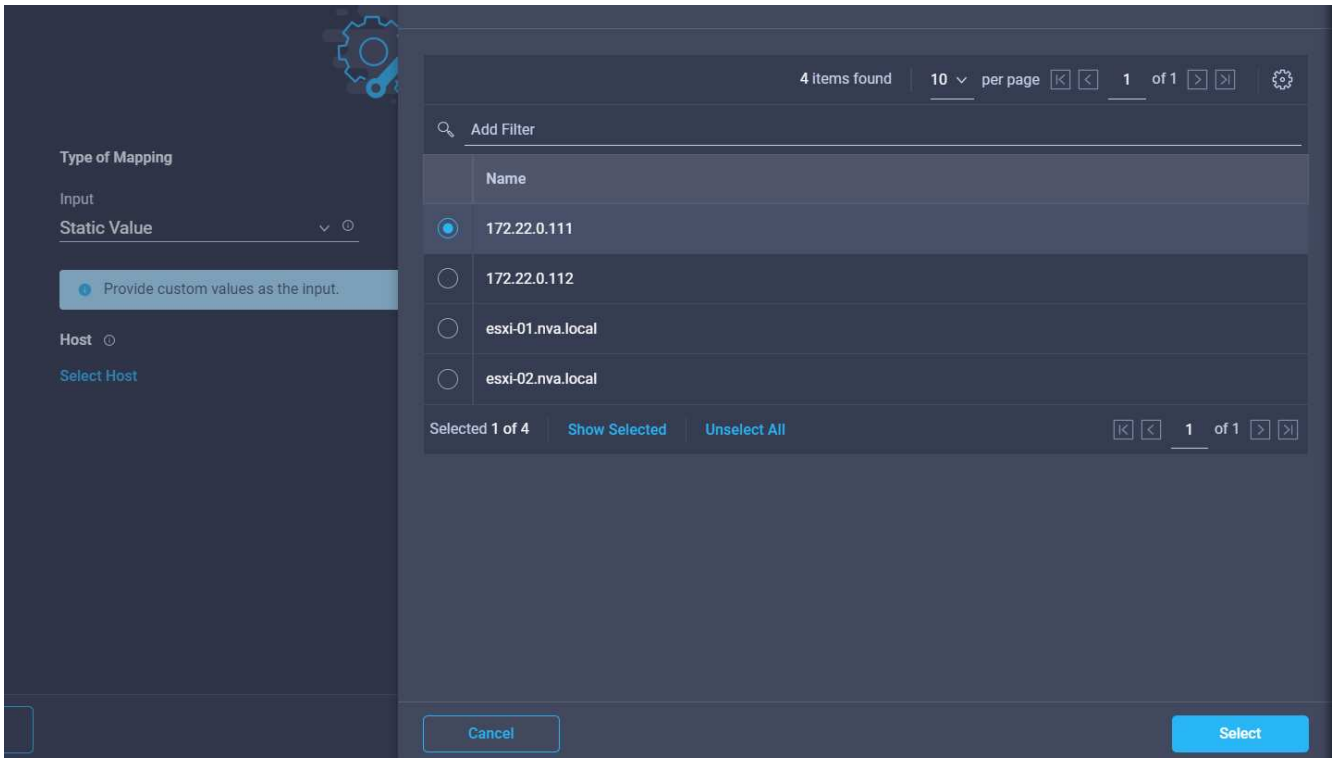


h. Clique em **Add**.

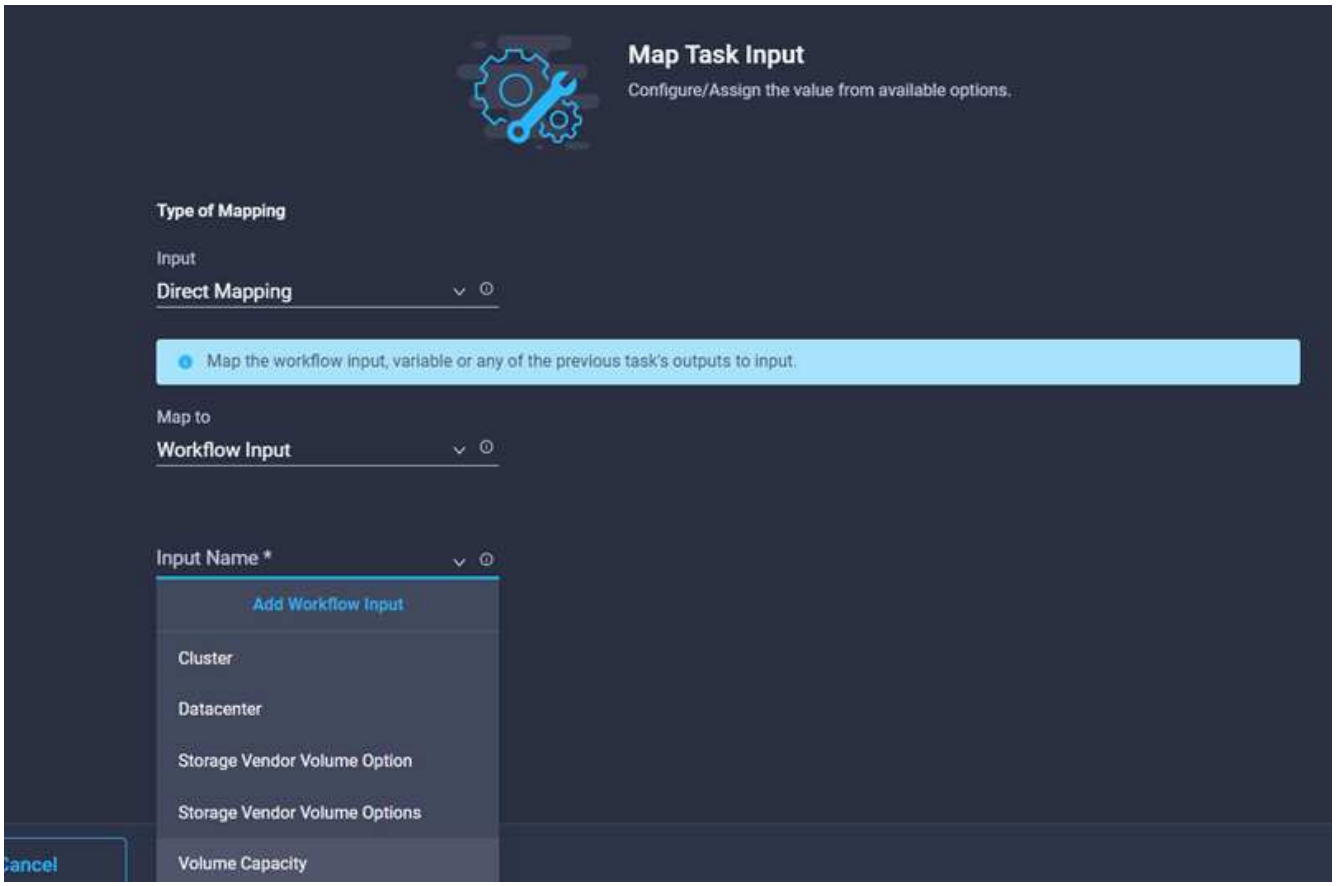
17. Clique em **mapa**.
18. Clique em **Map** no campo **Host**.



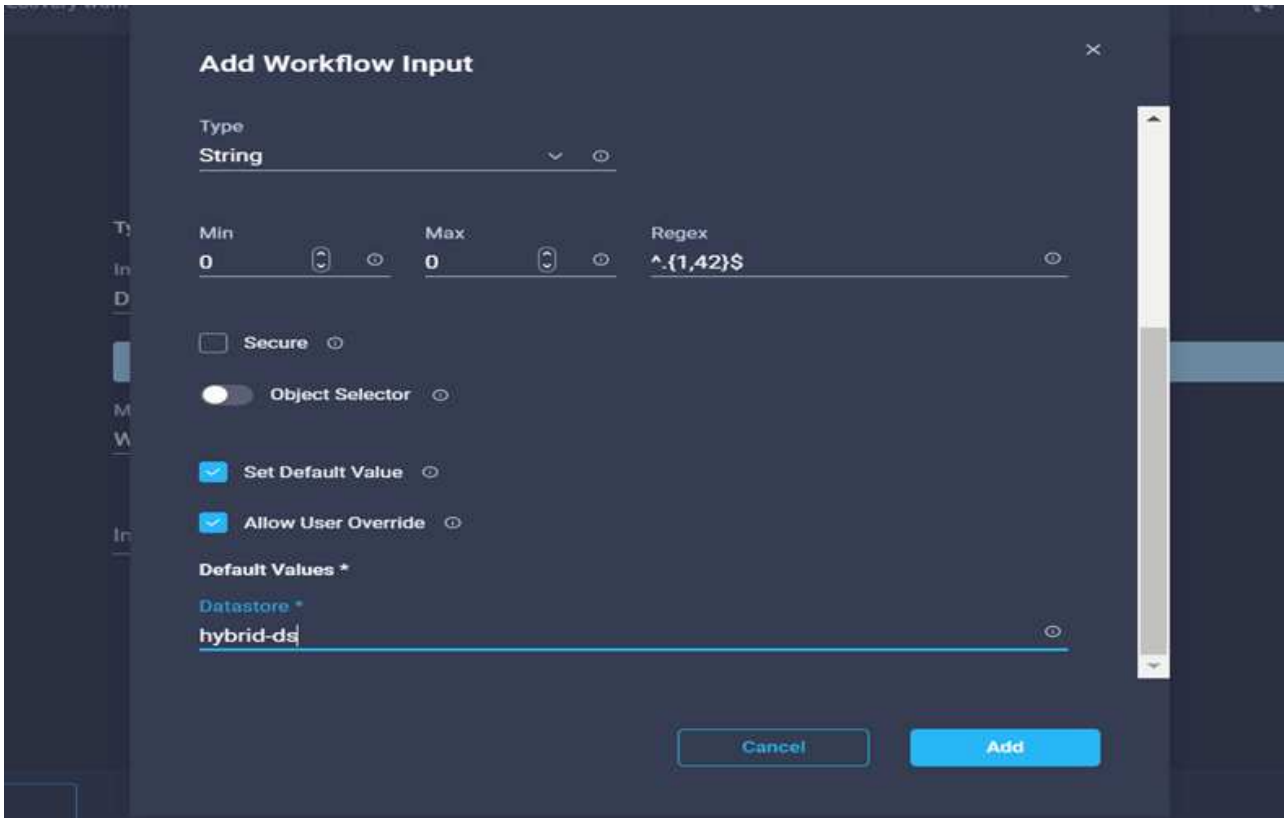
19. Escolha **Static Value** e clique no host no qual o datastore será hospedado. Se um cluster for especificado, o host será ignorado.



20. Clique em **Selecionar e mapear**.
21. Clique em **Map** no campo **datastore**.
22. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
23. Clique em **Input Name** e **Create Workflow Input**.

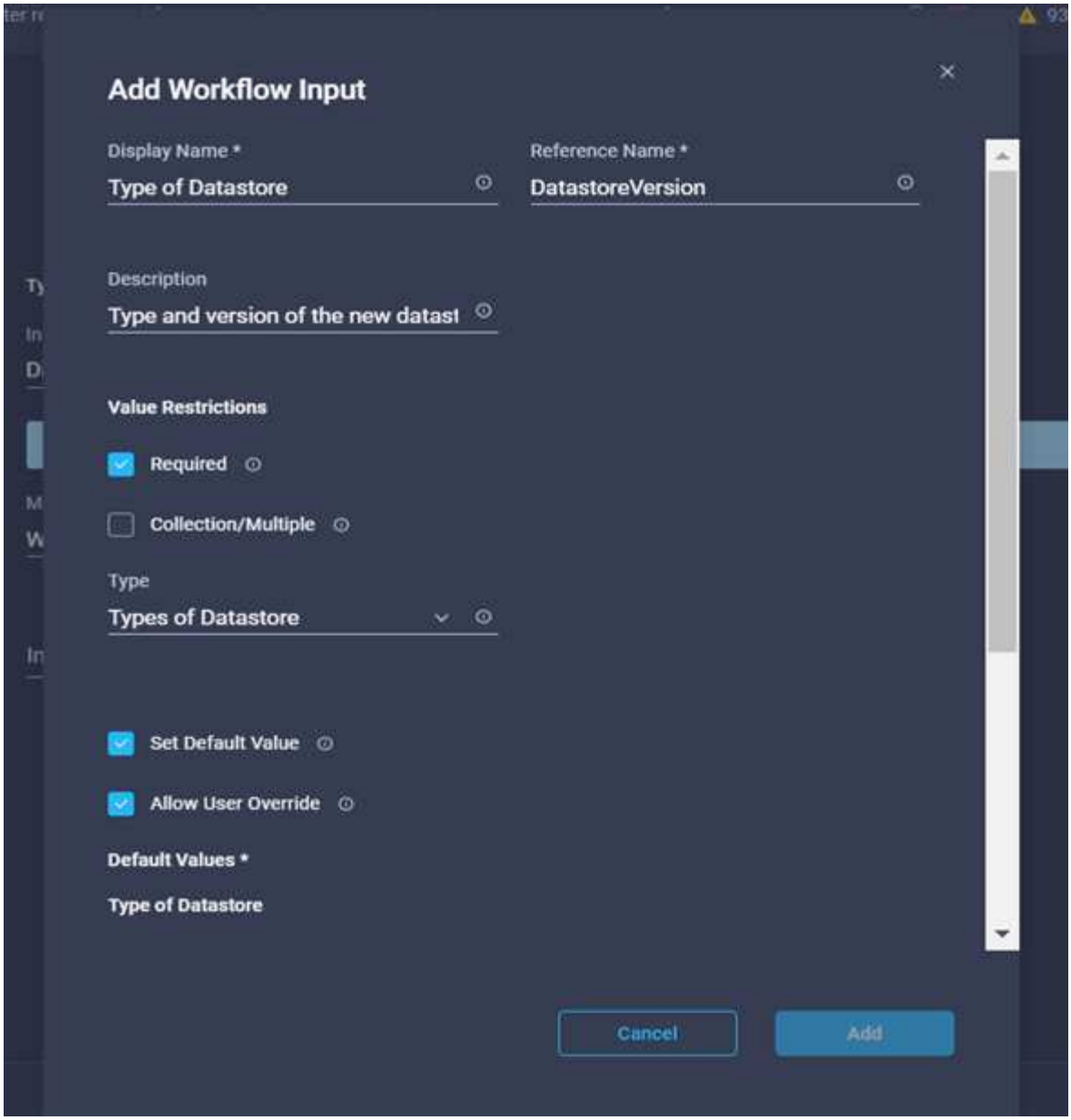


24. No assistente Adicionar entrada:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Clique em **obrigatório**.
    c. Clique em **Definir valor padrão e Substituir**.
    d. Forneça um valor padrão para o datastore e clique em **Add**.



25. Clique em **mapa**.
26. Clique em **Map** no campo de entrada **Type of datastore**.
27. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
28. Clique em **Input Name** e **Create Workflow Input**.

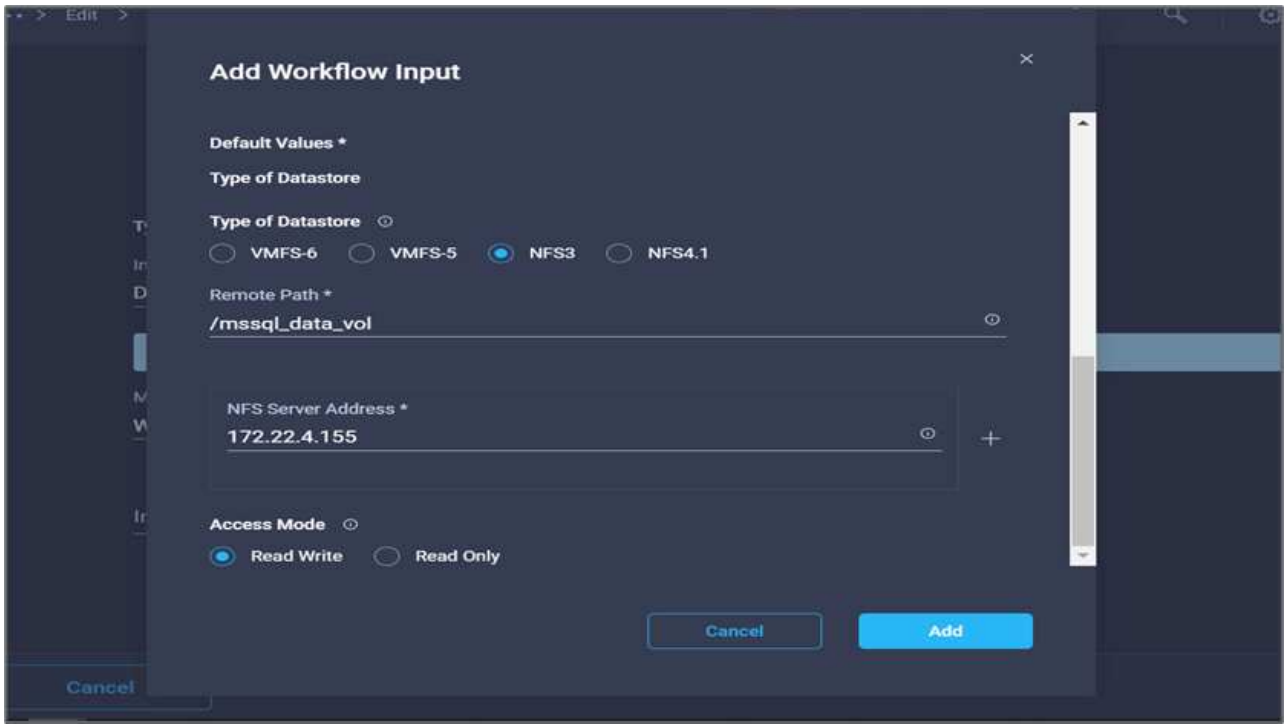
29. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional) e clique em **obrigatório**.
    b. Certifique-se de selecionar o tipo **tipos de datastore** e clique em **Definir valor padrão e Substituir**.



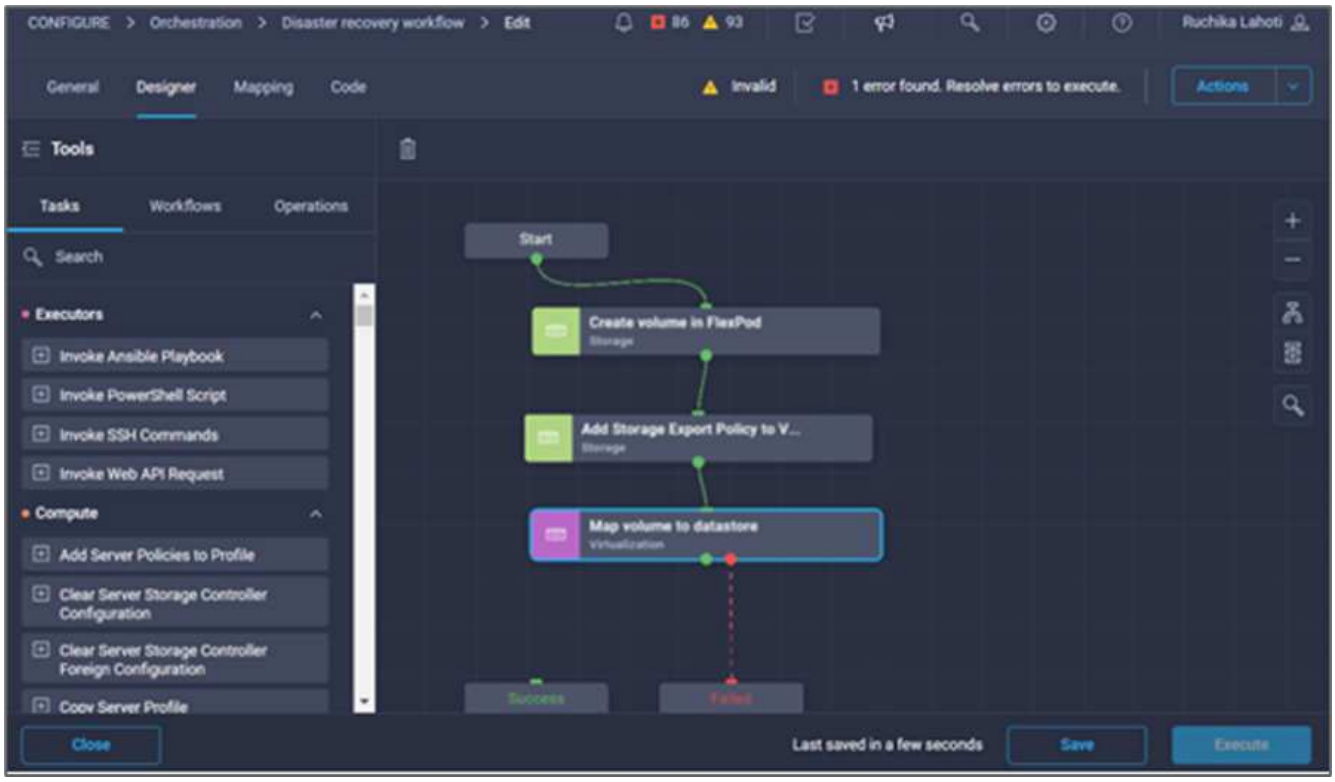
c. Forneça o caminho remoto. Este é o caminho remoto do ponto de montagem NFS.

d. Forneça os nomes de host ou endereços IP do servidor NFS remoto no endereço do servidor NFS.

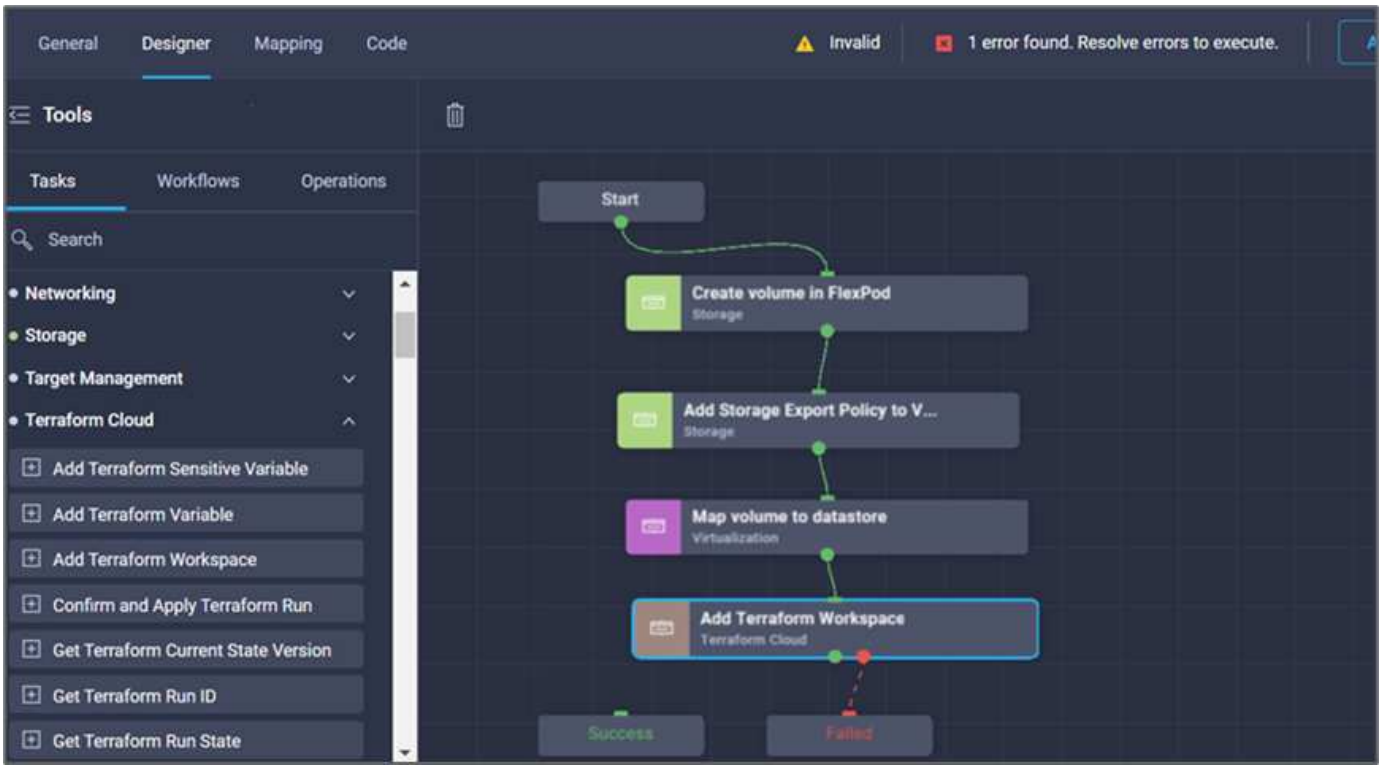
e. Clique no **modo de acesso**. O modo de acesso é para o servidor NFS. Clique em somente leitura se os volumes forem exportados como somente leitura. Clique em **Add**.



30. Clique em **mapa**.
31. Clique em **Salvar**.

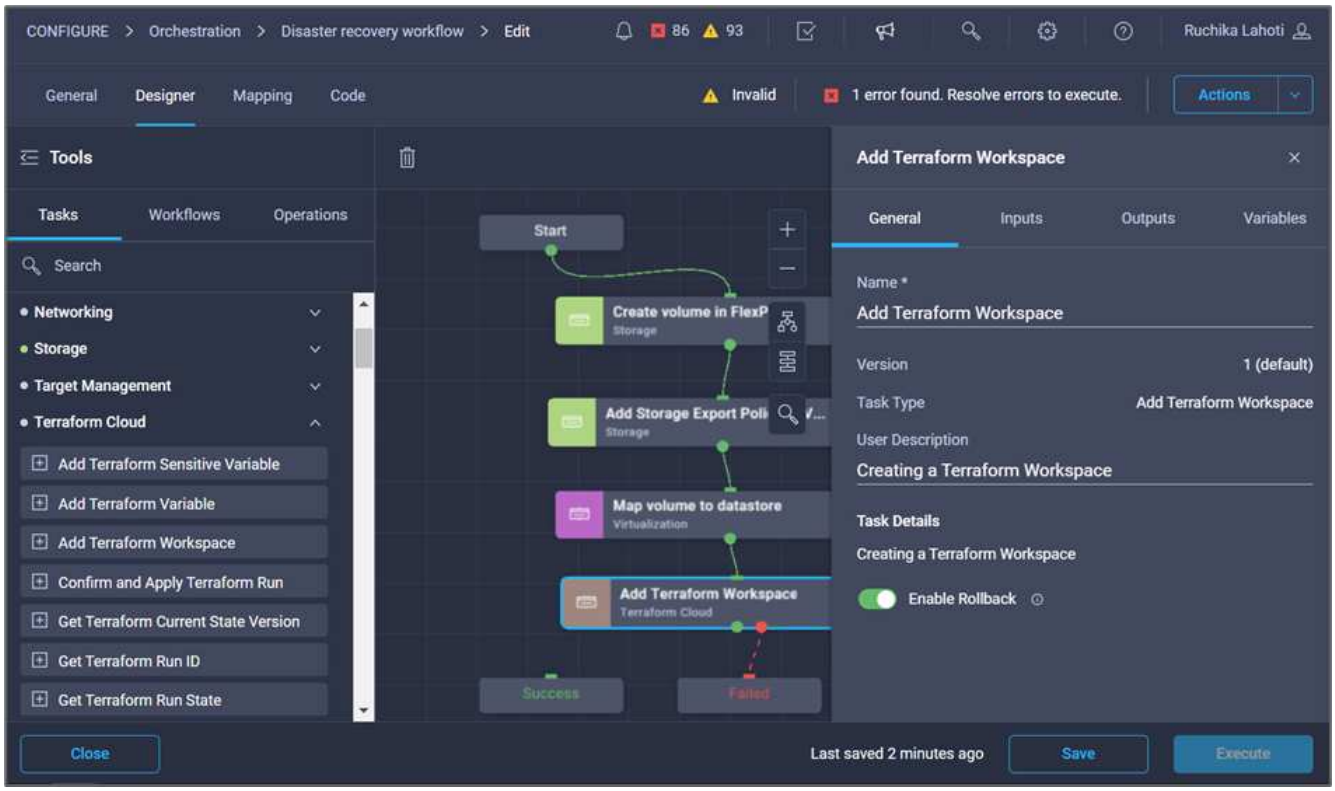


Isso conclui a tarefa de criar o datastore. Todas as tarefas realizadas no data center FlexPod local são concluídas.

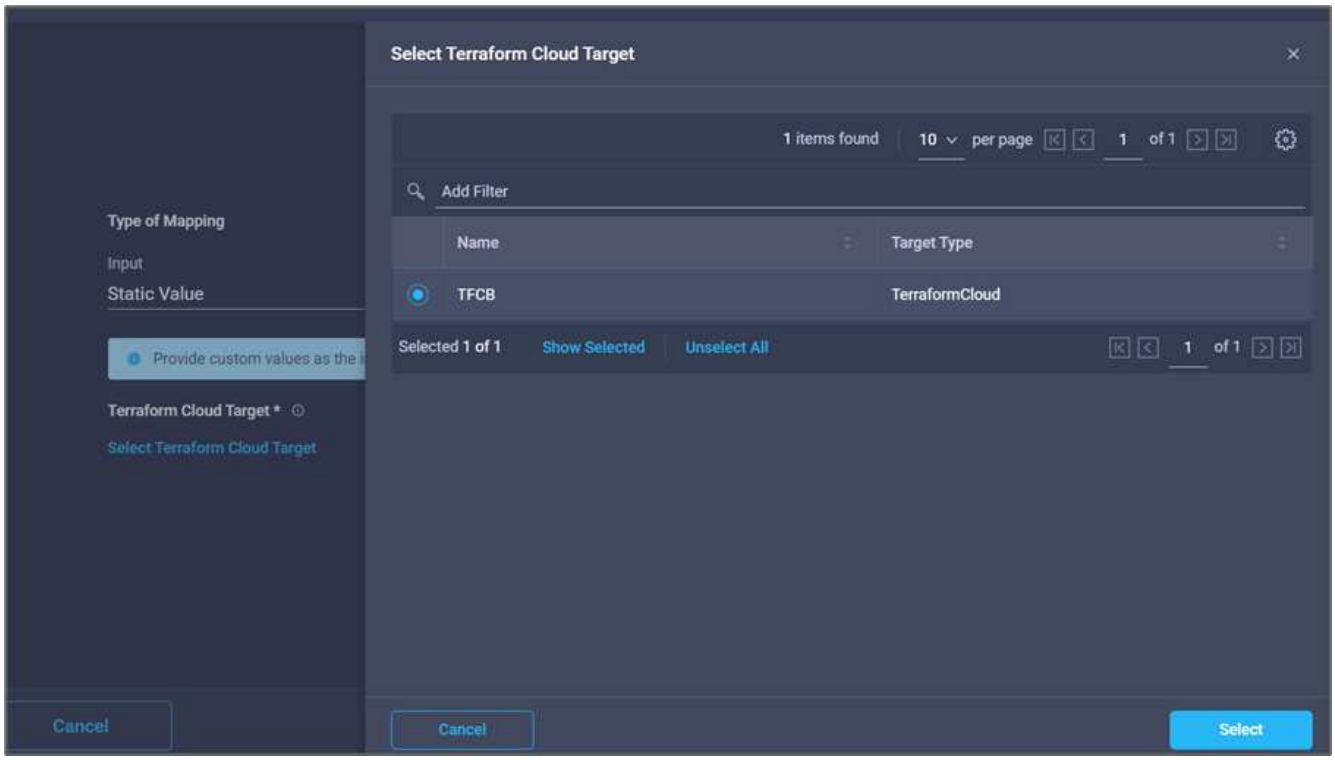


Procedimento 5: Adicione uma nova área de trabalho do Terraform

1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte a tarefa **Terraform Cloud > Adicionar espaço de trabalho do Terraform** na seção Ferramentas na área Design.
3. Use o conetor para conetar o **volume do mapa ao datastore** e **Adicionar tarefas do Terraform Workspace** e clique em **Salvar**.
4. Clique em **Add Terraform Workspace**. Na área Propriedades da tarefa, clique na guia **Geral**. Opcionalmente, você pode alterar o Nome e a Descrição para essa tarefa.

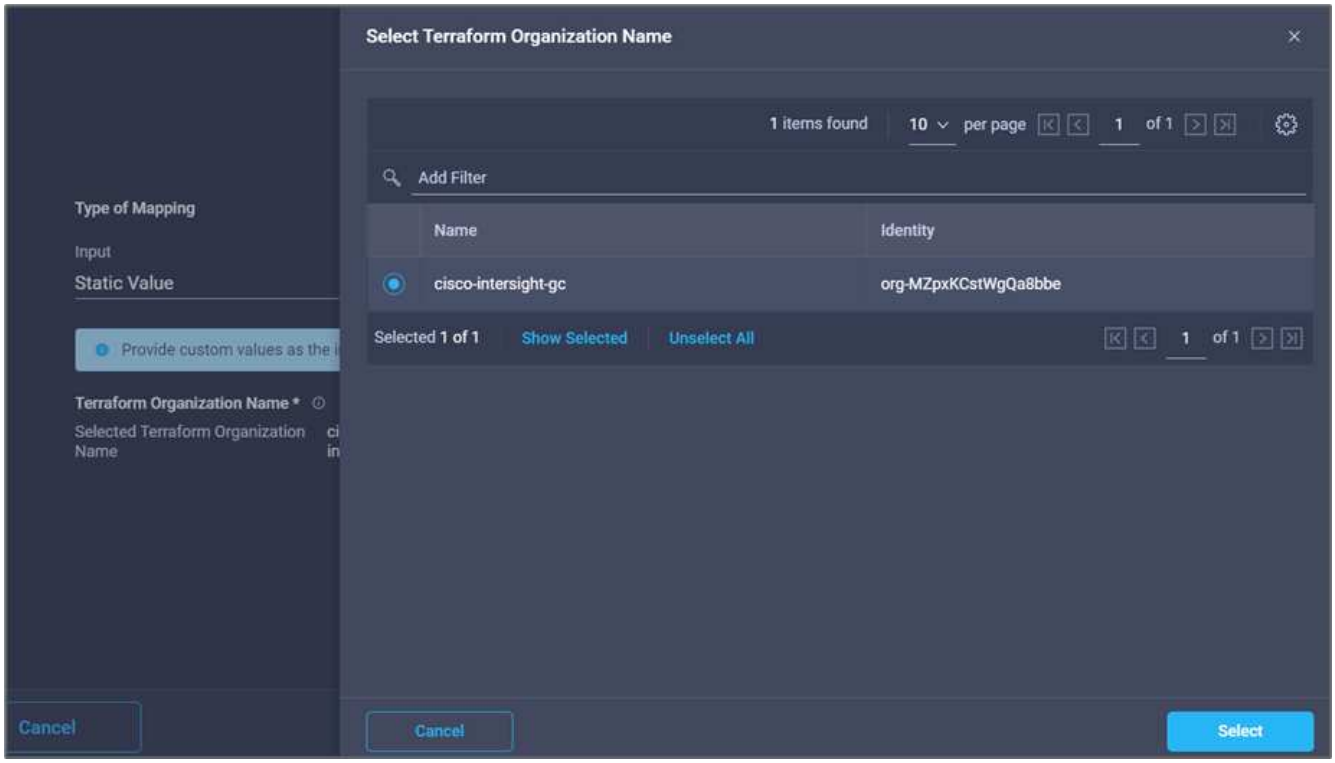


5. Na área Propriedades da tarefa, clique em **entradas**.
6. Clique em **Map** no campo de entrada **Terraform Cloud Target**.
7. Escolha **valor estático** e clique em **Select Terraform Cloud Target**. Selecione a conta Terraform Cloud for Business que foi adicionada conforme explicado em "Configurar o Serviço de Intersight do Cisco para o HashiCorp Terraform".".

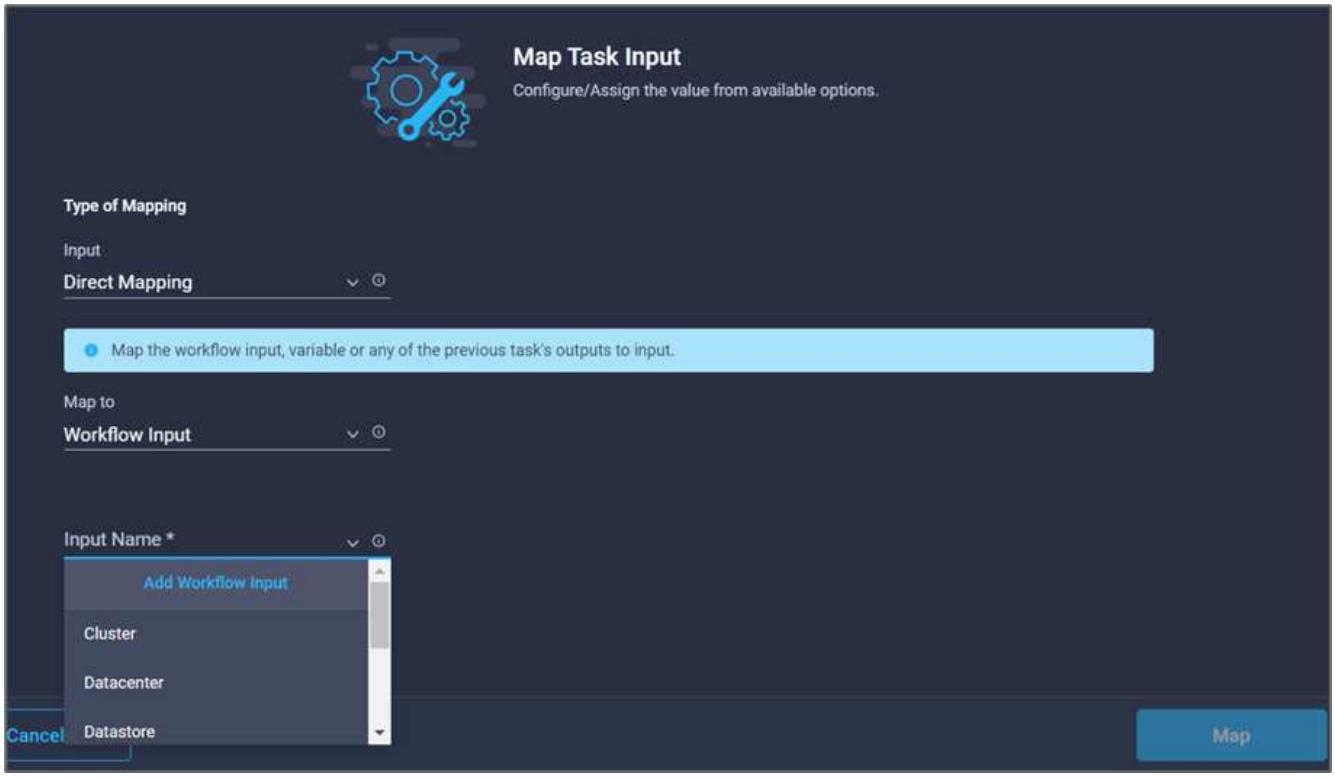


8. Clique em **mapa**.

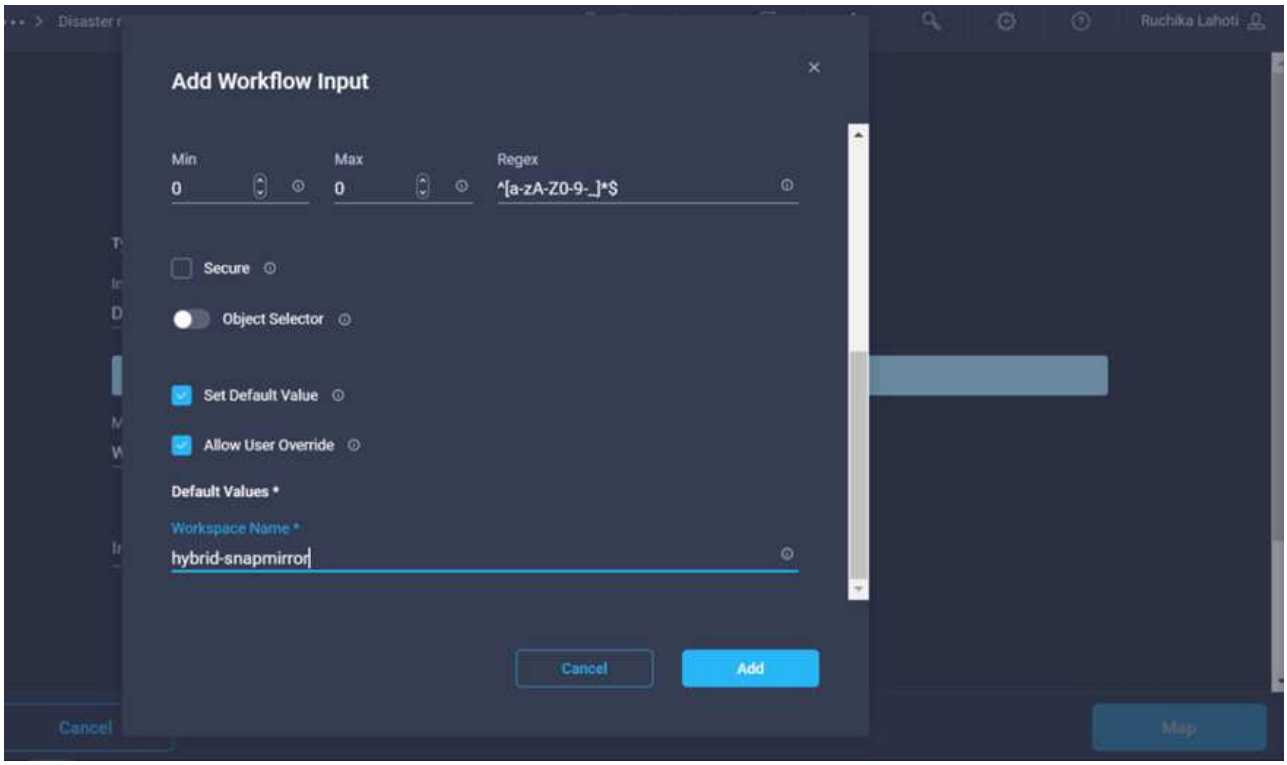
9. Clique em **Map** no campo de entrada **Terraform Organization Name**.
10. Escolha **Static Value** e clique em **Select Terraform Organization**. Selecione o nome da organização do Terraform que você faz parte da sua conta do Terraform Cloud para empresas.



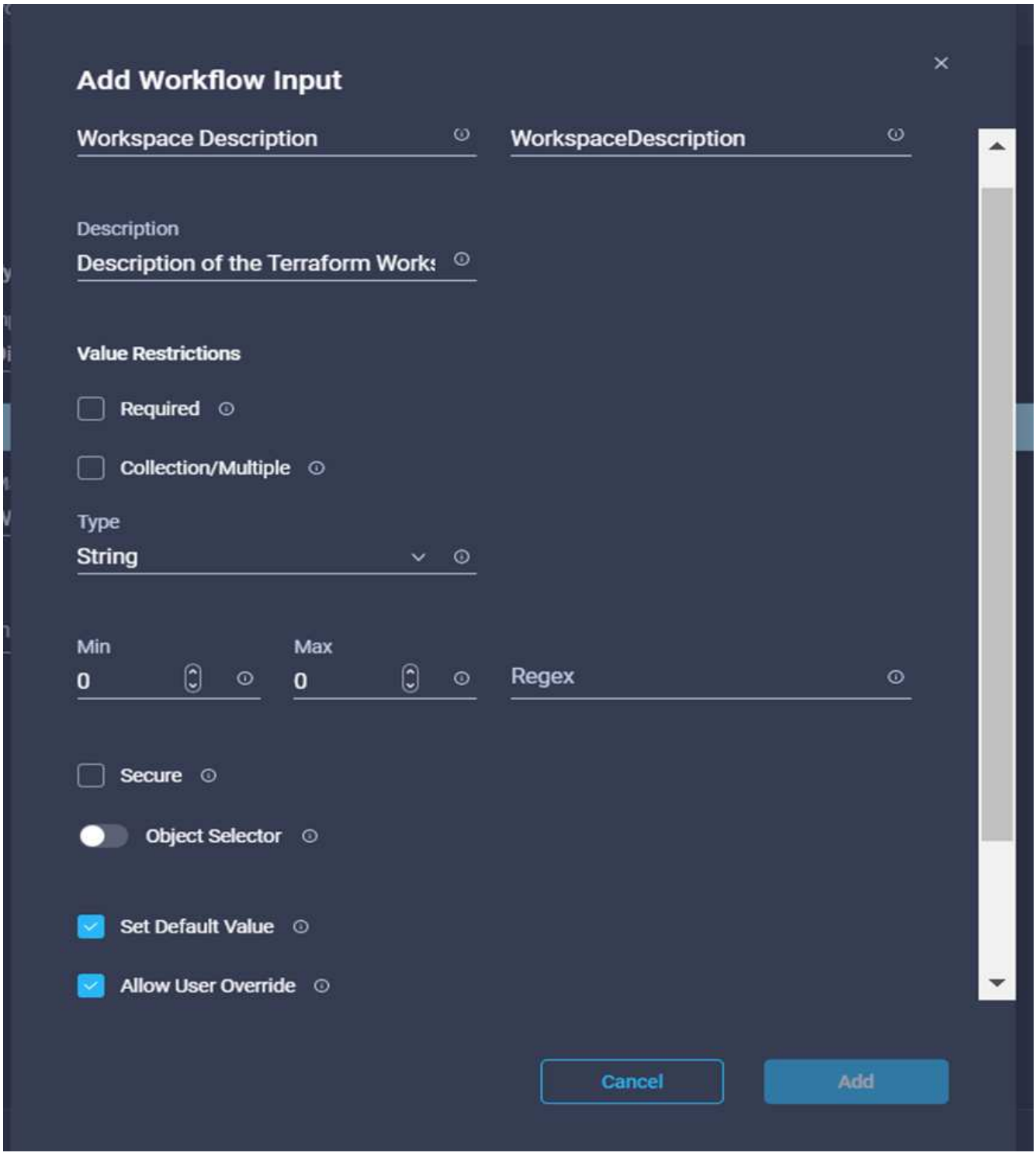
11. Clique em **mapa**.
12. Clique em **Map** no campo **Terraform Workspace Name**. Este é o novo workspace na conta do Terraform Cloud for Business.
13. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
14. Clique em **Input Name** e **Create Workflow Input**.



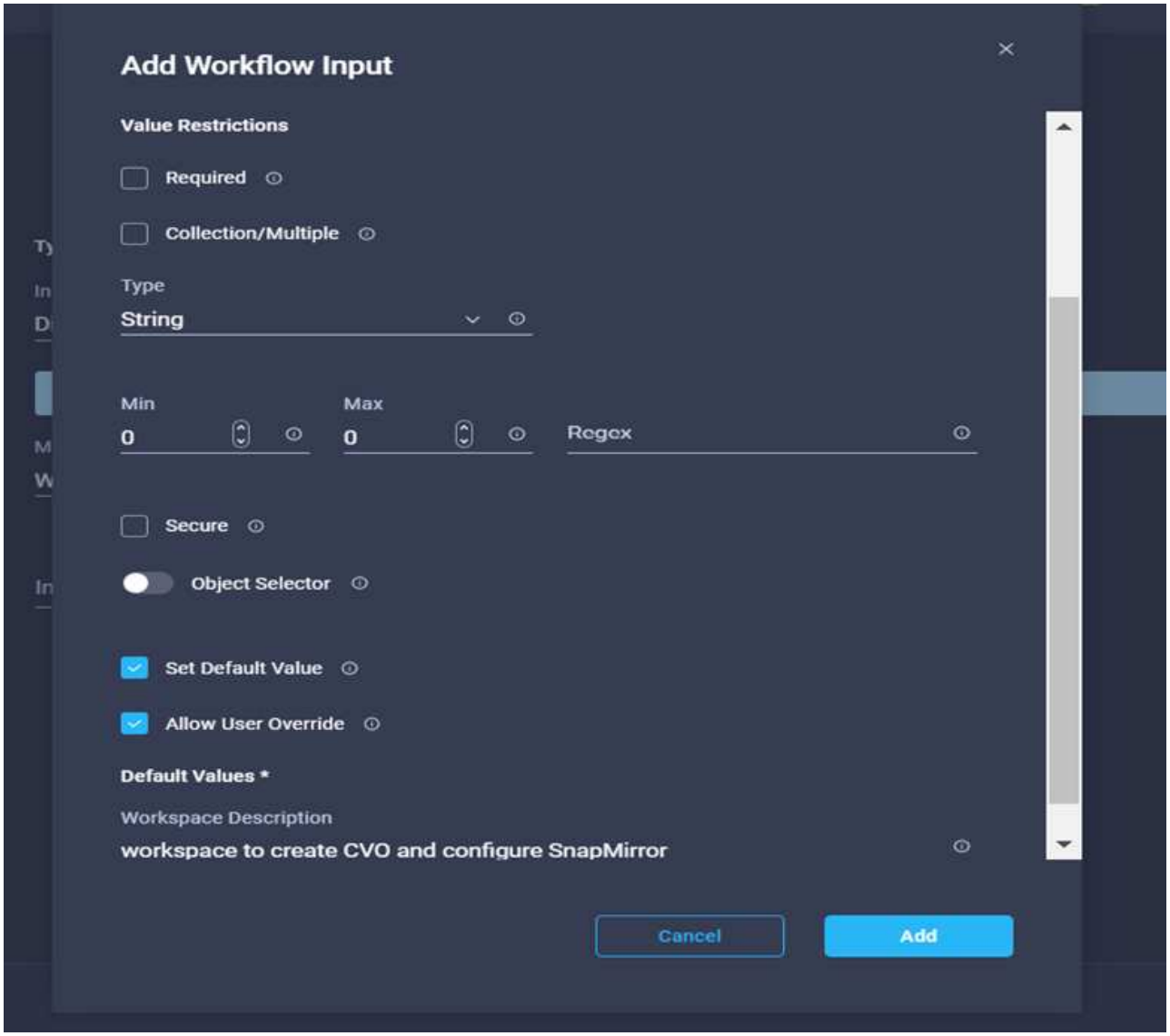
15. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Clique em **obrigatório**.
    c. Certifique-se de selecionar **String** para **Type**.
    d. Clique em **Definir valor padrão e Substituir**.
    e. Forneça um nome padrão para a área de trabalho.
    f. Clique em **Add**.



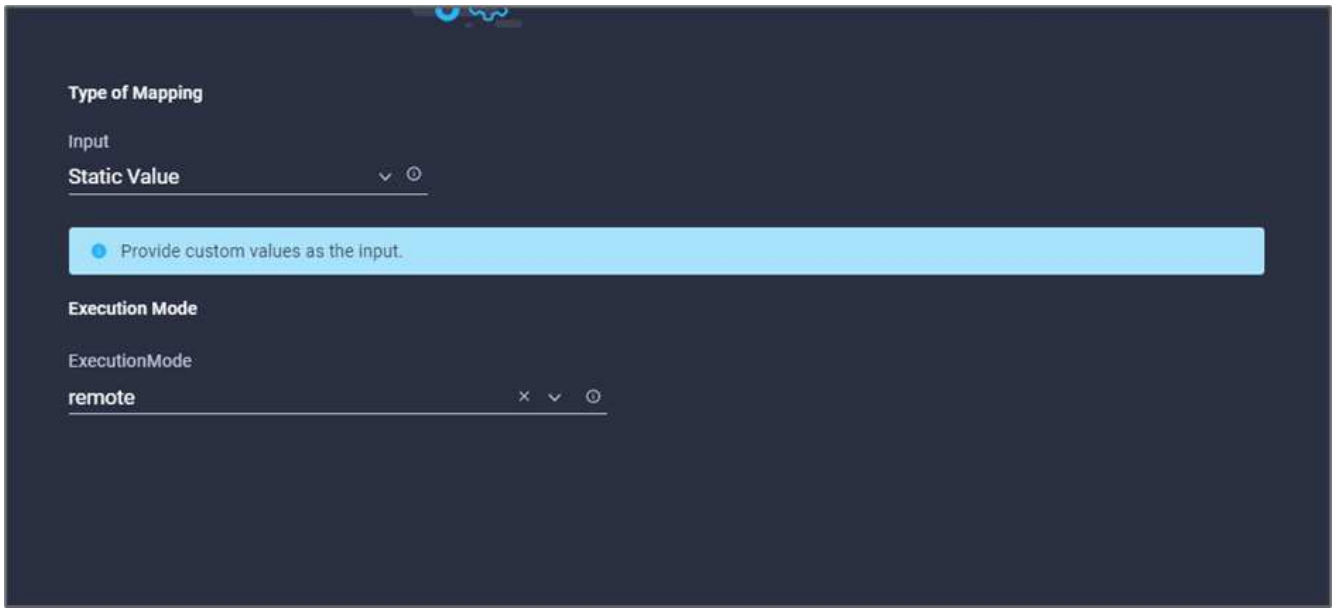
16. Clique em **mapa**.
17. Clique em **Map** no campo **Workspace Description**.
18. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
19. Clique em **Input Name** e **Create Workflow Input**.



20. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Certifique-se de selecionar **String** para **Type**.
    c. Clique em **Definir valor padrão e Substituir**.
    d. Forneça uma descrição da área de trabalho e clique em **Add**.



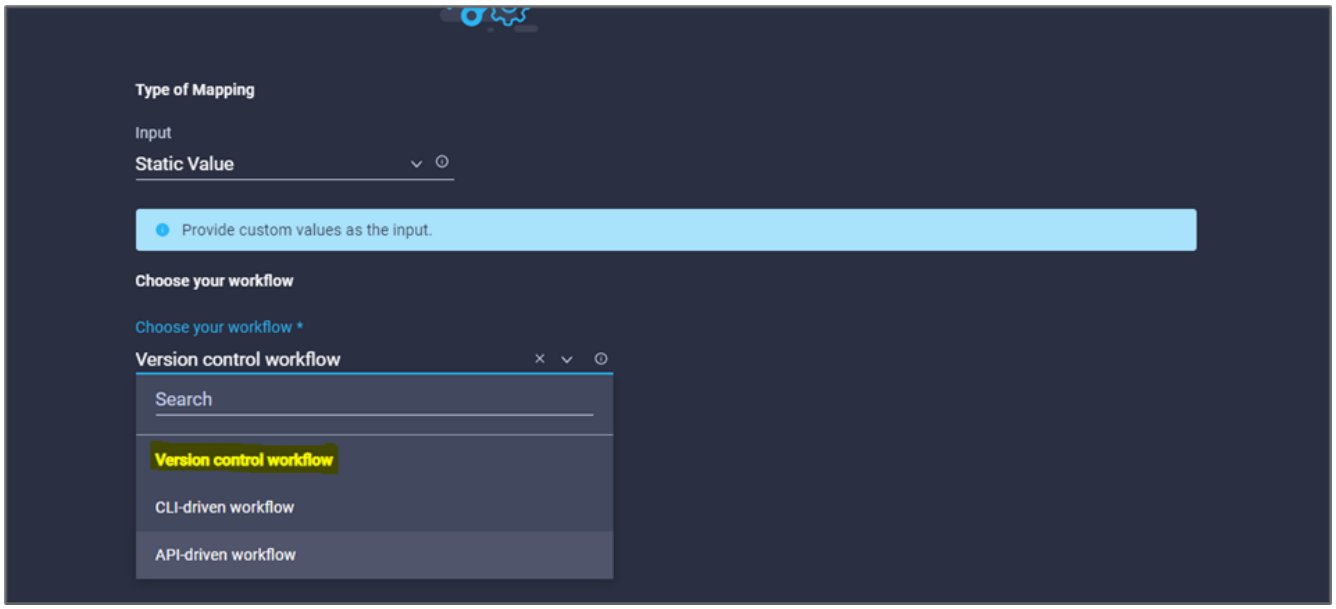
21. Clique em **mapa**.
22. Clique em **Map** no campo **Execution Mode** (modo de execução).
23. Escolha **valor estático**, clique em **modo de execução** e, em seguida, clique em **remoto**.



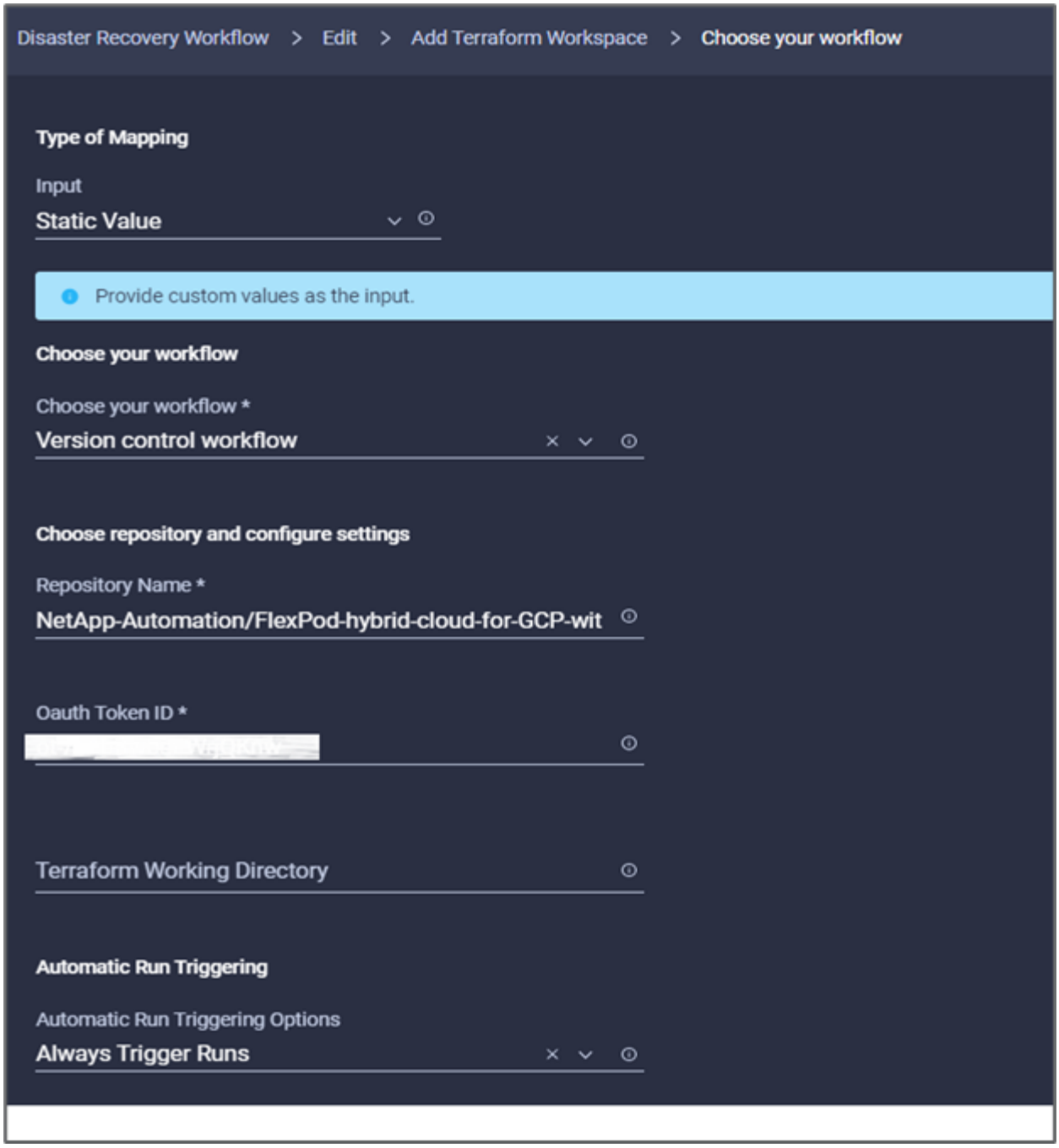
24. Clique em **mapa**.
25. Clique em **Map** no campo **Apply Method** (aplicar método).
26. Escolha **valor estático** e clique em **aplicar método**. Clique em **Manual Apply**.

27. Clique em **mapa**.
28. Clique em **Map** no campo **User Interface**.
29. Escolha **Static Value** e clique em **User Interface**. Clique em **Console UI**.

30. Clique em **mapa**.
31. Clique em **Map** no campo de entrada e selecione seu fluxo de trabalho.
32. Selecione **Static Value** e clique em **Choose Your Workflow**. Clique em **fluxo de trabalho de controle de versão**.



33. Forneça os seguintes detalhes do repositório do GitHub:
    a. Em **Nome do repositório**, insira o nome do repositório detalhado na ""Configurar pré-requisitos do ambiente""seção .
    b. Forneça o ID do token OAuth conforme detalhado na ""Configurar pré-requisitos do ambiente""seção .
    c. Selecione a opção **Automatic Run Triggering**.



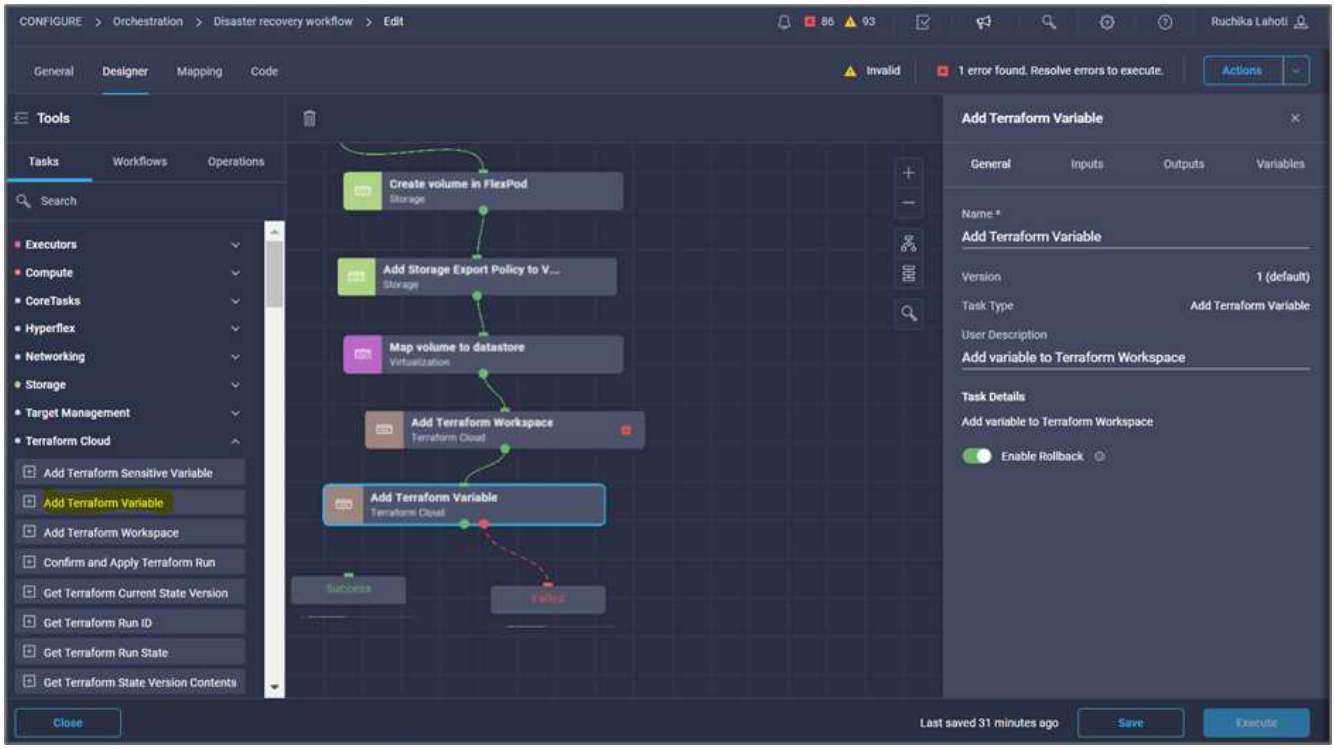
34. Clique em **mapa**.
35. Clique em **Salvar**.

Isso conclui a tarefa de criar uma área de trabalho em uma conta do Terraform Cloud for Business.

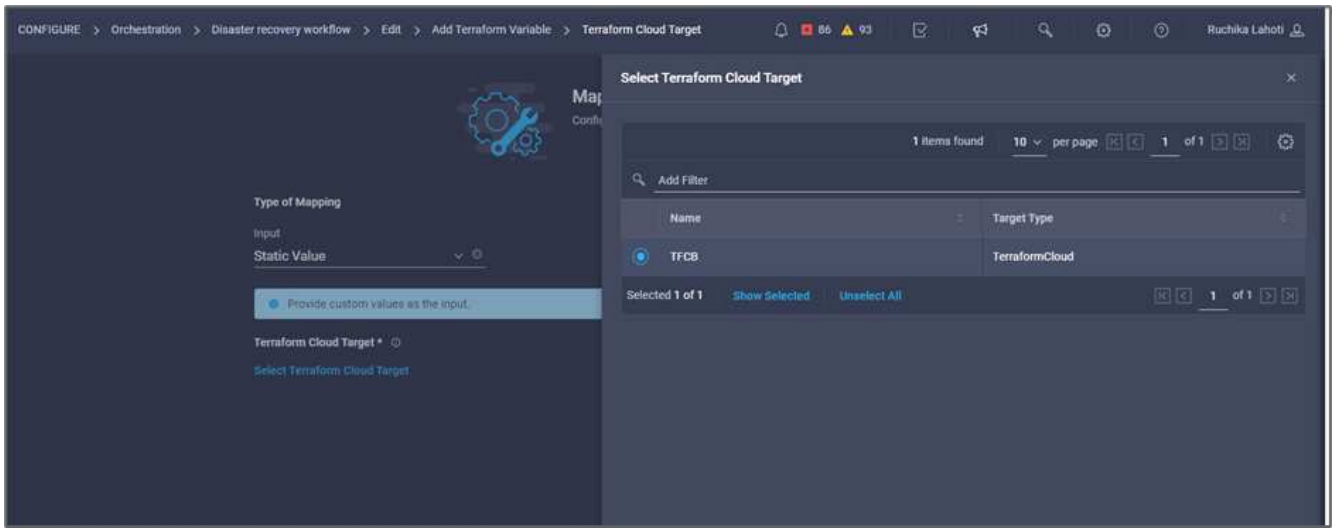
Procedimento 6: Adicione variáveis não sensíveis ao espaço de trabalho

1. Vá para a guia **Designer** e clique na seção **fluxos de trabalho de Ferramentas**.
2. Arraste e solte o fluxo de trabalho **Terraform > Add Terraform variables** na seção **Tools** na área **Design**.
3. Use o conetor para conetar as tarefas **Adicionar espaço de trabalho do Terraform** e **Adicionar variáveis do Terraform**. Clique em **Salvar**.
4. Clique em **Adicionar variáveis Terraform**. Na área **Propriedades do fluxo de trabalho**, clique na guia

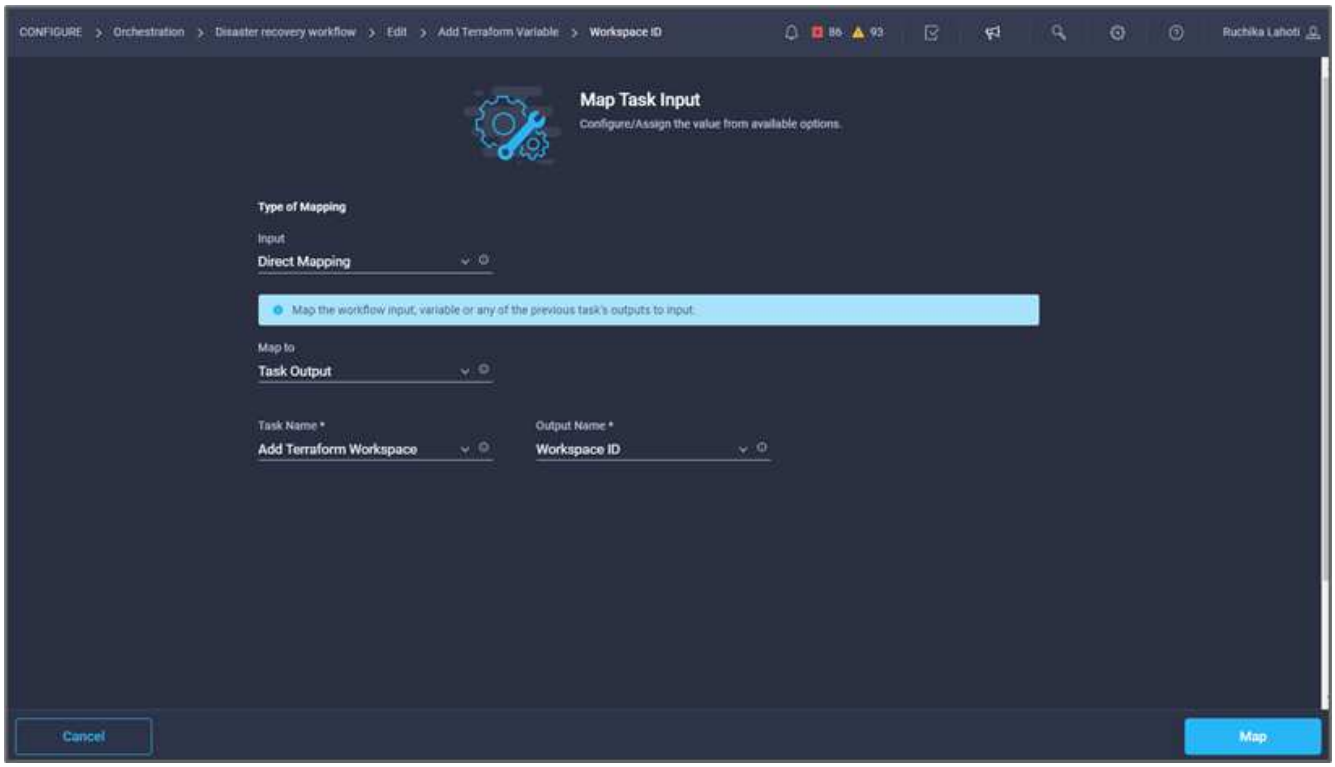
Geral. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa.



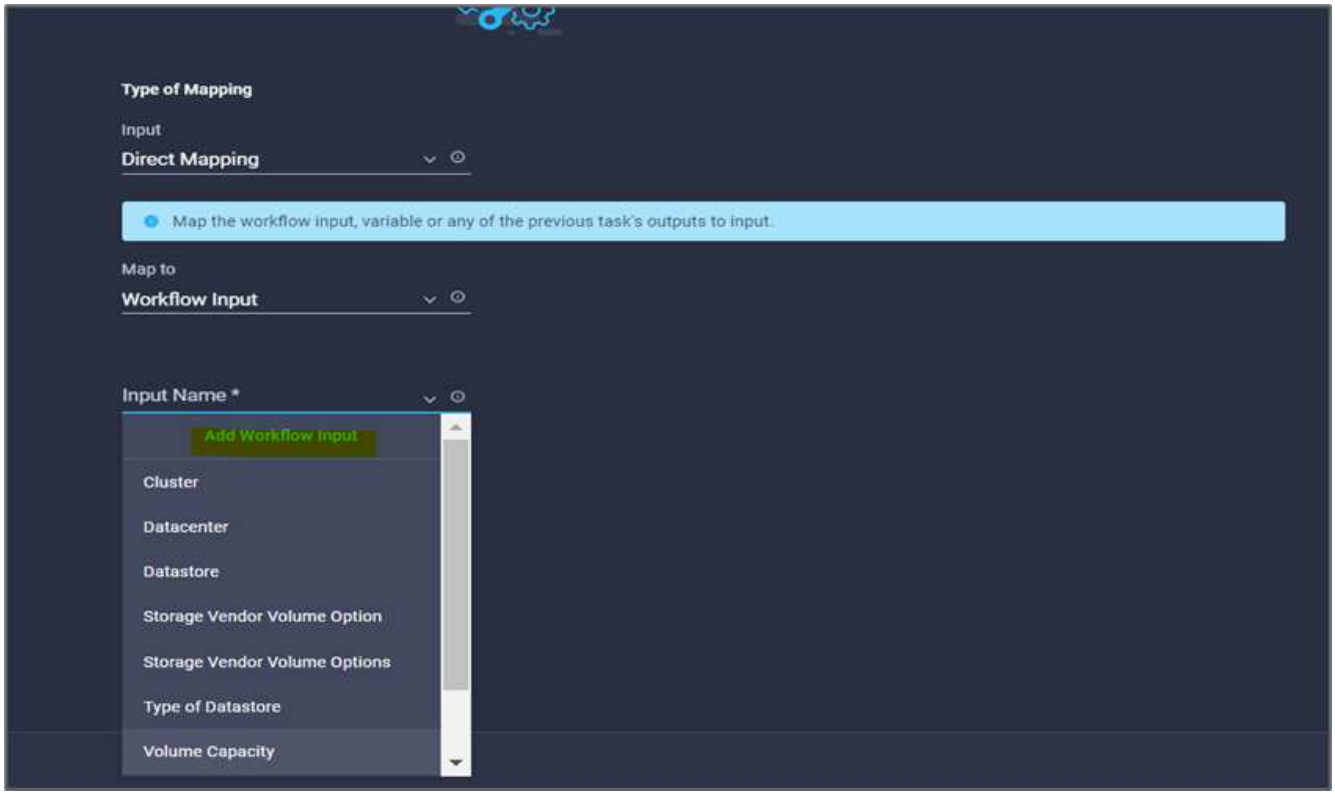
5. Na área **Propriedades do fluxo de trabalho**, clique em **entradas**.
6. Clique em **Map** no campo **Terraform Cloud Target**.
7. Escolha **valor estático** e clique em **Select Terraform Cloud Target**. Selecione a conta Terraform Cloud for Business que foi adicionada conforme explicado em "Configurar o Serviço de Intersight do Cisco para o HashiCorp Terraform".".



8. Clique em **mapa**.
9. Clique em **Map** no campo *Terraform Organization Name *.
10. Escolha **Static Value** e clique em **Select Terraform Organization**. Selecione o nome da organização do Terraform que você faz parte da sua conta do Terraform Cloud para empresas.

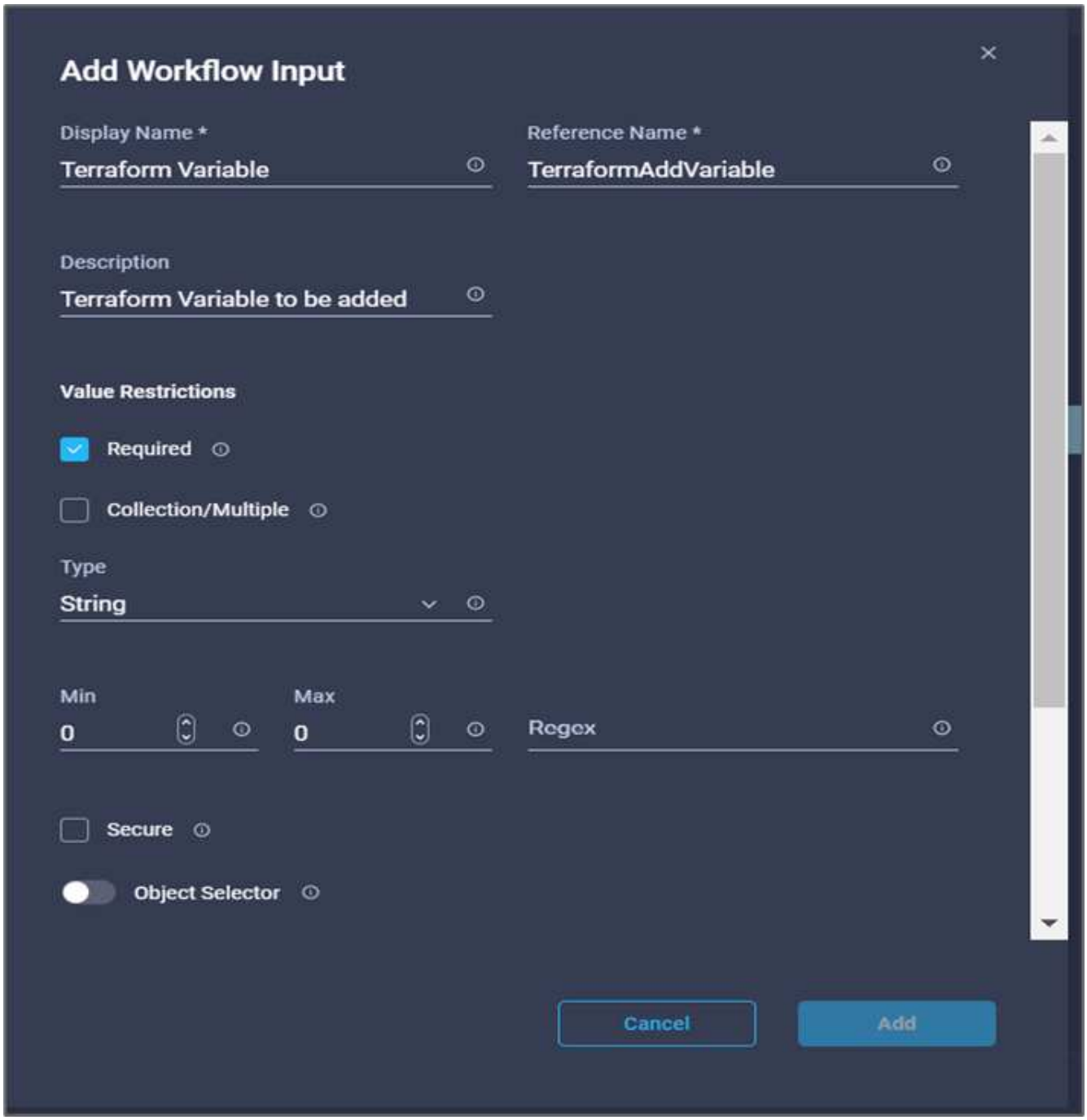


11. Clique em **mapa**.
12. Clique em **Map** no campo **Terraform Workspace Name**.
13. Escolha **Mapeamento direto** e clique em **saída de tarefa**.
14. Clique em **Nome da tarefa** e clique em **Adicionar espaço de trabalho do Terraform**.



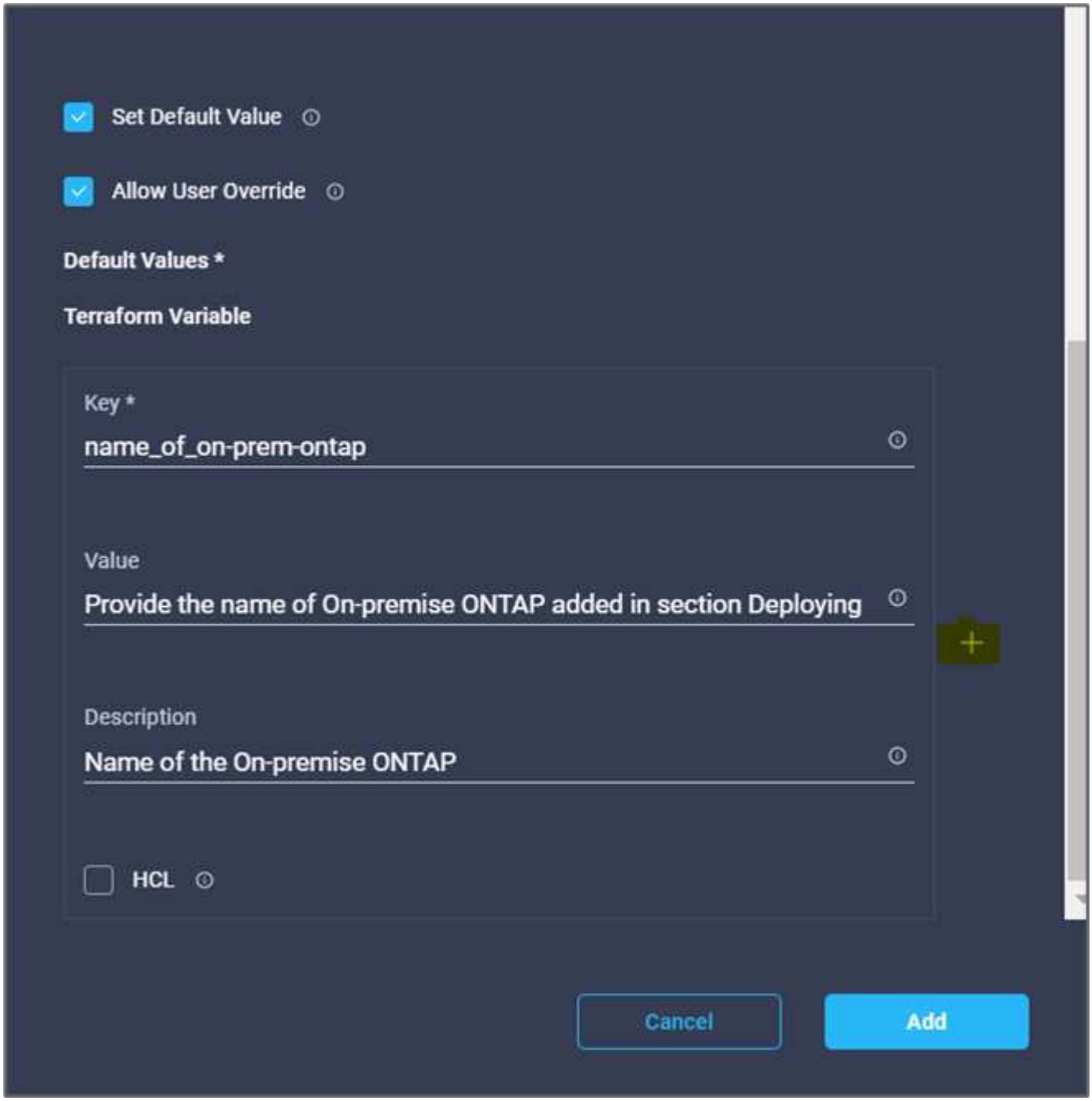
15. Clique em **Nome de saída** e clique em **Nome do espaço de trabalho**.

16. Clique em **mapa**.
17. Clique em **Map** no campo **Add Variables Options** (Adicionar opções de variáveis).
18. Escolha **Mapeamento direto** e clique em **Entrada do fluxo de trabalho**.
19. Clique em **Input Name** e **Create Workflow Input**.



20. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (Opcional).
    b. Certifique-se de selecionar **String** para **Type**.
    c. Clique em **Definir valor padrão e Substituir**.
    d. Clique em **tipo de variável** e, em seguida, clique em **variáveis não sensíveis**.

21. Na seção **Adicionar variáveis Terraform**, forneça as seguintes informações:
    - **Chave.** `name_of_on-prem-ontap`
    - **Valor.** Forneça o nome do ONTAP no local.
    - **Descrição.** Nome do ONTAP no local.
22. Clique em * para adicionar variáveis adicionais.

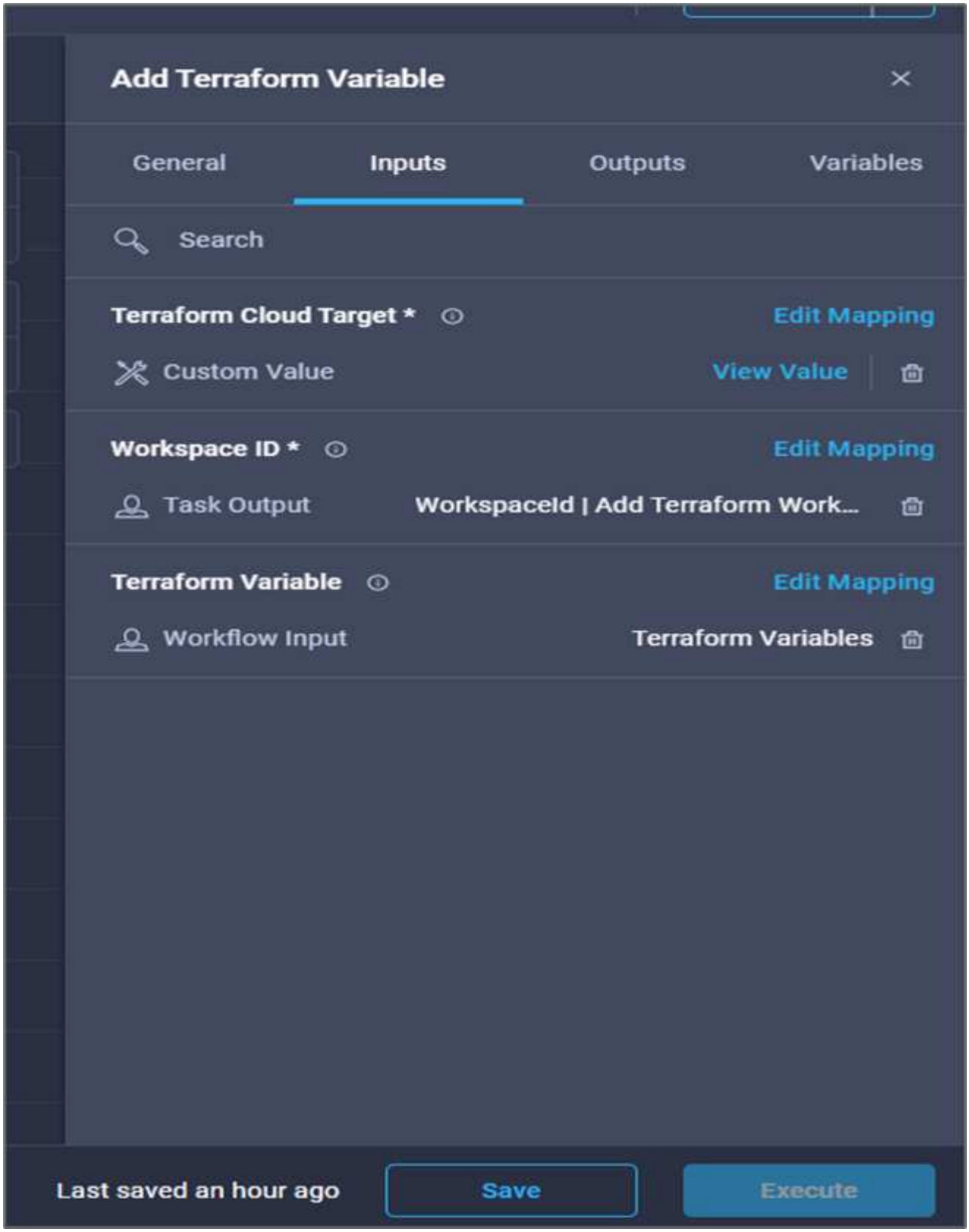


23. Adicione todas as variáveis do Terraform como mostrado na tabela a seguir. Você também pode fornecer um valor padrão.

Nome da variável Terraform	Descrição
name_of_on-prem-ONTAP	Nome do ONTAP no local (FlexPod)

Nome da variável Terraform	Descrição
on-premise-ONTAP_cluster_ip	O endereço IP da interface de gerenciamento do cluster de storage
on-premise-ONTAP_user_name	Nome de utilizador Admin para o cluster de armazenamento
Zona	Região do GCP onde o ambiente de trabalho será criado
subnet_id	ID de sub-rede do GCP onde o ambiente de trabalho será criado
vpc_id	O ID da VPC onde o ambiente de trabalho será criado
capacity_package_name	O tipo de licença a utilizar
source_volume (volume_fonte)	O nome do volume de origem
source_storage_vm_name	O nome da fonte SVM
volume_de destino	Nome do volume no Cloud Volumes ONTAP
schedule_of_reply	O padrão é 1 hora
name_of_volume_to_create_on_cvo	Nome do volume da nuvem
workspace_id	O Workspace_id onde o ambiente de trabalho será criado
Project_id	O project_id onde o ambiente de trabalho será criado
name_of_cvo_cluster	O nome do ambiente de trabalho Cloud Volumes ONTAP
gcp_service_account	gcp_Service_account do ambiente de trabalho do Cloud Volumes ONTAP

24. Clique em **Map** e depois em **Save**.



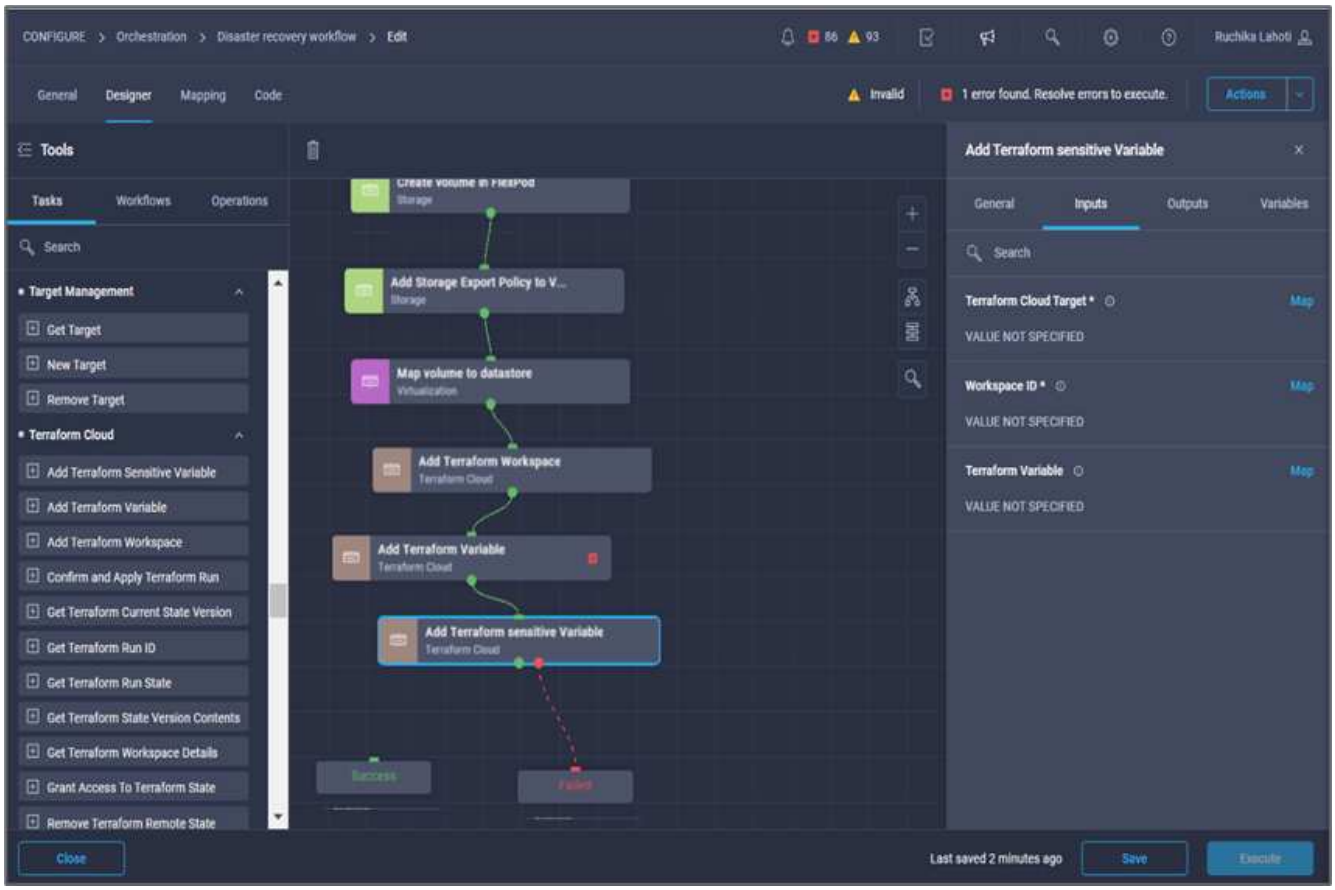
Isso conclui a tarefa de adicionar as variáveis Terraform necessárias à área de trabalho. Em seguida, adicione as variáveis Terraform sensíveis necessárias à área de trabalho. Você também pode combinar ambos em uma única tarefa.

Procedimento 7: Adicione variáveis sensíveis a uma área de trabalho

1. Vá para a guia **Designer** e clique em **fluxos de trabalho** na seção **Ferramentas**.
2. Arraste e solte o fluxo de trabalho **Terraform > Add Terraform variables** na seção **Tools** na área **Design**.
3. Use o conetor para conetar as duas tarefas **Adicionar espaço de trabalho do Terraform**. Clique em **Salvar**.

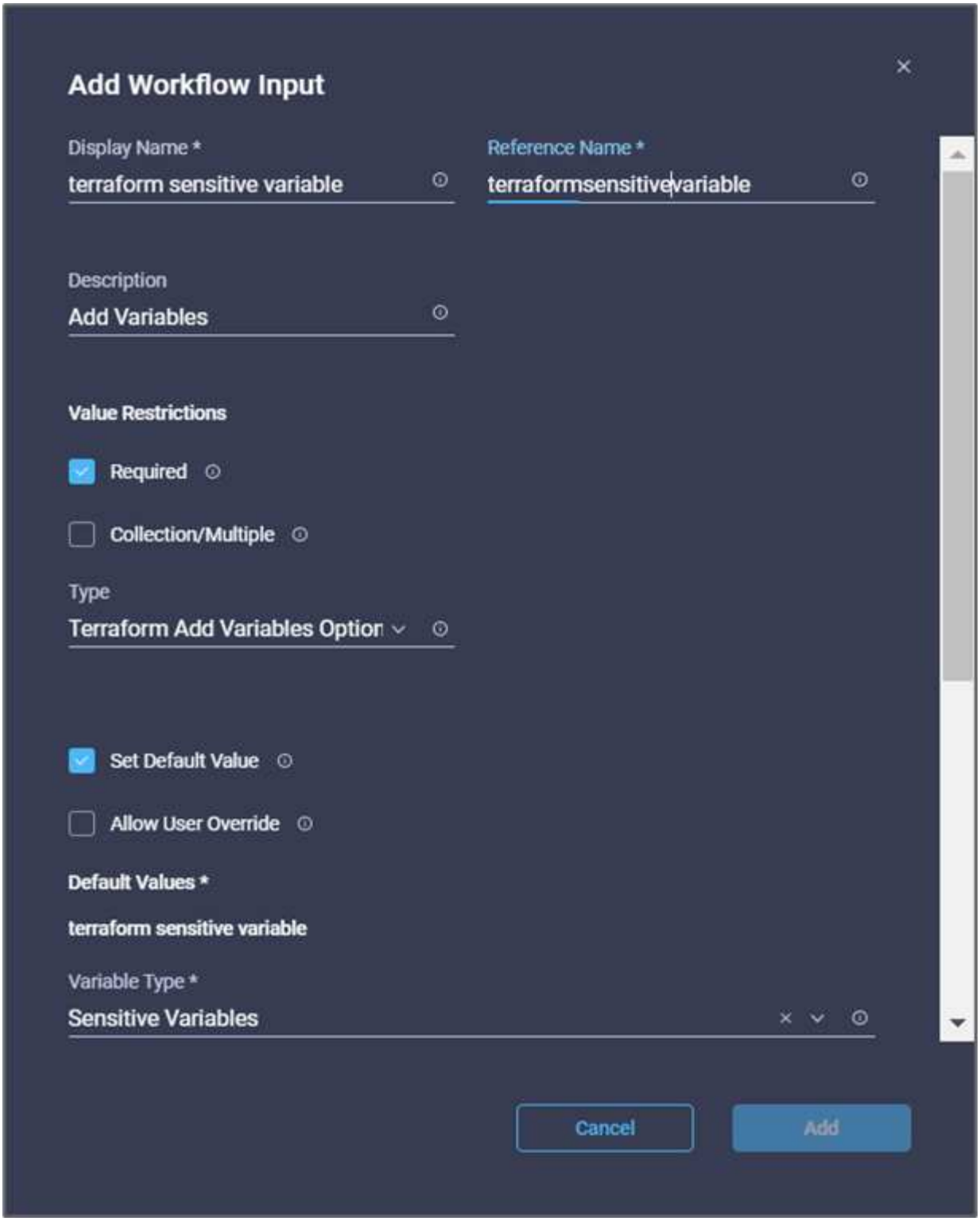
> É apresentado um aviso indicando que as duas tarefas têm o mesmo nome. Ignore o erro por enquanto porque você altera o nome da tarefa na próxima etapa.

4. Clique em **Adicionar variáveis Terraform**. Na área **Propriedades do fluxo de trabalho**, clique na guia **Geral**. Altere o nome para **Adicionar variáveis sensíveis ao Terraform**.



5. Na área **Propriedades do fluxo de trabalho**, clique em **entradas**.
6. Clique em **Map** no campo **Terraform Cloud Target**.
7. Escolha **valor estático** e clique em **Select Terraform Cloud Target**. Selecione a conta do Terraform Cloud for Business que foi adicionada na "Configurar o Serviço de Intersight do Cisco para o HashiCorp Terraform"seção ."
8. Clique em **mapa**.
9. Clique em **Map** no campo **Terraform Organization Name**.
10. Escolha **Static Value** e clique em **Select Terraform Organization**. Selecione o nome da organização do Terraform que você faz parte da sua conta do Terraform Cloud para empresas.
11. Clique em **mapa**.

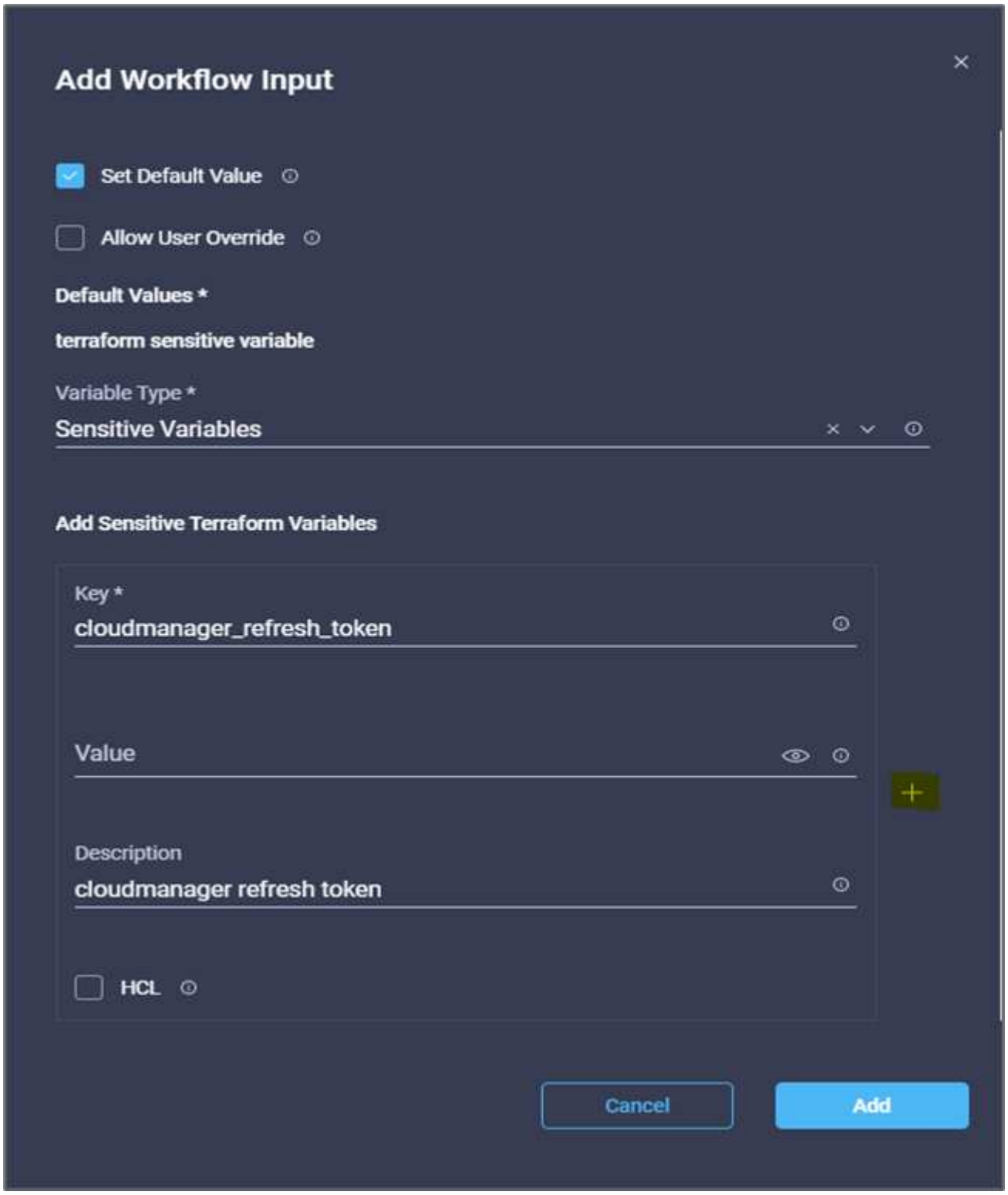
12. Clique em **Map** no campo **Terraform Workspace Name**.
13. Escolha **Mapeamento direto** e clique em **saída de tarefa**.
14. Clique em **Nome da tarefa** e em **Adicionar espaço de trabalho do Terraform**.
15. Clique em **Nome de saída** e clique na saída **Nome do espaço de trabalho**.
16. Clique em **mapa**.
17. Clique em **Map** no campo **Add Variables Options** (Adicionar opções de variáveis).
18. Escolha **Direct Mapping** e clique em **Workflow Input**.
19. Clique em **Input Name** e **Create Workflow Input**.
20. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Certifique-se de selecionar **Terraform Add Variables Options** para o tipo.
    c. Clique em **Definir valor padrão**.
    d. Clique em **tipo de variável** e, em seguida, clique em **variáveis sensíveis**.
    e. Clique em **Add**.



21. Na seção **Adicionar variáveis Terraform**, forneça as seguintes informações:

    - **Key.** `cloudmanager_refresh_token` .
    - **Valor.** Insira o token de atualização para as operações da API do NetApp Cloud Manager.
    - **Descrição.** Atualizar token.

Para obter mais informações sobre como obter um token de atualização para as operações da API do NetApp Cloud Manager, consulte a seção ""Configurar pré-requisitos do ambiente.""



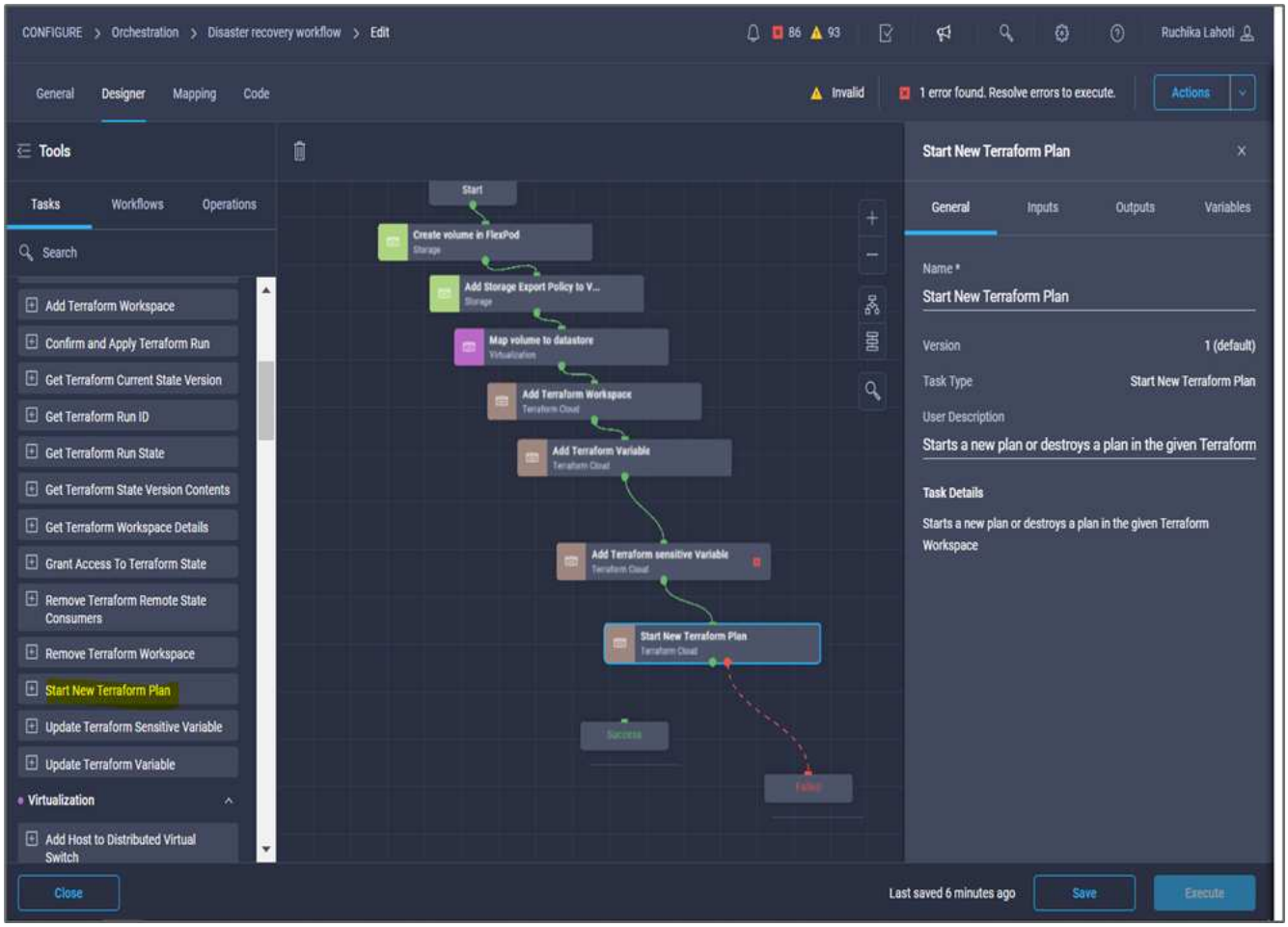
22. Adicione todas as variáveis sensíveis ao Terraform como mostrado na tabela abaixo. Você também pode fornecer um valor padrão.

Nome da variável sensível ao Terraform	Descrição
cloudmanager_refresh_token	Atualizar token. Obtenha-o de:
conetor_id	A ID do cliente do conetor do Cloud Manager. Obtenha-o de
cvo_admin_password	A senha de administrador do Cloud Volumes ONTAP
on-premise-ONTAP_user_password	Senha de administrador para o cluster de armazenamento

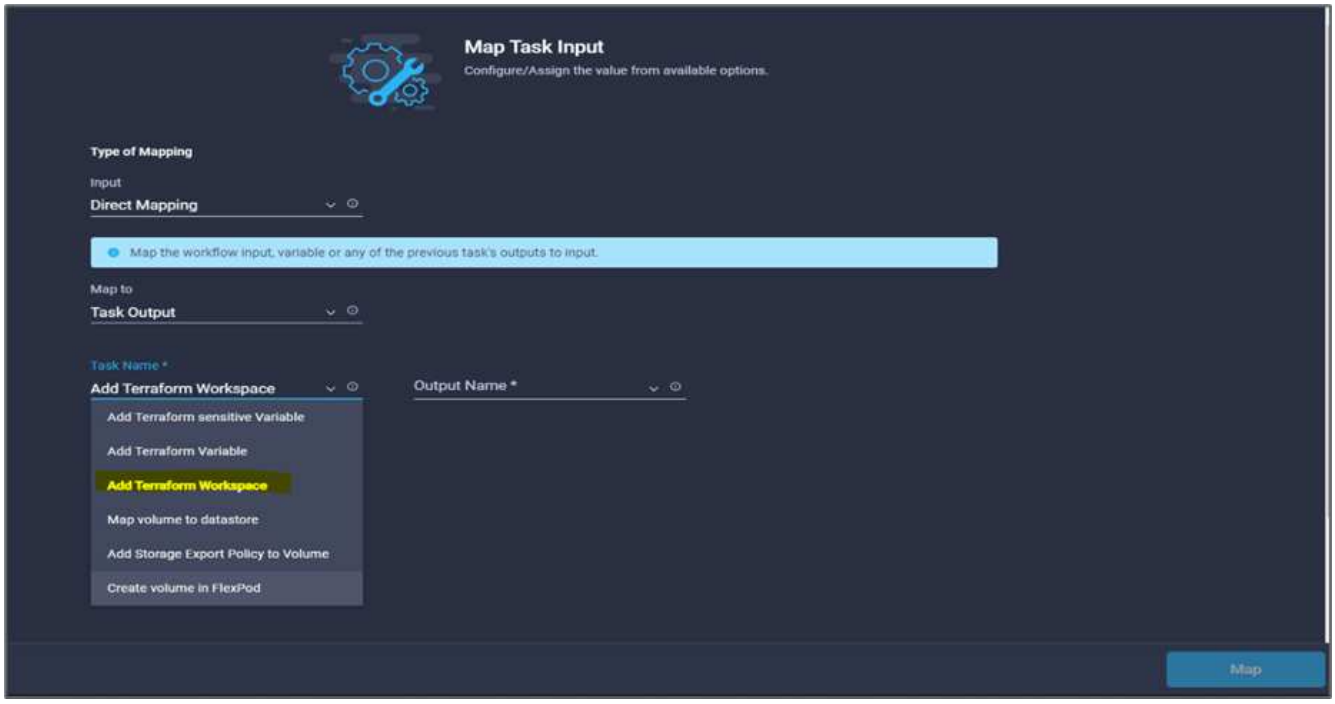
23. Clique em **Map**.isso conclui a tarefa de adicionar as variáveis sensíveis ao Terraform necessárias à área de trabalho. Em seguida, inicie um novo plano Terraform na área de trabalho configurada.

Procedimento 8: Inicie um novo plano Terraform

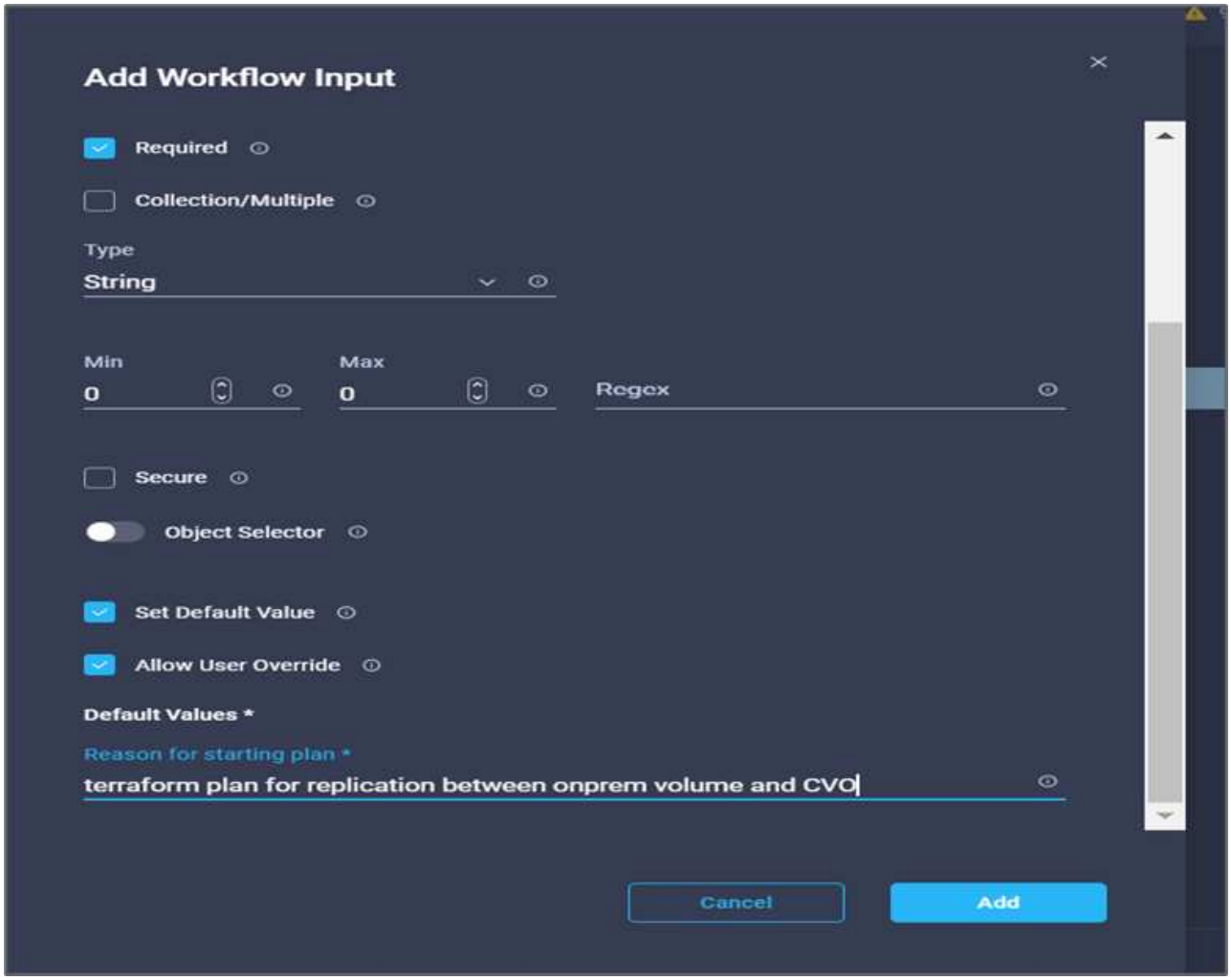
1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte a tarefa **Terraform Cloud > Iniciar novo plano Terraform** na seção **Ferramentas** na área **Design**.
3. Use o conetor para conetar entre as tarefas **Adicionar variáveis sensíveis ao Terraform** e **Iniciar novas tarefas do plano Terraform**. Clique em **Salvar**.
4. Clique em **Iniciar novo plano Terraform**. Na área **Propriedades da tarefa**, clique na guia **Geral**. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa.



5. Na área **Task Properties**, clique em **Inputs**.
6. Clique em **Map** no campo **Terraform Cloud Target**.
7. Escolha **valor estático** e clique em **Select Terraform Cloud Target**. Selecione a conta Terraform Cloud for Business que foi adicionada na seção "Configurando o serviço Cisco Intersight para HashiCorp Terraform".
8. Clique em **mapa**.
9. Clique em **Map** no campo **Workspace ID**.
10. Escolha **Mapeamento direto** e clique em **saída de tarefa**.
11. Clique em **Nome da tarefa** e em **Adicionar espaço de trabalho do Terraform**.



12. Clique em **Nome de saída**, **ID do espaço de trabalho** e, em seguida, em **mapa**.
13. Clique em **mapa** no campo **motivo para iniciar o plano**.
14. Escolha **Direct Mapping** e clique em **Workflow Input**.
15. Clique em **Input Name** e em **Create Workflow Input**.
16. No assistente Adicionar entrada, execute as seguintes etapas:
    a. Forneça um nome de exibição e um nome de referência (opcional).
    b. Certifique-se de selecionar **String** para **Type**.
    c. Clique em **Definir valor padrão e Substituir**.
    d. Insira um valor padrão para **motivo para iniciar o plano** e clique em **Adicionar**.



17. Clique em **mapa**.
18. Clique em **Map** no campo **Plan Operation** (operação do plano).
19. Escolha **Static Value** e clique em **Plan Operation**. Clique em **novo plano**.

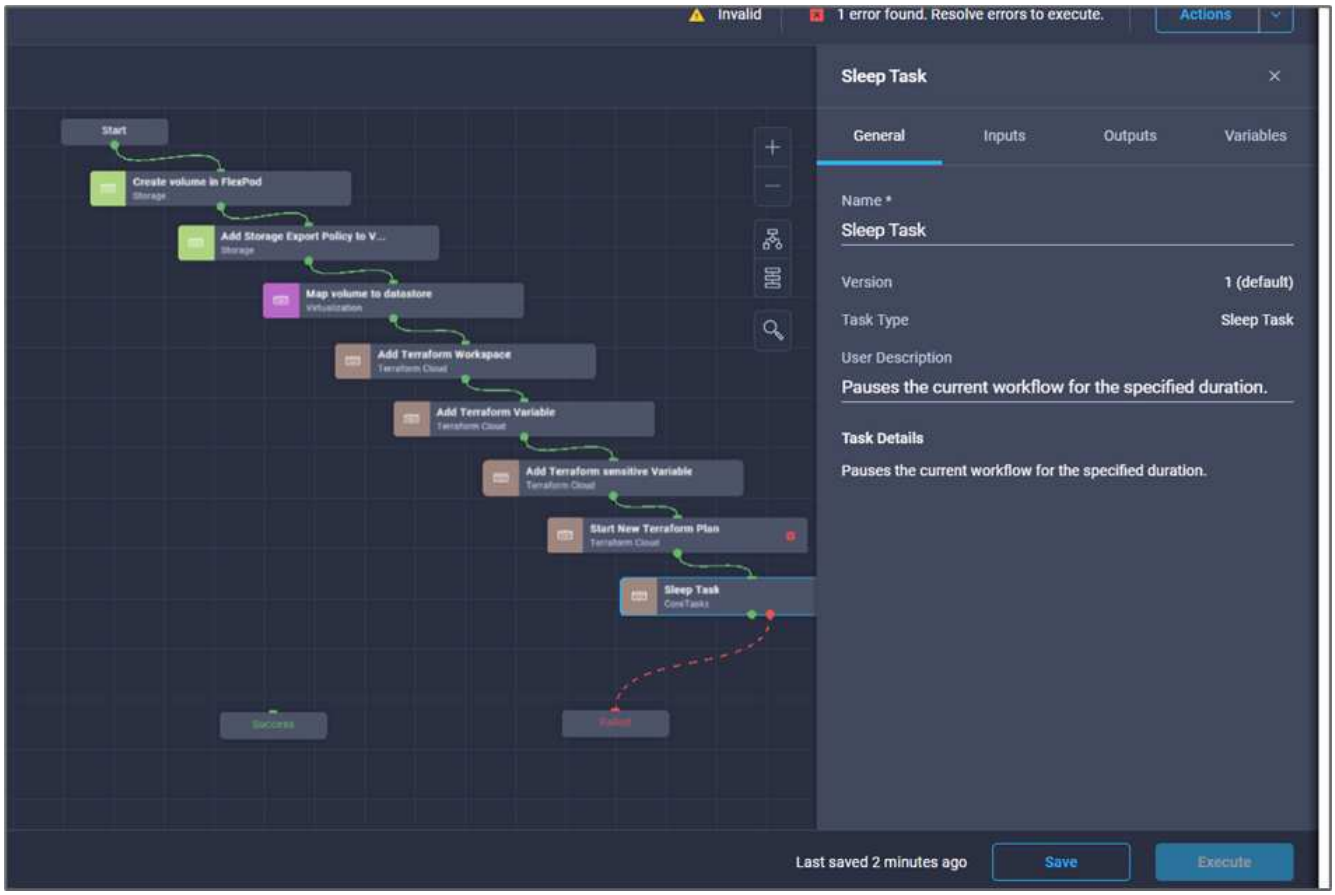
20. Clique em **mapa**.
21. Clique em **Salvar**.

Isso conclui a tarefa de adicionar um plano Terraform na conta Terraform Cloud for Business. Em seguida, crie uma tarefa de suspensão por alguns segundos.

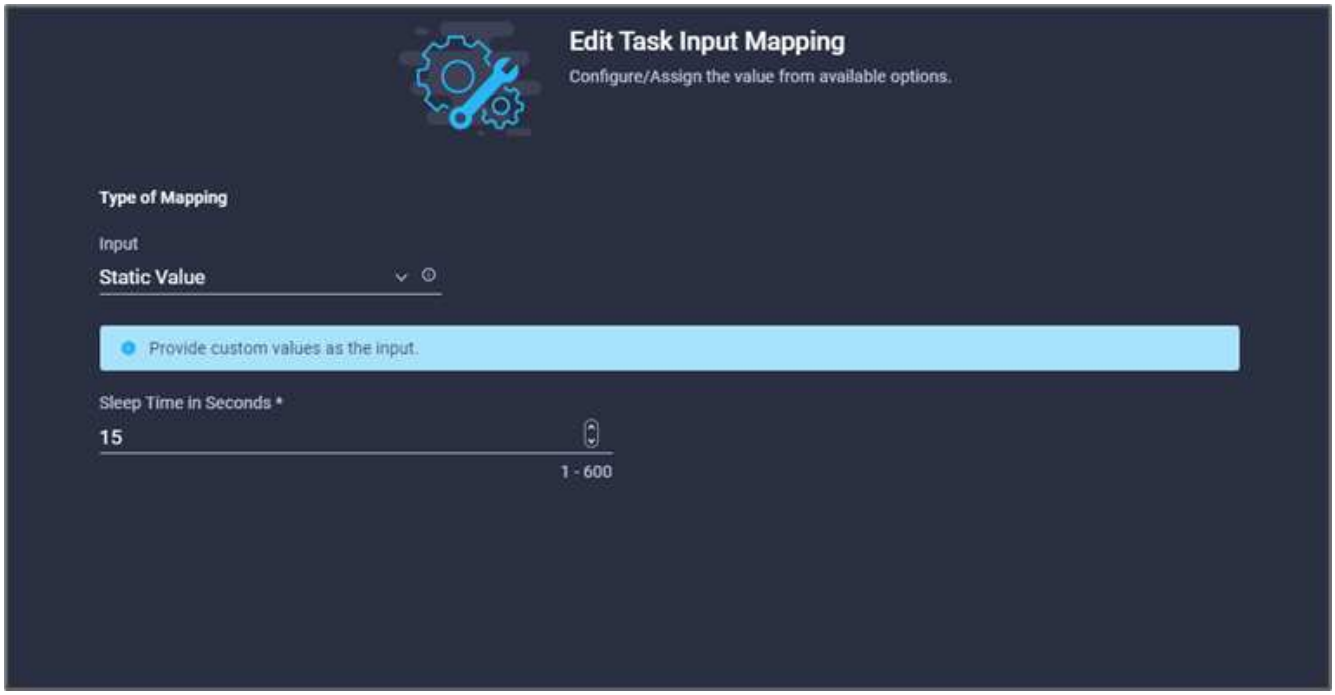
Procedimento 9: Tarefa de suspensão para sincronização

O Terraform Apply requer RunID, que é gerado como parte da tarefa do plano Terraform. Esperar alguns segundos entre o Terraform Plan e as ações aplicar do Terraform evitam problemas de tempo.

1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte as **tarefas principais > tarefa de suspensão** da seção **Ferramentas** na área **Design**.
3. Use o conetor para conetar as tarefas **Iniciar novo plano Terraform** e **tarefa de suspensão**. Clique em **Salvar**.



4. Clique em **Sleep Task**. Na área **Propriedades da tarefa**, clique na guia **Geral**. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa. Neste exemplo, o nome da tarefa é **Sincronizar**.
5. Na área **Task Properties**, clique em **Inputs**.
6. Clique em **Map** no campo **Sleep Time in Seconds** (tempo de inatividade em segundos).
7. Escolha **Static value** e insira **15** em para **Sleep Time in Seconds**.

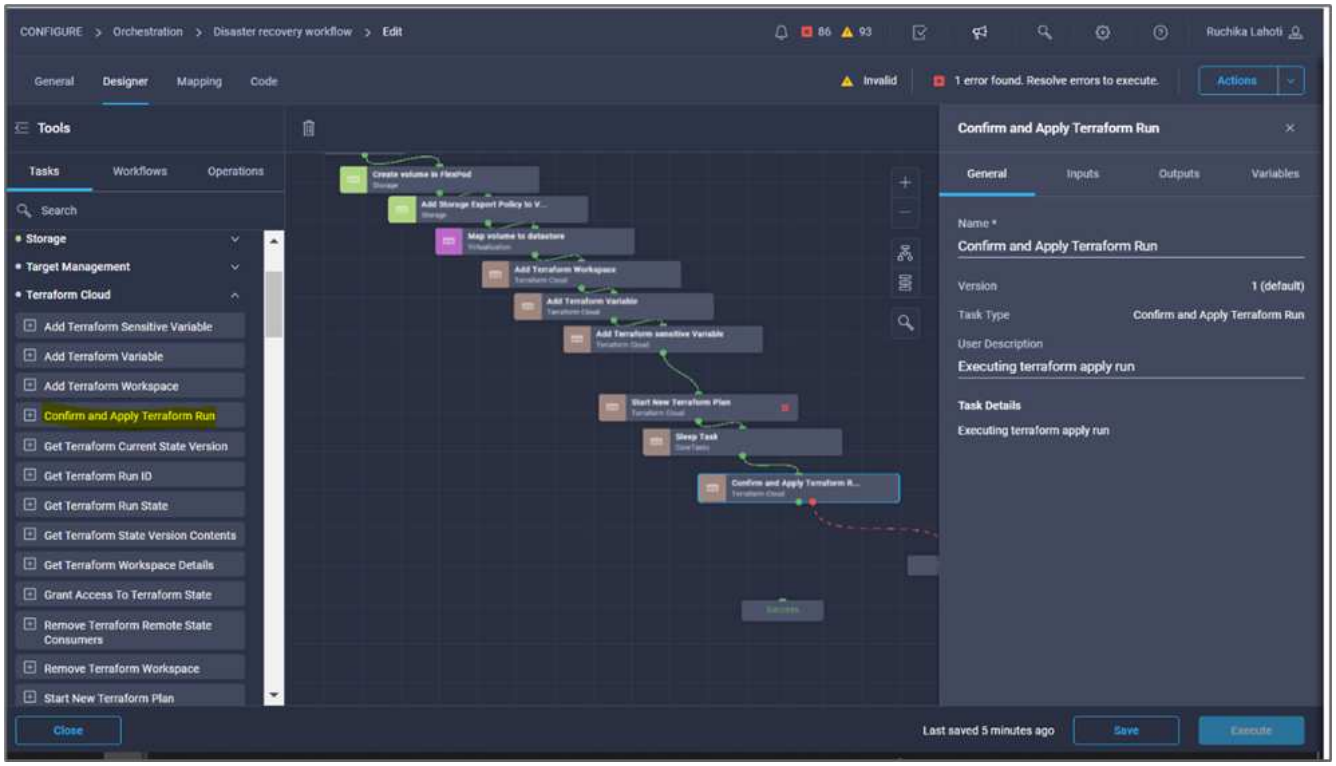


8. Clique em **mapa**.
9. Clique em **Salvar**.

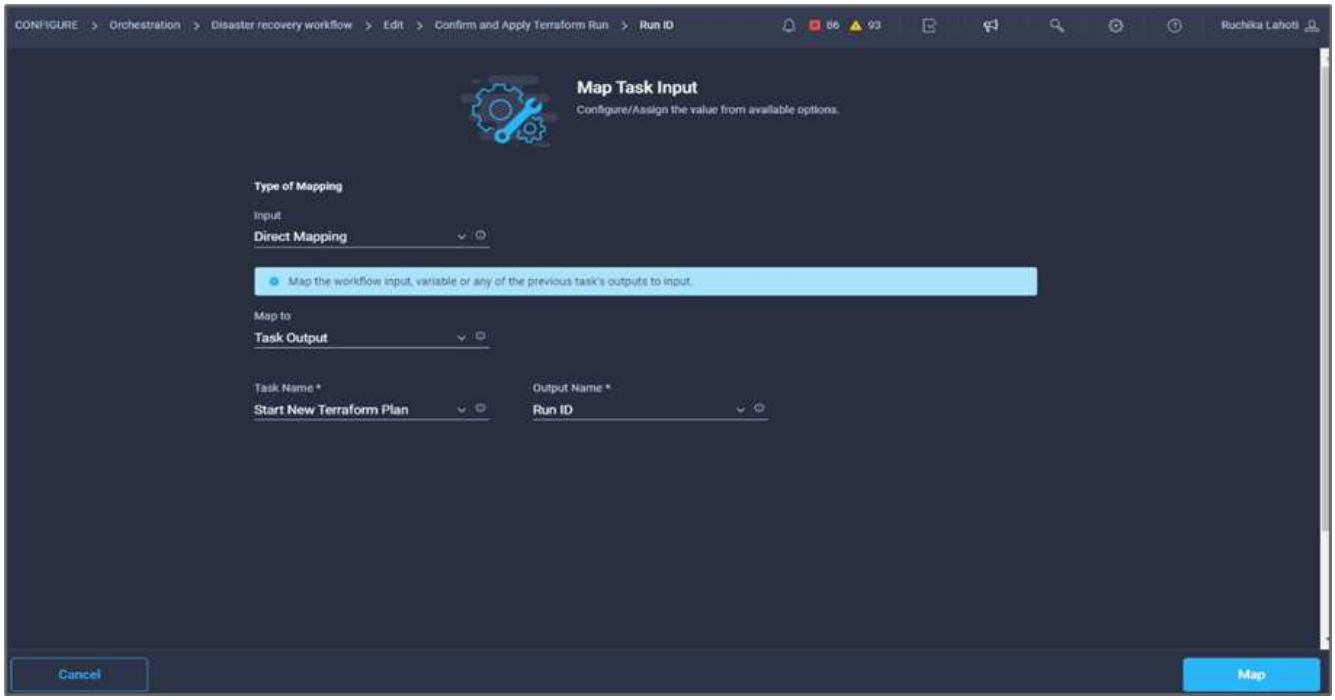
Isto conclui a tarefa de suspensão. Em seguida, crie a última tarefa desse fluxo de trabalho, confirmando e aplicando o Terraform Run.

Procedimento 10: Confirme e aplique o Terraform Run

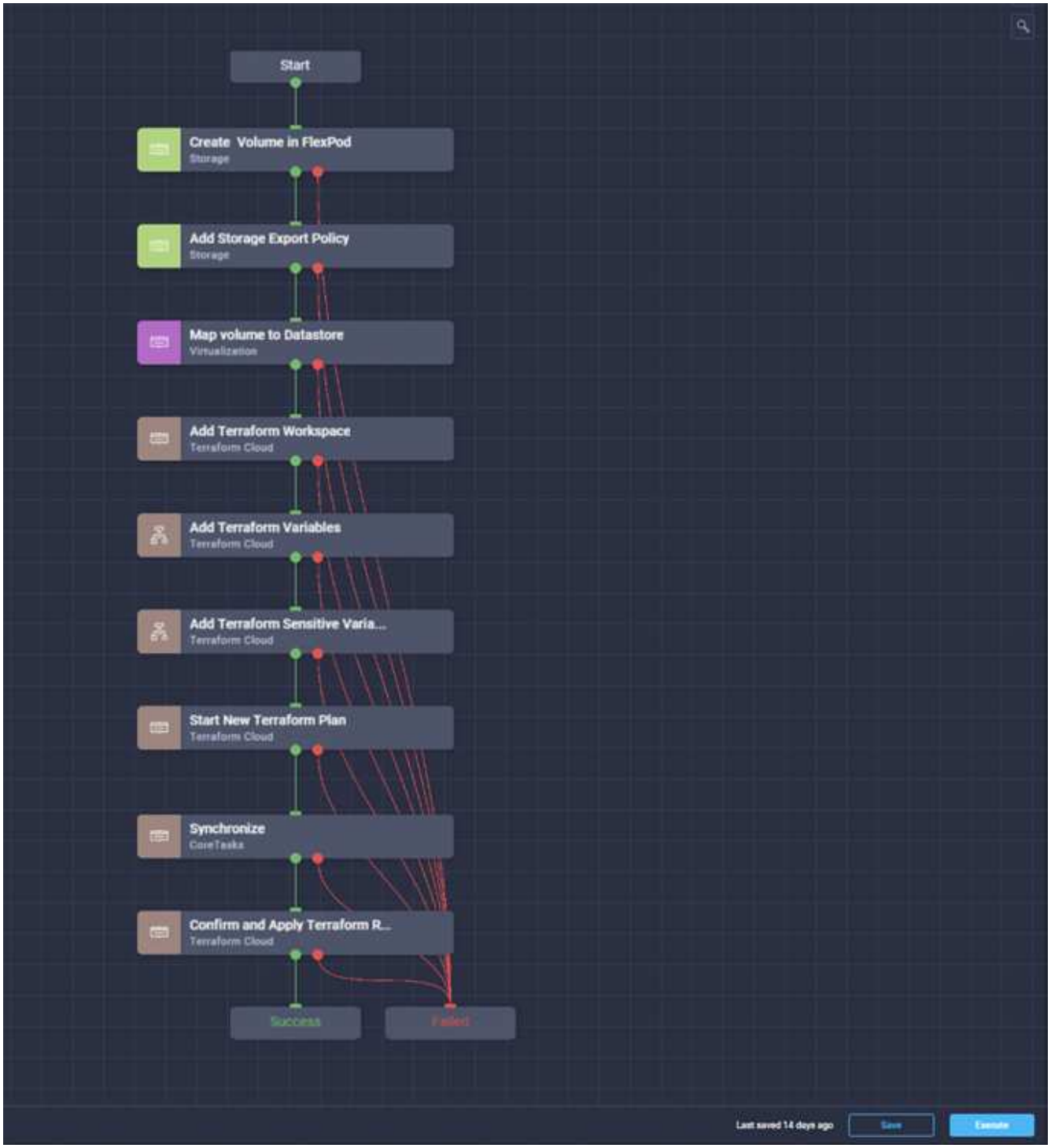
1. Vá para a guia **Designer** e clique em **tarefas** na seção **Ferramentas**.
2. Arraste e solte a tarefa **Terraform Cloud > confirmar e aplicar o Terraform Run** na seção **Tools** na área **Design**.
3. Use o conetor para conetar as tarefas **Sincronizar** e **confirmar e aplicar o Terraform Run**. Clique em **Salvar**.
4. Clique em **Confirm** e **Apply Terraform Run**. Na área **Propriedades da tarefa**, clique na guia **Geral**. Opcionalmente, você pode alterar o nome e a descrição dessa tarefa.



5. Na área **Task Properties**, clique em **Inputs**.
6. Clique em **Map** no campo **Terraform Cloud Target**.
7. Escolha **valor estático** e clique em **Select Terraform Cloud Target**. Selecione a conta do Terraform Cloud for Business que foi adicionada no "Configurar o Serviço de Intersight do Cisco para o HashiCorp Terraform"."
8. Clique em **mapa**.
9. Clique em **Map** no campo **Run ID**.
10. Escolha **Mapeamento direto** e clique em **saída de tarefa**.
11. Clique em **Nome da tarefa** e clique em **Iniciar novo plano Terraform**.
12. Clique em **Nome de saída** e, em seguida, clique em **ID de execução**.



13. Clique em **mapa**.
14. Clique em **Salvar**.
15. Clique em **Auto align Workflow** para que todas as tarefas estejam alinhadas. Clique em **Salvar**.



Isso conclui a tarefa confirmar e aplicar execução do Terraform. Use o conetor para conetar entre a tarefa **Confirme e aplique o Terraform Run** e as tarefas **success** e **Failed**.

Procedimento 11: Importar um fluxo de trabalho construído pelo Cisco

O Cisco Intersight Cloud Orchestrator permite exportar fluxos de trabalho de uma conta do Cisco Intersight para o sistema e importá-los para outra conta. Um arquivo JSON foi criado exportando o fluxo de trabalho criado que pode ser importado para sua conta.

Um arquivo JSON para o componente de fluxo de trabalho está disponível no "Repositório do GitHub".

"Próximo: Execução do Terraform a partir do controlador."

Execução do Terraform a partir do controlador

"Anterior: Fluxo de trabalho de DR."

Podemos executar o plano Terraform usando um controlador. Você pode ignorar esta seção se já tiver executado o plano Terraform usando um fluxo de trabalho do ICO.

Pré-requisitos

A configuração da solução começa com uma estação de trabalho de gerenciamento que tem acesso à Internet e com uma instalação funcional do Terraform.

Um guia para instalar o Terraform pode ser encontrado "aqui".

Clone o repositório do GitHub

O primeiro passo no processo é clonar o repositório do GitHub para uma nova pasta vazia na estação de trabalho de gerenciamento. Para clonar o repositório do GitHub, execute as seguintes etapas:

1. Na estação de trabalho de gerenciamento, crie uma nova pasta para o projeto. Crie uma nova pasta dentro dessa pasta chamada `/root/snapmirror-cvo` e clone o repositório do GitHub nela.
2. Abra uma interface de linha de comando ou console na estação de trabalho de gerenciamento e mude os diretórios para a nova pasta recém-criada.
3. Clonar a coleção GitHub usando o seguinte comando:

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Mude os diretórios para a nova pasta chamada `snapmirror-cvo`.

Execução do Terraform

- **Init.** Inicialize o ambiente (local) do Terraform. Normalmente executado apenas uma vez por sessão.
- **Plano.** Compare o estado do Terraform com o estado as-in na nuvem e crie e exiba um plano de execução. Isso não altera a implantação (somente leitura).
- **Aplicar.** Aplique o plano a partir da fase do plano. Isso potencialmente altera a implantação (leitura e gravação).
- **Destrua.** Todos os recursos que são governados por esse ambiente específico do Terraform.

  Para obter detalhes, "aqui" consulte .

"Próximo: Validação da solução."

Validação da solução

"Anterior: Execução do Terraform do controlador."

Nesta seção, revisitamos a solução com um fluxo de trabalho de exemplo de replicação de dados e fazemos algumas medições para verificar a integridade da replicação de dados da instância do NetApp ONTAP em execução no FlexPod para o NetApp Cloud Volumes ONTAP em execução no Google Cloud.

Usamos o orquestrador de fluxo de trabalho do Cisco Intersight nesta solução e continuaremos a usá-lo para nosso caso de uso.

Notavelmente, o conjunto limitado de fluxos de trabalho do Cisco Intersight usado nesta solução não representa o conjunto completo de fluxos de trabalho com os quais o Cisco Intersight está equipado. Você pode criar fluxos de trabalho personalizados com base em seus requisitos específicos e acioná-los a partir do Cisco Intersight.

Para executar a validação de um cenário de DR bem-sucedido, primeiro mova dados de um volume no ONTAP que faz parte do FlexPod para o Cloud Volumes ONTAP usando o SnapMirror. Depois, você pode tentar acessar os dados da instância de computação em nuvem do Google, seguido de uma verificação de integridade de dados.

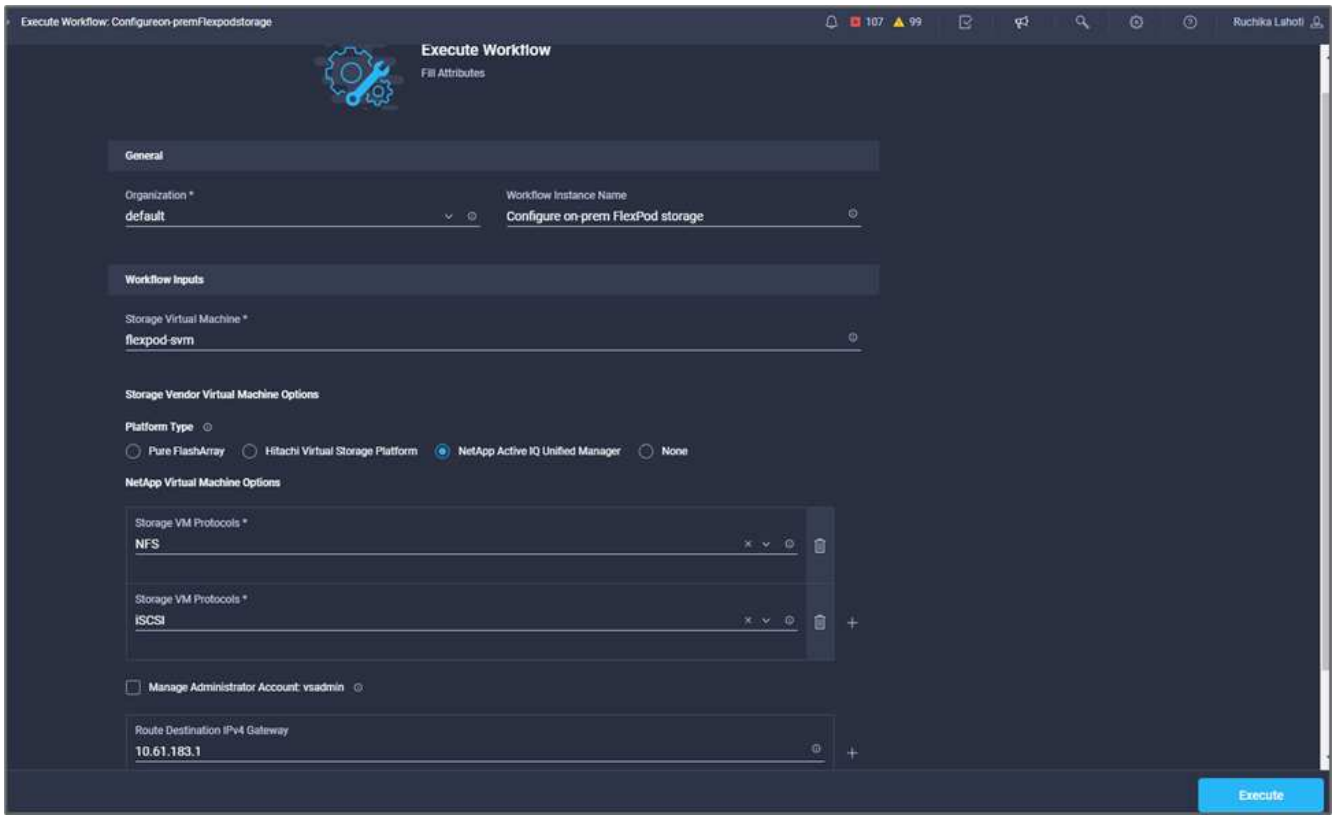
As etapas de alto nível a seguir são usadas para verificar os critérios de sucesso desta solução:

1. Gere um checksum SHA256 no conjunto de dados de amostra que está presente em um volume ONTAP no FlexPod.
2. Configure uma relação de volume SnapMirror entre o ONTAP no FlexPod e o Cloud Volumes ONTAP.
3. Replique o conjunto de dados de amostra do FlexPod para o Cloud Volumes ONTAP.
4. Quebre a relação SnapMirror e promova o volume em Cloud Volumes ONTAP para a produção.
5. Mapear o volume Cloud Volumes ONTAP com o conjunto de dados para uma instância de computação no Google Cloud.
6. Gere um checksum SHA256 no conjunto de dados de amostra no Cloud Volumes ONTAP.
7. Compare a soma de verificação na origem e no destino; presumivelmente, as somas de verificação em ambos os lados coincidem.

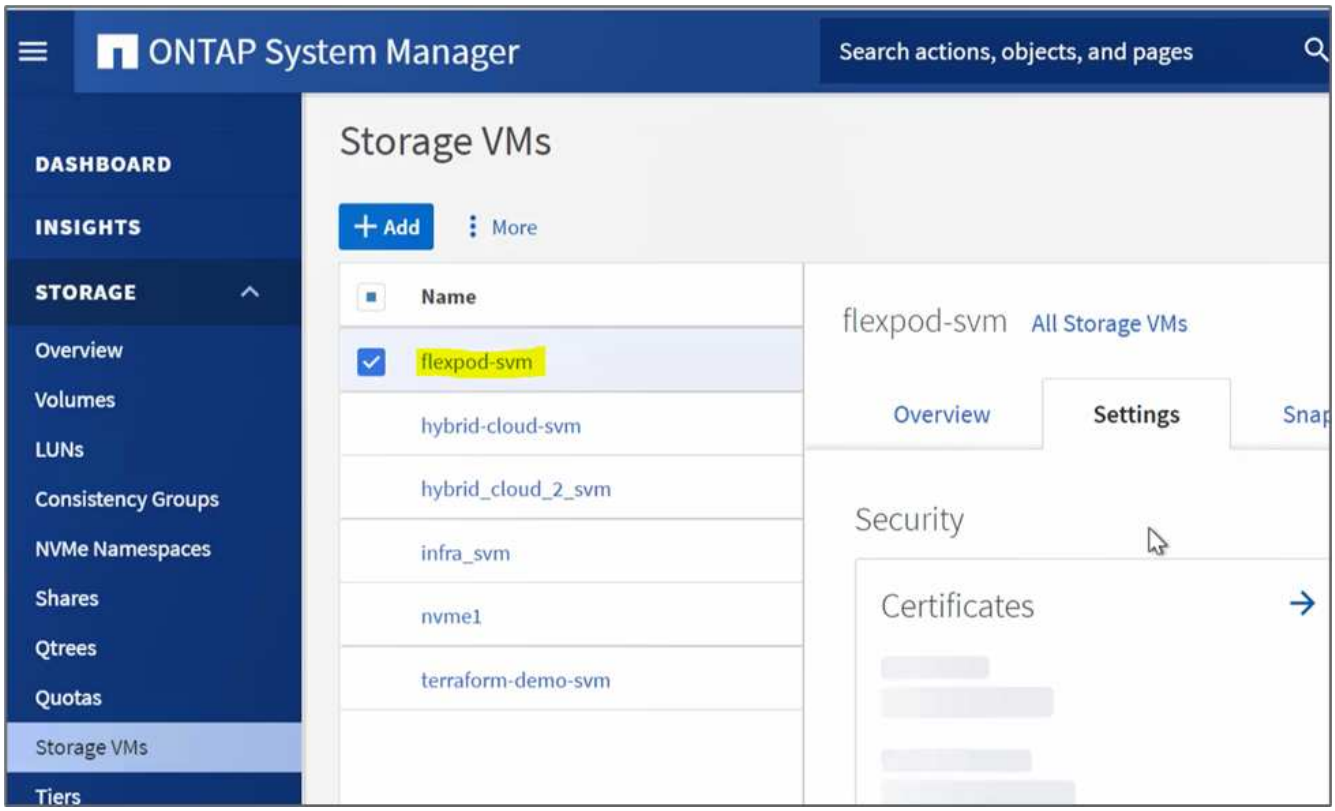
Para executar o fluxo de trabalho no local, execute as seguintes etapas:

1. Crie um fluxo de trabalho no Intersight para FlexPod on-premises.

2. Forneça as entradas necessárias e execute o fluxo de trabalho.

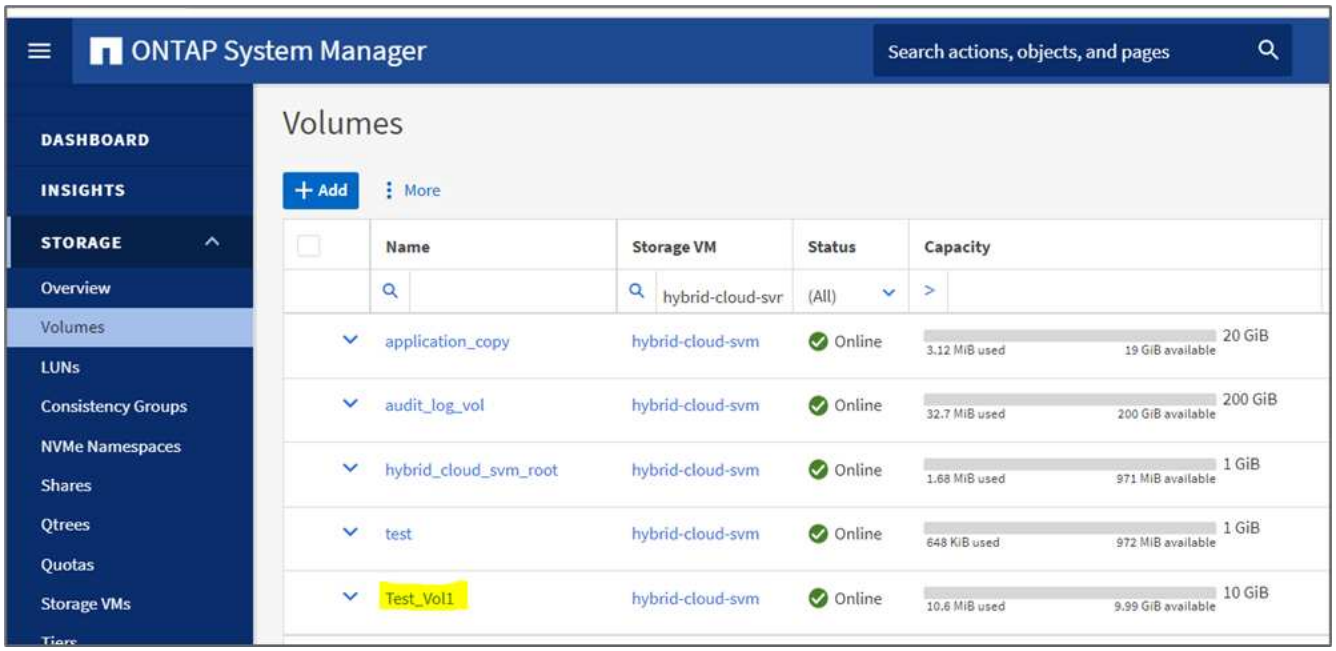


3. Verifique o SVM recém-criado no gerente do sistema.



4. Crie e execute outro fluxo de trabalho de recuperação de desastres para criar um volume no FlexPod local e estabelecer uma relação de SnapMirror entre esse volume no FlexPod e no Cloud Volumes ONTAP.

5. Verifique o volume recém-criado no gerenciador de sistema do ONTAP.

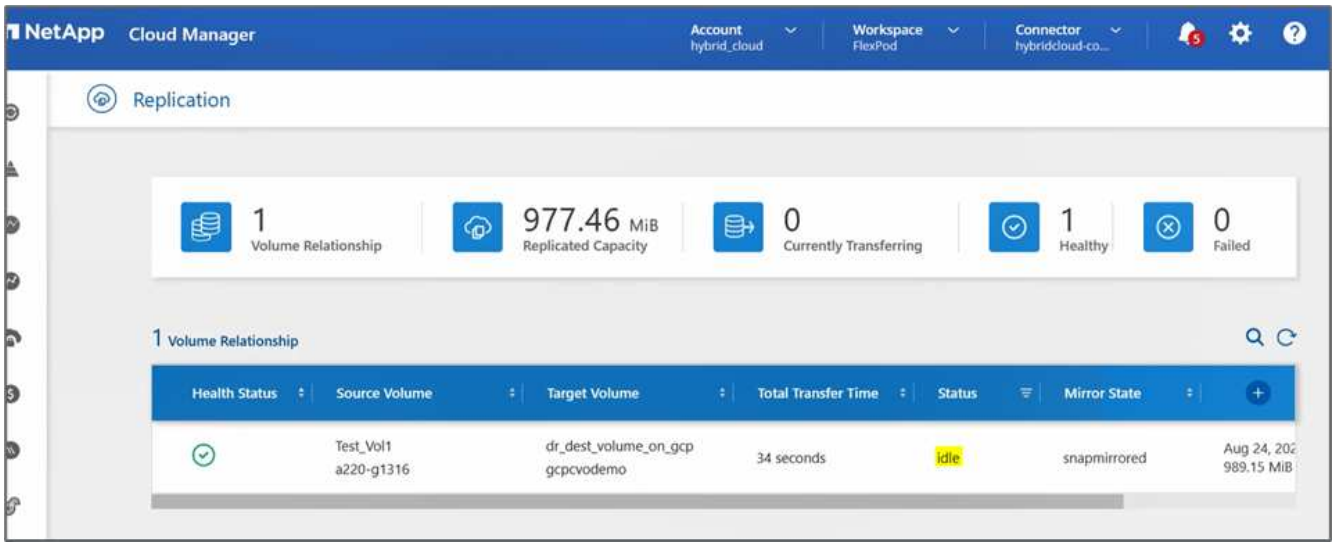


6. Monte o mesmo volume NFS em uma máquina virtual no local, copie o conjunto de dados de amostra e execute o checksum.

```
root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem                Size  Used Avail Use% Mounted on
udev                      1.9G     0  1.9G   0% /dev
tmpfs                     394M  1.1M  393M   1% /run
/dev/sda2                  16G   11G  4.2G  72% /
tmpfs                     2.0G     0  2.0G   0% /dev/shm
tmpfs                     5.0M     0  5.0M   0% /run/lock
tmpfs                     2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1                 55M   55M     0 100% /snap/core18/1705
/dev/loop2                 69M   69M     0 100% /snap/lxd/14804
/dev/loop0                 28M   28M     0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1    10G  512K   10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#
```

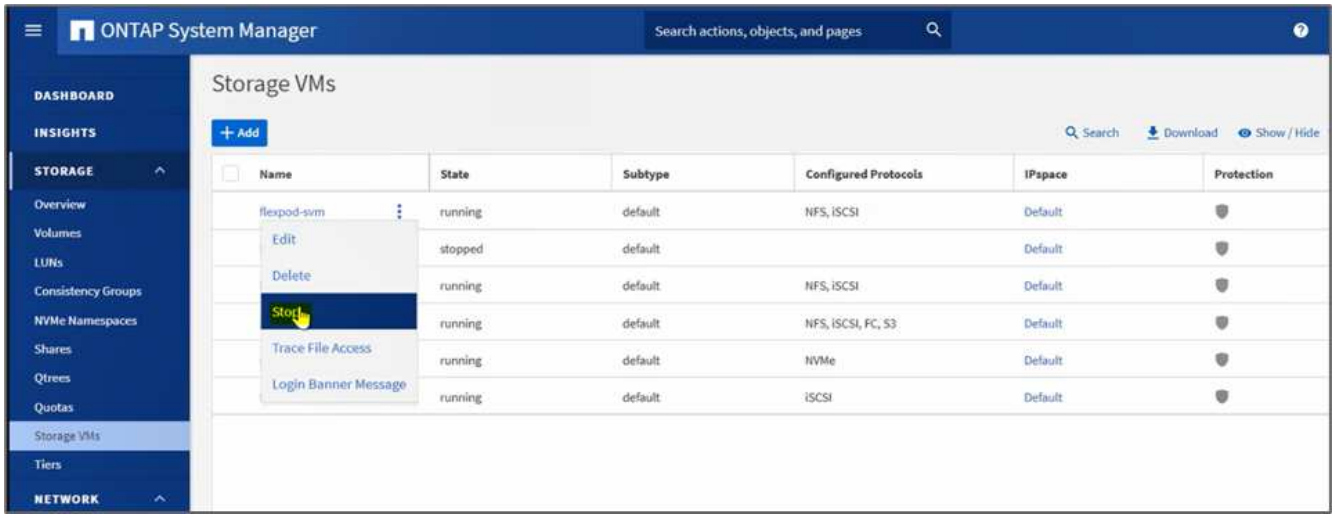
```
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#
```

7. Verifique o status da replicação no Cloud Manager. A transferência de dados pode levar alguns minutos com base no tamanho dos dados. Depois de concluído, você pode ver o status do SnapMirror como **Idle**.

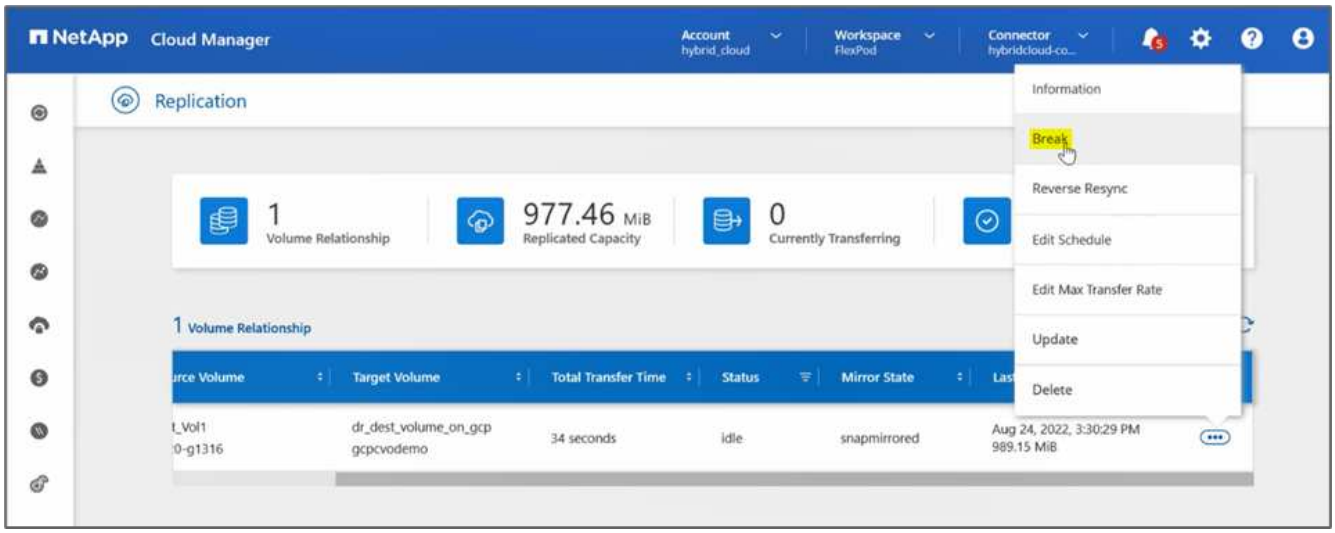


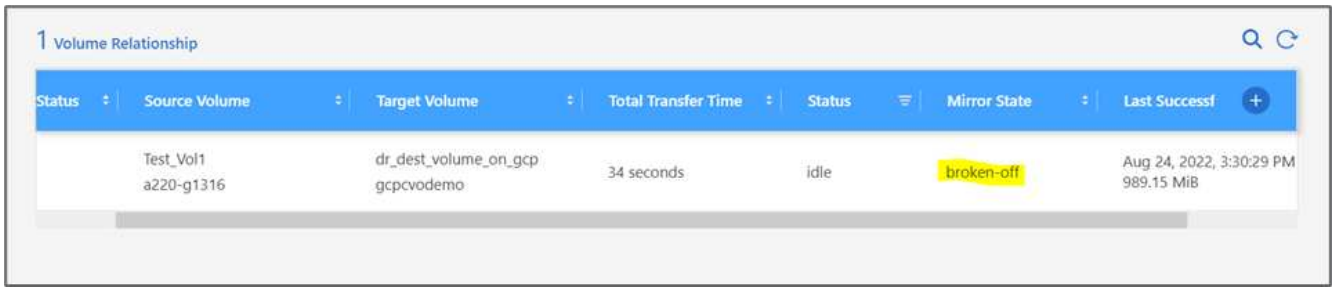
8. Quando a transferência de dados estiver concluída, simule um desastre no lado da fonte parando o SVM que hospeda o `Test_vol1` volume.

   Depois que o SVM tiver sido interrompido, o `Test_vol1` volume não ficará visível no Cloud Manager.

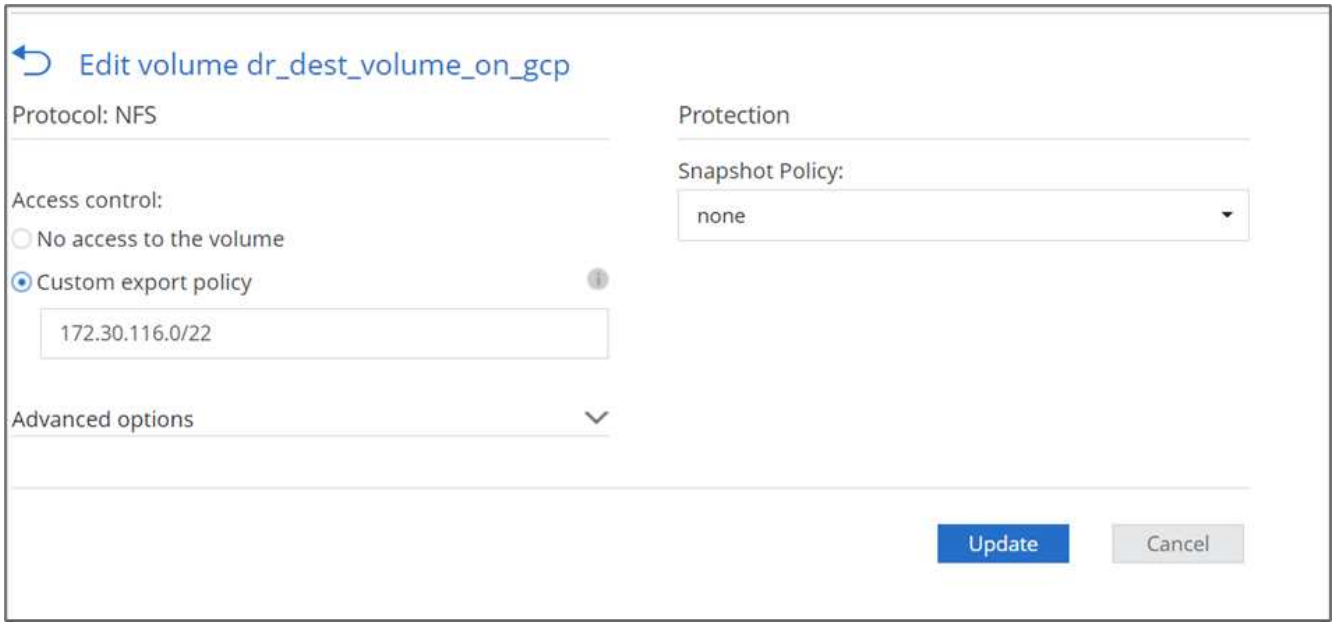


9. Quebre a relação de replicação e promova o volume de destino do Cloud Volumes ONTAP para a produção.

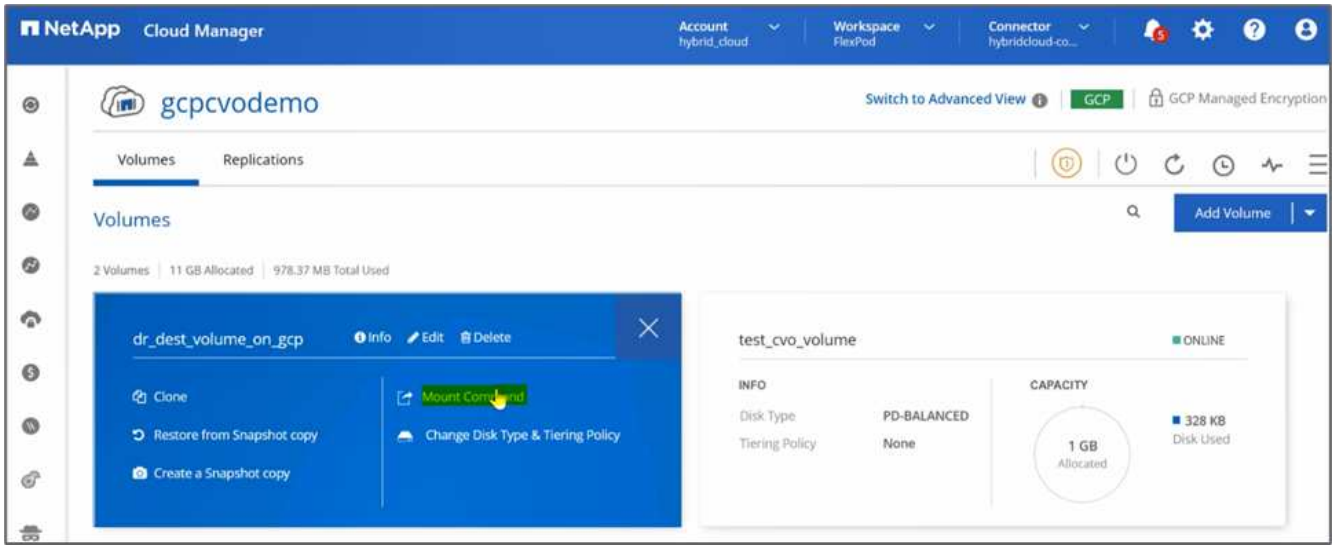




10. Edite o volume e ative o acesso do cliente associando-o a uma política de exportação.



11. Obtenha o comando READY-to-use mount para o volume.



12. Monte o volume em uma instância de computação, verifique se os dados estão presentes no volume de destino e gere a soma de verificação SHA256 do `sample_dataset_2GB` arquivo.

```
drwxr-xr-x 21 root   root            4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59  test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Compare os valores da soma de verificação tanto na origem (FlexPod) como no destino (Cloud Volumes ONTAP).
14. As somas de verificação correspondem à origem e ao destino.

Você pode confirmar se a replicação de dados da origem para o destino foi concluída com sucesso e a integridade dos dados foi mantida. Esses dados agora podem ser consumidos com segurança pelos aplicativos para atender clientes enquanto o site de origem passa por restauração.

"Próximo: Conclusão."

Conclusão

"Anterior: Validação da solução."

Nessa solução, o serviço de dados de nuvem NetApp, o Cloud Volumes ONTAP e a infraestrutura de data center FlexPod foram usados para criar uma solução de recuperação de desastres com uma nuvem pública habilitada pelo orquestrador de nuvem Cisco Intersight. A solução FlexPod evoluiu constantemente para permitir que os clientes modernizem seus processos de entrega de aplicações e negócios. Com essa solução, você pode criar um plano BCDR com a nuvem pública como local de destino para um plano de DR transitório ou em tempo integral, mantendo o custo da solução de DR baixo.

A replicação de dados entre o FlexPod no local e o NetApp Cloud Volumes ONTAP foi feita com tecnologia comprovada da SnapMirror, mas você também pode selecionar outras ferramentas de transferência e sincronização de dados do NetApp, como o Cloud Sync, para seus requisitos de mobilidade de dados. Segurança dos dados em trânsito fornecida pelas tecnologias de criptografia incorporadas baseadas em TLS/AES.

Não importa se você tem um plano de recuperação de desastres temporário para um aplicativo ou um plano de recuperação de desastres em tempo integral para uma empresa, o portfólio de produtos usados nessa solução pode atender a ambos os requisitos em escala. Equipado com o Cisco Intersight Workflow Orchestrator, o mesmo pode ser automatizado com fluxos de trabalho pré-criados que não apenas eliminam a necessidade de reconstruir processos, mas também aceleram a implementação de um plano BCDR.

A solução possibilita o gerenciamento do FlexPod no local e a replicação de dados em uma nuvem híbrida de maneira muito fácil e conveniente, com automação e orquestração oferecidas pelo Cisco Intersight Cloud Orchestrator.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

GitHub

- Todas as configurações do Terraform usadas

  "https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"

- Arquivos JSON para importação de fluxos de trabalho

  "https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"

Cisco Intersight

- Centro de Ajuda do Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentação do Cisco Intersight Cloud Orchestrator:

  "https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"

- Serviço de Intersight da Cisco para Documentação Terraform da HashiCorp

  "https://intersight.com/help/saas/features/terraform_cloud/admin"

- Folha de dados de Intersight da Cisco

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"

- Folha de dados do Cisco Intersight Cloud Orchestrator

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"

- Cisco Intersight Service para HashiCorp Terraform Folha de dados

  "https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"

FlexPod

- Página inicial do FlexPod

  "https://www.flexpod.com"

- Cisco validou guias de design e implantação para FlexPod

  "FlexPod Datacenter com Cisco UCS 4,2(1) no modo gerenciado UCS, VMware vSphere 7,0 U2 e NetApp ONTAP 9.9 Guia de Design"

- Data center FlexPod com Cisco UCS X-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"

Interoperabilidade

- Ferramenta de Matriz de interoperabilidade do NetApp

  "http://support.netapp.com/matrix/"

- Ferramenta de interoperabilidade de hardware e software Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Guia de compatibilidade da VMware

  "http://www.vmware.com/resources/compatibility/search.php"

Documentos de referência do NetApp Cloud Volumes ONTAP

- Gerenciador de nuvem do NetApp

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- Cloud Volumes ONTAP

  https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html

- Calculadora de TCO da Cloud Volumes ONTAP

  https://cloud.netapp.com/google-cloud-calculator

- Cloud Volumes ONTAP Sizer

  "https://cloud.netapp.com/cvo-sizer"

- Ferramenta de avaliação de nuvem

  https://cloud.netapp.com/assessments

- Nuvem híbrida da NetApp

  https://cloud.netapp.com/hybrid-cloud

- Documentação da API do Cloud Manager

  "https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"

Solução de problemas

"https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO)"

Terraform

- Terraform Cloud

  "https://www.terraform.io/cloud"

- Documentação do Terraform

  "https://www.terraform.io/docs/"

- Registro do NetApp Cloud Manager

  "https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/lates"

GCP

- Alta disponibilidade do ONTAP para GCP

  "https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"

- GCP perquisite

  https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6

Nuvem híbrida da FlexPod com NetApp Astra e Cisco Intersight para Red Hat OpenShift

TR-4936: Nuvem híbrida da FlexPod com NetApp Astra e Cisco Intersight para Red Hat OpenShift

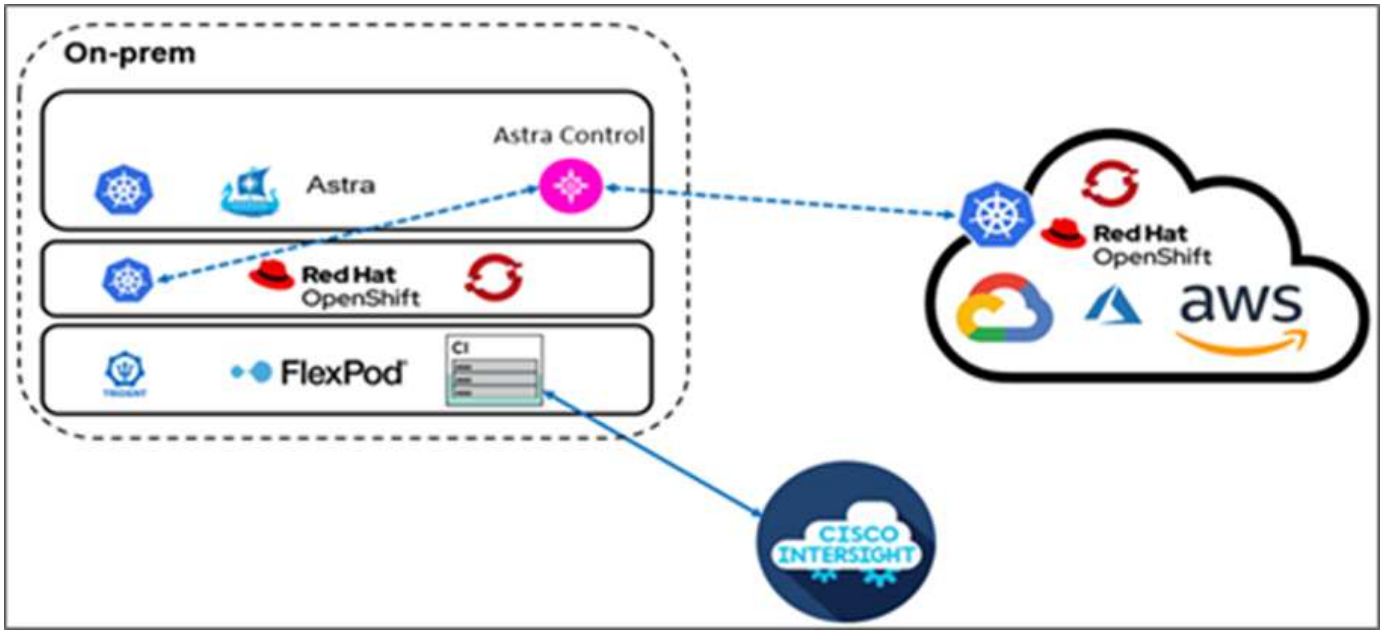
Abhinav Singh

Introdução

À medida que contêineres e Kubernetes se tornam a escolha de fato para desenvolver, implantar, executar, gerenciar e dimensionar aplicações em contêineres, as empresas estão executando cada vez mais aplicações essenciais aos negócios neles. As aplicações essenciais aos negócios dependem fortemente do estado. Um aplicativo com estado tem informações associadas de estado, dados e configuração e depende de transações de dados anteriores para executar sua lógica de negócios. As aplicações essenciais aos negócios enquanto executadas no Kubernetes continuam a ter requisitos de disponibilidade e continuidade dos negócios, como as aplicações tradicionais. Uma interrupção de serviço pode afetar seriamente a perda de receita, produtividade e reputação da empresa. Portanto, é muito essencial proteger, recuperar e mover workloads do Kubernetes com rapidez e facilidade dentro e entre clusters, data centers no local e ambientes de nuvem híbrida. As empresas viram os benefícios de migrar seus negócios para um modelo de nuvem híbrida e modernizar suas aplicações para um fator forma nativo da nuvem é o mais alto na lista.

Esse relatório técnico reúne o NetApp com o Red Hat OpenShift Container Platform em uma solução de infraestrutura convergente da FlexPod e se estende até a Amazon Web Services (AWS) para formar um data center de nuvem híbrida. Com base na familiaridade "FlexPod e Red Hat OpenShift" com o , este documento discute o NetApp Astra Control Center, a partir da instalação, configuração, workflows de proteção de aplicações e migração de aplicações entre o local e a nuvem. Ele também discute as vantagens dos recursos de gerenciamento de dados com reconhecimento de aplicações (como backup e recuperação, continuidade dos negócios) ao usar o NetApp Astra Control Center para aplicações em contêiner executadas no Red Hat OpenShift.

A figura a seguir ilustra a visão geral da solução.



Público-alvo

O público-alvo deste documento inclui diretores de tecnologia (CTOs), desenvolvedores de aplicações, arquitetos de soluções em nuvem, engenheiros de confiabilidade do site (SREs), engenheiros de DevOps, ITOps e equipes de serviços profissionais com foco em projetar, hospedar e gerenciar aplicações em contêiner.

NetApp Astra Control – principais casos de uso

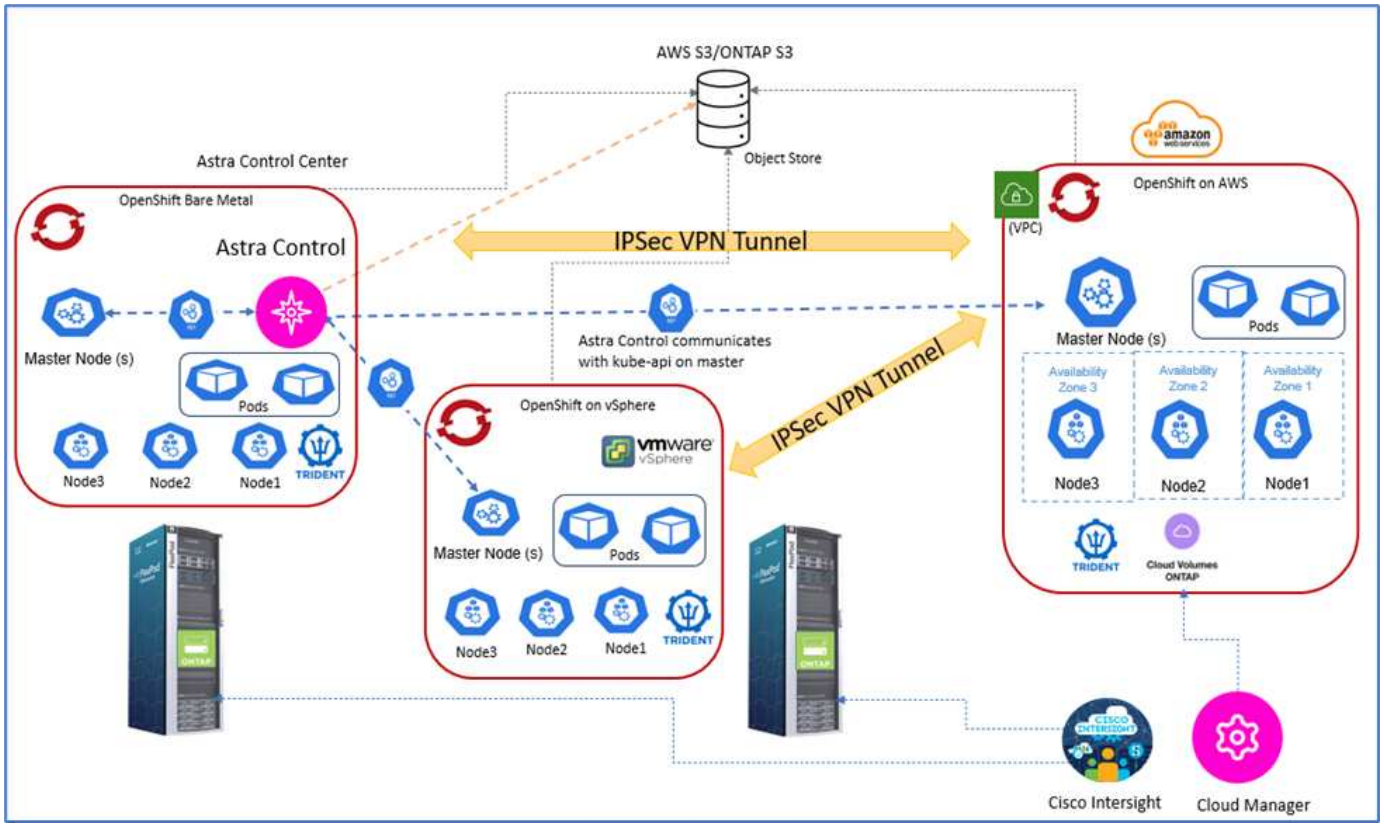
O NetApp Astra Control simplifica a proteção de aplicações para clientes que lidam com microsserviços nativos da nuvem:

- * Representação de aplicativos ponto-em-tempo (pit) com snapshots.* Com o Astra Control, você pode tirar snapshots completos das aplicações em contêiner, incluindo detalhes de configuração da aplicação em execução no Kubernetes e o storage persistente associado. No caso de um incidente, os aplicativos podem ser restaurados para um estado em boas condições no clique de botão.
- * Cópia de segurança completa do aplicativo.* Com o Astra Control, você pode fazer um backup completo de aplicação em um agendamento predefinido, que pode ser usado para restaurar a aplicação no mesmo cluster K8s ou para um cluster K8s sob demanda de maneira automatizada.
- * Portabilidade e migração de aplicativos com clones.* Com o Astra Control, você pode clonar uma aplicação inteira e seus dados de um cluster Kubernetes para outro ou dentro do mesmo cluster K8s. Esse recurso também ajuda na portabilidade ou migração de um aplicativo em K8s clusters, não importa onde os clusters estejam localizados (basta excluir a instância do aplicativo de origem após a clonagem).
- * Personalize a consistência da aplicação.* Com o Astra Control, você pode controlar a definição de estados de quiesce de aplicações utilizando os ganchos de execução. Solte os ganchos de execução "pré" e "pós" nos fluxos de trabalho de snapshot e backup, seus aplicativos serão desativados do seu jeito antes que um snapshot ou backup seja feito.
- **Automatize a recuperação de desastres (DR) no nível da aplicação.** Com o Astra Control, você pode configurar um plano de recuperação de desastre de continuidade dos negócios (BCDR) para suas aplicações em contêiner. O NetApp SnapMirror é usado no back-end e a implementação completa do fluxo de trabalho de DR é automatizada.

Topologia da solução

Esta seção descreve a topologia lógica da solução.

A ilustração a seguir representa a topologia da solução que inclui o ambiente local do FlexPod executando clusters do OpenShift Container Platform e um cluster autogerenciado do OpenShift Container Platform na AWS com a plataforma NetApp Cloud Volumes ONTAP, Cisco Intersight e NetApp Cloud Manager SaaS.



O primeiro cluster do OpenShift Container Platform é uma instalação bare-metal no FlexPod, o segundo cluster do OpenShift Container Platform é implantado no VMware vSphere em execução no FlexPod e o terceiro cluster do OpenShift Container Platform é implantado como um "cluster privado" em uma nuvem privada virtual (VPC) existente na AWS como uma infraestrutura autogerenciada.

Nessa solução, o FlexPod é conetado à AWS por meio de uma VPN site a site. No entanto, os clientes também podem usar as implementações de conexão direta para estender a uma nuvem híbrida. O Cisco Intersight é usado para gerenciar os componentes da infraestrutura do FlexPod.

Nessa solução, o Astra Control Center gerencia a aplicação em contêiner hospedada no cluster do OpenShift Container Platform executado no FlexPod e na AWS. O Centro de Controle Astra é instalado na instância bare-metal OpenShift executada no FlexPod. O Astra Control se comunica com a kube-api no nó principal e observa continuamente o cluster do Kubernetes em busca de alterações. Quaisquer novos aplicativos adicionados ao cluster K8s são automaticamente descobertos e disponibilizados para gerenciamento.

As representações de pit de aplicações em contêiner podem ser capturadas como snapshots usando o Astra Control Center. Os snapshots de aplicativos podem ser acionados por meio de uma política de proteção agendada ou sob demanda. Para aplicações compatíveis com Astra, o Snapshot é consistente com falhas. Um snapshot da aplicação constitui um snapshot dos dados da aplicação nos volumes persistentes, bem como os metadados da aplicação dos vários recursos do Kubernetes associados a essa aplicação.

É possível criar um backup completo de uma aplicação com o Astra Control usando uma programação de backup predefinida ou sob demanda. Um armazenamento de objetos é usado para armazenar o backup dos dados do aplicativo. NetApp ONTAP S3, NetApp StorageGRID e qualquer implementação genérica S3 podem ser usados como um armazenamento de objetos.

"Próximo: Componentes da solução."

Componentes da solução

"Anterior: Visão geral da solução."

FlexPod

O FlexPod é um conjunto definido de hardware e software que forma uma base integrada para soluções virtualizadas e não virtualizadas. O FlexPod inclui storage NetApp ONTAP, rede Cisco Nexus, rede de storage Cisco MDS, sistema de computação unificada da Cisco (Cisco UCS). O design é flexível o suficiente para que a rede, a computação e o storage possam se encaixar em um rack de data center ou possa ser implantado de acordo com o design do data center do cliente. A densidade da porta permite que os componentes de rede acomodem várias configurações.

Astra Control

O Astra Control oferece serviços de proteção de dados com reconhecimento de aplicações para aplicações nativas em nuvem hospedadas em nuvens públicas e no local. O Astra Control oferece recursos de proteção de dados, recuperação de desastres e migração para sua aplicação em contêiner executada no Kubernetes.

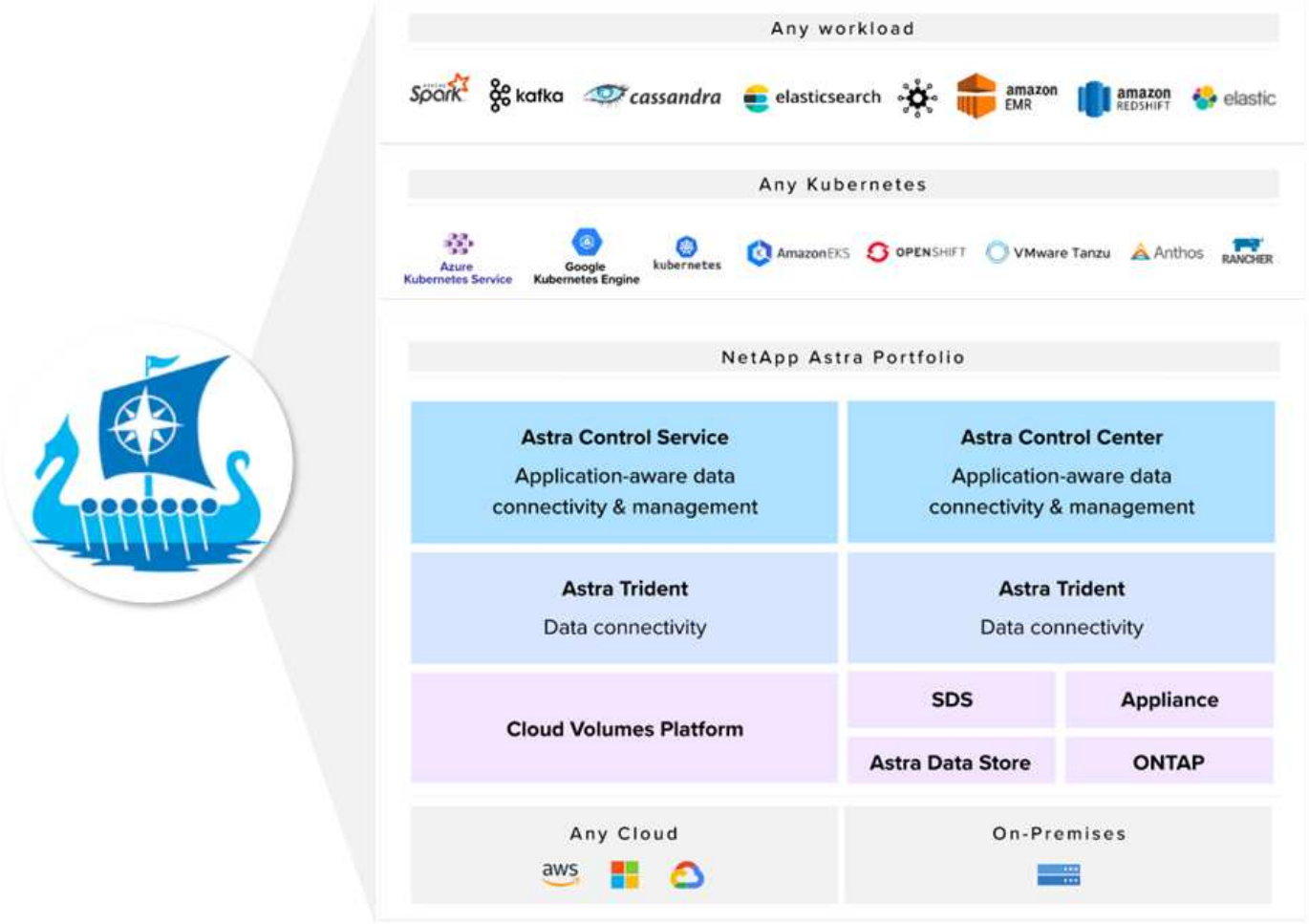
Caraterísticas

O Astra Control oferece funcionalidades essenciais para o gerenciamento do ciclo de vida dos dados da aplicação Kubernetes:

- Gerencie automaticamente o storage persistente
- Crie backups e snapshots sob demanda consistentes com aplicações
- Operações automatizadas de backup e snapshot voltadas a políticas
- Migre as aplicações e os dados associados de um cluster de Kubernetes para outro em uma configuração de nuvem híbrida
- Clonar uma aplicação para o mesmo cluster K8s ou para outro cluster K8s
- Visualizar o status de proteção da aplicação
- Fornece uma interface gráfica de usuário e uma lista exaustiva de APIs REST para implementar todos os fluxos de trabalho de proteção contra ferramentas internas existentes.

O Astra Control oferece uma visualização de painel único para suas aplicações em contêiner. Ele inclui um insight sobre os recursos associados criados no cluster do Kubernetes. Você pode visualizar todos os clusters, todas as aplicações, em todas as nuvens ou em todos os data centers usando um único portal. Use as APIs do Astra Control em todos os ambientes (no local ou nuvens públicas) para implementar seus workflows de gerenciamento de dados.

A imagem a seguir mostra os recursos do Astra Control.



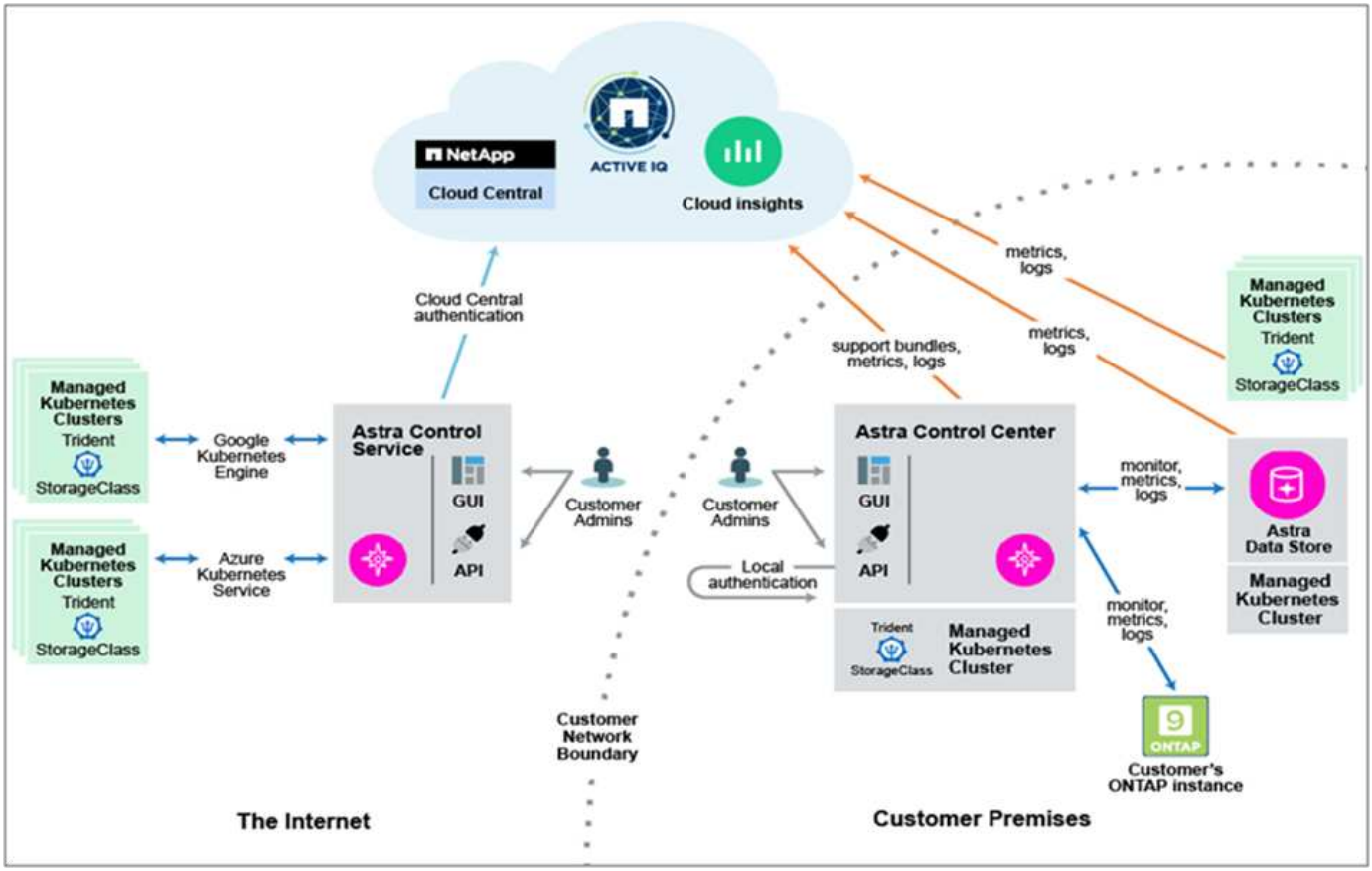
Modelos de consumo Astra Control

O Astra Control está disponível em dois modelos de consumo:

- **Serviço Astra Control.** Um serviço totalmente gerenciado hospedado pela NetApp que fornece gerenciamento de dados com reconhecimento de aplicações dos clusters do Kubernetes no Google Kubernetes Engine (GKE) e no Azure Kubernetes Service (AKS).
- **Centro de Controle Astra.** Software autogerenciado que fornece gerenciamento de dados com reconhecimento de aplicações dos clusters do Kubernetes executados no ambiente de nuvem híbrida e no local.

Esse relatório técnico utiliza o Astra Control Center para gerenciamento de aplicações nativas em nuvem executadas no Kubernetes.

A imagem a seguir mostra a arquitetura Astra Control.



Astra Trident

O Astra Trident é um orquestrador de storage de código aberto e totalmente compatível para distribuições de contêineres e Kubernetes. Ele foi criado desde o início para ajudar você a atender às demandas de persistência das aplicações em contêineres usando interfaces padrão do setor, como o "Interface de armazenamento de contentor (CSI)". Com o Astra Trident, os microsserviços e as aplicações em contêiner podem aproveitar os serviços de storage de classe empresarial fornecidos pelo portfólio de sistemas de storage da NetApp.

O Astra Trident é implantado em clusters de Kubernetes como pods e fornece serviços de orquestração de storage dinâmico para seus workloads do Kubernetes. Ele permite que suas aplicações em contêiner consumam storage persistente de forma rápida e fácil no amplo portfólio do NetApp, que inclui o NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, nuvem e Amazon FSX for NetApp ONTAP), o software NetApp Element (NetApp SolidFire) e o serviço Azure NetApp Files, o serviço de volume de nuvem no Google Cloud e o serviço de volume de nuvem na AWS. Em um ambiente FlexPod, o Astra Trident é usado para provisionar e gerenciar dinamicamente volumes persistentes para contêineres com respaldo de volumes NetApp FlexVol e LUNs hospedados em uma plataforma de storage ONTAP, como sistemas NetApp AFF e FAS e Cloud Volumes ONTAP. O Trident também desempenha um papel fundamental na implementação de esquemas de proteção de aplicações fornecidos pelo Astra Control. Para obter mais informações sobre o Astra Trident, consulte "Documentação do Astra Trident."

Back-end de storage

Para usar o Astra Trident, você precisa de back-end de storage compatível. Um back-end do Trident define a relação entre o Trident e um sistema de storage. Ele informa à Trident como se comunicar com esse sistema de storage e como o Trident deve provisionar volumes a partir dele. O Trident oferecerá automaticamente pools de storage de back-ends que, em conjunto, atendem aos requisitos definidos por uma classe de storage.

- Back-end de storage ONTAP AFF e FAS. Como uma plataforma de software de storage e hardware, o ONTAP fornece serviços básicos de storage, suporte para vários protocolos de acesso ao storage e recursos de gerenciamento de storage, como cópias e espelhamento do NetApp Snapshot.
- Back-end de storage do Cloud Volumes ONTAP
- "Armazenamento de dados Astra" back-end de storage

NetApp Cloud Volumes ONTAP

O NetApp Cloud Volumes ONTAP é uma oferta de storage definido por software que oferece gerenciamento avançado de dados para workloads de bloco e arquivo. Com o Cloud Volumes ONTAP, você pode otimizar seus custos de storage de nuvem e aumentar a performance das aplicações, além de aprimorar a proteção, a segurança e a conformidade dos dados.

Os principais benefícios incluem:

- Utilize deduplicação de dados incorporada, compressão, thin Provisioning e clonagem para minimizar os custos de storage.
- Garanta a confiabilidade empresarial e as operações contínuas em caso de falhas em seu ambiente de nuvem.
- O Cloud Volumes ONTAP utiliza o SnapMirror, a tecnologia de replicação líder do setor da NetApp, para replicar dados locais para a nuvem de modo que seja fácil ter cópias secundárias disponíveis para vários casos de uso.
- O Cloud Volumes ONTAP também se integra ao Cloud Backup Service para fornecer recursos de backup e restauração para proteção e arquivamento a longo prazo de seus dados de nuvem.
- Alterne entre pools de armazenamento de alto e baixo desempenho sob demanda sem colocar os aplicativos offline.
- Garanta a consistência das cópias Snapshot usando o NetApp SnapCenter.
- O Cloud Volumes ONTAP é compatível com a criptografia de dados e oferece proteção contra vírus e ransomware.
- A integração com o Cloud Data Sense ajuda você a entender o contexto dos dados e identificar dados confidenciais.

Cloud Central

O Cloud Central fornece um local centralizado para acessar e gerenciar os serviços de dados de nuvem da NetApp. Com esses serviços, você executa aplicações críticas na nuvem, cria locais de recuperação de desastres automatizados, faz backup dos dados e migra e controla dados com eficiência em várias nuvens. Para obter mais informações, consulte "Cloud Central."

Cloud Manager

O Cloud Manager é uma plataforma de gerenciamento baseada em SaaS de classe empresarial que permite que especialistas DE TI e arquitetos de nuvem gerenciem centralmente sua infraestrutura multicloud híbrida usando as soluções de nuvem da NetApp. Ele fornece um sistema centralizado para visualização e gerenciamento do storage de nuvem e no local, com suporte a contas e fornecedores de nuvem híbrida. Para obter mais informações, "Cloud Manager"consulte .

Conetor

O Connector é uma instância que permite que o Cloud Manager gerencie recursos e processos em ambiente

de nuvem pública. Um conetor é necessário para usar muitos recursos que o Cloud Manager oferece. Um conetor pode ser implantado na nuvem ou na rede local.

O conetor é suportado nos seguintes locais:

- AWS
- Microsoft Azure
- Google Cloud
- No local

Para saber mais sobre o conetor, consulte "este link."

NetApp Cloud Insights

O Cloud Insights, uma ferramenta de monitoramento de infraestrutura de nuvem da NetApp, permite que você monitore a performance e a utilização dos clusters do Kubernetes gerenciados pelo Astra Control Center. O Cloud Insights correlaciona o uso do storage com as cargas de trabalho. Quando você ativa a conexão Cloud Insights no Centro de Controle Astra, as informações de telemetria são exibidas nas páginas de IU do Centro de Controle Astra.

NetApp Active IQ Unified Manager

Com o NetApp Active IQ Unified Manager, você monitora seus clusters de storage do ONTAP a partir de uma única interface intuitiva e reprojetada que fornece inteligência do conhecimento da comunidade e análises de AI. Ele fornece insights operacionais, de performance e proativos abrangentes sobre o ambiente de storage e as máquinas virtuais (VMs) em execução nele. Quando ocorre um problema com a infraestrutura de storage, o Unified Manager pode notificá-lo sobre os detalhes do problema para ajudar a identificar a causa raiz. O painel da VM oferece uma visão das estatísticas de desempenho da VM para que você possa investigar todo o caminho de e/S do host VMware vSphere até a rede e, finalmente, até o storage. Alguns eventos também fornecem ações corretivas que podem ser tomadas para corrigir o problema. Você pode configurar alertas personalizados para eventos para que, quando os problemas ocorrem, você seja notificado por meio de traps de e-mail e SNMP. O Active IQ Unified Manager permite Planejar os requisitos de storage de seus usuários prevendo as tendências de capacidade e uso para agir proativamente antes que surjam problemas, evitando decisões reativas a curto prazo que podem levar a problemas adicionais a longo prazo.

Cisco Intersight

O Cisco Intersight é uma plataforma SaaS que oferece automação, observabilidade e otimização inteligentes para aplicações e infraestrutura tradicionais e nativas da nuvem. A plataforma ajuda a impulsionar a mudança com as equipes DE TI e fornece um modelo operacional projetado para a nuvem híbrida.

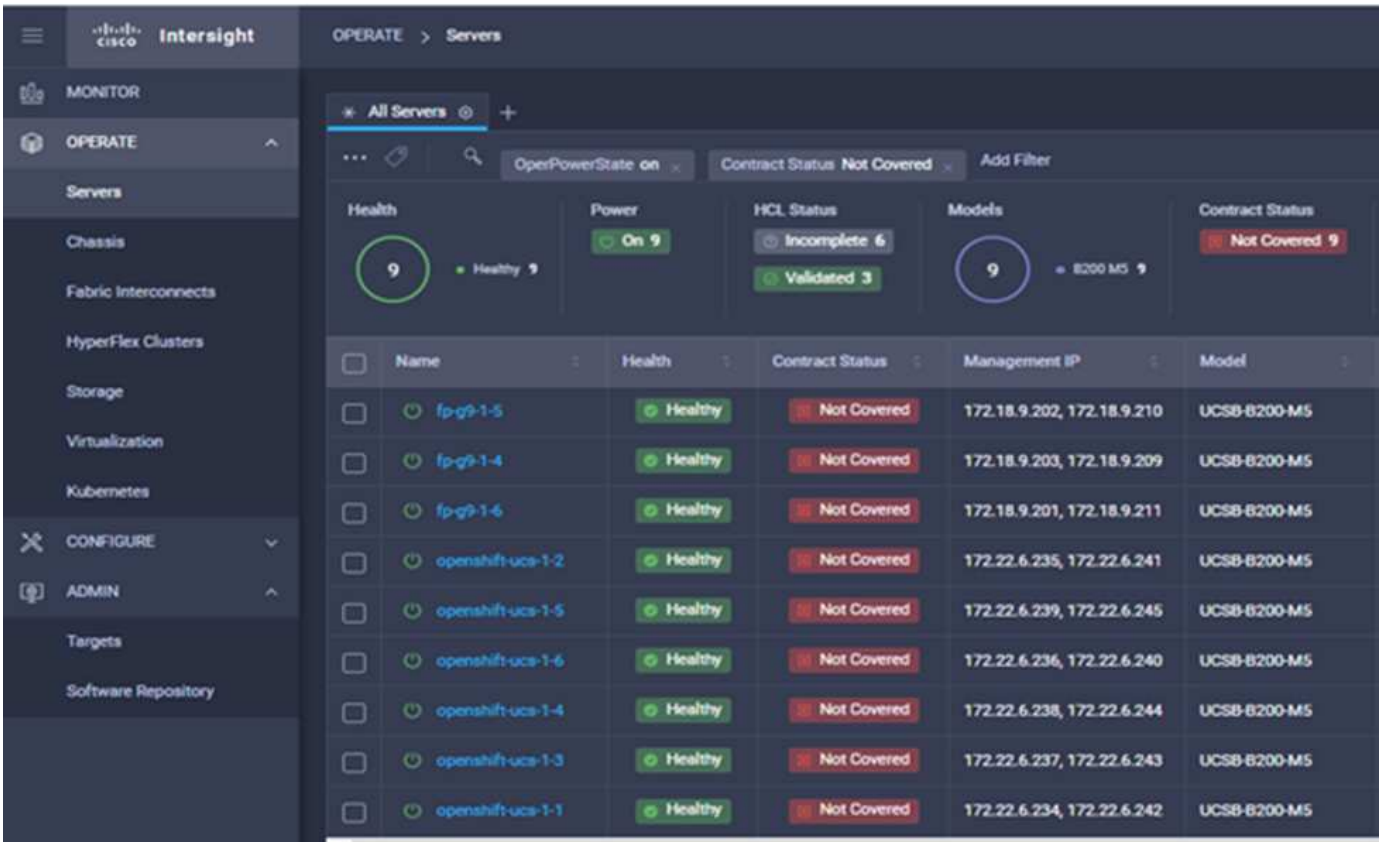
O Cisco Intersight oferece os seguintes benefícios:

- * Entrega mais rápida. * Fornecido como um serviço a partir da nuvem ou no data center do cliente com atualizações frequentes e inovação contínua, devido a um modelo de desenvolvimento de software baseado em agilidade. Dessa forma, o cliente pode se concentrar apenas em acelerar a entrega para a linha de negócios.
- **Operações simplificadas.** Simplifique as operações usando uma única ferramenta segura fornecida por SaaS com inventário, autenticação e APIs comuns para trabalhar em toda a stack e em todos os locais, eliminando silos entre as equipes. Desde o gerenciamento de servidores físicos e hipervisores no local, até VMs, K8s, sem servidor, automação, otimização e controle de custos nas nuvens locais e públicas.
- **Otimização contínua.** Otimize seu ambiente continuamente usando a inteligência fornecida pelo Cisco Intersight em todas as camadas, bem como o Cisco TAC. Essa inteligência é convertida em ações

recomendadas e automatizáveis para que você possa se adaptar em tempo real a cada mudança: Da movimentação de cargas de trabalho e monitoramento da integridade dos servidores físicos ao dimensionamento automático de clusters K8s, às recomendações de redução de custos nas nuvens públicas com as quais você trabalha.

Existem dois modos de operações de gerenciamento possíveis com o Cisco Intersight: O modo gerenciado de UMM e o modo gerenciado de Intersight (IMM). Você pode selecionar o UMM ou IMM nativo para os sistemas Cisco UCS conetados à malha durante a configuração inicial das interconexões de malha. Nesta solução, UMM nativo é usado.

A imagem a seguir mostra o painel do Cisco Intersight.

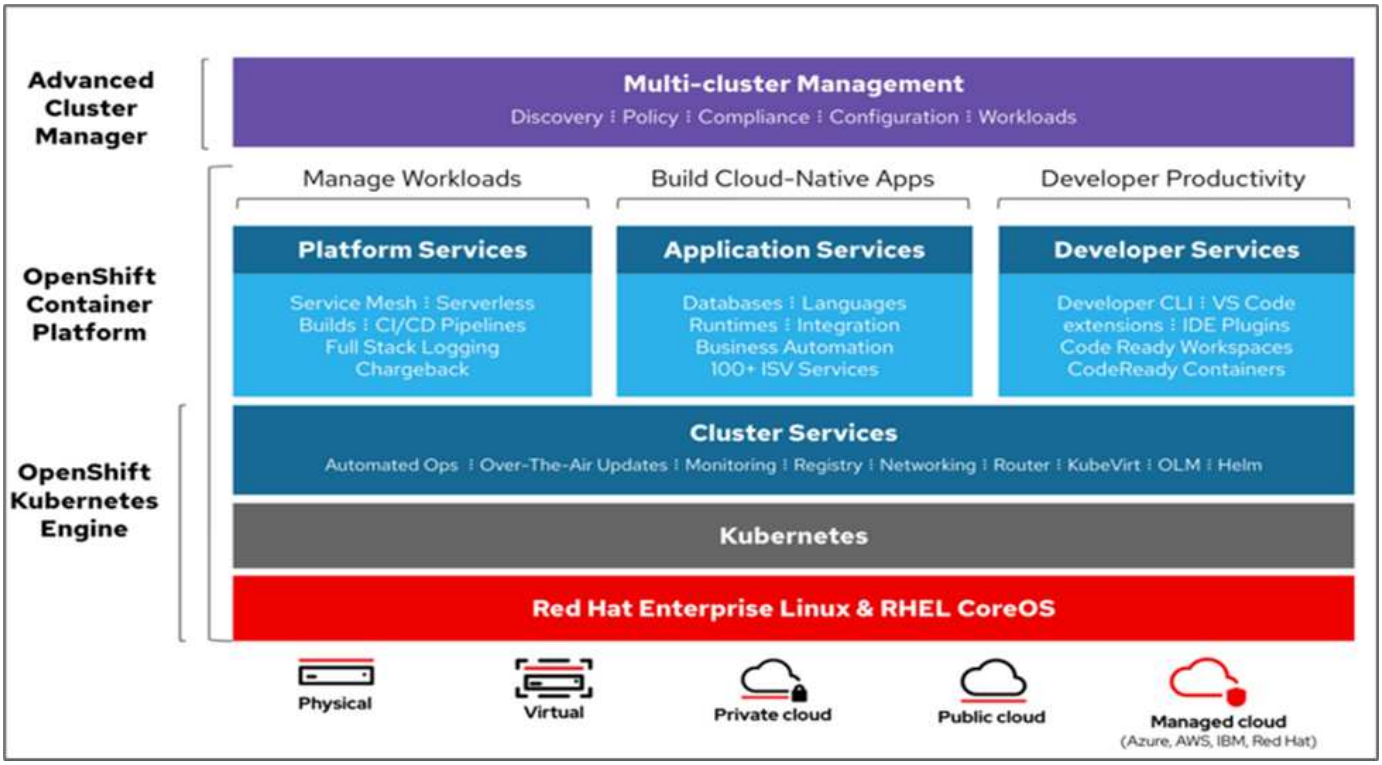


Red Hat OpenShift Container Platform

O Red Hat OpenShift Container Platform é uma plataforma de aplicativos de contêiner que reúne CRI-o e Kubernetes e fornece uma API e interface da Web para gerenciar esses serviços. O CRI-o é uma implementação da interface de tempo de execução de contentor (CRI) do Kubernetes para permitir o uso de tempos de execução compatíveis com a Open Container Initiative (OCI). É uma alternativa leve ao uso do Docker como o tempo de execução do Kubernetes.

OpenShift Container Platform permite que os clientes criem e gerenciem contentores. Os contêineres são processos autônomos que são executados em seu próprio ambiente, independentemente do sistema operacional e da infraestrutura subjacente. O OpenShift Container Platform ajuda a desenvolver, implantar e gerenciar aplicativos baseados em contentor. Ele fornece uma plataforma de autoatendimento para criar, modificar e implantar aplicativos sob demanda, permitindo, assim, ciclos de vida de desenvolvimento e liberação mais rápidos. O OpenShift Container Platform tem uma arquitetura baseada em microsserviços de unidades menores e desacopladas que trabalham juntas. Ele é executado em cima de um cluster do Kubernetes, com dados sobre os objetos armazenados no etcd, um armazenamento de chaves em cluster confiável.

A imagem a seguir é uma visão geral da plataforma de contentores Red Hat OpenShift.



Infraestrutura do Kubernetes

No OpenShift Container Platform, o Kubernetes gerencia aplicativos em contêineres em um conjunto de hosts de tempo de execução CRI-o e fornece mecanismos para implantação, manutenção e dimensionamento de aplicativos. O serviço CRI-o empacota, instancia e executa aplicativos em contêiner.

Um cluster do Kubernetes consiste em um ou mais mestres e um conjunto de nós de trabalho. O design da solução inclui funcionalidade de alta disponibilidade (HA) no hardware, bem como na pilha de software. Um cluster do Kubernetes foi projetado para ser executado no modo HA com três nós mestres e um mínimo de dois nós de trabalho para garantir que o cluster não tenha um ponto único de falha.

Red Hat Core os

O OpenShift Container Platform usa o Red Hat Enterprise Linux CoreOS (RHCOS), um sistema operacional orientado a contentores que combina alguns dos melhores recursos e funções dos sistemas operacionais CoreOS e Red Hat Atomic Host. O RHCOS foi projetado especificamente para executar aplicativos em contêiner da OpenShift Container Platform e trabalha com novas ferramentas para fornecer instalação rápida, gerenciamento baseado em operador e atualizações simplificadas.

O RHCOS inclui os seguintes recursos:

- Ignição, que a OpenShift Container Platform usa como primeira configuração do sistema de inicialização para iniciar e configurar máquinas.
- CRI-o, uma implementação de tempo de execução de contêineres nativa do Kubernetes que se integra estreitamente ao sistema operacional para oferecer uma experiência Kubernetes eficiente e otimizada. O CRI-o fornece instalações para executar, parar e reiniciar contentores. Ele substitui totalmente o Docker Container Engine, que foi usado na OpenShift Container Platform 3.
- Kubelet, o principal agente de nós do Kubernetes, é responsável pelo lançamento e monitoramento de contêineres.

VMware vSphere 7,0

O VMware vSphere é uma plataforma de virtualização para gerenciar holisticamente grandes coleções de infraestruturas (recursos incluindo CPUs, armazenamento e rede) como um ambiente operacional otimizado, versátil e dinâmico. Ao contrário dos sistemas operacionais tradicionais que gerenciam uma máquina individual, o VMware vSphere agrega a infraestrutura de um data center inteiro para criar uma única potência com recursos que podem ser alocados de forma rápida e dinâmica para qualquer aplicativo necessário.

Para obter mais informações, "VMware vSphere"consulte .

VMware vSphere vCenter

O VMware vCenter Server fornece gerenciamento unificado de todos os hosts e VMs a partir de um único console e agrega o monitoramento de desempenho de clusters, hosts e VMs. O VMware vCenter Server oferece aos administradores uma visão profunda sobre o status e a configuração de clusters de computação, hosts, VMs, armazenamento, SO convidado e outros componentes críticos de uma infraestrutura virtual. O VMware vCenter gerencia o rico conjunto de recursos disponíveis em um ambiente VMware vSphere.

Revisões de hardware e software

Essa solução pode ser estendida a qualquer ambiente FlexPod que esteja executando versões compatíveis de software, firmware e hardware, conforme definido no "Ferramenta de Matriz de interoperabilidade do NetApp" e "Lista de compatibilidade de hardware do Cisco UCS." o cluster OpenShift é instalado no FlexPod de forma bare-metal e no VMware vSphere.

Apenas uma única instância do Astra Control Center é necessária para gerenciar vários clusters OpenShift (k8s), enquanto o Trident CSI é instalado em cada cluster do OpenShift. O Astra Control Center pode ser instalado em qualquer um desses clusters do OpenShift. Nessa solução, o Astra Control Center é instalado no cluster bare-metal OpenShift.

A tabela a seguir lista as revisões de hardware e software do FlexPod para o OpenShift.

Componente	Produto	Versão
Computação	O tecido Cisco UCS interconeta 6454	4,1 mm (3c mm)
	Servidores Cisco UCS B200 M5	4,1 mm (3c mm)
Rede	Cisco Nexus 9336C-FX2P NX-os	9,3 mm (8 mm)
Armazenamento	NetApp AFF A700	9.11.1
	Centro de Controle NetApp Astra	22.04.0
	Plug-in NetApp Astra Trident CSI	22.04.0
	NetApp Active IQ Unified Manager	9,11
Software	Driver Ethernet nenic do VMware ESXi	1.0.35.0
	VSphere ESXi	7,0 MM (U2 MM)
	Dispositivo VMware vCenter	7,0 U2b
	Dispositivo virtual de assistência à monitorização da distância da Cisco	1,0.9-342

Componente	Produto	Versão
	OpenShift Container Platform	4,9
	Nó principal da plataforma de contêiner OpenShift	RHCOS 4,9
	OpenShift Container Platform Worker Node	RHCOS 4,9

A tabela a seguir lista as versões de software do OpenShift na AWS.

Componente	Produto	Versão
Computação	Tipo de instância mestre: M5.xlarge	n/a.
	Tipo de instância do trabalhador: M5.Large	n/a.
Rede	Gateway de trânsito em nuvem privada virtual	n/a.
Armazenamento	NetApp Cloud Volumes ONTAP	9.11.1
	Plug-in NetApp Astra Trident CSI	22.04.0
Software	OpenShift Container Platform	4,9
	Nó principal da plataforma de contêiner OpenShift	RHCOS 4,9
	OpenShift Container Platform Worker Node	RHCOS 4,9

"Próximo: FlexPod para instalação bare-metal da plataforma de contentores OpenShift 4."

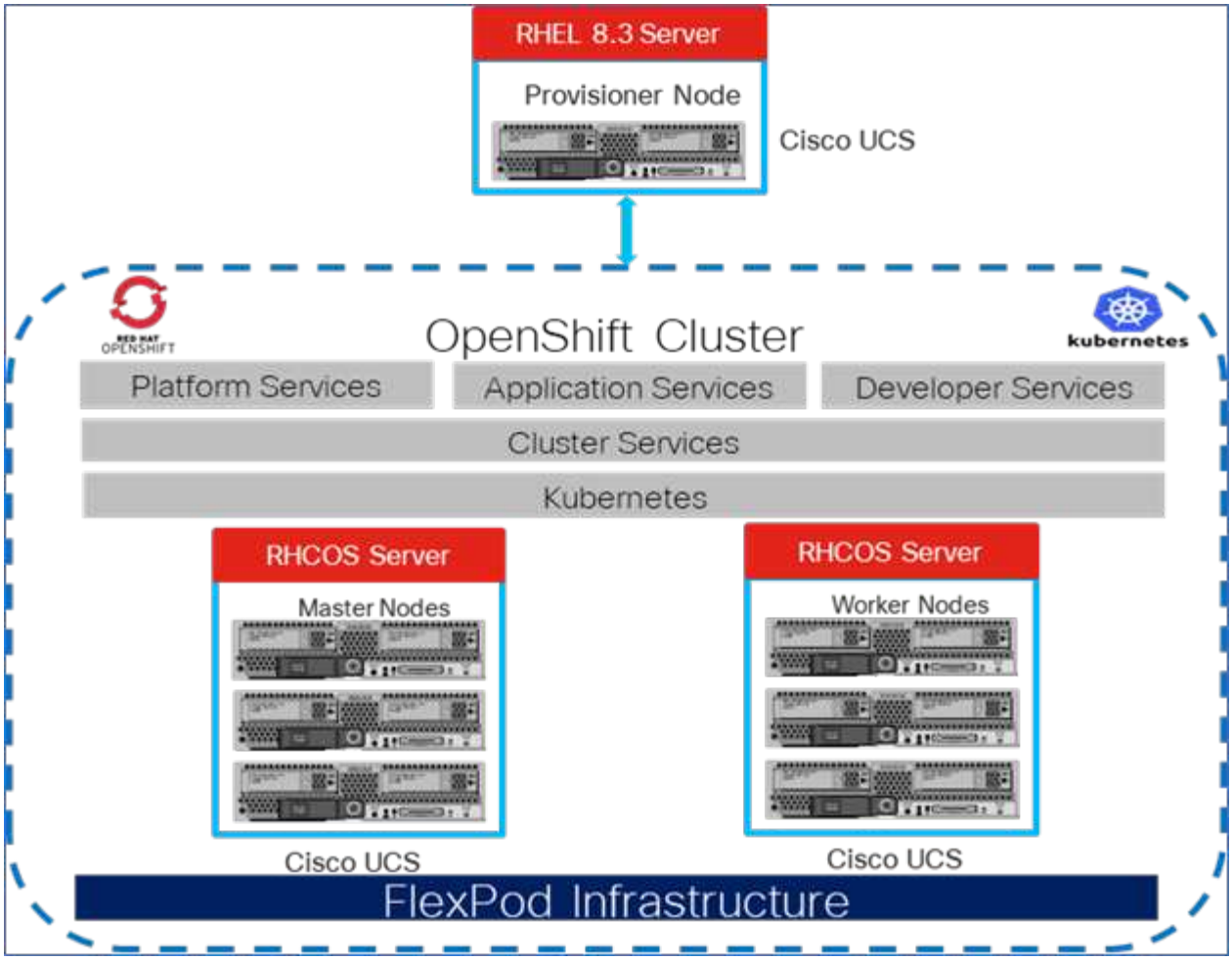
Instalação e configuração

FlexPod para instalação bare-metal da plataforma de contentores OpenShift 4

"Anterior: Componentes da solução."

Para entender o design bare-metal da plataforma de contêiner do FlexPod para OpenShift 4, os detalhes de implantação e a instalação e configuração do NetApp Astra Trident, "FlexPod com guia de projeto e implantação validados do OpenShift Cisco (CVD)" consulte . Esse CVD abrange a implantação do FlexPod e do OpenShift Container Platform usando o Ansible. O CVD também fornece informações detalhadas sobre a preparação de nós de trabalho, instalação do Astra Trident, back-end de storage e configurações de classe de storage, que são os poucos pré-requisitos para implantação e configuração do Astra Control Center.

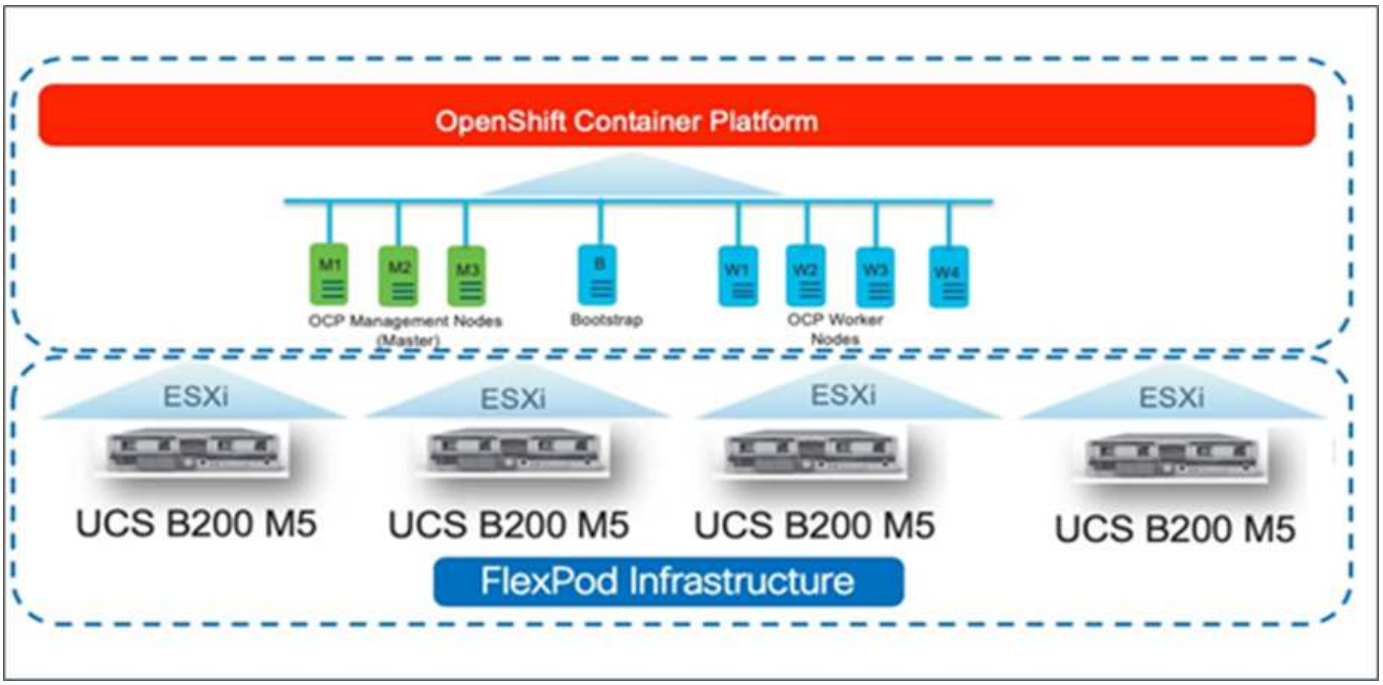
A figura a seguir ilustra o metal nu da plataforma de contentores OpenShift 4 no FlexPod.



FlexPod para OpenShift Container Platform 4 na instalação da VMware

Para obter mais informações sobre como implantar o Red Hat OpenShift Container Platform 4 no FlexPod executando o VMware vSphere, "FlexPod Datacenter para OpenShift Container Platform 4" consulte .

A figura a seguir ilustra o FlexPod para OpenShift Container Platform 4 no vSphere.

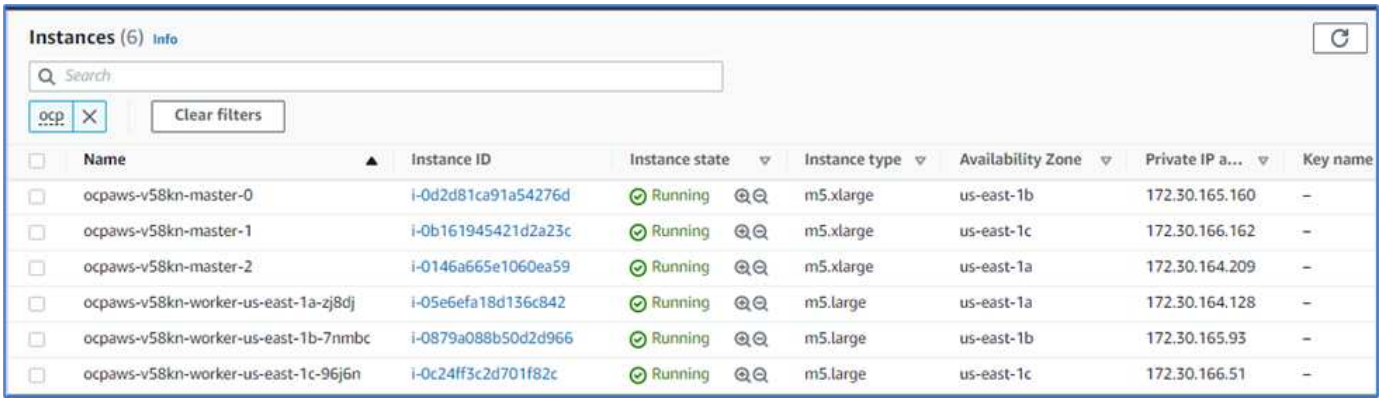


"Próximo: Red Hat OpenShift na AWS."

Red Hat OpenShift na AWS

"Anterior: FlexPod para instalação bare-metal da plataforma de contentores OpenShift 4."

Um cluster independente do OpenShift Container Platform 4 é implantado na AWS como um local de DR. Os nós master e worker abrangem três zonas de disponibilidade para alta disponibilidade.



Name	Instance ID	Instance state	Instance type	Availability Zone	Private IP a...	Key name
ocpaws-v58kn-master-0	i-0d2d81ca91a54276d	Running	m5.xlarge	us-east-1b	172.30.165.160	–
ocpaws-v58kn-master-1	i-0b161945421d2a23c	Running	m5.xlarge	us-east-1c	172.30.166.162	–
ocpaws-v58kn-master-2	i-0146a665e1060ea59	Running	m5.xlarge	us-east-1a	172.30.164.209	–
ocpaws-v58kn-worker-us-east-1a-zj8dj	i-05e6efa18d136c842	Running	m5.large	us-east-1a	172.30.164.128	–
ocpaws-v58kn-worker-us-east-1b-7nmbc	i-0879a088b50d2d966	Running	m5.large	us-east-1b	172.30.165.93	–
ocpaws-v58kn-worker-us-east-1c-96j6n	i-0c24ff3c2d701f82c	Running	m5.large	us-east-1c	172.30.166.51	–

```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

O OpenShift é implantado como a "cluster privado" em uma VPC existente na AWS. Um cluster privado OpenShift Container Platform não expõe endpoints externos e é acessível apenas a partir de uma rede interna e não é visível para a Internet. Um NetApp Cloud Volumes ONTAP de nó único é implantado usando o NetApp Cloud Manager, que fornece um back-end de storage para o Astra Trident.

Para obter mais informações sobre como instalar o OpenShift na AWS, "Documentação do OpenShift" consulte .

"Próximo: NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Anterior: Red Hat OpenShift na AWS."

A instância do NetApp Cloud Volumes ONTAP é implantada na AWS e serve como storage de back-end para o Astra Trident. Antes de adicionar um ambiente de trabalho Cloud Volumes ONTAP, um conetor deve ser implantado. O Cloud Manager solicita se você tentar criar seu primeiro ambiente de trabalho do Cloud Volumes ONTAP sem um conetor. Para implantar um conetor na AWS, "Crie um conetor" consulte .

Para implantar o Cloud Volumes ONTAP na AWS, "Início rápido para AWS" consulte .

Após a implantação do Cloud Volumes ONTAP, você poderá instalar o Astra Trident e configurar a classe de snapshot e back-end de storage no cluster do OpenShift Container Platform.

"Próximo: Instalação do Astra Control Center no OpenShift Container Platform."

Instalação do Astra Control Center no OpenShift Container Platform

"Anterior: NetApp Cloud Volumes ONTAP."

Você pode instalar o Astra Control Center no cluster OpenShift executado no FlexPod ou na AWS com um back-end de storage do Cloud Volumes ONTAP. Nessa solução, o Astra Control Center é implantado no cluster bare-metal OpenShift.

O Astra Control Center pode ser instalado usando o processo padrão descrito "aqui" ou a partir do Red Hat OpenShift OperatorHub. O Operador de Controle Astra é um operador certificado pela Red Hat. Nesta solução, o Astra Control Center é instalado usando o Red Hat OperatorHub.

Requisitos ambientais

- O Astra Control Center é compatível com várias distribuições do Kubernetes. Para o Red Hat OpenShift, as versões compatíveis incluem o Red Hat OpenShift Container Platform 4,8 ou 4,9.
- O Astra Control Center requer os seguintes recursos, além dos requisitos de recursos de aplicações do ambiente e do usuário final:

Componentes	Requisito
Capacidade de back-end de storage	Pelo menos 500GB disponível
Nós de trabalho	Pelo menos 3 nós de trabalho, com 4 núcleos de CPU e 12GB GB de RAM cada
Endereço FQDN (nome de domínio totalmente qualificado)	Um endereço FQDN para o Astra Control Center
Astra Trident	Astra Trident 21,04 ou mais recente instalado e configurado
Controlador de entrada ou balanceador de carga	Configure o controlador de entrada para expor o Astra Control Center com um balanceador de URL ou carga para fornecer endereço IP que será resolvido para o FQDN

- Você deve ter um Registro de imagem privado existente para o qual você pode enviar as imagens de compilação do Astra Control Center. Você precisa fornecer o URL do Registro de imagens onde você carrega as imagens.

> Algumas imagens são puxadas durante a execução de certos fluxos de trabalho, e os contentores são criados e destruídos quando necessário.

- O Astra Control Center exige que uma classe de storage seja criada e definida como a classe de storage padrão. O Astra Control Center é compatível com os seguintes drivers ONTAP fornecidos pelo Astra Trident:
  - ONTAP-nas
  - ONTAP-nas-FlexGroup
  - ONTAP-san
  - ONTAP-são-economia

> Presumimos que os clusters OpenShift implantados tenham o Astra Trident instalado e configurado com um back-end do ONTAP, e que uma classe de storage padrão também seja definida.

- Para clonagem de aplicações em ambientes OpenShift, o Astra Control Center precisa permitir que o OpenShift monte volumes e altere a propriedade dos arquivos. Para modificar a política de exportação do ONTAP para permitir essas operações, execute os seguintes comandos:

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

Para adicionar um segundo ambiente operacional do OpenShift como um recurso de computação gerenciado, verifique se o recurso snapshot do volume do Astra Trident está ativado. Para habilitar e testar snapshots de volume com o Astra Trident, consulte o oficial "Instruções do Astra Trident".

- É necessário configurar um "VolumeSnapClass" em todos os clusters do Kubernetes de onde as aplicações são gerenciadas. Isso também pode incluir o cluster K8s no qual o Astra Control Center está instalado. O Astra Control Center pode gerenciar aplicações no cluster K8s no qual ele está sendo executado.

Requisitos de gerenciamento de aplicativos

- **Licenciamento.** Para gerenciar aplicações usando o Astra Control Center, você precisa de uma licença do Astra Control Center.
- * Namespaces.* Um namespace é a maior entidade que pode ser gerenciada como uma aplicação pelo Astra Control Center. Você pode optar por filtrar componentes com base nos rótulos do aplicativo e rótulos personalizados em um namespace existente e gerenciar um subconjunto de recursos como um aplicativo.
- **StorageClass.** Se você instalar um aplicativo com um StorageClass explicitamente definido e precisar clonar o aplicativo, o cluster de destino para a operação de clone precisará ter o StorageClass originalmente especificado. A clonagem de um aplicativo com um StorageClass explicitamente definido para um cluster que não tem o mesmo StorageClass falha.
- **Recursos do Kubernetes.** As aplicações que usam recursos do Kubernetes não capturadas pelo Astra Control podem não ter recursos completos de gerenciamento de dados de aplicações. O Astra Control pode capturar os seguintes recursos do Kubernetes:

Recursos do Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	CustomResource	CronJob
DaemonSet	HorizontalPodAutoscaler	Entrada
DeploymentConfig	MutatingWebhook	PersistentVolumeClaim
Pod	PodDisruptionBudget	PodTemplate
NetworkPolicy	ReplicaSet	Função
RoleBinding	Rota	Segredo
ValidatingWebhook		

Instale o Astra Control Center usando o OpenShift OperatorHub

O procedimento a seguir instala o Astra Control Center usando o Red Hat OperatorHub. Nessa solução, o Astra Control Center é instalado em um cluster OpenShift bare-metal executado no FlexPod.

1. Faça o download do pacote Astra Control Center (`astra-control-center-[version].tar.gz`) no "Site de suporte da NetApp".
2. Faça o download do arquivo .zip para os certificados e chaves do Astra Control Center no "Site de suporte da NetApp".
3. Verifique a assinatura do pacote.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraia as imagens Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Mude para o diretório Astra.

```
cd astra-control-center-[version]
```

6. Adicione as imagens ao seu registo local.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Use o script apropriado para carregar as imagens, marcar as imagens e enviá-las para o Registro local.

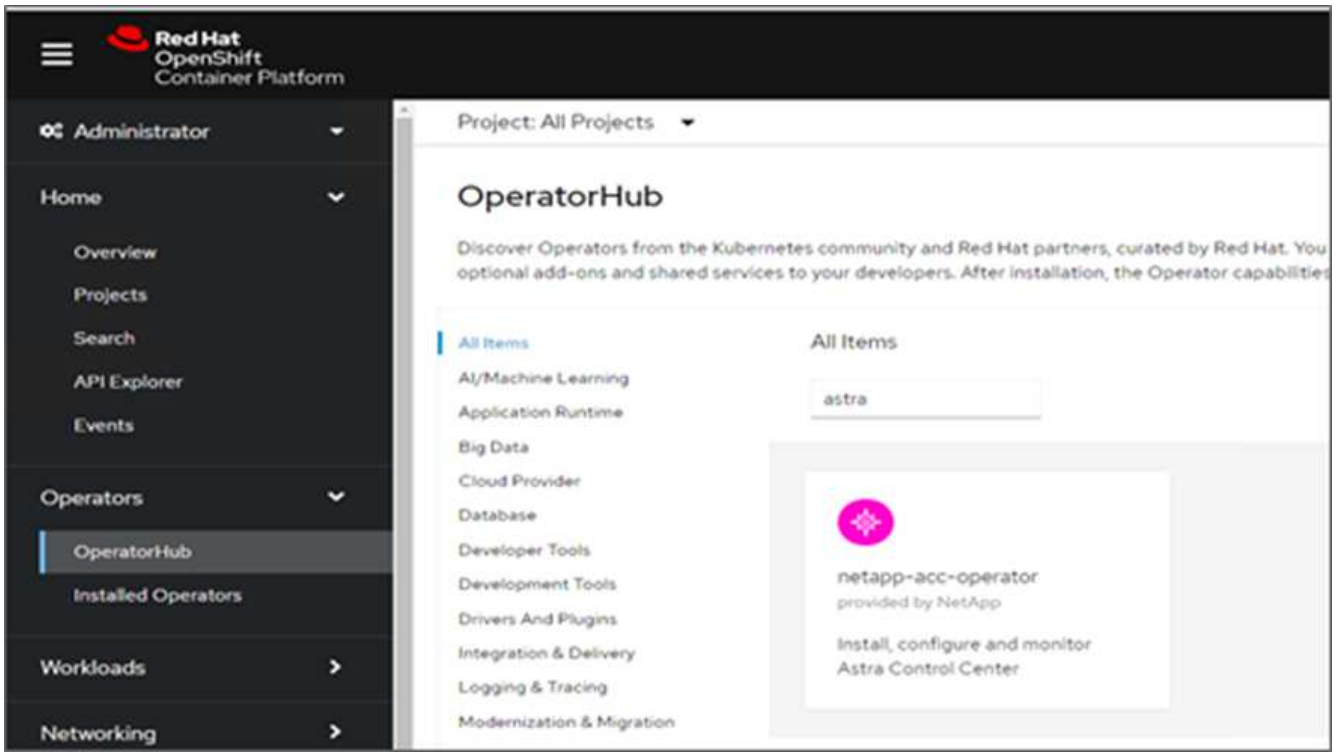
   Para Docker:

```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  docker tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  docker push ${REGISTRY}/${astraImage}
done
```

Para Podman:

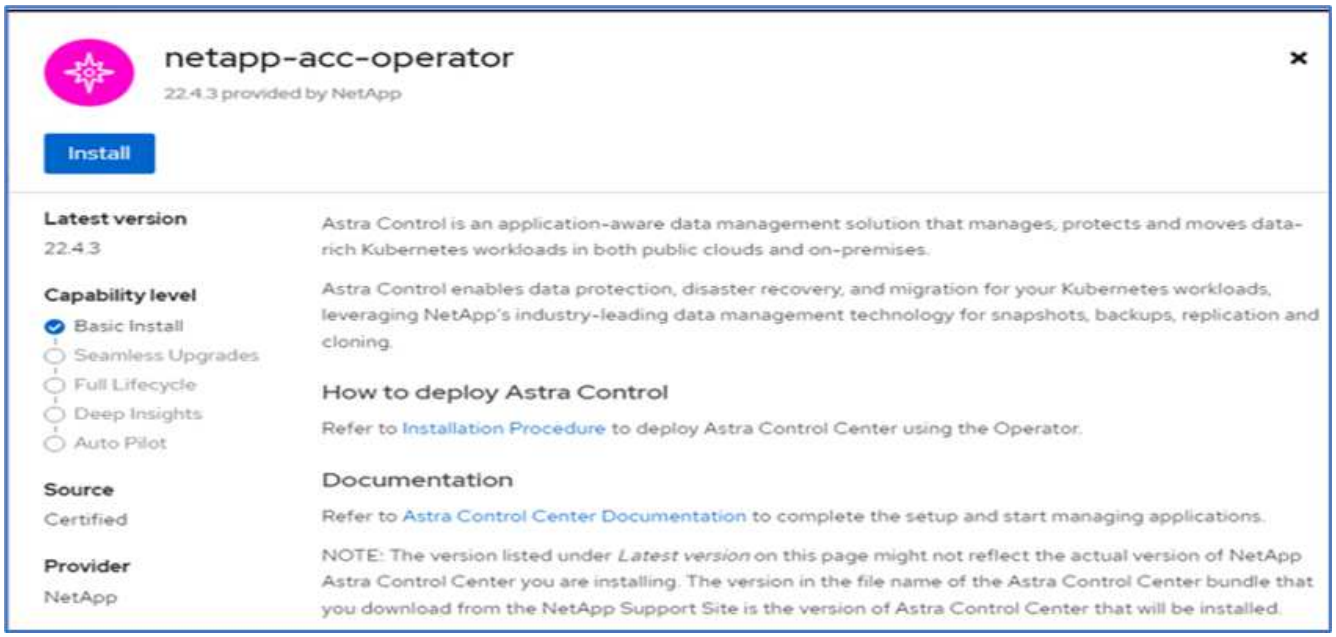
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```

8. Faça login no console da Web do cluster OpenShift em metal. No menu lateral, selecione operadores > OperatorHub. Digite `astra` para listar o `netapp-acc-operator`.

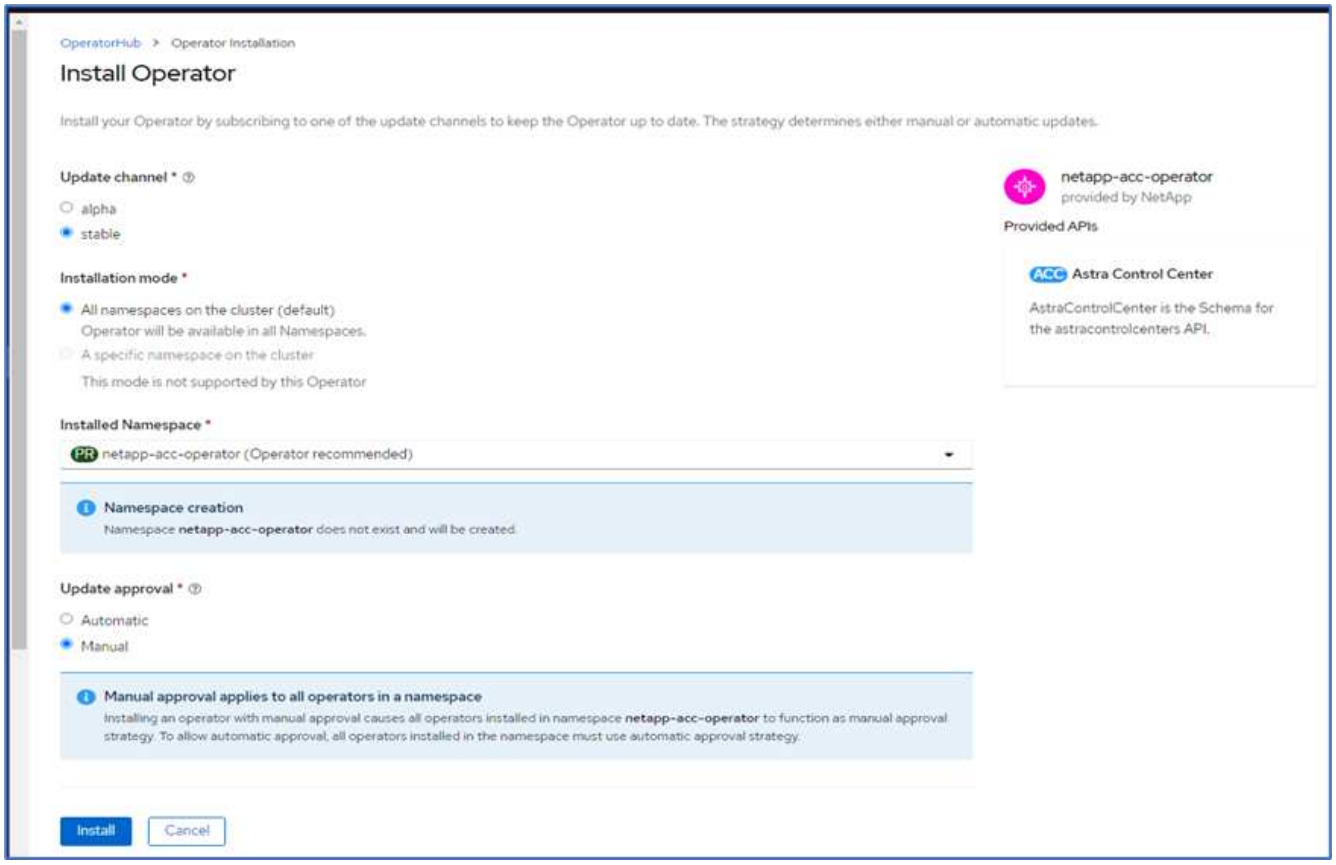


`netapp-acc-operator` É um operador Red Hat OpenShift certificado e está listado sob o catálogo OperatorHub.

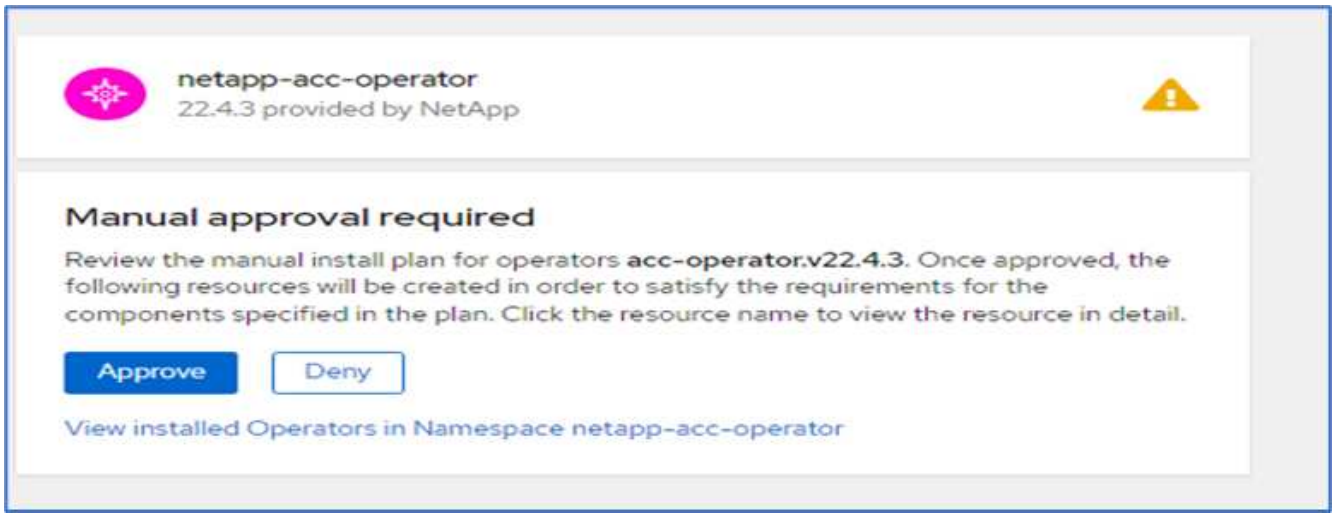
9. `netapp-acc-operator`Selecione e clique em Instalar.



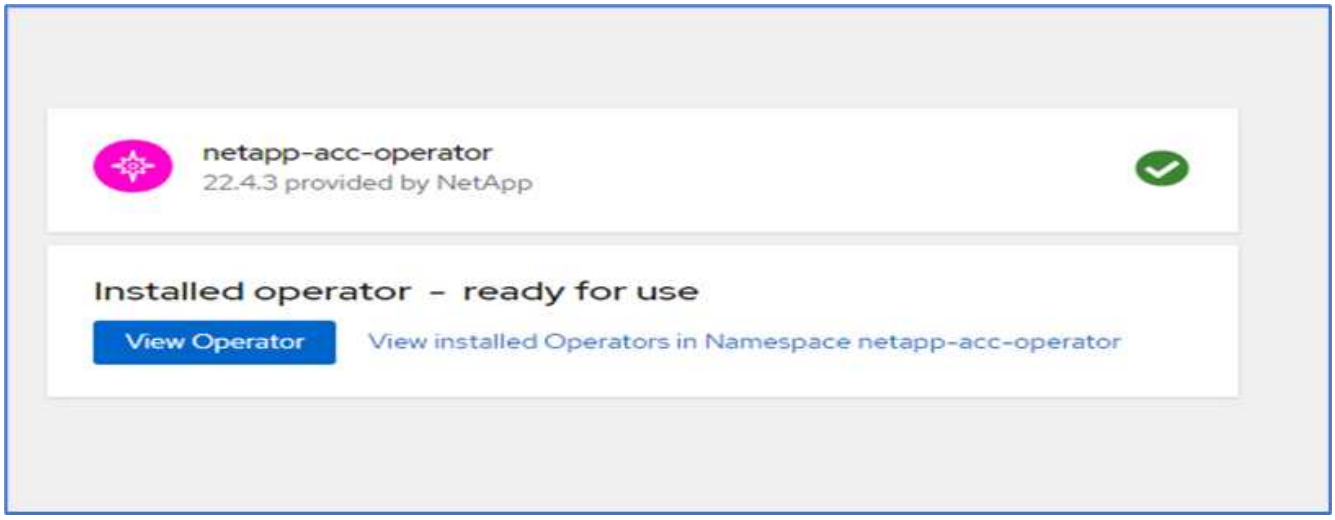
10. Selecione as opções apropriadas e clique em Instalar.



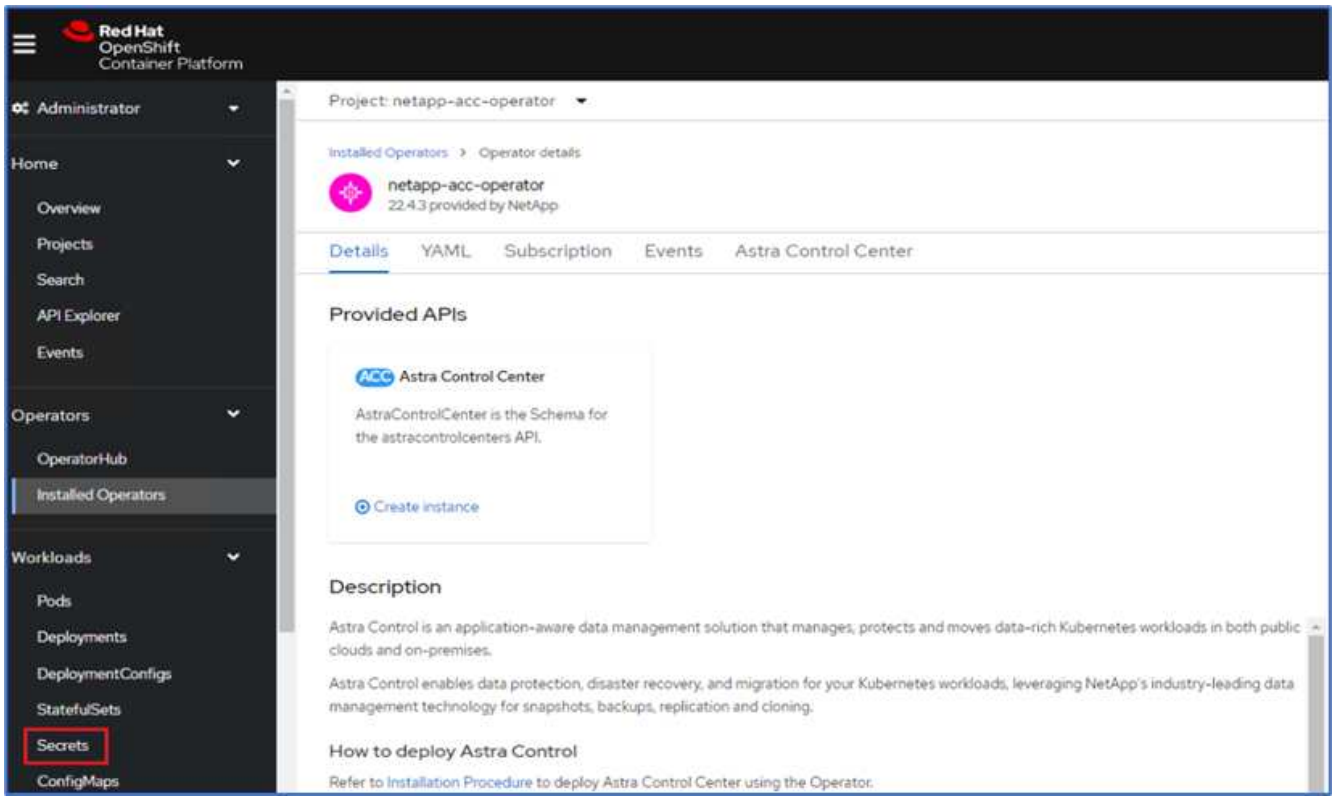
11. Aprove a instalação e aguarde a instalação do operador.



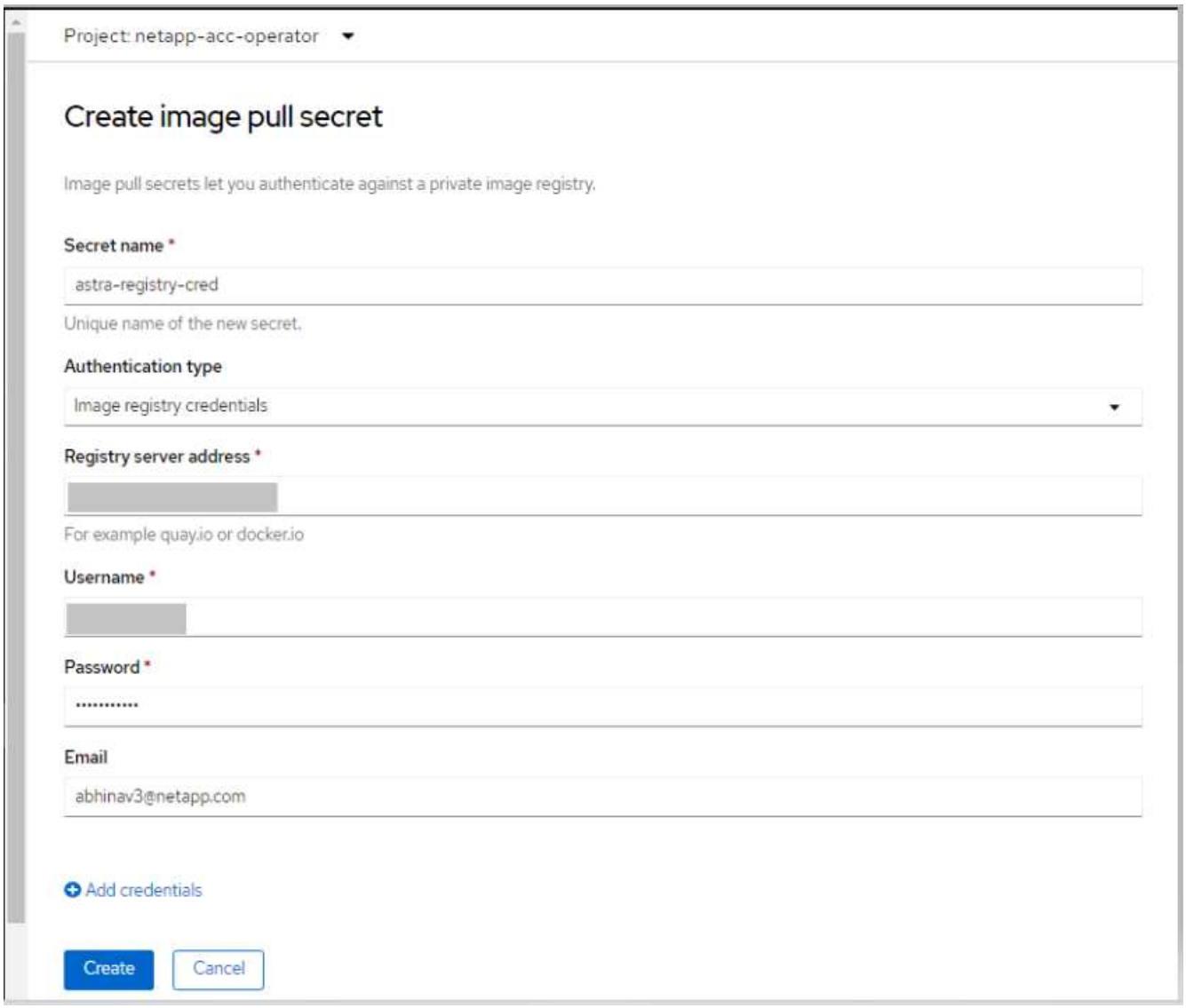
12. Nesta fase, o operador é instalado com êxito e pronto a ser utilizado. Clique em Exibir Operador para iniciar a instalação do Centro de Controle Astra.



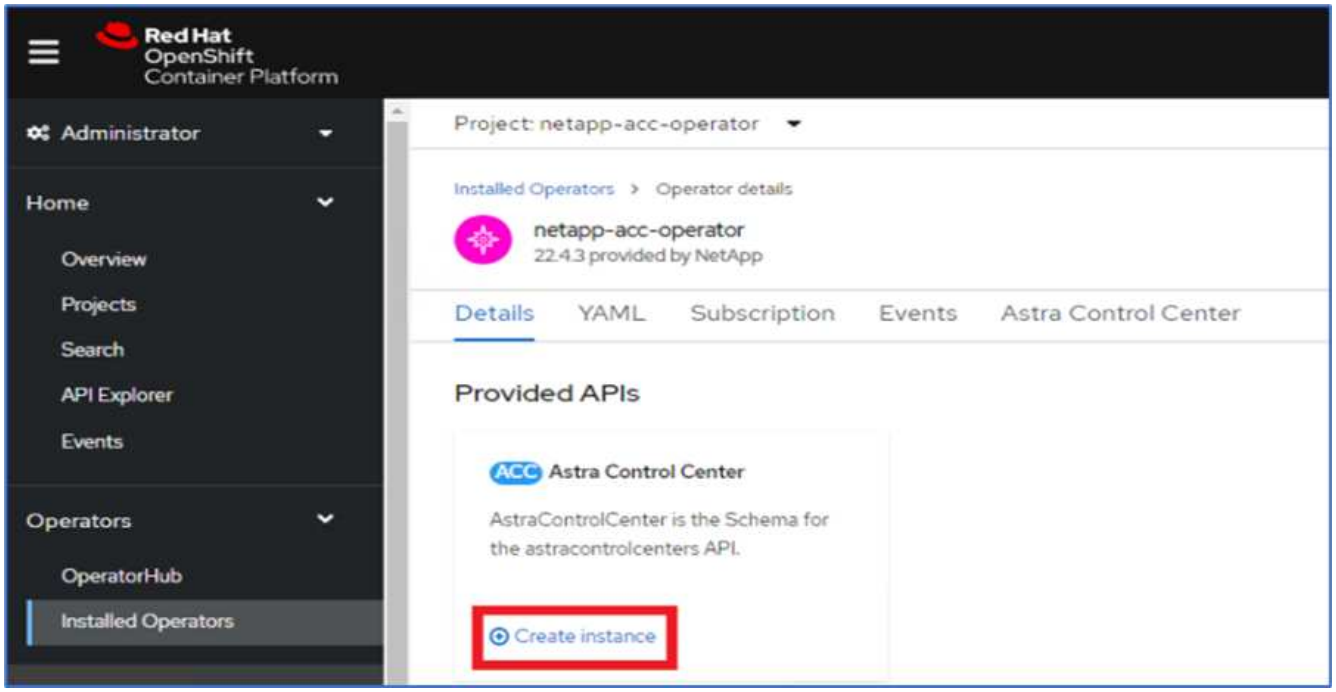
13. Antes de instalar o Astra Control Center, crie o segredo para fazer o download das imagens Astra do Registro Docker enviado anteriormente.



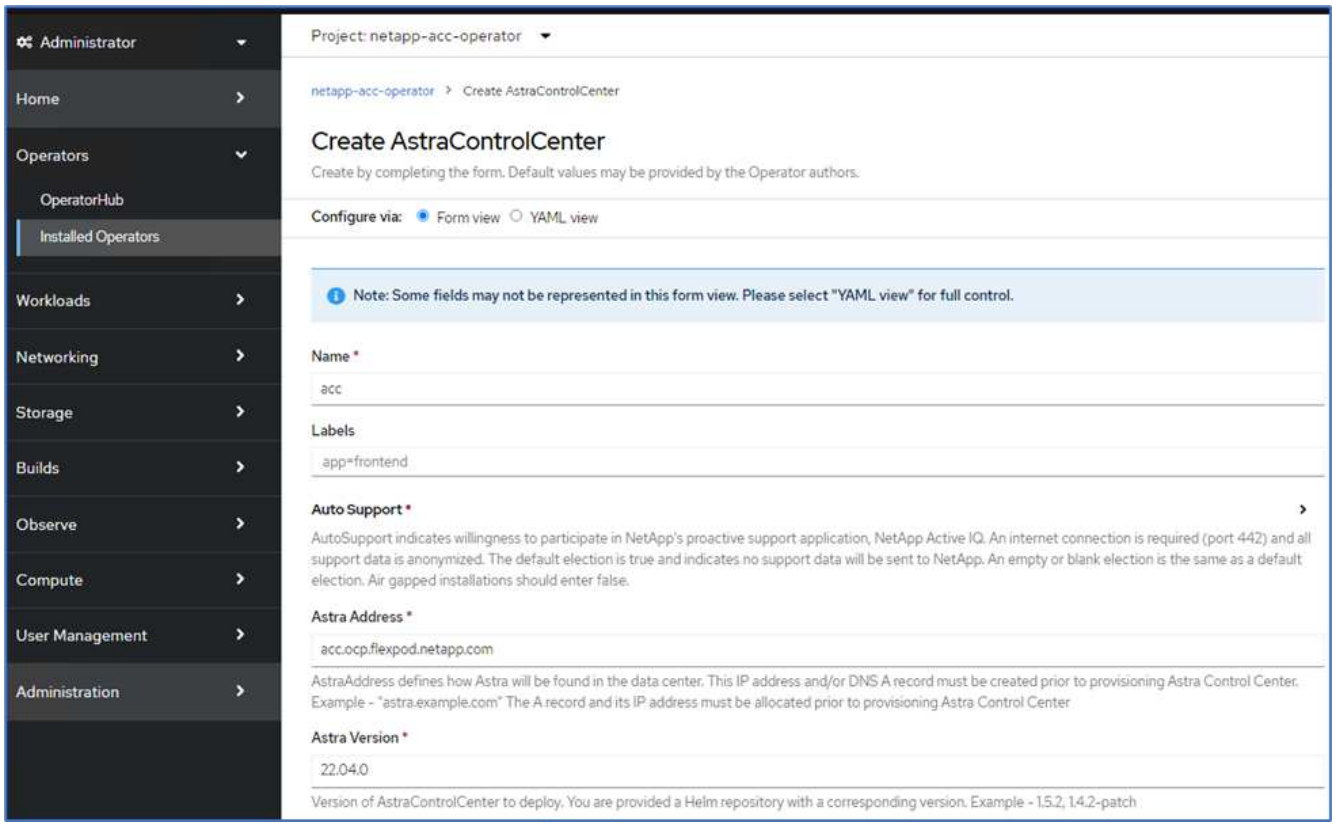
14. Para extrair as imagens do Astra Control Center do seu repositório privado do Docker, crie um segredo no `netapp-acc-operator` namespace. Esse nome secreto é fornecido no manifesto YAML do Astra Control Center em uma etapa posterior.



15. No menu lateral, selecione operadores > operadores instalados e clique em criar instância na seção APIs fornecidas.



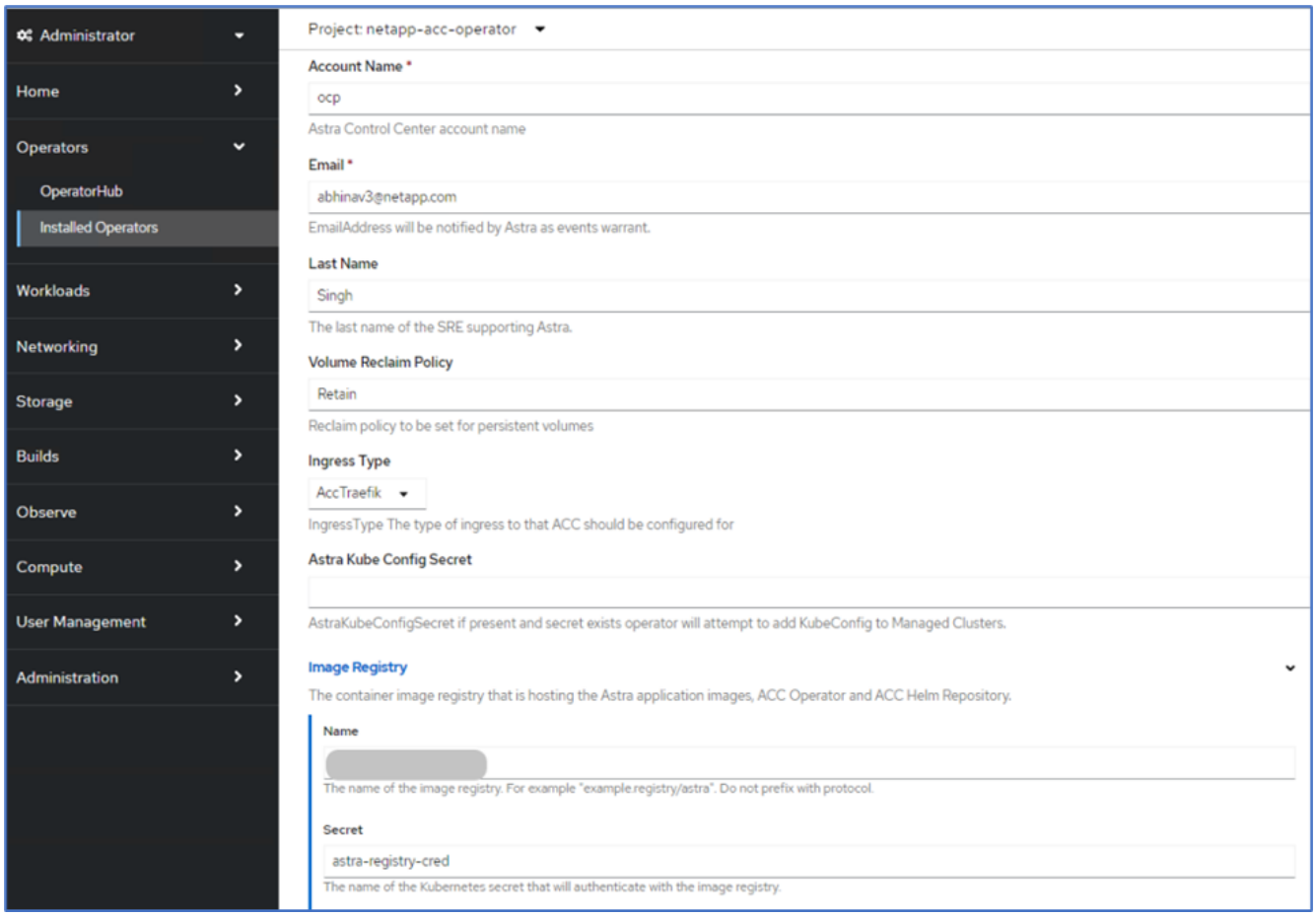
16. Preencha o formulário Create AstraControlCenter. Forneça o nome, o endereço Astra e a versão Astra.



Em Endereço Astra, forneça o endereço FQDN para o Centro de Controle Astra. Esse endereço é usado para acessar o console Web do Astra Control Center. O FQDN também deve ser resolvido para uma rede IP acessível e deve ser configurado no DNS.

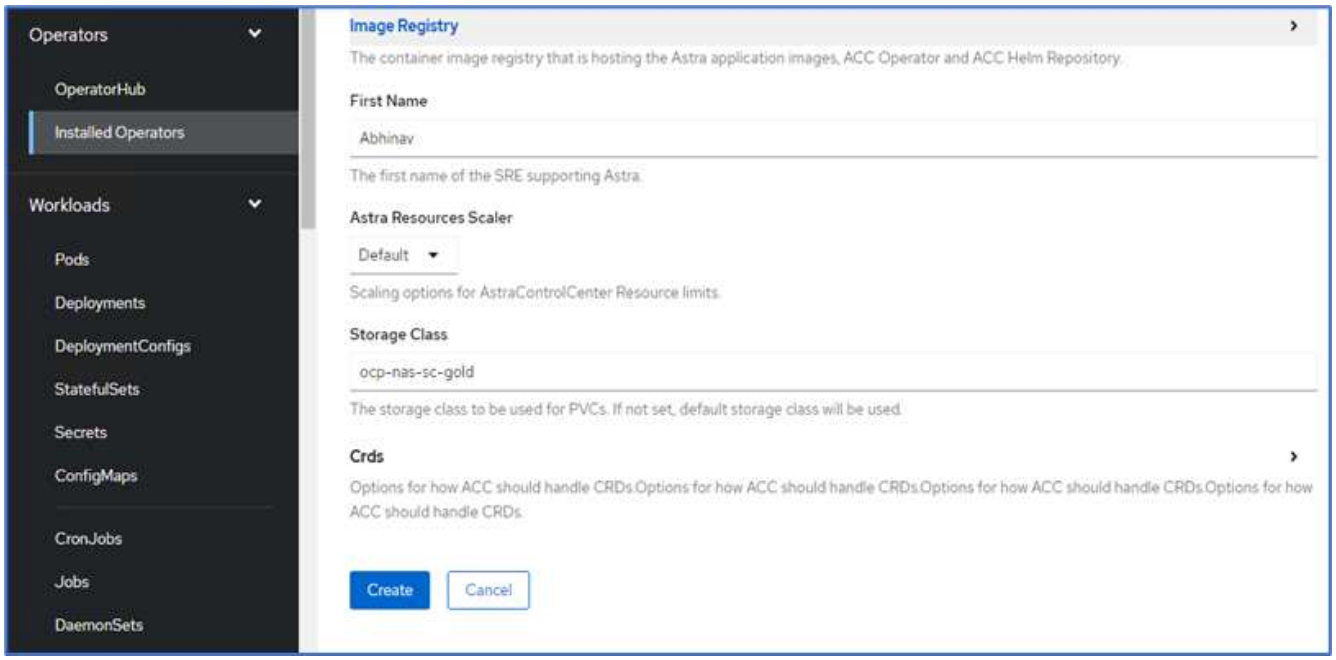
17. Insira um nome de conta, endereço de e-mail, sobrenome do administrador e mantenha a política de recuperação de volume padrão. Se estiver usando um balanceador de carga, defina o tipo de entrada

como `AccTraefik`. Caso contrário, selecione Genérico para `Ingress.Controller`. Em Registro de imagens, insira o caminho do Registro de imagem do contentor e o segredo.

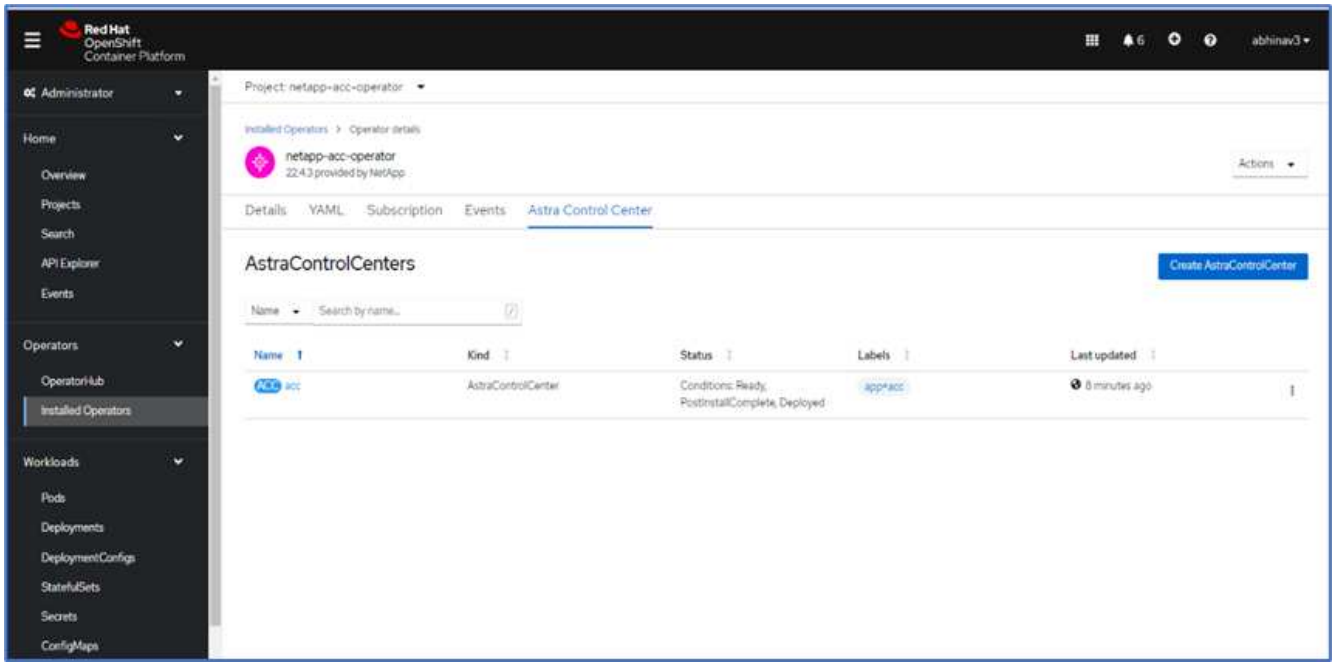


Nesta solução, o balanceador de carga Metallb é usado. Portanto, o tipo de ingresso é AcTraefik. Isso expõe o gateway traefik Astra Control Center como um serviço Kubernetes do tipo LoadBalancer.

18. Insira o nome do administrador, configure o dimensionamento de recursos e forneça a classe de armazenamento. Clique em criar.



O status da instância do Astra Control Center deve mudar de implantação para pronta.



19. Verifique se todos os componentes do sistema foram instalados com êxito e se todos os pods estão em execução.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

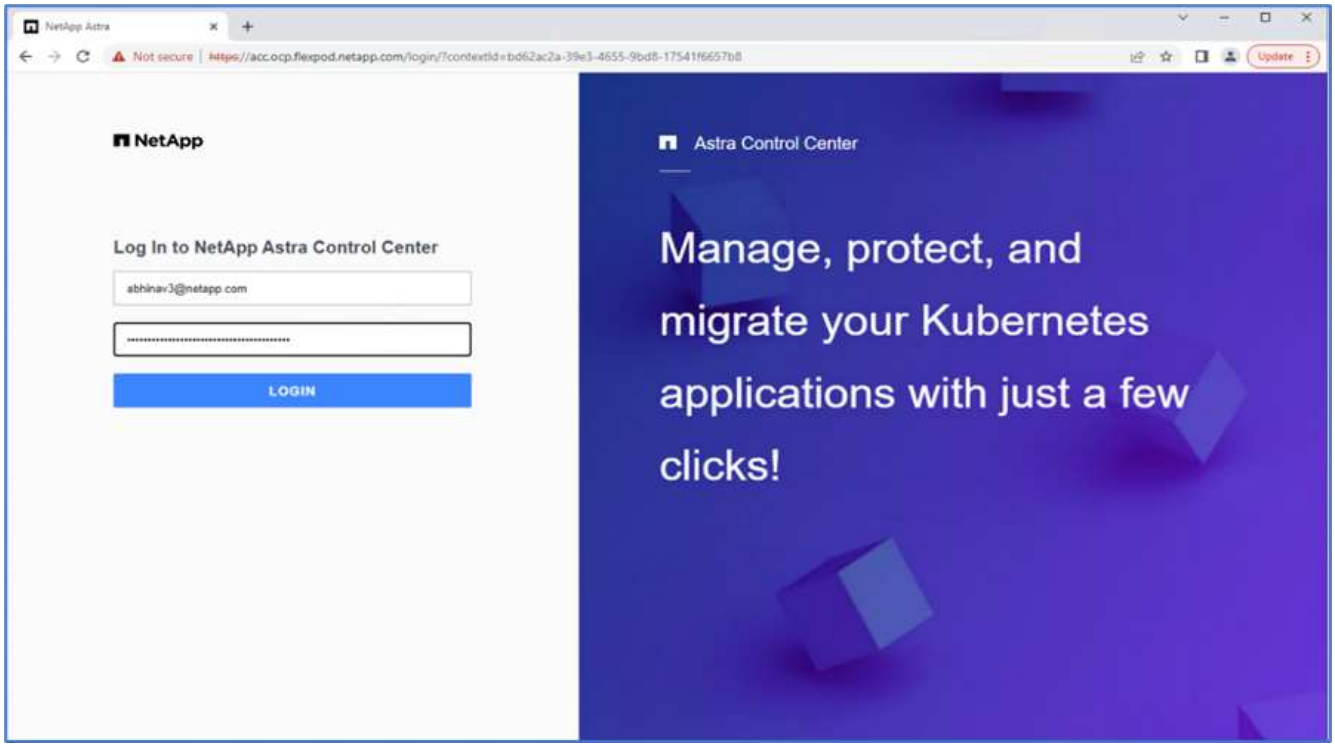
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

Cada pod deve ter um status de Running (em execução). Pode levar alguns minutos até que os pods do sistema sejam implantados.

20. Quando todos os pods estiverem em execução, execute o seguinte comando para recuperar a senha única. Na versão YAML da saída, verifique o `status.deploymentState` campo para o valor implantado e copie o valor `status.uuid`. A palavra-passe é `ACC-` seguida pelo valor UUID. (ACC-[UUID]).

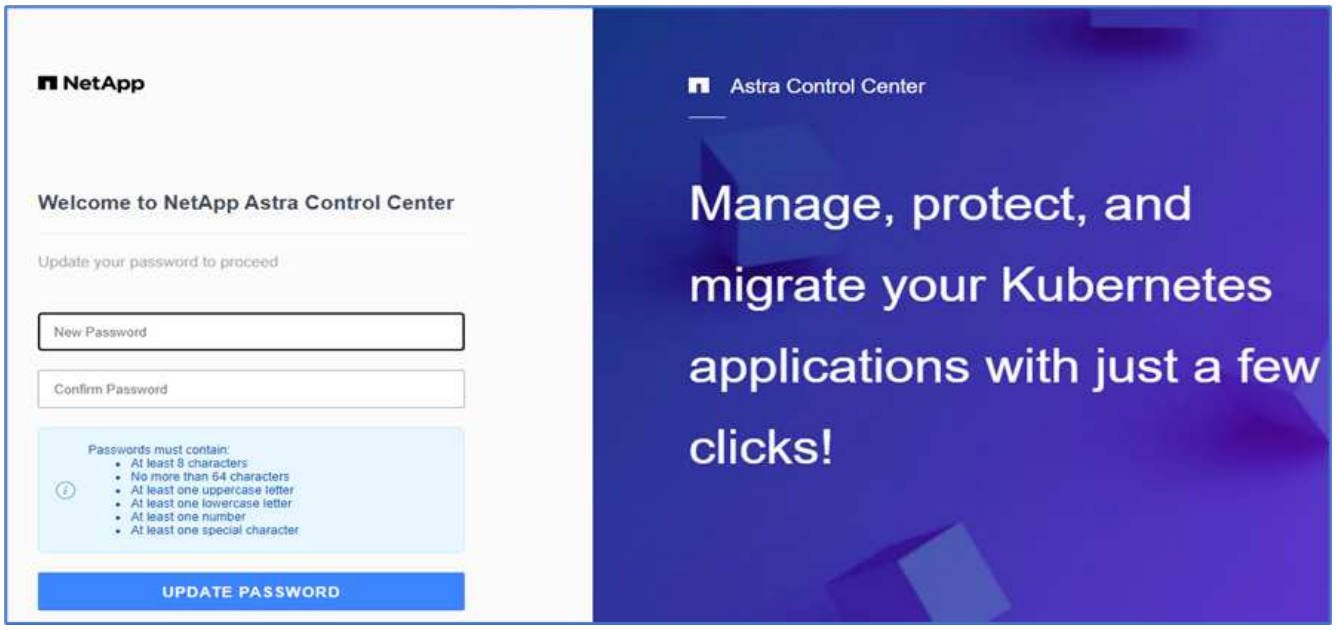
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. Em um navegador, navegue até o URL usando o FQDN fornecido.
22. Faça login usando o nome de usuário padrão, que é o endereço de e-mail fornecido durante a instalação e a senha de uso único ACC-[UUID].



Se você digitar uma senha incorreta três vezes, a conta de administrador será bloqueada por 15 minutos.

23. Altere a palavra-passe e prossiga.

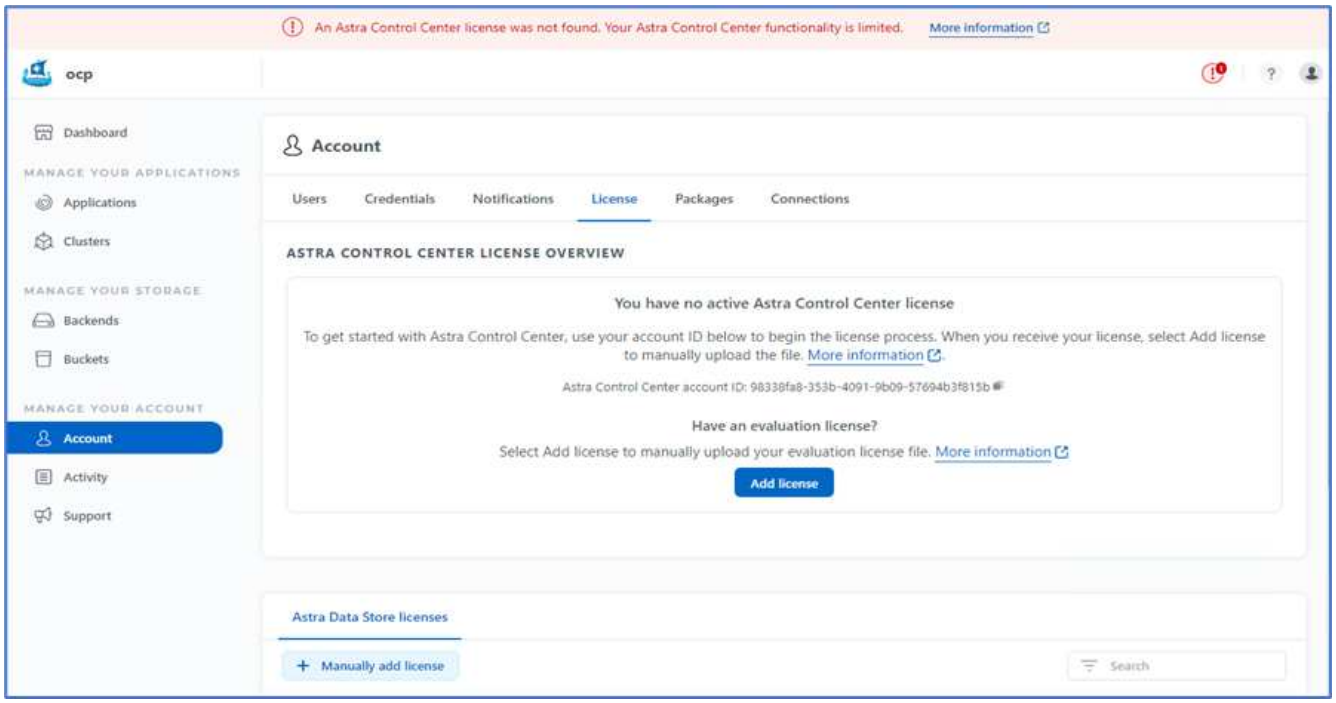


Para obter mais informações sobre a instalação do Astra Control Center, consulte a "Visão geral da instalação do Astra Control Center" página.

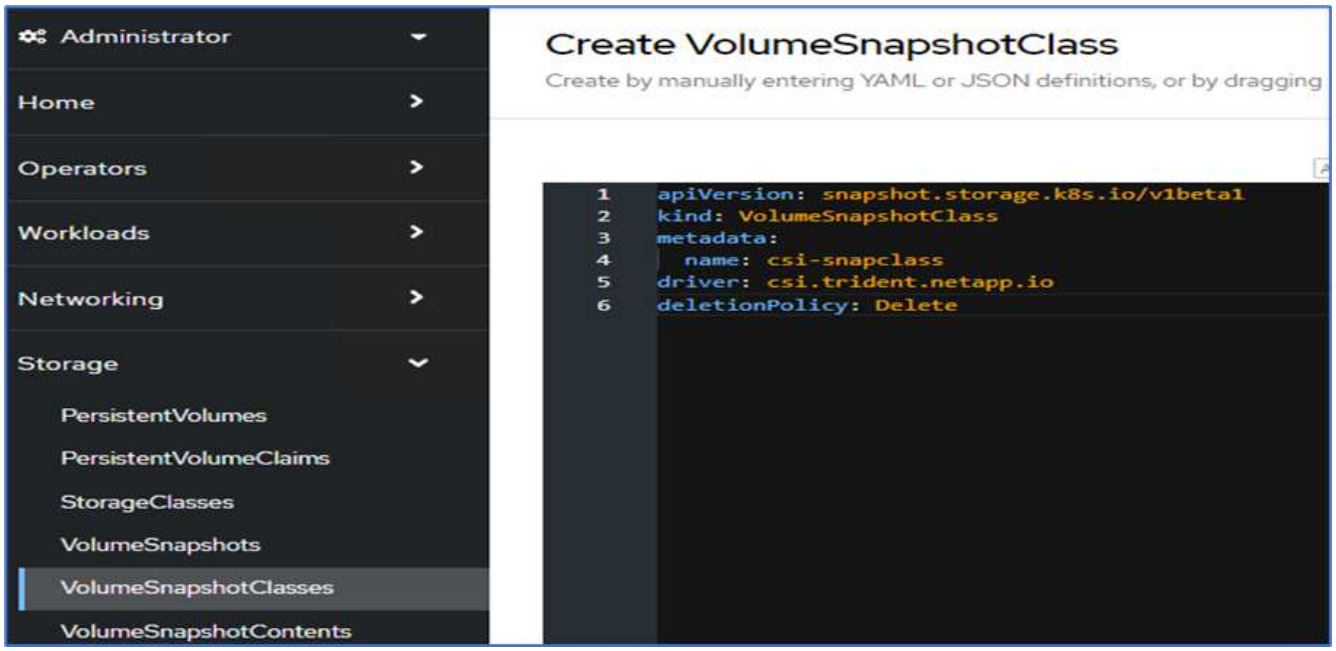
Configure o Astra Control Center

Depois de instalar o Astra Control Center, faça login na IU, carregue a licença, adicione clusters, gerencie o storage e adicione buckets.

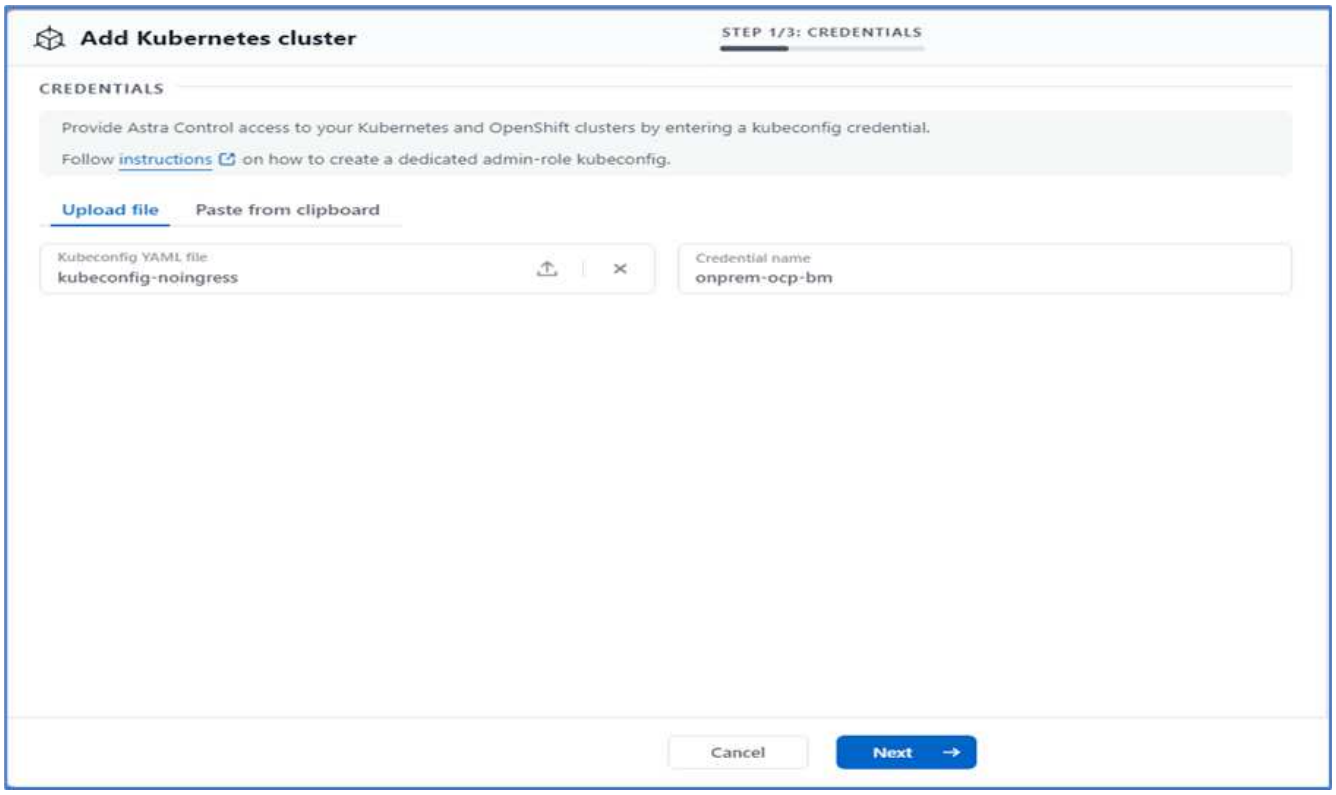
1. Na página inicial em conta, vá para a guia Licença e selecione Adicionar Licença para carregar a licença Astra.



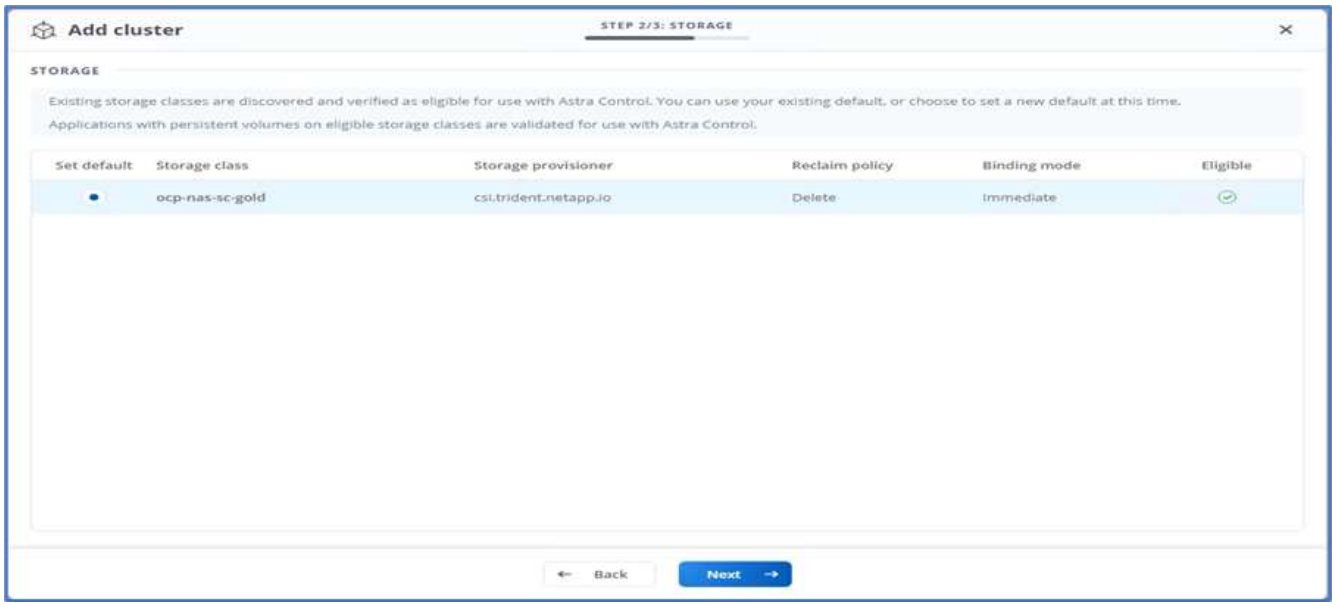
2. Antes de adicionar o cluster OpenShift, crie uma classe de snapshot volume Astra Trident a partir do console da Web OpenShift. A classe volume snapshot é configurada com `csi.trident.netapp.io` o driver.



3. Para adicionar o cluster do Kubernetes, vá para clusters na página inicial e clique em Adicionar cluster do Kubernetes. Em seguida, faça o upload do `kubeconfig` arquivo para o cluster e forneça um nome de credencial. Clique em seguinte.



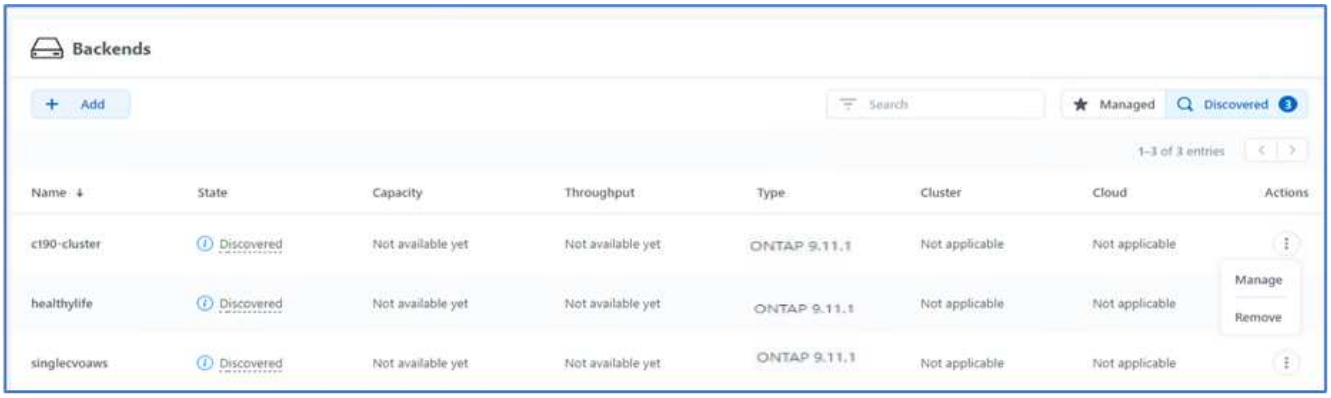
4. As classes de armazenamento existentes são descobertas automaticamente. Selecione a classe de armazenamento padrão, clique em Avançar e clique em Adicionar cluster.



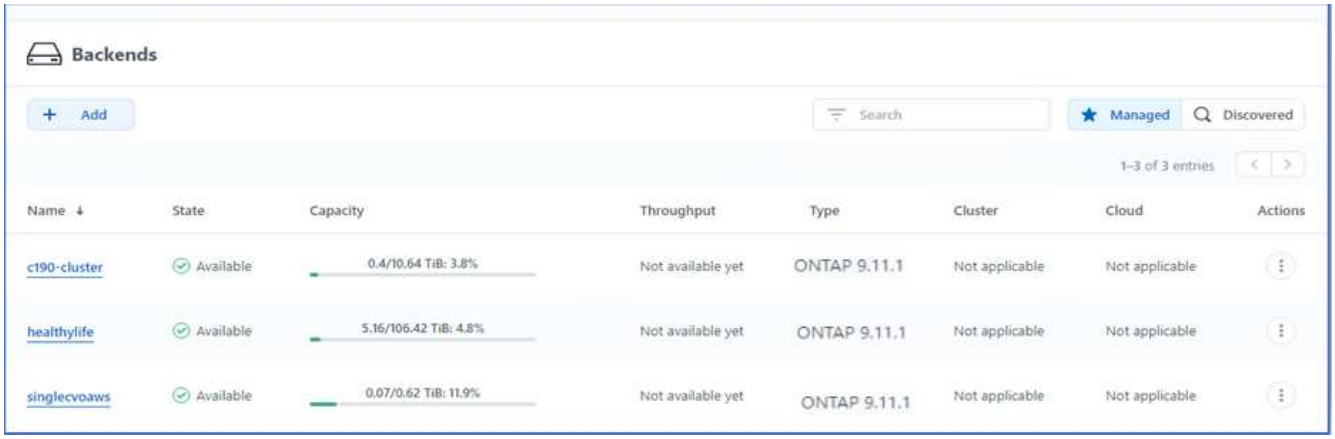
5. O cluster é adicionado em poucos minutos. Para adicionar clusters adicionais do OpenShift Container Platform, repita as etapas 1 a 4.

> Para adicionar um ambiente operacional OpenShift adicional como um recurso de computação gerenciado, verifique se o Astra Trident "Objetos VolumeSnapshotClass" está definido.

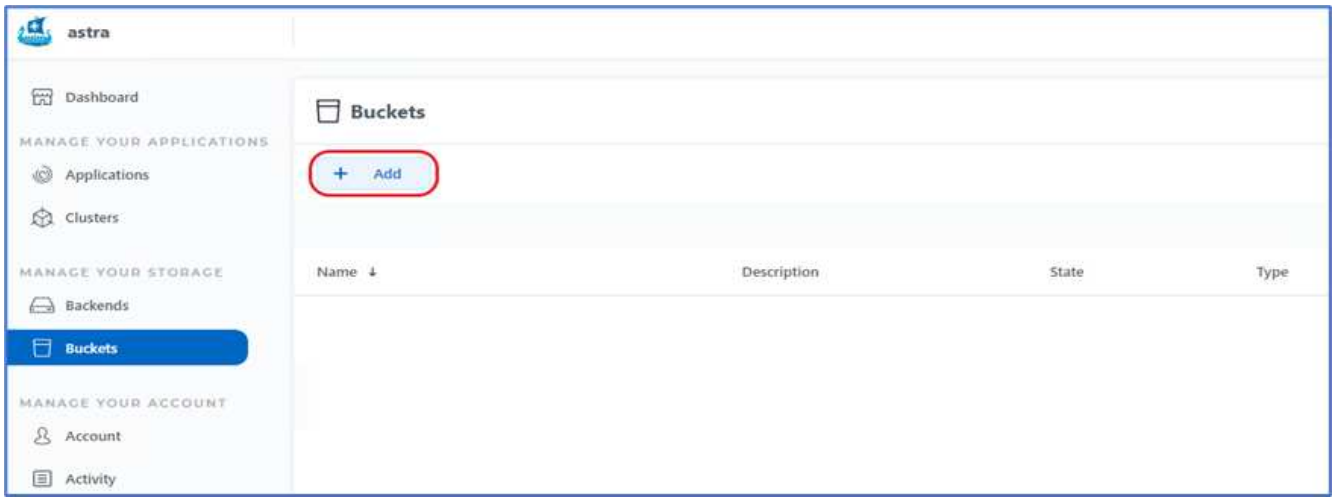
6. Para gerenciar o armazenamento, vá para backends, clique nos três pontos em ações contra o back-end que você gostaria de gerenciar. Clique em Gerenciar.



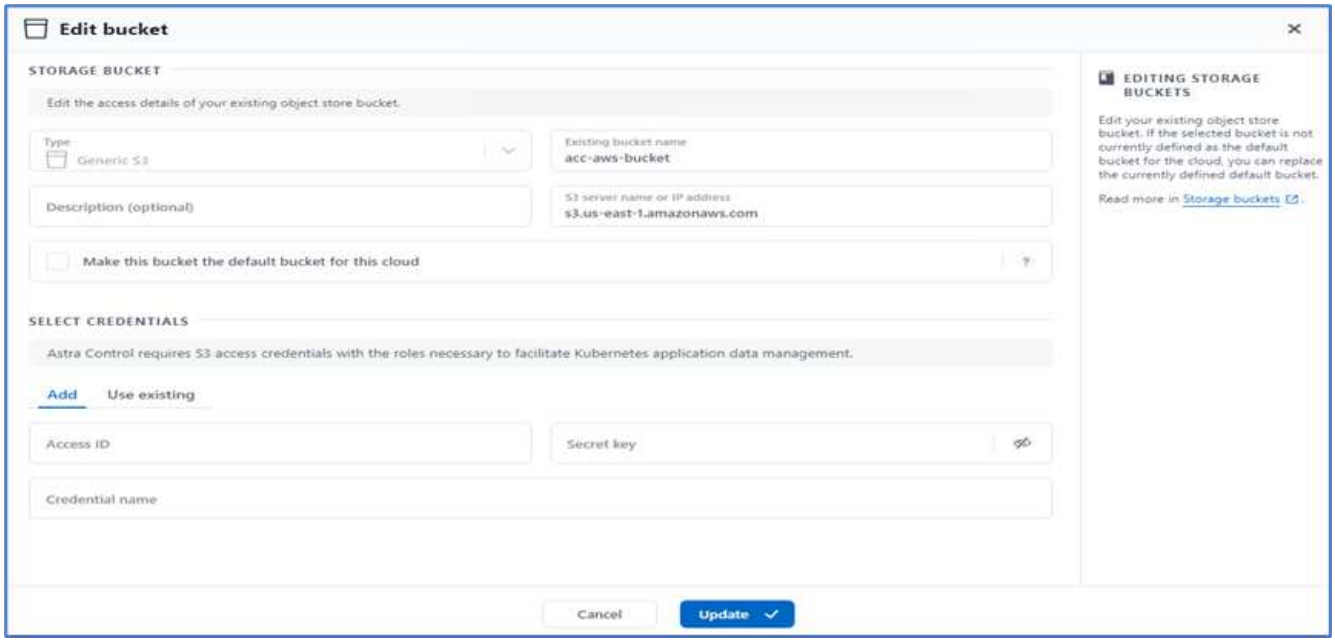
7. Forneça as credenciais do ONTAP e clique em Avançar. Revise as informações e clique em gerenciado. Os backends devem se parecer com o exemplo a seguir.



8. Para adicionar um bucket ao Astra Control, selecione baldes e clique em Adicionar.

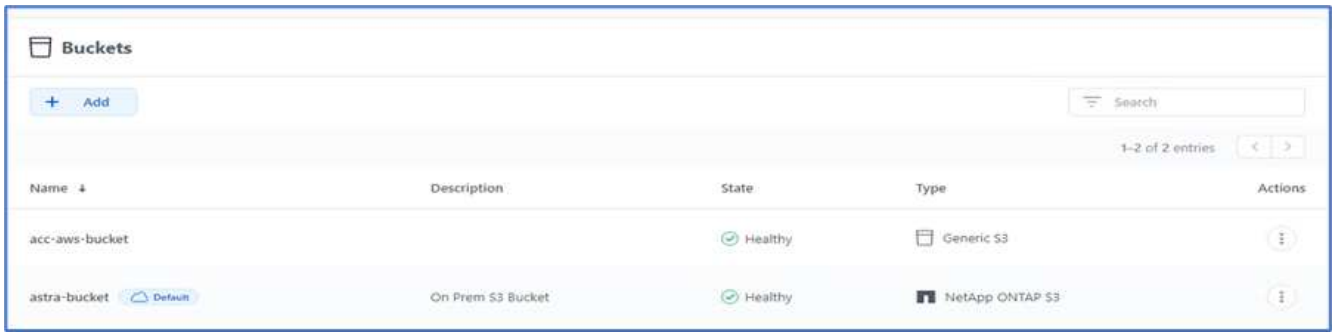


9. Selecione o tipo de bucket e forneça o nome do bucket, o nome do servidor S3 ou o endereço IP e a credencial S3. Clique em Atualizar.



Nessa solução, os buckets do AWS S3 e do ONTAP S3 são usados. Você também pode usar o StorageGRID.

O estado Bucket deve estar saudável.



Como parte do Registro de cluster do Kubernetes no Astra Control Center para gerenciamento de dados com reconhecimento de aplicações, o Astra Control cria automaticamente associações de funções e um namespace de monitoramento NetApp para coletar métricas e logs dos pods da aplicação e dos nós de trabalho. Faça de uma das classes de armazenamento baseadas em ONTAP suportadas o padrão.

Depois do "Adicionar um cluster ao gerenciamento do Astra Control", você poderá instalar aplicações no cluster (fora do Astra Control) e, em seguida, ir para a página aplicações no Astra Control para gerenciar as aplicações e seus recursos. Para obter mais informações sobre como gerenciar aplicações com o Astra, consulte o "Requisitos de gerenciamento de aplicativos".

"Próximo: Visão geral da validação da solução."

Validação da solução

Visão geral

"Anterior: Instalação do Astra Control Center no OpenShift Container Platform."

Nesta seção, revisitamos a solução com alguns casos de uso:

- Restaurar um aplicativo com estado de um backup remoto para outro cluster OpenShift em execução na nuvem.
- Restaurando um aplicativo com estado para o mesmo namespace no cluster OpenShift.
- Mobilidade de aplicativos por clonagem de um sistema FlexPod (OpenShift Container Platform bare metal) para outro sistema FlexPod (OpenShift Container Platform no VMware).

Notavelmente, apenas alguns casos de uso são validados nesta solução. Essa validação não representa, de forma alguma, toda a funcionalidade do Astra Control Center.

"Próximo: Recuperação de aplicativos com backups remotos."

Recuperação de aplicativos com backups remotos

"Anterior: Visão geral da validação da solução."

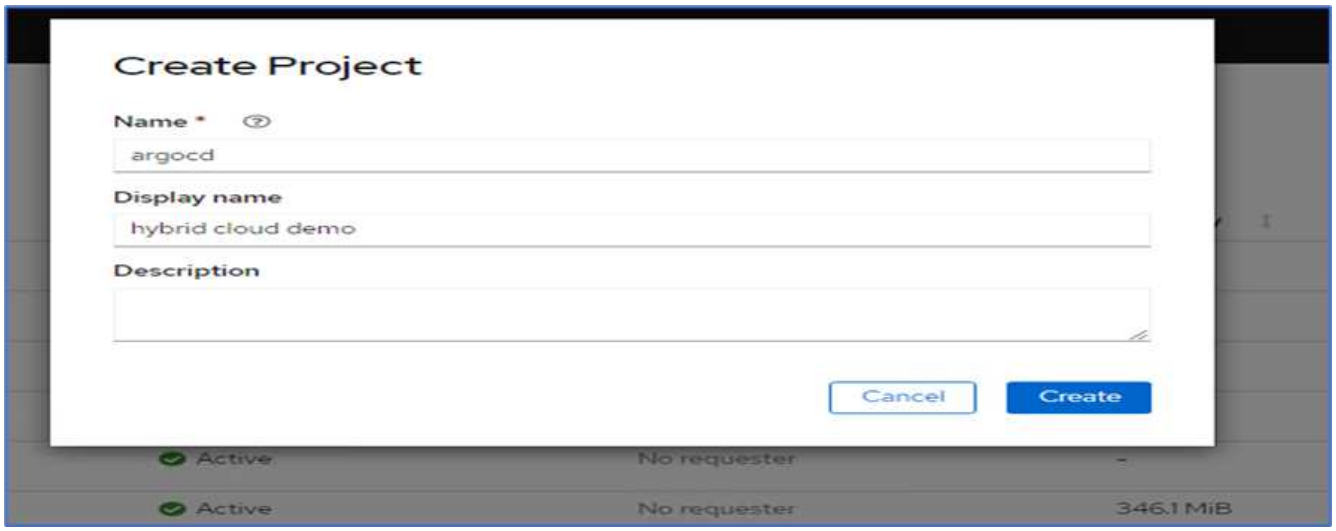
Com o Astra, você pode fazer um backup completo consistente com aplicações que

pode ser usado para restaurar sua aplicação com os dados em um cluster Kubernetes diferente executado em um data center no local ou em uma nuvem pública.

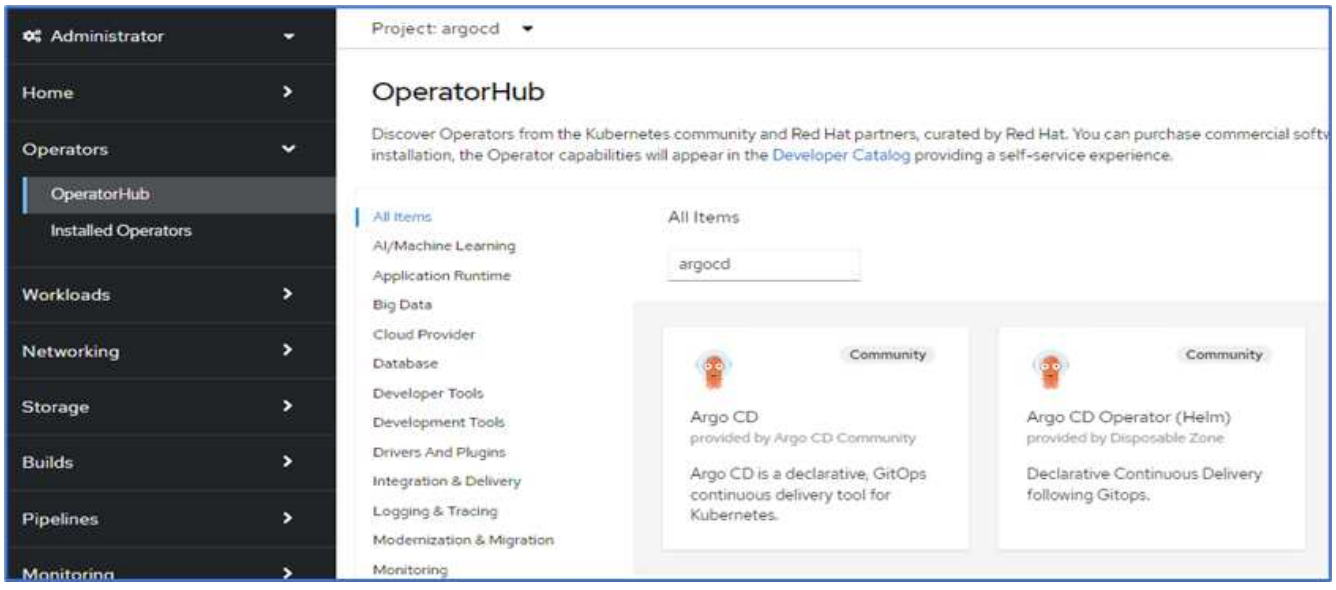
Para validar uma recuperação de aplicativos bem-sucedida, simule uma falha no local de um aplicativo executado no sistema FlexPod e restaure-o para um cluster K8s executado na nuvem usando um backup remoto.

O aplicativo de exemplo é um aplicativo de lista de preços que usa MySQL para o banco de dados. Para automatizar a implantação, usamos a "CD ARGO" ferramenta. O ARGO CD é uma ferramenta declarativa de entrega contínua GitOps para Kubernetes.

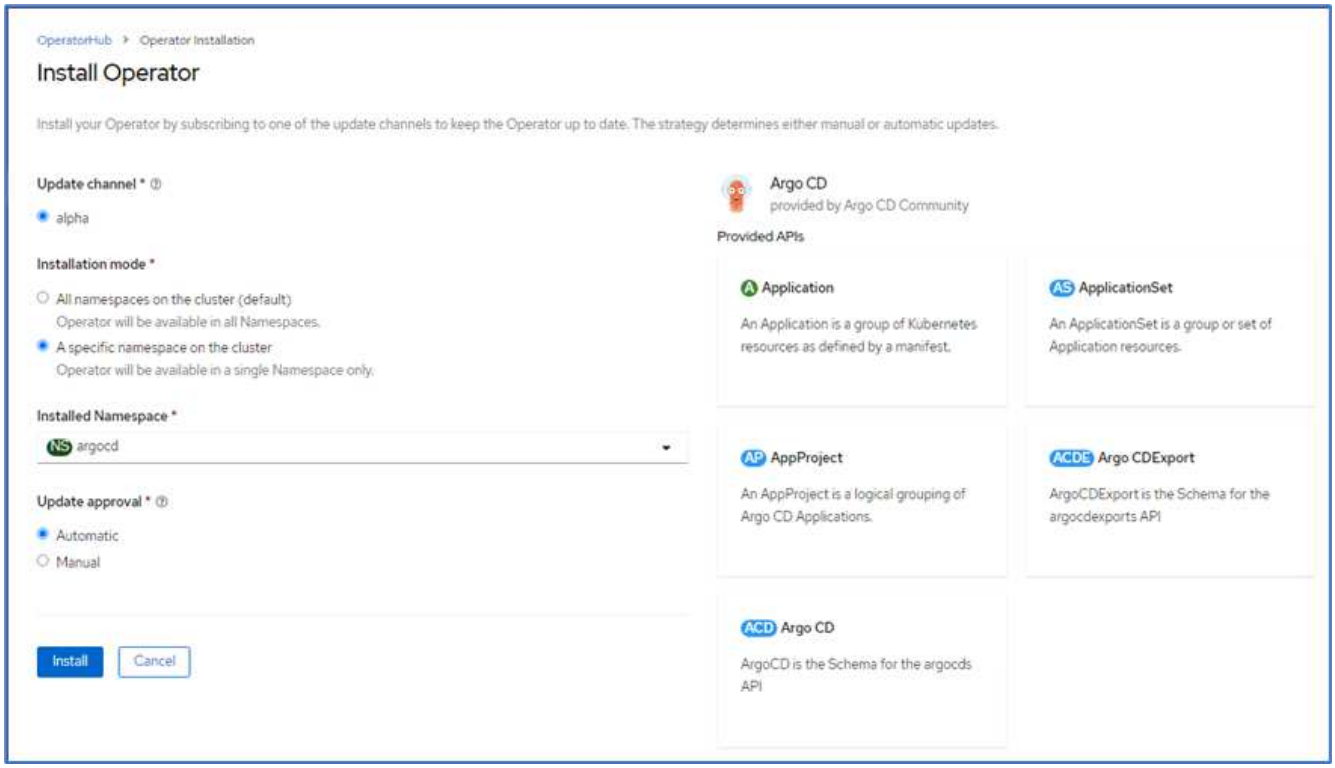
1. Faça login no cluster OpenShift local e crie um novo projeto com o `argocd` nome .



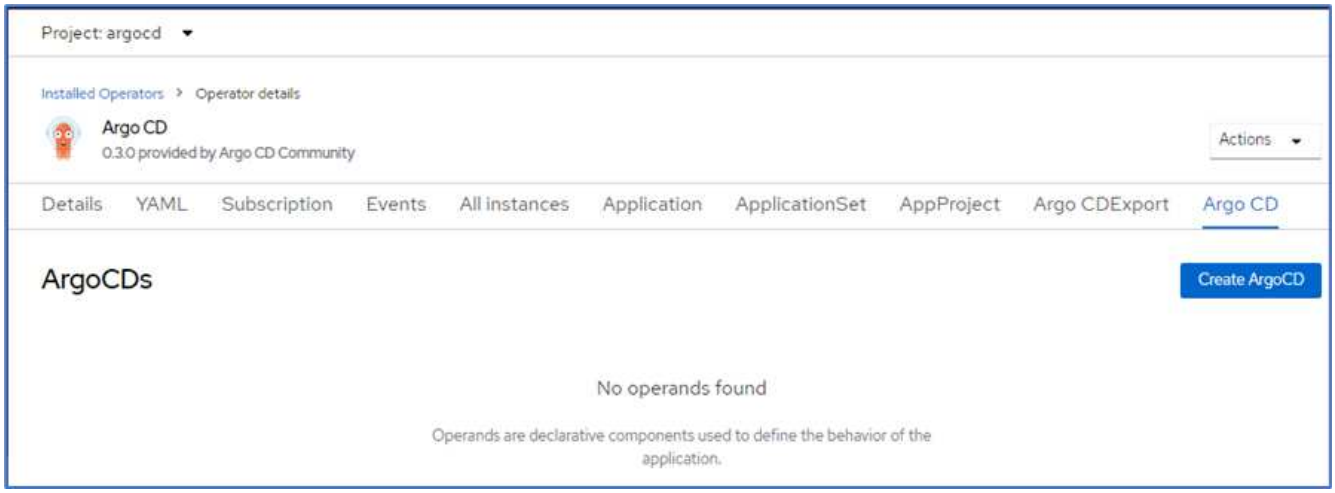
2. No OperatorHub, procure `argocd` e selecione o operador Argo CD.



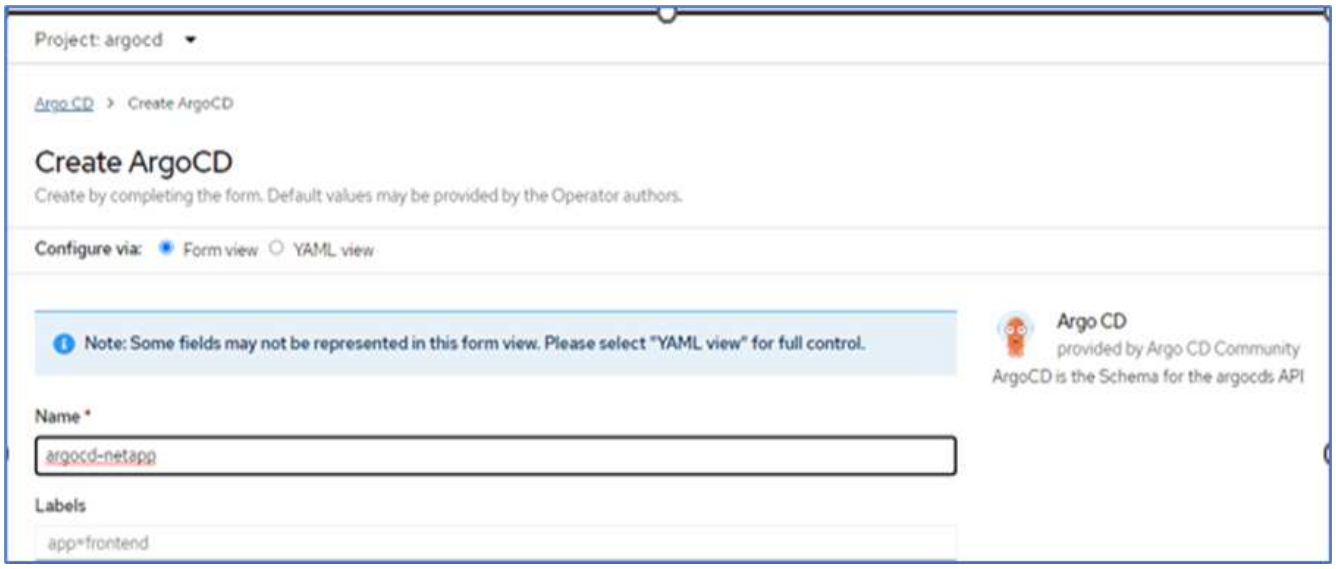
3. Instale o operador no `argocd` namespace.



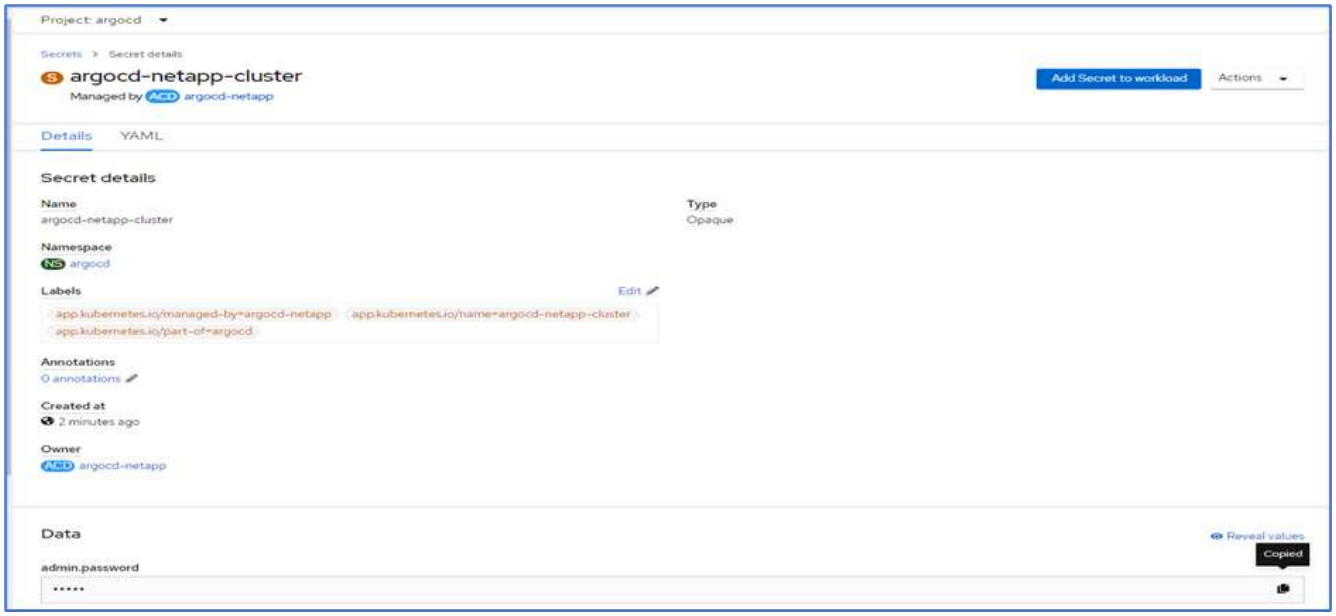
4. Vá para o operador e clique em criar ArgoCD.



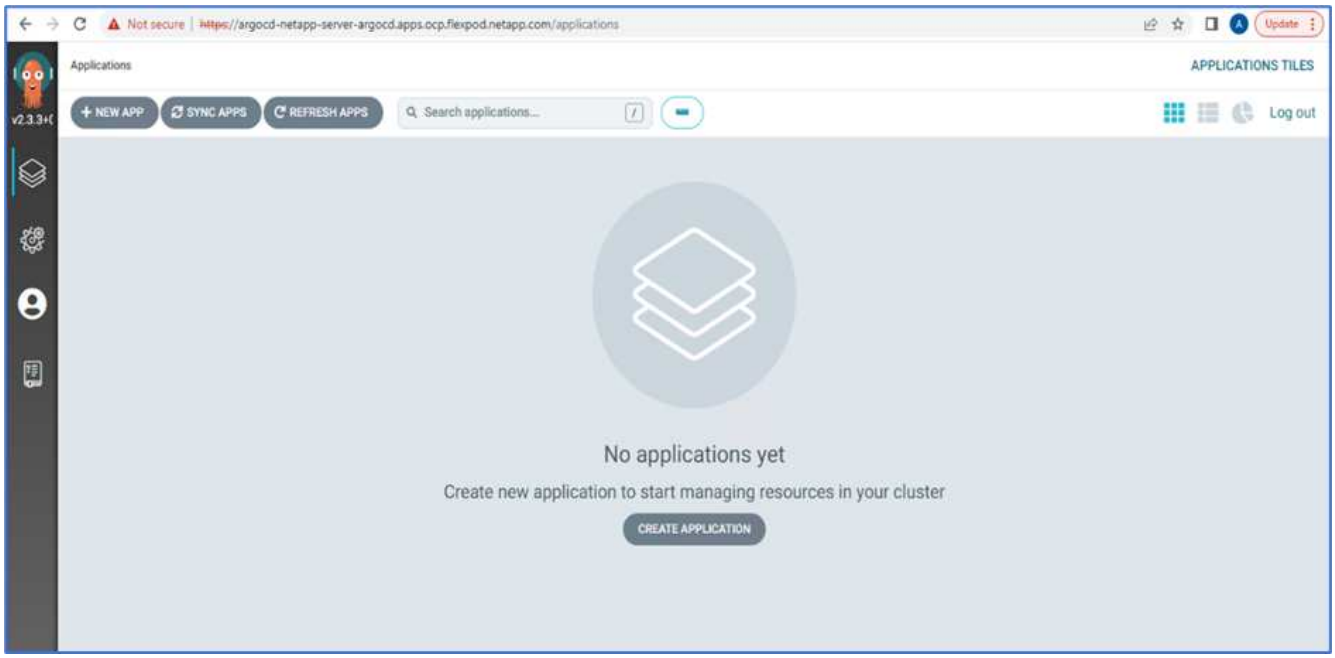
5. Para implantar a instância do CD Argo no `argocd` projeto, forneça um nome e clique em criar.



6. Para iniciar sessão no CD Argo, o utilizador predefinido é admin e a palavra-passe encontra-se num ficheiro secreto com o nome `argocd-netapp-cluster`.



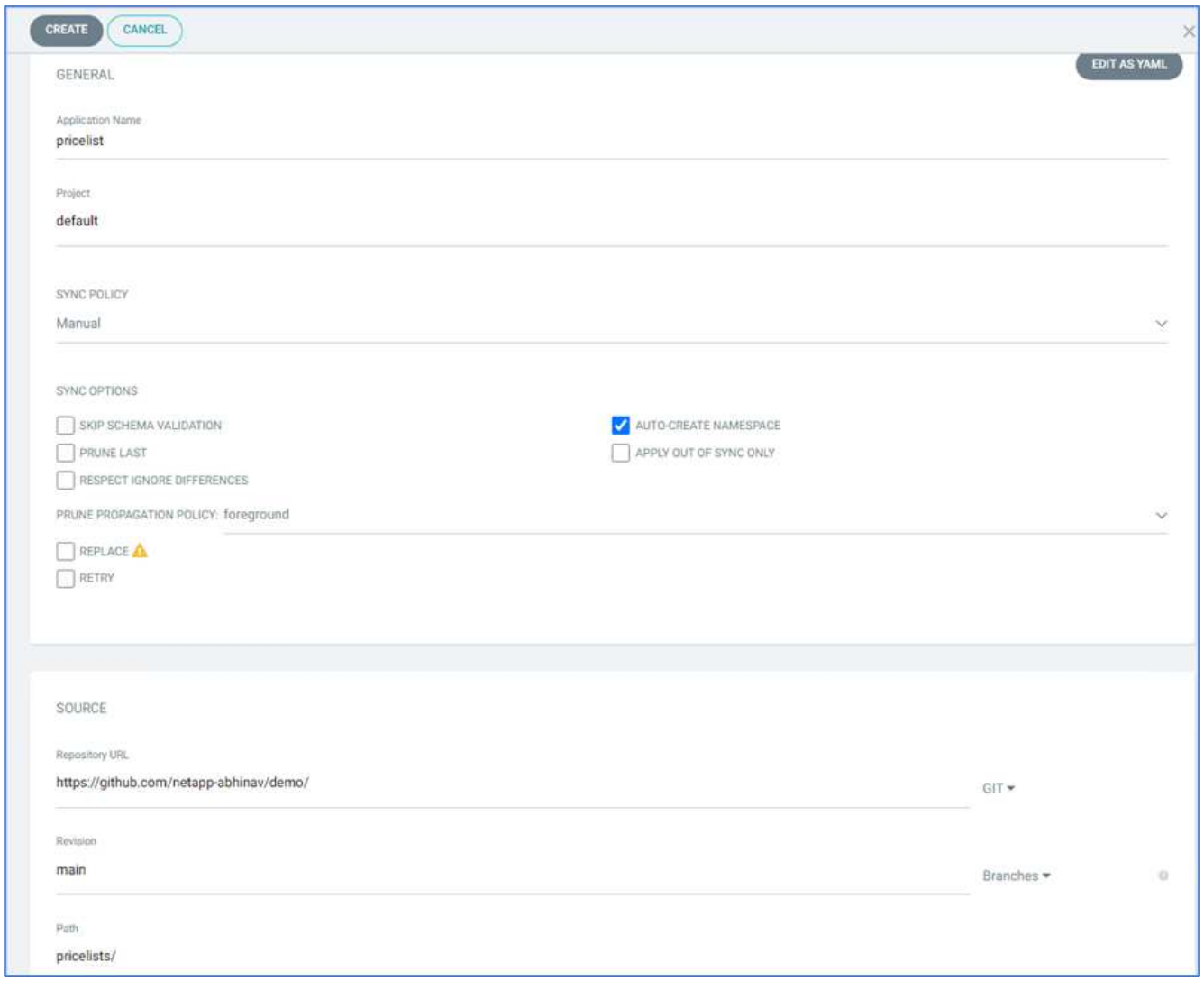
7. No menu lateral, selecione rotas > localização e clique no URL das `argocd` rotas. Introduza o nome de utilizador e a palavra-passe.



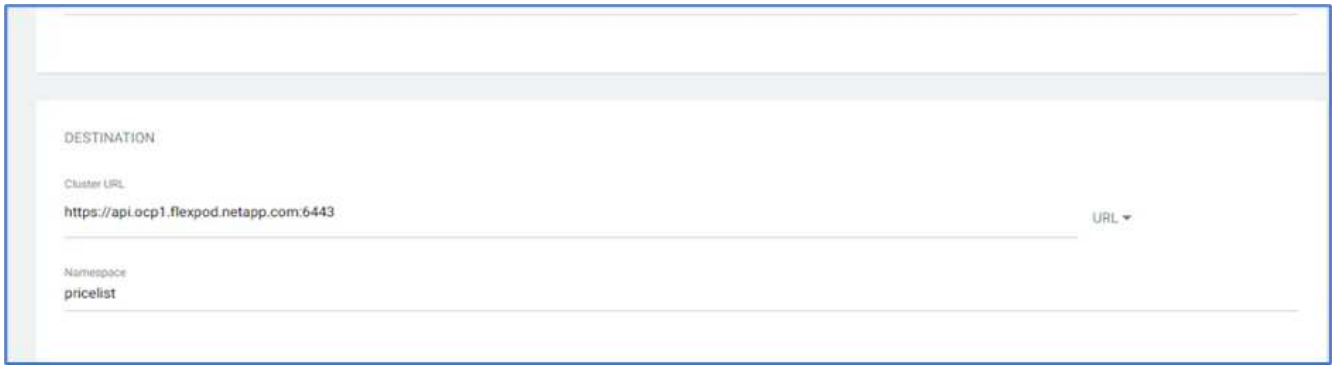
8. Adicione o cluster OpenShift no local ao CD Argo por meio da CLI.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

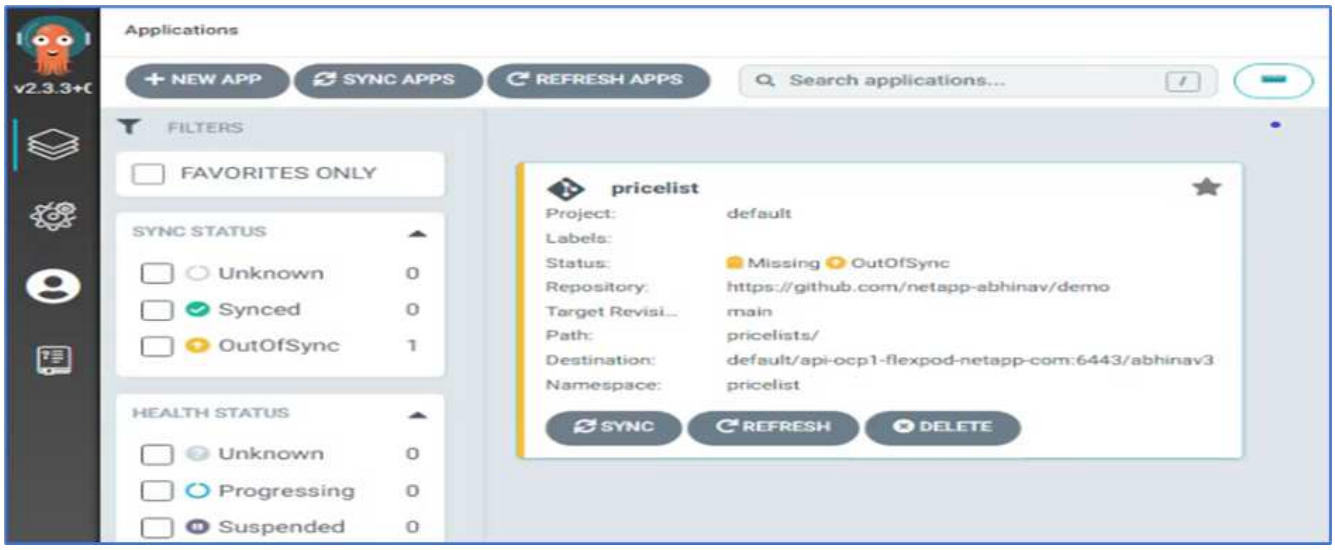
9. Na IU do ArgoCD, clique EM NOVO APLICATIVO e insira os detalhes sobre o nome do aplicativo e o repositório de código.



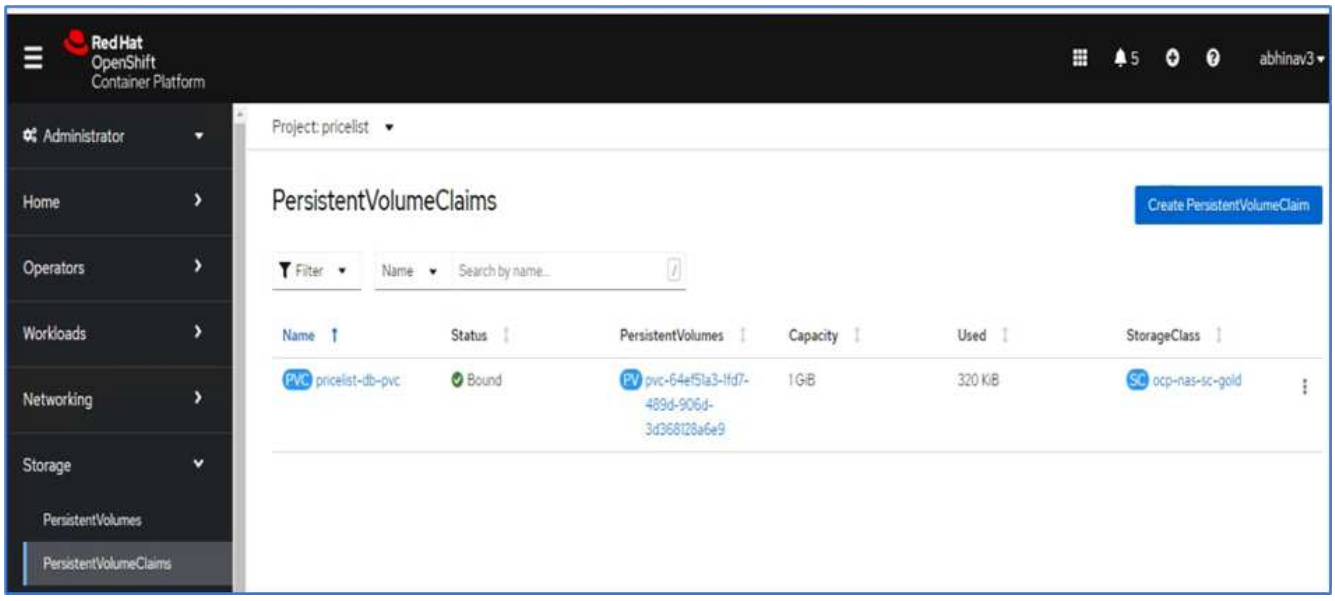
10. Entre no cluster OpenShift onde o aplicativo será implantado junto com o namespace.



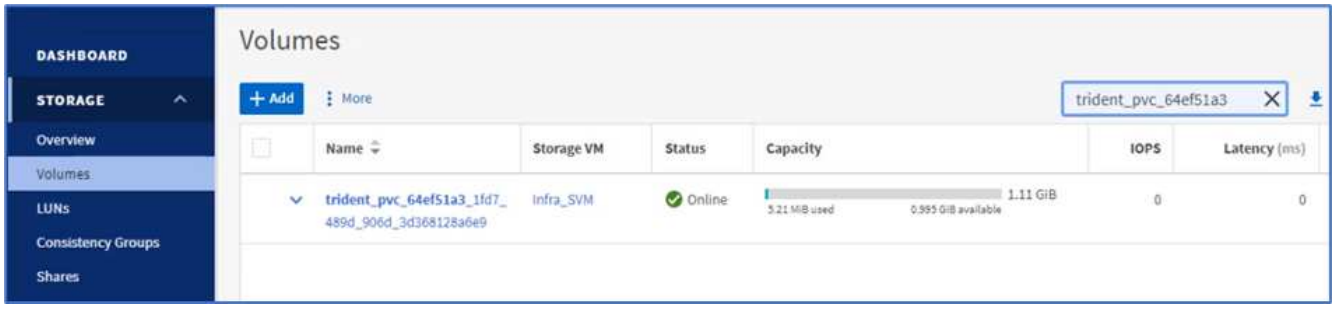
11. Para implantar o aplicativo no cluster OpenShift local, clique EM SYNC.



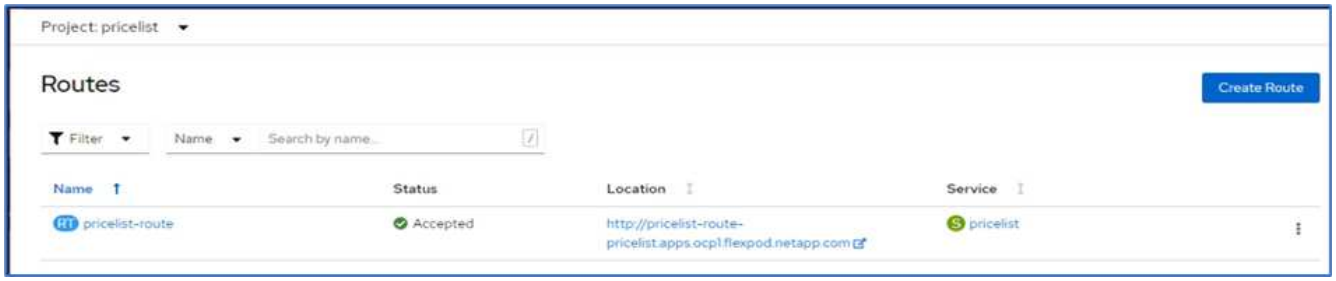
12. No console OpenShift Container Platform, vá para Lista de preços do Projeto e, em armazenamento, verifique o nome e o tamanho do PVC.



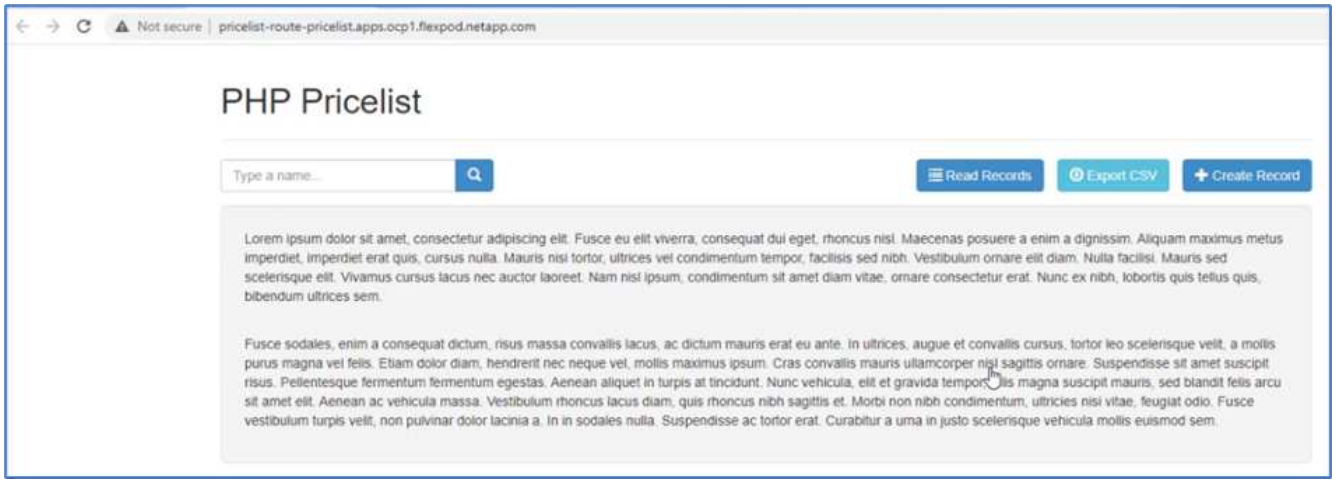
13. Faça login no System Manager e verifique o PVC.



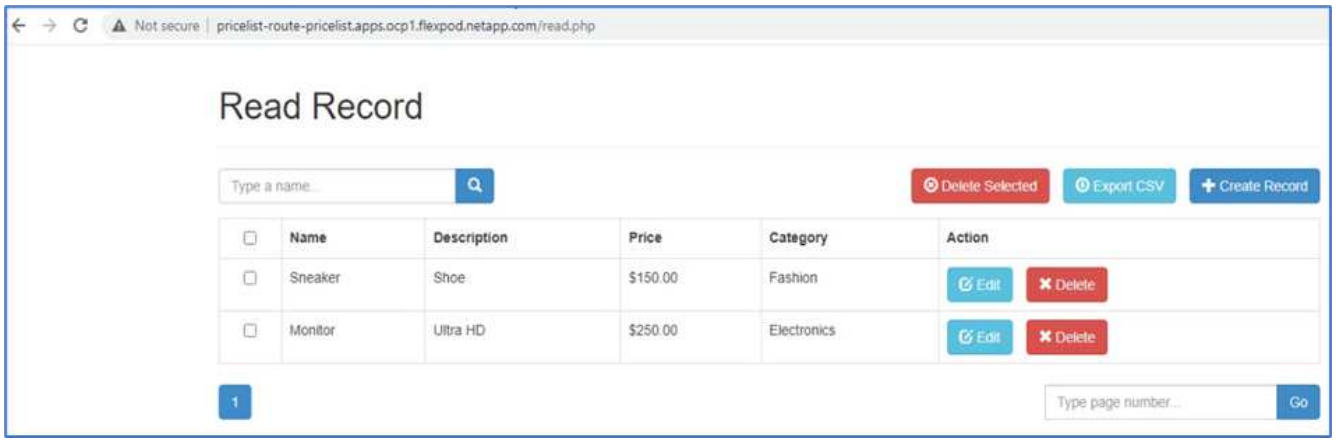
14. Depois que os pods estiverem em execução, selecione rede > rotas no menu lateral e clique no URL em localização.



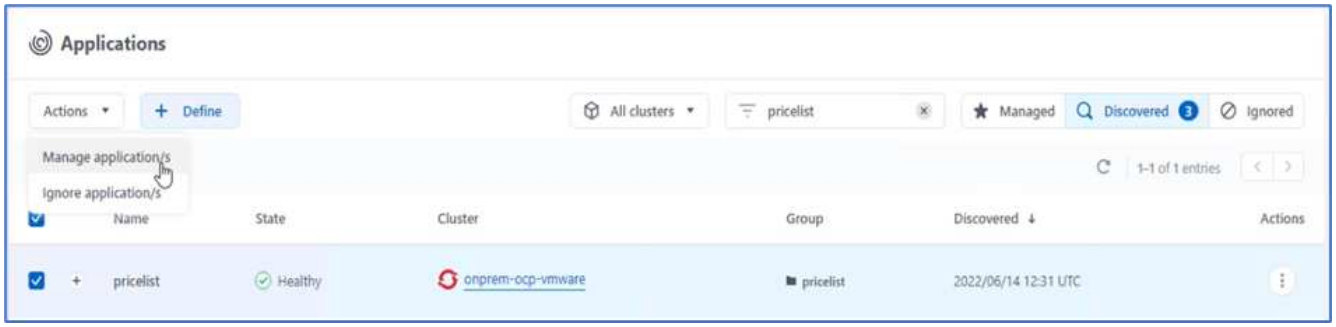
15. A página inicial da aplicação Pricelist é apresentada.



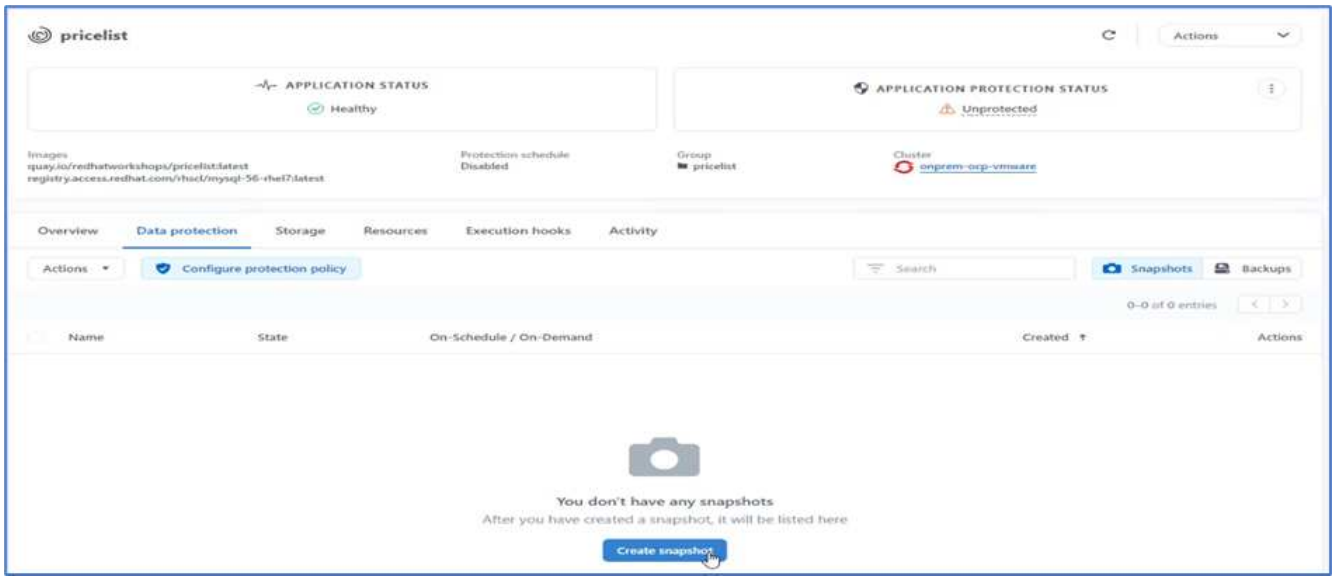
16. Crie alguns Registros na página da Web.



17. O aplicativo foi descoberto no Astra Control Center. Para gerir a aplicação, aceda a aplicações > descobertas, selecione a aplicação Pricelist e clique em gerir aplicações em ações.

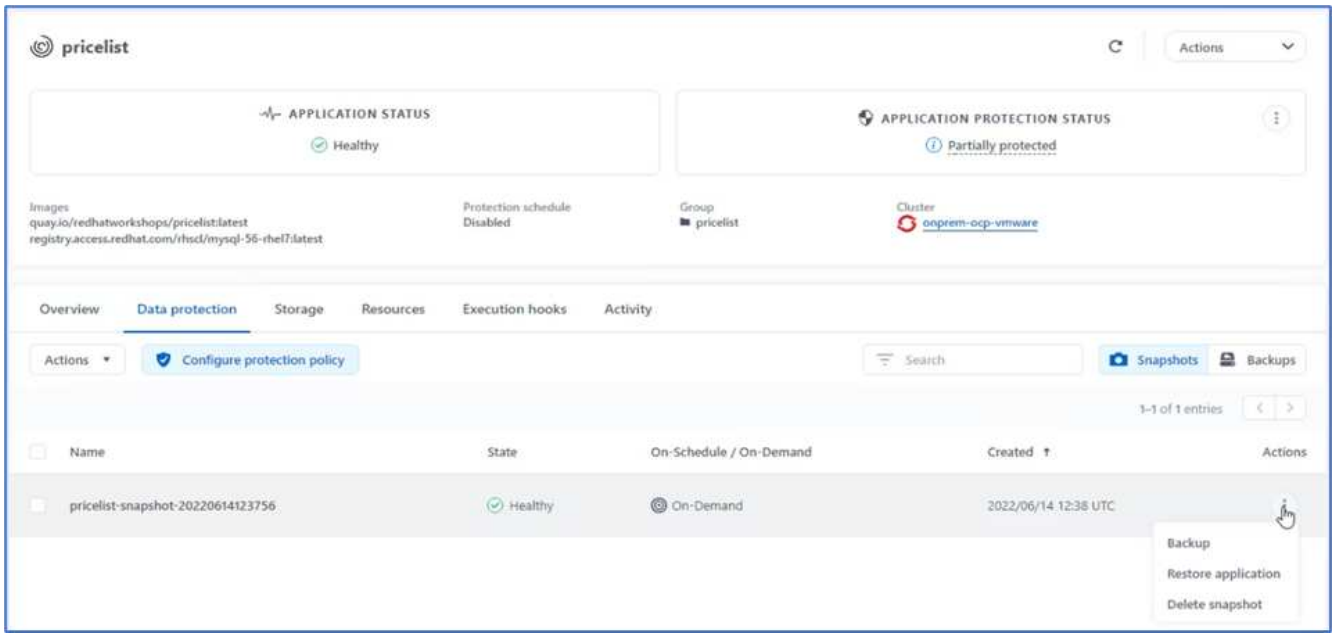


18. Clique no aplicativo Pricelist e selecione proteção de dados. Neste ponto, não deve haver snapshots ou backups. Clique em criar instantâneo para criar um instantâneo sob demanda.

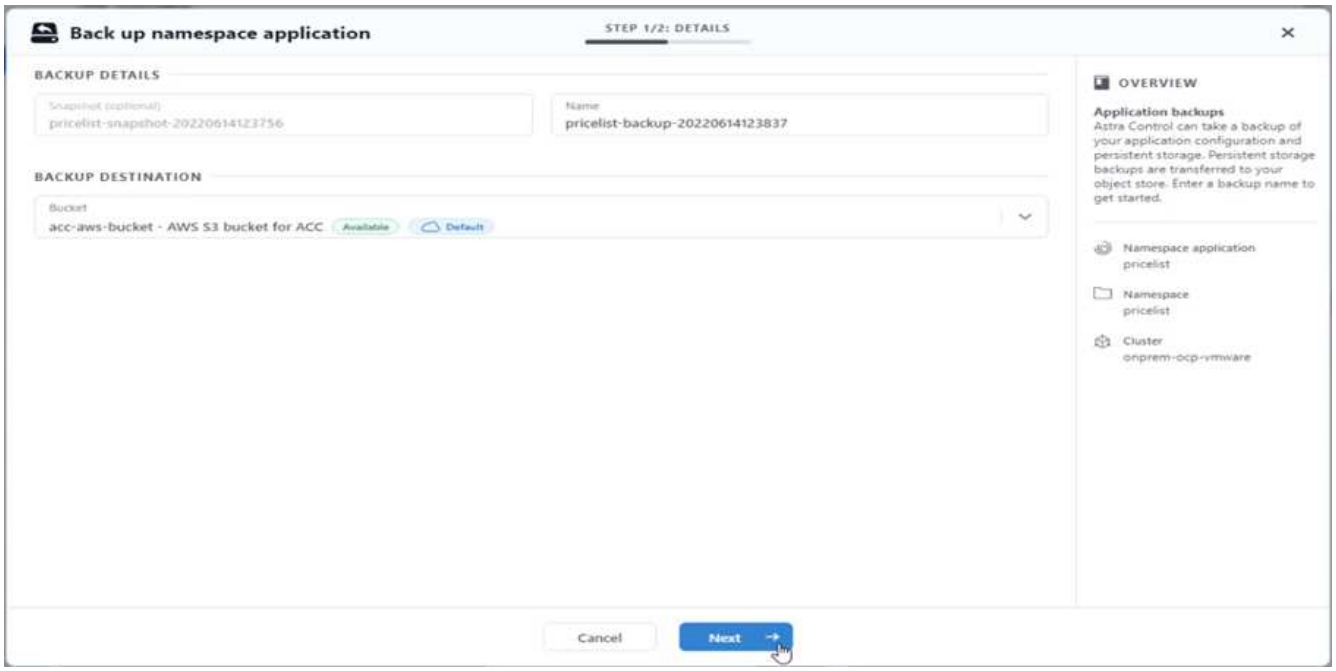


O NetApp Astra Control Center é compatível com backups e snapshots programados sob demanda.

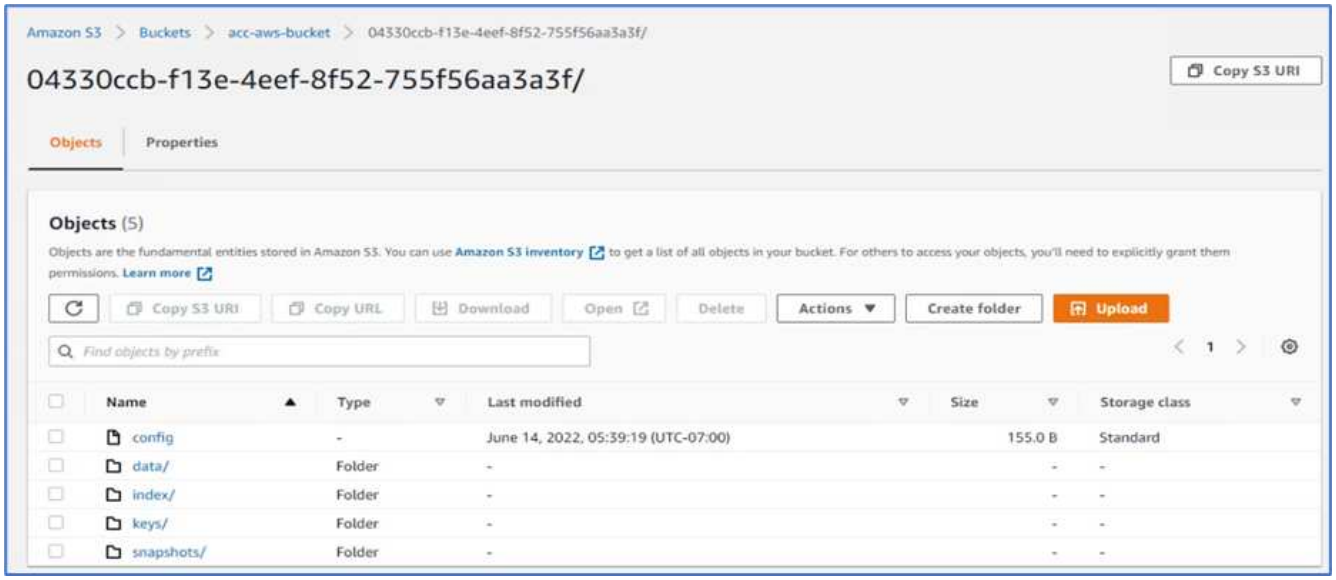
19. Depois que o instantâneo for criado e o Estado estiver saudável, crie um backup remoto usando esse instantâneo. Este backup é armazenado no bucket do S3.



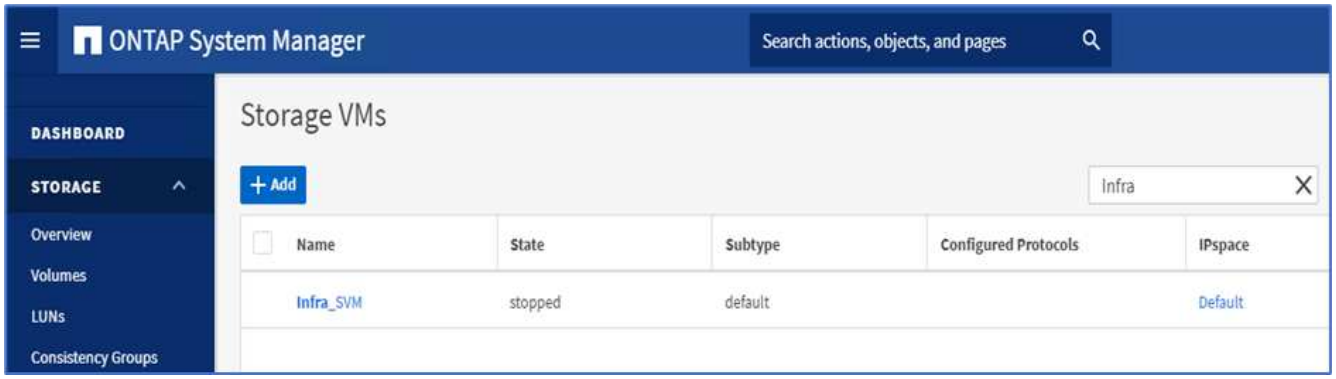
20. Selecione o bucket do AWS S3 e inicie a operação de backup.



21. A operação de backup deve criar uma pasta com vários objetos no bucket do AWS S3.



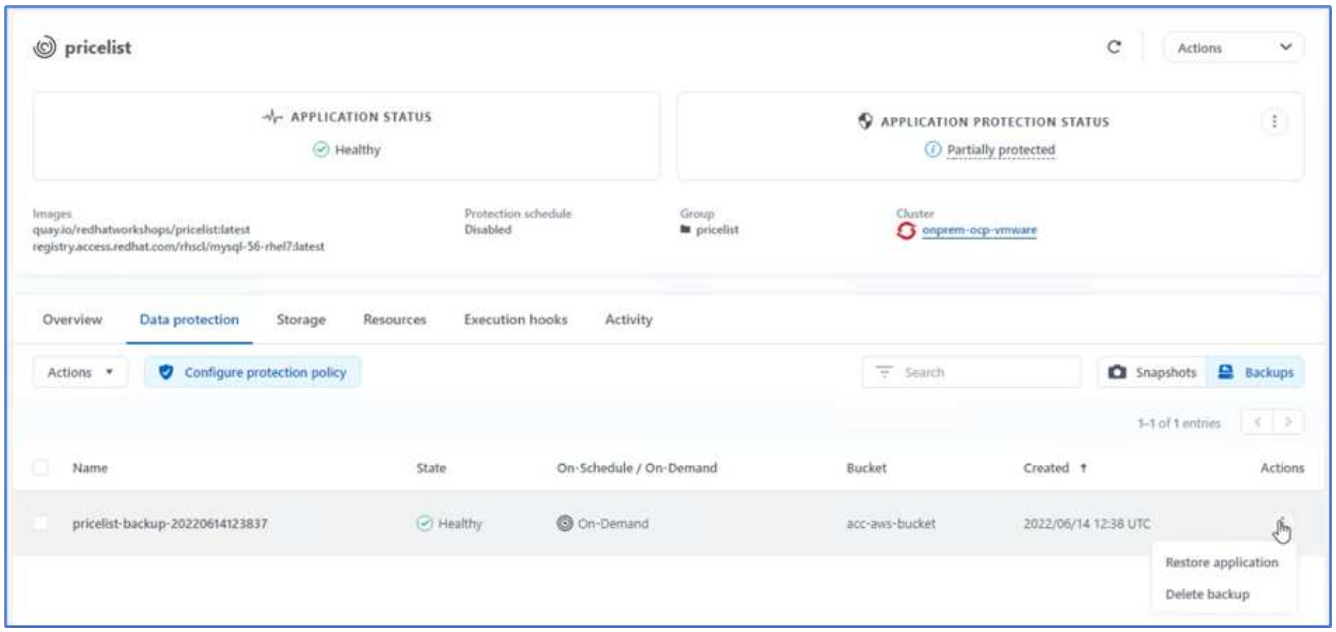
22. Quando o backup remoto estiver concluído, simule um desastre no local parando a máquina virtual de armazenamento (SVM) que hospeda o volume de backup do PV.



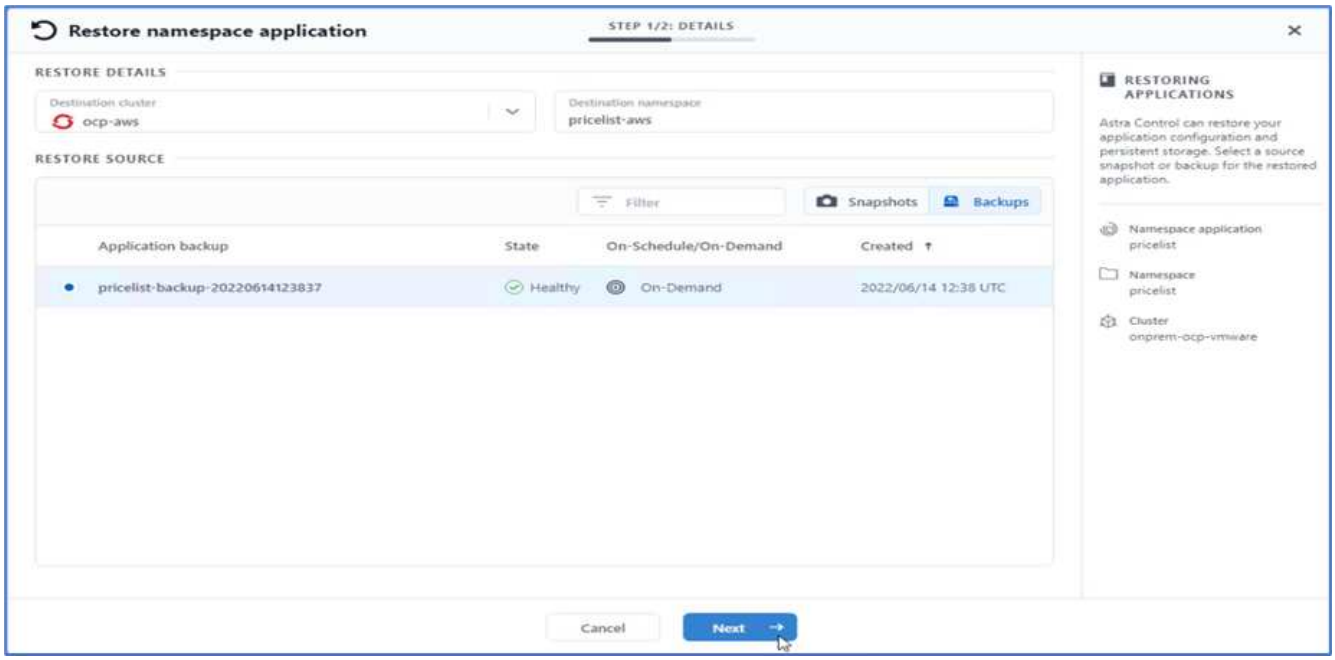
23. Atualize a página da Web para confirmar a interrupção. A página da Web não está disponível.

Como esperado, o site está inativo, então vamos recuperar rapidamente o aplicativo do backup remoto usando o Astra para o cluster OpenShift executado na AWS.

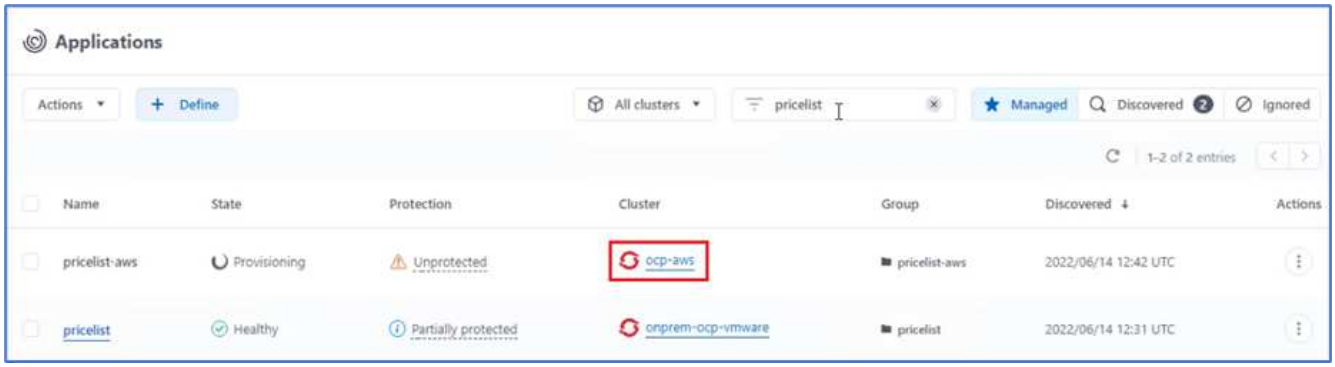
24. No Astra Control Center, clique no aplicativo Pricelist e selecione proteção de dados > backups. Selecione a cópia de segurança e clique em Restaurar aplicação em Ação.



25. `ocp-aws`Selecione como o cluster de destino e dê um nome ao namespace. Clique no backup sob demanda, em Avançar e em Restaurar.

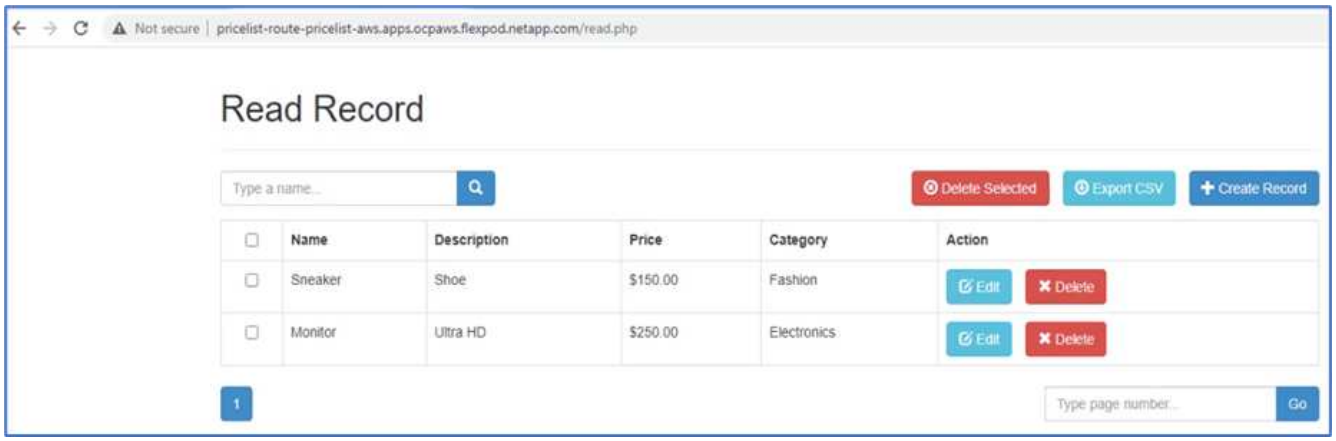


26. Um novo aplicativo com o nome `pricelist-app` é projetado no cluster OpenShift em execução na AWS.



27. Verifique o mesmo no console da Web OpenShift.

28. Depois que todos os pods no `pricelist-aws` projeto estiverem em execução, vá para rotas e clique no URL para iniciar a página da Web.



Esse processo valida que o aplicativo de lista de preços foi restaurado com sucesso e que a integridade dos dados foi mantida no cluster OpenShift executado perfeitamente na AWS com a ajuda do Astra Control Center.

Proteção de dados com cópias Snapshot e mobilidade de aplicações para DevTest

Este caso de uso é composto por duas partes, conforme descrito nas seções a seguir.

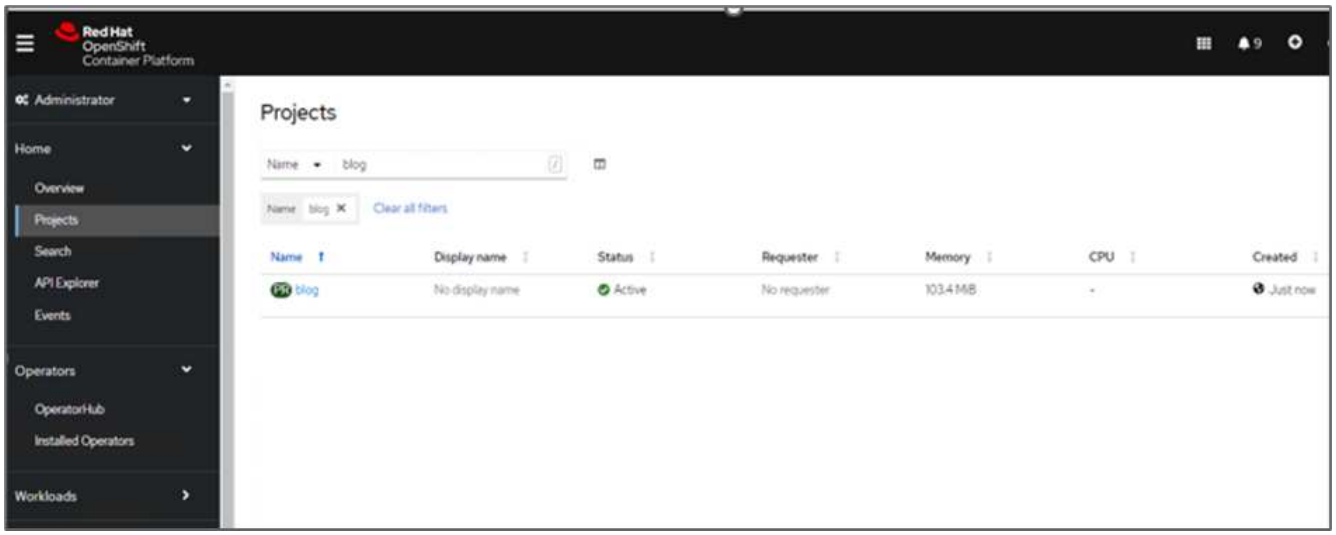
Parte 1

Com o Astra Control Center, você pode tirar snapshots com reconhecimento de aplicações para proteção de dados local. Se você acidentalmente excluir ou corromper seus dados, poderá reverter seus aplicativos e dados associados a um estado em boas condições usando um instantâneo gravado anteriormente.

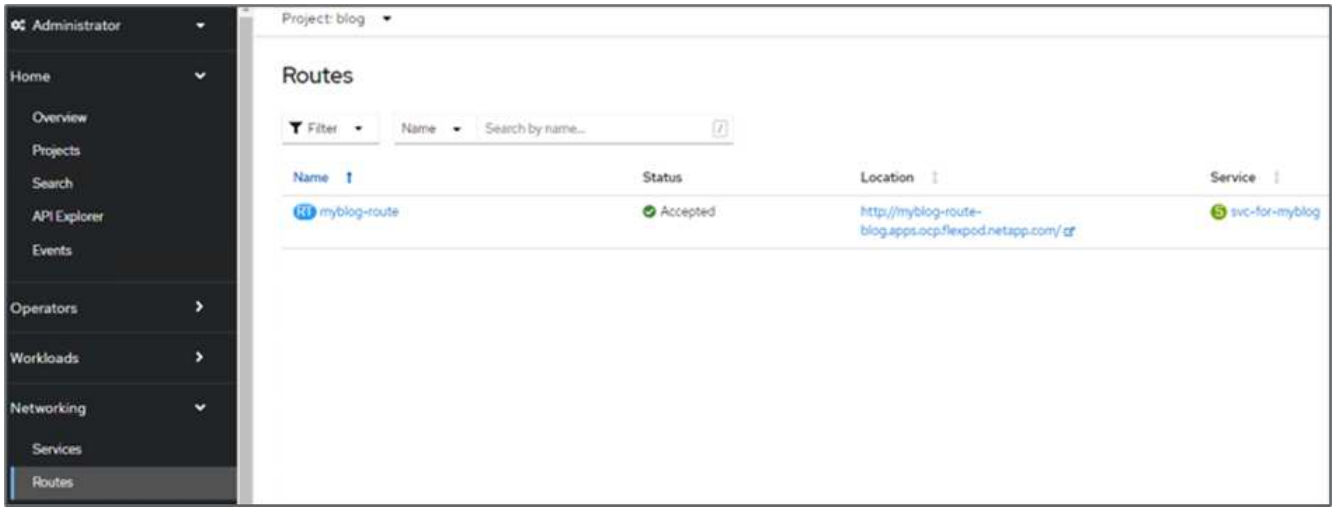
Nesse cenário, uma equipe de desenvolvimento e teste (DevTest) implanta um aplicativo de estado de amostra (site de blog) que é um aplicativo de blog Ghost, adiciona algum conteúdo e atualiza o aplicativo para a versão mais recente disponível. O aplicativo Ghost usa SQLite para o banco de dados. Antes de atualizar a aplicação, um snapshot (sob demanda) é usado no Astra Control Center para proteção de dados. As etapas detalhadas são as seguintes:

1. Implemente o aplicativo de blog de exemplo e sincronize-o a partir do ArgoCD.

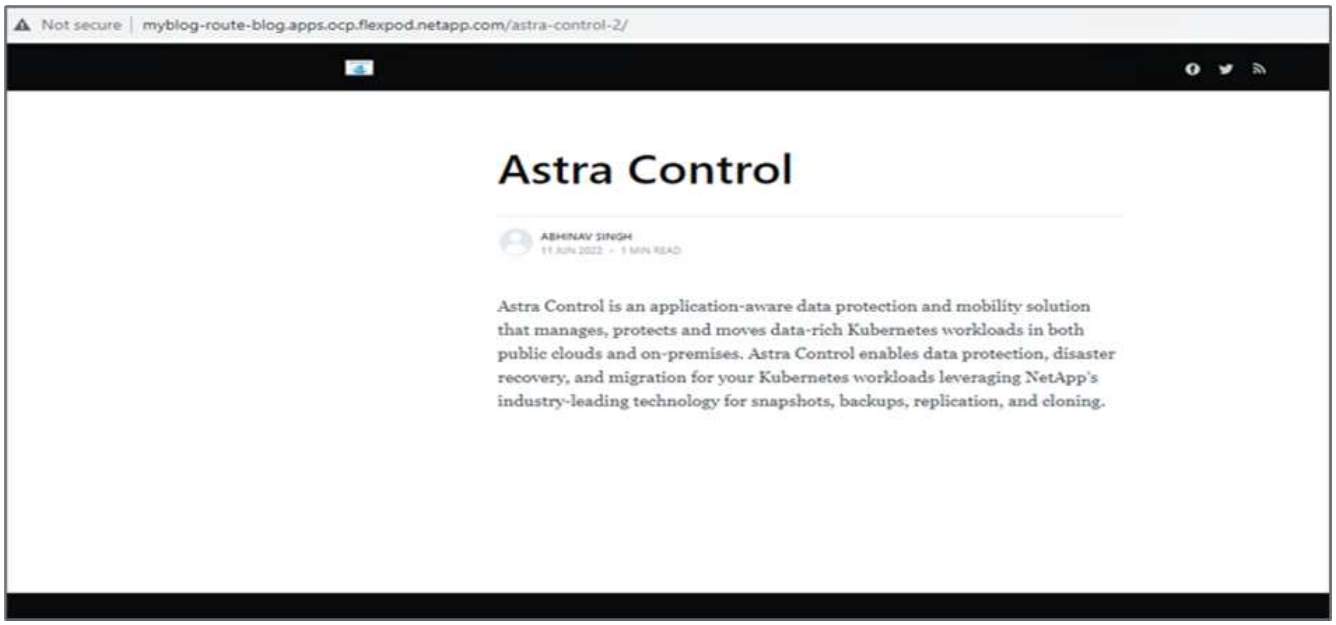
2. Faça login no primeiro cluster do OpenShift, vá para Project e entre em Blog na barra de pesquisa.



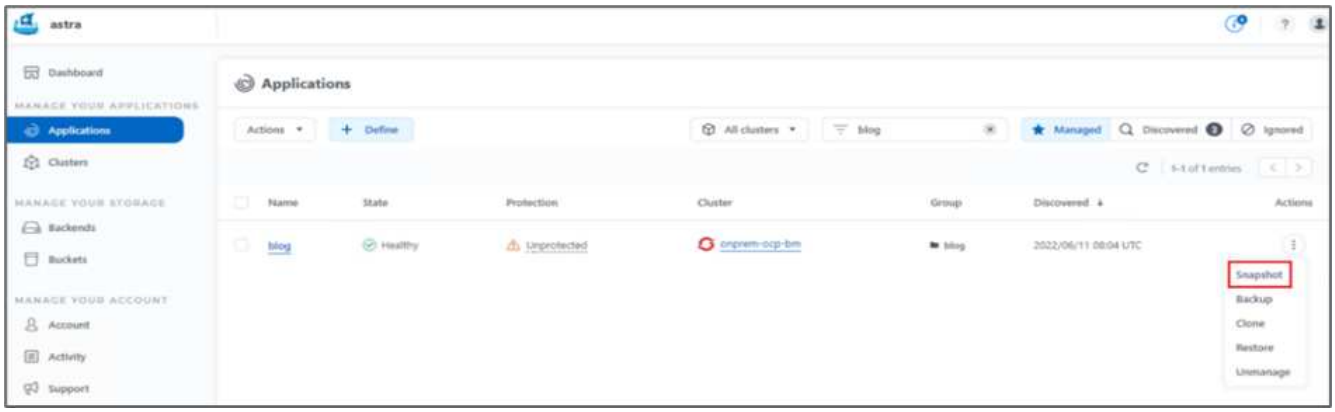
3. No menu lateral, selecione rede > rotas e clique no URL.



4. A página inicial do blog é exibida. Adicione algum conteúdo ao site do blog e publique-o.



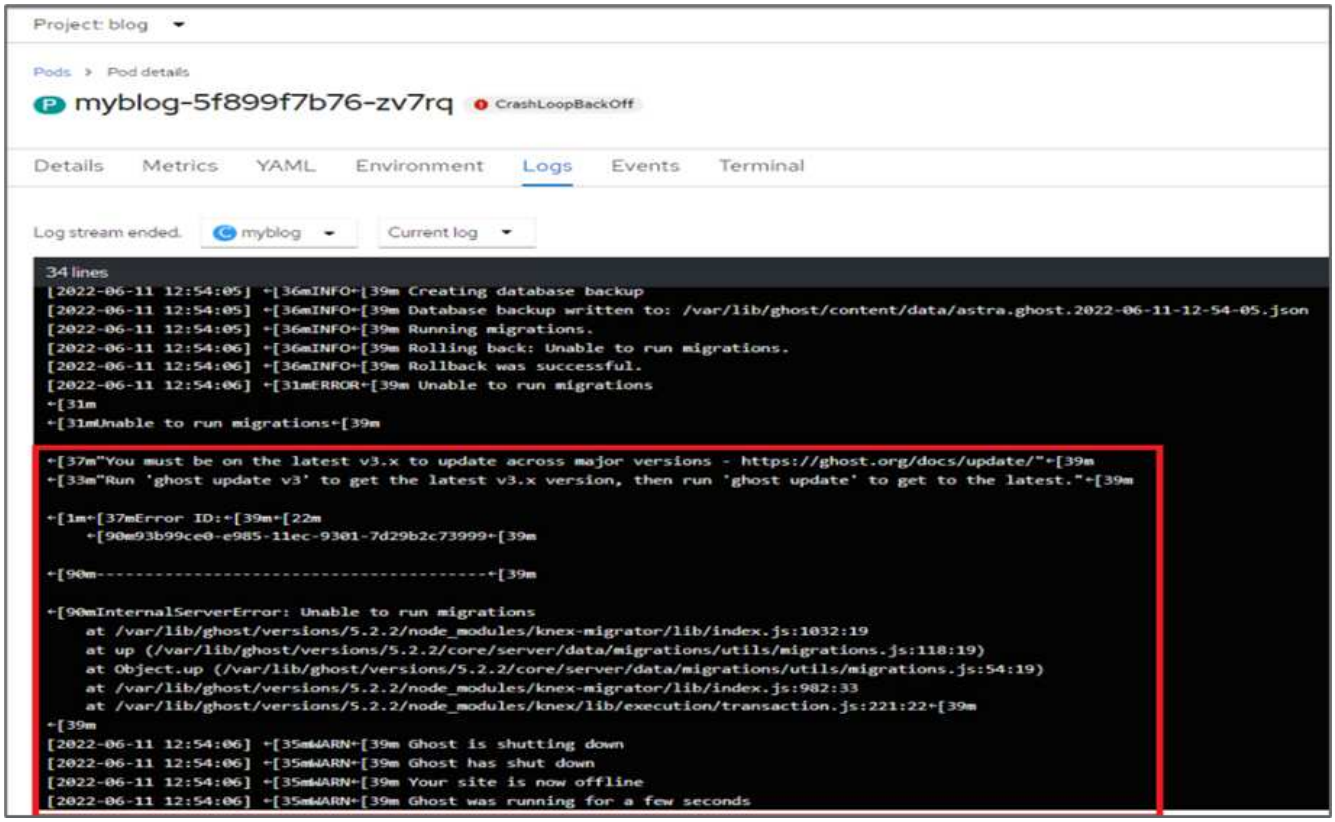
5. Vá para Astra Control Center. Primeiro, gerencie o aplicativo a partir da guia descoberta e, em seguida, faça uma cópia Snapshot.



Você também pode proteger seus aplicativos criando snapshots, backups ou ambos em um horário definido. Para obter mais informações, "Proteja aplicativos com snapshots e backups"consulte .

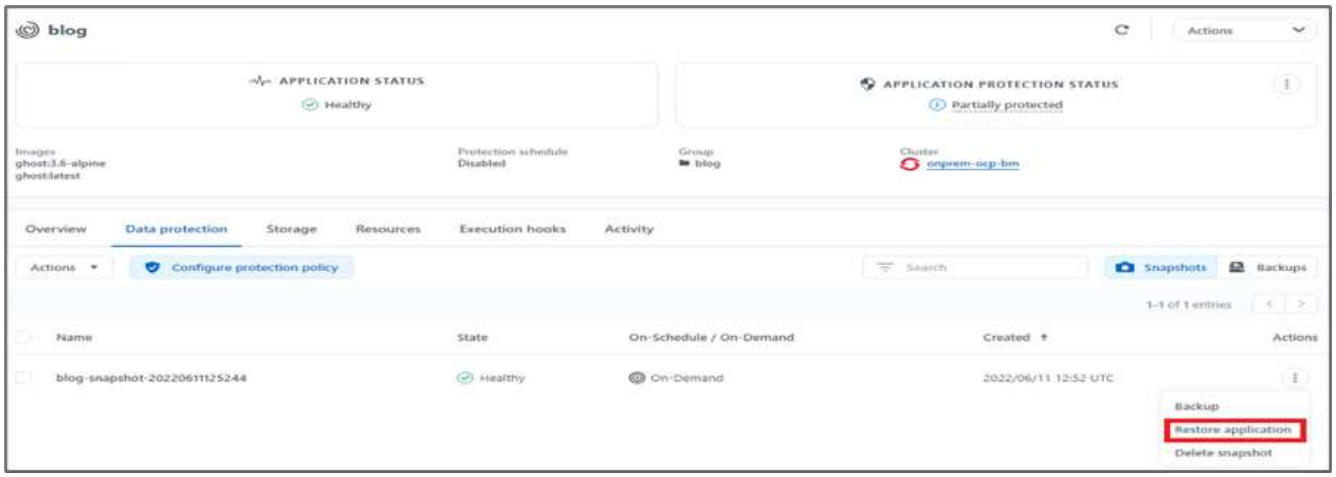
6. Depois que o instantâneo sob demanda for criado com sucesso, atualize o aplicativo para a versão mais recente. A versão atual da imagem é `ghost: 3.6-alpine` e a versão de destino é `ghost:latest`. Para atualizar o aplicativo, faça alterações diretamente no repositório Git e sincronize-as com o CD Argo.

7. Você pode ver que a atualização direta para a versão mais recente não é suportada devido ao site do blog estar em baixo e todo o aplicativo estar corrompido.

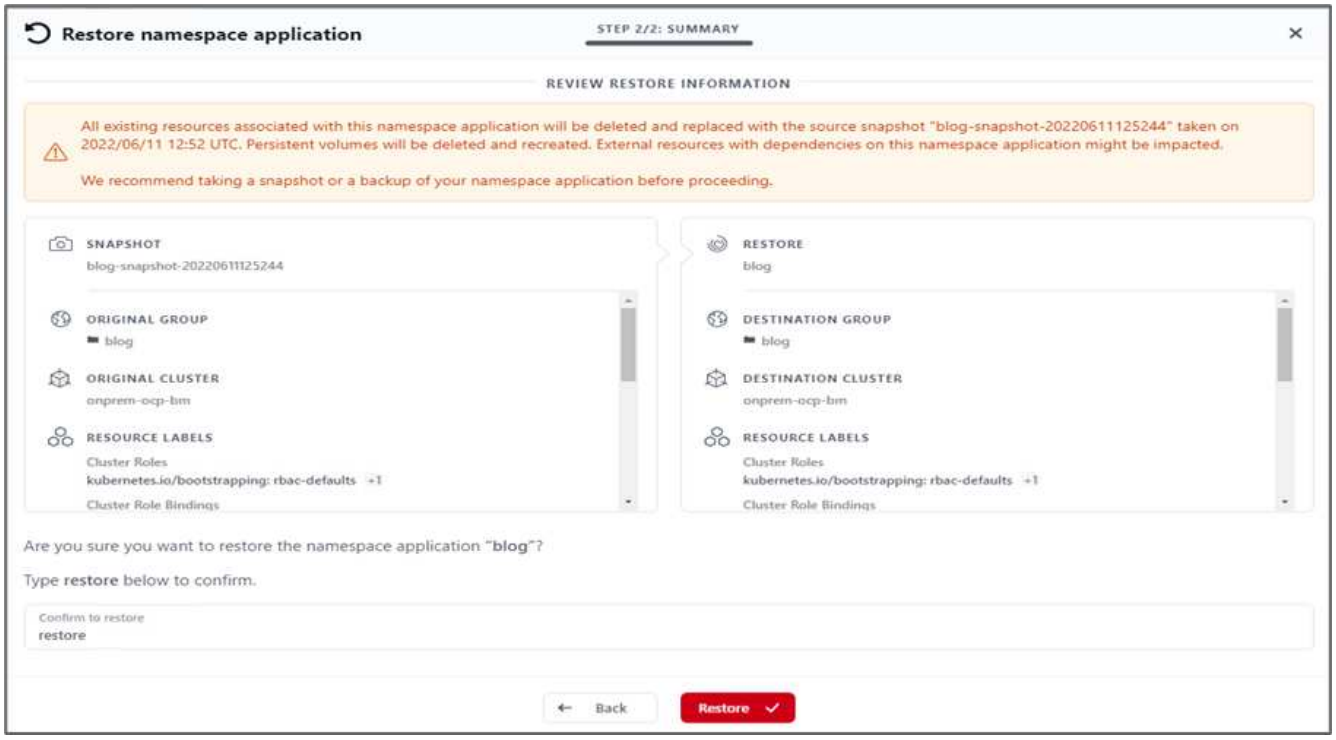


8. Para confirmar a indisponibilidade do site do blog, atualize o URL.

9. Restaure a aplicação a partir do instantâneo.



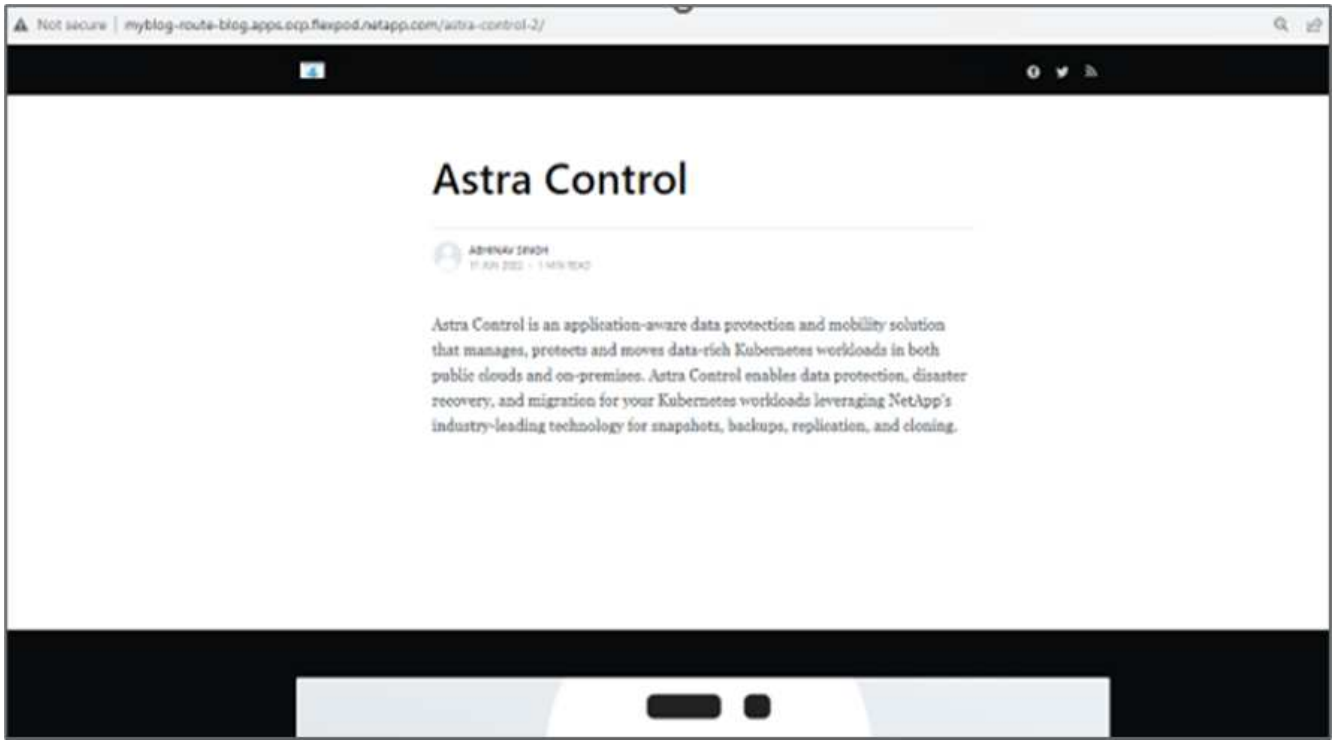
10. O aplicativo é restaurado no mesmo cluster OpenShift.



11. O processo de restauração do aplicativo é iniciado imediatamente.

12. Em poucos minutos, o aplicativo é restaurado com sucesso a partir do snapshot disponível.

13. Para ver se a página da Web está disponível, atualize a URL.

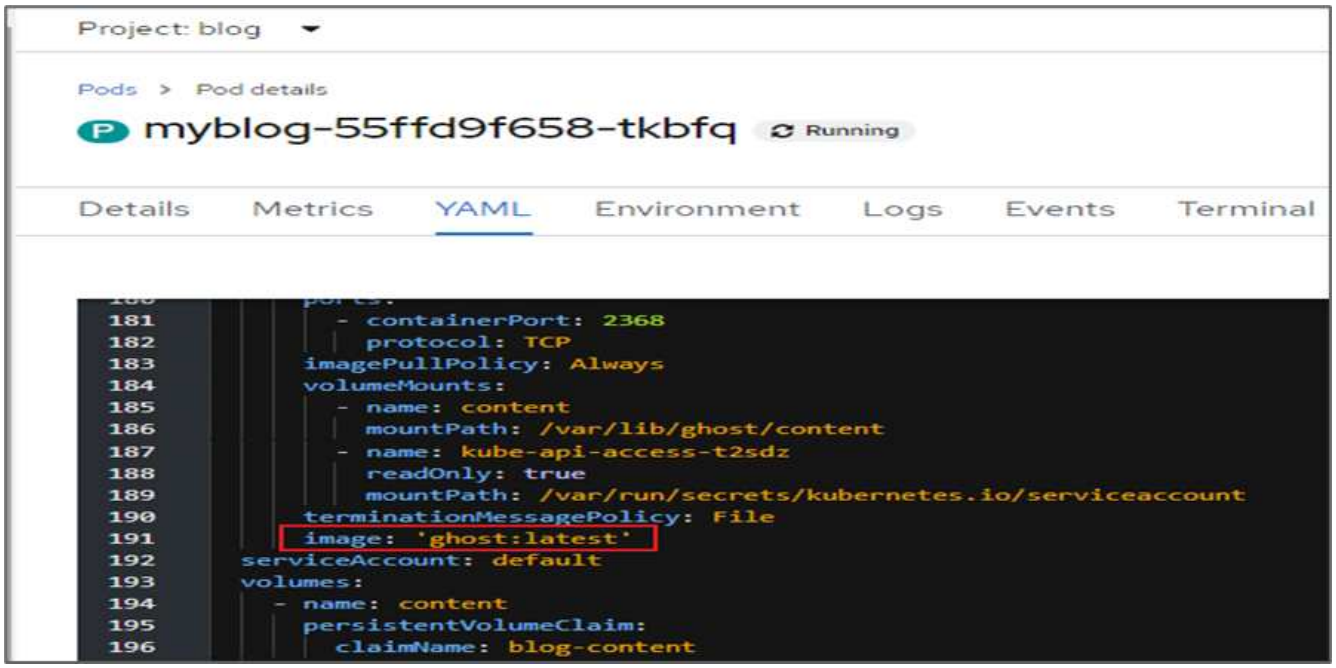


Com a ajuda do Astra Control Center, uma equipe de DevTest pode recuperar com sucesso um aplicativo de site de blog e seus dados associados usando o snapshot.

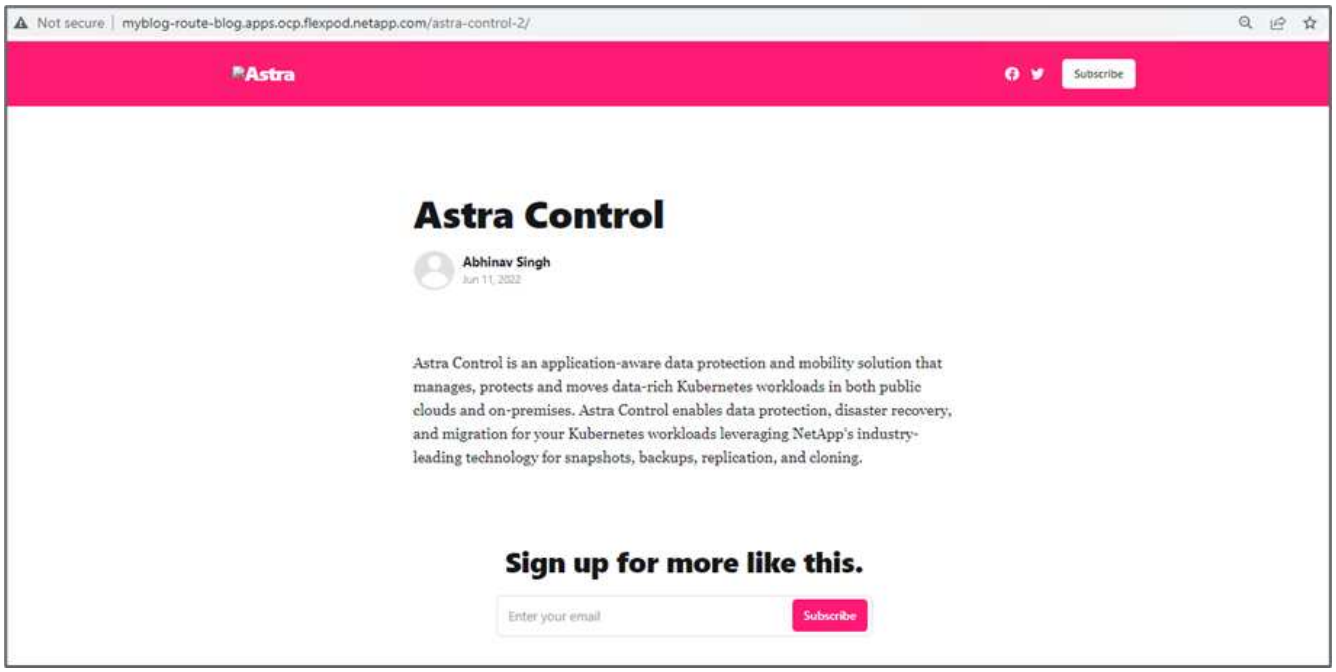
Parte 2

Com o Astra Control Center, é possível migrar uma aplicação inteira e seus dados entre clusters do Kubernetes, independentemente de onde os clusters estão localizados (no local ou na nuvem).

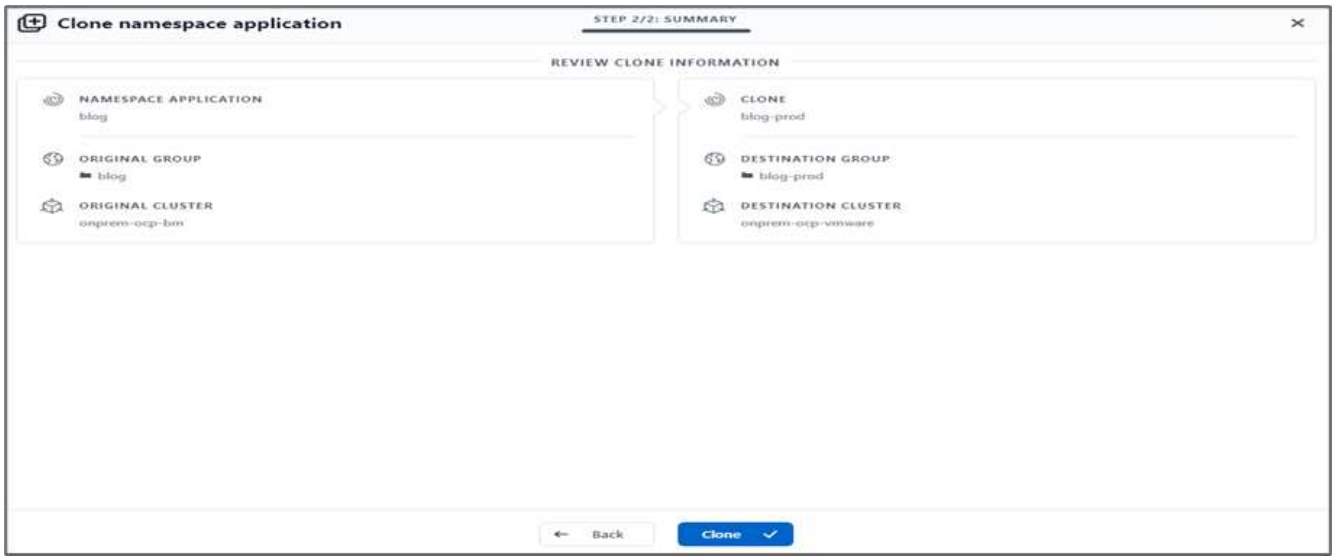
1. A equipe do DevTest inicialmente atualiza o aplicativo para a versão suportada (`ghost-4.6-alpine`) antes de atualizar para a versão (`ghost-latest`final) para torná-lo pronto para a produção. Em seguida, eles publicam uma atualização do aplicativo clonado para o cluster OpenShift de produção em execução em um sistema FlexPod diferente.
2. Neste ponto, o aplicativo é atualizado para a versão mais recente e pronto para ser clonado para o cluster de produção.



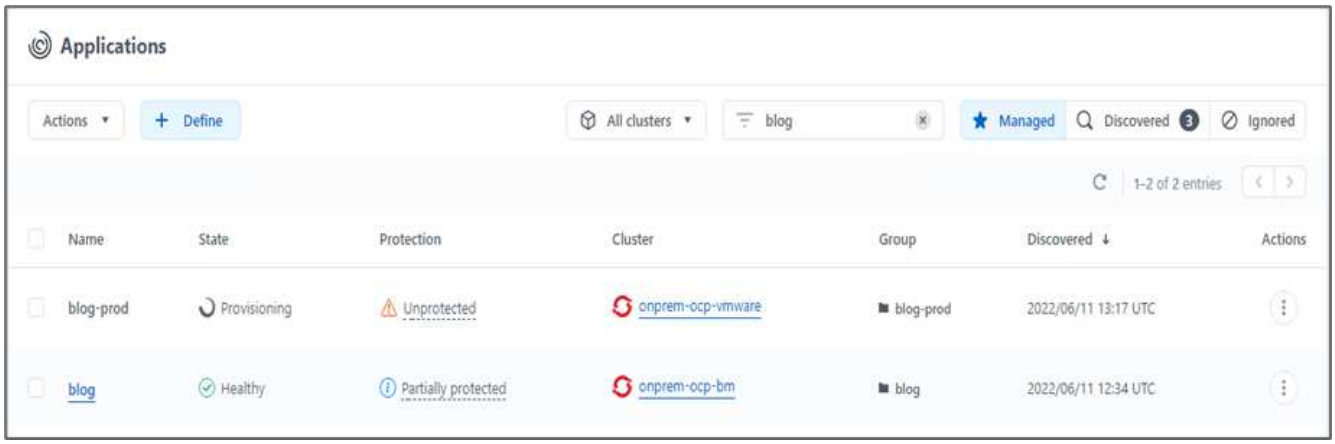
3. Para verificar o novo tema, atualize o site do blog.



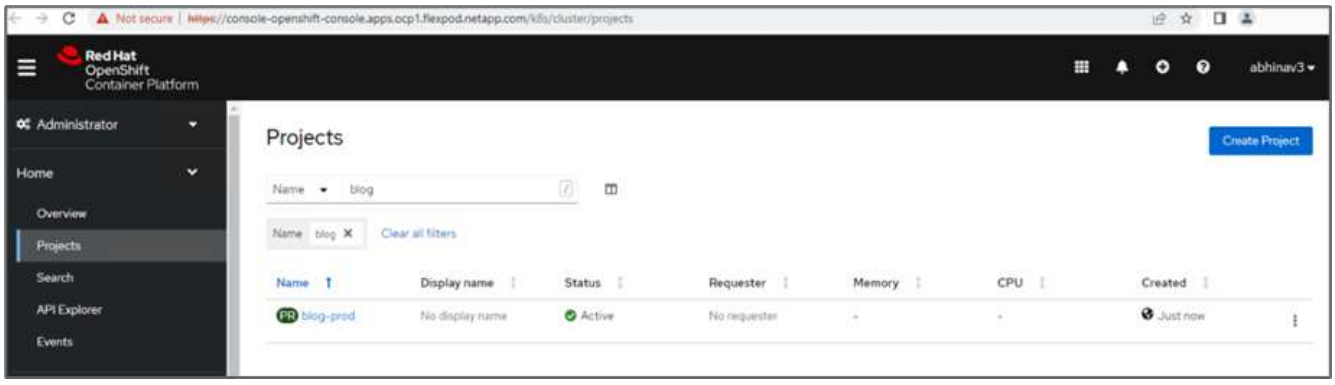
4. No Astra Control Center, clone o aplicativo para o outro cluster OpenShift de produção executado no VMware vSphere.



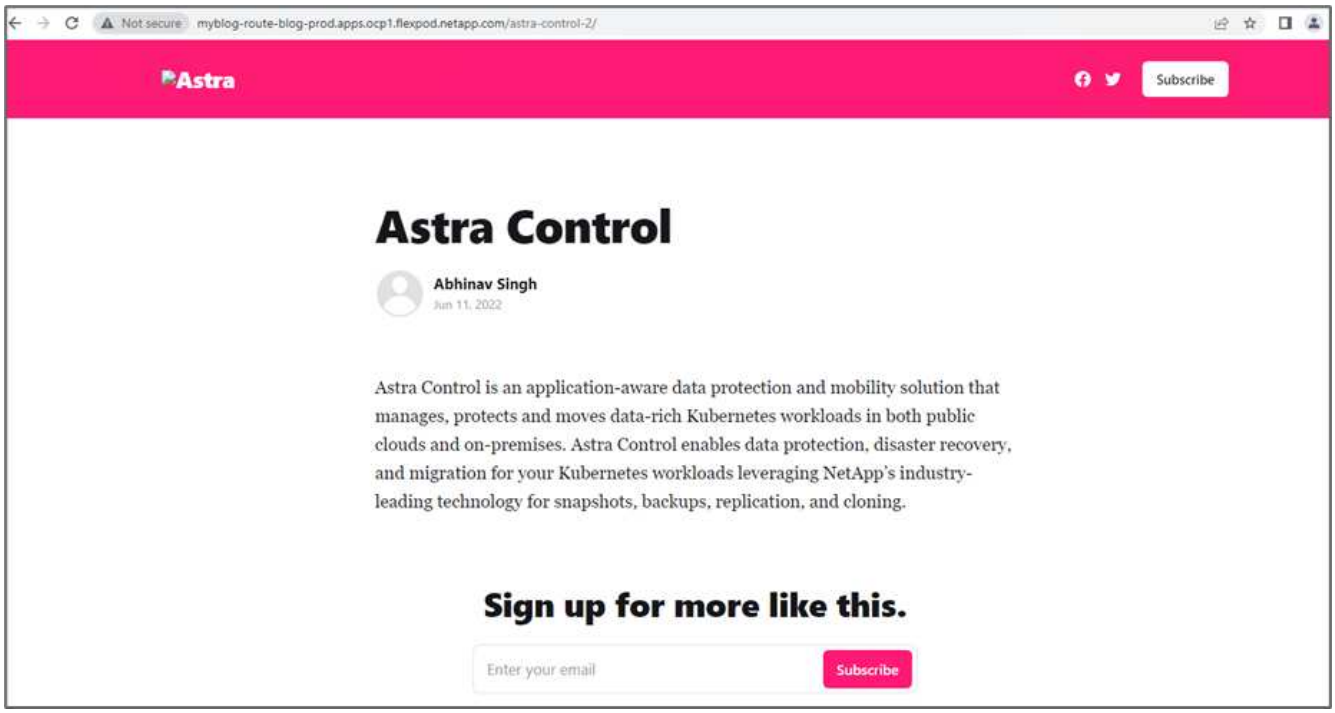
Um novo clone de aplicativo agora é provisionado no cluster OpenShift de produção.



5. Faça login no cluster OpenShift de produção e pesquise o blog do projeto.



6. No menu lateral, selecione rede > rotas e clique no URL em localização. A mesma página inicial com o conteúdo é exibida.



Isso conclui a validação da solução Astra Control Center. Agora você pode clonar uma aplicação inteira e seus dados de um cluster Kubernetes para outro, não importa onde o cluster Kubernetes esteja localizado.

"Próximo: Conclusão."

Conclusão

"Anterior: Recuperação de aplicativos com backups remotos."

Nessa solução, implementamos um plano de proteção para aplicações em contêiner executadas no FlexPod e na AWS usando o portfólio do NetApp Astra. O NetApp Astra Control Center e o Astra Trident, juntamente com o Cloud Volumes ONTAP, o Red Hat OpenShift e a infraestrutura FlexPod, formaram os principais componentes desta solução.

Demonstramos a proteção das aplicações com a captura de snapshots e executamos backups de cópias completas para restaurar aplicações em diferentes clusters de K8s U executados em ambientes na nuvem e no local.

Também demonstramos a clonagem de aplicações em K8s clusters, permitindo que os clientes migrem suas aplicações para os K8s clusters escolhidos nos locais desejados.

A FlexPod evoluiu constantemente para que os clientes modernizem seus processos de entrega de aplicações e negócios. Com essa solução, os clientes da FlexPod podem criar com confiança seu plano BCDR para seus aplicativos nativos em nuvem com a nuvem pública como um local para um plano de DR transitório ou em tempo integral, mantendo o custo da solução baixo.

Com o Astra Control, você migra uma aplicação inteira e seus dados de um cluster Kubernetes para outro, independentemente de onde os clusters estão localizados. Ele também pode ajudar você a acelerar a implantação, as operações e a proteção de suas aplicações nativas em nuvem.

Solução de problemas

Para obter instruções sobre solução de problemas, consulte "documentação online" .

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Página inicial do FlexPod

  "https://www.flexpod.com"

- Cisco validou guias de design e implantação para FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Implantação do FlexPod com infraestrutura como código para VMware usando Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Implantação do FlexPod com infraestrutura como código para o bare metal do Red Hat OpenShift com o Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Ferramenta de interoperabilidade de hardware e software Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Folha de dados de Intersight da Cisco

  "https://intersight.com/help/saas/home"

- Documentação do NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- Centro de Controle NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- Gerenciador de nuvem do NetApp

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

  "https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Ferramenta de Matriz de interoperabilidade do NetApp

  "http://support.netapp.com/matrix/"

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Julho de 2022	Solte para ACC 22.04.0.

NetApp Cloud Insights para FlexPod

TR-4868: NetApp Cloud Insights para FlexPod

Alan Cowles, NetApp

Em parceria com: 

A solução detalhada neste relatório técnico é a configuração do serviço NetApp Cloud Insights para monitorar o sistema de storage NetApp AFF A800 executando o NetApp ONTAP, que é implantado como parte de uma solução de datacenter FlexPod.

Valor do cliente

A solução detalhada aqui agrega valor aos clientes interessados em uma solução de monitoramento completa para seus ambientes de nuvem híbrida, em que o ONTAP é implantado como sistema de storage primário. Isso inclui ambientes FlexPod que usam sistemas de storage NetApp AFF e FAS.

Casos de uso

Esta solução aplica-se aos seguintes casos de uso:

- Organizações que querem monitorar vários recursos e utilização em seu sistema de storage ONTAP implantado como parte de uma solução FlexPod.
- Organizações que querem solucionar problemas e reduzir o tempo de resolução de incidentes que ocorrem em sua solução FlexPod com seus sistemas AFF ou FAS.
- Organizações interessadas em projeções de otimização de custos, incluindo painéis personalizados para fornecer informações detalhadas sobre o desperdício de recursos e onde economias de custo podem ser obtidas em seu ambiente FlexPod, incluindo o ONTAP.

Público-alvo

O público-alvo da solução inclui os seguintes grupos:

- Executivos DE TI e aqueles preocupados com a otimização de custos e a continuidade dos negócios.
- Arquitetos de soluções com interesse em design e gerenciamento de data center ou nuvem híbrida.
- Engenheiros de suporte técnico responsáveis pela solução de problemas e resolução de incidentes.

Você pode configurar o Cloud Insights para fornecer vários tipos úteis de dados que você pode usar para ajudar no Planejamento, solução de problemas, manutenção e garantir a continuidade dos negócios. Ao monitorar a solução de data center FlexPod com o Cloud Insights e apresentar os dados agregados em painéis personalizados de fácil digestão. Além disso, é possível prever quando os recursos em uma implantação podem precisar ser dimensionados para atender às demandas, também identificar aplicações específicas ou volumes de storage que estão causando problemas no sistema. Isso ajuda a garantir que a infraestrutura que está sendo monitorada seja previsível e tenha desempenho de acordo com as expetativa, permitindo que uma organização entregue com SLA definidos e dimensione a infraestrutura conforme necessário, eliminando desperdício e custos adicionais.

Arquitetura

Nesta seção, analisamos a arquitetura de uma infraestrutura convergente do data center FlexPod, incluindo um sistema NetApp AFF A800 monitorado pelo Cloud Insights.

Tecnologia da solução

Uma solução de data center FlexPod consiste nos seguintes componentes mínimos para fornecer um ambiente de infraestrutura convergente altamente disponível, facilmente dimensionável, validado e compatível.

- Dois nós de storage da NetApp ONTAP (um par de HA)
- Dois switches de rede de data center Cisco Nexus
- Dois switches de malha Cisco MDS (opcional para implantações FC)
- Duas interconexões de malha Cisco UCS
- Um chassi blade Cisco UCS com dois servidores blade da série B Cisco UCS

Ou

- Dois servidores de montagem em rack Cisco UCS C-Series

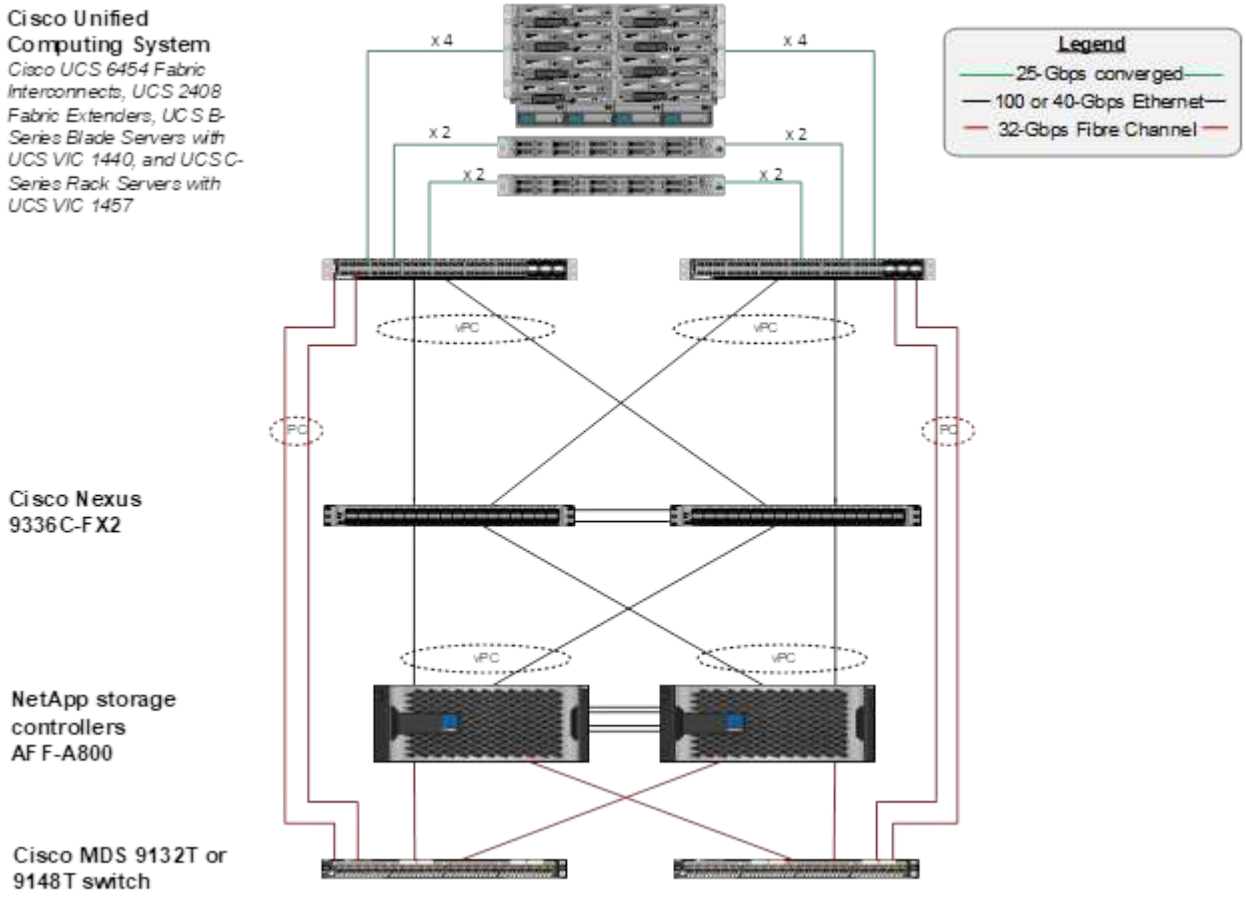
Para que a Cloud Insights colete dados, uma organização deve implantar uma Unidade de aquisição como uma máquina virtual ou física dentro de seu ambiente de data center FlexPod ou em um local onde possa entrar em Contato com os componentes dos quais está coletando dados. Pode instalar o software Unidade de aquisição num sistema com vários sistemas operativos Windows ou Linux suportados. A tabela a seguir lista os componentes da solução para este software.

Sistema operacional	Versão
Microsoft Windows	10
Microsoft Windows Server	2012, 2012 R2, 2016, 2019
Red Hat Enterprise Linux	7,2 – 7,6

Sistema operacional	Versão
CentOS	7,2 – 7,6
Oracle Enterprise Linux	7,5
Debian	9
Ubuntu	18,04 LTS

Diagrama arquitetônico

A figura a seguir mostra a arquitetura da solução.



Requisitos de hardware

A tabela a seguir lista os componentes de hardware necessários para implementar a solução. Os componentes de hardware que são usados em qualquer implementação específica da solução podem variar com base nos requisitos do cliente.

Hardware	Quantidade
Cisco Nexus 9336C-FX2	2
Interconexão de malha Cisco UCS 6454	2
Chassi de lâmina Cisco UCS 5108	1
Extensores de tecido Cisco UCS 2408	2

Hardware	Quantidade
Lâminas Cisco UCS B200 M5	2
NetApp AFF A800	2

Requisitos de software

A tabela a seguir lista os componentes de software necessários para implementar a solução. Os componentes de software usados em qualquer implementação específica da solução podem variar de acordo com os requisitos do cliente.

Software	Versão
Firmware Cisco Nexus	9,3 mm (5 mm)
Versão do Cisco UCS	4,1 mm (2a mm)
Versão do NetApp ONTAP	9,7
Versão do NetApp Cloud Insights	Setembro 2020, Básico
Red Hat Enterprise Linux	7,6
VMware vSphere	6.7U3

Detalhes do caso de uso

Esta solução aplica-se aos seguintes casos de uso:

- Análise do ambiente com dados fornecidos ao consultor digital da NetApp Active IQ para avaliação dos riscos do sistema de storage e recomendações para otimização do storage.
- Solução de problemas no sistema de storage ONTAP implantado em uma solução de data center FlexPod examinando as estatísticas do sistema em tempo real.
- Geração de painéis personalizados para monitorar facilmente pontos de interesse específicos dos sistemas de storage da ONTAP implantados em uma infraestrutura convergente do data center FlexPod.

Considerações de design

A solução de data center FlexPod é uma infraestrutura convergente projetada pela Cisco e pela NetApp para oferecer um ambiente de data center dinâmico, altamente disponível e dimensionável para a execução de workloads empresariais. Os recursos de computação e rede na solução são fornecidos pelos produtos Cisco UCS e Nexus, e os recursos de storage são fornecidos pelo sistema de storage da ONTAP. O design da solução é aprimorado regularmente, quando modelos de hardware atualizados ou versões de software e firmware ficam disponíveis. Esses detalhes, juntamente com as práticas recomendadas para o projeto e implantação da solução, são capturados em documentos de Cisco Validated Design (CVD) ou NetApp Verified Architecture (NVA) e publicados regularmente.

O documento CVD mais recente detalhando o design da solução de datacenter FlexPod está disponível "aqui".

Implante o Cloud Insights para FlexPod

Para implantar a solução, você deve concluir as seguintes tarefas:

1. Inscreva-se no serviço Cloud Insights
2. Crie uma máquina virtual VMware (VM) para configurar como uma unidade de aquisição
3. Instale o host Red Hat Enterprise Linux (RHEL)
4. Crie uma instância da Unidade de aquisição no Portal do Cloud Insights e instale o software
5. Adicione o sistema de storage monitorado do data center FlexPod ao Cloud Insights.

Inscreva-se no serviço NetApp Cloud Insights

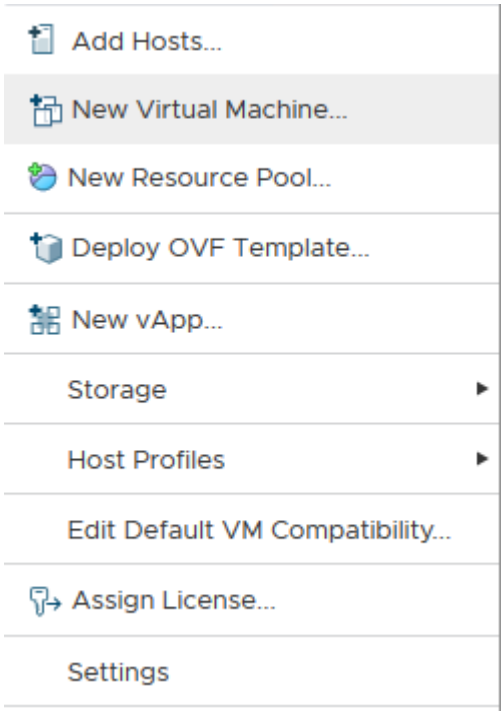
Para se inscrever no Serviço NetApp Cloud Insights, execute as seguintes etapas:

1. Vá para "https://cloud.netapp.com/cloud-insights"
2. Clique no botão no centro da tela para iniciar a avaliação gratuita de 14 dias ou no link no canto superior direito para se inscrever ou fazer login em uma conta existente do NetApp Cloud Central.

Crie uma máquina virtual VMware para configurar como uma unidade de aquisição

Para criar uma VM VMware para configurar como uma unidade de aquisição, execute as seguintes etapas:

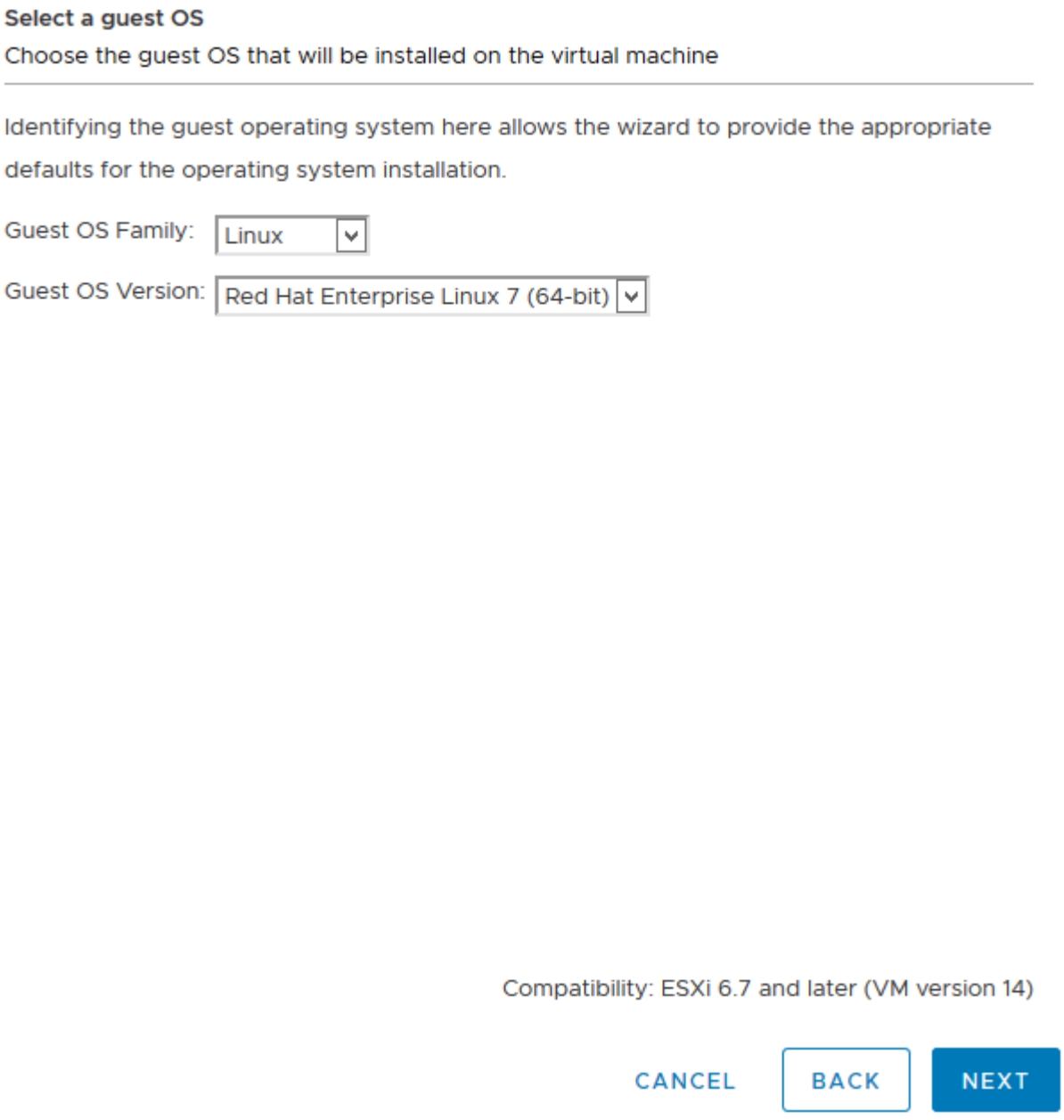
1. Inicie um navegador da Web e faça login no VMware vSphere e selecione o cluster que deseja hospedar uma VM.
2. Clique com o botão direito do rato nesse cluster e selecione criar Uma máquina virtual a partir do menu.



3. No assistente Nova Máquina Virtual, clique em Avançar.
4. Especifique o nome da VM e selecione o data center no qual você deseja instalá-lo e clique em Avançar.
5. Na página a seguir, selecione o cluster, nós ou grupo de recursos para o qual deseja instalar a VM e clique

em Avançar.

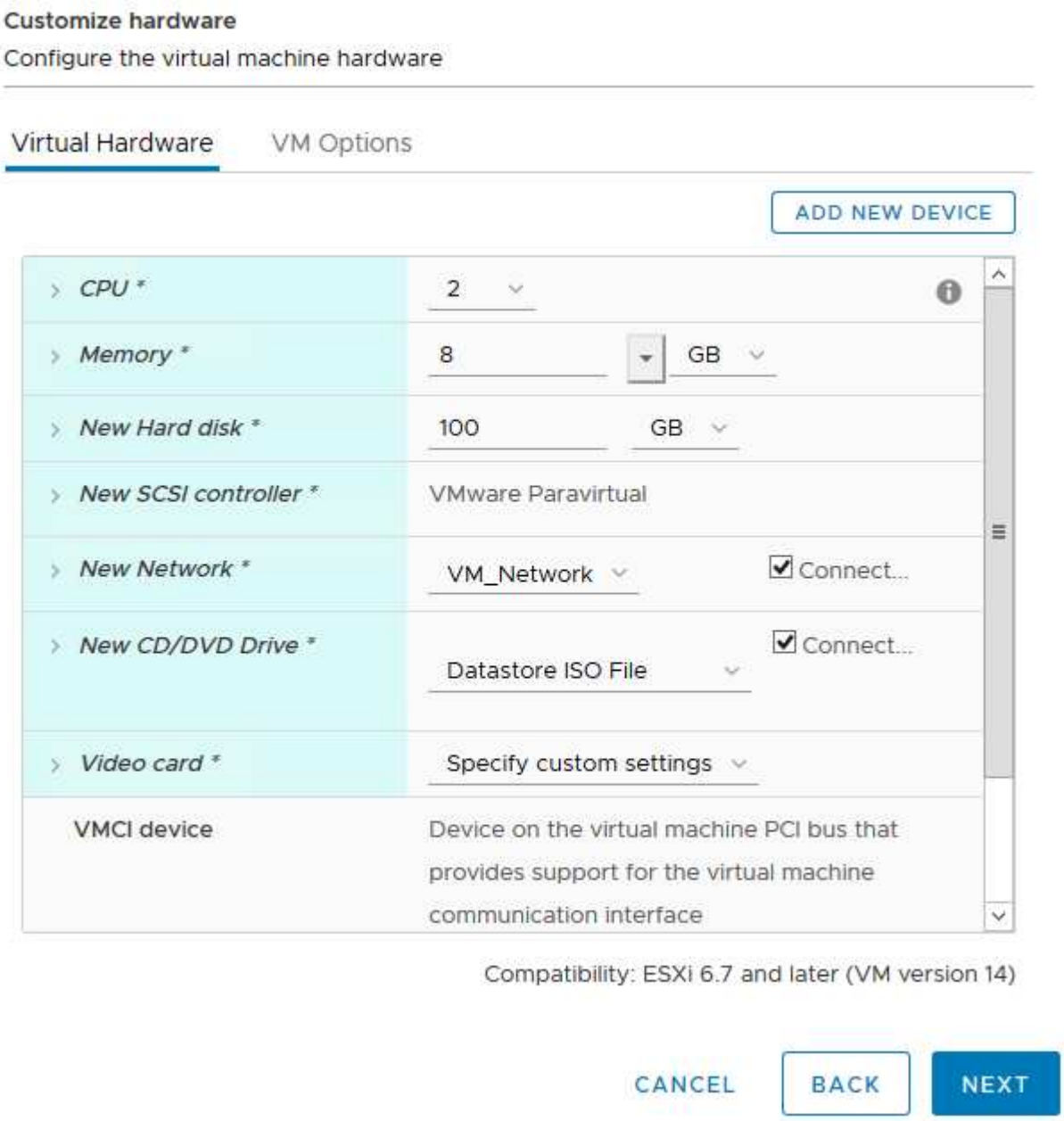
6. Selecione o datastore compartilhado que hospeda suas VMs e clique em Avançar.
7. Confirme se o modo de compatibilidade para a VM está definido como `ESXi 6.7 or later` e clique em seguinte.
8. Select Guest os Family Linux, Guest os versão: Red Hat Enterprise Linux 7 (64 bits).



9. A próxima página permite a personalização de recursos de hardware na VM. A Unidade de aquisição Cloud Insights requer os seguintes recursos. Depois que os recursos forem selecionados, clique em Avançar:
   a. Duas CPUs
   b. 8GB GB de RAM
   c. 100GB GB de espaço em disco rígido

d. Uma rede que pode alcançar recursos no datacenter FlexPod e no servidor Cloud Insights através de uma conexão SSL na porta 443.

e. Uma imagem ISO da distribuição Linux escolhida (Red Hat Enterprise Linux) para inicializar.

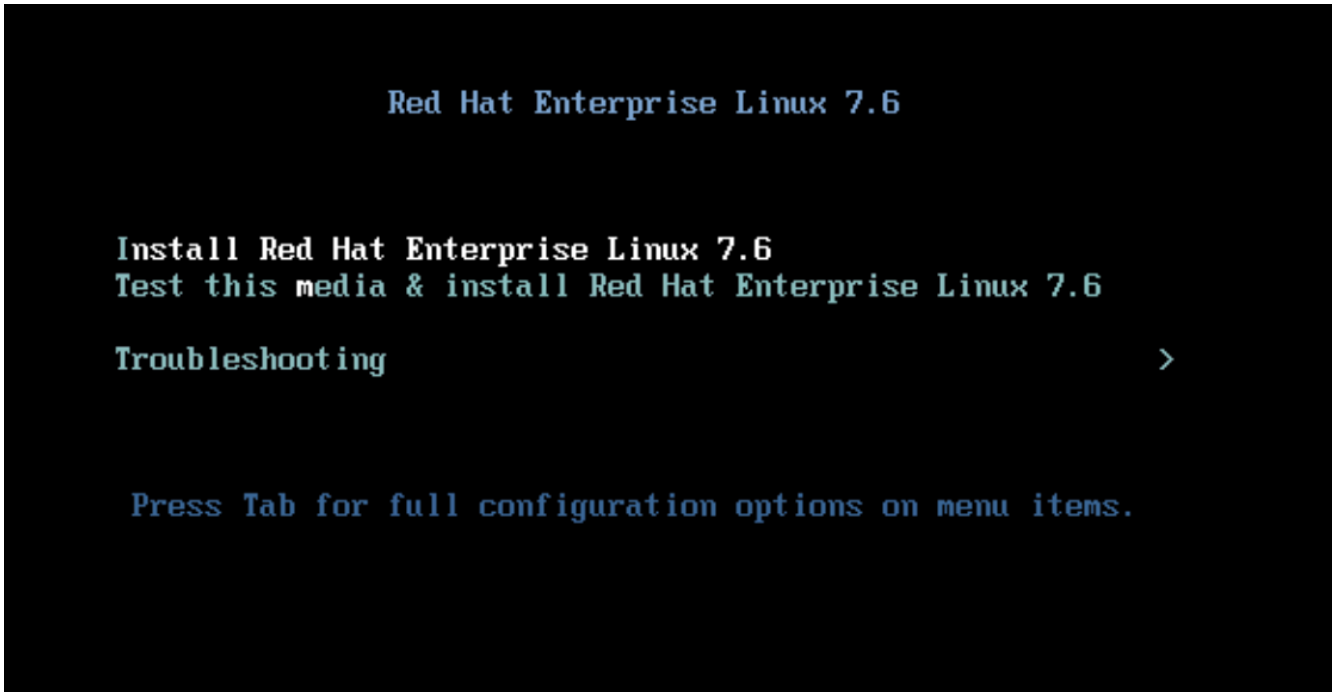


10. Para criar a VM, na página Pronto para concluir, revise as configurações e clique em concluir.

Instale o Red Hat Enterprise Linux

Para instalar o Red Hat Enterprise Linux, execute as seguintes etapas:

1. Ligue a VM, clique na janela para iniciar o console virtual e selecione a opção Instalar o Red Hat Enterprise Linux 7,6.

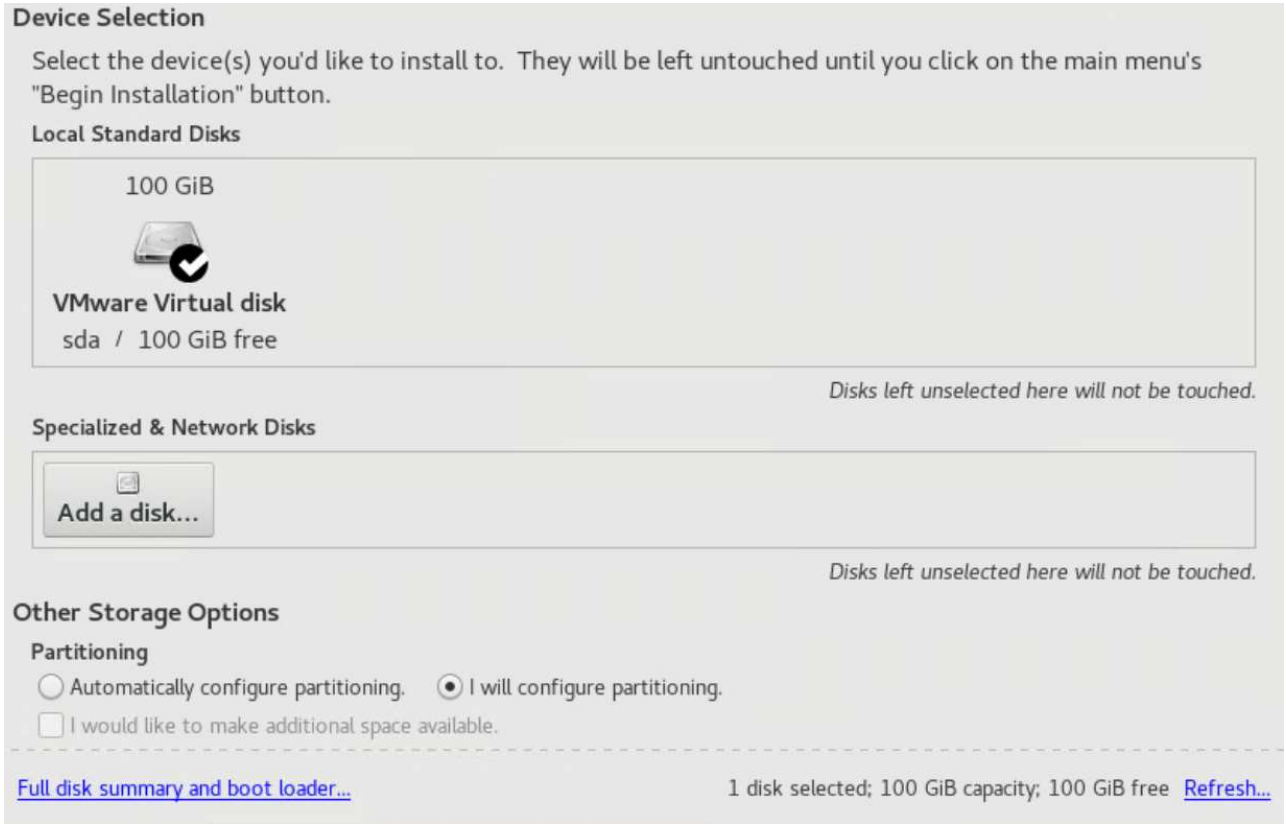


2. Selecione o idioma preferido e clique em continuar.

   A página seguinte é o Resumo da instalação. As configurações padrão devem ser aceitáveis para a maioria dessas opções.

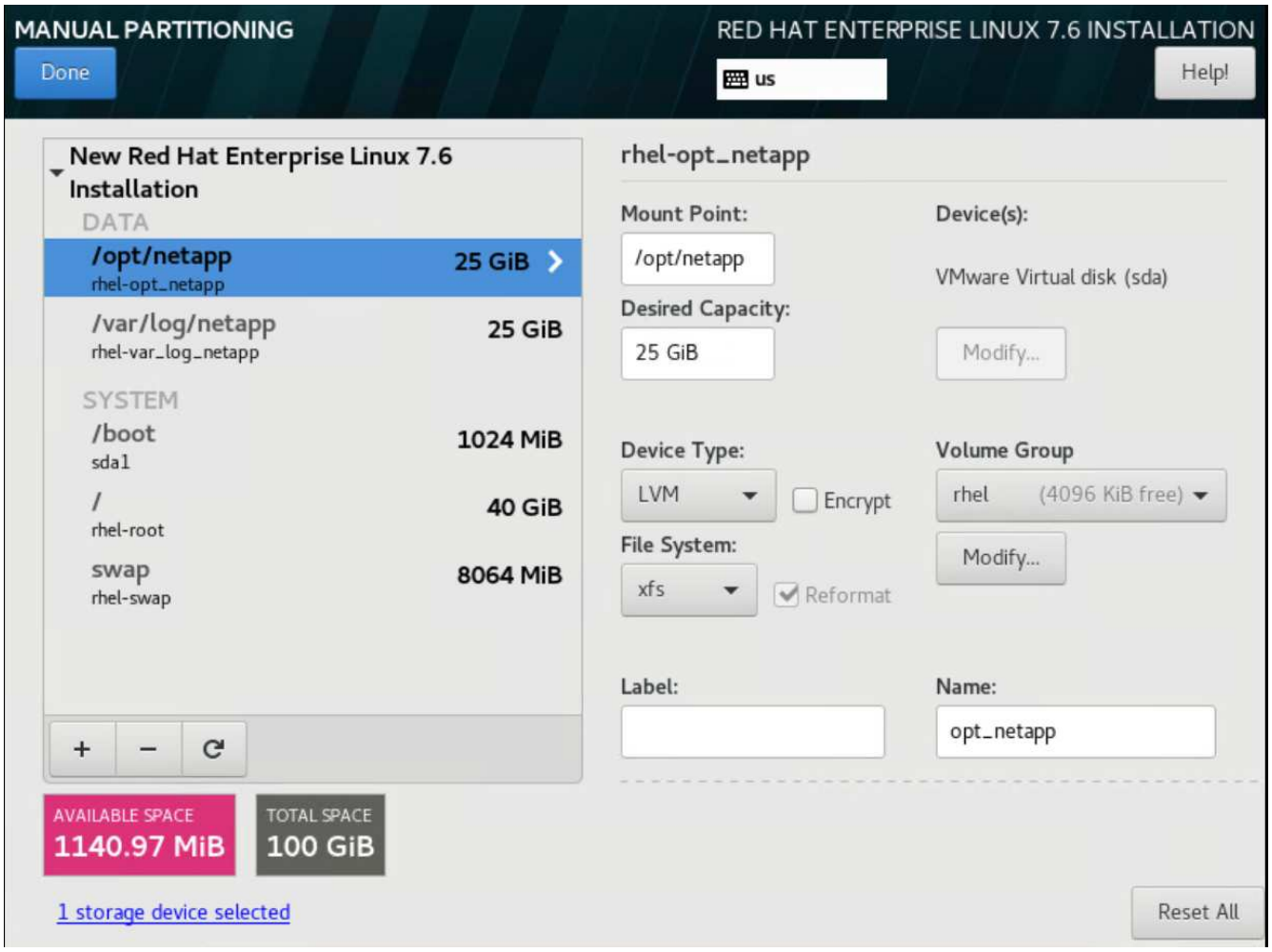
3. Você deve personalizar o layout de armazenamento executando as seguintes opções:

   a. Para personalizar o particionamento para o servidor, clique em Installation Destination (destino de instalação).
   b. Confirme se o VMware Virtual Disk of 100GiB está selecionado com uma marca de seleção preta e selecione o botão de opção I will Configure Partitioning (Configurar particionamento).



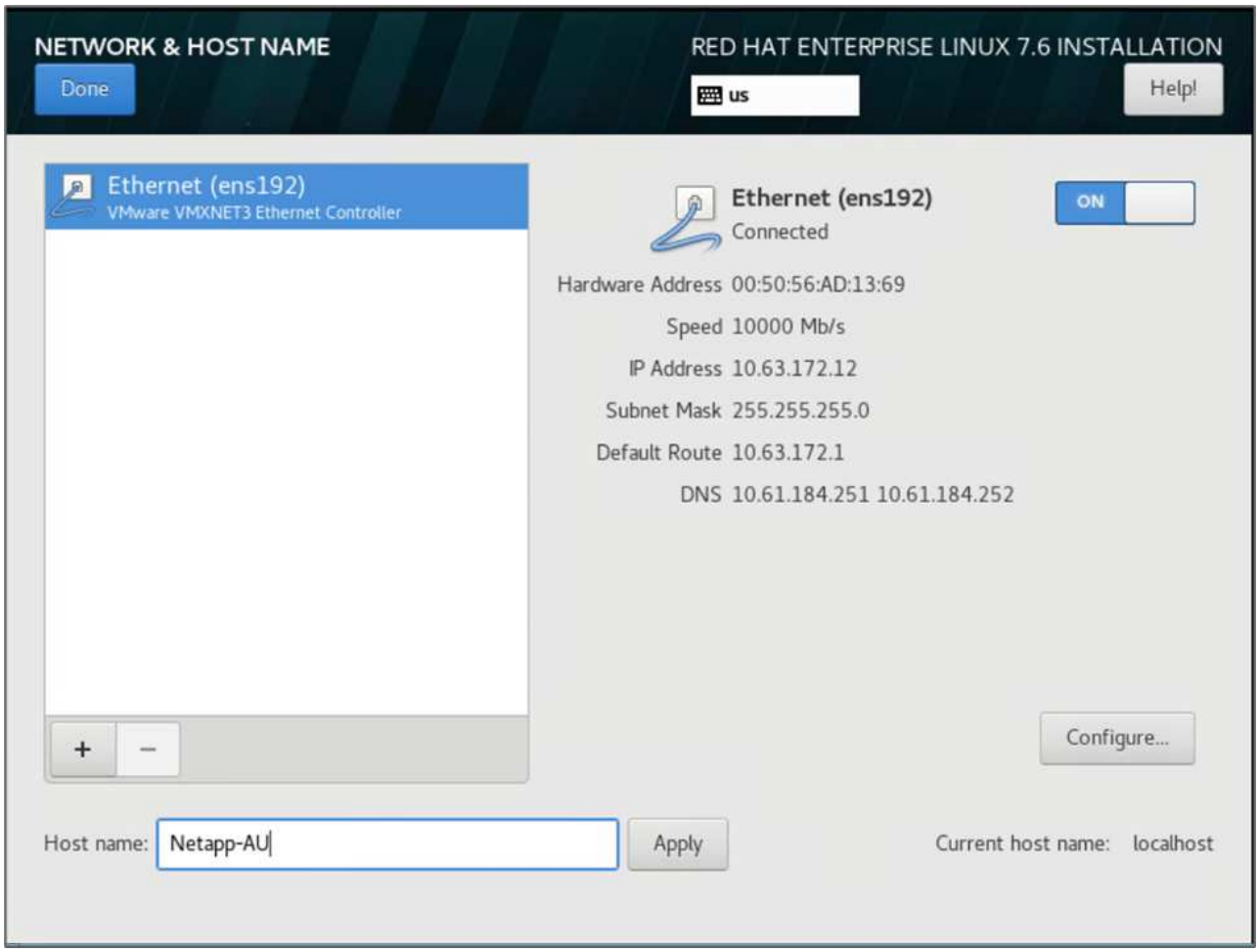
c. Clique em Concluído.

É apresentado um novo menu que permite personalizar a tabela de partições. Dedique 25 GB cada a `/opt/netapp` e `/var/log/netapp`. Você pode alocar automaticamente o restante do storage ao sistema.



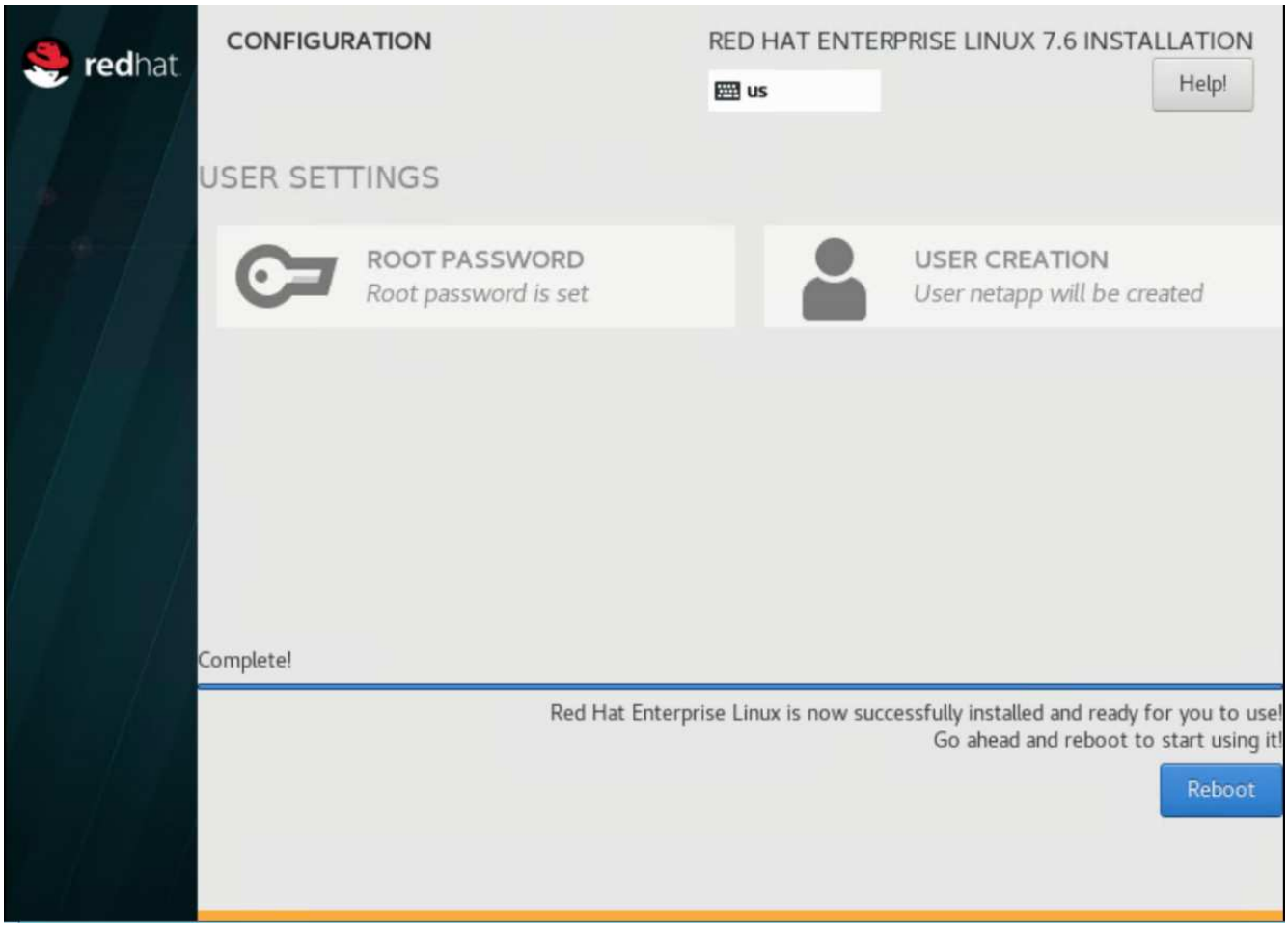
a. Para retornar ao Resumo da instalação, clique em Concluído.

4. Clique em rede e Nome do host.
   a. Insira um nome de host para o servidor.
   b. Ligue o adaptador de rede clicando no botão deslizante. Se o DHCP (Dynamic Host Configuration Protocol) estiver configurado na rede, receberá um endereço IP. Se não estiver, clique em Configurar e atribua um endereço manualmente.



c. . Clique em Concluído para retornar ao Resumo da instalação.

5. Na página Resumo da instalação, clique em Iniciar instalação.
6. Na página progresso da instalação, você pode definir a senha raiz ou criar uma conta de usuário local. Quando a instalação terminar, clique em Reiniciar para reiniciar o servidor.



7. Depois que o sistema reiniciar, faça login no seu servidor e Registre-o no Red Hat Subscription Manager.

```
[root@Netapp-AU ~]# subscription-manager register
Registering to: subscription.rhsm.redhat.com:443/subscription
Username: alan.cowles@netapp.com
Password:
The system has been registered with ID: a47f2e7b-81cd-4757-85c7-eb1818c2c2a1
The registered system name is: Netapp-AU
[root@Netapp-AU ~]#
```

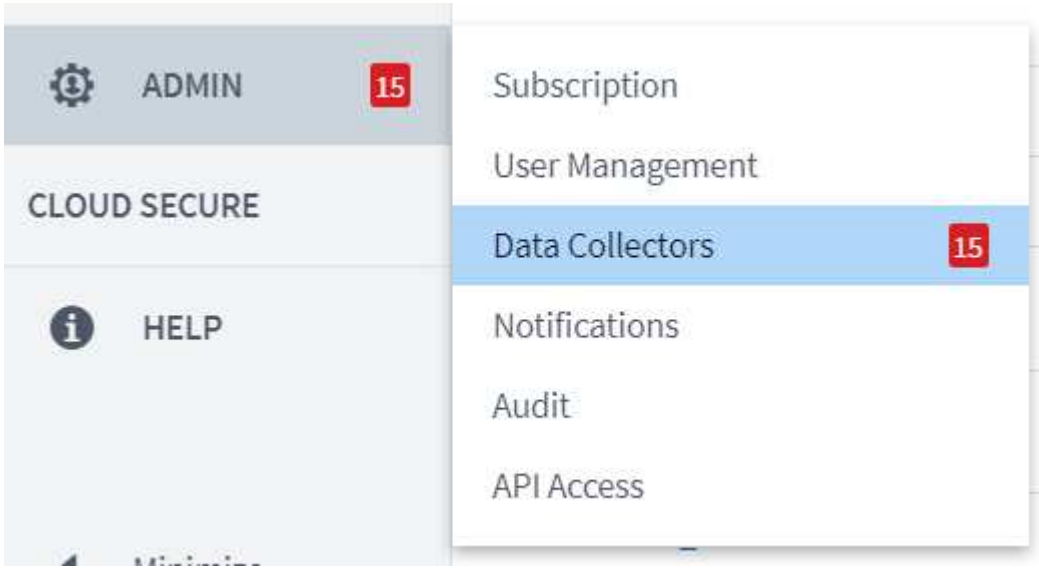
8. Anexe uma assinatura disponível para o Red Hat Enterprise Linux.

```
[root@Netapp-AU ~]# subscription-manager attach --pool=8a85f99b710f3b1901713b90b9e154cf
Successfully attached a subscription for: Red Hat Enterprise Linux, Standard Support (128 Sockets, NFR, Partner Only)
[root@Netapp-AU ~]#
```

Crie uma instância de unidade de aquisição no portal Cloud Insights e instale o software

Para criar uma instância de unidade de aquisição no portal Cloud Insights e instalar o software, execute as seguintes etapas:

1. Na página inicial do Cloud Insights, passe o Mouse sobre a entrada Admin no menu principal à esquerda e selecione coletores de dados no menu.

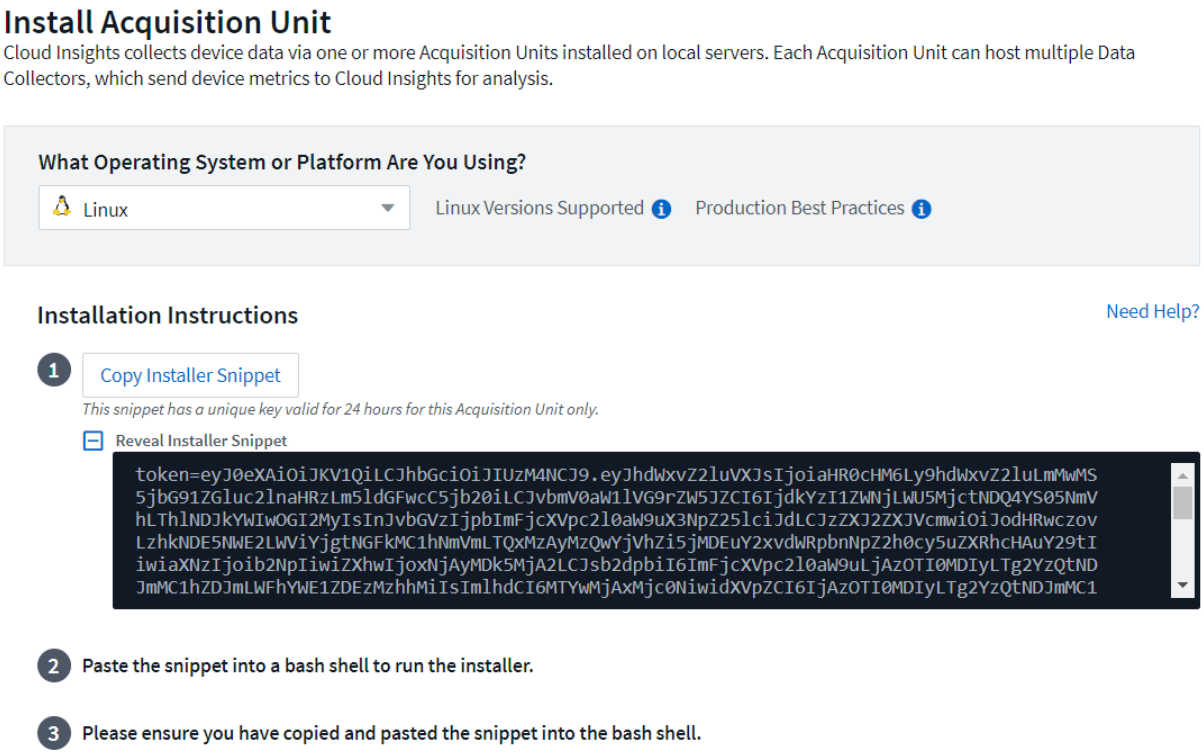


2. No centro superior da página coletores de dados, clique no link para unidades de aquisição.

3. Para criar uma nova unidade de aquisição, clique no botão à direita.

4. Selecione o sistema operacional que deseja usar para hospedar sua Unidade de aquisição e siga as etapas para copiar o script de instalação da página da Web.

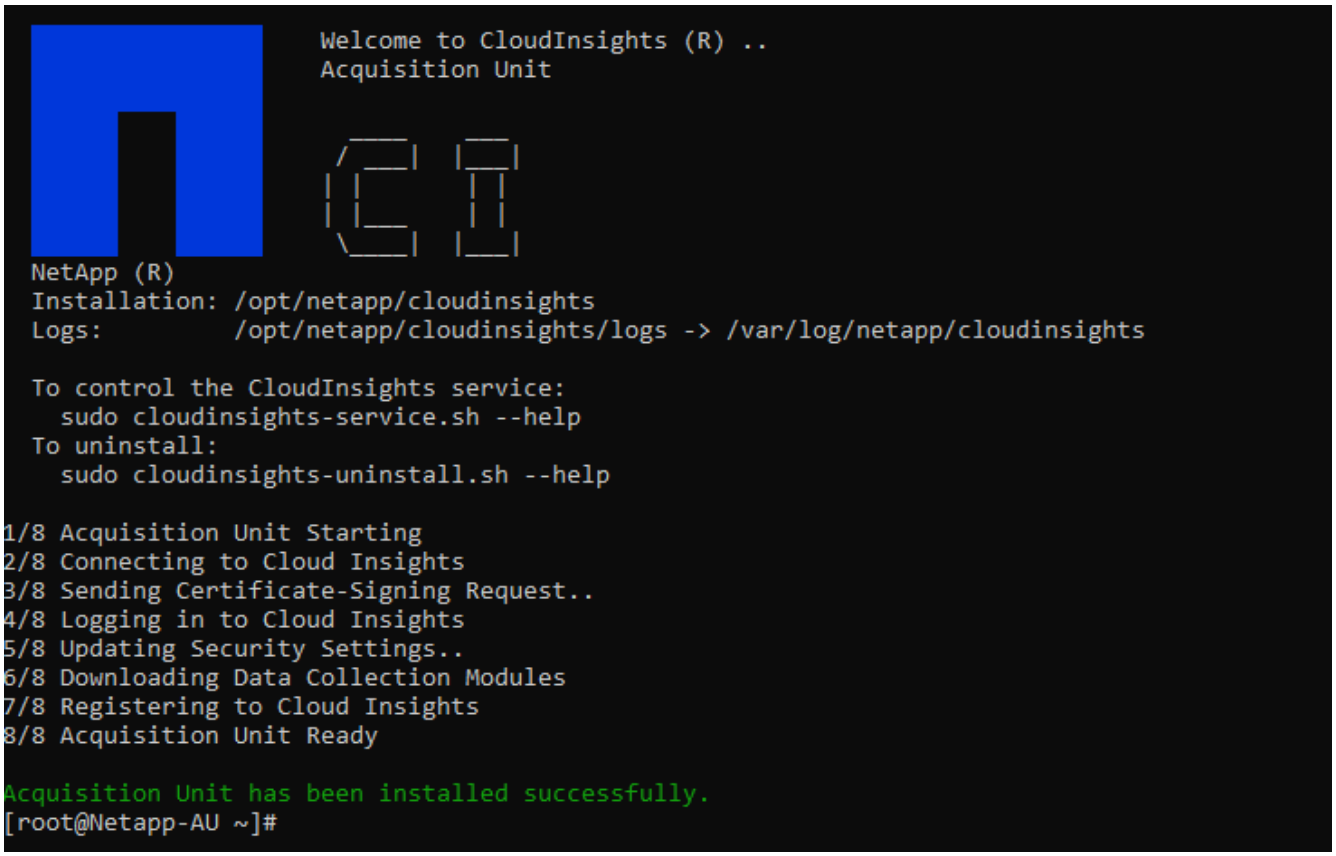
   Neste exemplo, é um servidor Linux, que fornece um snippet e um token para colar na CLI em nosso host. A página da Web aguarda a ligação da unidade de aquisição.



5. Cole o snippet na CLI da máquina Red Hat Enterprise Linux que foi provisionada e clique em Enter.

```
[root@Netapp-AU ~]# token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzM4NCJ9.eyJhdWxvZ2luVXJsIjoiaHR0cHM6Ly9hdWxvZ2luLmMwMS5jbG91ZGluc
2lnaHRzLm5ldGFwcC5jb20iLCJvbmV0aW1lVG9rZW5JZCI6IjQ5ZTY0MGM5LTY5MTItNDQ4Yi04YmI4LTIwNGY2OTQ2YzY1YSIsInJvbGVzIjpbImFjcXVpc
2l0aW9uX3NpZ25lciJdLCJzZXJ2ZXJVcmwiOiJodHRwczovLzhkNDE5NWE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZi5jMDEuY2xvdWRpbnNpZ2h0cy
y5uZXRhcHAuY29tIiwiaXNzIjoib2NpIiwiZXhwIjoxNjAyMTgyNzg2LCJsb2dpbiI6ImFjcXVpc2l0aW9uLjc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZ
TcxZjk0ODRiZCIsImlhdCI6MTYwMjA5NjMyNiwidXVpZCI6Ijc4MTliZGI3LTk5OWQtNGNiYS05YmU1LTMwZTcxZjk0ODRiZCIsInRlbmFudCI6IjhkNDE5N
WE2LWViYjgtNGFkMC1hNmVmLTQxMzAyMzQwYjVhZiIsInRlbmFudFN1YmRvbWFpbiI6InBzMTMyNSJ9.RvWLR3wH1_k6fIOCiO_h-Wok2STfFPDj7VksmXqw
-GZ-JqSIe8SZE4Sv3DuWrWM6 domainUrl=https://8d4195a6-ebb8-4ad0-a6ef-41302340b5af.c01.cloudinsights.netapp.com/rest/v1/au
version=1.253.0 bootstrap=cloudinsights-au-install-bootstrap.sh && curl $proxy_auth_scheme -H "Authorization: Bearer $to
ken" -o $bootstrap $domainUrl/installerBootstrap && sudo chmod 755 $bootstrap && sudo /bin/bash -c "TOKEN=$token HTTPS_P
ROXY=$https_proxy PROXY_AUTH_SCHEME=$proxy_auth_scheme AU_VERSION=$version INSTALLER_NAME=cloudinsights-linux-au-install
er-$version INSTALLER_URL=$domainUrl/installers/linux/$version ./$bootstrap"
```

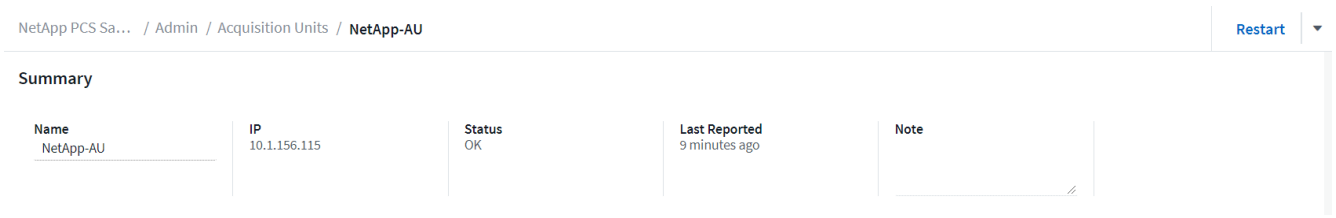
O programa de instalação baixa um pacote compactado e inicia a instalação. Quando a instalação estiver concluída, você receberá uma mensagem informando que a Unidade de aquisição foi registrada no NetApp Cloud Insights.



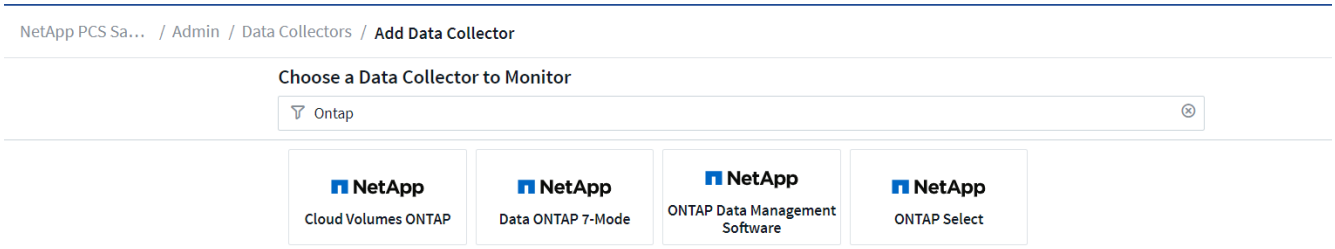
Adicione o sistema de storage monitorado do data center FlexPod ao Cloud Insights

Para adicionar o sistema de storage ONTAP a partir de uma implantação do FlexPod, siga estas etapas:

1. Regresse à página unidades de aquisição no portal Cloud Insights e encontre a unidade recém-registada listada. Para apresentar um resumo da unidade, clique na unidade.

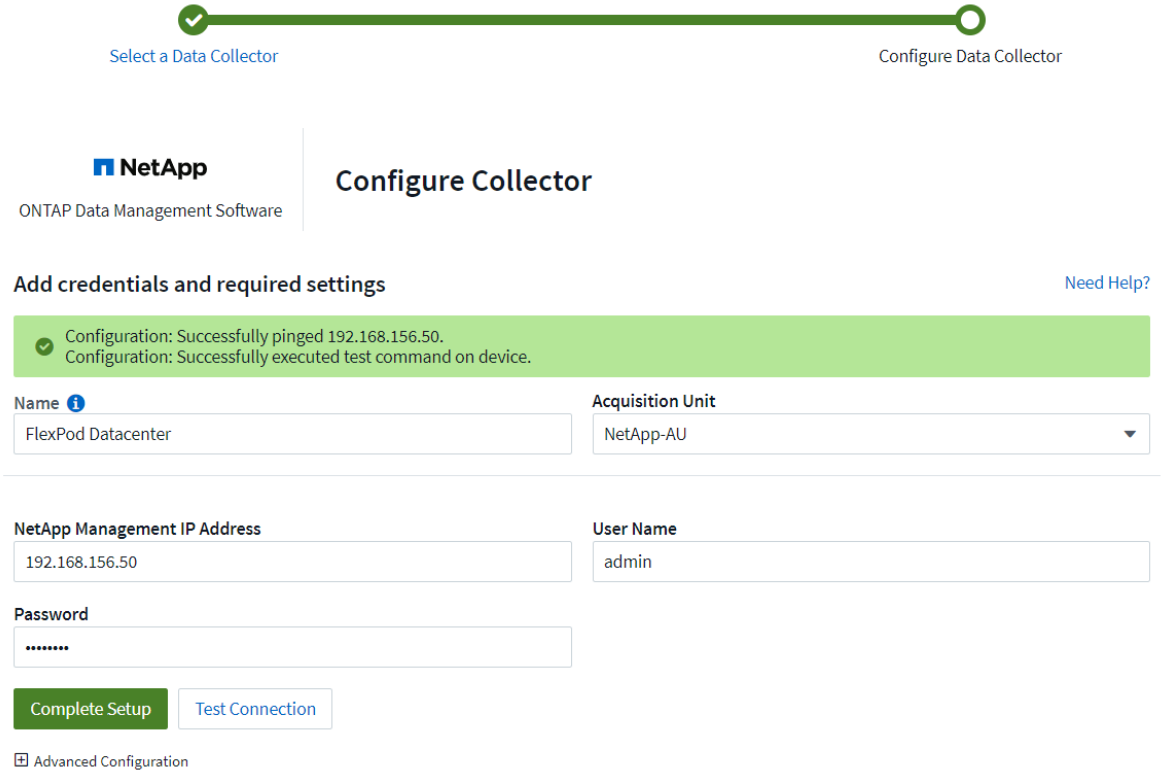


2. Para iniciar um assistente para adicionar o sistema de armazenamento, na página Resumo, clique no botão para criar um coletor de dados. A primeira página exibe todos os sistemas a partir dos quais os dados podem ser coletados. Utilize a barra de pesquisa para procurar ONTAP.



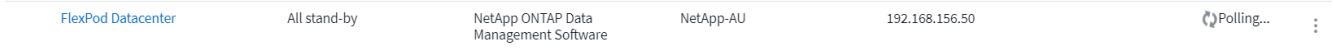
3. Selecione Software de gerenciamento de dados ONTAP.

   É apresentada uma página que lhe permite atribuir um nome à sua implementação e selecionar a Unidade de aquisição que pretende utilizar. Você pode fornecer as informações de conetividade e credenciais para o sistema ONTAP e testar a conexão para confirmar.



4. Clique em concluir configuração.

   O portal retorna à página coletores de dados e o coletor de dados começa sua primeira pesquisa para coletar dados do sistema de armazenamento ONTAP no datacenter FlexPod.



Casos de uso

Com o Cloud Insights configurado e configurado para monitorar sua solução de data

center FlexPod, podemos explorar algumas das tarefas que você pode executar no painel para avaliar e monitorar seu ambiente. Nesta seção, destacamos cinco casos de uso principais para o Cloud Insights:

- Integração com Active IQ
- Explorando painéis em tempo real
- Criando painéis personalizados
- Solução de problemas avançada
- Otimização de storage

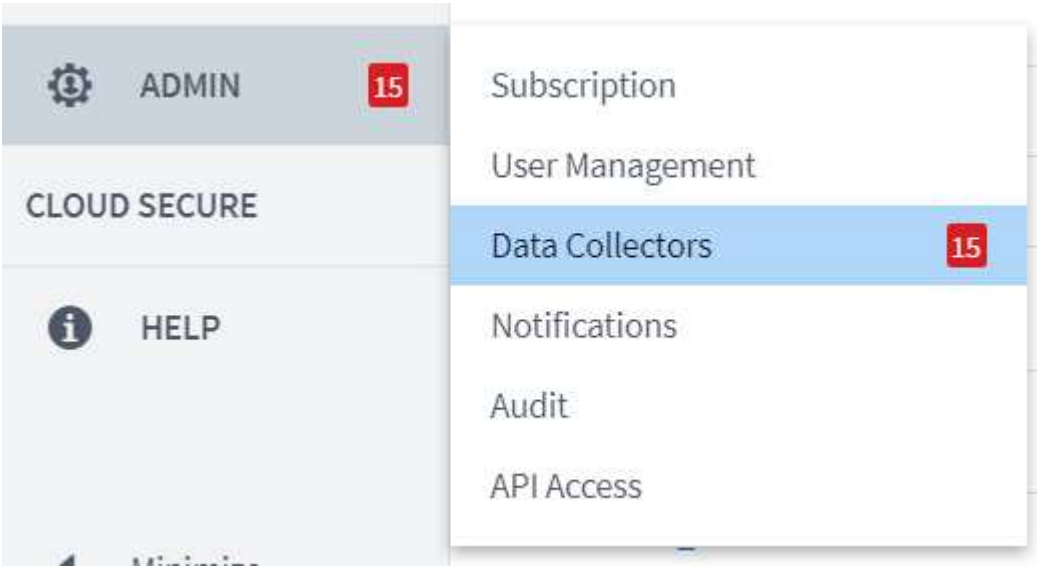
Integração com Active IQ

O Cloud Insights é totalmente integrado à plataforma de monitoramento de storage da Active IQ. Um sistema ONTAP, implantado como parte de uma solução de data center FlexPod, é configurado automaticamente para enviar informações de volta para o NetApp por meio da função AutoSupport, que está integrada em cada sistema. Esses relatórios são gerados em uma base programada, ou dinamicamente sempre que uma falha é detetada no sistema. Os dados comunicados por meio do AutoSupport são agregados e exibidos em painéis de fácil acesso no menu Active IQ no Cloud Insights.

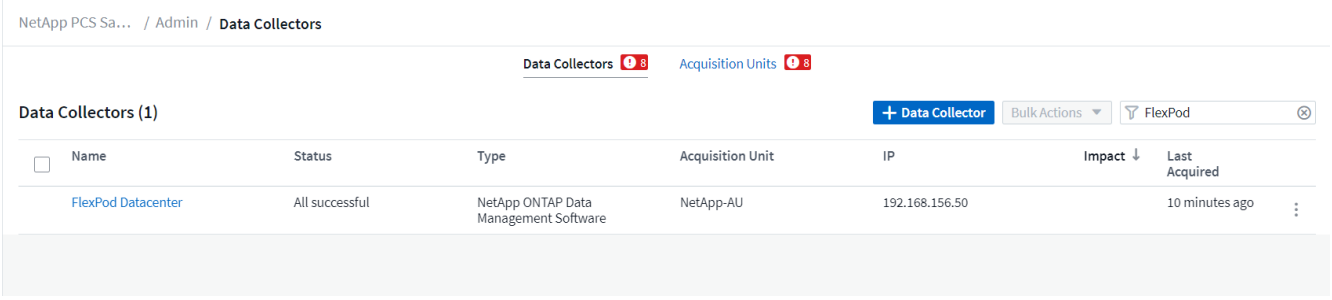
Acesse as informações do Active IQ por meio do painel do Cloud Insights

Para acessar as informações do Active IQ por meio do painel do Cloud Insights, execute as seguintes etapas:

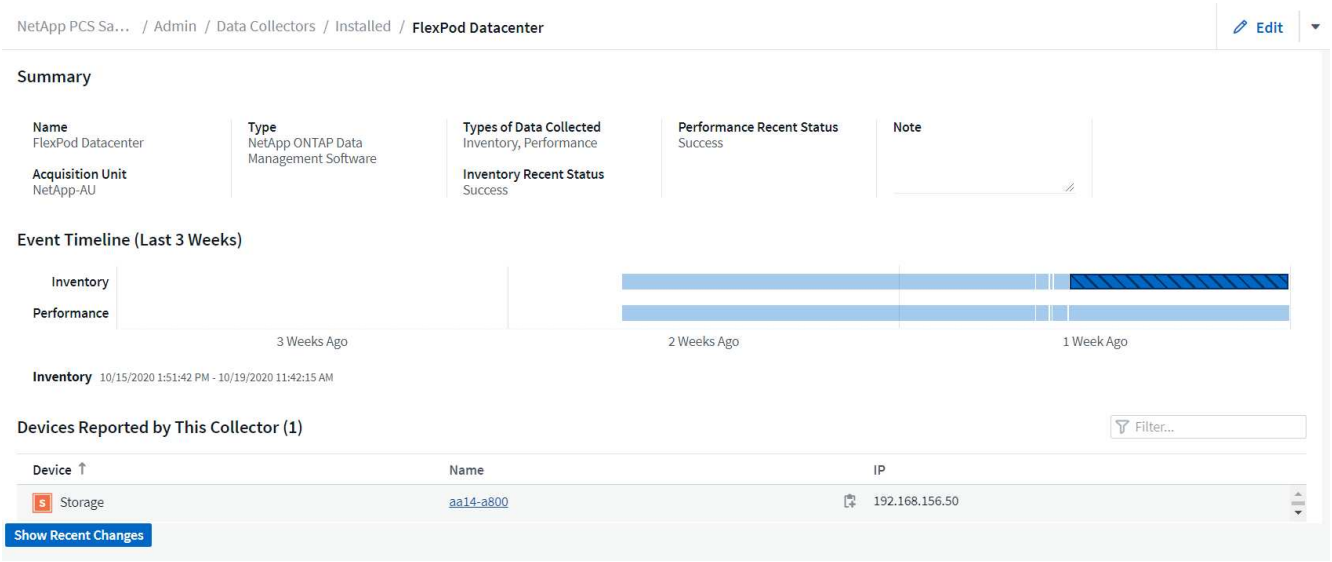
1. Clique na opção Coletor de dados no menu Admin à esquerda.



2. Filtro para o coletor de dados específico em seu ambiente. Neste exemplo, filtramos pelo termo FlexPod.

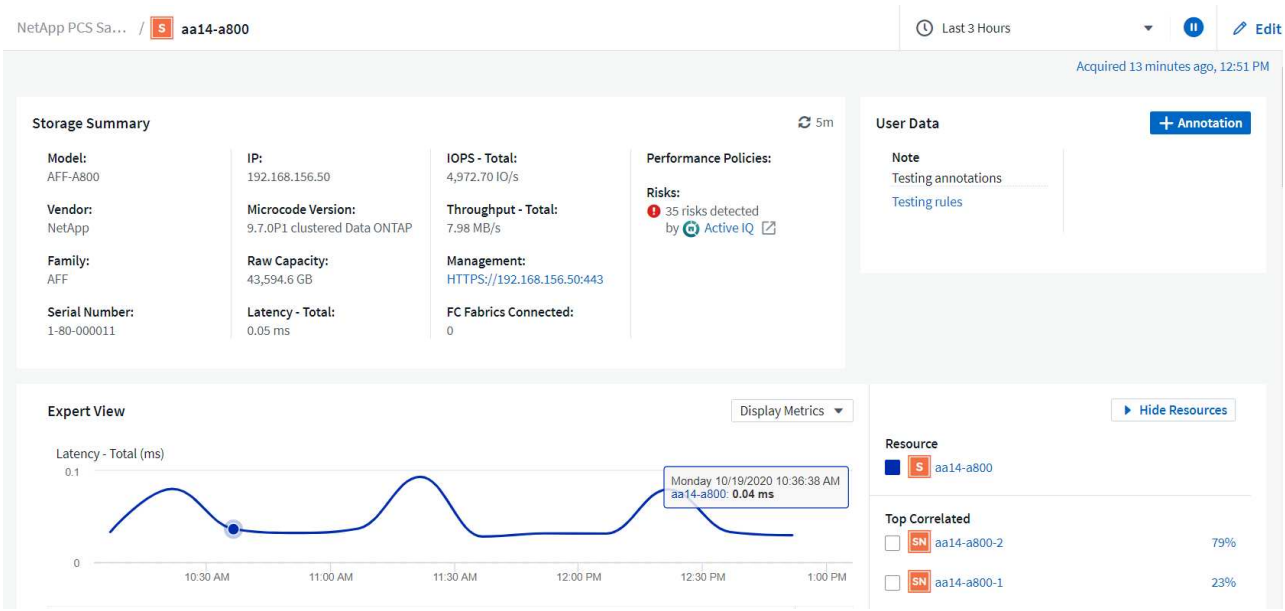


3. Clique no coletor de dados para obter um resumo do ambiente e dos dispositivos que estão sendo monitorados por esse coletor.

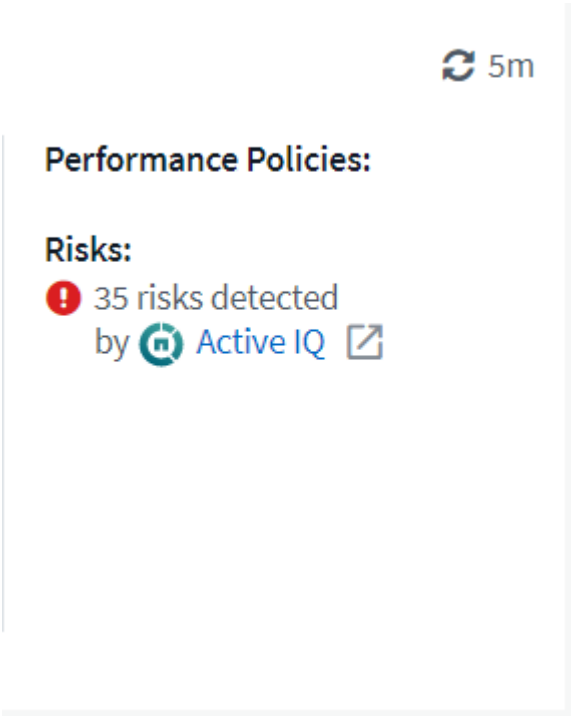


Na lista de dispositivos perto da parte inferior, clique no nome do sistema de armazenamento ONTAP que está a ser monitorizado. Isso exibe um painel de informações coletadas sobre o sistema, incluindo os seguintes detalhes:

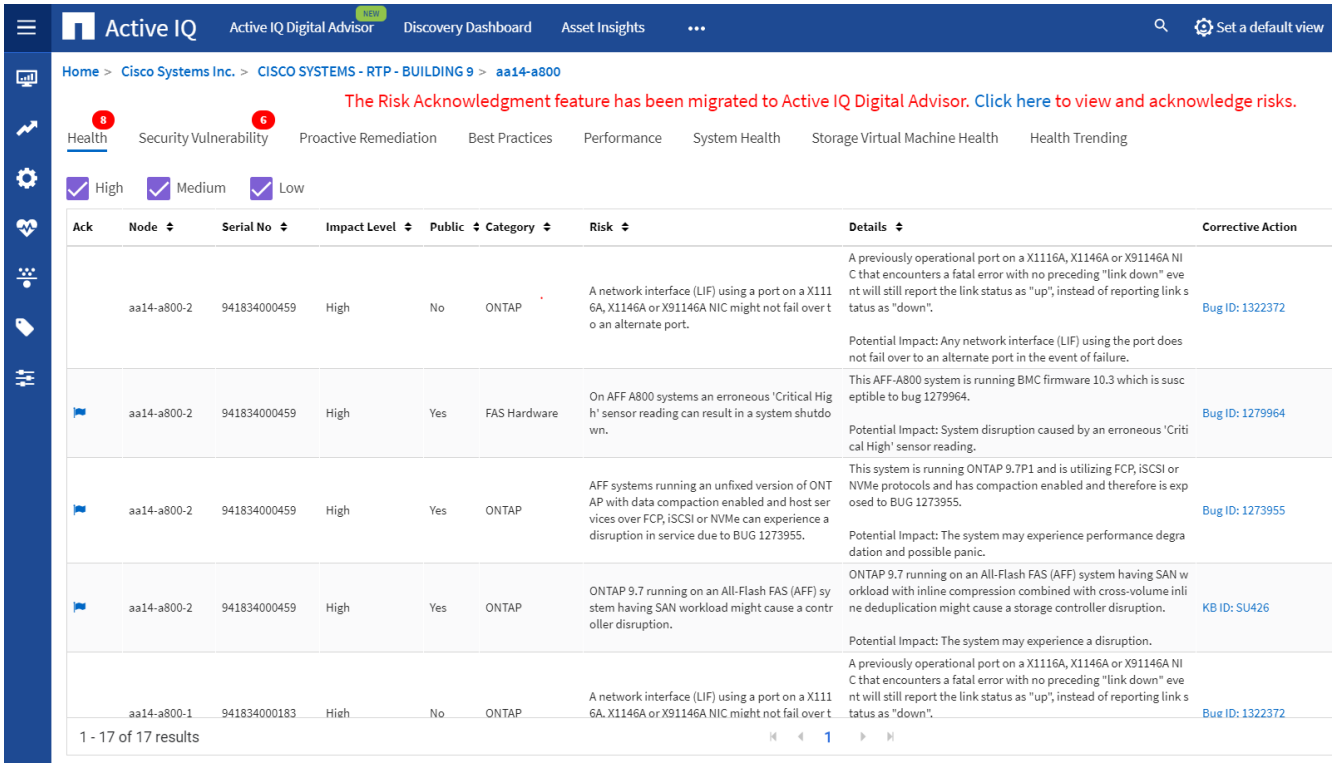
- Modelo
- Família
- Versão do ONTAP
- Capacidade bruta
- IOPS médio
- Latência média
- Taxa de transferência média



Além disso, nesta página, na seção políticas de desempenho, você pode encontrar um link para o NetApp Active IQ.



4. Para abrir uma nova guia do navegador e levá-lo à página de mitigação de riscos, que mostra quais nós são afetados, quão críticos são os riscos e qual é a ação apropriada que precisa ser tomada para corrigir os problemas identificados, clique no link para Active IQ.

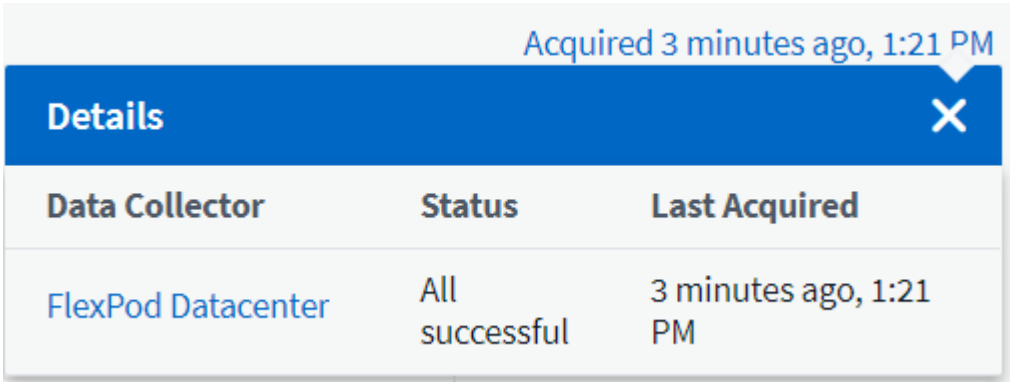


Explore painéis em tempo real

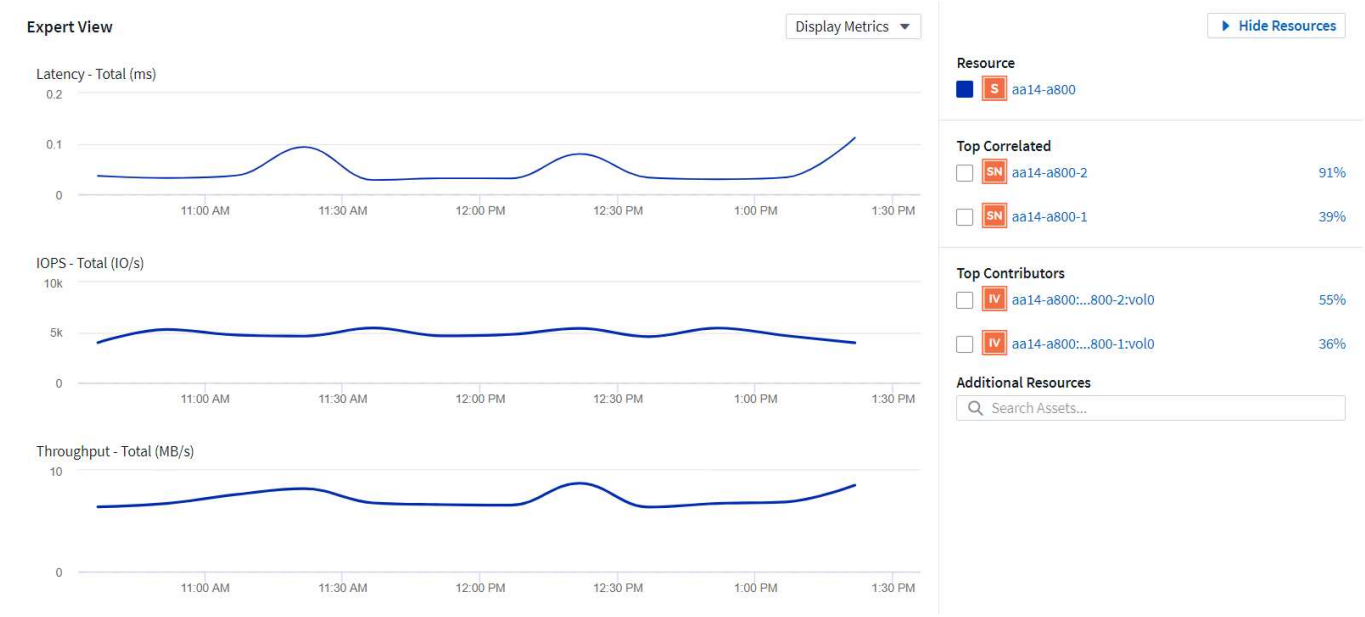
O Cloud Insights pode exibir painéis em tempo real das informações que foram pesquisadas do sistema de storage da ONTAP implantado em uma solução de data center FlexPod. A Unidade de aquisição Cloud Insights recolhe dados em intervalos regulares e preenche o painel do sistema de armazenamento predefinido com as informações recolhidas.

Acesse gráficos em tempo real através do painel do Cloud Insights

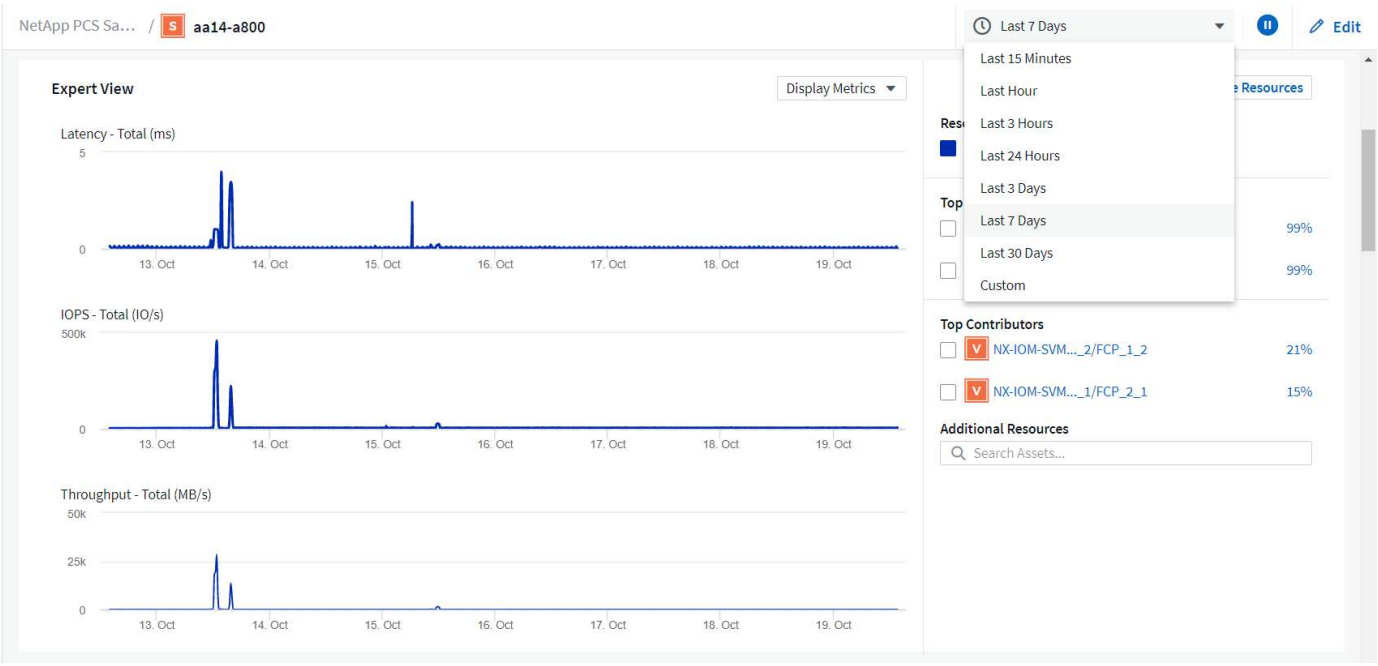
No painel do sistema de armazenamento, você pode ver a última vez que o Data Collector atualizou as informações. Um exemplo disso é mostrado na figura abaixo.



Por padrão, o painel do sistema de armazenamento exibe vários gráficos interativos que mostram métricas de todo o sistema do sistema de armazenamento a ser polled, ou de cada nó individual, incluindo: Latência, IOPS e taxa de transferência, na seção Expert View. Exemplos desses gráficos padrão são mostrados na figura abaixo.



Por padrão, os gráficos mostram informações das últimas três horas, mas você pode definir isso para um número de valores diferentes ou um valor personalizado na lista suspensa próxima à parte superior direita do painel do sistema de armazenamento. Isto é mostrado na figura abaixo.



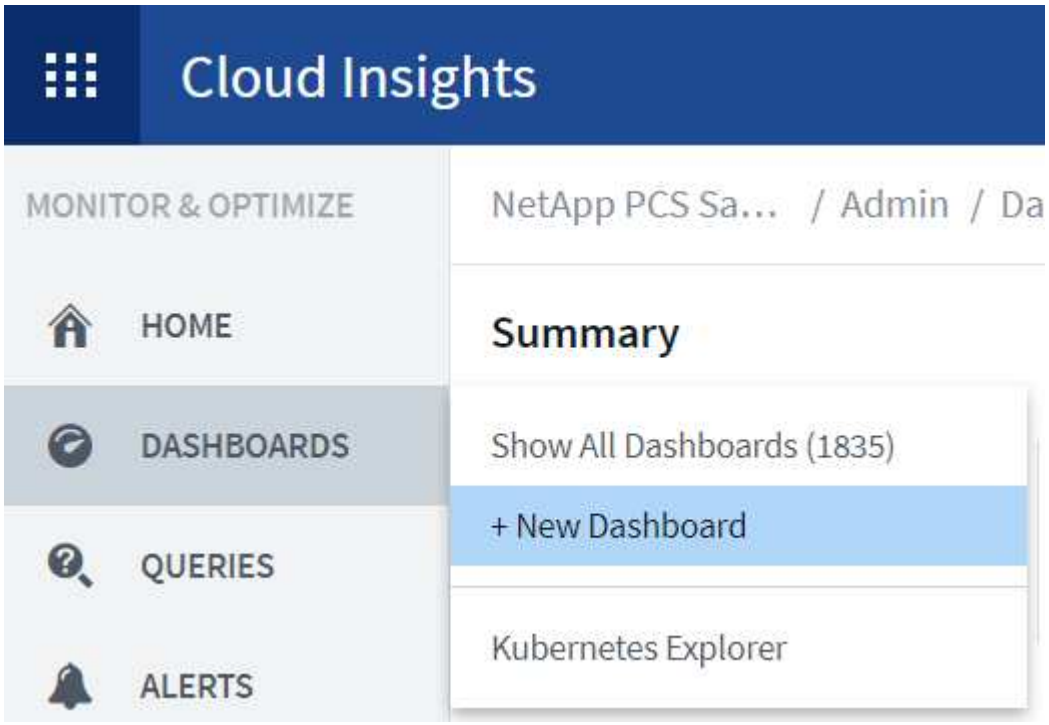
Crie painéis personalizados

Além de usar os painéis padrão que exibem informações em todo o sistema, você pode usar o Cloud Insights para criar painéis totalmente personalizados que permitem que você se concentre no uso de recursos para volumes de storage específicos na solução de data center FlexPod e, assim, os aplicativos implantados na infraestrutura convergente que dependem desses volumes para serem executados com eficiência. Isso pode ajudar você a criar uma melhor visualização de aplicações específicas e dos recursos que elas consomem no ambiente de data center.

Crie um painel personalizado para avaliar os recursos de storage

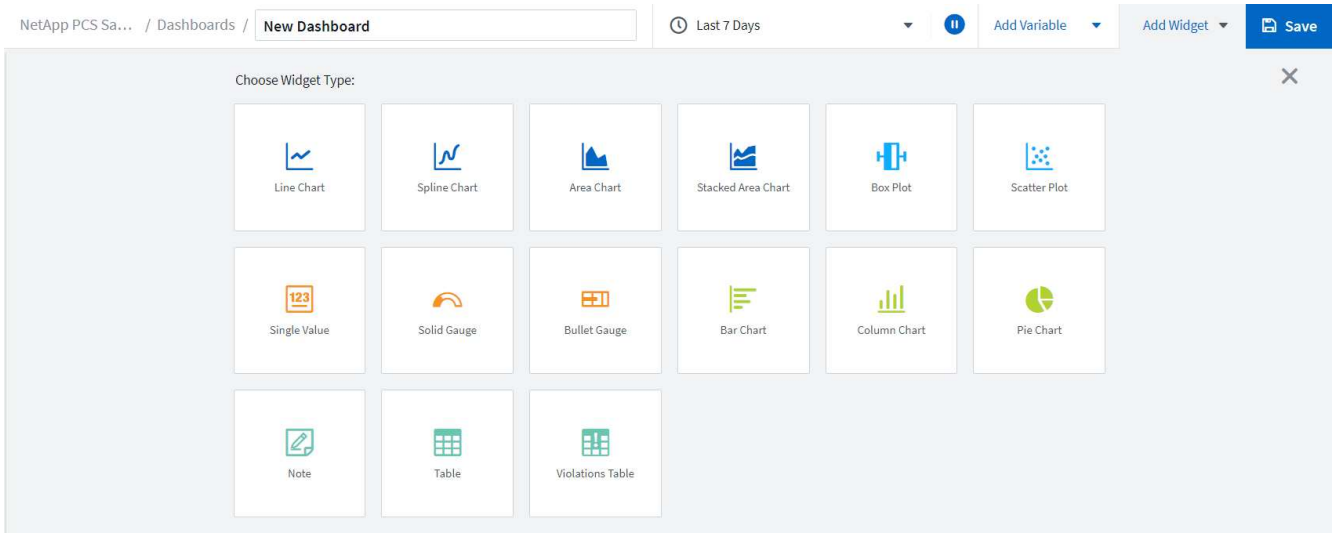
Para criar um painel personalizado para avaliar os recursos de armazenamento, execute as seguintes etapas:

1. Para criar um painel personalizado, passe o Mouse sobre painéis no menu principal do Cloud Insights e clique em novo painel na lista suspensa.



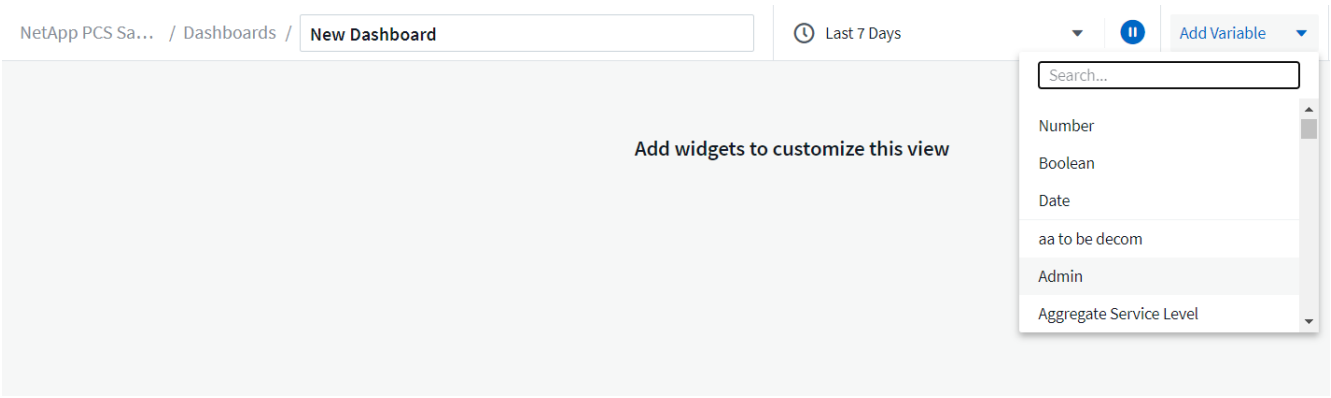
   Abre-se a janela novo painel de instrumentos.

2. Nomeie o painel e selecione o tipo de widget usado para exibir os dados. Você pode selecionar entre vários tipos de gráfico ou até mesmo notas ou tipos de tabela para apresentar os dados coletados.



3. Escolha variáveis personalizadas no menu Adicionar variável.

   Isso permite que os dados apresentados sejam focados para exibir fatores mais específicos ou especializados.



4. Para criar um painel personalizado, selecione o tipo de widget que você gostaria de usar, por exemplo, um gráfico de pizza para exibir a utilização do armazenamento por volume:

   a. Selecione o widget Gráfico de pizza na lista suspensa Adicionar widget.

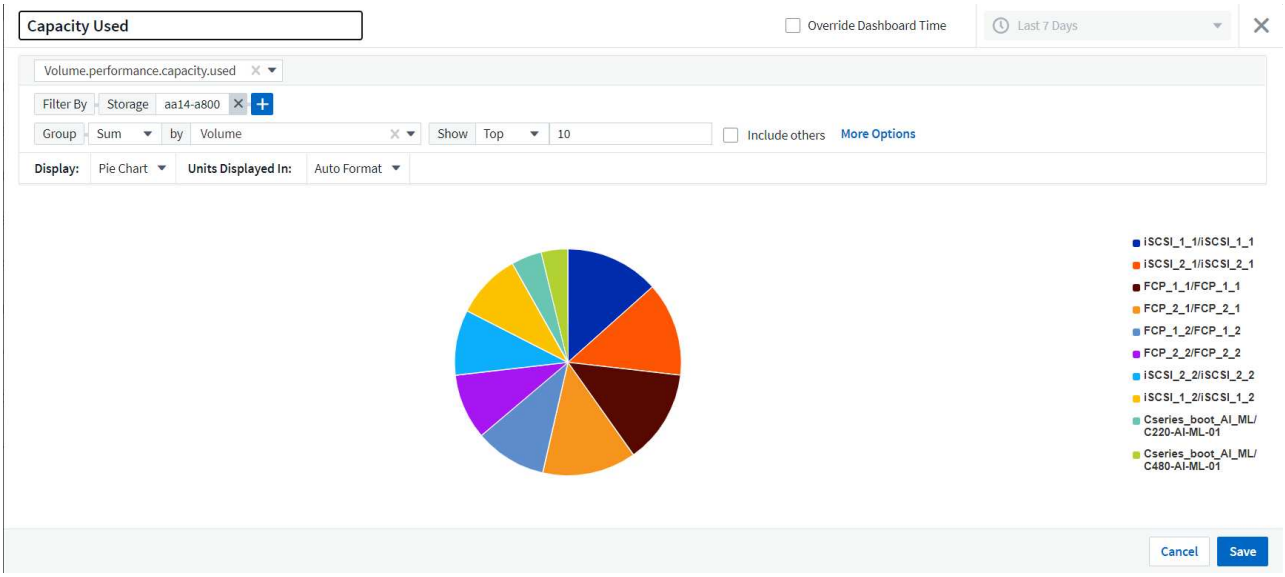
   b. Nomeie o widget com um identificador descritivo, como `Capacity Used`.

   c. Selecione o objeto que deseja exibir. Por exemplo, você pode pesquisar pelo volume do termo-chave e `volume.performance.capacity.used` selecionar .

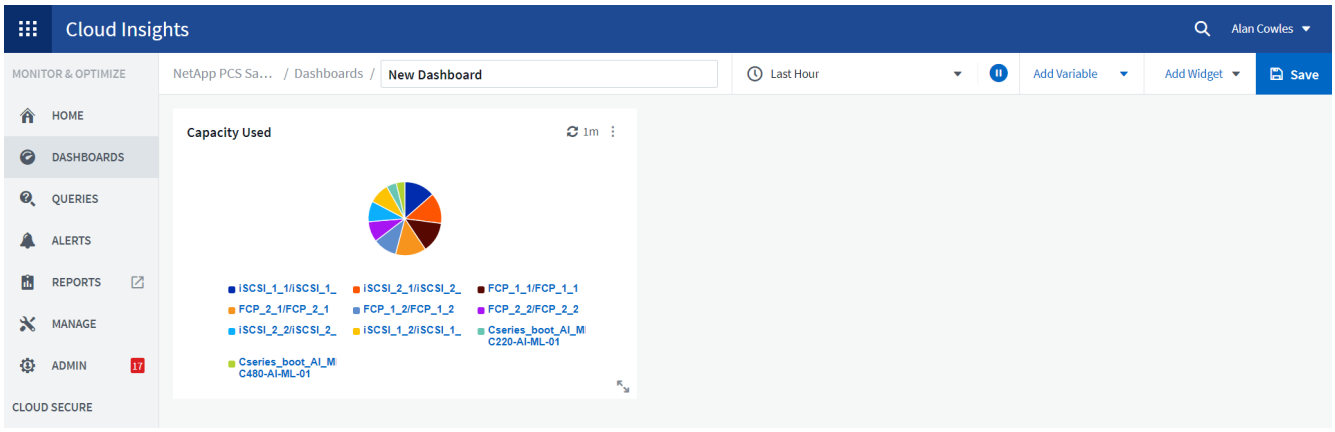
   d. Para filtrar por sistemas de storage, use o filtro e digite o nome do sistema de storage na solução FlexPod Datacenter.

   e. Personalize as informações a serem exibidas. Por padrão, essa seleção mostra os volumes de dados do ONTAP e lista os 10 principais.

   f. Para salvar o painel personalizado, clique em Salvar.



   Depois de salvar o widget personalizado, o navegador retorna à página novo painel, onde exibe o widget recém-criado e permite a ação interativa a ser realizada, como modificar o período de polling de dados.



Solução de problemas avançada

O Cloud Insights permite que métodos avançados de solução de problemas sejam aplicados a qualquer ambiente de storage em uma infraestrutura convergente do data center FlexPod. Usando componentes de cada um dos recursos mencionados acima: Integração com Active IQ, painéis padrão com estatísticas em tempo real e painéis personalizados, os problemas que podem surgir são detetados com antecedência e resolvidos rapidamente. Usando a lista de riscos no Active IQ, um cliente pode encontrar erros de configuração relatados que podem levar a problemas ou descobrir bugs que foram relatados e corrigidos versões de código que podem remediá-los. Observar os dashboards em tempo real na página inicial do Cloud Insights pode ajudar a descobrir padrões de desempenho do sistema que podem ser um indicador precoce de um problema em ascensão e ajudar a resolvê-lo rapidamente. Por fim, a capacidade de criar painéis personalizados permite que os clientes se concentrem nos ativos mais importantes de sua infraestrutura e monitorem os mesmos diretamente para garantir que eles possam atender aos objetivos de continuidade de negócios.

Otimização de storage

Além da solução de problemas, é possível usar os dados coletados pela Cloud Insights para otimizar o sistema de storage ONTAP implantado em uma solução de infraestrutura convergente do FlexPod Datacenter. Se um volume mostrar uma alta latência, talvez porque várias VMs com demandas de alta performance estejam compartilhando o mesmo datastore, essas informações serão exibidas no painel do Cloud Insights. Com essas informações, um administrador de storage pode optar por migrar uma ou mais VMs para outros volumes, migrar volumes de storage entre camadas de agregados ou entre nós no sistema de storage ONTAP, o que resulta em um ambiente otimizado para performance. As informações obtidas com a integração do Active IQ com o Cloud Insights podem destacar problemas de configuração que levam a um desempenho inferior ao esperado e fornecer a ação corretiva recomendada que, se implementada, pode corrigir quaisquer problemas e garantir um sistema de armazenamento otimizado.

Vídeos e demonstrações

Você pode ver uma demonstração em vídeo do uso do NetApp Cloud Insights para avaliar os recursos em um ambiente "aqui"local .

Você pode ver uma demonstração em vídeo do uso do NetApp Cloud Insights para monitorar a infraestrutura e definir limites de alerta para a infraestrutura "aqui".

Você pode ver uma demonstração em vídeo do uso do NetApp Cloud Insights para avaliar aplicativos individuais no ambiente "aqui".

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes sites:

- Documentação do produto Cisco

  "https://www.cisco.com/c/en/us/support/index.html"

- Data center FlexPod

  "https://www.flexpod.com"

- NetApp Cloud Insights

  "https://cloud.netapp.com/cloud-insights"

- Documentação do produto NetApp

  "https://docs.netapp.com"

FlexPod com FabricPool: Disposição em camadas de dados inativos no Amazon AWS S3

TR-4801: FlexPod com FabricPool - disposição em camadas de dados inativos no Amazon AWS S3

Scott Kovacs, NetApp

Os preços do storage flash continuam a cair, tornando-os disponíveis para workloads e aplicações que não eram consideradas anteriormente candidatas ao storage flash. No entanto, fazer o uso mais eficiente do investimento em armazenamento ainda é extremamente importante para os gerentes DE TI. Os departamentos DE TI continuam pressionados a fornecer serviços de alto desempenho com pouco ou nenhum aumento do orçamento. Para ajudar a atender a essas necessidades, o NetApp FabricPool permite que você aproveite a economia da nuvem movendo dados pouco usados de storage flash caro no local para uma camada de storage mais econômica na nuvem pública. A migração de dados que não são acessados com frequência para a nuvem libera espaço valioso de storage flash em sistemas AFF ou FAS para fornecer mais capacidade para workloads essenciais aos negócios para a camada flash de alta performance.

Este relatório técnico analisa o recurso de disposição em camadas de dados do FabricPool do NetApp ONTAP no contexto de uma arquitetura de infraestrutura convergente do FlexPod da NetApp e do Cisco. Você deve se familiarizar com a arquitetura da infraestrutura convergente do data center do FlexPod e o software de storage do ONTAP para se beneficiar totalmente dos conceitos discutidos neste relatório técnico. Com base na familiaridade com o FlexPod e o ONTAP, discutimos o FabricPool, como ele funciona e como ele pode ser usado para uso mais eficiente do storage flash no local. Grande parte do conteúdo deste relatório é abordado com mais detalhes na "TR-4598 melhores práticas da FabricPool" documentação do produto ONTAP e em outras documentações. O conteúdo foi condensado para uma infraestrutura do FlexPod e não cobre

completamente todos os casos de uso do FabricPool. Todos os recursos e conceitos examinados estão disponíveis no ONTAP 9.6.

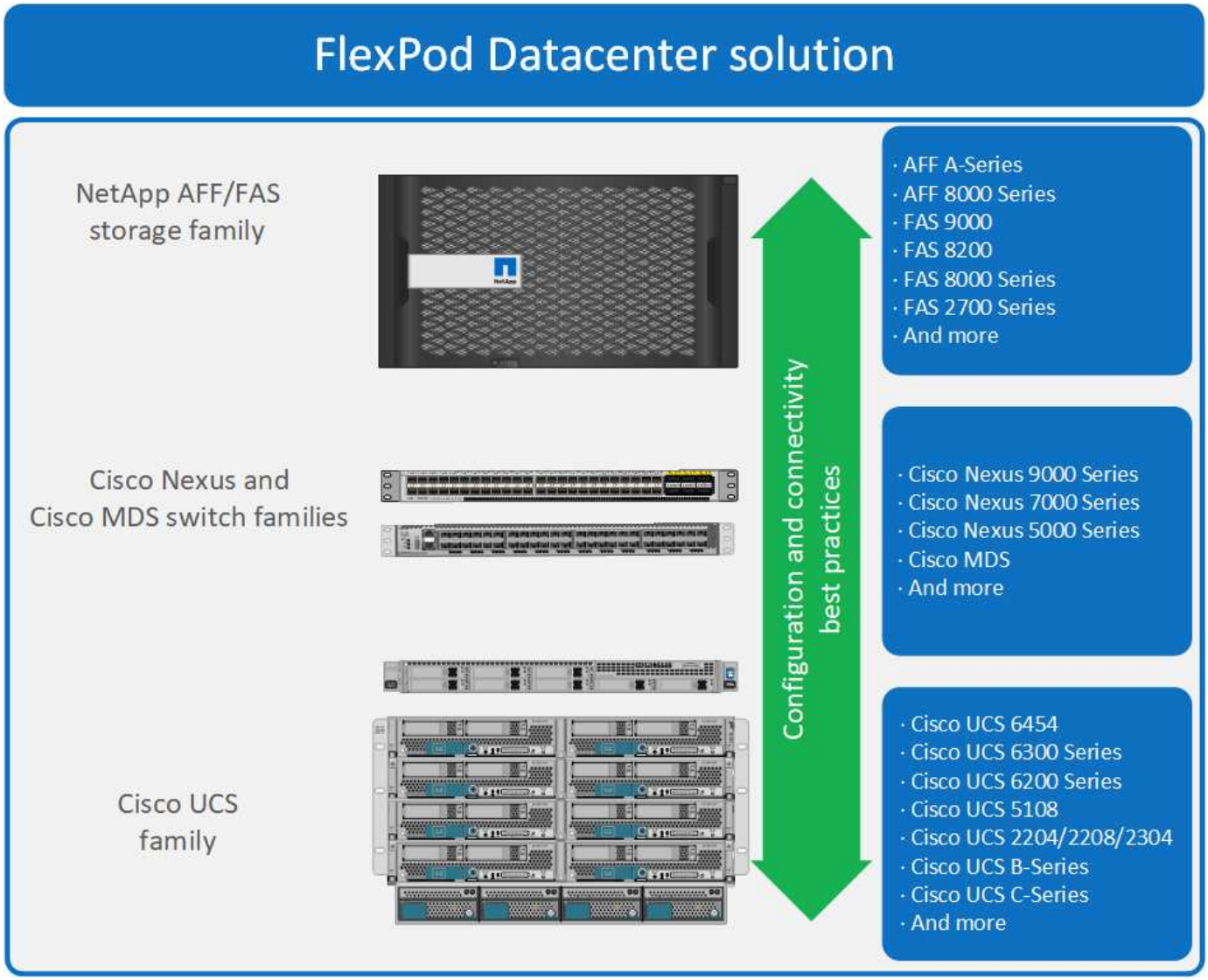
Para mais informações sobre o FlexPod, consulte "TR-4036 FlexPod Datacenter Especificações técnicas".

Visão geral e arquitetura do FlexPod

Visão geral do FlexPod

O FlexPod é um conjunto definido de hardware e software que forma uma base integrada para soluções virtualizadas e não virtualizadas. O FlexPod inclui armazenamento NetApp AFF, rede Cisco Nexus, rede de storage Cisco MDS, o sistema de computação unificada da Cisco (Cisco UCS) e o software VMware vSphere em um único pacote. O design é flexível o suficiente para que a rede, a computação e o storage possam se encaixar em um rack de data center ou possa ser implantado de acordo com o design do data center do cliente. A densidade da porta permite que os componentes de rede acomodem várias configurações.

Um dos benefícios da arquitetura FlexPod é a capacidade de personalizar ou flexibilizar o ambiente de acordo com os requisitos de um cliente. Uma unidade FlexPod pode ser facilmente dimensionada conforme os requisitos e a demanda mudam. Uma unidade pode ser dimensionada tanto para cima (adicionando recursos a uma unidade FlexPod) quanto para fora (adicionando mais unidades FlexPod). A arquitetura de referência do FlexPod destaca a resiliência, o custo-benefício e a facilidade de implantação de uma solução de storage baseada em Fibre Channel e IP. Um sistema de storage capaz de atender a vários protocolos em uma única interface oferece aos clientes opções e protege seu investimento porque ela é realmente uma arquitetura completa. A figura a seguir mostra muitos dos componentes de hardware do FlexPod.

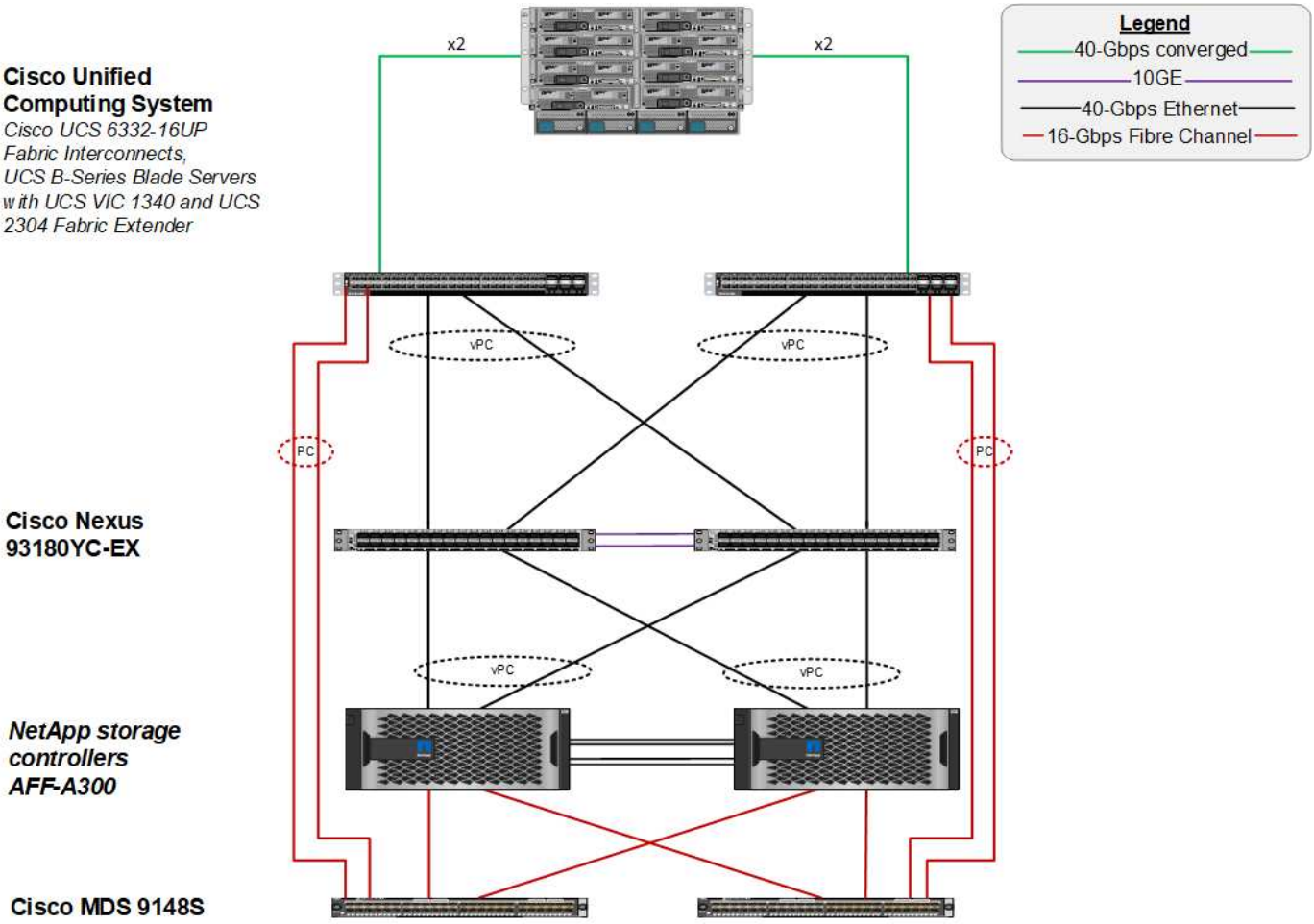


Arquitetura da FlexPod

A figura a seguir mostra os componentes de uma solução VMware vSphere e FlexPod e as conexões de rede necessárias para interconexões de malha do Cisco UCS 6454. Este design tem os seguintes componentes:

- Conexões Ethernet de 40GB GB canalizadas por porta entre o chassi blade Cisco UCS 5108 e a malha Cisco UCS interconeta
- 40GB conexões Ethernet entre a interconexão de malha Cisco UCS e o Cisco Nexus 9000
- 40GB conexões Ethernet entre o Cisco Nexus 9000 e a matriz de armazenamento NetApp AFF A300

Essas opções de infraestrutura expandiram-se com a introdução dos switches MDS do Cisco entre a interconexão de malha do Cisco UCS e o NetApp AFF A300. Essa configuração fornece hosts com inicialização FC com acesso em nível de bloco FC de 16GB GB ao storage compartilhado. A arquitetura de referência reforça a estratégia "wire-Once", porque, à medida que o armazenamento adicional é adicionado à arquitetura, não é necessário desativar desde os hosts até a interconexão de malha Cisco UCS.



FabricPool

Visão geral do FabricPool

O FabricPool é uma solução de storage híbrido no ONTAP que usa um agregado all-flash (SSD) como uma categoria de performance e um armazenamento de objetos em um serviço de nuvem pública como uma categoria de nuvem. Essa configuração permite a movimentação de dados baseada em políticas, dependendo se os dados são acessados ou não com frequência. O FabricPool é compatível com ONTAP para agregados AFF e all-SSD em plataformas FAS. O Data Processing é executado no nível do bloco, com blocos de dados acessados com frequência na camada de desempenho all-flash marcados como blocos ativos e acessados com pouca frequência marcados como inativos.

O uso do FabricPool ajuda a reduzir os custos de storage sem comprometer a performance, a eficiência, a segurança ou a proteção. O FabricPool é transparente para as aplicações empresariais e aproveita as eficiências de nuvem ao reduzir o TCO de storage sem precisar rearquitetar a infraestrutura de aplicações.

O FlexPod pode se beneficiar das funcionalidades de disposição em camadas de storage do FabricPool para usar mais eficiência o storage flash ONTAP. As máquinas virtuais (VMs) inativas, modelos de VM pouco usados e backups de VMs do NetApp SnapCenter para vSphere podem consumir espaço valioso no volume do datastore. Mover dados inativos para a camada de nuvem libera espaço e recursos para aplicações de alta performance e essenciais hospedadas na infraestrutura do FlexPod.

Os protocolos Fibre Channel e iSCSI geralmente demoram mais tempo antes de ocorrerem um tempo limite (60 a 120 segundos), mas eles não tentam estabelecer uma conexão da mesma maneira que os protocolos nas o fazem. Se um protocolo SAN expirar, o aplicativo deve ser reiniciado. Mesmo uma breve interrupção pode ser desastrosa para aplicativos de produção usando protocolos SAN, porque não há como garantir a conetividade com nuvens públicas. Para evitar esse problema, a NetApp recomenda o uso de nuvens privadas ao dispor dados em camadas acessados por protocolos SAN.

No ONTAP 9.6, o FabricPool se integra a todos os principais fornecedores de nuvem pública: Alibaba Cloud Object Storage Service, Amazon AWS S3, Google Cloud Storage, IBM Cloud Object Storage e Microsoft Azure Blob Storage. Esse relatório concentra o storage do Amazon AWS S3 como a camada de objeto de nuvem escolhida.

O agregado composto

Uma instância do FabricPool é criada associando um agregado flash ONTAP a um armazenamento de objetos na nuvem, como um bucket do AWS S3, para criar um agregado composto. Quando os volumes são criados dentro do agregado composto, eles podem aproveitar as funcionalidades de disposição em camadas do FabricPool. Quando os dados são gravados no volume, o ONTAP atribui uma temperatura a cada um dos blocos de dados. Quando o bloco é escrito pela primeira vez, é atribuída uma temperatura de quente. Com o passar do tempo, se os dados não forem acessados, eles passam por um processo de resfriamento até que finalmente seja atribuído um status de frio. Esses blocos de dados acessados com pouca frequência são dispostos fora do agregado SSD de desempenho e no armazenamento de objetos na nuvem.

O período de tempo entre quando um bloco é designado como inativo e quando é movido para o storage de objetos em nuvem é modificado pela política de disposição em categorias de volume no ONTAP. Maior granularidade é obtida modificando as configurações do ONTAP que controlam o número de dias necessários para que um bloco fique frio. Os candidatos à disposição em camadas de dados são snapshots de volume tradicionais, backups de VM do SnapCenter para vSphere e outros backups baseados em Snapshot do NetApp e quaisquer blocos pouco usados em um datastore do vSphere, como modelos de VM e dados de VM acessados com pouca frequência.

Relatórios de dados inativos

O relatório de dados inativos (IDR) está disponível no ONTAP para ajudar a avaliar a quantidade de dados inativos que podem ser dispostos de um agregado. O IDR é habilitado por padrão no ONTAP 9.6 e usa uma política de resfriamento padrão de 31 dias para determinar quais dados no volume estão inativos.

A quantidade de dados inativos em camadas depende das políticas de disposição em camadas definidas no volume. Essa quantidade pode ser diferente da quantidade de dados frios detetados pelo IDR usando o período de resfriamento padrão de 31 dias.

Criação de objetos e movimentação de dados

O FabricPool funciona no nível de bloco do NetApp WAFL, resfriando blocos, concatenando-os em objetos de storage e migrando esses objetos para uma camada de nuvem. Cada objeto FabricPool é 4MB e é composto por 1.024 4KB blocos. O tamanho do objeto é fixado em 4MB com base nas recomendações de desempenho dos principais fornecedores de nuvem e não pode ser alterado. Se os blocos frios forem lidos e ficarem quentes, somente os blocos solicitados no objeto 4MB serão obtidos e movidos de volta para o nível de desempenho. Nem todo o objeto nem todo o arquivo são migrados de volta. Apenas os blocos necessários são migrados.

Se o ONTAP detetar uma oportunidade de readahheads sequenciais, ele solicita que sejam bloqueados da categoria de nuvem antes que eles sejam lidos para melhorar a performance.

Por padrão, os dados são movidos para a categoria de nuvem somente quando o agregado de desempenho é maior que 50% utilizado. Esse limite pode ser definido para uma porcentagem menor para permitir que uma quantidade menor de storage de dados na categoria flash de performance seja movida para a nuvem. Isso pode ser útil se a estratégia de disposição em camadas for mover dados inativos somente quando o agregado estiver próximo da capacidade.

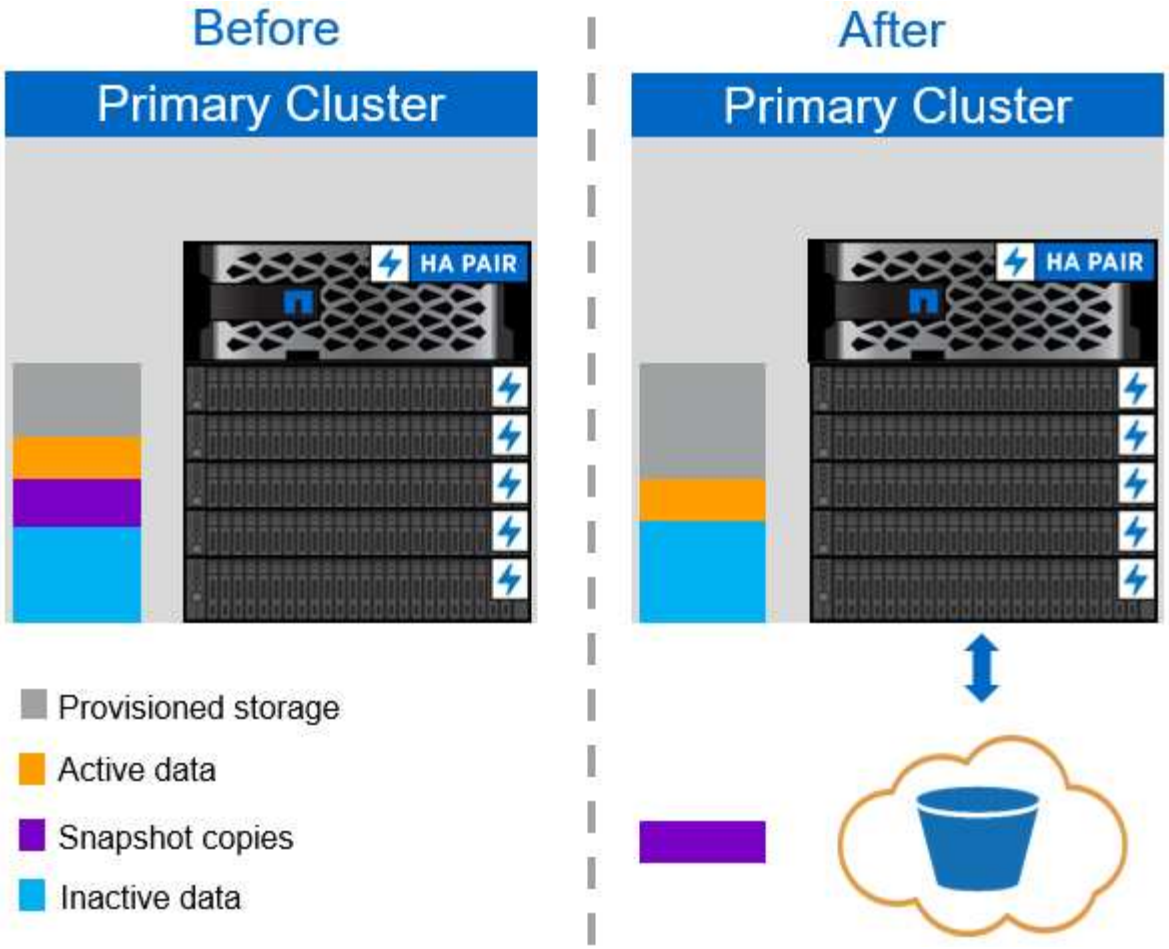
Se a utilização de categorias de performance tiver capacidade superior a 70%, os dados inativos serão lidos diretamente na categoria de nuvem sem serem gravados de volta na categoria de performance. Ao impedir a gravação de dados inativos em agregados altamente usados, o FabricPool preserva o agregado para dados ativos.

Recupere espaço em camadas de performance

Como mencionado anteriormente, o principal caso de uso do FabricPool é facilitar o uso mais eficiente do storage flash no local de alta performance. Dados inativos na forma de snapshots de volume e backups de VMs da infraestrutura virtual FlexPod podem ocupar uma quantidade significativa de storage flash caro. Com a implementação de uma das duas políticas de disposição em camadas: Somente snapshot ou Automático.

Política de disposição em camadas somente snapshot

A política de disposição em camadas somente Snapshot, ilustrada na figura a seguir, move os dados de snapshot de volume frio e os backups do SnapCenter para vSphere de VMs que estão ocupando espaço, mas não estão compartilhando blocos com o sistema de arquivos ativo em um armazenamento de objetos na nuvem. A política de disposição em camadas somente Snapshot move blocos de dados inativos para a camada de nuvem. Se for necessária uma restauração, os blocos inativos na nuvem ficam ativos e são movidos de volta para a camada flash de performance no local.

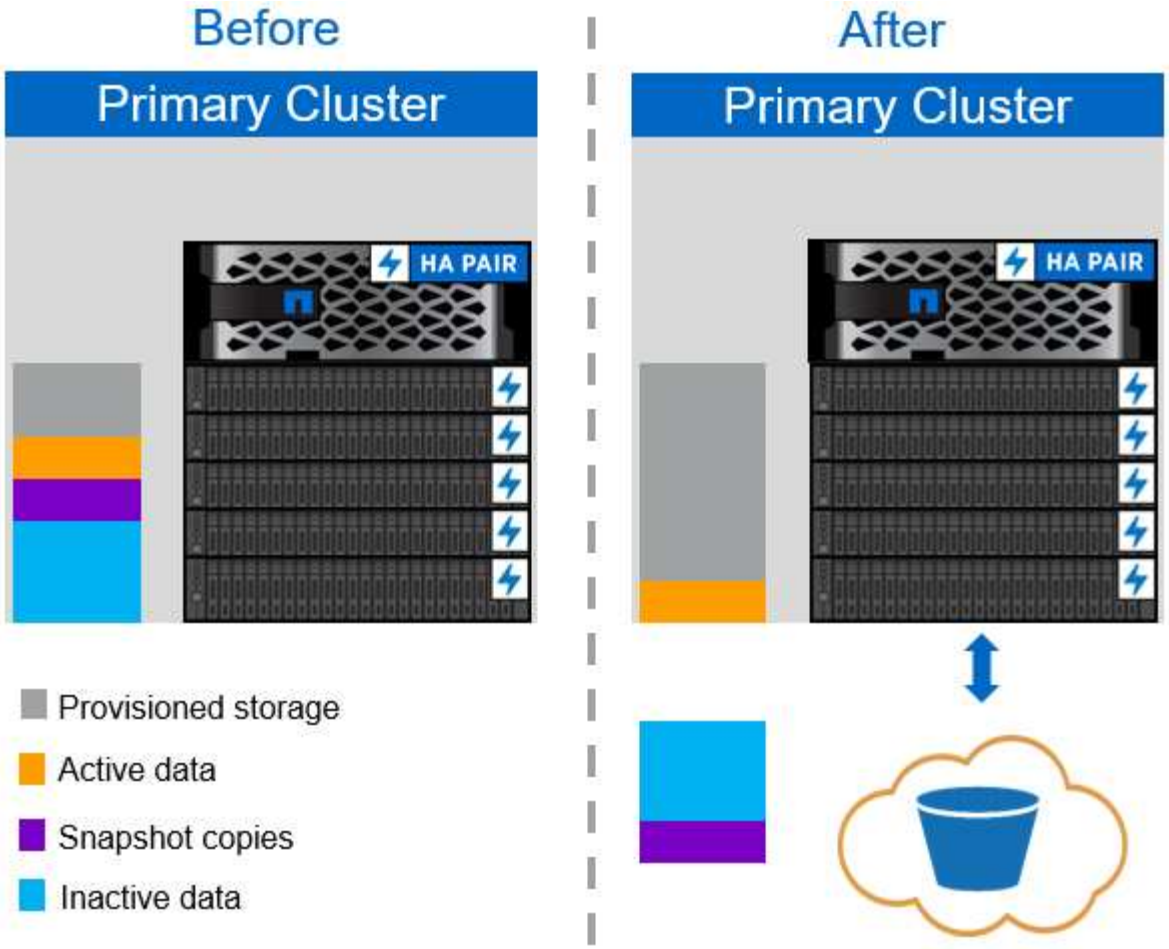


Política de disposição automática em categorias

A política de disposição automática em camadas do FabricPool, ilustrada na figura a seguir, além de migrar blocos de dados de snapshot frio para a nuvem, além de migrar blocos inativos no sistema de arquivos ativo. Isso pode incluir modelos de VM e quaisquer dados de VM não utilizados no volume do datastore. Que blocos frios são movidos é controlado pela `tiering-minimum-cooling-days` definição do volume. Se os blocos frios do nível de nuvem forem lidos aleatoriamente por uma aplicação, esses blocos ficarão ativos e serão devolvidos ao nível de performance. No entanto, se os blocos inativos forem lidos por um processo sequencial, como um antivírus, os blocos permanecem frios e persistem no armazenamento de objetos em nuvem; eles não são movidos de volta para o nível de desempenho.

Ao usar a política de disposição automática em camadas, os blocos acessados com pouca frequência são retirados da camada de nuvem na velocidade da conectividade da nuvem. Isso pode afetar o desempenho da VM se o aplicativo for sensível à latência, o que deve ser considerado antes de usar a política de disposição automática em camadas no datastore. A NetApp recomenda a colocação de LIFs Intercluster em portas com uma velocidade de 10GbEMbps para um desempenho adequado.

O profiler de armazenamento de objetos deve ser usado para testar a latência e a taxa de transferência ao armazenamento de objetos antes de anexá-lo a um agregado FabricPool.



Todas as políticas de disposição em camadas

Diferentemente das políticas Auto e somente Snapshot, a política de categorias all move volumes inteiros de dados imediatamente para a camada de nuvem. Essa política é mais adequada para proteção de dados secundária ou volumes de arquivamento para os quais os dados devem ser mantidos para fins históricos ou regulatórios, mas raramente acessados. A política All (tudo) não é recomendada para volumes do VMware datastore porque todos os dados gravados no datastore são movidos imediatamente para a camada de nuvem. Operações de leitura subsequentes são executadas a partir da nuvem e podem potencialmente introduzir problemas de desempenho para VMs e aplicações que residem no volume do datastore.

Segurança

A segurança é uma preocupação central para a nuvem e para o FabricPool. Todos os recursos de segurança nativos do ONTAP são compatíveis na camada de performance, e a movimentação dos dados é protegida à medida que são transferidos para a camada de nuvem. O FabricPool usa o "AES-256-GCM" algoritmo de criptografia na camada de performance e mantém essa criptografia de ponta a ponta na camada de nuvem. Os blocos de dados movidos para o armazenamento de objetos em nuvem são protegidos com TLS (Transport Layer Security) v1,2 para manter a confidencialidade e a integridade dos dados entre as camadas de storage.

A comunicação com o armazenamento de objetos em nuvem através de uma conexão não criptografada é suportada, mas não recomendada pelo NetApp.

Criptografia de dados

A criptografia de dados é vital para a proteção da propriedade intelectual, informações comerciais e informações de clientes pessoalmente identificáveis. O FabricPool é totalmente compatível com o NetApp volume Encryption (NVE) e o NetApp Storage Encryption (NSE) para manter as estratégias de proteção de dados existentes. Todos os dados criptografados na camada de performance permanecem criptografados quando migrados para a camada de nuvem. As chaves de criptografia do lado do cliente são propriedade do ONTAP e as chaves de criptografia do armazenamento de objetos do lado do servidor são propriedade do respetivo armazenamento de objetos na nuvem. Todos os dados não criptografados com NVE são criptografados com o algoritmo AES-256-GCM. Não são suportadas outras cifras AES-256.

O uso de NSE ou NVE é opcional e não é necessário para usar o FabricPool.

Requisitos da FabricPool

O FabricPool requer o ONTAP 9.2 ou posterior e o uso de agregados SSD em qualquer uma das plataformas listadas nesta seção. Requisitos adicionais do FabricPool dependem da categoria de nuvem anexada. Para plataformas AFF de nível básico que têm uma capacidade fixa e relativamente pequena, como o NetApp AFF C190, o FabricPool pode ser altamente eficaz na migração de dados inativos para a camada de nuvem.

Plataformas

O FabricPool é compatível com as seguintes plataformas:

- NetApp AFF
  - A800
  - A700S, A700
  - A320, A300
  - A220, A200
  - C190
  - AFF8080, AFF8060 E AFF8040
- NetApp FAS
  - FAS9000
  - FAS8200
  - FAS8080, FAS8060 E FAS8040
  - FAS2750, FAS2720
  - FAS2650, FAS2620

Somente agregados SSD em plataformas FAS podem usar o FabricPool.

- Categorias de nuvem
  - Alibaba Cloud Object Storage Service (padrão, acesso não frequente)
  - Amazon S3 (padrão, IA padrão, IA de uma zona, disposição inteligente em categorias)

- Serviços de nuvem comerciais da Amazon (C2S)
- Google Cloud Storage (multiregional, regional, Nearline, Coldline)
- IBM Cloud Object Storage (padrão, Vault, Cold Vault, Flex)
- Microsoft Azure Blob Storage (ativo e inativo)

LIFs entre clusters

Os pares de alta disponibilidade de cluster (HA) que usam FabricPool exigem duas interfaces lógicas (LIFs) entre clusters para se comunicar com a camada de nuvem. A NetApp recomenda a criação de um LIF entre clusters em pares de HA adicionais para anexar camadas de nuvem a agregados também nesses nós.

O LIF que o ONTAP usa para se conetar ao armazenamento de objetos AWS S3 deve estar em uma porta 10Gbps.

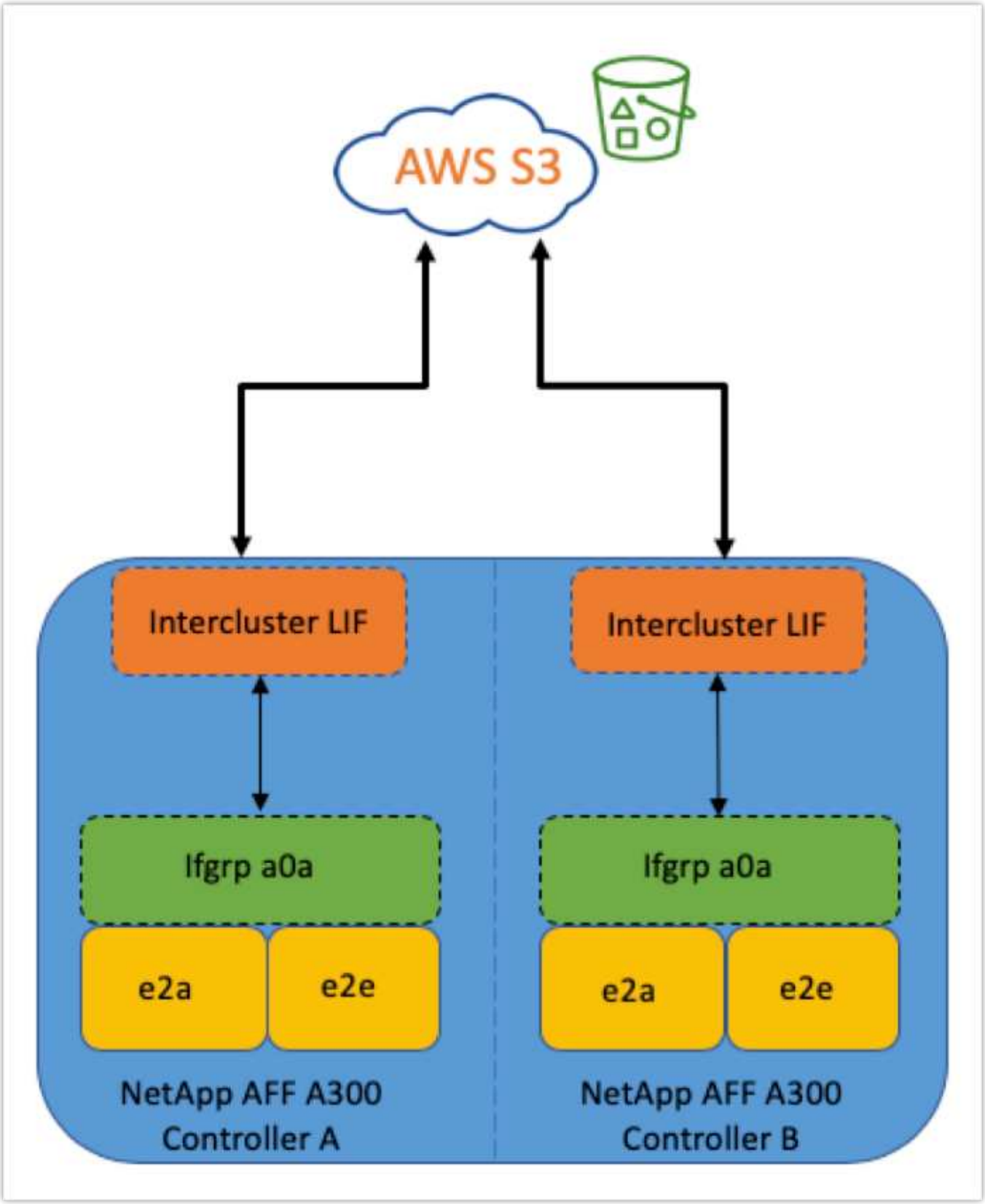
Se mais de um LIF Intercluser for usado em um nó com roteamento diferente, o NetApp recomenda colocá-los em diferentes espaços IPspaces. Durante a configuração, o FabricPool pode selecionar entre vários IPspaces, mas não é capaz de selecionar LIFs de clusters específicos dentro de um IPspace.

A desativação ou exclusão de um LIF entre clusters interrompe a comunicação com a camada de nuvem.

Conetividade

A latência de leitura do FabricPool é uma função da conectividade à camada de nuvem. LIFs entre clusters usando portas 10Gbps, ilustradas na figura a seguir, fornecem desempenho adequado. A NetApp recomenda validar a latência e a taxa de transferência do ambiente de rede específico para determinar o efeito que ele tem no desempenho do FabricPool.

Ao usar o FabricPool em ambientes de baixa performance, os requisitos mínimos de desempenho para aplicações clientes devem continuar a ser atendidos. Os objetivos de tempo de recuperação devem ser ajustados adequadamente.



Profiler de armazenamento de objetos

O profiler de armazenamento de objetos, um exemplo do qual é mostrado abaixo e está disponível por meio da CLI do ONTAP, testa a latência e o desempenho da taxa de transferência de armazenamentos de objetos antes que eles sejam anexados a um agregado FabricPool.

A camada de nuvem deve ser adicionada ao ONTAP antes que ela possa ser usada com o profiler de armazenamento de objetos.

Inicie o profiler de armazenamento de objetos a partir do modo de privilégio avançado no ONTAP com o seguinte comando:

```
storage aggregate object-store profiler start -object-store-name <name>
-node <name>
```

Para visualizar os resultados, execute o seguinte comando:

```
storage aggregate object-store profiler show
```

As camadas de nuvem não fornecem performance semelhante à encontrada na categoria de performance (geralmente GB por segundo). Embora os agregados FabricPool possam fornecer facilmente performance semelhante a SATA, eles também podem tolerar latências de até 10 segundos e taxa de transferência baixa para soluções em camadas que não exigem performance semelhante a SATA.

```
bb09-a300-2::*> storage aggregate object-store profiler show
Object store config name: aws_infra_fp_bk_1
Node name: bb09-a300-2-1
Status: Active. Issuing GETs
Start time: 10/3/2019 12:37:24

Op      Size       Total     Failed            Latency(ms)          Throughput
                                          min       max       avg
-------------------------------------------------------------------------------
PUT     4MB        1084      0         336       5951      2817     69.55MB
GET     4KB        158636    0         27        1132      41       32.22MB
GET     8KB        0         0         0         0         0        0B
GET     32KB       0         0         0         0         0        0B
GET     256KB      0         0         0         0         0        0B
5 entries were displayed.
```

Volumes

O thin Provisioning de storage é uma prática padrão para o administrador da infraestrutura virtual do FlexPod. O console de storage virtual (VSC) do NetApp provisiona volumes de storage para armazenamentos de dados VMware sem qualquer garantia de espaço (thin Provisioning) e com configurações otimizadas de eficiência de storage de acordo com as práticas recomendadas da NetApp. Se o VSC for usado para criar datastores VMware, nenhuma ação adicional será necessária, pois nenhuma garantia de espaço deve ser atribuída ao volume do datastore.

O FabricPool não pode anexar um nível de nuvem a um agregado que contenha volumes usando uma garantia de espaço diferente de nenhum (por exemplo, volume).

```
volume modify -space-guarantee none
```

A configuração `space-guarantee none` do parâmetro fornece provisionamento fino para o volume. A quantidade de espaço consumida por volumes com esse tipo de garantia cresce à medida que os dados são adicionados em vez de serem determinados pelo tamanho inicial do volume. Essa abordagem é essencial para o FabricPool porque o volume precisa dar suporte aos dados da camada de nuvem que ficam ativos e são trazidos de volta para a camada de performance.

Licenciamento

O FabricPool requer uma licença baseada em capacidade ao anexar fornecedores de storage de objetos de terceiros (como Amazon S3) como camadas de nuvem para sistemas flash híbridos AFF e FAS.

As licenças FabricPool estão disponíveis em formato perpétuo ou baseado em prazo (1 ou 3 anos).

A disposição em categorias na categoria de nuvem para quando a quantidade de dados (capacidade usada) armazenada na categoria de nuvem atinge a capacidade licenciada. Os dados adicionais, incluindo cópias do SnapMirror para volumes que usam a política de categorias all, não podem ser dispostos em camadas até que a capacidade da licença seja aumentada. Embora a disposição em camadas seja interrompida, os dados ainda podem ser acessados pela camada de nuvem. Dados inativos adicionais permanecem nos SSDs até que a capacidade licenciada seja aumentada.

Uma licença FabricPool baseada em termos e capacidade de 10TB TB gratuita vem com a compra de qualquer novo cluster ONTAP 9.5 ou posterior, embora possam ser aplicados custos adicionais de suporte. As licenças FabricPool (incluindo capacidade adicional para licenças existentes) podem ser adquiridas em incrementos de 1TB U.

Uma licença FabricPool só pode ser excluída de um cluster que não contém agregados FabricPool.

> As licenças do FabricPool são de todo o cluster. Você deve ter o UUID disponível ao comprar uma licença (`cluster identify show`). Para obter informações adicionais sobre licenciamento, consulte o "Base de conhecimento da NetApp".

Configuração

Revisões de software

A tabela a seguir ilustra versões validadas de hardware e software.

Camada	Dispositivo	Imagem	Comentários
Armazenamento	NetApp AFF A300	ONTAP 9.6P2	
Computação	Servidores blade Cisco UCS B200 M5 com Cisco UCS VIC 1340	Lançamento 4,0(4b)	
Rede	Interconexão de malha Cisco Nexus 6332-16UP	Lançamento 4,0(4b)	
	Switch Cisco Nexus 93180YC-EX no modo autônomo NX-os	Solte 7,0(3)i7(6)	
Rede de armazenamento	Cisco MDS 9148S	Lançamento 8,3(2)	

Camada	Dispositivo	Imagem	Comentários
Hipervisor		VMware vSphere ESXi 6.7U2	ESXi 6.7.0,13006603
		VMware vCenter Server	VCenter Server 6.7.0.30000 build 13639309
Fornecedor de nuvem		Amazon AWS S3	Balde S3 padrão com opções padrão

Os requisitos básicos do FabricPool estão descritos na "Requisitos da FabricPool". Depois que todos os requisitos básicos tiverem sido atendidos, execute as seguintes etapas para configurar o FabricPool:

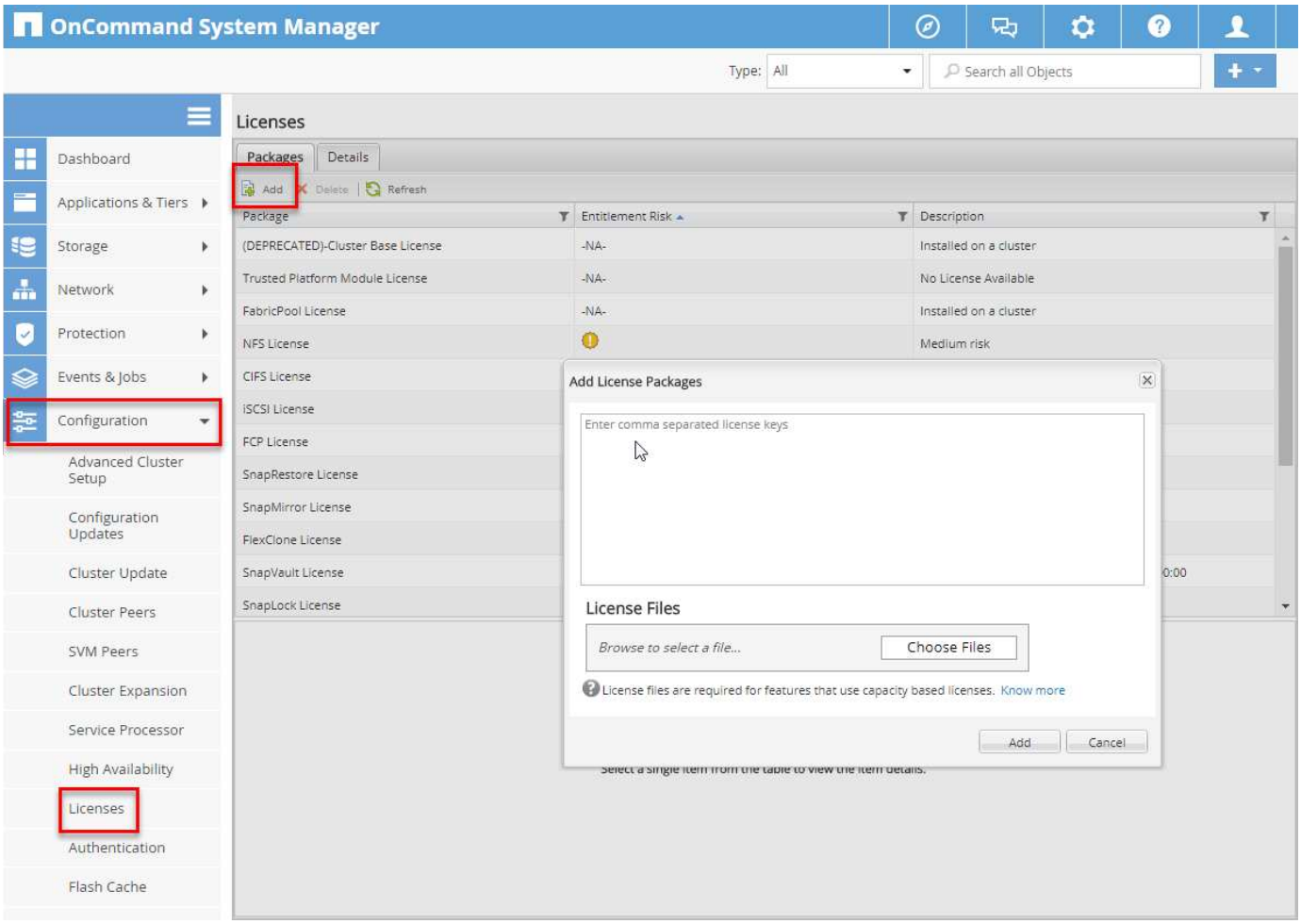
1. Instale uma licença FabricPool.
2. Crie um bucket do armazenamento de objetos do AWS S3.
3. Adicionar uma camada de nuvem ao ONTAP.
4. Anexar a camada de nuvem a um agregado.
5. Definir a política de disposição em categorias de volume.

"Próximo: Instale a licença FabricPool."

Instale a licença FabricPool

Depois de adquirir um ficheiro de licença do NetApp, pode instalá-lo com o OnCommand System Manager. Para instalar o arquivo de licença, execute as seguintes etapas:

1. Clique em Configurações.
2. Clique em Cluster.
3. Clique em licenças.
4. Clique em Adicionar.
5. Clique em escolher arquivos para procurar e selecione um arquivo.
6. Clique em Adicionar.



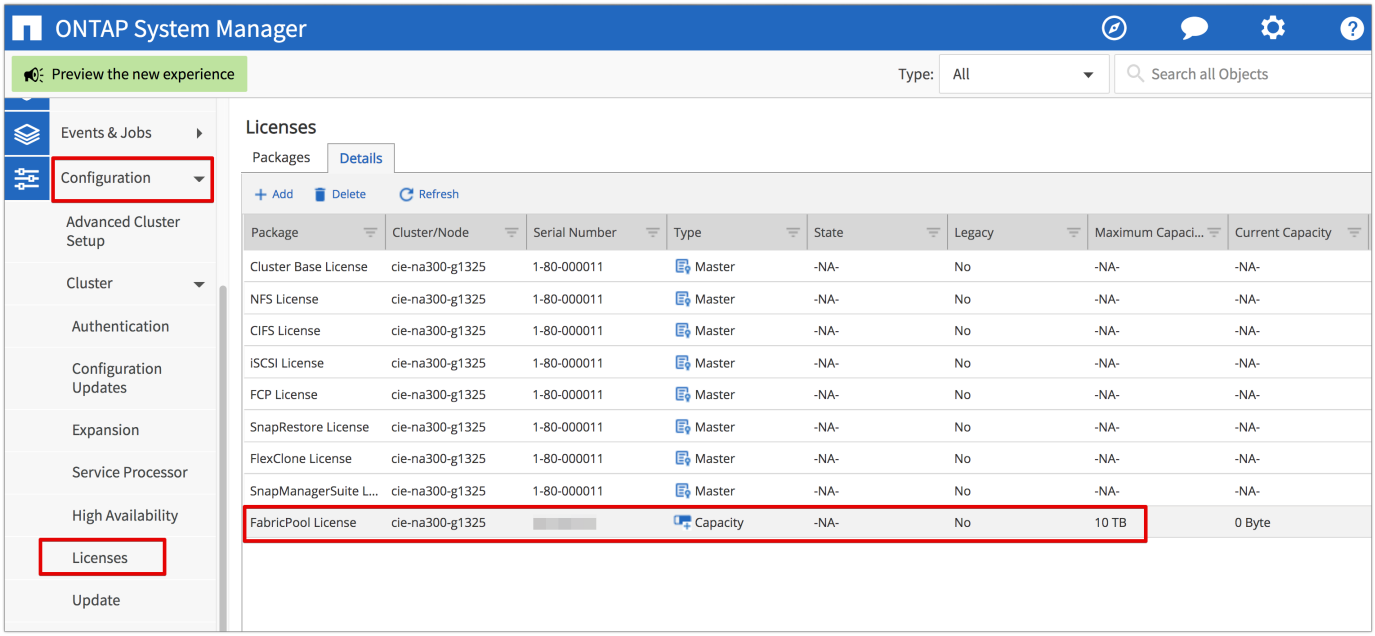
Capacidade da licença

Você pode visualizar a capacidade da licença usando a CLI ou o OnCommand System Manager do ONTAP. Para ver a capacidade licenciada, execute o seguinte comando na CLI do ONTAP:

```
system license show-status
```

No OnCommand System Manager, execute as seguintes etapas:

1. Clique em Configurações.
2. Clique em licenças.
3. Clique na guia Detalhes.



A capacidade máxima e a capacidade atual estão listadas na linha Licença FabricPool.

"Próximo: Crie o bucket do AWS S3."

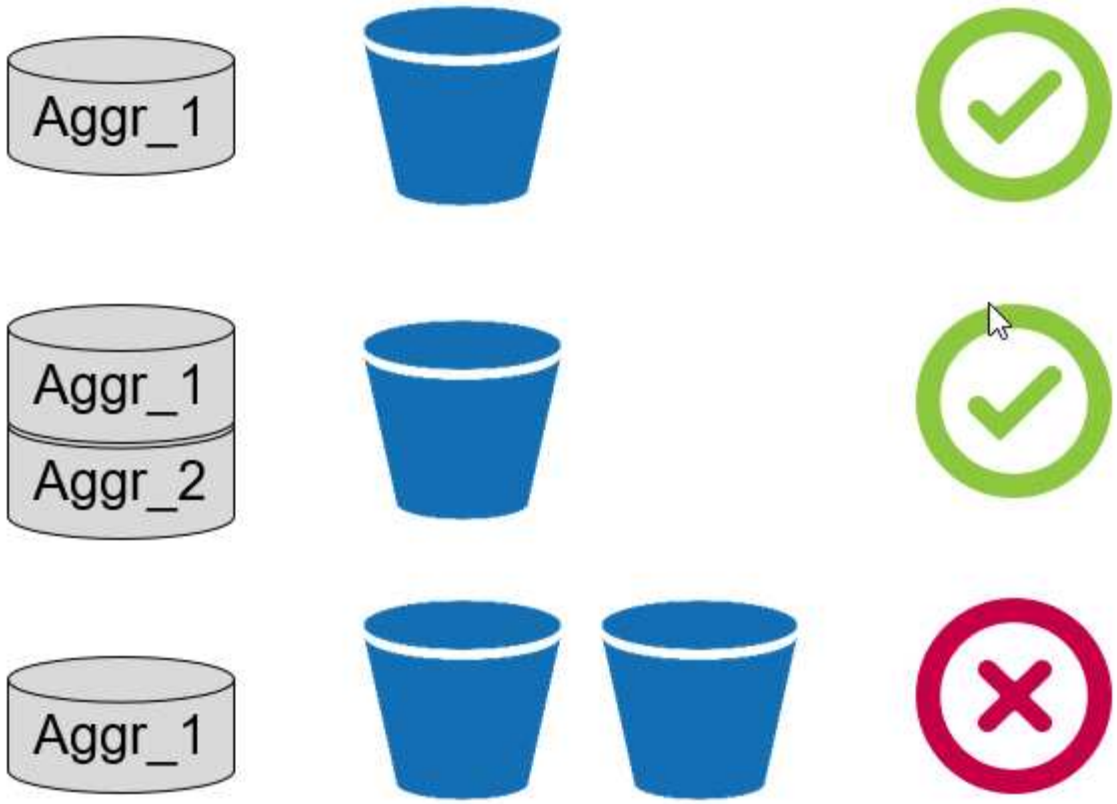
Crie o bucket do AWS S3

Buckets são contêineres de armazenamento de objetos que armazenam dados. Você precisa fornecer o nome e o local do bucket no qual os dados são armazenados antes que possam ser adicionados a um agregado como uma categoria de nuvem.

Buckets não podem ser criados com o OnCommand System Manager, o OnCommand Unified Manager ou o ONTAP.

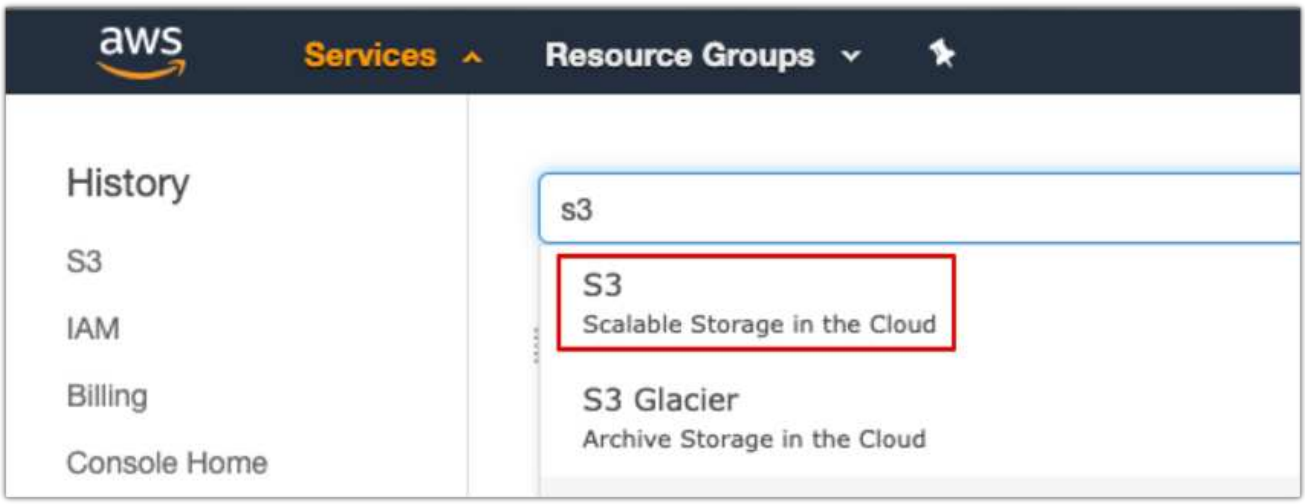
O FabricPool suporta a fixação de um balde por agregado, conforme ilustrado na figura seguinte. Um único bucket pode ser anexado a um único agregado e um único bucket pode ser anexado a vários agregados. No entanto, um único agregado não pode ser anexado a vários buckets. Embora um único bucket possa ser anexado a vários agregados em um cluster, o NetApp não recomenda a vinculação de um único bucket a agregados em vários clusters.

Ao Planejar uma arquitetura de storage, considere como o relacionamento bucket-to-agregado pode afetar o desempenho. Muitos provedores de armazenamento de objetos definem um número máximo de IOPS compatíveis no nível do bucket ou do contêiner. Os ambientes que exigem desempenho máximo devem usar vários buckets para reduzir a possibilidade de que as limitações de IOPS do armazenamento de objetos possam afetar o desempenho em vários agregados FabricPool. Conectar um único bucket ou contêiner a todos os agregados do FabricPool em um cluster pode ser mais benéfico para ambientes que valorizam a capacidade de gerenciamento sobre o desempenho de camada de nuvem.

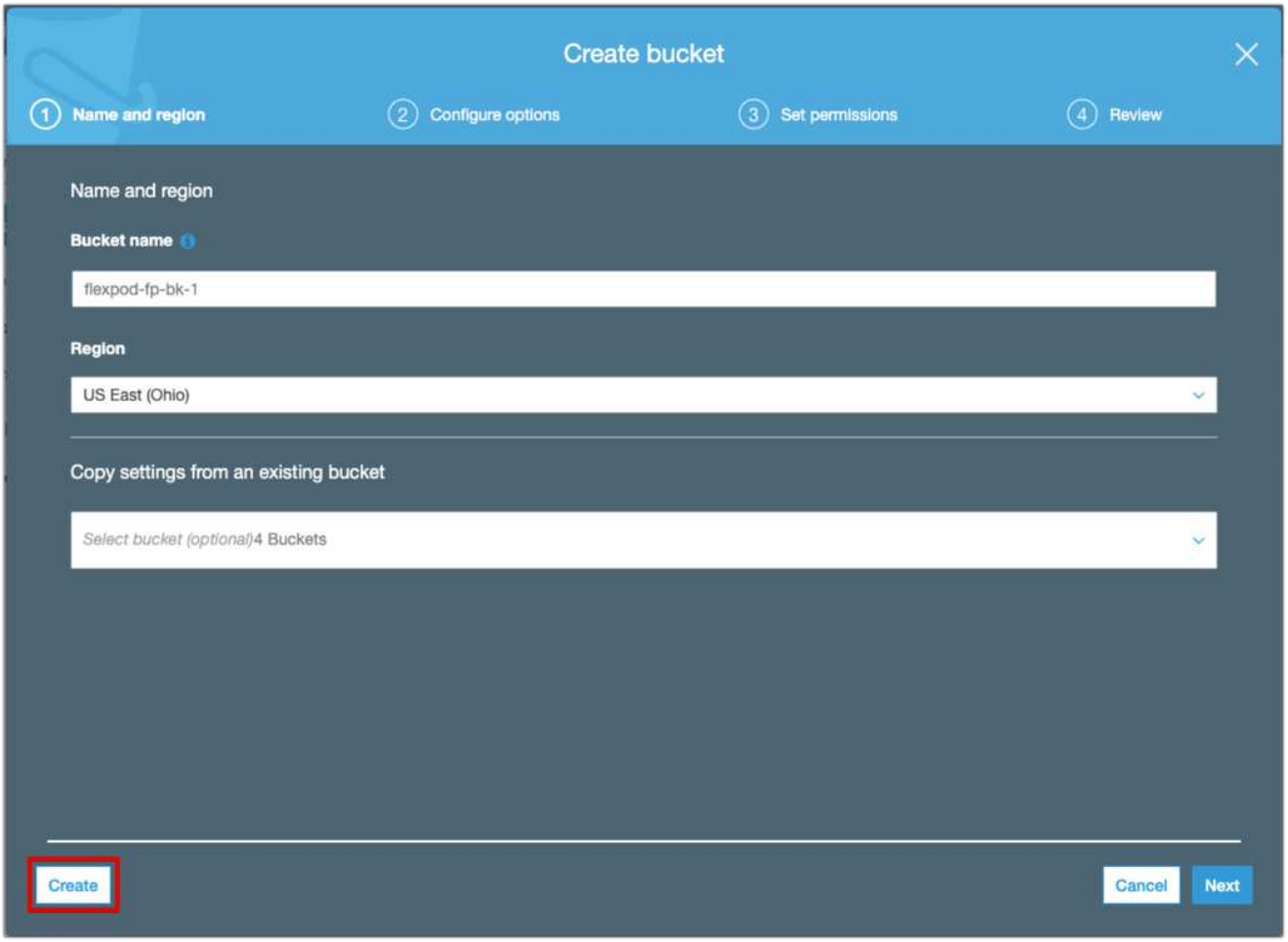


Crie um bucket do S3

1. No console de gerenciamento da AWS na página inicial, digite S3 na barra de pesquisa.
2. Selecione S3 armazenamento escalável na nuvem.



3. Na página inicial do S3, selecione criar balde.
4. Insira um nome compatível com DNS e escolha a região para criar o intervalo.



5. Clique em criar para criar o bucket do armazenamento de objetos.

"Próximo: Adicionar uma camada de nuvem ao ONTAP"

Adicionar uma camada de nuvem ao ONTAP

Antes que um armazenamento de objetos possa ser anexado a um agregado, ele deve ser adicionado e identificado pelo ONTAP. Essa tarefa pode ser concluída com o OnCommand System Manager ou com a CLI do ONTAP.

O FabricPool é compatível com armazenamentos de objetos Amazon S3, IBM Object Cloud Storage e Microsoft Azure Blob Storage como camadas de nuvem.

Você precisa das seguintes informações:

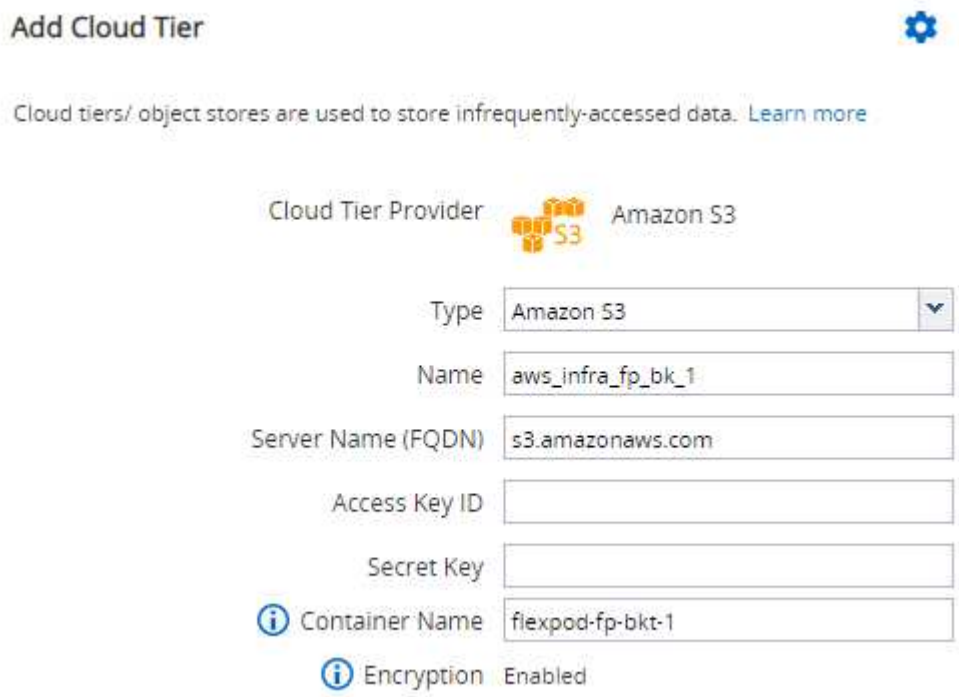
- Nome do servidor (FQDN); por exemplo, `s3.amazonaws.com`
- ID da chave de acesso
- Chave secreta
- Nome do recipiente (nome do balde)

OnCommand System Manager

Para adicionar um nível de nuvem ao OnCommand System Manager, siga estas etapas:

1. Inicie o OnCommand System Manager.
2. Clique em armazenamento.
3. Clique em agregados e discos.
4. Clique em categorias de nuvem.
5. Selecione um fornecedor de armazenamento de objetos.
6. Preencha os campos de texto conforme necessário para o fornecedor do armazenamento de objetos.

   No campo Nome do contentor, insira o nome do bucket ou do contentor do armazenamento de objetos.
7. Clique em Salvar e anexar agregados.



CLI do ONTAP

Para adicionar um nível de nuvem com a CLI do ONTAP, digite os seguintes comandos:

```
object-store config create
-object-store-name <name>
-provider-type <AWS>
-port <443/8082> (AWS)
-server <name>
-container-name <bucket-name>
-access-key <string>
-secret-password <string>
-ssl-enabled true
-ipspace default
```

"Próximo: Conecte uma categoria de nuvem a um agregado da ONTAP."

Anexar uma camada de nuvem a um agregado da ONTAP

Depois que um armazenamento de objetos tiver sido adicionado e identificado pelo ONTAP, ele deve ser anexado a um agregado para criar um FabricPool. Essa tarefa pode ser concluída usando o OnCommand System Manager ou a CLI do ONTAP.

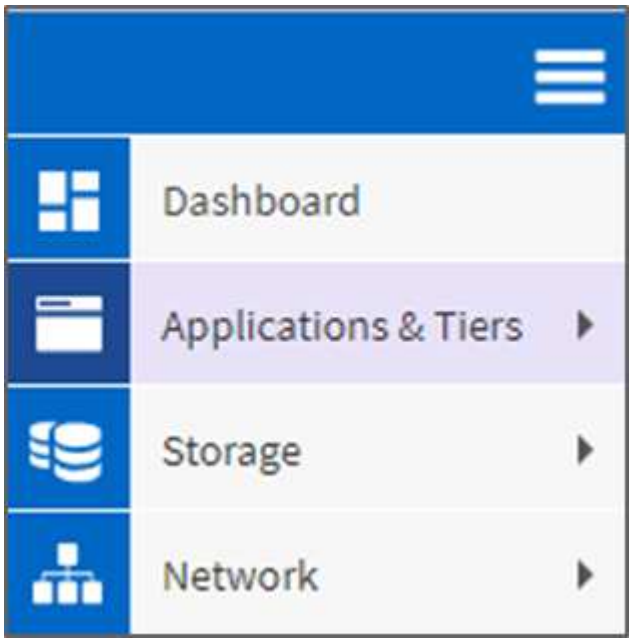
Mais de um tipo de armazenamento de objetos pode ser conetado a um cluster, mas apenas um tipo de armazenamento de objetos pode ser anexado a cada agregado. Por exemplo, um agregado pode usar o Google Cloud e outro agregado pode usar o Amazon S3, mas um agregado não pode ser anexado a ambos.

Conectar uma camada de nuvem a um agregado é uma ação permanente. Um nível de nuvem não pode ser desanexado de um agregado ao qual ele foi anexado.

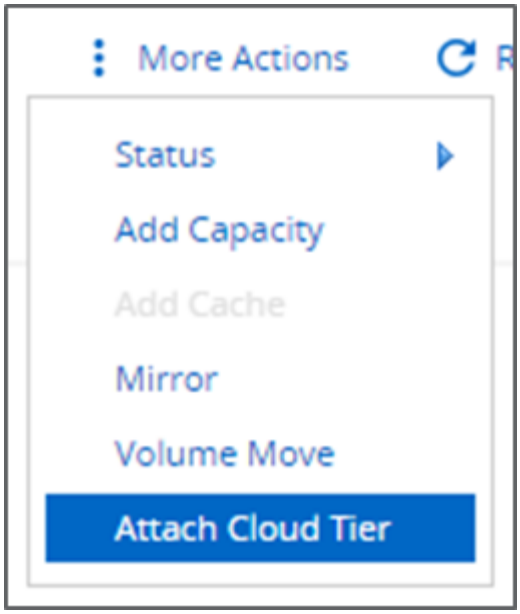
OnCommand System Manager

Para anexar um nível de nuvem a um agregado usando o OnCommand System Manager, siga estas etapas:

1. Inicie o OnCommand System Manager.
2. Clique em aplicações e camadas.



3. Clique em camadas de armazenamento.
4. Clique em um agregado.
5. Clique em ações e selecione Anexar nível de nuvem.



6. Selecione um nível de nuvem.
7. Visualizar e atualizar as políticas de disposição em camadas dos volumes no agregado (opcional). Por padrão, a política de disposição em categorias de volume é definida como somente Snapshot.
8. Clique em Guardar.

CLI do ONTAP

Para anexar um nível de nuvem a um agregado usando a CLI do ONTAP, execute os seguintes comandos:

```
storage aggregate object-store attach
-aggregate <name>
-object-store-name <name>
```

Exemplo:

```
storage aggregate object-store attach -aggregate aggr1 -object-store-name
- aws_infra_fp_bk_1
```

"Próximo: Definir a política de disposição em categorias de volume."

Definir a política de disposição em categorias de volume

Por padrão, os volumes usam a política de disposição em categorias de volume Nenhuma. Após a criação do volume, a política de disposição em categorias de volume pode ser alterada com o OnCommand System Manager ou a CLI do ONTAP.

Quando usado com o FlexPod, o FabricPool fornece três políticas de disposição em categorias de volumes, Automático, somente Snapshot e nenhum.

- **Auto**

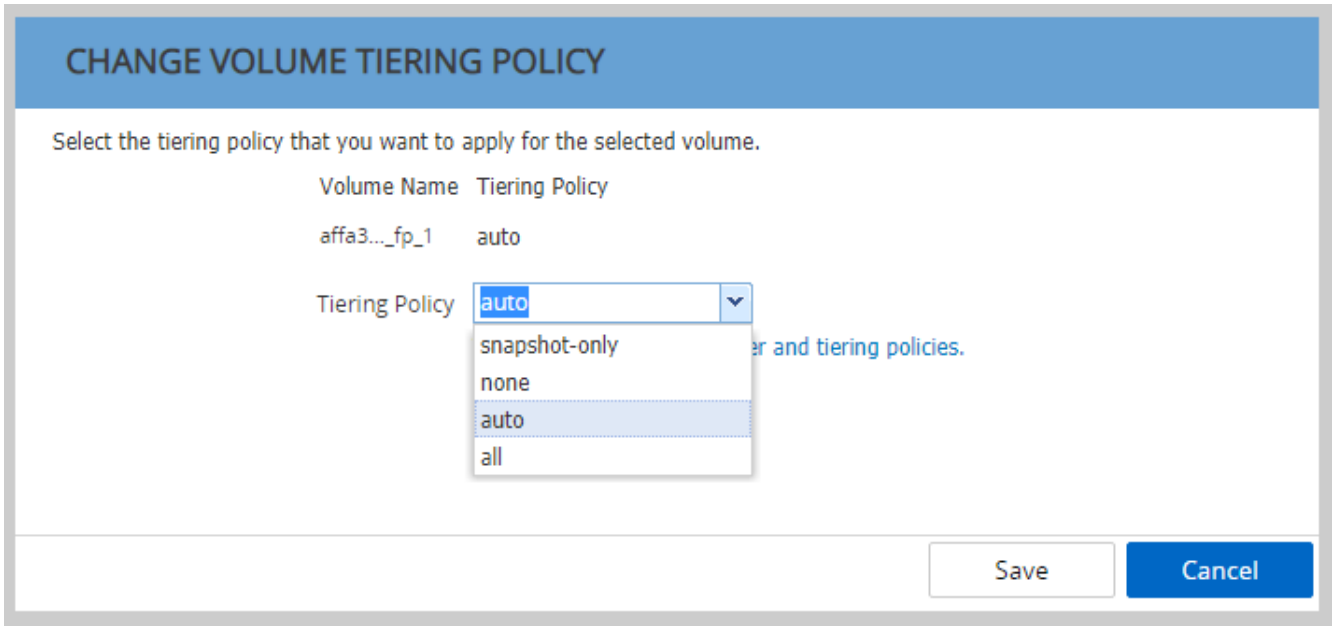
- Todos os blocos inativos do volume são movidos para a camada de nuvem. Supondo que o agregado seja mais de 50% utilizado, leva aproximadamente 31 dias para que os blocos inativos fiquem frios. O período de arrefecimento automático é ajustável entre 2 dias e 63 dias utilizando a `tiering-minimum-cooling-days` definição.
- Quando os blocos frios em um volume com uma política de disposição em camadas definida como Automático são lidos aleatoriamente, eles ficam ativos e gravados no nível de performance.
- Quando os blocos inativos de um volume com uma política de disposição em camadas definida como Automático são lidos sequencialmente, eles permanecem inativos e na camada de nuvem. Eles não são gravados no nível de performance.

- **Somente snapshot**
  - Os blocos de snapshot bloqueado no volume que não é compartilhado com o sistema de arquivos ativo são movidos para a camada de nuvem. Supondo que o agregado seja mais de 50% utilizado, leva aproximadamente 2 dias para que os blocos de snapshot inativos fiquem inativos. O período de resfriamento somente de snapshot pode ser ajustável de 2 a 63 dias usando a `tiering-minimum-cooling-days` configuração.
  - Quando os blocos inativos de um volume com uma política de disposição em categorias definida como somente Snapshot são lidos, eles são postos em funcionamento e gravados no nível de performance.
- **Nenhum (padrão)**
  - Volumes configurados para usar nenhum como sua política de disposição em categorias não categorizam dados inativos na camada de nuvem.
  - Definir a política de disposição em categorias como Nenhuma impede a nova disposição em categorias.
  - Os dados de volume anteriormente movidos para a camada de nuvem permanecem na camada de nuvem até que fiquem ativos e são movidos automaticamente de volta para a camada de performance.

OnCommand System Manager

Para alterar a política de disposição em camadas de um volume usando o OnCommand System Manager, siga estas etapas:

1. Inicie o OnCommand System Manager.
2. Selecione um volume.
3. Clique em mais ações e selecione alterar Diretiva de disposição em categorias.
4. Selecione a política de disposição em camadas a aplicar ao volume.
5. Clique em Guardar.



CLI do ONTAP

Para alterar a política de disposição em camadas de um volume usando a CLI do ONTAP, execute o seguinte comando:

```
volume modify -vserver <svm_name> -volume <volume_name>
-tiering-policy <auto|snapshot-only|all|none>
```

"Próximo: Definir os dias mínimos de resfriamento em categorias de volume."

Definir os dias mínimos de resfriamento em disposição de volume em categorias

A `tiering-minimum-cooling-days` configuração determina quantos dias devem passar antes que os dados inativos em um volume usando a política automática ou somente snapshot sejam considerados inativos e qualificados para disposição em categorias.

Auto

A configuração padrão `tiering-minimum-cooling-days` para a política de disposição automática em categorias é de 31 dias.

Como as leituras mantêm as temperaturas de bloco quentes, o aumento desse valor pode reduzir a quantidade de dados qualificados para serem dispostos em camadas e aumentar a quantidade de dados mantidos na categoria de performance.

Se você quiser reduzir esse valor dos 31 dias padrão, lembre-se de que os dados não devem mais estar ativos antes de serem marcados como frios. Por exemplo, se uma carga de trabalho de vários dias for esperada para executar um número significativo de gravações no dia 7, a configuração do volume `tiering-minimum-cooling-days` não deve ser definida inferior a 8 dias.

O storage de objetos não é transacional, como storage de arquivos ou blocos. Fazer alterações em arquivos armazenados como objetos em volumes com dias de resfriamento mínimos excessivamente agressivos pode resultar na criação de novos objetos, na fragmentação dos objetos existentes e na adição de ineficiências de storage.

Apenas Snapshot

A configuração padrão `tiering-minimum-cooling-days` da política de disposição em camadas somente Snapshot é de 2 dias. Um mínimo de 2 dias fornece tempo adicional para processos em segundo plano para fornecer a máxima eficiência de storage e impede que processos diários de proteção de dados precisem ler dados da categoria de nuvem.

CLI do ONTAP

Para alterar a configuração de um volume `tiering-minimum-cooling-days` usando a CLI do ONTAP, execute o seguinte comando:

```
volume modify -vserver <svm_name> -volume <volume_name> -tiering-minimum
-cooling-days <2-63>
```

É necessário o nível de privilégio avançado.

Alterar a política de disposição em camadas entre Automático e somente Snapshot (ou vice-versa) redefine o período de inatividade dos blocos no nível de performance. Por exemplo, um volume usando a política de disposição automática de volumes com dados no nível de desempenho que estejam inativos por 20 dias terá a inatividade dos dados do nível de desempenho redefinida para 0 dias se a política de disposição em camadas estiver definida como somente snapshot.

Considerações de desempenho

Dimensione o nível de performance

Ao considerar o dimensionamento, tenha em mente que o nível de desempenho deve ser capaz das seguintes tarefas:

- Suporte a dados ativos
- Dá suporte a dados inativos até que a digitalização em categorias mova os dados para a camada de nuvem
- Dando suporte a dados de categorias de nuvem que se tornam ativos e são gravados de volta na categoria de performance
- Compatível com metadados do WAFL associados à categoria de nuvem anexada

Para a maioria dos ambientes, uma taxa de performance/capacidade de 1:10 em agregados FabricPool é extremamente conservadora, ao mesmo tempo em que proporciona uma economia significativa de storage. Por exemplo, se o objetivo for categorizar 200TB na categoria de nuvem, o agregado da categoria de desempenho deve ser de 20TB no mínimo.

As gravações da categoria de nuvem para a categoria de performance serão desativadas se a capacidade da categoria de performance for superior a 70%. Se isso ocorrer, os blocos serão lidos diretamente na camada de nuvem.

Dimensione a camada de nuvem

Ao considerar o dimensionamento, o armazenamento de objetos que atua como a camada de nuvem deve ser capaz das seguintes tarefas:

- Compatível com leituras de dados inativos existentes
- Suporte a gravações de novos dados inativos
- Suporte à exclusão e desfragmentação de objetos

Custo de propriedade

O "Calculadora econômica da FabricPool" está disponível por meio da empresa independente de analistas DE TI Evaluator Group para ajudar a projetar a economia de custos entre o local e a nuvem para storage de dados inativos. A calculadora fornece uma interface simples para determinar o custo de armazenar dados acessados com pouca frequência em uma camada de performance, em vez de enviá-los para uma camada de nuvem pelo restante do ciclo de vida dos dados. Com base em um cálculo de 5 anos, os quatro principais fatores, capacidade de origem, crescimento de dados, capacidade Snapshot e porcentagem de dados inativos, são usados para determinar os custos de storage no período de tempo.

Conclusão

A jornada para a nuvem varia entre organizações, entre unidades de negócios e até mesmo entre unidades de negócios dentro das organizações. Alguns escolhem uma adoção rápida, enquanto outros adotam uma abordagem mais conservadora. A FabricPool se encaixa na estratégia de nuvem das organizações, independentemente do seu tamanho e velocidade de adoção da nuvem, demonstrando ainda mais os benefícios de eficiência e escalabilidade de uma infraestrutura FlexPod.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Práticas recomendadas da FabricPool

  "www.NetApp.com/us/media/tr-4598.pdf"

- Documentação do produto NetApp

  "https://docs.netapp.com"

- TR-4036: Especificação técnica de datacenter FlexPod

"https://www.netapp.com/us/media/tr-4036.pdf"

FlexPod Datacenter com IBM Cloud Private

Cisco, NetApp

O IBM Cloud Private (ICP) é uma plataforma local para desenvolver e gerenciar aplicativos em contêiner para casos de uso nativos da nuvem e de modernização de aplicativos. Ele é um ambiente integrado desenvolvido com o Kubernetes como sua orquestração de contêineres e inclui um repositório de imagens privado para contentores Docker, um console de gerenciamento, uma estrutura de monitoramento, muitos aplicativos em contêiner IBM e baseados em código aberto e muito mais. Combinar ICP com FlexPod, a infraestrutura convergente da Cisco e NetApp, pode simplificar a implantação e o gerenciamento de sua infraestrutura. Você também pode se beneficiar de eficiência de storage aprimorada, melhor proteção de dados, menor risco e flexibilidade para escalar esse stack de infraestrutura de nível empresarial altamente disponível para acomodar novos requisitos de negócios e outras alterações ao longo do tempo.

"FlexPod Datacenter com IBM Cloud Private"

Data center FlexPod para nuvem híbrida com Cisco CloudCenter e armazenamento privado NetApp - projete

Haseeb Niazi, Cisco David Arnette, NetApp

Os Cisco Validated designs (CVDs) fornecem sistemas e soluções projetados, testados e documentados para facilitar e melhorar as implantações dos clientes. Esses designs incorporam uma ampla gama de tecnologias e produtos em um portfólio de soluções que foram desenvolvidas para atender às necessidades de negócios dos clientes e orientá-los desde o design até a implantação.

"Data center FlexPod para nuvem híbrida com Cisco CloudCenter e armazenamento privado NetApp - projete"

Data center FlexPod para multicloud com o Cisco CloudCenter e o NetApp Data Fabric

Haseeb Niazi, Cisco David Arnette, NetApp

Este documento fornece diretrizes detalhadas de configuração e implementação para a configuração do data center FlexPod para nuvem híbrida. Os seguintes elementos de design distinguem esta versão do FlexPod dos modelos anteriores:

- Integração do Cisco CloudCenter com o FlexPod Datacenter com ACI como a nuvem privada
- Integração do Cisco CloudCenter com nuvens públicas do Amazon Web Services (AWS) e do Microsoft Azure Resource Manager (MS Azure RM)

- Fornecimento de conectividade segura entre o data center FlexPod e as nuvens públicas para obter tráfego seguro entre máquinas virtuais (VMs)
- Proporcionar conectividade segura entre o data center do FlexPod e o NetApp Private Storage (NPS) para tráfego de replicação de dados
- Capacidade de implantar instâncias de aplicações em nuvens públicas ou privadas e disponibilizar dados de aplicações atualizados para essas instâncias por meio de orquestração orientada pelo Cisco CloudCenter
- Configuração, validação e destaque de aspectos operacionais de um ambiente de desenvolvimento e teste nesse novo modo de nuvem híbrida.

"Data center FlexPod para multicloud com o Cisco CloudCenter e o NetApp Data Fabric"

Bancos de dados empresariais

SAP

Introdução ao SAP no FlexPod

A plataforma FlexPod é uma arquitetura de data center pré-projetada e com práticas recomendadas desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e nas controladoras de storage da NetApp.

O FlexPod é uma plataforma adequada para a execução de aplicativos SAP, e as soluções fornecidas aqui permitem que você implante o SAP HANA de forma rápida e confiável com um modelo de integração de data center personalizada. O FlexPod oferece não apenas uma configuração de linha de base, mas também a flexibilidade de ser dimensionada e otimizada para acomodar vários casos de uso e requisitos diferentes.

Solução FlexPod Datacenter para SAP usando SAN Fibre Channel com Cisco UCS Manager 4,0 e NetApp ONTAP 9.7

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve o data center Cisco e NetApp FlexPod com o NetApp ONTAP 9.7 no armazenamento NetApp AFF A400 e o software unificado do Cisco UCS Manager versão 4,1 (1) com processadores escaláveis Intel Xeon de segunda geração para SAP HANA em particular.

O FlexPod Datacenter com o NetApp ONTAP 9.7 e o Cisco UCS Unified Software Release 4,1() é uma arquitetura de data center pré-projetada e de práticas recomendadas, desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), a família de switches Cisco Nexus 9000, switches de malha multicamadas MDS 9000 e arrays de armazenamento NetApp AFF A-Series executando o sistema operacional de armazenamento ONTAP 9 1.

"Solução FlexPod Datacenter para SAP usando SAN Fibre Channel com Cisco UCS Manager 4,0 e NetApp ONTAP 9.7"

SAP Non-HANA com white paper SQL - Design

O atual setor DE TI está testemunhando uma transformação dramática nas soluções de data center. Nos últimos anos, houve um interesse considerável em soluções de data center pré-validadas e projetadas. A introdução da tecnologia de virtualização em áreas críticas teve um grande impactos nos princípios de design e arquitetura dessas soluções. Isso permitiu que muitos aplicativos executados em sistemas bare-metal migrassem para novas soluções integradas virtualizadas. O FlexPod é uma solução de data center pré-validada e projetada para atender às necessidades em rápida mudança dos departamentos DE TI. A Cisco e a NetApp fizeram uma parceria para fornecer o FlexPod, que usa componentes de computação, rede e storage de classe bestin como base para uma variedade de cargas de trabalho empresariais, incluindo bancos de dados, Planejamento de recursos empresariais (ERP), gerenciamento de relacionamento com o cliente (CRM) e aplicações Web.

A consolidação de APLICAÇÕES DE TI, em particular de bancos de dados, tem gerado um interesse considerável nos últimos anos. A plataforma de banco de dados mais adotada e implantada nos últimos anos é o Microsoft SQL Server. Os bancos de dados do SQL Server frequentemente estão sujeitos à expansão de bancos de dados, levando a desafios DE TI, como servidores subutilizados, licenciamento incorreto, preocupações de segurança, preocupações de gerenciamento e enormes custos operacionais. Portanto, os bancos de dados SQL Server são bons candidatos para consolidação em uma plataforma mais robusta, flexível e resiliente. Este documento discute uma arquitetura de referência do FlexPod para implantar e consolidar bancos de dados do SQL Server.

"SAP Non-HANA com white paper SQL - Design"

Solução de data center FlexPod para SAP com malha de terceira geração Cisco UCS e NetApp AFF A-Series

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a metodologia de implantação do Cisco e do NetApp FlexPod Datacenter para SAP HANA com base em processadores escaláveis Intel Xeon de segunda geração suportados pelo sistema de computação Cisco UCS (Cisco UCS).

O Cisco UCS Manager (UCSM) 4,0(4) fornece suporte consolidado de todos os modelos atuais de interconexão de malha Cisco UCS (6200, 6300, 6324 e 6454), IOM da série 2200/2300, blade da série Cisco UCS B e servidores de formFactor de rack Cisco UCS C-Series. O FlexPod Datacenter com o software unificado Cisco UCS versão 4,0(4D) e o NetApp ONTAP 9.6, é uma arquitetura de data center pré-projetada e com práticas recomendadas, desenvolvida com base no Cisco UCS, na família de switches Cisco Nexus 9000 e nos storage arrays NetApp AFF A-Series.

"Solução de data center FlexPod para SAP com malha de terceira geração Cisco UCS e NetApp AFF A-Series"

Solução FlexPod Datacenter para SAP usando SAN Fibre Channel com Cisco UCS Manager 4,0 e NetApp ONTAP 9.7 - Design

Ramamurthy, Cisco Marco Schoen, NetApp

A Cisco e a NetApp fizeram uma parceria para fornecer uma série de soluções FlexPod que permitem plataformas estratégicas de data center. A solução FlexPod oferece uma arquitetura integrada que incorpora práticas recomendadas de computação, storage e design de rede, minimizando os riscos DE TI validando a arquitetura integrada para garantir a compatibilidade entre vários componentes. A solução também aborda os pontos problemáticos DA TI, fornecendo orientação de projeto documentada, orientação de implantação e suporte que podem ser usados em várias etapas (Planejamento, projeto e implementação) de uma implantação.

"Solução FlexPod Datacenter para SAP usando SAN Fibre Channel com Cisco UCS Manager 4,0 e NetApp ONTAP 9.7 - Design"

Solução FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a solução FlexPod integrada ACI da Cisco como uma abordagem validada para a implantação de ambientes de integração de data center (TDI) personalizados. Esse design validado fornece diretrizes e uma estrutura para implementar o SAP HANA com as práticas recomendadas da Cisco e da NetApp.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS) usando uma versão unificada de software para oferecer suporte às plataformas de hardware Cisco UCS que incluem os seguintes componentes:

- Servidores blade da série B do Cisco UCS e servidores em rack da série C do Cisco UCS configuráveis com a opção de módulo de memória persistente do Centro de dados Optane (DCPMM)
- Interconexões de tecido da série Cisco UCS 6400
- Interrutores de folha e coluna da série Cisco Nexus 9000
- Storage arrays NetApp All Flash Series

Além disso, este documento fornece validações para Red Hat Enterprise Linux e SUSE Linux Enterprise Server para SAP HANA.

"Solução FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design"

FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series - implantação

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a arquitetura e os procedimentos de implantação da opção de integração de data center adaptada do SAP HANA na infraestrutura do FlexPod, que é composta por:

- Sistema de computação UCS Cisco (Cisco UCS) suportado pelos processadores escaláveis Intel Xeon de segunda geração.
- Produtos de switching que utilizam a infraestrutura centrada em aplicativos (ACI) da Cisco.
- Arrays AFF da série A NetApp.

O objetivo deste documento é mostrar as etapas de configuração detalhadas para a implantação do SAP HANA

"FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series - implantação"

Solução FlexPod Datacenter para SAP com Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a solução Cisco e NetApp FlexPod, que é uma abordagem validada para a implantação de ambientes de integração de data centers personalizados (TDI) do SAP HANA. Esse design validado fornece diretrizes e uma estrutura para

implementar o SAP HANA com as práticas recomendadas da Cisco e da NetApp.

O FlexPod é uma infraestrutura integrada líder que dá suporte a uma ampla variedade de workloads e casos de uso empresariais. Essa solução permite que você implante o SAP HANA de forma rápida e confiável com um modelo de modo de integração de data center personalizado.

"Solução FlexPod Datacenter para SAP com Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design"

Solução FlexPod Datacenter para SAP com Cisco ACI em servidores Cisco UCS M5 com SLES 12 SP3 e RHEL 7,4

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a arquitetura e os procedimentos de implantação para a opção de integração de data center personalizada do SAP HANA na infraestrutura FlexPod composta por produtos de computação e comutação da Cisco que utilizam a infraestrutura centrada em aplicativos (ACI) da Cisco - a solução de rede definida por software (SDN) líder do setor - junto com os arrays AFF da série A da NetApp. O objetivo deste documento é mostrar os princípios de design com as etapas de configuração detalhadas para a implantação do SAP HANA.

"Solução FlexPod Datacenter para SAP com Cisco ACI em servidores Cisco UCS M5 com SLES 12 SP3 e RHEL 7,4"

Solução FlexPod Datacenter para SAP com storage baseado em IP usando o NetApp AFF A-Series e o Cisco UCS Manager 3,2

Cisco, Cisco, NetApp

A arquitetura de referência detalhada neste documento destaca a resiliência, o custo-benefício e a facilidade de implantação de uma solução de storage baseada em IP. Um sistema de storage capaz de atender a vários protocolos em uma única interface permite a escolha do cliente e a proteção do investimento, pois ele realmente é uma arquitetura completa. A solução foi projetada para hospedar workloads SAP HANA escaláveis.

"Solução FlexPod Datacenter para SAP com storage baseado em IP usando o NetApp AFF A-Series e o Cisco UCS Manager 3,2"

Solução FlexPod Datacenter para SAP usando SAN Fibre Channel com Cisco UCS Manager 4,0 e NetApp ONTAP 9.7

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve o data center Cisco e NetApp FlexPod com o NetApp ONTAP 9.7 no armazenamento NetApp AFF A400 e o software unificado do Cisco UCS Manager versão 4,1 (1) com processadores escaláveis Intel Xeon de segunda geração para SAP HANA em particular.

O FlexPod Datacenter com o NetApp ONTAP 9.7 e o Cisco UCS Unified Software Release 4,1() é uma arquitetura de data center pré-projetada e de práticas recomendadas, desenvolvida com base no sistema de

computação unificada da Cisco (Cisco UCS), a família de switches Cisco Nexus 9000, switches de malha multicamadas MDS 9000 e arrays de armazenamento NetApp AFF A-Series executando o sistema operacional de armazenamento ONTAP 9 1.

"Solução FlexPod Datacenter para SAP usando SAN Fibre Channel com Cisco UCS Manager 4,0 e NetApp ONTAP 9.7"

Implante servidores de aplicativos SAP no FlexPod com SQL

O FlexPod é uma solução de data center pré-validada e projetada para atender às necessidades em rápida mudança dos departamentos DE TI. A Cisco e a NetApp fizeram uma parceria para fornecer o FlexPod, que usa os melhores componentes de computação, rede e storage da categoria como base para uma variedade de workloads empresariais, incluindo bancos de dados, Planejamento de recursos empresariais (ERP), gerenciamento de relacionamento com o cliente (CRM) e aplicações da Web. A consolidação de APLICAÇÕES DE TI, em particular de bancos de dados, tem gerado um interesse considerável nos últimos anos. A plataforma de banco de dados mais adotada e implantada nos últimos anos é o Microsoft SQL Server. Os bancos de dados do SQL Server frequentemente estão sujeitos à expansão de bancos de dados, levando a desafios DE TI, como servidores subutilizados, licenciamento incorreto, preocupações de segurança, preocupações de gerenciamento e enormes custos operacionais. Portanto, os bancos de dados SQL Server são bons candidatos para consolidação em uma plataforma mais robusta, flexível e resiliente. Este documento discute uma arquitetura de referência do FlexPod para implantar e consolidar bancos de dados do SQL Server.

"Implante servidores de aplicativos SAP no FlexPod com SQL"

FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a arquitetura e os procedimentos de implantação da opção de integração de data center adaptada do SAP HANA na infraestrutura do FlexPod, que é composta por:

- Sistema de computação UCS Cisco (Cisco UCS) suportado pelos processadores escaláveis Intel Xeon de segunda geração.
- Produtos de switching que utilizam a infraestrutura centrada em aplicativos (ACI) da Cisco.
- Arrays AFF da série A NetApp.

"FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series"

Solução FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a solução FlexPod integrada ACI da Cisco como uma

abordagem validada para a implantação de ambientes de integração de data center (TDI) personalizados. Esse design validado fornece diretrizes e uma estrutura para implementar o SAP HANA com as práticas recomendadas da Cisco e da NetApp.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS) usando uma versão unificada de software para oferecer suporte às plataformas de hardware Cisco UCS que incluem os seguintes componentes:

- Servidores blade da série B Cisco UCS e servidores em rack da série C Cisco UCS configuráveis com a opção de módulo de memória persistente do Centro de dados Optane (DCPMM)
- Interconexões de tecido da série Cisco UCS 6400
- Interrutores de folha e coluna da série Cisco Nexus 9000
- Storage arrays NetApp All Flash Series

Além disso, este documento fornece validações para Red Hat Enterprise Linux e SUSE Linux Enterprise Server para SAP HANA.

"Solução FlexPod Datacenter para SAP com Cisco ACI, Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design"

Solução FlexPod Datacenter para SAP com Cisco UCS de terceira geração e NetApp AFF A-Series

Cisco, Cisco, NetApp

Este documento descreve a metodologia de implantação do Cisco e do NetApp FlexPod Datacenter para SAP HANA com base no sistema de computação Cisco UCS (Cisco UCS) suportado pelos processadores escaláveis Intel Xeon de segunda geração.

O Cisco UCS Manager (UCSM) 4,0(4) fornece suporte consolidado de todos os modelos atuais de interconexão de malha Cisco UCS (6200, 6300, 6324 e 6454), IOM da série 2200/2300, blade da série Cisco UCS B e servidores de formFactor de rack Cisco UCS C-Series. O data center FlexPod com o software unificado Cisco UCS versão 4,0(4D) e o NetApp ONTAP 9.6 é uma arquitetura de data center pré-projetada e com práticas recomendadas, desenvolvida com base no Cisco UCS, na família de switches Cisco Nexus 9000 e nos storage arrays NetApp AFF A-Series.

"Solução FlexPod Datacenter para SAP com Cisco UCS de terceira geração e NetApp AFF A-Series"

Solução FlexPod Datacenter para SAP com Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design

Ramamurthy, Cisco Marco Schoen, NetApp

Este documento descreve a solução Cisco e NetApp FlexPod, que é uma abordagem validada para a implantação de ambientes de integração de data centers personalizados (TDI) do SAP HANA. Esse design validado fornece diretrizes e uma estrutura para implementar o SAP HANA com as práticas recomendadas da Cisco e da NetApp.

O FlexPod é uma infraestrutura integrada líder que dá suporte a uma ampla variedade de workloads e casos de uso empresariais. Essa solução permite que você implante o SAP HANA de forma rápida e confiável com um modelo de modo de integração de data center personalizado.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS) usando uma versão unificada de software para oferecer suporte às plataformas de hardware Cisco UCS que incluem os seguintes componentes:

- Servidores blade da série B do Cisco UCS e servidores em rack da série C do Cisco UCS configuráveis com a opção de módulo de memória persistente do Centro de dados Optane (DCPMM)
- Interconexões de tecido da série Cisco UCS 6300
- Switches Cisco Nexus 9000 Series
- Storage arrays NetApp All Flash Series

Além disso, este documento fornece validações para Red Hat Enterprise Linux e SUSE Linux Enterprise Server para SAP HANA.

"Solução FlexPod Datacenter para SAP com Cisco UCS Manager 4,0 e NetApp AFF A-Series - Design"

Oracle

FlexPod Datacenter com bancos de dados Oracle 19Cg RAC no Cisco UCS e NetApp AFF com NVMe em Fibre Channel

Tushar Patel, Cisco Hardikkkumar Vyas, Cisco

Os Cisco Validated designs (CVDs) consistem em sistemas e soluções projetados, testados e documentados para facilitar e melhorar as implantações dos clientes. Este documento CVD descreve a solução Cisco e NetApp FlexPod, que é uma abordagem validada para implantar um ambiente de banco de dados Oracle RAC altamente disponível. A Cisco e a NetApp validaram a arquitetura de referência com vários workloads de banco de dados, como OLTP (processamento transacional on-line) e Data Warehouse no laboratório de data center UCS da Cisco. Este documento mostra a configuração de hardware e software dos componentes envolvidos e os resultados de vários testes. Além disso, o documento oferece uma estrutura para a implementação de bancos de dados do Oracle RAC no NVMe/FC usando o Cisco UCS e o sistema de armazenamento NetApp.

"FlexPod Datacenter com bancos de dados Oracle 19Cg RAC no Cisco UCS e NetApp AFF com NVMe em Fibre Channel"

FlexPod Datacenter com bancos de dados Oracle RAC no Cisco UCS e NetApp AFF Série A.

Tushar Patel, Cisco Hardikkkumar Vyas, Cisco

Os designs validados da Cisco incluem sistemas e soluções que são projetados, testados e documentados para facilitar e melhorar as implantações dos clientes. Esses designs incorporam uma ampla gama de tecnologias e produtos em um portfólio de soluções que foram desenvolvidas para atender às necessidades de negócios dos clientes. A Cisco e a NetApp fizeram uma parceria para fornecer o FlexPod, que serve de base para uma variedade de workloads e permite designs de arquitetura eficientes

baseados nos requisitos do cliente. Uma solução FlexPod é uma abordagem validada para implantar as tecnologias Cisco e NetApp como uma infraestrutura de nuvem compartilhada.

O data center FlexPod com o sistema NetApp All Flash AFF é uma plataforma de infraestrutura convergente que combina as melhores tecnologias do Cisco e do NetApp em uma poderosa plataforma convergente para aplicações empresariais. A Cisco e a NetApp trabalham em conjunto com a Oracle para dar suporte aos bancos de dados transacionais e sensíveis ao tempo de resposta mais exigentes exigidos pelos negócios atuais.

Este Cisco Validated Design (CVD) descreve a arquitetura de data center FlexPod de referência usando Cisco UCS e NetApp All Flash AFF Storage para implantar um ambiente de banco de dados Oracle RAC altamente disponível. Este documento mostra a configuração de hardware e software dos componentes envolvidos e os resultados de vários testes. Além disso, este documento oferece orientação de implementação e práticas recomendadas usando servidores de computação UCS Cisco, switches de interconexão de malha Cisco, switches MDS Cisco, switches Cisco Nexus, armazenamento NetApp AFF e banco de dados RAC Oracle.

"FlexPod Datacenter com bancos de dados Oracle RAC no Cisco UCS e NetApp AFF Série A."

FlexPod Datacenter com Oracle RAC em Oracle Linux

Cisco, Cisco, NetApp

O sistema de computação unificada da Cisco (Cisco UCS) é uma plataforma de data center de última geração que une computação, rede, acesso ao storage e virtualização em um único sistema coeso. O Cisco UCS é uma plataforma ideal para a arquitetura de workloads de bancos de dados essenciais. A combinação da plataforma Cisco UCS, do armazenamento NetApp e da arquitetura do Oracle Real Application Cluster (RAC) pode acelerar a transformação DA TI ao permitir implantações mais rápidas, maior flexibilidade de escolha, eficiência e riscos menores. Este Cisco Validated Design (CVD) destaca uma arquitetura de referência FlexPod flexível, multitenant, de alto desempenho e resiliente com o banco de dados Oracle 12c RAC.

A plataforma FlexPod, desenvolvida pela NetApp and Cisco, é uma solução de infraestrutura flexível e integrada que oferece tecnologias de servidor, rede e storage pré-validadas. Ele foi projetado para aumentar a capacidade de resposta DA TI às demandas de negócios e, ao mesmo tempo, reduzir o custo geral da computação. Pense no máximo tempo de atividade, risco mínimo. Os componentes do FlexPod são integrados e padronizados para ajudar você a alcançar implantações consistentes, repetíveis e oportunas. Você pode Planejar com precisão a energia, o espaço físico, a capacidade utilizável, o desempenho e o custo de cada implantação do FlexPod.

A FlexPod adota a tecnologia mais recente e simplifica de forma eficiente as cargas de trabalho do data center que redefinem a maneira COMO ELA agrega valor:

- Aproveite a funcionalidade dos arrays híbridos NetApp FAS com flash Pool para fornecer a funcionalidade de implantar a proporção precisa de flash para a Mídia giratória de sua aplicação ou ambiente específico.
- Utilize uma plataforma pré-validada para minimizar a interrupção dos negócios, melhorar a agilidade DA TI e reduzir o tempo de implantação de meses para semanas.
- Reduzir o tempo de administração e o custo total de propriedade (TCO) em 50%.
- Atenda ou supere as demandas de desempenho de hardware em constante expansão para workloads de data center.

"FlexPod Datacenter com Oracle RAC em Oracle Linux"

FlexPod Datacenter com bancos de dados Oracle RAC no Cisco UCS e NetApp AFF Série A.

Tushar Patel, Cisco Hardikkkumar Vyas, Cisco

O data center FlexPod com o sistema NetApp All Flash AFF é uma plataforma de infraestrutura convergente que combina as melhores tecnologias do Cisco e do NetApp em uma poderosa plataforma convergente para aplicações empresariais. A Cisco e a NetApp trabalham em conjunto com a Oracle para dar suporte aos bancos de dados transacionais e sensíveis ao tempo de resposta mais exigentes exigidos pelos negócios atuais.

Este Cisco Validated Design (CVD) descreve a arquitetura de data center FlexPod de referência usando Cisco UCS e NetApp All Flash AFF Storage para implantar um ambiente de banco de dados Oracle RAC altamente disponível. Este documento mostra a configuração de hardware e software dos componentes envolvidos e os resultados de vários testes. Além disso, este documento oferece orientação de implementação e práticas recomendadas usando servidores de computação UCS Cisco, switches de interconexão de malha Cisco, switches MDS Cisco, switches Cisco Nexus, armazenamento NetApp AFF e banco de dados RAC Oracle.

"FlexPod Datacenter com bancos de dados Oracle RAC no Cisco UCS e NetApp AFF Série A."

Microsoft SQL Server

FlexPod Datacenter para Microsoft SQL Server 2019 e VMware vSphere 6,7

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Este documento descreve uma arquitetura de referência do FlexPod usando os produtos de hardware e software mais recentes e fornece recomendações de implantação para hospedagem de bancos de dados do Microsoft SQL Server 2019 em ambientes virtualizados VMware ESXi. Essa solução também usa o Cisco Workload Otimization Manager (CWOM), que fornece recomendações automatizadas para a utilização ideal e eficiente de recursos tanto para cargas de trabalho SQL quanto para a infraestrutura.

A solução foi desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS) usando a versão de software unificada 4,1.1c para dar suporte às plataformas de hardware Cisco UCS, incluindo servidores blade da série B Cisco UCS, interconexões de malha Cisco UCS 6400, switches Cisco Série Nexus 9000 e arrays de storage da série NetApp AFF.

"FlexPod Datacenter para Microsoft SQL Server 2019 e VMware vSphere 6,7"

FlexPod Datacenter com Microsoft SQL Server 2016 e VMware vSphere 6,5

Cisco, Cisco, NetApp

Este documento discute uma arquitetura de referência do FlexPod usando os produtos de hardware e software mais recentes e fornece recomendações de configuração para a implantação de bancos de dados do Microsoft SQL Server em um ambiente virtualizado.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), usando a versão unificada de software para oferecer suporte às plataformas de hardware Cisco UCS, incluindo servidores tipo lâmina Cisco UCS da série B, interconexões de malha Cisco UCS 6300, switches Cisco da série 9000 e arrays de armazenamento NetApp All Flash. Além disso, essa solução inclui o VMware vSphere 6,5 e o vSphere 6,5, fornecendo vários novos recursos para otimizar a utilização do storage e facilitar uma nuvem privada.

"FlexPod Datacenter com Microsoft SQL Server 2016 e VMware vSphere 6,5"

FlexPod Datacenter com Microsoft SQL Server 2017 em VM Linux em execução em VMware e Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Este documento discute uma arquitetura de referência do FlexPod usando os produtos de hardware e software mais recentes e fornece recomendações de implantação para hospedagem de bancos de dados do Microsoft SQL Server em ambientes virtualizados VMware ESXi e Microsoft Windows Hyper-V com habilitação de suporte do Linux da Microsoft para implantação do SQL Server.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada (Cisco UCS) da Cisco, usando a versão de software unificada 4,0.1c para oferecer suporte às plataformas de hardware Cisco UCS, incluindo servidores tipo lâmina Cisco UCS da série B, interconexões de malha Cisco UCS 6300, switches da série Cisco Nexus 9000 e arrays de armazenamento da série NetApp AFF.

"FlexPod Datacenter com Microsoft SQL Server 2017 em VM Linux em execução em VMware e Hyper-V."

FlexPod Datacenter com Microsoft SQL Server 2017 em VM Linux em execução em VMware e Hyper-V.

Gopu Narasimha Reddy, Cisco Sanjeev Naldurgkar, Cisco Atul Bhalodia, NetApp

Este documento discute uma arquitetura de referência do FlexPod usando os produtos de hardware e software mais recentes e fornece recomendações de implantação para hospedagem de bancos de dados do Microsoft SQL Server em ambientes virtualizados VMware ESXi e Microsoft Windows Hyper-V com habilitação de suporte do Linux da Microsoft para implantação do SQL Server.

A arquitetura de solução recomendada foi desenvolvida com base no sistema de computação unificada (Cisco UCS) da Cisco, usando a versão de software unificada 4,0.1c para oferecer suporte às plataformas de hardware Cisco UCS, incluindo servidores tipo lâmina Cisco UCS da série B, interconexões de malha Cisco UCS 6300, switches da série Cisco Nexus 9000 e arrays de armazenamento da série NetApp AFF.

"FlexPod Datacenter com Microsoft SQL Server 2017 em VM Linux em execução em VMware e Hyper-V."

Saúde

FlexPod para genômica

TR-4911: Genômica de FlexPod

JayaKishore Esanakula, NetApp

Há poucos campos da medicina que são mais importantes do que a genômica para a saúde e as ciências da vida, e a genômica está rapidamente se tornando uma ferramenta clínica chave para médicos e enfermeiros. A genômica, quando combinada com imagens médicas e patologia digital, nos ajuda a entender como os genes de um paciente podem ser afetados por protocolos de tratamento. O sucesso da genômica na saúde depende cada vez mais da interoperabilidade de dados em escala. O objetivo final é fazer sentido dos enormes volumes de dados genéticos e identificar correlações e variantes clinicamente relevantes que melhoram o diagnóstico e tornam a medicina de precisão uma realidade. A genômica nos ajuda a entender a origem dos surtos de doenças, como as doenças evoluem e quais tratamentos e estratégias podem ser eficazes. Claramente, a genômica tem muitos benefícios que abrangem a prevenção, o diagnóstico e o tratamento. As organizações de saúde estão enfrentando vários desafios, incluindo os seguintes:

- Melhoria da qualidade dos cuidados
- Cuidado baseado em valor
- Explosão de dados
- Medicina de precisão
- Pandemias
- Wearables, monitoração remota, e cuidado
- Segurança cibernética

Vias clínicas padronizadas e protocolos clínicos são um dos componentes críticos da medicina moderna. Um dos principais aspetos da padronização é a interoperabilidade entre os prestadores de cuidados, não apenas para Registros médicos, mas também para dados genômicos. A grande questão é que as organizações de saúde abandonarão a propriedade de dados genômicos em vez da propriedade dos pacientes de seus dados pessoais de genômica e Registros médicos relacionados?

Os dados interoperáveis dos pacientes são fundamentais para permitir a medicina de precisão, uma das forças impulsionadoras da recente explosão de crescimento de dados. O objetivo da medicina de precisão é tornar a manutenção da saúde, prevenção de doenças, diagnósticos e soluções de tratamento mais eficazes e precisas.

A taxa de crescimento de dados tem sido exponencial. No início de fevereiro de 2021, os laboratórios dos EUA sequenciaram aproximadamente 8.000 cepas de COVID-19 por semana. O número de genomas sequenciados aumentou para 29.000 por semana em abril de 2021. Cada genoma humano totalmente sequenciado tem cerca de 125GB mm de tamanho. Portanto, a uma taxa de 29.000 genomas sequenciados por semana, o armazenamento total do genoma em repouso seria mais de 180 petabytes por ano. Vários países comprometeram recursos para a epidemiologia genômica para melhorar a vigilância genômica e se

preparar para a próxima onda de desafios globais de saúde.

O custo reduzido da pesquisa genômica está impulsionando testes genéticos e pesquisas a um ritmo sem precedentes. Os três PS estão em um ponto de inflexão: Poder do computador, privacidade de dados e personalização da medicina. Em 2025, os pesquisadores estimam que 100 milhões a 2 bilhões de genomas humanos serão sequenciados. Para que a genômica seja eficaz e uma proposta valiosa, os recursos de genômica devem ser parte perfeita dos fluxos de trabalho de cuidados; eles devem ser fáceis de acessar e úteis durante a visita do paciente. Também é igualmente importante que os dados de registo médico eletrónico do paciente sejam integrados com os dados genómicos do paciente. Com o advento da infraestrutura convergente de última geração, como o FlexPod, as organizações podem levar suas capacidades genômicas para os fluxos de trabalho diários de médicos, enfermeiros e gerentes clínicos. Para obter as informações mais recentes sobre a plataforma FlexPod, consulte este "FlexPod Datacenter com Cisco UCS X-Series White Paper".

Para um médico, o verdadeiro valor da genômica inclui medicina de precisão e planos de tratamento personalizados com base nos dados genômicos de um paciente. Nunca houve tal sinergia entre clínicos e cientistas de dados no passado, e a genômica está se beneficiando das inovações tecnológicas no passado recente, e também parcerias reais entre organizações de saúde e líderes de tecnologia no setor.

Centros médicos acadêmicos e outras organizações de saúde e ciências da vida estão a caminho de estabelecer o centro de excelência (COE) na ciência do genoma. De acordo com o Dr. Charlie Gersbach, Dr. Greg Crawford, e o Dr. Tim e Reddy da Duke University, "sabemos que os genes não são ligados ou desligados por um simples interrutor binário, mas em vez disso é um resultado de vários interrutores reguladores de genes que trabalham juntos. Eles também determinaram que "nenhuma dessas partes do genoma funciona isoladamente. O genoma é uma teia muito complicada que a evolução tem tecido" ("ref").

A NetApp e a Cisco têm trabalhado arduamente na implementação de melhorias incrementais na plataforma FlexPod há mais de 10 anos. Todo o feedback do cliente é ouvido, avaliado e vinculado aos fluxos de valor e conjuntos de recursos no FlexPod. É esse loop contínuo de feedback, colaboração, aprimoramento e celebração que diferencia a FlexPod como uma plataforma de infraestrutura convergente confiável em todo o mundo. Ela foi simplificada e projetada do zero para ser a plataforma mais confiável, robusta, versátil e ágil para organizações de saúde.

Âmbito de aplicação

A plataforma de infraestrutura convergente do FlexPod permite que uma organização de saúde hospede um ou mais workloads genômicos, além de outras aplicações clínicas e não clínicas do setor de saúde. Este relatório técnico usa uma ferramenta de genômica padrão do setor de código aberto chamada GATK durante a validação da plataforma FlexPod. No entanto, uma discussão mais profunda sobre genômica ou GATK está fora do escopo deste documento.

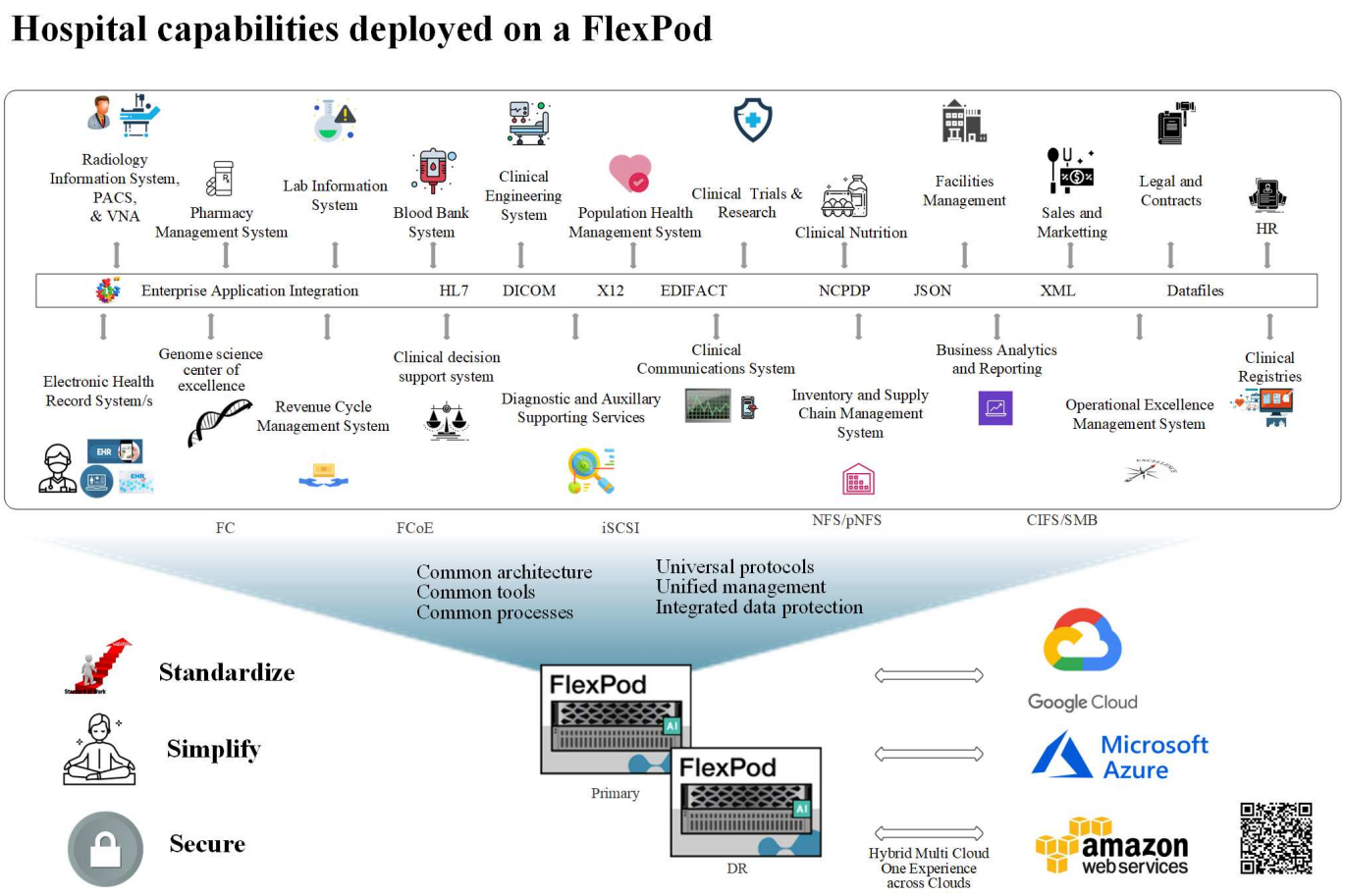
Público-alvo

Este documento destina-se a líderes técnicos do setor de saúde e a engenheiros de soluções de parceiros da Cisco e da NetApp e à equipe de serviços profissionais. O NetApp presume que o leitor entenda bem os conceitos de dimensionamento de storage e computação, além de ter familiaridade técnica com ameaças ao setor de saúde, segurança do setor de saúde, sistemas DE TI do setor de saúde, Cisco UCS e sistemas de storage NetApp.

Recursos hospitalares implantados no FlexPod

Um hospital típico tem um conjunto diversificado de SISTEMAS DE TI. A maioria desses sistemas é comprada de um fornecedor, enquanto muito poucos são construídos pelo sistema hospitalar em casa. Portanto, o sistema hospitalar deve gerenciar um ambiente de infraestrutura diversificado em seus data centers. Quando os hospitais unificam seus sistemas em uma plataforma de infraestrutura convergente, como a FlexPod, as

organizações podem padronizar as operações de data center. Com o FlexPod, as organizações de saúde podem implementar sistemas clínicos e não clínicos na mesma plataforma, unificando as operações do data center.



"Próximo: Benefícios da implantação de workloads genômicos no FlexPod."

Benefícios da implantação de workloads genômicos no FlexPod

"Anterior: Introdução."

Esta seção fornece uma breve lista de benefícios para a execução de um workload genômico em uma plataforma de infraestrutura convergente do FlexPod. Vamos descrever rapidamente as capacidades de um hospital. A visualização da arquitetura de negócios a seguir mostra os recursos de um hospital implantados em uma plataforma de infraestrutura convergente FlexPod pronta para nuvem híbrida.

- **Evite silos na área de saúde.** Silos na saúde são uma preocupação muito real. Os departamentos costumam ser isolados em seu próprio conjunto de hardware e software, não por escolha, mas organicamente pela evolução. Por exemplo, radiologia, cardiologia, EHR, genômica, análise, ciclo de receita e outros departamentos acabam com seu conjunto individual de software e hardware dedicados. As organizações de saúde mantêm um conjunto limitado de profissionais DE TI para gerenciar seus ativos de hardware e software. O ponto de inflexão surge quando este conjunto de indivíduos é esperado para gerenciar um conjunto muito diversificado de hardware e software. A heterogeneidade é agravada por um conjunto incongruente de processos trazidos à organização de saúde pelos fornecedores.
- **Comece pequeno e cresça.** O kit de ferramentas GATK é ajustado para execução de CPU, que melhor

suites plataformas como o FlexPod. O FlexPod permite escalabilidade independente de rede, computação e storage. Escale os negócios gradualmente e de acordo com o crescimento das funcionalidades de genômica e do ambiente. As organizações de saúde não precisam investir em plataformas especializadas para executar workloads genômicos. Em vez disso, as organizações podem utilizar plataformas versáteis, como um FlexPod, para executar workloads genômicos e não genômicos na mesma plataforma. Por exemplo, se o departamento de pediatria quiser implementar funcionalidade genômica, a liderança DE TI pode provisionar computação, storage e rede em uma instância existente do FlexPod. À medida que a unidade de negócios genômica cresce, as organizações de saúde podem escalar a plataforma FlexPod conforme necessário.

- * Painel de controle único e flexibilidade incomparável.* O Cisco Intersight simplifica significativamente as operações DE TI ao unir aplicativos à infraestrutura, fornecendo visibilidade e gerenciamento de servidores bare-metal e hipervisores a aplicativos sem servidor, reduzindo custos e mitigando riscos. Essa plataforma SaaS unificada usa um design unificado de API aberta que se integra nativamente a plataformas e ferramentas de terceiros. Além disso, permite que o gerenciamento ocorra da equipe de operações do data center no local ou de qualquer lugar usando um aplicativo móvel.

  Os usuários rapidamente desbloqueiam valor tangível em seu ambiente, aproveitando a Intersight como plataforma de gerenciamento. Habilitando a automação para muitas tarefas manuais diárias, o Intersight remove erros e simplifica suas operações diárias. Além disso, os recursos avançados de suporte facilitados pelo Intersight permitem que os adotantes se mantenham à frente dos problemas e acelerem a resolução de problemas. Combinadas, as organizações gastam muito menos tempo e dinheiro em sua infraestrutura de aplicações e mais tempo no desenvolvimento dos negócios principais.

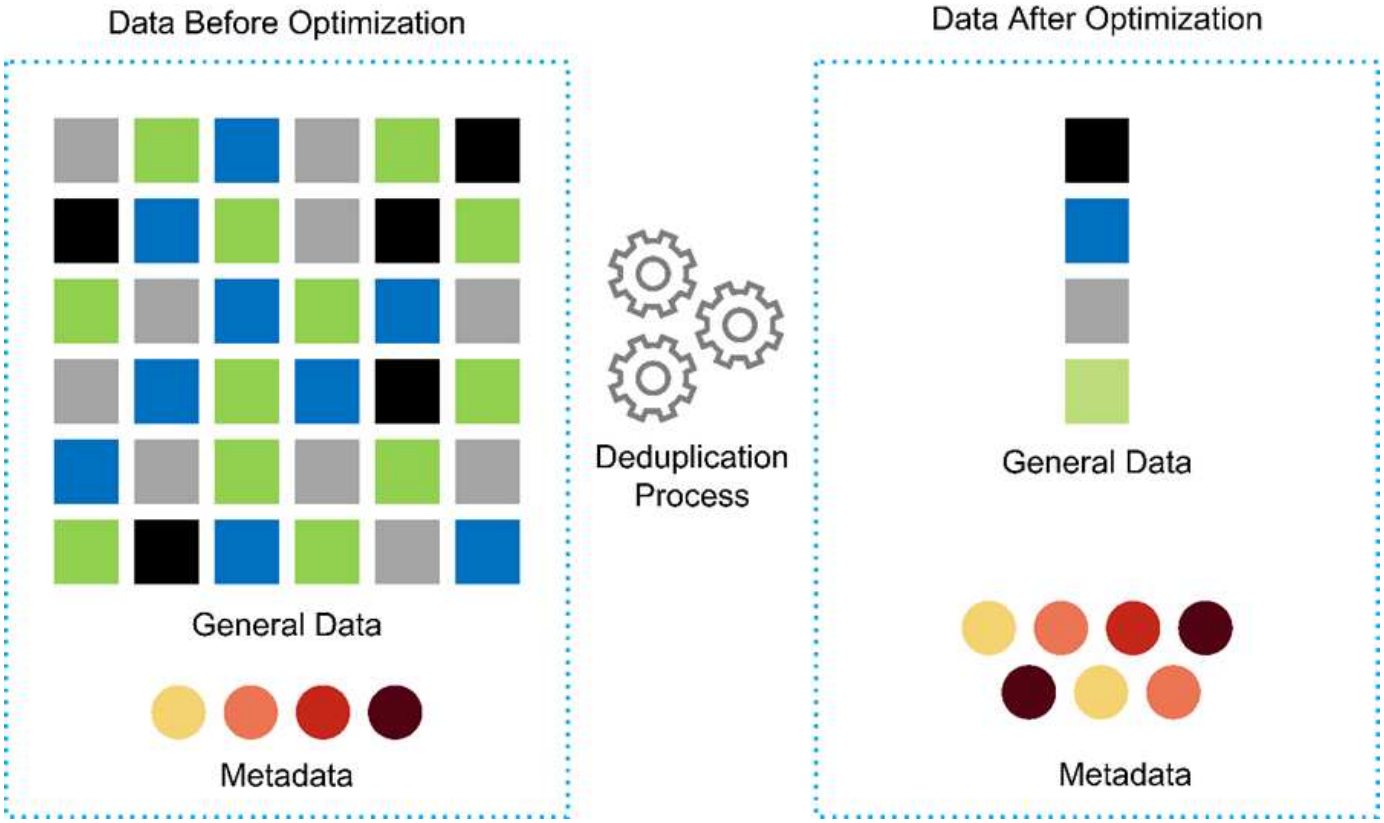
  Com o gerenciamento do Intersight e a arquitetura facilmente dimensionável do FlexPod, as organizações podem executar vários workloads de genoma em uma única plataforma FlexPod, aumentando a utilização e reduzindo o custo total de propriedade (TCO). O FlexPod permite um dimensionamento flexível, com opções começando com nosso pequeno FlexPod Express e dimensionando para implementações de data center FlexPod grandes. Com os recursos de controle de acesso baseados em função integrados ao Cisco Intersight, as organizações de saúde podem implementar mecanismos robustos de controle de acesso, evitando a necessidade de stacks de infraestrutura separados. Várias unidades de negócios dentro da organização de saúde podem aproveitar a genômica como uma competência principal.

  Em última análise, o FlexPod ajuda a simplificar as operações DE TI e reduzir os custos operacionais, e permite que os administradores de infraestrutura DE TI se concentrem em tarefas que ajudam os médicos a inovar em vez de serem relegados para manter as luzes acesas.

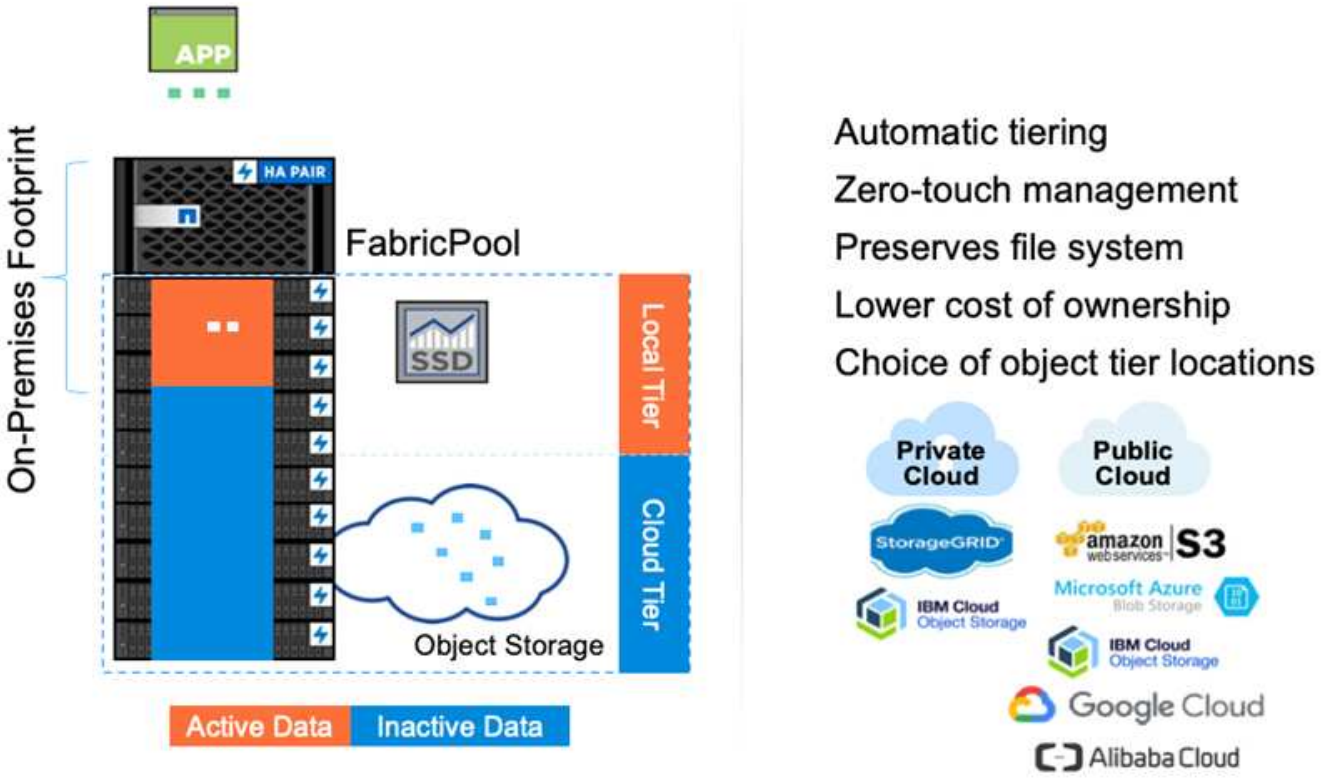
- **Design validado e resultados garantidos.** Os guias de design e implantação do FlexPod são validados para serem repetíveis, e abrangem detalhes abrangentes de configuração e práticas recomendadas do setor, necessárias para implantar um FlexPod com confiança. Os guias de design, guias de implantação e arquiteturas validados pela Cisco e pela NetApp ajudam sua organização de saúde ou ciências biológicas a remover suposições da implementação de uma plataforma validada e confiável desde o início. Com o FlexPod, você acelera os tempos de implantação e reduz custos, complexidade e riscos. Os designs validados da FlexPod e os guias de implantação estabelecem o FlexPod como a plataforma ideal para uma variedade de workloads genômicos.
- **Inovação e agilidade.** O FlexPod é recomendado como uma plataforma ideal por EHRs como Epic, Cerner, Meditech e sistemas de imagem como Agfa, GE, Philips. Para obter mais informações sobre "Rolo de honra épico" a arquitetura da plataforma e de destino, consulte a web do usuário Epic. Executar genômica no "FlexPod" permite que as organizações de saúde continuem sua jornada de inovação com agilidade. Com o FlexPod, a implementação da mudança organizacional vem naturalmente. Quando as organizações padronizam a plataforma FlexPod, os especialistas EM TI do setor de saúde podem provisionar seu tempo, esforço e recursos para inovar e, assim, ser tão ágeis quanto o ecossistema exige.
- **Dados liberados.** Com a plataforma de infraestrutura convergente da FlexPod e um sistema de storage da NetApp ONTAP, os dados genômicos podem ser disponibilizados e acessados por meio de uma ampla

variedade de protocolos em escala em uma plataforma única. O FlexPod com NetApp ONTAP oferece uma plataforma de nuvem híbrida simples, intuitiva e poderosa. Seu Data Fabric com tecnologia da NetApp ONTAP truta dados juntos em diferentes locais, além de fronteiras físicas e entre aplicações. Seu Data Fabric foi desenvolvido para empresas orientadas pelos dados em um mundo centrado nos dados. Os dados são criados e usados em vários locais, e geralmente precisam ser aproveitados e compartilhados com outros locais, aplicações e infraestruturas. Portanto, você precisa de uma maneira consistente e integrada de gerenciá-la. A FlexPod coloca sua equipe DE TI no controle e simplifica a complexidade cada vez maior DA TI.

- **Alocação segura a vários clientes.** O FlexPod usa módulos criptográficos compatíveis com FIPS 140-2, permitindo que as organizações implementem a segurança como um elemento fundamental, e não um pensamento posterior. O FlexPod permite que as organizações implementem a alocação segura a vários clientes a partir de uma única plataforma de infraestrutura convergente, independentemente do tamanho da plataforma. O FlexPod com alocação segura a vários clientes e a QoS ajuda na separação de workloads e maximiza a utilização. Isso ajuda a evitar que o capital seja bloqueado em plataformas especializadas que sejam potencialmente subutilizadas e que exijam um conjunto de habilidades especializado para gerenciar.
- **Eficiência de armazenamento.** A genômica exige que o storage subjacente tenha funcionalidades de eficiência de storage líderes do setor. Você pode reduzir os custos de storage com recursos de eficiência de storage da NetApp, como deduplicação (in-line e sob demanda), compressão de dados e compactação de dados ("ref"). A deduplicação do NetApp fornece deduplicação em nível de bloco em um FlexVol volume. Essencialmente, a deduplicação remove blocos duplicados, armazenando apenas blocos exclusivos no FlexVol volume. A deduplicação funciona com um alto grau de granularidade e opera no sistema de arquivos ativo do FlexVol volume. A figura a seguir mostra uma visão geral de como a deduplicação do NetApp funciona. A deduplicação é transparente para aplicativos. Portanto, ele pode ser usado para deduplicar dados provenientes de qualquer aplicativo que use o sistema NetApp. Você pode executar a deduplicação de volume como um processo inline e como um processo em segundo plano. Você pode configurá-lo para ser executado automaticamente, agendado ou manualmente por meio da CLI, do Gerenciador de sistemas do NetApp ONTAP ou do NetApp Active IQ Unified Manager.



- **Ativar interoperabilidade genômica.** O ONTAP FlexCache é um recurso de armazenamento em cache remoto que simplifica a distribuição de arquivos, reduz a latência da WAN e reduz os custos de largura de banda da WAN ("ref"). Uma das principais atividades durante a identificação e anotação de variantes genômicas é a colaboração entre clínicos. A tecnologia ONTAP FlexCache aumenta a taxa de transferência de dados mesmo quando os clínicos colaboradores estão em diferentes locais geográficos. Dado o tamanho típico de um arquivo *.BAM (1GB a 100s GB), é fundamental que a plataforma subjacente possa disponibilizar arquivos para médicos em diferentes locais geográficos. O FlexPod com ONTAP FlexCache torna os dados genômicos e as aplicações verdadeiramente prontos para multisite, o que torna a colaboração entre pesquisadores do mundo todo otimizada com baixa latência e alta taxa de transferência. As organizações do setor de saúde que executam aplicações genômicas em uma configuração multisite podem fazer escalabilidade horizontal usando o Data Fabric para equilibrar a gerenciabilidade com custo e velocidade.
- **Uso inteligente da plataforma de armazenamento.** O FlexPod com disposição automática em camadas do ONTAP e a tecnologia NetApp Fabric Pool simplificam o gerenciamento de dados. O FabricPool ajuda a reduzir os custos de storage sem comprometer o desempenho, a eficiência, a segurança ou a proteção. O FabricPool é transparente para as aplicações empresariais e aproveita as eficiências de nuvem ao reduzir o TCO de storage sem a necessidade de rearquitetar a infraestrutura de aplicações. O FlexPod pode se beneficiar das funcionalidades de disposição em camadas de storage do FabricPool para usar mais eficiência o storage flash ONTAP. Para obter mais informações, "FlexPod com FabricPool"consulte . O diagrama a seguir fornece uma visão geral de alto nível do FabricPool e seus benefícios.

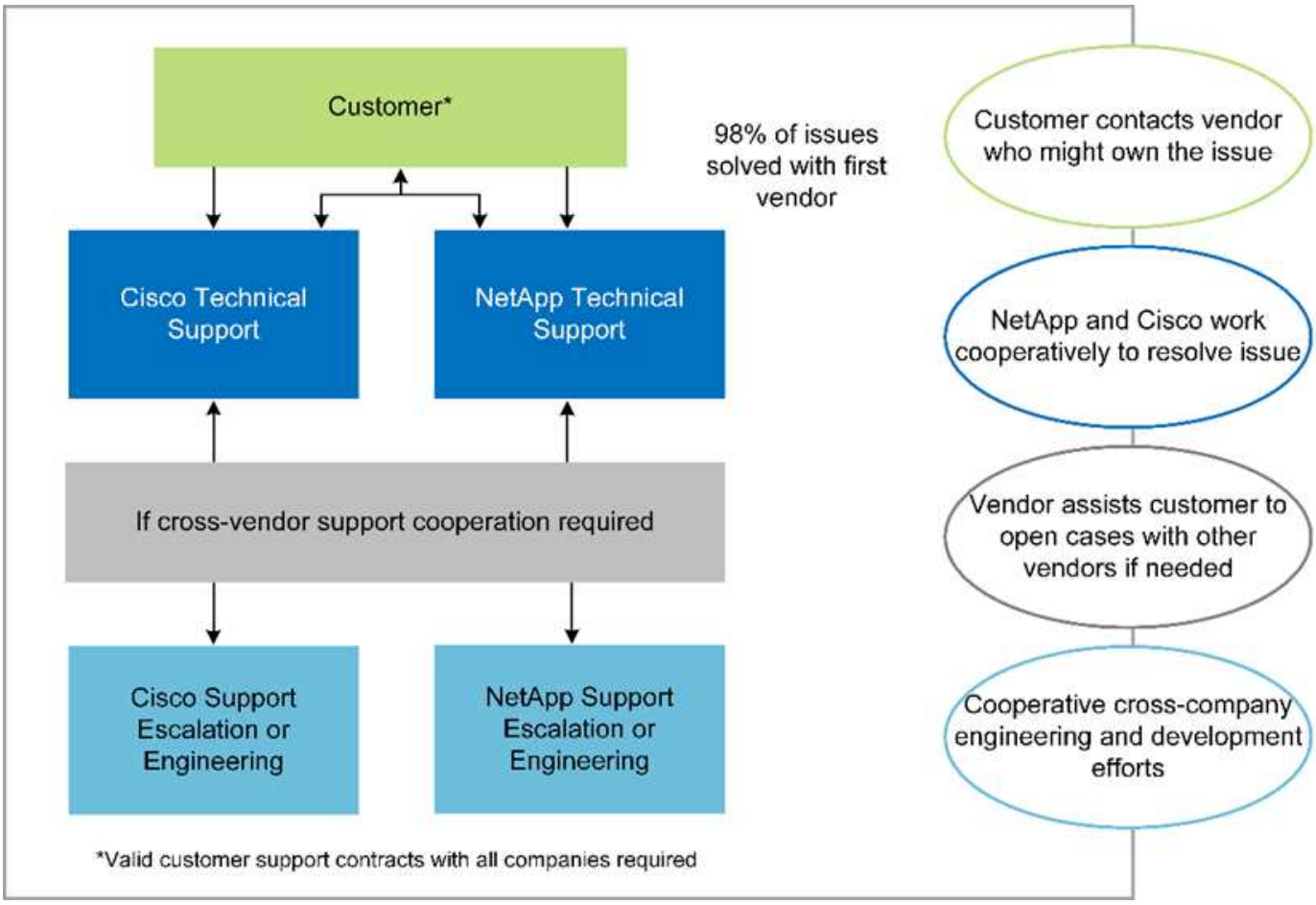


- * Análise de variantes mais rápidas e anotação.* A plataforma FlexPod é mais rápida de implantar e operacionalizar. A plataforma FlexPod permite a colaboração do médico ao disponibilizar dados em escala com baixa latência e maior taxa de transferência. O aumento da interoperabilidade permite a inovação. As organizações de saúde podem executar seus workloads genômicos e não genômicos lado a lado, o que significa que as organizações não precisam de plataformas especializadas para iniciar sua jornada genômica.

O FlexPod ONTAP rotineiramente adiciona recursos de ponta à plataforma de armazenamento. O data center FlexPod é a base ideal de infraestrutura compartilhada para implantar o FC-NVMe a fim de permitir acesso ao storage de alto desempenho às aplicações que precisam dele. À medida que o FC-NVMe evolui para incluir suporte a alta disponibilidade, multipathing e sistemas operacionais adicionais, o FlexPod é adequado como a plataforma escolhida, fornecendo a escalabilidade e a confiabilidade necessárias para dar suporte a esses recursos. O ONTAP com e/S mais rápido e NVMe completo permite que análises genômicas sejam concluídas com mais rapidez ("ref").

Os dados do genoma bruto sequenciado produzem grandes tamanhos de arquivo, e é importante que esses arquivos sejam disponibilizados aos analisadores variantes para reduzir o tempo total que leva da coleta de amostras para anotação variante. O NVMe (nonvolatile Memory Express), quando usado como protocolo de transporte de dados e acesso ao storage, fornece níveis sem precedentes de taxa de transferência e tempos de resposta mais rápidos. O FlexPod implanta o protocolo NVMe ao acessar o storage flash por meio do barramento PCI Express (PCIe). O PCIe permite a implementação de dezenas de milhares de filas de comando, aumentando a paralelização e a taxa de transferência. Um único protocolo, desde o armazenamento até a memória, torna o acesso aos dados mais rápido.

- **Agilidade para pesquisa clínica desde o início.** A capacidade de armazenamento e o desempenho flexíveis e expansíveis permitem que as organizações de pesquisa de saúde otimizem o ambiente de forma elástica ou just-in-time (JIT). Ao desacoplar o storage da infraestrutura de computação e rede, a plataforma FlexPod pode ser escalada e horizontal sem interrupção. Com o Cisco Intersight, a plataforma FlexPod pode ser gerenciada com workflows automatizados incorporados e personalizados. Os workflows do Cisco Intersight permitem que as organizações de saúde reduzam o tempo de gerenciamento do ciclo de vida das aplicações. Quando um centro médico acadêmico exige que os dados do paciente sejam anonimizados e disponibilizados ao seu centro para informática de pesquisa e/ou centro para qualidade, sua organização DE TI pode aproveitar os fluxos de trabalho do Cisco Intersight FlexPod para fazer backups, clonar e restaurar dados em questão de segundos, não horas. Com o NetApp Trident e o Kubernetes, as ORGANIZAÇÕES DE TI podem provisionar novos cientistas de dados e disponibilizar dados clínicos para desenvolvimento de modelos em questão de minutos, às vezes até em segundos.
- **Proteção de dados do genoma.** O NetApp SnapLock fornece um volume de propósito especial no qual os arquivos podem ser armazenados e comprometidos com um estado não apagável e não regravável. Os dados de produção do usuário que residem em um FlexVol volume podem ser espelhados ou abobadados a um volume SnapLock por meio da tecnologia NetApp SnapMirror ou SnapVault. Os arquivos no volume SnapLock, o próprio volume e seu agregado de hospedagem não podem ser excluídos até o final do período de retenção. Usando o software ONTAP FPolicy, as organizações podem evitar ataques de ransomware, despermitindo operações em arquivos com extensões específicas. Um evento FPolicy pode ser acionado para operações de arquivo específicas. O evento está vinculado a uma política, que chama o mecanismo que ele precisa usar. Você pode configurar uma política com um conjunto de extensões de arquivo que podem potencialmente conter ransomware. Quando um arquivo com uma extensão não permitida tenta executar uma operação não autorizada, o FPolicy impede que essa operação seja executada ("ref").
- **Suporte cooperativo do FlexPod.** A NetApp e a Cisco estabeleceram o suporte cooperativo do FlexPod, um modelo de suporte forte, dimensionável e flexível para atender aos requisitos exclusivos de suporte da infraestrutura convergente do FlexPod. Esse modelo usa a experiência, os recursos e a experiência combinada de suporte técnico da NetApp e da Cisco para oferecer um processo simplificado para identificar e resolver problemas de suporte da FlexPod, independentemente de onde o problema reside. A figura a seguir fornece uma visão geral do modelo de suporte cooperativo do FlexPod. O cliente entra em Contato com o fornecedor que pode ser o dono do problema, e tanto a Cisco quanto a NetApp trabalham cooperativamente para resolvê-lo. A Cisco e a NetApp têm equipes de engenharia e desenvolvimento entre empresas que trabalham lado a lado para resolver problemas. Esse modelo de suporte reduz a perda de informações durante a tradução, permite a confiança e reduz o tempo de inatividade.

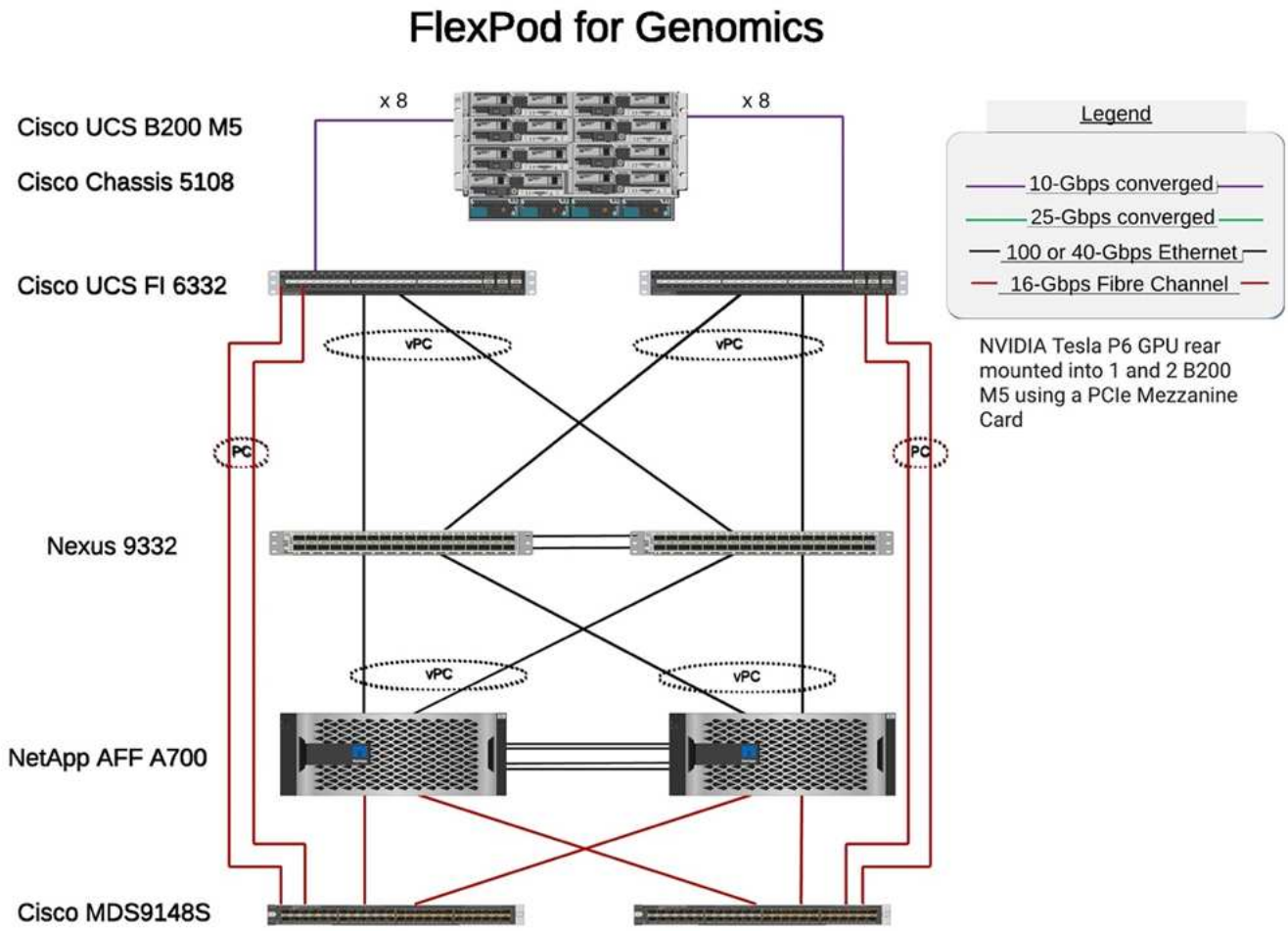


"Próximo: Componentes de hardware e software da infraestrutura da solução."

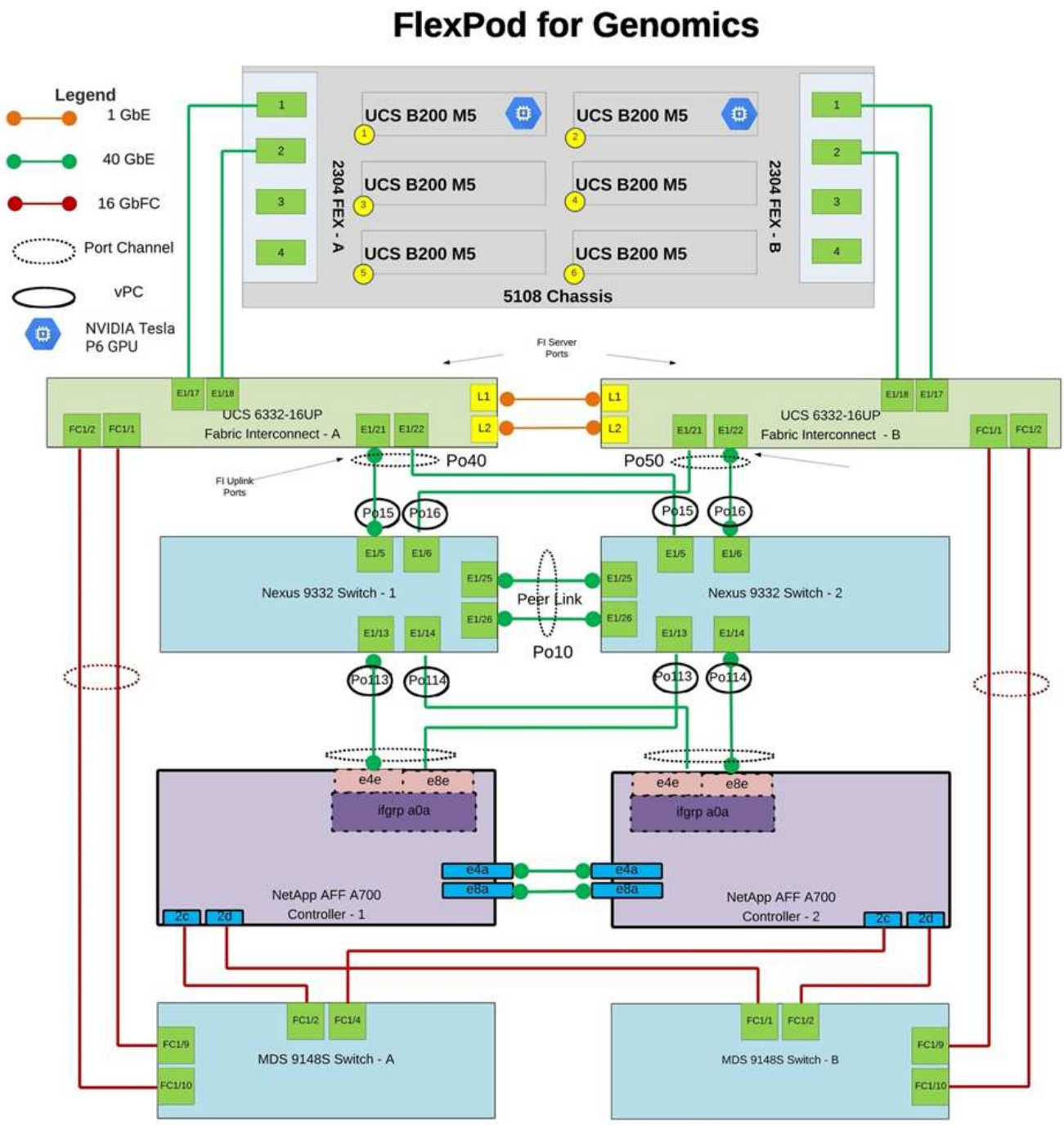
Componentes de hardware e software da infraestrutura da solução

"Anterior: Benefícios da implantação de workloads genômicos no FlexPod."

A figura seguinte mostra o sistema FlexPod utilizado para a configuração e validação do GATK. Usamos "Data center FlexPod com VMware vSphere 7,0 e NetApp ONTAP 9 .7 Cisco Validated Design (CVD)" durante o processo de configuração.



O diagrama a seguir mostra os detalhes do cabeamento do FlexPod.



A tabela a seguir lista os componentes de hardware usados durante a ativação do teste GATK em um FlexPod. Aqui está o "Ferramenta de Matriz de interoperabilidade do NetApp" (IMT) e "Lista de compatibilidade de hardware Cisco (HCL)".

Camada	Família de produtos	Quantidade e modelo	Detalhes
Computação	Chassi do Cisco UCS 5108	1 ou 2	
	Servidores blade Cisco UCS	6 B200 M5	Cada um com 2x 20 ou mais núcleos, 2,7GHz GB e 128-384GB GB de RAM

Camada	Família de produtos	Quantidade e modelo	Detalhes
	Cartão de interface virtual Cisco UCS (VIC)	Cisco UCS 1440	Consulte
	2x interconexões de tecido Cisco UCS	6332	-
Rede	Switches Cisco Nexus	2x Cisco Nexus 9332	-
Rede de armazenamento	Rede IP para acesso ao storage por protocolos SMB/CIFS, NFS ou iSCSI	Mesmos switches de rede como acima	-
	Acesso ao storage por FC	2x Cisco MDS 9148S	-
Armazenamento	Sistema de storage all-flash NetApp AFF A700	Cluster de 1 GbE	Cluster com dois nós
	Compartimento de disco	Um compartimento de disco de DS224C TB ou NS224 TB	Totalmente preenchido com 24 unidades
	SSD	24, 1,2TB ou maior capacidade	-

Esta tabela lista o software de infraestrutura.

Software	Família de produtos	Versão ou lançamento	Detalhes
Vários	Linux	RHEL 8,3	-
	Windows	Windows Server 2012 R2 (64 bits)	-
	NetApp ONTAP	ONTAP 9 .8 ou posterior	-
	Interconexão de malha Cisco UCS	Cisco UCS Manager 4,1 ou posterior	-
	Switches Ethernet Cisco série 3000 ou 9000	Para a série 9000, 7,0(3)i7(7) ou posterior para a série 3000, 9,2(4) ou posterior	-
	Cisco FC: Cisco MDS 9132T	8,4(1a) ou posterior	-
	Hipervisor	VMware vSphere ESXi 7,0	-
Armazenamento	Sistema de gerenciamento de hipervisor	VMware vCenter Server 7,0 (vCSA) ou posterior	-
Rede	Console de storage virtual (VSC) do NetApp	VSC 9,7 ou posterior	-
	NetApp SnapCenter	SnapCenter 4,3 ou posterior	-

Software	Família de produtos	Versão ou lançamento	Detalhes
	Gerente do Cisco UCS	4,1(3c) ou posterior	
Hipervisor	ESXi		
Gerenciamento	Sistema de gerenciamento de hypervisor VMware vCenter Server 7,0 (vCSA) ou posterior		
	Console de storage virtual (VSC) do NetApp	VSC 9,7 ou posterior	
	NetApp SnapCenter	SnapCenter 4,3 ou posterior	
	Gerente do Cisco UCS	4,1(3c) ou posterior	

"Próximo: Genômica - configuração e execução do GATK."

Genômica - configuração e execução do GATK

"Anterior: Componentes de hardware e software de infraestrutura de solução."

De acordo com o National Human Genome Research Institute ("NHGRI"), "a genômica é o estudo de todos os genes de uma pessoa (o genoma), incluindo interações desses genes entre si e com o ambiente de uma pessoa. "

De acordo com o "NHGRI", "o ácido desoxirribonucleico (DNA) é o composto químico que contém as instruções necessárias para desenvolver e direcionar as atividades de quase todos os organismos vivos. As moléculas de DNA são feitas de dois fios torcidos, emparelhados, muitas vezes referidos como uma hélice dupla." "O conjunto completo de DNA de um organismo é chamado de genoma."

Sequenciamento é o processo de determinação da ordem exata das bases em uma cadeia de DNA. Um dos tipos mais comuns de sequenciamento usado hoje é chamado sequenciamento por síntese. Esta técnica utiliza a emissão de sinais fluorescentes para ordenar as bases. Os pesquisadores podem usar o sequenciamento de DNA para procurar variações genéticas e quaisquer mutações que possam desempenhar um papel no desenvolvimento ou progressão de uma doença enquanto uma pessoa ainda está em estágio embrionário.

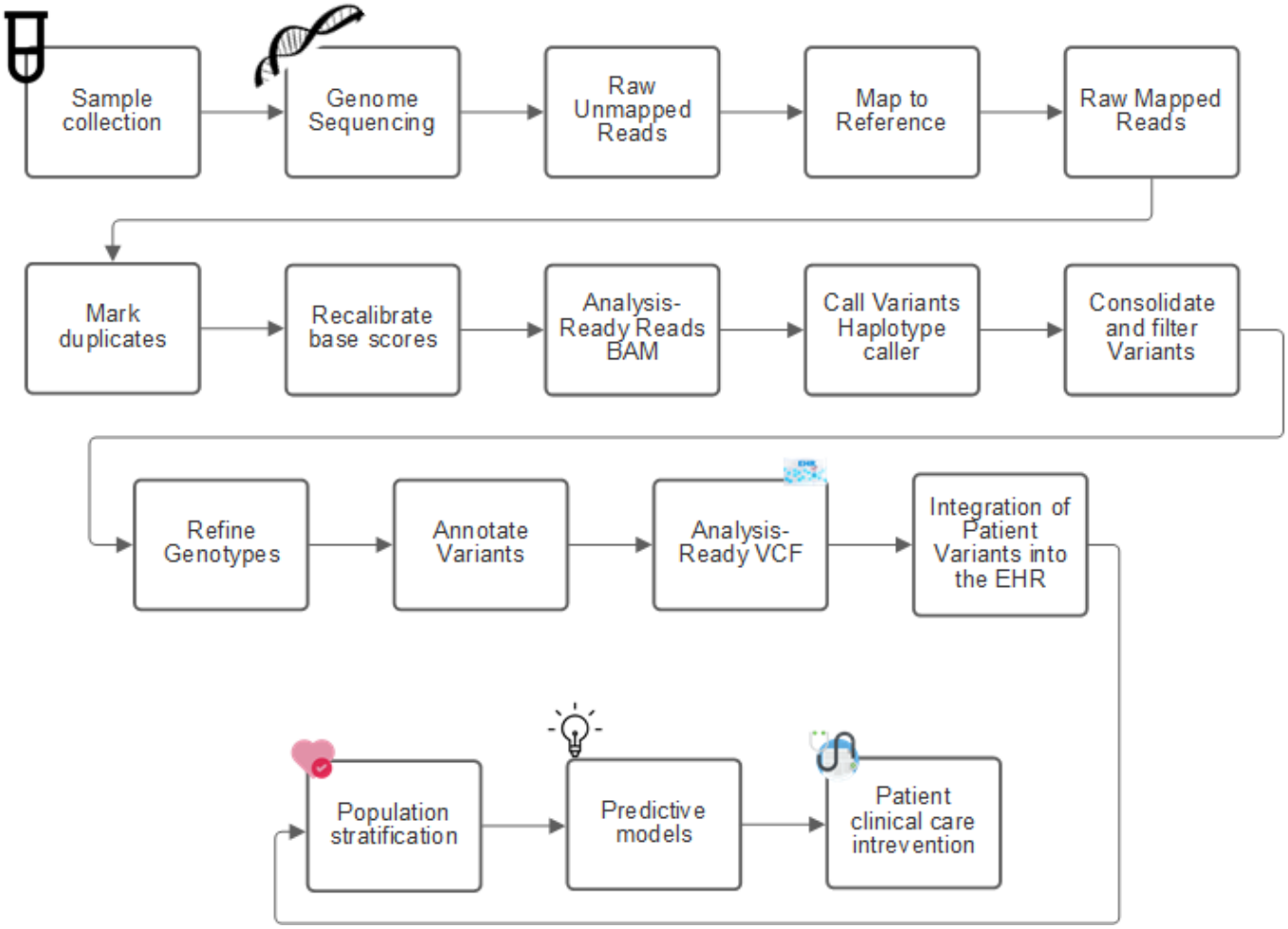
Da amostra à identificação, anotação e previsão da variante

Em um nível elevado, a genômica pode ser classificada nas seguintes etapas. Esta não é uma lista exaustiva:

1. Colheita de amostras.
2. "Sequenciamento do genoma" usando um sequenciador para gerar os dados brutos.
3. Pré-processamento. Por exemplo "deduplicação", usando "Picard".
4. Análise genômica.
    a. Mapeamento para um genoma de referência.
    b. "Variante" Identificação e anotação normalmente realizadas usando o GATK e ferramentas semelhantes.

5. Integração no sistema de registo eletrónico de saúde (EHR).
6. "Estratificação populacional" e identificação da variação genética entre localização geográfica e origem étnica.
7. "Modelos preditivos" usando polimorfismo de um único nucleotídeo significativo.
8. "Validação".

A figura a seguir mostra o processo de amostragem à identificação, anotação e previsão da variante.



O projeto Genoma humano foi concluído em abril de 2003, e o projeto fez uma simulação de alta qualidade da sequência do genoma humano disponível no domínio público. Este genoma de referência iniciou uma explosão na pesquisa e desenvolvimento de capacidades genômicas. Praticamente toda doença humana tem uma assinatura nos genes desse ser humano. Até recentemente, os médicos estavam alavancando genes para prever e determinar defeitos congênitos como anemia falciforme, que é causada por um certo padrão de herança causado por uma mudança em um único gene. O tesouro dos dados que estão sendo disponibilizados pelo projeto do genoma humano levou ao advento do estado atual das capacidades genômicas.

A genômica tem um amplo conjunto de benefícios. Aqui está um pequeno conjunto de benefícios nos domínios da saúde e ciências da vida:

- Melhor diagnóstico no ponto de atendimento
- Melhor prognóstico

- Medicina de precisão
- Planos de tratamento personalizados
- Melhor monitoramento de doenças
- Redução de eventos adversos
- Melhor acesso a terapias
- Melhor monitoramento de doenças
- Participação efetiva em ensaios clínicos e melhor seleção de pacientes para ensaios clínicos com base em genótipos.

A genômica ocorre "besta de quatro cabeças," devido às demandas computacionais em todo o ciclo de vida de um conjunto de dados: Aquisição, storage, distribuição e análise.

Genoma Analysis Toolkit (GATK)

O GATK foi desenvolvido como uma plataforma de ciência de dados na "Instituto amplo". O GATK é um conjunto de ferramentas de código aberto que permitem a análise do genoma, especificamente descoberta de variantes, identificação, anotação e genotipagem. Um dos benefícios do GATK é que o conjunto de ferramentas e comandos ou podem ser encadeados para formar um fluxo de trabalho completo. Os principais desafios que o instituto amplo enfrenta são os seguintes:

- Compreender as causas e os mecanismos biológicos das doenças.
- Identificar intervenções terapêuticas que atuam na causa fundamental de uma doença.
- Entenda a linha de visão de variantes para funcionar na fisiologia humana.
- Crie padrões e políticas "frameworks" para representação de dados do genoma, armazenamento, análise, segurança e assim por diante.
- Padronize e socialize bancos de dados interoperáveis de agregação de genoma (gnomAD).
- Monitoramento, diagnóstico e tratamento baseados em genoma de pacientes com maior precisão.
- Ajude a implementar ferramentas que predizem doenças bem antes que os sintomas apareçam.
- Criar e capacitar uma comunidade de colaboradores multidisciplinares para ajudar a resolver os problemas mais difíceis e mais importantes da biomedicina.

De acordo com o GATK e o instituto amplo, o sequenciamento do genoma deve ser Tratado como um protocolo em um laboratório de patologia; cada tarefa é bem documentada, otimizada, reprodutível e consistente em amostras e experimentos. A seguir está um conjunto de etapas recomendadas pelo Broad Institute. Para obter mais informações, consulte o "Website da GATK".

Configuração FlexPod

A validação da carga de trabalho genômica inclui uma configuração do zero de uma plataforma de infraestrutura FlexPod. A plataforma FlexPod é altamente disponível e pode ser dimensionada de forma independente. Por exemplo, a rede, o storage e a computação podem ser dimensionados de forma independente. Usamos o seguinte guia de design validado pela Cisco como o documento de arquitetura de referência para configurar o ambiente FlexPod: "Data center FlexPod com VMware vSphere 7,0 e NetApp ONTAP 9 .7". Veja os seguintes destaques de configuração da plataforma FlexPod:

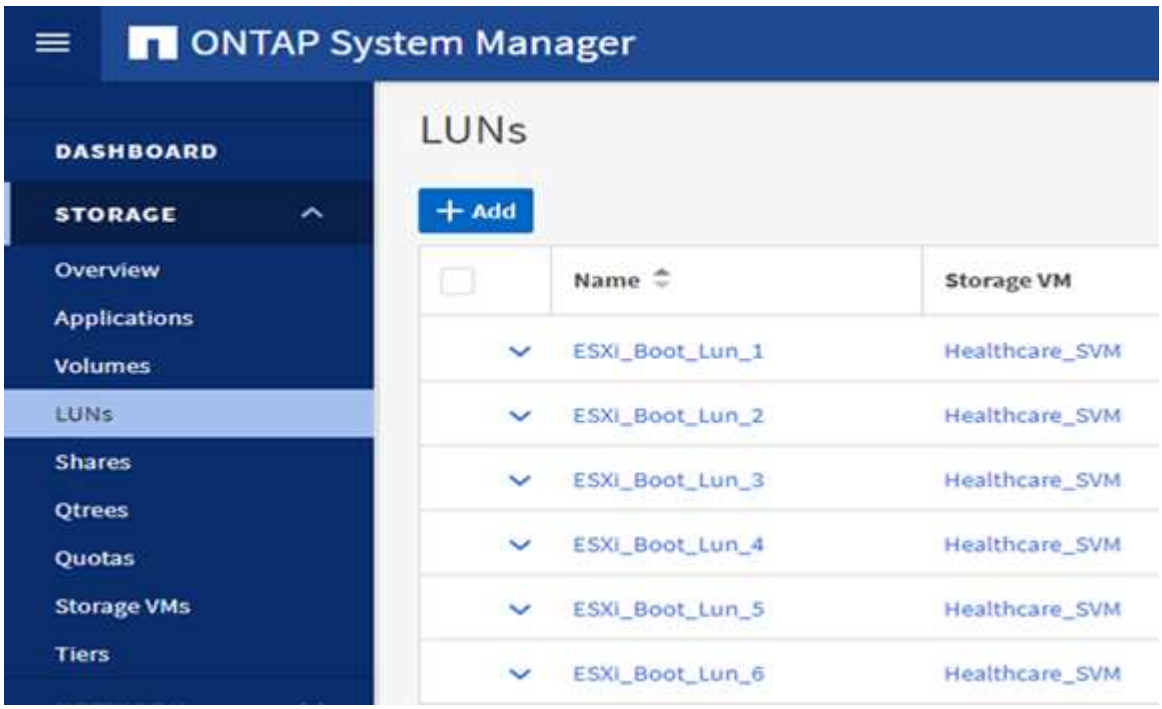
Para executar a configuração do laboratório do FlexPod, execute as seguintes etapas:

1. A configuração e a validação do laboratório FlexPod usam as seguintes reservas e VLANs IP4.1X.

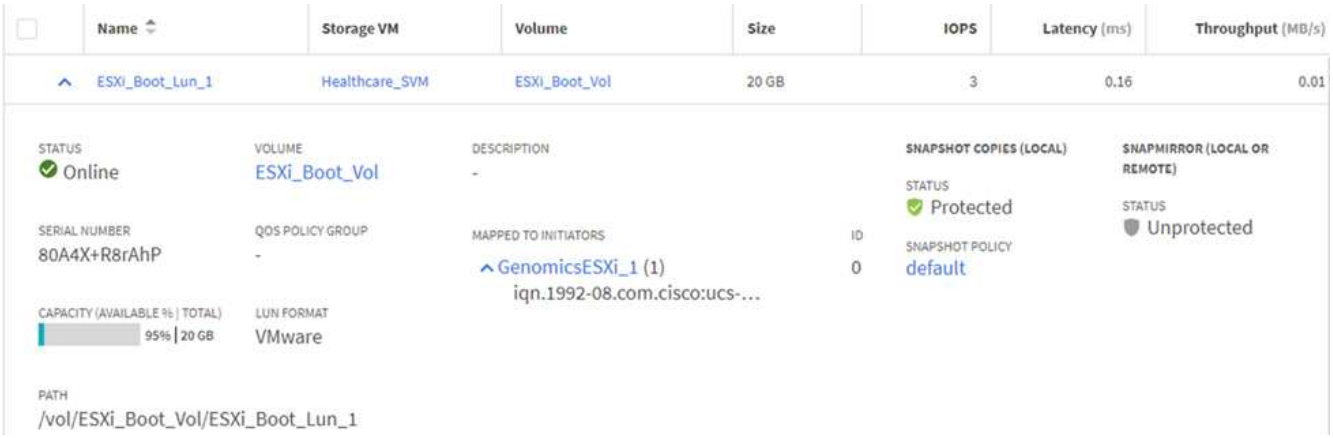
IP Reservations

VLAN	IP Range	Subnet Mask	Purpose
3281	172.21.25 /24	255.255.255.0	IB-MGMT
3282	172.21.26 /24	255.255.255.0	vMotion
3283	172.21.27 /24	255.255.255.0	VM
3284	172.21.28 /24	255.255.255.0	NFS
3285	172.21.29 /24	255.255.255.0	iSCSI-A
3286	172.21.30 /24	255.255.255.0	iSCSI-B

2. Configurar LUNs de inicialização baseados em iSCSI no ONTAP SVM.

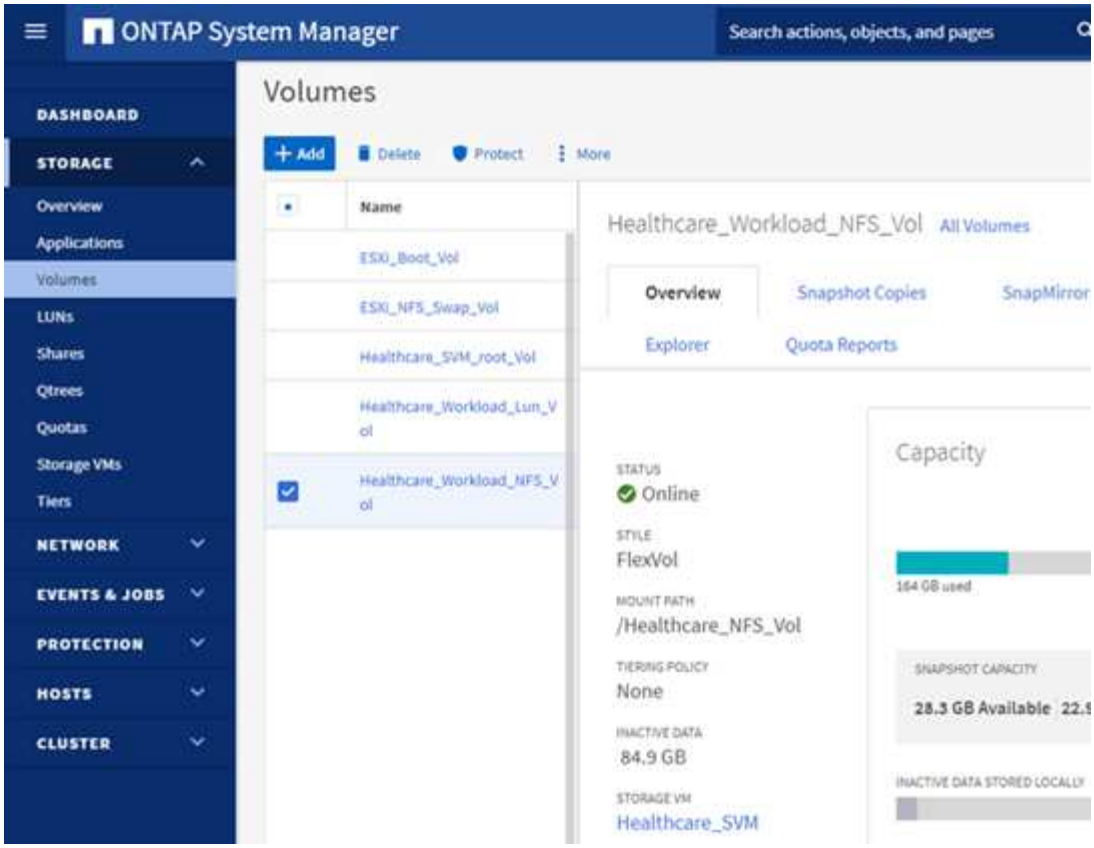


3. Mapear LUNs para grupos de iniciadores iSCSI.

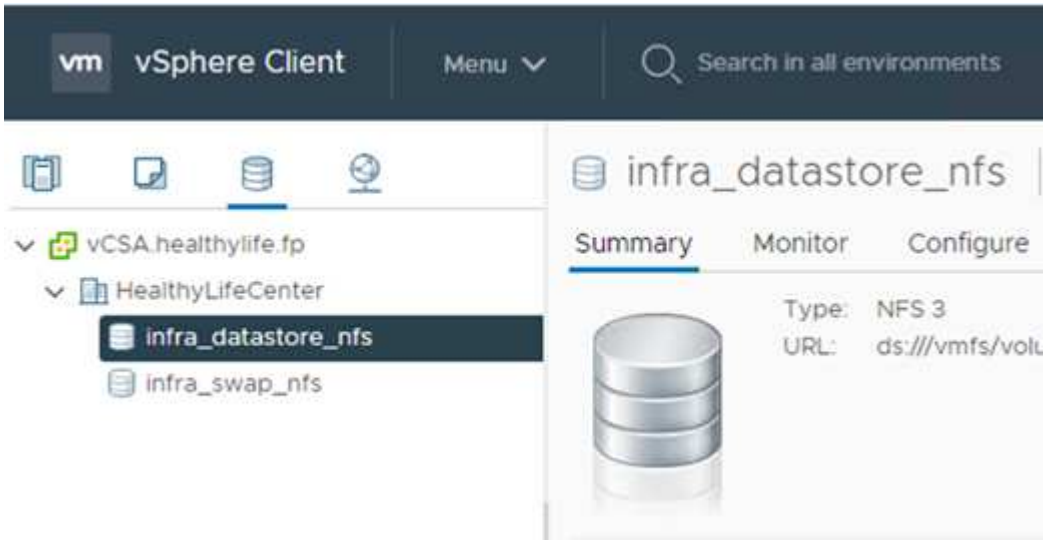


4. Instale o vSphere 7,0 com a inicialização iSCSI.
5. Registre hosts ESXi com o vCenter.

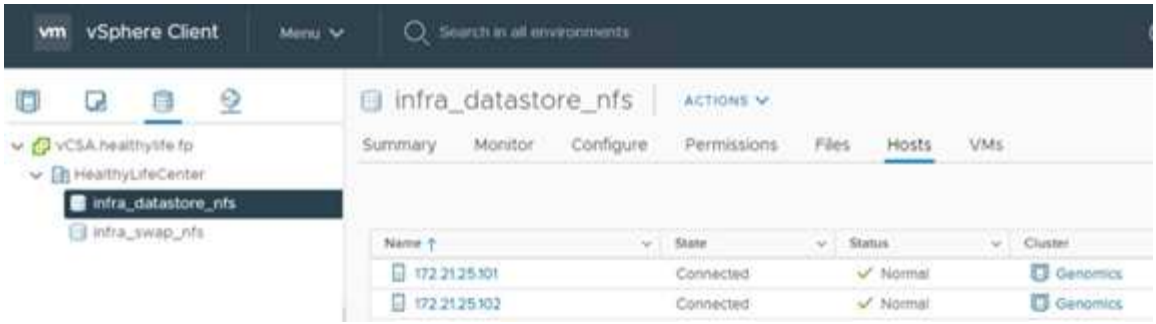
6. Provisionar um armazenamento de dados NFS `infra_datastore_nfs` no storage ONTAP.



7. Adicione o datastore ao vCenter.



8. Usando o vCenter, adicione um datastore NFS aos hosts ESXi.



9. Usando o vCenter, crie uma VM Red Hat Enterprise Linux (RHEL) 8,3 para executar o GATK.
10. Um datastore NFS é apresentado à VM e montado no `/mnt/genomics`, que é usado para armazenar executáveis GATK, scripts, arquivos de mapa de alinhamento binário (BAM), arquivos de referência, arquivos de índice, arquivos de dicionário e arquivos de saída para chamadas variantes.

```
[root@genomics1 genomics]# df | grep genomics
/dev/sdb              308587328  5699492 287142812   2% /mnt/genomics
[root@genomics1 genomics]#
```

Configuração e execução do GATK

Instale os seguintes pré-requisitos na VM Linux do RedHat Enterprise 8,3:

- Java 8 ou SDK 1,8 ou posterior
- Baixe o GATK 4.2.0.0 do Broad Institute "Site do GitHub". Os dados de sequência do genoma são geralmente armazenados na forma de uma série de colunas ASCII delimitadas por tabulações. No entanto, ASCII ocupa muito espaço para armazenar. Portanto, um novo padrão evoluiu chamado um arquivo BAM (**.bam). Um arquivo BAM armazena os dados de sequência em uma forma compactada, indexada e binária. Nós "transferido" um conjunto de arquivos BAM disponíveis publicamente para execução do GATK a partir do "domínio público". Também baixamos arquivos de índice (**.bai), arquivos de dicionário (**. Dict) e arquivos de dados de referência (**. fasta) do mesmo domínio público.

Após o download, o kit de ferramentas GATK tem um arquivo jar e um conjunto de scripts de suporte.

- `gatk-package-4.2.0.0-local.jar` executável
- `gatk` ficheiro de script.

Nós baixamos os arquivos BAM e os arquivos correspondentes de índice, dicionário e genoma de referência para uma família que consistia em arquivos pai, mãe e filho *.bam.

Motor Cromwell

Cromwell é um mecanismo de código aberto voltado para fluxos de trabalho científicos que permite o gerenciamento de fluxos de trabalho. O mecanismo Cromwell pode ser executado em dois "modos" modos , servidor ou em um modo de execução de fluxo de trabalho único. O comportamento do motor Cromwell pode ser controlado com o "Ficheiro de configuração do motor Cromwell".

- **Modo servidor.** Permite "Repousante" a execução de fluxos de trabalho no motor Cromwell.
- **Modo de execução.** O modo de execução é mais adequado para a execução de fluxos de trabalho individuais no Cromwell, "ref" para um conjunto completo de opções disponíveis no modo de execução.

Usamos o motor Cromwell para executar os fluxos de trabalho e pipelines em escala. O motor Cromwell usa uma linguagem de script baseada em WDL (user-friendly "idioma de descrição do fluxo de trabalho"). Cromwell também suporta um segundo padrão de script de fluxo de trabalho chamado linguagem de fluxo de trabalho comum (CWL). Ao longo deste relatório técnico, utilizamos a WDL. O WDL foi originalmente desenvolvido pelo Instituto amplo para pipelines de análise de genoma. O uso dos fluxos de trabalho WDL pode ser implementado usando várias estratégias, incluindo as seguintes:

- * Encadeamento linear.* Como o nome sugere, a saída da tarefa nº 1 é enviada para a tarefa nº 2 como entrada.
- * Multi-in / out. * Isso é semelhante ao encadeamento linear, na medida em que cada tarefa pode ter várias saídas sendo enviadas como entrada para tarefas subsequentes.
- **Scatter-GET.** Essa é uma das estratégias de integração de aplicativos empresariais (EAI) mais poderosas disponíveis, especialmente quando usada em arquitetura orientada a eventos. Cada tarefa é executada de forma dissociada, e a saída para cada tarefa é consolidada na saída final.

Há três etapas quando o WDL é usado para executar o GATK em um modo autônomo:

1. Valide a sintaxe `womtool.jar` usando .

```
[root@genomics1 ~]#  java -jar womtool.jar validate ghplo.wdl
```

2. Gerar entradas JSON.

```
[root@genomics1 ~]#  java -jar womtool.jar inputs ghplo.wdl > ghplo.json
```

3. Execute o fluxo de trabalho usando o mecanismo Cromwell e `Cromwell.jar`.

```
[root@genomics1 ~]#  java -jar cromwell.jar run ghplo.wdl --inputs
ghplo.json
```

O GATK pode ser executado usando vários métodos; este documento explora três desses métodos.

Execução do GATK usando o arquivo jar

Vamos olhar para uma única execução de pipeline de chamada variante usando o chamador da variante haplotype.

```
[root@genomics1 ~]#  java -Dsamjdk.use_async_io_read_samtools=false \
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta
```

Neste método de execução, usamos o arquivo jar de execução local GATK, usamos um único comando java para invocar o arquivo jar, e passamos vários parâmetros para o comando.

1. Este parâmetro indica que estamos invocando o `HaplotypeCaller` pipeline de chamadas variante.
2. `-- input` Especifica o arquivo BAM de entrada.
3. `--output` especifica o arquivo de saída da variante no formato de chamada variante (*.vcf("ref")).
4. Com o `--reference` parâmetro, estamos passando um genoma de referência.

Uma vez executado, os detalhes de saída podem ser encontrados na seção "Saída para execução do GATK usando o arquivo jar."

Execução do GATK usando script ./gatk

O kit de ferramentas GATK pode ser executado usando o `./gatk` script. Vamos examinar o seguinte comando:

```
[root@genomics1 execution]# ./gatk \
--java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
```

Passamos vários parâmetros para o comando.

- Este parâmetro indica que estamos invocando o `HaplotypeCaller` pipeline de chamadas variante.
- `-I` Especifica o arquivo BAM de entrada.
- `-O` especifica o arquivo de saída da variante no formato de chamada variante (*.vcf("ref")).
- Com o `-R` parâmetro, estamos passando um genoma de referência.

Uma vez executado, os detalhes de saída podem ser encontrados na seção

Execução do GATK usando o motor Cromwell

Usamos o motor Cromwell para gerenciar a execução do GATK. Vamos examinar a linha de comando e seus parâmetros.

```
[root@genomics1 genomics]# java -jar cromwell-65.jar \
run /mnt/genomics/GATK/seq/ghplo.wdl  \
--inputs /mnt/genomics/GATK/seq/ghplo.json
```

Aqui, invocamos o comando Java passando o `-jar` parâmetro para indicar que pretendemos executar um arquivo jar, por exemplo, `Cromwell-65.jar`. O próximo parâmetro passado (`run`) indica que o motor Cromwell está em funcionamento no modo Run (Executar), a outra opção possível é o modo Server (servidor). O próximo parâmetro é `*.wdl` que o modo Run deve ser usado para executar os pipelines. O próximo parâmetro é o conjunto de parâmetros de entrada para os fluxos de trabalho que estão sendo executados.

Veja como é o conteúdo do `ghplo.wdl` arquivo:

```
[root@genomics1 seq]# cat ghplo.wdl
workflow helloHaplotypeCaller {
  call haplotypeCaller
}
task haplotypeCaller {
  File GATK
  File RefFasta
  File RefIndex
  File RefDict
  String sampleName
  File inputBAM
  File bamIndex
  command {
    java -jar ${GATK} \
         HaplotypeCaller \
        -R ${RefFasta} \
        -I ${inputBAM} \
        -O ${sampleName}.raw.indels.snps.vcf
  }
  output {
    File rawVCF = "${sampleName}.raw.indels.snps.vcf"
  }
}
[root@genomics1 seq]#
```

Aqui está o arquivo JSON correspondente com as entradas para o motor Cromwell.

```
[root@genomics1 seq]# cat ghplo.json
{
"helloHaplotypeCaller.haplotypeCaller.GATK": "/mnt/genomics/GATK/gatk-
4.2.0.0/gatk-package-4.2.0.0-local.jar",
"helloHaplotypeCaller.haplotypeCaller.RefFasta": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta",
"helloHaplotypeCaller.haplotypeCaller.RefIndex": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta.fai",
"helloHaplotypeCaller.haplotypeCaller.RefDict": "/mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.dict",
"helloHaplotypeCaller.haplotypeCaller.sampleName": "fatherbam",
"helloHaplotypeCaller.haplotypeCaller.inputBAM": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bam",
"helloHaplotypeCaller.haplotypeCaller.bamIndex": "/mnt/genomics/GATK/TEST
DATA/bam/workshop_1906_2-germline_bams_father.bai"
}
[root@genomics1 seq]#
```

Por favor, note que Cromwell usa um banco de dados na memória para a execução. Uma vez executado, o log de saída pode ser visto na seção "Saída para execução do GATK usando o motor Cromwell."

Para obter um conjunto abrangente de etapas sobre como executar o GATK, consulte o "Documentação do GATK".

"Próximo: Saída para execução do GATK usando o arquivo jar."

Saída para execução do GATK usando o arquivo jar

"Anterior: Genômica - configuração e execução do GATK."

A execução do GATK usando o arquivo jar produziu a seguinte saída de amostra.

```
[root@genomics1 execution]# java -Dsamjdk.use_async_io_read_samtools=false
\
-Dsamjdk.use_async_io_write_samtools=true \
-Dsamjdk.use_async_io_write_tribble=false \
-Dsamjdk.compression_level=2 \
-jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar \
HaplotypeCaller \
--input /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
--output workshop_1906_2-germline_bams_father.validation.vcf \
--reference /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
22:52:58.430 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
```

```
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 10:52:58 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
22:52:58.541 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
22:52:58.542 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
22:52:58.542 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
22:52:58.542 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v1.8.0_302-b08
22:52:58.542 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021
10:52:58 PM EDT
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller -
------------------------------------------------------------
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
22:52:58.542 INFO  HaplotypeCaller - Picard Version: 2.25.0
22:52:58.542 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
22:52:58.542 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
22:52:58.543 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
22:52:58.543 INFO  HaplotypeCaller - Deflater: IntelDeflater
22:52:58.543 INFO  HaplotypeCaller - Inflater: IntelInflater
22:52:58.543 INFO  HaplotypeCaller - GCS max retries/reopens: 20
22:52:58.543 INFO  HaplotypeCaller - Requester pays: disabled
22:52:58.543 INFO  HaplotypeCaller - Initializing engine
22:52:58.804 INFO  HaplotypeCaller - Done initializing engine
22:52:58.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
22:52:58.820 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
22:52:58.821 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
22:52:58.854 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
```

```
22:52:58.854 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
22:52:58.854 INFO  IntelPairHmm - Available threads: 16
22:52:58.854 INFO  IntelPairHmm - Requested threads: 4
22:52:58.854 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
22:52:58.872 INFO  ProgressMeter - Starting traversal
22:52:58.873 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
22:53:00.733 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
22:53:08.873 INFO  ProgressMeter -          20:17538652              0.2
58900         353400.0
22:53:17.681 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
22:53:17.681 INFO  ProgressMeter -          20:63024652              0.3
210522         671592.9
22:53:17.681 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
22:53:17.687 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.010347438
22:53:17.687 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.259172573
22:53:17.687 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.27 sec
22:53:17.687 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 10:53:17 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.32 minutes.
Runtime.totalMemory()=5561122816
[root@genomics1 execution]#
```

Observe que o arquivo de saída está localizado no local especificado após a execução.

Saída para execução do GATK usando o script ./gatk

"Anterior: Saída para execução do GATK usando o arquivo jar."

A execução do GATK usando o `./gatk` script produziu a seguinte saída de amostra.

```
[root@genomics1 gatk-4.2.0.0]# ./gatk --java-options "-Xmx4G" \
HaplotypeCaller \
-I /mnt/genomics/GATK/TEST\ DATA/bam/workshop_1906_2-
germline_bams_father.bam \
-R /mnt/genomics/GATK/TEST\ DATA/ref/workshop_1906_2-
germline_ref_ref.fasta \
-O /mnt/genomics/GATK/TEST\ DATA/variants.vcf
Using GATK jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar
Running:
    java -Dsamjdk.use_async_io_read_samtools=false
-Dsamjdk.use_async_io_write_samtools=true
-Dsamjdk.use_async_io_write_tribble=false -Dsamjdk.compression_level=2
-Xmx4G -jar /mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-local.jar
HaplotypeCaller -I /mnt/genomics/GATK/TEST DATA/bam/workshop_1906_2-
germline_bams_father.bam -R /mnt/genomics/GATK/TEST
DATA/ref/workshop_1906_2-germline_ref_ref.fasta -O /mnt/genomics/GATK/TEST
DATA/variants.vcf
23:29:45.553 INFO  NativeLibraryLoader - Loading libgkl_compression.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_compression.so
Aug 17, 2021 11:29:45 PM
shaded.cloud_nio.com.google.auth.oauth2.ComputeEngineCredentials
runningOnComputeEngine
INFO: Failed to detect whether we are running on Google Compute Engine.
23:29:45.686 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.686 INFO  HaplotypeCaller - The Genome Analysis Toolkit (GATK)
v4.2.0.0
23:29:45.686 INFO  HaplotypeCaller - For support and documentation go to
https://software.broadinstitute.org/gatk/
23:29:45.687 INFO  HaplotypeCaller - Executing as
root@genomics1.healthylife.fp on Linux v4.18.0-305.3.1.el8_4.x86_64 amd64
23:29:45.687 INFO  HaplotypeCaller - Java runtime: OpenJDK 64-Bit Server
VM v11.0.12+7-LTS
23:29:45.687 INFO  HaplotypeCaller - Start Date/Time: August 17, 2021 at
11:29:45 PM EDT
23:29:45.687 INFO  HaplotypeCaller -
------------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller -
```

```
-----------------------------------------------------------
23:29:45.687 INFO  HaplotypeCaller - HTSJDK Version: 2.24.0
23:29:45.687 INFO  HaplotypeCaller - Picard Version: 2.25.0
23:29:45.687 INFO  HaplotypeCaller - Built for Spark Version: 2.4.5
23:29:45.688 INFO  HaplotypeCaller - HTSJDK Defaults.COMPRESSION_LEVEL : 2
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_READ_FOR_SAMTOOLS : false
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_SAMTOOLS : true
23:29:45.688 INFO  HaplotypeCaller - HTSJDK
Defaults.USE_ASYNC_IO_WRITE_FOR_TRIBBLE : false
23:29:45.688 INFO  HaplotypeCaller - Deflater: IntelDeflater
23:29:45.688 INFO  HaplotypeCaller - Inflater: IntelInflater
23:29:45.688 INFO  HaplotypeCaller - GCS max retries/reopens: 20
23:29:45.688 INFO  HaplotypeCaller - Requester pays: disabled
23:29:45.688 INFO  HaplotypeCaller - Initializing engine
23:29:45.804 INFO  HaplotypeCaller - Done initializing engine
23:29:45.809 INFO  HaplotypeCallerEngine - Disabling physical phasing,
which is supported only for reference-model confidence output
23:29:45.818 INFO  NativeLibraryLoader - Loading libgkl_utils.so from
jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_utils.so
23:29:45.819 INFO  NativeLibraryLoader - Loading libgkl_pairhmm_omp.so
from jar:file:/mnt/genomics/GATK/gatk-4.2.0.0/gatk-package-4.2.0.0-
local.jar!/com/intel/gkl/native/libgkl_pairhmm_omp.so
23:29:45.852 INFO  IntelPairHmm - Using CPU-supported AVX-512 instructions
23:29:45.852 INFO  IntelPairHmm - Flush-to-zero (FTZ) is enabled when
running PairHMM
23:29:45.852 INFO  IntelPairHmm - Available threads: 16
23:29:45.852 INFO  IntelPairHmm - Requested threads: 4
23:29:45.852 INFO  PairHMM - Using the OpenMP multi-threaded AVX-
accelerated native PairHMM implementation
23:29:45.868 INFO  ProgressMeter - Starting traversal
23:29:45.868 INFO  ProgressMeter -        Current Locus  Elapsed Minutes
Regions Processed   Regions/Minute
23:29:47.772 WARN  InbreedingCoeff - InbreedingCoeff will not be
calculated at position 20:9999900 and possibly subsequent; at least 10
samples must have called genotypes
23:29:55.868 INFO  ProgressMeter -          20:18885652              0.2
63390         380340.0
23:30:04.389 INFO  HaplotypeCaller - 405 read(s) filtered by:
MappingQualityReadFilter
0 read(s) filtered by: MappingQualityAvailableReadFilter
0 read(s) filtered by: MappedReadFilter
0 read(s) filtered by: NotSecondaryAlignmentReadFilter
6628 read(s) filtered by: NotDuplicateReadFilter
```

```
0 read(s) filtered by: PassesVendorQualityCheckReadFilter
0 read(s) filtered by: NonZeroReferenceLengthAlignmentReadFilter
0 read(s) filtered by: GoodCigarReadFilter
0 read(s) filtered by: WellformedReadFilter
7033 total reads filtered
23:30:04.389 INFO  ProgressMeter -          20:63024652              0.3
210522         681999.9
23:30:04.389 INFO  ProgressMeter - Traversal complete. Processed 210522
total regions in 0.3 minutes.
23:30:04.395 INFO  VectorLoglessPairHMM - Time spent in setup for JNI call
: 0.012129203000000002
23:30:04.395 INFO  PairHMM - Total compute time in PairHMM
computeLogLikelihoods() : 0.267345217
23:30:04.395 INFO  SmithWatermanAligner - Total compute time in java
Smith-Waterman : 1.23 sec
23:30:04.395 INFO  HaplotypeCaller - Shutting down engine
[August 17, 2021 at 11:30:04 PM EDT]
org.broadinstitute.hellbender.tools.walkers.haplotypecaller.HaplotypeCalle
r done. Elapsed time: 0.31 minutes.
Runtime.totalMemory()=2111832064
[root@genomics1 gatk-4.2.0.0]#
```

Observe que o arquivo de saída está localizado no local especificado após a execução.

"Próximo: Saída para execução do GATK usando o motor Cromwell."

Saída para execução do GATK usando o motor Cromwell

A execução do GATK usando o motor Cromwell produziu a seguinte saída de amostra.

```
[root@genomics1 genomics]# java -jar  cromwell-65.jar run
/mnt/genomics/GATK/seq/ghplo.wdl  --inputs
/mnt/genomics/GATK/seq/ghplo.json
[2021-08-18 17:10:50,78] [info] Running with database db.url =
jdbc:hsqldb:mem:856a1f0d-9a0d-42e5-9199-
5e6c1d0f72dd;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:57,74] [info] Running migration
RenameWorkflowOptionsInMetadata with a read batch size of 100000 and a
write batch size of 100000
[2021-08-18 17:10:57,75] [info] [RenameWorkflowOptionsInMetadata] 100%
[2021-08-18 17:10:57,83] [info] Running with database db.url =
jdbc:hsqldb:mem:6afe0252-2dc9-4e57-8674-
ce63c67aa142;shutdown=false;hsqldb.tx=mvcc
[2021-08-18 17:10:58,17] [info] Slf4jLogger started
[2021-08-18 17:10:58,33] [info] Workflow heartbeat configuration:
{
```

```
  "cromwellId" : "cromid-41b7e30",
  "heartbeatInterval" : "2 minutes",
  "ttl" : "10 minutes",
  "failureShutdownDuration" : "5 minutes",
  "writeBatchSize" : 10000,
  "writeThreshold" : 10000
}
[2021-08-18 17:10:58,38] [info] Metadata summary refreshing every 1
second.
[2021-08-18 17:10:58,38] [info] No metadata archiver defined in config
[2021-08-18 17:10:58,38] [info] No metadata deleter defined in config
[2021-08-18 17:10:58,40] [info] KvWriteActor configured to flush with
batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,40] [info] WriteMetadataActor configured to flush
with batch size 200 and process rate 5 seconds.
[2021-08-18 17:10:58,44] [info] CallCacheWriteActor configured to flush
with batch size 100 and process rate 3 seconds.
[2021-08-18 17:10:58,44] [warn] 'docker.hash-lookup.gcr-api-queries-per-
100-seconds' is being deprecated, use 'docker.hash-lookup.gcr.throttle'
instead (see reference.conf)
[2021-08-18 17:10:58,54] [info] JobExecutionTokenDispenser - Distribution
rate: 50 per 1 seconds.
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Version 65
[2021-08-18 17:10:58,58] [info] SingleWorkflowRunnerActor: Submitting
workflow
[2021-08-18 17:10:58,64] [info] Unspecified type (Unspecified version)
workflow 3e246147-b1a9-41dc-8679-319f81b7701e submitted
[2021-08-18 17:10:58,66] [info] SingleWorkflowRunnerActor: Workflow
submitted 3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,66] [info] 1 new workflows fetched by cromid-41b7e30:
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,67] [info] WorkflowManagerActor: Starting workflow
3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] WorkflowManagerActor: Successfully started
WorkflowActor-3e246147-b1a9-41dc-8679-319f81b7701e
[2021-08-18 17:10:58,68] [info] Retrieved 1 workflows from the
WorkflowStoreActor
[2021-08-18 17:10:58,70] [info] WorkflowStoreHeartbeatWriteActor
configured to flush with batch size 10000 and process rate 2 minutes.
[2021-08-18 17:10:58,76] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Parsing workflow as WDL draft-2
[2021-08-18 17:10:59,34] [info] MaterializeWorkflowDescriptorActor
[3e246147]: Call-to-Backend assignments:
helloHaplotypeCaller.haplotypeCaller -> Local
[2021-08-18 17:11:00,54] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Starting
```

```
helloHaplotypeCaller.haplotypeCaller
[2021-08-18 17:11:01,56] [info] Assigned new job execution tokens to the
following groups: 3e246147: 1
[2021-08-18 17:11:01,70] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: java -jar
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/inputs/-179397211/gatk-package-
4.2.0.0-local.jar \
     HaplotypeCaller \
    -R /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604632695/workshop_1906_2-germline_ref_ref.fasta \
    -I /mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-
b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/inputs/604617202/workshop_1906_2-germline_bams_father.bam
\
    -O fatherbam.raw.indels.snps.vcf
[2021-08-18 17:11:01,72] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: executing: /bin/bash
/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-41dc-
8679-319f81b7701e/call-haplotypeCaller/execution/script
[2021-08-18 17:11:03,49] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: job id: 26867
[2021-08-18 17:11:03,53] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from -
to WaitingForReturnCode
[2021-08-18 17:11:03,54] [info] Not triggering log of token queue status.
Effective log interval = None
[2021-08-18 17:11:23,65] [info] BackgroundConfigAsyncJobExecutionActor
[3e246147helloHaplotypeCaller.haplotypeCaller:NA:1]: Status change from
WaitingForReturnCode to Done
[2021-08-18 17:11:25,04] [info] WorkflowExecutionActor-3e246147-b1a9-41dc-
8679-319f81b7701e [3e246147]: Workflow helloHaplotypeCaller complete.
Final Outputs:
{
  "helloHaplotypeCaller.haplotypeCaller.rawVCF": "/mnt/genomics/cromwell-
executions/helloHaplotypeCaller/3e246147-b1a9-41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
}
[2021-08-18 17:11:28,43] [info] WorkflowManagerActor: Workflow actor for
3e246147-b1a9-41dc-8679-319f81b7701e completed with status 'Succeeded'.
The workflow will be removed from the workflow store.
[2021-08-18 17:11:32,24] [info] SingleWorkflowRunnerActor workflow
finished with status 'Succeeded'.
{
  "outputs": {
```

```
    "helloHaplotypeCaller.haplotypeCaller.rawVCF":
"/mnt/genomics/cromwell-executions/helloHaplotypeCaller/3e246147-b1a9-
41dc-8679-319f81b7701e/call-
haplotypeCaller/execution/fatherbam.raw.indels.snps.vcf"
  },
  "id": "3e246147-b1a9-41dc-8679-319f81b7701e"
}
[2021-08-18 17:11:33,45] [info] Workflow polling stopped
[2021-08-18 17:11:33,46] [info] 0 workflows released by cromid-41b7e30
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowStoreActor - Timeout
= 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down WorkflowLogCopyRouter -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Shutting down JobExecutionTokenDispenser -
Timeout = 5 seconds
[2021-08-18 17:11:33,46] [info] Aborting all running workflows.
[2021-08-18 17:11:33,46] [info] JobExecutionTokenDispenser stopped
[2021-08-18 17:11:33,46] [info] WorkflowStoreActor stopped
[2021-08-18 17:11:33,47] [info] WorkflowLogCopyRouter stopped
[2021-08-18 17:11:33,47] [info] Shutting down WorkflowManagerActor -
Timeout = 3600 seconds
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor: All workflows
finished
[2021-08-18 17:11:33,47] [info] WorkflowManagerActor stopped
[2021-08-18 17:11:33,64] [info] Connection pools shut down
[2021-08-18 17:11:33,64] [info] Shutting down SubWorkflowStoreActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down JobStoreActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down CallCacheWriteActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] SubWorkflowStoreActor stopped
[2021-08-18 17:11:33,64] [info] Shutting down ServiceRegistryActor -
Timeout = 1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down DockerHashActor - Timeout =
1800 seconds
[2021-08-18 17:11:33,64] [info] Shutting down IoProxy - Timeout = 1800
seconds
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor Shutting down: 0
queued messages to process
[2021-08-18 17:11:33,64] [info] JobStoreActor stopped
[2021-08-18 17:11:33,64] [info] CallCacheWriteActor stopped
[2021-08-18 17:11:33,64] [info] KvWriteActor Shutting down: 0 queued
messages to process
[2021-08-18 17:11:33,64] [info] IoProxy stopped
[2021-08-18 17:11:33,64] [info] WriteMetadataActor Shutting down: 0 queued
```

```
messages to process
[2021-08-18 17:11:33,65] [info] ServiceRegistryActor stopped
[2021-08-18 17:11:33,65] [info] DockerHashActor stopped
[2021-08-18 17:11:33,67] [info] Database closed
[2021-08-18 17:11:33,67] [info] Stream materializer shut down
[2021-08-18 17:11:33,67] [info] WDL HTTP import resolver closed
[root@genomics1 genomics]#
```

"Próximo: Configuração da GPU."

Configuração GPU

"Anterior: Saída para execução do GATK usando o motor Cromwell."

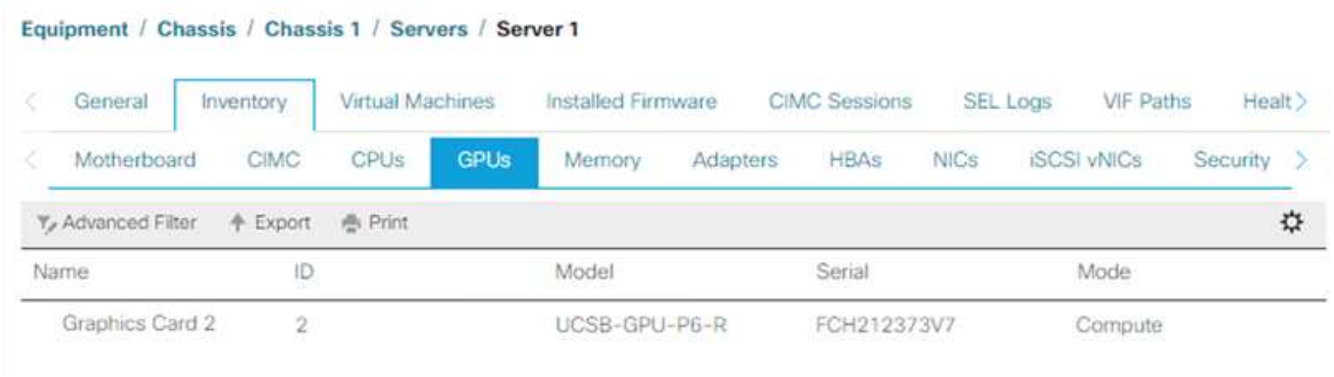
No momento da publicação, a ferramenta GATK não tem suporte nativo para execução baseada em GPU no local. A configuração e orientação a seguir são fornecidas para permitir que os leitores entendam como é simples usar o FlexPod com uma GPU NVIDIA Tesla P6 montada na traseira usando uma placa mezzanine PCIe para GATK.

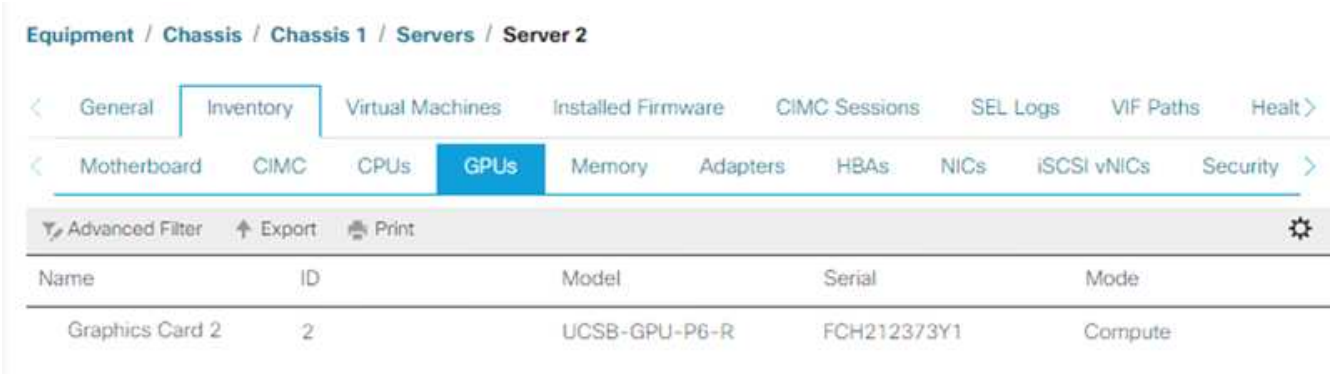
Usamos o Cisco-Validated Design (CVD) a seguir como arquitetura de referência e guia de práticas recomendadas para configurar o ambiente FlexPod para que possamos executar aplicativos que usam GPUs.

- "Data center FlexPod para IA/ML com Cisco UCS 480 ml para aprendizado profundo"

Aqui está um conjunto de pontos-chave durante esta configuração:

1. Usamos uma GPU PCIe NVIDIA Tesla P6 em um slot mezzanine nos servidores UCS B200 M5.





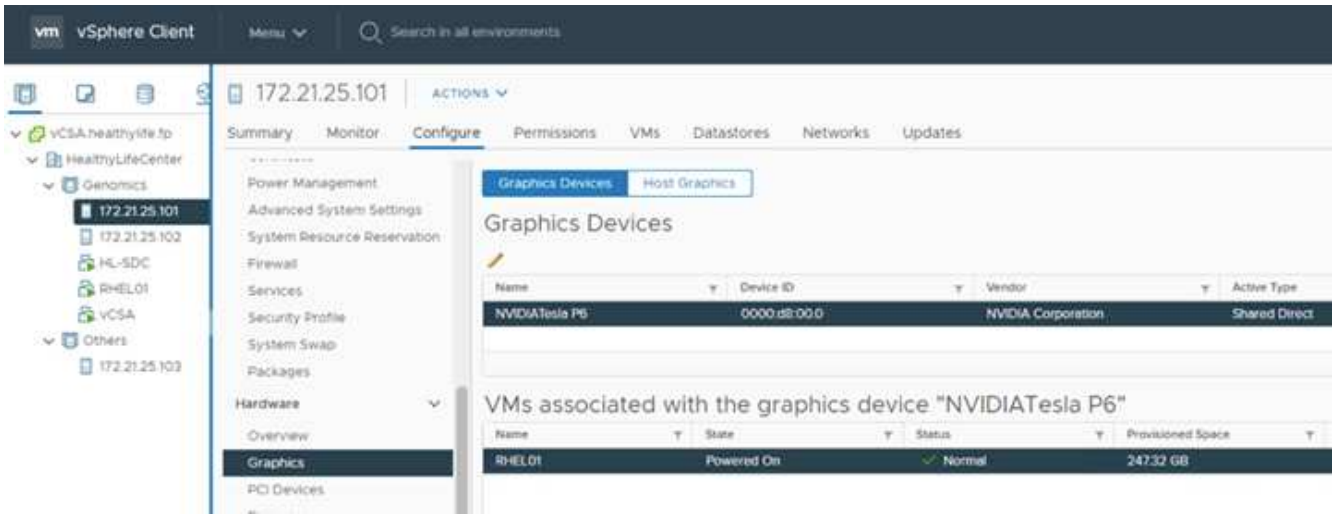
2. Para essa configuração, nos registramos no portal de parceiros da NVIDIA e obtivemos uma licença de avaliação (também conhecida como direito) para poder usar as GPUs no modo de computação.
3. Nós baixamos o software vGPU NVIDIA necessário no site do parceiro NVIDIA.
4. Nós baixamos o arquivo de direitos `*.bin` do site do parceiro NVIDIA.
5. Instalamos um servidor de licença NVIDIA vGPU e adicionamos os direitos ao servidor de licenças usando o `*.bin` arquivo baixado do site do parceiro NVIDIA.
6. Certifique-se de escolher a versão correta do software NVIDIA vGPU para sua implantação no portal de parceiros da NVIDIA. Para esta configuração, usamos o driver versão 460.73.02.
7. Este comando instala o "Gerenciador de vGPU do NVIDIA" no ESXi.

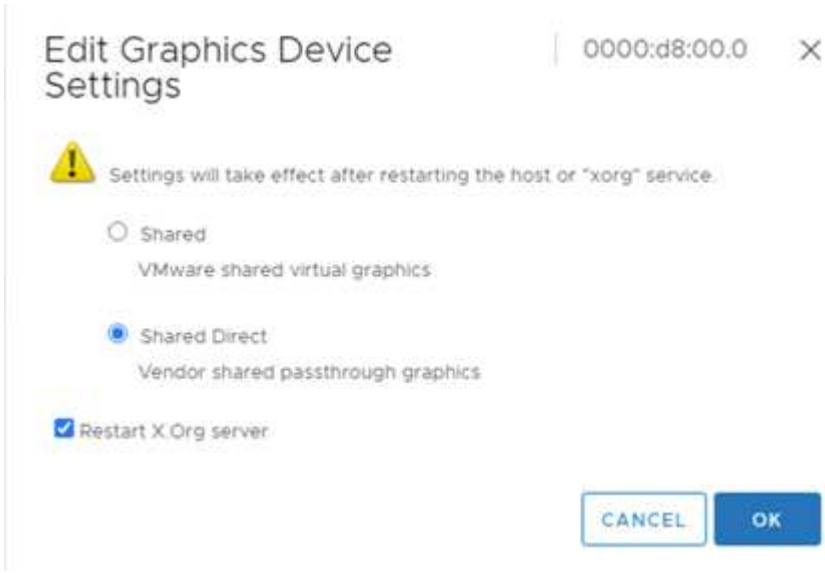
```
[root@localhost:~] esxcli software vib install -v
/vmfs/volumes/infra_datastore_nfs/nvidia/vib/NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: NVIDIA_bootbank_NVIDIA-
VMware_ESXi_7.0_Host_Driver_460.73.02-1OEM.700.0.0.15525992
VIBs Removed:
VIBs Skipped:
```

8. Depois de reiniciar o servidor ESXi, execute o seguinte comando para validar a instalação e verificar a integridade das GPUs.

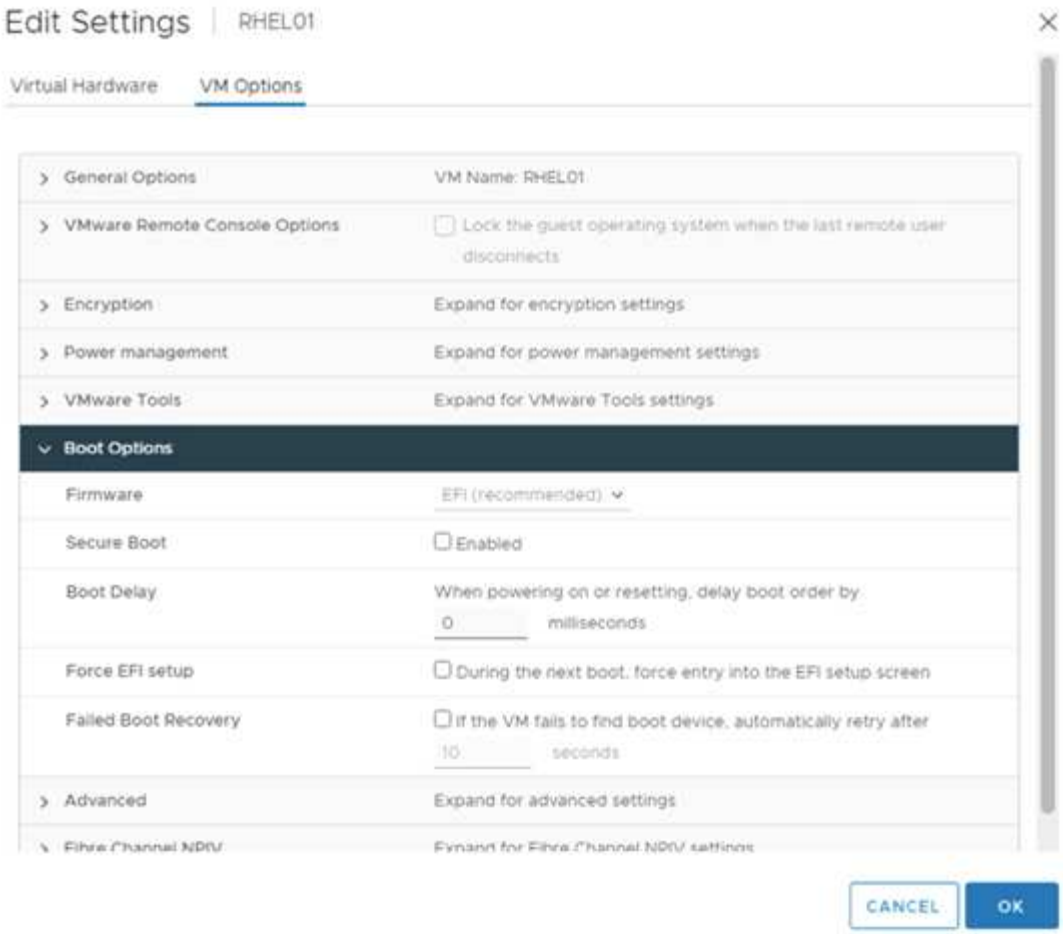
```
[root@localhost:~] nvidia-smi
Wed Aug 18 21:37:19 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.02    Driver Version: 460.73.02    CUDA Version: N/A
|
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  Tesla P6            On   | 00000000:D8:00.0 Off |
0 |
| N/A   35C    P8     9W /  90W |  15208MiB / 15359MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A   2812553    C+G   RHEL01
15168MiB |
+-----------------------------------------------------------------------------
------+
[root@localhost:~]
```

9. Usando o vCenter, "configurar" as configurações do dispositivo gráfico para "Shared Direct".





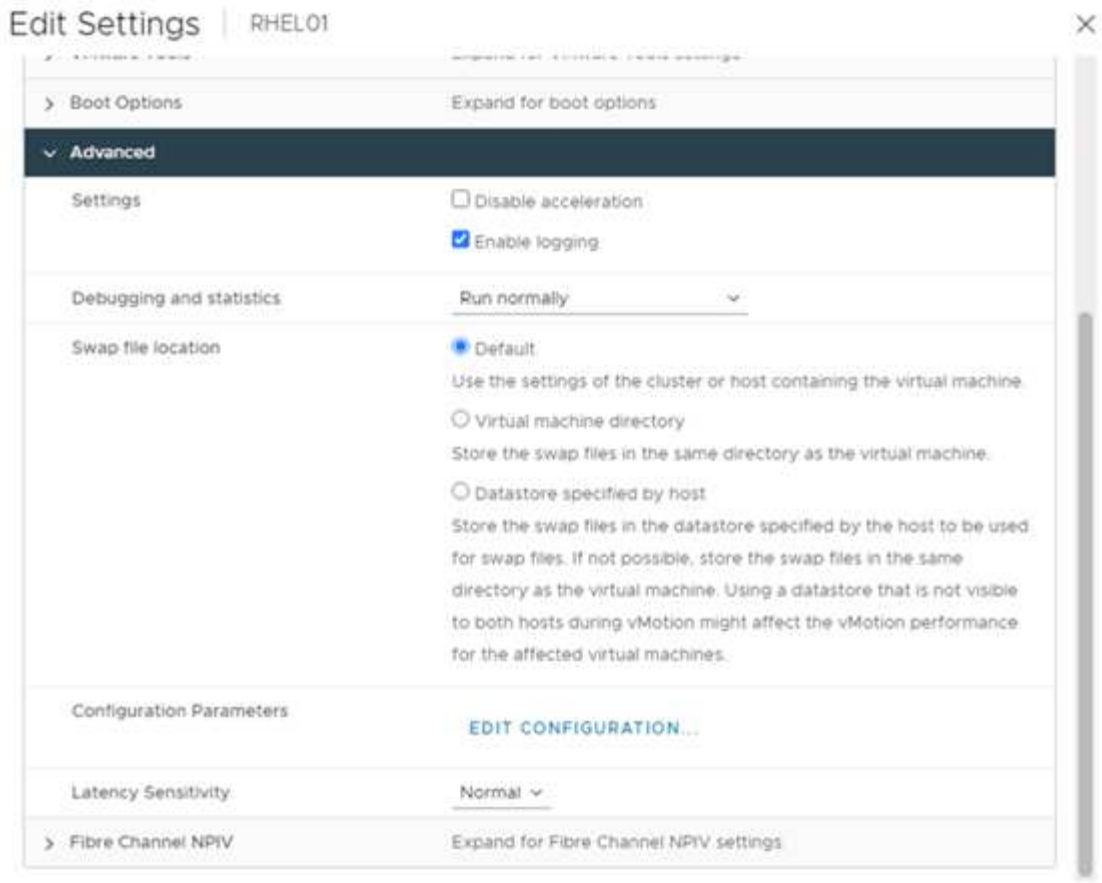
10. Certifique-se de que a inicialização segura esteja desativada para a VM RedHat.
11. Certifique-se de que o firmware das opções de inicialização da VM está definido como EFI ("ref").

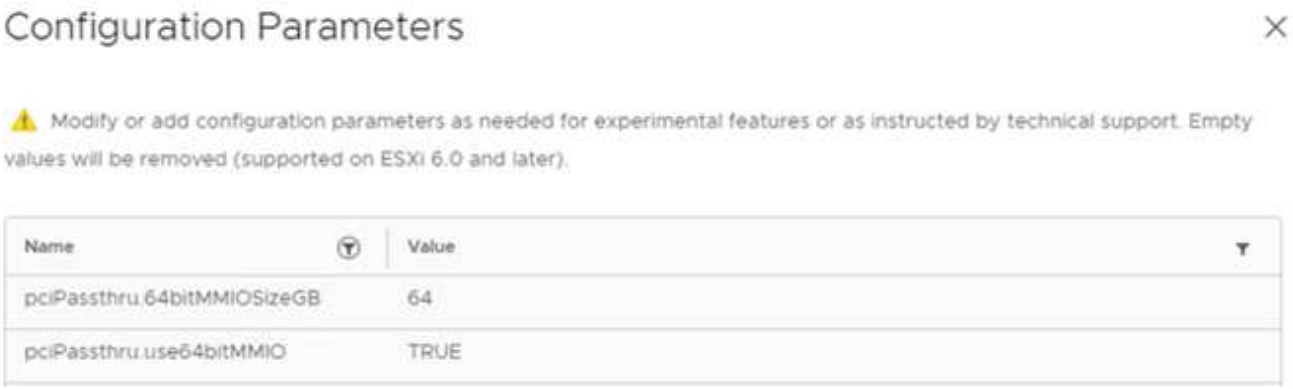


12. Certifique-se de que os PARÂMETROS a seguir sejam adicionados à Configuração de edição avançada de opções da VM. O valor do `pciPassthru.64bitMMIOSizeGB` parâmetro depende da memória da GPU e do número de GPUs atribuídas à VM. Por exemplo:

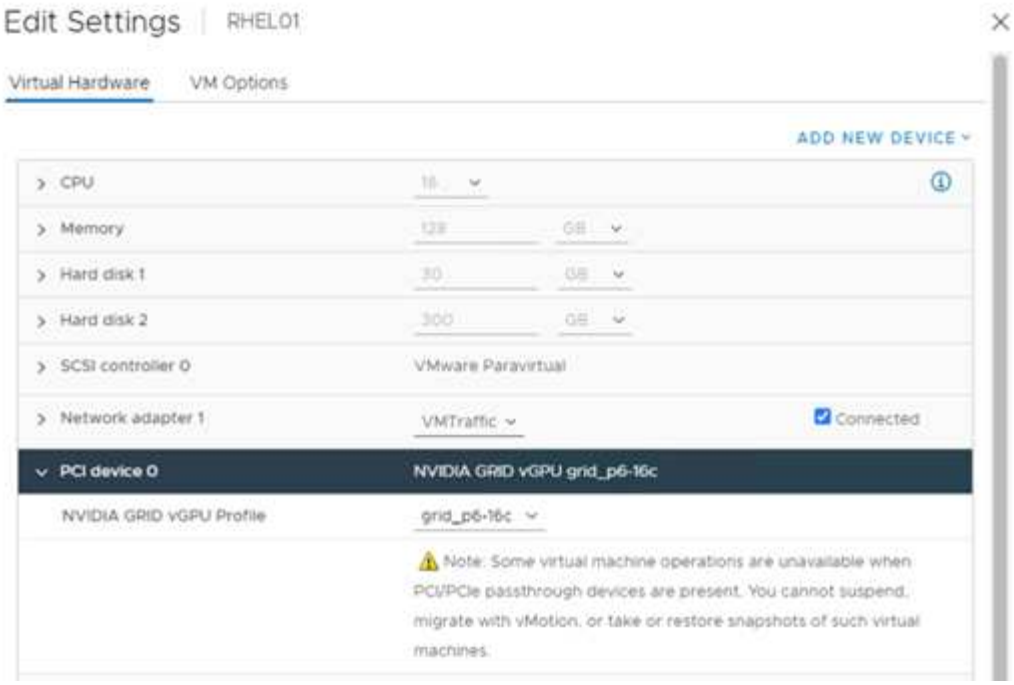
    a. Se uma VM tiver 4 GPUs x 32GB V100, esse valor deverá ser 128.

    b. Se uma VM tiver 4 GPUs x 16GB P6, esse valor deverá ser 64.





13. Ao adicionar vGPUs como um novo dispositivo PCI à máquina virtual no vCenter, certifique-se de selecionar NVIDIA GRID vGPU como o tipo de dispositivo PCI.
14. Escolha o perfil de GPU correto que combina a GPU que está sendo usada, a memória de GPU e o propósito de uso: Por exemplo, gráficos versus computação.



15. Na VM RedHat Linux, os drivers NVIDIA podem ser instalados executando o seguinte comando:

```
[root@genomics1 genomics]#sh NVIDIA-Linux-x86_64-460.73.01-grid.run
```

16. Verifique se o perfil vGPU correto está sendo relatado executando o seguinte comando:

```
[root@genomics1 genomics]# nvidia-smi -query-gpu=gpu_name
-format=csv,noheader -id=0 | sed -e 's/ /-/g'
GRID-P6-16C
[root@genomics1 genomics]#
```

17. Após a reinicialização, verifique se o vGPU NVIDIA correto é relatado juntamente com as versões do driver.

```
[root@genomics1 genomics]# nvidia-smi
Wed Aug 18 20:30:56 2021
+-----------------------------------------------------------------------------
------+
| NVIDIA-SMI 460.73.01    Driver Version: 460.73.01    CUDA Version:
11.2     |
|-------------------------------+----------------------
+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile
Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util
Compute M. |
|                               |                      |
MIG M. |
|===============================+======================+===============
======|
|   0  GRID P6-16C         On   | 00000000:02:02.0 Off |
N/A |
| N/A   N/A    P8    N/A /  N/A |   2205MiB / 16384MiB |      0%
Default |
|                               |                      |
N/A |
+-------------------------------+----------------------
+----------------------+
+-----------------------------------------------------------------------------
------+
| Processes:
|
|  GPU   GI   CI        PID   Type   Process name                  GPU
Memory |
|        ID   ID                                                   Usage
|
|=============================================================================
======|
|    0   N/A  N/A      8604      G   /usr/libexec/Xorg
13MiB |
+-----------------------------------------------------------------------------
------+
[root@genomics1 genomics]#
```

18. Verifique se o IP do servidor de licença está configurado na VM no arquivo de configuração de grade vGPU.
    a. Copie o modelo.

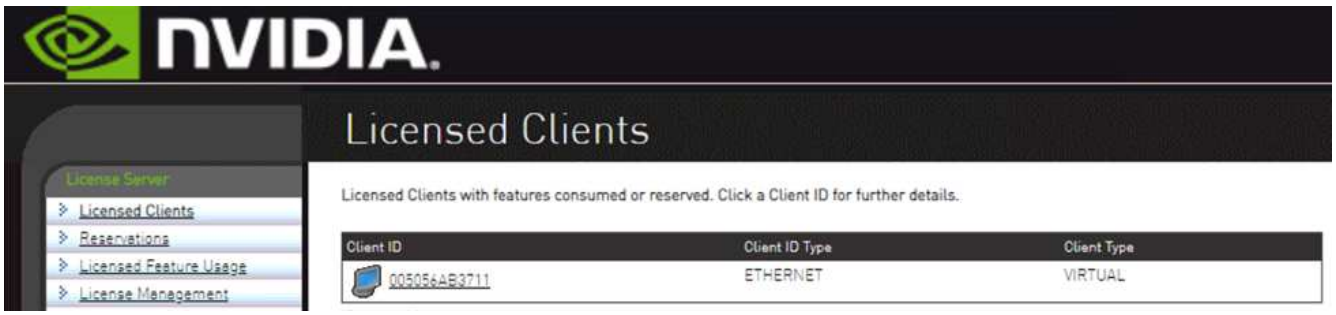
```
[root@genomics1 genomics]# cp /etc/nvidia/gridd.conf.template
/etc/nvidia/gridd.conf
```

b. Edite o `/etc/nvidia/rid.conf` arquivo , adicione o endereço IP do servidor de licença e defina o tipo de recurso como 1.

```
ServerAddress=192.168.169.10
```

```
FeatureType=1
```

19. Depois de reiniciar a VM, você deve ver uma entrada sob Clientes Licenciados no servidor de licenças, conforme mostrado abaixo.



20. Consulte a seção Configuração de soluções para obter mais informações sobre como baixar o software GATK e Cromwell.
21. Depois que o GATK pode usar GPUs no local, a linguagem de descrição do fluxo de trabalho `*. wdl` tem os atributos de tempo de execução, como mostrado abaixo.

```
task ValidateBAM {
  input {
    # Command parameters
    File input_bam
    String output_basename
    String? validation_mode
    String gatk_path
    # Runtime parameters
    String docker
    Int machine_mem_gb = 4
    Int addtional_disk_space_gb = 50
  }
  Int disk_size = ceil(size(input_bam, "GB")) + addtional_disk_space_gb
  String output_name = "${output_basename}_${validation_mode}.txt"
  command {
    ${gatk_path} \
      ValidateSamFile \
      --INPUT ${input_bam} \
      --OUTPUT ${output_name} \
      --MODE ${default="SUMMARY" validation_mode}
  }
  runtime {
    gpuCount: 1
    gpuType: "nvidia-tesla-p6"
    docker: docker
    memory: machine_mem_gb + " GB"
    disks: "local-disk " + disk_size + " HDD"
  }
  output {
    File validation_report = "${output_name}"
  }
}
```

"Próximo: Conclusão."

Conclusão

"Anterior: Configuração da GPU."

Muitas organizações de saúde em todo o mundo padronizaram o FlexPod como uma plataforma comum. Com o FlexPod, você pode implantar funcionalidades do setor de saúde com confiança. O FlexPod com NetApp ONTAP vem de série com a capacidade de implementar um conjunto de protocolos líder do setor pronto para uso. Independentemente da origem da solicitação para executar genômica de um determinado paciente, a interoperabilidade, acessibilidade, disponibilidade e

escalabilidade vêm de série com uma plataforma FlexPod. Quando padronizada em uma plataforma FlexPod, a cultura da inovação se torna contagiosa.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- Data center FlexPod para IA/ML com Cisco UCS 480 ml para aprendizado profundo

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_480ml_aiml_deployment.pdf"

- Data center FlexPod com VMware vSphere 7,0 e NetApp ONTAP 9 .7

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/fp_vmware_vsphere_7_0_ontap_9_7.html"

- Centro de Documentação do ONTAP 9

  "http://docs.netapp.com"

- Ágil e eficiente: Como a FlexPod impulsiona a modernização do data center

  "https://www.flexpod.com/idc-white-paper/"

- Ai na saúde

  "https://www.netapp.com/us/media/na-369.pdf"

- FlexPod para o setor de saúde facilite sua transformação

  "https://flexpod.com/solutions/verticals/healthcare/"

- FlexPod de Cisco e NetApp

  "https://flexpod.com/"

- Inteligência artificial e análise para o setor de saúde (NetApp)

  "https://www.netapp.com/us/artificial-intelligence/healthcare-ai-analytics/index.aspx"

- As opções de infraestrutura inteligente no setor de saúde aumentam o sucesso

  https://www.netapp.com/pdf.html?item=/media/7410-wp-7314.pdf

- Data center FlexPod com ONTAP 9.8, conetor de storage ONTAP para Cisco Intersight e modo gerenciado Cisco Intersight.

  https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf

- Data center FlexPod com a plataforma OpenStack empresarial Red Hat

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_openstack_osp6.html"

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Novembro de 2021	Lançamento inicial.

FlexPod para guia de dimensionamento direcional MEDITECH

TR-4774: FlexPod para dimensionamento direcional MEDITECH

John Duignan, NetApp, Cisco

Em parceria com: 

Este relatório fornece orientações para o dimensionamento de FlexPod para um ambiente de software de aplicação EHR da MEDITECH.

Finalidade

Os sistemas FlexPod podem ser implantados para hospedar serviços de EXPANSÃO MEDITECH, 6.x, 5.x e MAGIC. Os servidores FlexPod que hospedam a camada de aplicação MEDITECH fornecem uma plataforma integrada para uma infraestrutura confiável e de alto desempenho. A plataforma integrada da FlexPod é implantada rapidamente por parceiros de canal qualificados da FlexPod e conta com suporte dos centros de assistência técnica da Cisco e da NetApp.

O dimensionamento baseia-se nas informações contidas na proposta de configuração de hardware da MEDITECH e no documento de tarefa da MEDITECH. O objetivo é determinar o tamanho ideal para componentes de infraestrutura de computação, rede e storage.

"Visão geral do workload DA MEDITECH"A seção descreve os tipos de workloads de computação e storage que podem ser encontrados em ambientes MEDITECH.

A "Especificações técnicas para arquiteturas pequenas, médias e grandes" seção detalha um exemplo de lista de materiais para as diferentes arquiteturas de storage descrito na seção. As configurações fornecidas são apenas diretrizes gerais. Sempre dimensione os sistemas usando os siders com base na carga de trabalho e ajuste as configurações de acordo.

Benefícios gerais da solução

A execução de um ambiente MEDITECH na base arquitetônica da FlexPod pode ajudar as organizações de saúde a melhorar a produtividade e diminuir as despesas operacionais e de capital. O FlexPod fornece uma infraestrutura convergente pré-validada, rigorosamente testada pela parceria estratégica da Cisco com a NetApp. Ele foi projetado e projetado especificamente para fornecer desempenho previsível do sistema de baixa latência e alta disponibilidade. Esta abordagem resulta num tempo de resposta mais rápido para os utilizadores do sistema EHR MEDITECH.

A solução FlexPod da Cisco and NetApp atende aos requisitos do sistema MEDITECH com uma plataforma

de alto desempenho, modular, pré-validado, convergente, virtualizada, eficiente, escalável e econômica. O FlexPod Datacenter com MEDITECH oferece vários benefícios específicos para o setor de saúde:

- * Arquitetura modular*. A FlexPod atende às diversas necessidades da arquitetura modular MEDITECH com sistemas FlexPod personalizados para cada workload específico. Todos os componentes são conectados por meio de uma malha de gerenciamento de storage e servidor em cluster e usam um toolset de gerenciamento coeso.
- **Operações simplificadas e custos reduzidos**. Você pode eliminar as despesas e a complexidade das plataformas legadas substituindo-as por um recurso compartilhado mais eficiente e escalável que pode oferecer suporte aos médicos onde quer que estejam. Essa solução oferece melhor uso de recursos para maior retorno do investimento (ROI).
- * Implantação mais rápida da infraestrutura*. O design integrado do data center FlexPod com MEDITECH permite que os clientes tenham a nova infraestrutura em funcionamento de forma rápida e fácil para data centers no local e remotos.
- * Arquitetura com escalabilidade horizontal*. É possível escalar SAN e nas de terabytes para dezenas de petabytes sem reconfigurar as aplicações em execução.
- **Operações ininterruptas**. É possível realizar manutenção do storage, operações de ciclo de vida do hardware e atualizações de software sem interromper os negócios.
- **Alocação segura a vários clientes**. Esse benefício dá suporte às crescentes necessidades de servidor virtualizado e infraestrutura de storage compartilhado, permitindo a alocação segura a vários clientes de informações específicas das instalações. Esse benefício é importante se você estiver hospedando várias instâncias de bancos de dados e software.
- * Otimização de recursos em pool*. Esse benefício pode ajudar a reduzir contagens físicas de controladores de storage e servidor, equilibrar as demandas de carga de trabalho, aumentar a utilização e, ao mesmo tempo, melhorar o desempenho.
- **Qualidade do serviço (QoS).** O FlexPod oferece qualidade do serviço (QoS) em toda a pilha. Políticas de storage de QoS líderes do setor permitem níveis de serviço diferenciados em um ambiente compartilhado. Essas políticas permitem a performance ideal para workloads e ajudam a isolar e controlar aplicações sem controle.
- **Eficiência de armazenamento**. Você pode reduzir os custos de storage com a eficiência de storage do NetApp 7:1.
- **Agilidade**. As ferramentas de gerenciamento, orquestração e automação do fluxo de trabalho líderes do setor oferecidas pelos sistemas FlexPod permitem QUE A TI seja muito mais responsiva às solicitações de negócios. Essas solicitações de negócios podem variar desde o backup e o provisionamento da MEDITECH de mais ambientes de teste e treinamento a replicações de banco de dados de análise para iniciativas de gerenciamento de saúde da população.
- **Produtividade**. Você pode implantar e escalar rapidamente essa solução para obter as melhores experiências do usuário final do médico.
- **Data Fabric**. A arquitetura do NetApp Data Fabric unifica os dados entre locais, além dos limites físicos e entre as aplicações. O NetApp Data Fabric foi desenvolvido para empresas orientadas pelos dados em um mundo centrado nos dados. Os dados são criados e usados em vários locais, e geralmente são compartilhados com aplicações e infraestruturas. O Data Fabric fornece uma forma de gerenciar dados consistente e integrada. Ele também oferece À TI mais controle dos dados e simplifica a complexidade cada vez maior DA TI.

Âmbito de aplicação

Este documento abrange ambientes que usam o Cisco UCS e o storage baseado no NetApp ONTAP. Ele fornece exemplos de arquiteturas de referência para hospedagem da MEDITECH.

Não cobre:

- Orientação detalhada de dimensionamento usando o modelo de desempenho do sistema (SPM) da NetApp ou outras ferramentas de dimensionamento do NetApp.
- Dimensionamento de workloads que não são de produção.

Público-alvo

Este documento destina-se aos engenheiros de sistemas do NetApp e do parceiro e ao pessoal dos Serviços profissionais da NetApp. O NetApp presume que o leitor tenha um bom entendimento dos conceitos de dimensionamento de computação e storage, bem como familiaridade técnica com os sistemas de storage Cisco UCS e NetApp.

Documentos relacionados

Os seguintes relatórios técnicos e outros documentos são relevantes para este Relatório Técnico e constituem um conjunto completo de documentos necessários para dimensionar, projetar e implantar a MEDITECH na infraestrutura FlexPod.

- "TR-4753: Guia de implantação do FlexPod Datacenter para MEDITECH"
- "TR-4190: Diretrizes de dimensionamento NetApp para ambientes MEDITECH"
- "TR-4319: Diretrizes de implantação da NetApp para ambientes MEDITECH"

As credenciais de login para o Portal de Campo do NetApp são necessárias para acessar alguns desses relatórios.

Visão geral do workload DA MEDITECH

Esta seção descreve os tipos de workloads de computação e storage que você pode encontrar em ambientes MEDITECH.

Workloads MEDITECH e backup

Ao dimensionar os sistemas de storage da NetApp para ambientes MEDITECH, você deve considerar o workload de produção da MEDITECH e o workload de backup.

MEDITECH Host
Um host MEDITECH é um servidor de banco de dados. Este host também é conhecido como um servidor de arquivos MEDITECH (para a plataforma EXPANSE, 6.x ou C/S 5.x) ou uma MÁQUINA MÁGICA (para a PLATAFORMA MÁGICA). Este documento usa o termo host MEDITECH para se referir a um servidor de arquivos MEDITECH e a uma MÁQUINA MÁGICA.

As seções a seguir descrevem as caraterísticas de e/S e os requisitos de desempenho dessas duas cargas de trabalho.

Carga de trabalho DA MEDITECH

Em um ambiente MEDITECH, vários servidores que executam o software MEDITECH executam várias tarefas como um sistema integrado conhecido como o sistema MEDITECH. Para obter mais informações sobre o sistema MEDITECH, consulte a documentação MEDITECH:

- Para ambientes MEDITECH de produção, consulte a documentação MEDITECH apropriada para determinar o número de hosts MEDITECH e a capacidade de armazenamento que deve ser incluída como parte do dimensionamento do sistema de armazenamento NetApp.
- Para novos ambientes MEDITECH, consulte o documento de proposta de configuração de hardware. Para ambientes MEDITECH existentes, consulte o documento de tarefa de avaliação de hardware. A tarefa de avaliação de hardware está associada a um ticket MEDITECH. Os clientes podem solicitar qualquer um destes documentos à MEDITECH.

Você pode escalar o sistema MEDITECH para oferecer maior capacidade e desempenho adicionando hosts. Cada host requer capacidade de armazenamento para seus arquivos de banco de dados e aplicativos. O storage disponível para cada host MEDITECH também deve suportar a e/S gerada pelo host. Em um ambiente MEDITECH, um LUN está disponível para cada host para dar suporte aos requisitos de storage de aplicativos e bancos de dados desse host. O tipo de categoria MEDITECH e o tipo de plataforma que você implantar determinam as caraterísticas da carga de trabalho de cada host MEDITECH e, portanto, do sistema como um todo.

Categoria MEDITECH

A MEDITECH associa o tamanho da implantação com um número de categoria que varia de 1 a 6. A categoria 1 representa as menores implantações MEDITECH; a categoria 6 representa a maior. Exemplos da especificação da aplicação MEDITECH associada a cada categoria incluem métricas como:

- Número de camas hospitalares
- Pacientes internados por ano
- Pacientes ambulatoriais por ano
- Visitas de emergência por ano
- Exames por ano
- Prescrições de internação por dia
- Prescrições ambulatoriais por dia

Para obter mais informações sobre as categorias MEDITECH, consulte a folha de referência da categoria MEDITECH. Pode obter esta folha da MEDITECH através do cliente ou através do instalador do sistema MEDITECH.

Plataformas MEDITECH

MEDITECH tem quatro plataformas:

- EXPANSÃO
- MEDITECH 6.x
- Cliente/servidor 5.x (C/S 5.x)
- MAGIA

Para as plataformas MEDITECH EXPANSE, 6.x e C/S 5.x, as caraterísticas de e/S de cada host são definidas como 100% aleatórias com um tamanho de solicitação de 4.000. Para a plataforma MÁGICA MEDITECH, as caraterísticas de e/S de cada host são definidas como 100% aleatórias com um tamanho de solicitação de 8.000 ou 16.000. De acordo com a MEDITECH, o tamanho da solicitação para uma implantação típica DE PRODUÇÃO MÁGICA é 8.000 ou 16.000.

A proporção de leituras e gravações varia dependendo da plataforma que é implantada. A MEDITECH estima

a mistura média de leitura e escrita e, em seguida, expressa-as como porcentagens. A MEDITECH também estima o valor médio de IOPS contínuo necessário para cada host MEDITECH em uma determinada plataforma MEDITECH. A tabela abaixo resume as caraterísticas de e/S específicas da plataforma fornecidas pela MEDITECH.

Categoria MEDITECH	Plataforma MEDITECH	Média de leitura aleatória %	% Média de escrita aleatória	IOPS contínuo médio por host MEDITECH
1	EXPANSÃO, 6.x	20	80	750
2-6	EXPANSÃO	20	80	750
	6.x	20	80	750
	C/S 5.x	40	60	600
	MAGIA	90	10	400

Em um sistema MEDITECH, o nível médio de IOPS de cada host deve ser igual aos valores de IOPS definidos na tabela acima. Para determinar o dimensionamento correto do armazenamento com base em cada plataforma, os valores de IOPS especificados na tabela acima são usados como parte da metodologia de dimensionamento descrita na "Especificações técnicas para arquiteturas pequenas, médias e grandes" seção.

A MEDITECH requer a latência média de gravação aleatória para ficar abaixo de 1ms para cada host. No entanto, aumentos temporários de latência de gravação até 2ms ms durante tarefas de backup e realocação são considerados aceitáveis. A MEDITECH também requer a latência média de leitura aleatória para permanecer abaixo de 7ms para hosts da categoria 1 e abaixo de 5ms para hosts da categoria 2. Esses requisitos de latência se aplicam a todos os hosts, independentemente da plataforma MEDITECH que está sendo usada.

A tabela abaixo resume as características de e/S que você deve considerar ao dimensionar o storage NetApp para workloads MEDITECH.

Parâmetro	Categoria MEDITECH	EXPANSÃO	MEDITECH 6.x	C/S 5.x	MAGIA
Tamanho da solicitação	1-6	4K	4K	4K	8K ou 16K
Aleatório/sequencial		100% aleatório	100% aleatório	100% aleatório	100% aleatório
IOPS contínuo médio	1	750	750	N/A.	N/A.
	2-6	750	750	600	400
Relação de leitura/gravação	1-6	20% de leitura, 80% de escrita	20% de leitura, 80% de escrita	40% de leitura, 60% de escrita	90% de leitura, 10% de escrita
Latência de gravação		1ms	1ms	1ms	1ms
Latência de gravação de pico temporário	1-6	2ms	2ms	2ms	2ms

Parâmetro	Categoria MEDITECH	EXPANSÃO	MEDITECH 6.x	C/S 5.x	MAGIA
Latência de leitura	1	7ms	7ms	N/A.	N/A.
	2-6	5ms	5ms	5ms	5ms

Os hosts DA MEDITECH nas categorias 3 a 6 têm as mesmas caraterísticas de e/S da categoria 2. Para as categorias MEDITECH 2 a 6, o número de hosts que são implantados em cada categoria difere.

O sistema de storage NetApp deve ser dimensionado para atender aos requisitos de desempenho descritos nas seções anteriores. Além da carga de trabalho de produção da MEDITECH, o sistema de storage da NetApp deve ser capaz de manter esses destinos de performance da MEDITECH durante as operações de backup, conforme descrito na seção a seguir.

Descrição do workload de backup

O software de backup certificado PELA MEDITECH faz backup do LUN usado por cada host MEDITECH em um sistema MEDITECH. Para que os backups estejam em um estado consistente com aplicativos, o software de backup desativa o sistema MEDITECH e suspende solicitações de e/S para o disco. Embora o sistema esteja em estado de inatividade, o software de backup emite um comando para o sistema de storage NetApp para criar uma cópia Snapshot do NetApp dos volumes que contêm os LUNs. O software de backup mais tarde desbloqueia o sistema MEDITECH, o que permite que as solicitações de e/S de produção continuem para o banco de dados. O software cria um volume NetApp FlexClone com base na cópia Snapshot. Esse volume é usado pela fonte de backup enquanto as solicitações de e/S de produção continuam nos volumes pai que hospedam as LUNs.

O workload gerado pelo software de backup provém da leitura sequencial dos LUNs que residem nos volumes do FlexClone. O workload é definido como um workload de leitura sequencial de 100% com um tamanho de solicitação de 64.000. Para a carga de trabalho de produção da MEDITECH, o critério de desempenho é manter as IOPS necessárias e os níveis de latência de leitura/gravação associados. No entanto, para a carga de trabalho de backup, a atenção é transferida para a taxa de transferência de dados geral (Mbps) que é gerada durante a operação de backup. Os backups de LUN DA MEDITECH devem ser concluídos em uma janela de backup de oito horas, mas a NetApp recomenda que o backup de todos os LUNs MEDITECH seja concluído em seis horas ou menos. Com o objetivo de concluir o backup em menos de seis horas, mitiga eventos como um aumento não planejado na carga de trabalho da MEDITECH, operações em segundo plano da NetApp ONTAP ou crescimento de dados ao longo do tempo. Qualquer um desses eventos pode incorrer em tempo extra de backup. Independentemente da quantidade de dados de aplicativos armazenados, o software de backup executa um backup completo em nível de bloco de todo o LUN para cada host MEDITECH.

Calcule a taxa de transferência de leitura sequencial necessária para concluir a cópia de segurança nesta janela em função dos outros fatores envolvidos:

- A duração de cópia de segurança pretendida
- O número de LUNs
- O tamanho de cada LUN a ser feito backup

Por exemplo, em um ambiente MEDITECH de 50 hosts no qual o tamanho LUN de cada host é de 200GB GB, a capacidade total de LUN para fazer backup é de 10TB GB.

Para fazer backup de 10TB TB de dados em oito horas, é necessário o seguinte throughput:

- (10 x 10 6)MB (8 x 3.600)s
- 347,2MBps

No entanto, para considerar eventos não planejados, uma janela de backup conservadora de 5,5 horas é selecionada para fornecer espaço livre além das seis horas recomendadas.

Para fazer backup de 10TB TB de dados em oito horas, é necessário o seguinte throughput:

- (10 x 10 6)MB (5,5 x 3.600)s
- 500MBps

Com uma taxa de transferência de 500MBps Gbps, o backup pode ser concluído dentro de um período de 5,5 horas, confortavelmente dentro do requisito de backup de 8 horas.

A tabela abaixo resume as características de e/S do workload de backup a ser usado quando você dimensiona o sistema de storage.

Parâmetro	Todas as plataformas
Tamanho da solicitação	64K
Aleatório/sequencial	100% sequencial
Relação de leitura/gravação	100% de leitura
Taxa de transferência média	Depende do número de hosts MEDITECH e do tamanho de cada LUN: O backup deve ser concluído dentro de 8 horas.
Duração da cópia de segurança necessária	8 horas

Arquitetura de referência Cisco UCS para MEDITECH

A arquitetura da MEDITECH na FlexPod baseia-se nas orientações da MEDITECH, da Cisco e da NetApp e na experiência do parceiro em trabalhar com clientes da MEDITECH de todos os tamanhos. A arquitetura é adaptável e aplica as melhores práticas para a MEDITECH, dependendo da estratégia do data center do cliente: Seja pequeno ou grande, centralizado, distribuído ou multitenant.

Ao implantar a MEDITECH, a Cisco projetou arquiteturas de referência Cisco UCS que se alinham diretamente às práticas recomendadas da MEDITECH. O Cisco UCS oferece uma solução totalmente integrada para alto desempenho, alta disponibilidade, confiabilidade e escalabilidade para suportar práticas médicas e sistemas hospitalares com milhares de leitos.

Especificações técnicas para arquiteturas pequenas, médias e grandes

Esta seção discute uma lista de materiais de amostra para arquiteturas de armazenamento de diferentes tamanhos.

Lista de material para arquiteturas pequenas, médias e grandes.

O design do FlexPod é uma infraestrutura flexível que abrange muitos componentes e versões de software diferentes. "TR-4036: Especificações técnicas da FlexPod"Use como guia para montar uma configuração válida do FlexPod. As configurações na tabela abaixo são os requisitos mínimos para o FlexPod e são apenas uma amostra. A configuração pode ser expandida para cada família de produtos conforme necessário para diferentes ambientes e casos de uso.

Para este exercício de dimensionamento pequeno corresponde a um ambiente MEDITECH Categoria 3, médio a categoria 5 e grande a categoria 6.

	Pequeno	Média	Grande
Plataforma	Um par de HA de sistema de storage all-flash NetApp AFF A220	Um par de HA da NetApp AFF A220	Um par de HA de sistema de storage all-flash NetApp AFF A300
Compartimentos de disco	9TB x 3,8TB	13TB x 3,8TB	19TB x 3,8TB
Tamanho do banco de dados MEDITECH	3TB-12TB	17 TB	>30TB
IOPS DA MEDITECH	Menos de 22.000 IOPs	>25.000 IOPs	>32.000 IOPs
Total de IOPS	22000	27000	35000
Bruto	34,2 TB	49,4 TB	68,4 TB
Capacidade utilizável	18.53TiB	27.96TiB	33.82TiB
Capacidade efetiva (eficiência de storage de 2:1 TB)	55.6TiB	83.89TiB	101.47TiB

Alguns ambientes de clientes podem ter vários workloads de produção da MEDITECH executados simultaneamente ou podem ter requisitos de IOPS mais altos. Nesses casos, trabalhe com a equipe de conta do NetApp para dimensionar os sistemas de storage de acordo com as IOPS e a capacidade necessárias. Você deve ser capaz de determinar a plataforma certa para atender aos workloads. Por exemplo, há clientes executando com sucesso vários ambientes MEDITECH em um par de HA de sistema de storage all-flash NetApp AFF A700.

A tabela a seguir mostra o software padrão necessário para as configurações MEDITECH.

Software	Família de produtos	Versão ou lançamento	Detalhes
Armazenamento	ONTAP	ONTAP 9.4 disponibilidade geral (GA)	
Rede	O Cisco UCS Fabric interconecta-se	Cisco UCSM 4.x	Versão recomendada atual
	Switches Ethernet Cisco Nexus	7,0 (3)I7 (6)	Versão recomendada atual
	Cisco FC: Cisco MDS 9132T	8,3 mm (2 mm)	Versão recomendada atual
Hipervisor	Hipervisor	VMware vSphere ESXi 6,7	
	Máquinas virtuais (VMs)	Windows 2016	

Software	Família de produtos	Versão ou lançamento	Detalhes
Gerenciamento	Sistema de gerenciamento de hipervisor	VMware vCenter Server 6,7 U1 (VCSA)	
	Console de storage virtual (VSC) do NetApp	VSC 7.0P1	
	NetApp SnapCenter	SnapCenter 4,0	
	Gerente do Cisco UCS	4.x	

A tabela a seguir mostra um exemplo pequeno (categoria 3) de configuração – componentes de infraestrutura.

Camada	Família de produtos	Quantidade e modelo	Detalhes
Computação	Chassi Cisco UCS 5108	1	Suporta até oito lâminas de meia largura ou quatro de largura total. Adicione chassis à medida que a exigência do servidor aumenta.
	Módulos de e/S do chassis Cisco	2 x 2208	8GB portas de uplink de 10GB mm
	Servidores blade Cisco UCS	4 x B200 M5	Cada um com 2 x 14 núcleos, velocidade de clock de 2,6GHz MHz ou superior e BIOS 3,2 de 384GB GB (nº 3)
	Placas de interface virtual Cisco UCS	4 x UCS 1440	Driver do VMware ESXi fNIC FC: 1.6.0.47 driver Ethernet do VMware ESXi ENIC: 1.0.27.0 (consulte matriz de interoperabilidade https://ucshcltool.cloudapps.cisco.com/public/:)
	2 x interconexões de tecido Cisco UCS (Fi)	2 x UCS 6454 FI	Interconexões de malha de 4tha geração com suporte para Ethernet de 10/25/100GB GbE e FC de 32GB GB
Rede	Switches Ethernet Cisco	2 x Nexus 9336c-FX2	1GB, 10GB, 25GB, 40GB, 100GB
Rede de armazenamento	Rede IP Nexus 9k para armazenamento BLOB		Chassis Fi e UCS
	FC: Cisco MDS 9132T		Dois switches Cisco 9132T

Camada	Família de produtos	Quantidade e modelo	Detalhes
Armazenamento	Sistema de storage all-flash NetApp AFF A300	1 par de HA	Cluster de 2 nós para todas as cargas de trabalho MEDITECH (servidor de arquivos, servidor de imagem, SQL Server, VMware etc.)
	Compartimento de disco de DS224C TB	Compartimento de disco de 1 DS224C TB	
	Unidade de estado sólido (SSD)	9 x 3,8TB	

A tabela a seguir mostra configuração de exemplo de meio (categoria 5) – componentes de infra-estrutura

Camada	Família de produtos	Quantidade e modelo	Detalhes
Computação	Chassi do Cisco UCS 5108	1	Suporta até oito lâminas de meia largura ou quatro de largura total. Adicione chassis à medida que a exigência do servidor aumenta.
	Módulos de e/S de chassi do Cisco	2 x 2208	8GB portas de uplink de 10GB mm
	Servidores blade Cisco UCS	6 x B200 M5	Cada um com 2 x 16 núcleos, velocidade de clock 2,5GHz/ou mais alta e BIOS 3,2 de memória de 384GB GB ou mais (nº 3)
	Placa de interface virtual Cisco UCS (VIC)	6 x UCS 1440 VICS	Driver do VMware ESXi fNIC FC: 1.6.0.47 driver Ethernet do VMware ESXi ENIC: 1.0.27.0 (consulte matriz de interoperabilidade:)
	2 x interconexões de tecido Cisco UCS (Fi)	2 x UCS 6454 FI	Interconexões de malha de 4tha geração com suporte para Ethernet de 10GB/25GB/100GB GbE e FC de 32GB GB
Rede	Switches Ethernet Cisco	2 x Nexus 9336c-FX2	1GB, 10GB, 25GB, 40GB, 100GB
Rede de armazenamento	Rede IP Nexus 9k para armazenamento BLOB		
	FC: Cisco MDS 9132T		Dois switches Cisco 9132T

Camada	Família de produtos	Quantidade e modelo	Detalhes
Armazenamento	Sistema de storage all-flash NetApp AFF A220	2 par de HA	Cluster de 2 nós para todas as cargas de trabalho MEDITECH (servidor de arquivos, servidor de imagem, SQL Server, VMware etc.)
	Compartimento de disco de DS224C TB	1 x compartimento de disco de DS224C TB	
	SSD	13 x 3,8TB	

A tabela a seguir mostra um exemplo de configuração grande (categoria 6) – componentes de infraestrutura.

Camada	Família de produtos	Quantidade e modelo	Detalhes
Computação	Chassi do Cisco UCS 5108	1	
	Módulos de e/S de chassi do Cisco	2 x 2208	8 portas de uplink de 10GB mm
	Servidores blade Cisco UCS	8 x B200 M5	Cada um com 2 x 24 núcleos, BIOS 3,2 de 2,7GHz GHz e 768GB GHz (nº 3)
	Placa de interface virtual Cisco UCS (VIC)	8 x UCS 1440 VICS	VMware ESXi fNIC FC driver: 1.6.0.47 VMware ESXi ENIC Ethernet driver: 1.0.27.0 (ver matriz de interoperabilidade https://ucshcltool.cloudapps.cisco.com/public/:)
	2 x interconexões de tecido Cisco UCS (Fi)	2 x UCS 6454 FI	Interconexões de malha de 4tha geração com suporte para Ethernet de 10GB/25GB/100GB GbE e FC de 32GB GB
Rede	Switches Ethernet Cisco	2 x Nexus 9336c-FX2	2 x Cisco Nexus 9332PQ1, 10GB, 25GB, 40GB, 100GB
Rede de armazenamento	Rede IP N9k para armazenamento BLOB		
	FC: Cisco MDS 9132T		Dois switches Cisco 9132T

Camada	Família de produtos	Quantidade e modelo	Detalhes
Armazenamento	AFF A300	1 par de HA	Cluster de 2 nós para todas as cargas de trabalho MEDITECH (servidor de arquivos, servidor de imagem, SQL Server, VMware etc.)
	Compartimento de disco de DS224C TB	1 x DS224C compartimentos de disco	
	SSD	19 x 3,8TB	

Essas configurações fornecem um ponto de partida para orientação de dimensionamento. Alguns ambientes de clientes podem ter vários workloads de produção MEDITECH e não-meDITECH executados simultaneamente, ou podem ter requisitos de IOP mais altos. Você deve trabalhar com a equipe de conta do NetApp para dimensionar os sistemas de storage com base nas operações de entrada/saída por segundo, workloads e capacidade necessárias para determinar a plataforma certa para atender aos workloads.

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos ou sites:

- Data center FlexPod com FC Cisco Validated Design.

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Diretrizes de implantação da NetApp para ambientes MEDITECH.

  "https://fieldportal.netapp.com/content/248456" (É necessário iniciar sessão no NetApp)

- Diretrizes de dimensionamento da NetApp para ambientes MEDITECH.

  "www.NetApp.com/us/media/tr-4190.pdf"

- Data center FlexPod para implantação de EHR da Epic

  "www.NetApp.com/us/media/tr-4693.pdf"

- Zona de Design de FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- FlexPod DC com storage FC (switches MDS) usando NetApp AFF, vSphere 6.5U1 e Cisco UCS Manager

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_esxi65u1_n9fc.html"

- Cisco Saúde

  https://www.cisco.com/c/en/us/solutions/industries/healthcare.html?dtid=osscdc000283

Agradecimentos

As seguintes pessoas contribuíram para a escrita e criação deste guia.

- Brandon Agee, engenheiro técnico de marketing, NetApp
- John Duignan, arquiteto de soluções - Saúde, NetApp
- Ketan Mota, Gerente de produto, NetApp
- Jon Ebmeier, arquiteto de soluções técnicas, Cisco Systems, Inc
- Mike Brennan, gerente de produto, Cisco Systems, Inc

Guia de implantação do FlexPod Datacenter para MEDITECH

TR-4753: Guia de implantação do FlexPod Datacenter para MEDITECH

NetApp e John Duignan, Mike Brennan e Jon Ebmeier, Cisco

Em parceria com: 

Benefícios gerais da solução

Ao administrar um ambiente MEDITECH na base arquitetônica da FlexPod, sua organização de saúde pode esperar uma melhoria na produtividade da equipe e uma diminuição no capital e nas despesas operacionais. O FlexPod Datacenter para MEDITECH oferece vários benefícios específicos para o setor de saúde, incluindo:

- **Operações simplificadas e custos reduzidos.** Elimine as despesas e a complexidade das plataformas legadas substituindo-as por um recurso compartilhado mais eficiente e escalável que pode oferecer suporte aos médicos onde quer que estejam. Essa solução oferece maior utilização de recursos para maior retorno do investimento (ROI).
- * Implantação mais rápida da infraestrutura.* Seja um data center existente ou um local remoto, com o design integrado e testado do data center FlexPod, você pode ter sua nova infraestrutura funcionando em menos tempo e com menos esforço.
- **Armazenamento certificado.** O software de gerenciamento de dados NetApp ONTAP com MEDITECH oferece a você a confiabilidade superior de um fornecedor de storage testado e certificado. A MEDITECH não certifica outros componentes de infraestrutura.
- * Arquitetura de escalabilidade horizontal.* Dimensione SAN e nas de terabytes (TB) para dezenas de petabytes (PB) sem reconfigurar as aplicações em execução.
- **Operações ininterruptas.** Realizar manutenção do storage, operações de ciclo de vida do hardware e atualizações do FlexPod sem interromper os negócios.
- **Alocação segura a vários clientes.** Dar suporte às necessidades crescentes de infraestrutura compartilhada de storage e servidor virtualizado, permitindo a alocação segura a vários clientes de informações específicas das instalações, especialmente se o sistema hospedar várias instâncias de bancos de dados e software.

- * Otimização de recursos em pool.* Ajude a reduzir a contagem de servidores físicos e controladores de storage, a equilibrar a carga de trabalho e aumentar a utilização, melhorando o desempenho.
- **Qualidade do serviço (QoS).** O FlexPod oferece QoS em toda a pilha. As políticas de rede, computação e storage de QoS líderes do setor permitem níveis de serviço diferenciados em um ambiente compartilhado. Essas políticas permitem a performance ideal para workloads e ajudam a isolar e controlar aplicações sem controle.
- **Eficiência de armazenamento.** Reduza os custos de armazenamento com o "Garantia de eficiência de storage do NetApp 7:1".
- **Agilidade.** Com as ferramentas de gerenciamento, orquestração e automação do fluxo de trabalho líderes do setor que os sistemas FlexPod fornecem, sua EQUIPE DE TI pode responder muito mais às solicitações de negócios. Essas solicitações de negócios podem variar desde o backup e o provisionamento da MEDITECH de mais ambientes de teste e treinamento a replicações de banco de dados de análise para iniciativas de gerenciamento de integridade populacional.
- **Aumento da produtividade.** Implante e dimensione rapidamente essa solução para obter as melhores experiências do usuário final do médico.
- **Data Fabric da NetApp.** A arquitetura do NetApp Data Fabric unifica os dados entre locais, além dos limites físicos e entre as aplicações. O NetApp Data Fabric foi desenvolvido para empresas orientadas pelos dados em um mundo centrado nos dados. Os dados são criados e usados em vários locais, e geralmente você precisa aproveitá-los e compartilhá-los com outros locais, aplicações e infraestruturas. Você precisa de uma maneira consistente e integrada de gerenciar seus dados. O Data Fabric fornece uma forma de gerenciar dados que OS coloca em controle e simplifica a complexidade cada vez maior DA TI.

FlexPod

Nova abordagem de infraestrutura para EHRs MEDITECH

Organizações de profissionais de saúde como a sua permanecem sob pressão para maximizar os benefícios de investimentos substanciais em Registros eletrônicos de saúde (EHRs) MEDITECH líderes do setor. Para aplicações de missão crítica, quando os clientes projetam seus data centers para soluções MEDITECH, eles geralmente identificam os seguintes objetivos para a arquitetura do data center:

- Alta disponibilidade das aplicações MEDITECH
- Alto desempenho
- Facilidade de implementação do MEDITECH no data center
- Agilidade e escalabilidade para permitir o crescimento com novas versões ou aplicações MEDITECH
- Custo-benefício
- Alinhamento com orientação MEDITECH e plataformas-alvo
- Capacidade de gerenciamento, estabilidade e facilidade de suporte
- Proteção de dados, backup, recuperação e continuidade dos negócios robustos

À medida que os usuários da MEDITECH evoluem suas organizações para se tornarem organizações de atendimento responsável e se ajustarem a modelos de reembolso mais apertados e agrupados, o desafio passa a ser fornecer a infraestrutura MEDITECH necessária em um modelo de entrega DE TI mais eficiente e ágil.

Valor da infraestrutura convergente pré-validada

Devido a um requisito abrangente para fornecer desempenho previsível do sistema de baixa latência e alta

disponibilidade, a MEDITECH é prescritiva quanto aos requisitos de hardware de seus clientes.

O FlexPod é uma infraestrutura convergente pré-validada e rigorosamente testada pela parceria estratégica da Cisco e da NetApp. Ele foi projetado e projetado especificamente para fornecer desempenho previsível do sistema de baixa latência e alta disponibilidade. Esta abordagem resulta em conformidade com a MEDITECH e, em última análise, um tempo de resposta ideal para os utilizadores do sistema MEDITECH.

A solução FlexPod da Cisco and NetApp atende aos requisitos do sistema MEDITECH com uma plataforma de alto desempenho, modular, pré-validado, convergente, virtualizada, eficiente, escalável e econômica. Ele fornece:

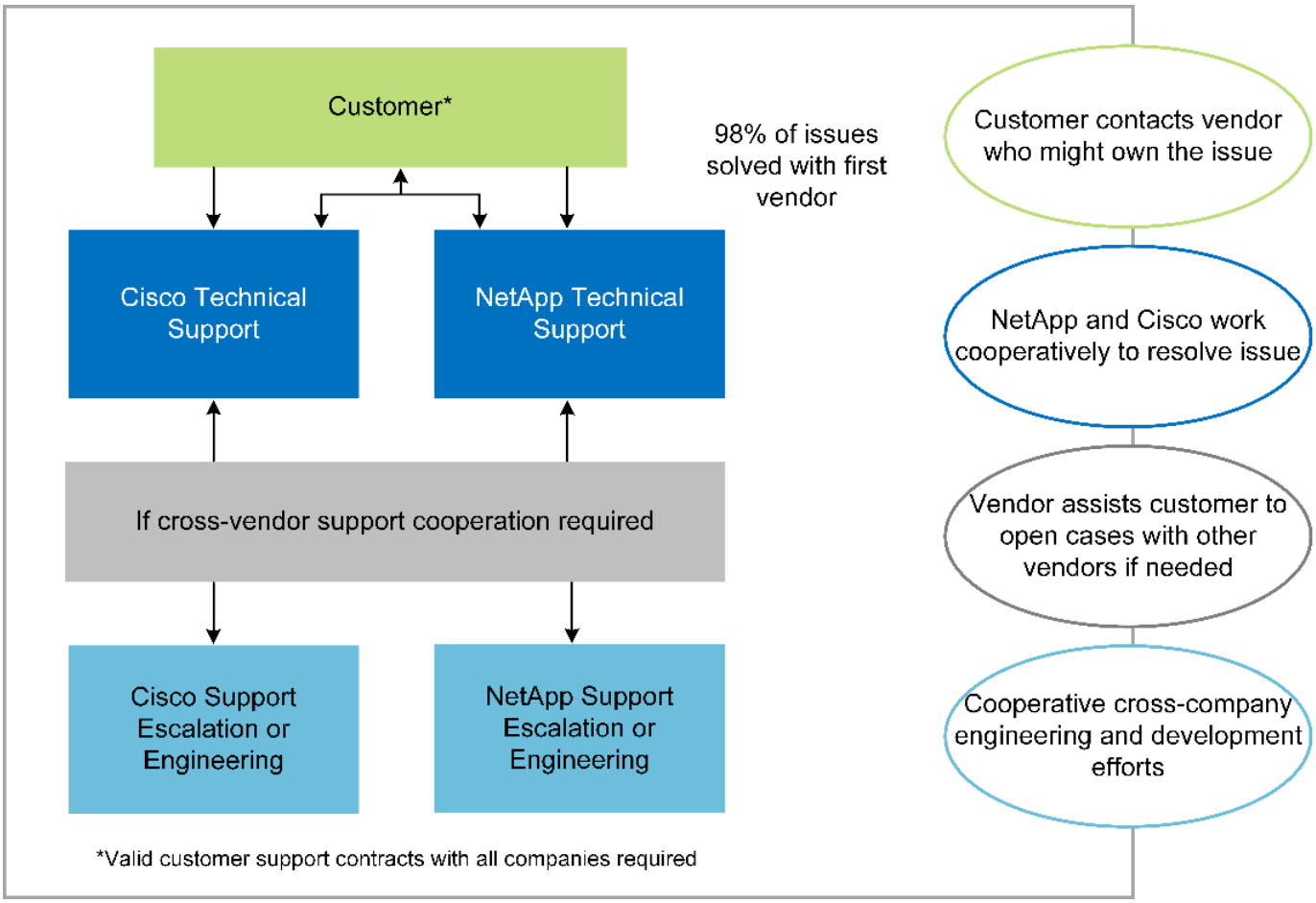
- * Arquitetura modular.* A FlexPod atende às diversas necessidades da arquitetura modular MEDITECH com plataformas FlexPod configuradas sob medida para cada carga de trabalho específica. Todos os componentes são conectados por meio de um servidor em cluster, uma malha de gerenciamento de storage e um toolset de gerenciamento coeso.
- **Tecnologia líder do setor em cada nível da pilha convergente.** Cisco, NetApp, VMware e Microsoft Windows são classificados como número 1 ou número 2 por analistas do setor em suas respetivas categorias de servidores, rede, storage e sistemas operacionais.
- * Proteção de investimento com TI padronizada e flexível.* A arquitetura de referência da FlexPod antecipa novas versões e atualizações de produtos, com rigorosos testes contínuos de interoperabilidade para acomodar tecnologias futuras à medida que elas se tornam disponíveis.
- * Implantação comprovada em uma ampla gama de ambientes.* Pré-testado e validado em conjunto com hipervisores, sistemas operacionais, aplicações e software de infraestrutura populares, o FlexPod foi instalado em várias organizações de clientes da MEDITECH.

Arquitetura FlexPod comprovada e suporte cooperativo

O FlexPod é uma solução de data center comprovada que oferece uma infraestrutura compartilhada flexível que pode ser dimensionada facilmente para atender às crescentes demandas de workloads sem afetar negativamente a performance. Ao aproveitar a arquitetura FlexPod, essa solução oferece todos os benefícios do FlexPod, incluindo:

- **Desempenho para atender aos requisitos de carga de trabalho da MEDITECH.** Dependendo dos requisitos da proposta de configuração de hardware da MEDITECH, diferentes plataformas ONTAP podem ser implantadas para atender aos requisitos de e/S e latência necessários.
- * Escalabilidade para acomodar facilmente o crescimento de dados clínicos.* Escale dinamicamente as máquinas virtuais (VMs), os servidores e a capacidade de storage sob demanda, sem limites tradicionais.
- **Eficiência melhorada.** Reduza o tempo de administração e o TCO com uma infraestrutura virtualizada convergente, que é mais fácil de gerenciar e que armazena dados com mais eficiência, ao mesmo tempo em que gera mais desempenho com o software MEDITECH.
- **Risco reduzido.** Minimizar a interrupção dos negócios com uma plataforma pré-validada que é baseada em uma arquitetura definida que elimina a adivinhação da implantação e acomoda a otimização contínua do workload.
- **Suporte cooperativo do FlexPod.** A NetApp e a Cisco estabeleceram o suporte cooperativo, um modelo de suporte forte, dimensionável e flexível para atender aos requisitos exclusivos de suporte da infraestrutura convergente do FlexPod. Esse modelo usa a experiência, os recursos e a experiência combinada de suporte técnico da NetApp e da Cisco para fornecer um processo simplificado para identificar e resolver seu problema de suporte da FlexPod, independentemente de onde o problema reside. Com o modelo de suporte cooperativo da FlexPod, seu sistema FlexPod opera de forma eficiente e se beneficia da tecnologia mais atualizada, e você trabalha com uma equipe experiente para ajudá-lo a resolver problemas de integração.

O suporte cooperativo do FlexPod é especialmente valioso para organizações de saúde que executam aplicações essenciais aos negócios, como MEDITECH na infraestrutura convergente do FlexPod. A figura a seguir ilustra o modelo de suporte cooperativo do FlexPod.



Além desses benefícios, cada componente da pilha de data center FlexPod com solução MEDITECH oferece benefícios específicos para fluxos de trabalho de EHR da MEDITECH.

Sistema de computação unificada da Cisco

Sistema de computação unificada da Cisco (Cisco UCS), um sistema de autointegração e autoconhecimento, consiste em um único domínio de gerenciamento que está interconetado com uma infraestrutura de e/S unificada. Para que a infraestrutura possa fornecer informações essenciais aos pacientes com disponibilidade máxima, o Cisco UCS para ambientes MEDITECH foi alinhado com as recomendações e as práticas recomendadas da infraestrutura MEDITECH.

A base da MEDITECH na arquitetura Cisco UCS é a tecnologia Cisco UCS, com gerenciamento de sistemas integrados, processadores Intel Xeon e virtualização de servidores. Essas tecnologias integradas resolvem os desafios do data center e ajudam você a atingir suas metas de design de data center para a MEDITECH. O Cisco UCS unifica o gerenciamento de LAN, SAN e sistemas em um link simplificado para servidores de rack, servidores blade e VMs. O Cisco UCS é uma arquitetura de e/S completa que incorpora a malha unificada da Cisco e a tecnologia Cisco Fabric Extender (tecnologia FEX) para conetar todos os componentes do Cisco UCS com uma única malha de rede e uma única camada de rede.

O sistema pode ser implantado como uma única ou várias unidades lógicas que incorporam e dimensionam em vários chassis blade, servidores de rack, racks e data centers. O sistema implementa uma arquitetura radicalmente simplificada que elimina os vários dispositivos redundantes que povoam o chassi do servidor

blade tradicional e os servidores de rack. Em sistemas tradicionais, dispositivos redundantes como adaptadores Ethernet e FC e módulos de gerenciamento de chassi resultam em camadas de complexidade. O Cisco UCS consiste em um par redundante de interconexões de malha (FIs) do Cisco UCS que fornecem um único ponto de gerenciamento e um único ponto de controle para todo o tráfego de e/S.

O Cisco UCS usa perfis de serviço para ajudar a garantir que os servidores virtuais na infraestrutura do Cisco UCS estejam configurados corretamente. Os perfis de serviço são compostos de políticas de rede, storage e computação criadas uma vez por especialistas no assunto em cada disciplina. Os perfis de serviço incluem informações críticas do servidor sobre a identidade do servidor, como endereçamento LAN e SAN, configurações de e/S, versões de firmware, ordem de inicialização, LAN virtual de rede (VLAN), porta física e políticas de QoS. Os perfis de serviço podem ser criados dinamicamente e associados a qualquer servidor físico no sistema em minutos, em vez de horas ou dias. A associação de perfis de serviço com servidores físicos é realizada como uma operação simples e única e permite a migração de identidades entre servidores no ambiente sem exigir alterações físicas na configuração. Ele facilita o rápido provisionamento bare-metal de substituições para servidores aposentados.

O uso de perfis de serviço ajuda a garantir que os servidores sejam configurados de forma consistente em toda a empresa. Quando vários domínios de gerenciamento do Cisco UCS são empregados, o Cisco UCS Central pode usar perfis de serviço globais para sincronizar informações de configuração e política entre domínios. Se a manutenção precisar ser realizada em um domínio, a infraestrutura virtual pode ser migrada para outro domínio. Essa abordagem ajuda a garantir que, mesmo quando um único domínio está off-line, os aplicativos continuam sendo executados com alta disponibilidade.

Para demonstrar que ele atende aos requisitos de configuração do servidor, o Cisco UCS foi extensivamente testado com MEDITECH durante um período de vários anos. O Cisco UCS é uma plataforma de servidor compatível, conforme listado no site de suporte do sistema de recursos de produto MEDITECH.

Rede Cisco

Os switches Cisco Nexus e os diretores multicamadas Cisco MDS fornecem conetividade de classe empresarial e consolidação de SAN. A rede de storage multiprotocolo Cisco reduz o risco dos negócios fornecendo flexibilidade e opções: FC, conexão de fibra (FICON), FC sobre Ethernet (FCoE), SCSI sobre IP (iSCSI) e FC sobre IP (FCIP).

Os switches Cisco Nexus oferecem um dos conjuntos de recursos de rede de data center mais abrangentes em uma única plataforma. Eles oferecem alto desempenho e densidade para núcleos de data center e campus. Eles também oferecem um conjunto completo de recursos para implantações de agregação de data center, de fim de linha e de interconexão de data center em uma plataforma modular altamente resiliente.

O Cisco UCS integra recursos de computação com switches Cisco Nexus e uma malha de e/S unificada que identifica e lida com diferentes tipos de tráfego de rede. Esse tráfego inclui e/S de armazenamento, tráfego de desktop transmitido, gerenciamento e acesso a aplicativos clínicos e empresariais. Você obtém:

- **Escalabilidade de infraestrutura.** Virtualização, energia e refrigeração eficientes, escala de nuvem com automação, alta densidade e alto desempenho, tudo isso dá suporte ao crescimento eficiente do data center.
- **Continuidade operacional.** O design integra hardware, recursos de software NX-os e gerenciamento para dar suporte a ambientes sem inatividade.
- **QoS de rede e computador.** O Cisco oferece classe de serviço (CoS) e QoS orientada por políticas na malha de rede, storage e computação para performance ideal de aplicações essenciais.
- * Flexibilidade de transporte. * Adote novas tecnologias de rede de forma incremental com uma solução econômica.

Juntos, o Cisco UCS com switches Cisco Nexus e diretores multicamadas Cisco MDS oferecem uma solução

ideal de computação, rede e conetividade SAN para a MEDITECH.

NetApp ONTAP

O storage da NetApp que executa o software ONTAP reduz os custos gerais de storage e fornece os tempos de resposta de leitura e gravação de baixa latência e IOPS de que os workloads MEDITECH precisam. O ONTAP dá suporte a configurações de storage all-flash e híbrido para criar uma plataforma de storage ideal que atenda aos requisitos MEDITECH. Os sistemas acelerados por flash da NetApp receberam a validação e a certificação MEDITECH, oferecendo a você, como cliente MEDITECH, a performance e a capacidade de resposta essenciais às operações MEDITECH sensíveis à latência. Ao criar vários domínios de falha em um único cluster, os sistemas NetApp também podem isolar a produção da não produção. Os sistemas NetApp também reduzem problemas de desempenho com um nível mínimo de performance garantido para workloads com QoS ONTAP.

A arquitetura com escalabilidade horizontal do software ONTAP pode se adaptar com flexibilidade a vários workloads de e/S. Para fornecer a taxa de transferência necessária e a baixa latência de que os aplicativos clínicos precisam e, ao mesmo tempo, fornecer uma arquitetura modular com escalabilidade horizontal, as configurações all-flash geralmente são usadas em arquiteturas ONTAP. Os nós de NetApp AFF podem ser combinados no mesmo cluster de escalabilidade horizontal com nós de storage híbrido (HDD e flash) adequados para armazenar grandes conjuntos de dados com taxa de transferência alta. Juntamente com uma solução de backup aprovada pela MEDITECH, você pode clonar, replicar e fazer backup do seu ambiente MEDITECH, desde um armazenamento de unidade de estado sólido (SSD) caro até um armazenamento de HDD mais econômico em outros nós. Essa abordagem atende ou excede as diretrizes da MEDITECH para clonagem baseada em SAN e backup de pools de produção.

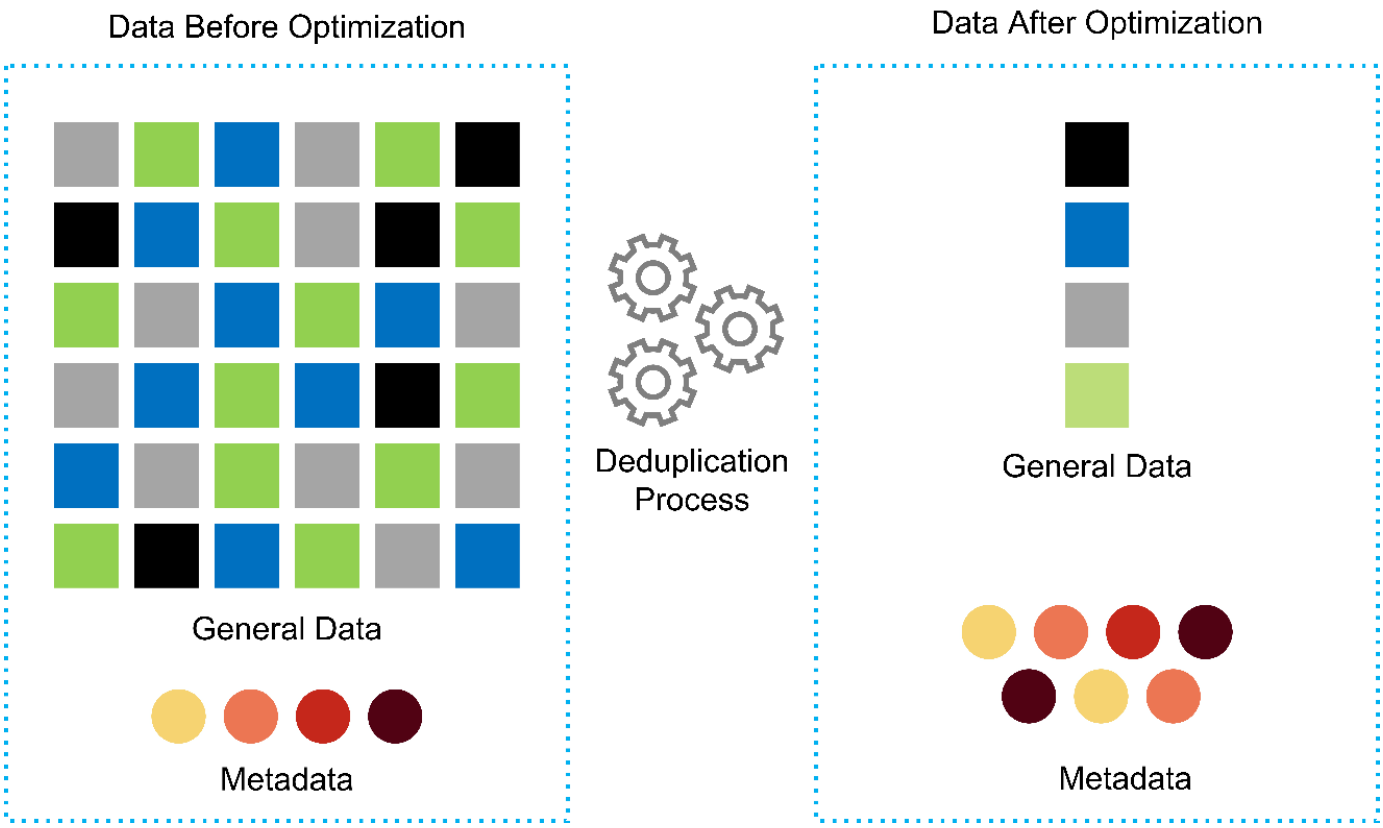
Muitos dos recursos do ONTAP são especialmente úteis em ambientes MEDITECH: Simplificar o gerenciamento, aumentar a disponibilidade e a automação e reduzir a quantidade total de storage necessária. Com esses recursos, você obtém:

- * Desempenho excecional. * A solução NetApp AFF compartilha a arquitetura de storage unificado, o software ONTAP, a interface de gerenciamento, os serviços de rich data e o conjunto avançado de recursos que as outras famílias de produtos NetApp FAS têm. Essa combinação inovadora de Mídia all-flash com o ONTAP oferece a baixa latência consistente e IOPS alto do storage all-flash com a qualidade do software ONTAP líder do setor.
- **Eficiência de armazenamento.** Reduza os requisitos de capacidade total com deduplicação, tecnologia de replicação de dados NetApp FlexClone, compressão e compactação in-line, thin replication, thin Provisioning e deduplicação de agregados.

  A deduplicação do NetApp fornece deduplicação em nível de bloco em um NetApp FlexVol volume ou componente de dados. Essencialmente, a deduplicação remove blocos duplicados, armazenando apenas blocos exclusivos no FlexVol volume ou componente de dados.

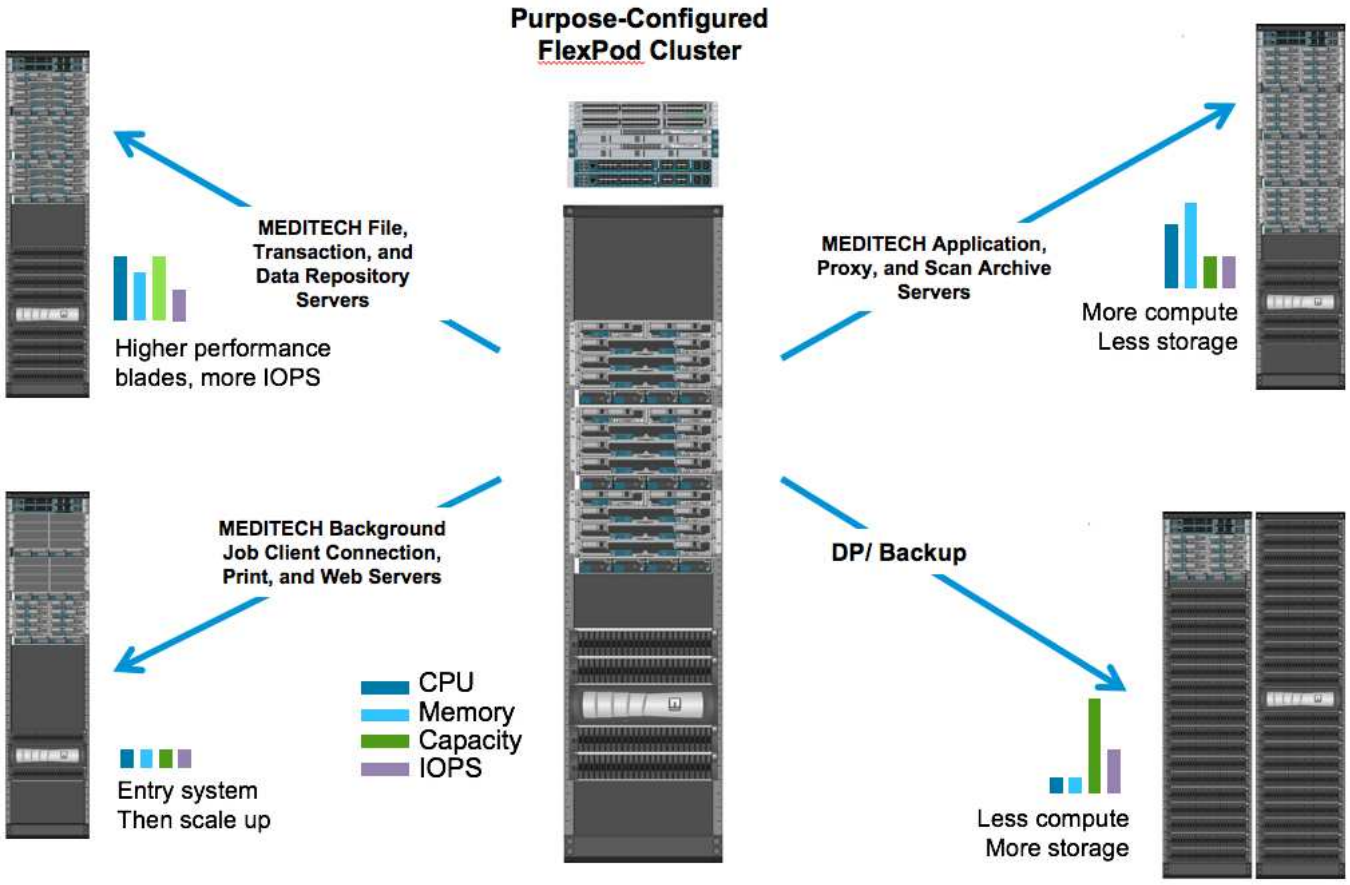
  A deduplicação funciona com um alto grau de granularidade e opera no sistema de arquivos ativo do FlexVol volume ou componente de dados. É transparente de aplicação; portanto, você pode usá-lo para deduplicar dados que se originam de qualquer aplicativo que usa o sistema NetApp. Você pode executar a deduplicação de volume como um processo inline (a partir do ONTAP 8,3.2). Você também pode executá-lo como um processo em segundo plano que pode configurar para ser executado automaticamente, agendado ou executado manualmente por meio da CLI, do Gerenciador de sistemas do NetApp ONTAP ou do NetApp Active IQ Unified Manager.

  A figura a seguir ilustra como a deduplicação do NetApp funciona no nível mais alto.



- **Clonagem eficiente em espaço.** Com a funcionalidade do FlexClone, você cria clones quase instantaneamente para dar suporte à atualização do ambiente de backup e teste. Esses clones consomem mais storage somente quando são feitas alterações.
- **NetApp Snapshot e tecnologias SnapMirror.** O ONTAP pode criar cópias Snapshot com uso eficiente de espaço dos LUNs (números de unidade lógica) que o host MEDITECH usa. Para implantações de dois locais, você pode implementar o software SnapMirror para aumentar a resiliência e a replicação de dados.
- **Proteção de dados integrada.** Os recursos completos de proteção de dados e recuperação de desastres ajudam você a proteger ativos de dados essenciais e fornecer recuperação de desastres.
- **Operações ininterruptas.** Você pode realizar atualizações e manutenção sem colocar os dados offline.
- * QoS e QoS adaptável (AQos).* A QoS de storage permite limitar possíveis workloads de bully. Mais importante, a QoS pode garantir um mínimo de desempenho para workloads essenciais, como a produção MEDITECH. Ao limitar a contenção, a QoS do NetApp pode reduzir problemas relacionados ao desempenho. O AQoS funciona com grupos de políticas predefinidos, que podem ser aplicados diretamente a um volume. Esses grupos de políticas podem dimensionar automaticamente um limite de taxa de transferência ou um tamanho do chão ao volume, mantendo a proporção de IOPS para terabytes e gigabytes à medida que o tamanho do volume muda.
- **Data Fabric da NetApp.** O NetApp Data Fabric simplifica e integra o gerenciamento de dados em ambientes de nuvem e locais para acelerar a transformação digital. Ele fornece serviços de gerenciamento de dados consistentes e integrados, além de aplicações para visibilidade e insights, acesso, controle, proteção e segurança de dados. O NetApp é integrado ao Amazon Web Services (AWS), Azure, Google Cloud Platform e IBM Cloud Clouds, oferecendo uma ampla variedade de opções.

A figura a seguir ilustra a arquitetura da FlexPod para workloads MEDITECH.



Visão geral DA MEDITECH

Medical Information Technology, Inc., comumente conhecida como MEDITECH, é uma empresa de software baseada em Massachusetts que fornece sistemas de informação para organizações de saúde. A MEDITECH fornece um sistema EHR concebido para armazenar e organizar os dados mais recentes do paciente e fornece os dados à equipa clínica. Os dados do paciente incluem, entre outros, dados demográficos; histórico médico; medicação; resultados de testes laboratoriais; imagens de radiologia; e informações pessoais, como idade, altura e peso.

Está além do escopo deste documento cobrir a ampla gama de funções que o software MEDITECH suporta. O Apêndice A fornece mais informações sobre estes amplos conjuntos de funções MEDITECH. As aplicações MEDITECH requerem várias VMs para suportar estas funções. Para implantar esses aplicativos, consulte as recomendações da MEDITECH.

Para cada implantação, do ponto de vista do sistema de storage, todos os sistemas de software MEDITECH exigem um banco de dados distribuído centrado no paciente. A MEDITECH tem seu próprio banco de dados proprietário, que usa o sistema operacional Windows.

Bridgehead e CommVault são as duas aplicações de software de backup certificadas pela NetApp e MEDITECH. O escopo deste documento não abrange a implantação desses aplicativos de backup.

O foco principal deste documento é permitir que a pilha FlexPod (servidores e armazenamento) atenda aos requisitos de desempenho para o banco de dados MEDITECH e os requisitos de backup no ambiente de EHR.

Criado sob medida para cargas de trabalho específicas da MEDITECH

A MEDITECH não revenda hardware, hypervisors ou sistemas operacionais de servidor, rede ou armazenamento; no entanto, tem requisitos específicos para cada componente da pilha de infraestrutura. Portanto, a Cisco e a NetApp trabalharam juntas para testar e permitir que o datacenter FlexPod seja configurado, implantado e suportado com sucesso para atender aos requisitos do ambiente de produção MEDITECH de clientes como você.

Categorias de MEDITECH

A MEDITECH associa o tamanho da implantação a um número de categoria que varia de 1 a 6. A categoria 1 representa as menores implantações MEDITECH e a categoria 6 representa as maiores implantações MEDITECH.

Para obter informações sobre as caraterísticas de e/S e os requisitos de desempenho de um host MEDITECH em cada categoria, consulte NetApp "TR-4190: Diretrizes de dimensionamento NetApp para ambientes MEDITECH" .

Plataforma MEDITECH

A plataforma expanse MEDITECH é a versão mais recente do software EHR da empresa. As plataformas MEDITECH anteriores são Cliente/servidor 5.x e MAGIC. Esta seção descreve a plataforma MEDITECH (aplicável ao Expanse, 6.x, C/S 5.x e MAGIC), referente ao host MEDITECH e seus requisitos de armazenamento.

Para todas as plataformas MEDITECH anteriores, vários servidores executam o software MEDITECH, executando várias tarefas. A figura anterior mostra um sistema MEDITECH típico, incluindo hosts MEDITECH que servem como servidores de banco de dados de aplicativos e outros servidores MEDITECH. Exemplos de outros servidores MEDITECH incluem o aplicativo Repository de dados, o aplicativo Scanning and Archiving e os clientes de trabalho em segundo plano. Para obter a lista completa de outros servidores MEDITECH, consulte os documentos "proposta de configuração de hardware" (para novas implantações) e "tarefa de avaliação de hardware" (para implantações existentes). Você pode obter esses documentos da MEDITECH através do integrador de sistemas MEDITECH ou do seu gerente técnico de contas (TAM) da MEDITECH.

MEDITECH anfitrião

Um host MEDITECH é um servidor de banco de dados. Este host também é conhecido como um servidor de arquivos MEDITECH (para a plataforma expanse, 6.x ou C/S 5.x) ou como uma MÁQUINA MÁGICA (para a PLATAFORMA MÁGICA). Este documento usa o termo host MEDITECH para se referir a um servidor de arquivos MEDITECH ou a uma MÁQUINA MÁGICA.

Os hosts DA MEDITECH podem ser servidores físicos ou VMs que são executados no sistema operacional Microsoft Windows Server. Mais comumente no campo, os hosts MEDITECH são implantados como VMs Windows que são executadas em um servidor VMware ESXi. A partir dessa gravação, o VMware é o único hypervisor que a MEDITECH suporta. Um host MEDITECH armazena seus arquivos de programa, dicionário e dados em uma unidade do Microsoft Windows (por exemplo, unidade e) no sistema Windows.

Em um ambiente virtual, uma unidade do Windows e reside em um LUN que é conetado à VM por meio de um mapeamento de dispositivo bruto (RDM) no modo de compatibilidade física. O uso de arquivos VMDK (Virtual Machine Disk) como uma unidade do Windows e neste cenário não é suportado pela MEDITECH.

Característica de e/S da carga de trabalho do host DA MEDITECH

A caraterística de e/S de cada host MEDITECH e do sistema como um todo depende da plataforma MEDITECH que você implantar. Todas as plataformas MEDITECH (expansão, 6.x, C/S 5.x e Magic) geram

cargas de trabalho 100% aleatórias.

A plataforma expanse MEDITECH gera a carga de trabalho mais exigente, pois possui a maior porcentagem de operações de gravação e IOPS geral por host, seguida de 6.x, C/S 5.x e as plataformas MÁGICAS.

Para obter mais detalhes sobre as descrições da carga de trabalho da MEDITECH, "TR-4190: Diretrizes de dimensionamento NetApp para ambientes MEDITECH" consulte .

Rede de armazenamento

A MEDITECH exige que o protocolo FC seja usado para tráfego de dados entre o sistema NetApp FAS ou AFF e os hosts MEDITECH de todas as categorias.

Apresentação de armazenamento para um host MEDITECH

Cada host MEDITECH usa duas unidades do Windows:

- **Drive C.** esta unidade armazena o sistema operacional Windows Server e os arquivos do aplicativo host MEDITECH.
- **Drive E.** o host MEDITECH armazena seus arquivos de programa, dicionário e dados na unidade e do sistema operacional Windows Server. A unidade e é um LUN que é mapeado a partir do sistema NetApp FAS ou AFF usando o protocolo FC. A MEDITECH exige que o protocolo FC seja usado para que os requisitos de latência de leitura e leitura e gravação do host MEDITECH sejam atendidos.

Convenção de nomenclatura de volume e LUN

A MEDITECH exige que uma convenção de nomenclatura específica seja usada para todos os LUNs.

Antes de qualquer implantação de armazenamento, verifique a proposta de configuração de hardware da MEDITECH para confirmar a convenção de nomenclatura dos LUNs. O processo de backup da MEDITECH depende da convenção de nomes de volume e LUN para identificar adequadamente os LUNs específicos para backup.

Ferramentas de gerenciamento abrangentes e recursos de automação

Cisco UCS com o Cisco UCS Manager

A Cisco se concentra em três elementos-chave para fornecer uma infraestrutura de data center superior: Simplificação, segurança e escalabilidade. O software Cisco UCS Manager, combinado com a modularidade da plataforma, fornece uma plataforma de virtualização de desktop simplificada, segura e escalável:

- **Simplificado.** O Cisco UCS oferece uma abordagem nova e radical à computação padrão do setor e fornece o núcleo da infraestrutura de data center para todos os workloads. O Cisco UCS oferece muitos recursos e benefícios, incluindo redução no número de servidores que você precisa e redução no número de cabos usados por servidor. Outro recurso importante é a capacidade de implantar ou reprovisionar servidores rapidamente por meio de perfis de serviço do Cisco UCS. Com menos servidores e cabos para gerenciar e com o provisionamento simplificado de workload de servidor e aplicações, as operações são simplificadas. As pontuações de servidores blade e rack podem ser provisionadas em minutos com os perfis de serviço do Cisco UCS Manager. Os perfis de serviço Cisco UCS eliminam os runbooks de integração do servidor e eliminam o desvio de configuração. Essa abordagem acelera o tempo de produtividade para os usuários finais, melhora a agilidade nos negócios e permite que os recursos DE TI sejam alocados para outras tarefas.

  O Cisco UCS Manager automatiza muitas operações mundanas de data center sujeitas a erros, como configuração e provisionamento de infraestrutura de acesso a servidor, rede e storage. Além disso, os

servidores blade da série B Cisco UCS e os servidores em rack da série C com grandes pegadas de memória permitem uma alta densidade de usuários de aplicativos, o que ajuda a reduzir os requisitos de infraestrutura de servidor.

A simplificação leva a uma implantação de infraestrutura MEDITECH mais rápida e bem-sucedida.

- **Seguro.** Embora as VMs sejam inerentemente mais seguras do que seus antecessores físicos, elas apresentam novos desafios de segurança. Os servidores de aplicativos e da Web de missão crítica que usam uma infraestrutura comum, como desktops virtuais, estão agora em um risco maior para ameaças à segurança. O tráfego entre VMs agora representa uma importante consideração de segurança que seus gerentes DE TI devem abordar, especialmente em ambientes dinâmicos nos quais as VMs, usando o VMware vMotion, se movem pela infraestrutura do servidor.

  A virtualização, portanto, aumenta significativamente a necessidade de conscientização em nível de VM sobre política e segurança, especialmente dada a natureza dinâmica e fluida da mobilidade de VM em uma infraestrutura de computação estendida. A facilidade com que novos desktops virtuais podem se proliferar amplia a importância de uma infraestrutura de rede e segurança com reconhecimento de virtualização. A infraestrutura de data center do Cisco (soluções da família Cisco UCS, Cisco MDS e Cisco Nexus) para virtualização de desktop fornece segurança forte do data center, da rede e do desktop, com segurança abrangente do desktop ao hypervisor. A segurança é aprimorada com segmentação de desktops virtuais, políticas e administração com reconhecimento de VM e segurança de rede em toda a infraestrutura de LAN e WAN.

- **Escalável.** O crescimento das soluções de virtualização é inevitável, portanto, uma solução precisa ser capaz de escalar e escalar de forma previsível com esse crescimento. As soluções de virtualização Cisco suportam alta densidade de VM (VMs por servidor) e mais servidores são dimensionados com desempenho quase linear. A infraestrutura de data center da Cisco fornece uma plataforma flexível para o crescimento e melhora a agilidade nos negócios. Os perfis de serviço do Cisco UCS Manager permitem o provisionamento de host sob demanda e facilitam a implantação de centenas de hosts como a implantação de dezenas.

  Os servidores UCS Cisco oferecem desempenho e escala quase lineares. O Cisco UCS implementa a tecnologia patenteada de memória estendida Cisco para oferecer grandes pegadas de memória com menos soquetes (com escalabilidade de até 1TB GB de memória com servidores de 2 e 4 soquetes). Usando a tecnologia de malha unificada como um componente básico, a largura de banda agregada do servidor Cisco UCS pode ser dimensionada até 80Gbps Gbps por servidor e a interconexão de malha Cisco UCS pode produzir 2Tbps Gbps na taxa de linha. Esse recurso ajuda a evitar gargalos de e/S e memória de virtualização de desktop. O Cisco UCS, com sua arquitetura de rede baseada em malha unificada de alta performance e baixa latência, dá suporte a altos volumes de tráfego de desktop virtual, incluindo tráfego de comunicações e vídeo de alta resolução. Além disso, o ONTAP ajuda a manter a disponibilidade dos dados e o desempenho ideal durante tempestades de inicialização e login como parte das soluções de virtualização da FlexPod.

  Os designs de infraestrutura de data center Cisco UCS, Cisco MDS e Cisco Nexus fornecem uma excelente plataforma para crescimento. Você obtém o dimensionamento transparente de recursos de servidor, rede e storage para oferecer suporte à virtualização de desktop, aplicativos de data center e computação em nuvem.

VMware vCenter Server

O VMware vCenter Server fornece uma plataforma centralizada para gerenciar ambientes MEDITECH para que sua organização de saúde possa automatizar e fornecer uma infraestrutura virtual com confiança:

- * Implantação simples.* Implante o vCenter Server com rapidez e facilidade usando um dispositivo virtual.

- * Controle centralizado e visibilidade.* Administre toda a infraestrutura do VMware vSphere a partir de um único local.
- **Otimização proativa.** Alocar e otimizar recursos para máxima eficiência.
- **Gestão.** Use poderosos plug-ins e ferramentas para simplificar o gerenciamento e estender o controle.

Console de armazenamento virtual para VMware vSphere

O console de armazenamento virtual (VSC), o provedor de reconhecimento de armazenamento (VASA) do vSphere e o adaptador de replicação de armazenamento VMware (SRA) para VMware vSphere da NetApp compõem um único dispositivo virtual. O pacote de produtos inclui o SRA e o provedor VASA como plug-ins do vCenter Server, que fornece gerenciamento de ciclo de vida completo para VMs em ambientes VMware que usam sistemas de storage NetApp.

O dispositivo virtual para VSC, provedor VASA e SRA se integra perfeitamente ao VMware vSphere Web Client e permite que você use serviços SSO. Em um ambiente com várias instâncias do VMware vCenter Server, cada instância do vCenter Server que você deseja gerenciar deve ter sua própria instância registrada do VSC. A página do painel do VSC permite que você verifique rapidamente o status geral de seus datastores e VMs.

Ao implantar o dispositivo virtual para o VSC, o provedor VASA e o SRA, você pode executar as seguintes tarefas:

- **Use o VSC para implantar e gerenciar o armazenamento e configurar o host ESXi.** Você pode usar o VSC para adicionar credenciais, remover credenciais, atribuir credenciais e configurar permissões para controladores de storage em seu ambiente VMware. Além disso, você pode gerenciar servidores ESXi que estão conetados aos sistemas de armazenamento NetApp. Com alguns cliques, você pode definir os valores de práticas recomendadas recomendados para tempos limite de host, nas e multipathing para todos os hosts. Também pode visualizar os detalhes do armazenamento e recolher informações de diagnóstico.
- **Use o provedor VASA para criar perfis de capacidade de armazenamento e definir alarmes.** O fornecedor VASA para ONTAP é registado no VSC quando ativa a extensão do fornecedor VASA. Você pode criar e usar perfis de capacidade de storage e datastores virtuais. Você também pode definir alarmes para alertá-lo quando os limites para volumes e agregados estiverem quase cheios. Você pode monitorar a performance das VMDKs e das VMs criadas em datastores virtuais.
- **Use o SRA para recuperação de desastres.** Você pode usar o SRA para configurar locais protegidos e de recuperação em seu ambiente para recuperação de desastres durante falhas.

NetApp OnCommand Insight e ONTAP

A NetApp OnCommand Insight integra o gerenciamento da infraestrutura na cadeia de fornecimento de serviços MEDITECH. Com essa abordagem, sua organização de saúde terá mais controle, automação e análise da infraestrutura de storage, rede e computação. ELE pode otimizar sua infraestrutura atual para obter o máximo de benefícios, simplificando o processo de determinação do que e quando comprar. Ele também atenua os riscos associados a migrações complexas de tecnologia. Como não requer agentes, a instalação é direta e sem interrupções. Armazenamento instalado e dispositivos SAN são constantemente descobertos, e informações detalhadas são coletadas para visibilidade total de todo o seu ambiente de storage. Você pode identificar rapidamente ativos mal utilizados, desalinhados, subutilizados ou órfãos e recuperá-los para impulsionar a expansão futura. O OnCommand Insight ajuda você a:

- **Otimize os recursos existentes.** Identifique ativos mal utilizados, subutilizados ou órfãos usando as práticas recomendadas estabelecidas para evitar problemas e atender aos níveis de serviço.
- **Tome melhores decisões.** Os dados em tempo real ajudam a resolver problemas de capacidade com mais rapidez para Planejar com precisão futuras compras, evitar gastos excessivos e adiar as despesas

de capital.

- **Acelere iniciativas DE TI.** Entenda melhor seus ambientes virtuais para ajudá-lo a gerenciar riscos, minimizar o tempo de inatividade e acelerar a implantação da nuvem.

Design

A arquitetura da FlexPod para a MEDITECH baseia-se nas orientações da MEDITECH, Cisco e NetApp e na experiência do parceiro em trabalhar com clientes da MEDITECH de todos os tamanhos. A arquitetura é adaptável e aplica as melhores práticas para a MEDITECH, dependendo da sua estratégia de data center, do tamanho da sua organização e se seu sistema é centralizado, distribuído ou multitenant.

A arquitetura de armazenamento correta pode ser determinada pelo tamanho geral com o total de IOPS. A performance por si só não é o único fator, e você pode decidir usar uma contagem de nós maior com base em requisitos adicionais do cliente. A vantagem de usar o storage NetApp é que você pode escalar o cluster de maneira fácil e sem interrupções, de acordo com suas mudanças de requisitos. Também é possível remover nós do cluster sem interrupções para adaptar o equipamento ou durante atualizações de equipamento.

Aqui estão alguns dos benefícios da arquitetura de storage do NetApp ONTAP:

- **Escalabilidade vertical e horizontal fácil e sem interrupções.** É possível atualizar, adicionar ou remover discos e nós usando operações ininterruptas da ONTAP. Você pode começar com quatro nós e migrar para seis nós ou atualizar para controladoras maiores sem interrupções.
- * Eficiências de armazenamento.* Reduza seus requisitos de capacidade total com deduplicação, NetApp FlexClone, compressão e compactação in-line, thin replication, thin Provisioning e deduplicação de agregados. Com a funcionalidade FlexClone, você cria clones quase instantaneamente para dar suporte a atualizações de ambiente de backup e teste. Esses clones consomem mais storage somente quando são feitas alterações.
- **Servidor de banco de dados sombra de recuperação de desastres.** O servidor de banco de dados de sombra de recuperação de desastres faz parte da estratégia de continuidade de negócios (usado para suportar a funcionalidade somente leitura de armazenamento e potencialmente configurado para ser uma instância de leitura/gravação de armazenamento). Portanto, o posicionamento e o dimensionamento do terceiro sistema de storage geralmente são os mesmos do sistema de storage do banco de dados de produção.
- **Consistência do banco de dados (requer alguma consideração).** Se você usar cópias de backup do NetApp SnapMirror em relação à continuidade dos negócios, "TR-3446: Visão geral e Guia de melhores práticas do SnapMirror Async"consulte .

Layout de storage

Agregados dedicados para hosts MEDITECH

O primeiro passo para atender aos requisitos de alto desempenho e alta disponibilidade da MEDITECH é projetar adequadamente o layout de armazenamento para o ambiente MEDITECH para isolar a carga de trabalho de produção do host MEDITECH em um armazenamento dedicado de alto desempenho.

Um agregado dedicado deve ser provisionado em cada controlador de armazenamento para armazenar o programa, dicionário e arquivos de dados dos hosts MEDITECH. Para eliminar a possibilidade de outros workloads usarem os mesmos discos e afetarem a performance, nenhum outro storage é provisionado a partir desses agregados.

O armazenamento que você fornece para os outros servidores MEDITECH não deve ser colocado no agregado dedicado para os LUNs usados pelos hosts MEDITECH. Você deve colocar o armazenamento para outros servidores MEDITECH em um agregado separado. Os requisitos de armazenamento para outros servidores MEDITECH estão disponíveis nos documentos "proposta de configuração de hardware" (para novas implantações) e "tarefa de avaliação de hardware" (para implantações existentes). Você pode obter esses documentos da MEDITECH através do integrador de sistemas MEDITECH ou do seu gerente técnico de contas (TAM) da MEDITECH. Os engenheiros de soluções da NetApp podem consultar a equipe de fornecedores independentes de software (ISV) da NetApp MEDITECH para facilitar uma configuração de dimensionamento de storage da NetApp adequada e completa.

Distribuir uniformemente a carga de trabalho do host MEDITECH em todos os controladores de storage

Os sistemas NetApp FAS e AFF são implantados como um ou mais pares de alta disponibilidade. A NetApp recomenda que você distribua uniformemente as cargas de trabalho 6.x e expansão MEDITECH em cada controlador de storage para aplicar os recursos de computação, rede e armazenamento em cache em cada controlador de storage.

Use as diretrizes a seguir para distribuir uniformemente as cargas de trabalho da MEDITECH em cada controlador de storage:

- Se você conhece as IOPS de cada host MEDITECH, pode espalhar as cargas de trabalho de expansão MEDITECH e 6.x uniformemente entre todas as controladoras de storage, confirmando que cada controladora atende a um número semelhante de IOPS dos hosts MEDITECH.
- Se você não conhece as IOPS de cada host MEDITECH, ainda poderá distribuir uniformemente as cargas de trabalho de expansão MEDITECH e 6.x em todas as controladoras de storage. Conclua esta tarefa confirmando que a capacidade dos agregados para os hosts MEDITECH é distribuída uniformemente por todas as controladoras de storage. Ao fazer isso, o número de discos é o mesmo em todos os agregados de dados dedicados aos hosts MEDITECH.
- Use tipos de disco semelhantes e grupos RAID idênticos para criar agregados de storage de ambas as controladoras para distribuir os workloads igualmente. Antes de criar o agregado de storage, entre em Contato com um integrador certificado NetApp.

Segundo a MEDITECH, dois hosts no sistema MEDITECH geram IOPS mais altos do que o restante dos hosts. Os LUNs desses dois hosts devem ser colocados em controladores de storage separados. Você deve identificar esses dois hosts com a ajuda da equipe MEDITECH antes de implantar seu sistema.

Posicionamento do storage

Armazenamento de banco de dados para hosts MEDITECH

O armazenamento de banco de dados para um host MEDITECH é apresentado como um dispositivo de bloco (ou seja, um LUN) do sistema NetApp FAS ou AFF. O LUN é normalmente montado no sistema operacional Windows como a unidade E.

Outro armazenamento

O sistema operacional host MEDITECH e o aplicativo de banco de dados normalmente geram uma quantidade considerável de IOPS no storage. O provisionamento de storage das VMs host MEDITECH e seus arquivos VMDK, se necessário, é considerado independente do armazenamento necessário para atender aos limites de desempenho da MEDITECH.

O armazenamento provisionado para os outros servidores MEDITECH não deve ser colocado no agregado dedicado para os LUNs que os hosts MEDITECH usam. Coloque o armazenamento de outros servidores MEDITECH em um agregado separado.

Configuração do controlador de storage

Alta disponibilidade

Para atenuar o efeito de falha de controladora e permitir atualizações sem interrupções do sistema de storage, configure seu sistema de storage com controladores em um par de alta disponibilidade no modo de alta disponibilidade.

Com a configuração de par de controladores de alta disponibilidade, os compartimentos de disco devem ser conectados a controladoras por vários caminhos. Essa conexão aumenta a resiliência do storage ao proteger contra uma falha de caminho único e melhora a consistência do desempenho se ocorrer um failover de controladora.

Desempenho de storage durante failover de controladora de storage

Para sistemas de storage configurados com controladores em um par de alta disponibilidade, no caso improvável de uma falha na controladora, o controlador do parceiro assume os recursos de storage e os workloads da controladora com falha. É importante consultar o cliente para determinar os requisitos de desempenho que devem ser atendidos se houver uma falha no controlador e dimensionar o sistema de acordo com isso.

Takeover assistido por hardware

A NetApp recomenda que você ative o recurso de takeover assistido por hardware em ambos os controladores de storage.

A takeover assistido por hardware foi projetada para minimizar o tempo de failover do controlador de storage. Ele permite que o módulo de LAN remota de um controlador ou o módulo de processador de serviço notifique seu parceiro sobre uma falha de controladora mais rápido do que um gatilho de tempo limite de batimento cardíaco pode, reduzindo o tempo necessário para o failover. O recurso de aquisição assistido por hardware é habilitado por padrão para controladores de storage em uma configuração de alta disponibilidade.

Para obter mais informações sobre a aquisição assistida por hardware, consulte o "Centro de Documentação do ONTAP 9".

Tipo de disco

Para dar suporte ao requisito de baixa latência de leitura dos workloads MEDITECH, a NetApp recomenda que você use um SSD de alta performance para agregados em sistemas AFF dedicados aos hosts MEDITECH.

NetApp AFF

A NetApp oferece arrays AFF de alto desempenho para lidar com workloads MEDITECH que exigem alta taxa de transferência e que têm padrões aleatórios de acesso a dados e requisitos de baixa latência. Para workloads MEDITECH, os arrays AFF oferecem vantagens de desempenho em relação aos sistemas baseados em HDDs. A combinação da tecnologia flash e do gerenciamento de dados empresariais oferece vantagens em três áreas principais: Performance, disponibilidade e eficiência de storage.

Ferramentas e serviços de suporte da NetApp

O NetApp oferece um conjunto completo de ferramentas e serviços de suporte. A ferramenta NetApp AutoSupport deve ser ativada e configurada em sistemas NetApp AFF/FAS para ligar para casa se houver uma falha de hardware ou configuração incorreta do sistema. Ligar para casa alerta a equipe de suporte da NetApp para corrigir quaisquer problemas em tempo hábil. O NetApp Active IQ é uma aplicação baseada na Web baseada em informações do AutoSupport de seus sistemas NetApp que fornece insights preditivos e proativos para ajudar a melhorar a disponibilidade, a eficiência e o desempenho.

Implantação e configuração

Visão geral

O guia de storage do NetApp para implantação do FlexPod fornecido neste documento abrange:

- Ambientes que usam ONTAP
- Ambientes que usam servidores blade Cisco UCS e de montagem em rack

Este documento não abrange:

- Implantação detalhada do ambiente de data center FlexPod

  Para obter mais informações, consulte "Data center FlexPod com FC Cisco Validated Design" (CVD).

- Uma visão geral dos ambientes de software MEDITECH, das arquiteturas de referência e das melhores práticas de integração.

  Para obter mais informações, consulte "TR-4300i: Guia de práticas recomendadas de sistemas de storage all-flash e NetApp FAS para ambientes MEDITECH" (login NetApp necessário).

- Requisitos quantitativos de desempenho e orientação de dimensionamento.

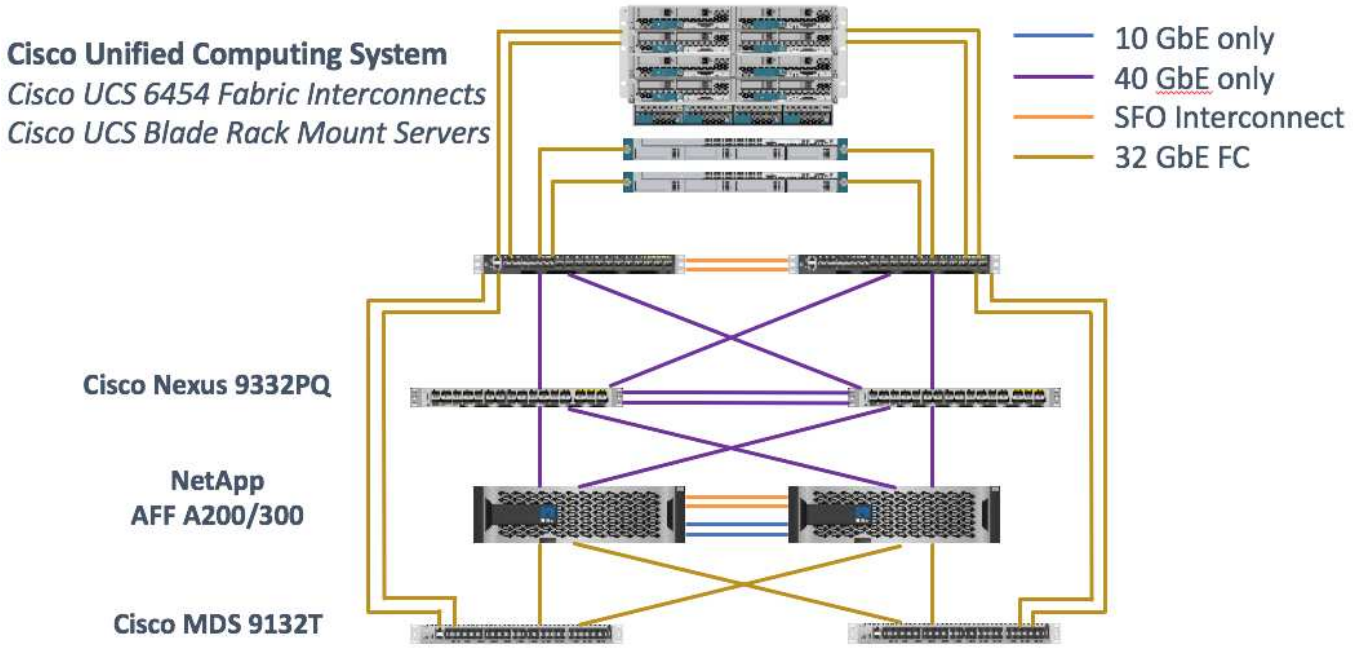
  Para obter mais informações, "TR-4190: Diretrizes de dimensionamento NetApp para ambientes MEDITECH"consulte .

- Uso das tecnologias NetApp SnapMirror para atender aos requisitos de backup e recuperação de desastres.
- Orientação genérica de implantação de storage do NetApp.

Esta seção fornece um exemplo de configuração com práticas recomendadas de implantação de infraestrutura e lista os vários componentes de hardware e software de infraestrutura e as versões que você pode usar.

Diagrama de cabeamento

A figura a seguir ilustra o diagrama de topologia 32GB FC/40GbE para uma implantação MEDITECH.



Utilize sempre o "Ferramenta de Matriz de interoperabilidade (IMT)" para validar que todas as versões de software e firmware são suportadas. A tabela na seção "Módulos e componentes DA MEDITECH" lista os componentes de hardware e software de infraestrutura que foram usados nos testes de solução.

"Próximo: Configuração da infra-estrutura base."

Configuração de infraestrutura de base

Conetividade de rede

As seguintes conexões de rede devem estar em vigor antes de configurar a infra-estrutura:

- A agregação de links que usa canais de portas e canais de portas virtuais (VPCs) é usada em toda a parte, permitindo o design para maior largura de banda e alta disponibilidade:
  - A VPC é usada entre os switches Cisco FI e Cisco Nexus.
  - Cada servidor tem placas de interface de rede virtual (vNICs) com conetividade redundante à malha unificada. O failover de NIC é usado entre FIs para redundância.
  - Cada servidor tem adaptadores de barramento de host virtual (vHBAs) com conetividade redundante à malha unificada.
- O Cisco UCS FI é configurado no modo de host final como recomendado, fornecendo pinning dinâmico de vNICs a switches uplink.

Conectividade de storage

As seguintes conexões de armazenamento devem estar em vigor antes de configurar a infraestrutura:

- Grupos de interface de porta de armazenamento (ifgroups, VPC)
- 10Gb ligação para o interrutor N9K-A
- 10Gb ligação para o interrutor N9K-B
- Gestão na banda (ligação ativo-passivo):

    - 1GB ligação ao interrutor de gestão N9K-A
    - 1GB ligação ao interrutor de gestão N9K-B
- Conectividade de 32GB GB via FC de ponta a ponta por meio de switches MDS Cisco; zoneamento de iniciador único configurado
- Inicialização de SAN FC para alcançar a computação sem monitoração de estado; os servidores são inicializados a partir de LUNs no volume de inicialização hospedado no cluster de storage AFF
- Todos os workloads da MEDITECH são hospedados em LUNs FC, que se espalham pelos nós do controlador de storage

Software de host

O seguinte software deve ser instalado:

- ESXi instalado nos blades Cisco UCS
- VMware vCenter instalado e configurado (com todos os hosts registrados no vCenter)
- VSC instalado e registrado no VMware vCenter
- Cluster NetApp configurado

"Próximo: Configuração do servidor blade Cisco UCS e do switch."

Configuração do servidor blade Cisco UCS e do switch

O software FlexPod for MEDITECH foi concebido com tolerância a falhas em todos os níveis. Não existe um único ponto de falha no sistema. Para um desempenho ideal, a Cisco recomenda o uso de servidores blade hot spare.

Este documento fornece orientações de alto nível sobre a configuração básica de um ambiente FlexPod para o software MEDITECH. Nesta seção, apresentamos etapas de alto nível com alguns exemplos para preparar o elemento da plataforma de computação Cisco UCS da configuração do FlexPod. Um pré-requisito para este guia é que a configuração do FlexPod é em rack, alimentada e cabeada de acordo com as instruções no "FlexPod Datacenter com armazenamento Fibre Channel usando o VMware vSphere 6,5 Update 1, NetApp AFF A-series e Cisco UCS Manager 3,2"CVD.

Configuração de switch Cisco Nexus

Um par tolerante a falhas de switches Ethernet Cisco Nexus 9300 Series é implantado para a solução. Você deve fazer o cabo desses interrutores conforme descrito na "Diagrama de cabeamento"seção. A configuração do Cisco Nexus ajuda a garantir que os fluxos de tráfego Ethernet sejam otimizados para a aplicação MEDITECH.

1. Depois de concluir a configuração inicial e o licenciamento, execute os seguintes comandos para definir os parâmetros de configuração global em ambos os switches:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
port-channel load-balance src-dst l4port
ntp server <global-ntp-server-ip> use-vrf management
ntp master 3
ip route 0.0.0.0/0 <ib-mgmt-vlan-gateway>
copy run start
```

2. Crie as VLANs para a solução em cada switch usando o modo de configuração global:

```
vlan <ib-mgmt-vlan-id>
name IB-MGMT-VLAN
vlan <native-vlan-id>
name Native-VLAN
vlan <vmotion-vlan-id>
name vMotion-VLAN
vlan <vm-traffic-vlan-id>
name VM-Traffic-VLAN
vlan <infra-nfs-vlan-id>
name Infra-NFS-VLAN
exit
copy run start
```

3. Crie a interface de distribuição do Network Time Protocol (NTP), os canais de portas, os parâmetros do canal da porta e as descrições das portas para a solução de problemas por "FlexPod Datacenter com armazenamento Fibre Channel usando o VMware vSphere 6,5 Update 1, NetApp AFF A-series e Cisco UCS Manager 3,2"CVD.

Configuração do Cisco MDS 9132T

Os switches FC da série Cisco MDS 9100 fornecem conectividade de FC de 32GB GB redundante entre os controladores NetApp AFF A200 ou AFF A300 e a malha de computação Cisco UCS. Deve ligar os cabos conforme descrito na "Diagrama de cabeamento" secção.

1. Nos consoles em cada switch MDS, execute os seguintes comandos para habilitar os recursos necessários para a solução:

```
configure terminal
feature npiv
feature fport-channel-trunk
```

2. Configure portas individuais, canais de portas e descrições de acordo com a seção de configuração do switch FlexPod Cisco MDS em "Data center FlexPod com FC Cisco Validated Design".
3. Para criar as SANs virtuais (VSANs) necessárias para a solução, execute as seguintes etapas no modo de

configuração global:

a. Para o switch MDS Fabric-A, execute os seguintes comandos:

```
vsan database
vsan <vsan-a-id>
vsan <vsan-a-id> name Fabric-A
exit
zone smart-zoning enable vsan <vsan-a-id>
vsan database
vsan <vsan-a-id> interface fc1/1
vsan <vsan-a-id> interface fc1/2
vsan <vsan-a-id> interface port-channel110
vsan <vsan-a-id> interface port-channel112
```

Os números de canal de porta nas duas últimas linhas do comando foram criados quando portas individuais, canais de porta e descrições foram provisionados usando o documento de referência.

b. Para o switch MDS Fabric-B, execute os seguintes comandos:

```
vsan database
vsan <vsan-b-id>
vsan <vsan-b-id> name Fabric-B
exit
zone smart-zoning enable vsan <vsan-b-id>
vsan database
vsan <vsan-b-id> interface fc1/1
vsan <vsan-b-id> interface fc1/2
vsan <vsan-b-id> interface port-channel111
vsan <vsan-b-id> interface port-channel113
```

Os números de canal de porta nas duas últimas linhas do comando foram criados quando portas individuais, canais de porta e descrições foram provisionados usando o documento de referência.

4. Para cada switch FC, crie nomes de alias de dispositivo que tornam a identificação de cada dispositivo intuitiva para operações contínuas usando os detalhes no documento de referência.
5. Por fim, crie as zonas FC usando os nomes de alias do dispositivo criados na etapa 4 para cada switch MDS da seguinte forma:

a. Para o switch MDS Fabric-A, execute os seguintes comandos:

```
configure terminal
zone name VM-Host-Infra-01-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-01-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zone name VM-Host-Infra-02-A vsan <vsan-a-id>
member device-alias VM-Host-Infra-02-A init
member device-alias Infra-SVM-fcp_lif01a target
member device-alias Infra-SVM-fcp_lif02a target
exit
zoneset name Fabric-A vsan <vsan-a-id>
member VM-Host-Infra-01-A
member VM-Host-Infra-02-A
exit
zoneset activate name Fabric-A vsan <vsan-a-id>
exit
show zoneset active vsan <vsan-a-id>
```

b. Para o switch MDS Fabric-B, execute os seguintes comandos:

```
configure terminal
zone name VM-Host-Infra-01-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-01-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zone name VM-Host-Infra-02-B vsan <vsan-b-id>
member device-alias VM-Host-Infra-02-B init
member device-alias Infra-SVM-fcp_lif01b target
member device-alias Infra-SVM-fcp_lif02b target
exit
zoneset name Fabric-B vsan <vsan-b-id>
member VM-Host-Infra-01-B
member VM-Host-Infra-02-B
exit
zoneset activate name Fabric-B vsan <vsan-b-id>
exit
show zoneset active vsan <vsan-b-id>
```

Orientação de configuração do Cisco UCS

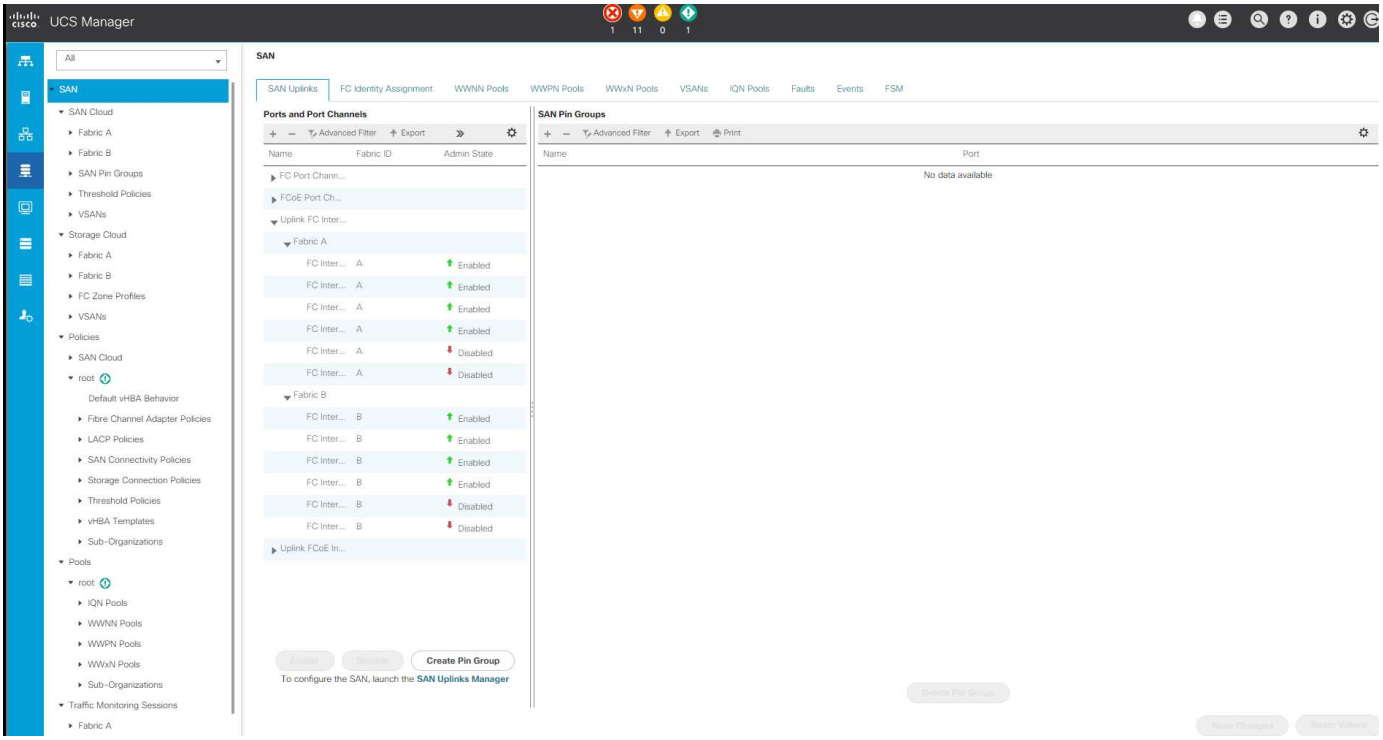
O Cisco UCS permite que você, como cliente MEDITECH, aproveite seus especialistas no assunto em rede, storage e computação para criar políticas e modelos que personalizem o ambiente de acordo com suas

necessidades específicas. Depois que eles são criados, essas políticas e modelos podem ser combinados em perfis de serviço que oferecem implantações consistentes, repetíveis, confiáveis e rápidas de servidores blade e rack Cisco.

O Cisco UCS oferece três métodos para gerenciar um sistema Cisco UCS, chamado de domínio:

- GUI do Cisco UCS Manager HTML5
- CLI do Cisco UCS
- Cisco UCS Central para ambientes de vários domínios

A figura a seguir mostra uma captura de tela de exemplo do nó SAN no Gerenciador Cisco UCS.



Em implantações maiores, domínios Cisco UCS independentes podem ser criados para maior tolerância a falhas no nível de componentes funcionais MEDITECH.

Em designs altamente tolerantes a falhas com dois ou mais data centers, o Cisco UCS Central desempenha um papel fundamental na definição de políticas globais e perfis de serviços globais para consistência entre hosts em toda a empresa.

Para configurar a plataforma de computação do Cisco UCS, execute os procedimentos a seguir. Execute esses procedimentos após os servidores blade Cisco UCS B200 M5 serem instalados no chassi blade AC do Cisco UCS 5108. Além disso, você deve competir com os requisitos de cabeamento, conforme descrito na "Diagrama de cabeamento"seção.

1. Atualize o firmware do Cisco UCS Manager para a versão 3,2(2f) ou posterior.
2. Configure os relatórios, os recursos de início de chamadas do Cisco e as configurações do NTP para o domínio.
3. Configure o servidor e as portas uplink em cada interconexão de malha.
4. Edite a política de deteção de chassis.
5. Crie os pools de endereços para gerenciamento fora da banda, identificadores únicos universais (UUIDs),

endereço MAC, servidores, nome de nó mundial (WWNN) e nome de porta mundial (WWPN).

6. Crie os canais de porta uplink Ethernet e FC e VSANs.
7. Crie políticas para conetividade SAN, controle de rede, qualificação de pool de servidores, controle de energia, BIOS de servidor e manutenção padrão.
8. Crie modelos vNIC e vHBA.
9. Crie políticas de inicialização vMedia e FC.
10. Crie modelos de perfil de serviço e perfis de serviço para cada elemento da plataforma MEDITECH.
11. Associe os perfis de serviço aos servidores blade apropriados.

Para obter as etapas detalhadas para configurar cada elemento-chave dos perfis de serviço do Cisco UCS para FlexPod, consulte o "FlexPod Datacenter com armazenamento Fibre Channel usando o VMware vSphere 6,5 Update 1, NetApp AFF A-series e Cisco UCS Manager 3,2" documento CVD.

"Próximo: Melhores práticas de configuração do ESXi."

Práticas recomendadas de configuração do ESXi

Para a configuração do lado do host ESXi, configure os hosts VMware como você executaria qualquer workload de banco de dados empresarial:

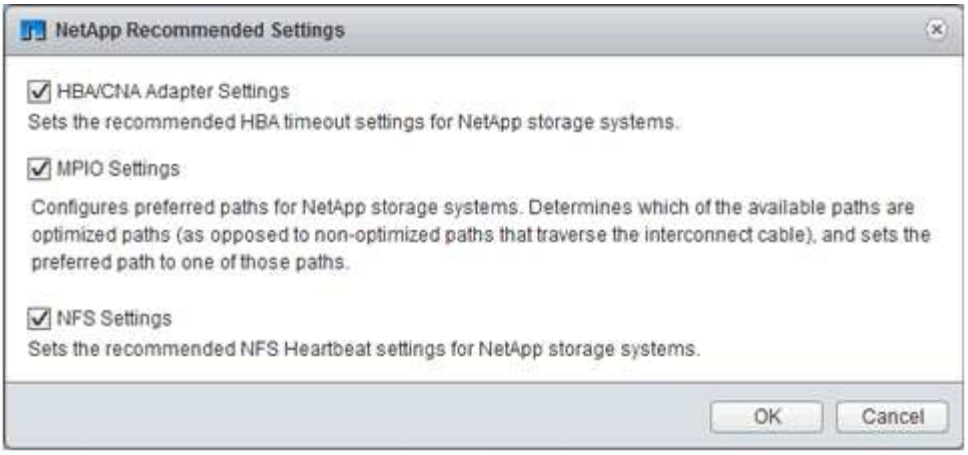
- O VSC para VMware vSphere verifica e define as configurações de multipathing do host ESXi e as configurações de tempo limite do HBA que funcionam melhor com os sistemas de armazenamento NetApp. Os valores que o VSC define são baseados em rigorosos testes internos da NetApp.
- Para obter um desempenho ideal de storage, considere o uso de hardware de storage compatível com VMware vStorage APIs - Array Integration (VAAI). O plug-in do NetApp para VAAI é uma biblioteca de software que integra as bibliotecas de disco virtual da VMware instaladas no host ESXi. O pacote VMware VAAI permite o descarregamento de certas tarefas dos hosts físicos para o storage array.

  É possível executar tarefas como provisionamento de thin Provisioning e aceleração de hardware no nível do array para reduzir o workload nos hosts ESXi. O recurso de descarga de cópia e o recurso de reserva de espaço melhoram o desempenho das operações do VSC. Você pode baixar o pacote de instalação do plug-in e obter as instruções para instalar o plug-in no site de suporte da NetApp.

  O VSC define tempos limite de host ESXi, configurações de multipath e configurações de tempo limite HBA e outros valores para desempenho ideal e failover bem-sucedido dos controladores de armazenamento NetApp. Siga estes passos:

  a. Na página inicial do VMware vSphere Web Client, selecione vCenter > hosts.
  b. Clique com o botão direito do rato num anfitrião e selecione ações > NetApp VSC > Definir valores recomendados.
  c. Na caixa de diálogo Configurações recomendadas do NetApp , selecione os valores que funcionam melhor com o sistema.

     Os valores padrão recomendados são definidos por padrão.



a. Clique em OK.

"Próximo: Configuração do NetApp."

Configuração do NetApp

O storage NetApp implantado para ambientes de software MEDITECH usa controladores de storage em uma configuração de par de alta disponibilidade. O storage deve ser apresentado de ambas as controladoras para servidores de banco de dados MEDITECH pelo protocolo FC. A configuração apresenta armazenamento de ambos os controladores para equilibrar uniformemente a carga da aplicação durante a operação normal.

Configuração ONTAP

Esta seção descreve um exemplo de procedimentos de implantação e provisionamento que usam os comandos ONTAP relevantes. A ênfase é mostrar como o storage é provisionado para implementar o layout de storage recomendado pela NetApp, que usa um par de controladores de alta disponibilidade. Uma das principais vantagens do ONTAP é a capacidade de fazer escalabilidade horizontal sem perturbar os pares de alta disponibilidade existentes.

Licenças ONTAP

Depois de configurar os controladores de storage, aplique licenças para ativar os recursos do ONTAP recomendados pela NetApp. As licenças para workloads MEDITECH são as tecnologias FC, CIFS e NetApp Snapshot, SnapRestore, FlexClone e SnapMirror.

Para configurar licenças, abra o Gerenciador de sistema do NetApp ONTAP, vá para licenças de configuração e adicione as licenças apropriadas.

Como alternativa, execute o seguinte comando para adicionar licenças usando a CLI:

```
license add -license-code <code>
```

Configuração do AutoSupport

A ferramenta NetApp AutoSupport envia informações de suporte resumidas para o NetApp por meio de

HTTPS. Para configurar o AutoSupport, execute os seguintes comandos ONTAP:

```
autosupport modify -node * -state enable
autosupport modify -node * -mail-hosts <mailhost.customer.com>
autosupport modify -node prod1-01 -from prod1-01@customer.com
autosupport modify -node prod1-02 -from prod1-02@customer.com
autosupport modify -node * -to storageadmins@customer.com
autosupport modify -node * -support enable
autosupport modify -node * -transport https
autosupport modify -node * -hostnamesubj true
```

Configuração de takeover assistido por hardware

Em cada nó, habilite o takeover assistido por hardware para minimizar o tempo necessário para iniciar um takeover no caso improvável de uma falha do controlador. Para configurar a aquisição assistida por hardware, execute as seguintes etapas:

1. Execute o seguinte comando ONTAP para xxx.

   Defina a opção endereço do parceiro como endereço IP da porta de gerenciamento `prod1-01` do .

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist-partner-ip
   <prod1-02-mgmt-ip>
   ```

2. Execute o seguinte comando ONTAP para xxx:

   Defina a opção endereço do parceiro como endereço IP da porta de gerenciamento `cluster1-02` do .

   ```
   MEDITECH::> storage failover modify -node prod1-02 -hwassist-partner-ip
   <prod1-01-mgmt-ip>
   ```

3. Execute o seguinte comando ONTAP para habilitar o takeover assistido por hardware no `prod1-01` par de controladores de HA e no `prod1-02` par.

   ```
   MEDITECH::> storage failover modify -node prod1-01 -hwassist true
   MEDITECH::> storage failover modify -node prod1-02 -hwassist true
   ```

"Próximo: Configuração agregada."

Configuração de agregado

NetApp RAID DP

A NetApp recomenda a tecnologia NetApp RAID DP como tipo RAID para todos os agregados em um sistema NetApp FAS ou AFF, incluindo agregados regulares de pool flash NetApp. A documentação DA MEDITECH

pode especificar o uso do RAID 10, mas a MEDITECH aprovou o uso do RAID DP.

Tamanho do grupo RAID e número de grupos RAID

O tamanho padrão do grupo RAID é 16. Esse tamanho pode ou não ser ideal para os agregados para os hosts MEDITECH em seu site específico. Para saber o número de discos que o NetApp recomenda que você use em um grupo RAID, "NetApp TR-3838: Guia de configuração do subsistema de armazenamento" consulte .

O tamanho do grupo RAID é importante para a expansão de armazenamento porque o NetApp recomenda que você adicione discos a um agregado com um ou mais grupos de discos iguais ao tamanho do grupo RAID. O número de grupos RAID depende do número de discos de dados e do tamanho do grupo RAID. Para determinar o número de discos de dados de que você precisa, use a ferramenta de dimensionamento do modelo de desempenho do sistema (SPM) da NetApp. Depois de determinar o número de discos de dados, ajuste o tamanho do grupo RAID para minimizar o número de discos de paridade para dentro do intervalo recomendado para o tamanho do grupo RAID por tipo de disco.

Para obter detalhes sobre como usar a ferramenta de dimensionamento SPM para ambientes MEDITECH, "NetApp TR-4190: Diretrizes de dimensionamento NetApp para ambientes MEDITECH" consulte .

Considerações sobre a expansão do armazenamento de dados

Quando expandir agregados com mais discos, adicione os discos em grupos iguais ao tamanho do grupo RAID agregado. Seguir essa abordagem ajuda a fornecer consistência de desempenho em todo o agregado.

Por exemplo, para adicionar armazenamento a um agregado que foi criado com um tamanho de grupo RAID de 20, o número de discos que o NetApp recomenda adicionar é um ou mais grupos de 20 discos. Então, você deve adicionar 20, 40, 60, e assim por diante, discos.

Depois de expandir agregados, você pode melhorar a performance executando tarefas de realocação nos volumes afetados ou agregados para espalhar as faixas de dados existentes nos novos discos. Esta ação é útil especialmente se o agregado existente estava quase cheio.

> Você deve Planejar a realocação de programações durante as horas de não produção, porque é uma tarefa de alto consumo de CPU e disco.

Para obter mais informações sobre como usar a realocação após uma expansão agregada, "NetApp TR-3929: Guia de práticas recomendadas de realocar"consulte .

Cópias Snapshot em nível de agregado

Defina a reserva de cópia Snapshot do NetApp em nível agregado como zero e desative a programação Snapshot agregada padrão. Exclua quaisquer cópias Snapshot de nível agregado pré-existentes, se possível.

"Próximo: Configuração da máquina virtual de armazenamento."

Configuração da máquina virtual de armazenamento

Esta seção se refere à implantação no ONTAP 8,3 e versões posteriores.

> Uma máquina virtual de storage (SVM) também é conhecida como SVM na API do ONTAP e na CLI do ONTAP.

SVM para LUNs de host MEDITECH

Você deve criar um SVM dedicado por cluster de storage ONTAP para ter e gerenciar agregados que contêm LUNs para os hosts MEDITECH.

Configuração de codificação de idioma SVM

O NetApp recomenda que você defina a codificação de idioma para todos os SVMs. Se nenhuma configuração de codificação de idioma for especificada no momento em que o SVM é criado, a configuração de codificação de idioma padrão será usada. A configuração padrão de codificação de idioma é C.UTF-8 para ONTAP. Depois que a codificação de idioma tiver sido definida, você não poderá modificar o idioma de um SVM com Infinite volume posteriormente.

Os volumes associados ao SVM herdam a configuração de codificação da linguagem SVM, a menos que você especifique explicitamente outra configuração quando os volumes são criados. Para permitir que certas operações funcionem, você deve usar a configuração de codificação de idioma de forma consistente em todos os volumes do seu site. Por exemplo, o SnapMirror requer que o SVM de origem e destino tenha a mesma configuração de codificação de idioma.

"Próximo: Configuração do volume."

Configuração do volume

Provisionamento de volume

Os volumes DA MEDITECH dedicados aos hosts da MEDITECH podem ser provisionados de forma grossa ou fina.

Cópias Snapshot padrão em nível de volume

As cópias snapshot são criadas como parte do fluxo de trabalho de backup. Cada cópia Snapshot pode ser usada para acessar os dados armazenados nas LUNs MEDITECH em momentos diferentes. A solução de backup aprovada pela MEDITECH cria volumes FlexClone com thin Provisioning com base nessas cópias Snapshot para fornecer cópias pontuais dos LUNs MEDITECH. O ambiente MEDITECH é integrado com uma solução de software de backup aprovada. Portanto, a NetApp recomenda que você desative o agendamento de cópia Snapshot padrão em cada um dos volumes NetApp FlexVol que compõem as LUNs do banco de dados de produção da MEDITECH.

Importante: os volumes FlexClone compartilham espaço de volume de dados pai, por isso é vital que o volume tenha espaço suficiente para os LUNs de dados MEDITECH e os volumes FlexClone criados pelos servidores de backup. Os volumes FlexClone não ocupam mais espaço da maneira que os volumes de dados. No entanto, se houver grandes exclusões nas LUNs MEDITECH em pouco tempo, os volumes de clones podem crescer.

Número de volumes por agregado

Para um sistema NetApp FAS que usa o armazenamento em cache Flash Pool ou Flash Cache da NetApp, a NetApp recomenda o provisionamento de três ou mais volumes por agregado dedicados ao armazenamento dos arquivos de dados, dicionário e programa MEDITECH.

Para sistemas AFF, a NetApp recomenda dedicar quatro ou mais volumes por agregado para armazenar o programa MEDITECH, dicionário e arquivos de dados.

Programa de reatribuição em nível de volume

O layout de dados do storage se torna menos ideal ao longo do tempo, especialmente quando é usado por workloads com uso intenso de gravação, como as plataformas MEDITECH Expanse, 6.x e C/S 5.x. Com o tempo, essa situação pode aumentar a latência de leitura sequencial, resultando em um tempo mais longo para concluir o backup. O layout ou a fragmentação de dados ruins também podem afetar a latência de gravação. Você pode usar a realocação em nível de volume para otimizar o layout de dados em disco a fim de aprimorar as latências de gravação e o acesso de leitura sequencial. O layout de armazenamento melhorado ajuda a concluir o backup dentro do período de tempo alocado de 8 horas.

Prática recomendada
No mínimo, a NetApp recomenda que você implemente um cronograma semanal de realocação de volume para executar operações de realocação durante o tempo de inatividade de manutenção alocado ou durante horas fora de pico em um local de produção. A NetApp recomenda vivamente que execute a tarefa de realocação num volume de cada vez por controlador.

Para obter mais informações sobre como determinar uma agenda de realocação de volume apropriada para o armazenamento do banco de dados de produção, consulte a seção 3,12 em "NetApp TR-3929: Guia de práticas recomendadas de realocar". essa seção também o orienta sobre como criar uma agenda de realocação semanal para um local ocupado.

"Próximo: Configuração LUN."

Configuração LUN

O número de hosts MEDITECH em seu ambiente determina o número de LUNs criados no sistema NetApp FAS ou AFF. A proposta de Configuração de hardware especifica o tamanho de cada LUN.

Provisionamento DE LUN

Os LUNs DA MEDITECH dedicados aos hosts da MEDITECH podem ser provisionados de forma grossa ou fina.

Tipo de sistema operativo LUN

Para alinhar corretamente os LUNs criados, você deve definir corretamente o tipo de sistema operacional para os LUNs. LUNs desalinhados geram sobrecarga de operação de gravação desnecessária e é caro corrigir um LUN desalinhado.

O servidor host MEDITECH normalmente é executado no ambiente virtualizado do Windows Server usando o hipervisor VMware vSphere. O servidor host também pode ser executado no ambiente Windows Server em um servidor bare-metal. Para determinar o valor correto do tipo de sistema operacional a ser definido, consulte a seção "criar LUN" de "Comandos do Clustered Data ONTAP 8.3: Referência de página manual".

Tamanho da LUN

Para determinar o tamanho do LUN para cada host MEDITECH, consulte a proposta de configuração de hardware (nova implantação) ou o documento de tarefa de avaliação de hardware (implantação existente) da MEDITECH.

Apresentação de LUN

A MEDITECH exige que o armazenamento para arquivos de programa, dicionário e dados seja apresentado aos hosts MEDITECH como LUNs usando o protocolo FC. No ambiente virtual da VMware, os LUNs são apresentados aos servidores VMware ESXi que hospedam os hosts MEDITECH. Em seguida, cada LUN que é apresentado ao servidor VMware ESXi é mapeado para cada VM host MEDITECH usando RDM no modo de compatibilidade física.

Você deve apresentar os LUNs aos hosts MEDITCH usando as convenções de nomenclatura de LUN adequadas. Por exemplo, para facilitar a administração, é necessário apresentar o LUN `MTFS01E` ao host MEDITECH `mt-host-01` .

Consulte a proposta de configuração de hardware da MEDITECH quando consultar o instalador do sistema MEDITECH e de backup para elaborar uma convenção de nomenclatura consistente para os LUNs que os hosts da MEDITECH usam.

Um exemplo de um nome LUN MEDITECH é `MTFS05E`, no qual:

- `MTFS` Indica o servidor de arquivos MEDITECH (para o host MEDITECH).
- `05` indica o número de host 5.
- `E` Indica a unidade do Windows E.

"Próximo: Configuração do Grupo de iniciadores."

Configuração do grupo de iniciadores

Quando você usa FC como protocolo de rede de dados, crie dois grupos de iniciadores (grupos de iniciadores) em cada controlador de storage. O primeiro grupo contém as WWPNs das placas de interface de host FC nos servidores VMware ESXi que hospedam as VMs de host MEDITECH (igrop para MEDITECH).

Tem de definir o tipo de sistema operativo MEDITECH igroup de acordo com a configuração do ambiente. Por exemplo:

- Use o tipo de sistema operacional igrop `Windows` para aplicativos instalados em hardware de servidor bare-metal em um ambiente Windows Server.
- Use o tipo de sistema operacional igrop `VMware` para aplicativos virtualizados usando o hipervisor VMware vSphere.

> O tipo de sistema operacional para um grupo pode ser diferente do tipo de sistema operacional para um LUN. Por exemplo, para hosts virtualizados MEDITECH, você deve definir o tipo de sistema operacional igrop como `VMware`. Para os LUNs usados pelos hosts virtualizados MEDITECH, você deve definir o tipo de sistema operacional como `Windows 2008 or later`. Use essa configuração porque o sistema operacional host MEDITECH é o Windows Server Enterprise Edition de 2008 R2 64 bits.

Para determinar o valor correto para o tipo de sistema operacional, consulte as seções "LUN Igroup create" e "LUN create" no "Comandos do Clustered Data ONTAP 8.2: Referência de página manual".

"Próximo: Mapeamentos LUN."

Mapeamentos LUN

Mapeamentos LUN para os hosts MEDITECH são estabelecidos quando os LUNs são criados.

Módulos e componentes DA MEDITECH

A aplicação MEDITECH abrange vários módulos e componentes. A tabela a seguir lista as funções que são cobertas por esses módulos. Para obter informações adicionais sobre como configurar e implantar esses módulos, consulte a documentação da MEDITECH.

Função	Tipo
Conetividade	• Servidor Web • Servidor de aplicações Live (WI – integração Web) • Servidor de aplicativos de teste (Wi) • Servidor de autenticação SAML (Wi) • Servidor proxy SAML (Wi) • Servidor de banco de dados
Infraestrutura	• Servidor de arquivos • Cliente trabalho em segundo plano • Servidor de conexão • Servidor de transações
Digitalização e arquivamento	• Servidor de imagens
Repositório de dados	• SQL Server
Análises comerciais e clínicas	• Servidor de inteligência em tempo real (BCA) • Servidor de inteligência de teste (BCA) • Servidor de banco de dados (BCA)

Função	Tipo
Cuidados domésticos	• Solução local remoto • Conetividade • Infraestrutura • Impressão • Dispositivos de campo • Digitalização • Requisitos do site hospedado • Configuração da firewall
Suporte	• Cliente de trabalho em segundo plano (CALs – Licença de Acesso ao Cliente)
Dispositivos do utilizador	• Comprimidos • Dispositivos fixos
Impressão	• Servidor de impressão em rede ativa (necessário; pode já existir) • Servidor de impressão de rede de teste (necessário; pode já existir)
Requisito de terceiros	• Primeiro Databank (FDB) MedKnowledge Framework v4,3

Agradecimentos

As seguintes pessoas contribuíram para a criação deste guia.

- Brandon Agee, engenheiro técnico de marketing, NetApp
- Atul Bhalodia, Engenheiro de Marketing Técnico, NetApp
- Ketan Mota, gerente sênior de produto, NetApp
- John Duignan, arquiteto de soluções de saúde, NetApp
- Cisco
- Mike Brennan, Cisco

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos ou sites:

Zona de design FlexPod

- "Zona de Design de FlexPod"

- "Data center do FlexPod com storage FC (switches MDS) usando NetApp AFF, vSphere 6.5U1 e Cisco UCS Manager"

Relatórios técnicos da NetApp

- "TR-3929: Guia de práticas recomendadas de realocar"
- "TR-3987: Snap Creator Framework Plug-in para InterSystems Caché"
- "TR-4300i: Guia de práticas recomendadas de sistemas de storage all-flash e NetApp FAS para ambientes MEDITECH"
- "TR-4017: Melhores práticas FC SAN"
- "TR-3446: Visão geral e Guia de melhores práticas do SnapMirror Async"

Documentação do ONTAP

- "Documentação do produto NetApp"
- "Console de armazenamento virtual (VSC) para documentação do vSphere"
- "Centro de Documentação do ONTAP 9":
  - "Guia do FC Express para ESXi"
- "Toda a documentação do ONTAP 9.3":
  - "Guia de configuração do software"
  - "Guia de alimentação de discos e agregados"
  - "Guia de administração DE SAN"
  - "Guia de configuração do SAN"
  - "Guia de configuração FC para Windows Express"
  - "Guia de configuração do AFF otimizado para SAN FC"
  - "Guia de configuração de alta disponibilidade"
  - "Guia de gerenciamento de storage lógico"
  - "Guia de potência de gestão de desempenho"
  - "Guia de alimentação de configuração SMB/CIFS"
  - "Referência SMB/CIFS"
  - "Guia de alimentação de proteção de dados"
  - "Guia de backup e recuperação de fita de proteção de dados"
  - "Guia de alimentação de encriptação NetApp"
  - "Guia de gerenciamento de rede"
  - "Comandos: Manual de Referência de Página para ONTAP 9.3"

Guias do Cisco Nexus, MDS, Cisco UCS e Cisco UCS Manager

- "Visão geral dos servidores Cisco UCS"
- "Visão geral dos servidores blade Cisco UCS"
- "Folha de dados do Cisco UCS B200 M5"

- "Visão geral do Cisco UCS Manager"
- "Pacote de infraestrutura do Cisco UCS Manager 3,2(3a)" (Requer autorização Cisco.com)
- "Switches da plataforma Cisco Nexus 9300"
- "Switch Cisco MDS 9132T FC"

FlexPod para imagens médicas

TR-4865: FlexPod para imagens médicas

São Paulo, Brasil and Atul Bhalodia, NetApp

As imagens médicas são responsáveis por 70% de todos os dados gerados pelas organizações de saúde. À medida que as modalidades digitais continuam a avançar e novas modalidades surgem, a quantidade de dados continuará a aumentar. Por exemplo, a transição da patologia analógica para a digital aumentará drasticamente os tamanhos das imagens a uma taxa que desafiará qualquer estratégia de gerenciamento de dados atualmente em vigor.

A COVID-19 reformulou claramente a transformação digital; de acordo com um recente "relatório", a COVID-19 acelerou o comércio digital em 5 anos. A inovação tecnológica impulsionada pelos solucionadores de problemas está mudando fundamentalmente a maneira como passamos em nossa vida diária. Esta mudança orientada pela tecnologia irá rever muitos aspetos críticos da nossa vida, incluindo a saúde.

Os cuidados de saúde estão preparados para sofrer uma grande mudança nos próximos anos. A COVID está acelerando a inovação em saúde que impulsionará o setor em pelo menos vários anos. No centro desta mudança está a necessidade de tornar os cuidados de saúde mais flexíveis no tratamento de pandemias, por serem mais acessíveis, disponíveis e acessíveis, sem comprometer a fiabilidade.

Na base dessa mudança de saúde está uma plataforma bem projetada. Uma das principais métricas para medir a plataforma é a facilidade com que as mudanças de plataforma podem ser implementadas. Velocidade é a nova escala e a proteção de dados não pode ser comprometida. Alguns dos dados mais críticos do mundo estão sendo criados e consumidos pelos sistemas clínicos que dão suporte aos médicos. A NetApp disponibilizou dados críticos para o atendimento ao paciente onde os médicos precisam, no local, na nuvem ou em um ambiente híbrido. Os ambientes multicloud híbridos são o estado atual da ARQUITETURA DE TI.

A saúde como sabemos gira em torno de prestadores (médicos, enfermeiros, radiologistas, técnicos de dispositivos médicos, etc.) e pacientes. À medida que aproximamos pacientes e provedores, tornando a localização geográfica um mero ponto de dados, torna-se ainda mais importante que a plataforma subjacente esteja disponível quando provedores e pacientes precisarem dela. A plataforma deve ser eficiente e econômica a longo prazo. Em seus esforços para impulsionar os custos de atendimento ao paciente ainda mais baixos, "Organizações de cuidados responsáveis" a (acos) seria capacitada por uma plataforma eficiente.

Quando se trata de sistemas de informação de saúde usados por organizações de saúde, a questão de construção versus compra tende a ter uma única resposta: Compra. Isso pode ser por muitas razões subjetivas. As decisões de compra tomadas ao longo de muitos anos podem criar sistemas de informação heterogêneos. Cada sistema tem um conjunto específico de requisitos para a plataforma na qual eles são implantados. O problema mais significativo é o grande e diversificado conjunto de protocolos de storage e níveis de performance que os sistemas de informações exigem, o que torna a padronização da plataforma e a eficiência operacional ideal um desafio significativo. As organizações de saúde não podem se concentrar em questões críticas de missão, porque sua atenção é espalhada por necessidades operacionais triviais, como o

grande conjunto de plataformas que exigem um conjunto diversificado de habilidades e, portanto, retenção de PME.

Os desafios podem ser classificados nas seguintes categorias:

- Necessidades heterogêneas de storage
- Silos departamentais
- Complexidade operacional DA TI
- Conectividade da nuvem
- Segurança cibernética
- Inteligência artificial e aprendizagem profunda

Com o FlexPod, você tem uma única plataforma compatível com FC, FCoE, iSCSI, NFS/pNFS, SMB/CIFS e assim por diante a partir de uma única plataforma. As pessoas, os processos e a tecnologia fazem parte do DNA que o FlexPod foi projetado e construído. A QoS adaptável do FlexPod ajuda a quebrar os silos departamentais, apoiando vários sistemas clínicos críticos na mesma plataforma FlexPod subjacente. A FlexPod tem certificação FedRAMP e certificação FIPS 140-2. Além disso, as organizações de saúde enfrentam oportunidades como inteligência artificial e aprendizagem profunda. A FlexPod e a NetApp resolvem esses desafios e disponibilizam os dados onde eles são necessários, no local ou em um ambiente de multicloud híbrida em uma plataforma padronizada. Para obter mais informações e histórias de sucesso de clientes de uma série, "FlexPod Saúde"consulte .

As informações típicas de imagiologia médica e os sistemas PACS têm o seguinte conjunto de capacidades:

- Receção e registo
- Agendamento
- Imagiologia
- Transcrição
- Gerenciamento
- Troca de dados
- Arquivo de imagens
- Visualização de imagens para captura e leitura de imagens para técnicos e visualização de imagens para médicos

Em relação à imagem, o setor de saúde está tentando resolver os seguintes desafios clínicos:

- Adoção mais ampla de "processamento de linguagem natural" assistentes baseados em PNL por técnicos e médicos para leitura de imagens. O departamento de radiologia pode se beneficiar do reconhecimento de voz para transcrever relatórios. A PNL pode ser utilizada para identificar e tornar anónimo o registo de um paciente, especificamente as etiquetas DICOM incorporadas na imagem DICOM. Os recursos de NLP exigem plataformas de alto desempenho com tempos de resposta de baixa latência para processamento de imagens. A qualidade do serviço do FlexPod não só fornece performance e fornece projeções de capacidade maduras para crescimento futuro.
- Adoção mais ampla de vias clínicas padronizadas e protocolos por acos e organizações comunitárias de saúde. Historicamente, as vias clínicas têm sido usadas como um conjunto estático de diretrizes em vez de um fluxo de trabalho integrado que orienta decisões clínicas. Com os avanços em PNL e processamento de imagens, as etiquetas DICOM nas imagens podem ser integradas em vias clínicas como fatos para conduzir decisões clínicas. Portanto, esses processos exigem alto desempenho, baixa latência e alta taxa de transferência a partir da plataforma de infraestrutura subjacente e dos sistemas de

storage.

- Os modelos DE ML que utilizam redes neurais convolucionais permitem a automação dos recursos de processamento de imagens em tempo real e, portanto, exigem uma infraestrutura capaz de GPU. O FlexPod oferece componentes de computação de CPU e GPU integrados ao mesmo sistema, e CPUs e GPUs podem ser dimensionados independentemente um do outro.
- Se as etiquetas DICOM forem utilizadas como factos nos avisos clínicos de melhores práticas, o sistema tem de efetuar mais leituras de artefactos DICOM com baixa latência e alta produtividade.
- Ao avaliar imagens, a colaboração em tempo real entre radiologistas entre organizações requer processamento gráfico de alto desempenho nos dispositivos de computação do usuário final. A NetApp oferece soluções de VDI líderes do setor, projetadas e comprovadas especificamente para casos de uso de gráficos avançados. Mais informações podem ser "aqui"encontradas .
- A gestão de imagens e multimédia nas organizações de saúde ACO pode utilizar uma única plataforma, independentemente do sistema de registo para a imagem, utilizando protocolos como Digital Imaging and Communications in Medicine ("DICOM") e acesso à Web a objetos persistentes DICOM ( ) "WADO"
- A troca de informações de saúde ("HIE") inclui imagens incorporadas nas mensagens.
- As modalidades móveis, como dispositivos portáteis de digitalização sem fio (por exemplo, scanners de ultrassom portáteis de bolso conetados a um telefone), exigem uma infraestrutura de rede robusta com segurança, confiabilidade e latência no nível DoD na borda, no núcleo e na nuvem. "Data fabric desenvolvido pela NetApp" proporcionar às organizações essa capacidade em escala.
- As modalidades mais recentes têm necessidades exponenciais de armazenamento; por exemplo, a TC e a RM requerem algumas centenas de MBs para cada modalidade, mas as imagens de patologia digital (incluindo imagens de lâminas inteiras) podem ter alguns GBs de tamanho. FlexPod é projetado com "desempenho, confiabilidade e dimensionamento como caraterísticas fundamentais".

Uma plataforma de sistema de imagem médica bem arquitetada está no centro da inovação. A arquitetura do FlexPod oferece funcionalidades flexíveis de computação e storage com eficiência de storage líder do setor.

Benefícios gerais da solução

Ao executar um ambiente de aplicação de imagem em uma base arquitetônica da FlexPod, sua organização de saúde pode esperar uma melhoria na produtividade da equipe e uma diminuição no capital e nas despesas operacionais. O FlexPod fornece uma convergente, pré-validada e rigorosamente testada que foi projetada para oferecer alta disponibilidade e performance previsível do sistema de baixa latência. Esta abordagem resulta em elevados níveis de conforto e, em última análise, tempos de resposta ideais para os utilizadores do sistema de imagiologia médica.

Componentes diferentes do sistema de imagem podem exigir o armazenamento de dados em sistemas de arquivos SMB/CIFS, NFS, EXT4 ou NTFS. Esse requisito significa que a infraestrutura precisa fornecer acesso aos dados pelos protocolos NFS, SMB/CIFS e SAN. Um único sistema de storage NetApp pode dar suporte aos protocolos NFS, SMB/CIFS e SAN, eliminando a necessidade de práticas legadas de sistemas de storage específicos a protocolos.

A infraestrutura do FlexPod é uma plataforma modular, convergente, virtualizada, escalável (escalabilidade horizontal e vertical) e econômica. Com a plataforma FlexPod, você pode fazer escalabilidade horizontal independente de computação, rede e storage para acelerar a implantação de aplicações. E a arquitetura modular permite operações ininterruptas mesmo durante as atividades de escalabilidade horizontal e atualização do sistema.

A FlexPod oferece vários benefícios específicos para a indústria de imagens médicas:

- * Desempenho do sistema de baixa latência.* O tempo do radiologista é um recurso de alto valor, e o uso eficiente do tempo de um radiologista é fundamental. A espera por imagens ou vídeos para carregar pode

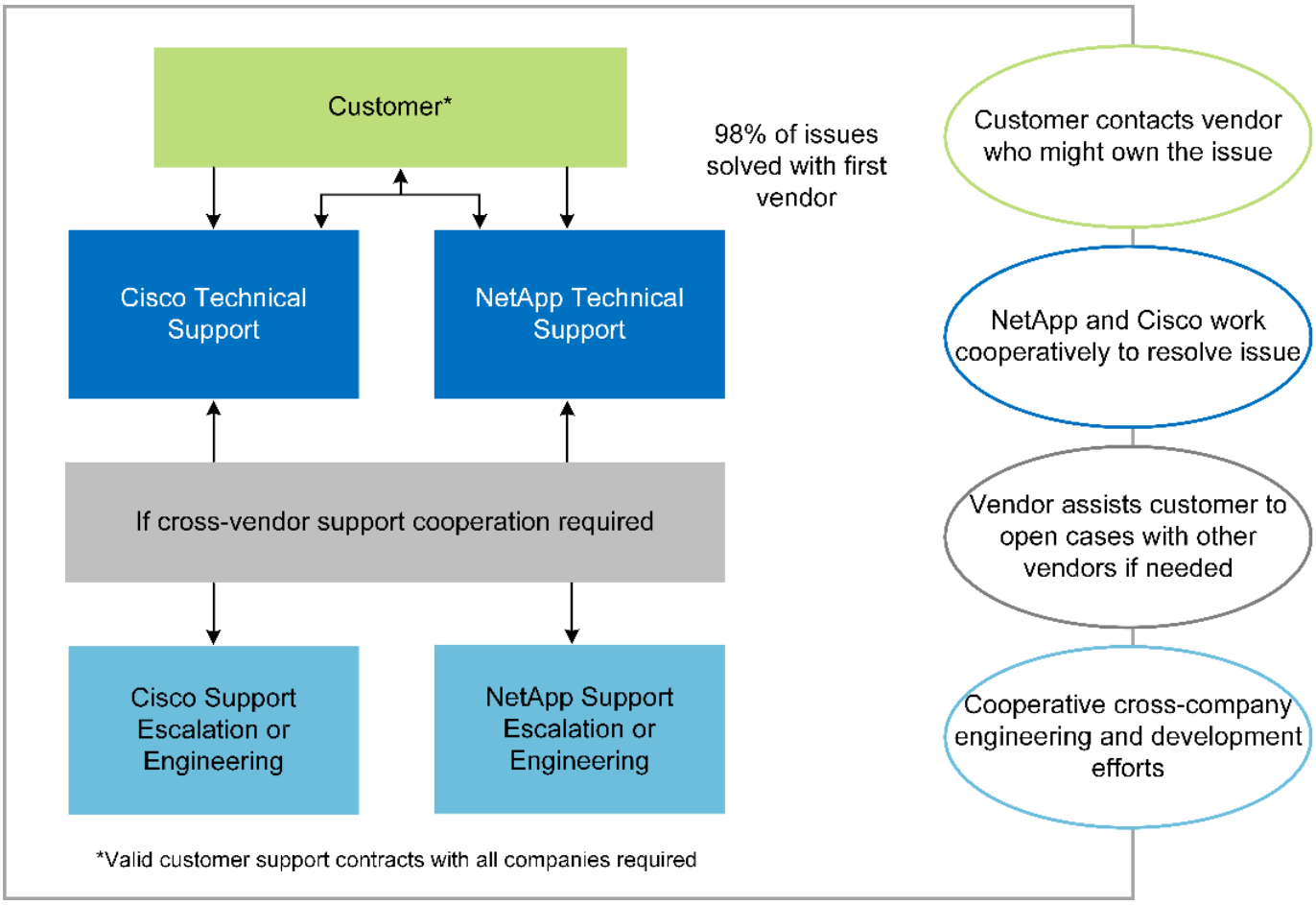
contribuir para o esgotamento clínico e pode afetar a eficiência do médico e a segurança do paciente.

- * Arquitetura modular.* Os componentes do FlexPod são conectados por meio de um servidor em cluster, uma malha de gerenciamento de storage e um toolset de gerenciamento coeso. À medida que as instalações de imagem crescem ano a ano e o número de estudos aumenta, haverá a necessidade de a infraestrutura subjacente se dimensionar em conformidade. O FlexPod pode escalar a computação, o storage e a rede de forma independente.
- * Implantação mais rápida da infraestrutura.* Seja em um data center existente ou em um local remoto, o design integrado e testado do data center FlexPod com imagens médicas permite que você coloque a nova infraestrutura em funcionamento em menos tempo, com menos esforço.
- **Implantação acelerada de aplicativos.** Uma arquitetura pré-validada reduz o tempo e o risco de integração da implementação para qualquer workload, e a tecnologia NetApp automatiza a implantação da infraestrutura. Se você usa a solução para uma implantação inicial de imagens médicas, uma atualização de hardware ou expansão, pode transferir mais recursos para o valor de negócios do projeto.
- **Operações simplificadas e custos mais baixos.** Você pode eliminar as despesas e a complexidade das plataformas proprietárias herdadas substituindo-as por um recurso compartilhado mais eficiente e escalável que pode atender às necessidades dinâmicas de sua carga de trabalho. Essa solução oferece maior utilização de recursos de infraestrutura para obter maior retorno do investimento (ROI).
- * Arquitetura de escalabilidade horizontal.* É possível escalar SAN e nas de terabytes para dezenas de petabytes sem reconfigurar as aplicações em execução.
- **Operações ininterruptas.** É possível realizar manutenção de storage, operações de ciclo de vida de hardware e atualizações de software sem interromper os negócios.
- **Alocação segura a vários clientes.** Esse benefício dá suporte às crescentes necessidades de infraestrutura compartilhada de servidor e armazenamento virtualizado, permitindo a alocação segura de informações específicas de instalações, especialmente se você estiver hospedando várias instâncias de bancos de dados e software.
- * Otimização de recursos em pool.* Esse benefício pode ajudar você a reduzir contagens físicas de servidores e controladores de storage, equilibrar a carga de trabalho e aumentar a utilização, melhorando o desempenho.
- **Qualidade do serviço (QoS).** O FlexPod oferece QoS em toda a pilha. Essas políticas de storage de QoS líderes do setor permitem níveis de serviço diferenciados em um ambiente compartilhado. Essas políticas ajudam a otimizar a performance dos workloads e ajudam a isolar e controlar aplicações fugitivas.
- **Suporte para SLAs de nível de armazenamento usando QoS.** Não é necessário implantar sistemas de storage diferentes para as diferentes camadas de storage que um ambiente de geração de imagens médicas normalmente exige. Para esse fim, é possível atender a um único cluster de storage com vários volumes NetApp FlexVol com políticas de QoS específicas para diferentes camadas. Com essa abordagem, a infraestrutura de storage pode ser compartilhada acomodando dinamicamente as necessidades dinâmicas de uma determinada camada de storage. O NetApp AFF pode dar suporte a diferentes SLAs para camadas de storage ao permitir a QoS no nível do FlexVol volume, eliminando a necessidade de diferentes sistemas de storage para diferentes camadas de storage para a aplicação.
- **Eficiência de armazenamento.** As imagens médicas são normalmente pré-comprimidas pela aplicação de imagem à compressão sem perdas jpeg2k, que é em torno de 2,5:1. No entanto, esta é a aplicação de imagem e o fornecedor específico. Em ambientes de aplicações de geração de imagens maiores (acima de 1PB TB), é possível economizar de 5 a 10% no storage. Além disso, você reduz os custos de storage com os recursos de eficiência de storage da NetApp. Trabalhe com os fornecedores de aplicativos de imagem e com o especialista no assunto da NetApp para descobrir possíveis eficiências de storage para seu sistema de imagens médicas.
- **Agilidade.** Com as ferramentas de gerenciamento, orquestração e automação do workflow líderes do setor que os sistemas FlexPod oferecem, sua EQUIPE DE TI pode responder muito mais às solicitações de negócios. Essas solicitações de negócios podem variar de backup de imagens médicas e

provisionamento de ambientes adicionais de teste e treinamento a replicações de banco de dados de análise para iniciativas de gerenciamento de saúde da população.

- **Maior produtividade.** Você pode implantar e escalar rapidamente essa solução para obter as melhores experiências do usuário final do médico.
- **Data Fabric.** Seu Data Fabric com tecnologia da NetApp truta dados juntos em diferentes locais, além de fronteiras físicas e entre aplicações. Seu Data Fabric com tecnologia NetApp foi desenvolvido para empresas orientadas pelos dados em um mundo centrado nos dados. Os dados são criados e usados em vários locais, e geralmente precisam ser aproveitados e compartilhados com outros locais, aplicações e infraestruturas. Então, você quer uma maneira consistente e integrada de gerenciá-la. Essa solução oferece uma maneira de gerenciar dados que coloca sua EQUIPE DE TI no controle e simplifica a complexidade cada vez maior DA TI.
- **FabricPool.** O NetApp ONTAP FabricPool ajuda a reduzir os custos de storage sem comprometer o desempenho, a eficiência, a segurança ou a proteção. O FabricPool é transparente para as aplicações empresariais e aproveita as eficiências de nuvem ao reduzir o TCO de storage sem a necessidade de rearquitetar a infraestrutura de aplicações. O FlexPod pode se beneficiar das funcionalidades de disposição em camadas de storage do FabricPool para usar mais eficiência o storage flash ONTAP. Para obter informações completas, "FlexPod com FabricPool"consulte .
- **Segurança FlexPod.** A segurança está na base da FlexPod. Nos últimos anos, o ransomware se tornou uma ameaça significativa e crescente. Ransomware é um malware que é baseado em virologia cripto, o uso de criptografia para construir software malicioso. Esse malware pode usar criptografia de chave simétrica e assimétrica para bloquear os dados da vítima e exigir um resgate para fornecer a chave para descriptografar os dados. Para saber como o FlexPod ajuda a mitigar ameaças como ransomware, "A solução para ransomware" consulte . Os componentes da infraestrutura da FlexPod também estão em conformidade com o padrão Federal de processamento de informações "(FIPS) 140-2".
- **Suporte cooperativo do FlexPod.** A NetApp e a Cisco estabeleceram o suporte cooperativo do FlexPod, um modelo de suporte forte, dimensionável e flexível para atender aos requisitos exclusivos de suporte da infraestrutura convergente do FlexPod. Esse modelo usa a experiência, os recursos e a experiência combinada de suporte técnico da NetApp e da Cisco para fornecer um processo simplificado para identificar e resolver seu problema de suporte da FlexPod, independentemente de onde o problema reside. O modelo de suporte cooperativo da FlexPod ajuda a confirmar que seu sistema FlexPod opera de forma eficiente e se beneficia da tecnologia mais atualizada, ao mesmo tempo em que fornece uma equipe experiente para ajudar a resolver problemas de integração.

  O suporte cooperativo do FlexPod é especialmente valioso se sua organização de saúde executar aplicações essenciais aos negócios. A ilustração abaixo mostra uma visão geral do modelo de suporte cooperativo do FlexPod.



Âmbito de aplicação

Este documento fornece uma visão geral técnica de um sistema de computação unificada da Cisco (Cisco UCS) e da infraestrutura FlexPod baseada em NetApp ONTAP para hospedar essa solução de imagem médica.

Público-alvo

Este documento destina-se a líderes técnicos do setor de saúde e a engenheiros de soluções de parceiros da Cisco e da NetApp e à equipe de serviços profissionais. O NetApp presume que o leitor tenha uma boa compreensão dos conceitos de dimensionamento de computação e armazenamento, bem como familiaridade técnica com o sistema de imagem médica, o Cisco UCS e os sistemas de armazenamento NetApp.

Aplicação de imagiologia médica

Uma aplicação típica de imagiologia médica oferece um conjunto de aplicações que, em conjunto, constituem uma solução de imagiologia de nível empresarial para pequenas, médias e grandes organizações de saúde.

No coração do conjunto de produtos estão as seguintes capacidades clínicas:

- Repositório de imagiologia empresarial
- Suporta fontes de imagem tradicionais, como radiologia e cardiologia. Também suporta outras áreas de cuidados como oftalmologia, dermatologia, colonoscopia e outros objetos de imagem médica, como fotos e vídeos.
- "Arquivo de imagens e sistema de comunicação" (PACS), que é um meio informatizado para substituir as

funções do filme radiológico convencional

- Arquivo neutro do fornecedor de imagens empresariais (VNA):
  - Consolidação escalável de documentos DICOM e não DICOM
  - Sistema de imagiologia médica centralizado
  - Suporte para sincronização de documentos e integridade de dados entre vários (PACSs) na empresa
  - Documentar o gerenciamento do ciclo de vida por um sistema especializado baseado em regras que utiliza metadados de documentos, como:
  - Tipo de modalidade
  - Idade do estudo
  - Idade do paciente (atual e no momento da captura de imagens)
  - Ponto único de integração dentro e fora da empresa (HIE):
  - Vinculação de documentos com reconhecimento de contexto
  - Health Level Seven International (HL7), DICOM e WADO
  - Capacidade de arquivamento independente de storage
- Integração com outros sistemas de informação em saúde que utilizam HL7 e ligação consciente do contexto:
  - Permite que as EHRs implementem links diretos para imagens de pacientes a partir de gráficos de pacientes, fluxos de trabalho de imagiologia, etc.
  - Ajuda a incorporar o histórico de imagens de cuidados longitudinais de um paciente em EHRs.
- Fluxos de trabalho do tecnólogo de radiologia
- Visualizadores de espaço zero corporativo para visualização de imagens de qualquer lugar em qualquer dispositivo capaz
- Ferramentas analíticas que alavancam dados retrospetivos e em tempo real:
  - Geração de relatórios de conformidade
  - Relatórios operacionais
  - Relatórios de controle de qualidade e garantia de qualidade

Tamanho da organização de saúde e dimensionamento da plataforma

As organizações de saúde podem ser amplamente classificadas usando métodos baseados em padrões que ajudam programas como ACO. Uma dessas classificações utiliza o conceito de rede clínica integrada (NIC). Um grupo de hospitais pode ser chamado de NIC se eles colaborarem e aderirem a protocolos clínicos padrão comprovados e caminhos para melhorar o valor dos cuidados e reduzir os custos dos pacientes. Hospitais dentro de uma NIC têm controles e práticas para os médicos a bordo que seguem os valores fundamentais da NIC. Tradicionalmente, uma rede integrada de entrega (IDN) tem sido limitada a hospitais e grupos médicos. Um CIN atravessa fronteiras de IDN tradicionais, e um CIN ainda pode fazer parte de uma ACO. Seguindo os princípios de uma NIC, as organizações de saúde podem ser classificadas em pequenas, médias e grandes.

Pequenas organizações de saúde

Uma organização de saúde é pequena se incluir apenas um único hospital com clínicas ambulatórias e um departamento de internação, mas não faz parte de uma NIC. Os médicos trabalham como cuidadores e coordenam o atendimento ao paciente durante um contínuo de atendimento. Essas pequenas organizações geralmente incluem instalações operadas por médicos. Eles podem ou não oferecer cuidados de emergência e trauma como cuidados integrados para o paciente. Normalmente, uma organização de saúde de pequeno

porte realiza cerca de 250.000 estudos de imagem clínica anualmente. Os centros de imagem são considerados pequenas organizações de saúde e fornecem serviços de imagem. Alguns também fornecem serviços de ditado radiológico para outras organizações.

Organizações de saúde médias

Uma organização de saúde considerada de tamanho médio se incluir vários sistemas hospitalares com organizações focadas, como o seguinte:

- Clínicas de cuidados de adultos e hospitais internados adultos
- Departamentos de trabalho e entrega
- Clínicas de cuidados infantis e hospitais de internamento infantil
- Um centro de tratamento do Câncer
- Departamentos de emergência adultos
- Departamentos de emergência infantil
- Um escritório de medicina familiar e cuidados primários
- Um centro de tratamento de trauma adulto
- Um centro de cuidados de trauma infantil

Em uma organização de saúde de médio porte, os médicos seguem os princípios de uma NIC e operam como uma única unidade. Os hospitais têm funções separadas de faturamento hospitalar, médico e farmácia. Os hospitais podem estar associados a institutos de pesquisa acadêmica e realizar pesquisas e ensaios clínicos intervencionistas. Uma organização de saúde de médio porte realiza até 500.000 estudos de imagem clínica anualmente.

Grandes organizações de saúde

Uma organização de saúde é considerada grande se incluir as caraterísticas de uma organização de saúde de médio porte e oferecer as capacidades clínicas de médio porte para a comunidade em vários locais geográficos.

Uma grande organização de saúde normalmente executa as seguintes funções:

- Tem um escritório central para gerenciar as funções gerais
- Participa em joint ventures com outros hospitais
- Negoceia taxas com organizações pagantes anualmente
- Negoceia as taxas de pagador por estado e região
- Participa em programas de uso significativo (MU)
- Realiza pesquisa clínica avançada em coortes de saúde da população usando ferramentas de gerenciamento de saúde da população (PHM) baseadas em padrões
- Realiza até um milhão de estudos de imagem clínica anualmente

Algumas grandes organizações de saúde que participam de um CIN também têm recursos de leitura de imagens baseadas em IA. Essas organizações geralmente realizam um a dois milhões de estudos de imagem clínica anualmente.

Antes de analisar como essas organizações de diferentes tamanhos se traduzem em um sistema FlexPod de tamanho ideal, você deve entender os vários componentes do FlexPod e os diferentes recursos de um sistema FlexPod.

FlexPod

Sistema de computação unificada da Cisco

O Cisco UCS consiste em um único domínio de gerenciamento que está interconetado com uma infraestrutura de e/S unificada. O Cisco UCS para ambientes de imagiologia médica foi alinhado com as recomendações e as práticas recomendadas da infraestrutura do sistema de imagiologia médica da NetApp para que a infraestrutura possa fornecer informações essenciais aos pacientes com disponibilidade máxima.

A base de computação da imagem médica empresarial é a tecnologia Cisco UCS, com seu gerenciamento de sistemas integrado, processadores Intel Xeon e virtualização de servidores. Essas tecnologias integradas solucionam os desafios do data center e permitem que você atinja seus objetivos de design de data center com um sistema de imagem médica típico. O Cisco UCS unifica o gerenciamento de LAN, SAN e sistemas em um link simplificado para servidores de rack, servidores blade e máquinas virtuais (VMs). O Cisco UCS consiste em um par redundante de interconexões de malha do Cisco UCS que fornecem um ponto único de gerenciamento e um único ponto de controle para todo o tráfego de e/S.

O Cisco UCS usa perfis de serviço para que os servidores virtuais na infraestrutura do Cisco UCS sejam configurados de forma correta e consistente. Os perfis de serviço incluem informações críticas do servidor sobre a identidade do servidor, como endereçamento LAN e SAN, configurações de e/S, versões de firmware, ordem de inicialização, LAN virtual de rede (VLAN), porta física e políticas de QoS. Os perfis de serviço podem ser criados dinamicamente e associados a qualquer servidor físico no sistema em minutos, em vez de horas ou dias. A associação de perfis de serviço com servidores físicos é realizada como uma única operação simples que permite a migração de identidades entre servidores no ambiente sem exigir alterações físicas na configuração. Ele também facilita o rápido provisionamento bare-metal de substituições para servidores com falha.

O uso de perfis de serviço ajuda a confirmar que os servidores são configurados de forma consistente em toda a empresa. Ao usar vários domínios de gerenciamento do Cisco UCS, o Cisco UCS Central pode usar perfis de serviço globais para sincronizar informações de configuração e política entre domínios. Se a manutenção tiver de ser efetuada num domínio, a infra-estrutura virtual pode ser migrada para outro domínio. Com essa abordagem, mesmo quando um único domínio está off-line, os aplicativos continuam sendo executados com alta disponibilidade.

O Cisco UCS é uma solução de última geração para computação em servidores blade e rack. O sistema integra uma malha de rede unificada de 40GbE GbE, sem perdas e de baixa latência com servidores de arquitetura x86 de classe empresarial. O sistema é uma plataforma integrada, escalável e multi-chassis, na qual todos os recursos participam de um domínio de gerenciamento unificado. O Cisco UCS acelera o fornecimento de novos serviços de forma simples, confiável e segura por meio de provisionamento e suporte de migração completos para sistemas virtualizados e não virtualizados. O Cisco UCS oferece os seguintes recursos:

- Gerenciamento abrangente
- Simplificação radical
- Alto desempenho

O Cisco UCS consiste nos seguintes componentes:

- **Compute.** O sistema é baseado em uma classe totalmente nova de sistema de computação que incorpora servidores blade e montados em rack baseados na família de produtos de processadores escaláveis Intel Xeon.
- **Rede.** O sistema é integrado a uma malha de rede unificada de 40Gbps de baixa latência, sem perdas. Essa base de rede consolida LANs, SANs e redes de computação de alto desempenho, que são redes separadas hoje em dia. A malha unificada reduz os custos reduzindo o número de adaptadores de rede,

switches e cabos, além de diminuir os requisitos de energia e refrigeração.

- **Virtualização.** O sistema libera todo o potencial da virtualização aprimorando a escalabilidade, o desempenho e o controle operacional de ambientes virtuais. Os recursos de segurança, imposição de políticas e diagnóstico da Cisco agora são estendidos para ambientes virtualizados para oferecer melhor suporte às mudanças nos requisitos de negócios e TI.
- **Acesso ao armazenamento.** O sistema fornece acesso consolidado ao storage SAN e nas na malha unificada. Ele também é um sistema ideal para armazenamento definido por software. Combinando os benefícios de uma única estrutura para gerenciar a computação e os servidores de storage em um único painel, o QoS pode ser implementado se necessário para injetar a limitação de e/S no sistema. E os administradores de servidor podem pré-atribuir políticas de acesso ao storage a recursos de storage, o que simplifica a conetividade e o gerenciamento do storage e pode ajudar a aumentar a produtividade. Além do armazenamento externo, os servidores em rack e blade têm armazenamento interno que pode ser acessado por meio de controladores RAID de hardware integrados. Ao configurar o perfil de armazenamento e a política de configuração de disco no Cisco UCS Manager, as necessidades de armazenamento do sistema operacional do host e dos dados do aplicativo são atendidas por grupos RAID definidos pelo usuário. O resultado é alta disponibilidade e melhor desempenho.
- **Gestão.** O sistema integra exclusivamente todos os componentes do sistema para que toda a solução possa ser gerenciada como uma única entidade pelo Cisco UCS Manager. Para gerenciar todas as configurações e operações do sistema, o Cisco UCS Manager tem uma GUI intuitiva, uma CLI e um poderoso módulo de biblioteca de scripts para o Microsoft Windows PowerShell que são desenvolvidos em uma API robusta.

O sistema de computação unificada da Cisco funde redes e servidores da camada de acesso. Esse sistema de servidor de alta performance e próxima geração oferece ao seu data center um alto nível de agilidade e escalabilidade de carga de trabalho.

Gerente do Cisco UCS

O Cisco UCS Manager fornece gerenciamento unificado e integrado para todos os componentes de software e hardware no Cisco UCS. Usando a tecnologia de conexão única, o UCS Manager gerencia, controla e administra vários gabinetes para milhares de VMs. Por meio de uma GUI intuitiva, uma CLI ou uma API XML, seus administradores usam o software para gerenciar todo o Cisco UCS como uma única entidade lógica. O Cisco UCS Manager reside em um par de interconexões de malha da série Cisco UCS 6300 que usam configuração em cluster e em espera ativa para alta disponibilidade.

O Cisco UCS Manager oferece uma interface de gerenciamento unificada incorporada que integra seus servidores, rede e storage. O Cisco UCS Manager executa a descoberta automática para detetar o inventário, gerenciar e provisionar componentes do sistema que você adicionar ou alterar. Ele oferece um conjunto abrangente de APIs XML para integração de terceiros e expõe 9.000 pontos de integração. Ele também facilita o desenvolvimento personalizado para automação, orquestração e alcance de novos níveis de visibilidade e controle do sistema.

Os perfis de serviço beneficiam ambientes virtualizados e não virtualizados. Eles aumentam a mobilidade de servidores não virtualizados, como quando você move cargas de trabalho de servidor para servidor ou quando você coloca um servidor off-line para serviço ou atualização. Você também pode usar perfis em conjunto com clusters de virtualização para colocar novos recursos on-line facilmente, complementando a mobilidade de VM existente.

Para obter mais informações sobre o Cisco UCS Manager, consulte "Página do produto Cisco UCS Manager".

Diferenciais do Cisco UCS

O sistema de computação unificada da Cisco está revolucionando a maneira como os servidores são gerenciados no data center. Veja os diferenciais exclusivos a seguir do Cisco UCS e do Cisco UCS Manager:

- **Gerenciamento incorporado.** No Cisco UCS, os servidores são gerenciados pelo firmware incorporado nas interconexões de malha, eliminando a necessidade de qualquer dispositivo físico ou virtual externo gerenciá-los.
- **Tecido unificado.** No Cisco UCS, desde o chassi do servidor blade ou servidores de rack até as interconexões de malha, um único cabo Ethernet é usado para tráfego de LAN, SAN e gerenciamento. Essa e/S convergente reduz o número de cabos, SFPs e adaptadores de que você precisa, reduzindo suas despesas operacionais e de capital para a solução geral.
- **Autodescoberta.** Ao simplesmente inserir o servidor blade no chassi ou conetar servidores de rack às interconexões de malha, a descoberta e o inventário dos recursos de computação ocorre automaticamente sem qualquer intervenção de gerenciamento. A combinação da malha unificada e da descoberta automática habilita a arquitetura Wire-Once do Cisco UCS, onde sua capacidade de computação pode ser estendida facilmente, ao mesmo tempo em que mantém a conectividade externa existente com LAN, SAN e redes de gerenciamento.
- **Classificação de recursos baseada em políticas.** Quando um recurso de computação é descoberto pelo Cisco UCS Manager, ele pode ser automaticamente classificado em um determinado pool de recursos com base nas políticas definidas. Esse recurso é útil na computação em nuvem multitenant.
- * Gerenciamento combinado de servidores blade e rack.* O Cisco UCS Manager pode gerenciar servidores blade da série B e servidores de rack da série C no mesmo domínio do Cisco UCS. Esse recurso, juntamente com a computação sem monitoração de estado, torna os recursos de computação verdadeiramente independente do fator de forma de hardware.
- * Arquitetura de gerenciamento baseada em modelo.* A arquitetura e o banco de dados de gerenciamento do Cisco UCS Manager são baseados em modelo e orientados por dados. A API Open XML que é fornecida para operar no modelo de gerenciamento permite a integração fácil e escalável do Cisco UCS Manager com outros sistemas de gerenciamento.
- **Políticas, pools e modelos.** A abordagem de gerenciamento do Cisco UCS Manager é baseada na definição de políticas, pools e modelos em vez de uma configuração confusa. Ele oferece uma abordagem simples, flexível e orientada por dados no gerenciamento de recursos de computação, rede e storage.
- **Integridade referencial solta.** No Cisco UCS Manager, um perfil de serviço, um perfil de porta ou políticas podem se referir a outras políticas ou a outros recursos lógicos com integridade referencial solta. Uma política referida não pode existir no momento da criação da política de referência, mas uma política referida pode ser excluída mesmo que outras políticas estejam se referindo a ela. Esse recurso permite que diferentes especialistas no assunto trabalhem independentemente um do outro. Você obtém grande flexibilidade ao permitir que diferentes especialistas de diferentes domínios, como rede, armazenamento, segurança, servidor e virtualização, trabalhem juntos para realizar uma tarefa complexa.
- **Resolução da política.** No Cisco UCS Manager, você pode criar uma estrutura em árvore de hierarquia de unidades organizacionais que imita os inquilinos da vida real e os relacionamentos organizacionais. Você pode definir várias políticas, pools e modelos em diferentes níveis da hierarquia organizacional. Uma política que se refere a outra política por nome é resolvida na hierarquia organizacional com a correspondência de política mais próxima. Se nenhuma política com um nome específico for encontrada na hierarquia da organização raiz, uma política especial chamada "padrão" será pesquisada. Essa prática de resolução de políticas permite APIs de gerenciamento amigáveis à automação e oferece grande flexibilidade aos proprietários das diferentes organizações.
- **Perfis de serviço e computação sem estado.** Um perfil de serviço é uma representação lógica de um servidor, carregando suas várias identidades e políticas. Você pode atribuir esse servidor lógico a qualquer recurso de computação física, desde que ele atenda aos requisitos de recursos. A computação sem estado permite a aquisição de um servidor em poucos minutos, o que costumava levar dias em sistemas de gerenciamento de servidores legados.
- **Suporte de multitenancy incorporado.** A combinação de políticas, pools, modelos, uma integridade referencial solta, resolução de políticas na hierarquia organizacional e uma abordagem baseada em perfis de serviço aos recursos de computação tornam o Cisco UCS Manager inerentemente amigável para

ambientes multitenant que normalmente são observados em nuvens privadas e públicas.

- **Memória estendida.** O servidor blade Cisco UCS B200 M5 de classe empresarial amplia os recursos do portfólio do sistema de computação unificada da Cisco em um formato blade de meia largura. O Cisco UCS B200 M5 aproveita o poder das mais recentes CPUs de processador Intel Xeon escaláveis com até 3TB GB de RAM. Esse recurso permite a enorme proporção de VM para servidor físico de que muitas implantações precisam ou permite que certas arquiteturas suportem operações de memória grande, como big data.
- **Rede ciente da virtualização.** A tecnologia Cisco Virtual Machine Fabric Extender (VM-FEX) torna a camada de rede de acesso ciente da virtualização de host. Essa conscientização impede a poluição dos domínios de computação e rede com a virtualização quando uma rede virtual é gerenciada por perfis de porta definidos pela equipe de administrador de rede. A VM-FEX também descarrega a CPU do hipervisor executando a comutação no hardware, permitindo assim que a CPU do hipervisor execute mais tarefas relacionadas à virtualização. Para simplificar o gerenciamento da nuvem, a tecnologia VM-FEX está bem integrada com VMware vCenter, Linux Kernel-Based Virtual Machine (KVM) e Microsoft Hyper-V SR-IOV.
- **QoS simplificado.** Mesmo que FC e Ethernet sejam convergentes no Cisco UCS, o suporte integrado para QoS e Ethernet sem perda torna isso otimizado. Ao representar todas as classes de sistema em um painel GUI, a QoS de rede é simplificada no Gerenciador Cisco UCS.

Switches Cisco Nexus IP e MDS

Os switches Cisco Nexus e os diretores multicamadas Cisco MDS oferecem conetividade de classe empresarial e consolidação de SAN. A rede de storage multiprotocolo da Cisco ajuda a reduzir o risco de seus negócios fornecendo flexibilidade e opções: FC, conexão de fibra (FICON), FC sobre Ethernet (FCoE), iSCSI e FC sobre IP (FCIP).

Os switches Cisco Nexus oferecem um dos conjuntos de recursos de rede de data center mais abrangentes em uma única plataforma. Eles oferecem alto desempenho e densidade para o data center e o núcleo do campus. Eles também oferecem um conjunto completo de recursos para implantações de agregação de data center, de fim de linha e de interconexão de data center em uma plataforma modular altamente resiliente.

O Cisco UCS integra recursos de computação com os switches Cisco Nexus e uma malha unificada que identifica e manipula diferentes tipos de tráfego de rede. Esse tráfego inclui e/S de armazenamento, tráfego de desktop transmitido, gerenciamento e acesso a aplicativos clínicos e empresariais. Você obtém os seguintes recursos:

- **Escalabilidade de infraestrutura.** Virtualização, energia e refrigeração eficientes, escala de nuvem com automação, alta densidade e desempenho, tudo isso dá suporte ao crescimento eficiente do data center.
- **Continuidade operacional.** O design integra hardware, recursos de software Cisco NX-os e gerenciamento para dar suporte a ambientes sem inatividade.
- * Flexibilidade de transporte. * Você pode adotar novas tecnologias de rede de forma incremental com essa solução econômica.

Juntos, o Cisco UCS com switches Cisco Nexus e diretores multicamadas MDS fornecem uma solução de computação, rede e conetividade SAN para um sistema de imagem médica empresarial.

Storage all-flash NetApp

O storage da NetApp que executa o software ONTAP reduz os custos gerais de storage, além de fornecer tempos de resposta de leitura e gravação de baixa latência e IOPS alto de que os workloads do sistema de imagem médica precisam. Para criar um sistema de storage ideal que atenda aos requisitos típicos do sistema de imagem médica, o ONTAP oferece suporte a configurações de storage all-flash e híbrido. O storage flash da NetApp oferece aos clientes do sistema de imagem médica, como você, os principais componentes da alta performance e capacidade de resposta, para dar suporte às operações do sistema de imagem médica

sensível à latência. Ao criar vários domínios de falha em um único cluster, a tecnologia NetApp também pode isolar seus ambientes de produção de ambientes que não sejam de produção. E, ao garantir que a performance do sistema não fique abaixo de um determinado nível para workloads com QoS mínima do ONTAP, o NetApp reduz os problemas de performance do sistema.

A arquitetura com escalabilidade horizontal do software ONTAP pode se adaptar com flexibilidade aos vários workloads de e/S. Para fornecer a taxa de transferência necessária e a baixa latência de que os aplicativos clínicos precisam e para fornecer uma arquitetura modular com escalabilidade horizontal, as configurações all-flash geralmente são usadas em arquiteturas ONTAP. Os nós de NetApp AFF podem ser combinados no mesmo cluster de escalabilidade horizontal com nós de storage híbrido (HDD e flash), adequados para armazenar grandes conjuntos de dados com alta taxa de transferência. Você pode clonar, replicar e fazer backup do ambiente do seu sistema de imagem médica, desde o armazenamento SSD caro até o armazenamento HDD mais econômico em outros nós. Com o storage habilitado para nuvem da NetApp e um Data Fabric fornecido pela NetApp, você pode fazer backup no storage de objetos no local ou na nuvem.

Para imagens médicas, o ONTAP foi validado pela maioria dos principais sistemas de imagens médicas. Isso significa que foi testado para oferecer desempenho rápido e confiável para imagens médicas. Além disso, os recursos a seguir simplificam o gerenciamento, aumentam a disponibilidade e a automação e reduzem a quantidade total de storage de que você precisa.

- * Desempenho excecional. * A solução NetApp AFF compartilha a mesma arquitetura de storage unificada, o software ONTAP, a interface de gerenciamento, os serviços de rich data e o conjunto avançado de recursos das demais famílias de produtos NetApp FAS. Essa combinação inovadora de Mídia all-flash com o ONTAP oferece a baixa latência consistente e IOPS alto do storage all-flash com o software ONTAP líder do setor.
- **Eficiência de armazenamento.** Você pode reduzir seus requisitos de capacidade total trabalhar com seu NetApp SME para entender como isso aplicou seu sistema de imagem médica específico.
- **Clonagem eficiente em espaço.** Com a funcionalidade FlexClone, seu sistema pode criar clones quase instantaneamente para dar suporte à atualização do ambiente de backup e teste. Esses clones consomem storage adicional apenas quando são feitas alterações.
- **Proteção de dados integrada.** Os recursos completos de proteção de dados e recuperação de desastres ajudam você a proteger seus ativos de dados essenciais e fornecer recuperação de desastres.
- **Operações ininterruptas.** Você pode realizar atualizações e manutenção sem colocar os dados offline.
- **QoS.** A QoS de storage ajuda a limitar possíveis workloads de bully. Mais importante ainda, a QoS cria uma garantia de desempenho mínima de que o desempenho do sistema não ficará abaixo de um certo nível para workloads críticos, como o ambiente de produção de um sistema de imagem médica. E, ao limitar a contenção, a QoS do NetApp também pode reduzir problemas relacionados ao desempenho.
- **Data Fabric.** Para acelerar a transformação digital, o Data Fabric da NetApp simplifica e integra o gerenciamento de dados em ambientes na nuvem e no local. Ele fornece aplicações e serviços de gerenciamento de dados consistentes e integrados para obter insights e visibilidade de dados superiores, acesso, controle, proteção e segurança de dados. O NetApp é integrado a grandes nuvens públicas, como AWS, Azure, Google Cloud e IBM Cloud, oferecendo uma ampla variedade de opções.

Virtualização de host: VMware vSphere

As arquiteturas FlexPod são validadas com o VMware vSphere 6.x, que é a plataforma de virtualização líder do setor. O VMware ESXi 6.x é usado para implantar e executar as VMs. O vCenter Server Appliance 6.x é usado para gerenciar os hosts e as VMs ESXi. Vários hosts ESXi executados em blades do Cisco UCS B200 M5 são usados para formar um cluster VMware ESXi. O cluster do VMware ESXi agrupa os recursos de computação, memória e rede de todos os nós de cluster e fornece uma plataforma resiliente para as VMs em execução no cluster. Os recursos do cluster VMware ESXi, a alta disponibilidade do vSphere e o DRS (Distributed Resource Scheduler) contribuem para a tolerância do cluster vSphere para suportar falhas e

ajudam a distribuir os recursos pelos hosts do VMware ESXi.

O plug-in de storage do NetApp e o plug-in do Cisco UCS se integram ao VMware vCenter para permitir workflows operacionais para os recursos de storage e computação necessários.

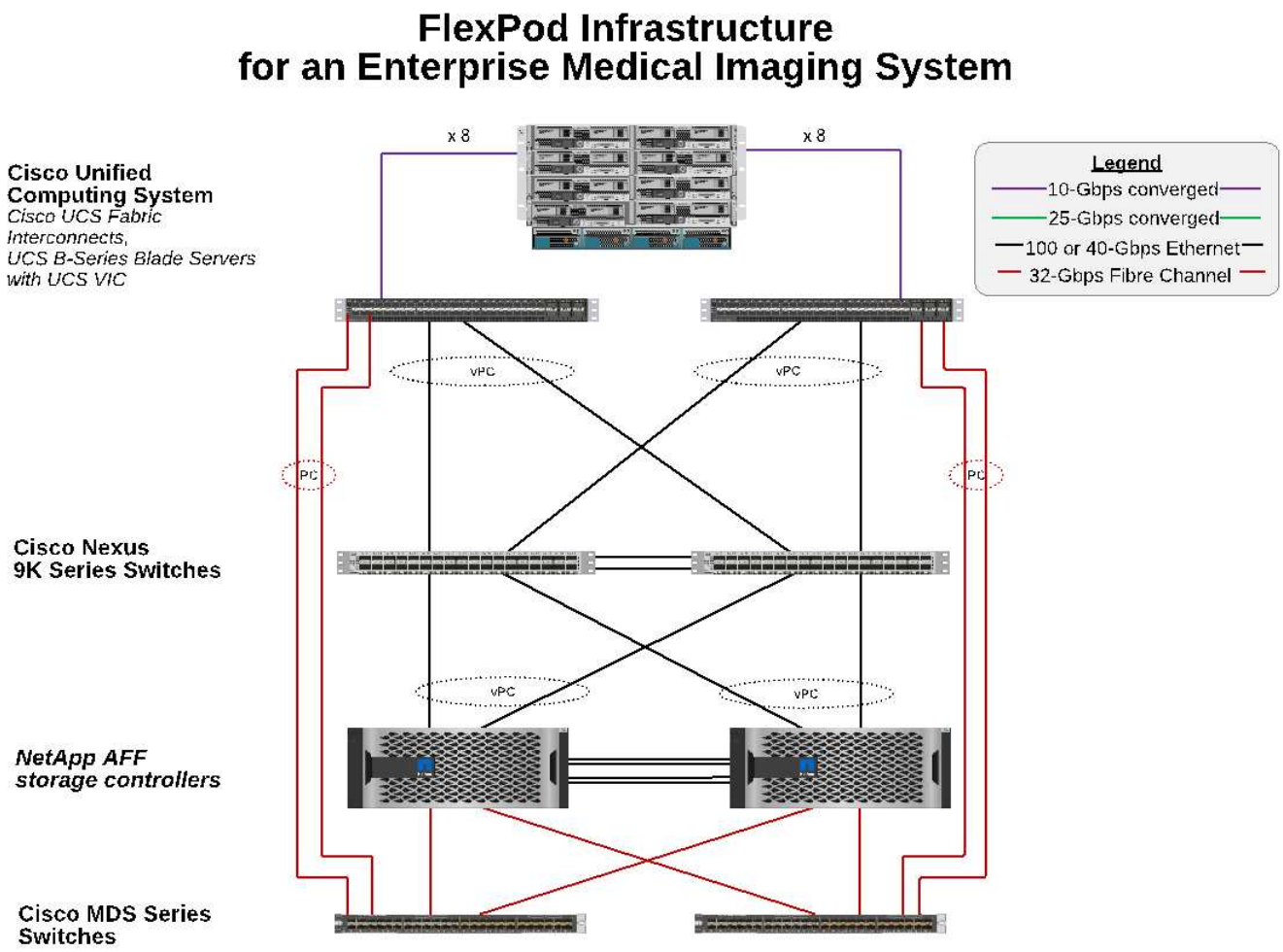
O cluster VMware ESXi e o vCenter Server oferecem uma plataforma centralizada para a implantação de ambientes de imagem médica em VMs. Sua organização de saúde pode obter todos os benefícios de uma infraestrutura virtual líder do setor com confiança, como o seguinte:

- * Implantação simples.* Implante o vCenter Server com rapidez e facilidade usando um dispositivo virtual.
- * Controle centralizado e visibilidade.* Administrar toda a infraestrutura do vSphere a partir de um único local.
- **Otimização proativa.** Aloque, otimize e migre recursos para eficiência máxima.
- **Gestão.** Use poderosos plug-ins e ferramentas para simplificar o gerenciamento e estender o controle.

Arquitetura

A arquitetura do FlexPod foi projetada para fornecer alta disponibilidade se um componente ou um link falhar em toda a sua pilha de computação, rede e storage. Vários caminhos de rede para acesso ao cliente e acesso ao storage fornecem balanceamento de carga e utilização ideal de recursos.

A figura a seguir ilustra a topologia Ethernet de 16GB GB/40GB GB (40GbE) para a implantação da solução de sistema de imagem médica.



Arquitetura de storage

Use as diretrizes de arquitetura de armazenamento nesta seção para configurar sua infraestrutura de armazenamento para um sistema de imagiologia médica empresarial.

Camadas de storage

Um ambiente de imagem médica empresarial típico consiste em várias camadas de armazenamento diferentes. Cada camada tem requisitos específicos de protocolo de storage e desempenho. O armazenamento NetApp suporta várias tecnologias RAID; mais informações podem ser encontradas "aqui". Veja como os sistemas de storage da NetApp AFF atendem às necessidades de diferentes camadas de storage para o sistema de geração de imagens:

- **Armazenamento de desempenho (camada 1).** Esse nível oferece alto desempenho e alta redundância para bancos de dados, unidades de sistema operacional, armazenamentos de dados do VMware Virtual Machine File System (VMFS) e assim por diante. A e/S de bloco passa pela fibra para uma matriz de armazenamento compartilhado de SSD, conforme configurado no ONTAP. A latência mínima é de 1ms a 3ms ms, com um pico ocasional de 5ms ms. Esta camada de armazenamento é normalmente utilizada para cache de armazenamento a curto prazo, normalmente de 6 a 12 meses de armazenamento de imagens para acesso rápido a imagens DICOM online. Esse nível oferece alto desempenho e alta redundância para caches de imagens, backup de banco de dados e assim por diante. Os all-flash arrays NetApp fornecem latência inferior a 1ms ms em uma largura de banda contínua, o que é muito menor do que os tempos de serviço esperados por um ambiente típico de imagiologia médica empresarial. O

NetApp ONTAP é compatível com RAID-TEC (RAID de paridade tripla para sustentar três falhas de disco) e RAID DP (RAID de paridade dupla para sustentar duas falhas de disco).

- **Armazenamento de arquivos (nível 2).** Esse nível é usado para acesso típico a arquivos com custo otimizado, armazenamento RAID 5 ou RAID 6 para volumes maiores e arquivamento de longo prazo com custo/desempenho mais baixo. O NetApp ONTAP é compatível com RAID-TEC (RAID de paridade tripla para sustentar três falhas de disco) e RAID DP (RAID de paridade dupla para sustentar duas falhas de disco). O NetApp FAS in FlexPod permite a geração de imagens de e/S de aplicações em NFS/SMB para um array de disco SAS. Os sistemas NetApp FAS fornecem latência de cerca de 10ms ms com largura de banda contínua, o que é muito menor do que os tempos de serviço esperados para a categoria de storage 2 em um ambiente de sistema de imagiologia médica empresarial.

O arquivamento baseado em nuvem em um ambiente de nuvem híbrida pode ser usado para arquivamento em um provedor de storage de nuvem pública usando S3 ou protocolos semelhantes. A tecnologia NetApp SnapMirror permite a replicação de dados de imagem de matrizes all-flash ou FAS para matrizes de armazenamento mais lentas baseadas em disco ou para o Cloud Volumes ONTAP para AWS, Azure ou Google Cloud.

A NetApp SnapMirror oferece funcionalidades de replicação de dados líderes do setor que ajudam a proteger o seu sistema de imagiologia médica com replicação de dados unificada. Simplifique o gerenciamento de proteção de dados no Data Fabric com replicação entre plataformas, do flash ao disco e à nuvem:

- Transportar dados de forma otimizada e eficiente entre os sistemas de storage da NetApp para dar suporte a backup e recuperação de desastres com o mesmo volume de destino e fluxo de e/S.
- Failover para qualquer volume secundário. Fazer recuperação de qualquer Snapshot pontual no storage secundário.
- Proteger seus workloads mais críticos com a replicação síncrona sem perda de dados (RPO igual a 0).
- Cortar o tráfego de rede. Reduzir o espaço físico do storage por meio de operações eficientes.
- Reduza o tráfego de rede transportando apenas blocos de dados alterados.
- Preserve os benefícios de eficiência de storage no storage primário durante o transporte, incluindo deduplicação, compressão e compactação.
- Forneça eficiências in-line adicionais com compactação de rede.

Mais informações podem ser "aqui"encontradas .

A tabela abaixo lista cada nível que um sistema de imagiologia médica típico requer para latência específica e as caraterísticas de desempenho de rendimento.

Camada de storage	Requisitos	Recomendação da NetApp
1	Taxa de transferência de 1 a 5ms ms de latência de 35 a 500MBps Gbps	O AFF com um par de alta disponibilidade (HA) AFF A300 de latência inferior a 1ms ms com dois compartimentos de disco pode lidar com uma taxa de transferência de até 1,6GBps Gbps
2	Arquivamento no local	FAS com latência de até 30ms ms
	Arquivamento na nuvem	Replicação do SnapMirror para Cloud Volumes ONTAP ou arquivamento de backup com o software NetApp StorageGRID

Conetividade de rede de storage

FC Fabric

- O FC Fabric destina-se à e/S de sistema operacional do host, desde a computação até o storage.
- Duas malhas FC (malha A e malha B) são conectadas à malha A do Cisco UCS e à malha B, respetivamente.
- Uma máquina virtual de storage (SVM) com duas interfaces lógicas FC (LIFs) está em cada nó da controladora. Em cada nó, um LIF é conectado à malha A e o outro é conetado à malha B..
- A conectividade de ponta a ponta com FC de 16Gbps GB é feita por meio dos switches Cisco MDS. Um único iniciador, várias portas de destino e zoneamento são todos configurados.
- A inicialização FC SAN é usada para criar computação totalmente sem estado. Os servidores são inicializados a partir de LUNs no volume de arranque que está alojado no cluster de armazenamento AFF.

Rede IP para acesso ao storage por iSCSI, NFS e SMB/CIFS

- Duas LIFs iSCSI estão na SVM em cada nó da controladora. Em cada nó, um LIF é conectado à malha A e o segundo é conectado à malha B..
- Duas LIFs de dados nas estão na SVM em cada nó da controladora. Em cada nó, um LIF é conectado à malha A e o segundo é conectado à malha B..
- Grupos de interface de porta de armazenamento (canal de porta virtual [VPC]) para o link 10Gbps para o switch N9k-A e para o link 10Gbps para o switch N9k-B.
- Carga de trabalho em sistemas de arquivos EXT4 ou NTFS da VM para o armazenamento:
  - Protocolo iSCSI sobre IP.
- VMs hospedadas no armazenamento de dados NFS:
  - A e/S de VM os passa por vários caminhos Ethernet por meio de switches Nexus.

Gestão na banda (ligação ativo-passivo)

- 1Gbps link para o switch de gerenciamento N9k-A e 1Gbps link para o switch de gerenciamento N9k-B.

Backup e recuperação

O data center FlexPod foi desenvolvido em um storage array gerenciado pelo software de gerenciamento de dados NetApp ONTAP. O software ONTAP evoluiu ao longo de 20 anos para fornecer muitos recursos de gerenciamento de dados para VMs, bancos de dados Oracle, compartilhamentos de arquivos SMB/CIFS e NFS. Ele também fornece tecnologia de proteção, como a tecnologia NetApp Snapshot, a tecnologia SnapMirror e a tecnologia de replicação de dados NetApp FlexClone. O software NetApp SnapCenter tem um servidor e um cliente de GUI para usar os recursos ONTAP Snapshot, SnapRestore e FlexClone para VM, compartilhamentos de arquivos SMB/CIFS, backup e recuperação de banco de dados NFS e Oracle.

O software NetApp SnapCenter emprega "patenteado" a tecnologia Snapshot para criar um backup de uma VM inteira ou banco de dados Oracle em um volume de storage NetApp instantaneamente. Em comparação com o Oracle Recovery Manager (RMAN), as cópias Snapshot não exigem uma cópia de backup de linha de base completa, porque não são armazenadas como cópias físicas de blocos. Cópias snapshot são armazenadas como ponteiros para os blocos de armazenamento como existiam no sistema de arquivos ONTAP WAFL quando as cópias snapshot foram criadas. Devido a essa estreita relação física, as cópias Snapshot são mantidas no mesmo storage array que os dados originais. As cópias snapshot também podem ser criadas no nível do arquivo para ter controle mais granular do backup.

A tecnologia Snapshot é baseada em uma técnica de redirecionamento em gravação. Ele inicialmente contém apenas ponteiros de metadados e não consome muito espaço até que os primeiros dados mudem para um bloco de armazenamento. Se um bloco existente for bloqueado por uma cópia Snapshot, um novo bloco será gravado pelo sistema de arquivos ONTAP WAFL como uma cópia ativa. Essa abordagem evita as gravações duplas que ocorrem com a técnica de mudança na gravação.

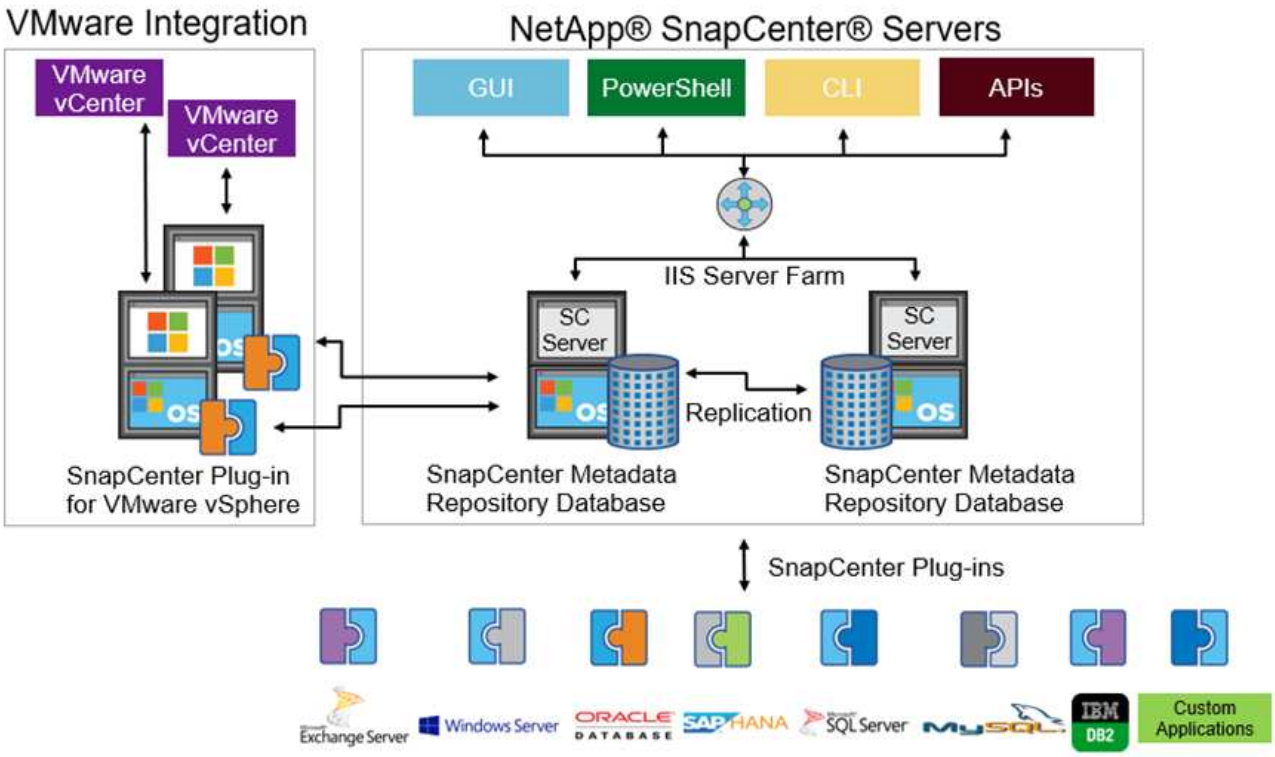
Para o backup do banco de dados Oracle, as cópias Snapshot geram uma economia de tempo incrível. Por exemplo, um backup que levou 26 horas para ser concluído usando o RMAN sozinho pode levar menos de 2 minutos para ser concluído usando o software SnapCenter.

E como a restauração de dados não copia nenhum bloco de dados, mas, em vez disso, vira os ponteiros para as imagens de bloco Snapshot consistentes com o aplicativo quando a cópia Snapshot foi criada, uma cópia de backup Snapshot pode ser restaurada quase instantaneamente. A clonagem do SnapCenter cria uma cópia separada de ponteiros de metadados para uma cópia Snapshot existente e monta a nova cópia em um host de destino. Esse processo também é rápido e eficiente em armazenamento.

A tabela a seguir resume as principais diferenças entre o Oracle RMAN e o software NetApp SnapCenter.

	Backup	**Restaurar**	**Clone**	**Precisa de backup completo**	**Utilização de espaço**	**Cópia externa**
RMAN	Lento	Lento	Lento	Sim	Alta	Sim
SnapCenter	Rápido	Rápido	Rápido	Não	Baixo	Sim

A figura a seguir apresenta a arquitetura SnapCenter.



As configurações do NetApp MetroCluster são usadas por milhares de empresas em todo o mundo para alta disponibilidade (HA), sem perda de dados e operações ininterruptas dentro e fora do data center. O

MetroCluster é um recurso gratuito do software ONTAP que espelha de forma síncrona os dados e a configuração entre dois clusters ONTAP em locais separados ou domínios de falha. O MetroCluster fornece storage disponível continuamente para aplicações ao lidar automaticamente com dois objetivos: Objetivo de ponto de restauração (RPO) sem espelhamento síncrono de dados gravados no cluster. Objetivo de tempo de recuperação quase zero (rto) espelhando a configuração e automatizando o acesso aos dados no segundo local, o MetroCluster oferece simplicidade com o espelhamento automático de dados e a configuração entre os dois clusters independentes localizados nos dois locais. À medida que o storage é provisionado em um cluster, ele é espelhado automaticamente para o segundo cluster no segundo local. A tecnologia NetApp SyncMirror fornece uma cópia completa de todos os dados com RPO zero. , Portanto, as cargas de trabalho de um local podem alternar a qualquer momento para o local oposto e continuar fornecendo dados sem perda de dados. Mais informações podem ser "aqui"encontradas .

Rede

Um par de switches Cisco Nexus fornece caminhos redundantes para o tráfego IP da computação para o armazenamento e para clientes externos do visualizador de imagens do sistema de imagem médica:

- A agregação de links que usa canais de porta e VPCs é empregada em toda parte, permitindo o design para maior largura de banda e alta disponibilidade:
  - A VPC é usada entre o storage array do NetApp e os switches Cisco Nexus.
  - A VPC é usada entre a interconexão de malha do Cisco UCS e os switches Cisco Nexus.
  - Cada servidor tem placas de interface de rede virtual (vNICs) com conetividade redundante à malha unificada. O failover de NIC é usado entre interconexões de malha para redundância.
  - Cada servidor tem adaptadores de barramento de host virtual (vHBAs) com conetividade redundante à malha unificada.
- As interconexões de malha Cisco UCS são configuradas no modo de host final, conforme recomendado, proporcionando pinçamento dinâmico de vNICs a switches uplink.
- Uma rede de storage FC é fornecida por um par de switches MDS Cisco.

Computação: Sistema de computação unificada da Cisco

Duas telas Cisco UCS através de diferentes interconexões de malha fornecem dois domínios de falha. Cada malha é conectada a switches de rede IP e a diferentes switches de rede FC.

Perfis de serviço idênticos para cada blade Cisco UCS são criados de acordo com as práticas recomendadas do FlexPod para executar o VMware ESXi. Cada perfil de serviço deve ter os seguintes componentes:

- Dois vNICs (um em cada malha) para transportar NFS, SMB/CIFS e tráfego de cliente ou gerenciamento
- VLANs necessárias adicionais aos vNICs para NFS, SMB/CIFS e tráfego de cliente ou gerenciamento
- Dois vNICs (um em cada malha) para transportar tráfego iSCSI
- Dois HBAs FC de storage (um em cada malha) para tráfego FC para storage
- Inicialização de SAN

Virtualização

O cluster de host do VMware ESXi executa VMs de workload. O cluster compreende instâncias ESXi executadas em servidores blade Cisco UCS.

Cada host ESXi inclui os seguintes componentes de rede:

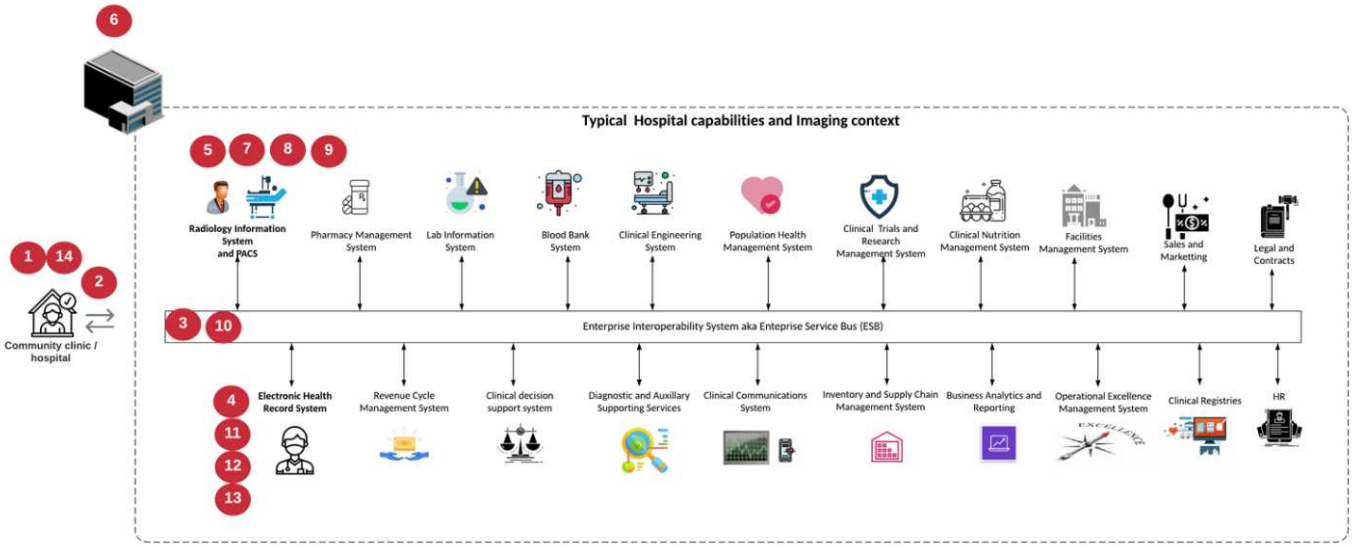
- Inicialização SAN em FC ou iSCSI
- Inicializar LUNs no armazenamento NetApp (em um FlexVol dedicado para SO de inicialização)
- Dois vmnics (Cisco UCS vNIC) para NFS, SMB/CIFS ou tráfego de gerenciamento
- Dois HBAs de storage (Cisco UCS FC vHBA) para tráfego FC para storage
- Switch padrão ou switch virtual distribuído (conforme necessário)
- Armazenamento de dados NFS para VMs de workload
- Gerenciamento, rede de tráfego de clientes e grupos de portas de rede de armazenamento para VMs
- Adaptador de rede para gerenciamento, tráfego de clientes e acesso ao storage (NFS, iSCSI ou SMB/CIFS) para cada VM
- VMware DRS ativado
- Multipathing nativo habilitado para caminhos FC ou iSCSI para armazenamento
- Snapshots VMware para VM desativados
- O NetApp SnapCenter implantou para backups de VMs VMware

Arquitetura do sistema de imagem médica

Nas organizações de saúde, os sistemas de imagem médica são aplicações críticas e bem integrados nos fluxos de trabalho clínicos que começam com o Registro do paciente e terminam com atividades relacionadas ao faturamento no ciclo de receita.

O diagrama a seguir mostra os vários sistemas envolvidos em um hospital típico de grande porte; este diagrama destina-se a fornecer contexto arquitetônico a um sistema de imagem médica antes de ampliarmos os componentes arquitetônicos de um sistema de imagem médica típico. Os fluxos de trabalho variam amplamente e são hospitalares e específicos para casos de uso.

A figura abaixo mostra o sistema de imagem médica no contexto de um paciente, uma clínica comunitária e um grande hospital.



1. O paciente visita a clínica comunitária com sintomas. Durante a consulta, o médico da comunidade coloca uma ordem de imagem que é enviada para o hospital maior sob a forma de uma mensagem de ordem de HL7.

2. O sistema EHR do médico comunitário envia a mensagem de pedido/ORD HL7 para o hospital de grande porte.
3. O sistema de interoperabilidade empresarial (também conhecido como Enterprise Service Bus [ESB]) processa a mensagem de encomenda e envia a mensagem de encomenda para o sistema EHR.
4. A EHR processa a mensagem de encomenda. Se não existir um registo de paciente, é criado um novo registo de paciente.
5. A EHR envia uma ordem de imagiologia para o sistema de imagiologia médica.
6. O paciente liga para o hospital grande para uma consulta por imagem.
7. A receção de imagens e o balcão de registo programam o paciente para uma consulta de imagiologia utilizando uma informação radiológica ou um sistema semelhante.
8. O paciente chega para a consulta de imagiologia e as imagens ou o vídeo são criados e enviados para o PACS.
9. O radiologista lê as imagens e anota as imagens no PACS utilizando um visualizador de diagnóstico avançado/compatível com gráficos GPU. Certos sistemas de imagem têm capacidades de melhoria de eficiência habilitadas por inteligência artificial (IA) incorporadas nos fluxos de trabalho de imagem.
10. Os resultados da encomenda de imagens são enviados para a EHR na forma de uma mensagem ORU de resultados de encomenda HL7 através da ESB.
11. A EHR processa os resultados da encomenda no registo do paciente, coloca a imagem em miniatura com uma ligação sensível ao contexto à imagem DICOM real. Os médicos podem iniciar o visualizador de diagnóstico se for necessária uma imagem de resolução mais elevada a partir da EHR.
12. O médico revê a imagem e insere as notas do médico no registo do paciente. O médico poderia usar o sistema de apoio à decisão clínica para melhorar o processo de revisão e auxiliar no diagnóstico adequado para o paciente.
13. Em seguida, o sistema EHR envia os resultados da encomenda na forma de uma mensagem de resultados da encomenda para o hospital comunitário. Neste ponto, se o hospital comunitário puder receber a imagem completa, a imagem é enviada através de WADO ou DICOM.
14. O médico comunitário conclui o diagnóstico e fornece os próximos passos ao paciente.

Um sistema de imagiologia médica típico utiliza uma arquitetura N-Layered. O componente principal de um sistema de imagem médica é um servidor de aplicativos para hospedar vários componentes de aplicativos. Os servidores de aplicativos típicos são baseados em Java runtime ou baseados em C no .Net CLR. A maioria das soluções de imagiologia médica empresarial utiliza um banco de dados Oracle Server ou MS SQL Server ou Sybase como base de dados principal. Além disso, alguns sistemas de imagem médica corporativos também usam bancos de dados para aceleração de conteúdo e armazenamento em cache em uma região geográfica. Alguns sistemas de imagiologia médica empresarial também usam bancos de dados NoSQL como MongoDB, Redis e assim por diante em conjunto com servidores de integração empresarial para interfaces DICOM e APIs.

Um sistema de imagiologia médica típico fornece acesso a imagens para dois conjuntos distintos de utilizadores: Utilizador de diagnóstico/radiologista ou médico que encomendou a imagiologia.

Os radiologistas geralmente usam visualizadores de diagnóstico habilitados para gráficos avançados que estão sendo executados em estações de trabalho de computação e gráficos de alta qualidade físicas ou parte de uma infraestrutura de desktop virtual. Se você estiver prestes a iniciar sua jornada de infraestrutura de desktop virtual, mais informações poderão ser encontradas "aqui".

Quando o furacão Katrina destruiu dois dos principais hospitais de ensino da Louisiana, os líderes se reuniram e construíram um sistema de Registro eletrônico resiliente de saúde que incluía mais de 3000 desktops virtuais em tempo recorde. Mais informações sobre arquitetura de referência de casos de uso e pacotes de

referência do FlexPod podem ser "aqui"encontradas .

Os médicos acessam imagens de duas maneiras principais:

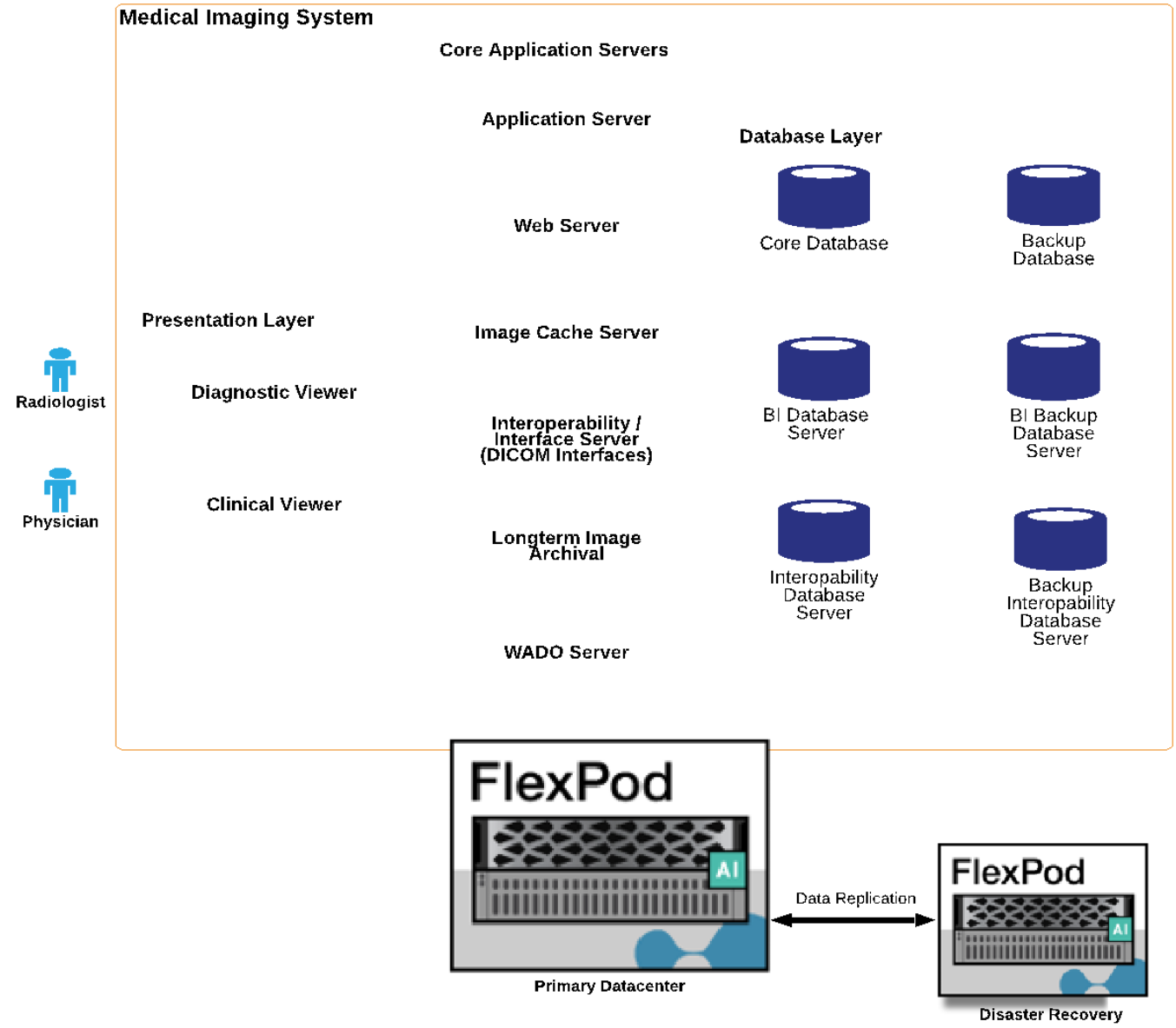
- * Acesso baseado na Web.* que é normalmente usado por sistemas EHR para incorporar imagens PACS como links sensíveis ao contexto no Registro médico eletrônico (EMR) do paciente e links que podem ser colocados em fluxos de trabalho de imagem, fluxos de trabalho de procedimentos, fluxos de trabalho de notas de progresso e assim por diante. Os links baseados na Web também são usados para fornecer acesso à imagem aos pacientes através dos portais de pacientes. O acesso baseado na Web usa um padrão de tecnologia chamado links sensíveis ao contexto. Os links sensíveis ao contexto podem ser links/URIs estáticos para o suporte DICOM diretamente ou links/URIs gerados dinamicamente usando macros personalizadas.
- **Cliente grosso.** Alguns sistemas médicos corporativos também permitem que você use uma abordagem grossa baseada no cliente para visualizar as imagens. Você pode iniciar um cliente thick a partir do EMR do paciente ou como um aplicativo autônomo.

O sistema de imagem médica pode fornecer acesso à imagem a uma comunidade de médicos ou a médicos participantes da NIC. Os sistemas de imagem médica típicos incluem componentes que permitem a interoperabilidade da imagem com outros sistemas DE TI DE saúde dentro e fora da sua organização de saúde. Os médicos comunitários podem acessar imagens através de um aplicativo baseado na Web ou aproveitar uma plataforma de troca de imagens para interoperabilidade de imagens. As plataformas de troca de imagens utilizam normalmente WADO ou DICOM como o protocolo de troca de imagens subjacente.

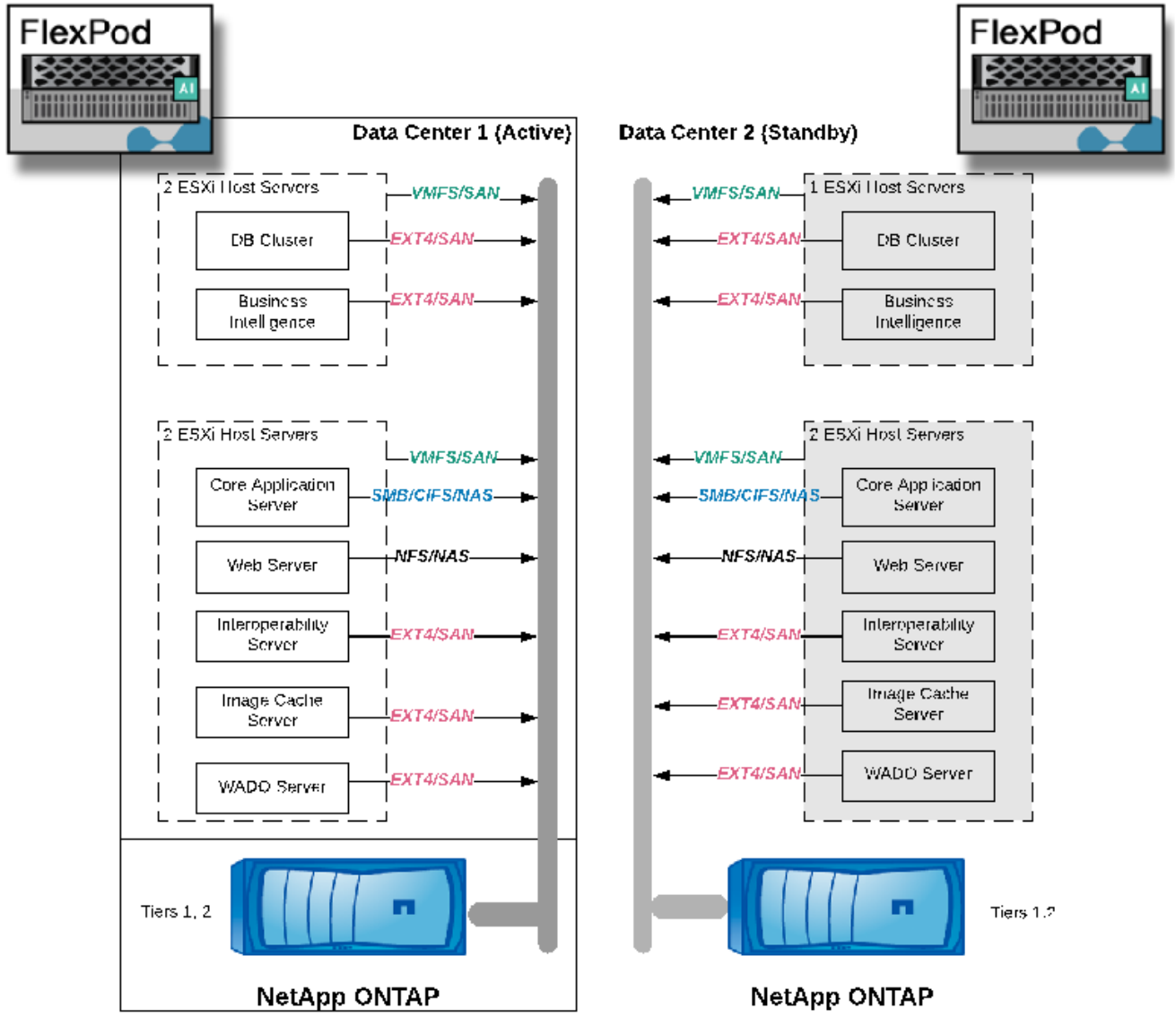
Os sistemas de imagiologia médica também podem suportar centros médicos académicos que necessitam de PACS ou sistemas de imagiologia para utilização numa sala de aula. Para apoiar atividades acadêmicas, um sistema de imagem médica típico pode ter as capacidades de um sistema PACS em uma pegada menor ou em um ambiente de imagem somente ensino. Os sistemas de arquivamento neutros e alguns sistemas de imagiologia médica de classe empresarial oferecem capacidades de morphing de etiquetas de imagem DICOM para anonimizar as imagens que são utilizadas para fins de ensino. A tag morphing permite que a organização de saúde troque imagens DICOM entre diferentes sistemas de imagem médica de fornecedores de forma neutra em termos de fornecedor. Além disso, a tag morphing permite que os sistemas de imagem médica implementem uma capacidade de arquivamento neutra para imagens médicas em toda a empresa.

Os sistemas de imagiologia médica estão a começar a utilizar "Recursos de computação baseados em GPU" para melhorar os fluxos de trabalho humanos através do pré-processamento das imagens e, assim, melhorar a eficiência. Os sistemas típicos de imagiologia médica empresarial aproveitam as funcionalidades de eficiência de storage da NetApp líderes do setor. Os sistemas de imagiologia médica empresarial normalmente utilizam o RMAN para atividades de backup, recuperação e restauração. Para melhor performance e reduzir o tempo necessário para criar backups, a tecnologia Snapshot está disponível para operações de backup e a tecnologia SnapMirror está disponível para replicação.

A figura abaixo mostra os componentes lógicos da aplicação numa vista arquitetónica em camadas.



A figura abaixo mostra os componentes físicos da aplicação.



Os componentes da aplicação lógica exigem que a infraestrutura dê suporte a um conjunto diversificado de protocolos e sistemas de arquivos. O software NetApp ONTAP é compatível com um conjunto líder do setor de protocolos e sistemas de arquivos.

A tabela abaixo lista os componentes do aplicativo, o protocolo de armazenamento e os requisitos do sistema de arquivos.

Componente de aplicação	SAN/NAS	Tipo de sistema de ficheiros	Camada de storage	Tipo de replicação
Banco de dados de produtos de host VMware	local	SAN	VMFS	Categoria 1
Aplicação	Banco de dados de produtos de host VMware	REP	SAN	VMFS

Componente de aplicação	SAN/NAS	Tipo de sistema de ficheiros	Camada de storage	Tipo de replicação
Categoria 1	Aplicação	Aplicação de produtos de host VMware	local	SAN
VMFS	Categoria 1	Aplicação	Aplicação de produtos de host VMware	REP
SAN	VMFS	Categoria 1	Aplicação	Servidor de banco de dados central
SAN	Ext4	Categoria 1	Aplicação	Servidor de banco de dados de backup
SAN	Ext4	Categoria 1	Nenhum	Servidor de cache de imagem
NAS	SMB/CIFS	Categoria 1	Nenhum	Servidor de arquivo
NAS	SMB/CIFS	Categoria 2	Aplicação	Servidor Web
NAS	SMB/CIFS	Categoria 1	Nenhum	WADO Server
SAN	NFS	Categoria 1	Aplicação	Servidor de business intelligence
SAN	NTFS	Categoria 1	Aplicação	Backup de business intelligence
SAN	NTFS	Categoria 1	Aplicação	Servidor de interoperabilidade
SAN	Ext4	Categoria 1	Aplicação	Servidor de banco de dados de interoperabilidade

Componentes de hardware e software da infraestrutura da solução

As tabelas a seguir listam os componentes de hardware e software, respetivamente, da infraestrutura FlexPod para o sistema de imagens médicas.

Camada	Família de produtos	Quantidade e modelo	Detalhes
Computação	Chassi do Cisco UCS 5108	1 ou 2	Com base no número de lâminas necessárias para suportar o número de estudos anuais
	Servidores blade Cisco UCS	B200 M5	Número de blades com base no número de estudos anualmente, cada um com 2 x 20 ou mais núcleos, 2,7GHz e 128-384GB de RAM
	Cartão de interface virtual Cisco UCS (VIC)	Cisco UCS 1440	Consulte
	2 x interconexões de tecido Cisco UCS	6454 ou posterior	–
Rede	Switches Cisco Nexus	2 x Cisco Nexus 3000 Series ou 9000 Series	–
Rede de armazenamento	Rede IP para acesso ao storage por protocolos SMB/CIFS, NFS ou iSCSI	Mesmos switches de rede como acima	–
	Acesso ao storage por FC	2 x Cisco MDS 9132T	–
Armazenamento	Sistema de storage all-flash NetApp AFF A400	1 ou mais par de HA	Cluster com dois ou mais nós
	Compartimento de disco	1 ou mais compartimentos de disco DS224C ou NS224	Totalmente preenchido com 24 unidades
	SSD	>24, 1,2TB ou maior capacidade	–

Software	Família de produtos	Versão ou lançamento	Detalhes
Sistema de imagiologia médica empresarial			
	MS SQL ou Oracle Database Server	Como sugerido pelo fornecedor do sistema de imagem médica	
	Nenhum SQL DBS como o MongoDB Server	Como sugerido pelo fornecedor do sistema de imagem médica	
	Servidores de aplicativos	Como sugerido pelo fornecedor do sistema de imagem médica	
	Servidor de integração (MS BizTalk, MuleSoft, Rhapsody, Tibco)	Como sugerido pelo fornecedor do sistema de imagem médica	
	VMs	Linux (64 bits)	
	VMs	Windows Server (64 bits)	
Armazenamento	ONTAP	ONTAP 9,7 ou posterior	
Rede	Interconexão de malha Cisco UCS	Cisco UCS Manager 4,1 ou posterior	
	Switches Ethernet Cisco	9,2(3)i7(2) ou posterior	
	Cisco FC: Cisco MDS 9132T	8,4(2) ou posterior	
Hipervisor	Hipervisor	VMware vSphere ESXi 6,7 U2 ou posterior	
Gerenciamento	Sistema de gerenciamento de hipervisor	VMware vCenter Server 6,7 U1 (vCSA) ou posterior	
	Console de storage virtual (VSC) do NetApp	VSC 9,7 ou posterior	
	SnapCenter	SnapCenter 4,3 ou posterior	

Dimensionamento da solução

Dimensionamento do storage

Esta secção descreve o número de estudos e os requisitos de infra-estrutura correspondentes.

Os requisitos de storage listados na tabela a seguir pressupõem que os dados existentes valem 1 ano, mais o crescimento projetado para 1 ano de estudo no sistema primário (camada 1, 2). As necessidades de storage adicionais para crescimento projetado por 3 anos além dos primeiros 2 anos são listadas separadamente.

	Pequeno	Média	Grande
Estudos anuais	Menos de 250K estudos	250k–500K estudos	500K–1 milhões de estudos
Storage de camada 1			
IOPS (média)	1,5K–5K	5K–15K	15K–40K
IOPS (pico)	5K	20K	65K
Taxa de transferência	50–100Mbps	50–150MBps	100–300Mbps
Data center de capacidade 1 (1 ano de dados antigos e 1 ano de novo estudo)	70 TB	140 TB	260 TB
Data center de capacidade 1 (necessidade adicional de 4 anos para novo estudo)	25 TB	45 TB	80 TB
Data center de capacidade 2 (1 ano de dados antigos e 1 ano de novo estudo)	45 TB	110 TB	165 TB
Data center de capacidade 2 (necessidade adicional de 4 anos para novo estudo)	25 TB	45 TB	80 TB
Storage de camada 2			
IOPS (média)	1K	2K	3K
Data center de capacidade 1	320 TB	800 TB	2000 TB

Dimensionamento da computação

A tabela abaixo lista os requisitos de computação para sistemas de imagem médica pequenos, médios e grandes.

	Pequeno	Média	Grande
Estudos anuais	Menos de 250K estudos	250k–500K estudos	500K–1 milhões de estudos
Centro de dados 1			
Número de VMs	21	27	35
Contagem total de CPU virtual (vCPU)	56	124	220
Requisito total de memória	225 GB	450 GB	900 GB

	Pequeno	Média	Grande
Especificações de servidor físico (blades) (suponha 1 vCPU - 1 núcleo)	4 servidores com 20 núcleos e 192GB GB de RAM cada	8 servidores com 20 núcleos e 128GB GB de RAM cada	14 servidores com 20 núcleos e 128GB GB de RAM cada
Centro de dados 2			
Número de VMs	15	17	22
Contagem total de vCPU	42	72	140
Requisito total de memória	179 GB	243 GB	513 GB
Especificações do servidor físico (blades) (suponha que 1 vCPU seja 1 núcleo)	3 servidores com 20 núcleos e 168GB GB de RAM cada	6 servidores com 20 núcleos e 128GB GB de RAM cada	8 servidores com 24 núcleos e 128GB GB de RAM cada

Rede e dimensionamento da infraestrutura do Cisco UCS

A tabela abaixo lista os requisitos de rede e infraestrutura do Cisco UCS para sistemas de imagem médica de pequeno, médio e grande porte.

	Pequeno	Média	Grande
Centro de dados 1			
Número de portas de nó de storage	2 adaptadores de rede convergidos (CNAs); 2 FCS	2 CNAs; 2 FCS	2 CNAs; 2 FCS
Portas de switch de rede IP (Cisco Nexus 9000)	switch de 48 portas	switch de 48 portas	switch de 48 portas
Switch FC (Cisco MDS)	switch de 32 portas	switch de 32 portas	switch de 48 portas
Contagem de chassis do Cisco UCS	1 x 5108	1 x 5108	2 x 5108
Interconexão de malha Cisco UCS	2 x 6332	2 x 6332	2 x 6332
Centro de dados 2			
Contagem de chassis do Cisco UCS	1 x 5108	1 x 5108	1 x 5108
Interconexão de malha Cisco UCS	2 x 6332	2 x 6332	2 x 6332
Número de portas de nó de storage	2 CNAs; 2 FCS	2 CNAs; 2 FCS	2 CNAs; 2 FCS
Portas de switch de rede IP (Cisco Nexus 9000)	switch de 48 portas	switch de 48 portas	switch de 48 portas
Switch FC (Cisco MDS)	switch de 32 portas	switch de 32 portas	switch de 48 portas

Práticas recomendadas

Práticas recomendadas de storage

Alta disponibilidade

O design do cluster de storage do NetApp oferece alta disponibilidade em todos os níveis:

- Nós de cluster
- Conectividade de storage de back-end
- RAID TEC que pode sustentar três falhas de disco
- RAID DP que pode sustentar duas falhas de disco
- Conetividade física a duas redes físicas de cada nó
- Vários caminhos de dados para LUNs e volumes de storage

Alocação segura a vários clientes

As máquinas virtuais de storage (SVMs) da NetApp fornecem uma construção de storage array virtual para separar o domínio de segurança, as políticas e a rede virtual. A NetApp recomenda que você crie SVMs separadas para cada organização de locatário que hospeda dados no cluster de storage.

Práticas recomendadas de storage da NetApp

Considere as práticas recomendadas de storage da NetApp a seguir:

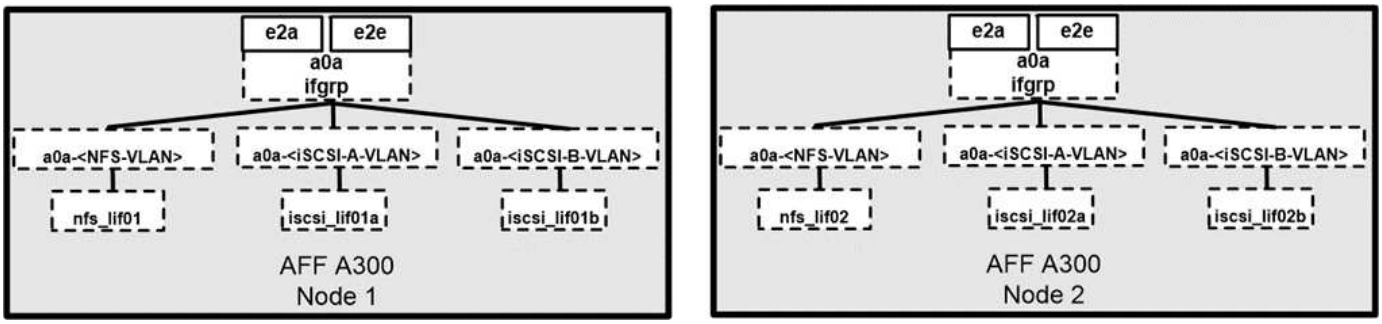
- Sempre ative a tecnologia NetApp AutoSupport, que envia informações resumidas de suporte para o NetApp por meio de HTTPS.
- Para ter o máximo de disponibilidade e mobilidade, certifique-se de que um LIF seja criado para cada SVM em cada nó no cluster do NetApp ONTAP. O acesso por unidade lógica assimétrica (ALUA) é usado para analisar caminhos e identificar caminhos otimizados ativos (diretos) versus caminhos não otimizados ativos. O ALUA é usado tanto para FC ou FCoE quanto para iSCSI.
- Um volume que contém apenas LUNs não precisa ser montado internamente, nem é necessário um caminho de junção.
- Se você usar o CHAP (Challenge-Handshake Authentication Protocol) no ESXi para autenticação de destino, você também deverá configurá-lo no ONTAP. Use a CLI (`vserver iscsi security create`) ou o Gerenciador de sistema do NetApp ONTAP (edite a segurança do iniciador em armazenamento > SVMs > Configurações de SVM > Protocolos > iSCSI).

Inicialização de SAN

A NetApp recomenda que você implemente a inicialização SAN para servidores Cisco UCS na solução de datacenter FlexPod. Esta etapa permite que o sistema operacional seja protegido com segurança pelo sistema de armazenamento NetApp AFF, proporcionando melhor desempenho. O design descrito nesta solução usa inicialização SAN iSCSI.

Na inicialização de SAN iSCSI, cada servidor Cisco UCS recebe dois vNICs iSCSI (um para cada malha SAN), que fornecem conetividade redundante até o armazenamento. As portas de armazenamento neste exemplo, E2A e E2E, que são conetadas aos switches Cisco Nexus, são agrupadas para formar uma porta lógica chamada grupo de interfaces (ifgrp) (neste exemplo, a0a). As VLANs iSCSI são criadas no iggroup e as LIFs iSCSI são criadas em grupos de portas iSCSI (neste exemplo, a0a-<iSCSI-A-VLAN>). O LUN de inicialização iSCSI é exposto aos servidores através do iSCSI LIF usando igrupos. Essa abordagem permite

que apenas o servidor autorizado tenha acesso ao LUN de inicialização. Para o layout de porta e LIF, consulte a figura abaixo.



Ao contrário das interfaces de rede nas, as interfaces de rede SAN não são configuradas para failover durante uma falha. Em vez disso, se uma interface de rede ficar indisponível, o host escolhe um novo caminho otimizado para uma interface de rede disponível. O ALUA, um padrão com suporte do NetApp, fornece informações sobre destinos SCSI, o que permite que um host identifique o melhor caminho para o storage.

Eficiência de storage e thin Provisioning

A NetApp liderou o setor na inovação em eficiência de storage, como a primeira deduplicação para workloads primários e com compactação de dados in-line, o que aprimora a compressão e armazena pequenos arquivos e e/S com eficiência. O ONTAP dá suporte à deduplicação in-line e em segundo plano, bem como à compactação in-line e em segundo plano.

Para obter os benefícios da deduplicação em um ambiente de bloco, os LUNs precisam ser thin Provisioning. Embora o LUN ainda seja visto pelo administrador da VM como tendo a capacidade provisionada, a economia de deduplicação é retornada ao volume a ser usado para outras necessidades. A NetApp recomenda que você implante esses LUNs em volumes FlexVol que também sejam thin Provisioning com uma capacidade duas vezes maior do que o LUN. Quando você implementa o LUN dessa forma, o FlexVol volume atua meramente como uma cota. O storage que o LUN consome é reportado no FlexVol volume e no agregado que contém.

Para obter o máximo de economia de deduplicação, considere agendar deduplicação em segundo plano. No entanto, esses processos usam recursos do sistema quando estão em execução. Portanto, idealmente, você deve programá-los em horários menos ativos (como fins de semana) ou executá-los com mais frequência para reduzir a quantidade de dados alterados a serem processados. A deduplicação automática em segundo plano em sistemas AFF tem muito menos efeito nas atividades de primeiro plano. A compactação em segundo plano (para sistemas baseados em disco rígido) também consome recursos, portanto, você deve considerá-la apenas para workloads secundários com requisitos de desempenho limitados.

Qualidade do serviço

Os sistemas que executam o software ONTAP podem usar o recurso de QoS de storage ONTAP para limitar a taxa de transferência em megabits por segundo (Mbps) e limitar o IOPS para diferentes objetos de storage, como arquivos, LUNs, volumes ou SVMs inteiras. O QoS adaptável é usado para definir um piso de IOPS (mínimo de QoS) e um teto (máximo de QoS), que se ajustam dinamicamente com base na capacidade do datastore e no espaço usado.

Os limites de taxa de transferência são úteis para controlar cargas de trabalho desconhecidas ou de teste antes de uma implantação para confirmar que elas não afetam outras cargas de trabalho. Você também pode usar esses limites para restringir uma carga de trabalho bully depois que ela foi identificada. Níveis mínimos de serviço baseados em IOPS também são compatíveis para fornecer performance consistente para objetos SAN no ONTAP.

Com um armazenamento de dados NFS, uma política de QoS pode ser aplicada a todo o FlexVol volume ou a arquivos VMDK (disco de máquina virtual) individuais dentro dele. Com armazenamentos de dados VMFS (Cluster Shared volumes [CSV] em Hyper-V) que usam LUNs ONTAP, você pode aplicar as políticas de QoS ao FlexVol volume que contém os LUNs ou aos LUNs individuais. No entanto, como o ONTAP não tem conhecimento do VMFS, você não pode aplicar as políticas de QoS a arquivos VMDK individuais. Ao usar o VMware Virtual volumes (VVols) com o VSC 7,1 ou posterior, é possível definir a QoS máxima em VMs individuais usando o perfil de funcionalidades de storage.

Para atribuir uma política de QoS a um LUN, incluindo VMFS ou CSV, é possível obter o SVM do ONTAP (exibido como `Vserver`), caminho de LUN e número de série no menu sistemas de armazenamento na página inicial do VSC. Selecione o sistema de storage (SVM) e, em seguida, objetos relacionados > SAN. Use essa abordagem quando especificar QoS usando uma das ferramentas do ONTAP.

Você pode definir o limite máximo de taxa de transferência de QoS em um objeto em Mbps e em IOPS. Se você usar ambos, o primeiro limite que é atingido é imposto pelo ONTAP. Um workload pode conter vários objetos e uma política de QoS pode ser aplicada a um ou mais workloads. Quando você aplica uma política a vários workloads, os workloads compartilham o limite total da política. Objetos aninhados não são suportados (por exemplo, para um arquivo dentro de um volume, eles não podem ter sua própria política). Os mínimos de QoS podem ser definidos apenas em IOPS.

Layout de storage

Esta seção fornece práticas recomendadas para layout de LUNs, volumes e agregados no storage.

LUNs de storage

Para obter o melhor desempenho, gerenciamento e backup, a NetApp recomenda as seguintes práticas recomendadas de design de LUN:

- Crie um LUN separado para armazenar dados de banco de dados e arquivos de log.
- Crie um LUN separado para cada instância para armazenar backups de log de banco de dados Oracle. Os LUNs podem fazer parte do mesmo volume.
- Provisione LUNs com thin Provisioning (desative a opção reserva de espaço) para arquivos de banco de dados e arquivos de log.
- Todos os dados de imagem são hospedados em LUNs FC. Crie essas LUNs em volumes FlexVol que se espalhem pelos agregados que pertencem a diferentes nós de controladora de storage.

Para o posicionamento dos LUNs em um volume de armazenamento, siga as diretrizes na próxima seção.

Volumes de storage

Para obter o melhor desempenho e gerenciamento, a NetApp recomenda as seguintes práticas recomendadas de design de volume:

- Isole bancos de dados com consultas com uso intenso de e/S em volumes de storage separados.
- Os arquivos de dados podem ser colocados em um único LUN ou um volume, mas vários volumes/LUNs são recomendados para maior taxa de transferência.
- O paralelismo de e/S pode ser alcançado usando qualquer sistema de arquivos suportado quando vários LUNs são usados.
- Coloque arquivos de banco de dados e Registros de transações em volumes separados para aumentar a granularidade de recuperação.

- Considere o uso de atributos de volume, como tamanho automático, reserva de snapshot, QoS, etc.

Agregados

Agregados são os contêineres de storage primário para configurações de storage NetApp e contêm um ou mais grupos RAID que consistem em discos de dados e discos de paridade.

A NetApp realizou vários testes de caraterização de carga de trabalho de e/S usando agregados compartilhados e dedicados com arquivos de dados e arquivos de log de transações separados. Os testes mostram que um agregado grande com mais grupos RAID e unidades (HDDs ou SSDs) otimiza e melhora o desempenho de storage, além de facilitar o gerenciamento dos administradores por dois motivos:

- Um agregado grande torna as habilidades de e/S de todas as unidades disponíveis para todos os arquivos.
- Um agregado grande permite o uso mais eficiente do espaço em disco.

Para uma recuperação de desastres efetiva, a NetApp recomenda que você coloque a réplica assíncrona em um agregado que faça parte de um cluster de storage separado no local de recuperação de desastres e use a tecnologia SnapMirror para replicar conteúdo.

Para obter um desempenho de storage ideal, a NetApp recomenda que você tenha pelo menos 10% de espaço livre disponível em um agregado.

A orientação de layout de agregado de storage para sistemas AFF A300 (com dois compartimentos de disco com 24 unidades) inclui:

- Mantenha duas unidades de reserva.
- Use particionamento de disco avançado para criar três partições em cada unidade: Raiz e dados.
- Use um total de 20 partições de dados e duas partições de paridade para cada agregado.

Práticas recomendadas de backup

O NetApp SnapCenter é usado para backups de VM e banco de dados. A NetApp recomenda as seguintes práticas recomendadas de backup:

- Quando o SnapCenter for implantado para criar cópias Snapshot para backups, desative a programação do Snapshot para o FlexVol que hospeda VMs e dados da aplicação.
- Crie um FlexVol dedicado para LUNs de inicialização de host.
- Use uma política de backup semelhante ou única para VMs que atendem ao mesmo propósito.
- Use uma política de backup semelhante ou única por tipo de workload; por exemplo, use uma política semelhante para todas as cargas de trabalho de banco de dados. Use políticas diferentes para bancos de dados, servidores da Web, desktops virtuais do usuário final e assim por diante.
- Ative a verificação do backup no SnapCenter.
- Configurar o arquivamento das cópias Snapshot de backup para a solução de backup NetApp SnapVault.
- Configurar a retenção dos backups no storage primário com base na programação de arquivamento.

Práticas recomendadas de infraestrutura

Melhores práticas de rede

A NetApp recomenda as seguintes práticas recomendadas de rede:

- Certifique-se de que o sistema inclui placas de rede físicas redundantes para tráfego de produção e armazenamento.
- VLANs separadas para tráfego iSCSI, NFS e SMB/CIFS entre computação e storage.
- Certifique-se de que o seu sistema inclui uma VLAN dedicada para acesso do cliente ao sistema de imagiologia médica.

Você pode encontrar práticas recomendadas de rede adicionais nos guias de design e implantação da infraestrutura do FlexPod.

Práticas recomendadas de computação

A NetApp recomenda a seguinte prática recomendada de computação:

- Certifique-se de que cada vCPU especificado seja suportado por um núcleo físico.

Práticas recomendadas de virtualização

A NetApp recomenda as seguintes práticas recomendadas de virtualização:

- Use o VMware vSphere 6 ou posterior.
- Defina o BIOS e a camada de SO do servidor host ESXi como Custom Controlled–High Performance (Controle personalizado – Alto desempenho).
- Crie backups durante horas fora do horário de pico.

Melhores práticas do sistema de imagem médica

Consulte as práticas recomendadas a seguir e alguns requisitos de um sistema de imagem médica típico:

- Não comprometer a memória virtual.
- Certifique-se de que o número total de vCPUs seja igual ao número de CPUs físicas.
- Se você tiver um ambiente grande, VLANs dedicadas são necessárias.
- Configurar VMs de banco de dados com clusters de HA dedicados.
- Certifique-se de que as VMDKs VM os estejam hospedadas em storage rápido de camada 1.
- Trabalhe com o fornecedor do sistema de imagem médica para identificar a melhor abordagem para preparar modelos de VM para implantação e manutenção rápidas.
- As redes de gerenciamento, armazenamento e produção exigem segregação de LAN para o banco de dados, com VLANs isoladas para VMware vMotion.
- Use a tecnologia de replicação baseada em storage array do NetApp chamada "SnapMirror" em vez de replicação baseada no vSphere.
- Use tecnologias de backup que utilizam APIs VMware; as janelas de backup devem estar fora do horário normal de produção.

Conclusão

Ao executar um ambiente de imagem médica no FlexPod, sua organização de saúde

pode esperar uma melhoria na produtividade da equipe e uma diminuição no capital e nas despesas operacionais. O FlexPod fornece uma infraestrutura convergente pré-validada e rigorosamente testada pela parceria estratégica da Cisco com a NetApp. Ele foi projetado e projetado especificamente para fornecer desempenho previsível do sistema de baixa latência e alta disponibilidade. Essa abordagem resulta em uma experiência de usuário superior e tempo de resposta ideal para usuários do sistema de imagem médica.

Componentes diferentes de um sistema de imagiologia médica requerem armazenamento de dados em sistemas de ficheiros SMB/CIFS, NFS, EXT4 e NTFS. Portanto, sua infraestrutura precisa fornecer acesso aos dados por protocolos NFS, SMB/CIFS e SAN. Os sistemas de storage NetApp dão suporte a esses protocolos a partir de um único storage array.

Alta disponibilidade, eficiência de storage, backups rápidos programados baseados em cópias Snapshot, operações de restauração rápida, replicação de dados para recuperação de desastres e funcionalidades de infraestrutura de storage da FlexPod oferecem um sistema de gerenciamento e storage de dados líder do setor.

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- FlexPod Datacenter para AI/ML com Cisco UCS 480 ml para Guia de design de deep learning

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_c480m5l_aiml_design.html"

- Infraestrutura de data center do FlexPod com VMware vSphere 6,7 U1, Cisco UCS 4tha geração e NetApp AFF A-Series

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_datacenter_vmware_netappaffa.html"

- Resumo da solução FlexPod Datacenter Backup de banco de dados Oracle com SnapCenter

  "https://www.netapp.com/us/media/sb-3999.pdf"

- FlexPod Datacenter com bancos de dados Oracle RAC no Cisco UCS e NetApp AFF Série A.

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orc12cr2_affaseries.html"

- FlexPod Datacenter com Oracle RAC em Oracle Linux

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_orcrac_12c_bm.html"

- FlexPod para Microsoft SQL Server

  "https://flexpod.com/solutions/use-cases/microsoft-sql-server/"

- FlexPod de Cisco e NetApp

"https://flexpod.com/"

- "Soluções NetApp para MongoDB" Resumo da solução (login NetApp necessário)

  "https://fieldportal.netapp.com/content/734702"

- TR-4700: Plug-in SnapCenter para banco de dados Oracle

  "https://www.netapp.com/us/media/tr-4700.pdf"

- Documentação do produto NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- FlexPod para soluções de infraestrutura de desktops virtuais (VDI)

  "https://flexpod.com/solutions/use-cases/virtual-desktop-infrastructure/"

Infraestrutura de desktop virtual

FlexPod Datacenter com Citrix Virtual Apps & desktops 1912 LTSR e VMware vSphere 7 para até 6000 licenças

Cisco, NetApp Dre Jackson, NetApp

Este documento fornece a arquitetura e o design de uma infraestrutura de desktop virtual para até 6000 usuários de computação de usuário final. A solução é virtualizada em servidores blade Cisco UCS B200 M5 de quinta geração, inicializando o VMware vSphere 7,01 Update 1 por meio de SAN FC a partir do storage array AFF A400. Os desktops virtuais são alimentados usando o Citrix Provisioning Server 1912 LTSR e o Citrix RDS/Citrix Virtual Apps & desktops 1912 LTSR, com uma combinação de desktops compartilhados hospedados em RDS (6000), desktops virtuais hospedados em pool e/ou não persistentes do Windows 10 (5000) e desktops virtuais hospedados em persistente do Windows 10 provisionados com o Citrix Machine Creation Services (5000) para dar suporte à população de usuários. Quando aplicável, o documento fornece recomendações de práticas recomendadas e diretrizes de dimensionamento para implantações de clientes desta solução.

"FlexPod Datacenter com Citrix Virtual Apps desktops 1912 LTSR e VMware vSphere 7 para até 6000 assentos"

FlexPod Datacenter com VMware Horizon View, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 e NetApp ONTAP 9 7,10 para até 6700 assentos

Vadim Lebedev, Cisco Suresh Toppay, NetApp

Este documento fornece uma arquitetura de referência e um guia de design para uma carga de trabalho de desktop de 5000 a 6000 lugares, ambiente de computação de usuário final no FlexPod Datacenter com o Cisco UCS e o software de gerenciamento de dados NetApp AFF A300 e NetApp ONTAP. A solução inclui sessões RDS Windows Server 2019 baseadas no servidor VMware Horizon, desktops virtuais Microsoft Windows 10 de clone completo persistente do VMware Horizon e desktops virtuais do Microsoft Windows 10 não persistentes e de clone instantâneo do VMware Horizon no VMware vSphere 6.7U2

"FlexPod Datacenter com VMware Horizon View, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 e NetApp ONTAP 9 7,10 para até 6700 assentos"

Visualização de gráficos 3DD com Citrix e NVIDIA - White paper

Este documento descreve o desempenho do Citrix XenDesktop no Citrix XenServer com

placas NVIDIA Tesla P4, P6 e P40 em servidores Cisco UCS C240 M5 e B200 M5 com SPECviewperf 13.

"Visualização de gráficos 3DD com Citrix e NVIDIA - White paper"

FlexPod Datacenter com Citrix XenDesktop/XenApp 7,15 e VMware vSphere 6,5 Update 1 para 6000 assentos

Vadim Lebedev, Cisco Chris Rodriguez, NetApp

Este documento fornece uma arquitetura de referência para um design de desktop virtual e aplicativo usando o Citrix XenApp/XenDesktop 7,15 desenvolvido no Cisco UCS com um storage NetApp All Flash FAS (AFF) A300 e a plataforma de hypervisor VMware vSphere ESXi 6,5.

O cenário da virtualização de desktops e aplicativos está mudando constantemente. Os novos servidores tipo lâmina Cisco UCS de alto desempenho M5 e a malha unificada Cisco UCS combinados como parte da infraestrutura comprovada da FlexPod, com o armazenamento NetApp AFF de última geração resultam em uma plataforma mais compacta, mais poderosa, mais confiável e eficiente.

"FlexPod Datacenter com Citrix XenDesktop/XenApp 7,15 e VMware vSphere 6,5 Update 1 para 6000 assentos"

FlexPod Datacenter com VMware Horizon View 7,3 e VMware vSphere 6,5 Update 1 com Cisco UCS Manager 3,2 para 5000 assentos

Ramesh Guduru, Cisco David Arnette, NetApp

Este documento fornece uma arquitetura de referência, um guia de design e uma implantação para um ambiente de computação de usuário final com carga de trabalho mista de até 5000 lugares no data center do FlexPod com storage Cisco UCS e NetApp All Flash FAS (AFF) A300. A solução inclui sessões hospedadas do servidor de desktop remoto baseadas no servidor VMware Horizon, desktops virtuais persistentes do Microsoft Windows 10 do VMware Horizon e desktops virtuais de clone instantâneo do Microsoft Windows 10 não persistentes no VMware vSphere 6,5.

"FlexPod Datacenter com VMware Horizon View 7,3 e VMware vSphere 6,5 Update 1 com Cisco UCS Manager 3,2 para 5000 assentos"

FlexPod Datacenter com VMware Horizon View, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 e NetApp ONTAP 9 7,10 para até 6700 assentos

Vadim Lebedev, Cisco Suresh Toppay, NetApp

Este documento fornece uma arquitetura de referência e um guia de design para um

ambiente de computação de usuário final de workload de desktop de 5000 a 6000 lugares no FlexPod Datacenter com o Cisco UCS e o software de gerenciamento de dados NetApp AFF A300 e NetApp ONTAP. A solução inclui sessões RDS Windows Server 2019 baseadas no servidor VMware Horizon, desktops virtuais Microsoft Windows 10 persistentes, clone completo e VMware Horizon, desktops virtuais Microsoft Windows 10 não persistentes e de clone instantâneo no VMware vSphere 6,7 U2.

"FlexPod Datacenter com VMware Horizon View, VMware vSphere 6,7 U2, Cisco UCS Manager 4,0 e NetApp ONTAP 9 7,10 para até 6700 assentos"

Aplicativos modernos

Data center FlexPod para IA e ML combinados com Cisco UCS 480 ml para deep learning - Design

Arvind Ramakrishnan, Cisco, NetApp

Este documento fornece detalhes de design sobre a integração da plataforma Cisco UCS C480 ml M5 à solução de data center FlexPod para fornecer uma abordagem unificada para fornecer recursos de AI e ML na infraestrutura convergente. Ao oferecer aos clientes a capacidade de gerenciar os servidores com recursos combinados de AI e ML com as ferramentas conhecidas que eles usam para administrar sistemas FlexPod tradicionais, a sobrecarga administrativa e o custo de implantação da plataforma de deep learning são bastante reduzidos. O design apresentado neste CVD também inclui outras plataformas Cisco UCS, como o servidor C220 M5 com duas GPUs NVIDIA T4 e o servidor C240 M5 equipado com duas placas NVIDIA V100 32GB PCIe, como opções adicionais para lidar com cargas de trabalho simultâneas de IA e ML.

"Data center FlexPod para IA e ML combinados com Cisco UCS 480 ml para aprendizado profundo - design"

Implante o plug-in NetApp Trident CSI na plataforma de contêiner Cisco com o FlexPod

Este documento fornece procedimentos passo a passo para implantar o plug-in da NetApp Trident Container Storage Interface (CSI) em um cluster de locatário do Kubernetes da plataforma de contêiner da Cisco em uma solução da FlexPod.

"Implante o plug-in NetApp Trident CSI na plataforma de contêiner Cisco com o FlexPod"

FlexPod Datacenter para OpenShift Container Platform 4 - implantação

Cisco Alan Cowles, NetApp

O Red Hat OpenShift é uma plataforma de contêiner do Kubernetes pronta para uso empresarial para gerenciar implantações de nuvem híbrida e multicloud. O Red Hat OpenShift Container Platform inclui tudo o que é necessário para a nuvem híbrida, contêiner empresarial e desenvolvimento e implantações do Kubernetes. Ele inclui um sistema operacional Linux de nível empresarial, runtime de contentor, rede, monitoramento, Registro de contentor, autenticação e soluções de autorização.

A combinação do Red Hat OpenShift com a solução FlexPod Datacenter pode simplificar a implantação e o gerenciamento da infraestrutura de contentores. Os clientes podem se beneficiar de eficiência aprimorada, melhor proteção de dados, menor risco e flexibilidade para escalar esse stack de infraestrutura de nível empresarial altamente disponível para acomodar novos requisitos de negócios. A abordagem de solução convergente pré-validada ajuda as organizações a alcançar a velocidade, a flexibilidade e a escala

necessárias para todas as iniciativas de modernização de aplicações e transformação digital.

"FlexPod Datacenter para OpenShift Container Platform 4 - implantação"

Data center do FlexPod com Docker Enterprise Edition para gerenciamento de contêineres

Cisco, Cisco Amit Borulkar, NetApp, são Paulo, são Paulo, são Paulo, Brasil

O Docker é a plataforma de contentor de software líder mundial para desenvolvedores e operações DE TI para criar, enviar e executar aplicativos distribuídos em qualquer lugar. Com a arquitetura de microsserviços moldando a próxima geração DE TI, empresas com grandes investimentos em aplicações monolíticas estão encontrando maneiras de adotar o Docker como uma estratégia para modernizar suas arquiteturas de aplicativos e manter a organização competitiva e econômica. A Conteinerização fornece a agilidade, o controle e a portabilidade que os desenvolvedores e as operações DE TI exigem para criar e implantar aplicativos em qualquer infraestrutura. A plataforma Docker permite que aplicativos distribuídos sejam facilmente compostos em um contentor de aplicativos leve que pode mudar dinamicamente, mas sem interrupções. Esse recurso torna os aplicativos portáteis em ambientes de desenvolvimento, teste e produção executados em máquinas físicas ou virtuais localmente, em data centers e em redes de diferentes provedores de serviços em nuvem.

"Data center do FlexPod com Docker Enterprise Edition para gerenciamento de contêineres"

FlexPod Datacenter para OpenShift Container Platform 4 - Design

Cisco Alan Cowles, NetApp

A Cisco e a NetApp fizeram uma parceria para fornecer uma série de soluções FlexPod que permitem plataformas estratégicas de data center. A solução FlexPod oferece uma arquitetura integrada que incorpora as práticas recomendadas para computação, armazenamento e design de rede, minimizando assim os riscos DE TI validando a arquitetura integrada para garantir a compatibilidade entre vários componentes. A solução também aborda os pontos problemáticos DA TI, fornecendo orientação de projeto documentada, orientação de implantação e suporte que podem ser usados em várias etapas (Planejamento, projeto e implementação) de uma implantação.

"FlexPod Datacenter para OpenShift Container Platform 4 - Design"

Data center FlexPod para IA e ML combinados com o Cisco UCS 480 ml para deep learning - implantação

Arvind Ramakrishnan, Cisco, NetApp

Este documento fornece detalhes de implantação e orientações sobre a integração da plataforma Cisco UCS C480 ml M5 à solução de data center FlexPod, a fim de fornecer uma abordagem unificada para fornecer recursos de AI e ML na infraestrutura convergente. Este documento também explica a configuração das GPUs NVIDIA nas plataformas Cisco UCS C220 e C240. Para uma discussão detalhada sobre o projeto sobre as plataformas e tecnologias usadas nesta solução, consulte o "Data center FlexPod para IA e ML combinados com o Cisco UCS 480 ML para design de deep learning".

"Data center FlexPod para IA e ML combinados com o Cisco UCS 480 ml para deep learning - implantação"

Visualização de gráficos 3DD com VMware e NVIDIA no Cisco UCS - White paper

Este documento descreve o desempenho do hypervisor VMware ESXi e do VMware Horizon com a solução NVIDIA Tesla P4, P6 e P40 em servidores de rack Cisco UCS C240 M5 e servidores blade B200 M5.

"Visualização de gráficos 3DD com VMware e NVIDIA no Cisco UCS - White paper"

Visualização de gráficos 3DD com Citrix e NVIDIA - White paper

Este documento descreve o desempenho do Citrix XenDesktop no Citrix XenServer com placas NVIDIA Tesla P4, P6 e P40 em servidores Cisco UCS C240 M5 e B200 M5 com SPECviewperf 13.

"Visualização de gráficos 3DD com Citrix e NVIDIA - White paper"

FlexPod Express

FlexPod Express com o guia de design da série C do Cisco UCS e da série NetApp AFF C190

NVA-1139-DESIGN: FlexPod Express com Cisco UCS C-Series e NetApp AFF C190 Series

Saraiva, NetApp

Em parceria com: 

As tendências do setor indicam uma grande transformação do data center em direção à infraestrutura compartilhada e à computação em nuvem. Além disso, as organizações buscam uma solução simples e eficaz para escritórios remotos e filiais que usem a tecnologia que já conhecem em seu data center.

O FlexPod Express é uma arquitetura de data center pré-projetada e com práticas recomendadas. Ele foi desenvolvido com base no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e nos sistemas NetApp AFF. Os componentes do FlexPod Express são como os seus homólogos do data center FlexPod, permitindo sinergias de gerenciamento em todo o ambiente de INFRAESTRUTURA DE TI em menor escala. O data center FlexPod e o FlexPod Express são plataformas ideais para virtualização e para sistemas operacionais bare-metal e workloads empresariais.

"Próximo: Resumo do programa."

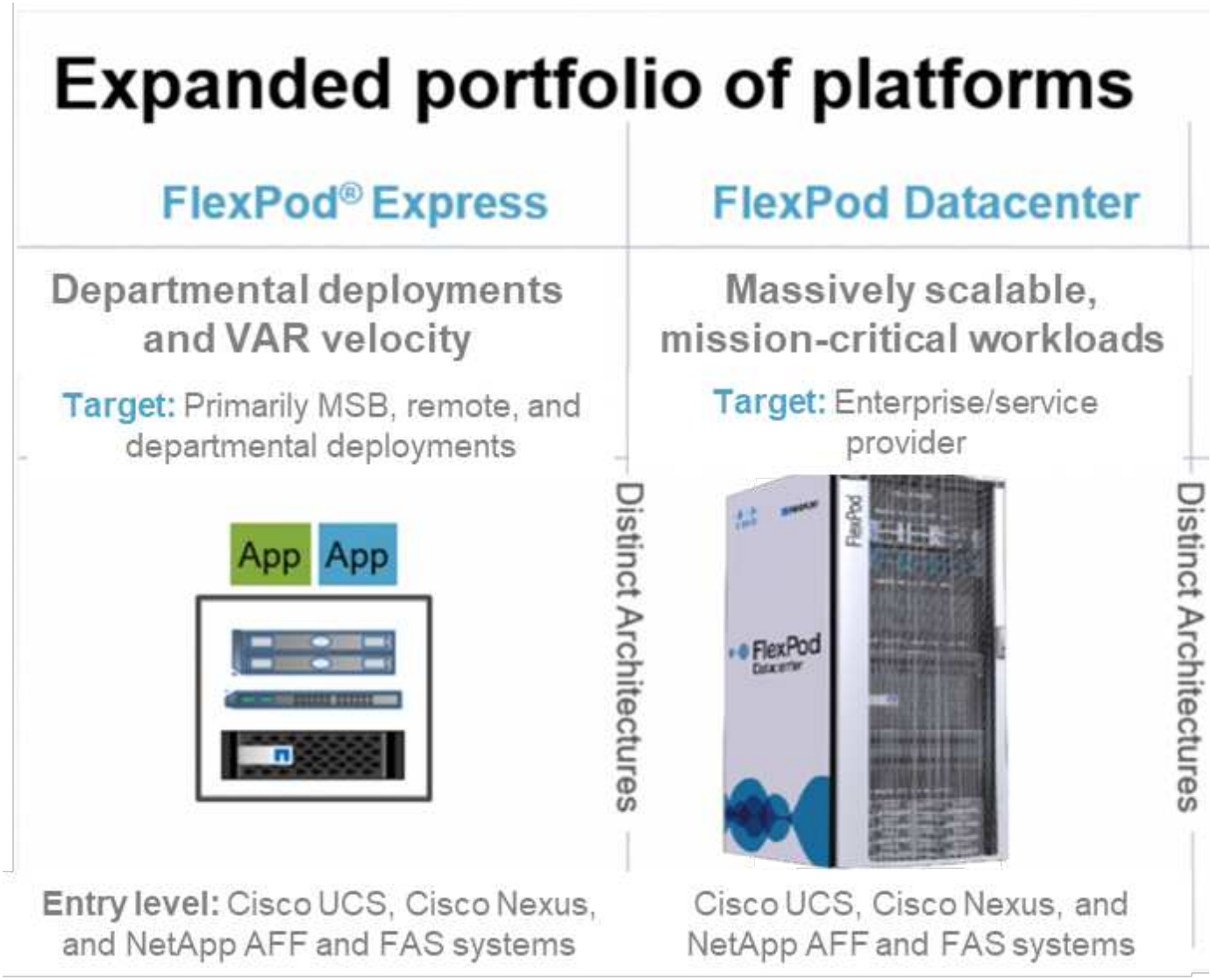
Resumo do programa

Portfólio de infraestrutura convergente do FlexPod

As arquiteturas de referência do FlexPod são entregues como Cisco Validated designs (CVDs) ou como NetApp Verified Architectures (NVAs). Desvios que são baseados nos requisitos do cliente de um determinado CVD ou NVA são permitidos se essas variações não resultarem na implantação de configurações não suportadas.

Conforme ilustrado na figura a seguir, o portfólio do FlexPod inclui as seguintes soluções: FlexPod Express e FlexPod Datacenter.

- **O FlexPod Express** é uma solução de nível básico com tecnologias da Cisco e da NetApp.
- **O FlexPod Datacenter** oferece uma base ideal para uso geral para várias cargas de trabalho e aplicações.



Programa NetApp Verified Architecture

O programa NetApp Verified Architecture oferece aos clientes uma arquitetura verificada para soluções NetApp. Uma solução NVA tem as seguintes qualidades:

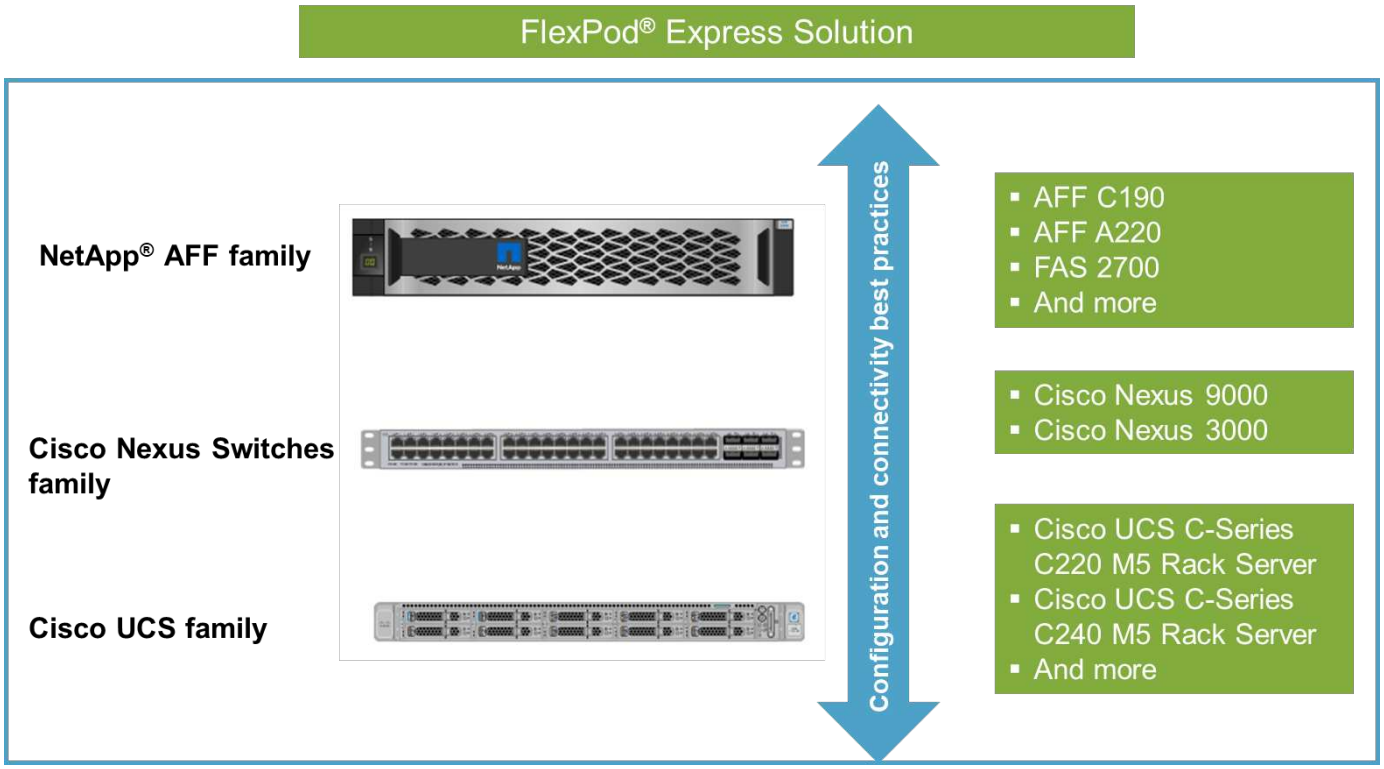
- É completamente testado
- É prescritiva por natureza
- Minimiza os riscos de implantação
- Este guia detalha o design do FlexPod Express com o VMware vSphere.

Além disso, esse design utiliza o novo sistema AFF C190, que executa o software NetApp ONTAP 9.6, os switches Cisco Nexus 31108 e os servidores Cisco UCS C220 M5 como nós de hipervisor.

Visão geral da solução

O FlexPod Express foi projetado para executar workloads de virtualização mistos. Ele é destinado a escritórios remotos e filiais e para empresas de pequeno e médio porte. Também é ideal para grandes empresas que desejam implementar uma solução dedicada para um propósito específico. Essa nova solução para o FlexPod Express adiciona novas tecnologias, como o NetApp ONTAP 9.6, o sistema NetApp AFF C190 e o VMware vSphere 6.7U2.

A figura a seguir mostra os componentes de hardware incluídos na solução FlexPod Express.

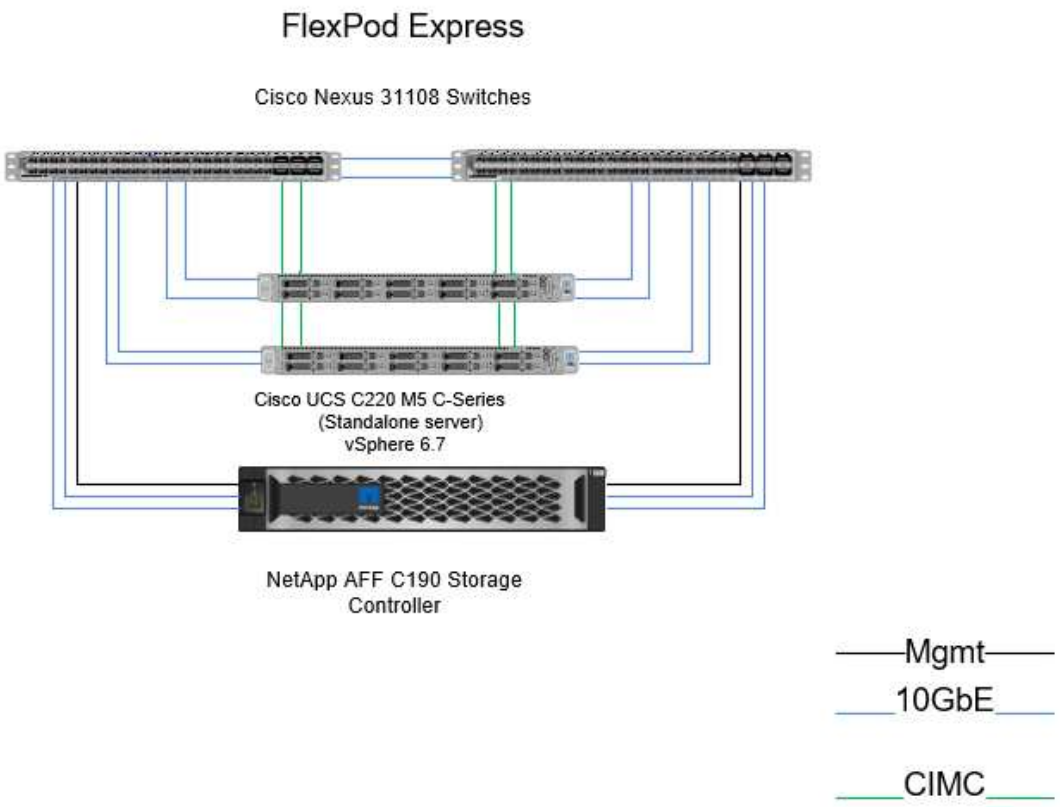


Público-alvo

Este documento destina-se a pessoas que desejam aproveitar uma infraestrutura construída para fornecer eficiência DE TI e permitir a inovação DE TI. O público-alvo deste documento inclui, entre outros, engenheiros de vendas, consultores de campo, pessoal de serviços profissionais, gerentes DE TI, engenheiros DE parceiros e clientes.

Tecnologia da solução

Essa solução utiliza as tecnologias mais recentes da NetApp, Cisco e VMware. Ele apresenta o novo sistema NetApp AFF C190, que executa o software ONTAP 9.6, os switches Cisco Nexus 31108 duplos e os servidores de rack Cisco UCS C220 M5 que executam o VMware vSphere 6.7U2. Esta solução validada, ilustrada na figura a seguir, usa a tecnologia 10 Gigabit Ethernet (10GbE). Também são fornecidas orientações sobre como escalar adicionando dois nós de hipervisor de cada vez, para que a arquitetura FlexPod Express se adapte às crescentes necessidades de negócios da organização.



"Próximo: Requisitos de tecnologia."

Requisitos de tecnologia

O FlexPod Express requer uma combinação de componentes de hardware e software que depende do hipervisor selecionado e da velocidade da rede. Além disso, o FlexPod Express estabelece os componentes de hardware necessários para adicionar nós de hipervisor ao sistema em unidades de dois.

Requisitos de hardware

Independentemente do hypervisor escolhido, todas as configurações do FlexPod Express usam o mesmo hardware. Portanto, mesmo que os requisitos de negócios mudem, você pode usar um hypervisor diferente no mesmo hardware do FlexPod Express.

A tabela a seguir lista os componentes de hardware necessários para essa configuração do FlexPod Express e para implementar essa solução. Os componentes de hardware usados em qualquer implementação da solução podem variar de acordo com os requisitos do cliente.

Hardware	Quantidade
Cluster de 2 nós do AFF C190	1
Servidor Cisco UCS C220 M5	2
Switch Cisco Nexus 31108	2

Hardware	Quantidade
Placa de interface virtual (VIC) Cisco UCS 1457 para servidor de rack Cisco UCS C220 M5	2

Requisitos de software

A tabela a seguir lista os componentes de software necessários para implementar as arquiteturas da solução FlexPod Express.

Software	Versão	Detalhes
Controlador de gerenciamento integrado Cisco (CIMC)	4.0.4	Para C220 M5 servidores de rack
Cisco NX-os	7,0 (3)I7 (6)	Para switches Cisco Nexus 31108
NetApp ONTAP	9,6	Para controladores NetApp AFF C190

A tabela a seguir lista o software necessário para todas as implementações do VMware vSphere no FlexPod Express.

Software	Versão
Dispositivo VMware vCenter Server	6.7U2
VMware vSphere ESXi	6.7U2
Plug-in NetApp VAAI para ESXi	1.1.2
Console de storage virtual do NetApp	9,6

"Próximo: Opções de design."

Opções de design

As tecnologias listadas nesta seção foram escolhidas durante a fase de projeto arquitetônico. Cada tecnologia atende a um propósito específico na solução de infraestrutura FlexPod Express.

Série NetApp AFF C190 com ONTAP 9 .6

Essa solução aproveita dois dos mais novos produtos NetApp: O sistema NetApp AFF C190 e o software ONTAP 9.6.

Sistema AFF C190

O grupo-alvo são os clientes que querem modernizar a INFRAESTRUTURA DE TI com tecnologia all-flash a um preço acessível. O sistema AFF C190 vem com o novo ONTAP 9.6 e licenciamento de pacotes flash, o que significa que as seguintes funções estão integradas:

- CIFS, NFS, iSCSI e FCP
- Software de replicação de dados NetApp SnapMirror, software de backup NetApp SnapVault, software de recuperação de dados NetApp SnapRestore, pacote de produtos de software de gerenciamento de

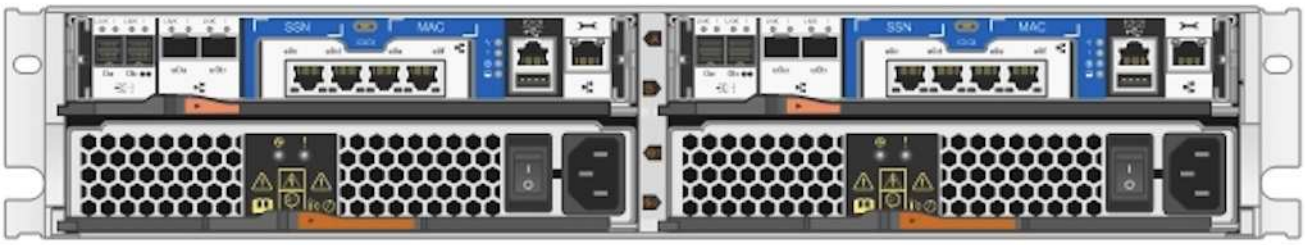
storage NetApp SnapManager e software NetApp SnapCenter

- Tecnologia FlexVol
- Deduplicação, compressão e compactação
- Thin Provisioning
- QoS de storage
- Tecnologia NetApp RAID DP
- Tecnologia NetApp Snapshot
- FabricPool

As figuras a seguir mostram as duas opções de conetividade de host.

A figura a seguir ilustra as portas UTA 2 onde o módulo SFP pode ser inserido.

A figura a seguir ilustra portas 10GBASEBASE-T para conexão por meio de cabos Ethernet RJ-45 convencionais.



Para a opção de porta 10GBASEBASE-T, você deve ter um switch uplink baseado em 10GBASEBASE-T.

O sistema AFF C190 é oferecido exclusivamente com SSDs de 960GB TB. Existem quatro estágios de expansões a partir dos quais você pode escolher:

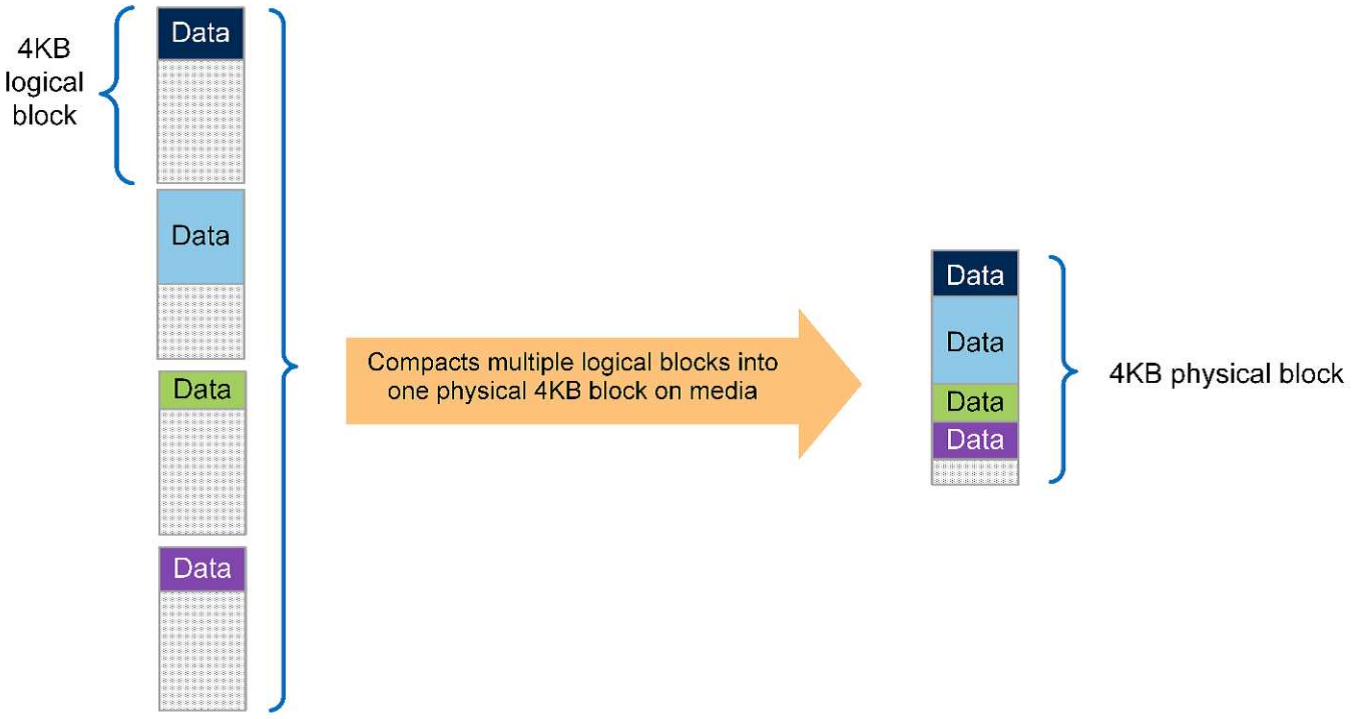
- 8x 960GB
- 12x 960GB
- 18x 960GB
- 24x 960GB

Para obter informações completas sobre o sistema de hardware AFF C190, consulte "Página de array all-flash NetApp AFF C190".

ONTAP 9 1.6 software

Os sistemas NetApp AFF C190 usam o novo software de gerenciamento de dados ONTAP 9.6. O ONTAP 9.6 é o software empresarial de gerenciamento de dados líder do setor. Ele combina novos níveis de simplicidade e flexibilidade com funcionalidades avançadas de gerenciamento de dados, eficiências de storage e integração com a nuvem líder.

O ONTAP 9.6 tem vários recursos que são adequados para a solução FlexPod Express. O mais importante é o compromisso da NetApp com a eficiência de storage, que pode ser um dos recursos mais importantes para implantações de pequeno porte. Os recursos de eficiência de storage da NetApp, como deduplicação, compressão, compactação e thin Provisioning, estão disponíveis no ONTAP 9.6. O sistema NetApp WAFL grava sempre 4KB blocos; portanto, a compactação combina vários blocos em um bloco 4KB quando os blocos não estão usando o espaço alocado de 4KB. A figura a seguir ilustra esse processo.



O ONTAP 9.6 agora oferece suporte a um tamanho de bloco opcional de 512 bytes para volumes NVMe. Essa capacidade funciona bem com o VMware Virtual Machine File System (VMFS), que usa nativamente um bloco de 512 bytes. Você pode ficar com o tamanho padrão 4K ou opcionalmente definir o tamanho do bloco de 512 bytes.

Outras melhorias de recursos no ONTAP 9.6 incluem:

- **Criptografia agregada NetApp (NAE).** O NAE atribui chaves no nível agregado, criptografando assim todos os volumes no agregado. Esse recurso permite que os volumes sejam criptografados e desduplicados no nível agregado.
- * NetApp ONTAP FlexGroup aumento de volume*. No ONTAP 9.6, você pode facilmente renomear um volume FlexGroup. Não é necessário criar um novo volume para o qual migrar os dados. O tamanho do volume também pode ser reduzido usando o Gerenciador de sistemas ou a CLI do ONTAP.
- **Aprimoramento de FabricPool.** O ONTAP 9.6 adicionou suporte adicional para armazenamentos de objetos como camadas de nuvem. O suporte ao Google Cloud e ao Alibaba Cloud Object Storage Service (OSS) também foi adicionado à lista. O FabricPool é compatível com vários armazenamentos de objetos, incluindo AWS S3, Azure Blob, storage de objetos IBM Cloud e software de storage baseado em objetos NetApp StorageGRID.

- **Aprimoramento de SnapMirror.** No ONTAP 9.6, uma nova relação de replicação de volume é criptografada por padrão antes de sair da matriz de origem e é descriptografada no destino do SnapMirror.

Cisco Série Nexus 3000

O Cisco Nexus 31108PC-V é um switch topo de rack (Tor) baseado em 10Gbps SFP com mais de 48 portas SFP e 6 QSFP28 portas. Cada porta SFP pode operar em 100Mbps GbE, 10Gbps GbE e cada porta QSFP28 GbE pode operar em modo nativo 100Gbps GbE ou 40Gbps GbE ou modo 4x 10Gbps GbE, oferecendo opções de migração flexíveis. Esse switch é um verdadeiro switch sem PHY otimizado para baixa latência e baixo consumo de energia.

A especificação Cisco Nexus 31108PC-V inclui os seguintes componentes:

- Capacidade de comutação de 2,16Tbps W e taxa de encaminhamento de até 1,2Tbps Mbps para 31108PC V
- 48 portas SFP suportam 1 e 10 Gigabit Ethernet (10GbE); 6x QSFP28 portas suportam 4x 10GbE ou 40GbE cada ou 100GbE

A figura a seguir ilustra o switch Cisco Nexus 31108PC-V.

Para obter mais informações sobre os switches Cisco Nexus 31108PC-V, "Ficha de dados dos switches Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL e 3172TQ-XL" consulte .

Cisco UCS C-Series

O servidor de rack Cisco UCS C-Series foi escolhido para o FlexPod Express porque suas muitas opções de configuração permitem que ele seja adaptado para requisitos específicos em uma implantação do FlexPod Express.

Os servidores de rack Cisco UCS C-Series oferecem computação unificada em um fator forma padrão do setor para reduzir o TCO e aumentar a agilidade.

Os servidores de rack Cisco UCS C-Series oferecem os seguintes benefícios:

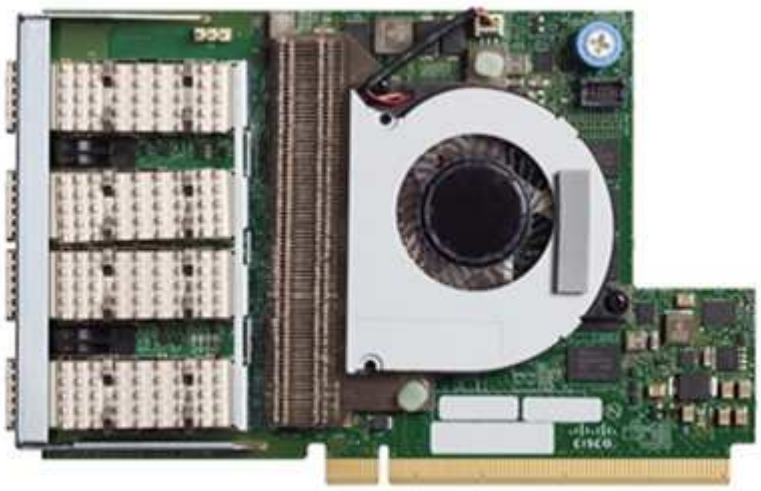
- Um ponto de entrada independente de fator de forma no Cisco UCS
- Implantação de aplicações simplificada e rápida
- Extensão das inovações e benefícios da computação unificada para servidores em rack
- Maior escolha do cliente com benefícios exclusivos em um pacote de rack familiar

O servidor de rack Cisco UCS C220 M5, mostrado na figura acima, está entre os servidores de aplicativos e infraestrutura empresarial de uso geral mais versáteis do setor. É um servidor em rack de dois soquetes de alta densidade que oferece desempenho e eficiência líderes do setor para uma ampla variedade de workloads, incluindo virtualização, colaboração e aplicações bare-metal. Os servidores de rack Cisco UCS C-Series podem ser implantados como servidores autônomos ou como parte do Cisco UCS para aproveitar as inovações de computação unificada baseadas em padrões da Cisco que ajudam a reduzir o TCO dos clientes e a aumentar a agilidade nos negócios.

Para obter mais informações sobre servidores C220 M5, "Folha de dados do servidor de rack Cisco UCS C220 M5" consulte .

Conetividade Cisco UCS VIC 1457 para servidores de rack C220 M5

O adaptador Cisco UCS VIC 1457 mostrado na figura a seguir é uma placa de rede local modular conetável de fator de forma pequeno (SFP28) de quatro portas na placa-mãe (mLOM) projetada para a geração M5 de servidores Cisco UCS C-Series. A placa suporta Ethernet 10/25Gbps ou FCoE. A placa pode apresentar interfaces compatíveis com padrões PCIe para o host, e estas podem ser configuradas dinamicamente como NICs ou HBAs.



Para obter informações completas sobre o adaptador Cisco UCS VIC 1457, "Folha de dados da série 1400 da placa de interface virtual do Cisco UCS" consulte .

VMware vSphere 6.7U2

O VMware vSphere 6.7U2 é uma das opções de hypervisor para uso com o FlexPod Express. O VMware vSphere permite que as organizações reduzam sua capacidade de energia e refrigeração, ao mesmo tempo em que confirmam que a capacidade de computação comprada é usada ao máximo. Além disso, o VMware vSphere permite a proteção contra falhas de hardware (VMware High Availability, ou VMware HA) e o balanceamento de carga de recursos de computação em um cluster de hosts vSphere (VMware Distributed Resource Scheduler no modo de manutenção ou VMware DRS-MM).

Como ele reinicia apenas o kernel, o VMware vSphere 6.7U2 permite que os clientes iniciem rapidamente, carregando o vSphere ESXi sem reiniciar o hardware. O cliente vSphere 6.7U2 vSphere (cliente baseado em HTML5) tem algumas novas melhorias, como o Developer Center com captura de código e exploração de API. Com o Code Capture, você pode gravar suas ações no cliente vSphere para fornecer saída de código simples e utilizável. O vSphere 6.7U2 também contém novos recursos, como DRS no modo de manutenção (DRS-MM).

O VMware vSphere 6.7U2 oferece os seguintes recursos:

- A VMware está depreciando o modelo de implantação externa do VMware Platform Services Controller (PSC).

> A partir da próxima versão principal do vSphere, o PSC externo não será uma opção disponível.

- Novo suporte ao protocolo para fazer backup e restaurar um dispositivo do vCenter Server. Apresentando o NFS e o SMB como opções de protocolo compatíveis, até um total de 7 (HTTP, HTTPS, FTP, FTPS, SCP, NFS e SMB) ao configurar um vCenter Server para operações de backup ou restauração baseadas em arquivos.
- Nova funcionalmente ao usar a biblioteca de conteúdo. A sincronização de um modelo de VM nativo entre bibliotecas de conteúdo agora está disponível quando o vCenter Server é configurado para o modo vinculado aprimorado.
- Atualize para o "Página de plug-ins do cliente".
- O VMware vSphere Update Manager também adiciona melhorias ao cliente vSphere. Você pode executar a conformidade de verificação de anexação e as ações corretivas, tudo em uma única tela.

Para obter mais informações sobre o VMware vSphere 6,7 U2, consulte "Página do blog do VMware vSphere".

Para obter mais informações sobre as atualizações do VMware vCenter Server 6,7 U2, consulte o "Notas de versão".

> Embora essa solução tenha sido validada com o vSphere 6.7U2, ela oferece suporte a qualquer versão do vSphere qualificada com os outros componentes pelo "Ferramenta de Matriz de interoperabilidade NetApp (IMT)". A NetApp recomenda que você implante a próxima versão lançada do vSphere para suas correções e recursos aprimorados.

Arquitetura de inicialização

As opções suportadas para a arquitetura de arranque do FlexPod Express incluem:

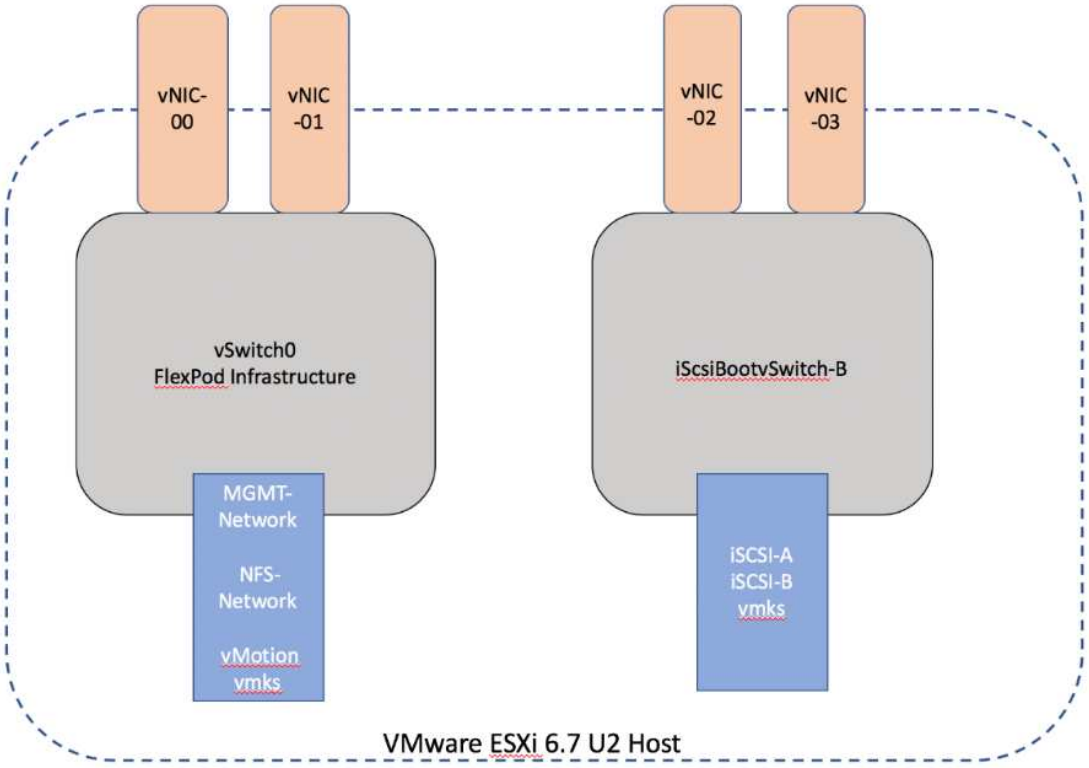
- ISCSI SAN LUN
- Cartão SD Cisco FlexFlash
- Disco local

O FlexPod Datacenter é inicializado a partir de iSCSI LUNs; portanto, a capacidade de gerenciamento da solução também é aprimorada usando o iSCSI boot para FlexPod Express.

Layout da placa de interface de rede virtual do host ESXi

Cisco UCS VIC 1457 tem quatro portas físicas. Essa validação da solução inclui essas quatro portas físicas no uso do host ESXi. Se você tiver um número menor ou maior de NICs, poderá ter números VMNIC diferentes.

Numa implementação de arranque iSCSI, o arranque iSCSI requer placas de interface de rede virtual (vNICs) separadas para o arranque iSCSI. Esses vNICs usam a VLAN iSCSI da malha apropriada como VLAN nativa e são conetados aos vSwitches de inicialização iSCSI, como mostrado na figura a seguir.



"Próximo: Conclusão."

Conclusão

O design validado pela FlexPod Express é uma solução simples e eficaz que usa componentes líderes do setor. Ao dimensionar e fornecer opções para a plataforma de hypervisor, o FlexPod Express pode ser adaptado para necessidades específicas de negócios. O FlexPod Express foi desenvolvido para empresas de pequeno e médio porte, escritórios remotos e filiais e outras empresas que exigem soluções dedicadas.

"Próximo: Onde encontrar informações adicionais."

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- Centro de Documentação do sistema AFF e FAS

  "https://docs.netapp.com/platstor/index.jsp"

- Página de recursos da documentação do AFF

  "https://www.netapp.com/us/documentation/all-flash-fas.aspx"

- FlexPod Express com o VMware vSphere 6,7 e o Guia de implantação do NetApp AFF C190 (em andamento)

- Documentação do NetApp

  "https://docs.netapp.com"

Guia de implantação do FlexPod Express com o Cisco UCS C-Series e o NetApp AFF C190 Series

NVA-1142-DEPLOY: FlexPod Express com Cisco UCS C-Series e NetApp AFF C190 Series - implantação NVA

Saraiva, NetApp

As tendências do setor indicam que uma grande transformação do data center está ocorrendo em relação à infraestrutura compartilhada e à computação em nuvem. Além disso, as organizações buscam uma solução simples e eficaz para escritórios remotos e filiais que usem a tecnologia que já conhecem em seu data center.

O FlexPod Express é uma arquitetura de data center pré-projetada e de práticas recomendadas, desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e nas tecnologias de armazenamento NetApp. Os componentes de um sistema FlexPod Express são como os seus homólogos do data center FlexPod, permitindo sinergias de gerenciamento em todo o ambiente de INFRAESTRUTURA DE TI em menor escala. O data center FlexPod e o FlexPod Express são plataformas ideais para virtualização e para sistemas operacionais bare-metal e workloads empresariais.

O data center FlexPod e o FlexPod Express oferecem uma configuração de linha de base e têm a flexibilidade de ser dimensionados e otimizados para acomodar vários casos de uso e requisitos diferentes. Os clientes de data center FlexPod existentes podem gerenciar o sistema FlexPod Express com as ferramentas às quais estão acostumados. Os novos clientes do FlexPod Express podem fazer a transição para o gerenciamento do data center FlexPod à medida que seu ambiente cresce.

O FlexPod Express é uma base ideal de infraestrutura para escritórios remotos e filiais e para empresas de pequeno e médio porte. Ele também é uma solução ideal para clientes que desejam fornecer infraestrutura para um workload dedicado.

O FlexPod Express fornece uma infraestrutura fácil de gerenciar, adequada para praticamente qualquer workload.

Visão geral da solução

Esta solução FlexPod Express faz parte do Programa de infraestrutura convergente da FlexPod.

Programa de infraestrutura convergente do FlexPod

As arquiteturas de referência do FlexPod são entregues como Cisco Validated designs (CVDs) ou NetApp Verified Architectures (NVAs). Desvios com base nos requisitos do cliente de um determinado CVD ou NVA são permitidos se essas variações não criarem uma configuração não suportada.

O programa FlexPod inclui duas soluções: FlexPod Express e FlexPod Datacenter.

- **FlexPod Express.** Oferece aos clientes uma solução de nível básico com tecnologias da Cisco e NetApp.

- **Centro de dados FlexPod.** Fornece uma base ideal para uso geral para vários workloads e aplicações.

Programa NetApp Verified Architecture

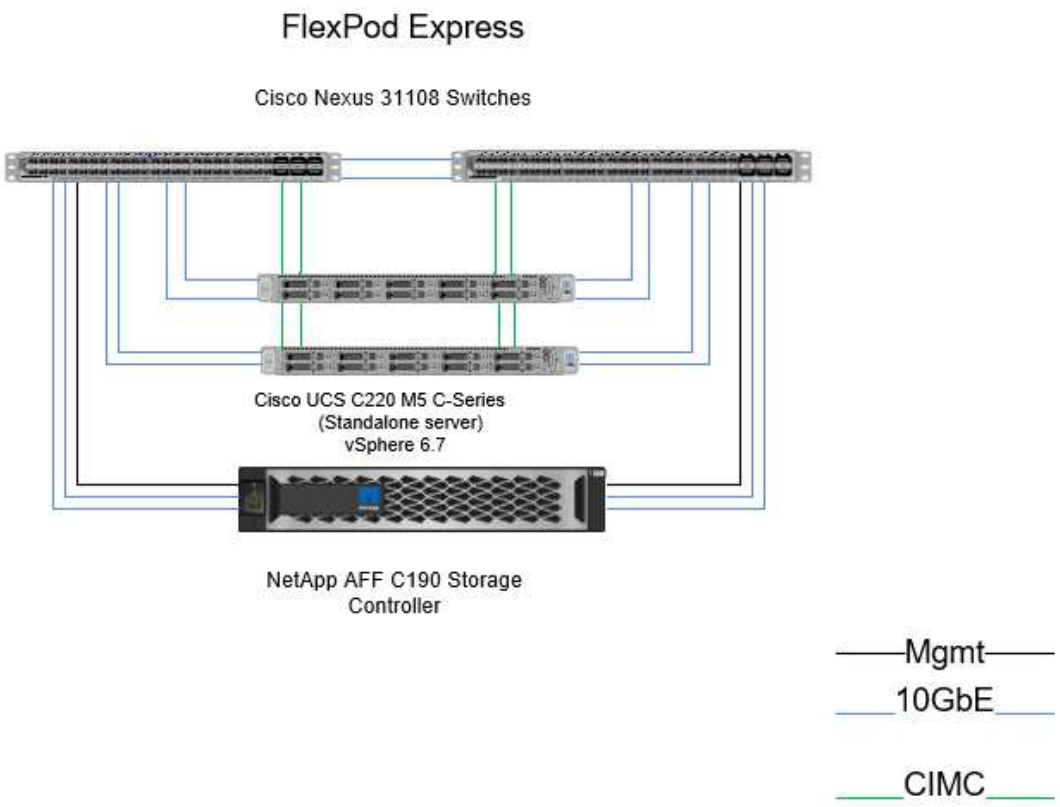
O programa NetApp Verified Architecture oferece aos clientes uma arquitetura verificada para soluções NetApp. Uma arquitetura verificada do NetApp fornece uma arquitetura de solução NetApp com as seguintes qualidades:

- Testes completos
- Natureza prescritiva
- Redução dos riscos de implantação
- Time-to-market acelerado

Este guia detalha o design do FlexPod Express com o VMware vSphere. Além disso, esse projeto usa o novo sistema AFF C190 (executando o NetApp ONTAP 9,6), o Cisco Nexus 31108 e os servidores Cisco UCS C-Series C220 M5 como nós de hipervisor.

Tecnologia da solução

Essa solução utiliza as tecnologias mais recentes da NetApp, Cisco e VMware. Essa solução conta com o novo NetApp AFF C190 executando o ONTAP 9.6, os switches duplos Cisco Nexus 31108 e os servidores de rack Cisco UCS C220 M5 executando o VMware vSphere 6.7U2. Essa solução validada usa a tecnologia 10GbE. Também são fornecidas orientações sobre como dimensionar a capacidade computacional adicionando dois nós de hipervisor de cada vez, para que a arquitetura FlexPod Express se adapte às crescentes necessidades de negócios da organização.



Para utilizar as quatro portas 10GbE físicas no VIC 1457 de forma eficiente, crie duas ligações adicionais de cada servidor para os interrutores do rack superior.

Resumo do caso de uso

A solução FlexPod Express pode ser aplicada a vários casos de uso, incluindo os seguintes:

- Escritórios remotos ou filiais
- Pequenas e médias empresas
- Ambientes que exigem uma solução dedicada e econômica

O FlexPod Express é mais adequado para workloads virtualizados e mistos. Embora essa solução tenha sido validada com o vSphere 6.7U2, ela suporta qualquer versão do vSphere qualificada com os outros componentes pela ferramenta de Matriz de interoperabilidade do NetApp. A NetApp recomenda a implantação do vSphere 6.7U2 por causa de suas correções e recursos aprimorados, como o seguinte:

- Novo suporte de protocolo para backup e restauração de um dispositivo de servidor vCenter, incluindo HTTP, HTTPS, FTP, FTPS, SCP, NFS e SMB.
- Nova funcionalmente ao utilizar a biblioteca de conteúdo. A sincronização de modelos de VM nativos entre bibliotecas de conteúdo agora está disponível quando o vCenter Server é configurado para o modo vinculado aprimorado.
- Uma página atualizada do Client Plug-in.
- Melhorias adicionadas no vSphere Update Manager (VUM) e no cliente vSphere. Agora você pode executar as ações de anexação, verificação de conformidade e correção, tudo em uma única tela.

Para obter mais informações sobre este assunto, consulte a "Página do vSphere 6.7U2" e "Notas de versão do vCenter Server 6.7U2" a .

Requisitos de tecnologia

Um sistema FlexPod Express requer uma combinação de componentes de hardware e software. O FlexPod Express também descreve os componentes de hardware necessários para adicionar nós de hipervisor ao sistema em unidades de dois.

Requisitos de hardware

Independentemente do hypervisor escolhido, todas as configurações do FlexPod Express usam o mesmo hardware. Portanto, mesmo que os requisitos de negócios mudem, você pode usar um hypervisor diferente no mesmo hardware do FlexPod Express.

A tabela a seguir lista os componentes de hardware necessários para a configuração e implementação do FlexPod Express. Os componentes de hardware usados em qualquer implementação da solução podem variar de acordo com os requisitos do cliente.

Hardware	Quantidade
Cluster de dois nós do AFF C190	1
Servidor Cisco C220 M5	2
Switch Cisco Nexus 31108PC-V.	2
Placa de interface virtual (VIC) Cisco UCS 1457 para servidor de rack Cisco UCS C220 M5	2

Esta tabela lista o hardware necessário, além da configuração base para a implementação do 10GbE.

Hardware	Quantidade
Servidor Cisco UCS C220 M5	2
Cisco VIC 1457	2

Requisitos de software

A tabela a seguir lista os componentes de software necessários para implementar as arquiteturas das soluções FlexPod Express.

Software	Versão	Detalhes
Controlador de gerenciamento integrado Cisco (CIMC)	4.0.4	Para servidores de rack Cisco UCS C220 M5
Cisco nenic driver	1.0.0.29	Para placas de interface VIC 1457
Cisco NX-os	7,0 (3)I7 (6)	Para switches Cisco Nexus 31108PC-V.
NetApp ONTAP	9,6	Para controladores AFF C190

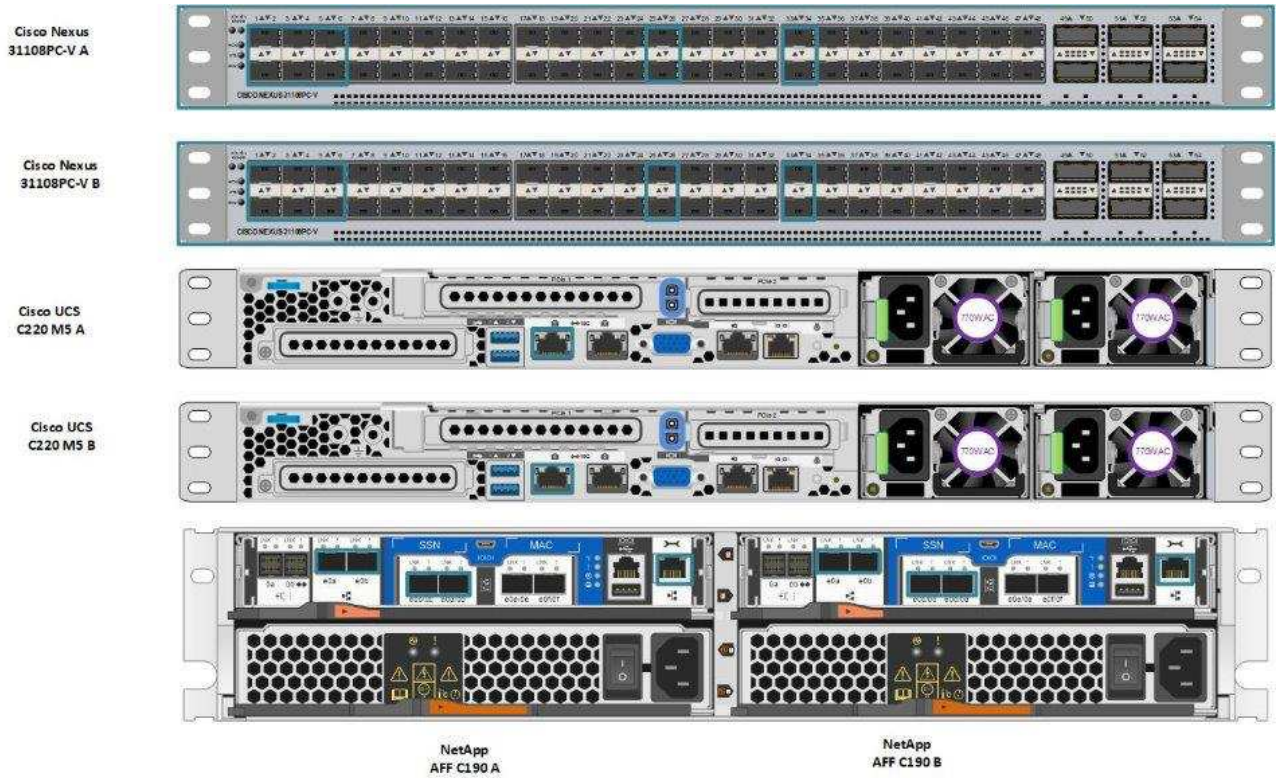
Esta tabela lista o software necessário para todas as implementações do VMware vSphere no FlexPod Express.

Software	Versão
Dispositivo de servidor VMware vCenter	6.7U2
Hipervisor VMware vSphere ESXi	6.7U2
Plug-in NetApp VAAI para ESXi	1.1.2
NetApp VSC	9,6

Informações de cabeamento do FlexPod Express

Esta validação de referência é cabeada como mostrado nas figuras e tabelas a seguir.

Esta figura mostra o cabeamento de validação de referência.



A tabela a seguir lista as informações de cabeamento do switch Cisco Nexus 31108PC-V-A.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Interrutor Cisco Nexus 31108PC-V A	Eth1/1	Controlador de storage NetApp AFF C190 A	e0c
	Eth1/2	Controlador de storage NetApp AFF C190 B	e0c
	Eth1/3	Servidor independente A do Cisco UCS C220 C-Series	MLOM0
	Eth1/4	Servidor independente B do Cisco UCS C220 C-Series	MLOM0
	Eth1/5	Servidor independente A do Cisco UCS C220 C-Series	MLOM1
	Eth1/6	Servidor independente B do Cisco UCS C220 C-Series	MLOM1
	Eth1/25	Interrutor Cisco Nexus 31108PC-V B	Eth1/25
	Eth1/26	Interrutor Cisco Nexus 31108PC-V B	Eth1/26
	Eth1/33	Controlador de storage NetApp AFF C190 A	e0M
	Eth1/34	Servidor independente A do Cisco UCS C220 C-Series	CIMC (FEX135/1/25)

Esta tabela lista as informações de cabeamento do switch Cisco Nexus 31108PC-V- B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Interrutor Cisco Nexus 31108PC-V B	Eth1/1	Controlador de storage NetApp AFF C190 A	e0d
	Eth1/2	Controlador de storage NetApp AFF C190 B	e0d
	Eth1/3	Servidor independente A do Cisco UCS C220 C-Series	MLOM2
	Eth1/4	Servidor independente B do Cisco UCS C220 C-Series	MLOM2
	Eth1/5	Servidor independente A do Cisco UCS C220 C-Series	MLOM3
	Eth1/6	Servidor independente B do Cisco UCS C220 C-Series	MLOM3
	Eth1/25	Switch Cisco Nexus 31108 A	Eth1/25
	Eth1/26	Switch Cisco Nexus 31108 A	Eth1/26
	Eth1/33	Controlador de storage NetApp AFF C190 B	e0M
	Eth1/34	Servidor independente B do Cisco UCS C220 C-Series	CIMC (FEX135/1/26)

Esta tabela lista as informações de cabeamento para o controlador de armazenamento NetApp AFF C190 A..

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Controlador de storage NetApp AFF C190 A	e0a	Controlador de storage NetApp AFF C190 B	e0a
	e0b	Controlador de storage NetApp AFF C190 B	e0b
	e0c	Interrutor Cisco Nexus 31108PC-V A	Eth1/1
	e0d	Interrutor Cisco Nexus 31108PC-V B	Eth1/1
	e0M	Interrutor Cisco Nexus 31108PC-V A	Eth1/33

Esta tabela lista as informações de cabeamento do controlador de armazenamento NetApp AFF C190 B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Controlador de storage NetApp AFF C190 B	e0a	Controlador de storage NetApp AFF C190 A	e0a
	e0b	Controlador de storage NetApp AFF C190 A	e0b
	e0c	Interrutor Cisco Nexus 31108PC-V A	Eth1/2
	e0d	Interrutor Cisco Nexus 31108PC-V B	Eth1/2
	e0M	Interrutor Cisco Nexus 31108PC-V B	Eth1/33

Procedimentos de implantação

Visão geral

Este documento fornece detalhes para configurar um sistema FlexPod Express totalmente redundante e altamente disponível. Para refletir essa redundância, os componentes que estão sendo configurados em cada etapa são referidos como componente A ou componente B. por exemplo, controlador A e controlador B identificam os dois controladores de storage NetApp que são provisionados neste documento. O switch A e o switch B identificam um par de switches Cisco Nexus.

Além disso, este documento descreve etapas para provisionar vários hosts Cisco UCS, que são identificados sequencialmente como servidor A, servidor B e assim por diante.

Para indicar que você deve incluir informações pertinentes ao seu ambiente em uma etapa, `<<text>>` aparece como parte da estrutura de comando. Veja o exemplo a seguir para o `vlan create` comando:

```
Controller01> network port vlan create –node <<var_nodeA>> -vlan-name
<<var_vlan-name>>
```

Este documento permite configurar totalmente o ambiente do FlexPod Express. Nesse processo, várias etapas exigem que você insira convenções de nomenclatura específicas do cliente, endereços IP e esquemas de rede local virtual (VLAN). A tabela a seguir descreve as VLANs necessárias para implantação, conforme descrito neste guia. Esta tabela pode ser concluída com base nas variáveis específicas do site e usada para implementar as etapas de configuração do documento.

Se você usar VLANs separadas de gerenciamento dentro e fora da banda, será necessário criar uma rota de camada 3 entre elas. Para essa validação, uma VLAN de gerenciamento comum foi usada.

Nome da VLAN	Finalidade do VLAN	ID DA VLAN	
VLAN de gerenciamento	VLAN para interfaces de gerenciamento	3437	vSwitch0

Nome da VLAN	Finalidade do VLAN	ID DA VLAN	
VLAN NFS	VLAN para tráfego NFS	3438	vSwitch0
VLAN do VMware vMotion	VLAN designada para o movimento de máquinas virtuais (VMs) de um host físico para outro	3441	vSwitch0
VLAN de tráfego de VM	VLAN para tráfego de aplicação de VM	3442	vSwitch0
ISCSI-A-VLAN	VLAN para tráfego iSCSI na malha A	3439	IScsiBootvSwitch
ISCSI-B-VLAN	VLAN para tráfego iSCSI na malha B	3440	IScsiBootvSwitch
VLAN nativo	VLAN à qual os quadros não marcados são atribuídos	2	

Os números de VLAN são necessários durante toda a configuração do FlexPod Express. As VLANs são referidas como `<<var_xxxx_vlan>>`, onde `xxxx` é a finalidade da VLAN (como iSCSI-A).

Existem dois vSwitches criados nesta validação.

A tabela a seguir lista os vSwitches da solução.

Nome do vSwitch	Adaptadores ativos	Portas	MTU	Balanceamento de carga
vSwitch0	Vmnic2, vmnic4	padrão (120)	9000	Rota baseada em hash IP
IScsiBootvSwitch	Vmnic3, vmnic5	padrão (120)	9000	Rota com base no ID de porta virtual de origem.

O método de hash IP de balanceamento de carga requer uma configuração adequada para o switch físico subjacente usando SRC-DST-IP EtherChannel com um canal de porta estático (modo ligado). Em caso de conetividade intermitente devido a uma possível configuração incorreta do switch, desligue temporariamente uma das duas portas de uplink associadas no switch Cisco para restaurar a comunicação com a porta vmkernel de gerenciamento ESXi enquanto soluciona problemas de configurações do canal de porta.

A tabela a seguir lista as VMs VMware criadas.

Descrição da VM	Nome do host
VMware vCenter Server	FlexPod-VCSA
Console de armazenamento virtual	FlexPod-VSC

Implante o Cisco Nexus 31108PC-V

Esta seção detalha a configuração do switch Cisco Nexus 331108PC-V usada em um ambiente FlexPod Express.

Configuração inicial do switch Cisco Nexus 31108PC-V.

Os procedimentos a seguir descrevem como configurar os switches Cisco Nexus para uso em um ambiente FlexPod Express básico.

> Este procedimento pressupõe que você está usando um Cisco Nexus 31108PC-V executando o software NX-os versão 7,0(3)i7(6).

1. Após a inicialização inicial e a conexão à porta do console do switch, a configuração do Cisco NX-os é iniciada automaticamente. Esta configuração inicial aborda as configurações básicas, como o nome do switch, a configuração da interface mgmt0 e a configuração do Secure Shell (SSH).
2. A rede de gerenciamento FlexPod Express pode ser configurada de várias maneiras. As interfaces mgmt0 nos switches 31108PC-V podem ser conetadas a uma rede de gerenciamento existente, ou as interfaces mgmt0 dos switches 31108PC-V podem ser conetadas em uma configuração back-to-back. No entanto, este link não pode ser usado para acesso de gerenciamento externo, como tráfego SSH.

   > Neste guia de implantação, os switches FlexPod Express Cisco Nexus 31108PC-V estão conetados a uma rede de gerenciamento existente.

3. Para configurar os switches Cisco Nexus 31108PC-V, ligue o switch e siga as instruções na tela, conforme ilustrado aqui para a configuração inicial de ambos os switches, substituindo os valores apropriados para as informações específicas do switch.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 31108PC-V-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]: <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: <enter>
```

4. Em seguida, você verá um resumo de sua configuração e será perguntado se deseja editá-la. Se a configuração estiver correta, introduza `n`.

```
Would you like to edit the configuration? (y
es/no) [n]: n
```

5. Então, você será perguntado se deseja usar essa configuração e salvá-la. Em caso afirmativo, introduza `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita este procedimento para o interrutor B do Cisco Nexus

Ative as funcionalidades avançadas

Certos recursos avançados devem ser ativados no Cisco NX-os para fornecer opções de configuração adicionais. Para habilitar os recursos apropriados no switch A e no switch B do Cisco Nexus, entre no modo de configuração usando o comando (config t) e execute os seguintes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

O hash padrão de balanceamento de carga do canal de porta usa os endereços IP de origem e destino para determinar o algoritmo de balanceamento de carga entre as interfaces no canal de porta. Você pode obter uma melhor distribuição entre os membros do canal de porta fornecendo mais entradas para o algoritmo hash além dos endereços IP de origem e destino. Pela mesma razão, o NetApp recomenda fortemente adicionar as portas TCP de origem e destino ao algoritmo de hash.

No modo de configuração (config t), digite os seguintes comandos para definir a configuração de balanceamento de carga do canal de porta global no switch A e no switch B do Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Configure a árvore de expansão global

A plataforma Cisco Nexus usa um novo recurso de proteção chamado bridge Assurance. O Bridge Assurance ajuda a proteger contra uma ligação unidirecional ou outra falha de software com um dispositivo que continua a encaminhar o tráfego de dados quando não está mais a executar o algoritmo spanning-tree. As portas podem ser colocadas em um dos vários estados, incluindo rede ou borda, dependendo da plataforma.

A NetApp recomenda a configuração da garantia de ponte para que todas as portas sejam consideradas como portas de rede por padrão. Essa configuração força o administrador de rede a revisar a configuração de cada porta. Ele também revela os erros de configuração mais comuns, como portas de borda não identificadas ou um vizinho que não tenha o recurso de garantia de ponte ativado. Além disso, é mais seguro ter o bloco de árvore de expansão muitas portas em vez de muito poucas, o que permite que o estado de porta padrão aumente a estabilidade geral da rede.

Preste muita atenção ao estado spanning-tree ao adicionar servidores, armazenamento e switches uplink, especialmente se eles não suportarem a garantia de bridge. Nesses casos, talvez seja necessário alterar o tipo de porta para tornar as portas ativas.

A proteção da Unidade de dados do Protocolo de Ponte (BPDU) é ativada por padrão nas portas de borda como outra camada de proteção. Para evitar loops na rede, esse recurso desliga a porta se BPDUs de outro switch forem vistos nessa interface.

A partir do modo de configuração (config t), execute os seguintes comandos para configurar as opções de spanning tree padrão, incluindo o tipo de porta padrão e a proteção BPDU, no switch Cisco Nexus A e no switch B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
ntp server <<var_ntp_ip>> use-vrf management
ntp master 3
```

Defina as VLANs

Antes que portas individuais com VLANs diferentes sejam configuradas, as VLANs de camada 2 devem ser definidas no switch. Também é uma boa prática nomear as VLANs para facilitar a solução de problemas no futuro.

No modo de configuração (config t), execute os seguintes comandos para definir e descrever as VLANs de camada 2 no switch A e no switch B do Cisco Nexus:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurar descrições de portas de acesso e gerenciamento

Como acontece com a atribuição de nomes às VLANs de camada 2, as descrições de configuração para todas as interfaces podem ajudar no provisionamento e na solução de problemas.

A partir do modo de configuração (config t) em cada um dos switches, insira as seguintes descrições de porta para a configuração FlexPod Express Large:

Switch Cisco Nexus A

```
int eth1/1
  description AFF C190-A e0c
int eth1/2
  description AFF C190-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0 vSwitch0
int eth1/4
  description UCS-Server-B: MLOM port 0 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 1 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 1 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-B 1/25
int eth1/26
  description vPC peer-link 31108PC-V-B 1/26
int eth1/33
  description AFF C190-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Switch Cisco Nexus B

```
int eth1/1
  description AFF C190-A e0d
int eth1/2
  description AFF C190-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 2 vSwitch0
int eth1/4
description UCS-Server-B: MLOM port 2 vSwitch0
int eth1/5
  description UCS-Server-A: MLOM port 3 iScsiBootvSwitch
int eth1/6
  description UCS-Server-B: MLOM port 3 iScsiBootvSwitch
int eth1/25
  description vPC peer-link 31108PC-V-A 1/25
int eth1/26
  description vPC peer-link 31108PC-V-A 1/26
int eth1/33
  description AFF C190-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Configurar interfaces de gerenciamento de storage e servidor

As interfaces de gerenciamento para o servidor e o storage normalmente usam apenas uma única VLAN. Portanto, configure as portas da interface de gerenciamento como portas de acesso. Defina a VLAN de gerenciamento para cada switch e altere o tipo de porta spanning-tree para Edge.

No modo de configuração (config t), digite os seguintes comandos para configurar as configurações de porta para as interfaces de gerenciamento dos servidores e do armazenamento:

Switch Cisco Nexus A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Execute a configuração global do canal de porta virtual

Um canal de porta virtual (VPC) permite que os links fisicamente conetados a dois switches Cisco Nexus diferentes apareçam como um canal de porta única para um terceiro dispositivo. O terceiro dispositivo pode ser um switch, servidor ou qualquer outro dispositivo de rede. Uma VPC pode fornecer multipathing de camada 2, o que permite criar redundância aumentando a largura de banda, habilitando vários caminhos paralelos entre nós e o tráfego de balanceamento de carga onde existem caminhos alternativos.

Uma VPC oferece os seguintes benefícios:

- Ativar um único dispositivo para usar um canal de porta em dois dispositivos upstream
- Eliminando portas bloqueadas do protocolo spanning-tree
- Fornecendo uma topologia sem loop
- Usando toda a largura de banda de uplink disponível
- Fornecendo convergência rápida se o link ou um dispositivo falhar
- Fornecer resiliência no nível de link
- Ajudando a fornecer alta disponibilidade

O recurso VPC requer alguma configuração inicial entre os dois switches Cisco Nexus para funcionar corretamente. Se você usar a configuração back-to-back mgmt0, use os endereços definidos nas interfaces e

verifique se eles podem se comunicar usando o `ping <<switch_A/B_mgmt0_ip_addr>>vrf` comando Management.

No modo de configuração (config t), execute os seguintes comandos para configurar a configuração global da VPC para ambos os switches:

Switch Cisco Nexus A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf
management
peer-switch
peer-gateway
auto-recovery
delay restore 150
ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Switch Cisco Nexus B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  delay-restore 150
   ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configure os canais da porta de armazenamento

Os controladores de armazenamento NetApp permitem uma conexão ativo-ativo à rede usando o protocolo de controle de agregação de link (LACP). O uso do LACP é preferido porque adiciona negociação e Registro entre os switches. Como a rede está configurada para VPC, essa abordagem permite que você tenha conexões ativo-ativo do armazenamento para switches físicos separados. Cada controlador tem dois links para cada um dos switches. No entanto, todos os quatro links fazem parte do mesmo VPC e grupo de interface (ifgrp).

A partir do modo de configuração (config t), execute os seguintes comandos em cada um dos switches para configurar as interfaces individuais e a configuração de canal de porta resultante para as portas conetadas ao controlador NetApp AFF.

1. Execute os seguintes comandos no interrutor A e no interrutor B para configurar os canais de porta para o controlador de armazenamento A:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Execute os seguintes comandos no interrutor A e no interrutor B para configurar os canais de porta para o controlador de armazenamento B:

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

Configure as conexões do servidor

Os servidores Cisco UCS têm uma placa de interface virtual de quatro portas, VIC1457, que é usada para tráfego de dados e inicialização do sistema operacional ESXi usando iSCSI. Essas interfaces são configuradas para fazer failover entre si, proporcionando redundância adicional além de um único link. Espalhar esses links por vários switches permite que o servidor sobreviva até mesmo a uma falha completa do switch.

No modo de configuração (config t), execute os seguintes comandos para configurar as configurações de porta para as interfaces conetadas a cada servidor.

Switch Cisco Nexus A: Configuração do servidor Cisco UCS-A e do servidor Cisco UCS-B.

```
int eth1/5
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Switch Cisco B: Configuração do Cisco UCS Server-A e do Cisco UCS Server-B.

```
int eth1/6
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Configure os canais da porta do servidor

Execute os seguintes comandos no switch A e no switch B para configurar os canais de porta para o Server-A:

```
int eth1/3
  channel-group 13 mode active
int Po13
  description vPC to Server-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 13
  no shut
```

Execute os seguintes comandos no switch A e no switch B para configurar os canais de porta para o Server-B:

```
int eth1/4
  channel-group 14 mode active
int Po14
  description vPC to Server-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_id>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 14
  no shut
```

Uma MTU de 9000 foi utilizada na validação desta solução. No entanto, você pode configurar um valor diferente para o MTU apropriado para os requisitos do aplicativo. É importante definir o mesmo valor MTU na solução FlexPod. Configurações incorretas de MTU entre componentes resultam em pacotes sendo descartados e esses pacotes precisarão ser transmitidos novamente, afetando o desempenho geral da solução.

Para escalar a solução adicionando servidores Cisco UCS adicionais, execute os comandos anteriores com as portas de switch às quais os servidores recém-adicionados foram conetados nos switches A e B.

Uplink em uma infra-estrutura de rede existente

Dependendo da infraestrutura de rede disponível, vários métodos e recursos podem ser usados para uplink o ambiente FlexPod. Se um ambiente Cisco Nexus existente estiver presente, a NetApp recomenda o uso de VPCs para uplink os switches Cisco Nexus 31108 incluídos no ambiente FlexPod na infraestrutura. Os uplinks

podem ser 10GbE uplinks para uma solução de infraestrutura 10GbE ou 1GbE para uma solução de infraestrutura 1GbE, se necessário. Os procedimentos descritos anteriormente podem ser usados para criar uma VPC uplink no ambiente existente. Certifique-se de executar o copy start para salvar a configuração em cada switch depois que a configuração for concluída.

"Próximo: Procedimento de implantação de storage do NetApp (parte 1)."

Procedimento de implantação de storage do NetApp (parte 1)

Esta seção descreve o procedimento de implantação de storage do NetApp AFF.

Instalação da série AFF C190 do controlador de storage NetApp

NetApp Hardware Universe

O aplicativo NetApp Hardware Universe (HWU) fornece componentes de hardware e software suportados para qualquer versão específica do ONTAP. Ele fornece informações de configuração para todos os dispositivos de storage NetApp atualmente compatíveis com o software ONTAP. Ele também fornece uma tabela de compatibilidades de componentes.

Confirme se os componentes de hardware e software que você gostaria de usar são suportados com a versão do ONTAP que você pretende instalar:

Acesse o "HWU" aplicativo para exibir os guias de configuração do sistema. Clique na guia Controladores para exibir a compatibilidade entre diferentes versões do software ONTAP e os dispositivos de armazenamento NetApp com as especificações desejadas.

Como alternativa, para comparar componentes por dispositivo de armazenamento, clique em comparar sistemas de armazenamento.

Pré-requisitos da Série Controller AFFC190
Para Planejar a localização física dos sistemas de storage, consulte o NetApp Hardware Universe. Consulte as seguintes secções: • Requisitos elétricos • Cabos de energia compatíveis • Portas e cabos integrados

Controladores de storage

Siga os procedimentos de instalação física dos controladores na Documentação do AFF "C190".

NetApp ONTAP 9,6

Folha de cálculo de configuração

Antes de executar o script de configuração, conclua a Planilha de configuração no manual do produto. A Planilha de configuração está disponível no Guia de configuração do software ONTAP 9.6.

Este sistema é configurado em uma configuração de cluster sem switch de dois nós.

A tabela a seguir fornece as informações de instalação e configuração do ONTAP 9.6.

Detalhe do cluster	Valor de detalhe do cluster
Nó de cluster Um endereço IP	"Cliente <var_nodeA_mgmt_ip>>
Cluster node Uma máscara de rede	"Cliente <var_nodeA_mgmt_mask>>
Nó de cluster A gateway	"Cliente <var_nodeA_mgmt_gateway>>
Nome do nó do cluster	"Cliente <var_nodeA>>
Endereço IP do nó B do cluster	"Cliente <var_nodeB_mgmt_ip>>
Nó de cluster B netmask	"Cliente <var_nodeB_mgmt_mask>>
Gateway do nó B do cluster	"Cliente <var_nodeB_mgmt_gateway>>
Nome B do nó do cluster	"Cliente <var_nodeB>>
URL do ONTAP 9.6	"cliente <var_url_boot_software>>
Nome do cluster	"cliente <var_clustername>>
Endereço IP de gerenciamento de cluster	"cliente <var_clustermgmt_ip>>
Gateway do cluster B.	"cliente <var_clustermgmt_gateway>>
Cluster B netmask	"cliente <var_clustermgmt_mask>>
Nome de domínio	"cliente <var_domain_name>>
IP do servidor DNS (pode introduzir mais de um)	o que é que você está procurando
IP do servidor NTP (pode introduzir mais de um)	"cliente <var_ntp_server_ip>>

Configure o nó A

Para configurar o nó A, execute as seguintes etapas:

1. Conete-se à porta do console do sistema de armazenamento. Você deve ver um prompt Loader-A. No entanto, se o sistema de armazenamento estiver em um loop de reinicialização, pressione Ctrl-C para sair do loop autoboot quando você vir esta mensagem:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

   Permita que o sistema inicialize.

   ```
   autoboot
   ```

2. Pressione Ctrl-C para entrar no menu Boot (Inicialização).

   Se o ONTAP 9.6 não for a versão do software que está sendo inicializada, continue com as etapas a seguir para instalar o novo software. Se o ONTAP 9.6 for a versão que está sendo inicializada, selecione a opção 8 e y para reinicializar o nó. Em seguida, continue com o passo 14.

3. Para instalar um novo software, selecione a opção 7.
4. Introduza y para efetuar uma atualização.
5. Selecione e0M para a porta de rede que pretende utilizar para a transferência.
6. Introduza y para reiniciar agora.
7. Introduza o endereço IP, a máscara de rede e o gateway predefinido para e0M nos respetivos locais.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

8. Introduza a URL onde o software pode ser encontrado.

Este servidor Web deve ser pingável.

```
<<var_url_boot_software>>
```

9. Pressione Enter para o nome de usuário, indicando nenhum nome de usuário.
10. Introduza y para definir o software recém-instalado como o padrão a ser utilizado para reinicializações subsequentes.
11. Introduza y para reiniciar o nó.

Ao instalar um novo software, o sistema pode executar atualizações de firmware para o BIOS e placas adaptadoras, causando reinicializações e possíveis paradas no prompt do Loader-A. Se estas acões ocorrerem, o sistema poderá desviar-se deste procedimento.

12. Pressione Ctrl-C para entrar no menu Boot (Inicialização).
13. Selecione a opção 4 para Configuração limpa e Inicializar todos os discos.
14. Insira y para zero discos, redefina a configuração e instale um novo sistema de arquivos.
15. Introduza y para apagar todos os dados nos discos.

A inicialização e a criação do agregado raiz podem levar 90 minutos ou mais para ser concluída, dependendo do número e do tipo de discos anexados. Quando a inicialização estiver concluída, o sistema de armazenamento reinicializa. Note que os SSDs demoram consideravelmente menos tempo para inicializar. Você pode continuar com a configuração do nó B enquanto os discos do nó A estão zerando.

Enquanto o nó A estiver inicializando, comece a configurar o nó B.

Configurar nó B

Para configurar o nó B, execute as seguintes etapas:

1. Conete-se à porta do console do sistema de armazenamento. Você deve ver um prompt Loader-A. No entanto, se o sistema de armazenamento estiver em um loop de reinicialização, pressione Ctrl-C para sair do loop autoboot quando você vir esta mensagem:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Pressione Ctrl-C para entrar no menu Boot (Inicialização).

```
autoboot
```

3. Pressione Ctrl-C quando solicitado.

> Se o ONTAP 9.6 não for a versão do software que está sendo inicializada, continue com as etapas a seguir para instalar o novo software. Se o ONTAP 9.6 for a versão que está sendo inicializada, selecione a opção 8 e y para reinicializar o nó. Em seguida, continue com o passo 14.

4. Para instalar um novo software, selecione a opção 7.a..
5. Introduza y para efetuar uma atualização.
6. Selecione e0M para a porta de rede que pretende utilizar para a transferência.
7. Introduza y para reiniciar agora.
8. Introduza o endereço IP, a máscara de rede e o gateway predefinido para e0M nos respetivos locais.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Introduza a URL onde o software pode ser encontrado.

> Este servidor Web deve ser pingável.

```
<<var_url_boot_software>>
```

10. Pressione Enter para o nome de usuário, indicando nenhum nome de usuário.
11. Introduza y para definir o software recém-instalado como o padrão a ser utilizado para reinicializações subsequentes.
12. Introduza y para reiniciar o nó.

> Ao instalar um novo software, o sistema pode executar atualizações de firmware para o BIOS e placas adaptadoras, causando reinicializações e possíveis paradas no prompt do Loader-A. Se estas acões ocorrerem, o sistema poderá desviar-se deste procedimento.

13. Pressione Ctrl-C para entrar no menu Boot (Inicialização).
14. Selecione a opção 4 para Configuração limpa e Inicializar todos os discos.
15. Insira y para zero discos, redefina a configuração e instale um novo sistema de arquivos.
16. Introduza y para apagar todos os dados nos discos.

A inicialização e a criação do agregado raiz podem levar 90 minutos ou mais para ser concluída, dependendo do número e do tipo de discos anexados. Quando a inicialização estiver concluída, o sistema de armazenamento reinicializa. Note que os SSDs demoram consideravelmente menos tempo para inicializar.

Continuação do nó A configuração e configuração de cluster

A partir de um programa de porta de console conetado à porta de console do controlador de storage A (nó A), execute o script de configuração do nó. Este script aparece quando o ONTAP 9.6 é inicializado no nó pela primeira vez.

O procedimento de configuração do nó e do cluster mudou ligeiramente no ONTAP 9.6. O assistente de configuração do cluster agora é usado para configurar o primeiro nó em um cluster, e o Gerenciador de sistema do NetApp ONTAP (antigo Gerenciador de sistema do OnCommand) é usado para configurar o cluster.

1. Siga as instruções para configurar o nó A..

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Navegue até o endereço IP da interface de gerenciamento do nó.

> A configuração do cluster também pode ser realizada usando a CLI. Este documento descreve a configuração do cluster utilizando a configuração guiada do System Manager.

3. Clique em Configuração Guiada para configurar o cluster.
4. Introduza `<<var_clustername>>` o nome do cluster e `<<var_nodeA>>` e `<<var_nodeB>>` para cada um dos nós que está a configurar. Introduza a palavra-passe que pretende utilizar para o sistema de armazenamento. Selecione cluster sem switch para o tipo de cluster. Introduza a licença base do cluster.
5. Você também pode inserir licenças de recursos para Cluster, NFS e iSCSI.
6. Você verá uma mensagem de status informando que o cluster está sendo criado. Esta mensagem de estado passa por vários Estados. Este processo demora vários minutos.
7. Configure a rede.
   a. Desmarque a opção IP Address Range (intervalo de endereços IP).

b. Introduza `<<var_clustermgmt_ip>>` no campo Endereço IP de gestão de clusters, `<<var_clustermgmt_mask>>` no campo Máscara de rede e `<<var_clustermgmt_gateway>>` no campo Gateway. Use o seletor… no campo porta para selecionar e0M do nó A.

c. O IP de gerenciamento do Nó para o nó A já está preenchido. Introduza `<<var_nodeA_mgmt_ip>>` para o nó B.

d. Introduza `<<var_domain_name>>` no campo DNS Domain Name (Nome de domínio DNS). Introduza `<<var_dns_server_ip>>` no campo Endereço IP do servidor DNS.

> Você pode inserir vários endereços IP do servidor DNS.

e. Introduza `10.63.172.162` no campo servidor NTP principal.

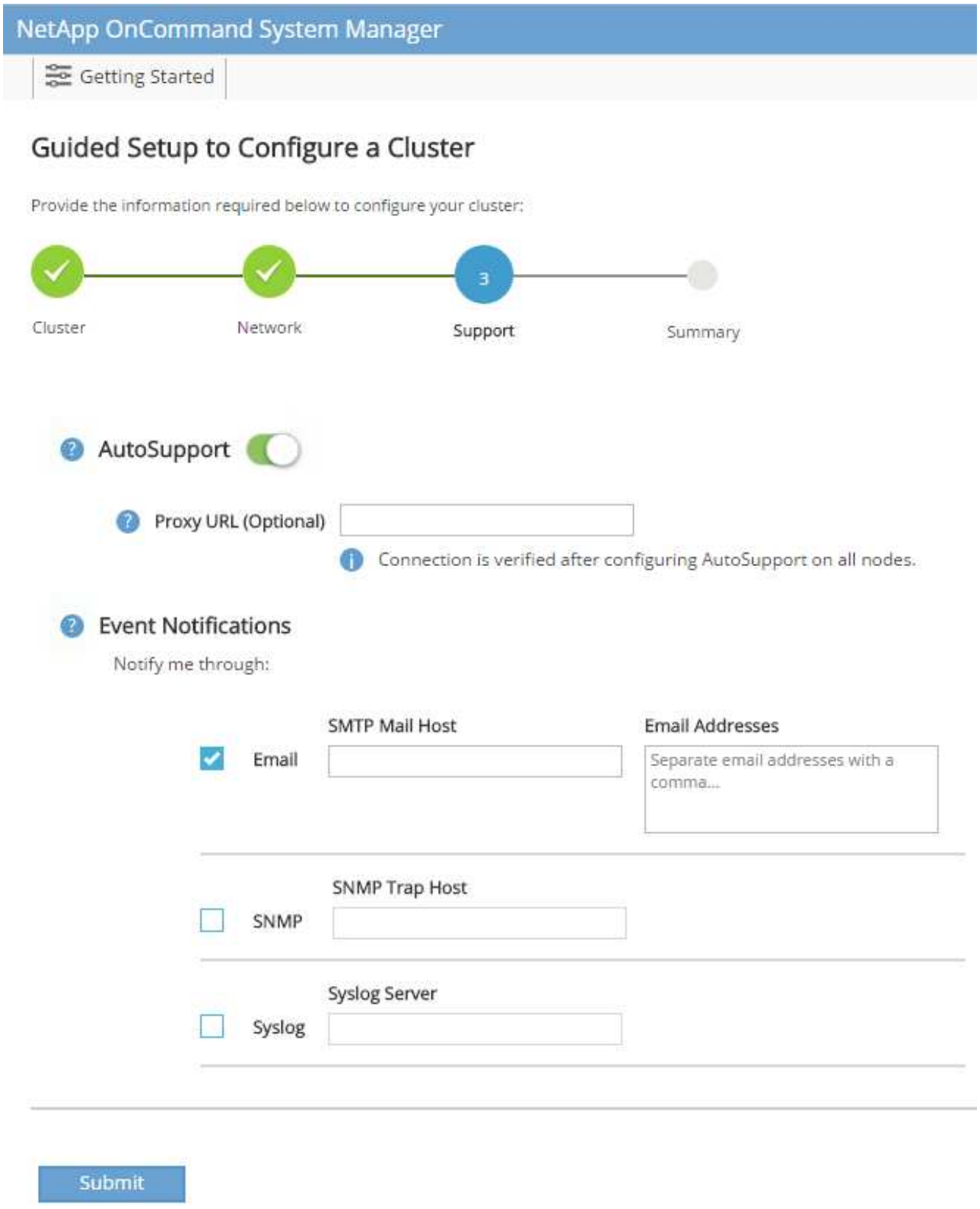
> Você também pode inserir um servidor NTP alternativo. O endereço IP `10.63.172.162` de `<<var_ntp_server_ip>>` é o Nexus Mgmt IP.

8. Configure as informações de suporte.

a. Se o seu ambiente exigir um proxy para acessar o AutoSupport, insira o URL no URL do proxy.

b. Insira o host de e-mail SMTP e o endereço de e-mail para notificações de eventos.

> Você deve, no mínimo, configurar o método de notificação de evento antes de prosseguir. Você pode selecionar qualquer um dos métodos.



Quando o sistema indicar que a configuração do cluster foi concluída, clique em Gerenciar seu cluster para configurar o armazenamento.

Continuação da configuração do cluster de armazenamento

Após a configuração dos nós de storage e do cluster base, você pode continuar com a configuração do cluster de storage.

Zero todos os discos sobressalentes

Para zerar todos os discos sobressalentes no cluster, execute o seguinte comando:

```
disk zerospares
```

Defina a personalidade de UTA2 portas a bordo

1. Verifique o modo atual e o tipo atual das portas executando o `ucadmin show` comando.

```
AFF C190::> ucadmin show
                      Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF C190_A     0c       cna       target     -        -          online
AFF C190_A     0d       cna       target     -        -          online
AFF C190_A     0e       cna       target     -        -          online
AFF C190_A     0f       cna       target     -        -          online
AFF C190_B     0c       cna       target     -        -          online
AFF C190_B     0d       cna       target     -        -          online
AFF C190_B     0e       cna       target     -        -          online
AFF C190_B     0f       cna       target     -        -          online
8 entries were displayed.
```

2. Verifique se o modo atual das portas que estão em uso é cna e se o tipo atual está definido como destino. Caso contrário, altere a personalidade da porta usando o seguinte comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

> As portas devem estar offline para executar o comando anterior. Para colocar uma porta off-line, execute o seguinte comando:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

> Se você alterou a personalidade da porta, será necessário reinicializar cada nó para que a alteração tenha efeito.

Renomeie as interfaces lógicas de gerenciamento

Para renomear as interfaces lógicas de gerenciamento (LIFs), execute as seguintes etapas:

1. Mostrar os nomes de LIF de gerenciamento atuais.

```
network interface show –vserver <<clustername>>
```

2. Renomeie o LIF de gerenciamento de cluster.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Renomeie o nó B Management LIF.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF C190_B_1 -newname AFF C190-02_mgmt1
```

Defina a reversão automática no gerenciamento de cluster

Defina o parâmetro de reversão automática na interface de gerenciamento de cluster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configure a interface de rede do processador de serviço

Para atribuir um endereço IPv4 estático ao processador de serviço em cada nó, execute os seguintes comandos:

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Os endereços IP do processador de serviço devem estar na mesma sub-rede que os endereços IP de gerenciamento de nós.

Ativar failover de storage no ONTAP

Para confirmar se o failover de armazenamento está ativado, execute os seguintes comandos em um par de failover:

1. Verifique o status do failover de storage.

```
storage failover show
```

> Ambos <<var_nodeA>> e <<var_nodeB>> devem ser capazes de realizar uma aquisição. Vá para a etapa 3 se os nós puderem executar um takeover.

2. Habilite o failover em um dos dois nós.

```
storage failover modify -node <<var_nodeA>> -enabled true
```

> A ativação do failover em um nó permite a TI para ambos os nós.

3. Verifique o status de HA do cluster de dois nós.

> Esta etapa não se aplica a clusters com mais de dois nós.

```
cluster ha show
```

4. Vá para a etapa 6 se a alta disponibilidade estiver configurada. Se a alta disponibilidade estiver configurada, você verá a seguinte mensagem ao emitir o comando:

```
High Availability Configured: true
```

5. Ative o modo HA apenas para o cluster de dois nós.

> Não execute este comando para clusters com mais de dois nós porque causa problemas com failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Verifique se a assistência ao hardware está corretamente configurada e, se necessário, modifique o endereço IP do parceiro.

```
storage failover hwassist show
```

> A mensagem `Keep Alive Status: Error:` indica que um dos controladores não recebeu alertas hwassist Keep Alive de seu parceiro, indicando que a assistência de hardware não está configurada. Execute os seguintes comandos para configurar a assistência de hardware.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Crie um domínio de transmissão MTU de quadro jumbo no ONTAP

Para criar um domínio de transmissão de dados com uma MTU de 9000, execute os seguintes comandos:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Remova as portas de dados do domínio de broadcast padrão

As portas de dados 10GbE são usadas para tráfego iSCSI/NFS e essas portas devem ser removidas do domínio padrão. As portas e0e e e0f não são usadas e também devem ser removidas do domínio padrão.

Para remover as portas do domínio de broadcast, execute o seguinte comando:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Desative o controle de fluxo nas portas UTA2

É uma prática recomendada do NetApp desativar o controle de fluxo em todas as UTA2 portas conetadas a dispositivos externos. Para desativar o controle de fluxo, execute o seguinte comando:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

Configure o grupo de interfaces LACP no ONTAP

Esse tipo de grupo de interfaces requer duas ou mais interfaces Ethernet e um switch que suporte LACP. Certifique-se de que ele esteja configurado com base nas etapas deste guia na seção 5,1.

No prompt do cluster, execute as seguintes etapas:

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Configure os quadros jumbo no ONTAP

Para configurar uma porta de rede ONTAP para usar quadros jumbo (geralmente com um MTU de 9.000 bytes), execute os seguintes comandos a partir do shell do cluster:

```
AFF C190::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF C190::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Crie VLANs no ONTAP

Para criar VLANs no ONTAP, execute as seguintes etapas:

1. Crie portas VLAN NFS e adicione-as ao domínio de transmissão de dados.

   ```
   network port vlan create –node <<var_nodeA>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   network port vlan create –node <<var_nodeB>> -vlan-name a0a-
   <<var_nfs_vlan_id>>
   broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
   <<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
   <<var_nfs_vlan_id>>
   ```

2. Crie portas iSCSI VLAN e adicione-as ao domínio de transmissão de dados.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>,<<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. Crie portas MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Criar agregados de dados no ONTAP

Um agregado contendo o volume raiz é criado durante o processo de configuração do ONTAP. Para criar agregados adicionais, determine o nome do agregado, o nó no qual criá-lo e o número de discos que ele contém.

Para criar agregados, execute os seguintes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Guarde pelo menos um disco (selecione o disco maior) na configuração como um sobressalente. Uma prática recomendada é ter pelo menos um sobressalente para cada tipo e tamanho de disco.

Comece com cinco discos; você pode adicionar discos a um agregado quando for necessário armazenamento adicional.

O agregado não pode ser criado até que a restauração do disco seja concluída. Execute o `aggr show` comando para exibir o status de criação agregada. Não prossiga até que aggr1_nodeA esteja online.

Configure o fuso horário no ONTAP

Para configurar a sincronização de hora e definir o fuso horário no cluster, execute o seguinte comando:

```
timezone <<var_timezone>>
```

Por exemplo, no leste dos Estados Unidos, o fuso horário é America/New_York. Depois de começar a digitar o nome do fuso horário, pressione a tecla Tab para ver as opções disponíveis.

Configurar SNMP no ONTAP

Para configurar o SNMP, execute as seguintes etapas:

1. Configurar informações básicas do SNMP, como a localização e o contacto. Quando polled, esta informação é visível como `sysLocation` as variáveis e `sysContact` no SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Configurar traps SNMP para enviar para hosts remotos.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Configure o SNMPv1 no ONTAP

Para configurar o SNMPv1, defina a senha secreta compartilhada de texto simples chamada comunidade.

```
snmp community add ro <<var_snmp_community>>
```

Use o `snmp community delete all` comando com cuidado. Se strings de comunidade forem usadas para outros produtos de monitoramento, esse comando as removerá.

Configure o SNMPv3 no ONTAP

SNMPv3 requer que você defina e configure um usuário para autenticação. Para configurar o SNMPv3, execute as seguintes etapas:

1. Execute o `security snmpusers` comando para visualizar a ID do motor.

2. Crie um usuário `snmpv3user` chamado .

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduza a ID do motor da entidade autorizada e selecione md5 como o protocolo de autenticação.
4. Insira uma senha de comprimento mínimo de oito carateres para o protocolo de autenticação quando solicitado.
5. Selecione des como o protocolo de privacidade.
6. Insira uma senha de comprimento mínimo de oito carateres para o protocolo de privacidade quando solicitado.

Configure o HTTPS do AutoSupport no ONTAP

A ferramenta NetApp AutoSupport envia informações resumidas de suporte para o NetApp por meio de HTTPS. Para configurar o AutoSupport, execute o seguinte comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Crie uma máquina virtual de armazenamento

Para criar uma máquina virtual de storage de infraestrutura (SVM), siga estas etapas:

1. Executar o `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Adicione o agregado de dados à lista de agregados de infraestrutura SVM para o VSC do NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Remova os protocolos de storage não utilizados da SVM, deixando NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite e execute o protocolo NFS no SVM de infraestrutura.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Ative o `SVM vstorage` parâmetro para o plug-in NetApp NFS VAAI. Em seguida, verifique se o NFS foi configurado.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Os comandos são pré-enfrentados `vserver` na linha de comando porque SVMs eram anteriormente chamados de VServers.

Configure o NFSv3 no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
ESXi Hospeda Um endereço IP NFS	"Cliente <var_esxi_hostA_nfs_ip>>
Endereço IP NFS do host ESXi B.	"Cliente <var_esxi_hostB_nfs_ip>>

Para configurar o NFS na SVM, execute os seguintes comandos:

1. Crie uma regra para cada host ESXi na política de exportação padrão.
2. Para cada host ESXi sendo criado, atribua uma regra. Cada host tem seu próprio índice de regras. Seu primeiro host ESXi tem o índice de regra 1, seu segundo host ESXi tem o índice de regra 2, e assim por diante.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Atribua a política de exportação ao volume raiz da infraestrutura SVM.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

O VSC do NetApp manipula automaticamente as políticas de exportação se você optar por instalá-las após a configuração do vSphere. Se você não instalá-lo, você deve criar regras de política de exportação quando servidores adicionais da série C do Cisco UCS forem adicionados.

Crie o serviço iSCSI no ONTAP

Para criar o serviço iSCSI na SVM, execute o seguinte comando. Esse comando também inicia o serviço iSCSI e define o IQN iSCSI para o SVM. Verifique se o iSCSI foi configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Criar espelho de compartilhamento de carga do volume raiz da SVM no ONTAP

Para criar um espelhamento de compartilhamento de carga do volume raiz do SVM no ONTAP, siga estas etapas:

1. Crie um volume para ser o espelhamento de compartilhamento de carga do volume raiz da infraestrutura SVM em cada nó.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. Crie uma agenda de trabalhos para atualizar as relações de espelho de volume raiz a cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Crie as relações de espelhamento.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Inicialize a relação de espelhamento e verifique se ela foi criada.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Configurar o acesso HTTPS no ONTAP

Para configurar o acesso seguro ao controlador de armazenamento, execute as seguintes etapas:

1. Aumente o nível de privilégio para acessar os comandos do certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. Geralmente, um certificado auto-assinado já está em vigor. Verifique o certificado executando o seguinte comando:

```
security certificate show
```

3. Para cada SVM mostrado, o nome comum do certificado deve corresponder ao FQDN DNS do SVM. Os quatro certificados predefinidos devem ser suprimidos e substituídos por certificados auto-assinados ou certificados de uma autoridade de certificação.

> Excluir certificados expirados antes de criar certificados é uma prática recomendada. Execute o `security certificate delete` comando para excluir certificados expirados. No comando a seguir, use conclusão de TABULAÇÃO para selecionar e excluir cada certificado padrão.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Para gerar e instalar certificados autoassinados, execute os seguintes comandos como comandos únicos. Gerar um certificado de servidor para a infraestrutura SVM e o cluster SVM. Novamente, use TAB Completion para ajudar a completar esses comandos.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 3650 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obter os valores para os parâmetros necessários na etapa a seguir, execute o comando security certificate show.
6. Ative cada certificado que acabou de ser criado usando os `-server-enabled true` parâmetros e. `-client-enabled false` Novamente, use A conclusão DA GUIA.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configure e ative o acesso SSL e HTTPS e desative o acesso HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

> É normal que alguns desses comandos retornem uma mensagem de erro informando que a entrada não existe.

8. Reverta para o nível de privilégio de administrador e crie a configuração para permitir que o SVM esteja disponível pela Web.

```
set -privilege admin
vserver services web modify -name spi -vserver * -enabled true
```

Crie um NetApp FlexVol volume no ONTAP

Para criar um volume NetApp FlexVol, insira o nome do volume, o tamanho e o agregado no qual ele existe. Crie dois volumes do VMware datastore e um volume de inicialização do servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore -aggregate
aggr1_nodeB -size 500GB -state online -policy default -junction-path
/infra_datastore -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
-efficiency-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Criar LUNs no ONTAP

Para criar dois LUNs de inicialização, execute os seguintes comandos:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Ao adicionar um servidor Cisco UCS C-Series extra, você deve criar um LUN de inicialização extra.

Criar iSCSI LIFs no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
Nó de storage A iSCSI LIF01A	"Cliente <var_nodeA_iscsi_lif01a_ip>>
Nó de armazenamento Uma máscara de rede iSCSI LIF01A	"Cliente <var_nodeA_iscsi_lif01a_mask>>
Nó de storage A iSCSI LIF01B	"Cliente <var_nodeA_iscsi_lif01b_ip>>
Nó de armazenamento Uma máscara de rede iSCSI LIF01B	"Cliente <var_nodeA_iscsi_lif01b_mask>>
Nó de storage B iSCSI LIF01A	"Cliente <var_nodeB_iscsi_lif01a_ip>>
Máscara de rede do nó de armazenamento B iSCSI LIF01A	"Cliente <var_nodeB_iscsi_lif01a_mask>>
Nó de storage B iSCSI LIF01B	"Cliente <var_nodeB_iscsi_lif01b_ip>>
Máscara de rede do nó de armazenamento B iSCSI LIF01B	"Cliente <var_nodeB_iscsi_lif01b_mask>>

Crie quatro LIFs iSCSI, dois em cada nó.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy disabled
–firewall-policy data –auto-revert false
network interface show
```

Criar LIFs NFS no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
Nó de storage A NFS LIF 01 IP	"Cliente <var_nodeA_nfs_lif_01_ip>>
Nó de storage Uma máscara de rede NFS LIF 01	"Cliente <var_nodeA_nfs_lif_01_mask>>
Nó de storage B NFS LIF 02 IP	"Cliente <var_nodeB_nfs_lif_02_ip>>
Máscara de rede do nó de storage B NFS LIF 02	"Cliente <var_nodeB_nfs_lif_02_mask>>

Criar um NFS LIF.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Adicionar um administrador de infraestrutura SVM

A tabela a seguir lista as informações necessárias para adicionar um administrador SVM.

Detalhe	Valor do detalhe
IP Vsmgmt	"cliente <var_svm_mgmt_ip>>
Máscara de rede Vsmgmt	"cliente <var_svm_mgmt_mask>>
Gateway padrão Vsmgmt	"cliente <var_svm_mgmt_gateway>>

Para adicionar a interface lógica de administração do SVM e administrador de infraestrutura à rede de gerenciamento, siga estas etapas:

1. Execute o seguinte comando:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> O IP de gerenciamento do SVM deve estar na mesma sub-rede que o IP de gerenciamento do cluster de storage.

2. Crie uma rota padrão para permitir que a interface de gerenciamento SVM alcance o mundo externo.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Defina uma senha para o usuário SVM vsadmin e desbloqueie o usuário.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"Próximo: Implantar o servidor de rack Cisco UCS C-Series."

Implante o servidor de rack Cisco UCS C-Series

Esta seção fornece um procedimento detalhado para a configuração de um servidor de rack autônomo do Cisco UCS C-Series para uso na configuração do FlexPod Express.

Execute a configuração inicial do servidor autônomo do Cisco UCS C-Series para CIMC

Conclua estas etapas para a configuração inicial da interface CIMC para servidores autônomos do Cisco UCS C-Series.

A tabela a seguir lista as informações necessárias para configurar o CIMC para cada servidor autônomo do Cisco UCS C-Series.

Detalhe	Valor do detalhe
Endereço IP CIMC	"cliente <cimc_ip>>
Máscara de sub-rede CIMC	a máscara de rede do cliente
Gateway padrão CIMC	"cliente <cimc_gateway>>

A versão CIMC utilizada nesta validação é o CIMC 4,0.(4).

Todos os servidores

1. Conete o teclado Cisco, vídeo e dongle do Mouse (KVM) (fornecido com o servidor) à porta KVM na parte frontal do servidor. Ligue um monitor VGA e um teclado USB às portas de dongle KVM apropriadas.

   Ligue o servidor e pressione F8 quando solicitado a inserir a configuração do CIMC.

2. No utilitário de configuração CIMC, defina as seguintes opções:
   a. Modo de placa de interface de rede (NIC):

      Dedicado `[X]`

   b. IP (básico):

      IPV4: `[X]`

      DHCP ativado: `[ ]`

      IP CIMC: `<<cimc_ip>>`

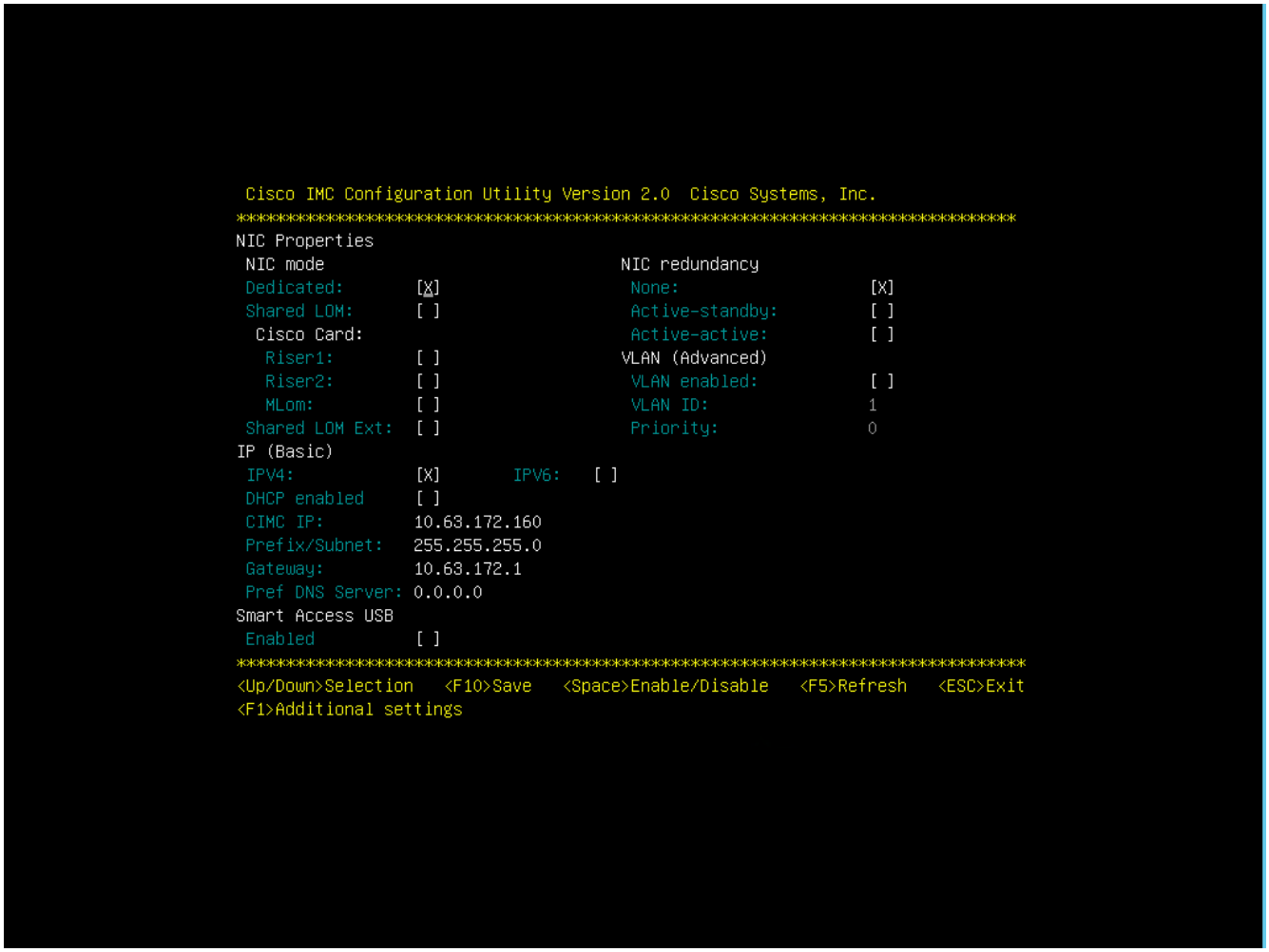
      Prefixo/sub-rede: `<<cimc_netmask>>`

      Gateway: `<<cimc_gateway>>`

   c. VLAN (Avançado): Deixe limpo para desativar a marcação de VLAN.

      Redundância de NIC

      Nenhum: `[X]`



3. Pressione F1 para ver as configurações adicionais:
   a. Propriedades comuns:

      Nome do anfitrião: `<<esxi_host_name>>`

      DNS dinâmico: `[ ]`

      Predefinições de fábrica: Deixe limpo.

   b. Utilizador predefinido (básico):

      Palavra-passe predefinida: `<<admin_password>>`

      Reintroduza a palavra-passe: `<<admin_password>>`

      Propriedades da porta: Use valores padrão.

   Perfis de porta: Deixe limpo.
4. Pressione F10 para salvar a configuração da interface CIMC.
5. Depois de guardar a configuração, prima ESC para sair.

Configurar a inicialização iSCSI dos servidores Cisco UCS C-Series

Nesta configuração do FlexPod Express, o VIC1457 é usado para inicialização iSCSI.

A tabela a seguir lista as informações necessárias para configurar a inicialização iSCSI.

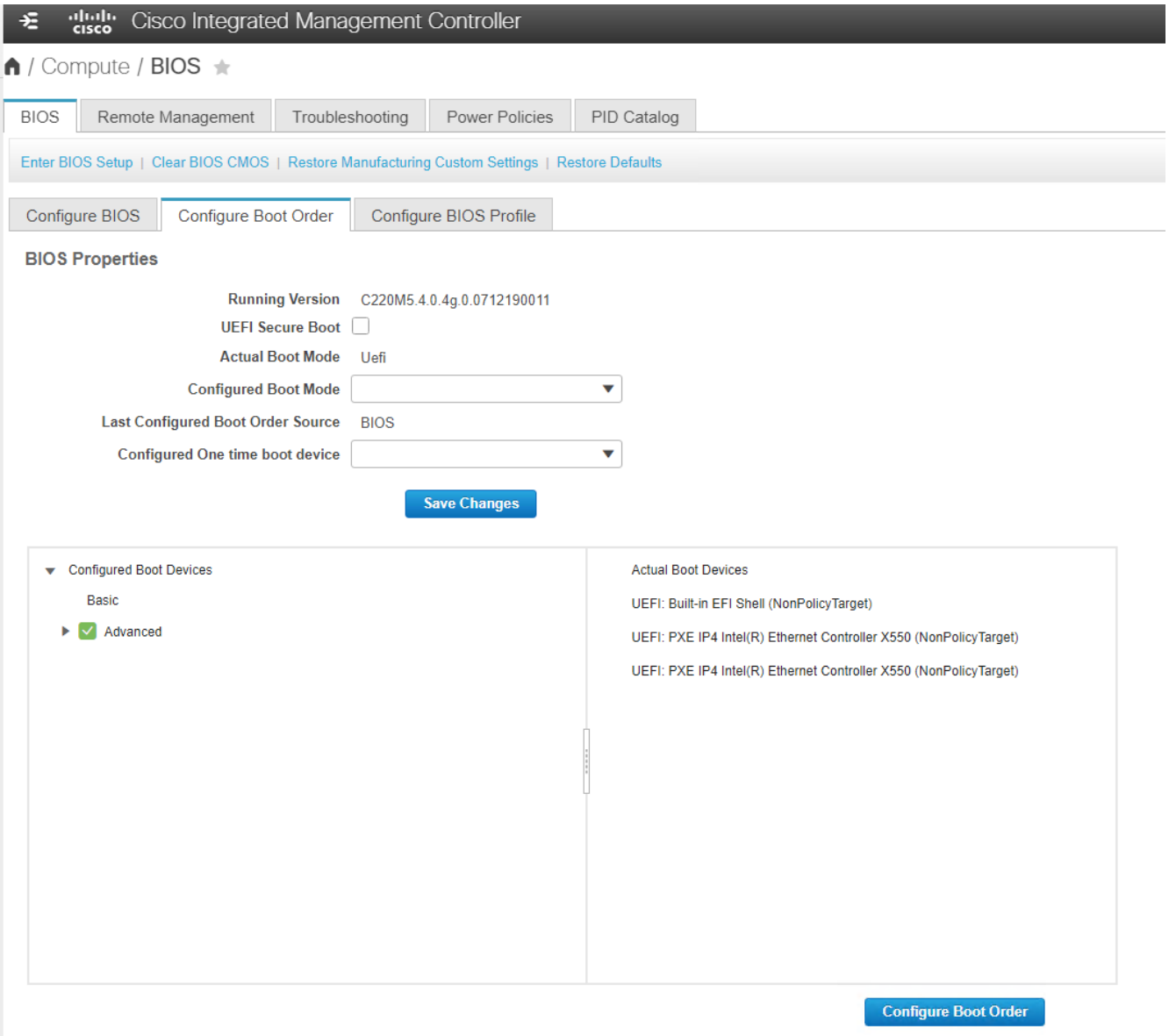
Uma fonte em itálico indica variáveis que são exclusivas para cada host ESXi.

Detalhe	Valor do detalhe
Nome do iniciador do host ESXi	"Cliente <var_ucs_initiator_name_A>>
IP iSCSI-A do host ESXi	"Cliente <var_esxi_host_iscsiA_ip>>
Máscara de rede iSCSI-A. do host ESXi	"Cliente <var_esxi_host_iscsiA_mask>>
ESXi host Iscsi Um gateway padrão	"Cliente <var_esxi_host_iscsiA_gateway>>
Nome B do iniciador do host ESXi	"Cliente <var_ucs_initiator_name_B>>
IP iSCSI-B do host ESXi	"Cliente <var_esxi_host_iscsiB_ip>>
Máscara de rede iSCSI-B. do host ESXi	"Cliente <var_esxi_host_iscsiB_mask>>
Gateway iSCSI-B. do host ESXi	"Cliente <var_esxi_host_iscsiB_gateway>>
Endereço ip iSCSI_lif01a	"cliente <var_iscsi_lif01a>>
Endereço ip iSCSI_lif02a	"cliente <var_iscsi_lif02a>>
Endereço ip iSCSI_lif01b	"cliente <var_iscsi_lif01b>>
Endereço ip iSCSI_lif02b	"cliente <var_iscsi_lif02b>>
Infraestrutura_SVM IQN	"Cliente <var_SVM_IQN>>

Configuração da ordem de inicialização

Para definir a configuração da ordem de inicialização, execute as seguintes etapas:

1. Na janela do navegador da interface CIMC, clique na guia Compute (calcular) e selecione BIOS.
2. Clique em Configurar ordem de inicialização e, em seguida, clique em OK.



3. Configure os seguintes dispositivos clicando no dispositivo em Adicionar dispositivo de inicialização e indo para a guia Avançado:

   a. Adicionar suporte virtual:

      NOME: KVM-CD-DVD

      SUBTIPO: KVM MAPEADO DVD

      Estado: Ativado

      Pedido mínimo: 1

   b. Adicionar arranque iSCSI:

      Nome: ISCSI-A.

      Estado: Ativado

      Pedido mínimo: 2

Slot: MLOM

Porta: 1

c. Clique em Add iSCSI Boot (Adicionar iSCSI Boot):

Nome: ISCSI-B

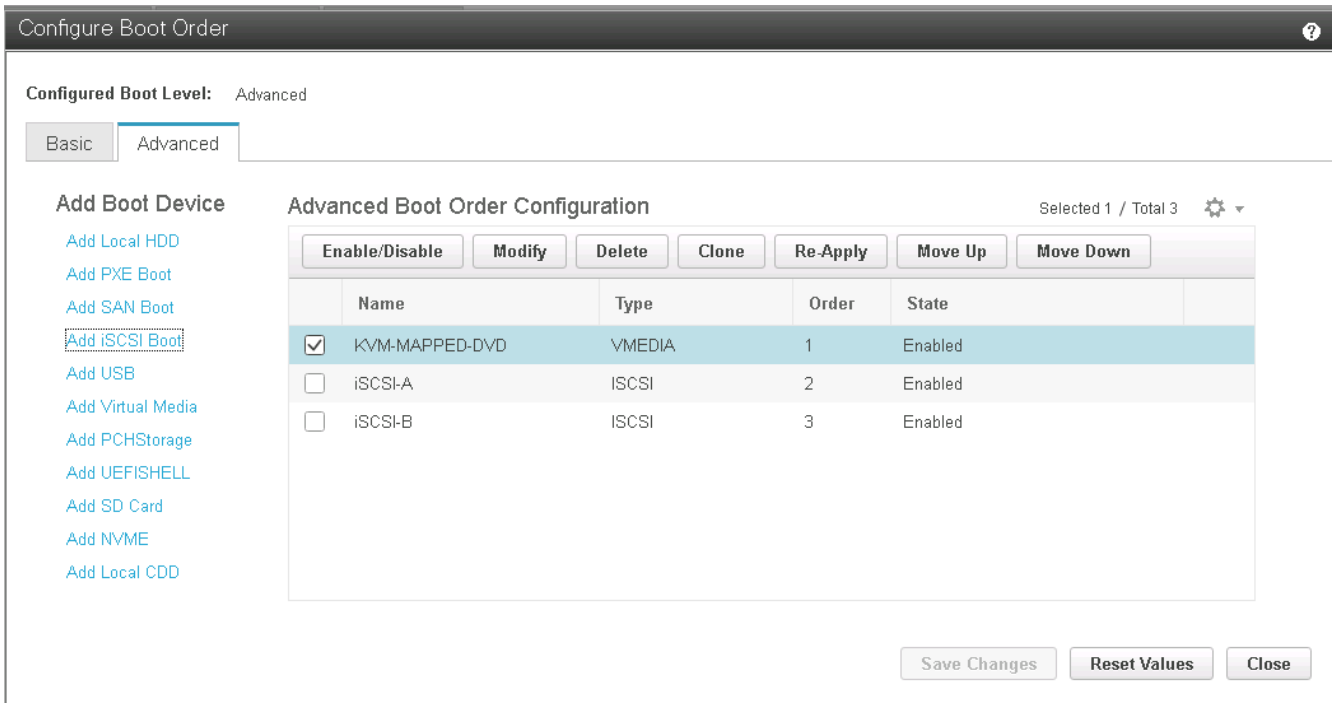
Estado: Ativado

Pedido mínimo: 3

Slot: MLOM

Porta: 3

4. Clique em Adicionar dispositivo.
5. Clique em Salvar alterações e, em seguida, clique em Fechar.

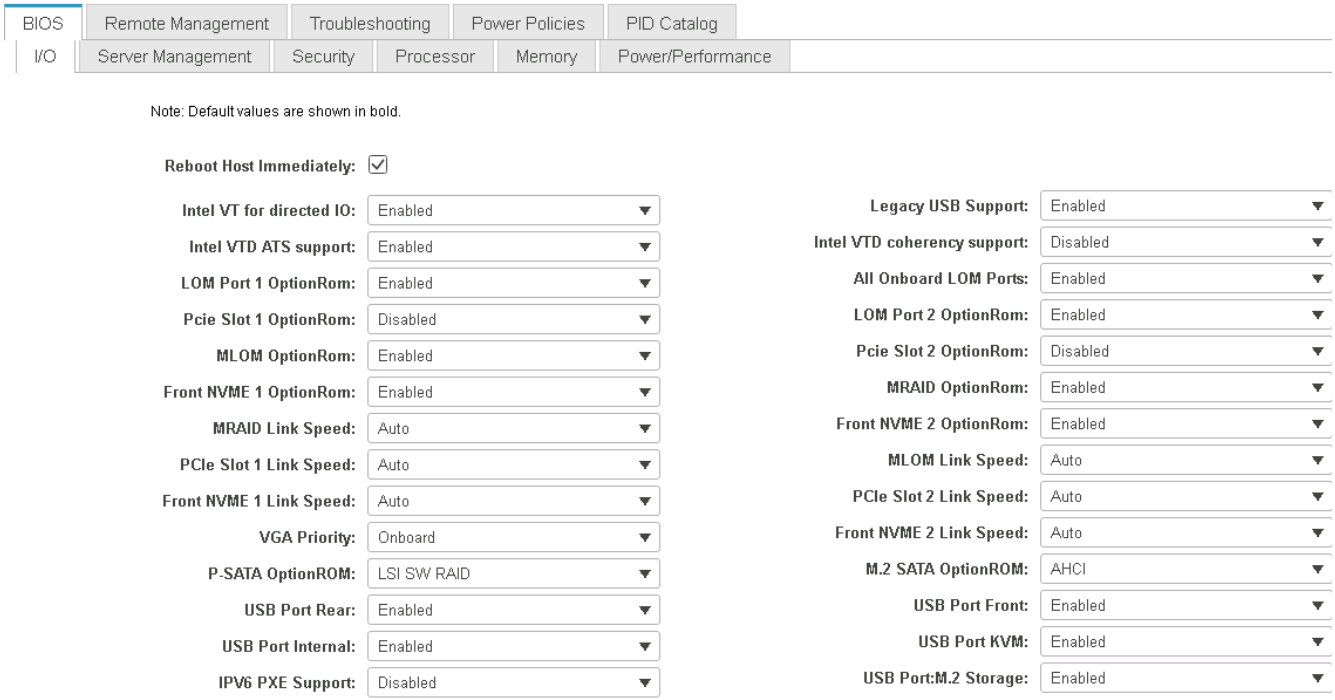


6. Reinicie o servidor para inicializar com sua nova ordem de inicialização.

Desativar o controlador RAID (se presente)

Siga as etapas a seguir se o servidor C-Series contiver um controlador RAID. Não é necessário um controlador RAID na inicialização a partir da configuração SAN. Opcionalmente, você também pode remover fisicamente o controlador RAID do servidor.

1. Na guia Compute (calcular), clique em BIOS no painel de navegação esquerdo do CIMC.
2. Selecione Configurar BIOS.
3. Role para baixo até slot PCIe:ROM de opção HBA.
4. Se o valor ainda não estiver desativado, defina-o como desativado.

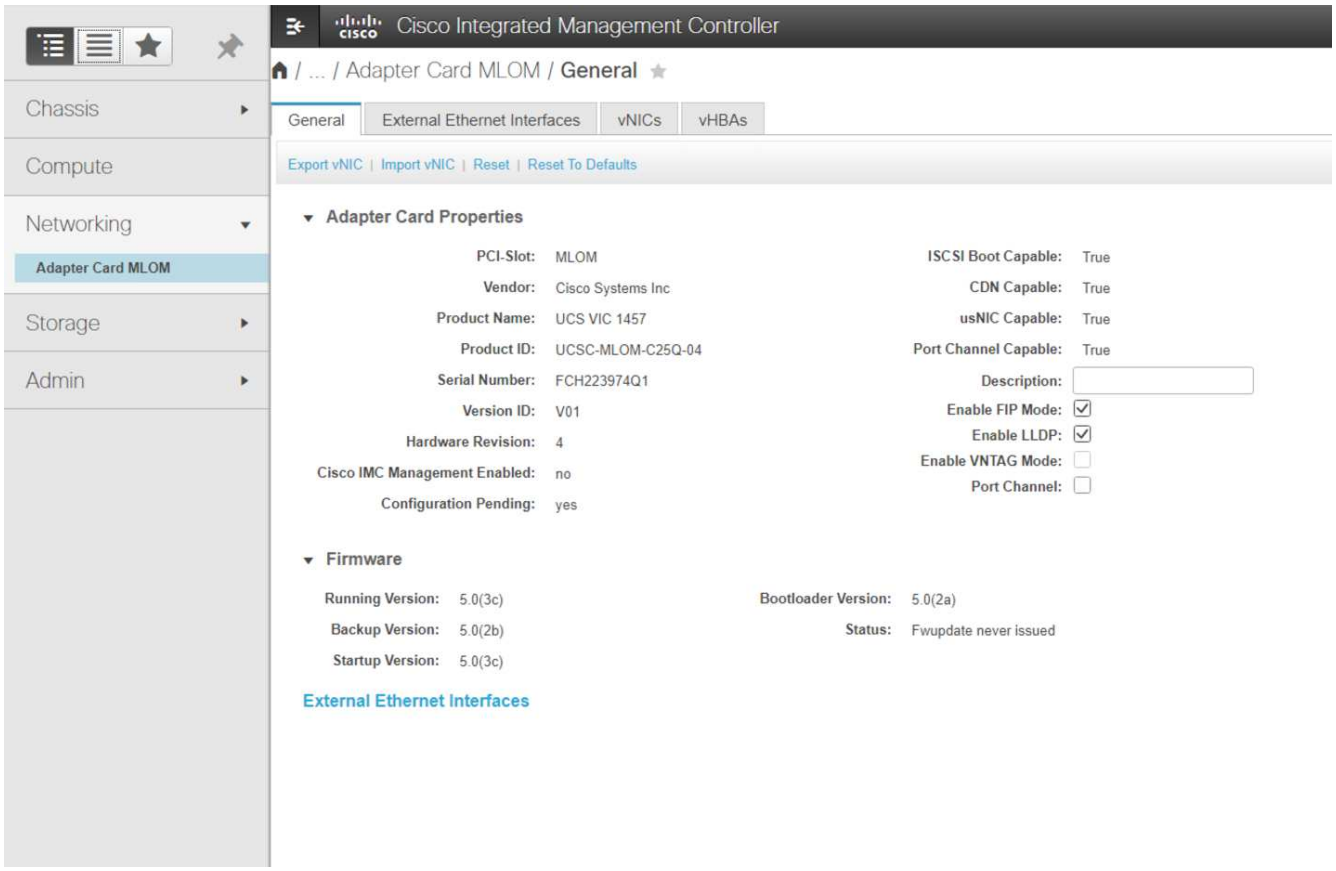


Configurar o Cisco VIC1457 para inicialização iSCSI

Os seguintes passos de configuração são para o Cisco VIC 1457 para arranque iSCSI.

> A canalização de portas padrão entre as portas 0, 1, 2 e 3 deve ser desligada antes que as quatro portas individuais possam ser configuradas. Se a canalização da porta não estiver desligada, apenas duas portas aparecem para o VIC 1457. Execute as etapas a seguir para ativar o canal de porta no CIMC:

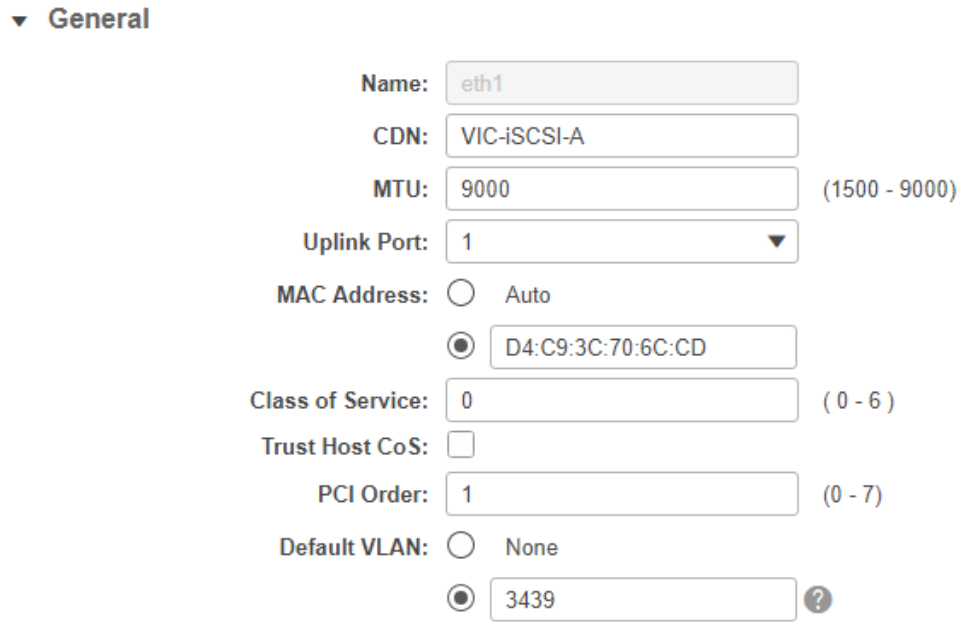
1. Na guia rede, clique no cartão adaptador MLOM.
2. Na guia Geral, desmarque o canal da porta.
3. Salve as alterações e reinicie o CIMC.



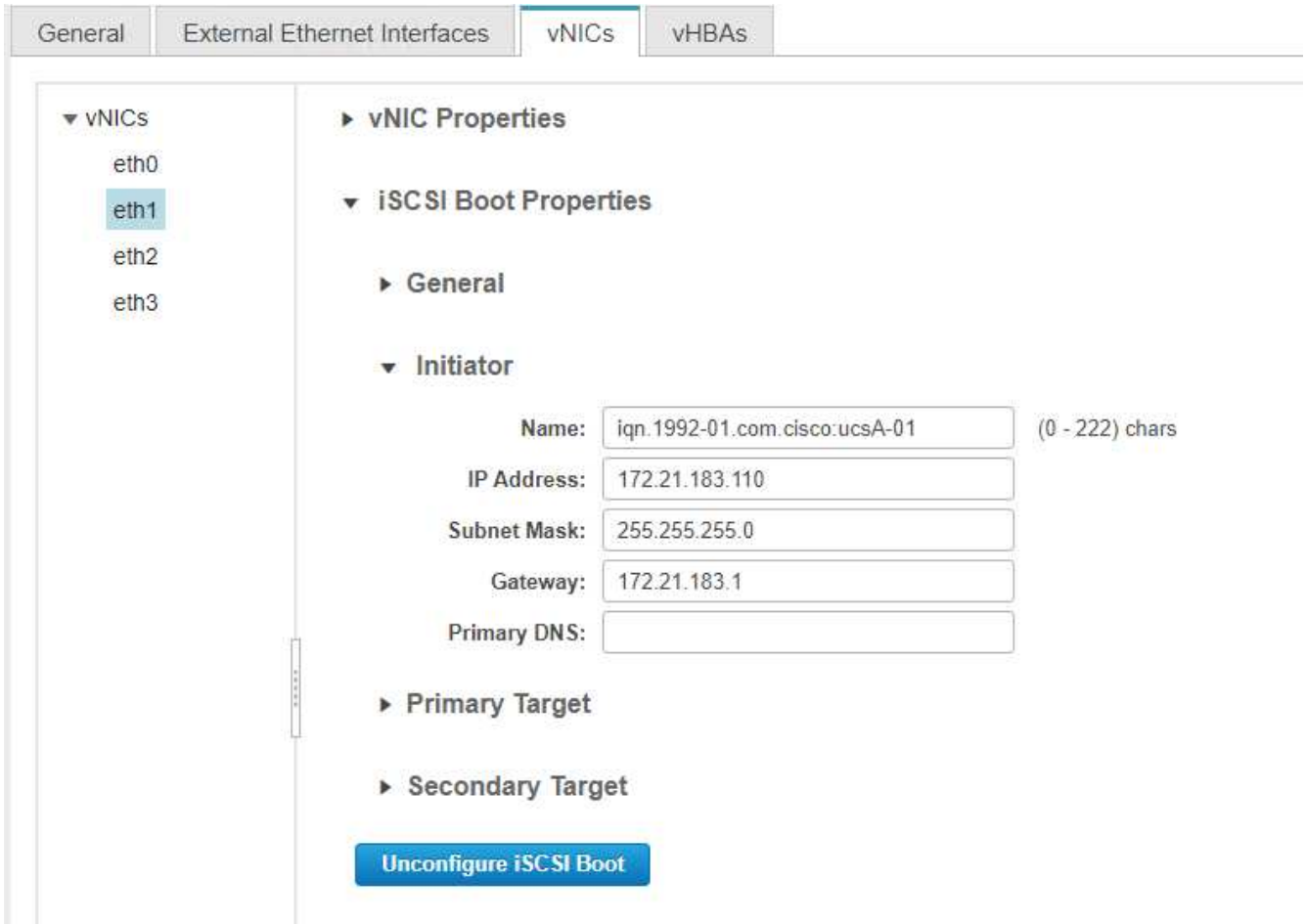
Criar iSCSI vNICs

Para criar iSCSI vNICs, execute as seguintes etapas:

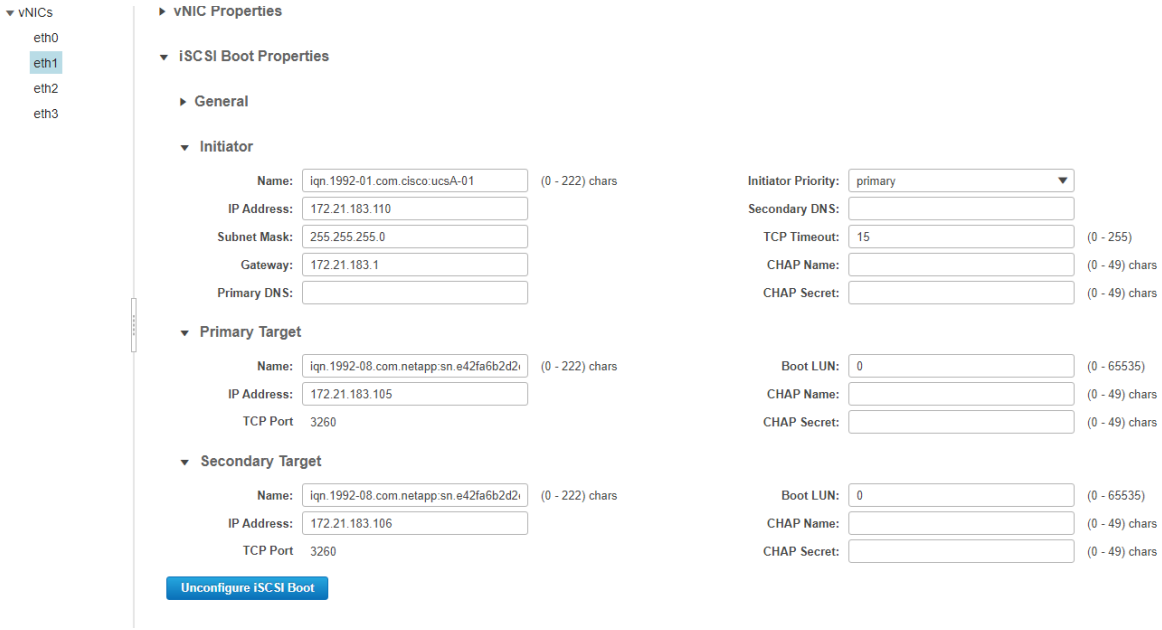
1. Na guia rede, clique em placa de adaptador MLOM.
2. Clique em Adicionar vNIC para criar um vNIC.
3. Na seção Adicionar vNIC, insira as seguintes configurações:
   - Nome: eth1
   - Nome CDN: ISCSI-vNIC-A
   - MTU: 9000
   - VLAN predefinida: `<<var_iscsi_vlan_a>>`
   - Modo VLAN: TRONCO
   - Ativar arranque PXE: Verificar
4. Clique em Adicionar vNIC e, em seguida, clique em OK.
5. Repita o processo para adicionar um segundo vNIC:
   - Nomeie o vNIC eth3.
   - Nome CDN: ISCSI-vNIC-B
   - `<<var_iscsi_vlan_b>>`Insira como VLAN.
   - Defina a porta de uplink como 3.



6. Selecione o vNIC eth1 à esquerda.



7. Em Propriedades de inicialização iSCSI, insira os detalhes do iniciador:
   - Nome: `<<var_ucsa_initiator_name_a>>`
   - Endereço IP: `<<var_esxi_hostA_iscsiA_ip>>`
   - Máscara de sub-rede: `<<var_esxi_hostA_iscsiA_mask>>`
   - Gateway: `<<var_esxi_hostA_iscsiA_gateway>>`



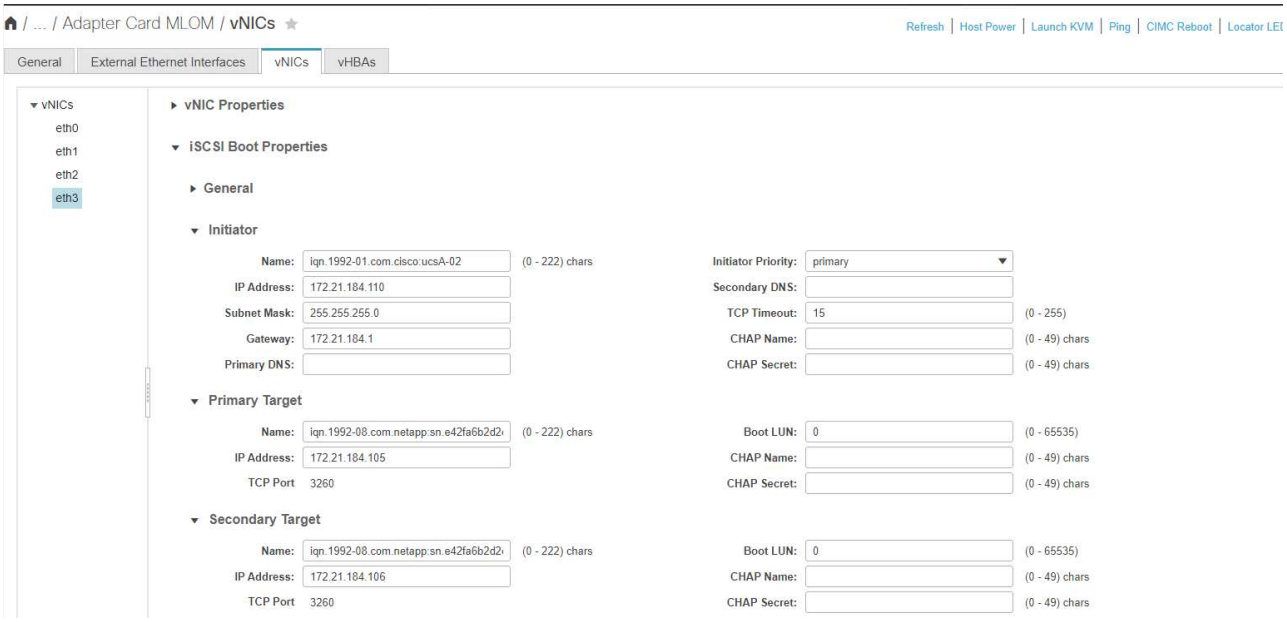
8. Introduza os detalhes do alvo principal:
   - Nome: IQN número de infraestrutura SVM
   - Endereço IP: Endereço IP de iscsi_lif01a
   - LUN de arranque: 0
9. Introduza os detalhes do alvo secundário:
   - Nome: IQN número de infraestrutura SVM
   - Endereço IP: Endereço IP de iscsi_lif02a
   - LUN de arranque:0

> Você pode obter o número IQN de armazenamento executando o `vserver iscsi show` comando.

> Certifique-se de gravar os nomes IQN para cada vNIC. Você precisa deles para um passo posterior. Além disso, os nomes IQN para iniciadores devem ser exclusivos para cada servidor e para o iSCSI vNIC.

10. Clique em Salvar alterações.
11. Selecione o vNIC eth3 e clique no botão iSCSI Boot localizado na parte superior da seção interfaces Ethernet do host.
12. Repita o processo para configurar o eth3.

13. Introduza os detalhes do iniciador:
    - Nome: `<<var_ucsa_initiator_name_b>>`
    - Endereço IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Máscara de sub-rede: `<<var_esxi_hostb_iscsib_mask>>`
    - Gateway: `<<var_esxi_hostb_iscsib_gateway>>`



14. Introduza os detalhes do alvo principal:
    - Nome: IQN número de infraestrutura SVM
    - Endereço IP: Endereço IP de iscsi_lif01b
    - LUN de arranque: 0
15. Introduza os detalhes do alvo secundário:
    - Nome: IQN número de infraestrutura SVM
    - Endereço IP: Endereço IP de iscsi_lif02b
    - LUN de arranque: 0

> Você pode obter o número IQN de armazenamento usando o `vserver iscsi show` comando.

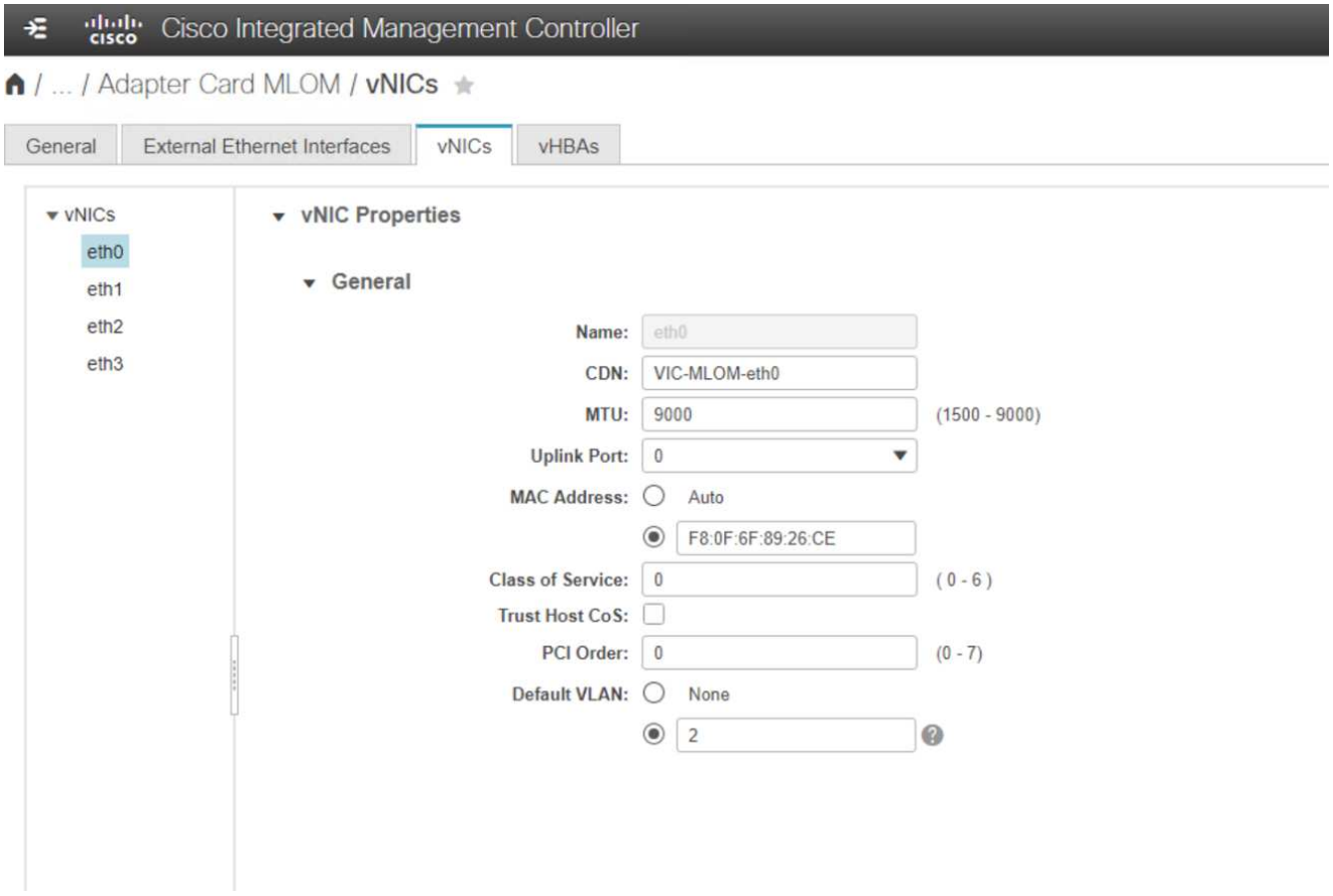
> Certifique-se de gravar os nomes IQN para cada vNIC. Você precisa deles para um passo posterior.

16. Clique em Salvar alterações.
17. Repita este processo para configurar a inicialização iSCSI para o servidor Cisco UCS B.

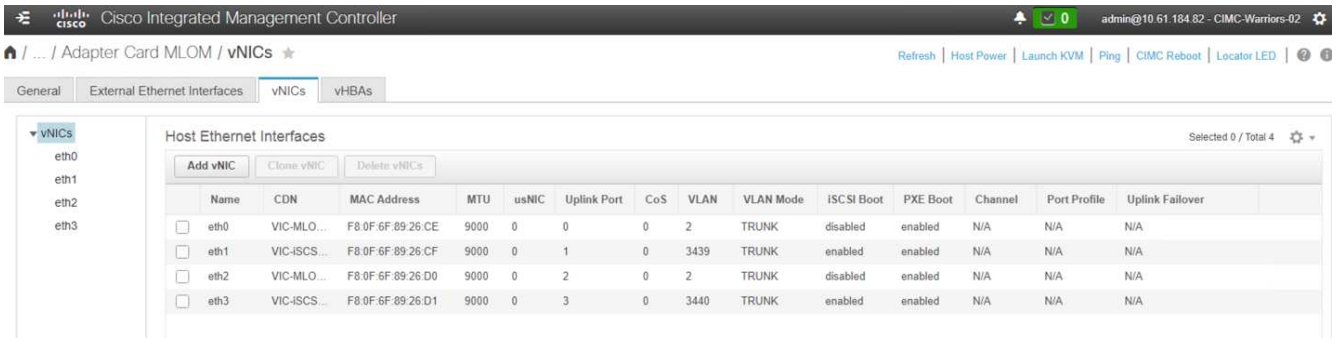
Configure vNICs para ESXi

Para configurar vNICs para ESXi, execute as seguintes etapas:

1. Na janela do navegador da interface CIMC, clique em Inventário e, em seguida, clique em adaptadores VIC Cisco no painel direito.
2. Em rede > placa de adaptador MLOM, selecione o separador vNICs e, em seguida, selecione os vNICs abaixo.
3. Selecione eth0 e clique em Propriedades.
4. Defina a MTU como 9000. Clique em Salvar alterações.
5. Defina a VLAN como VLAN nativa 2.



6. Repita as etapas 3 e 4 para eth1, verificando se a porta uplink está definida como 1 para eth1.



Esse procedimento deve ser repetido para cada nó inicial do servidor Cisco UCS e para cada nó adicional do servidor Cisco UCS adicionado ao ambiente.

"Próximo: Procedimento de implantação de storage do NetApp AFF (parte 2)."

Procedimento de implantação de storage do NetApp AFF (parte 2)

Configurar o armazenamento de arranque SAN ONTAP

Criar grupos iSCSI

Você precisa do iniciador iSCSI IQNs da configuração do servidor para esta etapa.

Para criar grupos, execute os seguintes comandos a partir da conexão SSH do nó de gerenciamento de cluster. Para ver os três grupos criados nesta etapa, execute o `igroup show` comando.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-
A_vNIC_IQN>>,<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Esta etapa deve ser concluída ao adicionar servidores Cisco UCS C-Series adicionais.

Mapeie LUNs de inicialização para grupos

```
To map boot LUNs to igroups, run the following commands from the cluster
management SSH connection:
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-A –igroup
VM-Host-Infra-A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra-B –igroup
VM-Host-Infra-B –lun-id 0
```

Esta etapa deve ser concluída ao adicionar servidores Cisco UCS C-Series adicionais.

"Próximo: Procedimento de implantação do VMware vSphere 6.7U2."

Procedimento de implantação do VMware vSphere 6.7U2

Esta seção fornece procedimentos detalhados para a instalação do VMware ESXi 6.7U2 em uma configuração do FlexPod Express. Os procedimentos de implantação a seguir são personalizados para incluir as variáveis de ambiente descritas nas seções anteriores.

Existem vários métodos para instalar o VMware ESXi em tal ambiente. Este procedimento usa o console KVM virtual e os recursos de Mídia virtual da interface CIMC para servidores Cisco UCS C-Series para mapear Mídia de instalação remota para cada servidor individual.

Esse procedimento deve ser concluído para o servidor A do Cisco UCS e o servidor B. do Cisco UCS

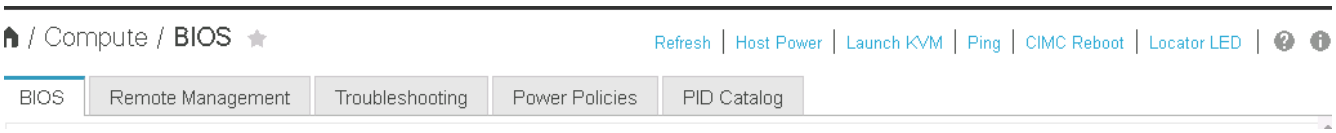
Este procedimento deve ser concluído para quaisquer nós adicionais adicionados ao cluster.

Faça login na interface CIMC para servidores autônomos do Cisco UCS C-Series

As etapas a seguir detalham o método para fazer login na interface CIMC para servidores autônomos do Cisco UCS C-Series. Você deve fazer login na interface CIMC para executar o KVM virtual, o que permite que o administrador inicie a instalação do sistema operacional por meio de Mídia remota.

Todos os anfitriões

1. Navegue até um navegador da Web e insira o endereço IP da interface CIMC para a série C do Cisco UCS. Esta etapa inicia o aplicativo GUI CIMC.
2. Faça login na IU do CIMC usando o nome de usuário e as credenciais do administrador.
3. No menu principal, selecione a guia servidor.
4. Clique em Launch KVM Console.



5. No console KVM virtual, selecione a guia Mídia virtual.
6. Selecione Map CD/DVD (CD/DVD de mapa).

Primeiro, você pode precisar clicar em Ativar dispositivos virtuais. Selecione aceitar esta sessão, se solicitado.

7. Navegue até o arquivo de imagem ISO do instalador do VMware ESXi 6.7U2 e clique em abrir. Clique em dispositivo de mapa.
8. Selecione o menu alimentação e selecione sistema de ciclo de alimentação (arranque a frio). Clique em Sim.

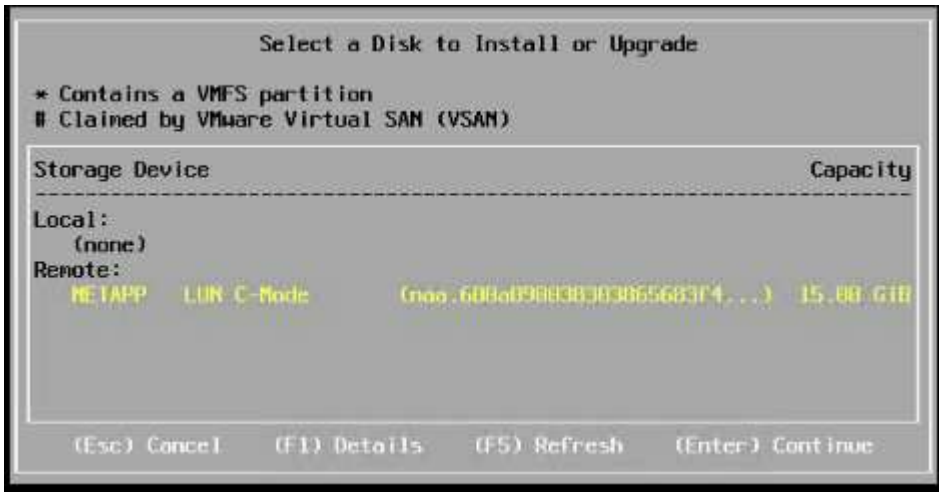
Instale o VMware ESXi

As etapas a seguir descrevem como instalar o VMware ESXi em cada host.

Faça o download da imagem personalizada do ESXI 6.7U2 Cisco

1. Navegue até a "Página de download do VMware vSphere" para ISOs personalizados.
2. Clique em ir para Downloads ao lado da imagem personalizada do Cisco para o CD de instalação do ESXi 6.7U2.
3. Faça o download da imagem personalizada do Cisco para o CD de instalação ESXi 6.7U2 (ISO).
4. Quando o sistema é inicializado, a máquina deteta a presença da Mídia de instalação do VMware ESXi.
5. Selecione o instalador do VMware ESXi no menu exibido. O instalador carrega, o que pode levar vários minutos.
6. Depois que o instalador terminar de carregar, pressione Enter para continuar com a instalação.
7. Depois de ler o contrato de licença do usuário final, aceite-o e continue com a instalação pressionando F11.

8. Selecione o LUN NetApp que foi configurado anteriormente como o disco de instalação do ESXi e pressione Enter para continuar com a instalação.



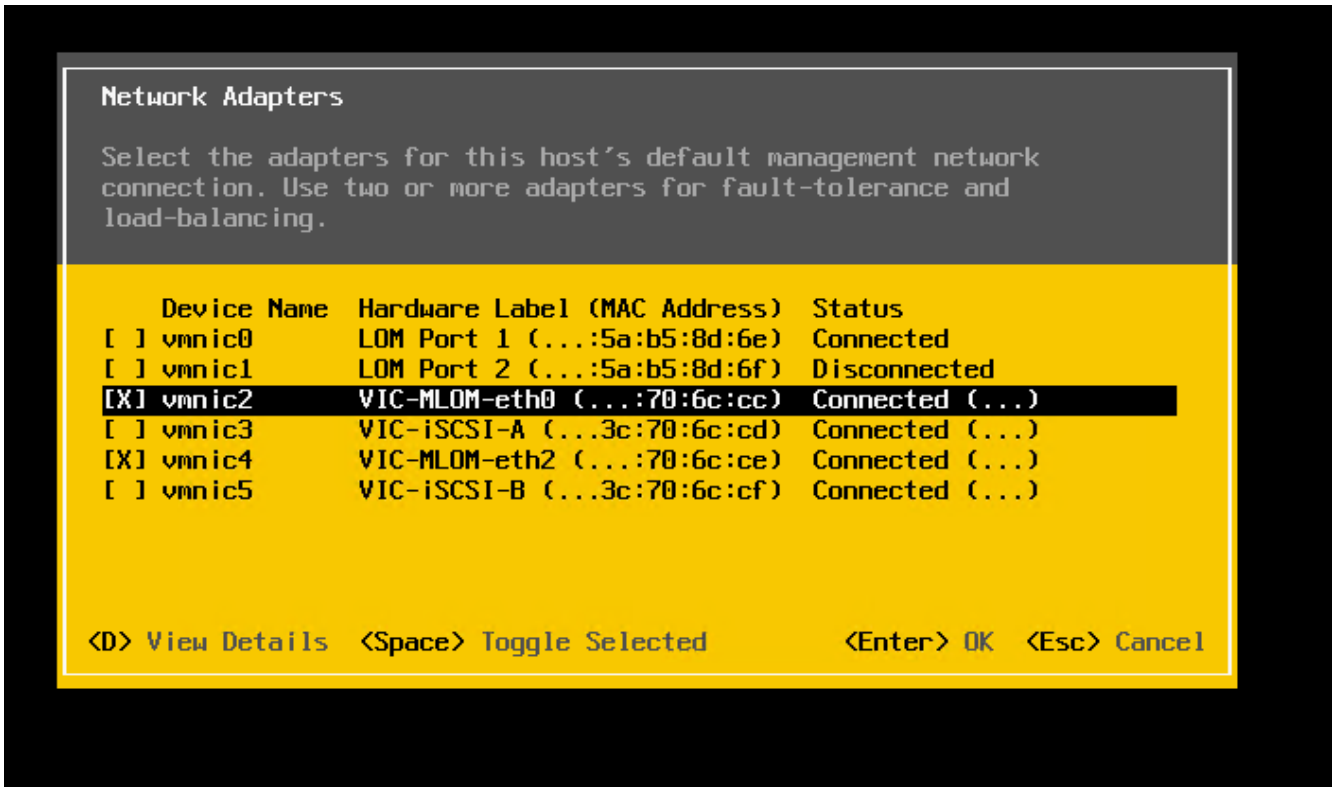
9. Selecione o layout do teclado apropriado e pressione Enter.
10. Introduza e confirme a palavra-passe de raiz e prima Enter.
11. O instalador avisa que as partições existentes são removidas no volume. Continue com a instalação pressionando F11. O servidor reinicializa após a instalação do ESXi.

Configurar a rede de gerenciamento de host VMware ESXi

As etapas a seguir descrevem como adicionar a rede de gerenciamento para cada host VMware ESXi.

Todos os anfitriões

1. Depois que o servidor terminar de reiniciar, digite a opção para personalizar o sistema pressionando F2.
2. Inicie sessão com root como o nome de início de sessão e a palavra-passe de raiz anteriormente introduzida durante o processo de instalação.
3. Selecione a opção Configurar rede de gerenciamento.
4. Selecione adaptadores de rede e pressione Enter.
5. Selecione as portas desejadas para vSwitch0. Prima Enter.
6. Selecione as portas que correspondem a eth0 e eth1 no CIMC.



7. Selecione VLAN (opcional) e pressione Enter.
8. Insira o ID da VLAN `<<mgmt_vlan_id>>` . Prima Enter.
9. No menu Configure Management Network (Configurar rede de gestão), selecione IPv4 Configuration (Configuração) para configurar o endereço IP da interface de gestão. Prima Enter.
10. Use as teclas de seta para realçar Set Static Address (Definir endereço estático IPv4) e use a barra de espaço para selecionar essa opção.
11. Insira o endereço IP para gerenciar o host VMware ESXi `<<esxi_host_mgmt_ip>>` .
12. Insira a máscara de sub-rede do host VMware ESXi `<<esxi_host_mgmt_netmask>>` .
13. Insira o gateway padrão do host VMware ESXi `<<esxi_host_mgmt_gateway>>` .
14. Pressione Enter para aceitar as alterações na configuração IP.
15. Aceder ao menu de configuração IPv6D.
16. Utilize a barra de espaço para desativar o IPv6 desmarcando a opção Ativar IPv6 (reiniciar necessário). Prima Enter.
17. Aceda ao menu para configurar as definições de DNS.
18. Como o endereço IP é atribuído manualmente, as informações de DNS também devem ser inseridas manualmente.
19. Introduza o endereço IP do servidor DNS primário `<<nameserver_ip>>` .
20. (Opcional) Introduza o endereço IP do servidor DNS secundário.
21. Digite o FQDN para o nome do host VMware ESXi: `<<esxi_host_fqdn>>`.
22. Pressione Enter para aceitar as alterações na configuração DNS.
23. Saia do submenu Configurar rede de gerenciamento pressionando ESC.
24. Pressione Y para confirmar as alterações e reinicializar o servidor.

25. Selecione Opções de solução de problemas e, em seguida, ative o Shell ESXi e o SSH.

> Essas opções de solução de problemas podem ser desativadas após a validação de acordo com a política de segurança do cliente.

26. Prima ESC duas vezes para regressar ao ecrã da consola principal.
27. Clique em Alt-F1 a partir do menu suspenso CIMC Macros > Macros estáticos > Alt-F na parte superior da tela.
28. Faça login com as credenciais apropriadas para o host ESXi.
29. No prompt, digite a seguinte lista de comandos esxcli sequencialmente para ativar a conetividade de rede.

```
esxcli network vswitch standard policy failover set -v vSwitch0 -a
vmnic2,vmnic4 -l iphash
```

Configurar o host ESXi

Use as informações na tabela a seguir para configurar cada host ESXi.

Detalhe	Valor do detalhe
Nome do host ESXi	"cliente <esxi_host_fqdn>>
IP de gerenciamento de host ESXi	"cliente <esxi_host_mgmt_ip>>
Máscara de gerenciamento de host ESXi	"cliente <esxi_host_mgmt_netmask>>
Gateway de gerenciamento de host ESXi	"cliente <esxi_host_mgmt_gateway>>
IP NFS do host ESXi	"Cliente <esxi_host_NFS_ip>>
Máscara NFS do host ESXi	"Cliente <esxi_host_NFS_netmask>>
Gateway NFS de host ESXi	"Cliente <esxi_host_NFS_gateway>>
ESXi host vMotion IP	"Cliente <esxi_host_vMotion_ip>>
Máscara ESXi host vMotion	"Cliente <esxi_host_vMotion_netmask>>
Gateway vMotion do host ESXi	"Cliente <esxi_host_vMotion_gateway>>
IP iSCSI-A do host ESXi	"Cliente <esxi_host_iSCSI-A_ip>>
Máscara iSCSI-A. do host ESXi	"Cliente <esxi_host_iSCSI-A_netmask>>
Gateway iSCSI-A. host ESXi	"Cliente <esxi_host_iSCSI-A_gateway>>
IP iSCSI-B do host ESXi	"Cliente <esxi_host_iSCSI-B_ip>>
Máscara do host ESXi iSCSI-B.	"Cliente <esxi_host_iSCSI-B_netmask>>
Gateway iSCSI-B. do host ESXi	"Cliente <esxi_host_SCSI-B_gateway>>

Faça login no host ESXi

Para fazer login no host ESXi, execute as seguintes etapas:

1. Abra o endereço IP de gerenciamento do host em um navegador da Web.
2. Faça login no host ESXi usando a conta raiz e a senha especificada durante o processo de instalação.
3. Leia a declaração sobre o Programa de Melhoramento da experiência do Cliente da VMware. Depois de selecionar a resposta adequada, clique em OK.

Configurar o arranque iSCSI

Para configurar a inicialização iSCSI, execute as seguintes etapas:

1. Selecione rede à esquerda.
2. À direita, selecione o separador Virtual switches (interrutores virtuais).

3. Clique em iScsiBootvSwitch.
4. Selecione Editar definições.
5. Altere a MTU para 9000 e clique em Salvar.
6. Renomeie a porta iSCSIBootPG para iSCSIBootPG-A.

> Vmnic3 e vmnic5 são usados para inicialização iSCSI nesta configuração. Se você tiver NICs adicionais no host ESXi, poderá ter números vmnic diferentes. Para confirmar quais NICs são usados para inicialização iSCSI, faça a correspondência dos endereços MAC nos vNICs iSCSI no CIMC com os vmnics no ESXi.

7. No painel central, selecione a guia NICs do VMkernel.
8. Selecione Adicionar NIC VMkernel.
   a. Especifique um novo nome de grupo de portas do iScsiBootPG-B.
   b. Selecione iScsiBootvSwitch para o switch virtual.
   c. Insira `<<iscsib_vlan_id>>` para a ID da VLAN.
   d. Altere a MTU para 9000.
   e. Expanda Configurações IPv4.

f. Selecione Configuração estática.

g. Introduza `<<var_hosta_iscsib_ip>>` o endereço.

h. Introduza `<<var_hosta_iscsib_mask>>` para Máscara de sub-rede.

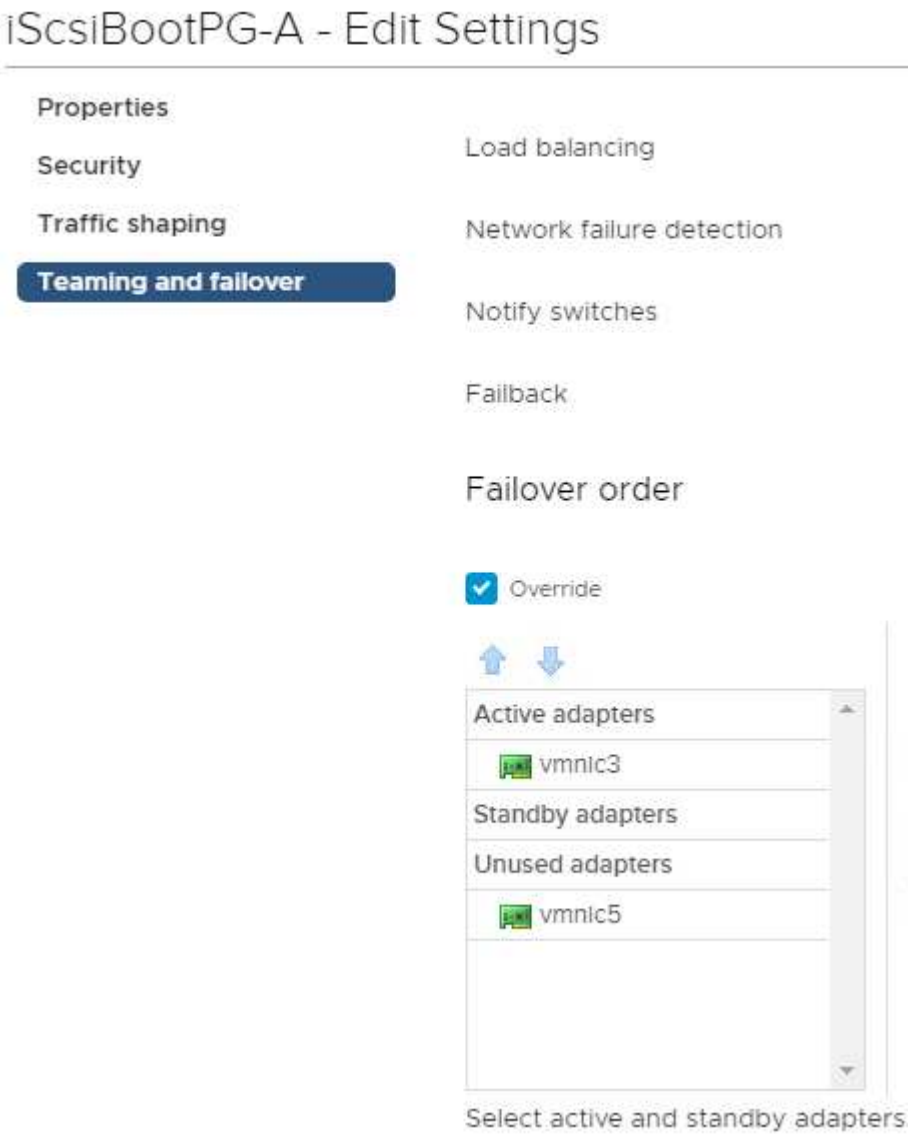
i. Clique em criar.

Defina a MTU como 9000 no iScsiBootPG-A.

9. Para definir o failover, execute as seguintes etapas:

a. Clique em Editar definições no iSCSIBootPG-A > disposição em categorias e failover > Ordem de failover > Vmnic3. Vmnic3 deve estar ativo e vmnic5 deve ser não utilizado.

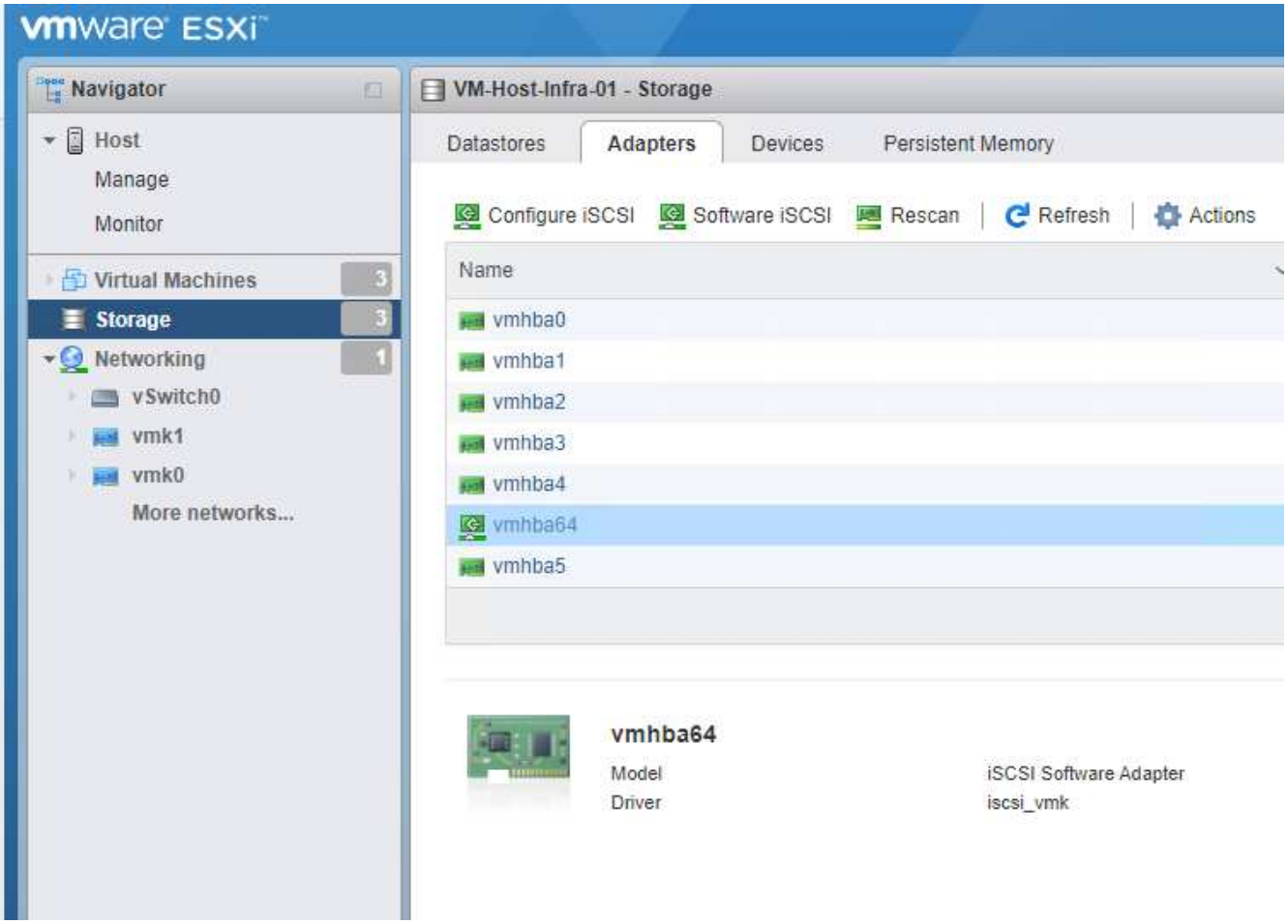
b. Clique em Editar definições no iSCSIBootPG-B > agrupamento e failover > Ordem de failover > Vmnic5. Vmnic5 deve estar ativo e vmnic3 deve ser não utilizado.



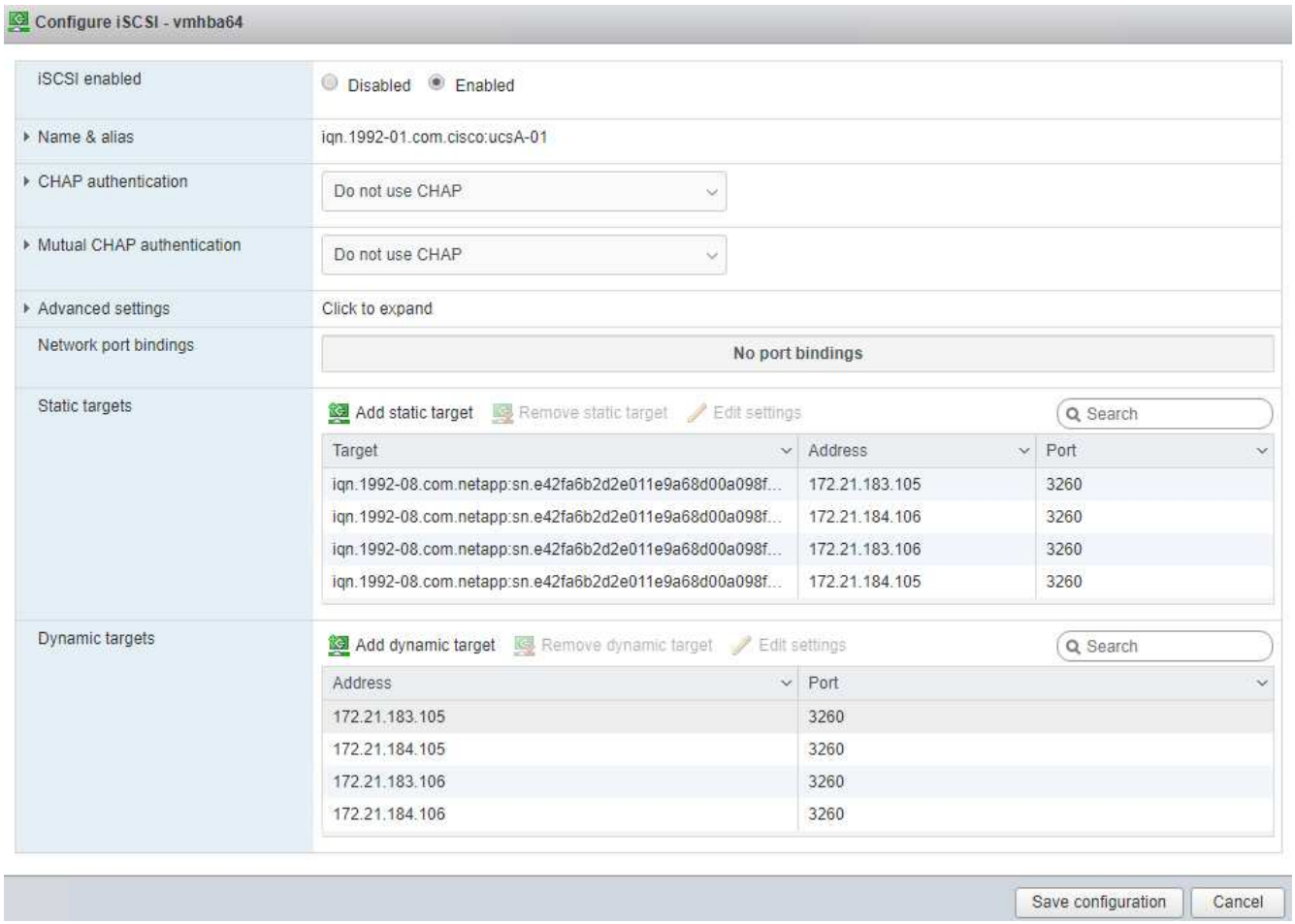
Configurar multipathing iSCSI

Para configurar multipathing iSCSI nos hosts ESXi, execute as seguintes etapas:

1. Selecione armazenamento no painel de navegação esquerdo. Clique em adaptadores.
2. Selecione o adaptador de software iSCSI e clique em Configurar iSCSI.



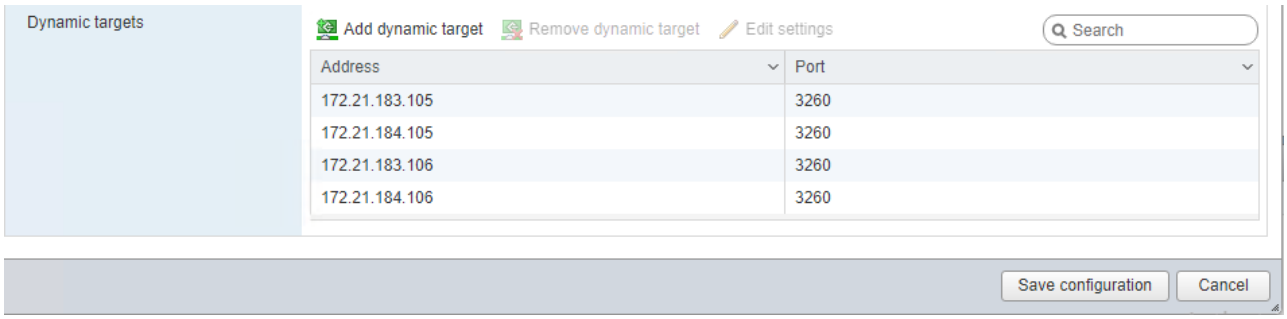
3. Em alvos dinâmicos, clique em Adicionar alvo dinâmico.



4. Introduza o endereço `iscsi_lif01a` IP .

   a. Repita com os endereços IP `iscsi_lif01b` , `iscsi_lif02a`, e `iscsi_lif02b`.

   b. Clique em Save Configuration (Guardar configuração).



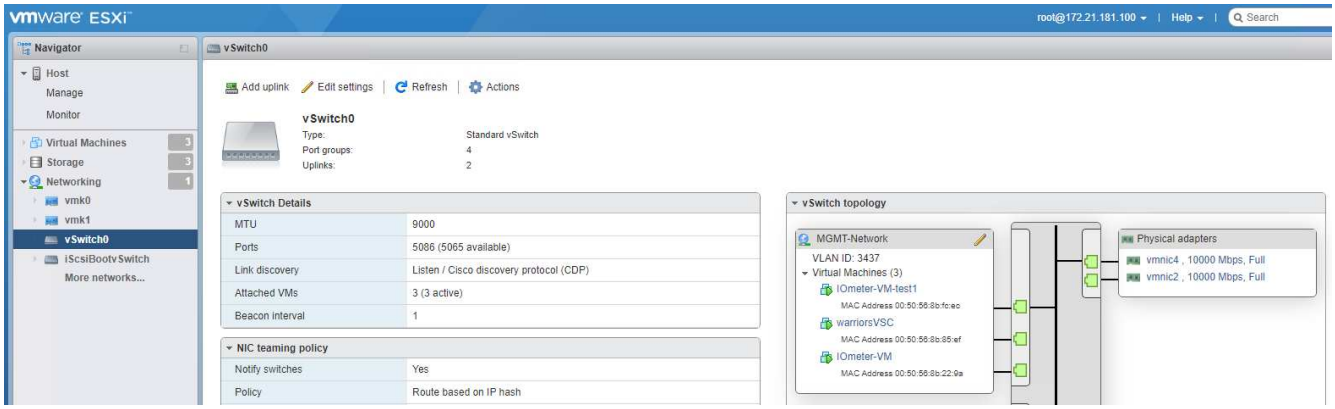
Você pode encontrar os endereços IP iSCSI LIF executando o comando show de interface de rede no cluster NetApp ou olhando para a guia interfaces de rede no Gerenciador de sistema.

Configure o host ESXi

Para configurar a inicialização do ESXi, execute as seguintes etapas:

1. No painel de navegação esquerdo, selecione rede.

2. Selecione vSwitch0.



3. Selecione Editar definições.
4. Altere a MTU para 9000.
5. Expanda o agrupamento NIC e verifique se o vmnic2 e o vmnic4 estão definidos como ativo e o agrupamento NIC e failover estão definidos como Rota com base no Hash IP.

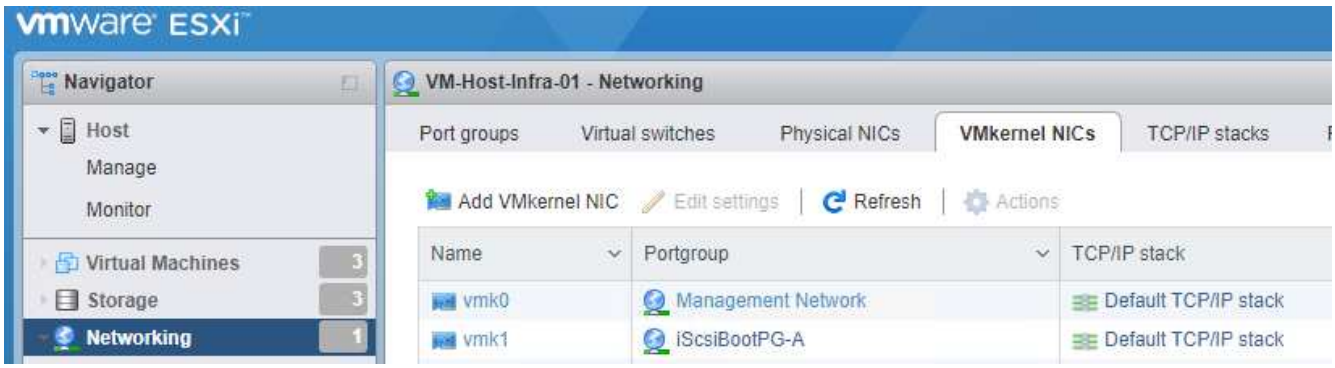
> O método de hash IP de balanceamento de carga requer que o switch físico subjacente seja configurado corretamente usando SRC-DST-IP EtherChannel com um canal de porta estático (mode- on). Você pode experimentar conetividade intermitente devido à possível configuração incorreta do switch. Em caso afirmativo, encerre temporariamente uma das duas portas uplink associadas no switch Cisco para restaurar a comunicação com a porta vmkernel de gerenciamento ESXi enquanto soluciona as configurações do canal de porta.

Configure os grupos de portas e as NICs do VMkernel

Para configurar os grupos de portas e as NICs do VMkernel, execute as seguintes etapas:

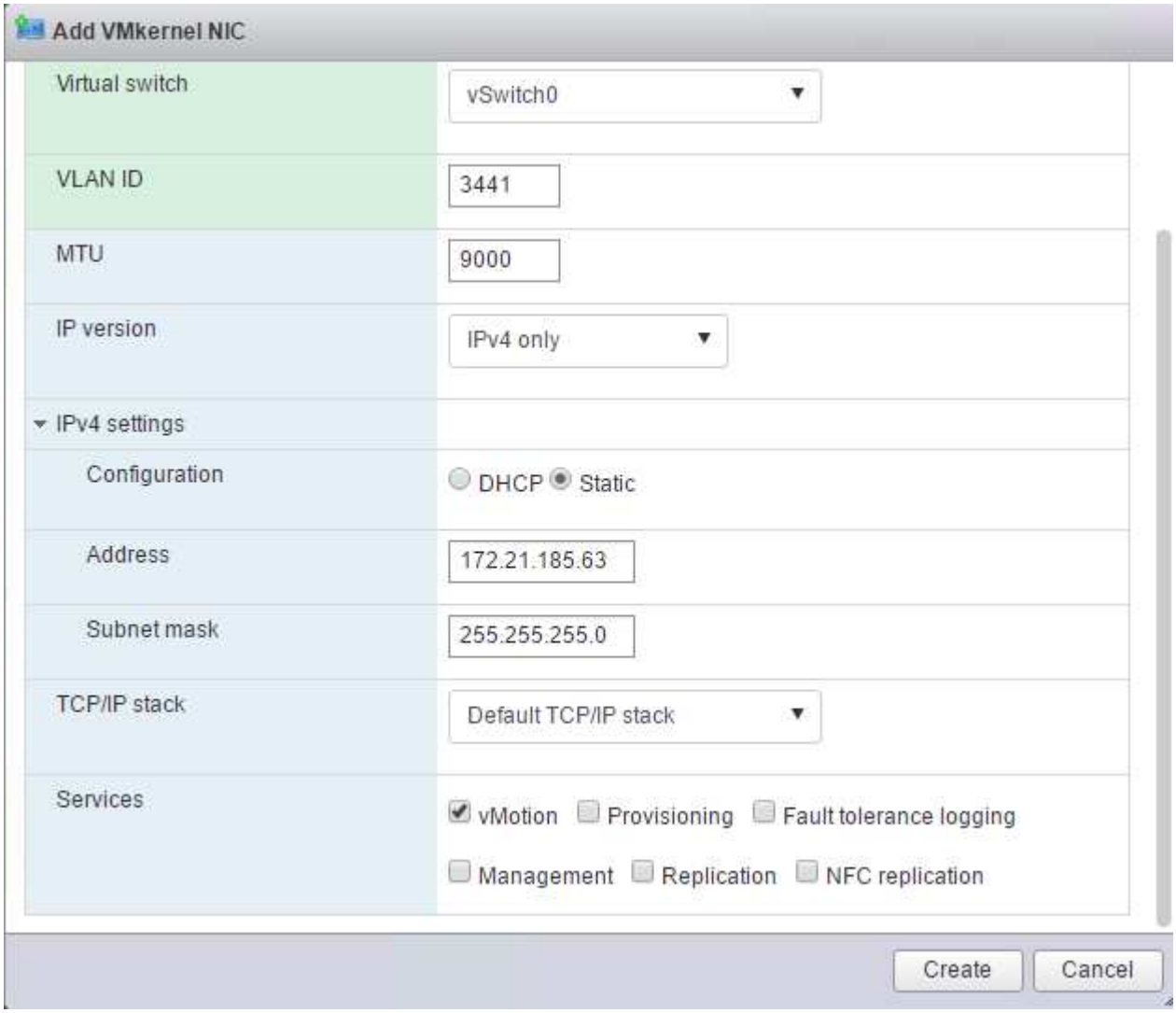
1. No painel de navegação esquerdo, selecione rede.
2. Clique com o botão direito do rato no separador grupos de portas.

3. Clique com o botão direito do rato em rede VM e selecione Editar. Altere a ID da VLAN para `<<var_vm_traffic_vlan>>`.
4. Clique em Adicionar grupo de portas.
    a. Nomeie o grupo de portas MGMT-Network.
    b. Insira `<<mgmt_vlan>>` para a ID da VLAN.
    c. Certifique-se de que vSwitch0 está selecionado.
    d. Clique em Save (Guardar).
5. Clique na guia NICs do VMkernel.



6. Selecione Adicionar NIC VMkernel.
    a. Selecione novo grupo de portas.
    b. Nomeie o grupo de portas NFS-Network.
    c. Insira `<<nfs_vlan_id>>` para a ID da VLAN.
    d. Altere a MTU para 9000.
    e. Expanda Configurações IPv4.
    f. Selecione Configuração estática.
    g. Introduza `<<var_hosta_nfs_ip>>` o endereço.
    h. Introduza `<<var_hosta_nfs_mask>>` para Máscara de sub-rede.
    i. Clique em criar.
7. Repita esse processo para criar a porta VMkernel do vMotion.
8. Selecione Adicionar NIC VMkernel.
    a. Selecione novo grupo de portas.
    b. Nomeie o grupo de portas vMotion.
    c. Insira `<<vmotion_vlan_id>>` para a ID da VLAN.
    d. Altere a MTU para 9000.
    e. Expanda Configurações IPv4.
    f. Selecione Configuração estática.
    g. Introduza `<<var_hosta_vmotion_ip>>` o endereço.
    h. Introduza `<<var_hosta_vmotion_mask>>` para Máscara de sub-rede.

i. Certifique-se de que a caixa de verificação vMotion está selecionada após IPv4 Settings (Definições).

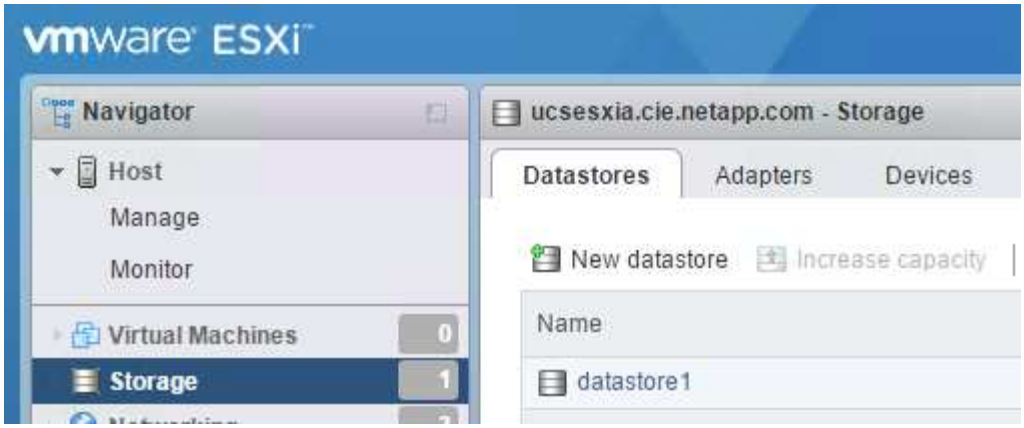


Há muitas maneiras de configurar a rede ESXi, inclusive usando o switch distribuído do VMware vSphere se o licenciamento permitir. Configurações de rede alternativas são suportadas no FlexPod Express se forem necessárias para atender aos requisitos empresariais.

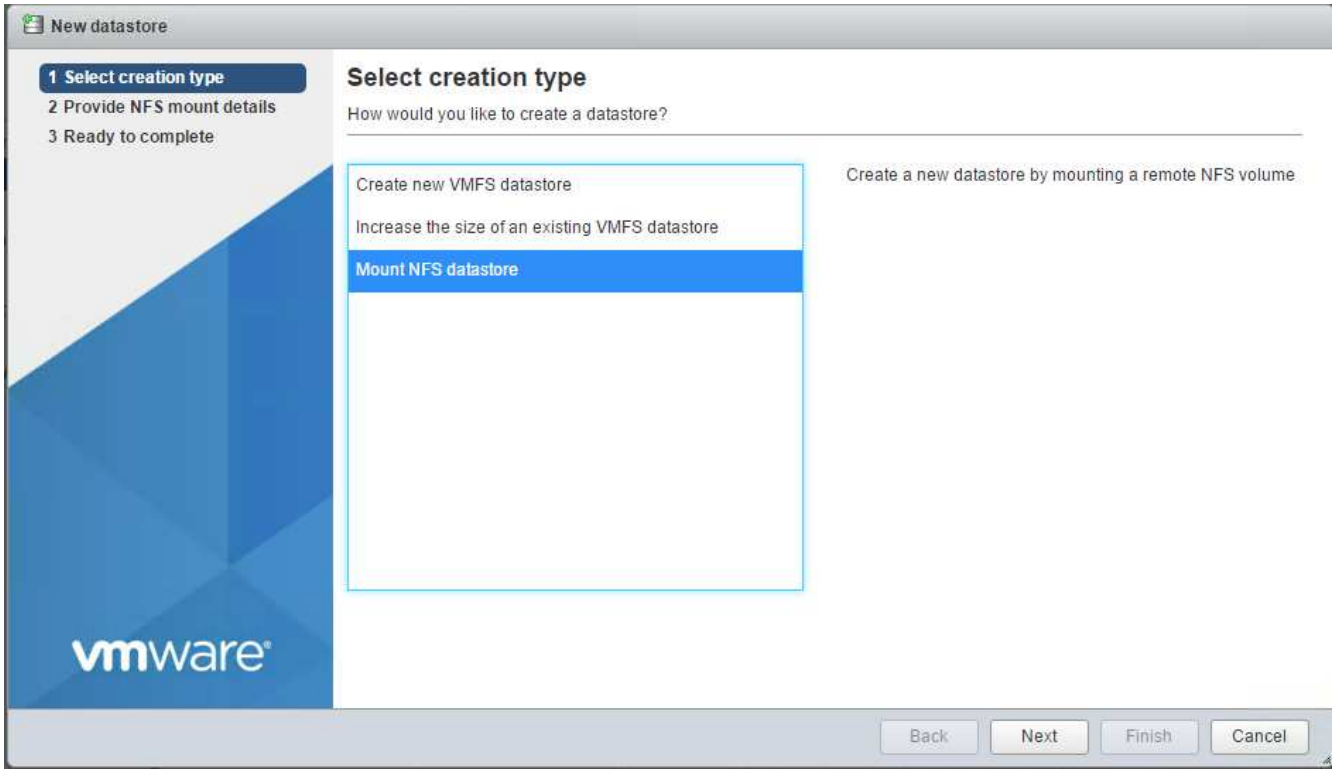
Monte os primeiros datastores

Os primeiros datastores a serem montados são o `infra_datastore` datastore para VMs e o `infra_swap` datastore para arquivos swap VM.

1. Clique em Storage (armazenamento) no painel de navegação esquerdo e, em seguida, clique em New datastore (novo armazenamento de dados).



2. Selecione Monte o armazenamento de dados NFS.



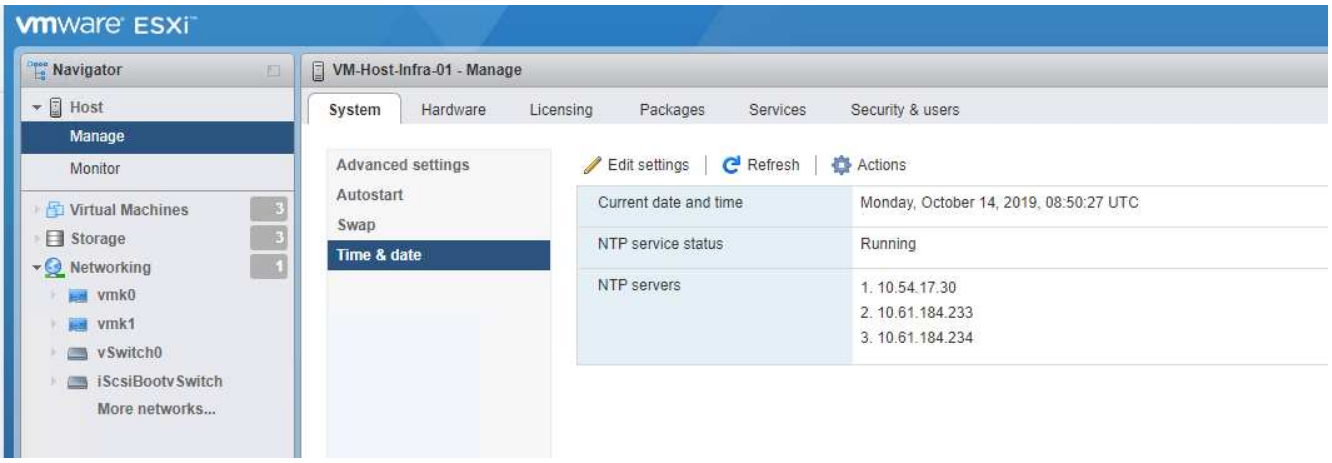
3. Insira as seguintes informações na página fornecer detalhes da montagem NFS:
   - Nome: `infra_datastore`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Partilhar: `/infra_datastore`
   - Certifique-se de que NFS 3 está selecionado.
4. Clique em concluir. Pode ver a tarefa a concluir no painel tarefas recentes.
5. Repita este processo para montar o `infra_swap` datastore:
   - Nome: `infra_swap`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Partilhar: `/infra_swap`

◦ Certifique-se de que NFS 3 está selecionado.

Configure o NTP

Para configurar o NTP para um host ESXi, execute as seguintes etapas:

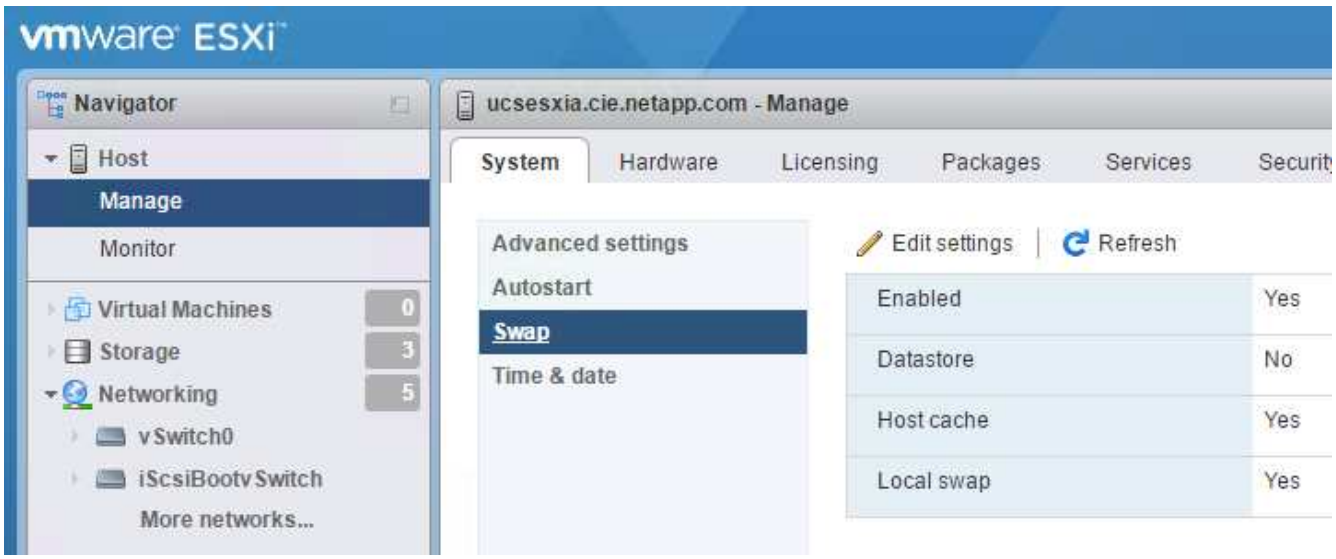
1. Clique em Gerenciar no painel de navegação esquerdo. Selecione System (sistema) no painel direito e, em seguida, clique em Time & Date (hora e data).
2. Selecione utilizar protocolo de tempo de rede (Ativar cliente NTP).
3. Selecione Iniciar e Parar com Host como a política de inicialização do serviço NTP.
4. `<<var_ntp>>`Introduza como servidor NTP. Você pode definir vários servidores NTP.
5. Clique em Guardar.



Mova o local do arquivo de troca de VM

Estas etapas fornecem detalhes para mover o local do arquivo de troca de VM.

1. Clique em Gerenciar no painel de navegação esquerdo. Selecione System (sistema) no painel direito e, em seguida, clique em Swap (trocar).



2. Clique em Edit Settings (Editar definições). Selecione `infra_swap` a partir das opções do datastore.

3. Clique em Guardar.

"Próximo: Procedimento de instalação do VMware vCenter Server 6.7U2."

Procedimento de instalação do VMware vCenter Server 6.7U2

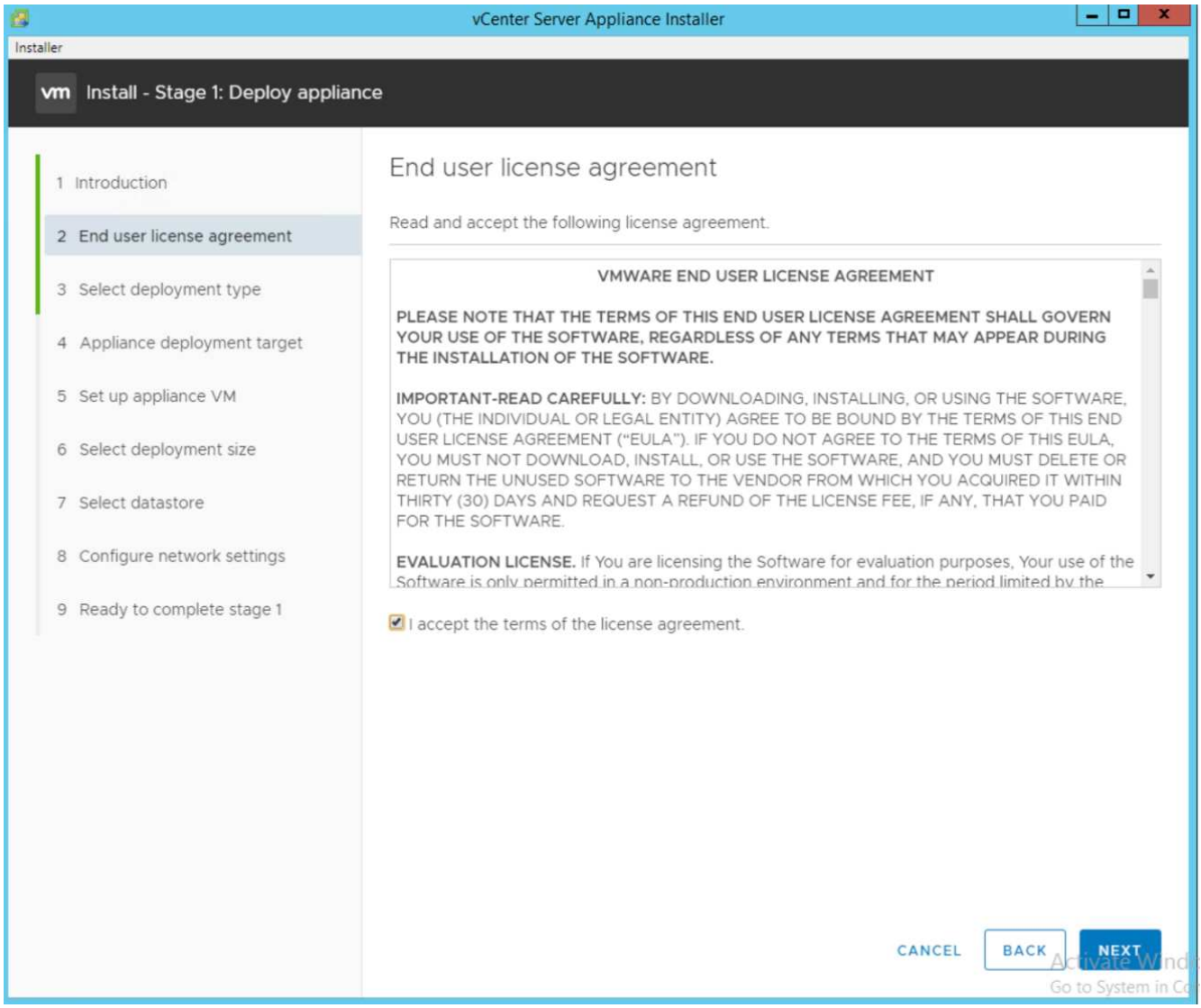
Esta seção fornece procedimentos detalhados para instalar o VMware vCenter Server 6,7 em uma configuração do FlexPod Express.

O FlexPod Express usa o VMware vCenter Server Appliance (VCSA).

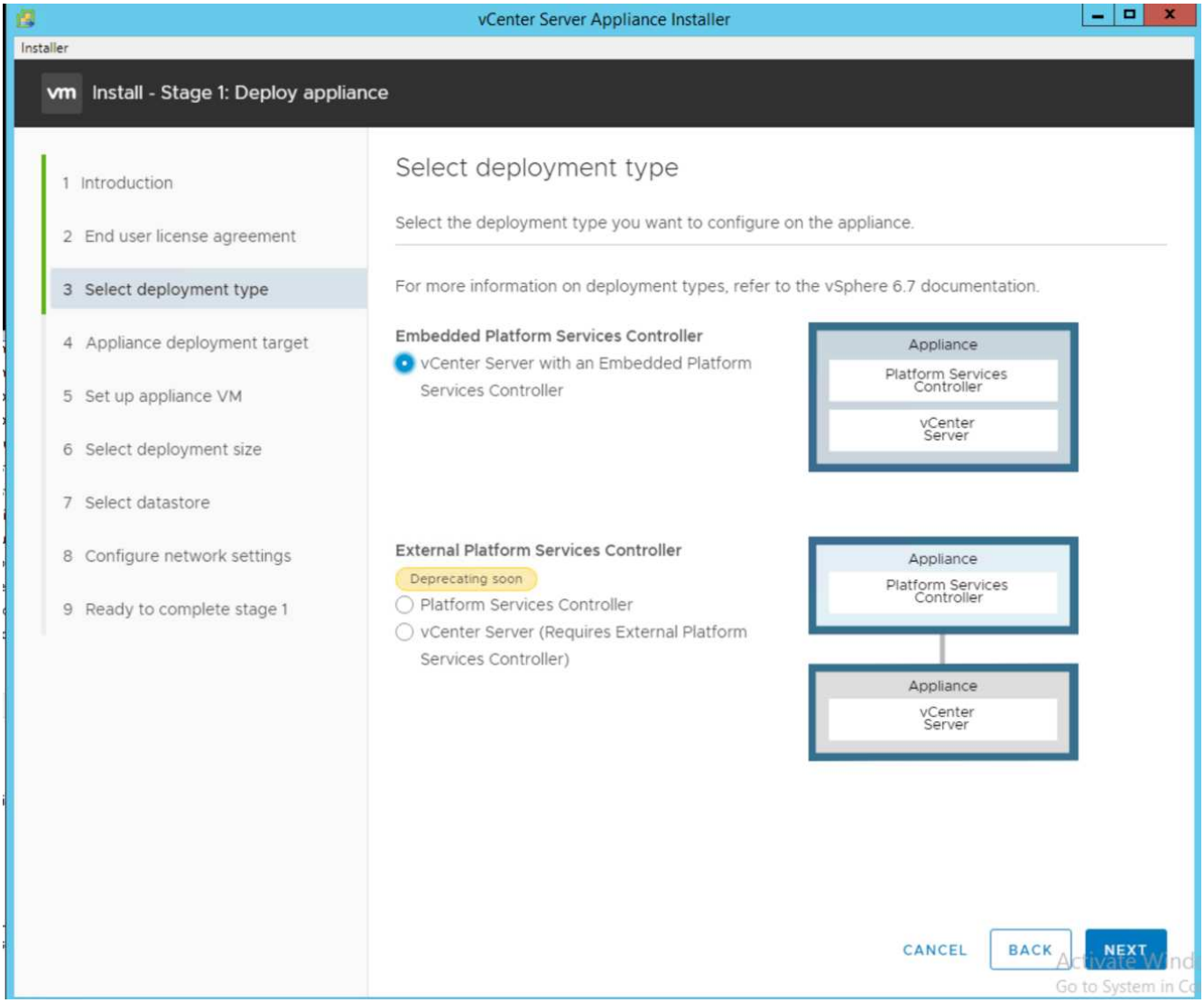
Faça download do dispositivo VMware vCenter Server

Para fazer o download do VMware vCenter Server Appliance (VCSA), siga estas etapas:

1. Faça o download do VCSA. Acesse o link de download clicando no ícone obter vCenter Server ao gerenciar o host ESXi.
2. Faça download do VCSA a partir do site da VMware.
3. Embora o Microsoft Windows vCenter Server instalável seja suportado, a VMware recomenda o VCSA para novas implantações.
4. Monte a imagem ISO.
5. Navegue até o diretório vcsa- ui-installer > Win32. Clique duas vezes `installer.exe` em .
6. Clique em Instalar.
7. Clique em Avançar na página Introdução.

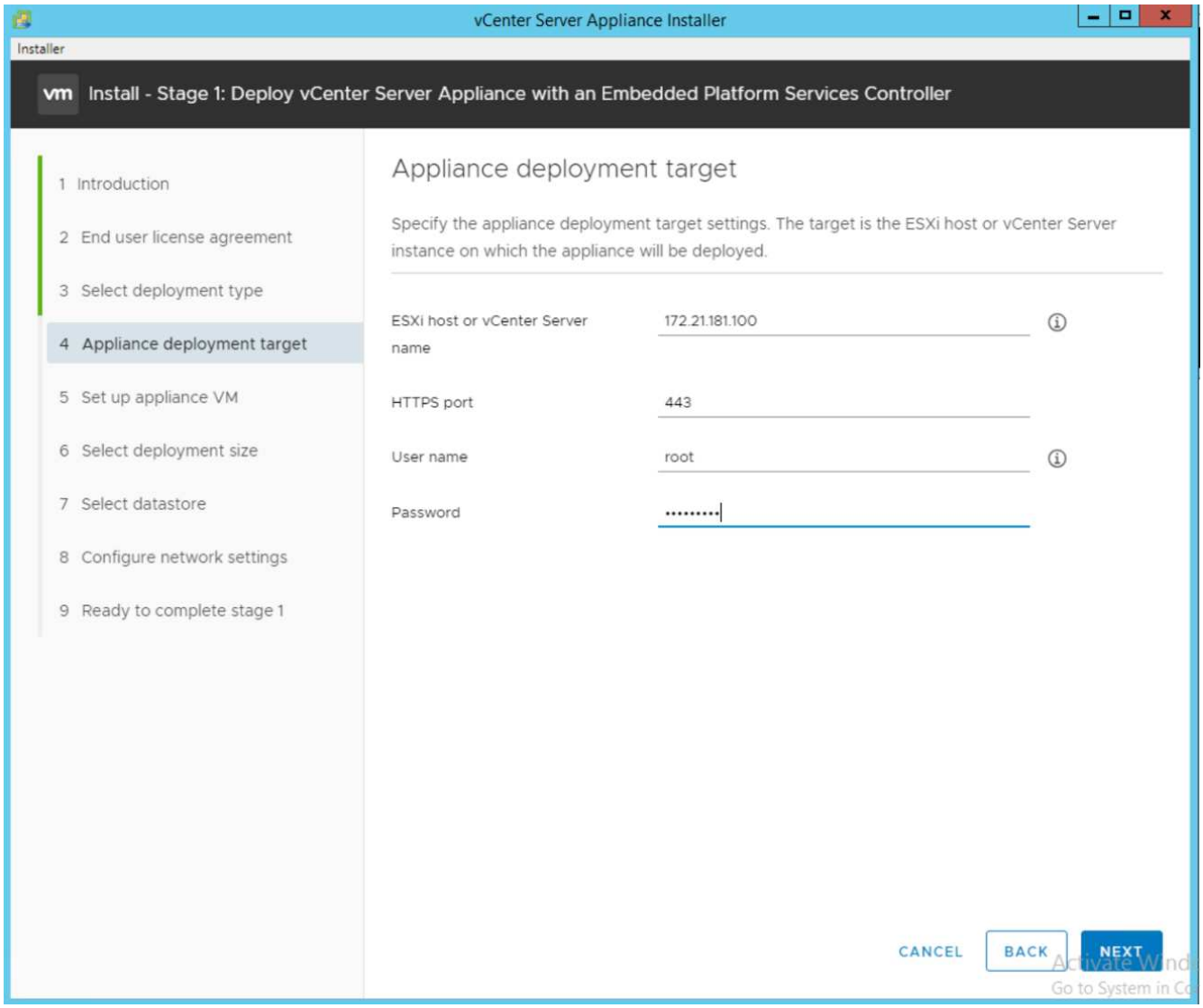


8. Selecione controlador de serviços de plataforma incorporada como o tipo de implantação.

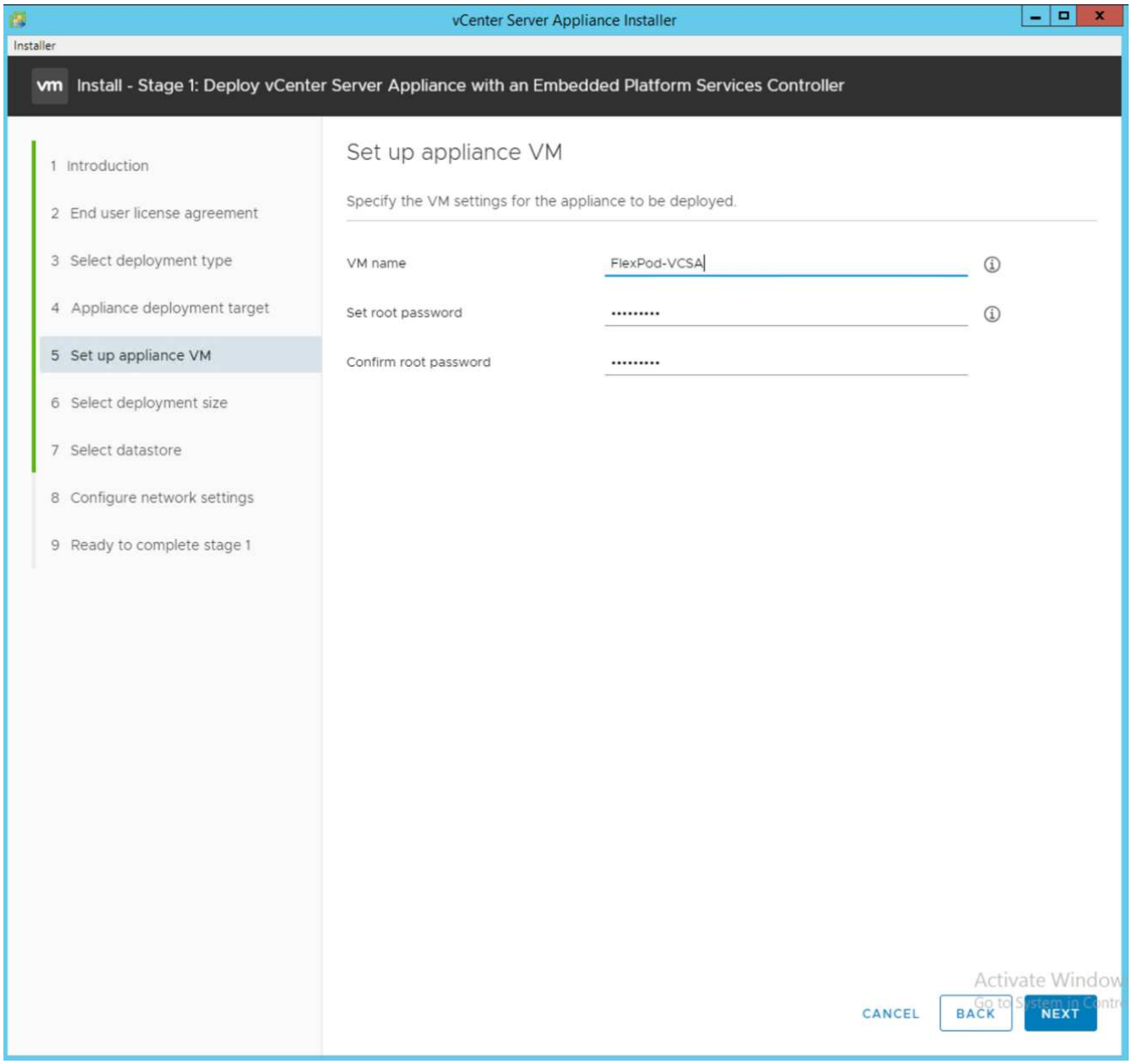


Se necessário, a implantação do controlador de serviços de plataforma externa também é suportada como parte da solução FlexPod Express.

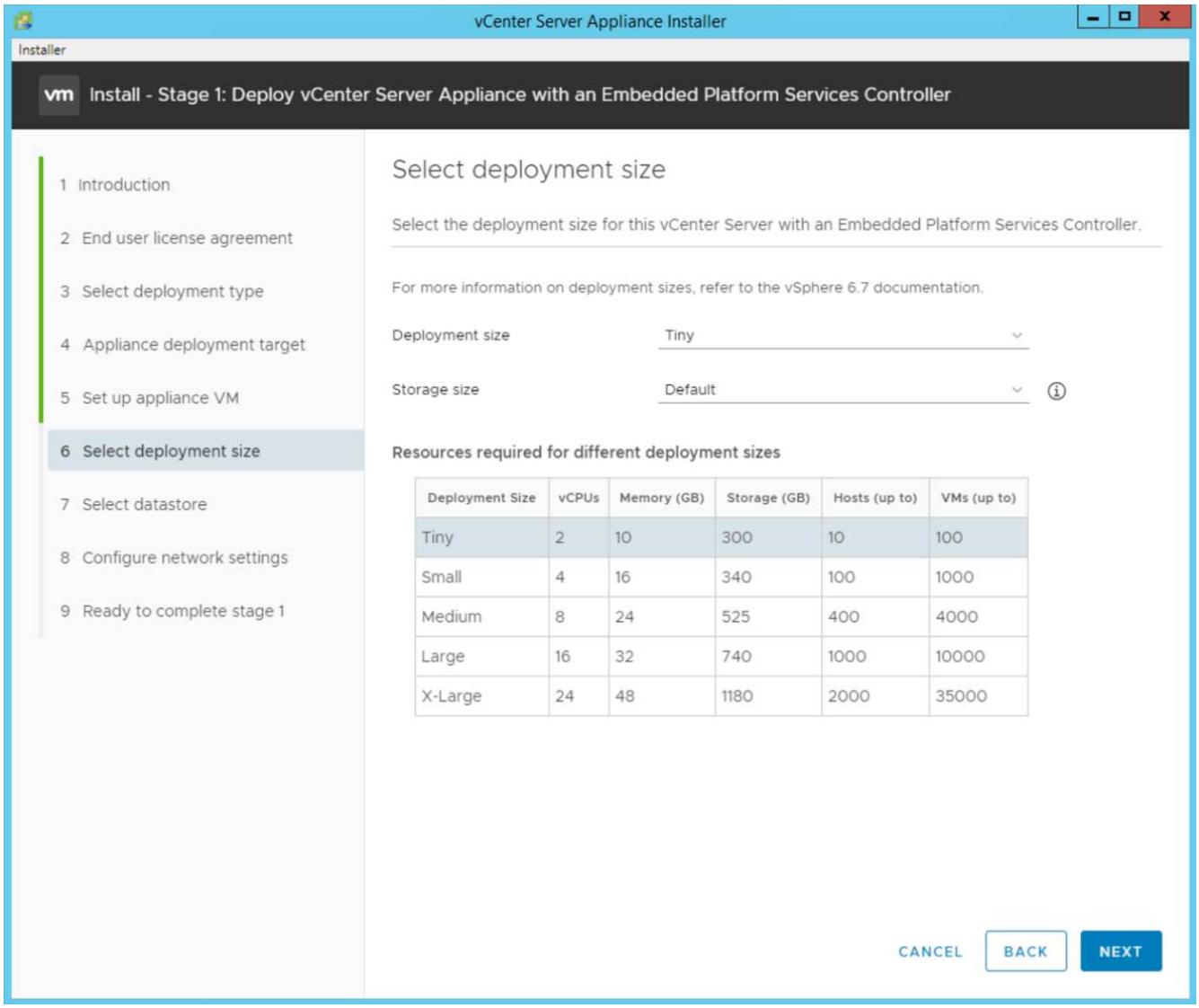
9. No destino de implantação do dispositivo, insira o endereço IP de um host ESXi que você implantou, o nome de usuário raiz e a senha raiz.



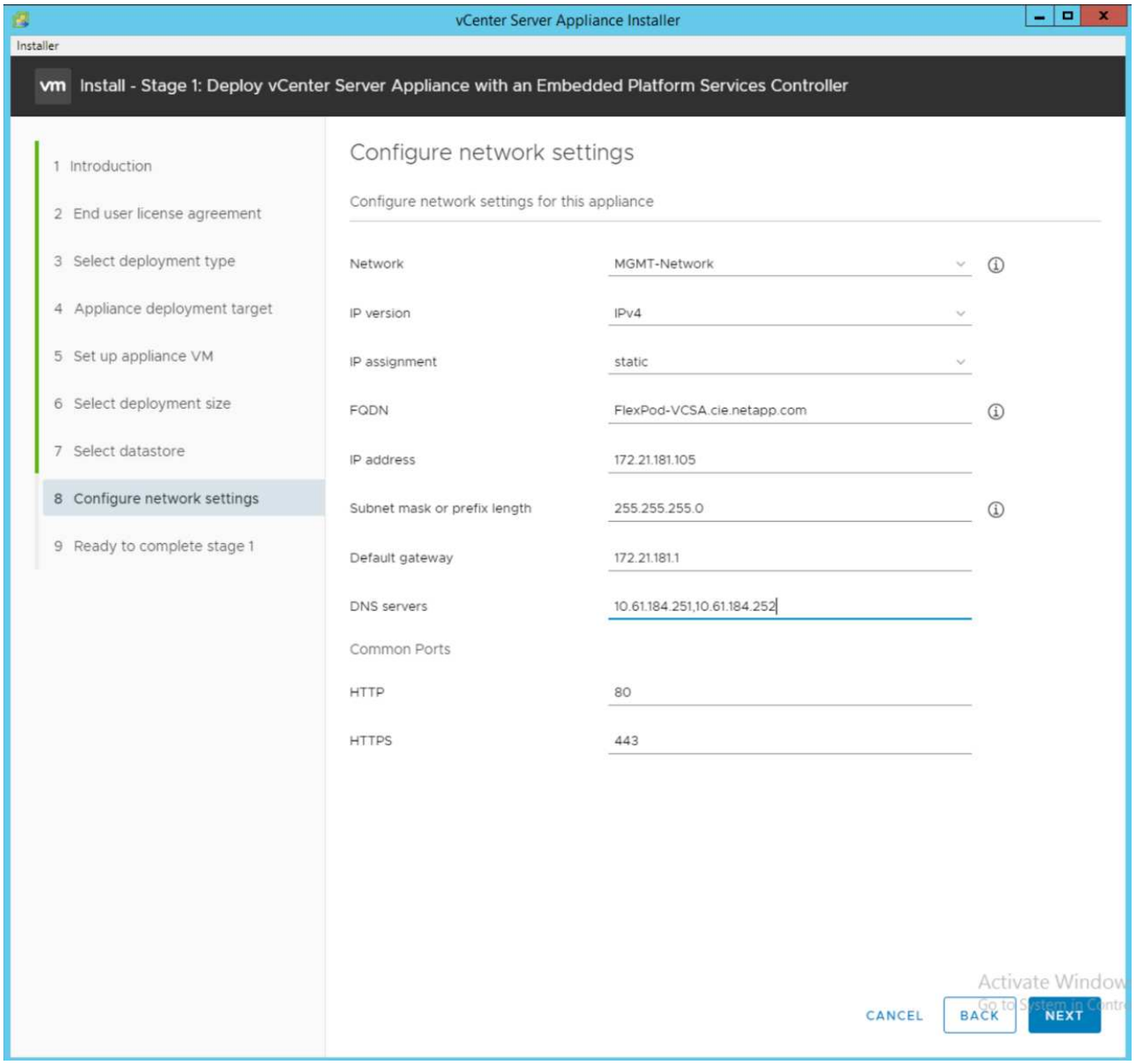
10. Defina a VM do appliance inserindo o VCSA como o nome da VM e a senha raiz que você gostaria de usar para o VCSA.



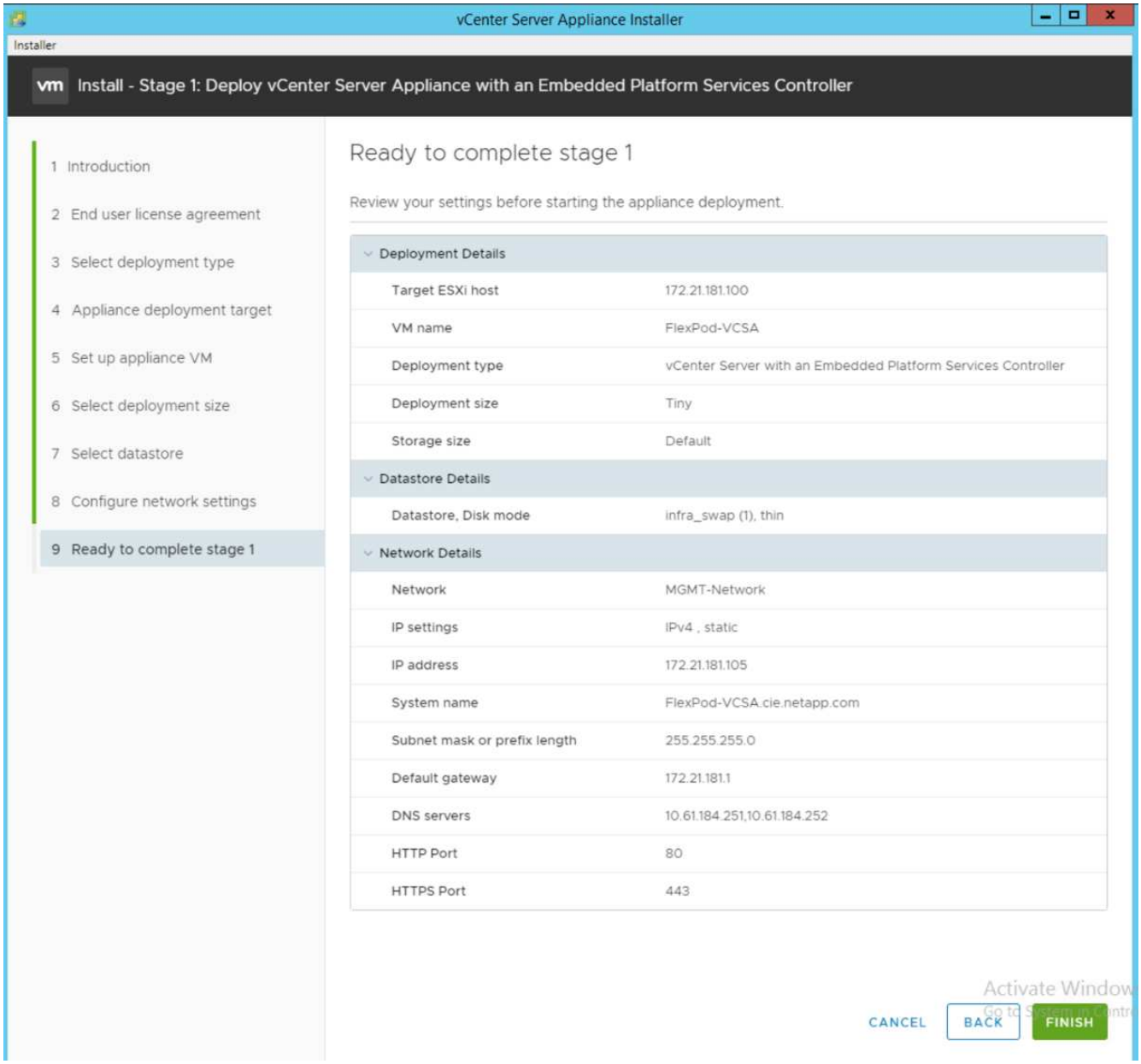
11. Selecione o tamanho de implantação que melhor se adapta ao seu ambiente. Clique em seguinte.



12. Selecione o `infra_datastore` datastore. Clique em seguinte.
13. Introduza as seguintes informações na página Configurar definições de rede e clique em seguinte.
    a. Selecione MGMT-Network para rede.
    b. Introduza o FQDN ou IP a utilizar para o VCSA.
    c. Introduza o endereço IP a utilizar.
    d. Introduza a máscara de sub-rede a utilizar.
    e. Introduza o gateway predefinido.
    f. Introduza o servidor DNS.
14. Na página Pronto para concluir a fase 1, verifique se as configurações inseridas estão corretas. Clique em concluir.

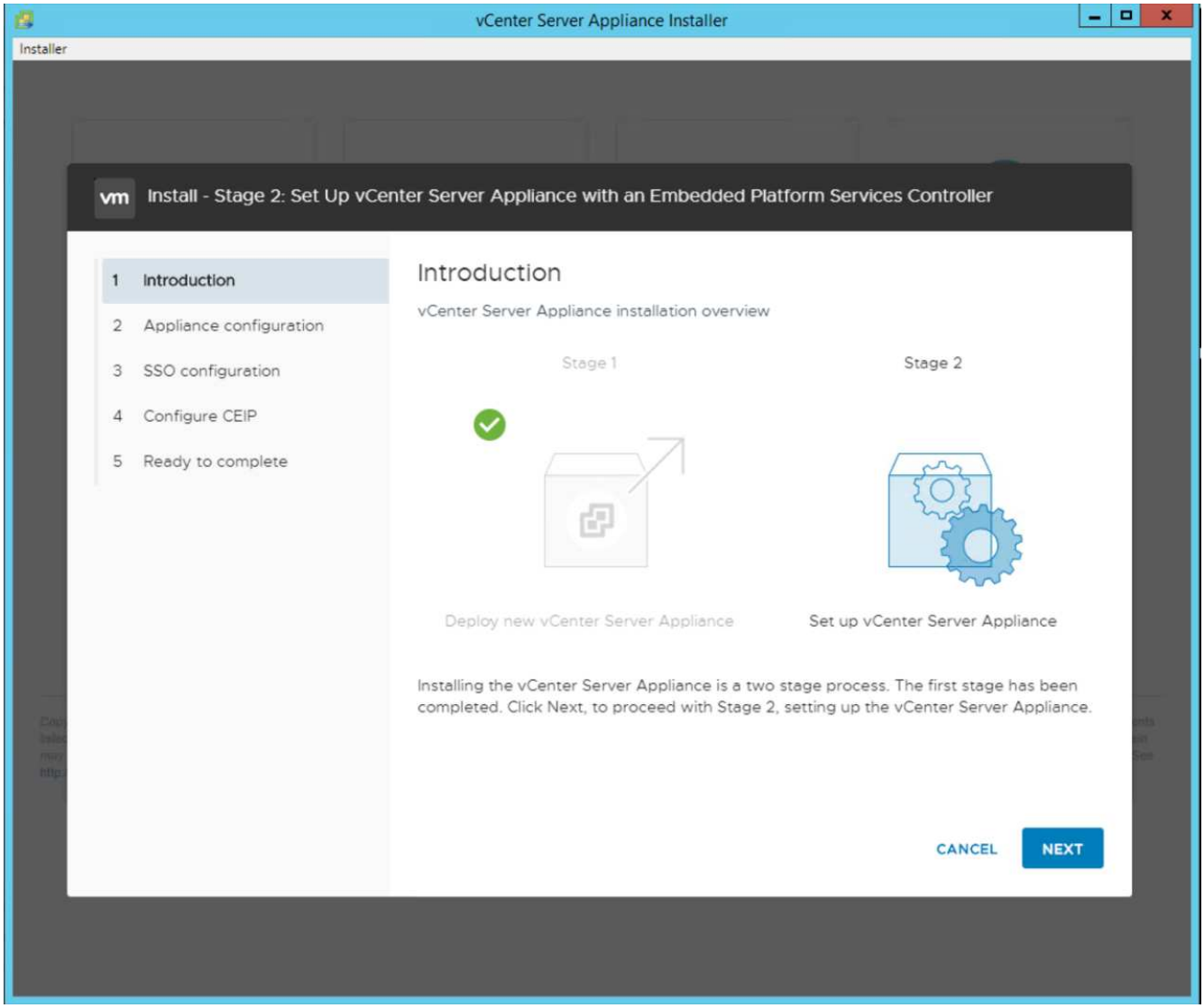


15. Reveja as suas definições na fase 1 antes de iniciar a implementação do dispositivo.

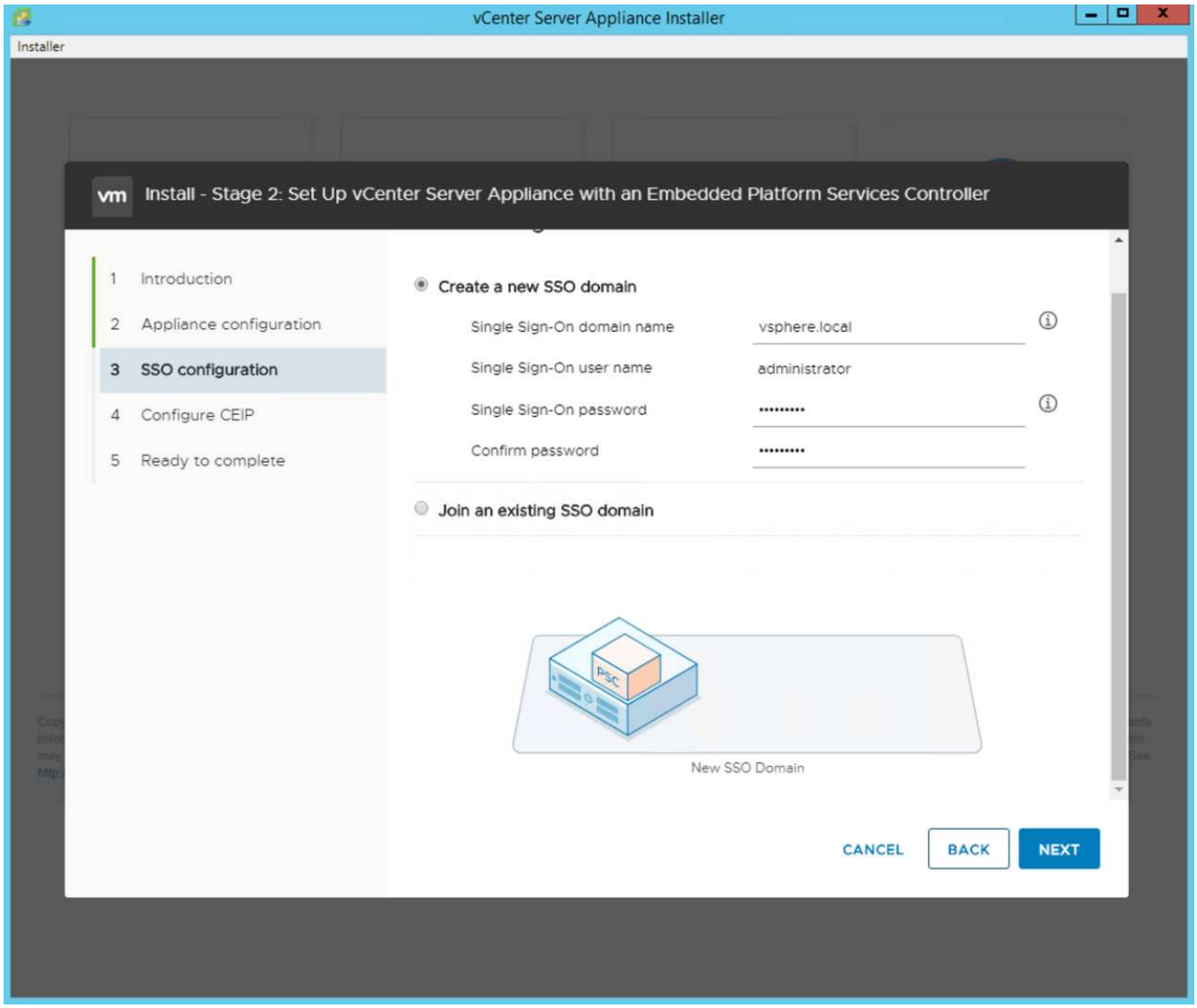


O VCSA é instalado agora. Este processo demora vários minutos.

16. Após a conclusão da fase 1, aparece uma mensagem informando que ela foi concluída. Clique em continuar para iniciar a configuração da fase 2.
17. Na página Introdução do Estágio 2, clique em Avançar.

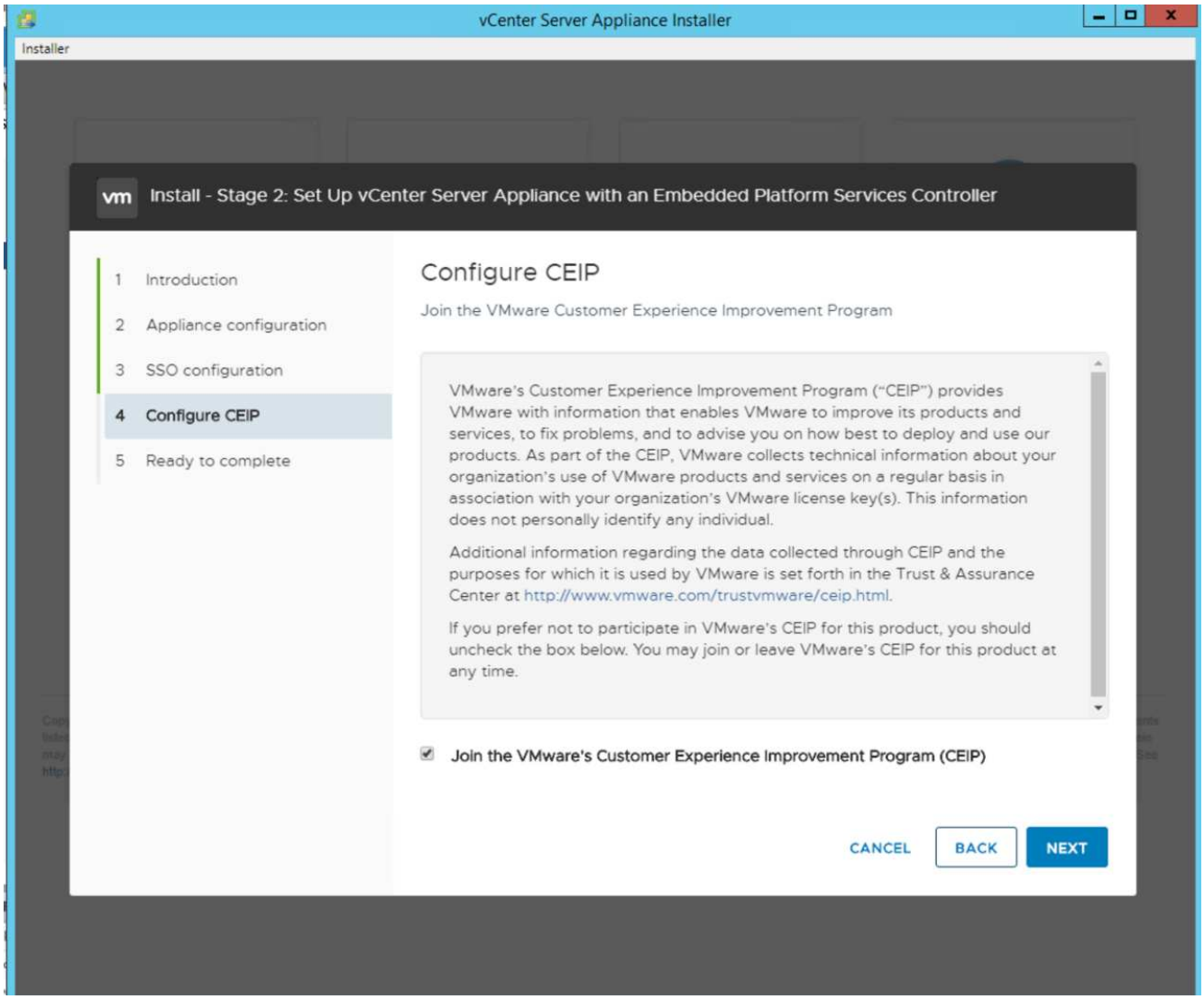


18. Introduza `<<var_ntp_id>>` para o endereço do servidor NTP. Pode introduzir vários endereços IP NTP.
19. Se você planeja usar o vCenter Server High Availability (HA), verifique se o acesso SSH está habilitado.
20. Configure o nome de domínio SSO, a senha e o nome do site. Clique em seguinte.

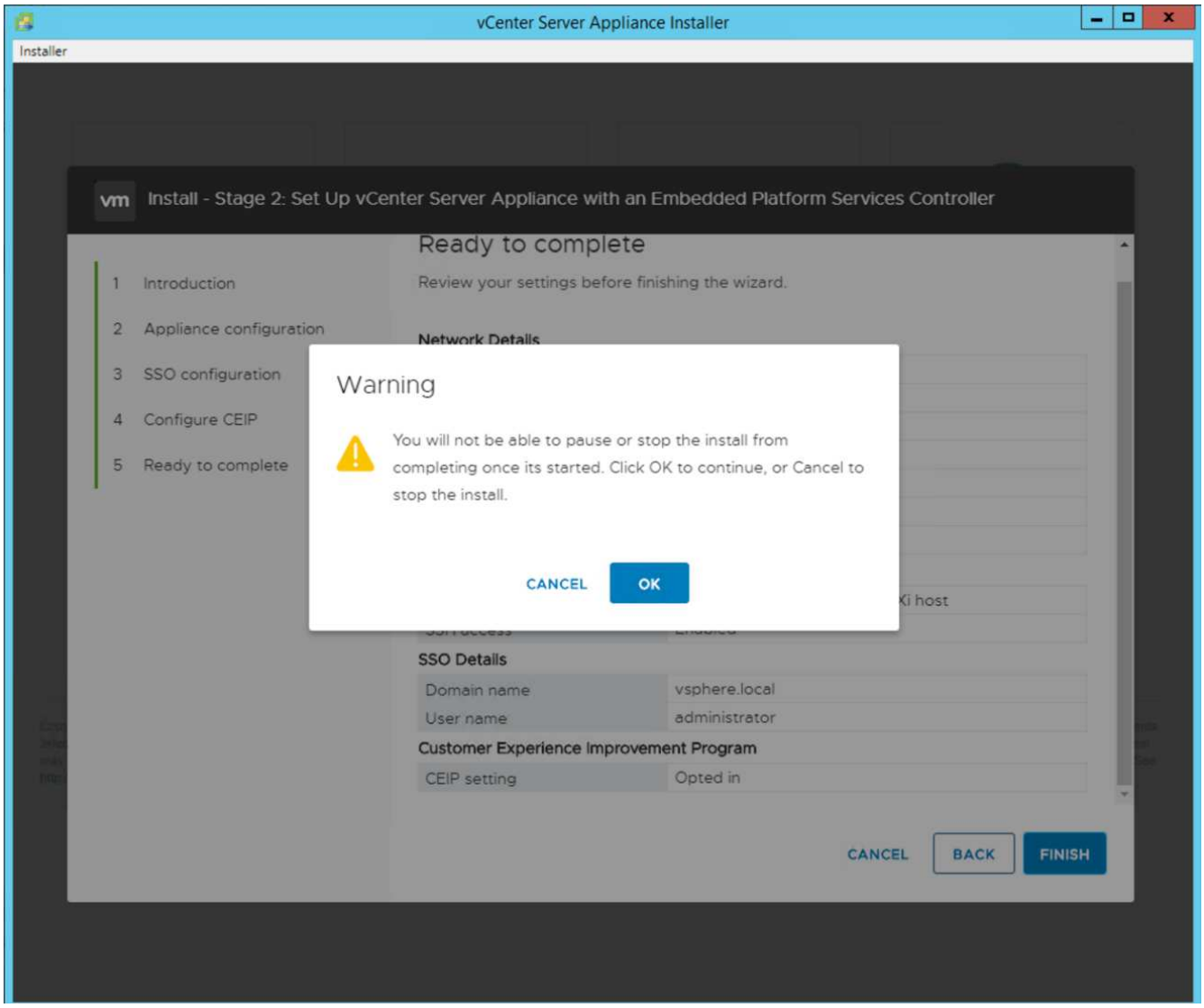


Registe estes valores para a sua referência, especialmente se se desviar do `vsphere.local` nome de domínio.

21. Junte-se ao Programa de experiência do Cliente da VMware, se desejado. Clique em seguinte.



22. Veja o resumo das suas definições. Clique em concluir ou use o botão voltar para editar as configurações.
23. Uma mensagem é exibida informando que você não será capaz de pausar ou parar a instalação de ser concluída depois que ela for iniciada. Clique em OK para continuar.



A configuração do aparelho continua. Isso leva vários minutos.

É apresentada uma mensagem a indicar que a configuração foi bem-sucedida.

24. Os links que o instalador fornece para acessar o vCenter Server são clicáveis.

"Próximo: Configuração de cluster do VMware vCenter Server 6.7U2 e vSphere."

Configuração de cluster do VMware vCenter Server 6.7U2 e vSphere

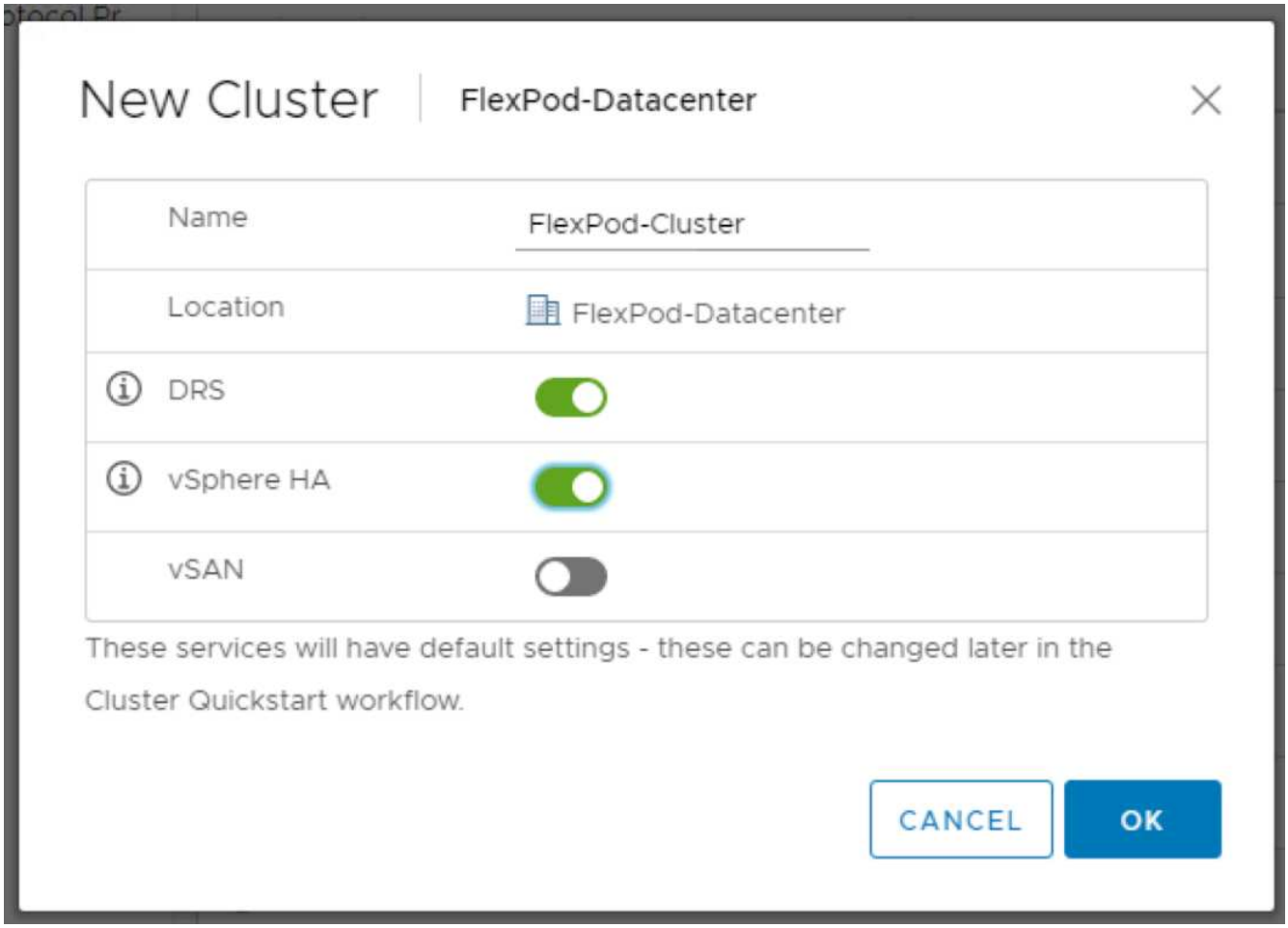
Para configurar o cluster do VMware vCenter Server 6,7 e vSphere, execute as seguintes etapas:

1. Navegue até `https://<<FQDN or IP of vCenter>>/vsphere-client/`.
2. Clique em Launch vSphere Client.
3. Faça login com o nome de usuário mailto:administrator e a senha SSO que você inseriu durante o processo de configuração do VCSA.
4. Clique com o botão direito no nome do vCenter e selecione novo data center.
5. Introduza um nome para o centro de dados e clique em OK.

Crie um cluster vSphere

Para criar um cluster vSphere, execute as seguintes etapas:

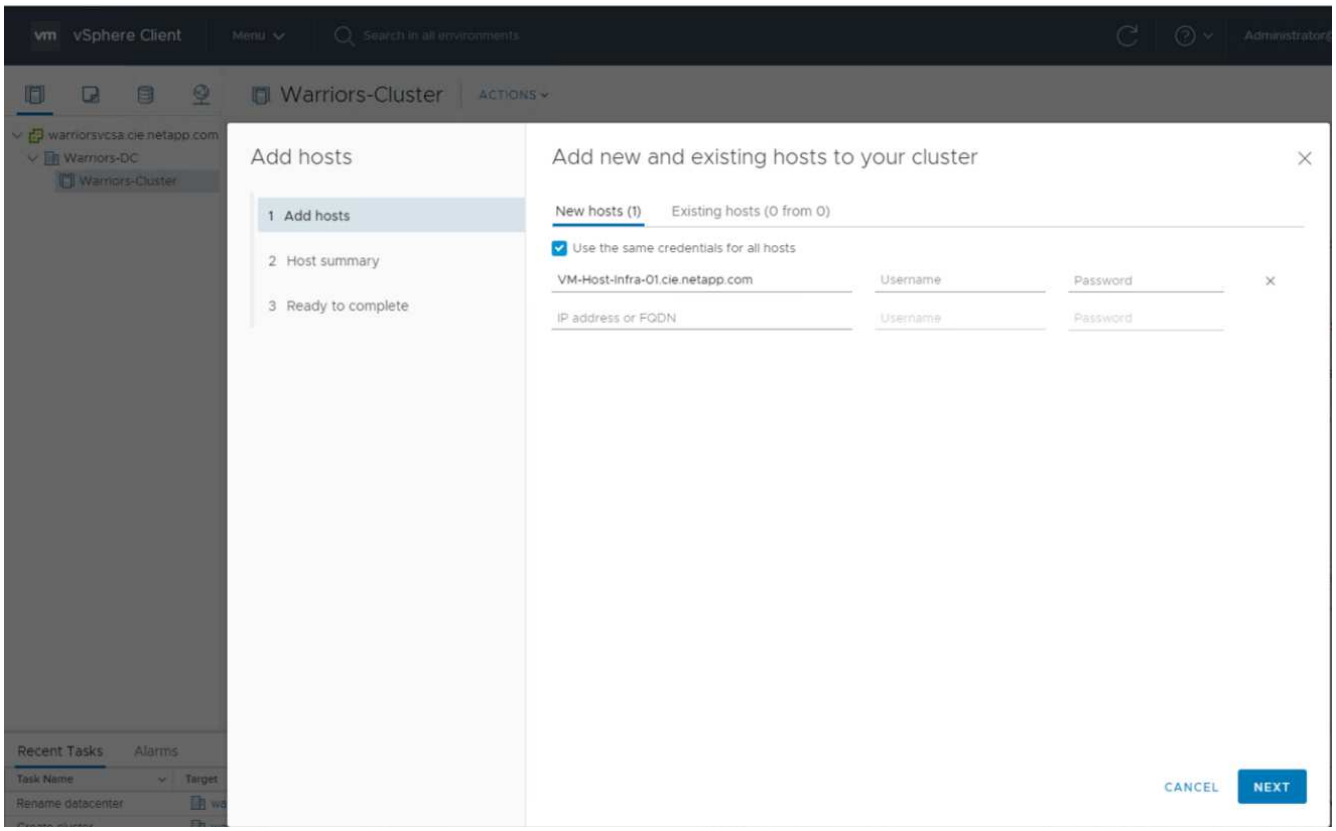
1. Clique com o botão direito do rato no data center recém-criado e selecione novo cluster.
2. Introduza um nome para o cluster.
3. Ative o DR e o vSphere HA selecionando as caixas de seleção.
4. Clique em OK.



Adicione os hosts ESXi ao cluster

Para adicionar os hosts ESXi ao cluster, execute as seguintes etapas:

1. Clique com o botão direito do rato no cluster e selecione Adicionar anfitrião.



2. Para adicionar um host ESXi ao cluster, execute as seguintes etapas:
   a. Insira o IP ou FQDN do host. Clique em seguinte.
   b. Introduza o nome de utilizador e a palavra-passe raiz. Clique em seguinte.
   c. Clique em Sim para substituir o certificado do host por um certificado assinado pelo servidor de certificados VMware.
   d. Clique em Next (seguinte) na página Host Summary (Resumo do anfitrião).
   e. Clique no ícone verde para adicionar uma licença ao host vSphere.
3. Este passo pode ser concluído mais tarde, se desejado.
   a. Clique em seguinte para deixar o modo de bloqueio desativado.
   b. Clique em Avançar na página de localização da VM.
   c. Reveja a página Pronto para concluir. Use o botão voltar para fazer quaisquer alterações ou selecione concluir.
4. Repita as etapas 1 e 2 para o host B. do Cisco UCS

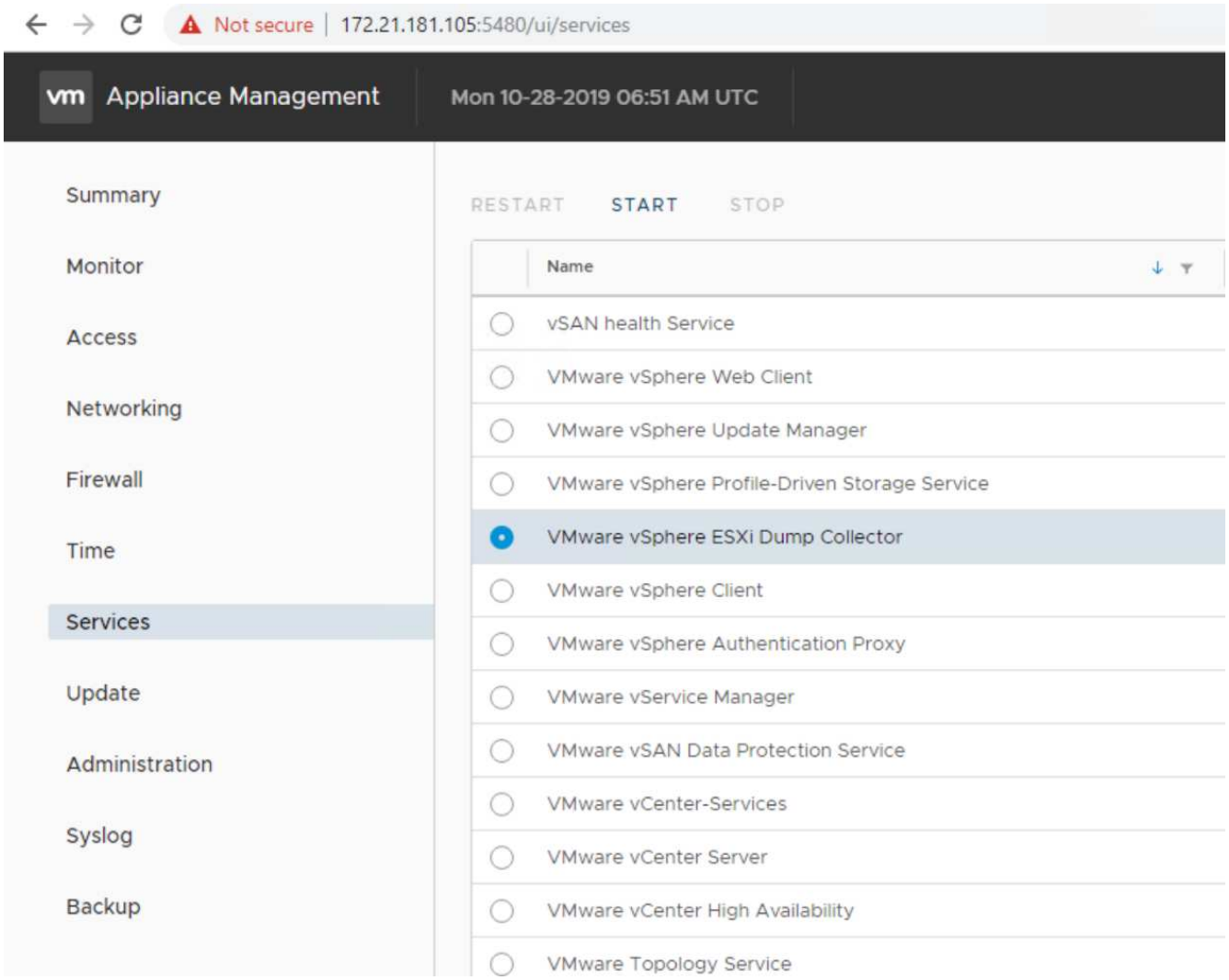
> Esse processo deve ser concluído para quaisquer hosts adicionais adicionados à configuração do FlexPod Express.

Configure o coredump nos hosts ESXi

Para configurar o coredump nos hosts ESXi, execute as seguintes etapas:

1. Inicie sessão em https:// "VCenter" IP:5480/, introduza root para o nome de utilizador e introduza a palavra-passe de raiz.

2. Clique em serviços e selecione o coletor de despejo VMware vSphere ESXI.
3. Inicie o serviço coletor de despejo VMware vSphere ESXI.



4. Usando SSH, conete-se ao host IP ESXi de gerenciamento, insira raiz para o nome de usuário e insira a senha raiz.
5. Execute os seguintes comandos:

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

6. A mensagem `Verified the configured netdump server is running` aparece depois de inserir o comando final.

```
root@VM-Host-Infra-01:~] esxcli system coredump network set -i 172.21.181.105 -
 vmk0 -o 6500
root@VM-Host-Infra-01:~]
root@VM-Host-Infra-01:~] esxcli system coredump network set --enable=true
root@VM-Host-Infra-01:~] esxcli system coredump network check
erified the configured netdump server is running
```

Esse processo deve ser concluído para quaisquer hosts adicionais adicionados ao FlexPod Express.

`ip_address_of_core_dump_collector` Nesta validação está o vCenter IP.

"Próximo: Procedimentos de implantação do console de storage virtual NetApp 9,6."

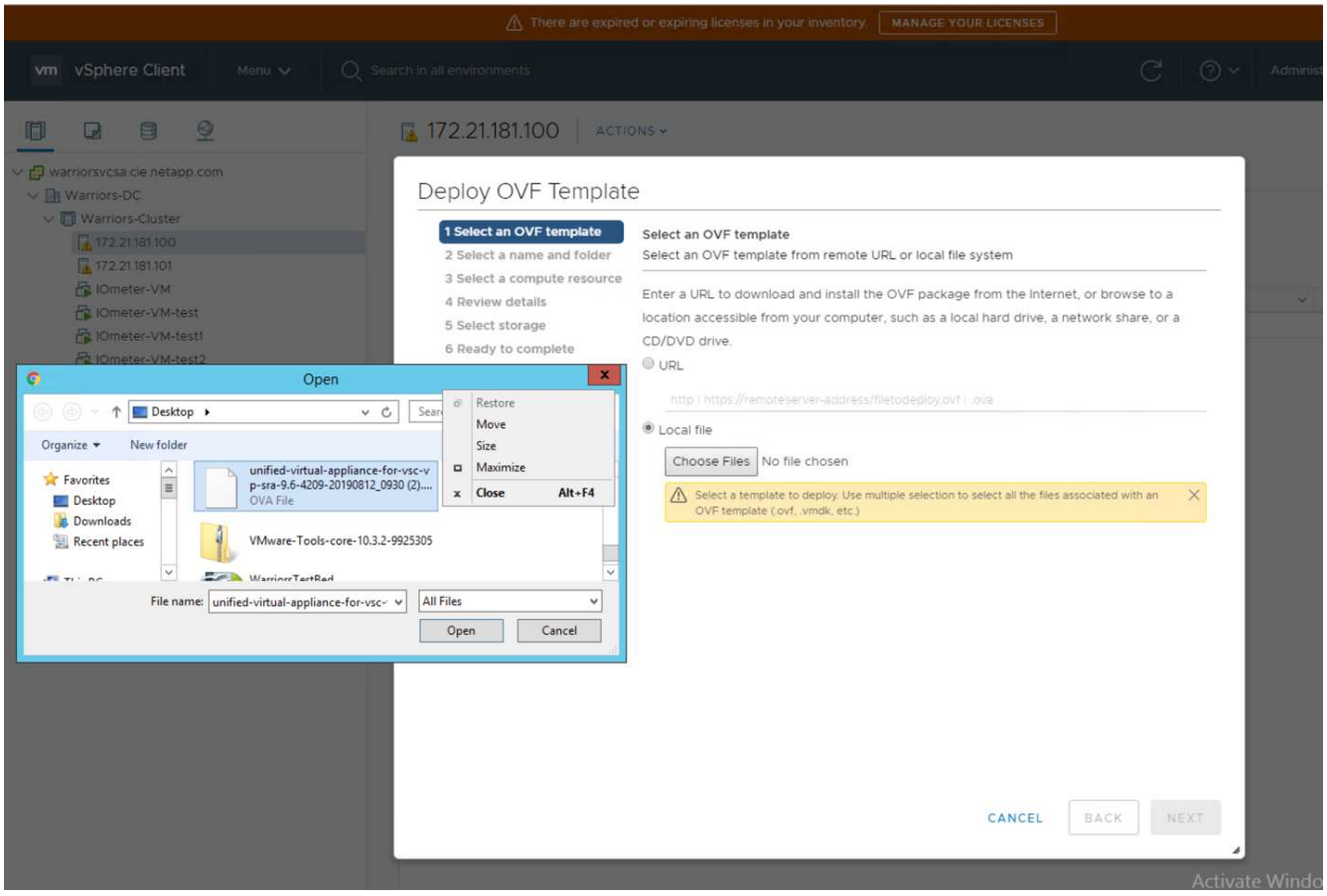
Procedimentos de implantação do console de storage virtual NetApp 9,6

Esta seção descreve os procedimentos de implantação do console de storage virtual (VSC) do NetApp.

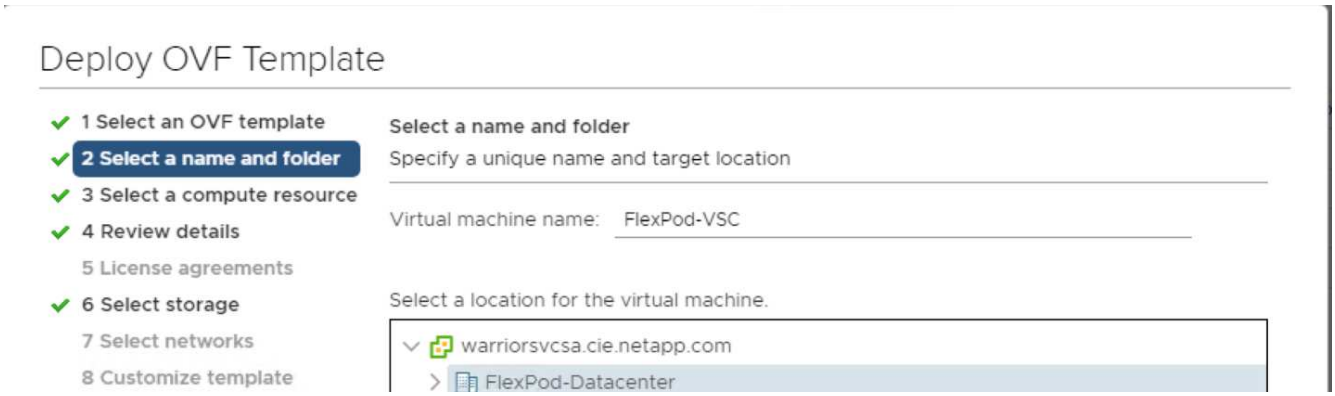
Instale o Virtual Storage Console 9,6

Para instalar o software VSC 9,6 usando uma implantação Open Virtualization Format (OVF), siga estas etapas:

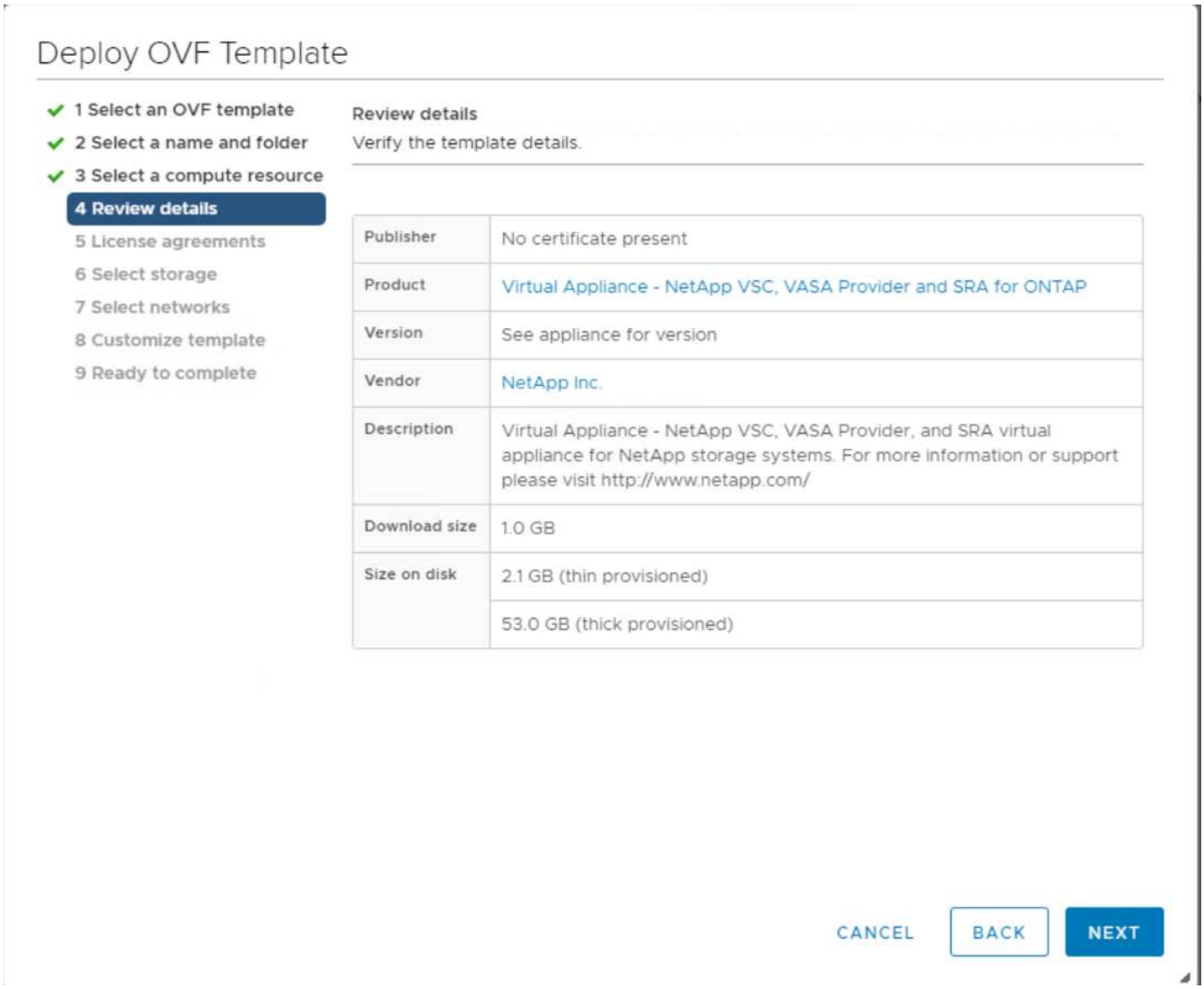
1. Vá para vSphere Web Client > Host Cluster > Deploy OVF Template.
2. Navegue até o arquivo OVF do VSC baixado do site de suporte da NetApp.



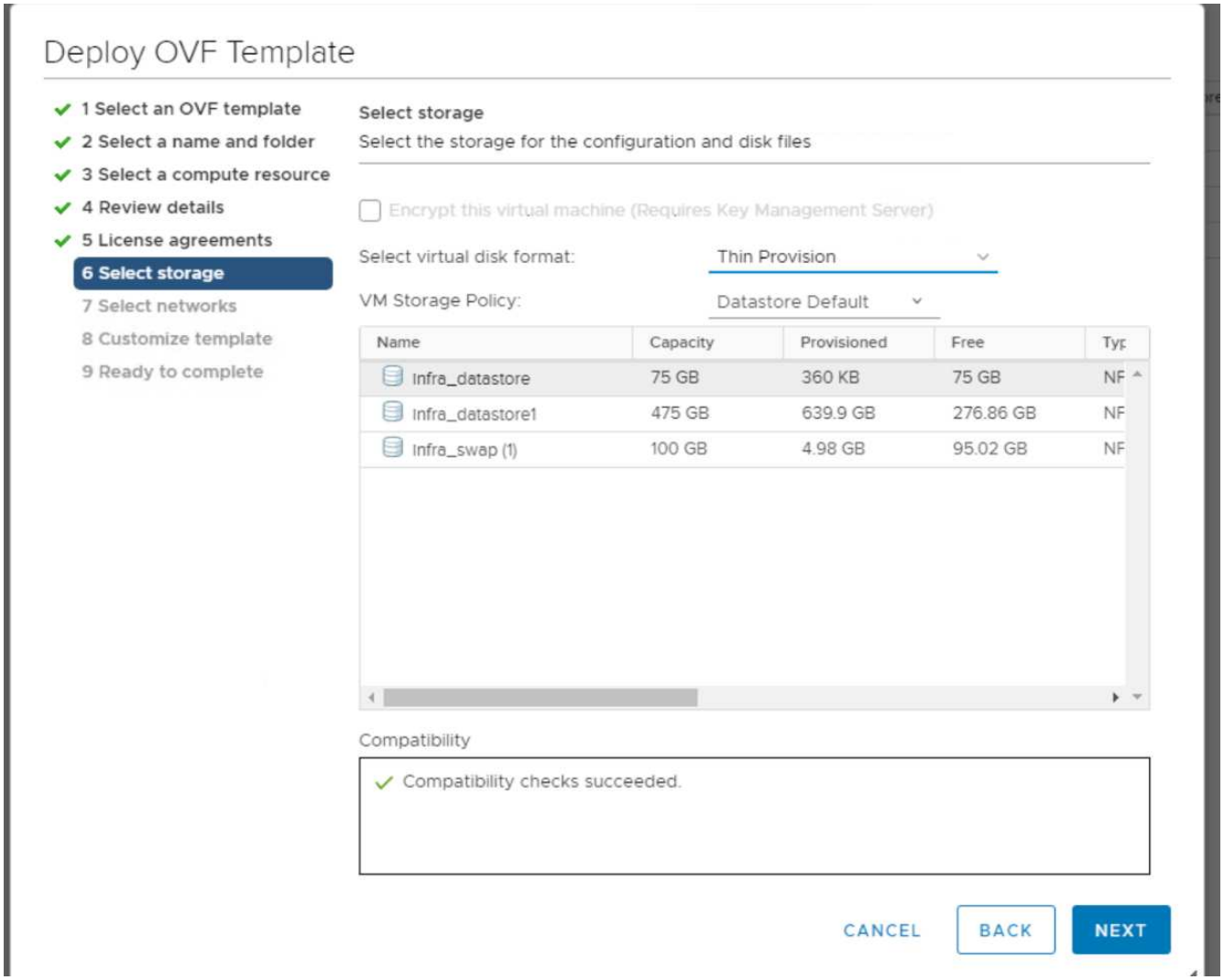
3. Introduza o nome da VM e selecione um centro de dados ou pasta na qual pretende implementar. Clique em seguinte.



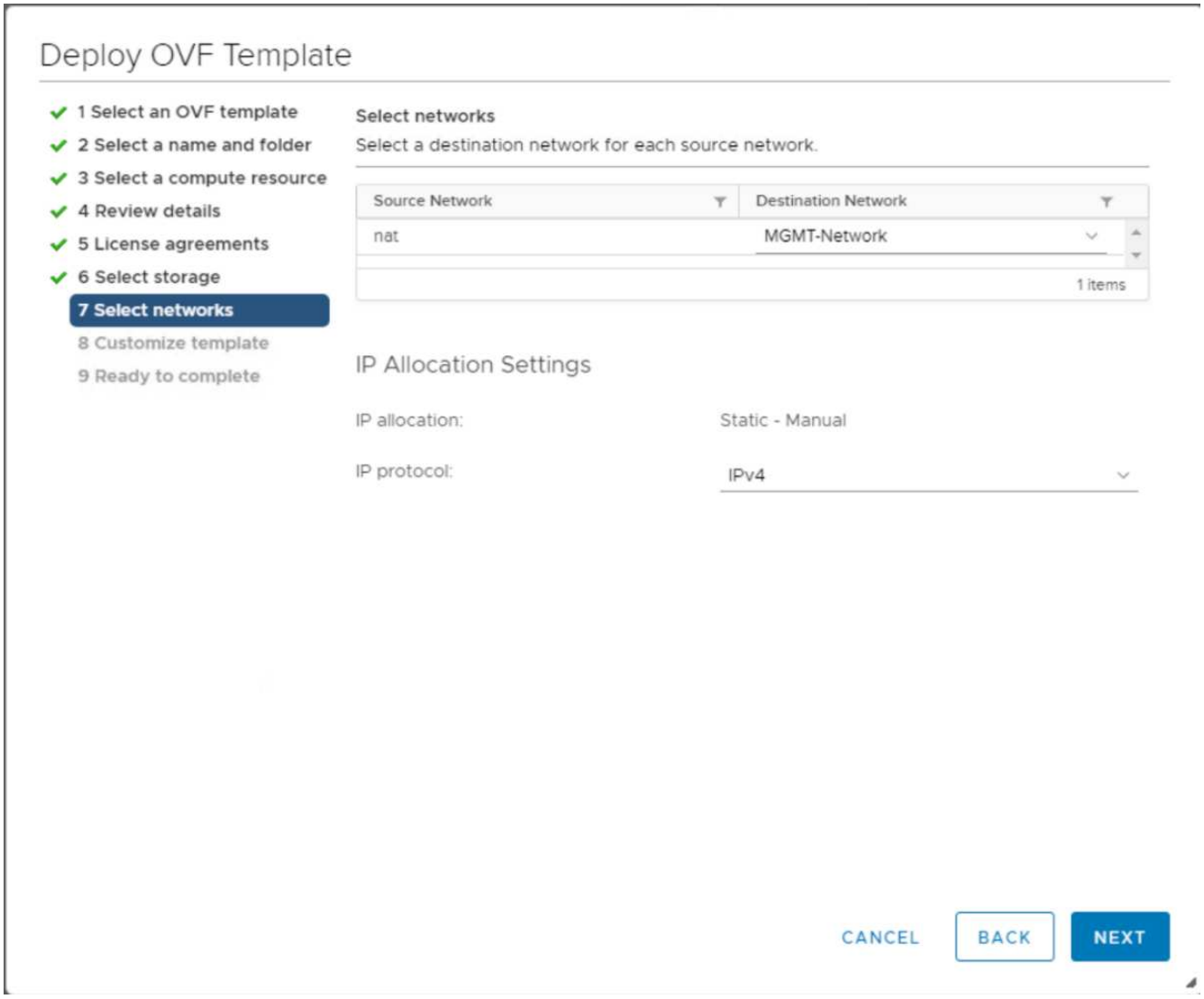
4. Selecione o cluster ESXi do FlexPod-Cluster e clique em Avançar.
5. Reveja os detalhes e clique em seguinte.



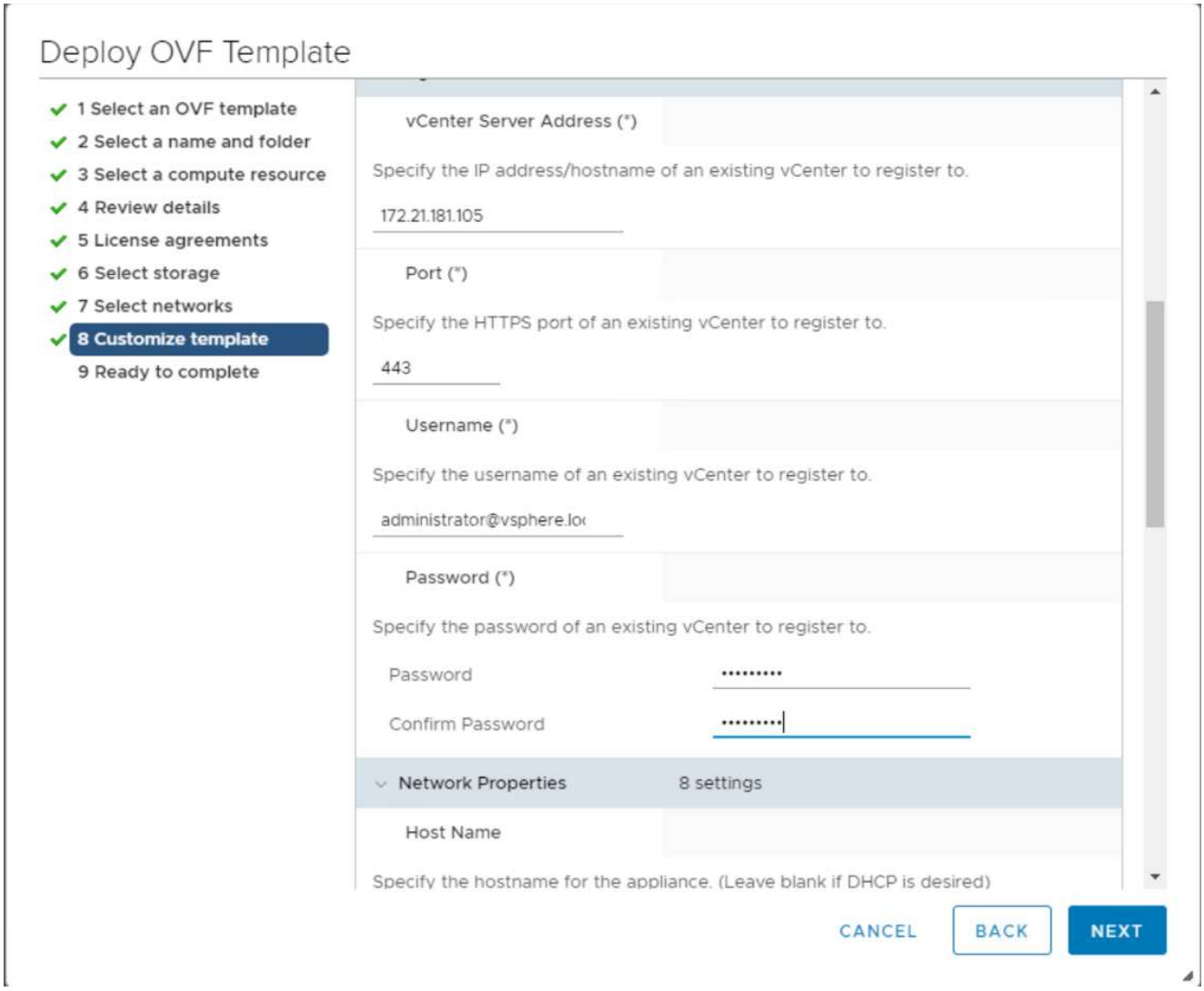
6. Clique em aceitar para aceitar a licença e clique em Avançar.
7. Selecione o formato de disco virtual de thin Provisioning e um dos datastores NFS. Clique em seguinte.



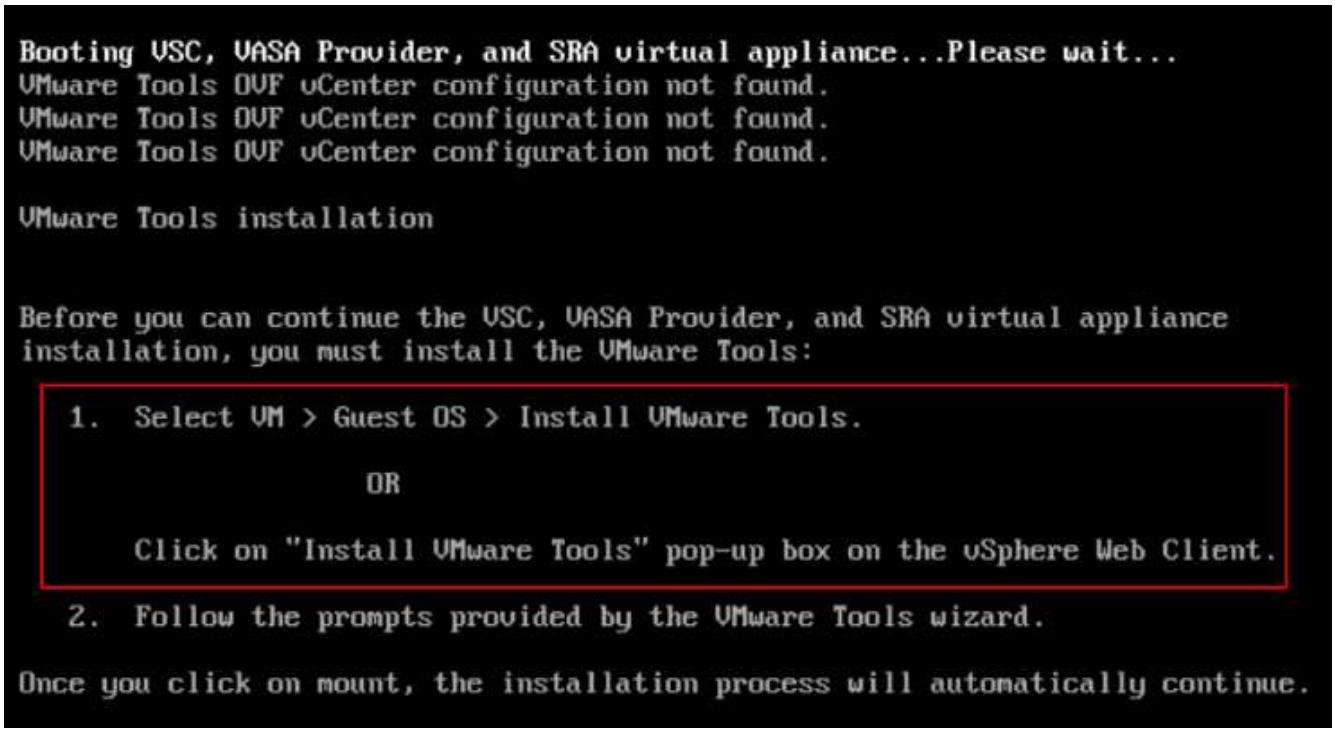
8. Em Selecionar redes, escolha uma rede de destino e clique em Avançar.



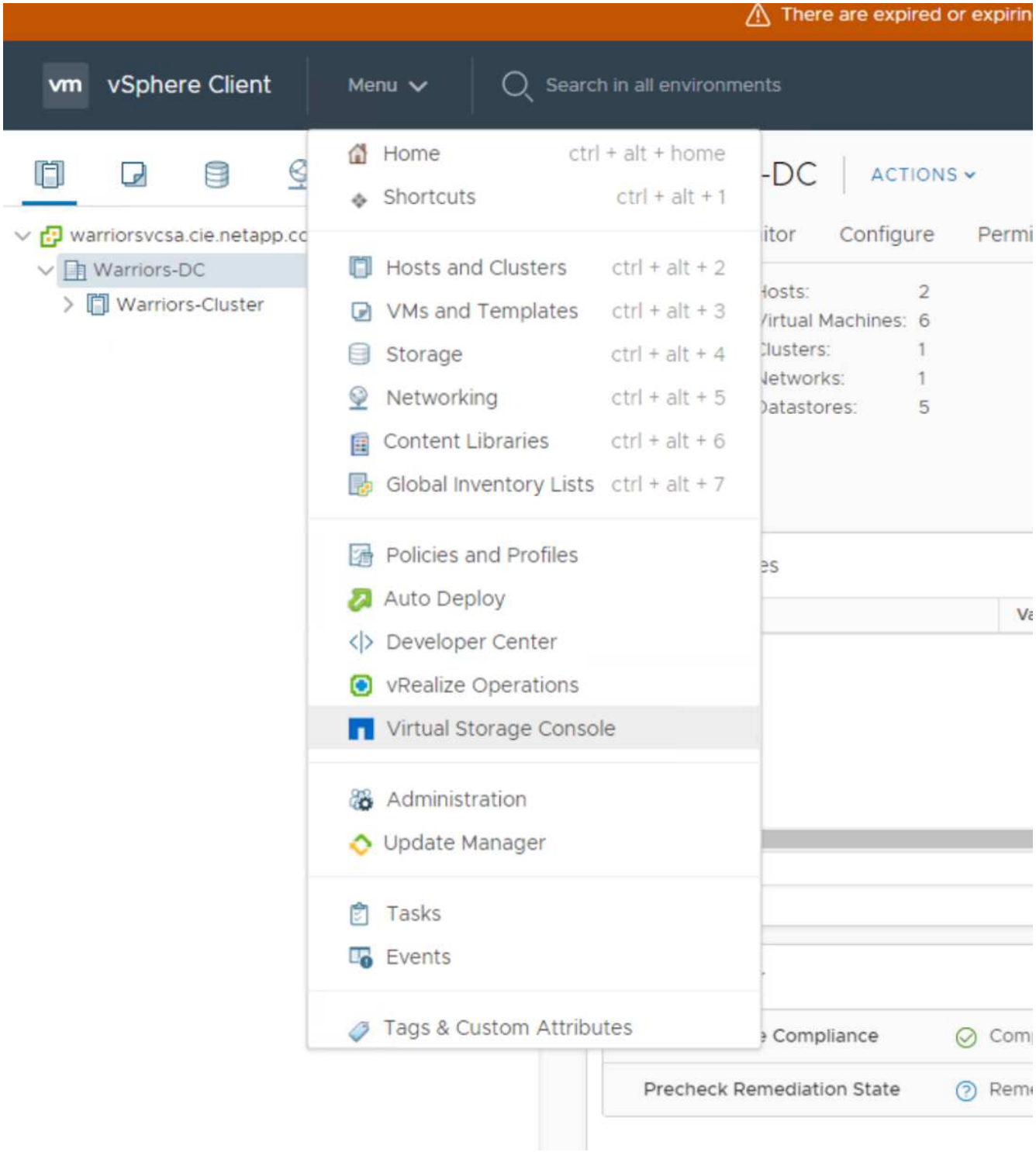
9. Em Personalizar modelo, insira a senha do administrador do VSC, o nome do vCenter ou o endereço IP e outros detalhes de configuração e clique em Avançar.



10. Revise os detalhes de configuração inseridos e clique em concluir para concluir a implantação da VM NetApp-VSC.
11. Ligue a VM NetApp-VSC e abra o console da VM.
12. Durante o processo de inicialização da VM do NetApp-VSC, você verá um prompt para instalar o VMware Tools. No vCenter, selecione NetApp-VSC VM > SO convidado > Instalar ferramentas VMware.



13. As informações de configuração de rede e Registro do vCenter foram fornecidas durante a personalização do modelo OVF. Portanto, depois que a VM NetApp-VSC estiver em execução, o VSC, a API vSphere for Storage Awareness (VASA) e o adaptador de replicação de armazenamento (SRA) da VMware são registrados no vCenter.
14. Faça logout do vCenter Client e faça login novamente. No menu inicial, confirme se o VSC do NetApp está instalado.



Faça o download e instale o plug-in NetApp NFS VAAI

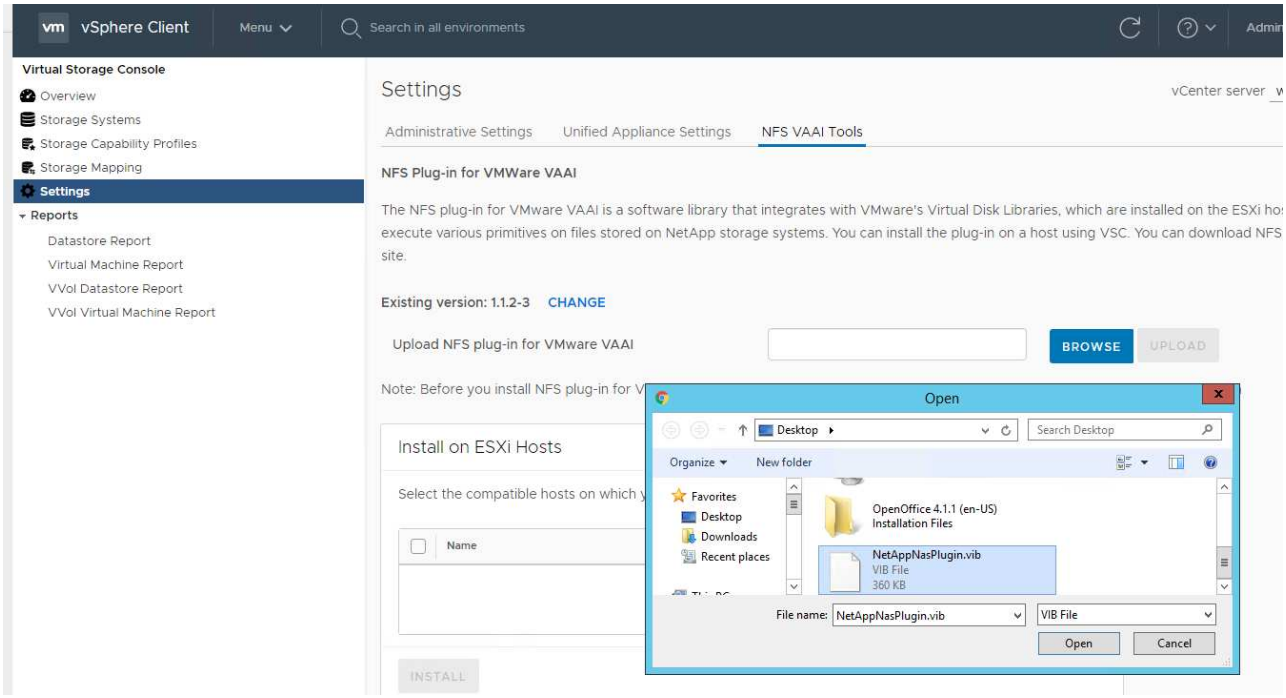
Para fazer o download e instalar o plug-in NetApp NFS VAAI, siga estas etapas:

1. Faça o download do plug-in NFS NetApp 1.1.2 para VMware `.vib` na página de download do plug-in NFS e salve-o em sua máquina local ou host admin.
2. Faça o download do plug-in NFS do NetApp para VMware VAAI:
   a. Vá para "página de download do software" .

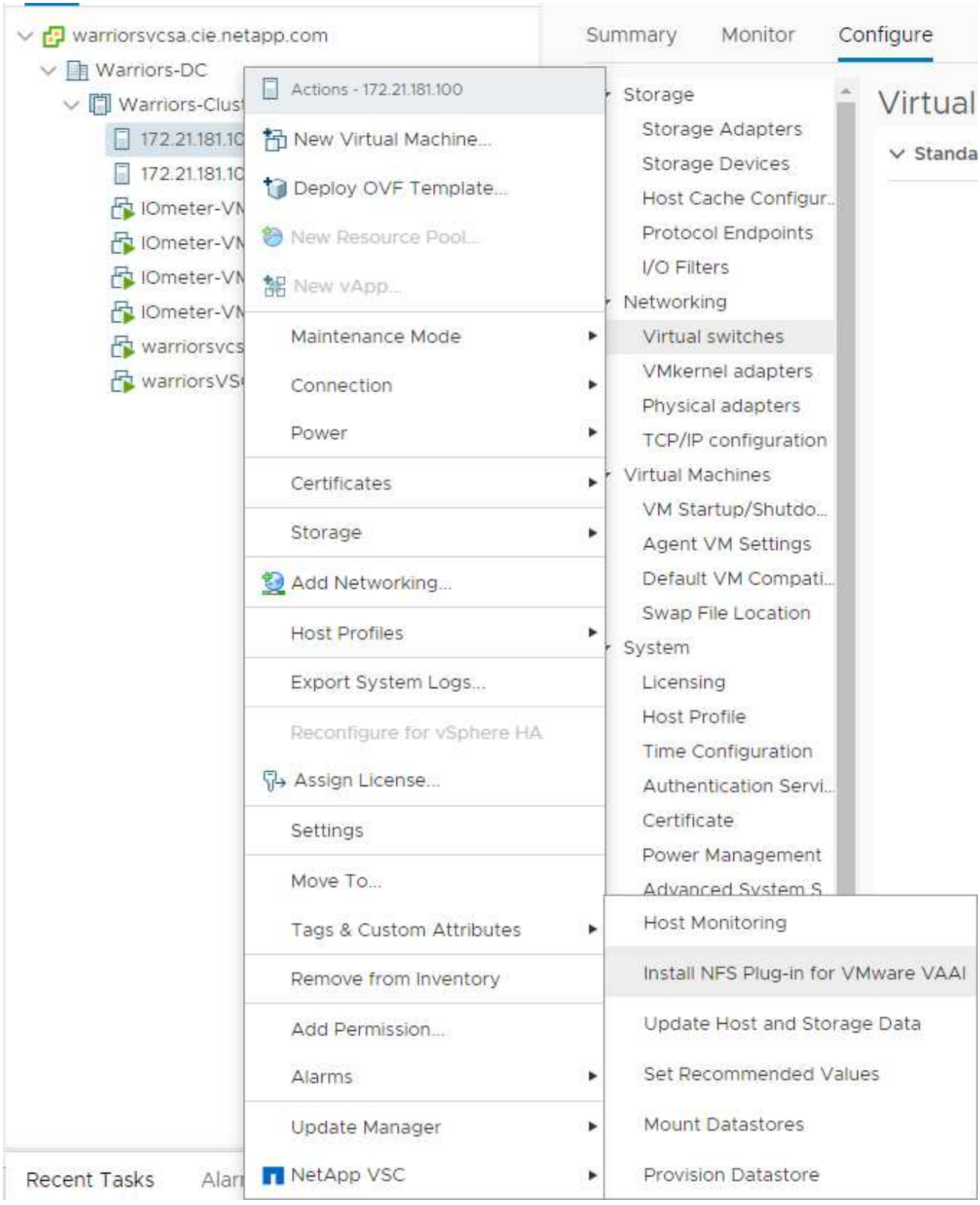
b. Role para baixo e clique em NetApp NFS Plug-in para VMware VAAI.

c. Na tela inicial do cliente da Web vSphere, selecione Virtual Storage Console.

d. Em Virtual Storage Console > Configurações > Ferramentas NFS VAAI, carregue o plug-in NFS escolhendo Selecionar arquivo e navegando até o local onde o plug-in baixado está armazenado.



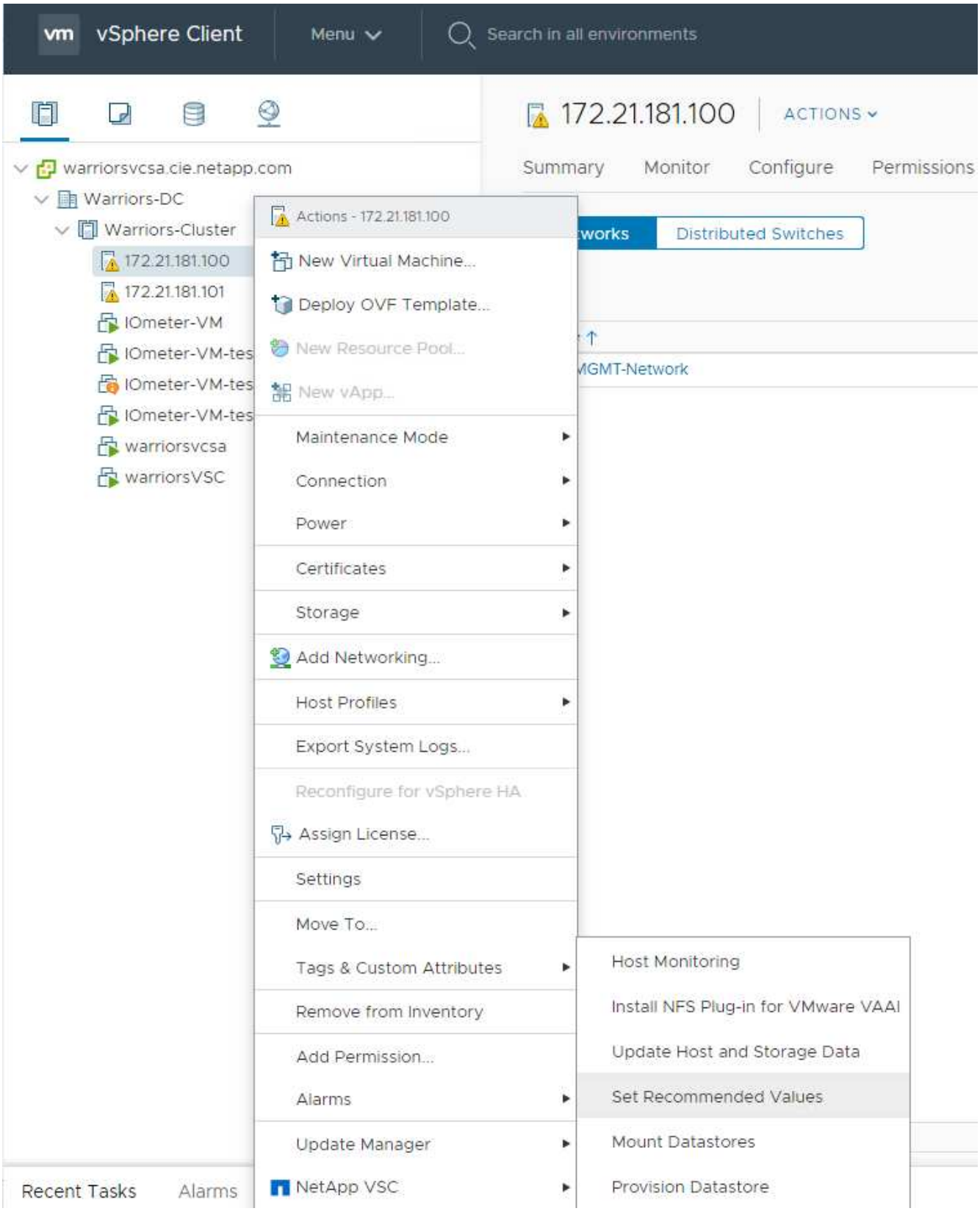
3. Clique em carregar para transferir o plug-in para o vCenter.
4. Selecione o host e, em seguida, selecione NetApp VSC > Instalar plug-in NFS para VMware VAAI.



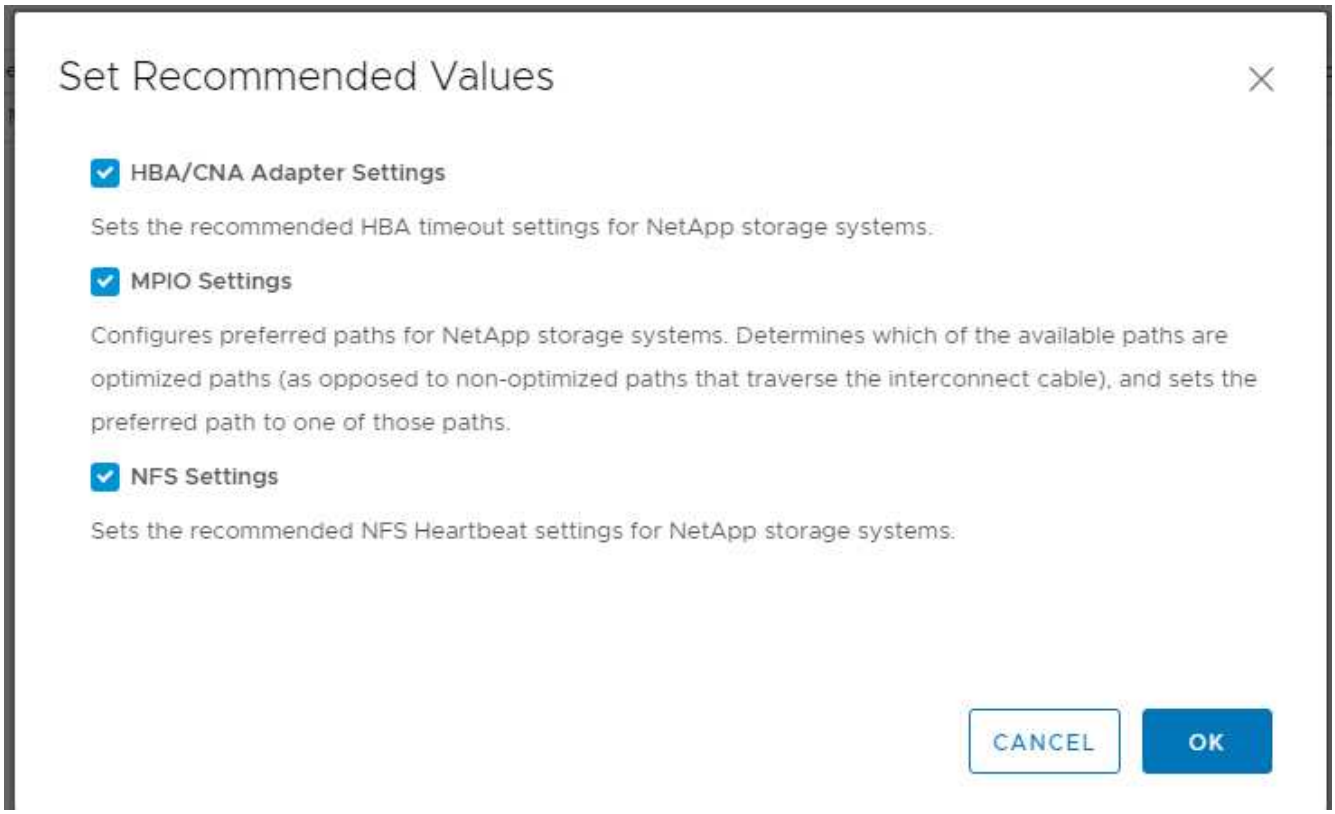
Use as configurações de armazenamento ideais para os hosts ESXi

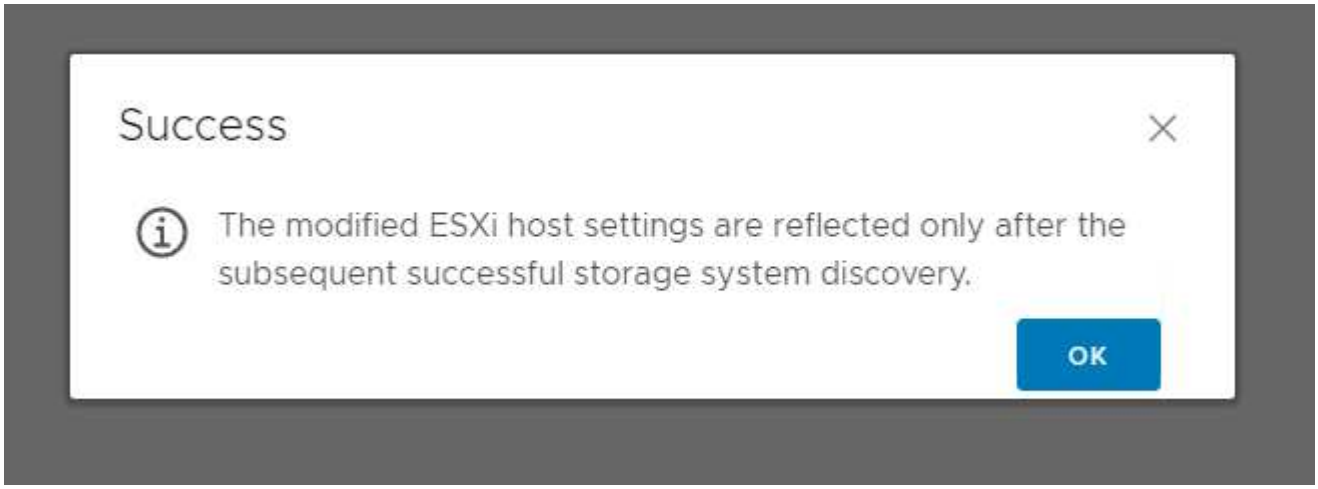
O VSC permite a configuração automatizada de configurações relacionadas ao armazenamento para todos os hosts ESXi que estão conetados aos controladores de armazenamento NetApp. Para usar essas configurações, execute as seguintes etapas:

1. Na tela inicial, selecione vCenter > hosts e clusters. Para cada host ESXi, clique com o botão direito do Mouse e selecione NetApp VSC > Definir valores recomendados.



2. Verifique as configurações que você gostaria de aplicar aos hosts vSphere selecionados. Clique em OK para aplicar as definições.





3. Reinicie o host ESXI após essas configurações serem aplicadas.

Conclusão

O FlexPod Express fornece uma solução simples e eficaz fornecendo um design validado que usa componentes líderes do setor. Com o dimensionamento por meio da adição de componentes, o FlexPod Express pode ser personalizado para necessidades específicas de negócios. O FlexPod Express foi projetado para empresas de pequeno e médio porte, ROBOs e outras empresas que exigem soluções dedicadas.

Agradecimentos

Os autores gostariam de reconhecer John George por seu apoio e contribuição para este

projeto.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

Documentação do produto NetApp

http://docs. "NetApp".com

FlexPod Express com guia

NVA-1139-DESIGN: FlexPod Express com Cisco UCS C-Series e NetApp AFF C190 Series

"https://www.netapp.com/us/media/nva-1139-design.pdf"

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Novembro de 2019	Lançamento inicial.

FlexPod Express com o guia de design da série C do Cisco UCS e da série AFF A220

NVA-1125-DESIGN: FlexPod Express com Cisco UCS C-Series e AFF A220 Series

Savita Kumari, NetApp em parceria com: 

As tendências do setor indicam uma grande transformação do data center em direção à infraestrutura compartilhada e à computação em nuvem. Além disso, as organizações buscam uma solução simples e eficaz para escritórios remotos e filiais, aproveitando a tecnologia com a qual elas estão familiarizadas no data center.

O FlexPod Express é uma arquitetura de data center pré-projetada e com práticas recomendadas desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e no NetApp AFF. Os componentes do FlexPod Express são como os seus homólogos do data center FlexPod, permitindo sinergias de gerenciamento em todo o ambiente de INFRAESTRUTURA DE TI em menor escala. O data center FlexPod e o FlexPod Express são plataformas ideais para virtualização e para sistemas operacionais bare-metal e workloads empresariais.

"Próximo: Resumo do programa."

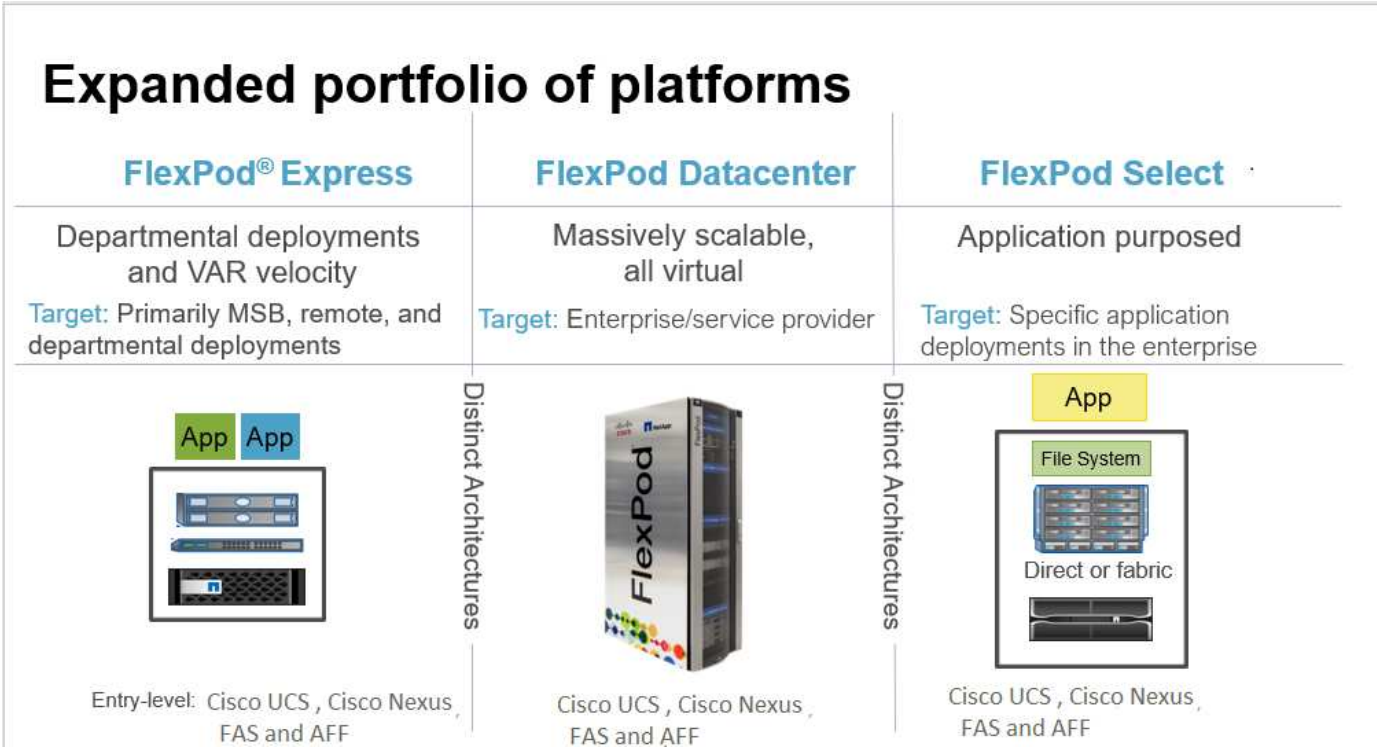
Resumo do programa

Portfólio de infraestrutura convergente do FlexPod

As arquiteturas de referência do FlexPod são entregues como Cisco Validated designs (CVDs) ou como NetApp Verified Architectures (NVAs). Desvios que são baseados nos requisitos do cliente de um determinado CVD ou NVA são permitidos se as variações não resultarem na implantação de configurações não suportadas.

Conforme ilustrado na figura a seguir, o portfólio do FlexPod inclui três soluções: FlexPod Express, FlexPod Datacenter e FlexPod Select:

- **FlexPod Express.** Oferece uma solução de nível básico que consiste em tecnologias da Cisco e da NetApp.
- **Centro de dados FlexPod.** Fornece uma base ideal para uso geral para vários workloads e aplicações.
- **FlexPod Select.** Incorpora os melhores aspetos do data center FlexPod e adapta a infraestrutura a uma determinada aplicação.



Programa NetApp Verified Architecture

O programa NVA oferece aos clientes uma arquitetura verificada para soluções NetApp. Um NVA significa que a solução NetApp tem as seguintes qualidades:

- É completamente testado
- É prescritiva por natureza
- Minimiza os riscos de implantação
- Acelera o time-to-market

Este guia detalha o design do FlexPod Express com o VMware vSphere. Além disso, esse design utiliza o novo sistema AFF A220, que executa o software NetApp ONTAP 9.4, os switches Cisco Nexus 3172P e os

servidores Cisco UCS C220 M5 como nós de hipervisor.

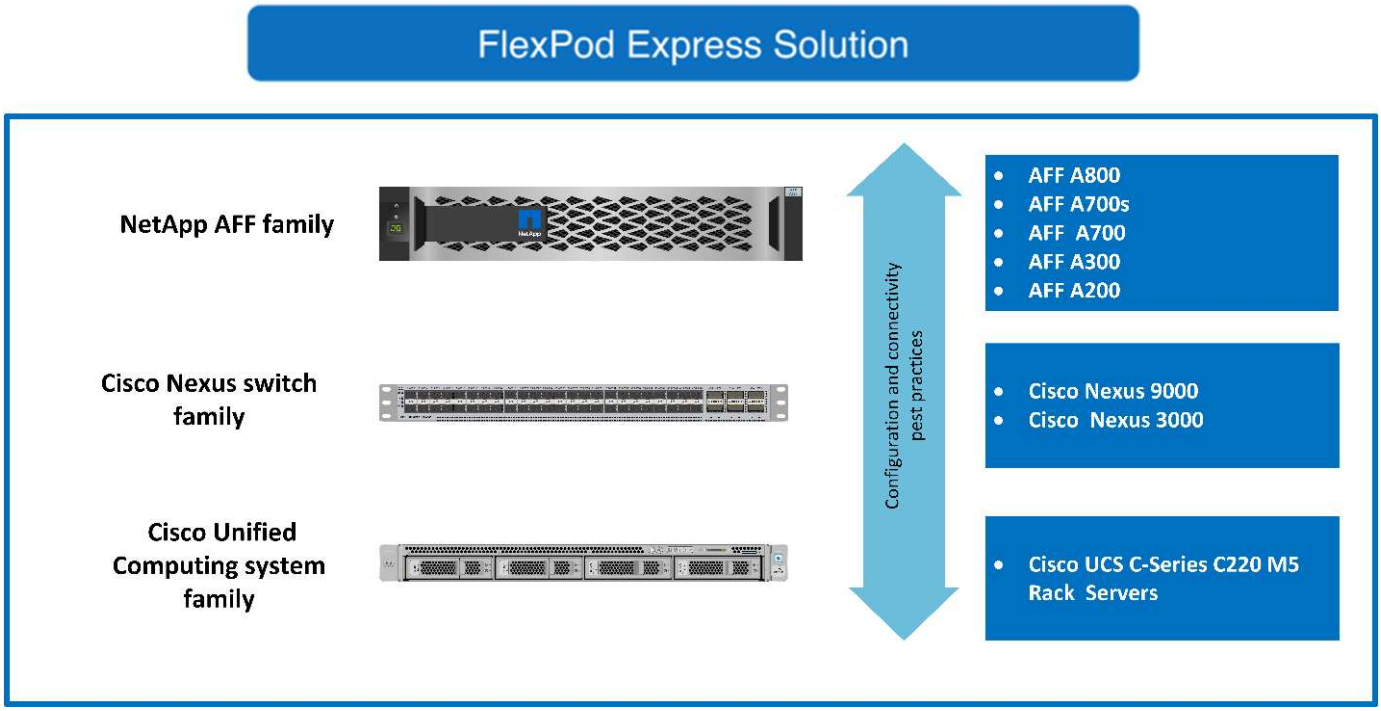
Embora este documento tenha sido validado para o AFF A220, essa solução também oferece suporte ao FAS2700.

"Próximo: Visão geral da solução."

Visão geral da solução

O FlexPod Express foi projetado para executar workloads de virtualização mistos. Ele é destinado a escritórios remotos e filiais e para empresas de pequeno e médio porte. Também é ideal para grandes empresas que desejam implementar uma solução dedicada para um propósito. Essa nova solução para o FlexPod Express adiciona novas tecnologias, como NetApp ONTAP 9.4, NetApp AFF A220 e VMware vSphere 6,7.

A figura a seguir mostra os componentes de hardware incluídos na solução FlexPod Express.



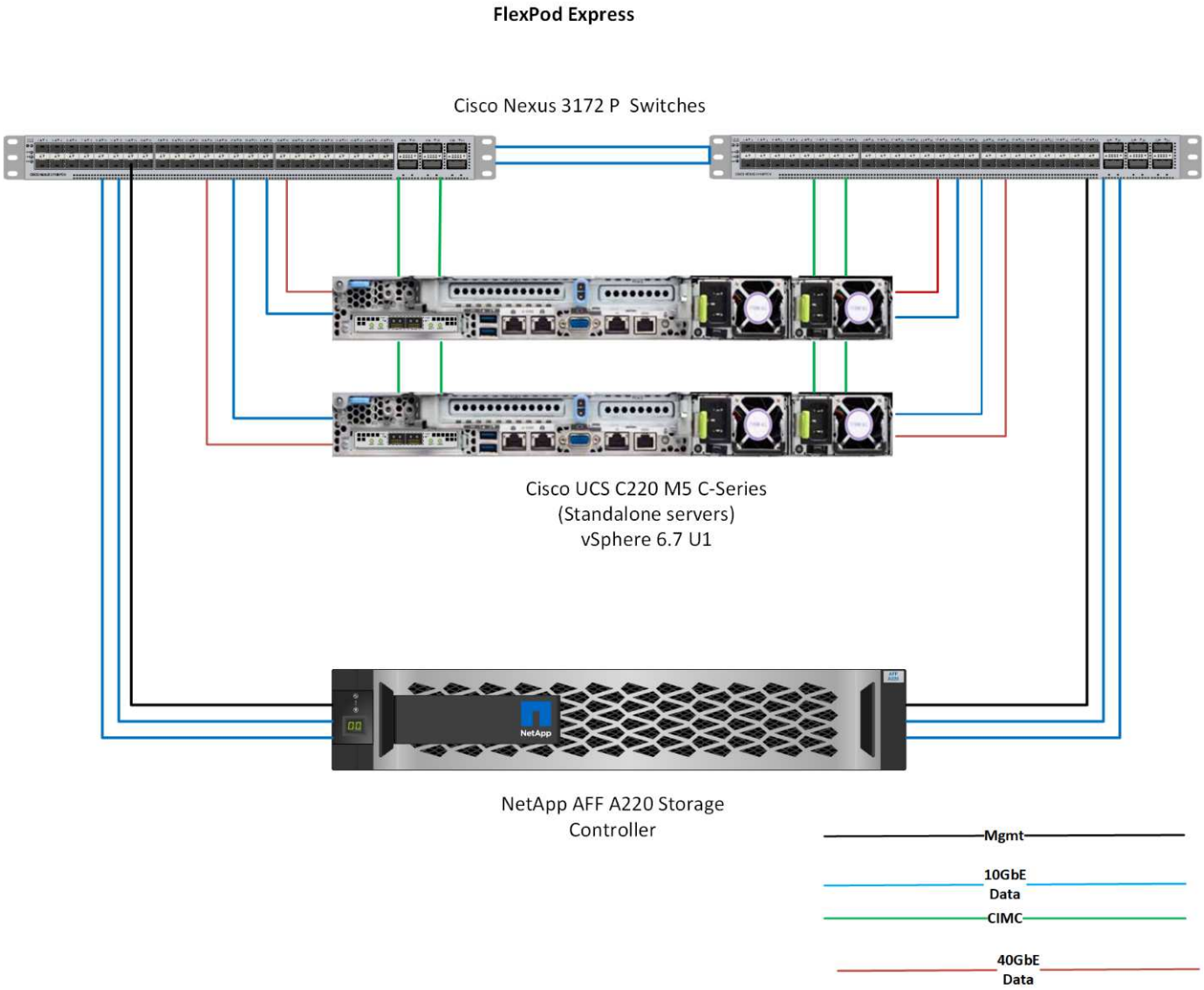
Público-alvo

Este documento destina-se àqueles que desejam aproveitar uma infraestrutura construída para fornecer eficiência DE TI e permitir a inovação DE TI. O público-alvo deste documento inclui, entre outros, engenheiros de vendas, consultores de campo, pessoal de serviços profissionais, gerentes DE TI, engenheiros DE parceiros e clientes.

Tecnologia da solução

Essa solução utiliza as tecnologias mais recentes da NetApp, Cisco e VMware. Essa solução conta com o novo sistema NetApp AFF A220, que executa o software ONTAP 9.4, os switches duplos Cisco Nexus 3172P e os servidores em rack Cisco UCS C220 M5 que executam o VMware vSphere 6,7. Essa solução validada usa a tecnologia 10-Gigabit Ethernet (10GbE). A figura a seguir apresenta uma visão geral. Também são fornecidas orientações sobre como escalar adicionando dois nós de hipervisor de cada vez, para que a

arquitetura FlexPod Express se adapte às crescentes necessidades de negócios da organização.



O 40GbE não foi validado, mas é uma infraestrutura compatível.

"Próximo: Requisitos de tecnologia."

Requisitos de tecnologia

O FlexPod Express requer uma combinação de componentes de hardware e software que depende do hipervisor selecionado e da velocidade da rede. Além disso, o FlexPod Express estabelece os componentes de hardware necessários para adicionar nós de hipervisor ao sistema em unidades de dois.

Requisitos de hardware

Independentemente do hypervisor escolhido, todas as configurações do FlexPod Express usam o mesmo hardware. Portanto, mesmo que os requisitos de negócios sejam alterados, qualquer hipervisor pode ser executado no mesmo hardware FlexPod Express.

A tabela a seguir lista os componentes de hardware necessários para todas as configurações do FlexPod Express e para implementar a solução. Os componentes de hardware que são usados em qualquer implementação específica da solução podem variar com base nos requisitos do cliente.

Hardware	Quantidade
Cluster de dois nós do AFF A220	1
Servidor Cisco UCS C220 M5	2
Switch Cisco Nexus 3172P	2
Placa de interface virtual (VIC) Cisco UCS 1387 para servidor de rack Cisco UCS C220 M5	2
Adaptador Cisco CVR-QSFP-SFP10G	4

Requisitos de software

As tabelas a seguir listam os componentes de software necessários para implementar as arquiteturas da solução FlexPod Express.

A tabela a seguir lista os requisitos de software para a implementação básica do FlexPod Express.

Software	Versão	Detalhes
Controlador de gerenciamento integrado Cisco (CIMC)	3.1.3	Para servidores em rack C220 M5
Cisco NX-os	nxos.7.0.3.I7.5.bin	Para switches Cisco Nexus 3172P
NetApp ONTAP	9,4	Para controladores AFF A220

A tabela a seguir lista o software necessário para todas as implementações do VMware vSphere no FlexPod Express.

Software	Versão
Dispositivo VMware vCenter Server	6,7
VMware vSphere ESXi	6,7
Plug-in NetApp VAAI para ESXi	1.1.2

"Próximo: Opções de design."

Opções de design

As seguintes tecnologias foram escolhidas durante o processo de arquitetura deste projeto. Cada tecnologia atende a um propósito específico na solução de infraestrutura FlexPod Express.

Série NetApp AFF A220 com ONTAP 9 .4

Essa solução aproveita dois dos mais novos produtos NetApp: O software NetApp AFF A220 e ONTAP 9.4.

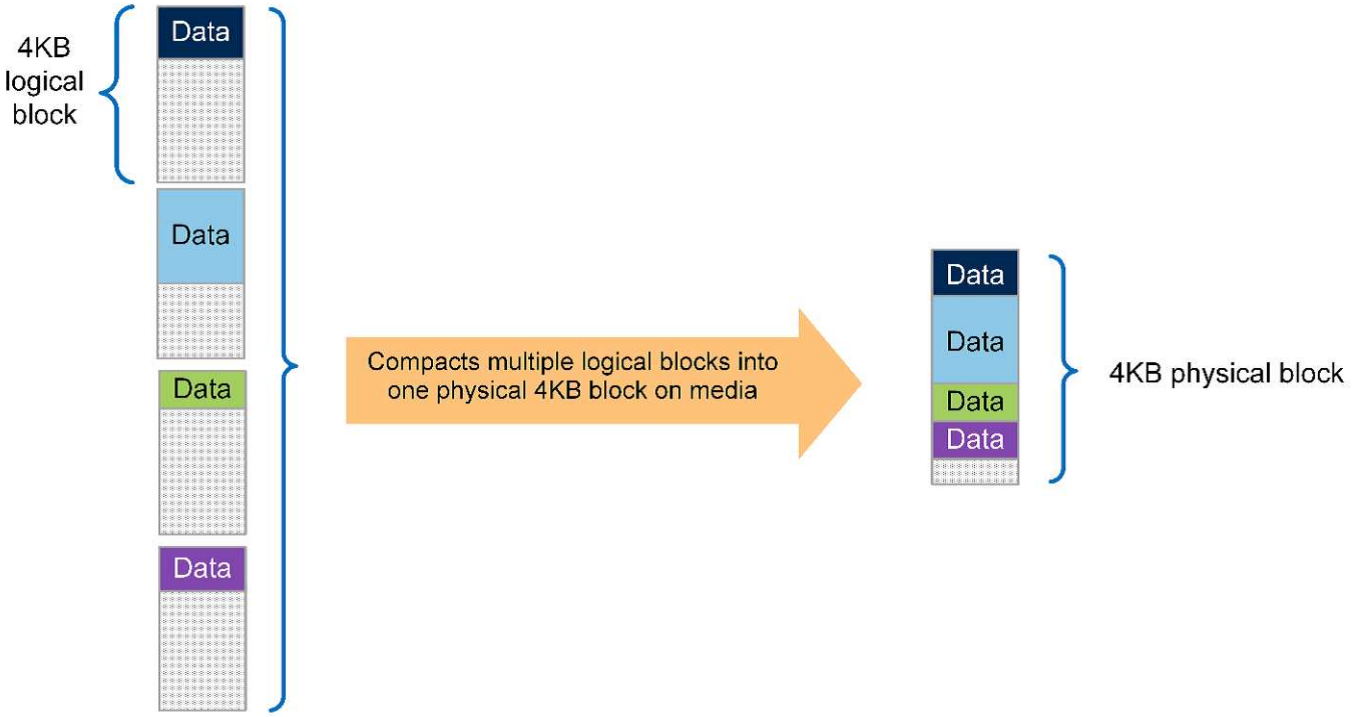
Sistema AFF A220

Para obter mais informações sobre o sistema de hardware AFF A220, consulte "Página inicial do AFF Série A.".

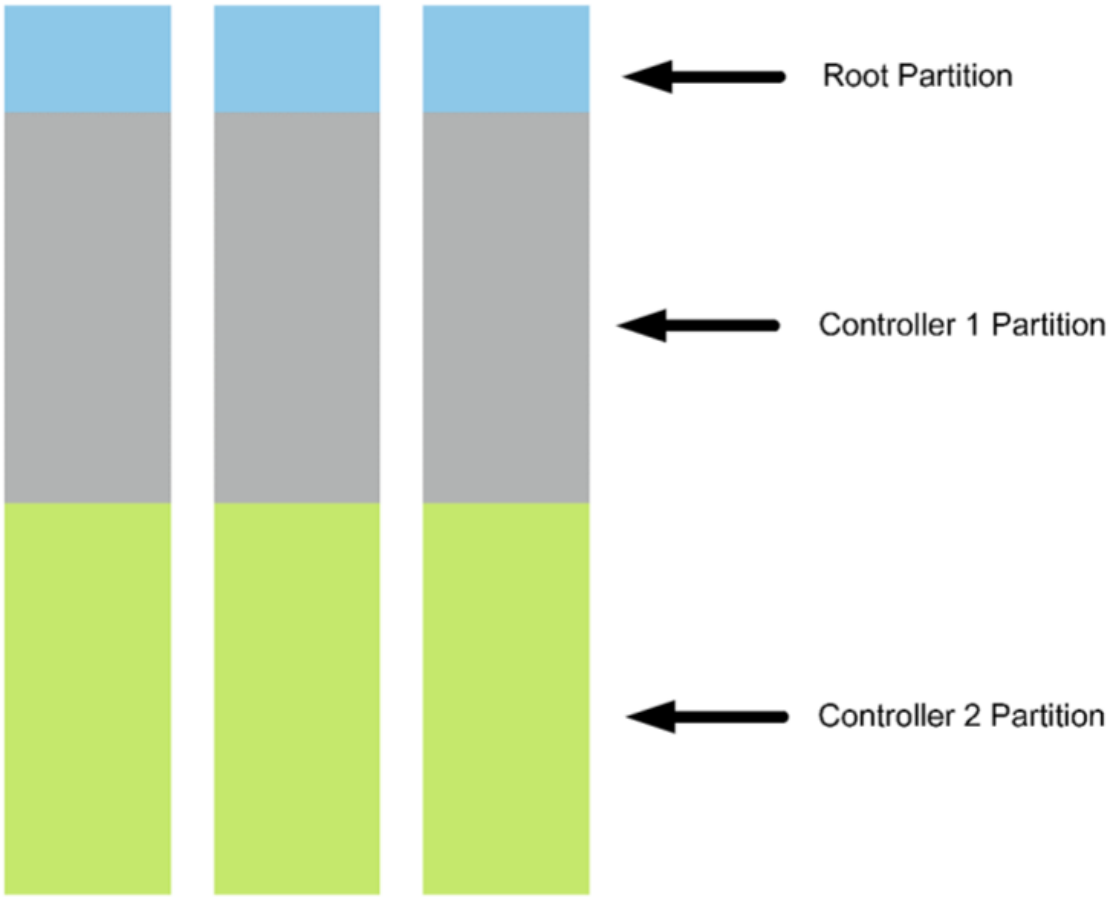
Software ONTAP 9.4

Os sistemas NetApp AFF A220 usam o novo software ONTAP 9.4. O ONTAP 9.4 é o software empresarial de gerenciamento de dados líder do setor. Ele combina novos níveis de simplicidade e flexibilidade com funcionalidades avançadas de gerenciamento de dados, eficiências de storage e integração com a nuvem líder.

O ONTAP 9.4 tem vários recursos que são adequados para a solução FlexPod Express. O mais importante é o compromisso da NetApp com a eficiência de storage, que pode ser um dos recursos mais importantes para implantações de pequeno porte. Os recursos de eficiência de storage da NetApp, como deduplicação, compressão e thin Provisioning, estão disponíveis no ONTAP 9.4 com uma nova adição e compactação. Como o sistema NetApp WAFL grava sempre blocos 4KB, a compactação combina vários blocos em um bloco 4KB quando os blocos não estão usando o espaço alocado de 4KB. A figura a seguir ilustra esse processo.



Além disso, o particionamento de dados raiz pode ser aproveitado no sistema AFF A220. Esse particionamento permite que o agregado raiz e dois agregados de dados sejam distribuídos pelos discos no sistema. Portanto, ambas as controladoras em um cluster de AFF A220 de dois nós podem aproveitar o desempenho de todos os discos no agregado. Consulte a figura a seguir.



Esses são apenas alguns dos principais recursos que complementam a solução FlexPod Express. Para obter detalhes sobre os recursos adicionais e a funcionalidade do ONTAP 9.4, consulte "Folha de dados do software de gerenciamento de dados ONTAP 9". Além disso, consulte o NetApp "Centro de Documentação do ONTAP 9" , que foi atualizado para incluir o ONTAP 9.4.

Cisco Série Nexus 3000

O Cisco Nexus 3172P é um switch robusto e econômico que oferece comutação 1/10/40/100Gbps. O switch Cisco Nexus 3172PQ, parte da família Unified Fabric, é um switch compacto de 1 unidades de rack (1RUU) para implantações de data center topo do rack. (Consulte a figura a seguir.) Ele oferece até setenta e duas portas 1/10GbE em 1RU ou quarenta e oito 1/10GbE mais seis portas 40GbE em 1RU. E para a máxima flexibilidade da camada física, ele também suporta 1/10/40Gbps.

Como todos os vários modelos da série Cisco Nexus executam o mesmo sistema operacional subjacente, NX-os, vários modelos Cisco Nexus são suportados nas soluções FlexPod Express e FlexPod Datacenter.

As especificações de desempenho incluem:

- Taxa de transferência de tráfego de taxa de linha (ambas as camadas 2 e 3) em todas as portas
- Unidades de transmissão máxima configuráveis (MTUs) de até 9216 bytes (quadros jumbo)

Para obter mais informações sobre os switches Cisco Nexus 3172, consulte "Ficha de dados dos switches Cisco Nexus 3172PQ, 3172TQ, 3172TQ-32T, 3172PQ-XL e 3172TQ-XL".

Cisco UCS C-Series

O servidor de rack Cisco UCS C-Series foi escolhido para o FlexPod Express porque suas muitas opções de configuração permitem que ele seja adaptado para requisitos específicos em uma implantação do FlexPod Express.

Os servidores de rack Cisco UCS C-Series oferecem computação unificada em um fator forma padrão do setor para reduzir o TCO e aumentar a agilidade.

Os servidores de rack Cisco UCS C-Series oferecem os seguintes benefícios:

- Um ponto de entrada independente de fator de forma no Cisco UCS
- Implantação de aplicações simplificada e rápida
- Extensão das inovações e benefícios da computação unificada para servidores em rack
- Maior escolha do cliente com benefícios exclusivos em um pacote de rack familiar

O servidor de rack Cisco UCS C220 M5 (na figura anterior) está entre os servidores de aplicativos e infraestrutura empresarial de uso geral mais versáteis do setor. É um servidor em rack de dois soquetes de alta densidade que oferece desempenho e eficiência líderes do setor para uma ampla variedade de workloads, incluindo virtualização, colaboração e aplicações bare-metal. Os servidores em rack Cisco UCS C-Series podem ser implantados como servidores autônomos ou como parte do Cisco UCS para aproveitar as inovações de computação unificada baseadas em padrões da Cisco que ajudam a reduzir o TCO dos clientes e a aumentar a agilidade nos negócios.

Para obter mais informações sobre servidores C220 M5, consulte "Folha de dados do servidor de rack Cisco UCS C220 M5".

Opções de conetividade para C220 M5 servidores de rack

As opções de conetividade para os servidores de rack C220 M5 são as seguintes:

- **Cisco 1387**

  O Cisco UCS VIC 1387 (na figura a seguir) oferece duas portas melhoradas QSFP 40GbE e FC sobre Ethernet (FCoE) em um fator de forma modular-laN-on-motherboard (mLOM). O slot mLOM pode ser

usado para instalar um VIC Cisco sem consumir um slot PCIe (Peripheral Component Interconnect Express), proporcionando maior capacidade de expansão de e/S.

Para obter mais informações sobre o adaptador Cisco UCS VIC 1387, consulte a "Placa de interface virtual Cisco UCS 1387" folha de dados.

- **ADAPTADOR CVR-QSFP-SFP10G**

  O módulo Cisco QSA converte uma porta QSFP em uma porta SFP ou SFP. Com este adaptador, os clientes têm a flexibilidade de usar qualquer módulo ou cabo SFP ou SFP para se conetar a uma porta de menor velocidade na outra extremidade da rede. Essa flexibilidade permite uma transição econômica para o 40GbE, maximizando o uso de plataformas QSFP de alta densidade 40GbE. Este adaptador suporta todas as óticas SFP e alcances de cabo, e suporta vários módulos SFP 1GbE. Como este projeto foi validado usando a conetividade 10GbE e como o VIC 1387 usado é 40GbE, o adaptador CVR-QSFP-SFP10G (na figura a seguir) é usado para conversão.

VMware vSphere 6,7

O VMware vSphere 6,7 é uma opção de hipervisor para uso com o FlexPod Express. O VMware vSphere permite que as organizações reduzam sua capacidade de energia e refrigeração, ao mesmo tempo em que confirmam que a capacidade de computação comprada é usada ao máximo. Além disso, o VMware vSphere permite a proteção contra falhas de hardware (VMware High Availability, ou VMware HA) e o balanceamento

de carga de recursos de computação em um cluster de hosts vSphere (VMware Distributed Resource Scheduler ou VMware DRS).

Como ele reinicia apenas o kernel, o VMware vSphere 6,7 permite que os clientes "iniciem rápido" onde carrega o vSphere ESXi sem reiniciar o hardware. Esse recurso está disponível apenas com plataformas e drivers que estão na lista de permissões de Inicialização rápida. O vSphere 6,7 amplia os recursos do vSphere Client, que pode fazer cerca de 90% do que o vSphere Web Client pode fazer.

No vSphere 6,7, a VMware estendeu essa capacidade para permitir que os clientes definam a compatibilidade aprimorada do vMotion (EVC) por máquina virtual (VM) em vez de por host. No vSphere 6,7, a VMware também expôs as APIs que podem ser usadas para criar clones instantâneos.

Veja a seguir alguns dos recursos do vSphere 6,7 U1:

- VSphere Client baseado na Web HTML5 totalmente equipado
- VMotion para VMs vGPU DA GRADE do NVIDIA. Suporte para Intel FPGA.
- VCenter Server Converge Tool para passar de PSC externo para PCS internos.
- Aprimoramentos para VSAN (atualizações de HCI).
- Biblioteca de conteúdo aprimorada.

Para obter detalhes sobre o vSphere 6,7 U1, "Novidades no vCenter Server 6,7 Update 1" consulte . Embora essa solução tenha sido validada com o vSphere 6,7, ela suporta qualquer versão do vSphere qualificada com os outros componentes pela ferramenta de Matriz de interoperabilidade do NetApp. A NetApp recomenda a implantação do vSphere 6.7U1 para suas correções e recursos aprimorados.

Arquitetura de inicialização

A seguir estão as opções suportadas para a arquitetura de arranque do FlexPod Express:

- ISCSI SAN LUN
- Cartão SD Cisco FlexFlash
- Disco local

Como o FlexPod Datacenter é inicializado a partir de iSCSI LUNs, a capacidade de gerenciamento da solução é aprimorada também usando o iSCSI boot para FlexPod Express.

"Próximo: Verificação da solução."

Verificação da solução

A Cisco e a NetApp projetaram e construíram o FlexPod Express para servir como uma plataforma de infraestrutura de primeira linha para seus clientes. Por ser desenvolvido com componentes líderes do setor, os clientes podem confiar no FlexPod Express como sua base de infraestrutura. De acordo com os princípios fundamentais do portfólio do FlexPod, a arquitetura do FlexPod Express foi completamente testada pelos arquitetos e engenheiros do data center Cisco e NetApp. Da redundância e disponibilidade a cada recurso individual, toda a arquitetura do FlexPod Express é validada para incutir confiança em nossos clientes e criar confiança no processo de design.

O VMware vSphere 6,7 foi verificado nos componentes da infraestrutura do FlexPod Express. Essa validação

incluiu 10GbE opções de conetividade uplink para o hipervisor.

"Próximo: Conclusão."

Conclusão

O FlexPod Express oferece uma solução simples e eficaz fornecendo um design validado que usa componentes líderes do setor. Ao dimensionar e ao fornecer opções para a plataforma de hypervisor, o FlexPod Express pode ser adaptado para necessidades específicas de negócios. O FlexPod Express foi projetado tendo em mente empresas de pequeno e médio porte, escritórios remotos e filiais e outras empresas que exigem soluções dedicadas.

"Próximo: Onde encontrar informações adicionais."

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- Documentação do NetApp

  "https://docs.netapp.com"

- FlexPod Express com o VMware vSphere 6,7 e o Guia de implantação do NetApp AFF A220

  "https://www.netapp.com/us/media/nva-1123-deploy.pdf"

Guia de implantação do FlexPod Express com o Cisco UCS C-Series e o AFF A220 Series

NVA-1123-DEPLOY: FlexPod Express com o guia de implantação do VMware vSphere 6,7 e NetApp AFF A220

Saraiva, NetApp

Em parceria com: 

As tendências do setor indicam uma grande transformação do data center em direção à infraestrutura compartilhada e à computação em nuvem. Além disso, as organizações buscam uma solução simples e eficaz para escritórios remotos e filiais, aproveitando a tecnologia com a qual elas estão familiarizadas em seu data center.

O FlexPod Express é uma arquitetura de data center pré-projetada e com práticas recomendadas desenvolvida com base no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e nas tecnologias de storage da NetApp. Os componentes de um sistema FlexPod Express são

como os seus homólogos do data center FlexPod, permitindo sinergias de gerenciamento em todo o ambiente de INFRAESTRUTURA DE TI em menor escala. O data center FlexPod e o FlexPod Express são plataformas ideais para virtualização e para sistemas operacionais bare-metal e workloads empresariais.

O data center FlexPod e o FlexPod Express oferecem uma configuração de linha de base e têm a flexibilidade de ser dimensionados e otimizados para acomodar vários casos de uso e requisitos diferentes. Os clientes de data center FlexPod existentes podem gerenciar o sistema FlexPod Express com as ferramentas às quais estão acostumados. Os novos clientes do FlexPod Express podem se adaptar facilmente ao gerenciamento do data center FlexPod à medida que seu ambiente cresce.

O FlexPod Express é uma base ideal de infraestrutura para escritórios remotos e filiais e para empresas de pequeno e médio porte. Ele também é uma solução ideal para clientes que desejam fornecer infraestrutura para um workload dedicado.

O FlexPod Express fornece uma infraestrutura fácil de gerenciar, adequada para praticamente qualquer workload.

Visão geral da solução

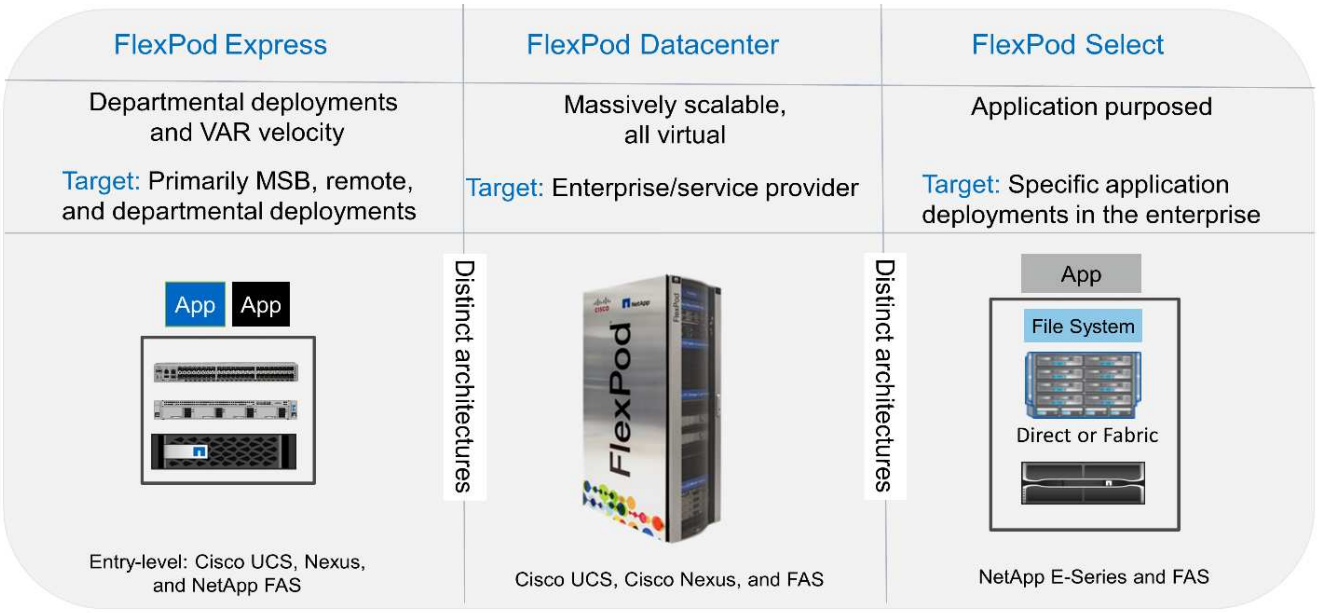
Esta solução FlexPod Express faz parte do Programa de infraestrutura convergente da FlexPod.

Programa de infraestrutura convergente da FlexPod

As arquiteturas de referência do FlexPod são entregues como Cisco Validated designs (CVDs) ou NetApp Verified Architectures (NVAs). Desvios com base nos requisitos do cliente de um determinado CVD ou NVA são permitidos se essas variações não criarem uma configuração não suportada.

Como descrito na figura abaixo, o programa FlexPod inclui três soluções: FlexPod Express, FlexPod Datacenter e FlexPod Select:

- **FlexPod Express.** Oferece aos clientes uma solução de nível básico com tecnologias da Cisco e NetApp.
- **Centro de dados FlexPod.** Fornece uma base ideal para uso geral para vários workloads e aplicações.
- **FlexPod Select.** Incorpora os melhores aspetos do data center FlexPod e adapta a infraestrutura a uma determinada aplicação.



Programa de arquitetura verificada NetApp

O programa NetApp Verified Architecture oferece aos clientes uma arquitetura verificada para soluções NetApp. Uma arquitetura verificada do NetApp fornece uma arquitetura de solução NetApp com as seguintes qualidades:

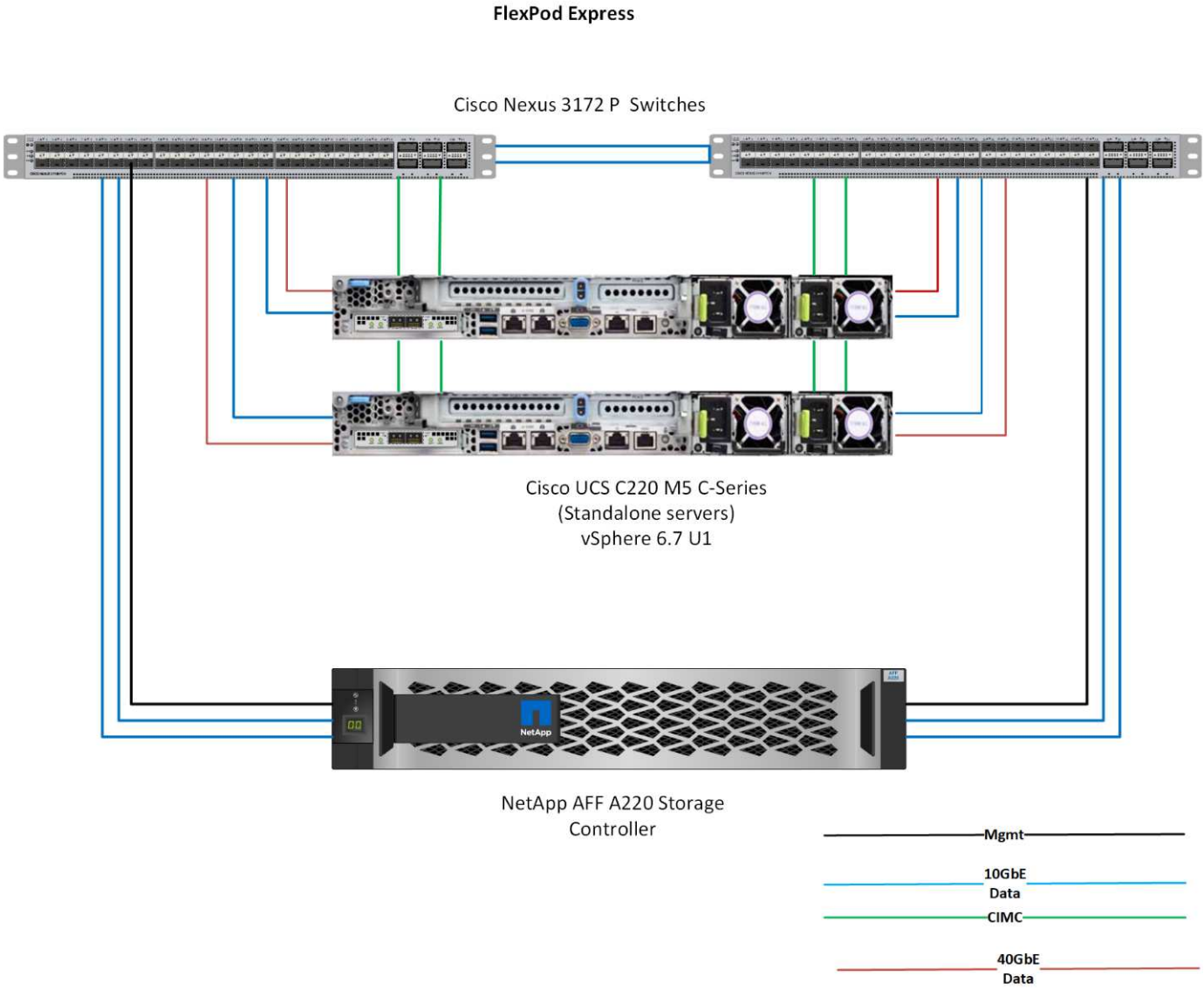
- É completamente testado
- É prescritiva por natureza
- Minimiza os riscos de implantação
- Acelera o time-to-market

Este guia detalha o design do FlexPod Express com o VMware vSphere. Além disso, esse design usa o novo sistema AFF A220, que executa o NetApp ONTAP 9.4; o Cisco Nexus 3172P e os servidores Cisco UCS C-Series C220 M5 como nós de hipervisor.

Tecnologia da solução

Essa solução utiliza as tecnologias mais recentes da NetApp, Cisco e VMware. Essa solução conta com o novo NetApp AFF A220 executando o ONTAP 9.4, os switches duplos Cisco Nexus 3172P e os servidores de rack Cisco UCS C220 M5 que executam o VMware vSphere 6,7. Essa solução validada usa a tecnologia 10GbE. Também são fornecidas orientações sobre como dimensionar a capacidade computacional adicionando dois nós de hipervisor de cada vez, para que a arquitetura FlexPod Express se adapte às crescentes necessidades de negócios da organização.

A figura a seguir mostra o FlexPod Express com a arquitetura do VMware vSphere 10GbE.



Esta validação utiliza a conetividade 10GbE e um Cisco UCS VIC 1387, que é 40GbE. Para alcançar a conetividade 10GbEG, o adaptador CVR-QSFP-SFP10G é usado.

Resumo do caso de uso

A solução FlexPod Express pode ser aplicada a vários casos de uso, incluindo os seguintes:

- Escritórios remotos ou filiais
- Pequenas e médias empresas
- Ambientes que exigem uma solução dedicada e econômica

O FlexPod Express é mais adequado para workloads virtualizados e mistos.

Embora essa solução tenha sido validada com o vSphere 6,7, ela suporta qualquer versão do vSphere qualificada com os outros componentes pela ferramenta de Matriz de interoperabilidade do NetApp. A NetApp recomenda a implantação do vSphere 6.7U1 para suas correções e recursos aprimorados.

A seguir estão alguns recursos do vSphere 6,7 U1:

- Cliente vSphere baseado na web HTML5 totalmente equipado
- VMotion para VMs vGPU DA GRADE do NVIDIA. Suporte para Intel FPGA
- VCenter Server Converge Tool para passar de PSC externo para PCS internos
- Aprimoramentos para VSAN (atualizações de HCI)
- Biblioteca de conteúdo aprimorada

Para obter detalhes sobre o vSphere 6,7 U1, "Novidades no vCenter Server 6,7 Update 1" consulte .

Requisitos de tecnologia

Um sistema FlexPod Express requer uma combinação de componentes de hardware e software. O FlexPod Express também descreve os componentes de hardware necessários para adicionar nós de hipervisor ao sistema em unidades de dois.

Requisitos de hardware

Independentemente do hypervisor escolhido, todas as configurações do FlexPod Express usam o mesmo hardware. Portanto, mesmo que os requisitos de negócios sejam alterados, qualquer hipervisor pode ser executado no mesmo hardware FlexPod Express.

A tabela a seguir lista os componentes de hardware necessários para todas as configurações do FlexPod Express.

Hardware	Quantidade
Par de HA do AFF A220	1
Servidor Cisco C220 M5	2
Switch Cisco Nexus 3172P	2
Placa de interface virtual Cisco UCS (VIC) 1387 para o servidor C220 M5	2
ADAPTADOR CVR-QSFP-SFP10G	4

A tabela a seguir lista o hardware necessário além da configuração base para a implementação do 10GbE.

Hardware	Quantidade
Servidor Cisco UCS C220 M5	2
Cisco VIC 1387	2
ADAPTADOR CVR-QSFP-SFP10G	4

Requisitos de software

A tabela a seguir lista os componentes de software necessários para implementar as arquiteturas das soluções FlexPod Express.

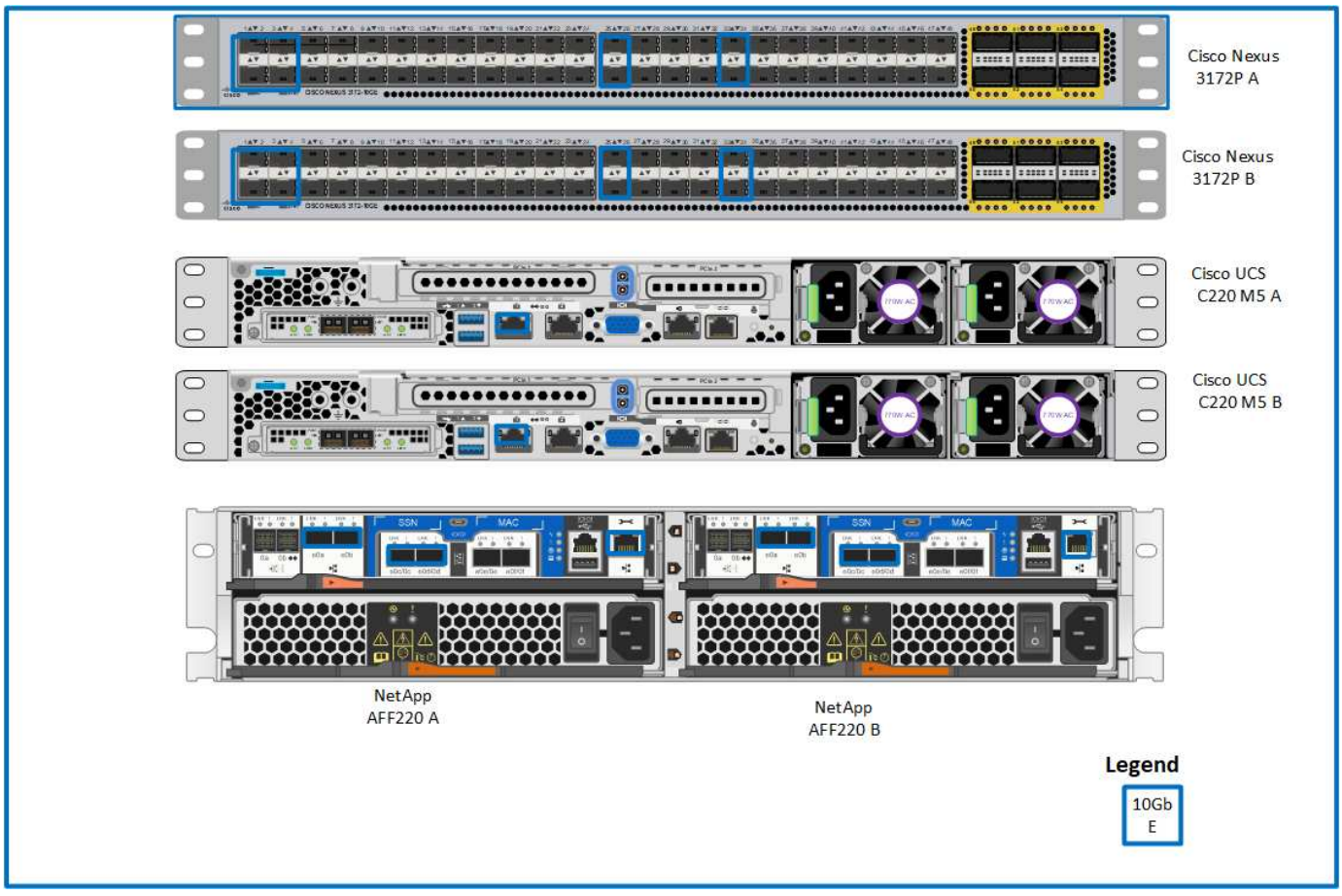
Software	Versão	Detalhes
Controlador de gerenciamento integrado Cisco (CIMC)	3,1 mm (3g mm)	Para servidores de rack Cisco UCS C220 M5
Cisco nenic driver	1.0.25.0	Para placas de interface VIC 1387
Cisco NX-os	nxos.7.0.3.I7.5.bin	Para switches Cisco Nexus 3172P
NetApp ONTAP	9,4	Para controladores AFF A220

A tabela a seguir lista o software necessário para todas as implementações do VMware vSphere no FlexPod Express.

Software	Versão
Dispositivo de servidor VMware vCenter	6,7
Hipervisor VMware vSphere ESXi	6,7
Plug-in NetApp VAAI para ESXi	1.1.2

Informações de cabeamento do FlexPod Express

A figura a seguir mostra o cabeamento de validação de referência.



A tabela a seguir mostra as informações de cabeamento do switch Cisco Nexus 3172P A.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Switch Cisco Nexus 3172P A	Eth1/1	Controlador de storage NetApp AFF A220 A	e0c
	Eth1/2	Controlador de storage NetApp AFF A220 B	e0c
	Eth1/3	Servidor independente A do Cisco UCS C220 C-Series	MLOM1 com adaptador CVR-QSFP-SFP10G
	Eth1/4	Servidor independente B do Cisco UCS C220 C-Series	MLOM1 com adaptador CVR-QSFP-SFP10G
	Eth1/25	Interrutor Cisco Nexus 3172P B	Eth1/25
	Eth1/26	Interrutor Cisco Nexus 3172P B	Eth1/26
	Eth1/33	Controlador de storage NetApp AFF A220 A	e0M
	Eth1/34	Servidor independente A do Cisco UCS C220 C-Series	CIMC

A tabela a seguir mostra as informações de cabeamento do switch Cisco Nexus 3172P B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Interrutor Cisco Nexus 3172P B	Eth1/1	Controlador de storage NetApp AFF A220 A	e0d
	Eth1/2	Controlador de storage NetApp AFF A220 B	e0d
	Eth1/3	Servidor independente A do Cisco UCS C220 C-Series	MLOM2 com adaptador CVR-QSFP-SFP10G
	Eth1/4	Servidor independente B do Cisco UCS C220 C-Series	MLOM2 com adaptador CVR-QSFP-SFP10G
	Eth1/25	Switch Cisco Nexus 3172P A	Eth1/25
	Eth1/26	Switch Cisco Nexus 3172P A	Eth1/26
	Eth1/33	Controlador de storage NetApp AFF A220 B	e0M
	Eth1/34	Servidor independente B do Cisco UCS C220 C-Series	CIMC

A tabela a seguir mostra as informações de cabeamento do controlador de armazenamento NetApp AFF A220 A.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Controlador de storage NetApp AFF A220 A	e0a	Controlador de storage NetApp AFF A220 B	e0a
	e0b	Controlador de storage NetApp AFF A220 B	e0b
	e0c	Switch Cisco Nexus 3172P A	Eth1/1
	e0d	Interrutor Cisco Nexus 3172P B	Eth1/1
	e0M	Switch Cisco Nexus 3172P A	Eth1/33

A tabela a seguir mostra informações de cabeamento para o controlador de armazenamento NetApp AFF A220 B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Controlador de storage NetApp AFF A220 B	e0a	Controlador de storage NetApp AFF A220 A	e0a
	e0b	Controlador de storage NetApp AFF A220 A	e0b
	e0c	Switch Cisco Nexus 3172P A	Eth1/2
	e0d	Interrutor Cisco Nexus 3172P B	Eth1/2
	e0M	Interrutor Cisco Nexus 3172P B	Eth1/33

Procedimentos de implantação

Este documento fornece detalhes para configurar um sistema FlexPod Express totalmente redundante e altamente disponível. Para refletir essa redundância, os componentes que estão sendo configurados em cada etapa são referidos como componente A ou componente B. por exemplo, controlador A e controlador B identificam os dois controladores de storage NetApp que são provisionados neste documento. O switch A e o switch B identificam um par de switches Cisco Nexus.

Além disso, este documento descreve etapas para provisionar vários hosts Cisco UCS, que são identificados sequencialmente como servidor A, servidor B e assim por diante.

Para indicar que você deve incluir informações pertinentes ao seu ambiente em uma etapa, `<<text>>` aparece como parte da estrutura de comando. Veja o exemplo a seguir para o `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Este documento permite configurar totalmente o ambiente do FlexPod Express. Nesse processo, várias etapas exigem que você insira convenções de nomenclatura específicas do cliente, endereços IP e esquemas de rede local virtual (VLAN). A tabela abaixo descreve as VLANs necessárias para implantação, conforme descrito neste guia. Esta tabela pode ser concluída com base nas variáveis específicas do site e usada para implementar as etapas de configuração do documento.

Se você usar VLANs separadas de gerenciamento dentro e fora da banda, será necessário criar uma rota de camada 3 entre elas. Para essa validação, uma VLAN de gerenciamento comum foi usada.

Nome AN	Finalidade da VLAN	ID utilizada na validação deste documento
VLAN de gerenciamento	VLAN para interfaces de gerenciamento	3437
VLAN nativo	VLAN à qual os quadros não marcados são atribuídos	2
VLAN NFS	VLAN para tráfego NFS	3438
VLAN do VMware vMotion	VLAN designada para o movimento de máquinas virtuais de um host físico para outro	3441
VLAN de tráfego de máquina virtual	VLAN para tráfego de aplicativos de máquina virtual	3442
ISCSI-A-VLAN	VLAN para tráfego iSCSI na malha A	3439
ISCSI-B-VLAN	VLAN para tráfego iSCSI na malha B	3440

Os números de VLAN são necessários durante toda a configuração do FlexPod Express. As VLANs são referidas como `<<var_xxxx_vlan>>`, onde `xxxx` é a finalidade da VLAN (como iSCSI-A).

A tabela abaixo lista as máquinas virtuais VMware criadas.

Descrição da máquina virtual	Nome do host
VMware vCenter Server	

Procedimento de implantação do Cisco Nexus 3172P

A seção a seguir detalha a configuração do switch Cisco Nexus 3172P usada em um ambiente FlexPod Express.

Configuração inicial do switch Cisco Nexus 3172P

Os procedimentos a seguir descrevem como configurar os switches Cisco Nexus para uso em um ambiente FlexPod Express básico.

Este procedimento pressupõe que você está usando um Cisco Nexus 3172P executando o software NX-os versão 7,0(3)i7(5).

1. Após a inicialização inicial e a conexão à porta do console do switch, a configuração do Cisco NX-os é iniciada automaticamente. Esta configuração inicial aborda as configurações básicas, como o nome do switch, a configuração da interface mgmt0 e a configuração do Secure Shell (SSH).
2. A rede de gerenciamento FlexPod Express pode ser configurada de várias maneiras. As interfaces mgmt0 nos switches 3172P podem ser conetadas a uma rede de gerenciamento existente, ou as interfaces mgmt0 dos switches 3172P podem ser conetadas em uma configuração back-to-back. No entanto, este link não pode ser usado para acesso de gerenciamento externo, como tráfego SSH.

   Neste guia de implantação, os switches FlexPod Express Cisco Nexus 3172P são conetados a uma rede de gerenciamento existente.
3. Para configurar os switches Cisco Nexus 3172P, ligue o switch e siga as instruções na tela, conforme ilustrado aqui para a configuração inicial de ambos os switches, substituindo os valores apropriados pelas informações específicas do switch.

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.
*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
  Create another login account (yes/no) [n]: n
  Configure read-only SNMP community string (yes/no) [n]: n
  Configure read-write SNMP community string (yes/no) [n]: n
  Enter the switch name : 3172P-B
  Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
    Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
    Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
  Configure the default gateway? (yes/no) [y]: y
    IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
  Configure advanced IP options? (yes/no) [n]: n
  Enable the telnet service? (yes/no) [n]: n
  Enable the ssh service? (yes/no) [y]: y
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
    Number of rsa key bits <1024-2048> [1024]:  <enter>
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_ntp_ip>>
  Configure default interface layer (L3/L2) [L2]: <enter>
  Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:  <enter>
```

4. Em seguida, você verá um resumo de sua configuração e será perguntado se deseja editá-la. Se a configuração estiver correta, introduza `n`.

```
Would you like to edit the configuration? (yes/no) [n]: n
```

5. Então, você será perguntado se deseja usar essa configuração e salvá-la. Em caso afirmativo, introduza `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita este procedimento para o interrutor B do Cisco Nexus

Ativar funcionalidades avançadas

Certos recursos avançados devem ser ativados no Cisco NX-os para fornecer opções de configuração adicionais.

> O `interface-vlan` recurso só é necessário se você usar a opção voltar para trás `mgmt0` descrita em todo este documento. Esse recurso permite que você atribua um endereço IP à interface VLAN (switch virtual interface), que permite a comunicação de gerenciamento na banda para o switch (como por meio de SSH).

1. Para habilitar os recursos apropriados no switch A e no switch B do Cisco Nexus, entre no modo de configuração usando o comando `(config t)` e execute os seguintes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

   O hash padrão de balanceamento de carga do canal de porta usa os endereços IP de origem e destino para determinar o algoritmo de balanceamento de carga entre as interfaces no canal de porta. Você pode obter uma melhor distribuição entre os membros do canal de porta fornecendo mais entradas para o algoritmo hash além dos endereços IP de origem e destino. Pela mesma razão, o NetApp recomenda fortemente adicionar as portas TCP de origem e destino ao algoritmo de hash.

2. No modo de configuração (`config t`), digite os seguintes comandos para definir a configuração de balanceamento de carga do canal de porta global no switch A e no switch B do Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Execute a configuração global de spanning-tree

A plataforma Cisco Nexus usa um novo recurso de proteção chamado bridge Assurance. O Bridge Assurance ajuda a proteger contra uma ligação unidirecional ou outra falha de software com um dispositivo que continua a encaminhar o tráfego de dados quando não está mais a executar o algoritmo spanning-tree. As portas podem ser colocadas em um dos vários estados, incluindo rede ou borda, dependendo da plataforma.

A NetApp recomenda a configuração da garantia de ponte para que todas as portas sejam consideradas como portas de rede por padrão. Essa configuração força o administrador de rede a revisar a configuração de cada porta. Ele também revela os erros de configuração mais comuns, como portas de borda não identificadas ou um vizinho que não tenha o recurso de garantia de ponte ativado. Além disso, é mais seguro ter o bloco de árvore de expansão muitas portas em vez de muito poucas, o que permite que o estado de porta padrão aumente a estabilidade geral da rede.

Preste muita atenção ao estado de spanning-tree ao adicionar servidores, armazenamento e switches uplink, especialmente se eles não suportarem a garantia de bridge. Nesses casos, talvez seja necessário alterar o tipo de porta para tornar as portas ativas.

A proteção da Unidade de dados do Protocolo de Ponte (BPDU) é ativada por padrão nas portas de borda como outra camada de proteção. Para evitar loops na rede, esse recurso desliga a porta se BPDUs de outro

switch forem vistos nessa interface.

No modo de configuração (`config t`), execute os seguintes comandos para configurar as opções de spanning-tree padrão, incluindo o tipo de porta padrão e a proteção BPDU, no switch A do Cisco Nexus e no switch B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Definir VLANs

Antes que portas individuais com VLANs diferentes sejam configuradas, as VLANs de camada 2 devem ser definidas no switch. Também é uma boa prática nomear as VLANs para facilitar a solução de problemas no futuro.

No modo de configuração (`config t`), execute os seguintes comandos para definir e descrever as VLANs de camada 2 no switch A e no switch B do Cisco Nexus:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurar descrições de portas de acesso e gerenciamento

Como acontece com a atribuição de nomes às VLANs de camada 2, as descrições de configuração para todas as interfaces podem ajudar no provisionamento e na solução de problemas.

A partir do modo de configuração (`config t`) em cada um dos switches, insira as seguintes descrições de porta para a configuração grande do FlexPod Express:

Switch Cisco Nexus A

```
int eth1/1
  description AFF A220-A e0c
int eth1/2
  description AFF A220-B e0c
int eth1/3
  description UCS-Server-A: MLOM port 0
int eth1/4
  description UCS-Server-B: MLOM port 0
int eth1/25
  description vPC peer-link 3172P-B 1/25
int eth1/26
  description vPC peer-link 3172P-B 1/26
int eth1/33
  description AFF A220-A e0M
int eth1/34
  description UCS Server A: CIMC
```

Switch Cisco Nexus B

```
int eth1/1
  description AFF A220-A e0d
int eth1/2
  description AFF A220-B e0d
int eth1/3
  description UCS-Server-A: MLOM port 1
int eth1/4
  description UCS-Server-B: MLOM port 1
int eth1/25
  description vPC peer-link 3172P-A 1/25
int eth1/26
  description vPC peer-link 3172P-A 1/26
int eth1/33
  description AFF A220-B e0M
int eth1/34
  description UCS Server B: CIMC
```

Configurar interfaces de gerenciamento de storage e servidor

As interfaces de gerenciamento para o servidor e o storage normalmente usam apenas uma única VLAN. Portanto, configure as portas da interface de gerenciamento como portas de acesso. Defina a VLAN de gerenciamento para cada switch e altere o tipo de porta spanning-tree para Edge.

No modo de configuração (`config t`), digite os seguintes comandos para configurar as configurações de porta para as interfaces de gerenciamento dos servidores e do armazenamento:

Switch Cisco Nexus A

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Switch Cisco Nexus B

```
int eth1/33-34
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Execute a configuração global do canal de porta virtual

Um canal de porta virtual (VPC) permite que os links fisicamente conetados a dois switches Cisco Nexus diferentes apareçam como um canal de porta única para um terceiro dispositivo. O terceiro dispositivo pode ser um switch, servidor ou qualquer outro dispositivo de rede. Uma VPC pode fornecer multipathing de camada 2, o que permite criar redundância aumentando a largura de banda, habilitando vários caminhos paralelos entre nós e o tráfego de balanceamento de carga onde existem caminhos alternativos.

Uma VPC oferece os seguintes benefícios:

- Ativar um único dispositivo para usar um canal de porta em dois dispositivos upstream
- Eliminação de portas bloqueadas de protocolo spanning-tree
- Fornecendo uma topologia sem loop
- Usando toda a largura de banda de uplink disponível
- Fornecendo convergência rápida se o link ou um dispositivo falhar
- Fornecer resiliência no nível de link
- Ajudando a fornecer alta disponibilidade

O recurso VPC requer alguma configuração inicial entre os dois switches Cisco Nexus para funcionar corretamente. Se você usar a configuração back-to-back mgmt0, use os endereços definidos nas interfaces e verifique se eles podem se comunicar usando o comando ping `[switch_A/B_mgmt0_ip_addr]vrf` Management.

No modo de configuração (`config t`), execute os seguintes comandos para configurar a configuração global da VPC para ambos os switches:

Switch Cisco Nexus A

```
vpc domain 1
 role priority 10
  peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25-26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
  no shut
exit
copy run start
```

Switch Cisco Nexus B

```
vpc domain 1
  peer-switch
  role priority 20
  peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
int eth1/25- 26
  channel-group 10 mode active
int Po10
  description vPC peer-link
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type network
  vpc peer-link
no shut
exit
copy run start
```

Configurar canais de porta de armazenamento

Os controladores de armazenamento NetApp permitem uma conexão ativo-ativo à rede usando o protocolo de controle de agregação de link (LACP). O uso do LACP é preferido porque adiciona negociação e Registro entre os switches. Como a rede está configurada para VPC, essa abordagem permite que você tenha conexões ativo-ativo do armazenamento para switches físicos separados. Cada controlador tem dois links para cada um dos switches. No entanto, todos os quatro links fazem parte do mesmo VPC e grupo de interfaces (IFGRP).

No modo de configuração (`config t`), execute os seguintes comandos em cada um dos switches para configurar as interfaces individuais e a configuração de canal de porta resultante para as portas conetadas ao controlador NetApp AFF.

1. Execute os seguintes comandos no interrutor A e no interrutor B para configurar os canais de porta para o controlador de armazenamento A:

```
int eth1/1
  channel-group 11 mode active
int Po11
  description vPC to Controller-A
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<nfs_vlan_id>>,<<mgmt_vlan_id>>,<<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11
  no shut
```

2. Execute os seguintes comandos no interrutor A e no interrutor B para configurar os canais de porta para o controlador de armazenamento B.

```
int eth1/2
  channel-group 12 mode active
int Po12
  description vPC to Controller-B
  switchport
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan <<nfs_vlan_id>>,<<mgmt_vlan_id>>,
<<iSCSI_A_vlan_id>>, <<iSCSI_B_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12
  no shut
exit
copy run start
```

Na validação desta solução, foi utilizada uma MTU de 9000. No entanto, com base nos requisitos do aplicativo, você pode configurar um valor apropriado de MTU. É importante definir o mesmo valor MTU na solução FlexPod. Configurações incorretas de MTU entre componentes resultarão em pacotes sendo descartados e esses pacotes.

Configure as conexões do servidor

Os servidores Cisco UCS têm uma placa de interface virtual de duas portas, VIC1387, que é usada para tráfego de dados e inicialização do sistema operacional ESXi usando iSCSI. Essas interfaces são configuradas para fazer failover entre si, proporcionando redundância adicional além de um único link. Espalhar esses links por vários switches permite que o servidor sobreviva até mesmo a uma falha completa

do switch.

No modo de configuração (`config t`), execute os seguintes comandos para configurar as configurações de porta para as interfaces conetadas a cada servidor.

Switch Cisco Nexus A: Configuração do servidor Cisco UCS-A e do servidor Cisco UCS-B.

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_A_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu9216
  no shut
exit
copy run start
```

Switch Cisco B: Configuração do Cisco UCS Server-A e do Cisco UCS Server-B.

```
int eth1/3-4
  switchport mode trunk
  switchport trunk native vlan <<native_vlan_id>>
  switchport trunk allowed vlan
<<iSCSI_B_vlan_id>>,<<nfs_vlan_id>>,<<vmotion_vlan_id>>,<<vmtraffic_vlan_i
d>>,<<mgmt_vlan_id>>
  spanning-tree port type edge trunk
  mtu 9216
  no shut
exit
copy run start
```

Na validação desta solução, foi utilizada uma MTU de 9000. No entanto, com base nos requisitos do aplicativo, você pode configurar um valor apropriado de MTU. É importante definir o mesmo valor MTU na solução FlexPod. Configurações incorretas de MTU entre componentes resultarão em pacotes sendo descartados e esses pacotes precisarão ser transmitidos novamente. Isso afetará o desempenho geral da solução.

Para escalar a solução adicionando servidores Cisco UCS adicionais, execute os comandos anteriores com as portas de switch às quais os servidores recém-adicionados foram conetados nos switches A e B.

Uplink em infra-estrutura de rede existente

Dependendo da infraestrutura de rede disponível, vários métodos e recursos podem ser usados para uplink o ambiente FlexPod. Se um ambiente Cisco Nexus existente estiver presente, a NetApp recomenda o uso de VPCs para uplink os switches Cisco Nexus 3172P incluídos no ambiente FlexPod na infraestrutura. Os uplinks

podem ser 10GbE uplinks para uma solução de infraestrutura 10GbE ou 1GbE para uma solução de infraestrutura 1GbE, se necessário. Os procedimentos descritos anteriormente podem ser usados para criar uma VPC uplink no ambiente existente. Certifique-se de executar o copy run start para salvar a configuração em cada switch depois que a configuração for concluída.

"Próximo: Procedimento de implantação de armazenamento NetApp (parte 1)"

Procedimento de implantação de storage do NetApp (parte 1)

Esta seção descreve o procedimento de implantação de storage do NetApp AFF.

Instalação do controlador de armazenamento NetApp série AFF2xx

NetApp Hardware Universe

O aplicativo NetApp Hardware Universe (HWU) fornece componentes de hardware e software suportados para qualquer versão específica do ONTAP. Ele fornece informações de configuração para todos os dispositivos de storage NetApp atualmente compatíveis com o software ONTAP. Ele também fornece uma tabela de compatibilidades de componentes.

Confirme se os componentes de hardware e software que você gostaria de usar são suportados com a versão do ONTAP que você pretende instalar:

1. Acesse o "HWU" aplicativo para exibir os guias de configuração do sistema. Clique na guia Controladores para exibir a compatibilidade entre diferentes versões do software ONTAP e os dispositivos de armazenamento NetApp com as especificações desejadas.
2. Como alternativa, para comparar componentes por dispositivo de armazenamento, clique em comparar sistemas de armazenamento.

Pré-requisitos da Série Controller AFF2XX
Para Planejar a localização física dos sistemas de storage, consulte o NetApp Hardware Universe. Consulte as seguintes seções: Requisitos elétricos, cabos de alimentação suportados e portas e cabos integrados.

Controladores de storage

Siga os procedimentos de instalação física dos controladores no "Documentação do AFF A220".

NetApp ONTAP 9,4

Folha de cálculo de configuração

Antes de executar o script de configuração, conclua a Planilha de configuração no manual do produto. A folha de cálculo de configuração está disponível no "Guia de configuração do software ONTAP 9.4".

Este sistema é configurado em uma configuração de cluster sem switch de dois nós.

A tabela a seguir mostra as informações de instalação e configuração do ONTAP 9.4.

Detalhe do cluster	Valor de detalhe do cluster
Nó de cluster Um endereço IP	"Cliente <var_nodeA_mgmt_ip>>
Cluster node Uma máscara de rede	"Cliente <var_nodeA_mgmt_mask>>

Detalhe do cluster	Valor de detalhe do cluster
Nó de cluster A gateway	"Cliente <var_nodeA_mgmt_gateway>>
Nome do nó do cluster	"Cliente <var_nodeA>>
Endereço IP do nó B do cluster	"Cliente <var_nodeB_mgmt_ip>>
Nó de cluster B netmask	"Cliente <var_nodeB_mgmt_mask>>
Gateway do nó B do cluster	"Cliente <var_nodeB_mgmt_gateway>>
Nome B do nó do cluster	"Cliente <var_nodeB>>
URL do ONTAP 9.4	"cliente <var_url_boot_software>>
Nome do cluster	"cliente <var_clustername>>
Endereço IP de gerenciamento de cluster	"cliente <var_clustermgmt_ip>>
Gateway do cluster B.	"cliente <var_clustermgmt_gateway>>
Cluster B netmask	"cliente <var_clustermgmt_mask>>
Nome de domínio	"cliente <var_domain_name>>
IP do servidor DNS (pode introduzir mais de um)	"cliente <var_dns_server_ip>>
IP do servidor NTP (pode introduzir mais de um)	"cliente <var_ntp_server_ip>>

Configure o nó A

Para configurar o nó A, execute as seguintes etapas:

1. Conete-se à porta do console do sistema de armazenamento. Você deve ver um prompt Loader-A. No entanto, se o sistema de armazenamento estiver em um loop de reinicialização, pressione Ctrl-C para sair do loop autoboot quando você vir esta mensagem:

   ```
   Starting AUTOBOOT press Ctrl-C to abort…
   ```

2. Permita que o sistema inicialize.

   ```
   autoboot
   ```

3. Pressione Ctrl-C para entrar no menu Boot (Inicialização).

   Se o ONTAP 9.4 não for a versão do software que está sendo inicializada, continue com as etapas a seguir para instalar o novo software. Se o ONTAP 9.4 for a versão que está sendo inicializada, selecione a opção 8 e y para reinicializar o nó. Em seguida, continue com o passo 14.

4. Para instalar um novo software, selecione a opção `7`.
5. Introduza `y` para efetuar uma atualização.
6. `e0M`Selecione para a porta de rede que pretende utilizar para a transferência.
7. Introduza `y` para reiniciar agora.

8. Introduza o endereço IP, a máscara de rede e o gateway predefinido para e0M nos respetivos locais.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Introduza a URL onde o software pode ser encontrado.

   Este servidor Web deve ser pingável.

```
<<var_url_boot_software>>
```

10. Pressione Enter para o nome de usuário, indicando nenhum nome de usuário.
11. Introduza `y` para definir o software recém-instalado como o padrão a ser usado para reinicializações subsequentes.
12. Digite `y` para reinicializar o nó.

    Ao instalar um novo software, o sistema pode executar atualizações de firmware para o BIOS e placas adaptadoras, causando reinicializações e possíveis paradas no prompt do Loader-A. Se estas acões ocorrerem, o sistema poderá desviar-se deste procedimento.

13. Pressione Ctrl-C para entrar no menu Boot (Inicialização).
14. Selecione a opção `4` para Configuração limpa e Inicializar todos os discos.
15. Digite `y` zero discos, redefina a configuração e instale um novo sistema de arquivos.
16. Introduza `y` para apagar todos os dados nos discos.

    A inicialização e a criação do agregado raiz podem levar 90 minutos ou mais para ser concluída, dependendo do número e do tipo de discos anexados. Quando a inicialização estiver concluída, o sistema de armazenamento reinicializa. Note que os SSDs demoram consideravelmente menos tempo para inicializar. Você pode continuar com a configuração do nó B enquanto os discos do nó A estão zerando.

17. Enquanto o nó A estiver inicializando, comece a configurar o nó B.

Configurar nó B

Para configurar o nó B, execute as seguintes etapas:

1. Conete-se à porta do console do sistema de armazenamento. Você deve ver um prompt Loader-A. No entanto, se o sistema de armazenamento estiver em um loop de reinicialização, pressione Ctrl-C para sair do loop autoboot quando você vir esta mensagem:

```
Starting AUTOBOOT press Ctrl-C to abort…
```

2. Pressione Ctrl-C para entrar no menu Boot (Inicialização).

```
autoboot
```

3. Pressione Ctrl-C quando solicitado.

   Se o ONTAP 9.4 não for a versão do software que está sendo inicializada, continue com as etapas a seguir para instalar o novo software. Se o ONTAP 9.4 for a versão que está sendo inicializada, selecione a opção 8 e y para reinicializar o nó. Em seguida, continue com o passo 14.

4. Para instalar um novo software, selecione a opção 7.
5. Introduza `y` para efetuar uma atualização.
6. `e0M`Selecione para a porta de rede que pretende utilizar para a transferência.
7. Introduza `y` para reiniciar agora.
8. Introduza o endereço IP, a máscara de rede e o gateway predefinido para e0M nos respetivos locais.

   ```
   <<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
   ```

9. Introduza a URL onde o software pode ser encontrado.

   Este servidor Web deve ser pingável.

   ```
   <<var_url_boot_software>>
   ```

10. Pressione Enter para o nome de usuário, indicando nenhum nome de usuário.
11. Introduza `y` para definir o software recém-instalado como o padrão a ser usado para reinicializações subsequentes.
12. Digite `y` para reinicializar o nó.

    Ao instalar um novo software, o sistema pode executar atualizações de firmware para o BIOS e placas adaptadoras, causando reinicializações e possíveis paradas no prompt do Loader-A. Se estas acões ocorrerem, o sistema poderá desviar-se deste procedimento.

13. Pressione Ctrl-C para entrar no menu Boot (Inicialização).
14. Selecione a opção 4 para Configuração limpa e Inicializar todos os discos.
15. Digite `y` zero discos, redefina a configuração e instale um novo sistema de arquivos.
16. Introduza `y` para apagar todos os dados nos discos.

    A inicialização e a criação do agregado raiz podem levar 90 minutos ou mais para ser concluída, dependendo do número e do tipo de discos anexados. Quando a inicialização estiver concluída, o sistema de armazenamento reinicializa. Note que os SSDs demoram consideravelmente menos tempo para inicializar.

Continuação da configuração do nó A e configuração do cluster

A partir de um programa de porta de console conetado à porta de console do controlador de storage A (nó A), execute o script de configuração do nó. Este script aparece quando o ONTAP 9.4 inicializa no nó pela primeira vez.

O procedimento de configuração do nó e do cluster mudou ligeiramente no ONTAP 9.4. O assistente de configuração do cluster agora é usado para configurar o primeiro nó em um cluster e o System Manager é usado para configurar o cluster.

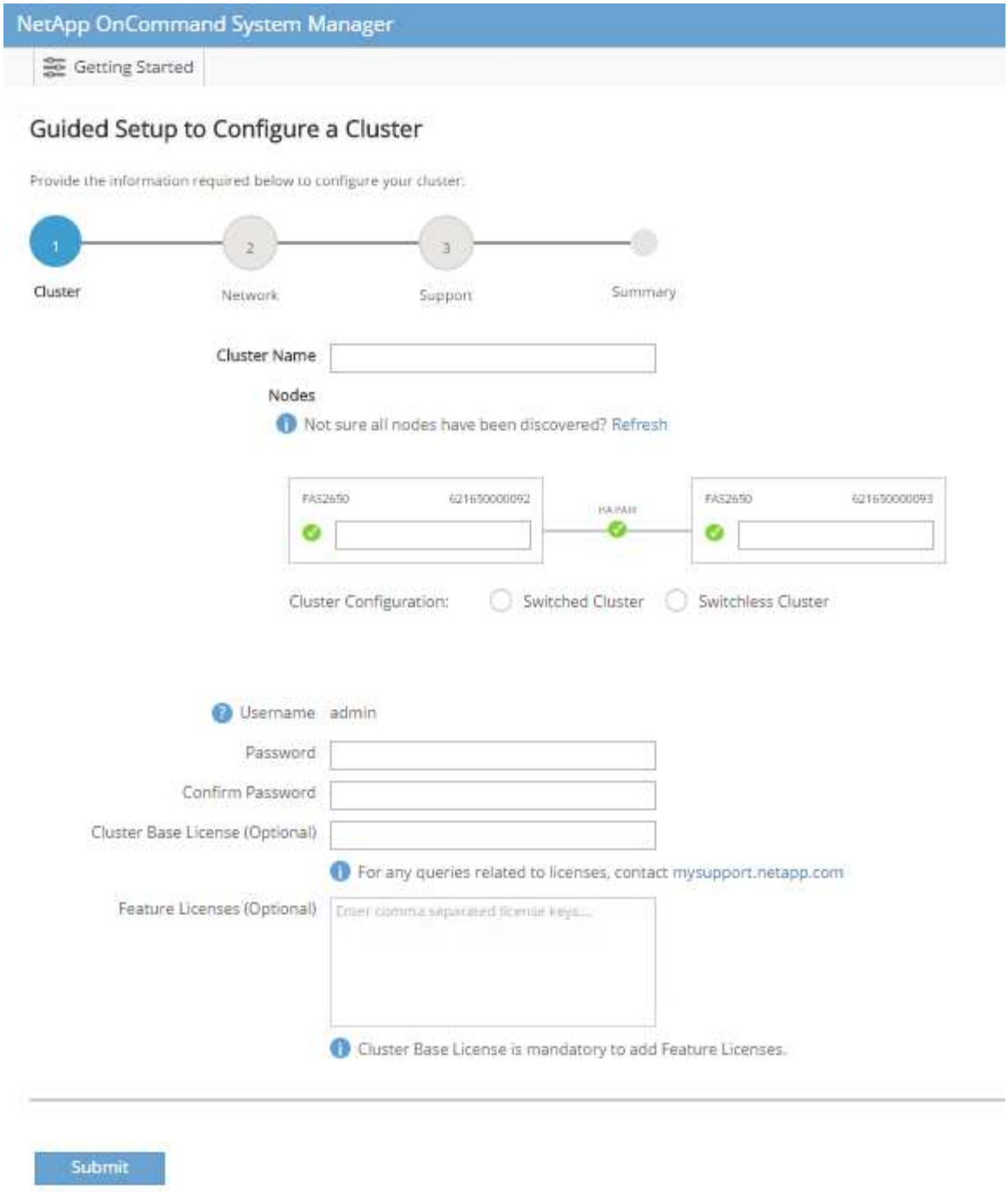
1. Siga as instruções para configurar o nó A..

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical
Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Navegue até o endereço IP da interface de gerenciamento do nó.

   A configuração do cluster também pode ser realizada usando a CLI. Este documento descreve a configuração do cluster usando a configuração guiada pelo Gerenciador de sistema do NetApp.

3. Clique em Configuração Guiada para configurar o cluster.
4. Introduza `<<var_clustername>>` o nome do cluster e `<<var_nodeA>>` e `<<var_nodeB>>` para cada um dos nós que está a configurar. Introduza a palavra-passe que pretende utilizar para o sistema de armazenamento. Selecione cluster sem switch para o tipo de cluster. Introduza a licença base do cluster.



5. Você também pode inserir licenças de recursos para Cluster, NFS e iSCSI.
6. Você verá uma mensagem de status informando que o cluster está sendo criado. Esta mensagem de estado passa por vários Estados. Este processo demora vários minutos.
7. Configure a rede.
   a. Desmarque a opção IP Address Range (intervalo de endereços IP).
   b. Introduza `<<var_clustermgmt_ip>>` no campo Endereço IP de gestão de clusters, `<<var_clustermgmt_mask>>` no campo Máscara de rede e `<<var_clustermgmt_gateway>>` no campo Gateway. Use o seletor… no campo porta para selecionar e0M do nó A.
   c. O IP de gerenciamento do Nó para o nó A já está preenchido. Introduza `<<var_nodeA_mgmt_ip>>` para o nó B.

d. Introduza `<<var_domain_name>>` no campo DNS Domain Name (Nome de domínio DNS). Introduza `<<var_dns_server_ip>>` no campo Endereço IP do servidor DNS.

   Você pode inserir vários endereços IP do servidor DNS.

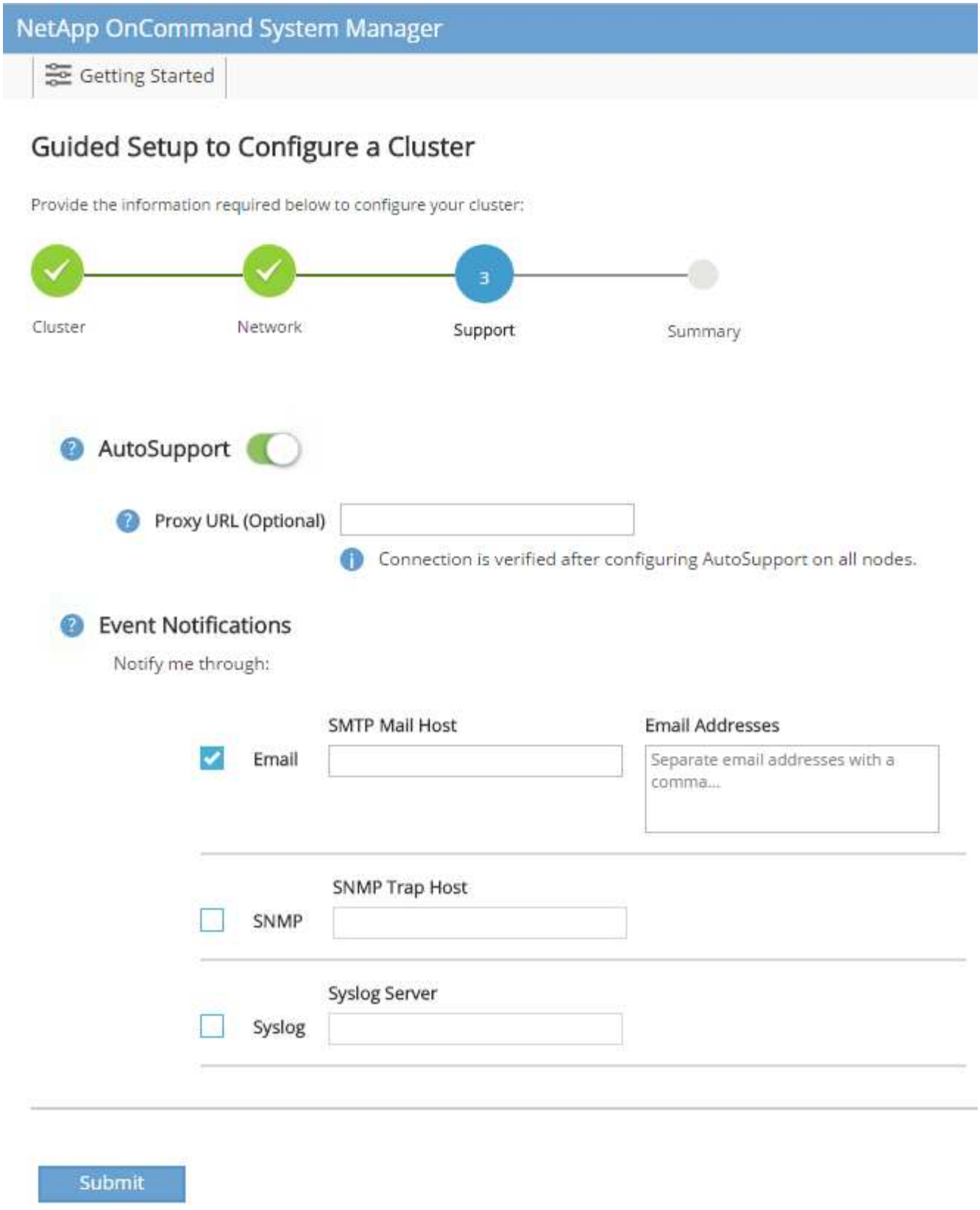
e. Introduza `<<var_ntp_server_ip>>` no campo servidor NTP principal.

   Você também pode inserir um servidor NTP alternativo.

8. Configure as informações de suporte.

   a. Se o seu ambiente exigir um proxy para acessar o AutoSupport, insira o URL no URL do proxy.
   b. Insira o host de e-mail SMTP e o endereço de e-mail para notificações de eventos.

      Você deve, no mínimo, configurar o método de notificação de evento antes de prosseguir. Você pode selecionar qualquer um dos métodos.



9. Quando for indicado que a configuração do cluster foi concluída, clique em Gerenciar seu cluster para configurar o armazenamento.

Continuação da configuração do cluster de armazenamento

Após a configuração dos nós de storage e do cluster base, você pode continuar com a configuração do cluster de storage.

Zero todos os discos sobressalentes

Para zerar todos os discos sobressalentes no cluster, execute o seguinte comando:

```
disk zerospares
```

Defina a personalidade de UTA2 portas a bordo

1. Verifique o modo atual e o tipo atual das portas executando o `ucadmin show` comando.

```
AFF A220::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFF A220_A     0c       fc       target     -        -          online
AFF A220_A     0d       fc       target     -        -          online
AFF A220_A     0e       fc       target     -        -          online
AFF A220_A     0f       fc       target     -        -          online
AFF A220_B     0c       fc       target     -        -          online
AFF A220_B     0d       fc       target     -        -          online
AFF A220_B     0e       fc       target     -        -          online
AFF A220_B     0f       fc       target     -        -          online
8 entries were displayed.
```

2. Verifique se o modo atual das portas que estão em uso é `cna` e se o tipo atual está definido como `target`. Caso contrário, altere a personalidade da porta usando o seguinte comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

As portas devem estar offline para executar o comando anterior. Para colocar uma porta off-line, execute o seguinte comando:

```
`network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down`
```

Se você alterou a personalidade da porta, será necessário reinicializar cada nó para que a alteração tenha efeito.

Renomear interfaces lógicas de gerenciamento (LIFs)

Para renomear os LIFs de gerenciamento, execute as seguintes etapas:

1. Mostrar os nomes de LIF de gerenciamento atuais.

```
network interface show –vserver <<clustername>>
```

2. Renomeie o LIF de gerenciamento de cluster.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Renomeie o nó B Management LIF.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_B_1 -newname AFF A220-02_mgmt1
```

Defina a reversão automática no gerenciamento de cluster

Defina `auto-revert` o parâmetro na interface de gerenciamento de cluster.

```
network interface modify –vserver <<clustername>> -lif cluster_mgmt –auto-
revert true
```

Configure a interface de rede do processador de serviço

Para atribuir um endereço IPv4 estático ao processador de serviço em cada nó, execute os seguintes comandos:

```
system service-processor network modify –node <<var_nodeA>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify –node <<var_nodeB>> -address
-family IPv4 –enable true –dhcp none –ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Os endereços IP do processador de serviço devem estar na mesma sub-rede que os endereços IP de gerenciamento de nós.

Ativar failover de storage no ONTAP

Para confirmar se o failover de armazenamento está ativado, execute os seguintes comandos em um par de

failover:

1. Verifique o status do failover de storage.

   ```
   storage failover show
   ```

   Ambos <<var_nodeA>> e <<var_nodeB>> devem ser capazes de realizar uma aquisição. Vá para a etapa 3 se os nós puderem executar um takeover.

2. Habilite o failover em um dos dois nós.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

   A ativação do failover em um nó permite a TI para ambos os nós.

3. Verifique o status de HA do cluster de dois nós.

   Esta etapa não se aplica a clusters com mais de dois nós.

   ```
   cluster ha show
   ```

4. Vá para a etapa 6 se a alta disponibilidade estiver configurada. Se a alta disponibilidade estiver configurada, você verá a seguinte mensagem ao emitir o comando:

   ```
   High Availability Configured: true
   ```

5. Ative o modo HA apenas para o cluster de dois nós.

   > Não execute este comando para clusters com mais de dois nós porque causa problemas com failover.

   ```
   cluster ha modify -configured true
   Do you want to continue? {y|n}: y
   ```

6. Verifique se a assistência ao hardware está corretamente configurada e, se necessário, modifique o endereço IP do parceiro.

   ```
   storage failover hwassist show
   ```

   A mensagem `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica que a assistência ao hardware não está configurada. Execute os seguintes comandos para configurar a assistência de hardware.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Crie um domínio de transmissão MTU de quadro jumbo no ONTAP

Para criar um domínio de transmissão de dados com uma MTU de 9000, execute os seguintes comandos:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Remover portas de dados do domínio de broadcast padrão

As portas de dados 10GbE são usadas para tráfego iSCSI/NFS e essas portas devem ser removidas do domínio padrão. As portas e0e e e0f não são usadas e também devem ser removidas do domínio padrão.

Para remover as portas do domínio de broadcast, execute o seguinte comando:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Desative o controle de fluxo nas portas UTA2

É uma prática recomendada do NetApp desativar o controle de fluxo em todas as UTA2 portas conetadas a dispositivos externos. Para desativar o controle de fluxo, execute o seguinte comando:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier.
Do you want to continue? {y|n}: y
```

Configure o LACP IFGRP no ONTAP

Esse tipo de grupo de interfaces requer duas ou mais interfaces Ethernet e um switch que suporte LACP. Certifique-se de que o interrutor está configurado corretamente.

No prompt do cluster, execute as etapas a seguir.

```
ifgrp create -node <<var_nodeA>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeA>> -ifgrp a0a -port e0d
ifgrp create -node << var_nodeB>> -ifgrp a0a -distr-func port -mode
multimode_lacp
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0c
network port ifgrp add-port -node <<var_nodeB>> -ifgrp a0a -port e0d
```

Configurar quadros jumbo no NetApp ONTAP

Para configurar uma porta de rede ONTAP para usar quadros jumbo (que geralmente têm uma MTU de 9.000 bytes), execute os seguintes comandos a partir do shell do cluster:

```
AFF A220::> network port modify -node node_A -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port a0a -mtu 9000
Warning: This command will cause a several second interruption of service
on
         this network port.
Do you want to continue? {y|n}: y
```

Crie VLANs no ONTAP

Para criar VLANs no ONTAP, execute as seguintes etapas:

1. Crie portas VLAN NFS e adicione-as ao domínio de transmissão de dados.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>:a0a-<<var_nfs_vlan_id>>, <<var_nodeB>>:a0a-
<<var_nfs_vlan_id>>
```

2. Crie portas iSCSI VLAN e adicione-as ao domínio de transmissão de dados.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_A_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>:a0a-<<var_iscsi_vlan_B_id>>, <<var_nodeB>>:a0a-
<<var_iscsi_vlan_B_id>>
```

3. Crie portas MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name a0a-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name a0a-
<<mgmt_vlan_id>>
```

Criar agregados no ONTAP

Um agregado contendo o volume raiz é criado durante o processo de configuração do ONTAP. Para criar agregados adicionais, determine o nome do agregado, o nó no qual criá-lo e o número de discos que ele contém.

Para criar agregados, execute os seguintes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Guarde pelo menos um disco (selecione o disco maior) na configuração como um sobressalente. Uma prática recomendada é ter pelo menos um sobressalente para cada tipo e tamanho de disco.

Comece com cinco discos; você pode adicionar discos a um agregado quando for necessário armazenamento adicional.

O agregado não pode ser criado até que a restauração do disco seja concluída. Execute o `aggr show` comando para exibir o status de criação agregada. Não prossiga até `aggr1`_`nodeA` que esteja online.

Configure o fuso horário no ONTAP

Para configurar a sincronização de hora e definir o fuso horário no cluster, execute o seguinte comando:

```
timezone <<var_timezone>>
```

Por exemplo, no leste dos Estados Unidos, o fuso horário é `America/New York`. Depois de começar a digitar o nome do fuso horário, pressione a tecla Tab para ver as opções disponíveis.

Configurar SNMP no ONTAP

Para configurar o SNMP, execute as seguintes etapas:

1. Configurar informações básicas do SNMP, como a localização e o contacto. Quando polled, esta informação é visível como `sysLocation` as variáveis e `sysContact` no SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Configurar traps SNMP para enviar para hosts remotos.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Configure o SNMPv1 no ONTAP

Para configurar o SNMPv1, defina a senha secreta compartilhada de texto simples chamada comunidade.

```
snmp community add ro <<var_snmp_community>>
```

Use o `snmp community delete all` comando com cuidado. Se strings de comunidade forem usadas para outros produtos de monitoramento, esse comando as removerá.

Configure o SNMPv3 no ONTAP

SNMPv3 requer que você defina e configure um usuário para autenticação. Para configurar o SNMPv3, execute as seguintes etapas:

1. Execute o `security snmpusers` comando para visualizar a ID do motor.
2. Crie um usuário `snmpv3user` chamado .

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduza a ID do motor da entidade autorizada e `md5` selecione como o protocolo de autenticação.
4. Insira uma senha de comprimento mínimo de oito carateres para o protocolo de autenticação quando solicitado.
5. `des`Selecione como o protocolo de privacidade.
6. Insira uma senha de comprimento mínimo de oito carateres para o protocolo de privacidade quando solicitado.

Configure o HTTPS do AutoSupport no ONTAP

A ferramenta NetApp AutoSupport envia informações resumidas de suporte para o NetApp por meio de HTTPS. Para configurar o AutoSupport, execute o seguinte comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Crie uma máquina virtual de armazenamento

Para criar uma máquina virtual de storage de infraestrutura (SVM), siga estas etapas:

1. Executar o `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume-security-style unix
```

2. Adicione o agregado de dados à lista de agregados de infraestrutura SVM para o VSC do NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Remova os protocolos de storage não utilizados da SVM, deixando NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite e execute o protocolo NFS no SVM de infraestrutura.

```
`nfs create -vserver Infra-SVM -udp disabled`
```

5. Ative o `SVM vstorage` parâmetro para o plug-in NetApp NFS VAAI. Em seguida, verifique se o NFS foi

configurado.

```
`vserver nfs modify –vserver Infra-SVM –vstorage enabled`
`vserver nfs show `
```

Os comandos são prefaciados `vserver` na linha de comando porque as máquinas virtuais de armazenamento eram anteriormente chamadas de servidores.

Configure o NFSv3 no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
ESXi Hospeda Um endereço IP NFS	"Cliente <var_esxi_hostA_nfs_ip>>
Endereço IP NFS do host ESXi B.	"Cliente <var_esxi_hostB_nfs_ip>>

Para configurar o NFS na SVM, execute os seguintes comandos:

1. Crie uma regra para cada host ESXi na política de exportação padrão.
2. Para cada host ESXi sendo criado, atribua uma regra. Cada host tem seu próprio índice de regras. Seu primeiro host ESXi tem o índice de regra 1, seu segundo host ESXi tem o índice de regra 2, e assim por diante.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 2 –protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Atribua a política de exportação ao volume raiz da infraestrutura SVM.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

O VSC do NetApp manipula automaticamente as políticas de exportação se você optar por instalá-las após a configuração do vSphere. Se você não instalá-lo, você deve criar regras de política de exportação quando servidores adicionais da série C do Cisco UCS forem adicionados.

Criar serviço iSCSI no ONTAP

Para criar o serviço iSCSI, execute o seguinte passo:

1. Crie o serviço iSCSI no SVM. Esse comando também inicia o serviço iSCSI e define o IQN iSCSI para o SVM. Verifique se o iSCSI foi configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Criar espelho de compartilhamento de carga do volume raiz da SVM no ONTAP

1. Crie um volume para ser o espelho de compartilhamento de carga do volume raiz da infraestrutura SVM em cada nó.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DP
volume create –vserver Infra_Vserver –volume rootvol_m02 –aggregate
aggr1_nodeB –size 1GB –type DP
```

2. Crie uma agenda de trabalhos para atualizar as relações de espelho de volume raiz a cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Crie as relações de espelhamento.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Inicialize a relação de espelhamento e verifique se ela foi criada.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol
snapmirror show
```

Configurar o acesso HTTPS no ONTAP

Para configurar o acesso seguro ao controlador de armazenamento, execute as seguintes etapas:

1. Aumente o nível de privilégio para acessar os comandos do certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. Geralmente, um certificado auto-assinado já está em vigor. Verifique o certificado executando o seguinte comando:

```
security certificate show
```

3. Para cada SVM mostrado, o nome comum do certificado deve corresponder ao FQDN DNS do SVM. Os quatro certificados predefinidos devem ser suprimidos e substituídos por certificados auto-assinados ou certificados de uma autoridade de certificação.

   Excluir certificados expirados antes de criar certificados é uma prática recomendada. Execute o `security certificate delete` comando para excluir certificados expirados. No comando a seguir, use conclusão de TABULAÇÃO para selecionar e excluir cada certificado padrão.

```
security certificate delete [TAB] …
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM -type server -serial 552429A6
```

4. Para gerar e instalar certificados autoassinados, execute os seguintes comandos como comandos únicos. Gerar um certificado de servidor para a infraestrutura SVM e o cluster SVM. Novamente, use TAB Completion para ajudar a completar esses comandos.

```
security certificate create [TAB] …
Example: security certificate create -common-name infra-svm. netapp.com
-type  server -size 2048 -country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email-addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obter os valores para os parâmetros necessários na etapa seguinte, execute o `security certificate show` comando.
6. Ative cada certificado que acabou de ser criado usando os `-server-enabled true` parâmetros e. `-client-enabled false` Novamente, use A conclusão DA GUIA.

```
security ssl modify [TAB] …
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configure e ative o acesso SSL e HTTPS e desative o acesso HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be
         interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
system services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

É normal que alguns desses comandos retornem uma mensagem de erro informando que a entrada não existe.

8. Reverta para o nível de privilégios de administrador e crie a configuração para permitir que o SVM esteja disponível na Web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Crie um NetApp FlexVol volume no ONTAP

Para criar um NetApp FlexVol volume, insira o nome do volume, o tamanho e o agregado no qual ele existe. Crie dois volumes do VMware datastore e um volume de inicialização do servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB -state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -junction-path /infra_swap
-space-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Ativar a deduplicação no ONTAP

Para habilitar a deduplicação em volumes apropriados, execute os seguintes comandos:

```
volume efficiency on –vserver Infra-SVM -volume infra_datastore_1
volume efficiency on –vserver Infra-SVM -volume esxi_boot
```

Criar LUNs no ONTAP

Para criar dois LUNs de inicialização, execute os seguintes comandos:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware -space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware -space-reserve disabled
```

Ao adicionar um servidor Cisco UCS C-Series extra, um LUN de inicialização extra deve ser criado.

Criar iSCSI LIFs no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
Nó de storage A iSCSI LIF01A	"Cliente <var_nodeA_iscsi_lif01a_ip>>
Nó de armazenamento Uma máscara de rede iSCSI LIF01A	"Cliente <var_nodeA_iscsi_lif01a_mask>>
Nó de storage A iSCSI LIF01B	"Cliente <var_nodeA_iscsi_lif01b_ip>>
Nó de armazenamento Uma máscara de rede iSCSI LIF01B	"Cliente <var_nodeA_iscsi_lif01b_mask>>
Nó de storage B iSCSI LIF01A	"Cliente <var_nodeB_iscsi_lif01a_ip>>
Máscara de rede do nó de armazenamento B iSCSI LIF01A	"Cliente <var_nodeB_iscsi_lif01a_mask>>
Nó de storage B iSCSI LIF01B	"Cliente <var_nodeB_iscsi_lif01b_ip>>
Máscara de rede do nó de armazenamento B iSCSI LIF01B	"Cliente <var_nodeB_iscsi_lif01b_mask>>

1. Crie quatro LIFs iSCSI, dois em cada nó.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi -home-node <<var_nodeA>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi -home-node <<var_nodeB>> -home-port a0a-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up –failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Criar LIFs NFS no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
Nó de storage A NFS LIF 01 IP	"Cliente <var_nodeA_nfs_lif_01_ip>>
Nó de storage Uma máscara de rede NFS LIF 01	"Cliente <var_nodeA_nfs_lif_01_mask>>
Nó de storage B NFS LIF 02 IP	"Cliente <var_nodeB_nfs_lif_02_ip>>
Máscara de rede do nó de storage B NFS LIF 02	"Cliente <var_nodeB_nfs_lif_02_mask>>

1. Criar um NFS LIF.

```
network interface create -vserver Infra-SVM -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_ip>> -netmask <<
var_nodeA_nfs_lif_01_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02 -role data
-data-protocol nfs -home-node <<var_nodeA>> -home-port a0a-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_ip>> -netmask <<
var_nodeB_nfs_lif_02_mask>> -status-admin up –failover-policy broadcast-
domain-wide –firewall-policy data –auto-revert true
network interface show
```

Adicionar administrador de infraestrutura SVM

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
IP Vsmgmt	"cliente <var_svm_mgmt_ip>>
Máscara de rede Vsmgmt	"cliente <var_svm_mgmt_mask>>
Gateway padrão Vsmgmt	"cliente <var_svm_mgmt_gateway>>

Para adicionar a interface lógica de administração do SVM e administrador de infraestrutura à rede de gerenciamento, siga estas etapas:

1. Execute o seguinte comando:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port  e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> -status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

> O IP de gerenciamento do SVM deve estar na mesma sub-rede que o IP de gerenciamento do cluster de storage.

2. Crie uma rota padrão para permitir que a interface de gerenciamento SVM alcance o mundo externo.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>>
network route show
```

3. Defina uma senha para o usuário SVM vsadmin e desbloqueie o usuário.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver Infra-SVM
```

"Próximo: Procedimento de implantação do servidor de rack Cisco UCS C-Series"

Procedimento de implantação do servidor em rack Cisco UCS C-Series

A seção a seguir fornece um procedimento detalhado para a configuração de um servidor de rack autônomo do Cisco UCS C-Series para uso na configuração do FlexPod Express.

Execute a configuração inicial do servidor autônomo do Cisco UCS C-Series para o servidor de gerenciamento integrado do Cisco

Conclua estas etapas para a configuração inicial da interface CIMC para servidores autônomos do Cisco UCS C-Series.

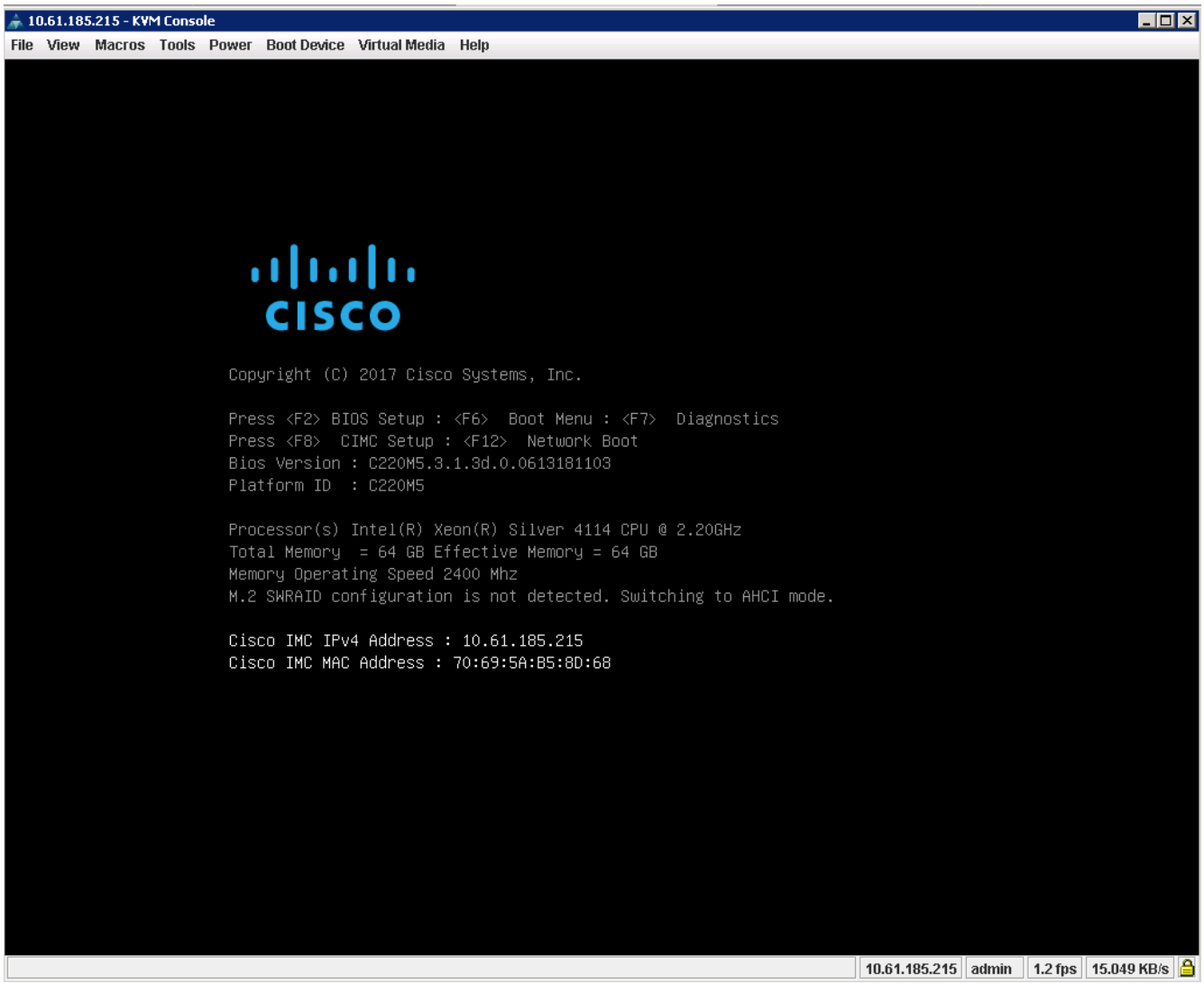
A tabela a seguir lista as informações necessárias para configurar o CIMC para cada servidor autônomo do Cisco UCS C-Series.

Detalhe	Valor do detalhe
Endereço IP CIMC	"cliente <cimc_ip>>
Máscara de sub-rede CIMC	"cliente <cimc_netmask>>
Gateway padrão CIMC	"cliente <cimc_gateway>>

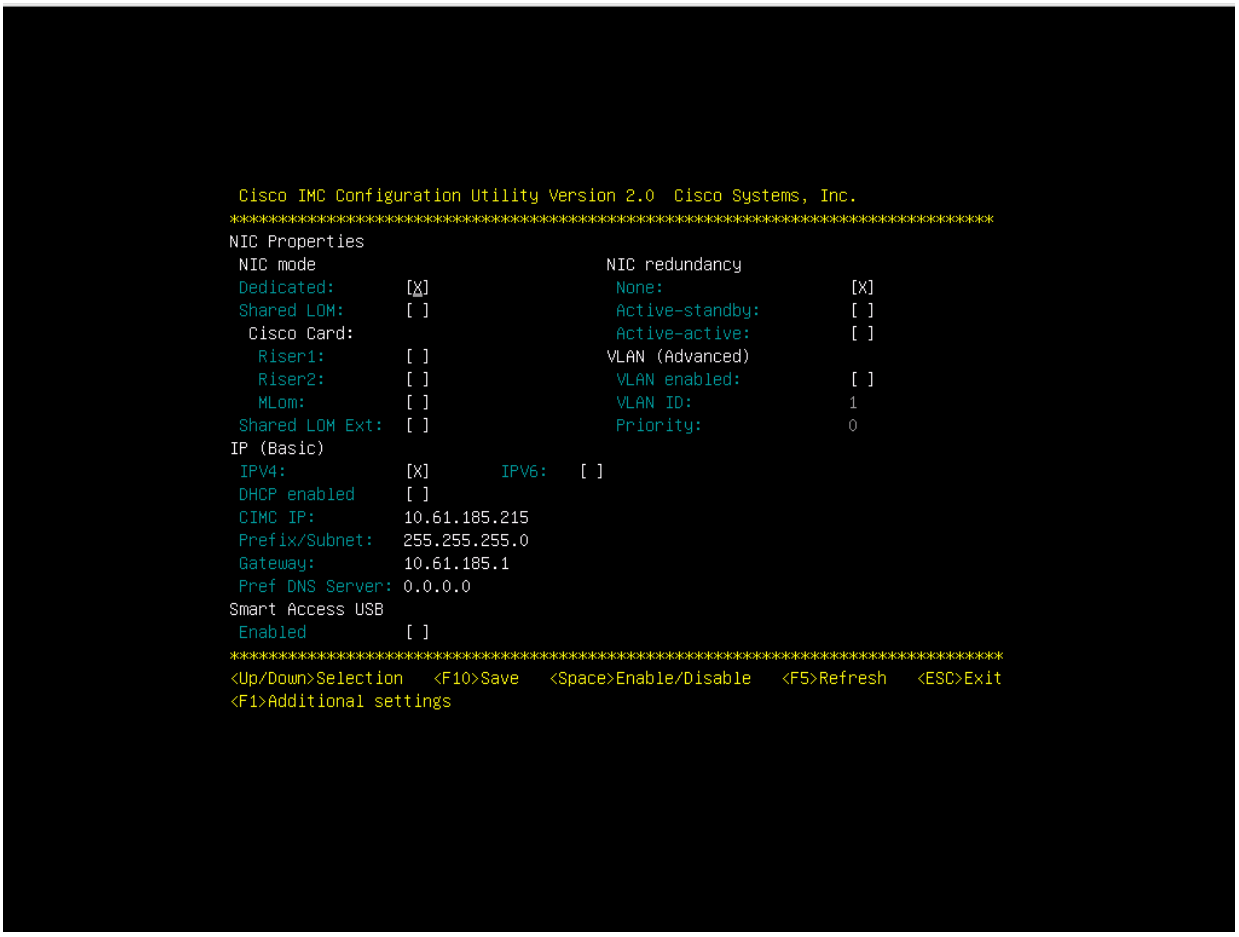
A versão CIMC utilizada nesta validação é CIMC 3,1.3(g).

Todos os servidores

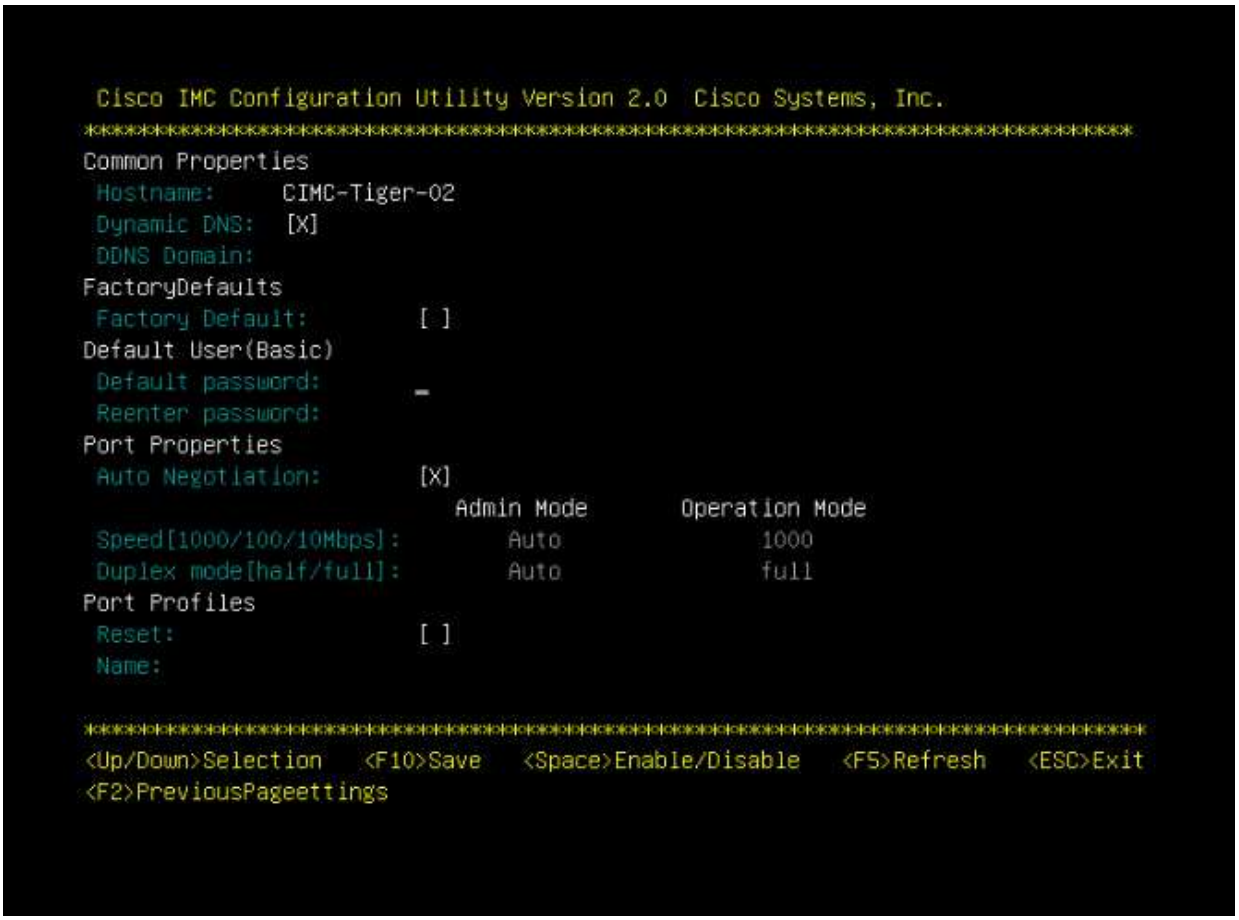
1. Conete o teclado Cisco, vídeo e dongle do Mouse (KVM) (fornecido com o servidor) à porta KVM na parte frontal do servidor. Ligue um monitor VGA e um teclado USB às portas de dongle KVM apropriadas.
2. Ligue o servidor e pressione F8 quando solicitado a inserir a configuração do CIMC.



3. No utilitário de configuração CIMC, defina as seguintes opções:
   - Modo de placa de interface de rede (NIC):
     - Dedicado [X]
   - IP (básico):
     - IPV4: [X]
     - DHCP ativado: [ ]
     - IP CIMC: 'Cliente <cimc_ip>>
     - Prefixo/sub-rede: /<cimc_netmask>>
     - Gateway: "Cliente <cimc_gateway>>"
   - VLAN (Avançado): Deixe limpo para desativar a marcação de VLAN.
     - Redundância de NIC
     - Nenhum: [X]



4. Prima F1 para ver definições adicionais.
   - Propriedades comuns:
     - Nome do host: "Cliente <esxi_host_name>>"
     - DNS dinâmico: [ ]
     - Predefinições de fábrica: Deixe limpo.
   - Utilizador predefinido (básico):
     - Palavra-passe predefinida: "Cliente <admin_password>>"
     - Digite novamente a senha: "Cliente <admin_password>>"
     - Propriedades da porta: Use valores padrão.
     - Perfis de porta: Deixe limpo.



5. Pressione F10 para salvar a configuração da interface CIMC.
6. Depois de guardar a configuração, prima ESC para sair.

Configurar a inicialização iSCSI dos servidores Cisco UCS C-Series

Nesta configuração do FlexPod Express, o VIC1387 é usado para inicialização iSCSI.

A tabela a seguir lista as informações necessárias para configurar a inicialização iSCSI.

Fonte itálico indica variáveis que são exclusivas para cada host ESXi.

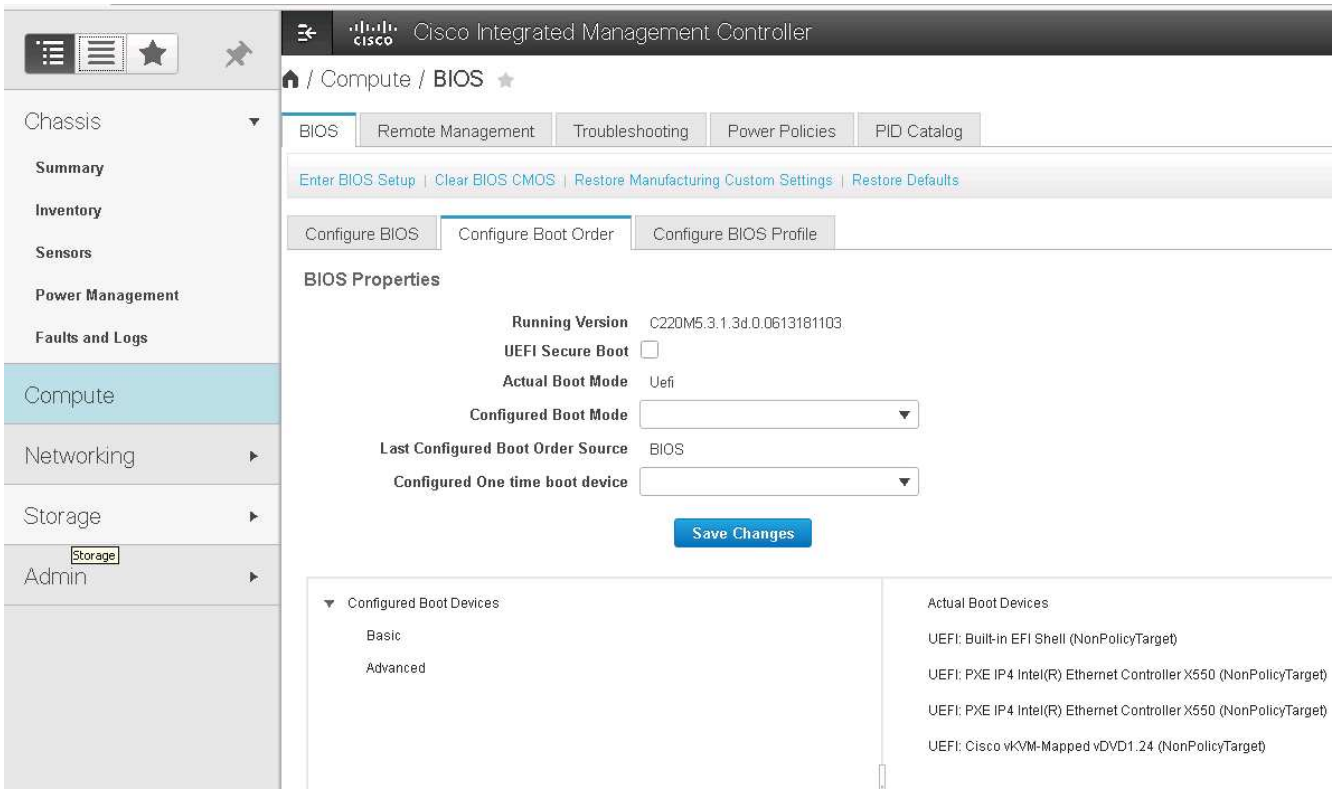
Detalhe	Valor do detalhe
Nome do iniciador do host ESXi	"Cliente <var_ucs_initiator_name_A>>
IP iSCSI-A do host ESXi	"Cliente <var_esxi_host_iscsiA_ip>>
Máscara de rede iSCSI-A. do host ESXi	"Cliente <var_esxi_host_iscsiA_mask>>
ESXi host Iscsi Um gateway padrão	"Cliente <var_esxi_host_iscsiA_gateway>>
Nome B do iniciador do host ESXi	"Cliente <var_ucs_initiator_name_B>>
IP iSCSI-B do host ESXi	"Cliente <var_esxi_host_iscsiB_ip>>
Máscara de rede iSCSI-B. do host ESXi	"Cliente <var_esxi_host_iscsiB_mask>>
Gateway iSCSI-B. do host ESXi	"Cliente <var_esxi_host_iscsiB_gateway>>

Detalhe	Valor do detalhe
Endereço ip iSCSI_lif01a	
Endereço ip iSCSI_lif02a	
Endereço ip iSCSI_lif01b	
Endereço ip iSCSI_lif02b	
Infraestrutura_SVM IQN	

Configuração da ordem de inicialização

Para definir a configuração da ordem de inicialização, execute as seguintes etapas:

1. Na janela do navegador da interface CIMC, clique na guia servidor e selecione BIOS.
2. Clique em Configurar ordem de inicialização e, em seguida, clique em OK.



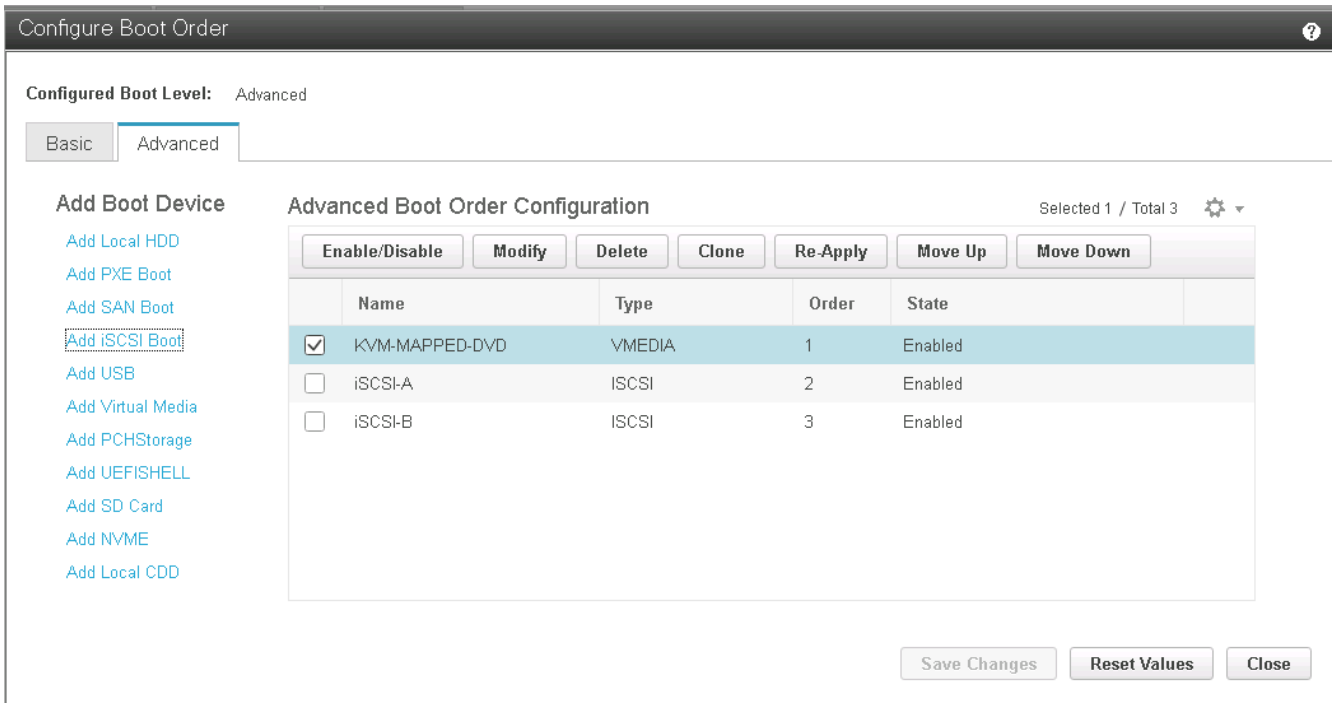
3. Configure os seguintes dispositivos clicando no dispositivo em Adicionar dispositivo de inicialização e indo para a guia Avançado.
   - Adicionar Mídia virtual
     - NOME: KVM-CD-DVD
     - SUBTIPO: KVM MAPEADO DVD
     - Estado: Ativado
     - Pedido mínimo: 1
   - Adicionar iSCSI Boot.
     - Nome: ISCSI-A.

- Estado: Ativado
- Pedido mínimo: 2
- Slot: MLOM
- Porta: 0

◦ Clique em Adicionar iSCSI Boot.

- Nome: ISCSI-B
- Estado: Ativado
- Pedido mínimo: 3
- Slot: MLOM
- Porta: 1

4. Clique em Adicionar dispositivo.
5. Clique em Salvar alterações e, em seguida, clique em Fechar.

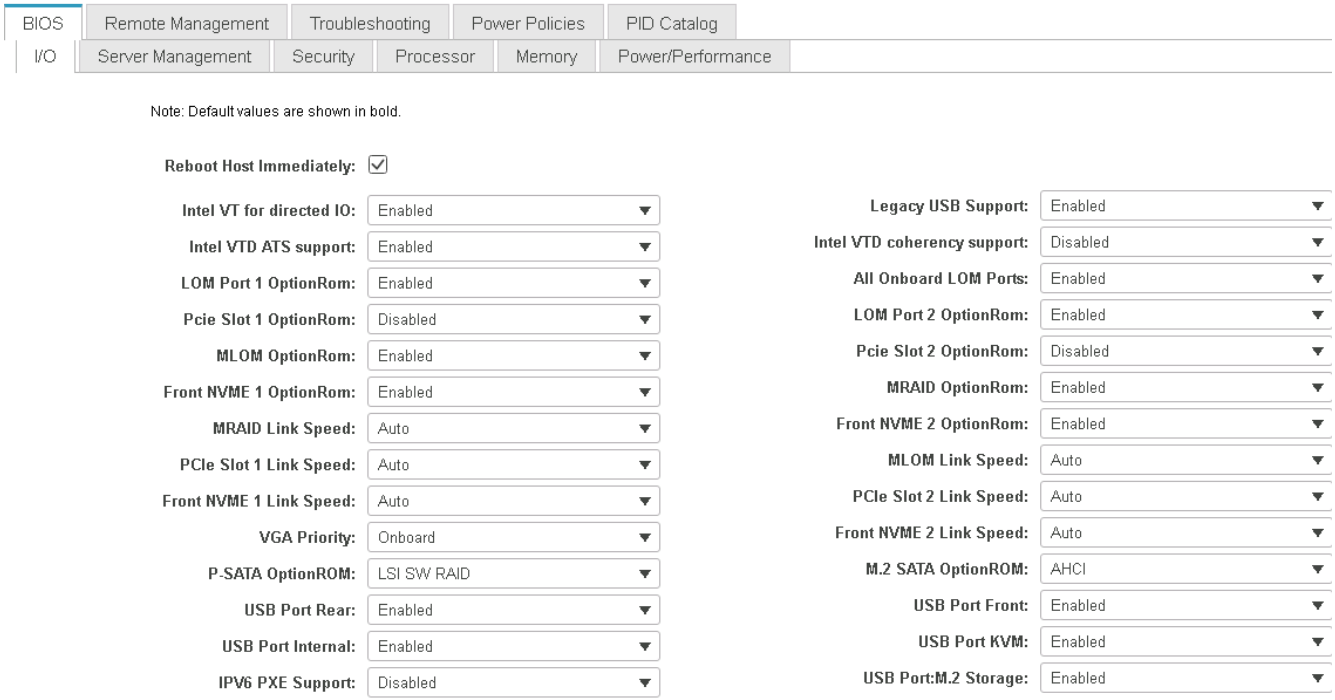


6. Reinicie o servidor para inicializar com sua nova ordem de inicialização.

Desativar o controlador RAID (se presente)

Siga as etapas a seguir se o servidor C-Series contiver um controlador RAID. Não é necessário um controlador RAID na inicialização a partir da configuração SAN. Opcionalmente, você também pode remover fisicamente o controlador RAID do servidor.

1. Clique em BIOS no painel de navegação esquerdo no CIMC.
2. Selecione Configurar BIOS.
3. Role para baixo até slot PCIe:ROM de opção HBA.
4. Se o valor ainda não estiver desativado, defina-o como desativado.



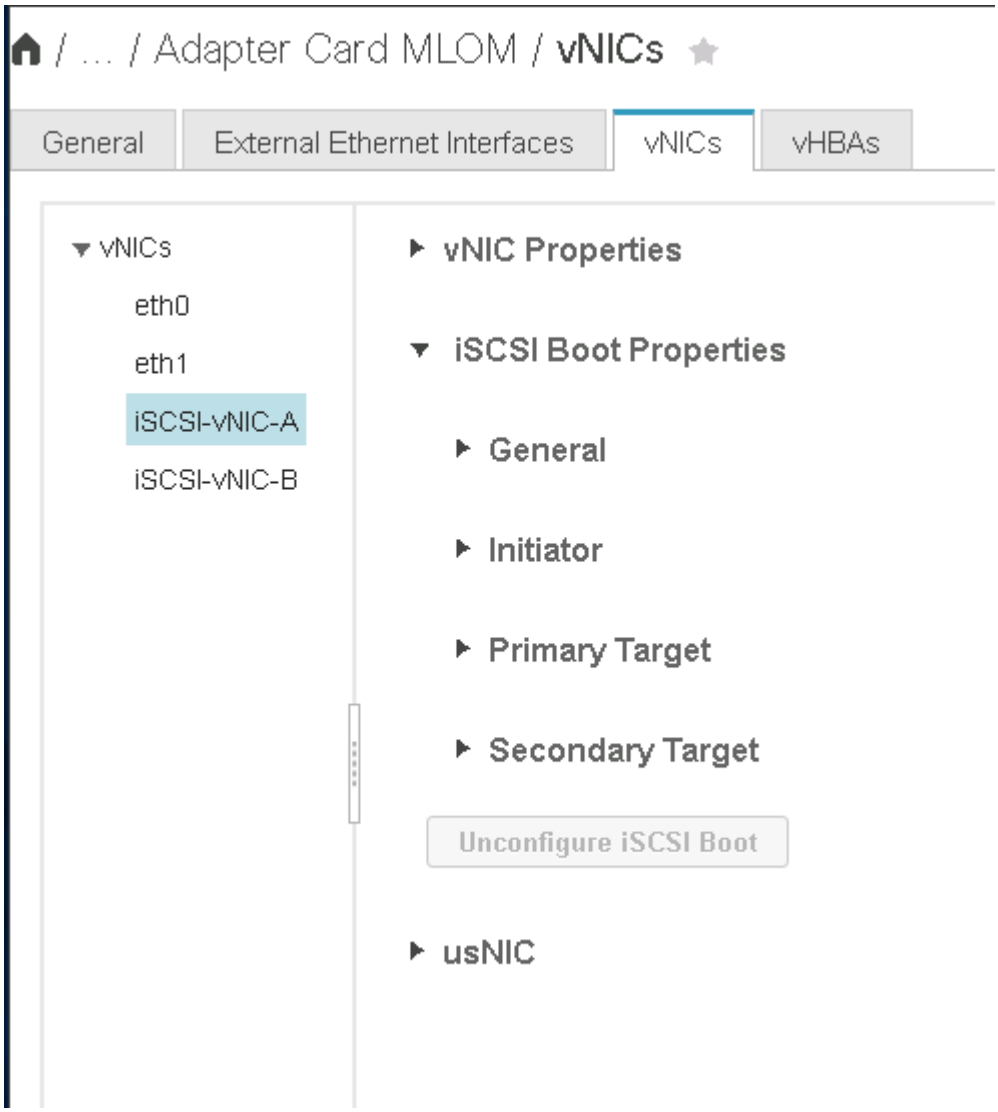
Configurar o Cisco VIC1387 para inicialização iSCSI

Os seguintes passos de configuração são para o Cisco VIC 1387 para arranque iSCSI.

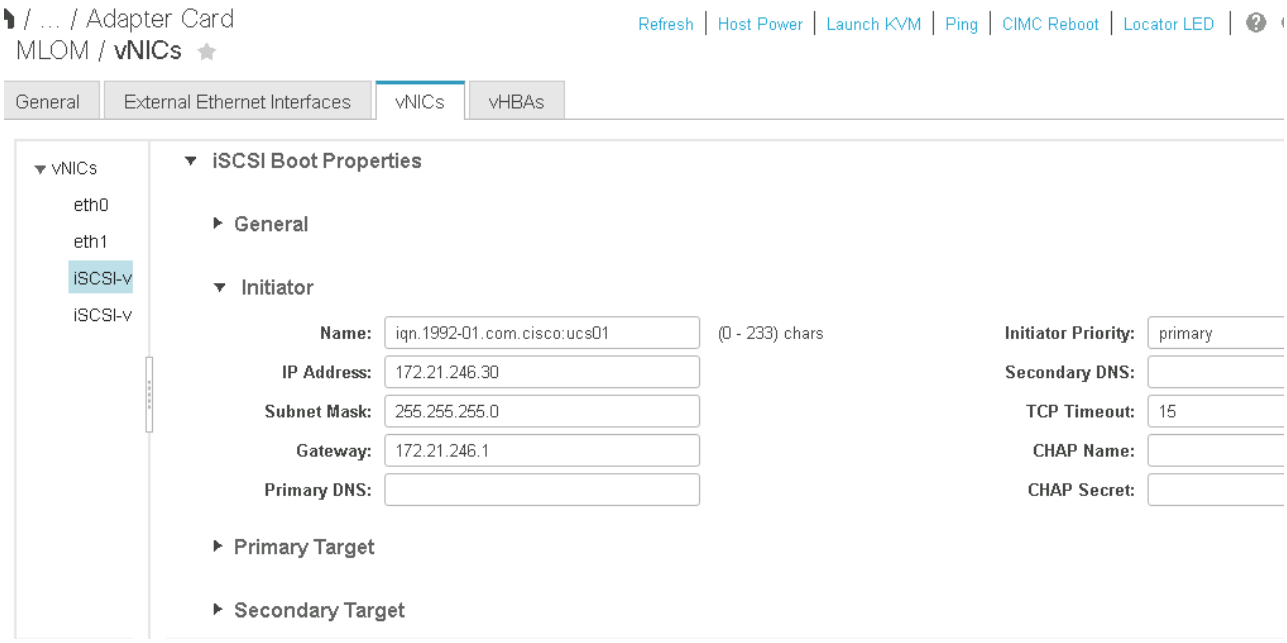
Criar iSCSI vNICs

1. Clique em Adicionar para criar um vNIC.
2. Na seção Adicionar vNIC, insira as seguintes configurações:
   - Nome: ISCSI-vNIC-A
   - MTU: 9000
   - VLAN predefinida: `<<var_iscsi_vlan_a>>`
   - Modo VLAN: TRONCO
   - Ativar arranque PXE: Verificar

3. Clique em Adicionar vNIC e, em seguida, clique em OK.
4. Repita o processo para adicionar um segundo vNIC.
   a. Nomeie o vNIC . `iSCSI-vNIC-B`
   b. `<<var_iscsi_vlan_b>>`Insira como VLAN.
   c. Defina a porta de uplink como `1`.
5. Selecione o vNIC `iSCSI-vNIC-A` à esquerda.



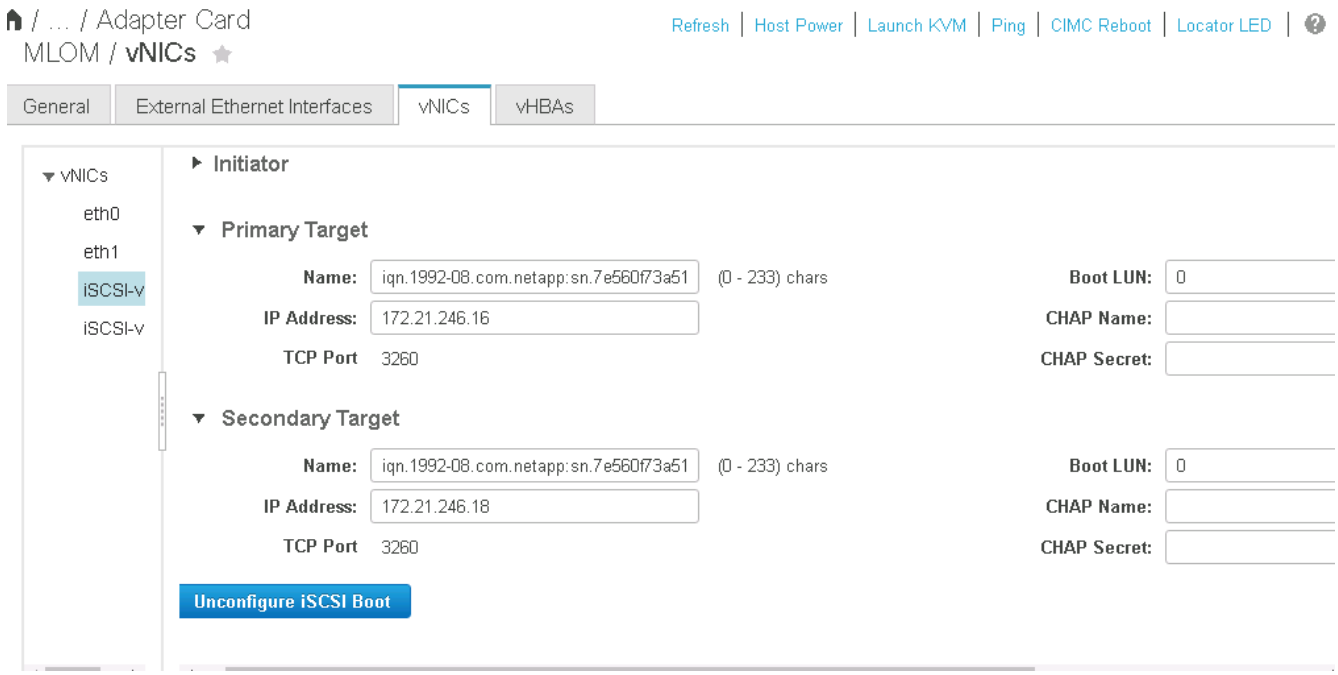
6. Em Propriedades de inicialização iSCSI, insira os detalhes do iniciador:
   - Nome: "Cliente <var_ucsa_initiator_name_a>>
   - Endereço IP: 'Cliente <var_esxi_hostA_iscsiA_ip>>
   - Máscara de sub-rede: "Cliente <var_esxi_hostA_iscsiA_mask>>"
   - Gateway: "Cliente <var_esxi_hostA_iscsiA_gateway>>"



7. Introduza os detalhes do alvo principal.
   - Nome: IQN número de infraestrutura SVM
   - Endereço IP: Endereço IP de `iscsi_lif01a`
   - LUN de arranque: 0
8. Introduza os detalhes do alvo secundário.
   - Nome: IQN número de infraestrutura SVM
   - Endereço IP: Endereço IP de `iscsi_lif02a`
   - LUN de arranque: 0

   Você pode obter o número IQN de armazenamento executando o `vserver iscsi show` comando.

   Certifique-se de gravar os nomes IQN para cada vNIC. Você precisa deles para um passo posterior.



9. Clique em Configurar iSCSI.
10. Selecione o vNIC `iSCSI-vNIC- B` e clique no botão iSCSI Boot localizado na parte superior da seção interfaces Ethernet do host.
11. Repita o processo para configurar `iSCSI-vNIC-B`o .
12. Introduza os detalhes do iniciador.
    - Nome: `<<var_ucsa_initiator_name_b>>`
    - Endereço IP: `<<var_esxi_hostb_iscsib_ip>>`
    - Máscara de sub-rede: `<<var_esxi_hostb_iscsib_mask>>`
    - Gateway: `<<var_esxi_hostb_iscsib_gateway>>`
13. Introduza os detalhes do alvo principal.
    - Nome: IQN número de infraestrutura SVM
    - Endereço IP: Endereço IP de `iscsi_lif01b`
    - LUN de arranque: 0
14. Introduza os detalhes do alvo secundário.
    - Nome: IQN número de infraestrutura SVM
    - Endereço IP: Endereço IP de `iscsi_lif02b`
    - LUN de arranque: 0

    Você pode obter o número IQN de armazenamento usando o `vserver iscsi show` comando.

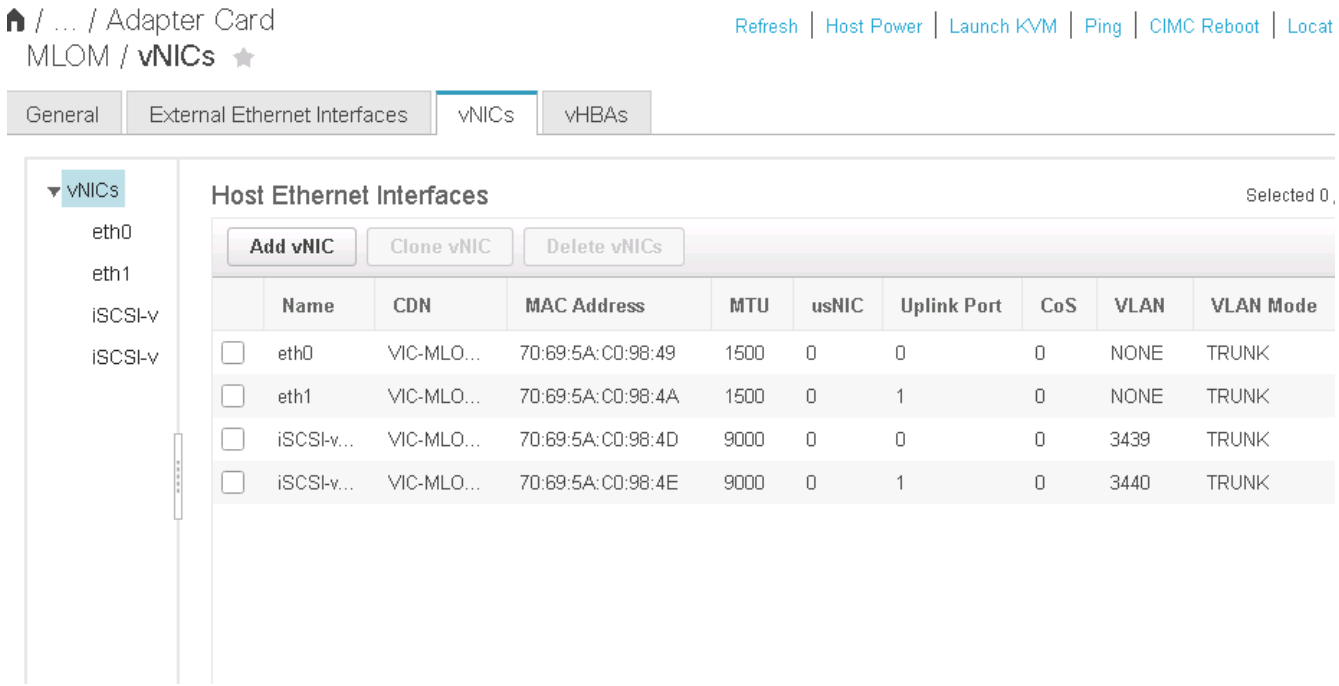
    Certifique-se de gravar os nomes IQN para cada vNIC. Você precisa deles para um passo posterior.

15. Clique em Configurar ISCSI.

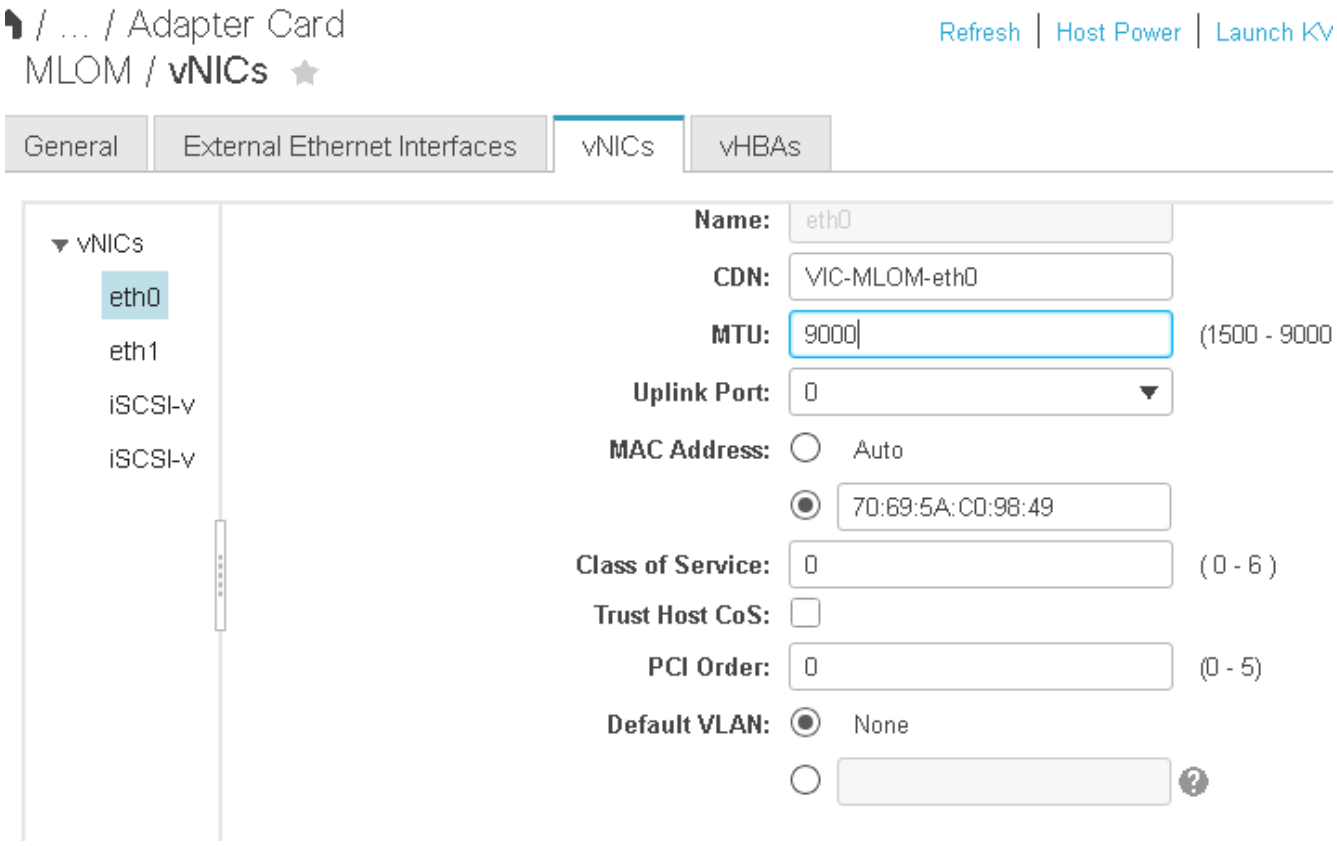
16. Repita este processo para configurar a inicialização iSCSI para o servidor Cisco UCS B.

Configure vNICs para ESXi

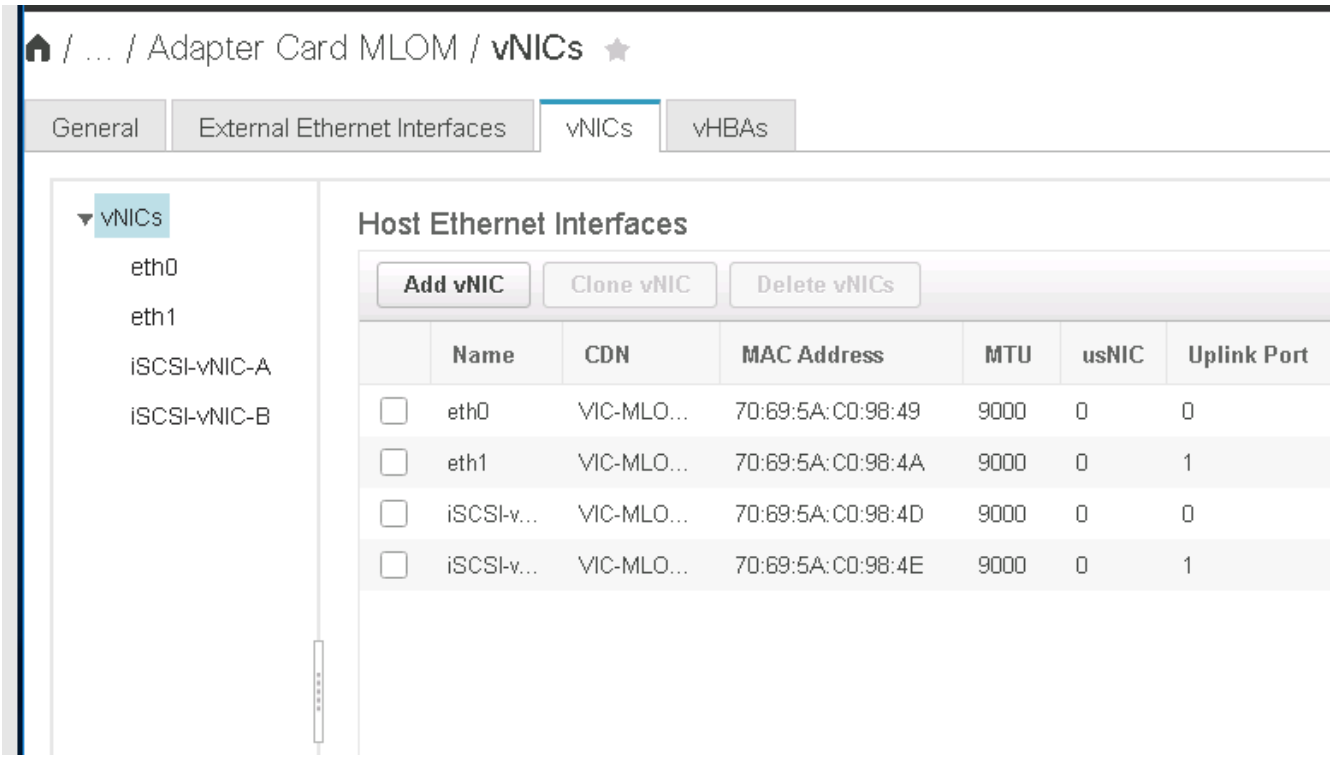
1. Na janela do navegador da interface CIMC, clique em Inventário e, em seguida, clique em adaptadores VIC Cisco no painel direito.
2. Em placas de adaptador, selecione Cisco UCS VIC 1387 e, em seguida, selecione os vNICs abaixo.



3. Selecione eth0 e clique em Propriedades.
4. Defina a MTU como 9000. Clique em Salvar alterações.



5. Repita as etapas 3 e 4 para eth1, verificando se a porta uplink está definida como `1` para eth1.



Esse procedimento deve ser repetido para cada nó inicial do servidor Cisco UCS e cada nó adicional do servidor Cisco UCS adicionado ao ambiente.

"Próximo: Procedimento de implantação de armazenamento NetApp AFF (parte 2)"

Procedimento de implantação de armazenamento NetApp AFF (parte 2)

Configuração de armazenamento de inicialização SAN ONTAP

Criar grupos iSCSI

Para criar grupos, execute o seguinte passo:

Você precisa do iniciador iSCSI IQNs da configuração do servidor para esta etapa.

1. A partir da conexão SSH do nó de gerenciamento de cluster, execute os seguintes comandos. Para exibir os três grupos criados nesta etapa, execute o comando igrop show.

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-A –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_a_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_a_iSCSI-B_vNIC_IQN>>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-B –protocol iscsi
–ostype vmware –initiator <<var_vm_host_infra_b_iSCSI-A_vNIC_IQN>>,
<<var_vm_host_infra_b_iSCSI-B_vNIC_IQN>>
```

Esta etapa deve ser concluída ao adicionar servidores adicionais da série C do Cisco UCS.

Mapeie LUNs de inicialização para grupos

Para mapear LUNs de inicialização para grupos, execute os seguintes comandos da conexão SSH de gerenciamento de cluster:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A –igroup
VM-Host-Infra- A –lun-id 0
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- B –igroup
VM-Host-Infra- B –lun-id 0
```

Esta etapa deve ser concluída ao adicionar servidores Cisco UCS C-Series adicionais.

"Próximo: Procedimento de implantação do VMware vSphere 6,7."

Procedimento de implantação do VMware vSphere 6,7

Esta seção fornece procedimentos detalhados para instalar o VMware ESXi 6,7 em uma configuração do FlexPod Express. Os procedimentos de implantação a seguir são personalizados para incluir as variáveis de ambiente descritas nas seções anteriores.

Existem vários métodos para instalar o VMware ESXi em tal ambiente. Este procedimento usa o console KVM virtual e os recursos de Mídia virtual da interface CIMC para servidores Cisco UCS C-Series para mapear Mídia de instalação remota para cada servidor individual.

Esse procedimento deve ser concluído para o servidor A do Cisco UCS e o servidor B. do Cisco UCS

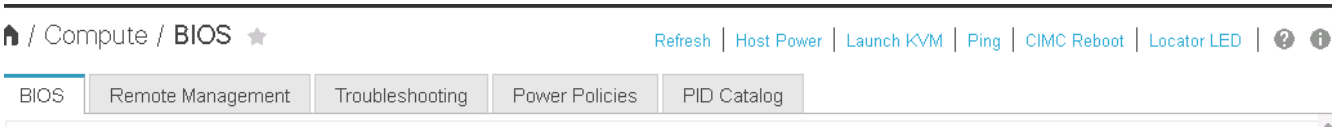
Este procedimento deve ser concluído para quaisquer nós adicionais adicionados ao cluster.

Faça login na interface CIMC para servidores autônomos do Cisco UCS C-Series

As etapas a seguir detalham o método para fazer login na interface CIMC para servidores autônomos do Cisco UCS C-Series. Você deve fazer login na interface CIMC para executar o KVM virtual, o que permite que o administrador inicie a instalação do sistema operacional por meio de Mídia remota.

Todos os anfitriões

1. Navegue até um navegador da Web e insira o endereço IP da interface CIMC para a série C do Cisco UCS. Esta etapa inicia o aplicativo GUI CIMC.
2. Faça login na IU do CIMC usando o nome de usuário e as credenciais do administrador.
3. No menu principal, selecione a guia servidor.
4. Clique em Launch KVM Console.



5. No console KVM virtual, selecione a guia Mídia virtual.
6. Selecione Map CD/DVD (CD/DVD de mapa).

Primeiro, você pode precisar clicar em Ativar dispositivos virtuais. Selecione aceitar esta sessão, se solicitado.

7. Navegue até o arquivo de imagem ISO do instalador do VMware ESXi 6,7 e clique em abrir. Clique em dispositivo de mapa.
8. Selecione o menu alimentação e selecione sistema de ciclo de alimentação (arranque a frio). Clique em Sim.

Instale o VMware ESXi

As etapas a seguir descrevem como instalar o VMware ESXi em cada host.

Faça o download da imagem personalizada do ESXI 6,7 Cisco

1. Navegue até a "Página de download do VMware vSphere" para ISOs personalizados.
2. Clique em ir para Downloads ao lado do CD de instalação da imagem personalizada do Cisco para ESXi 6,7 GA.
3. Baixe o CD de instalação (ISO) da imagem personalizada do Cisco para ESXi 6,7 GA.

Todos os anfitriões

1. Quando o sistema é inicializado, a máquina deteta a presença da Mídia de instalação do VMware ESXi.
2. Selecione o instalador do VMware ESXi no menu exibido.

O instalador é carregado. Isso leva vários minutos.

3. Depois que o instalador terminar de carregar, pressione Enter para continuar com a instalação.
4. Depois de ler o contrato de licença do usuário final, aceite-o e continue com a instalação pressionando F11.
5. Selecione o LUN NetApp que foi configurado anteriormente como o disco de instalação do ESXi e pressione Enter para continuar com a instalação.

6. Selecione o layout do teclado apropriado e pressione Enter.
7. Introduza e confirme a palavra-passe de raiz e prima Enter.
8. O instalador avisa que as partições existentes são removidas no volume. Continue com a instalação pressionando F11. O servidor reinicializa após a instalação do ESXi.

Configurar a rede de gerenciamento de host VMware ESXi

As etapas a seguir descrevem como adicionar a rede de gerenciamento para cada host VMware ESXi.

Todos os anfitriões

1. Depois que o servidor terminar de reiniciar, digite a opção para personalizar o sistema pressionando F2.
2. Inicie sessão com root como o nome de início de sessão e a palavra-passe de raiz anteriormente introduzida durante o processo de instalação.
3. Selecione a opção Configurar rede de gerenciamento.
4. Selecione adaptadores de rede e pressione Enter.
5. Selecione as portas desejadas para vSwitch0. Prima Enter.

Selecione as portas que correspondem a eth0 e eth1 no CIMC.

6. Selecione VLAN (opcional) e pressione Enter.
7. Insira o ID da VLAN `<<mgmt_vlan_id>>` . Prima Enter.
8. No menu Configure Management Network (Configurar rede de gestão), selecione IPv4 Configuration (Configuração) para configurar o endereço IP da interface de gestão. Prima Enter.
9. Use as teclas de seta para realçar Set Static address (Definir endereço estático IPv4) e use a barra de espaço para selecionar esta opção.
10. Insira o endereço IP para gerenciar o host VMware ESXi `<<esxi_host_mgmt_ip>>` .
11. Insira a máscara de sub-rede do host VMware ESXi `<<esxi_host_mgmt_netmask>>`.
12. Insira o gateway padrão do host VMware ESXi `<<esxi_host_mgmt_gateway>>` .
13. Pressione Enter para aceitar as alterações na configuração IP.
14. Aceder ao menu de configuração IPv6D.
15. Utilize a barra de espaço para desativar o IPv6 desmarcando a opção Ativar IPv6 (reiniciar necessário). Prima Enter.
16. Aceda ao menu para configurar as definições de DNS.
17. Como o endereço IP é atribuído manualmente, as informações de DNS também devem ser inseridas manualmente.
18. Introduza o endereço IP do servidor DNS primário[nameserver_ip] .
19. (Opcional) Introduza o endereço IP do servidor DNS secundário.
20. Digite o FQDN para o nome do host VMware ESXi:[esxi_host_fqdn].
21. Pressione Enter para aceitar as alterações na configuração DNS.
22. Saia do submenu Configurar rede de gerenciamento pressionando ESC.
23. Pressione Y para confirmar as alterações e reinicializar o servidor.
24. Faça logout do VMware Console pressionando ESC.

Configurar o host ESXi

Você precisa das informações na tabela a seguir para configurar cada host ESXi.

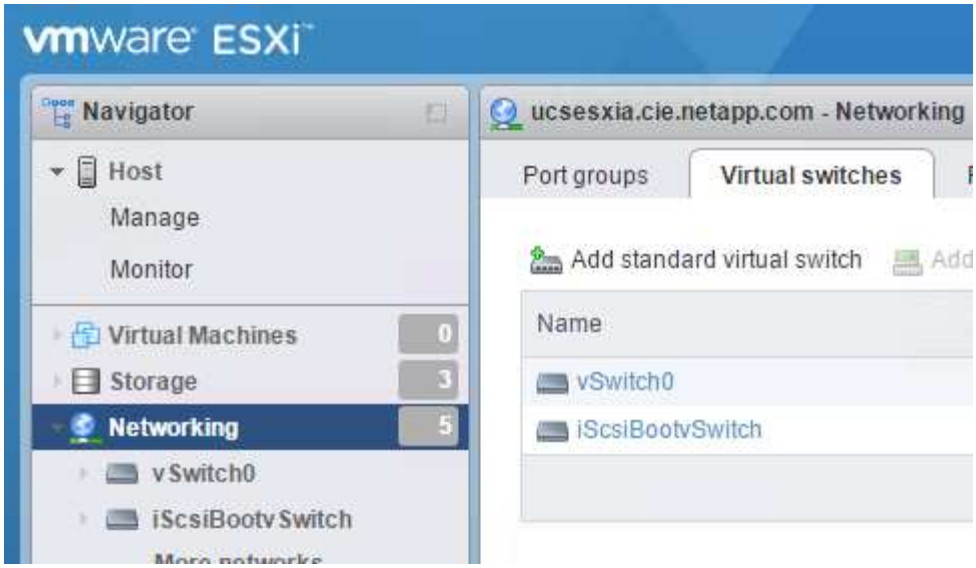
Detalhe	Valor
Nome do host ESXi	
IP de gerenciamento de host ESXi	
Máscara de gerenciamento de host ESXi	
Gateway de gerenciamento de host ESXi	
IP NFS do host ESXi	
Máscara NFS do host ESXi	
Gateway NFS de host ESXi	
ESXi host vMotion IP	
Máscara ESXi host vMotion	
Gateway vMotion do host ESXi	
IP iSCSI-A do host ESXi	
Máscara iSCSI-A. do host ESXi	
Gateway iSCSI-A. host ESXi	
IP iSCSI-B do host ESXi	
Máscara do host ESXi iSCSI-B.	
Gateway iSCSI-B. do host ESXi	

Faça login no host ESXi

1. Abra o endereço IP de gerenciamento do host em um navegador da Web.
2. Faça login no host ESXi usando a conta raiz e a senha especificada durante o processo de instalação.
3. Leia a declaração sobre o Programa de Melhoramento da experiência do Cliente da VMware. Depois de selecionar a resposta adequada, clique em OK.

Configurar o arranque iSCSI

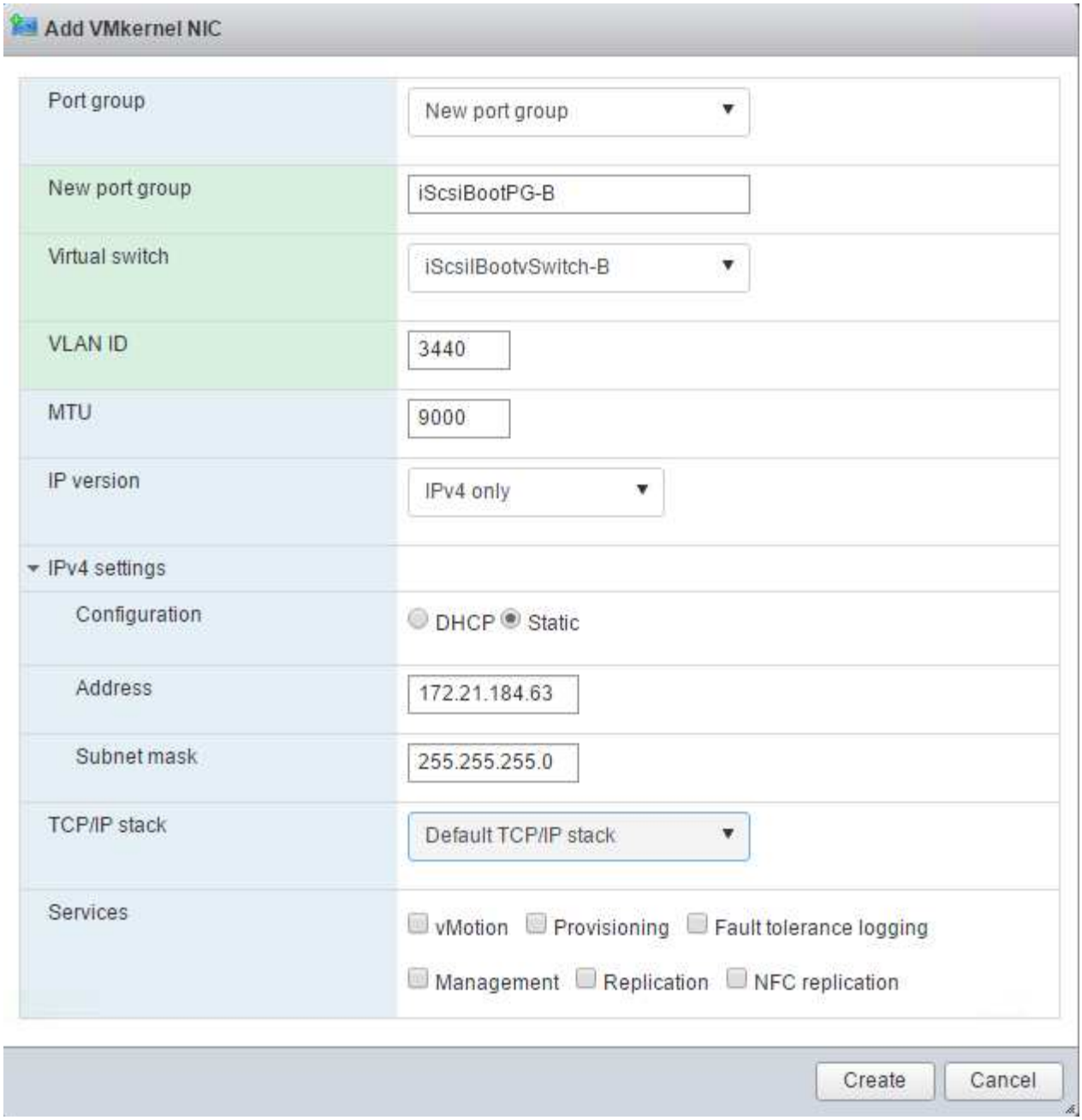
1. Selecione rede à esquerda.
2. À direita, selecione o separador Virtual switches (interrutores virtuais).



3. Clique em iScsiBootvSwitch.
4. Selecione Editar definições.
5. Altere a MTU para 9000 e clique em Salvar.
6. Clique em rede no painel de navegação esquerdo para retornar à guia switches virtuais.
7. Clique em Adicionar comutador virtual padrão.
8. Forneça o `iScsiBootvSwitch-B` nome para o nome do vSwitch.
   - Defina a MTU como 9000.
   - Selecione vmnic3 nas opções Uplink 1.
   - Clique em Adicionar.

> vmnic2 e vmnic3 são usados para inicialização iSCSI nesta configuração. Se você tiver NICs adicionais no host ESXi, poderá ter números vmnic diferentes. Para confirmar quais NICs são usados para inicialização iSCSI, faça a correspondência dos endereços MAC nos vNICs iSCSI no CIMC com os vmnics no ESXi.

9. No painel central, selecione a guia NICs do VMkernel.
10. Selecione Adicionar NIC VMkernel.
    - Especifique um novo nome de grupo de portas `iScsiBootPG-B` de .
    - Selecione iScsiBootvSwitch-B para o switch virtual.
    - Insira `<<iscsib_vlan_id>>` para a ID da VLAN.
    - Altere a MTU para 9000.
    - Expanda Configurações IPv4.
    - Selecione Configuração estática.
    - Introduza `<<var_hosta_iscsib_ip>>` o endereço.
    - Introduza `<<var_hosta_iscsib_mask>>` para Máscara de sub-rede.
    - Clique em criar.

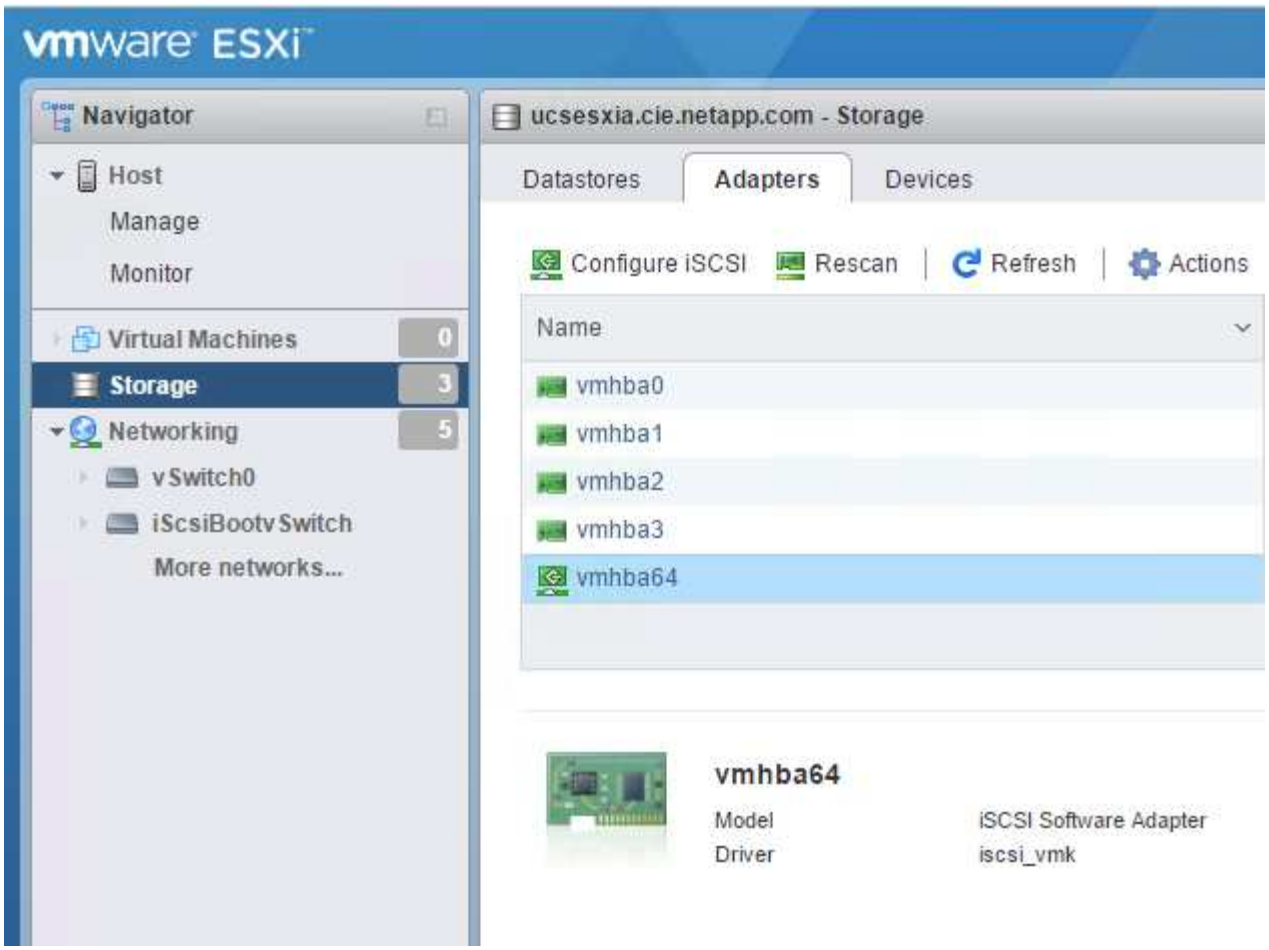


Defina a MTU como 9000 ativada `iScsiBootPG- A.`

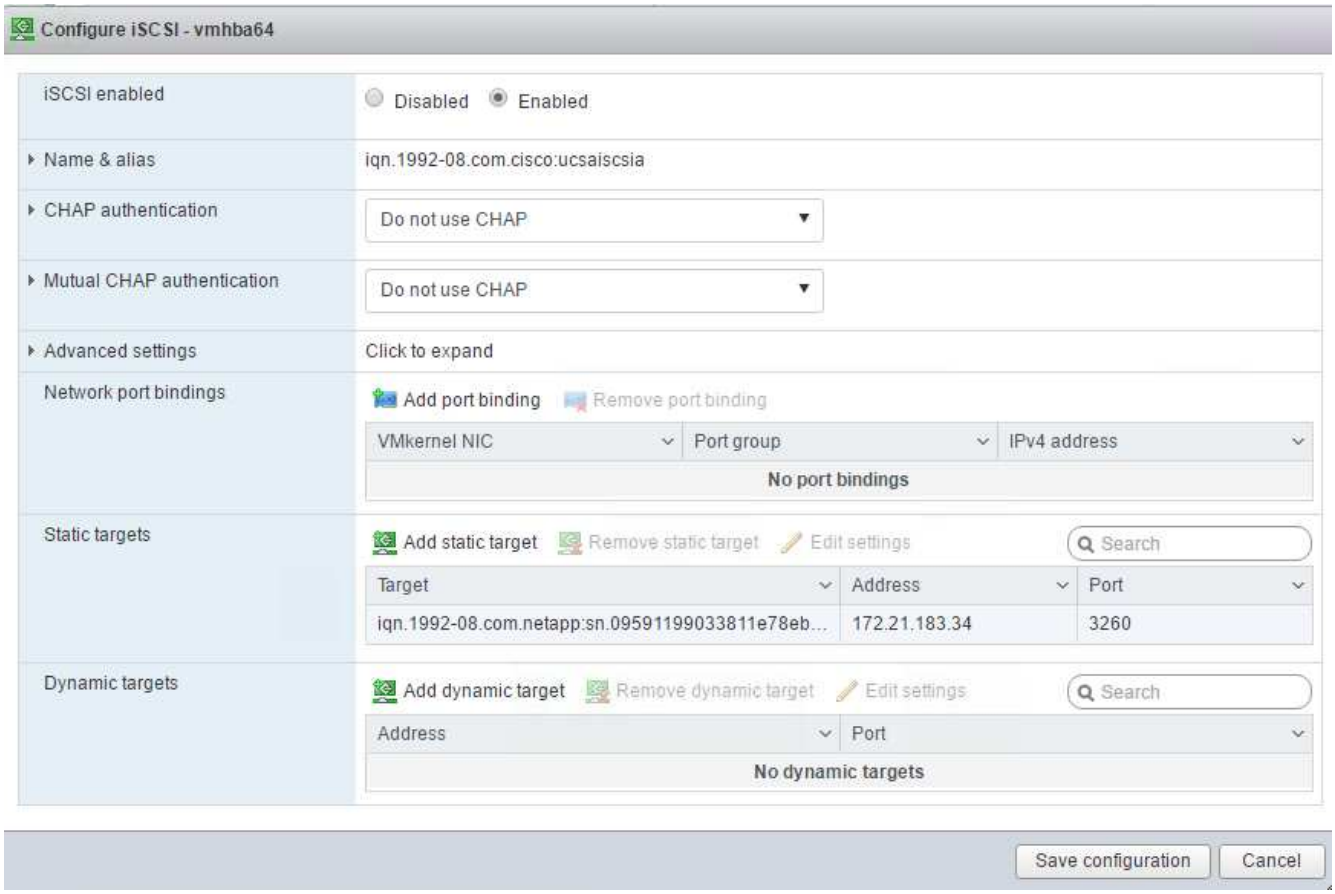
Configurar multipathing iSCSI

Para configurar multipathing iSCSI nos hosts ESXi, execute as seguintes etapas:

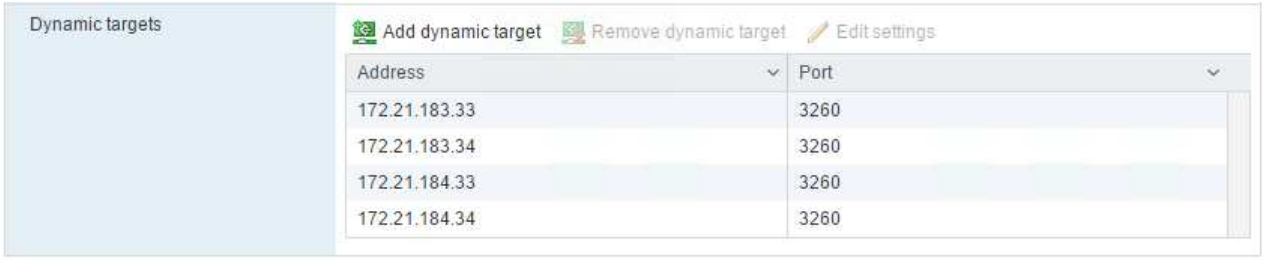
1. Selecione armazenamento no painel de navegação esquerdo. Clique em adaptadores.
2. Selecione o adaptador de software iSCSI e clique em Configurar iSCSI.



3. Em alvos dinâmicos, clique em Adicionar alvo dinâmico.



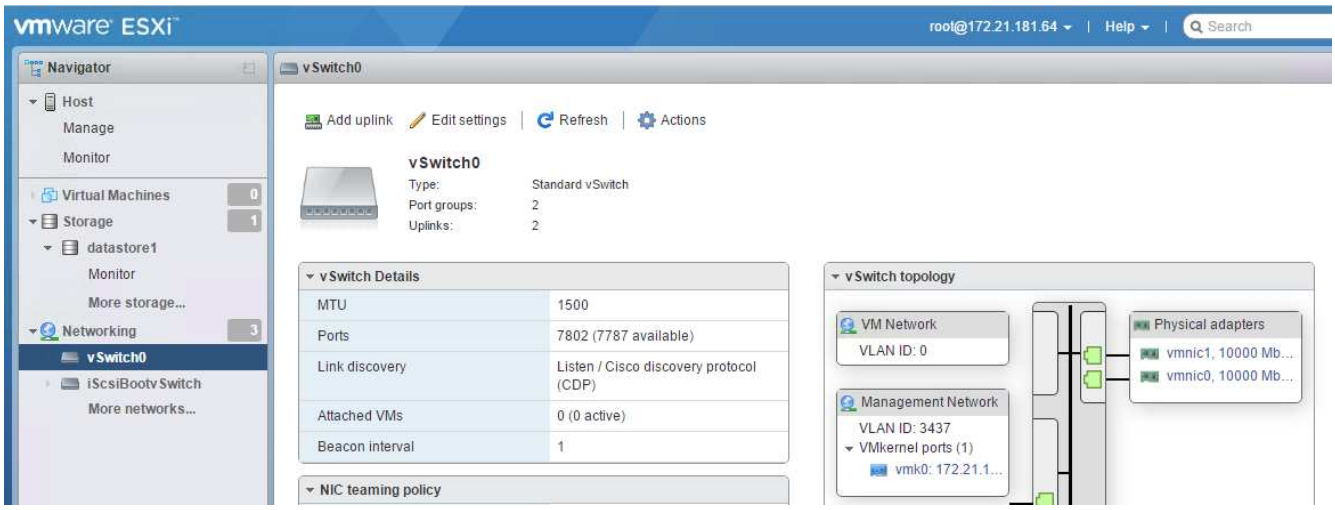
4. Introduza o endereço `iscsi_lif01a` IP .
   - Repita com os endereços IP `iscsi_lif01b` , `iscsi_lif02a`, e `iscsi_lif02b`.
   - Clique em Save Configuration (Guardar configuração).



Você pode encontrar os endereços IP iSCSI LIF executando o comando "Network interface show" no cluster NetApp ou olhando para a guia interfaces de rede no OnCommand System Manager.

Configurar o host ESXi

1. No painel de navegação esquerdo, selecione rede.
2. Selecione vSwitch0.



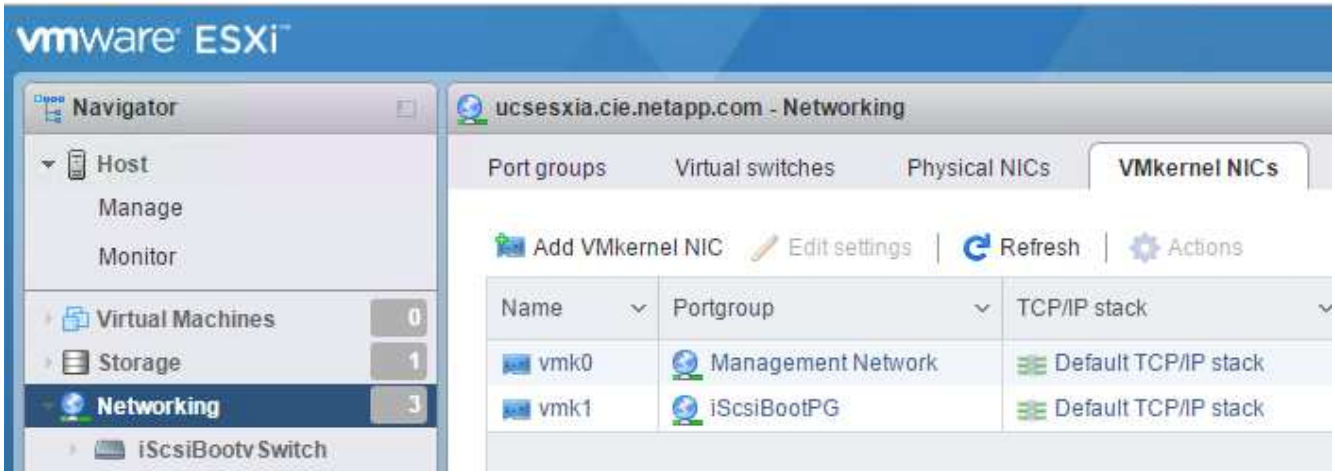
3. Selecione Editar definições.
4. Altere a MTU para 9000.
5. Expanda agrupamento NIC e verifique se o vmnic0 e o vmnic1 estão definidos como ativo.

Configurar grupos de portas e NICs do VMkernel

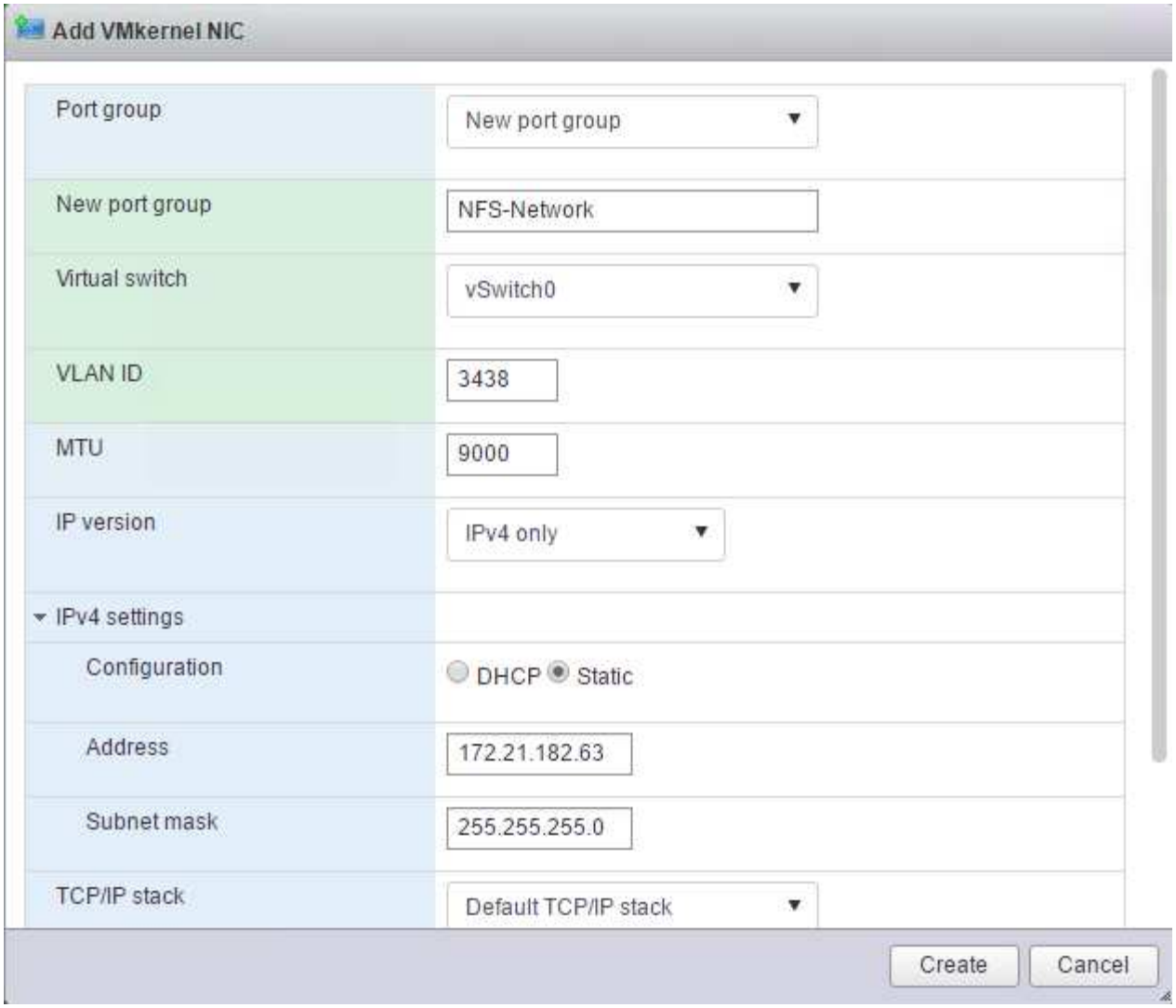
1. No painel de navegação esquerdo, selecione rede.
2. Clique com o botão direito do rato no separador grupos de portas.

3. Clique com o botão direito do rato em rede VM e selecione Editar. Altere a ID da VLAN para `<<var_vm_traffic_vlan>>`.
4. Clique em Adicionar grupo de portas.
   - Nomeie o grupo de portas `MGMT-Network` .
   - Insira `<<mgmt_vlan>>` para a ID da VLAN.
   - Certifique-se de que vSwitch0 está selecionado.
   - Clique em Adicionar.

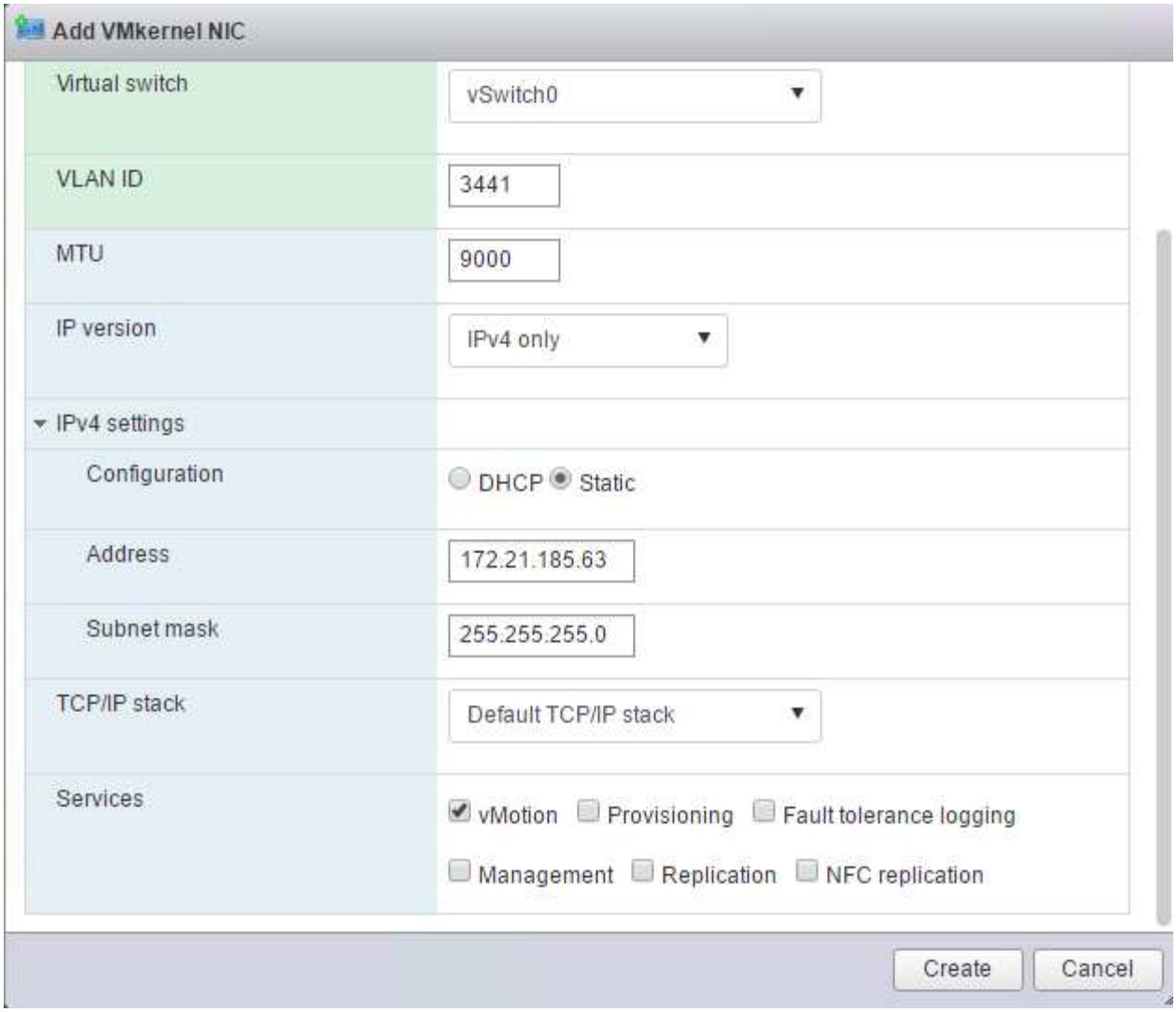
5. Clique na guia NICs do VMkernel.



6. Selecione Adicionar NIC VMkernel.
   - Selecione novo grupo de portas.
   - Nomeie o grupo de portas `NFS-Network` .
   - Insira `<<nfs_vlan_id>>` para a ID da VLAN.
   - Altere a MTU para 9000.
   - Expanda Configurações IPv4.
   - Selecione Configuração estática.
   - Introduza `<<var_hosta_nfs_ip>>` o endereço.
   - Introduza `<<var_hosta_nfs_mask>>` para Máscara de sub-rede.
   - Clique em criar.



7. Repita esse processo para criar a porta VMkernel do vMotion.
8. Selecione Adicionar NIC VMkernel.
    a. Selecione novo grupo de portas.
    b. Nomeie o grupo de portas vMotion.
    c. Insira `<<vmotion_vlan_id>>` para a ID da VLAN.
    d. Altere a MTU para 9000.
    e. Expanda Configurações IPv4.
    f. Selecione Configuração estática.
    g. Introduza `<<var_hosta_vmotion_ip>>` o endereço.
    h. Introduza `<<var_hosta_vmotion_mask>>` para Máscara de sub-rede.
    i. Certifique-se de que a caixa de verificação vMotion está selecionada após IPv4 Settings (Definições).

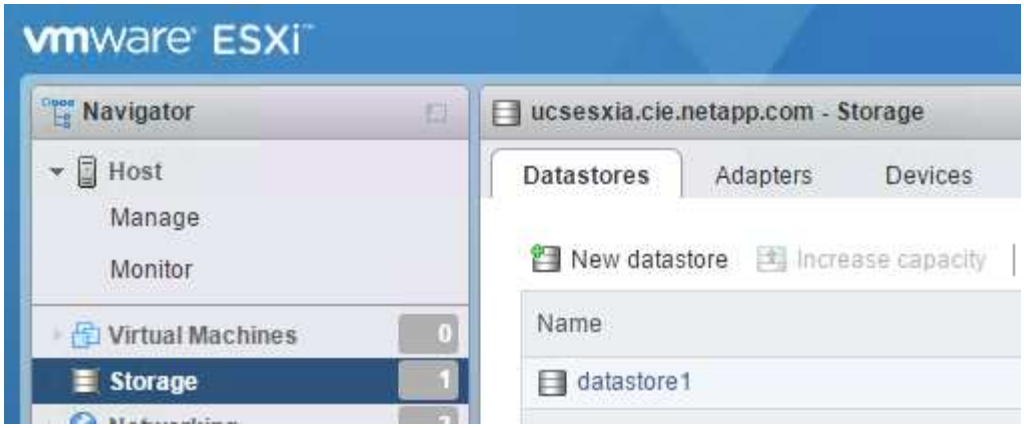


Há muitas maneiras de configurar a rede ESXi, inclusive usando o switch distribuído do VMware vSphere se o licenciamento permitir. Configurações de rede alternativas são suportadas no FlexPod Express se forem necessárias para atender aos requisitos empresariais.

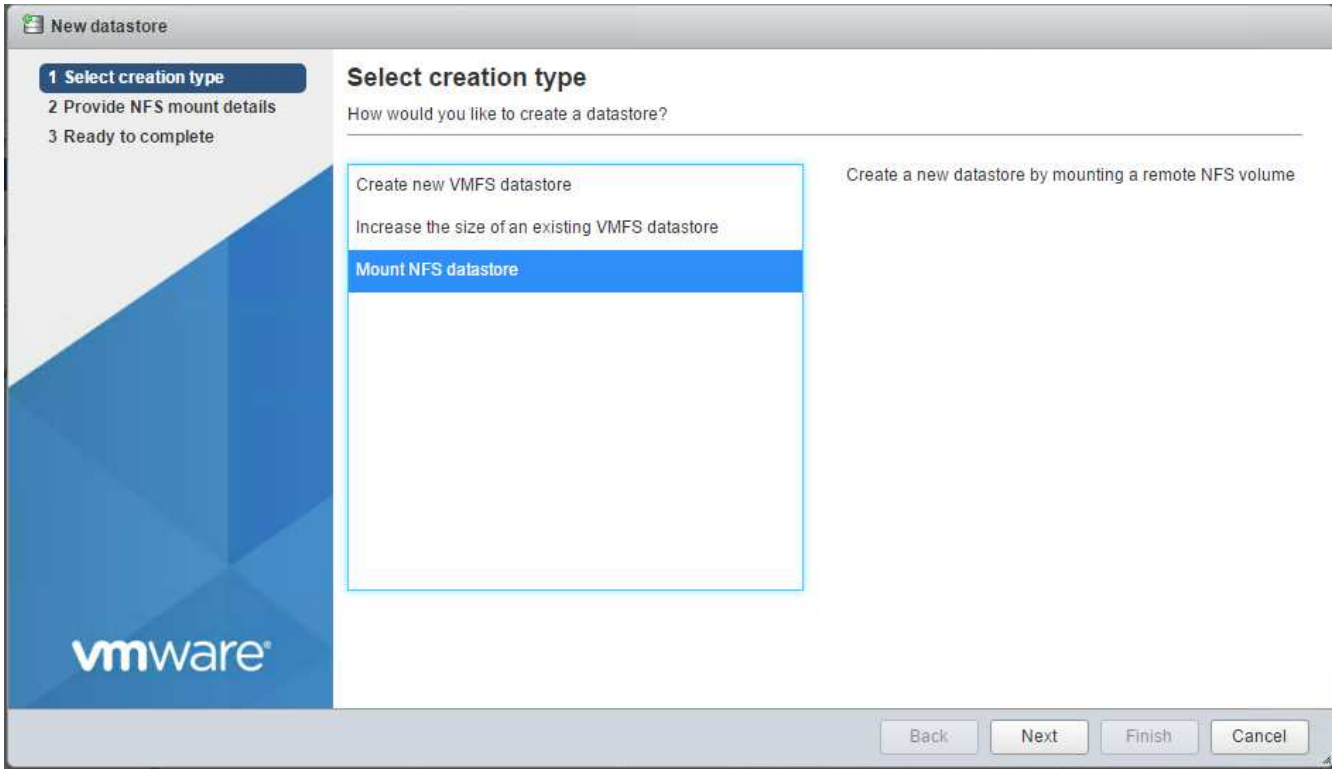
Monte os primeiros datastores

Os primeiros datastores a serem montados são o datastore infra_datastore_1 para máquinas virtuais e o datastore infra_swap para arquivos de swap de máquina virtual.

1. Clique em Storage (armazenamento) no painel de navegação esquerdo e, em seguida, clique em New datastore (novo armazenamento de dados).



2. Selecione Monte o armazenamento de dados NFS.



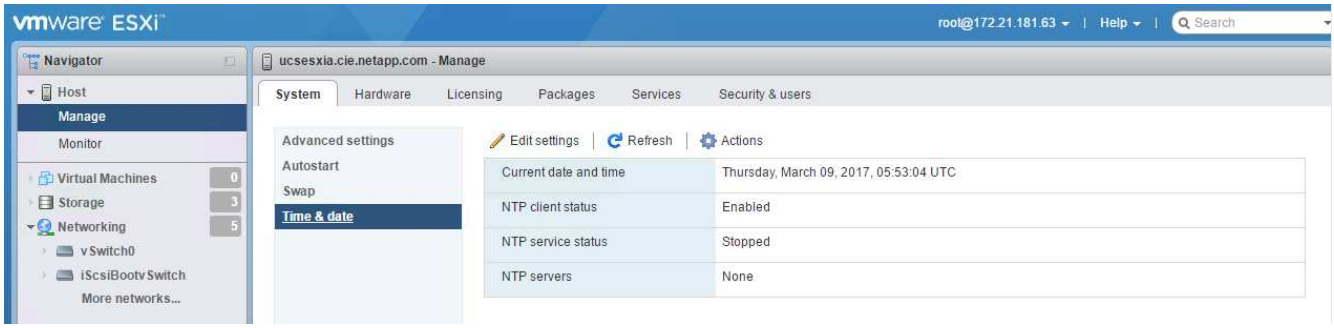
3. Em seguida, insira as seguintes informações na página fornecer detalhes da montagem NFS:
   - Nome: `infra_datastore_1`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Compartilhar: /Infra_datastore_1
   - Certifique-se de que NFS 3 está selecionado.
4. Clique em concluir. Pode ver a tarefa a concluir no painel tarefas recentes.
5. Repita este processo para montar o datastore infra_swap:
   - Nome: `infra_swap`
   - Servidor NFS: `<<var_nodea_nfs_lif>>`
   - Partilhar: `/infra_swap`

◦ Certifique-se de que NFS 3 está selecionado.

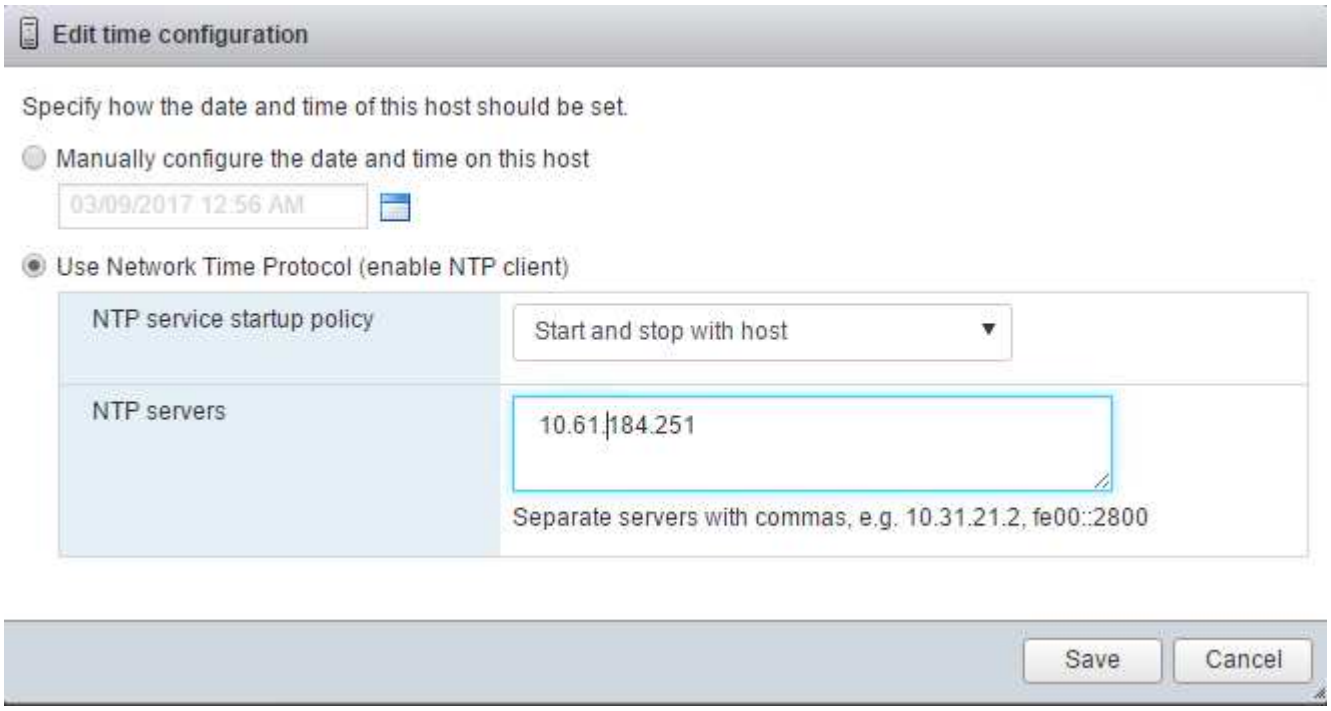
Configure o NTP

Para configurar o NTP para um host ESXi, execute as seguintes etapas:

1. Clique em Gerenciar no painel de navegação esquerdo. Selecione System (sistema) no painel direito e, em seguida, clique em Time & Date (hora e data).



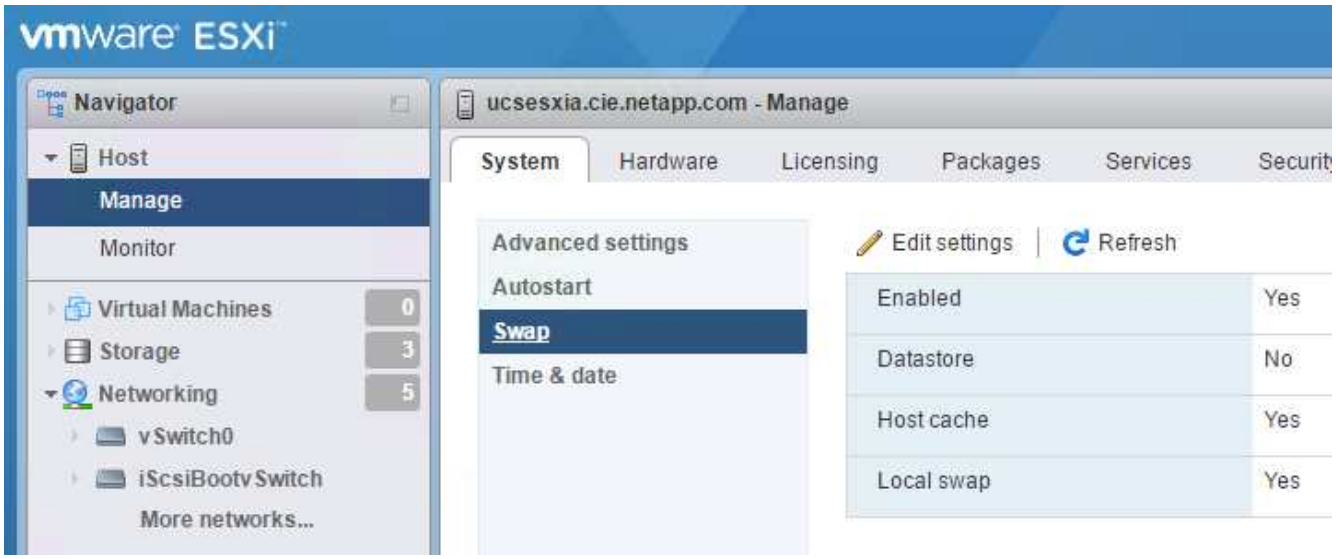
2. Selecione utilizar protocolo de tempo de rede (Ativar cliente NTP).
3. Selecione Iniciar e Parar com Host como a política de inicialização do serviço NTP.
4. `<<var_ntp>>`Introduza como servidor NTP. Você pode definir vários servidores NTP.
5. Clique em Guardar.



Mova o local do arquivo swap da máquina virtual

Estas etapas fornecem detalhes para mover a localização do arquivo swap da máquina virtual.

1. Clique em Gerenciar no painel de navegação esquerdo. Selecione System (sistema) no painel direito e, em seguida, clique em Swap (trocar).



2. Clique em Edit Settings (Editar definições). Selecione infra_swap nas opções do datastore.

3. Clique em Guardar.

Instale o plug-in NFS NetApp 1.0.20 para VMware VAAI

Para instalar o plug-in NFS NetApp 1.0.20 para VMware VAAI, siga estas etapas.

1. Digite os seguintes comandos para verificar se o VAAI está ativado:

```
esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
```

   Se o VAAI estiver ativado, estes comandos produzem a seguinte saída:

```
~ #  esxcfg-advcfg -g /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
~ # esxcfg-advcfg -g /DataMover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
```

2. Se o VAAI não estiver ativado, digite os seguintes comandos para ativar o VAAI:

```
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedInit
esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
```

Estes comandos produzem a seguinte saída:

```
~ # esxcfg-advcfg -s 1 /Data Mover/HardwareAcceleratedInit
Value of HardwareAcceleratedInit is 1
~ #  esxcfg-advcfg -s 1 /DataMover/HardwareAcceleratedMove
Value of HardwareAcceleratedMove is 1
```

3. Faça o download do plug-in NFS do NetApp para VMware VAAI:
   a. Vá para "página de download do software" .
   b. Role para baixo e clique em NetApp NFS Plug-in para VMware VAAI.
   c. Selecione a plataforma ESXi.
   d. Transfira o pacote offline (.zip) ou o pacote online (.vib) do plug-in mais recente.
4. Instale o plug-in no host ESXi usando a CLI do ESX.
5. Reinicie o host ESXI.

```
[root@vm-host-infra-04:~] ls /vmfs/volumes/datastore1/NetAppNasPlugin.vib
/vmfs/volumes/datastore1/NetAppNasPlugin.vib
[root@vm-host-infra-04:~] esxcli software vib install -v /vmfs/volumes/datastore1/NetAppNasPlugin.vib
Installation Result
   Message: The update completed successfully, but the system needs to be rebooted for the changes to be effective.
   Reboot Required: true
   VIBs Installed: NetApp_bootbank_NetAppNasPlugin_1.1.2-3
   VIBs Removed:
   VIBs Skipped:
[root@vm-host-infra-04:~]
```

"Próximo: Instale o VMware vCenter Server 6,7"

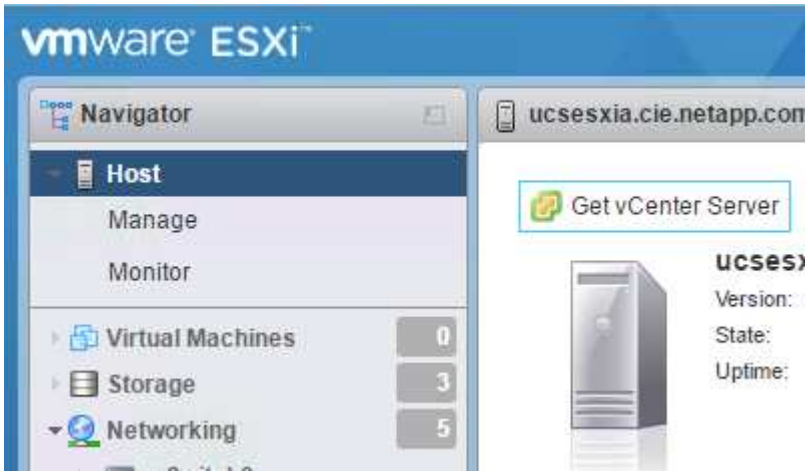
Instale o VMware vCenter Server 6,7

Esta seção fornece procedimentos detalhados para instalar o VMware vCenter Server 6,7 em uma configuração do FlexPod Express.

O FlexPod Express usa o VMware vCenter Server Appliance (VCSA).

Faça download do dispositivo de servidor VMware vCenter

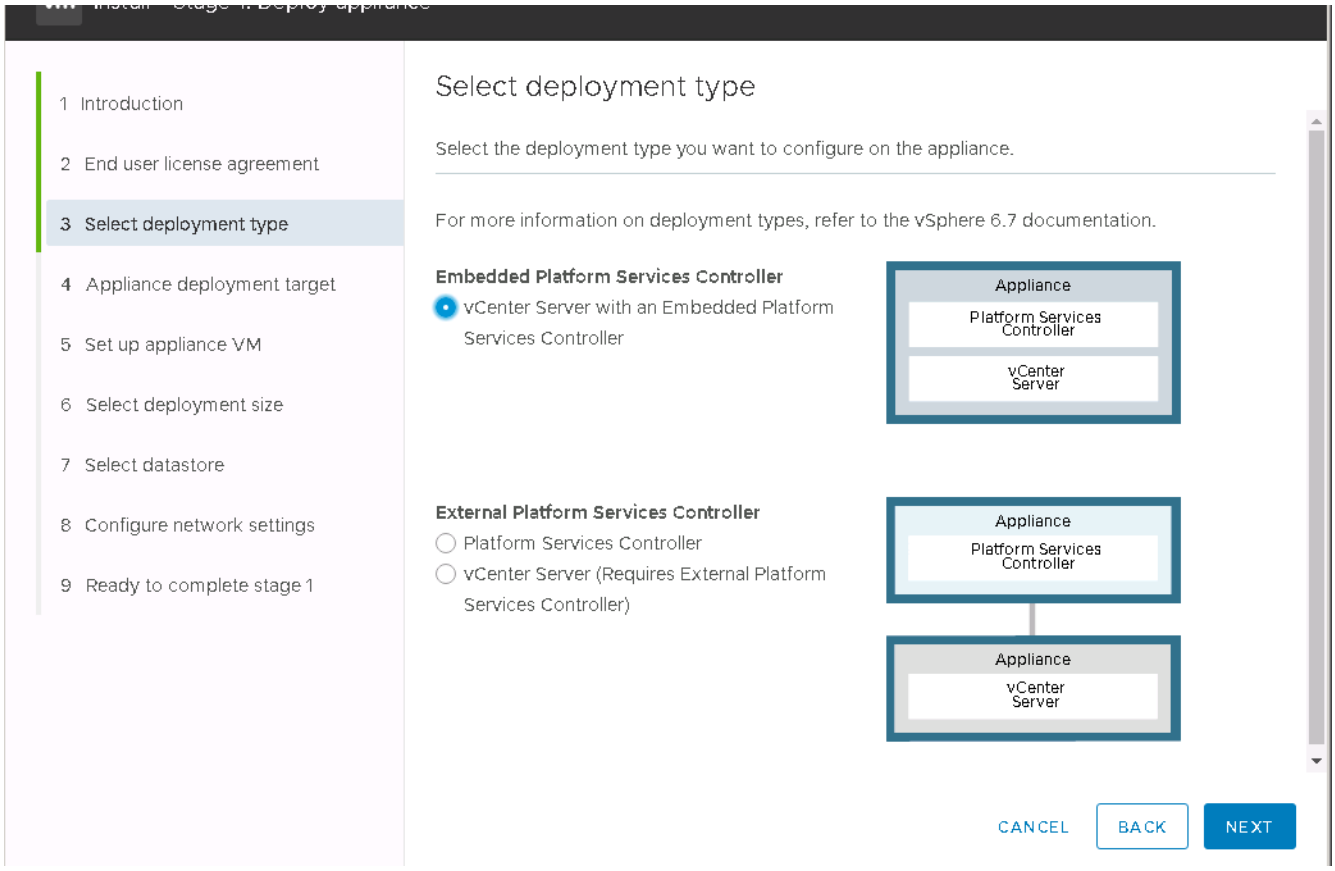
1. Faça o download do VCSA. Acesse o link de download clicando no ícone obter vCenter Server ao gerenciar o host ESXi.



2. Faça download do VCSA a partir do site da VMware.

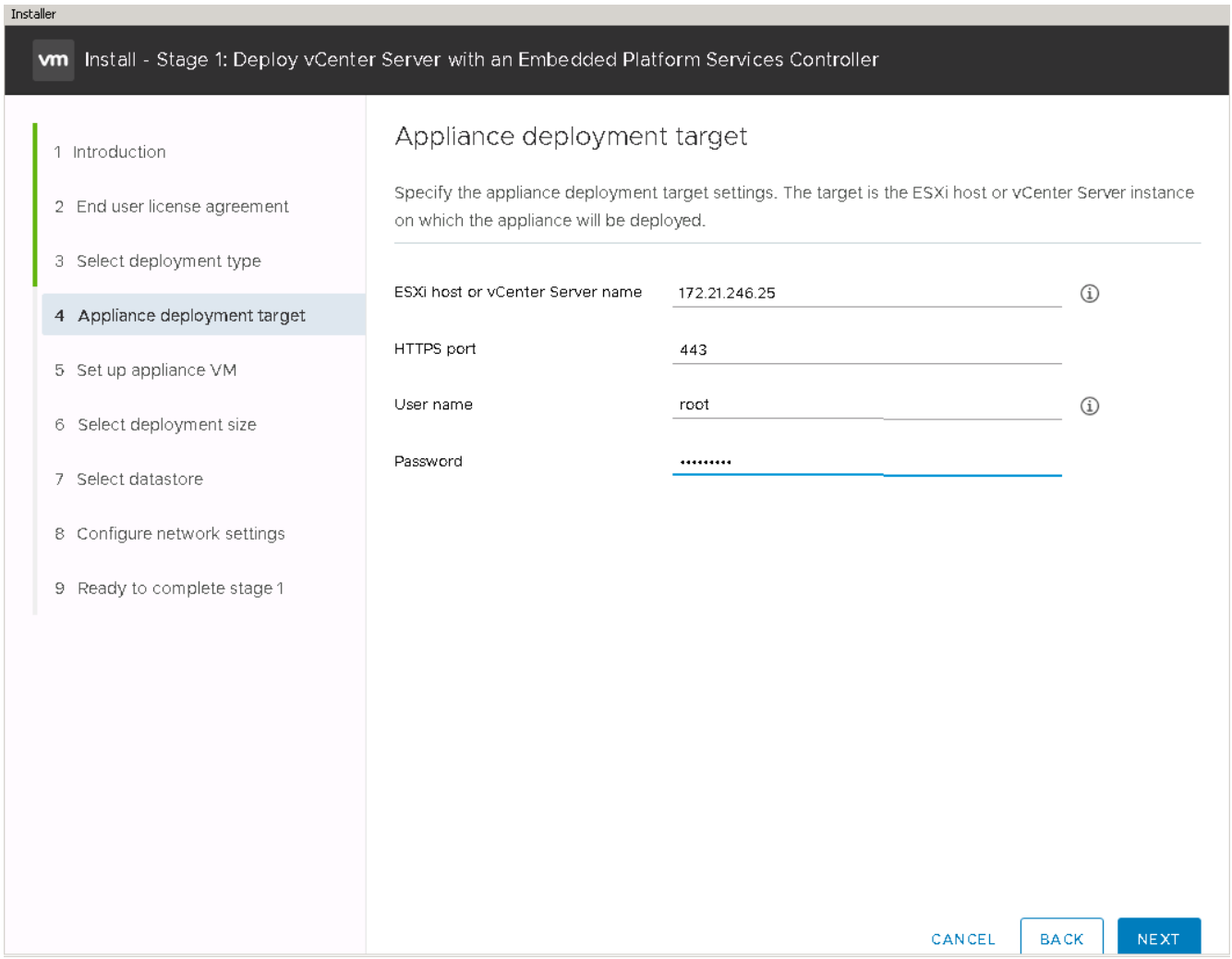
> Embora o Microsoft Windows vCenter Server instalável seja suportado, a VMware recomenda o VCSA para novas implantações.

3. Monte a imagem ISO.
4. Navegue até o diretório vcsa-ui-installer> Win32. Clique duas vezes em installer.exe.
5. Clique em Instalar.
6. Clique em Avançar na página Introdução.
7. Aceite o contrato de licença do utilizador final.
8. Selecione controlador de serviços de plataforma incorporada como o tipo de implantação.

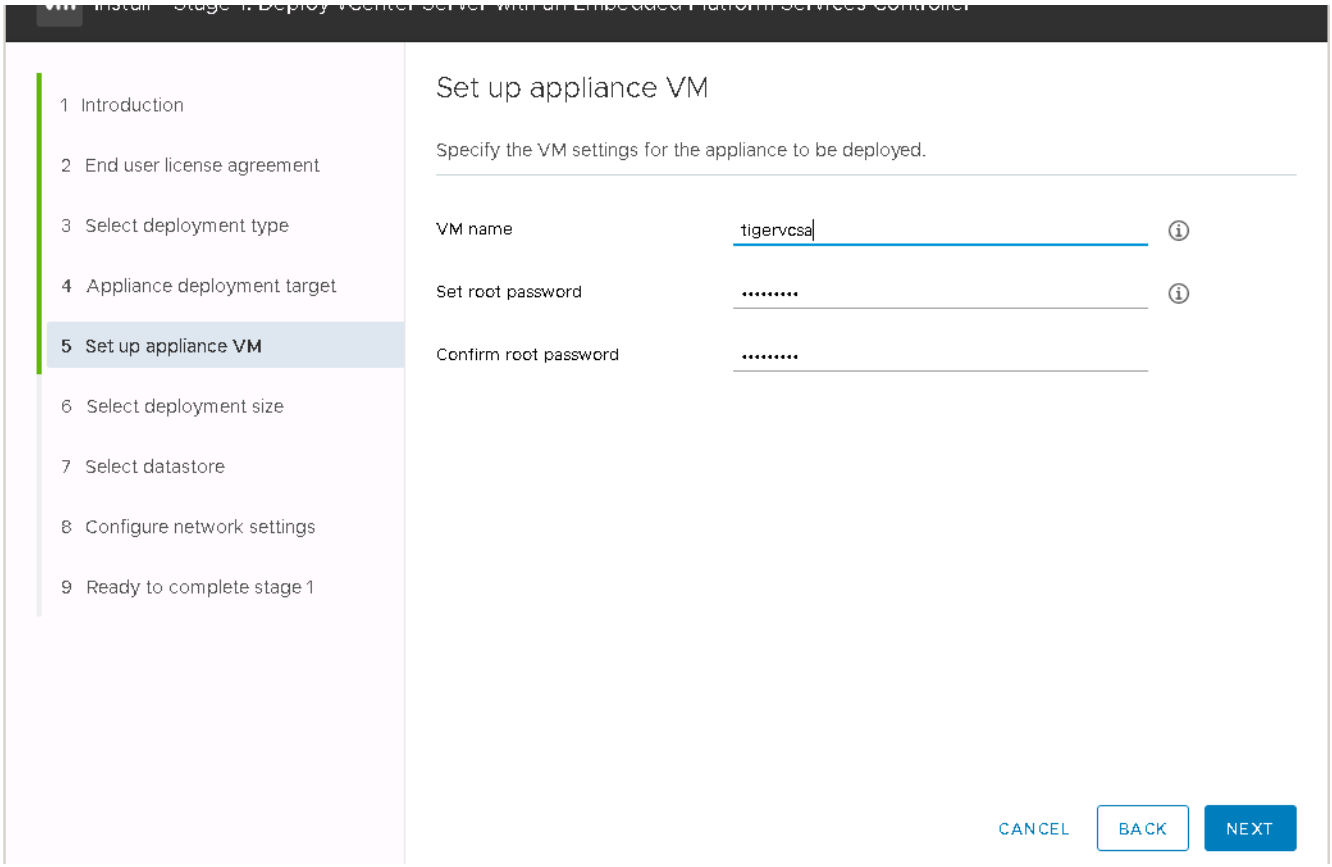


Se necessário, a implantação do controlador de serviços de plataforma externa também é suportada como parte da solução FlexPod Express.

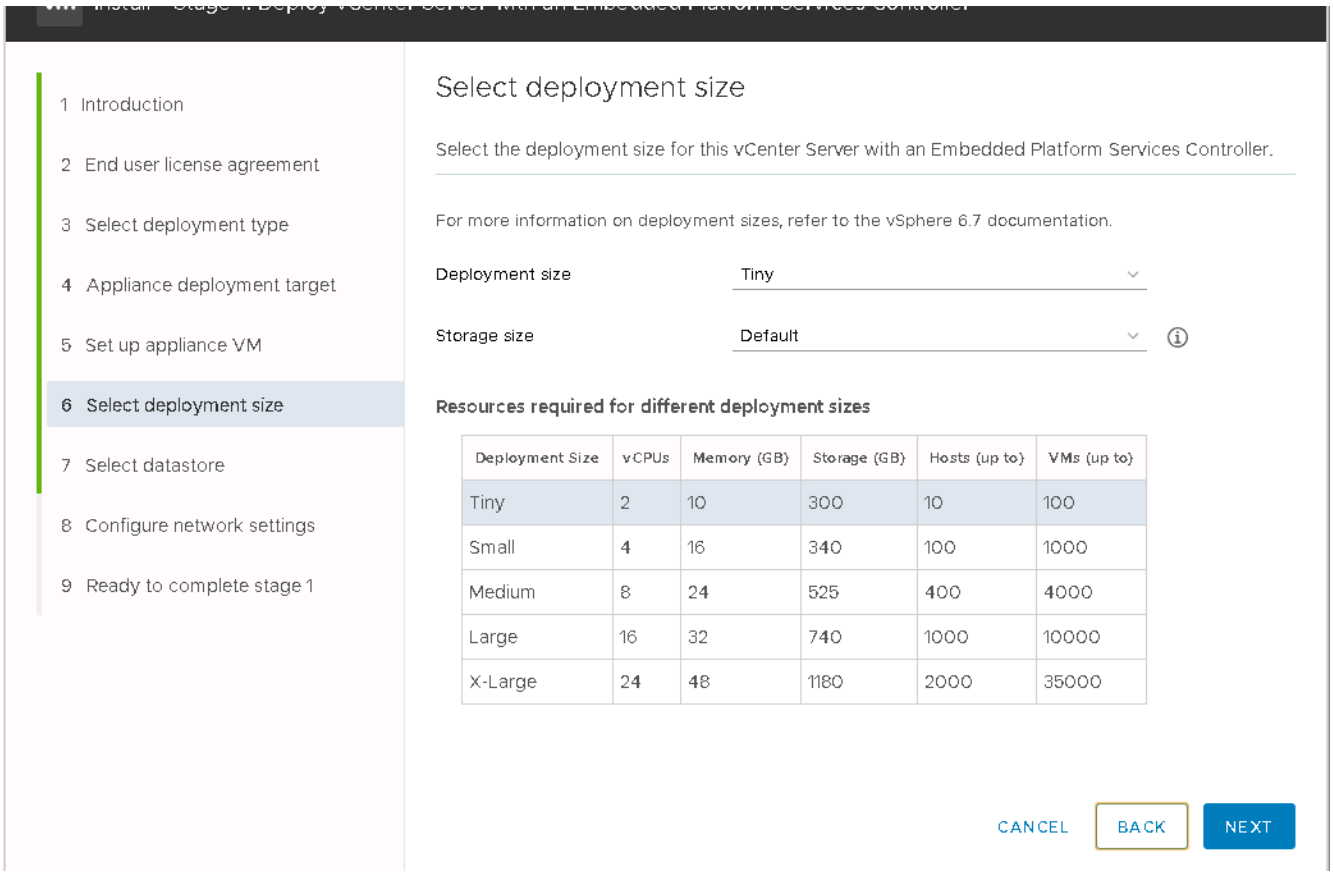
9. No destino de implantação do dispositivo, insira o endereço IP de um host ESXi que você implantou e o nome de usuário raiz e a senha de raiz.



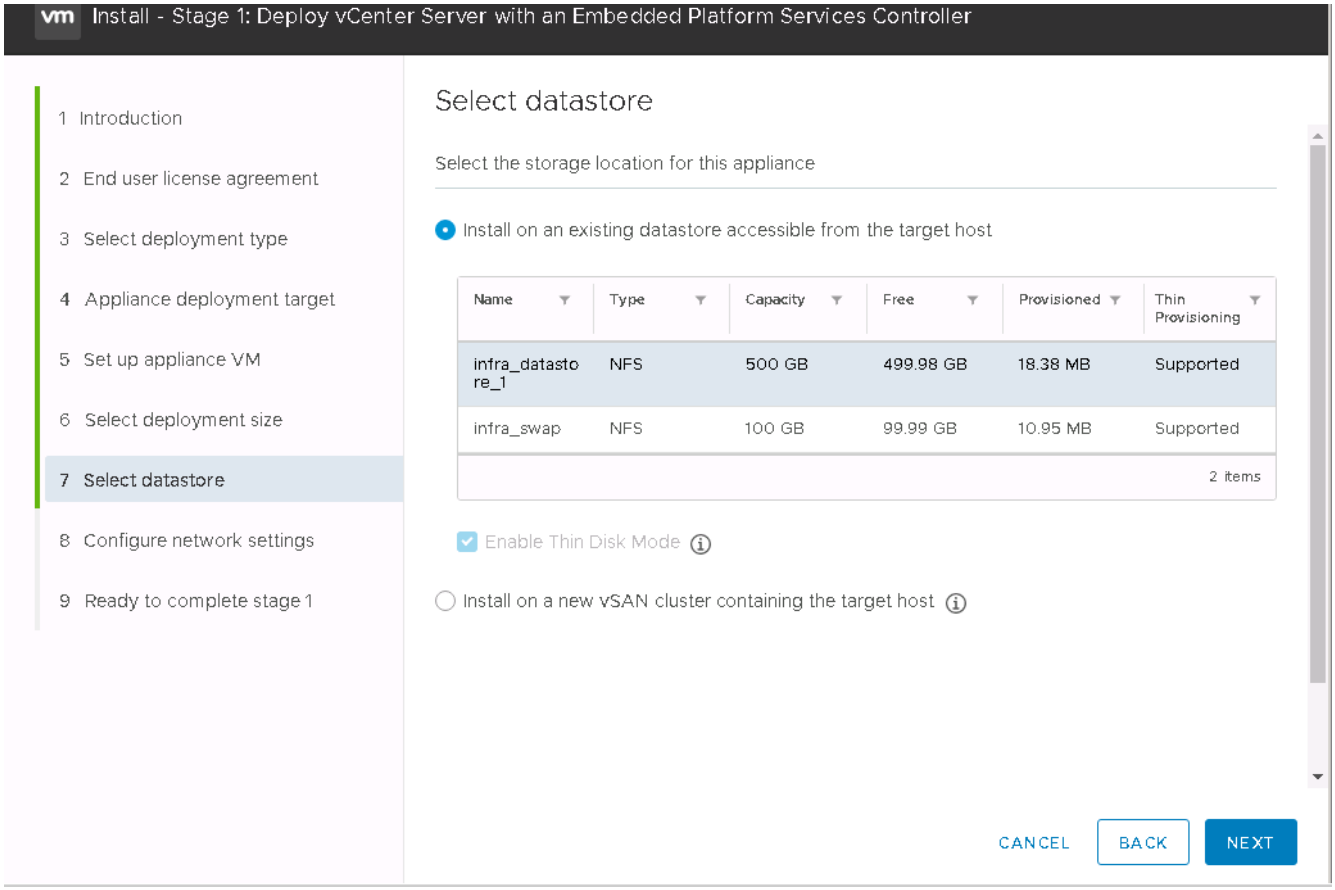
10. Defina a VM do appliance inserindo `VCSA` como o nome da VM e a senha raiz que você gostaria de usar para o VCSA.



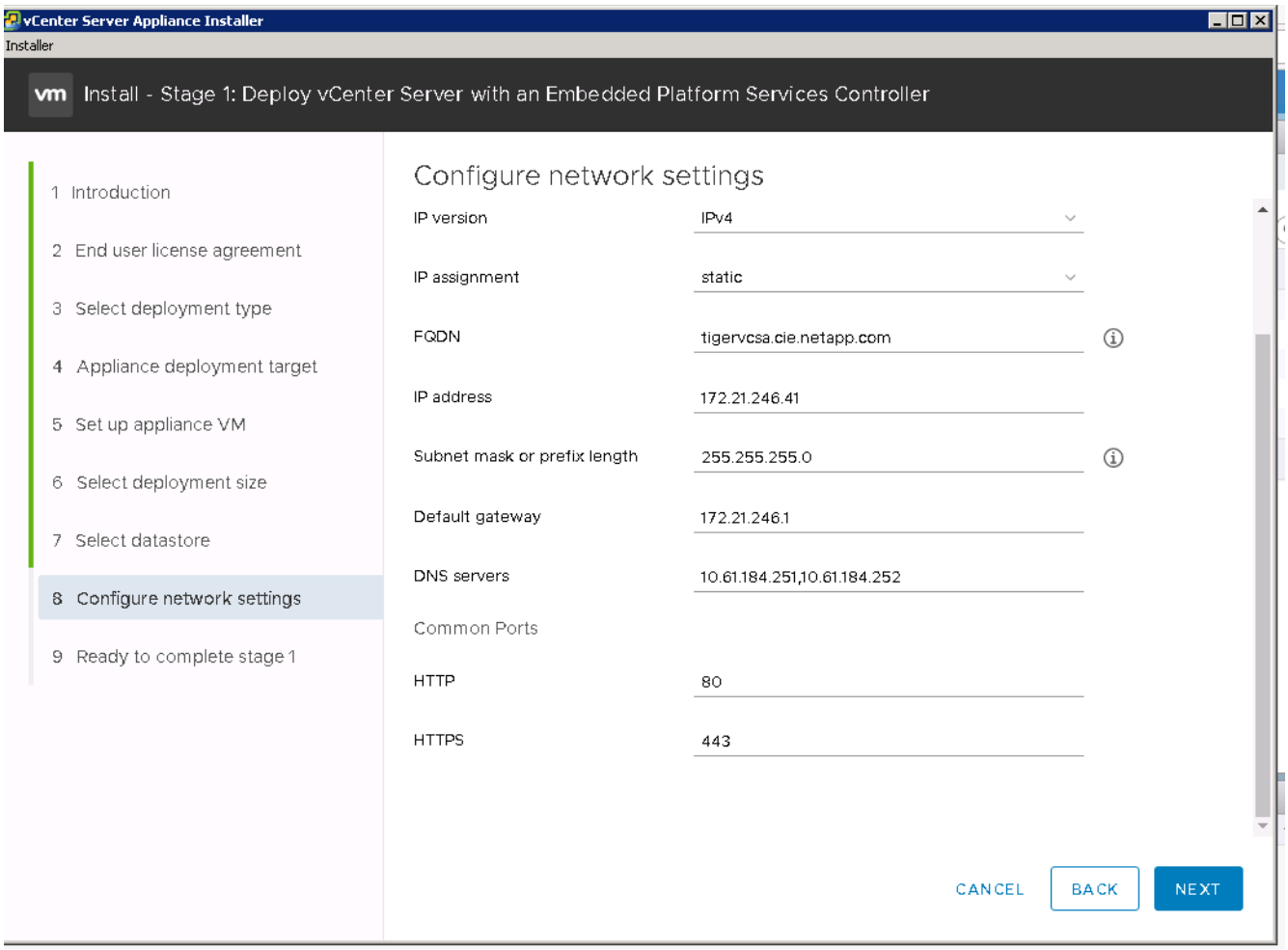
11. Selecione o tamanho de implantação que melhor se adapta ao seu ambiente. Clique em seguinte.



12. Selecione o datastore infra_datastore_1. Clique em seguinte.

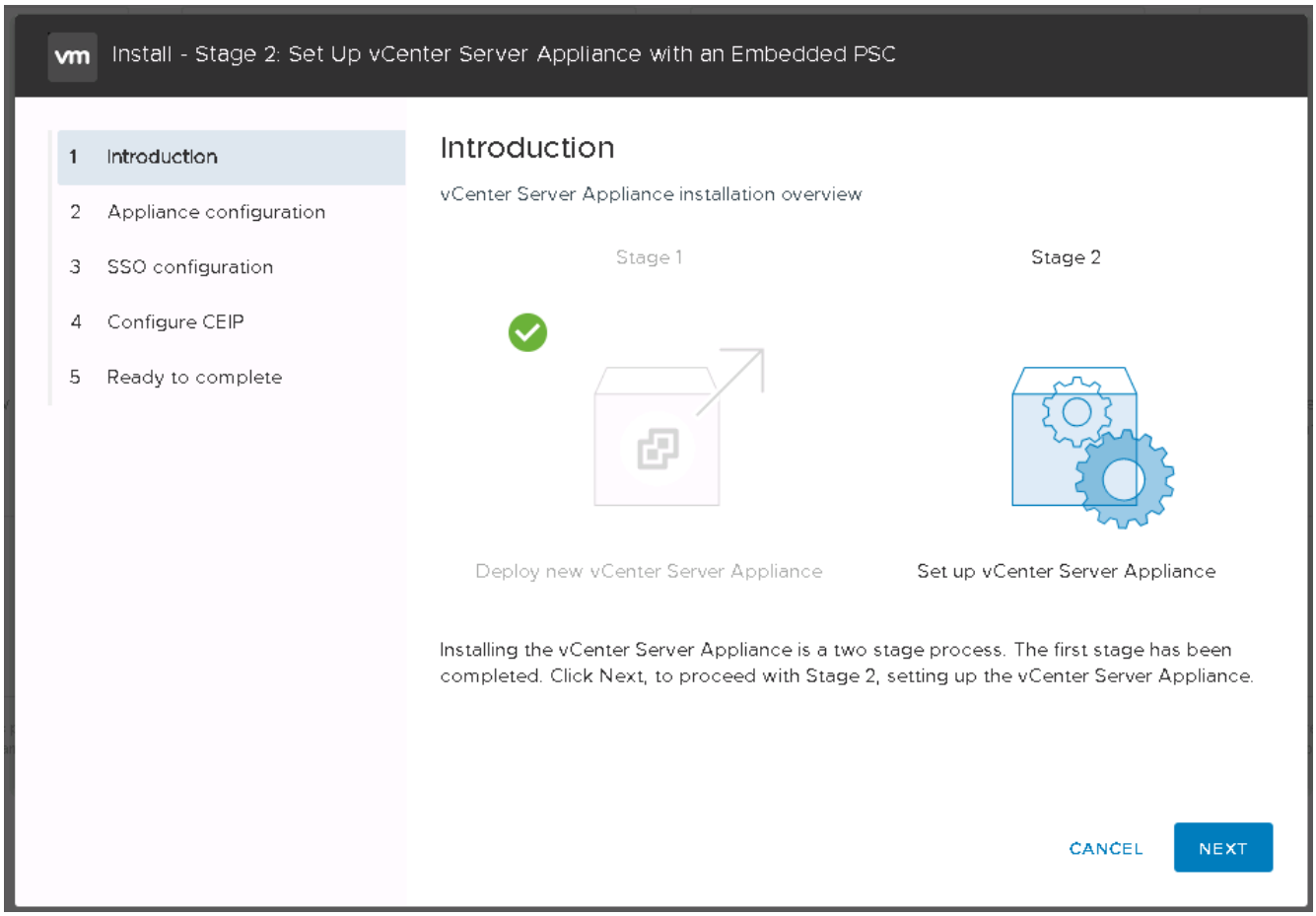


13. Introduza as seguintes informações na página Configurar definições de rede e clique em seguinte.
    a. Selecione MGMT-Network para rede.
    b. Introduza o FQDN ou IP a utilizar para o VCSA.
    c. Introduza o endereço IP a utilizar.
    d. Introduza a máscara de sub-rede a utilizar.
    e. Introduza o gateway predefinido.
    f. Introduza o servidor DNS.
14. Na página Pronto para concluir a fase 1, verifique se as configurações inseridas estão corretas. Clique em concluir.



O VCSA é instalado agora. Este processo demora vários minutos.

15. Após a conclusão da fase 1, aparece uma mensagem informando que ela foi concluída. Clique em continuar para iniciar a configuração da fase 2.
16. Na página Introdução do Estágio 2, clique em Avançar.



17. Introduza `<<var_ntp_id>>` para o endereço do servidor NTP. Pode introduzir vários endereços IP NTP.

    Se você planeja usar o vCenter Server High Availability (HA), verifique se o acesso SSH está habilitado.

18. Configure o nome de domínio SSO, a senha e o nome do site. Clique em seguinte.

    Registre esses valores para sua referência, especialmente se você se desviar do nome de domínio vSphere.local.

19. Junte-se ao Programa de experiência do Cliente da VMware, se desejado. Clique em seguinte.
20. Veja o resumo das suas definições. Clique em concluir ou use o botão voltar para editar as configurações.
21. Uma mensagem é exibida informando que você não será capaz de pausar ou parar a instalação de ser concluída depois que ela for iniciada. Clique em OK para continuar.

    A configuração do aparelho continua. Isso leva vários minutos.

    É apresentada uma mensagem a indicar que a configuração foi bem-sucedida.

    Os links que o instalador fornece para acessar o vCenter Server são clicáveis.

"Próximo: Configurar o cluster do VMware vCenter Server 6,7 e vSphere."

Configurar o cluster do VMware vCenter Server 6,7 e vSphere

Para configurar o cluster do VMware vCenter Server 6,7 e vSphere, execute as

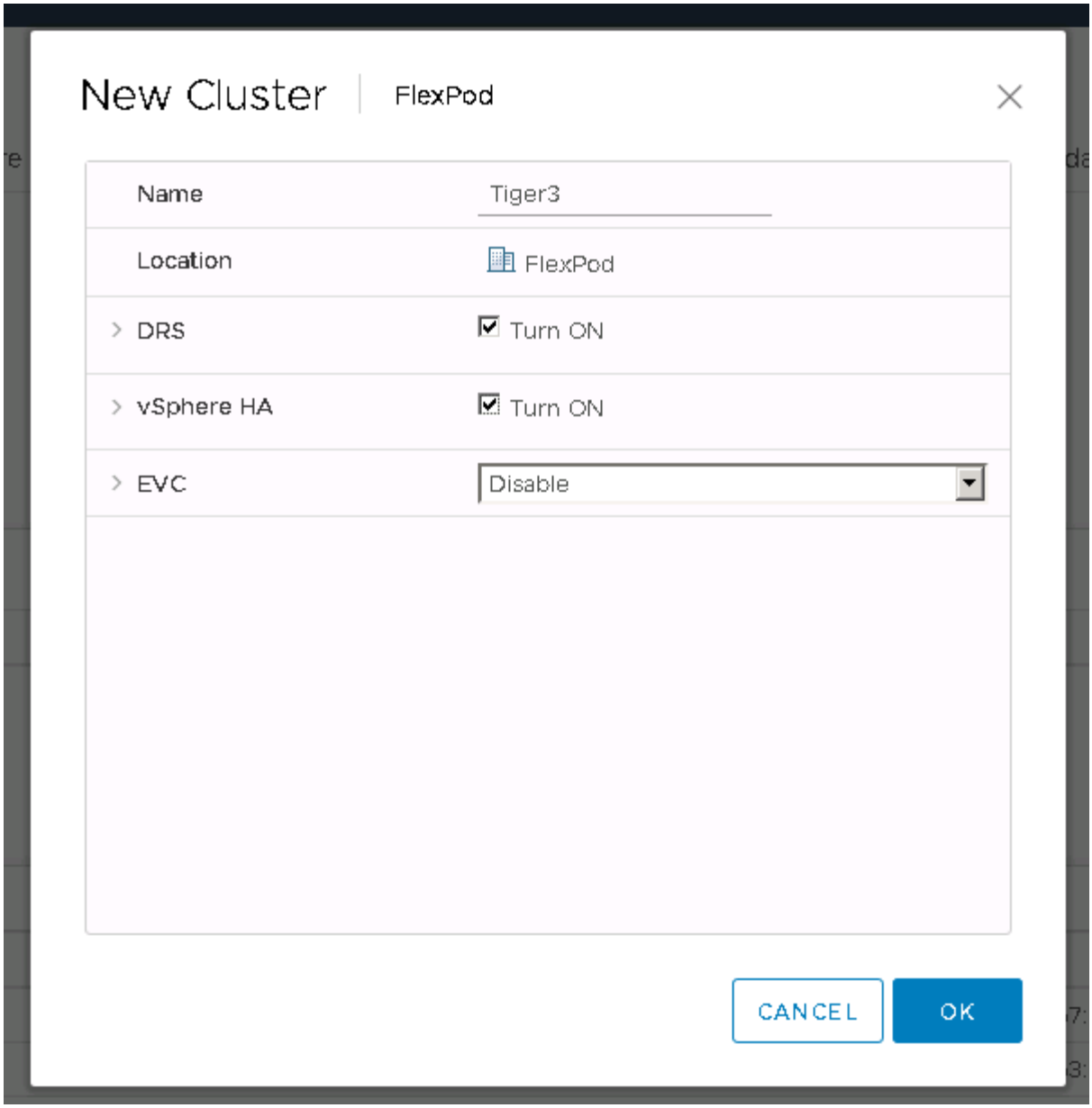
seguintes etapas:

1. Navegue até https://<<FQDN ou IP do vCenter>>/vsphere-client/.
2. Clique em Launch vSphere Client.
3. Inicie sessão com o nome de utilizador mailto:administrator.local e a palavra-passe SSO que introduziu durante o processo de configuração do VCSA.
4. Clique com o botão direito no nome do vCenter e selecione novo data center.
5. Introduza um nome para o centro de dados e clique em OK.

Crie o cluster vSphere

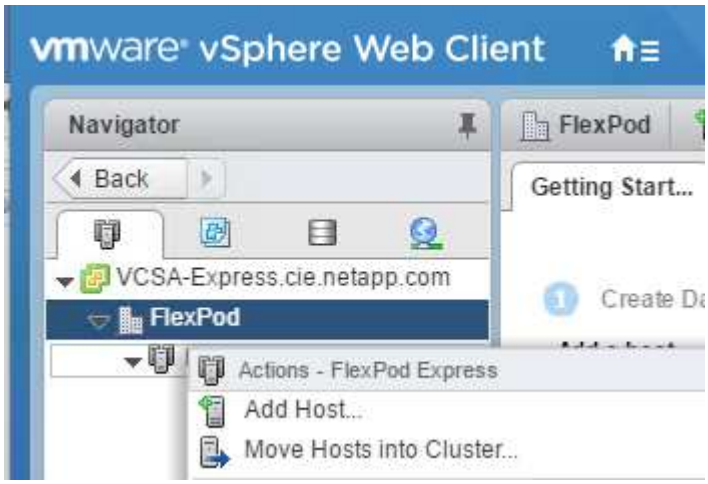
Siga as etapas a seguir para criar um cluster vSphere:

1. Clique com o botão direito do rato no data center recém-criado e selecione novo cluster.
2. Introduza um nome para o cluster.
3. Ative o DR e o vSphere HA selecionando as caixas de seleção.
4. Clique em OK.



Adicione hosts ESXi ao cluster

1. Clique com o botão direito do rato no cluster e selecione Adicionar anfitrião.



2. Para adicionar um host ESXi ao cluster, execute as seguintes etapas:
   a. Insira o IP ou FQDN do host. Clique em seguinte.
   b. Introduza o nome de utilizador e a palavra-passe raiz. Clique em seguinte.
   c. Clique em Sim para substituir o certificado do host por um certificado assinado pelo servidor de certificados VMware.
   d. Clique em Next (seguinte) na página Host Summary (Resumo do anfitrião).
   e. Clique no ícone verde para adicionar uma licença ao host vSphere.

      Este passo pode ser concluído mais tarde, se desejado.

   f. Clique em seguinte para deixar o modo de bloqueio desativado.
   g. Clique em Avançar na página de localização da VM.
   h. Reveja a página Pronto para concluir. Use o botão voltar para fazer quaisquer alterações ou selecione concluir.
3. Repita as etapas 1 e 2 para o host do Cisco UCS B. esse processo deve ser concluído para quaisquer hosts adicionais adicionados à configuração do FlexPod Express.

Configure o coredump em hosts ESXi

1. Usando SSH, conete-se ao host IP ESXi de gerenciamento, insira raiz para o nome de usuário e insira a senha raiz.
2. Execute os seguintes comandos:

```
esxcli system coredump network set -i ip_address_of_core_dump_collector
-v vmk0 -o 6500
esxcli system coredump network set --enable=true
esxcli system coredump network check
```

3. A mensagem `Verified the configured netdump server is running` aparece depois de inserir o comando final.

Esse processo deve ser concluído para quaisquer hosts adicionais adicionados ao FlexPod Express.

Conclusão

O FlexPod Express fornece uma solução simples e eficaz fornecendo um design validado que usa componentes líderes do setor. Com o dimensionamento por meio da adição de componentes adicionais, o FlexPod Express pode ser personalizado para necessidades específicas de negócios. O FlexPod Express foi projetado tendo em mente empresas de pequeno e médio porte, ROBOs e outras empresas que exigem soluções dedicadas.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes

documentos e/ou sites:

- Documentação do produto NetApp

  "http://docs.netapp.com"

- FlexPod Express com VMware vSphere 6,7 e Guia de design do NetApp AFF A220

  "https://www.netapp.com/us/media/nva-1125-design.pdf"

FlexPod Express com VMware vSphere 6.7U1 e NetApp AFF A220 com armazenamento baseado em IP de conexão direta

NVA-1131-DEPLOY: FlexPod Express com VMware vSphere 6.7U1 e NetApp AFF A220 com armazenamento baseado em IP de conexão direta

Rio de Janeiro, NetApp

As tendências do setor indicam uma grande transformação do data center em direção à infraestrutura compartilhada e à computação em nuvem. Além disso, as organizações buscam uma solução simples e eficaz para escritórios remotos e filiais, aproveitando a tecnologia com a qual elas estão familiarizadas em seu data center.

O FlexPod Express é uma arquitetura pré-projetada e de práticas recomendadas baseada no sistema de computação unificada da Cisco (Cisco UCS), na família de switches Cisco Nexus e nas tecnologias de storage da NetApp. Os componentes de um sistema FlexPod Express são como os seus homólogos do data center FlexPod, permitindo sinergias de gerenciamento em todo o ambiente de INFRAESTRUTURA DE TI em menor escala. O data center FlexPod e o FlexPod Express são plataformas ideais para virtualização, sistemas operacionais bare-metal e workloads empresariais.

O data center FlexPod e o FlexPod Express oferecem uma configuração de linha de base e têm a versatilidade a ser dimensionados e otimizados para acomodar vários casos de uso e requisitos diferentes. Os clientes de data center FlexPod existentes podem gerenciar o sistema FlexPod Express com as ferramentas às quais estão acostumados. Os novos clientes do FlexPod Express podem se adaptar facilmente ao gerenciamento do data center FlexPod à medida que seu ambiente cresce.

O FlexPod Express é uma base ideal de infraestrutura para escritórios remotos e filiais (ROBOs) e para empresas de pequeno e médio porte. Ele também é uma solução ideal para clientes que desejam fornecer infraestrutura para um workload dedicado.

O FlexPod Express fornece uma infraestrutura fácil de gerenciar, adequada para praticamente qualquer workload.

Visão geral da solução

Esta solução FlexPod Express faz parte do programa de infraestrutura convergente da FlexPod.

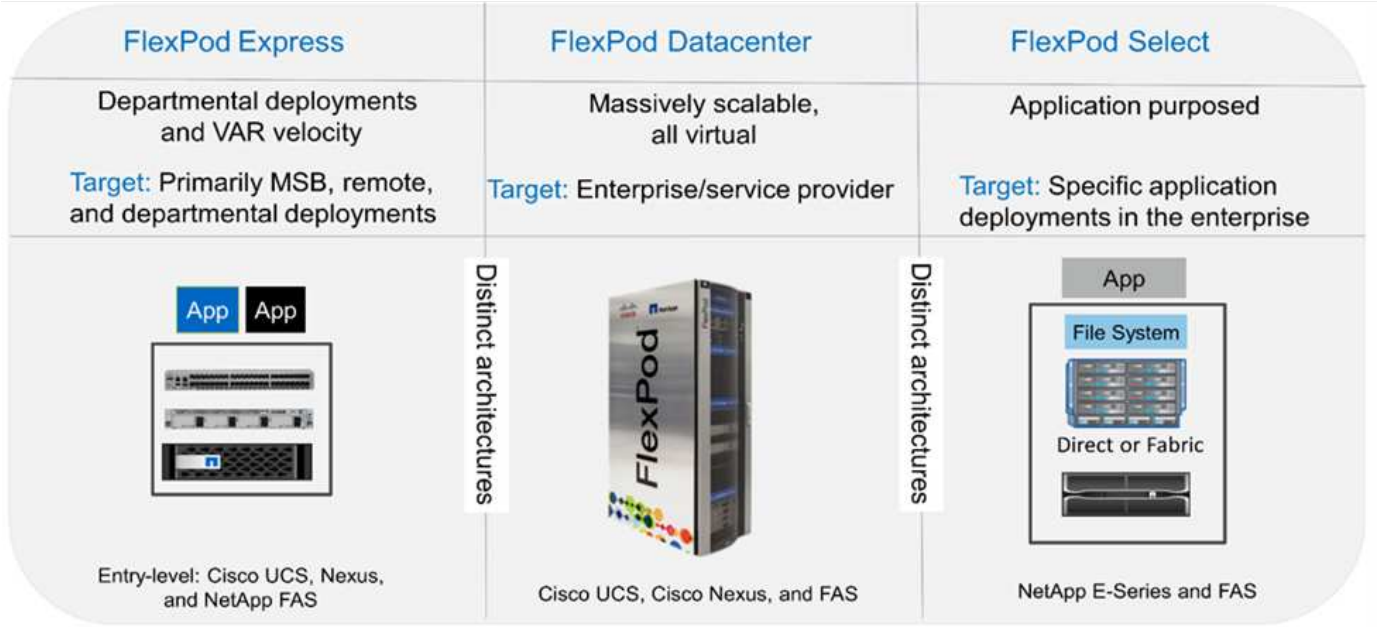
Programa de infraestrutura convergente da FlexPod

As arquiteturas de referência do FlexPod são entregues como Cisco Validated designs (CVDs) ou NetApp Verified Architectures (NVAs). Desvios com base nos requisitos do cliente de um determinado CVD ou NVA são permitidos se essas variações não criarem uma configuração não suportada.

Como descrito na figura abaixo, o programa FlexPod inclui três soluções: FlexPod Express, FlexPod Datacenter e FlexPod Select:

- **O FlexPod Express** oferece aos clientes uma solução de nível básico com tecnologias da Cisco e da NetApp.
- **O FlexPod Datacenter** oferece uma base ideal para uso geral para várias cargas de trabalho e aplicações.
- **O FlexPod Select** incorpora os melhores aspetos do datacenter FlexPod e adapta a infraestrutura a um determinado aplicativo.

A figura a seguir mostra os componentes técnicos da solução.



Programa de arquitetura verificada NetApp

O programa NVA oferece aos clientes uma arquitetura verificada para soluções NetApp. Um NVA fornece uma arquitetura de solução NetApp com as seguintes qualidades:

- É completamente testado
- É prescritiva por natureza
- Minimiza os riscos de implantação
- Acelera o time-to-market

Este guia detalha o design do FlexPod Express com armazenamento NetApp de conexão direta. As seções a seguir listam os componentes usados para o projeto desta solução.

Componentes de hardware

- NetApp AFF A220
- Cisco UCS Mini
- Cisco UCS B200 M5
- Cisco UCS VIC 1440/1480.
- Switches Cisco Nexus 3000 Series

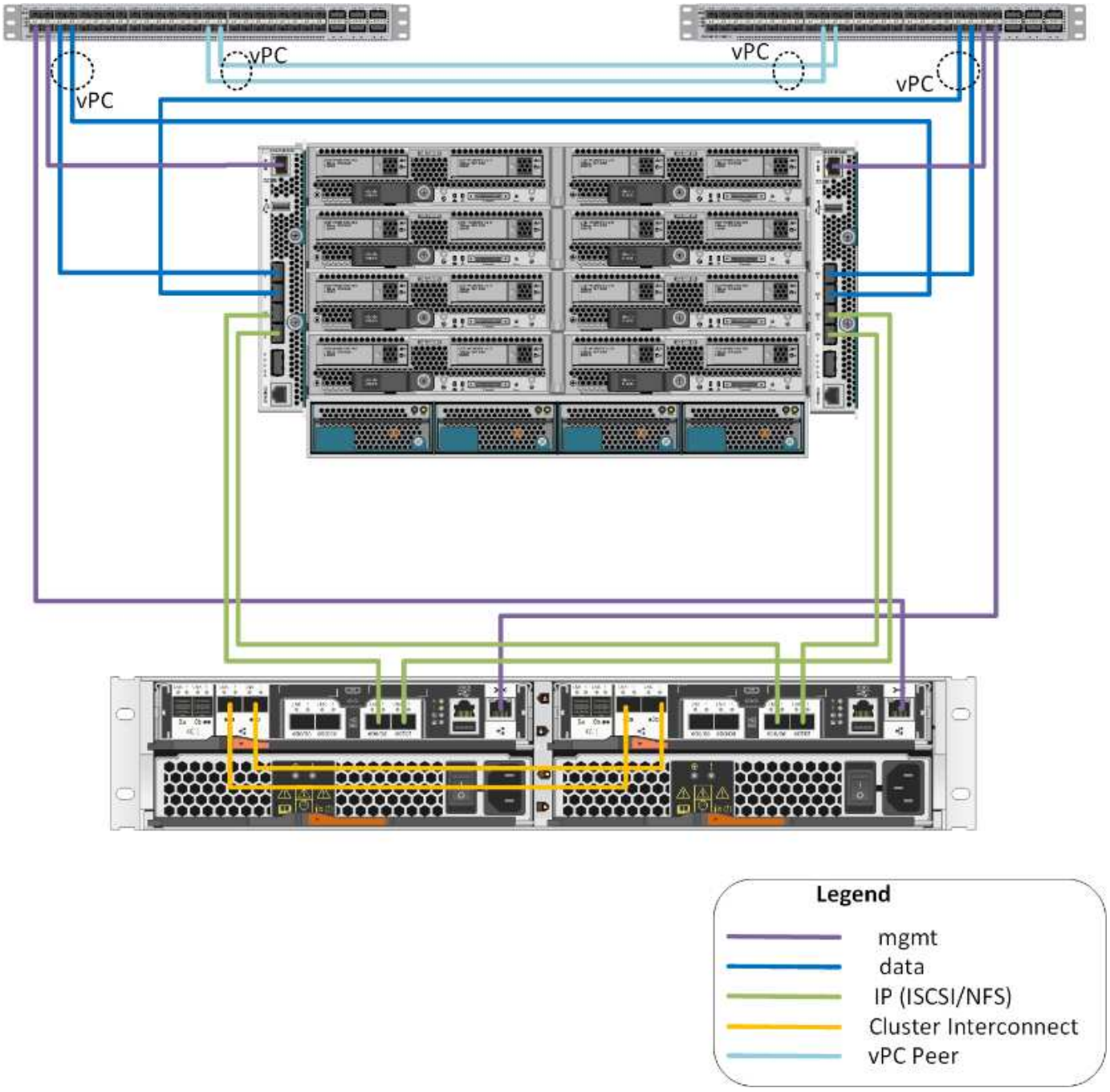
Componentes de software

- NetApp ONTAP 9. 5
- VMware vSphere 6.7U1
- Cisco UCS Manager 4,0(1b)
- Cisco NXOS firmware 7,0(3)I6(1)

Tecnologia da solução

Essa solução utiliza as tecnologias mais recentes da NetApp, Cisco e VMware. Ele apresenta o novo NetApp AFF A220 executando o ONTAP 9.5, os switches duplos Cisco Nexus 31108PCV e os servidores Cisco UCS B200 M5 que executam o VMware vSphere 6.7U1. Esta solução validada usa o armazenamento IP Direct Connect em tecnologia 10GbEG.

A figura a seguir ilustra o FlexPod Express com a arquitetura de conexão direta baseada em IP do VMware vSphere 6.7U1.



Resumo do caso de uso

A solução FlexPod Express pode ser aplicada a vários casos de uso, incluindo os seguintes:

- ROBOs
- Pequenas e médias empresas
- Ambientes que exigem uma solução dedicada e econômica

O FlexPod Express é mais adequado para workloads virtualizados e mistos.

Requisitos de tecnologia

Um sistema FlexPod Express requer uma combinação de componentes de hardware e

software. O FlexPod Express também descreve os componentes de hardware necessários para adicionar nós de hipervisor ao sistema em unidades de dois.

Requisitos de hardware

Independentemente do hypervisor escolhido, todas as configurações do FlexPod Express usam o mesmo hardware. Portanto, mesmo que os requisitos de negócios sejam alterados, qualquer hipervisor pode ser executado no mesmo hardware FlexPod Express.

A tabela a seguir lista os componentes de hardware necessários para todas as configurações do FlexPod Express.

Hardware	Quantidade
Par de HA do AFF A220	1
Servidor Cisco UCS B200 M5	2
Switch Cisco Nexus 31108PCV	2
Cartão de interface virtual (VIC) Cisco UCS 1440 para o servidor Cisco UCS B200 M5	2
Cisco UCS Mini com duas interconexões integradas de tecido UCS-Fi-M-6324	1

Requisitos de software

A tabela a seguir lista os componentes de software necessários para implementar as arquiteturas das soluções FlexPod Express.

Software	Versão	Detalhes
Gerente do Cisco UCS	4,0 mm (1b mm)	Para o Cisco UCS Fabric Interconnect FI-6324UP
Software Cisco Blade	4,0 mm (1b mm)	Para servidores Cisco UCS B200 M5
Cisco nenic driver	1.0.25.0	Para placas de interface Cisco VIC 1440
Cisco NX-os	7,0 (3)I6 (1)	Para switches Cisco Nexus 31108PCV
NetApp ONTAP	9,5	Para controladores AFF A220

A tabela a seguir lista o software necessário para todas as implementações do VMware vSphere no FlexPod Express.

Software	Versão
Dispositivo VMware vCenter Server	6.7U1
Hipervisor VMware vSphere ESXi	6.7U1

Informações sobre cabeamento expresso da FlexPod

O cabeamento de validação de referência está documentado nas tabelas a seguir.

A tabela a seguir lista as informações de cabeamento do switch Cisco Nexus 31108PCV A.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Switch Cisco Nexus 31108PCV A	Eth1/1	Controlador de storage NetApp AFF A220 A	e0M
	Eth1/2	Cisco UCS-mini FI-A	mgmt0
	Eth1/3	Cisco UCS-mini FI-A	Eth1/1
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/1
	ETH 1/13	Cisco NX 31108PCV B.	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV B.	ETH 1/14

A tabela a seguir lista as informações de cabeamento do switch Cisco Nexus 31108PCV B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Interrutor Cisco Nexus 31108PCV B	Eth1/1	Controlador de storage NetApp AFF A220 B	e0M
	Eth1/2	Cisco UCS-mini FI-B	mgmt0
	Eth1/3	Cisco UCS-mini FI-A	Eth1/2
	ETH 1/4	Cisco UCS-mini FI-B	Eth1/2
	ETH 1/13	Cisco NX 31108PCV A	ETH 1/13
	ETH 1/14	Cisco NX 31108PCV A	ETH 1/14

A tabela a seguir lista as informações de cabeamento para o controlador de armazenamento NetApp AFF A220 A..

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Controlador de storage NetApp AFF A220 A	e0a	Controlador de storage NetApp AFF A220 B	e0a
	e0b	Controlador de storage NetApp AFF A220 B	e0b
	e0e	Cisco UCS-mini FI-A	Eth1/3
	e0f	Cisco UCS-mini FI-B	Eth1/3
	e0M	Cisco NX 31108PCV A	Eth1/1

A tabela a seguir lista as informações de cabeamento do controlador de armazenamento NetApp AFF A220 B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Controlador de storage NetApp AFF A220 B	e0a	Controlador de storage NetApp AFF A220 B	e0a
	e0b	Controlador de storage NetApp AFF A220 B	e0b
	e0e	Cisco UCS-mini FI-A	Eth1/4
	e0f	Cisco UCS-mini FI-B	Eth1/4
	e0M	Cisco NX 31108PCV B.	Eth1/1

A tabela a seguir lista as informações de cabeamento do Cisco UCS Fabric Interconnect A.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Interconexão A da malha do Cisco UCS	Eth1/1	Cisco NX 31108PCV A	Eth1/3
	Eth1/2	Cisco NX 31108PCV B.	Eth1/3
	Eth1/3	Controlador de storage NetApp AFF A220 A	e0e
	Eth1/4	Controlador de storage NetApp AFF A220 B	e0e
	mgmt0	Cisco NX 31108PCV A	Eth1/2

A tabela a seguir lista as informações de cabeamento do Cisco UCS Fabric Interconnect B.

Dispositivo local	Porta local	Dispositivo remoto	Porta remota
Interconexão B da malha do Cisco UCS	Eth1/1	Cisco NX 31108PCV A	Eth1/4
	Eth1/2	Cisco NX 31108PCV B.	Eth1/4
	Eth1/3	Controlador de storage NetApp AFF A220 A	e0f
	Eth1/4	Controlador de storage NetApp AFF A220 B	e0f
	mgmt0	Cisco NX 31108PCV B.	Eth1/2

Procedimentos de implantação

Este documento fornece detalhes para configurar um sistema FlexPod Express totalmente redundante e altamente disponível. Para refletir essa redundância, os componentes que estão sendo configurados em cada etapa são referidos como componente A ou componente B. por exemplo, controlador A e controlador B identificam os dois controladores de storage NetApp que são provisionados neste documento. O switch A e o switch B identificam um par de switches Cisco Nexus. A interconexão de malha A e a interconexão de malha B são as duas interconexões de malha Nexus integradas.

Além disso, este documento descreve etapas para provisionar vários hosts Cisco UCS, que são identificados sequencialmente como servidor A, servidor B e assim por diante.

Para indicar que você deve incluir informações pertinentes ao seu ambiente em uma etapa, `<<text>>` aparece como parte da estrutura de comando. Veja o exemplo a seguir para o `vlan create` comando:

```
Controller01>vlan create vif0 <<mgmt_vlan_id>>
```

Este documento permite configurar totalmente o ambiente do FlexPod Express. Nesse processo, várias etapas exigem que você insira convenções de nomenclatura específicas do cliente, endereços IP e esquemas de rede local virtual (VLAN). A tabela abaixo descreve as VLANs necessárias para implantação, conforme descrito neste guia. Esta tabela pode ser concluída com base nas variáveis específicas do site e usada para implementar as etapas de configuração do documento.

Se você usar VLANs separadas de gerenciamento dentro e fora da banda, será necessário criar uma rota de camada 3 entre elas. Para essa validação, uma VLAN de gerenciamento comum foi usada.

Nome da VLAN	Finalidade do VLAN	ID usada na validação deste documento
VLAN de gerenciamento	VLAN para interfaces de gerenciamento	18
VLAN nativo	VLAN à qual os quadros não marcados são atribuídos	2
VLAN NFS	VLAN para tráfego NFS	104
VLAN do VMware vMotion	VLAN designada para o movimento de máquinas virtuais (VMs) de um host físico para outro	103
VLAN de tráfego de VM	VLAN para tráfego de aplicação de VM	102
ISCSI-A-VLAN	VLAN para tráfego iSCSI na malha A	124
ISCSI-B-VLAN	VLAN para tráfego iSCSI na malha B	125

Os números de VLAN são necessários durante toda a configuração do FlexPod Express. As VLANs são referidas como `<<var_xxxx_vlan>>`, onde `xxxx` é a finalidade da VLAN (como iSCSI-A).

A tabela a seguir lista as VMs VMware criadas.

Descrição VM	Nome do host
VMware vCenter Server	Seahawks-vcsa.cie.NetApp.com

Procedimento de implantação do Cisco Nexus 31108PCV

Esta seção detalha a configuração do switch Cisco Nexus 31308PCV usada em um ambiente FlexPod

Express.

Configuração inicial do switch Cisco Nexus 31108PCV

Este procedimento descreve como configurar os switches Cisco Nexus para uso em um ambiente FlexPod Express básico.

> Este procedimento pressupõe que você está usando um Cisco Nexus 31108PCV executando o software NX-os versão 7,0(3)I6(1).

1. Após a inicialização inicial e a conexão à porta do console do switch, a configuração do Cisco NX-os é iniciada automaticamente. Esta configuração inicial aborda as configurações básicas, como o nome do switch, a configuração da interface mgmt0 e a configuração do Secure Shell (SSH).
2. A rede de gerenciamento FlexPod Express pode ser configurada de várias maneiras. As interfaces mgmt0 nos switches 31108PCV podem ser conetadas a uma rede de gerenciamento existente, ou as interfaces mgmt0 dos switches 31108PCV podem ser conetadas em uma configuração back-to-back. No entanto, este link não pode ser usado para acesso de gerenciamento externo, como tráfego SSH.

   Neste guia de implantação, os switches FlexPod Express Cisco Nexus 31108PCV são conetados a uma rede de gerenciamento existente.
3. Para configurar os switches Cisco Nexus 31108PCV, ligue o switch e siga as instruções na tela, conforme ilustrado aqui para a configuração inicial de ambos os switches, substituindo os valores apropriados para as informações específicas do switch.

```
This setup utility will guide you through the basic configuration of the
system. Setup configures only enough connectivity for management of the
system.
```

```
*Note: setup is mainly used for configuring the system initially, when
no configuration is present. So setup always assumes system defaults and
not the current system configuration values.
Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip
the remaining dialogs.
Would you like to enter the basic configuration dialog (yes/no): y
Do you want to enforce secure password standard (yes/no) [y]: y
Create another login account (yes/no) [n]: n
Configure read-only SNMP community string (yes/no) [n]: n
Configure read-write SNMP community string (yes/no) [n]: n
Enter the switch name : 31108PCV-A
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y
Mgmt0 IPv4 address : <<var_switch_mgmt_ip>>
Mgmt0 IPv4 netmask : <<var_switch_mgmt_netmask>>
Configure the default gateway? (yes/no) [y]: y
IPv4 address of the default gateway : <<var_switch_mgmt_gateway>>
Configure advanced IP options? (yes/no) [n]: n
Enable the telnet service? (yes/no) [n]: n
Enable the ssh service? (yes/no) [y]: y
Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
Number of rsa key bits <1024-2048> [1024]: <enter>
Configure the ntp server? (yes/no) [n]: y
NTP server IPv4 address : <<var_ntp_ip>>
Configure default interface layer (L3/L2) [L2]: <enter>
Configure default switchport interface state (shut/noshut) [noshut]:
<enter>
Configure CoPP system profile (strict/moderate/lenient/dense) [strict]:
<enter>
```

4. É apresentado um resumo da sua configuração e é-lhe perguntado se pretende editar a configuração. Se a configuração estiver correta, introduza `n`.

```
Would you like to edit the configuration? (yes/no) [n]: no
```

5. Então, você será perguntado se deseja usar essa configuração e salvá-la. Em caso afirmativo, introduza `y`.

```
Use this configuration and save it? (yes/no) [y]: Enter
```

6. Repita os passos 1 a 5 para o switch Cisco B.

Ativar funcionalidades avançadas

Certos recursos avançados devem ser ativados no Cisco NX-os para fornecer opções de configuração adicionais.

1. Para habilitar os recursos apropriados no switch A e no switch B do Cisco Nexus, entre no modo de configuração usando o comando `(config t)` e execute os seguintes comandos:

```
feature interface-vlan
feature lacp
feature vpc
```

> O hash padrão de balanceamento de carga do canal de porta usa os endereços IP de origem e destino para determinar o algoritmo de balanceamento de carga entre as interfaces no canal de porta. Você pode obter uma melhor distribuição entre os membros do canal de porta fornecendo mais entradas para o algoritmo hash além dos endereços IP de origem e destino. Pela mesma razão, o NetApp recomenda fortemente adicionar as portas TCP de origem e destino ao algoritmo de hash.

2. No modo de configuração `(config t)` , execute os seguintes comandos para definir a configuração de balanceamento de carga do canal de porta global no switch A e no switch B do Cisco Nexus:

```
port-channel load-balance src-dst ip-l4port
```

Execute a configuração global de spanning-tree

A plataforma Cisco Nexus usa um novo recurso de proteção chamado bridge Assurance. O Bridge Assurance ajuda a proteger contra uma ligação unidirecional ou outra falha de software com um dispositivo que continua a encaminhar o tráfego de dados quando não está mais a executar o algoritmo spanning-tree. As portas podem ser colocadas em um dos vários estados, incluindo rede ou borda, dependendo da plataforma.

A NetApp recomenda a configuração da garantia de ponte para que todas as portas sejam consideradas como portas de rede por padrão. Essa configuração força o administrador de rede a revisar a configuração de cada porta. Ele também revela os erros de configuração mais comuns, como portas de borda não identificadas ou um vizinho que não tenha o recurso de garantia de ponte ativado. Além disso, é mais seguro ter o bloco de árvore de expansão muitas portas em vez de muito poucas, o que permite que o estado de porta padrão aumente a estabilidade geral da rede.

Preste muita atenção ao estado spanning-tree ao adicionar servidores, armazenamento e switches uplink, especialmente se eles não suportarem a garantia de bridge. Nesses casos, talvez seja necessário alterar o tipo de porta para tornar as portas ativas.

A proteção da Unidade de dados do Protocolo de Ponte (BPDU) é ativada por padrão nas portas de borda como outra camada de proteção. Para evitar loops na rede, esse recurso desliga a porta se BPDUs de outro switch forem vistos nessa interface.

No modo de configuração (`config t`), execute os seguintes comandos para configurar as opções de spanning-tree padrão, incluindo o tipo de porta padrão e a proteção BPDU, no switch A do Cisco Nexus e no switch B:

```
spanning-tree port type network default
spanning-tree port type edge bpduguard default
```

Definir VLANs

Antes que portas individuais com VLANs diferentes sejam configuradas, as VLANs de camada 2 devem ser definidas no switch. Também é uma boa prática nomear as VLANs para facilitar a solução de problemas no futuro.

No modo de configuração (`config t`), execute os seguintes comandos para definir e descrever as VLANs de camada 2 no switch A e no switch B do Cisco Nexus:

```
vlan <<nfs_vlan_id>>
  name NFS-VLAN
vlan <<iSCSI_A_vlan_id>>
  name iSCSI-A-VLAN
vlan <<iSCSI_B_vlan_id>>
  name iSCSI-B-VLAN
vlan <<vmotion_vlan_id>>
  name vMotion-VLAN
vlan <<vmtraffic_vlan_id>>
  name VM-Traffic-VLAN
vlan <<mgmt_vlan_id>>
  name MGMT-VLAN
vlan <<native_vlan_id>>
  name NATIVE-VLAN
exit
```

Configurar descrições de portas de acesso e gerenciamento

Como acontece com a atribuição de nomes às VLANs de camada 2, as descrições de configuração para todas as interfaces podem ajudar no provisionamento e na solução de problemas.

A partir do modo de configuração (`config t`) em cada um dos switches, insira as seguintes descrições de porta para a configuração grande do FlexPod Express:

Switch Cisco Nexus A

```
int eth1/1
  description AFF A220-A e0M
int eth1/2
  description Cisco UCS FI-A mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/1
int eth1/4
  description Cisco UCS FI-B eth1/1
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Interrutor B do Cisco Nexus

```
int eth1/1
  description AFF A220-B e0M
int eth1/2
  description Cisco UCS FI-B mgmt0
int eth1/3
  description Cisco UCS FI-A eth1/2
int eth1/4
  description Cisco UCS FI-B eth1/2
int eth1/13
  description vPC peer-link 31108PVC-B 1/13
int eth1/14
  description vPC peer-link 31108PVC-B 1/14
```

Configurar interfaces de gerenciamento de storage e servidor

As interfaces de gerenciamento para o servidor e o storage normalmente usam apenas uma única VLAN. Portanto, configure as portas da interface de gerenciamento como portas de acesso. Defina a VLAN de gerenciamento para cada switch e altere o tipo de porta spanning-tree para Edge.

No modo de configuração (`config t`), execute os seguintes comandos para configurar as configurações de porta para as interfaces de gerenciamento dos servidores e do storage:

Switch Cisco Nexus A

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Interrutor B do Cisco Nexus

```
int eth1/1-2
  switchport mode access
  switchport access vlan <<mgmt_vlan>>
  spanning-tree port type edge
  speed 1000
exit
```

Adicionar interface de distribuição NTP

Switch Cisco Nexus A

No modo de configuração global, execute os seguintes comandos.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch-a-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-b-ntp-ip> use-vrf default
```

Interrutor B do Cisco Nexus

No modo de configuração global, execute os seguintes comandos.

```
interface Vlan<ib-mgmt-vlan-id>
ip address <switch- b-ntp-ip>/<ib-mgmt-vlan-netmask-length>
no shutdown
exitntp peer <switch-a-ntp-ip> use-vrf default
```

Execute a configuração global do canal de porta virtual

Um canal de porta virtual (VPC) permite que os links fisicamente conetados a dois switches Cisco Nexus diferentes apareçam como um canal de porta única para um terceiro dispositivo. O terceiro dispositivo pode ser um switch, servidor ou qualquer outro dispositivo de rede. Uma VPC pode fornecer multipathing de camada 2, o que permite criar redundância aumentando a largura de banda, habilitando vários caminhos paralelos entre nós e o tráfego de balanceamento de carga onde existem caminhos alternativos.

Uma VPC oferece os seguintes benefícios:

- Ativar um único dispositivo para usar um canal de porta em dois dispositivos upstream
- Eliminação de portas bloqueadas de protocolo spanning-tree
- Fornecendo uma topologia sem loop
- Usando toda a largura de banda de uplink disponível
- Fornecendo convergência rápida se o link ou um dispositivo falhar
- Fornecer resiliência no nível de link
- Ajudando a fornecer alta disponibilidade

O recurso VPC requer alguma configuração inicial entre os dois switches Cisco Nexus para funcionar corretamente. Se você usar a configuração back-to-back mgmt0, use os endereços definidos nas interfaces e verifique se eles podem se comunicar usando o comando ping `<<switch_A/B_mgmt0_ip_addr>>vrf` Management.

No modo de configuração (`config t`), execute os seguintes comandos para configurar a configuração global da VPC para ambos os switches:

Switch Cisco Nexus A

```
vpc domain 1
 role priority 10
peer-keepalive destination <<switch_B_mgmt0_ip_addr>> source
<<switch_A_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10description vPC peer-link
switchport
switchport mode trunkswitchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
  channel-group 14 mode active
copy run start
```

Interrutor B do Cisco Nexus

```
vpc domain 1
peer-switch
role priority 20
peer-keepalive destination <<switch_A_mgmt0_ip_addr>> source
<<switch_B_mgmt0_ip_addr>> vrf management
  peer-gateway
  auto-recovery
  ip arp synchronize
  int eth1/13-14
  channel-group 10 mode active
int Po10
description vPC peer-link
switchport
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<nfs_vlan_id>>,<<vmotion_vlan_id>>,
<<vmtraffic_vlan_id>>, <<mgmt_vlan>>, <<iSCSI_A_vlan_id>>,
<<iSCSI_B_vlan_id>> spanning-tree port type network
vpc peer-link
no shut
exit
int Po13
description vPC ucs-FI-A
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 13
no shut
exit
int eth1/3
  channel-group 13 mode active
int Po14
description vPC ucs-FI-B
switchport mode trunk
switchport trunk native vlan <<native_vlan_id>>
switchport trunk allowed vlan <<vmotion_vlan_id>>, <<vmtraffic_vlan_id>>,
<<mgmt_vlan>> spanning-tree port type network
mtu 9216
vpc 14
no shut
exit
int eth1/4
```

```
  channel-group 14 mode active
copy run start
```

Na validação desta solução, foi utilizada uma unidade máxima de transmissão (MTU) de 9000. No entanto, com base nos requisitos do aplicativo, você pode configurar um valor apropriado de MTU. É importante definir o mesmo valor MTU na solução FlexPod. Configurações incorretas de MTU entre componentes resultam em pacotes sendo descartados.

Uplink em infra-estrutura de rede existente

Dependendo da infraestrutura de rede disponível, vários métodos e recursos podem ser usados para uplink o ambiente FlexPod. Se um ambiente Cisco Nexus existente estiver presente, a NetApp recomenda o uso de VPCs para uplink os switches Cisco Nexus 31108PVC incluídos no ambiente FlexPod na infraestrutura. Os uplinks podem ser 10GbE uplinks para uma solução de infraestrutura 10GbE ou 1GbE para uma solução de infraestrutura 1GbE, se necessário. Os procedimentos descritos anteriormente podem ser usados para criar uma VPC uplink no ambiente existente. Certifique-se de executar o copy run start para salvar a configuração em cada switch depois que a configuração for concluída.

Procedimento de implantação de storage do NetApp (parte 1)

Esta seção descreve o procedimento de implantação de storage do NetApp AFF.

Instalação do controlador de armazenamento NetApp série AFF2xx

NetApp Hardware Universe

O "NetApp Hardware Universe" aplicativo (HWU) fornece componentes de hardware e software suportados para qualquer versão específica do ONTAP. Ele fornece informações de configuração para todos os dispositivos de storage NetApp atualmente compatíveis com o software ONTAP. Ele também fornece uma tabela de compatibilidades de componentes.

Confirme se os componentes de hardware e software que você gostaria de usar são suportados com a versão do ONTAP que você pretende instalar:

1. Acesse o "HWU" aplicativo para exibir os guias de configuração do sistema. Selecione a guia comparar sistemas de armazenamento para exibir a compatibilidade entre diferentes versões do software ONTAP e os dispositivos de armazenamento NetApp com as especificações desejadas.
2. Como alternativa, para comparar componentes por dispositivo de armazenamento, clique em comparar sistemas de armazenamento.

Pré-requisitos da Série Controller AFF2XX
Para Planejar a localização física dos sistemas de armazenamento, consulte as seções a seguir: Requisitos elétricos cabos de alimentação suportados portas e cabos integrados

Controladores de storage

Siga os procedimentos de instalação física dos controladores no "Documentação do AFF A220".

NetApp ONTAP 9,5

Folha de cálculo de configuração

Antes de executar o script de configuração, conclua a Planilha de configuração no manual do produto. A folha de cálculo de configuração está disponível na "Guia de configuração do software ONTAP 9.5" (disponível na "Centro de Documentação do ONTAP 9"). A tabela abaixo ilustra as informações de instalação e configuração do ONTAP 9.5.

Este sistema é configurado em uma configuração de cluster sem switch de dois nós.

Detalhe do cluster	Valor Detalhe do cluster
Nó de cluster Um endereço IP	"Cliente <var_nodeA_mgmt_ip>>
Cluster node Uma máscara de rede	"Cliente <var_nodeA_mgmt_mask>>
Nó de cluster A gateway	"Cliente <var_nodeA_mgmt_gateway>>
Nome do nó do cluster	"Cliente <var_nodeA>>
Endereço IP do nó B do cluster	"Cliente <var_nodeB_mgmt_ip>>
Nó de cluster B netmask	"Cliente <var_nodeB_mgmt_mask>>
Gateway do nó B do cluster	"Cliente <var_nodeB_mgmt_gateway>>
Nome B do nó do cluster	"Cliente <var_nodeB>>
URL do ONTAP 9.5	"cliente <var_url_boot_software>>
Nome do cluster	"cliente <var_clustername>>
Endereço IP de gerenciamento de cluster	"cliente <var_clustermgmt_ip>>
Gateway do cluster B.	"cliente <var_clustermgmt_gateway>>
Cluster B netmask	"cliente <var_clustermgmt_mask>>
Nome de domínio	"cliente <var_domain_name>>
IP do servidor DNS (pode introduzir mais de um)	"cliente <var_dns_server_ip>>
SERVIDOR NTP UM IP	o switch-a-ntp-ip >>
IP DO SERVIDOR NTP B.	o switch-b-ntp-ip >>

Configure o nó A

Para configurar o nó A, execute as seguintes etapas:

1. Conete-se à porta do console do sistema de armazenamento. Você deve ver um prompt Loader-A. No entanto, se o sistema de armazenamento estiver em um loop de reinicialização, pressione Ctrl- C para sair do loop autoboot quando você vir esta mensagem:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Permita que o sistema inicialize.

```
autoboot
```

3. Pressione Ctrl- C para entrar no menu Boot (Inicialização).

   Se ONTAP 9. 5 não é a versão do software que está sendo inicializada, continue com as etapas a seguir para instalar o novo software. Se ONTAP 9. 5 é a versão que está sendo inicializada, selecione a opção 8 e y para reinicializar o nó. Em seguida, continue com o passo 14.

4. Para instalar um novo software, selecione a opção `7`.
5. Introduza `y` para efetuar uma atualização.
6. `e0M`Selecione para a porta de rede que pretende utilizar para a transferência.
7. Introduza `y` para reiniciar agora.
8. Introduza o endereço IP, a máscara de rede e o gateway predefinido para e0M nos respetivos locais.

```
<<var_nodeA_mgmt_ip>> <<var_nodeA_mgmt_mask>> <<var_nodeA_mgmt_gateway>>
```

9. Introduza a URL onde o software pode ser encontrado.

   Este servidor Web deve ser pingável.

10. Pressione Enter para o nome de usuário, indicando nenhum nome de usuário.
11. Introduza `y` para definir o software recém-instalado como o padrão a ser usado para reinicializações subsequentes.
12. Digite `y` para reinicializar o nó.

    Ao instalar um novo software, o sistema pode executar atualizações de firmware para o BIOS e placas adaptadoras, causando reinicializações e possíveis paradas no prompt do Loader-A. Se estas acões ocorrerem, o sistema poderá desviar-se deste procedimento.

13. Pressione Ctrl- C para entrar no menu Boot (Inicialização).
14. Selecione a opção `4` para Configuração limpa e Inicializar todos os discos.
15. Digite `y` zero discos, redefina a configuração e instale um novo sistema de arquivos.
16. Introduza `y` para apagar todos os dados nos discos.

    A inicialização e a criação do agregado raiz podem levar 90 minutos ou mais para ser concluída, dependendo do número e do tipo de discos anexados. Quando a inicialização estiver concluída, o sistema de armazenamento reinicializa. Note que os SSDs demoram consideravelmente menos tempo para inicializar. Você pode continuar com a configuração do nó B enquanto os discos do nó A estão zerando.

17. Enquanto o nó A estiver inicializando, comece a configurar o nó B.

Configure o nó B

Para configurar o nó B, execute as seguintes etapas:

1. Conete-se à porta do console do sistema de armazenamento. Você deve ver um prompt Loader-A. No entanto, se o sistema de armazenamento estiver em um loop de reinicialização, pressione Ctrl-C para sair do loop autoboot quando você vir esta mensagem:

```
Starting AUTOBOOT press Ctrl-C to abort...
```

2. Pressione Ctrl-C para entrar no menu Boot (Inicialização).

```
autoboot
```

3. Pressione Ctrl-C quando solicitado.

   Se ONTAP 9. 5 não é a versão do software que está sendo inicializada, continue com as etapas a seguir para instalar o novo software. Se o ONTAP 9.4 for a versão que está sendo inicializada, selecione a opção 8 e y para reinicializar o nó. Em seguida, continue com o passo 14.

4. Para instalar um novo software, selecione a opção 7.
5. Introduza `y` para efetuar uma atualização.
6. `e0M`Selecione para a porta de rede que pretende utilizar para a transferência.
7. Introduza `y` para reiniciar agora.
8. Introduza o endereço IP, a máscara de rede e o gateway predefinido para e0M nos respetivos locais.

```
<<var_nodeB_mgmt_ip>> <<var_nodeB_mgmt_ip>><<var_nodeB_mgmt_gateway>>
```

9. Introduza a URL onde o software pode ser encontrado.

   Este servidor Web deve ser pingável.

```
<<var_url_boot_software>>
```

10. Pressione Enter para o nome de usuário, indicando nenhum nome de usuário
11. Introduza `y` para definir o software recém-instalado como o padrão a ser usado para reinicializações subsequentes.
12. Digite `y` para reinicializar o nó.

    Ao instalar um novo software, o sistema pode executar atualizações de firmware para o BIOS e placas adaptadoras, causando reinicializações e possíveis paradas no prompt do Loader-A. Se estas acões ocorrerem, o sistema poderá desviar-se deste procedimento.

13. Pressione Ctrl-C para entrar no menu Boot (Inicialização).
14. Selecione a opção 4 para Configuração limpa e Inicializar todos os discos.
15. Digite `y` zero discos, redefina a configuração e instale um novo sistema de arquivos.

16. Introduza `y` para apagar todos os dados nos discos.

    A inicialização e a criação do agregado raiz podem levar 90 minutos ou mais para ser concluída, dependendo do número e do tipo de discos anexados. Quando a inicialização estiver concluída, o sistema de armazenamento reinicializa. Note que os SSDs demoram consideravelmente menos tempo para inicializar.

Continuação do nó Uma configuração e configuração de cluster

A partir de um programa de porta de console conetado à porta de console do controlador de storage A (nó A), execute o script de configuração do nó. Este script aparece quando o ONTAP 9.5 é inicializado no nó pela primeira vez.

O procedimento de configuração do nó e do cluster mudou ligeiramente no ONTAP 9.5. O assistente de configuração do cluster agora é usado para configurar o primeiro nó em um cluster e o System Manager é usado para configurar o cluster.

1. Siga as instruções para configurar o nó A..

```
Welcome to the cluster setup wizard.
You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
     Any changes you made before quitting will be saved.
You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value.
This system will send event messages and periodic reports to NetApp
Technical Support. To disable this feature, enter
autosupport modify -support disable
within 24 hours.
Enabling AutoSupport can significantly speed problem determination and
resolution should a problem occur on your system.
For further information on AutoSupport, see:
http://support.netapp.com/autosupport/
Type yes to confirm and continue {yes}: yes
Enter the node management interface port [e0M]:
Enter the node management interface IP address: <<var_nodeA_mgmt_ip>>
Enter the node management interface netmask: <<var_nodeA_mgmt_mask>>
Enter the node management interface default gateway:
<<var_nodeA_mgmt_gateway>>
A node management interface on port e0M with IP address
<<var_nodeA_mgmt_ip>> has been created.
Use your web browser to complete cluster setup by accessing
https://<<var_nodeA_mgmt_ip>>
Otherwise, press Enter to complete cluster setup using the command line
interface:
```

2. Navegue até o endereço IP da interface de gerenciamento do nó.

> A configuração do cluster também pode ser realizada usando a CLI. Este documento descreve a configuração do cluster usando a configuração guiada pelo Gerenciador de sistema do NetApp.

3. Clique em Configuração Guiada para configurar o cluster.
4. Introduza `<<var_clustername>>` o nome do cluster e `<<var_nodeA>>` e `<<var_nodeB>>` para cada um dos nós que está a configurar. Introduza a palavra-passe que pretende utilizar para o sistema de armazenamento. Selecione cluster sem switch para o tipo de cluster. Introduza a licença base do cluster.
5. Você também pode inserir licenças de recursos para Cluster, NFS e iSCSI.
6. Você verá uma mensagem de status informando que o cluster está sendo criado. Esta mensagem de estado passa por vários Estados. Este processo demora vários minutos.
7. Configure a rede.
   a. Desmarque a opção IP Address Range (intervalo de endereços IP).
   b. Introduza `<<var_clustermgmt_ip>>` no campo Endereço IP de gestão de clusters, `<<var_clustermgmt_mask>>` no campo Máscara de rede e `<<var_clustermgmt_gateway>>` no campo Gateway. Utilize o seletor … no campo porta para selecionar e0M do nó A.
   c. O IP de gerenciamento do Nó para o nó A já está preenchido. Introduza `<<var_nodeA_mgmt_ip>>` para o nó B.
   d. Introduza `<<var_domain_name>>` no campo DNS Domain Name (Nome de domínio DNS). Introduza `<<var_dns_server_ip>>` no campo Endereço IP do servidor DNS.

      Você pode inserir vários endereços IP do servidor DNS.

   e. Introduza `<<switch-a-ntp-ip>>` no campo servidor NTP principal.

      Você também pode inserir um servidor NTP alternativo como `<<switch- b-ntp-ip>>`.

8. Configure as informações de suporte.
   a. Se o seu ambiente exigir um proxy para acessar o AutoSupport, insira o URL no URL do proxy.
   b. Insira o host de e-mail SMTP e o endereço de e-mail para notificações de eventos.

      Você deve, no mínimo, configurar o método de notificação de evento antes de prosseguir. Você pode selecionar qualquer um dos métodos.

9. Quando for indicado que a configuração do cluster foi concluída, clique em Gerenciar seu cluster para configurar o armazenamento.

Continuação da configuração do cluster de armazenamento

Após a configuração dos nós de storage e do cluster base, você pode continuar com a configuração do cluster de storage.

Zero todos os discos sobressalentes

Para zerar todos os discos sobressalentes no cluster, execute o seguinte comando:

```
disk zerospares
```

Defina a personalidade de UTA2 portas a bordo

1. Verifique o modo atual e o tipo atual das portas executando o `ucadmin show` comando.

```
AFFA220-Clus::> ucadmin show
                     Current  Current    Pending  Pending    Admin
Node          Adapter  Mode     Type       Mode     Type       Status
------------  -------  -------  ---------  -------  ---------
-----------
AFFA220-Clus-01
              0c       cna      target     -        -          offline
AFFA220-Clus-01
              0d       cna      target     -        -          offline
AFFA220-Clus-01
              0e       cna      target     -        -          offline
AFFA220-Clus-01
              0f       cna      target     -        -          offline
AFFA220-Clus-02
              0c       cna      target     -        -          offline
AFFA220-Clus-02
              0d       cna      target     -        -          offline
AFFA220-Clus-02
              0e       cna      target     -        -          offline
AFFA220-Clus-02
              0f       cna      target     -        -          offline
8 entries were displayed.
```

2. Verifique se o modo atual das portas que estão em uso é `cna` e se o tipo atual está definido como `target`. Caso contrário, altere a personalidade da porta executando o seguinte comando:

```
ucadmin modify -node <home node of the port> -adapter <port name> -mode
cna -type target
```

As portas devem estar offline para executar o comando anterior. Para colocar uma porta off-line, execute o seguinte comando:

```
network fcp adapter modify -node <home node of the port> -adapter <port
name> -state down
```

Se você alterou a personalidade da porta, será necessário reinicializar cada nó para que a alteração tenha efeito.

Ativar o protocolo de deteção de Cisco

Para ativar o Protocolo de detecção de Cisco (CDP) nos controladores de armazenamento NetApp, execute o seguinte comando:

```
node run -node * options cdpd.enable on
```

Ative o Link-layer Discovery Protocol em todas as portas Ethernet

Ative a troca de informações de vizinhos do protocolo de descoberta de camada de link (LLDP) entre os switches de armazenamento e rede executando o seguinte comando. Este comando permite o LLDP em todas as portas de todos os nós no cluster.

```
node run * options lldp.enable on
```

Renomeie interfaces lógicas de gerenciamento

Para renomear as interfaces lógicas de gerenciamento (LIFs), execute as seguintes etapas:

1. Mostrar os nomes de LIF de gerenciamento atuais.

```
network interface show –vserver <<clustername>>
```

2. Renomeie o LIF de gerenciamento de cluster.

```
network interface rename –vserver <<clustername>> –lif
cluster_setup_cluster_mgmt_lif_1 –newname cluster_mgmt
```

3. Renomeie o nó B Management LIF.

```
network interface rename -vserver <<clustername>> -lif
cluster_setup_node_mgmt_lif_AFF A220_A_1 - newname AFF A220-01_mgmt1
```

Defina a reversão automática no gerenciamento de cluster

Defina `auto-revert` o parâmetro na interface de gerenciamento de cluster.

```
network interface modify -vserver <<clustername>> -lif cluster_mgmt -auto-
revert true
```

Configure a interface de rede do processador de serviço

Para atribuir um endereço IPv4 estático ao processador de serviço em cada nó, execute os seguintes comandos:

```
system service-processor network modify -node <<var_nodeA>> -address
-family IPv4 -enable true – dhcp none -ip-address <<var_nodeA_sp_ip>>
-netmask <<var_nodeA_sp_mask>> -gateway <<var_nodeA_sp_gateway>>
system service-processor network modify -node <<var_nodeB>> -address
-family IPv4 -enable true – dhcp none -ip-address <<var_nodeB_sp_ip>>
-netmask <<var_nodeB_sp_mask>> -gateway <<var_nodeB_sp_gateway>>
```

Os endereços IP do processador de serviço devem estar na mesma sub-rede que os endereços IP de gerenciamento de nós.

Ativar failover de storage no ONTAP

Para confirmar se o failover de armazenamento está ativado, execute os seguintes comandos em um par de failover:

1. Verifique o status do failover de storage.

   ```
   storage failover show
   ```

   Ambos `<<var_nodeA>>` e `<<var_nodeB>>` devem ser capazes de realizar uma aquisição. Vá para a etapa 3 se os nós puderem executar um takeover.

2. Habilite o failover em um dos dois nós.

   ```
   storage failover modify -node <<var_nodeA>> -enabled true
   ```

3. Verifique o status de HA do cluster de dois nós.

   Esta etapa não se aplica a clusters com mais de dois nós.

   ```
   cluster ha show
   ```

4. Vá para a etapa 6 se a alta disponibilidade estiver configurada. Se a alta disponibilidade estiver configurada, você verá a seguinte mensagem ao emitir o comando:

```
High Availability Configured: true
```

5. Ative o modo HA apenas para o cluster de dois nós.

   Não execute este comando para clusters com mais de dois nós porque causa problemas com failover.

```
cluster ha modify -configured true
Do you want to continue? {y|n}: y
```

6. Verifique se a assistência ao hardware está corretamente configurada e, se necessário, modifique o endereço IP do parceiro.

```
storage failover hwassist show
```

   A mensagem `Keep Alive Status : Error: did not receive hwassist keep alive alerts from partner` indica que a assistência ao hardware não está configurada. Execute os seguintes comandos para configurar a assistência de hardware.

```
storage failover modify –hwassist-partner-ip <<var_nodeB_mgmt_ip>> -node
<<var_nodeA>>
storage failover modify –hwassist-partner-ip <<var_nodeA_mgmt_ip>> -node
<<var_nodeB>>
```

Crie um domínio de transmissão MTU de quadro jumbo no ONTAP

Para criar um domínio de transmissão de dados com uma MTU de 9000, execute os seguintes comandos:

```
broadcast-domain create -broadcast-domain Infra_NFS -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-A -mtu 9000
broadcast-domain create -broadcast-domain Infra_iSCSI-B -mtu 9000
```

Remover portas de dados do domínio de broadcast padrão

As portas de dados 10GbE são usadas para tráfego iSCSI/NFS e essas portas devem ser removidas do domínio padrão. As portas e0e e e0f não são usadas e também devem ser removidas do domínio padrão.

Para remover as portas do domínio de broadcast, execute o seguinte comando:

```
broadcast-domain remove-ports -broadcast-domain Default -ports
<<var_nodeA>>:e0c, <<var_nodeA>>:e0d, <<var_nodeA>>:e0e,
<<var_nodeA>>:e0f, <<var_nodeB>>:e0c, <<var_nodeB>>:e0d,
<<var_nodeA>>:e0e, <<var_nodeA>>:e0f
```

Desative o controle de fluxo nas portas UTA2

É uma prática recomendada do NetApp desativar o controle de fluxo em todas as UTA2 portas conetadas a dispositivos externos. Para desativar o controle de fluxo, execute os seguintes comandos:

```
net port modify -node <<var_nodeA>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeA>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0c -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0d -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0e -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
net port modify -node <<var_nodeB>> -port e0f -flowcontrol-admin none
Warning: Changing the network port settings will cause a several second
interruption in carrier. Do you want to continue? {y|n}: y
```

A conexão direta do Cisco UCS Mini ao ONTAP não suporta LACP.

Configurar quadros jumbo no NetApp ONTAP

Para configurar uma porta de rede ONTAP para usar quadros jumbo (que geralmente têm uma MTU de 9.000 bytes), execute os seguintes comandos a partir do shell do cluster:

```
AFF A220::> network port modify -node node_A -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0e -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_A -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
AFF A220::> network port modify -node node_B -port e0f -mtu 9000
Warning: This command will cause a several second interruption of service
on this network port.
Do you want to continue? {y|n}: y
```

Crie VLANs no ONTAP

Para criar VLANs no ONTAP, execute as seguintes etapas:

1. Crie portas VLAN NFS e adicione-as ao domínio de transmissão de dados.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_nfs_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_nfs_vlan_id>>
broadcast-domain add-ports -broadcast-domain Infra_NFS -ports
<<var_nodeA>>: e0e- <<var_nfs_vlan_id>>, <<var_nodeB>>: e0e-
<<var_nfs_vlan_id>> , <<var_nodeA>>:e0f- <<var_nfs_vlan_id>>,
<<var_nodeB>>:e0f-<<var_nfs_vlan_id>>
```

2. Crie portas iSCSI VLAN e adicione-as ao domínio de transmissão de dados.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeA>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0e-
<<var_iscsi_vlan_A_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0f-
<<var_iscsi_vlan_B_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-A -ports
<<var_nodeA>>: e0e- <<var_iscsi_vlan_A_id>>,<<var_nodeB>>: e0e-
<<var_iscsi_vlan_A_id>>
broadcast-domain add-ports -broadcast-domain Infra_iSCSI-B -ports
<<var_nodeA>>: e0f- <<var_iscsi_vlan_B_id>>,<<var_nodeB>>: e0f-
<<var_iscsi_vlan_B_id>>
```

3. Crie portas MGMT-VLAN.

```
network port vlan create –node <<var_nodeA>> -vlan-name e0m-
<<mgmt_vlan_id>>
network port vlan create –node <<var_nodeB>> -vlan-name e0m-
<<mgmt_vlan_id>>
```

Criar agregados no ONTAP

Um agregado contendo o volume raiz é criado durante o processo de configuração do ONTAP. Para criar agregados adicionais, determine o nome do agregado, o nó no qual criá-lo e o número de discos que ele contém.

Para criar agregados, execute os seguintes comandos:

```
aggr create -aggregate aggr1_nodeA -node <<var_nodeA>> -diskcount
<<var_num_disks>>
aggr create -aggregate aggr1_nodeB -node <<var_nodeB>> -diskcount
<<var_num_disks>>
```

Guarde pelo menos um disco (selecione o disco maior) na configuração como um sobressalente. Uma prática recomendada é ter pelo menos um sobressalente para cada tipo e tamanho de disco.

Comece com cinco discos; você pode adicionar discos a um agregado quando for necessário armazenamento adicional.

O agregado não pode ser criado até que a restauração do disco seja concluída. Execute o `aggr show` comando para exibir o status de criação agregada. Não prossiga até `aggr1_nodeA` que esteja online.

Configure o fuso horário no ONTAP

Para configurar a sincronização de hora e definir o fuso horário no cluster, execute o seguinte comando:

```
timezone <<var_timezone>>
```

Por exemplo, no leste dos Estados Unidos, o fuso horário é `America/New_York`. Depois de começar a digitar o nome do fuso horário, pressione a tecla Tab para ver as opções disponíveis.

Configurar SNMP no ONTAP

Para configurar o SNMP, execute as seguintes etapas:

1. Configurar informações básicas do SNMP, como a localização e o contacto. Quando polled, esta informação é visível como `sysLocation` as variáveis e `sysContact` no SNMP.

   ```
   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on
   ```

2. Configurar traps SNMP para enviar para hosts remotos.

   ```
   snmp traphost add <<var_snmp_server_fqdn>>
   ```

Configure o SNMPv1 no ONTAP

Para configurar o SNMPv1, defina a senha secreta compartilhada de texto simples chamada comunidade.

```
snmp community add ro <<var_snmp_community>>
```

Use o `snmp community delete all` comando com cuidado. Se strings de comunidade forem usadas para outros produtos de monitoramento, esse comando as removerá.

Configure o SNMPv3 no ONTAP

SNMPv3 requer que você defina e configure um usuário para autenticação. Para configurar o SNMPv3, execute as seguintes etapas:

1. Execute o `security snmpusers` comando para visualizar a ID do motor.
2. Crie um usuário `snmpv3user` chamado .

```
security login create -username snmpv3user -authmethod usm -application
snmp
```

3. Introduza a ID do motor da entidade autorizada e `md5` selecione como o protocolo de autenticação.
4. Insira uma senha de comprimento mínimo de oito carateres para o protocolo de autenticação quando solicitado.
5. `des`Selecione como o protocolo de privacidade.
6. Insira uma senha de comprimento mínimo de oito carateres para o protocolo de privacidade quando solicitado.

Configure o HTTPS do AutoSupport no ONTAP

A ferramenta NetApp AutoSupport envia informações resumidas de suporte para o NetApp por meio de HTTPS. Para configurar o AutoSupport, execute o seguinte comando:

```
system node autosupport modify -node * -state enable –mail-hosts
<<var_mailhost>> -transport https -support enable -noteto
<<var_storage_admin_email>>
```

Crie uma máquina virtual de armazenamento

Para criar uma máquina virtual de storage de infraestrutura (SVM), siga estas etapas:

1. Executar o `vserver create` comando.

```
vserver create –vserver Infra-SVM –rootvolume rootvol –aggregate
aggr1_nodeA –rootvolume- security-style unix
```

2. Adicione o agregado de dados à lista de agregados de infraestrutura SVM para o VSC do NetApp.

```
vserver modify -vserver Infra-SVM -aggr-list aggr1_nodeA,aggr1_nodeB
```

3. Remova os protocolos de storage não utilizados da SVM, deixando NFS e iSCSI.

```
vserver remove-protocols –vserver Infra-SVM -protocols cifs,ndmp,fcp
```

4. Habilite e execute o protocolo NFS no SVM de infraestrutura.

```
nfs create -vserver Infra-SVM -udp disabled
```

5. Ative o `SVM vstorage` parâmetro para o plug-in NetApp NFS VAAI. Em seguida, verifique se o NFS foi

configurado.

```
vserver nfs modify –vserver Infra-SVM –vstorage enabled
vserver nfs show
```

Os comandos são pré-enfrentados `vserver` na linha de comando porque SVMs eram anteriormente chamados de servidores

Configure o NFSv3 no ONTAP

A tabela abaixo lista as informações necessárias para concluir esta configuração.

Detalhe	Valor do detalhe
ESXi Hospeda Um endereço IP NFS	"Cliente <var_esxi_hostA_nfs_ip>>
Endereço IP NFS do host ESXi B.	"Cliente <var_esxi_hostB_nfs_ip>>

Para configurar o NFS na SVM, execute os seguintes comandos:

1. Crie uma regra para cada host ESXi na política de exportação padrão.
2. Para cada host ESXi sendo criado, atribua uma regra. Cada host tem seu próprio índice de regras. Seu primeiro host ESXi tem o índice de regra 1, seu segundo host ESXi tem o índice de regra 2, e assim por diante.

```
vserver export-policy rule create –vserver Infra-SVM -policyname default
–ruleindex 1 –protocol nfs -clientmatch <<var_esxi_hostA_nfs_ip>>
-rorule sys –rwrule sys -superuser sys –allow-suid falsevserver export-
policy rule create –vserver Infra-SVM -policyname default –ruleindex 2
–protocol nfs -clientmatch <<var_esxi_hostB_nfs_ip>> -rorule sys –rwrule
sys -superuser sys –allow-suid false
vserver export-policy rule show
```

3. Atribua a política de exportação ao volume raiz da infraestrutura SVM.

```
volume modify –vserver Infra-SVM –volume rootvol –policy default
```

O VSC do NetApp manipula automaticamente as políticas de exportação se você optar por instalá-las após a configuração do vSphere. Se você não instalá-lo, você deve criar regras de política de exportação quando servidores adicionais da série B do Cisco UCS forem adicionados.

Criar serviço iSCSI no ONTAP

Para criar o serviço iSCSI, execute o seguinte passo:

1. Crie o serviço iSCSI no SVM. Esse comando também inicia o serviço iSCSI e define o IQN (iSCSI Qualified Name) para o SVM. Verifique se o iSCSI foi configurado.

```
iscsi create -vserver Infra-SVM
iscsi show
```

Criar espelho de compartilhamento de carga do volume raiz da SVM no ONTAP

Para criar um espelhamento de compartilhamento de carga do volume raiz do SVM no ONTAP, siga estas etapas:

1. Crie um volume para ser o espelhamento de compartilhamento de carga do volume raiz da infraestrutura SVM em cada nó.

```
volume create –vserver Infra_Vserver –volume rootvol_m01 –aggregate
aggr1_nodeA –size 1GB –type DPvolume create –vserver Infra_Vserver
–volume rootvol_m02 –aggregate aggr1_nodeB –size 1GB –type DP
```

2. Crie uma agenda de trabalhos para atualizar as relações de espelho de volume raiz a cada 15 minutos.

```
job schedule interval create -name 15min -minutes 15
```

3. Crie as relações de espelhamento.

```
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m01 -type LS -schedule 15min
snapmirror create -source-path Infra-SVM:rootvol -destination-path
Infra-SVM:rootvol_m02 -type LS -schedule 15min
```

4. Inicialize a relação de espelhamento e verifique se ela foi criada.

```
snapmirror initialize-ls-set -source-path Infra-SVM:rootvol snapmirror
show
```

Configurar o acesso HTTPS no ONTAP

Para configurar o acesso seguro ao controlador de armazenamento, execute as seguintes etapas:

1. Aumente o nível de privilégio para acessar os comandos do certificado.

```
set -privilege diag
Do you want to continue? {y|n}: y
```

2. Geralmente, um certificado auto-assinado já está em vigor. Verifique o certificado executando o seguinte comando:

```
security certificate show
```

3. Para cada SVM mostrado, o nome comum do certificado deve corresponder ao nome de domínio totalmente qualificado (FQDN) do SVM. Os quatro certificados predefinidos devem ser suprimidos e substituídos por certificados auto-assinados ou certificados de uma autoridade de certificação.

   Excluir certificados expirados antes de criar certificados é uma prática recomendada. Execute o `security certificate delete` comando para excluir certificados expirados. No comando a seguir, use conclusão de TABULAÇÃO para selecionar e excluir cada certificado padrão.

```
security certificate delete [TAB] ...
Example: security certificate delete -vserver Infra-SVM -common-name
Infra-SVM -ca Infra-SVM - type server -serial 552429A6
```

4. Para gerar e instalar certificados autoassinados, execute os seguintes comandos como comandos únicos. Gerar um certificado de servidor para a infraestrutura SVM e o cluster SVM. Novamente, use TAB Completion para ajudar a completar esses comandos.

```
security certificate create [TAB] ...
Example: security certificate create -common-name infra-svm.netapp.com
-type server -size 2048 - country US -state "North Carolina" -locality
"RTP" -organization "NetApp" -unit "FlexPod" -email- addr
"abc@netapp.com" -expire-days 365 -protocol SSL -hash-function SHA256
-vserver Infra-SVM
```

5. Para obter os valores para os parâmetros necessários na etapa seguinte, execute o `security certificate show` comando.
6. Ative cada certificado que acabou de ser criado usando os `-server-enabled true` parâmetros e. `-client- enabled false` Novamente, use A conclusão DA GUIA.

```
security ssl modify [TAB] ...
Example: security ssl modify -vserver Infra-SVM -server-enabled true
-client-enabled false -ca infra-svm.netapp.com -serial 55243646 -common
-name infra-svm.netapp.com
```

7. Configure e ative o acesso SSL e HTTPS e desative o acesso HTTP.

```
system services web modify -external true -sslv3-enabled true
Warning: Modifying the cluster configuration will cause pending web
service requests to be interrupted as the web servers are restarted.
Do you want to continue {y|n}: y
System services firewall policy delete -policy mgmt -service http
-vserver <<var_clustername>>
```

ⓘ É normal que alguns desses comandos retornem uma mensagem de erro informando que a entrada não existe.

8. Reverta para o nível de privilégios de administrador e crie a configuração para permitir que o SVM esteja disponível na Web.

```
set –privilege admin
vserver services web modify –name spi|ontapi|compat –vserver * -enabled
true
```

Crie um NetApp FlexVol volume no ONTAP

Para criar um volume NetApp FlexVol, insira o nome do volume, o tamanho e o agregado no qual ele existe. Crie dois volumes do VMware datastore e um volume de inicialização do servidor.

```
volume create -vserver Infra-SVM -volume infra_datastore_1 -aggregate
aggr1_nodeA -size 500GB - state online -policy default -junction-path
/infra_datastore_1 -space-guarantee none -percent- snapshot-space 0
volume create -vserver Infra-SVM -volume infra_datastore_2 -aggregate
aggr1_nodeB -size 500GB - state online -policy default -junction-path
/infra_datastore_2 -space-guarantee none -percent- snapshot-space 0
```

```
volume create -vserver Infra-SVM -volume infra_swap -aggregate aggr1_nodeA
-size 100GB -state online -policy default -juntion-path /infra_swap -space
-guarantee none -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver Infra-SVM -volume esxi_boot -aggregate aggr1_nodeA
-size 100GB -state online -policy default -space-guarantee none -percent
-snapshot-space 0
```

Ativar a deduplicação no ONTAP

Para habilitar a deduplicação em volumes apropriados uma vez por dia, execute os seguintes comandos:

```
volume efficiency modify –vserver Infra-SVM –volume esxi_boot –schedule
sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_1
–schedule sun-sat@0
volume efficiency modify –vserver Infra-SVM –volume infra_datastore_2
–schedule sun-sat@0
```

Criar LUNs no ONTAP

Para criar dois números de unidade lógica de inicialização (LUNs), execute os seguintes comandos:

```
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-A -size
15GB -ostype vmware - space-reserve disabled
lun create -vserver Infra-SVM -volume esxi_boot -lun VM-Host-Infra-B -size
15GB -ostype vmware - space-reserve disabled
```

Ao adicionar um servidor Cisco UCS C-Series extra, um LUN de inicialização extra deve ser criado.

Criar iSCSI LIFs no ONTAP

A tabela abaixo lista as informações necessárias para concluir esta configuração.

Detalhe	Valor do detalhe
Nó de storage A iSCSI LIF01A	"Cliente <var_nodeA_iscsi_lif01a_ip>>
Nó de armazenamento Uma máscara de rede iSCSI LIF01A	"Cliente <var_nodeA_iscsi_lif01a_mask>>
Nó de storage A iSCSI LIF01B	"Cliente <var_nodeA_iscsi_lif01b_ip>>
Nó de armazenamento Uma máscara de rede iSCSI LIF01B	"Cliente <var_nodeA_iscsi_lif01b_mask>>
Nó de storage B iSCSI LIF01A	"Cliente <var_nodeB_iscsi_lif01a_ip>>
Máscara de rede do nó de armazenamento B iSCSI LIF01A	"Cliente <var_nodeB_iscsi_lif01a_mask>>
Nó de storage B iSCSI LIF01B	"Cliente <var_nodeB_iscsi_lif01b_ip>>
Máscara de rede do nó de armazenamento B iSCSI LIF01B	"Cliente <var_nodeB_iscsi_lif01b_mask>>

1. Crie quatro LIFs iSCSI, dois em cada nó.

```
network interface create -vserver Infra-SVM -lif iscsi_lif01a -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeA_iscsi_lif01a_ip>> -netmask
<<var_nodeA_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif01b -role data
-data-protocol iscsi - home-node <<var_nodeA>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeA_iscsi_lif01b_ip>> -netmask
<<var_nodeA_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02a -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0e-
<<var_iscsi_vlan_A_id>> -address <<var_nodeB_iscsi_lif01a_ip>> -netmask
<<var_nodeB_iscsi_lif01a_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface create -vserver Infra-SVM -lif iscsi_lif02b -role data
-data-protocol iscsi - home-node <<var_nodeB>> -home-port e0f-
<<var_iscsi_vlan_B_id>> -address <<var_nodeB_iscsi_lif01b_ip>> -netmask
<<var_nodeB_iscsi_lif01b_mask>> –status-admin up – failover-policy
disabled –firewall-policy data –auto-revert false
network interface show
```

Criar LIFs NFS no ONTAP

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
Nó de storage A NFS LIF 01 a IP	"Cliente <var_nodeA_nfs_lif_01_a_ip>>
Nó de storage A NFS LIF 01 uma máscara de rede	"Cliente <var_nodeA_nfs_lif_01_a_mask>>
Nó de storage A NFS LIF 01 b IP	"Cliente <var_nodeA_nfs_lif_01_b_ip>>
Nó de storage Uma máscara de rede NFS LIF 01 b	"Cliente <var_nodeA_nfs_lif_01_b_mask>>
Nó de storage B NFS LIF 02 a IP	"Cliente <var_nodeB_nfs_lif_02_a_ip>>
Nó de storage B NFS LIF 02 a máscara de rede	"Cliente <var_nodeB_nfs_lif_02_a_mask>>
Nó de storage B NFS LIF 02 b IP	"Cliente <var_nodeB_nfs_lif_02_b_ip>>
Nó de storage B máscara de rede NFS LIF 02 b	"Cliente <var_nodeB_nfs_lif_02_b_mask>>

1. Criar um NFS LIF.

```
network interface create -vserver Infra-SVM -lif nfs_lif01_a -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0e-
<<var_nfs_vlan_id>> -address <<var_nodeA_nfs_lif_01_a_ip>> - netmask <<
var_nodeA_nfs_lif_01_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif01_b -role data
-data-protocol nfs -home- node <<var_nodeA>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeA_nfs_lif_01_b_ip>> - netmask <<
var_nodeA_nfs_lif_01_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_a -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0e-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_a_ip>> - netmask <<
var_nodeB_nfs_lif_02_a_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface create -vserver Infra-SVM -lif nfs_lif02_b -role data
-data-protocol nfs -home- node <<var_nodeB>> -home-port e0f-
<<var_nfs_vlan_id>> –address <<var_nodeB_nfs_lif_02_b_ip>> - netmask <<
var_nodeB_nfs_lif_02_b_mask>> -status-admin up –failover-policy
broadcast-domain-wide – firewall-policy data –auto-revert true
network interface show
```

Adicionar administrador de infraestrutura SVM

A tabela a seguir lista as informações necessárias para concluir essa configuração.

Detalhe	Valor do detalhe
IP Vsmgmt	"cliente <var_svm_mgmt_ip>>
Máscara de rede Vsmgmt	"cliente <var_svm_mgmt_mask>>
Gateway padrão Vsmgmt	"cliente <var_svm_mgmt_gateway>>

Para adicionar o administrador da infraestrutura SVM e o LIF de administração da SVM à rede de gerenciamento, siga estas etapas:

1. Execute o seguinte comando:

```
network interface create –vserver Infra-SVM –lif vsmgmt –role data
–data-protocol none –home-node <<var_nodeB>> -home-port e0M –address
<<var_svm_mgmt_ip>> -netmask <<var_svm_mgmt_mask>> - status-admin up
–failover-policy broadcast-domain-wide –firewall-policy mgmt –auto-
revert true
```

O IP de gerenciamento do SVM deve estar na mesma sub-rede que o IP de gerenciamento do cluster de storage.

2. Crie uma rota padrão para permitir que a interface de gerenciamento SVM alcance o mundo externo.

```
network route create –vserver Infra-SVM -destination 0.0.0.0/0 –gateway
<<var_svm_mgmt_gateway>> network route show
```

3. Defina uma senha para o usuário SVM `vsadmin` e desbloqueie o usuário.

```
security login password –username vsadmin –vserver Infra-SVM
Enter a new password: <<var_password>>
Enter it again: <<var_password>>
security login unlock –username vsadmin –vserver
```

Configuração do servidor Cisco UCS

Base FlexPod Cisco UCS

Execute a configuração inicial da interconexão de malha do Cisco UCS 6324 para ambientes FlexPod.

Esta seção fornece procedimentos detalhados para configurar o Cisco UCS para uso em um ambiente FlexPod ROBO usando o Cisco UCS Manager.

Interconexão de malha Cisco UCS Fabric 6324 A.

O Cisco UCS usa servidores e redes de camada de acesso. Esse sistema de servidor de alta performance e próxima geração fornece um data center com alto nível de agilidade e escalabilidade de carga de trabalho.

O Cisco UCS Manager 4,0(1b) é compatível com a interconexão de malha 6324 que integra a interconexão de malha ao chassi do Cisco UCS e fornece uma solução integrada para um ambiente de implantação menor. O Cisco UCS Mini simplifica o gerenciamento do sistema e economiza custos para implantações de baixa escala.

Os componentes de hardware e software são compatíveis com a malha unificada da Cisco, que executa vários tipos de tráfego de data center em um único adaptador de rede convergente.

Configuração inicial do sistema

Na primeira vez que você acessa uma interconexão de malha em um domínio do Cisco UCS, um assistente de configuração solicita as seguintes informações necessárias para configurar o sistema:

- Método de instalação (GUI ou CLI)
- Modo de configuração (restauração a partir de backup completo do sistema ou configuração inicial)
- Tipo de configuração do sistema (configuração autônoma ou de cluster)
- Nome do sistema
- Palavra-passe de administrador

- Endereço da porta de gerenciamento IPv4 e máscara de sub-rede, ou endereço IPv6 e prefixo
- Endereço IPv4 ou IPv6 do gateway padrão
- Endereço DNS Server IPv4 ou IPv6
- Nome de domínio padrão

A tabela a seguir lista as informações necessárias para concluir a configuração inicial do Cisco UCS no Fabric Interconnect A

Detalhe	**Detalhe/valor**
Nome do sistema	"cliente <var_ucs_clustername>>
Palavra-passe de administrador	"cliente <var_password>>
Endereço IP de gerenciamento: Interconexão de malha A	"cliente <var_ucsa_mgmt_ip>>
Máscara de rede de gestão: Interligação de tecido A	"cliente <var_ucsa_mgmt_mask>>
Gateway padrão: Interconexão de malha A	"cliente <var_ucsa_mgmt_gateway>>
Endereço IP do cluster	"cliente <var_ucs_cluster_ip>>
Endereço IP do servidor DNS	"cliente <var_nameserver_ip>>
Nome de domínio	"cliente <var_domain_name>>

Para configurar o Cisco UCS para uso em um ambiente FlexPod, siga estas etapas:

1. Conete-se à porta do console no primeiro Cisco UCS 6324 Fabric Interconnect A..

```
Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup.
(setup/restore) ? setup

  You have chosen to setup a new Fabric interconnect. Continue? (y/n): y

  Enforce strong password? (y/n) [y]: Enter

  Enter the password for "admin":<<var_password>>
  Confirm the password for "admin":<<var_password>>

  Is this Fabric interconnect part of a cluster(select 'no' for
standalone)? (yes/no) [n]: yes

  Enter the switch fabric (A/B) []: A

  Enter the system name: <<var_ucs_clustername>>

  Physical Switch Mgmt0 IP address : <<var_ucsa_mgmt_ip>>

  Physical Switch Mgmt0 IPv4 netmask : <<var_ucsa_mgmt_mask>>

  IPv4 address of the default gateway : <<var_ucsa_mgmt_gateway>>

  Cluster IPv4 address : <<var_ucs_cluster_ip>>

  Configure the DNS Server IP address? (yes/no) [n]: y

       DNS IP address : <<var_nameserver_ip>>

  Configure the default domain name? (yes/no) [n]: y
Default domain name: <<var_domain_name>>

  Join centralized management environment (UCS Central)? (yes/no) [n]:
no

 NOTE: Cluster IP will be configured only after both Fabric
Interconnects are initialized. UCSM will be functional only after peer
FI is configured in clustering mode.

  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Reveja as definições apresentadas na consola. Se estiverem corretas, responda `yes` para aplicar e guardar a configuração.
3. Aguarde até que o prompt de login verifique se a configuração foi salva.

A tabela a seguir lista as informações necessárias para concluir a configuração inicial do Cisco UCS na interconexão B.

Detalhe	Detalhe/valor
Nome do sistema	"cliente <var_ucs_clustername>>
Palavra-passe de administrador	"cliente <var_password>>
Endereço IP de gestão FI B	"cliente <var_ucsb_mgmt_ip>>
Gerenciamento Netmask-FI B	"cliente <var_ucsb_mgmt_mask>>
Gateway-Fi B predefinido	"cliente <var_ucsb_mgmt_gateway>>
Endereço IP do cluster	"cliente <var_ucs_cluster_ip>>
Endereço IP do servidor DNS	"cliente <var_nameserver_ip>>
Nome de domínio	"cliente <var_domain_name>>

1. Conete-se à porta do console no segundo Cisco UCS 6324 Fabric Interconnect B.

```
 Enter the configuration method. (console/gui) ? console

  Installer has detected the presence of a peer Fabric interconnect.
This Fabric interconnect will be added to the cluster. Continue (y/n) ?
y

  Enter the admin password of the peer Fabric
interconnect:<<var_password>>
    Connecting to peer Fabric interconnect... done
    Retrieving config from peer Fabric interconnect... done
    Peer Fabric interconnect Mgmt0 IPv4 Address: <<var_ucsb_mgmt_ip>>
    Peer Fabric interconnect Mgmt0 IPv4 Netmask: <<var_ucsb_mgmt_mask>>
    Cluster IPv4 address: <<var_ucs_cluster_address>>

    Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric
Interconnect Mgmt0 IPv4 Address

  Physical Switch Mgmt0 IP address : <<var_ucsb_mgmt_ip>>


  Apply and save the configuration (select 'no' if you want to re-
enter)? (yes/no): yes
  Applying configuration. Please wait.

  Configuration file - Ok
```

2. Aguarde até que o prompt de login confirme se a configuração foi salva.

Faça login no Cisco UCS Manager

Para fazer login no ambiente do Cisco Unified Computing System (UCS), siga estas etapas:

1. Abra um navegador da Web e navegue até o endereço do cluster do Cisco UCS Fabric Interconnect.

   Talvez seja necessário esperar pelo menos 5 minutos depois de configurar a segunda interconexão de malha para que o Cisco UCS Manager apareça.

2. Clique no link Launch UCS Manager para iniciar o Cisco UCS Manager.
3. Aceite os certificados de segurança necessários.
4. Quando solicitado, digite admin como o nome de usuário e insira a senha do administrador.
5. Clique em Iniciar sessão para iniciar sessão no Gestor Cisco UCS.

Software Cisco UCS Manager versão 4,0(1b)

Este documento assume o uso do software Cisco UCS Manager versão 4,0(1b). Para atualizar o software do Cisco UCS Manager e o software de interconexão de malha Cisco UCS 6324, consulte "Guias de instalação e atualização do Cisco UCS Manager."

Configurar o Início de chamada do Cisco UCS

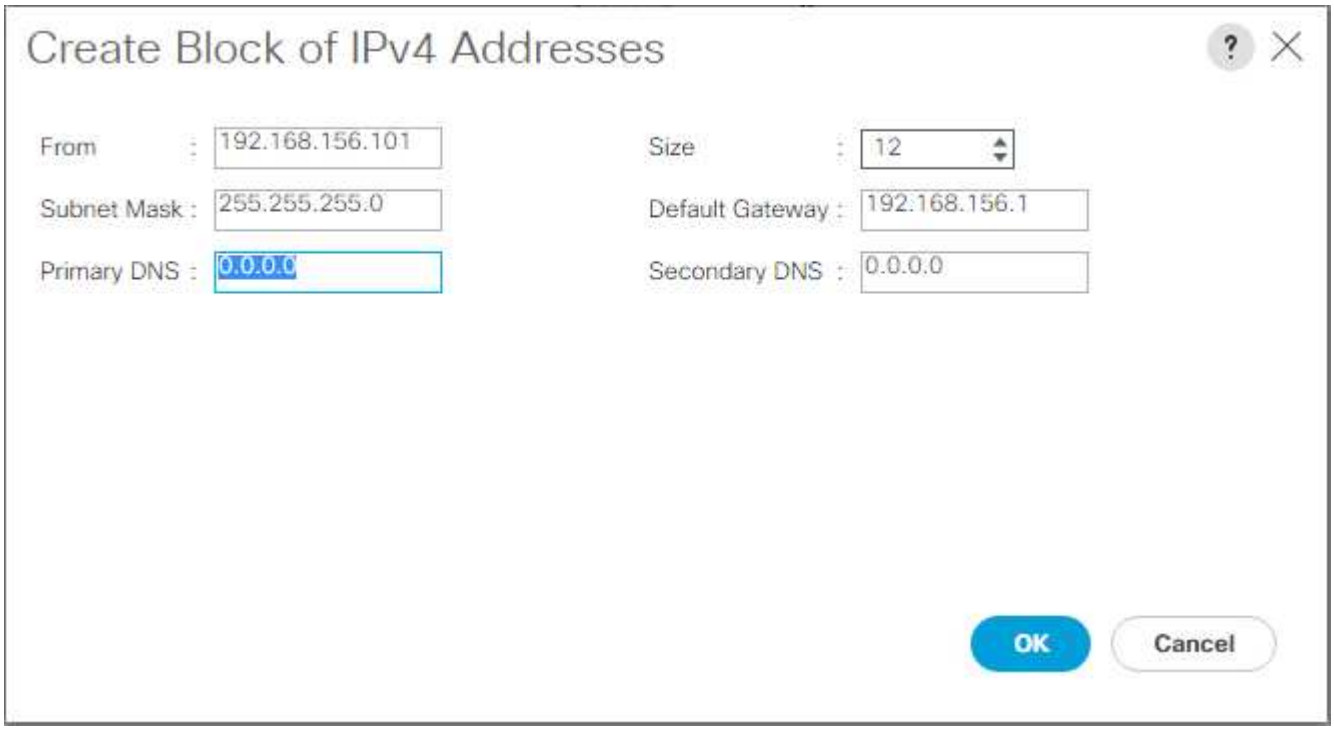
A Cisco recomenda altamente que você configure o Início de chamada no Gerenciador de UCS do Cisco. Configurar o Call Home acelera a resolução de casos de suporte. Para configurar o Call Home, execute as seguintes etapas:

1. No Gerenciador do Cisco UCS, clique em Admin à esquerda.
2. Selecione tudo > Gestão de Comunicação > chamar Casa.
3. Altere o Estado para ligado.
4. Preencha todos os campos de acordo com suas preferências de gerenciamento e clique em Salvar alterações e OK para concluir a configuração Início de chamada.

Adicionar bloco de endereços IP para acesso ao teclado, vídeo e Mouse

Para criar um bloco de endereços IP para acesso ao teclado do servidor de banda, vídeo, Mouse (KVM) no ambiente Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Expanda pools > raiz > pools IP.
3. Clique com o botão direito do Mouse IP Pool ext-mgmt e selecione criar bloco de endereços IPv4.
4. Introduza o endereço IP inicial do bloco, o número de endereços IP necessários e a máscara de sub-rede e as informações do gateway.



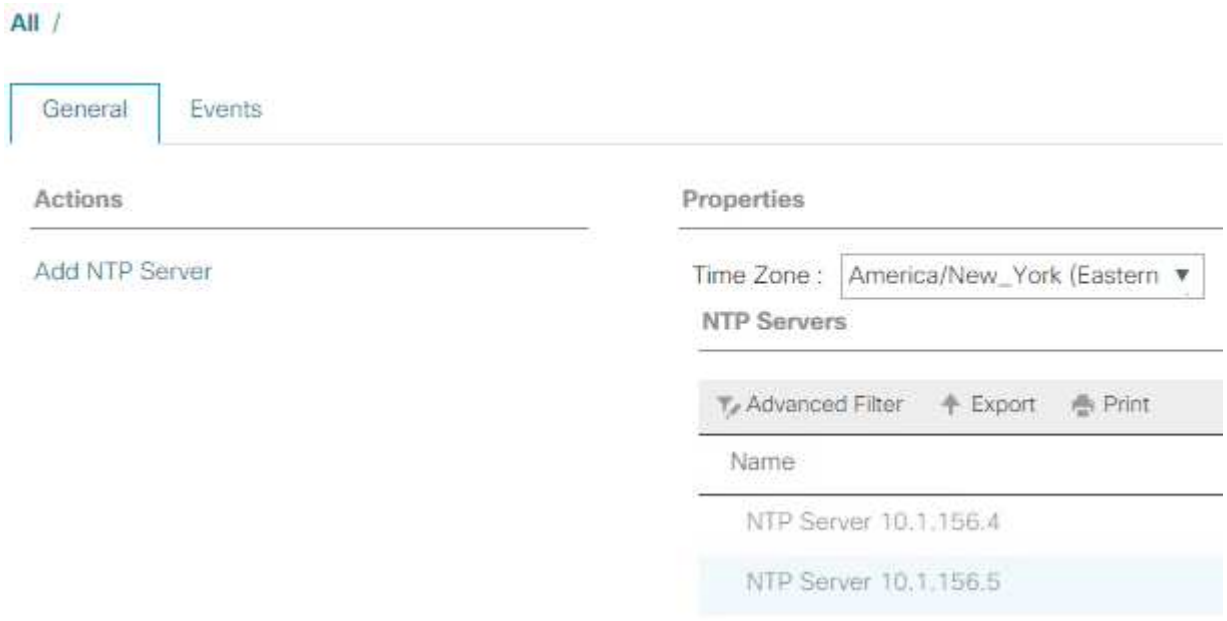
5. Clique em OK para criar o bloco.
6. Clique em OK na mensagem de confirmação.

Sincronizar Cisco UCS para NTP

Para sincronizar o ambiente do Cisco UCS com os servidores NTP nos switches Nexus, execute as seguintes etapas:

1. No Gerenciador do Cisco UCS, clique em Admin à esquerda.
2. Expandir tudo > Gerenciamento de Fuso horário.
3. Selecione Fuso horário.
4. No painel Propriedades, selecione o fuso horário apropriado no menu Fuso horário.
5. Clique em Salvar alterações e clique em OK.
6. Clique em Adicionar servidor NTP.
7. Introduza `<switch-a-ntp-ip> or <Nexus-A-mgmt-IP>` e clique em OK. Clique em OK.

8. Clique em Adicionar servidor NTP.
9. Introduza `<switch-b-ntp-ip> or <Nexus-B-mgmt-IP>` e clique em OK. Clique em OK na confirmação.



Editar política de deteção de chassis

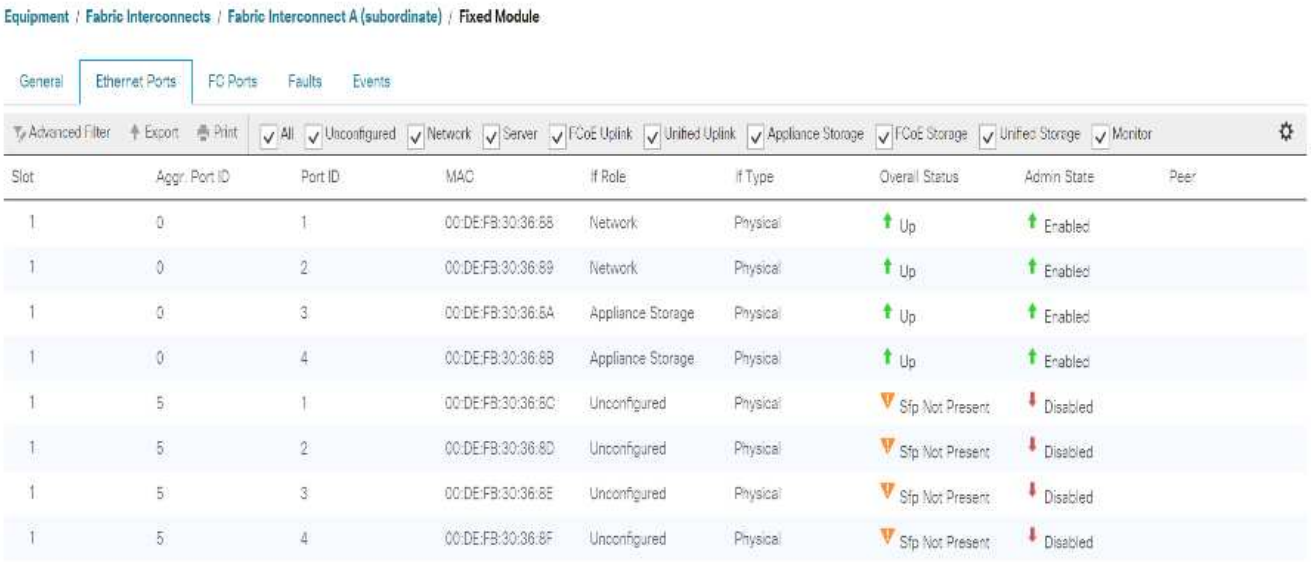
A definição da política de descoberta simplifica a adição do chassi do Cisco UCS B-Series e de extensores de malha adicionais para conectividade adicional do Cisco UCS C-Series. Para modificar a política de deteção de chassis, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em Equipamento à esquerda e selecione Equipamento na segunda lista.
2. No painel direito, selecione a guia políticas.
3. Em políticas globais, defina a Política de descoberta de Chassi/FEX para corresponder ao número mínimo de portas de uplink que são cabeadas entre o chassi ou extensores de malha (FEXes) e as interconexões de malha.
4. Defina a preferência de agrupamento de ligações para Canal de portas. Se o ambiente que está sendo configurado contiver uma grande quantidade de tráfego multicast, defina a configuração Multicast hardware Hash como ativado.
5. Clique em Salvar alterações.
6. Clique em OK.

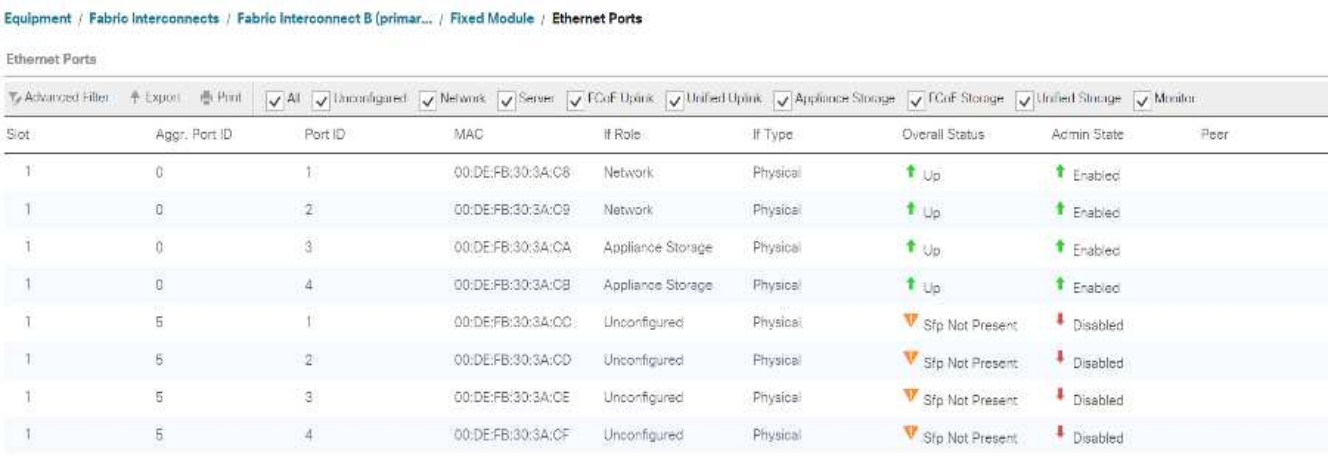
Ative as portas de servidor, uplink e armazenamento

Para ativar as portas de servidor e uplink, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, no painel de navegação, selecione a guia Equipamento.
2. Expandir equipamento > interconexões de malha > Interconexão de malha A > módulo fixo.
3. Expanda as portas Ethernet.
4. Selecione as portas 1 e 2 conetadas aos switches Cisco Nexus 31108, clique com o botão direito do Mouse e selecione Configurar como porta de uplink.
5. Clique em Sim para confirmar as portas uplink e clique em OK.
6. Selecione as portas 3 e 4 conetadas aos controladores de armazenamento NetApp, clique com o botão direito do Mouse e selecione Configurar como porta do dispositivo.
7. Clique em Sim para confirmar as portas do dispositivo.
8. Na janela Configurar como porta do dispositivo, clique em OK.
9. Clique em OK para confirmar.
10. No painel esquerdo, selecione módulo fixo sob interconexão de malha A.
11. Na guia portas Ethernet, confirme se as portas foram configuradas corretamente na coluna função if. Se algum servidor da série C de porta tiver sido configurado na porta de escalabilidade, clique nele para verificar a conetividade da porta lá.



12. Expandir equipamento > interconexões de malha > Interconexão de malha B > módulo fixo.
13. Expanda as portas Ethernet.
14. Selecione as portas Ethernet 1 e 2 conetadas aos switches Cisco Nexus 31108, clique com o botão direito do Mouse e selecione Configurar como porta de uplink.
15. Clique em Sim para confirmar as portas uplink e clique em OK.
16. Selecione as portas 3 e 4 conetadas aos controladores de armazenamento NetApp, clique com o botão direito do Mouse e selecione Configurar como porta do dispositivo.
17. Clique em Sim para confirmar as portas do dispositivo.
18. Na janela Configurar como porta do dispositivo, clique em OK.
19. Clique em OK para confirmar.
20. No painel esquerdo, selecione módulo fixo sob interconexão de malha B.
21. Na guia portas Ethernet, confirme se as portas foram configuradas corretamente na coluna função if. Se algum servidor da série C de porta tiver sido configurado na porta de escalabilidade, clique nele para verificar a conetividade da porta lá.



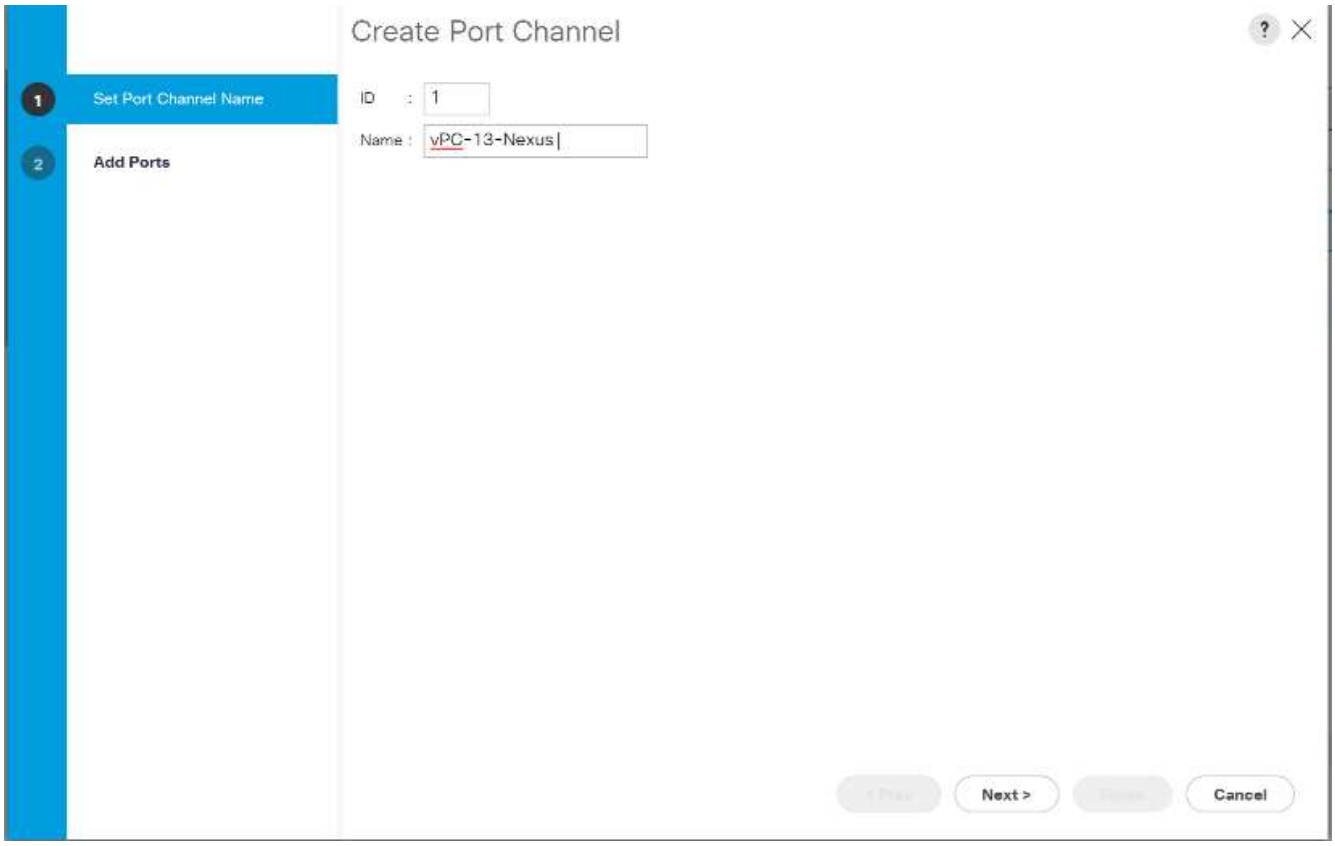
Crie canais de porta uplink para os switches Cisco Nexus 31108

Para configurar os canais de porta necessários no ambiente do Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, selecione a guia LAN no painel de navegação.

> Nesse procedimento, dois canais de porta são criados: Um da malha A aos switches Cisco Nexus 31108 e outro da malha B para ambos os switches Cisco Nexus 31108. Se estiver a utilizar comutadores padrão, modifique este procedimento em conformidade. Se você estiver usando switches 1 Gigabit Ethernet (1GbE) e SFPs GLC-T nas interconexões de malha, as velocidades de interface das portas Ethernet 1/1 e 1/2 nas interconexões de malha devem ser definidas como 1Gbps.

2. Em LAN > LAN Cloud, expanda a estrutura de Uma árvore.
3. Clique com o botão direito do rato em Canais de portas.
4. Selecione criar canal de porta.
5. Introduza 13 como a ID exclusiva do canal da porta.
6. Digite VPC-13-Nexus como o nome do canal da porta.
7. Clique em seguinte.



8. Selecione as seguintes portas a serem adicionadas ao canal da porta:
   a. ID do slot 1 e porta 1
   b. ID do slot 1 e porta 2
9. Clique em >> para adicionar as portas ao canal da porta.
10. Clique em concluir para criar o canal da porta. Clique em OK.

11. Em Canais de porta, selecione o canal de porta recém-criado.

    O canal da porta deve ter um status geral de Up.

12. No painel de navegação, em LAN > LAN Cloud, expanda a árvore Fabric B.
13. Clique com o botão direito do rato em Canais de portas.
14. Selecione criar canal de porta.
15. Introduza 14 como a ID exclusiva do canal da porta.
16. Digite VPC-14-Nexus como o nome do canal da porta. Clique em seguinte.
17. Selecione as seguintes portas a serem adicionadas ao canal da porta:
    a. ID do slot 1 e porta 1
    b. ID do slot 1 e porta 2
18. Clique em >> para adicionar as portas ao canal da porta.
19. Clique em concluir para criar o canal da porta. Clique em OK.
20. Em Canais de porta, selecione o canal de porta recém-criado.
21. O canal da porta deve ter um status geral de Up.

Criar uma organização (opcional)

As organizações estão acostumadas a organizar recursos e restringir o acesso a vários grupos dentro da organização DE TI, permitindo, assim, a multilocação dos recursos de computação.

> Embora este documento não assuma o uso de organizações, este procedimento fornece instruções para a criação de uma.

Para configurar uma organização no ambiente do Cisco UCS, execute as seguintes etapas:

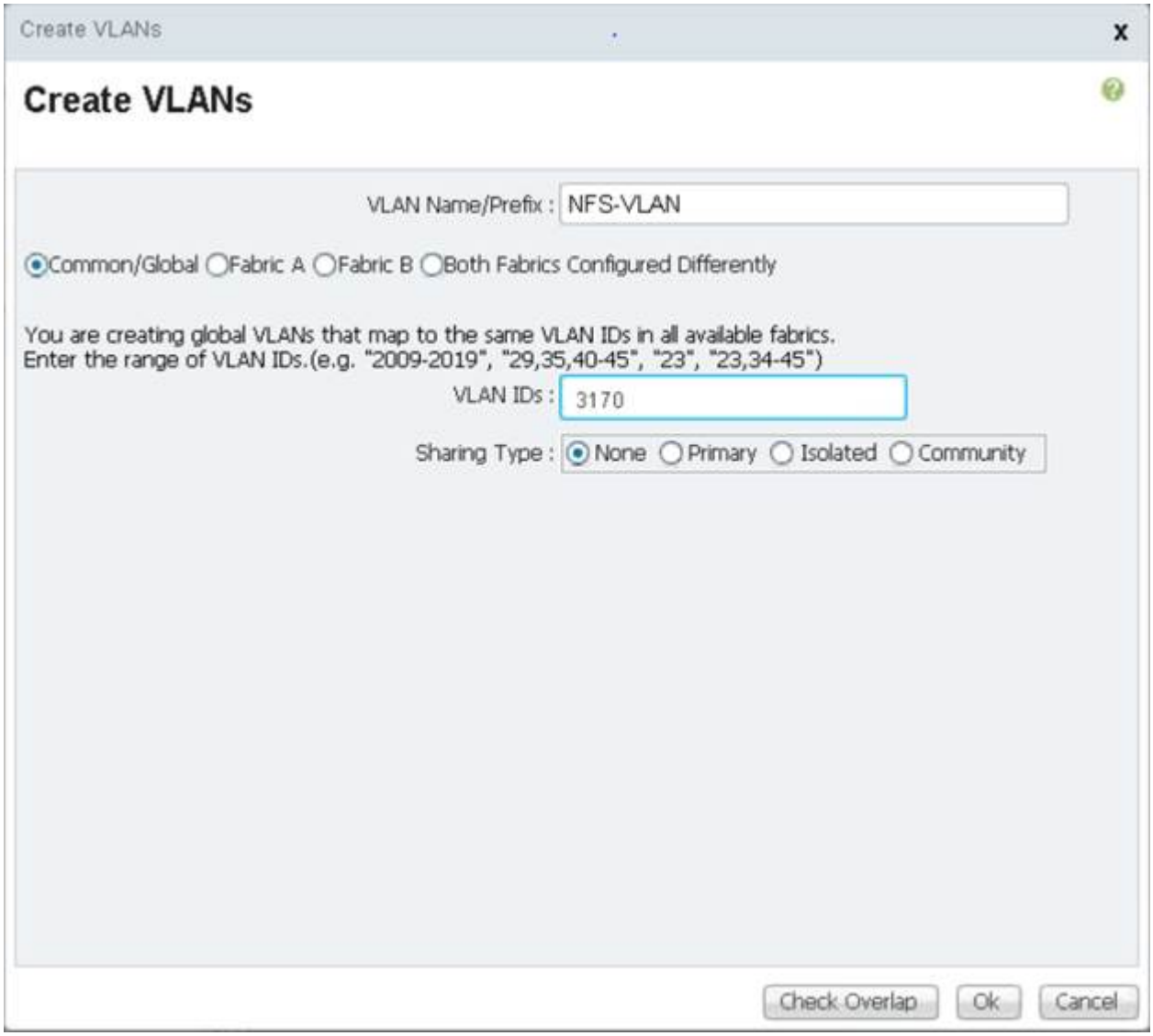
1. No Gerenciador Cisco UCS, no menu novo na barra de ferramentas na parte superior da janela, selecione criar Organização.
2. Introduza um nome para a organização.
3. Opcional: Insira uma descrição para a organização. Clique em OK.
4. Clique em OK na mensagem de confirmação.

Configurar portas de dispositivos de armazenamento e VLANs de armazenamento

Para configurar as portas do dispositivo de armazenamento e as VLANs de armazenamento, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, selecione a guia LAN.
2. Expanda a nuvem dos dispositivos.
3. Clique com o botão direito do Mouse em VLANs na nuvem de dispositivos.
4. Selecione criar VLANs.
5. Insira NFS-VLAN como o nome da VLAN NFS de infraestrutura.
6. Deixe Comum/Global selecionado.
7. Insira `<<var_nfs_vlan_id>>` para a ID da VLAN.

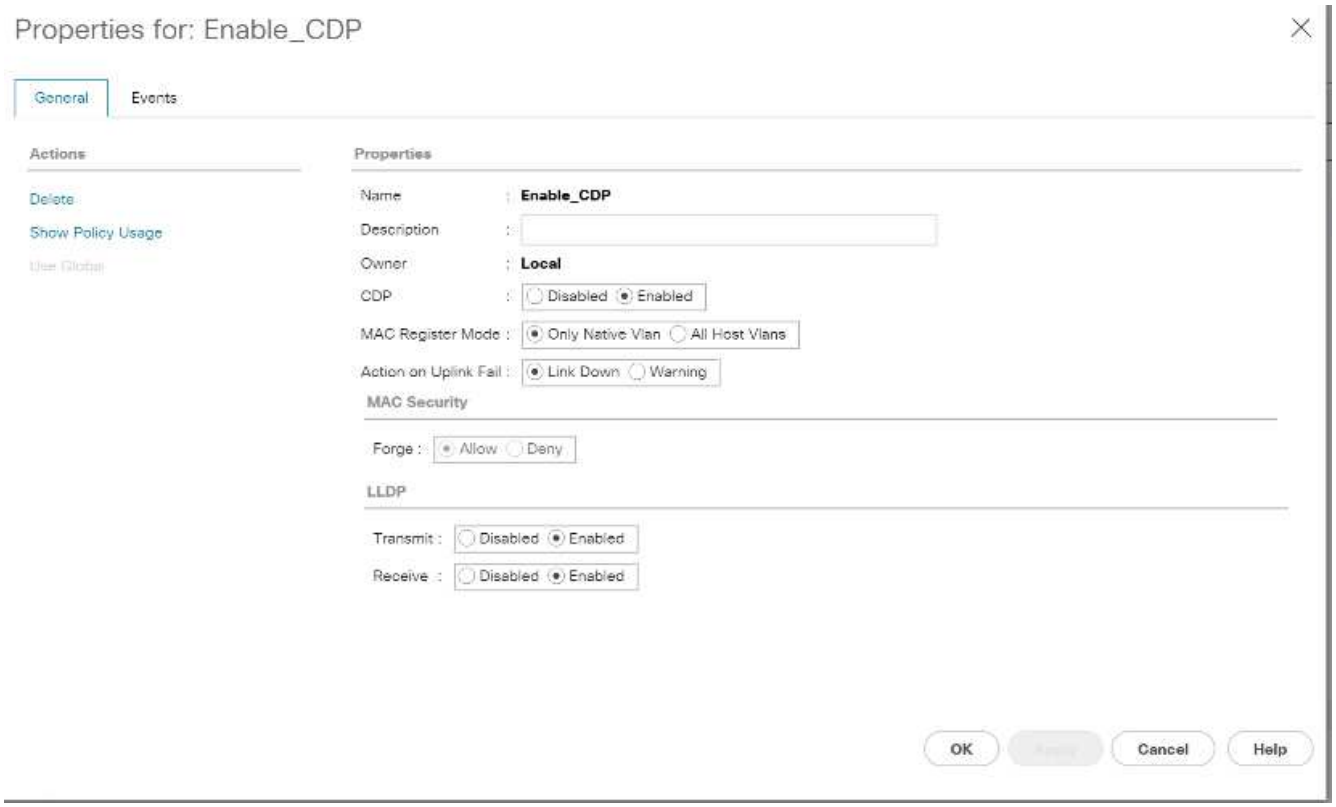
8. Deixe o tipo de partilha definido como nenhum.



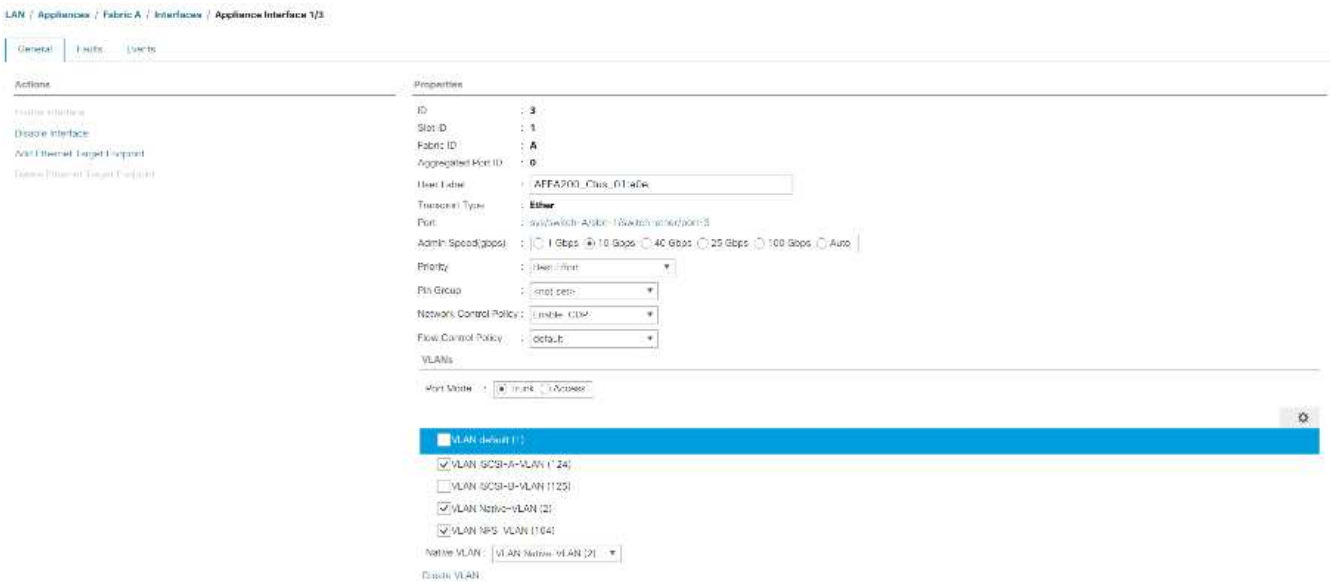
9. Clique em OK e, em seguida, clique em OK novamente para criar a VLAN.
10. Clique com o botão direito do Mouse em VLANs na nuvem de dispositivos.
11. Selecione criar VLANs.
12. Insira iSCSI-A-VLAN como o nome da VLAN de estrutura iSCSI A.
13. Deixe Comum/Global selecionado.
14. Insira `<<var_iscsi-a_vlan_id>>` para a ID da VLAN.
15. Clique em OK e, em seguida, clique em OK novamente para criar a VLAN.
16. Clique com o botão direito do Mouse em VLANs na nuvem de dispositivos.
17. Selecione criar VLANs.
18. Insira iSCSI-B-VLAN como o nome da VLAN de estrutura iSCSI Fabric B.
19. Deixe Comum/Global selecionado.
20. Insira `<<var_iscsi-b_vlan_id>>` para a ID da VLAN.
21. Clique em OK e, em seguida, clique em OK novamente para criar a VLAN.

22. Clique com o botão direito do Mouse em VLANs na nuvem de dispositivos.
23. Selecione criar VLANs.
24. Insira Native-VLAN como o nome da VLAN nativa.
25. Deixe Comum/Global selecionado.
26. Insira `<<var_native_vlan_id>>` para a ID da VLAN.
27. Clique em OK e, em seguida, clique em OK novamente para criar a VLAN.

28. No painel de navegação, em LAN > políticas, expanda dispositivos e clique com o botão direito do rato em políticas de controlo de rede.
29. Selecione criar política de controlo de rede.
30. Nomeie a política `Enable_CDP_LLPD` e selecione Enabled (habilitado) ao lado de CDP.
31. Ative os recursos de transmissão e receção para LLDP.

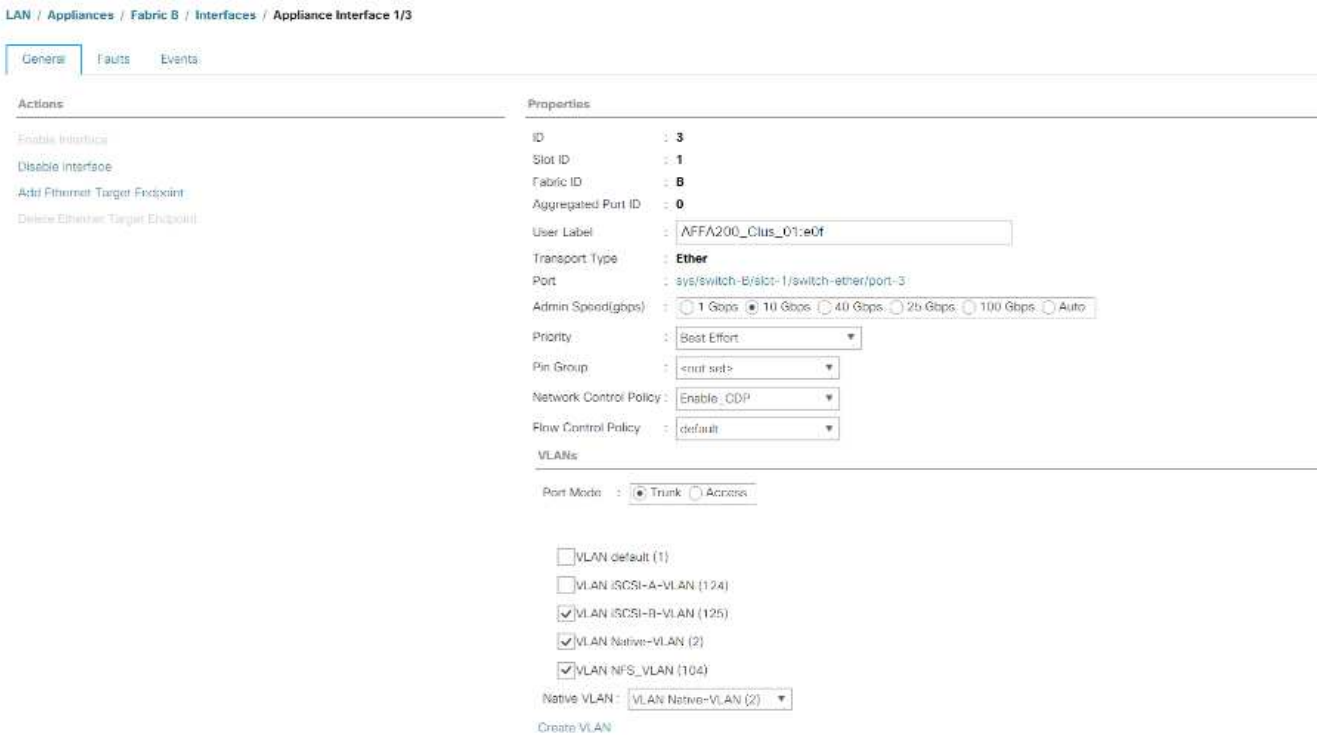


32. Clique em OK e, em seguida, clique em OK novamente para criar a política.
33. No painel de navegação, em LAN > Appliances Cloud, expanda a estrutura A árvore.
34. Expanda as interfaces.
35. Selecione Device Interface 1/3.
36. No campo User Label (Etiqueta do usuário), coloque informações indicando a porta do controlador de armazenamento, como `<storage_controller_01_name>:e0e` o . Clique em Salvar alterações e OK.
37. Selecione a política de controle de rede Enable_CDP e selecione Salvar alterações e OK.
38. Em VLANs, selecione iSCSI-A-VLAN, NFS VLAN e Native VLAN. Defina a Native-VLAN como Native VLAN (VLAN nativa). Limpe a seleção de VLAN padrão.
39. Clique em Salvar alterações e OK.



40. Selecione a Interface do dispositivo 1/4 sob a estrutura A..
41. No campo User Label (Etiqueta do usuário), coloque informações indicando a porta do controlador de armazenamento, como `<storage_controller_02_name>:e0e` o . Clique em Salvar alterações e OK.
42. Selecione a política de controle de rede Enable_CDP e selecione Salvar alterações e OK.
43. Em VLANs, selecione iSCSI-A-VLAN, NFS VLAN e Native VLAN.
44. Defina a Native-VLAN como Native VLAN (VLAN nativa).
45. Limpe a seleção de VLAN padrão.
46. Clique em Salvar alterações e OK.
47. No painel de navegação, em LAN > Appliances Cloud, expanda a árvore da malha B.
48. Expanda as interfaces.
49. Selecione Device Interface 1/3.
50. No campo User Label (Etiqueta do usuário), coloque informações indicando a porta do controlador de armazenamento, como `<storage_controller_01_name>:e0f` o . Clique em Salvar alterações e OK.
51. Selecione a política de controle de rede Enable_CDP e selecione Salvar alterações e OK.
52. Em VLANs, selecione iSCSI-B-VLAN, NFS VLAN e Native VLAN. Defina a Native-VLAN como Native

VLAN (VLAN nativa). Desmarque a VLAN padrão.

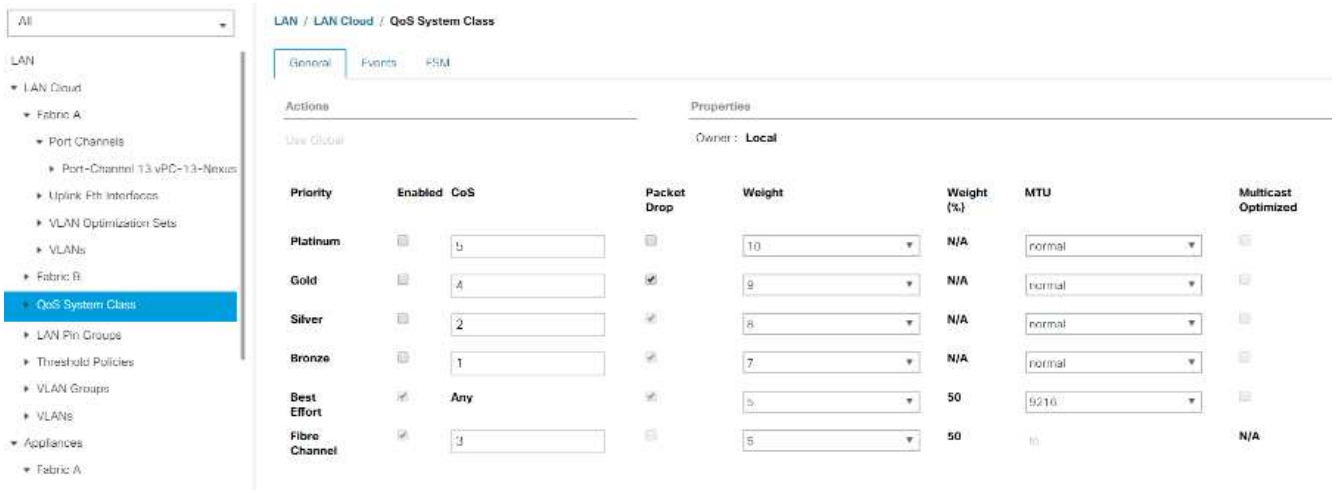


53. Clique em Salvar alterações e OK.
54. Selecione Interface do dispositivo 1/4 sob a tela B.
55. No campo User Label (Etiqueta do usuário), coloque informações indicando a porta do controlador de armazenamento, como `<storage_controller_02_name>:e0f` o . Clique em Salvar alterações e OK.
56. Selecione a política de controle de rede Enable_CDP e selecione Salvar alterações e OK.
57. Em VLANs, selecione iSCSI-B-VLAN, NFS VLAN e Native VLAN. Defina a Native-VLAN como Native VLAN (VLAN nativa). Desmarque a VLAN padrão.
58. Clique em Salvar alterações e OK.

Defina quadros jumbo em tecido Cisco UCS

Para configurar quadros jumbo e habilitar a qualidade do serviço na malha do Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, no painel de navegação, clique na guia LAN.
2. Selecione LAN > LAN Cloud > QoS System Class.
3. No painel direito, clique na guia Geral.
4. Na linha melhor esforço, digite 9216 na caixa sob a coluna MTU.



5. Clique em Salvar alterações.
6. Clique em OK.

Confirme o chassi do Cisco UCS

Para confirmar todos os chassis do Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, selecione a guia Equipamento e expanda a guia Equipamento à direita.
2. Expandir equipamento > chassis.
3. Nas ações para o chassis 1, selecione confirmar chassis.
4. Clique em OK e, em seguida, clique em OK para concluir o reconhecimento do chassi.
5. Clique em Fechar para fechar a janela Propriedades.

Carregue imagens de firmware do Cisco UCS 4,0(1b)

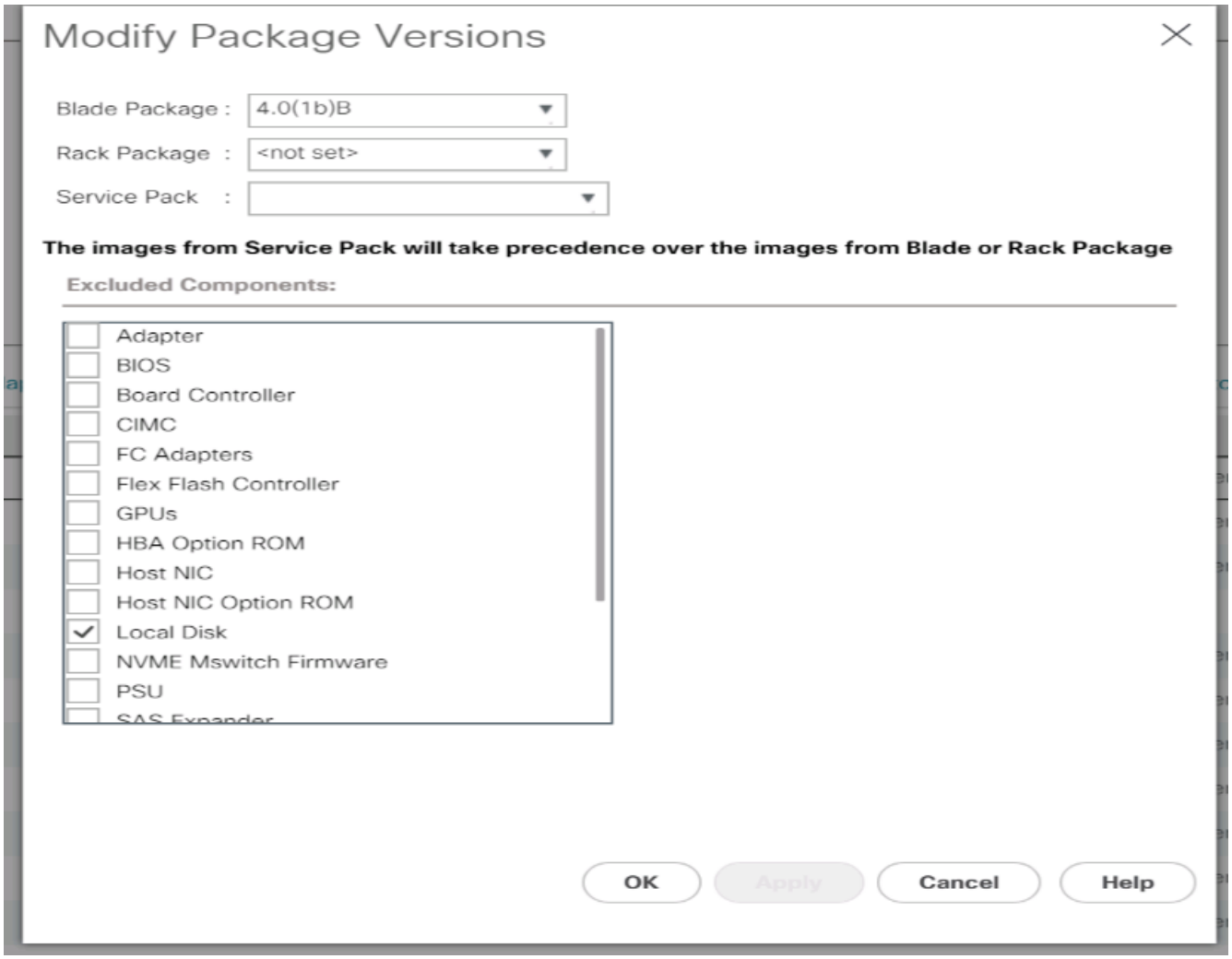
Para atualizar o software do Cisco UCS Manager e o software de interconexão de malha do Cisco UCS para a versão 4,0(1b), "Guias de instalação e atualização do Cisco UCS Manager" consulte a .

Criar pacote de firmware do host

As políticas de gerenciamento de firmware permitem que o administrador selecione os pacotes correspondentes para uma determinada configuração de servidor. Essas políticas geralmente incluem pacotes para adaptador, BIOS, controladora de placa, adaptadores FC, ROM de opção do adaptador de barramento do host (HBA) e propriedades do controlador de armazenamento.

Para criar uma política de gerenciamento de firmware para uma determinada configuração de servidor no ambiente Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione políticas > raiz.
3. Expanda Pacotes de firmware do host.
4. Selecione Default (predefinição).
5. No painel ações, selecione Modificar versões do pacote.
6. Selecione a versão 4,0(1b) para ambos os pacotes Blade.



7. Clique em OK e depois em OK novamente para modificar o pacote de firmware do host.

Criar pools de endereços MAC

Para configurar os pools de endereços MAC necessários para o ambiente Cisco UCS, execute as seguintes etapas:

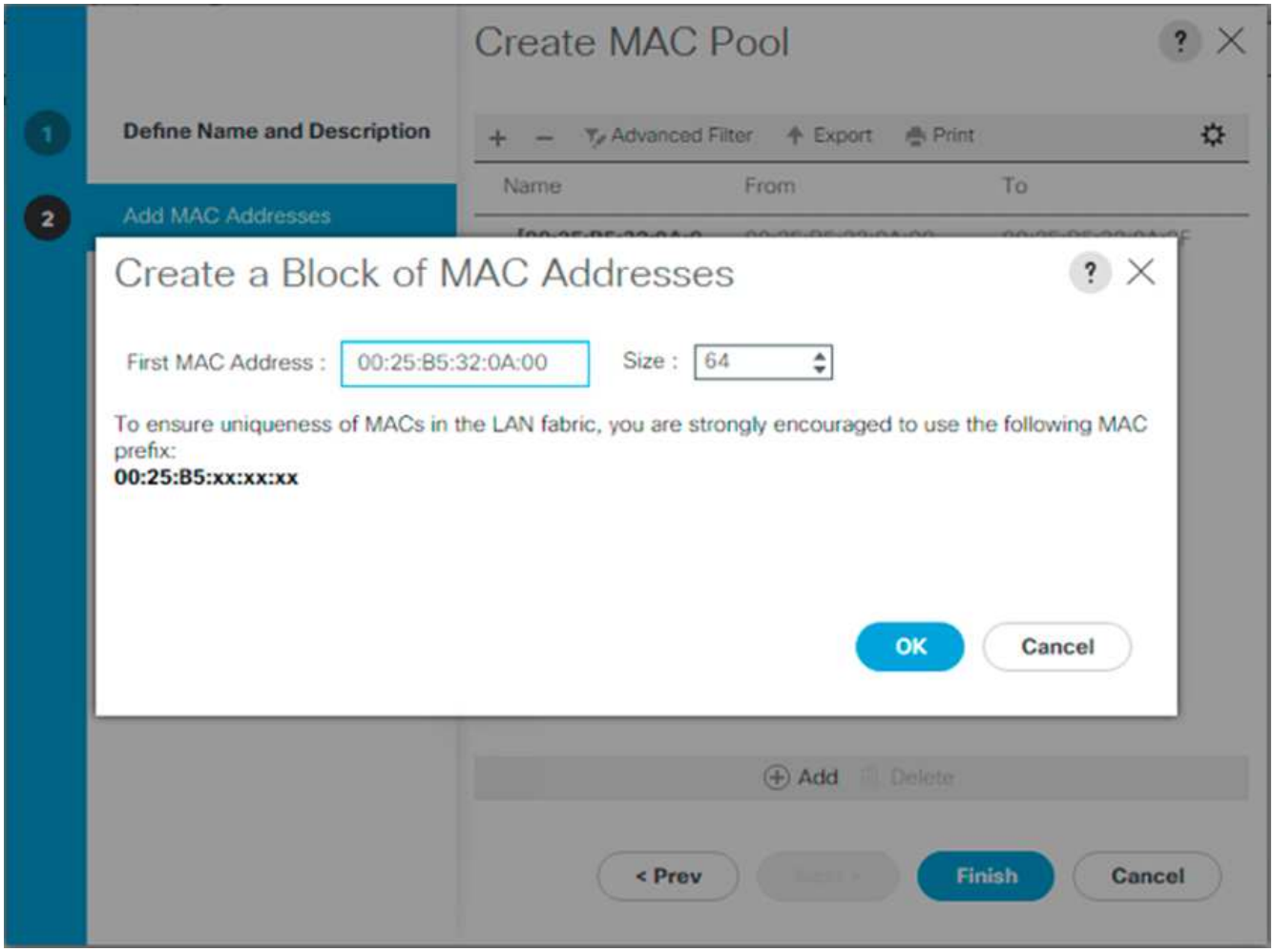
1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Selecione pools > raiz.

   Neste procedimento, dois pools de endereços MAC são criados, um para cada malha de comutação.

3. Clique com o botão direito do Mouse em pools MAC na organização raiz.
4. Selecione criar pool MAC para criar o pool de endereços MAC.
5. Digite MAC-Pool-A como o nome do pool MAC.
6. Opcional: Insira uma descrição para o pool MAC.
7. Selecione sequencial como a opção para Ordem atribuição. Clique em seguinte.
8. Clique em Adicionar.
9. Especifique um endereço MAC inicial.

Para a solução FlexPod, a recomendação é colocar o 0A no próximo ao último octeto do endereço MAC inicial para identificar todos os endereços MAC como endereços de malha A. Em nosso exemplo, nós levamos adiante o exemplo de incorporar também a informação do número de domínio Cisco UCS, dando-nos 00:25:B5:32:0A:00 como nosso primeiro endereço MAC.

10. Especifique um tamanho para o pool de endereços MAC que seja suficiente para suportar os recursos de servidor ou blade disponíveis. Clique em OK.



11. Clique em concluir.
12. Na mensagem de confirmação, clique em OK.
13. Clique com o botão direito do Mouse em pools MAC na organização raiz.
14. Selecione criar pool MAC para criar o pool de endereços MAC.
15. Digite MAC-Pool-B como o nome do pool MAC.
16. Opcional: Insira uma descrição para o pool MAC.
17. Selecione sequencial como a opção para Ordem atribuição. Clique em seguinte.
18. Clique em Adicionar.
19. Especifique um endereço MAC inicial.

Para a solução FlexPod, recomenda-se colocar 0B no próximo ao último octeto do endereço MAC inicial para identificar todos os endereços MAC neste pool como endereços de malha B. Mais uma vez, temos levado adiante em nosso exemplo de incorporar também a informação do número de domínio Cisco UCS dando-nos 00:25:B5:32:0B:00 como nosso primeiro endereço MAC.

20. Especifique um tamanho para o pool de endereços MAC que seja suficiente para suportar os recursos de servidor ou blade disponíveis. Clique em OK.
21. Clique em concluir.
22. Na mensagem de confirmação, clique em OK.

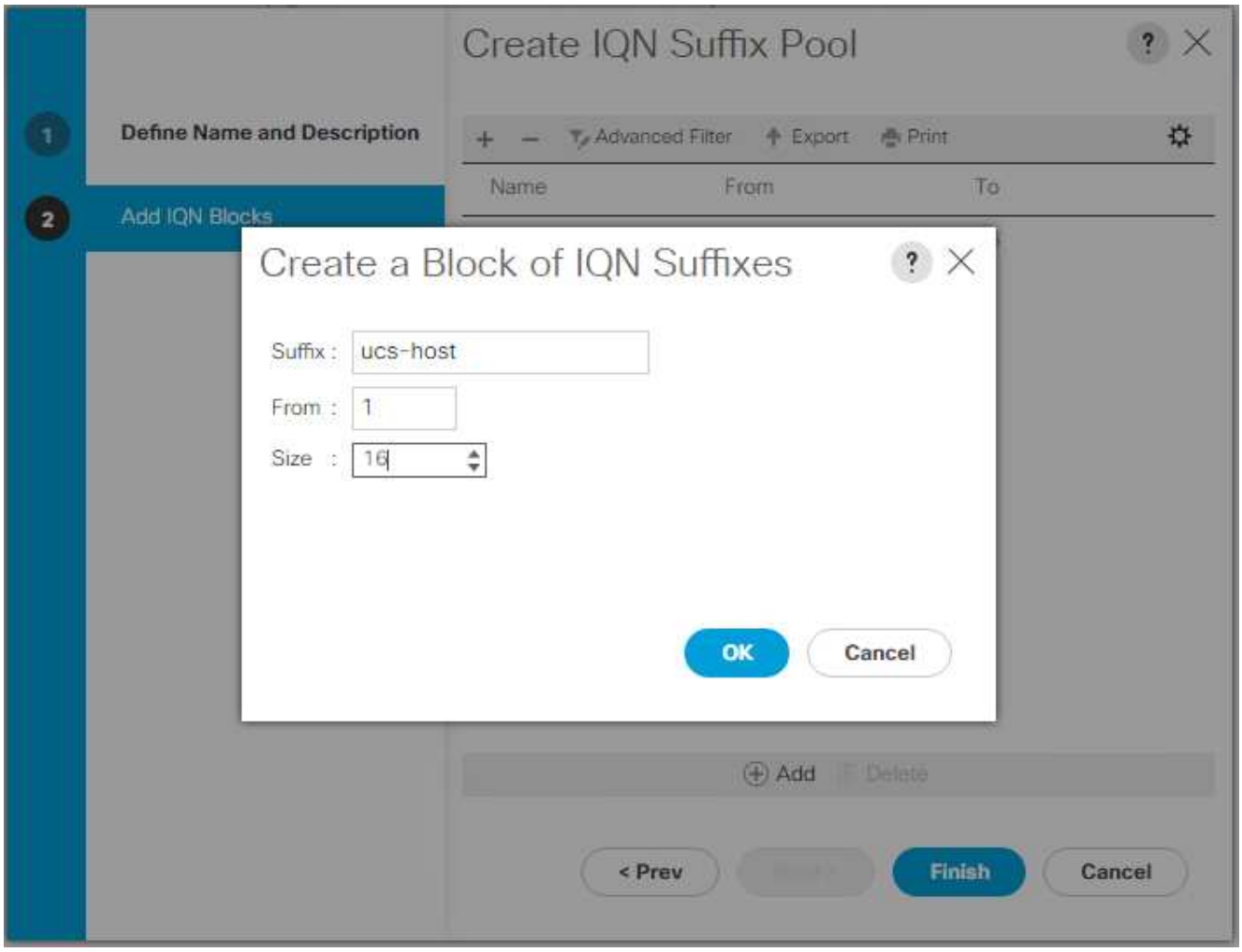
Crie um pool iSCSI IQN

Para configurar os pools IQN necessários para o ambiente do Cisco UCS, execute as seguintes etapas:

1. No Cisco UCS Manager, clique em SAN à esquerda.
2. Selecione pools > raiz.
3. Clique com o botão direito do rato em IQN Pools.
4. Selecione criar pool IQN Suffix para criar o pool IQN.
5. Digite IQN-Pool para o nome do pool IQN.
6. Opcional: Insira uma descrição para o pool IQN.
7. `iqn.1992-08.com.cisco`Introduza como prefixo.
8. Selecione sequencial para Ordem atribuição. Clique em seguinte.
9. Clique em Adicionar.
10. `ucs-host`Introduza como sufixo.

Se vários domínios Cisco UCS estiverem sendo usados, um sufixo IQN mais específico pode precisar ser usado.

11. Introduza 1 no campo de.
12. Especifique o tamanho do bloco IQN suficiente para suportar os recursos do servidor disponíveis. Clique em OK.



13. Clique em concluir.

Criar conjuntos de endereços IP do iniciador iSCSI

Para configurar a inicialização iSCSI de pools IP necessários para o ambiente Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Selecione pools > raiz.
3. Clique com o botão direito do rato em IP Pools.
4. Selecione criar pool IP.
5. Insira iSCSI-IP-Pool-A como o nome do pool IP.
6. Opcional: Insira uma descrição para o pool IP.
7. Selecione sequencial para a ordem de atribuição. Clique em seguinte.
8. Clique em Adicionar para adicionar um bloco de endereço IP.
9. No campo de, introduza o início do intervalo a atribuir como endereços IP iSCSI.
10. Defina o tamanho para endereços suficientes para acomodar os servidores. Clique em OK.
11. Clique em seguinte.
12. Clique em concluir.

13. Clique com o botão direito do rato em IP Pools.
14. Selecione criar pool IP.
15. Insira iSCSI-IP-Pool-B como o nome do pool IP.
16. Opcional: Insira uma descrição para o pool IP.
17. Selecione sequencial para a ordem de atribuição. Clique em seguinte.
18. Clique em Adicionar para adicionar um bloco de endereço IP.
19. No campo de, introduza o início do intervalo a atribuir como endereços IP iSCSI.
20. Defina o tamanho para endereços suficientes para acomodar os servidores. Clique em OK.
21. Clique em seguinte.
22. Clique em concluir.

Criar conjunto de sufixos UUID

Para configurar o conjunto de sufixo UUID (identificador universal único) necessário para o ambiente Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione pools > raiz.
3. Clique com o botão direito do rato em conjuntos de sufixos UUID.
4. Selecione criar conjunto sufixo UUID.
5. Digite UUID-Pool como o nome do conjunto de sufixos UUID.
6. Opcional: Insira uma descrição para o conjunto de sufixos UUID.
7. Mantenha o prefixo na opção derivada.
8. Selecione sequencial para a Ordem atribuição.
9. Clique em seguinte.
10. Clique em Adicionar para adicionar um bloco de UUIDs.
11. Mantenha o campo de na predefinição.
12. Especifique um tamanho para o bloco UUID que seja suficiente para suportar os recursos de servidor ou blade disponíveis. Clique em OK.
13. Clique em concluir.
14. Clique em OK.

Criar pool de servidores

Para configurar o pool de servidores necessário para o ambiente do Cisco UCS, execute as seguintes etapas:

> Considere a criação de pools de servidores exclusivos para obter a granularidade necessária no seu ambiente.

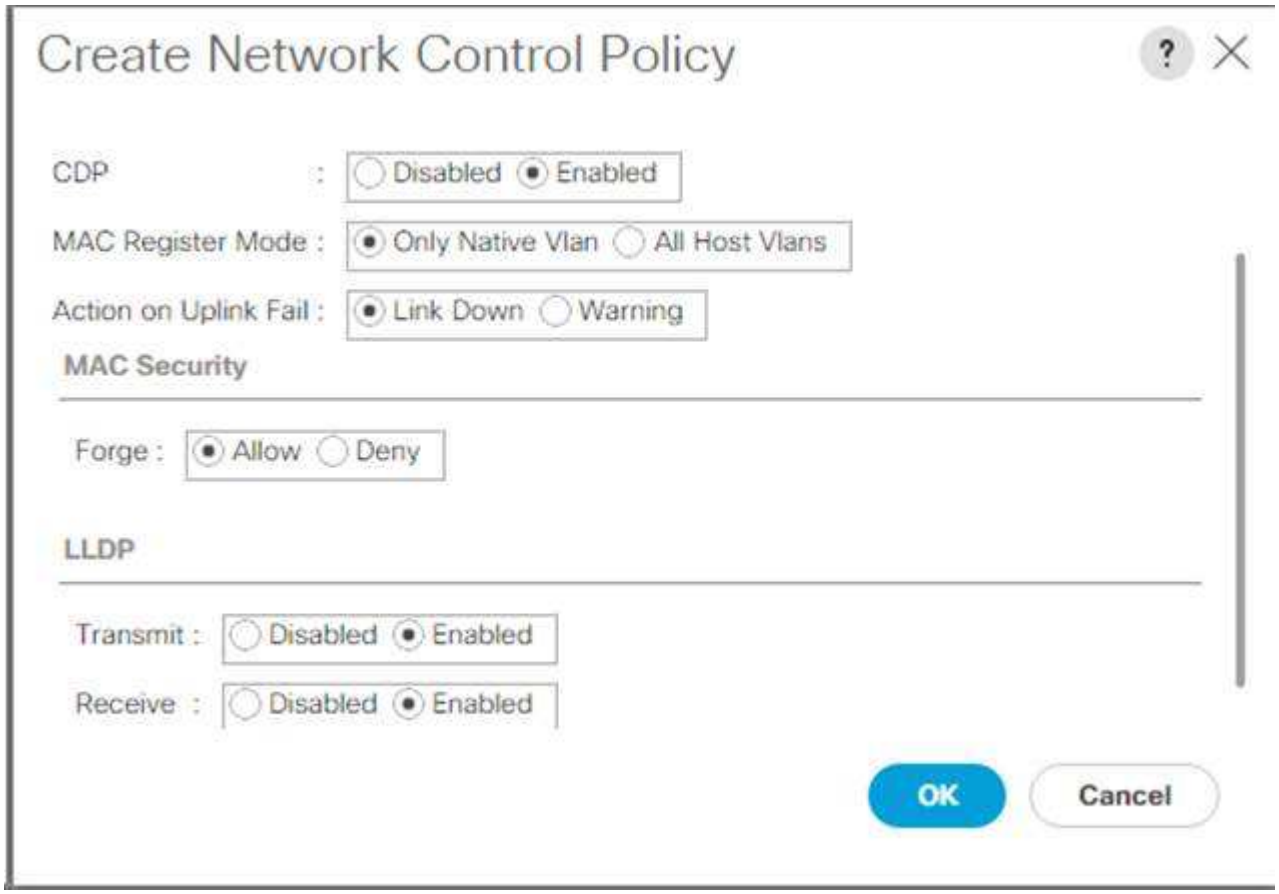
1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione pools > raiz.
3. Clique com o botão direito do rato em pools de servidores.

4. Selecione criar pool de servidores.
5. Digite "infra-Pool" como o nome do pool de servidores.
6. Opcional: Insira uma descrição para o pool de servidores. Clique em seguinte.
7. Selecione dois (ou mais) servidores a serem usados para o cluster de gerenciamento VMware e clique em >> para adicioná-los ao pool de serviços "infra-Pool".
8. Clique em concluir.
9. Clique em OK.

Criar política de controle de rede para o Protocolo de descoberta de Cisco e o Protocolo de descoberta de camada de enlace

Para criar uma Política de Controle de rede para o Protocolo de descoberta de Cisco (CDP) e Protocolo de descoberta de camada de enlace (LLDP), execute as seguintes etapas:

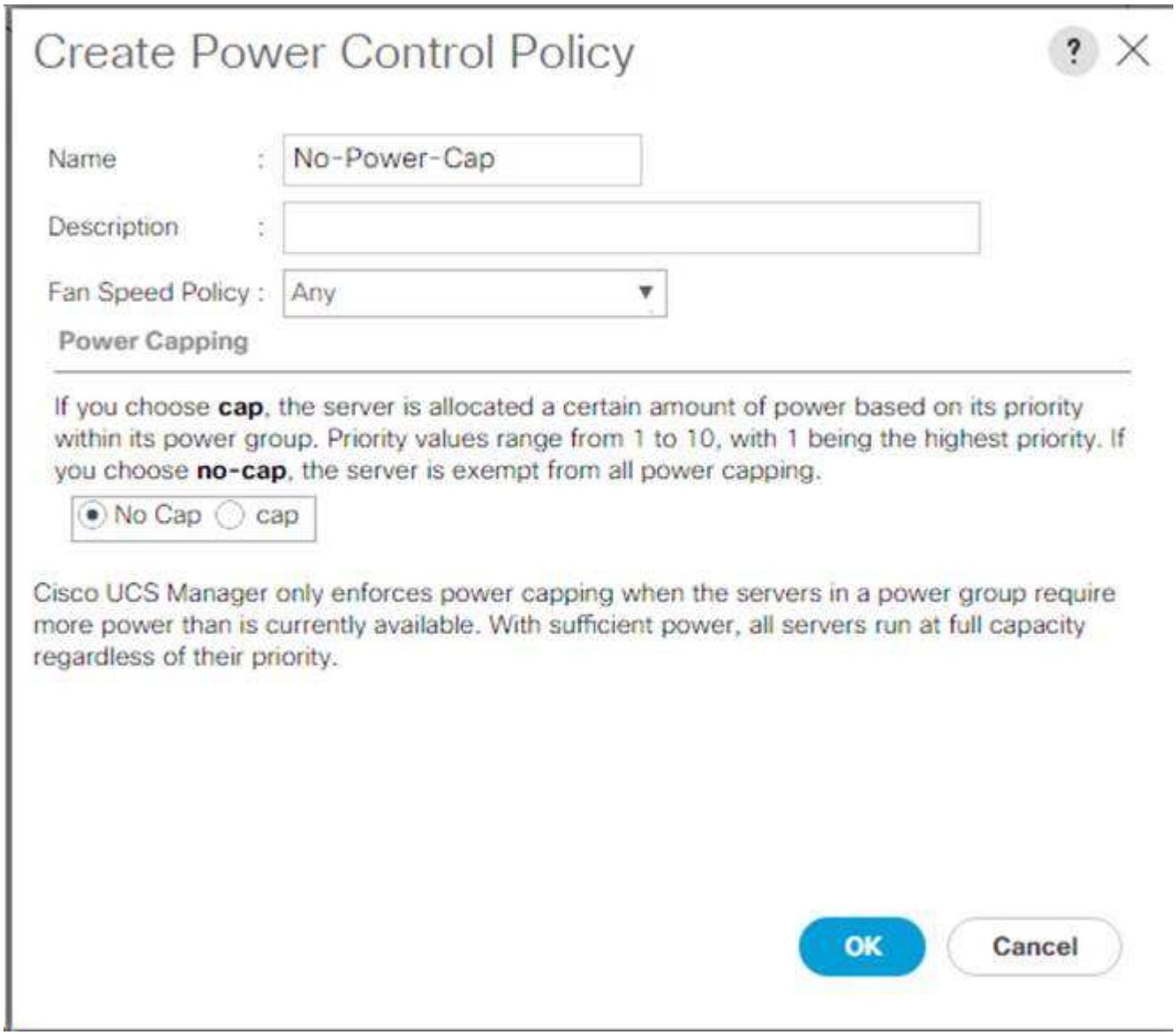
1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em políticas de controlo de rede.
4. Selecione criar política de controlo de rede.
5. Introduza o nome da política Enable-CDP-LLDP.
6. Para CDP, selecione a opção Enabled (activado).
7. Para LLDP, role para baixo e selecione habilitado para transmissão e recebimento.
8. Clique em OK para criar a política de controle de rede. Clique em OK.



Criar política de controle de energia

Para criar uma política de controle de energia para o ambiente do Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique na guia servidores à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em políticas de controlo de energia.
4. Selecione criar política de controlo de energia.
5. Introduza no-Power-Cap como o nome da política de controlo de energia.
6. Altere a definição de limitação de energia para sem tampa.
7. Clique em OK para criar a política de controle de energia. Clique em OK.

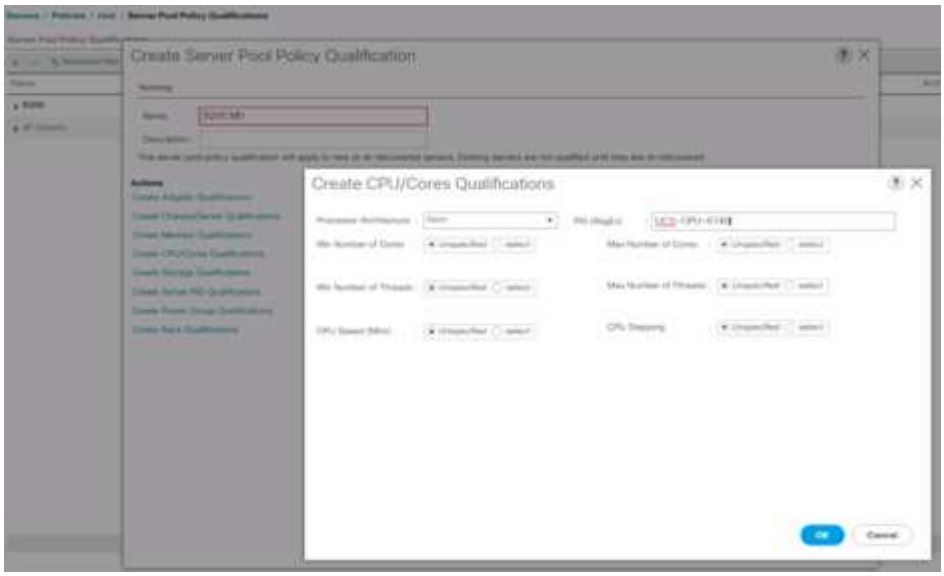


Criar política de qualificação de pool de servidores (Opcional)

Para criar uma política de qualificação de pool de servidor opcional para o ambiente do Cisco UCS, execute as seguintes etapas:

Este exemplo cria uma política para servidores Cisco UCS B-Series com os processadores Intel E2660 v4 Xeon Broadwell.

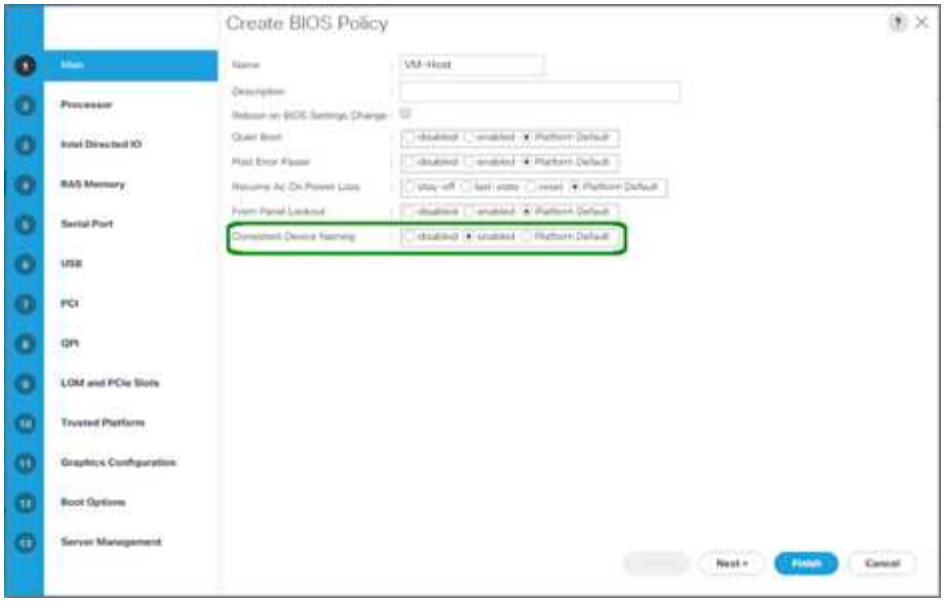
1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione políticas > raiz.
3. Selecione Qualificações de políticas de pool de servidores.
4. Selecione criar Qualificação de políticas de pool de servidores ou Adicionar.
5. Nomeie a política Intel.
6. Selecione criar CPU/cores Qualificações.
7. Selecione Xeon para o processador/arquitetura.
8. `<UCS-CPU- PID>`Introduza como ID do processo (PID).
9. Clique em OK para criar a qualificação CPU/núcleo.
10. Clique em OK para criar a política e, em seguida, clique em OK para confirmar.



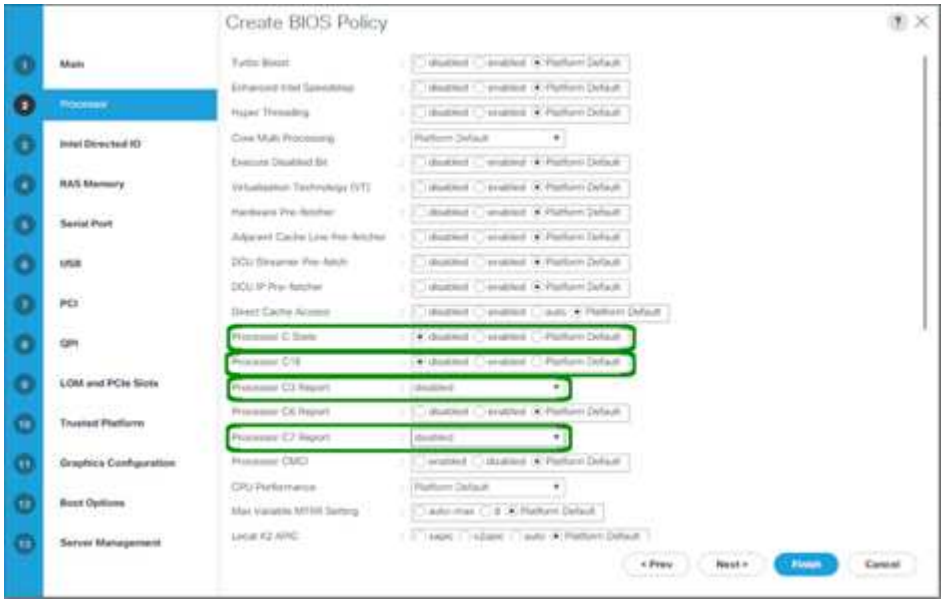
Criar política de BIOS de servidor

Para criar uma política de BIOS de servidor para o ambiente Cisco UCS, execute as seguintes etapas:

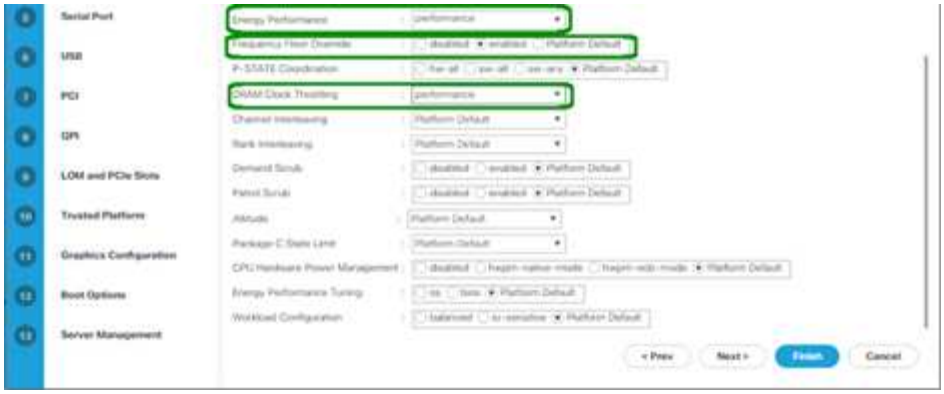
1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em políticas do BIOS.
4. Selecione criar política do BIOS.
5. Insira VM-Host como o nome da política do BIOS.
6. Altere a configuração Quiet Boot (Inicialização silenciosa) para Disabled (desativada).
7. Altere Nome de dispositivo consistente para ativado.



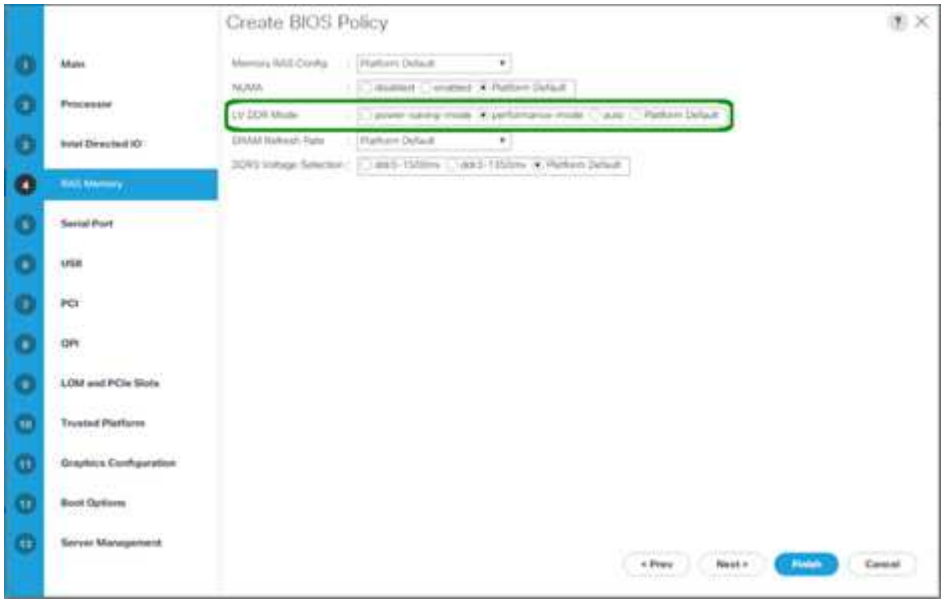
8. Selecione a guia processador e defina os seguintes parâmetros:
   - Estado C do processador: Desativado
   - Processador C1E: Desativado
   - Relatório do processador C3: Desativado
   - Relatório do processador C7: Desativado



9. Role para baixo até as opções restantes do processador e defina os seguintes parâmetros:
   - Desempenho energético: Desempenho
   - Anulação do piso de frequência: Ativada
   - DRAM Clock throttling: Desempenho



10. Clique em memória RAS e defina os seguintes parâmetros:
    - Modo DDR LV: Modo de desempenho

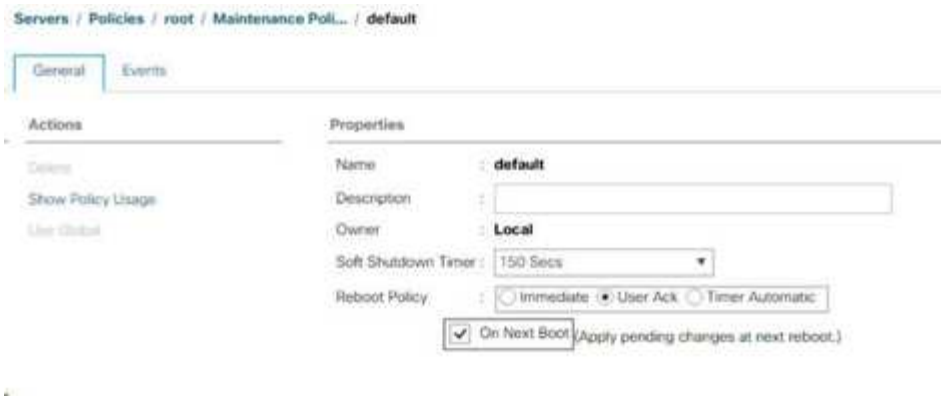


11. Clique em concluir para criar a política do BIOS.
12. Clique em OK.

Atualize a política de manutenção predefinida

Para atualizar a Política de Manutenção padrão, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione políticas > raiz.
3. Selecione políticas de manutenção > predefinição.
4. Altere a Política de reinicialização para User Ack.
5. Selecione na próxima inicialização para delegar janelas de manutenção aos administradores do servidor.



6. Clique em Salvar alterações.
7. Clique em OK para aceitar a alteração.

Crie modelos vNIC

Para criar vários modelos de placa de interface de rede virtual (vNIC) para o ambiente Cisco UCS, execute os procedimentos descritos nesta seção.

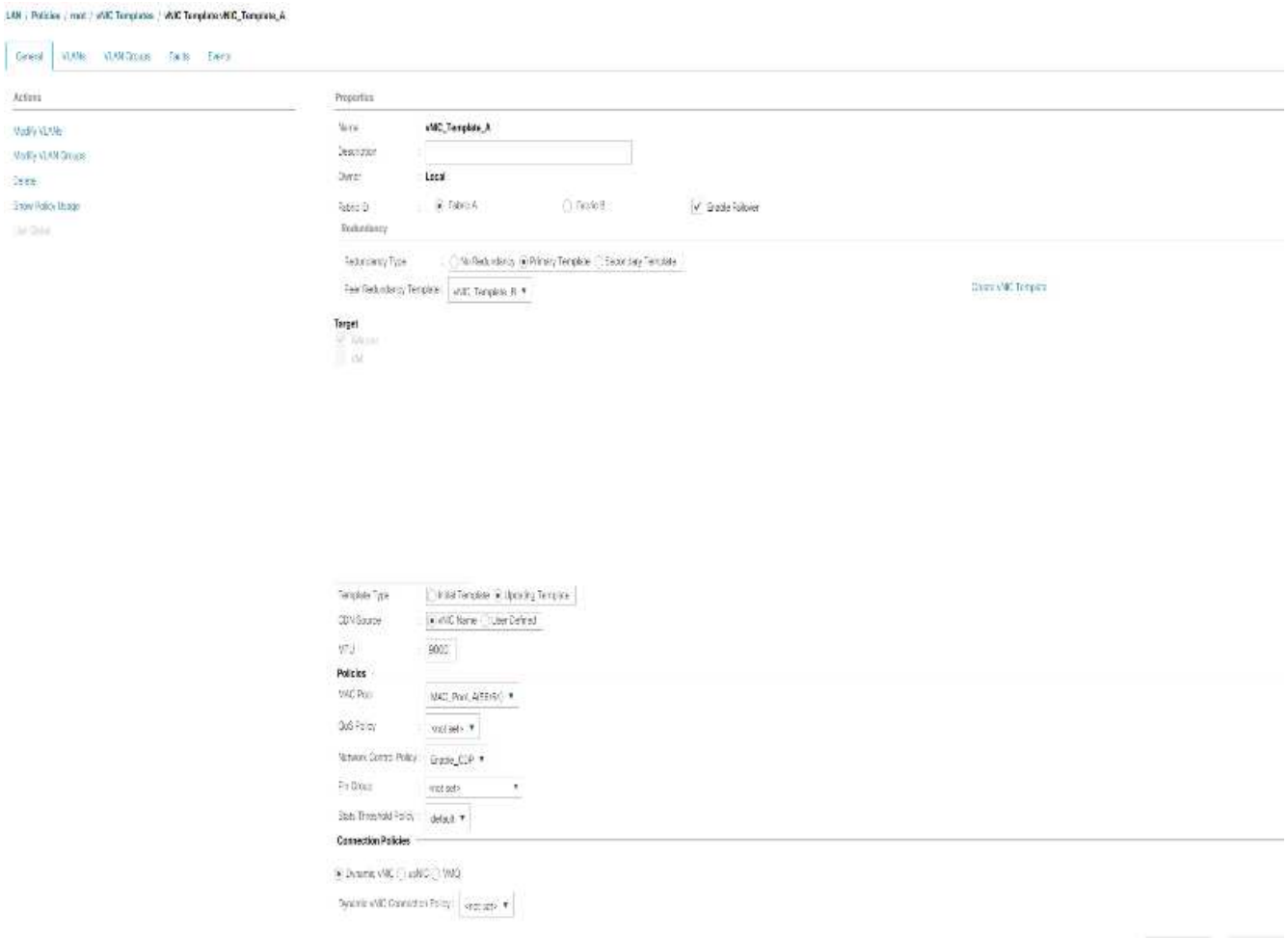
Um total de quatro modelos vNIC são criados.

Crie vNICs de infraestrutura

Para criar uma infraestrutura vNIC, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em modelos vNIC.
4. Selecione criar modelo vNIC.
5. Digite `Site-XX-vNIC_A` como o nome do modelo vNIC.
6. Selecione Atualizar modelo como o tipo de modelo.
7. Para ID de tecido, selecione tecido
8. Certifique-se de que a opção Ativar failover não está selecionada.
9. Selecione modelo primário para tipo de redundância.
10. Deixe o modelo de redundância de pares definido como `<not set>`.
11. Em Target (alvo), certifique-se de que apenas a opção Adapter (adaptador) está selecionada.
12. Defina `Native-VLAN` como VLAN nativa.
13. Selecione Nome vNIC para a origem CDN.
14. Para MTU, introduza 9000.
15. Em VLANs permitidas, selecione `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic` e Site-XX-vMotion. Use a tecla Ctrl para fazer essa seleção múltipla.
16. Clique em Selecionar. Essas VLANs agora devem aparecer em VLANs selecionadas.
17. Na lista pool MAC, `MAC_Pool_A`selecione .

18. Na lista Diretiva de Controle de rede, selecione Pool-A.
19. Na lista Network Control Policy (Política de controlo de rede), selecione Enable-CDP-LLDP (Ativar-CDP-LLDP).
20. Clique em OK para criar o modelo vNIC.
21. Clique em OK.

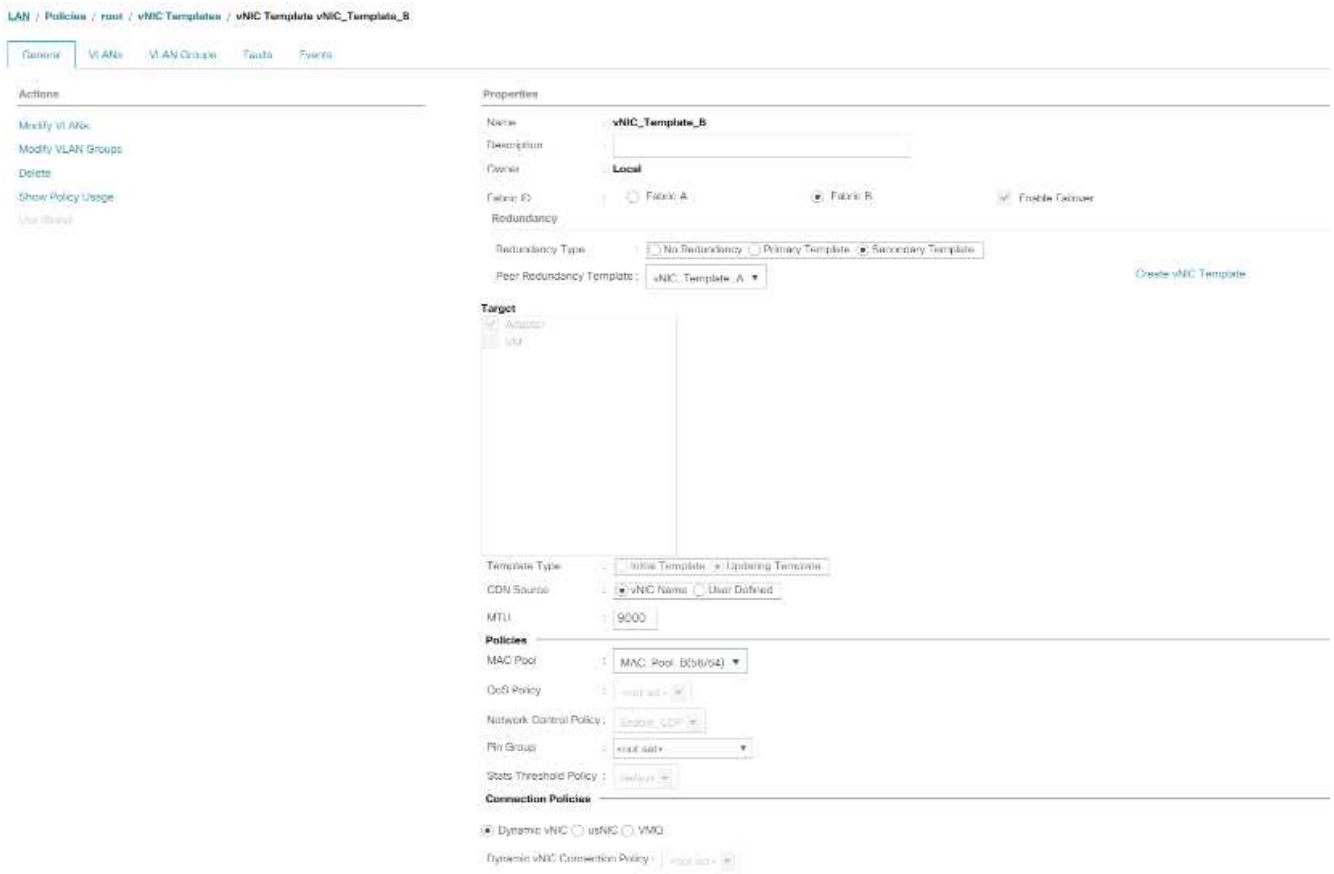


Para criar o modelo de redundância secundária infra-B, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em modelos vNIC.
4. Selecione criar modelo vNIC.
5. Digite 'Site-XX-vNIC_B' como o nome do modelo vNIC.
6. Selecione Atualizar modelo como o tipo de modelo.
7. Para ID de tecido, selecione tecido B..
8. Selecione a opção Ativar failover.

Selecionar failover é uma etapa crítica para melhorar o tempo de failover de link, manipulando-o no nível de hardware e para proteger contra qualquer potencial de falha de NIC não ser detetada pelo switch virtual.

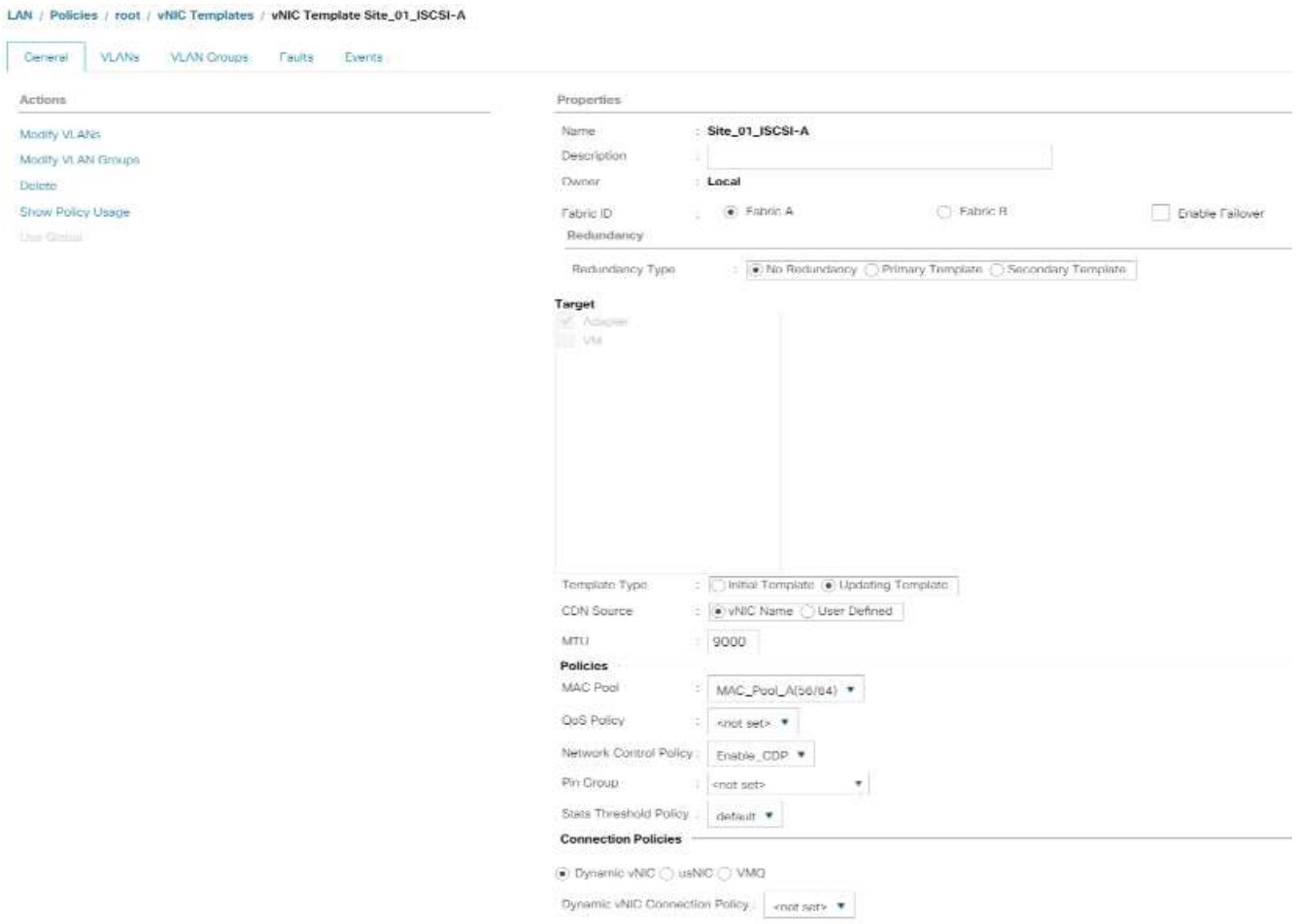
9. Selecione modelo primário para tipo de redundância.
10. Deixe o modelo de redundância de pares definido como `vNIC_Template_A`.
11. Em Target (alvo), certifique-se de que apenas a opção Adapter (adaptador) está selecionada.
12. Defina `Native-VLAN` como VLAN nativa.
13. Selecione Nome vNIC para a origem CDN.
14. Para MTU, introduza `9000`.
15. Em VLANs permitidas, selecione `Native-VLAN, Site-XX-IB-MGMT, Site-XX-NFS, Site-XX-VM-Traffic` e Site-XX-vMotion. Use a tecla Ctrl para fazer essa seleção múltipla.
16. Clique em Selecionar. Essas VLANs agora devem aparecer em VLANs selecionadas.
17. Na lista pool MAC, `MAC_Pool_B`selecione .
18. Na lista Diretiva de Controle de rede, selecione Pool-B.
19. Na lista Network Control Policy (Política de controlo de rede), selecione Enable-CDP-LLDP (Ativar-CDP-LLDP).
20. Clique em OK para criar o modelo vNIC.
21. Clique em OK.



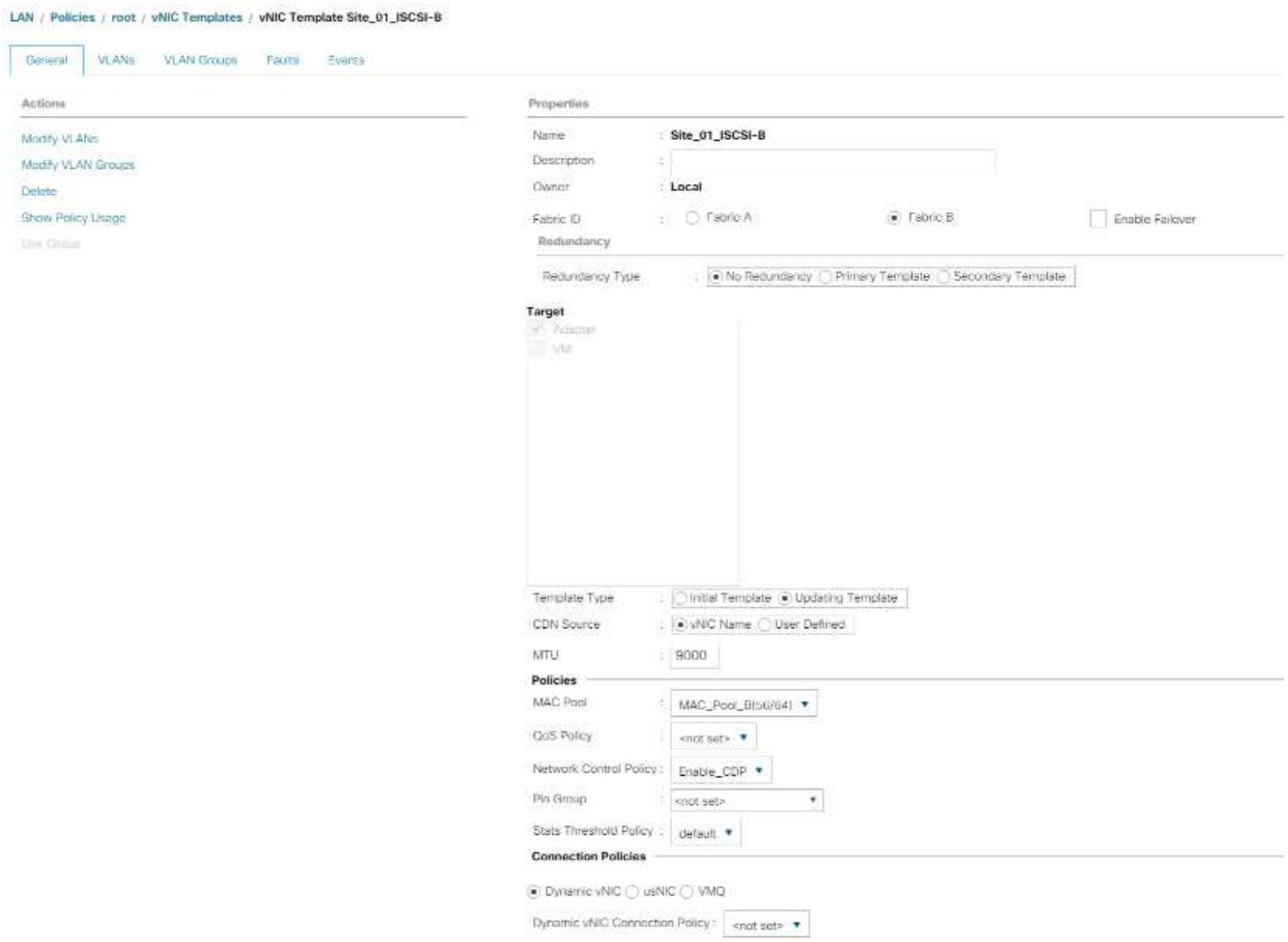
Criar iSCSI vNICs

Para criar iSCSI vNICs, execute as seguintes etapas:

1. Selecione LAN à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em modelos vNIC.
4. Selecione criar modelo vNIC.
5. Digite `Site- 01-iSCSI_A` como o nome do modelo vNIC.
6. Selecione tecido A. não selecione a opção Ativar failover.
7. Deixe o tipo de redundância definido como sem redundância.
8. Em Target (alvo), certifique-se de que apenas a opção Adapter (adaptador) está selecionada.
9. Selecione Atualizar modelo para tipo modelo.
10. Em VLANs, selecione somente Site- 01-iSCSI_A_VLAN.
11. Selecione Site- 01-iSCSI_A_VLAN como VLAN nativa.
12. Deixe o nome vNIC definido para a origem CDN.
13. Em MTU, introduza 9000.
14. Na lista pool MAC, selecione MAC-Pool-A.
15. Na lista Network Control Policy (Política de controlo de rede), selecione Enable-CDP-LLDP (Ativar-CDP-LLDP).
16. Clique em OK para concluir a criação do modelo vNIC.
17. Clique em OK.



18. Selecione LAN à esquerda.
19. Selecione políticas > raiz.
20. Clique com o botão direito do rato em modelos vNIC.
21. Selecione criar modelo vNIC.
22. Digite `Site- 01-iSCSI_B` como o nome do modelo vNIC.
23. Selecione tecido B. não selecione a opção Ativar failover.
24. Deixe o tipo de redundância definido como sem redundância.
25. Em Target (alvo), certifique-se de que apenas a opção Adapter (adaptador) está selecionada.
26. Selecione Atualizar modelo para tipo modelo.
27. Em VLANs, selecione somente `Site- 01-iSCSI_B_VLAN`.
28. `Site- 01-iSCSI_B_VLAN`Selecione como VLAN nativa.
29. Deixe o nome vNIC definido para a origem CDN.
30. Em MTU, introduza 9000.
31. Na lista pool MAC, `MAC-Pool-B`selecione .
32. Na lista Network Control Policy (Política de controlo de rede), `Enable-CDP-LLDP` selecione .
33. Clique em OK para concluir a criação do modelo vNIC.
34. Clique em OK.



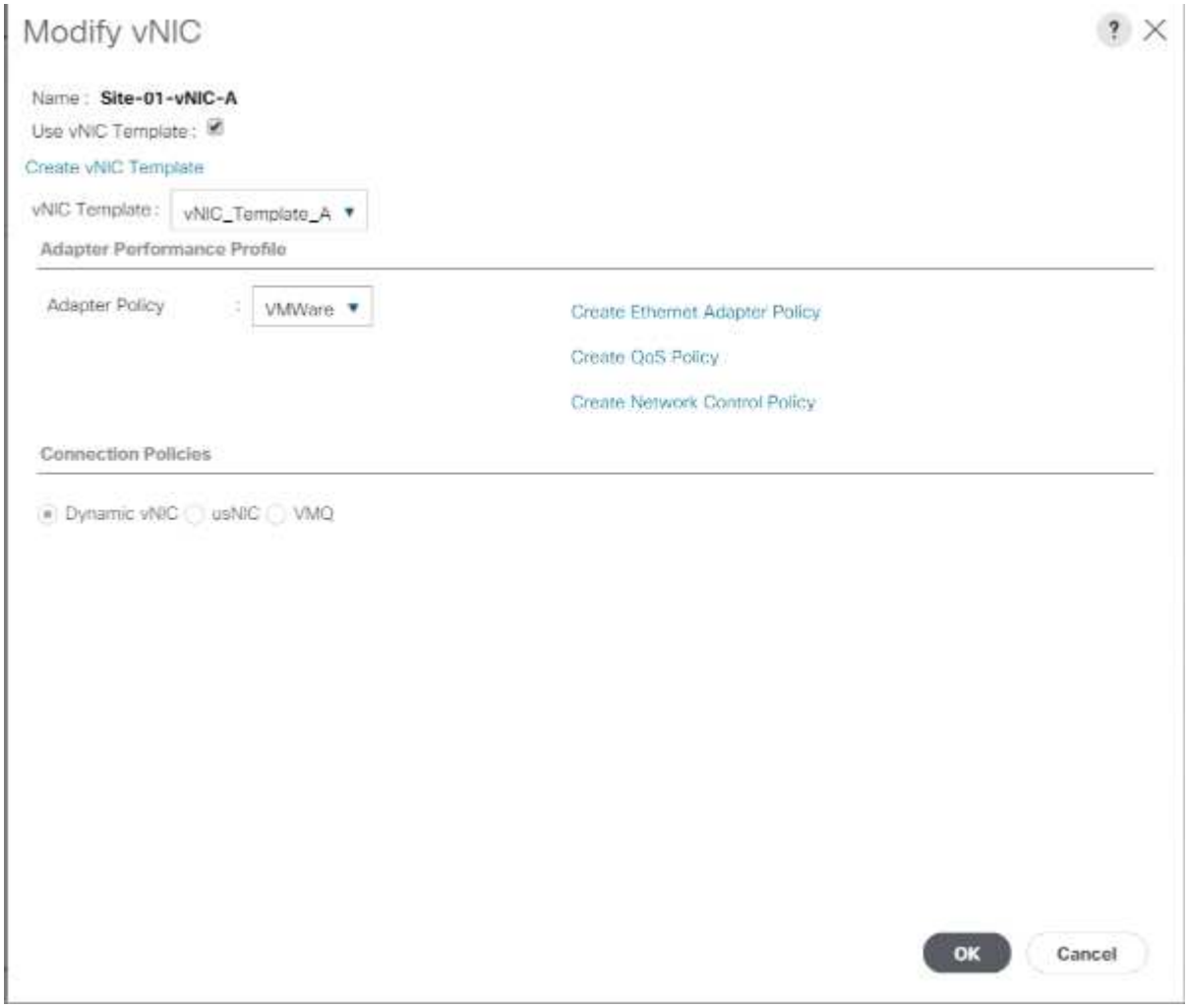
Criar política de conetividade LAN para inicialização iSCSI

Este procedimento aplica-se a um ambiente Cisco UCS no qual duas LIFs iSCSI estão no nó de cluster 1 (`iscsi_lif01a` e `iscsi_lif01b`) e duas LIFs iSCSI estão no nó de cluster 2 (`iscsi_lif02a` e `iscsi_lif02b`). Além disso, supõe-se que os LIFs A são conetados à malha A (Cisco UCS 6324 A) e que os LIFs B são conetados à malha B (Cisco UCS 6324 B).

Para configurar a Política de conetividade de LAN de infra-estrutura necessária, execute as seguintes etapas:

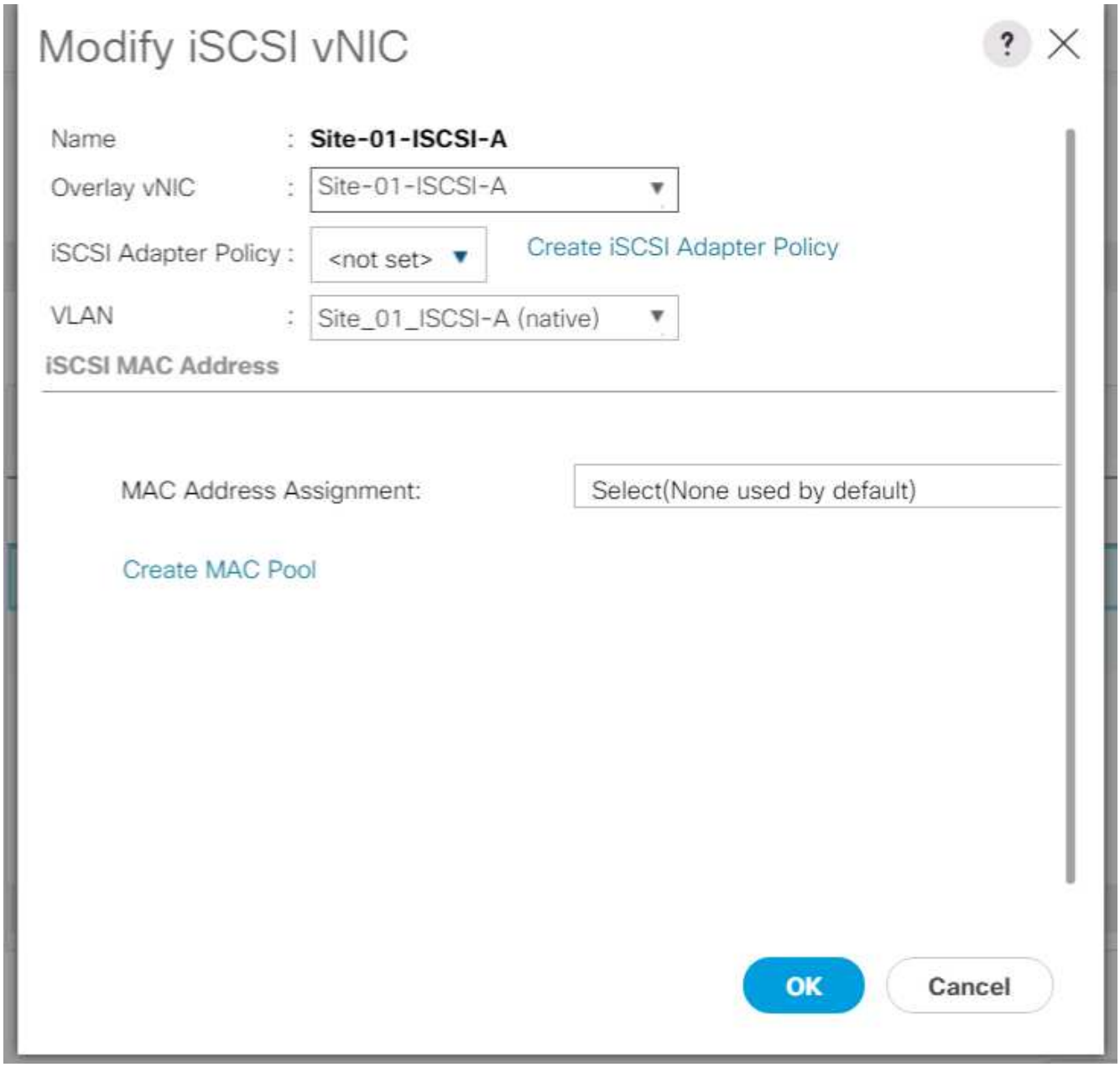
1. No Gerenciador Cisco UCS, clique em LAN à esquerda.
2. Selecione LAN > políticas > raiz.
3. Clique com o botão direito do rato em políticas de conetividade LAN.
4. Selecione criar política de conetividade LAN.
5. Introduza `Site-XX-Fabric-A` como o nome da política.
6. Clique na opção superior Adicionar para adicionar um vNIC.
7. Na caixa de diálogo criar vNIC, digite `Site-01-vNIC-A` como o nome do vNIC.
8. Selecione a opção usar modelo vNIC.
9. Na lista modelo vNIC , `vNIC_Template_A` selecione .

10. Na lista suspensa Política de adaptador, selecione VMware.
11. Clique em OK para adicionar este vNIC à política.

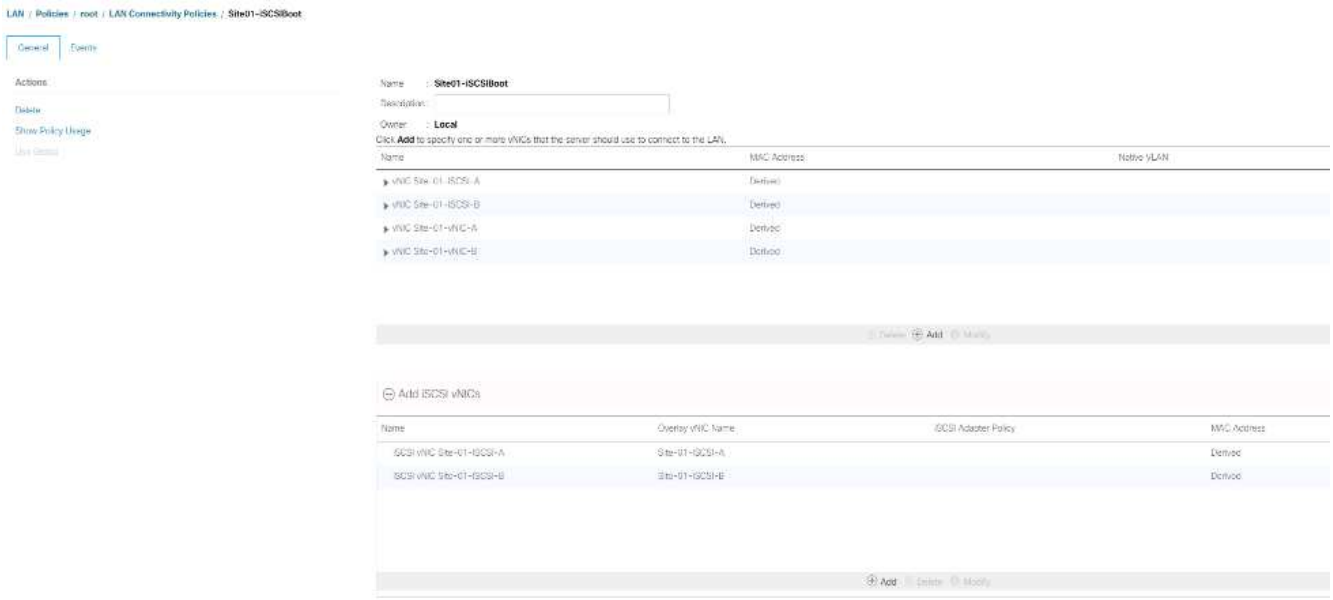


12. Clique na opção superior Adicionar para adicionar um vNIC.
13. Na caixa de diálogo criar vNIC, digite `Site-01-vNIC-B` como o nome do vNIC.
14. Selecione a opção usar modelo vNIC.
15. Na lista modelo vNIC , `vNIC_Template_B` selecione .
16. Na lista suspensa Política de adaptador, selecione VMware.
17. Clique em OK para adicionar este vNIC à política.
18. Clique na opção superior Adicionar para adicionar um vNIC.
19. Na caixa de diálogo criar vNIC, digite `Site-01- iSCSI-A` como o nome do vNIC.
20. Selecione a opção usar modelo vNIC.
21. Na lista modelo vNIC , `Site-01-iSCSI-A` selecione .
22. Na lista suspensa Política de adaptador, selecione VMware.
23. Clique em OK para adicionar este vNIC à política.
24. Clique na opção superior Adicionar para adicionar um vNIC.

25. Na caixa de diálogo criar vNIC, digite `Site-01-iSCSI-B` como o nome do vNIC.
26. Selecione a opção usar modelo vNIC.
27. Na lista modelo vNIC , `Site-01-iSCSI-B` selecione .
28. Na lista suspensa Política de adaptador, selecione VMware.
29. Clique em OK para adicionar este vNIC à política.
30. Expanda a opção Add iSCSI vNICs (Adicionar iSCSI vNICs).
31. Clique na opção Adicionar inferior no espaço Adicionar iSCSI vNICs para adicionar o iSCSI vNIC.
32. Na caixa de diálogo criar iSCSI vNIC, digite `Site-01-iSCSI-A` como o nome do vNIC.
33. Selecione a opção Overlay vNIC como `Site-01-iSCSI-A`.
34. Deixe a opção iSCSI Adapter Policy (Política do adaptador iSCSI) para não definir.
35. Selecione a VLAN como `Site-01-iSCSI-Site-A` (nativa).
36. Selecione nenhum (usado por padrão) como atribuição de endereço MAC.
37. Clique em OK para adicionar o iSCSI vNIC à política.



38. Clique na opção Adicionar inferior no espaço Adicionar iSCSI vNICs para adicionar o iSCSI vNIC.
39. Na caixa de diálogo criar iSCSI vNIC, digite `Site-01-iSCSI-B` como o nome do vNIC.
40. Selecione a opção Overlay vNIC como Site-01-iSCSI-B.
41. Deixe a opção iSCSI Adapter Policy (Política do adaptador iSCSI) para não definir.
42. Selecione a VLAN como `Site-01-iSCSI-Site-B` (nativa).
43. Selecione nenhum (usado por padrão) como atribuição de endereço MAC.
44. Clique em OK para adicionar o iSCSI vNIC à política.
45. Clique em Salvar alterações.



Criar política vMedia para o arranque de instalação do VMware ESXi 6.7U1

Nas etapas de configuração do NetApp Data ONTAP é necessário um servidor web HTTP, que é usado para hospedar o NetApp Data ONTAP e o software VMware. A política vMedia criada aqui mapeia o VMware ESXi 6. 7U1 ISO para o servidor Cisco UCS para inicializar a instalação ESXi. Para criar esta política, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, selecione servidores à esquerda.
2. Selecione políticas > raiz.
3. Selecione políticas vMedia.
4. Clique em Adicionar para criar nova política vMedia.
5. Nomeie a política ESXi-6.7U1-HTTP.
6. Digite Mounts ISO for ESXi 6.7U1 no campo Description (Descrição).
7. Selecione Yes (Sim) para tentar novamente em caso de falha de montagem.
8. Clique em Adicionar.
9. Nomeie a montagem ESXi-6.7U1-HTTP.
10. Selecione o tipo de dispositivo CDD.
11. Selecione o protocolo HTTP.
12. Introduza o endereço IP do servidor Web.

> Os IPs do servidor DNS não foram inseridos no IP KVM anteriormente, portanto, é necessário inserir o IP do servidor Web em vez do nome do host.

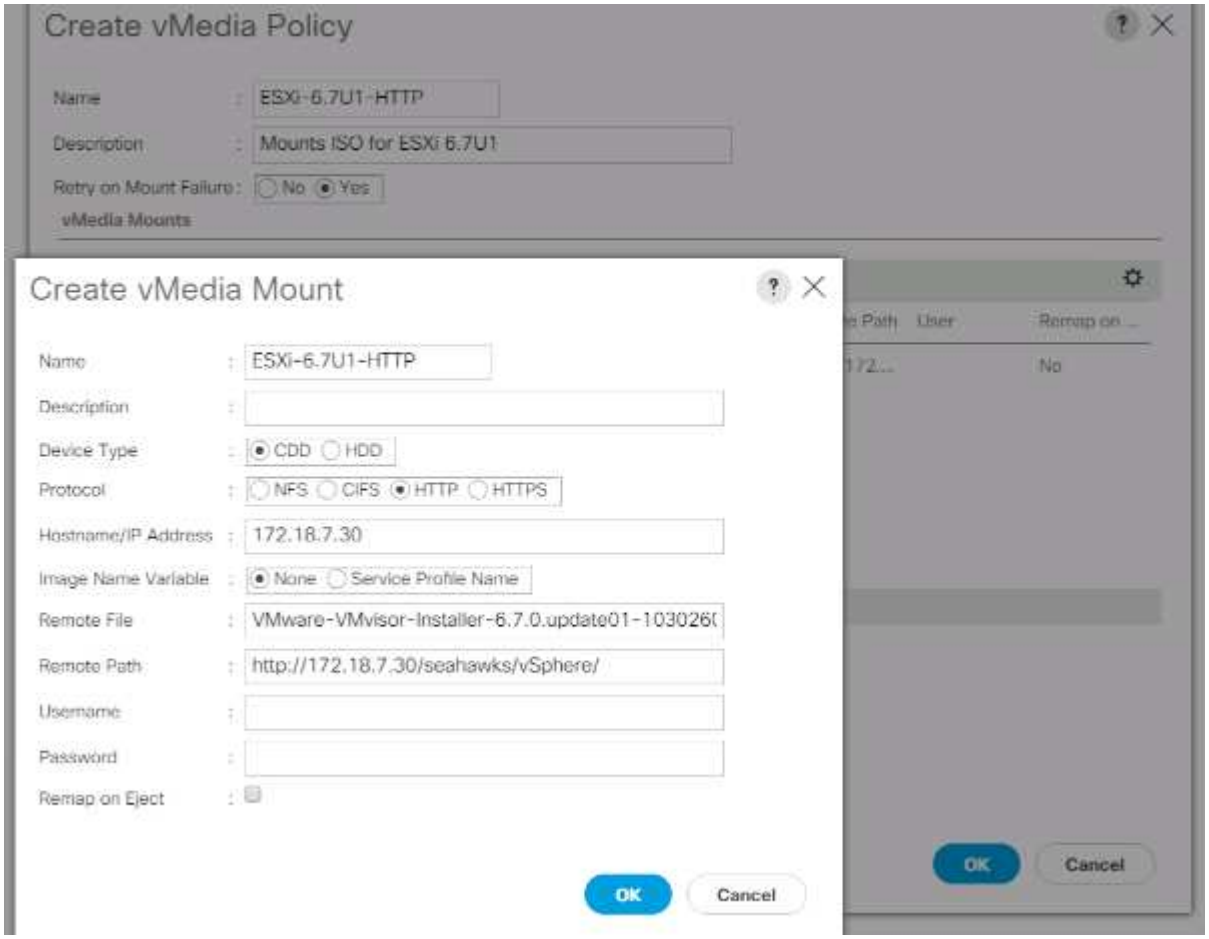
13. `VMware-VMvisor-Installer-6.7.0.update01-10302608.x86_64.iso`Introduza como o nome do ficheiro remoto.

    Este ISO do VMware ESXi 6.7U1 pode ser baixado do "Downloads da VMware".

14. Introduza o caminho do servidor Web para o ficheiro ISO no campo caminho remoto.

15. Clique em OK para criar o suporte vMedia.
16. Clique em OK e depois em OK novamente para concluir a criação da política vMedia.

    Para todos os novos servidores adicionados ao ambiente do Cisco UCS, o modelo de perfil de serviço vMedia pode ser usado para instalar o host ESXi. Na primeira inicialização, o host inicializa no instalador ESXi, já que o disco montado na SAN está vazio. Após a instalação do ESXi, o vMedia não é referenciado enquanto o disco de inicialização estiver acessível.



Criar política de arranque iSCSI

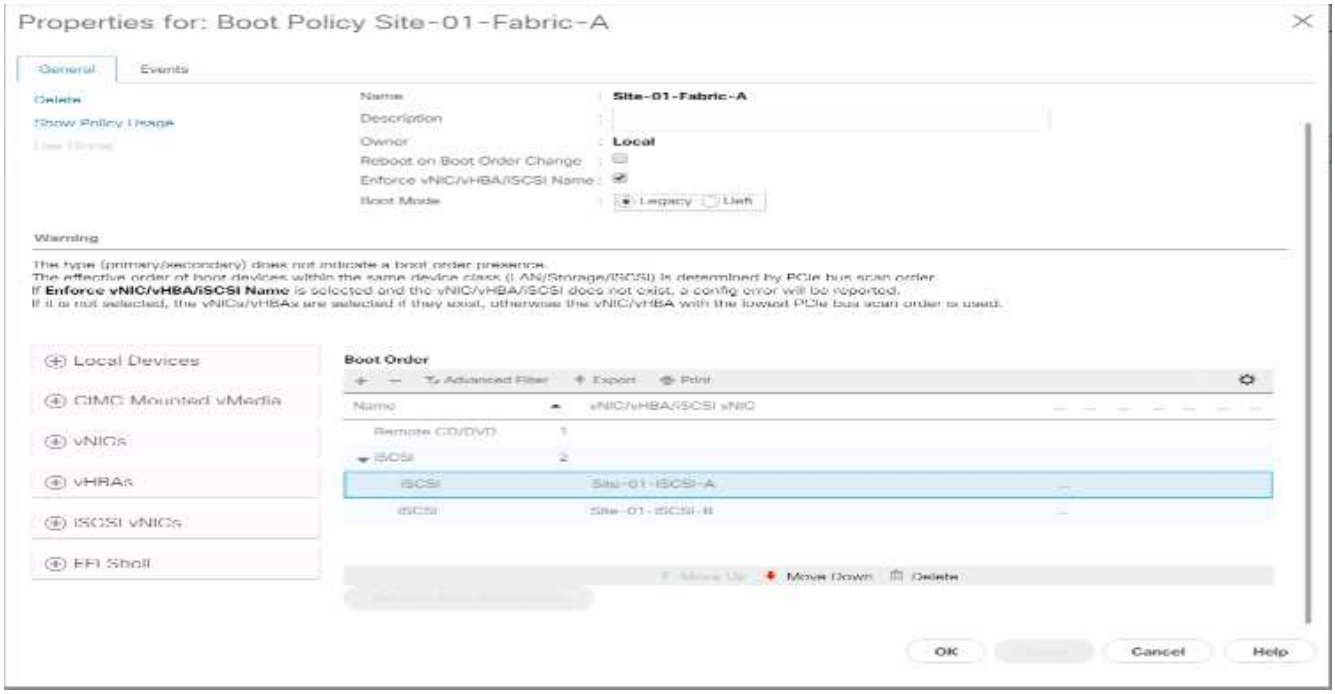
O procedimento nesta seção se aplica a um ambiente Cisco UCS no qual duas interfaces lógicas iSCSI (LIFs) estão nos nós de cluster 1 (`iscsi_lif01a` e `iscsi_lif01b`) e duas LIFs iSCSI estão nos nós de cluster 2 (`iscsi_lif02a` e `iscsi_lif02b`). Além disso, presume-se que as LIFs A sejam conetadas à malha A (interconexão A da malha UCS Cisco) e que as LIFs B sejam conetadas à malha B (interconexão B da malha UCS Cisco).

> Uma política de inicialização é configurada neste procedimento. A política configura o destino principal para ser `iscsi_lif01a`.

Para criar uma política de inicialização para o ambiente do Cisco UCS, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione políticas > raiz.
3. Clique com o botão direito do rato em políticas de arranque.

4. Selecione criar política de inicialização.
5. Introduza `Site-01-Fabric-A` como o nome da política de arranque.
6. Opcional: Insira uma descrição para a política de inicialização.
7. Mantenha a opção Reboot on Boot Order Change (Reiniciar na alteração da ordem de inicialização) limpa.
8. O modo de arranque é legado.
9. Expanda o menu pendente dispositivos locais e selecione Adicionar CD/DVD remoto.
10. Expanda o menu pendente iSCSI vNICs e selecione Adicionar arranque iSCSI.
11. Na caixa de diálogo Add iSCSI Boot (Adicionar inicialização iSCSI), `Site-01-iSCSI-A` digite . Clique em OK.
12. Selecione Adicionar inicialização iSCSI.
13. Na caixa de diálogo Add iSCSI Boot (Adicionar inicialização iSCSI), `Site-01-iSCSI-B` digite . Clique em OK.
14. Clique em OK para criar a política.



Criar modelo de perfil de serviço

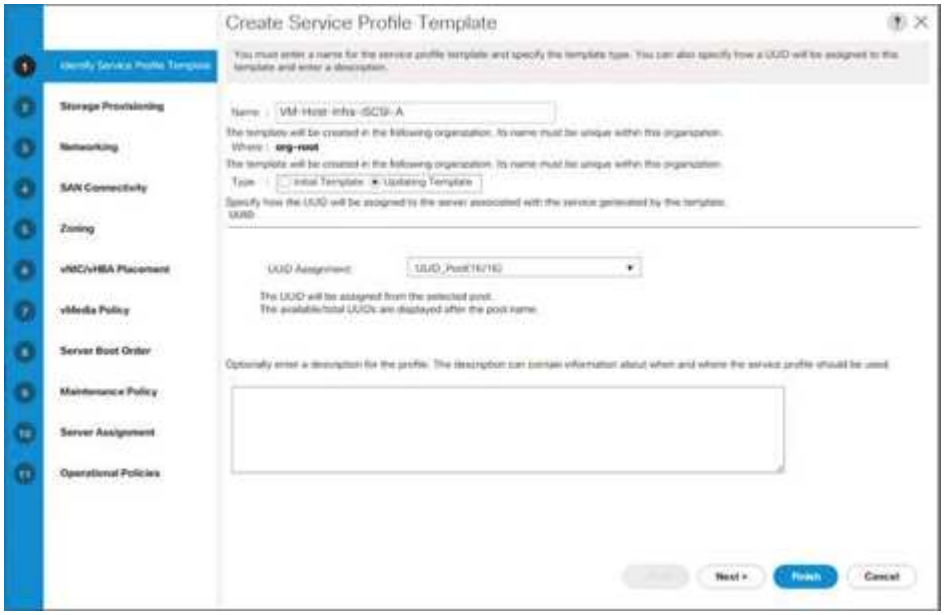
Neste procedimento, um modelo de perfil de serviço para hosts do Infrastructure ESXi é criado para a inicialização da malha A.

Para criar o modelo de perfil de serviço, execute as seguintes etapas:

1. No Gerenciador Cisco UCS, clique em servidores à esquerda.
2. Selecione modelos de perfil de serviço > raiz.
3. Clique com o botão direito do rato em raiz.
4. Selecione criar modelo de perfil de serviço para abrir o assistente criar modelo de perfil de serviço.
5. Introduza `VM-Host-Infra-iSCSI-A` como o nome do modelo de perfil de serviço. Este modelo de perfil

de serviço é configurado para inicializar a partir do nó de storage 1 na malha A..

6. Selecione a opção Atualizar modelo.
7. Em UUID, `UUID_Pool` selecione como o pool UUID. Clique em seguinte.



Configurar o provisionamento de storage

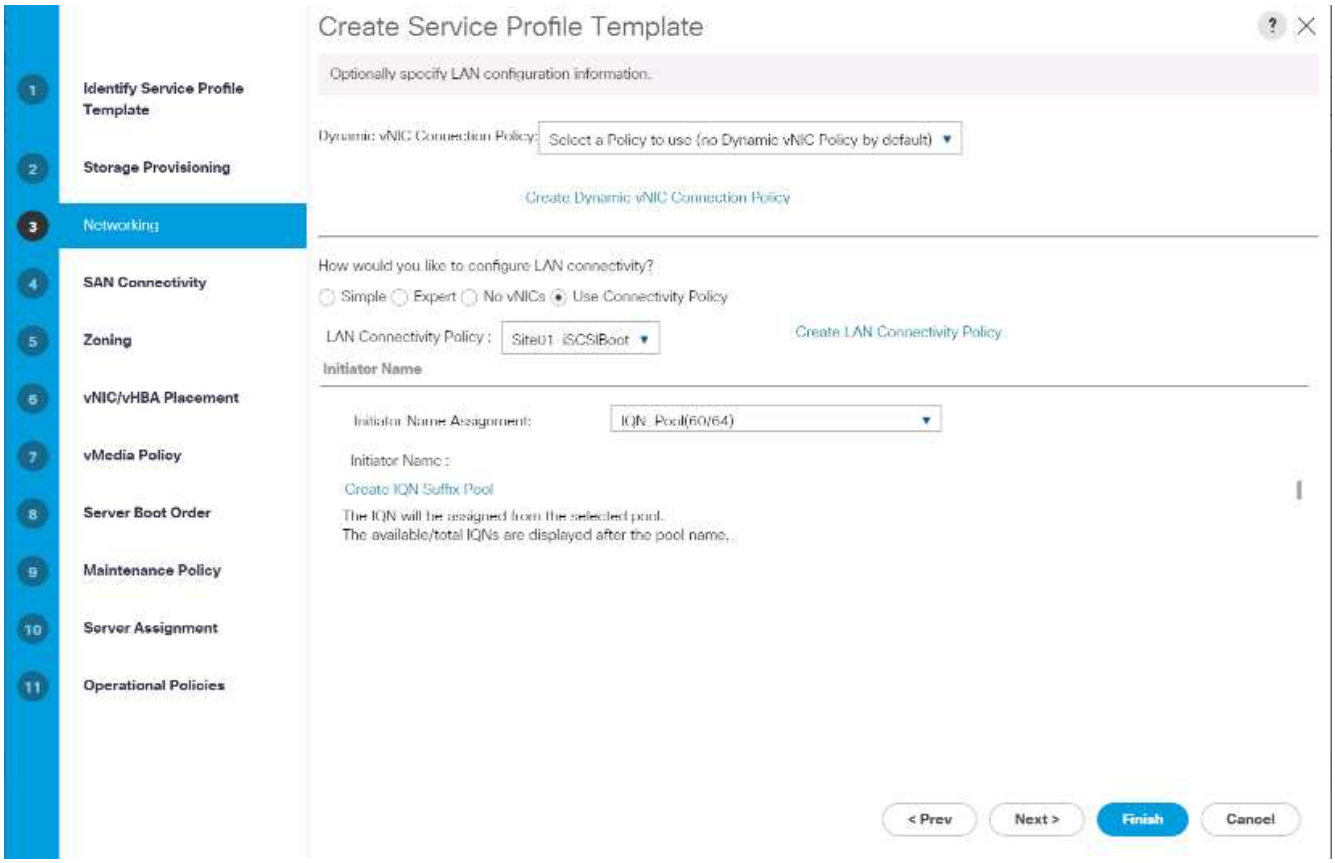
Para configurar o provisionamento de armazenamento, execute as seguintes etapas:

1. Se você tiver servidores sem discos físicos, clique em Diretiva de configuração de disco local e selecione a Diretiva de armazenamento local de inicialização SAN. Caso contrário, selecione a Política de armazenamento local padrão.
2. Clique em seguinte.

Configurar opções de rede

Para configurar as opções de rede, execute as seguintes etapas:

1. Mantenha a configuração padrão para Dynamic vNIC Connection Policy.
2. Selecione a opção usar política de conetividade para configurar a conetividade LAN.
3. Selecione iSCSI-Boot (Inicialização iSCSI) no menu pendente LAN Connectivity Policy (Política de conetividade LAN).
4. `IQN_Pool`Selecione em Designação de Nome do Iniciador. Clique em seguinte.



Configurar a conectividade do SAN

Para configurar a conetividade SAN, execute as seguintes etapas:

1. Para os vHBAs, selecione não para a opção como você gostaria de configurar a conetividade SAN?.
2. Clique em seguinte.

Configure o zoneamento

Para configurar o zoneamento, basta clicar em Avançar.

Configurar o posicionamento do vNIC/HBA

Para configurar o posicionamento do vNIC/HBA, execute as seguintes etapas:

1. Na lista suspensa Selecionar posicionamento, deixe a política de posicionamento como deixe o sistema executar o posicionamento.
2. Clique em seguinte.

Configurar a política vMedia

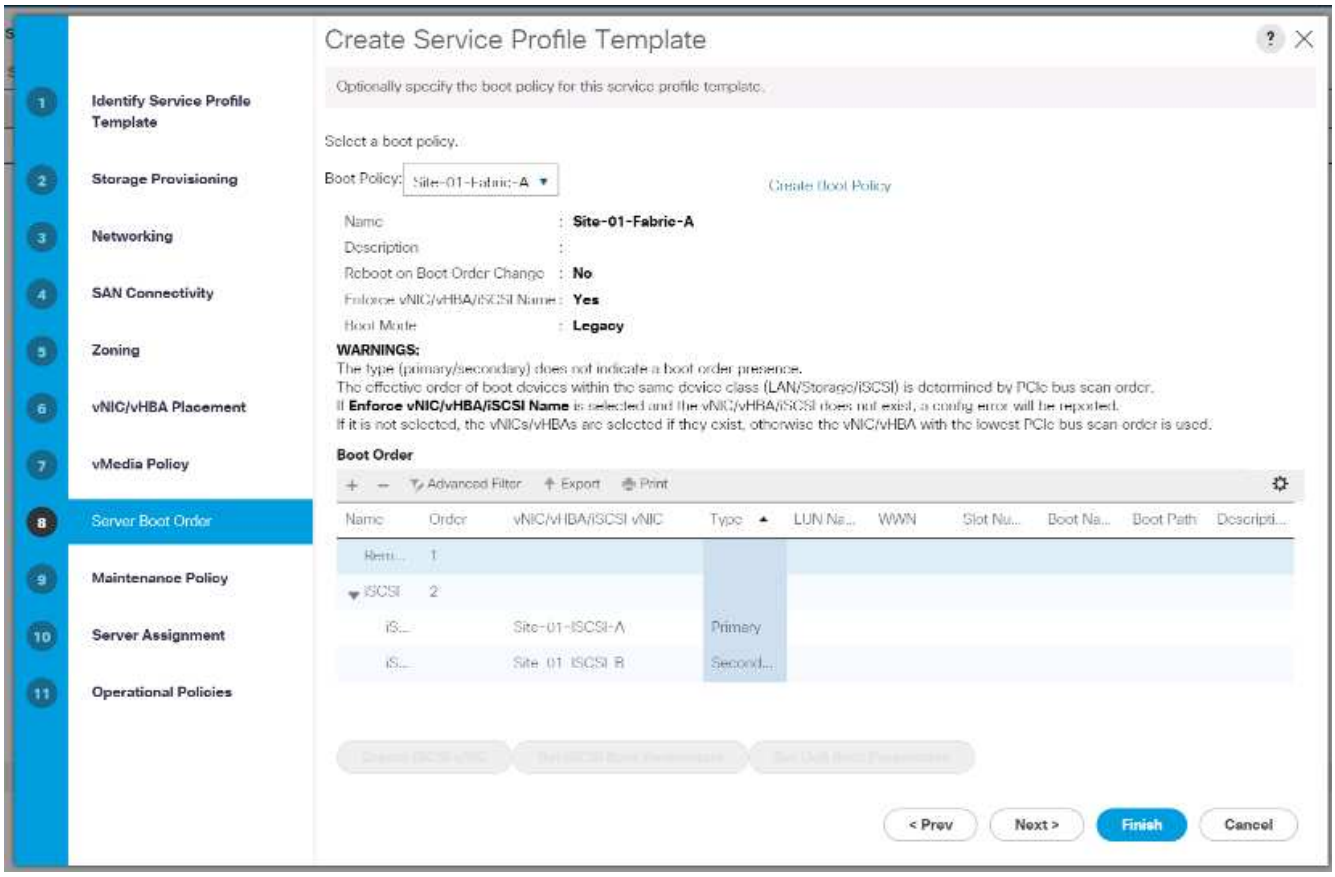
Para configurar a política vMedia, execute as seguintes etapas:

1. Não selecione uma política vMedia.
2. Clique em seguinte.

Configurar a ordem de inicialização do servidor

Para configurar a ordem de inicialização do servidor, execute as seguintes etapas:

1. `Boot-Fabric-A`Selecione para Política de Inicialização.



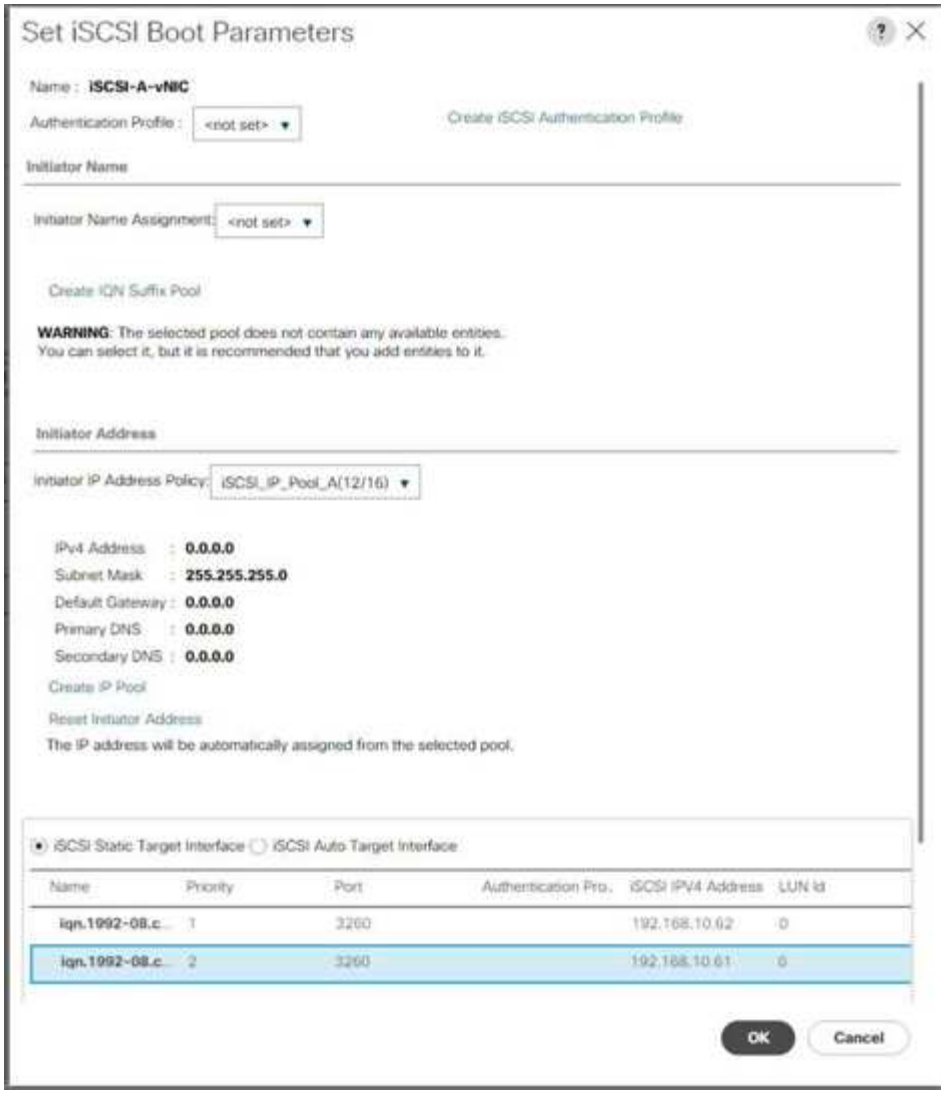
2. Na Ordem Boor, `Site-01- iSCSI-A`selecione .
3. Clique em Definir parâmetros de arranque iSCSI.
4. Na caixa de diálogo Definir parâmetros de inicialização iSCSI, deixe a opção Perfil de autenticação não definida, a menos que você tenha criado independentemente um apropriado para o seu ambiente.
5. Deixe a caixa de diálogo Designação de Nome do Iniciador não definida para usar o Nome do Iniciador de Perfil de Serviço único definido nas etapas anteriores.
6. Defina `iSCSI_IP_Pool_A` como a política de endereço IP do iniciador.
7. Selecione a opção iSCSI Static Target Interface.
8. Clique em Adicionar.
9. Introduza o nome de destino iSCSI. Para obter o nome de destino iSCSI de infra-SVM, faça login na interface de gerenciamento de cluster de storage e execute o `iscsi show` comando.

```
bb04-aff300::> iscsi show
            Target                          Target                          Status
Vserver     Name                            Alias                           Admin
----------- ------------------------------- ------------------------------- ------
Infra-SVM   iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                            Infra-SVM                       up
```

10. Introduza o endereço IP de `iscsi_lif_02a` para o campo Endereço IPv4.

11. Clique em OK para adicionar o destino estático iSCSI.
12. Clique em Adicionar.
13. Introduza o nome de destino iSCSI.
14. Introduza o endereço IP de `iscsi_lif_01a` para o campo Endereço IPv4.

15. Clique em OK para adicionar o destino estático iSCSI.



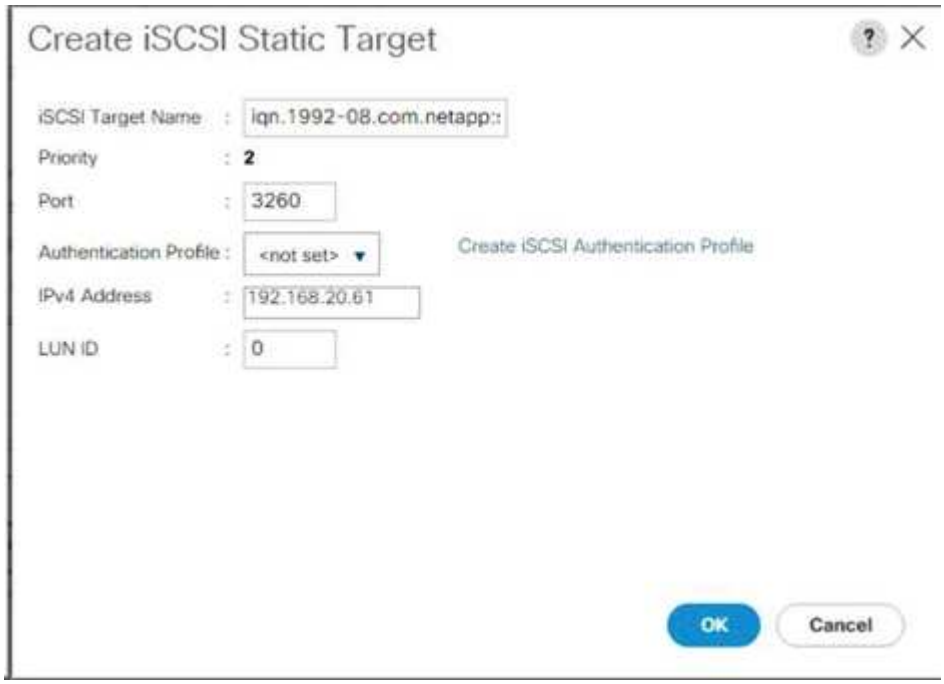
Os IPs de destino foram colocados com o nó de armazenamento 02 IP primeiro e o nó de armazenamento 01 IP segundo. Isso está supondo que o LUN de inicialização esteja no nó 01. O host inicializa usando o caminho para o nó 01 se a ordem neste procedimento for usada.

16. Na ordem de inicialização, selecione iSCSI-B-vNIC.
17. Clique em Definir parâmetros de arranque iSCSI.
18. Na caixa de diálogo Definir parâmetros de inicialização iSCSI, deixe a opção Perfil de autenticação como não definida, a menos que você tenha criado independentemente um apropriado ao seu ambiente.
19. Deixe a caixa de diálogo Designação de Nome do Iniciador não definida para usar o Nome do Iniciador de Perfil de Serviço único definido nas etapas anteriores.
20. Defina `iSCSI_IP_Pool_B` como a política de endereço IP do iniciador.
21. Selecione a opção iSCSI Static Target Interface (Interface de destino estático iSCSI).
22. Clique em Adicionar.
23. Introduza o nome de destino iSCSI. Para obter o nome de destino iSCSI de infra-SVM, faça login na interface de gerenciamento de cluster de storage e execute o `iscsi show` comando.

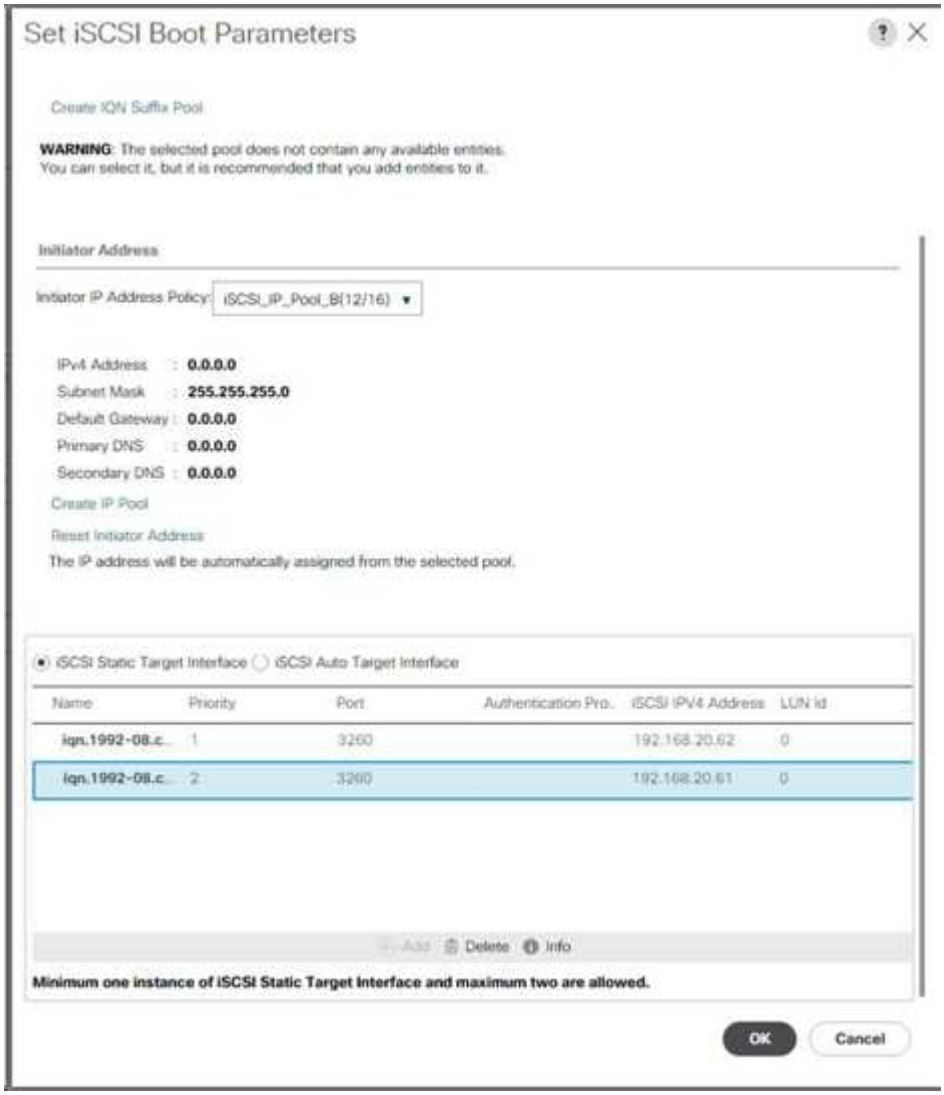
```
bb04-aff300::> iscsi show
          Target                          Target                         Status
Vserver   Name                            Alias                          Admin
--------- ------------------------------- ------------------------------ ------
Infra-SVM iqn.1992-08.com.netapp:sn.b5acab9ef1c811e68d9d00a098a9fec2:vs.3
                                          Infra-SVM                      up
```

24. Introduza o endereço IP de `iscsi_lif_02b` para o campo Endereço IPv4.

25. Clique em OK para adicionar o destino estático iSCSI.
26. Clique em Adicionar.
27. Introduza o nome de destino iSCSI.
28. Introduza o endereço IP de `iscsi_lif_01b` para o campo Endereço IPv4.



29. Clique em OK para adicionar o destino estático iSCSI.

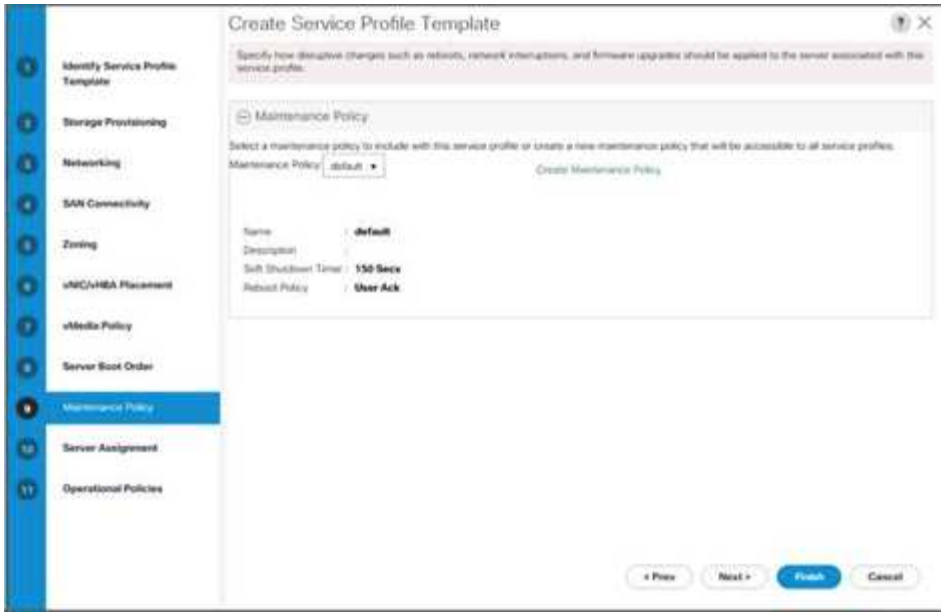


30. Clique em seguinte.

Configurar a política de manutenção

Para configurar a política de manutenção, execute as seguintes etapas:

1. Altere a política de manutenção para predefinição.

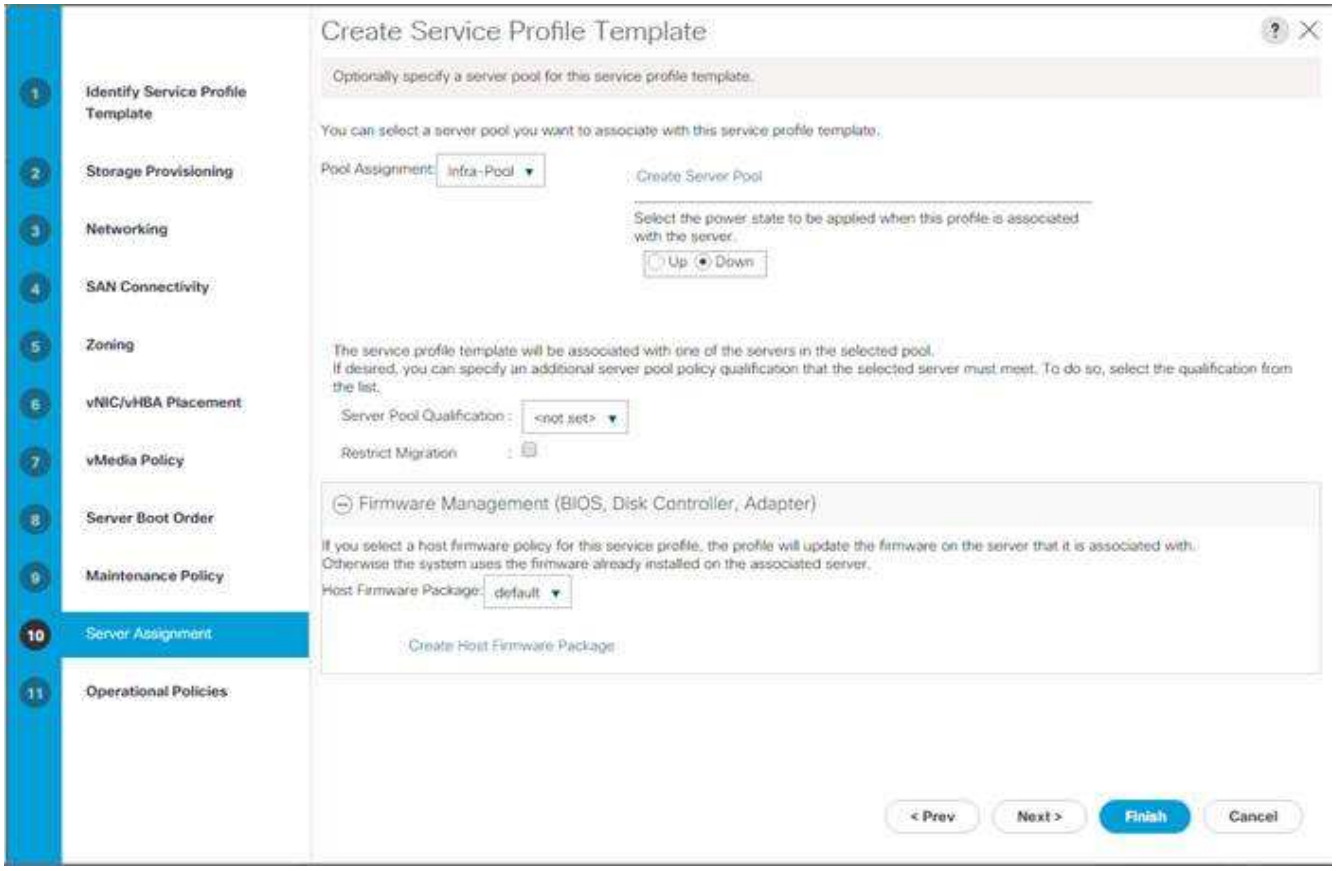


2. Clique em seguinte.

Configure a atribuição do servidor

Para configurar a atribuição do servidor, execute as seguintes etapas:

1. Na lista atribuição de pool, selecione infra-pool.
2. Selecione para baixo como o estado de energia a ser aplicado quando o perfil estiver associado ao servidor.
3. Expanda Gerenciamento de firmware na parte inferior da página e selecione a política padrão.

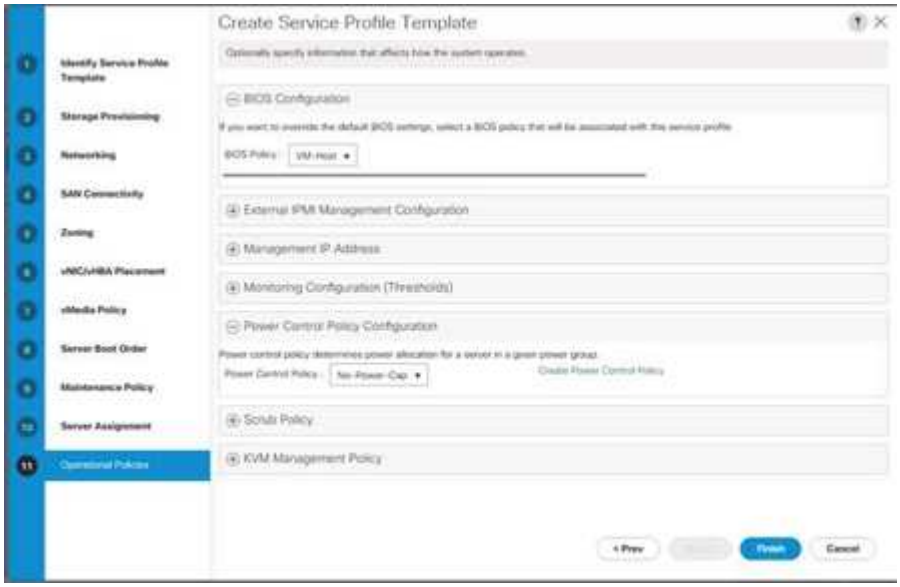


4. Clique em seguinte.

Configurar políticas operacionais

Para configurar as políticas operacionais, execute as seguintes etapas:

1. Na lista suspensa Política do BIOS, selecione VM-Host.
2. Expanda Configuração da política de controle de energia e selecione sem tampa de energia na lista suspensa Política de controle de energia.



3. Clique em concluir para criar o modelo de perfil de serviço.
4. Clique em OK na mensagem de confirmação.

Criar modelo de perfil de serviço habilitado para vMedia

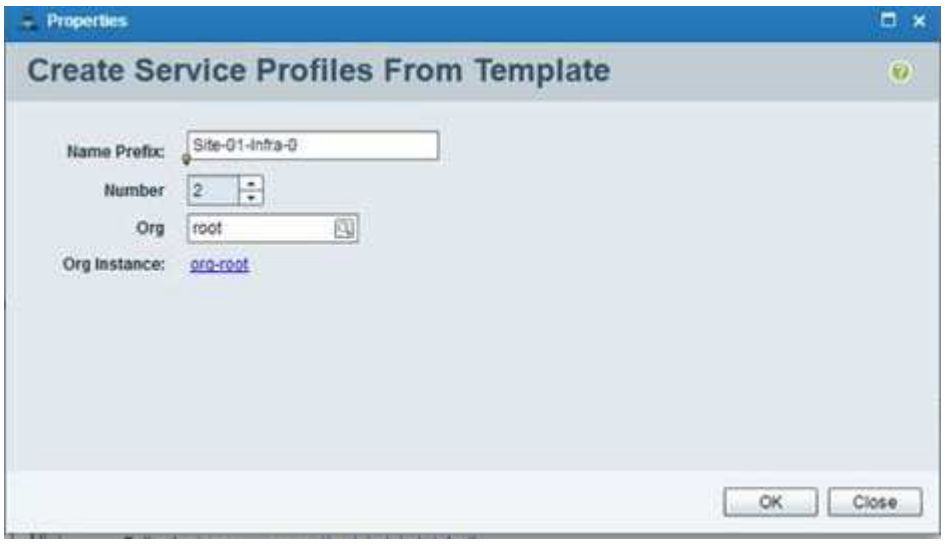
Para criar um modelo de perfil de serviço com o vMedia ativado, execute as seguintes etapas:

1. Conete-se ao UCS Manager e clique em servidores à esquerda.
2. Selecione modelos de perfil de serviço > raiz > modelo de serviço VM-Host-infra-iSCSI-A.
3. Clique com o botão direito do Mouse VM-Host-infra-iSCSI-A e selecione criar um clone.
4. Nomeie o `VM-Host-Infra-iSCSI-A-vM` clone .
5. Selecione a nova VM-Host-infra-iSCSI-A-VM criada e selecione a guia vMedia Policy à direita.
6. Clique em Modificar política vMedia.
7. Selecione o ESXi-6. 7U1-HTTP vMedia Policy e clique em OK.
8. Clique em OK para confirmar.

Crie perfis de serviço

Para criar perfis de serviço a partir do modelo de perfil de serviço, execute as seguintes etapas:

1. Conete-se ao Cisco UCS Manager e clique em servidores à esquerda.
2. Expanda servidores > modelos de perfil de serviço > raiz > modelo de serviço <name>.
3. Em ações, clique em criar perfil de serviço a partir do modelo e compita os seguintes passos:
   a. `Site- 01-Infra-0`Introduza como prefixo de nomenclatura.
   b. `2`Insira como o número de instâncias a serem criadas.
   c. Selecione root como a org.
   d. Clique em OK para criar os perfis de serviço.



4. Clique em OK na mensagem de confirmação.
5. Verifique se os perfis de serviço `Site-01-Infra-01` e `Site-01-Infra-02` foram criados.

Os perfis de serviço são automaticamente associados aos servidores em seus pools de servidores atribuídos.

Configuração de armazenamento parte 2: Inicialização de LUNs e grupos de iniciadores

Configuração de armazenamento de inicialização do ONTAP

Crie grupos de iniciadores

Para criar grupos de iniciadores (grupos de iniciadores), execute as seguintes etapas:

1. Execute os seguintes comandos a partir da conexão SSH do nó de gerenciamento de cluster:

```
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-01 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-01-iqn>
igroup create –vserver Infra-SVM –igroup VM-Host-Infra-02 –protocol
iscsi –ostype vmware –initiator <vm-host-infra-02-iqn>
igroup create –vserver Infra-SVM –igroup MGMT-Hosts –protocol iscsi
–ostype vmware –initiator <vm-host-infra-01-iqn>, <vm-host-infra-02-iqn>
```

Use os valores listados na Tabela 1 e na Tabela 2 para obter informações sobre IQN.

2. Para ver os três grupos criados, execute o `igroup show` comando.

Mapeie LUNs de inicialização para grupos

Para mapear LUNs de inicialização para grupos, execute o seguinte passo:

1. Na conexão SSH de gerenciamento de cluster de armazenamento, execute os seguintes comandos:

```
lun map –vserver Infra-SVM –volume esxi_boot –lun VM-Host-Infra- A
–igroup VM-Host-Infra-01 –lun-id 0lun map –vserver Infra-SVM –volume
esxi_boot –lun VM-Host-Infra- B –igroup VM-Host-Infra-02 –lun-id 0
```

Procedimento de implantação do VMware vSphere 6.7U1

Esta seção fornece procedimentos detalhados para a instalação do VMware ESXi 6.7U1 em uma configuração do FlexPod Express. Após a conclusão dos procedimentos, dois hosts ESXi inicializados são provisionados.

Existem vários métodos para instalar o ESXi em um ambiente VMware. Esses procedimentos se concentram em como usar o console KVM integrado e os recursos de Mídia virtual no Gerenciador do Cisco UCS para mapear Mídia de instalação remota para servidores individuais e se conetar aos LUNs de inicialização.

Faça o download da imagem personalizada do Cisco para ESXi 6.7U1

Se a imagem personalizada do VMware ESXi não tiver sido baixada, execute as seguintes etapas para concluir o download:

1. Clique no link a seguir: VMware vSphere Hypervisor (ESXi) 6.7U1.
2. Você precisa de uma ID de usuário e senha para "vmware.com" baixar este software.
3. Transfira o `.iso` ficheiro.

Gerente do Cisco UCS

O Cisco UCS IP KVM permite que o administrador inicie a instalação do sistema operacional por meio de Mídia remota. É necessário fazer login no ambiente do Cisco UCS para executar o KVM IP.

Para fazer login no ambiente do Cisco UCS, siga estas etapas:

1. Abra um navegador da Web e insira o endereço IP do endereço do cluster do Cisco UCS. Esta etapa inicia o aplicativo Cisco UCS Manager.
2. Clique no link Launch UCS Manager em HTML para iniciar o HTML 5 UCS Manager GUI.
3. Se solicitado a aceitar certificados de segurança, aceite conforme necessário.
4. Quando solicitado, digite `admin` como o nome de usuário e insira a senha administrativa.
5. Para fazer login no Gerenciador do Cisco UCS, clique em Login.
6. No menu principal, clique em servidores à esquerda.
7. Selecione servidores > Perfis de serviço > raiz > `VM-Host-Infra-01`.
8. Clique com o botão direito do rato `VM-Host-Infra-01` e selecione KVM Console.
9. Siga as instruções para iniciar o console KVM baseado em Java.
10. Selecione servidores > Perfis de serviço > raiz > `VM-Host-Infra-02`.
11. Clique com o botão direito do rato `VM-Host-Infra-02`em . e selecione Consola KVM.
12. Siga as instruções para iniciar o console KVM baseado em Java.

Configurar a instalação do VMware ESXi

O ESXi hospeda VM-Host-infra-01 e VM-Host- infra-02

Para preparar o servidor para a instalação do sistema operacional, execute as seguintes etapas em cada host ESXi:

1. Na janela KVM, clique em Mídia virtual.
2. Clique em Ativar dispositivos virtuais.
3. Se solicitado a aceitar uma sessão KVM não criptografada, aceite conforme necessário.
4. Clique em Mídia virtual e selecione CD/DVD de mapa.
5. Navegue até o arquivo de imagem ISO do instalador ESXi e clique em abrir.
6. Clique em dispositivo de mapa.
7. Clique na guia KVM para monitorar a inicialização do servidor.

Instale o ESXi

O ESXi hospeda VM-Host-infra-01 e VM-Host-infra-02

Para instalar o VMware ESXi no LUN inicializável iSCSI dos hosts, execute as seguintes etapas em cada host:

1. Inicialize o servidor selecionando Boot Server e clicando em OK. Em seguida, clique em OK novamente.
2. Ao reiniciar, a máquina deteta a presença do suporte de instalação ESXi. Selecione o instalador ESXi no menu de inicialização exibido.
3. Depois que o instalador terminar de carregar, pressione Enter para continuar com a instalação.
4. Leia e aceite o contrato de licença do utilizador final (EULA). Pressione F11 para aceitar e continuar.
5. Selecione o LUN que foi configurado anteriormente como o disco de instalação do ESXi e pressione Enter para continuar com a instalação.
6. Selecione o layout do teclado apropriado e pressione Enter.
7. Introduza e confirme a palavra-passe de raiz e prima Enter.
8. O instalador emite um aviso de que o disco selecionado será reparticionado. Pressione F11 para continuar com a instalação.
9. Após a conclusão da instalação, selecione a guia Mídia virtual e desmarque a marca P ao lado da Mídia de instalação ESXi. Clique em Sim.

> A imagem de instalação do ESXi deve ser desmapeada para garantir que o servidor reinicialize no ESXi e não no instalador.

10. Após a conclusão da instalação, pressione Enter para reinicializar o servidor.
11. No Gerenciador Cisco UCS, vincule o perfil de serviço atual ao modelo de perfil de serviço não vMedia para evitar a montagem da iso de instalação ESXi em HTTP.

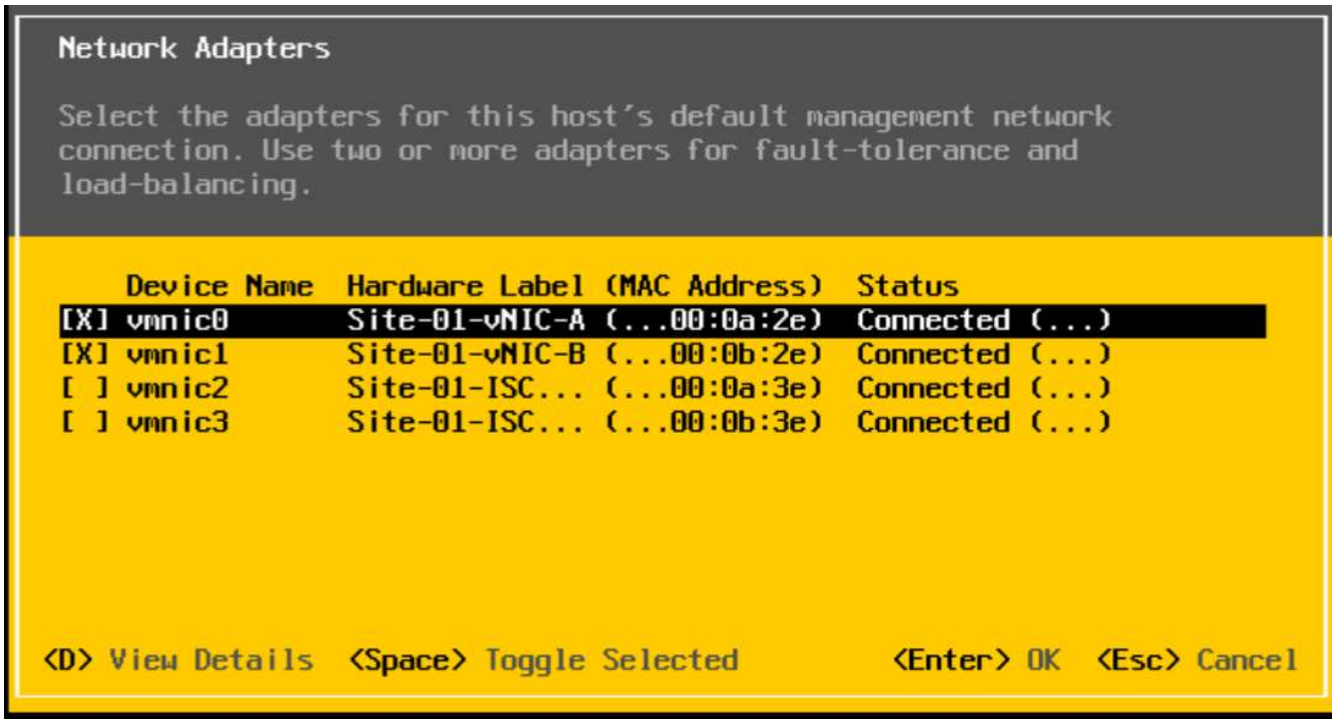
Configure a rede de gerenciamento para hosts ESXi

A adição de uma rede de gerenciamento para cada host VMware é necessária para gerenciar o host. Para adicionar uma rede de gerenciamento aos hosts VMware, execute as seguintes etapas em cada host ESXi:

ESXi Host VM-Host-infra-01 e VM-Host-infra-02

Para configurar cada host ESXi com acesso à rede de gerenciamento, execute as seguintes etapas:

1. Depois que o servidor terminar de reiniciar, pressione F2 para personalizar o sistema.
2. Inicie sessão como `root`, introduza a palavra-passe correspondente e prima Enter para iniciar sessão.
3. Selecione Opções de solução de problemas e pressione Enter.
4. Selecione Ativar Shell ESXi e pressione Enter.
5. Selecione Ativar SSH e pressione Enter.
6. Pressione Esc para sair do menu Opções de solução de problemas.
7. Selecione a opção Configurar rede de gerenciamento e pressione Enter.
8. Selecione adaptadores de rede e pressione Enter.
9. Verifique se os números no campo Etiqueta de hardware correspondem aos números no campo Nome do dispositivo.
10. Prima Enter.



11. Selecione a opção VLAN (Opcional) e pressione Enter.
12. Introduza `<ib-mgmt-vlan-id>` e prima Enter.
13. Selecione IPv4 Configuration (Configuração) e prima Enter.
14. Selecione a opção Definir Endereço estático IPv4 e Configuração de rede usando a barra de espaço.
15. Insira o endereço IP para gerenciar o primeiro host ESXi.
16. Insira a máscara de sub-rede do primeiro host ESXi.
17. Insira o gateway padrão para o primeiro host ESXi.
18. Pressione Enter para aceitar as alterações na configuração IP.
19. Selecione a opção Configuração DNS e pressione Enter.

> Como o endereço IP é atribuído manualmente, as informações de DNS também devem ser inseridas manualmente.

20. Introduza o endereço IP do servidor DNS primário.
21. Opcional: Insira o endereço IP do servidor DNS secundário.
22. Digite o FQDN para o primeiro host ESXi.
23. Pressione Enter para aceitar as alterações na configuração DNS.
24. Prima ESC para sair do menu Configurar rede de gestão.
25. Selecione Test Management Network (testar rede de gestão) para verificar se a rede de gestão está corretamente configurada e prima Enter.
26. Pressione Enter para executar o teste, pressione Enter novamente assim que o teste for concluído, revise o ambiente se houver uma falha.
27. Selecione Configurar rede de gestão novamente e prima Enter.
28. Selecione a opção Configuração IPv6 e pressione Enter.

29. Usando a barra de espaço, selecione Desativar IPv6 (reiniciar necessário) e pressione Enter.
30. Prima ESC para sair do submenu Configurar rede de gestão.
31. Pressione Y para confirmar as alterações e reinicializar o host ESXi.

Redefinir o endereço MAC da porta vmk0 do VMware ESXi host VMkernel (opcional)

ESXi Host VM-Host-infra-01 e VM-Host-infra-02

Por padrão, o endereço MAC da porta VMkernel de gerenciamento vmk0 é o mesmo que o endereço MAC da porta Ethernet na qual ela é colocada. Se o LUN de inicialização do host ESXi for remapeado para um servidor diferente com endereços MAC diferentes, ocorrerá um conflito de endereço MAC porque o vmk0 retém o endereço MAC atribuído, a menos que a configuração do sistema ESXi seja redefinida. Para redefinir o endereço MAC de vmk0 para um endereço MAC aleatório atribuído pela VMware, execute as seguintes etapas:

1. Na tela principal do menu do console ESXi, pressione Ctrl-Alt-F1 para acessar a interface da linha de comando do console VMware. No UCSM KVM, Ctrl-Alt-F1 aparece na lista de macros estáticas.
2. Faça login como root.
3. Digite `esxcfg-vmknic –l` para obter uma listagem detalhada da interface vmk0. O vmk0 deve fazer parte do grupo de portas da rede de Gerenciamento. Anote o endereço IP e a máscara de rede do vmk0.
4. Para remover vmk0, digite o seguinte comando:

```
esxcfg-vmknic –d “Management Network”
```

5. Para adicionar vmk0 novamente com um endereço MAC aleatório, digite o seguinte comando:

```
esxcfg-vmknic –a –i <vmk0-ip> -n <vmk0-netmask> “Management Network””.
```

6. Verifique se vmk0 foi adicionado novamente com um endereço MAC aleatório

```
esxcfg-vmknic –l
```

7. Digite `exit` para sair da interface de linha de comando.
8. Pressione Ctrl-Alt-F2 para retornar à interface do menu do console ESXi.

Faça login em hosts do VMware ESXi com o cliente de host VMware

ESXi Host VM-Host-infra-01

Para fazer login no host ESXi VM-Host-infra-01 usando o VMware Host Client, execute as seguintes etapas:

1. Abra um navegador da Web na estação de trabalho de gerenciamento e navegue até o `VM-Host-Infra-01` endereço IP de gerenciamento.
2. Clique em abrir o VMware Host Client.
3. Introduza `root` o nome de utilizador.

4. Introduza a palavra-passe raiz.
5. Clique em Login para conetar.
6. Repita esse processo para fazer login `VM-Host-Infra-02` em uma guia ou janela separada do navegador.

Instalar drivers VMware para a placa de interface virtual (VIC) do Cisco

Faça o download e extraia o pacote off-line para o seguinte driver VMware VIC para a estação de trabalho de gerenciamento:

- Driver nenic versão 1.0.25.0

O ESXi hospeda VM-Host-infra-01 e VM-Host-infra-02

Para instalar os drivers do VMware VIC no host ESXi VM-Host-infra-01 e VM-Host-infra-02, execute as seguintes etapas:

1. Em cada cliente anfitrião, selecione armazenamento.
2. Clique com o botão direito do rato em datastore1 e selecione Procurar.
3. No navegador do datastore, clique em carregar.
4. Navegue até o local guardado para os controladores VIC transferidos e selecione VMW-ESX-6,7.0-nenic-1,0.25,0-offline_bundle-11271332.zip.
5. No navegador do datastore, clique em carregar.
6. Clique em abrir para carregar o ficheiro para datastore1.
7. Certifique-se de que o arquivo foi carregado para ambos os hosts ESXi.
8. Coloque cada host no modo Manutenção se ainda não estiver.
9. Conete-se a cada host ESXi através do ssh a partir de uma conexão shell ou terminal de massa.
10. Faça login como root com a senha root.
11. Execute os seguintes comandos em cada host:

```
esxcli software vib update -d /vmfs/volumes/datastore1/VMW-ESX-6.7.0-
nenic-1.0.25.0-offline_bundle-11271332.zip
reboot
```

12. Faça login no Host Client em cada host assim que a reinicialização estiver concluída e saia do Maintenance Mode.

Configure portas VMkernel e switch virtual

ESXi Host VM-Host-infra-01 e VM-Host-infra-02

Para configurar as portas VMkernel e os switches virtuais nos hosts ESXi, execute as seguintes etapas:

1. No Host Client, selecione rede à esquerda.
2. No painel central, selecione a guia switches virtuais .
3. Selecione vSwitch0.

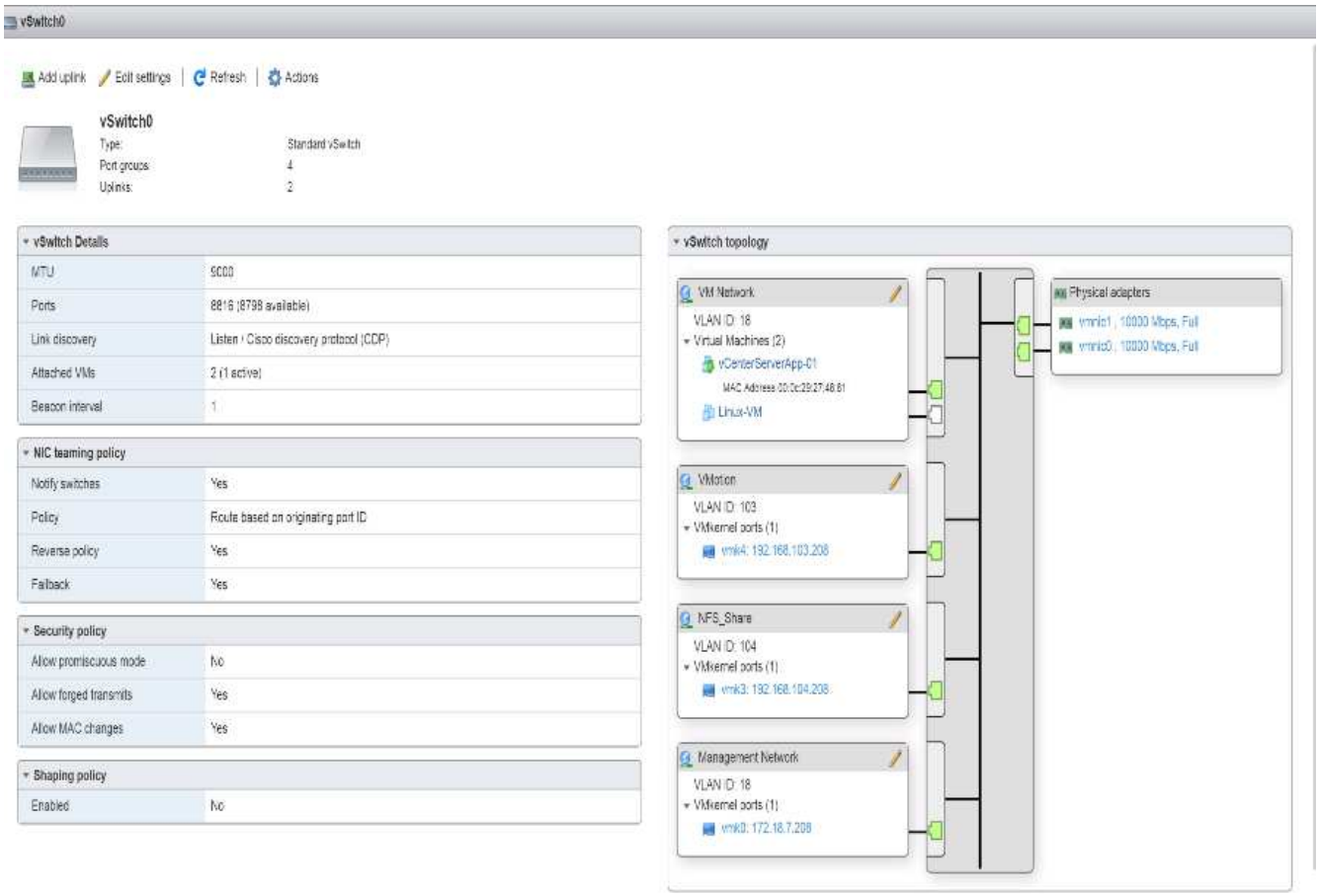
4. Selecione Editar definições.
5. Altere a MTU para 9000.
6. Expanda agrupamento NIC.
7. Na seção Ordem de failover, selecione vmnic1 e clique em Marcar ativo.
8. Verifique se vmnic1 agora tem um status de Ativo.
9. Clique em Guardar.
10. Selecione rede à esquerda.
11. No painel central, selecione a guia switches virtuais .
12. Selecione iScsiBootvSwitch.
13. Selecione Editar definições.
14. Altere a MTU para 9000
15. Clique em Guardar.
16. Selecione a guia NICs do VMkernel.
17. Selecione vmk1 iScsiBootPG.
18. Selecione Editar definições.
19. Altere a MTU para 9000.
20. Expanda as configurações IPv4 e altere o endereço IP para um endereço fora do UCS iSCSI-IP-Pool-A.

> Para evitar conflitos de endereço IP se os endereços do pool IP iSCSI do Cisco UCS forem reatribuídos, é recomendável usar endereços IP diferentes na mesma sub-rede para as portas VMkernel iSCSI.

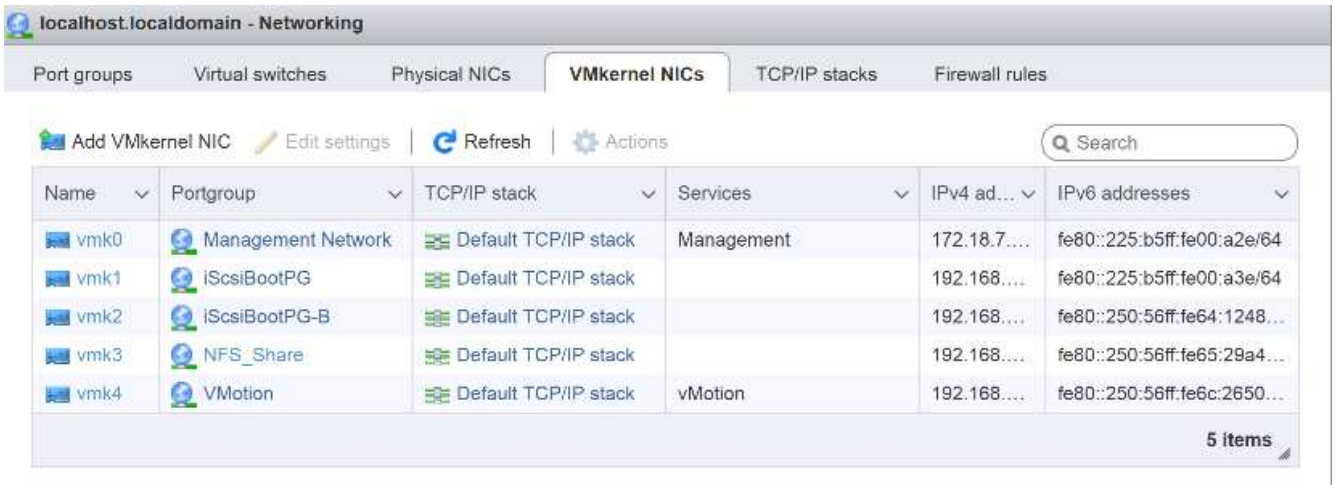
21. Clique em Guardar.
22. Selecione o separador Virtual switches (interrutores virtuais).
23. Selecione a opção Adicionar virtual padrão.
24. Forneça um nome de `iScsciBootvSwitch-B` para o nome do vSwitch.
25. Defina a MTU como 9000.
26. Selecione vmnic3 no menu suspenso Uplink 1.
27. Clique em Adicionar.
28. No painel central, selecione a guia NICs do VMkernel.
29. Selecione Adicionar NIC VMkernel
30. Especifique um novo nome de grupo de portas do iScsiBootPG-B.
31. Selecione iScsciBootvSwitch-B para Virtual switch.
32. Defina a MTU como 9000. Não insira um ID de VLAN.
33. Selecione estático para as definições IPv4D e expanda a opção para fornecer o Endereço e a Máscara de sub-rede na Configuração.

> Para evitar conflitos de endereço IP, se os endereços do pool IP iSCSI do Cisco UCS forem reatribuídos, é recomendável usar endereços IP diferentes na mesma sub-rede para as portas VMkernel iSCSI.

34. Clique em criar.
35. À esquerda, selecione rede e, em seguida, selecione a guia grupos de portas.
36. No painel central, clique com o botão direito do rato em rede VM e selecione Remover.
37. Clique em Remover para concluir a remoção do grupo de portas.
38. No painel central, selecione Adicionar grupo de portas.
39. Atribua um nome ao grupo de portas Management Network e introduza `<ib-mgmt-vlan-id>` no campo VLAN ID (ID da VLAN) e certifique-se de que o Virtual switch vSwitch0 está selecionado.
40. Clique em Adicionar para finalizar as edições da rede IB-MGMT.
41. Na parte superior, selecione a guia NICs do VMkernel.
42. Clique em Adicionar NIC VMkernel.
43. Para novo grupo de portas, digite VMotion.
44. Para o interrutor virtual, selecione vSwitch0 selecionado.
45. Insira `<vmotion-vlan-id>` para a ID da VLAN.
46. Altere a MTU para 9000.
47. Selecione Static IPv4 settings e expanda IPv4 settings.
48. Insira o endereço IP e a máscara de rede do host ESXi vMotion.
49. Selecione a pilha TCP/IP do vMotion.
50. Selecione vMotion em Serviços.
51. Clique em criar.
52. Clique em Adicionar NIC VMkernel.
53. Para novo grupo de portas, insira NFS_share.
54. Para o interrutor virtual, selecione vSwitch0 selecionado.
55. Insira `<infra-nfs-vlan-id>` para a ID da VLAN
56. Altere a MTU para 9000.
57. Selecione Static IPv4 settings e expanda IPv4 settings.
58. Insira o endereço IP e a máscara de rede NFS da infraestrutura do host ESXi.
59. Não selecione nenhum dos Serviços.
60. Clique em criar.
61. Selecione a guia Virtual switches e, em seguida, selecione vSwitch0. As propriedades para NICs do VMkernel vSwitch0 devem ser semelhantes ao exemplo a seguir:



62. Selecione a guia NICs do VMkernel para confirmar os adaptadores virtuais configurados. Os adaptadores listados devem ser semelhantes ao seguinte exemplo:



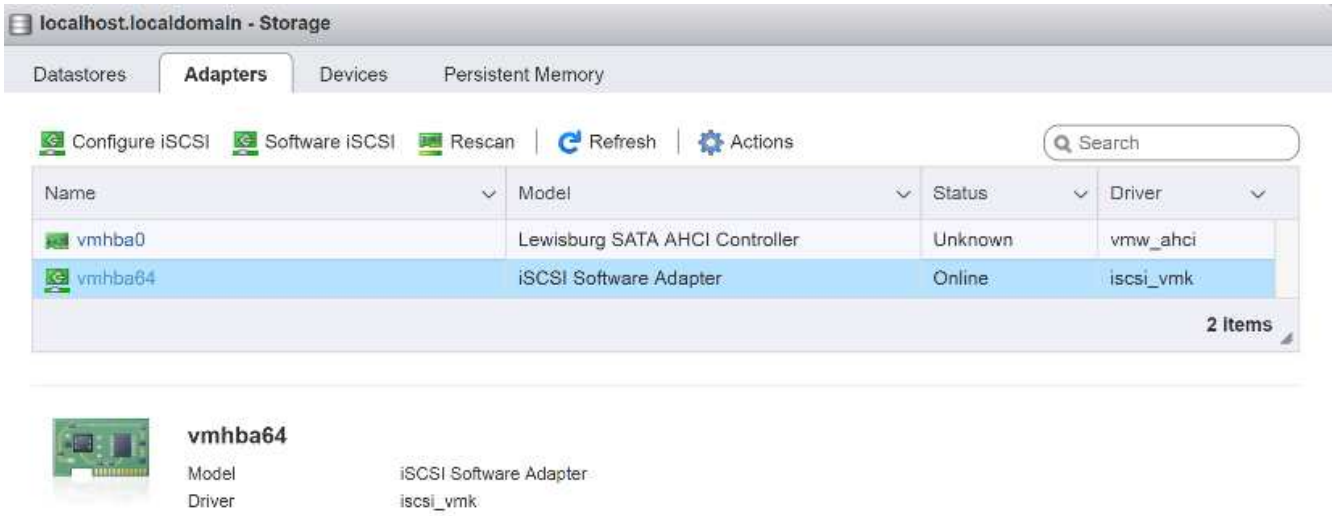
Configurar multipathing iSCSI

O ESXi hospeda VM-Host-infra-01 e VM-Host-infra-02

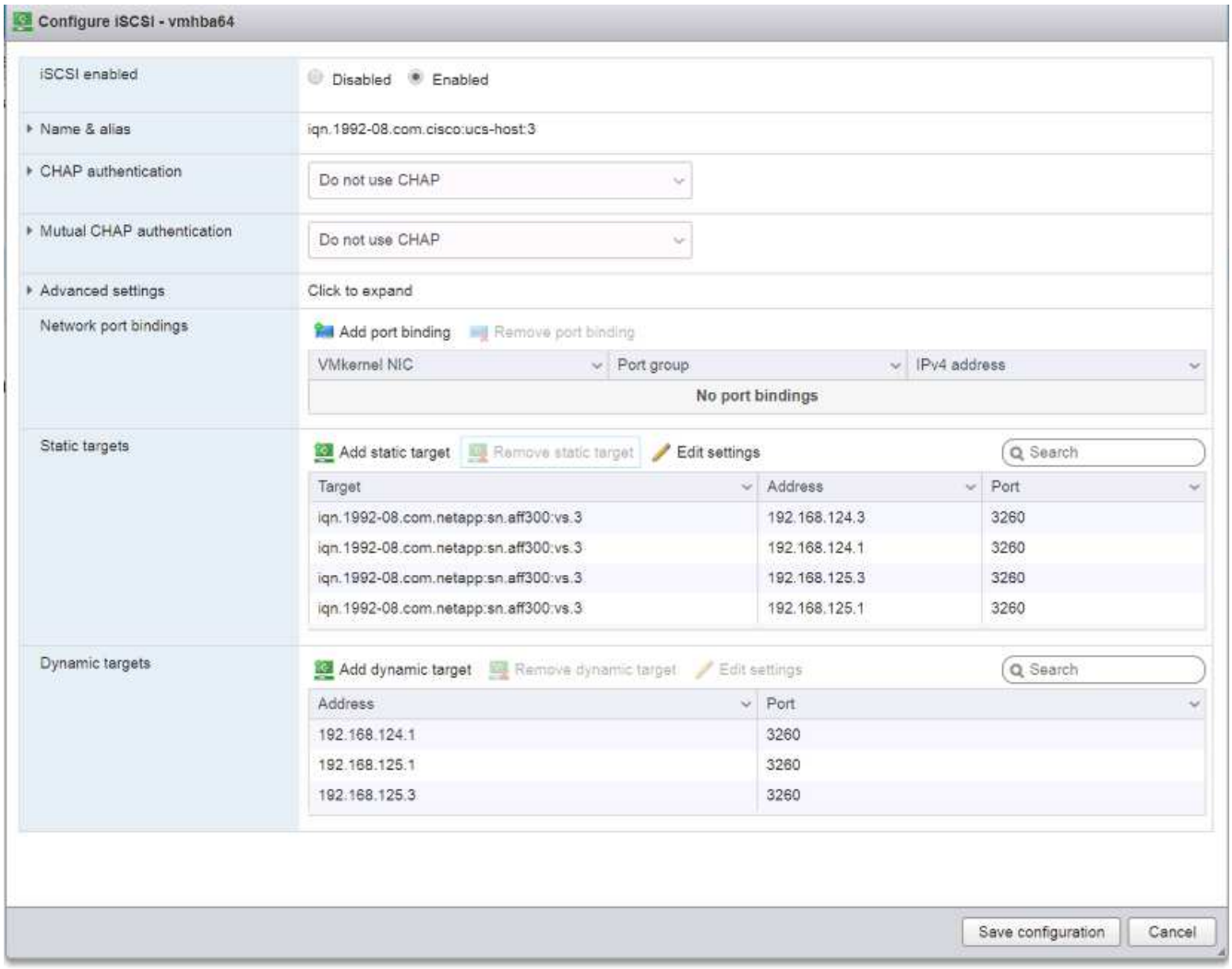
Para configurar o multipathing iSCSI no host ESXi VM-Host-infra-01 e VM-Host-infra-02, execute as seguintes etapas:

1. Em cada cliente anfitrião, selecione armazenamento à esquerda.

2. No painel central, clique em adaptadores.
3. Selecione o adaptador de software iSCSI e clique em Configurar iSCSI.



4. Em alvos dinâmicos, clique em Adicionar alvo dinâmico.
5. Introduza o endereço IP de `iSCSI_lif01a`.
6. Repita a introdução destes endereços IP: `iscsi_lif01b` `iscsi_lif02a` , , E `iscsi_lif02b`.
7. Clique em Save Configuration (Guardar configuração).



Para obter todos os `iscsi_lif` endereços IP, faça login na interface de gerenciamento de cluster de storage do NetApp e execute o `network interface show` comando.

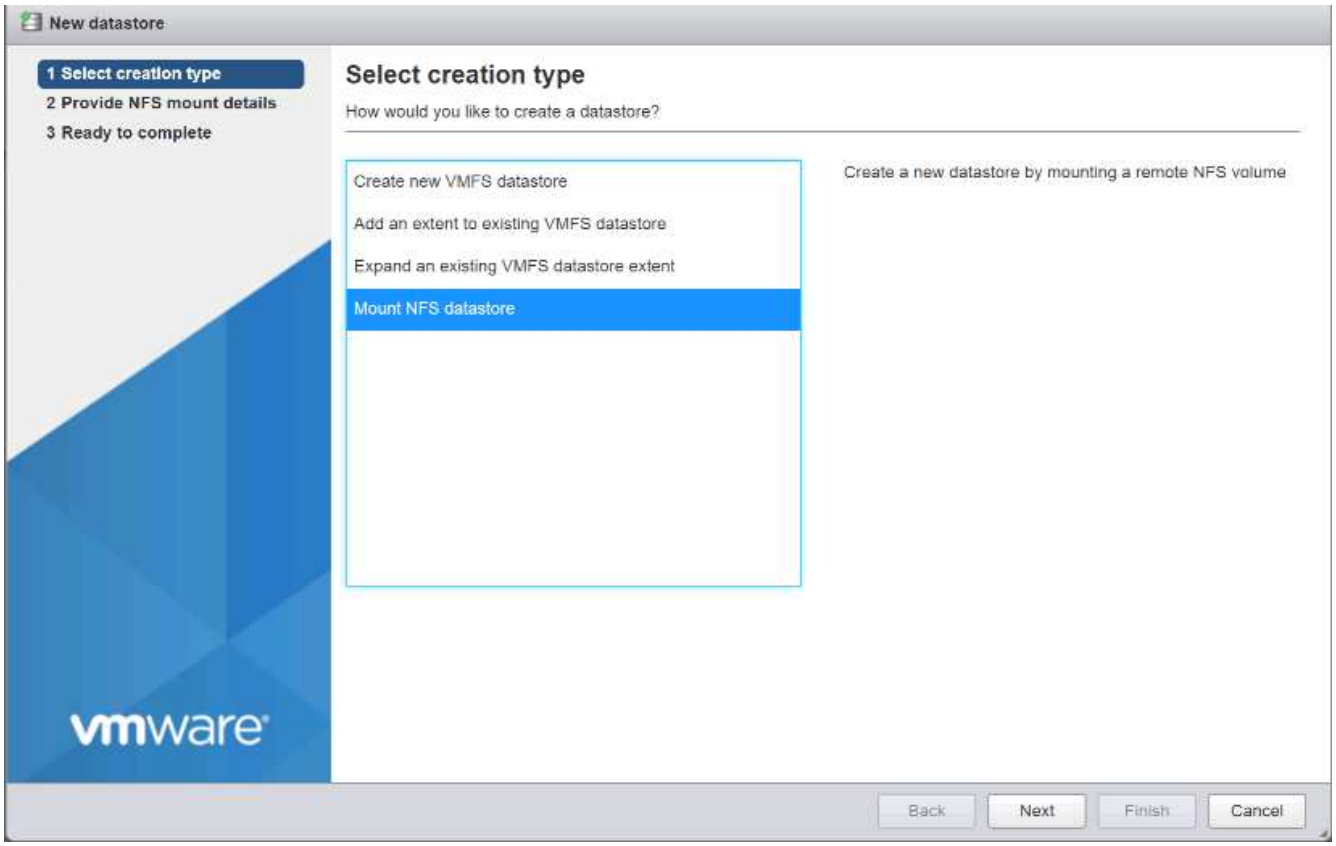
O host reenvia automaticamente o adaptador de armazenamento e os destinos são adicionados aos destinos estáticos.

Monte os armazenamentos de dados necessários

O ESXi hospeda VM-Host-infra-01 e VM-Host-infra-02

Para montar os datastores necessários, execute as seguintes etapas em cada host ESXi:

1. No Host Client, selecione armazenamento à esquerda.
2. No painel central, selecione datastores.
3. No painel central, selecione novo datastore para adicionar um novo datastore.
4. Na caixa de diálogo novo datastore, selecione montar datastore NFS e clique em Avançar.

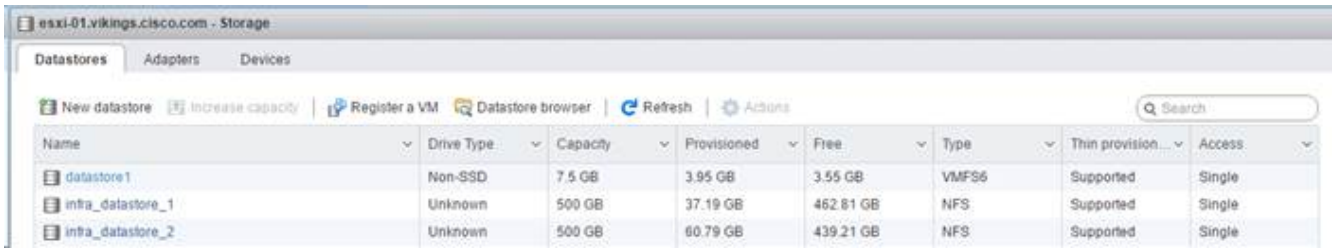


5. Na página fornecer detalhes da montagem NFS, execute estas etapas:
   a. Insira `infra_datastore_1` o nome do datastore.
   b. Introduza o endereço IP do `nfs_lif01_a` LIF para o servidor NFS.
   c. Insira `/infra_datastore_1` para o compartilhamento NFS.
   d. Deixe a versão NFS definida em NFS 3.
   e. Clique em seguinte.

6. Clique em concluir. O datastore agora deve aparecer na lista de datastore.
7. No painel central, selecione novo datastore para adicionar um novo datastore.
8. Na caixa de diálogo novo datastore, selecione montar datastore NFS e clique em Avançar.
9. Na página fornecer detalhes da montagem NFS, execute estas etapas:

a. Insira `infra_datastore_2` o nome do datastore.
b. Introduza o endereço IP do `nfs_lif02_a` LIF para o servidor NFS.
c. Insira `/infra_datastore_2` para o compartilhamento NFS.
d. Deixe a versão NFS definida em NFS 3.
e. Clique em seguinte.

10. Clique em concluir. O datastore agora deve aparecer na lista de datastore.



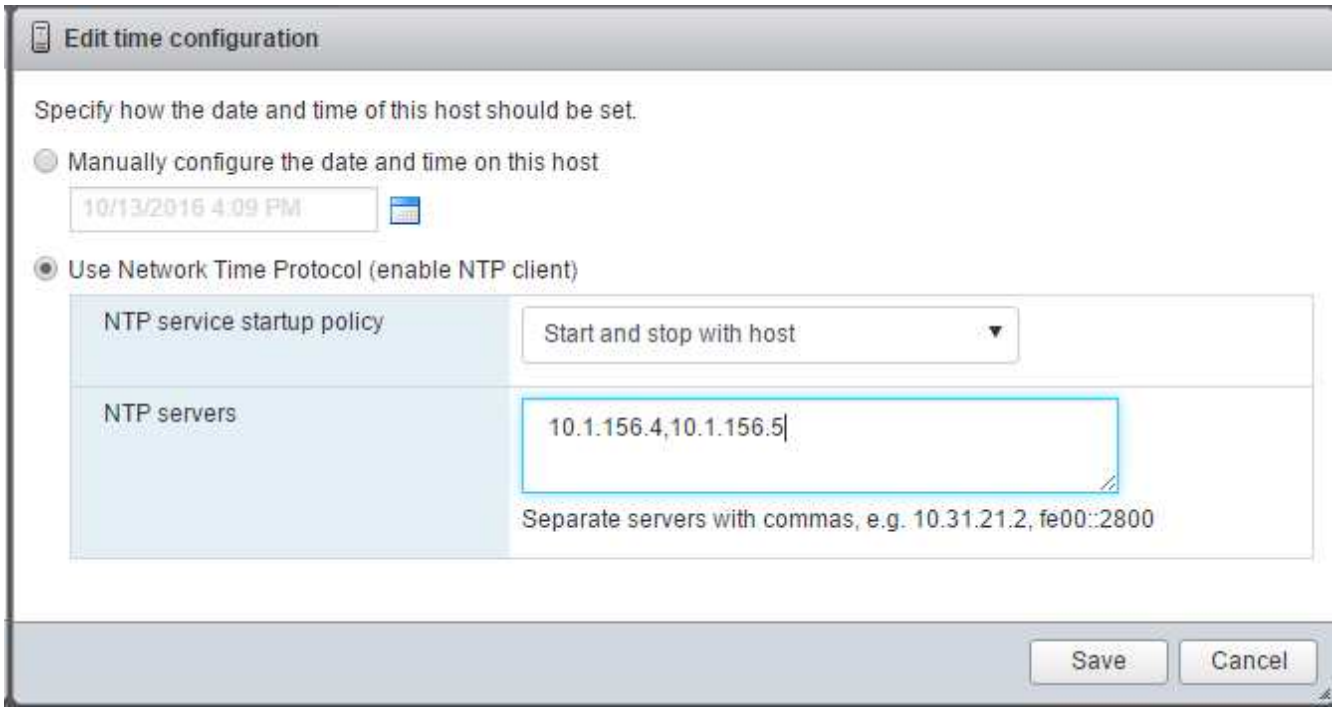
11. Monte ambos os datastores em ambos os hosts ESXi.

Configure o NTP em hosts ESXi

O ESXi hospeda VM-Host-infra-01 e VM-Host-infra-02

Para configurar o NTP nos hosts ESXi, execute as seguintes etapas em cada host:

1. No Host Client, selecione Manage (gerir) à esquerda.
2. No painel central, selecione a guia hora e data .
3. Clique em Edit Settings (Editar definições).
4. Certifique-se de que a opção utilizar protocolo de tempo de rede (Ativar cliente NTP) está selecionada.
5. Use o menu suspenso para selecionar Iniciar e Parar com Host.
6. Insira os dois endereços NTP switch Nexus na caixa servidores NTP separados por uma vírgula.



7. Clique em Save (Guardar) para guardar as alterações de configuração.
8. Selecione ações > Serviço NTP > Iniciar.
9. Verifique se o serviço NTP está em execução e o relógio está agora definido para aproximadamente a hora correta

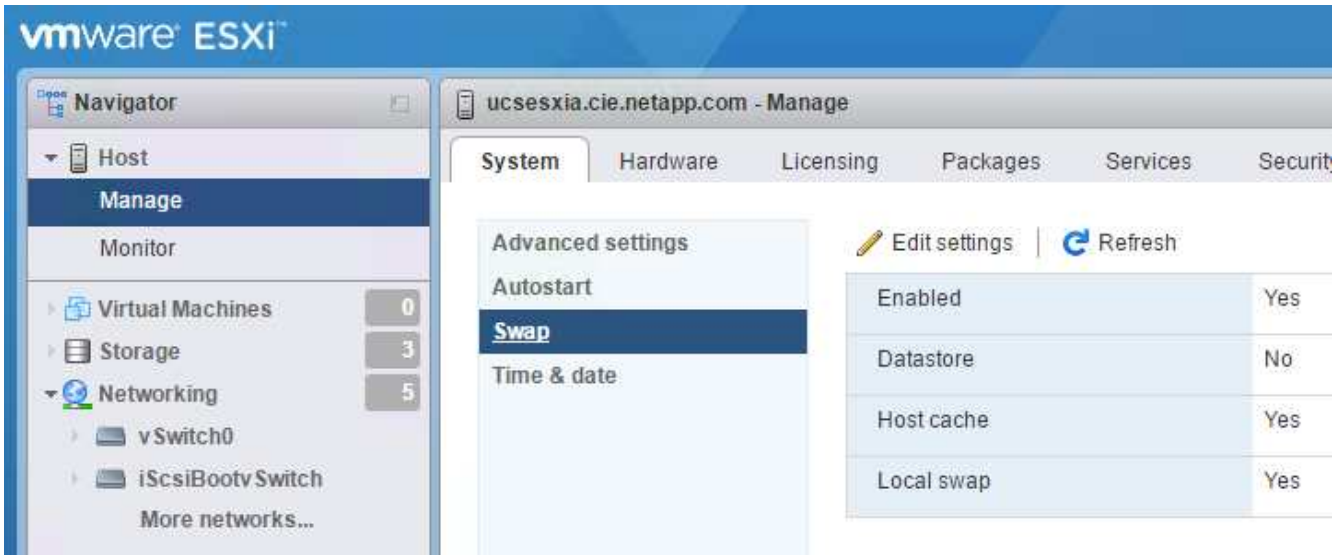
O tempo do servidor NTP pode variar ligeiramente em relação ao tempo do host.

Configurar a troca de host ESXi

O ESXi hospeda VM-Host-infra-01 e VM-Host-infra-02

Para configurar a troca de host nos hosts ESXi, siga estas etapas em cada host:

1. Clique em Gerenciar no painel de navegação esquerdo. Selecione sistema no painel direito e clique em trocar.



2. Clique em Edit Settings (Editar definições). Selecione `infra_swap` a partir das opções do datastore.

3. Clique em Guardar.

Instale o plug-in NFS NetApp 1.1.2 para VMware VAAI

Para instalar o plug-in NFS NetApp 1. 1,2 para VMware VAAI, execute as etapas a seguir.

1. Faça o download do plug-in NFS do NetApp para VMware VAAI:
   a. Vá para "Página de download do software NetApp" .
   b. Role para baixo e clique em NetApp NFS Plug-in para VMware VAAI.
   c. Selecione a plataforma ESXi.
   d. Transfira o pacote offline (.zip) ou o pacote online (.vib) do plug-in mais recente.
2. O plug-in NetApp NFS para VMware VAAI está pendente de qualificação IMT com o ONTAP 9.5 e os detalhes de interoperabilidade serão publicados no NetApp IMT em breve.
3. Instale o plug-in no host ESXi usando a CLI do ESX.
4. Reinicie o host ESXI.

Instale o VMware vCenter Server 6,7

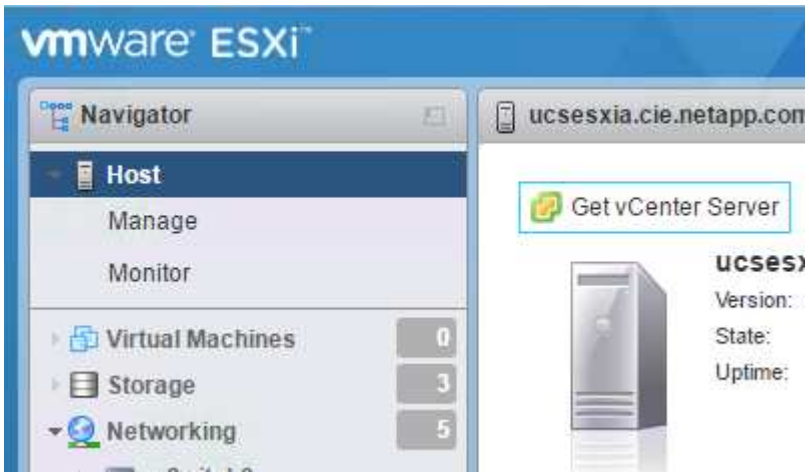
Esta seção fornece procedimentos detalhados para instalar o VMware vCenter Server 6,7 em uma configuração do FlexPod Express.

O FlexPod Express usa o VMware vCenter Server Appliance (VCSA).

Instale o VMware vCenter Server Appliance

Para instalar o VCSA, execute as seguintes etapas:

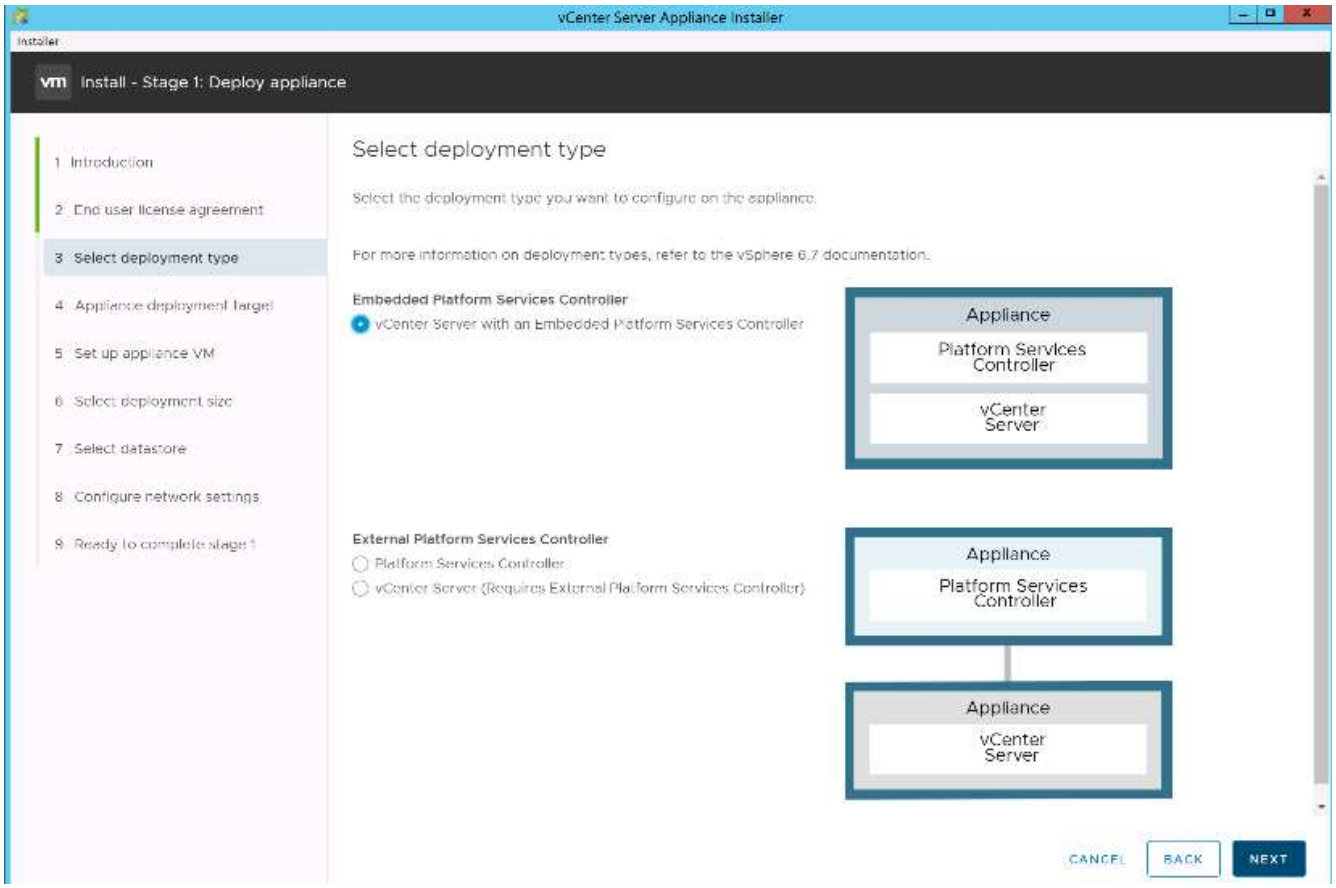
1. Faça o download do VCSA. Acesse o link de download clicando no ícone obter vCenter Server ao gerenciar o host ESXi.



2. Faça download do VCSA a partir do site da VMware.

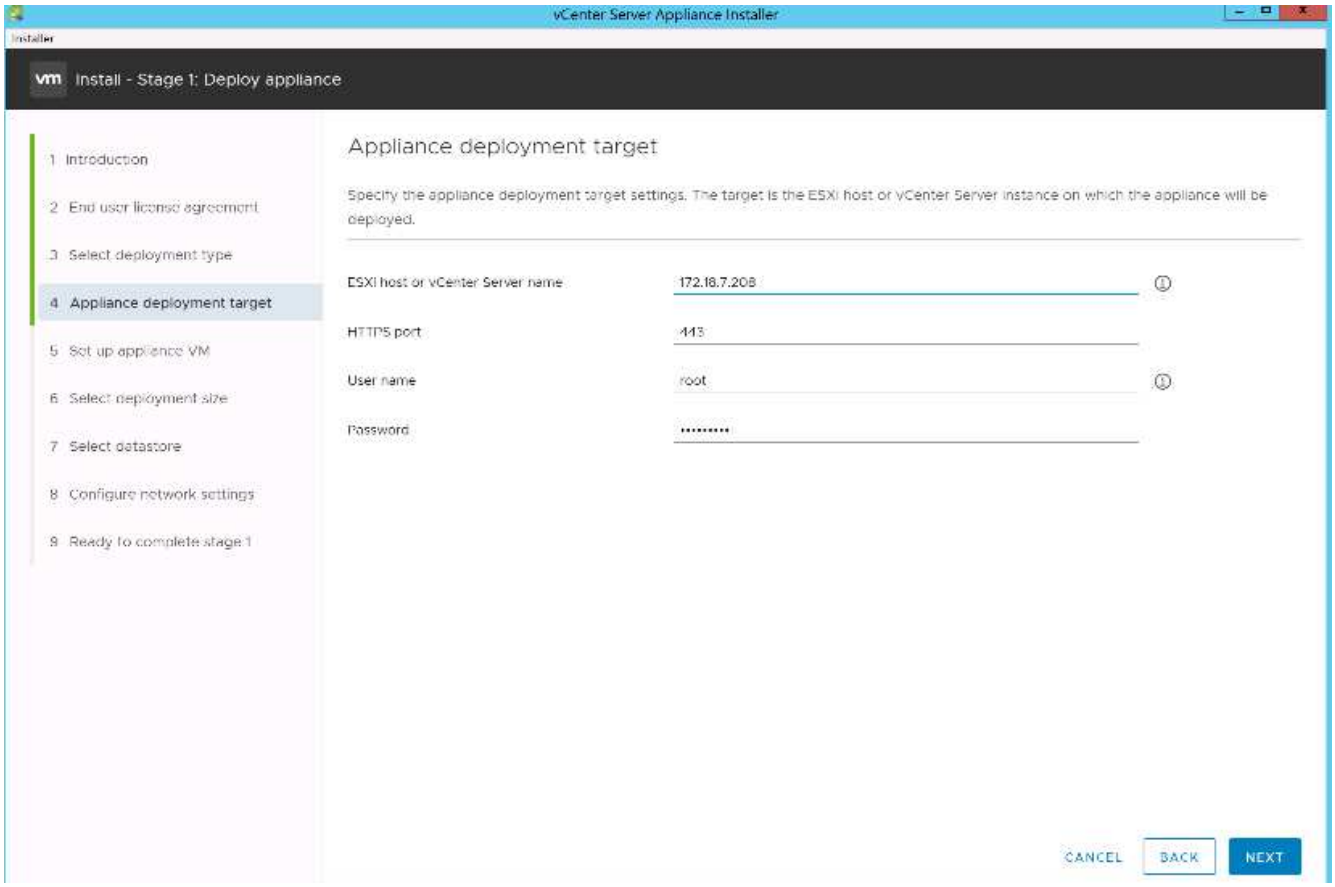
Embora o Microsoft Windows vCenter Server instalável seja suportado, a VMware recomenda o VCSA para novas implantações.

3. Monte a imagem ISO.
4. Navegue para o `vcsa-ui-installer` diretório > `win32`. Clique duas vezes `installer.exe` em .
5. Clique em Instalar.
6. Clique em Avançar na página Introdução.
7. Aceite o EULA.
8. Selecione controlador de serviços de plataforma incorporada como o tipo de implantação.

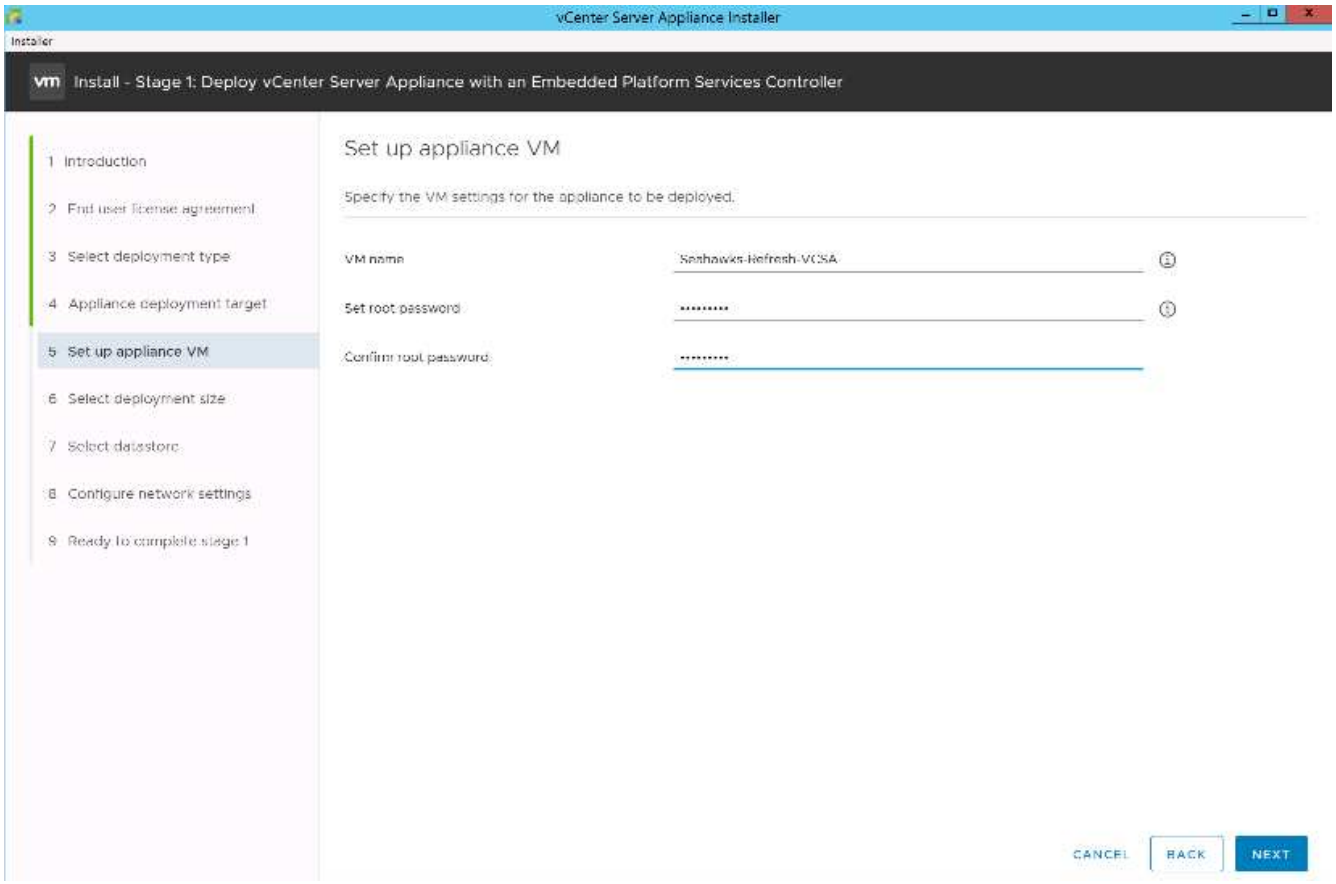


Se necessário, a implantação do controlador de serviços de plataforma externa também é suportada como parte da solução FlexPod Express.

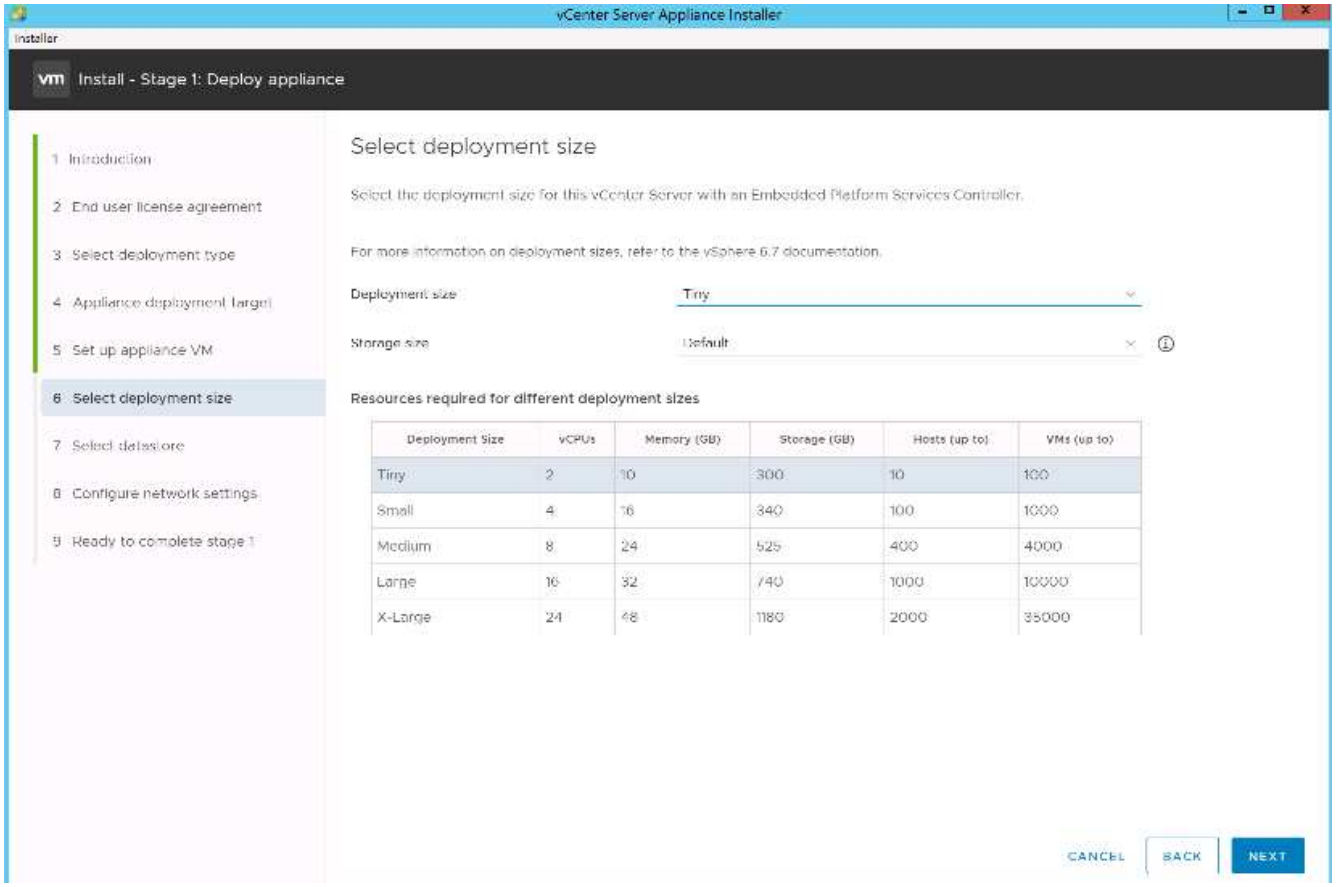
9. Na página destino de implantação do dispositivo, insira o endereço IP de um host ESXi que você implantou, o nome de usuário raiz e a senha raiz. Clique em seguinte.



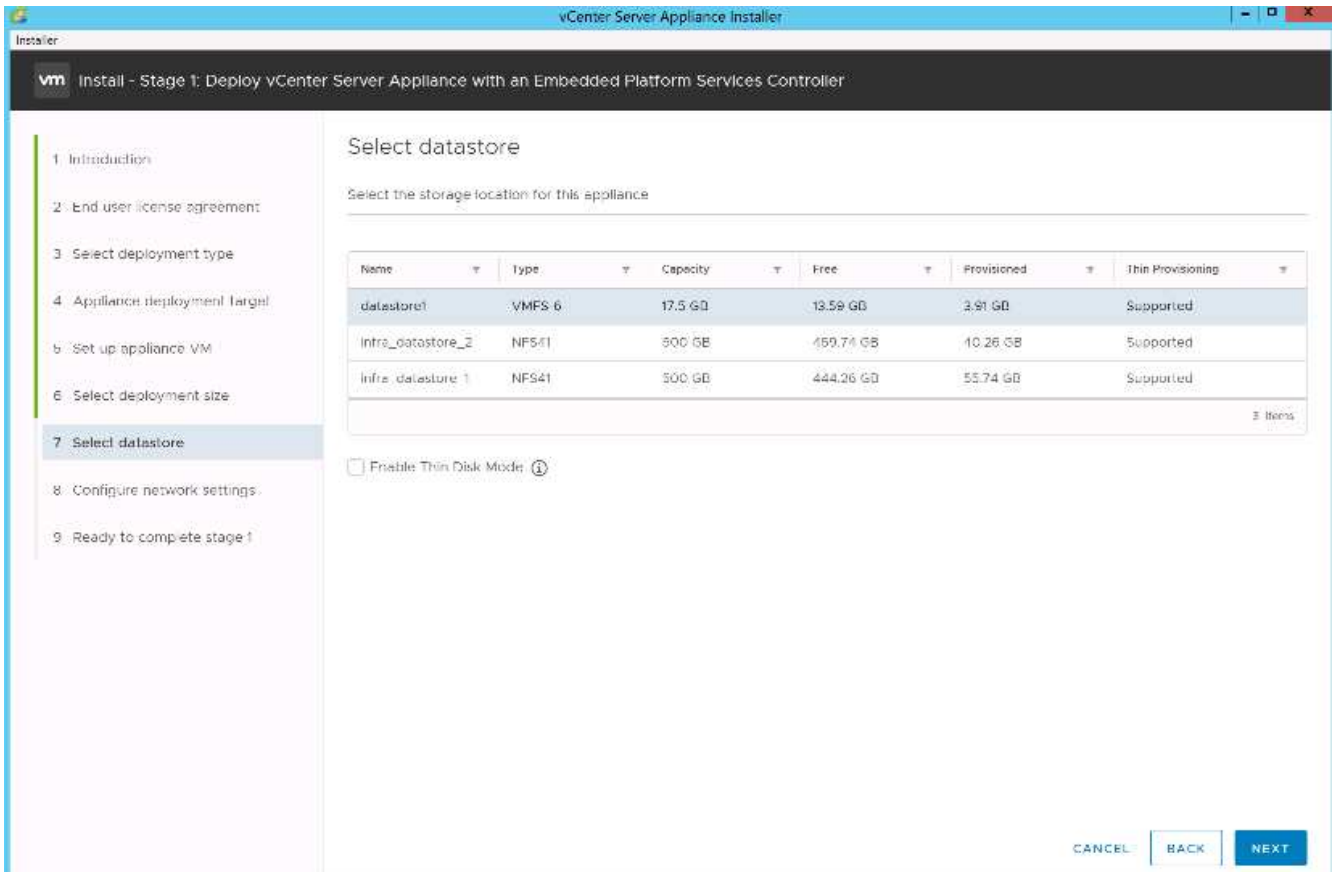
10. Defina a VM do appliance inserindo o VCSA como o nome da VM e a senha raiz que você gostaria de usar para o VCSA. Clique em seguinte.



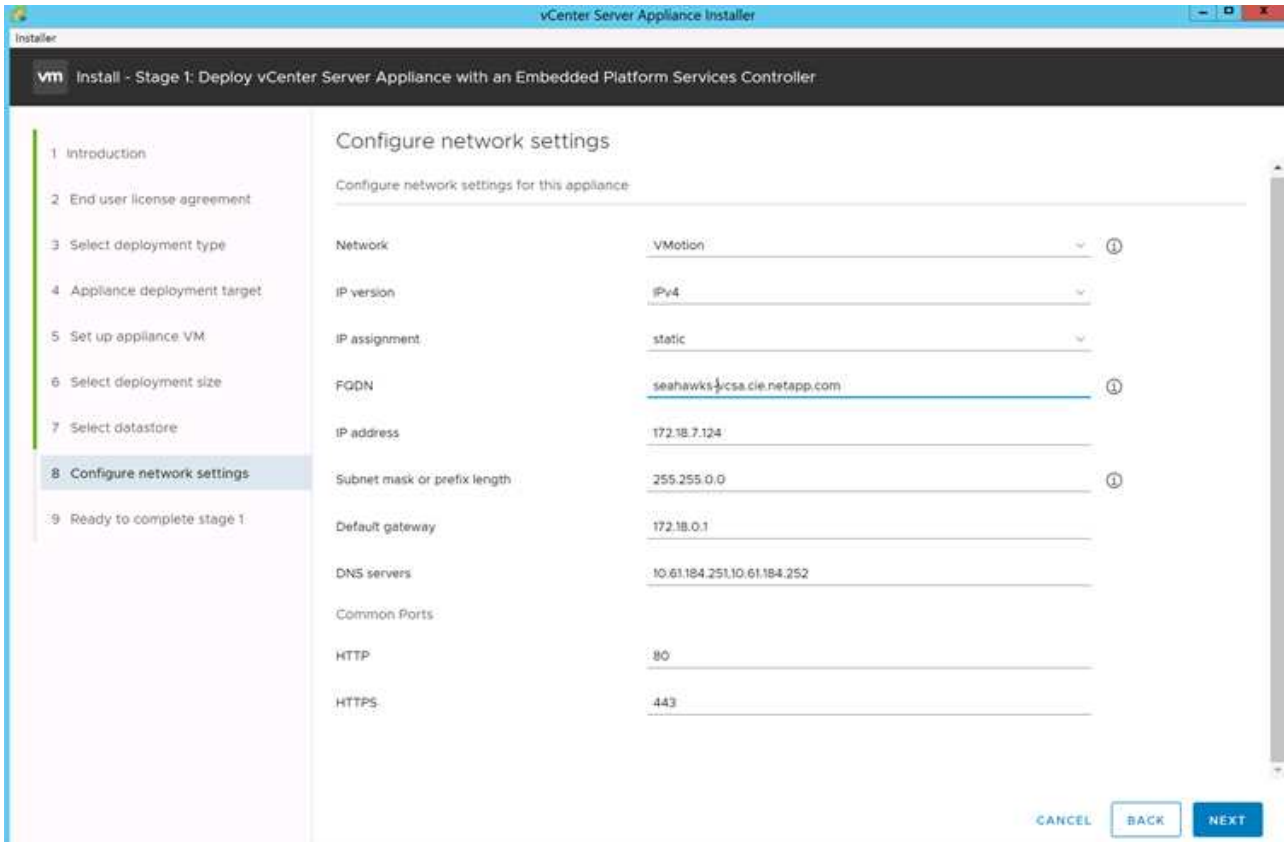
11. Selecione o tamanho de implantação que melhor se adapta ao seu ambiente. Clique em seguinte.



12. Selecione o `infra_datastore_1` datastore. Clique em seguinte.



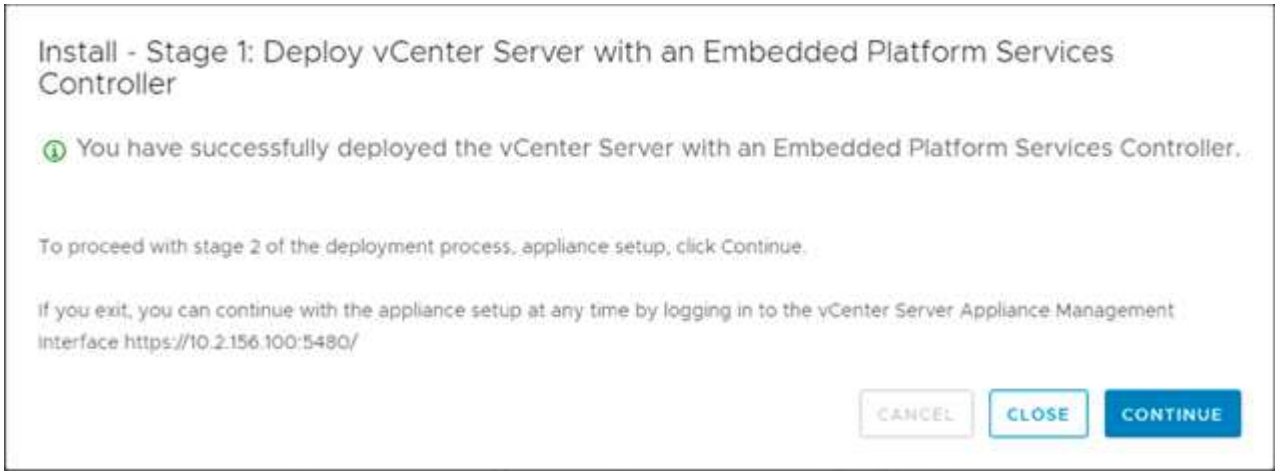
13. Introduza as seguintes informações na página Configurar definições de rede e clique em seguinte.
    a. Selecione MGMT-Network como sua rede.
    b. Introduza o FQDN ou IP a utilizar para o VCSA.
    c. Introduza o endereço IP a utilizar.
    d. Introduza a máscara de sub-rede a utilizar.
    e. Introduza o gateway predefinido.
    f. Introduza o servidor DNS.



14. Na página Pronto para concluir a fase 1, verifique se as configurações inseridas estão corretas. Clique em concluir.

    O VCSA é instalado agora. Este processo demora vários minutos.

15. Após a conclusão da fase 1, aparece uma mensagem informando que ela foi concluída. Clique em continuar para iniciar a configuração da fase 2.



16. Na página Introdução do Estágio 2, clique em Avançar.
17. Introduza `<<var_ntp_id>>` para o endereço do servidor NTP. Pode introduzir vários endereços IP NTP.

    Se você planeja usar a alta disponibilidade do vCenter Server, verifique se o acesso SSH está habilitado.

18. Configure o nome de domínio SSO, a senha e o nome do site. Clique em seguinte.

Registe estes valores para a sua referência, especialmente se se desviar do `vsphere.local` nome de domínio.

19. Junte-se ao Programa de experiência do Cliente da VMware, se desejado. Clique em seguinte.
20. Veja o resumo das suas definições. Clique em concluir ou use o botão voltar para editar as configurações.
21. Uma mensagem é exibida informando que você não é capaz de pausar ou parar a instalação de concluir depois que ela foi iniciada. Clique em OK para continuar.

    A configuração do aparelho continua. Isso leva vários minutos.

    É apresentada uma mensagem a indicar que a configuração foi bem-sucedida.

    Os links que o instalador fornece para acessar o vCenter Server são clicáveis.

Configurar o cluster do VMware vCenter Server 6,7 e vSphere

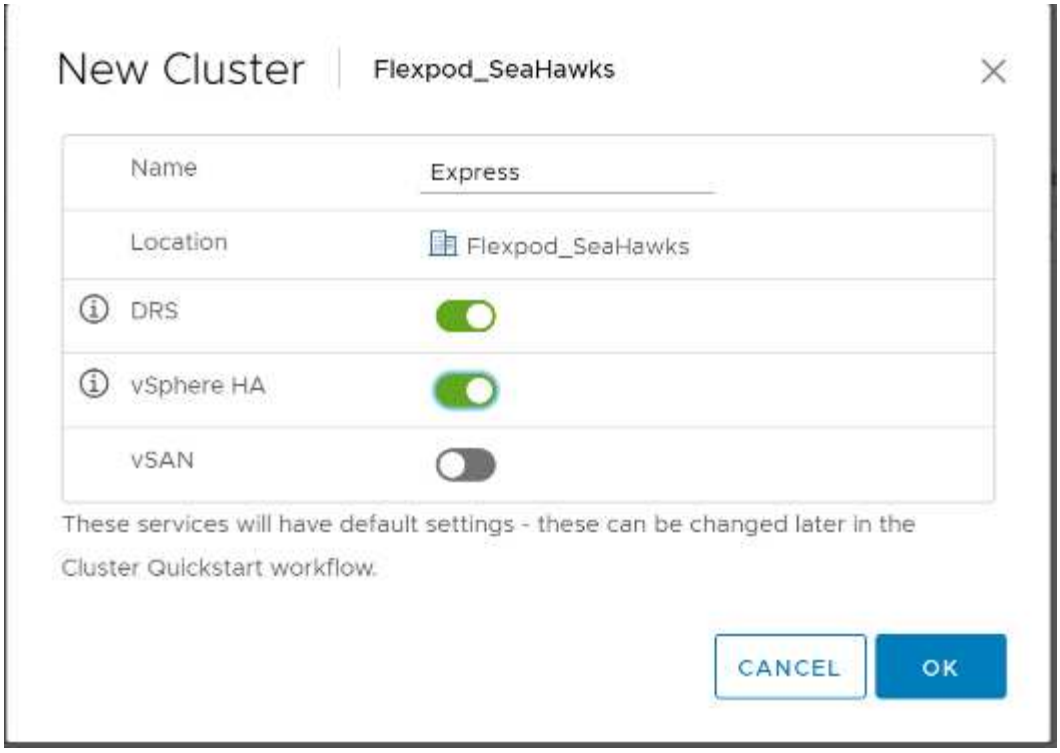
Para configurar o cluster do VMware vCenter Server 6,7 e vSphere, execute as seguintes etapas:

1. Navegue até https://<<FQDN ou IP do vCenter>>/vsphere-client/.
2. Clique em Launch vSphere Client.
3. Inicie sessão com o nome de utilizador administrator e a palavra-passe SSO que introduziu durante o processo de configuração do VCSA.
4. Clique com o botão direito no nome do vCenter e selecione novo data center.
5. Introduza um nome para o centro de dados e clique em OK.

Criar cluster do vSphere.

Para criar um cluster vSphere, execute as seguintes etapas:

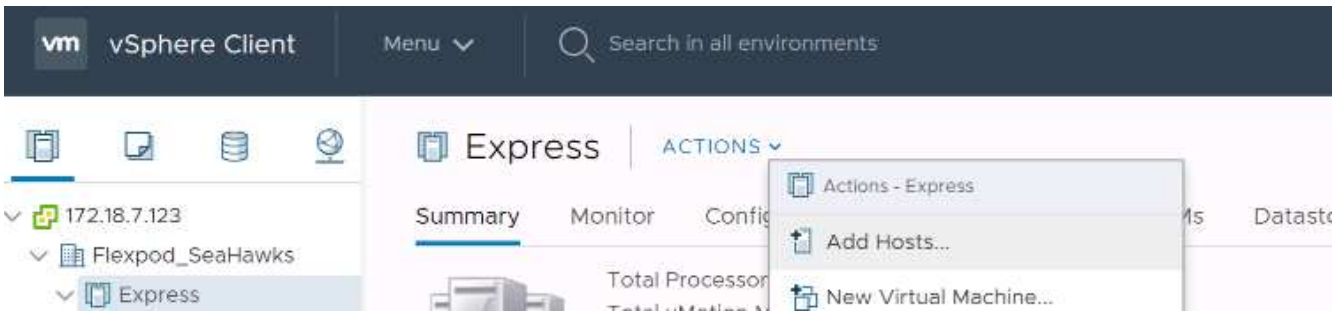
1. Clique com o botão direito do rato no data center recém-criado e selecione novo cluster.
2. Introduza um nome para o cluster.
3. Selecione e ative as opções DRS e vSphere HA.
4. Clique em OK.



Adicione hosts ESXi ao Cluster

Para adicionar hosts ESXi ao cluster, execute as seguintes etapas:

1. Selecione Adicionar anfitrião no menu ações do cluster.



2. Para adicionar um host ESXi ao cluster, execute as seguintes etapas:
   a. Insira o IP ou FQDN do host. Clique em seguinte.
   b. Introduza o nome de utilizador e a palavra-passe raiz. Clique em seguinte.
   c. Clique em Sim para substituir o certificado do host por um certificado assinado pelo servidor de certificados VMware.
   d. Clique em Next (seguinte) na página Host Summary (Resumo do anfitrião).
   e. Clique no ícone verde para adicionar uma licença ao host vSphere.

      Este passo pode ser concluído mais tarde, se desejado.

   f. Clique em seguinte para deixar o modo de bloqueio desativado.
   g. Clique em Avançar na página de localização da VM.

h. Reveja a página Pronto para concluir. Use o botão voltar para fazer quaisquer alterações ou selecione concluir.

3. Repita as etapas 1 e 2 para o host B. do Cisco UCS

   Esse processo deve ser concluído para quaisquer hosts adicionais adicionados à configuração do FlexPod Express.

Configure o coredump em hosts ESXi

Configuração do coletor de descarga ESXi para hosts inicializados por iSCSI

Os hosts ESXi inicializados com iSCSI usando o iniciador de software VMware iSCSI precisam ser configurados para fazer despejos principais no coletor de despejo ESXi que faz parte do vCenter. O Coletor de descarga não está habilitado por padrão no vCenter Appliance. Esse procedimento deve ser executado no final da seção implantação do vCenter. Para configurar o coletor de descarga ESXi, siga estas etapas:

1. Faça login no vSphere Web Client como mailto:administrator e selecione Home.
2. No painel central, clique em Configuração do sistema.
3. No painel esquerdo, selecione Serviços.
4. Em Serviços, clique em VMware vSphere ESXi Dump Collector.
5. No painel central, clique no ícone verde Iniciar para iniciar o serviço.
6. No menu ações, clique em Editar tipo de inicialização.
7. Selecione Automático.
8. Clique em OK.
9. Conete-se a cada host ESXi usando ssh como root.
10. Execute os seguintes comandos:

```
esxcli system coredump network set –v vmk0 –j <vcenter-ip>
esxcli system coredump network set –e true
esxcli system coredump network check
```

A mensagem `Verified the configured netdump server is running` aparece depois de executar o comando final.

Esse processo deve ser concluído para quaisquer hosts adicionais adicionados ao FlexPod Express.

Conclusão

O FlexPod Express fornece uma solução simples e eficaz fornecendo um design validado que usa componentes líderes do setor. Com o dimensionamento por meio da adição de componentes adicionais, o FlexPod Express pode ser personalizado para necessidades específicas de negócios. O FlexPod Express foi projetado tendo em mente empresas de pequeno e médio porte, ROBOs e outras empresas que exigem soluções dedicadas.

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- DESIGN de NVA- 1130: FlexPod Express com VMware vSphere 6.7U1 e NetApp AFF A220 com design de NVA de armazenamento baseado em IP de conexão direta

  "https://www.netapp.com/us/media/nva-1130-design.pdf"

- Centro de Documentação de sistemas AFF e FAS

  "http://docs.netapp.com/platstor/index.jsp"

- Centro de Documentação do ONTAP 9

  "http://docs.netapp.com/ontap-9/index.jsp"

- Documentação do produto NetApp

  "https://docs.netapp.com"

FlexPod Express para VMware vSphere 7,0 com Cisco UCS Mini e NetApp AFF/FAS - NVA - implantação

Jyh-shing Chen, NetApp

O FlexPod Express para VMware vSphere com a solução Cisco UCS Mini e NetApp AFF/FAS aproveita o Cisco UCS Mini com B200 M5 servidores blade, interconexões de malha no chassi do Cisco UCS 6324, switches Cisco Nexus 31108PC-V ou outros switches compatíveis e o par de HA do controlador da série NetApp AFF A220, C190 ou FAS2700, que executa o software de gerenciamento de dados NetApp ONTAP 9 7,0. Este documento de implantação da arquitetura verificada do NetApp (NVA) fornece as etapas detalhadas necessárias para configurar os componentes da infraestrutura e implantar o VMware vSphere 7,0 e as ferramentas associadas para criar uma infraestrutura virtual baseada no FlexPod Express altamente confiável e altamente disponível.

"FlexPod Express para VMware vSphere 7,0 com Cisco UCS Mini e NetApp AFF/FAS - NVA - implantação"

FlexPod e Segurança

FlexPod, a solução para ransomware

TR-4802: FlexPod, a solução para ransomware

Arvind Ramakrishnan, NetApp

Em parceria com: 

Para entender o ransomware, é necessário primeiro entender alguns pontos-chave sobre criptografia. Os métodos criptográficos permitem a criptografia de dados com uma chave secreta compartilhada (criptografia de chave simétrica) ou um par de chaves (criptografia de chave assimétrica). Uma dessas chaves é uma chave pública amplamente disponível e a outra é uma chave privada não revelada.

Ransomware é um tipo de malware que é baseado em criptovirologia, que é o uso de criptografia para construir software malicioso. Esse malware pode fazer uso de criptografia de chave simétrica e assimétrica para bloquear os dados da vítima e exigir um resgate para fornecer a chave para descriptografar os dados da vítima.

Como funciona o ransomware?

As etapas a seguir descrevem como o ransomware usa criptografia para criptografar os dados da vítima sem qualquer escopo de descriptografia ou recuperação pela vítima:

1. O invasor gera um par de chaves como em criptografia de chave assimétrica. A chave pública que é gerada é colocada dentro do malware, e o malware é então lançado.
2. Depois que o malware entrou no computador ou sistema da vítima, ele gera uma chave simétrica aleatória usando um gerador de números pseudorandom (PRNG) ou qualquer outro algoritmo gerador de números aleatórios viável.
3. O malware usa essa chave simétrica para criptografar os dados da vítima. Ele eventualmente criptografa a chave simétrica usando a chave pública do invasor que foi incorporada no malware. A saída desta etapa é um cifrotexto assimétrico da chave simétrica criptografada e o cifrotexto simétrico dos dados da vítima.
4. O malware zeroiza (apaga) os dados da vítima e a chave simétrica que foi usada para criptografar os dados, não deixando espaço para recuperação.
5. A vítima agora é mostrado o texto cifrado assimétrico da chave simétrica e um valor de resgate que deve ser pago para obter a chave simétrica que foi usada para criptografar os dados.
6. A vítima paga o resgate e compartilha o texto cifrado assimétrico com o atacante. O invasor descriptografa o texto cifrado com sua chave privada, o que resulta na chave simétrica.
7. O invasor compartilha essa chave simétrica com a vítima, que pode ser usada para descriptografar todos os dados e, assim, recuperar do ataque.

Desafios

Indivíduos e organizações enfrentam os seguintes desafios quando são atacados por ransomware:

- O desafio mais importante é que isso afeta imediatamente a produtividade da organização ou do indivíduo. Leva tempo para retornar a um estado de normalidade, porque todos os arquivos importantes devem ser recuperados e os sistemas devem ser protegidos.
- Isso pode levar a uma violação de dados que contenha informações confidenciais e confidenciais que pertençam a clientes ou clientes e que leve a uma situação de crise que uma organização claramente gostaria de evitar.
- Há uma chance muito boa de os dados entrarem nas mãos erradas ou serem apagados completamente, o que leva a um ponto sem retorno que pode ser desastroso para organizações e indivíduos.
- Depois de pagar o resgate, não há garantia de que o invasor fornecerá a chave para restaurar os dados.
- Não há garantia de que o invasor se abstenha de transmitir os dados confidenciais, apesar de pagar o resgate.
- Em grandes empresas, identificar a lacuna que levou a um ataque de ransomware é uma tarefa tediosa e proteger todos os sistemas envolve muito esforço.

Quem está em risco?

Qualquer pessoa pode ser atacada por ransomware, incluindo indivíduos e grandes organizações. As organizações que não implementam medidas e práticas de segurança bem definidas são ainda mais vulneráveis a tais ataques. O efeito do ataque em uma grande organização pode ser várias vezes maior do que o que um indivíduo pode suportar.

O ransomware é responsável por aproximadamente 28% de todos os ataques de malware. Em outras palavras, mais de um em cada quatro incidentes de malware é um ataque de ransomware. O ransomware pode se espalhar automaticamente e indiscriminadamente pela internet e, quando houver um lapso de segurança, ele pode entrar nos sistemas da vítima e continuar a se espalhar para outros sistemas conetados. Os invasores tendem a segmentar pessoas ou organizações que realizam muito compartilhamento de arquivos, têm muitos dados confidenciais e críticos ou mantêm proteção inadequada contra ataques.

Os atacantes tendem a se concentrar nos seguintes alvos potenciais:

- Universidades e comunidades estudantis
- Escritórios e agências governamentais
- Hospitais
- Bancos

Esta não é uma lista exaustiva de alvos. Você não pode se considerar seguro de ataques se você cair fora de uma dessas categorias.

Como o ransomware entra em um sistema ou se espalha?

Existem várias maneiras pelas quais o ransomware pode entrar em um sistema ou se espalhar para outros sistemas. No mundo de hoje, quase todos os sistemas estão conetados uns aos outros através da internet, LANs, WANs, e assim por diante. A quantidade de dados que está sendo gerada e trocada entre esses sistemas está aumentando apenas.

Algumas das maneiras mais comuns pelas quais o ransomware pode se espalhar incluem métodos que usamos diariamente para compartilhar ou acessar dados:

- E-mail
- Redes P2PG.
- Downloads de arquivos
- Redes sociais
- Dispositivos móveis
- Conetando-se a redes públicas inseguras
- Acessando URLs da Web

Consequências da perda de dados

As consequências ou os efeitos da perda de dados podem chegar mais amplamente do que as organizações podem prever. Os efeitos podem variar dependendo da duração do tempo de inatividade ou do período durante o qual uma organização não tem acesso aos seus dados. Quanto mais tempo o ataque durar, maior será o efeito sobre a receita, a marca e a reputação da organização. Uma organização também pode enfrentar problemas legais e um declínio acentuado na produtividade.

À medida que essas questões continuam a persistir ao longo do tempo, elas começam a ampliar e podem acabar mudando a cultura de uma organização, dependendo de como ela responde ao ataque. No mundo de hoje, as informações se espalham rapidamente e as notícias negativas sobre uma organização podem causar danos permanentes à sua reputação. Uma organização pode enfrentar grandes penalidades por perda de dados, o que pode eventualmente levar ao encerramento de um negócio.

Efeitos financeiros

De acordo com um "Relatório da McAfee" recente , os custos globais incorridos devido ao cibercrime são cerca de $600 mil milhões de dólares, o que representa cerca de 0,8% do PIB global. Quando este montante é comparado com a crescente economia mundial da Internet de $4,2 biliões de dólares, equivale a um imposto de 14% sobre o crescimento.

O ransomware tem uma parte significativa desse custo financeiro. Em 2018, os custos incorridos devido a ataques de ransomware foram de aproximadamente $8 bilhões de dólares—um valor previsto para chegar a $11,5 bilhões de dólares em 2019.

Qual é a solução?

A recuperação de um ataque de ransomware com o mínimo de tempo de inatividade só é possível com a implementação de um plano proativo de recuperação de desastres. Ter a capacidade de se recuperar de um ataque é bom, mas prevenir um ataque é ideal.

Embora existam várias frentes que você deve revisar e corrigir para evitar um ataque, o componente principal que permite prevenir ou recuperar de um ataque é o data center.

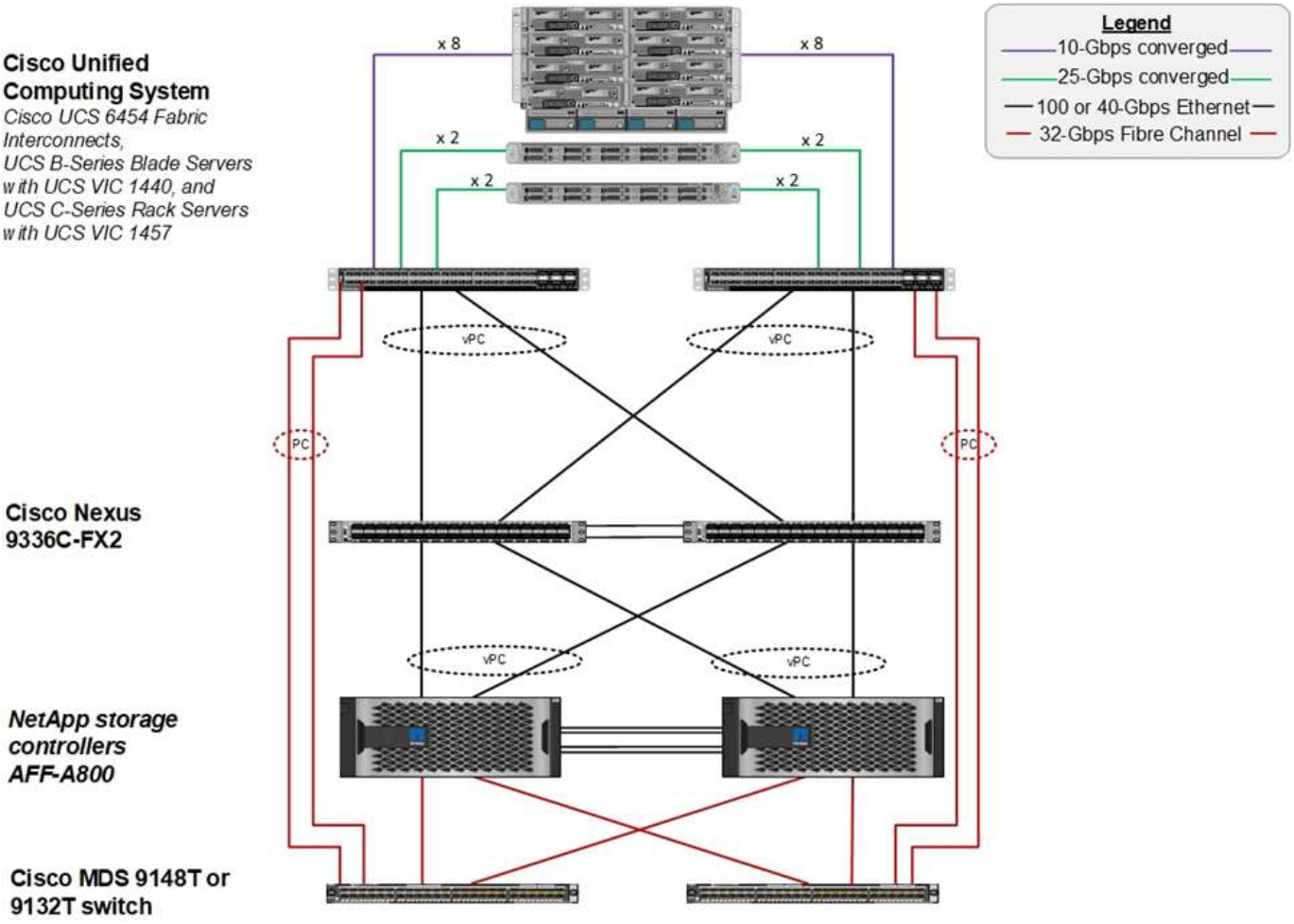
O design do data center e os recursos fornecidos para proteger a rede, a computação e os pontos de extremidade de storage desempenham um papel essencial na criação de um ambiente seguro para operações diárias. Este documento mostra como os recursos de uma infraestrutura de nuvem híbrida da FlexPod podem ajudar na recuperação rápida de dados em caso de ataque e também podem ajudar a prevenir ataques completamente.

Visão geral do FlexPod

O FlexPod é uma arquitetura pré-projetada, integrada e validada que combina servidores

do sistema de computação unificada (Cisco UCS) da Cisco, a família de switches Cisco Nexus, switches de malha Cisco MDS e storage arrays NetApp em uma única arquitetura flexível. As soluções da FlexPod foram desenvolvidas para oferecer alta disponibilidade sem um único ponto de falha, ao mesmo tempo em que mantêm economia e flexibilidade de design para dar suporte a uma ampla variedade de workloads. Um design FlexPod pode dar suporte a diferentes hipervisores e servidores bare metal, além de poder ser dimensionado e otimizado com base nos requisitos de carga de trabalho do cliente.

A figura abaixo ilustra a arquitetura do FlexPod e destaca claramente a alta disponibilidade em todas as camadas da pilha. Os componentes de infraestrutura de storage, rede e computação são configurados de tal forma que as operações podem falhar instantaneamente para o parceiro sobrevivente, no caso de um dos componentes falhar.



Uma grande vantagem para um sistema FlexPod é que ele foi pré-projetado, integrado e validado para vários workloads. Guias detalhados de projeto e implantação são publicados para cada validação de solução. Esses documentos incluem as práticas recomendadas que você precisa empregar para que os workloads sejam executados de forma otimizada no FlexPod. Essas soluções são criadas com os melhores produtos de computação, rede e storage da categoria, além de uma série de recursos que se concentram na segurança e no fortalecimento de toda a infraestrutura.

"Índice de Inteligência de ameaças X-Force da IBM" afirma: "Erro humano responsável por dois terços dos Registros comprometidos, incluindo o salto histórico de 424% na infraestrutura de nuvem mal configurada."

Com o sistema FlexPod, você evita a configuração incorreta da infraestrutura usando a automação por meio

dos playbooks do Ansible que executam uma configuração completa da infraestrutura de acordo com as práticas recomendadas descritas em Cisco Validated designs (CVDs) e NetApp Verified Architectures (NVAs).

Medidas de proteção contra ransomware

Esta seção discute os principais recursos do software de gerenciamento de dados do NetApp ONTAP e as ferramentas do Cisco UCS e do Cisco Nexus que você pode usar para proteger e recuperar de ataques de ransomware com eficácia.

Armazenamento: NetApp ONTAP

O software ONTAP fornece muitos recursos úteis para a proteção de dados, a maioria dos quais é gratuita para clientes que têm um sistema ONTAP. Você pode usar os recursos a seguir em todos os momentos para proteger dados contra ataques:

- **Tecnologia NetApp Snapshot.** Uma cópia Snapshot é uma imagem somente leitura de um volume que captura o estado de um sistema de arquivos em um momento. Essas cópias ajudam a proteger os dados sem afetar a performance do sistema e, ao mesmo tempo, não ocupam muito espaço de storage. A NetApp recomenda que você crie um cronograma para a criação de cópias Snapshot. Você também deve manter um longo tempo de retenção porque alguns malwares podem ficar inativos e reativar semanas ou meses após uma infeção. No caso de um ataque, o volume pode ser revertido usando uma cópia Snapshot obtida antes da infeção.
- **Tecnologia NetApp SnapRestore.** Software de recuperação de dados SnapRestore é extremamente útil para recuperar de corrupção de dados ou para reverter apenas o conteúdo do arquivo. O SnapRestore não reverte os atributos de um volume; é muito mais rápido do que o que um administrador pode conseguir copiando arquivos da cópia Snapshot para o sistema de arquivos ativo. A velocidade em que os dados podem ser recuperados é útil quando muitos arquivos devem ser recuperados o mais rápido possível. No caso de um ataque, esse processo de recuperação altamente eficiente ajuda a colocar os negócios de volta on-line rapidamente.
- **Tecnologia NetApp SnapCenter.** O software SnapCenter usa funções de replicação e backup baseadas em storage da NetApp para fornecer proteção de dados consistente com aplicações. Esse software é integrado a aplicações empresariais e fornece fluxos de trabalho específicos para aplicações e bancos de dados para atender às necessidades dos administradores de infraestrutura virtual, banco de dados e aplicativos. O SnapCenter fornece uma plataforma empresarial fácil de usar para coordenar e gerenciar com segurança a proteção de dados em aplicações, bancos de dados e sistemas de arquivos. A capacidade de fornecer proteção de dados consistente com aplicações é essencial durante a recuperação de dados, porque facilita a restauração das aplicações para um estado consistente com mais rapidez.
- **Tecnologia NetApp SnapLock.** O SnapLock fornece um volume de propósito especial no qual os arquivos podem ser armazenados e comprometidos com um estado não apagável e não regravável. Os dados de produção do usuário que residem em um FlexVol volume podem ser espelhados ou abobadados a um volume SnapLock por meio da tecnologia NetApp SnapMirror ou SnapVault, respetivamente. Os arquivos no volume SnapLock, o próprio volume e seu agregado de hospedagem não podem ser excluídos até o final do período de retenção.
- **Tecnologia NetApp FPolicy.** Use o software FPolicy para evitar ataques, despermitindo operações em arquivos com extensões específicas. Um evento FPolicy pode ser acionado para operações de arquivo específicas. O evento está vinculado a uma política, que chama o mecanismo que ele precisa usar. Você pode configurar uma política com um conjunto de extensões de arquivo que podem potencialmente conter ransomware. Quando um arquivo com uma extensão não permitida tenta executar uma operação não autorizada, o FPolicy impede que essa operação seja executada.

Rede: Cisco

O software Cisco NX os suporta o recurso NetFlow que permite a deteção aprimorada de anomalias e segurança da rede. O NetFlow captura os metadados de cada conversa na rede, as partes envolvidas na comunicação, o protocolo que está sendo usado e a duração da transação. Depois que as informações são agregadas e analisadas, elas podem fornecer informações sobre o comportamento normal.

Os dados coletados também permitem a identificação de padrões questionáveis de atividade, como malware que se espalha pela rede, o que pode passar despercebido.

O NetFlow usa fluxos para fornecer estatísticas para monitoramento de rede. Um fluxo é um fluxo unidirecional de pacotes que chega em uma interface de origem (ou VLAN) e tem os mesmos valores para as chaves. Uma chave é um valor identificado para um campo dentro do pacote. Você cria um fluxo usando um Registro de fluxo para definir as chaves exclusivas para o seu fluxo. Você pode exportar os dados que o NetFlow coleta para seus fluxos usando um exportador de fluxo para um coletor NetFlow remoto, como o Cisco Stealthwatch. O Stealthwatch usa essas informações para monitoramento contínuo da rede e fornece deteção de ameaças em tempo real e respostas forenses a incidentes se ocorrer um surto de ransomware.

Computação: Cisco UCS

O Cisco UCS é o ponto de extremidade de computação em uma arquitetura FlexPod. Você pode usar vários produtos Cisco que podem ajudar a proteger essa camada da pilha no nível do sistema operacional.

Você pode implementar os seguintes produtos-chave na camada de computação ou aplicação:

- **Proteção avançada contra malware (AMP) da Cisco para Endpoints.** Suportada em sistemas operativos Microsoft Windows e Linux, esta solução integra capacidades de prevenção, deteção e resposta. Este software de segurança impede violações, bloqueia malware no ponto de entrada e monitora e analisa continuamente as atividades de arquivo e processo para detetar, conter e corrigir rapidamente ameaças que podem evitar defesas de linha de frente.

  O componente proteção contra atividades maliciosas (MAP) do AMP monitora continuamente todas as atividades de endpoint e fornece deteção em tempo de execução e bloqueio de comportamento anormal de um programa em execução no endpoint. Por exemplo, quando o comportamento do endpoint indica ransomware, os processos ofensivos são encerrados, impedindo a criptografia do endpoint e interrompendo o ataque.

- **Proteção avançada contra malware da Cisco para segurança de e-mail.** Os e-mails se tornaram o principal veículo para espalhar malware e realizar ataques cibernéticos. Em média, cerca de 100 bilhões de e-mails são trocados em um único dia, o que fornece aos invasores um excelente vetor de penetração nos sistemas do usuário. Portanto, é absolutamente essencial defender-se contra esta linha de ataque.

  AMP analisa e-mails para ameaças como explorações de dia zero e malware furtivo escondido em anexos maliciosos. Ele também usa inteligência de URL líder do setor para combater links maliciosos. Ele oferece aos usuários proteção avançada contra spear phishing, ransomware e outros ataques sofisticados.

- **Sistema de prevenção de intrusão de próxima geração (NGIPS).** O Cisco Firepower NGIPS pode ser implantado como um dispositivo físico no data center ou como um dispositivo virtual no VMware (NGIPSv para VMware). Este sistema de prevenção de intrusão altamente eficaz proporciona um desempenho fiável e um baixo custo total de propriedade. A proteção contra ameaças pode ser expandida com licenças de assinatura opcionais para fornecer AMP, visibilidade e controle de aplicativos e recursos de filtragem de URL. O NGIPS virtualizado inspeciona o tráfego entre máquinas virtuais (VMs) e facilita a implantação e o gerenciamento de soluções NGIPS em locais com recursos limitados, aumentando a proteção para ativos físicos e virtuais.

Proteja e recupere dados no FlexPod

Esta seção descreve como os dados de um usuário final podem ser recuperados em caso de ataque e como os ataques podem ser evitados usando um sistema FlexPod.

Visão geral do testbed

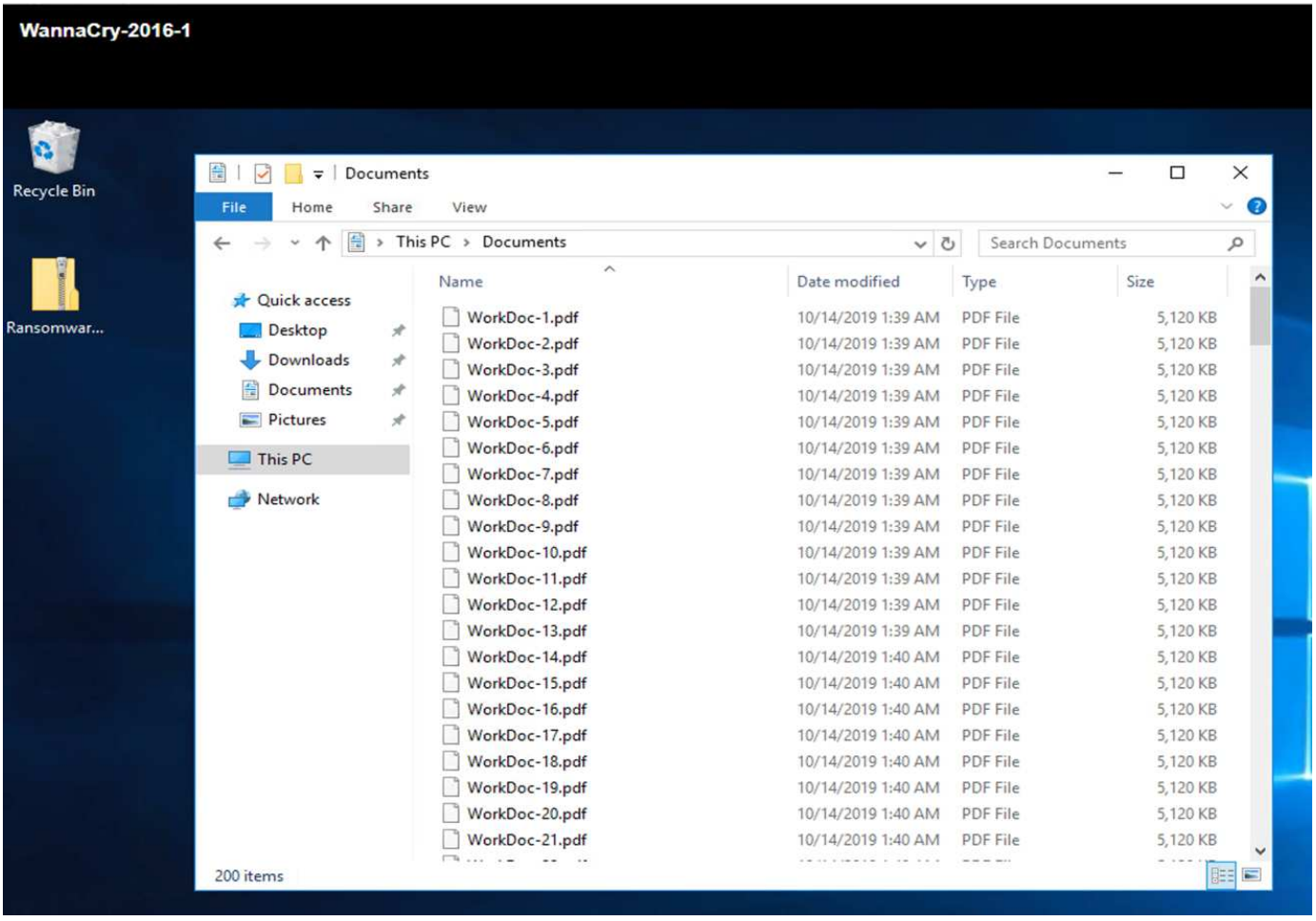
Para mostrar a deteção, correção e prevenção do FlexPod, um testbed foi construído com base nas diretrizes que são especificadas na plataforma mais recente disponível CVD no momento em que este documento foi escrito: "Data center FlexPod com VMware vSphere 6,7 U1, Cisco UCS 4th geração e NetApp AFF A-Series CVD".

Uma VM do Windows 2016, que forneceu um compartilhamento CIFS do software NetApp ONTAP, foi implantada na infraestrutura do VMware vSphere. Então o NetApp FPolicy foi configurado no compartilhamento CIFS para impedir a execução de arquivos com determinados tipos de extensão. O software NetApp SnapCenter também foi implantado para gerenciar as cópias Snapshot das VMs na infraestrutura, a fim de fornecer cópias Snapshot consistentes com aplicações.

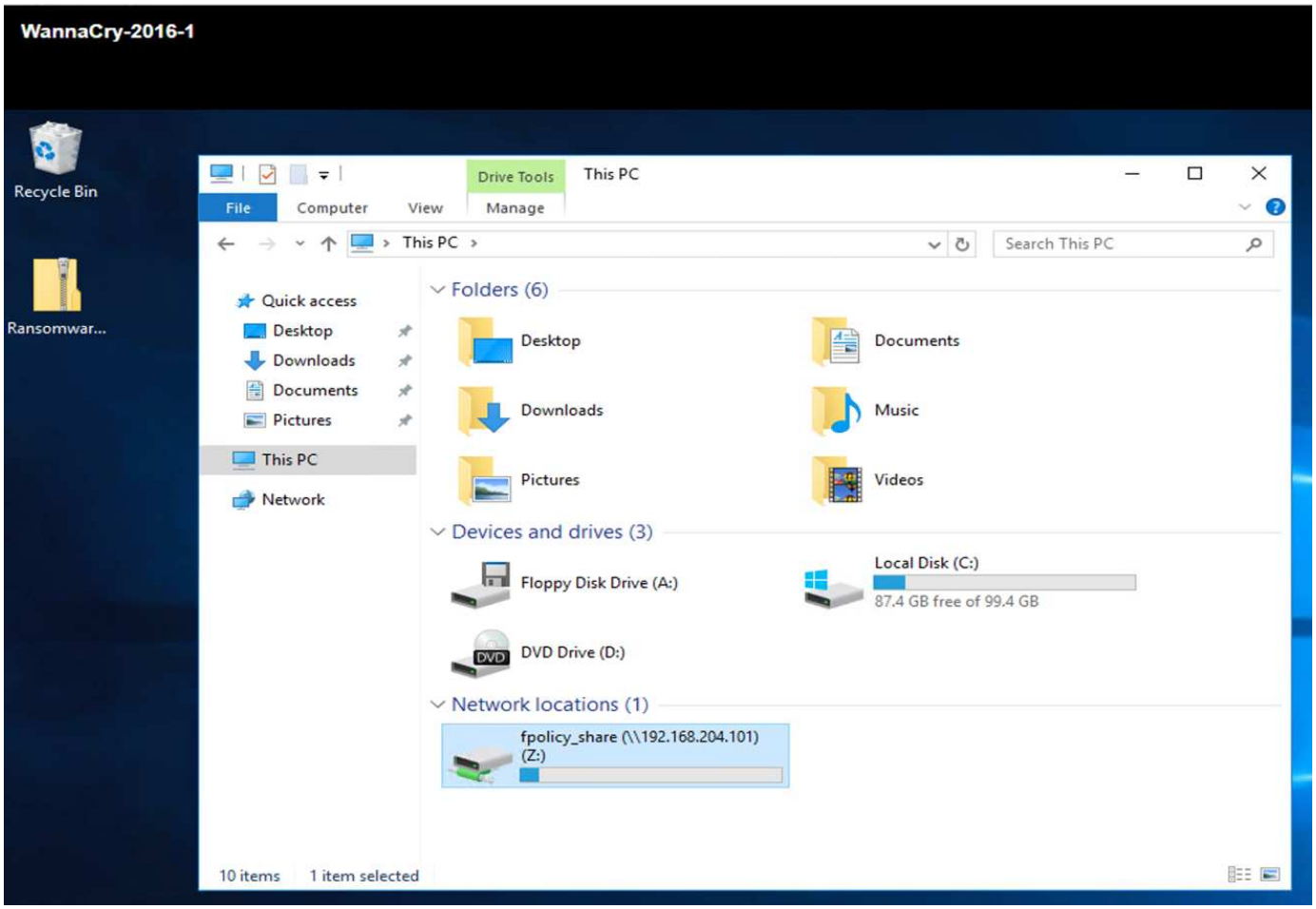
Estado da VM e seus arquivos antes de um ataque

Esta seção mostra o estado dos arquivos antes de um ataque à VM e o compartilhamento CIFS que foi mapeado para ela.

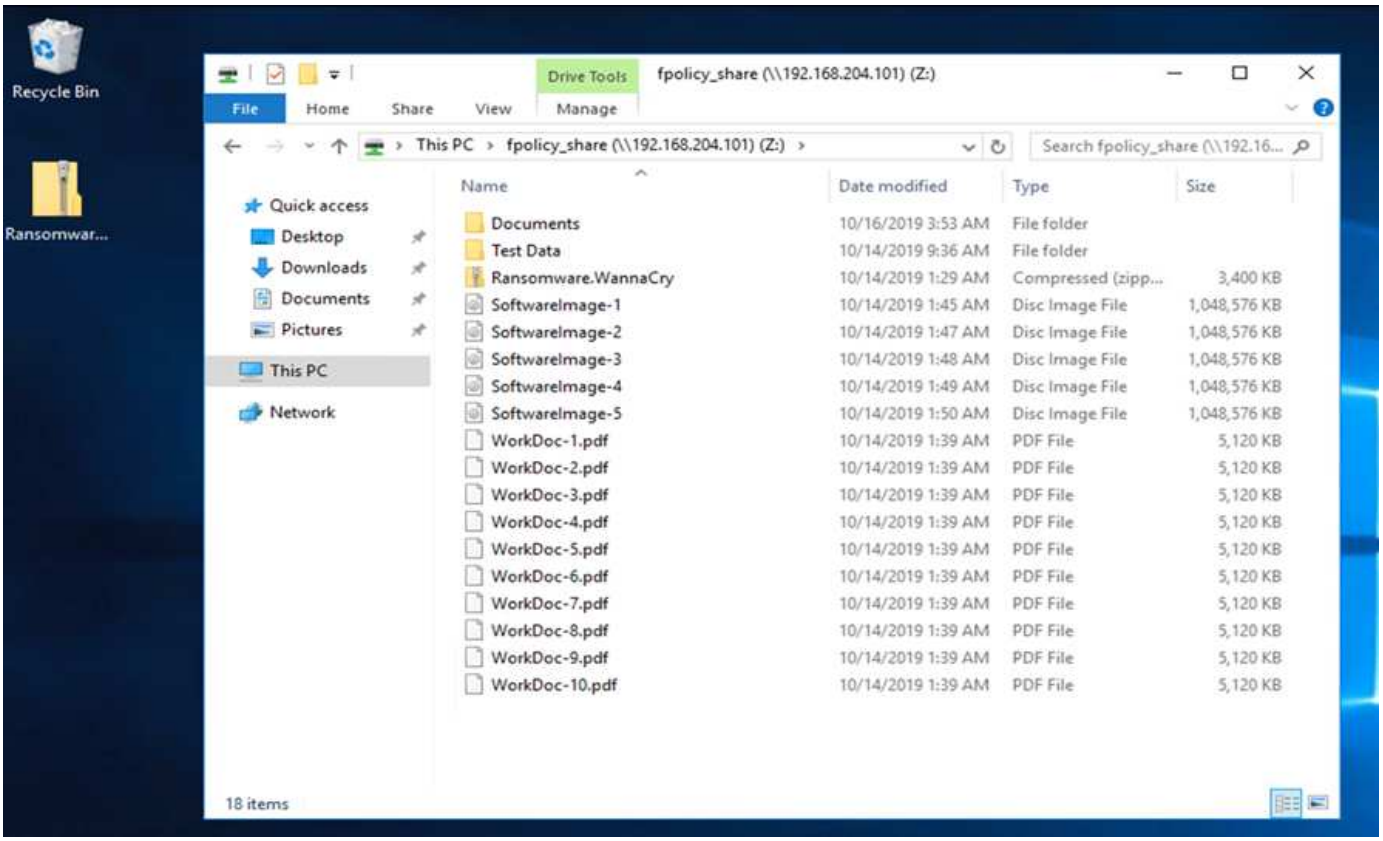
A pasta documentos da VM tinha um conjunto de arquivos PDF que ainda não foram criptografados pelo malware WannaCry.



A captura de tela a seguir mostra o compartilhamento CIFS que foi mapeado para a VM.



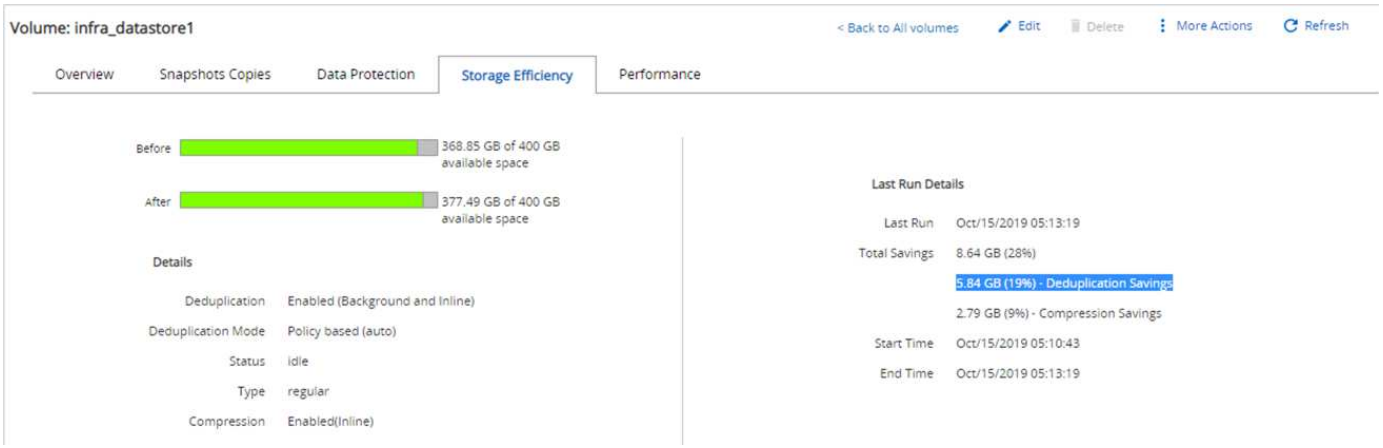
A captura de tela a seguir mostra os arquivos no compartilhamento CIFS `fpolicy_share` que ainda não foram criptografados pelo malware WannaCry.



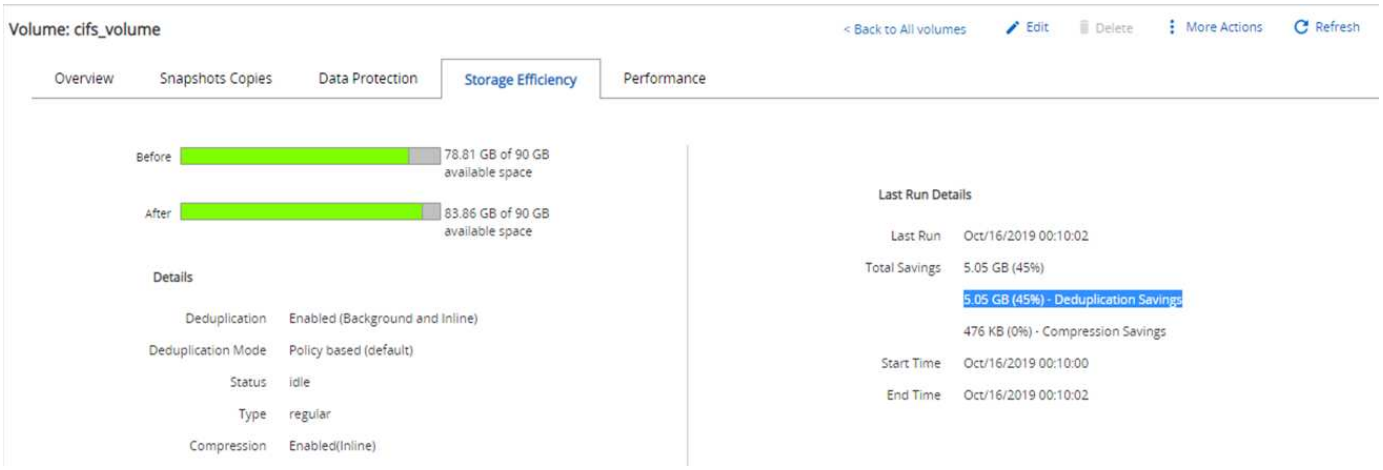
Deduplicação e informações do Snapshot antes de um ataque

Os detalhes de eficiência de storage e o tamanho da cópia Snapshot antes de um ataque são indicados e usados como referência durante a fase de detecção.

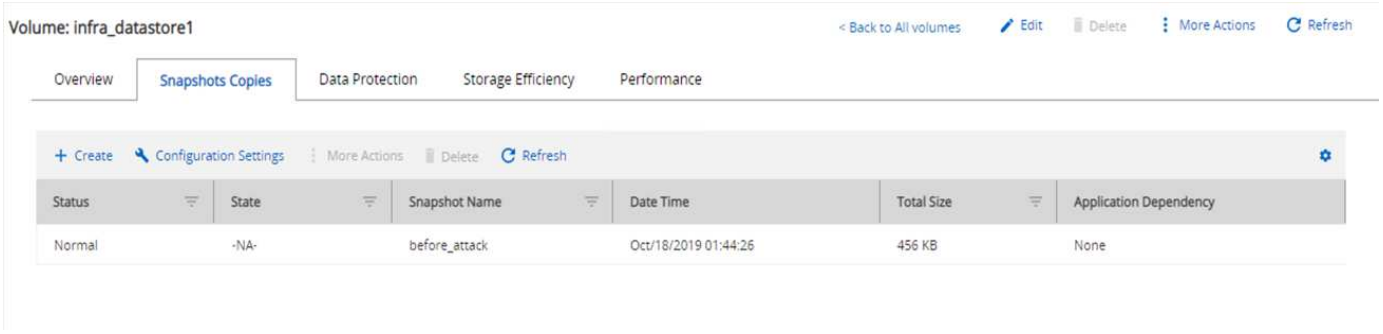
Economias de storage de 19% foram obtidas com a deduplicação no volume que hospeda a VM.



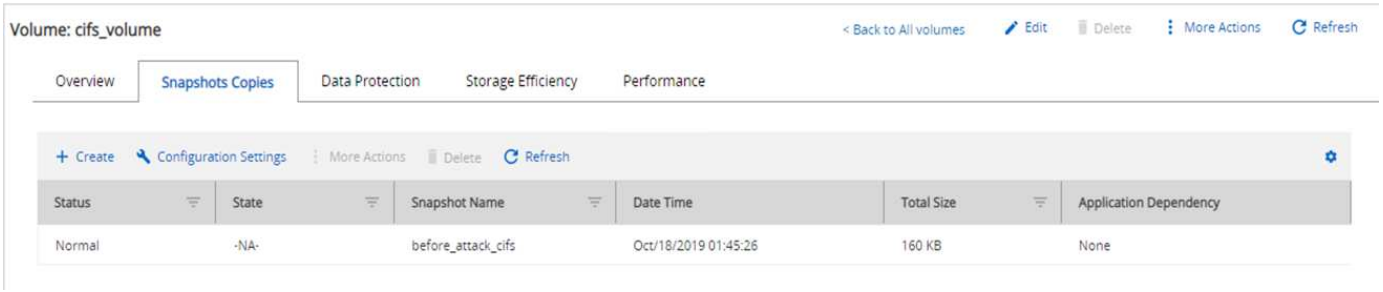
Economias de storage de 45% foram obtidas com a deduplicação no compartilhamento CIFS `fpolicy_share` .



Foi observado um tamanho de cópia Snapshot de 456KB para o volume que hospeda a VM.



Foi observado um tamanho de cópia Snapshot de 160KB para o compartilhamento CIFS `fpolicy_share` .



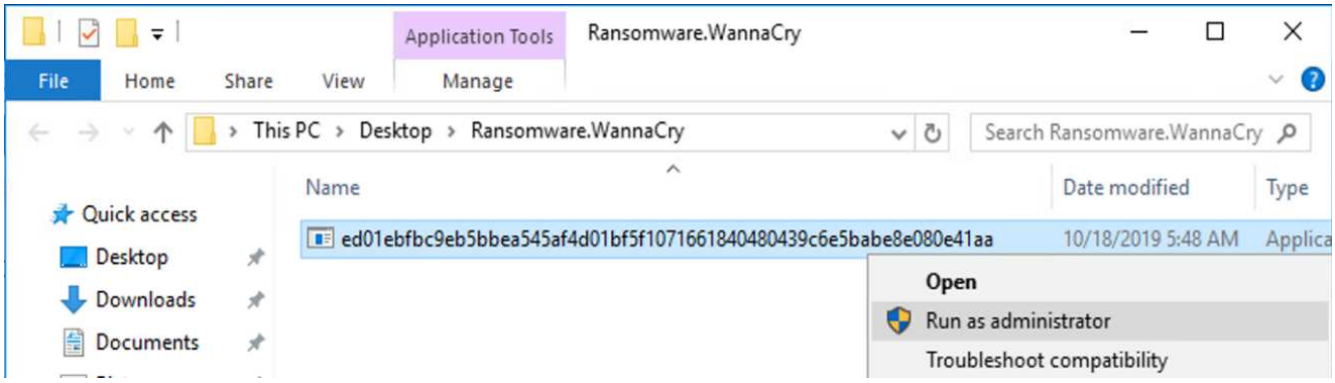
Infecção WannaCry em VM e compartilhamento CIFS

Nesta seção, mostramos como o malware WannaCry foi introduzido no ambiente FlexPod e as mudanças subsequentes no sistema que foram observadas.

As etapas a seguir demonstram como o binário do malware WannaCry foi introduzido na VM:

1. O malware protegido foi extraído.

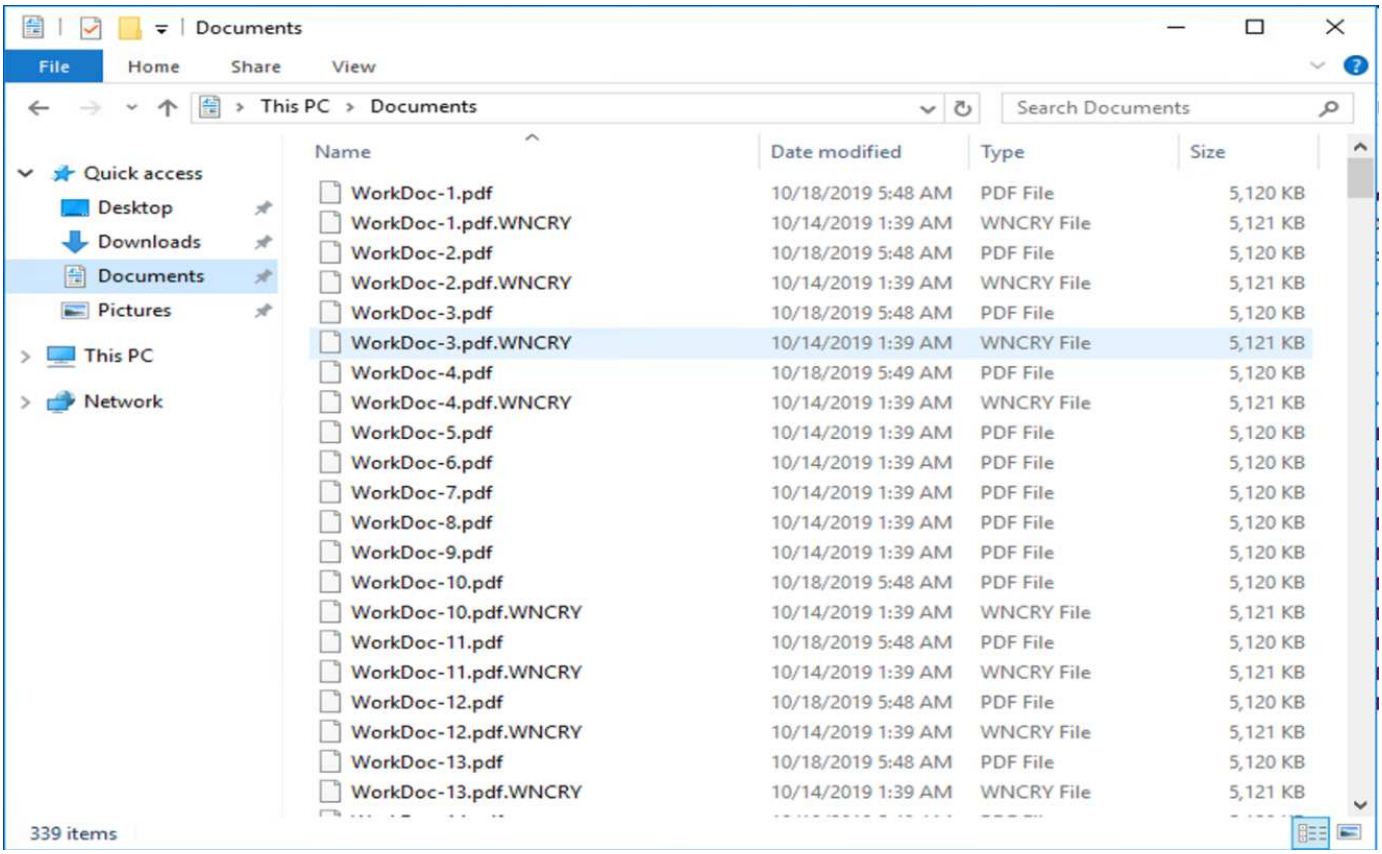
2. O binário foi executado.



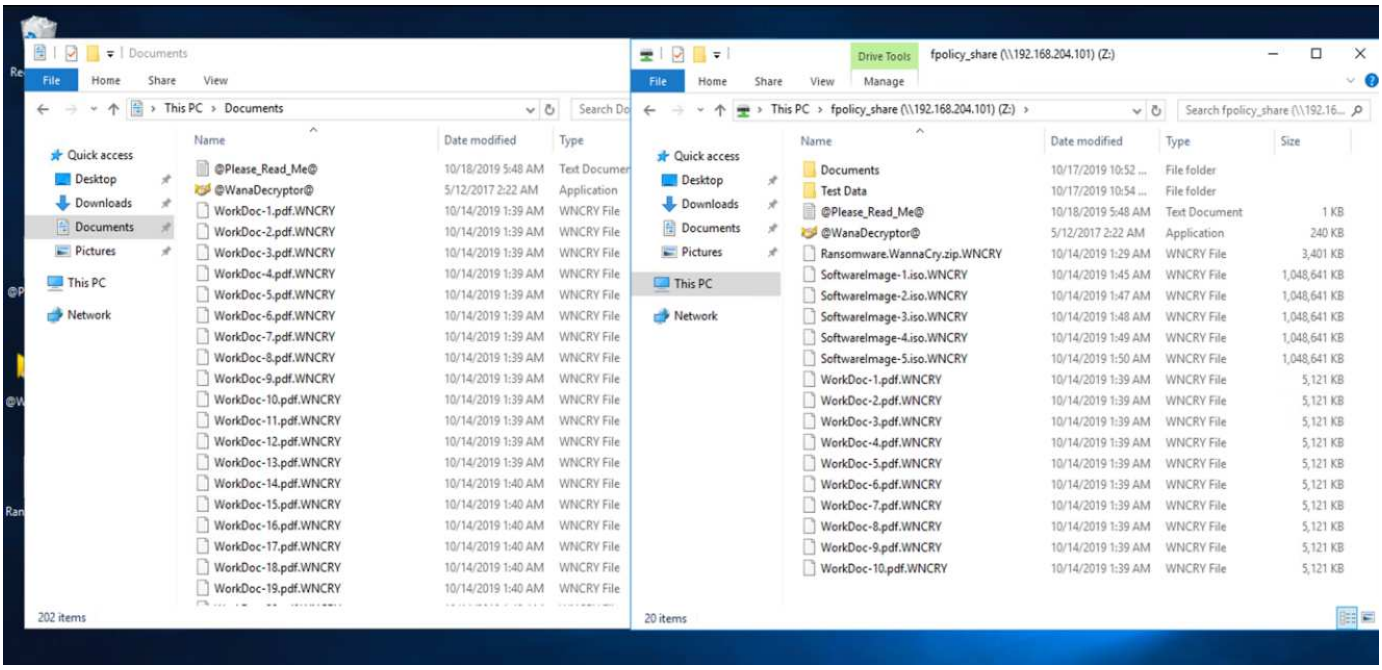
Caso 1: WannaCry criptografa o sistema de arquivos dentro da VM e mapeou o compartilhamento CIFS

O sistema de arquivos local e o compartilhamento CIFS mapeado foram criptografados pelo malware WannaCry.

O malware começa a criptografar arquivos com extensões WNCRY.



O malware criptografa todos os arquivos na VM local e o compartilhamento mapeado.

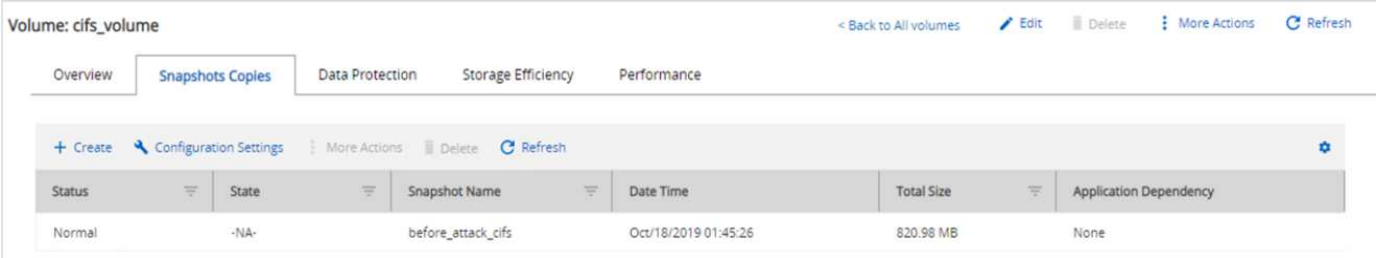


Detecção

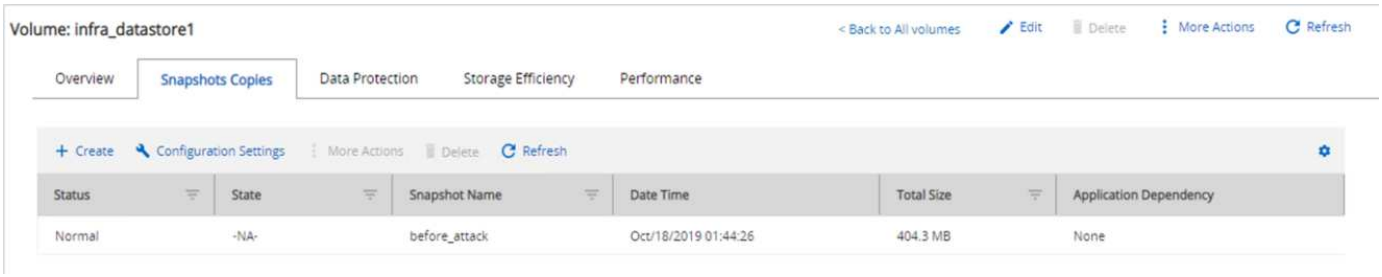
A partir do momento em que o malware começou a criptografar os arquivos, ele desencadeou um aumento exponencial no tamanho das cópias Snapshot e uma diminuição exponencial na porcentagem de eficiência de storage.

Detetamos um aumento dramático no tamanho do Snapshot para 820,98MB para o volume que hospeda o

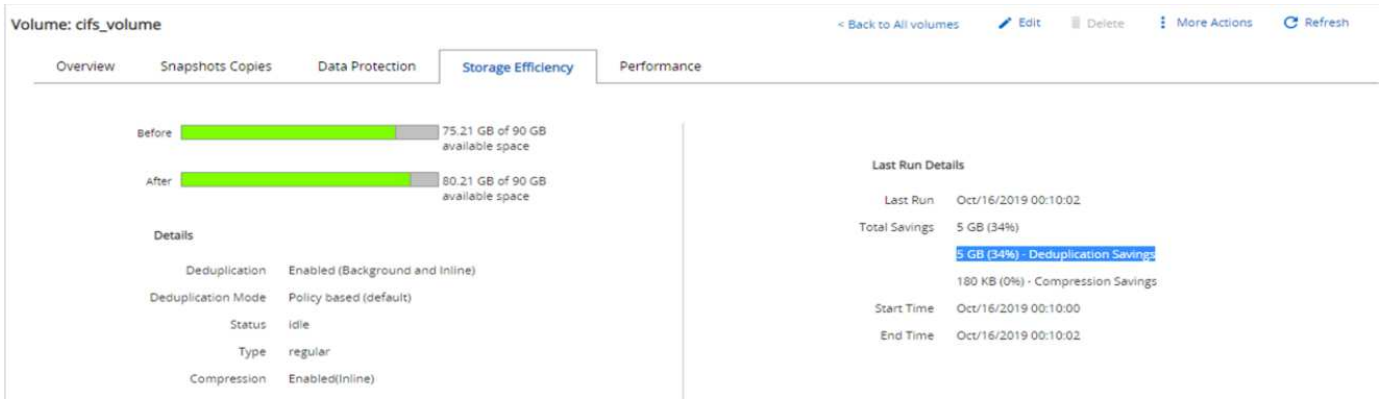
compartilhamento CIFS durante o ataque.



Detetamos um aumento no tamanho da cópia Snapshot para 404,3MB para o volume que hospeda a VM.



A eficiência de storage do volume que hospeda o compartilhamento CIFS diminuiu para 34%.



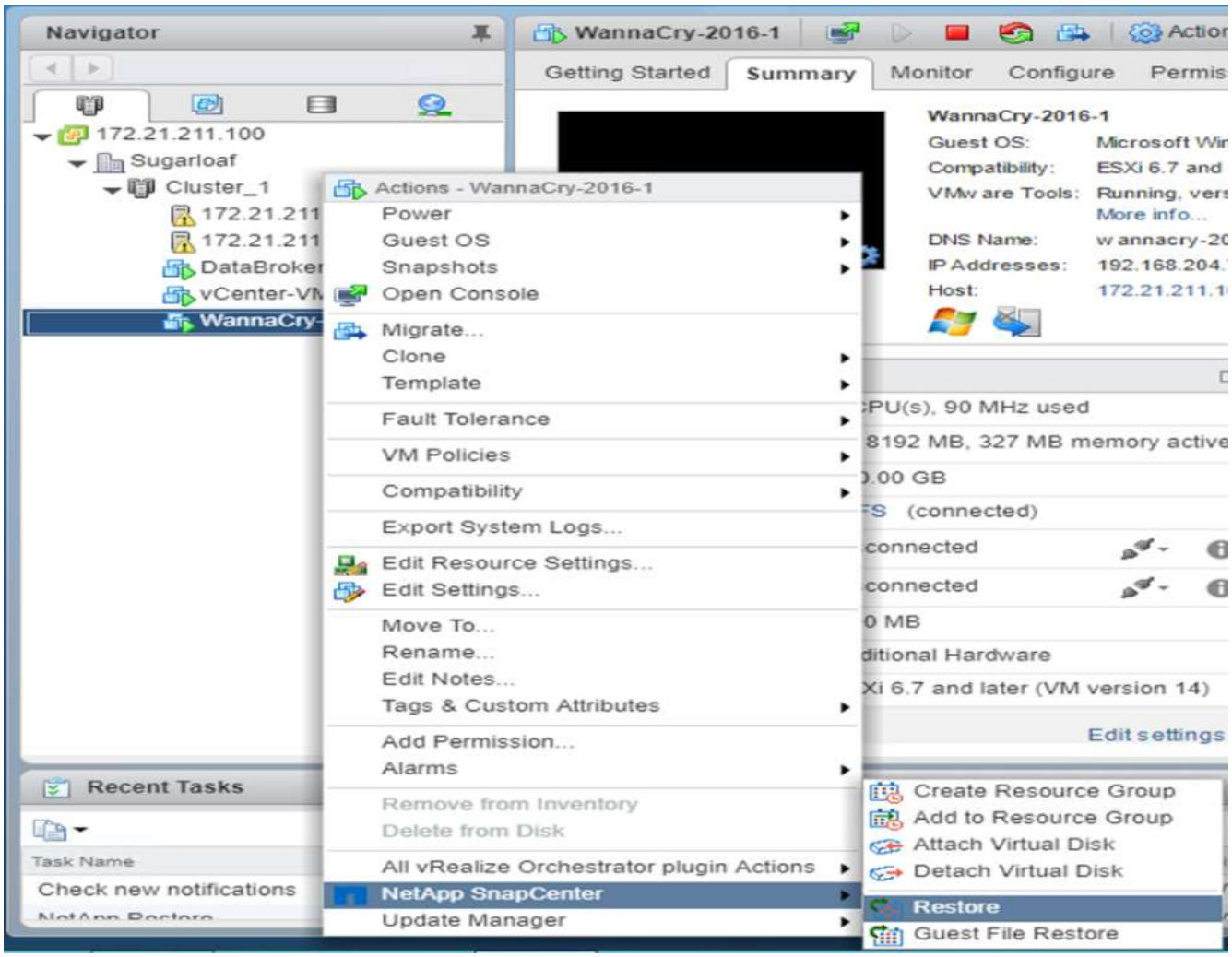
Remediação

Restaure a VM e o compartilhamento CIFS mapeado usando uma cópia Snapshot limpa criar antes do ataque.

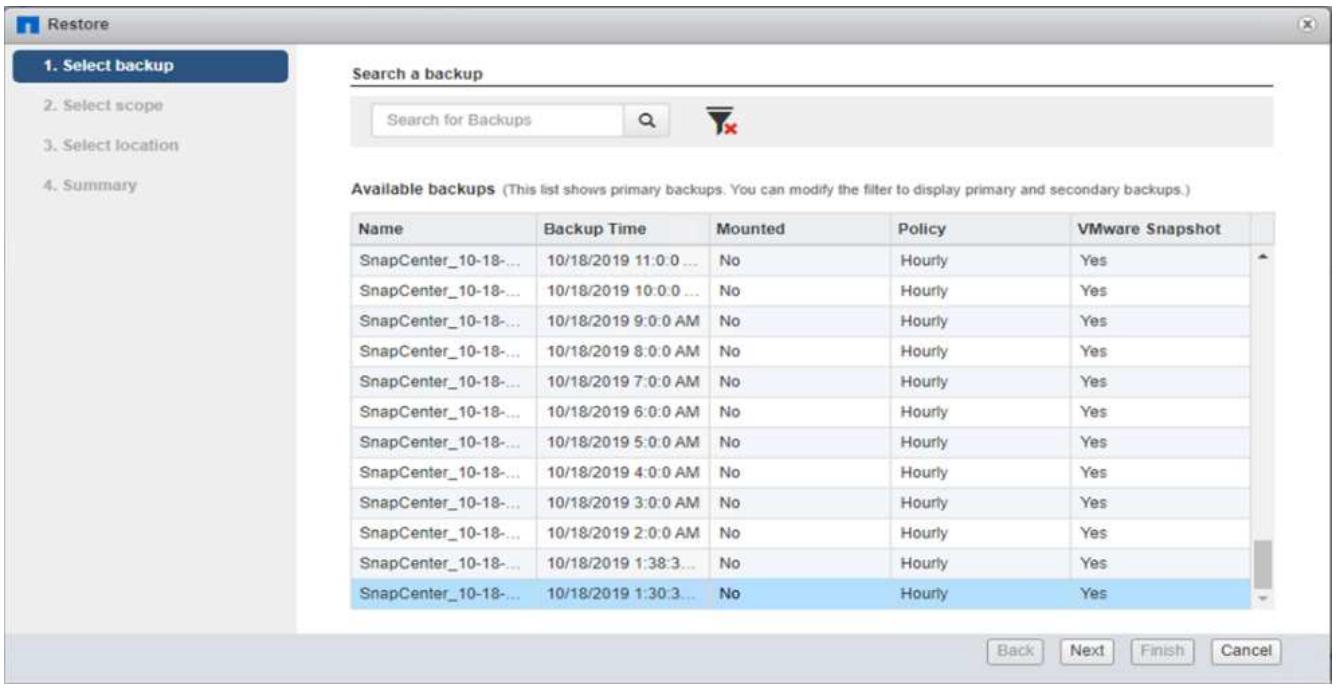
Restaurar VM

Para restaurar a VM, execute as seguintes etapas:

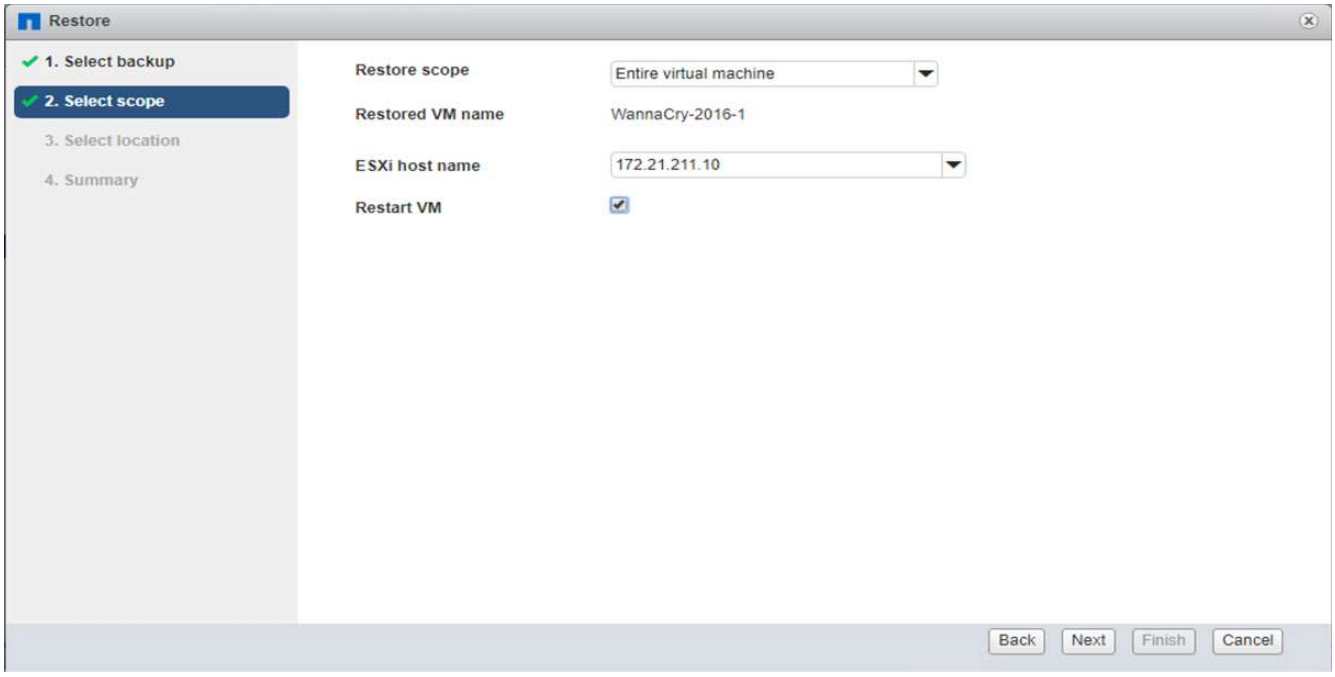
1. Use a cópia Snapshot criada com o SnapCenter para restaurar a VM.



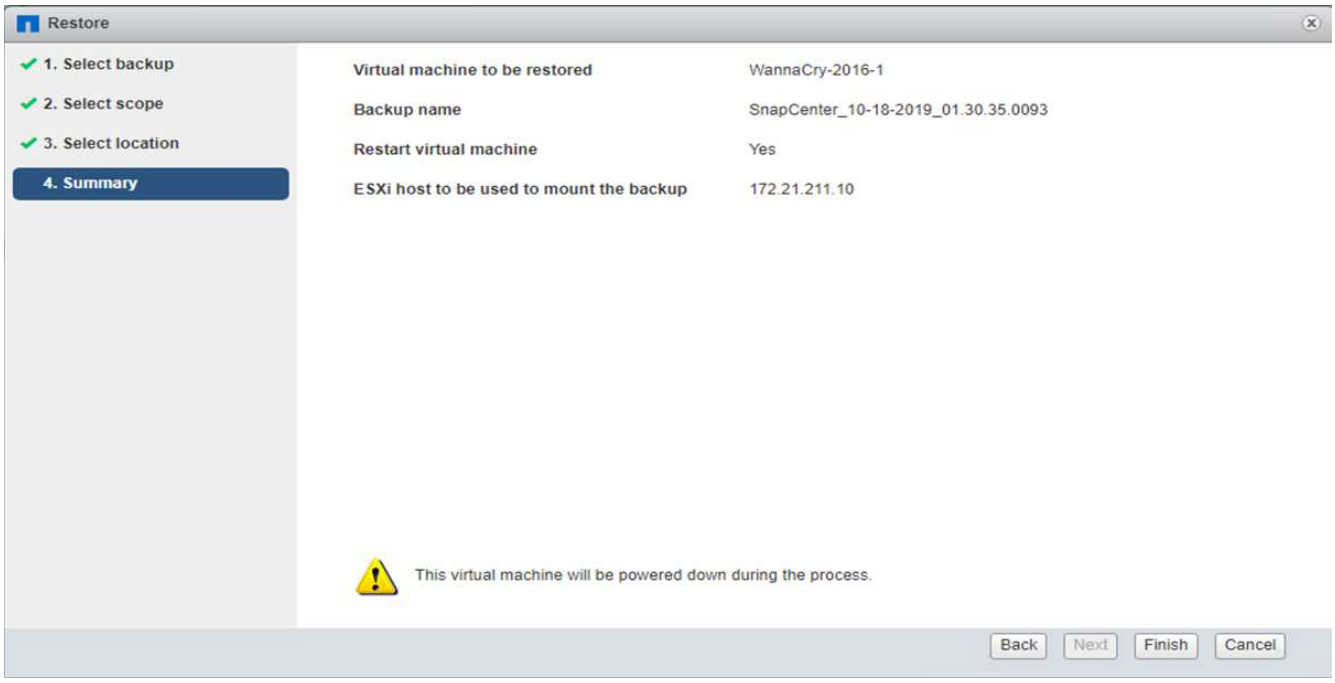
2. Selecione a cópia Snapshot consistente VMware desejada para restauração.



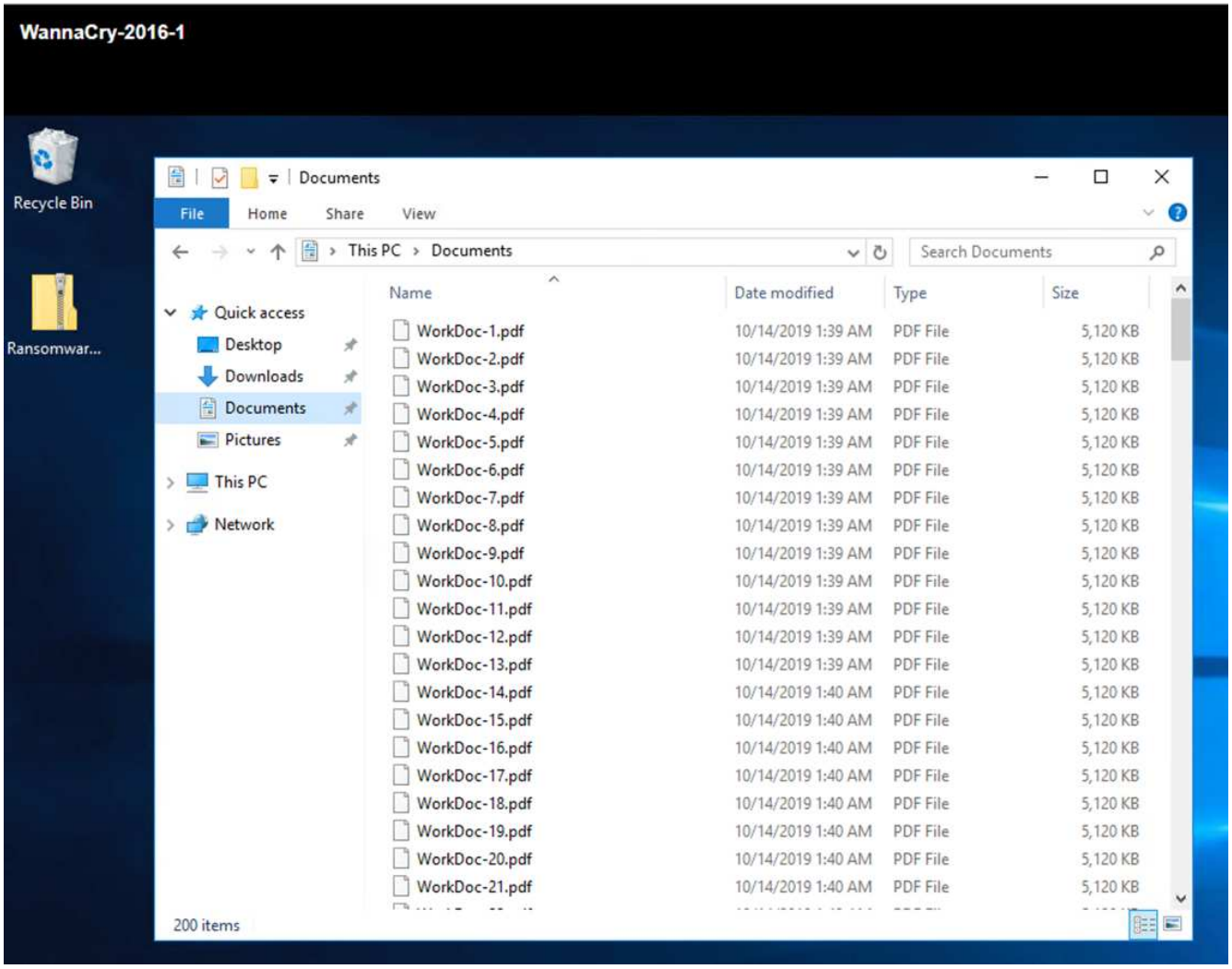
3. Toda a VM é restaurada e reiniciada.



4. Clique em concluir para iniciar o processo de restauração.



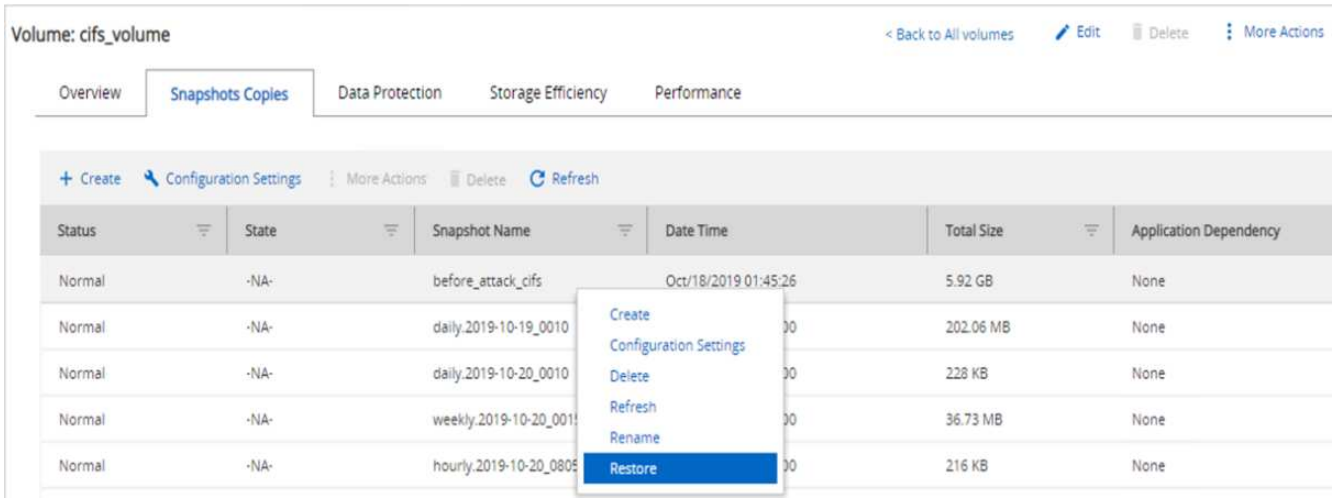
5. A VM e seus arquivos são restaurados.



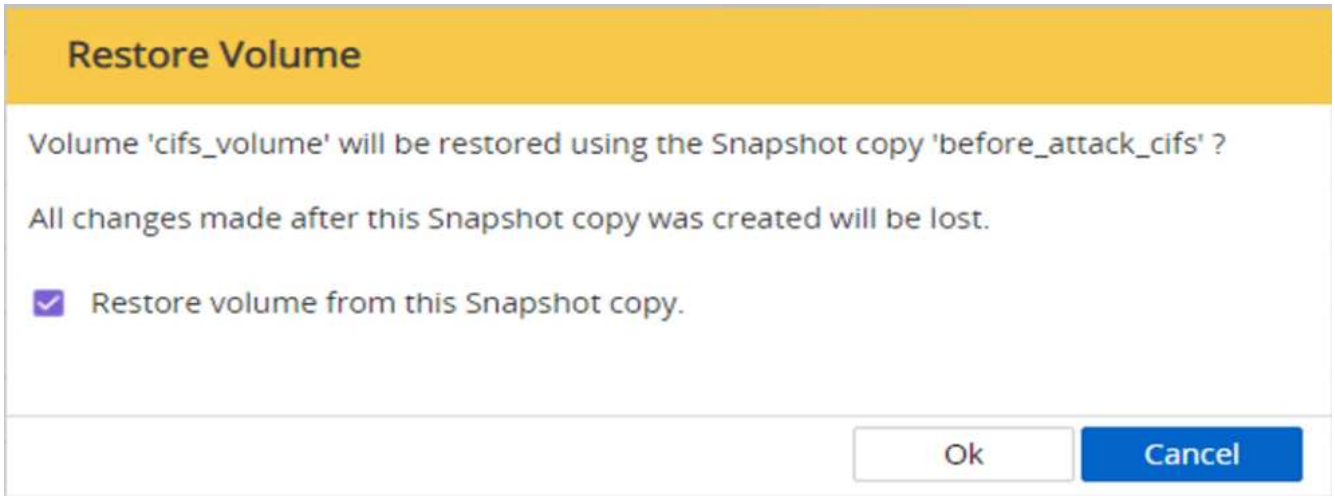
Restaurar compartilhamento CIFS

Para restaurar o compartilhamento CIFS, execute as seguintes etapas:

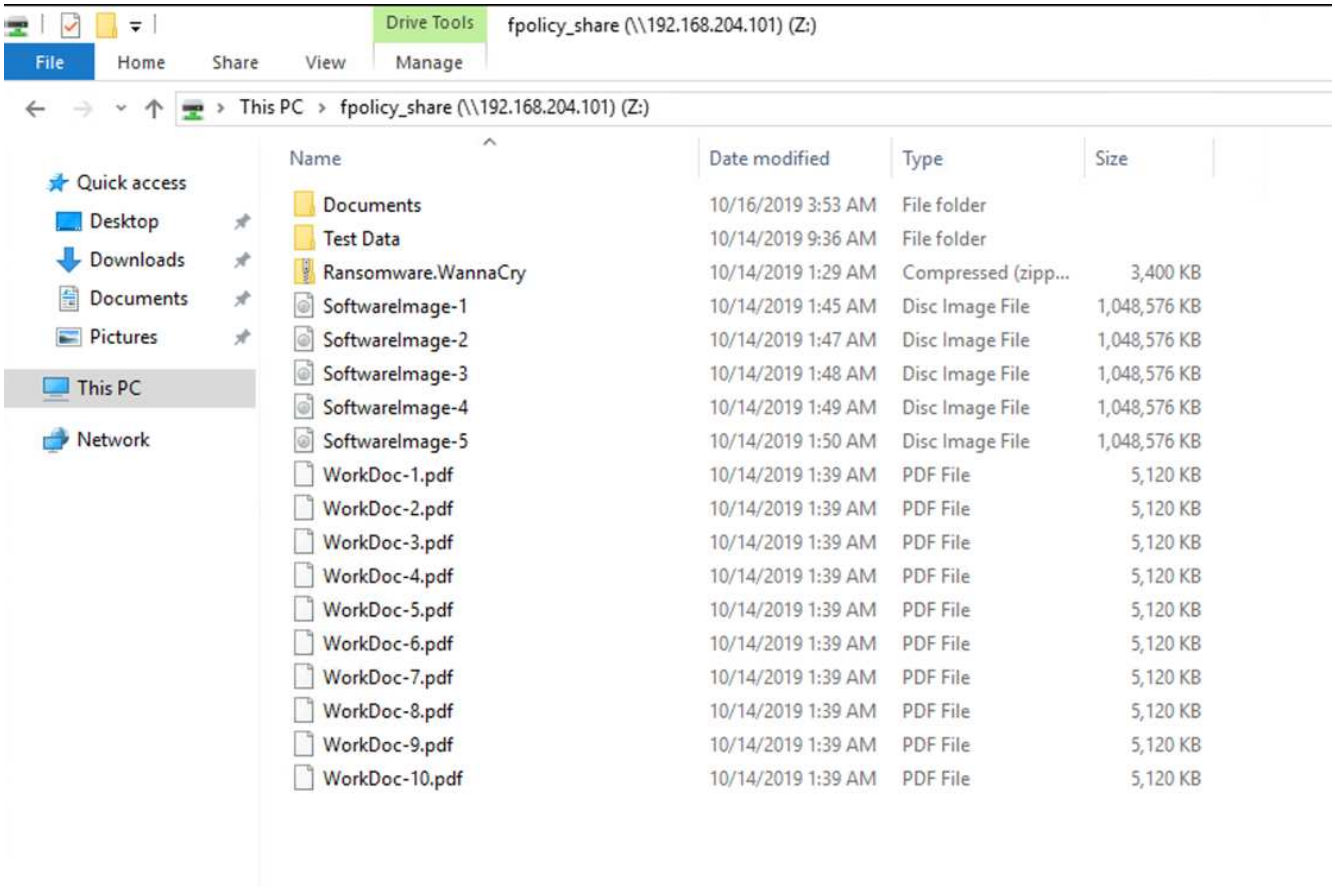
1. Use a cópia Snapshot do volume obtido antes do ataque para restaurar o compartilhamento.



2. Clique em OK para iniciar a operação de restauração.



3. Visualize o compartilhamento CIFS após a restauração.



Caso 2: O WannaCry criptografa o sistema de arquivos dentro da VM e tenta criptografar o compartilhamento CIFS mapeado que é protegido por FPolicy

Prevenção

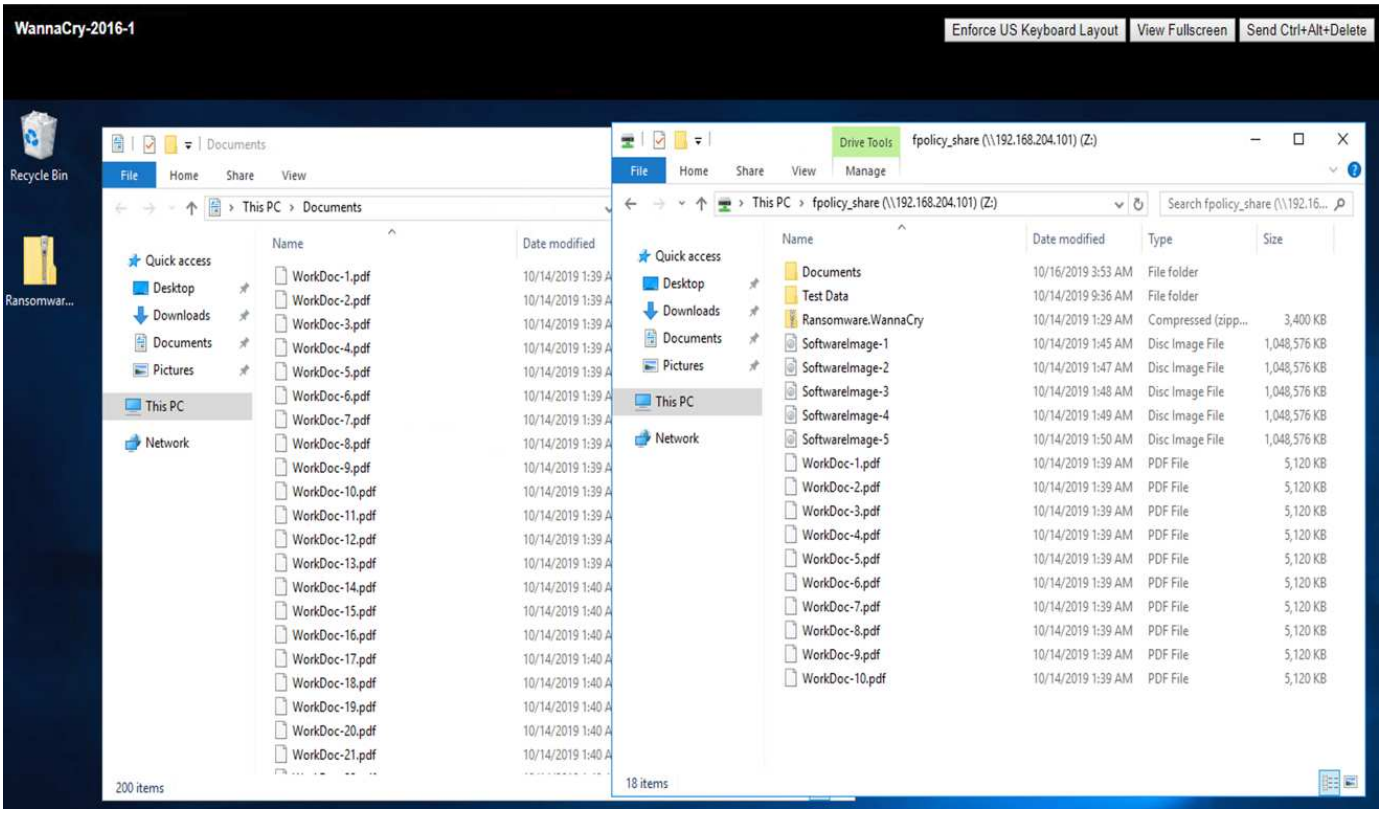
Configurar FPolicy

Para configurar o FPolicy no compartilhamento CIFS, execute os seguintes comandos no cluster ONTAP:

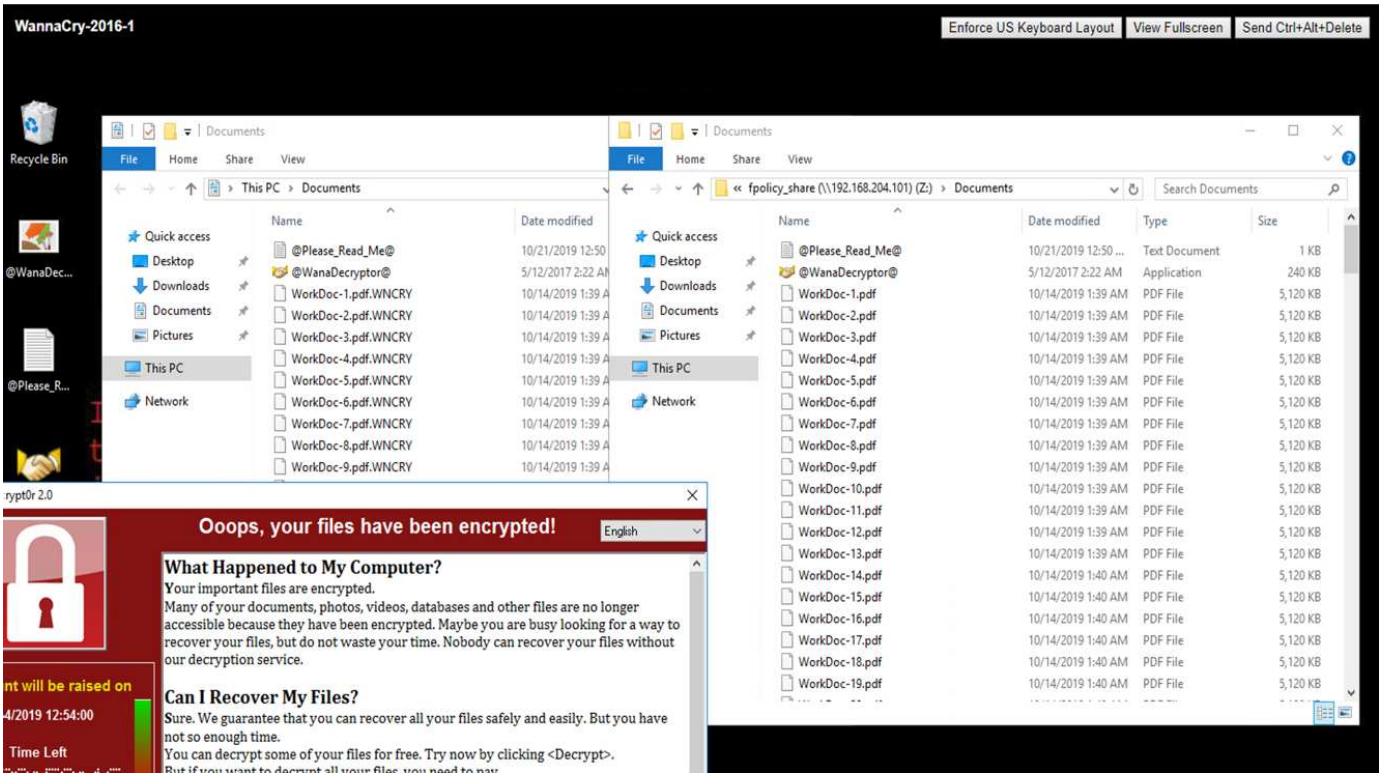
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Com essa política, arquivos com extensões WNCRY, Locky e ad4c não têm permissão para executar as operações de arquivo criar, renomear, gravar ou abrir.

Visualize o status dos arquivos antes do ataque – eles não são criptografados e em um sistema limpo.



Os arquivos na VM são criptografados. O malware WannaCry tenta criptografar os arquivos no compartilhamento CIFS, mas o FPolicy impede que ele afete os arquivos.



Continue as operações de negócios sem pagar resgate

As funcionalidades do NetApp descritas neste documento ajudam a restaurar os dados em minutos após um ataque e a prevenir ataques, antes de mais, para que você possa continuar sem obstáculos nas operações de negócios.

É possível definir o cronograma de cópia Snapshot para atender ao objetivo do ponto de restauração desejado (RPO). As operações de restauração baseadas em cópias snapshot são muito rápidas; portanto, é possível alcançar um objetivo de tempo de recuperação (rto) muito baixo.

Acima de tudo, você não precisa pagar nenhum resgate como resultado de um ataque, e você pode rapidamente voltar às operações regulares.

Conclusão

O ransomware é um produto do crime organizado, e os atacantes não operam com ética. Eles podem abster-se de fornecer a chave para descriptografia, mesmo depois de receber o resgate. A vítima não só perde seus dados, mas também uma quantidade substancial de dinheiro e enfrentará consequências associadas à perda de dados de produção.

De acordo com a "Artigo da Forbes", apenas 19% das vítimas de ransomware recuperam os dados depois de pagar o resgate. Portanto, os autores recomendam não pagar um resgate em caso de ataque, porque isso reforça a fé do invasor em seu modelo de negócios.

As operações de backup e restauração de dados desempenham um papel importante na recuperação de ransomware. Portanto, eles devem ser incluídos como parte integrante do Planejamento de negócios. A implementação dessas operações deve ser orçamentada para que não haja comprometimento das capacidades de recuperação em caso de ataque.

A chave é selecionar o parceiro de tecnologia correto nessa jornada, e a FlexPod oferece a maioria das funcionalidades necessárias de forma nativa, sem custo adicional em um sistema all-flash FAS.

Agradecimentos

O autor gostaria de agradecer às seguintes pessoas pelo seu apoio na criação deste documento:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Software Snapshot da NetApp

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- Gerenciamento de backup do SnapCenter

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- Conformidade de dados do SnapLock

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- Documentação do produto NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- Proteção avançada contra malware (AMP) da Cisco

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco Stealthwatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

Solução FlexPod compatível com segurança FIPS 140-2 para serviços de saúde

TR-4892: Solução FlexPod compatível com segurança FIPS 140-2 para cuidados de saúde

NetApp, John Mcebel, Cisco

A Health Information Technology for Economic and Clinical Health Act (HITECH) requer criptografia validada pela Federal Information Processing Standard (FIPS) 140-2 de informações eletrônicas protegidas de Saúde (ePHI). Os aplicativos e software de

tecnologia da informação em saúde (HIT) devem estar em conformidade com o FIPS 140-2 para obter a certificação Programa de promoção da interoperabilidade (anteriormente, Programa de incentivo ao uso significativo). Os fornecedores e hospitais elegíveis devem utilizar um HIT compatível com FIPS 140-2 (nível 1) para receber incentivos Medicare e Medicaid e para evitar penalidades de reembolso do Center for Medicare and Medicaid (CMS). Os algoritmos de criptografia com certificação FIPS 140-2 se qualificam como salvaguardas técnicas necessárias de acordo com a "Regra de segurança" Health Information Portability and Accountability Act (HIPAA).

O FIPS 140-2 é um padrão do governo dos EUA que define requisitos de segurança para módulos criptográficos em hardware, software e firmware que protegem informações confidenciais. A conformidade com a norma é mandatada para uso por agências governamentais dos EUA, e também é frequentemente usada em setores regulamentados como serviços financeiros e de saúde. Este relatório técnico ajuda o leitor a entender o padrão de segurança FIPS 140-2 em alto nível. Ele também ajuda o público a entender várias ameaças enfrentadas pelas organizações de saúde. Por fim, o relatório técnico ajuda a entender como um sistema FlexPod em conformidade com FIPS 140-2 pode ajudar a proteger ativos de saúde quando implantado em uma infraestrutura convergente da FlexPod.

Âmbito de aplicação

Este documento é uma visão geral técnica de um sistema de computação unificada da Cisco (Cisco UCS), Cisco Nexus, Cisco MDS e infraestrutura FlexPod baseada em NetApp ONTAP para hospedar um ou mais aplicativos ou soluções DE TI DE saúde que exigem conformidade com a segurança FIPS 140-2.

Público-alvo

Este documento destina-se a líderes técnicos do setor de saúde e a engenheiros de soluções de parceiros da Cisco e da NetApp e à equipe de serviços profissionais. O NetApp presume que o leitor entenda bem os conceitos de dimensionamento de storage e computação, além de ter familiaridade técnica com ameaças ao setor de saúde, segurança do setor de saúde, sistemas DE TI do setor de saúde, Cisco UCS e sistemas de storage NetApp.

"Próximo: Ameaças de segurança cibernética na saúde."

Ameaças de segurança cibernética na saúde

"Anterior: Introdução."

Cada problema apresenta uma nova oportunidade: Um exemplo dessa oportunidade é apresentado pela pandemia de COVID. De acordo com a "relatório" do Programa de cibersegurança do Departamento de Saúde e Serviços Humanos (HHS), a resposta à COVID resultou em um número maior de ataques de ransomware. Havia 6.000 novos domínios de internet registrados apenas na terceira semana de março de 2020. Mais de 50% dos domínios hospedaram malware. Os ataques de ransomware foram responsáveis por quase 50% de todas as violações de dados de saúde em 2020, afetando mais de 630 organizações de saúde e aproximadamente 29 milhões de Registros de saúde. Dezenove leakers/sites dobraram a extorsão. Com 24,5%, o setor de saúde registrou o maior número de violações de dados em 2020.

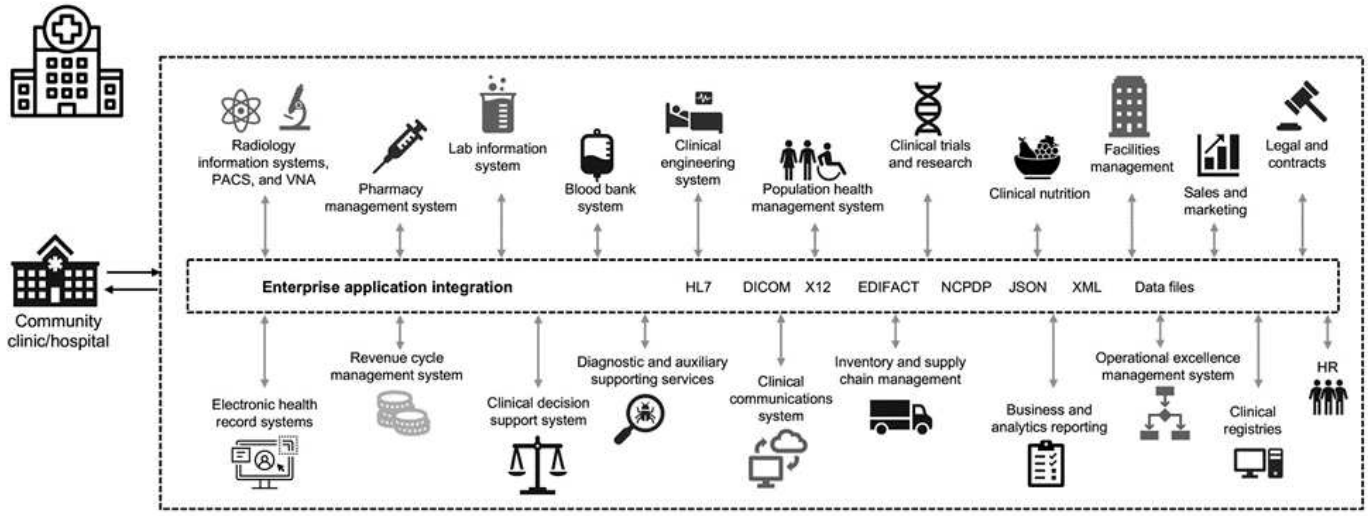
Agentes maliciosos tentaram violar a segurança e a privacidade das informações de saúde protegidas (PHI)

vendendo as informações ou ameaçando destruí-las ou expô-las. Tentativas direcionadas e de transmissão em massa são frequentemente feitas para obter acesso não autorizado ao ePHI. Aproximadamente 75% dos prontuários expostos no segundo semestre de 2020 foram devidos a colaboradores comprometidos.

A seguinte lista de organizações de saúde foi direcionada pelos agentes maliciosos:

- Sistemas hospitalares
- Laboratórios de ciências da vida
- Laboratórios de pesquisa
- Instalações de reabilitação
- Hospitais e clínicas comunitárias

A diversidade de aplicações que constituem uma organização de saúde é inegável e cada vez mais crescente em complexidade. Os escritórios de segurança da informação são desafiados a fornecer governança para a vasta gama de sistemas e ativos DE TI. A figura a seguir mostra as capacidades clínicas de um sistema hospitalar típico.



Os dados do paciente estão no centro desta imagem. A perda de dados do paciente e o estigma associado a condições médicas sensíveis são muito reais. Outras questões sensíveis incluem o risco de exclusão social, chantagem, perfil de perfil, vulnerabilidade a marketing direcionado, exploração e potencial responsabilidade financeira para com os pagadores sobre informações médicas além do Privileges do pagador.

As ameaças à saúde são multidimensionais na natureza e no impactos. Os governos em todo o mundo promulgaram várias disposições para garantir a ePHI. Os efeitos prejudiciais e a natureza evolutiva das ameaças aos cuidados de saúde dificultam a defesa de todas as ameaças pelas organizações de saúde.

Aqui está uma lista de ameaças comuns identificadas nos cuidados de saúde:

- Ataques de ransomware
- Perda ou roubo de equipamentos ou dados com informações confidenciais
- Ataques de phishing
- Ataques contra dispositivos médicos conetados que podem afetar a segurança do paciente
- Ataques de phishing por e-mail
- Perda ou roubo de equipamentos ou dados

- Comprometimento do protocolo de desktop remoto
- Vulnerabilidade de software

As organizações de saúde operam em um ambiente legal e regulatório tão complicado quanto seus ecossistemas digitais. Esse ambiente inclui, entre outros, o seguinte:

- Escritório do Coordenador Nacional (para tecnologia de Saúde) padrões de interoperabilidade de tecnologia de Informação em Saúde Eletrônica certificada pela ONC
- Medicare Access e a Lei de reautorização do Programa de seguro de Saúde Infantil (MACRA)/uso significativo
- Múltiplas obrigações sob a Food and Drug Administration (FDA)
- Processos de acreditação da Comissão Conjunta
- Requisitos da HIPAA
- Requisitos da HITECH
- Normas mínimas de risco aceitáveis para os pagadores
- Regras de privacidade e segurança do Estado
- Requisitos da Lei Federal de modernização da Segurança da Informação conforme incorporado em contratos federais e bolsas de pesquisa por meio de agências como os Institutos nacionais de Saúde
- Padrão de segurança de dados do setor de cartões de pagamento (PCI-DSS)
- Requisitos da Administração de Serviços de Saúde mental e abuso de substâncias (SAMHSA)
- A Lei Gramm-Leach-Bliley para o processamento financeiro
- A Lei Stark diz respeito à prestação de serviços a organizações afiliadas
- Lei de Direitos educacionais e Privacidade da Família (FERPA) para instituições que participam do ensino superior
- Lei de não discriminação de Informação genética (GINA)
- O novo Regulamento Geral de proteção de dados (RGPD) na União Europeia

Os padrões de arquitetura de segurança estão evoluindo rapidamente para impedir que os agentes mal-intencionados afetem os sistemas de informações de saúde. Um desses padrões é o FIPS 140-2, definido pelo National Institute of Standards and Technology (NIST). A publicação FIPS 140-2 detalha os requisitos governamentais dos EUA para um módulo criptográfico. Os requisitos de segurança abrangem áreas relacionadas com um design seguro e implementação de um módulo criptográfico e podem ser aplicados para HIT. Limites criptográficos bem definidos permitem um gerenciamento de segurança mais fácil, mantendo-se atualizado com os módulos criptográficos. Esses limites ajudam a evitar módulos cripto fracos que podem ser facilmente explorados por agentes maliciosos. Eles também podem ajudar a evitar erros humanos ao gerenciar módulos criptográficos padrão.

O NIST, juntamente com o Communications Security establishment (CSE), estabeleceu o Programa de Validação de módulos criptográficos (CMVP) para certificar módulos criptográficos para níveis de validação FIPS 140-2. Usando um módulo certificado FIPS 140-2, as organizações federais precisam proteger dados confidenciais ou valiosos enquanto em repouso e em movimento. Devido ao seu sucesso na proteção de informações confidenciais ou valiosas, muitos sistemas de saúde optaram por criptografar ePHI usando módulos criptográficos FIPS 140-2 além do nível mínimo de segurança legalmente exigido.

A utilização e a implementação das funcionalidades do FlexPod FIPS 140-2 levam apenas horas (não dias). Tornar-se compatível com FIPS está ao alcance da maioria das organizações de saúde, independentemente do tamanho. Com limites criptográficos claramente definidos e etapas de implementação simples e bem

documentadas, uma arquitetura FlexPod compatível com FIPS 140-2 pode definir uma base sólida de segurança para a infraestrutura e permitir melhorias simples para aumentar ainda mais a proteção contra ameaças à segurança.

"Próximo: Visão geral do FIPS 140-2."

Visão geral do FIPS 140-2

"Anterior: Ameaças de segurança cibernética na saúde."

"FIPS 140-2" especifica os requisitos de segurança para um módulo criptográfico usado dentro de um sistema de segurança que protege informações confidenciais em computadores e sistemas de telecomunicações. Um módulo criptográfico deve ser um conjunto de hardware, software, firmware ou uma combinação. O FIPS aplica-se aos algoritmos criptográficos, geração de chaves e gerenciadores de chaves contidos dentro de um limite criptográfico. É importante entender que o FIPS 140-2 se aplica especificamente ao módulo criptográfico, não ao produto, arquitetura, dados ou ecossistema. O módulo criptográfico, que é definido nos termos-chave mais adiante neste documento, é o componente específico (seja hardware, software e/ou firmware) que implementa funções de segurança aprovadas. Além disso, o FIPS 140-2 especifica quatro níveis. Algoritmos criptográficos aprovados são comuns a todos os níveis. Os principais elementos e requisitos de cada nível de segurança incluem:

- **Nível de segurança 1**
  - Especifica os requisitos básicos de segurança para um módulo criptográfico (pelo menos um algoritmo aprovado ou função de segurança é necessária).
  - Não são necessários mecanismos de segurança física especificados para o nível 1 além dos requisitos básicos para componentes de nível de produção.
- **Nível de segurança 2**
  - Melhora os mecanismos de segurança física adicionando a exigência de inviolabilidade usando soluções invioláveis, como revestimentos ou vedações, fechaduras em tampas removíveis ou portas dos módulos criptográficos.
  - Requer, no mínimo, controle de acesso baseado em função (RBAC) no qual o módulo criptográfico autentica a autorização de um operador ou administrador para assumir uma função específica e executar um conjunto de funções correspondente.
- **Nível de segurança 3**
  - Baseia-se nos requisitos invioláveis do nível 2 e tenta impedir o acesso adicional a parâmetros críticos de segurança (CSPs) dentro do módulo criptográfico.
  - Os mecanismos de segurança física necessários no nível 3 destinam-se a ter uma alta probabilidade de detetar e responder a tentativas de acesso físico, ou qualquer uso ou modificação do módulo criptográfico. Os exemplos podem incluir gabinetes fortes, deteção de adulteração e circuitos de resposta que zera todos os CSPs de texto simples quando uma tampa removível no módulo criptográfico é aberta.
  - Requer mecanismos de autenticação baseados em identidade para aprimorar a segurança dos mecanismos RBAC especificados no nível 2. Um módulo criptográfico autentica a identidade de um operador e verifica se o operador está autorizado a usar uma função e executar as funções da função.
- **Nível de segurança 4**

- O mais alto nível de segurança no FIPS 140-2.
- O nível mais útil para operações em ambientes fisicamente desprotegidos.
- Neste nível, os mecanismos de segurança física destinam-se a fornecer proteção completa em torno do módulo criptográfico com a responsabilidade de detetar e responder a quaisquer tentativas não autorizadas de acesso físico.
- A penetração ou a exposição do módulo criptográfico deve ter uma alta probabilidade de deteção e resultar na zeroização imediata de todos os CSPs não seguros ou em texto simples.

"Próximo: Plano de controle versus plano de dados."

Plano de controle versus plano de dados

"Anterior: Visão geral do FIPS 140-2."

Ao implementar uma estratégia FIPS 140-2, é importante entender o que está sendo protegido. Isso pode ser facilmente dividido em duas áreas: Plano de controle e plano de dados. Um plano de controle refere-se aos aspetos que afetam o controle e a operação dos componentes dentro do sistema FlexPod: Por exemplo, acesso administrativo aos controladores de storage NetApp, switches Cisco Nexus e servidores Cisco UCS. A proteção nesta camada é fornecida limitando os protocolos e cifras criptográficas que os administradores podem usar para se conetar a dispositivos e fazer alterações. Um plano de dados refere-se às informações reais, como a PHI, no sistema FlexPod. Isso é protegido criptografando dados em repouso e novamente para FIPS, garantindo que os módulos criptográficos em uso atendam aos padrões.

"Próximo: Computação do FlexPod Cisco UCS e FIPS 140-2."

Computação do FlexPod Cisco UCS e FIPS 140-2-2

"Anterior: Plano de controle versus plano de dados."

Uma arquitetura FlexPod pode ser projetada com um servidor Cisco UCS compatível com FIPS 140-2-2. De acordo com o NIST dos EUA, o servidor Cisco UCS pode operar no modo de conformidade FIPS 140-2 nível 1. Para obter uma lista completa de componentes Cisco compatíveis com FIPS, "Página FIPS 140 da Cisco" consulte . O Cisco UCS Manager está validado para FIPS 140-2.

Cisco UCS e interconexão de malha

O Cisco UCS Manager é implantado e executado a partir das interconexões de malha (FIs) do Cisco.

Para obter mais informações sobre o Cisco UCS e como ativar o FIPS, consulte "Documentação do Cisco UCS Manager".

Para ativar o modo FIPS na interconexão de malha do Cisco em cada malha A e B, execute os seguintes comandos:

```
fp-health-fabric-A# connect local-mgmt
fp-health-fabric-A(local-mgmt)# enable fips-mode
FIPS mode is enabled
```

Para substituir um FI em um cluster no Gerenciador de UCS do Cisco versão 3,2(3) por um FI em uma versão anterior ao Cisco UCS versão 3,2(3), desative o modo FIPS (desative `fips-mode`) no FI existente antes de adicionar o FI de substituição ao cluster. Após a formação do cluster, como parte da inicialização do Cisco UCS Manager, o modo FIPS é ativado automaticamente.

A Cisco oferece os seguintes produtos-chave que podem ser implementados na camada de computação ou aplicação:

- **Proteção avançada contra malware (AMP) da Cisco para endpoints.** Suportada em sistemas operativos Microsoft Windows e Linux, esta solução integra capacidades de prevenção, deteção e resposta. Este software de segurança impede violações, bloqueia malware no ponto de entrada e monitora e analisa continuamente as atividades de arquivo e processo para detetar, conter e corrigir rapidamente ameaças que podem evitar defesas de linha de frente. O componente proteção contra atividades maliciosas (MAP) do AMP monitora continuamente todas as atividades de endpoint e fornece deteção em tempo de execução e bloqueio de comportamento anormal de um programa em execução no endpoint. Por exemplo, quando o comportamento do endpoint indica ransomware, os processos ofensivos são encerrados, impedindo a criptografia do endpoint e interrompendo o ataque.
- * AMP para segurança de e-mail.* Os e-mails se tornaram o principal veículo para espalhar malware e realizar ataques cibernéticos. Em média, cerca de 100 bilhões de e-mails são trocados em um único dia, o que fornece aos invasores um excelente vetor de penetração nos sistemas do usuário. Portanto, é absolutamente essencial defender-se contra esta linha de ataque. AMP analisa e-mails para ameaças como explorações de dia zero e malware furtivo escondido em anexos maliciosos. Ele também usa inteligência de URL líder do setor para combater links maliciosos. Ele oferece aos usuários proteção avançada contra spear phishing, ransomware e outros ataques sofisticados.
- **Sistema de prevenção de intrusão de próxima geração (NGIPS).** O Cisco Firepower NGIPS pode ser implantado como um dispositivo físico no data center ou como um dispositivo virtual no VMware (NGIPSv for VMware). Este sistema de prevenção de intrusão altamente eficaz proporciona um desempenho fiável e um baixo custo total de propriedade. A proteção contra ameaças pode ser expandida com licenças de assinatura opcionais para fornecer AMP, visibilidade e controle de aplicativos e recursos de filtragem de URL. O NGIPS virtualizado inspeciona o tráfego entre máquinas virtuais (VMs) e facilita a implantação e o gerenciamento de soluções NGIPS em locais com recursos limitados, aumentando a proteção para ativos físicos e virtuais.

"Próximo: Rede FlexPod Cisco e FIPS 140-2."

Rede FlexPod Cisco e FIPS 140-2-2

"Anterior: Computação do FlexPod Cisco UCS e FIPS 140-2."

MDS do Cisco

A plataforma da série Cisco MDS 9000 com o software 8,4.x é "Compatível com FIPS 140-2". O Cisco MDS implementa módulos criptográficos e os seguintes serviços para SNMPv3 e SSH.

- Estabelecimento de sessão que apoia cada serviço

- Todos os algoritmos criptográficos subjacentes que suportam cada função de derivação de chave de serviços
- Hashing para cada serviço
- Criptografia simétrica para cada serviço

Antes de ativar o modo FIPS, execute as seguintes tarefas no comutador MDS:

1. Faça suas senhas com um mínimo de oito carateres.
2. Desativar o Telnet. Os usuários devem fazer login usando apenas SSH.
3. Desative a autenticação remota através do RADIUS/TACACS. Apenas os utilizadores locais da central podem ser autenticados.
4. Desative o SNMP v1 e v2. Todas as contas de usuário existentes no switch que foram configuradas para SNMPv3 devem ser configuradas somente com SHA para autenticação e AES/3DES para privacidade.
5. Desativar VRRP.
6. Exclua todas as políticas IKE que tenham MD5 para autenticação ou DES para criptografia. Modifique as políticas para que elas usem SHA para autenticação e 3DES/AES para criptografia.
7. Excluir todos os pares de chaves SSH Server RSA1.

Para ativar o modo FIPS e exibir o status FIPS no comutador MDS, execute as seguintes etapas:

1. Mostrar o status FIPS.

```
MDSSwitch# show fips status
FIPS mode is disabled
MDSSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Configure a chave SSH de 2048 bits.

```
MDSSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
MDSSwitch(config)# no ssh key
MDSSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
MDSSwitch(config)# ssh key
dsa   rsa
MDSSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Ative o modo FIPS.

```
MDSSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
```

4. Mostrar o status FIPS.

```
MDSSwitch(config)# show fips status
FIPS mode is enabled
MDSSwitch(config)# feature ssh
MDSSwitch(config)# show feature | grep ssh
sshServer            1        enabled
```

5. Salve a configuração na configuração em execução.

```
MDSSwitch(config)# copy ru st
[##################################################] 100%
exitCopy complete.
MDSSwitch(config)# exit
```

6. Reinicie o MDS switch

```
MDSSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

7. Mostrar o status FIPS.

```
Switch(config)# fips mode enable
Switch(config)# show fips status
```

Para obter mais informações, "Ativar o modo FIPS"consulte .

Cisco Nexus

Os switches da série Cisco Nexus 9000 (versão 9,3) são "Compatível com FIPS 140-2". O Cisco implementa módulos criptográficos e os seguintes serviços para SNMPv3 e SSH.

- Estabelecimento de sessão que apoia cada serviço
- Todos os algoritmos criptográficos subjacentes que suportam cada função de derivação de chave de serviços
- Hashing para cada serviço
- Criptografia simétrica para cada serviço

Antes de ativar o modo FIPS, execute as seguintes tarefas no switch Cisco Nexus:

1. Desativar o Telnet. Os usuários devem fazer login usando o Secure Shell (SSH) somente.
2. Desativar SNMPv1 e v2. Todas as contas de usuário existentes no dispositivo que foram configuradas para SNMPv3 devem ser configuradas somente com SHA para autenticação e AES/3DES para privacidade.
3. Exclua todos os pares de chaves do servidor SSH RSA1.
4. Ative a verificação de integridade de mensagens (MIC) HMAC-SHA1 para usar durante a negociação do protocolo de associação de segurança (SAP) do Cisco TrustSec. Para fazer isso, digite o comando sap hash-algorithm `HMAC-SHA-1` no `cts-manual` modo ou `cts-dot1x`.

Para ativar o modo FIPS no switch Nexus, execute as seguintes etapas:

1. Configure a chave SSH de 2048 bits.

```
NexusSwitch# show fips status
FIPS mode is disabled
NexusSwitch# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

2. Configure a chave SSH de 2048 bits.

```
NexusSwitch(config)# no feature ssh
XML interface to system may become unavailable since ssh is disabled
NexusSwitch(config)# no ssh key
NexusSwitch(config)# show ssh key
**************************************
could not retrieve rsa key information
bitcount: 0
**************************************
could not retrieve dsa key information
bitcount: 0
**************************************
no ssh keys present. you will have to generate them
**************************************
NexusSwitch(config)# ssh key
dsa   rsa
NexusSwitch(config)# ssh key rsa 2048 force
generating rsa key(2048 bits).....
...
generated rsa key
```

3. Ative o modo FIPS.

```
NexusSwitch(config)# fips mode enable
FIPS mode is enabled
System reboot is required after saving the configuration for the system
to be in FIPS mode
Warning: As per NIST requirements in 6.X, the minimum RSA Key Size has
to be 2048
Show fips status
NexusSwitch(config)# show fips status
FIPS mode is enabled
NexusSwitch(config)# feature ssh
NexusSwitch(config)# show feature | grep ssh
sshServer            1        enabled
Save configuration to the running configuration
NexusSwitch(config)# copy ru st
[########################################] 100%
exitCopy complete.
NexusSwitch(config)# exit
```

4. Reinicie o switch Nexus.

```
NexusSwitch# reload
This command will reboot the system. (y/n)?  [n] y
```

5. Mostrar o status FIPS.

```
NexusSwitch(config)# fips mode enable
NexusSwitch(config)# show fips status
```

Além disso, o software Cisco NX os suporta o recurso NetFlow que permite a deteção aprimorada de anomalias e segurança da rede. O NetFlow captura os metadados de cada conversa na rede, as partes envolvidas na comunicação, o protocolo que está sendo usado e a duração da transação. Depois que as informações são agregadas e analisadas, elas podem fornecer informações sobre o comportamento normal. Os dados coletados também permitem a identificação de padrões questionáveis de atividade, como malware que se espalha pela rede, o que pode passar despercebido. O NetFlow usa fluxos para fornecer estatísticas para monitoramento de rede. Um fluxo é um fluxo unidirecional de pacotes que chega em uma interface de origem (ou VLAN) e tem os mesmos valores para as chaves. Uma chave é um valor identificado para um campo dentro do pacote. Você cria um fluxo usando um Registro de fluxo para definir as chaves exclusivas para o seu fluxo. Você pode exportar os dados que o NetFlow coleta para seus fluxos usando um exportador de fluxo para um coletor NetFlow remoto, como o Cisco Stealthwatch. O Stealthwatch usa essas informações para monitoramento contínuo da rede e fornece deteção de ameaças em tempo real e respostas forenses a incidentes se ocorrer um surto de ransomware.

"Próximo: Storage FlexPod NetApp ONTAP e FIPS 140-2."

Storage FlexPod NetApp ONTAP e FIPS 140-2-2

"Anterior: Rede FlexPod Cisco e FIPS 140-2."

O NetApp oferece uma variedade de hardware, software e serviços, que podem incluir vários componentes dos módulos criptográficos validados sob o padrão. Portanto, o NetApp usa várias abordagens para conformidade com o FIPS 140-2 para o plano de controle e o plano de dados:

- O NetApp inclui módulos criptográficos que alcançaram a validação de nível 1 para criptografia de dados em trânsito e dados em repouso.
- A NetApp adquire módulos de hardware e software que foram validados pelo FIPS 140-2 pelos fornecedores desses componentes. Por exemplo, a solução de criptografia de storage da NetApp aproveita as unidades validadas FIPS de nível 2.
- Os produtos NetApp podem usar um módulo validado de uma forma que esteja em conformidade com a norma, mesmo que o produto ou recurso não esteja dentro do limite da validação. Por exemplo, o NetApp volume Encryption (NVE) está em conformidade com FIPS 140-2-2. Embora não seja validado separadamente, ele utiliza o módulo criptográfico NetApp, que é validado de nível 1. Para entender as especificações de conformidade da sua versão do ONTAP, entre em Contato com seu SME da FlexPod.

Os módulos criptográficos NetApp são validados pelo FIPS 140-2 nível 1

- O módulo de Segurança criptográfica (NCSM) da NetApp é validado para FIPS 140-2 nível 1.

As unidades com autocriptografia da NetApp têm validação FIPS 140-2 nível 2

A NetApp compra unidades com autocriptografia (SEDs) que foram 140-2 validadas pelo fabricante do equipamento original (OEM). Os clientes que buscam essas unidades precisam especificá-las ao fazer pedidos. As unidades são validadas no nível 2. Os seguintes produtos da NetApp podem utilizar SEDs validados:

- Sistemas de storage AFF A-Series e FAS
- Sistemas de storage e-Series e EF-Series

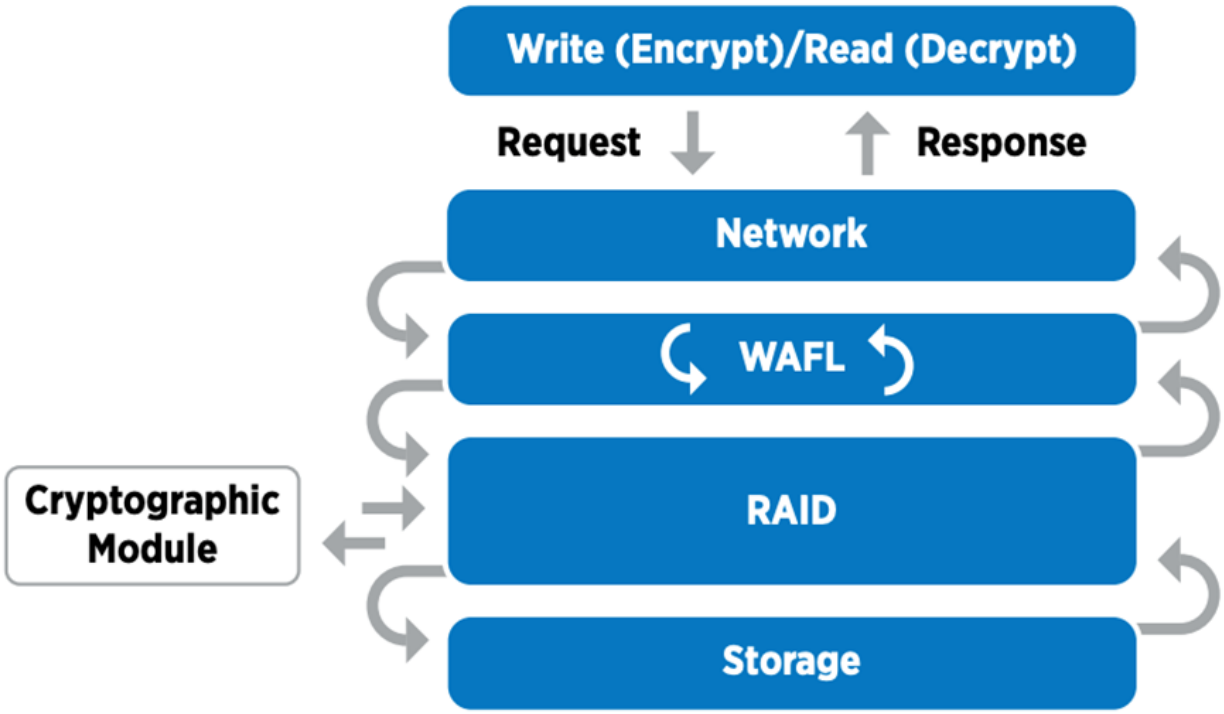
Criptografia agregada NetApp e criptografia de volume NetApp

As tecnologias NVE e NetApp Aggregate Encryption (NAE) permitem a criptografia de dados no volume e no nível agregado, respetivamente, tornando a solução agnóstica quanto à unidade física.

O NVE é uma solução de criptografia de dados em repouso baseada em software, disponível a partir do ONTAP 9.1, compatível com FIPS 140-2-2 desde o ONTAP 9.2. O NVE permite que o ONTAP criptografe dados em cada volume para obter granularidade. O NAE, disponível com o ONTAP 9.6, é uma consequência da NVE. Ele permite que o ONTAP criptografe dados para cada volume, e os volumes podem compartilhar chaves no agregado. Tanto o NVE quanto o NAE usam criptografia AES de 256 bits. Os dados também podem ser armazenados no disco sem SEDs. O NVE e o NAE permitem que você use recursos de eficiência de storage mesmo quando a criptografia está ativada. Uma criptografia somente de camada de aplicação derrota todos os benefícios da eficiência de storage. Com o NVE e o NAE, as eficiências de storage são mantidas porque os dados entram da rede por meio do NetApp WAFL à camada RAID, que determina se os dados devem ser criptografados. Para maior eficiência de storage, você pode usar a deduplicação agregada com NAE. Os volumes NVE e os volumes NAE podem coexistir no mesmo agregado NAE. Os agregados NAE não suportam volumes não criptografados.

Veja como o processo funciona: Quando os dados são criptografados, eles são enviados para o módulo

criptográfico que é validado pelo FIPS 140-2 nível 1. O módulo criptográfico criptografa os dados e os envia de volta para a camada RAID. Os dados criptografados são então enviados para o disco. Portanto, com a combinação de NVE e NAE, os dados já estão criptografados no caminho para o disco. As leituras seguem o caminho inverso. Em outras palavras, os dados deixam o disco criptografado, são enviados para RAID, são descriptografados pelo módulo criptográfico e, em seguida, são enviados para o resto da pilha, como mostrado na figura a seguir.



O NVE usa um módulo criptográfico de software validado pela FIPS 140-2 nível 1.

Para obter mais informações sobre o NVE, consulte "Datasheet NVE".

O NVE protege os dados na nuvem. A Cloud Volumes ONTAP e a Azure NetApp Files são capazes de fornecer criptografia de dados em repouso compatível com FIPS 140-2.

A partir do ONTAP 9.7, agregados e volumes recém-criados são criptografados por padrão quando você tem a licença NVE e o gerenciamento de chaves integradas ou externas. A partir do ONTAP 9.6, você pode usar a criptografia em nível de agregado para atribuir chaves ao agregado contendo para que os volumes sejam criptografados. Os volumes criados no agregado são criptografados por padrão. Você pode substituir o padrão quando criptografar o volume.

Comandos ONTAP NAE CLI

Antes de executar os seguintes comandos de CLI, verifique se o cluster tem a licença NVE necessária.

Para criar um agregado e criptografá-lo, execute o seguinte comando (quando executado em uma CLI de cluster ONTAP 9.6 e posterior):

```
fp-health::> storage aggregate create -aggregate aggregatename -encrypt
-with-aggr-key true
```

Para converter um agregado não-naE em um NAE an Aggregate, execute o seguinte comando (quando executado em um ONTAP 9.6 e CLI de cluster posterior):

```
fp-health::> storage aggregate modify -aggregate aggregatename  -node
svmname -encrypt-with-aggr-key true
```

Para converter um agregado NAE em um agregado não-naE, execute o seguinte comando (quando executado em um ONTAP 9.6 e CLI de cluster posterior):

```
fp-health::> storage aggregate modify -aggregate aggregatename -node
svmname -encrypt-with-aggr-key false
```

Comandos de CLI do ONTAP NVE

A partir do ONTAP 9.6, você pode usar a criptografia em nível de agregado para atribuir chaves ao agregado contendo para que os volumes sejam criptografados. Os volumes criados no agregado são criptografados por padrão.

Para criar um volume em um agregado que esteja habilitado para NAE, execute o seguinte comando (quando executado em uma CLI de cluster ONTAP 9.6 e posterior):

```
fp-health::> volume create -vserver svmname -volume volumename -aggregate
aggregatename -encrypt true
```

Para habilitar a criptografia de um volume existente "inplace" sem uma movimentação de volume, execute o seguinte comando (quando executado em uma CLI de cluster ONTAP 9.6 e posterior):

```
fp-health::> volume encryption conversion start -vserver svmname -volume
volumename
```

Para verificar se os volumes estão ativados para criptografia, execute o seguinte comando CLI:

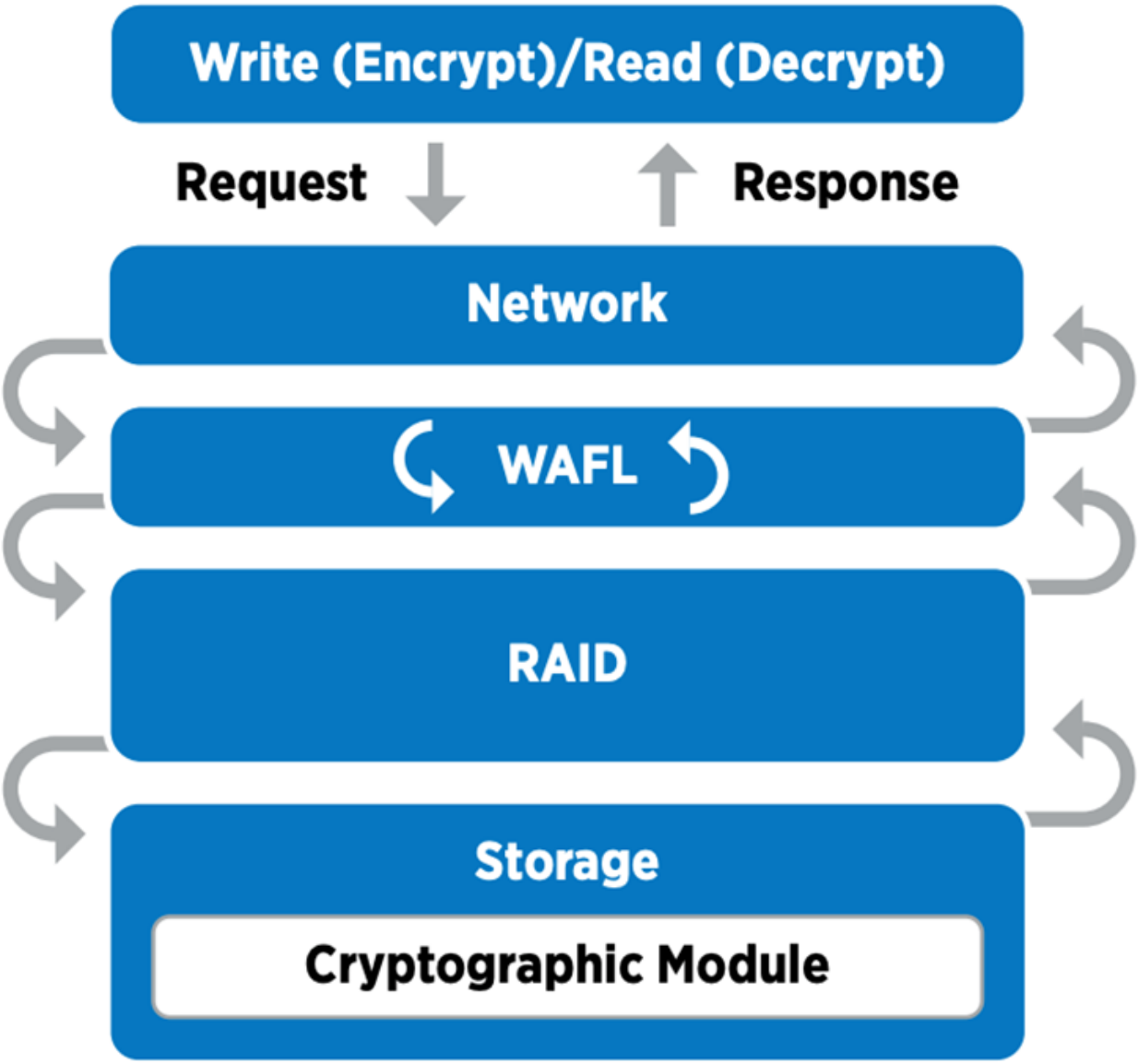
```
fp-health::> volume show -is-encrypted true
```

NSE

O NSE usa SEDs para executar a criptografia de dados por meio de um mecanismo acelerado por hardware.

O NSE está configurado para usar unidades de autocriptografia FIPS 140-2 nível 2 para facilitar a conformidade e o retorno de peças sobressalentes, habilitando a proteção de dados em repouso por meio da

criptografia de disco transparente AES de 256 bits. As unidades executam todas as operações de criptografia de dados internamente, como descrito na figura a seguir, incluindo a geração de chaves de criptografia. Para impedir o acesso não autorizado aos dados, o sistema de armazenamento deve se autenticar com a unidade usando uma chave de autenticação estabelecida na primeira vez que a unidade é usada.



O NSE usa criptografia de hardware em cada unidade, que é validada para FIPS 140-2 nível 2.

Para obter mais informações sobre o NSE, consulte "Datasheet do NSE".

Gerenciamento de chaves

O padrão FIPS 140-2 aplica-se ao módulo criptográfico conforme definido pelo limite, como mostrado na figura a seguir.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

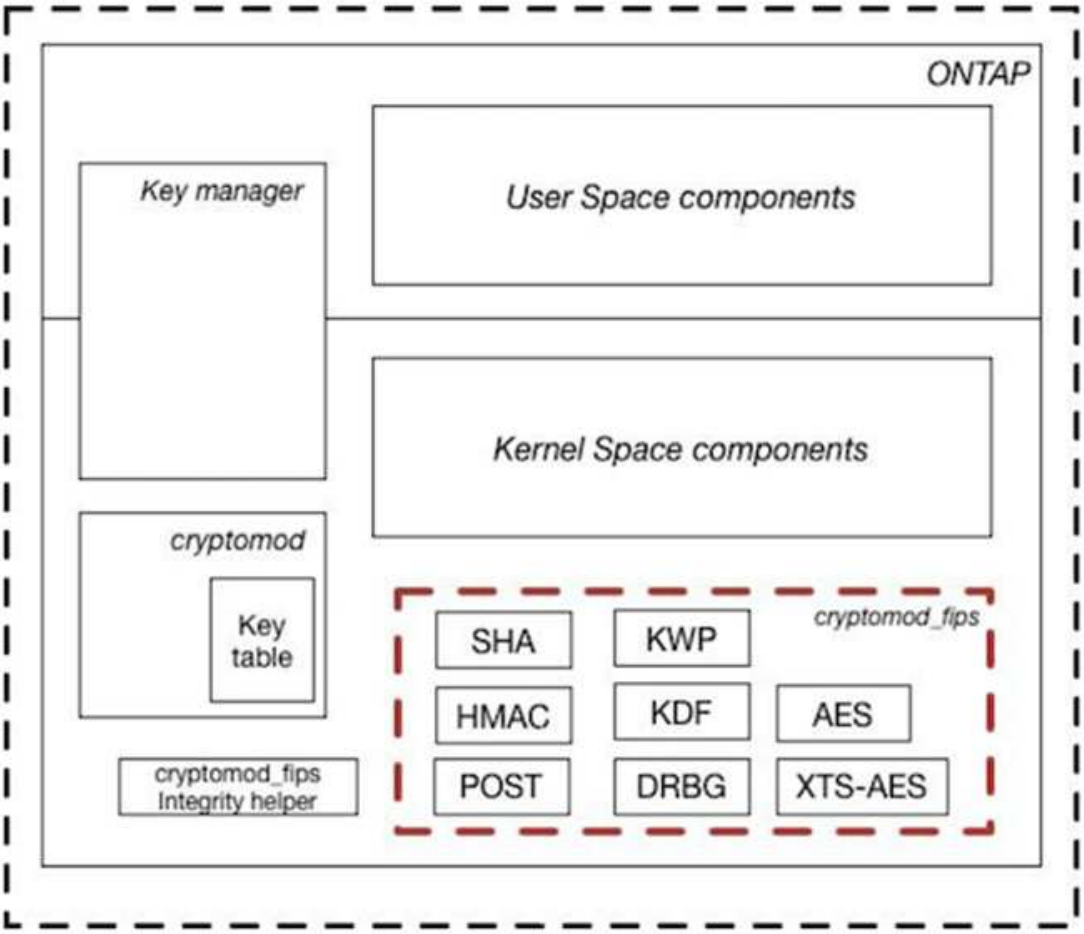


Figure 1 - Block Diagram

O gerenciador de chaves mantém o controle de todas as chaves de criptografia usadas pelo ONTAP. Os SEDs do NSE usam o gerenciador de chaves para definir as chaves de autenticação para SEDs do NSE. Ao usar o gerenciador de chaves, a solução NVE e NAE combinada é composta por um módulo criptográfico de software, chaves de criptografia e um gerenciador de chaves. Para cada volume, o NVE usa uma chave de criptografia de dados XTS-AES 256 exclusiva, que o gerenciador de chaves armazena. A chave usada para um volume de dados é exclusiva do volume de dados nesse cluster e é gerada quando o volume criptografado é criado. Da mesma forma, um volume NAE usa chaves de criptografia de dados XTS-AES 256 exclusivas por agregado, que o gerenciador de chaves também armazena. As chaves NAE são geradas quando o agregado criptografado é criado. O ONTAP não gera chaves, as reutiliza ou as exibe em texto sem formatação – elas são armazenadas e protegidas pelo gerenciador de chaves.

Suporte para gerenciador de chaves externo

A partir do ONTAP 9.3, os gerenciadores de chaves externos são suportados nas soluções NVE e NSE. O padrão FIPS 140-2 se aplica ao módulo criptográfico usado na implementação do fornecedor específico. Na maioria das vezes, os clientes FlexPod e ONTAP usam um dos seguintes gerenciadores-chave validados (de acordo com o "Matriz de interoperabilidade do NetApp"):

- Gemalto ou SAFENET AT
- Vormetric (Thales)
- IBM SKLM
- Utimaco (anteriormente Microfocus, HPE)

O backup da chave de autenticação NSE e NVMe SED é feito em um gerenciador de chaves externo usando o OASIS Key Management Interoperability Protocol (KMIP) padrão do setor. Somente o sistema de armazenamento, a unidade e o gerenciador de chaves têm acesso à chave, e a unidade não pode ser desbloqueada se for movida para fora do domínio de segurança, evitando assim vazamento de dados. O gerenciador de chaves externo também armazena chaves de criptografia de volume NVE e chaves de criptografia agregada NAE. Se a controladora e os discos forem movidos e não tiverem mais acesso ao gerenciador de chaves externo, os volumes NVE e NAE não estarão acessíveis e não poderão ser descriptografados.

O comando de exemplo a seguir adiciona dois servidores de gerenciamento de chaves à lista de servidores usados pelo gerenciador de chaves externo para armazenar máquina virtual (SVM) `svmname1`.

```
fp-health::> security key-manager external add-servers -vserver svmname1
-key-servers 10.0.0.20:15690, 10.0.0.21:15691
```

Quando um data center FlexPod está sendo usado em um cenário de alocação a vários clientes, o ONTAP capacita os usuários fornecendo separação de alocação por motivos de segurança no nível da SVM.

Para verificar a lista de gerenciadores de chaves externos, execute o seguinte comando CLI:

```
fp-health::> security key-manager external show
```

Combinar criptografia para criptografia dupla (defesa em camadas)

Se você precisar segregar o acesso aos dados e garantir que eles estejam protegidos o tempo todo, os SEDs do NSE podem ser combinados com criptografia no nível de rede ou malha. Os SEDs do NSE agem como um backstop se um administrador esquecer de configurar ou desconfigurar a criptografia de nível superior. Para duas camadas distintas de criptografia, você pode combinar SEDs NSE com NVE e NAE.

Plano de controle NetApp ONTAP em todo o cluster, modo FIPS

O software de gerenciamento de dados NetApp ONTAP tem uma configuração em modo FIPS que instancia um nível adicional de segurança para o cliente. Este modo FIPS aplica-se apenas ao plano de controlo. Quando o modo FIPS está ativado, de acordo com os principais elementos do FIPS 140-2, Transport Layer Security v1 (TLSv1) e SSLv3 são desativados e apenas TLS v1,1 e TLS v1,2 permanecem ativados.

> O painel de controle do cluster do ONTAP no modo FIPS está em conformidade com FIPS 140-2 nível 1. O modo FIPS de todo o cluster usa um módulo criptográfico baseado em software fornecido pelo NCSM.

O modo de conformidade FIPS 140-2 para o plano de controle de todo o cluster protege todas as interfaces de controle do ONTAP. Por padrão, o modo FIPS 140-2 only está desativado; no entanto, você pode ativar esse modo definindo o `is- fips-enabled` parâmetro para para `true` o `security config modify` comando.

Para ativar o modo FIPS no cluster ONTAP, execute o seguinte comando:

```
fp-health::> security config modify -interface SSL -is-fips-enabled true
```

Quando o modo SSL FIPS está ativado, a comunicação SSL do ONTAP para o cliente externo ou componentes de servidor fora do ONTAP usará a criptografia de reclamação FIPS para SSL.

Para mostrar o status FIPS de todo o cluster, execute os seguintes comandos:

```
fp-health::> set advanced
fp-health::*> security config modify -interface SSL -is-fips-enabled true
```

"Próximo: Benefícios da solução da infraestrutura convergente do FlexPod."

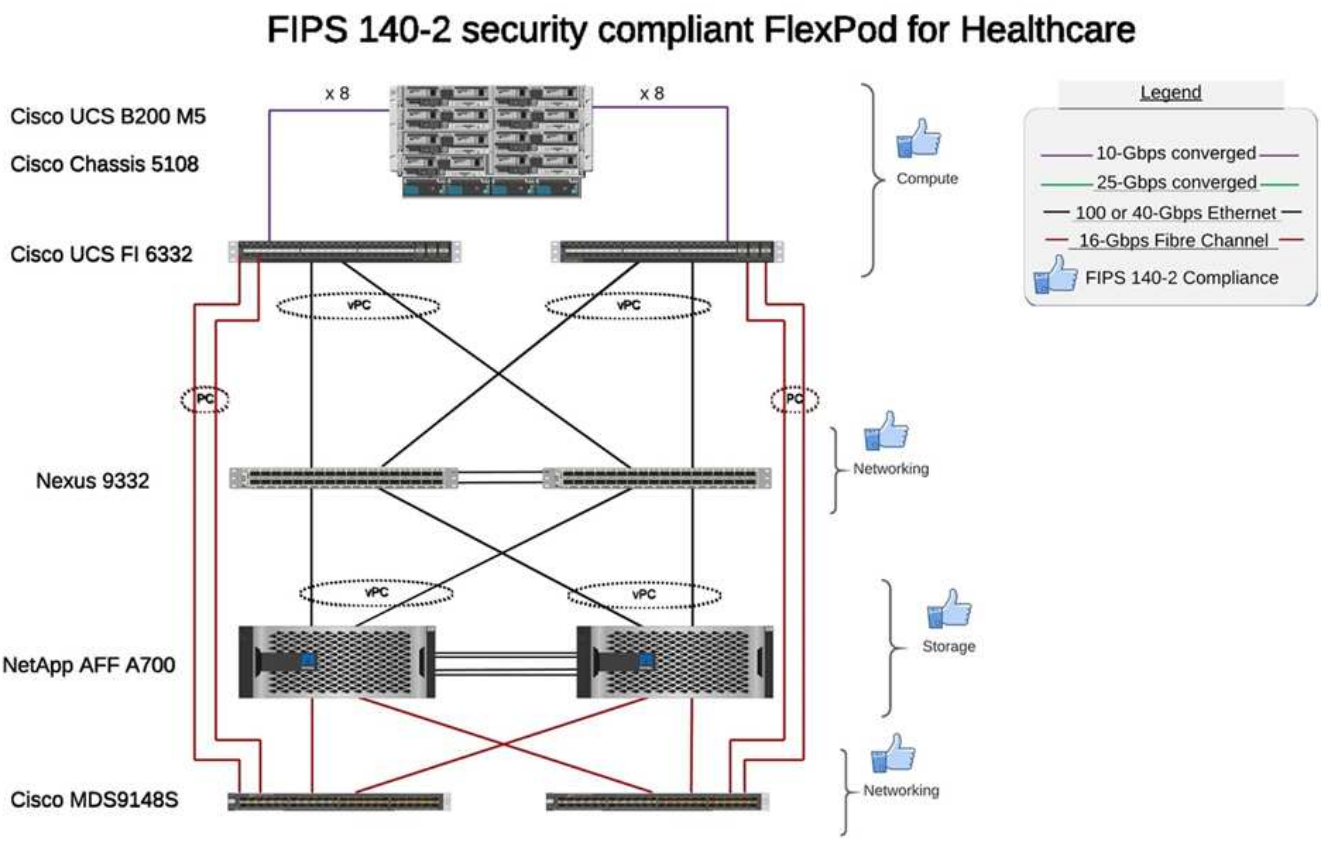
Benefícios da solução da infraestrutura convergente do FlexPod

"Anterior: Armazenamento FlexPod NetApp ONTAP e FIPS 140-2."

As organizações de saúde têm vários sistemas de missão crítica. Dois dos sistemas mais críticos são os sistemas de registo eletrónico de saúde (EHR) e os sistemas de imagiologia médica. Para demonstrar a configuração FIPS num sistema FlexPod, utilizamos uma EHR de código aberto e um sistema de arquivamento e comunicação de imagens (PACS) de código aberto para a configuração do laboratório e validação da carga de trabalho no sistema FlexPod. Para obter uma lista completa de capacidades EHR, componentes de aplicações lógicas EHR e como os sistemas EHR se beneficiam quando implementados num sistema FlexPod, "TR-4881: FlexPod para sistemas de Registro Eletrônico de Saúde"consulte . Para obter uma lista completa das capacidades de um sistema de imagiologia médica, componentes lógicos de aplicação e como os sistemas de imagiologia médica beneficiam quando implementados no FlexPod, "TR-4865: FlexPod para imagens médicas" consulte .

Durante a configuração do FIPS e a validação da carga de trabalho, exercemos caraterísticas de carga de trabalho representativas de uma organização típica de saúde. Por exemplo, exercemos um sistema EHR de código aberto para incluir cenários realistas de acesso aos dados do paciente e mudança. Além disso, exercitamos cargas de trabalho de imagem médica que incluíam imagens digitais e comunicações em objetos de medicina (DICOM) em um `*. dcm` formato de arquivo. Os objetos DICOM com metadados foram armazenados no arquivo e no armazenamento de blocos. Além disso, implementamos recursos multipathing de dentro de um servidor virtualizado RedHat Enterprise Linux (RHEL). Armazenamos objetos DICOM em um NFS, LUNs montados usando iSCSI e LUNs montados usando FC. Durante a configuração e validação do FIPS, observamos que a infraestrutura convergente do FlexPod superou nossas expectativas e teve um bom desempenho.

A figura a seguir mostra o sistema FlexPod usado para configuração e validação FIPS. Aproveitamos o "Data center FlexPod com VMware vSphere 7,0 e NetApp ONTAP 9 .7 Cisco Validated Design (CVD)" durante o processo de configuração.



Componentes de hardware e software da infraestrutura da solução

As duas figuras a seguir listam os componentes de hardware e software usados respetivamente durante o teste FIPS ativado em um FlexPod. As recomendações nestas tabelas são exemplos; você deve trabalhar com o seu NetApp SME para garantir que os componentes são adequados para a sua organização. Além disso, certifique-se de que os componentes e as versões são suportados nos "Ferramenta de Matriz de interoperabilidade do NetApp" (IMT) e "Lista de compatibilidade de hardware Cisco (HCL)".

Camada	Família de produtos	Quantidade e modelo	Detalhes
Computação	Chassi do Cisco UCS 5108	1 ou 2	
	Servidores blade Cisco UCS	3 B200 M5	Cada um com 2x 20 ou mais núcleos, 2,7GHz GB e 128-384GB GB de RAM
	Cartão de interface virtual Cisco UCS (VIC)	Cisco UCS 1440	Consulte
	2x interconexões de tecido Cisco UCS	6332	-
Rede	Switches Cisco Nexus	2x Cisco Nexus 9332	-
Rede de armazenamento	Rede IP para acesso ao storage por protocolos SMB/CIFS, NFS ou iSCSI	Mesmos switches de rede como acima	-
	Acesso ao storage por FC	2x Cisco MDS 9148S	-

Camada	Família de produtos	Quantidade e modelo	Detalhes
Armazenamento	Sistema de storage all-flash NetApp AFF A700	Cluster de 1 GbE	Cluster com dois nós
	Compartimento de disco	Um compartimento de disco de DS224C TB ou NS224 TB	Totalmente preenchido com 24 unidades
	SSD	>24, 1,2TB ou maior capacidade	-

Software	Família de produtos	Versão ou lançamento	Detalhes
Vários	Linux	RHEL 7.X	-
	Windows	Windows Server 2012 R2 (64 bits)	-
	NetApp ONTAP	ONTAP 9,7 ou posterior	-
	Interconexão de malha Cisco UCS	Cisco UCS Manager 4,1 ou posterior	-
	Switches Ethernet Cisco série 3000 ou 9000	Para a série 9000, 7,0(3)i7(7) ou posterior para a série 3000, 9,2(4) ou posterior	-
	Cisco FC: Cisco MDS 9132T	8,4(1a) ou posterior	-
	Hipervisor	VMware vSphere ESXi 6,7 U2 ou posterior	-
Armazenamento	Sistema de gerenciamento de hipervisor	VMware vCenter Server 6,7 U3 (vCSA) ou posterior	-
Rede	Console de storage virtual (VSC) do NetApp	VSC 9,7 ou posterior	-
	NetApp SnapCenter	SnapCenter 4,3 ou posterior	-
	Gerente do Cisco UCS	4,1(1c) ou posterior	
Hipervisor	ESXi		
Gerenciamento	Sistema de gerenciamento de hypervisor VMware vCenter Server 6,7 U3 (vCSA) ou posterior		
	Console de storage virtual (VSC) do NetApp	VSC 9,7 ou posterior	
	NetApp SnapCenter	SnapCenter 4,3 ou posterior	

Software	Família de produtos	Versão ou lançamento	Detalhes
	Gerente do Cisco UCS	4,1(1c) ou posterior	

"Próximo: Considerações adicionais de segurança do FlexPod."

Considerações adicionais de segurança do FlexPod

"Anterior: Benefícios da solução da infraestrutura convergente do FlexPod."

A infraestrutura do FlexPod é uma plataforma modular, convergente, opcionalmente virtualizada, dimensionável (com escalabilidade horizontal e vertical) e econômica. Com a plataforma FlexPod, você pode fazer escalabilidade horizontal independente de computação, rede e storage para acelerar a implantação de aplicações. E a arquitetura modular permite operações ininterruptas mesmo durante as atividades de escalabilidade horizontal e atualização do sistema.

Componentes diferentes de um SISTEMA DE HIT exigem que os dados sejam armazenados em sistemas de arquivos SMB/CIFS, NFS, EXT4 e NTFS. Esse requisito significa que a infraestrutura precisa fornecer acesso aos dados pelos protocolos NFS, CIFS e SAN. Um único sistema de storage NetApp pode dar suporte a todos esses protocolos, eliminando a necessidade de práticas legadas de sistemas de storage específicos a protocolos. Além disso, um único sistema de storage NetApp pode dar suporte a várias cargas de TRABALHO DE SUCESSO, como EHRs, PACS ou VNA, genômica, VDI e muito mais, com níveis de desempenho garantidos e configuráveis.

Quando implantado em um sistema FlexPod, O HIT oferece vários benefícios específicos para o setor de saúde. A lista a seguir é uma descrição de alto nível desses benefícios:

- **Segurança FlexPod**. A segurança está na base de um sistema FlexPod. Nos últimos anos, o ransomware se tornou uma ameaça. Ransomware é um tipo de malware que é baseado em criptovirologia, o uso de criptografia para construir software malicioso. Esse malware pode usar criptografia de chave simétrica e assimétrica para bloquear os dados da vítima e exigir um resgate para fornecer a chave para descriptografar os dados. Para saber como a solução FlexPod ajuda a mitigar ameaças como ransomware, "TR-4802: A solução para ransomware" consulte . Os componentes da infraestrutura do FlexPod também "Compatível com FIPS 140-2" são .
- **Cisco Intersight.** O Cisco Intersight é uma plataforma inovadora, baseada na nuvem e de gerenciamento como serviço que fornece um painel único para gerenciamento e orquestração de FlexPod de toda a stack. A plataforma Intersight usa módulos criptográficos compatíveis com segurança FIPS 140-2. A arquitetura de gerenciamento fora da banda da plataforma torna-a fora do escopo de alguns padrões ou auditorias, como HIPAA. Nenhuma informação individual identificável de saúde na rede é enviada para o portal Intersight.
- **Tecnologia NetApp FPolicy.** O NetApp FPolicy (uma evolução da política de arquivos de nome) é uma estrutura de notificação de acesso a arquivos para monitoramento e gerenciamento do acesso a arquivos nos protocolos NFS ou SMB/CIFS. Essa tecnologia faz parte do software de gerenciamento de dados da ONTAP há mais de uma década. Ela é útil para detectar ransomware. Esse mecanismo Zero Trust fornece medidas de segurança extras além das permissões em listas de controle de acesso (ACLs). FPolicy tem dois modos de operação: Nativo e externo:
  - O modo nativo fornece listas negras e listas brancas de extensões de arquivos.
  - O modo externo tem os mesmos recursos do modo nativo, mas também se integra com um servidor FPolicy que é executado externamente para o sistema ONTAP, bem como um sistema de gerenciamento de informações e eventos de segurança (SIEM). Para obter mais informações sobre

como combater ransomware, consulte o "Fighting ransomware: Parte três – ONTAP FPolicy, outra poderosa ferramenta nativa (também conhecida como livre)" blog.

- **Dados em repouso**. O ONTAP 9 e posterior têm três soluções de criptografia de dados em repouso compatíveis com FIPS 140-2:
  - O NSE é uma solução de hardware que usa unidades com autocriptografia.
  - O NVE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade em que ele esteja habilitado com uma chave exclusiva para cada volume.
  - NAE é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele é habilitado com chaves exclusivas para cada agregado.

> A partir do ONTAP 9.7, o NAE e o NVE são ativados por padrão se o pacote de licença do NetApp NVE com o nome VE estiver no lugar.

- **Dados em voo**. A partir do ONTAP 9.8, a segurança de protocolo de Internet (IPsec) fornece suporte de criptografia de ponta a ponta para todo o tráfego IP entre um cliente e um SVM do ONTAP. A criptografia de dados IPsec para todo o tráfego IP inclui protocolos NFS, iSCSI e SMB/CIFS. O IPsec fornece a única opção de criptografia em voo para tráfego iSCSI.
- **Criptografia de dados completa em um data fabric de multicloud híbrida**. Os clientes que usam tecnologias de criptografia de dados em repouso, como NSE ou NVE e Cluster Peering Encryption (CPE) para tráfego de replicação de dados, agora podem usar criptografia completa entre cliente e storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9.8 ou posterior e usando IPsec. A partir do ONTAP 9, é possível ativar o modo de conformidade FIPS 140-2 para interfaces do plano de controle em todo o cluster. Por predefinição, o modo apenas FIPS 140-2 está desativado. A partir do ONTAP 9.6, o CPE fornece suporte de criptografia TLS 1,2 AES-256 GCM para recursos de replicação de dados do ONTAP, como as tecnologias NetApp SnapMirror, NetApp SnapVault e NetApp FlexCache. A criptografia é configurada por meio de uma chave pré-compartilhada (PSK) entre dois pares de cluster.
- **Alocação segura a vários clientes**. Oferece suporte às necessidades crescentes de infraestrutura compartilhada de servidor e armazenamento virtualizado, permitindo a alocação segura a vários clientes de informações específicas de instalações, particularmente ao hospedar várias instâncias de bancos de dados e software.

"Próximo: Conclusão."

Conclusão

"Anterior: Considerações adicionais de segurança do FlexPod."

Ao executar seu aplicativo de saúde em uma plataforma FlexPod, sua organização de saúde fica mais protegida por uma plataforma habilitada para FIPS 140-2. O FlexPod oferece proteção em várias camadas em todos os componentes: Computação, rede e storage. Os recursos de proteção de dados da FlexPod protegem dados em repouso ou em trânsito, além de manter os backups seguros e prontos quando necessário.

Evite erros humanos aproveitando os designs pré-validados da FlexPod que são infraestruturas convergentes rigorosamente testadas pela parceria estratégica da Cisco e da NetApp. Um sistema FlexPod projetado e projetado para fornecer desempenho previsível e de baixa latência e alta disponibilidade com pouco impacto, mesmo quando o FIPS 140-2-2 está habilitado nas camadas de computação, rede e storage. Essa abordagem resulta em uma experiência de usuário superior e tempo de resposta ideal para os usuários do seu SISTEMA HIT.

"Próximo: Agradecimentos, histórico de versões e onde encontrar informações adicionais."

Agradecimentos, histórico de versões e onde encontrar informações adicionais

"Anterior: Conclusão."

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e sites:

- Guia de configuração de segurança da família NX-os do Cisco MDS 9000

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_fips.html#task_1188151

- Guia de configuração de segurança do Cisco Nexus 9000, versão 9,3(x)

  https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/security/configuration/guide/b-cisco-nexus-9000-nx-os-security-configuration-guide-93x/m-configuring-fips.html

- Publicação NetApp e Federal Information Processing Standard (FIPS) 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- FIPS 140-2

  https://fieldportal.netapp.com/content/902303

- Guia de endurecimento da NetApp ONTAP 9

  https://www.netapp.com/pdf.html?item=/media/10674-tr4569pdf.pdf

- Guia de alimentação de encriptação NetApp

  https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- Detalhes completos do NVE e NAE

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- Folha de dados NSE

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- Centro de Documentação do ONTAP 9

  http://docs.netapp.com

- Publicação NetApp e Federal Information Processing Standard (FIPS) 140-2

  https://www.netapp.com/company/trust-center/compliance/fips-140-2/

- Conformidade com Cisco e FIPS 140-2-2

  https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

- Módulo de segurança criptográfica NetApp

  https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2648.pdf

- Práticas de segurança cibernética para organizações de saúde de médio e grande porte

  https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

- Programa de Validação de módulo criptográfico e Cisco (CMVP)

  https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules/search?SearchMode=Basic&Vendor=cisco&CertificateStatus=Active&ValidationYear=0

- Criptografia de storage NetApp, unidades com criptografia automática NVMe, criptografia de volume NetApp e criptografia agregada NetApp

  https://www.netapp.com/pdf.html?item=/media/17073-ds-3898.pdf

- Criptografia de volumes do NetApp e criptografia agregada do NetApp

  https://www.netapp.com/pdf.html?item=/media/17070-ds-3899.pdf

- Criptografia de storage do NetApp

  https://www.netapp.com/pdf.html?item=/media/7563-ds-3213-en.pdf

- FlexPod para sistemas de Registro Eletrônico de Saúde

  https://www.netapp.com/pdf.html?item=/media/22199-tr-4881.pdf

- Dados agora: Melhoria da performance em ambientes EHR da Epic com a tecnologia flash conectada à nuvem

  https://www.netapp.com/media/10809-cloud-connected-flash-wp.pdf

- Data center FlexPod para infraestrutura EHR da Epic

  https://www.netapp.com/pdf.html?item=/media/17061-ds-3683.pdf

- Guia de implantação do FlexPod Datacenter para EPIC EHR

  https://www.netapp.com/media/10658-tr-4693.pdf

- Infraestrutura de data center FlexPod para software MEDITECH

  https://www.netapp.com/media/8552-flexpod-for-meditech-software.pdf

- A norma FlexPod estende-se ao software MEDITECH

  https://blog.netapp.com/the-flexpod-standard-extends-to-meditech-software/

- FlexPod para guia de dimensionamento direcional MEDITECH

  https://www.netapp.com/pdf.html?item=/media/12429-tr4774.pdf

- FlexPod para imagens médicas

  https://www.netapp.com/media/19793-tr-4865.pdf

- Ai em saúde

  https://www.netapp.com/pdf.html?item=/media/7393-na-369pdf.pdf

- FlexPod para o setor de saúde facilite sua transformação

  https://flexpod.com/solutions/verticals/healthcare/

- FlexPod de Cisco e NetApp

  https://flexpod.com/

Agradecimentos

- Abhinav Singh, Engenheiro de Marketing Técnico, NetApp
- Brian o'Mahony, arquiteto de soluções de saúde (Epic), NetApp
- Brian Pruitt, Gerente de Desenvolvimento de Negócios da Pursuit, NetApp
- Arvind Ramakrishnan, arquiteto sênior de soluções, NetApp
- Michael Hommer, CTO de campo global da FlexPod, NetApp

Histórico de versões

Versão	Data	Histórico de versões do documento
Versão 1,0	Abril de 2021	Lançamento inicial

Cisco Intersight com storage NetApp ONTAP

Guia de início rápido do Cisco Intersight com armazenamento NetApp

Em parceria com: 

Introdução

A NetApp e a Cisco se uniram para fornecer o Cisco Intersight, uma visualização de painel único do ecossistema do FlexPod. Essa integração simplificada cria uma plataforma de gerenciamento unificada para todos os componentes da infraestrutura FlexPod e da solução FlexPod. O Cisco Intersight permite monitorar o storage NetApp, a computação Cisco e o inventário VMware. Ele também permite orquestrar ou automatizar fluxos de trabalho para realizar tarefas de storage e virtualização em conjunto.

Informações relacionadas

Para saber mais, consulte os seguintes documentos e sites:

"TR 4883: Data center FlexPod com ONTAP 9.8, conetor de armazenamento ONTAP para Cisco Intersight e modo gerenciado Cisco Intersight"

"Centro de ajuda do Cisco Intersight"

"Visão geral de introdução ao Cisco Intersight"

"Guia de instalação e atualização do Intersight Appliance"

O que há de novo

Esta seção lista os novos recursos e funcionalidades disponíveis para o Cisco Intersight com armazenamento NetApp ONTAP.

Janeiro de 2024

- Orquestração de armazenamento do NetApp usando fluxos de trabalho de referência agora disponíveis para download no GitHub através do "Repositório do fluxo de trabalho do FlexPod Intersight". Para obter mais informações sobre os novos fluxos de trabalho de referência no GitHub, "Caso de uso 2: Orquestração de storage do NetApp usando workflows de referência"consulte .

Novembro de 2023

- Adicionada página namespaces NVMe sob a seção Inventário da interface do usuário.

Agosto de 2023

É necessária uma atualização para o NetApp Active IQ Unified Manager 9,13GA para garantir a compatibilidade e a funcionalidade completa com a versão mais recente.

- Melhorada a tarefa de LUN inteligente de novo NetApp para indicar claramente a disponibilidade de opções de seleção para criar um novo grupo de iniciadores ou selecionar um grupo de iniciadores existente. Quando os usuários agora selecionam a caixa para criar um novo grupo de iniciadores, o parâmetro para escolher um grupo de iniciadores existente não está mais disponível. Se os usuários desmarcar a caixa para criar um novo grupo de iniciadores, o parâmetro do grupo de iniciadores existente ficará disponível.
- Melhorou o novo mapa LUN NetApp e Remover tarefas de mapa LUN NetApp. A nova relação entre o LUN e o grupo de iniciadores é agora atualizada. O inventário da IU é atualizado imediatamente para o LUN e para o grupo de iniciadores na execução da tarefa.
- A página verificações agora carrega corretamente os usuários pela primeira vez que fazem login e não requer mais uma atualização.

Julho de 2023

É necessária uma atualização para o NetApp Active IQ Unified Manager 9,13GA para garantir a compatibilidade e a funcionalidade completa com a versão mais recente.

- Nomes atualizados para tarefas de armazenamento do NetApp. Consulte caso de uso 3 fluxos de trabalho personalizados usando formulário livre de designer para obter a lista completa de tarefas renomeadas.
- O endereço IP da interface NFS foi adicionado como uma saída da tarefa novo volume inteligente do NetApp nas.
- Uma verificação de que o transporte ASUP é HTTPS foi adicionada à guia Cheques.
- O tipo de camada correto para todos os níveis agora é exibido corretamente na interface do usuário de camadas.
- Todas as licenças compatíveis agora são exibidas corretamente na página licenças.
- O valor preciso para compartilhamentos CIFS sem ou sem um diretório inicial agora é exibido na página compartilhamentos.
- Classificação e filtragem agora ativados para a coluna mapeada na página LUNS.
- A classificação e filtragem agora habilitaram a coluna Autenticação ativada na página servidores NTP.
- Adicionadas novas verificações e as seguintes categorias correspondentes ao separador verificações.
  - Segurança
  - Anti-ransomware
  - Disponibilidade
  - Outros
- Na visualização de detalhes do inventário, o relatório agora é usado em vez da capacidade física usada.

Junho de 2023

É necessária uma atualização para o NetApp Active IQ Unified Manager 9.13RC1 para garantir a compatibilidade e a funcionalidade completa com a versão mais recente.

- Nomes atualizados para tarefas de armazenamento do NetApp. Consulte "Use Case 3 fluxos de trabalho

personalizados usando formulário livre de designer" para obter a lista completa de tarefas renomeadas.

Abril de 2023

- Adicionadas as guias políticas de proteção (SnapMirror) e políticas de captura instantânea na página políticas na seção Inventário da interface do usuário.
- Adicionada página clientes NFS na seção Inventário da interface do usuário.
- Coluna protegida adicionada na página VMs de armazenamento na seção Inventário da interface do usuário.
- Modificado como as informações de redução de dados são relatadas e exibidas.
- Adicionadas guias nível local e nível de nuvem sob a página camadas na seção Inventário da interface do usuário.
- A coluna nó agora é exibida após a coluna Nome na página portas na seção Inventário da interface do usuário.

Janeiro de 2023

É necessária uma atualização para o NetApp Active IQ Unified Manager 9,12 GA para garantir a compatibilidade e a funcionalidade total com a versão mais recente. Para obter uma lista de problemas conhecidos relacionados a esta versão, Problemas conhecidosconsulte .

- As verificações de interoperabilidade do Intersight podem agora distinguir entre os modos de firmware do UCSM e do IMM ao efetuar verificações de compatibilidade.
- As relações de proteção não serão exibidas no Intersight para ONTAP 9.7. Este problema foi corrigido no ONTAP 9.8RC1.

Agosto de 2022

É necessária uma atualização para o NetApp Active IQ Unified Manager 9,11 GA para garantir a compatibilidade e a funcionalidade total com a versão mais recente. Para obter uma lista de problemas conhecidos relacionados a esta versão, Problemas conhecidosconsulte .

- Cálculo atualizado da capacidade disponível do cluster para corresponder ao System Manager
- Página geral do cluster atualizado para ocultar o resumo das métricas de desempenho até que os dados de desempenho sejam preenchidos
- Corrigido o problema geral da interface de usuário da página que ocasionalmente fazia com que a página fosse suspensa
- Adição de políticas de compartilhamentos CIFS, serviços CIFS, Qtrees e SVM SnapMirror para inventário de back-end.
- Adicionados compartilhamentos e Qtrees ao menu de navegação da IU na seção Inventário lógico
- Compartilhamentos adicionados como guia de uma VM de armazenamento selecionada
- Foram adicionadas informações de Serviço CIFS na guia Geral da VM de armazenamento se a VM de armazenamento estiver ativada por CIFS
- Adicionada uma página de verificações de cluster que permite que os usuários validem a configuração dos sistemas de armazenamento NetApp aderem às práticas recomendadas

Julho de 2022

- Recursos visuais aprimorados para a taxa de redução de dados de cluster agora disponíveis sob o Widget de capacidade
- Adicionada a guia interfaces FC à página interfaces de rede
- Criar um novo volume usando a tarefa genérica "novo volume de armazenamento" agora define a garantia de espaço de volume para nenhum e a porcentagem de reserva de snapshot para 0%
- O campo de comentário na tarefa Editar política de instantâneo agora é opcional e não é mais obrigatório
- Consistência aprimorada de inventário e orquestração da IU
- As informações de capacidade do Intersight em capacidade de cluster agora são consistentes com o System Manager
- Caixa de seleção adicionada na tarefa New Storage Virtual Machine para exibir todos os parâmetros ao criar uma nova interface de gerenciamento para melhorar a usabilidade
- Protocolos movidos abaixo da correspondência do cliente, agora consistentes com o System Manager
- Página geral da política de exportação agora exibindo o(s) Protocolo(s) de acesso
- remoção do igroup agora registrado condicionalmente
- Adicionados parâmetros de "Política de failover" e "reversão automática" para nas em Nova Interface de dados nas de armazenamento e Nova Interface de dados iSCSI de armazenamento
- Reverter para a tarefa New Storage nas Smart volume agora remove a política de exportação se nenhum outro volume estiver anexado
- Aperfeiçoamentos feitos para tarefas Smart volume e Smart LUN

Abril de 2022

Para garantir a compatibilidade e a funcionalidade completa com versões futuras, recomenda-se que você atualize seu NetApp Active IQ Unified Manager para a versão 9.10P1.

- Adicionado domínio de transmissão à página de detalhes da porta Ethernet
- Alterado o termo "agregado" para "Categoria" para agregado e SVM na interface de usuário
- Alterado o termo "Estado do cluster" para "Estado da matriz"
- O filtro MTU agora funciona para carateres
- Adicionada página de interface de rede ao inventário de cluster
- Adicionado AutoSupport ao inventário de cluster
- Opção adicionada `cdpd.enable` ao nó
- Adicionado um objeto para o vizinho CDP
- Adicionadas tarefas de storage de fluxo de trabalho do NetApp no Cisco Intersight. Consulte "Use Case 3 fluxos de trabalho personalizados usando formulário livre de designer" para obter uma lista completa das tarefas de armazenamento do NetApp.

Janeiro de 2022

- Foram adicionados alarmes de Intersight baseados em eventos para NetApp Active IQ Unified Manager 9,10 ou superior.

Para garantir a compatibilidade e a funcionalidade completa com versões futuras, recomenda-se que você atualize seu NetApp Active IQ Unified Manager para a versão 9,10.

- Defina explicitamente cada protocolo habilitado (verdadeiro ou falso) para Storage Virtual Machine
- Mapeado o estado do cluserHealthStatus ok-with-suppressed para OK
- Coluna Saúde renomeada para coluna Status do cluster na página Lista de Cluster
- Mostrar matriz de armazenamento "inalcançável" se o cluster estiver inativo ou de outra forma inalcançável
- Coluna Saúde renomeada para coluna Status da matriz na página Geral do cluster
- O SVM agora tem uma guia "volumes" que mostra todos os volumes do SVM
- O volume tem uma seção de capacidade de snapshot
- As licenças agora são apresentadas corretamente

Outubro de 2021

- Lista atualizada de tarefas de storage do NetApp disponíveis no Cisco Intersight. Consulte "Use Case 3 fluxos de trabalho personalizados usando formulário livre de designer" para obter uma lista completa das tarefas de armazenamento do NetApp.
- Coluna Saúde adicionada sob a página de lista de cluster.
- Detalhes expandidos agora disponíveis na página Geral para um cluster selecionado.
- Tabela do servidor NTP agora acessível através do painel de navegação.
- Adicionada uma nova guia Sensores contendo a página Geral da Máquina Virtual de armazenamento.
- Resumo do grupo de agregação de VLAN e link agora disponível na página Geral da porta.
- Coluna capacidade total de dados adicionada sob a tabela capacidade total de volume.
- Colunas latência, IOPS e throughput adicionadas nas tabelas Estatísticas de volume médio, Estatísticas de LUN médias, Estatísticas de agregado médio, Estatísticas de VM de armazenamento médio e Estatísticas de nó médias

As métricas de performance acima estão disponíveis apenas para storage arrays monitorados pelo NetApp Active IQ Unified Manager 9,9 ou superior.

Problemas conhecidos

- Se estiver a utilizar uma versão do AIQUM 9,11 ou anterior, ocorrerá uma discrepância entre os valores apresentados na página Lista de armazenamento e o gráfico de barras de capacidade na página Geral armazenamento. Para resolver este problema, atualize para AIQUM 9,12 ou superior para garantir a precisão dos valores de capacidade apresentados.
- Se você estiver usando o AIQUM 9,11 ou anterior, quaisquer verificações realizadas pela guia "interoperabilidade" na página "sistemas integrados" não conseguirão distinguir os componentes IMM e UCSM Cisco com precisão. Para resolver este problema, atualize para o AIQUM 9,12 para garantir que todos os componentes estão devidamente identificados.
- Para garantir que os dados do inventário de armazenamento do Intersight não sejam afetados durante o processo de coleta de dados, quaisquer clusters ONTAP não suportados (ou seja, versões abaixo do ONTAP 9.7P1) devem ser removidos do Active IQ Unified Manager (AIQUM).

- Todos os alvos reivindicados requerem uma versão mínima do AIQUM do 9,11 para consultas de interoperabilidade do sistema integrado FlexPod para serem concluídas com êxito.
- A página verificações de inventário de armazenamento não será preenchida se o cluster ONTAP for adicionado ao AIQUM usando um FQDN. Os usuários devem adicionar clusters ONTAP ao AIQUM usando um endereço IP.

Requisitos

Verifique se você atende aos requisitos de hardware, software e licenciamento para a integração de storage do NetApp ONTAP com o Cisco Intersight.

Requisitos de hardware e software

Estes são os componentes mínimos de hardware e software necessários para implementar a solução. Os componentes que são usados em qualquer implementação específica da solução podem variar com base nos requisitos do cliente.

Componente	Detalhes da exigência
NetApp ONTAP	ONTAP 9.7P1 e posterior
NetApp Active IQ Unified Manager	É necessária a versão mais recente do NetApp Active IQ Unified Manager (atualmente 9.14RC1)
Array de storage NetApp	Todos os storage arrays ONTAP ASA, AFF e FAS são compatíveis com o ONTAP 9.7P1 e posterior
Hipervisor de virtualização	VSphere 7,0 e posterior

"Sistemas compatíveis com Cisco Intersight"Consulte para obter os requisitos mínimos dos componentes de computação do Cisco UCS e da versão do UCSM.

Requisitos de licenciamento do Cisco Intersight

O Cisco Intersight oferece serviços como o serviço de infraestrutura e o serviço Cloud Orchestrator para gerenciar, automatizar e otimizar o storage físico (storage NetApp). Você pode usar esses serviços para gerenciar o servidor Cisco UCS e o sistema Cisco HyperFlex. O serviço de infraestrutura e o Cloud Orchestrator usam um modelo de licenciamento baseado em subscrição com várias camadas. Você pode escolher o nível de volume de servidor Cisco UCS necessário para o período de assinatura selecionado.

Modelo de licenciamento

O modelo de licenciamento dos Serviços de infraestrutura do Cisco Intersight foi simplificado e agora oferece os dois níveis a seguir:

- **Princípios Básicos dos Serviços de infraestrutura Intersight da Cisco** - a camada de licença Essentials oferece gerenciamento de servidores, incluindo funcionalidade global de monitoramento de integridade, inventário, suporte proativo por meio da integração Cisco TAC, autenticação multifator, além de fornecer acesso a SDK e API.
- **Vantagem dos Serviços de infraestrutura Intersight da Cisco** - a camada de licença Advantage oferece gerenciamento avançado de servidores com visibilidade estendida, integração de ecossistemas, automação de Cisco e hardware e software de terceiros, além de fornecer soluções de vários domínios.

Para obter mais informações sobre os recursos cobertos por vários níveis de licenciamento, "Licença dos Serviços de infraestrutura" acesse .

Antes de começar

Para monitorar e orquestrar o storage do NetApp do Cisco Intersight, você precisa do NetApp Active IQ Unified Manager e do Cisco Intersight Assist Virtual Appliance instalados no ambiente do vCenter.

Instale ou atualize o NetApp Active IQ Unified Manager

Instale ou atualize para o Active IQ Unified Manager (é necessária a versão mais recente, atualmente 9.14RC1) se não o tiver feito. Para obter instruções, vá para "Documentação do NetApp Active IQ Unified Manager".

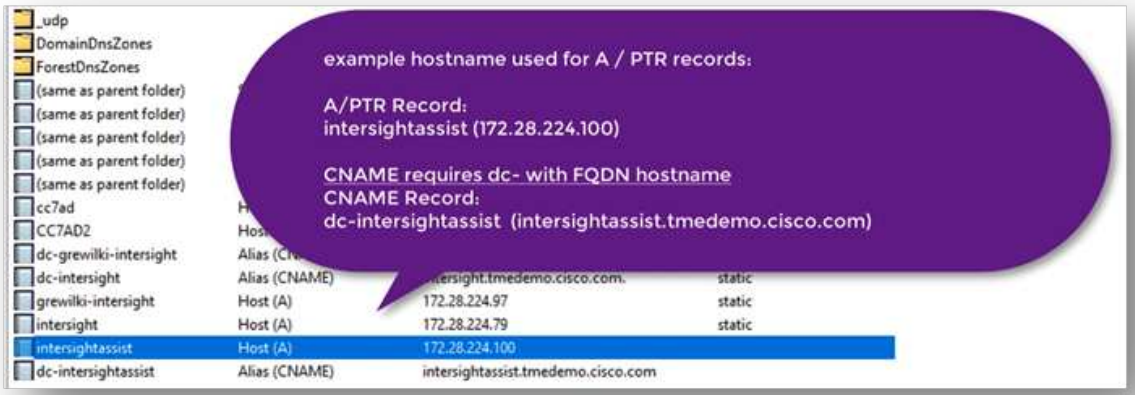
Instale o dispositivo virtual de assistência à inspeção Cisco

Certifique-se de que conhece o "Requisitos de licenciamento, sistema e rede de dispositivos virtuais do Cisco Intersight".

Passos

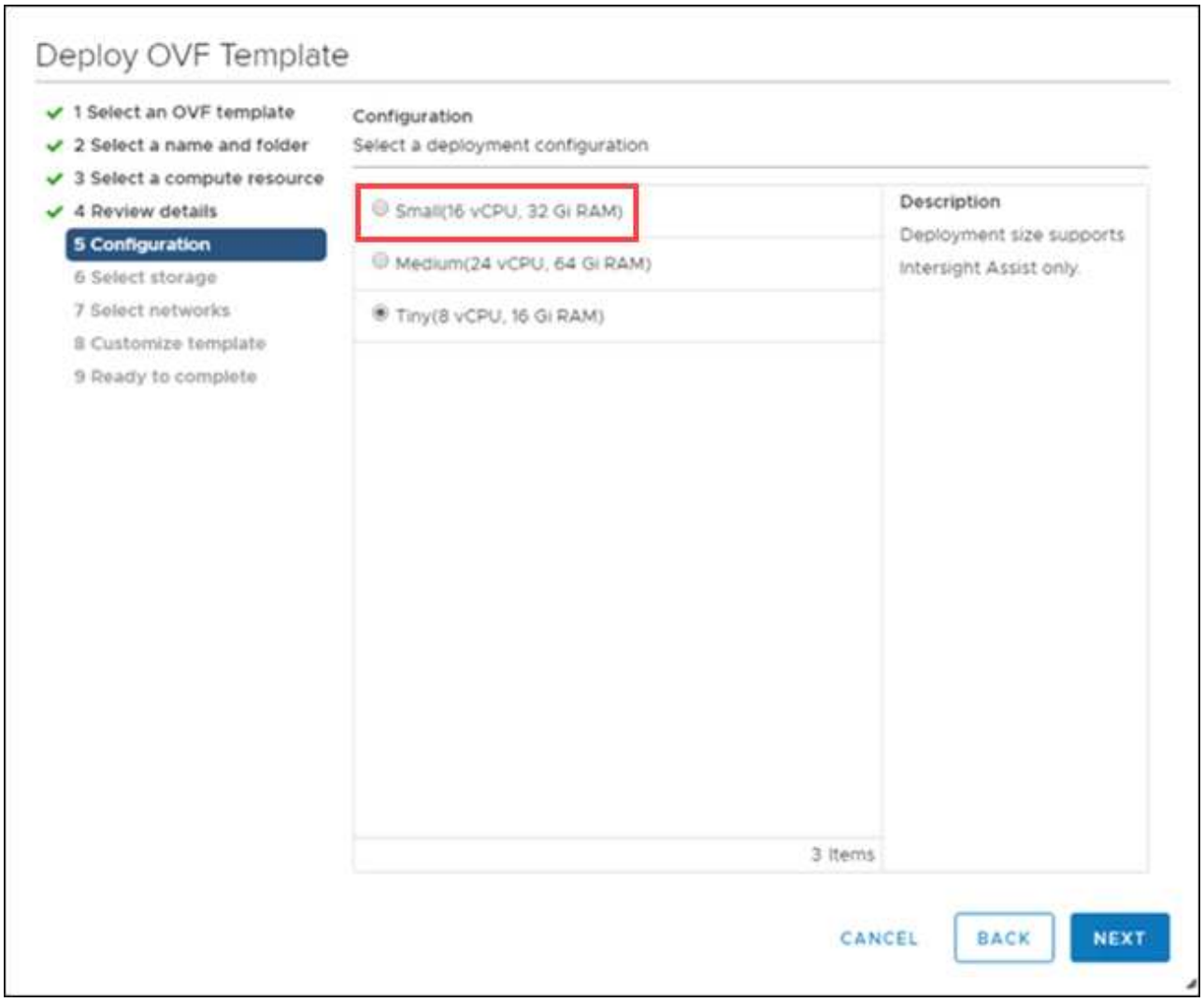
1. Crie uma conta do Cisco Intersight. "https://intersight.com/"Visite para criar sua conta Intersight. Você deve ter um ID Cisco válido para criar uma conta do Cisco Intersight.
2. Faça o download do Intersight Virtual Appliance em "software.Cisco.com". Para obter mais informações, vá para "Guia de instalação e atualização do Intersight Appliance" .
3. Implante os ÓVULOS. DNS e NTP são necessários para implantar o OVA.

    a. Configure DNS com Registros A/PTR e CNAME Alias antes de implantar o OVA. Veja o exemplo abaixo.

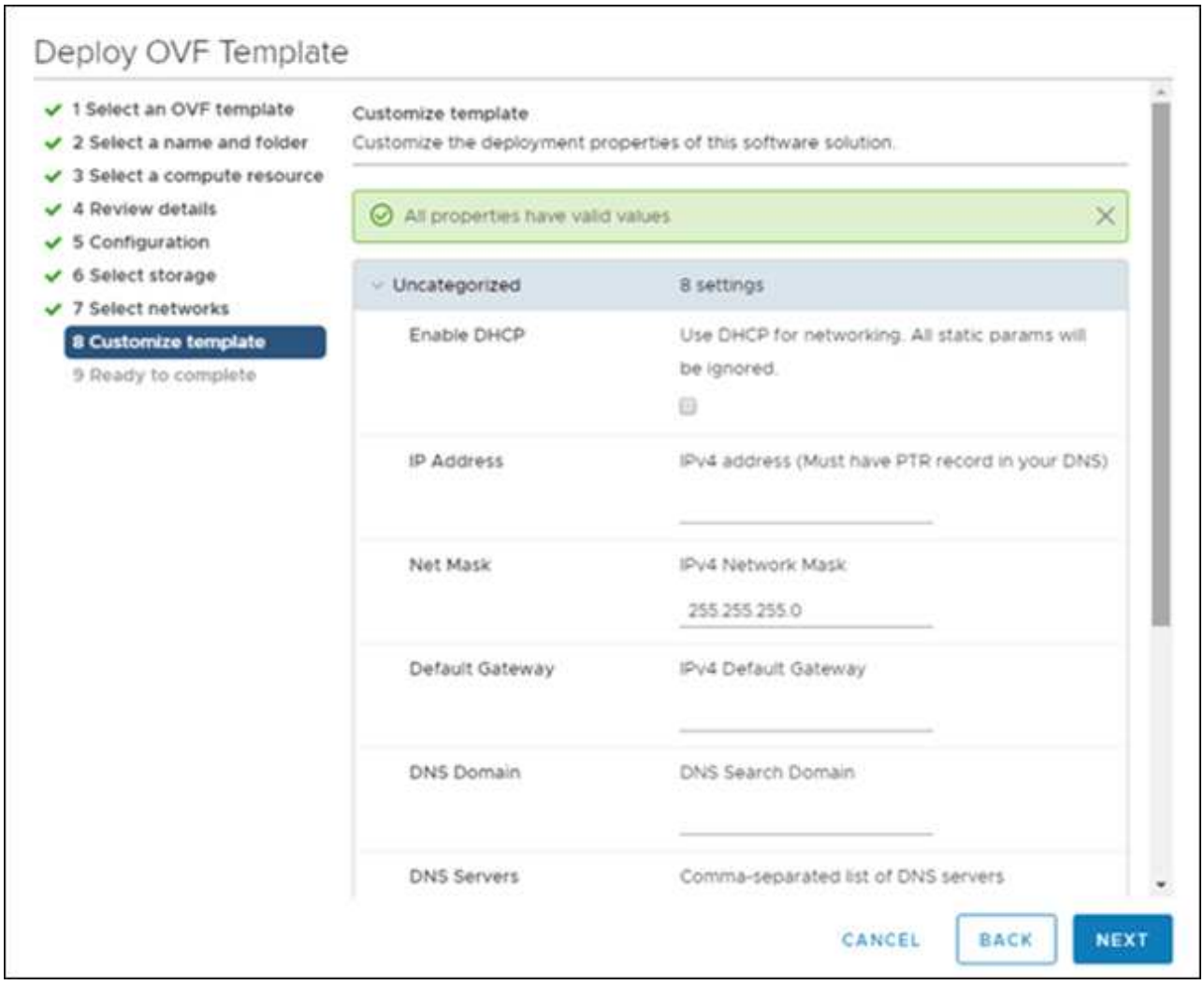


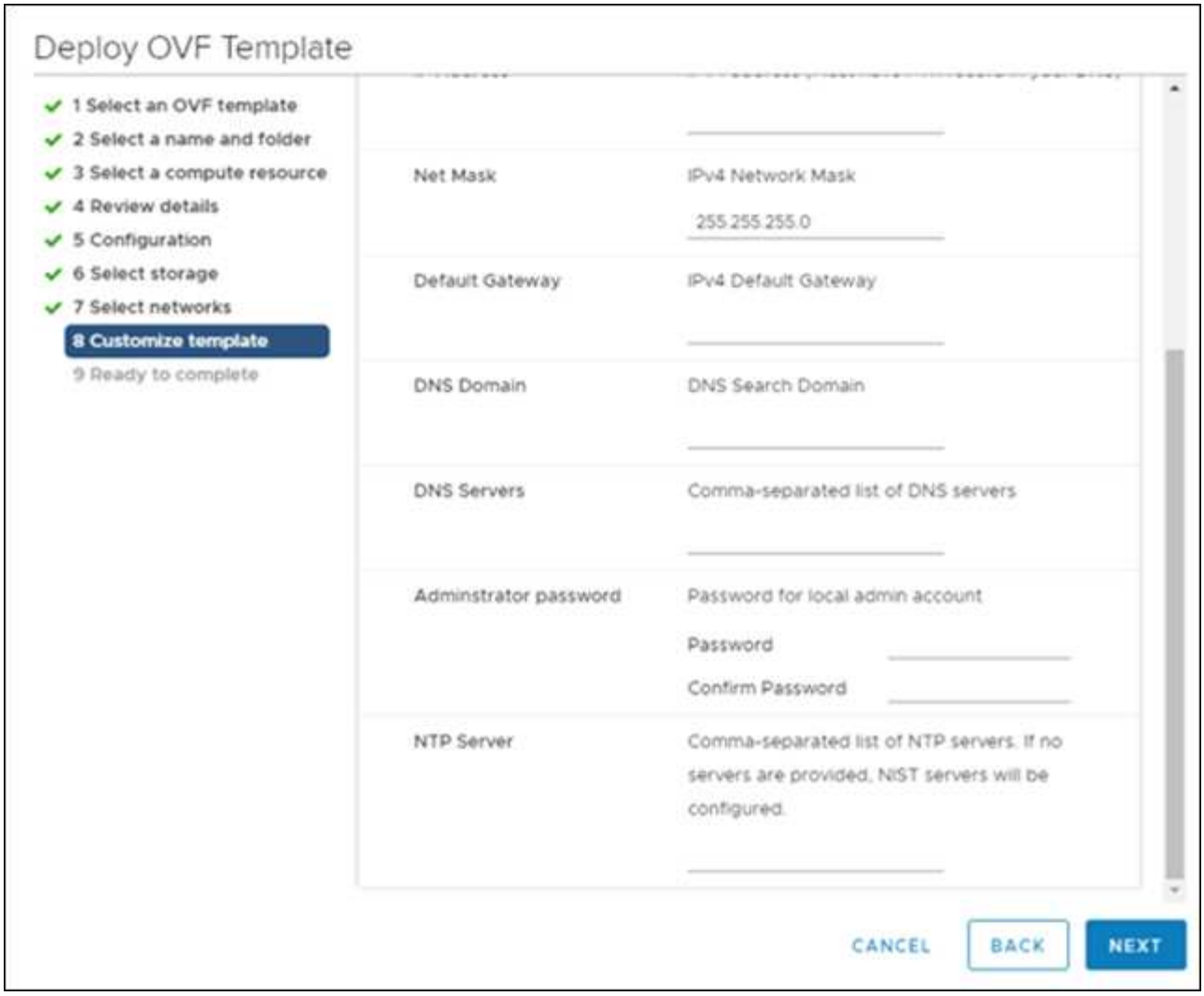
    b. Escolha o tamanho de configuração apropriado (pequeno, pequeno ou médio) com base nos requisitos de implantação DE OVA para o Intersight Virtual Appliance.

    DICA: para um cluster ONTAP de dois nós com um grande número de objetos de armazenamento, o NetApp recomenda que você use a opção pequena (16 vCPU, 32 GI RAM).



c. Na página **Personalizar modelo**, personalize as propriedades de implantação do modelo OVF. A senha do administrador é usada para os usuários locais: admin(`webUI/cli/ssh`).


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Configuration
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
All properties have valid values
Uncategorized
8 settings
Enable DHCP
Use DHCP for networking. All static params will be ignored.
IP Address
IPv4 address (Must have PTR record in your DNS)
Net Mask
IPv4 Network Mask
255.255.255.0
Default Gateway
IPv4 Default Gateway
DNS Domain
DNS Search Domain
DNS Servers
Comma-separated list of DNS servers
CANCEL
BACK
NEXT



a. Clique em **seguinte**.

4. Após a ativação do dispositivo de assistência Intersight.

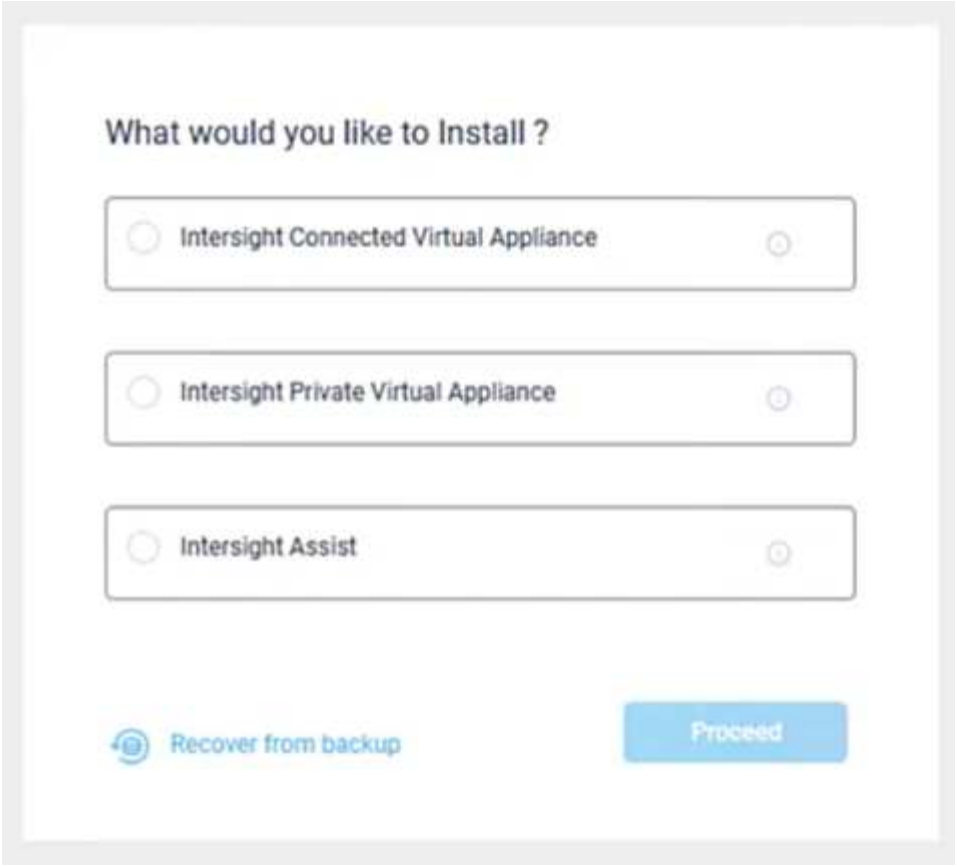
   a. Navegue para para para https://FQDN-of-your-appliance concluir a configuração pós-instalação do seu aparelho.

      O processo de instalação é iniciado automaticamente. A instalação pode demorar até uma hora, dependendo da largura de banda até Intersight.comMbps. Também pode levar vários segundos para que o site seguro esteja operacional após a ativação da VM.

   b. Durante o processo de pós-implantação, selecione a seguinte opção:

      - **Intersight Assist.** Essa implantação permite que o modelo SaaS se conete ao Cisco Intersight.

      > Ao selecionar o Intersight Assist, anote a ID do dispositivo e o código de reclamação antes de continuar.



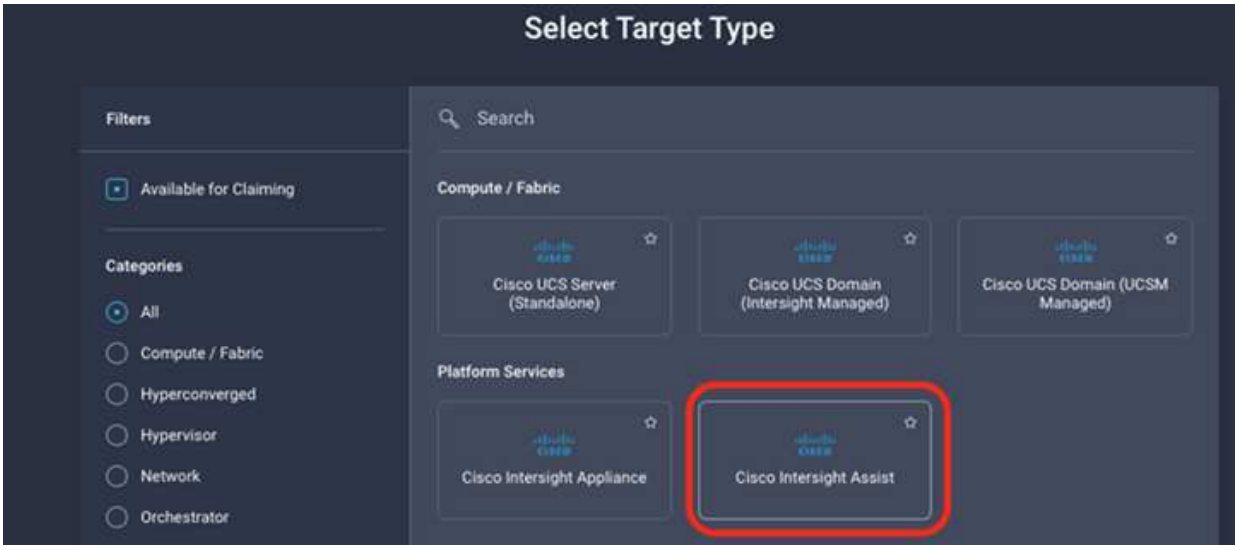
a. Clique em **Proceed**.

b. Selecione **Intersight Assist** e execute as seguintes etapas:

   i. Navegue até sua conta SaaS Intersight em "https://intersight.com".

   ii. Clique em **Targets**, **Cisco Intersight Assist** e, em seguida, em **Start**.

   iii. Solicite o equipamento **Cisco Intersight Assist** copiando e colando a ID do dispositivo e o código de reclamação do seu dispositivo virtual Intersight Assist recentemente implantado.



   iv. Regresse ao aparelho **Assistência Intersight Cisco** e clique em **continuar.** Talvez seja necessário atualizar o navegador.

O processo de download e instalação começa. Os binários são transferidos do Intersight Cloud para seu dispositivo local. O tempo de conclusão varia dependendo da largura de banda para o Intersight Cloud.

Configure o servidor PROXY AIQ UM para o serviço IMT

Se você estiver usando um servidor proxy com AIQ UM para Cisco Intersight com armazenamento NetApp ONTAP, configure a configuração por meio da interface de linha de comando (CLI) para utilizar o serviço de ferramenta de matriz de interoperabilidade (IMT). O serviço IMT está disponível no separador **interoperabilidade** da página **sistemas integrados**. Você deve usar o shell Diag da máquina virtual Active IQ Unified Manager (OVA) para configurar as configurações do servidor PROXY AIQ UM.

Para obter informações sobre como acessar o shell AIQ UM Diag, consulte "Como acessar o shell DIAG da máquina virtual Active IQ Unified Manager (OVA)"

Passos

1. Inicie sessão no terminal AIQ UM e execute o seguinte comando para iniciar sessão no um.

```
um cli login -u <um maintenance user name>
```

Exemplo

```
um cli login -u admin
```

2. Defina `imt_proxy_host` o e `imt_proxy_port` executando os seguintes comandos.

O proxy IMT é uma configuração separada das configurações de proxy do AutoSupport (ASUP).

```
um option set imt.https.proxy.host=<IMT_PROXY_HOST>
um option set imt.https.proxy.port=<IMT_PROXY_PORT>
```

Exemplo

```
um option set imt.https.proxy.host=example-proxy.cls.eng.com
um option set imt.https.proxy.port=8200
```

As configurações do servidor proxy IMT não suportam autenticação.

3. Visualize os detalhes do proxy do IMT para verificar as `proxy_host` configurações e `proxy_port` através do seguinte comando.

```
um option list |grep imt
```

Alvos do pedido de reembolso

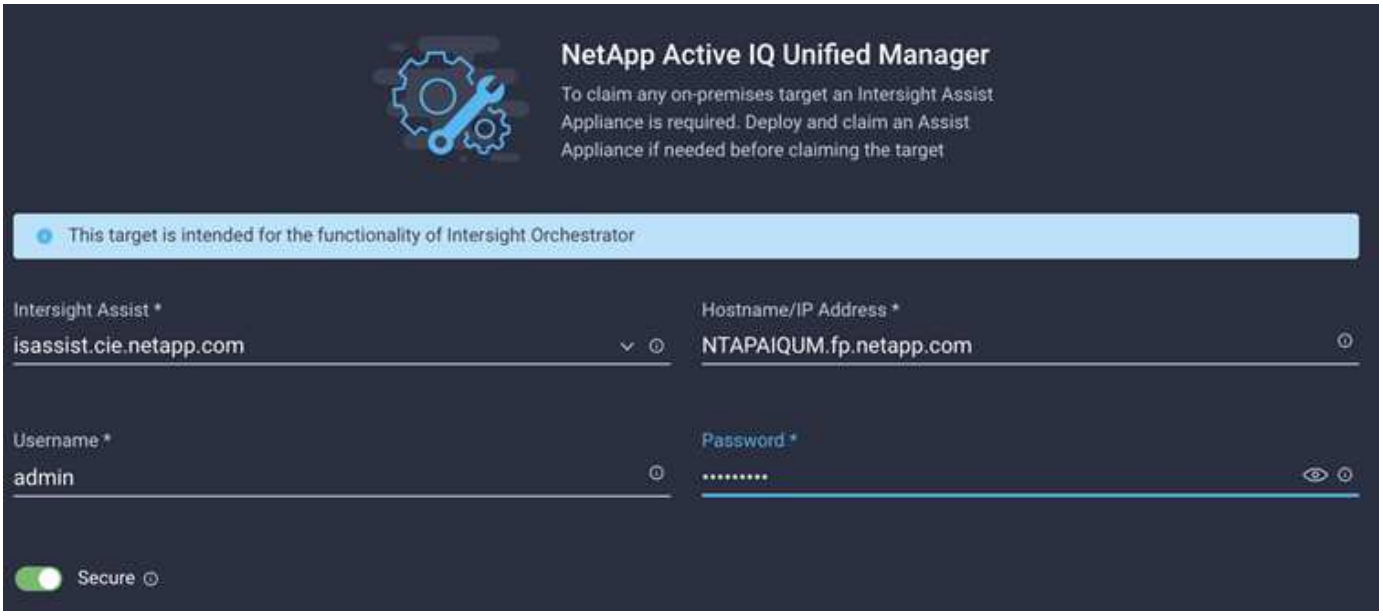
Após a instalação do Cisco Intersight Assist, você pode solicitar seus dispositivos de armazenamento e virtualização NetApp. Retorne à página **Intersight Targets** e adicione seus destinos do vCenter e do NetApp Active IQ Unified Manager.

Certifique-se de que o gateway da API NetApp Active IQ Unified Manager (AIQ UM) está ativado.

No Gerenciador Unificado do NetApp IQ, navegue até **Configurações > Geral > Configurações de recursos**.

O exemplo a seguir mostra o alvo NetApp AIQ UM que está sendo reivindicado ao Cisco Intersight.

Quando você reivindica o destino NetApp AIQ UM, todos os clusters gerenciados pelo Active IQ Unified Manager são adicionados automaticamente ao Intersight.

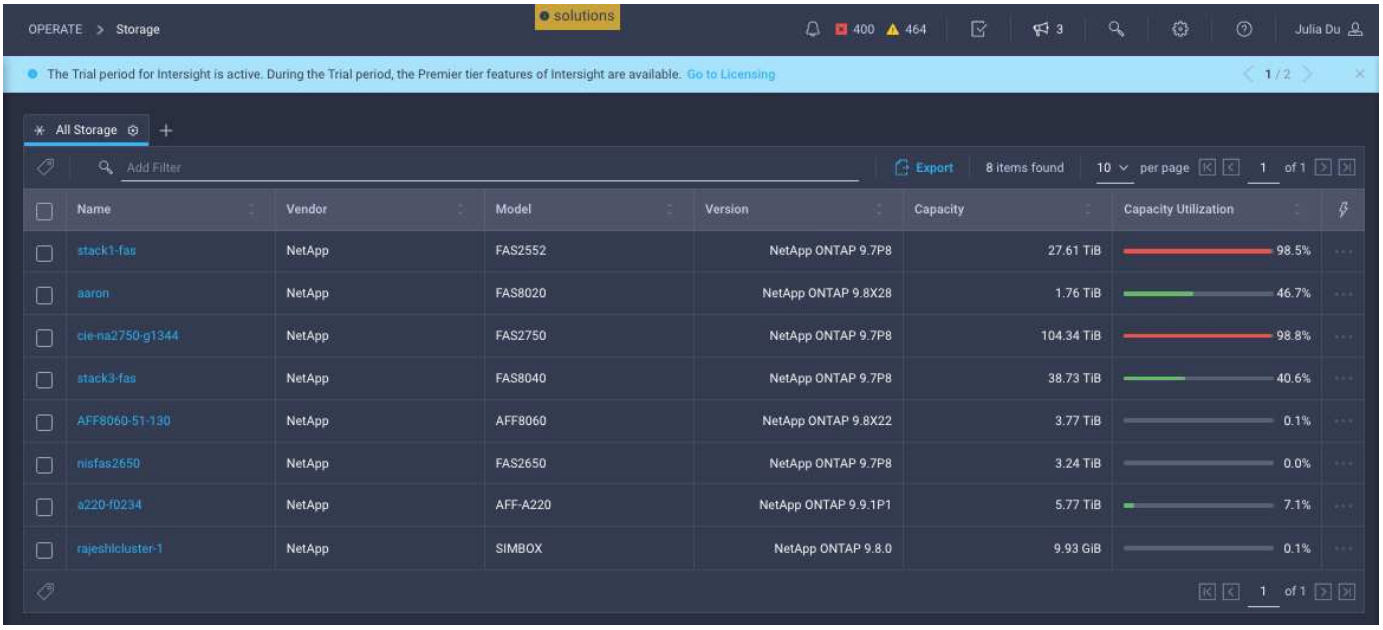


Monitore o storage do NetApp do Cisco Intersight

Depois que os destinos são reivindicados, os widgets de armazenamento do NetApp, o inventário de armazenamento e as guias de virtualização ficam disponíveis se você tiver uma licença de nível Advantage. As guias de orquestração estão disponíveis se você tiver uma licença do nível Premier.

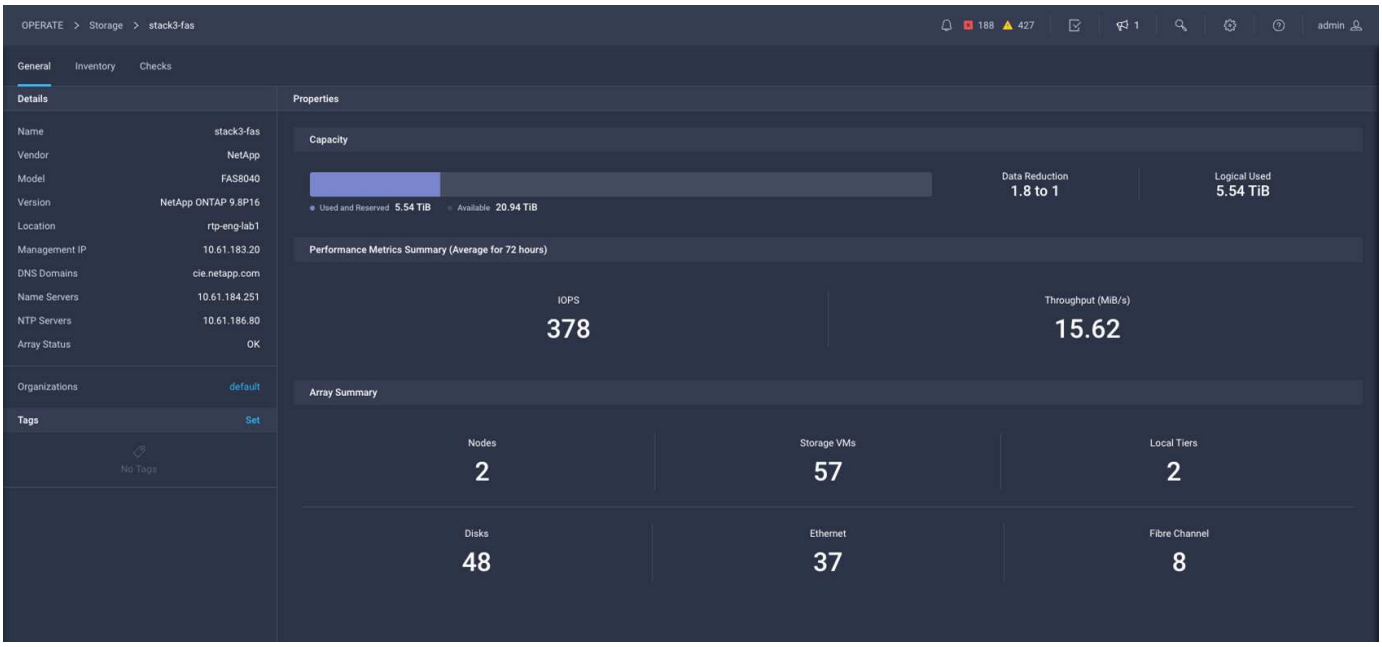
Visão geral do inventário de armazenamento

A captura de tela a seguir exibe a tela **operar > armazenamento**.



A captura de tela a seguir mostra a visão geral do cluster de armazenamento.

As informações de resumo da métrica de desempenho a seguir serão exibidas somente se o storage array for monitorado pelo NetApp Active IQ Unified Manager 9,9 ou superior.

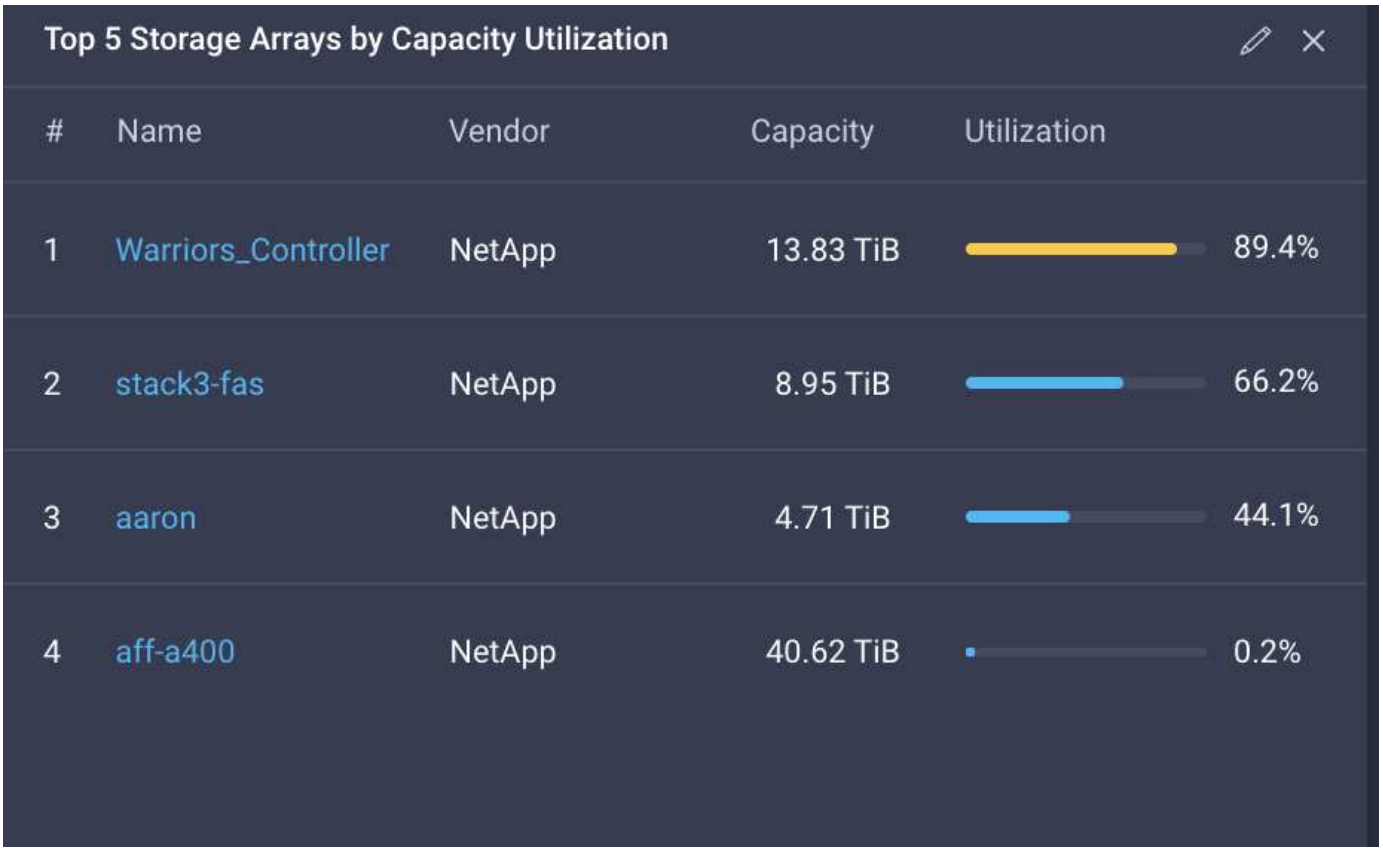


Widgets de armazenamento

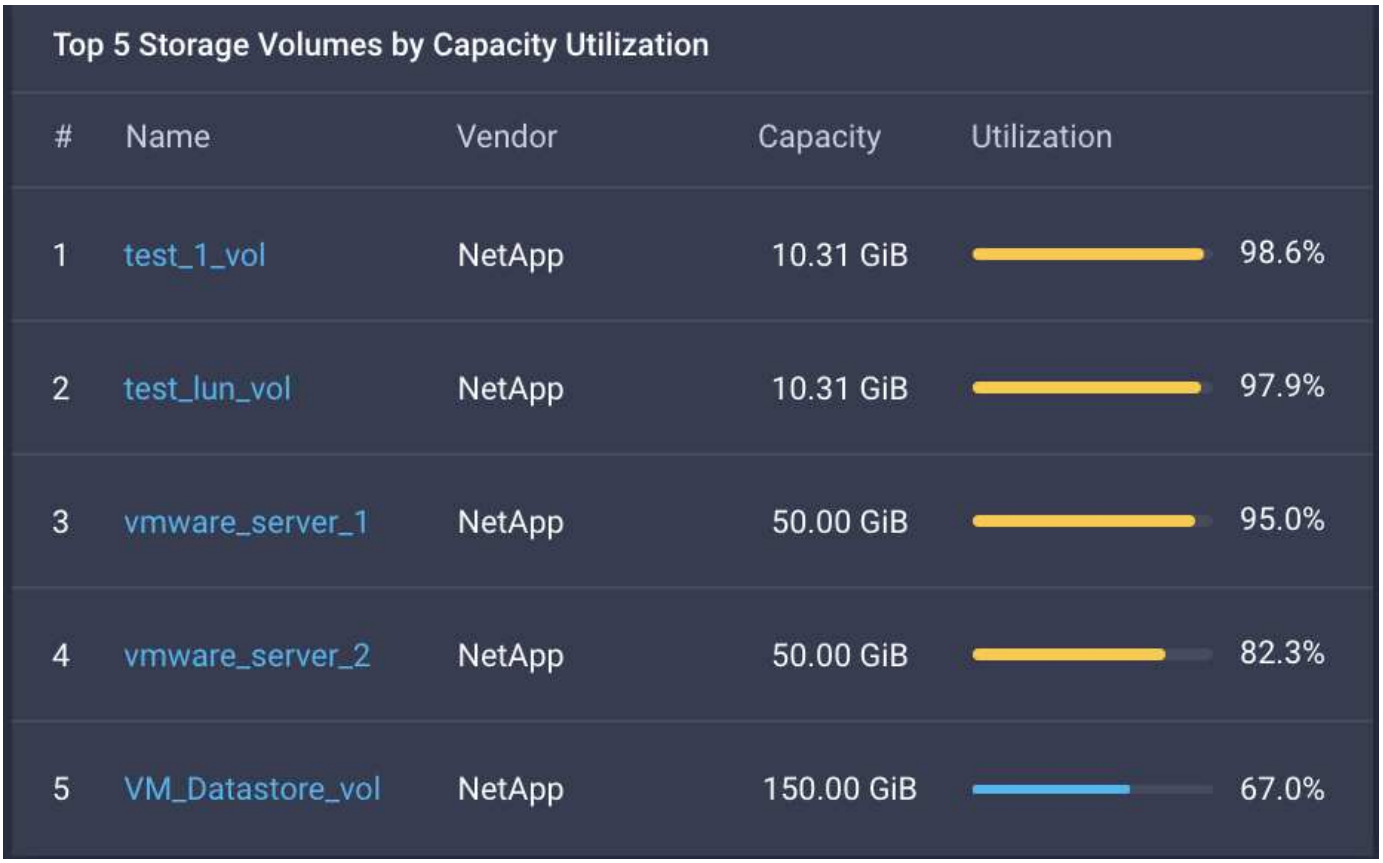
Para visualizar widgets de armazenamento, navegue até **Monitoramento > painéis > Exibir widgets de armazenamento do NetApp**.

- A captura de tela a seguir mostra o widget Resumo da versão do armazenamento.

- Esta captura de tela mostra os 5 principais arrays de armazenamento por widget de utilização de capacidade.



- Esta captura de tela mostra os 5 principais volumes de armazenamento por widget de utilização de capacidade.



Casos de uso

Estes são alguns exemplos de casos de uso para monitoramento e orquestração de storage NetApp do Cisco Intersight.

Caso de uso 1: Monitorando o inventário de armazenamento e widgets do NetApp

Quando o ambiente de armazenamento do NetApp está disponível no Cisco Intersight, você pode monitorar os objetos de armazenamento do NetApp em detalhes a partir do inventário de armazenamento e obter uma visão geral dos widgets de armazenamento.

1. Implante o Intersight Assist OVA (tarefa OnPrem no vCenter Environment).
2. Adicione dispositivos NetApp AIQ UM no Intersight Assist.
3. Vá para **armazenamento** e navegue pelo inventário de armazenamento do NetApp.
4. Adicione **Widgets** para armazenamento NetApp ao seu **Painel de monitorização**.

Caso de uso 2: Orquestração de storage do NetApp usando workflows de referência

Quando os ambientes de armazenamento e vCenter do NetApp estiverem disponíveis no Cisco Intersight, você poderá usar fluxos de trabalho de referência completos disponíveis no GitHub por meio do "Repositório do fluxo de trabalho do FlexPod Intersight".

Os fluxos de trabalho de referência incluem tarefas de armazenamento e virtualização. O arquivo README para o repositório fornece os pré-requisitos necessários para a execução de fluxos de trabalho, links para recursos úteis (incluindo documentação sobre como importar um fluxo de trabalho) e links de documentação para cada fluxo de trabalho de referência.

Cada fluxo de trabalho tem uma pasta no repositório contendo dois arquivos:

- O arquivo JSON para baixar e importar para o Intersight,
- Um arquivo de documentação que fornece uma visualização das tarefas no fluxo de trabalho, entradas de fluxo de trabalho e um exemplo de execução do fluxo de trabalho.

Execute o seguinte procedimento para importar e usar um fluxo de trabalho de referência:

1. Implante o Intersight Assist OVA (tarefa OnPrem no vCenter Environment).
2. Adicione dispositivos NetApp AIQ UM no Intersight Assist.
3. Adicione o destino do vCenter ao Intersight por meio do Intersight Assist.
4. Faça o download do arquivo JSON para um fluxo de trabalho de referência do repositório do FlexPod-Intersight-Workflow.
5. Importe o fluxo de trabalho para o Intersight e execute o fluxo de trabalho.

Aqui está uma lista de fluxos de trabalho disponíveis no repositório do GitHub FlexPod-Intersight-Workflow:

- Adicione iniciadores ao Grupo de iniciadores do NetApp
- Nova Política de exportação para volume NetApp
- Novo armazenamento de dados nas usando o NetApp Smart volume

- Nova interface de dados NetApp FC
- Novo Grupo de Iniciadores do NetApp
- Nova interface de dados iSCSI NetApp
- Nova interface de dados NetApp nas
- Nova máquina virtual de storage NetApp
- Novo armazenamento de dados VMFS usando o NetApp Smart LUN
- Remova os iniciadores do Grupo de iniciadores do NetApp
- Remova o armazenamento de dados nas usando o volume inteligente NetApp
- Remova a Política de exportação do NetApp
- Remova o Grupo Iniciador do NetApp
- Remova o armazenamento de dados VMFS usando o NetApp Smart LUN
- Atualize o armazenamento de dados nas usando o NetApp volume Inteligente
- Atualize o armazenamento de dados VMFS usando o NetApp Smart LUN

Caso de uso 3: Fluxos de trabalho personalizados usando formulário livre de designer

Quando os ambientes NetApp Storage e vCenter estiverem disponíveis no Cisco Intersight, você poderá criar fluxos de trabalho personalizados usando as tarefas de virtualização e storage da NetApp.

1. Implantar o Intersight Assist OVA (tarefa OnPrem no vCenter Environment)
2. Adicione dispositivos NetApp AIQ UM no Intersight Assist.
3. Adicione o vCenter Target ao Intersight por meio do Intersight Assist.
4. Navegue até a guia **Orchestration** no Intersight.
5. Selecione **criar fluxo de trabalho**.
6. Adicione tarefas de armazenamento e virtualização aos seus fluxos de trabalho.

   Aqui estão as tarefas de storage do NetApp disponíveis no Cisco Intersight:

   - Adicione ACL ao compartilhamento CIFS do NetApp
   - Adicionar correspondência de cliente à regra de política de exportação do NetApp
   - Adicionar política de exportação ao volume NetApp
   - Adicione iniciadores ao Grupo de iniciadores do NetApp
   - Adicionar regra à Política de exportação do NetApp
   - Adicionar Agendamento à Política de instantâneos do NetApp
   - Confirme o status da licença do NetApp
   - Confirmar o status do protocolo FCP da máquina virtual de storage NetApp
   - Editar agregados NetApp para máquina virtual de storage
   - Editar a política de SnapMirror assíncrona do NetApp
   - Editar permissão de compartilhamento de NetApp CIFS
   - Editar regra de política de exportação do NetApp

- Editar política de instantâneos do NetApp
- Editar Programa de políticas de instantâneos do NetApp
- Editar estilo de segurança de volume do NetApp
- Editar política de instantâneo de volume do NetApp
- Ative os serviços CIFS do NetApp
- Expanda NetApp LUN
- Nova política de SnapMirror assíncrona da NetApp
- Novo servidor CIFS NetApp
- Novo compartilhamento NetApp CIFS
- Encontre o mapa LUN do Grupo iniciador NetApp
- Encontrar LUN NetApp por ID
- Encontrar volume NetApp por ID
- Nova Política de exportação do NetApp
- Nova interface de dados NetApp FC
- Novo Grupo de Iniciadores do NetApp
- Nova interface de dados iSCSI NetApp
- Novos espelhos de compartilhamento de carga do NetApp para volume raiz da SVM
- Novo LUN NetApp
- Novo mapa LUN NetApp
- Nova interface de dados NetApp nas
- Novo NetApp nas Smart volume
- Novo LUN inteligente NetApp
- Nova relação NetApp SnapMirror para volume
- Nova Política de snapshot do NetApp
- Nova máquina virtual de storage NetApp
- Novo volume NetApp
- Novo Snapshot de volume do NetApp
- Registre o DNS para a Máquina Virtual de armazenamento NetApp
- Remova a ACL do compartilhamento CIFS do NetApp
- Remover correspondência Cliente da regra de Política de exportação do NetApp
- Remover a política de exportação do volume NetApp
- Remova o Iniciador do Grupo Iniciador do NetApp
- Remova o servidor CIFS do NetApp
- Remova o compartilhamento CIFS do NetApp
- Remova a Política de exportação do NetApp
- Remova a interface de dados NetApp FC
- Remova o Grupo Iniciador do NetApp

- Remova a interface IP do NetApp
- Remova os espelhos de compartilhamento de carga do NetApp para o volume raiz da SVM
- Remova o LUN NetApp
- Remover mapa LUN NetApp
- Remova o NetApp nas Smart volume
- Remova o NetApp Smart LUN
- Remover relação NetApp SnapMirror para volume
- Remova a Política de NetApp SnapMirror
- Remover a Política de instantâneos do NetApp
- Remova a máquina virtual de storage do NetApp
- Remover volume NetApp
- Remover instantâneo do volume do NetApp
- Remover regra da Política de exportação do NetApp
- Remover Programa da Política de instantâneos do NetApp
- Renomear captura Instantânea de volume do NetApp
- Atualize os espelhos de compartilhamento de carga do NetApp para volume raiz da SVM
- Atualizar a capacidade de volume do NetApp

Infraestrutura

NVMe completo para FlexPod com Cisco CSM, VMware vSphere 7,0 e NetApp ONTAP 9

TR-4914: NVMe completo para FlexPod com Cisco UCSM, VMware vSphere 7,0 e NetApp ONTAP 9

Chris Schmitt e Kamini Singh, NetApp

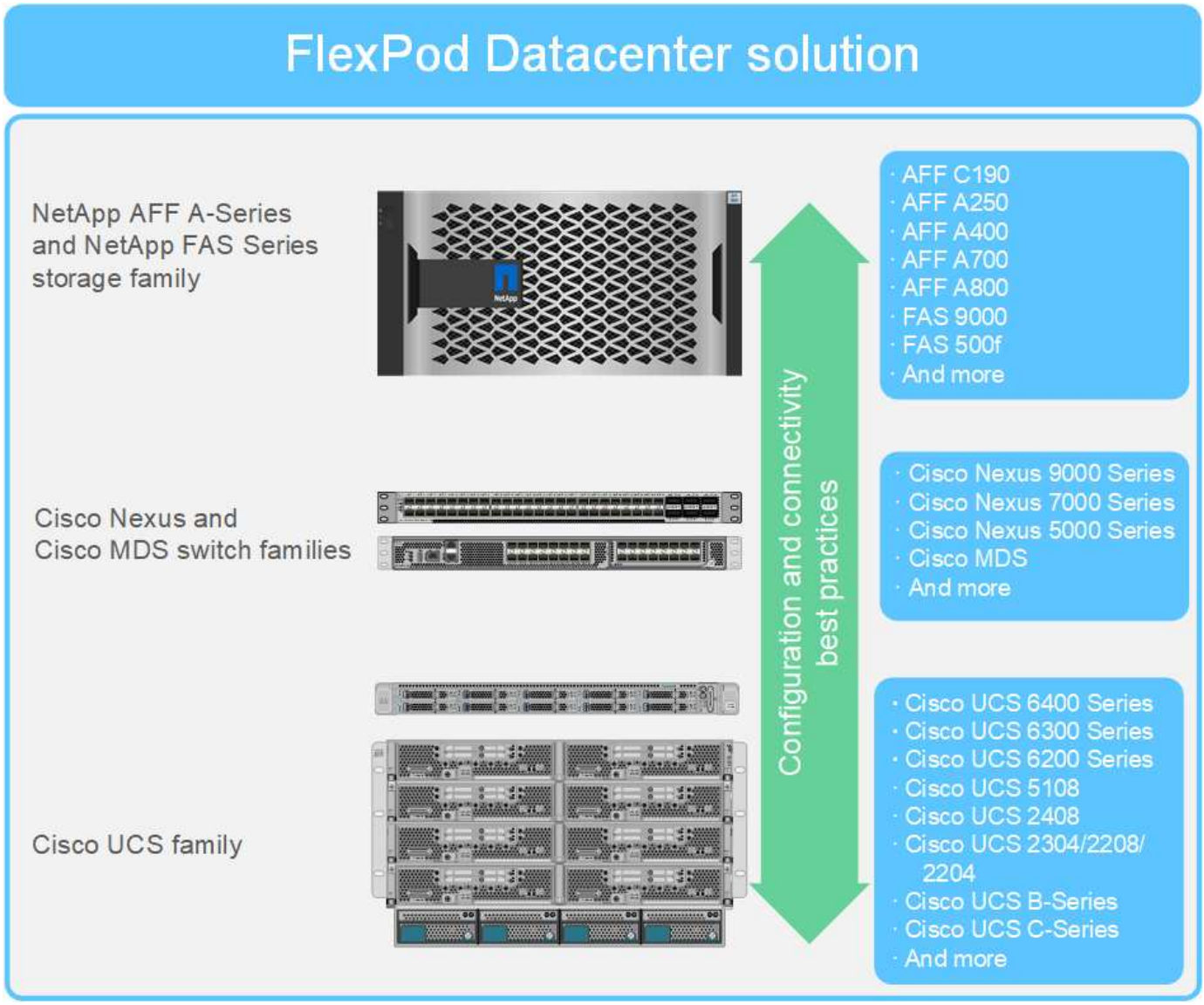
Em parceria com: 

O padrão de storage de dados NVMe, uma nova tecnologia central, está transformando o acesso e o transporte ao storage empresarial, fornecendo largura de banda muito alta e acesso ao storage de latência muito baixa para tecnologias de memória atuais e futuras. O NVMe substitui o conjunto de comandos SCSI pelo conjunto de comandos NVMe.

O NVMe foi projetado para funcionar com unidades flash não voláteis, CPUs multicore e gigabytes de memória. Ele também aproveita os avanços significativos na ciência da computação desde a década de 1970s, permitindo conjuntos de comandos simplificados que analisam e manipulam dados com mais eficiência. Uma arquitetura NVMe completa também permite que os administradores de data center repensem em até que ponto eles podem empurrar seus ambientes virtualizados e em contêiner, bem como a quantidade de escalabilidade que seus bancos de dados orientados a transações podem suportar.

O FlexPod é uma arquitetura de data center com práticas recomendadas que inclui o sistema de computação unificada da Cisco (Cisco UCS), os switches Cisco Nexus, os switches Cisco MDS e os sistemas NetApp AFF. Esses componentes são conectados e configurados de acordo com as práticas recomendadas do Cisco e do NetApp para fornecer uma excelente plataforma para executar uma variedade de workloads empresariais com confiança. O FlexPod pode fazer escalabilidade vertical para aumentar a performance e a capacidade (adicionando recursos de computação, rede ou storage individualmente conforme necessário) ou fazer escalabilidade horizontal para ambientes que exigem várias implantações consistentes (como a implementação de pilhas FlexPod adicionais).

A figura a seguir apresenta as famílias de componentes FlexPod.



O FlexPod é a plataforma ideal para apresentar o FC-NVMe. Ele pode ser compatível com a adição do Cisco UCS VIC 1400 Series e expansor de portas em servidores Cisco UCS B200 M5 ou M6 existentes ou servidores em rack Cisco UCS C-Series M5 ou M6 e atualizações de software simples e sem interrupções para o sistema Cisco UCS, os switches Cisco MDS 32Gbps e os storage arrays NetApp AFF. Depois que o hardware e o software com suporte estiverem em vigor, a configuração do FC-NVMe será semelhante à configuração FCP.

O NetApp ONTAP 9.5 e posteriores fornecem uma solução FC-NVMe completa. Uma atualização de software ONTAP sem interrupções para arrays AFF A300, AFF A400, AFF A700, AFF A700s e AFF A800 permite que esses dispositivos ofereçam suporte a uma pilha de storage NVMe completa. Portanto, servidores com adaptadores de barramento de host (HBAs) de sexta geração e suporte a driver NVMe podem se comunicar com esses arrays usando NVMe nativo.

Objetivo

Essa solução fornece um resumo de alto nível da performance de FC-NVMe com o VMware vSphere 7 no FlexPod. A solução foi verificada para passar com sucesso no tráfego FC-NVMe, e as metrices de desempenho foram capturadas para FC-NVMe com vários tamanhos de bloco de dados.

Benefícios da solução

O NVMe completo para FlexPod fornece valor excepcional para os clientes com os seguintes benefícios da solução:

- O NVMe conta com PCIe, um protocolo de hardware de alta velocidade e alta largura de banda que é substancialmente mais rápido do que os padrões mais antigos, como SCSI, SAS e SATA. Conetividade de latência ultrabaixa e alta largura de banda entre o servidor UCS Cisco e o storage array NetApp para a maioria dos aplicativos exigentes.
- Uma solução FC-NVMe é sem perda e pode lidar com os requisitos de escalabilidade das aplicações de nova geração. Essas novas tecnologias incluem inteligência artificial (AI), aprendizado de máquina (ML), aprendizado profundo (DL), análises em tempo real e outras aplicações essenciais.
- Reduz o custo DA TI ao usar todos os recursos DE forma eficiente em toda a pilha.
- Reduz significativamente os tempos de resposta e aumenta o desempenho da aplicação, o que corresponde a IOPS e taxa de transferência aprimorados com latência reduzida. A solução 60 aumenta a performance e reduz a latência em cerca de 50% para os workloads atuais.
- O FC-NVMe é um protocolo otimizado com excelentes funcionalidades de fila, principalmente em situações com mais operações de e/S por segundo (IOPS; ou seja, mais transações) e atividades paralelas.
- Oferece atualizações de software sem interrupções nos componentes do FlexPod, como o Cisco UCS, o Cisco MDS e os storage arrays NetApp AFF. Não requer nenhuma modificação para aplicações.

"Próximo: Abordagem de teste."

Abordagem de teste

"Anterior: Introdução."

Esta seção fornece um resumo de alto nível do FC-NVMe no teste de validação do FlexPod. Ele inclui o ambiente de teste/configuração e o plano de teste adotado para realizar os testes de workload com relação ao FC-NVMe para FlexPod com VMware vSphere 7.

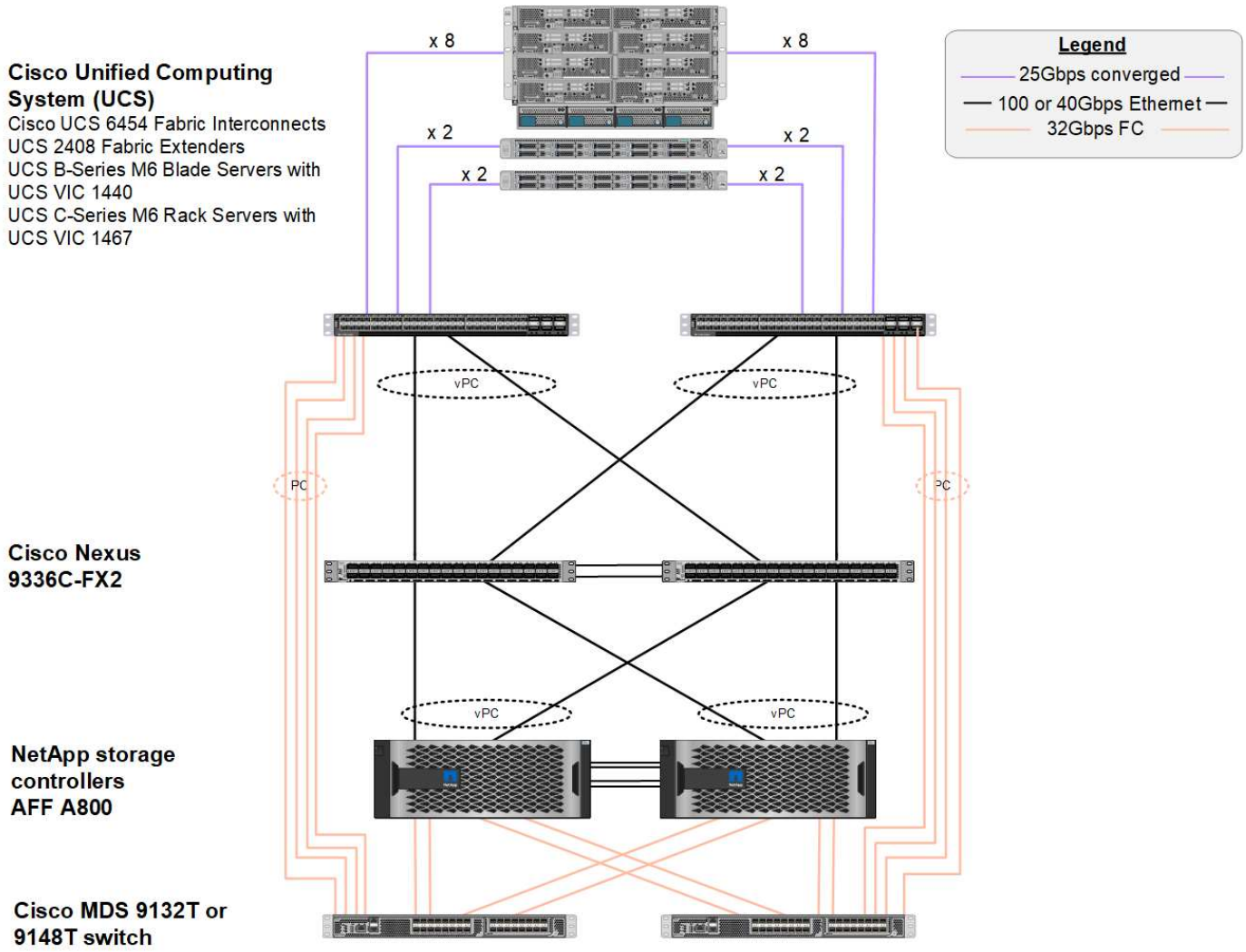
Ambiente de teste

Os switches da série Nexus 9000 da Cisco suportam dois modos de operação:

- Modo autónomo NX-os, utilizando o software Cisco NX-os
- Modo ACI Fabric, usando a plataforma Cisco Application Centric Infrastructure (Cisco ACI)

No modo autônomo, o switch funciona como um switch Cisco Nexus típico, com maior densidade de porta, baixa latência e conectividade 40GbE GbE e 100GbE GbE.

O FlexPod com NX-os foi projetado para ser totalmente redundante nas camadas de computação, rede e armazenamento. Não há um único ponto de falha a partir de um dispositivo ou do ponto de vista do caminho de tráfego. A figura abaixo mostra a conexão dos vários elementos do design FlexPod mais recente usado nessa validação do FC-NVMe.



Do ponto de vista da SAN FC, esse projeto usa as mais recentes interconexões de malha Cisco UCS 6454 de quarta geração e a plataforma Cisco UCS VICS 1400 com expansor de porta nos servidores. Os servidores blade Cisco UCS B200 M6 no chassi do Cisco UCS usam o Cisco UCS VIC 1440 com expansor de porta conetado ao Cisco UCS 2408 Fabric Extender IOM, e cada adaptador de barramento de host virtual (vHBA) de canal de fibra (Fibre Channel over Ethernet) tem uma velocidade de 40GbpsGbps. Os servidores em rack Cisco UCS C220 M5 gerenciados pelo Cisco UCS usam o Cisco UCS VIC 1457 com duas interfaces 25Gbps para cada interconexão de malha. Cada vHBA FCoE C220 M5 tem uma velocidade de 50Gbps.

A malha interconecta-se por meio de 32Gbps canais de porta SAN aos switches Cisco MDS 9148T ou FC de 9132T GB de última geração. A conectividade entre os switches MDS do Cisco e o cluster de storage do NetApp AFF A800 também é de 32Gbps GB FC. Essa configuração é compatível com FC de 32Gbps GB, para Fibre Channel Protocol (FCP) e storage FC-NVMe entre o cluster de storage e o Cisco UCS. Para essa validação, quatro conexões FC a cada controlador de storage são usadas. Em cada controlador de storage, as quatro portas FC são usadas nos protocolos FCP e FC-NVMe.

A conetividade entre os switches Cisco Nexus e o cluster de armazenamento NetApp AFF A800 de última geração também é de 100Gbps GB com canais de porta nos controladores de armazenamento e VPCs nos switches. As controladoras de storage NetApp AFF A800 são equipadas com discos NVMe no barramento PCIe (PCIe) de interface de conexão periférica de alta velocidade.

A implementação do FlexPod usada nesta validação é baseada "FlexPod Datacenter com Cisco UCS 4,2(1) no modo gerenciado UCS, VMware vSphere 7.0U2 e NetApp ONTAP 9.9" no .

Hardware e software validados

A tabela a seguir lista as versões de hardware e software usadas durante o processo de validação da solução. Observe que o Cisco e o NetApp têm matrizes de interoperabilidade que devem ser referenciadas para determinar o suporte para qualquer implementação específica do FlexPod. Para obter mais informações, consulte os seguintes recursos:

- "Ferramenta de Matriz de interoperabilidade do NetApp"
- "Ferramenta de interoperabilidade de hardware e software Cisco UCS"

Camada	Dispositivo	Imagem	Comentários
Computação	• Duas interconexões de tecido Cisco UCS 6454 • Um chassi blade Cisco UCS 5108 com dois módulos de e/S Cisco UCS 2408 • Quatro blades Cisco UCS B200 M6, cada um com um adaptador Cisco UCS VIC 1440 e placa de expansão de porta	Lançamento 4,2(1f)	Inclui o Cisco UCS Manager, o Cisco UCS VIC 1440 e o expansor de portas
CPU	Duas CPUs Intel Xeon Gold 6330 de 2,0 GHz, com cache de camada 3 de 42 MB e 28 núcleos por CPU	–	–
Memória	1024GB (16x 64GB DIMMS operando a 3200MHz MHz)	–	–
Rede	Dois switches Cisco Nexus 9336C-FX2 em modo autônomo NX-os	Lançamento 9,3(8)	–
Rede de armazenamento	Dois switches Cisco MDS FC de 9132T 32Gbps 32 portas	Lançamento 8,4(2c)	É compatível com análises SAN FC-NVMe
Armazenamento	Duas controladoras de storage NetApp AFF A800 com 24x 1,8TB SSDs NVMe	NetApp ONTAP 9.9.1P1	–
Software	Gerente do Cisco UCS	Lançamento 4,2(1f)	–
	VMware vSphere	7.0U2	–
	VMware ESXi	7.0.2	–

Camada	Dispositivo	Imagem	Comentários
	Driver de NIC Fibre Channel nativo do VMware ESXi (NFNIC)	5.0.0.12	Compatível com FC-NVMe no VMware
	Driver de NIC Ethernet nativo do VMware ESXi (NENIC)	1.0.35.0	–
Ferramenta de teste	FIO	3,19	–

Plano de teste

Desenvolvemos um plano de teste de desempenho para validar o NVMe no FlexPod com um workload sintético. Essa carga de trabalho nos permitiu executar 8KB leituras e gravações aleatórias, bem como 64KB leituras e gravações. Usamos os hosts do VMware ESXi para executar nossos casos de teste em relação ao storage do AFF A800.

Usamos fio, uma ferramenta de e/S sintética de código aberto que pode ser usada para medição de desempenho, para gerar nossa carga de trabalho sintética.

Para concluir nossos testes de desempenho, realizamos várias etapas de configuração tanto no storage quanto nos servidores. Abaixo estão as etapas detalhadas para a implementação:

1. No lado do storage, criamos quatro máquinas virtuais de storage (SVMs, anteriormente conhecidas como VServers), oito volumes por SVM e um namespace por volume. Criamos 1TB volumes e 960GB namespaces. Criamos quatro LIFs por SVM e um subsistema por SVM. Os LIFs do SVM foram distribuídos uniformemente pelas oito portas FC disponíveis no cluster.
2. No lado do servidor, criamos uma única máquina virtual (VM) em cada um dos nossos hosts ESXi, para um total de quatro VMs. Instalamos o fio em nossos servidores para executar as cargas de trabalho sintéticas.
3. Depois que o armazenamento e as VMs foram configurados, conseguimos nos conetar aos namespaces de armazenamento dos hosts ESXi. Isso nos permitiu criar datastores com base em nosso namespace e, em seguida, criar VMDKs (Virtual Machine Disks) com base nesses datastores.

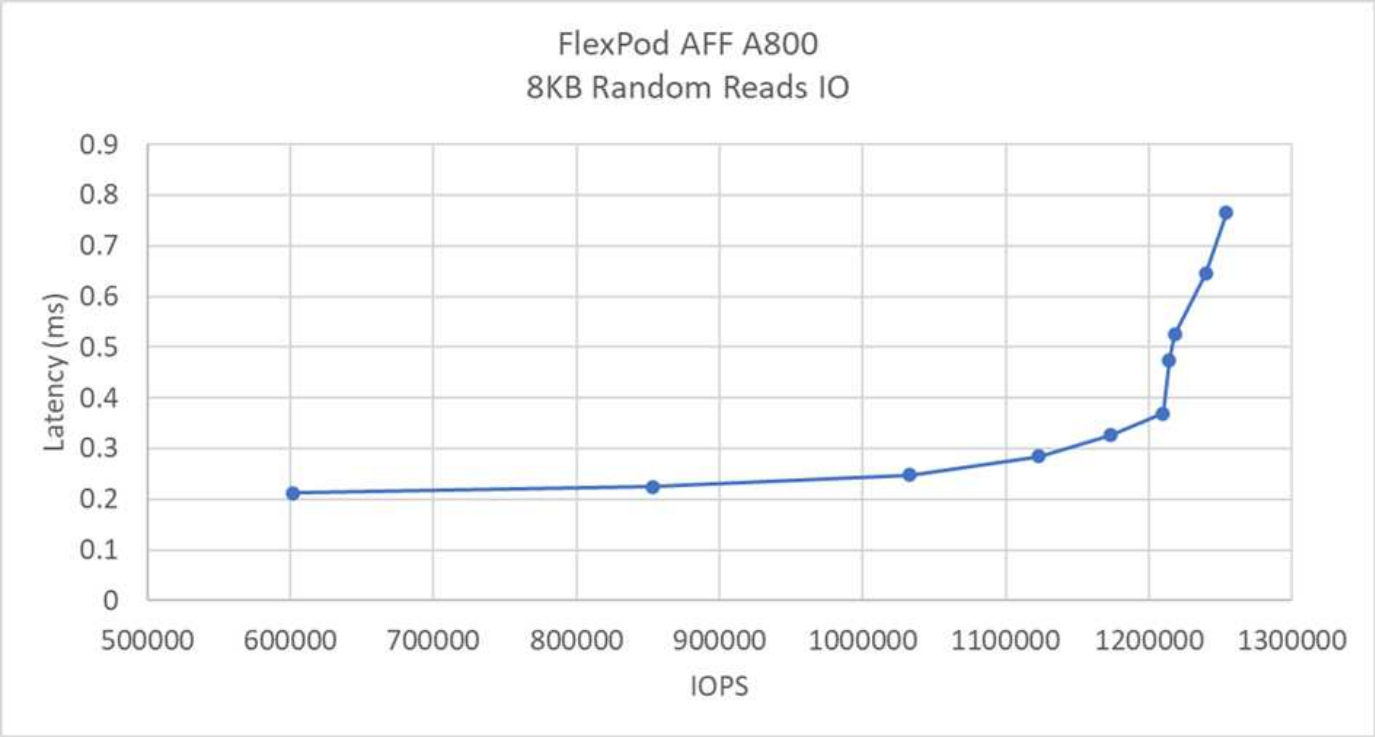
"Próximo: Resultados do teste."

Resultados do teste

"Anterior: Abordagem de teste."

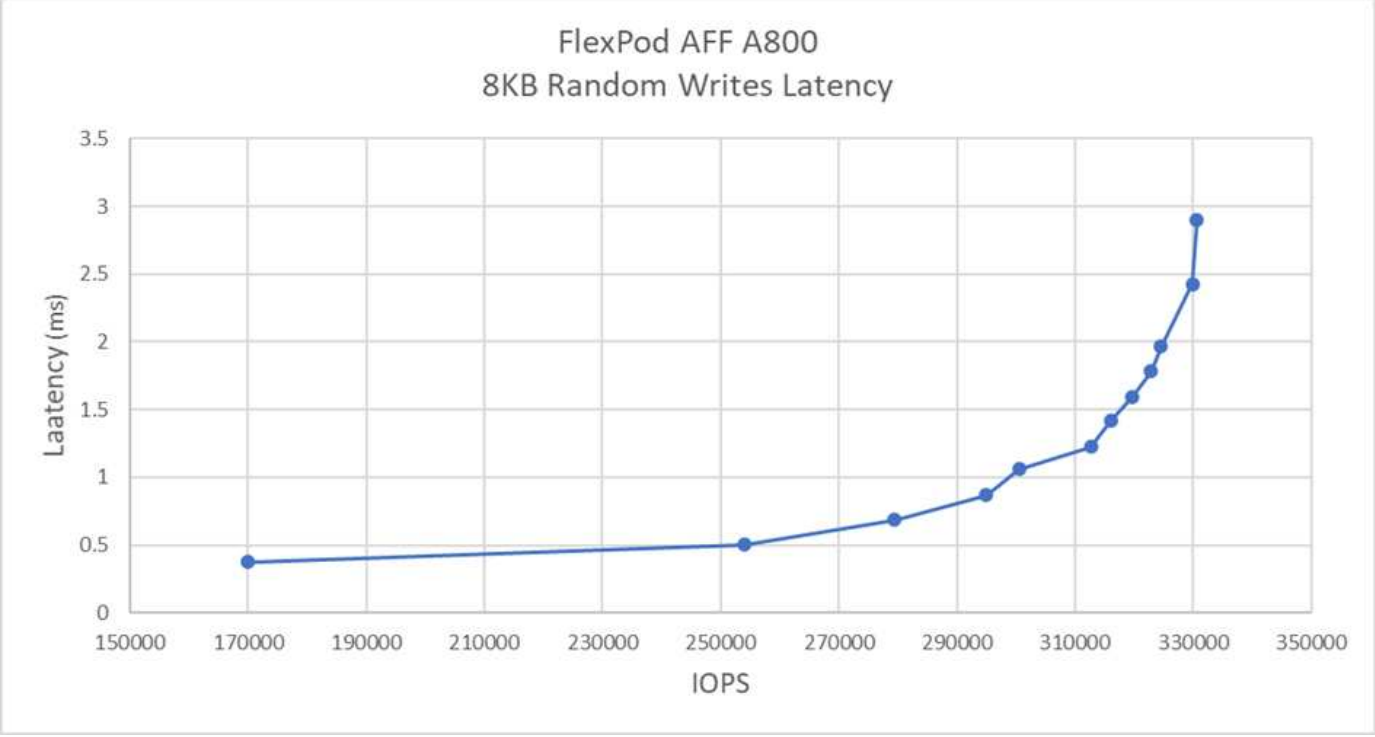
Os testes consistiram na execução de workloads FIO para medir o desempenho de FC-NVMe em termos de IOPS e latência.

O gráfico a seguir ilustra nossas descobertas ao executar uma carga de trabalho de leitura aleatória de 100% usando 8KB tamanhos de bloco.



Em nossos testes, descobrimos que o sistema alcançou mais de 1,2M IOPS enquanto mantinha pouco menos de 0,35ms ms de latência no lado do servidor.

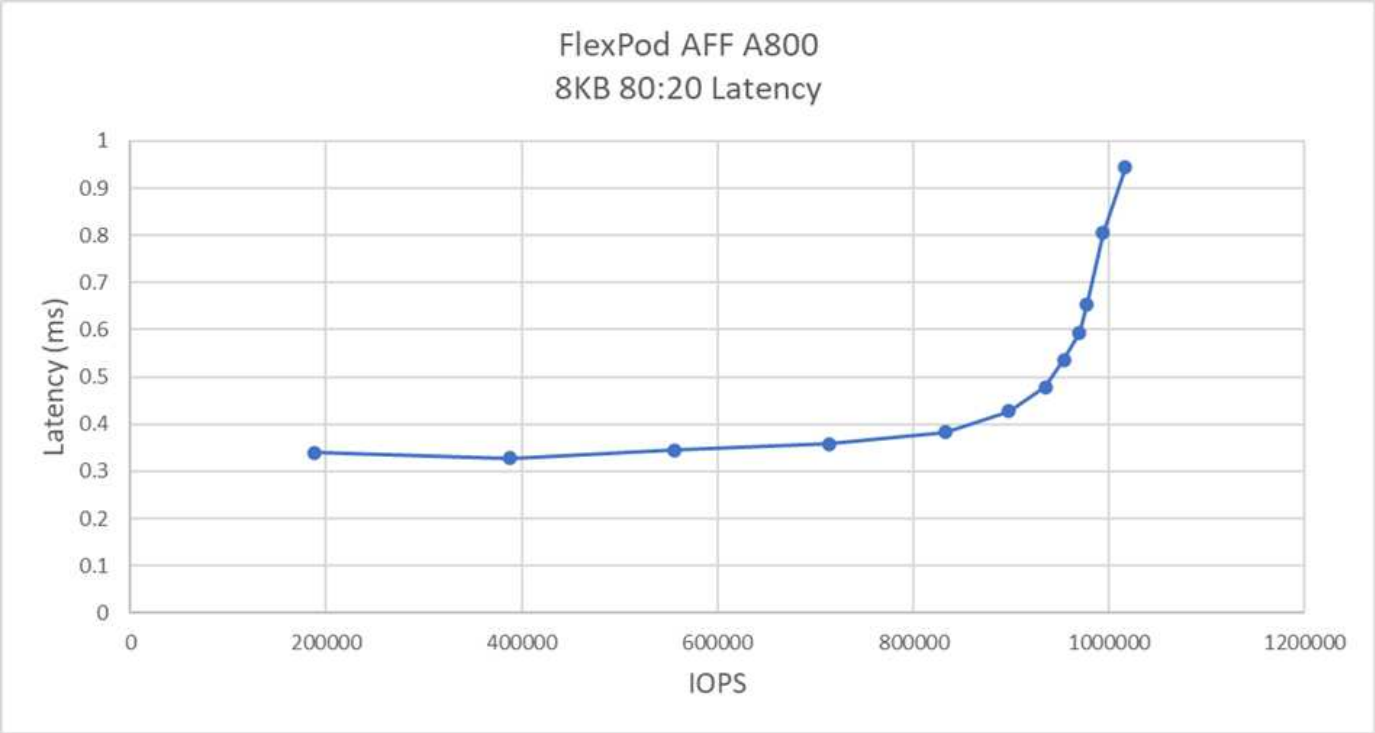
O gráfico a seguir ilustra nossas descobertas ao executar uma carga de trabalho de gravação aleatória de 100% usando 8KB tamanhos de bloco.



Em nossos testes, descobrimos que o sistema alcançou perto de 300k IOPS, mantendo pouco menos de 1ms ms de latência no lado do servidor.

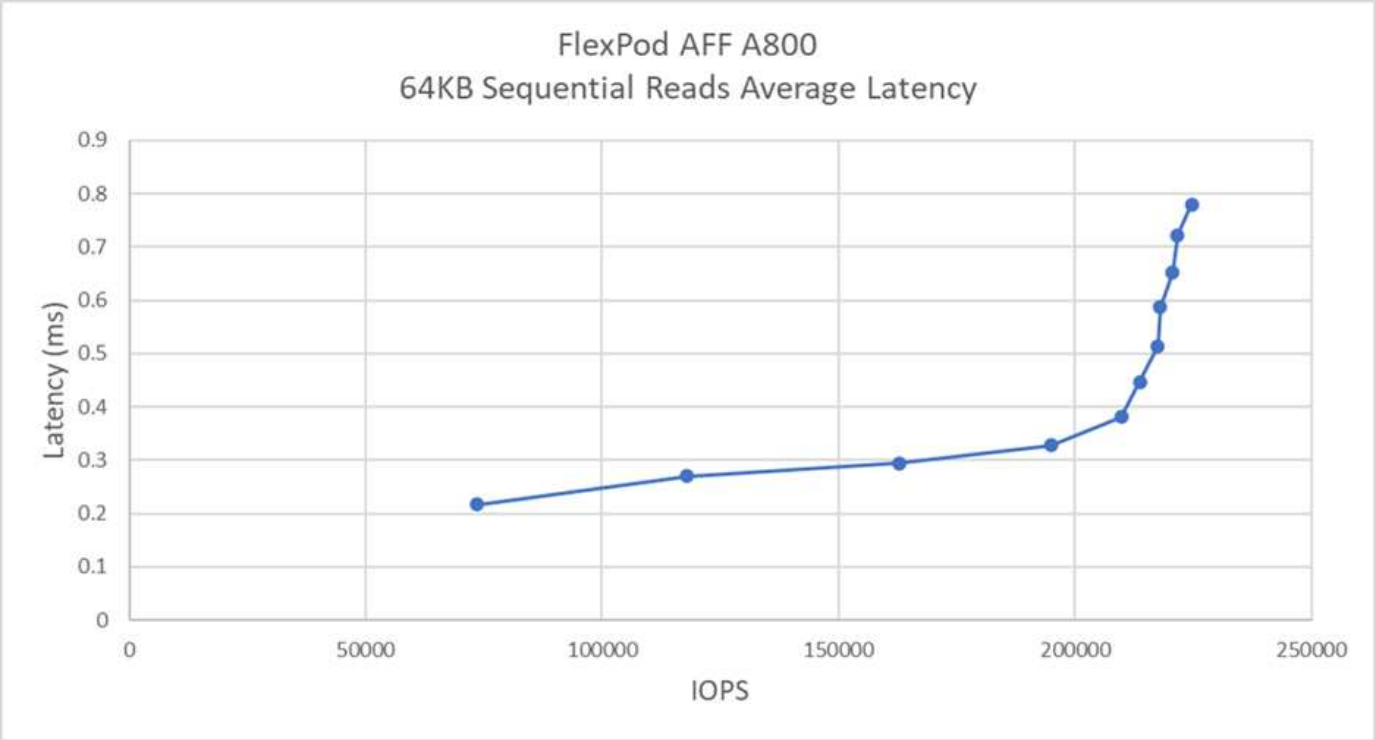
Para o tamanho de bloco 8KB com 80% de leituras aleatórias e 20% de gravações, observamos os seguintes

resultados:



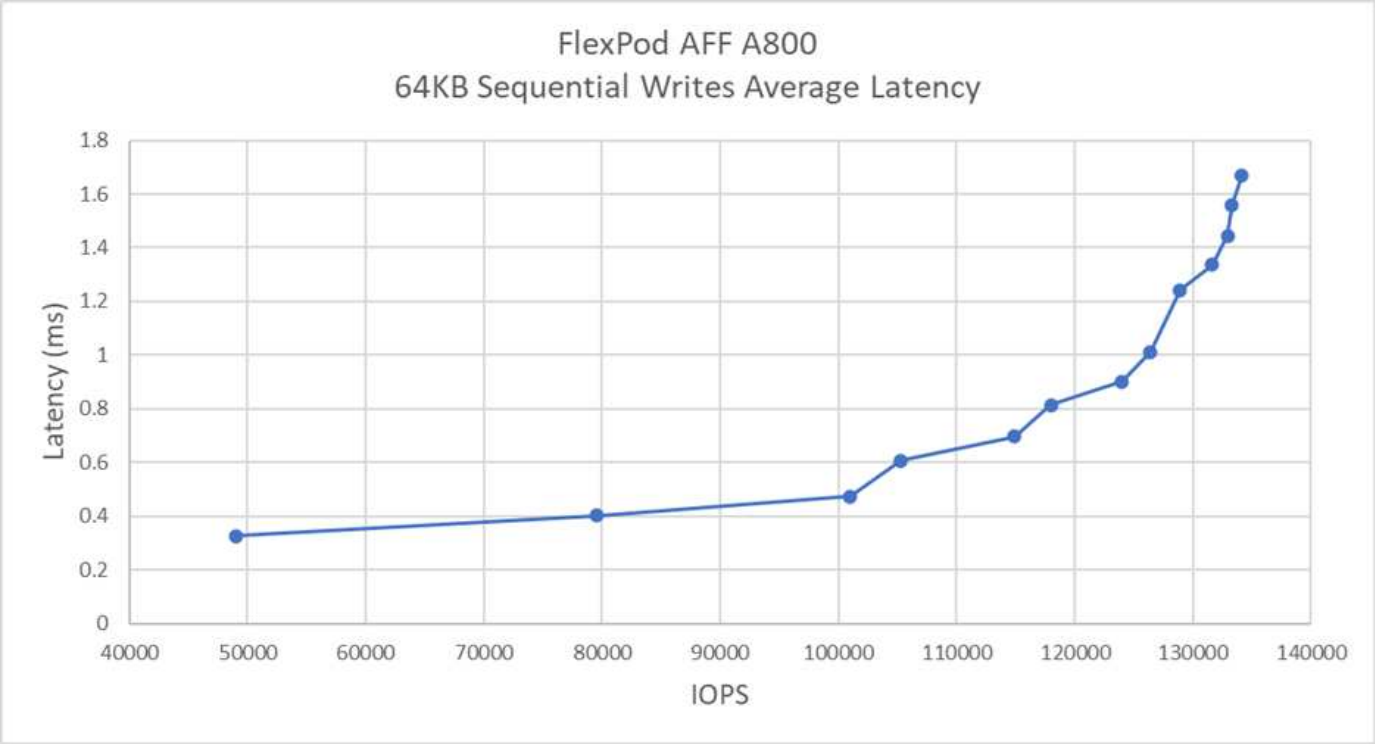
Em nossos testes, descobrimos que o sistema alcançou mais de 1M IOPS enquanto mantinha pouco menos de 1ms ms de latência no lado do servidor.

Para o tamanho de bloco 64KB e leituras sequenciais de 100%, foram observados os seguintes resultados:



Em nossos testes, descobrimos que o sistema alcançou cerca de 250k IOPS, mantendo pouco menos de 1ms ms de latência no lado do servidor.

Para o tamanho de bloco 64KB e 100% de gravações sequenciais, observamos os seguintes resultados:



Em nossos testes, descobrimos que o sistema alcançou cerca de 120k IOPS, mantendo menos de 1ms ms de latência no lado do servidor.

"Próximo: Conclusão."

Conclusão

"Anterior: Resultados do teste."

O throughput observado para essa solução foi de 14GBps e 220K IOPS para uma carga de trabalho de leitura sequencial com latência inferior a 1ms ms. Para workloads de leitura aleatória, chegamos a uma taxa de transferência de 9,5GBps Gbps e 1,25M IOPS. A capacidade do FlexPod de fornecer essa performance com FC-NVMe pode atender às necessidades de qualquer aplicação de missão crítica.

O FlexPod Datacenter com VMware vSphere 7,0 U2 é a base ideal de infraestrutura compartilhada para implantar o FC-NVMe em diversos workloads DE TI, fornecendo acesso de storage de alta performance às aplicações que o exigem. À medida que o FC-NVMe evolui para incluir suporte a alta disponibilidade, multipathing e sistemas operacionais adicionais, o FlexPod é adequado como a plataforma escolhida, fornecendo a escalabilidade e a confiabilidade necessárias para dar suporte a esses recursos.

Com o FlexPod, a Cisco e a NetApp criaram uma plataforma flexível e escalável para vários casos de uso e aplicativos. Com o FC-NVMe, o FlexPod adiciona outro recurso para ajudar as organizações a dar suporte eficiente e eficaz a aplicações essenciais aos negócios executadas simultaneamente a partir da mesma infraestrutura compartilhada. A flexibilidade e a escalabilidade do FlexPod também permitem que os clientes comecem com uma infraestrutura de tamanho certo que pode crescer e se adaptar às mudanças nos requisitos de negócios.

Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Sistema de computação unificada da Cisco (UCS)

  "http://www.cisco.com/en/US/products/ps10265/index.html"

- Cisco UCS 6400 Series Fabric interconecta a ficha de dados

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html"

- Chassi do servidor blade da série Cisco UCS 5100

  "http://www.cisco.com/en/US/products/ps10279/index.html"

- Servidores blade Cisco UCS B-Series

  "http://www.cisco.com/en/US/partner/products/ps10280/index.html"

- Servidores em rack Cisco UCS C-Series

  "http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html"

- Adaptadores de sistema de computação unificada da Cisco

  "http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html"

- Gerente do Cisco UCS

  "http://www.cisco.com/en/US/products/ps10281/index.html"

- Switches Cisco Nexus 9000 Series

  "http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html"

- Switches de malha multicamadas Cisco MDS 9000

  "http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html"

- Comutador de canal de fibra de 32 portas Cisco MDS de 9132T 32 Gbps

  "https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html"

- NetApp ONTAP 9

  "http://www.netapp.com/us/products/platform-os/ontap/index.aspx"

- NetApp AFF Série A.

  "http://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx"

- VMware vSphere

"https://www.vmware.com/products/vsphere"

- VMware vCenter Server

  "http://www.vmware.com/products/vcenter-server/overview.html"

- Práticas recomendadas para SAN moderna

  "https://www.netapp.com/us/media/tr-4080.pdf"

- Apresentação do NVMe completo para FlexPod

  "https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-741907.html"

Matrizes de interoperabilidade

- Ferramenta de Matriz de interoperabilidade do NetApp

  "http://support.netapp.com/matrix/"

- Matriz de compatibilidade de hardware Cisco UCS

  "https://ucshcltool.cloudapps.cisco.com/public/"

- Guia de compatibilidade da VMware

  "http://www.vmware.com/resources/compatibility"

Agradecimentos

Os autores gostariam de agradecer a John George de Cisco e Scott Lane e Bobby Oommen de NetApp pela assistência e orientação oferecida durante a execução deste projeto.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos de autor

http://www.netapp.com/us/legal/copyright.aspx

Marcas comerciais

NetApp, o logotipo DA NetApp e as marcas listadas na página de marcas comerciais da NetApp são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respetivos proprietários.

http://www.netapp.com/us/legal/netapptmlist.aspx

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/us/media/patents-page.pdf

Política de privacidade

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Informações sobre direitos autorais

Informações sobre marcas comerciais