VMware Cloud Foundation na NetApp

NetApp virtualization solutions

NetApp
August 24, 2025

This PDF was generated from https://docs.netapp.com/pt-br/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html on August 24, 2025. Always check docs.netapp.com for the latest.

Índice

VMware Cloud Foundation na NetApp . . . 1
- Simplifique a experiência de nuvem híbrida com VMware Cloud Foundation e ONTAP . . . 1
- Introdução . . . 1
  - Introdução ao NetApp ONTAP . . . 1
  - Introdução ao VMware Cloud Foundation . . . 1
  - Domínios VCF . . . 2
  - Armazenamento com VCF . . . 3
  - Por que ONTAP para VCF . . . 3
  - Informações adicionais: . . . 4
  - Resumo . . . 5
  - Recursos de documentação . . . 5
- Opções de design com VMware Cloud Foundation e ONTAP . . . 6
  - Opções de armazenamento . . . 6
  - Projetos . . . 7
- Configure ambientes de nuvem privada com VMware Cloud Foundation e ONTAP . . . 10
  - Implantar uma nova instância do VCF 9 . . . 11
  - Convergir componentes existentes no VCF 9 . . . 12
  - Atualizar um ambiente VCF existente para VCF 9 . . . 13
- Implementando recuperação de desastres com NetApp SnapMirror e BlueXP DRaaS . . . 13
  - Começando . . . 15
  - Configuração de BlueXP disaster recovery . . . 16
  - Configurando a replicação de armazenamento entre a matriz do site de origem e a matriz do site de destino . . . 17
  - Como configurá-lo para recuperação de desastres do VMware . . . 17
  - O que a BlueXP disaster recovery pode fazer por você? . . . 18
  - Teste de failover . . . 23
  - Operação de teste de failover de limpeza . . . 25
  - Migração planejada e failover . . . 26
  - Failback . . . 27
  - Monitoramento e Painel . . . 29
- Converter clusters vSphere existentes em VCF . . . 30
  - Saiba mais sobre como converter um ambiente vSphere com armazenamentos de dados existentes para VCF . . . 30
  - Converter instância do servidor vCenter em domínio de gerenciamento VCF (armazenamento de dados NFS) . . . 30
  - Converter instância do servidor vCenter em domínio de gerenciamento VCF (armazenamento de dados FC) . . . 44
- Provisionar VCF com armazenamento principal . . . 58
  - Provisione um ambiente VCF com ONTAP como a principal solução de armazenamento . . . 58
  - Use um armazenamento de dados VMFS baseado em FC no ONTAP como armazenamento principal para o domínio de gerenciamento VCF . . . 58
  - Use um armazenamento de dados NFS no ONTAP como armazenamento principal para o domínio de gerenciamento VCF . . . 60

Use um armazenamento de dados VMFS baseado em FC no ONTAP como armazenamento principal para um domínio de carga de trabalho VI . . . 61
Use um armazenamento de dados NFS no ONTAP como armazenamento principal para um domínio de carga de trabalho VI . . . 63
Expanda o VCF com armazenamento suplementar . . . 84
Aprenda sobre como expandir o armazenamento para um ambiente VCF usando armazenamento suplementar . . . 84
Adicione um armazenamento de dados iSCSI como armazenamento suplementar para um domínio de gerenciamento usando ONTAP tools for VMware vSphere . . . 84
Adicionar um armazenamento de dados VMFS baseado em FC como armazenamento suplementar para um domínio de gerenciamento usando ONTAP tools for VMware vSphere . . . 108
Adicione vVols como armazenamento suplementar aos domínios de carga de trabalho VI usando ONTAP tools for VMware vSphere . . . 109
Adicione NFS e vVols como armazenamento suplementar aos domínios de carga de trabalho VI usando ONTAP tools for VMware vSphere . . . 136
Adicionar NVMe sobre TCP como armazenamento suplementar aos domínios de carga de trabalho do VI . . . 161
Adicionar um armazenamento de dados VMFS baseado em FC como armazenamento suplementar aos domínios de carga de trabalho do VI . . . 185
Proteja o VCF com o SnapCenter . . . 186
Aprenda a proteger domínios de carga de trabalho VCF com o plug-in SnapCenter para VMware vSphere . . . 186
Proteja um domínio de carga de trabalho VCF com o plug-in SnapCenter para VMware vSphere . . . 187
Proteja os domínios de gerenciamento e carga de trabalho do VCF usando o plug-in SnapCenter para VMware vSphere . . . 222
Proteja domínios de carga de trabalho VCF com armazenamento NVMe sobre TCP e plug-in SnapCenter para VMware vSphere . . . 235
Proteja os datastores VMware com BlueXP . . . 242
Saiba mais sobre como proteger os datastores VMware usando a BlueXP disaster recovery . . . 242
Configurar a proteção de dados 3-2-1 para VMware com o plug-in SnapCenter para BlueXP backup and recovery . . . 242
Configurar recuperação de desastres para datastores VMFS usando a BlueXP disaster recovery . . . 287
Configurar recuperação de desastres para armazenamentos de dados NFS usando a BlueXP disaster recovery . . . 306
Proteja as cargas de trabalho com o vSphere Metro Storage Cluster . . . 327
Saiba mais sobre a integração de alta disponibilidade do ONTAP com o VMware vSphere Metro Storage Cluster (vMSC) . . . 327
Configurar um cluster de extensão para um domínio de gerenciamento VCF usando o MetroCluster . . . 328
Configurar um cluster de extensão para um domínio de carga de trabalho VI usando o MetroCluster . . . 339
Configurar um cluster de extensão para um domínio de gerenciamento VCF usando o SnapMirror Active Sync . . . 351
Configurar um cluster de extensão para um domínio de carga de trabalho de VI usando o SnapMirror Active Sync . . . 353
Migrar VMs do VMware vSphere para datastores ONTAP . . . 355
Requisitos de rede . . . 356

Cenários de migração de VM . . . 358
Cenários de migração de modelo de VM . . . 382
Casos de uso . . . 390
Recursos adicionais . . . 391
Proteção autônoma contra ransomware para armazenamento NFS . . . 391
Monitore o armazenamento local com o Data Infrastructure Insights . . . 401
Monitoramento de armazenamento local com Data Infrastructure Insights . . . 401
Visão geral da implantação da solução . . . 401
Pré-requisitos . . . 402
Implantação de solução . . . 402
Conclusão . . . 419
Informações adicionais . . . 419

VMware Cloud Foundation na NetApp

Simplifique a experiência de nuvem híbrida com VMware Cloud Foundation e ONTAP

O NetApp ONTAP integra-se ao VMware Cloud Foundation (VCF) para fornecer uma solução de armazenamento unificada com suporte a protocolos de bloco e de arquivo. Essa integração simplifica implantações de nuvem híbrida, melhora o gerenciamento e o desempenho de dados e garante serviços de dados consistentes em ambientes locais e na nuvem.

Introdução

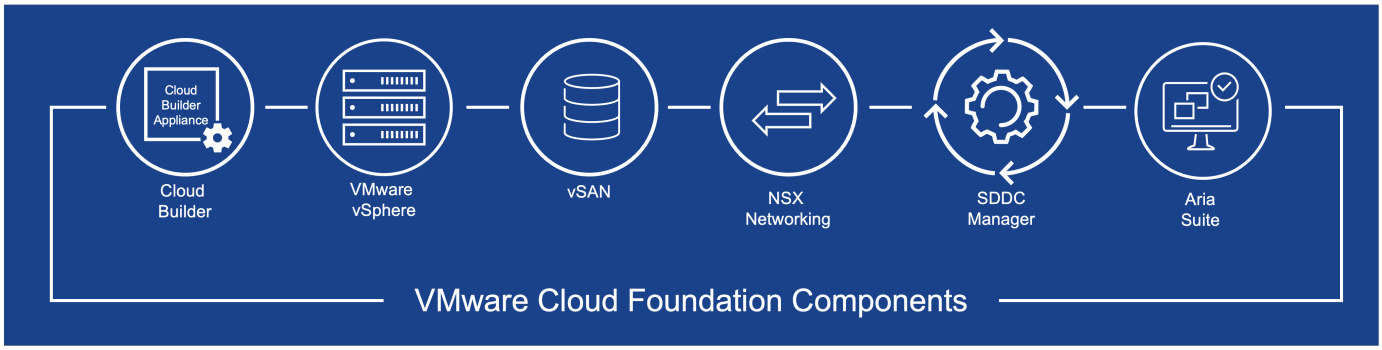
Usar o NetApp com VCF melhora o gerenciamento de dados e a eficiência de armazenamento por meio de recursos avançados do NetApp, como desduplicação, compactação e snapshots. Essa combinação proporciona integração perfeita, alto desempenho e escalabilidade para ambientes virtualizados. Além disso, ele simplifica as implantações de nuvem híbrida ao permitir serviços de dados e gerenciamento consistentes em infraestruturas locais e na nuvem.

Introdução ao NetApp ONTAP

O NetApp ONTAP é um software abrangente de gerenciamento de dados que oferece recursos avançados de armazenamento em uma ampla linha de produtos. O ONTAP está disponível como armazenamento definido por software, como um serviço primário por meio dos principais provedores de nuvem e como sistema operacional de armazenamento para plataformas NetApp ASA (All San Array), AFF (All-flash FAS) e FAS (Fabric-Attached Storage). O ONTAP oferece alto desempenho e baixa latência para uma variedade de casos de uso, incluindo virtualização VMware, sem criar silos.

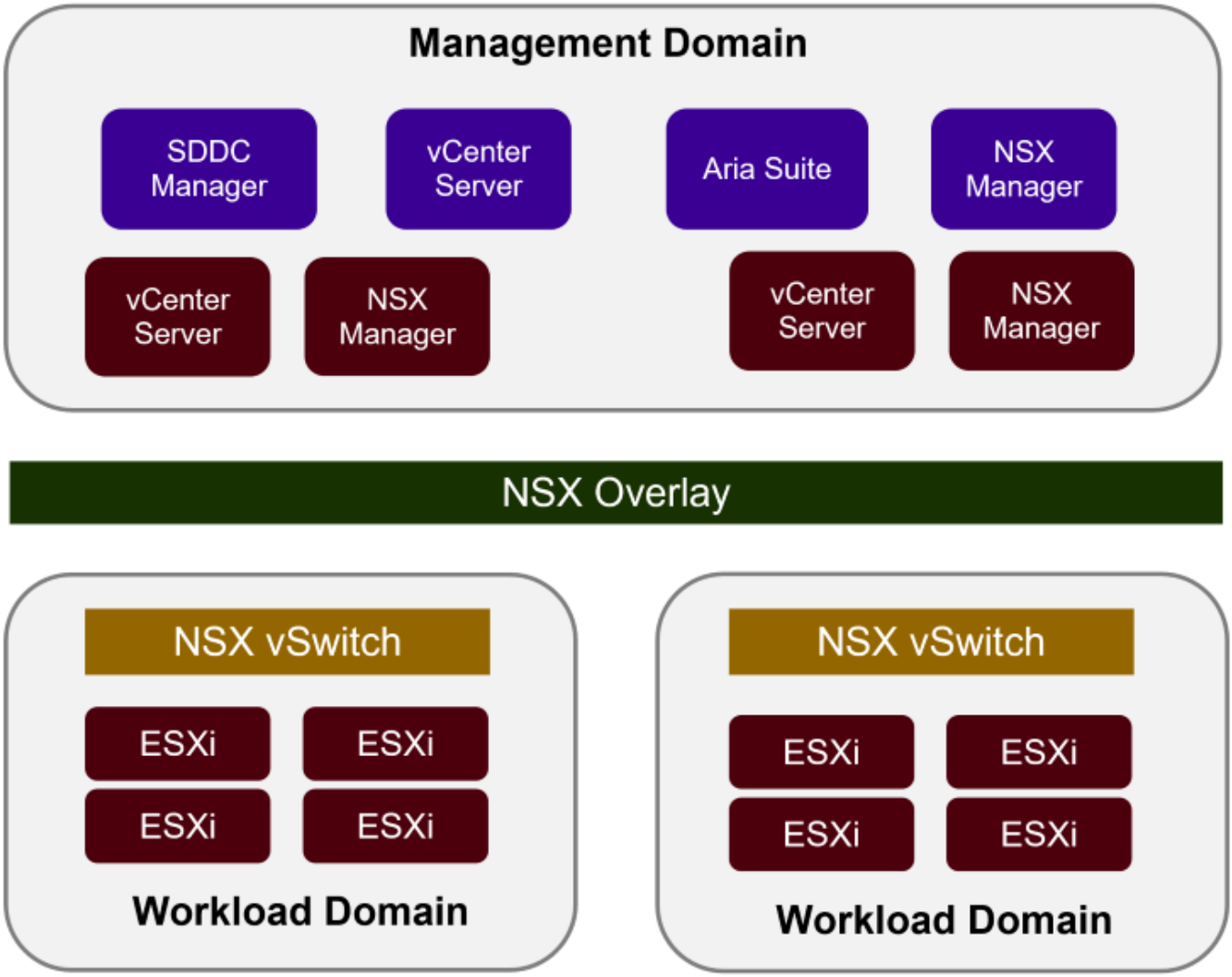
Introdução ao VMware Cloud Foundation

O VCF integra ofertas de computação, rede e armazenamento com produtos VMware e integrações de terceiros, facilitando cargas de trabalho nativas do Kubernetes e baseadas em máquinas virtuais. Esta plataforma de software inclui componentes-chave como VMware vSphere, NSX, Aria Suite Enterprise, Tanzu Kubernetes Grid, HCX Enterprise, SDDC Manager e capacidade de armazenamento vinculada aos núcleos de CPU do host via vSAN. O NetApp ONTAP integra-se perfeitamente a uma variedade de modelos de implantação de VCF, tanto no local quanto na nuvem pública.



Domínios VCF

Domínios são uma construção fundamental dentro do VCF que permite a organização de recursos em grupos distintos e independentes. Os domínios ajudam a organizar a infraestrutura de forma mais eficaz, garantindo que os recursos sejam utilizados com eficiência. Cada domínio é implantado com seus próprios elementos de computação, rede e armazenamento.



Existem dois tipos principais de domínios com VCF:

- **Domínio de gerenciamento** – O domínio de gerenciamento inclui componentes responsáveis pelas funções principais do ambiente VCF. Os componentes lidam com tarefas essenciais, como provisionamento de recursos, monitoramento, manutenção e incluem integrações de plug-ins de terceiros, como o NetApp ONTAP Tools for VMware. Domínios de gerenciamento podem ser implantados usando o Cloud Builder Appliance para garantir que as práticas recomendadas sejam seguidas, ou um ambiente vCenter existente pode ser convertido em um domínio de gerenciamento VCF.
- **Domínio de carga de trabalho de infraestrutura virtual** – Os domínios de carga de trabalho de infraestrutura virtual são projetados para serem conjuntos de recursos dedicados a uma necessidade operacional, carga de trabalho ou organização específica. Os domínios de carga de trabalho são implantados facilmente por meio do SDDC Manager, ajudando a automatizar uma série de tarefas complexas. Até 24 domínios de carga de trabalho podem ser provisionados em um ambiente VCF, com cada um representando uma unidade de infraestrutura pronta para aplicativos.

Armazenamento com VCF

O armazenamento que eles consomem é essencial para a funcionalidade dos domínios. Embora o VCF inclua capacidade vSAN baseada em núcleo de CPU para casos de uso hiperconvergentes, ele também oferece suporte a uma ampla gama de soluções de armazenamento externo. Essa flexibilidade é crucial para empresas que têm investimentos significativos em matrizes de armazenamento existentes ou precisam oferecer suporte a protocolos além do que o vSAN oferece. O VMware oferece suporte a vários tipos de armazenamento com VCF.

Existem dois tipos principais de armazenamento com VCF:

- **Armazenamento principal** – Este tipo de armazenamento é alocado durante a criação inicial do domínio. Para domínios de gerenciamento, esse armazenamento abriga os componentes administrativos e operacionais do VCF. Para domínios de carga de trabalho, esse armazenamento foi projetado para dar suporte às cargas de trabalho, VMs ou contêineres para os quais o domínio foi implantado.
- **Armazenamento suplementar** – O armazenamento suplementar pode ser adicionado a qualquer domínio de carga de trabalho após a implantação. Esse tipo de armazenamento ajuda as organizações a aproveitar os investimentos existentes em infraestrutura de armazenamento e integrar várias tecnologias de armazenamento para otimizar o desempenho, a escalabilidade e a relação custo-benefício.

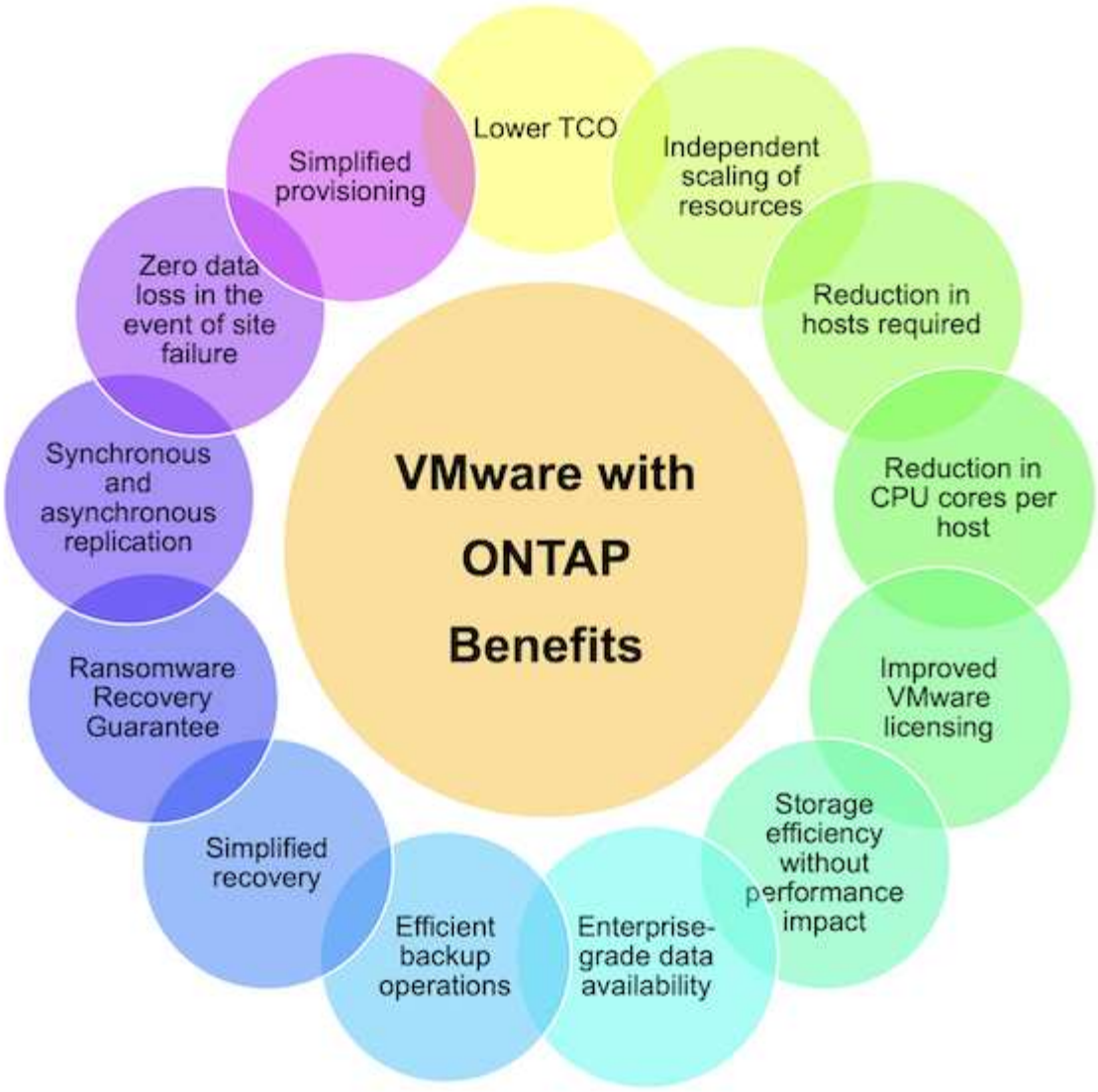
Suporta tipos de armazenamento VCF

Tipo de domínio	Armazenamento Principal	Armazenamento Suplementar
Domínio de Gestão	vSAN FC* NFS*	vVols (FC, iSCSI ou NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
Domínio de carga de trabalho de infraestrutura virtual	vSAN vVols (FC, iSCSI ou NFS) FC NFS	vVols (FC, iSCSI ou NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

Observação: * Suporte a protocolo específico fornecido ao usar a Ferramenta de importação VCF com ambientes vSphere existentes.

Por que ONTAP para VCF

Além dos casos de uso que envolvem proteção de investimento e suporte a vários protocolos, há muitos motivos adicionais para aproveitar o armazenamento compartilhado externo dentro de um domínio de carga de trabalho VCF. Pode-se presumir que o armazenamento provisionado para um domínio de carga de trabalho seja meramente um repositório para hospedar VMs e contêineres. No entanto, as necessidades da organização muitas vezes superam as capacidades da capacidade licenciada e exigem armazenamento empresarial. O armazenamento fornecido pelo ONTAP, alocado em domínios dentro do VCF, é fácil de implantar e oferece uma solução de armazenamento compartilhado preparada para o futuro.



Para obter mais informações sobre os principais benefícios do ONTAP para VMware VCF identificados abaixo, consulte"Por que ONTAP para VMware" .

- Flexibilidade no primeiro dia e à medida que você cresce
- Descarregue tarefas de armazenamento para o ONTAP
- Melhor eficiência de armazenamento da categoria
- Disponibilidade de dados de nível empresarial
- Operações eficientes de backup e recuperação
- Capacidades holísticas de continuidade de negócios

Informações adicionais:

- "Opções de armazenamento da NetApp"
- "Suporte ao vSphere Metro Storage Cluster (vMSC)"
- "Ferramentas ONTAP para VMware vSphere"
- "Automação VMware com ONTAP"

- "NetApp SnapCenter"
- "Multicloud híbrida com VMware e NetApp"
- "Segurança e proteção contra ransomware"
- "Migração fácil de cargas de trabalho VMware para NetApp"
- "Recuperação de Desastres BlueXP"
- "Insights sobre infraestrutura de dados"
- "Coletor de dados de VM"

Resumo

A ONTAP fornece uma plataforma que atende a todos os requisitos de carga de trabalho, oferecendo soluções personalizadas de armazenamento em bloco e ofertas unificadas para permitir resultados mais rápidos para VMs e aplicativos de maneira confiável e segura. O ONTAP incorpora técnicas avançadas de redução e movimentação de dados para minimizar o espaço ocupado pelo data center, ao mesmo tempo em que garante disponibilidade em nível empresarial para manter cargas de trabalho críticas on-line. Além disso, a AWS, o Azure e o Google oferecem suporte ao armazenamento externo com tecnologia NetApp para aprimorar o armazenamento vSAN em clusters baseados em nuvem da VMware como parte de suas ofertas VMware-in-the-Cloud. No geral, os recursos superiores do NetApp o tornam uma escolha mais eficaz para implantações do VMware Cloud Foundation.

Recursos de documentação

Para obter informações detalhadas sobre as ofertas da NetApp para o VMware Cloud Foundation, consulte o seguinte:

Documentação do VMware Cloud Foundation

- "Documentação do VMware Cloud Foundation"

Série de blogs de quatro (4) partes sobre VCF com NetApp

- "NetApp e VMware Cloud Foundation simplificados Parte 1: Introdução"
- "NetApp e VMware Cloud Foundation simplificados Parte 2: armazenamento principal VCF e ONTAP"
- "NetApp e VMware Cloud Foundation simplificados Parte 3: VCF e armazenamento principal Element"
- "NetApp e VMware Cloud Foundation simplificados - Parte 4: Ferramentas ONTAP para VMware e armazenamento suplementar"

*VMware Cloud Foundation com matrizes SAN All-Flash da NetApp *

- "VCF com matrizes NetApp ASA , introdução e visão geral da tecnologia"
- "Use ONTAP com FC como armazenamento principal para domínios de gerenciamento"
- "Use o ONTAP com FC como armazenamento principal para domínios de carga de trabalho do VI"
- "Use o Ontap Tools para implantar armazenamentos de dados iSCSI em um domínio de gerenciamento VCF"
- "Use o Ontap Tools para implantar datastores FC em um domínio de gerenciamento VCF"
- "Use o Ontap Tools para implantar datastores vVols (iSCSI) em um domínio de carga de trabalho VI"
- "Configurar armazenamentos de dados NVMe sobre TCP para uso em um domínio de carga de trabalho

VI"

- "Implante e use o SnapCenter Plug-in for VMware vSphere para proteger e restaurar VMs em um domínio de carga de trabalho VI"
- "Implante e use o SnapCenter Plug-in for VMware vSphere para proteger e restaurar VMs em um domínio de carga de trabalho VI (datastores NVMe/TCP)"

*VMware Cloud Foundation com matrizes NetApp All-Flash AFF *

- "VCF com matrizes NetApp AFF , introdução e visão geral da tecnologia"
- "Use ONTAP com NFS como armazenamento principal para domínios de gerenciamento"
- "Use ONTAP com NFS como armazenamento principal para domínios de carga de trabalho VI"
- "Use as ferramentas ONTAP para implantar armazenamentos de dados vVols (NFS) em um domínio de carga de trabalho VI"
- Soluções NetApp FlexPod para VMware Cloud Foundation*
- "Expandindo a nuvem híbrida FlexPod com o VMware Cloud Foundation"
- "FlexPod como um domínio de carga de trabalho para VMware Cloud Foundation"
- "Guia de design do FlexPod como domínio de carga de trabalho para VMware Cloud Foundation"

Opções de design com VMware Cloud Foundation e ONTAP

Você pode começar do zero com o VCF 9 ou reutilizar implantações existentes para criar um ambiente de Nuvem Privada usando o VCF 9 e o ONTAP. Saiba mais sobre projetos de design populares para o VCF 9 e como os produtos NetApp agregam valor.

Opções de armazenamento

O VMware Cloud Foundation com ONTAP oferece suporte a uma variedade de configurações de armazenamento para atender a diferentes requisitos de desempenho, escalabilidade e disponibilidade. As tabelas a seguir resumem as principais e suplementares opções de armazenamento disponíveis para seu ambiente.

Família de produtos	VMFS no FC	NFSv3
Série A e Série C da ASA	Sim	Não
Série A e Série C da AFF	Sim	Sim
FAS	Sim	Sim

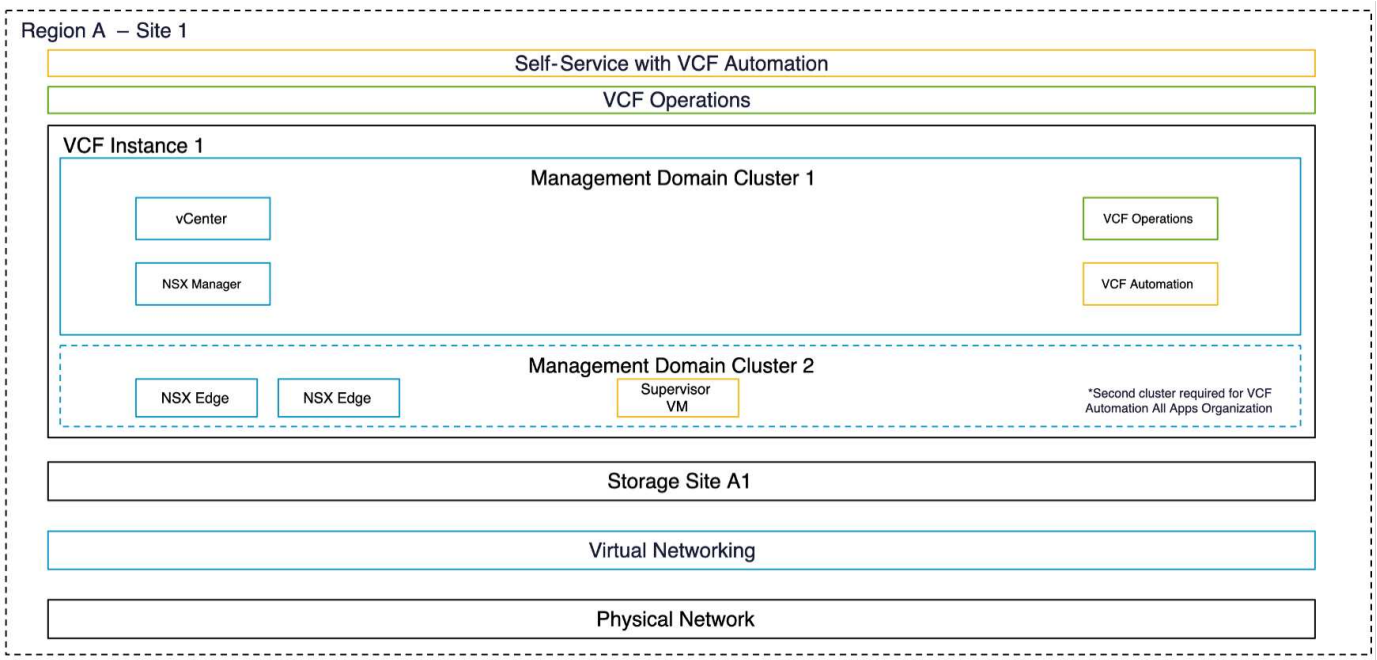
Família de produtos	VMFS no FC	VMFS em iSCSI	VMFS em NVMe-oF	NFSv3	NFSv4.1
Série A e Série C da ASA	Sim	Sim	Sim	Não	Não
Série A e Série C da AFF	Sim	Sim	Sim	Sim	Sim
FAS	Sim	Sim	Sim	Sim	Sim

Projetos

Os projetos a seguir ilustram modelos comuns de implantação para VMware Cloud Foundation e ONTAP em vários cenários de sites e recursos.

Frota VCF em um único local com pegada mínima

Este projeto de design é para implantar componentes de gerenciamento e carga de trabalho em um único cluster vSphere com recursos mínimos. Ele suporta VMFS e NFSv3 Principal Datastores e uma opção de implantação simples com uma configuração de dois nós. Se você planeja usar o VCF Automation com o modelo de organização de todos os aplicativos, precisará de um segundo cluster para implantar o vSphere Supervisor e os nós do NSX Edge.



Para minimizar o consumo de recursos, use uma instância de ferramentas ONTAP existente, se possível. Se não estiver disponível, um único nó com um perfil Pequeno é adequado. O SnapCenter Plug-in for VMware vSphere protege máquinas virtuais e datastores usando snapshots nativos e replicação para outro array de armazenamento ONTAP .

> Se você não tiver recursos para explorar o VCF, muitos provedores de nuvem oferecem o VCF como um serviço, e o ONTAP está disponível como um serviço próprio de provedores de nuvem.

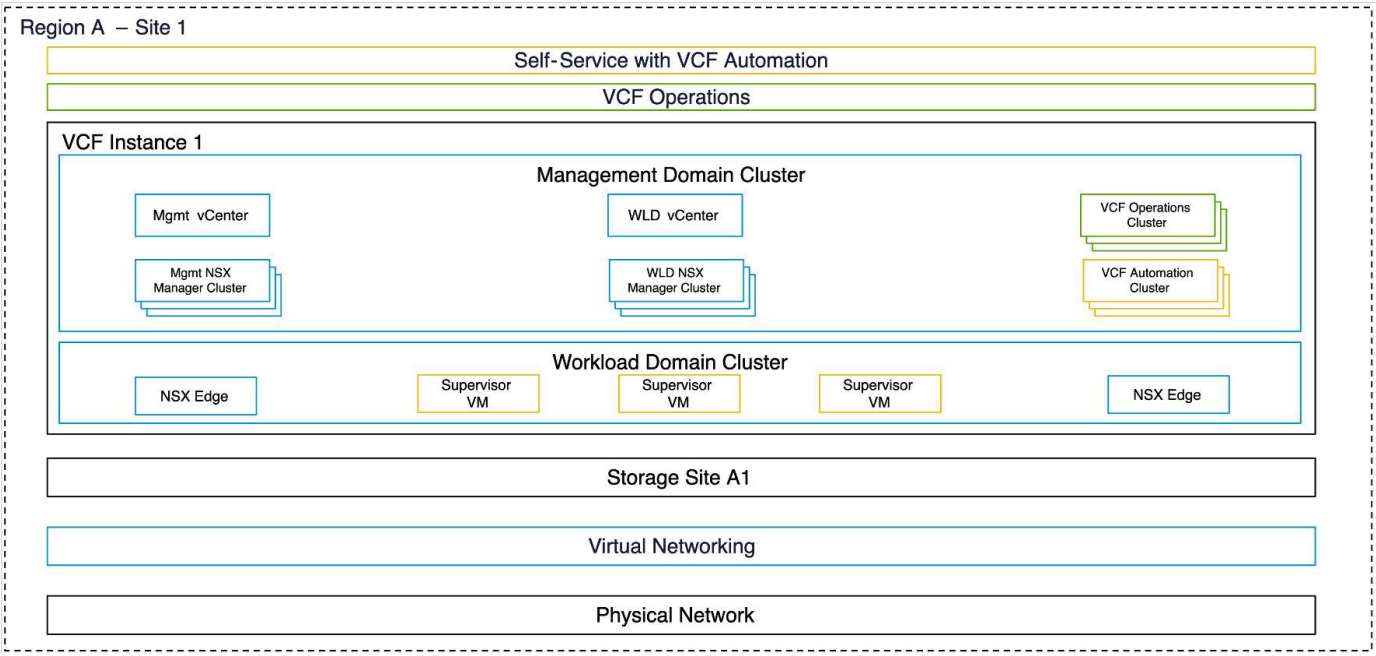
Para mais detalhes sobre este projeto, consulte o"Documentação técnica da Broadcom sobre frota VCF em um único local com pegada mínima" .

Frota VCF em um único local

Este projeto de design é para clientes com um único Datacenter Primário que dependem de Alta Disponibilidade de aplicativos. Normalmente, envolve um único ambiente VCF. Você pode usar o ASA para cargas de trabalho em bloco e o AFF para cargas de trabalho de arquivo/unificadas.

O Repositório de Conteúdo compartilha modelos de VM e registros de contêiner entre domínios VCF. Quando hospedado no FlexGroup Volume, o recurso FlexCache fica disponível para armazenamento de dados de assinatura.

Não há suporte para hospedagem de VMs no FlexCache Datastore.



Uma única instância de ferramentas ONTAP no modo HA pode gerenciar todos os vCenters na frota VCF. Consulte o"Limites de configuração das ferramentas ONTAP" para mais informações. As ferramentas ONTAP integram-se ao VCF SSO e ao agrupamento inteligente VCF OPS para acesso a vários vCenters na mesma interface de usuário.

Armazenamento de dados suplementar VCF com ferramentas ONTAP

Você deve implantar o SnapCenter Plug-in em cada instância do vCenter para proteção de VM e Datastore.

O gerenciamento baseado em políticas de armazenamento é usado com o vSphere Supervisor para hospedar VMs de controle do VKS. As tags são gerenciadas centralmente no VCF Ops. O NetApp Trident CSI é usado com o VKS para proteção de backup de aplicativos usando recursos de array nativos. Quando você usa o vSphere CSI, os detalhes do volume persistente aparecem no VCF Automation.

Para mais detalhes sobre este projeto, consulte o"Documentação técnica da Broadcom sobre frota VCF em um único site" .

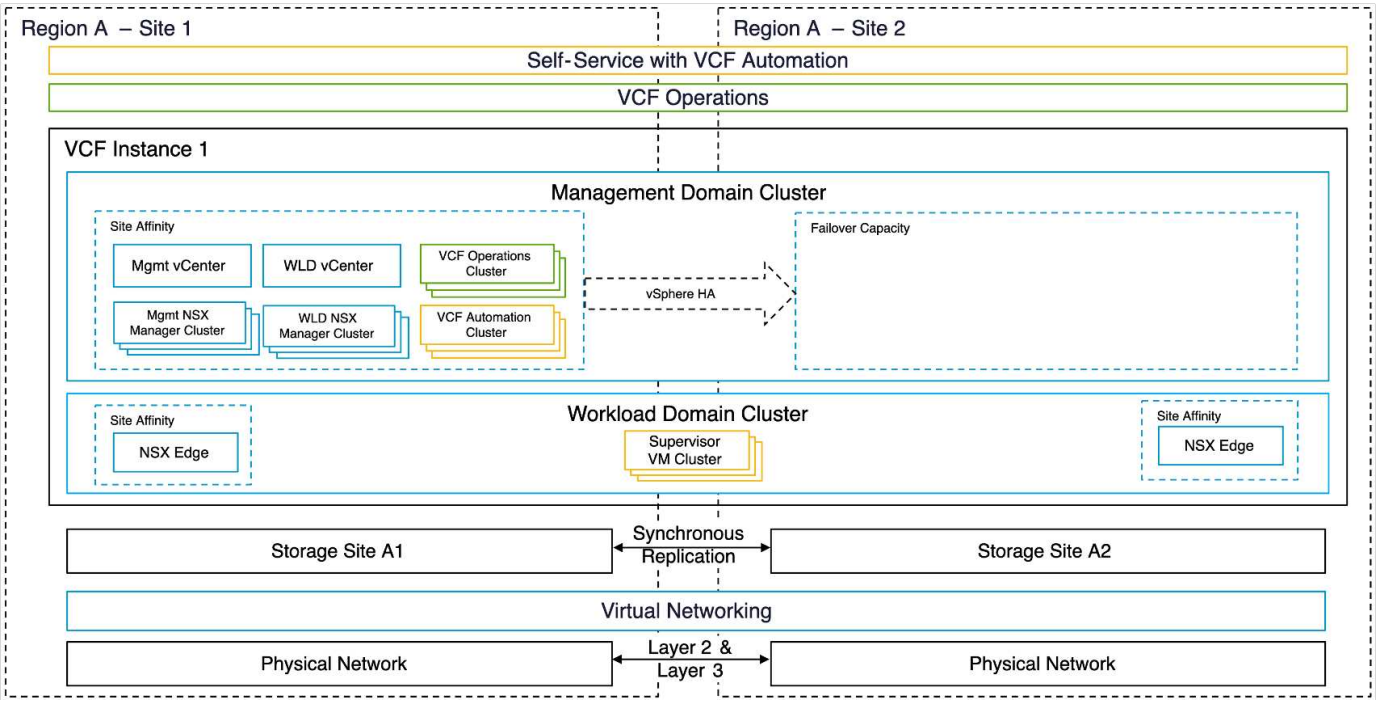
Frota VCF com vários locais em uma única região

Este design é para clientes que fornecem serviços semelhantes aos da nuvem com maior disponibilidade, distribuindo cargas de trabalho entre diferentes domínios de falhas.

Para armazenamentos de dados VMFS, o SnapMirror Active Sync fornece uma unidade de armazenamento ativa-ativa para uso com o vSphere Metro Storage Cluster. O modo de acesso uniforme oferece failover de armazenamento transparente, enquanto o modo de acesso não uniforme exige reinicialização da VM em caso de falha de domínio.

Para datastores NFS, o ONTAP MetroCluster com vSphere Metro Storage Cluster garante alta disponibilidade. Um mediador evita cenários de cérebro dividido e agora pode ser hospedado no BlueXP.

As regras de posicionamento de VM controlam VMs dentro do mesmo domínio de falha para componentes do Domínio de Gerenciamento.



As ferramentas ONTAP fornecem uma interface de usuário para configurar relacionamentos de sincronização ativa do SnapMirror . Os sistemas de armazenamento de ambos os domínios de falha devem ser registrados nas ferramentas ONTAP e no SnapCenter Plug-in for VMware vSphere.

Você pode implementar políticas de backup 3-2-1 usando o BlueXP Backup and Recovery para VMs via SnapMirror e SnapMirror to Cloud. Você pode executar restaurações de qualquer um dos três locais.

O Trident Protect ou o BlueXP Backup and Recovery para Kubernetes protegem aplicativos de cluster VKS.

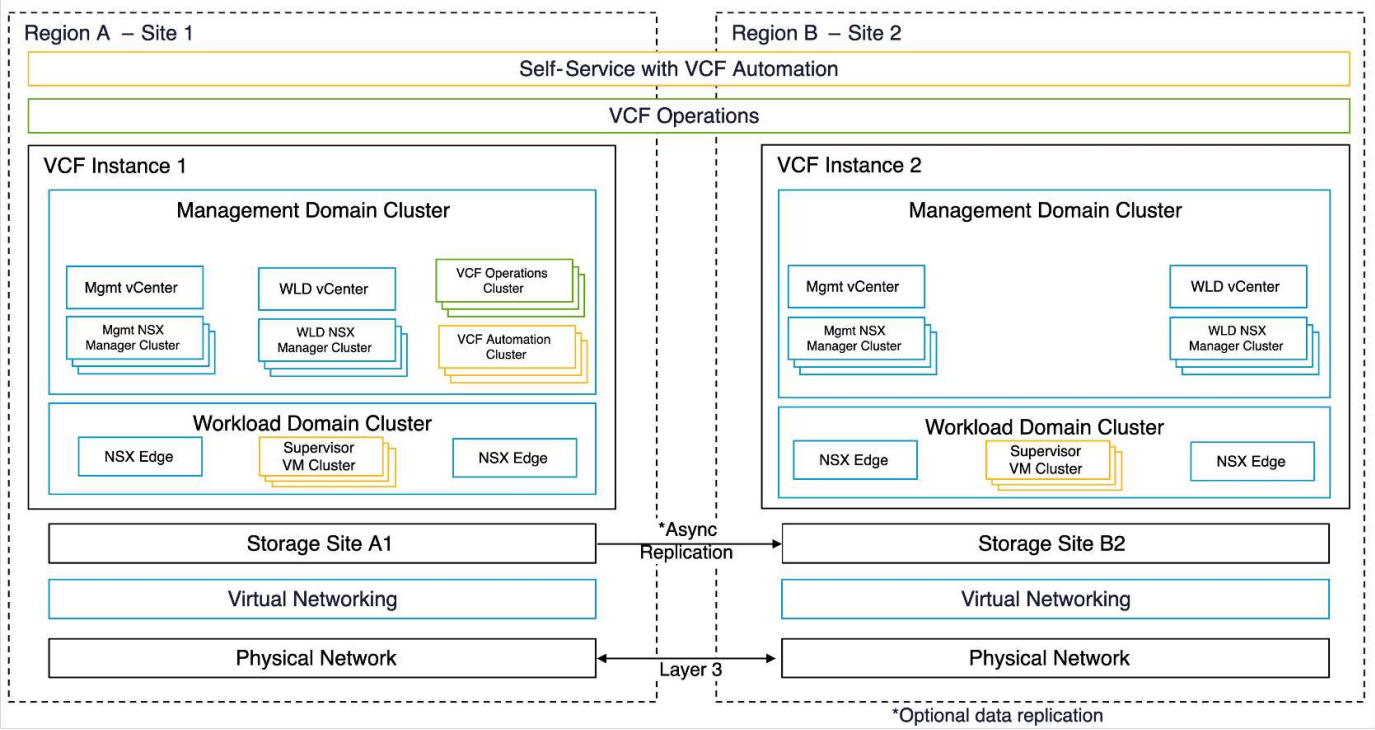
Para mais informações, consulte o"Documentação técnica da Broadcom sobre frota VCF com vários sites em uma única região" .

Frota VCF com vários locais em várias regiões

Este projeto é para clientes espalhados pelo mundo todo, fornecendo serviços de proximidade e soluções de recuperação de desastres.

Você pode gerenciar a recuperação de desastres para VMs com o VMware Live Site Recovery ou o BlueXP Disaster Recovery as a Service. As ferramentas ONTAP oferecem o SRA (Storage Replication Adapter) para orquestrar operações de armazenamento com o ONTAP.

Família de produtos	Sincronização ativa do SnapMirror	MetroCluster
Série A e Série C da ASA	Sim	Sim
Série A e Série C da AFF	Sim	Sim
FAS	Não	Sim



As ferramentas ONTAP fornecem uma interface de usuário para configuração de replicação de armazenamento de dados. O BlueXP também pode ser usado para replicação entre matrizes de armazenamento. O SnapCenter Plug-in for VMware vSphere utiliza relacionamentos SnapMirror existentes para SnapShots.

Para mais informações, consulte o"Documentação técnica da Broadcom sobre frota VCF com vários locais em várias regiões" .

Frota VCF com vários locais em uma única região, além de regiões adicionais

Este design aborda tanto a disponibilidade quanto a recuperação de desastres de VMs e aplicativos VKS.

ASA, AFF e FAS suportam esta opção de design.

Você pode usar ferramentas ONTAP ou BlueXP para configurar o relacionamento de replicação.

Para obter mais informações, consulte o "Documentação técnica da Broadcom sobre frota VCF com vários sites em uma única região, além de regiões adicionais" .

Configure ambientes de nuvem privada com VMware Cloud Foundation e ONTAP

Implante, converta ou atualize ambientes do VMware Cloud Foundation 9 com o ONTAP. Aprenda a configurar novos ambientes do VCF 9.0, convergir instâncias existentes do vCenter e armazenamentos de dados ONTAP e atualizar implantações anteriores do VCF.

Implantar uma nova instância do VCF 9

Use este fluxo de trabalho para implantar um ambiente limpo do VMware Cloud Foundation (VCF) 9.0. Após a implantação, você pode migrar cargas de trabalho ou começar a provisionar aplicativos e fornecer serviços de infraestrutura.

Para etapas de alto nível, consulte o"Build Journey – Instale uma nova implantação do VMware Cloud Foundation" .

Passos

1. Siga o"Etapas de implantação do Broadcom VCF 9" .
2. Na etapa de preparação da implantação, conclua as tarefas para sua opção de armazenamento principal.

VMFS no FC

1. Colete os WWPNs para todos os hosts ESXi. Você pode correr `esxcli storage san fc list` , use o ESXi Host Client ou use o PowerCLI.
2. Configurar zoneamento. Ver "Configurações de zoneamento FC recomendadas para sistemas ONTAP" .

   Use os WWPNs das interfaces lógicas (LIFs) do SVM, não os WWPNs do adaptador físico.

3. Crie um LUN e mapeie-o para os hosts pelo WWPN usando o Gerenciador do Sistema, o ONTAP CLI ou a API.
4. Examine novamente o adaptador de armazenamento no ESXi e crie o armazenamento de dados VMFS.

NFSv3

1. Crie uma interface VMkernel em um host ESXi.
2. Garantir a"O SVM tem NFS habilitado" e"O vStorage sobre NFS está habilitado" .
3. Crie um volume e exporte-o com uma política que permita os hosts ESXi.
4. Ajuste as permissões conforme necessário.
5. Implante o ONTAP NFS VAAI VIB e inclua-o na imagem vLCM. Por exemplo: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip` . (Baixe o ZIP do site de suporte da NetApp .)
6. Monte o volume NFS no host onde você criou a interface VMkernel. Por exemplo: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-cl01-nfs01` .

   O `nConnect` a contagem de sessões é por host. Atualize outros hosts após a implantação, conforme necessário.

1. No final de **Verificar resumo da implantação e revisar as próximas etapas** na fase **Implantar frota VCF**, conclua o seguinte:
   a. Implantar ferramentas ONTAP
      - "Baixe as ferramentas ONTAP 10.x"do site de suporte da NetApp .
      - Crie registros DNS para o Gerenciador de ferramentas ONTAP , nó(s) e o IP virtual usado para

comunicação interna.

- Implante o OVA no vCenter Server de gerenciamento.
- "Registre o domínio de gerenciamento vCenter"com o Gerenciador de ferramentas ONTAP .
- "Adicione o backend de armazenamento"usando a interface do usuário do vSphere Client.
- "Crie um armazenamento de dados suplementar"(inclua um para o registro de conteúdo).
- Crie o registro de conteúdo se você planeja uma implantação de HA.
- "Habilitar HA"no Gerenciador de ferramentas ONTAP .

b. Implantar o plug-in SnapCenter

- "Implantar o SnapCenter Plug-in for VMware vSphere" .
- "Adicione o backend de armazenamento" .
- "Criar políticas de backup" .
- "Criar grupos de recursos" .

c. Implantar o conector BlueXP

- "Revise o que você pode fazer sem um conector" .
- "Implantar o conector" .

d. Use BlueXP para backup e recuperação

- "Proteja cargas de trabalho VM" .
- "Proteja cargas de trabalho VKS" .

2. Depois de importar o vCenter como um domínio de carga de trabalho na instância do VCF, conclua o seguinte:

a. Registrar ferramentas ONTAP

- "Registre o domínio de carga de trabalho vCenter"com o Gerenciador de ferramentas ONTAP .
- "Adicione o backend de armazenamento"usando a interface do usuário do vSphere Client.
- "Crie um armazenamento de dados suplementar" .

b. Implantar o SnapCenter Plug-in for VMware vSphere

- "Implantar o SnapCenter Plug-in for VMware vSphere" .
- "Adicione o backend de armazenamento" .
- "Criar políticas de backup" .
- "Criar grupos de recursos" .

c. Use BlueXP para backup e recuperação

- "Proteja cargas de trabalho VM" .
- "Proteja cargas de trabalho VKS" .

Você pode reutilizar essas etapas sempre que criar um novo domínio de carga de trabalho.

Convergir componentes existentes no VCF 9

Talvez você já tenha alguns componentes da frota VCF e prefira reutilizá-los. Ao reutilizar uma instância do vCenter, os armazenamentos de dados são frequentemente provisionados com ferramentas ONTAP , que podem servir como armazenamento principal para VCF.

Pré-requisitos

- Confirme se as instâncias existentes do vCenter estão funcionais.
- Verifique se os armazenamentos de dados provisionados ONTAP estão disponíveis.
- Garantir o acesso ao"Matriz de Interoperabilidade" .

Passos

1. Revise o"cenários suportados para convergir para VCF" .
2. Convergir uma instância do vCenter com armazenamentos de dados provisionados ONTAP como armazenamento principal.
3. Verifique as versões suportadas usando o"Matriz de Interoperabilidade" .
4. Atualizar"Ferramentas ONTAP" se necessário.
5. Atualizar o"Plug-in SnapCenter para VMware vSphere" se necessário.

Atualizar um ambiente VCF existente para VCF 9

Atualize uma implantação anterior do VCF para a versão 9.0 usando o processo de atualização padrão. O resultado é um ambiente VCF executando a versão 9.0 com domínios de gerenciamento e carga de trabalho atualizados.

Pré-requisitos

- Faça backup do domínio de gerenciamento e dos domínios de carga de trabalho.
- Verifique a compatibilidade das ferramentas ONTAP e do plug-in SnapCenter com o VCF 9.0. Siga o"Matriz de Interoperabilidade" para"atualizar ferramentas ONTAP" e"Plug-in SnapCenter para VMware vSphere" que são suportados pelo VCF 9.

Passos

1. Atualize o domínio de gerenciamento do VCF. Ver"Atualizar o domínio de gerenciamento do VCF para VCF 9" para obter instruções.
2. Atualize qualquer domínio de carga de trabalho do VCF 5.x. Ver"Atualizar o domínio de carga de trabalho do VCF 5.x para o VCF 9" para obter instruções.

Implementando recuperação de desastres com NetApp SnapMirror e BlueXP DRaaS

Solução de recuperação de desastres VCF para armazenamento de dados NFS com NetApp SnapMirror e BlueXP DRaaS

A replicação em nível de bloco de um site de produção para um site de recuperação de desastres (DR) oferece uma estratégia resiliente e econômica para proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados, incluindo ataques de ransomware. A replicação do NetApp SnapMirror permite que domínios de carga de trabalho do VMware VCF 9 em execução em sistemas ONTAP locais, usando armazenamentos de dados NFS ou VMFS, sejam replicados para um sistema ONTAP secundário localizado em um data center de recuperação designado onde o VMware também está implantado.

Esta seção descreve a configuração do BlueXP Disaster Recovery as a Service (DRaaS) para estabelecer DR para máquinas virtuais VMware locais.

A configuração inclui:

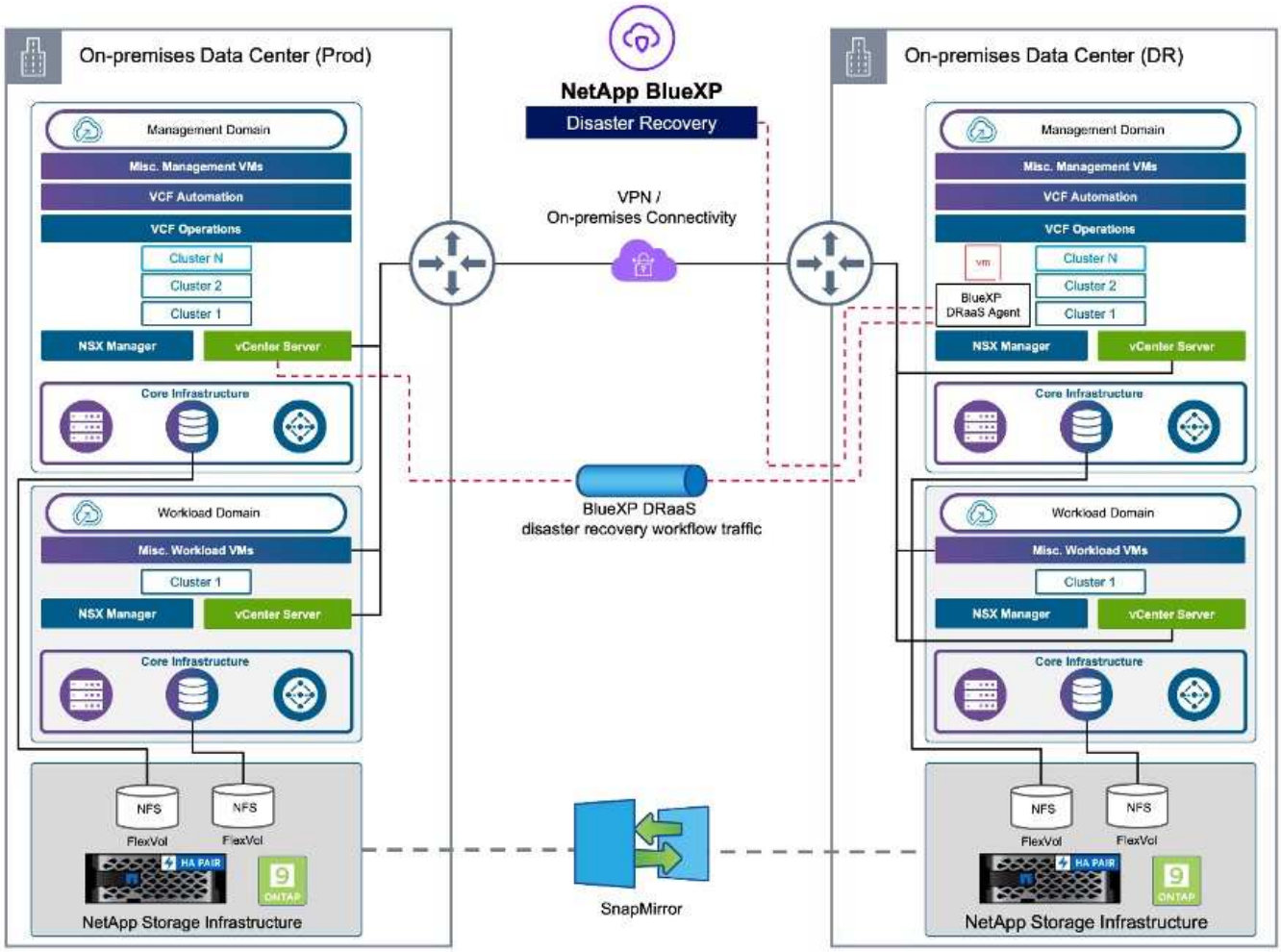
- Criando uma conta BlueXP e implantando um conector BlueXP .
- Adicionar matrizes ONTAP à tela BlueXP para facilitar a comunicação entre o VMware vCenter e o armazenamento ONTAP .
- Configurando replicação entre sites usando SnapMirror.
- Configurar e testar um plano de recuperação para validar a prontidão para failover.

O serviço de BlueXP disaster recovery , integrado ao console NetApp BlueXP , permite que as organizações descubram facilmente seus sistemas de armazenamento VMware vCenters e ONTAP locais. Uma vez descobertos, os administradores podem definir agrupamentos de recursos, criar planos de recuperação de desastres, associá-los aos recursos apropriados e iniciar ou testar operações de failover e failback. O NetApp SnapMirror fornece replicação eficiente em nível de bloco, garantindo que o site de DR permaneça sincronizado com o ambiente de produção por meio de atualizações incrementais. Isso permite um Objetivo de Ponto de Recuperação (RPO) de apenas cinco minutos.

O BlueXP DRaaS também oferece suporte a testes de recuperação de desastres sem interrupções. Aproveitando a tecnologia FlexClone da ONTAP, ele cria cópias temporárias e com eficiência de espaço do armazenamento de dados NFS a partir do Snapshot replicado mais recente, sem impactar as cargas de trabalho de produção ou incorrer em custos adicionais de armazenamento. Após o teste, o ambiente pode ser facilmente desmontado, preservando a integridade dos dados replicados.

No caso de um failover real, o BlueXP orquestra o processo de recuperação, trazendo automaticamente máquinas virtuais protegidas para o site de DR designado com intervenção mínima do usuário. Quando o site principal é restaurado, o serviço inverte o relacionamento do SnapMirror e replica quaisquer alterações de volta ao site original, permitindo um failback suave e controlado.

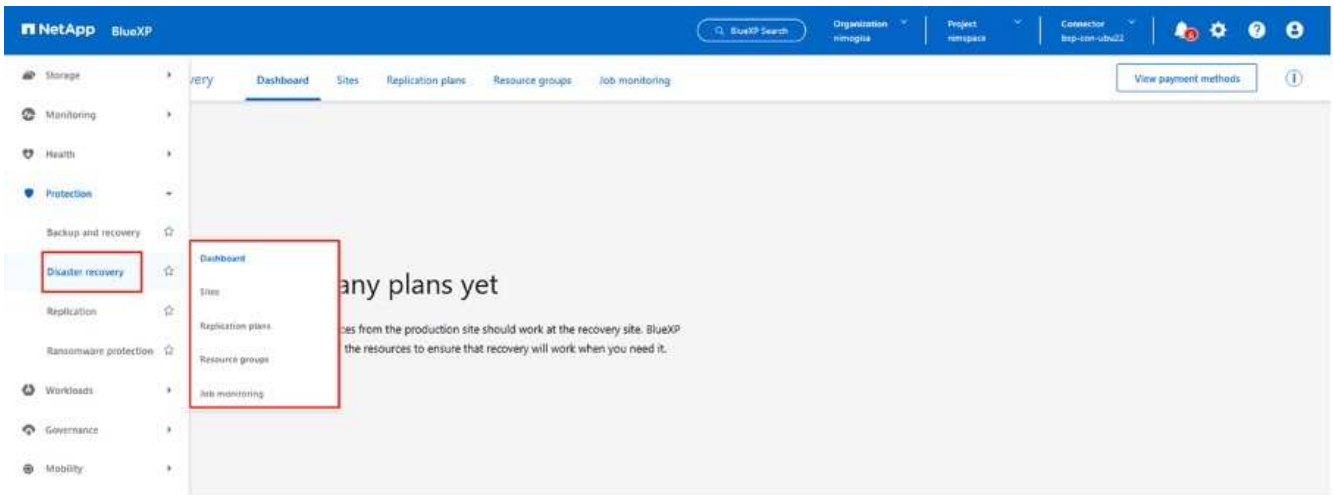
Todos esses recursos são fornecidos a um custo significativamente menor em comparação às soluções tradicionais de recuperação de desastres.



Começando

Para começar a BlueXP disaster recovery, use o console do BlueXP e acesse o serviço.

1. Faça login no BlueXP.
2. Na navegação à esquerda do BlueXP , selecione Proteção > Recuperação de desastres.
3. O painel de BlueXP disaster recovery é exibido.



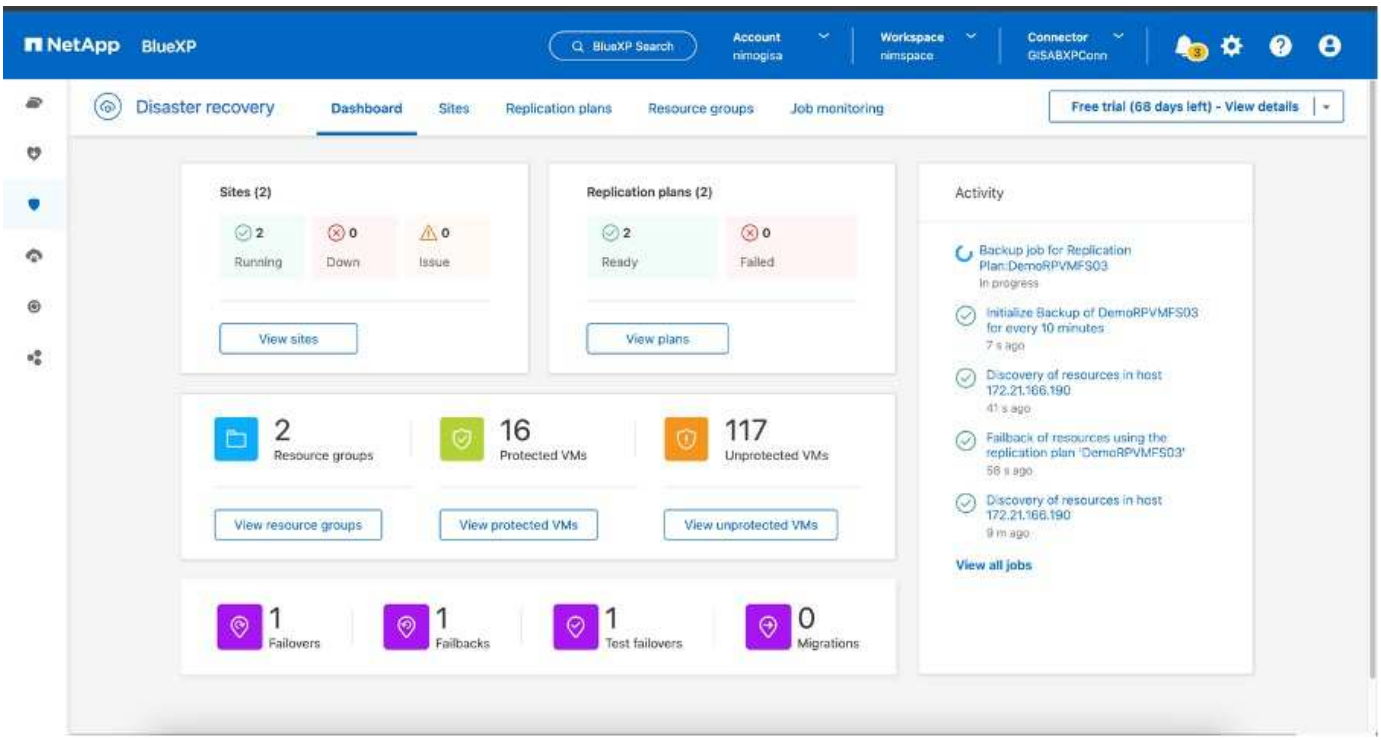
Antes de configurar o plano de recuperação de desastres, certifique-se do seguinte"pré-requisitos" são atendidas:

- O BlueXP Connector é configurado no NetApp BlueXP.
- A instância do conector BlueXP tem conectividade com o domínio de carga de trabalho de origem e destino vCenter e sistemas de armazenamento.
- Cluster NetApp Data ONTAP para fornecer armazenamento de dados NFS ou VMFS.
- Os sistemas de armazenamento NetApp locais que hospedam datastores NFS ou VMFS para VMware são adicionados no BlueXP.
- A resolução de DNS deve estar em vigor ao usar nomes DNS. Caso contrário, use endereços IP para o vCenter.
- A replicação do SnapMirror é configurada para os volumes de armazenamento de dados baseados em NFS ou VMFS designados.
- Certifique-se de que o ambiente tenha versões compatíveis dos servidores vCenter Server e ESXi.

Depois que a conectividade for estabelecida entre os sites de origem e destino, prossiga com as etapas de configuração, que devem levar alguns cliques e cerca de 3 a 5 minutos.

Observação: a NetApp recomenda implantar o conector BlueXP no site de destino ou em um terceiro site, para que o conector BlueXP possa se comunicar pela rede com os recursos de origem e destino.

Nesta demonstração, os domínios de carga de trabalho são configurados com armazenamento ONTAP NFS. As etapas em termos de fluxo de trabalho permanecem as mesmas para armazenamentos de dados baseados em VMFS.



Configuração de BlueXP disaster recovery

O primeiro passo na preparação para a recuperação de desastres é descobrir e adicionar os recursos de armazenamento e vCenter de origem à BlueXP disaster recovery.

Abra o console do BlueXP e selecione Proteção > Recuperação de desastres na navegação à esquerda. Selecione Descobrir servidores vCenter ou use o menu superior, selecione Sites > Adicionar > Adicionar vCenter.

Adicione as seguintes plataformas:

- Domínio de carga de trabalho de origem vCenter
- Domínio de carga de trabalho de destino vCenter.

Depois que os vCenters são adicionados, a descoberta automatizada é acionada.

Configurando a replicação de armazenamento entre a matriz do site de origem e a matriz do site de destino

O SnapMirror fornece replicação de dados em um ambiente NetApp . Construída com a tecnologia NetApp Snapshot®, a replicação SnapMirror é extremamente eficiente porque replica apenas os blocos que foram alterados ou adicionados desde a atualização anterior. O SnapMirror é facilmente configurado usando o NetApp OnCommand System Manager ou o ONTAP CLI. O BlueXP DRaaS também cria o relacionamento SnapMirror , desde que o cluster e o peering SVM sejam configurados previamente.

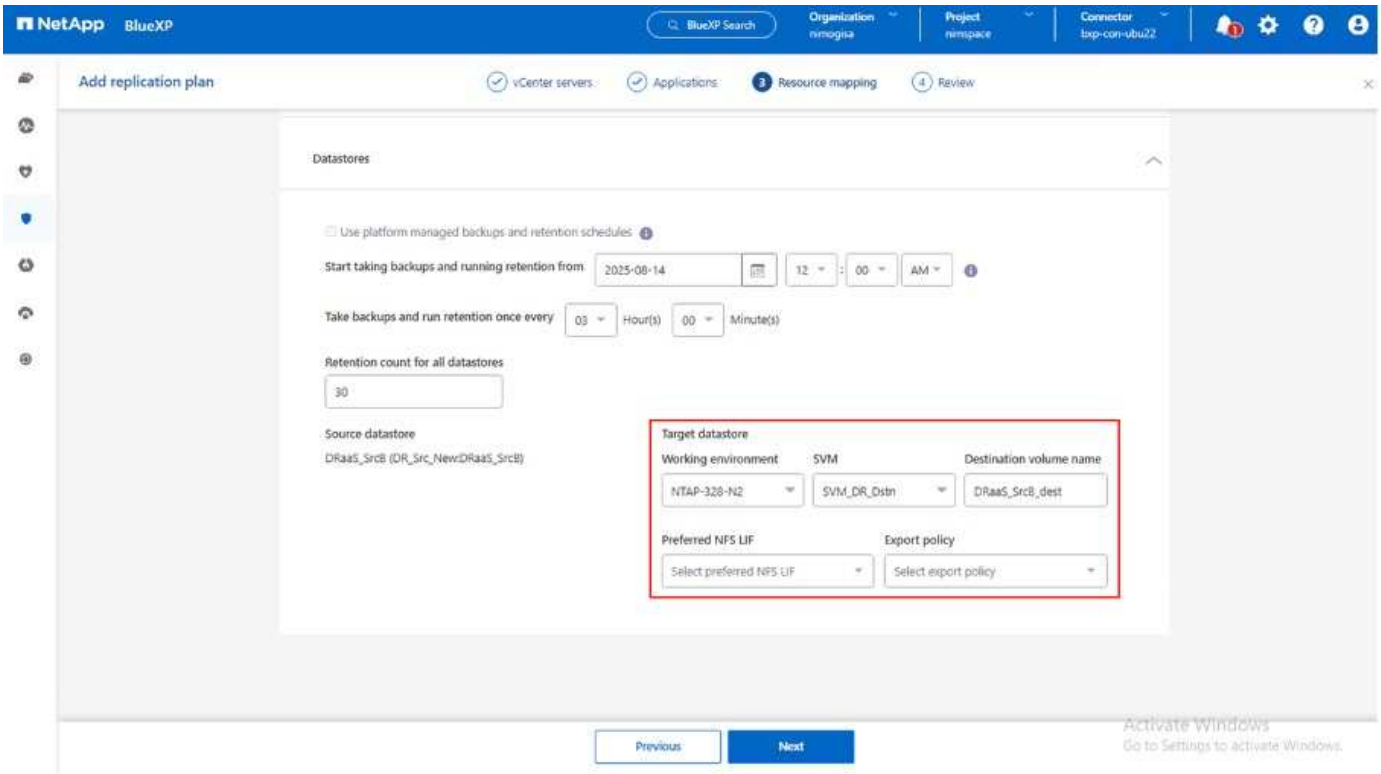
Para casos em que o armazenamento primário não é completamente perdido, o SnapMirror fornece um meio eficiente de ressincronizar os sites primário e de DR. O SnapMirror pode ressincronizar os dois sites, transferindo apenas dados alterados ou novos de volta para o site principal a partir do site de DR, simplesmente invertendo os relacionamentos do SnapMirror . Isso significa que os planos de replicação no BlueXP DRaaS podem ser ressincronizados em qualquer direção após um failover sem recopiar o volume inteiro. Se um relacionamento for ressincronizado na direção reversa, somente os novos dados que foram gravados desde a última sincronização bem-sucedida da cópia do Snapshot serão enviados de volta ao destino.

> Se o relacionamento do SnapMirror já estiver configurado para o volume via CLI ou System Manager, o BlueXP DRaaS assume o relacionamento e continua com o restante das operações de fluxo de trabalho.

Como configurá-lo para recuperação de desastres do VMware

O processo para criar a replicação do SnapMirror permanece o mesmo para qualquer aplicativo. O processo pode ser manual ou automatizado. A maneira mais fácil é aproveitar o BlueXP DRaaS, que automatizará o mesmo, desde que os dois critérios a seguir sejam atendidos:

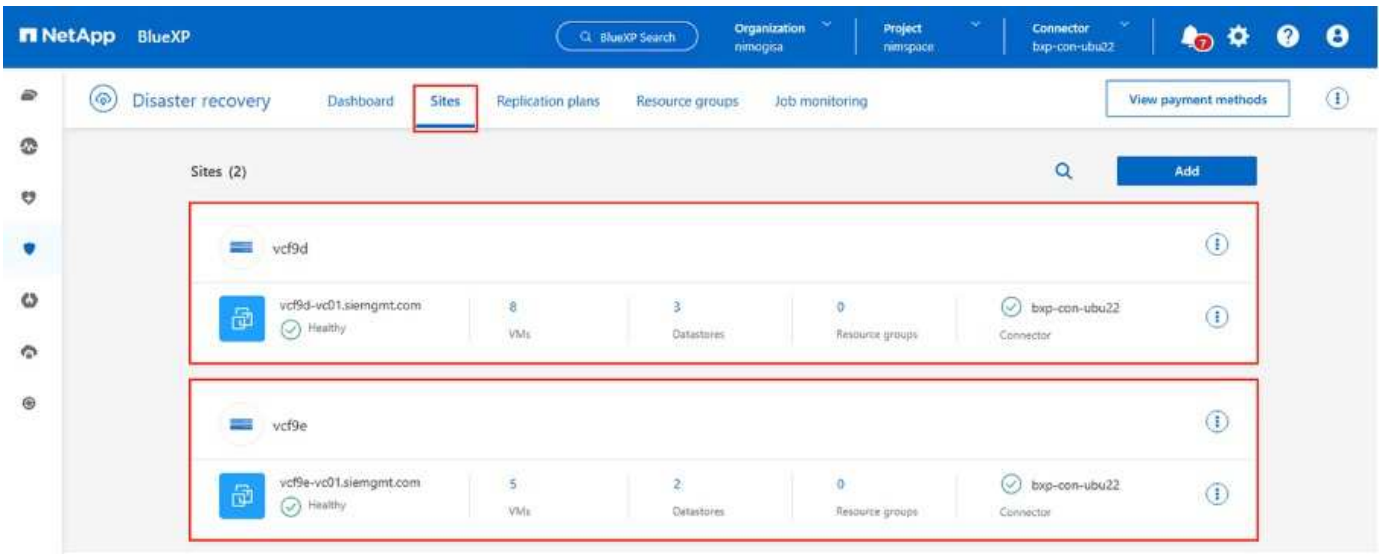
- Os clusters de origem e destino têm um relacionamento de pares.
- O SVM de origem e o SVM de destino têm um relacionamento de mesmo nível.



O BlueXP também fornece uma opção alternativa para configurar a replicação do SnapMirror usando o simples recurso de arrastar e soltar do sistema ONTAP de origem no ambiente para o destino para acionar o assistente que orienta o restante do processo.

O que a BlueXP disaster recovery pode fazer por você?

Depois que os sites de origem e destino são adicionados, a BlueXP disaster recovery executa a descoberta profunda automática e exibe as VMs junto com os metadados associados. A BlueXP disaster recovery também detecta automaticamente as redes e os grupos de portas usados pelas VMs e os preenche.

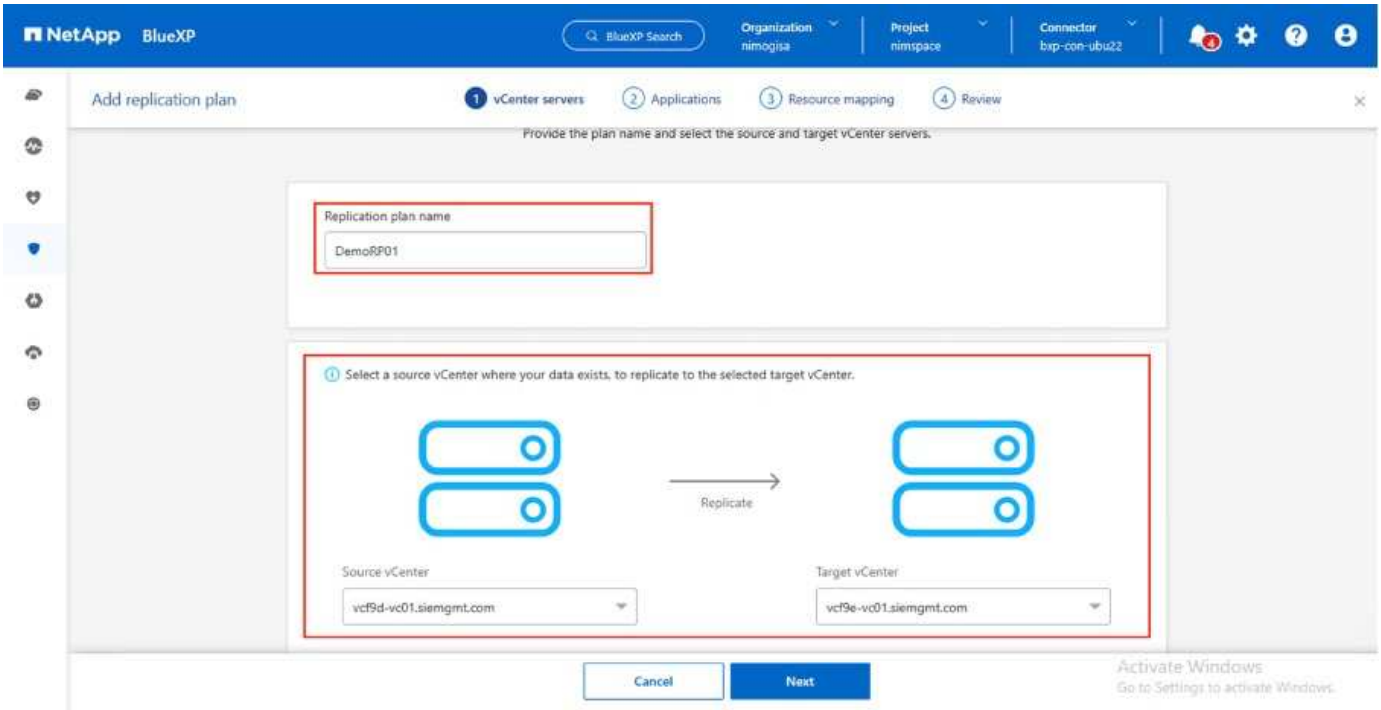


Após os sites serem adicionados, configure o plano de replicação selecionando as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos no plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados, além do mapeamento de clusters e redes. Para definir o plano de recuperação, navegue até a guia **Plano de Replicação** e clique em

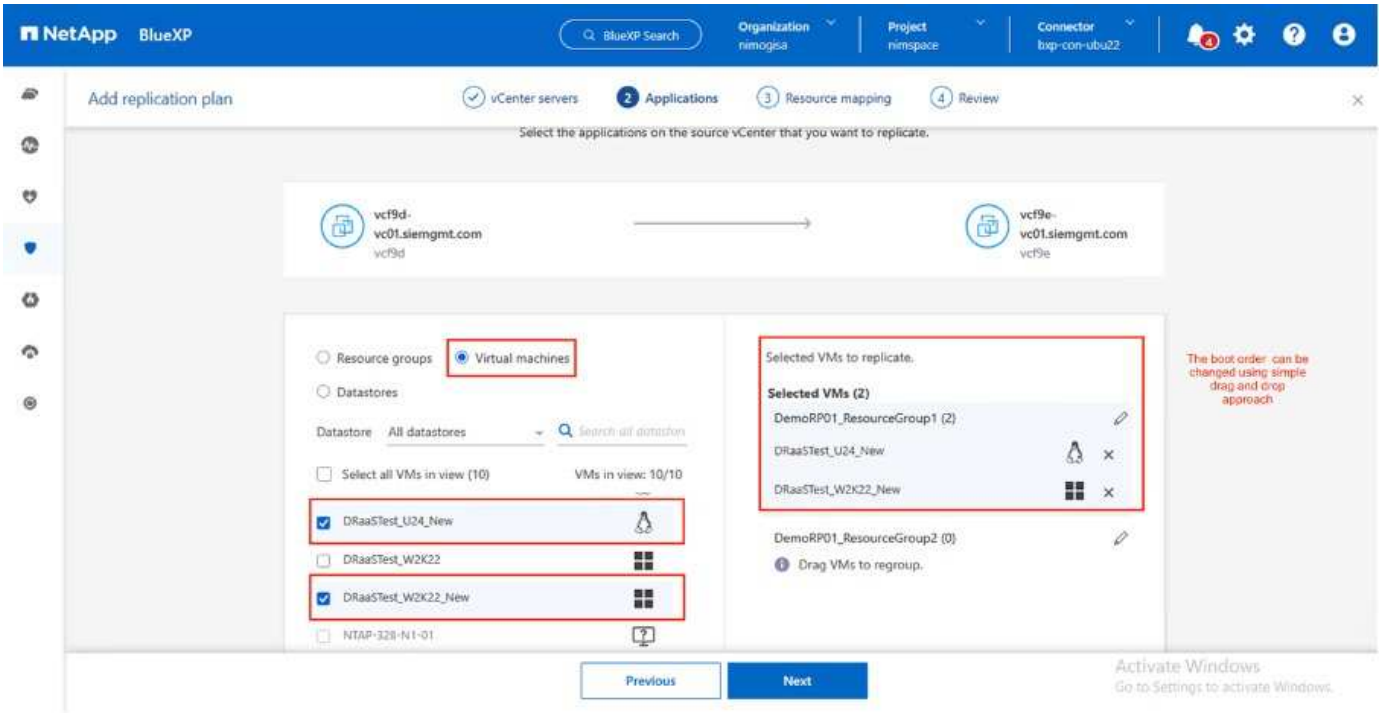
Adicionar Plano.

Nesta etapa, as VMs podem ser agrupadas em grupos de recursos. Os grupos de recursos de BlueXP disaster recovery permitem que você agrupe um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização e atrasos de inicialização que podem ser executados na recuperação. O grupo de recursos também pode ser criado usando a guia Grupo de recursos.

Primeiro, selecione o vCenter de origem e depois selecione o vCenter de destino.



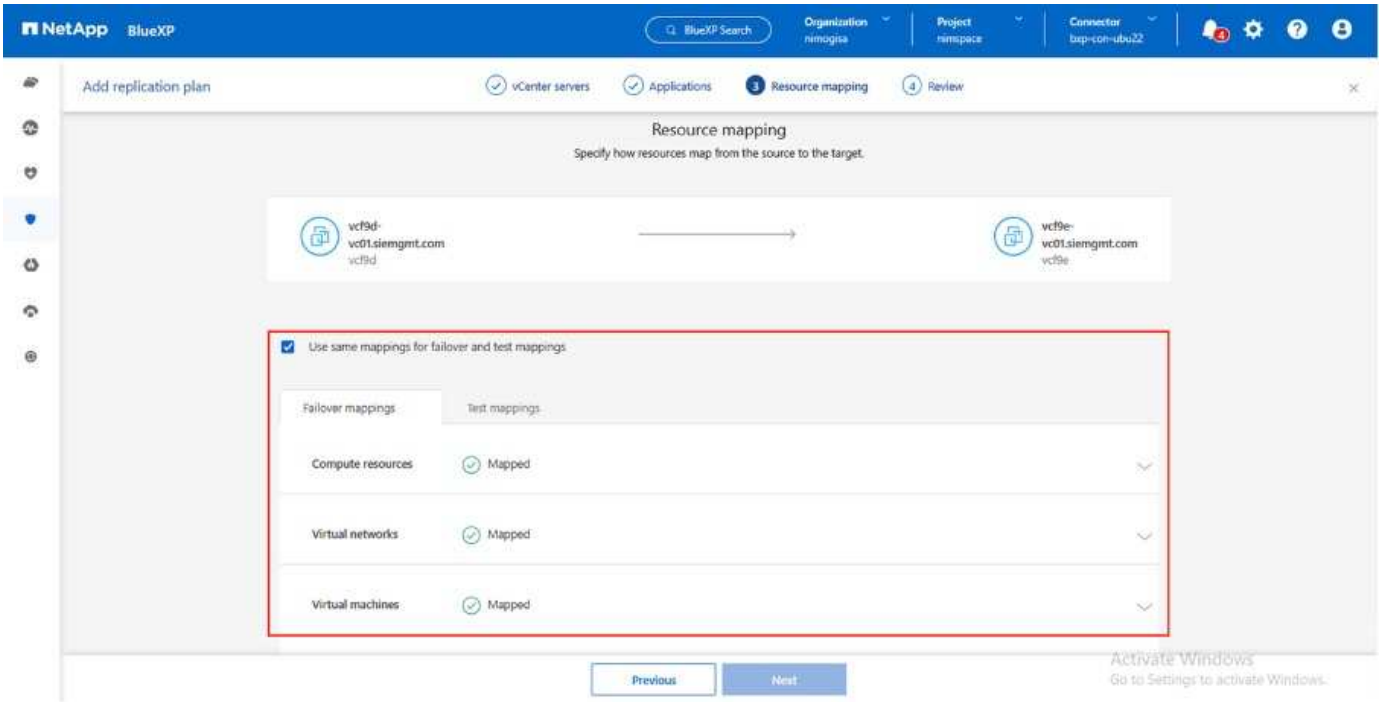
O próximo passo é selecionar grupos de recursos existentes. Se nenhum grupo de recursos for criado, o assistente ajudará a agrupar as máquinas virtuais necessárias (basicamente, criar grupos de recursos funcionais) com base nos objetivos de recuperação. Isso também ajuda a definir a sequência de operação de como as máquinas virtuais do aplicativo devem ser restauradas.



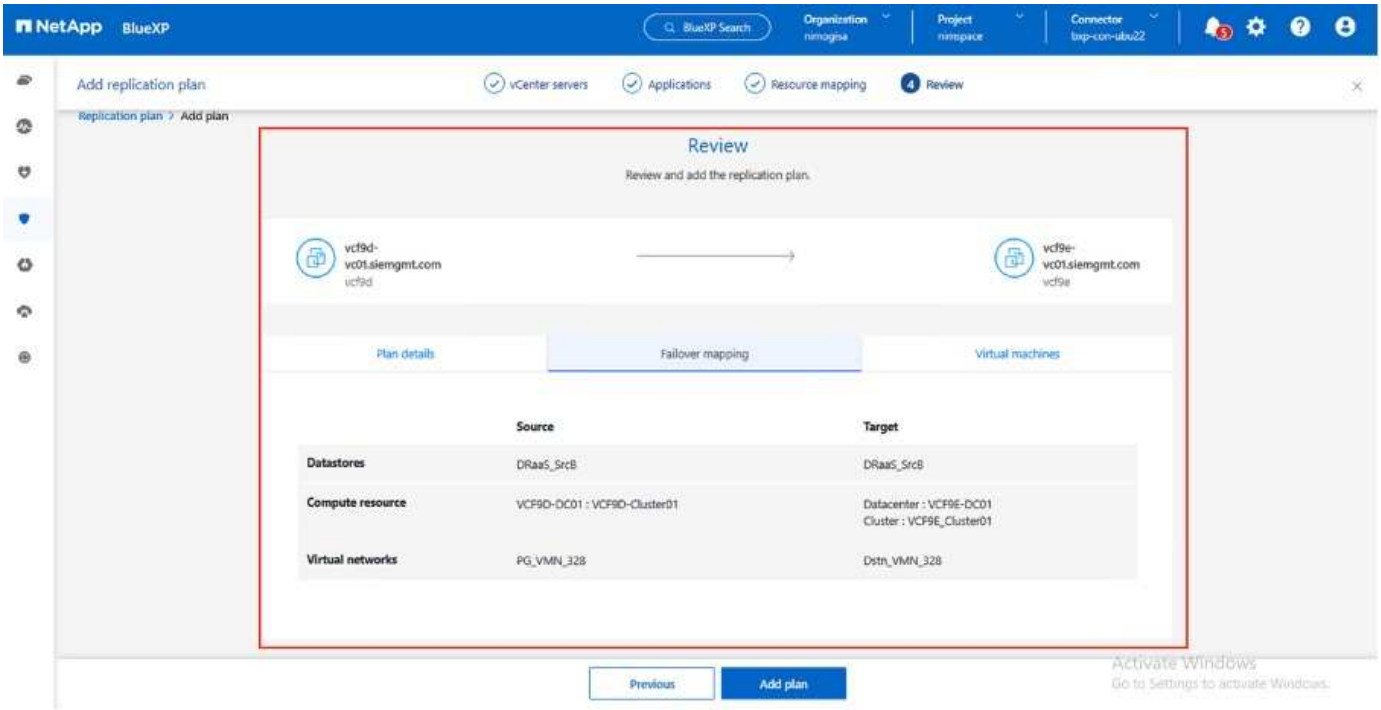
O grupo de recursos permite definir a ordem de inicialização usando a funcionalidade de arrastar e soltar. Ele pode ser usado para modificar facilmente a ordem em que as VMs serão ligadas durante o processo de recuperação.

Depois que os grupos de recursos são criados por meio do plano de replicação, a próxima etapa é selecionar o blueprint ou um mapeamento para recuperar máquinas virtuais e aplicativos em caso de desastre. Nesta etapa, especifique como os recursos do ambiente de origem são mapeados para o destino. Isso inclui recursos de computação, redes virtuais, personalização de IP, pré e pós-scripts, atrasos de inicialização, consistência de aplicativos e assim por diante. Para obter informações detalhadas, consulte"Crie um plano de replicação" . Conforme mencionado nos pré-requisitos, a replicação do SnapMirror pode ser configurada antecipadamente ou o DRaaS pode configurá-la usando o RPO e a contagem de retenção especificados durante a criação do plano de replicação.

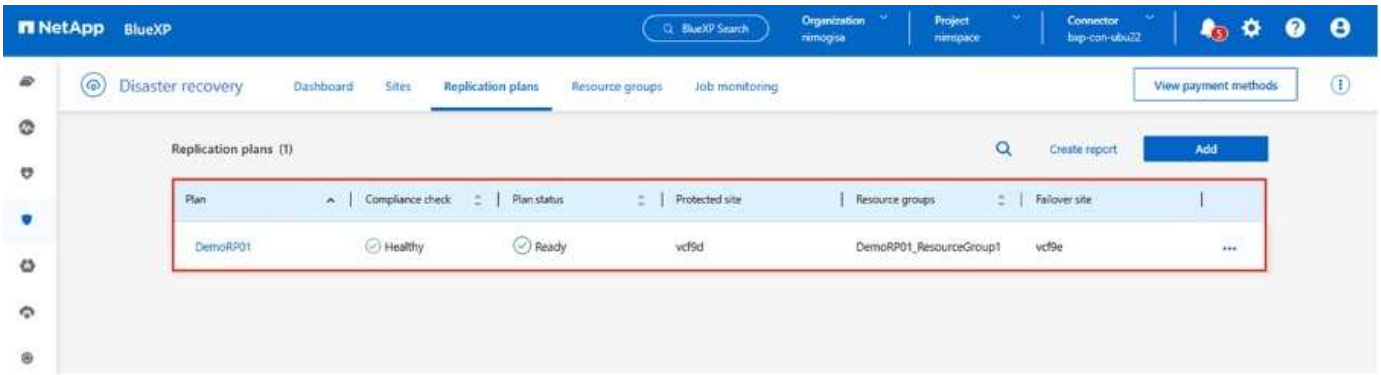
Observação: por padrão, os mesmos parâmetros de mapeamento são usados para operações de teste e failover. Para definir mapeamentos diferentes para o ambiente de teste, selecione a opção Mapeamento de teste após desmarcar a caixa de seleção “Usar os mesmos mapeamentos para failover e mapeamentos de teste”. Quando o mapeamento de recursos estiver concluído, clique em Avançar.



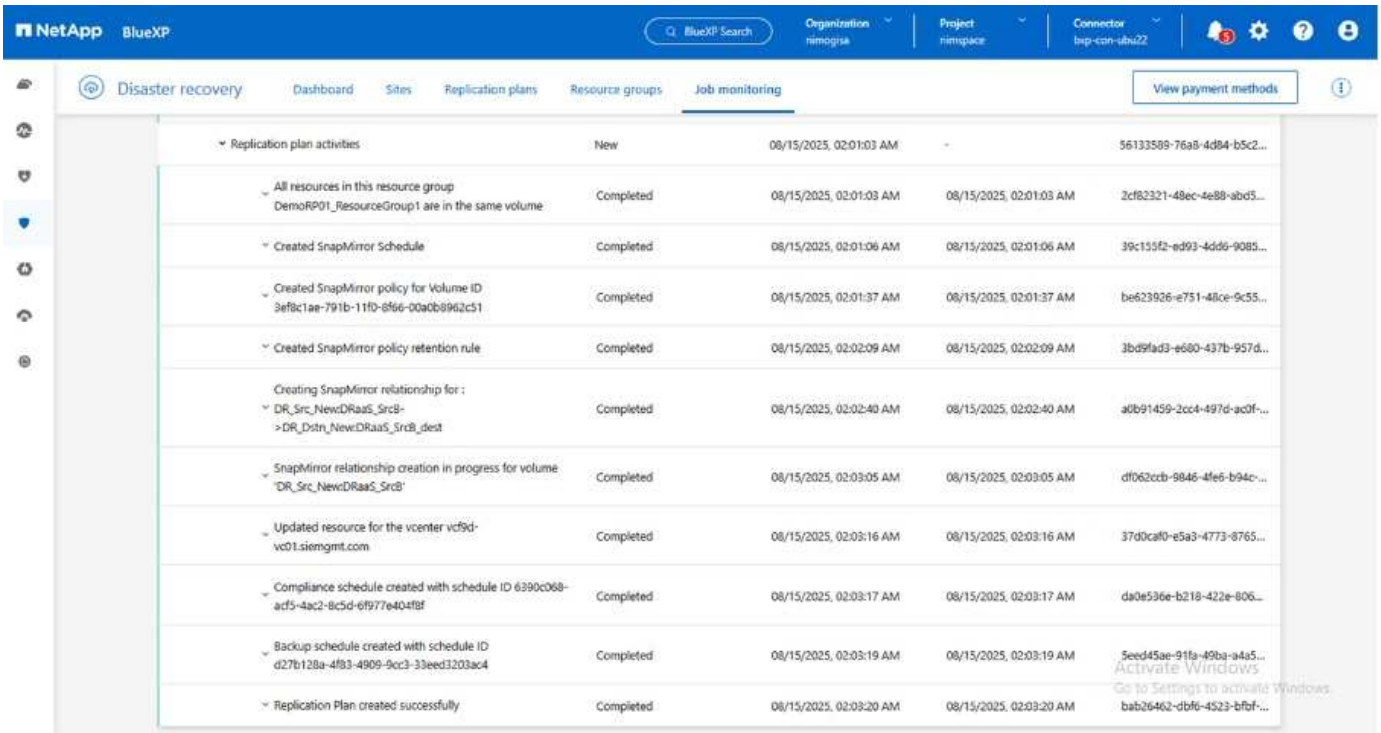
Uma vez concluído, revise os mapeamentos criados e clique em Adicionar plano.



VMs de diferentes volumes e SVMs podem ser incluídas em um plano de replicação. Dependendo do posicionamento da VM (seja no mesmo volume ou em volumes separados dentro da mesma SVM, volumes separados em SVMs diferentes), a BlueXP disaster recovery cria um instantâneo de grupo de consistência.

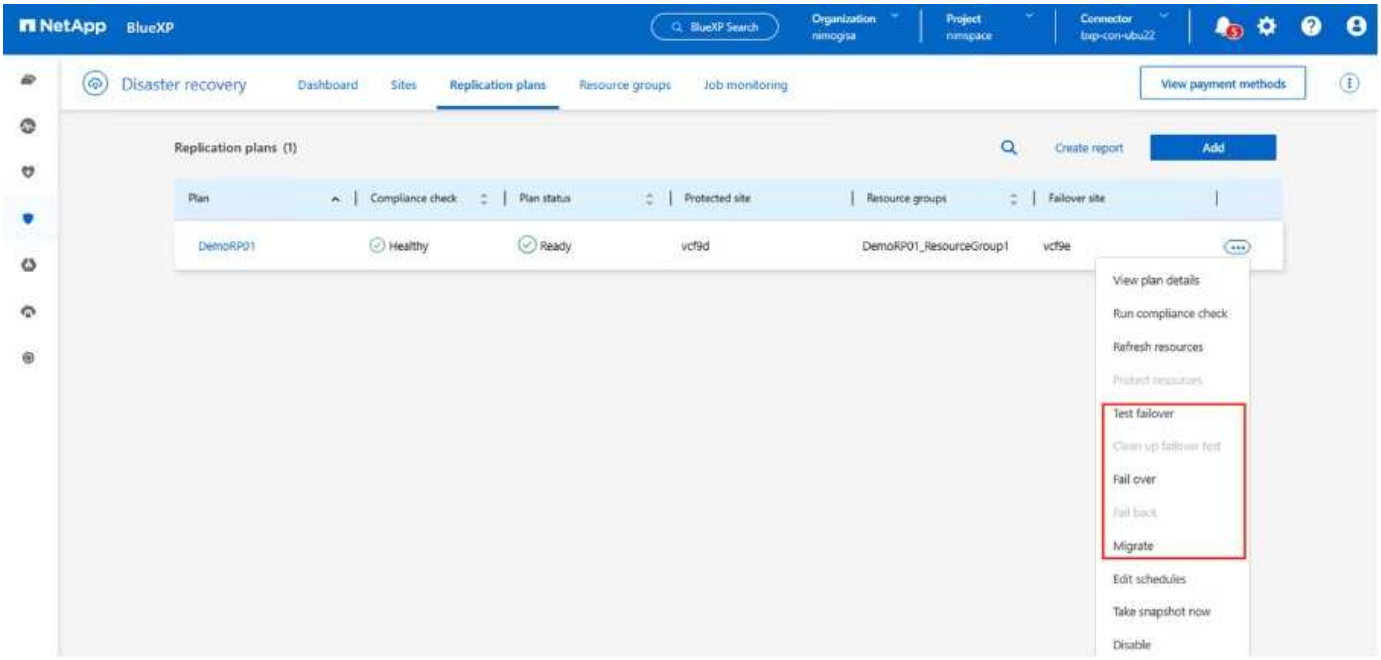


Assim que o plano é criado, uma série de validações são acionadas e a replicação e os agendamentos do SnapMirror são configurados conforme a seleção.



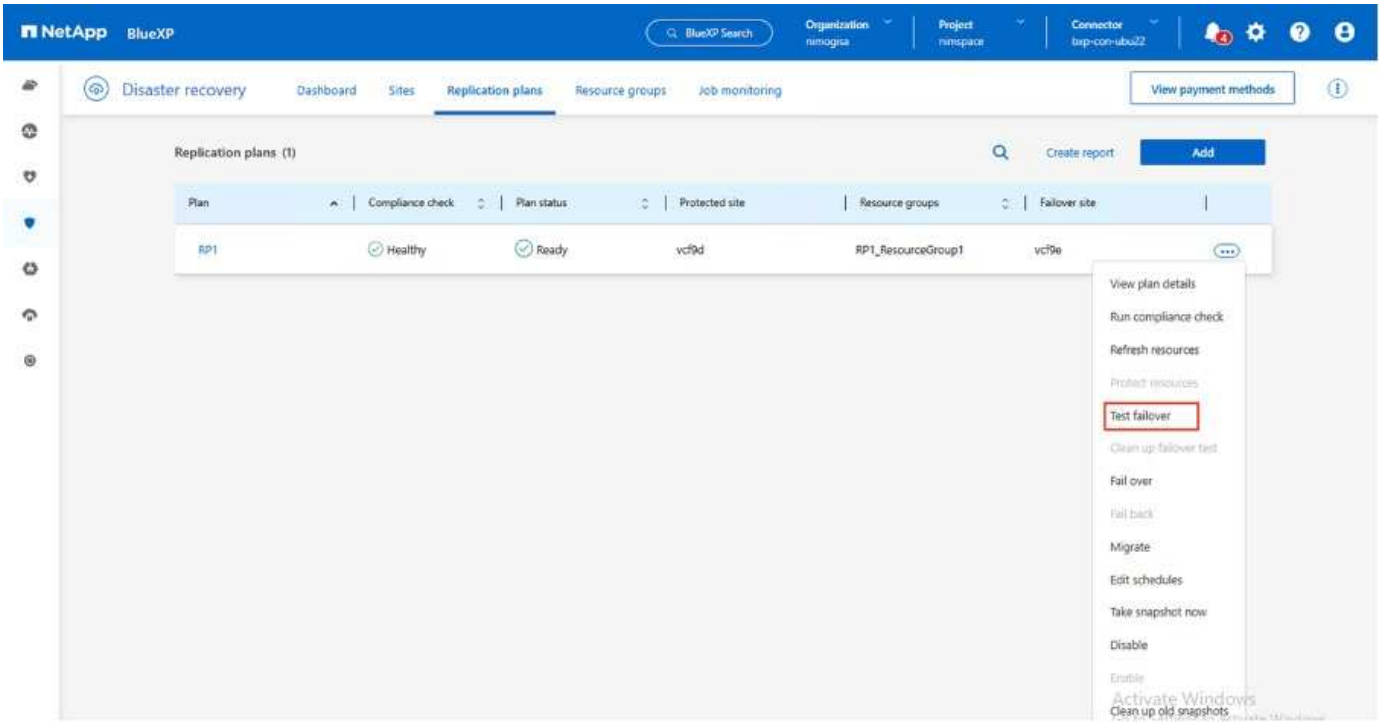
O BlueXP DRaaS consiste nos seguintes fluxos de trabalho:

- Teste de failover (incluindo simulações automatizadas periódicas)
- Teste de failover de limpeza
- Failover:
  - Migração planejada (estender o caso de uso para failover único)
  - Recuperação de desastres
- Failback

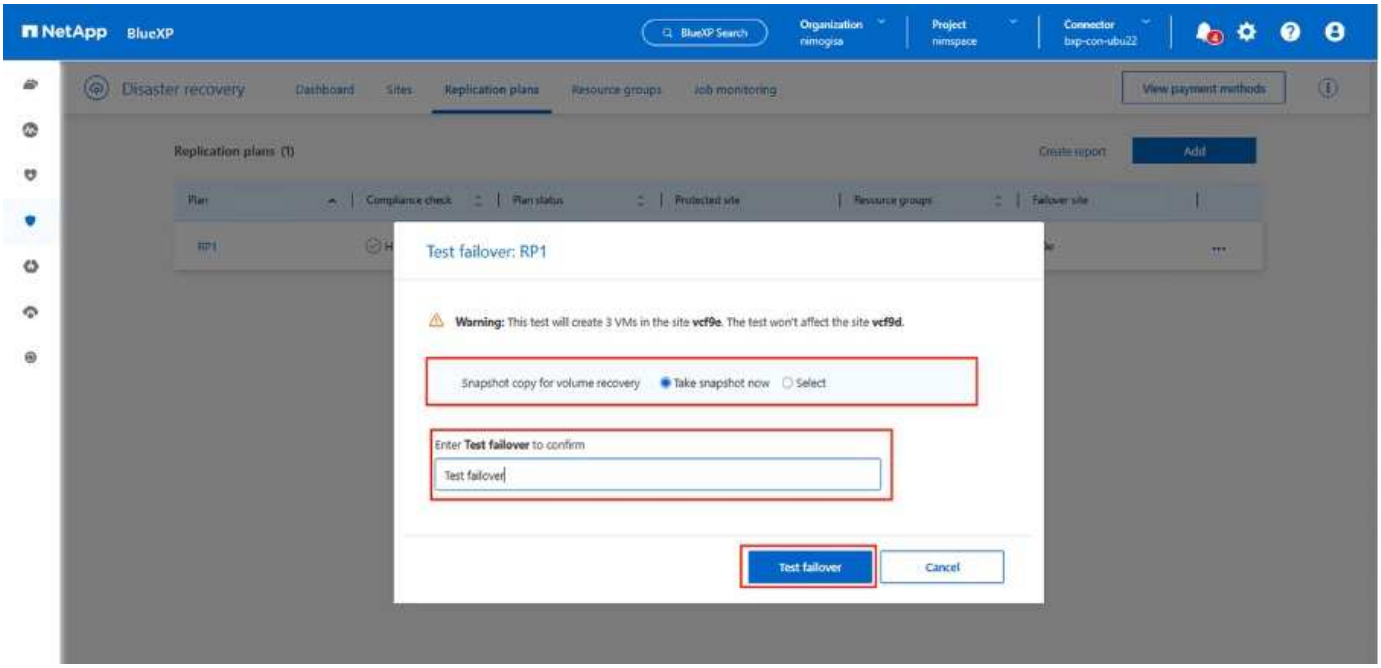


Teste de failover

O failover de teste no BlueXP DRaaS é um procedimento operacional que permite que os administradores do VMware validem totalmente seus planos de recuperação sem interromper seus ambientes de produção.

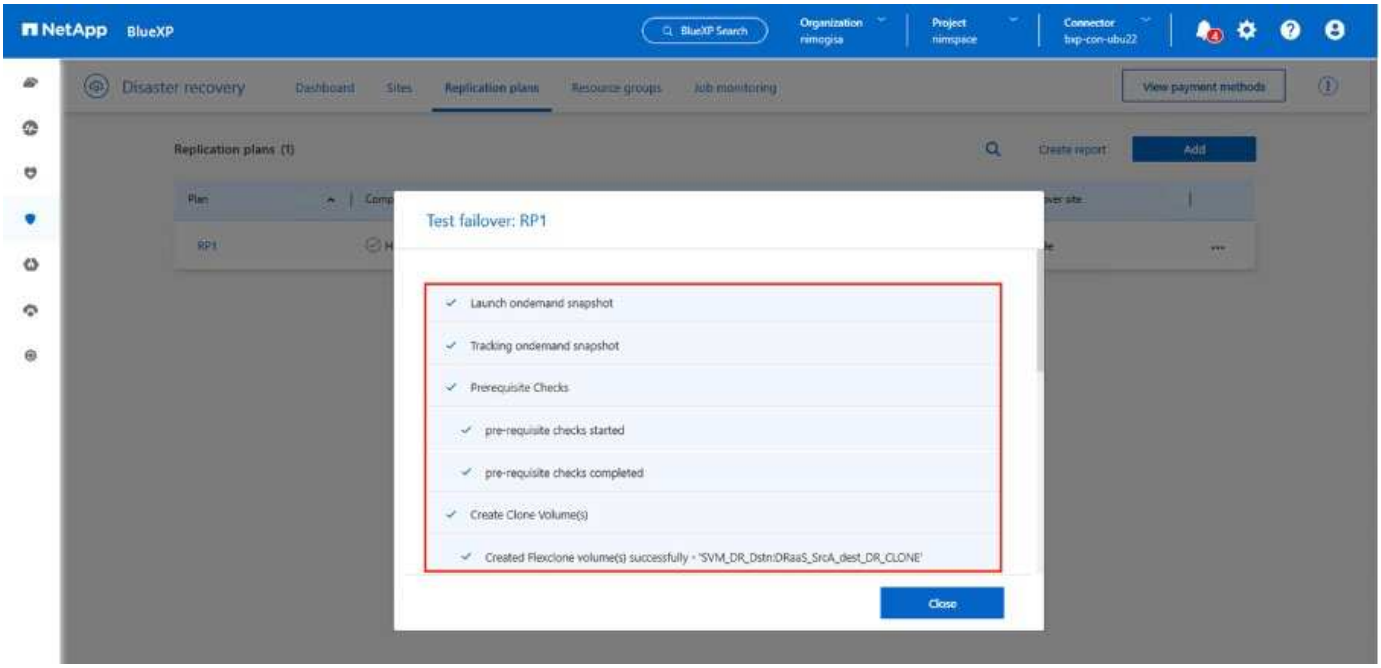


O BlueXP DRaaS incorpora a capacidade de selecionar o snapshot como um recurso opcional na operação de failover de teste. Esse recurso permite que o administrador do VMware verifique se quaisquer alterações feitas recentemente no ambiente são replicadas no site de destino e, portanto, estão presentes durante o teste. Essas mudanças incluem patches para o sistema operacional convidado da VM.



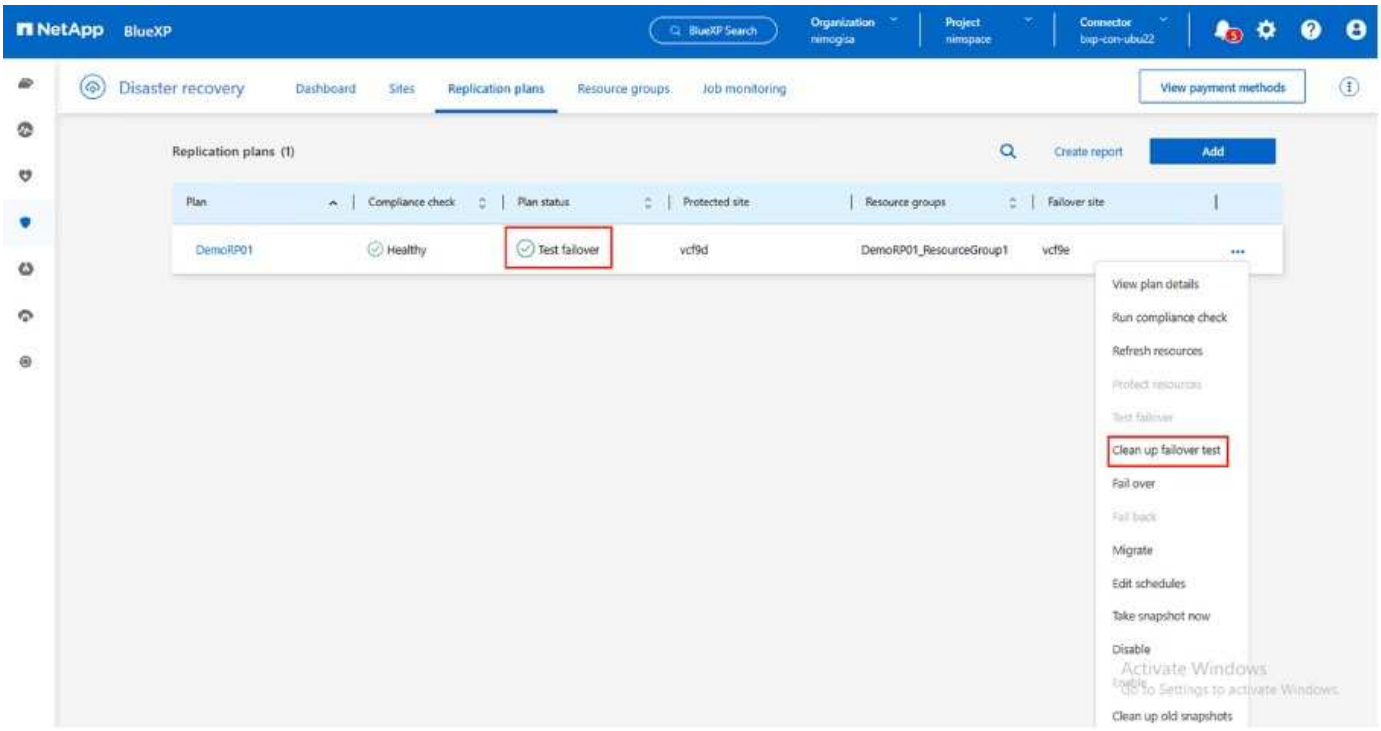
Quando o administrador do VMware executa uma operação de failover de teste, o BlueXP DRaaS automatiza as seguintes tarefas:

- Acionar relacionamentos do SnapMirror para atualizar o armazenamento no site de destino com quaisquer alterações recentes feitas no site de produção.
- Criação de volumes NetApp FlexClone dos volumes FlexVol no array de armazenamento DR.
- Conectando os datastores nos volumes FlexClone aos hosts ESXi no site de DR.
- Conectando os adaptadores de rede da VM à rede de teste especificada durante o mapeamento.
- Reconfigurando as configurações de rede do sistema operacional convidado da VM, conforme definido para a rede no site de DR.
- Executar quaisquer comandos personalizados que tenham sido armazenados no plano de replicação.
- Ligar as VMs na ordem definida no plano de replicação.



Operação de teste de failover de limpeza

A operação de teste de failover de limpeza ocorre após a conclusão do teste do plano de replicação e o administrador do VMware responde ao prompt de limpeza.

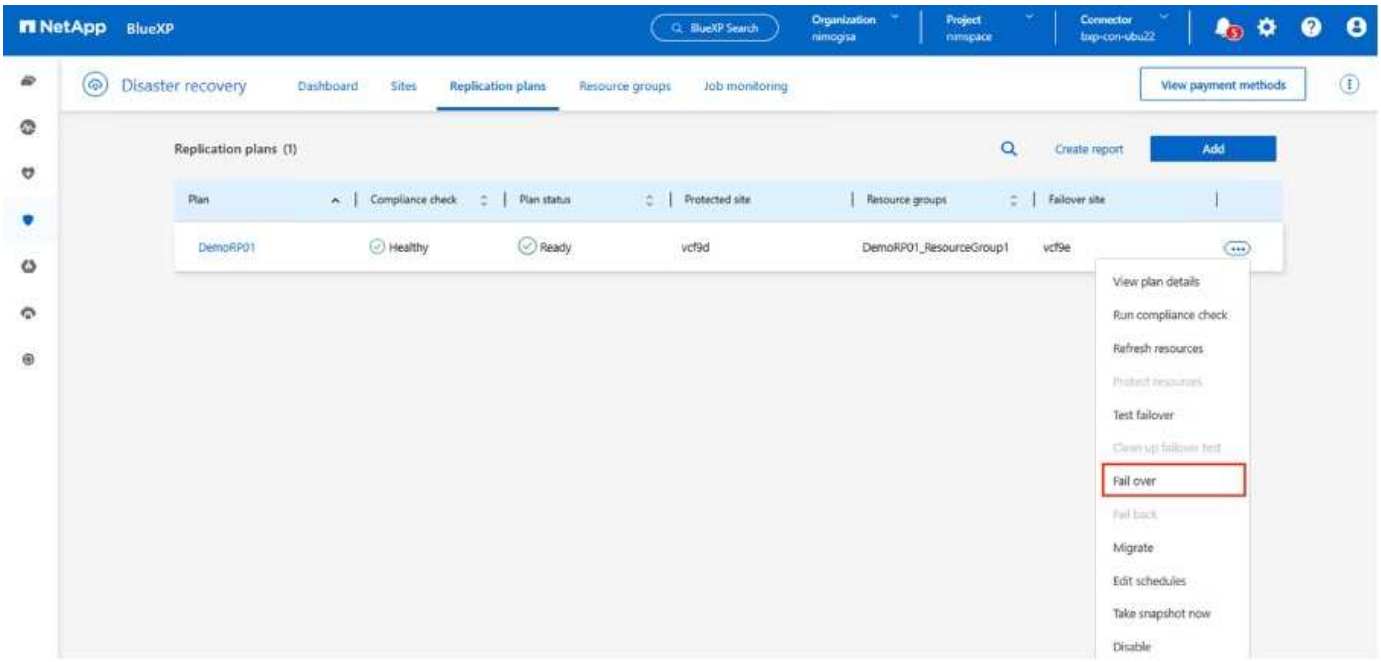


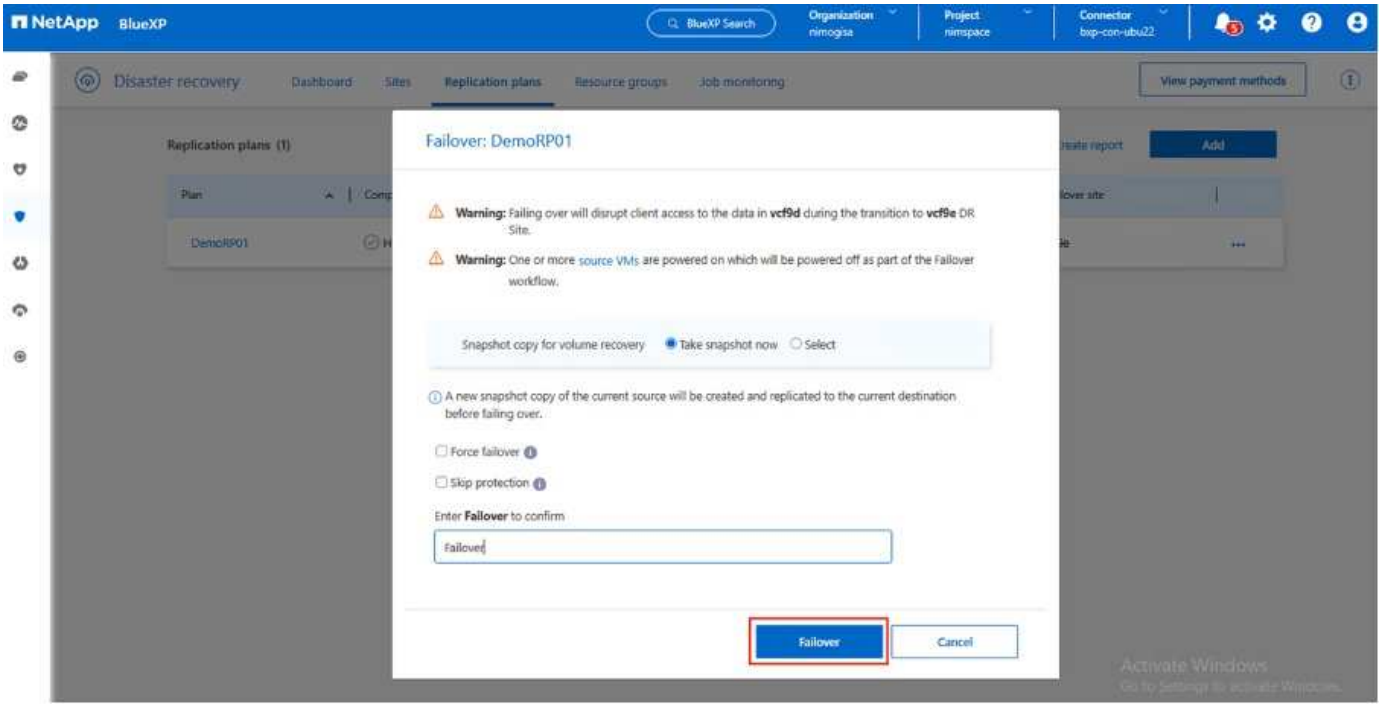
Esta ação redefinirá as máquinas virtuais (VMs) e o status do plano de replicação para o estado pronto. Quando o administrador do VMware executa uma operação de recuperação, o BlueXP DRaaS conclui o seguinte processo:

1. Ele desliga cada VM recuperada na cópia do FlexClone que foi usada para teste.
2. Ele exclui o volume FlexClone que foi usado para apresentar as VMs recuperadas durante o teste.

Migração planejada e failover

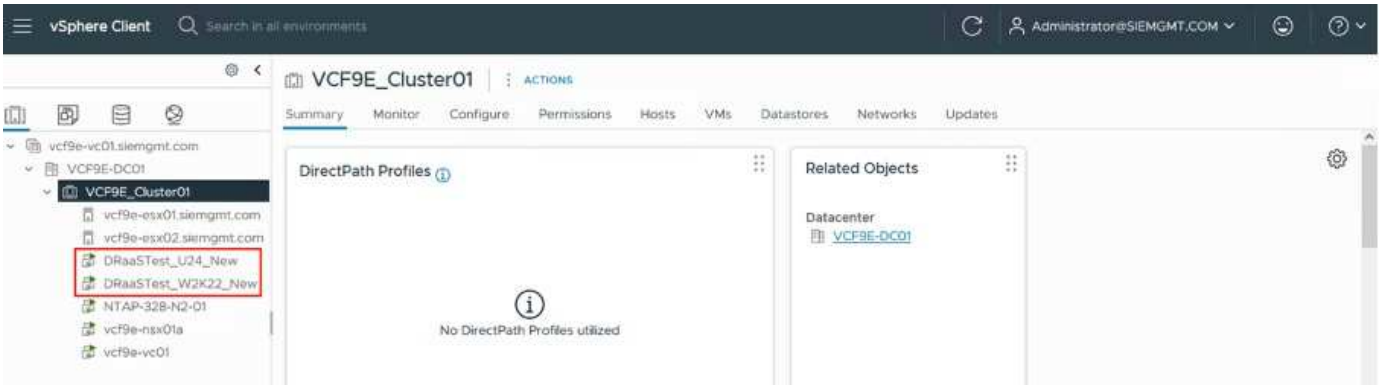
O BlueXP DRaaS tem dois métodos para executar um failover real: migração planejada e failover. O primeiro método, migração planejada, incorpora o desligamento da VM e a sincronização da replicação do armazenamento no processo para recuperar ou mover efetivamente as VMs para o site de destino. A migração planejada requer acesso ao site de origem. O segundo método, failover, é um failover planejado/não planejado no qual as VMs são recuperadas no site de destino a partir do último intervalo de replicação de armazenamento que foi concluído. Dependendo do RPO que foi projetado na solução, alguma perda de dados pode ser esperada no cenário de DR.





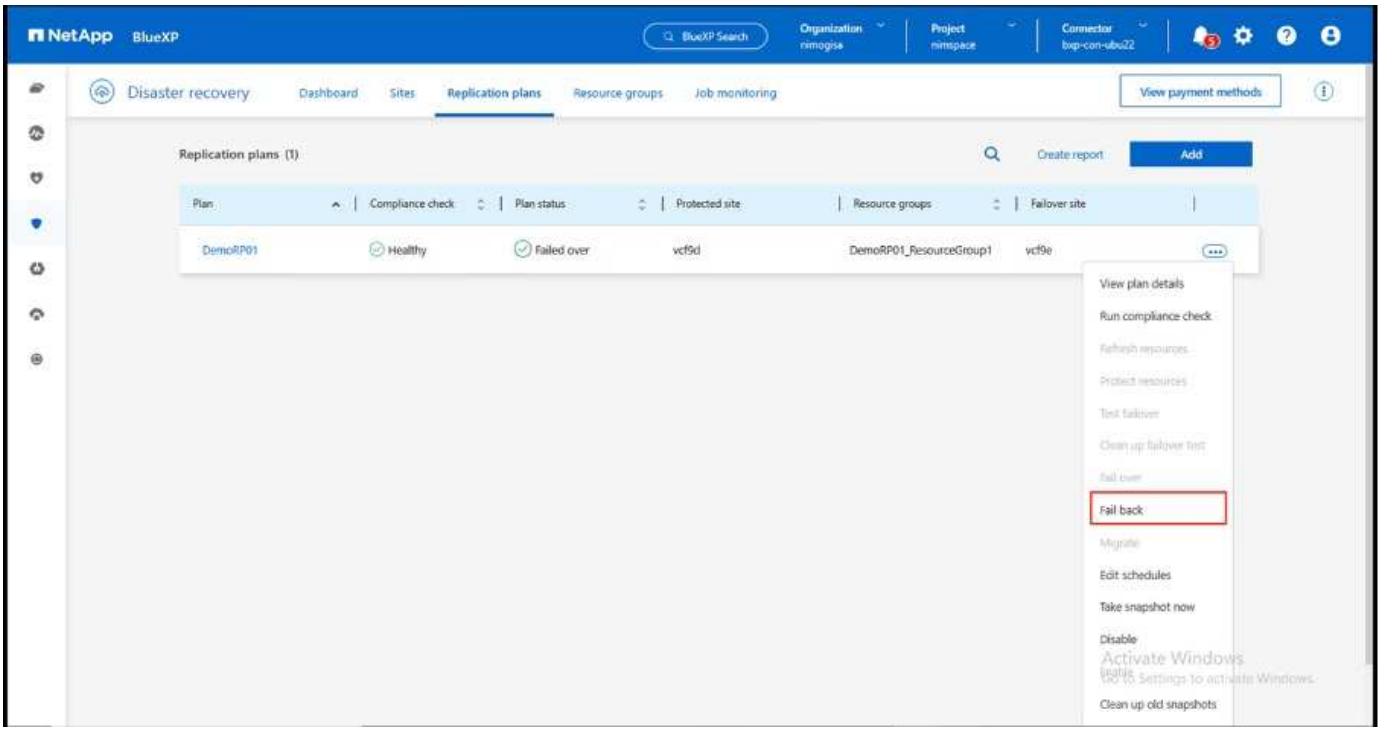
Quando o administrador do VMware executa uma operação de failover, o BlueXP DRaaS automatiza as seguintes tarefas:

- Interrompa e faça failover dos relacionamentos do NetApp SnapMirror .
- Conecte os armazenamentos de dados replicados aos hosts ESXi no site de DR.
- Conecte os adaptadores de rede da VM à rede do site de destino apropriada.
- Reconfigure as configurações de rede do sistema operacional convidado da VM, conforme definido para a rede no site de destino.
- Execute quaisquer comandos personalizados (se houver) que tenham sido armazenados no plano de replicação.
- Ligue as VMs na ordem definida no plano de replicação.



Failback

Um failback é um procedimento opcional que restaura a configuração original dos sites de origem e destino após uma recuperação.

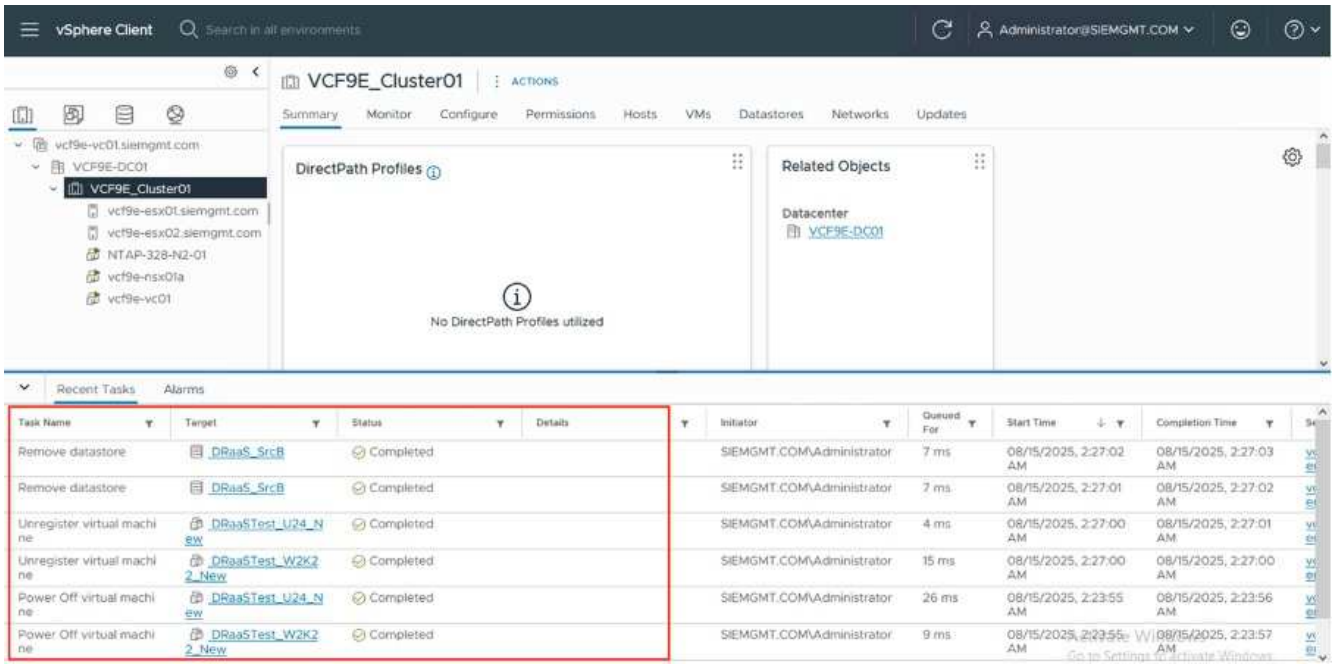


Os administradores do VMware podem configurar e executar um procedimento de failback quando estiverem prontos para restaurar serviços no site de origem original.

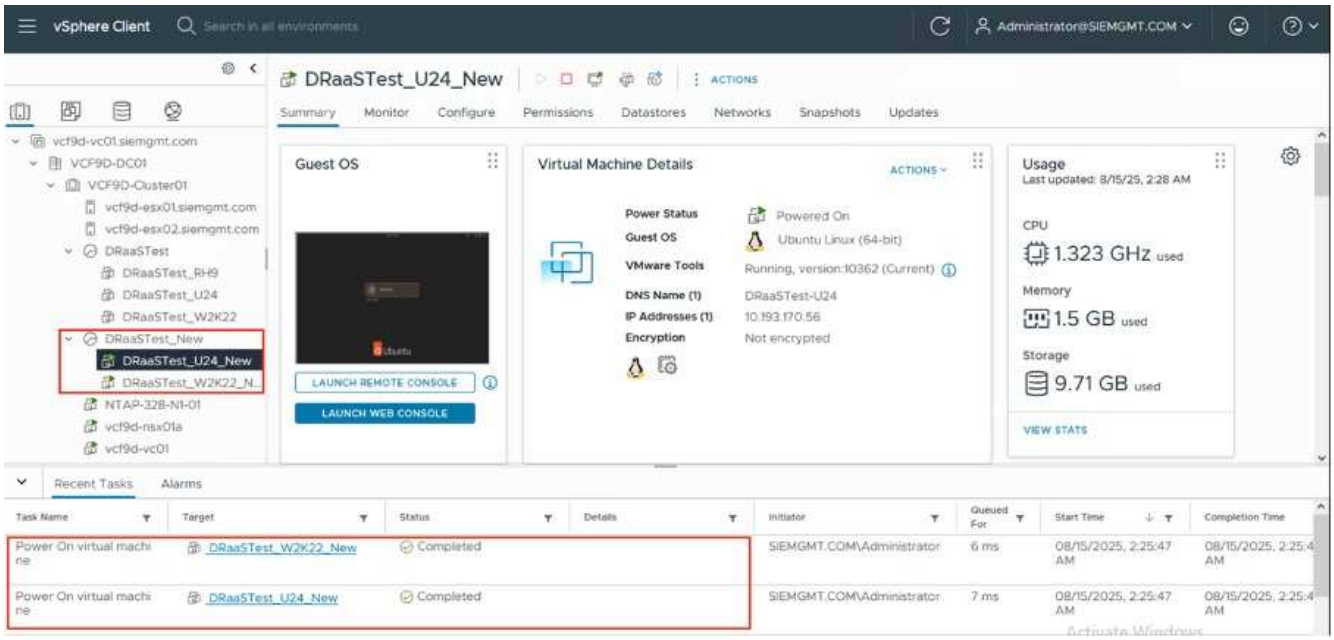
O BlueXP DRaaS replica (ressincroniza) quaisquer alterações de volta para a máquina virtual de origem antes de reverter a direção da replicação.

Esse processo começa com um relacionamento que concluiu o failover para um alvo e envolve as seguintes etapas:

- Desligue e cancele o registro das máquinas virtuais e os volumes no site de destino serão desmontados.



- Interrompa o relacionamento SnapMirror na fonte original para torná-lo de leitura/gravação.
- Ressincronize o relacionamento do SnapMirror para reverter a replicação.
- Monte o volume na origem, ligue e registre as máquinas virtuais de origem.

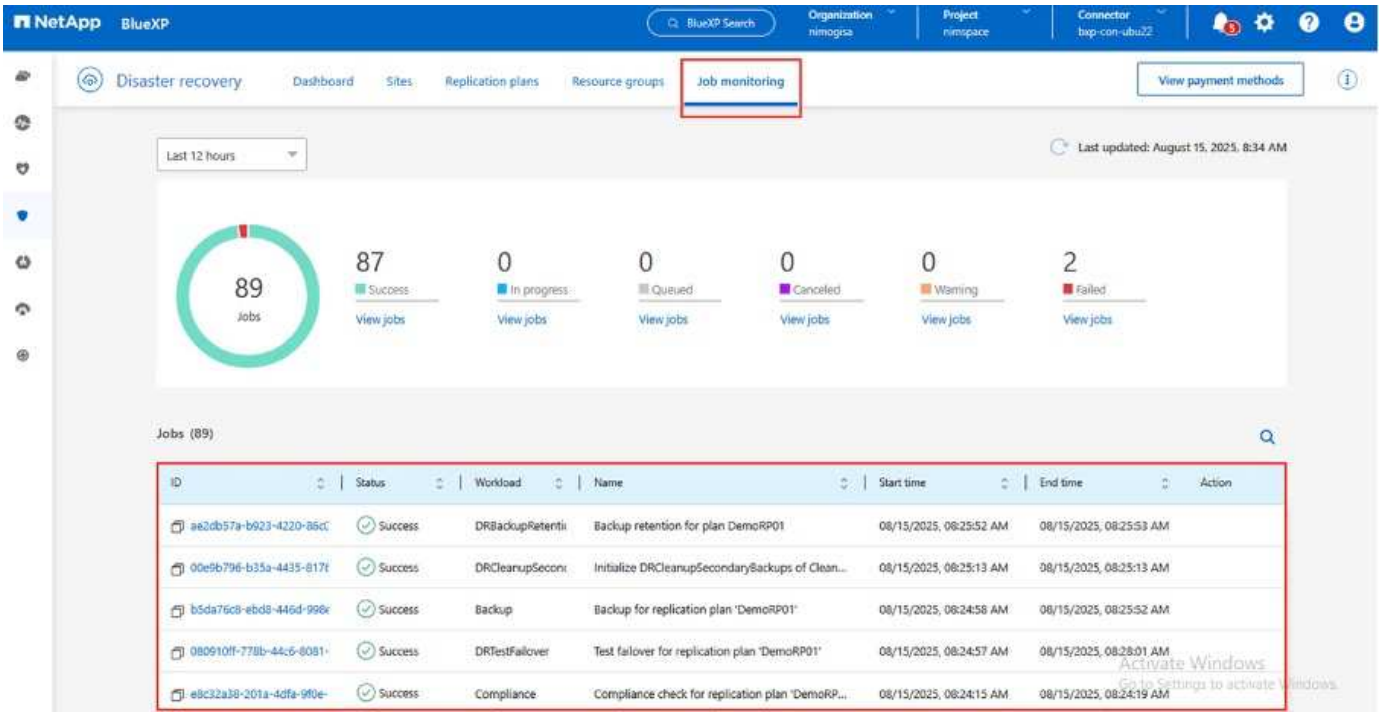


Para obter mais detalhes sobre como acessar e configurar o BlueXP DRaaS, consulte o"Saiba mais sobre o

BlueXP Disaster Recovery para VMware" .

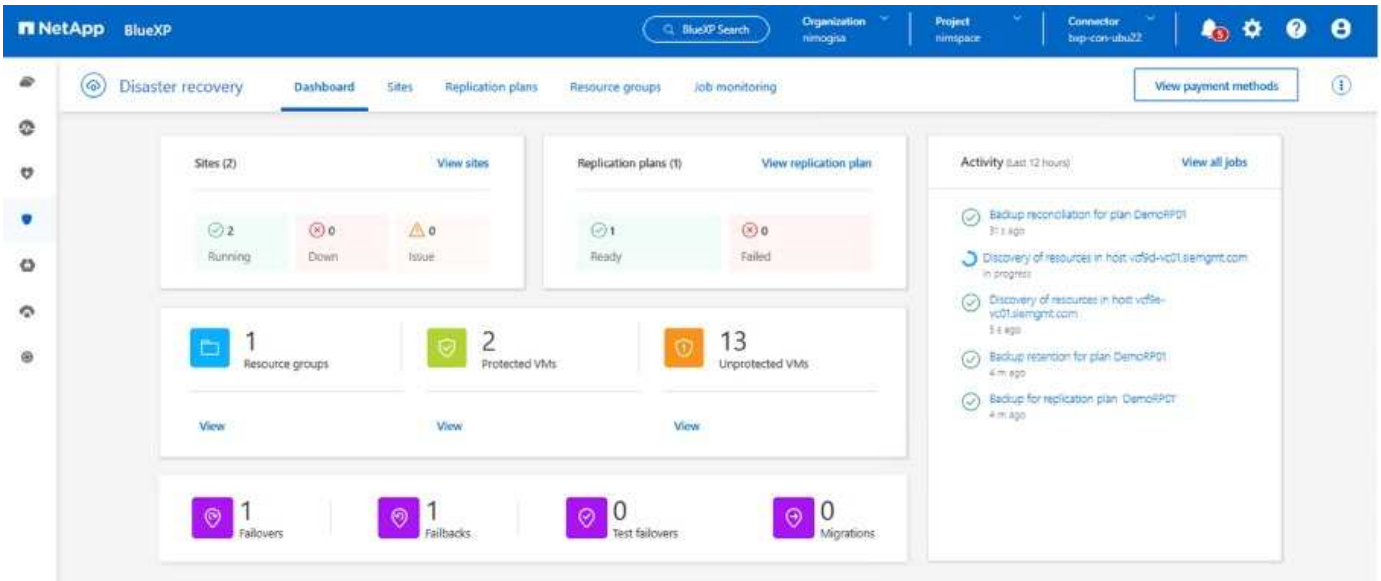
Monitoramento e Painel

No BlueXP ou no ONTAP CLI, você pode monitorar o status de integridade da replicação para os volumes de armazenamento de dados apropriados, e o status de um failover ou failover de teste pode ser rastreado por meio do Monitoramento de tarefas.



Se um trabalho estiver em andamento ou na fila e você desejar interrompê-lo, há uma opção para cancelá-lo.

Com o painel de BlueXP disaster recovery , avalie com confiança o status dos sites de recuperação de desastres e dos planos de replicação. Isso permite que os administradores identifiquem rapidamente sites e planos saudáveis, desconectados ou degradados.



Isso fornece uma solução poderosa para lidar com um plano de recuperação de desastres personalizado e personalizado. O failover pode ser feito como failover planejado ou failover com o clique de um botão quando ocorre um desastre e é tomada a decisão de ativar o site de DR.

Converter clusters vSphere existentes em VCF

Saiba mais sobre como converter um ambiente vSphere com armazenamentos de dados existentes para VCF

A conversão de um ambiente vSphere com armazenamentos de dados existentes em execução no ONTAP em um ambiente VMware Cloud Foundation (VCF) envolve a integração da infraestrutura atual em uma arquitetura de nuvem privada moderna.

Este processo aproveita a flexibilidade do armazenamento ONTAP para acesso e gerenciamento de dados contínuos. Depois que o domínio de gerenciamento do VCF estiver estabelecido, os administradores poderão importar com eficiência ambientes vSphere adicionais para o ecossistema do VCF. Essa integração melhora a utilização de recursos, simplifica o gerenciamento de nuvem privada e garante uma transição tranquila com interrupção mínima nas cargas de trabalho existentes.

Consulte as soluções a seguir para obter detalhes técnicos sobre a conversão de uma instância do vCenter.

- "Converter instância existente do vCenter em domínio de gerenciamento VCF (NFS)"
- "Converter instância do vCenter (armazenamento de dados FC) em domínio de gerenciamento VCF"

Converter instância do servidor vCenter em domínio de gerenciamento VCF (armazenamento de dados NFS)

Converta um cluster vSphere 8 existente com datastores NetApp ONTAP NFS em um domínio de gerenciamento VMware Cloud Foundation (VCF). Este procedimento inclui o provisionamento de armazenamento NFS, a implantação de ferramentas ONTAP para VMware e o uso da Ferramenta de Importação VCF para converter o cluster para gerenciamento simplificado e utilização otimizada de recursos dentro do VCF.

Introdução

A conversão de um cluster com um armazenamento de dados NFS existente em execução no ONTAP envolve a integração da infraestrutura existente em uma arquitetura de nuvem privada moderna. Este processo se beneficia da flexibilidade do armazenamento NFS, para garantir acesso e gerenciamento de dados contínuos. Depois que um domínio de gerenciamento do VCF é estabelecido por meio do processo de conversão, os administradores podem importar com eficiência clusters adicionais do vSphere, incluindo aqueles que usam armazenamentos de dados NFS, para o ecossistema do VCF. Essa integração não apenas melhora a utilização de recursos, mas também simplifica o gerenciamento da infraestrutura de nuvem privada, garantindo uma transição tranquila com interrupção mínima nas cargas de trabalho existentes.

Nesta solução, demonstraremos como um armazenamento de dados NFS no vSphere 8 se torna armazenamento principal quando o cluster é convertido em um domínio de gerenciamento VCF.

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Implante ONTAP tools for VMware vSphere 10.
- Provisione um armazenamento de dados NFS usando ferramentas ONTAP .
- Use a Ferramenta de Importação VCF para validar o cluster vSphere.
- Implante o SDDC Manager no cluster vSphere.
- Configure um arquivo JSON para criar o NSX durante a conversão do VCF.
- Use a ferramenta de importação VCF para converter o cluster vSphere 8 para VCF 5.2.

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Sistema de armazenamento NetApp AFF com uma máquina virtual de armazenamento (SVM) configurada para permitir tráfego NFS.
- A interface lógica (LIF) foi criada na rede IP que transportará o tráfego NFS e está associada ao SVM.
- Um cluster vSphere 8 com 4 hosts ESXi e um dispositivo vCenter colocalizados no cluster.
- Grupo de portas distribuídas configurado para tráfego de armazenamento vMotion e NFS nas VLANs ou segmentos de rede estabelecidos para essa finalidade.
- Baixe o software necessário para a conversão de VCF.

As ONTAP tools for VMware vSphere 10 podem ser instaladas em configurações HA ou não HA. Para obter informações completas sobre os pré-requisitos para ferramentas ONTAP , consulte "Pré-requisitos para ONTAP tools for VMware vSphere" .

Para armazenamento suportado e outras considerações para conversão ou importação do vSphere para VCF 5.2, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

Para o software necessário, vá para "Portal de Suporte Broadcom" .

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Etapas de implantação

A solução abrange o uso de ONTAP tools for VMware vSphere para provisionar armazenamentos de dados NFS e o processo de conversão de um cluster vSphere 8 existente em um domínio de gerenciamento VCF.

Conclua as seguintes etapas:

- Implante ONTAP tools for VMware vSphere 10.
- Provisione um armazenamento de dados NFS usando ferramentas ONTAP .
- Copie a ferramenta de importação VCF para o dispositivo vCenter.
- Execute uma pré-verificação no dispositivo vCenter usando a Ferramenta de Importação VCF.
- Implante a VM do gerenciador do SDDC no cluster do vCenter.
- Crie um arquivo JSON para um cluster NSX a ser implantado durante o processo de conversão.

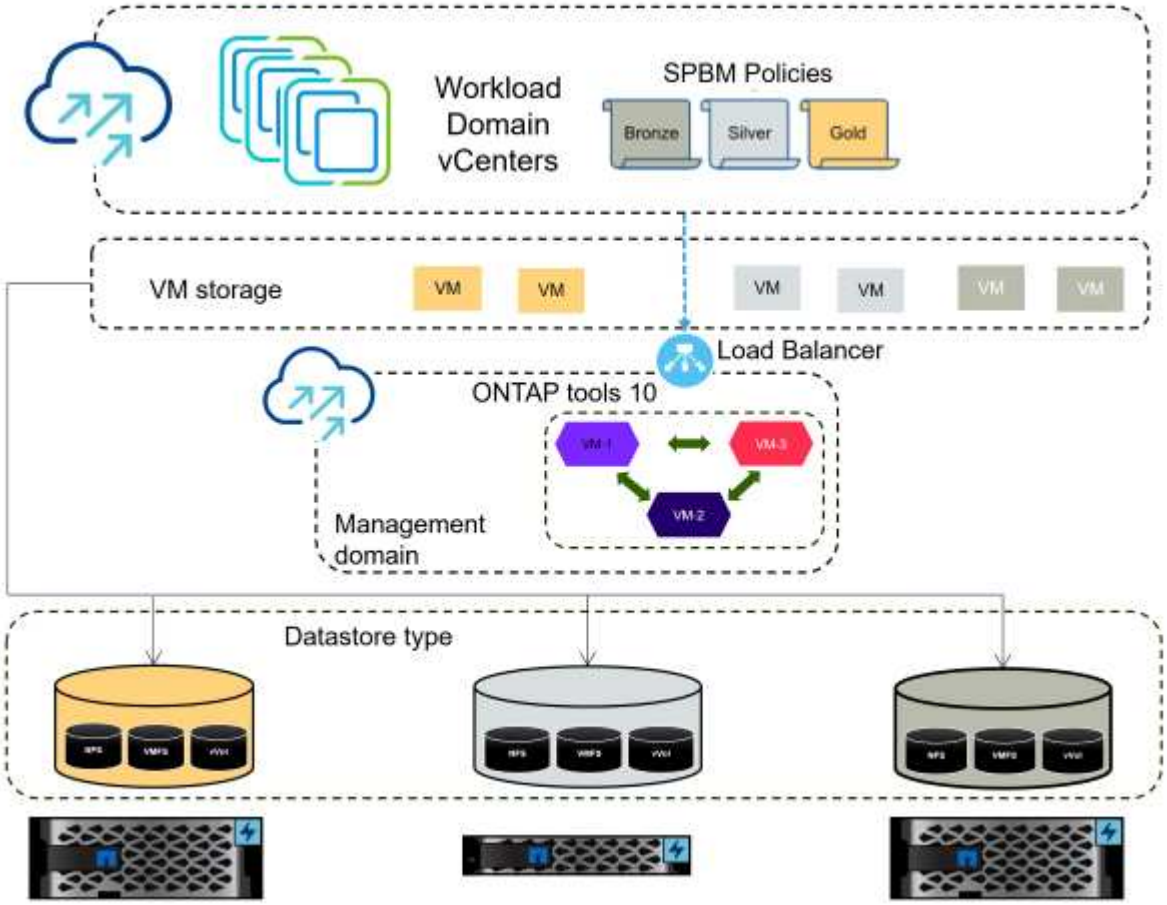
- Carregue o software necessário para o gerenciador do SDDC.
- Converta o cluster do vSphere no inventário do gerenciador do SDDC.

Para uma visão geral do processo de conversão, consulte "Converter um ambiente vSphere em um domínio de gerenciamento ou importar um ambiente vSphere como um domínio de carga de trabalho VI no VMware Cloud Foundation" .

Implantar ferramentas ONTAP e provisionar um armazenamento de dados NFS

A arquitetura das ferramentas ONTAP 10 foi projetada para integrar-se perfeitamente aos ambientes VMware, aproveitando uma estrutura modular e escalável que inclui os serviços das ferramentas ONTAP , o plug-in vSphere e as APIs REST para permitir gerenciamento de armazenamento eficiente, automação e proteção de dados.

As ONTAP tools for VMware vSphere 10 podem ser instaladas em configurações HA ou não HA.

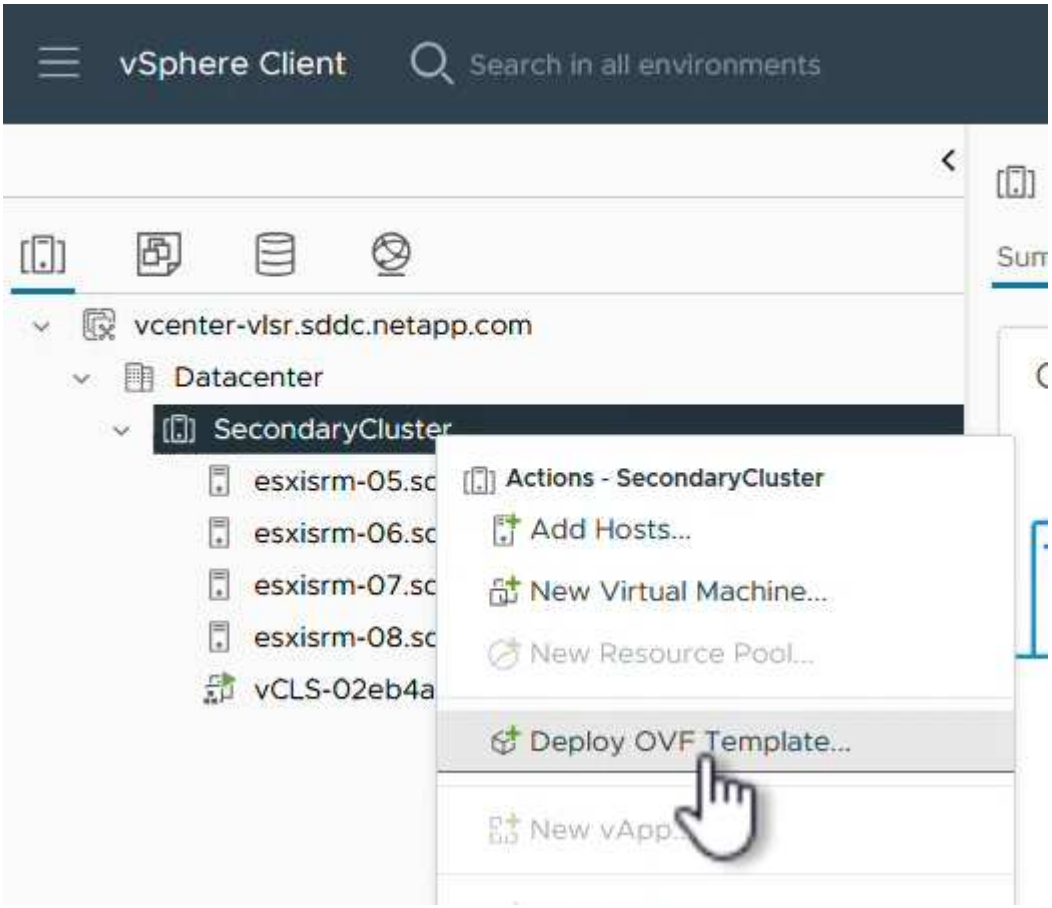


Implantar ONTAP tools for VMware vSphere 10

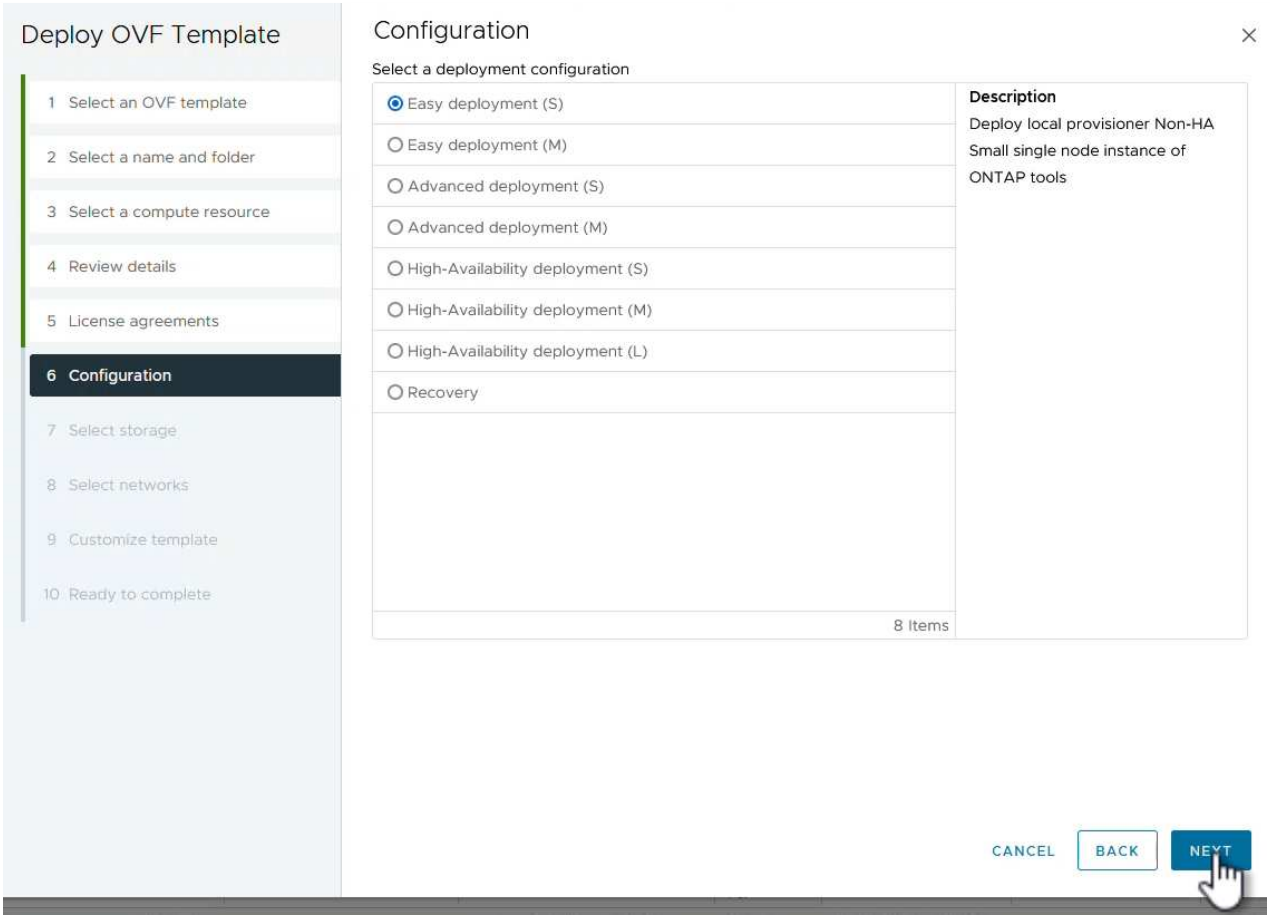
Nesta etapa, o ONTAP Tools 10 é implantado com uma configuração não HA.

Para obter detalhes adicionais de implantação em configurações HA e não HA, consulte "Implantar ONTAP tools for VMware vSphere" .

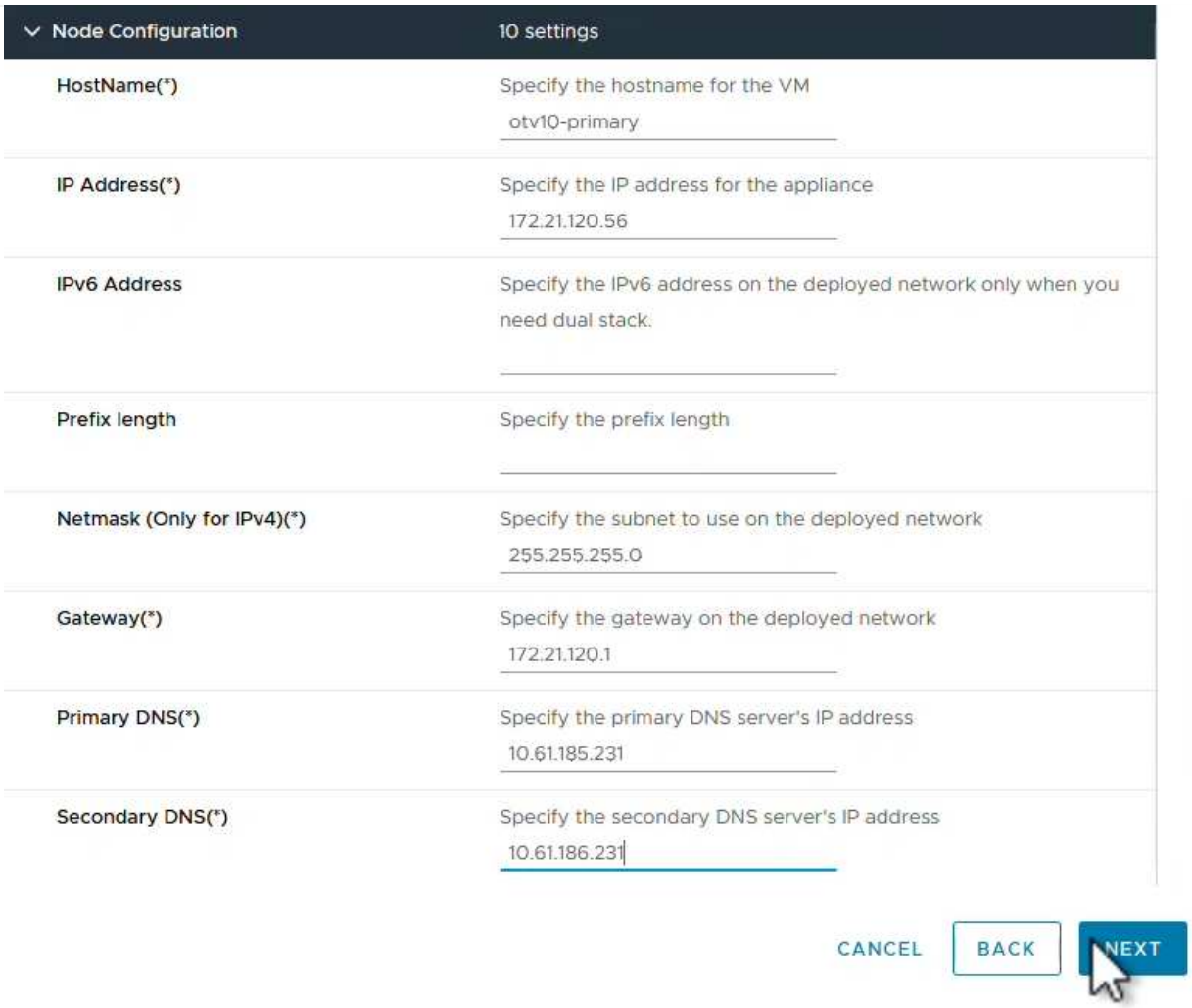
1. Baixe o modelo ONTAP tools 10 OVA do "Site de suporte da NetApp" .
2. No cliente vSphere, clique com o botão direito do mouse no cluster e clique em **Implantar modelo OVF**



3. No **Implantar modelo OVF**, conclua as etapas para:
   - Selecione um modelo OVF.
   - Selecione um nome e uma pasta.
   - Selecione um recurso de computação.
   - Detalhes da revisão.
   - Aceite o contrato de licença.
4. Na página **Configuração** do modelo, selecione o tipo de implantação, incluindo se as ferramentas ONTAP devem ser implantadas em uma configuração de HA. Clique em **Avançar** para continuar.



5. Na página **Selecionar armazenamento**, escolha o armazenamento de dados no qual deseja instalar a VM e clique em **Avançar**.
6. Selecione a rede na qual a VM das ferramentas ONTAP se comunicará. Clique em **Avançar** para continuar.
7. Na janela "Personalizar modelo", preencha todas as informações necessárias.
    - Nome de usuário e senha do aplicativo
    - Escolha se deseja habilitar o ASUP (suporte automático), incluindo uma URL de proxy.
    - Nome de usuário e senha do administrador.
    - Servidores NTP.
    - Nome de usuário e senha de manutenção (conta de manutenção usada no console).
    - Forneça os endereços IP necessários para a configuração de implantação.
    - Forneça todas as informações de rede para a configuração do nó.

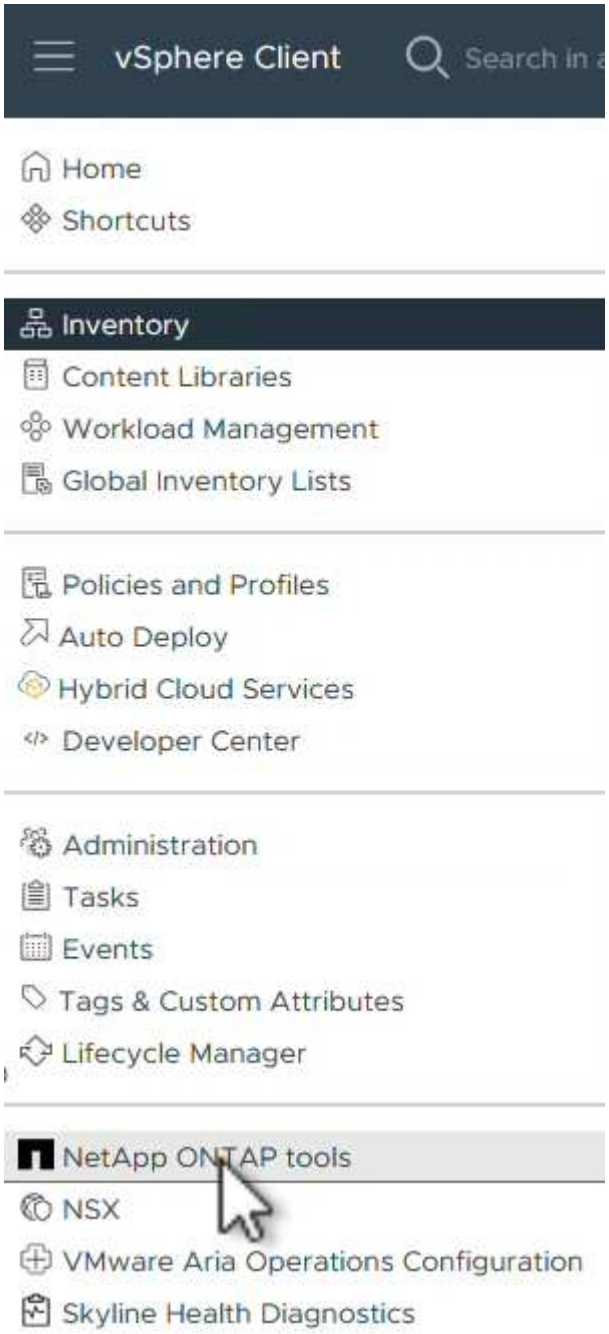


8. Por fim, clique em **Avançar** para continuar e depois em **Concluir** para iniciar a implantação.

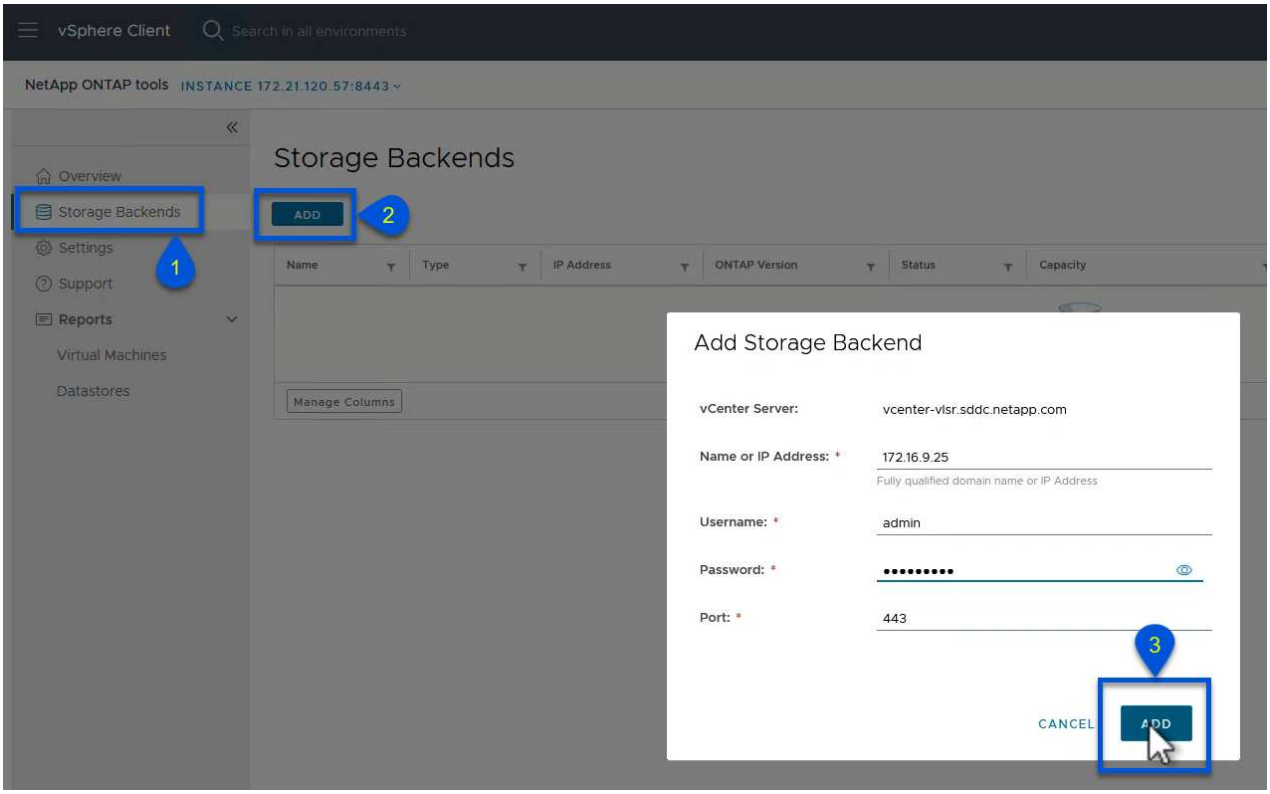
Configurar ferramentas ONTAP

Depois que a VM das ferramentas ONTAP estiver instalada e ligada, algumas configurações básicas serão necessárias, como adicionar servidores vCenter e sistemas de armazenamento ONTAP para gerenciar. Consulte a documentação em "Documentação das ONTAP tools for VMware vSphere" para obter informações detalhadas.

1. Consulte "Adicionar instâncias do vCenter" para configurar as instâncias do vCenter a serem gerenciadas com ferramentas ONTAP .
2. Para adicionar um sistema de armazenamento ONTAP , faça login no cliente vSphere e navegue até o menu principal à esquerda. Clique em * Ferramentas NetApp ONTAP * para iniciar a interface do usuário.



3. Navegue até **Storage Backends** no menu à esquerda e clique em **Adicionar** para acessar a janela **Adicionar Storage Backend**.
4. Preencha o endereço IP e as credenciais do sistema de armazenamento ONTAP a ser gerenciado. Clique em **Adicionar** para finalizar.

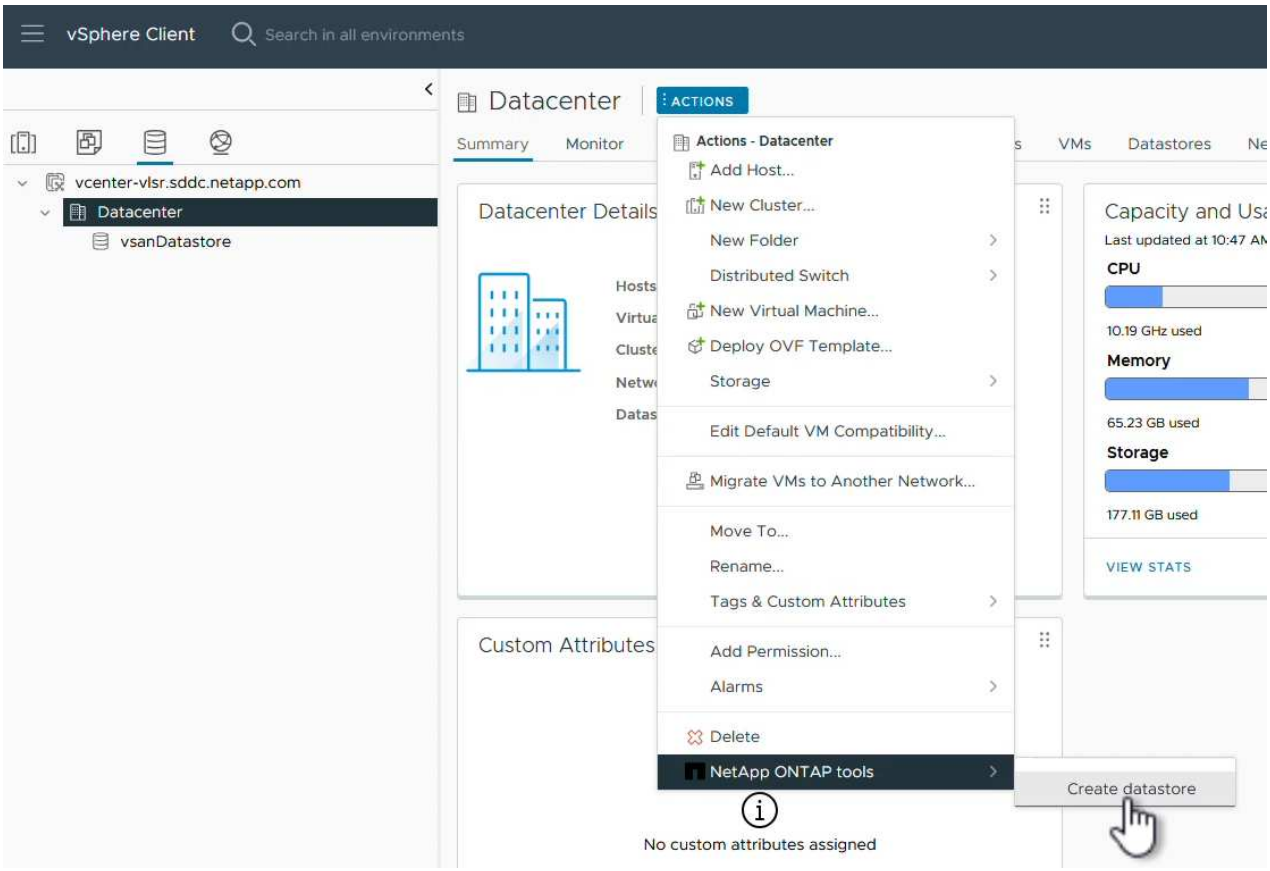


Aqui, o backend de armazenamento é adicionado na interface do cliente do vSphere usando o endereço IP do cluster. Isso permite o gerenciamento total de todas as SVMs no sistema de armazenamento. Como alternativa, o backend de armazenamento pode ser adicionado e associado a uma instância do vCenter usando o Gerenciador de ferramentas ONTAP em `https://loadBalanceIP:8443/virtualization/ui/` . Com esse método, somente credenciais SVM podem ser adicionadas à interface do cliente vSphere, fornecendo controle mais granular sobre o acesso ao armazenamento.

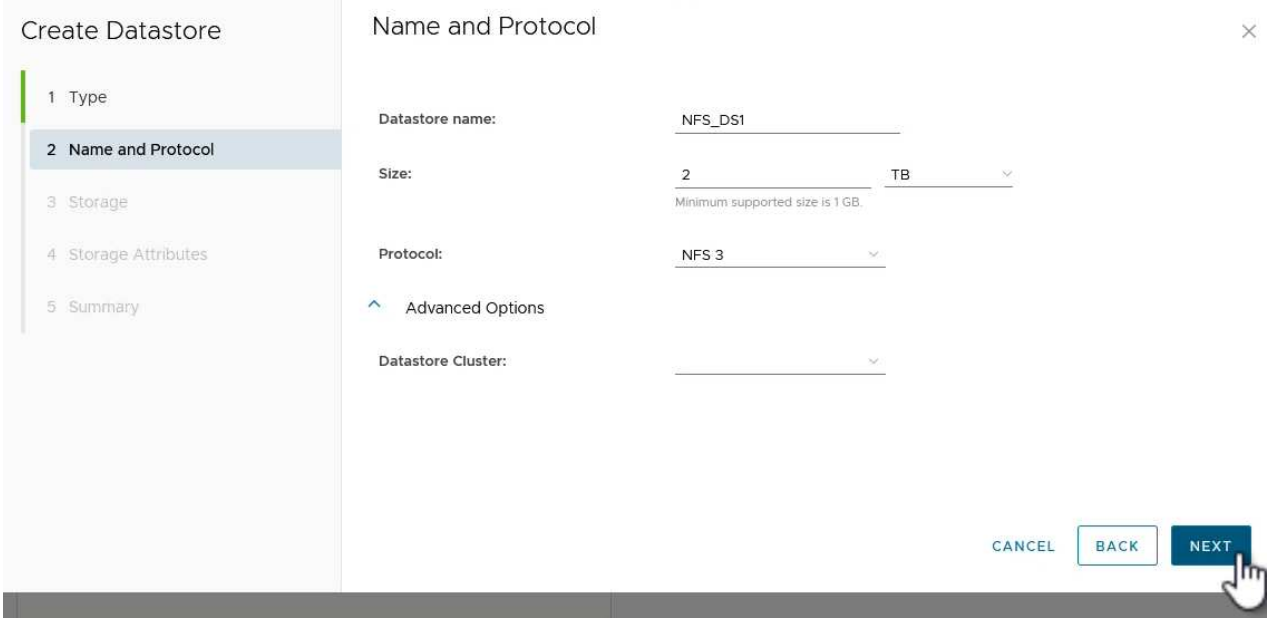
Provisionar armazenamento de dados NFS com ferramentas ONTAP

As ferramentas ONTAP integram funcionalidades em toda a interface do cliente vSphere. Nesta etapa, um armazenamento de dados NFS será provisionado a partir da página de inventário de armazenamento.

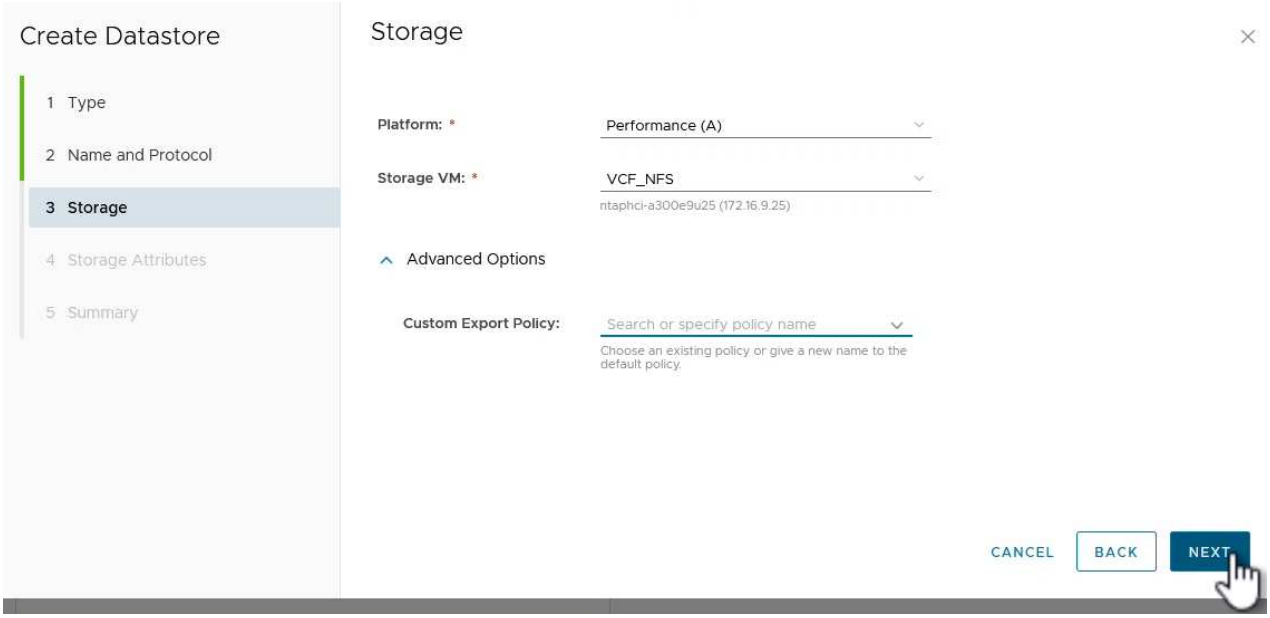
1. No cliente vSphere, navegue até o inventário de armazenamento.
2. Navegue até **AÇÕES > Ferramentas NetApp ONTAP > Criar armazenamento de dados**.



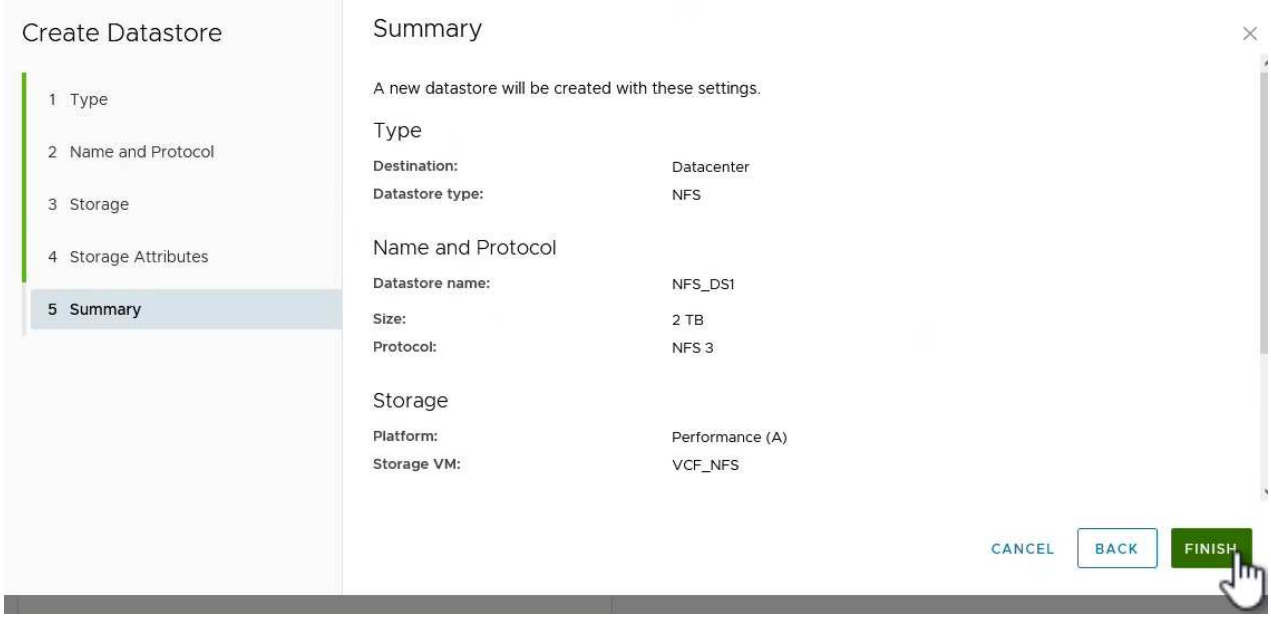
3. No assistente **Criar armazenamento de dados**, selecione o tipo de armazenamento de dados a ser criado. As opções são NFS ou VMFS.
4. Na página **Nome e Protocolo**, preencha um nome para o armazenamento de dados, o tamanho e o protocolo NFS a ser usado.



5. Na página **Armazenamento**, selecione a plataforma de armazenamento ONTAP e a máquina virtual de armazenamento (SVM). Você também pode selecionar quaisquer políticas de exportação personalizadas disponíveis aqui. Clique em **Avançar** para continuar.



6. Na página **Atributos de armazenamento**, selecione o agregado de armazenamento a ser usado. Clique em **Avançar** para continuar.
7. Na página **Resumo**, revise as informações e clique em **Concluir** para iniciar o processo de provisionamento. As ferramentas ONTAP criarão um volume no sistema de armazenamento ONTAP e o montarão como um armazenamento de dados NFS para todos os hosts ESXi no cluster.



Converter cluster vSphere para VCF 5.2

A seção a seguir aborda as etapas para implantar o gerenciador SDDC e converter o cluster vSphere 8 em um domínio de gerenciamento VCF 5.2. Quando apropriado, a documentação da VMware será consultada para obter detalhes adicionais.

A VCF Import Tool, da VMware by Broadcom, é um utilitário usado no dispositivo vCenter e no gerenciador SDDC para validar configurações e fornecer serviços de conversão e importação para ambientes vSphere e VCF.

Para obter mais informações, consulte "Opções e parâmetros da ferramenta de importação VCF" .

Ferramenta de importação de VCF para copiar e extrair

As Ferramentas de Importação de VCF são usadas no dispositivo vCenter para validar se o cluster vSphere está em um estado íntegro para o processo de conversão ou importação de VCF.

Conclua as seguintes etapas:

1. Siga os passos em "Copie a ferramenta de importação VCF para o dispositivo vCenter de destino" no VMware Docs para copiar a Ferramenta de Importação VCF para o local correto.
2. Extraia o pacote usando o seguinte comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar o dispositivo vCenter

Use a ferramenta de importação VCF para validar o dispositivo vCenter antes da conversão.

1. Siga os passos em "Execute uma pré-verificação no vCenter de destino antes da conversão" para executar a validação.
2. A saída a seguir mostra que o dispositivo vCenter passou na pré-verificação.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Implantar o Gerenciador do SDDC

O gerenciador do SDDC deve ser colocalizado no cluster vSphere que será convertido em um domínio de gerenciamento VCF.

Siga as instruções de implantação no VMware Docs para concluir a implantação.

Consulte "Implantar o SDDC Manager Appliance no vCenter de destino" .

Para mais informações, consulte"Anfitriões da Comissão" no Guia de Administração do VCF.

Crie um arquivo JSON para implantação do NSX

Para implantar o NSX Manager ao importar ou converter um ambiente vSphere no VMware Cloud Foundation, crie uma especificação de implantação do NSX. A implantação do NSX requer um mínimo de 3 hosts.

> Ao implantar um cluster do NSX Manager em uma operação de conversão ou importação, a rede NSX-VLAN é utilizada. Para obter detalhes sobre as limitações da rede NSX-VLAN, consulte a seção "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation". Para obter informações sobre as limitações de rede NSX-VLAN, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

A seguir está um exemplo de um arquivo JSON para implantação do NSX:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "NetApp!23456789",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie o arquivo JSON para um diretório no SDDC Manager.

Carregar software para o SDDC Manager

Copie a Ferramenta de Importação VCF e o pacote de implantação NSX para o diretório /home/vcf/vcfimport no Gerenciador SDDC.

Ver "Carregue o software necessário para o SDDC Manager Appliance" para obter instruções detalhadas.

Converter cluster vSphere em domínio de gerenciamento VCF

A ferramenta de importação VCF é usada para conduzir o processo de conversão. Execute o seguinte comando no diretório /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset para revisar uma impressão das funções da ferramenta de importação do VCF:

```
python3 vcf_brownfield.py --help
```

O comando a seguir é executado para converter o cluster vSphere em um domínio de gerenciamento VCF e implantar o cluster NSX:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Para obter instruções completas, consulte "Converter ou importar o ambiente vSphere para o inventário do SDDC Manager" .

Adicionar licenciamento ao VCF

Após concluir a conversão, o licenciamento deve ser adicionado ao ambiente.

1. Efetue login na interface de usuário do SDDC Manager.
2. Navegue até **Administração > Licenciamento** no painel de navegação.
3. Clique em **+ Chave de licença**.
4. Escolha um produto no menu suspenso.
5. Digite a chave de licença.
6. Forneça uma descrição para a licença.
7. Clique em **Adicionar**.
8. Repita essas etapas para cada licença.

Demonstração em vídeo das ONTAP tools for VMware vSphere 10

Armazenamento de dados NFS com ONTAP tools for VMware vSphere 10

Converter instância do servidor vCenter em domínio de gerenciamento VCF (armazenamento de dados FC)

Converta um cluster vSphere 8 usando datastores ONTAP Fibre Channel em um domínio de gerenciamento do VMware Cloud Foundation. Este procedimento inclui o provisionamento de armazenamento FC, a implantação de ferramentas ONTAP para VMware e o uso da ferramenta de importação VCF para migrar e gerenciar o cluster dentro do ambiente VCF.

Introdução

A conversão de um ambiente vSphere, com um armazenamento de dados Fibre Channel (FC) existente em execução no ONTAP, envolve a integração da infraestrutura existente em uma arquitetura de nuvem privada moderna. Este processo se beneficia da robustez do armazenamento FC, para garantir acesso e gerenciamento de dados contínuos. Depois que um domínio de gerenciamento do VCF é estabelecido por meio do processo de conversão, os administradores podem importar com eficiência ambientes vSphere adicionais, incluindo aqueles que usam armazenamentos de dados FC, para o ecossistema do VCF. Essa integração não apenas melhora a utilização de recursos, mas também simplifica o gerenciamento da infraestrutura de nuvem privada, garantindo uma transição tranquila com interrupção mínima nas cargas de trabalho existentes.

Nesta solução, demonstraremos como um armazenamento de dados FC no vSphere 8 se torna armazenamento principal quando o cluster é convertido em um domínio de gerenciamento VCF.

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Implante ONTAP tools for VMware vSphere 10.
- Provisione um armazenamento de dados FC usando ferramentas ONTAP .
- Use a Ferramenta de Importação VCF para validar o cluster vSphere.
- Implante o SDDC Manager no cluster vSphere.
- Configure um arquivo JSON para criar o NSX durante a conversão do VCF.
- Use a ferramenta de importação VCF para converter o cluster vSphere 8 para VCF 5.2.1

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Sistema de armazenamento NetApp ASA R2/ ASA/ AFF com uma máquina virtual de armazenamento (SVM) configurada para permitir tráfego Fibre Channel (FC).
- A interface lógica (LIF) foi criada para transportar tráfego FC e está associada ao SVM.
- O zoneamento FC foi configurado nos switches designados para transportar tráfego FC.
- Um cluster vSphere 8 com 4 hosts ESXi e um dispositivo vCenter colocalizados no cluster.
- Grupo de portas distribuídas configurado para vMotion nas VLANs ou segmentos de rede estabelecidos para essa finalidade.
- Baixe o software necessário para a conversão de VCF.

As ONTAP tools for VMware vSphere 10 podem ser instaladas em configurações HA ou não HA. Para obter

informações completas sobre os pré-requisitos para ferramentas ONTAP , consulte "Pré-requisitos para ONTAP tools for VMware vSphere" .

Para armazenamento suportado e outras considerações para conversão ou importação do vSphere para VCF 5.2, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

Para o software necessário, consulte "Baixe o software para converter ou importar ambientes vSphere existentes" .

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation 5.2" .

Etapas de implantação

A solução abrange o uso de ONTAP tools for VMware vSphere para provisionar armazenamentos de dados FC e o processo de conversão de um cluster vSphere 8 existente em um domínio de gerenciamento VCF.

Conclua as seguintes etapas:

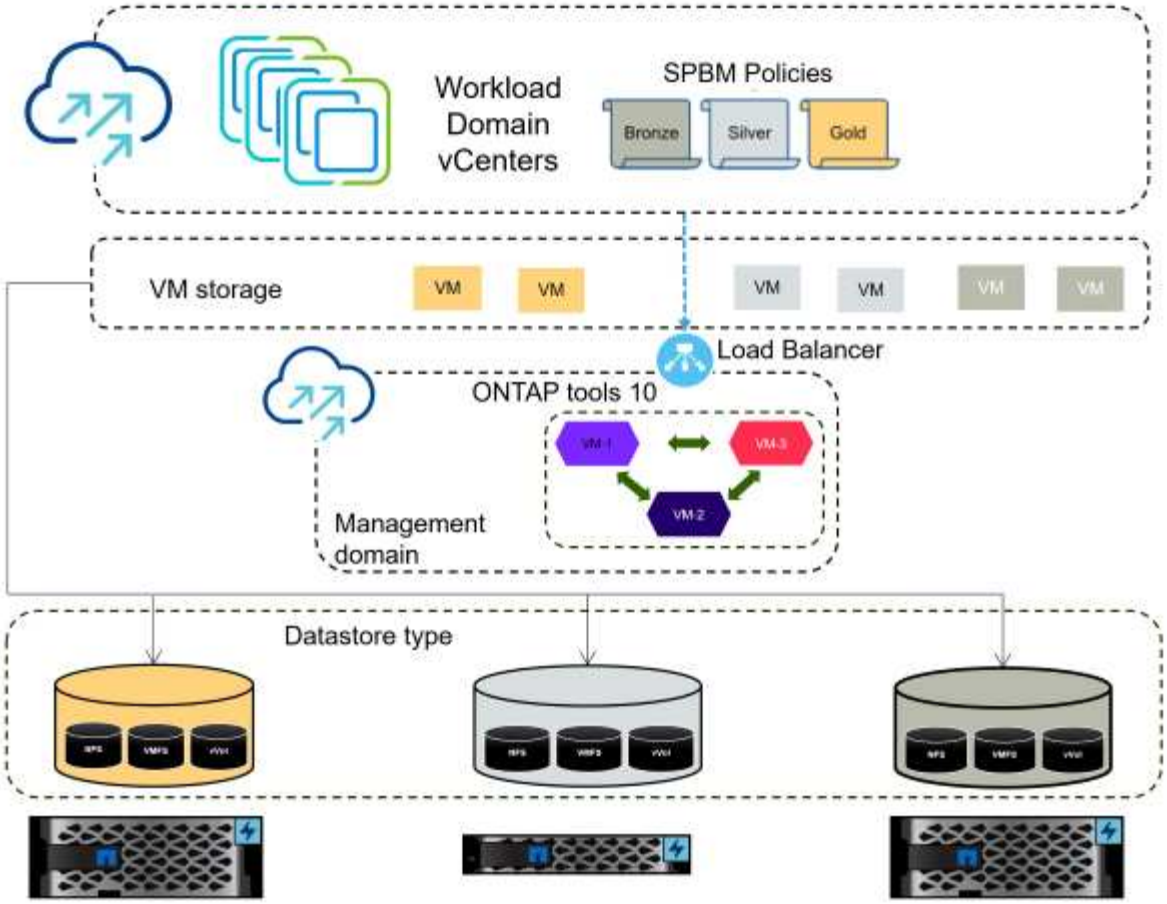
- Implante ONTAP tools for VMware vSphere 10.
- Provisione um armazenamento de dados FC usando ferramentas ONTAP .
- Copie a ferramenta de importação VCF para o dispositivo vCenter.
- Execute uma pré-verificação no dispositivo vCenter usando a Ferramenta de Importação VCF.
- Implante a VM do gerenciador do SDDC no cluster do vCenter.
- Crie um arquivo JSON para um cluster NSX a ser implantado durante o processo de conversão.
- Carregue o software necessário para o gerenciador do SDDC.
- Converta o cluster do vSphere no inventário do gerenciador do SDDC.

Para uma visão geral do processo de conversão, consulte "Converter um ambiente vSphere em um domínio de gerenciamento ou importar um ambiente vSphere como um domínio de carga de trabalho VI no VMware Cloud Foundation" .

Implantar ferramentas ONTAP e provisionar um armazenamento de dados FC

A arquitetura das ferramentas ONTAP 10 foi projetada para integrar-se perfeitamente aos ambientes VMware, aproveitando uma estrutura modular e escalável que inclui os serviços das ferramentas ONTAP , o plug-in vSphere e as APIs REST para permitir gerenciamento de armazenamento eficiente, automação e proteção de dados.

As ONTAP tools for VMware vSphere 10 podem ser instaladas em configurações HA ou não HA.

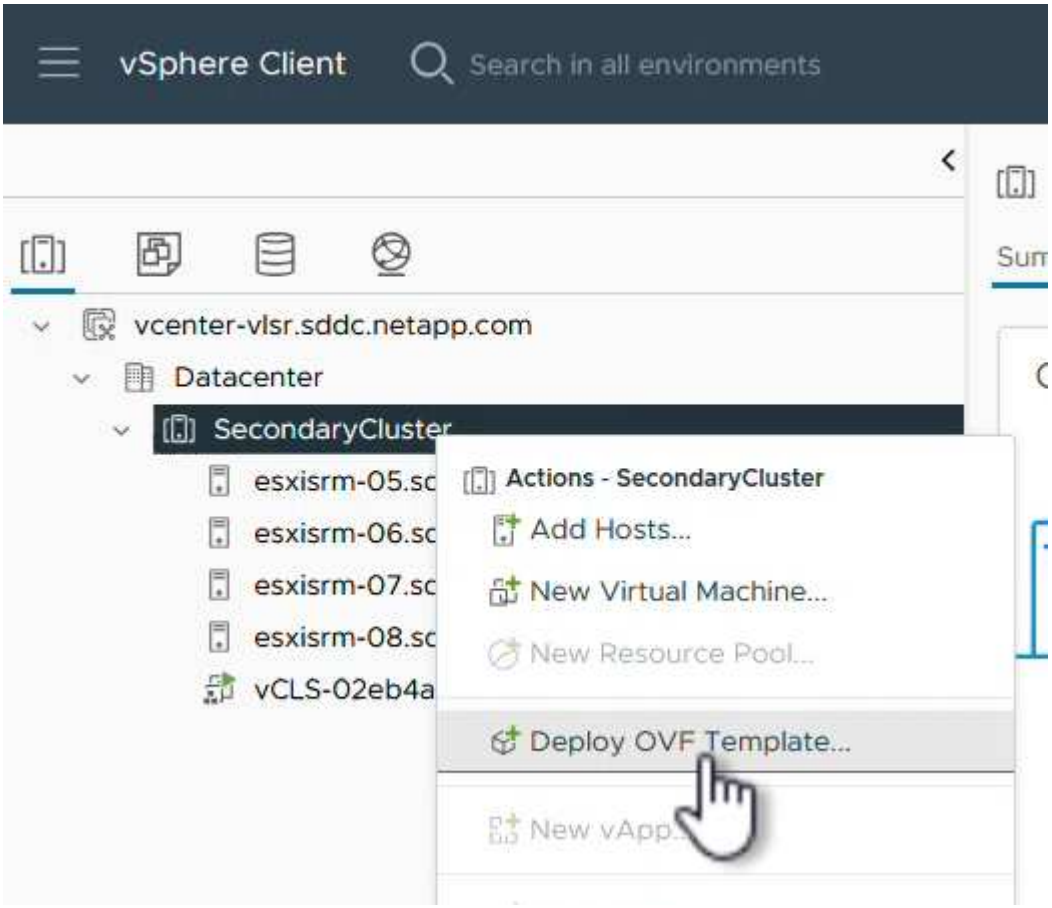

Workload
Domain
vCenters
SPBM Policies
Bronze
Silver
Gold
VM storage
VM
VM
VM
VM
VM
VM
Load Balancer
ONTAP tools 10
VM-1
VM-3
VM-2
Management
domain
Datastore type

Implantar ONTAP tools for VMware vSphere 10

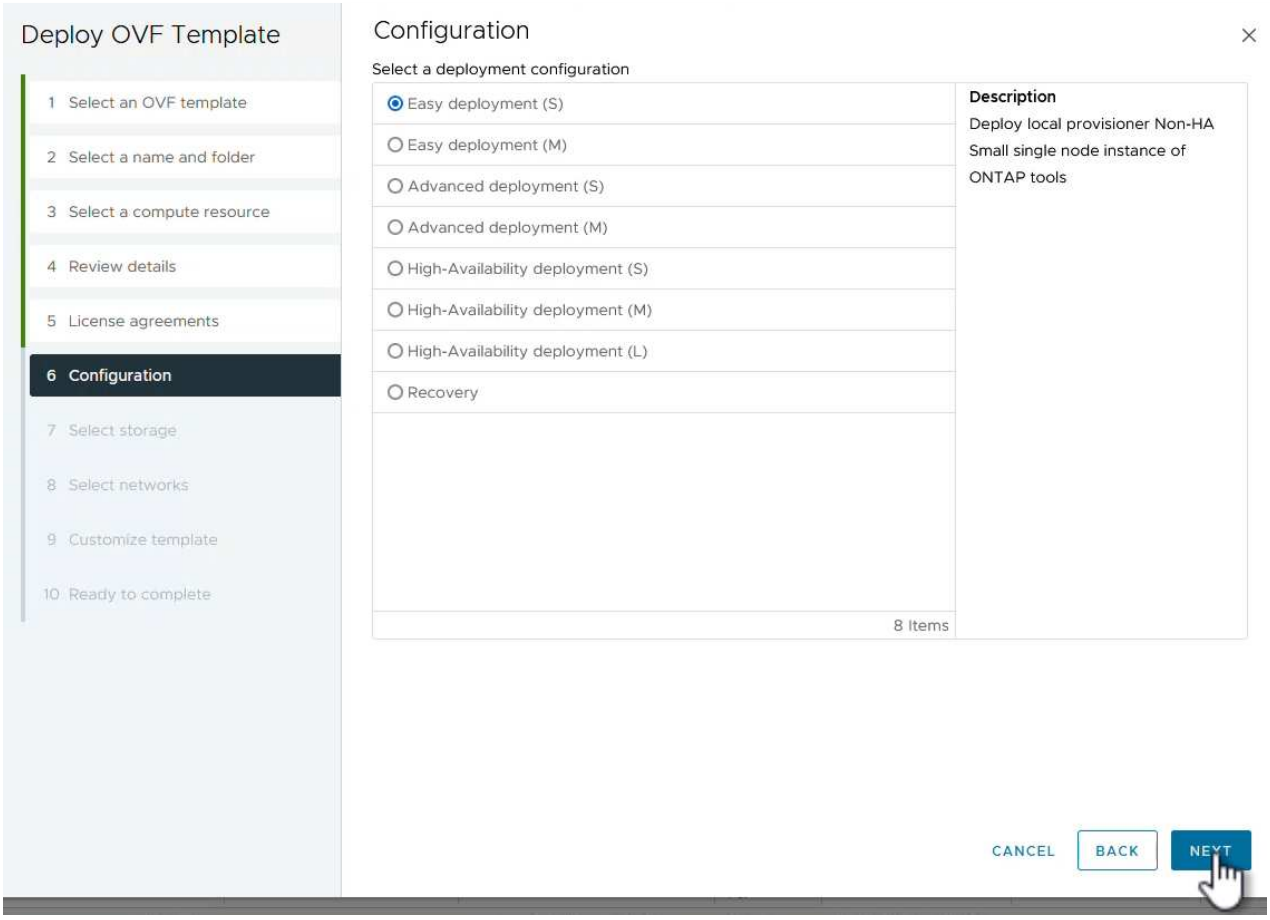
Nesta etapa, o ONTAP Tools 10 é implantado com uma configuração não HA.

Para obter detalhes adicionais de implantação em configurações HA e não HA, consulte "Implantar ONTAP tools for VMware vSphere" .

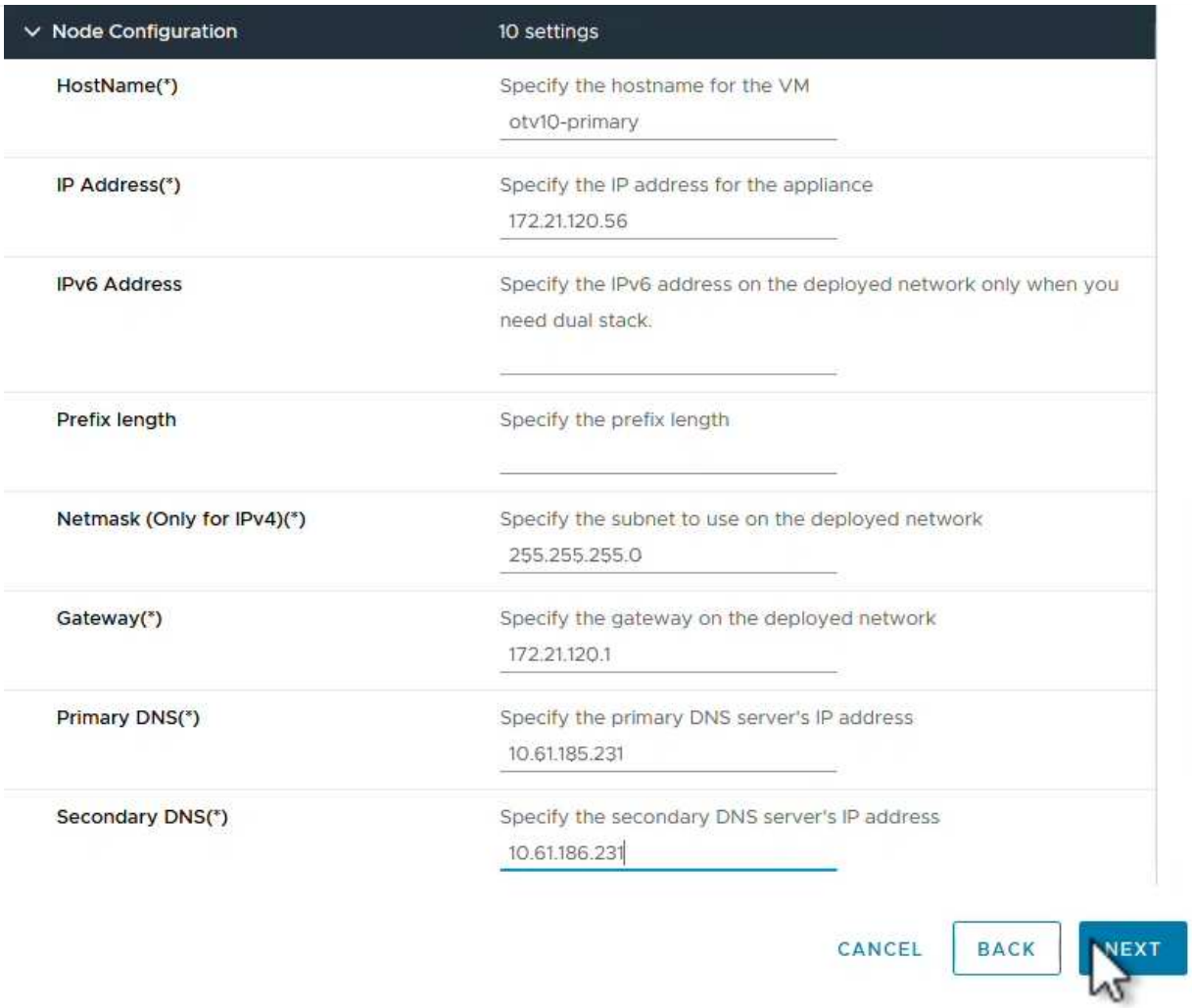
1. Baixe o modelo ONTAP tools 10 OVA do "Site de suporte da NetApp" .
2. No cliente vSphere, clique com o botão direito do mouse no cluster e clique em **Implantar modelo OVF**



3. No **Implantar modelo OVF**, conclua as etapas para:
   - Selecione um modelo OVF.
   - Selecione um nome e uma pasta.
   - Selecione um recurso de computação.
   - Detalhes da revisão.
   - Aceite o contrato de licença.
4. Na página **Configuração** do modelo, selecione o tipo de implantação, incluindo se as ferramentas ONTAP devem ser implantadas em uma configuração de HA. Clique em **Avançar** para continuar.



5. Na página **Selecionar armazenamento**, escolha o armazenamento de dados no qual deseja instalar a VM e clique em **Avançar**.
6. Selecione a rede na qual a VM das ferramentas ONTAP se comunicará. Clique em **Avançar** para continuar.
7. Na janela "Personalizar modelo", preencha todas as informações necessárias.
    - Nome de usuário e senha do aplicativo
    - Escolha se deseja habilitar o ASUP (suporte automático), incluindo uma URL de proxy.
    - Nome de usuário e senha do administrador.
    - Servidores NTP.
    - Nome de usuário e senha de manutenção (conta de manutenção usada no console).
    - Forneça os endereços IP necessários para a configuração de implantação.
    - Forneça todas as informações de rede para a configuração do nó.

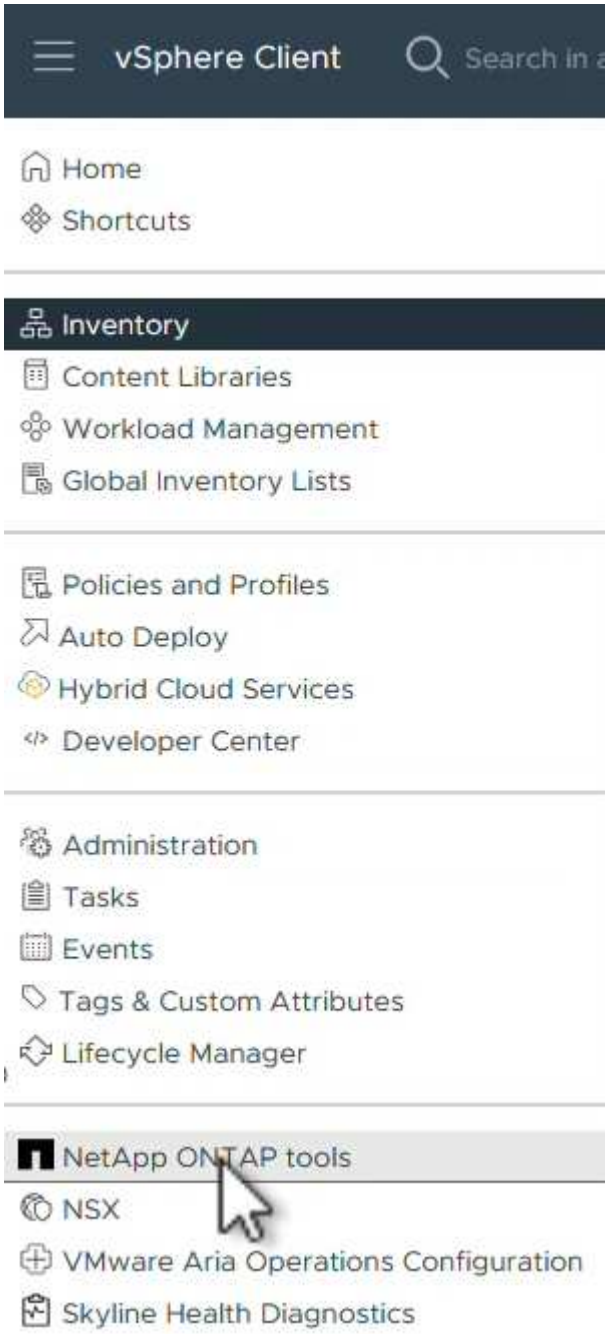


8. Por fim, clique em **Avançar** para continuar e depois em **Concluir** para iniciar a implantação.

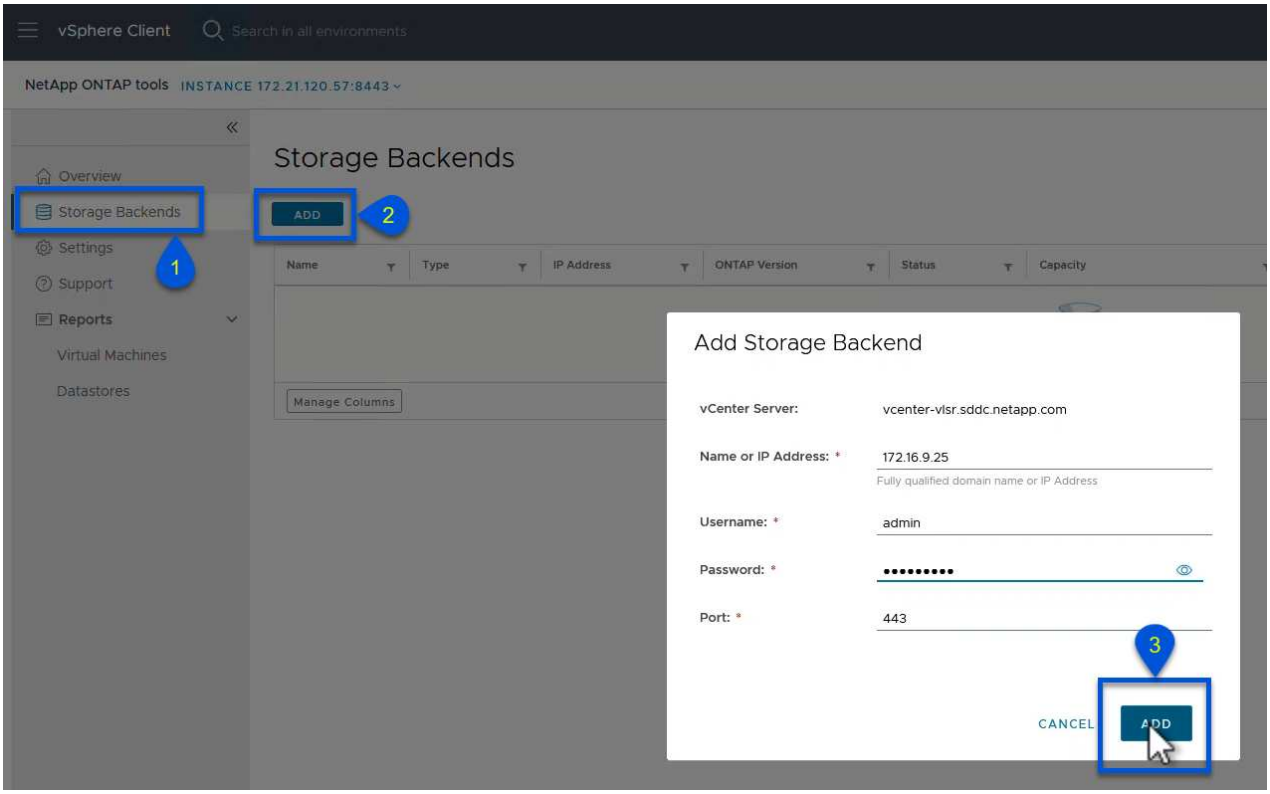
Configurar ferramentas ONTAP

Depois que a VM das ferramentas ONTAP estiver instalada e ligada, algumas configurações básicas serão necessárias, como adicionar servidores vCenter e sistemas de armazenamento ONTAP para gerenciar. Consulte a documentação em "Documentação das ONTAP tools for VMware vSphere" para obter informações detalhadas.

1. Consulte "Adicionar instâncias do vCenter" para configurar as instâncias do vCenter a serem gerenciadas com ferramentas ONTAP .
2. Para adicionar um sistema de armazenamento ONTAP , faça login no cliente vSphere e navegue até o menu principal à esquerda. Clique em * Ferramentas NetApp ONTAP * para iniciar a interface do usuário.



3. Navegue até **Storage Backends** no menu à esquerda e clique em **Adicionar** para acessar a janela **Adicionar Storage Backend**.
4. Preencha o endereço IP e as credenciais do sistema de armazenamento ONTAP a ser gerenciado. Clique em **Adicionar** para finalizar.

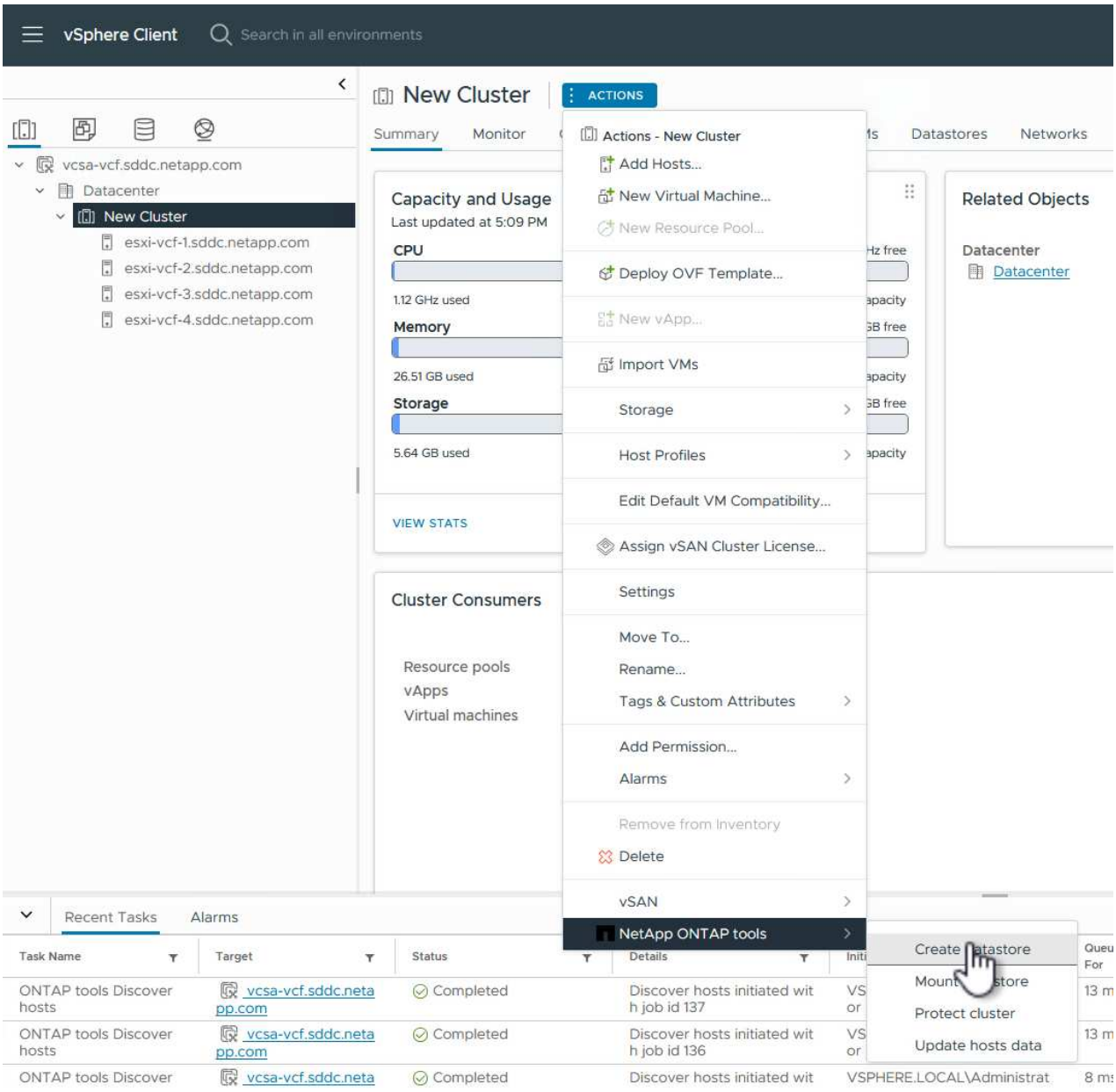


Aqui, o backend de armazenamento é adicionado na interface do cliente do vSphere usando o endereço IP do cluster. Isso permite o gerenciamento total de todas as SVMs no sistema de armazenamento. Como alternativa, o backend de armazenamento pode ser adicionado e associado a uma instância do vCenter usando o Gerenciador de ferramentas ONTAP em `https://loadBalanceIP:8443/virtualization/ui/` . Com esse método, somente credenciais SVM podem ser adicionadas à interface do cliente vSphere, fornecendo controle mais granular sobre o acesso ao armazenamento.

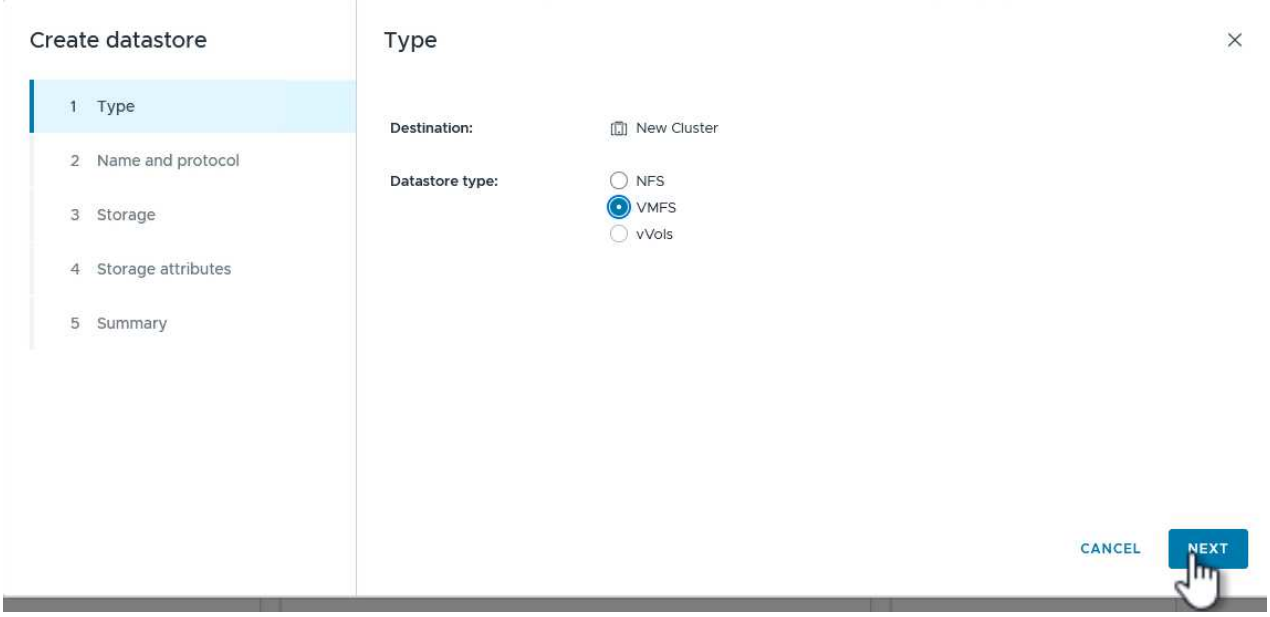
Provisionar armazenamento de dados FC com ferramentas ONTAP

As ferramentas ONTAP integram funcionalidades em toda a interface do cliente vSphere. Nesta etapa, um armazenamento de dados FC será provisionado a partir da página de inventário de hosts.

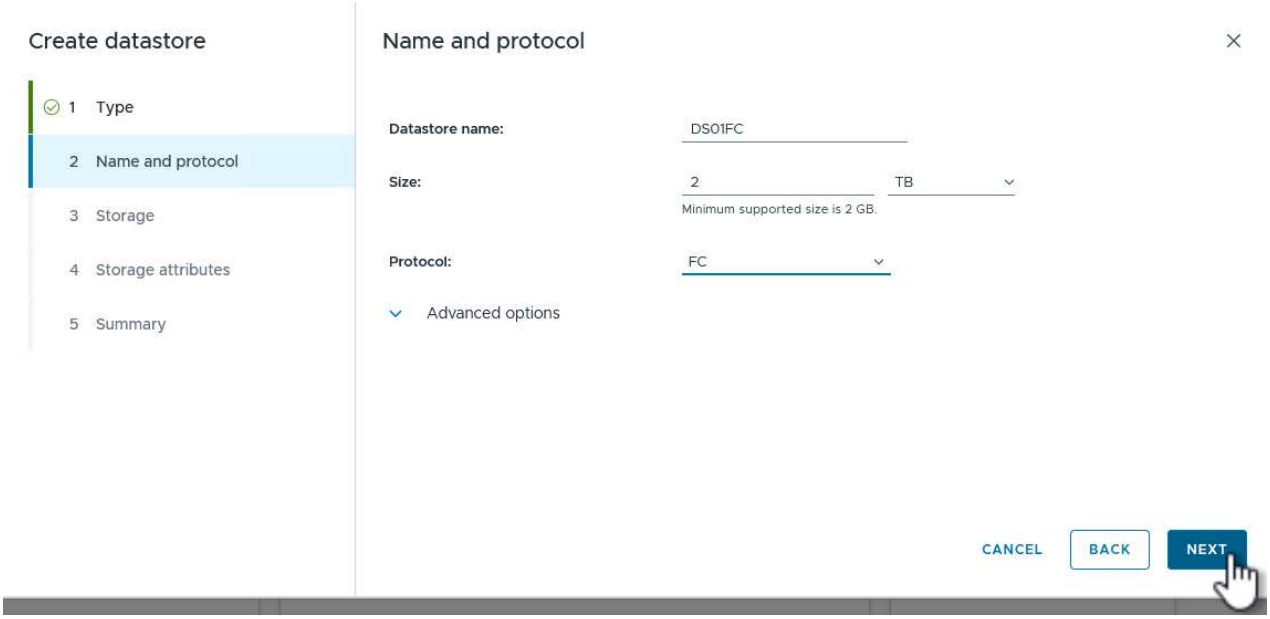
1. No cliente vSphere, navegue até o inventário de hosts (ou armazenamento).
2. Navegue até **AÇÕES > Ferramentas NetApp ONTAP > Criar armazenamento de dados**.



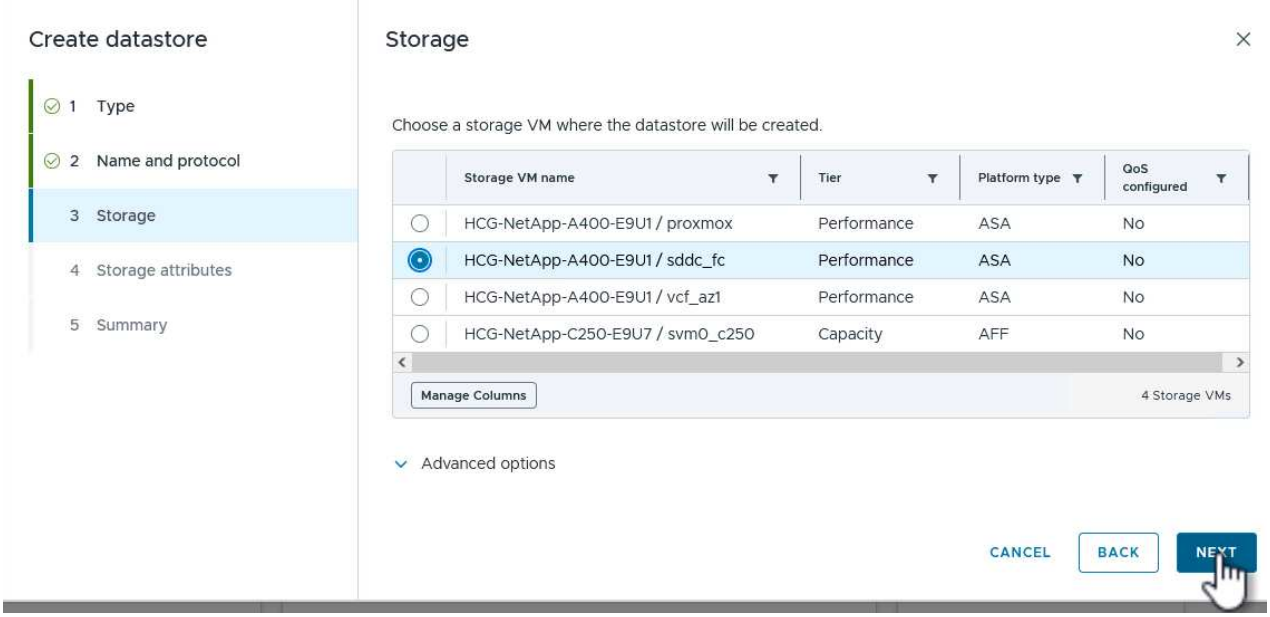
3. No assistente **Criar armazenamento de dados**, selecione VMFS para o tipo de armazenamento de dados a ser criado.



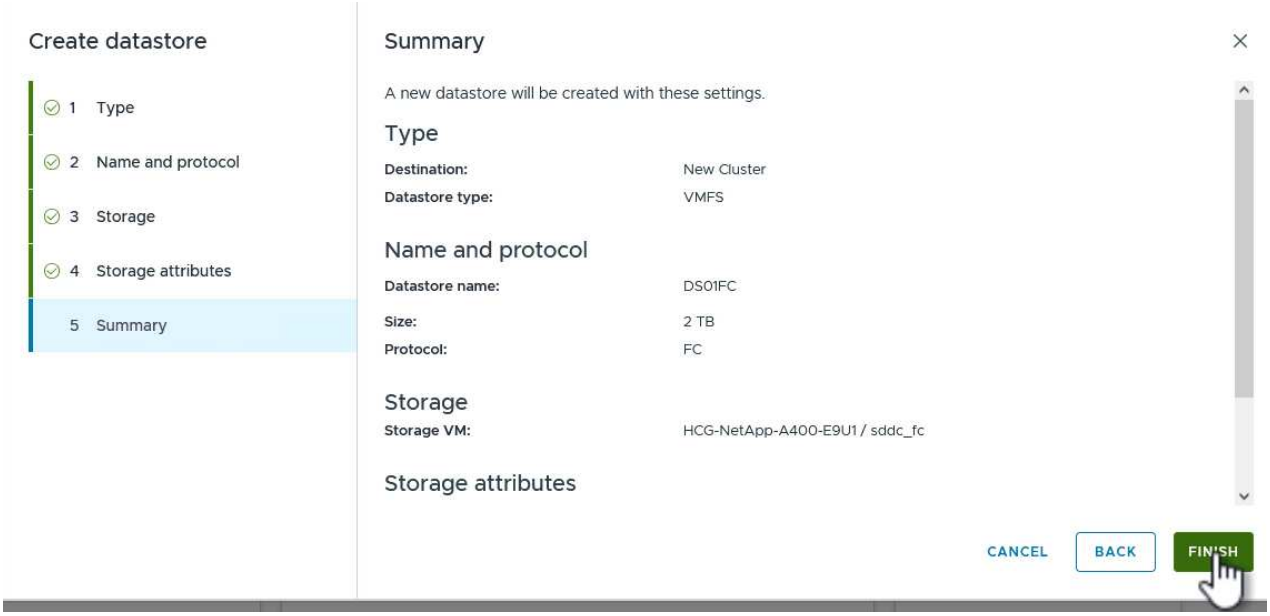
4. Na página **Nome e Protocolo**, preencha um nome para o armazenamento de dados, o tamanho e o protocolo FC a ser usado.



5. Na página **Armazenamento**, selecione a plataforma de armazenamento ONTAP e a máquina virtual de armazenamento (SVM). Você também pode selecionar quaisquer políticas de exportação personalizadas disponíveis aqui. Clique em **Avançar** para continuar.



6. Na página **Atributos de armazenamento**, selecione o agregado de armazenamento a ser usado. Clique em **Avançar** para continuar.
7. Na página **Resumo**, revise as informações e clique em **Concluir** para iniciar o processo de provisionamento. As ferramentas ONTAP criarão um volume no sistema de armazenamento ONTAP e o montarão como um armazenamento de dados FC para todos os hosts ESXi no cluster.



Converter ambiente vSphere para VCF 5.2

A seção a seguir aborda as etapas para implantar o gerenciador SDDC e converter o cluster vSphere 8 em um domínio de gerenciamento VCF 5.2. Quando apropriado, a documentação da VMware será consultada para obter detalhes adicionais.

A VCF Import Tool, da VMware by Broadcom, é um utilitário usado no dispositivo vCenter e no gerenciador

SDDC para validar configurações e fornecer serviços de conversão e importação para ambientes vSphere e VCF.

Para obter mais informações, consulte "Opções e parâmetros da ferramenta de importação VCF" .

Ferramenta de importação de VCF para copiar e extrair

As Ferramentas de Importação de VCF são usadas no dispositivo vCenter para validar se o cluster vSphere está em um estado íntegro para o processo de conversão ou importação de VCF.

Conclua as seguintes etapas:

1. Siga os passos em "Copie a ferramenta de importação VCF para o dispositivo vCenter de destino" no VMware Docs para copiar a Ferramenta de Importação VCF para o local correto.
2. Extraia o pacote usando o seguinte comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar o dispositivo vCenter

Use a ferramenta de importação VCF para validar o dispositivo vCenter antes da conversão.

1. Siga os passos em "Execute uma pré-verificação no vCenter de destino antes da conversão" para executar a validação.
2. A saída a seguir mostra que o dispositivo vCenter passou na pré-verificação.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Implantar o Gerenciador do SDDC

O gerenciador do SDDC deve ser colocalizado no cluster vSphere que será convertido em um domínio de gerenciamento VCF.

Siga as instruções de implantação no VMware Docs para concluir a implantação.

Consulte "Implantar o SDDC Manager Appliance no vCenter de destino" .

Para mais informações, consulte"Anfitriões da Comissão" no Guia de Administração do VCF.

Crie um arquivo JSON para implantação do NSX

Para implantar o NSX Manager ao importar ou converter um ambiente vSphere no VMware Cloud Foundation, crie uma especificação de implantação do NSX. A implantação do NSX requer um mínimo de 3 hosts.

Para obter informações completas, consulte "Gerar uma especificação de implantação do NSX para converter ou importar ambientes vSphere existentes" .

> Ao implantar um cluster do NSX Manager em uma operação de conversão ou importação, a rede NSX-VLAN é utilizada. Para obter detalhes sobre as limitações da rede NSX-VLAN, consulte a seção "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation". Para obter informações sobre as limitações de rede NSX-VLAN, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

A seguir está um exemplo de um arquivo JSON para implantação do NSX:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "************************",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie o arquivo JSON para um diretório no SDDC Manager.

Carregar software para o SDDC Manager

Copie a Ferramenta de Importação VCF e o pacote de implantação NSX para o diretório /home/vcf/vcfimport no Gerenciador SDDC.

Ver "Carregue o software necessário para o SDDC Manager Appliance" para obter instruções detalhadas.

Converter cluster vSphere em domínio de gerenciamento VCF

A ferramenta de importação VCF é usada para conduzir o processo de conversão. Execute o seguinte comando no diretório /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset para revisar uma impressão das funções da ferramenta de importação do VCF:

```
python3 vcf_brownfield.py --help
```

O comando a seguir é executado para converter o cluster vSphere em um domínio de gerenciamento VCF e implantar o cluster NSX:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Para obter instruções completas, consulte "Converter ou importar o ambiente vSphere para o inventário do SDDC Manager" .

Adicionar licenciamento ao VCF

Após concluir a conversão, o licenciamento deve ser adicionado ao ambiente.

1. Efetue login na interface de usuário do SDDC Manager.
2. Navegue até **Administração > Licenciamento** no painel de navegação.
3. Clique em **+ Chave de licença**.
4. Escolha um produto no menu suspenso.
5. Digite a chave de licença.
6. Forneça uma descrição para a licença.
7. Clique em **Adicionar**.
8. Repita essas etapas para cada licença.

Demonstração em vídeo das ONTAP tools for VMware vSphere 10

Armazenamento de dados NFS com ONTAP tools for VMware vSphere 10

Provisionar VCF com armazenamento principal

Provisione um ambiente VCF com ONTAP como a principal solução de armazenamento

O armazenamento NetApp ONTAP é uma solução de armazenamento primário ideal para gerenciamento do VMware Cloud Foundation (VCF) e domínios de carga de trabalho de infraestrutura virtual (VI). O ONTAP oferece alto desempenho, escalabilidade, gerenciamento avançado de dados e integração perfeita para melhorar a eficiência operacional e a proteção de dados.

Consulte as soluções a seguir para obter detalhes técnicos sobre o provisionamento de um ambiente VCF no domínio apropriado e com o protocolo apropriado.

- "Domínio de Gestão com FC"
- "Domínio de Gerenciamento com NFS"
- "Domínio de carga de trabalho de infraestrutura virtual com FC"
- "Domínio de carga de trabalho de infraestrutura virtual com NFS"

Use um armazenamento de dados VMFS baseado em FC no ONTAP como armazenamento principal para o domínio de gerenciamento VCF

Neste caso de uso, descrevemos o procedimento para usar um armazenamento de dados VMFS baseado em FC existente no ONTAP como armazenamento primário para domínios de gerenciamento do VMware Cloud Foundation (VCF). Este procedimento resume os componentes, configurações e etapas de implantação necessários.

Introdução

Quando apropriado, faremos referência à documentação externa para as etapas que devem ser executadas no SDDC Manager do VCF e faremos referência às etapas específicas da parte de configuração de armazenamento.

Para obter informações sobre como converter um ambiente vSphere baseado em FC existente com ONTAP, consulte"Converter ambiente vSphere (armazenamento de dados FC) em domínio de gerenciamento VCF" .

> A versão 5.2 do VCF introduziu a capacidade de converter um ambiente vSphere 8 existente em um domínio de gerenciamento VCF ou importar como domínios de carga de trabalho VCF VI. Antes desta versão, o VMware vSAN era a única opção de armazenamento principal para o domínio de gerenciamento do VCF.

> Esta solução é aplicável para plataformas ONTAP que suportam armazenamento FC, incluindo NetApp ASA, AFF e FAS.

Pré-requisitos

Os seguintes componentes e configurações são usados neste cenário:

- Sistema de armazenamento NetApp com uma máquina virtual de armazenamento (SVM) configurada para permitir tráfego FC.
- Interfaces lógicas (LIF) foram criadas na estrutura FC que transportará o tráfego FC e está associada ao SVM.
- O zoneamento foi configurado para usar zoneamento de iniciador-destino único em switches FC para HBAs de host e destinos de armazenamento.

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Etapas de implantação

Domínio de Gerenciamento - Cluster Padrão

O armazenamento principal do FC no cluster inicial só é suportado com a ferramenta de importação brownfield do VCF. Se o VCF for implantado com a ferramenta Cloud Builder (antes da versão 5.2.x), somente o vSAN será suportado.

Para obter mais informações sobre como usar um ambiente vSphere existente, consulte "convertendo o ambiente vSphere existente para o domínio de gerenciamento" para mais informações.

Domínio de Gerenciamento - Cluster Adicional

O cluster vSphere adicional no domínio de gerenciamento pode ser implantado com as seguintes opções:

- Tenha um cluster adicional no ambiente vSphere e use a ferramenta de importação brownfield do VCF para converter o ambiente vSphere em domínio de gerenciamento. "ONTAP tools for VMware vSphere" "Gerenciador de sistema ou API ONTAP" pode ser usado para implantar o armazenamento de dados VMFS no cluster vSphere.
- Use a API do SDDC para implantar um cluster adicional. Os hosts vSphere devem ter o armazenamento de dados VMFS configurado. Usar "Gerenciador de sistema ou API ONTAP" para implantar LUN em hosts vSphere.
- Use a interface de usuário do SDDC Manager para implantar um cluster adicional. Mas esta opção só cria um armazenamento de dados VSAN até a versão 5.2.x.

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Use um armazenamento de dados NFS no ONTAP como armazenamento principal para o domínio de gerenciamento VCF

Neste caso de uso, descrevemos o procedimento para usar um armazenamento de dados NFS existente no ONTAP como armazenamento primário para domínios de gerenciamento do VMware Cloud Foundation (VCF). Este procedimento resume os componentes necessários, as etapas de configuração e o processo de implantação.

Introdução

Quando apropriado, faremos referência à documentação externa para as etapas que devem ser executadas no SDDC Manager do VCF e faremos referência às etapas específicas da parte de configuração de armazenamento.

Para obter informações sobre como converter um ambiente vSphere baseado em NFS existente com ONTAP, consulte"Converter ambiente vSphere (armazenamento de dados NFS) em domínio de gerenciamento VCF" .

> A versão 5.2 do VCF introduziu a capacidade de converter um ambiente vSphere 8 existente em um domínio de gerenciamento VCF ou importar como domínios de carga de trabalho VCF VI. Antes desta versão, o VMware vSAN era a única opção de armazenamento principal para o domínio de gerenciamento do VCF.

> Esta solução é aplicável para plataformas ONTAP que suportam armazenamento NFS, incluindo NetApp AFF e FAS.

Pré-requisitos

Os seguintes componentes e configurações são usados neste cenário:

- Sistema de armazenamento NetApp com uma máquina virtual de armazenamento (SVM) configurada para permitir tráfego NFS.
- A interface lógica (LIF) foi criada na rede IP que transportará o tráfego NFS e está associada ao SVM.
- Um cluster vSphere 8 com 4 hosts ESXi e um dispositivo vCenter colocalizados no cluster.
- Grupo de portas distribuídas configurado para tráfego de armazenamento vMotion e NFS nas VLANs ou segmentos de rede estabelecidos para essa finalidade.
- Baixe o software necessário para a conversão de VCF.

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Etapas de implantação

Domínio de Gerenciamento - Cluster Padrão

O armazenamento principal do NFS no cluster inicial só é suportado com a ferramenta de importação brownfield do VCF. Se o VCF for implantado com a ferramenta Cloud Builder (até a versão 5.2.x), somente o VSAN será suportado.

Para obter mais informações sobre como usar um ambiente vSphere existente, consulte "convertendo o ambiente vSphere existente para o domínio de gerenciamento" para mais informações.

Domínio de Gerenciamento - Cluster Adicional

O cluster vSphere adicional no domínio de gerenciamento pode ser implantado com as seguintes opções:

- Tenha um cluster adicional no ambiente vSphere e use a ferramenta de importação brownfield do VCF para converter o ambiente vSphere em domínio de gerenciamento. "ONTAP tools for VMware vSphere" "Gerenciador de sistema ou API ONTAP" pode ser usado para implantar o armazenamento de dados NFS no cluster vSphere.
- Use a API do SDDC para implantar um cluster adicional. Os hosts do vSphere devem ter o armazenamento de dados NFS configurado. Usar "Gerenciador de sistema ou API ONTAP" para implantar LUN em hosts vSphere.
- Use a interface de usuário do SDDC Manager para implantar um cluster adicional. Mas essa opção só cria um armazenamento de dados vSAN com versões anteriores à 5.2.x.

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Use um armazenamento de dados VMFS baseado em FC no ONTAP como armazenamento principal para um domínio de carga de trabalho VI

Neste caso de uso, descrevemos o procedimento para configurar um armazenamento de dados VMFS Fibre Channel (FC) no ONTAP como a solução de armazenamento primária para um domínio de carga de trabalho de infraestrutura virtual (VI) do VMware Cloud Foundation (VCF). Este procedimento resume os componentes necessários, as etapas de configuração e o processo de implantação.

Benefícios do Fibre Channel

Alto desempenho: o FC fornece altas taxas de transferência de dados, tornando-o ideal para aplicações que exigem acesso rápido e confiável a grandes quantidades de dados.

Baixa latência: latência muito baixa, o que é crucial para aplicativos sensíveis ao desempenho, como bancos de dados e ambientes virtualizados.

Confiabilidade: As redes FC são conhecidas por sua robustez e confiabilidade, com recursos como redundância integrada e correção de erros.

Largura de banda dedicada: o FC fornece largura de banda dedicada para tráfego de armazenamento, reduzindo o risco de congestionamento da rede.

Para obter mais informações sobre o uso do Fibre Channel com sistemas de armazenamento NetApp , consulte "Provisionamento SAN com FC" .

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Crie uma máquina virtual de armazenamento (SVM) com interfaces lógicas (LIFs) para tráfego FC.
- Colete informações WWPN dos hosts a serem implantados e crie grupos iniciadores correspondentes no sistema de armazenamento ONTAP .
- Crie um volume FC no sistema de armazenamento ONTAP .
- Grupos de iniciadores de mapa para criar volume FC
- Utilize zoneamento de iniciador-alvo único em switches FC. Crie uma zona para cada iniciador (zona de iniciador único).
  - Para cada zona, inclua um destino que seja a interface lógica ONTAP FC (WWPN) para as SVMs. Deve haver pelo menos duas interfaces lógicas por nó por SVM. Não utilize o WWPN das portas físicas.
- Crie um pool de rede para tráfego vMotion no SDDC Manager.
- Comissionar hosts no VCF para uso em um domínio de carga de trabalho do VI.
- Implante um domínio de carga de trabalho VI no VCF usando um armazenamento de dados FC como armazenamento principal.

> Esta solução é aplicável para plataformas ONTAP que suportam armazenamento NFS, incluindo NetApp AFF e FAS.

Pré-requisitos

Os seguintes componentes e configurações são usados neste cenário:

- Um sistema de armazenamento ONTAP AFF ou ASA com portas FC conectadas a switches FC.
- SVM criado com FC lifs.
- vSphere com HBAs FC conectados a switches FC.
- O zoneamento de iniciador-alvo único é configurado em switches FC.

> A NetApp recomenda vários caminhos para LUNs FC.

Etapas de implantação

Domínio de Gerenciamento - Cluster Padrão

O armazenamento principal do FC no cluster inicial só é suportado com a ferramenta de importação brownfield do VCF. Se o VCF for implantado com a ferramenta cloudbuilder (até a versão 5.2.x), somente o VSAN será suportado. Referir "convertendo o ambiente vSphere existente para o domínio de gerenciamento" para mais informações.

Domínio de Gerenciamento - Cluster Adicional

O cluster vSphere adicional no domínio de gerenciamento pode ser implantado com as seguintes opções: * Ter um cluster adicional no ambiente vSphere e usar a ferramenta de importação brownfield do VCF para converter o ambiente vSphere em domínio de gerenciamento. "ONTAP tools for VMware vSphere" , "Gerenciador de sistema ou API ONTAP" pode ser usado para implantar o armazenamento de dados VMFS no cluster vSphere. * Use a API do SDDC para implantar um cluster adicional. Os hosts vSphere devem ter o

armazenamento de dados VMFS configurado. Usar "Gerenciador de sistema ou API ONTAP" para implantar LUN em hosts vSphere. * Use a interface de usuário do SDDC Manager para implantar um cluster adicional. Mas esta opção só cria um armazenamento de dados VSAN até a versão 5.2.x.

Domínio de Carga de Trabalho VI - Cluster Padrão

Depois que o domínio de gerenciamento estiver instalado e funcionando, o domínio de carga de trabalho do VI poderá ser criado:

- Usando a interface de usuário do SDDC Manager. Os hosts vSphere devem ter o armazenamento de dados VMFS configurado. Use o System Manager ou a API ONTAP para implantar LUN em hosts vSphere.
- Importe um ambiente vSphere existente como novo domínio de carga de trabalho do VI. ONTAP tools for VMware vSphere, System Manager ou API ONTAP podem ser usadas para implantar o armazenamento de dados VMFS no cluster vSphere.

Domínio de Carga de Trabalho VI - Cluster Adicional

Depois que a carga de trabalho do VI estiver ativa e em execução, clusters adicionais poderão ser implantados com o VMFS no FC LUN usando as seguintes opções.

- Clusters adicionais no ambiente vSphere importados usando a ferramenta de importação brownfield do VCF. ONTAP tools for VMware vSphere, System Manager ou API ONTAP podem ser usadas para implantar o armazenamento de dados VMFS no cluster vSphere.
- Usando a interface de usuário ou API do SDDC Manager para implantar um cluster adicional. Os hosts vSphere devem ter o armazenamento de dados VMFS configurado. Use o System Manager ou a API ONTAP para implantar LUN em hosts vSphere.

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Use um armazenamento de dados NFS no ONTAP como armazenamento principal para um domínio de carga de trabalho VI

Neste caso de uso, descrevemos o procedimento para configurar um armazenamento de dados NFS no ONTAP como a solução de armazenamento primária para um domínio de carga de trabalho de infraestrutura virtual (VI) do VMware Cloud Foundation (VCF). Este procedimento resume os componentes necessários, as etapas de configuração e o processo de implantação.

Benefícios do NFS

Simplicidade e facilidade de uso: O NFS é simples de configurar e gerenciar, o que o torna uma excelente escolha para ambientes que exigem compartilhamento de arquivos rápido e fácil.

Escalabilidade: a arquitetura do ONTAP permite que o NFS seja dimensionado de forma eficiente, dando suporte às crescentes necessidades de dados sem mudanças significativas na infraestrutura.

Flexibilidade: O NFS oferece suporte a uma ampla variedade de aplicativos e cargas de trabalho, o que o torna versátil para vários casos de uso, incluindo ambientes virtualizados.

Para obter mais informações, consulte o Guia de referência do NFS v3 para vSphere 8.

Para obter mais informações sobre o uso do Fibre Channel com sistemas de armazenamento NetApp , consulte"Guia de referência do NFS v3 para vSphere 8" .

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Crie uma máquina virtual de armazenamento (SVM) com interface lógica (LIFs) para tráfego NFS
- Verifique a rede da máquina virtual de armazenamento ONTAP (SVM) e se uma interface lógica (LIF) está presente para transportar o tráfego NFS.
- Crie uma política de exportação para permitir que os hosts ESXi acessem o volume NFS.
- Crie um volume NFS no sistema de armazenamento ONTAP .
- Crie um pool de rede para tráfego NFS e vMotion no SDDC Manager.
- Comissionar hosts no VCF para uso em um domínio de carga de trabalho do VI.
- Implante um domínio de carga de trabalho VI no VCF usando um armazenamento de dados NFS como armazenamento principal.
- Instalar o plug-in NetApp NFS para VMware VAAI

> Esta solução é aplicável para plataformas ONTAP que suportam armazenamento NFS, incluindo NetApp AFF e FAS.

Pré-requisitos

Os seguintes componentes e configurações são usados neste cenário:

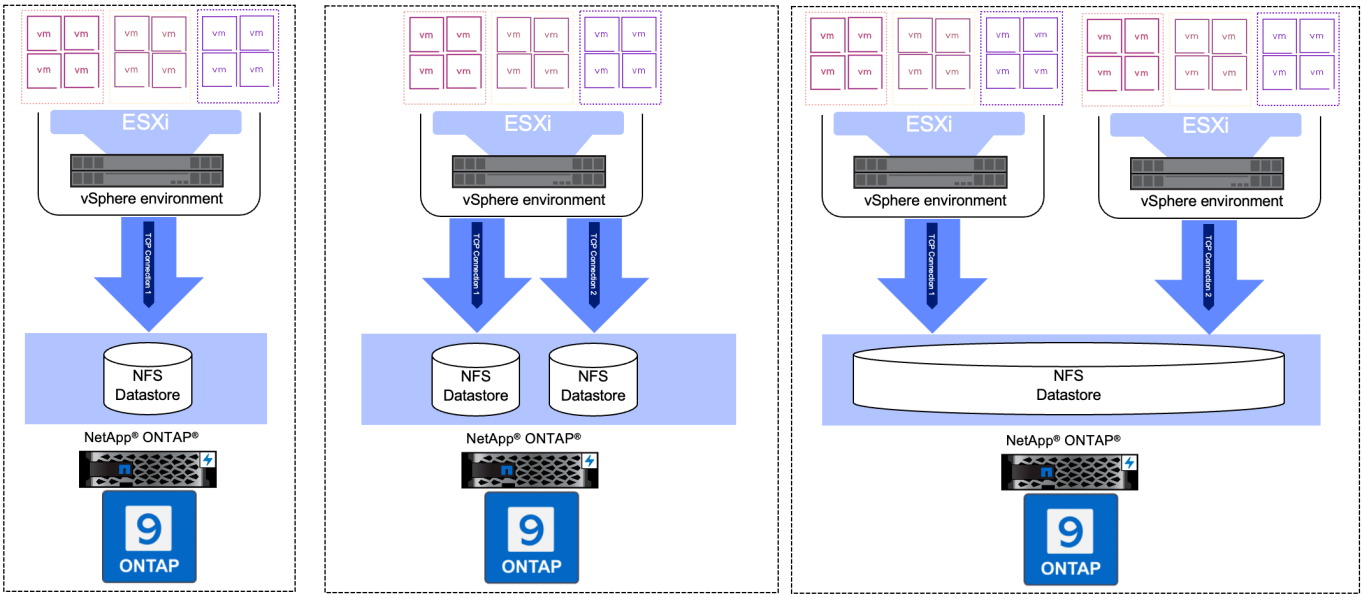
- Sistema de armazenamento NetApp AFF com uma máquina virtual de armazenamento (SVM) configurada para permitir tráfego NFS.
- A interface lógica (LIF) foi criada na rede IP que transportará o tráfego NFS e está associada ao SVM.
- A implantação do domínio de gerenciamento do VCF foi concluída e a interface do SDDC Manager está acessível.
- 4 hosts ESXi configurados para comunicação na rede de gerenciamento VCF.
- Endereços IP reservados para tráfego de armazenamento vMotion e NFS na VLAN ou segmento de rede estabelecido para essa finalidade.

> Ao implantar um domínio de carga de trabalho VI, o VCF valida a conectividade com o servidor NFS. Isso é feito usando o adaptador de gerenciamento nos hosts ESXi antes que qualquer adaptador vmkernel adicional seja adicionado com o endereço IP do NFS. Portanto, é necessário garantir que 1) a rede de gerenciamento seja roteável para o servidor NFS ou 2) um LIF para a rede de gerenciamento tenha sido adicionado ao SVM que hospeda o volume do armazenamento de dados NFS, para garantir que a validação possa prosseguir.

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Para obter mais informações sobre o uso do NFS com clusters vSphere, consulte o"Guia de referência do NFS v3 para vSphere 8" .



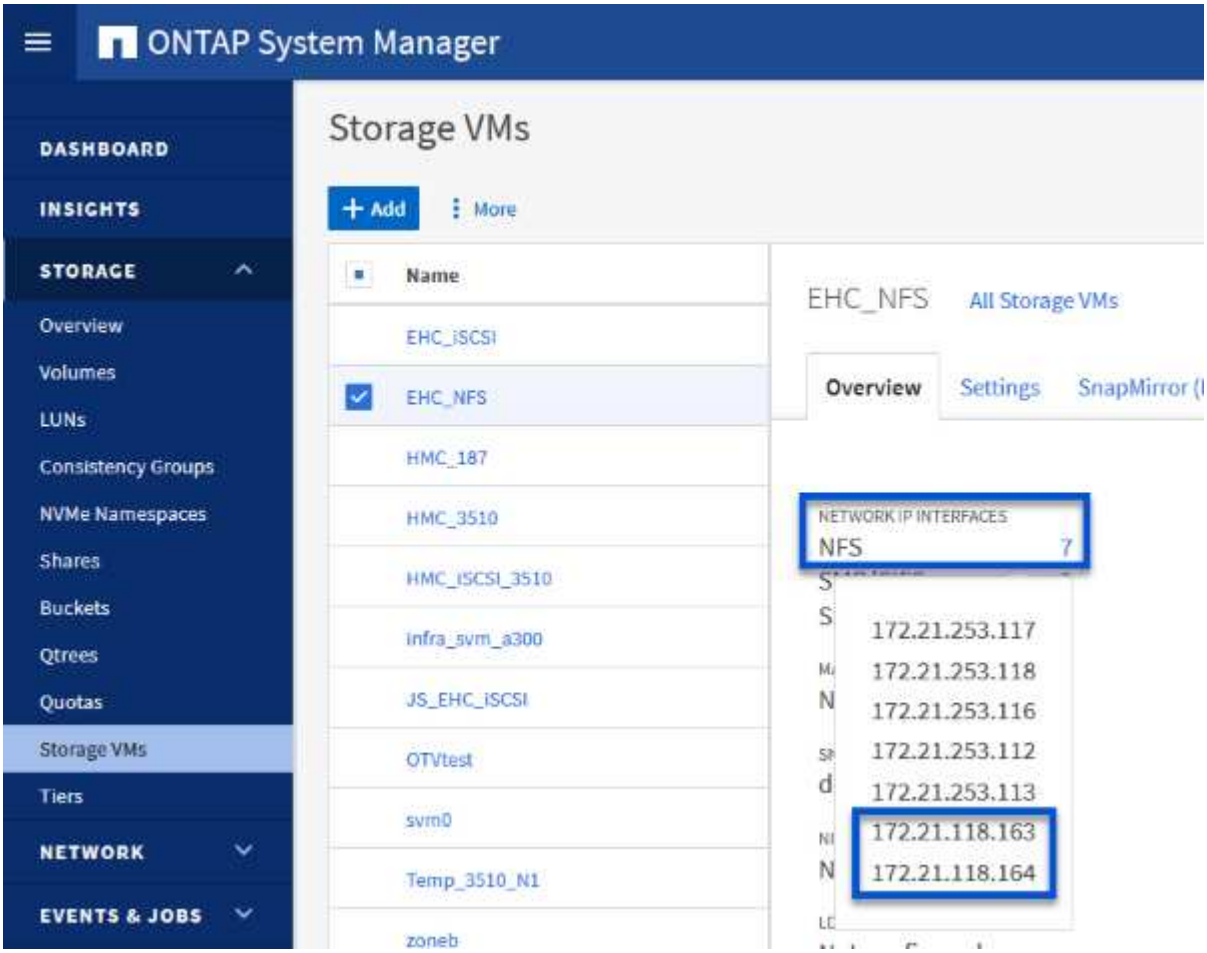
Etapas de implantação

Para implantar um domínio de carga de trabalho VI com um armazenamento de dados NFS como armazenamento principal, conclua as seguintes etapas:

Verificar rede para ONTAP SVM

Verifique se as interfaces lógicas necessárias foram estabelecidas para a rede que transportará o tráfego NFS entre o cluster de armazenamento ONTAP e o domínio de carga de trabalho VI.

1. No ONTAP System Manager, navegue até **VMs de armazenamento** no menu à esquerda e clique na SVM a ser usada para o tráfego NFS. Na guia **Visão geral**, em **INTERFACES IP DE REDE**, clique no número à direita de **NFS**. Na lista, verifique se os endereços IP do LIF necessários estão listados.



Como alternativa, verifique os LIFs associados a uma SVM na CLI do ONTAP com o seguinte comando:

```
network interface show -vserver <SVM_NAME>
```

1. Verifique se os hosts ESXi podem se comunicar com o servidor ONTAP NFS. Efetue login no host ESXi via SSH e faça ping no SVM LIF:

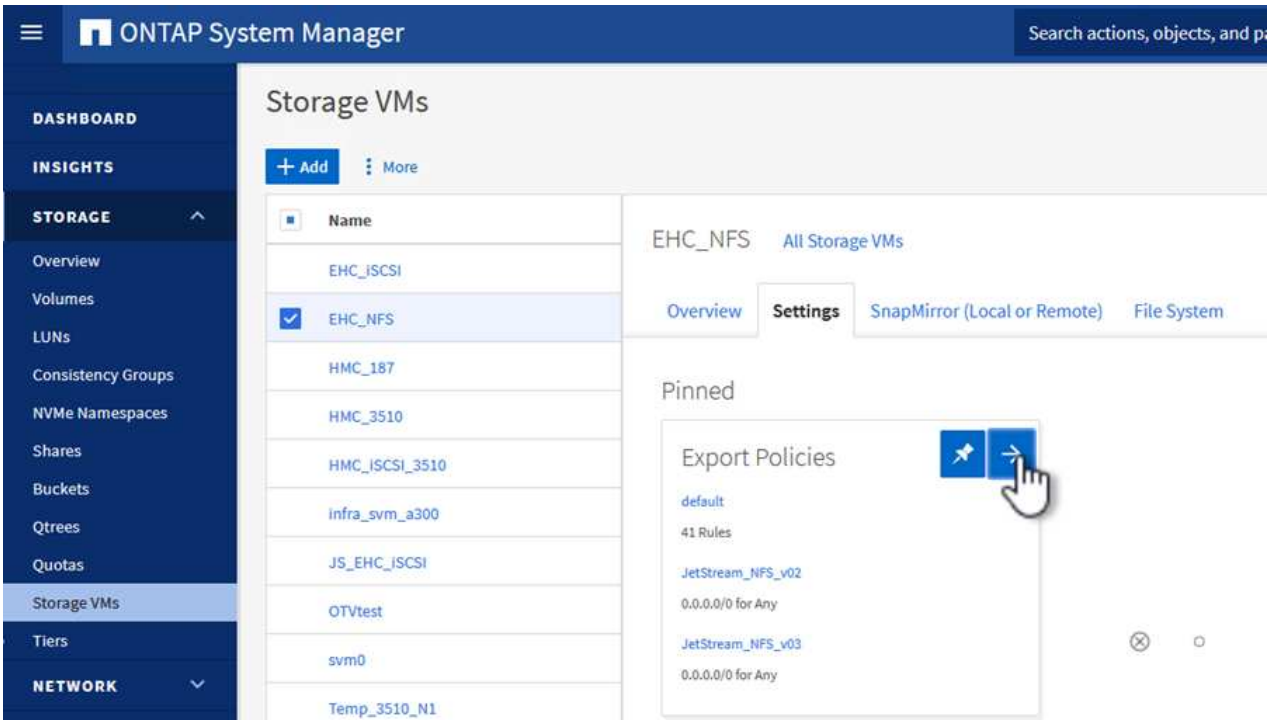
```
vmkping <IP Address>
```

Ao implantar um domínio de carga de trabalho VI, o VCF valida a conectividade com o servidor NFS. Isso é feito usando o adaptador de gerenciamento nos hosts ESXi antes que qualquer adaptador vmkernel adicional seja adicionado com o endereço IP do NFS. Portanto, é necessário garantir que 1) a rede de gerenciamento seja roteável para o servidor NFS ou 2) um LIF para a rede de gerenciamento tenha sido adicionado ao SVM que hospeda o volume do armazenamento de dados NFS, para garantir que a validação possa prosseguir.

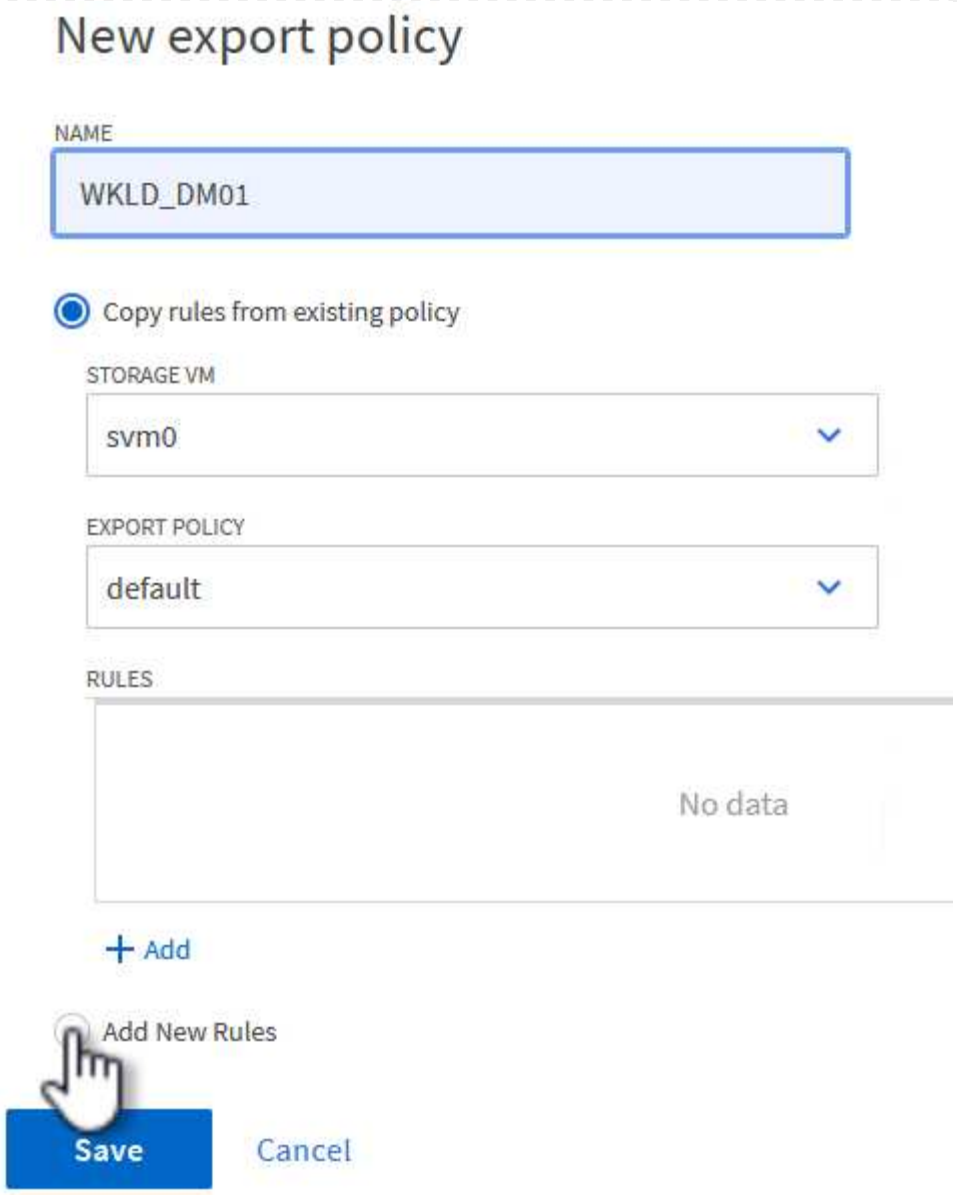
Criar política de exportação para compartilhar volume NFS

Crie uma política de exportação no ONTAP System Manager para definir o controle de acesso para volumes NFS.

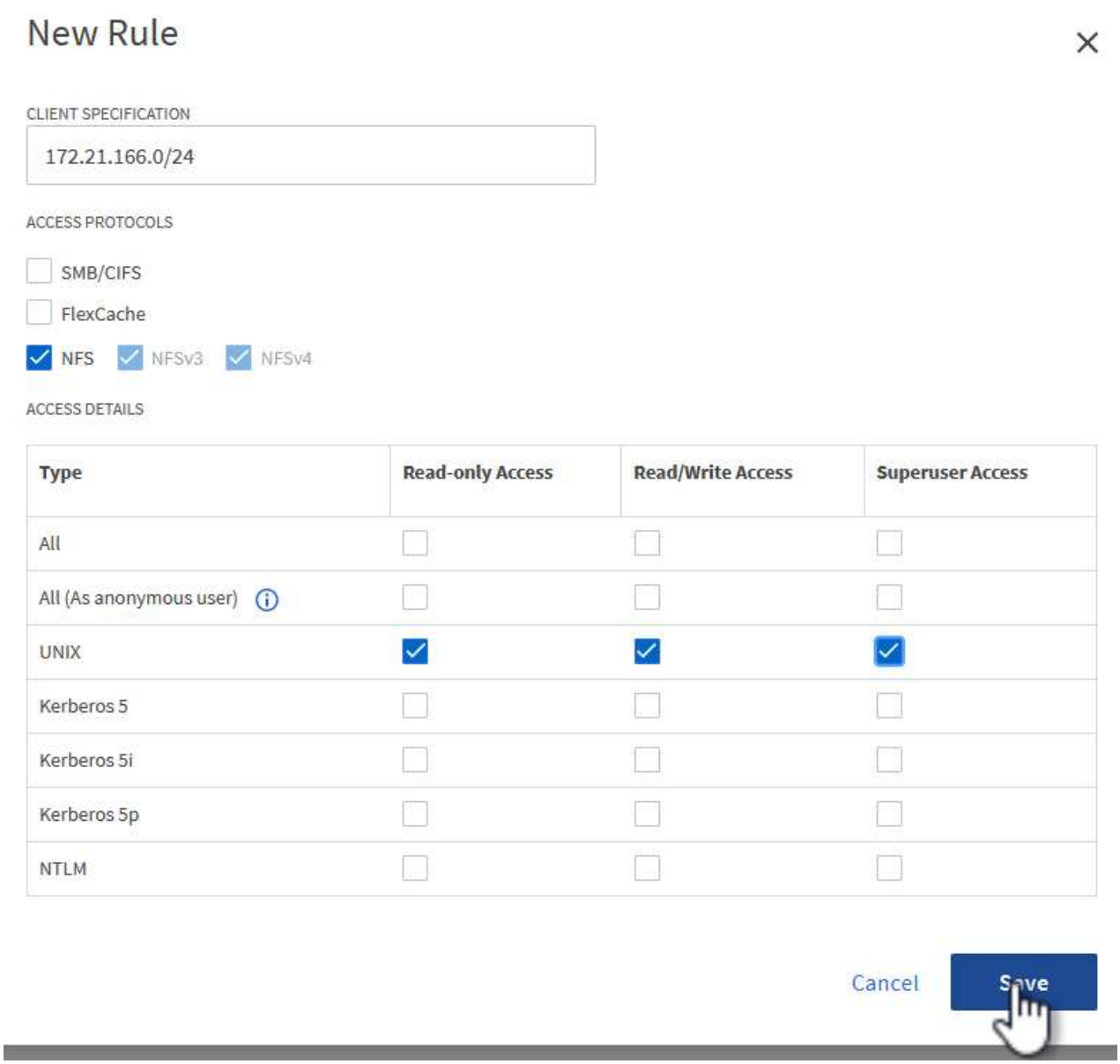
1. No ONTAP System Manager, clique em **VMs de armazenamento** no menu à esquerda e selecione uma SVM na lista.
2. Na aba **Configurações** localize **Políticas de Exportação** e clique na seta para acessar.



3. Na janela **Nova política de exportação**, adicione um nome para a política, clique no botão **Adicionar novas regras** e depois no botão **+Adicionar** para começar a adicionar uma nova regra.



4. Preencha os endereços IP, o intervalo de endereços IP ou a rede que você deseja incluir na regra. Desmarque as caixas **SMB/Cifs** e * FlexCache* e faça seleções para os detalhes de acesso abaixo. Selecionar as caixas UNIX é suficiente para acesso ao host ESXi.



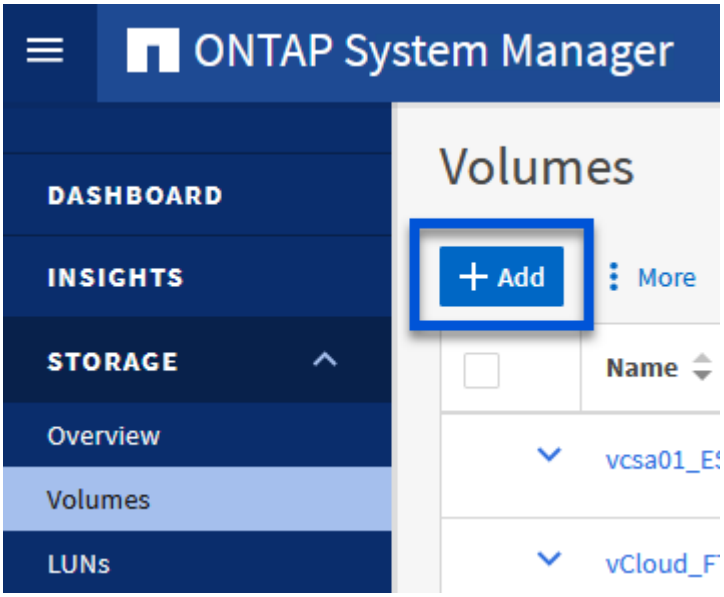
> Ao implantar um domínio de carga de trabalho VI, o VCF valida a conectividade com o servidor NFS. Isso é feito usando o adaptador de gerenciamento nos hosts ESXi antes que qualquer adaptador vmkernel adicional seja adicionado com o endereço IP do NFS. Portanto, é necessário garantir que a política de exportação inclua a rede de gerenciamento do VCF para permitir que a validação prossiga.

5. Depois que todas as regras forem inseridas, clique no botão **Salvar** para salvar a nova Política de Exportação.
6. Como alternativa, você pode criar políticas e regras de exportação no ONTAP CLI. Consulte as etapas para criar uma política de exportação e adicionar regras na documentação do ONTAP .
   - Use o ONTAP CLI para"Crie uma política de exportação" .
   - Use o ONTAP CLI para"Adicionar uma regra a uma política de exportação" .

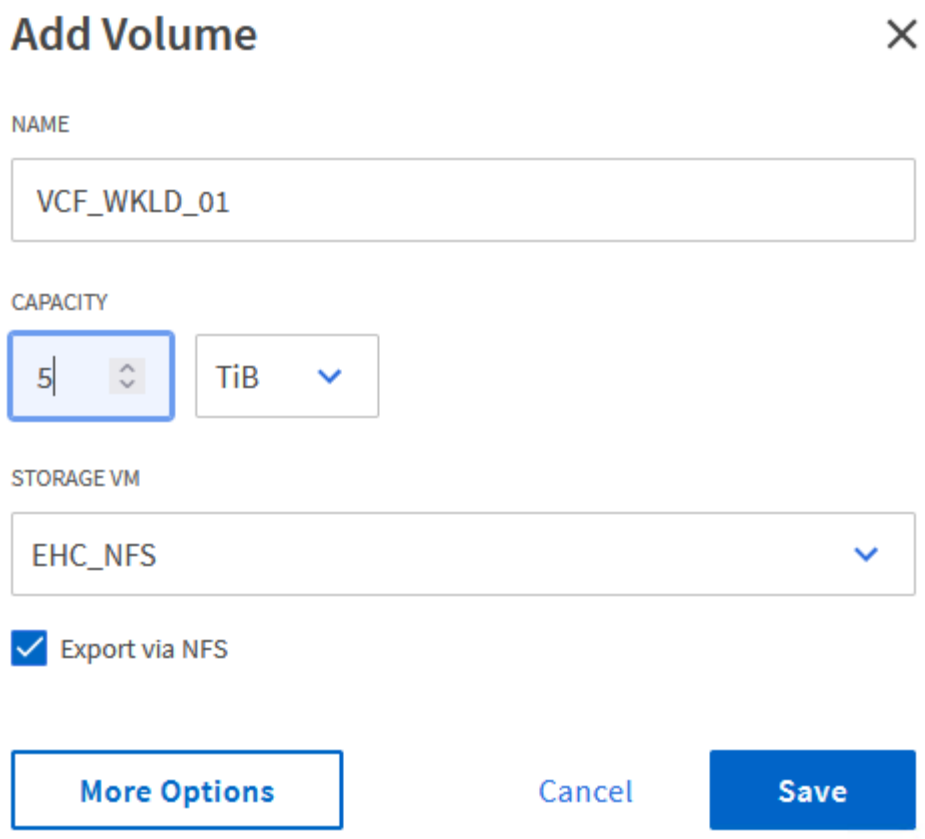
Criar volume NFS

Crie um volume NFS no sistema de armazenamento ONTAP para ser usado como um armazenamento de dados na implantação do Domínio de Carga de Trabalho.

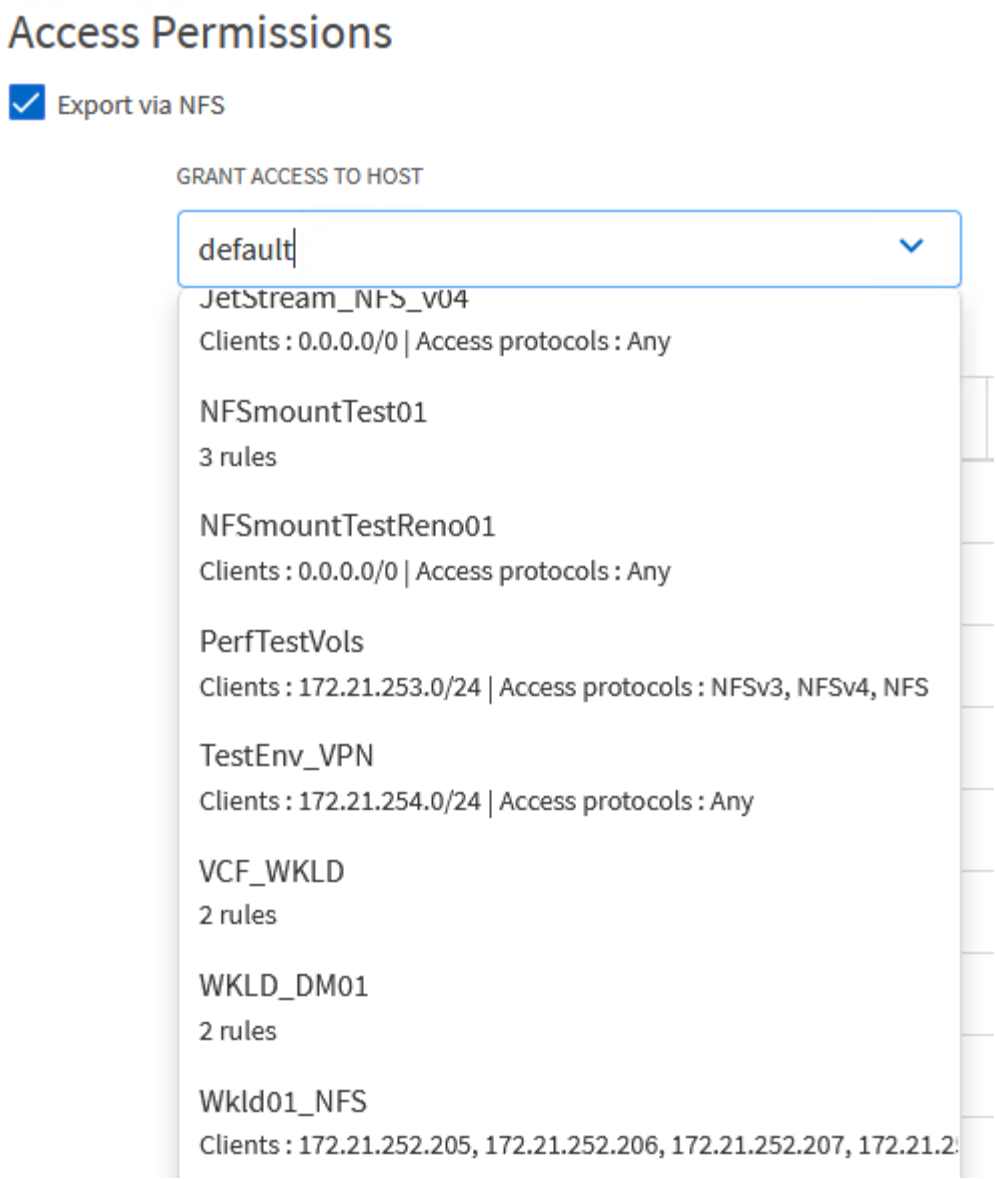
1. No ONTAP System Manager, navegue até **Armazenamento > Volumes** no menu à esquerda e clique em **+Adicionar** para criar um novo volume.



2. Adicione um nome para o volume, preencha a capacidade desejada e selecione a VM de armazenamento que hospedará o volume. Clique em **Mais opções** para continuar.



3. Em Permissões de acesso, selecione a Política de exportação que inclui a rede de gerenciamento do VCF ou endereço IP e endereços IP da rede NFS que serão usados para validação do servidor NFS e do tráfego NFS.



+

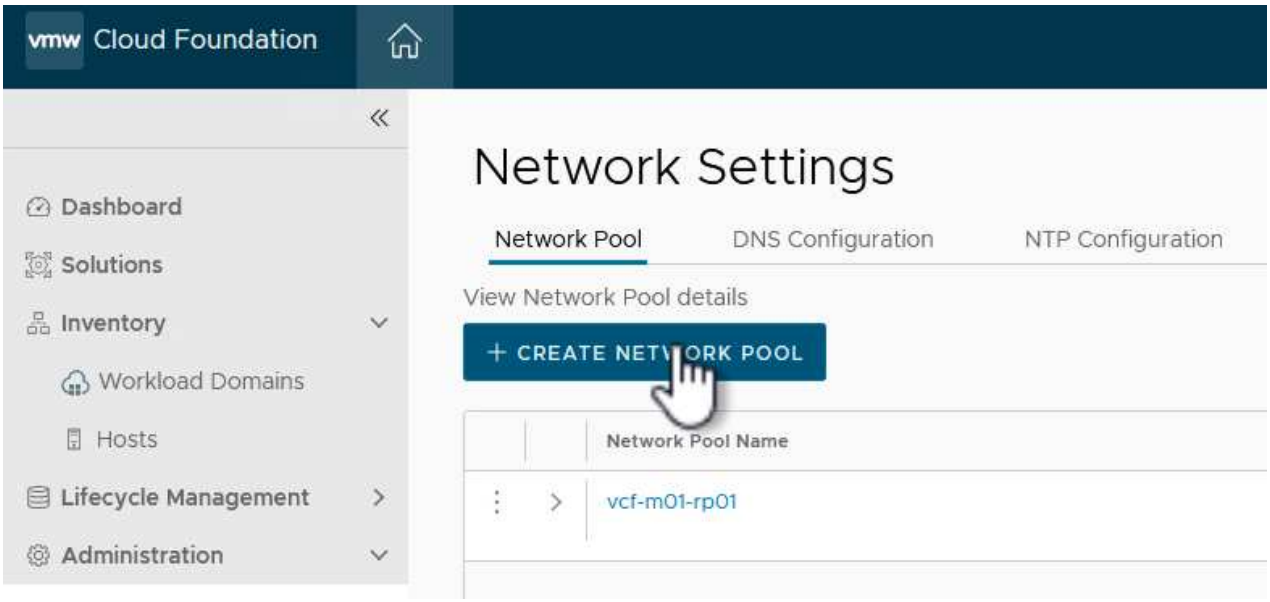
> Ao implantar um domínio de carga de trabalho VI, o VCF valida a conectividade com o servidor NFS. Isso é feito usando o adaptador de gerenciamento nos hosts ESXi antes que qualquer adaptador vmkernel adicional seja adicionado com o endereço IP do NFS. Portanto, é necessário garantir que 1) a rede de gerenciamento seja roteável para o servidor NFS ou 2) um LIF para a rede de gerenciamento tenha sido adicionado ao SVM que hospeda o volume do armazenamento de dados NFS, para garantir que a validação possa prosseguir.

4. Como alternativa, os volumes ONTAP podem ser criados no ONTAP CLI. Para mais informações consulte o"lun criar" comando na documentação de comandos do ONTAP .

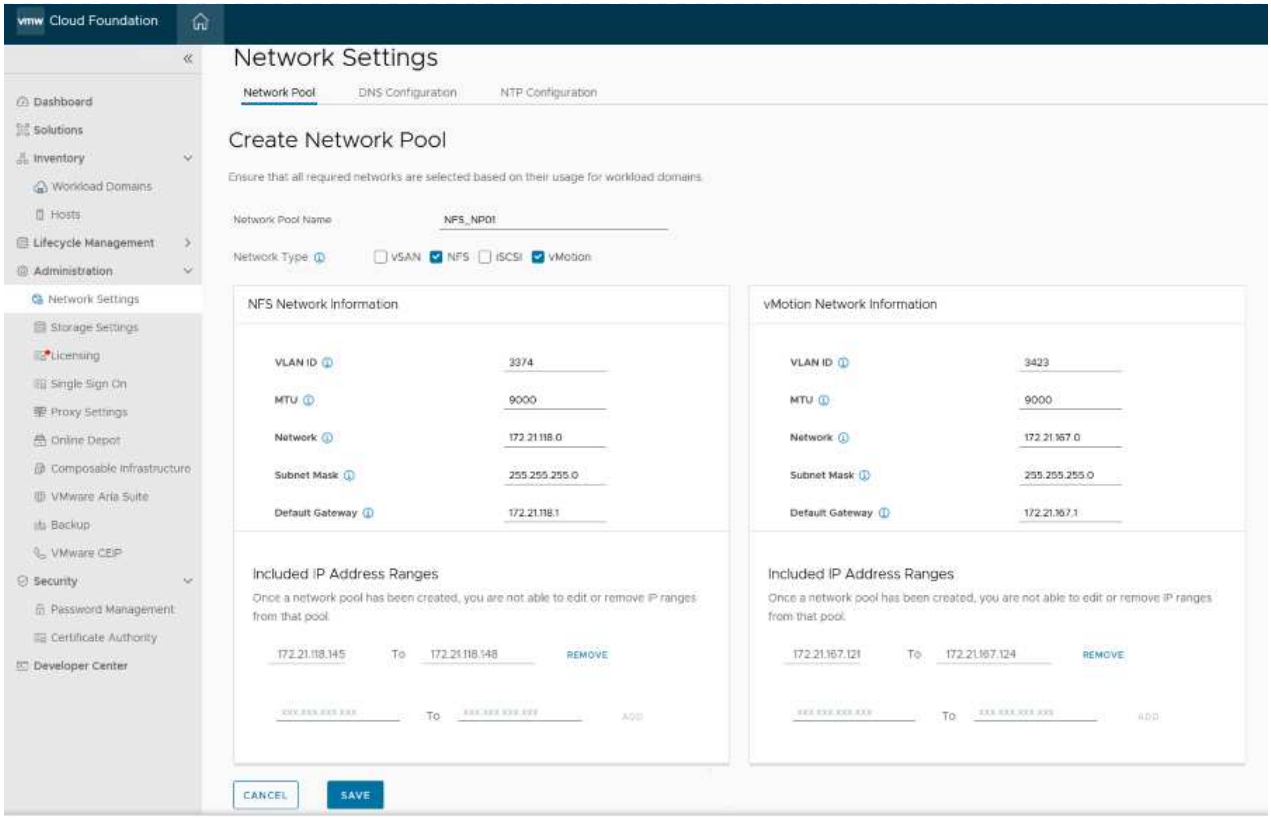
Criar pool de rede no Gerenciador SDDC

Um pool de rede deve ser criado no SDDC Manager antes de comissionar os hosts ESXi, como preparação para implantá-los em um domínio de carga de trabalho do VI. O pool de rede deve incluir as informações de rede e os intervalos de endereços IP para que os adaptadores VMkernel sejam usados para comunicação com o servidor NFS.

1. Na interface da web do SDDC Manager, navegue até **Configurações de rede** no menu à esquerda e clique no botão **+ Criar pool de rede**.



2. Preencha um nome para o Network Pool, marque a caixa de seleção para NFS e preencha todos os detalhes de rede. Repita isso para as informações de rede do vMotion.



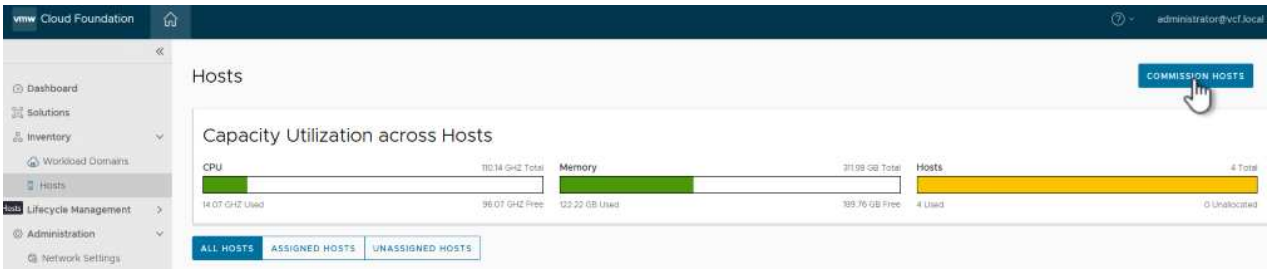
3. Clique no botão **Salvar** para concluir a criação do Pool de Rede.

Anfitriões da Comissão

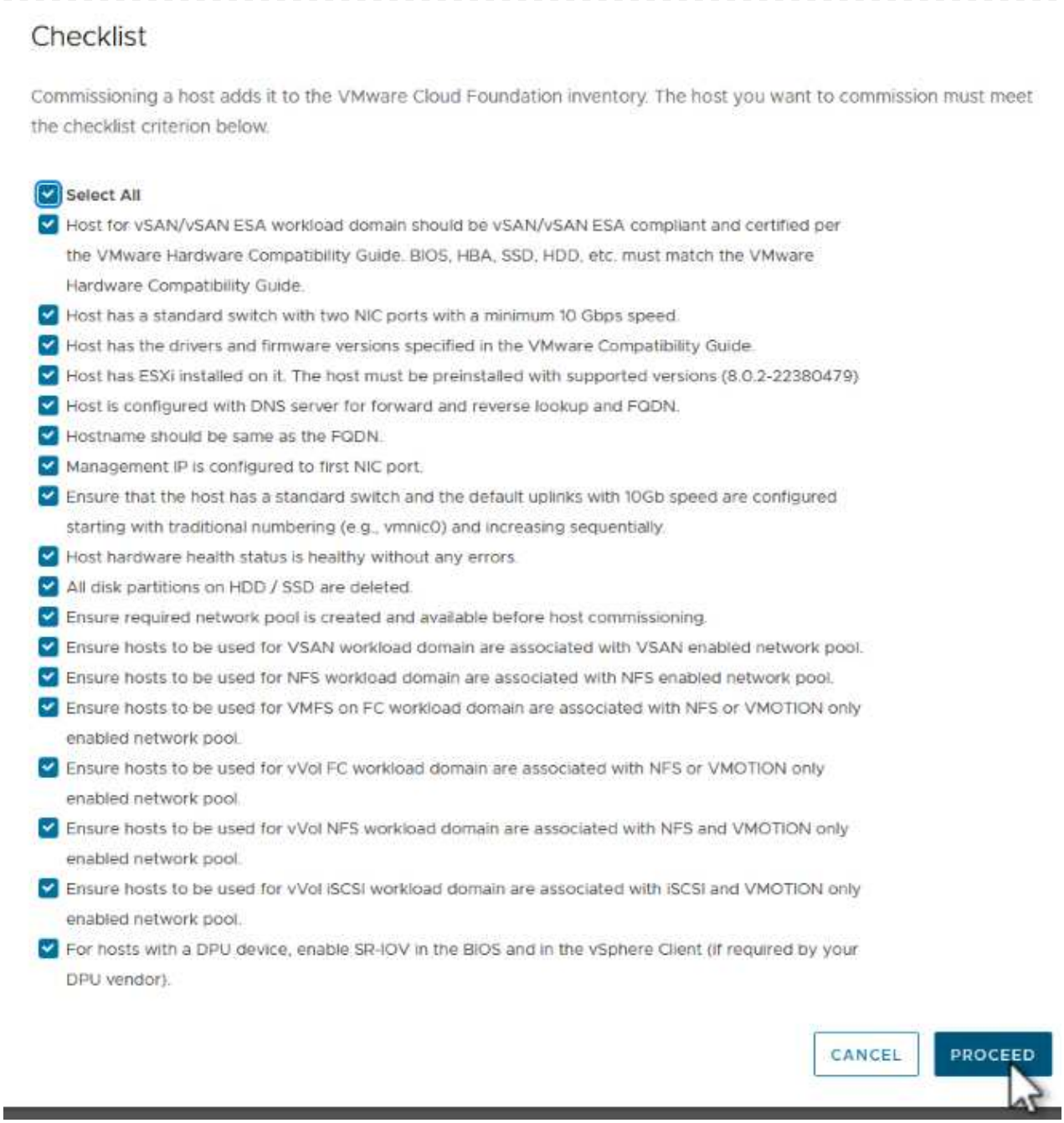
Antes que os hosts ESXi possam ser implantados como um domínio de carga de trabalho, eles devem ser adicionados ao inventário do SDDC Manager. Isso envolve fornecer as informações necessárias, passar pela validação e iniciar o processo de comissionamento.

Para mais informações, consulte"Anfitriões da Comissão" no Guia de Administração do VCF.

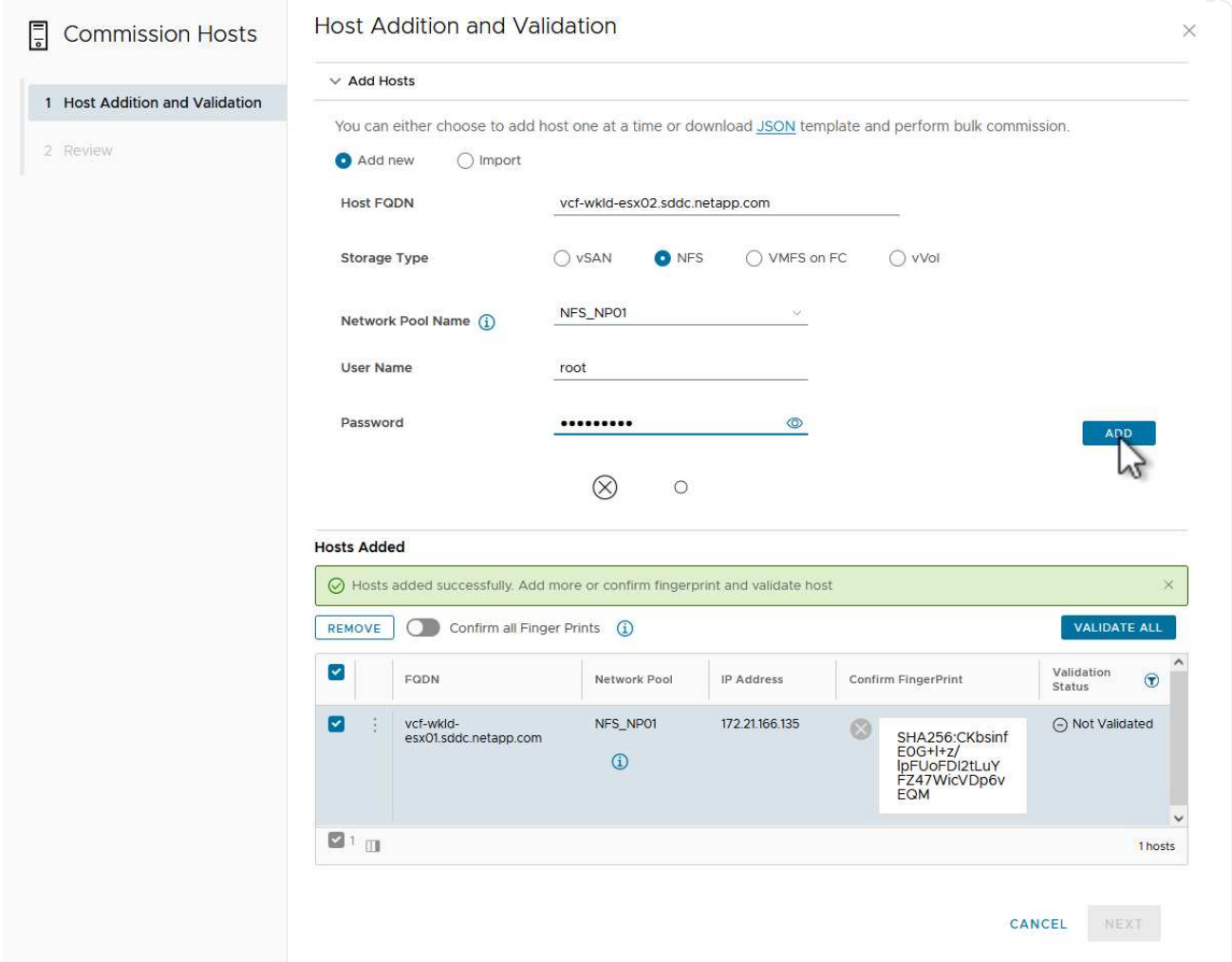
1. Na interface do SDDC Manager, navegue até **Hosts** no menu à esquerda e clique no botão **Comissionar Hosts**.



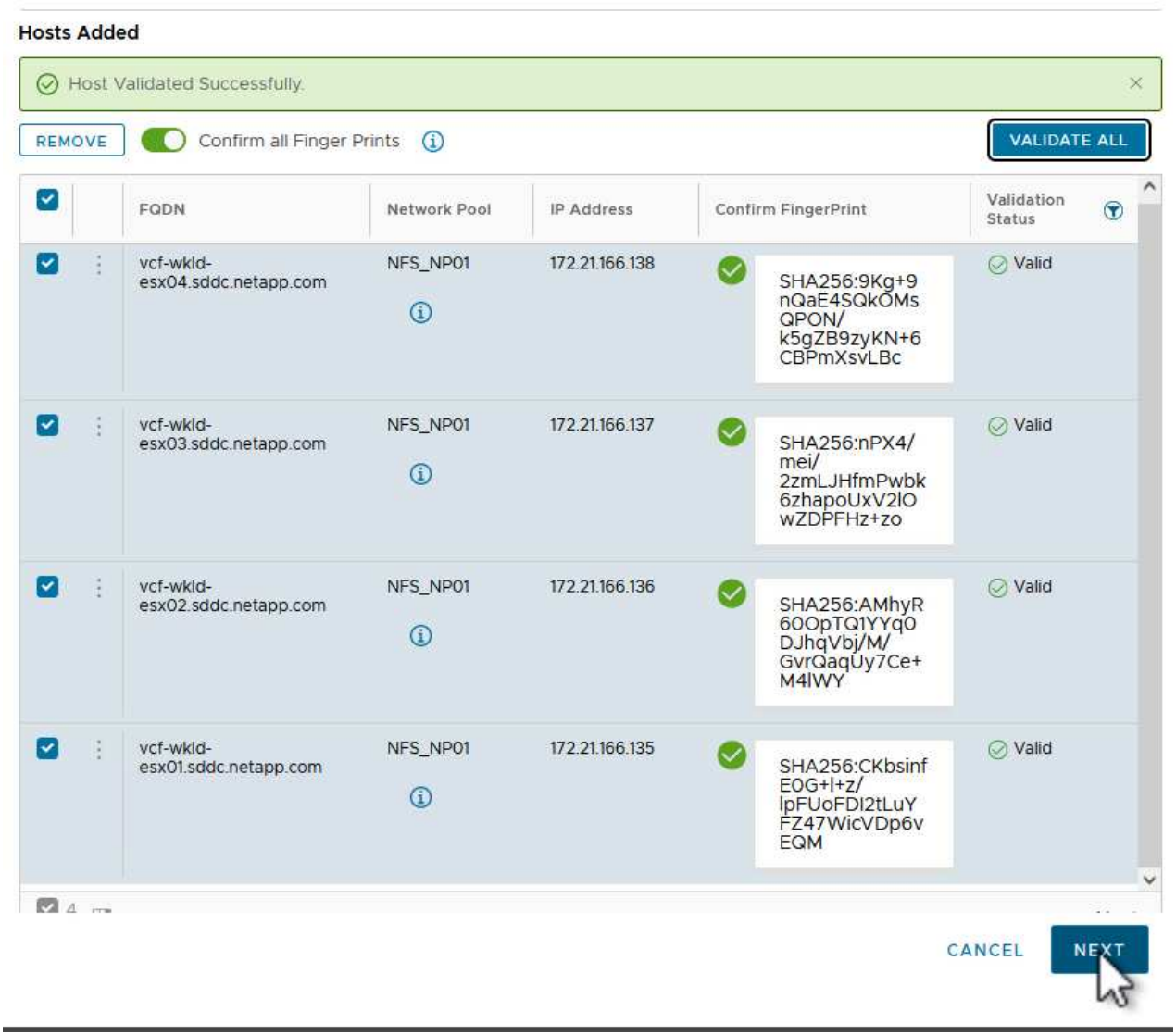
2. A primeira página é uma lista de verificação de pré-requisitos. Verifique novamente todos os pré-requisitos e marque todas as caixas de seleção para prosseguir.



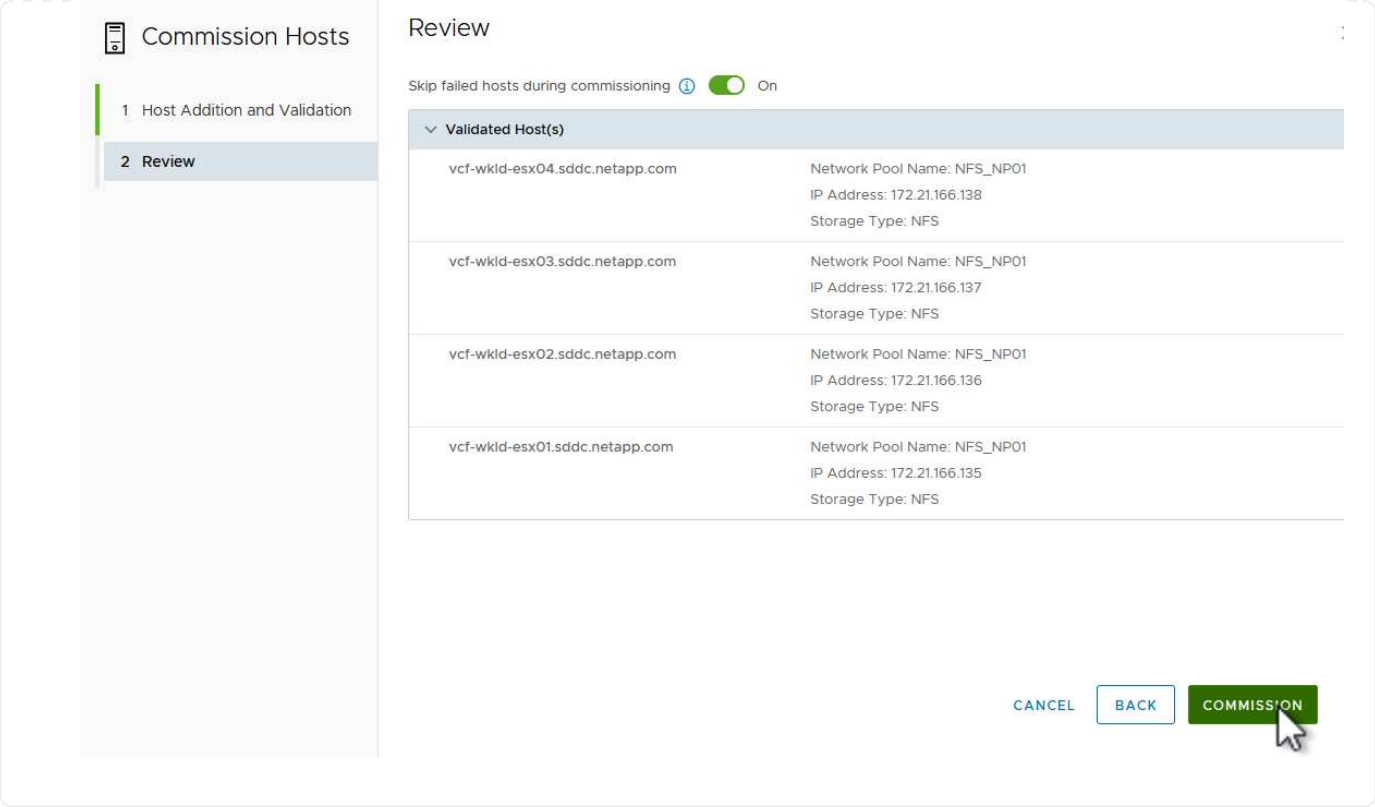
3. Na janela **Adição e validação de host**, preencha o **FQDN do host**, o **Tipo de armazenamento**, o nome do **pool de rede** que inclui os endereços IP de armazenamento vMotion e NFS a serem usados para o domínio de carga de trabalho e as credenciais para acessar o host ESXi. Clique em **Adicionar** para adicionar o host ao grupo de hosts a serem validados.



4. Depois que todos os hosts a serem validados forem adicionados, clique no botão **Validar todos** para continuar.
5. Supondo que todos os hosts estejam validados, clique em **Avançar** para continuar.



6. Revise a lista de hosts a serem comissionados e clique no botão **Comissão** para iniciar o processo. Monitore o processo de comissionamento no painel de tarefas no gerenciador do SDDC.

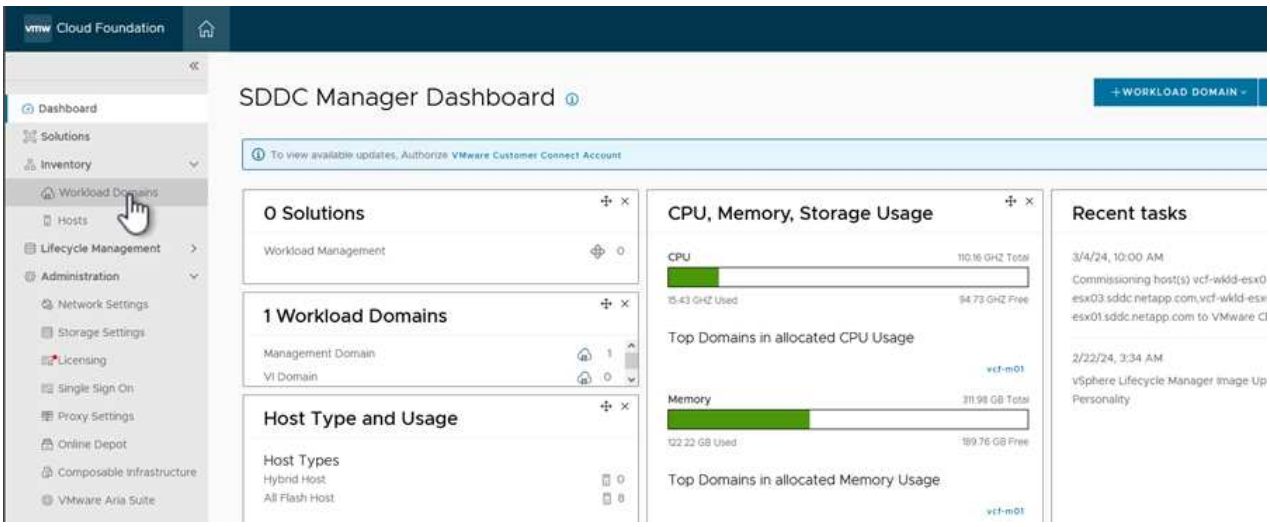

Commission Hosts
1 Host Addition and Validation
2 Review
Review
Skip failed hosts during commissioning
On
Validated Host(s)
vcf-wkld-esx04.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.138
Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.137
Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.136
Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.135
Storage Type: NFS
CANCEL
BACK
COMMISSION

Implantar domínio de carga de trabalho do VI

A implantação de domínios de carga de trabalho do VI é realizada usando a interface do VCF Cloud Manager. Aqui serão apresentadas apenas as etapas relacionadas à configuração do armazenamento.

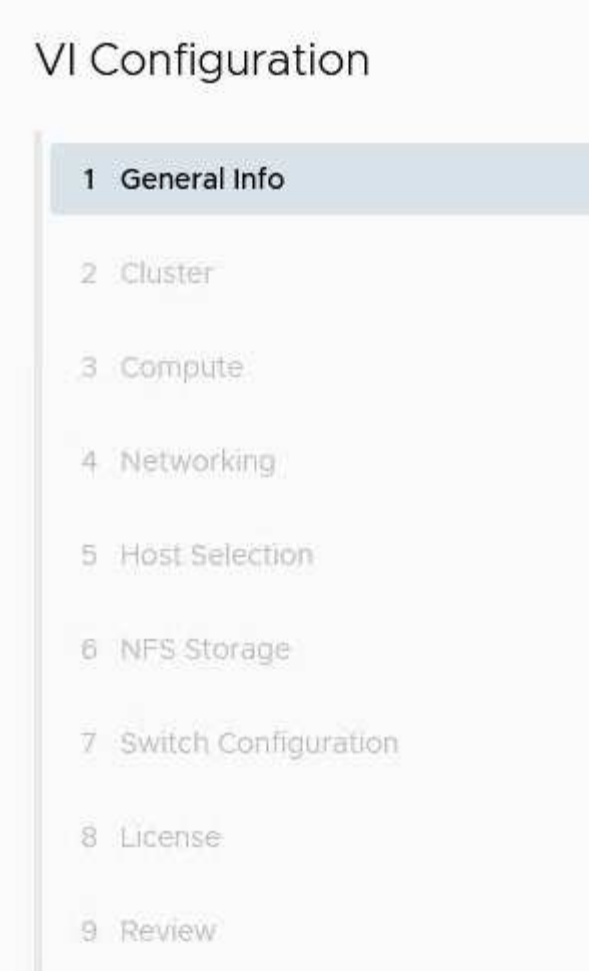
Para obter instruções passo a passo sobre como implantar um domínio de carga de trabalho VI, consulte"Implantar um domínio de carga de trabalho do VI usando a interface de usuário do Gerenciador do SDDC" .

1. No painel do SDDC Manager, clique em **+ Domínio de carga de trabalho** no canto superior direito para criar um novo domínio de carga de trabalho.



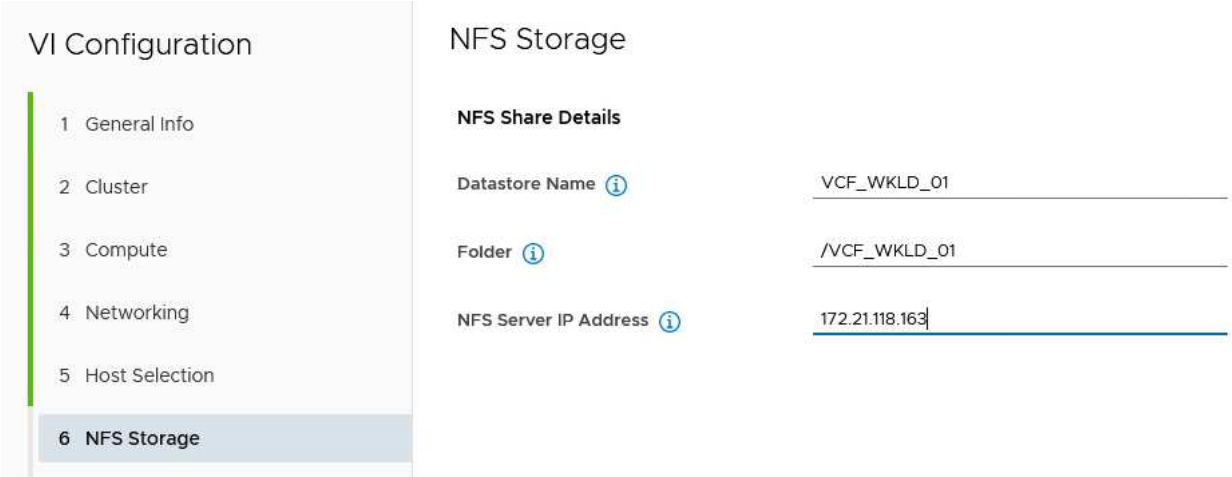
2. No assistente de configuração do VI, preencha as seções **Informações gerais, Cluster, Computação, Rede** e **Seleção de host**, conforme necessário.

Para obter informações sobre como preencher as informações necessárias no assistente de configuração do VI, consulte"Implantar um domínio de carga de trabalho do VI usando a interface de usuário do Gerenciador do SDDC" .

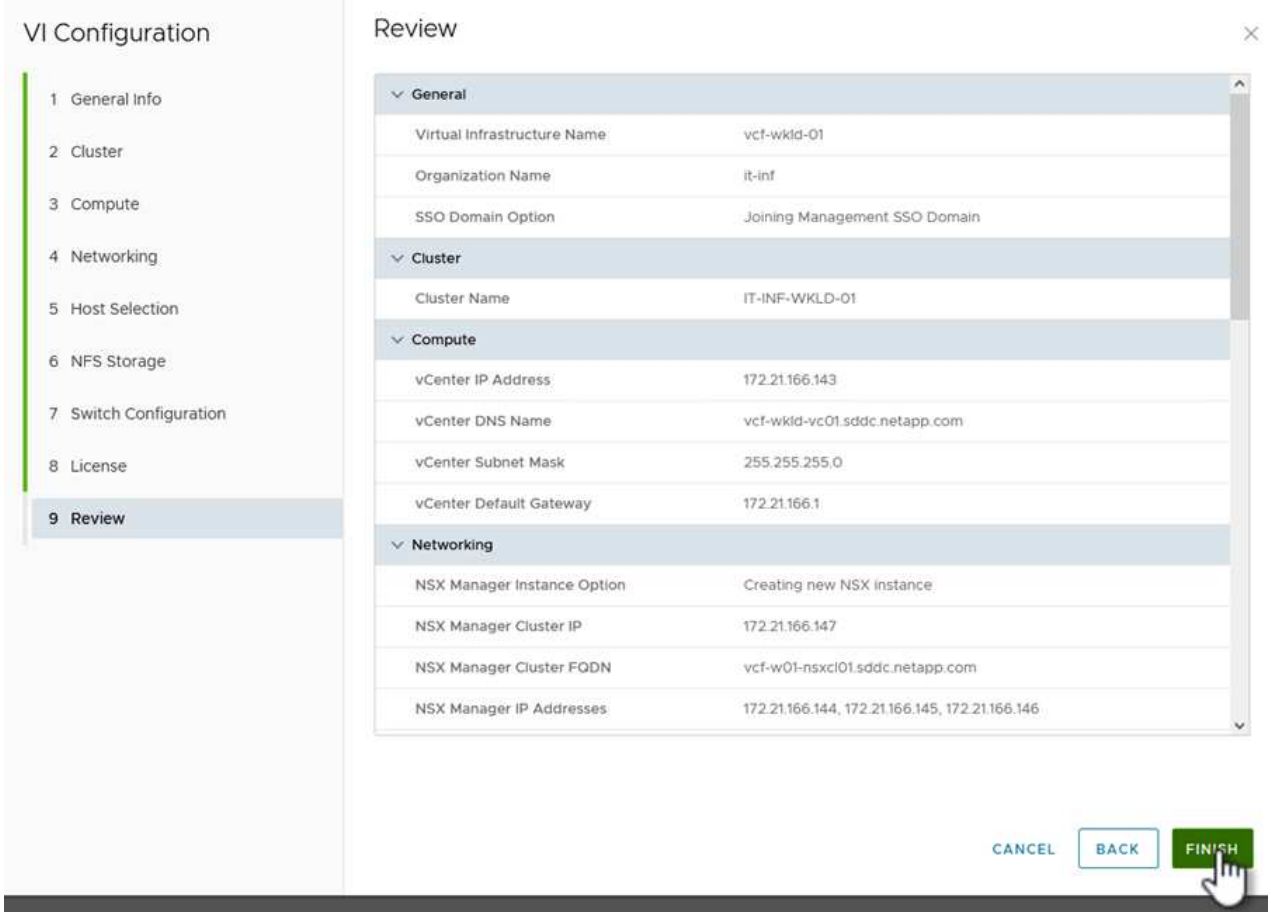


+

1. Na seção Armazenamento NFS, preencha o Nome do Datastore, o ponto de montagem da pasta do volume NFS e o endereço IP do LIF da VM de armazenamento NFS do ONTAP .



2. No assistente de configuração do VI, conclua as etapas de configuração do switch e licença e clique em **Concluir** para iniciar o processo de criação do domínio de carga de trabalho.



3. Monitore o processo e resolva quaisquer problemas de validação que surjam durante o processo.

Instalar o plug-in NetApp NFS para VMware VAAI

O NetApp NFS Plug-in para VMware VAAI integra as bibliotecas de discos virtuais VMware instaladas no host ESXi e fornece operações de clonagem de alto desempenho que terminam mais rapidamente. Este é um procedimento recomendado ao usar sistemas de armazenamento ONTAP com VMware vSphere.

Para obter instruções passo a passo sobre como implantar o NetApp NFS Plug-in para VMware VAAI seguindo as instruções em"Instalar o plug-in NetApp NFS para VMware VAAI" .

Demonstração em vídeo desta solução

Datastores NFS como armazenamento principal para domínios de carga de trabalho VCF

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Expanda o VCF com armazenamento suplementar

Aprenda sobre como expandir o armazenamento para um ambiente VCF usando armazenamento suplementar

O VMware Cloud Foundation (VCF) oferece suporte a uma ampla variedade de opções de armazenamento suplementar para expandir o armazenamento em domínios de gerenciamento de VCF e domínios de carga de trabalho de infraestrutura virtual (VI).

As ferramentas ONTAP da NetApp para VMware vSphere fornecem uma solução eficiente para essa expansão, integrando perfeitamente o armazenamento NetApp ao ambiente VCF. As ferramentas ONTAP simplificam a configuração e o gerenciamento de armazenamentos de dados, permitindo que os administradores provisionem e gerenciem o armazenamento diretamente do vSphere Client. Os recursos avançados do ONTAP, como snapshots, clonagem e proteção de dados, melhoram o desempenho, a eficiência e a escalabilidade do armazenamento no ambiente VCF.

Consulte as soluções a seguir para obter detalhes técnicos sobre como expandir o ambiente VCF.

- "Domínio de gerenciamento com iSCSI"
- "Domínio de Gestão com FC"
- "Domínio de carga de trabalho de infraestrutura virtual com vVols (iSCSI)"
- "Domínio de carga de trabalho de infraestrutura virtual com vVols (NFS)"
- "Domínio de carga de trabalho de infraestrutura virtual com NVMe/TCP"
- "Domínio de carga de trabalho de infraestrutura virtual com FC"

Adicione um armazenamento de dados iSCSI como armazenamento suplementar para um domínio de gerenciamento usando ONTAP tools for VMware vSphere

Neste caso de uso, descrevemos o procedimento para adicionar um armazenamento de dados iSCSI como armazenamento suplementar para um domínio de gerenciamento do VMware Cloud Foundation (VCF). Este procedimento resume a configuração de uma Máquina Virtual de Armazenamento (SVM) com interfaces lógicas (LIFs) para iSCSI, a configuração de rede iSCSI em hosts ESXi, a implantação do ONTAP Tools para VMware vSphere e a criação de um armazenamento de dados VMFS.

Benefícios do iSCSI

Alto desempenho: oferece alto desempenho para fornecer taxas de transferência de dados rápidas e eficientes e baixa latência. Ideal para aplicativos empresariais exigentes e ambientes virtualizados.

Facilidade de gerenciamento: simplifica o gerenciamento de armazenamento usando ferramentas e protocolos familiares baseados em IP.

Custo-benefício: utiliza a infraestrutura Ethernet existente, reduzindo a necessidade de hardware especializado e permitindo que as organizações obtenham soluções de armazenamento confiáveis e escaláveis.

Para obter mais informações sobre o uso do iSCSI com sistemas de armazenamento NetApp , consulte "Provisionamento SAN com iSCSI" .

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

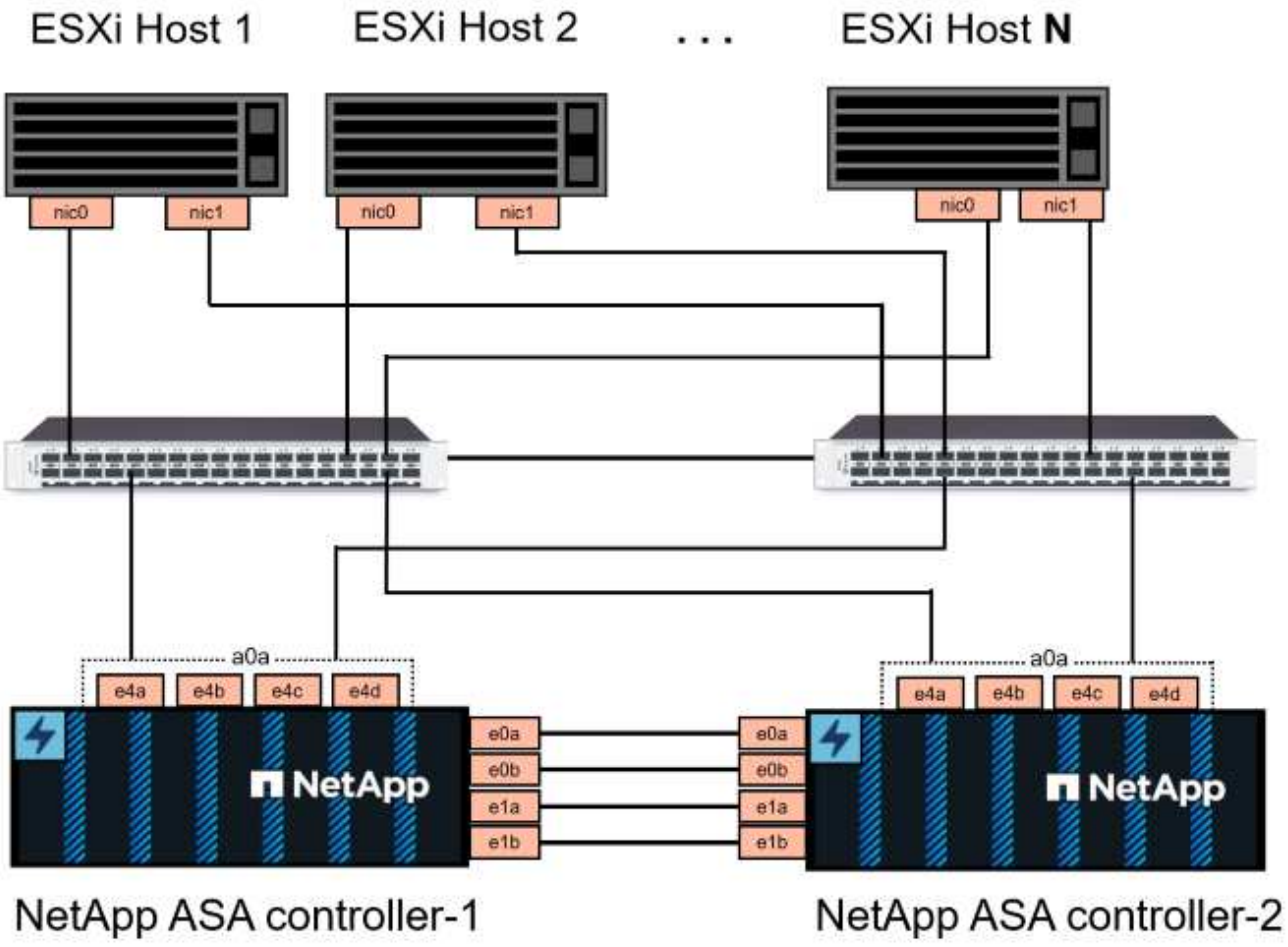
- Crie uma máquina virtual de armazenamento (SVM) com interfaces lógicas (LIFs) para tráfego iSCSI.
- Crie grupos de portas distribuídas para redes iSCSI no domínio de gerenciamento VCF.
- Crie adaptadores vmkernel para iSCSI nos hosts ESXi para o domínio de gerenciamento VCF.
- Implante o ONTAP Tools no domínio de gerenciamento do VCF.
- Crie um novo armazenamento de dados VMFS no domínio de gerenciamento do VCF.

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP AFF ou ASA com portas de dados físicas em switches Ethernet dedicados ao tráfego de armazenamento.
- A implantação do domínio de gerenciamento do VCF foi concluída e o cliente vSphere está acessível.

A NetApp recomenda projetos de rede totalmente redundantes para iSCSI. O diagrama a seguir ilustra um exemplo de configuração redundante, fornecendo tolerância a falhas para sistemas de armazenamento, switches, adaptadores de rede e sistemas host. Consulte o NetApp"Referência de configuração SAN" para obter informações adicionais.



Para multipathing e failover em vários caminhos, a NetApp recomenda ter no mínimo dois LIFs por nó de armazenamento em redes Ethernet separadas para todas as SVMs em configurações iSCSI.

Esta documentação demonstra o processo de criação de um novo SVM e especificação das informações de endereço IP para criar vários LIFs para tráfego iSCSI. Para adicionar novos LIFs a um SVM existente, consulte"Criar uma LIF (interface de rede)" .

Para obter informações adicionais sobre o uso de datastores VMFS iSCSI com VMware, consulte"vSphere VMFS Datastore - backend de armazenamento iSCSI com ONTAP" .

> Em situações em que vários adaptadores VMkernel são configurados na mesma rede IP, é recomendável usar a vinculação de porta iSCSI de software nos hosts ESXi para garantir que o balanceamento de carga entre os adaptadores ocorra. Consulte o artigo da KB"Considerações sobre o uso de vinculação de porta iSCSI de software no ESX/ESXi (2038869)" .

Etapas de implantação

Para implantar o ONTAP Tools e usá-lo para criar um armazenamento de dados VMFS no domínio de gerenciamento do VCF, conclua as seguintes etapas:

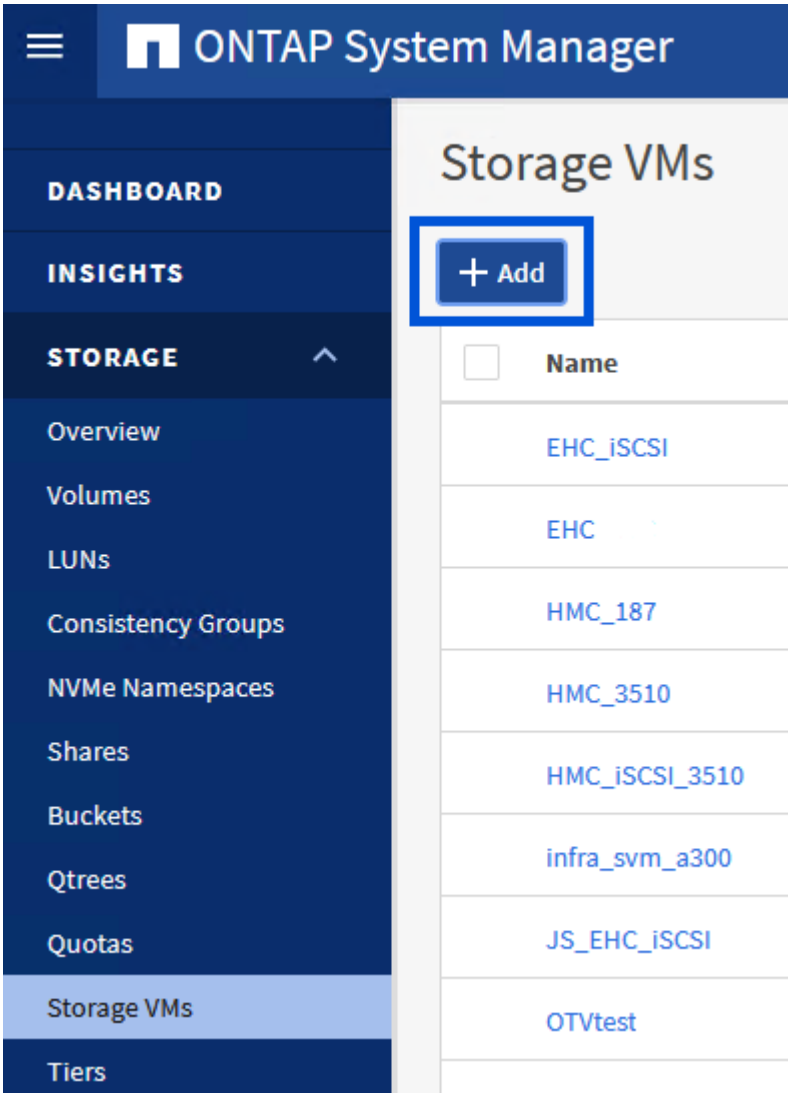
Crie SVM e LIFs no sistema de armazenamento ONTAP

A etapa seguinte é executada no ONTAP System Manager.

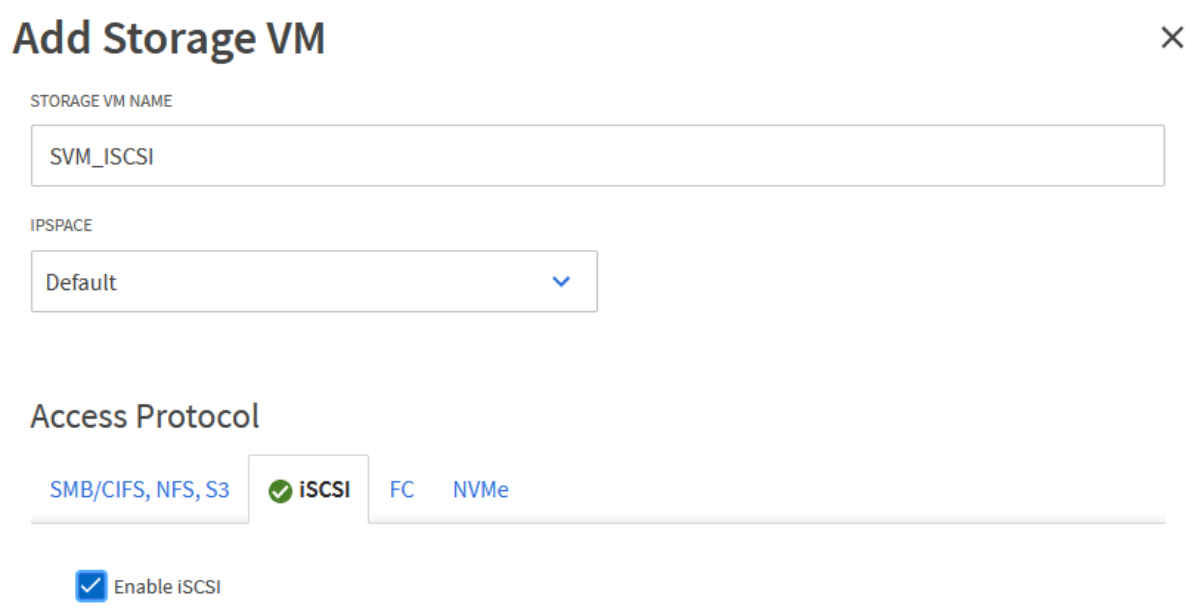
Crie a VM de armazenamento e os LIFs

Conclua as etapas a seguir para criar um SVM junto com vários LIFs para tráfego iSCSI.

1. No ONTAP System Manager, navegue até **VMs de armazenamento** no menu à esquerda e clique em **+ Adicionar** para iniciar.

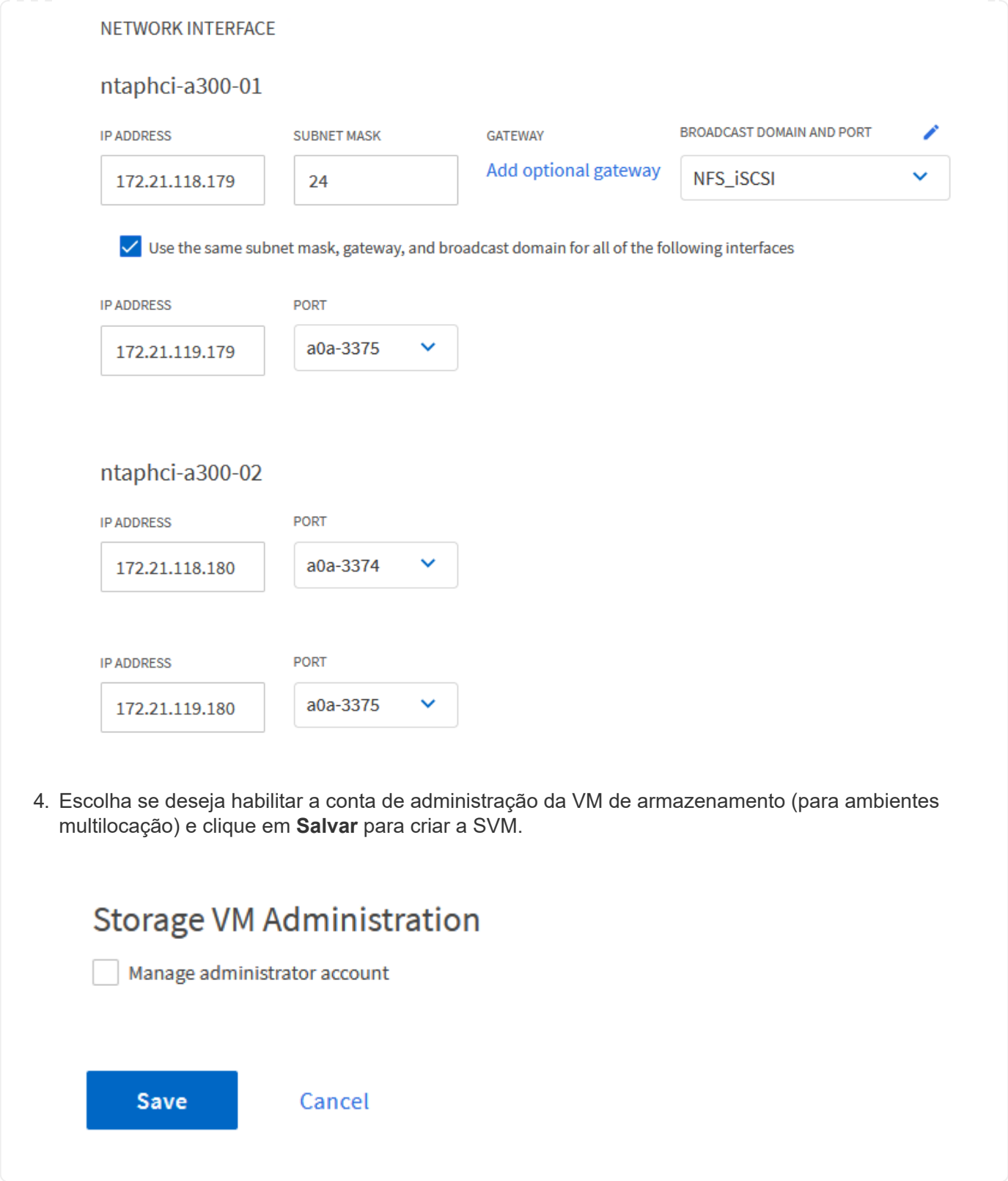


2. No assistente **Adicionar VM de armazenamento**, forneça um **Nome** para a SVM, selecione o **Espaço IP** e, em seguida, em **Protocolo de acesso, clique na guia *iSCSI** e marque a caixa para **Ativar iSCSI**.



3. Na seção **Interface de rede**, preencha o **endereço IP**, a **máscara de sub-rede** e o **domínio e porta de transmissão** para o primeiro LIF. Para LIFs subsequentes, a caixa de seleção pode ser marcada para usar configurações comuns em todos os LIFs restantes ou usar configurações separadas.

> Para multipathing e failover em vários caminhos, a NetApp recomenda ter no mínimo dois LIFs por nó de armazenamento em redes Ethernet separadas para todas as SVMs em configurações iSCSI.



4. Escolha se deseja habilitar a conta de administração da VM de armazenamento (para ambientes multilocação) e clique em **Salvar** para criar a SVM.

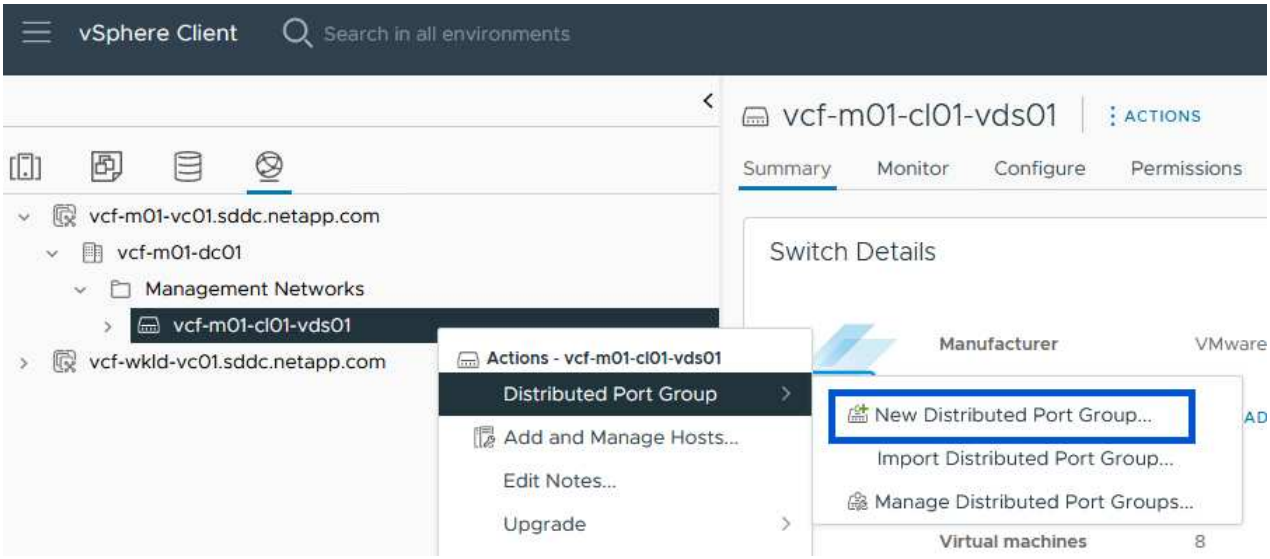
Configurar rede para iSCSI em hosts ESXi

As etapas a seguir são executadas no cluster de domínio de gerenciamento do VCF usando o cliente vSphere.

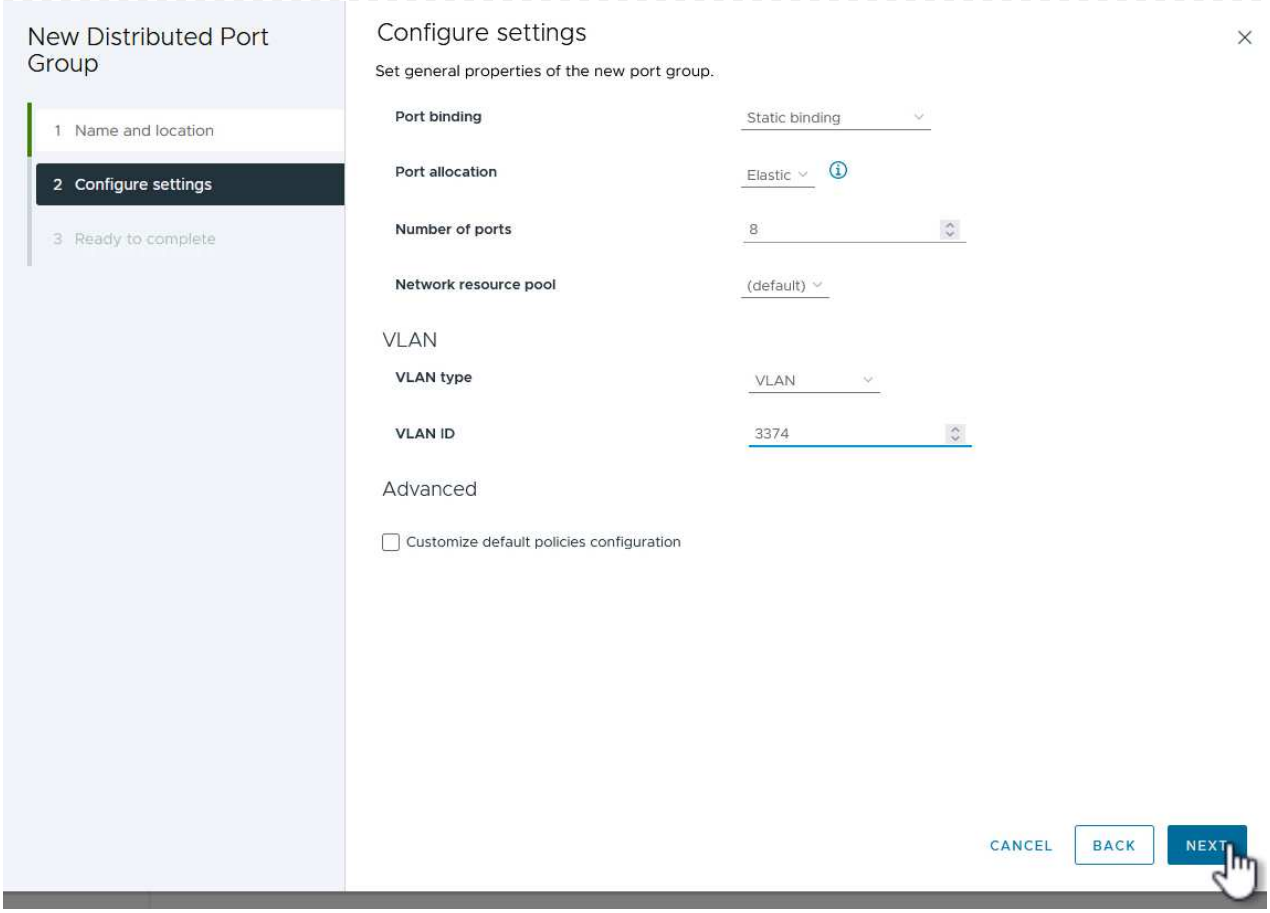
Criar grupos de portas distribuídas para tráfego iSCSI

Conclua o seguinte para criar um novo grupo de portas distribuídas para cada rede iSCSI:

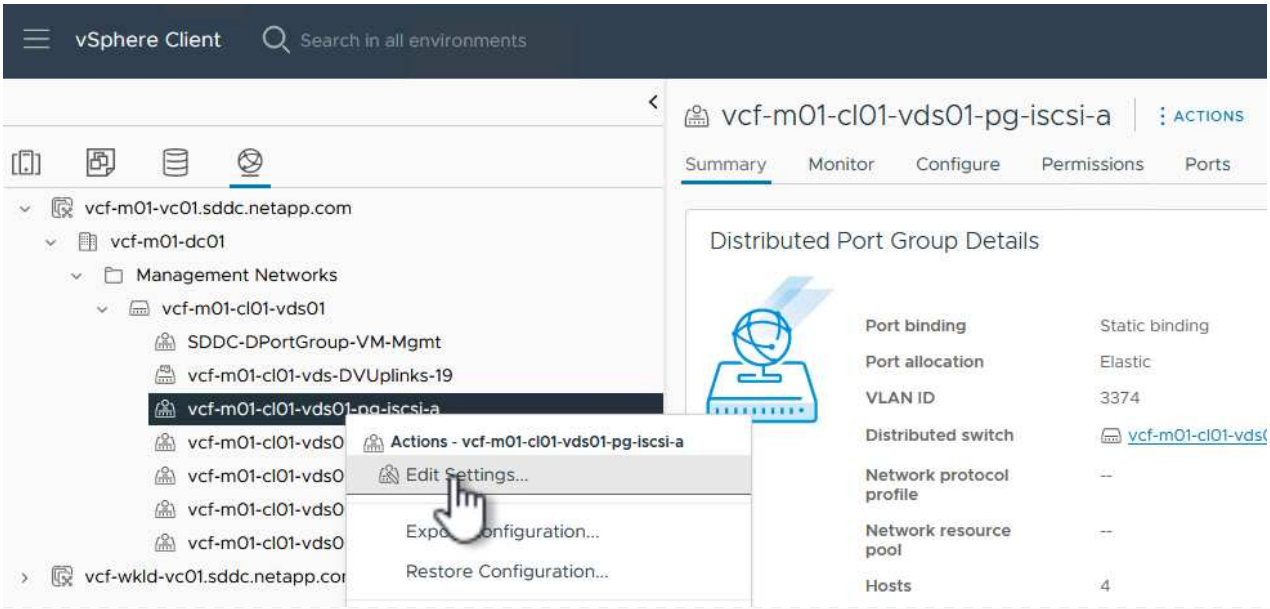
1. No cliente vSphere para o cluster de domínio de gerenciamento, navegue até **Inventário > Rede**. Navegue até o Distributed Switch existente e escolha a ação para criar **Novo Grupo de Portas Distribuídas…**.



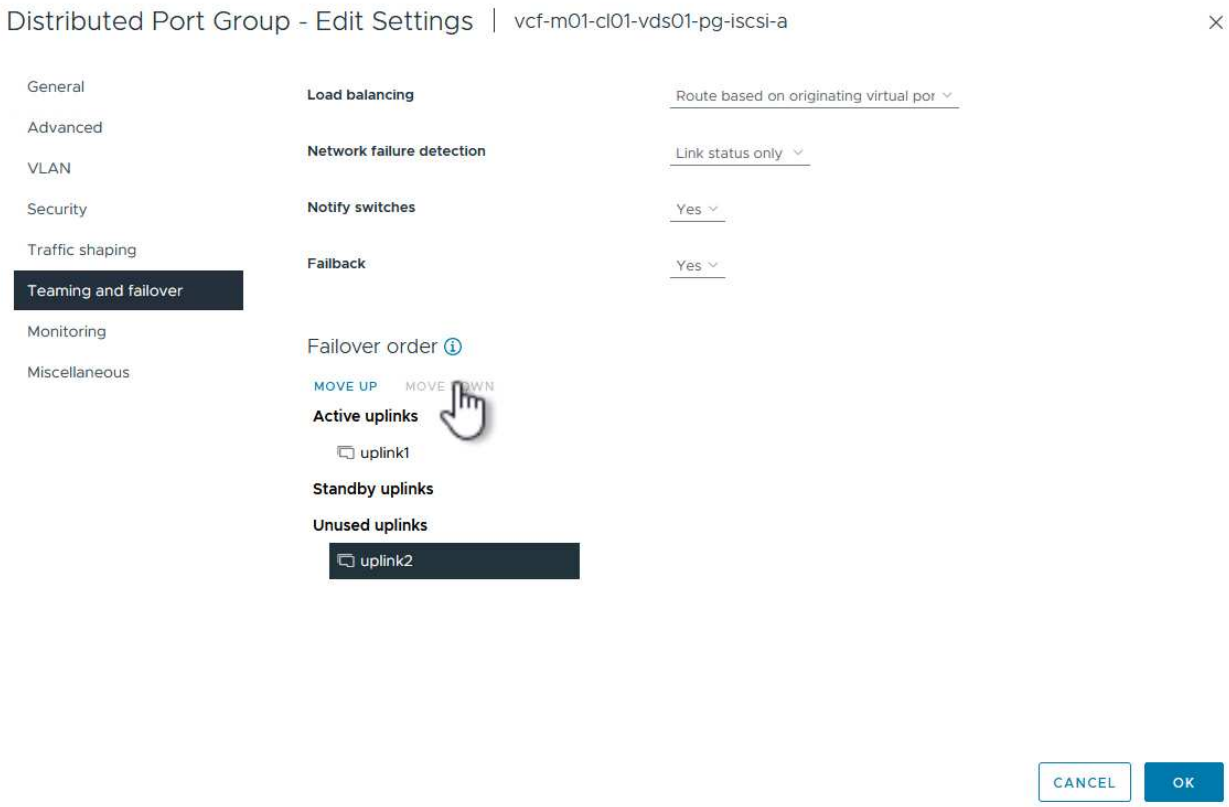
2. No assistente **Novo grupo de portas distribuídas**, preencha um nome para o novo grupo de portas e clique em **Avançar** para continuar.
3. Na página **Configurar configurações** preencha todas as configurações. Se VLANs estiverem sendo usadas, certifique-se de fornecer o ID de VLAN correto. Clique em **Avançar** para continuar.



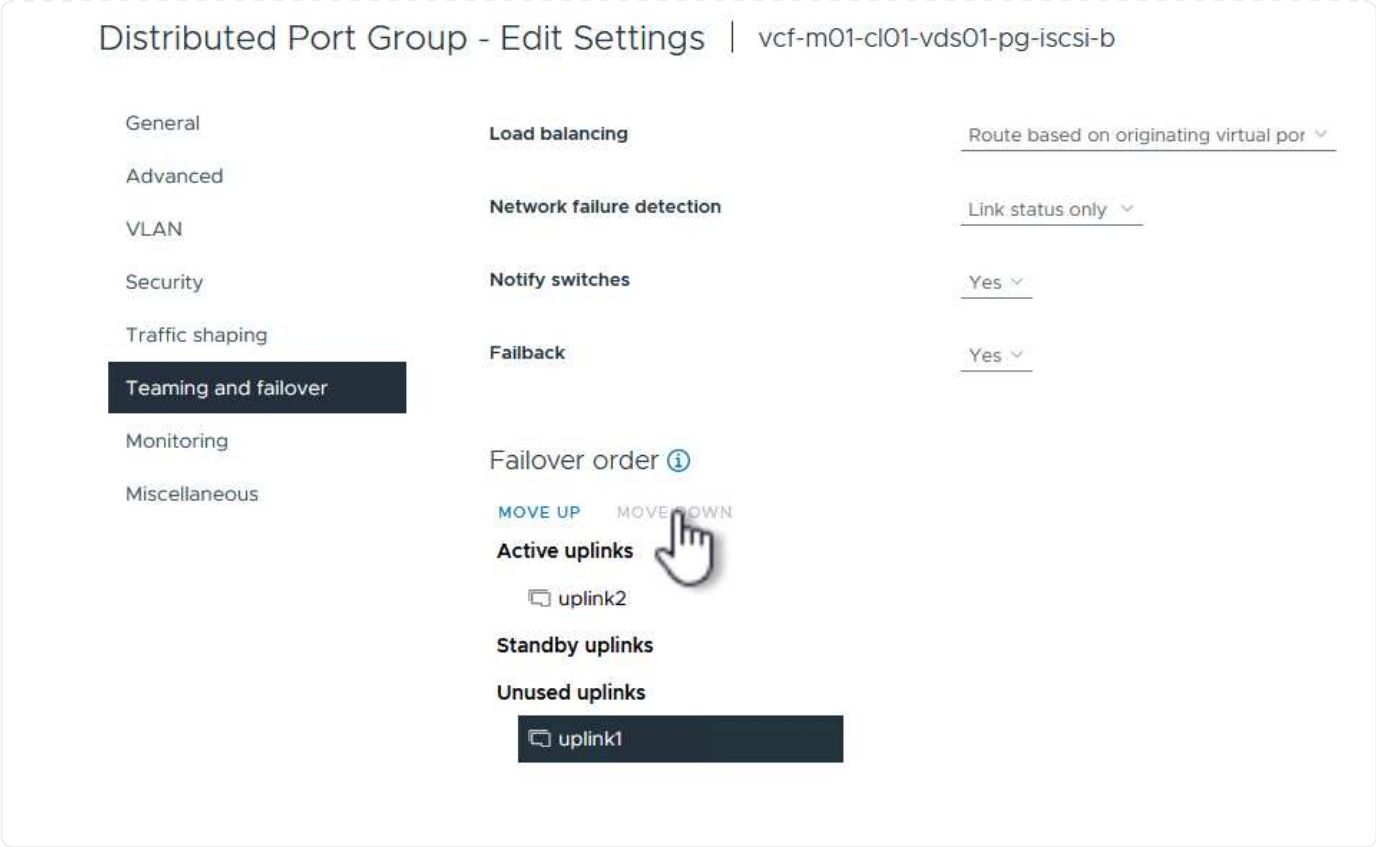
4. Na página **Pronto para concluir**, revise as alterações e clique em **Concluir** para criar o novo grupo de portas distribuídas.
5. Repita esse processo para criar um grupo de portas distribuídas para a segunda rede iSCSI que está sendo usada e certifique-se de ter inserido o **ID de VLAN** correto.
6. Depois que ambos os grupos de portas forem criados, navegue até o primeiro grupo de portas e selecione a ação **Editar configurações…**.



7. Na página **Grupo de portas distribuídas - Editar configurações**, navegue até **Agrupamento e failover** no menu à esquerda e clique em **uplink2** para movê-lo para **Uplinks não utilizados**.



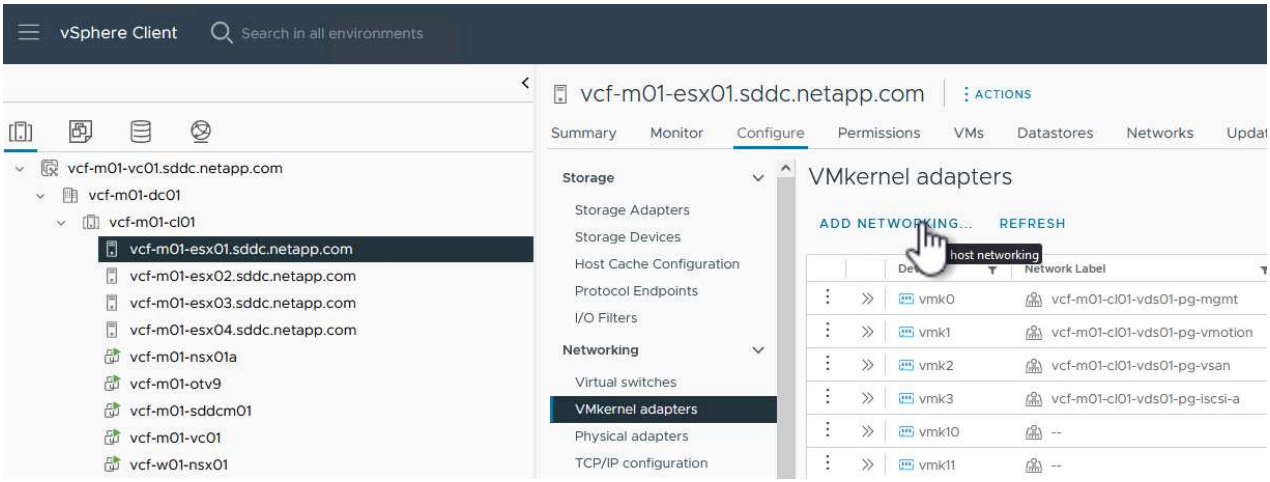
8. Repita esta etapa para o segundo grupo de portas iSCSI. Entretanto, desta vez mova **uplink1** para **Uplinks não utilizados**.


Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b
General
Advanced
VLAN
Security
Traffic shaping
Teaming and failover
Monitoring
Miscellaneous
Load balancing
Route based on originating virtual por
Network failure detection
Link status only
Notify switches
Yes
Failback
Yes
Failover order
MOVE UP
MOVE DOWN
Active uplinks
uplink2
Standby uplinks
Unused uplinks
uplink1

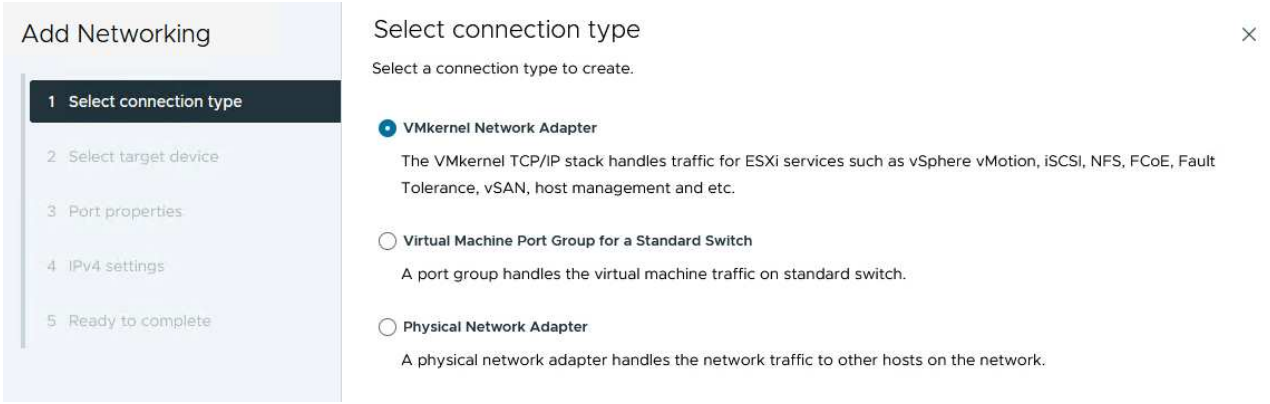
Crie adaptadores VMkernel em cada host ESXi

Repita esse processo em cada host ESXi no domínio de gerenciamento.

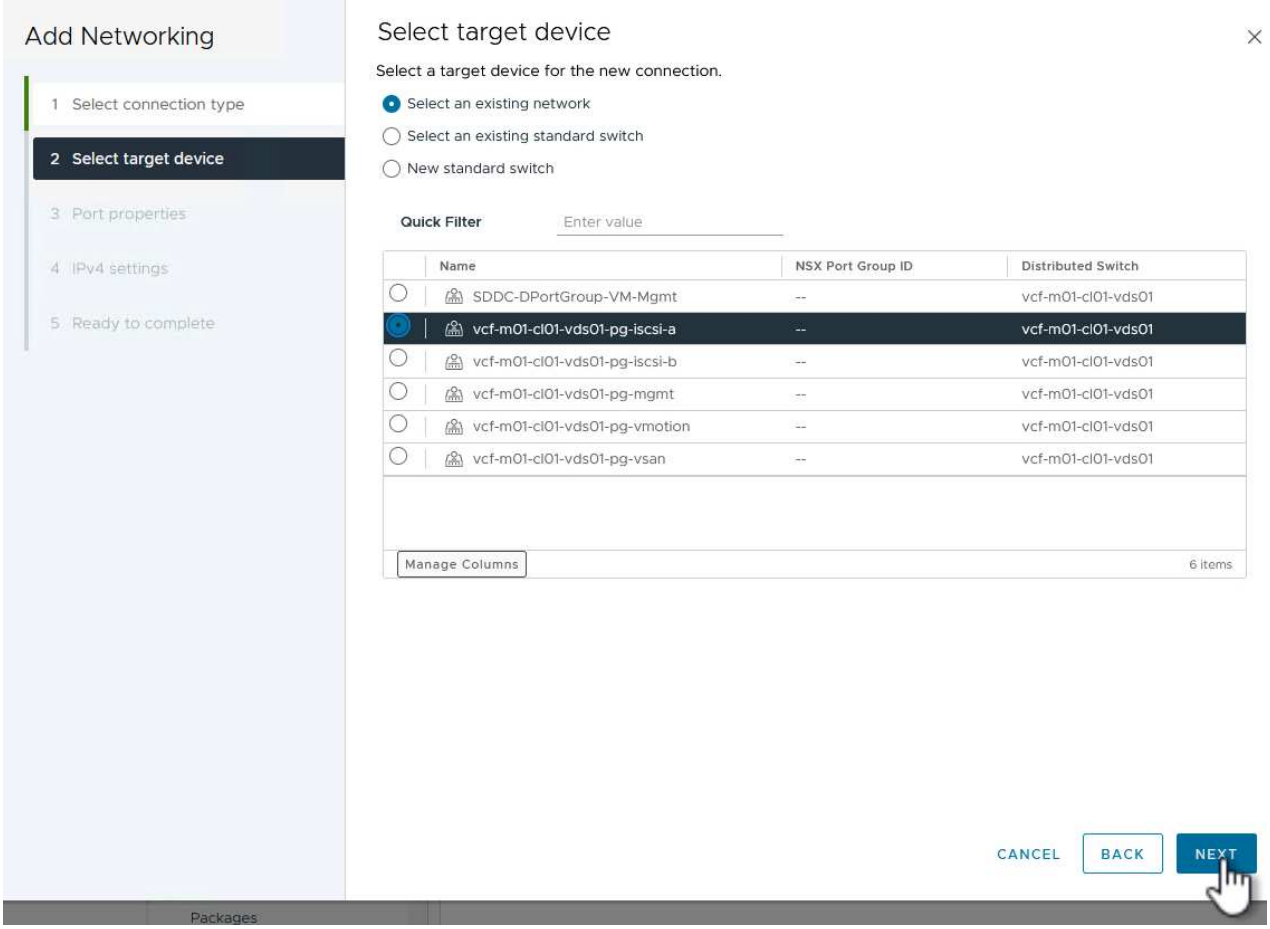
1. No cliente vSphere, navegue até um dos hosts ESXi no inventário do domínio de gerenciamento. Na aba **Configurar** selecione **Adaptadores VMkernel** e clique em **Adicionar Rede…** para iniciar.



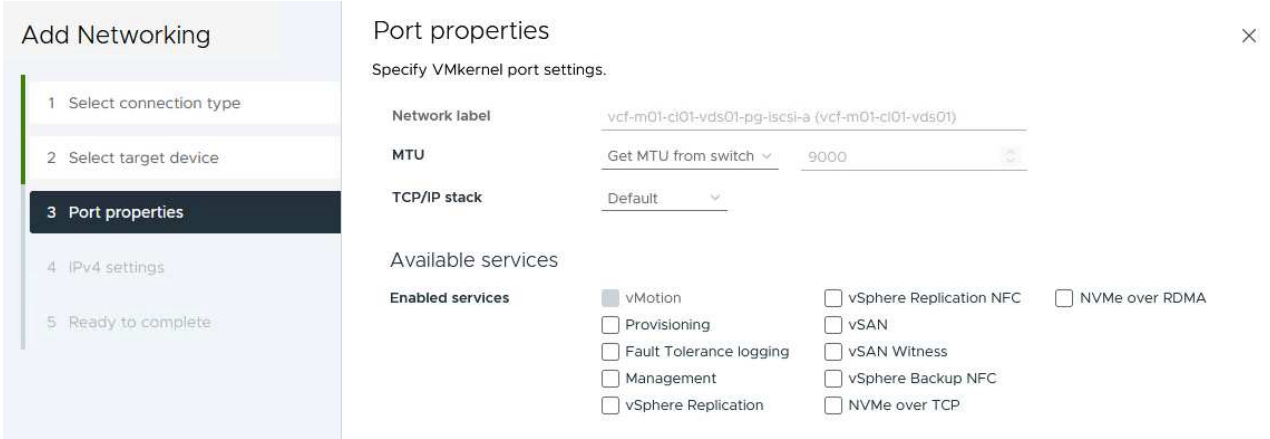
2. Na janela **Selecionar tipo de conexão**, escolha **Adaptador de rede VMkernel** e clique em **Avançar** para continuar.



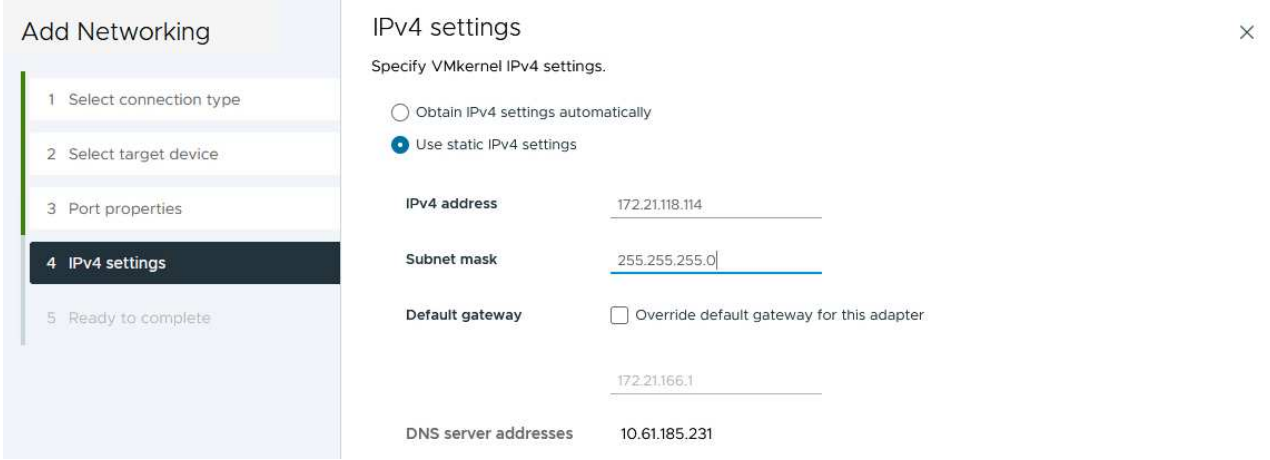
3. Na página **Selecionar dispositivo de destino**, escolha um dos grupos de portas distribuídas para iSCSI que foi criado anteriormente.



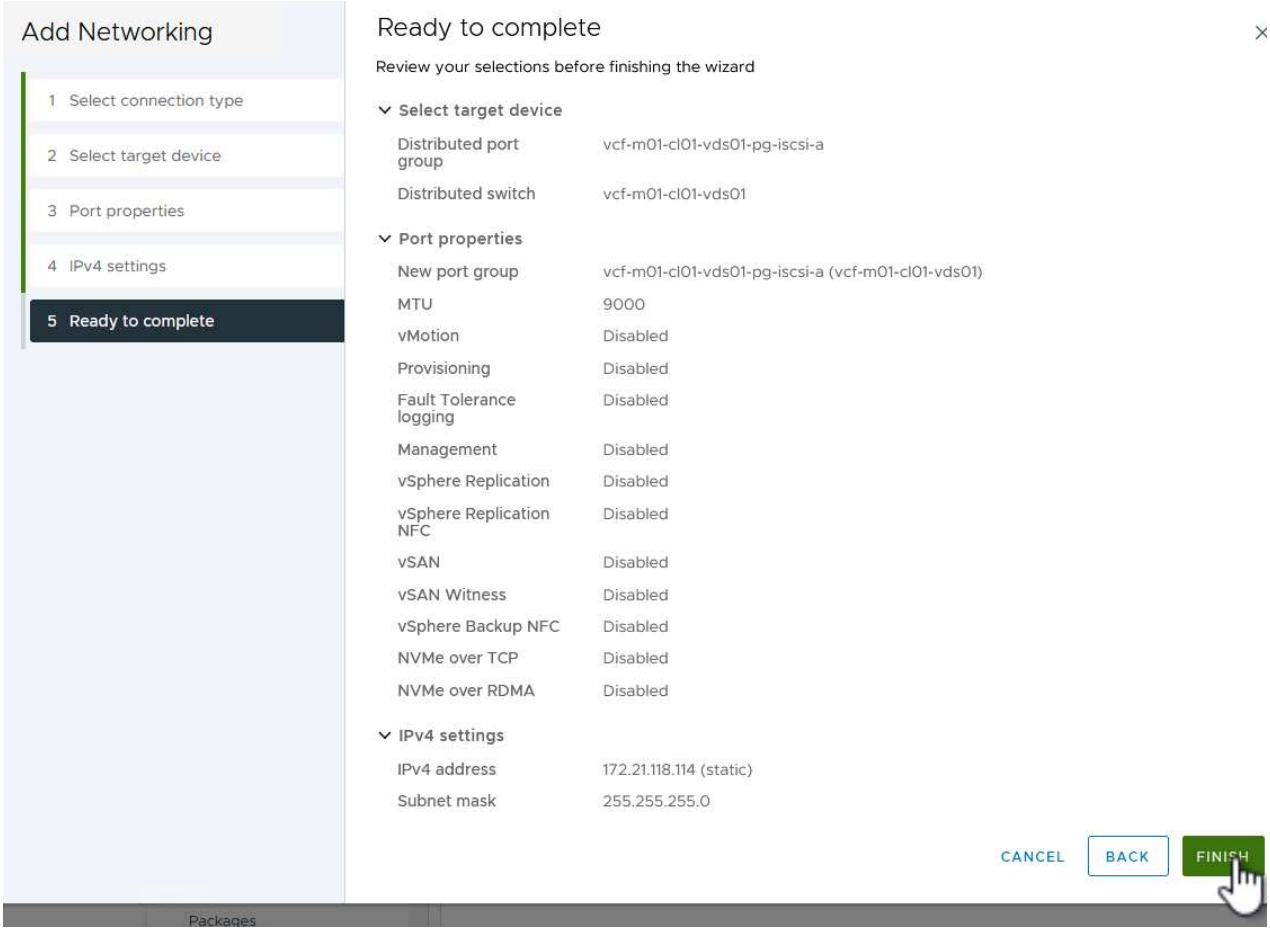
4. Na página **Propriedades da porta**, mantenha os padrões e clique em **Avançar** para continuar.



5. Na página **Configurações IPv4**, preencha o **endereço IP**, a **máscara de sub-rede** e forneça um novo endereço IP do gateway (somente se necessário). Clique em **Avançar** para continuar.



6. Revise suas seleções na página **Pronto para concluir** e clique em **Concluir** para criar o adaptador VMkernel.



7. Repita esse processo para criar um adaptador VMkernel para a segunda rede iSCSI.

Implantar e usar ferramentas ONTAP para configurar o armazenamento

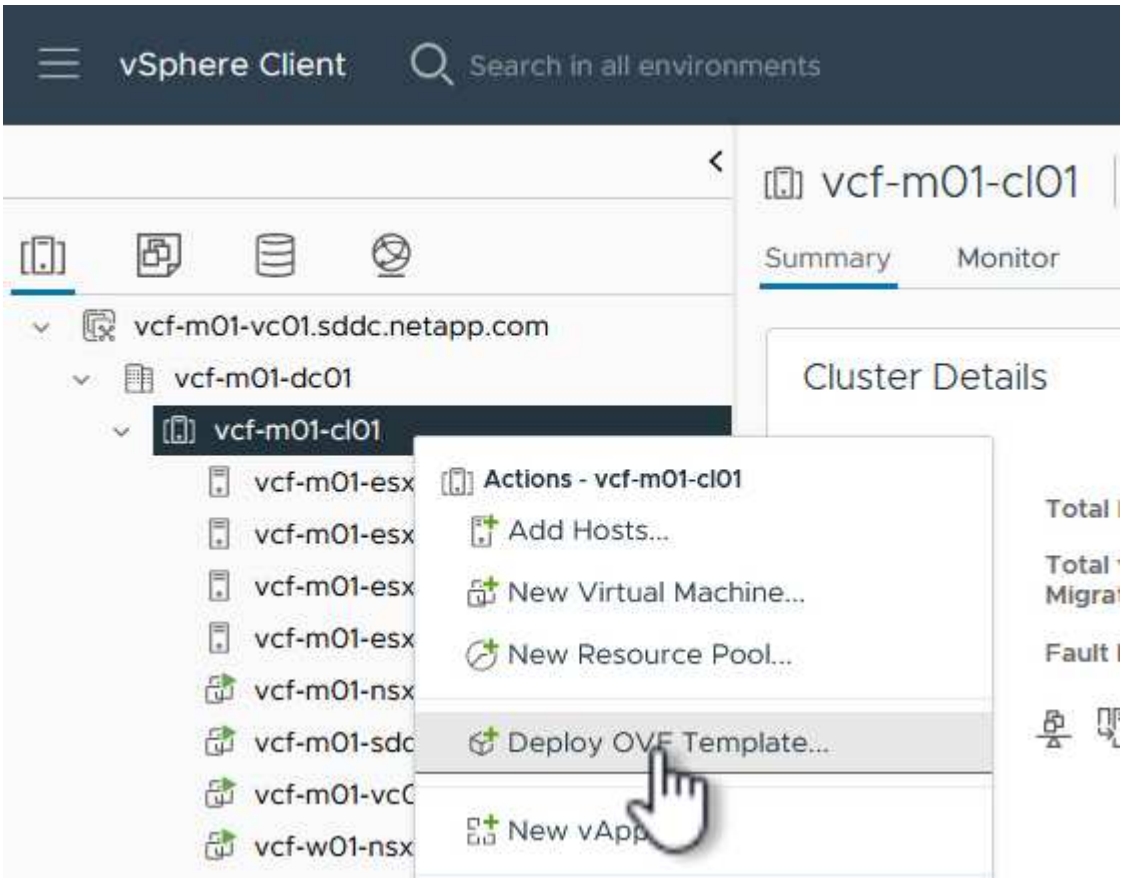
As etapas a seguir são executadas no cluster de domínio de gerenciamento do VCF usando o cliente vSphere e envolvem a implantação do OTV, a criação de um armazenamento de dados iSCSI VMFS e a migração de VMs de gerenciamento para o novo armazenamento de dados.

Implantar ONTAP tools for VMware vSphere

As ONTAP tools for VMware vSphere (OTV) são implantadas como um dispositivo de VM e fornecem uma interface de usuário do vCenter integrada para gerenciar o armazenamento ONTAP .

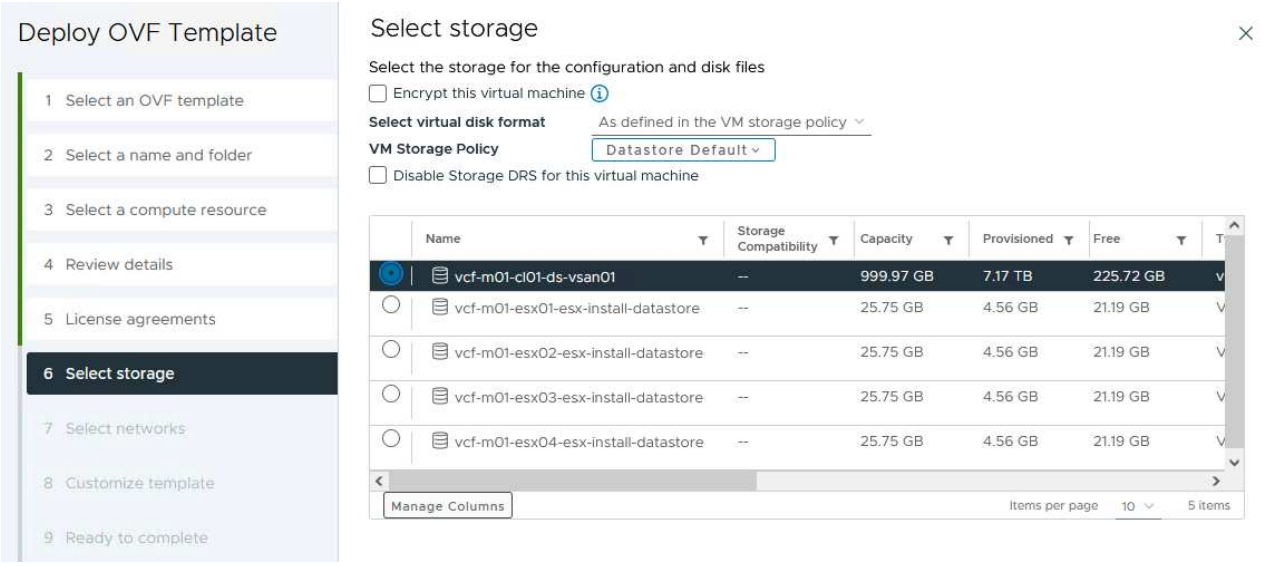
Conclua o seguinte para implantar ONTAP tools for VMware vSphere:

1. Obtenha a imagem OVA das ferramentas ONTAP do"Site de suporte da NetApp" e baixe para uma pasta local.
2. Efetue login no dispositivo vCenter para o domínio de gerenciamento do VCF.
3. Na interface do dispositivo vCenter, clique com o botão direito do mouse no cluster de gerenciamento e selecione **Implantar modelo OVF…**

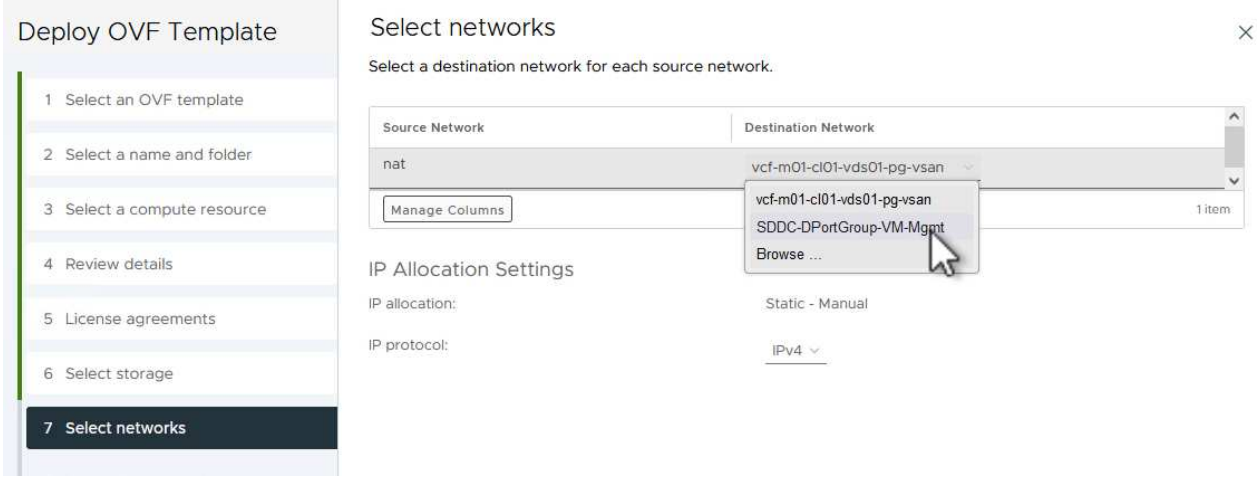


4. No assistente **Implantar modelo OVF**, clique no botão de opção **Arquivo local** e selecione o arquivo OVA das ferramentas ONTAP baixado na etapa anterior.

5. Para as etapas 2 a 5 do assistente, selecione um nome e uma pasta para a VM, selecione o recurso de computação, revise os detalhes e aceite o contrato de licença.
6. Para o local de armazenamento dos arquivos de configuração e de disco, selecione o armazenamento de dados vSAN do cluster de domínio de gerenciamento do VCF.

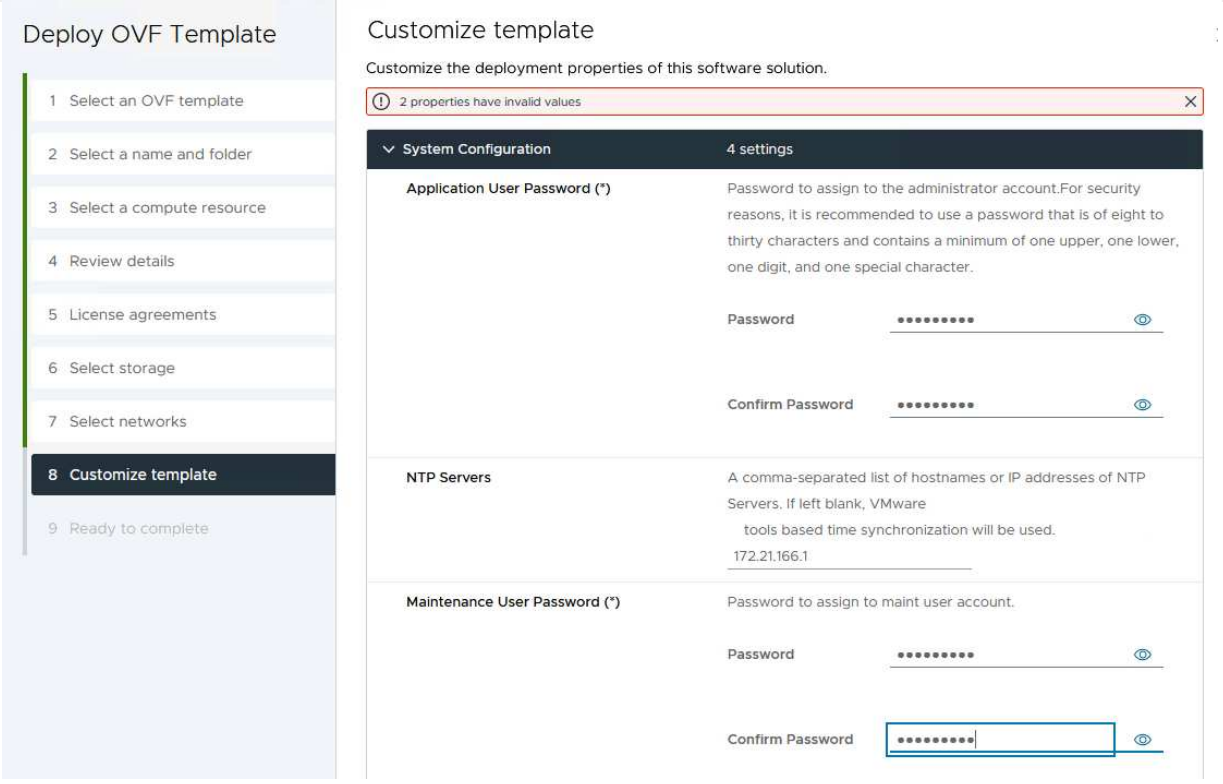


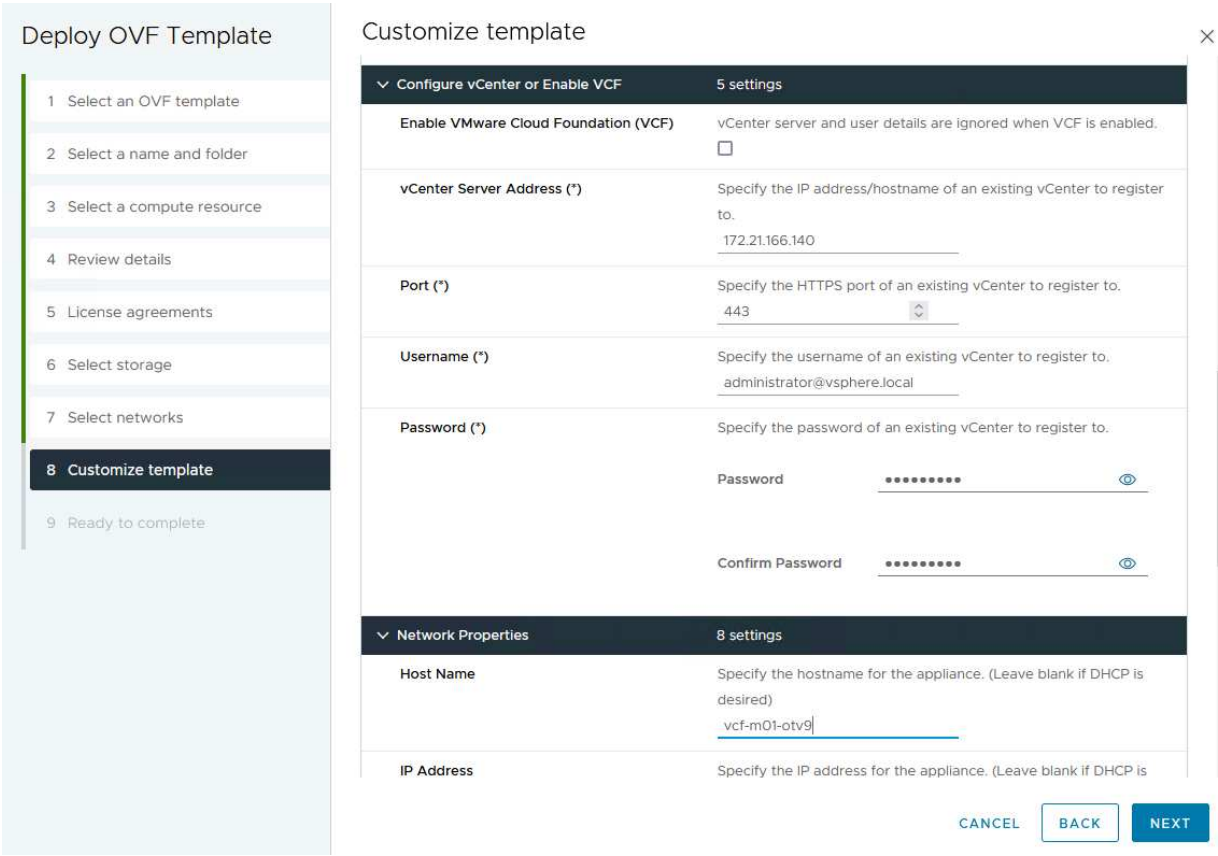
7. Na página Selecionar rede, selecione a rede usada para o tráfego de gerenciamento.



8. Na página Personalizar modelo, preencha todas as informações necessárias:
   - Senha a ser usada para acesso administrativo ao OTV.
   - Endereço IP do servidor NTP.
   - Senha da conta de manutenção do OTV.
   - Senha do banco de dados OTV Derby.
   - Não marque a caixa para **Ativar VMware Cloud Foundation (VCF)**. O modo VCF não é necessário para implantar armazenamento suplementar.
   - FQDN ou endereço IP do dispositivo vCenter e forneça credenciais para o vCenter.
   - Forneça os campos de propriedades de rede necessários.

     Clique em **Avançar** para continuar.



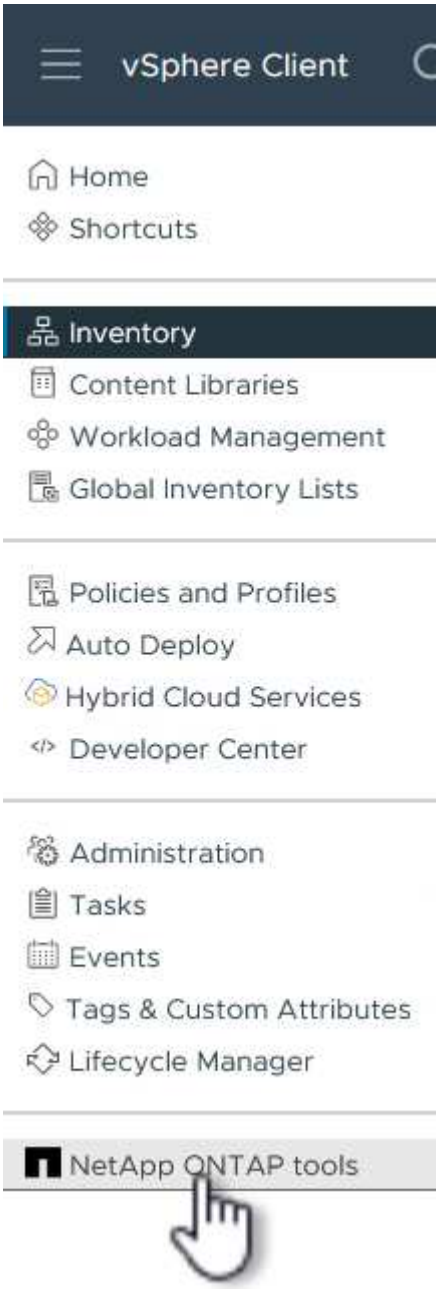


9. Revise todas as informações na página Pronto para concluir e clique em Concluir para começar a implantar o dispositivo OTV.

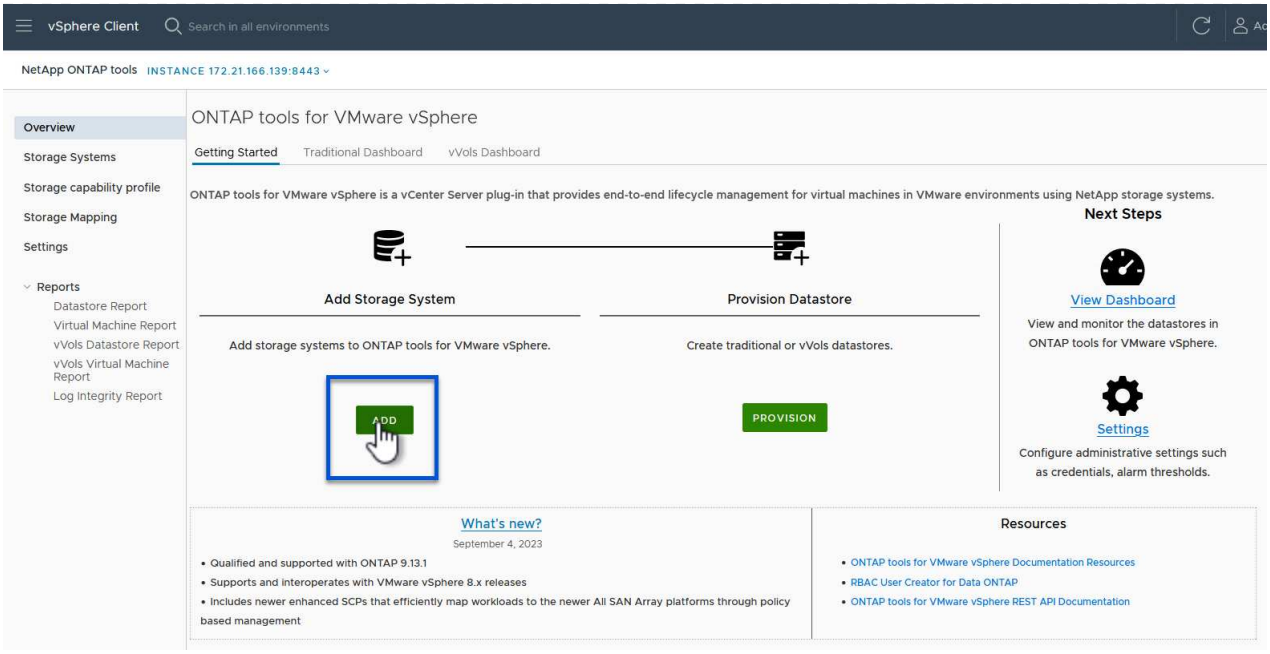
Configurar um armazenamento de dados VMFS iSCSI no domínio de gerenciamento usando OTV

Conclua o seguinte para usar o OTV para configurar um armazenamento de dados VMFS iSCSI como armazenamento suplementar no domínio de gerenciamento:

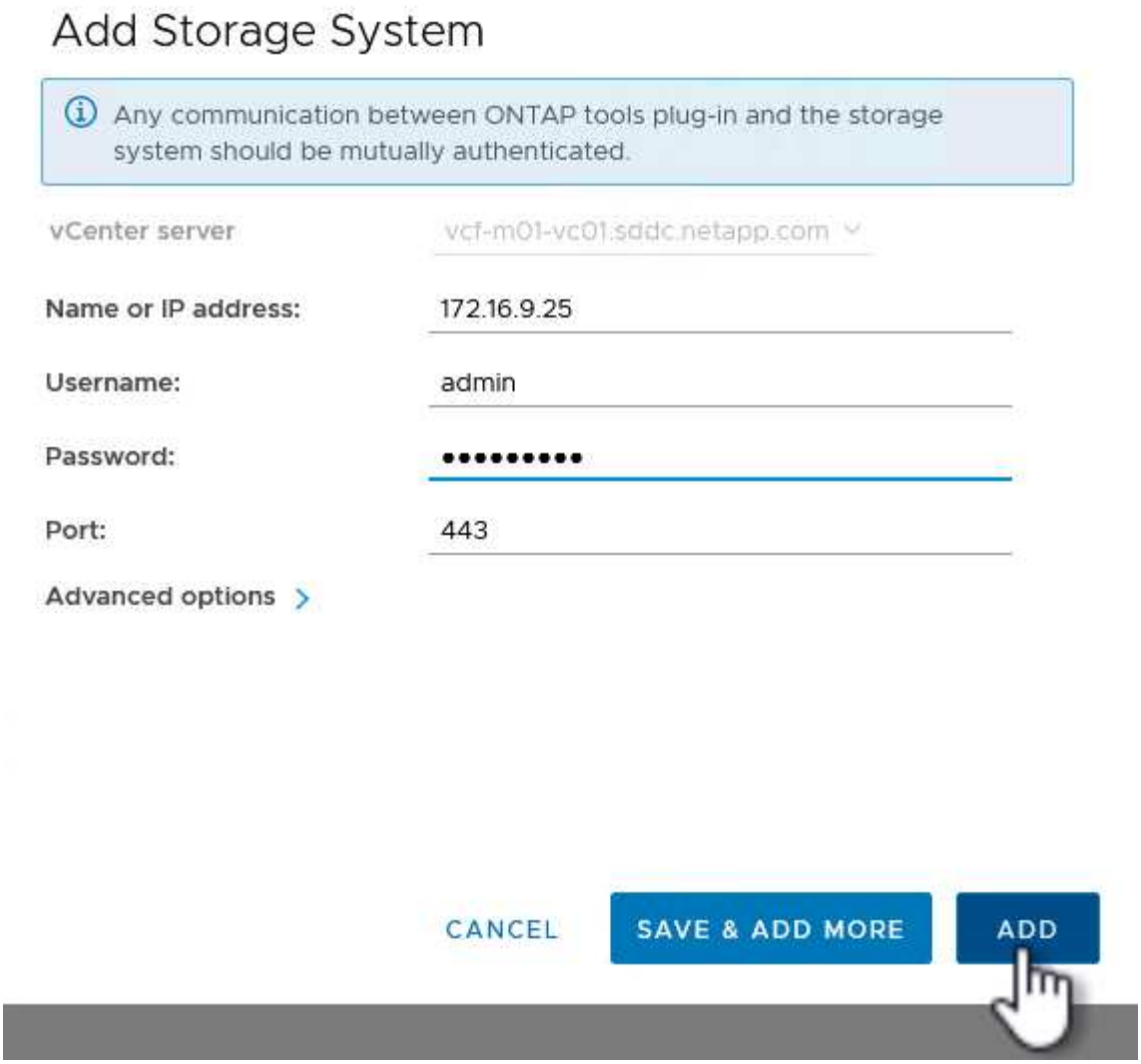
1. No cliente vSphere, navegue até o menu principal e selecione * NetApp ONTAP Tools*.



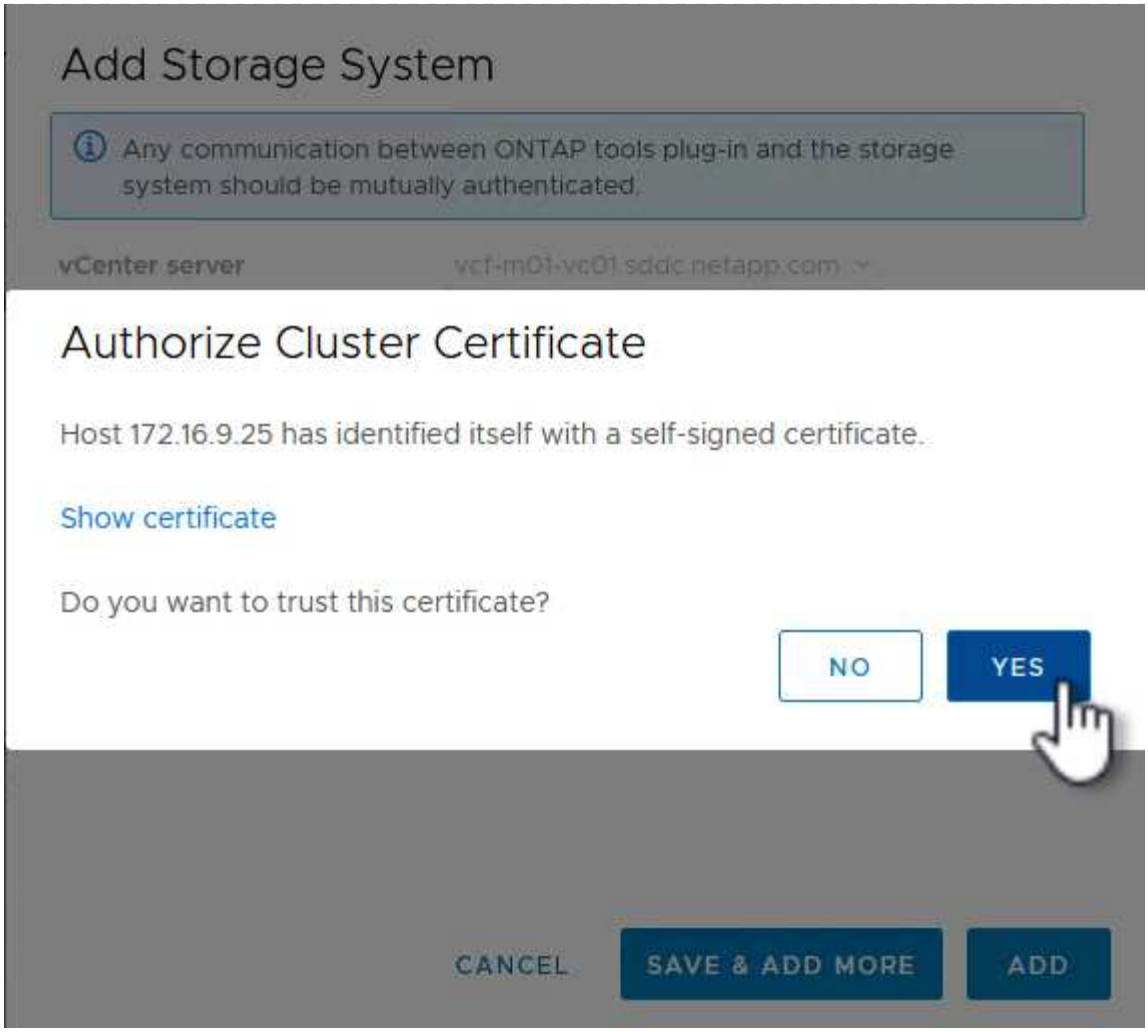
2. Uma vez em * ONTAP Tools*, na página Introdução (ou em **Sistemas de Armazenamento**), clique em **Adicionar** para adicionar um novo sistema de armazenamento.



3. Forneça o endereço IP e as credenciais do sistema de armazenamento ONTAP e clique em **Adicionar**.



4. Clique em **Sim** para autorizar o certificado do cluster e adicionar o sistema de armazenamento.

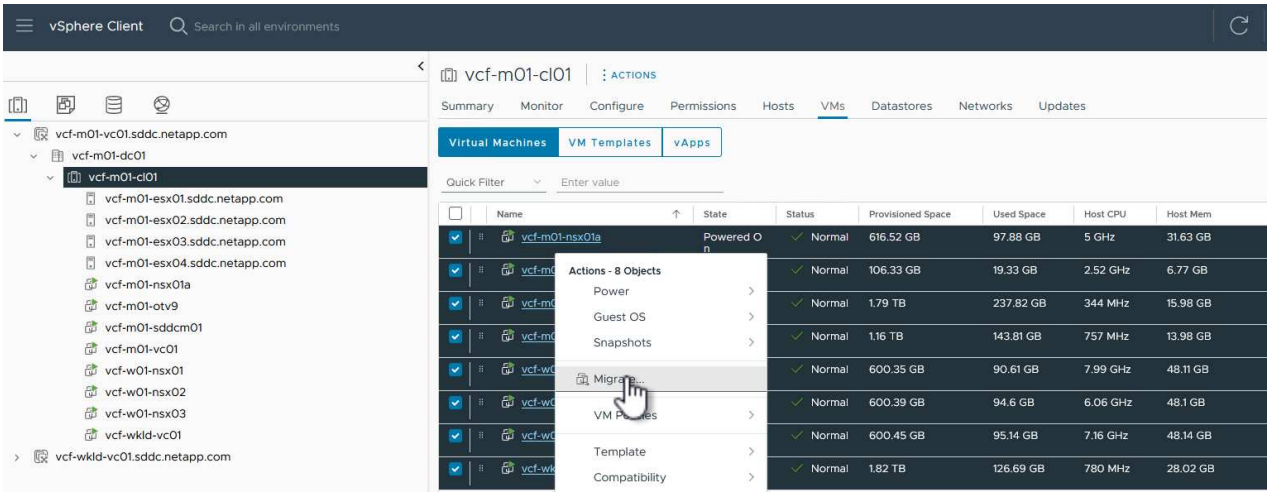

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Authorize Cluster Certificate
Host 172.16.9.25 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
SAVE & ADD MORE
ADD

Migrar VMs de gerenciamento para o iSCSI Datastore

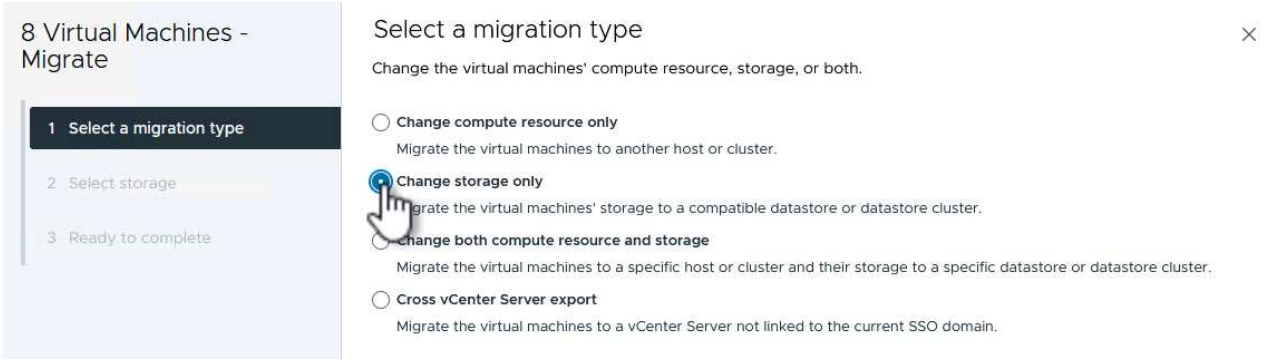
Nos casos em que é preferível usar o armazenamento ONTAP para proteger as VMs de gerenciamento do VCF, o vMotion pode ser usado para migrar as VMs para o armazenamento de dados iSCSI recém-criado.

Conclua as etapas a seguir para migrar as VMs de gerenciamento do VCF para o armazenamento de dados iSCSI.

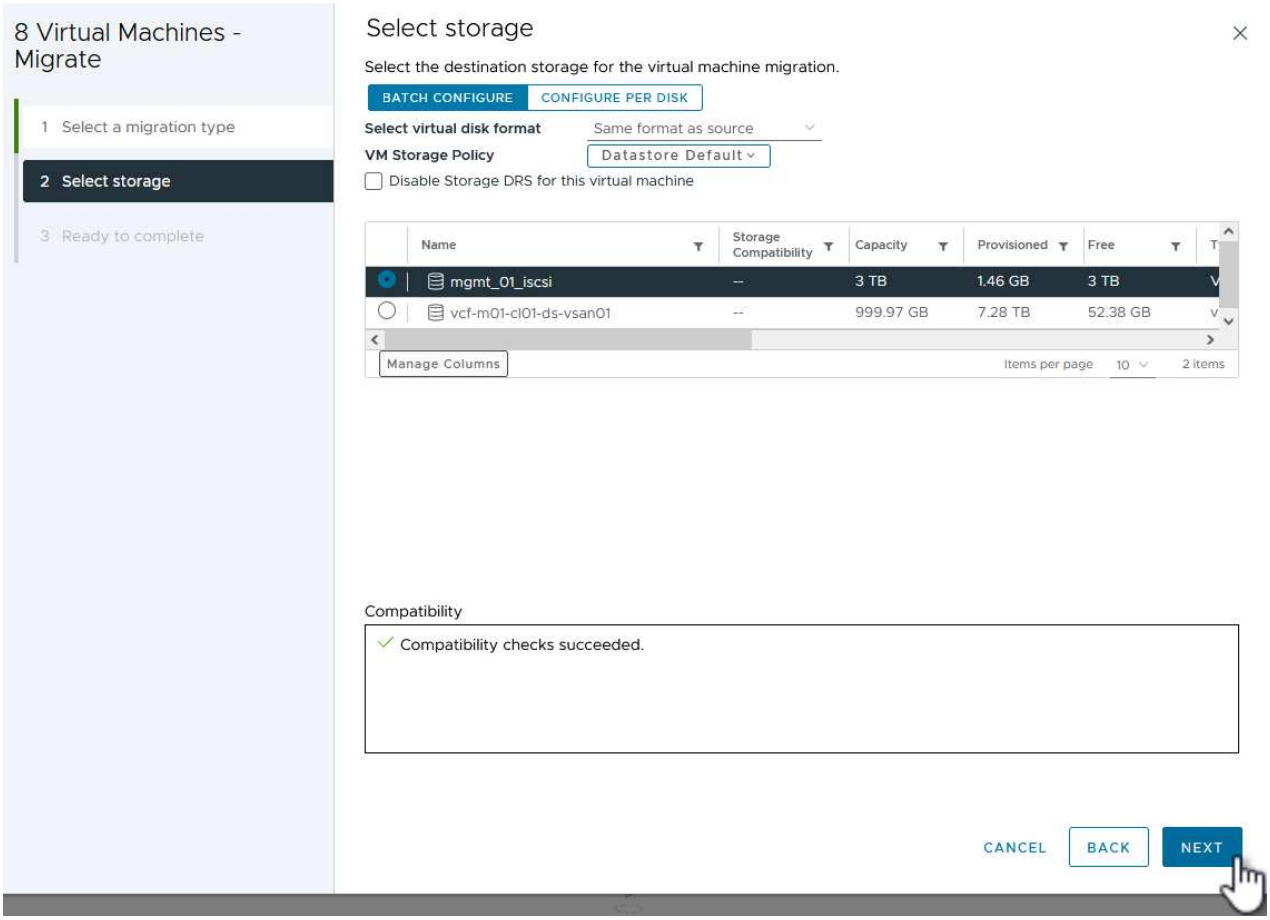
1. No vSphere Client, navegue até o cluster de domínio de gerenciamento e clique na guia **VMs**.
2. Selecione as VMs a serem migradas para o armazenamento de dados iSCSI, clique com o botão direito e selecione **Migrar...**.



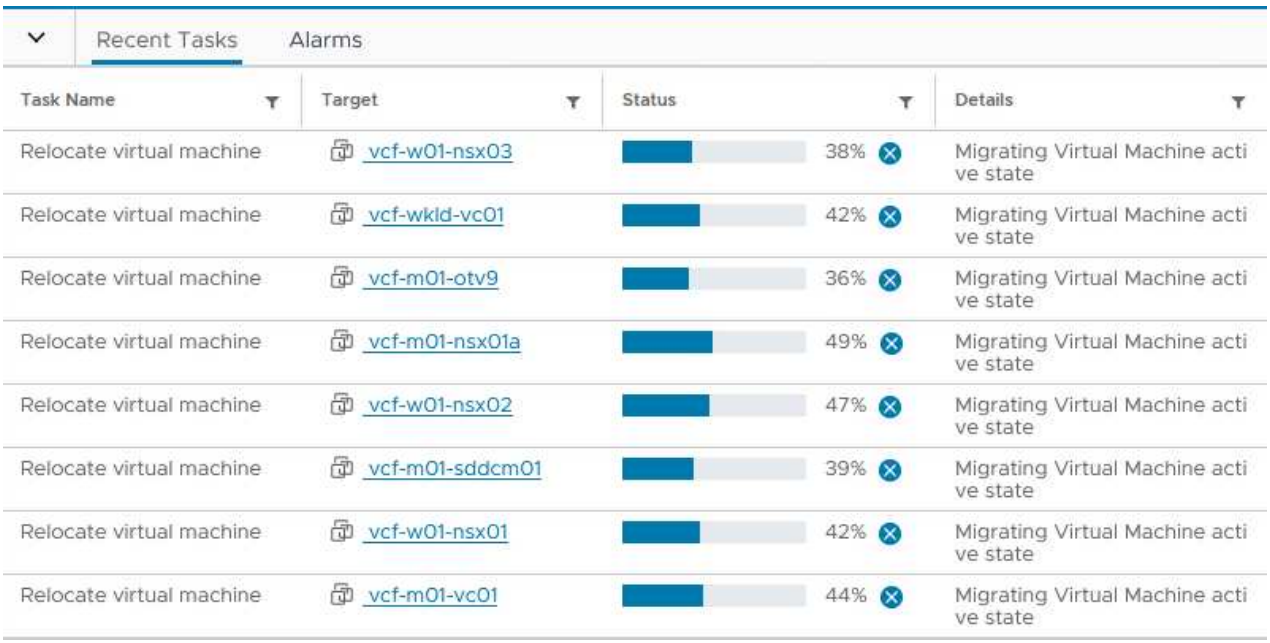
3. No assistente **Máquinas Virtuais - Migrar**, selecione **Alterar somente armazenamento** como o tipo de migração e clique em **Avançar** para continuar.



4. Na página **Selecionar armazenamento**, selecione o armazenamento de dados iSCSi e selecione **Avançar** para continuar.



5. Revise as seleções e clique em **Concluir** para iniciar a migração.
6. O status da realocação pode ser visualizado no painel **Tarefas recentes**.



Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Demonstração em vídeo desta solução

Armazenamentos de dados iSCSI como armazenamento suplementar para domínios de gerenciamento VCF

Adicionar um armazenamento de dados VMFS baseado em FC como armazenamento suplementar para um domínio de gerenciamento usando ONTAP tools for VMware vSphere

Neste caso de uso, descrevemos o procedimento para usar o ONTAP Tools for VMware para configurar um armazenamento de dados VMFS sobre Fibre Channel (FC) como armazenamento suplementar para o domínio de gerenciamento do VMware Cloud Foundation (VCF). Este procedimento resume a implantação do ONTAP Tools para VMware vSphere, o registro de servidores vCenter, a definição do backend de armazenamento e o provisionamento do armazenamento de dados FC.

Benefícios do Fibre Channel

Alto desempenho: o FC fornece altas taxas de transferência de dados, tornando-o ideal para aplicações que exigem acesso rápido e confiável a grandes quantidades de dados.

Baixa latência: latência muito baixa, o que é crucial para aplicativos sensíveis ao desempenho, como bancos de dados e ambientes virtualizados.

Confiabilidade: As redes FC são conhecidas por sua robustez e confiabilidade, com recursos como redundância integrada e correção de erros.

Largura de banda dedicada: o FC fornece largura de banda dedicada para tráfego de armazenamento, reduzindo o risco de congestionamento da rede.

Para obter mais informações sobre o uso do Fibre Channel com sistemas de armazenamento NetApp , consulte "Provisionamento SAN com FC" .

Visão geral do cenário

O armazenamento de dados suplementar do VCF é fornecido como parte das operações do dia 2 usando o vCenter. Este cenário abrange as seguintes etapas de alto nível:

- Implantação de ferramentas ONTAP no domínio de gerenciamento
- Registrar servidores vCenter de carga de trabalho VI em ferramentas ONTAP
- Definir backend de armazenamento no plugin de ferramentas ONTAP para VMware vSphere
- Provisionar VMFS no transporte FC

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP com portas FC conectadas a switches FC.
- SVM criado com FC lifs.
- vSphere com HBAs FC conectados a switches FC.
- O zoneamento de iniciador-alvo único é configurado em switches FC.

> Use a interface lógica SVM FC na configuração de zona em vez de portas FC físicas em sistemas ONTAP .

A NetApp recomenda vários caminhos para LUNs FC.

Para obter informações completas sobre a configuração do canal de fibra em sistemas de armazenamento ONTAP , consulte "Gerenciamento de armazenamento SAN" na documentação do ONTAP 9.

Para obter mais informações sobre o uso do VMFS com sistemas de armazenamento ONTAP , consulte o"Guia de implantação para VMFS" .

Etapas de implantação para domínio de gerenciamento

Para implantar o ONTAP Tools e usá-lo para criar um armazenamento de dados VMFS no domínio de gerenciamento do VCF, conclua as seguintes etapas:

- "Implantar ferramentas ONTAP no domínio de gerenciamento"
- "Definir backend de armazenamento usando a interface do cliente vSphere"
- "Provisionar VMFS no FC"

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Demonstração em vídeo desta solução

VMFS(FC) Datastore como armazenamento suplementar para domínio de gerenciamento VCF

Adicione vVols como armazenamento suplementar aos domínios de carga de trabalho VI usando ONTAP tools for VMware vSphere

Neste caso de uso, descrevemos o procedimento para configurar um armazenamento de dados vVols com iSCSI para armazenamento suplementar em um domínio de carga de trabalho de infraestrutura virtual (VI) do VMware Cloud Foundation (VCF). Este procedimento resume a configuração da rede iSCSI, a implantação do ONTAP Tools para VMware vSphere e o provisionamento do armazenamento de dados vVols .

iSCSI é usado como protocolo de armazenamento para o armazenamento de dados vVols .

Benefícios do iSCSI

Alto desempenho: oferece alto desempenho para fornecer taxas de transferência de dados rápidas e eficientes e baixa latência. Ideal para aplicativos empresariais exigentes e ambientes virtualizados.

Facilidade de gerenciamento: simplifica o gerenciamento de armazenamento usando ferramentas e protocolos familiares baseados em IP.

Custo-benefício: utiliza a infraestrutura Ethernet existente, reduzindo a necessidade de hardware especializado e permitindo que as organizações obtenham soluções de armazenamento confiáveis e escaláveis.

Para obter mais informações sobre o uso do iSCSI com sistemas de armazenamento NetApp , consulte "Provisionamento SAN com iSCSI" .

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

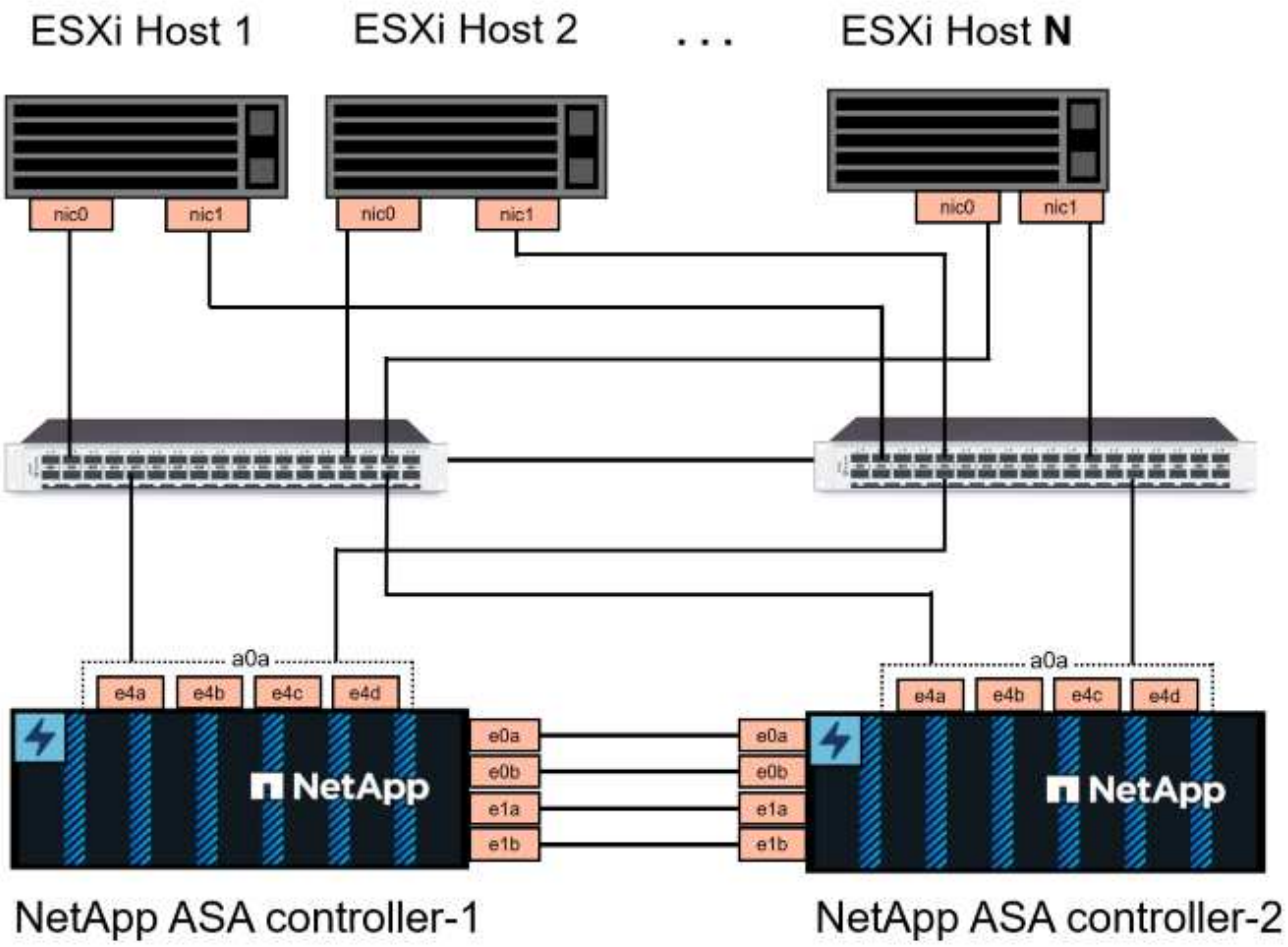
- Crie uma máquina virtual de armazenamento (SVM) com interfaces lógicas (LIFs) para tráfego iSCSI.
- Crie grupos de portas distribuídas para redes iSCSI no domínio de carga de trabalho do VI.
- Crie adaptadores vmkernel para iSCSI nos hosts ESXi para o domínio de carga de trabalho VI.
- Implante o ONTAP Tools no domínio de carga de trabalho do VI.
- Crie um novo armazenamento de dados vVols no domínio de carga de trabalho do VI.

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP AFF ou ASA com portas de dados físicas em switches Ethernet dedicados ao tráfego de armazenamento.
- A implantação do domínio de gerenciamento do VCF foi concluída e o cliente vSphere está acessível.
- Um domínio de carga de trabalho VI foi implantado anteriormente.

A NetApp recomenda projetos de rede totalmente redundantes para iSCSI. O diagrama a seguir ilustra um exemplo de configuração redundante, fornecendo tolerância a falhas para sistemas de armazenamento, switches, adaptadores de rede e sistemas host. Consulte o NetApp"Referência de configuração SAN" para obter informações adicionais.



Para multipathing e failover em vários caminhos, a NetApp recomenda ter no mínimo dois LIFs por nó de armazenamento em redes Ethernet separadas para todas as SVMs em configurações iSCSI.

Esta documentação demonstra o processo de criação de um novo SVM e especificação das informações de endereço IP para criar vários LIFs para tráfego iSCSI. Para adicionar novos LIFs a um SVM existente, consulte"Criar uma LIF (interface de rede)" .

> Em situações em que vários adaptadores VMkernel são configurados na mesma rede IP, é recomendável usar a vinculação de porta iSCSI de software nos hosts ESXi para garantir que o balanceamento de carga entre os adaptadores ocorra. Consulte o artigo da KB"Considerações sobre o uso de vinculação de porta iSCSI de software no ESX/ESXi (2038869)" .

Para obter informações adicionais sobre o uso de datastores VMFS iSCSI com VMware, consulte"vSphere VMFS Datastore - backend de armazenamento iSCSI com ONTAP" .

Etapas de implantação

Para implantar o ONTAP Tools e usá-lo para criar um armazenamento de dados vVols no domínio de gerenciamento do VCF, conclua as seguintes etapas:

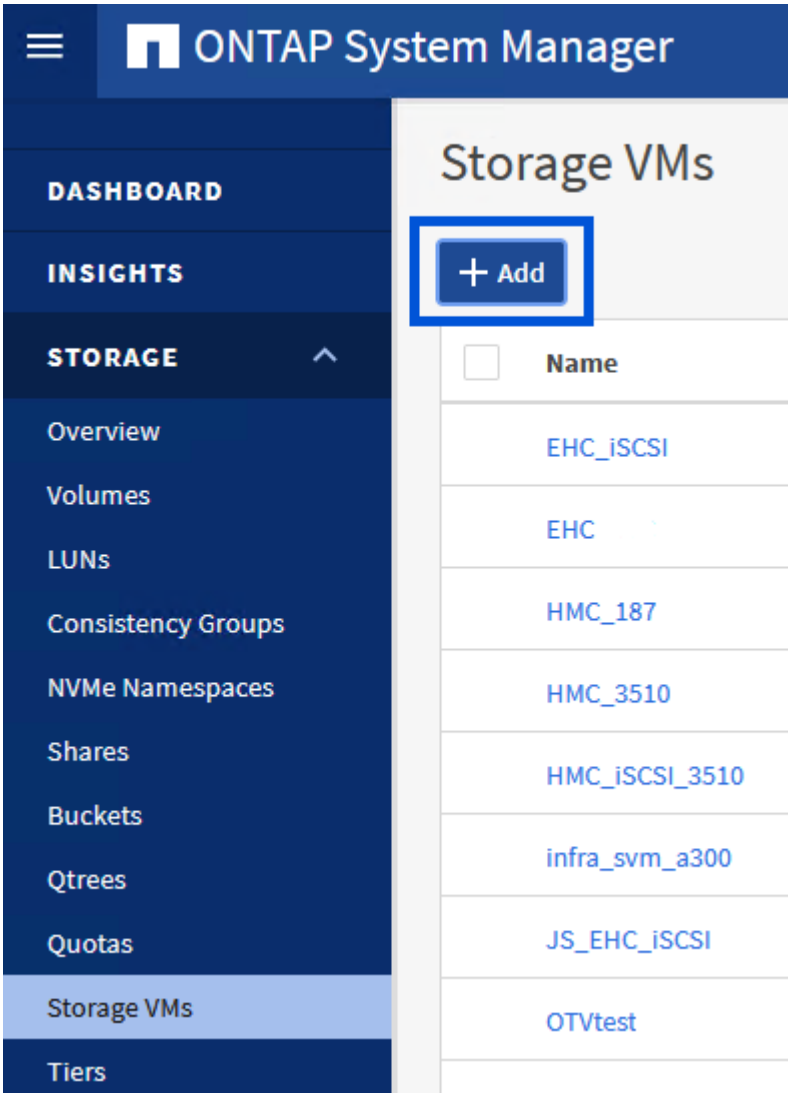
Crie SVM e LIFs no sistema de armazenamento ONTAP

A etapa seguinte é executada no ONTAP System Manager.

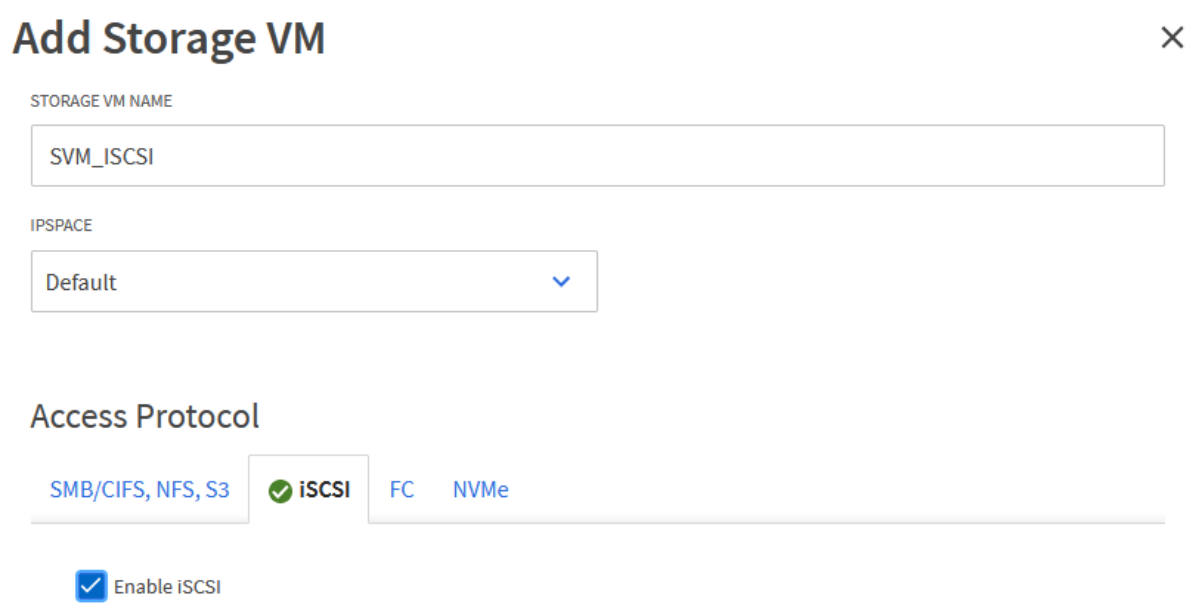
Crie a VM de armazenamento e os LIFs

Conclua as etapas a seguir para criar um SVM junto com vários LIFs para tráfego iSCSI.

1. No ONTAP System Manager, navegue até **VMs de armazenamento** no menu à esquerda e clique em **+ Adicionar** para iniciar.

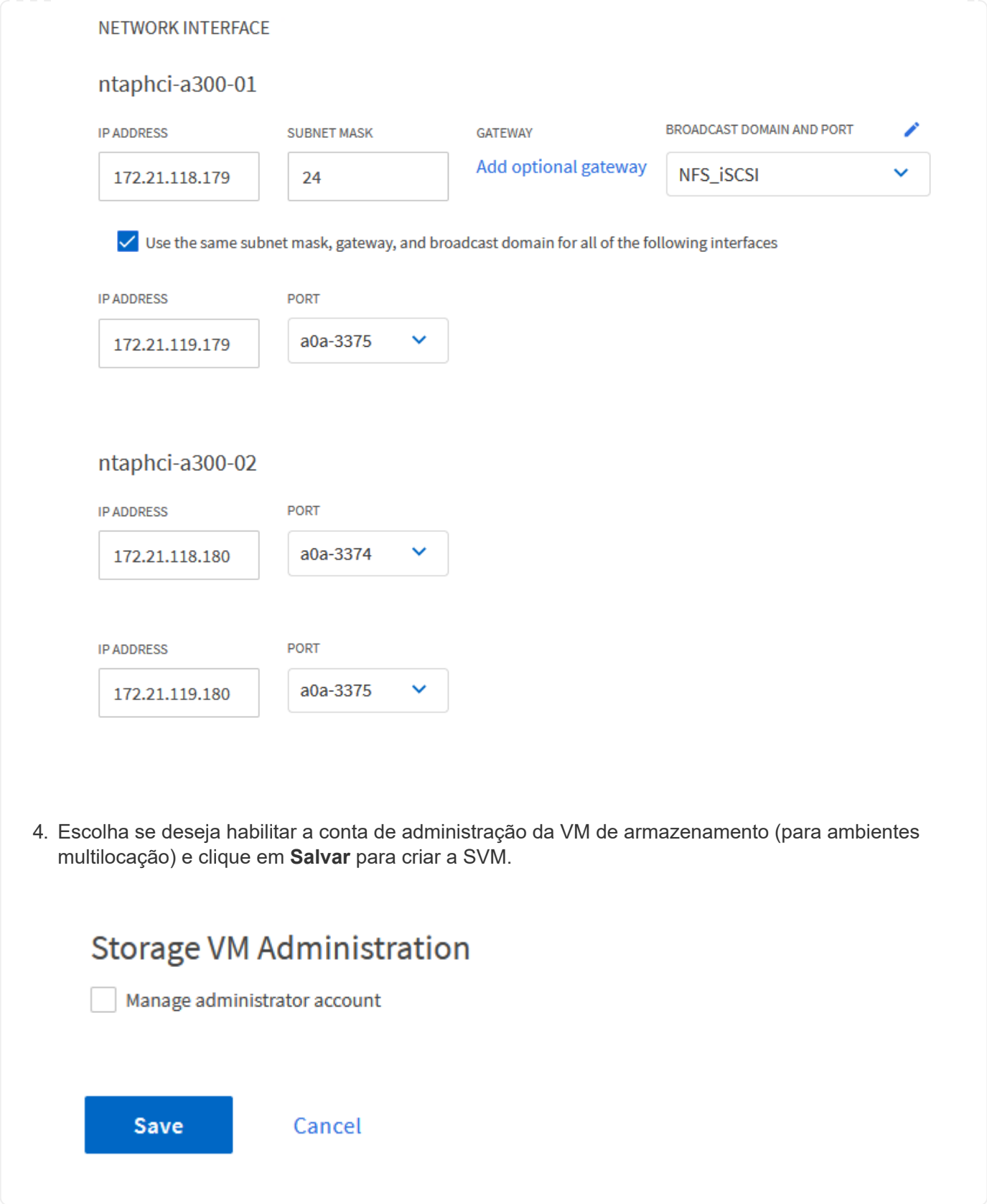


2. No assistente **Adicionar VM de armazenamento**, forneça um **Nome** para a SVM, selecione o **Espaço IP** e, em seguida, em **Protocolo de acesso**, clique na guia **iSCSI** e marque a caixa para **Ativar iSCSI**.



3. Na seção **Interface de rede**, preencha o **endereço IP**, a **máscara de sub-rede** e o **domínio e porta de transmissão** para o primeiro LIF. Para LIFs subsequentes, a caixa de seleção pode ser marcada para usar configurações comuns em todos os LIFs restantes ou usar configurações separadas.

> Para multipathing e failover em vários caminhos, a NetApp recomenda ter no mínimo dois LIFs por nó de armazenamento em redes Ethernet separadas para todas as SVMs em configurações iSCSI.



4. Escolha se deseja habilitar a conta de administração da VM de armazenamento (para ambientes multilocação) e clique em **Salvar** para criar a SVM.

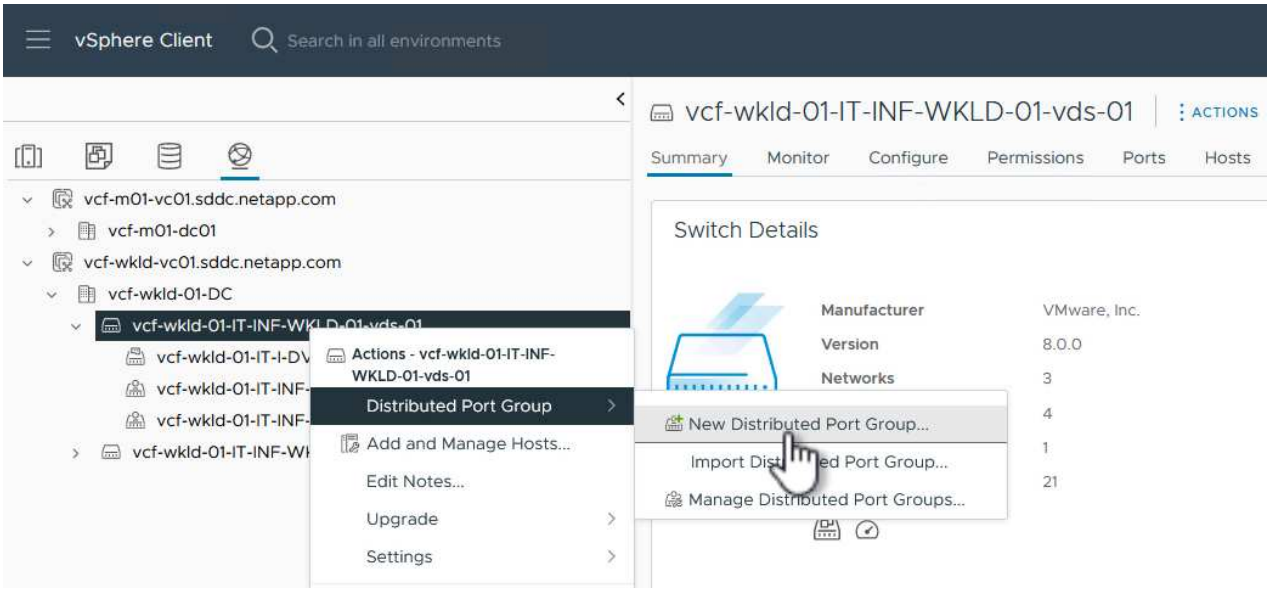
Configurar rede para iSCSI em hosts ESXi

As etapas a seguir são executadas no cluster do VI Workload Domain usando o cliente vSphere. Neste caso, o vCenter Single Sign-On está sendo usado para que o cliente vSphere seja comum em todos os domínios de gerenciamento e carga de trabalho.

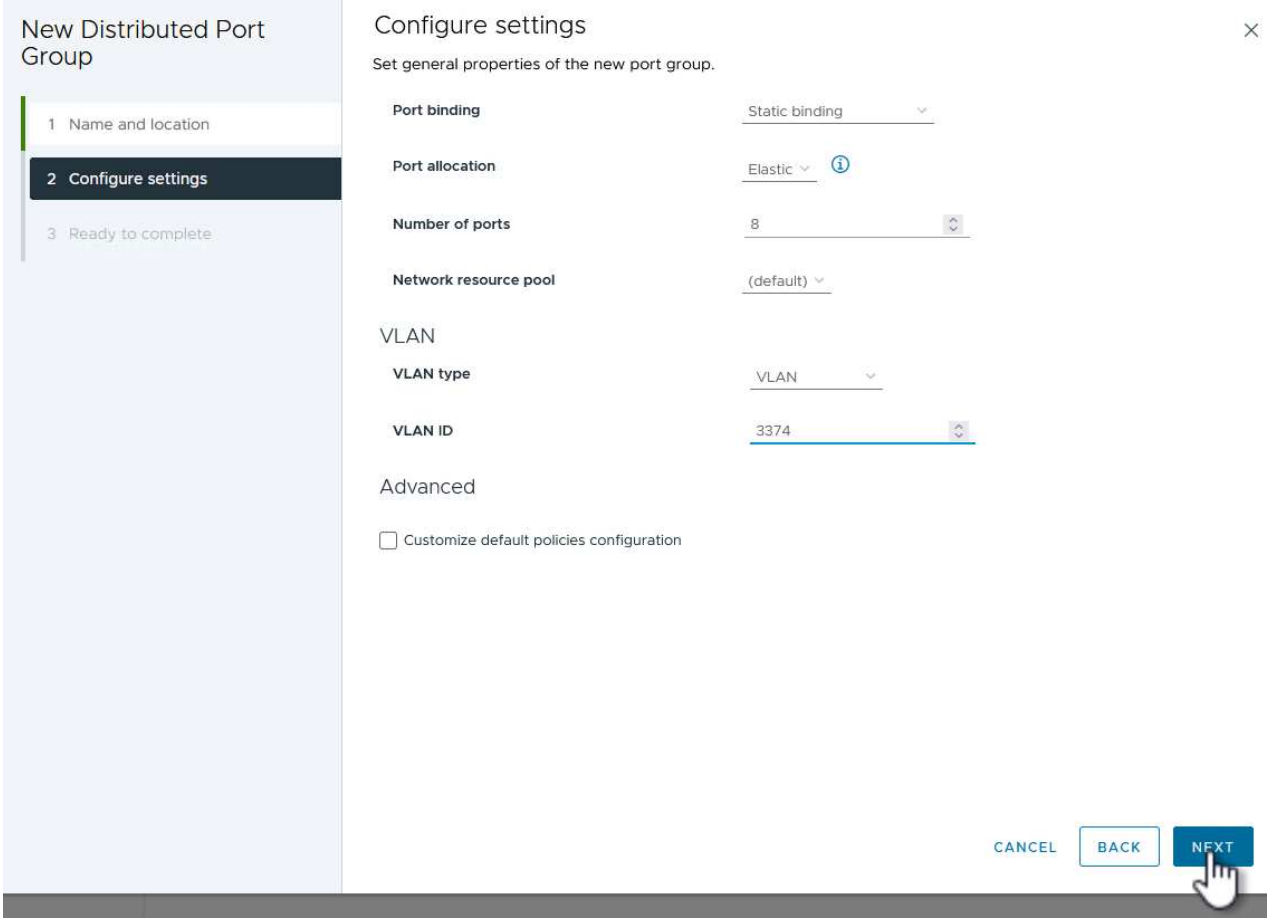
Criar grupos de portas distribuídas para tráfego iSCSI

Conclua o seguinte para criar um novo grupo de portas distribuídas para cada rede iSCSI:

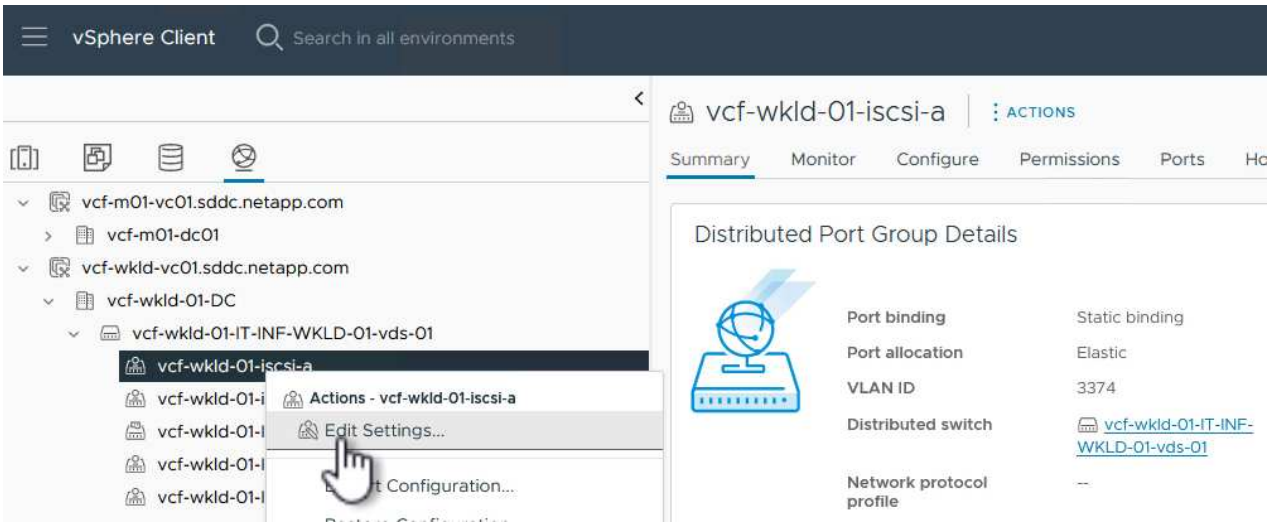
1. No cliente vSphere, navegue até **Inventário > Rede** para o domínio de carga de trabalho. Navegue até o Distributed Switch existente e escolha a ação para criar **Novo Grupo de Portas Distribuídas…** .



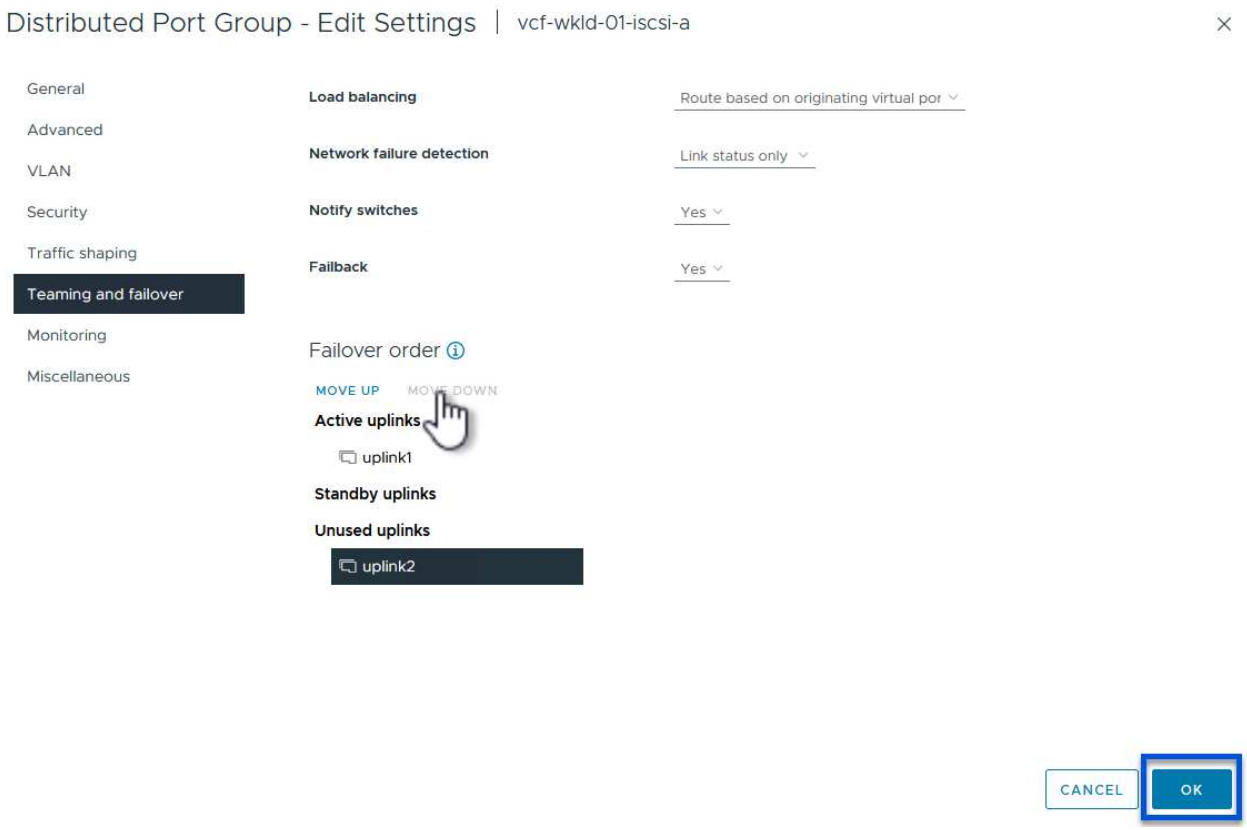
2. No assistente **Novo grupo de portas distribuídas**, preencha um nome para o novo grupo de portas e clique em **Avançar** para continuar.
3. Na página **Configurar configurações** preencha todas as configurações. Se VLANs estiverem sendo usadas, certifique-se de fornecer o ID de VLAN correto. Clique em **Avançar** para continuar.



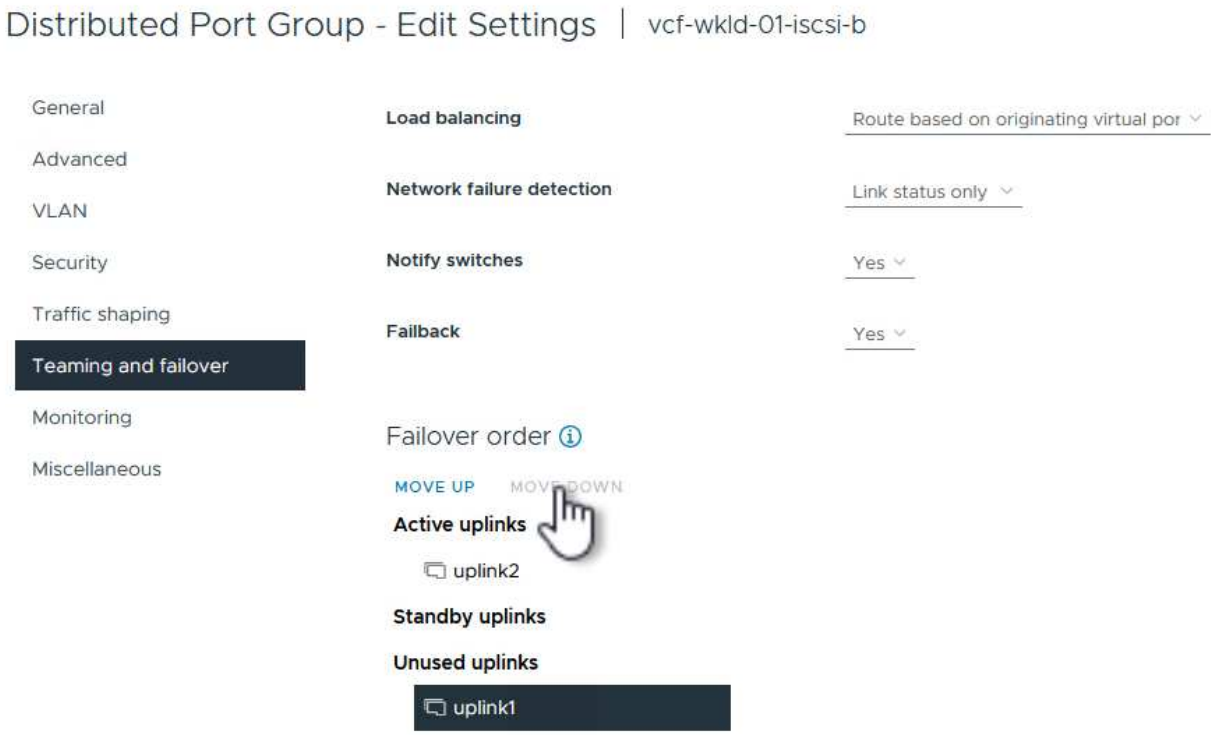
4. Na página **Pronto para concluir**, revise as alterações e clique em **Concluir** para criar o novo grupo de portas distribuídas.
5. Repita esse processo para criar um grupo de portas distribuídas para a segunda rede iSCSI que está sendo usada e certifique-se de ter inserido o **ID de VLAN** correto.
6. Depois que ambos os grupos de portas forem criados, navegue até o primeiro grupo de portas e selecione a ação **Editar configurações…**.



7. Na página **Grupo de portas distribuídas - Editar configurações**, navegue até **Agrupamento e failover** no menu à esquerda e clique em **uplink2** para movê-lo para **Uplinks não utilizados**.



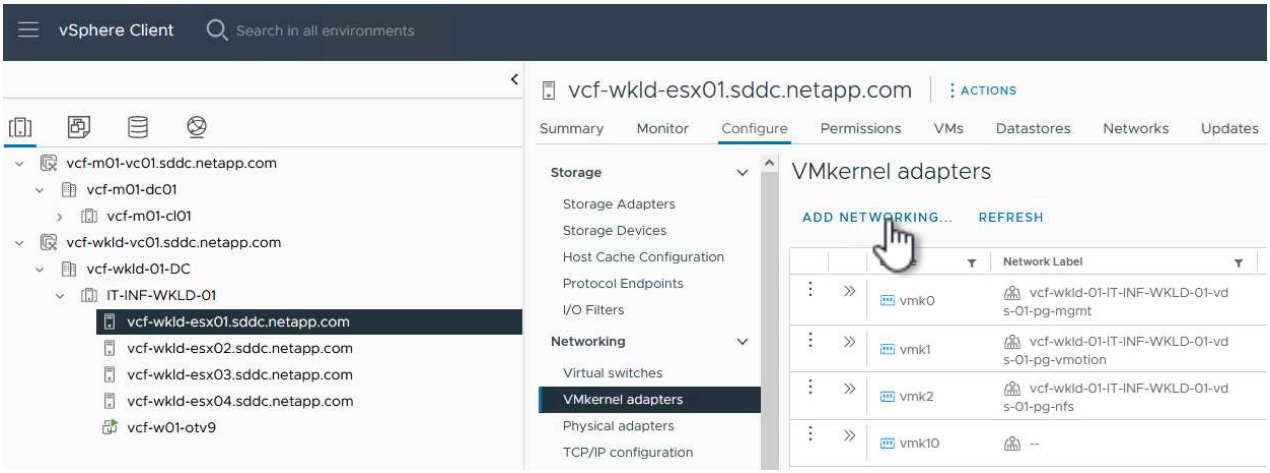
8. Repita esta etapa para o segundo grupo de portas iSCSI. Entretanto, desta vez mova **uplink1** para **Uplinks não utilizados**.



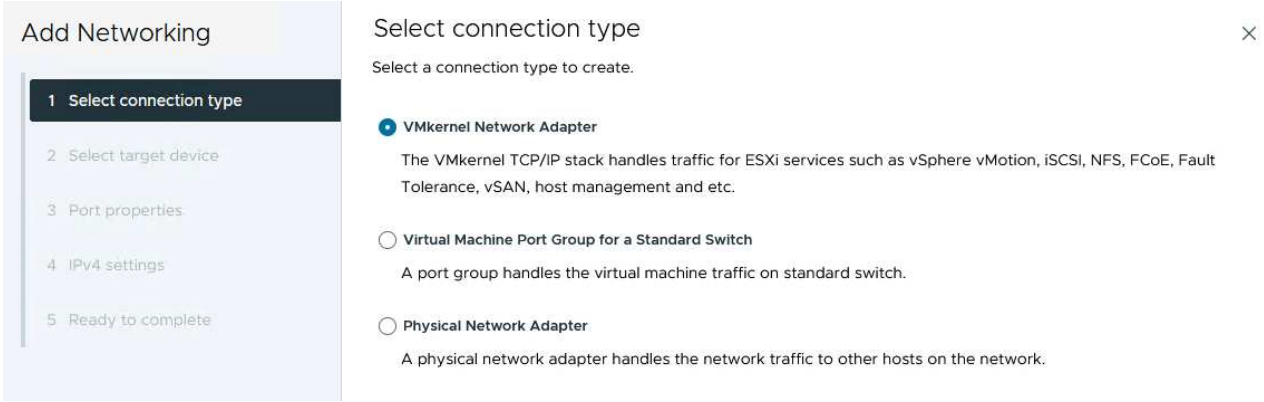
Crie adaptadores VMkernel em cada host ESXi

Repita esse processo em cada host ESXi no domínio de carga de trabalho.

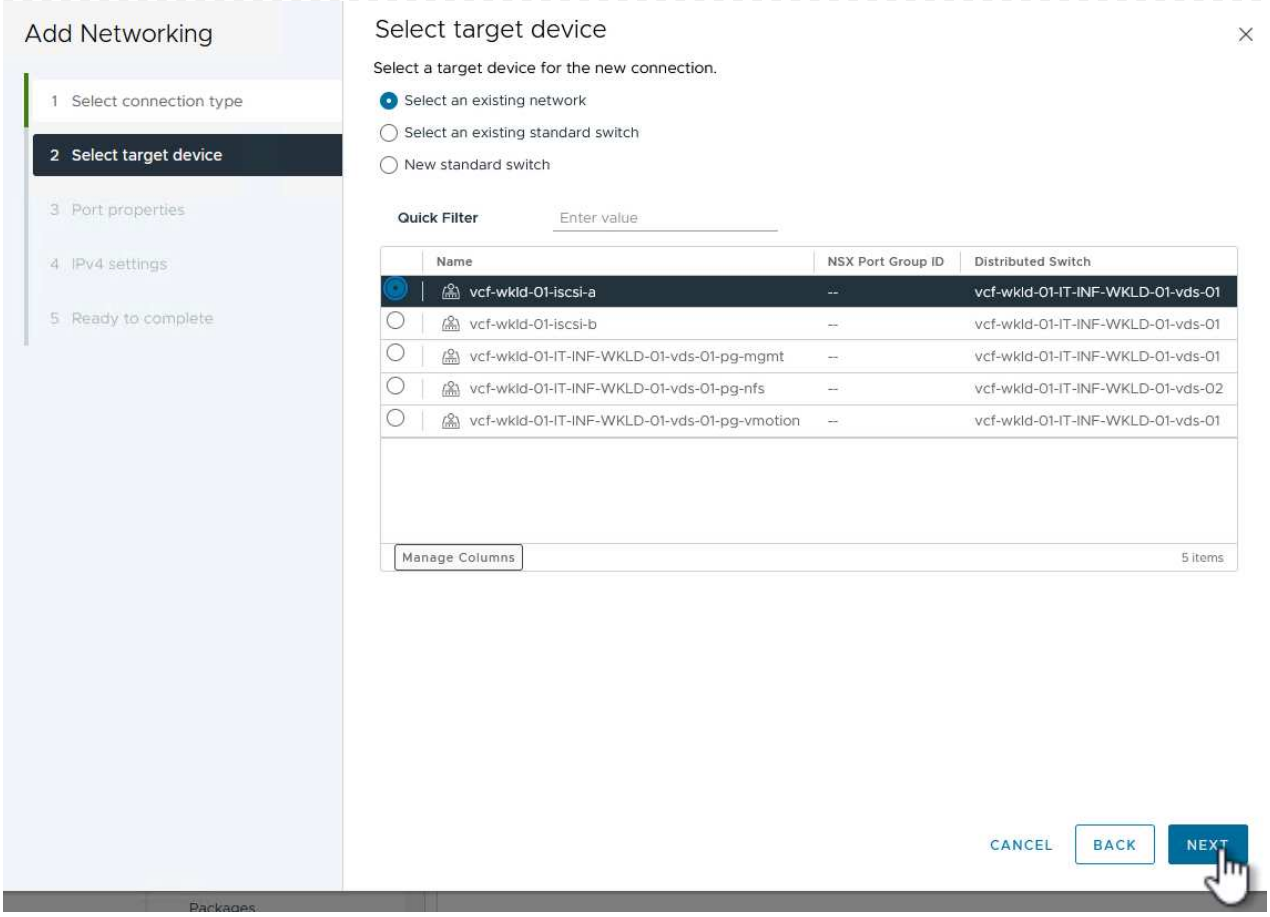
1. No cliente vSphere, navegue até um dos hosts ESXi no inventário do domínio de carga de trabalho. Na aba **Configurar** selecione **Adaptadores VMkernel** e clique em **Adicionar Rede…** para iniciar.



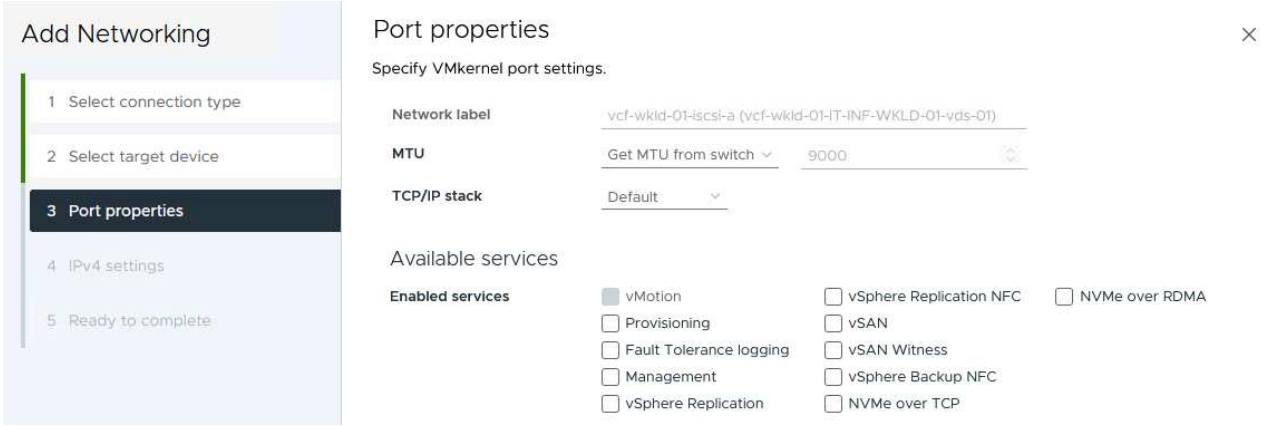
2. Na janela **Selecionar tipo de conexão**, escolha **Adaptador de rede VMkernel** e clique em **Avançar** para continuar.



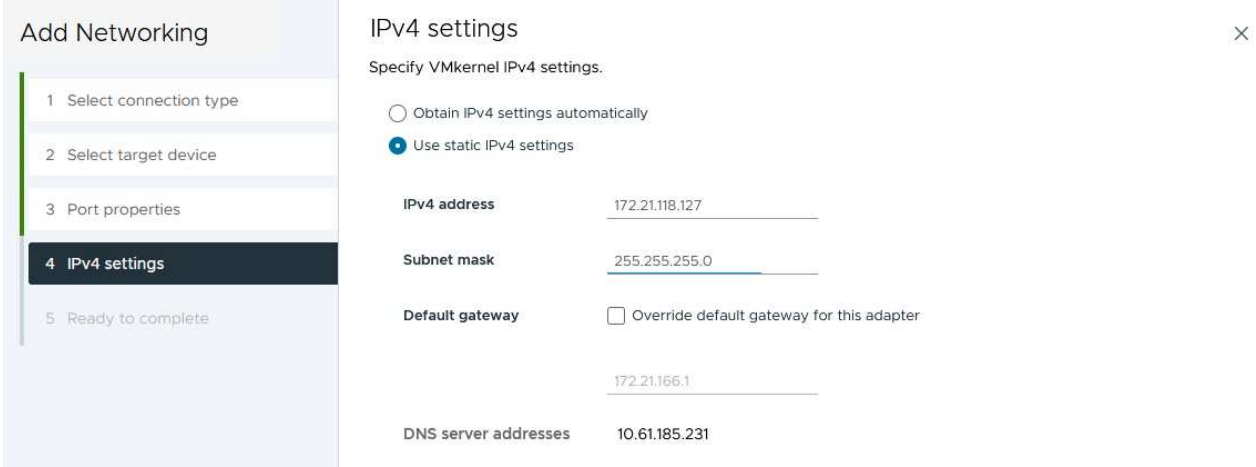
3. Na página **Selecionar dispositivo de destino**, escolha um dos grupos de portas distribuídas para iSCSI que foi criado anteriormente.



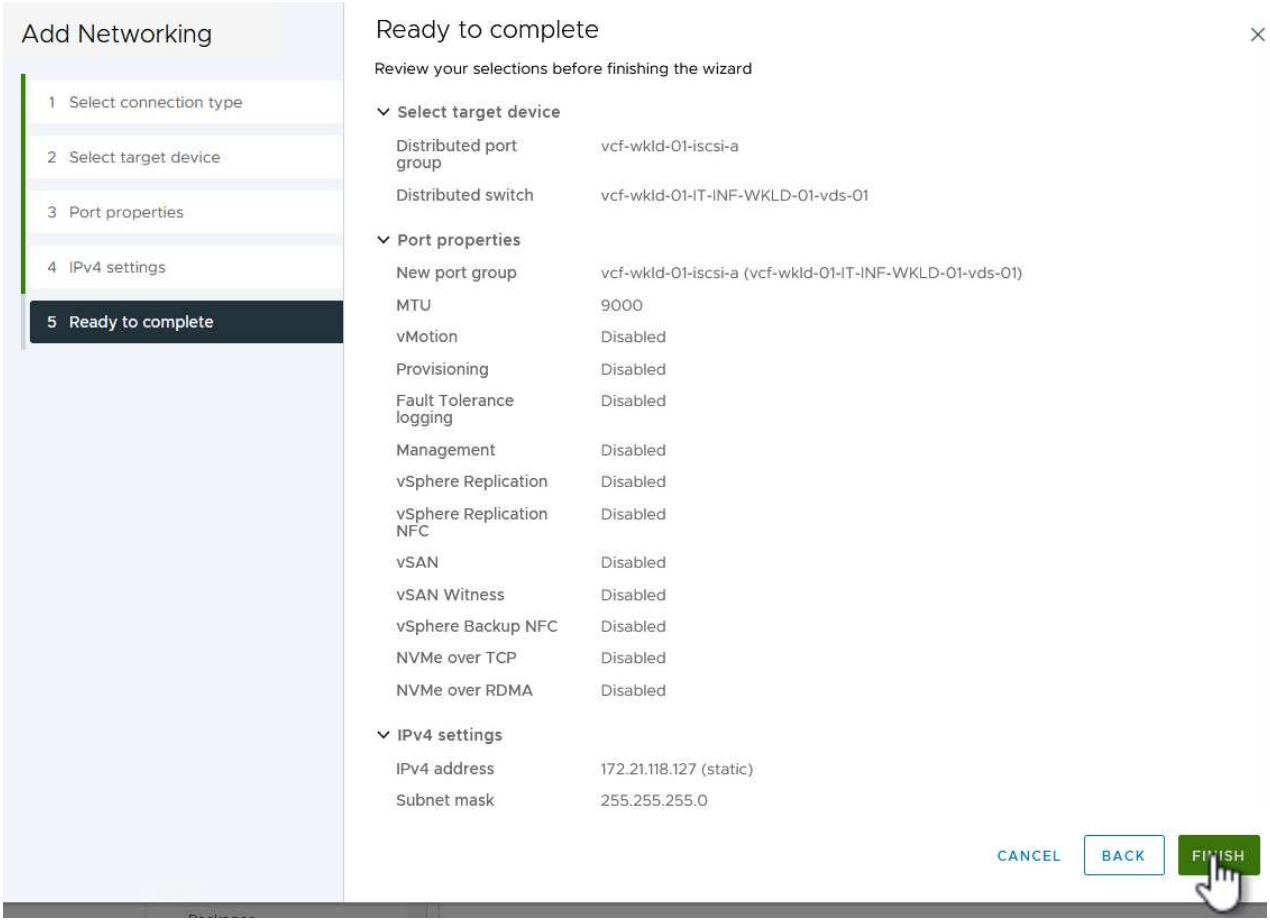
4. Na página **Propriedades da porta**, mantenha os padrões e clique em **Avançar** para continuar.



5. Na página **Configurações IPv4**, preencha o **endereço IP**, a **máscara de sub-rede** e forneça um novo endereço IP do gateway (somente se necessário). Clique em **Avançar** para continuar.



6. Revise suas seleções na página **Pronto para concluir** e clique em **Concluir** para criar o adaptador VMkernel.



7. Repita esse processo para criar um adaptador VMkernel para a segunda rede iSCSI.

Implantar e usar ferramentas ONTAP para configurar o armazenamento

As etapas a seguir são executadas no cluster de domínio de gerenciamento do VCF usando o cliente vSphere e envolvem a implantação do ONTAP Tools, a criação de um armazenamento de dados iSCSI vVols e a migração de VMs de gerenciamento para o novo armazenamento de dados.

Para domínios de carga de trabalho do VI, o ONTAP Tools é instalado no VCF Management Cluster, mas registrado no vCenter associado ao domínio de carga de trabalho do VI.

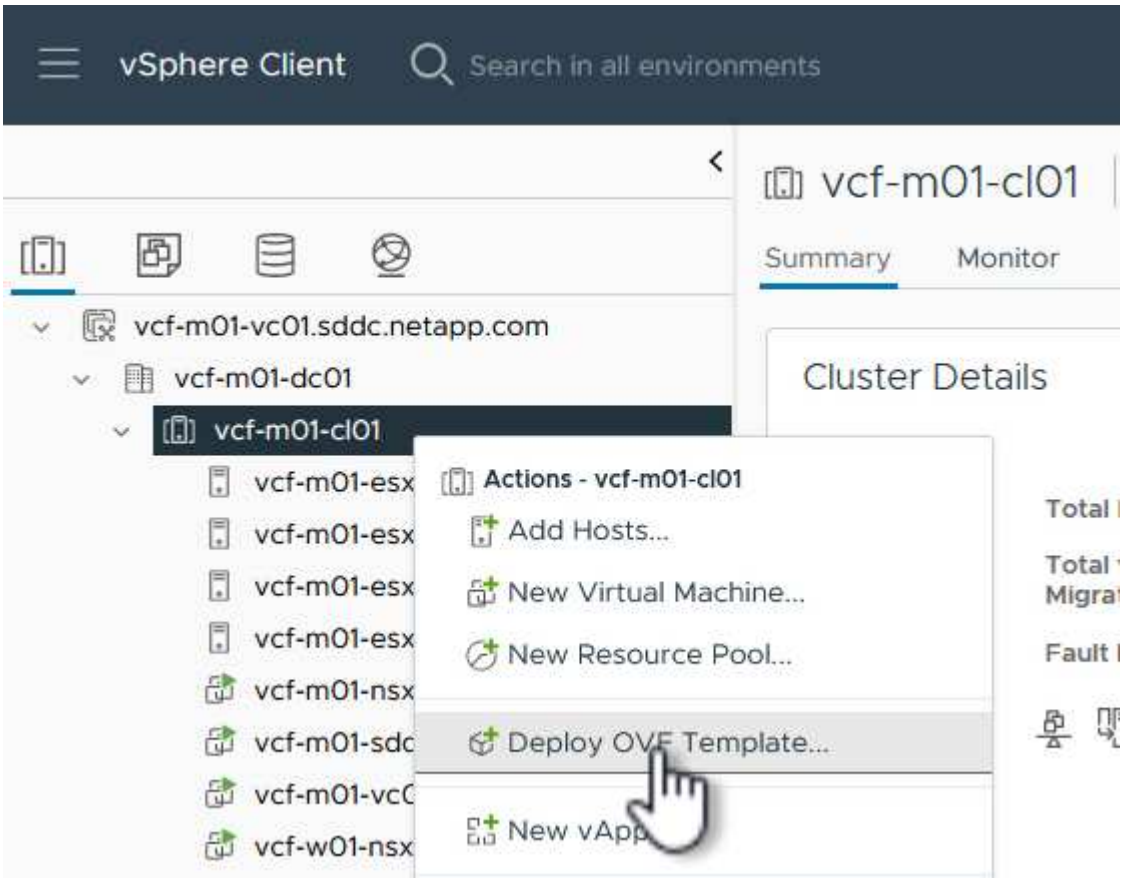
Para obter informações adicionais sobre a implantação e o uso do ONTAP Tools em um ambiente vCenter múltiplo, consulte"Requisitos para registrar ferramentas ONTAP em vários ambientes vCenter Servers" .

Implantar ONTAP tools for VMware vSphere

As ONTAP tools for VMware vSphere são implantadas como um dispositivo de VM e fornecem uma interface de usuário do vCenter integrada para gerenciar o armazenamento ONTAP .

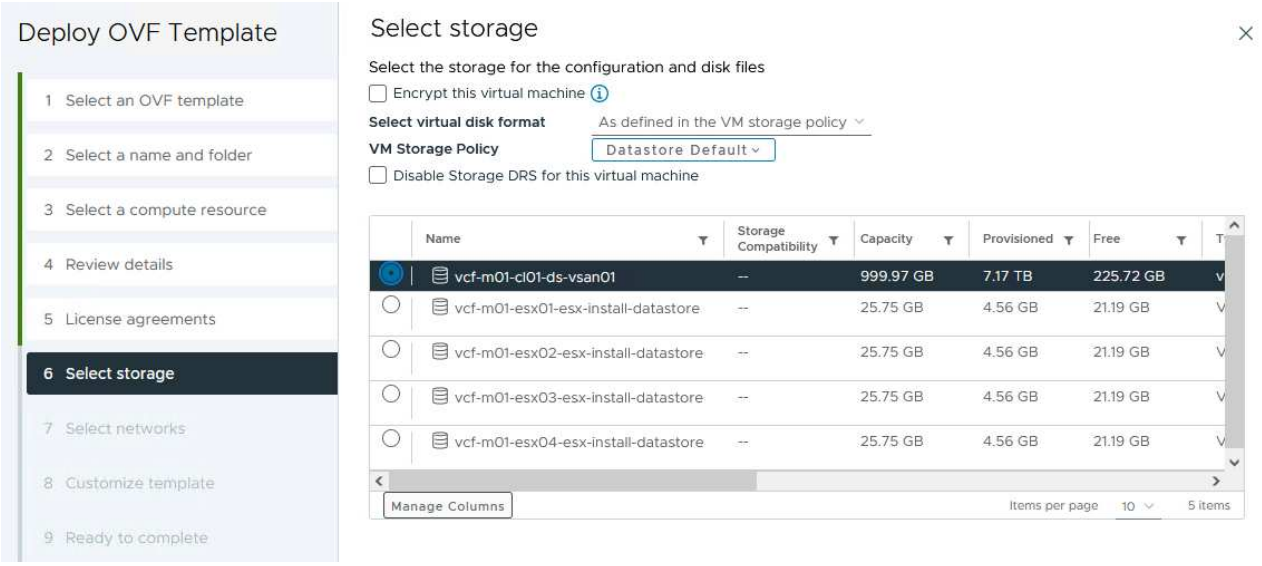
Conclua o seguinte para implantar ONTAP tools for VMware vSphere:

1. Obtenha a imagem OVA das ferramentas ONTAP do"Site de suporte da NetApp" e baixe para uma pasta local.
2. Efetue login no dispositivo vCenter para o domínio de gerenciamento do VCF.
3. Na interface do dispositivo vCenter, clique com o botão direito do mouse no cluster de gerenciamento e selecione **Implantar modelo OVF…**

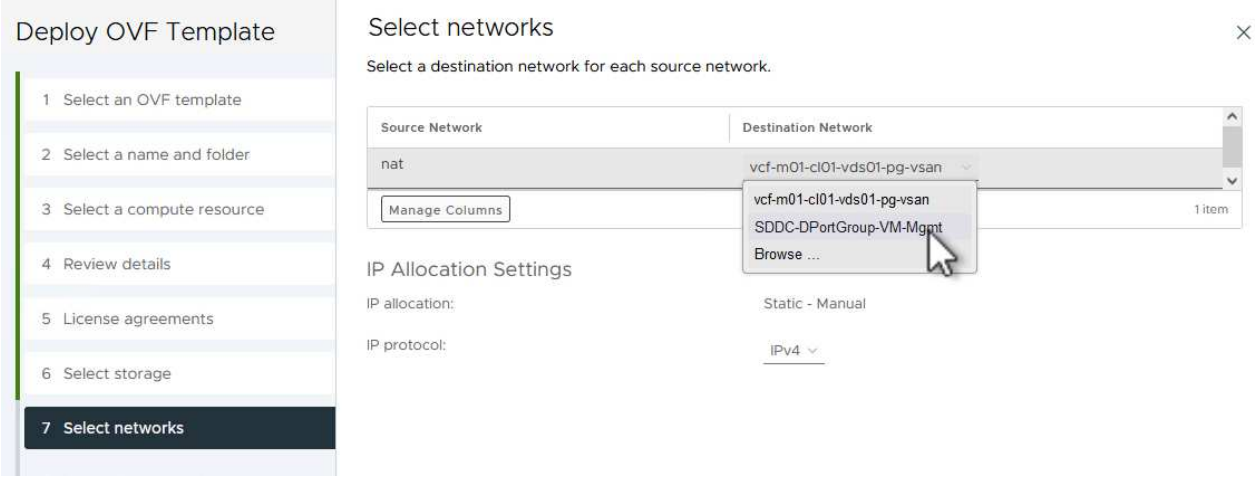


4. No assistente **Implantar modelo OVF**, clique no botão de opção **Arquivo local** e selecione o arquivo OVA das ferramentas ONTAP baixado na etapa anterior.

5. Para as etapas 2 a 5 do assistente, selecione um nome e uma pasta para a VM, selecione o recurso de computação, revise os detalhes e aceite o contrato de licença.
6. Para o local de armazenamento dos arquivos de configuração e de disco, selecione o armazenamento de dados vSAN do cluster de domínio de gerenciamento do VCF.

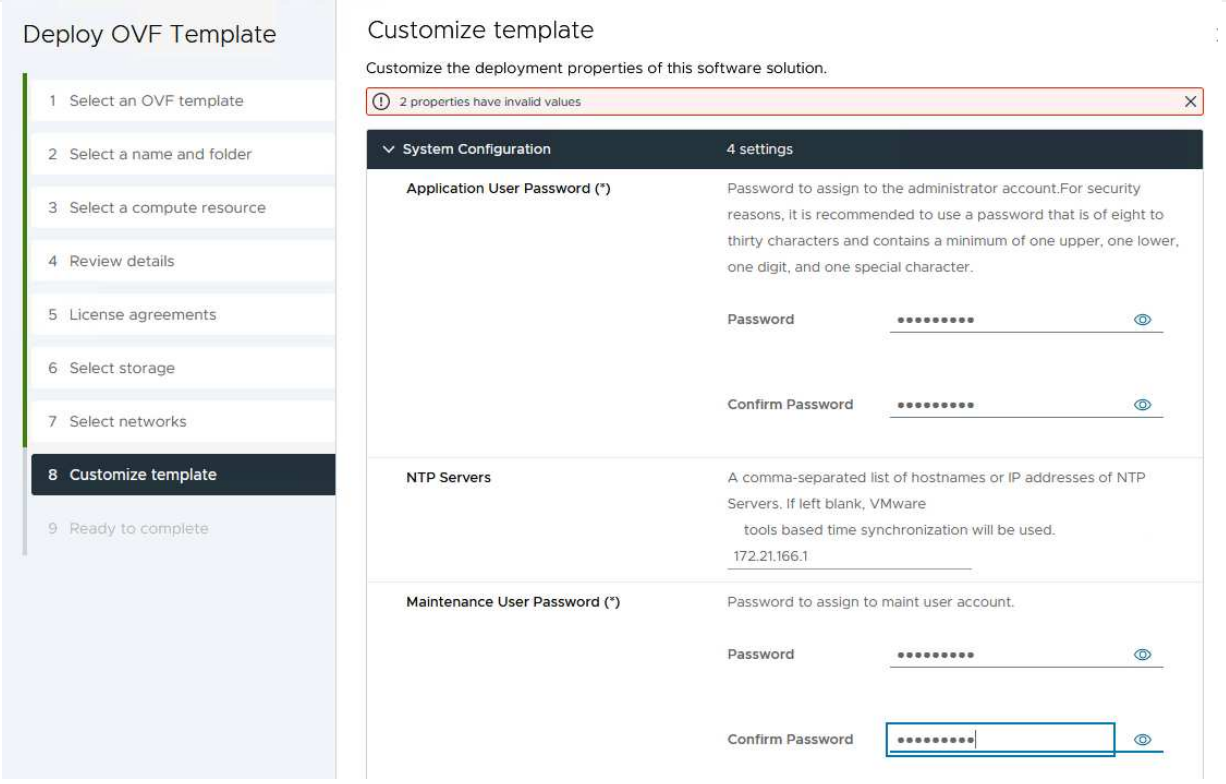


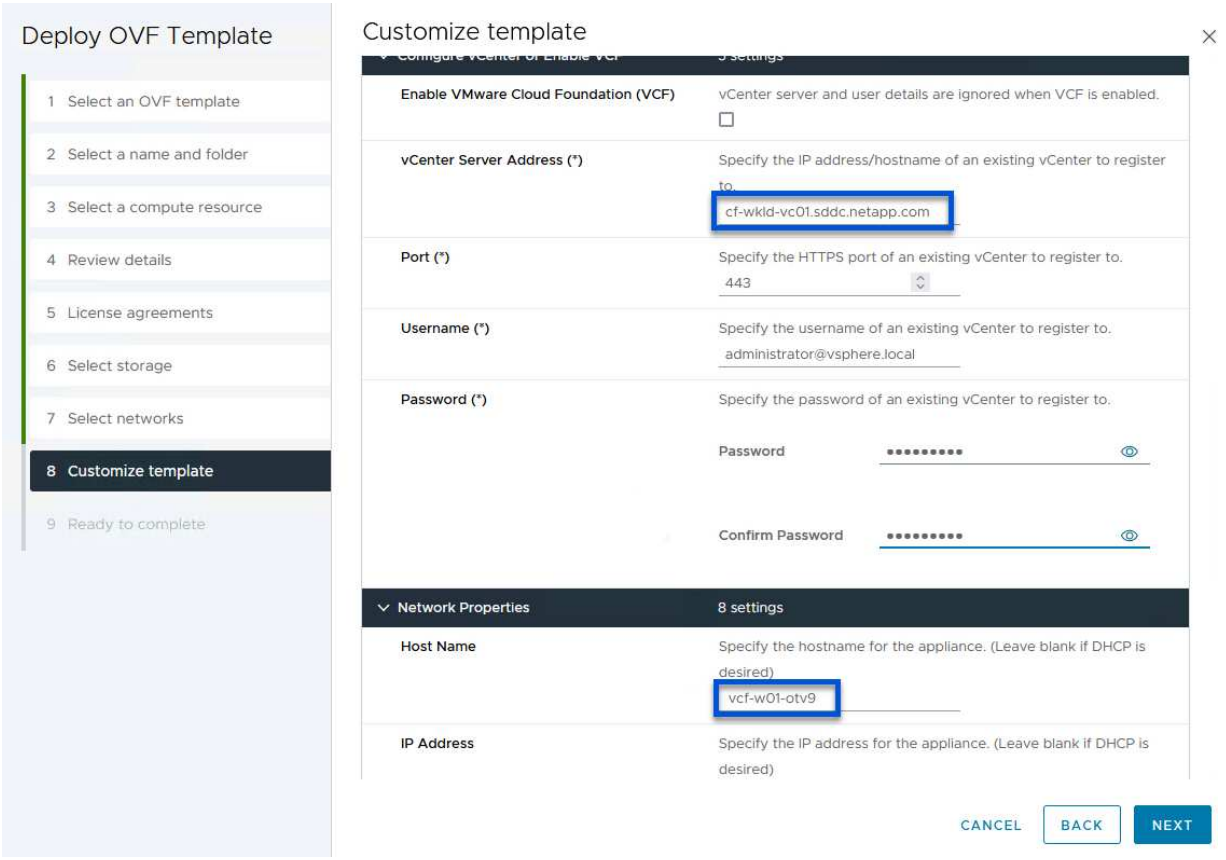
7. Na página Selecionar rede, selecione a rede usada para o tráfego de gerenciamento.



8. Na página Personalizar modelo, preencha todas as informações necessárias:
   - Senha a ser usada para acesso administrativo ao ONTAP Tools.
   - Endereço IP do servidor NTP.
   - Senha da conta de manutenção do ONTAP Tools.
   - Senha do banco de dados ONTAP Tools Derby.
   - Não marque a caixa para **Ativar VMware Cloud Foundation (VCF)**. O modo VCF não é necessário para implantar armazenamento suplementar.
   - FQDN ou endereço IP do dispositivo vCenter para o **Domínio de Carga de Trabalho VI**
   - Credenciais para o dispositivo vCenter do **Domínio de Carga de Trabalho VI**
   - Forneça os campos de propriedades de rede necessários.

     Clique em **Avançar** para continuar.

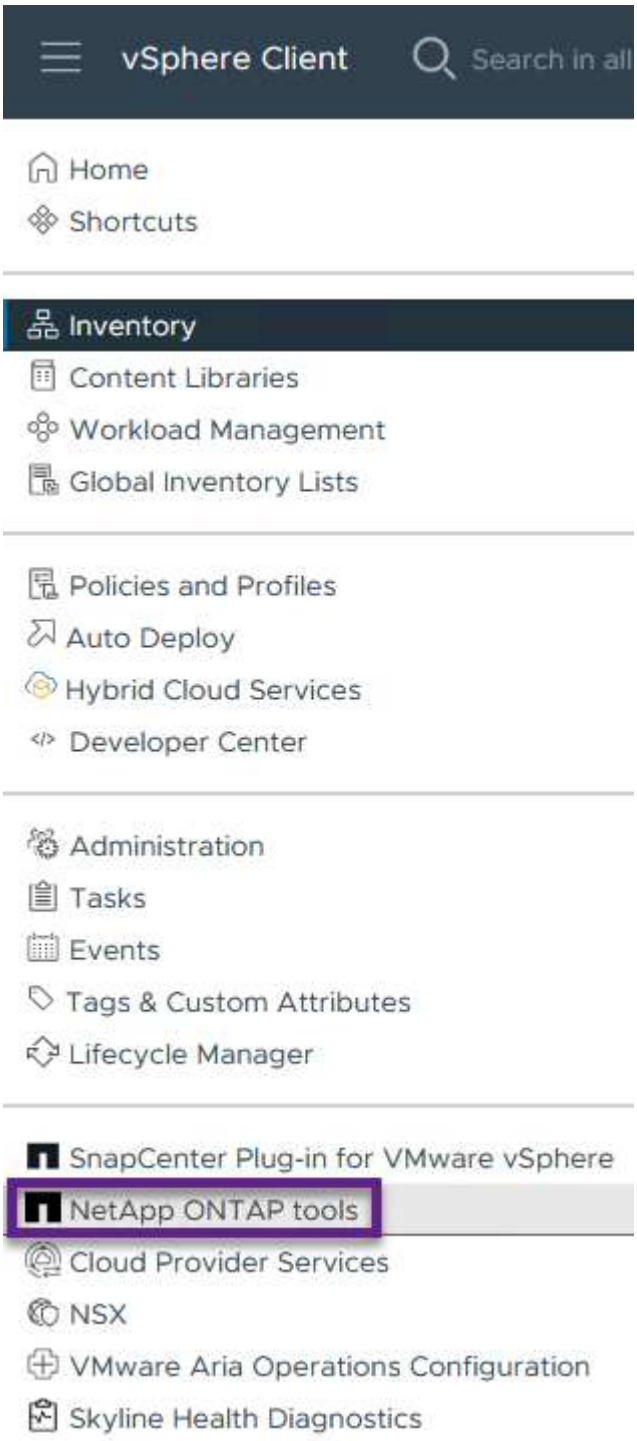




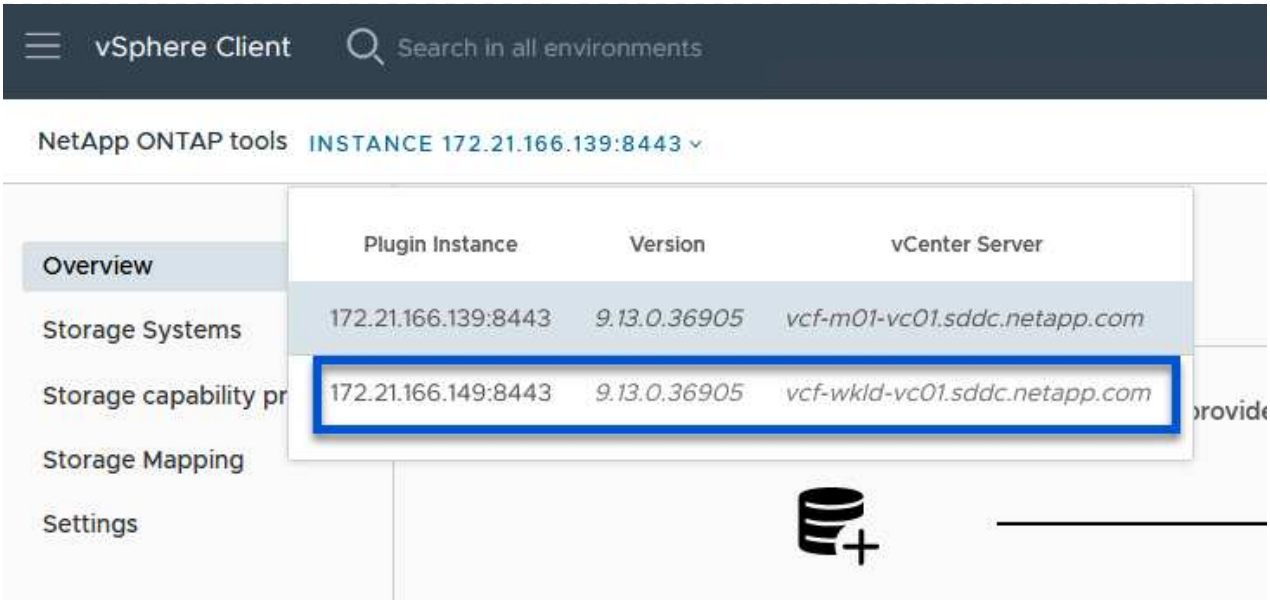
9. Revise todas as informações na página Pronto para concluir e clique em Concluir para começar a implantar o dispositivo ONTAP Tools.

Adicione um sistema de armazenamento ao ONTAP Tools.

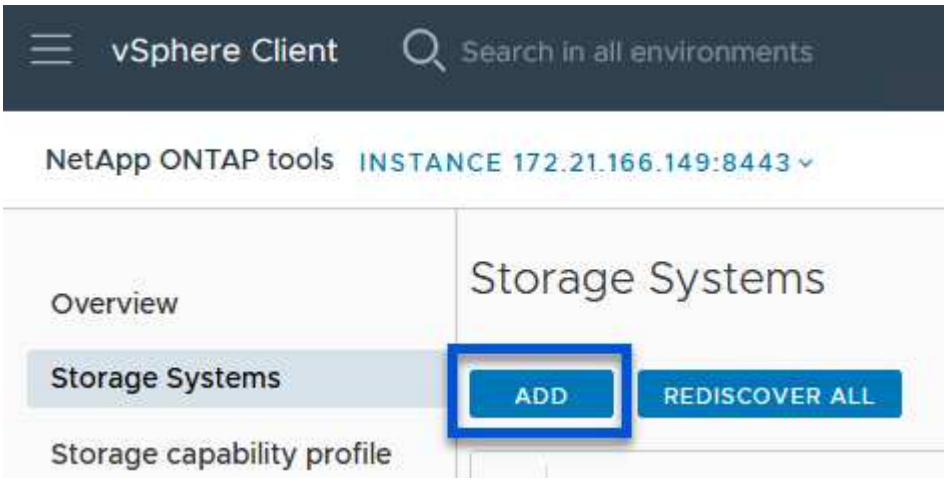
1. Acesse o NetApp ONTAP Tools selecionando-o no menu principal no cliente vSphere.



2. No menu suspenso **INSTÂNCIA** na interface da ferramenta ONTAP , selecione a instância da ferramenta ONTAP associada ao domínio de carga de trabalho a ser gerenciado.

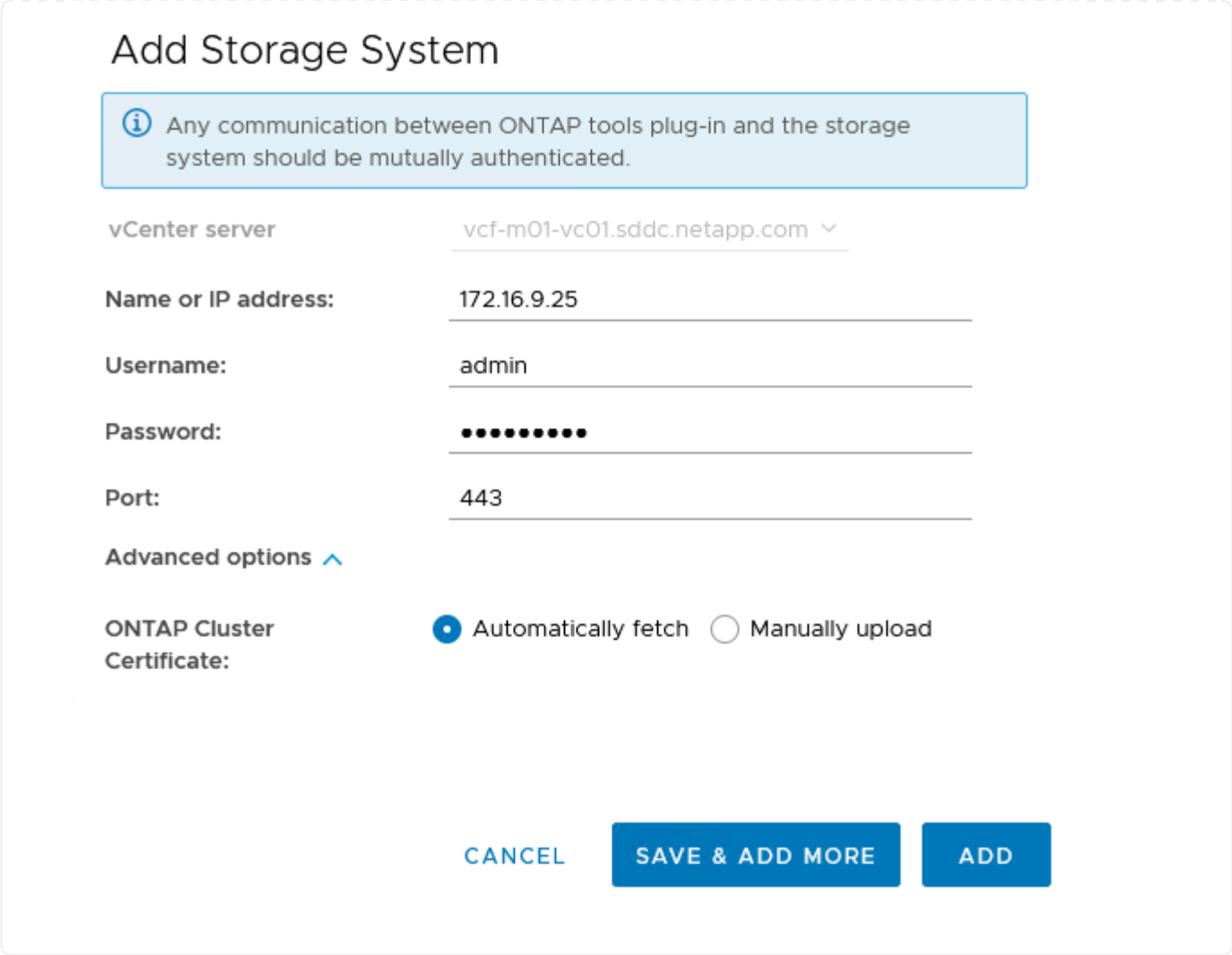


3. No ONTAP Tools, selecione **Sistemas de armazenamento** no menu à esquerda e pressione **Adicionar**.



4. Preencha o endereço IP, as credenciais do sistema de armazenamento e o número da porta. Clique em **Adicionar** para iniciar o processo de descoberta.

> O vVol requer credenciais de cluster ONTAP em vez de credenciais SVM. Para mais informações consulte "Adicionar sistemas de armazenamento" Na documentação das ferramentas ONTAP .

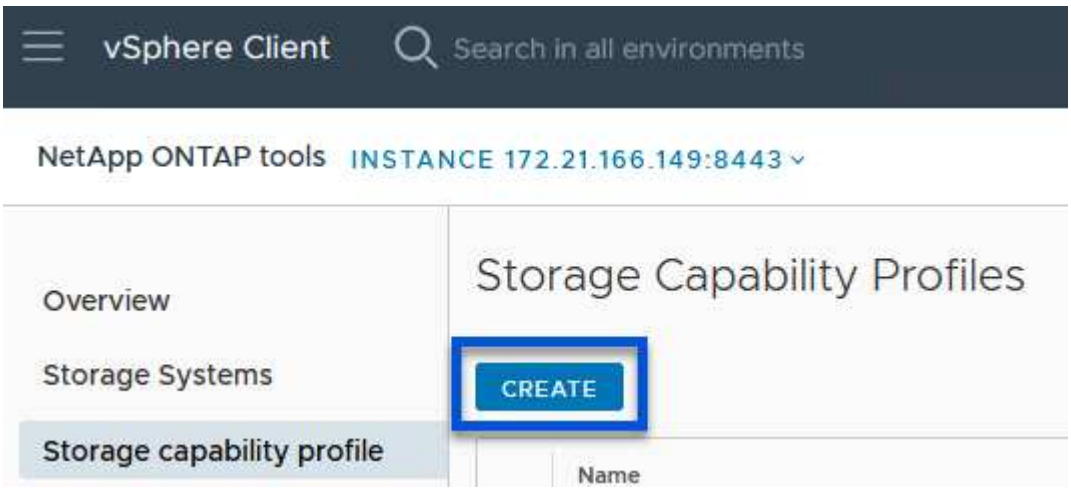

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Crie um perfil de capacidade de armazenamento no ONTAP Tools

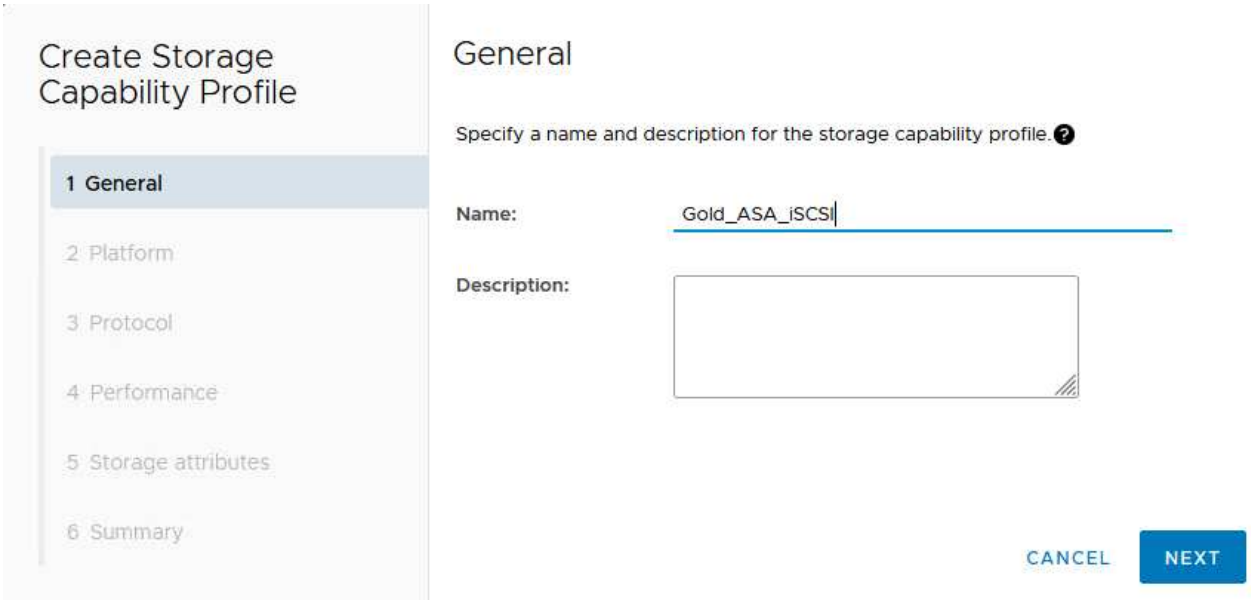
Os perfis de capacidade de armazenamento descrevem os recursos fornecidos por um conjunto de armazenamento ou sistema de armazenamento. Elas incluem definições de qualidade de serviço e são usadas para selecionar sistemas de armazenamento que atendem aos parâmetros definidos no perfil. Um dos perfis fornecidos pode ser usado ou novos podem ser criados.

Para criar um perfil de capacidade de armazenamento no ONTAP Tools, conclua as seguintes etapas:

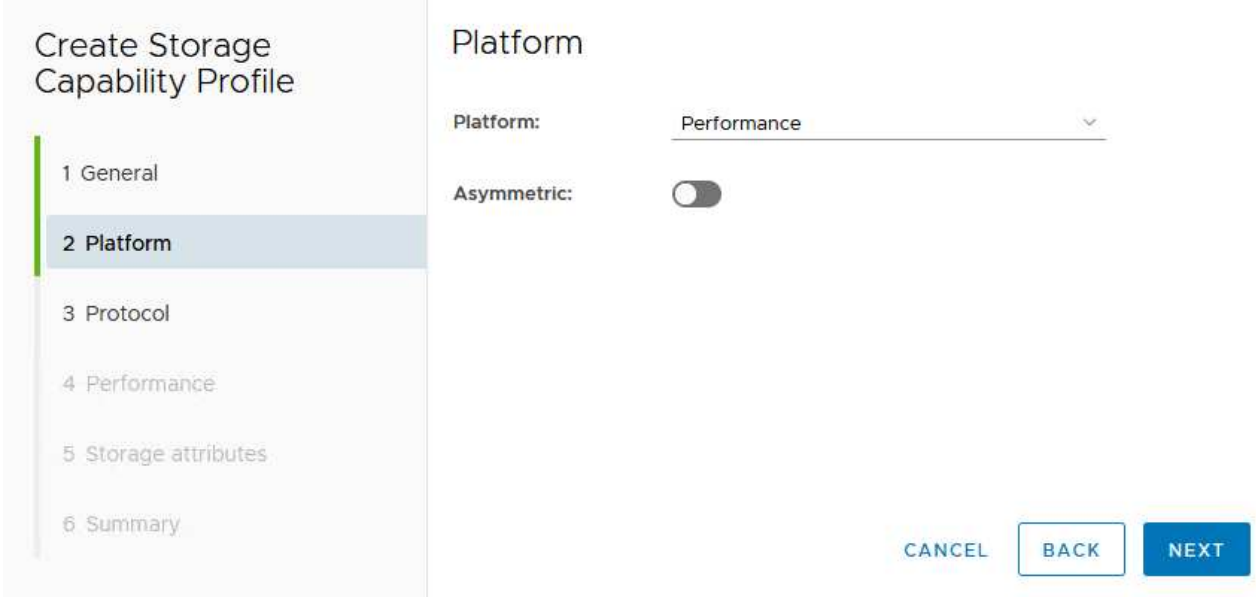
1. No ONTAP Tools, selecione **Perfil de capacidade de armazenamento** no menu à esquerda e pressione **Criar**.



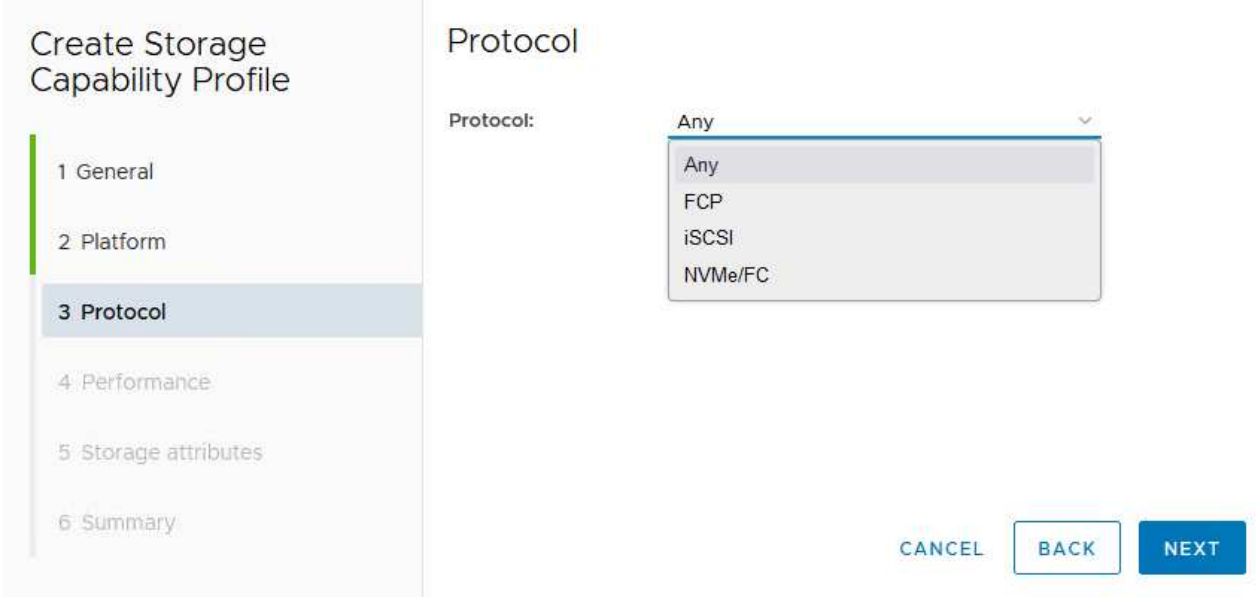
2. No assistente **Criar perfil de capacidade de armazenamento**, forneça um nome e uma descrição do perfil e clique em **Avançar**.



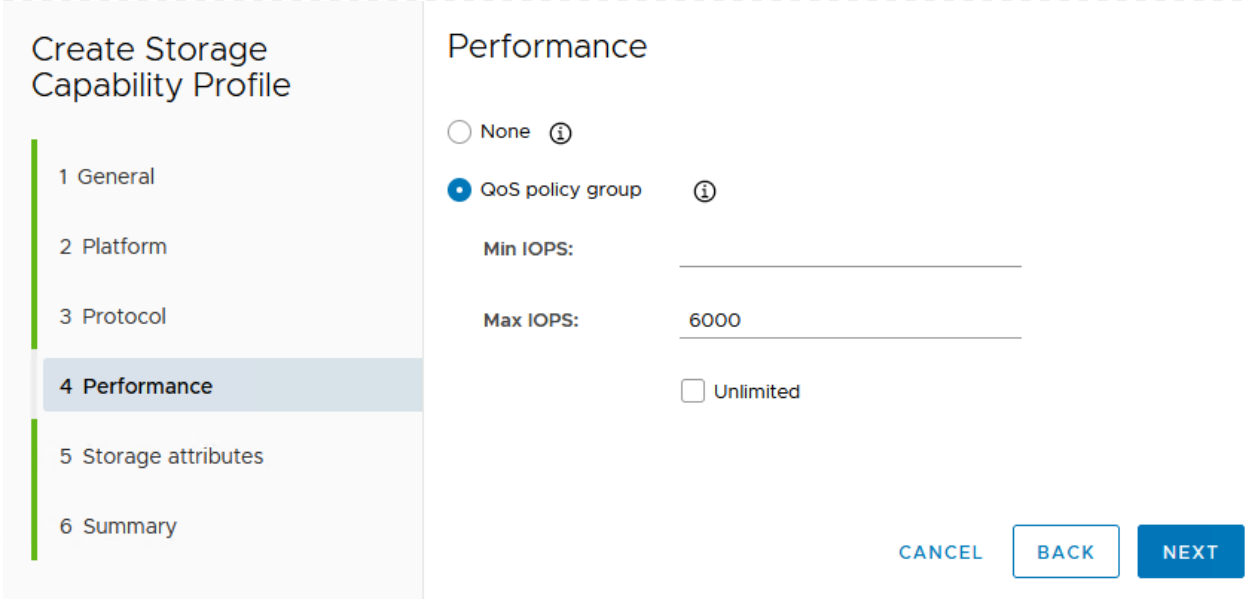
3. Selecione o tipo de plataforma e especifique que o sistema de armazenamento deve ser um All-Flash SAN Array definido como **Assimétrico** como falso.



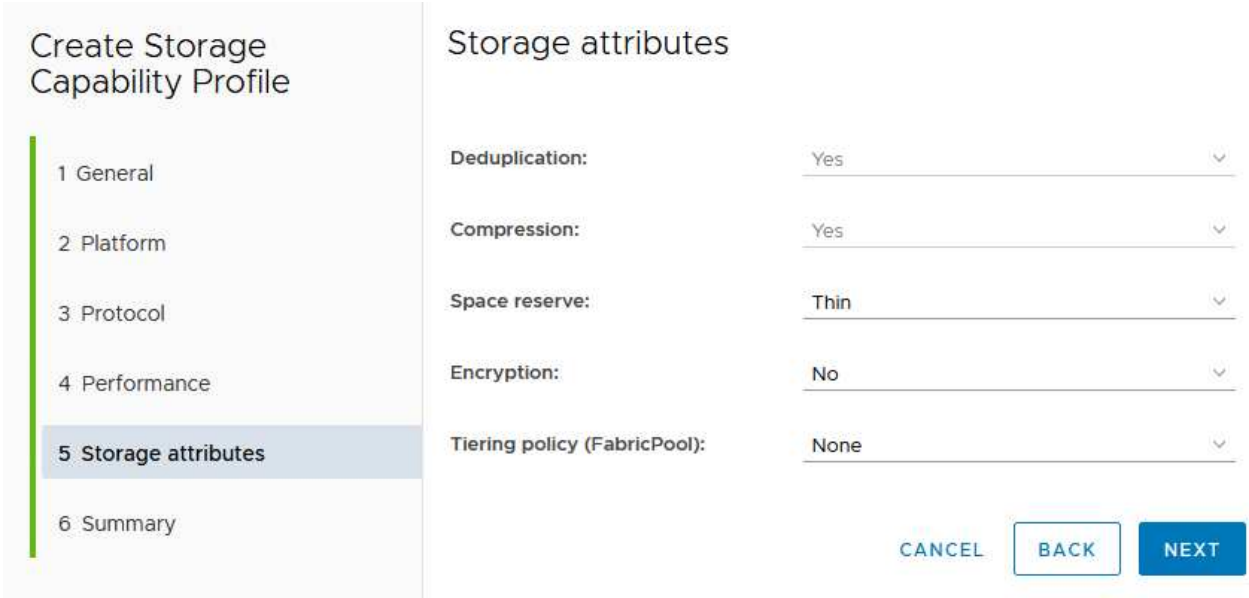
4. Em seguida, selecione a escolha do protocolo ou **Qualquer** para permitir todos os protocolos possíveis. Clique em **Avançar** para continuar.



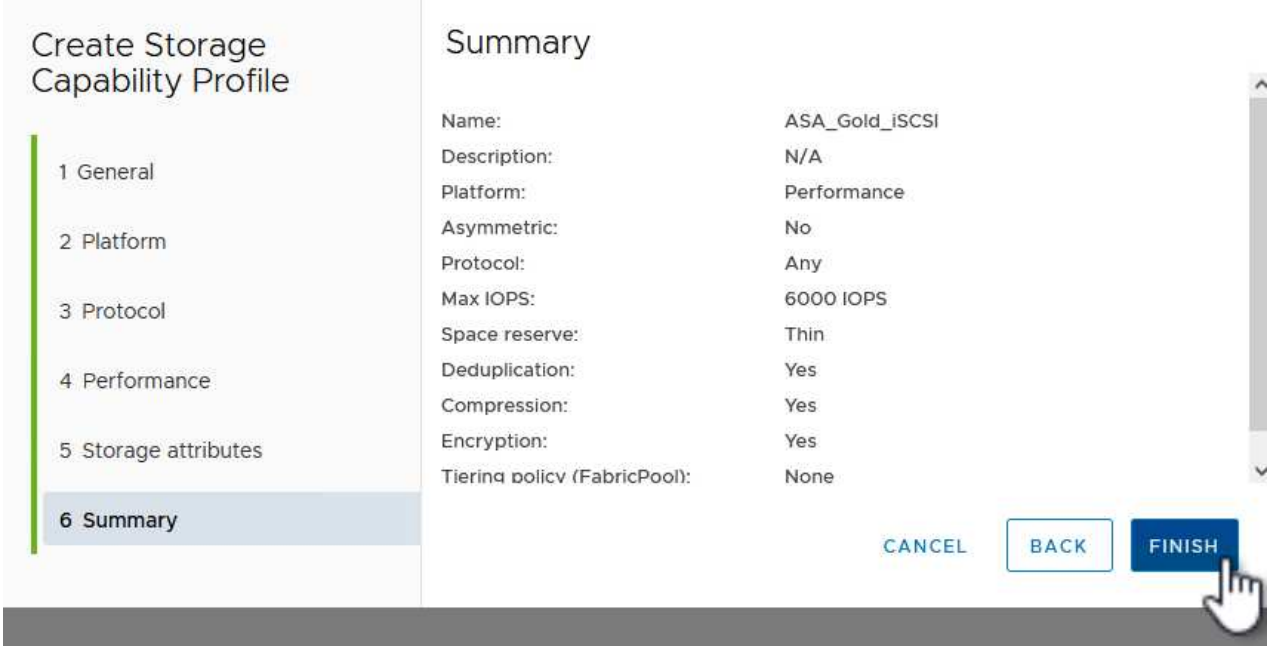
5. A página **desempenho** permite definir a qualidade do serviço na forma de IOPs mínimos e máximos permitidos.



6. Preencha a página **atributos de armazenamento** selecionando eficiência de armazenamento, reserva de espaço, criptografia e qualquer política de níveis, conforme necessário.



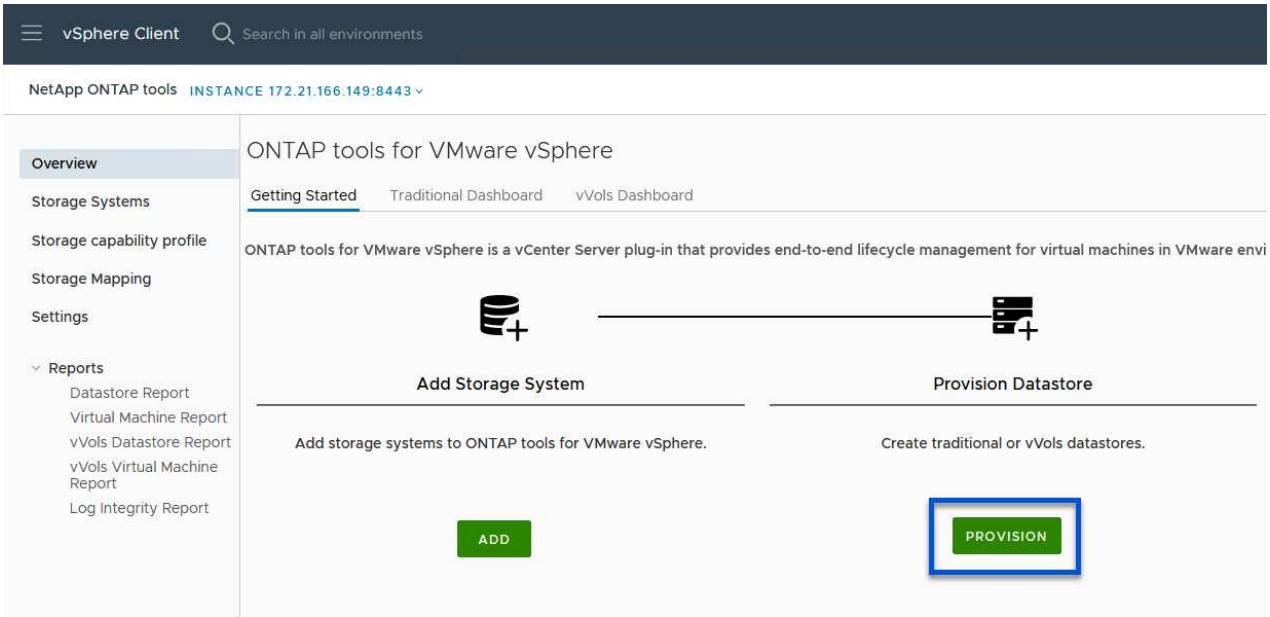
7. Por fim, revise o resumo e clique em Concluir para criar o perfil.


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Summary
Name: ASA_Gold_iSCSI
Description: N/A
Platform: Performance
Asymmetric: No
Protocol: Any
Max IOPS: 6000 IOPS
Space reserve: Thin
Deduplication: Yes
Compression: Yes
Encryption: Yes
Tiering policy (FabricPool): None
CANCEL
BACK
FINISH

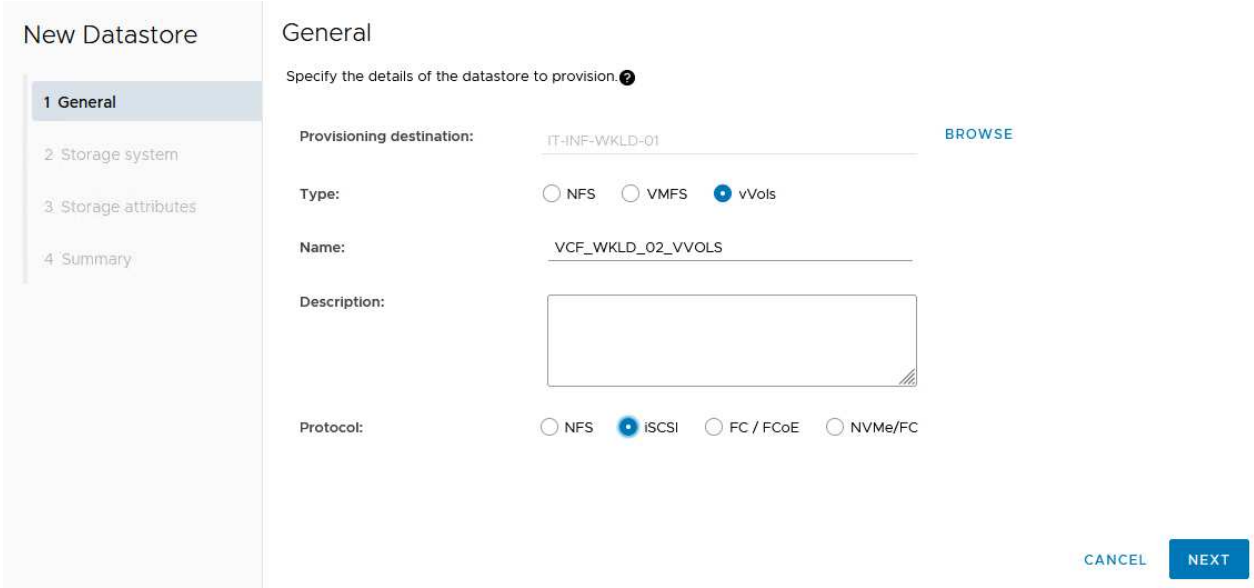
Crie um armazenamento de dados vVols no ONTAP Tools

Para criar um armazenamento de dados vVols no ONTAP Tools, conclua as seguintes etapas:

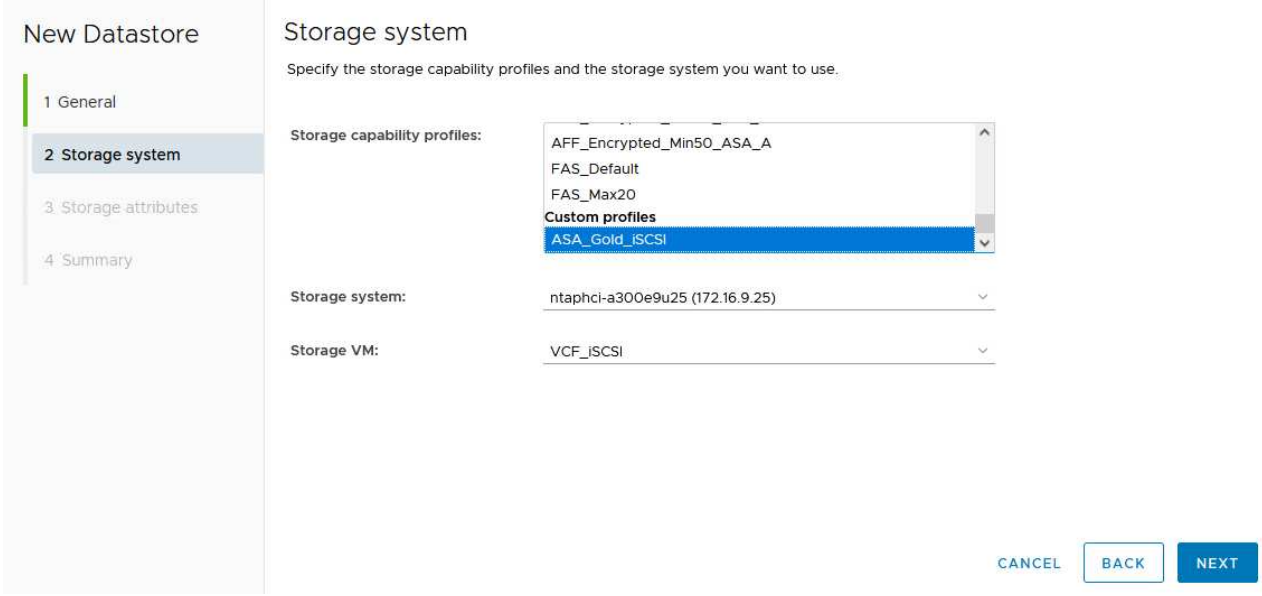
1. No ONTAP Tools, selecione **Visão geral** e na aba **Introdução** clique em **Provisionamento** para iniciar o assistente.



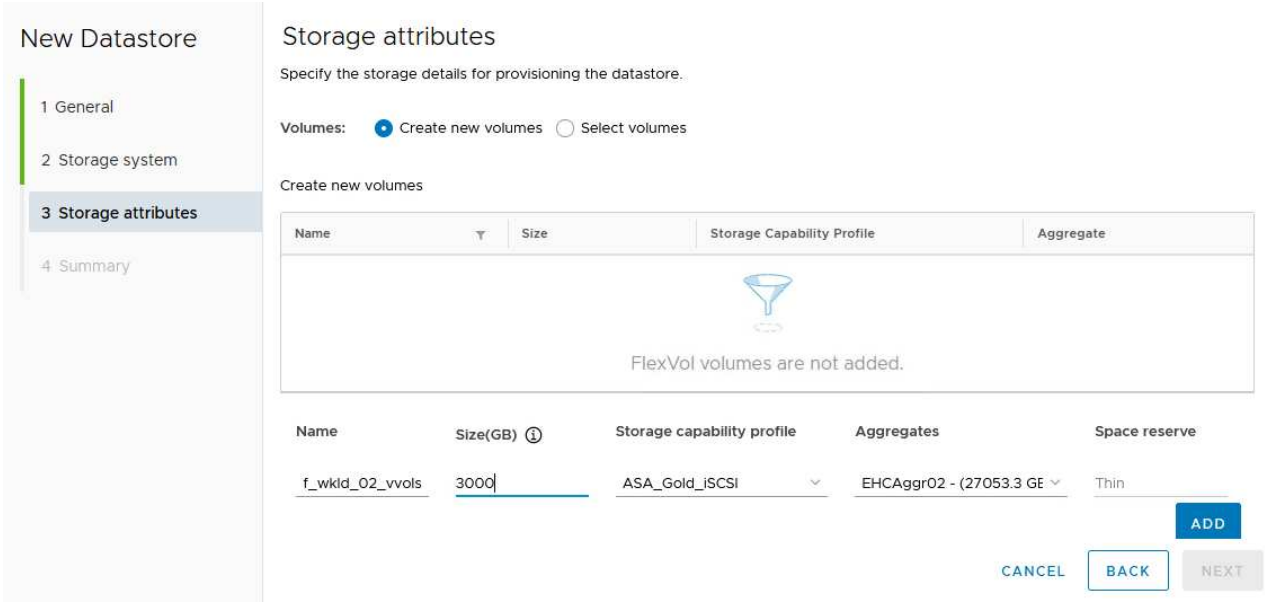
2. Na página **Geral** do assistente Novo armazenamento de dados, selecione o destino do datacenter ou cluster do vSphere. Selecione * vVols* como o tipo de armazenamento de dados, preencha um nome para o armazenamento de dados e selecione **iSCSI** como o protocolo. Clique em **Avançar** para continuar.



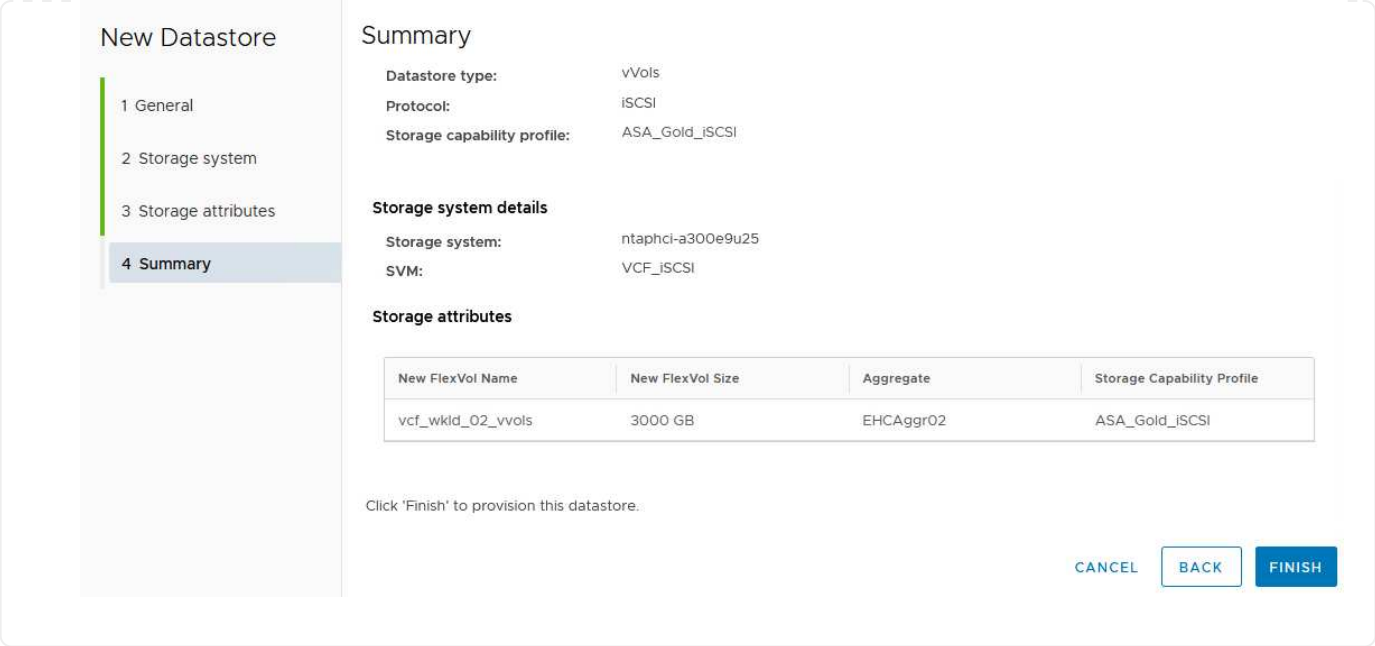
3. Na página **Sistema de armazenamento**, selecione um perfil de capacidade de armazenamento, o sistema de armazenamento e o SVM. Clique em **Avançar** para continuar.



4. Na página **Atributos de armazenamento**, selecione para criar um novo volume para o armazenamento de dados e preencha os atributos de armazenamento do volume a ser criado. Clique em **Adicionar** para criar o volume e depois em **Avançar** para continuar.



5. Por fim, revise o resumo e clique em **Concluir** para iniciar o processo de criação do armazenamento de dados vVol.



Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Adicione NFS e vVols como armazenamento suplementar aos domínios de carga de trabalho VI usando ONTAP tools for VMware vSphere

Neste caso de uso, descrevemos o procedimento para usar o ONTAP Tools for VMware para adicionar datastores NFS e vVols como armazenamento suplementar para um domínio de carga de trabalho de infraestrutura virtual (VI) do VMware Cloud Foundation (VCF). Este procedimento resume a implantação do ONTAP Tools para VMware vSphere, a configuração de uma Máquina Virtual de Armazenamento (SVM) com interfaces lógicas NFS e o provisionamento de armazenamentos de dados NFS e vVols .

NFS é usado como protocolo de armazenamento para o armazenamento de dados vVols .

Benefícios do NFS

Simplicidade e facilidade de uso: O NFS é simples de configurar e gerenciar, o que o torna uma excelente escolha para ambientes que exigem compartilhamento de arquivos rápido e fácil.

Escalabilidade: a arquitetura do ONTAP permite que o NFS seja dimensionado de forma eficiente, dando suporte às crescentes necessidades de dados sem mudanças significativas na infraestrutura.

Flexibilidade: O NFS oferece suporte a uma ampla variedade de aplicativos e cargas de trabalho, o que o torna versátil para vários casos de uso, incluindo ambientes virtualizados.

Para mais informações, consulte o "Guia de referência do NFS v3 para vSphere 8" .

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Crie uma máquina virtual de armazenamento (SVM) com interfaces lógicas (LIFs) para tráfego NFS.
- Crie um grupo de portas distribuídas para a rede NFS no domínio de carga de trabalho do VI.
- Crie um adaptador vmkernel para NFS nos hosts ESXi para o domínio de carga de trabalho do VI.
- Implante o ONTAP Tools no domínio de carga de trabalho do VI.
- Crie um novo armazenamento de dados NFS no domínio de carga de trabalho do VI.
- Crie um novo armazenamento de dados vVols no domínio de carga de trabalho do VI.

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP AFF ou FAS com portas de dados físicas em switches Ethernet dedicados ao tráfego de armazenamento.
- A implantação do domínio de gerenciamento do VCF foi concluída e o cliente vSphere está acessível.
- Um domínio de carga de trabalho VI foi implantado anteriormente.

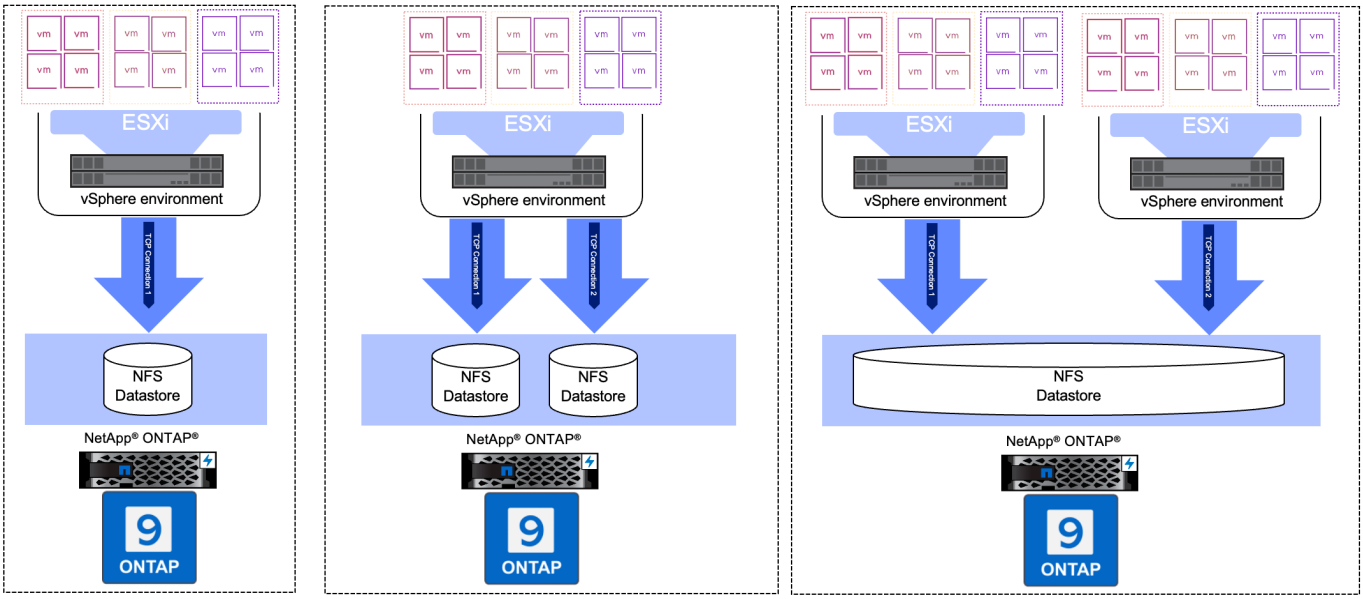
A NetApp recomenda projetos de rede redundantes para NFS, fornecendo tolerância a falhas para sistemas de armazenamento, switches, adaptadores de rede e sistemas host. É comum implantar o NFS com uma única sub-rede ou várias sub-redes, dependendo dos requisitos arquitetônicos.

Consulte "Melhores práticas para executar o NFS com o VMware vSphere" para obter informações detalhadas específicas do VMware vSphere.

Para obter orientação de rede sobre o uso do ONTAP com o VMware vSphere, consulte o "Configuração de rede - NFS" seção da documentação dos aplicativos empresariais da NetApp .

Esta documentação demonstra o processo de criação de um novo SVM e especificação das informações de endereço IP para criar vários LIFs para tráfego NFS. Para adicionar novos LIFs a um SVM existente, consulte"Criar uma LIF (interface de rede)" .

Para obter informações completas sobre o uso do NFS com clusters vSphere, consulte o"Guia de referência do NFS v3 para vSphere 8" .



Etapas de implantação

Para implantar o ONTAP Tools e usá-lo para criar um armazenamento de dados vVols e NFS no domínio de gerenciamento do VCF, conclua as seguintes etapas:

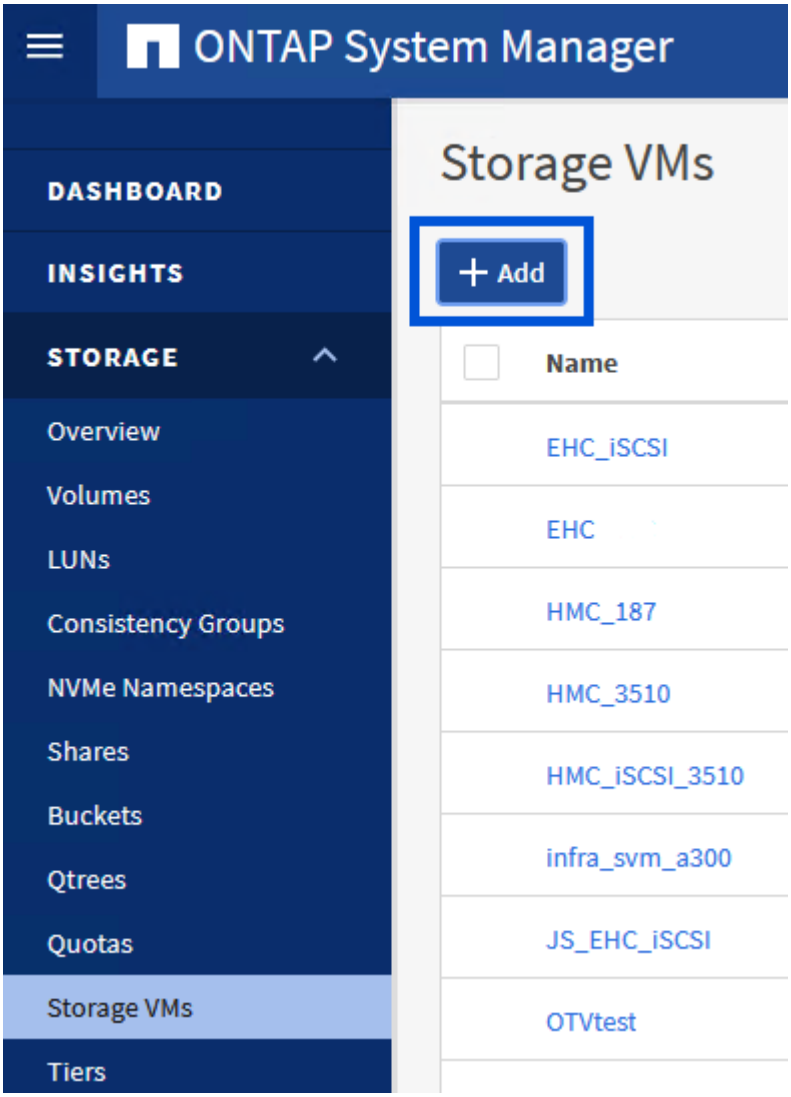
Crie SVM e LIFs no sistema de armazenamento ONTAP

A etapa seguinte é executada no ONTAP System Manager.

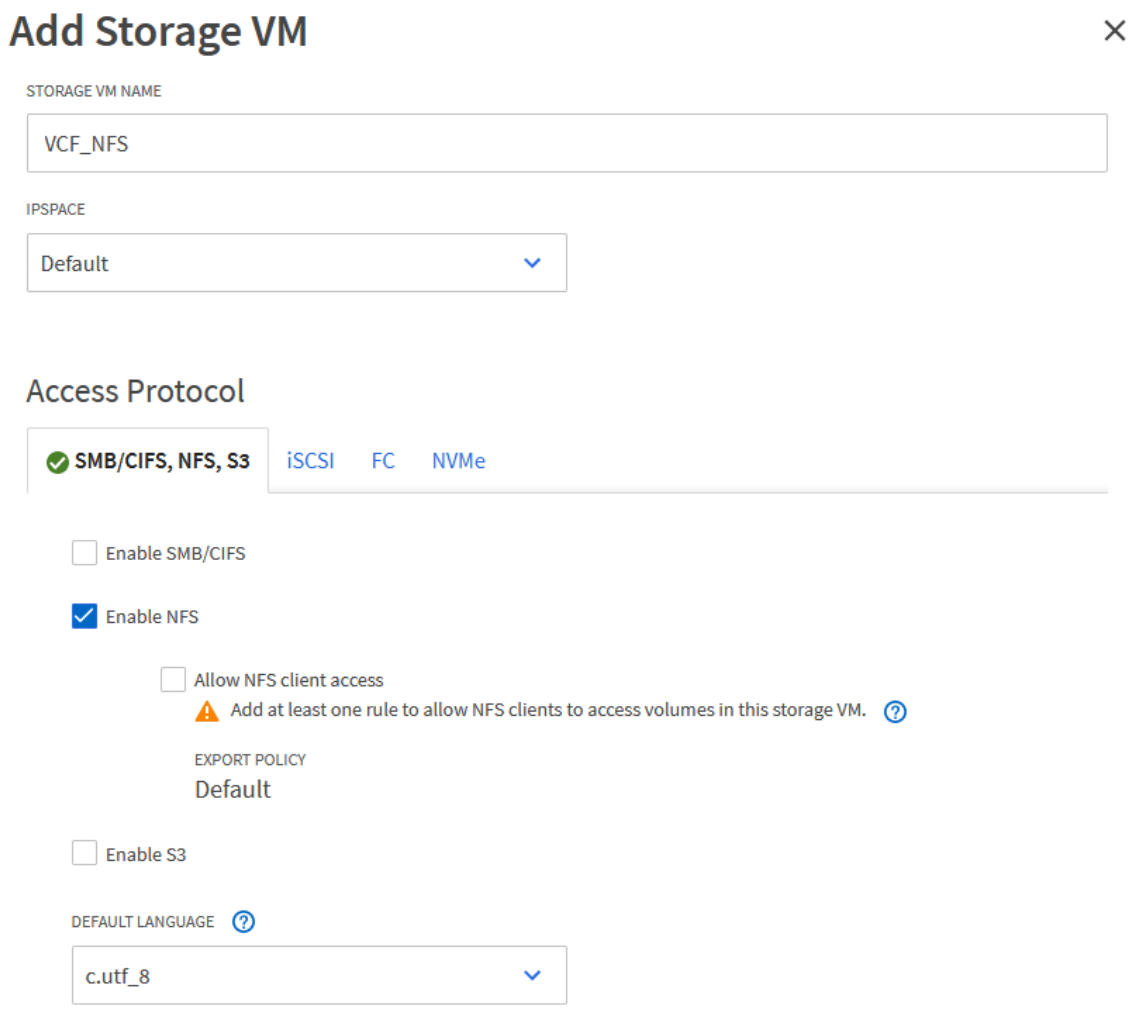
Crie a VM de armazenamento e os LIFs

Conclua as etapas a seguir para criar um SVM junto com vários LIFs para tráfego NFS.

1. No ONTAP System Manager, navegue até **VMs de armazenamento** no menu à esquerda e clique em **+ Adicionar** para iniciar.

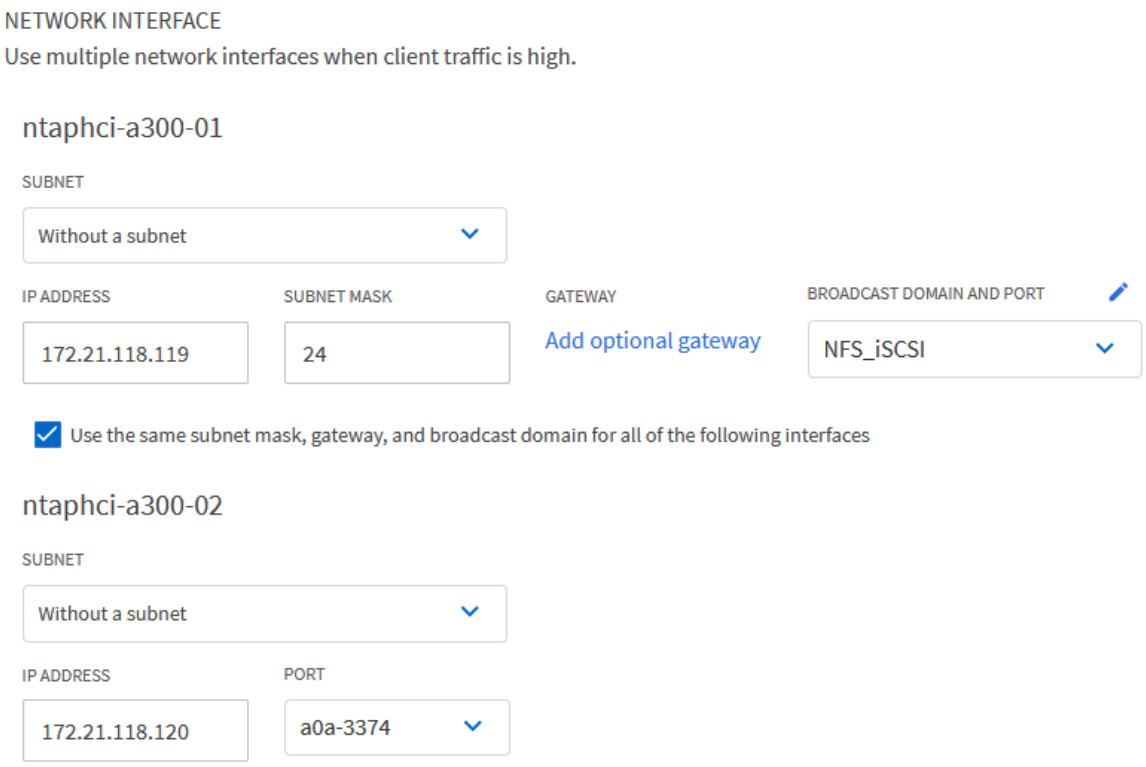


2. No assistente **Adicionar VM de armazenamento**, forneça um **Nome** para a SVM, selecione o **Espaço IP** e, em seguida, em **Protocolo de acesso**, clique na guia **SMB/CIFS, NFS, S3** e marque a caixa para **Habilitar NFS**.

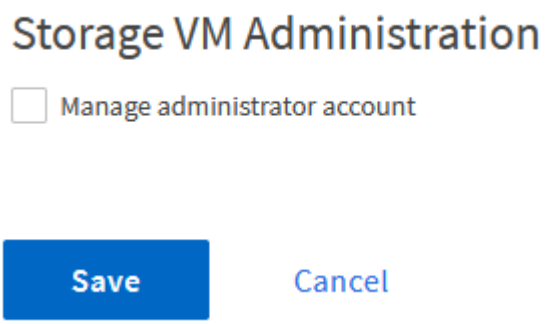


Não é necessário marcar o botão **Permitir acesso do cliente NFS** aqui, pois o Ontap Tools para VMware vSphere será usado para automatizar o processo de implantação do armazenamento de dados. Isso inclui fornecer acesso de cliente para os hosts ESXi.

3. Na seção **Interface de rede**, preencha o **endereço IP**, a **máscara de sub-rede** e o **domínio e porta de transmissão** para o primeiro LIF. Para LIFs subsequentes, a caixa de seleção pode ser marcada para usar configurações comuns em todos os LIFs restantes ou usar configurações separadas.



4. Escolha se deseja habilitar a conta de administração da VM de armazenamento (para ambientes multilocação) e clique em **Salvar** para criar a SVM.



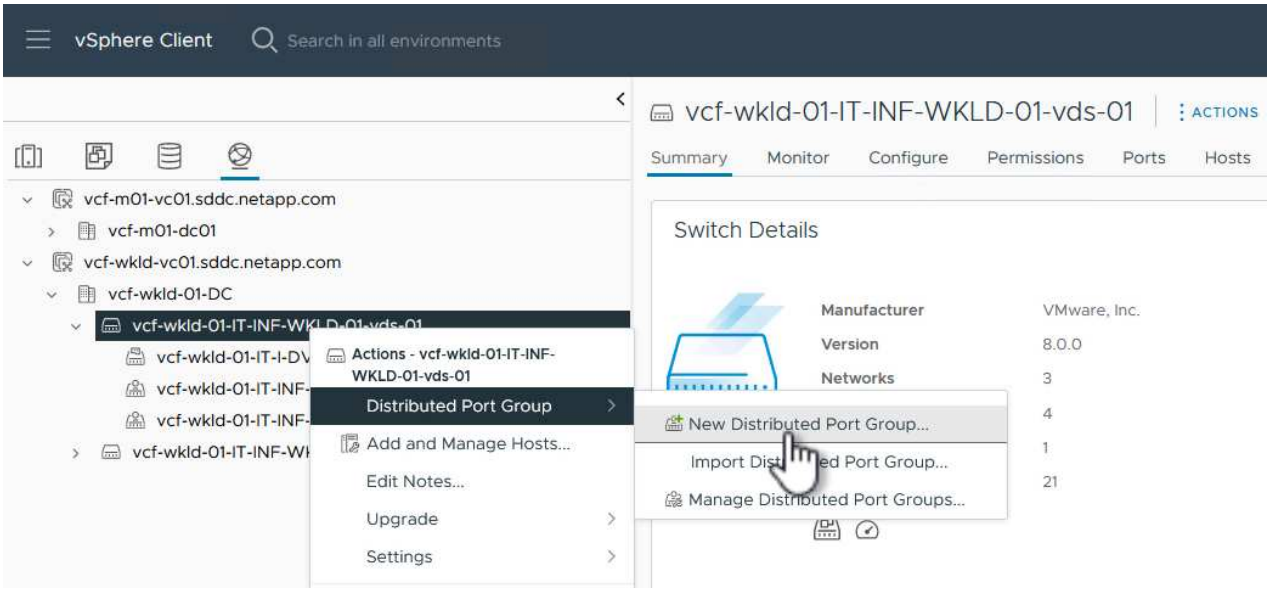
Configurar rede para NFS em hosts ESXi

As etapas a seguir são executadas no cluster do VI Workload Domain usando o cliente vSphere. Neste caso, o vCenter Single Sign-On está sendo usado para que o cliente vSphere seja comum em todos os domínios de gerenciamento e carga de trabalho.

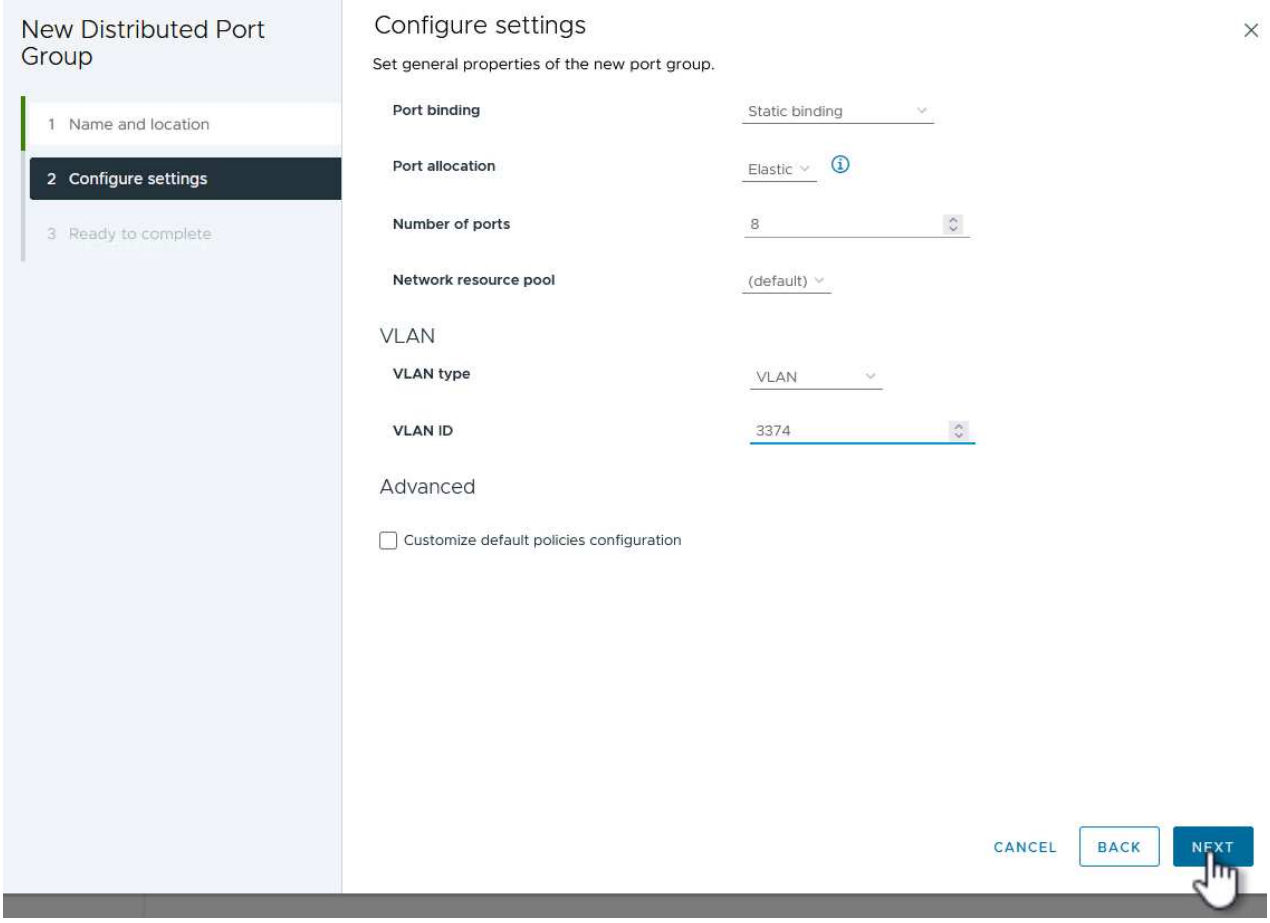
Crie um grupo de portas distribuídas para tráfego NFS

Conclua o seguinte para criar um novo grupo de portas distribuídas para a rede transportar tráfego NFS:

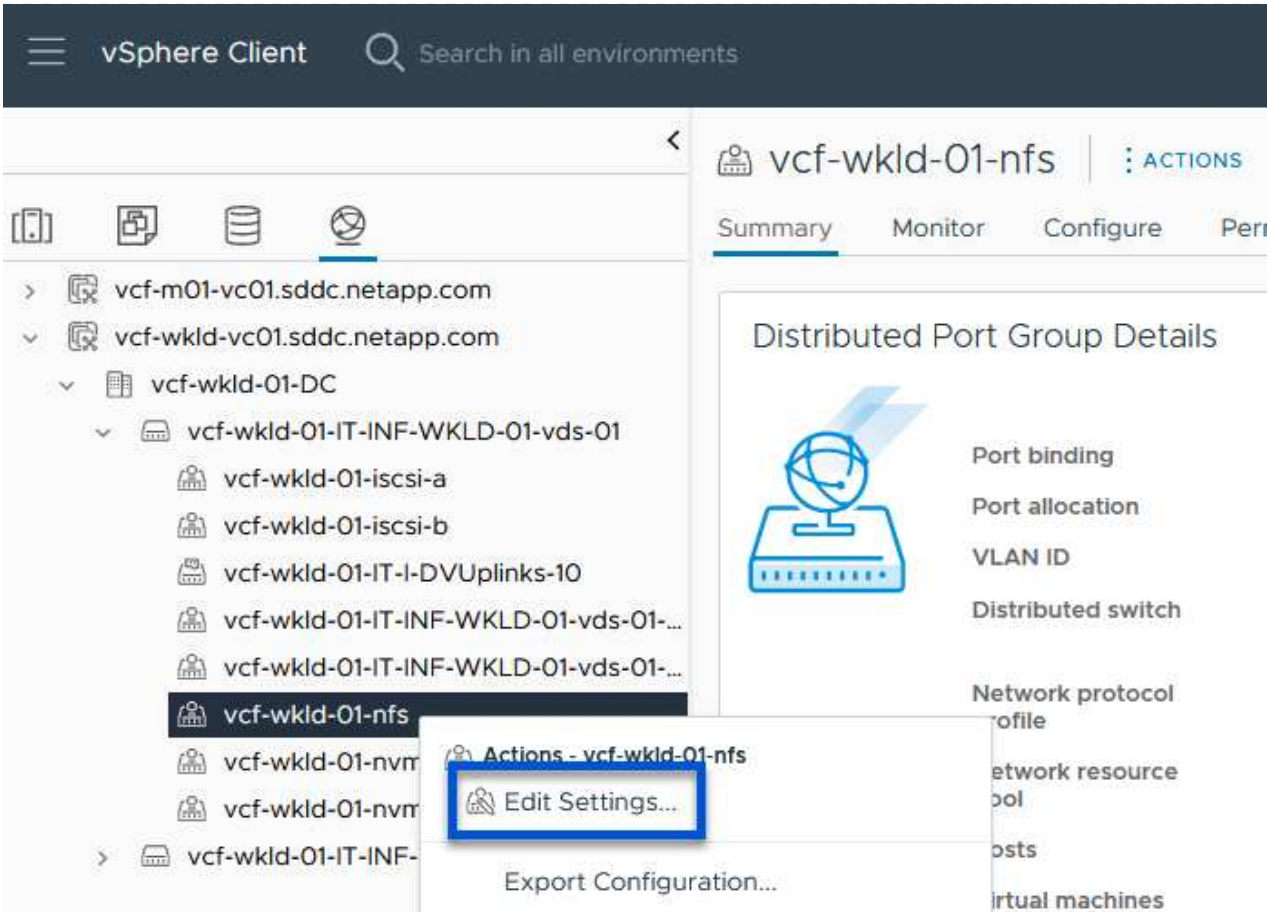
1. No cliente vSphere, navegue até **Inventário > Rede** para o domínio de carga de trabalho. Navegue até o Distributed Switch existente e escolha a ação para criar **Novo Grupo de Portas Distribuídas…** .



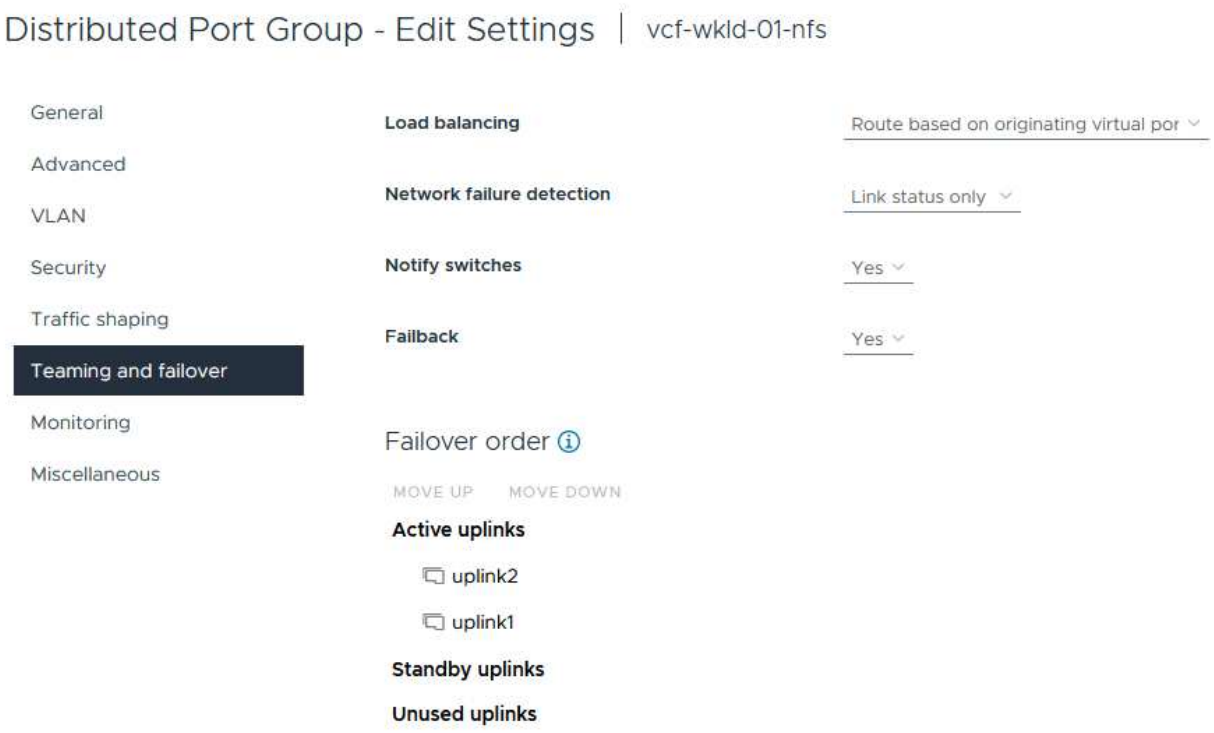
2. No assistente **Novo grupo de portas distribuídas**, preencha um nome para o novo grupo de portas e clique em **Avançar** para continuar.
3. Na página **Configurar configurações** preencha todas as configurações. Se VLANs estiverem sendo usadas, certifique-se de fornecer o ID de VLAN correto. Clique em **Avançar** para continuar.



4. Na página **Pronto para concluir**, revise as alterações e clique em **Concluir** para criar o novo grupo de portas distribuídas.
5. Depois que o grupo de portas for criado, navegue até ele e selecione a ação **Editar configurações…**.



6. Na página **Grupo de portas distribuídas - Editar configurações**, navegue até **Agrupamento e failover** no menu à esquerda. Habilite o agrupamento para que os Uplinks sejam usados para tráfego NFS, garantindo que eles estejam juntos na área **Uplinks ativos**. Mova todos os uplinks não utilizados para **Uplinks não utilizados**.

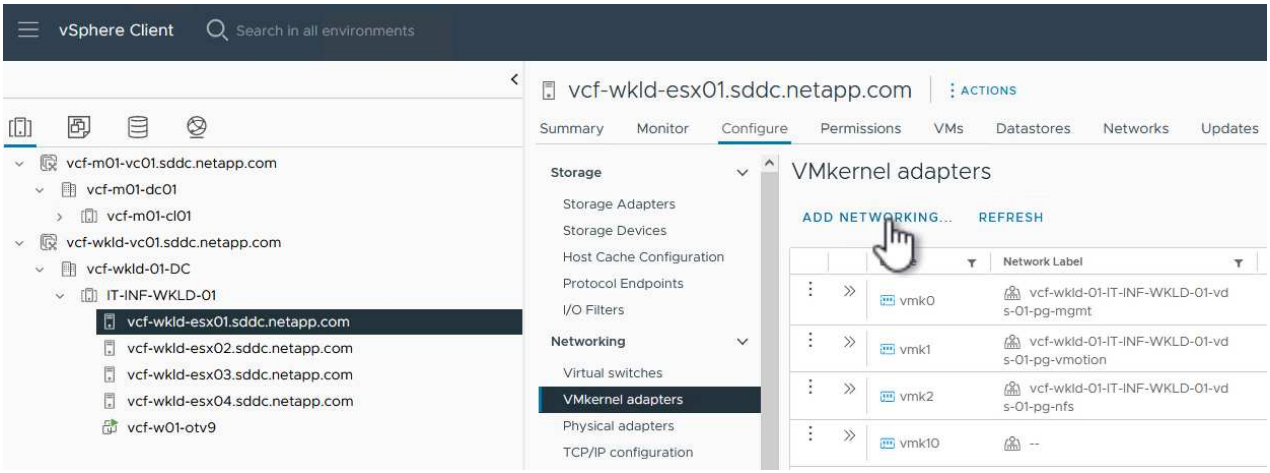


7. Repita esse processo para cada host ESXi no cluster.

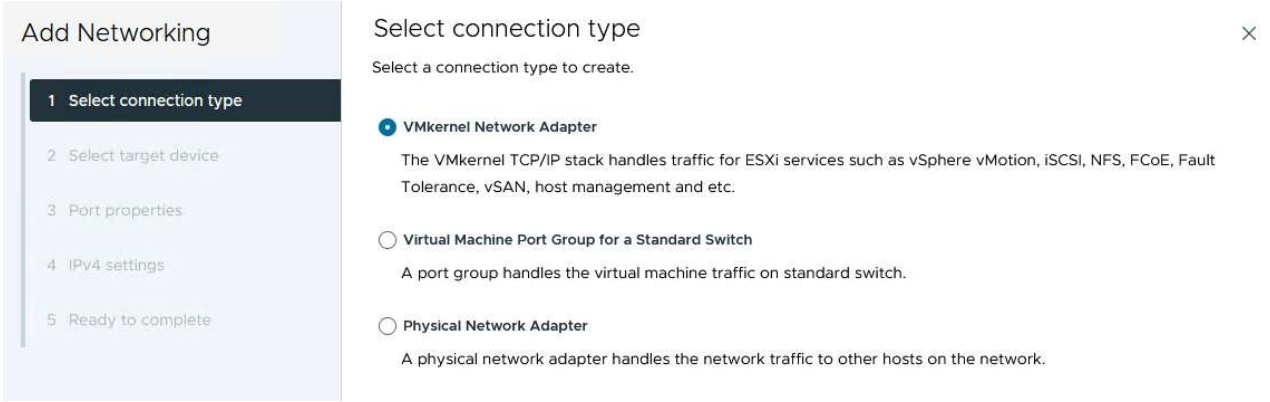
Crie um adaptador VMkernel em cada host ESXi

Repita esse processo em cada host ESXi no domínio de carga de trabalho.

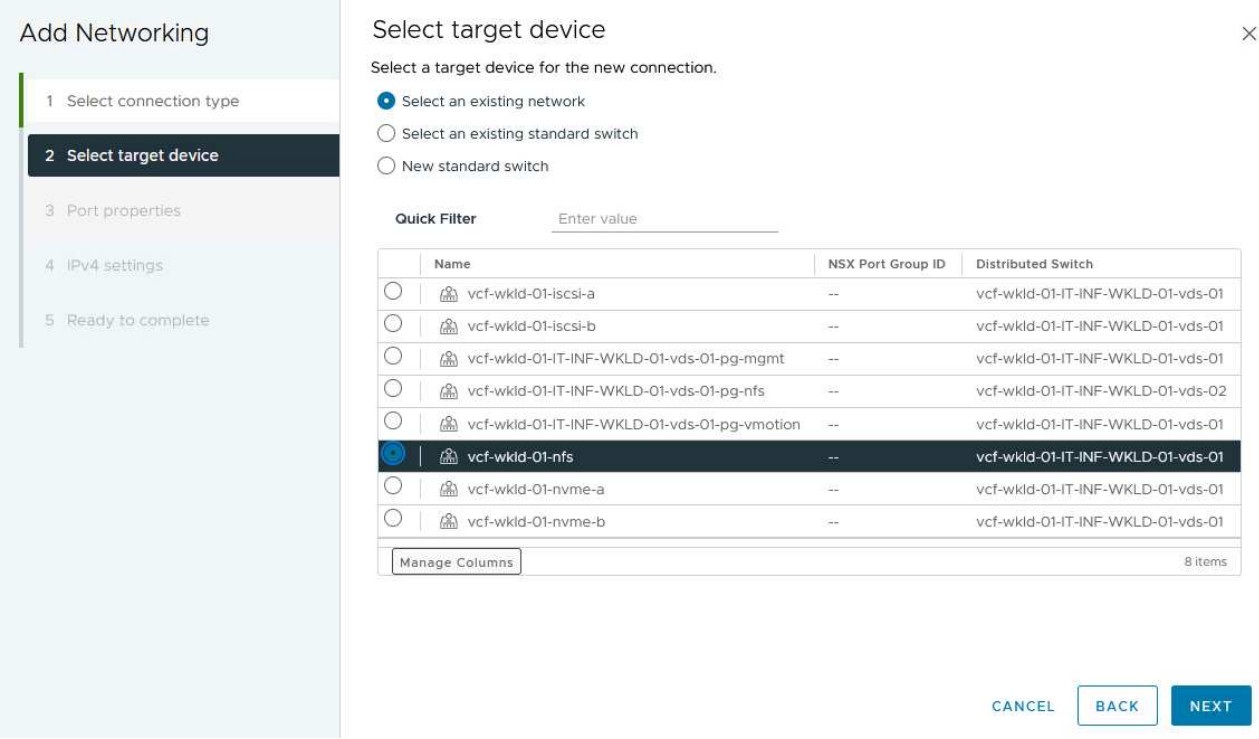
1. No cliente vSphere, navegue até um dos hosts ESXi no inventário do domínio de carga de trabalho. Na aba **Configurar** selecione **Adaptadores VMkernel** e clique em **Adicionar Rede…** para iniciar.



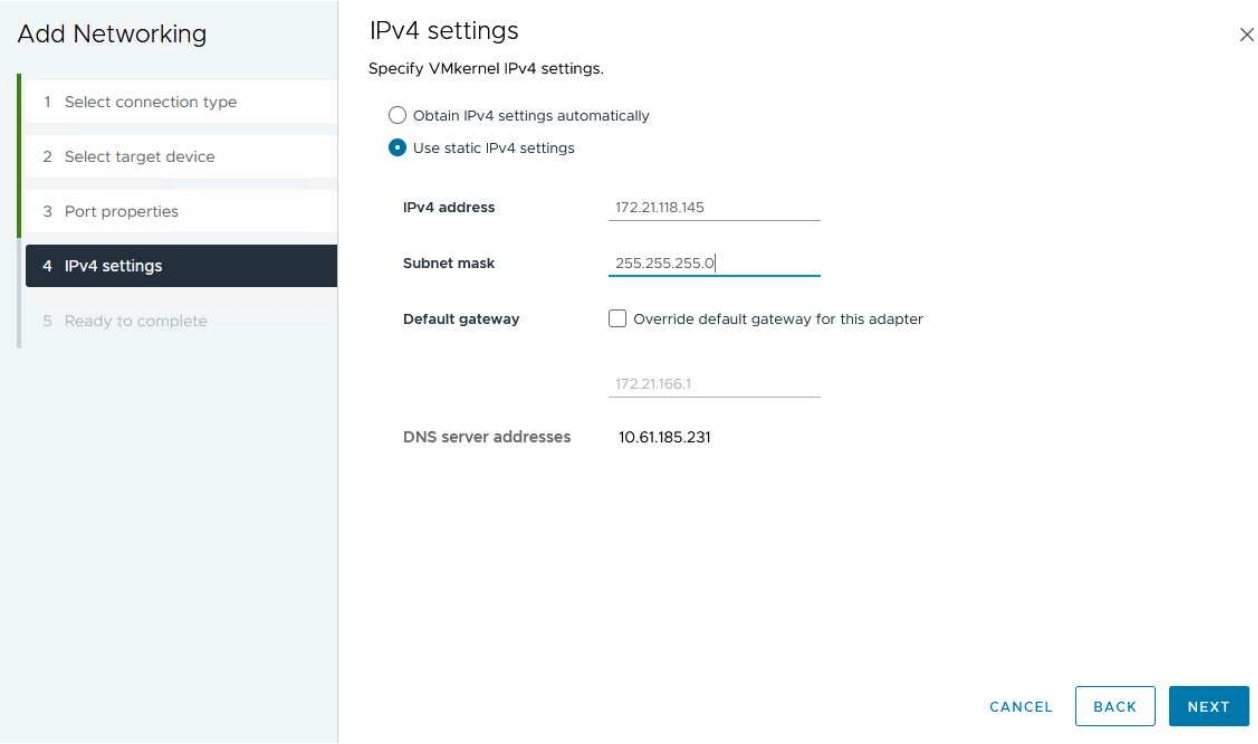
2. Na janela **Selecionar tipo de conexão**, escolha **Adaptador de rede VMkernel** e clique em **Avançar** para continuar.



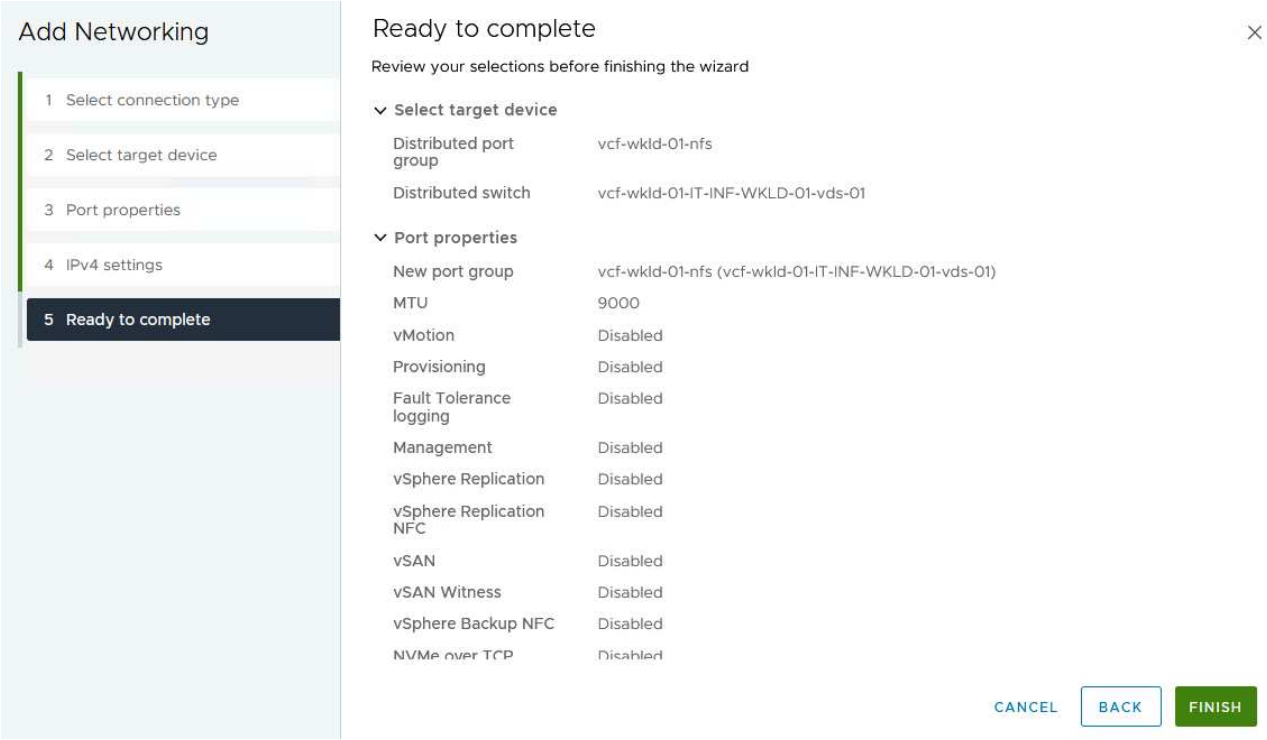
3. Na página **Selecionar dispositivo de destino**, escolha um dos grupos de portas distribuídas para NFS que foi criado anteriormente.



4. Na página **Propriedades da porta**, mantenha os padrões (sem serviços habilitados) e clique em **Avançar** para continuar.
5. Na página **Configurações IPv4**, preencha o **endereço IP**, a **máscara de sub-rede** e forneça um novo endereço IP do gateway (somente se necessário). Clique em **Avançar** para continuar.



6. Revise suas seleções na página **Pronto para concluir** e clique em **Concluir** para criar o adaptador VMkernel.



Implantar e usar ferramentas ONTAP para configurar o armazenamento

As etapas a seguir são executadas no cluster de domínio de gerenciamento do VCF usando o cliente vSphere e envolvem a implantação do OTV, a criação de um armazenamento de dados NFS do vVols e a migração de VMs de gerenciamento para o novo armazenamento de dados.

Para domínios de carga de trabalho do VI, o OTV é instalado no VCF Management Cluster, mas registrado no vCenter associado ao domínio de carga de trabalho do VI.

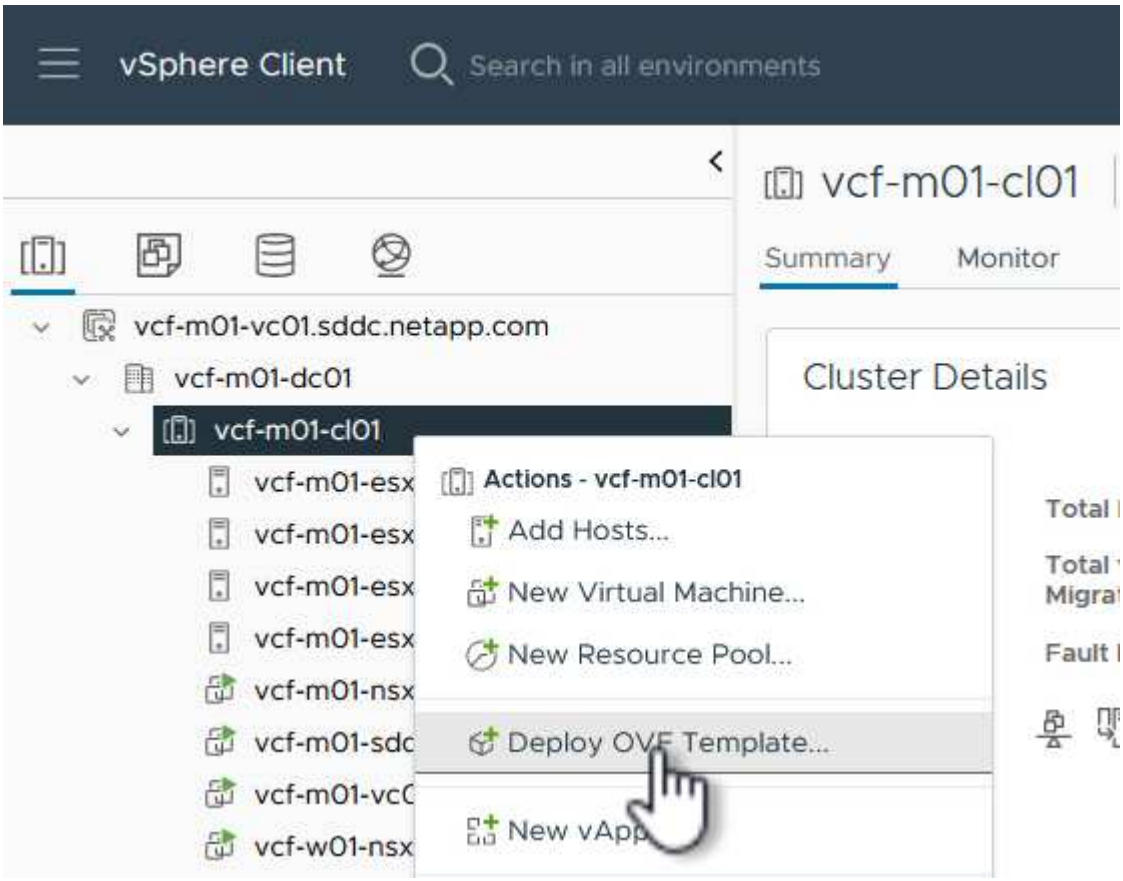
Para obter informações adicionais sobre a implantação e o uso do ONTAP Tools em um ambiente vCenter múltiplo, consulte"Requisitos para registrar ferramentas ONTAP em vários ambientes vCenter Servers" .

Implantar ONTAP tools for VMware vSphere

As ONTAP tools for VMware vSphere (OTV) são implantadas como um dispositivo de VM e fornecem uma interface de usuário do vCenter integrada para gerenciar o armazenamento ONTAP .

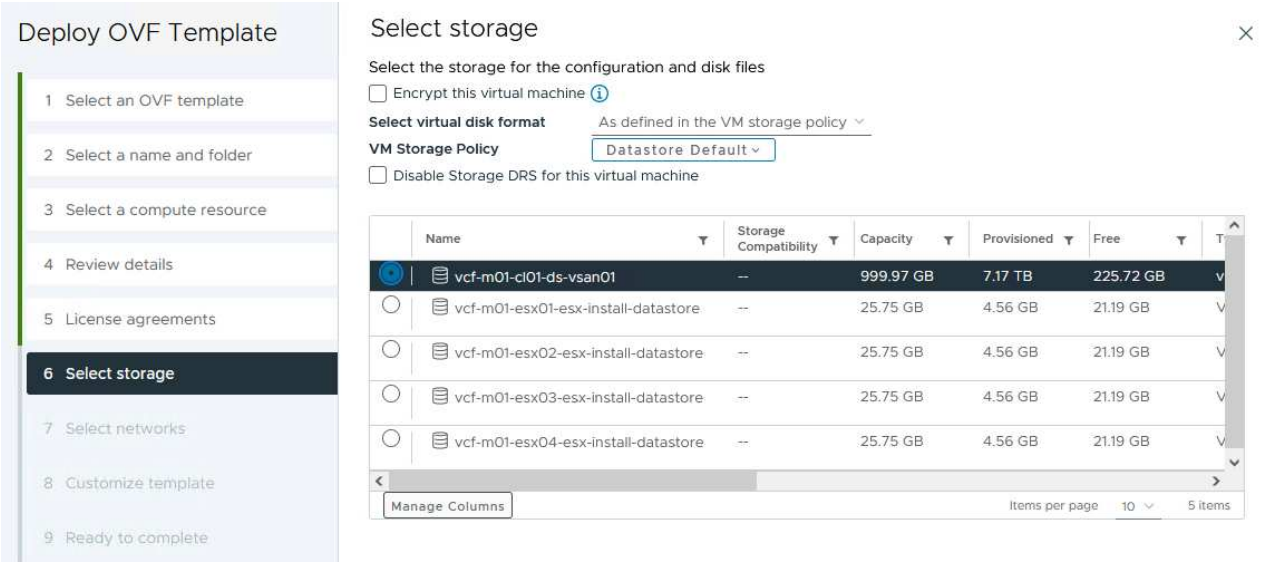
Conclua o seguinte para implantar ONTAP tools for VMware vSphere:

1. Obtenha a imagem OVA das ferramentas ONTAP do"Site de suporte da NetApp" e baixe para uma pasta local.
2. Efetue login no dispositivo vCenter para o domínio de gerenciamento do VCF.
3. Na interface do dispositivo vCenter, clique com o botão direito do mouse no cluster de gerenciamento e selecione **Implantar modelo OVF…**

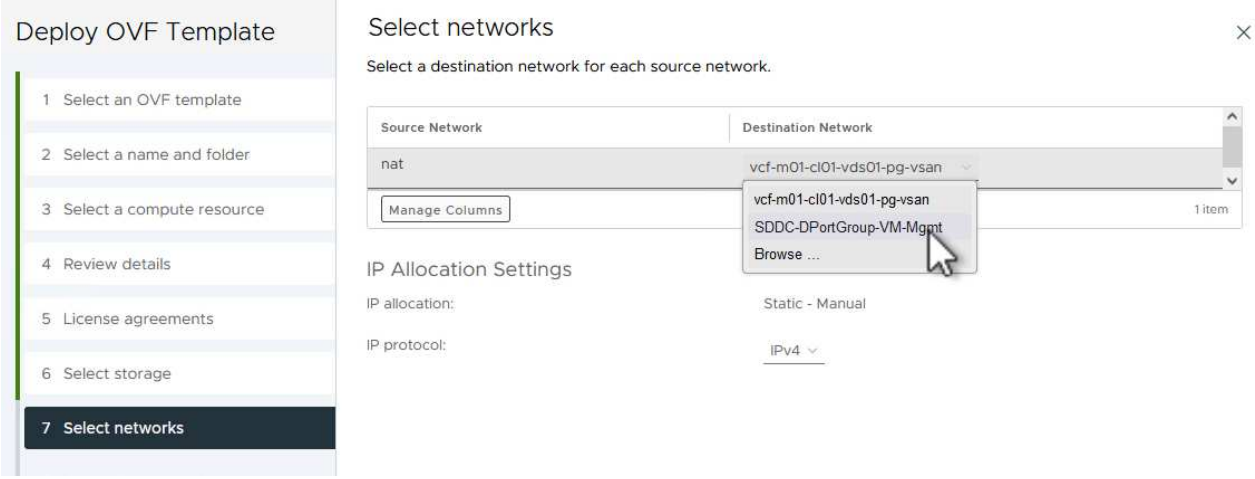


4. No assistente **Implantar modelo OVF**, clique no botão de opção **Arquivo local** e selecione o arquivo OVA das ferramentas ONTAP baixado na etapa anterior.

5. Para as etapas 2 a 5 do assistente, selecione um nome e uma pasta para a VM, selecione o recurso de computação, revise os detalhes e aceite o contrato de licença.
6. Para o local de armazenamento dos arquivos de configuração e de disco, selecione o armazenamento de dados vSAN do cluster de domínio de gerenciamento do VCF.

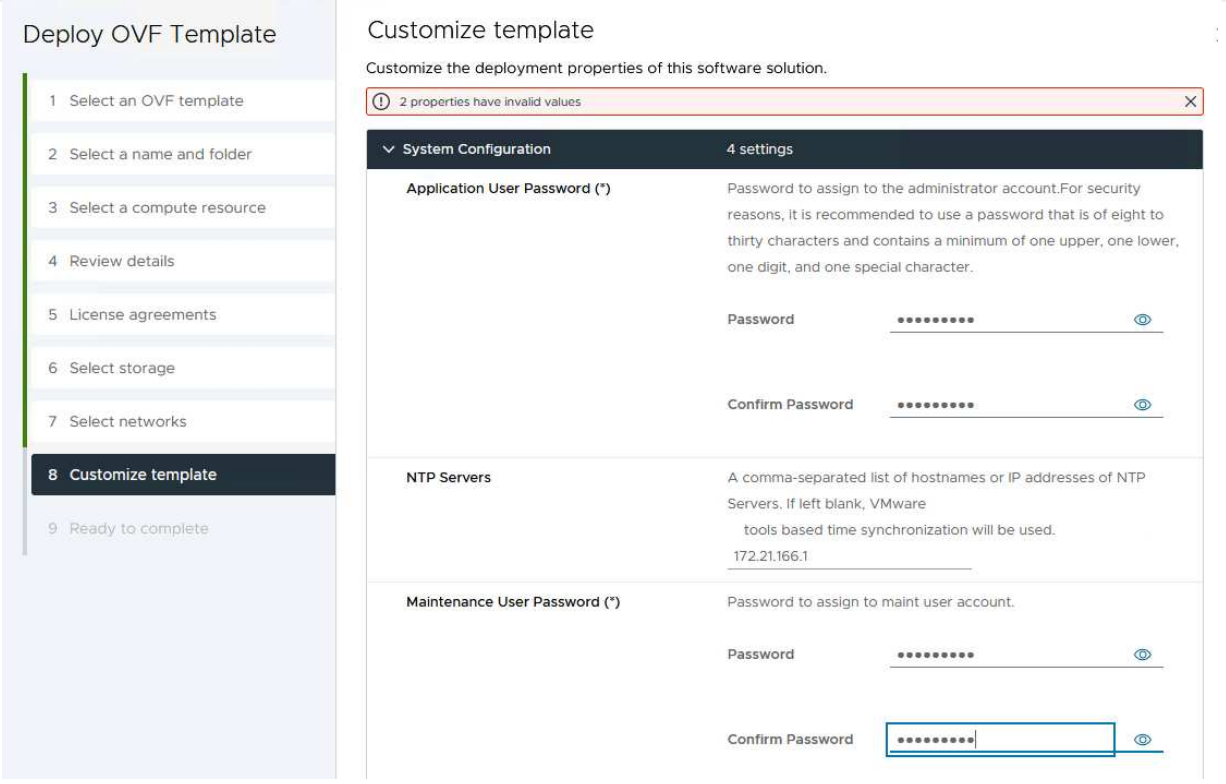


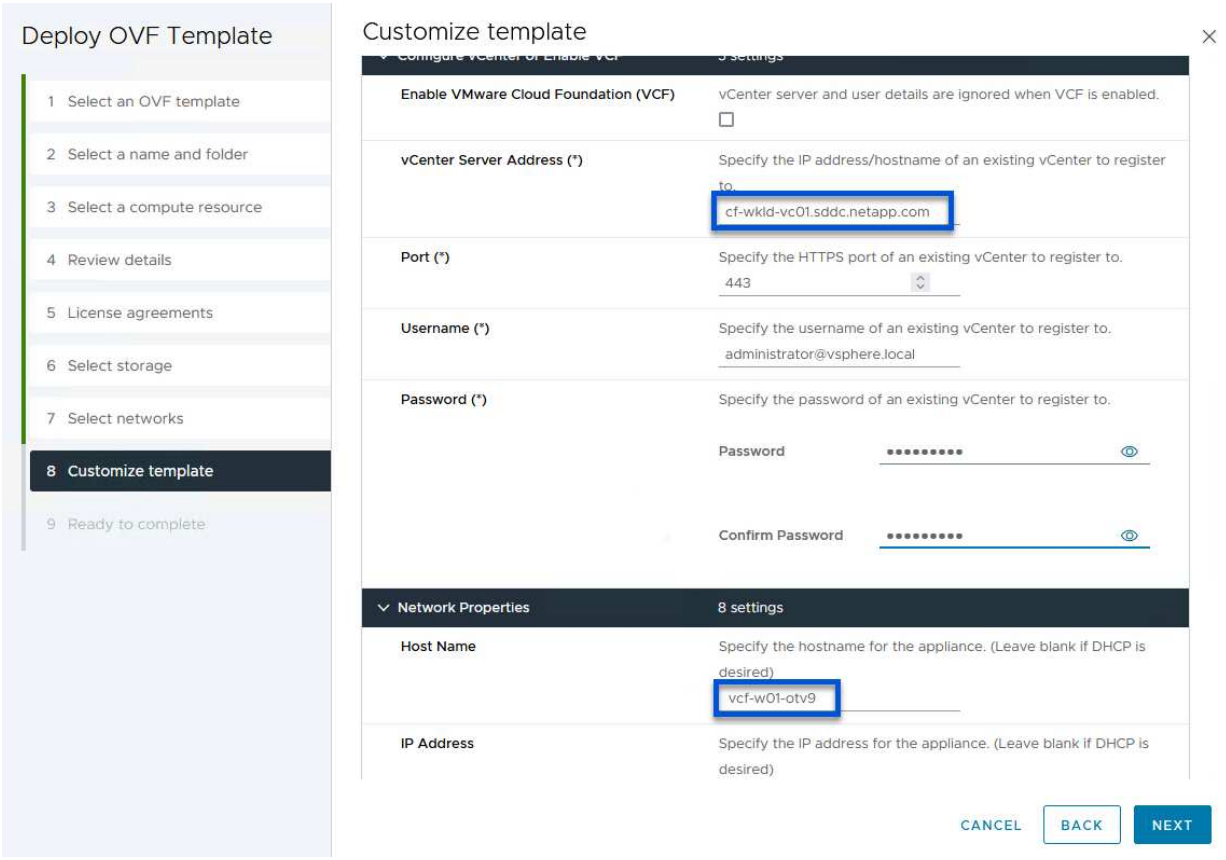
7. Na página Selecionar rede, selecione a rede usada para o tráfego de gerenciamento.



8. Na página Personalizar modelo, preencha todas as informações necessárias:
   - Senha a ser usada para acesso administrativo ao OTV.
   - Endereço IP do servidor NTP.
   - Senha da conta de manutenção do OTV.
   - Senha do banco de dados OTV Derby.
   - Não marque a caixa para **Ativar VMware Cloud Foundation (VCF)**. O modo VCF não é necessário para implantar armazenamento suplementar.
   - FQDN ou endereço IP do dispositivo vCenter para o **Domínio de Carga de Trabalho VI**
   - Credenciais para o dispositivo vCenter do **Domínio de Carga de Trabalho VI**
   - Forneça os campos de propriedades de rede necessários.

     Clique em **Avançar** para continuar.

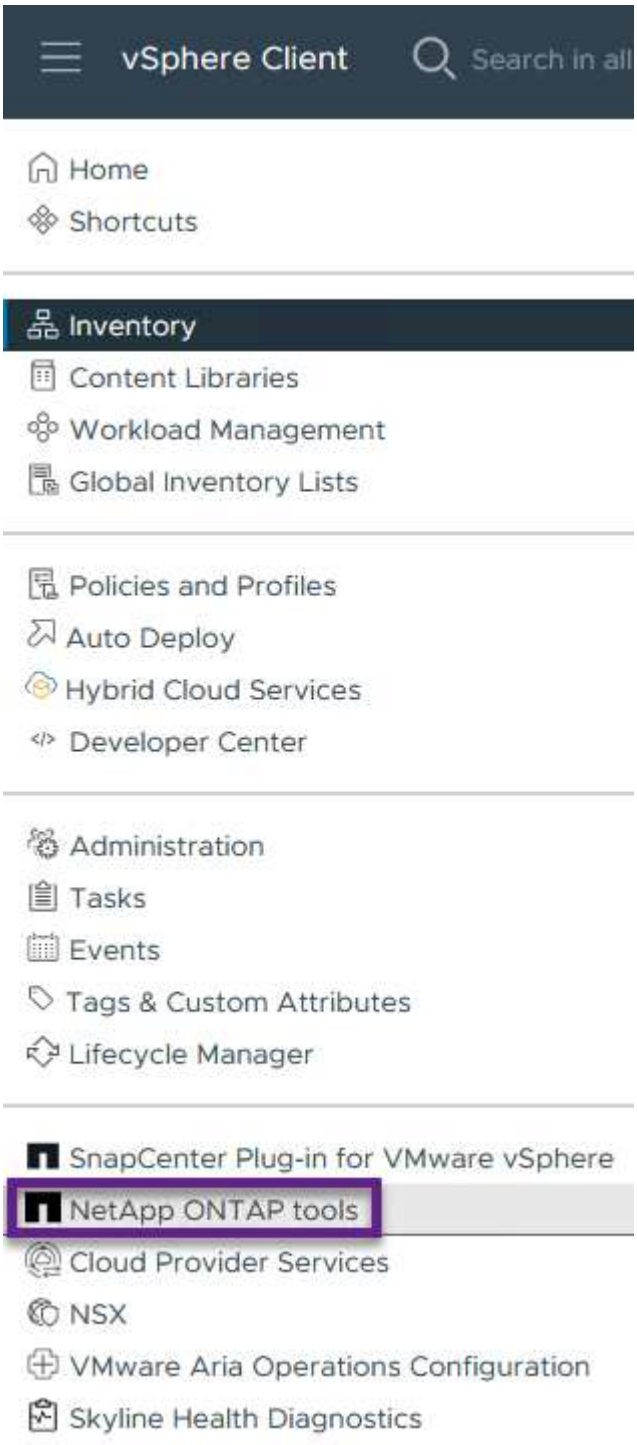




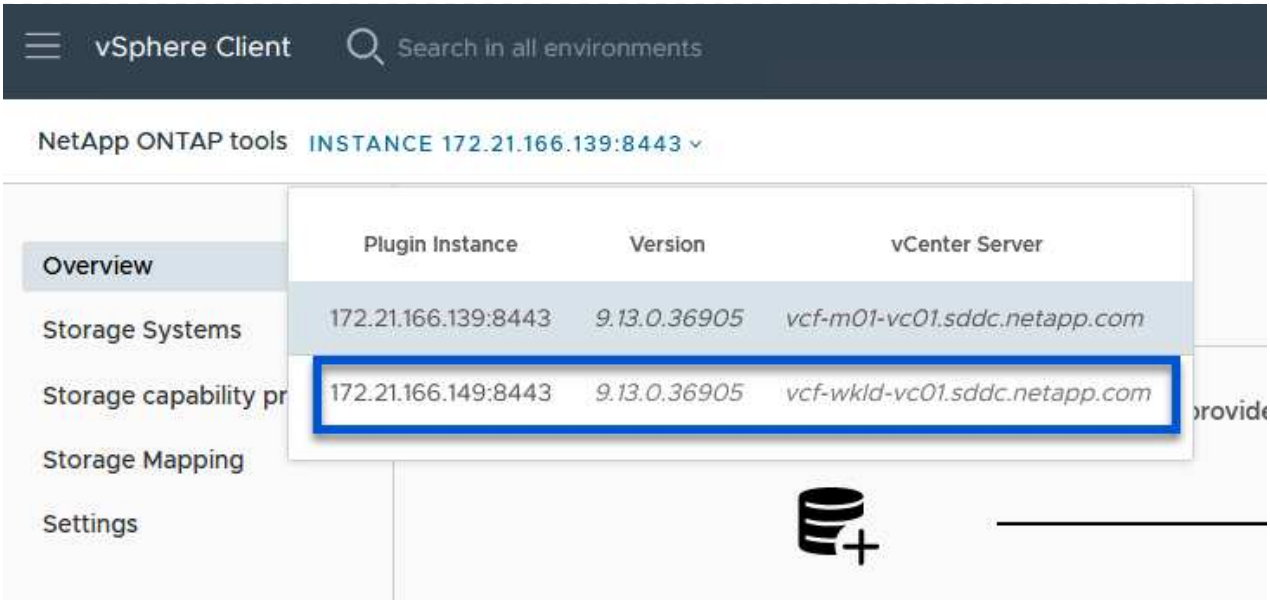
9. Revise todas as informações na página Pronto para concluir e clique em Concluir para começar a implantar o dispositivo OTV.

Adicione um sistema de armazenamento ao ONTAP Tools.

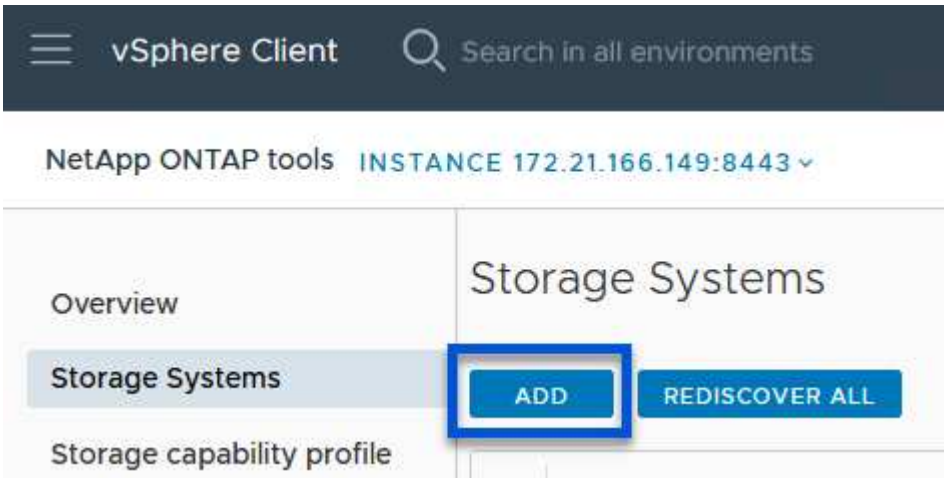
1. Acesse o NetApp ONTAP Tools selecionando-o no menu principal no cliente vSphere.



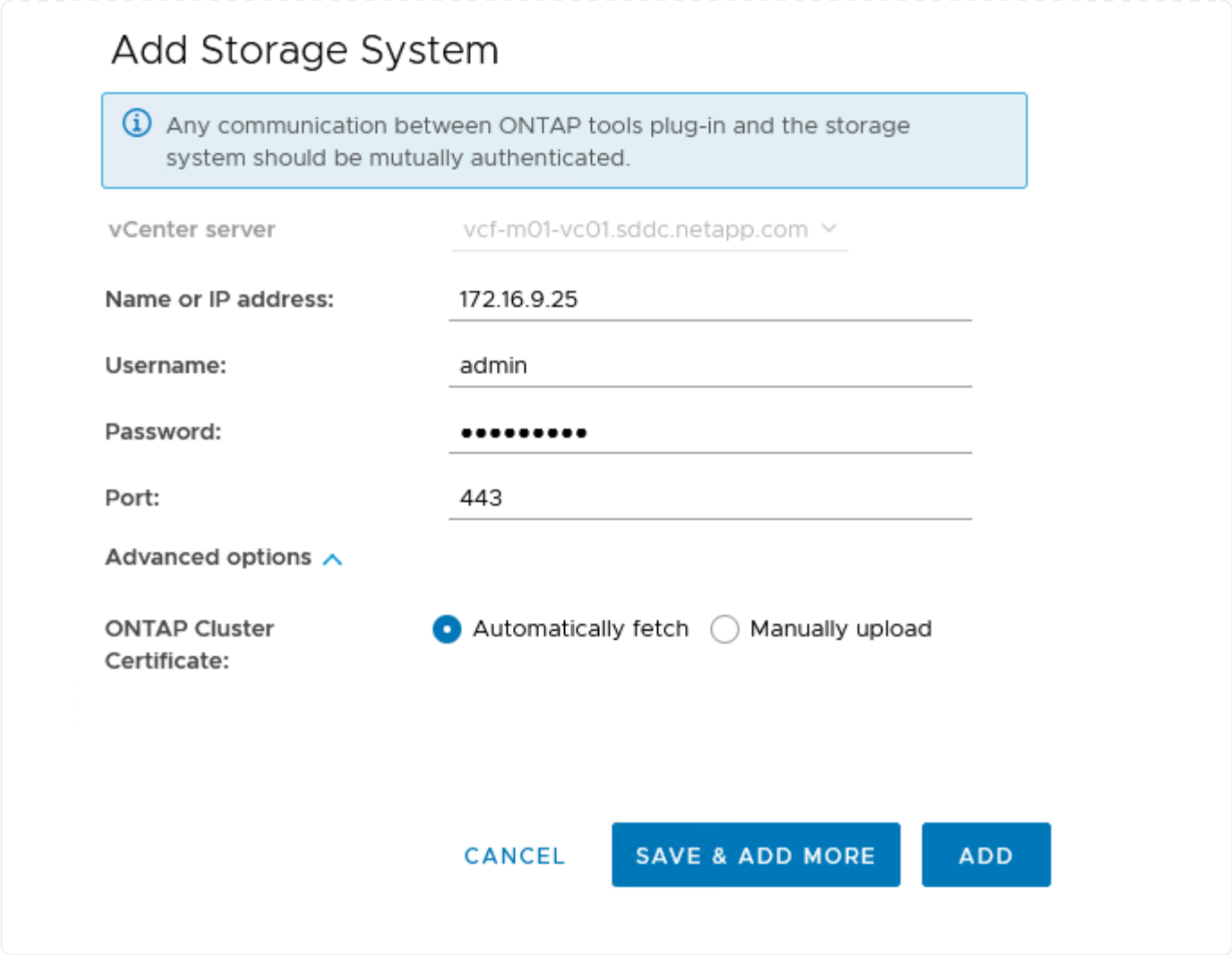
2. No menu suspenso **INSTÂNCIA** na interface da ferramenta ONTAP , selecione a instância do OTV associada ao domínio de carga de trabalho a ser gerenciado.



3. No ONTAP Tools, selecione **Sistemas de armazenamento** no menu à esquerda e pressione **Adicionar**.



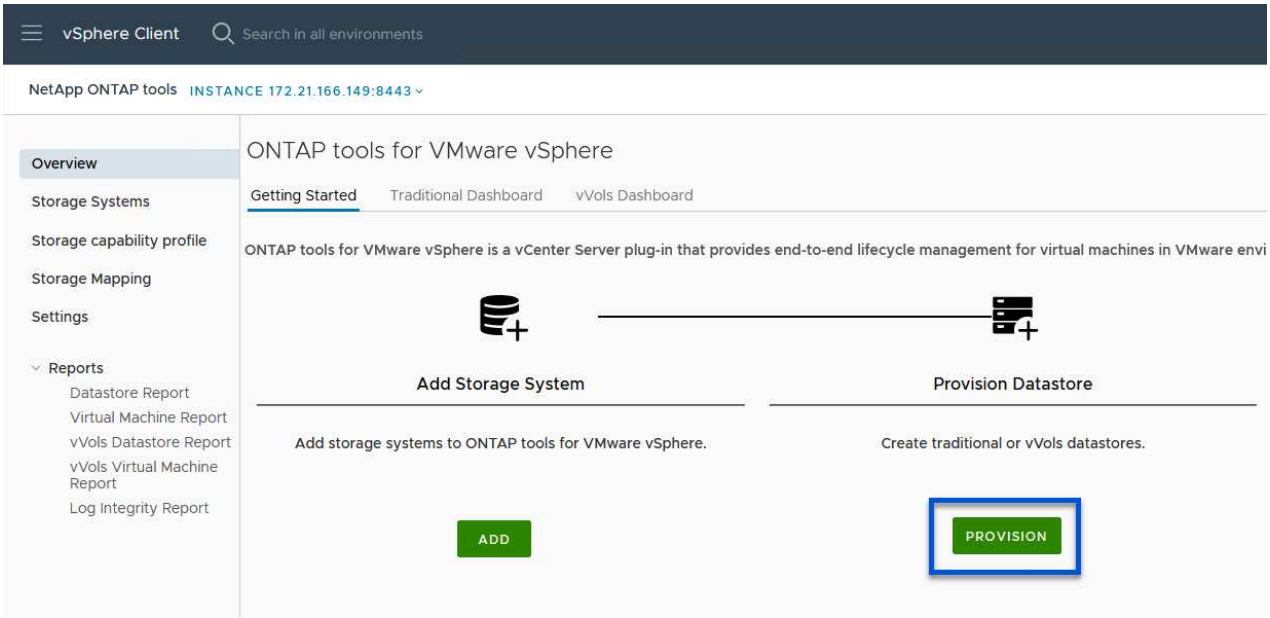
4. Preencha o endereço IP, as credenciais do sistema de armazenamento e o número da porta. Clique em **Adicionar** para iniciar o processo de descoberta.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Crie um armazenamento de dados NFS no ONTAP Tools

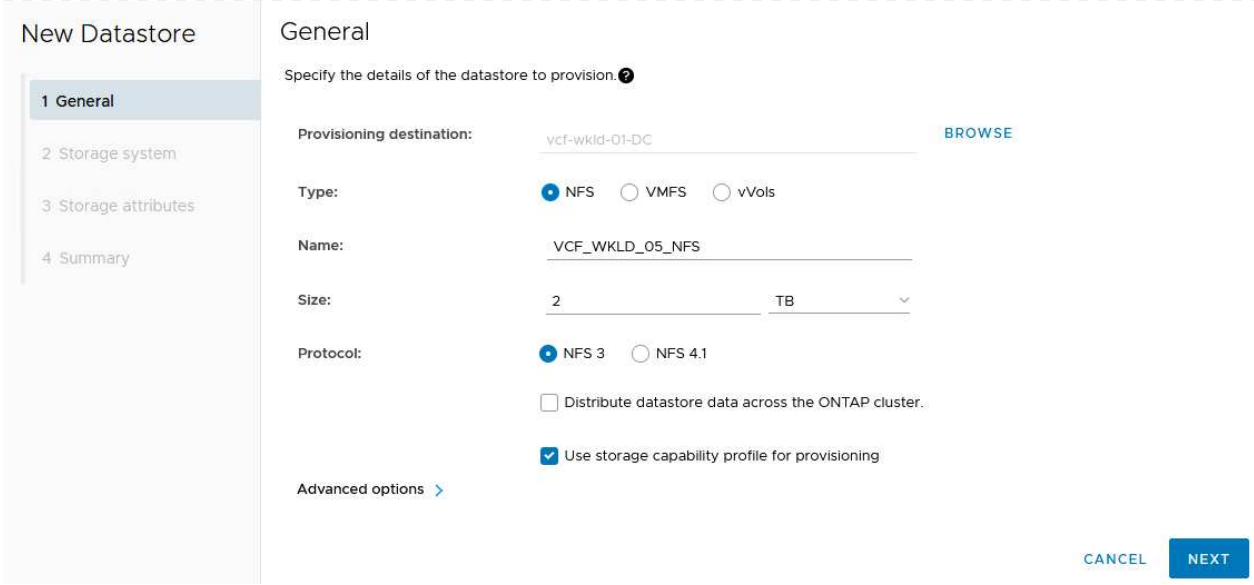
Conclua as etapas a seguir para implantar um armazenamento de dados ONTAP , em execução no NFS, usando o ONTAP Tools.

1. No ONTAP Tools, selecione **Visão geral** e na aba **Introdução** clique em **Provisionamento** para iniciar o assistente.

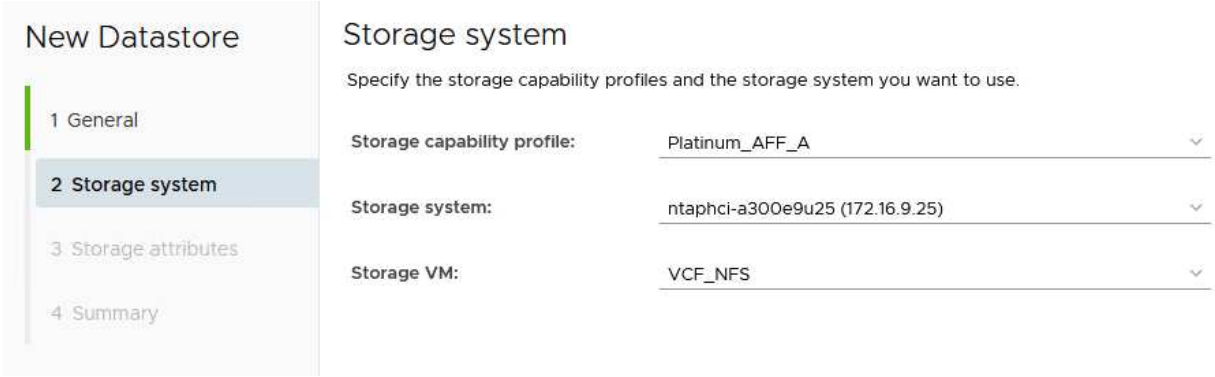


2. Na página **Geral** do assistente Novo armazenamento de dados, selecione o destino do datacenter ou cluster do vSphere. Selecione **NFS** como o tipo de armazenamento de dados, preencha um nome para o armazenamento de dados e selecione o protocolo. Escolha se deseja usar volumes FlexGroup e se deseja usar um arquivo de capacidade de armazenamento para provisionamento. Clique em **Avançar** para continuar.

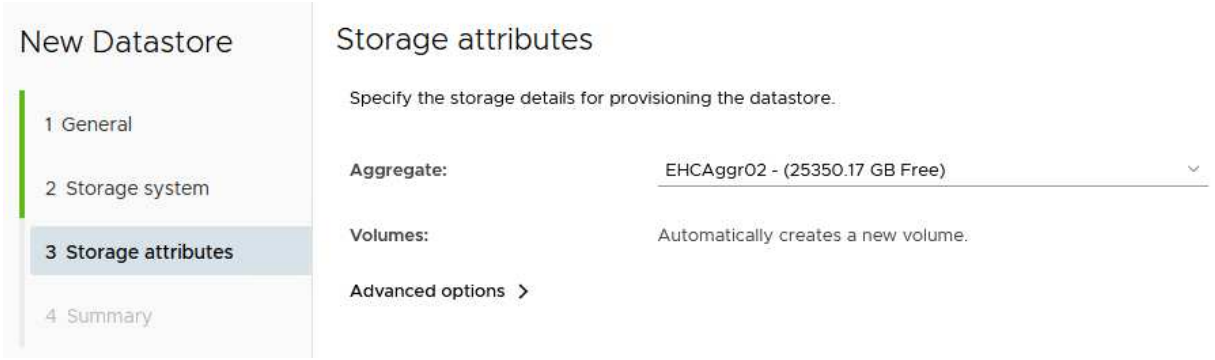
   Observação: selecionar **Distribuir dados do armazenamento de dados pelo cluster** criará o volume subjacente como um volume FlexGroup , o que impede o uso de Perfis de Capacidade de Armazenamento. Consulte "Configurações suportadas e não suportadas para volumes FlexGroup" para obter mais informações sobre o uso dos volumes FlexGroup .



3. Na página **Sistema de armazenamento**, selecione um perfil de capacidade de armazenamento, o sistema de armazenamento e o SVM. Clique em **Avançar** para continuar.

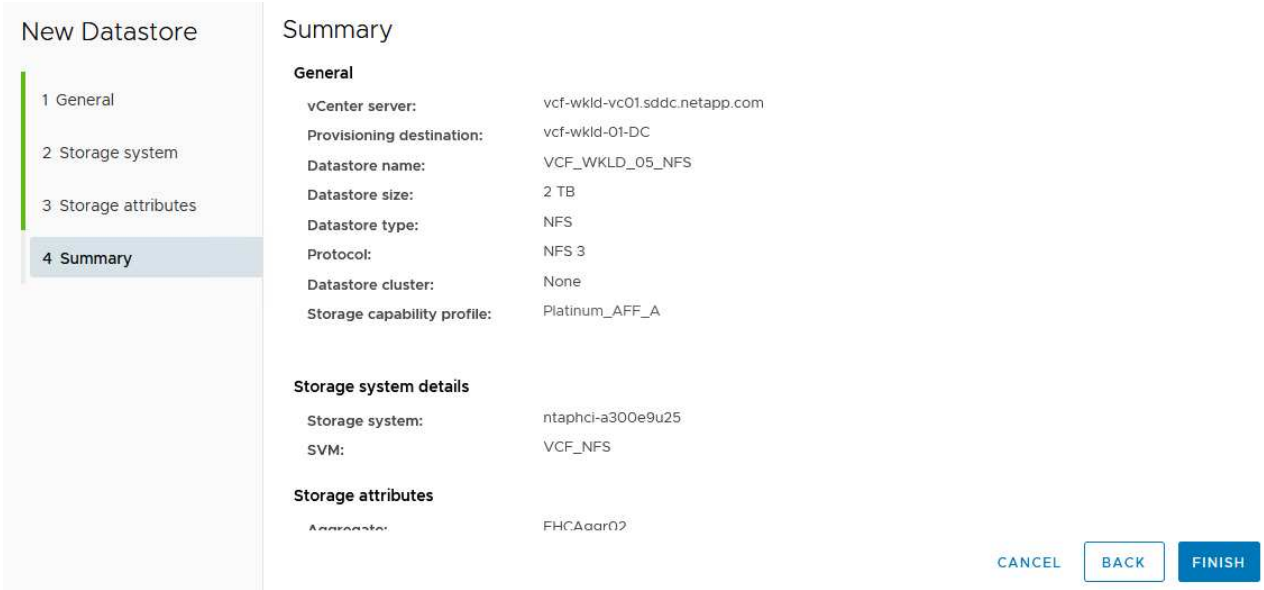


4. Na página **Atributos de armazenamento**, selecione o agregado a ser usado e clique em **Avançar** para continuar.



5. Por fim, revise o **Resumo** e clique em Concluir para começar a criar o armazenamento de dados

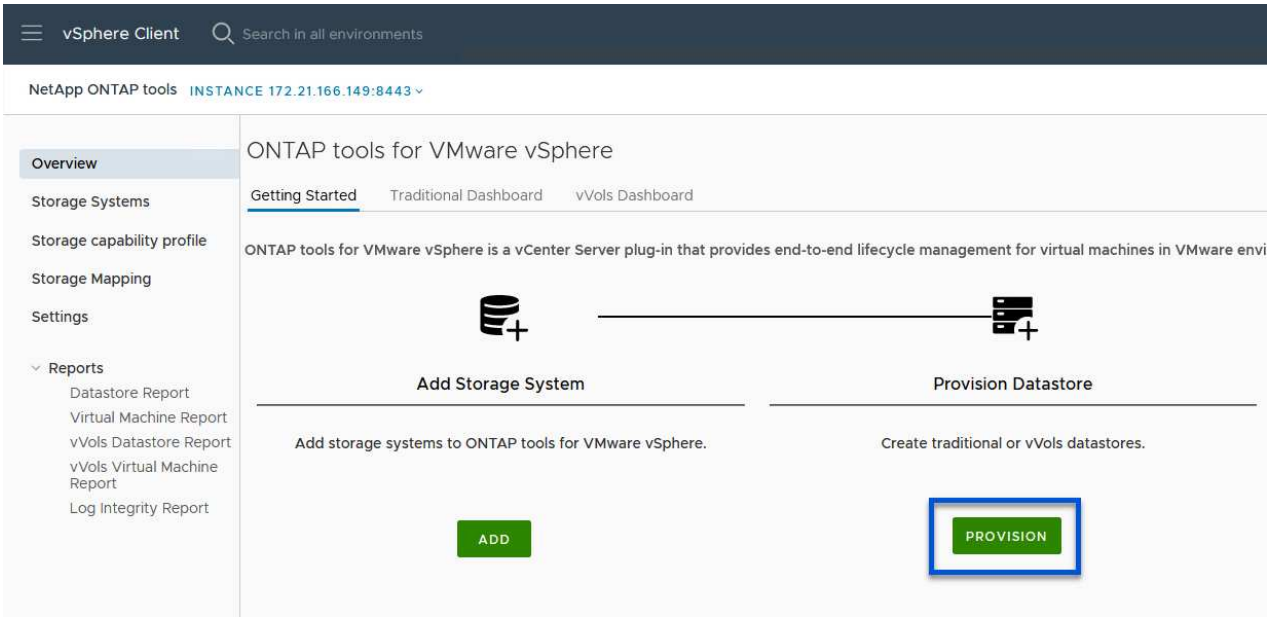
NFS.


New Datastore
1 General
2 Storage system
3 Storage attributes
4 Summary
Summary
General
vCenter server: vcf-wkld-vc01.sddc.netapp.com
Provisioning destination: vcf-wkld-01-DC
Datastore name: VCF_WKLD_05_NFS
Datastore size: 2 TB
Datastore type: NFS
Protocol: NFS 3
Datastore cluster: None
Storage capability profile: Platinum_AFF_A
Storage system details
Storage system: ntaphci-a300e9u25
SVM: VCF_NFS
Storage attributes
CANCEL
BACK
FINISH

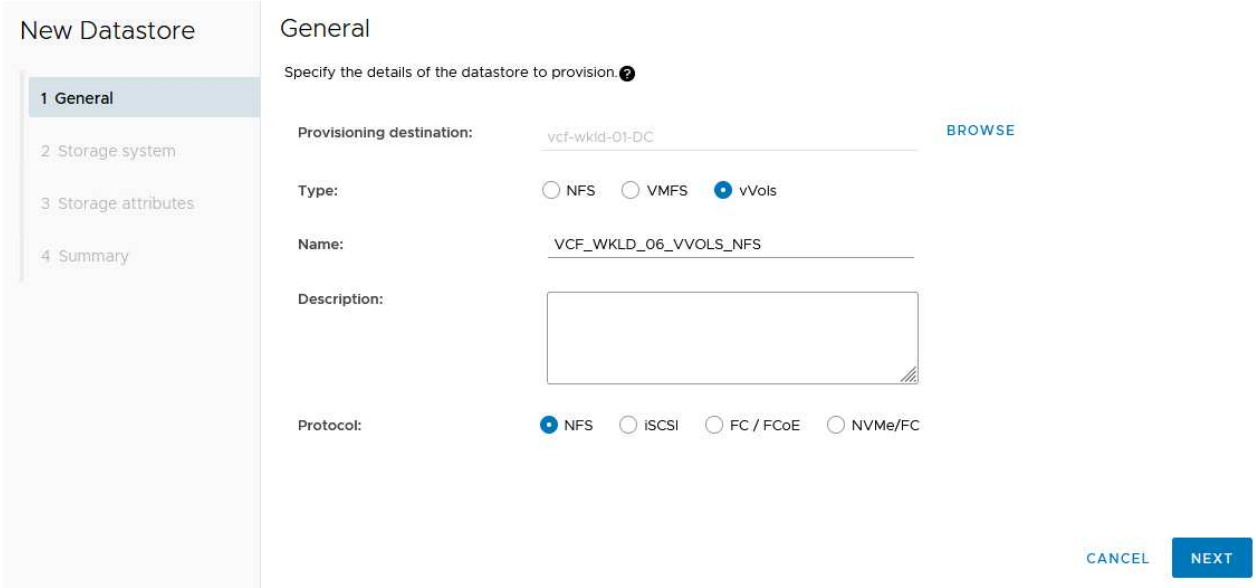
Crie um armazenamento de dados vVols no ONTAP Tools

Para criar um armazenamento de dados vVols no ONTAP Tools, conclua as seguintes etapas:

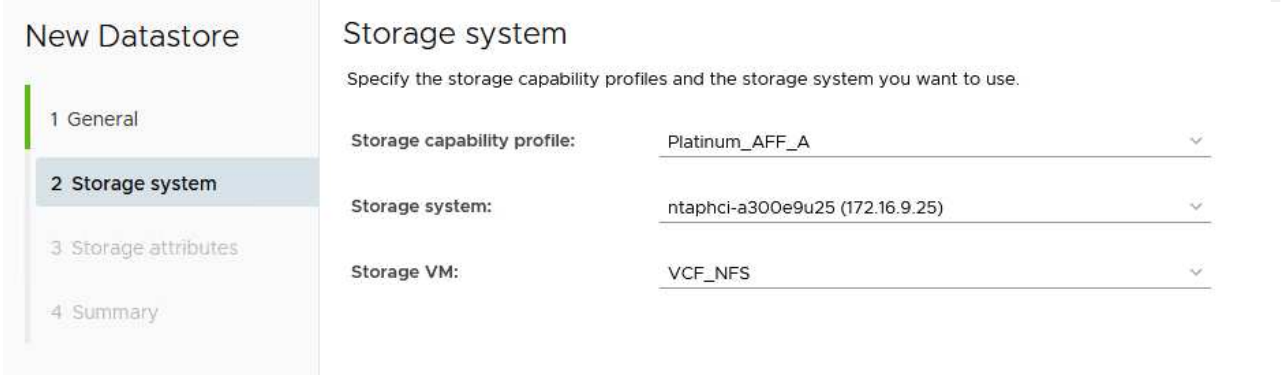
1. No ONTAP Tools, selecione **Visão geral** e na aba **Introdução** clique em **Provisionamento** para iniciar o assistente.



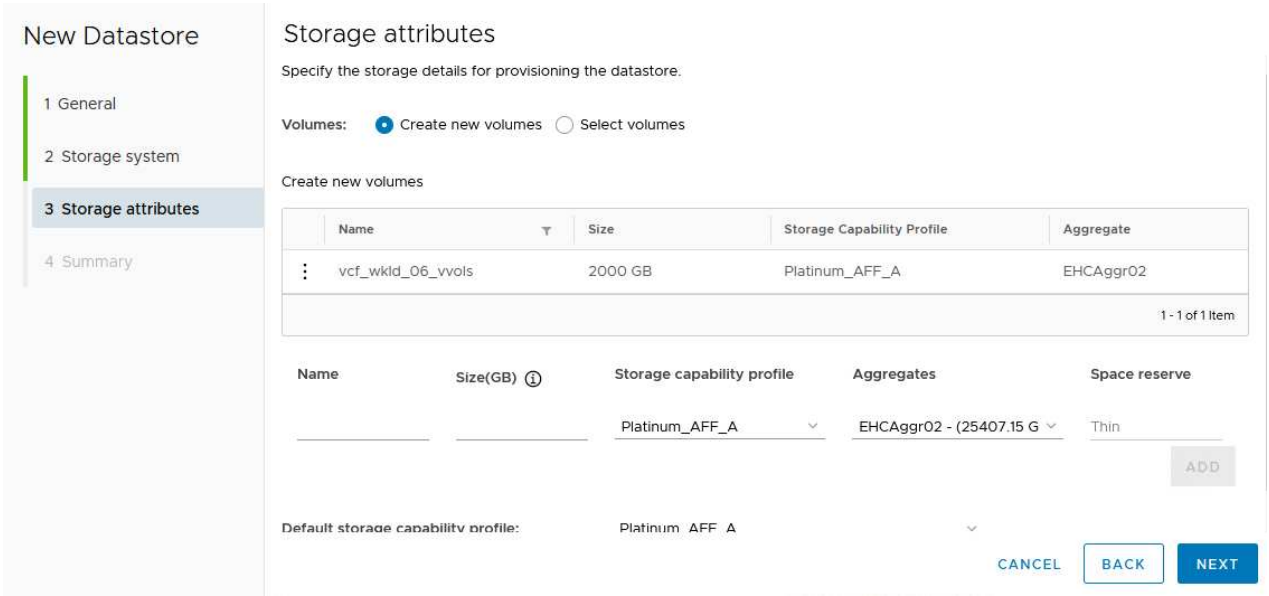
2. Na página **Geral** do assistente Novo armazenamento de dados, selecione o destino do datacenter ou cluster do vSphere. Selecione * vVols* como o tipo de armazenamento de dados, preencha um nome para o armazenamento de dados e selecione **NFS** como o protocolo. Clique em **Avançar** para continuar.



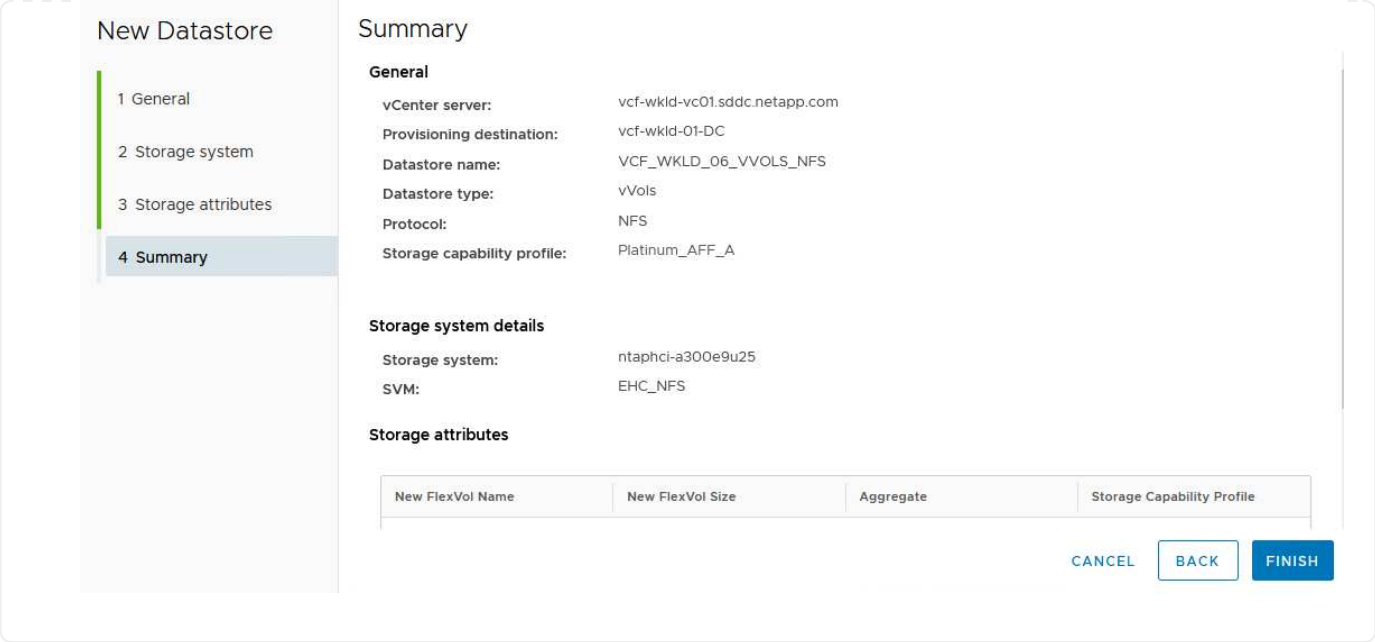
3. Na página **Sistema de armazenamento**, selecione um perfil de capacidade de armazenamento, o sistema de armazenamento e o SVM. Clique em **Avançar** para continuar.



4. Na página **Atributos de armazenamento**, selecione para criar um novo volume para o armazenamento de dados e preencha os atributos de armazenamento do volume a ser criado. Clique em **Adicionar** para criar o volume e depois em **Avançar** para continuar.



5. Por fim, revise o **Resumo** e clique em **Concluir** para iniciar o processo de criação do armazenamento de dados vVol.



Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Adicionar NVMe sobre TCP como armazenamento suplementar aos domínios de carga de trabalho do VI

Neste caso de uso, descrevemos o procedimento para usar o ONTAP Tools for VMware para configurar o NVMe sobre TCP (NVMe/TCP) como armazenamento suplementar para um domínio de carga de trabalho de infraestrutura virtual (VI) do VMware Cloud Foundation (VCF). Este procedimento resume a configuração de uma Máquina Virtual de Armazenamento (SVM) habilitada para NVMe/TCP, a criação de namespaces NVMe, a configuração de rede do host ESXi e a implantação de um armazenamento de dados VMFS.

Benefícios do NVMe sobre TCP

Alto desempenho: Oferece desempenho excepcional com baixa latência e altas taxas de transferência de dados. Isso é crucial para aplicativos exigentes e operações de dados em larga escala.

Escalabilidade: Suporta configurações escaláveis, permitindo que os administradores de TI expandam sua infraestrutura perfeitamente conforme os requisitos de dados aumentam.

Custo-benefício: Funciona em switches Ethernet padrão e é encapsulado dentro de datagramas TCP. Não é necessário equipamento especial para implementar.

Para obter mais informações sobre os benefícios do NVMe, consulte "O que é NVME?"

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

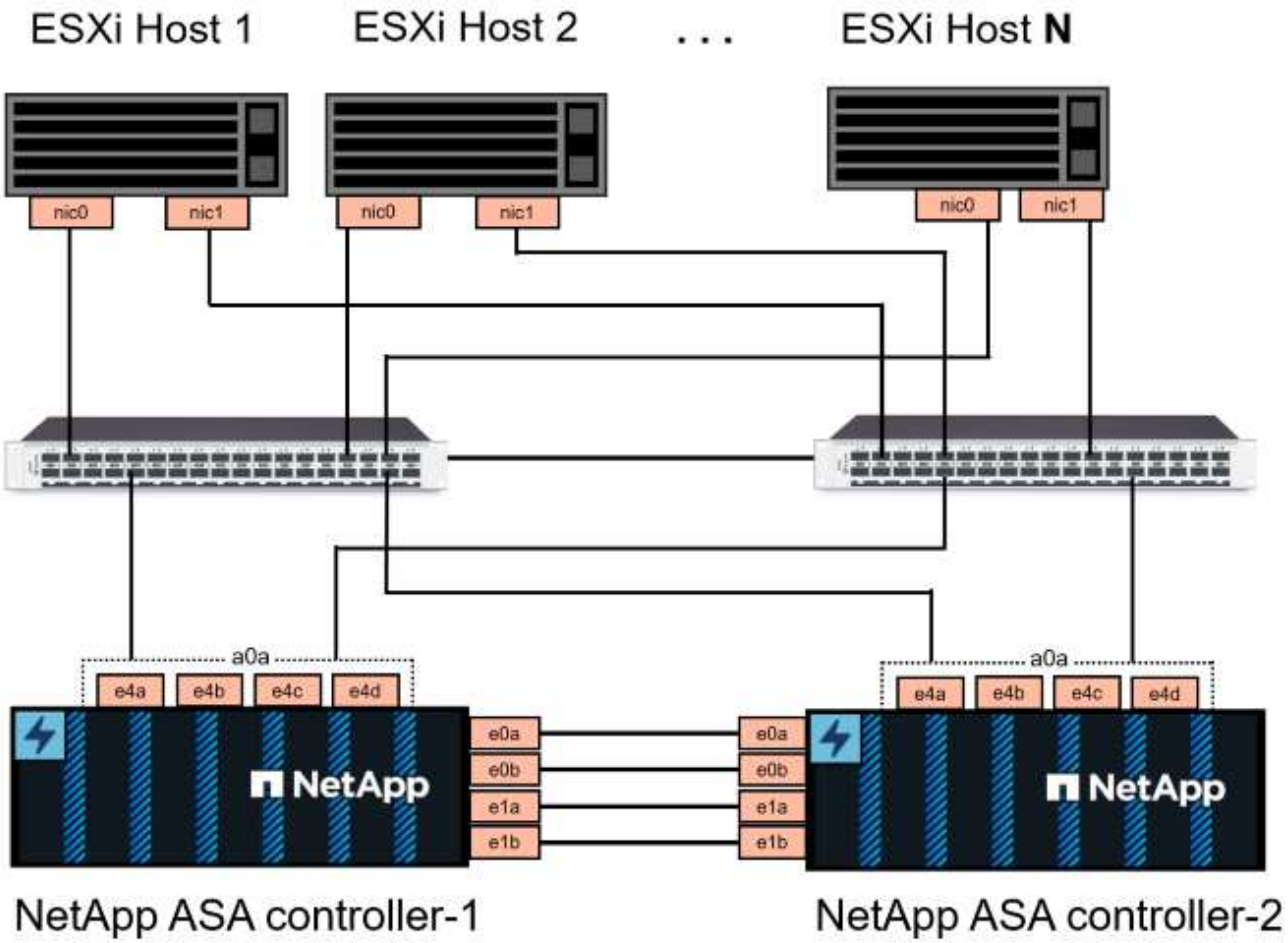
- Crie uma máquina virtual de armazenamento (SVM) com interfaces lógicas (LIFs) para tráfego NVMe/TCP.
- Crie grupos de portas distribuídas para redes iSCSI no domínio de carga de trabalho do VI.
- Crie adaptadores vmkernel para iSCSI nos hosts ESXi para o domínio de carga de trabalho VI.
- Adicione adaptadores NVMe/TCP em hosts ESXi.
- Implantar armazenamento de dados NVMe/TCP.

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP AFF ou ASA com portas de dados físicas em switches Ethernet dedicados ao tráfego de armazenamento.
- A implantação do domínio de gerenciamento do VCF foi concluída e o cliente vSphere está acessível.
- Um domínio de carga de trabalho VI foi implantado anteriormente.

A NetApp recomenda projetos de rede totalmente redundantes para NVMe/TCP. O diagrama a seguir ilustra um exemplo de configuração redundante, fornecendo tolerância a falhas para sistemas de armazenamento, switches, adaptadores de rede e sistemas host. Consulte o NetApp"Referência de configuração SAN" para obter informações adicionais.



Para multipathing e failover em vários caminhos, a NetApp recomenda ter no mínimo dois LIFs por nó de armazenamento em redes Ethernet separadas para todas as SVMs em configurações NVMe/TCP.

Esta documentação demonstra o processo de criação de um novo SVM e especificação das informações de endereço IP para criar vários LIFs para tráfego NVMe/TCP. Para adicionar novos LIFs a um SVM existente, consulte"Criar uma LIF (interface de rede)" .

Para obter informações adicionais sobre considerações de design NVMe para sistemas de armazenamento ONTAP , consulte"Configuração, suporte e limitações do NVMe" .

Etapas de implantação

Para criar um armazenamento de dados VMFS em um domínio de carga de trabalho VCF usando NVMe/TCP, conclua as seguintes etapas.

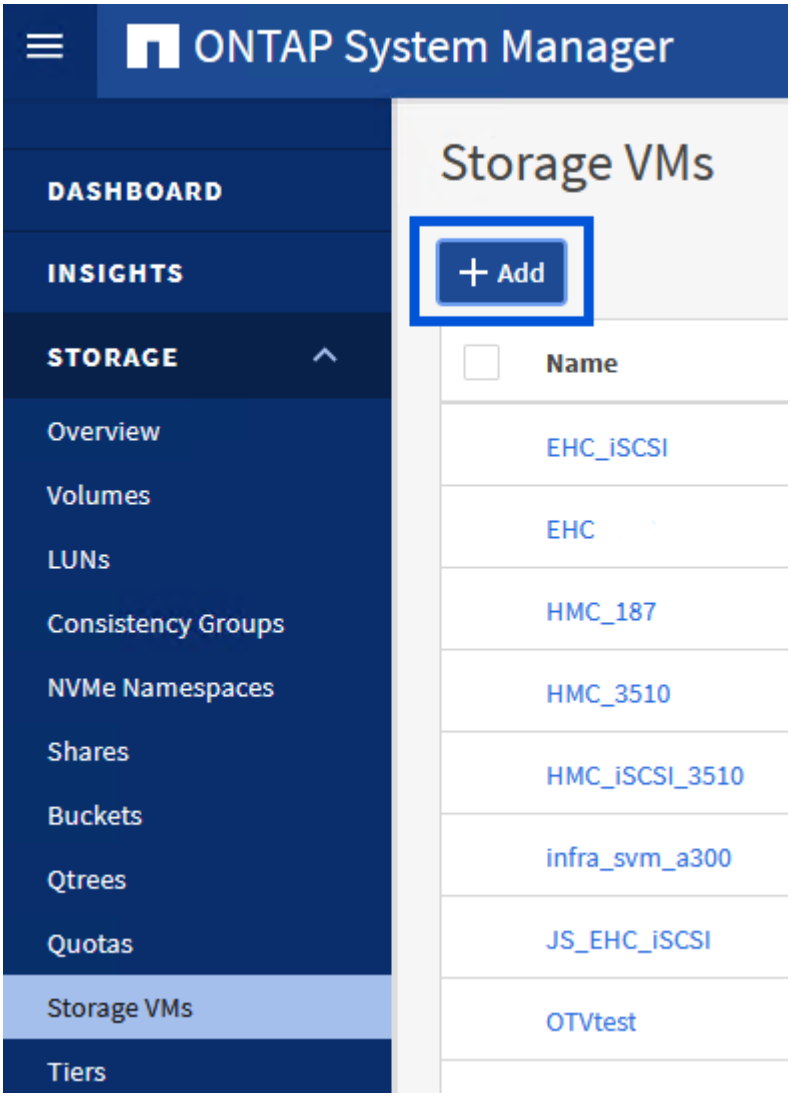
Crie SVM, LIFs e namespace NVMe no sistema de armazenamento ONTAP

A etapa seguinte é executada no ONTAP System Manager.

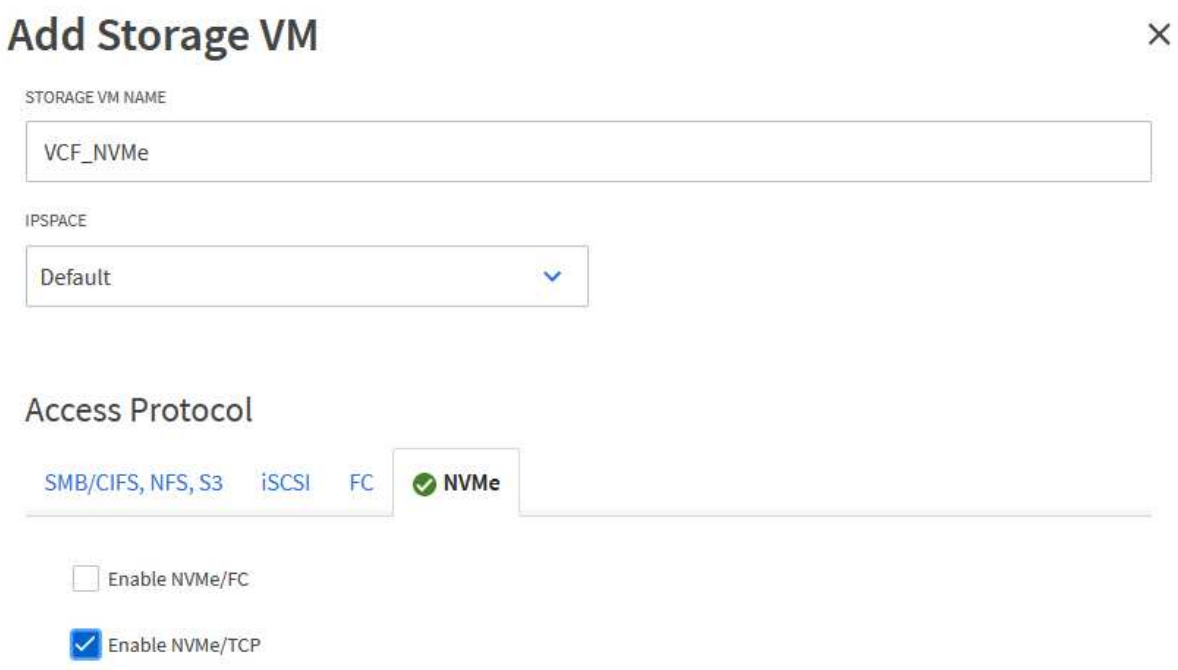
Crie a VM de armazenamento e os LIFs

Conclua as etapas a seguir para criar um SVM junto com vários LIFs para tráfego NVMe/TCP.

1. No ONTAP System Manager, navegue até **VMs de armazenamento** no menu à esquerda e clique em **+ Adicionar** para iniciar.

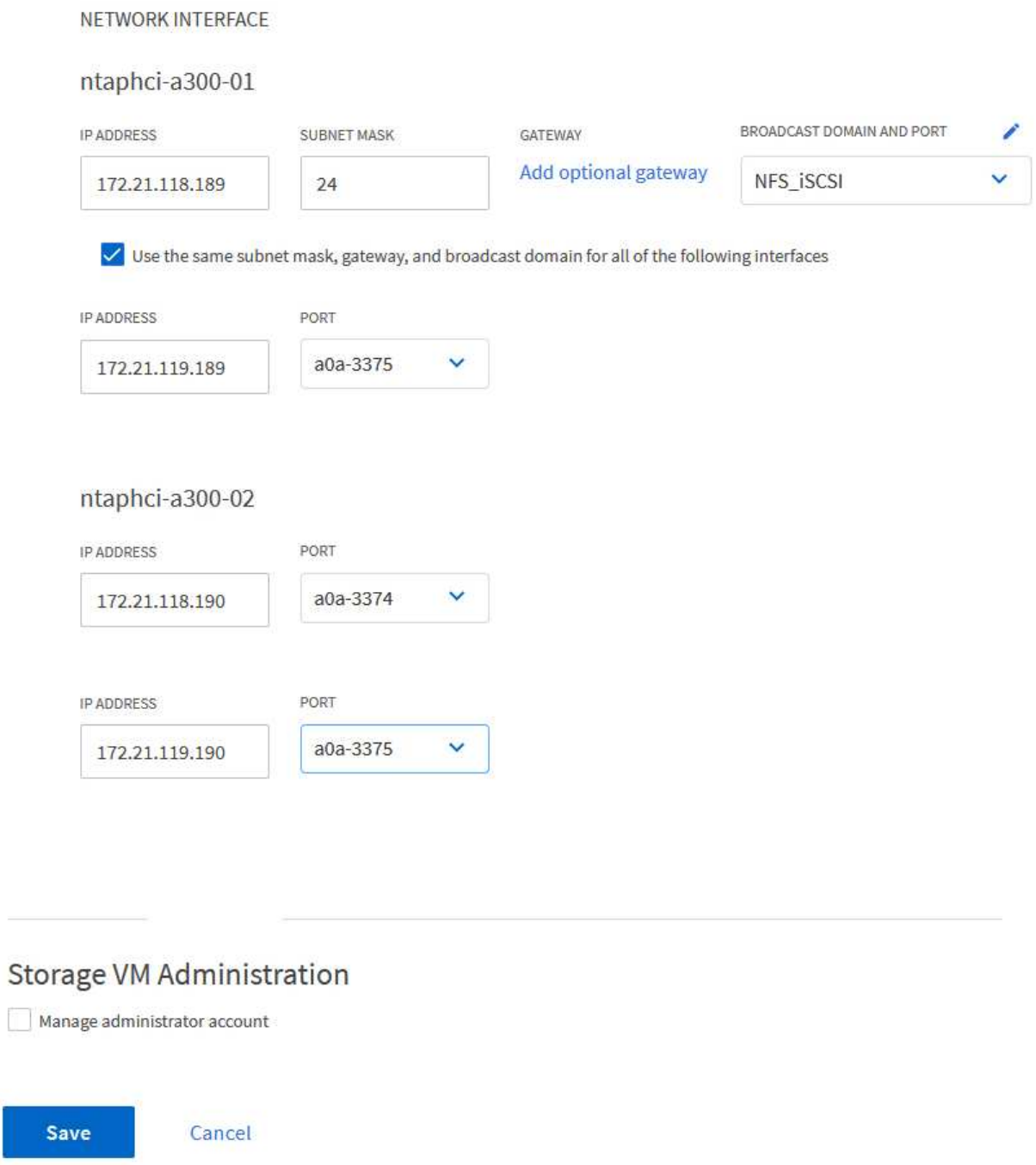


2. No assistente **Adicionar VM de armazenamento**, forneça um **Nome** para a SVM, selecione o **Espaço IP** e, em seguida, em **Protocolo de acesso**, clique na guia **NVMe** e marque a caixa para **Ativar NVMe/TCP**.

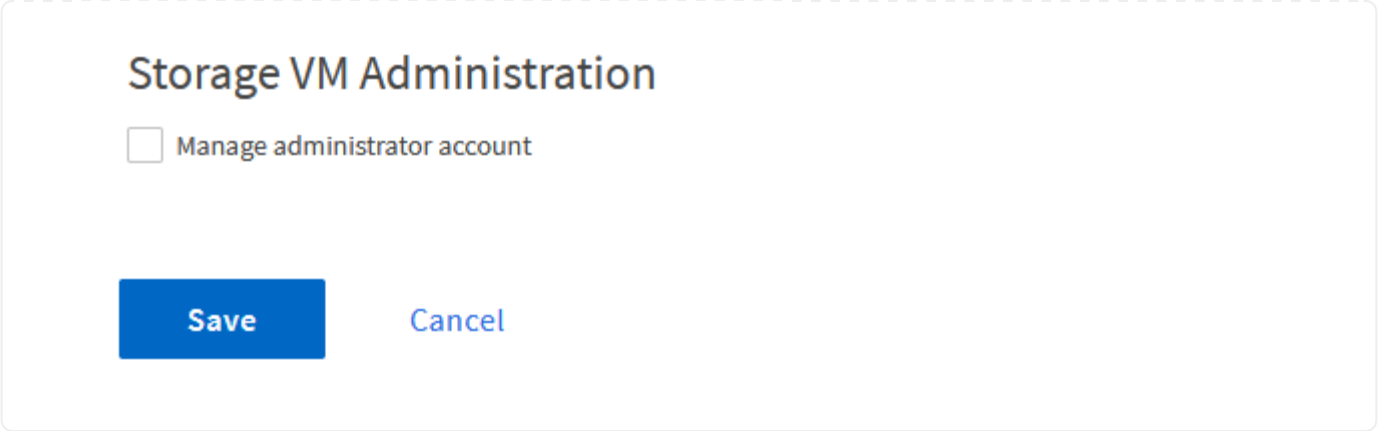


3. Na seção **Interface de rede**, preencha o **endereço IP**, a **máscara de sub-rede** e o **domínio e porta de transmissão** para o primeiro LIF. Para LIFs subsequentes, a caixa de seleção pode ser marcada para usar configurações comuns em todos os LIFs restantes ou usar configurações separadas.

> Para multipathing e failover em vários caminhos, a NetApp recomenda ter no mínimo dois LIFs por nó de armazenamento em redes Ethernet separadas para todas as SVMs em configurações NVMe/TCP.



4. Escolha se deseja habilitar a conta de administração da VM de armazenamento (para ambientes multilocação) e clique em **Salvar** para criar a SVM.


Storage VM Administration
Manage administrator account
Save
Cancel

Crie o namespace NVMe

Os namespaces NVMe são análogos aos LUNs para iSCSi ou FC. O namespace NVMe deve ser criado antes que um armazenamento de dados VMFS possa ser implantado a partir do vSphere Client. Para criar o namespace NVMe, o Nome Qualificado NVMe (NQN) deve primeiro ser obtido de cada host ESXi no cluster. O NQN é usado pelo ONTAP para fornecer controle de acesso ao namespace.

Conclua as seguintes etapas para criar um namespace NVMe:

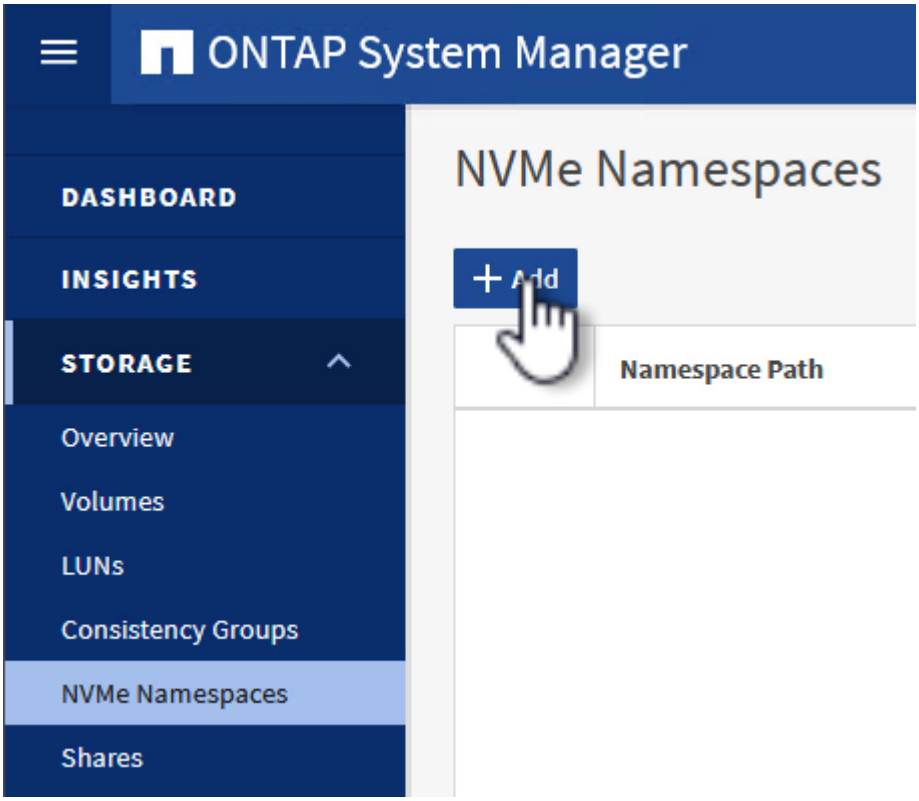
1. Abra uma sessão SSH com um host ESXi no cluster para obter seu NQN. Use o seguinte comando da CLI:

   ```
   esxcli nvme info get
   ```

   Uma saída semelhante à seguinte deve ser exibida:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

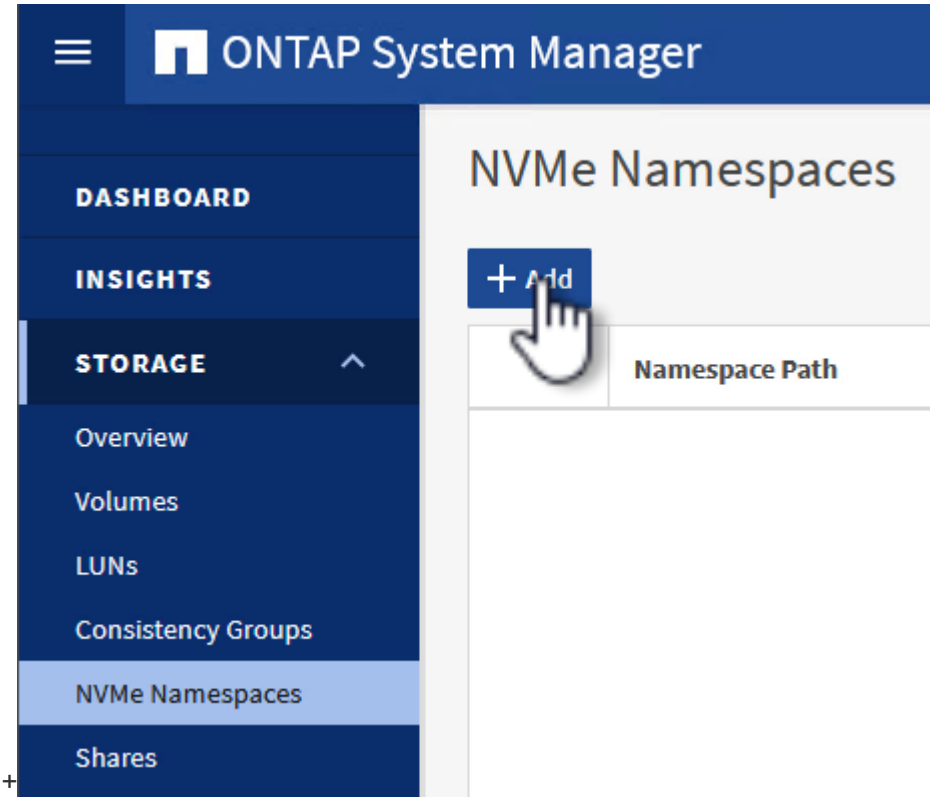
2. Registre o NQN para cada host ESXi no cluster
3. No ONTAP System Manager, navegue até **NVMe Namespaces** no menu à esquerda e clique em **+ Adicionar** para iniciar.



4. Na página **Adicionar namespace NVMe**, preencha um prefixo de nome, o número de namespaces a serem criados, o tamanho do namespace e o sistema operacional do host que acessará o

namespace. Na seção **Host NQN**, crie uma lista separada por vírgulas dos NQNs coletados anteriormente dos hosts ESXi que acessarão os namespaces.

Clique em **Mais opções** para configurar itens adicionais, como a política de proteção de instantâneos. Por fim, clique em **Salvar** para criar o Namespace NVMe.



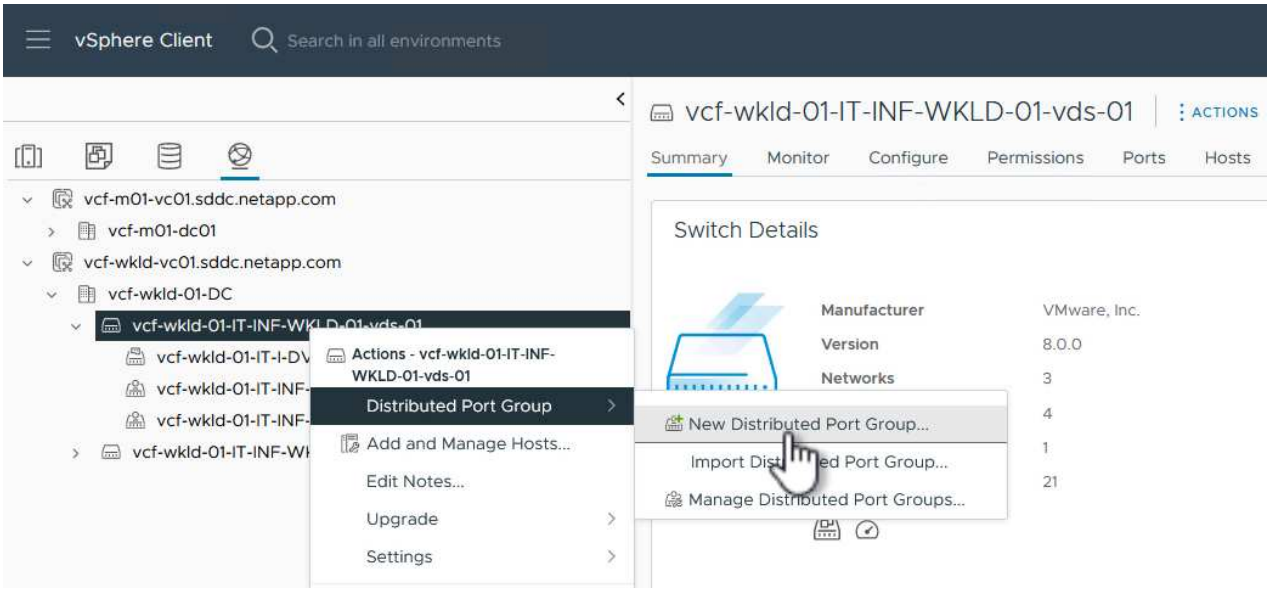
Configurar adaptadores de rede e software NVMe em hosts ESXi

As etapas a seguir são executadas no cluster de domínio de carga de trabalho do VI usando o cliente vSphere. Neste caso, o vCenter Single Sign-On está sendo usado para que o cliente vSphere seja comum aos domínios de gerenciamento e de carga de trabalho.

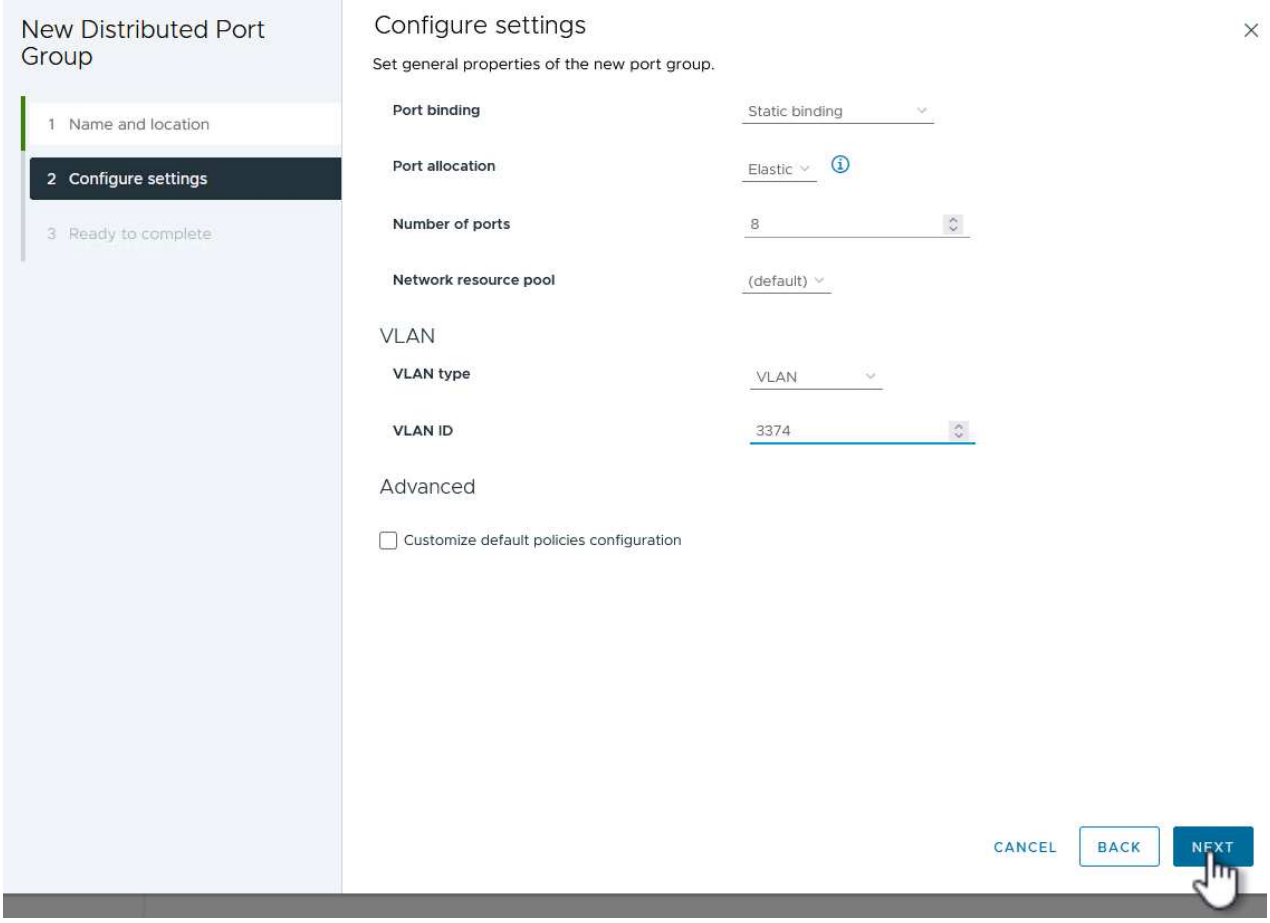
Criar grupos de portas distribuídas para tráfego NVME/TCP

Conclua o seguinte para criar um novo grupo de portas distribuídas para cada rede NVMe/TCP:

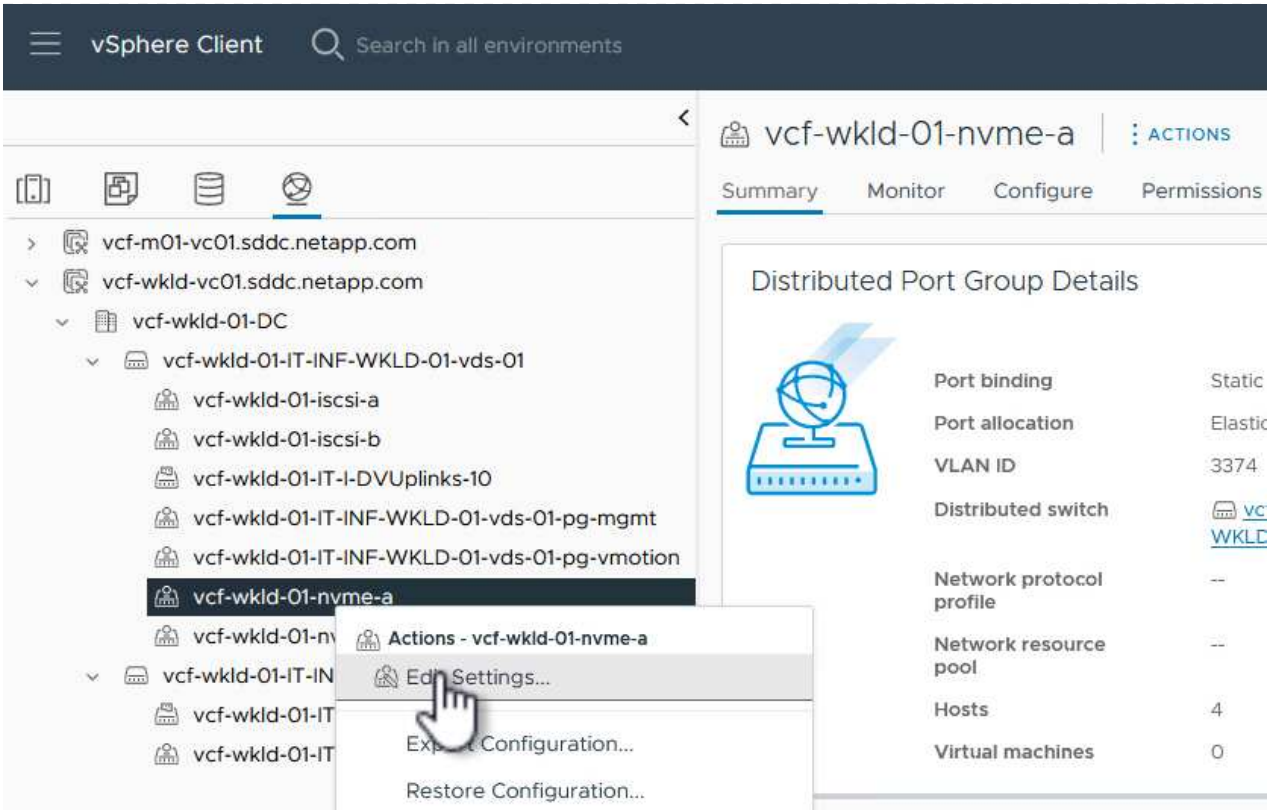
1. No cliente vSphere, navegue até **Inventário > Rede** para o domínio de carga de trabalho. Navegue até o Distributed Switch existente e escolha a ação para criar **Novo Grupo de Portas Distribuídas…** .



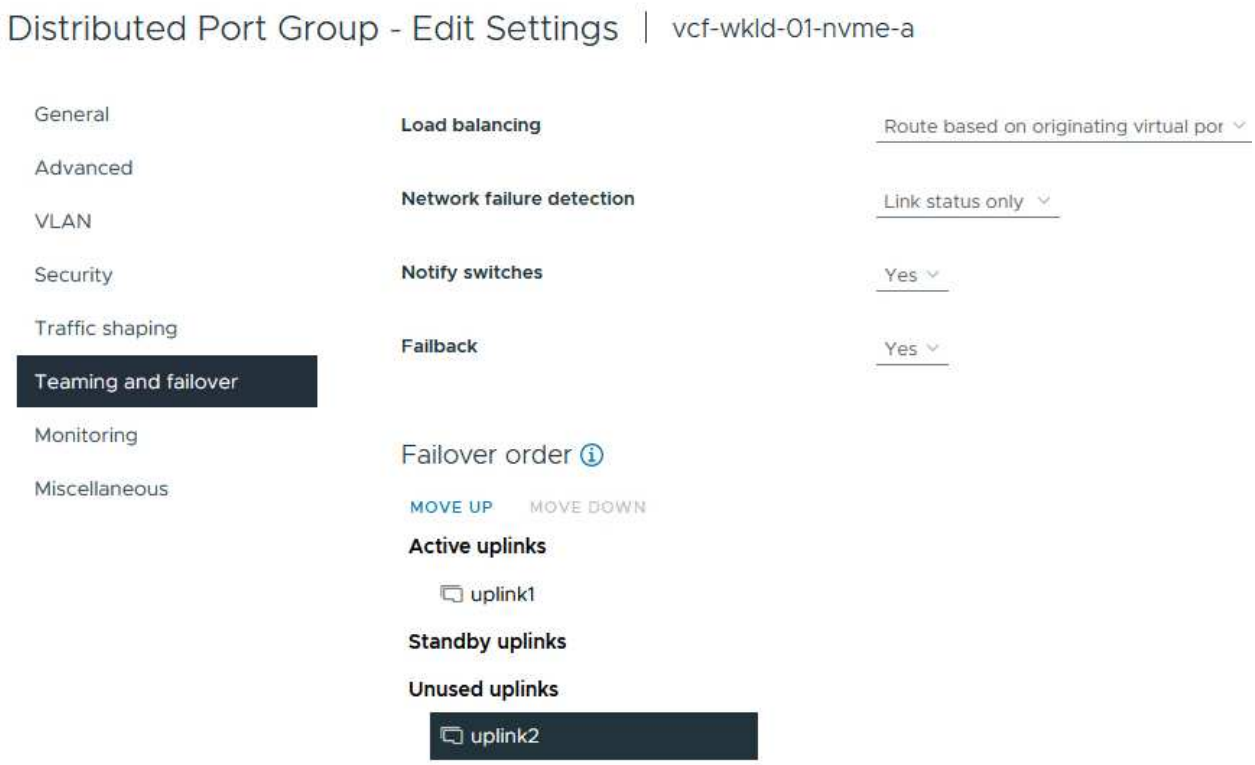
2. No assistente **Novo grupo de portas distribuídas**, preencha um nome para o novo grupo de portas e clique em **Avançar** para continuar.
3. Na página **Configurar configurações** preencha todas as configurações. Se VLANs estiverem sendo usadas, certifique-se de fornecer o ID de VLAN correto. Clique em **Avançar** para continuar.



4. Na página **Pronto para concluir**, revise as alterações e clique em **Concluir** para criar o novo grupo de portas distribuídas.
5. Repita esse processo para criar um grupo de portas distribuídas para a segunda rede NVMe/TCP que está sendo usada e certifique-se de ter inserido o **ID de VLAN** correto.
6. Depois que ambos os grupos de portas forem criados, navegue até o primeiro grupo de portas e selecione a ação **Editar configurações…**.

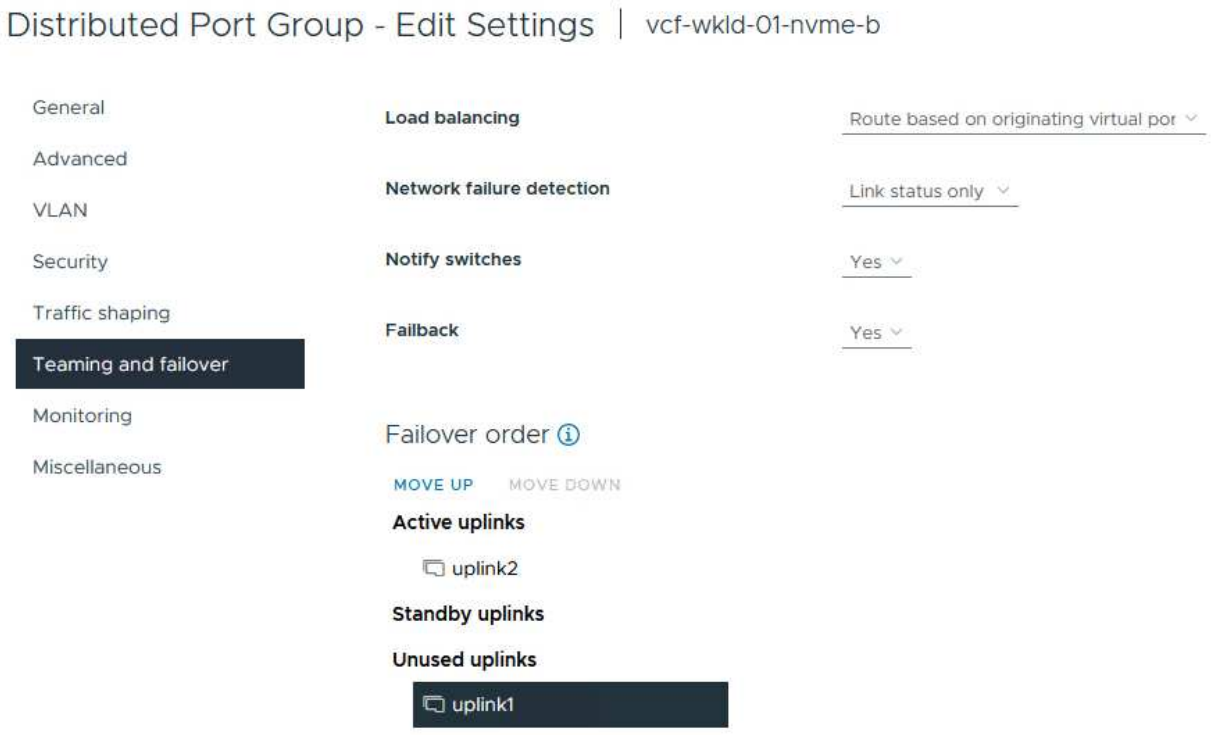


7. Na página **Grupo de portas distribuídas - Editar configurações**, navegue até **Agrupamento e failover** no menu à esquerda e clique em **uplink2** para movê-lo para **Uplinks não utilizados**.



8. Repita esta etapa para o segundo grupo de portas NVMe/TCP. Entretanto, desta vez mova **uplink1**

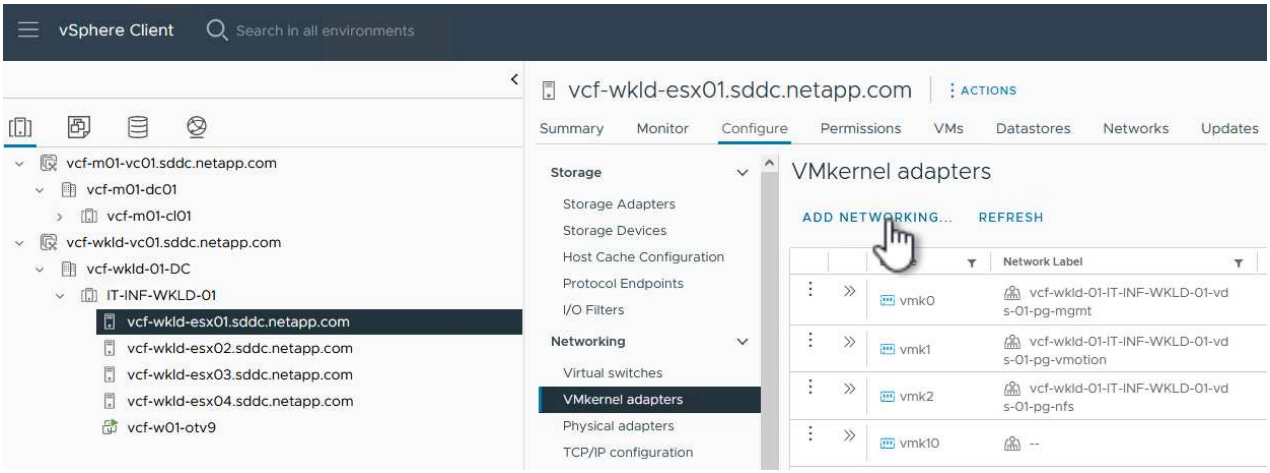
para **Uplinks não utilizados**.



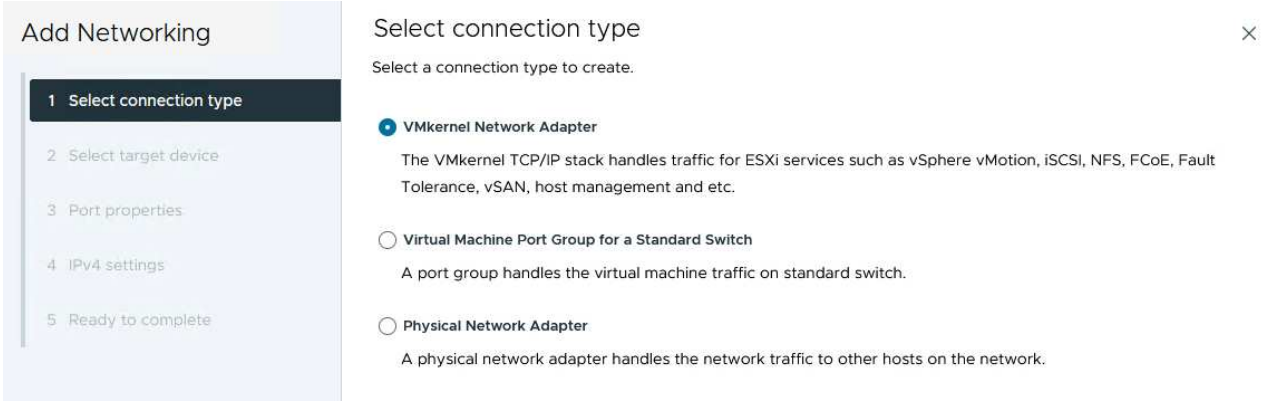
Crie adaptadores VMkernel em cada host ESXi

Repita esse processo em cada host ESXi no domínio de carga de trabalho.

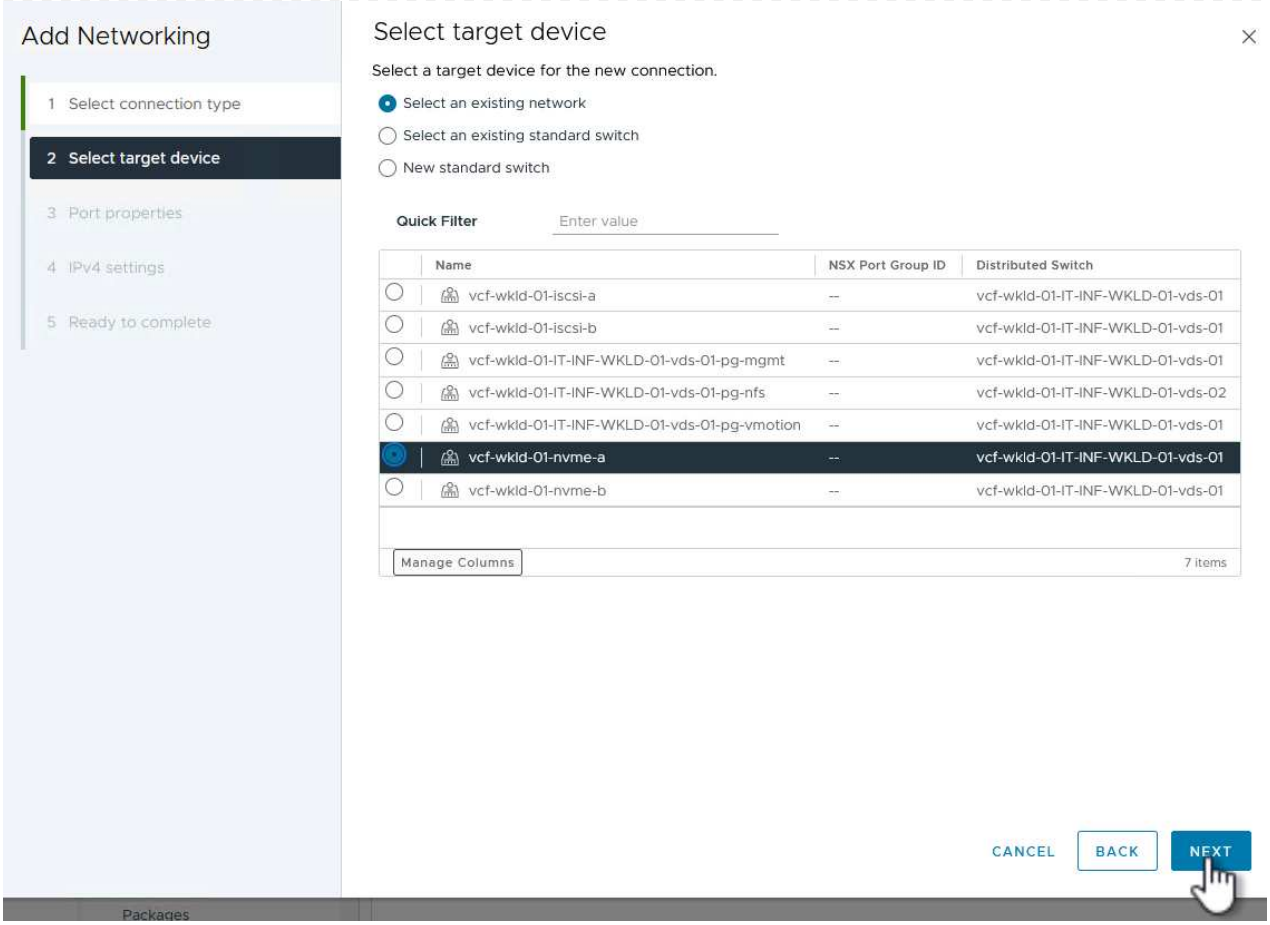
1. No cliente vSphere, navegue até um dos hosts ESXi no inventário do domínio de carga de trabalho. Na aba **Configurar** selecione **Adaptadores VMkernel** e clique em **Adicionar Rede…** para iniciar.



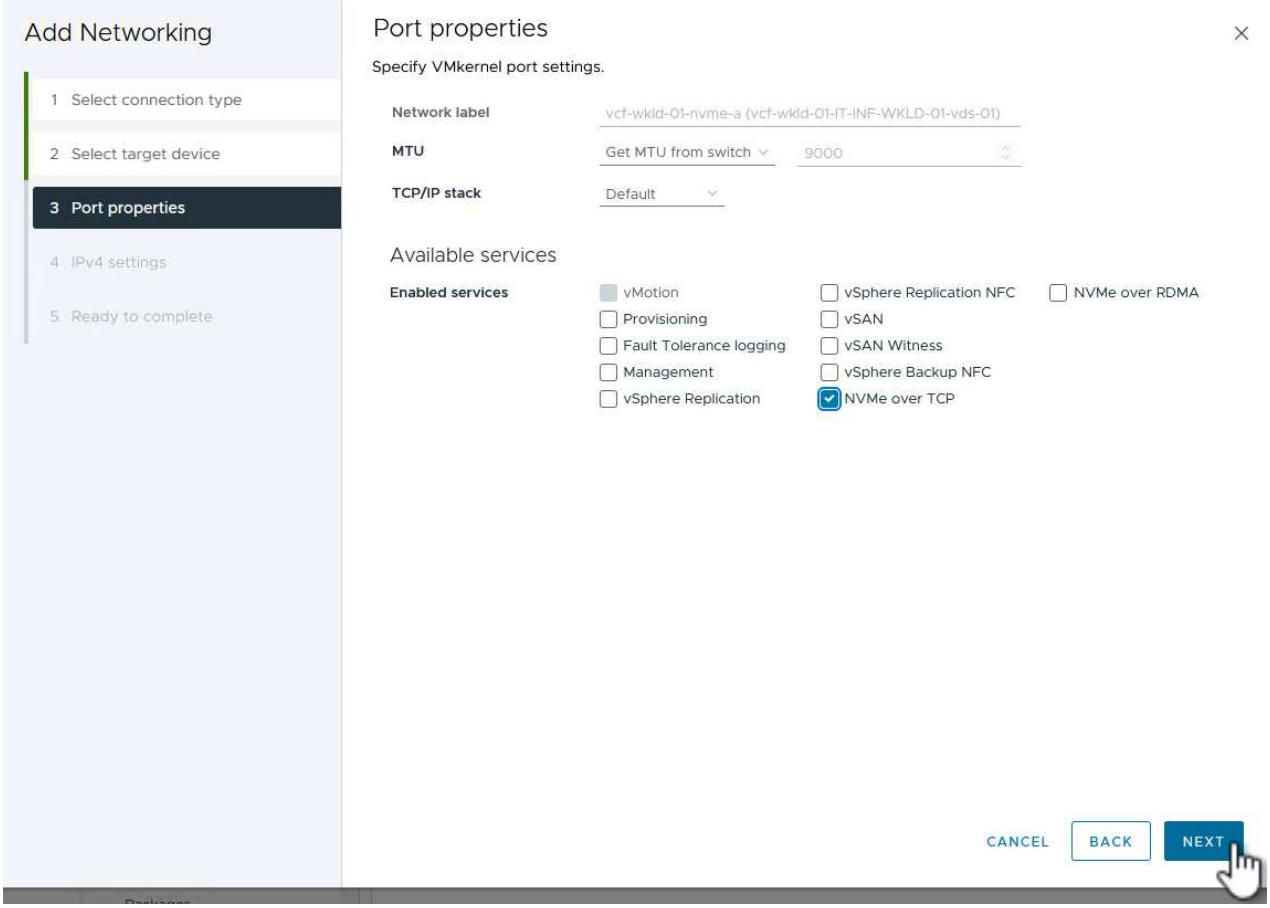
2. Na janela **Selecionar tipo de conexão**, escolha **Adaptador de rede VMkernel** e clique em **Avançar** para continuar.



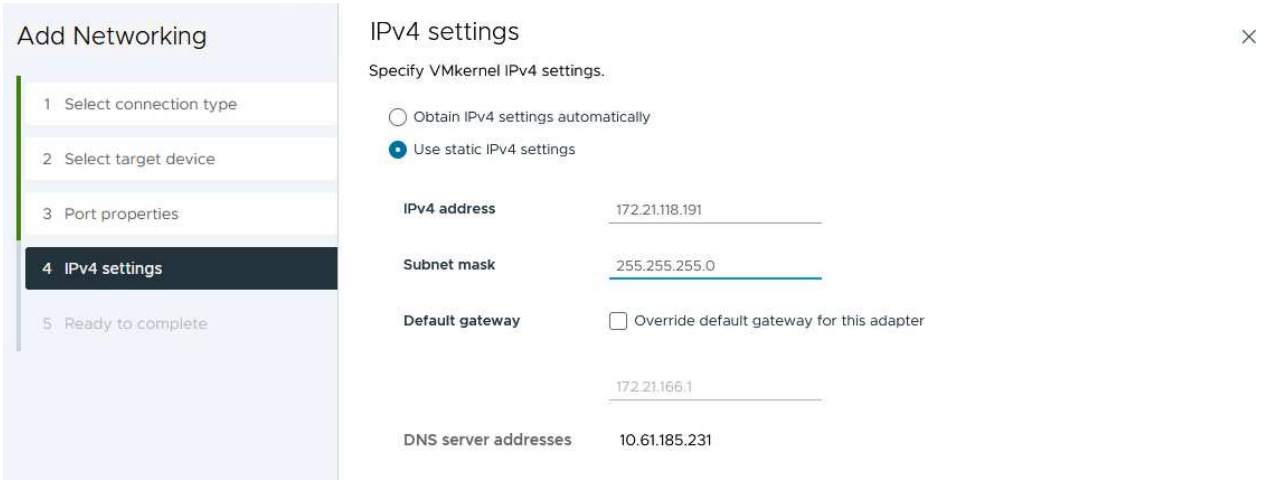
3. Na página **Selecionar dispositivo de destino**, escolha um dos grupos de portas distribuídas para iSCSI que foi criado anteriormente.



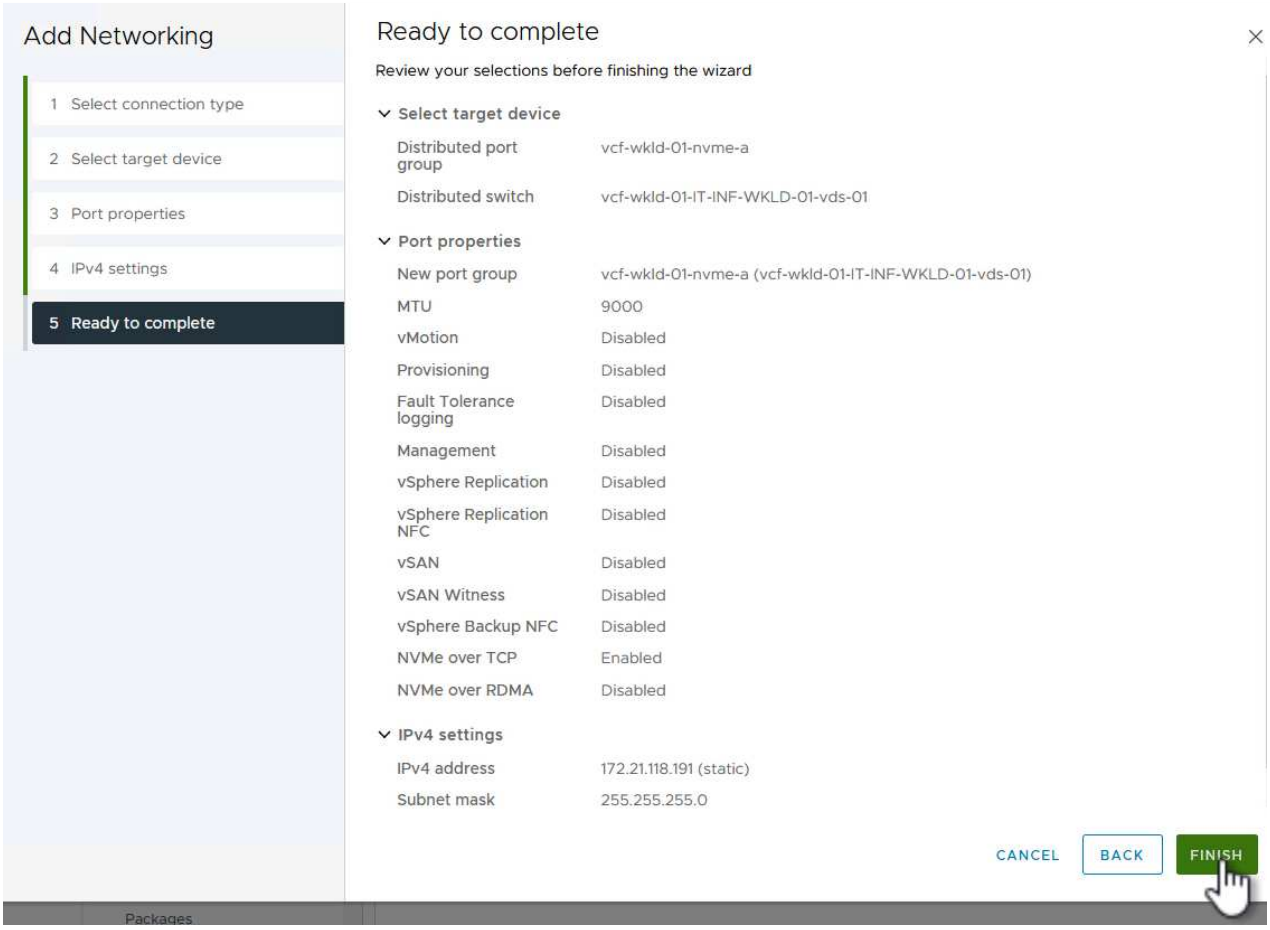
4. Na página **Propriedades da porta**, clique na caixa **NVMe sobre TCP** e clique em **Avançar** para continuar.



5. Na página **Configurações IPv4**, preencha o **endereço IP**, a **máscara de sub-rede** e forneça um novo endereço IP do gateway (somente se necessário). Clique em **Avançar** para continuar.



6. Revise suas seleções na página **Pronto para concluir** e clique em **Concluir** para criar o adaptador VMkernel.



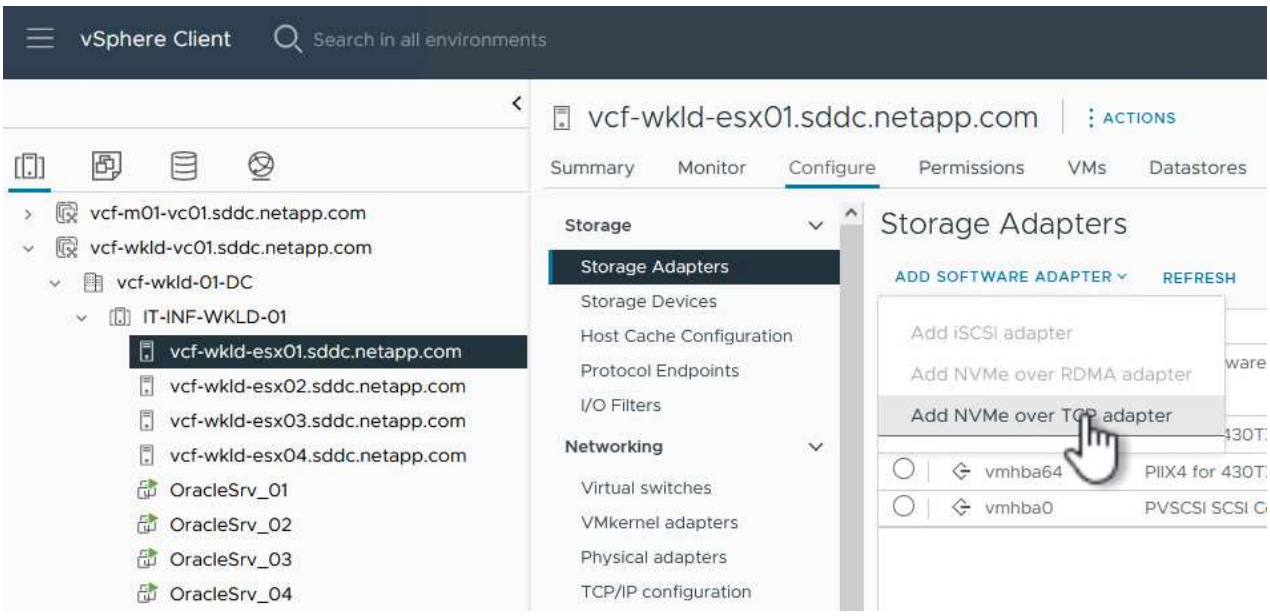
7. Repita esse processo para criar um adaptador VMkernel para a segunda rede iSCSI.

Adicionar adaptador NVMe sobre TCP

Cada host ESXi no cluster de domínio de carga de trabalho deve ter um adaptador de software NVMe sobre TCP instalado para cada rede NVMe/TCP estabelecida dedicada ao tráfego de armazenamento.

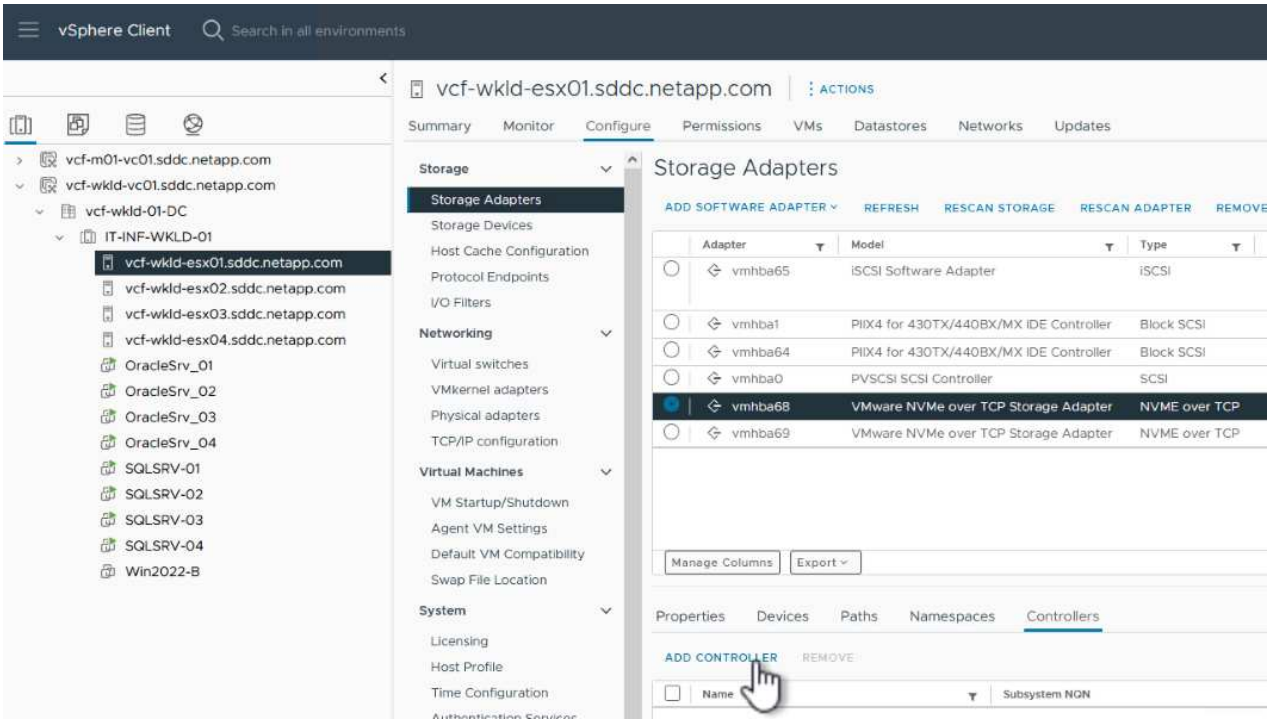
Para instalar adaptadores NVMe sobre TCP e descobrir os controladores NVMe, conclua as seguintes etapas:

1. No cliente vSphere, navegue até um dos hosts ESXi no cluster de domínio de carga de trabalho. Na guia **Configurar**, clique em **Adaptadores de armazenamento** no menu e, em seguida, no menu suspenso **Adicionar adaptador de software**, selecione **Adicionar adaptador NVMe sobre TCP**.

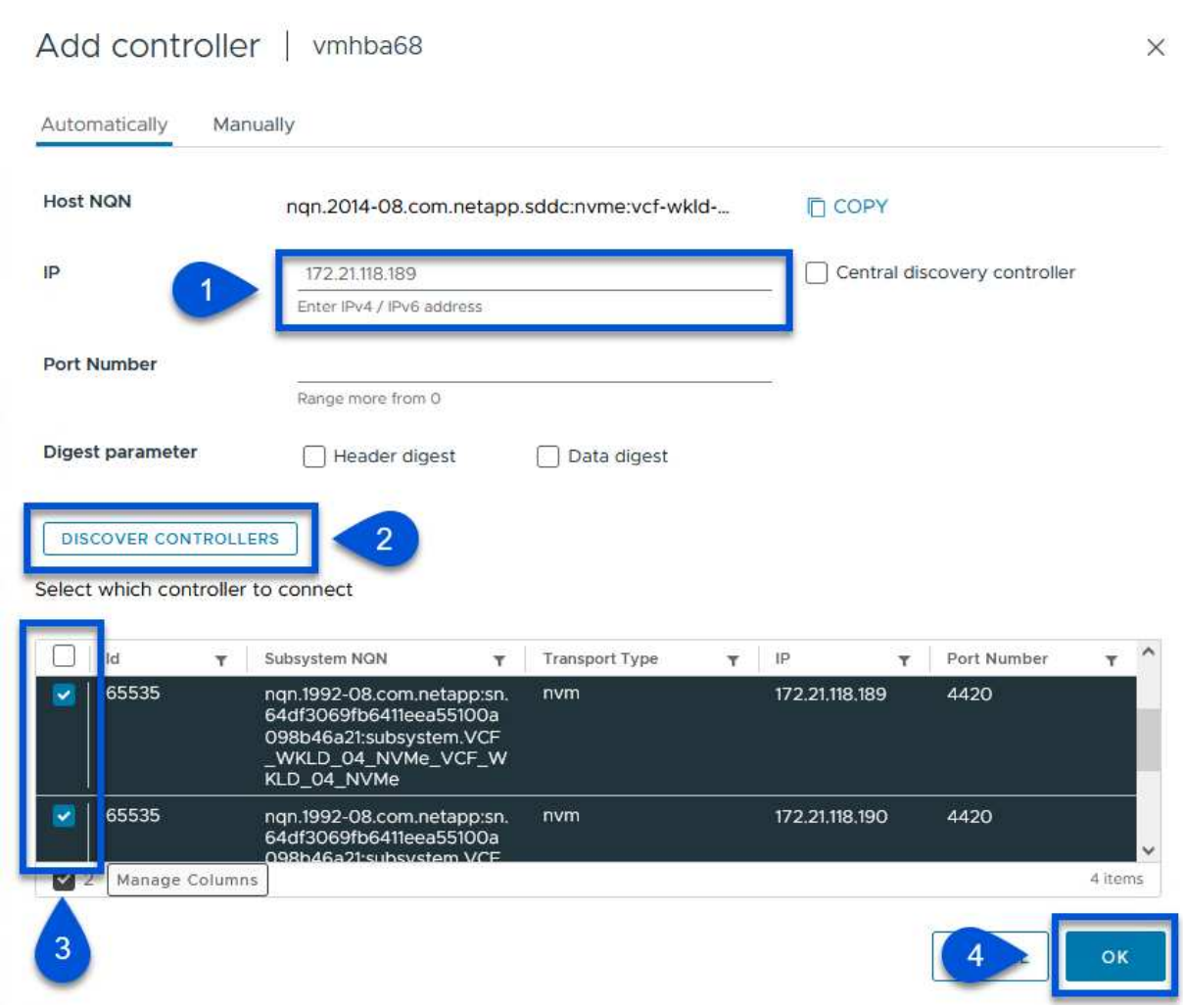


2. Na janela **Adicionar adaptador de software NVMe sobre TCP**, acesse o menu suspenso **Adaptador de rede física** e selecione o adaptador de rede física correto no qual deseja habilitar o adaptador NVMe.

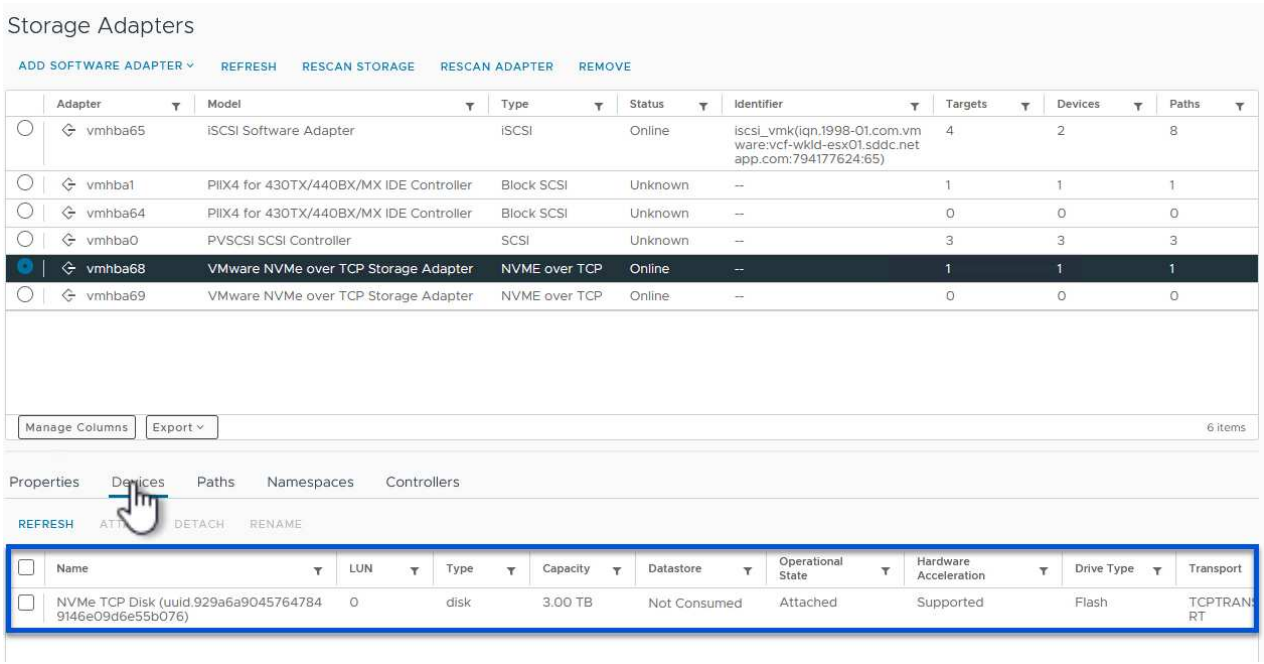
3. Repita esse processo para a segunda rede atribuída ao NVMe sobre tráfego TCP, atribuindo o adaptador físico correto.
4. Selecione um dos adaptadores NVMe sobre TCP recém-instalados e, na guia **Controladores**, selecione **Adicionar controlador**.



5. Na janela **Adicionar controlador**, selecione a aba **Automaticamente** e conclua as seguintes etapas.
    - Preencha um endereço IP para uma das interfaces lógicas SVM na mesma rede que o adaptador físico atribuído a este adaptador NVMe sobre TCP.
    - Clique no botão **Descobrir controladores**.
    - Na lista de controladores descobertos, clique na caixa de seleção dos dois controladores com endereços de rede alinhados com este adaptador NVMe sobre TCP.
    - Clique no botão **OK** para adicionar os controladores selecionados.



6. Após alguns segundos, você deverá ver o namespace NVMe aparecer na guia Dispositivos.

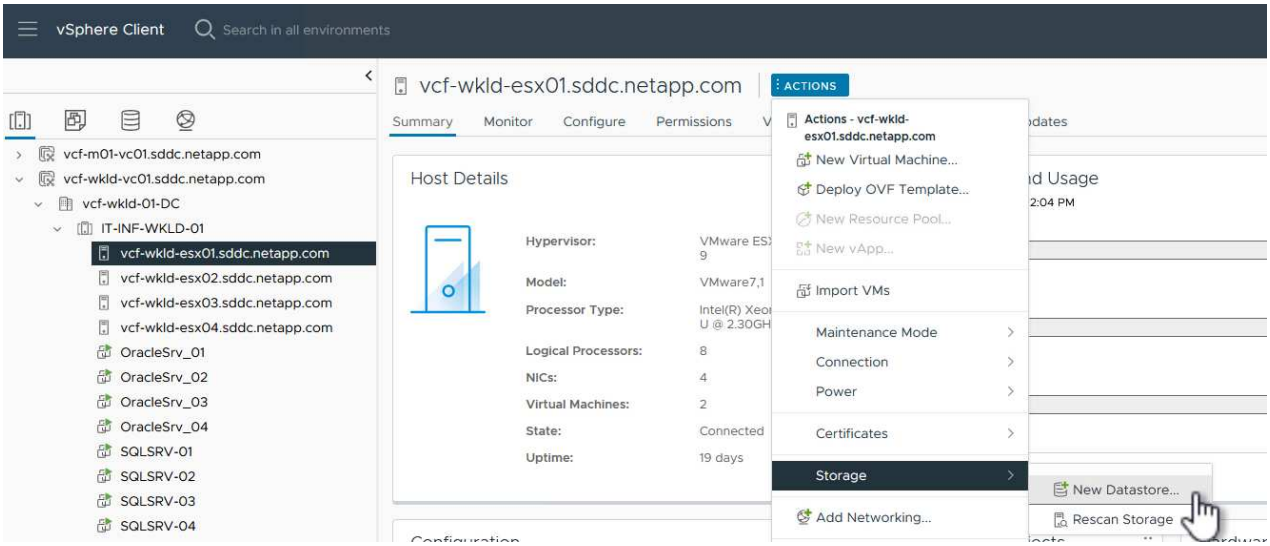


7. Repita este procedimento para criar um adaptador NVMe sobre TCP para a segunda rede estabelecida para tráfego NVMe/TCP.

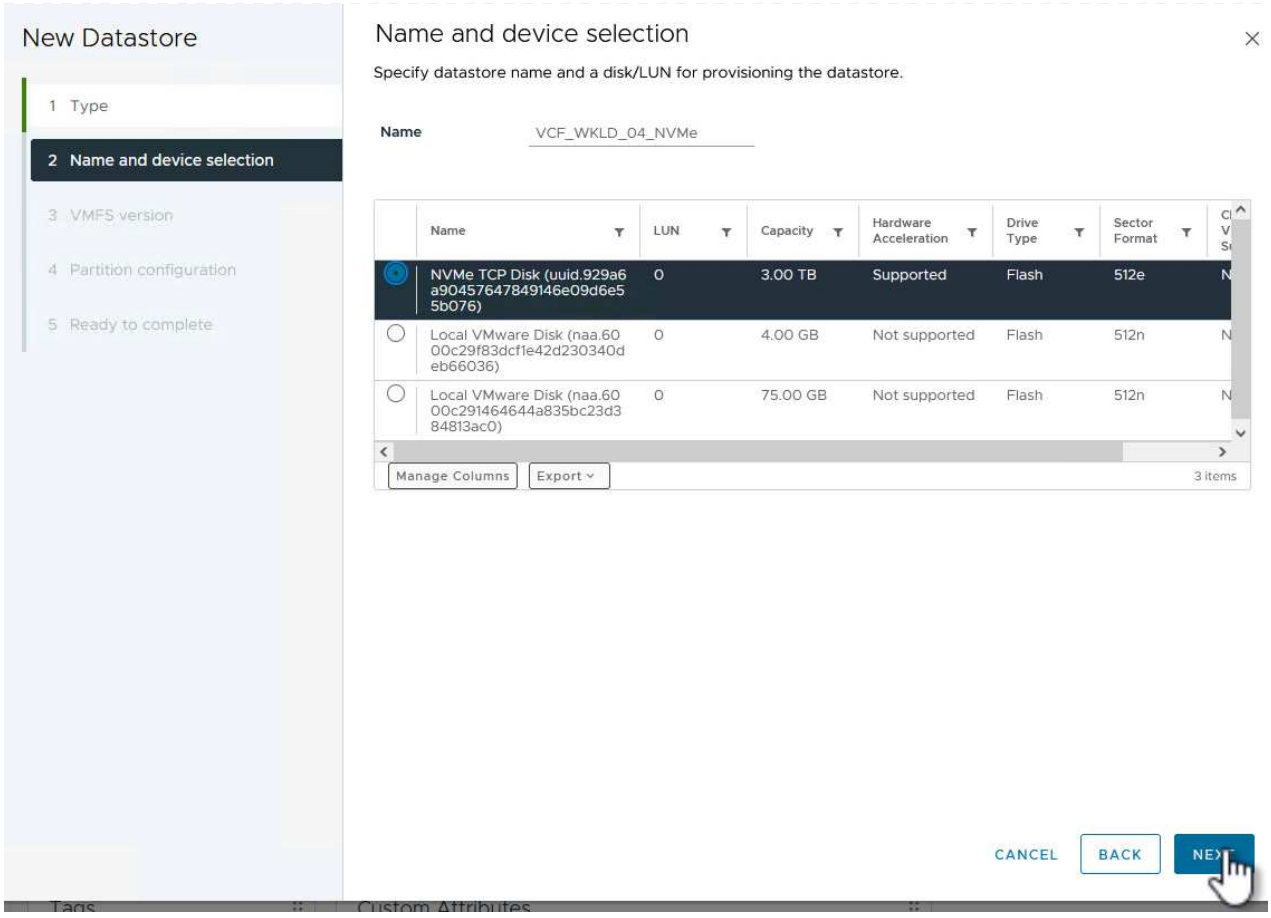
Implantar NVMe sobre armazenamento de dados TCP

Para criar um armazenamento de dados VMFS no namespace NVMe, conclua as seguintes etapas:

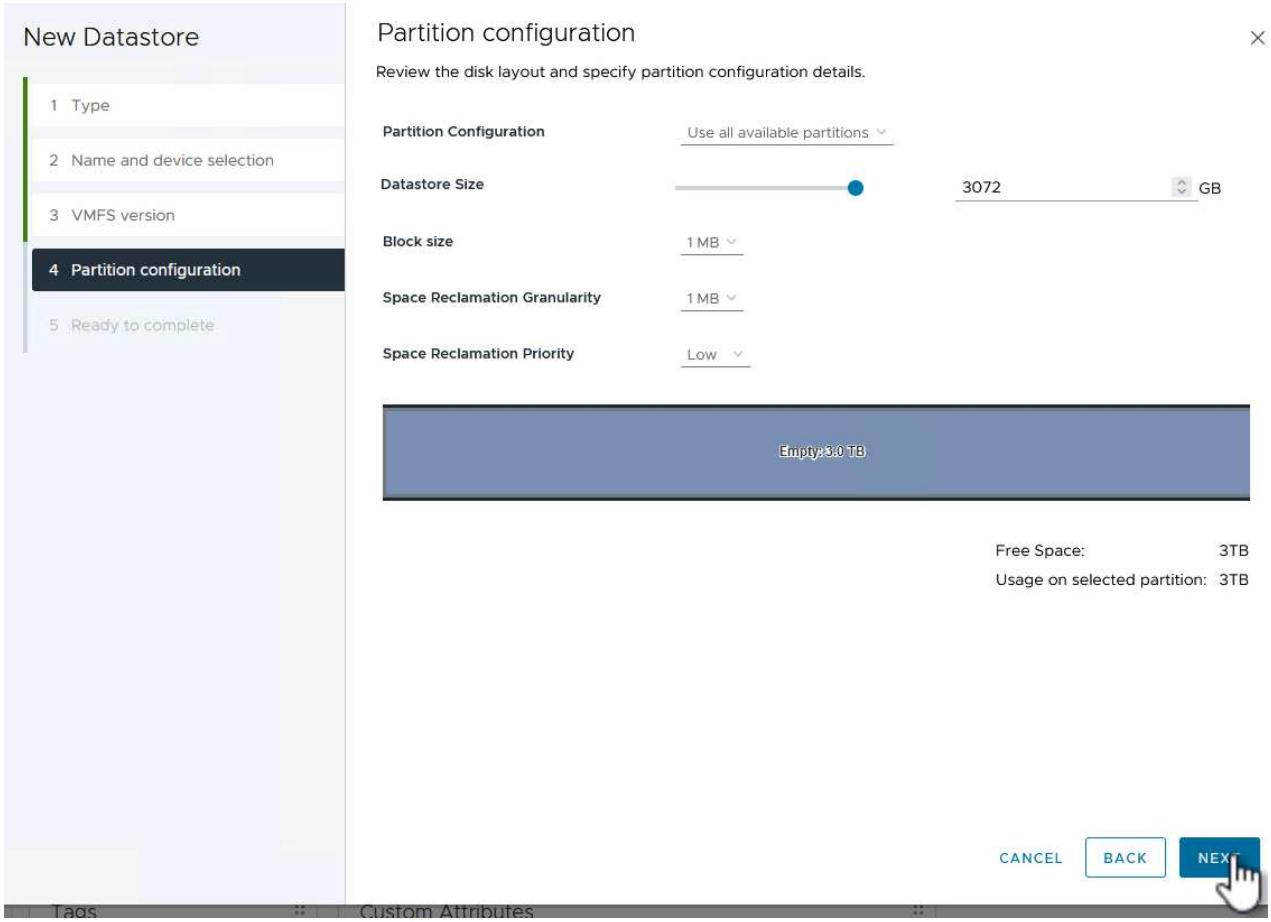
1. No cliente vSphere, navegue até um dos hosts ESXi no cluster de domínio de carga de trabalho. No menu **Ações**, selecione **Armazenamento > Novo armazenamento de dados…**.



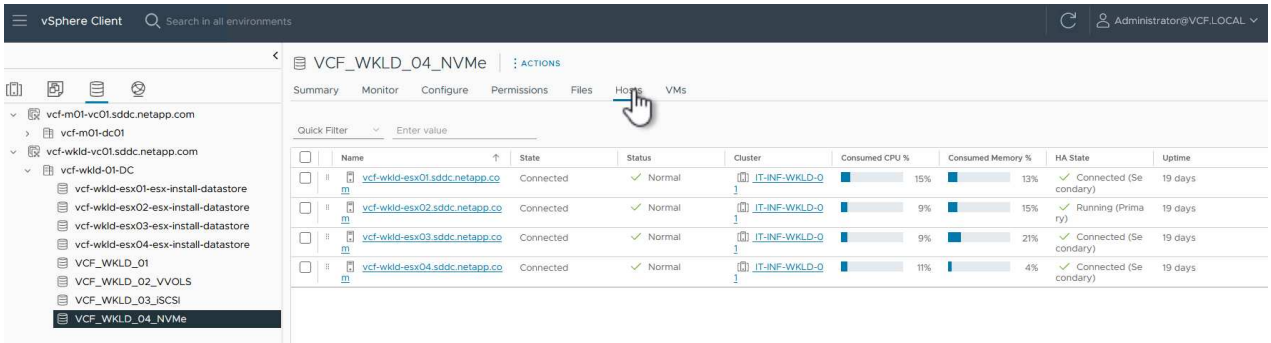
2. No assistente **Novo armazenamento de dados**, selecione **VMFS** como o tipo. Clique em **Avançar** para continuar.
3. Na página **Seleção de nome e dispositivo**, forneça um nome para o armazenamento de dados e selecione o namespace NVMe na lista de dispositivos disponíveis.



4. Na página **Versão do VMFS**, selecione a versão do VMFS para o armazenamento de dados.
5. Na página **Configuração da partição**, faça as alterações desejadas no esquema de partição padrão. Clique em **Avançar** para continuar.



6. Na página **Pronto para concluir**, revise o resumo e clique em **Concluir** para criar o armazenamento de dados.
7. Navegue até o novo armazenamento de dados no inventário e clique na guia **Hosts**. Se configurado corretamente, todos os hosts ESXi no cluster deverão ser listados e ter acesso ao novo armazenamento de dados.



Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Adicionar um armazenamento de dados VMFS baseado em FC como armazenamento suplementar aos domínios de carga de trabalho do VI

Neste caso de uso, descrevemos o procedimento para configurar um armazenamento de dados VMFS usando Fiber Channel (FC) como armazenamento suplementar para um domínio de carga de trabalho de infraestrutura virtual (VI) do VMware Cloud Foundation (VCF). Este procedimento resume a implantação do ONTAP Tools para VMware vSphere, o registro do servidor vCenter da carga de trabalho do VI, a definição do backend de armazenamento e o provisionamento do armazenamento de dados do FC.

Benefícios do Fibre Channel

Alto desempenho: o FC fornece altas taxas de transferência de dados, tornando-o ideal para aplicações que exigem acesso rápido e confiável a grandes quantidades de dados.

Baixa latência: latência muito baixa, o que é crucial para aplicativos sensíveis ao desempenho, como bancos de dados e ambientes virtualizados.

Confiabilidade: As redes FC são conhecidas por sua robustez e confiabilidade, com recursos como redundância integrada e correção de erros.

Largura de banda dedicada: o FC fornece largura de banda dedicada para tráfego de armazenamento, reduzindo o risco de congestionamento da rede.

Para obter mais informações sobre o uso do Fibre Channel com sistemas de armazenamento NetApp , consulte "Provisionamento SAN com FC" .

Visão geral do cenário

O armazenamento de dados suplementar do VCF é fornecido como parte das operações do dia 2 usando o vCenter. Este cenário abrange as seguintes etapas de alto nível:

- Implantação de ferramentas ONTAP no domínio de gerenciamento
- Registrar servidores vCenter de carga de trabalho VI em ferramentas ONTAP
- Definir backend de armazenamento no plugin de ferramentas ONTAP para VMware vSphere
- Provisionar VMFS no transporte FC

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP AFF ou ASA com portas FC conectadas a switches FC.
- SVM criado com FC lifs.
- vSphere com HBAs FC conectados a switches FC.
- O zoneamento de iniciador-alvo único é configurado em switches FC.

> Use a interface lógica SVM FC na configuração de zona em vez de portas FC físicas em sistemas ONTAP .

A NetApp recomenda vários caminhos para LUNs FC.

Para obter informações completas sobre a configuração do canal de fibra em sistemas de armazenamento ONTAP , consulte "Gerenciamento de armazenamento SAN" na documentação do ONTAP 9.

Para obter mais informações sobre o uso do VMFS com sistemas de armazenamento ONTAP , consulte o"Guia de implantação para VMFS" .

Etapas de implantação para o domínio de carga de trabalho do VI

Para implantar o ONTAP Tools e usá-lo para criar um armazenamento de dados VMFS no domínio de carga de trabalho do VCF VI, conclua as seguintes etapas:

- "Registre a carga de trabalho VI vCenter para habilitar o plug-in vCenter"
- "Definir backend de armazenamento usando a interface do cliente vSphere"
- "Provisionar VMFS no FC"

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Demonstração em vídeo desta solução

VMFS(FC) Datastore como armazenamento suplementar para domínio de gerenciamento VCF

Proteja o VCF com o SnapCenter

Aprenda a proteger domínios de carga de trabalho VCF com o plug-in SnapCenter para VMware vSphere

Saiba mais sobre as soluções NetApp que você pode usar para proteger cargas de trabalho do VMware Cloud Foundation (VCF) com o SnapCenter Plug-in for VMware vSphere. Este plug-in simplifica o backup e a recuperação, garantindo backups consistentes com os aplicativos e otimizando o armazenamento com as tecnologias de eficiência da NetApp.

Ele oferece suporte a fluxos de trabalho automatizados e operações escaláveis, além de fornecer integração perfeita com o cliente vSphere. Com a replicação do SnapMirror fornecendo backup secundário no local ou na nuvem, ele oferece proteção de dados robusta e eficiência operacional em ambientes virtualizados.

Consulte as soluções a seguir para obter mais detalhes.

- "Proteger o domínio de carga de trabalho do VCF"

- "Proteja múltiplos domínios de carga de trabalho do VCF"
- "Proteja o domínio de carga de trabalho VCF com NVMe"
- "Proteção de dados 3-2-1 para VMware com plug-in SnapCenter e BlueXP backup and recovery para VMs"

Proteja um domínio de carga de trabalho VCF com o plug-in SnapCenter para VMware vSphere

Neste caso de uso, descrevemos o procedimento para usar o plug-in SnapCenter para VMware vSphere para fazer backup e restaurar VMs e armazenamentos de dados em um domínio de carga de trabalho do VMware Cloud Foundation (VCF). Este procedimento resume a implantação do plug-in SnapCenter para VMware vSphere, a adição de sistemas de armazenamento, a criação de políticas de backup e a execução de restaurações de VMs e arquivos.

iSCSI é usado como protocolo de armazenamento para o armazenamento de dados VMFS nesta solução.

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Implante o SnapCenter Plug-in for VMware vSphere (SCV) no domínio de carga de trabalho do VI.
- Adicione sistemas de armazenamento ao SCV.
- Crie políticas de backup no SCV.
- Crie grupos de recursos no SCV.
- Use o SCV para fazer backup de armazenamentos de dados ou VMs específicas.
- Use o SCV para restaurar VMs em um local alternativo no cluster.
- Use o SCV para restaurar arquivos para um sistema de arquivos do Windows.

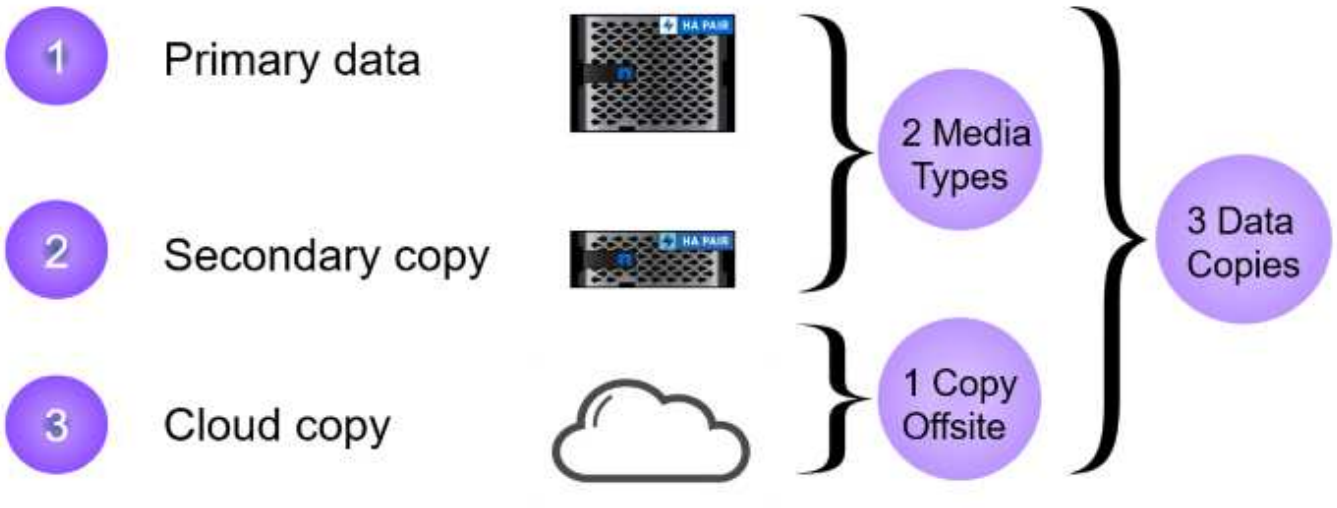
Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Um sistema de armazenamento ONTAP ASA com armazenamentos de dados iSCSI VMFS alocados ao cluster de domínio de carga de trabalho.
- Um sistema de armazenamento ONTAP secundário configurado para receber backups secundários usando SnapMirror.
- A implantação do domínio de gerenciamento do VCF foi concluída e o cliente vSphere está acessível.
- Um domínio de carga de trabalho VI foi implantado anteriormente.
- As máquinas virtuais estão presentes no cluster que o SCV foi designado para proteger.

Para obter informações sobre como configurar armazenamentos de dados iSCSI VMFS como armazenamento suplementar, consulte"**iSCSI como armazenamento suplementar para domínios de gerenciamento usando ferramentas ONTAP para VMware**" nesta documentação. O processo para usar o OTV para implantar armazenamentos de dados é idêntico para domínios de gerenciamento e carga de trabalho.

Além de replicar backups feitos com SCV para armazenamento secundário, cópias externas de dados podem ser feitas para armazenamento de objetos em um dos três (3) principais provedores de nuvem usando o BlueXP backup and recovery NetApp BlueXP para VMs. Para mais informações consulte a solução"Proteção de dados 3-2-1 para VMware com plug-in SnapCenter e BlueXP backup and recovery para VMs" .



Etapas de implantação

Para implantar o plug-in SnapCenter e usá-lo para criar backups e restaurar VMs e armazenamentos de dados, conclua as seguintes etapas:

Implantar e usar o SCV para proteger dados em um domínio de carga de trabalho do VI

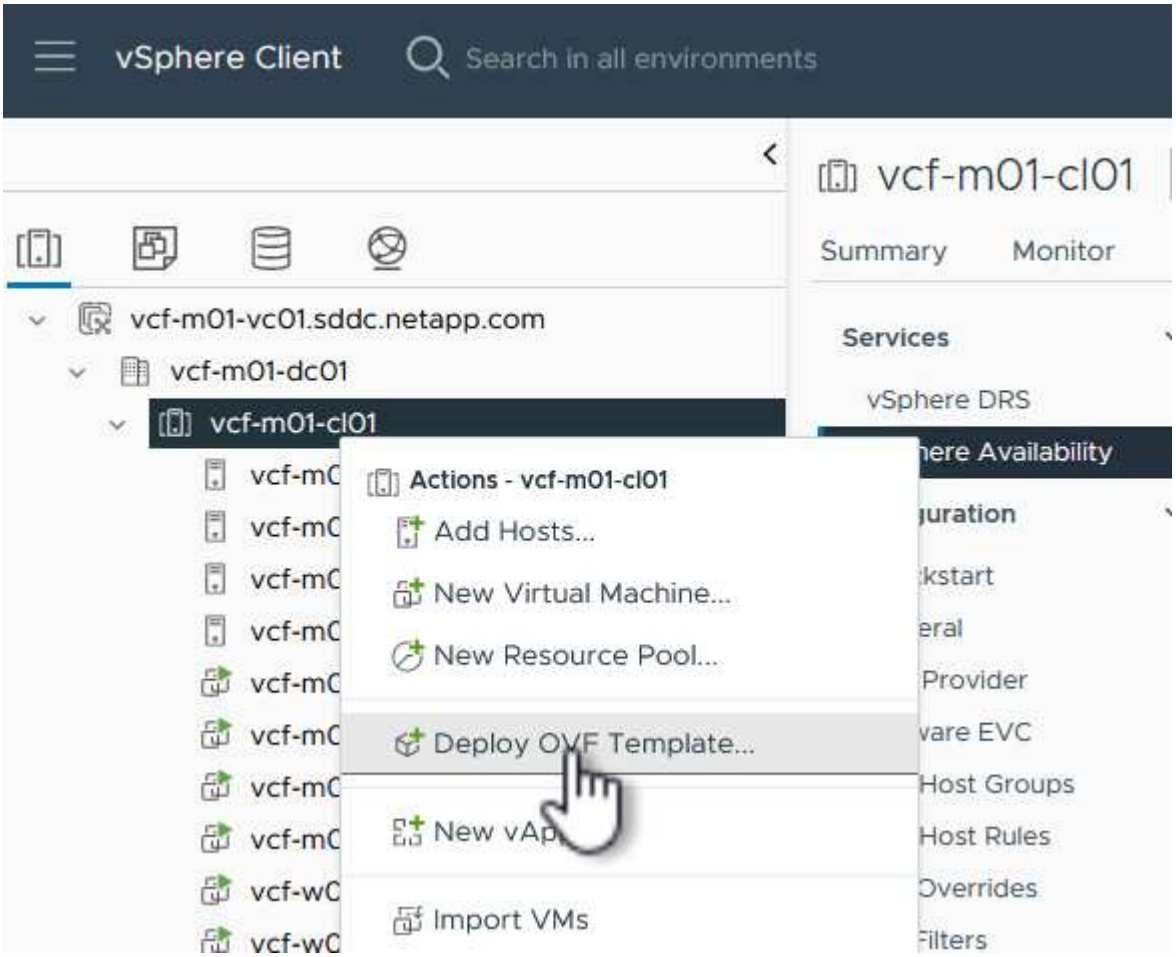
Conclua as seguintes etapas para implantar, configurar e usar o SCV para proteger dados em um domínio de carga de trabalho do VI:

Implantar o SnapCenter Plug-in for VMware vSphere

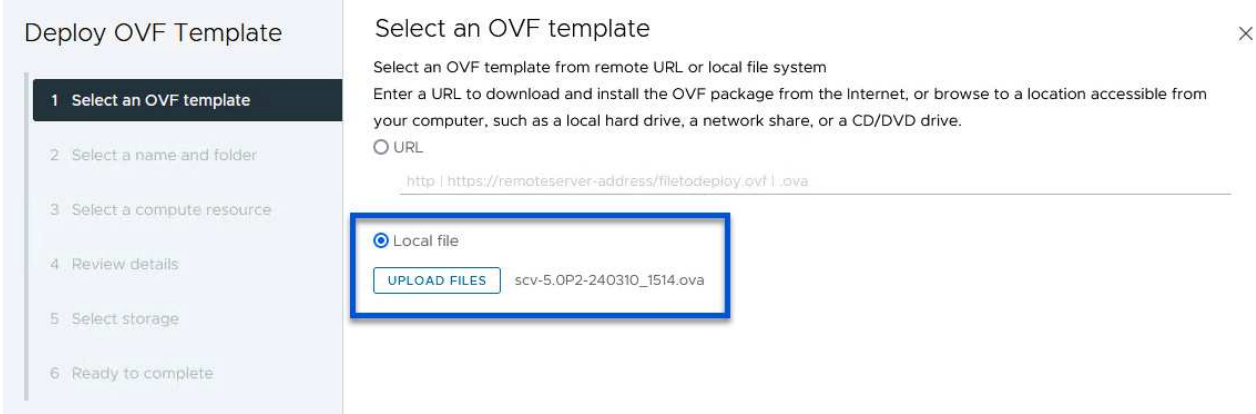
O plug-in SnapCenter é hospedado no domínio de gerenciamento do VCF, mas registrado no vCenter para o domínio de carga de trabalho do VI. Uma instância do SCV é necessária para cada instância do vCenter e lembre-se de que um domínio de carga de trabalho pode incluir vários clusters gerenciados por uma única instância do vCenter.

Conclua as seguintes etapas no cliente vCenter para implantar o SCV no domínio de carga de trabalho do VI:

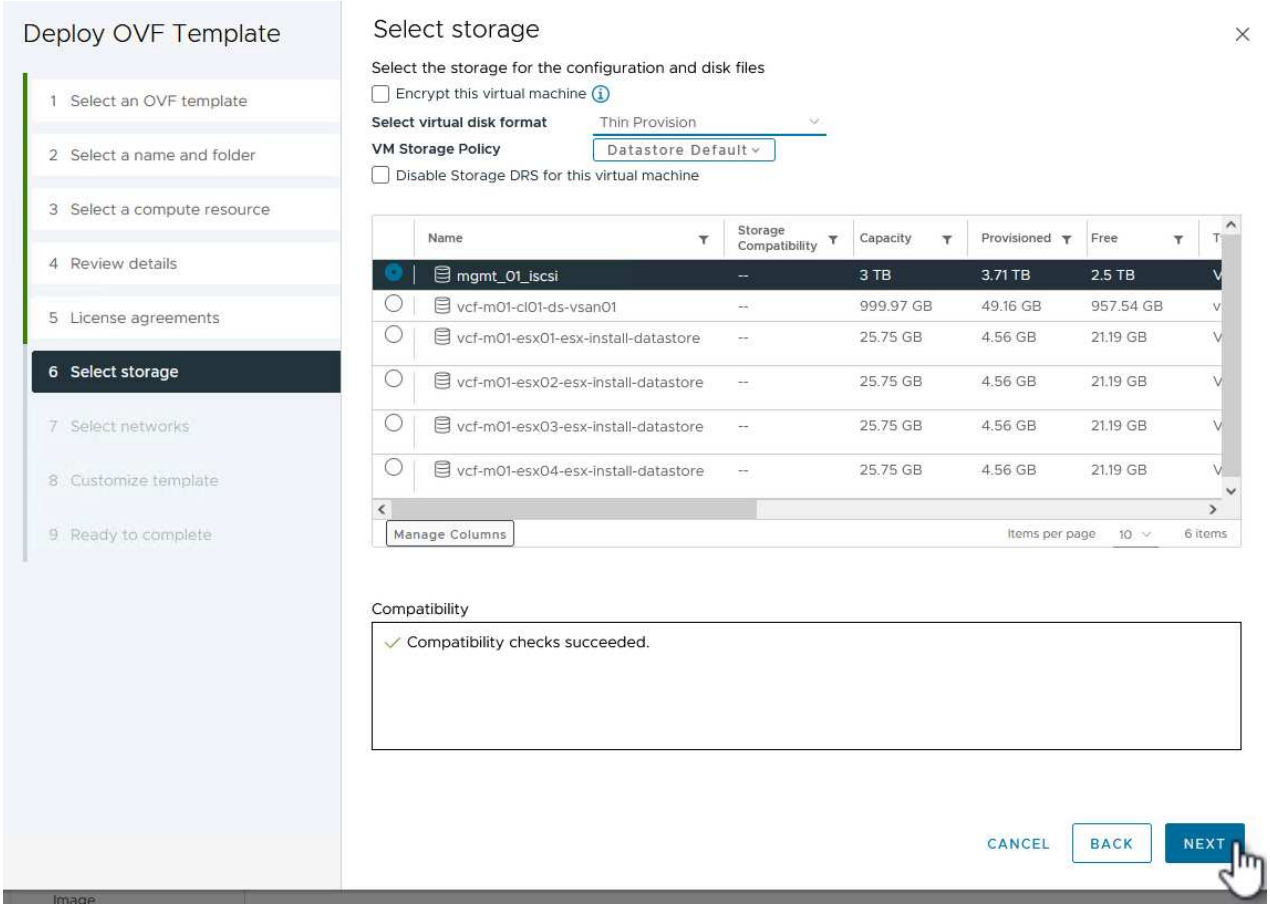
1. Baixe o arquivo OVA para a implantação do SCV na área de download do site de suporte da NetApp "AQUI" .
2. No domínio de gerenciamento vCenter Client, selecione **Implantar modelo OVF…**.



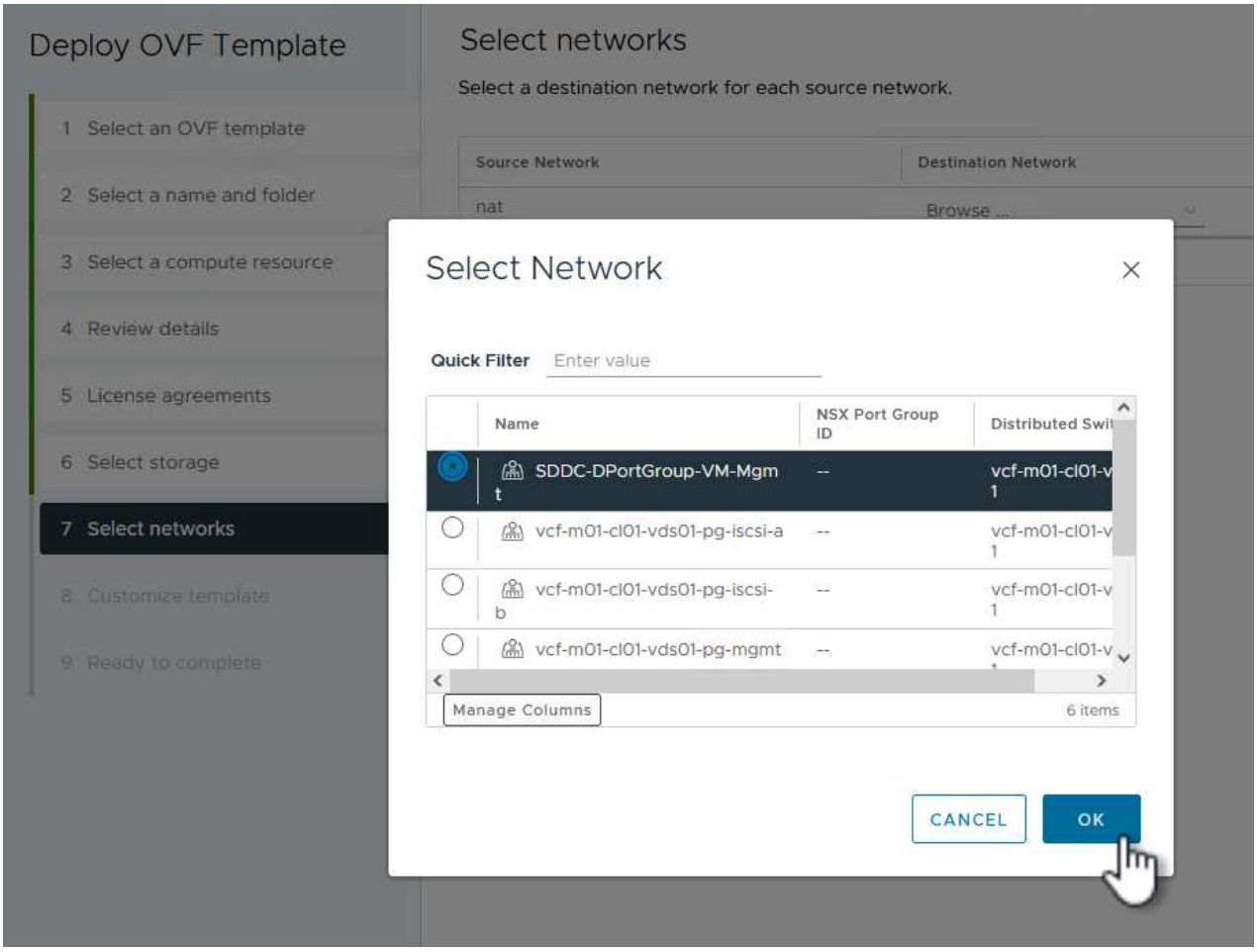
3. No assistente **Implantar modelo OVF**, clique no botão de opção **Arquivo local** e selecione para carregar o modelo OVF baixado anteriormente. Clique em **Avançar** para continuar.



4. Na página **Selecionar nome e pasta**, forneça um nome para a VM do SCV data broker e uma pasta no domínio de gerenciamento. Clique em **Avançar** para continuar.
5. Na página **Selecionar um recurso de computação**, selecione o cluster de domínio de gerenciamento ou o host ESXi específico dentro do cluster para instalar a VM.
6. Revise as informações referentes ao modelo OVF na página **Revisar detalhes** e concorde com os termos de licenciamento na página **Contratos de licenciamento**.
7. Na página **Selecionar armazenamento**, escolha o armazenamento de dados no qual a VM será instalada e selecione o **formato do disco virtual** e a **Política de armazenamento da VM**. Nesta solução, a VM será instalada em um armazenamento de dados iSCSI VMFS localizado em um sistema de armazenamento ONTAP , conforme implantado anteriormente em uma seção separada desta documentação. Clique em **Avançar** para continuar.

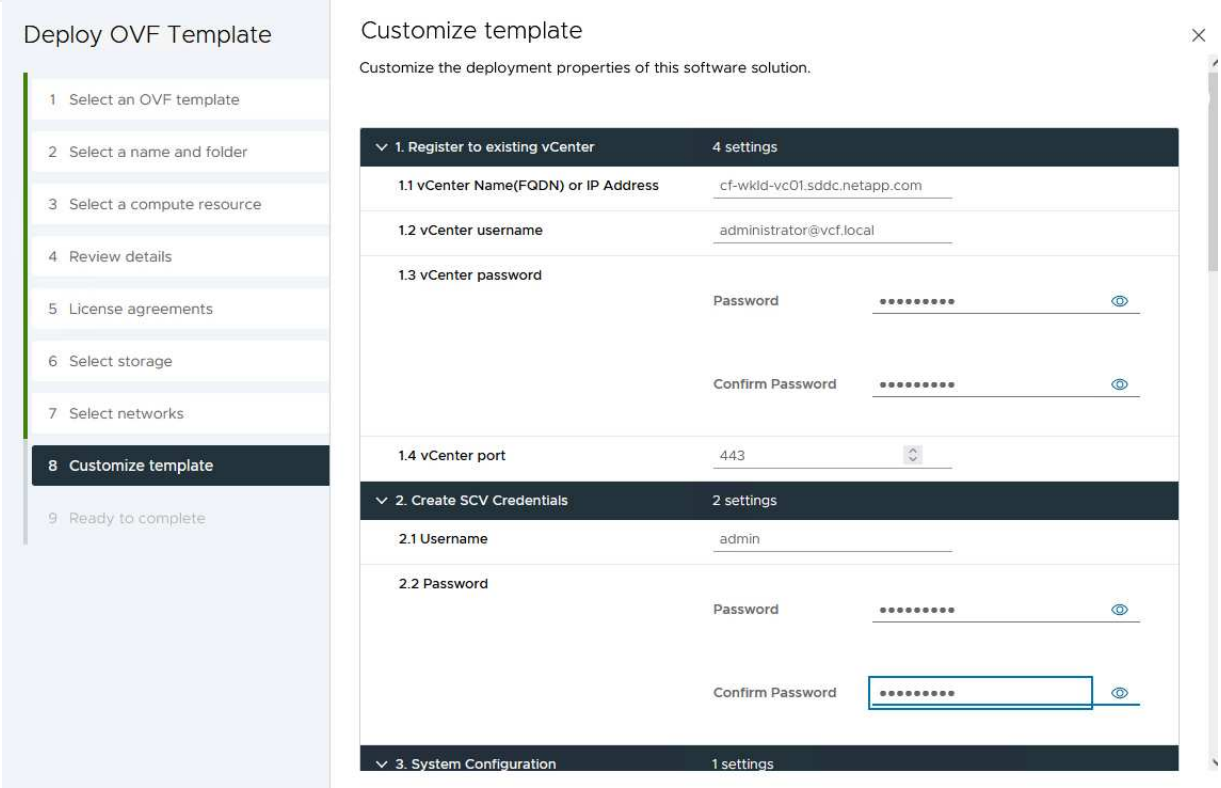


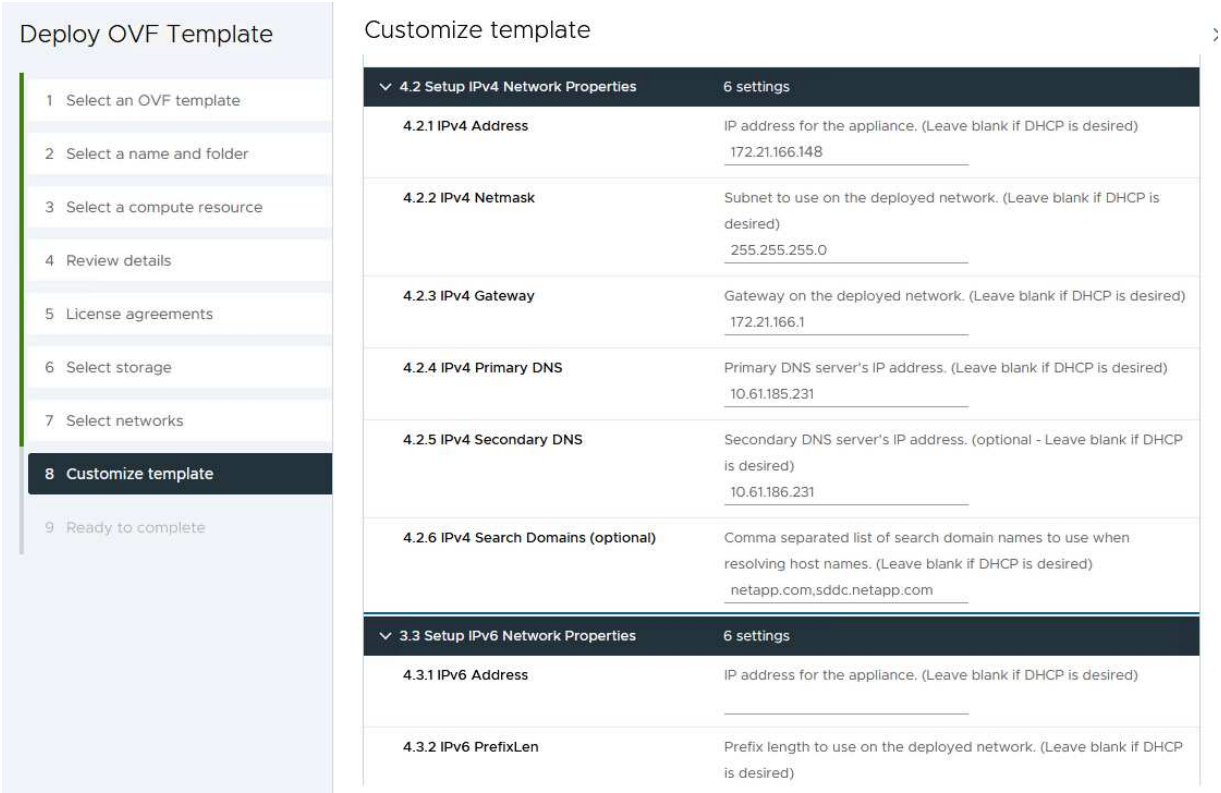
8. Na página **Selecionar rede**, selecione a rede de gerenciamento que pode se comunicar com o dispositivo vCenter do domínio de carga de trabalho e os sistemas de armazenamento ONTAP primário e secundário.

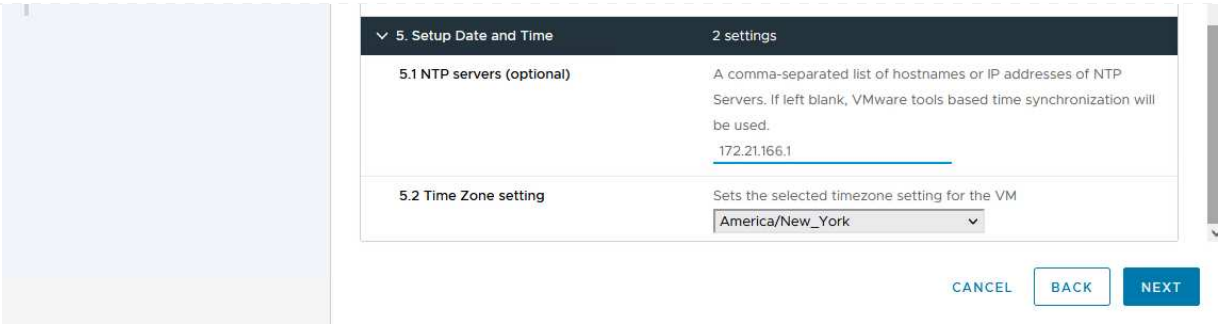


9. Na página **Personalizar modelo** preencha todas as informações necessárias para a implantação:
   - FQDN ou IP e credenciais para o domínio de carga de trabalho do dispositivo vCenter.
   - Credenciais para a conta administrativa do SCV.
   - Credenciais para a conta de manutenção do SCV.
   - Detalhes das propriedades da rede IPv4 (o IPv6 também pode ser usado).
   - Configurações de data e hora.

   Clique em **Avançar** para continuar.


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
1. Register to existing vCenter
4 settings
1.1 vCenter Name(FQDN) or IP Address
cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username
administrator@vcf.local
1.3 vCenter password
Password
Confirm Password
1.4 vCenter port
443
2. Create SCV Credentials
2 settings
2.1 Username
admin
2.2 Password
Password
Confirm Password
3. System Configuration
1 settings


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
4.2 Setup IPv4 Network Properties
6 settings
4.2.1 IPv4 Address
IP address for the appliance. (Leave blank if DHCP is desired)
172.21.166.148
4.2.2 IPv4 Netmask
Subnet to use on the deployed network. (Leave blank if DHCP is desired)
255.255.255.0
4.2.3 IPv4 Gateway
Gateway on the deployed network. (Leave blank if DHCP is desired)
172.21.166.1
4.2.4 IPv4 Primary DNS
Primary DNS server's IP address. (Leave blank if DHCP is desired)
10.61.185.231
4.2.5 IPv4 Secondary DNS
Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired)
10.61.186.231
4.2.6 IPv4 Search Domains (optional)
Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired)
netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties
6 settings
4.3.1 IPv6 Address
IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen
Prefix length to use on the deployed network. (Leave blank if DHCP is desired)

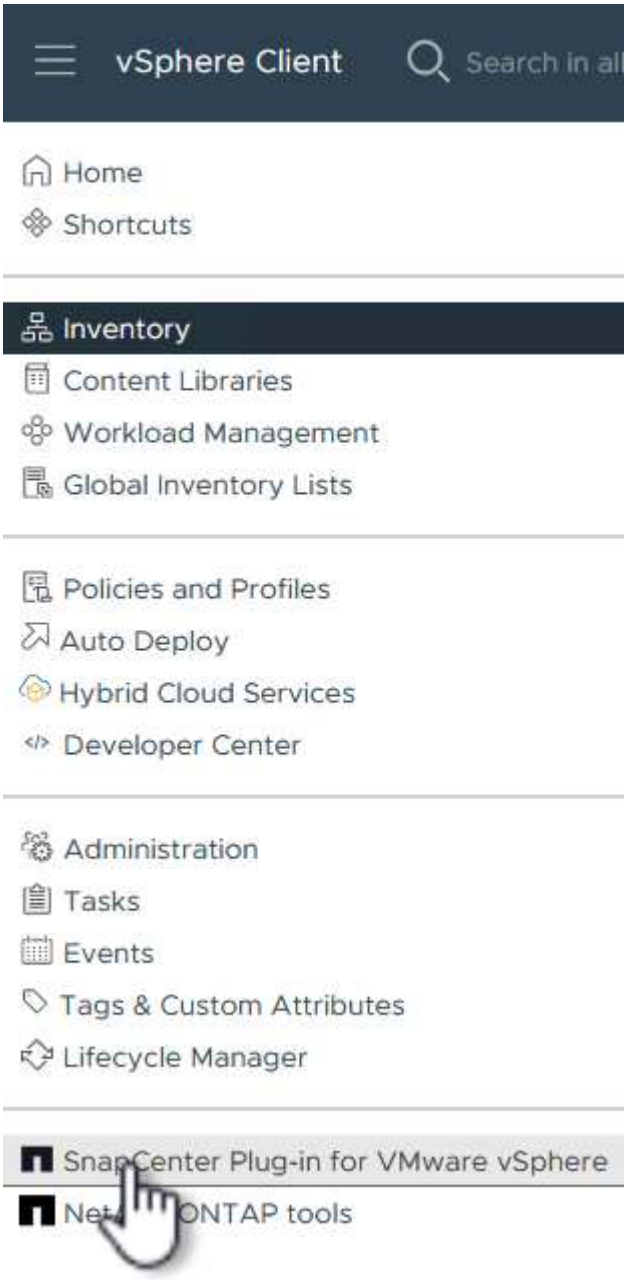


10. Por fim, na página **Pronto para concluir**, revise todas as configurações e clique em Concluir para iniciar a implantação.

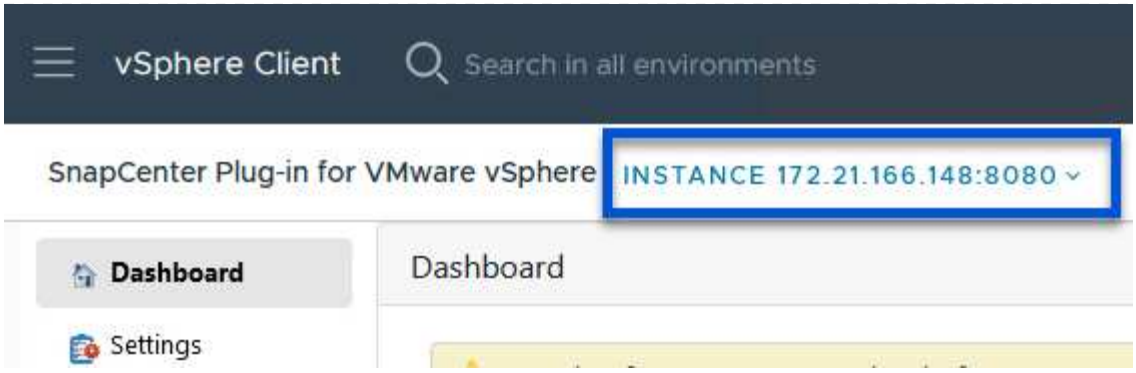
Adicionar sistemas de armazenamento ao SCV

Depois que o plug-in SnapCenter estiver instalado, conclua as seguintes etapas para adicionar sistemas de armazenamento ao SCV:

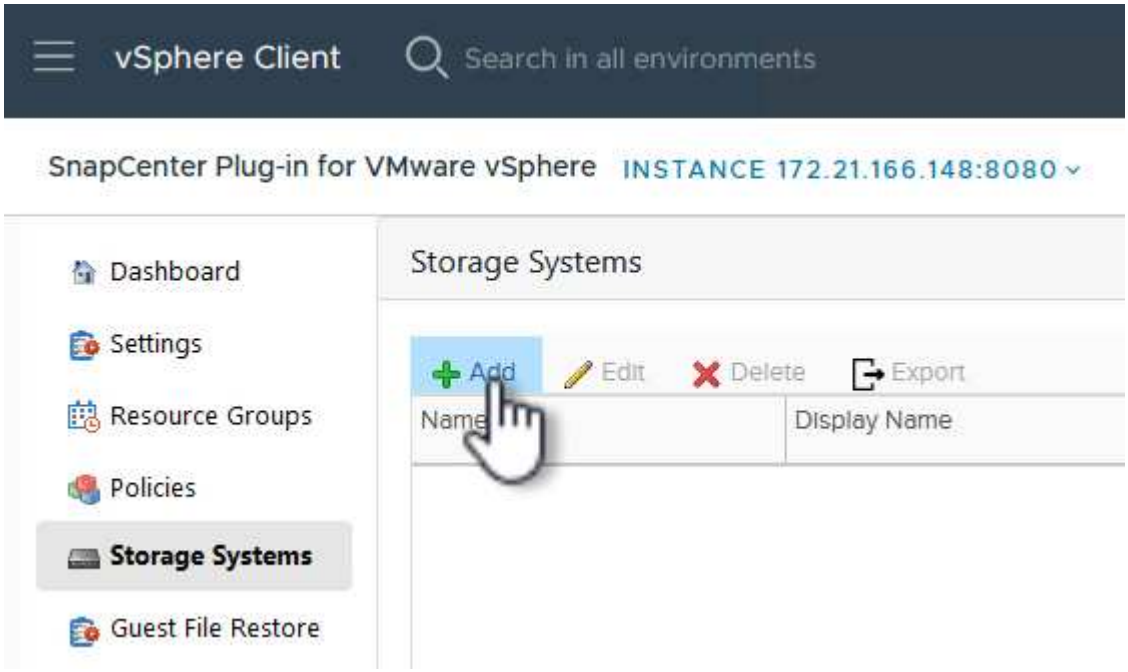
1. O SCV pode ser acessado no menu principal do vSphere Client.



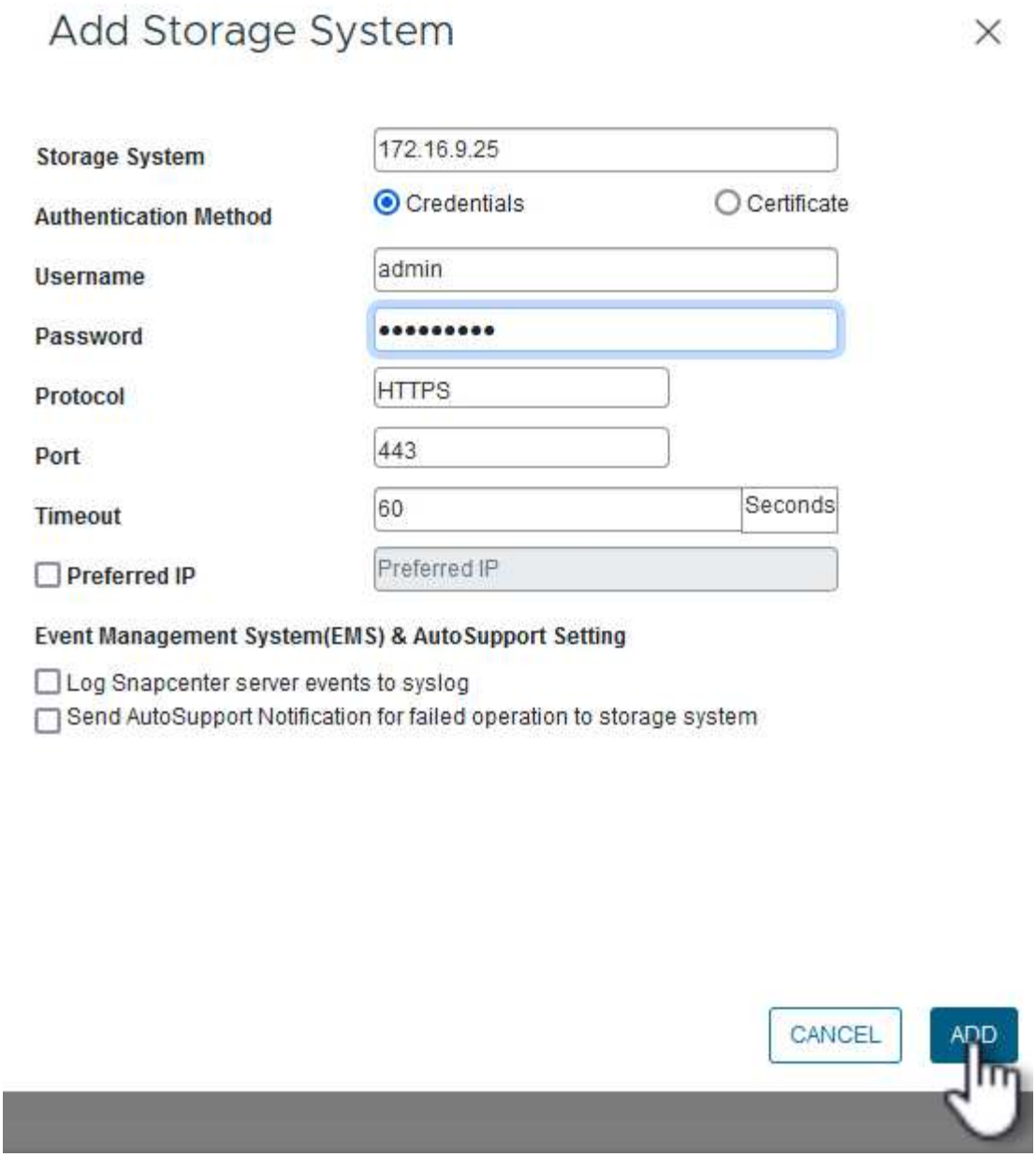
2. Na parte superior da interface do SCV UI, selecione a instância correta do SCV que corresponde ao cluster vSphere a ser protegido.



3. Navegue até **Sistemas de armazenamento** no menu à esquerda e clique em **Adicionar** para começar.



4. No formulário **Adicionar Sistema de Armazenamento**, preencha o endereço IP e as credenciais do sistema de armazenamento ONTAP a ser adicionado e clique em **Adicionar** para concluir a ação.



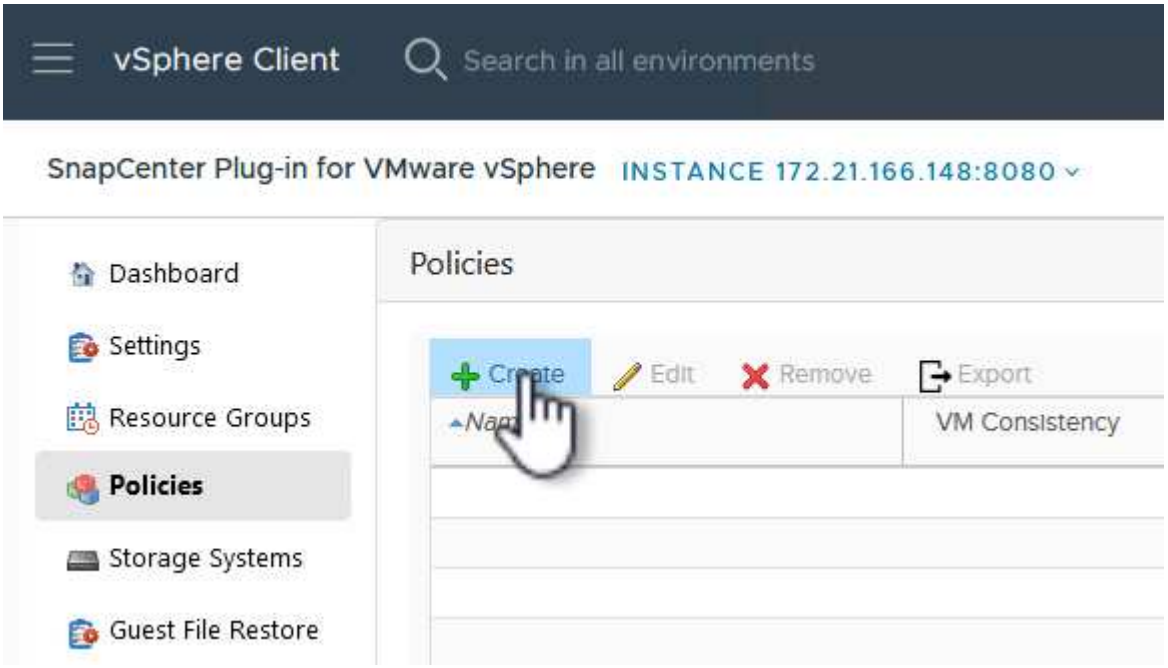
5. Repita esse procedimento para quaisquer sistemas de armazenamento adicionais a serem gerenciados, incluindo quaisquer sistemas a serem usados como destinos de backup secundários.

Configurar políticas de backup no SCV

Para obter mais informações sobre a criação de políticas de backup do SCV, consulte"Crie políticas de backup para VMs e armazenamentos de dados" .

Conclua as seguintes etapas para criar uma nova política de backup:

1. No menu à esquerda, selecione **Políticas** e clique em **Criar** para começar.



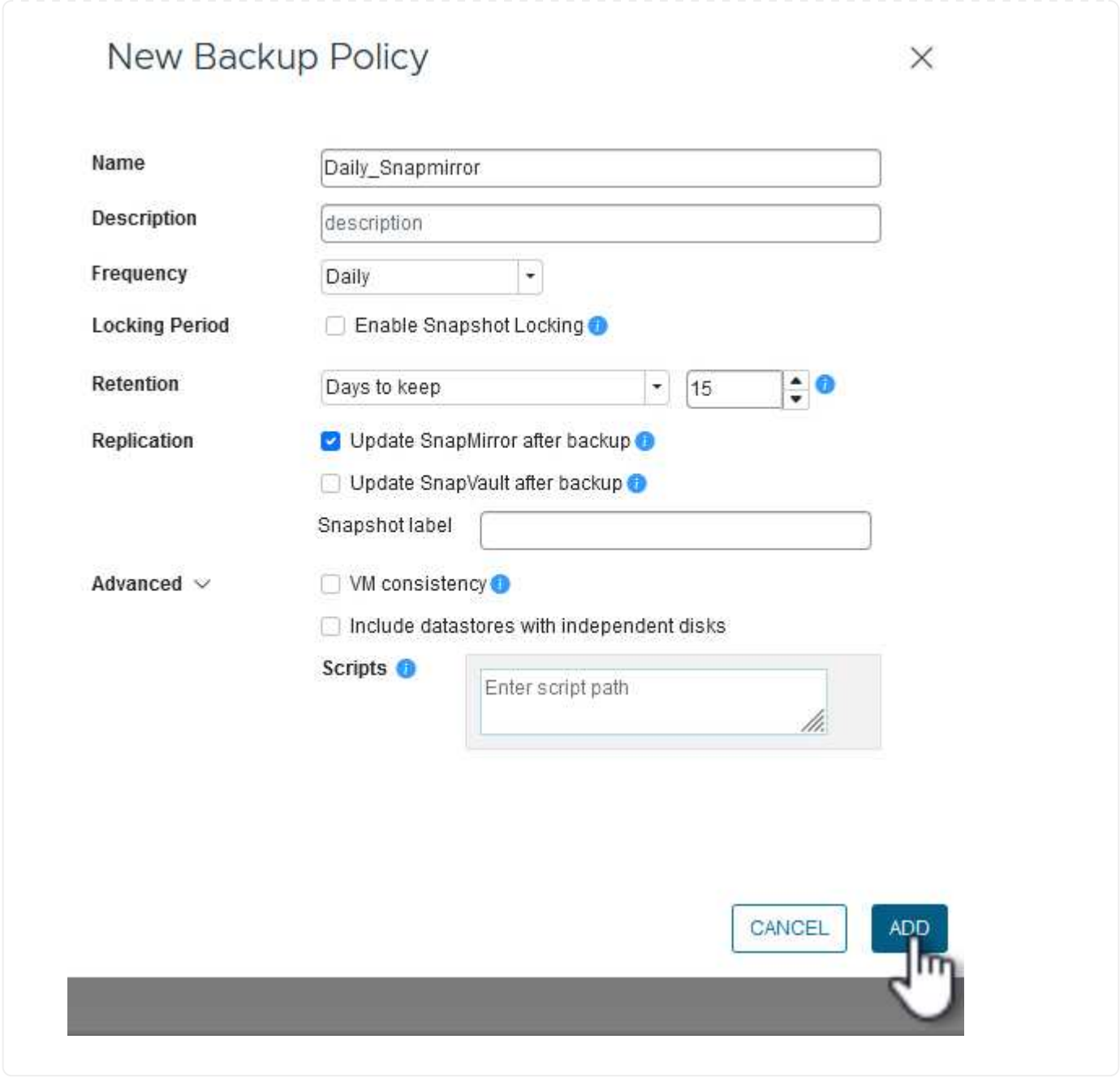
2. No formulário **Nova Política de Backup**, forneça um **Nome** e uma **Descrição** para a política, a **Frequência** em que os backups ocorrerão e o período de **Retenção** que especifica por quanto tempo o backup será retido.

   Período de bloqueio permite que o recurso ONTAP SnapLock crie instantâneos à prova de violação e permite a configuração do período de bloqueio.

   Para **Replicação** Selecione para atualizar os relacionamentos SnapMirror ou SnapVault subjacentes para o volume de armazenamento ONTAP .

   > A replicação do SnapMirror e do SnapVault são semelhantes, pois ambas utilizam a tecnologia ONTAP SnapMirror para replicar de forma assíncrona volumes de armazenamento para um sistema de armazenamento secundário para maior proteção e segurança. Para relacionamentos SnapMirror , o cronograma de retenção especificado na política de backup do SCV regerá a retenção para o volume primário e secundário. Com os relacionamentos do SnapVault , um cronograma de retenção separado pode ser estabelecido no sistema de armazenamento secundário para cronogramas de retenção de longo prazo ou diferentes. Nesse caso, o rótulo do instantâneo é especificado na política de backup do SCV e na política associada ao volume secundário, para identificar a quais volumes aplicar o cronograma de retenção independente.

   Escolha quaisquer opções avançadas adicionais e clique em **Adicionar** para criar a política.

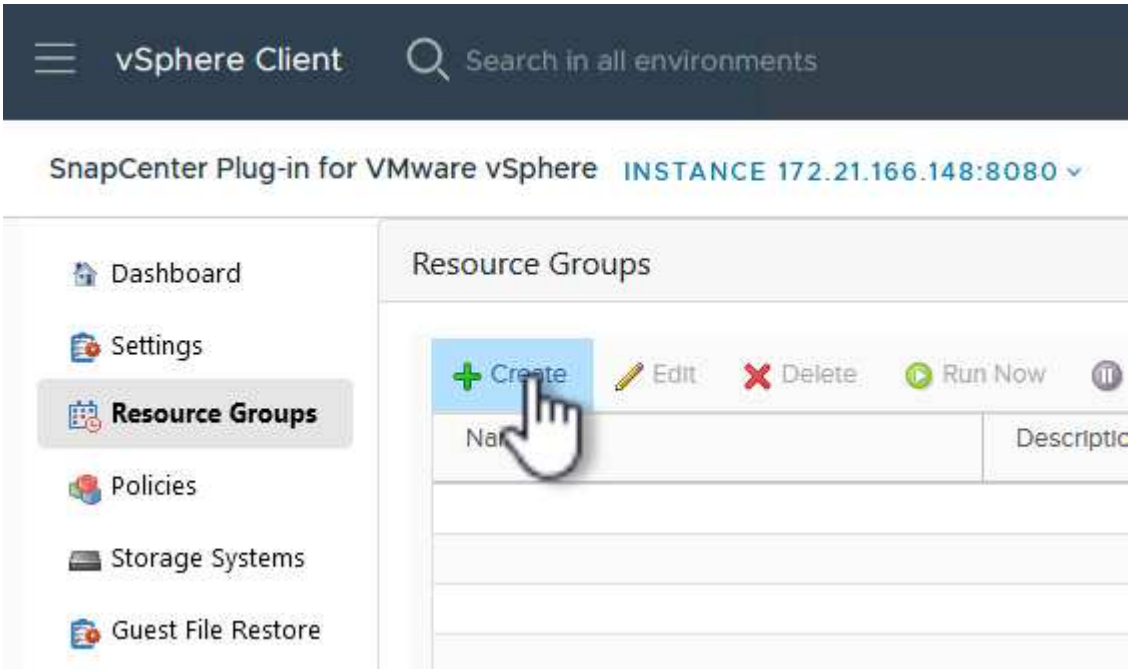

New Backup Policy
Name
Daily_Snapmirror
Description
description
Frequency
Daily
Locking Period
Enable Snapshot Locking
Retention
Days to keep
15
Replication
Update SnapMirror after backup
Update SnapVault after backup
Snapshot label
Advanced
VM consistency
Include datastores with independent disks
Scripts
Enter script path
CANCEL
ADD

Criar grupos de recursos no SCV

Para obter mais informações sobre a criação de Grupos de Recursos SCV, consulte"Criar grupos de recursos" .

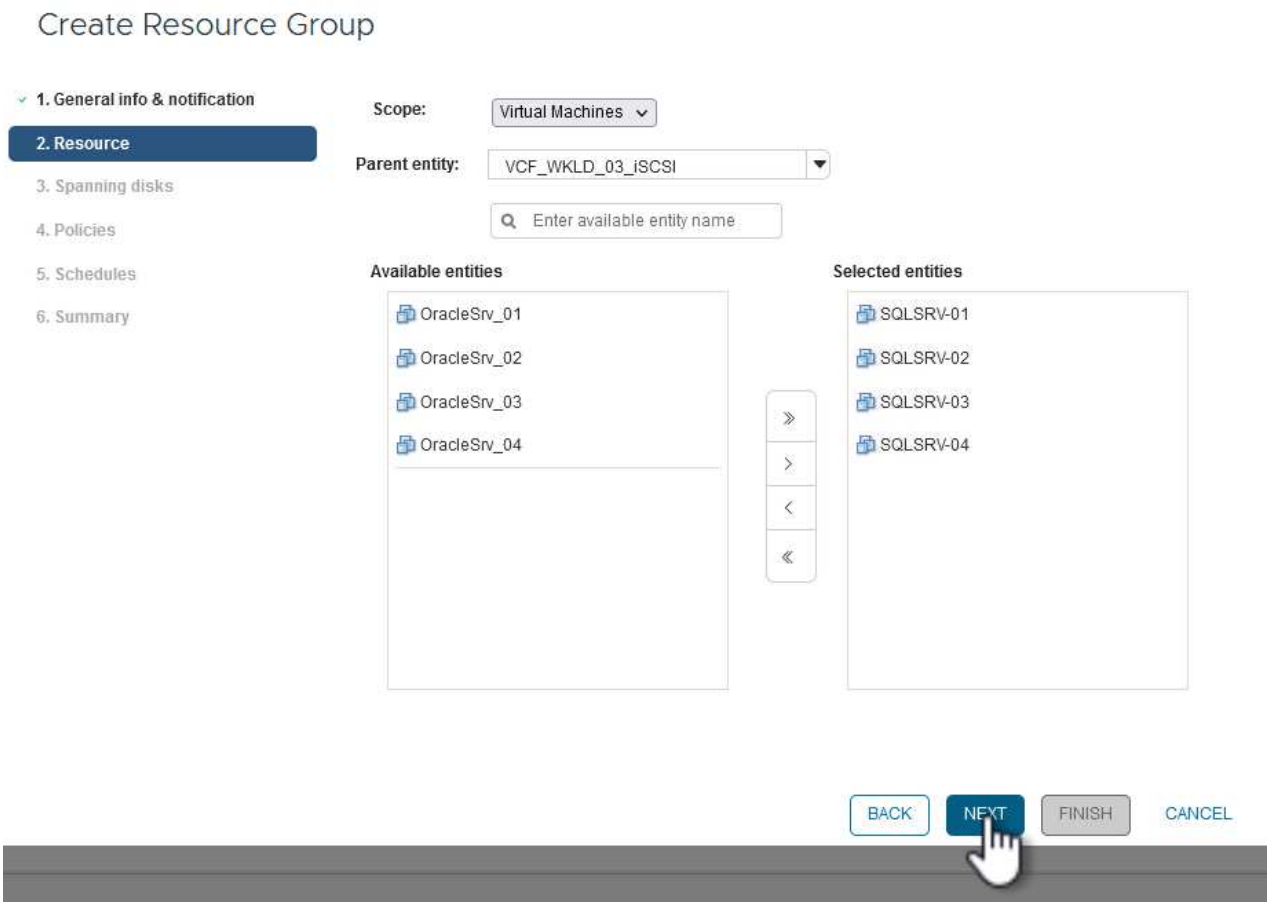
Conclua as seguintes etapas para criar um novo grupo de recursos:

1. No menu à esquerda, selecione **Grupos de recursos** e clique em **Criar** para começar.

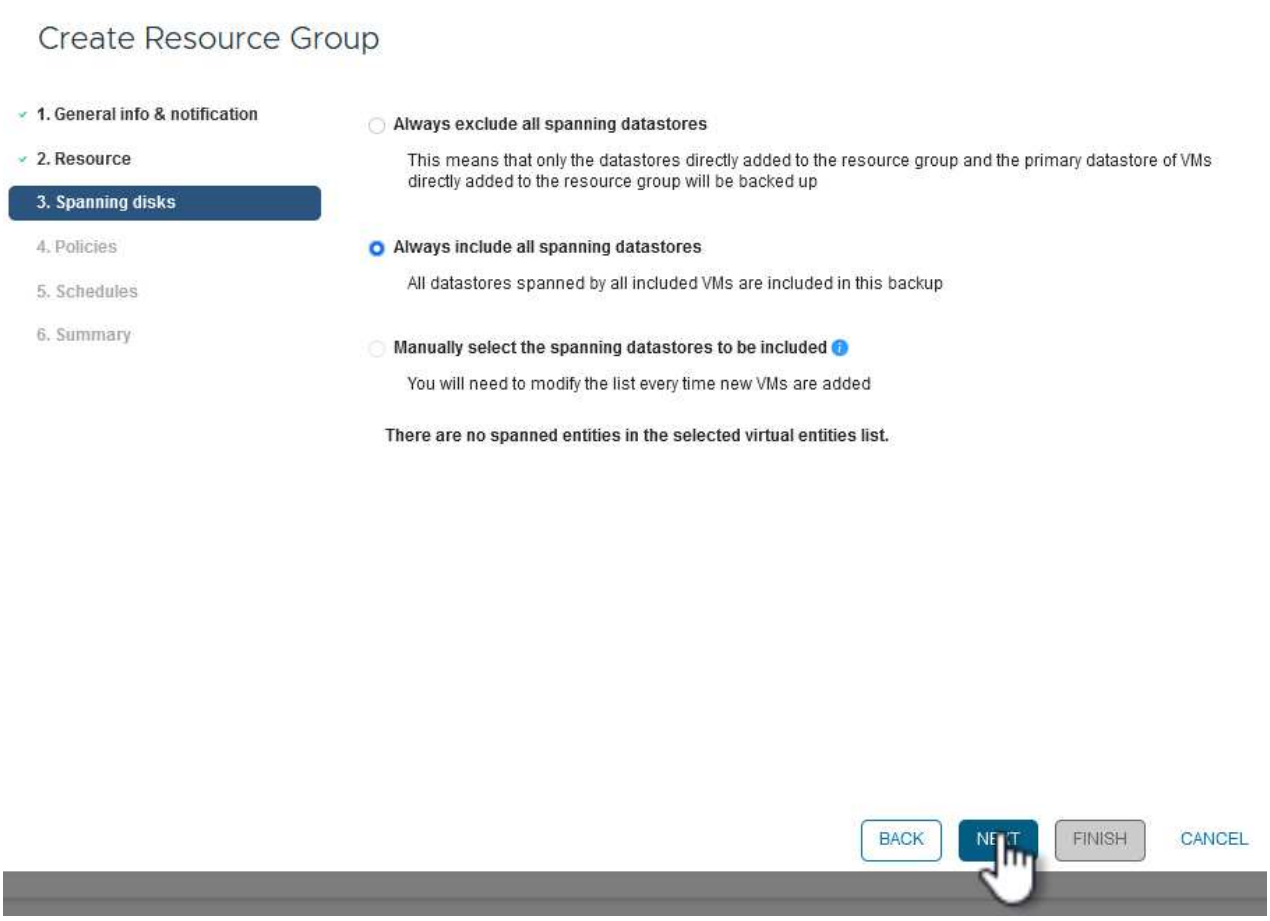


2. Na página **Informações gerais e notificação**, forneça um nome para o grupo de recursos, configurações de notificação e quaisquer opções adicionais para a nomenclatura dos instantâneos.
3. Na página **Recurso**, selecione os armazenamentos de dados e as VMs a serem protegidas no grupo de recursos. Clique em **Avançar** para continuar.

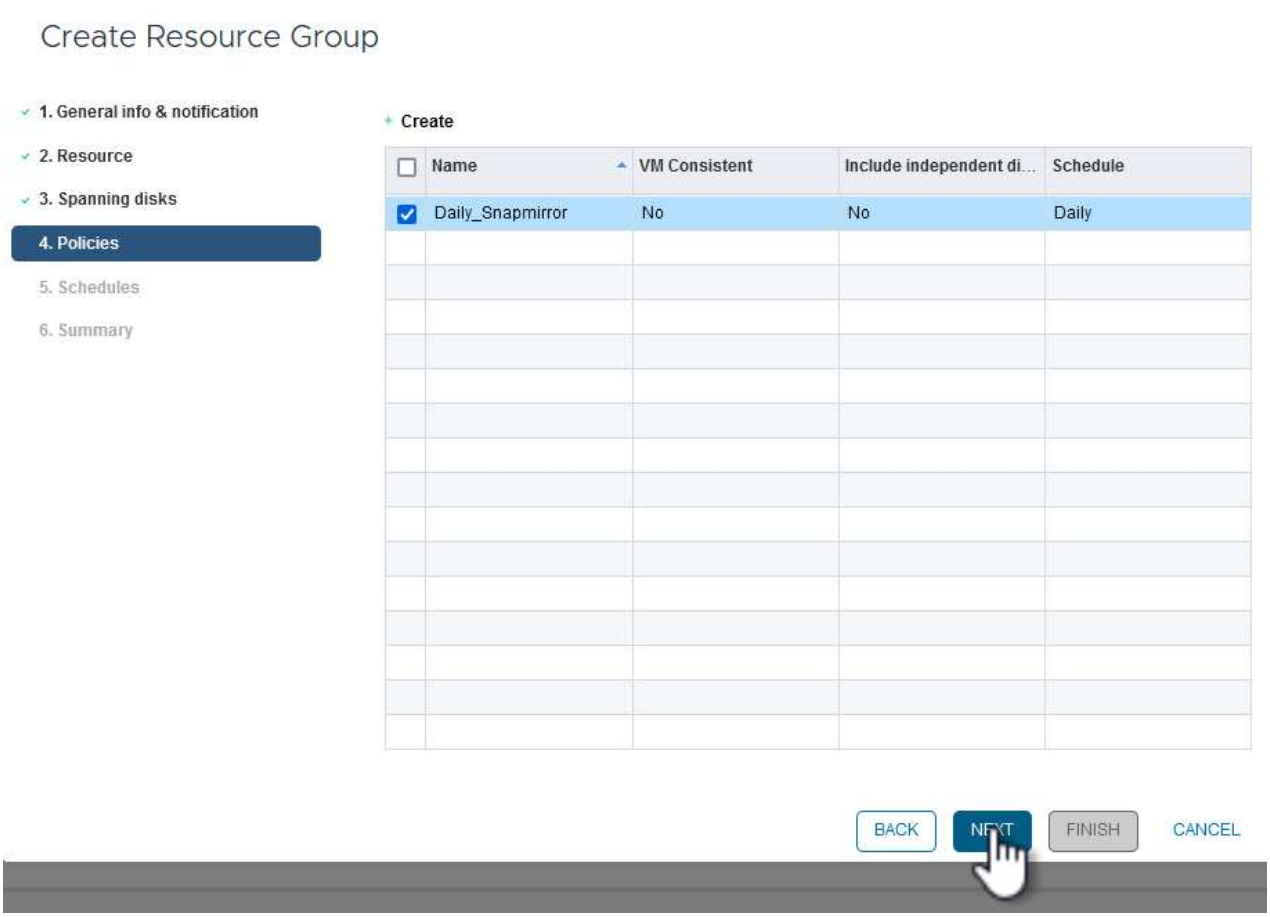
> Mesmo quando apenas VMs específicas são selecionadas, todo o armazenamento de dados sempre é feito backup. Isso ocorre porque o ONTAP tira instantâneos do volume que hospeda o armazenamento de dados. No entanto, observe que selecionar apenas VMs específicas para backup limita a capacidade de restauração apenas para essas VMs.



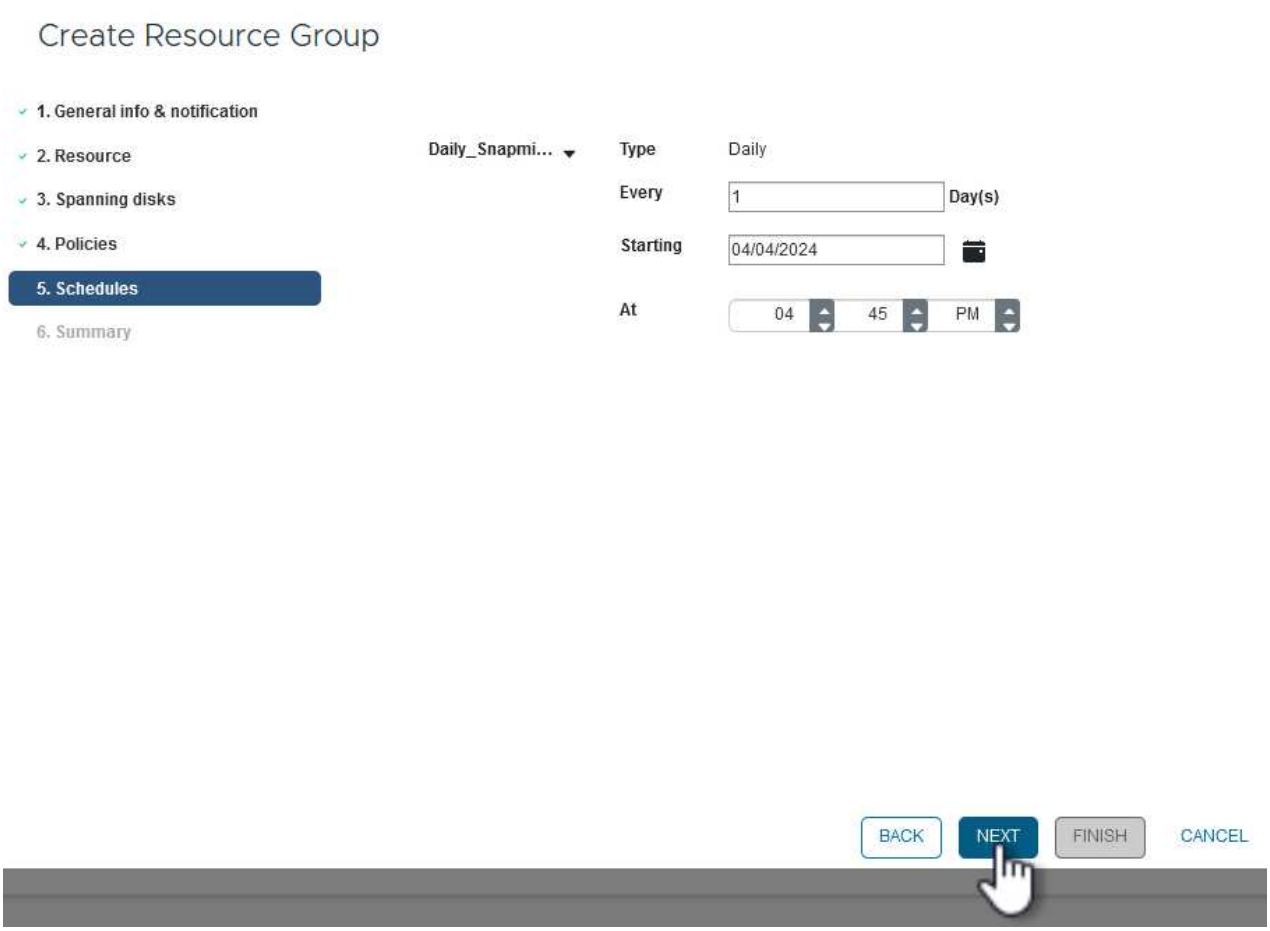
4. Na página **Discos de abrangência**, selecione a opção de como lidar com VMs com VMDKs que abrangem vários armazenamentos de dados. Clique em **Avançar** para continuar.



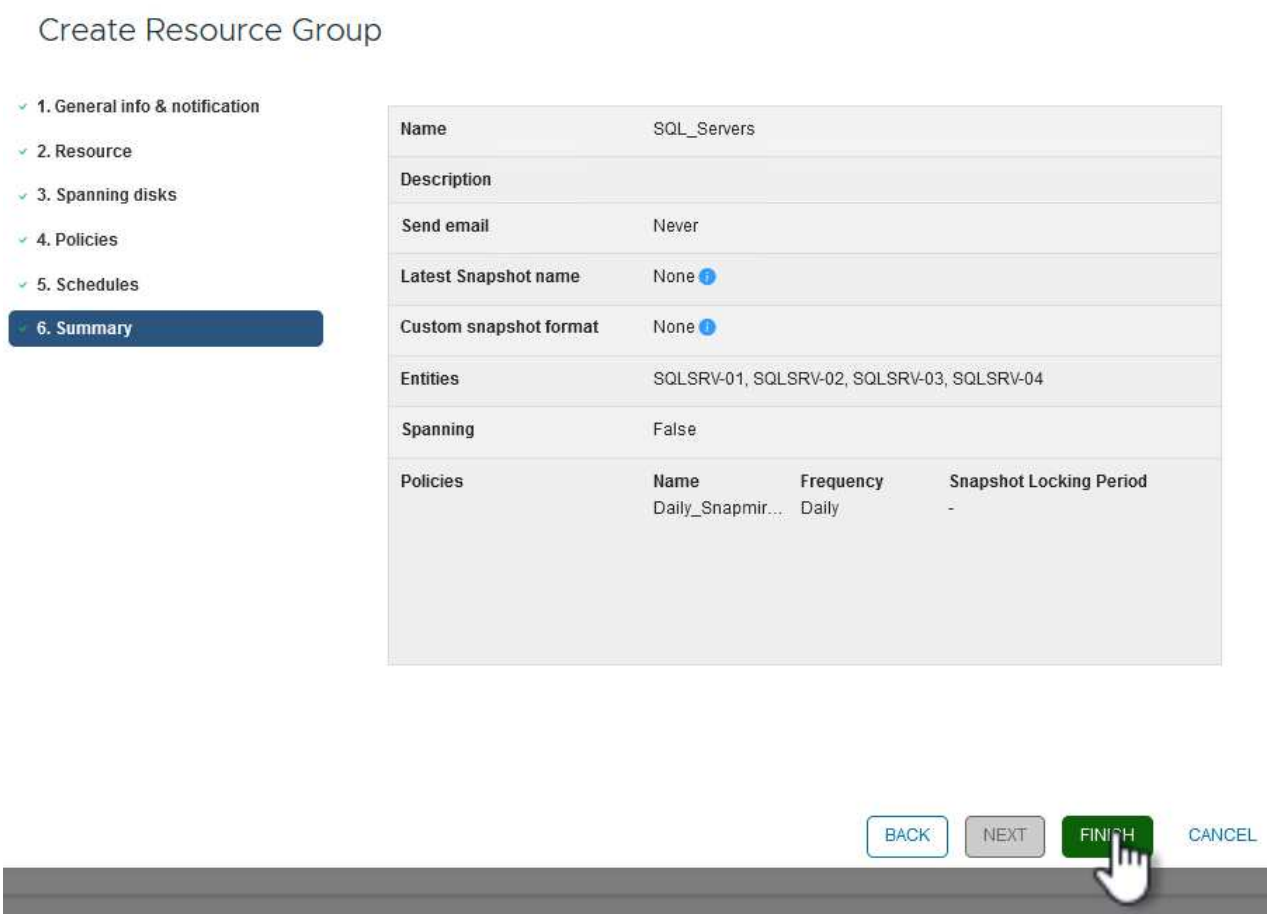
5. Na página **Políticas**, selecione uma política criada anteriormente ou várias políticas que serão usadas com este grupo de recursos. Clique em **Avançar** para continuar.



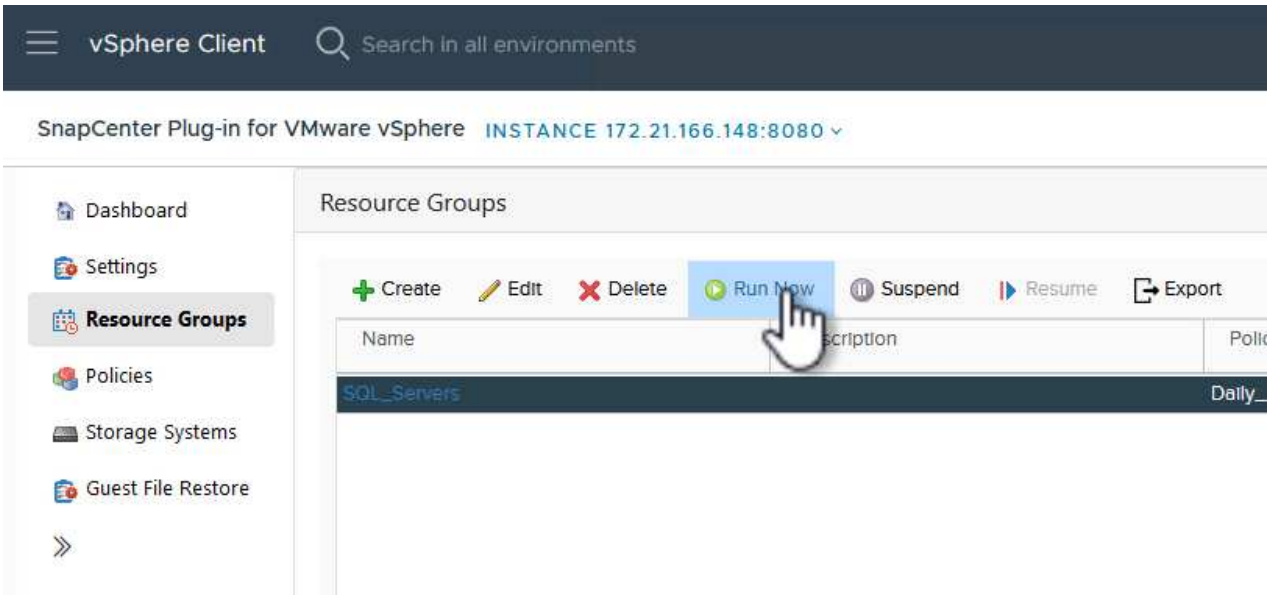
6. Na página **Agendamentos**, estabeleça quando o backup será executado configurando a recorrência e a hora do dia. Clique em **Avançar** para continuar.



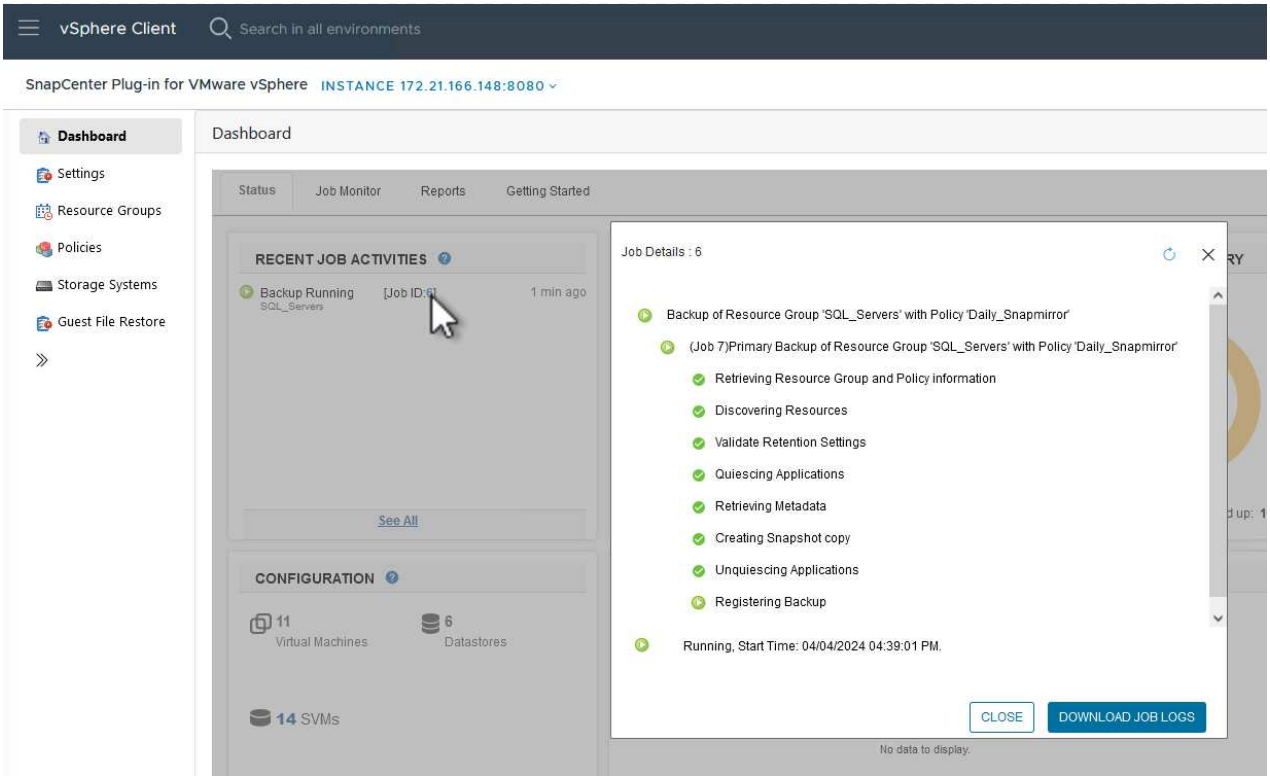
7. Por fim, revise o **Resumo** e clique em **Concluir** para criar o grupo de recursos.



8. Com o grupo de recursos criado, clique no botão **Executar agora** para executar o primeiro backup.



9. Navegue até o **Painel** e, em **Atividades recentes do trabalho**, clique no número ao lado de **ID do trabalho** para abrir o monitor de trabalhos e visualizar o andamento do trabalho em execução.



Use o SCV para restaurar VMs, VMDKs e arquivos

O plug-in SnapCenter permite restaurações de VMs, VMDKs, arquivos e pastas de backups primários ou secundários.

As VMs podem ser restauradas para o host original, para um host alternativo no mesmo vCenter Server ou para um host ESXi alternativo gerenciado pelo mesmo vCenter ou qualquer vCenter no modo vinculado.

VMs vVol podem ser restauradas para o host original.

VMDKs em VMs tradicionais podem ser restaurados no armazenamento de dados original ou em um alternativo.

VMDKs em VMs vVol podem ser restaurados para o armazenamento de dados original.

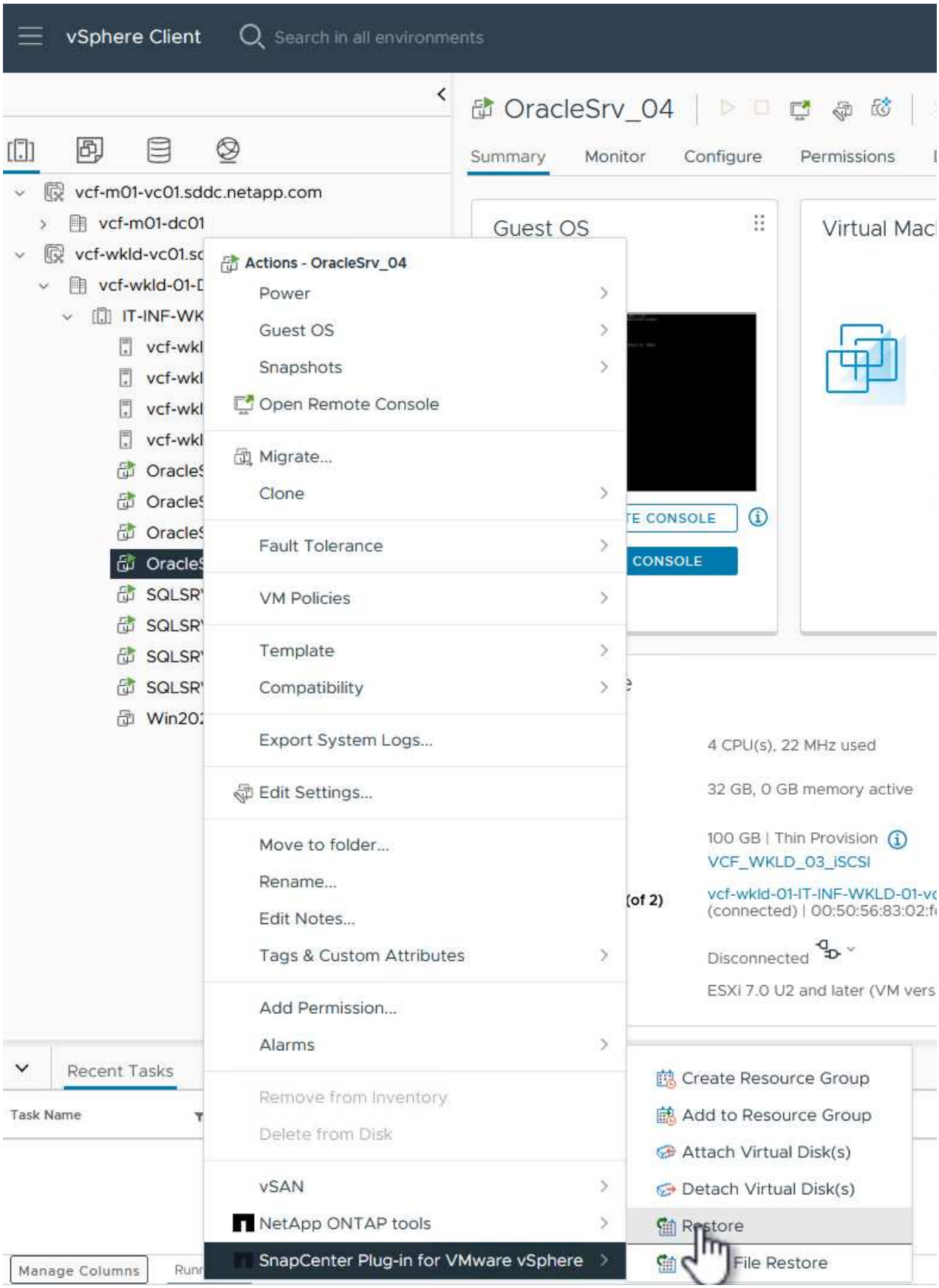
Arquivos e pastas individuais em uma sessão de restauração de arquivos de convidado podem ser restaurados, o que anexa uma cópia de backup de um disco virtual e restaura os arquivos ou pastas selecionados.

Conclua as etapas a seguir para restaurar VMs, VMDKs ou pastas individuais.

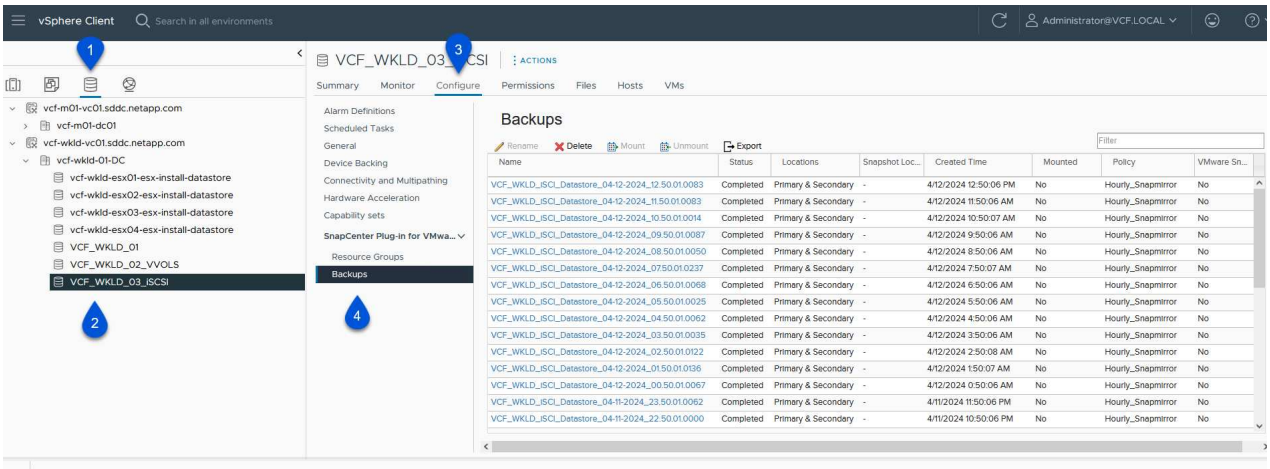
Restaurar VMs usando o plug-in SnapCenter

Conclua as seguintes etapas para restaurar uma VM com SCV:

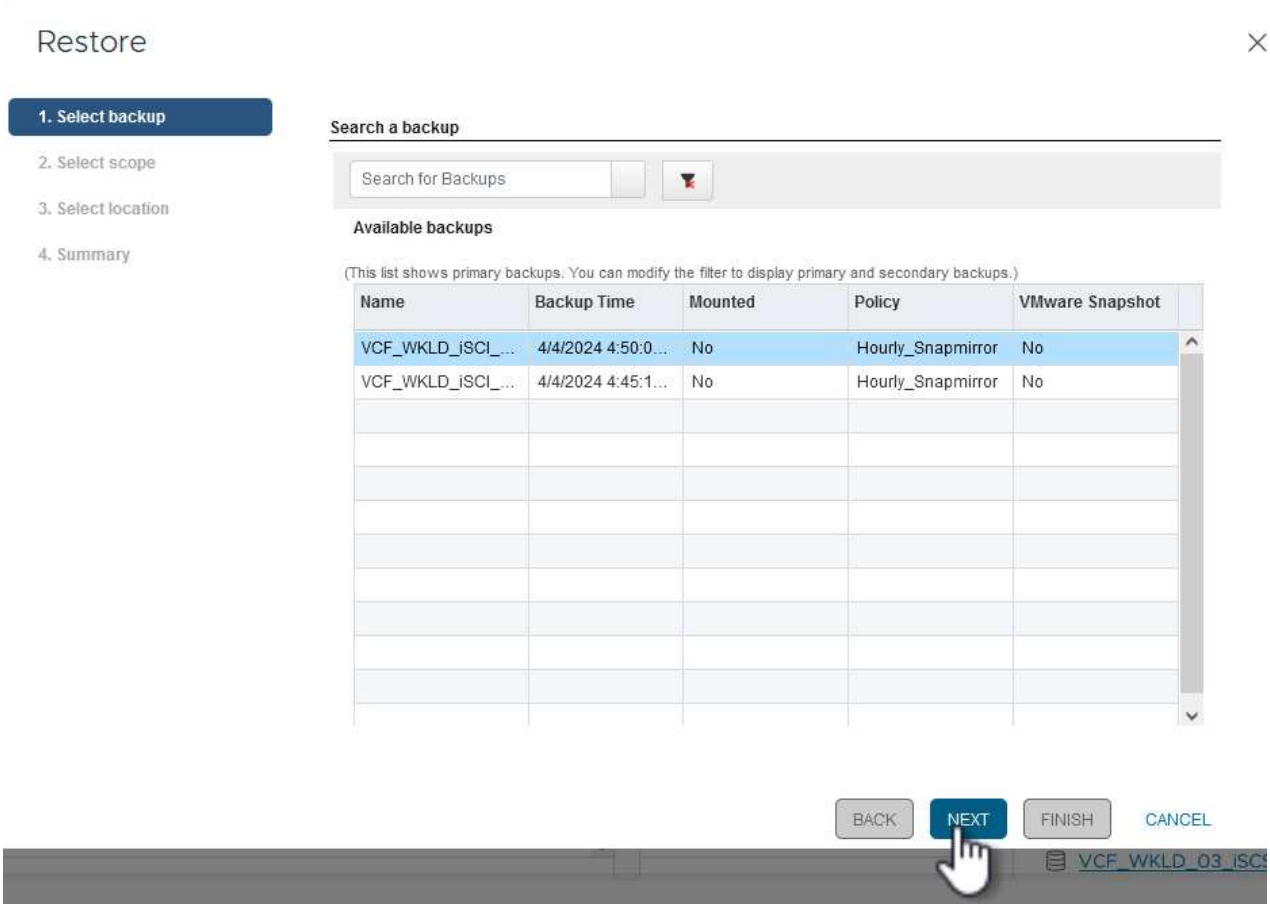
1. Navegue até a VM a ser restaurada no cliente vSphere, clique com o botão direito e navegue até * SnapCenter Plug-in for VMware vSphere*. Selecione **Restaurar** no submenu.


vSphere Client
Search in all environments
OracleSrv_04
Summary
Monitor
Configure
Permissions
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
Oracle
Oracle
Oracle
Oracle
SQLSR
SQLSR
SQLSR
SQLSR
Win20
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns

Uma alternativa é navegar até o armazenamento de dados no inventário e, na guia **Configurar**, ir para * SnapCenter Plug-in for VMware vSphere > Backups*. No backup escolhido, selecione as VMs a serem restauradas.

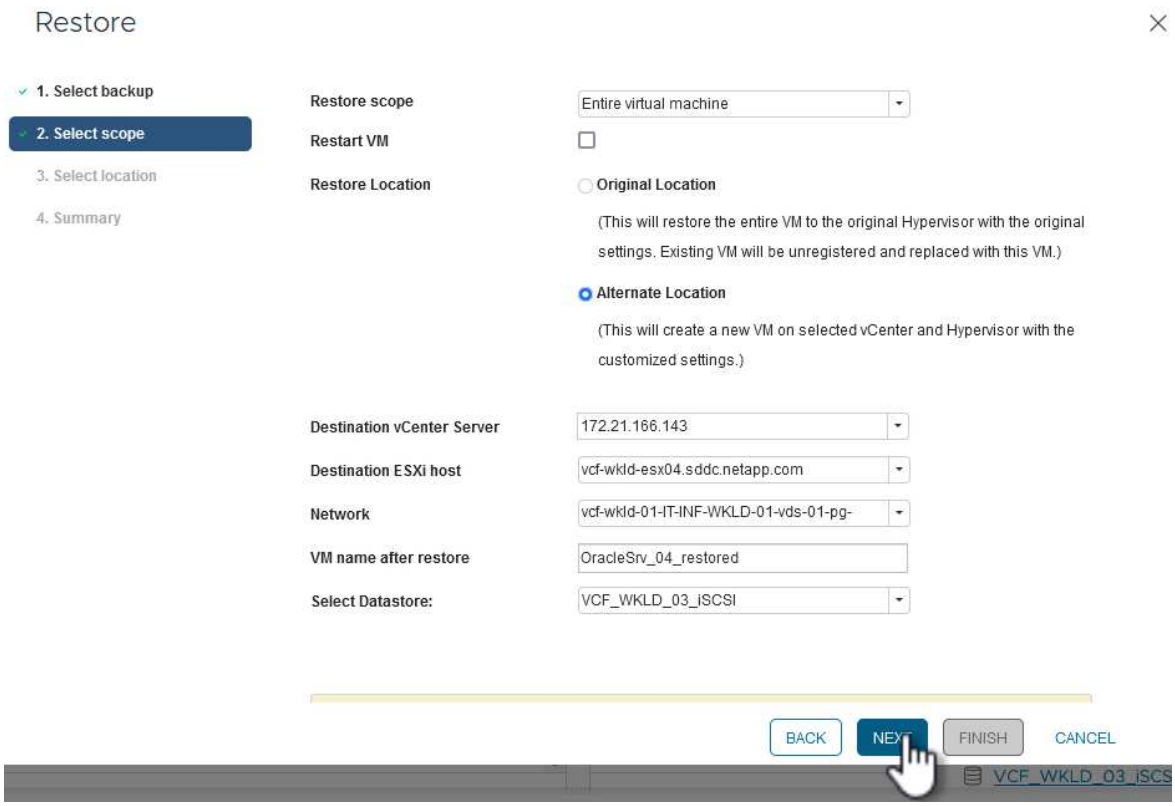


2. No assistente **Restaurar** selecione o backup a ser usado. Clique em **Avançar** para continuar.



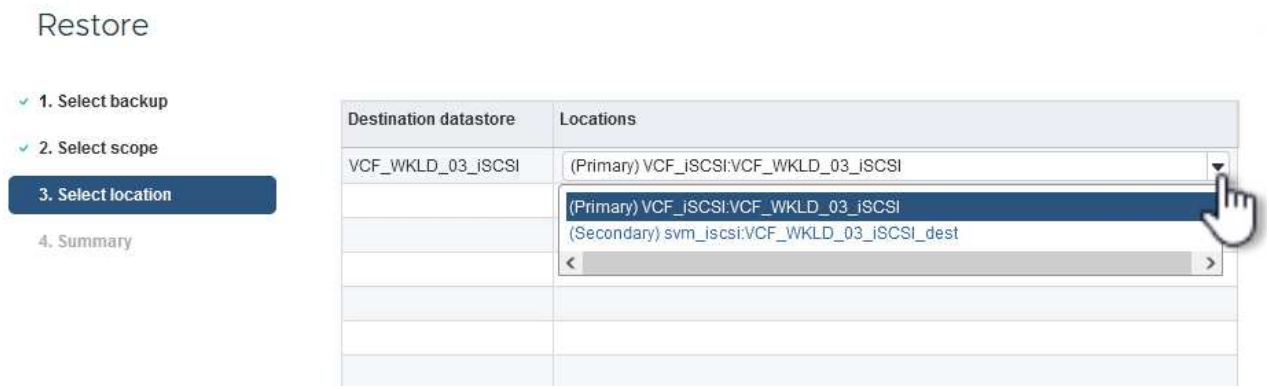
3. Na página **Selecionar escopo** preencha todos os campos obrigatórios:

- **Restaurar escopo** - Selecione para restaurar toda a máquina virtual.
- **Reiniciar VM** - Escolha se deseja iniciar a VM após a restauração.
- **Restaurar local** - Escolha restaurar para o local original ou para um local alternativo. Ao escolher o local alternativo, selecione as opções de cada um dos campos:
  - **Servidor vCenter de destino** - vCenter local ou vCenter alternativo no modo vinculado
  - **Host ESXi de destino**
  - **Rede**
  - **Nome da VM após restauração**
  - **Selecione o armazenamento de dados:**

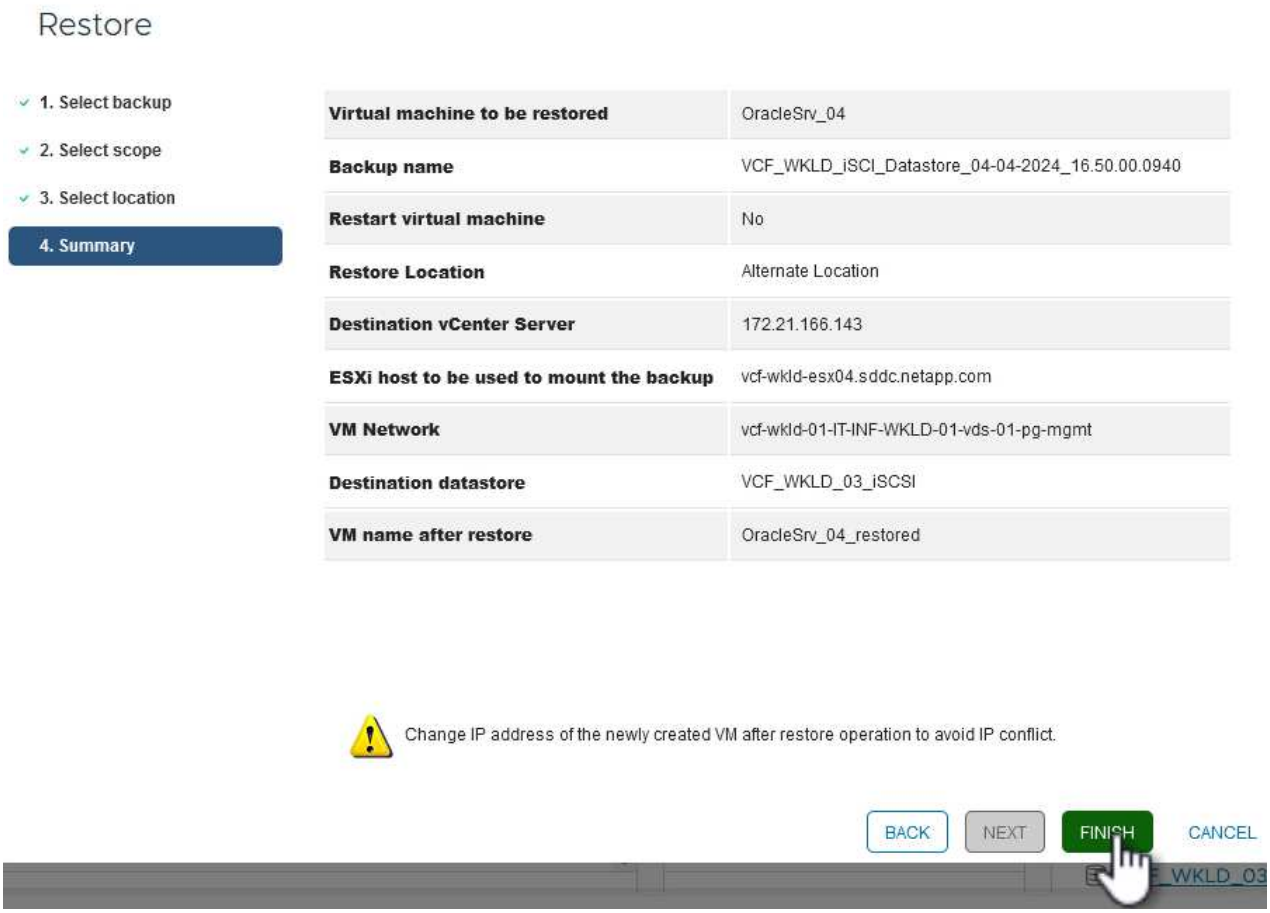


Clique em **Avançar** para continuar.

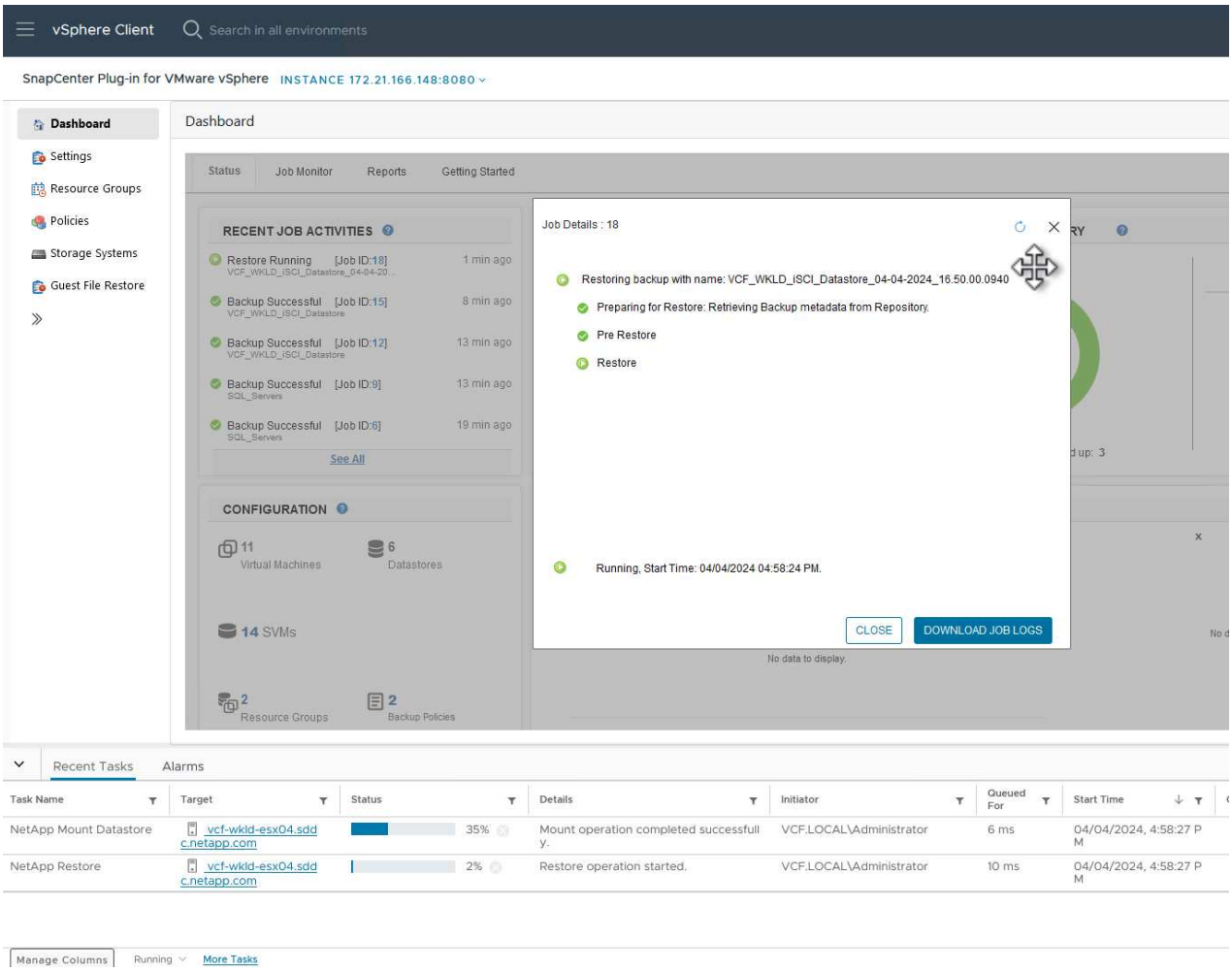
4. Na página **Selecionar local**, escolha restaurar a VM do sistema de armazenamento ONTAP primário ou secundário. Clique em **Avançar** para continuar.



5. Por fim, revise o **Resumo** e clique em **Concluir** para iniciar o trabalho de restauração.



6. O progresso do trabalho de restauração pode ser monitorado no painel **Tarefas recentes** no vSphere Client e no monitor de tarefas no SCV.

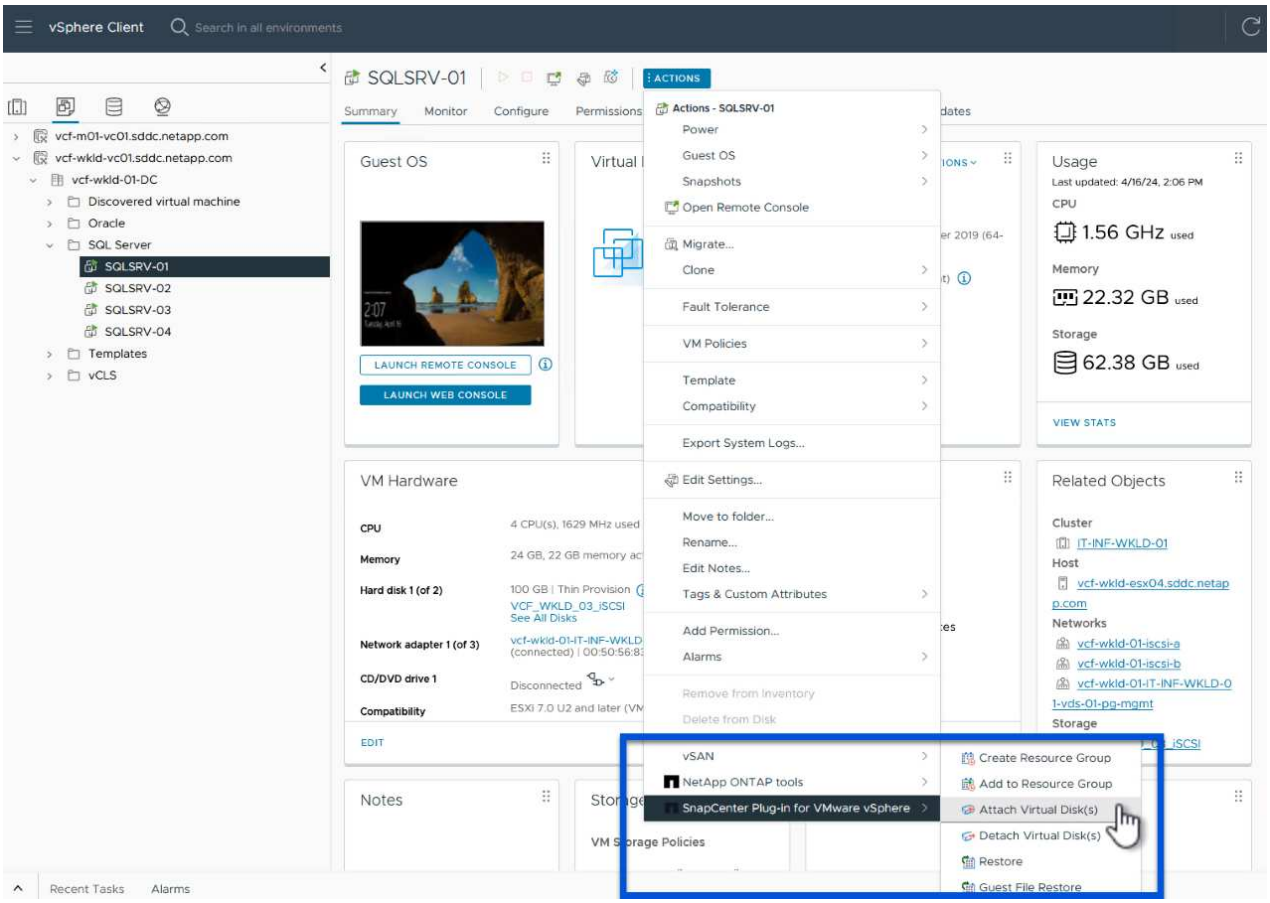

vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Dashboard
Status
Job Monitor
Reports
Getting Started
RECENT JOB ACTIVITIES
Restore Running [Job ID:18] 1 min ago
Backup Successful [Job ID:15] 8 min ago
Backup Successful [Job ID:12] 13 min ago
Backup Successful [Job ID:9] 13 min ago
Backup Successful [Job ID:6] 19 min ago
See All
CONFIGURATION
11 Virtual Machines
6 Datastores
14 SVMs
2 Resource Groups
2 Backup Policies
Job Details : 18
Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Preparing for Restore: Retrieving Backup metadata from Repository.
Pre Restore
Restore
Running, Start Time: 04/04/2024 04:58:24 PM.
CLOSE
DOWNLOAD JOB LOGS
No data to display.
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
NetApp Mount Datastore
vcf-wkld-esx04.sddc.netapp.com
35%
Mount operation completed successfully.
VCF.LOCAL\Administrator
6 ms
04/04/2024, 4:58:27 PM
NetApp Restore
vcf-wkld-esx04.sddc.netapp.com
2%
Restore operation started.
VCF.LOCAL\Administrator
10 ms
04/04/2024, 4:58:27 PM
Manage Columns
Running
More Tasks

Restaurar VMDKs usando o plug-in SnapCenter

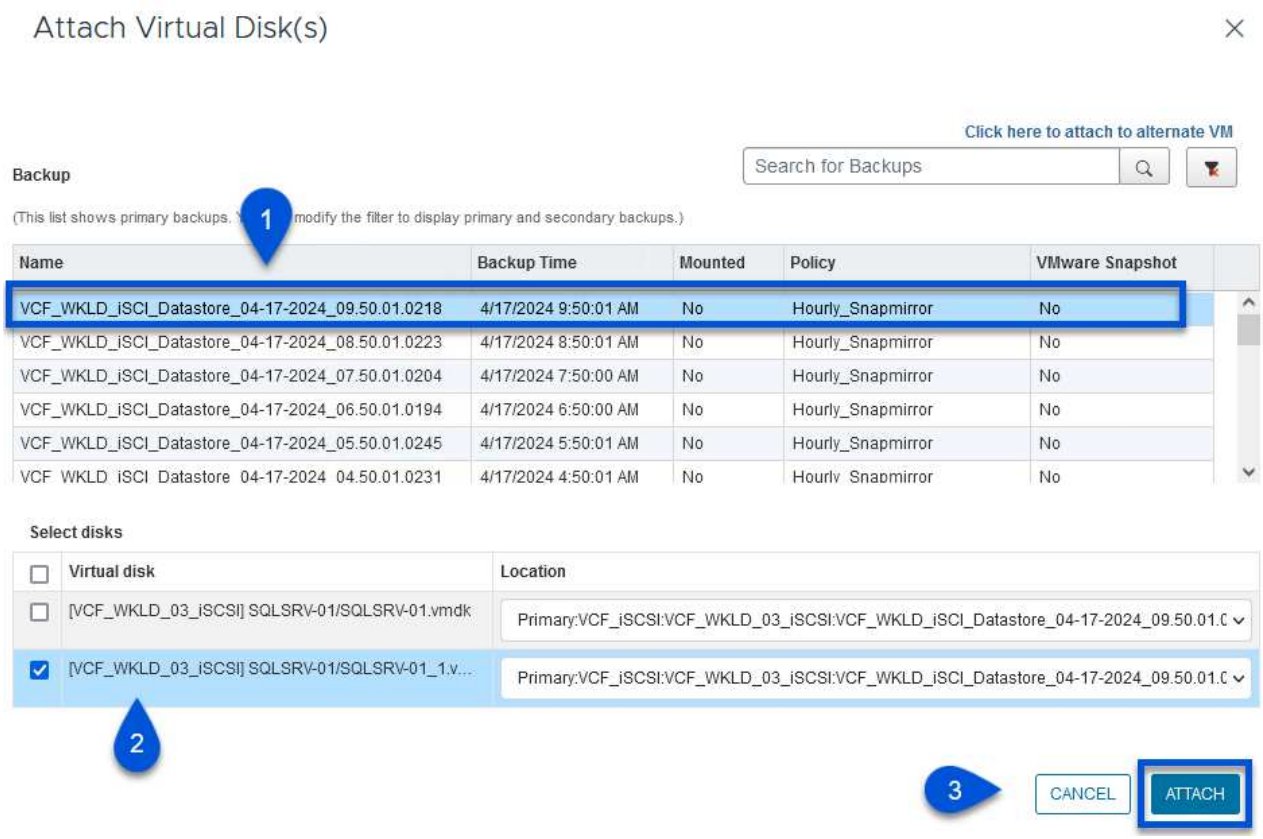
O ONTAP Tools permite a restauração completa de VMDKs para seu local original ou a capacidade de anexar um VMDK como um novo disco a um sistema host. Neste cenário, um VMDK será anexado a um host Windows para acessar o sistema de arquivos.

Para anexar um VMDK de um backup, conclua as seguintes etapas:

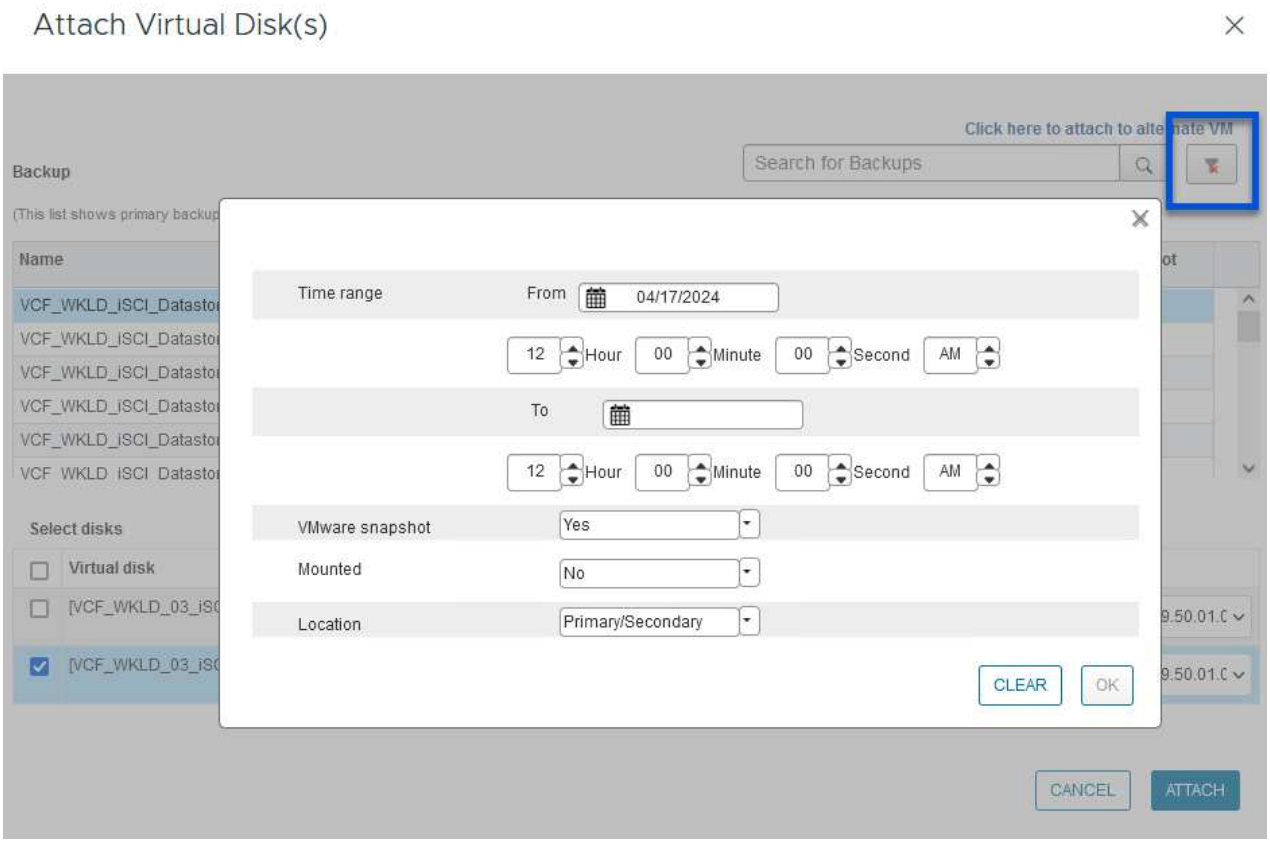
1. No vSphere Client, navegue até uma VM e, no menu **Ações**, selecione * SnapCenter Plug-in for VMware vSphere > Anexar disco(s) virtual(is)*.



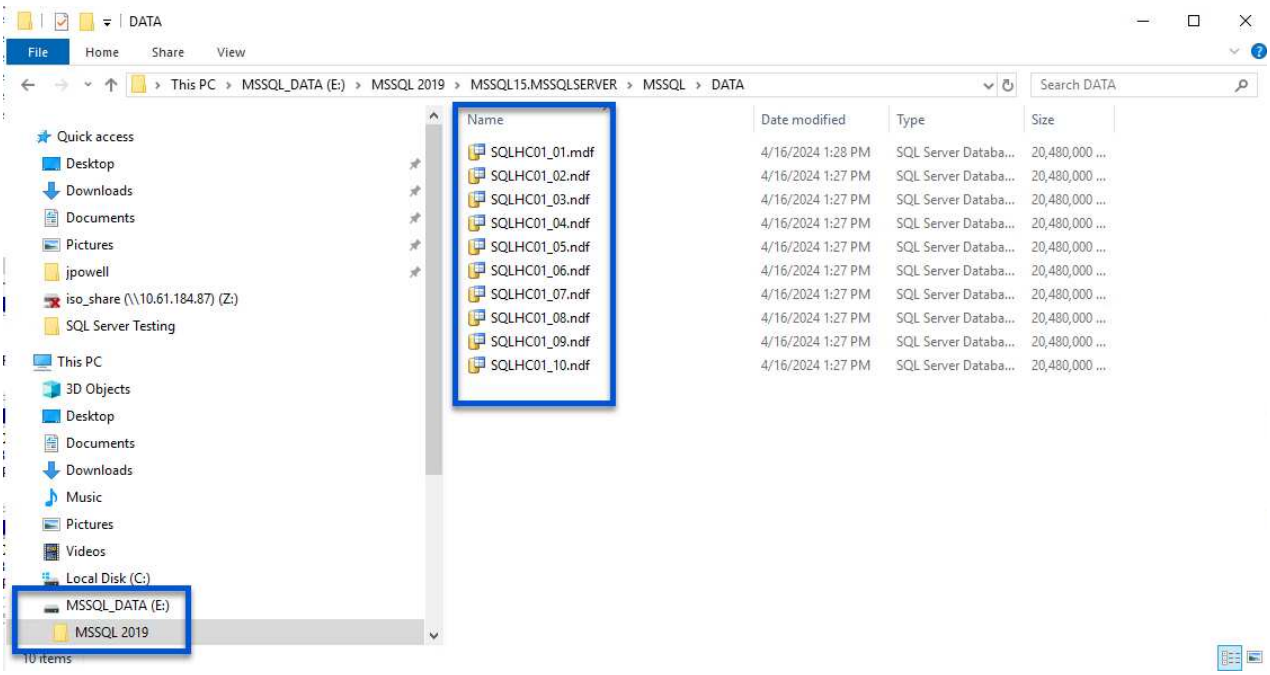
2. No assistente **Anexar disco(s) virtual(is)**, selecione a instância de backup a ser usada e o VMDK específico a ser anexado.



As opções de filtro podem ser usadas para localizar backups e exibir backups de sistemas de armazenamento primário e secundário.



3. Depois de selecionar todas as opções, clique no botão **Anexar** para iniciar o processo de restauração e anexar o VMDK ao host.
4. Após a conclusão do procedimento de anexação, o disco poderá ser acessado a partir do sistema operacional do host. Neste caso, o SCV anexou o disco com seu sistema de arquivos NTFS à unidade E: do nosso Windows SQL Server e os arquivos de banco de dados SQL no sistema de arquivos podem ser acessados pelo Explorador de Arquivos.



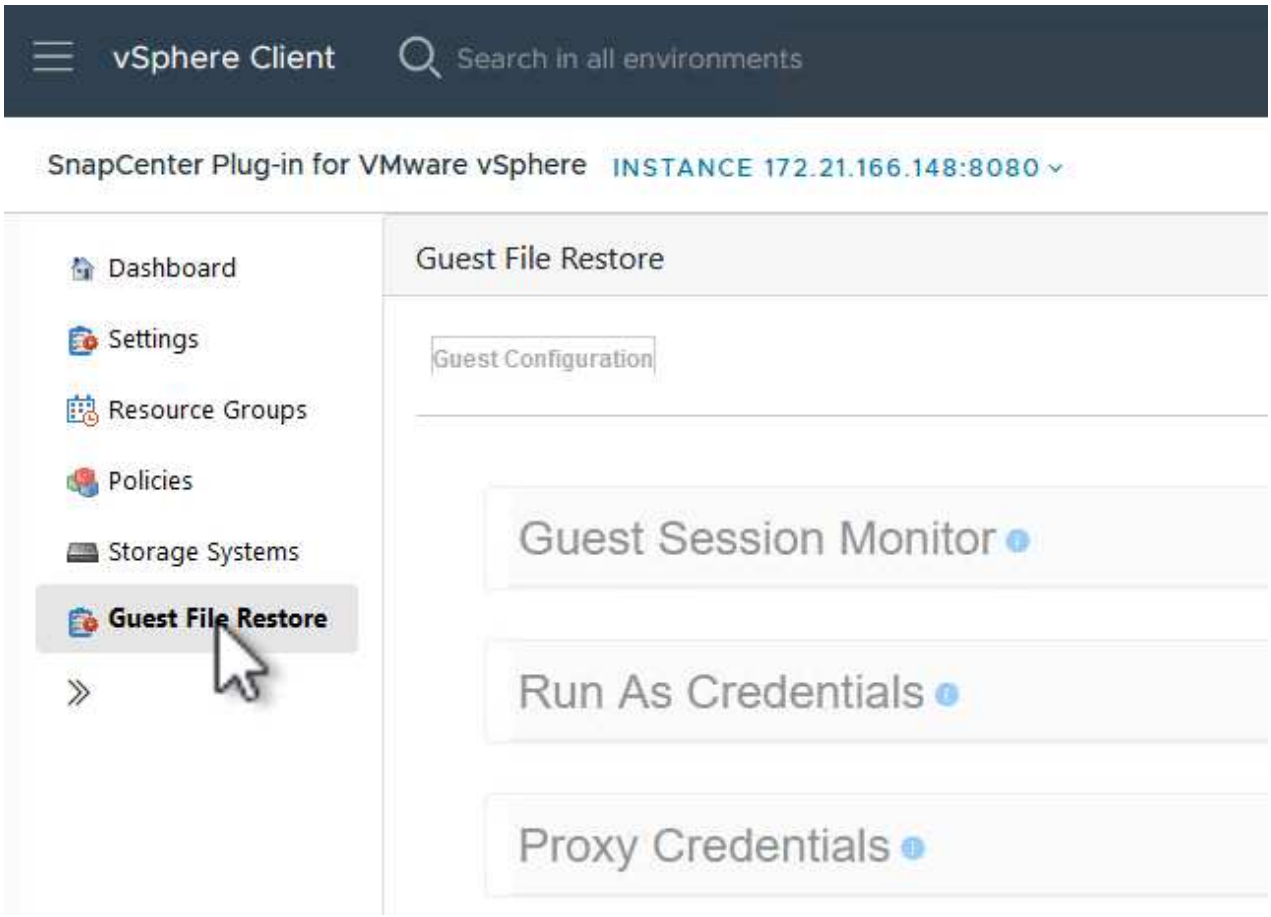
Restauração do sistema de arquivos convidado usando o plug-in SnapCenter

O ONTAP Tools oferece restaurações de sistemas de arquivos convidados a partir de um VMDK em sistemas operacionais Windows Server. Isso é realizado centralmente a partir da interface do plug-in SnapCenter .

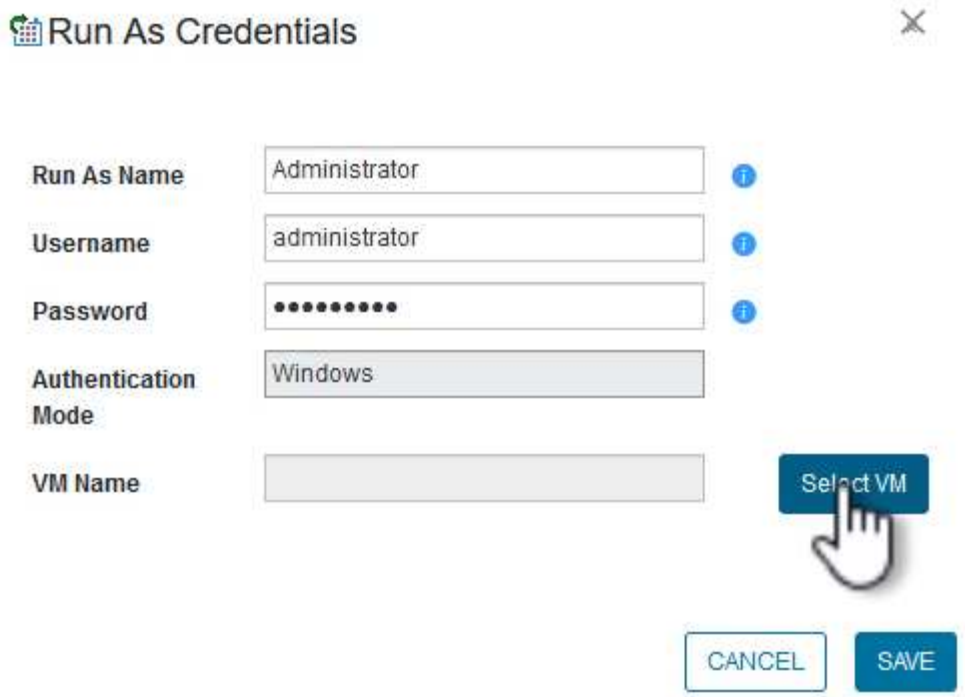
Para obter informações detalhadas, consulte"Restaurar arquivos e pastas de convidados" no site de documentação do SCV.

Para executar uma restauração do sistema de arquivos convidado para um sistema Windows, conclua as seguintes etapas:

1. O primeiro passo é criar credenciais Executar Como para fornecer acesso ao sistema host Windows. No vSphere Client, navegue até a interface do plug-in CSV e clique em **Guest File Restore** no menu principal.

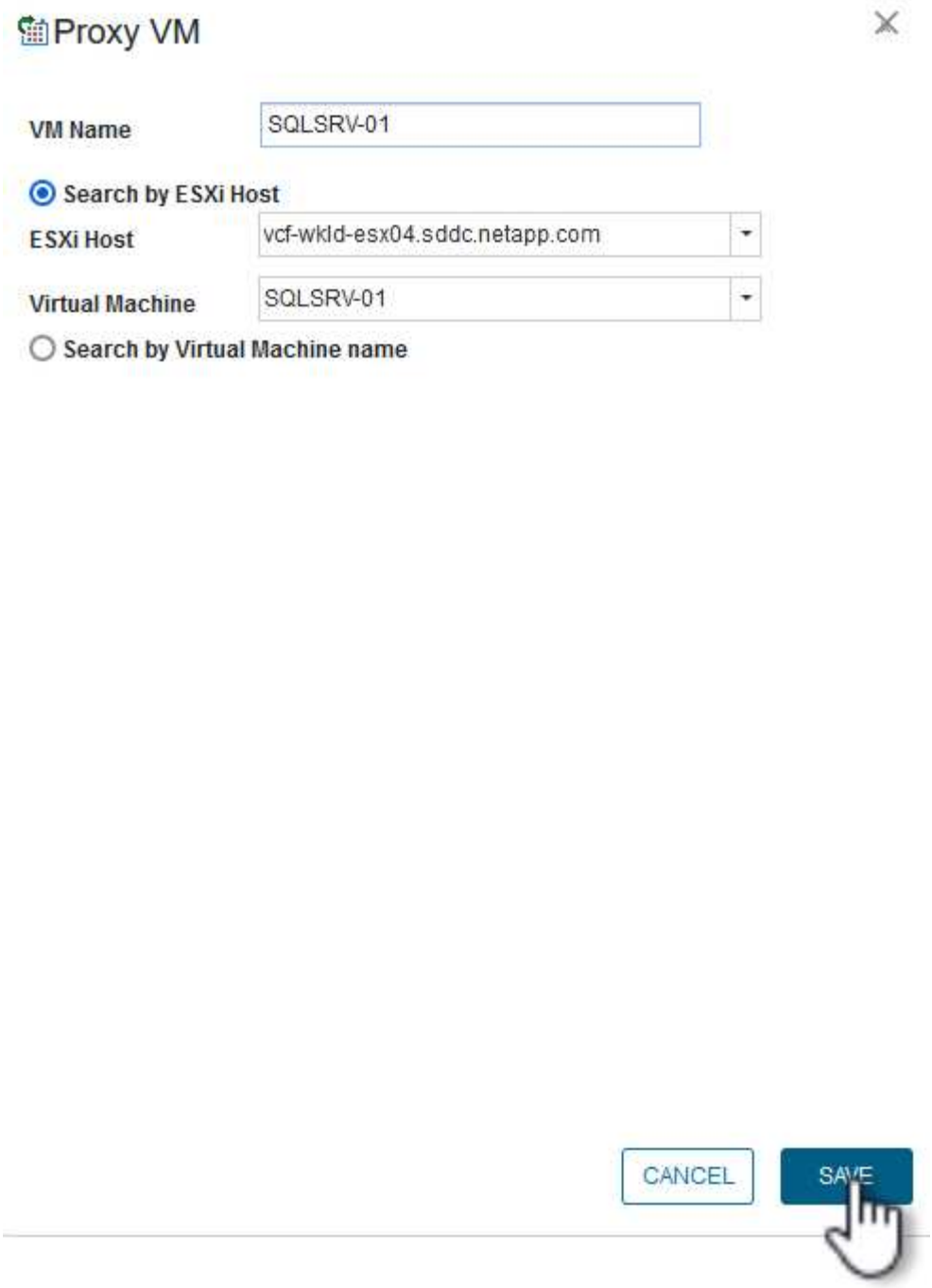


2. Em **Executar como credenciais**, clique no ícone **+** para abrir a janela **Executar como credenciais**.
3. Preencha um nome para o registro de credenciais, um nome de usuário e uma senha de administrador para o sistema Windows e, em seguida, clique no botão **Selecionar VM** para selecionar uma VM proxy opcional a ser usada para a

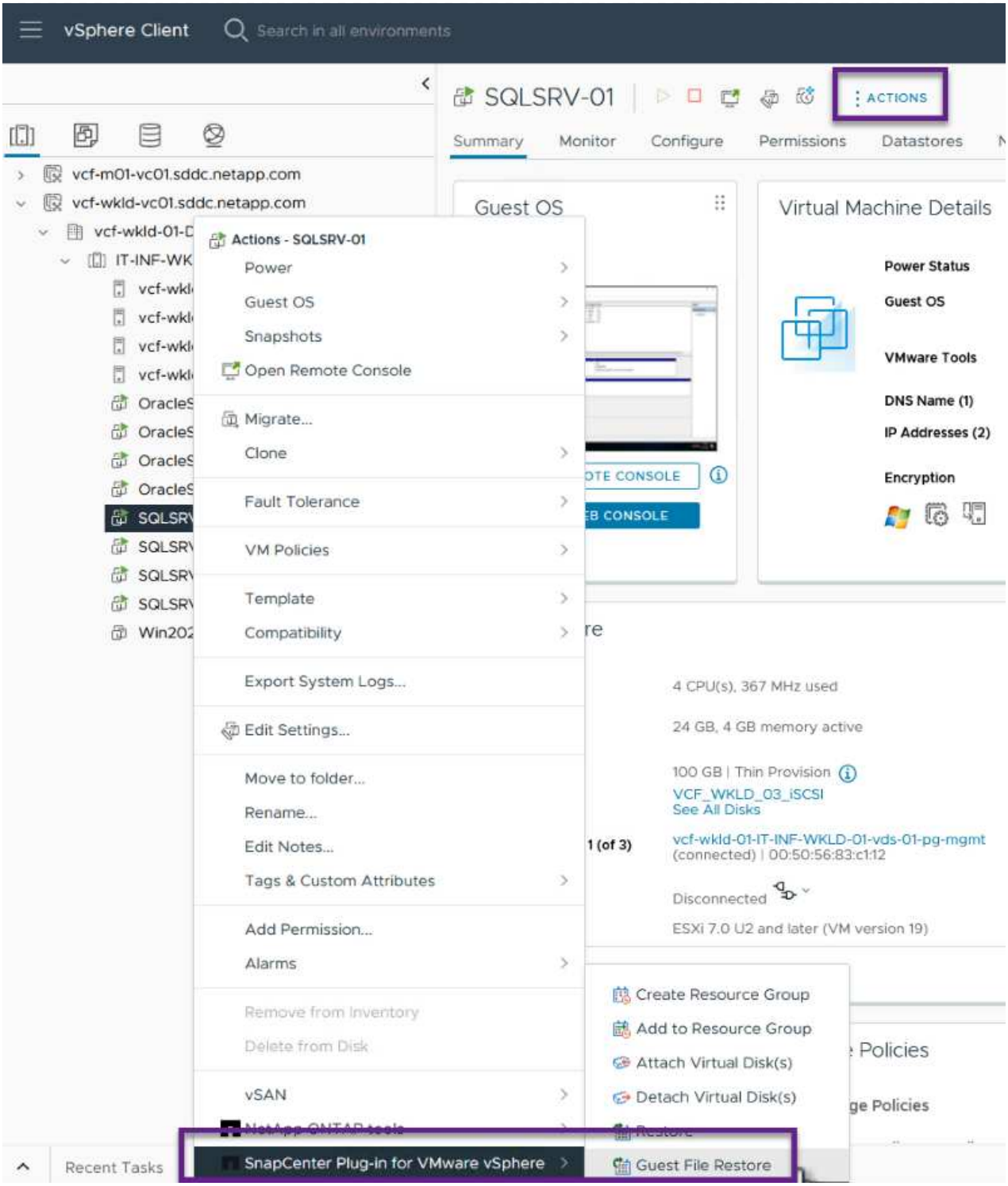


restauração.

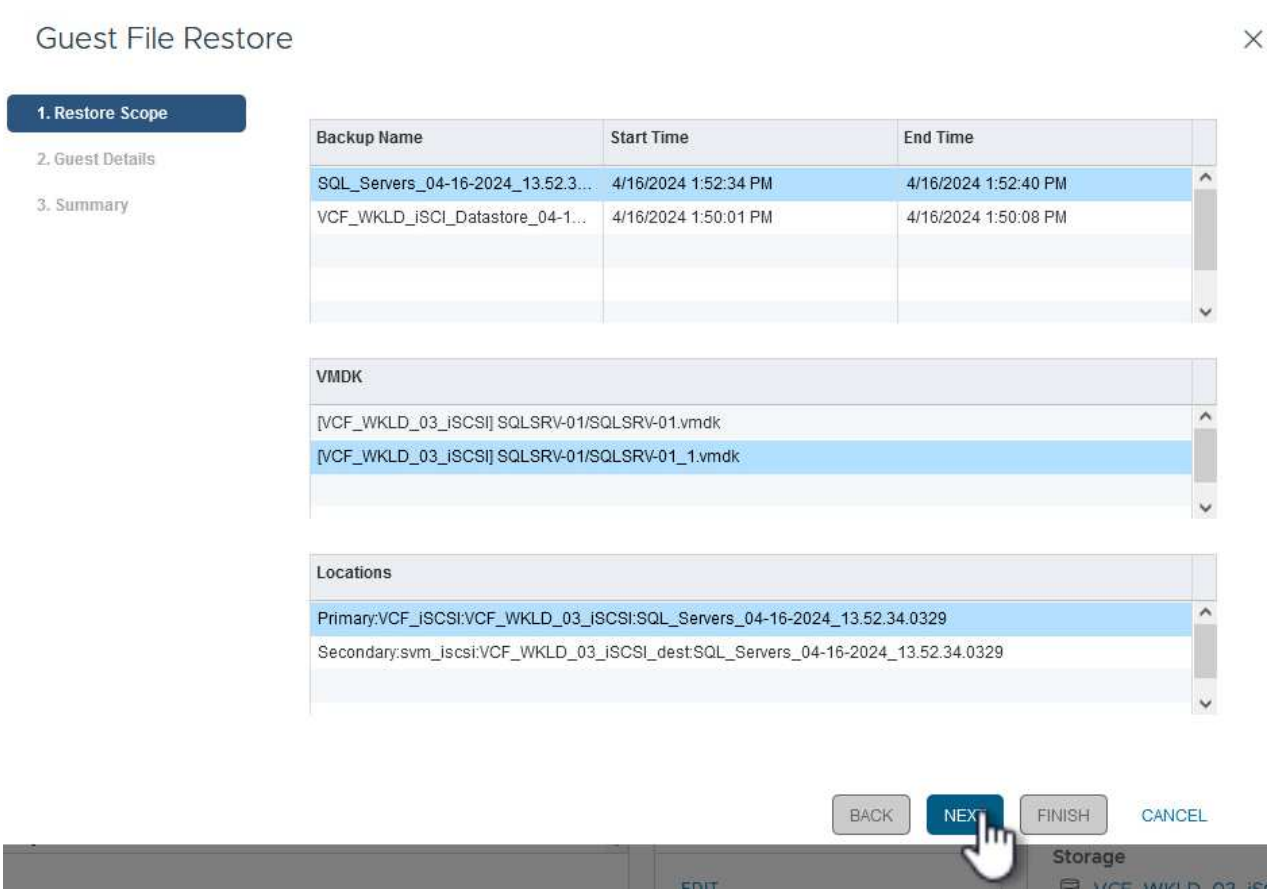
4. Na página Proxy VM, forneça um nome para a VM e localize-a pesquisando por host ESXi ou por nome. Depois de selecionado, clique em **Salvar**.



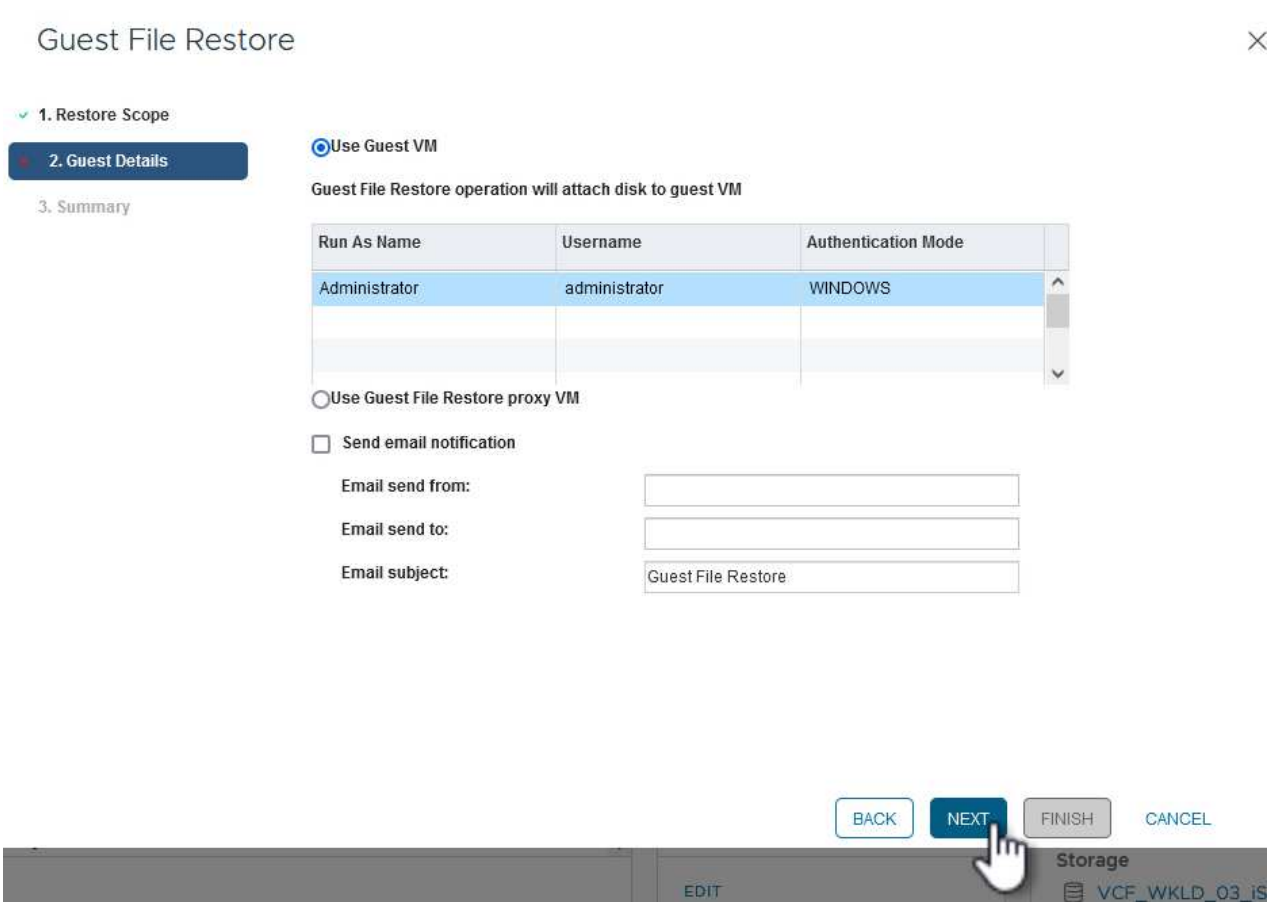
5. Clique em **Salvar** novamente na janela **Executar como credenciais** para concluir o salvamento do registro.
6. Em seguida, navegue até uma VM no inventário. No menu **Ações** ou clicando com o botão direito do mouse na VM, selecione * SnapCenter Plug-in for VMware vSphere > Restauração de arquivo convidado*.



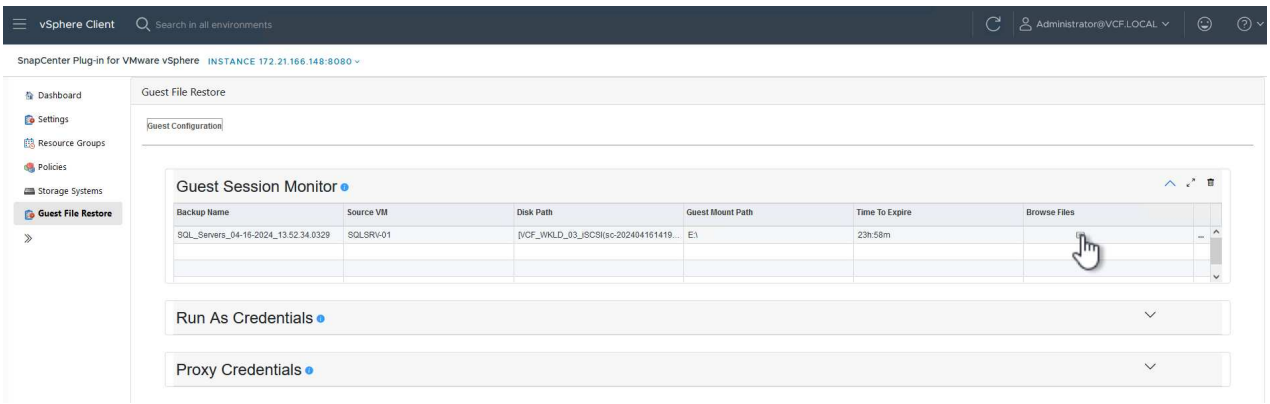
7. Na página **Escopo de restauração** do assistente **Restauração de arquivo de convidado**, selecione o backup a ser restaurado, o VMDK específico e o local (primário ou secundário) para restaurar o VMDK. Clique em **Avançar** para continuar.



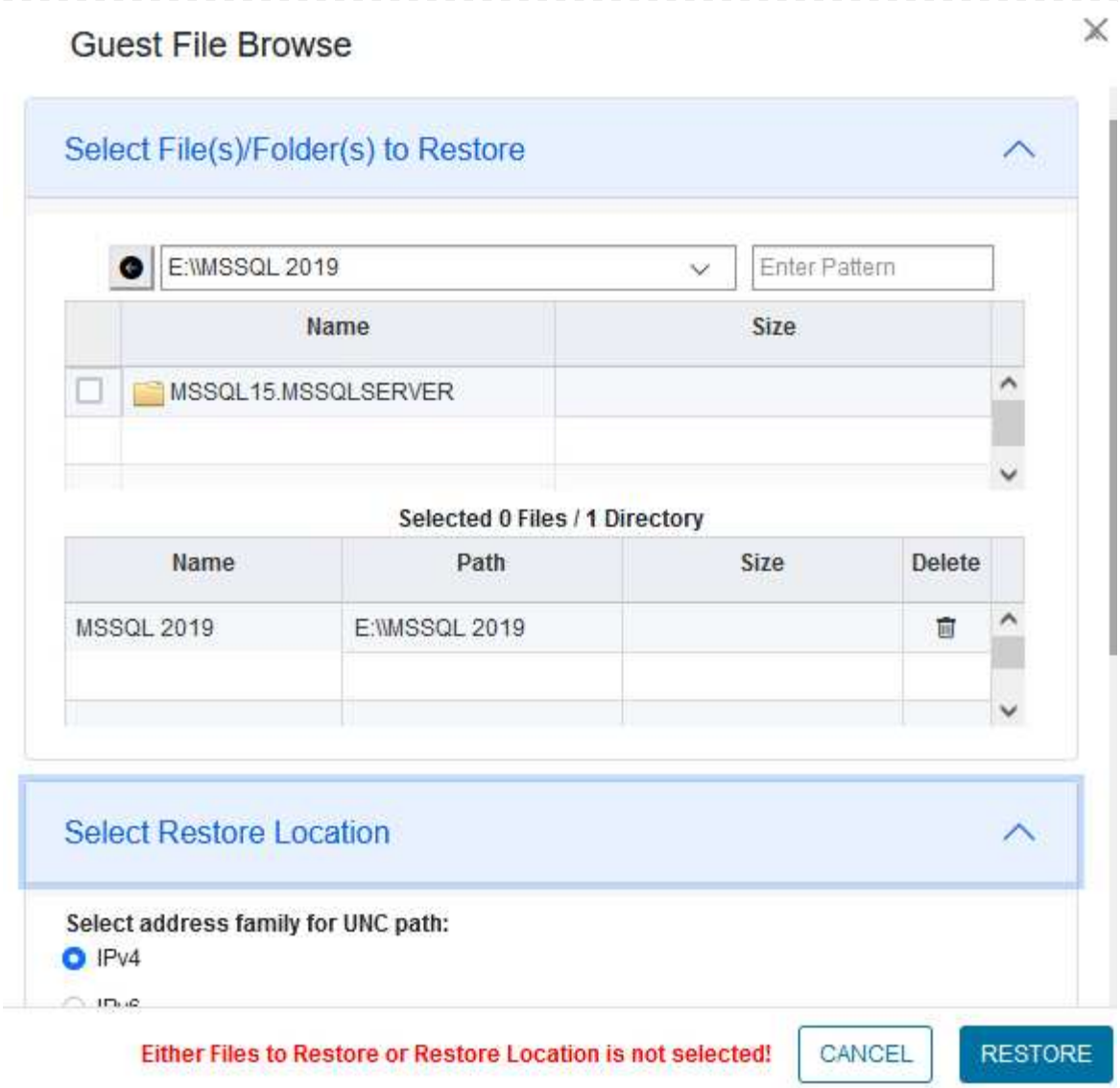
8. Na página **Detalhes do convidado**, selecione usar **VM convidada** ou **Usar VM proxy de restauração de arquivo do convidado** para a restauração. Além disso, preencha as configurações de notificação por e-mail aqui, se desejar. Clique em **Avançar** para continuar.

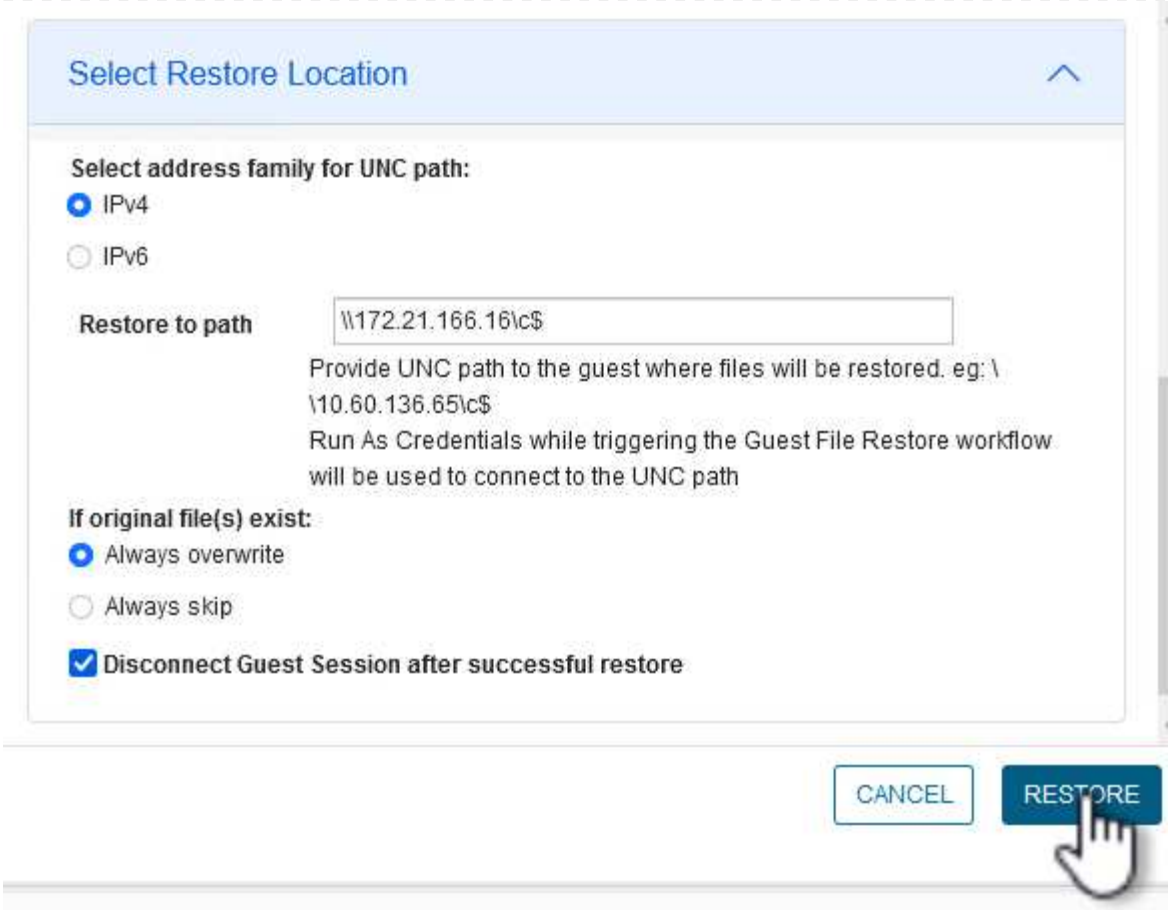


9. Por fim, revise a página **Resumo** e clique em **Concluir** para iniciar a sessão de Restauração do Sistema de Arquivos Convidado.
10. De volta à interface do plug-in SnapCenter , navegue até **Guest File Restore** novamente e visualize a sessão em execução em **Guest Session Monitor**. Clique no ícone em **Navegar pelos arquivos** para continuar.



11. No assistente **Guest File Browse**, selecione a pasta ou os arquivos a serem restaurados e o local do sistema de arquivos para restaurá-los. Por fim, clique em **Restaurar** para iniciar o processo de **Restauração**.


Guest File Browse
Select File(s)/Folder(s) to Restore
E:\MSSQL 2019
Enter Pattern
Name
Size
MSSQL15.MSSQLSERVER
Selected 0 Files / 1 Directory
Name
Path
Size
Delete
MSSQL 2019
E:\MSSQL 2019
Select Restore Location
Select address family for UNC path:
IPv4
Either Files to Restore or Restore Location is not selected!
CANCEL
RESTORE



12. O trabalho de restauração pode ser monitorado no painel de tarefas do vSphere Client.

Informações adicionais

Para obter informações sobre como configurar o VCF, consulte "Documentação do VMware Cloud Foundation" .

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o "Documentação do ONTAP 9" centro.

Para obter informações sobre como usar o SnapCenter Plug-in for VMware vSphere, consulte o "Documentação do SnapCenter Plug-in for VMware vSphere" .

Proteja os domínios de gerenciamento e carga de trabalho do VCF usando o plug-in SnapCenter para VMware vSphere

Use o SnapCenter Plug-in for VMware vSphere para proteger vários domínios VCF. Este procedimento inclui a configuração do plug-in para cada domínio, a configuração de políticas de backup e a execução de operações de restauração.

Os domínios de carga de trabalho do VMware Cloud Foundation (VCF) permitem que as organizações separem logicamente os recursos em diferentes domínios para agrupar diferentes cargas de trabalho, aumentar a segurança e a tolerância a falhas.

Introdução

Os domínios podem ser dimensionados de forma independente, atender a conformidades específicas e fornecer multilocação. A proteção de dados do VMware Cloud Foundation (VCF) é um aspecto crítico para garantir a disponibilidade, integridade e capacidade de recuperação de dados nos domínios de gerenciamento e carga de trabalho. O NetApp SnapCenter Plug-in for VMware vSphere (SCV) é uma ferramenta poderosa que integra os recursos de proteção de dados da NetApp em ambientes VMware. Ele simplifica o backup, a restauração e a clonagem de máquinas virtuais (VMs) VMware vSphere hospedadas no armazenamento NetApp .

Este documento fornece etapas de implantação sobre como proteger vários domínios VCF com SCV.

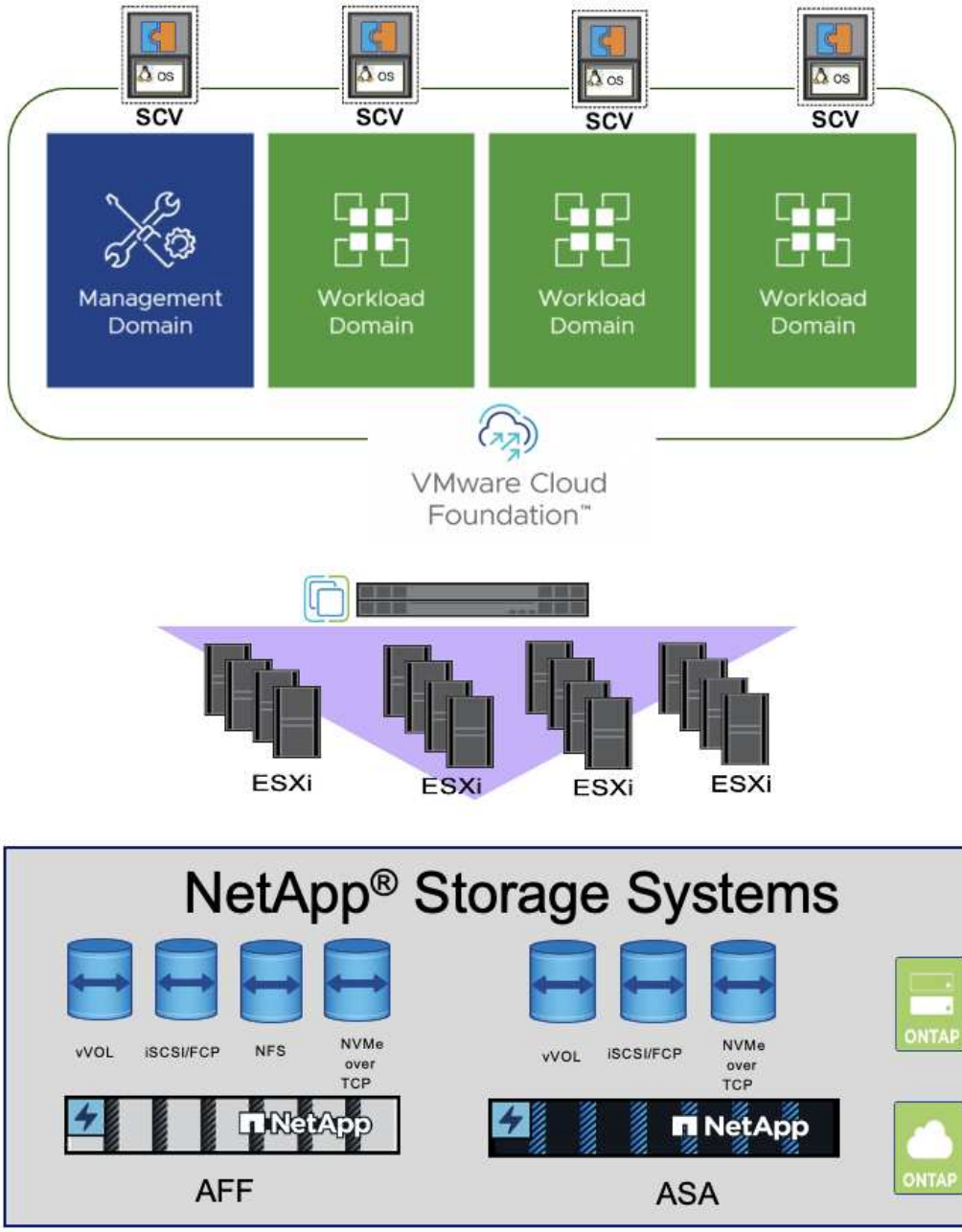
Público

Arquitetos de soluções ou administradores de armazenamento que garantem proteção de dados e recuperação de desastres para domínios de carga de trabalho do VMware VCF.

Visão geral da arquitetura

O SCV é implantado como um dispositivo virtual Linux usando um arquivo OVA para fornecer operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes com VMs, armazenamentos de dados, arquivos e pastas. O SCV usa uma arquitetura de plug-in remoto. Havia vários SCVs implantados e hospedados no domínio de gerenciamento do VCF vCenter. O domínio SCV e VCF é um relacionamento um para um, portanto o domínio de gerenciamento VCF e cada domínio de carga de trabalho requerem um SCV.

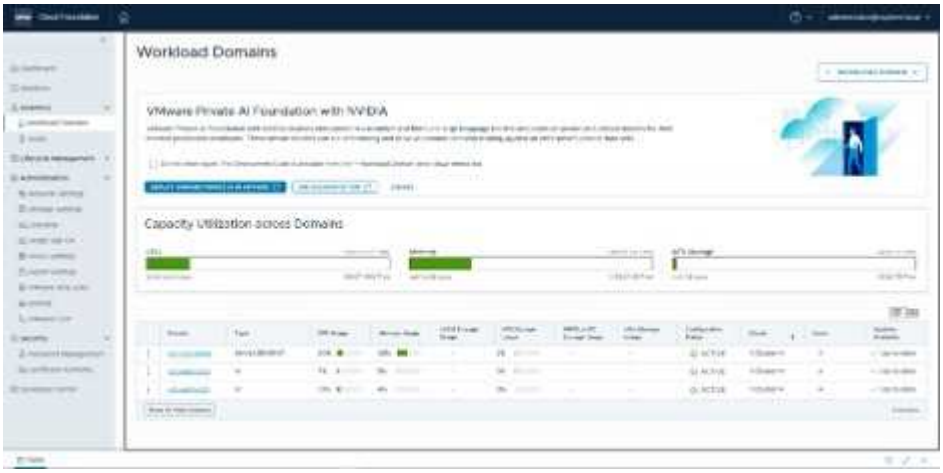
Dados que estão em sistemas primários ONTAP FAS, AFF ou All SAN Array (ASA) e replicados em sistemas secundários ONTAP FAS, AFF ou ASA . O SCV também funciona com o SnapCenter Server para dar suporte a operações de backup e restauração baseadas em aplicativos em ambientes VMware para plug-ins específicos de aplicativos SnapCenter . Para mais informações, consulte,"Documentação do SnapCenter Plug-in for VMware vSphere ."



A regra de backup 3-2-1 é uma estratégia de proteção de dados que envolve fazer três cópias de dados, armazená-las em dois tipos diferentes de mídia e manter uma cópia fora do local. O BlueXP backup and recovery é uma ferramenta baseada em nuvem para gerenciamento de dados que fornece um único plano de controle para uma ampla gama de operações de backup e recuperação em ambientes locais e na nuvem. Parte do pacote de BlueXP backup and recovery do NetApp BlueXP é um recurso que se integra ao SCV (local) para estender uma cópia dos dados para o armazenamento de objetos na nuvem. Isso estabelece uma terceira cópia dos dados fora do local, originada dos backups de armazenamento primário ou secundário. O BlueXP backup and recovery facilitam a configuração de políticas de armazenamento que transferem cópias dos seus dados de qualquer um desses dois locais locais. Para mais detalhes, consulte"Proteção de dados 3-2-1 para VMware com plug-in SnapCenter e BlueXP backup and recovery para VMs" .

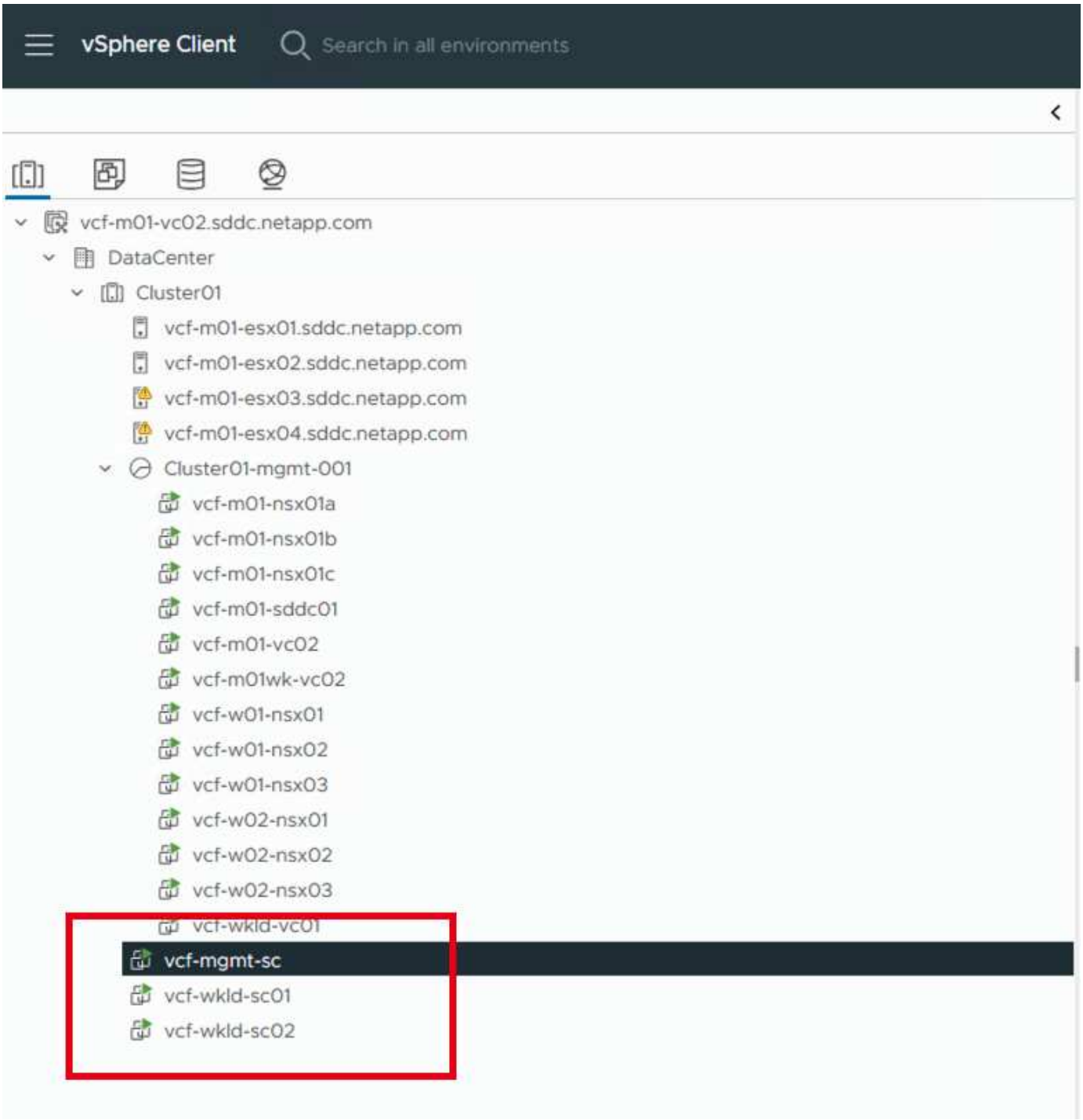
Implantar um VCF com domínio de gerenciamento e vários domínios de carga de trabalho

Um domínio de carga de trabalho VCF é um grupo de hosts ESXi com um ou mais clusters vSphere, provisionados pelo SDDC Manager e prontos para aplicativos. No exemplo de VCF abaixo, um domínio de gerenciamento e dois domínios de carga de trabalho foram implantados. Para obter mais detalhes sobre como implantar o VCF com armazenamento NetApp , verifique"Documentação de implantação do NetApp VCF."



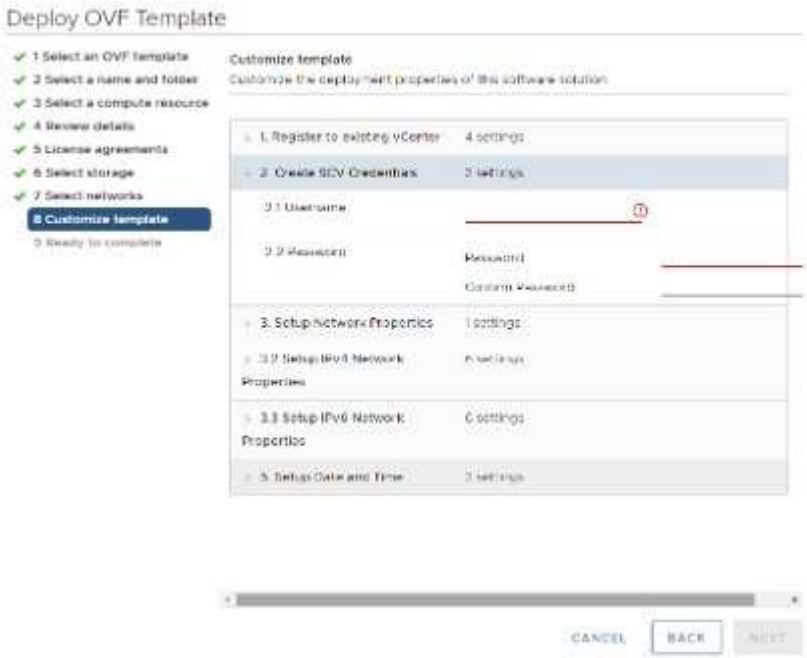
Etapas de implantação, configuração e restauração do SCV

Com base no número de domínios de carga de trabalho e no domínio de gerenciamento, vários SCVs precisam ser implantados. Com dois domínios de carga de trabalho e um domínio de gerenciamento, o exemplo abaixo mostra três SCVs implantados no domínio de gerenciamento VCF vCenter.


vSphere Client
Search in all environments
vcf-m01-vc02.sddc.netapp.com
DataCenter
Cluster01
vcf-m01-esx01.sddc.netapp.com
vcf-m01-esx02.sddc.netapp.com
vcf-m01-esx03.sddc.netapp.com
vcf-m01-esx04.sddc.netapp.com
Cluster01-mgmt-001
vcf-m01-nsx01a
vcf-m01-nsx01b
vcf-m01-nsx01c
vcf-m01-sddc01
vcf-m01-vc02
vcf-m01wk-vc02
vcf-w01-nsx01
vcf-w01-nsx02
vcf-w01-nsx03
vcf-w02-nsx01
vcf-w02-nsx02
vcf-w02-nsx03
vcf-wkld-vc01
vcf-mgmt-sc
vcf-wkld-sc01
vcf-wkld-sc02

Implantar SCV para domínio de gerenciamento e cada domínio de carga de trabalho

1. "Baixe o Open Virtual Appliance (OVA)."
2. Efetue login com o vSphere Client no vCenter Server. Navegue até Administração > Certificados > Gerenciamento de certificados. Adicione certificados raiz confiáveis e instale cada certificado na pasta certs. Depois que os certificados forem instalados, o OVA poderá ser verificado e implantado.
3. Efetue login no domínio de carga de trabalho do VCF vCenter e implante o modelo OVF para iniciar o assistente de implantação do



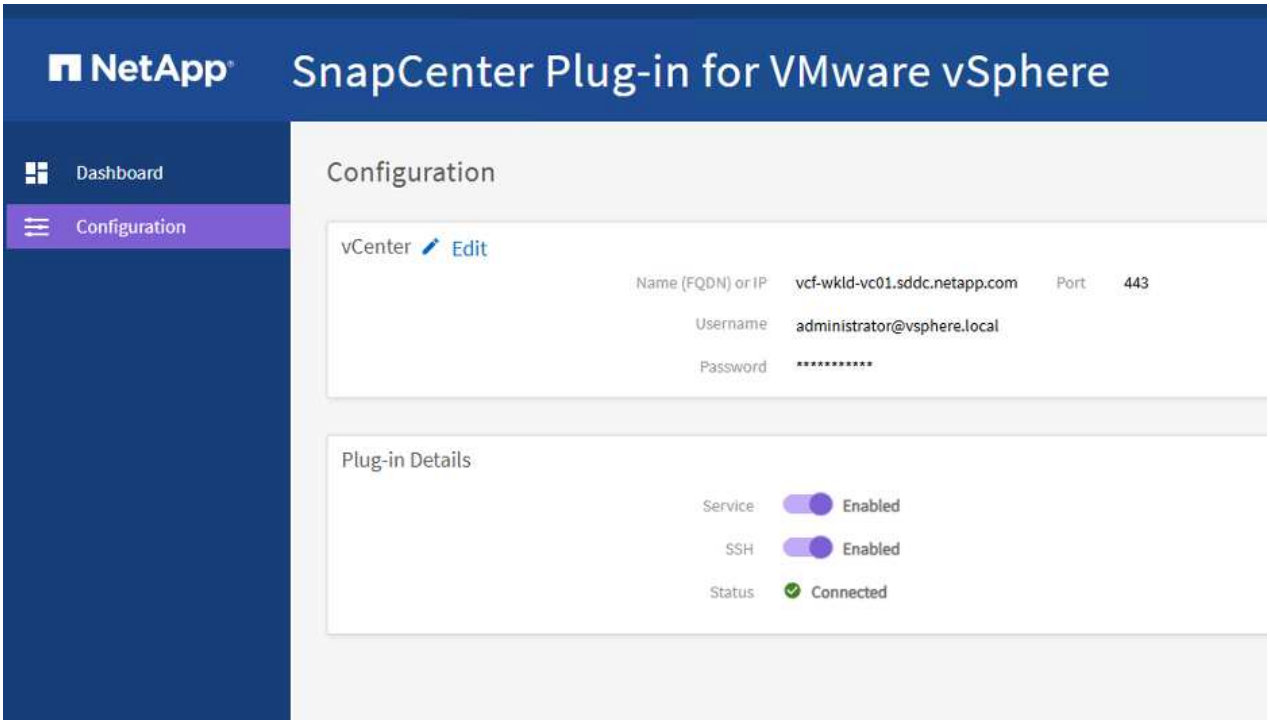
VMware.

4. Ligue o OVA para iniciar o SCV e clique em Instalar ferramentas VMware.
5. Gere o token MFA no console OVA, menu de configuração do

sistema.

```
System Configuration Menu:
--------------------------
   1 ) Reboot virtual machine
   2 ) Shut down virtual machine
   3 ) Change 'maint' user password
   4 ) Change time zone
   5 ) Change NTP server
   6 ) Enable SSH access
   7 ) Increase jail disk size (/jail)
   8 ) Upgrade
   9 ) Install VMware Tools
  10 ) Generate MFA Token

   b ) Back
   x ) Exit

 Enter your choice: 10


Generating MFA Token... Your MFA Token is : 435164

 Press ENTER to continue._
```

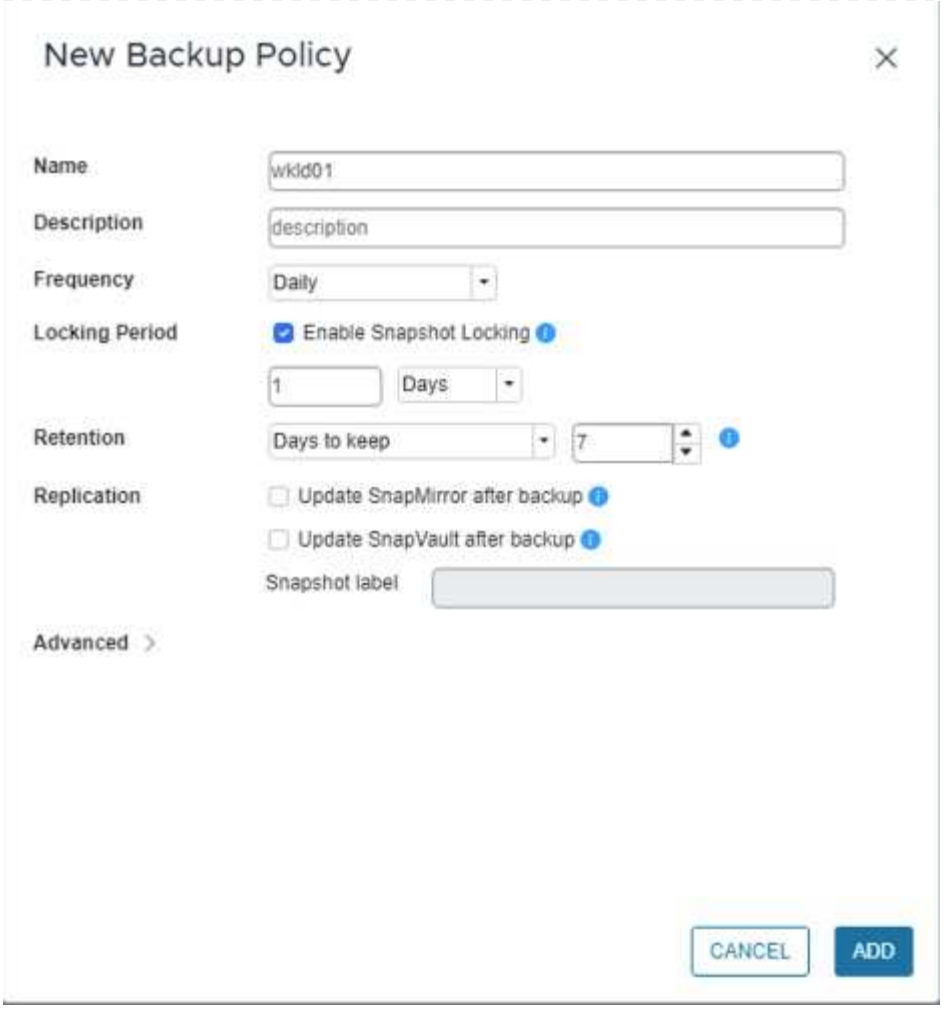
6. Efetue login na GUI de gerenciamento do SCV com o nome de usuário e a senha do administrador definidos no momento da implantação e o token MFA gerado usando o console de manutenção. `https://<appliance-IP-address>:8080` para acessar a GUI de gerenciamento.



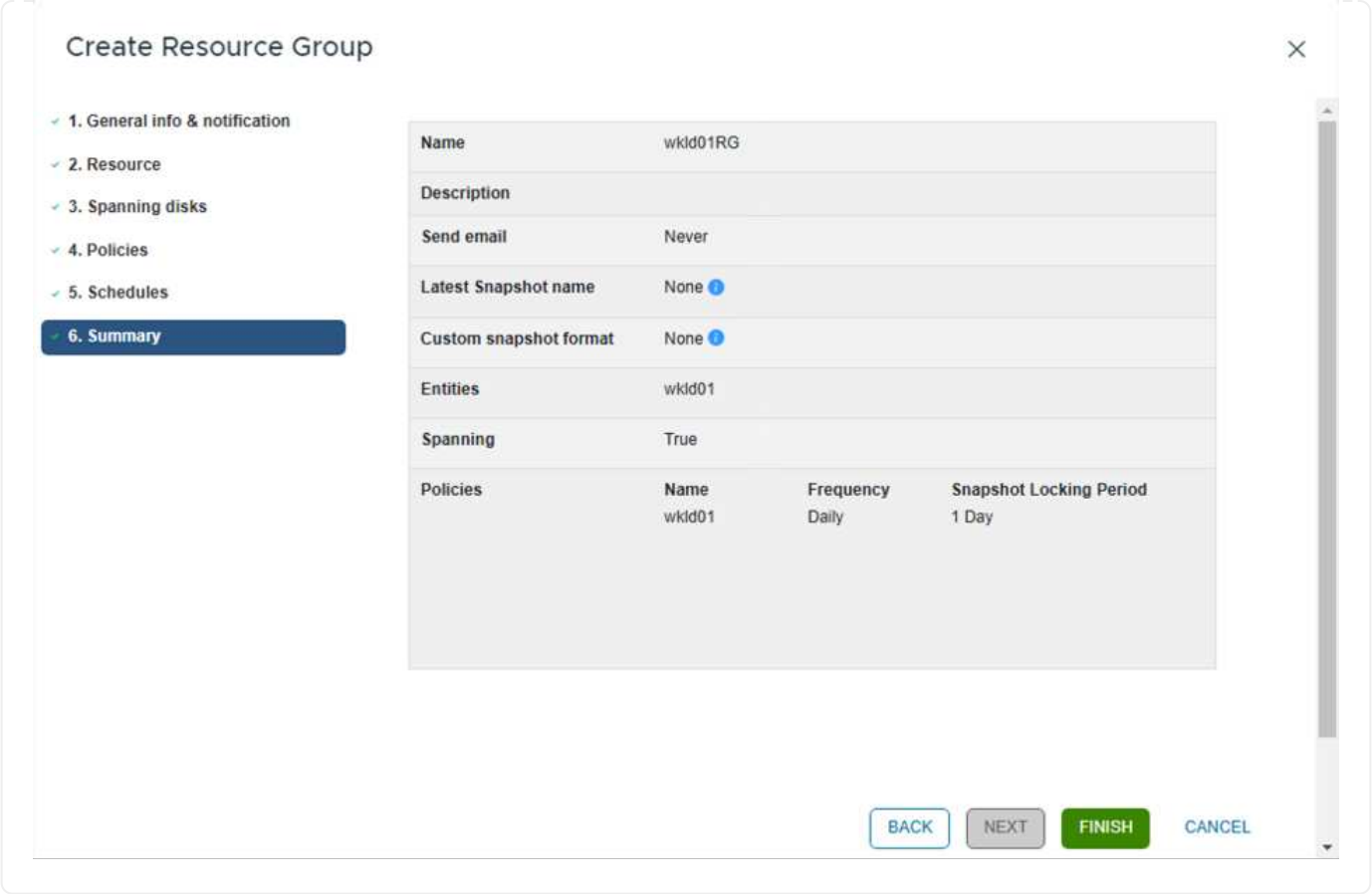
Configurar SCV

Para fazer backup ou restaurar VMs, primeiro adicione os clusters de armazenamento ou VMs que hospedam os repositórios de dados, depois crie políticas de backup para retenção e frequência e configure um grupo de recursos para proteger os
recursos.

1. Efetue login no cliente web do vCenter, clique em Menu na barra de ferramentas e selecione SnapCenter Plug-in for VMware vSphere e Adicionar um armazenamento. No painel de navegação esquerdo do plug-in SCV, clique em Sistemas de armazenamento e selecione Adicionar opção. Na caixa de diálogo Adicionar sistema de armazenamento, insira as informações básicas do SVM ou cluster e selecione Adicionar. Digite o endereço IP de armazenamento da NetApp e faça login.
2. Para criar uma nova política de backup, no painel de navegação esquerdo do plug-in SCV, clique em Políticas e selecione Nova política. Na página Nova Política de Backup, insira as informações de configuração da política e clique em Adicionar.



3. No painel de navegação esquerdo do plug-in SCV, clique em Grupos de recursos e selecione Criar. Insira as informações necessárias em cada página do assistente Criar Grupo de Recursos, selecione as VMs e os armazenamentos de dados a serem incluídos no grupo de recursos e, em seguida, selecione as políticas de backup a serem aplicadas ao grupo de recursos e especifique o agendamento de backup.

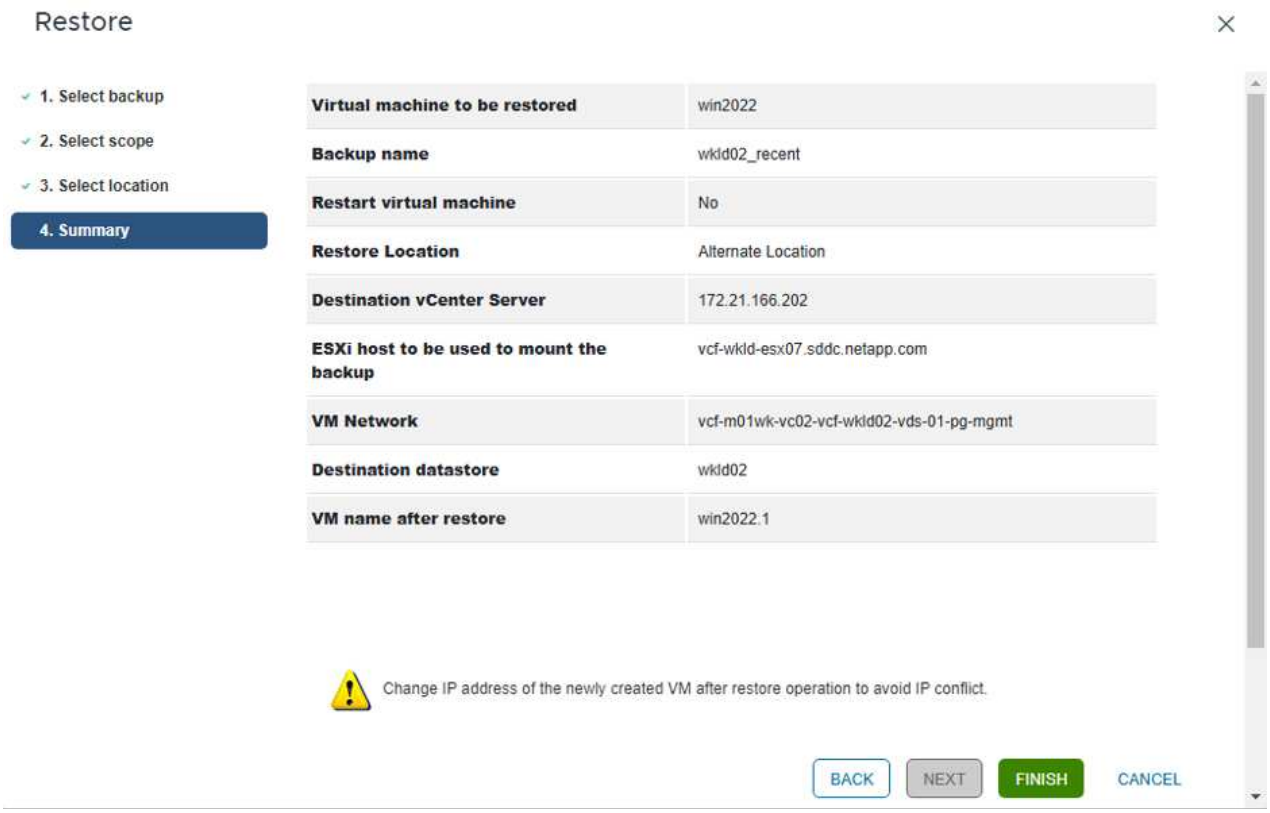

Create Resource Group
1. General info & notification
2. Resource
3. Spanning disks
4. Policies
5. Schedules
6. Summary
Name
wkld01RG
Description
Send email
Never
Latest Snapshot name
None
Custom snapshot format
None
Entities
wkld01
Spanning
True
Policies
Name
wkld01
Frequency
Daily
Snapshot Locking Period
1 Day
BACK
NEXT
FINISH
CANCEL

Restaurar backup de VM e arquivos ou pastas

VMs, VMDKs, arquivos e pastas de backups podem ser restaurados. A VM pode ser restaurada no host original ou em um host alternativo no mesmo vCenter Server, ou em um host ESXi alternativo gerenciado pelo mesmo vCenter. Você pode montar um armazenamento de dados tradicional a partir de um backup se quiser acessar arquivos no backup. Você pode montar o backup no mesmo host ESXi onde o backup foi criado ou em um host ESXi alternativo que tenha o mesmo tipo de VM e configurações de host. Você pode montar um armazenamento de dados várias vezes em um host. Arquivos e pastas individuais também podem ser restaurados em uma sessão de restauração de arquivos de convidado, que anexa uma cópia de backup de um disco virtual e restaura os arquivos ou pastas selecionados. Arquivos e pastas também podem ser restaurados.

Etapas de restauração da VM

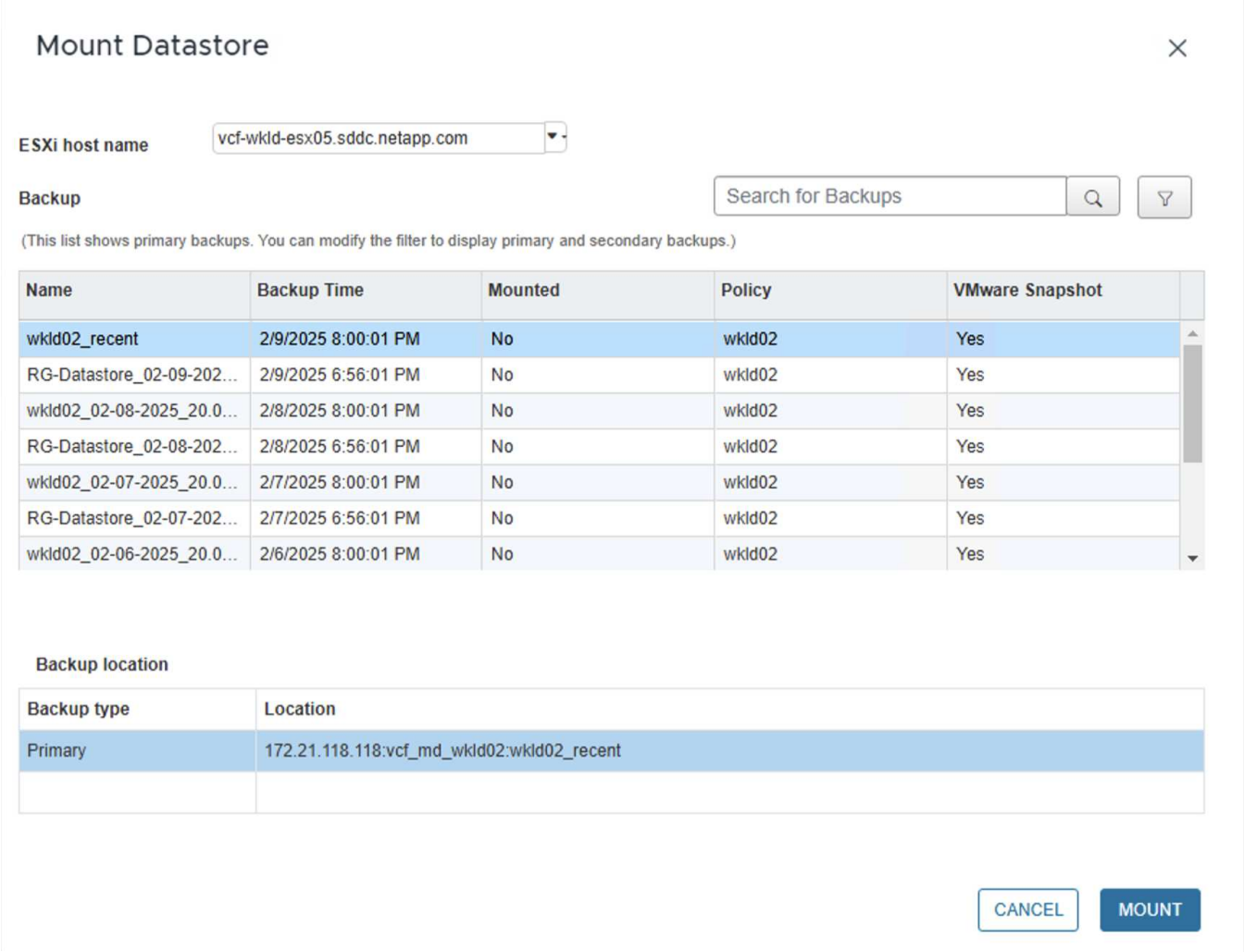
1. Na GUI do cliente VMware vSphere, clique em Menu na barra de ferramentas e selecione VMs e modelos na lista suspensa, clique com o botão direito do mouse em uma VM e selecione SnapCenter Plug-in for VMware vSphere na lista suspensa e, em seguida, selecione Restaurar na lista suspensa secundária para iniciar o assistente.
2. No assistente de restauração, selecione o instantâneo de backup que você deseja restaurar e selecione Máquina virtual inteira no campo Escopo da restauração, selecione o local de restauração e insira as informações de destino onde o backup deve ser montado. Na página Selecionar local, selecione o local para o armazenamento de dados restaurado. Revise a página Resumo e clique em Concluir.



3. Monitore o progresso da operação clicando em Tarefas recentes na parte inferior da tela.

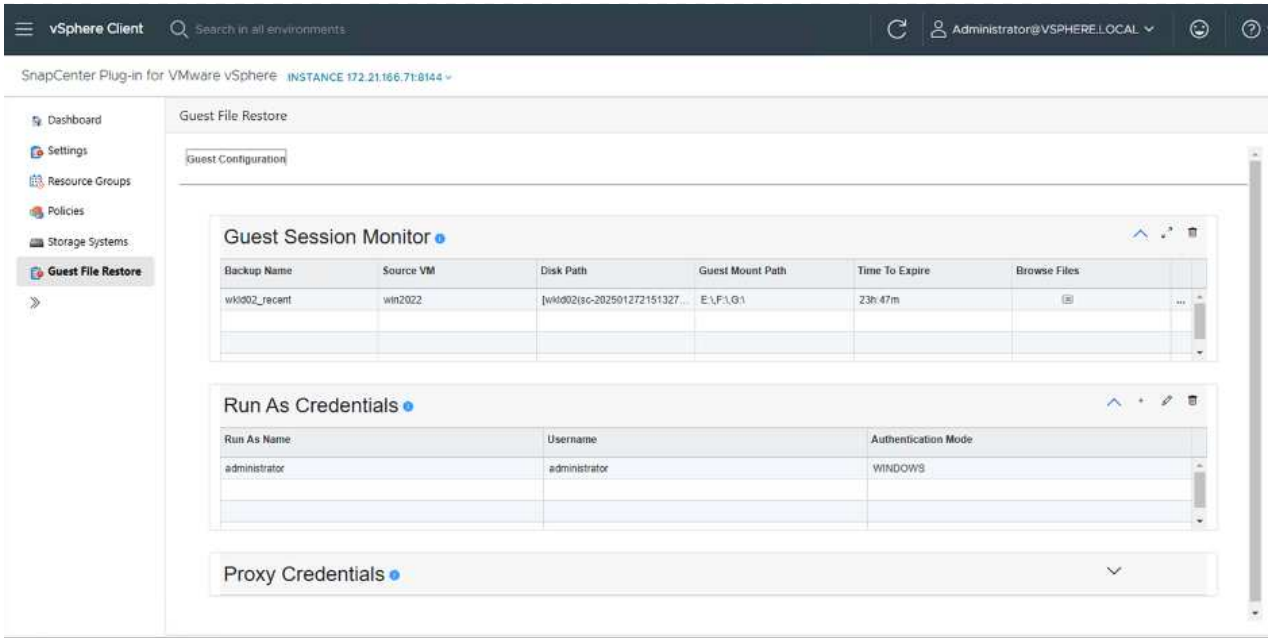
Etapas de restauração do armazenamento de dados

1. Clique com o botão direito do mouse em um armazenamento de dados e selecione SnapCenter Plug-in for VMware vSphere > Montar backup.
2. Na página Montar Datastore, selecione um backup e um local de backup (primário ou secundário) e clique em Montar.

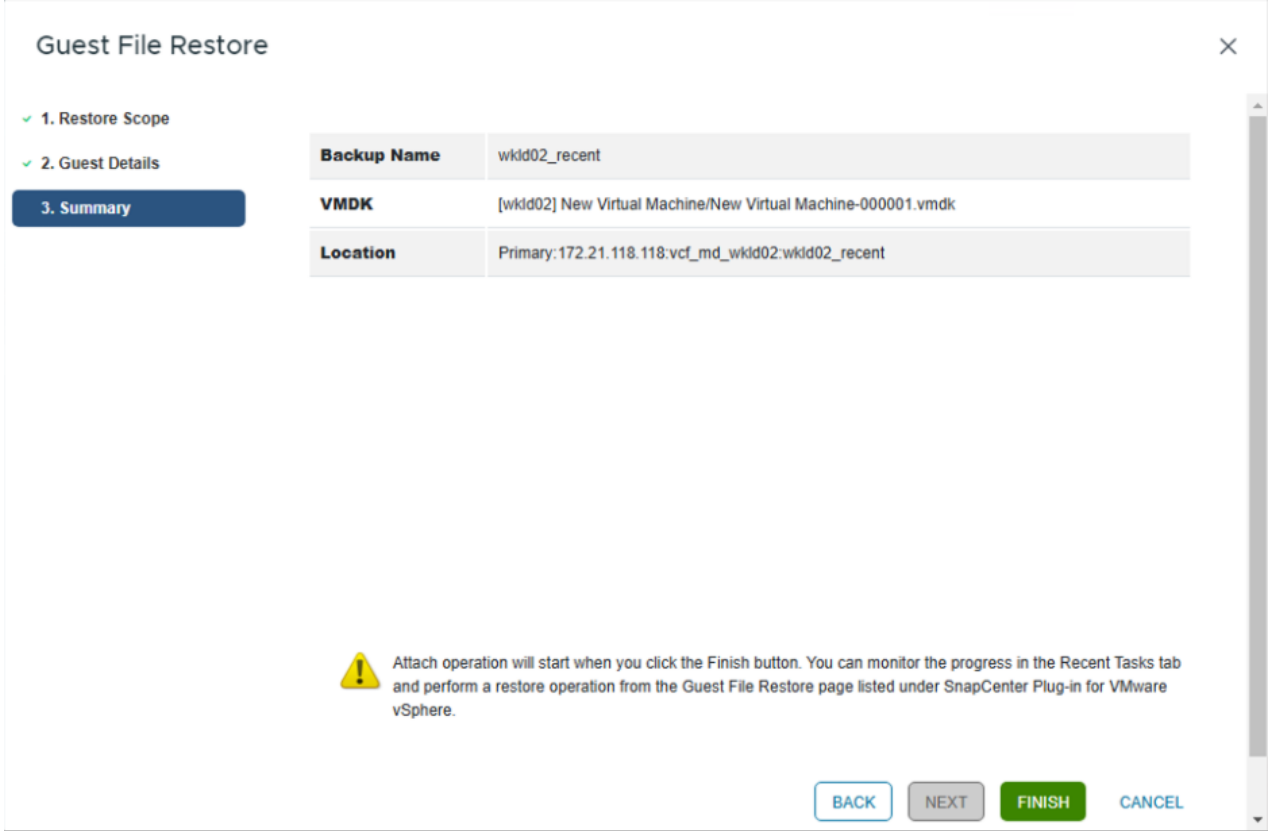


Etapas para restauração de arquivos e pastas

1. Ao anexar um disco virtual para operações de restauração de arquivos ou pastas de convidados, a VM de destino para a anexação deve ter credenciais configuradas antes da restauração. No SnapCenter Plug-in for VMware vSphere , em plug-ins, selecione a seção Restauração de arquivo de convidado e Credenciais de execução como, insira as credenciais do usuário. Para Nome de usuário, você deve digitar "Administrador".



2. Clique com o botão direito do mouse na VM do cliente vSphere e selecione SnapCenter Plug-in for VMware vSphere > Restauração de arquivo convidado. Na página Escopo de restauração, especifique o Nome do backup, o disco virtual VMDK e o Local – primário ou secundário. Clique em Sumário para confirmar.



O NetApp SnapCenter para VCP multidomínio centraliza a proteção de dados, reduz eficientemente o tempo e o espaço de armazenamento necessários para backups usando snapshots do NetApp , oferece suporte a ambientes VMware de larga escala com recursos robustos de backup e replicação e permite recuperação

granular de VMs inteiras, VMDKs específicos ou arquivos individuais.

Demonstração em vídeo para proteger múltiplos domínios VCF com SCV

Proteja vários domínios VMware VCF com NetApp SCV

Proteja domínios de carga de trabalho VCF com armazenamento NVMe sobre TCP e plug-in SnapCenter para VMware vSphere

Use o SnapCenter Plug-in for VMware vSphere para proteger domínios de carga de trabalho VCF com NVMe. Este procedimento inclui a configuração do plug-in, a configuração do NVMe sobre TCP para desempenho ideal e a execução de operações de backup, restauração ou clonagem.

NVMe (Non-Volatile Memory Express) sobre TCP é um protocolo de rede de ponta que facilita a transferência de dados em alta velocidade entre servidores VMware Cloud Foundation ESXi e armazenamento NetApp , incluindo All Flash FAS (AFF) e All SAN Array (ASA).

Introdução

Aproveitar NVMe sobre TCP proporciona baixa latência e alto rendimento para cargas de trabalho exigentes. A integração do NVMe sobre TCP com o NetApp SnapCenter Plug-in for VMware vSphere (SCV) oferece uma combinação poderosa para gerenciamento eficiente de dados, aprimorando operações de backup, restauração e clonagem em ambientes VMware.

Benefícios do NVMe sobre TCP

- Alto desempenho: oferece desempenho excepcional com baixa latência e altas taxas de transferência de dados. Isso é crucial para aplicativos exigentes e operações de dados em larga escala.
- Escalabilidade: oferece suporte a configurações escaláveis, permitindo que os administradores de TI expandam sua infraestrutura perfeitamente conforme os requisitos de dados aumentam.
- Eficiência: permite operações de backup e restauração mais rápidas, reduzindo o tempo de inatividade e melhorando a disponibilidade geral do sistema.

Este documento fornece etapas sobre como implantar e gerenciar o SCV em ambientes VMware Cloud Foundation (VCF), com foco no aproveitamento do NVMe sobre TCP para desempenho ideal.

Público

Arquitetos de soluções ou administradores de armazenamento que garantem proteção de dados e recuperação de desastres para domínios de carga de trabalho do VMware VCF.

Visão geral da arquitetura

O SCV é uma ferramenta poderosa projetada para facilitar operações de backup e restauração rápidas, com economia de espaço, consistentes em caso de falhas e consistentes com VMs, armazenamentos de dados, arquivos e pastas em ambientes VMware. O SCV é implantado como um dispositivo virtual Linux usando um arquivo OVA e aproveita uma arquitetura de plug-in remoto.

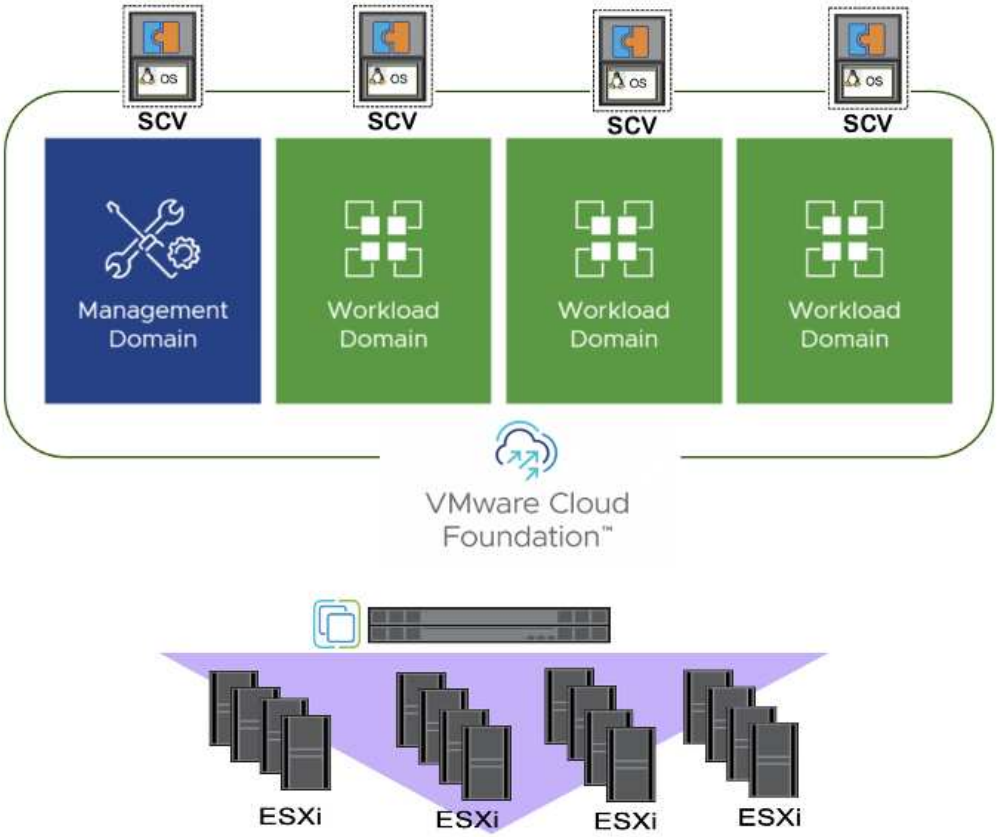
Arquitetura de implantação do SCV

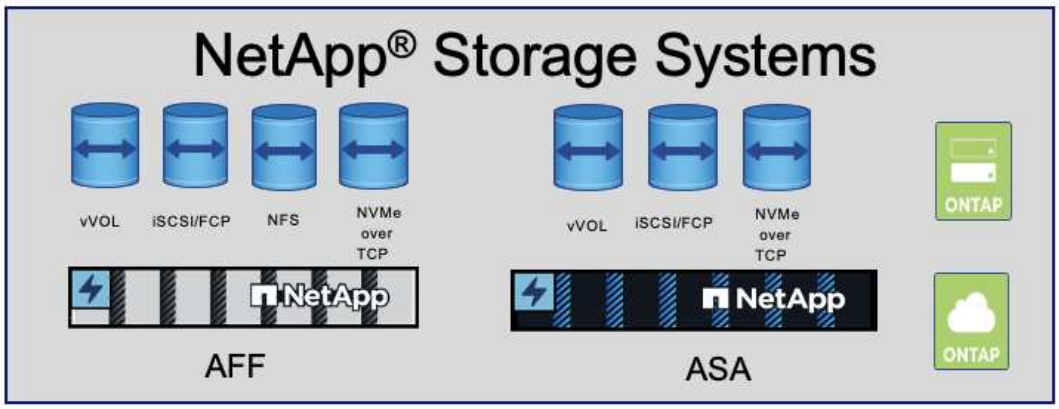
- Implantação de dispositivo virtual: o SCV é implantado como um dispositivo virtual Linux usando um

arquivo OVA. Este método de implantação garante um processo de configuração simplificado e eficiente.

- Arquitetura de plug-in remoto: o SCV usa uma arquitetura de plug-in remoto, permitindo escalabilidade e flexibilidade no gerenciamento de múltiplas instâncias.
- Relacionamento um-para-um: cada domínio VCF requer uma instância SCV dedicada, garantindo operações de backup e restauração isoladas e eficientes.

Com o ONTAP 9.10.1 e versões posteriores, o NetApp AFF e o ASA oferecem suporte a NVMe sobre TCP. Dados que estão em sistemas primários AFF ou ASA e podem ser replicados para sistemas secundários ONTAP AFF ou ASA . O SCV também funciona com o SnapCenter Server para dar suporte a operações de backup e restauração baseadas em aplicativos em ambientes VMware para plug-ins específicos de aplicativos SnapCenter . Para mais informações, consulte,"Documentação do SnapCenter Plug-in for VMware vSphere" e"Proteja cargas de trabalho com o SnapCenter"





A regra de backup 3-2-1 é uma estratégia de proteção de dados que envolve fazer três cópias de dados, armazená-las em dois tipos diferentes de mídia e manter uma cópia fora do local. O BlueXP backup and recovery é uma ferramenta baseada em nuvem para gerenciamento de dados que fornece um único plano de controle para uma ampla gama de operações de backup e recuperação em ambientes locais e na nuvem. Parte do pacote de BlueXP backup and recovery do NetApp BlueXP é um recurso que se integra ao SCV (local) para estender uma cópia dos dados para o armazenamento de objetos na nuvem. Isso estabelece uma terceira cópia dos dados fora do local, originada dos backups de armazenamento primário ou secundário. O BlueXP backup and recovery facilitam a configuração de políticas de armazenamento que transferem cópias dos seus dados de qualquer um desses dois locais locais. Para mais detalhes, consulte"Proteção de dados 3-2-1 para VMware com plug-in SnapCenter e BlueXP backup and recovery para VMs" .

SCV para VCF em etapas de implantação de NVMe

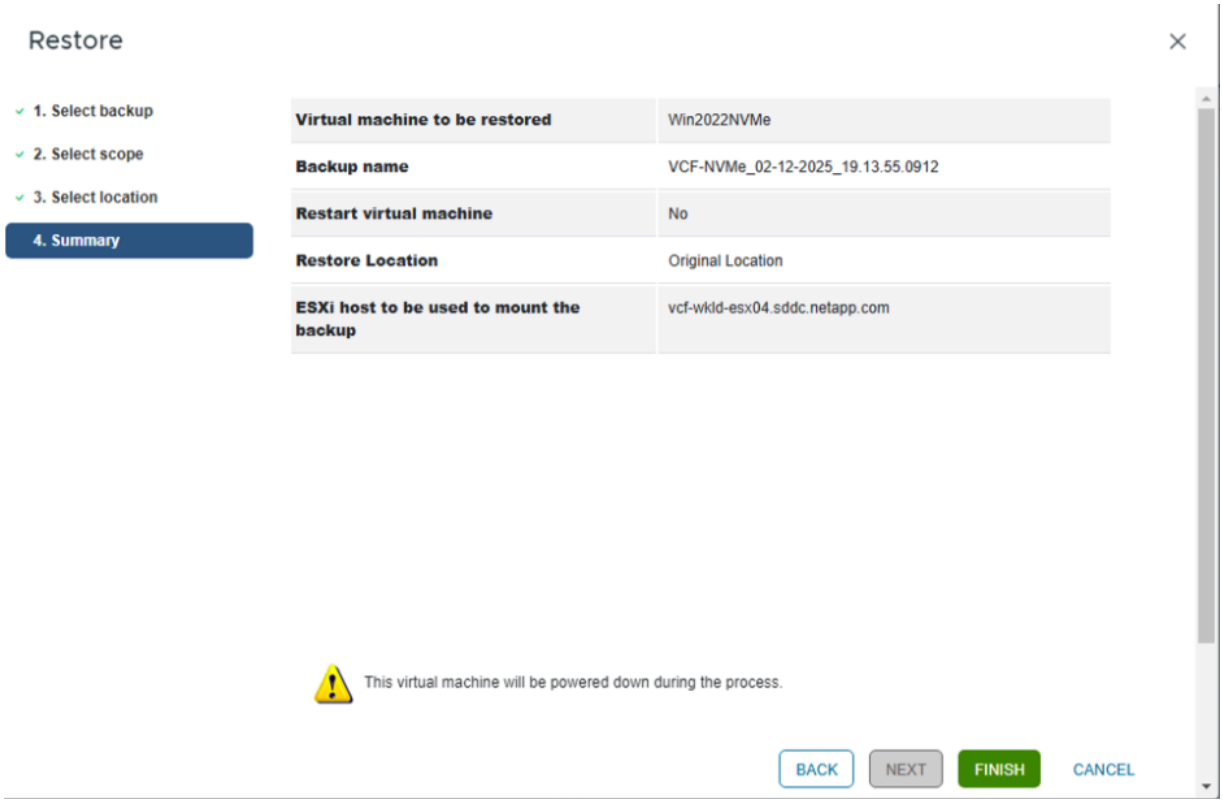
O"ONTAP tools for VMware vSphere" (OTV) fornece uma solução poderosa e eficiente para gerenciar o armazenamento NetApp em ambientes VMware. Ao integrar-se diretamente ao vCenter Server, o OTV simplifica o gerenciamento de armazenamento, melhora a proteção de dados e otimiza o desempenho. Embora opcional, a implantação do OTV pode melhorar significativamente os recursos de gerenciamento e a eficiência geral dos ambientes VMware.

- "Crie um armazenamento NVMe/TCP para domínios de carga de trabalho VCF"
- "Configurar o NetApp SnapCenter para VMware vSphere (SCV)"

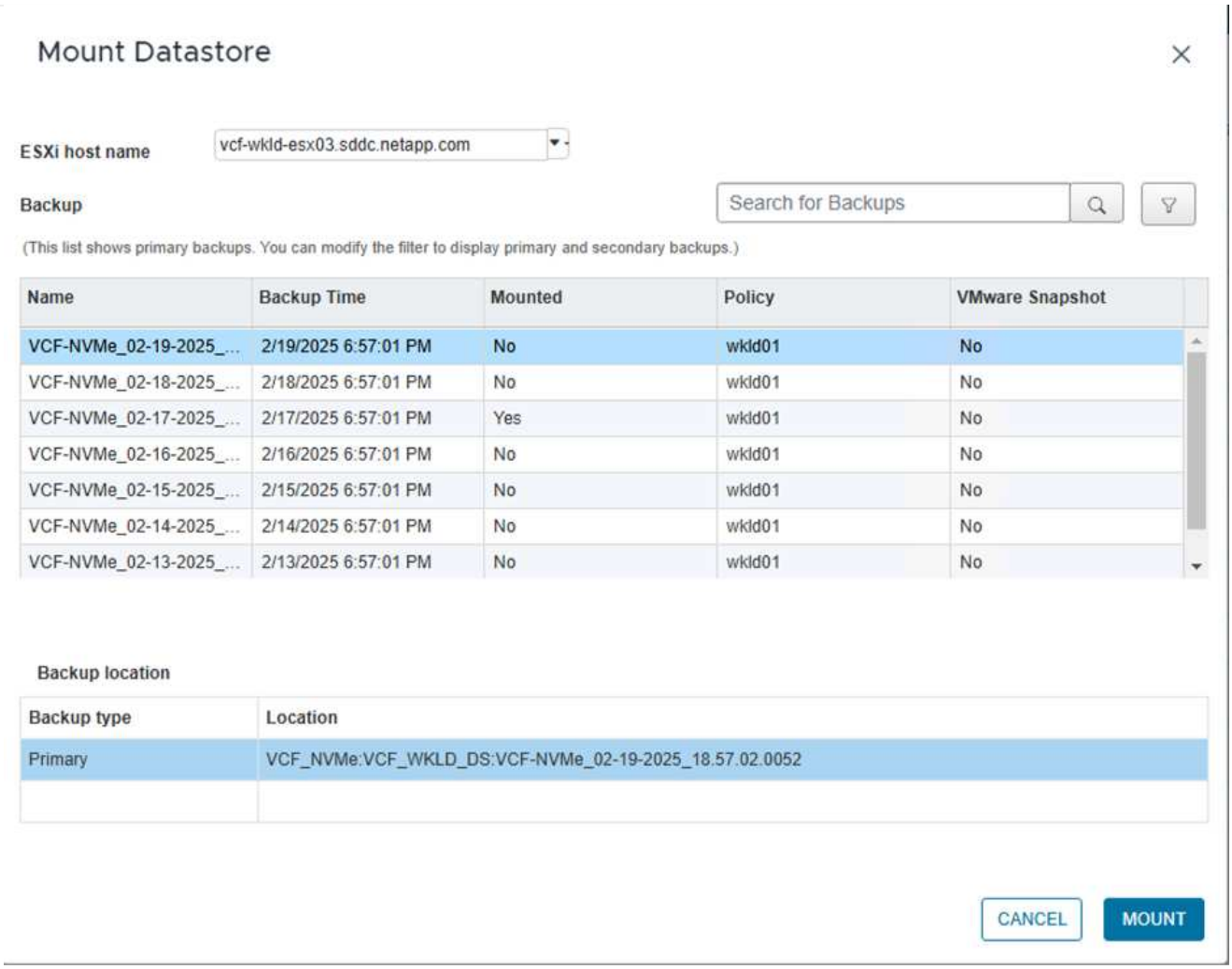
Restaurar VM, armazenamento de dados, disco virtual e arquivos ou pastas

O SCV fornece recursos abrangentes de backup e restauração para ambientes VMware. Para ambientes VMFS, o SCV usa operações de clonagem e montagem em conjunto com o Storage VMotion para executar operações de restauração. Isso garante uma restauração de dados eficiente e contínua. Para mais detalhes, verifique"como as operações de restauração são executadas."

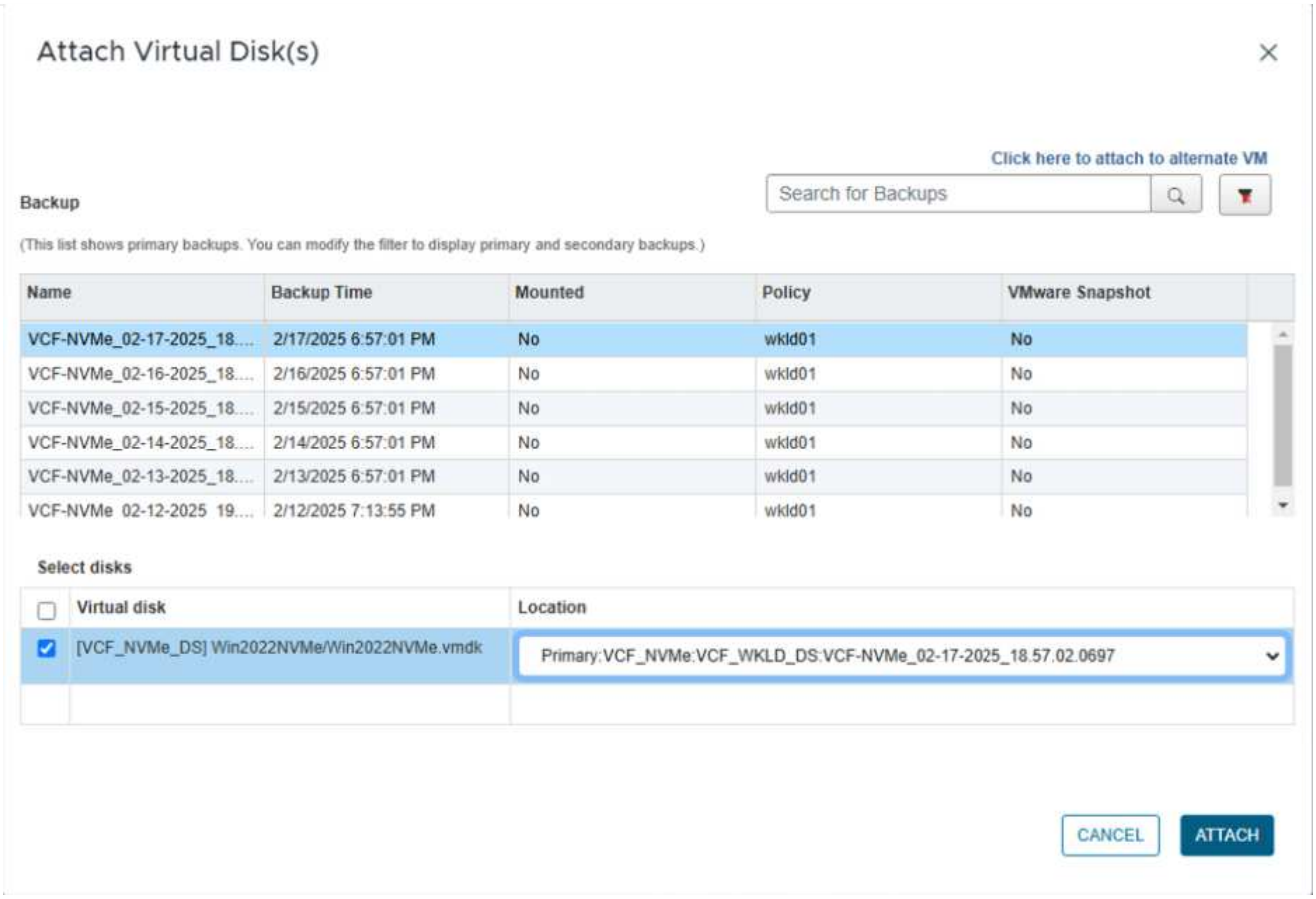
- Restauração de VM Você pode restaurar a VM para seu host original no mesmo vCenter Server ou para um host ESXi alternativo gerenciado pelo mesmo vCenter Server.
  a. Clique com o botão direito do mouse em uma VM e selecione SnapCenter Plug-in for VMware vSphere na lista suspensa e, em seguida, selecione Restaurar na lista suspensa secundária para iniciar o assistente.
  b. No assistente de restauração, selecione o instantâneo de backup que você deseja restaurar e selecione Máquina virtual inteira no campo Escopo da restauração, selecione o local de restauração e insira as informações de destino onde o backup deve ser montado. Na página Selecionar local, selecione o local para o armazenamento de dados restaurado. Revise a página Resumo e clique em
  Concluir.



- Montar um armazenamento de dados Você pode montar um armazenamento de dados tradicional a partir de um backup se quiser acessar arquivos no backup. Você pode montar o backup no mesmo host ESXi onde o backup foi criado ou em um host ESXi alternativo que tenha o mesmo tipo de VM e configurações de host. Você pode montar um armazenamento de dados várias vezes em um host.
  a. Clique com o botão direito do mouse em um armazenamento de dados e selecione SnapCenter Plug-in for VMware vSphere > Montar backup.
  b. Na página Montar Datastore, selecione um backup e um local de backup (primário ou secundário) e clique em Montar.

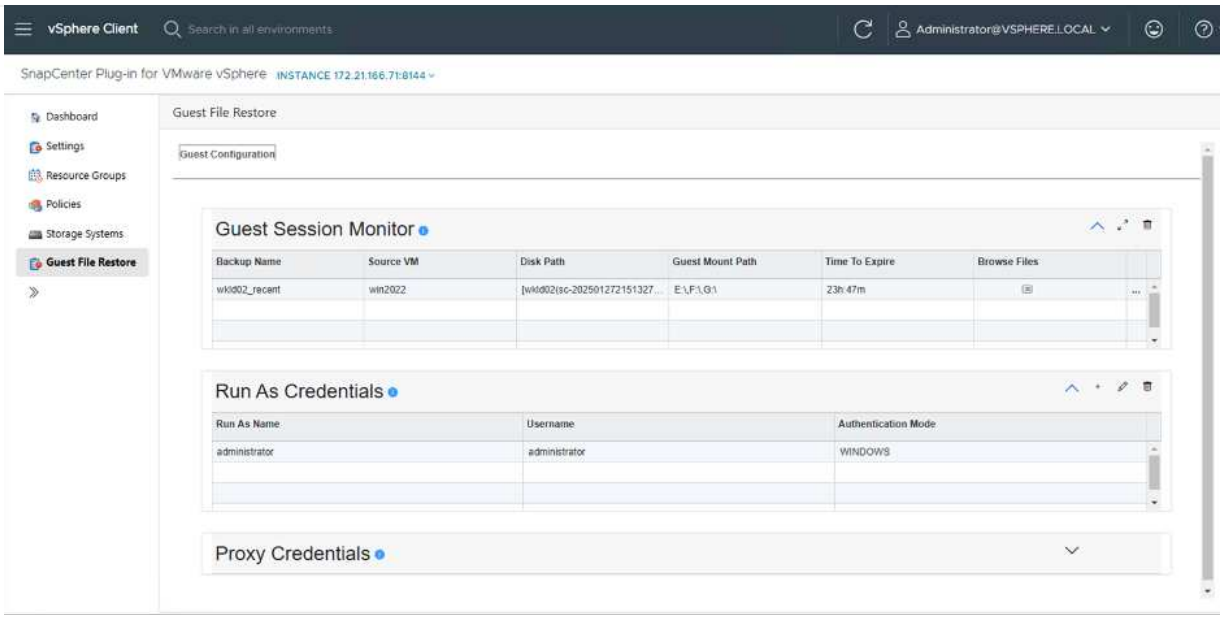


- Anexar um disco virtual Você pode anexar um ou mais VMDKs de um backup à VM pai, ou a uma VM alternativa no mesmo host ESXi, ou a uma VM alternativa em um host ESXi alternativo gerenciado pelo mesmo vCenter ou por um vCenter diferente no modo vinculado.
  a. Clique com o botão direito do mouse em uma VM, selecione SnapCenter Plug-in for VMware vSphere > Anexar disco(s) virtual(is).
  b. Na janela Anexar disco virtual, selecione um backup e selecione um ou mais discos que deseja anexar e o local de onde deseja anexar (primário ou secundário). Por padrão, os discos virtuais selecionados são anexados à VM pai. Para anexar os discos virtuais selecionados a uma VM alternativa no mesmo host ESXi, selecione Clique aqui para anexar à VM alternativa e especifique a VM alternativa. Clique em Anexar.

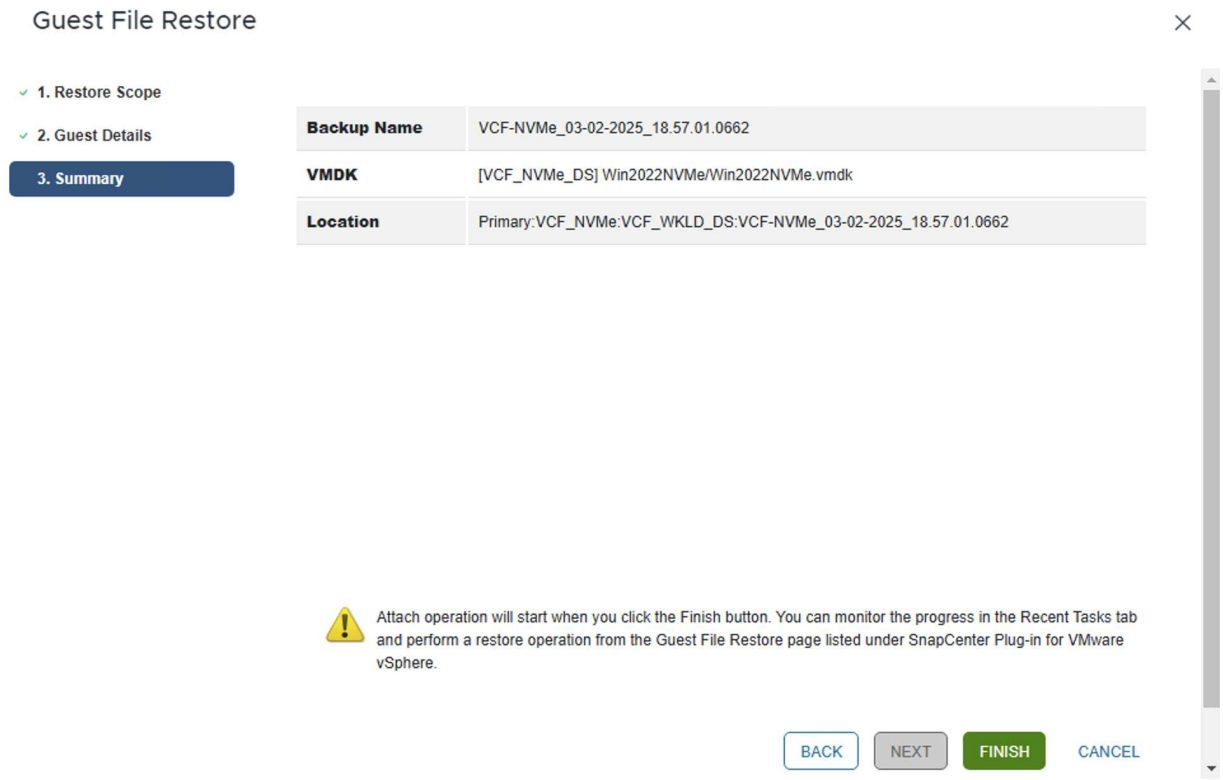


- Etapas de restauração de arquivos e pastas Arquivos e pastas individuais podem ser restaurados em uma sessão de restauração de arquivos de convidado, que anexa uma cópia de backup de um disco virtual e restaura os arquivos ou pastas selecionados. Arquivos e pastas também podem ser restaurados. Mais detalhes confira"Restauração de arquivos e pastas do SnapCenter ."

  a. Ao anexar um disco virtual para operações de restauração de arquivos ou pastas de convidados, a VM de destino para a anexação deve ter credenciais configuradas antes da restauração. No SnapCenter Plug-in for VMware vSphere , em plug-ins, selecione a seção Restauração de arquivo de convidado e Credenciais de execução como, insira as credenciais do usuário. Para Nome de usuário, você deve digitar "Administrador".

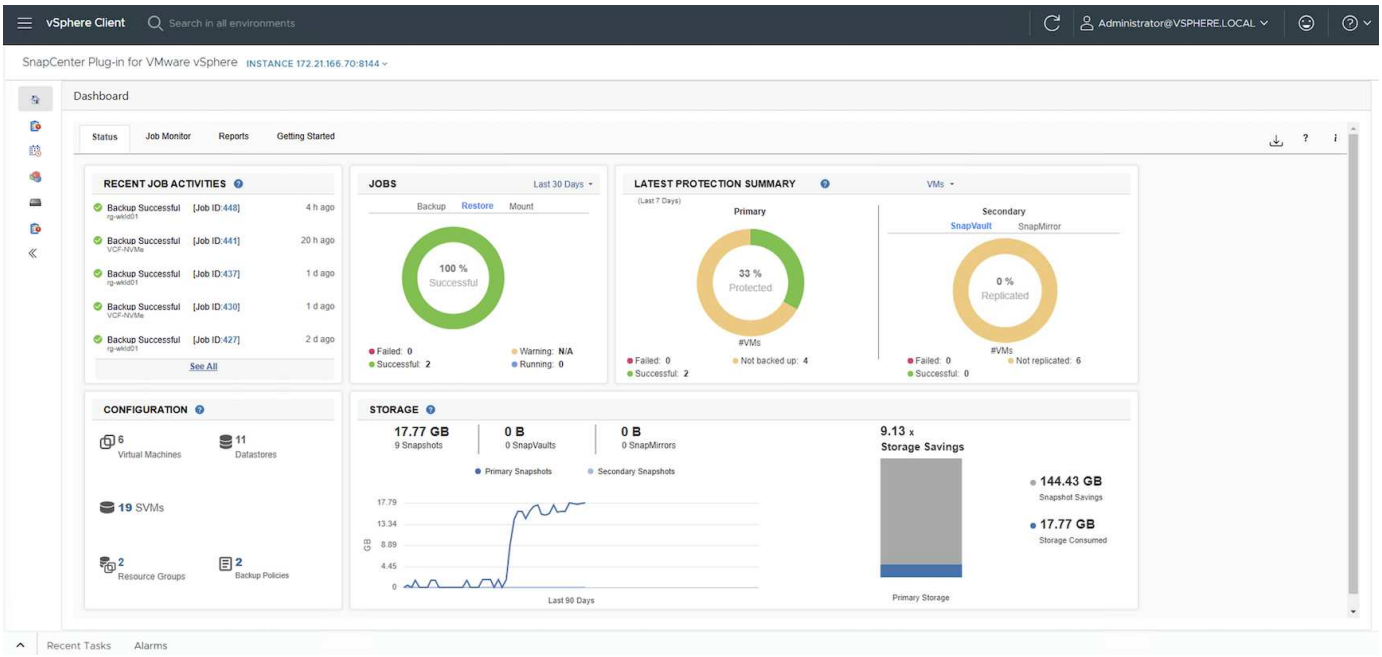


b. Clique com o botão direito do mouse na VM do cliente vSphere e selecione SnapCenter Plug-in for VMware vSphere > Restauração de arquivo convidado. Na página Escopo de restauração, especifique o Nome do backup, o disco virtual VMDK e o Local – primário ou secundário. Clique em Sumário para
confirmar.



Monitorar e relatar

O SCV fornece recursos robustos de monitoramento e geração de relatórios para ajudar os administradores a gerenciar operações de backup e restauração com eficiência. Você pode visualizar informações de status, monitorar trabalhos, baixar logs de trabalhos, acessar relatórios, para mais detalhes, verifique"Plug-in SnapCenter para VMware vSphere Monitor e Report."



Ao aproveitar o poder do NVMe sobre TCP e do NetApp SnapCenter Plug-in for VMware vSphere, as organizações podem obter proteção de dados de alto desempenho e recuperação de desastres para domínios de carga de trabalho do VMware Cloud Foundation. Essa abordagem garante operações de backup e restauração rápidas e confiáveis, minimizando o tempo de inatividade e protegendo dados críticos.

Proteja os datastores VMware com BlueXP

Saiba mais sobre como proteger os datastores VMware usando a BlueXP disaster recovery

Saiba mais sobre as soluções da NetApp para recuperação de desastres usando a BlueXP disaster recovery para VMware. Isso fornece soluções robustas para recuperação de desastres usando replicação em nível de bloco de um site primário para um site de recuperação de desastres.

O BlueXP DRaaS é um método eficaz e econômico para proteger cargas de trabalho contra falhas de site e problemas de integridade de dados, incluindo ataques de ransomware. Além disso, o NetApp BlueXP DRaaS aprimora essa estratégia ao fornecer uma solução de recuperação de desastres gerenciada e baseada em nuvem, garantindo recuperação rápida e tempo de inatividade mínimo durante desastres.

Consulte as soluções a seguir para obter detalhes técnicos.

- "DR usando BlueXP DRaaS para datastores VMFS"
- "DR usando BlueXP DRaaS para datastores NFS"

Configurar a proteção de dados 3-2-1 para VMware com o plug-in SnapCenter para BlueXP backup and recovery

Configure uma estratégia de proteção de dados 3-2-1 para ambientes VMware usando o plug-in SnapCenter para BlueXP backup and recovery. Este procedimento inclui a configuração de backups de VMs e armazenamentos de dados em clusters ONTAP

primários e secundários, a configuração do plug-in e do BlueXP e o gerenciamento da replicação de dados na nuvem ou em armazenamento externo para recuperação confiável.

A estratégia de backup 3-2-1 é um método de proteção de dados aceito pelo setor, fornecendo uma abordagem abrangente para proteger dados valiosos. Essa estratégia é confiável e garante que, mesmo se ocorrer algum desastre inesperado, ainda haverá uma cópia dos dados disponível.

Visão geral

A estratégia é composta por três regras fundamentais:

1. Mantenha pelo menos três cópias dos seus dados. Isso garante que, mesmo que uma cópia seja perdida ou corrompida, você ainda terá pelo menos duas cópias restantes para usar como reserva.
2. Armazene duas cópias de backup em diferentes mídias de armazenamento ou dispositivos. A diversificação da mídia de armazenamento ajuda a proteger contra falhas específicas do dispositivo ou da mídia. Se um dispositivo for danificado ou um tipo de mídia falhar, a outra cópia de backup permanecerá inalterada.
3. Por fim, certifique-se de que pelo menos uma cópia de backup esteja fora do local. O armazenamento externo serve como uma proteção contra desastres localizados, como incêndios ou inundações, que podem tornar cópias no local inutilizáveis.

Este documento de solução abrange uma solução de backups 3-2-1 usando o SnapCenter Plug-in for VMware vSphere (SCV) para criar backups primários e secundários de nossas máquinas virtuais locais e BlueXP backup and recovery para máquinas virtuais para fazer backup de uma cópia de nossos dados para armazenamento em nuvem ou StorageGRID.

Casos de uso

Esta solução aborda os seguintes casos de uso:

- Backup e restauração de máquinas virtuais e datastores locais usando o SnapCenter Plug-in for VMware vSphere.
- Backup e restauração de máquinas virtuais e datastores locais, hospedados em clusters ONTAP e com backup em armazenamento de objetos usando o BlueXP backup and recovery para máquinas virtuais.

Armazenamento de dados NetApp ONTAP

ONTAP é a solução de armazenamento líder do setor da NetApp que oferece armazenamento unificado, independentemente de você acessar por meio de protocolos SAN ou NAS. A estratégia de backup 3-2-1 garante que os dados locais sejam protegidos em mais de um tipo de mídia, e a NetApp oferece plataformas que vão desde flash de alta velocidade até mídia de baixo custo.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
Hybrid flash storage	**Capacity all-flash storage**	**Performance all-flash storage**	**All-flash SAN storage**
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

Para obter mais informações sobre todas as plataformas de hardware da NetApp, confira "Armazenamento de dados NetApp" .

SnapCenter Plug-in for VMware vSphere

O SnapCenter Plugin para VMware vSphere é uma oferta de proteção de dados totalmente integrada ao VMware vSphere e permite fácil gerenciamento de backup e restaurações para máquinas virtuais. Como parte dessa solução, o SnapMirror fornece um método rápido e confiável para criar uma segunda cópia de backup imutável de dados de máquina virtual em um cluster de armazenamento ONTAP secundário. Com essa arquitetura em vigor, as operações de restauração da máquina virtual podem ser facilmente iniciadas a partir dos locais de backup primário ou secundário.

O SCV é implantado como um dispositivo virtual Linux usando um arquivo OVA. O plug-in agora usa uma arquitetura de plug-in remoto. O plug-in remoto é executado fora do servidor vCenter e é hospedado no dispositivo virtual SCV.

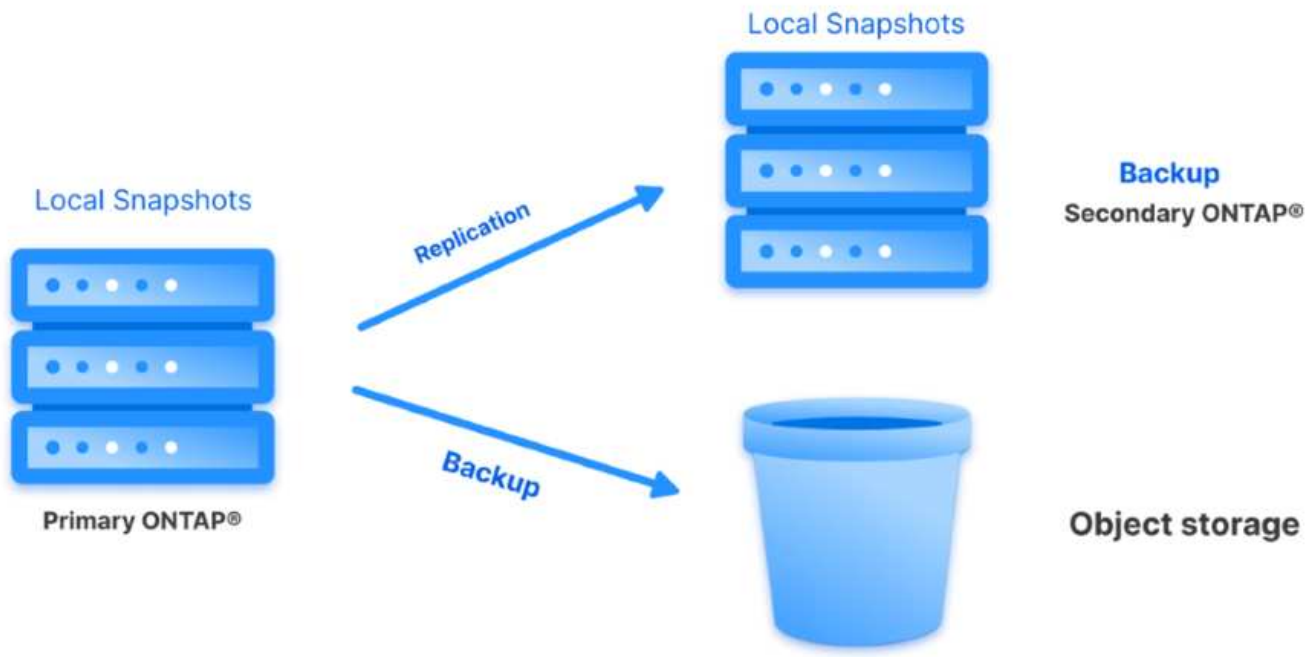
Para obter informações detalhadas sobre SCV, consulte "Documentação do SnapCenter Plug-in for VMware vSphere" .

BlueXP backup and recovery para máquinas virtuais

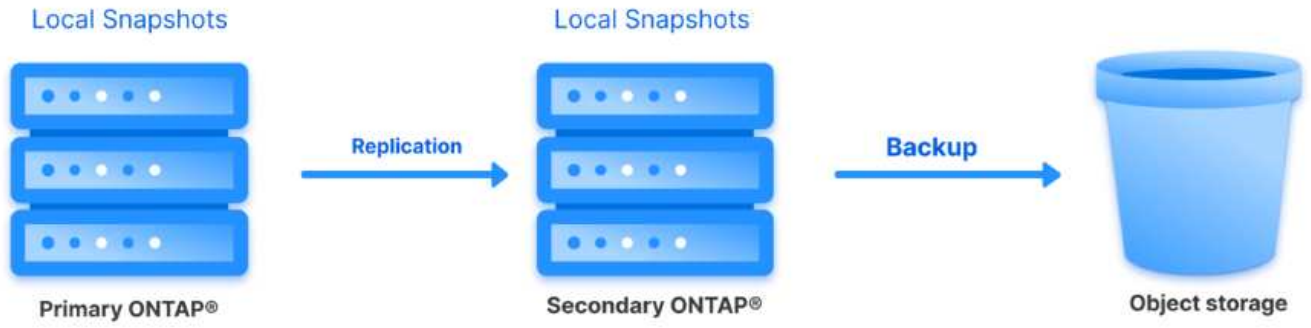
O BlueXP backup and recovery é uma ferramenta baseada em nuvem para gerenciamento de dados que fornece um único plano de controle para uma ampla gama de operações de backup e recuperação em ambientes locais e na nuvem. Parte do pacote de BlueXP backup and recovery do NetApp BlueXP é um recurso que se integra ao SnapCenter Plugin para VMware vSphere (local) para estender uma cópia dos dados para o armazenamento de objetos na nuvem. Isso estabelece uma terceira cópia dos dados fora do local, originada dos backups de armazenamento primário ou secundário. O BlueXP backup and recovery facilitam a configuração de políticas de armazenamento que transferem cópias dos seus dados de qualquer um desses dois locais locais.

A escolha entre os backups primário e secundário como origem no BlueXP Backup and Recovery resultará na implementação de uma das duas topologias:

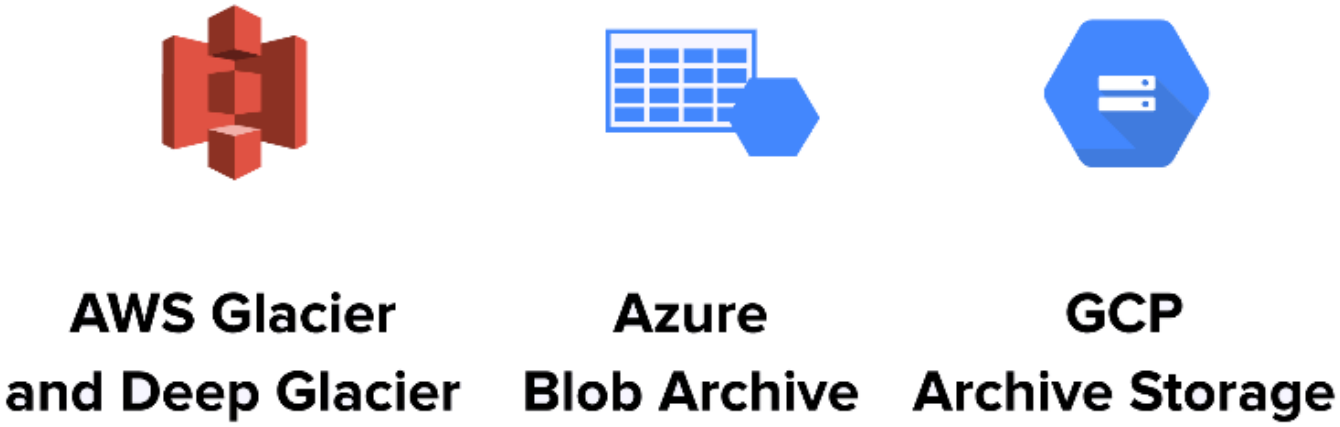
Topologia Fan-out – Quando um backup é iniciado pelo SnapCenter Plug-in for VMware vSphere, um instantâneo local é imediatamente tirado. O SCV então inicia uma operação SnapMirror que replica o instantâneo mais recente para o cluster ONTAP secundário. No BlueXP Backup and Recovery, uma política especifica o cluster ONTAP primário como a origem de uma cópia instantânea dos dados a serem transferidos para o armazenamento de objetos no provedor de nuvem de sua escolha.



Topologia em cascata – A criação de cópias de dados primárias e secundárias usando SCV é idêntica à topologia de fan-out mencionada acima. Entretanto, desta vez, uma política é criada no BlueXP Backup and Recovery especificando que o backup para armazenamento de objetos será originado do cluster ONTAP secundário.



O BlueXP backup and recovery podem criar cópias de backup de instantâneos ONTAP locais para armazenamento AWS Glacier, Azure Blob e GCP Archive.



Além disso, você pode usar o NetApp StorageGRID como destino de backup de armazenamento de objetos. Para mais informações sobre StorageGRID , consulte o "Página inicial do StorageGRID" .

Visão geral da implantação da solução

Esta lista fornece as etapas de alto nível necessárias para configurar esta solução e executar operações de backup e restauração do SCV e do BlueXP backup and recovery:

1. Configure o relacionamento do SnapMirror entre os clusters ONTAP a serem usados para cópias de dados primárias e secundárias.
2. Configurar o SnapCenter Plug-In para VMware vSphere.
   a. Adicionar sistemas de armazenamento
   b. Criar políticas de backup
   c. Criar grupos de recursos
   d. Execute os primeiros trabalhos de backup
3. Configurar BlueXP backup and recovery para máquinas virtuais
   a. Adicionar ambiente de trabalho
   b. Descubra os dispositivos SCV e vCenter
   c. Criar políticas de backup
   d. Ativar backups
4. Restaure máquinas virtuais do armazenamento primário e secundário usando SCV.
5. Restaure máquinas virtuais do armazenamento de objetos usando backup e restauração do BlueXP .

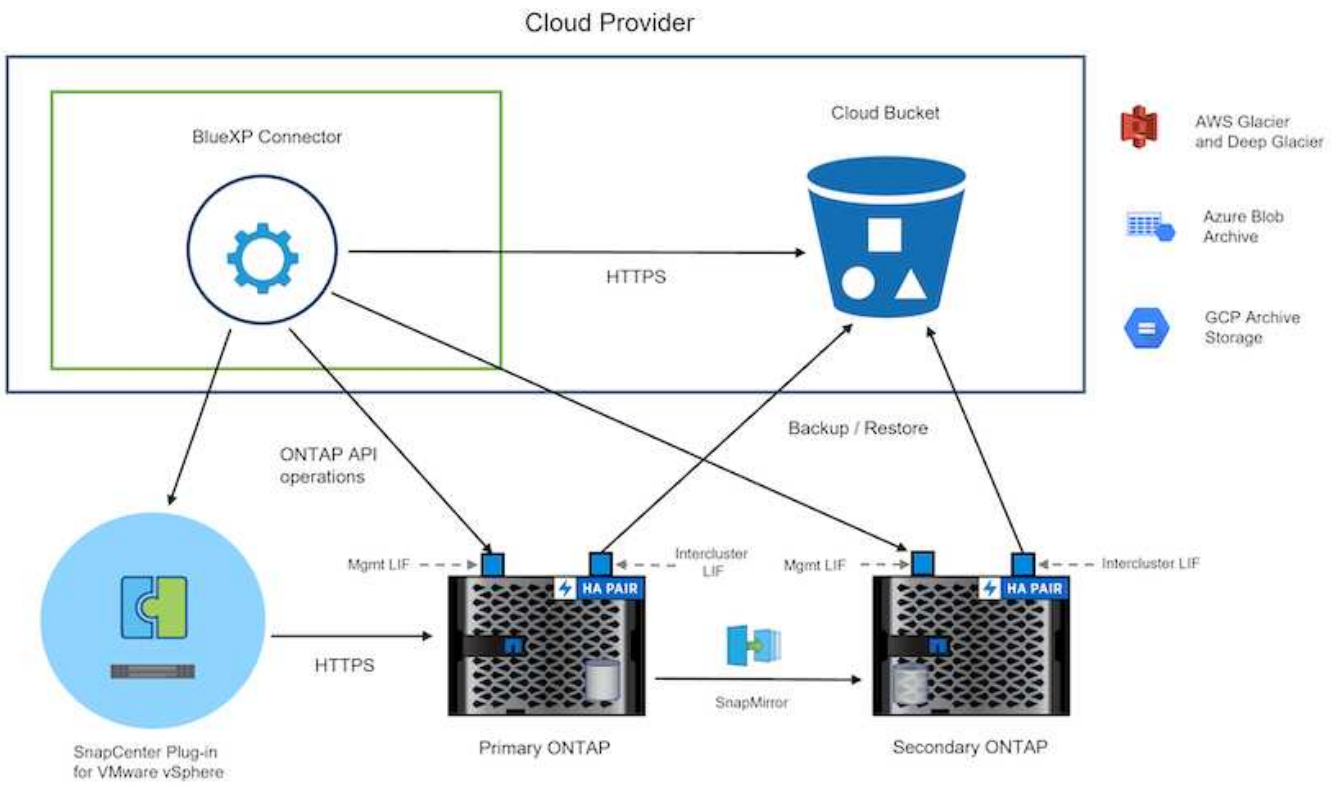
Pré-requisitos

O objetivo desta solução é demonstrar a proteção de dados de máquinas virtuais em execução no VMware vSphere, domínios de carga de trabalho VCF VI ou domínios de gerenciamento VCF. As máquinas virtuais nesta solução são hospedadas em armazenamentos de dados NFS fornecidos pelo NetApp ONTAP. Esta solução pressupõe que os seguintes componentes estejam configurados e prontos para uso:

1. Cluster de armazenamento ONTAP com datastores NFS ou VMFS conectados ao VMware vSphere. Os armazenamentos de dados NFS e VMFS são suportados. Os datastores NFS foram utilizados para esta solução.
2. Cluster de armazenamento ONTAP secundário com relacionamentos SnapMirror estabelecidos para volumes usados para armazenamentos de dados NFS.
3. Conector BlueXP instalado para provedor de nuvem usado para backups de armazenamento de objetos.
4. As máquinas virtuais a serem apoiadas estão em armazenamentos de dados NFS que residem no cluster de armazenamento ONTAP primário.
5. Conectividade de rede entre o conector BlueXP e as interfaces de gerenciamento de cluster de armazenamento ONTAP local.
6. Conectividade de rede entre o conector BlueXP e a VM do dispositivo SCV local e entre o conector BlueXP e o vCenter.
7. Conectividade de rede entre os LIFs intercluster ONTAP locais e o serviço de armazenamento de objetos.
8. DNS configurado para gerenciamento de SVM em clusters de armazenamento ONTAP primário e secundário. Para mais informações consulte "Configurar DNS para resolução de nome de host" .

Arquitetura de Alto Nível

O teste/validação desta solução foi realizado em um laboratório que pode ou não corresponder ao ambiente de implantação final.



Implantação de solução

Nesta solução, fornecemos instruções detalhadas para implantar e validar uma solução que utiliza o SnapCenter Plug-in for VMware vSphere, juntamente com o BlueXP backup and recovery, para executar o backup e a recuperação de máquinas virtuais Windows e Linux em um cluster VMware vSphere localizado em um data center local. As máquinas virtuais nesta configuração são armazenadas em datastores NFS hospedados por um cluster de armazenamento ONTAP A300. Além disso, um cluster de armazenamento ONTAP A300 separado serve como destino secundário para volumes replicados usando o SnapMirror. Além disso, o armazenamento de objetos hospedado no Amazon Web Services e no Azure Blob foram empregados como alvos para uma terceira cópia dos dados.

Abordaremos a criação de relacionamentos SnapMirror para cópias secundárias de nossos backups gerenciados pelo SCV e a configuração de tarefas de backup no BlueXP backup and recovery.

Para obter informações detalhadas sobre o SnapCenter Plug-in for VMware vSphere, consulte o "Documentação do SnapCenter Plug-in for VMware vSphere" .

Para obter informações detalhadas sobre BlueXP backup and recovery, consulte o "Documentação de BlueXP backup and recovery" .

Estabelecer relacionamentos SnapMirror entre clusters ONTAP

O SnapCenter Plug-in for VMware vSphere usa a tecnologia ONTAP SnapMirror para gerenciar o transporte de cópias secundárias do SnapMirror e/ou SnapVault para um cluster ONTAP secundário.

As políticas de backup do SCV têm a opção de usar relacionamentos SnapMirror ou SnapVault . A principal diferença é que, ao usar a opção SnapMirror , o cronograma de retenção configurado para backups na política será o mesmo nos locais primário e secundário. O SnapVault foi projetado para arquivamento e, ao usar essa opção, um cronograma de retenção separado pode ser estabelecido com o relacionamento SnapMirror para as cópias de instantâneo no cluster de armazenamento ONTAP secundário.

A configuração de relacionamentos do SnapMirror pode ser feita no BlueXP , onde muitas etapas são automatizadas, ou pode ser feita usando o System Manager e o ONTAP CLI. Todos esses métodos são discutidos abaixo.

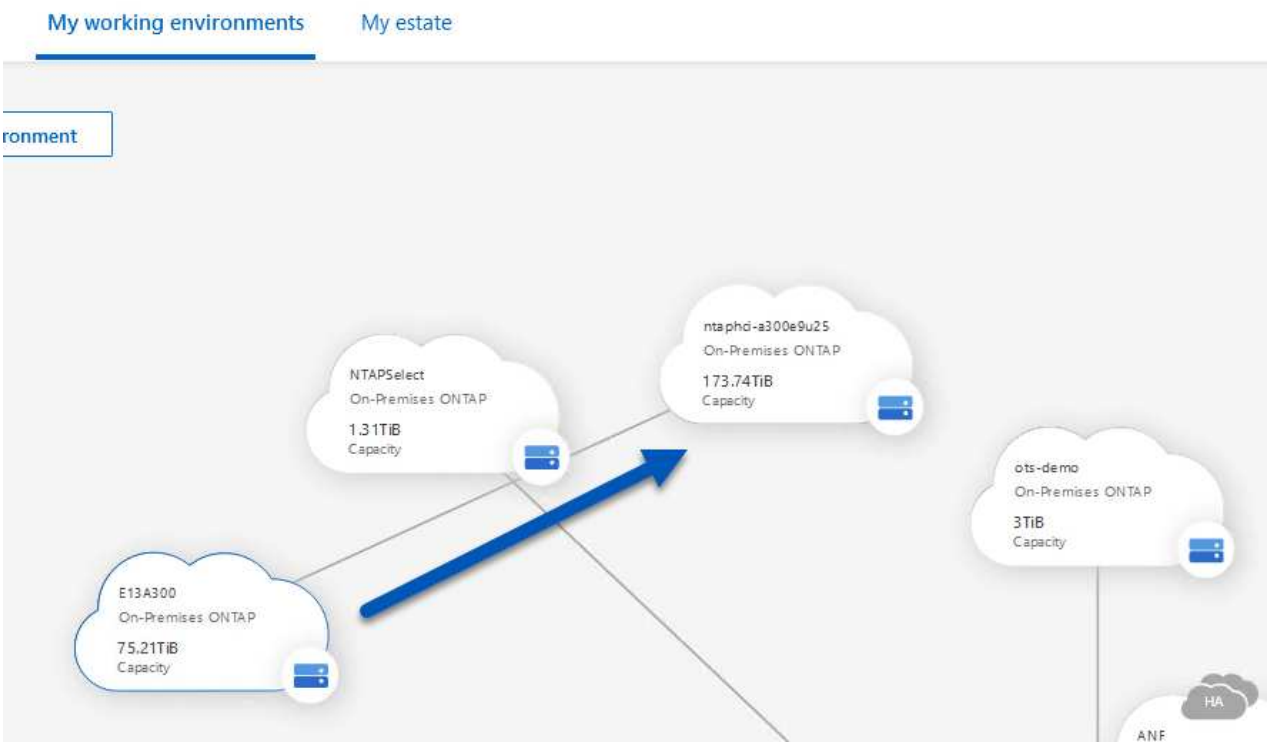
Estabelecer relacionamentos SnapMirror com BlueXP

As seguintes etapas devem ser concluídas no console da web BlueXP :

Configuração de replicação para sistemas de armazenamento ONTAP primário e secundário

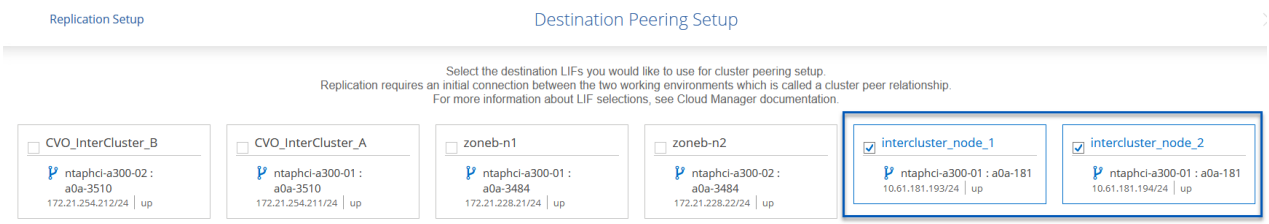
Comece fazendo login no console web do BlueXP e navegando até o Canvas.

1. Arraste e solte o sistema de armazenamento ONTAP de origem (primário) no sistema de armazenamento ONTAP de destino (secundário).

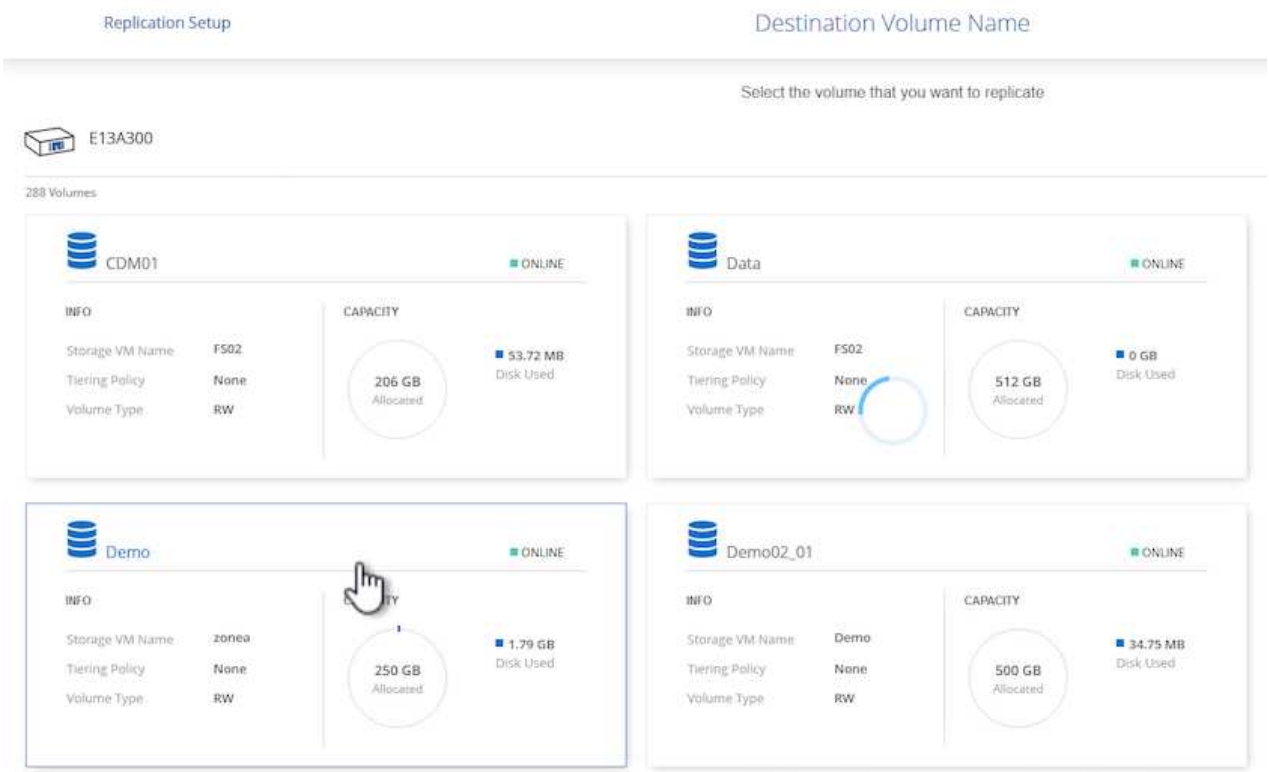


2. No menu que aparece, selecione **Replicação**.

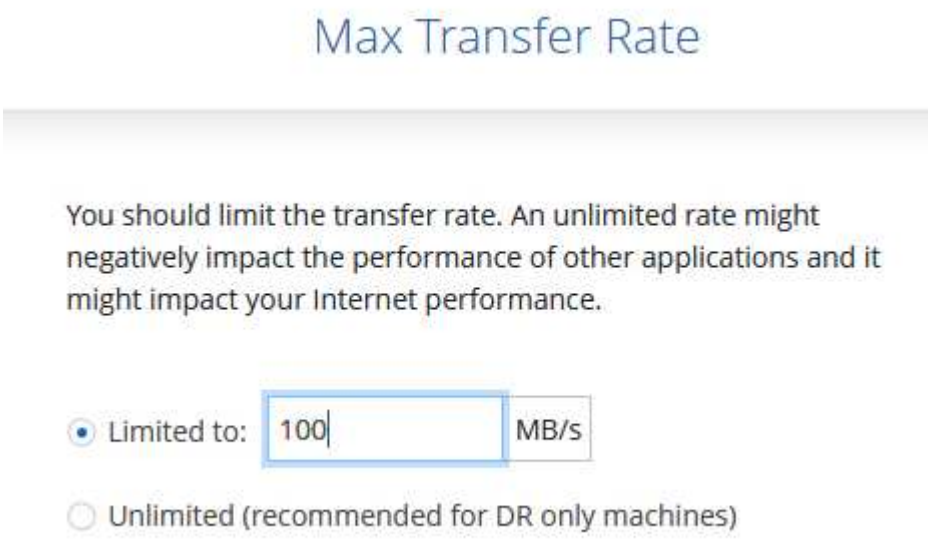
3. Na página **Configuração de peering de destino**, selecione os LIFs Intercluster de destino a serem usados para a conexão entre sistemas de armazenamento.



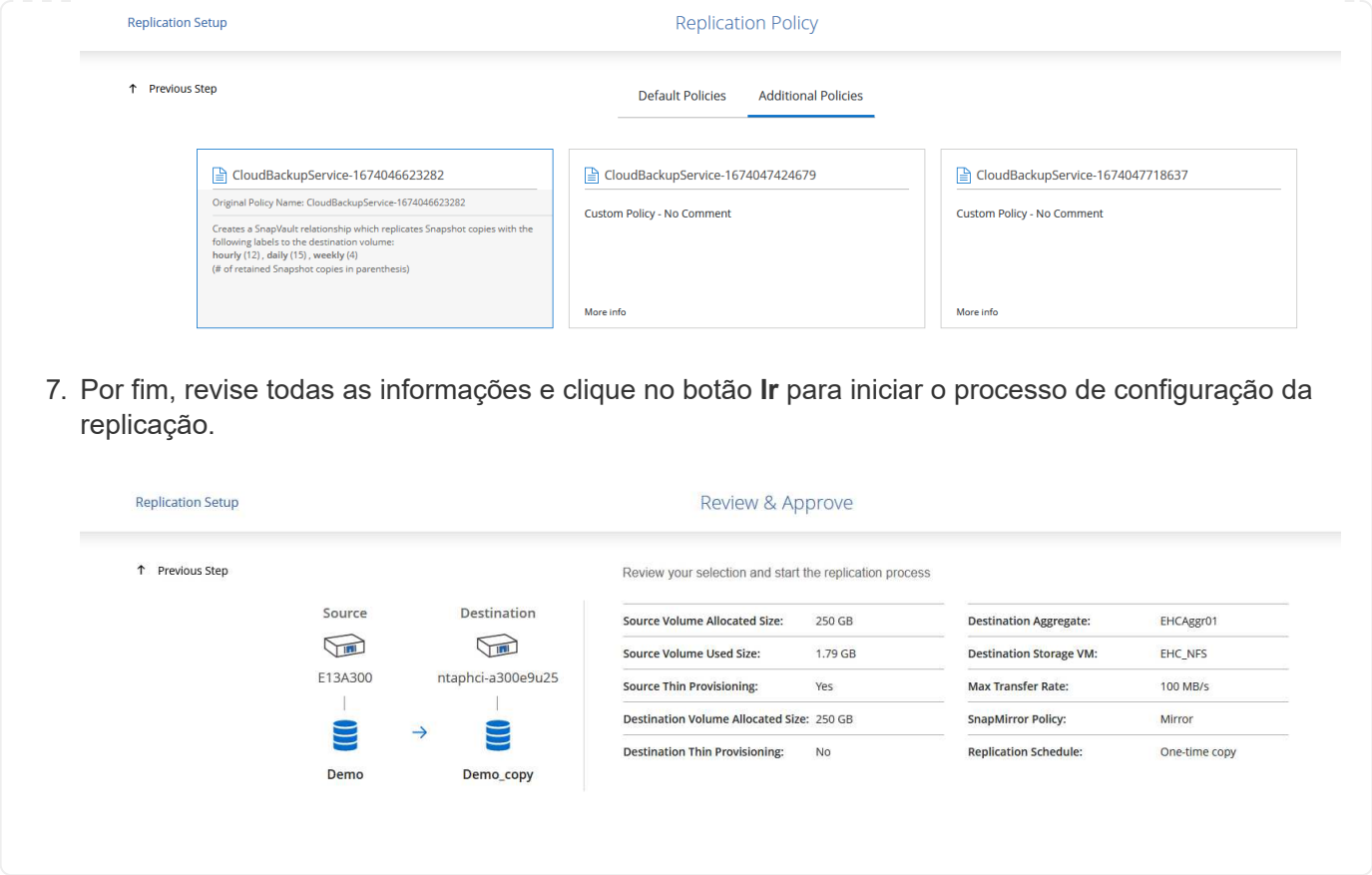
4. Na página **Nome do volume de destino**, primeiro selecione o volume de origem, depois preencha o nome do volume de destino e selecione o SVM de destino e o agregado. Clique em **Avançar** para continuar.



5. Escolha a taxa máxima de transferência para que a replicação ocorra.



6. Escolha a política que determinará o cronograma de retenção para backups secundários. Esta política pode ser criada previamente (veja o processo manual abaixo na etapa **Criar uma política de retenção de snapshots**) ou pode ser alterada posteriormente, se desejado.



7. Por fim, revise todas as informações e clique no botão **Ir** para iniciar o processo de configuração da replicação.

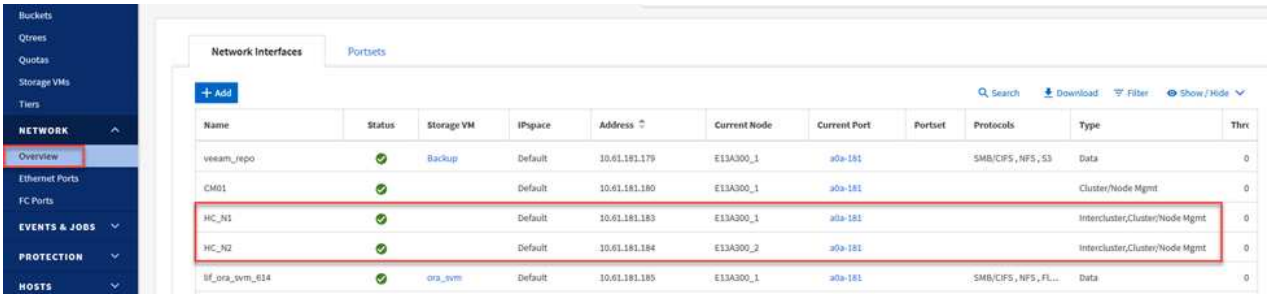
Estabelecer relacionamentos do SnapMirror com o System Manager e o ONTAP CLI

Todas as etapas necessárias para estabelecer relacionamentos do SnapMirror podem ser realizadas com o System Manager ou o ONTAP CLI. A seção a seguir fornece informações detalhadas para ambos os métodos:

Registre as interfaces lógicas do Intercluster de origem e destino

Para os clusters ONTAP de origem e destino, você pode recuperar as informações de LIF entre clusters do System Manager ou da CLI.

1. No ONTAP System Manager, navegue até a página Visão geral da rede e recupere os endereços IP do Tipo: Intercluster que estão configurados para se comunicar com a VPC da AWS onde o FSx está instalado.



2. Para recuperar os endereços IP do Intercluster usando a CLI, execute o seguinte comando:

```
ONTAP-Dest::> network interface show -role intercluster
```

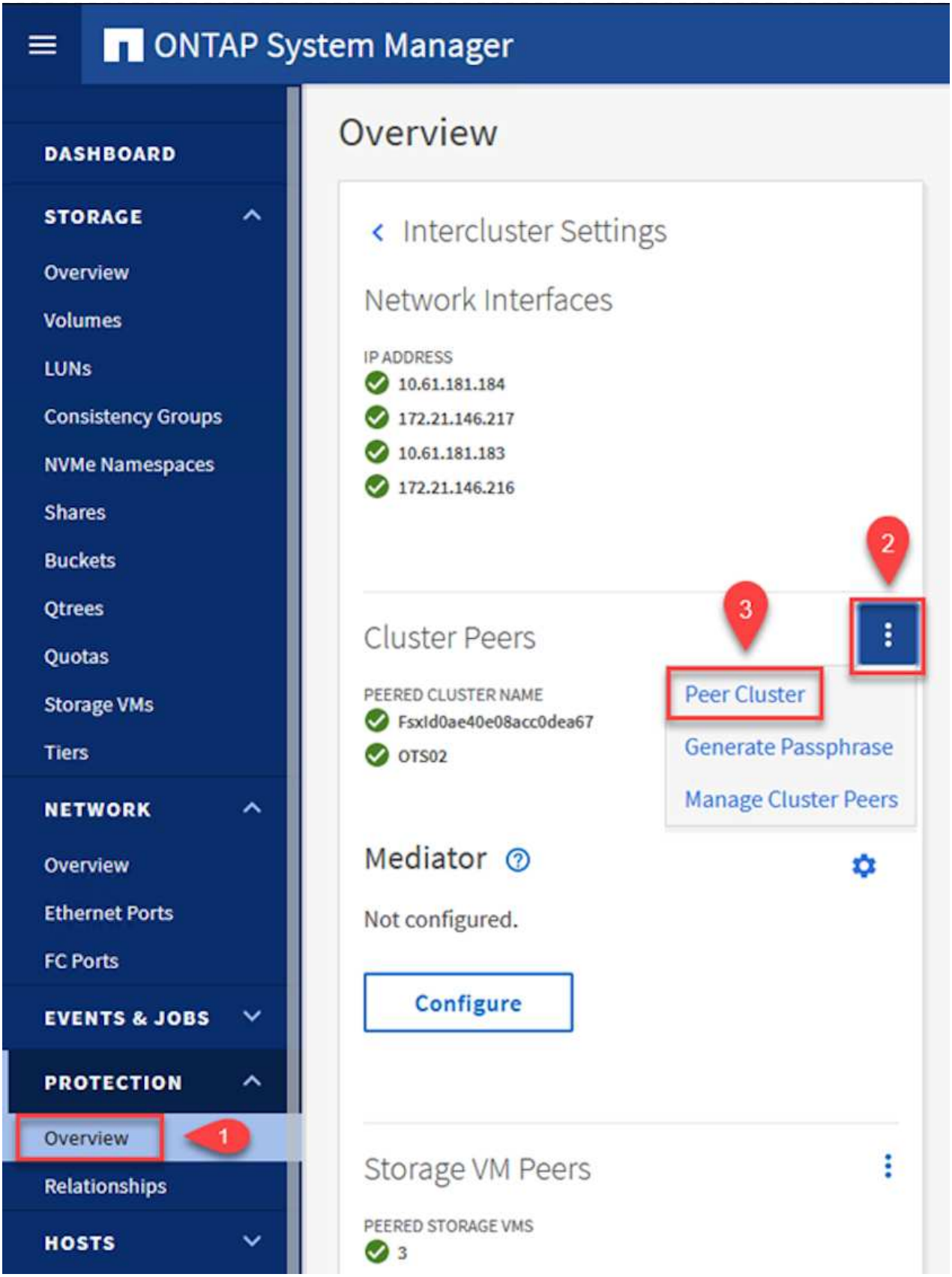
Estabelecer peering de cluster entre clusters ONTAP

Para estabelecer o peering de cluster entre clusters ONTAP , uma senha exclusiva inserida no cluster ONTAP inicial deve ser confirmada no outro cluster peer.

1. Configure o peering no cluster ONTAP de destino usando o `cluster peer create` comando. Quando solicitado, insira uma senha exclusiva que será usada posteriormente no cluster de origem para finalizar o processo de criação.

   ```
   ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
   source_intercluster_1, source_intercluster_2
   Enter the passphrase:
   Confirm the passphrase:
   ```

2. No cluster de origem, você pode estabelecer o relacionamento de pares do cluster usando o ONTAP System Manager ou a CLI. No ONTAP System Manager, navegue até Proteção > Visão geral e selecione Cluster de pares.

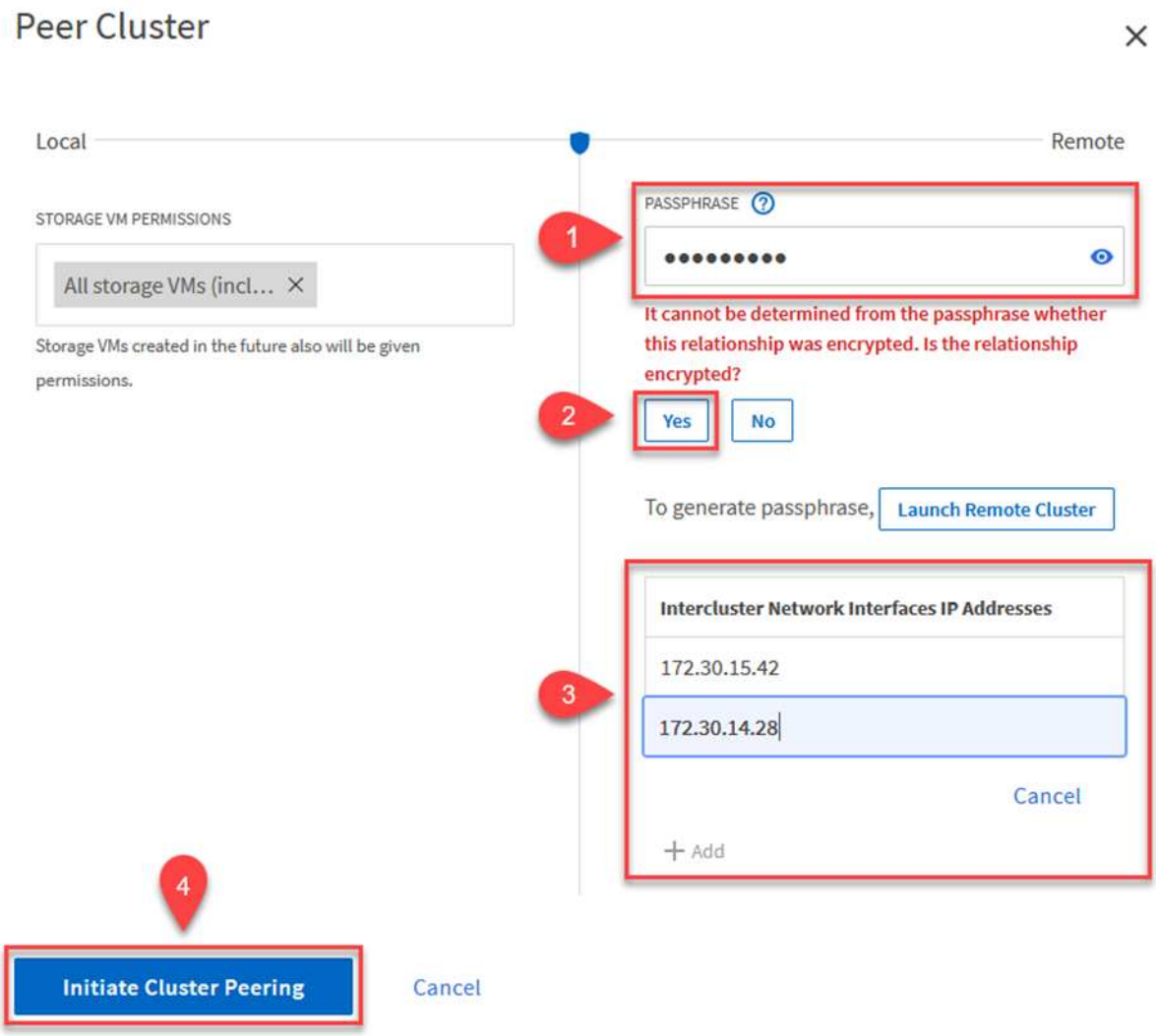


3. Na caixa de diálogo Cluster de Pares, preencha as informações necessárias:
   a. Digite a senha que foi usada para estabelecer o relacionamento do cluster de pares no cluster ONTAP de destino.

b. Selecione `Yes` para estabelecer um relacionamento criptografado.

c. Insira o(s) endereço(s) IP do LIF intercluster do cluster ONTAP de destino.

d. Clique em Iniciar peering de cluster para finalizar o processo.



4. Verifique o status do relacionamento entre pares do cluster do cluster ONTAP de destino com o seguinte comando:

```
ONTAP-Dest::> cluster peer show
```

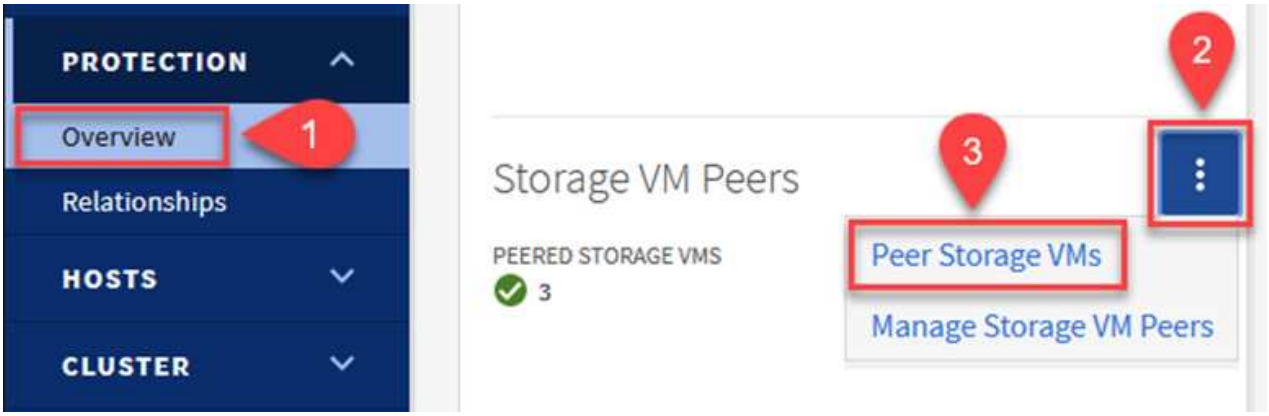
Estabelecer relacionamento de peering SVM

A próxima etapa é configurar um relacionamento SVM entre as máquinas virtuais de armazenamento de destino e de origem que contêm os volumes que estarão nos relacionamentos SnapMirror .

1. No cluster ONTAP de destino, use o seguinte comando da CLI para criar o relacionamento de peer SVM:

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. No cluster ONTAP de origem, aceite o relacionamento de peering com o ONTAP System Manager ou a CLI.
3. No ONTAP System Manager, acesse Proteção > Visão geral e selecione VMs de armazenamento peer em Pares de VM de armazenamento.



4. Na caixa de diálogo da VM de armazenamento de pares, preencha os campos obrigatórios:
   - A VM de armazenamento de origem
   - O cluster de destino
   - A VM de armazenamento de destino

5. Clique em VMs de armazenamento de pares para concluir o processo de peering de SVM.

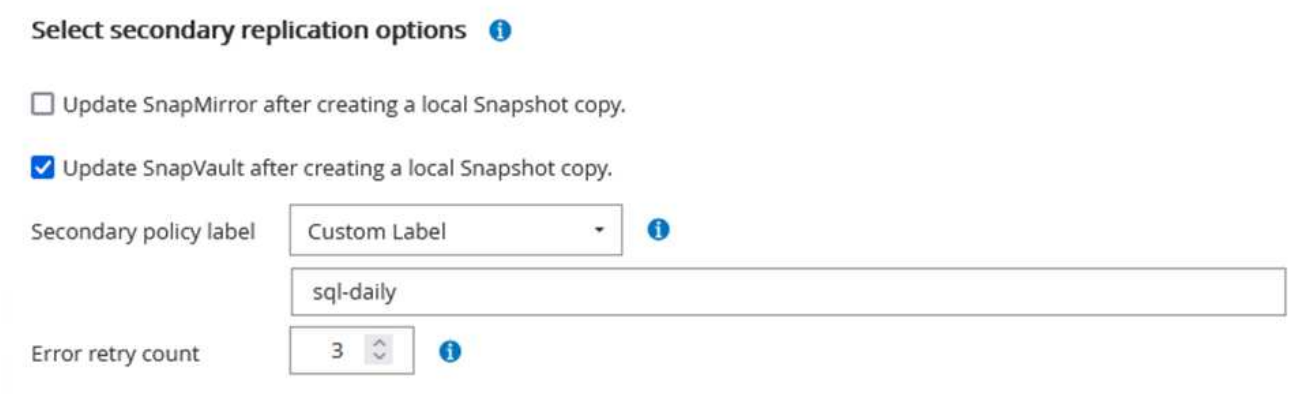
Crie uma política de retenção de instantâneos

O SnapCenter gerencia agendamentos de retenção para backups que existem como cópias instantâneas no sistema de armazenamento primário. Isso é estabelecido ao criar uma política no SnapCenter. O SnapCenter não gerencia políticas de retenção para backups retidos em sistemas de armazenamento secundário. Essas políticas são gerenciadas separadamente por meio de uma política SnapMirror criada no cluster FSx secundário e associada aos volumes de destino que estão em um relacionamento SnapMirror com o volume de origem.

Ao criar uma política do SnapCenter , você tem a opção de especificar um rótulo de política secundária que é adicionado ao rótulo do SnapMirror de cada instantâneo gerado quando um backup do SnapCenter é feito.

> No armazenamento secundário, esses rótulos são correspondidos às regras de política associadas ao volume de destino com a finalidade de impor a retenção de instantâneos.

O exemplo a seguir mostra um rótulo SnapMirror que está presente em todos os snapshots gerados como parte de uma política usada para backups diários do nosso banco de dados SQL Server e volumes de log.



Para obter mais informações sobre como criar políticas do SnapCenter para um banco de dados SQL Server, consulte o "Documentação do SnapCenter" .

Primeiro, você deve criar uma política do SnapMirror com regras que determinem o número de cópias de snapshots a serem retidas.

1. Crie a política SnapMirror no cluster FSx.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Adicione regras à política com rótulos do SnapMirror que correspondam aos rótulos de política secundária especificados nas políticas do SnapCenter .

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

O script a seguir fornece um exemplo de uma regra que pode ser adicionada a uma política:

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Crie regras adicionais para cada rótulo SnapMirror e o número de snapshots a serem retidos (período de retenção).

Criar volumes de destino

Para criar um volume de destino no ONTAP que será o destinatário de cópias de instantâneos dos nossos volumes de origem, execute o seguinte comando no cluster ONTAP de destino:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Crie os relacionamentos SnapMirror entre os volumes de origem e destino

Para criar um relacionamento SnapMirror entre um volume de origem e de destino, execute o seguinte comando no cluster ONTAP de destino:

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Inicializar os relacionamentos do SnapMirror

Inicialize o relacionamento SnapMirror . Este processo inicia um novo instantâneo gerado a partir do volume de origem e o copia para o volume de destino.

Para criar um volume, execute o seguinte comando no cluster ONTAP de destino:

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Configurar o SnapCenter Plug-in for VMware vSphere

Uma vez instalado, o SnapCenter Plug-in for VMware vSphere pode ser acessado na interface de gerenciamento de dispositivos do vCenter Server. O SCV gerenciará backups para os armazenamentos de dados NFS montados nos hosts ESXi e que contêm as VMs Windows e Linux.

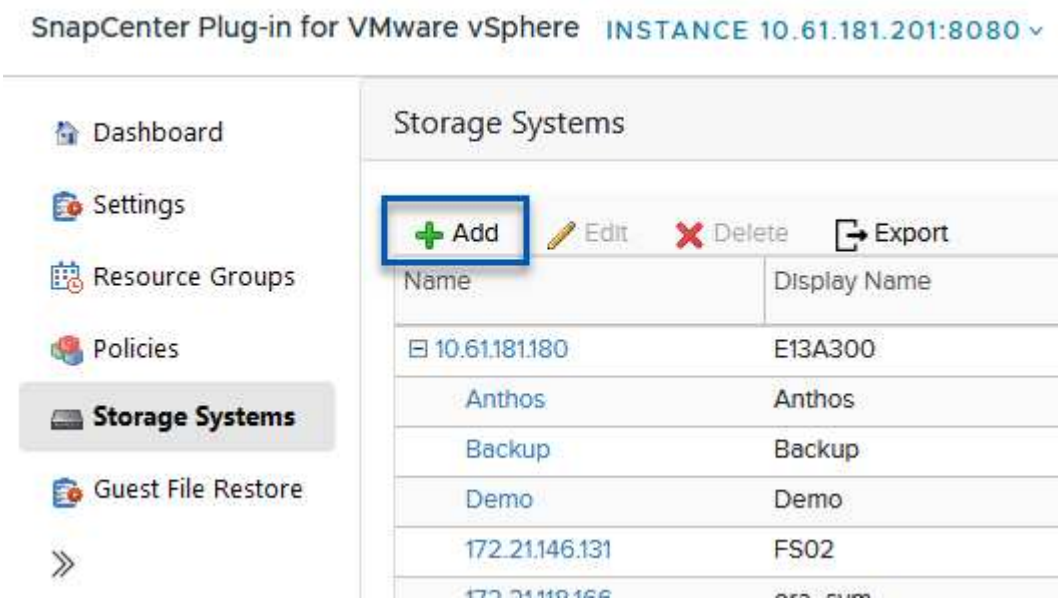
Revise o "Fluxo de trabalho de proteção de dados" seção da documentação do SCV para obter mais informações sobre as etapas envolvidas na configuração de backups.

Para configurar backups de suas máquinas virtuais e armazenamentos de dados, as seguintes etapas precisarão ser concluídas na interface do plug-in.

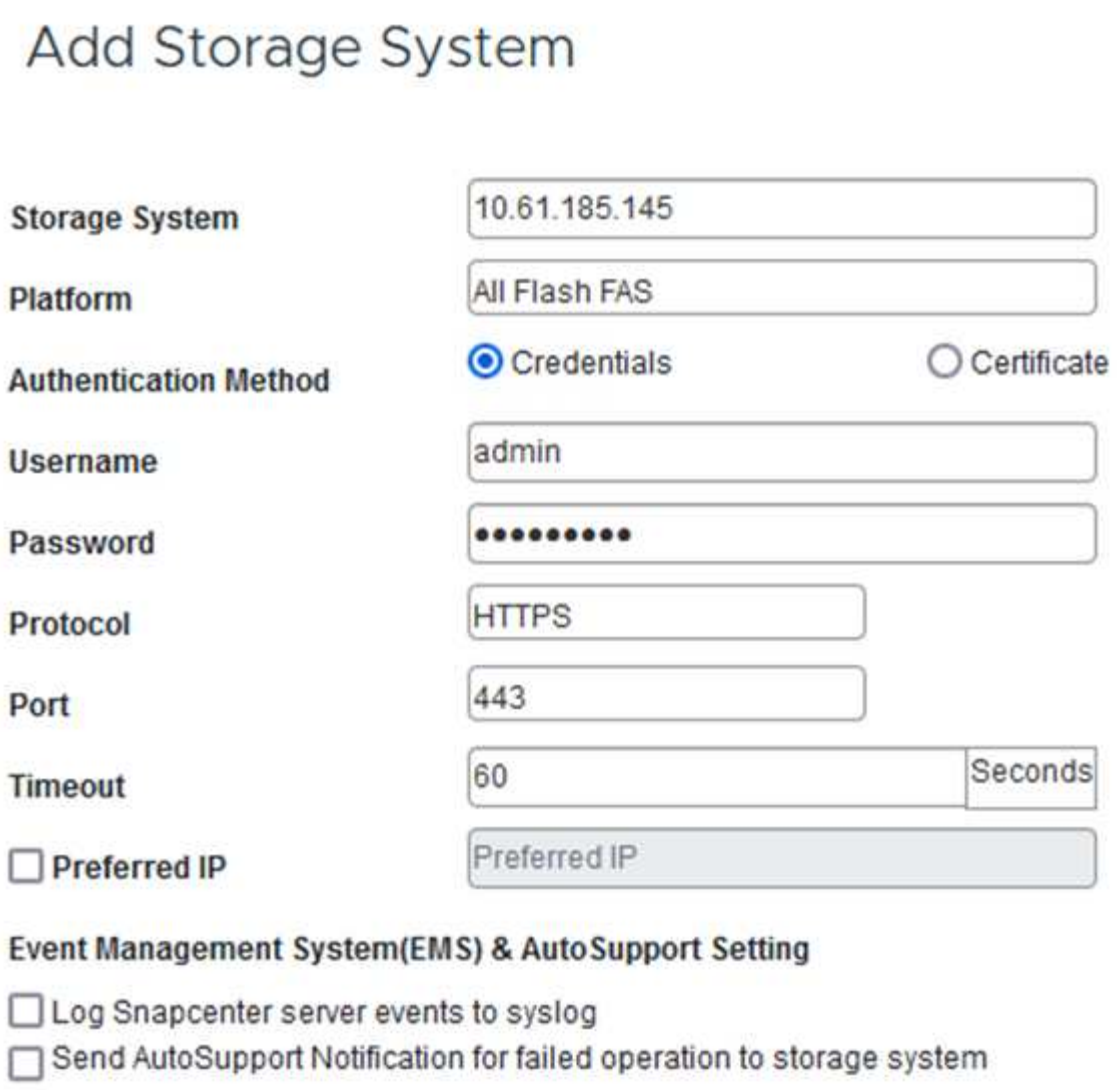
Sistemas de armazenamento Discovery ONTAP

Descubra os clusters de armazenamento ONTAP que podem ser usados para backups primários e secundários.

1. No SnapCenter Plug-in for VMware vSphere, navegue até **Sistemas de armazenamento** no menu à esquerda e clique no botão **Adicionar**.



2. Preencha as credenciais e o tipo de plataforma para o sistema de armazenamento ONTAP primário e clique em **Adicionar**.



3. Repita este procedimento para o sistema de armazenamento ONTAP secundário.

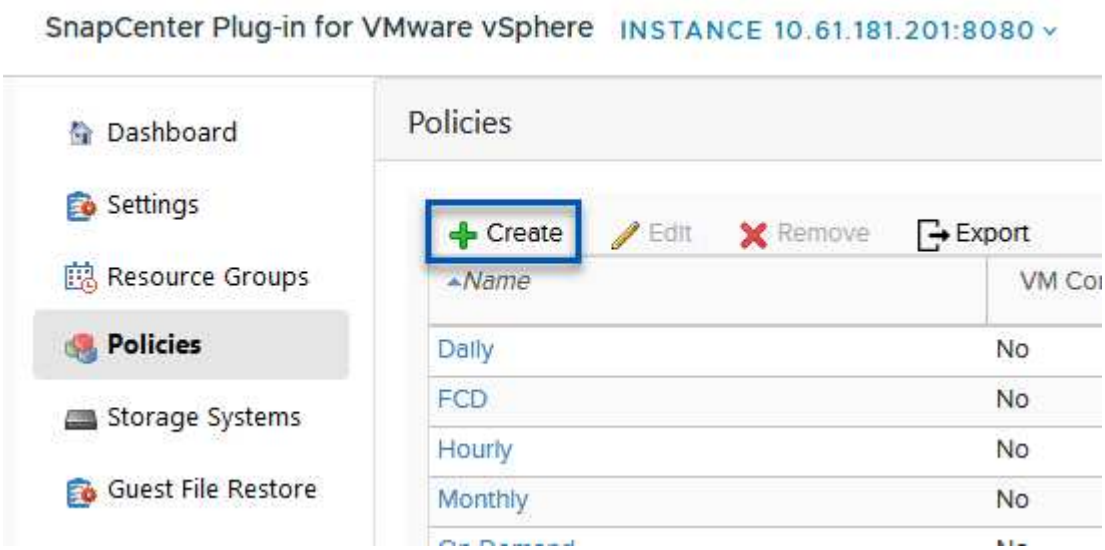
Criar políticas de backup do SCV

As políticas especificam o período de retenção, a frequência e as opções de replicação para os backups gerenciados pelo SCV.

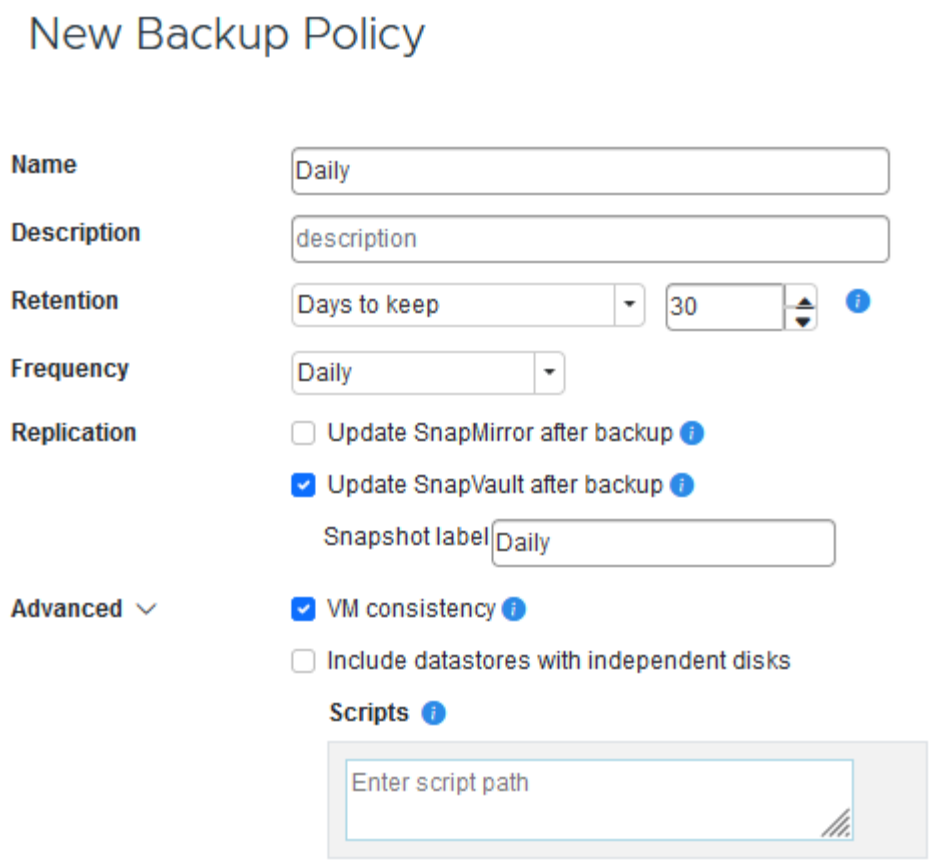
Revise o "Crie políticas de backup para VMs e armazenamentos de dados" seção da documentação para mais informações.

Para criar políticas de backup, conclua as seguintes etapas:

1. No SnapCenter Plug-in for VMware vSphere, navegue até **Políticas** no menu à esquerda e clique no botão **Criar**.



2. Especifique um nome para a política, período de retenção, frequência e opções de replicação, e rótulo de instantâneo.



Ao criar uma política no plug-in SnapCenter , você verá opções para SnapMirror e SnapVault. Se você escolher SnapMirror, o cronograma de retenção especificado na política será o mesmo para os snapshots primário e secundário. Se você escolher SnapVault, o cronograma de retenção para o snapshot secundário será baseado em um cronograma separado implementado com o relacionamento SnapMirror . Isso é útil quando você deseja períodos de retenção mais longos para backups secundários.

Os rótulos de instantâneo são úteis porque podem ser usados para promulgar políticas com um período de retenção específico para as cópias do SnapVault replicadas para o cluster ONTAP secundário. Quando o SCV é usado com o BlueXP Backup and Restore, o campo Rótulo do instantâneo deve estar em branco ou corresponder ao rótulo especificado na política de backup do BlueXP .

3. Repita o procedimento para cada política necessária. Por exemplo, políticas separadas para backups diários, semanais e mensais.

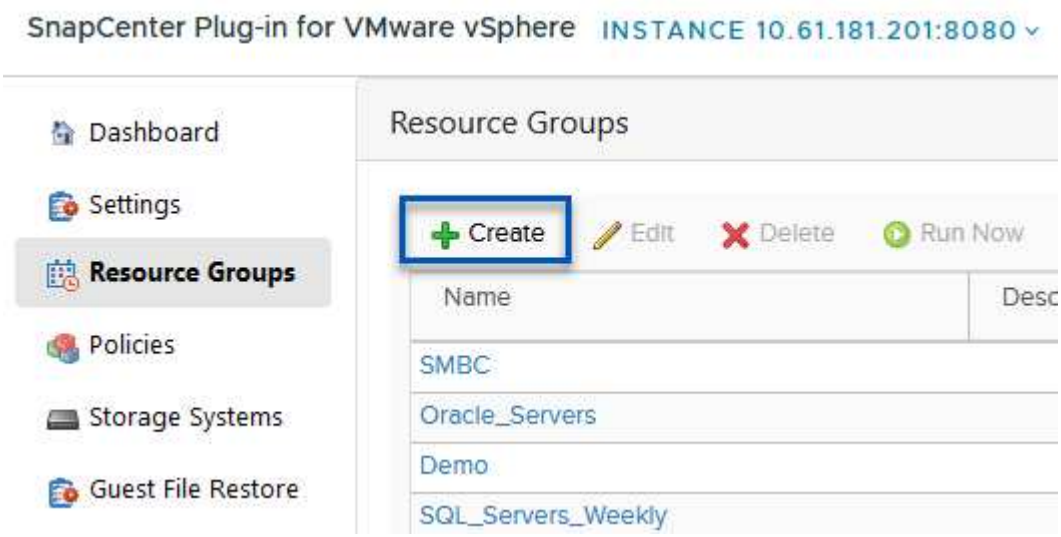
Criar grupos de recursos

Os grupos de recursos contêm os armazenamentos de dados e as máquinas virtuais a serem incluídos em uma tarefa de backup, juntamente com a política e o cronograma de backup associados.

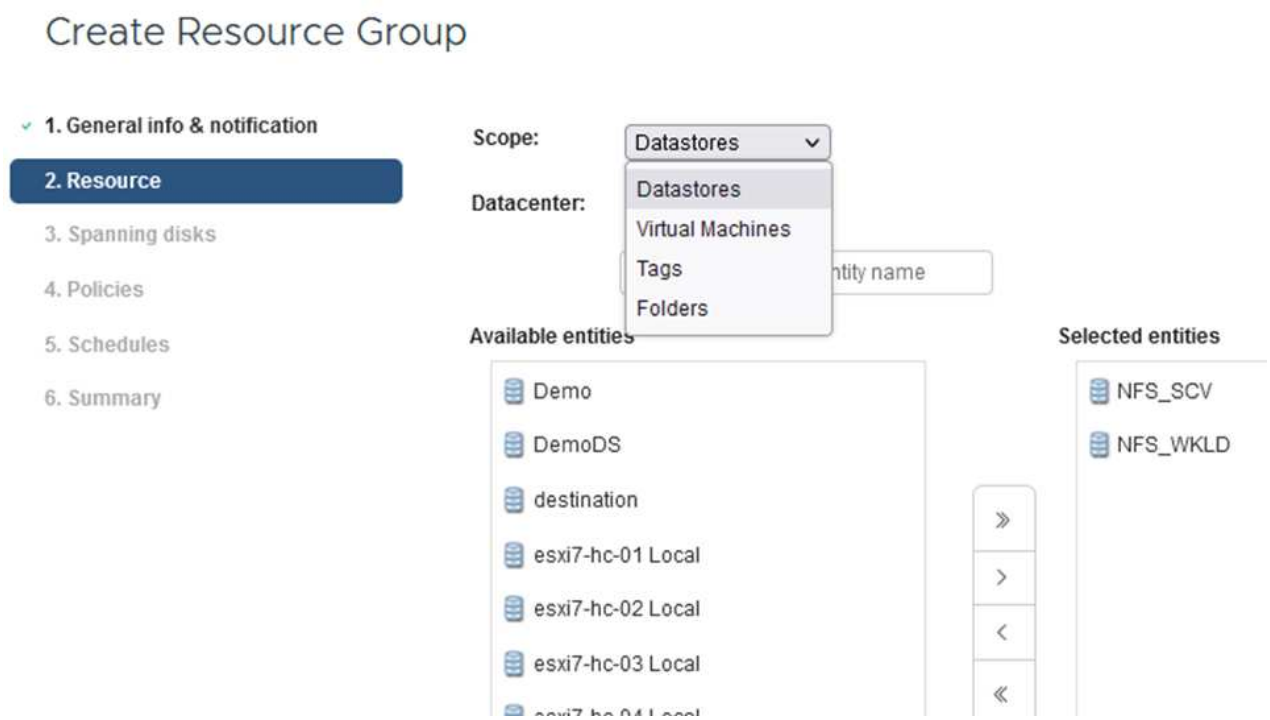
Revise o "Criar grupos de recursos" seção da documentação para mais informações.

Para criar grupos de recursos, conclua as seguintes etapas.

1. No SnapCenter Plug-in for VMware vSphere, navegue até **Grupos de recursos** no menu à esquerda e clique no botão **Criar**.

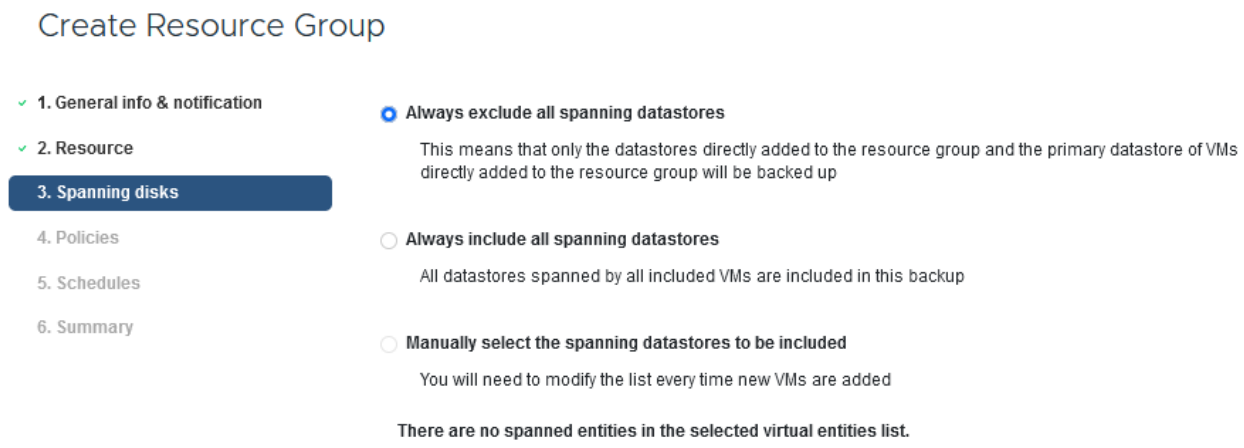


2. No assistente Criar grupo de recursos, insira um nome e uma descrição para o grupo, bem como as informações necessárias para receber notificações. Clique em **Avançar**
3. Na próxima página, selecione os armazenamentos de dados e máquinas virtuais que desejam ser incluídos na tarefa de backup e clique em **Avançar**.



Você tem a opção de selecionar VMs específicas ou armazenamentos de dados inteiros. Independentemente de qual você escolher, todo o volume (e armazenamento de dados) será copiado, pois o backup é o resultado da criação de um instantâneo do volume subjacente. Na maioria dos casos, é mais fácil escolher o armazenamento de dados inteiro. No entanto, se desejar limitar a lista de VMs disponíveis ao restaurar, você pode escolher apenas um subconjunto de VMs para backup.

4. Escolha opções para abranger datastores para VMs com VMDKs que residem em vários datastores e clique em **Avançar**.

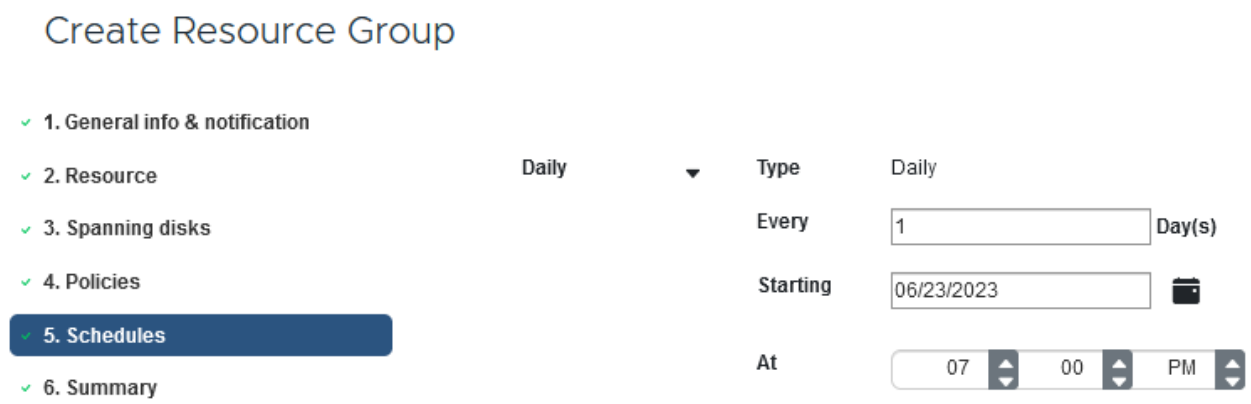


Atualmente, o BlueXP backup and recovery não oferecem suporte ao backup de VMs com VMDKs que abrangem vários armazenamentos de dados.

5. Na próxima página, selecione as políticas que serão associadas ao grupo de recursos e clique em **Avançar**.

Ao fazer backup de snapshots gerenciados pelo SCV para armazenamento de objetos usando o BlueXP backup and recovery, cada grupo de recursos só pode ser associado a uma única política.

6. Selecione uma programação que determinará em que horários os backups serão executados. Clique em **Avançar**.

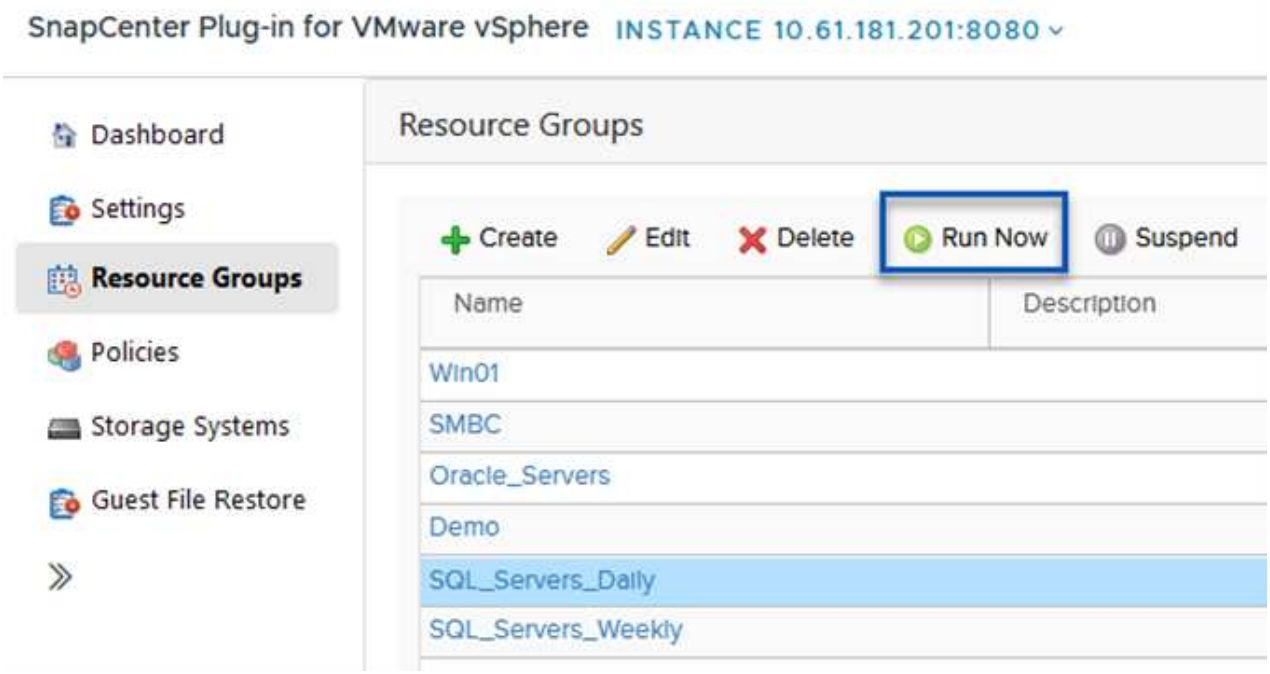


7. Por fim, revise a página de resumo e clique em **Concluir** para finalizar a criação do grupo de recursos.

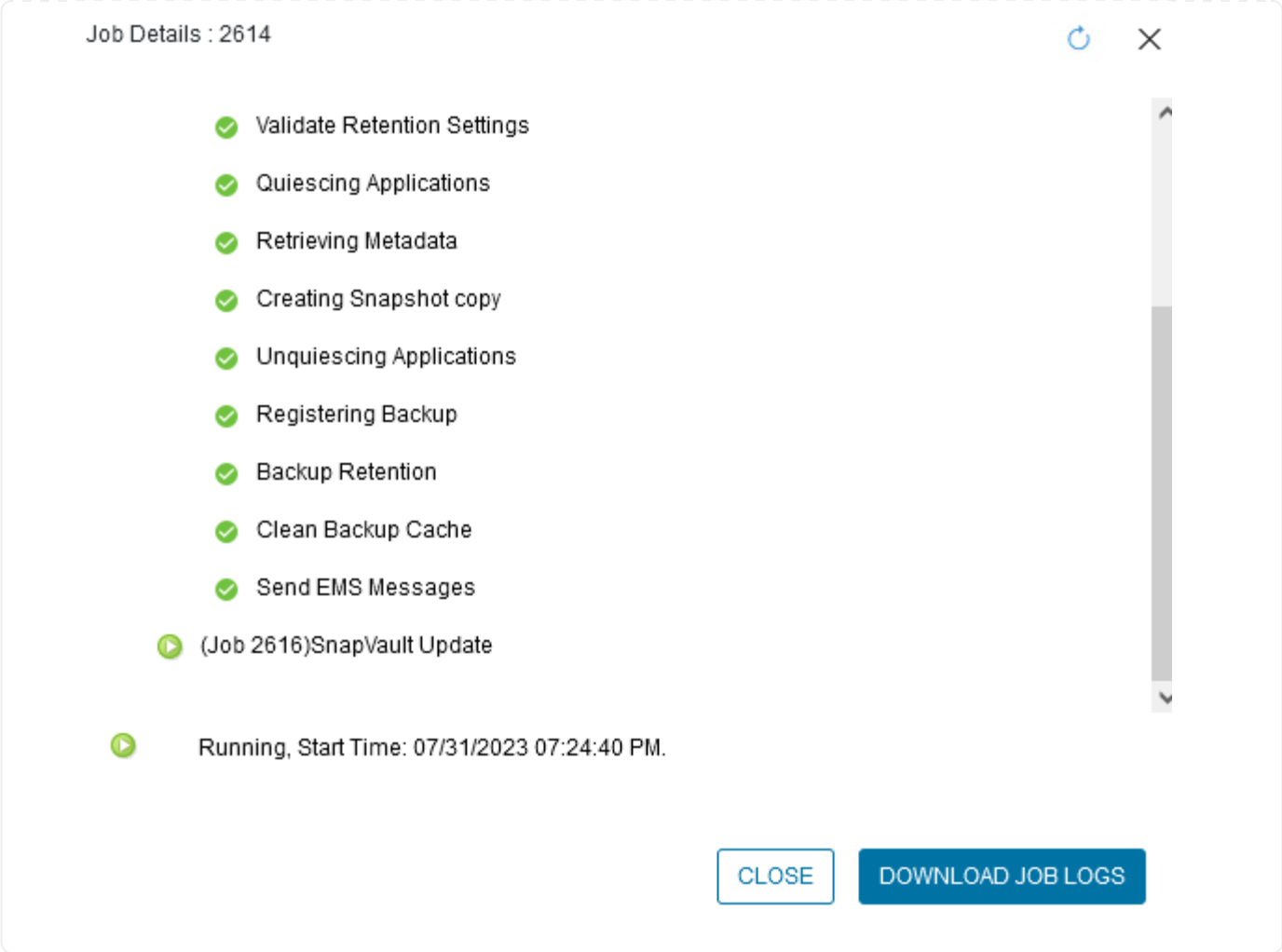
Executar uma tarefa de backup

Nesta etapa final, execute uma tarefa de backup e monitore seu progresso. Pelo menos uma tarefa de backup deve ser concluída com sucesso no SCV antes que os recursos possam ser descobertos no BlueXP backup and recovery.

1. No SnapCenter Plug-in for VMware vSphere, navegue até **Grupos de recursos** no menu à esquerda.
2. Para iniciar uma tarefa de backup, selecione o grupo de recursos desejado e clique no botão **Executar agora**.



3. Para monitorar o trabalho de backup, navegue até **Painel** no menu à esquerda. Em **Atividades recentes do trabalho**, clique no número de ID do trabalho para monitorar o andamento do trabalho.



Configurar backups para armazenamento de objetos no BlueXP backup and recovery

Para que o BlueXP gerencie a infraestrutura de dados de forma eficaz, é necessária a instalação prévia de um Conector. O Conector executa as ações envolvidas na descoberta de recursos e no gerenciamento de operações de dados.

Para obter mais informações sobre o conector BlueXP , consulte "Saiba mais sobre conectores" na documentação do BlueXP .

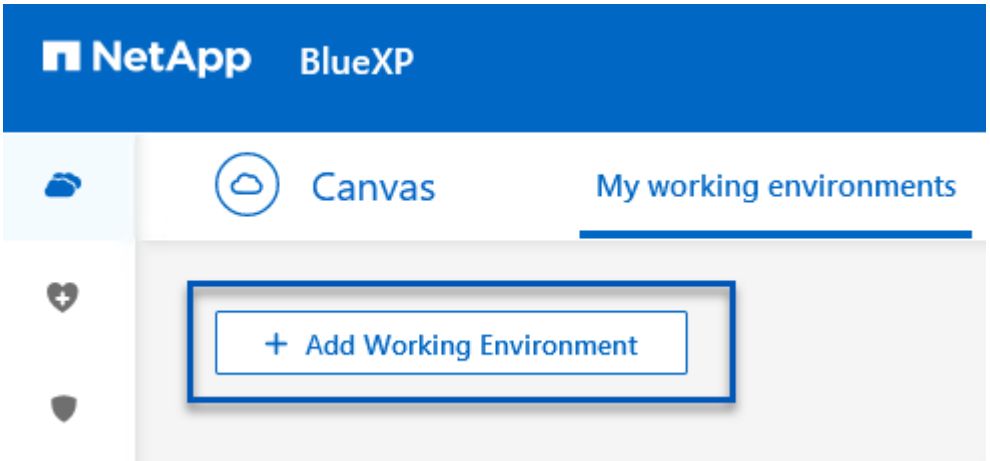
Depois que o conector for instalado para o provedor de nuvem que está sendo utilizado, uma representação gráfica do armazenamento de objetos poderá ser visualizada no Canvas.

Para configurar o BlueXP backup and recovery para fazer backup de dados gerenciados pelo SCV local, conclua as seguintes etapas:

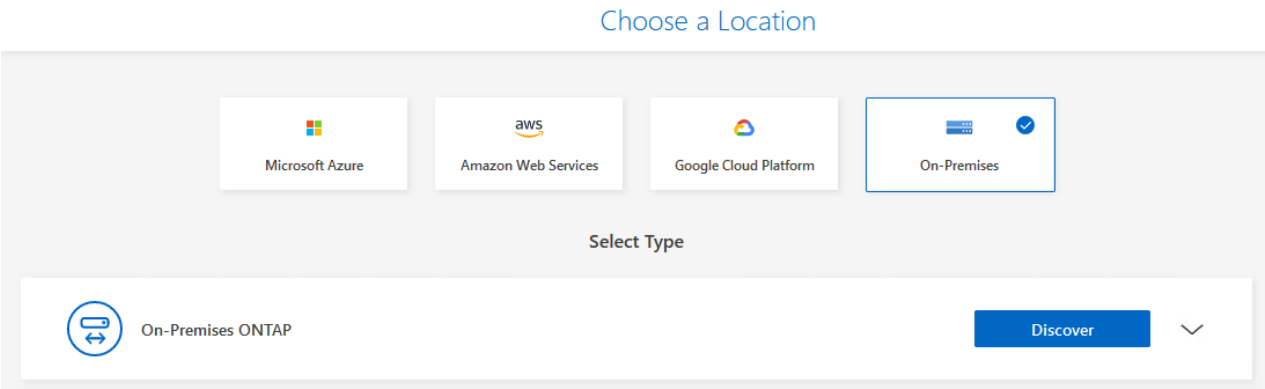
Adicionar ambientes de trabalho ao Canvas

O primeiro passo é adicionar os sistemas de armazenamento ONTAP locais ao BlueXP

1. No Canvas, selecione **Adicionar ambiente de trabalho** para começar.



2. Selecione **No local** entre as opções de locais e clique no botão **Descobrir**.



3. Preencha as credenciais do sistema de armazenamento ONTAP e clique no botão **Descobrir** para adicionar o ambiente de trabalho.

ONTAP Cluster IP

10.61.181.180

User Name

admin

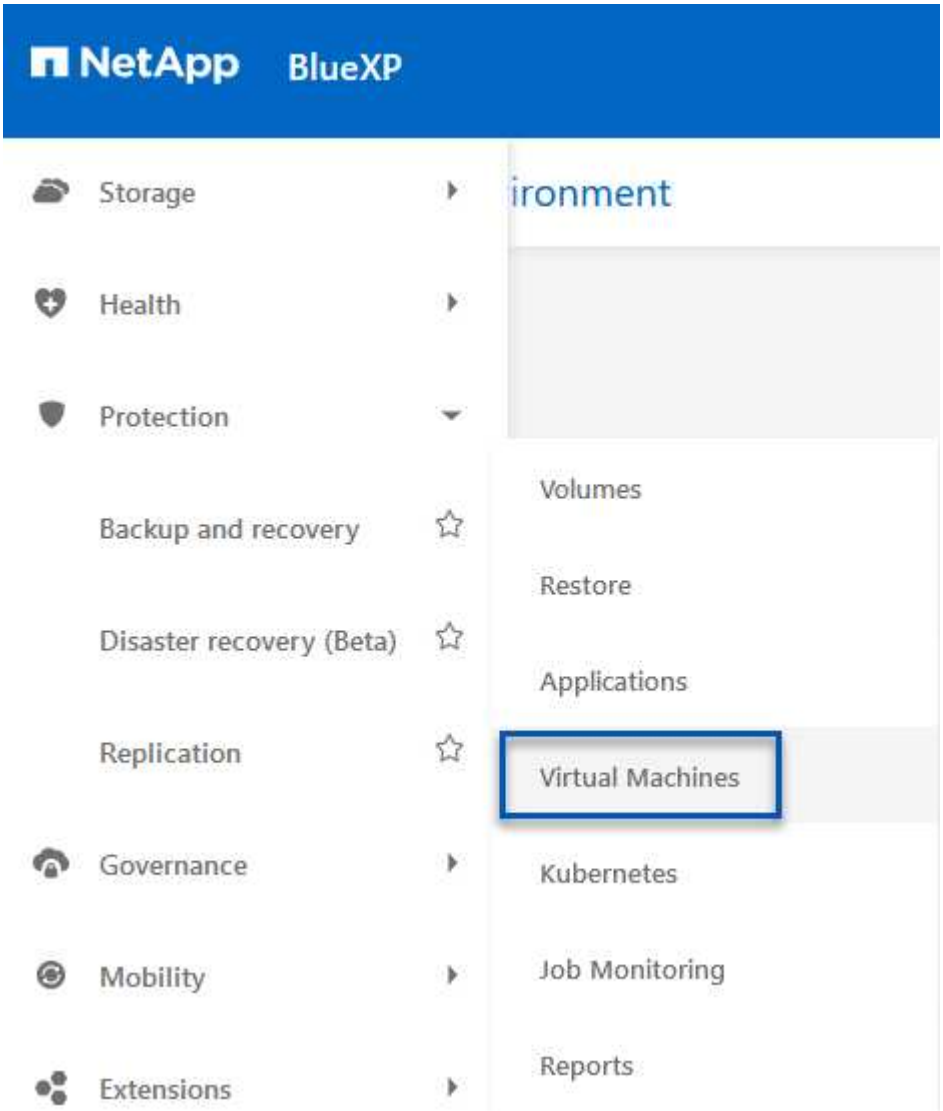
Password

••••••••••

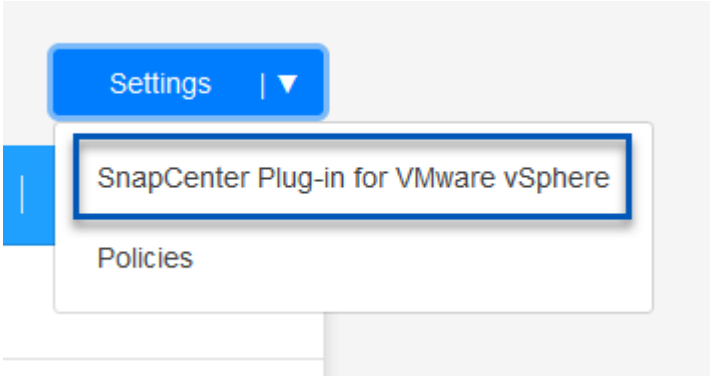
Descubra o dispositivo SCV local e o vCenter

Para descobrir os recursos do armazenamento de dados local e da máquina virtual, adicione informações para o broker de dados SCV e credenciais para o dispositivo de gerenciamento vCenter.

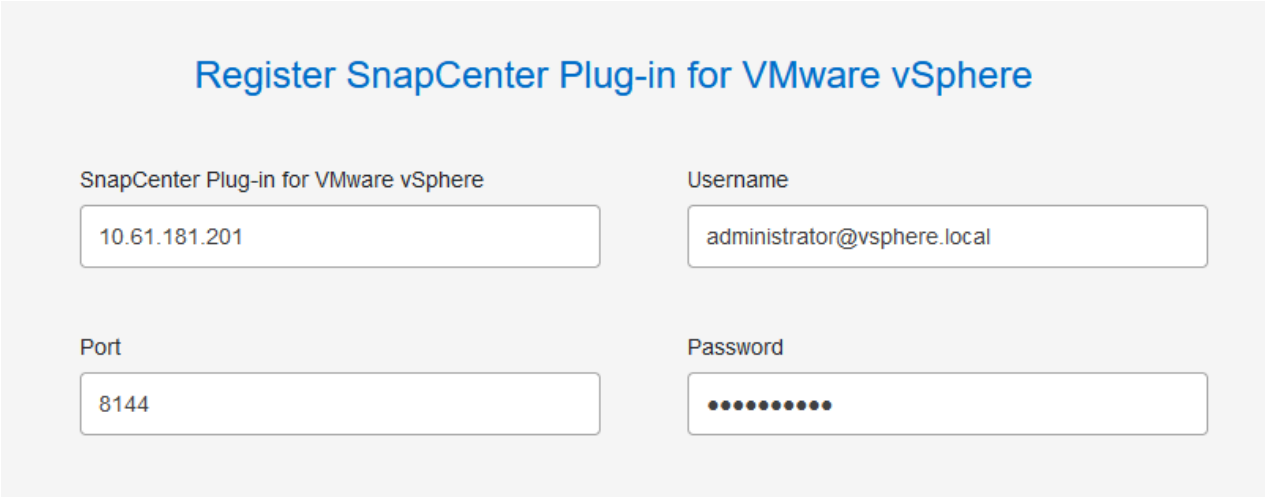
1. No menu esquerdo do BlueXP , selecione **Proteção > Backup e recuperação > Máquinas virtuais**



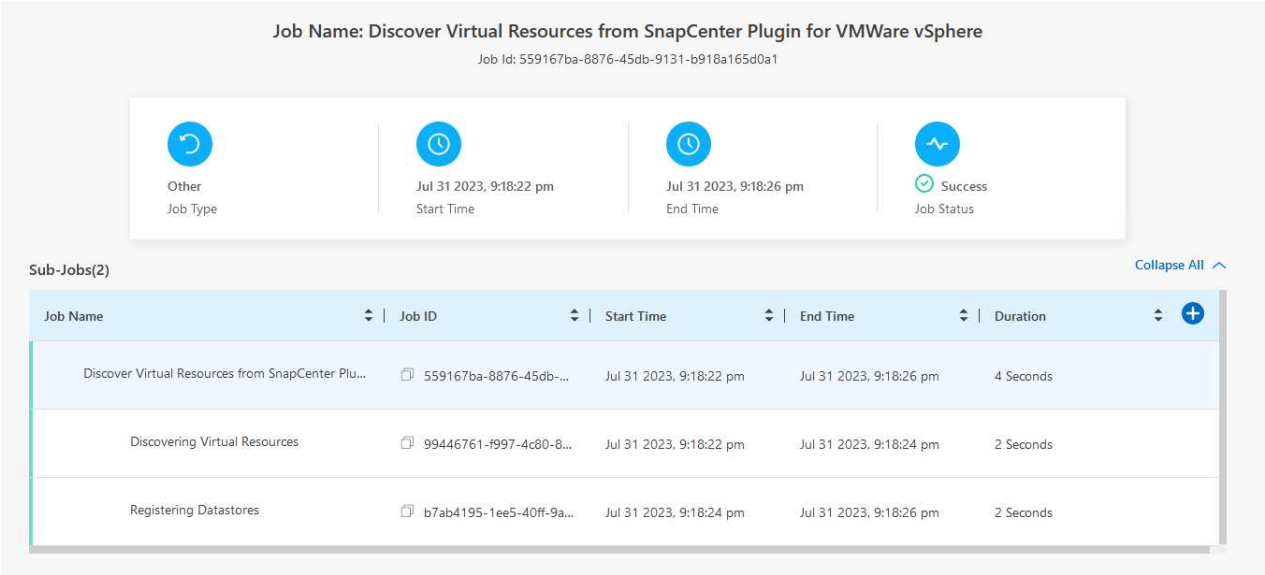
2. Na tela principal Máquinas Virtuais, acesse o menu suspenso **Configurações** e selecione * SnapCenter Plug-in for VMware vSphere*.



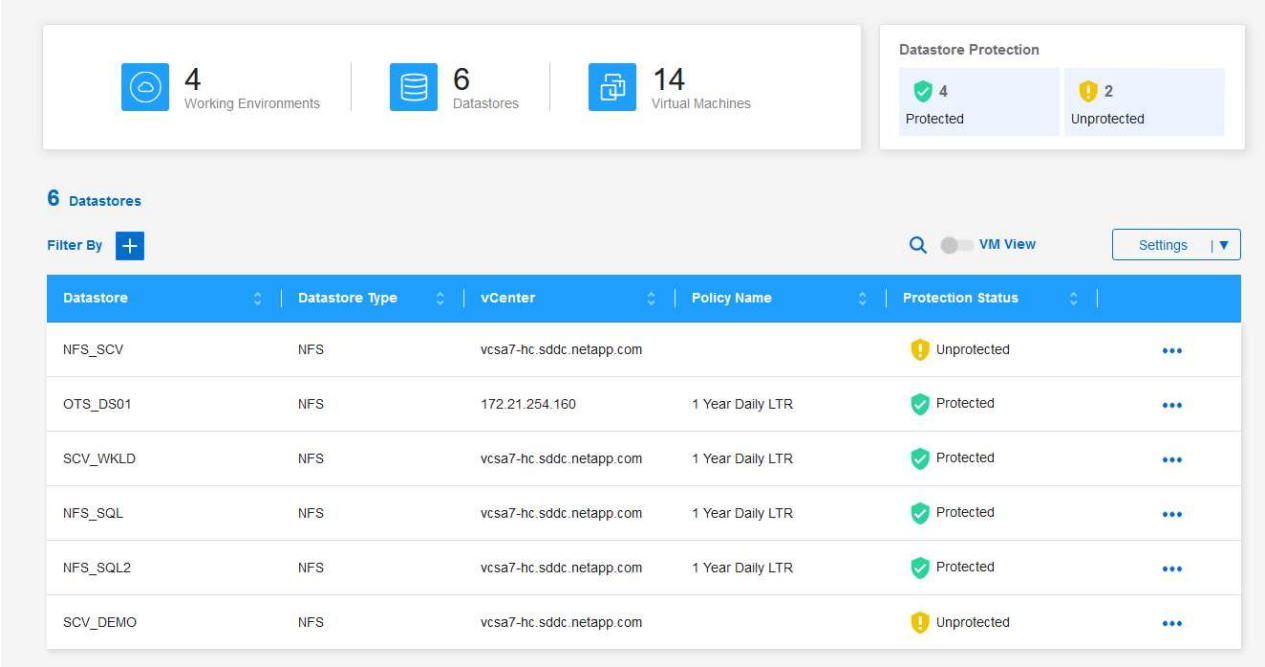
3. Clique no botão **Registrar** e insira o endereço IP e o número da porta do dispositivo SnapCenter Plug-in e o nome de usuário e a senha do dispositivo de gerenciamento vCenter. Clique no botão **Registrar** para iniciar o processo de descoberta.



4. O progresso dos trabalhos pode ser monitorado na aba Monitoramento de Trabalhos.



5. Após a conclusão da descoberta, você poderá visualizar os armazenamentos de dados e as máquinas virtuais em todos os dispositivos SCV descobertos.

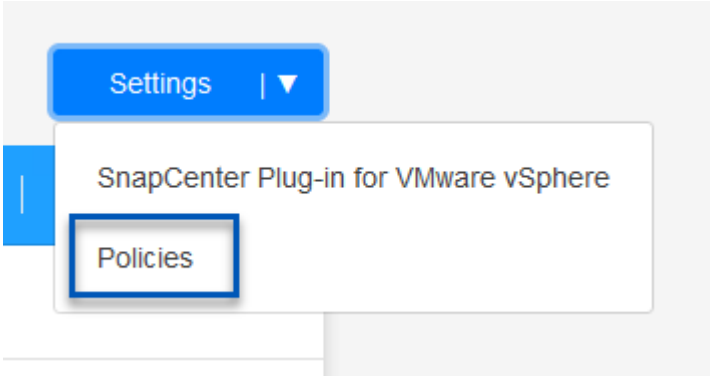

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV
NFS
vcsa7-hc.sddc.netapp.com
Unprotected
OTS_DS01
NFS
172.21.254.160
1 Year Daily LTR
Protected
SCV_WKLD
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL2
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
SCV_DEMO
NFS
vcsa7-hc.sddc.netapp.com
Unprotected

Criar políticas de backup do BlueXP

No BlueXP backup and recovery para máquinas virtuais, crie políticas para especificar o período de retenção, a origem do backup e a política de arquivamento.

Para obter mais informações sobre a criação de políticas, consulte "Crie uma política para fazer backup de armazenamentos de dados" .

1. Na página principal de BlueXP backup and recovery para máquinas virtuais, acesse o menu suspenso **Configurações** e selecione **Políticas**.



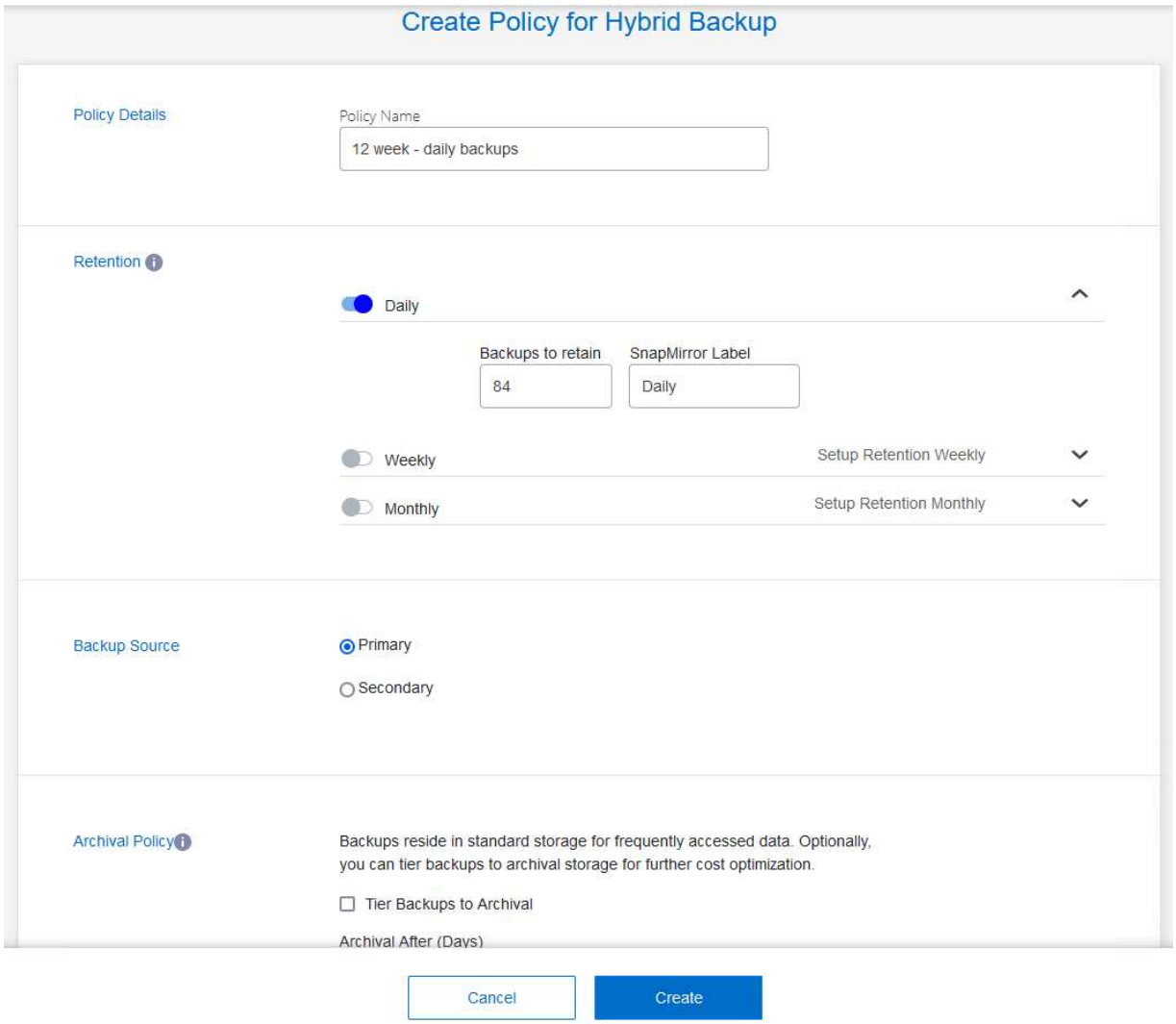
2. Clique em **Criar política** para acessar a janela **Criar política para backup híbrido**.

   a. Adicione um nome para a política

   b. Selecione o período de retenção desejado

   c. Selecione se os backups serão originados do sistema de armazenamento ONTAP primário ou secundário no local

   d. Opcionalmente, especifique após qual período de tempo os backups serão colocados em camadas para armazenamento de arquivamento para economia de custos adicional.



O rótulo SnapMirror inserido aqui é usado para identificar em quais backups a política será aplicada. O nome do rótulo deve corresponder ao nome do rótulo na política SCV local correspondente.

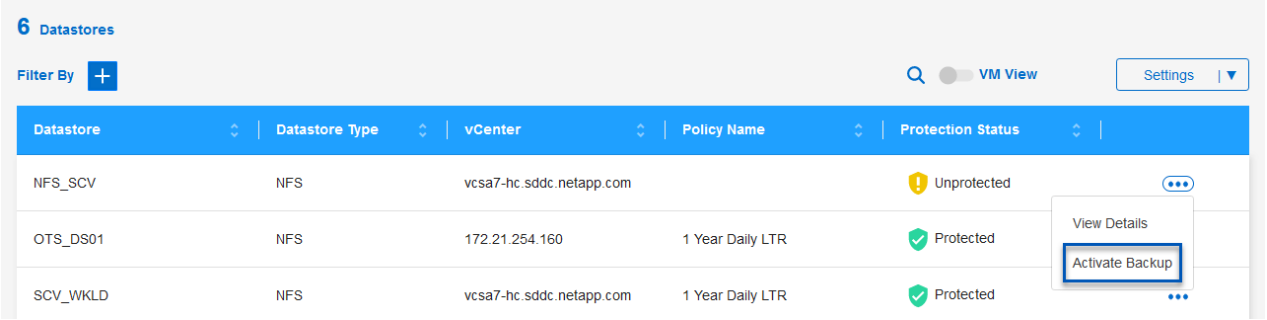
3. Clique em **Criar** para concluir a criação da política.

Fazer backup de datastores para Amazon Web Services

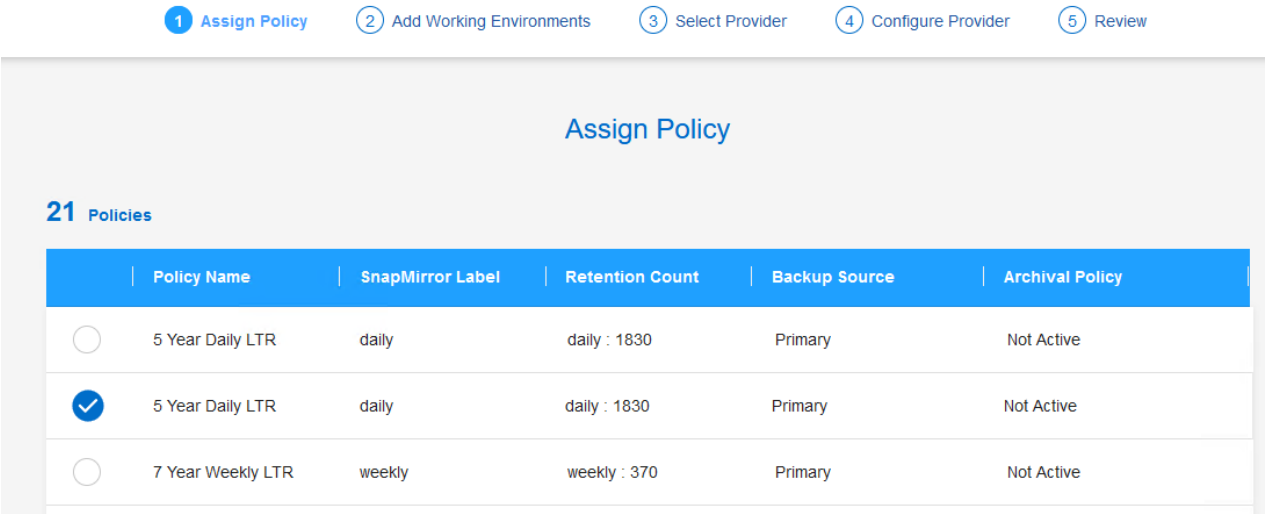
A etapa final é ativar a proteção de dados para os armazenamentos de dados e máquinas virtuais individuais. As etapas a seguir descrevem como ativar backups na AWS.

Para mais informações consulte "Fazer backup de datastores no Amazon Web Services" .

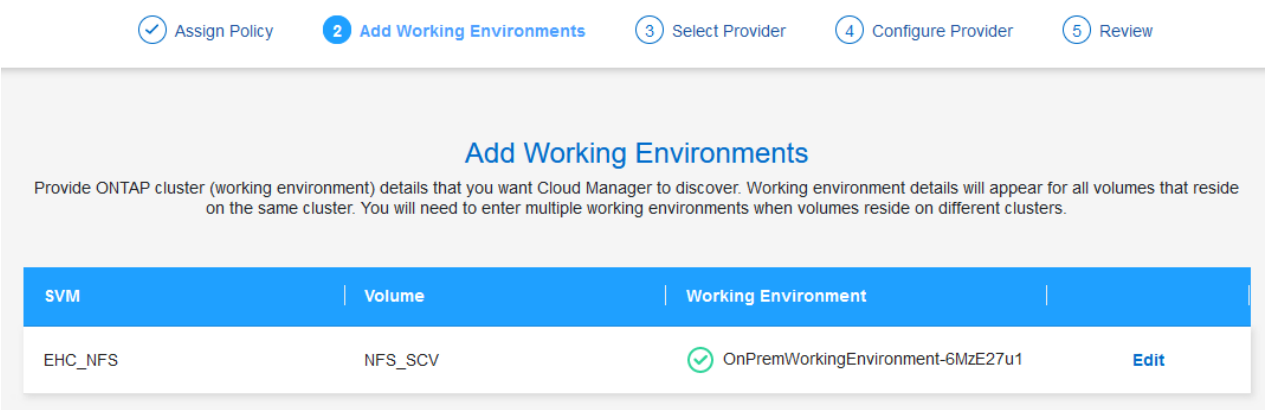
1. Na página principal de BlueXP backup and recovery para máquinas virtuais, acesse o menu suspenso de configurações do armazenamento de dados a ser copiado e selecione **Ativar backup**.



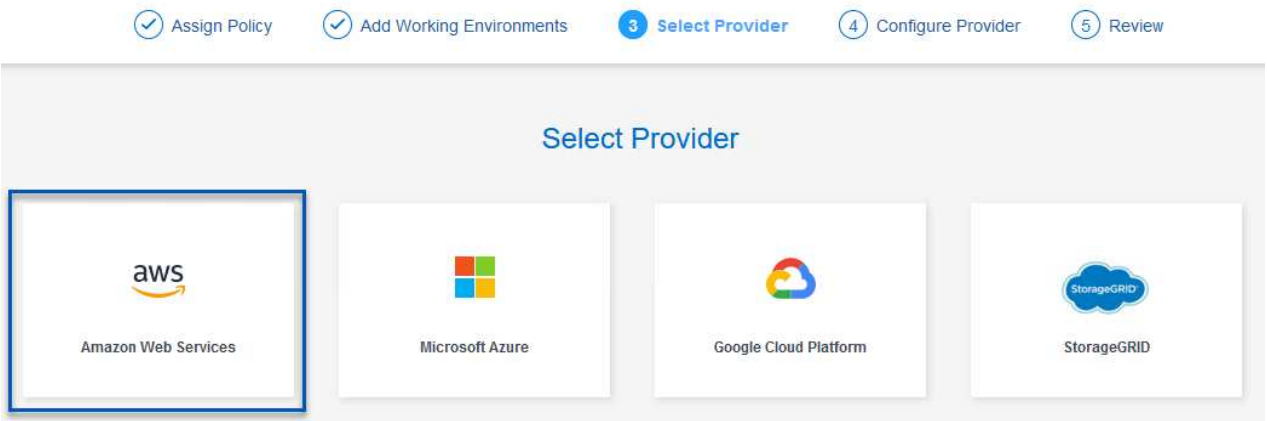
2. Atribua a política a ser usada para a operação de proteção de dados e clique em **Avançar**.



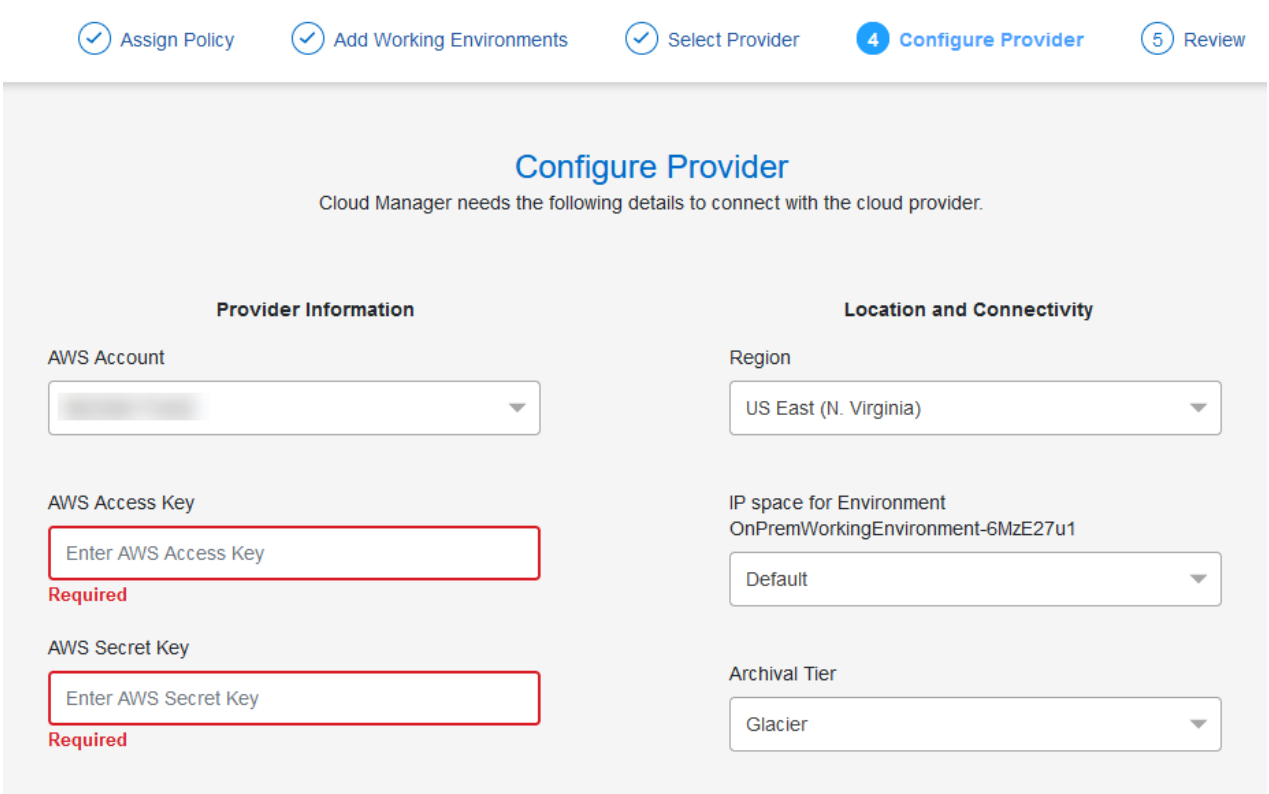
3. Na página **Adicionar ambientes de trabalho**, o armazenamento de dados e o ambiente de trabalho com uma marca de seleção devem aparecer se o ambiente de trabalho já tiver sido descoberto anteriormente. Se o ambiente de trabalho não tiver sido descoberto anteriormente, você pode adicioná-lo aqui. Clique em **Avançar** para continuar.



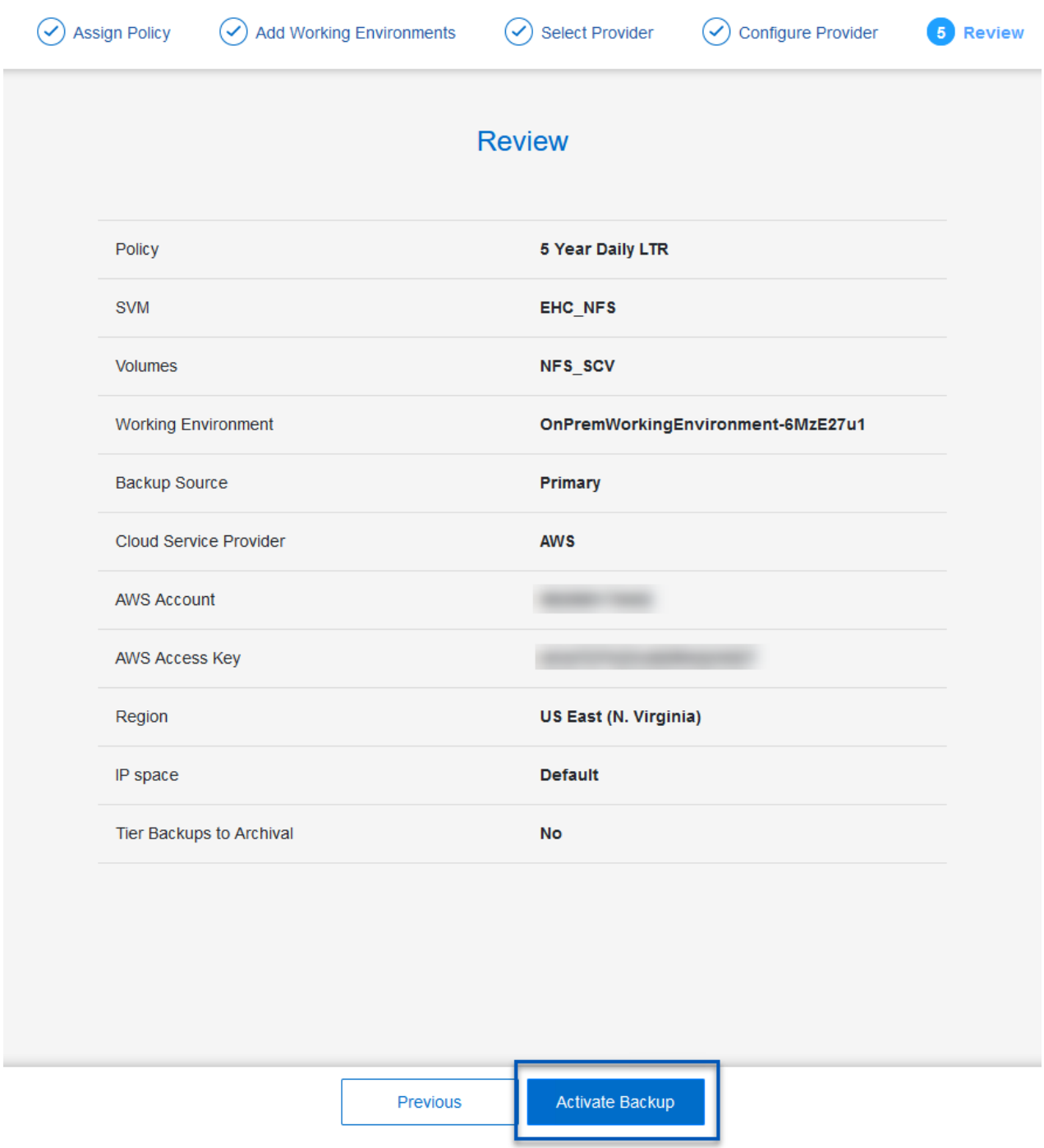
4. Na página **Selecionar provedor**, clique em AWS e depois clique no botão **Avançar** para continuar.



5. Preencha as informações de credenciais específicas do provedor para a AWS, incluindo a chave de acesso e a chave secreta da AWS, a região e a camada de arquivamento a ser usada. Selecione também o espaço IP do ONTAP para o sistema de armazenamento ONTAP local. Clique em **Avançar**.



6. Por fim, revise os detalhes do trabalho de backup e clique no botão **Ativar backup** para iniciar a proteção de dados do armazenamento de dados.



Neste ponto, a transferência de dados pode não começar imediatamente. O BlueXP backup and recovery verificam se há instantâneos pendentes a cada hora e depois os transferem para o armazenamento de objetos.

Restauração de máquinas virtuais em caso de perda de dados

Garantir a proteção dos seus dados é apenas um aspecto da proteção abrangente de dados. Igualmente crucial é a capacidade de restaurar dados prontamente de qualquer local em caso de perda de dados ou ataque de ransomware. Esse recurso é essencial para manter operações comerciais contínuas e atingir objetivos de ponto de recuperação.

A NetApp oferece uma estratégia 3-2-1 altamente adaptável, fornecendo controle personalizado sobre cronogramas de retenção nos locais de armazenamento primário, secundário e de objetos. Essa estratégia oferece flexibilidade para adaptar abordagens de proteção de dados a necessidades específicas.

Esta seção fornece uma visão geral do processo de restauração de dados do SnapCenter Plug-in for VMware vSphere e do BlueXP backup and recovery para máquinas virtuais.

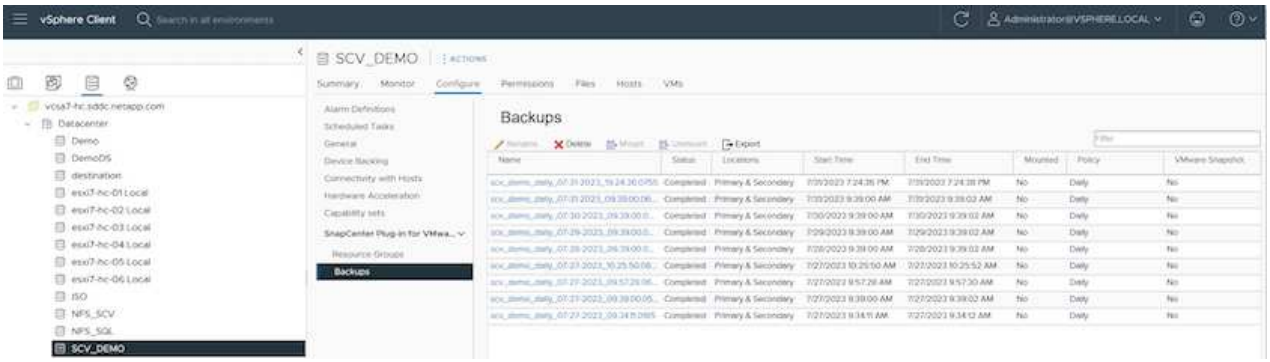
Restaurando máquinas virtuais do SnapCenter Plug-in for VMware vSphere

Para esta solução, as máquinas virtuais foram restauradas em locais originais e alternativos. Nem todos os aspectos dos recursos de restauração de dados do SCV serão abordados nesta solução. Para obter informações detalhadas sobre tudo o que a SCV tem a oferecer, consulte o "Restaurar VMs de backups" na documentação do produto.

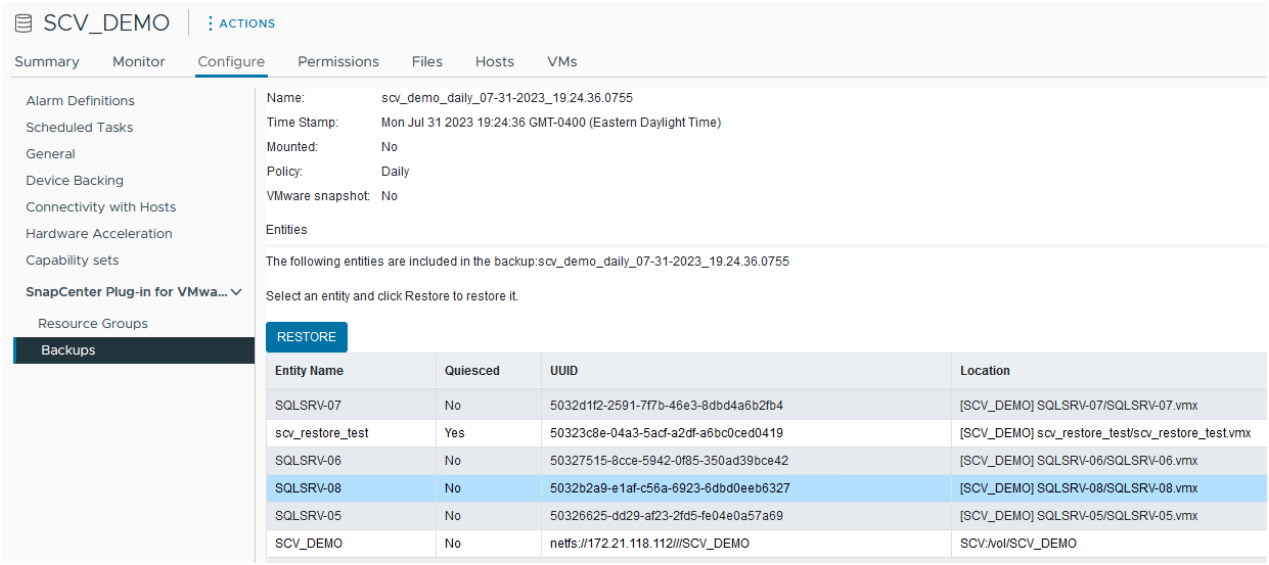
Restaurar máquinas virtuais do SCV

Conclua as etapas a seguir para restaurar uma máquina virtual do armazenamento primário ou secundário.

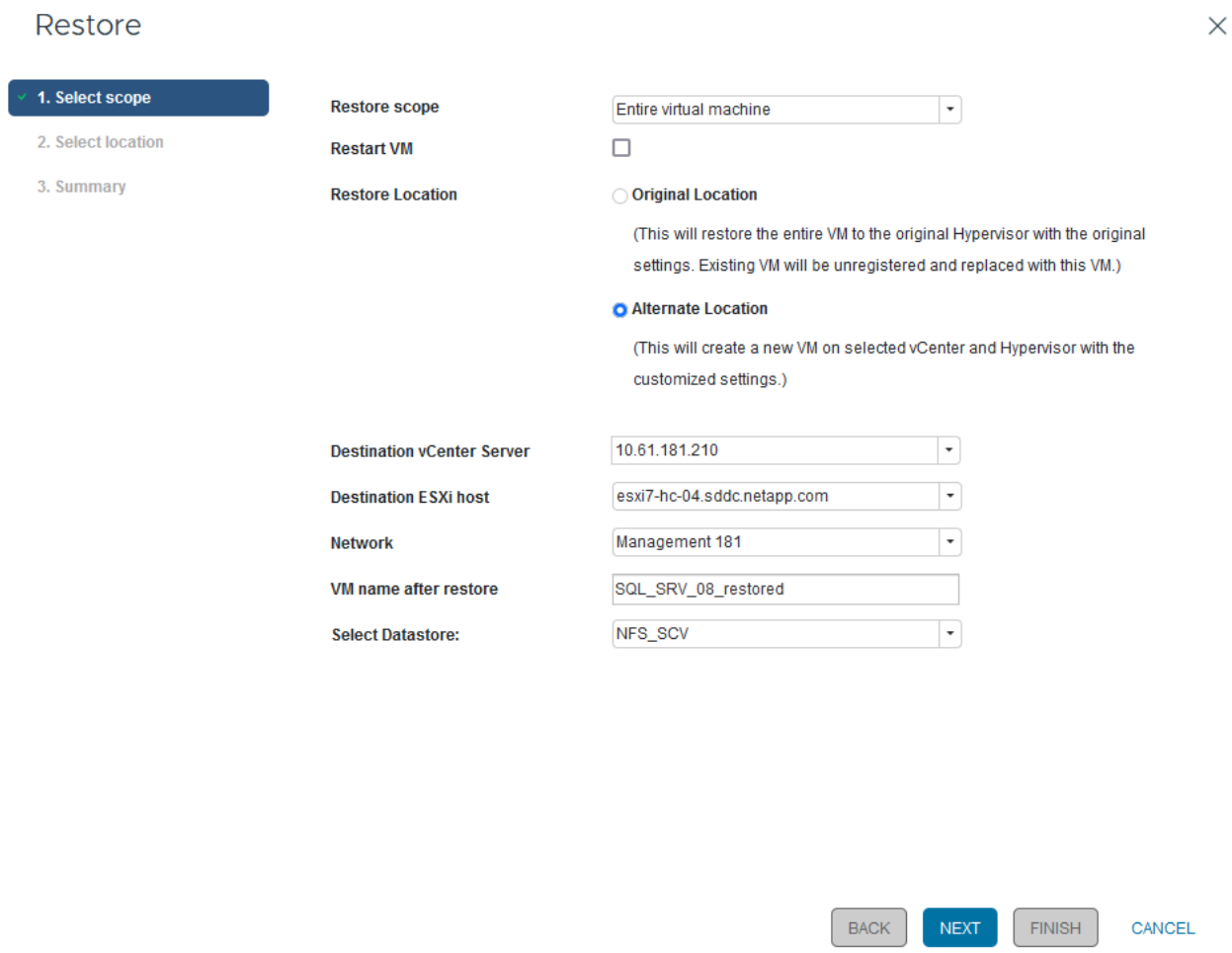
1. No cliente vCenter, navegue até **Inventário > Armazenamento** e clique no armazenamento de dados que contém as máquinas virtuais que você deseja restaurar.
2. Na aba **Configurar** clique em **Backups** para acessar a lista de backups disponíveis.



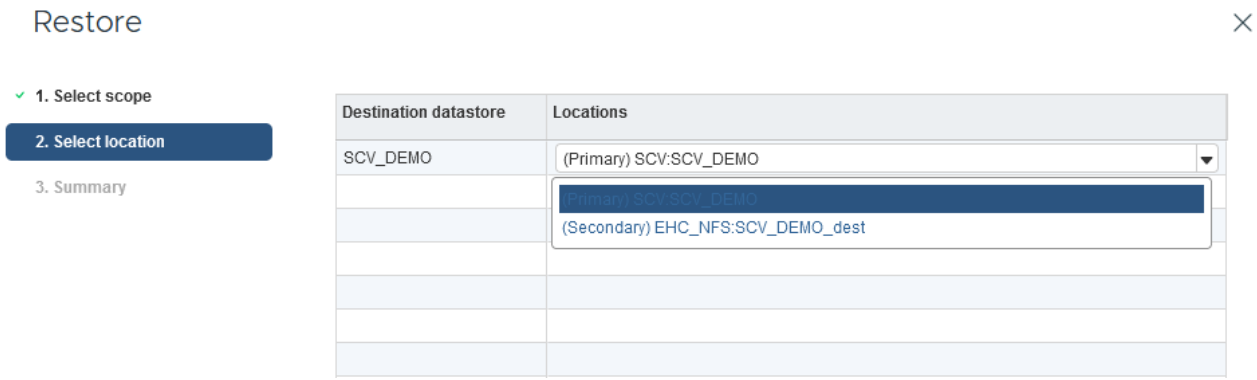
3. Clique em um backup para acessar a lista de VMs e selecione uma VM para restaurar. Clique em **Restaurar**.



4. No assistente de restauração, selecione restaurar a máquina virtual inteira ou um VMDK específico. Selecione para instalar no local original ou em um local alternativo, forneça o nome da VM após a restauração e o armazenamento de dados de destino. Clique em **Avançar**.



5. Escolha fazer backup do local de armazenamento primário ou secundário.



6. Por fim, revise um resumo do trabalho de backup e clique em Concluir para iniciar o processo de restauração.

Restaurando máquinas virtuais do BlueXP backup and recovery para máquinas virtuais

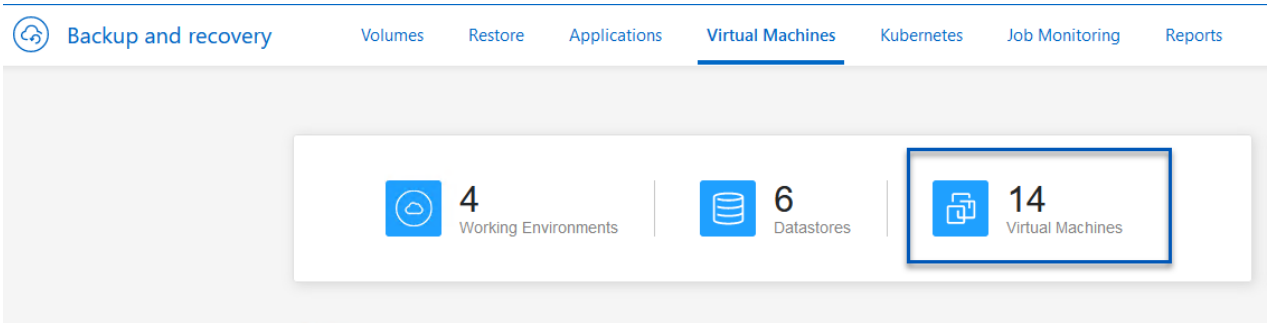
O BlueXP backup and recovery para máquinas virtuais permitem restaurações de máquinas virtuais para seus locais originais. As funções de restauração são acessadas por meio do console web do BlueXP .

Para mais informações consulte "Restaurar dados de máquinas virtuais da nuvem" .

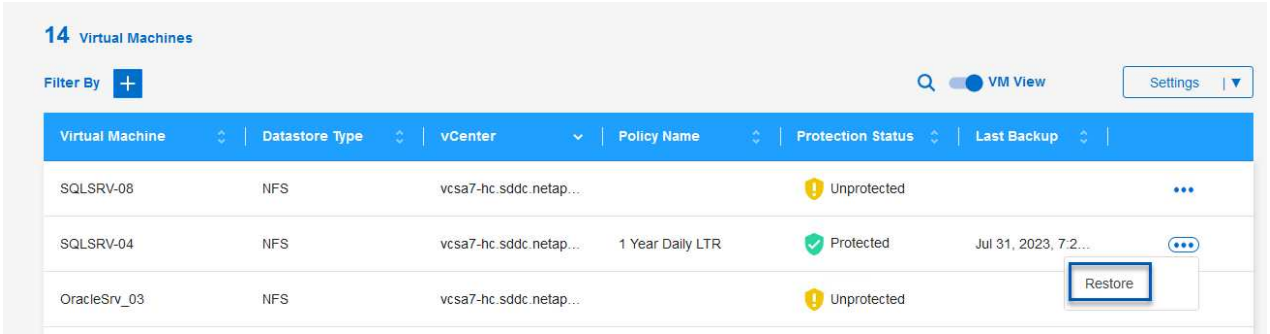
Restaurar máquinas virtuais do BlueXP backup and recovery

Para restaurar uma máquina virtual do BlueXP backup and recovery, conclua as seguintes etapas.

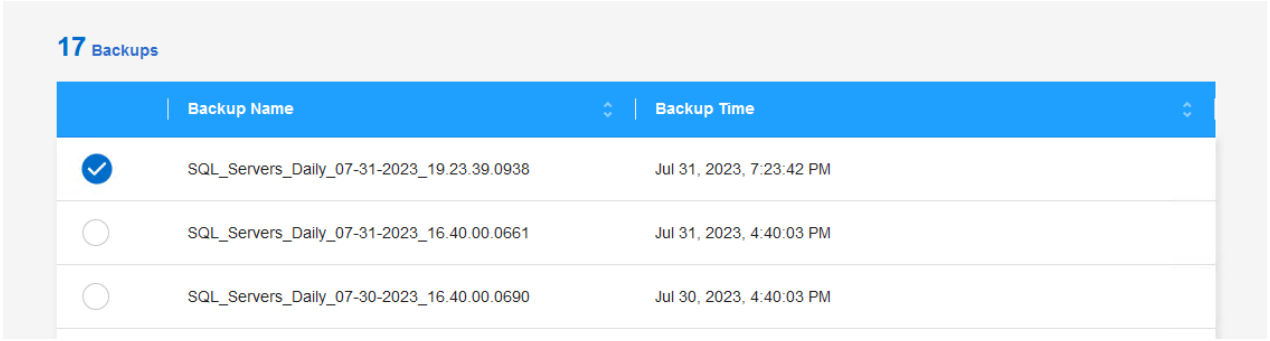
1. Navegue até **Proteção > Backup e recuperação > Máquinas virtuais** e clique em Máquinas virtuais para visualizar a lista de máquinas virtuais disponíveis para restauração.



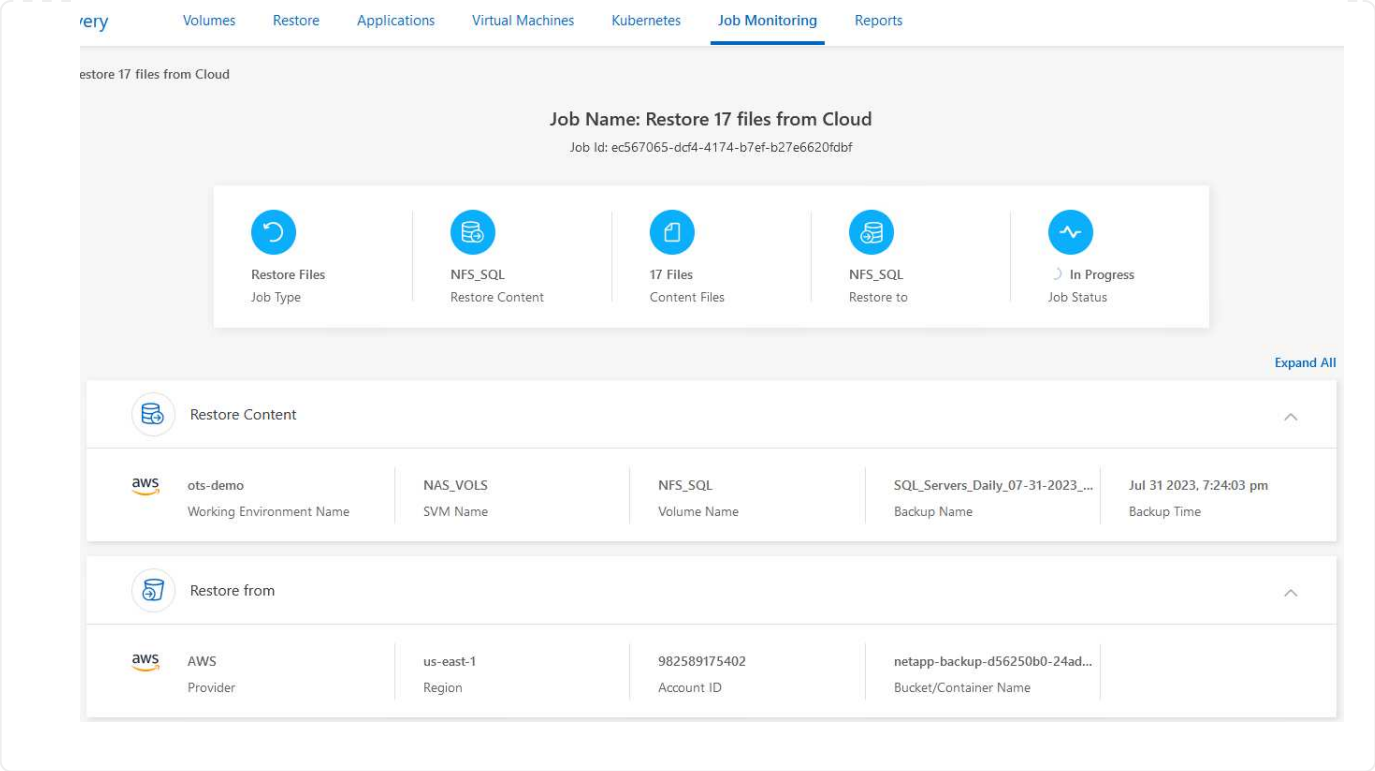
2. Acesse o menu suspenso de configurações da VM a ser restaurada e selecione



3. Selecione o backup a ser restaurado e clique em **Avançar**.



4. Revise um resumo do trabalho de backup e clique em **Restaurar** para iniciar o processo de restauração.
5. Monitore o progresso do trabalho de restauração na aba **Monitoramento de Trabalho**.



Conclusão

A estratégia de backup 3-2-1, quando implementada com o SnapCenter Plug-in for VMware vSphere e o BlueXP backup and recovery para máquinas virtuais, oferece uma solução robusta, confiável e econômica para proteção de dados. Essa estratégia não apenas garante redundância e acessibilidade de dados, mas também oferece a flexibilidade de restaurar dados de qualquer local e de sistemas de armazenamento ONTAP locais e armazenamento de objetos baseado em nuvem.

O caso de uso apresentado nesta documentação se concentra em tecnologias comprovadas de proteção de dados que destacam a integração entre a NetApp, a VMware e os principais provedores de nuvem. O SnapCenter Plug-in for VMware vSphere oferece integração perfeita com o VMware vSphere, permitindo o gerenciamento eficiente e centralizado das operações de proteção de dados. Essa integração simplifica os processos de backup e recuperação de máquinas virtuais, permitindo agendamento fácil, monitoramento e operações de restauração flexíveis dentro do ecossistema VMware. O BlueXP backup and recovery para máquinas virtuais oferece uma solução única (1) em 3-2-1, fornecendo backups seguros e com isolamento de dados de máquinas virtuais para armazenamento de objetos baseado em nuvem. A interface intuitiva e o fluxo de trabalho lógico fornecem uma plataforma segura para arquivamento de longo prazo de dados críticos.

Informações adicionais

Para saber mais sobre as tecnologias apresentadas nesta solução, consulte as seguintes informações adicionais.

- "Documentação do SnapCenter Plug-in for VMware vSphere"
- "Documentação do BlueXP"

Configurar recuperação de desastres para datastores VMFS usando a BlueXP disaster recovery

Neste caso de uso, descrevemos o procedimento para configurar a recuperação de

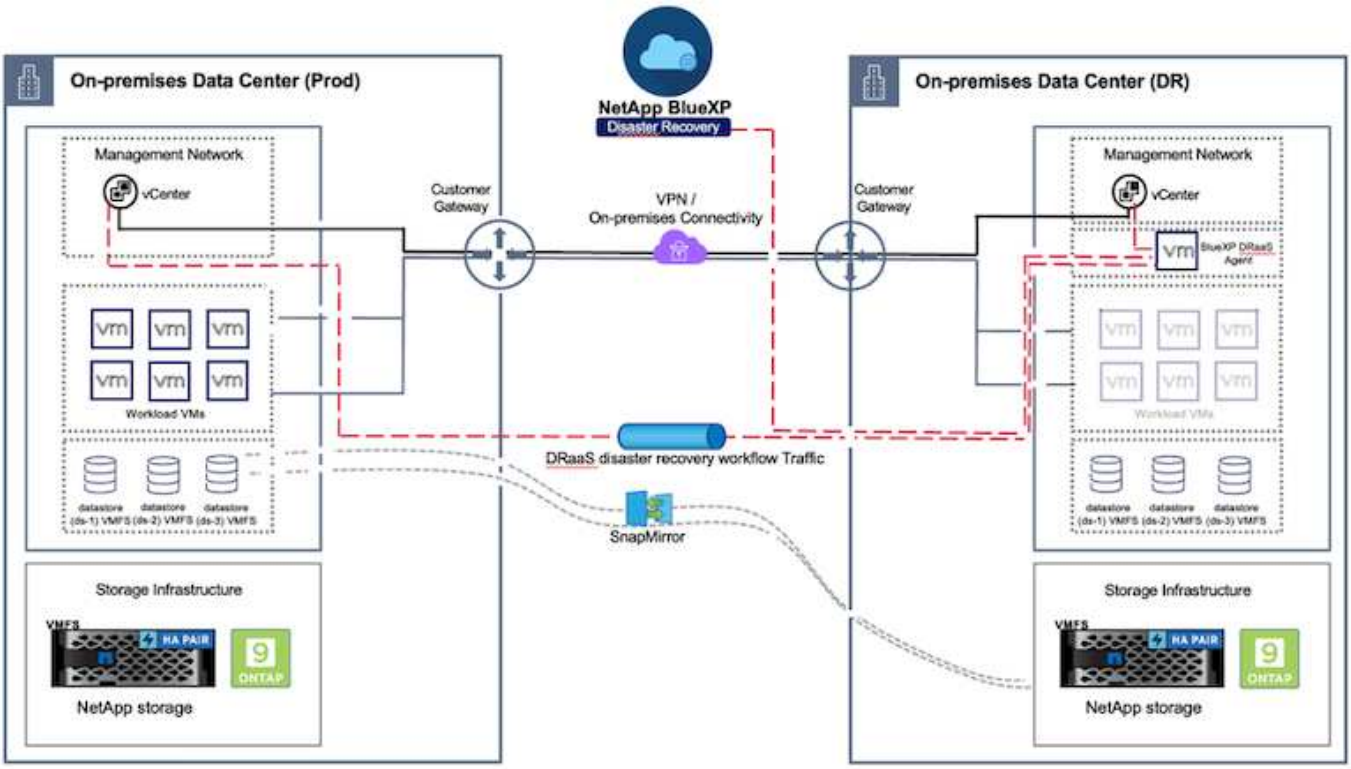
desastres usando a BlueXP disaster recovery para VMs VMware locais usando armazenamentos de dados do VMware Virtual Machine File System (VMFS). Este procedimento inclui a configuração da conta e do conector BlueXP , o estabelecimento da replicação do SnapMirror entre os sistemas ONTAP , a integração com o VMware vCenter e a automatização das operações de failover e failback.

A recuperação de desastres usando replicação em nível de bloco do site de produção para o site de recuperação de desastres é uma maneira resiliente e econômica de proteger as cargas de trabalho contra interrupções do site e eventos de corrupção de dados, como ataques de ransomware. Com a replicação do NetApp SnapMirror , as cargas de trabalho do VMware em execução em sistemas ONTAP locais usando o repositório de dados VMFS podem ser replicadas para outro sistema de armazenamento ONTAP em um datacenter de recuperação designado onde o VMware reside.

Introdução

Esta seção do documento descreve a configuração do BlueXP DRaaS para configurar a recuperação de desastres de VMs VMware locais para outro site designado. Como parte dessa configuração, a conta BlueXP , o conector BlueXP e os arrays ONTAP adicionados ao espaço de trabalho BlueXP são necessários para permitir a comunicação do VMware vCenter com o armazenamento ONTAP . Além disso, este documento detalha como configurar a replicação entre sites e como configurar e testar um plano de recuperação. A última seção contém instruções para executar um failover completo do site e como fazer failback quando o site principal é recuperado e comprado on-line.

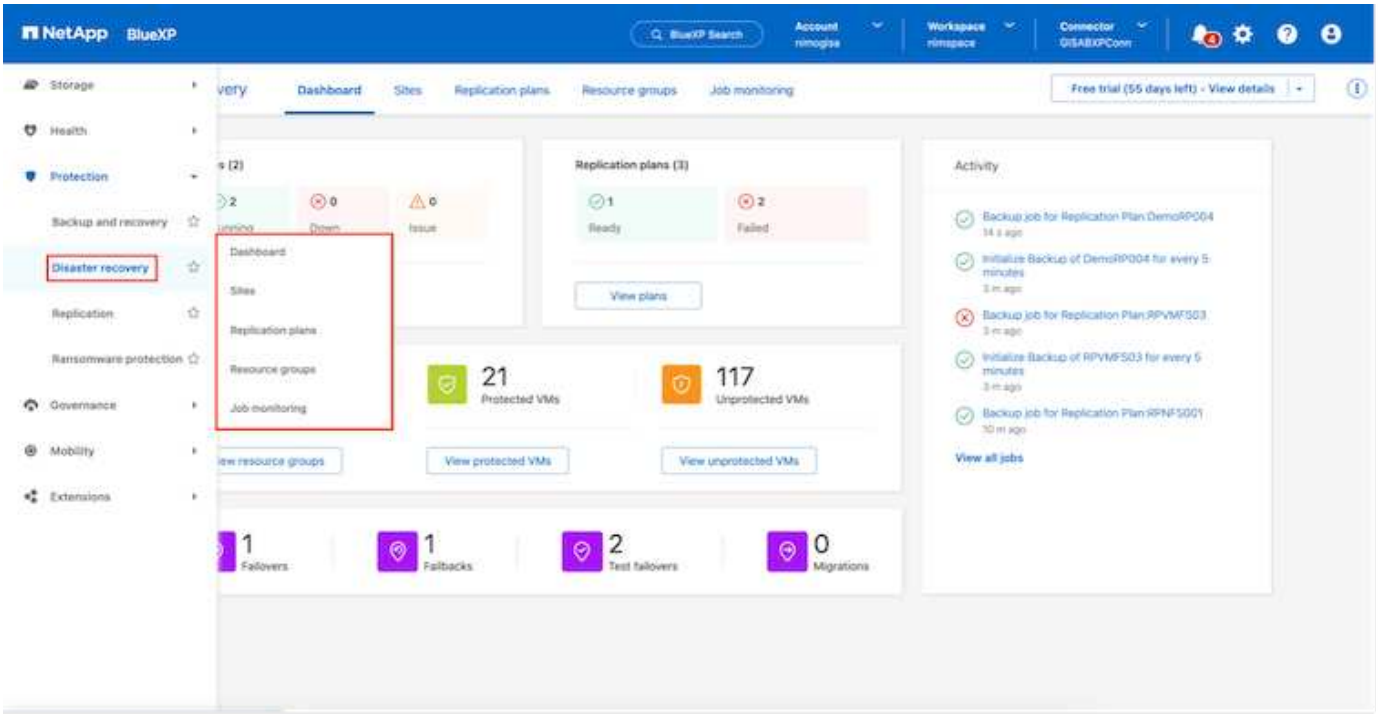
Usando o serviço de BlueXP disaster recovery , que é integrado ao console NetApp BlueXP , os clientes podem descobrir seus VMware vCenters locais junto com o armazenamento ONTAP , criar agrupamentos de recursos, criar um plano de recuperação de desastres, associá-lo a grupos de recursos e testar ou executar failover e failback. O SnapMirror fornece replicação de bloco em nível de armazenamento para manter os dois sites atualizados com alterações incrementais, resultando em um RPO de até 5 minutos. Também é possível simular procedimentos de DR como um exercício regular sem impactar a produção e os armazenamentos de dados replicados ou incorrer em custos adicionais de armazenamento. A BlueXP disaster recovery aproveita a tecnologia FlexClone da ONTAP para criar uma cópia com eficiência de espaço do armazenamento de dados VMFS a partir do último Snapshot replicado no site de DR. Após a conclusão do teste de DR, os clientes podem simplesmente excluir o ambiente de teste, novamente sem qualquer impacto nos recursos de produção replicados reais. Quando houver necessidade (planejada ou não) de failover real, com apenas alguns cliques, o serviço de BlueXP disaster recovery orquestrará todas as etapas necessárias para colocar automaticamente as máquinas virtuais protegidas no site de recuperação de desastres designado. O serviço também reverterá o relacionamento do SnapMirror com o site principal e replicará quaisquer alterações do secundário para o primário para uma operação de failback, quando necessário. Tudo isso pode ser alcançado com uma fração do custo em comparação a outras alternativas bem conhecidas.



Começando

Para começar a BlueXP disaster recovery, use o console do BlueXP e acesse o serviço.

1. Faça login no BlueXP.
2. Na navegação à esquerda do BlueXP , selecione Proteção > Recuperação de desastres.
3. O painel de BlueXP disaster recovery é exibido.

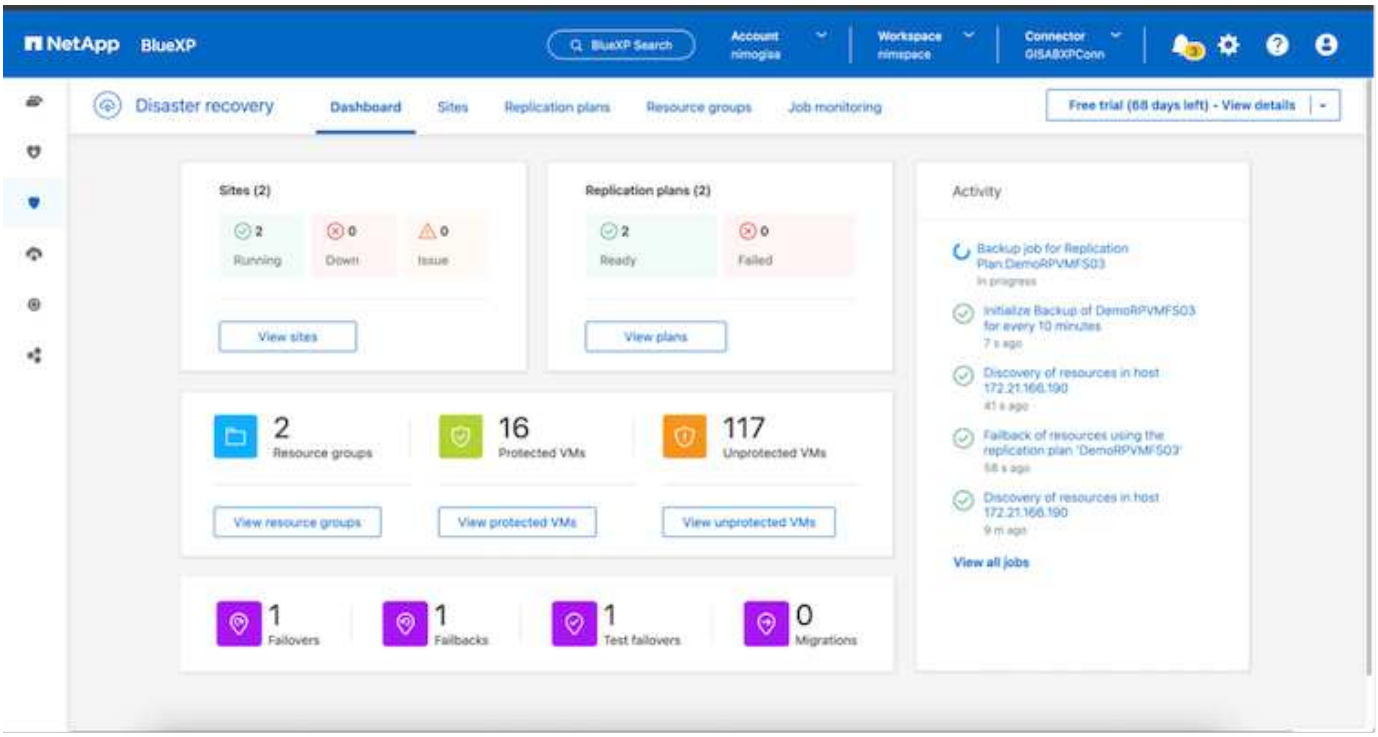


Antes de configurar o plano de recuperação de desastres, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O BlueXP Connector é configurado no NetApp BlueXP. O conector deve ser implantado no AWS VPC.
- A instância do conector BlueXP tem conectividade com os sistemas de armazenamento e vCenter de origem e destino.
- Os sistemas de armazenamento NetApp locais que hospedam datastores VMFS para VMware são adicionados no BlueXP.
- A resolução de DNS deve estar em vigor ao usar nomes DNS. Caso contrário, use endereços IP para o vCenter.
- A replicação do SnapMirror é configurada para os volumes de armazenamento de dados baseados em VMFS designados.

Depois que a conectividade for estabelecida entre os sites de origem e destino, prossiga com as etapas de configuração, que devem levar de 3 a 5 minutos.

> A NetApp recomenda implantar o conector BlueXP no site de recuperação de desastres ou em um terceiro site, para que o conector BlueXP possa se comunicar pela rede com recursos de origem e destino durante interrupções reais ou desastres naturais.

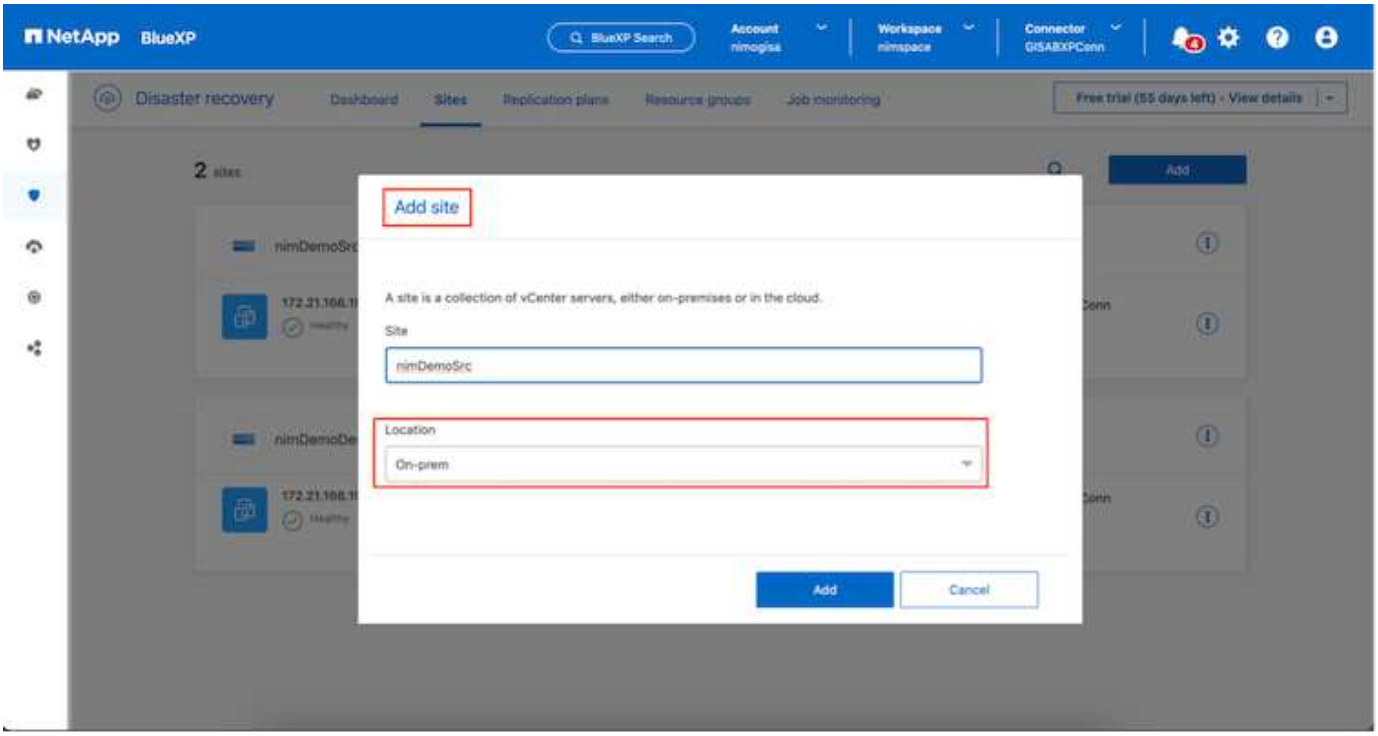


> O suporte para datastores VMFS locais para locais está em fase de pré-visualização de tecnologia no momento da redação deste documento. O recurso é suportado por armazenamentos de dados VMFS baseados nos protocolos FC e ISCSI.

Configuração de BlueXP disaster recovery

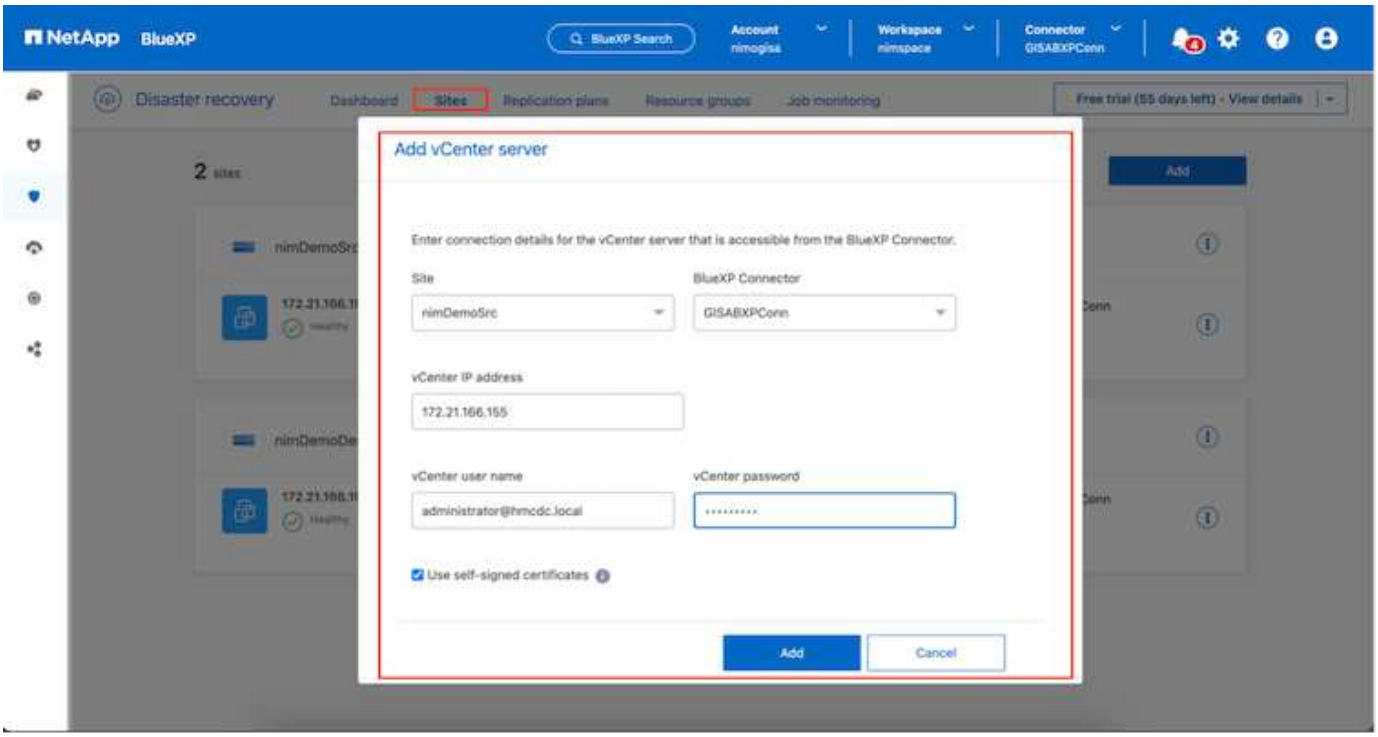
O primeiro passo na preparação para a recuperação de desastres é descobrir e adicionar os recursos de armazenamento e vCenter locais à BlueXP disaster recovery.

Garanta que os sistemas de armazenamento ONTAP sejam adicionados ao ambiente de trabalho dentro do canvas. Abra o console BlueXP e selecione **Proteção > Recuperação de desastres** na navegação à esquerda. Selecione **Descobrir servidores vCenter** ou use o menu superior, selecione **Sites > Adicionar > Adicionar vCenter**.

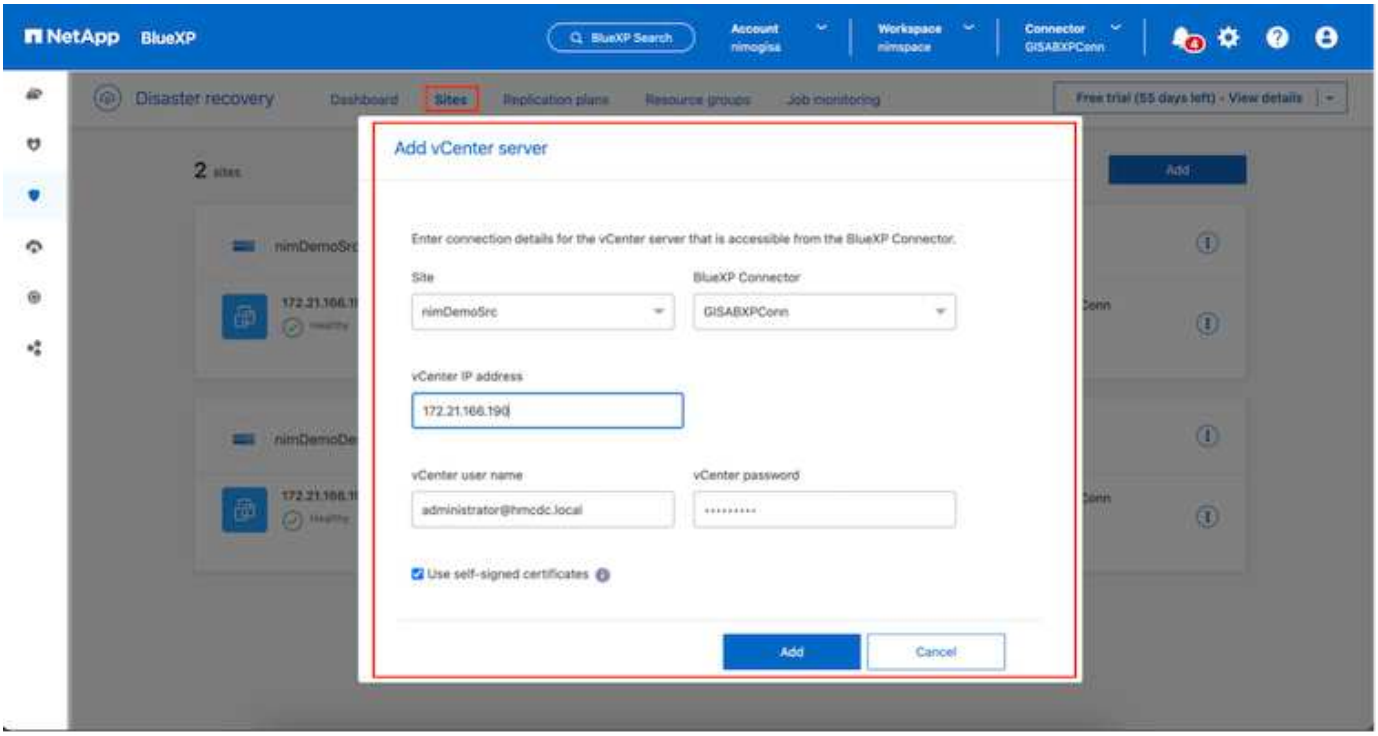


Adicione as seguintes plataformas:

- **Fonte**. vCenter local.



- **Destino**. VMC SDDC vCenter.



Depois que os vCenters são adicionados, a descoberta automatizada é acionada.

Configurando a replicação de armazenamento entre o site de origem e o de destino

O SnapMirror usa snapshots ONTAP para gerenciar a transferência de dados de um local para outro. Inicialmente, uma cópia completa baseada em um instantâneo do volume de origem é copiada para o destino para executar uma sincronização de linha de base. À medida que ocorrem alterações de dados na origem, um novo instantâneo é criado e comparado ao instantâneo de base. Os blocos que foram alterados são então replicados para o destino, com o instantâneo mais recente se tornando a linha de base atual ou o instantâneo comum mais recente. Isso permite que o processo seja repetido e atualizações incrementais sejam enviadas ao destino.

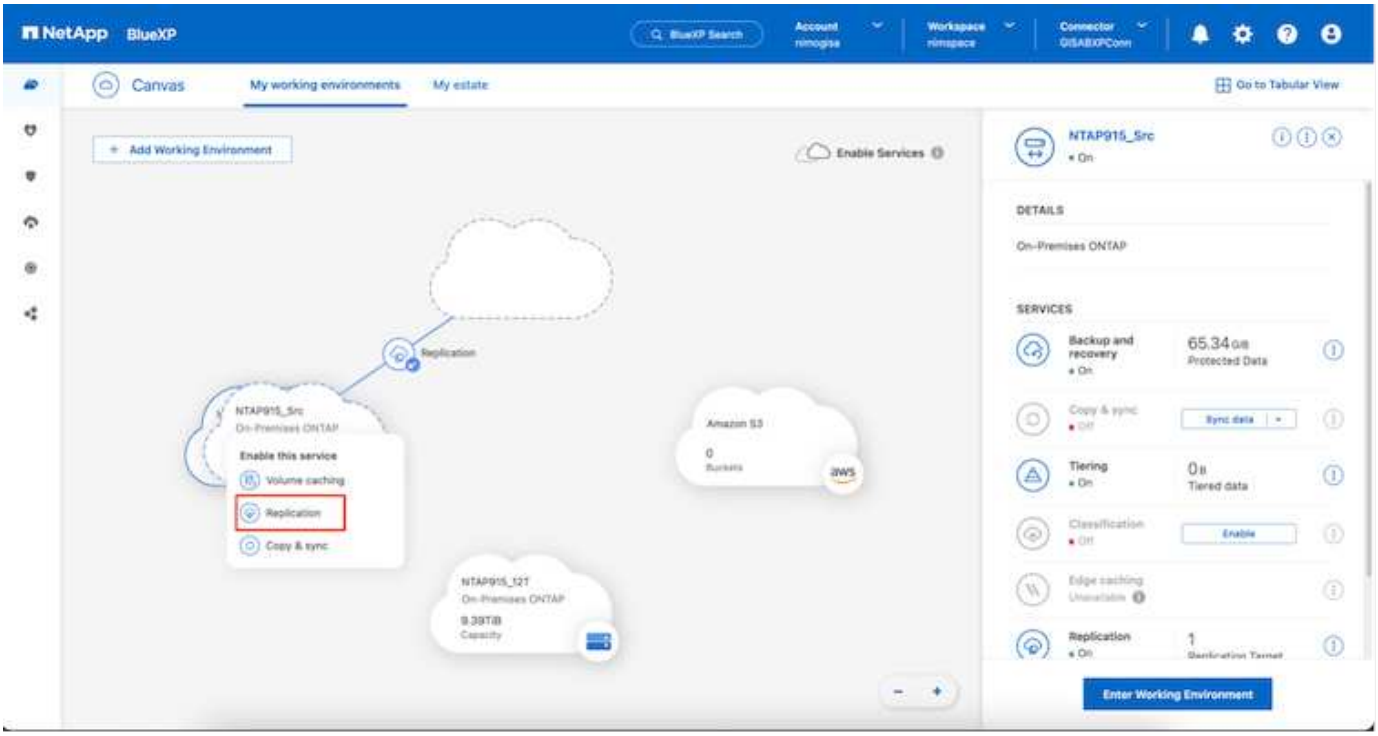
Quando um relacionamento SnapMirror é estabelecido, o volume de destino fica em um estado somente leitura online e, portanto, ainda está acessível. O SnapMirror funciona com blocos físicos de armazenamento, em vez de em um arquivo ou outro nível lógico. Isso significa que o volume de destino é uma réplica idêntica da origem, incluindo instantâneos, configurações de volume, etc. Se os recursos de eficiência de espaço do ONTAP , como compactação de dados e desduplicação de dados, estiverem sendo usados pelo volume de origem, o volume replicado manterá essas otimizações.

Interromper o relacionamento do SnapMirror torna o volume de destino gravável e normalmente seria usado para executar um failover quando o SnapMirror estiver sendo usado para sincronizar dados com um ambiente de DR. O SnapMirror é sofisticado o suficiente para permitir que os dados alterados no site de failover sejam ressincronizados de forma eficiente de volta ao sistema primário, caso ele volte a ficar on-line posteriormente, e então permitir que o relacionamento original do SnapMirror seja restabelecido.

Como configurá-lo para recuperação de desastres do VMware

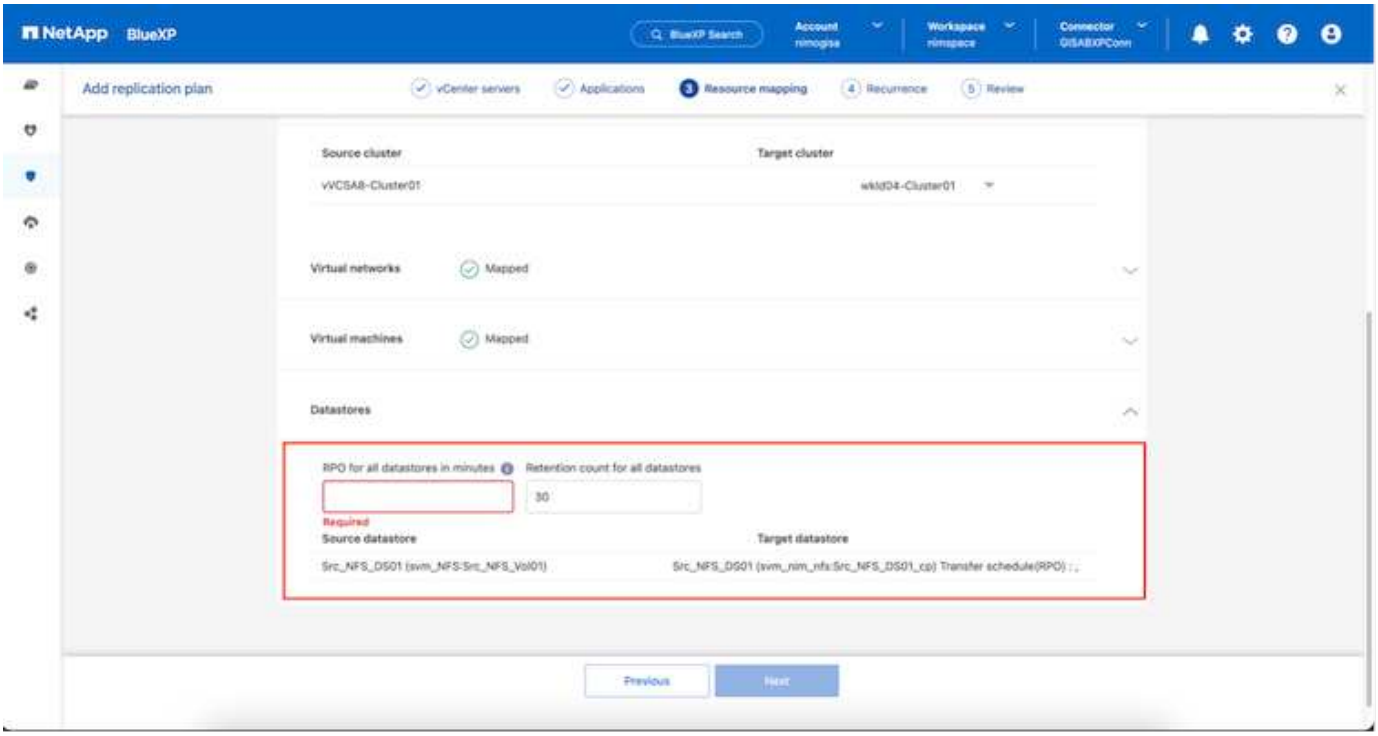
O processo para criar a replicação do SnapMirror permanece o mesmo para qualquer aplicativo. O processo pode ser manual ou automatizado. A maneira mais fácil é aproveitar o BlueXP para configurar a replicação do SnapMirror usando o simples recurso de arrastar e soltar do sistema ONTAP de origem no ambiente para o

destino para acionar o assistente que orienta o restante do processo.



O BlueXP DRaaS também pode automatizar o mesmo, desde que os dois critérios a seguir sejam atendidos:

- Os clusters de origem e destino têm um relacionamento de pares.
- O SVM de origem e o SVM de destino têm um relacionamento de mesmo nível.

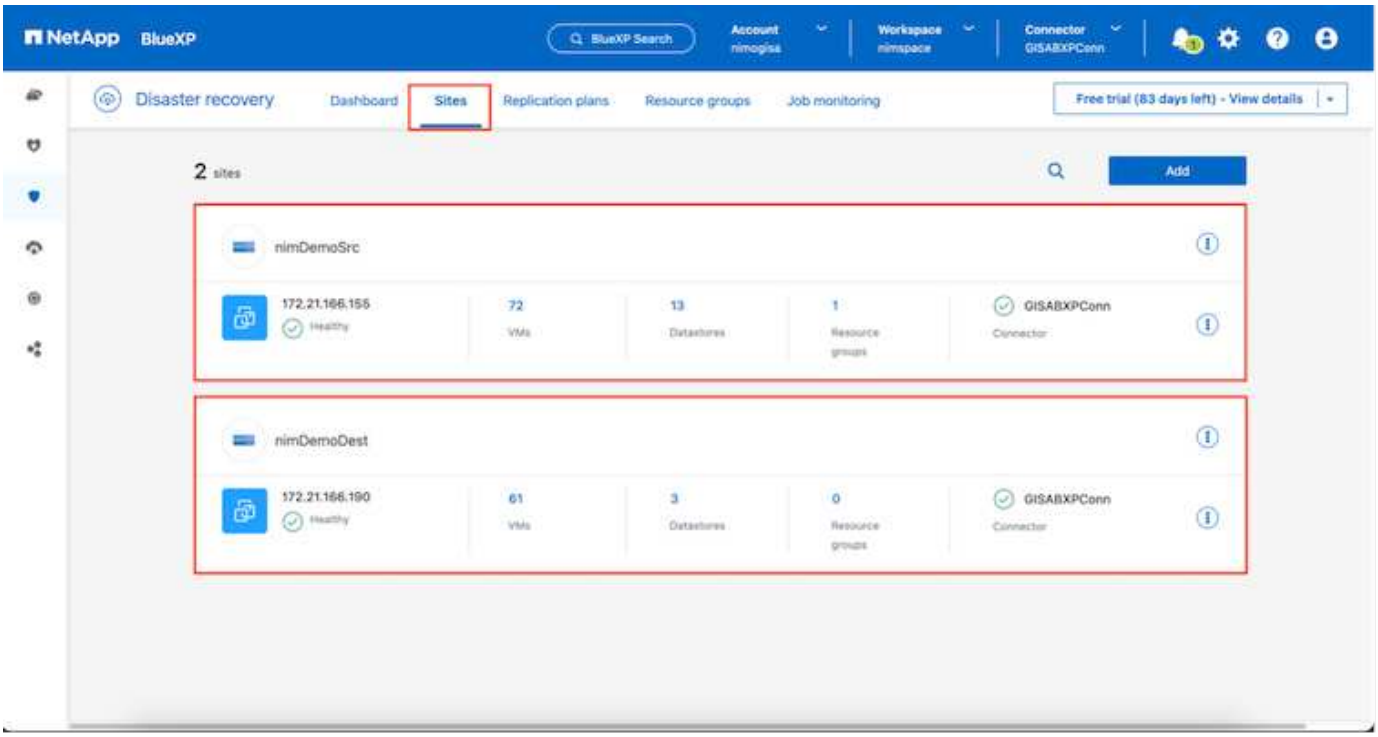


Se o relacionamento do SnapMirror já estiver configurado para o volume via CLI, o BlueXP DRaaS assume o relacionamento e continua com o restante das operações de fluxo de trabalho.

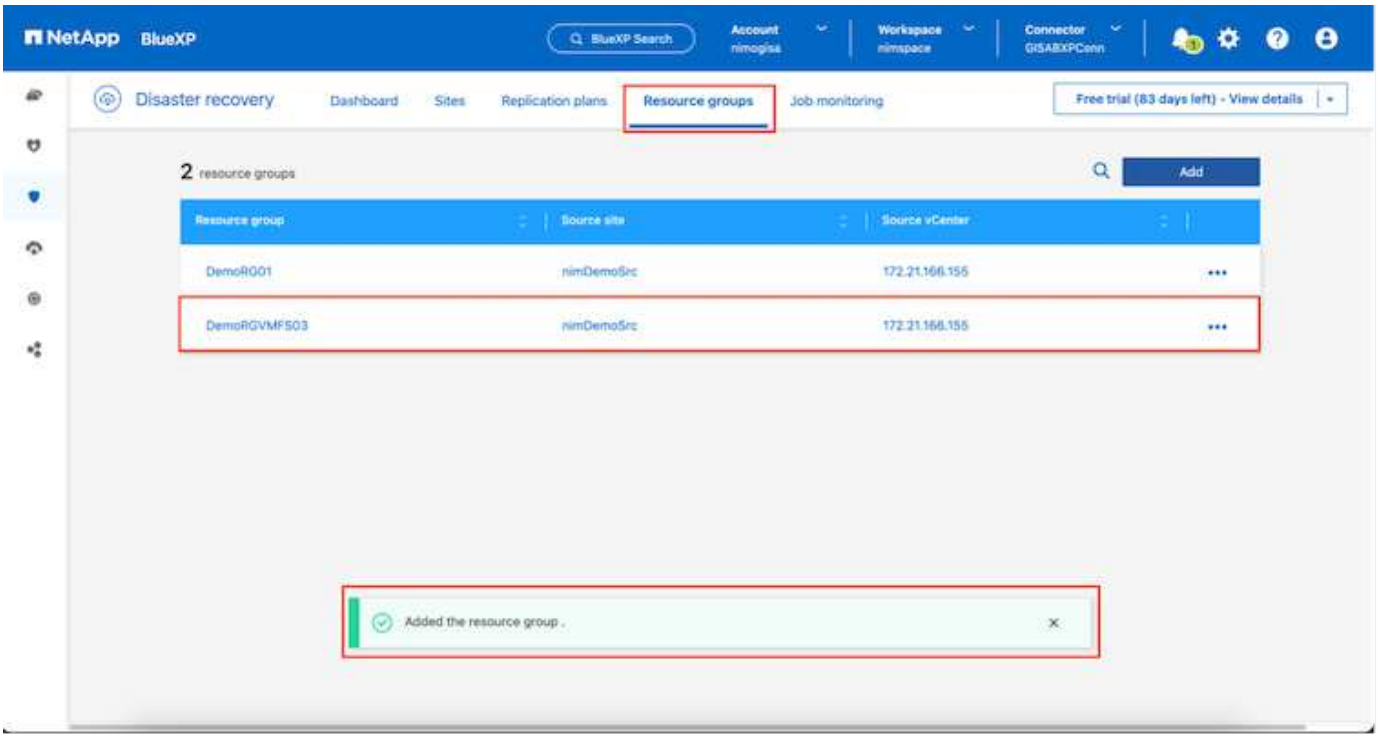
Além das abordagens acima, a replicação do SnapMirror também pode ser criada via ONTAP CLI ou System Manager. Independentemente da abordagem usada para sincronizar os dados usando o SnapMirror, o BlueXP DRaaS orquestra o fluxo de trabalho para operações de recuperação de desastres eficientes e contínuas.

O que a BlueXP disaster recovery pode fazer por você?

Depois que os sites de origem e destino são adicionados, a BlueXP disaster recovery executa a descoberta profunda automática e exibe as VMs junto com os metadados associados. A BlueXP disaster recovery também detecta automaticamente as redes e os grupos de portas usados pelas VMs e os preenche.

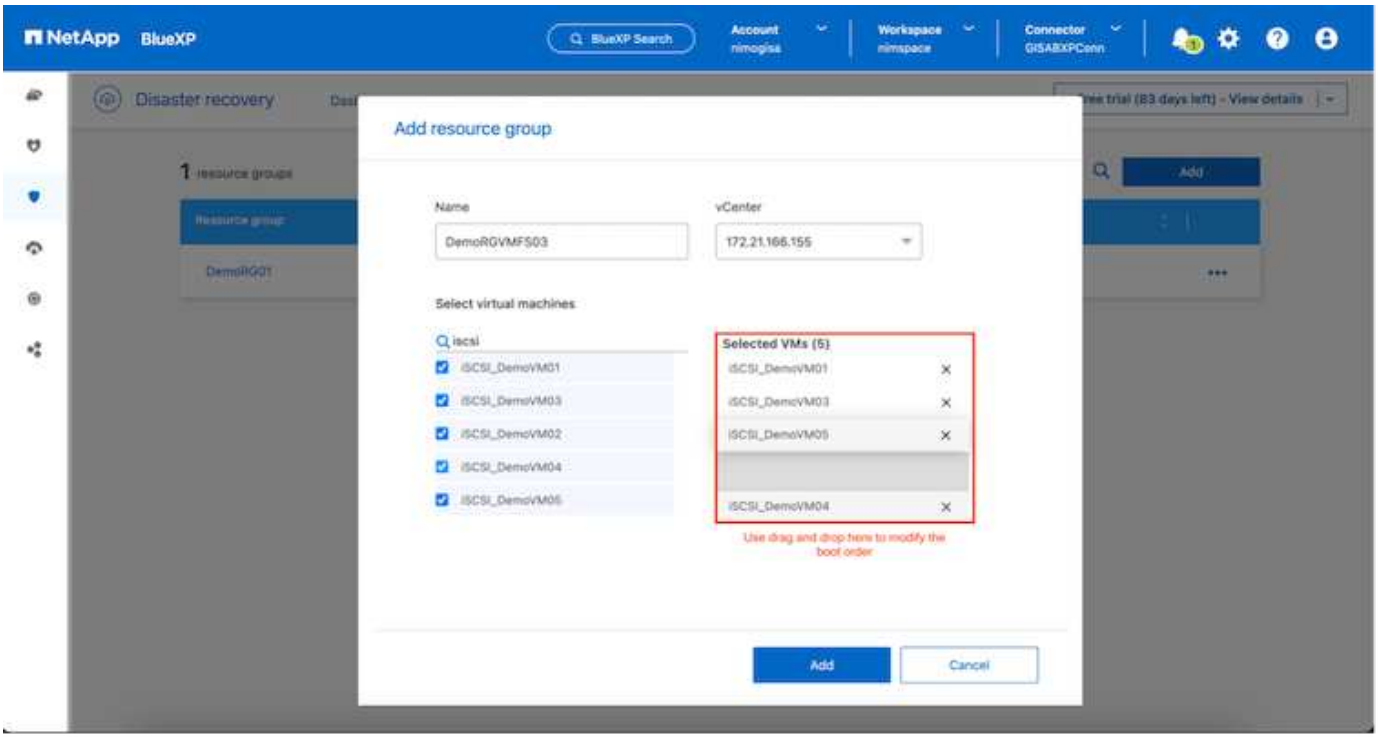


Depois que os sites forem adicionados, as VMs podem ser agrupadas em grupos de recursos. Os grupos de recursos de BlueXP disaster recovery permitem que você agrupe um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização e atrasos de inicialização que podem ser executados na recuperação. Para começar a criar grupos de recursos, navegue até **Grupos de recursos** e clique em **Criar novo grupo de recursos**.

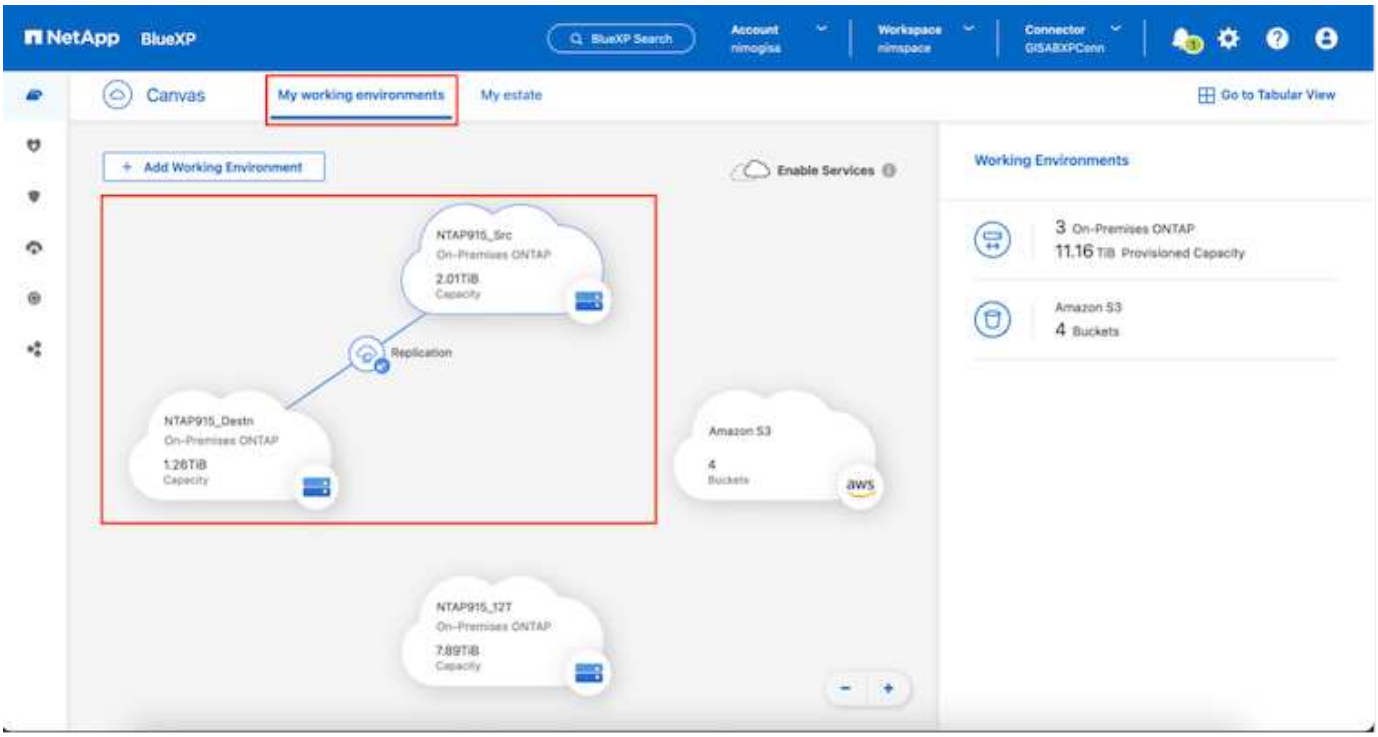


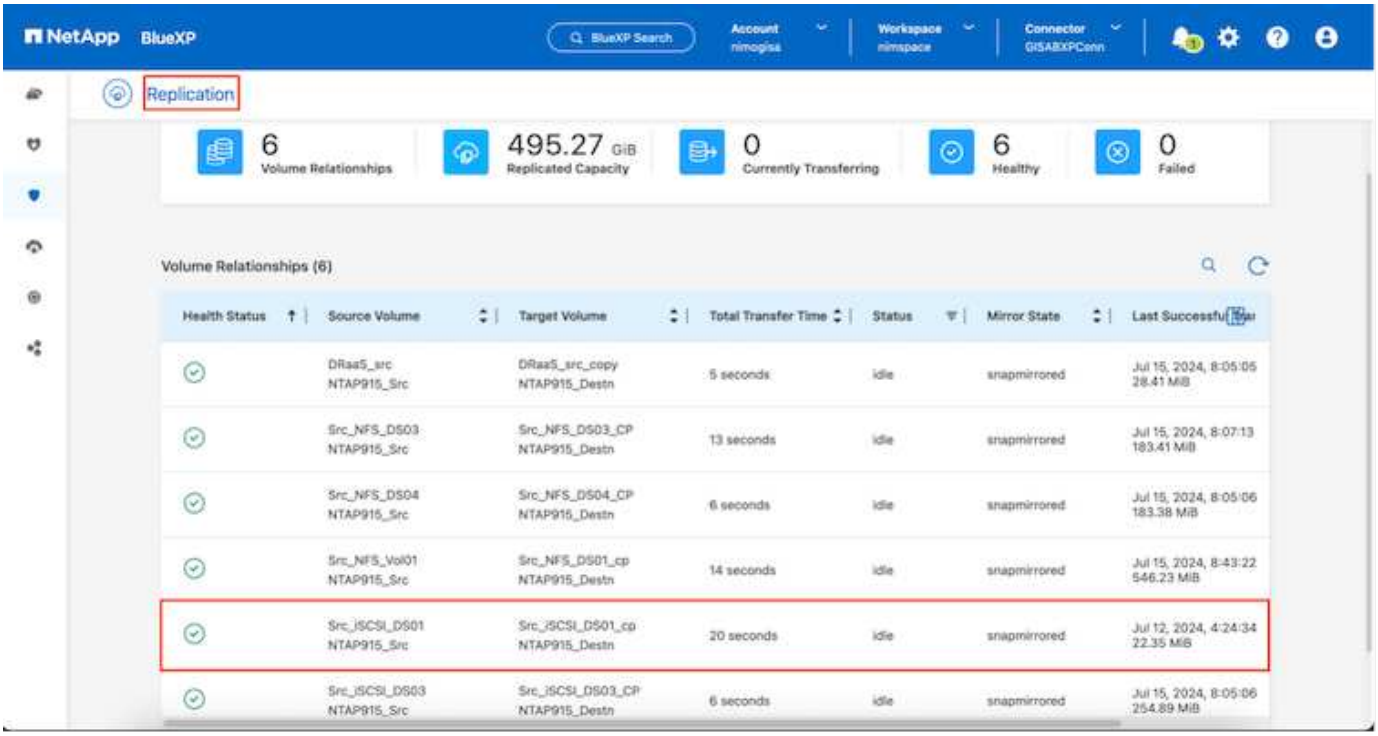
O grupo de recursos também pode ser criado durante a criação de um plano de replicação.

A ordem de inicialização das VMs pode ser definida ou modificada durante a criação de grupos de recursos usando um mecanismo simples de arrastar e soltar.



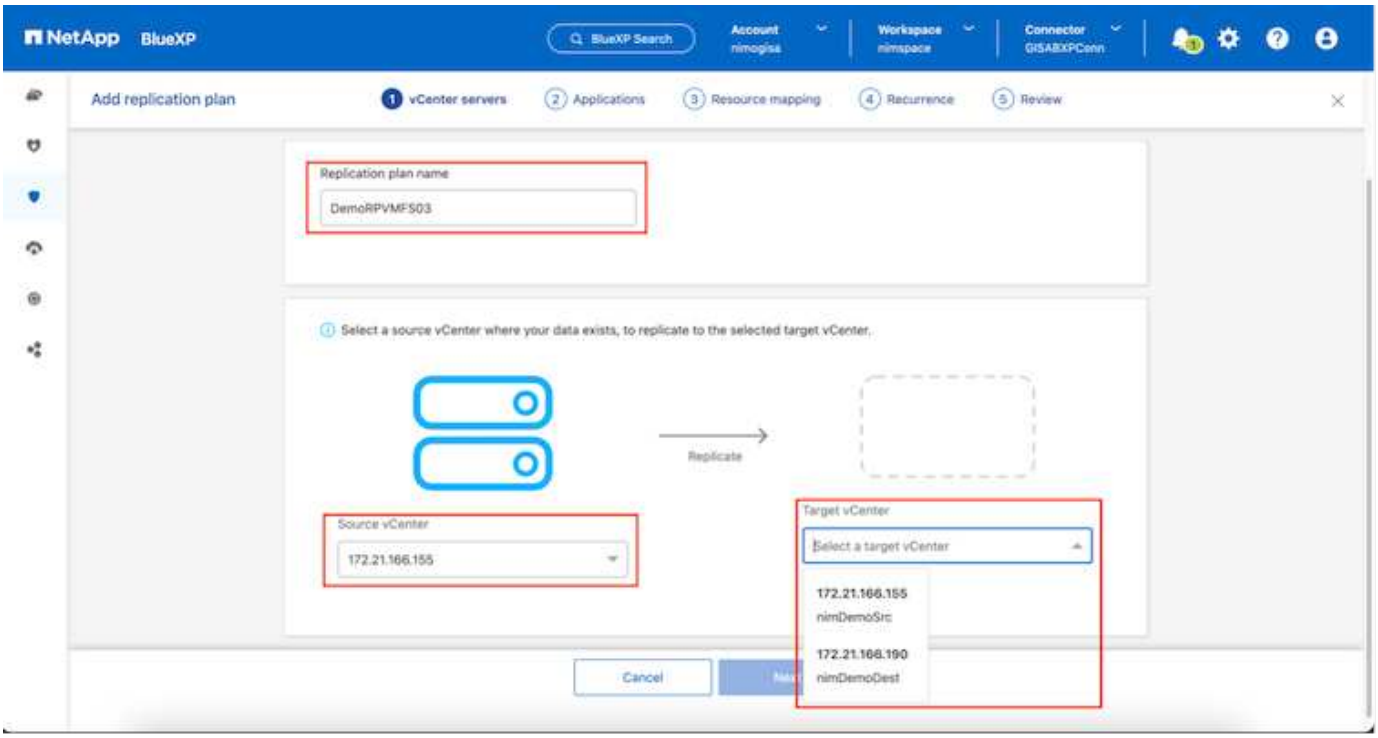
Depois que os grupos de recursos forem criados, a próxima etapa é criar o projeto de execução ou um plano para recuperar máquinas virtuais e aplicativos em caso de desastre. Conforme mencionado nos pré-requisitos, a replicação do SnapMirror pode ser configurada antecipadamente ou o DRaaS pode configurá-la usando o RPO e a contagem de retenção especificados durante a criação do plano de replicação.



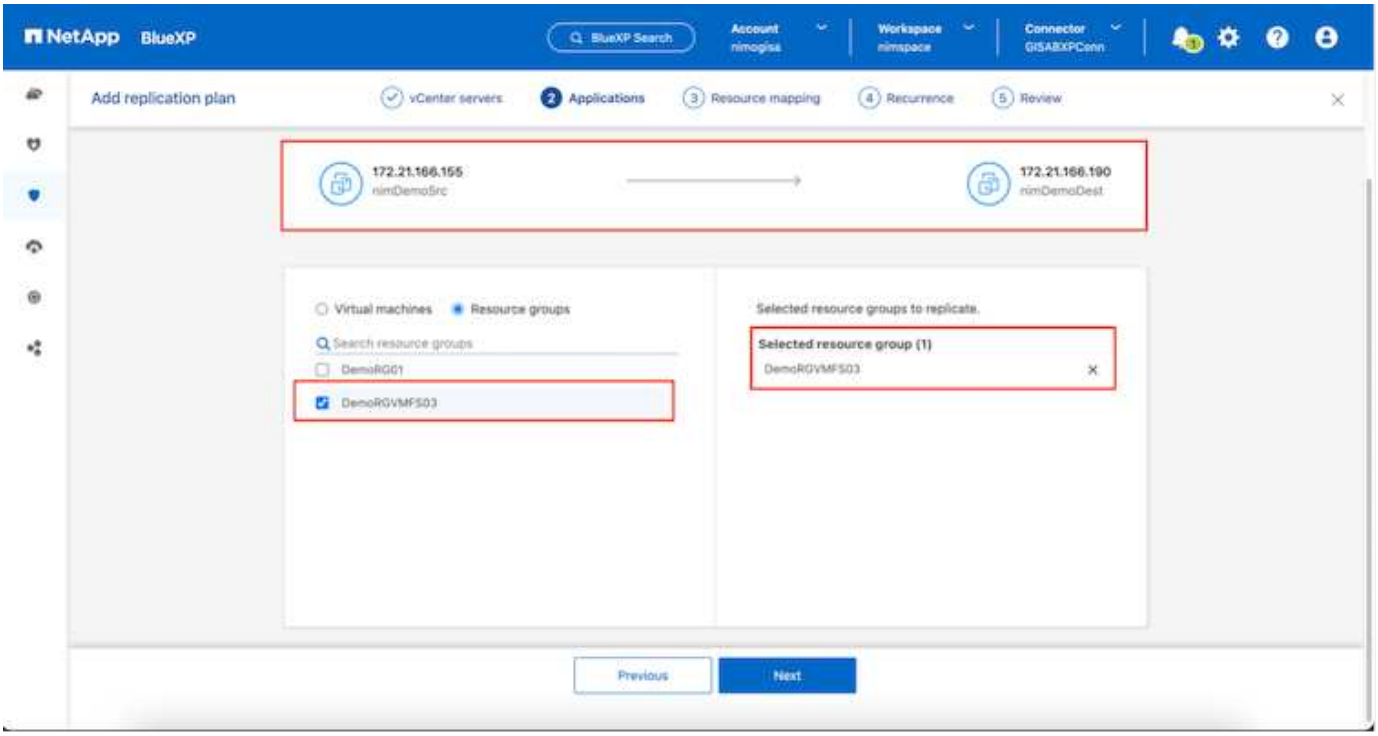


Configure o plano de replicação selecionando as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos no plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados e o mapeamento de clusters e redes. Para definir o plano de recuperação, navegue até a guia **Plano de Replicação** e clique em **Adicionar Plano**.

Primeiro, selecione o vCenter de origem e depois selecione o vCenter de destino.



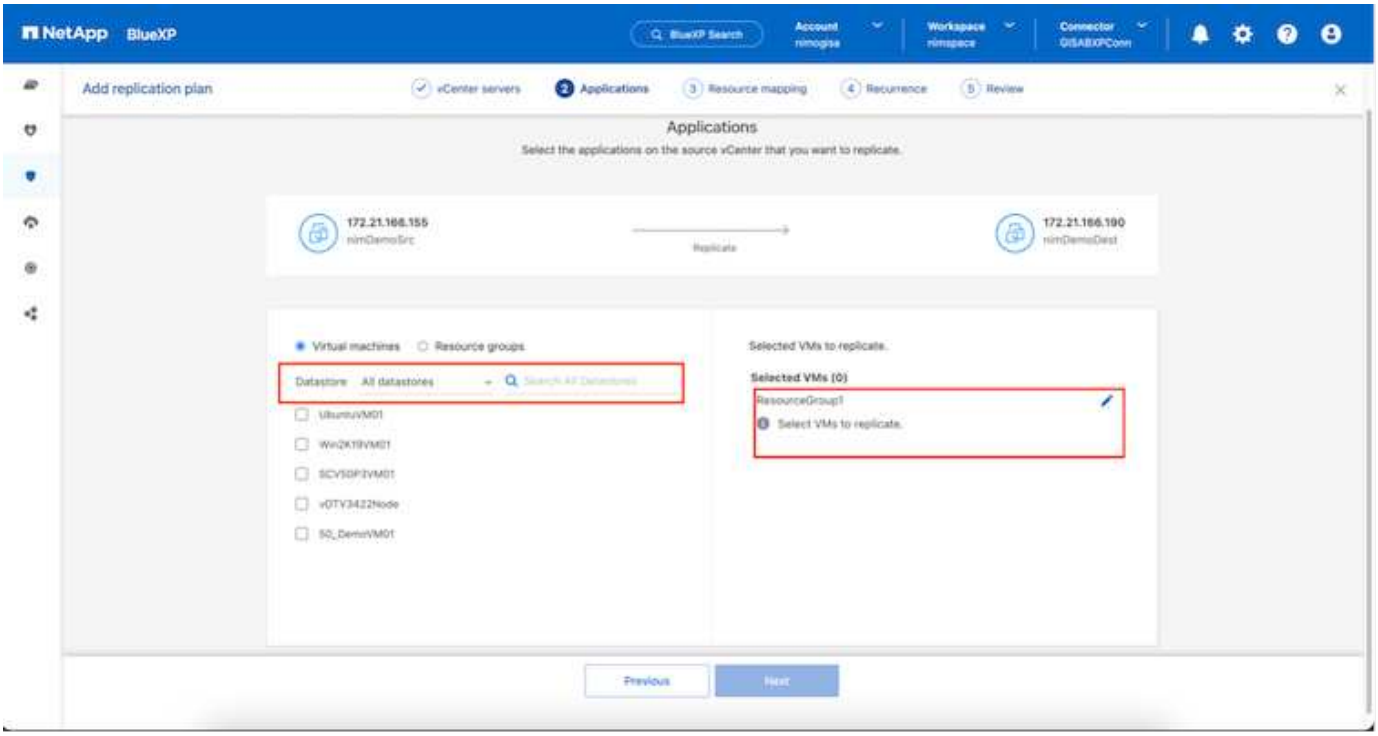
O próximo passo é selecionar grupos de recursos existentes. Se nenhum grupo de recursos for criado, o assistente ajudará a agrupar as máquinas virtuais necessárias (basicamente, criar grupos de recursos funcionais) com base nos objetivos de recuperação. Isso também ajuda a definir a sequência de operação de como as máquinas virtuais do aplicativo devem ser restauradas.



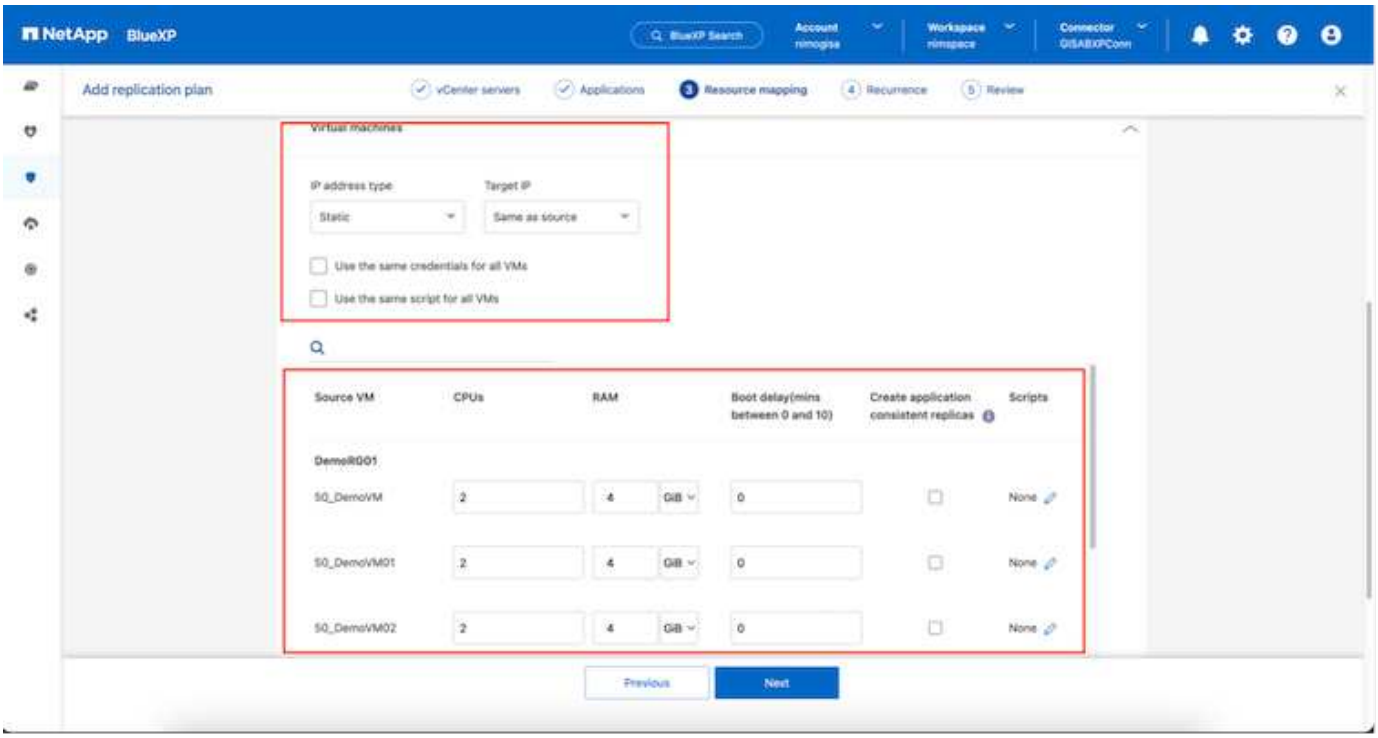
O grupo de recursos permite definir a ordem de inicialização usando a funcionalidade de arrastar e soltar. Ele pode ser usado para modificar facilmente a ordem em que as VMs serão ligadas durante o processo de recuperação.

Cada máquina virtual dentro de um grupo de recursos é iniciada em sequência com base na ordem. Dois grupos de recursos são iniciados em paralelo.

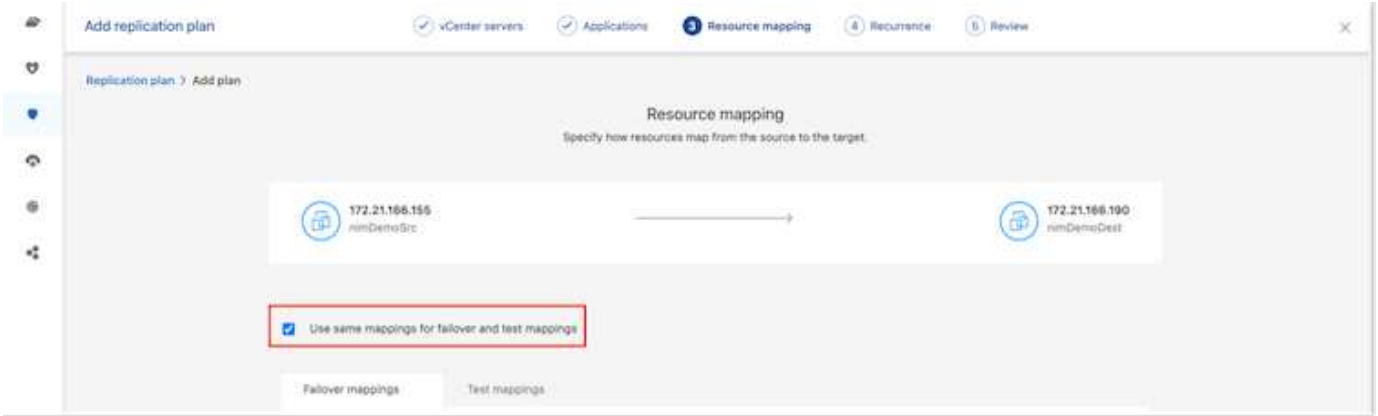
A captura de tela abaixo mostra a opção de filtrar máquinas virtuais ou armazenamentos de dados específicos com base em requisitos organizacionais, caso os grupos de recursos não sejam criados previamente.



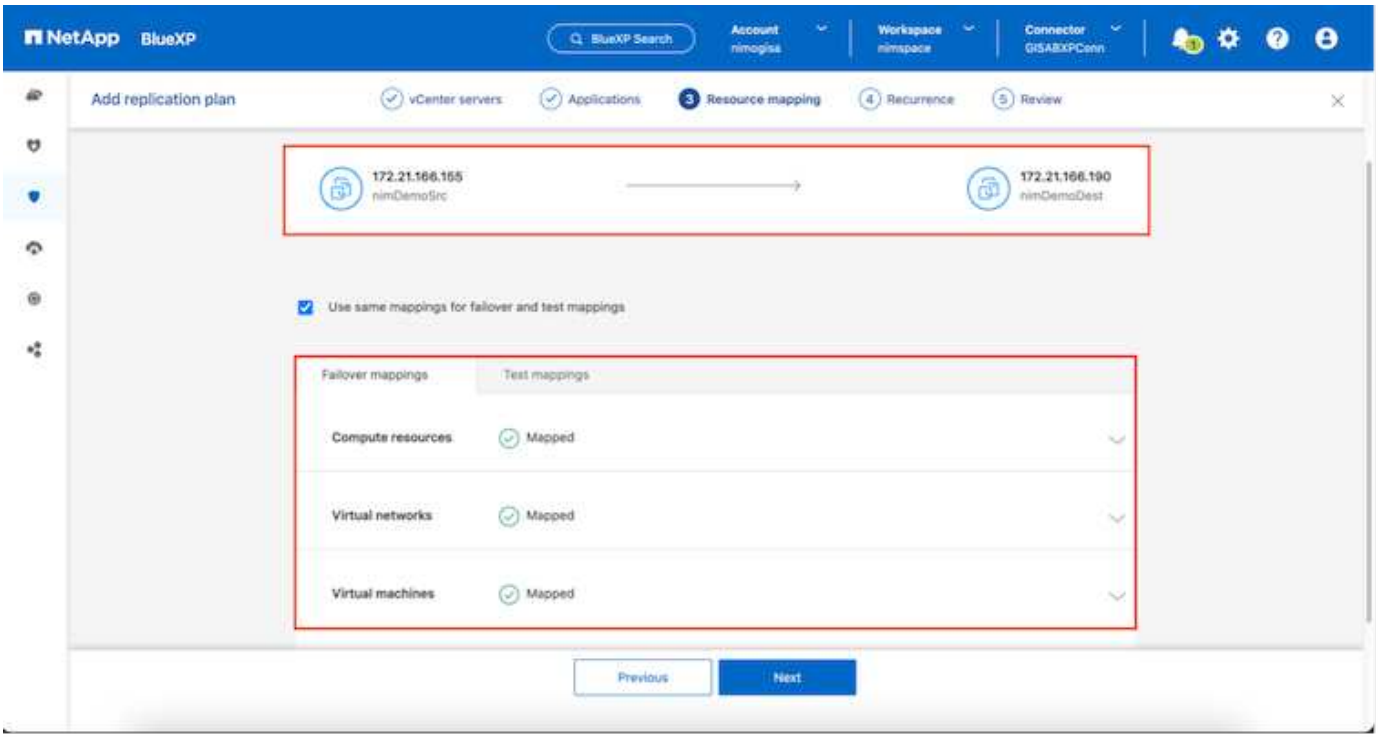
Depois que os grupos de recursos forem selecionados, crie os mapeamentos de failover. Nesta etapa, especifique como os recursos do ambiente de origem são mapeados para o destino. Isso inclui recursos de computação e redes virtuais. Personalização de IP, pré e pós-scripts, atrasos de inicialização, consistência de aplicativos e assim por diante. Para obter informações detalhadas, consulte"Crie um plano de replicação" .



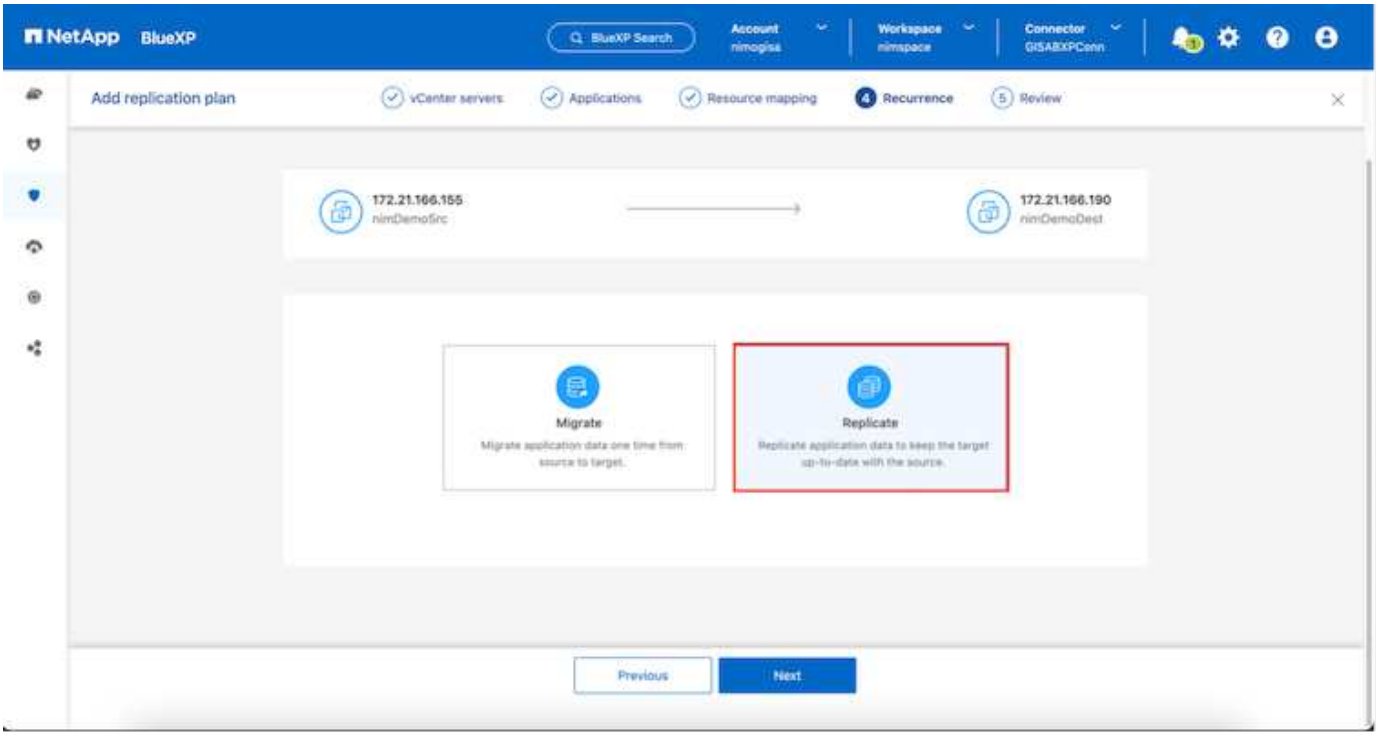
Por padrão, os mesmos parâmetros de mapeamento são usados para operações de teste e failover. Para aplicar mapeamentos diferentes para o ambiente de teste, selecione a opção Mapeamento de teste depois de desmarcar a caixa de seleção, conforme mostrado abaixo:



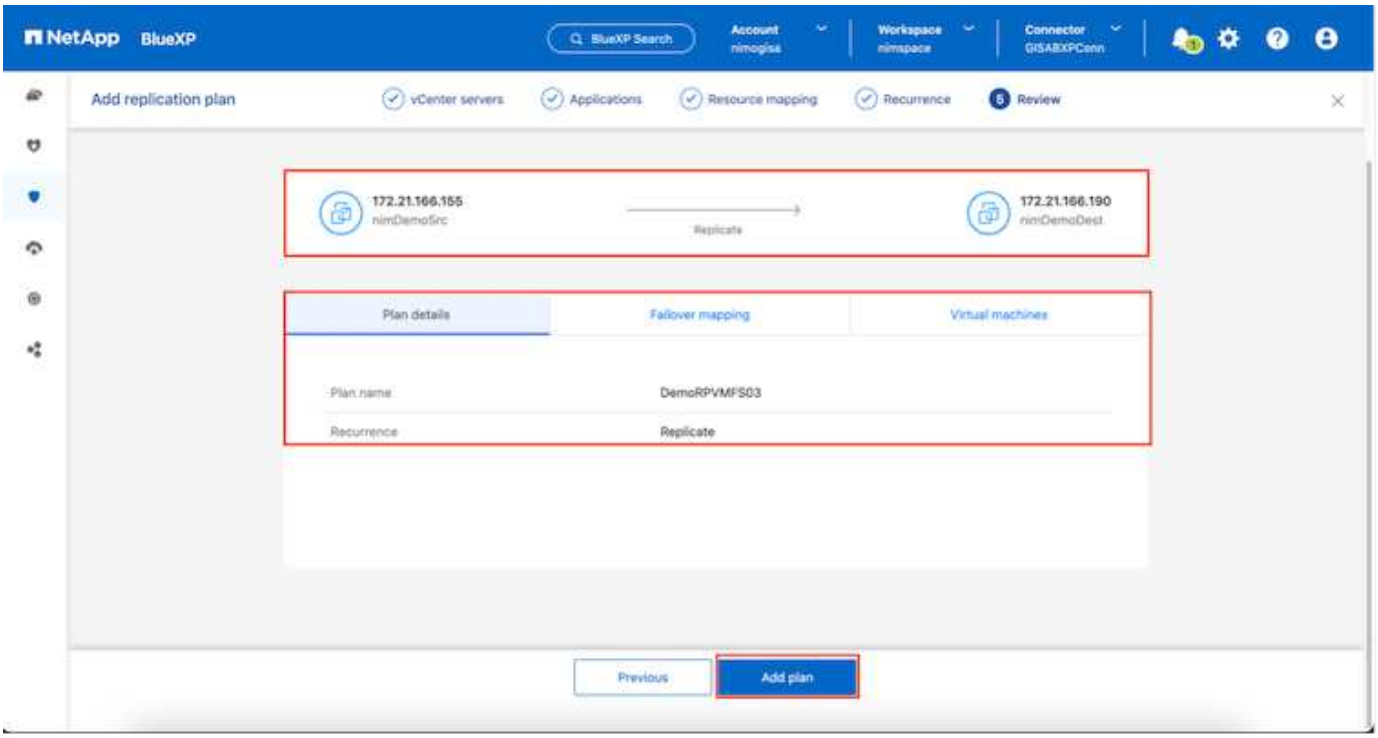
Quando o mapeamento de recursos estiver concluído, clique em Avançar.

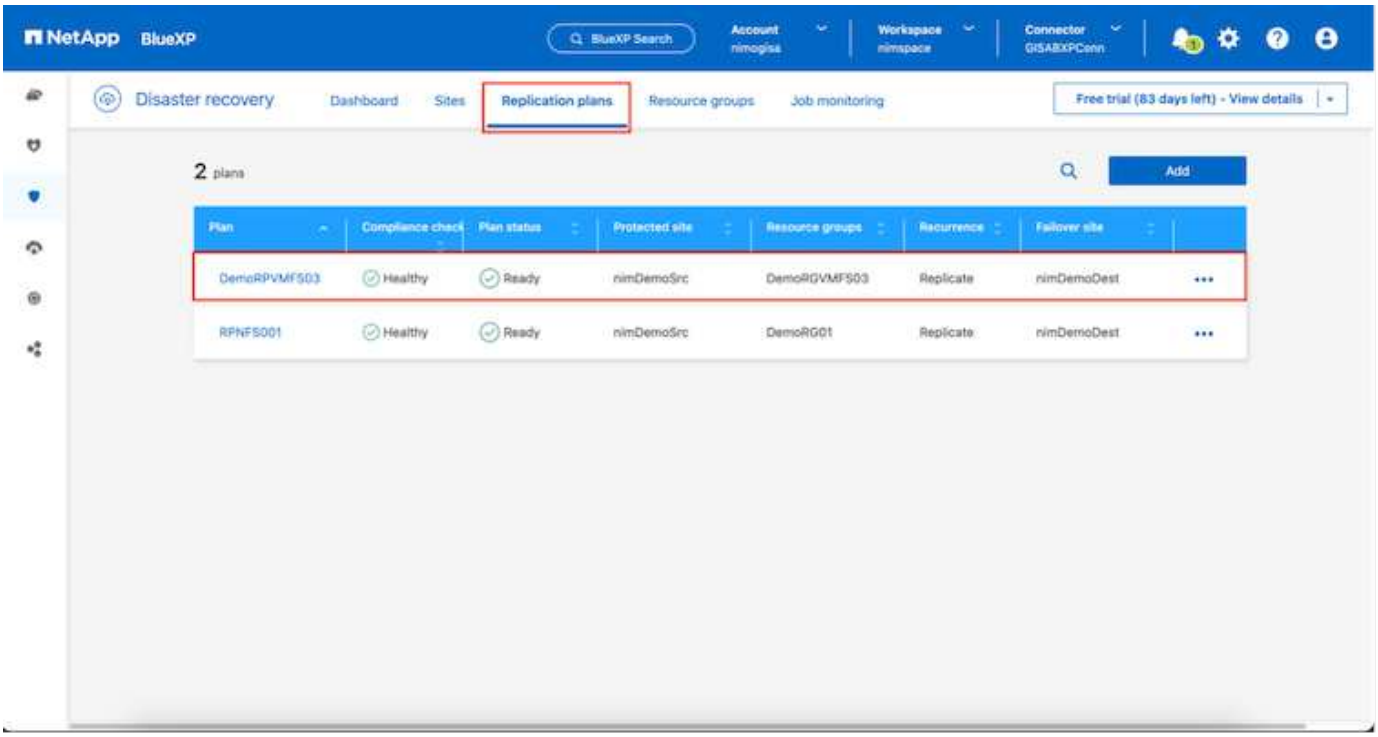


Selecione o tipo de recorrência. Em palavras simples, selecione Migrar (migração única usando failover) ou a opção de replicação contínua recorrente. Neste passo a passo, a opção Replicar está selecionada.

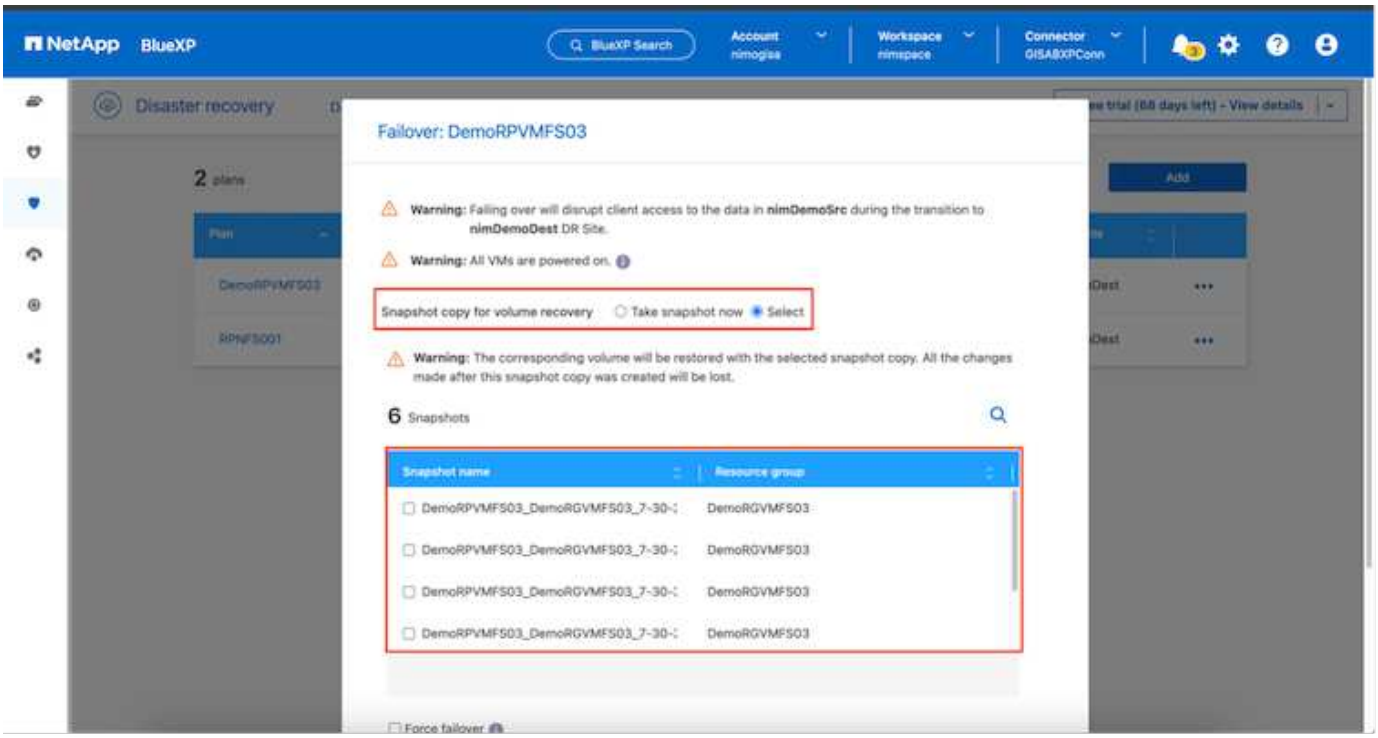


Uma vez concluído, revise os mapeamentos criados e clique em Adicionar plano.

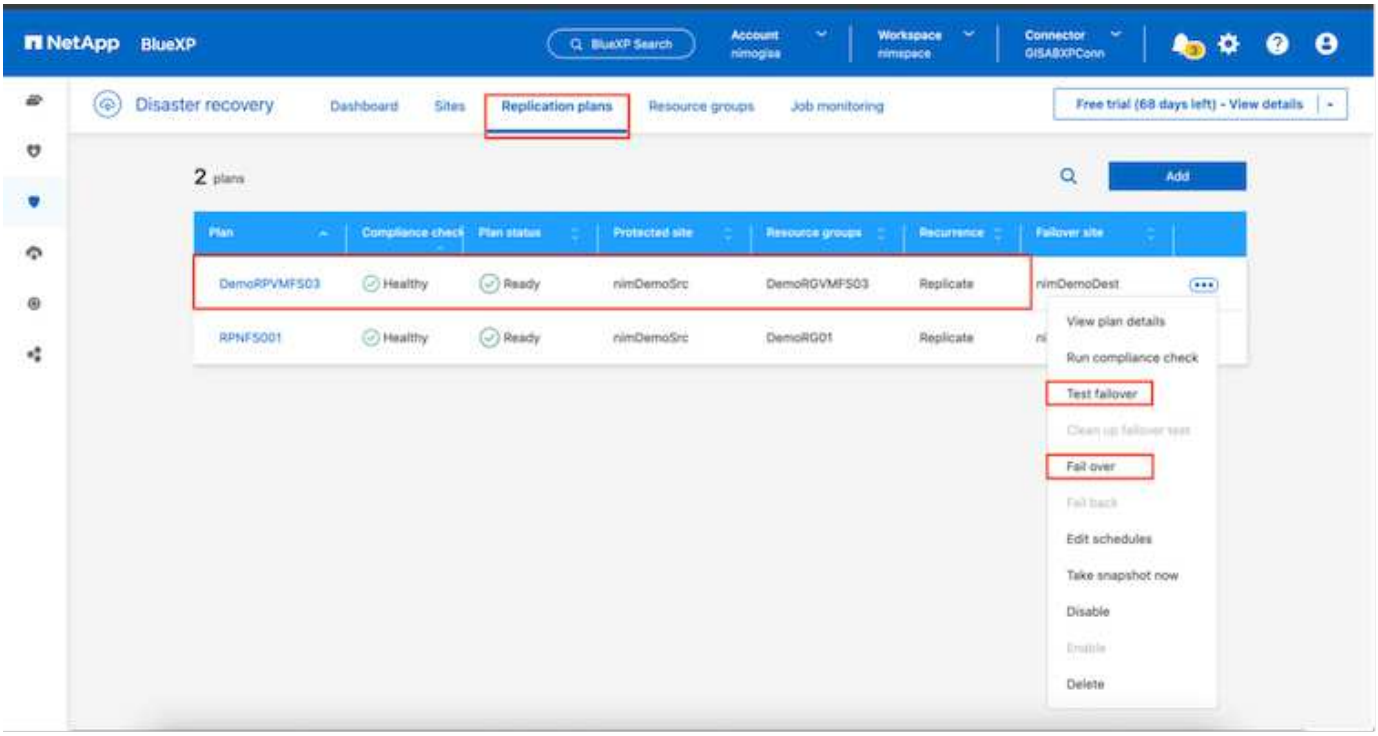




Depois que o plano de replicação for criado, o failover poderá ser executado dependendo dos requisitos, selecionando a opção failover, a opção test-failover ou a opção migrate. A BlueXP disaster recovery garante que o processo de replicação seja executado de acordo com o plano a cada 30 minutos. Durante as opções de failover e teste-failover, você pode usar a cópia mais recente do SnapMirror Snapshot ou selecionar uma cópia específica do Snapshot de uma cópia pontual do Snapshot (conforme a política de retenção do SnapMirror). A opção de momento específico pode ser muito útil se houver um evento de corrupção, como um ransomware, em que as réplicas mais recentes já estão comprometidas ou criptografadas. A BlueXP disaster recovery mostra todos os pontos de recuperação disponíveis.



Para acionar o failover ou testar o failover com a configuração especificada no plano de replicação, clique em **Failover** ou **Testar failover**.

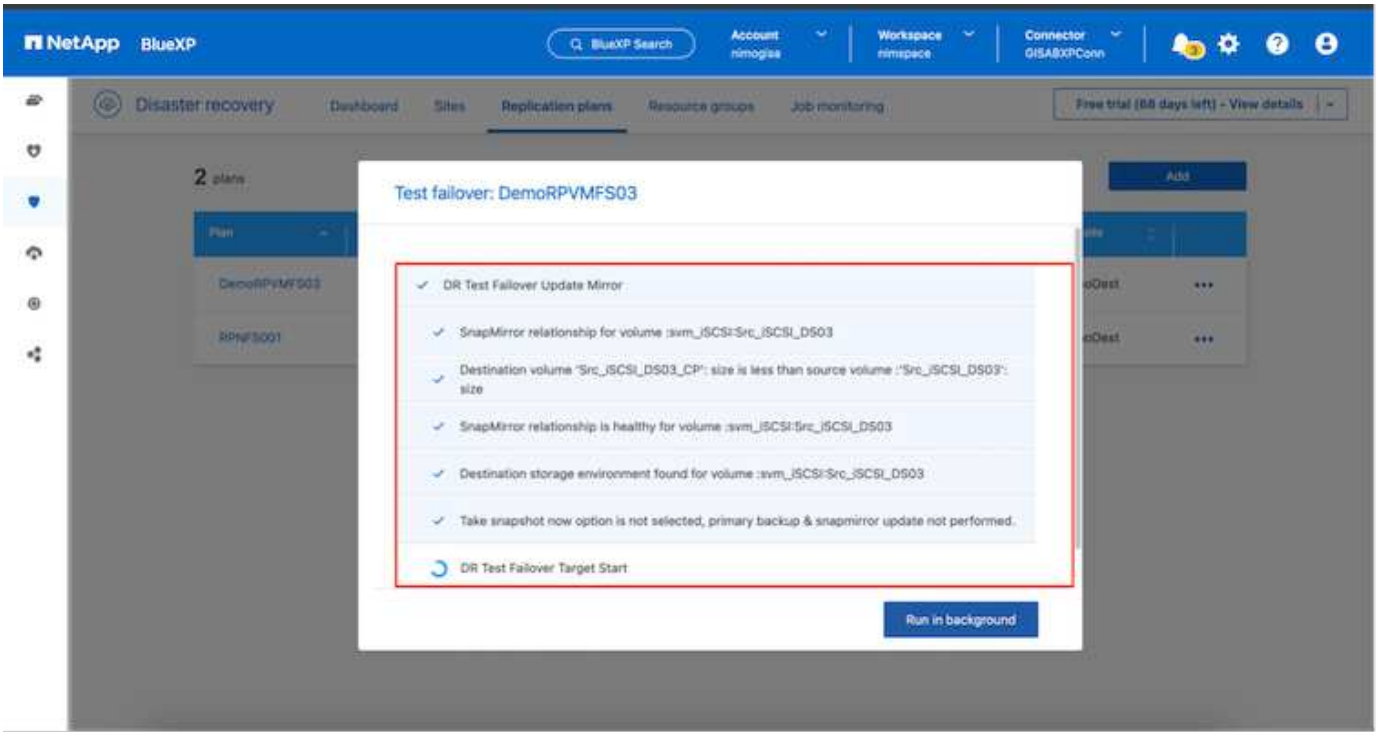


O que acontece durante uma operação de failover ou failover de teste?

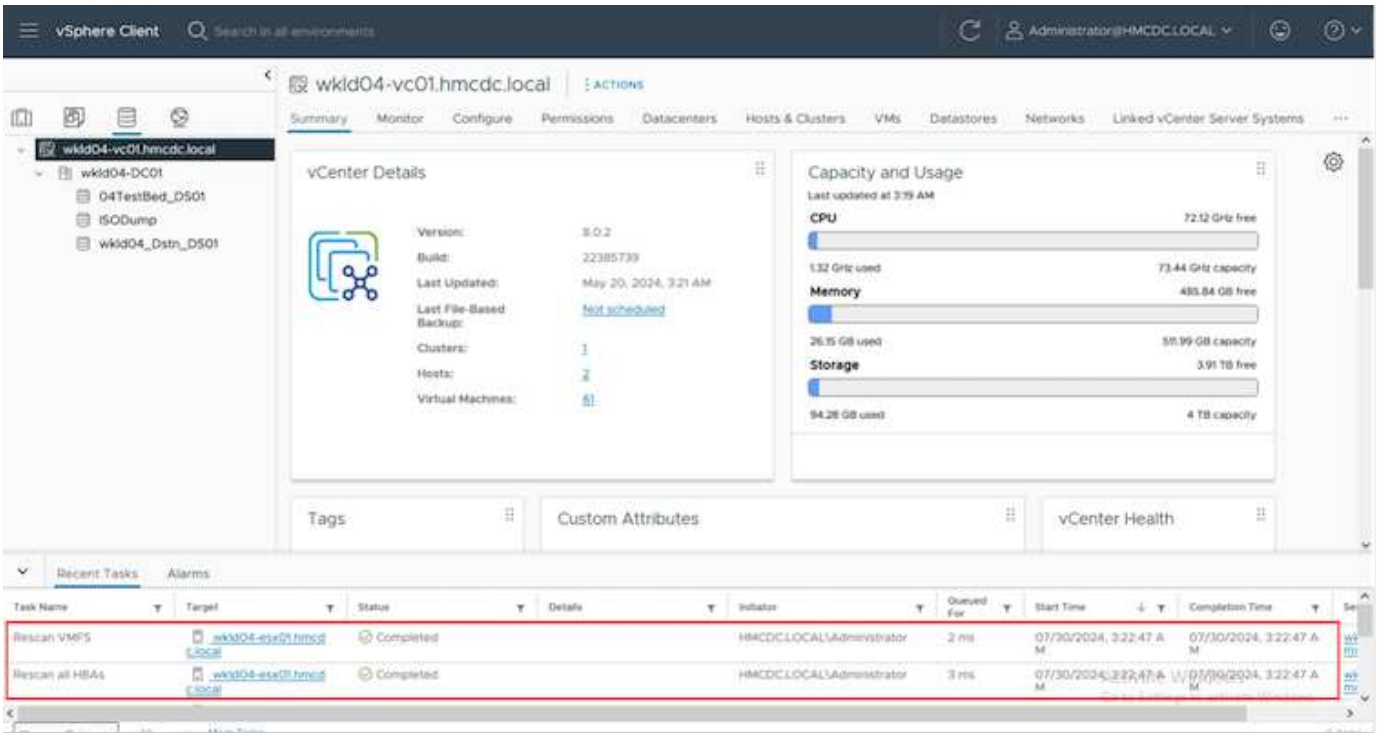
Durante uma operação de failover de teste, a BlueXP disaster recovery cria um volume FlexClone no sistema de armazenamento ONTAP de destino usando a cópia mais recente do Snapshot ou um snapshot selecionado do volume de destino.

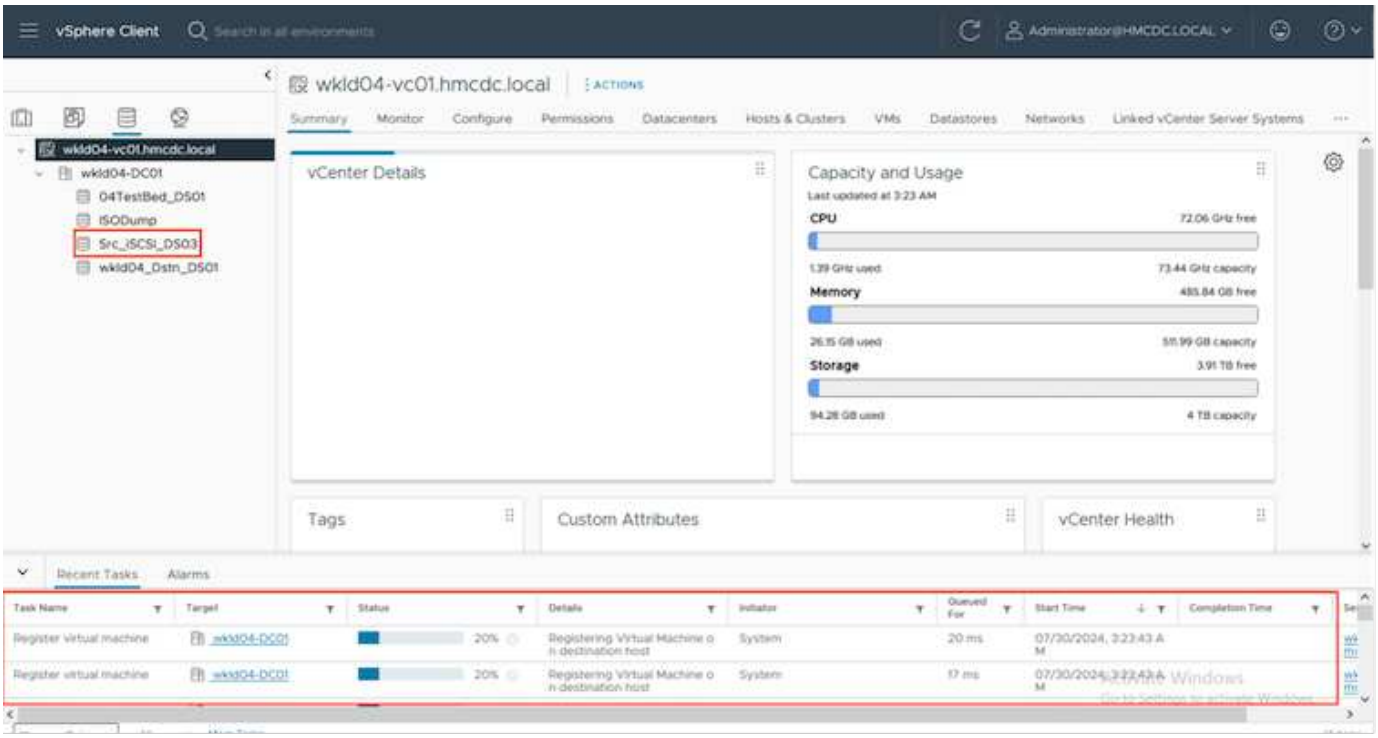
Uma operação de failover de teste cria um volume clonado no sistema de armazenamento ONTAP de destino.

Executar uma operação de recuperação de teste não afeta a replicação do SnapMirror .



Durante o processo, a BlueXP disaster recovery não mapeia o volume de destino original. Em vez disso, ele cria um novo volume FlexClone a partir do Snapshot selecionado e um armazenamento de dados temporário que faz o backup do volume FlexClone é mapeado para os hosts ESXi.

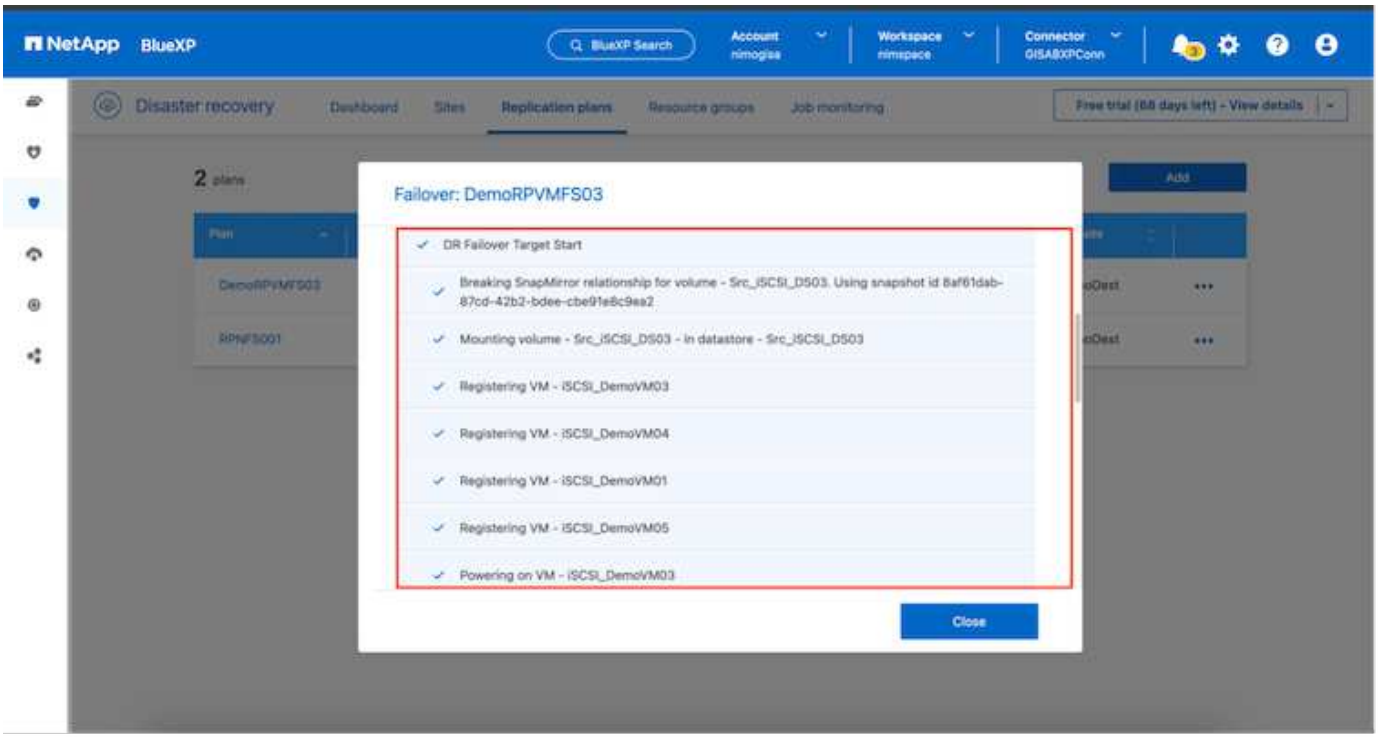




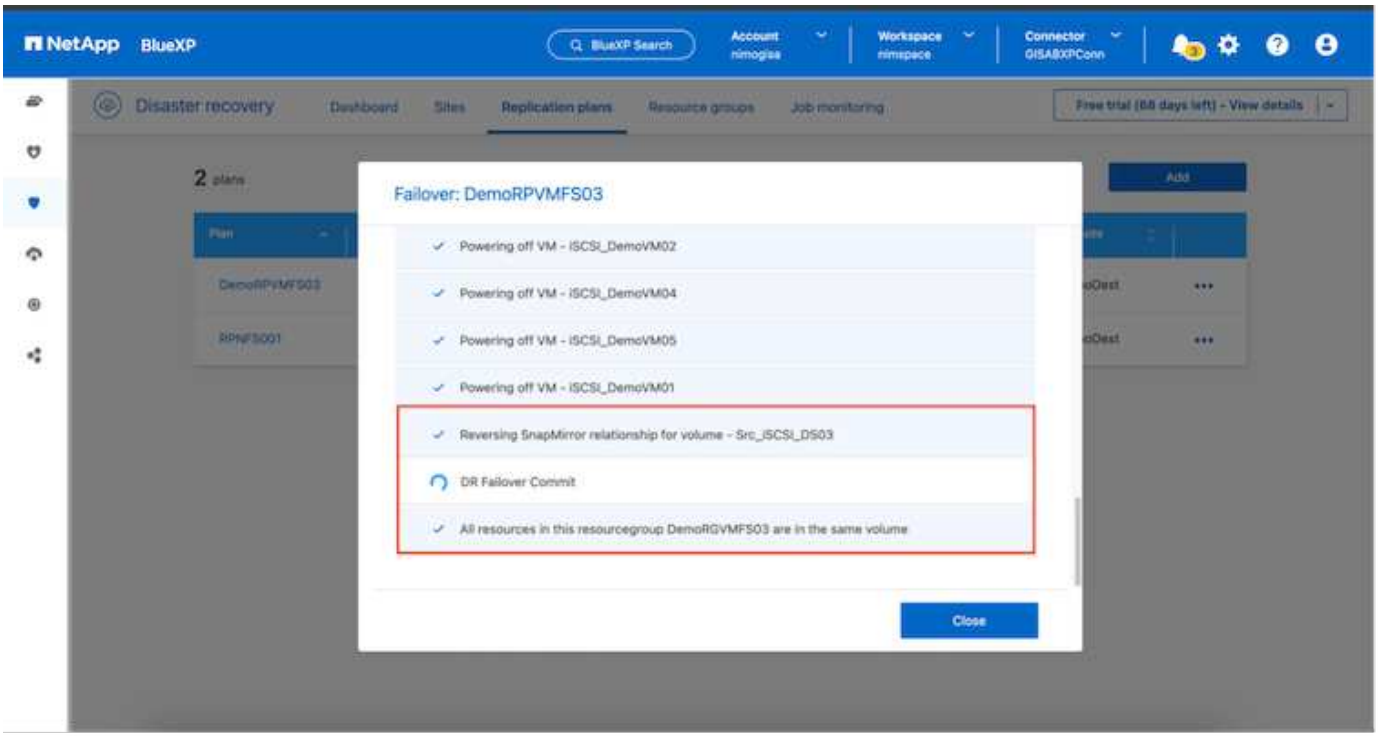
Quando a operação de failover de teste for concluída, a operação de limpeza poderá ser acionada usando **"Limpar teste de failover"**. Durante esta operação, a BlueXP disaster recovery destrói o volume FlexClone que foi usado na operação.

No caso de ocorrer um desastre real, a BlueXP disaster recovery executa as seguintes etapas:

1. Quebra o relacionamento SnapMirror entre os sites.
2. Monta o volume do armazenamento de dados VMFS após a resignação para uso imediato.
3. Registre as VMs
4. Ligar VMs



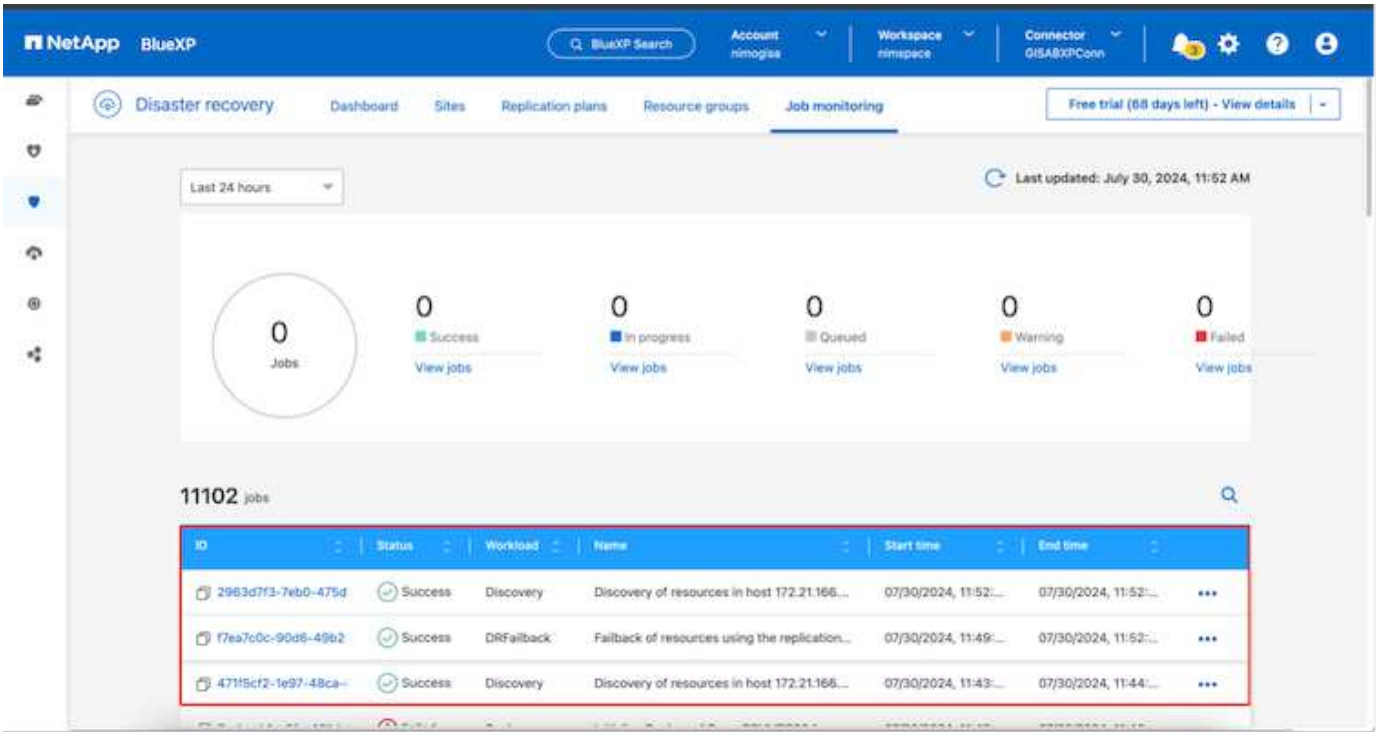
Depois que o site principal estiver instalado e funcionando, a BlueXP disaster recovery habilitará a ressincronização reversa para o SnapMirror e habilitará o failback, que novamente pode ser executado com o clique de um botão.



E se a opção de migração for escolhida, ela será considerada um evento de failover planejado. Nesse caso, uma etapa adicional é acionada, que é desligar as máquinas virtuais no site de origem. O restante das etapas permanece o mesmo do evento de failover.

No BlueXP ou no ONTAP CLI, você pode monitorar o status de integridade da replicação para os volumes de armazenamento de dados apropriados, e o status de um failover ou failover de teste pode ser rastreado por

meio do Monitoramento de tarefas.



Isso fornece uma solução poderosa para lidar com um plano de recuperação de desastres personalizado e personalizado. O failover pode ser feito como failover planejado ou failover com o clique de um botão quando ocorre um desastre e é tomada a decisão de ativar o site de DR.

Para saber mais sobre esse processo, fique à vontade para seguir o vídeo passo a passo detalhado ou usar o"simulador de soluções" .

Configurar recuperação de desastres para armazenamentos de dados NFS usando a BlueXP disaster recovery

Neste caso de uso, descrevemos o procedimento para configurar a recuperação de desastres usando a BlueXP disaster recovery para VMs VMware locais usando armazenamentos de dados NFS. Este procedimento inclui a configuração da conta e do conector BlueXP , a adição de matrizes ONTAP para permitir a comunicação entre o VMware vCenter e o armazenamento ONTAP , a configuração da replicação entre sites e a criação e o teste de planos de recuperação.

Implementar a recuperação de desastres por meio de replicação em nível de bloco do site de produção para o site de recuperação de desastres é um método resiliente e econômico para proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados, como ataques de ransomware. Usando a replicação do NetApp SnapMirror , as cargas de trabalho do VMware em execução em sistemas ONTAP locais com armazenamento de dados NFS podem ser replicadas para outro sistema de armazenamento ONTAP localizado em um datacenter de recuperação designado onde o VMware também está implantado.

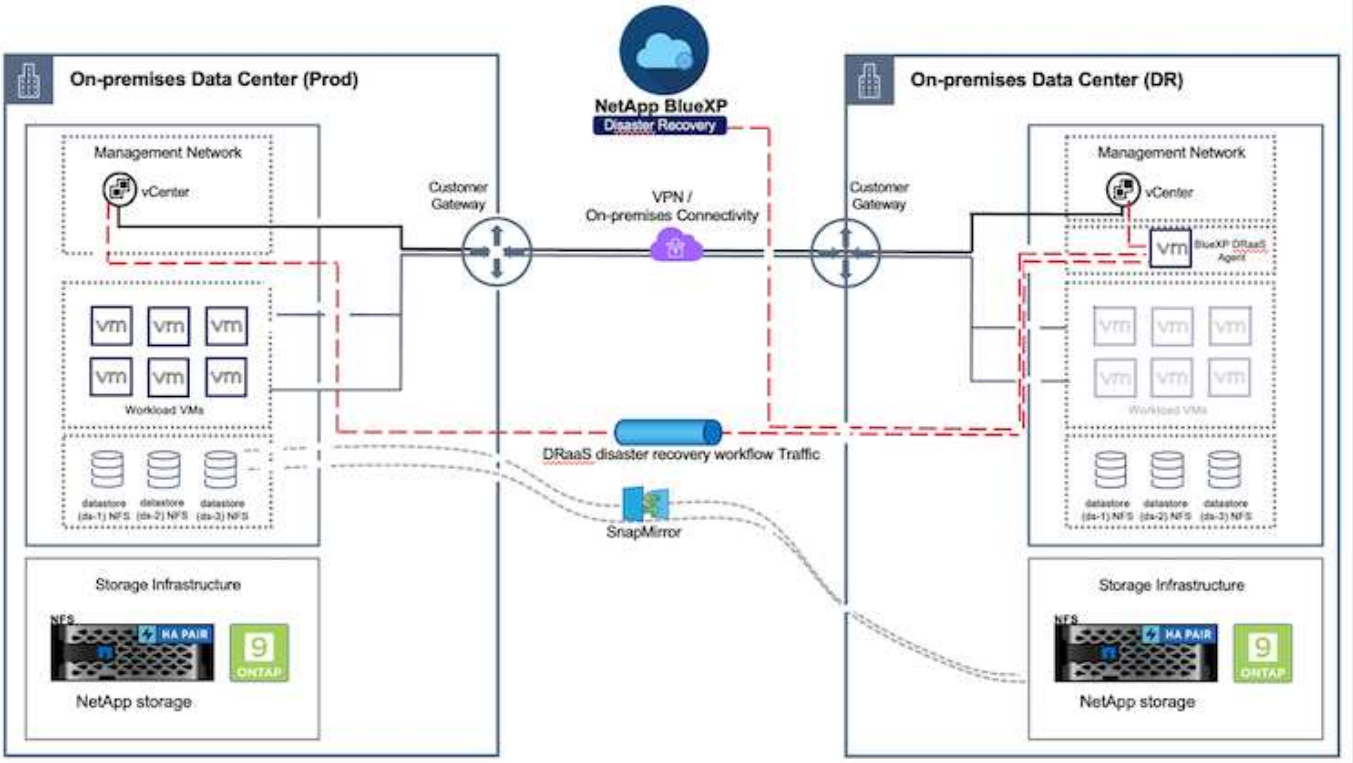
Introdução

Esta seção do documento descreve a configuração do BlueXP DRaaS para configurar a recuperação de desastres de VMs VMware locais para outro site designado. Como parte dessa configuração, a conta BlueXP , o conector BlueXP e os arrays ONTAP adicionados ao espaço de trabalho BlueXP são necessários para

permitir a comunicação do VMware vCenter com o armazenamento ONTAP . Além disso, este documento detalha como configurar a replicação entre sites e como configurar e testar um plano de recuperação. A última seção contém instruções para executar um failover completo do site e como fazer failback quando o site principal é recuperado e comprado on-line.

Utilizando o serviço de BlueXP disaster recovery , integrado ao console NetApp BlueXP , as empresas podem descobrir facilmente seus VMware vCenters locais e armazenamento ONTAP . As organizações podem então criar agrupamentos de recursos, criar um plano de recuperação de desastres, associá-lo a grupos de recursos e testar ou executar failover e failback. O SnapMirror fornece replicação de bloco em nível de armazenamento para manter os dois sites atualizados com alterações incrementais, resultando em um Objetivo de Ponto de Recuperação (RPO) de até 5 minutos. Além disso, é possível simular procedimentos de recuperação de desastres sem afetar a produção ou incorrer em custos adicionais de armazenamento.

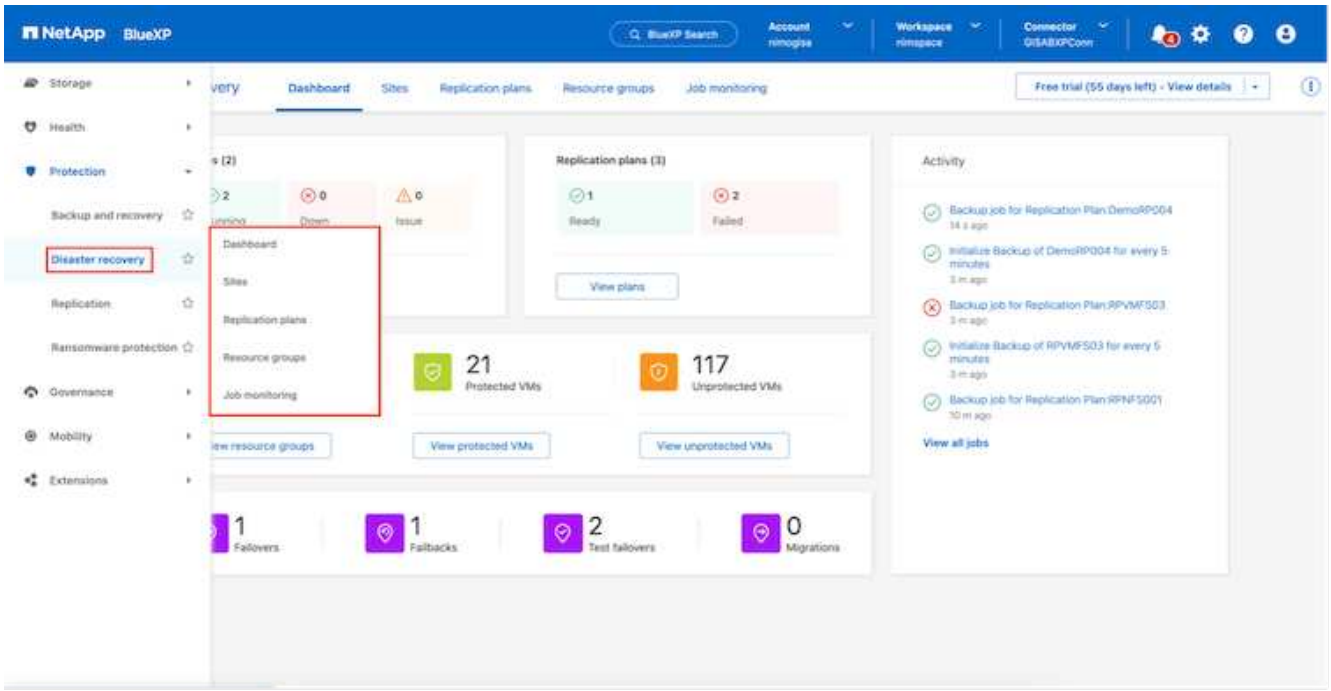
A BlueXP disaster recovery utiliza a tecnologia FlexClone da ONTAP para criar uma cópia com eficiência de espaço do armazenamento de dados NFS a partir do último Snapshot replicado no site de recuperação de desastres. Após concluir o teste de recuperação de desastres, os clientes podem excluir facilmente o ambiente de teste sem afetar os recursos de produção replicados reais. Em caso de failover real, o serviço de BlueXP disaster recovery orquestra todas as etapas necessárias para colocar automaticamente as máquinas virtuais protegidas no site de recuperação de desastres designado com apenas alguns cliques. O serviço também reverterá o relacionamento do SnapMirror com o site principal e replicará quaisquer alterações do secundário para o primário para uma operação de failback, quando necessário. Todos esses recursos custam uma fração do preço de outras alternativas conhecidas.



Começando

Para começar a BlueXP disaster recovery, use o console do BlueXP e acesse o serviço.

1. Faça login no BlueXP.
2. Na navegação à esquerda do BlueXP , selecione Proteção > Recuperação de desastres.
3. O painel de BlueXP disaster recovery é exibido.

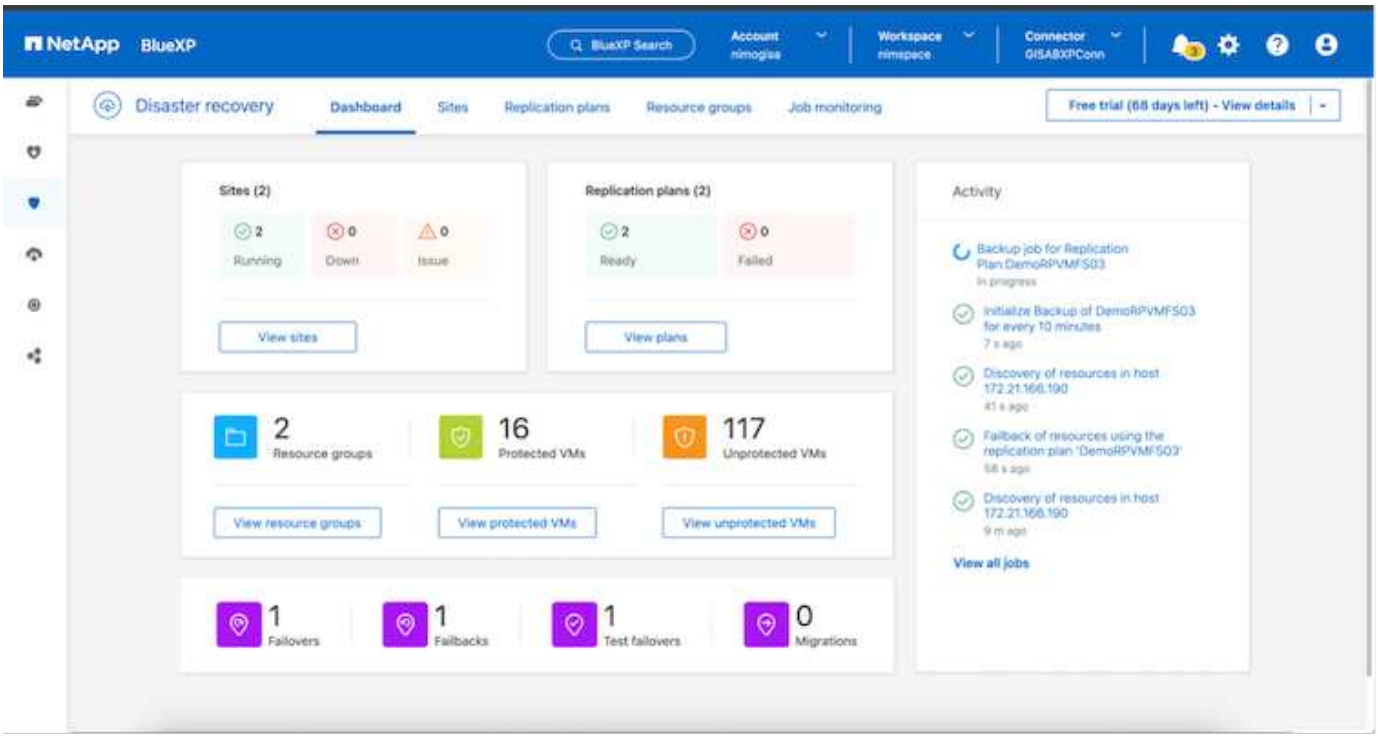


Antes de configurar o plano de recuperação de desastres, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O BlueXP Connector é configurado no NetApp BlueXP.
- A instância do conector BlueXP tem conectividade com os sistemas de armazenamento e vCenter de origem e destino.
- Cluster NetApp Data ONTAP para fornecer armazenamento de dados NFS.
- Os sistemas de armazenamento NetApp locais que hospedam datastores NFS para VMware são adicionados no BlueXP.
- A resolução de DNS deve estar em vigor ao usar nomes DNS. Caso contrário, use endereços IP para o vCenter.
- A replicação do SnapMirror é configurada para os volumes de armazenamento de dados baseados em NFS designados.
- Certifique-se de que o ambiente tenha versões compatíveis dos servidores vCenter Server e ESXi.

Depois que a conectividade for estabelecida entre os sites de origem e destino, prossiga com as etapas de configuração, que devem levar alguns cliques e cerca de 3 a 5 minutos.

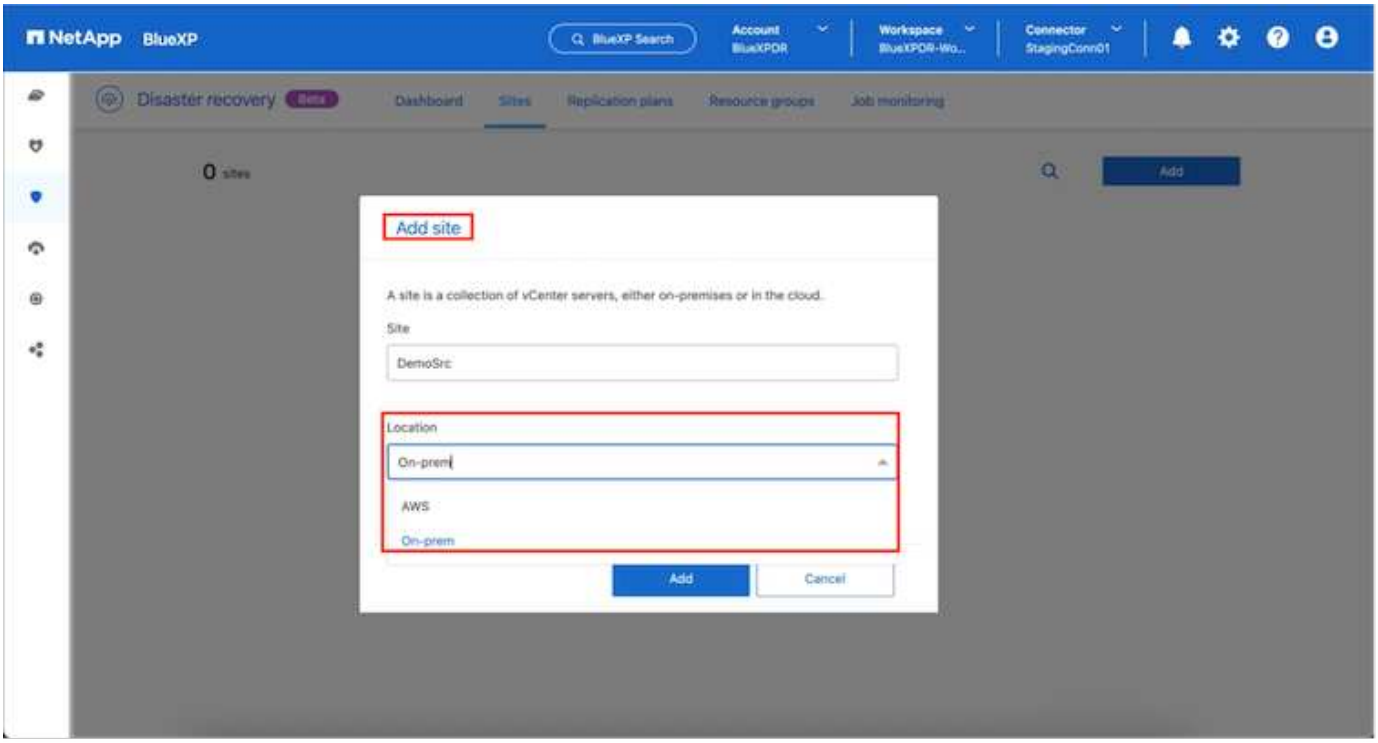
> A NetApp recomenda implantar o conector BlueXP no site de destino ou em um terceiro site, para que o conector BlueXP possa se comunicar pela rede com os recursos de origem e destino.



Configuração de BlueXP disaster recovery

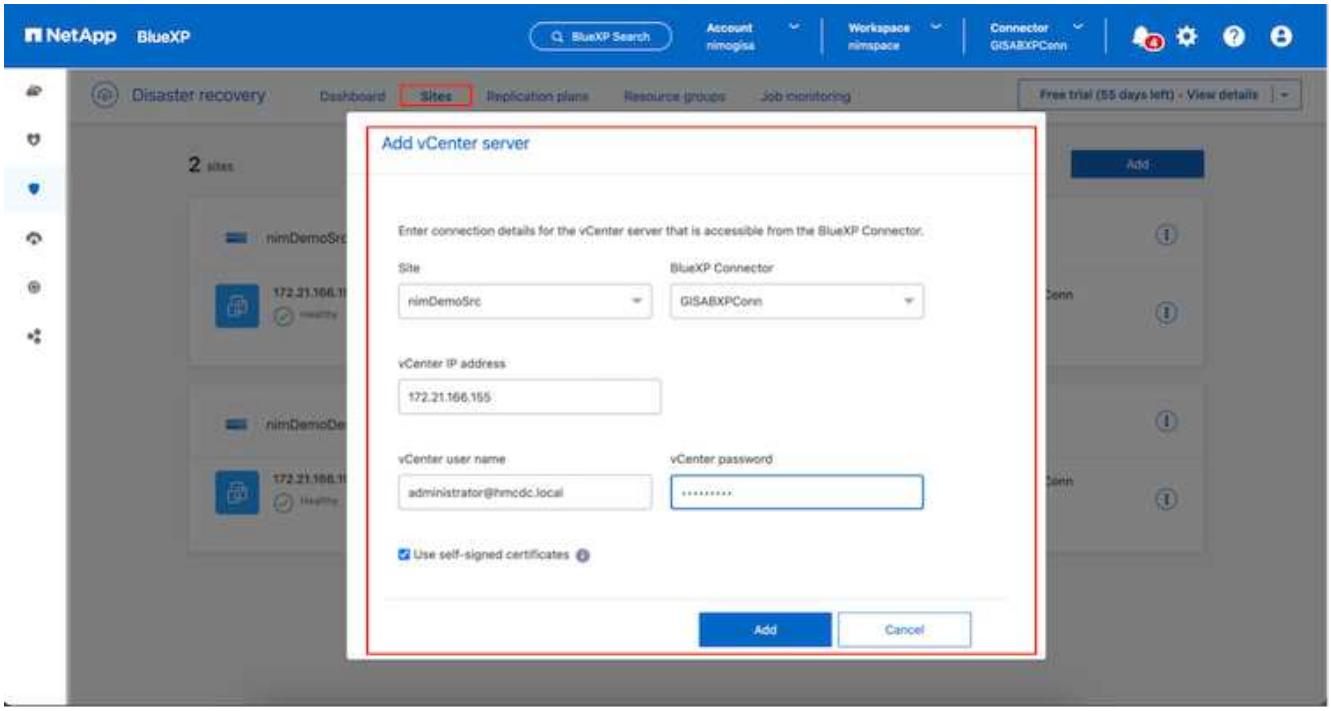
O primeiro passo na preparação para a recuperação de desastres é descobrir e adicionar os recursos de armazenamento e vCenter locais à BlueXP disaster recovery.

Abra o console BlueXP e selecione **Proteção > Recuperação de desastres** na navegação à esquerda. Selecione **Descobrir servidores vCenter** ou use o menu superior, selecione **Sites > Adicionar > Adicionar vCenter**.

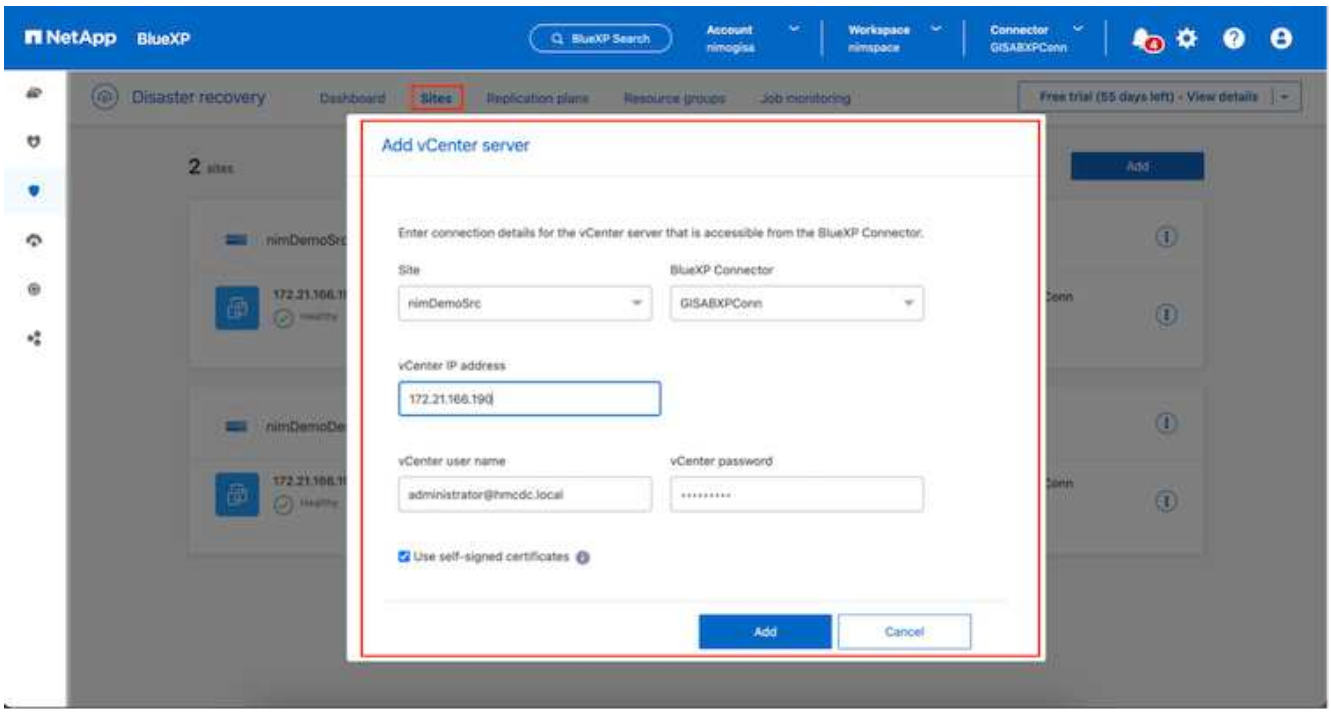


Adicione as seguintes plataformas:

- **Fonte**. vCenter local.



- **Destino**. VMC SDDC vCenter.



Depois que os vCenters são adicionados, a descoberta automatizada é acionada.

Configurando a replicação de armazenamento entre a matriz do site de origem e a matriz do site de destino

O SnapMirror fornece replicação de dados em um ambiente NetApp . Construída com base na tecnologia NetApp Snapshot, a replicação SnapMirror é extremamente eficiente porque replica apenas os blocos que

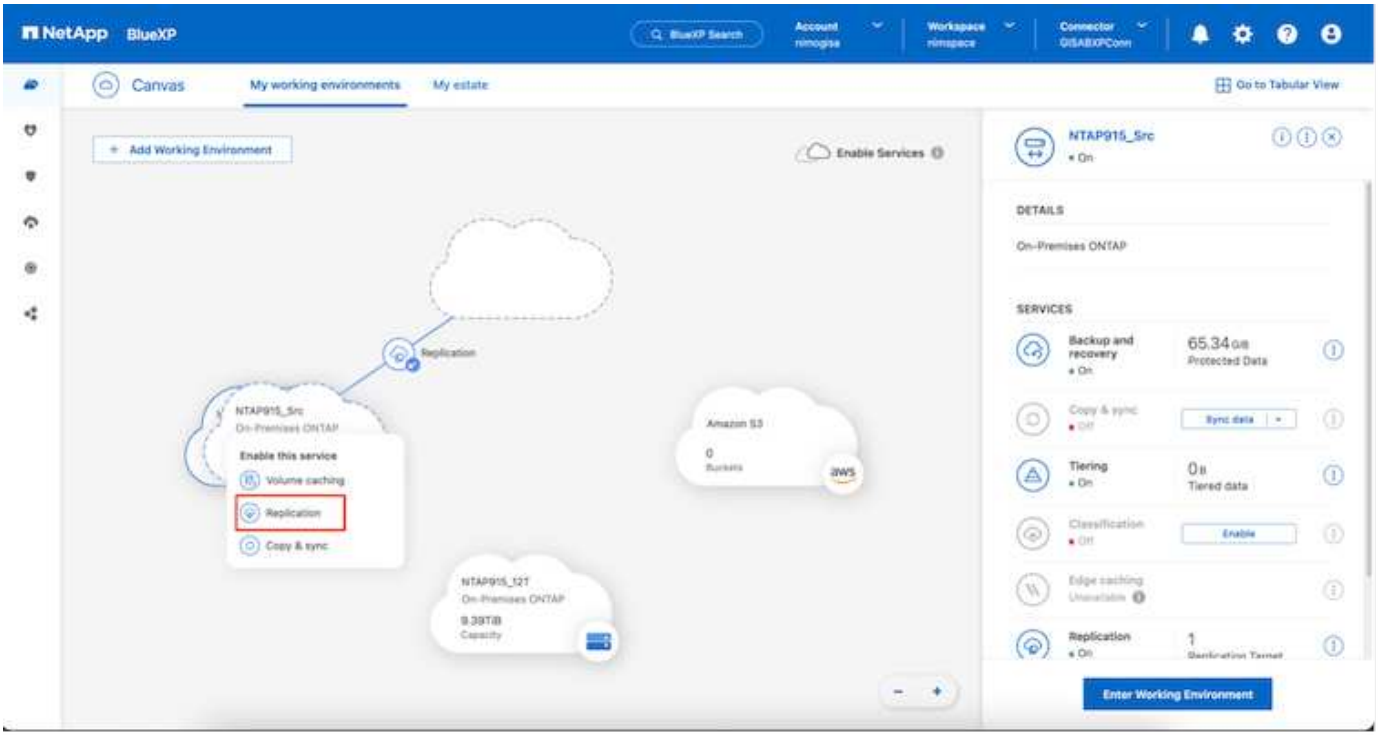
foram alterados ou adicionados desde a atualização anterior. O SnapMirror é facilmente configurado usando o NetApp OnCommand System Manager ou o ONTAP CLI. O BlueXP DRaaS também cria o relacionamento SnapMirror , desde que o cluster e o peering SVM sejam configurados previamente.

Para casos em que o armazenamento primário não é completamente perdido, o SnapMirror fornece um meio eficiente de ressincronizar os sites primário e de DR. O SnapMirror pode ressincronizar os dois sites, transferindo apenas dados alterados ou novos de volta para o site principal a partir do site de DR, simplesmente invertendo os relacionamentos do SnapMirror . Isso significa que os planos de replicação no BlueXP DRaaS podem ser ressincronizados em qualquer direção após um failover sem recopiar o volume inteiro. Se um relacionamento for ressincronizado na direção reversa, somente os novos dados que foram gravados desde a última sincronização bem-sucedida da cópia do Snapshot serão enviados de volta ao destino.

> Se o relacionamento do SnapMirror já estiver configurado para o volume via CLI ou System Manager, o BlueXP DRaaS assume o relacionamento e continua com o restante das operações de fluxo de trabalho.

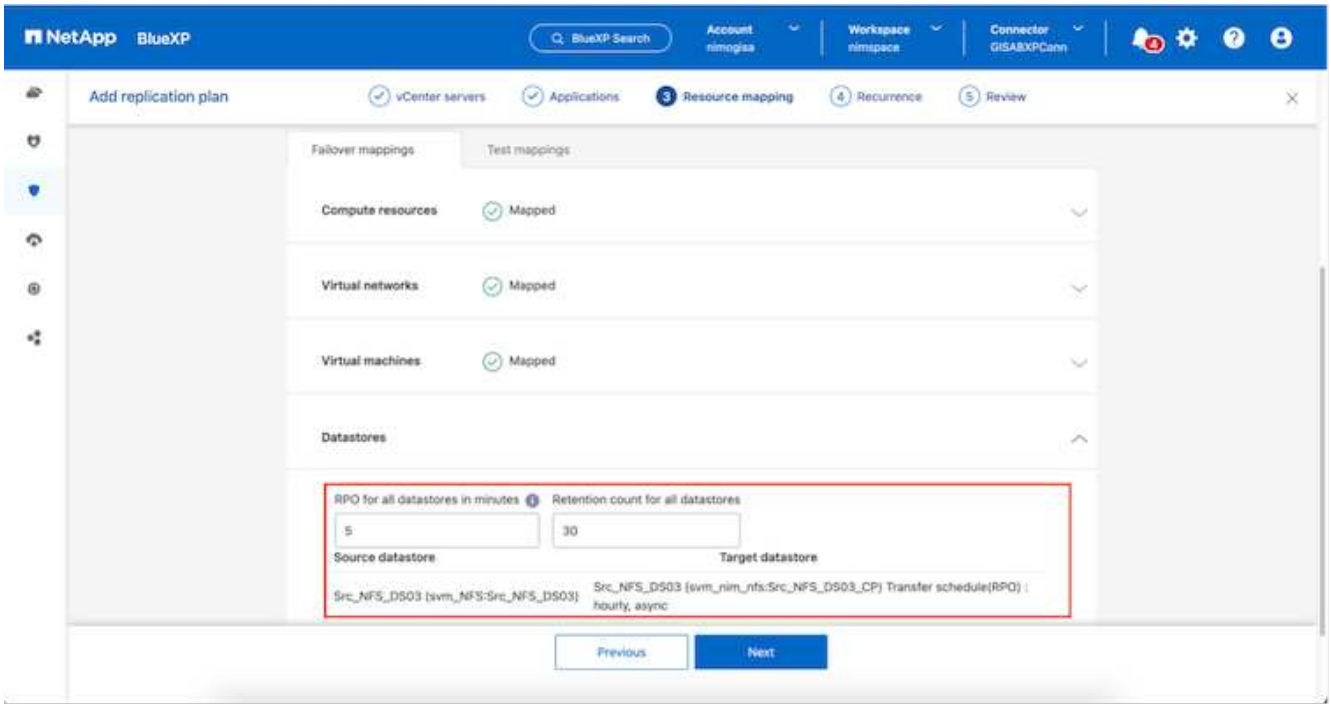
Como configurá-lo para recuperação de desastres do VMware

O processo para criar a replicação do SnapMirror permanece o mesmo para qualquer aplicativo. O processo pode ser manual ou automatizado. A maneira mais fácil é aproveitar o BlueXP para configurar a replicação do SnapMirror usando o simples recurso de arrastar e soltar do sistema ONTAP de origem no ambiente para o destino para acionar o assistente que orienta o restante do processo.



O BlueXP DRaaS também pode automatizar o mesmo, desde que os dois critérios a seguir sejam atendidos:

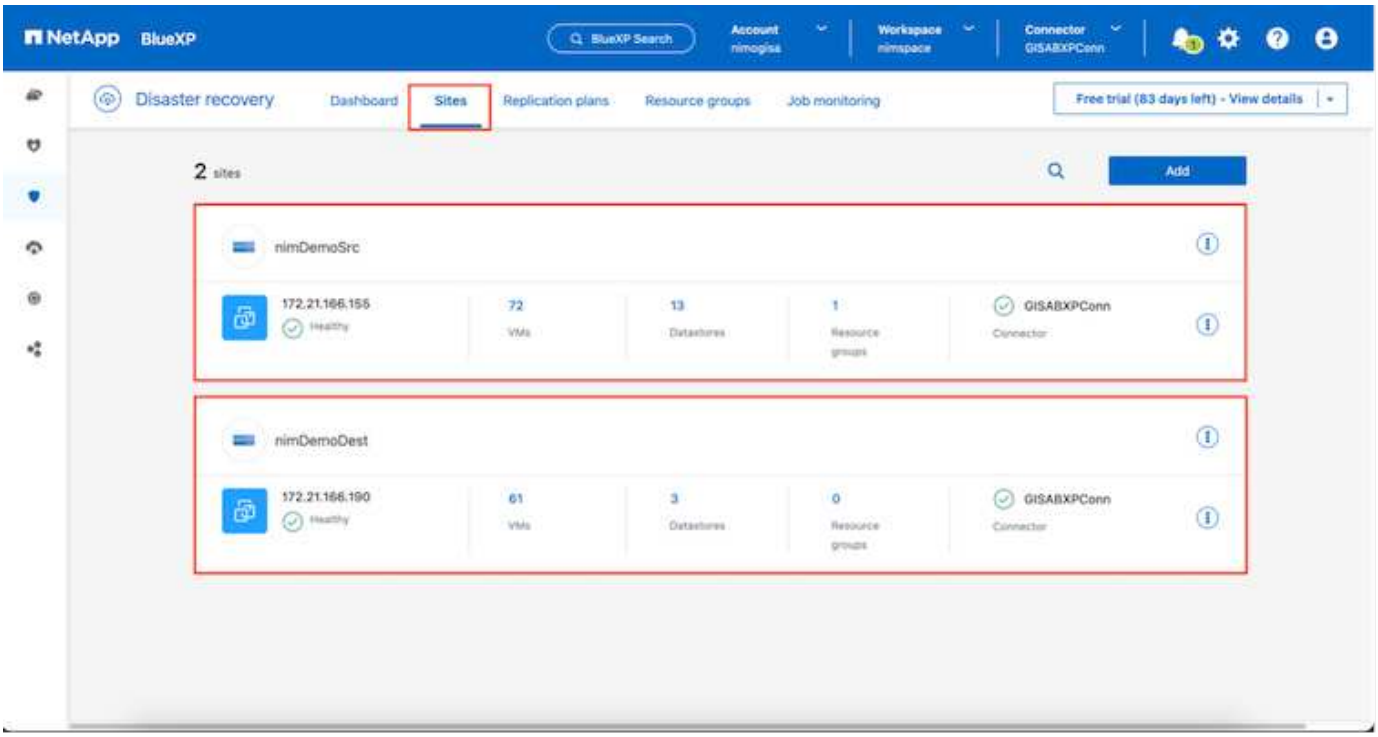
- Os clusters de origem e destino têm um relacionamento de pares.
- O SVM de origem e o SVM de destino têm um relacionamento de mesmo nível.



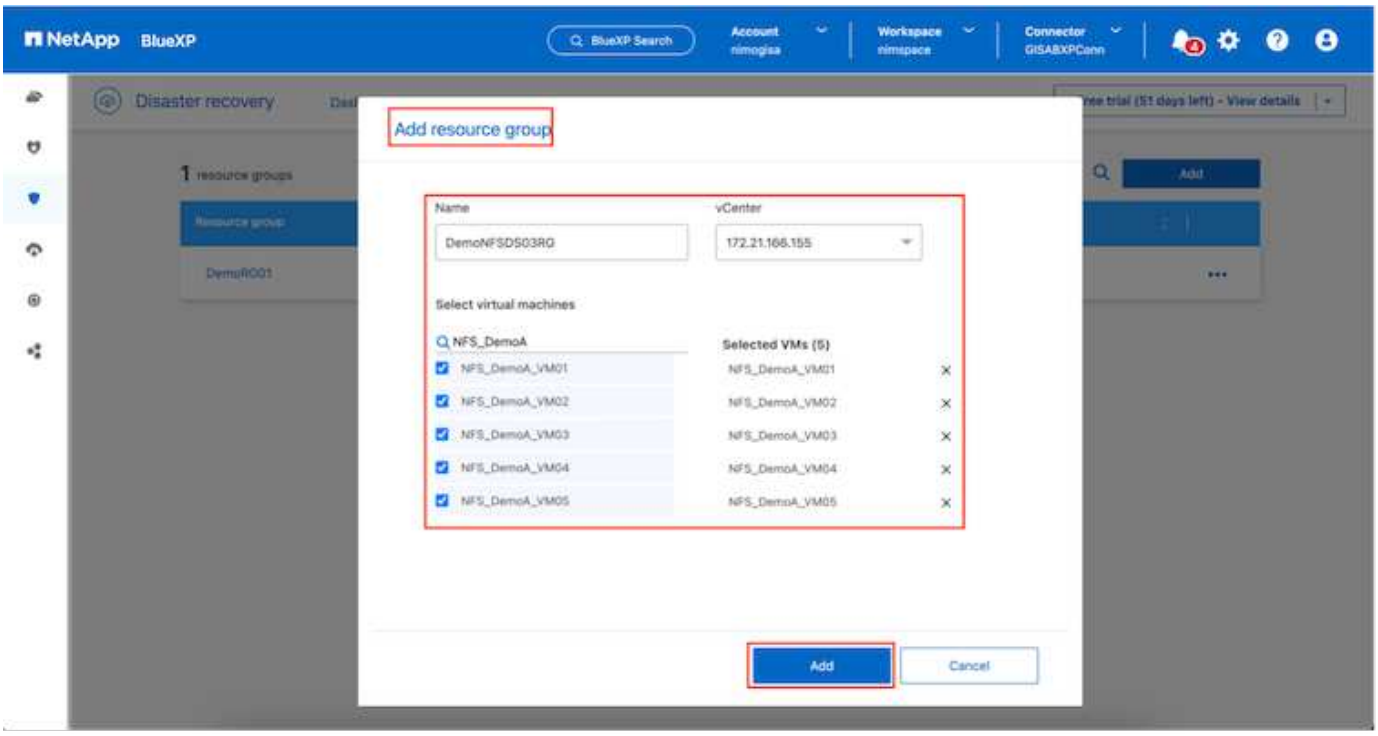
Se o relacionamento do SnapMirror já estiver configurado para o volume via CLI, o BlueXP DRaaS assume o relacionamento e continua com o restante das operações de fluxo de trabalho.

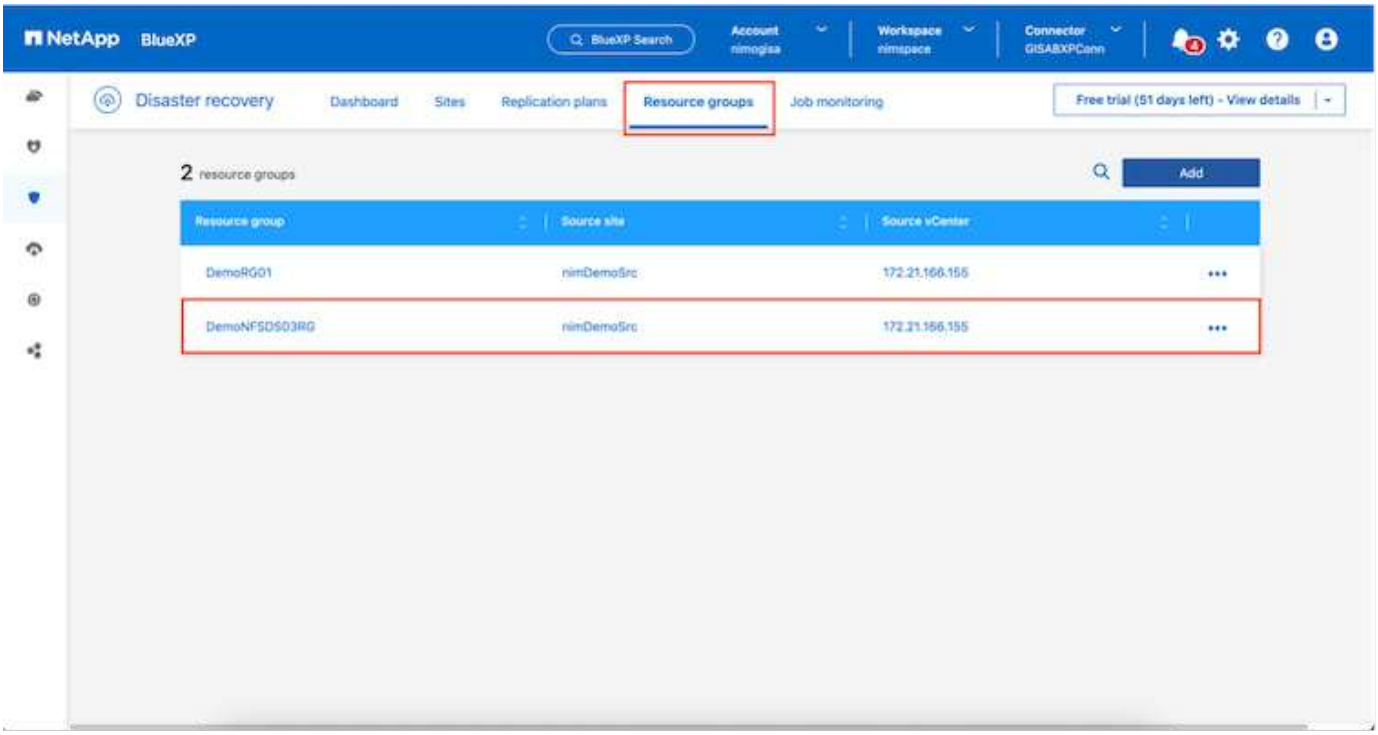
O que a BlueXP disaster recovery pode fazer por você?

Depois que os sites de origem e destino são adicionados, a BlueXP disaster recovery executa a descoberta profunda automática e exibe as VMs junto com os metadados associados. A BlueXP disaster recovery também detecta automaticamente as redes e os grupos de portas usados pelas VMs e os preenche.



Depois que os sites forem adicionados, as VMs podem ser agrupadas em grupos de recursos. Os grupos de recursos de BlueXP disaster recovery permitem que você agrupe um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização e atrasos de inicialização que podem ser executados na recuperação. Para começar a criar grupos de recursos, navegue até **Grupos de recursos** e clique em **Criar novo grupo de recursos**.

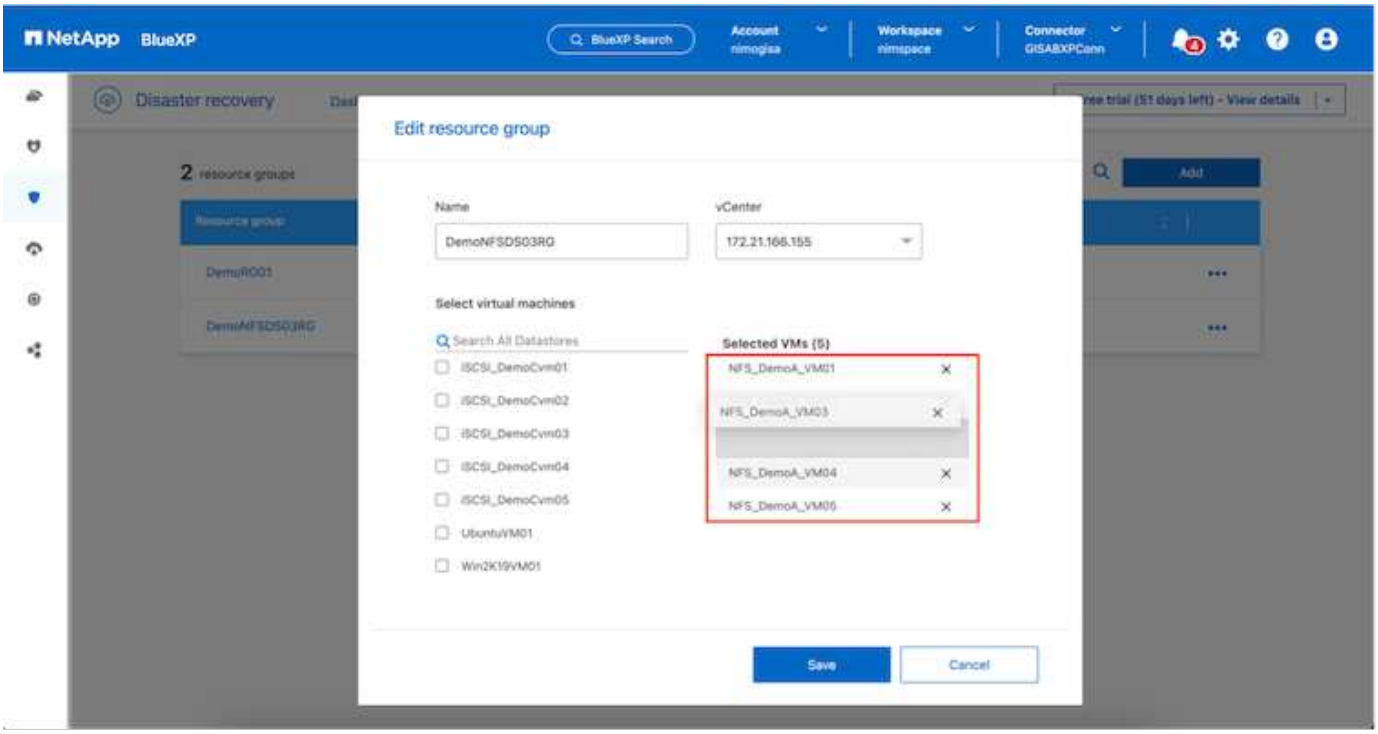




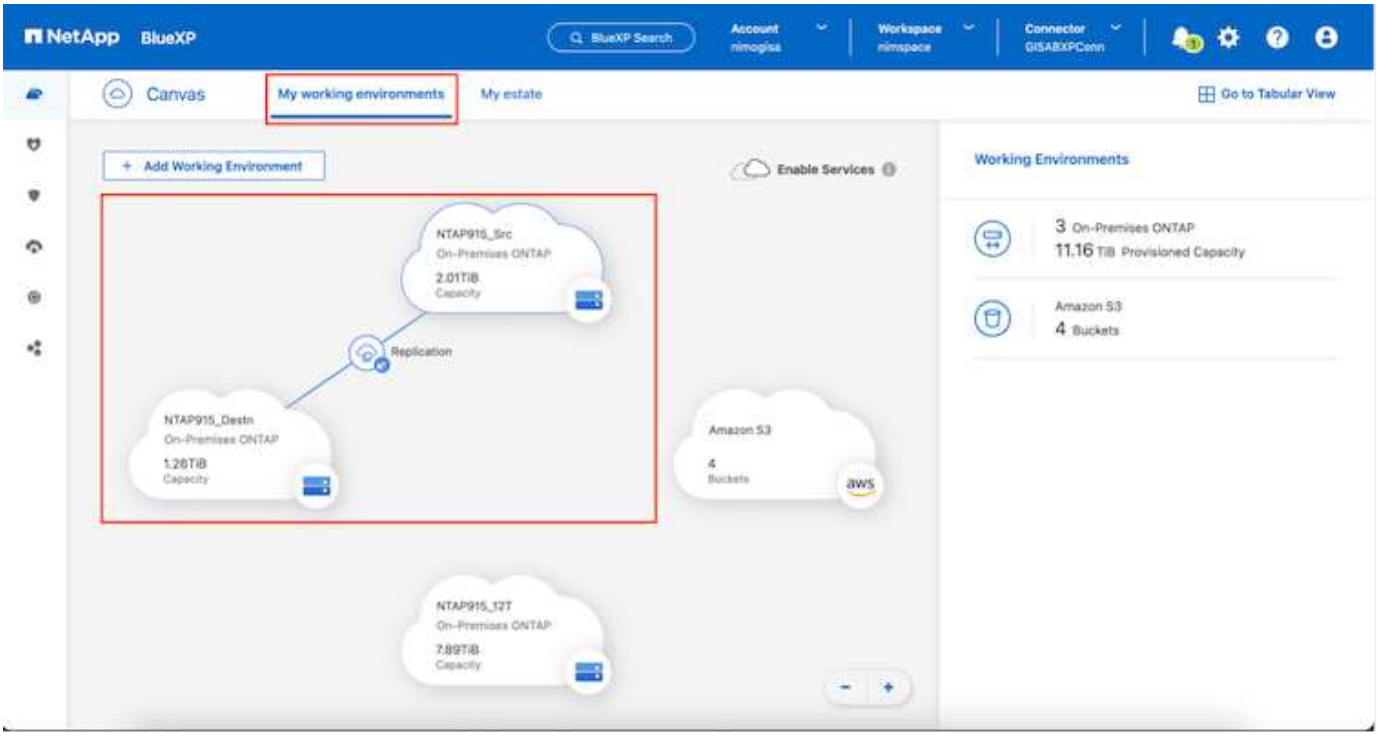
O grupo de recursos também pode ser criado durante a criação de um plano de replicação.

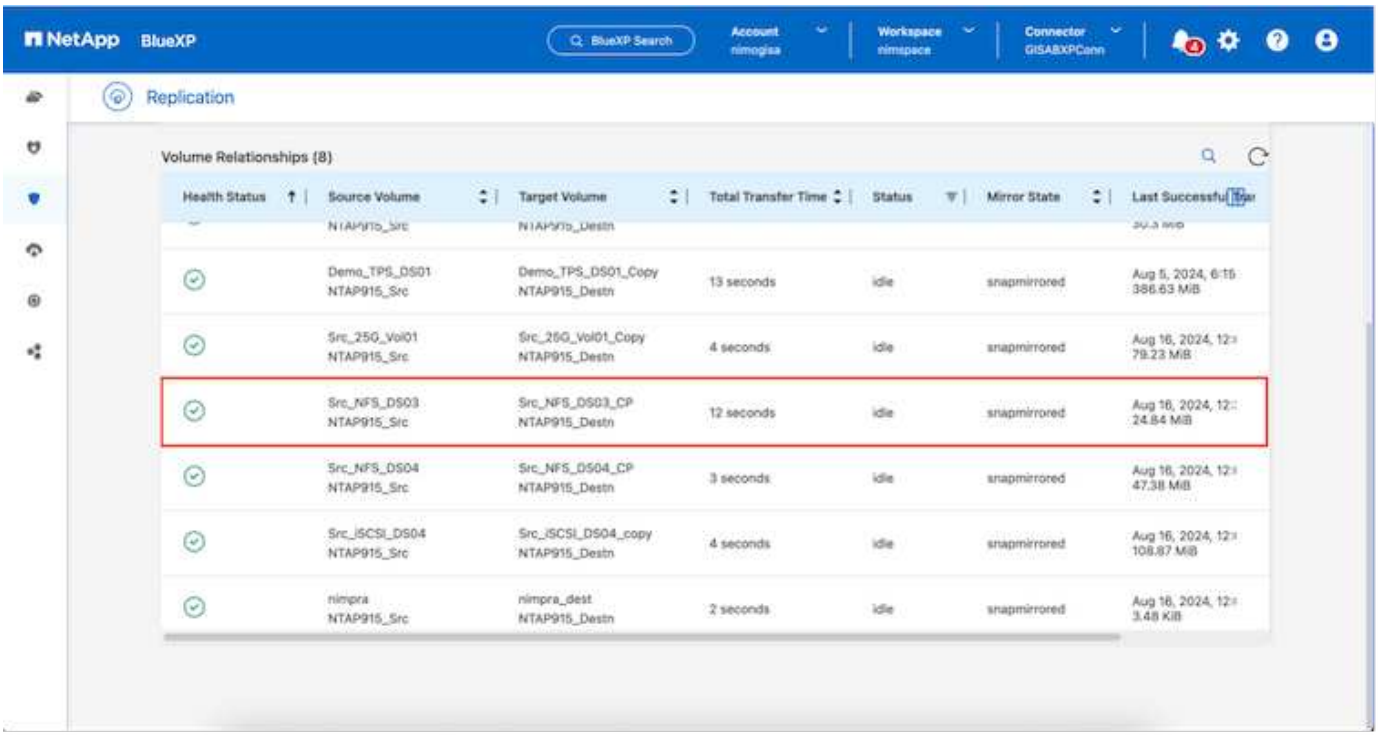
A ordem de inicialização das VMs pode ser definida ou modificada durante a criação de grupos de recursos

usando um mecanismo simples de arrastar e soltar.



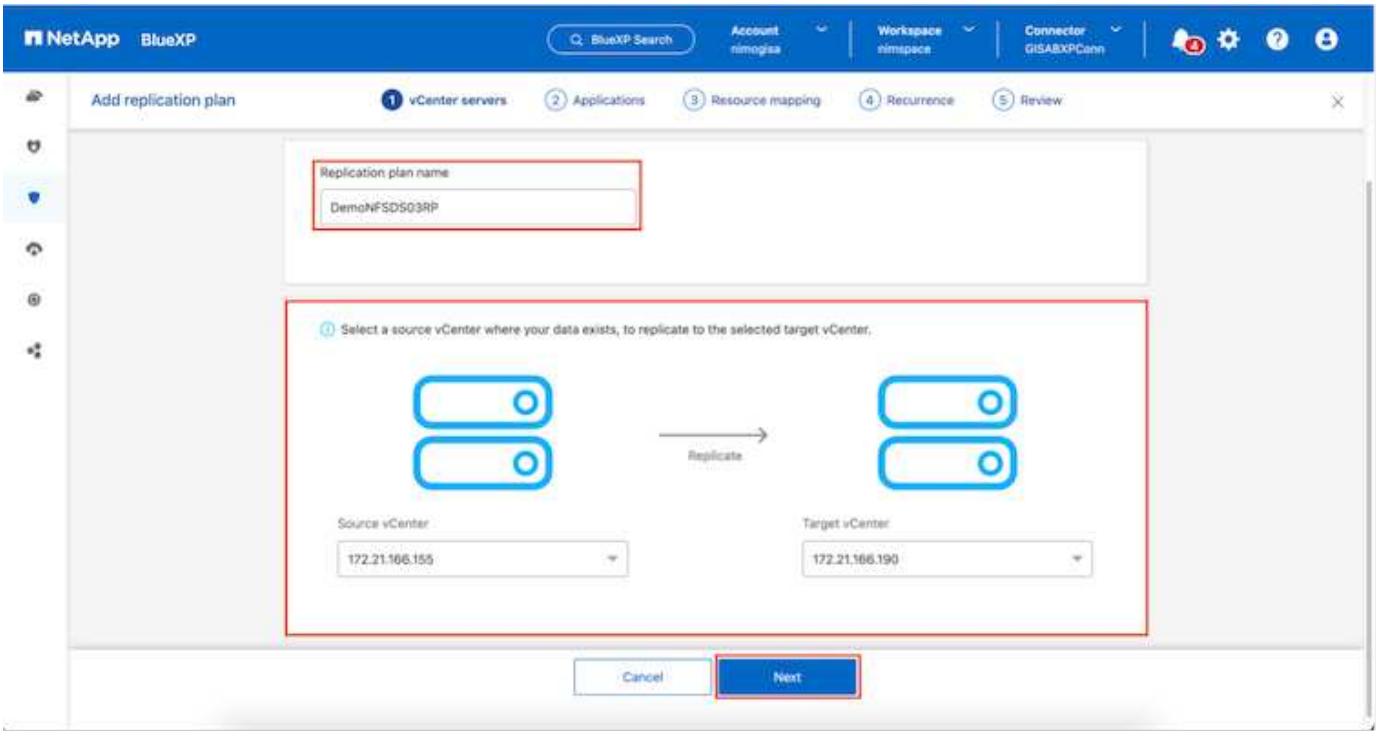
Depois que os grupos de recursos forem criados, a próxima etapa é criar o projeto de execução ou um plano para recuperar máquinas virtuais e aplicativos em caso de desastre. Conforme mencionado nos pré-requisitos, a replicação do SnapMirror pode ser configurada antecipadamente ou o DRaaS pode configurá-la usando o RPO e a contagem de retenção especificados durante a criação do plano de replicação.





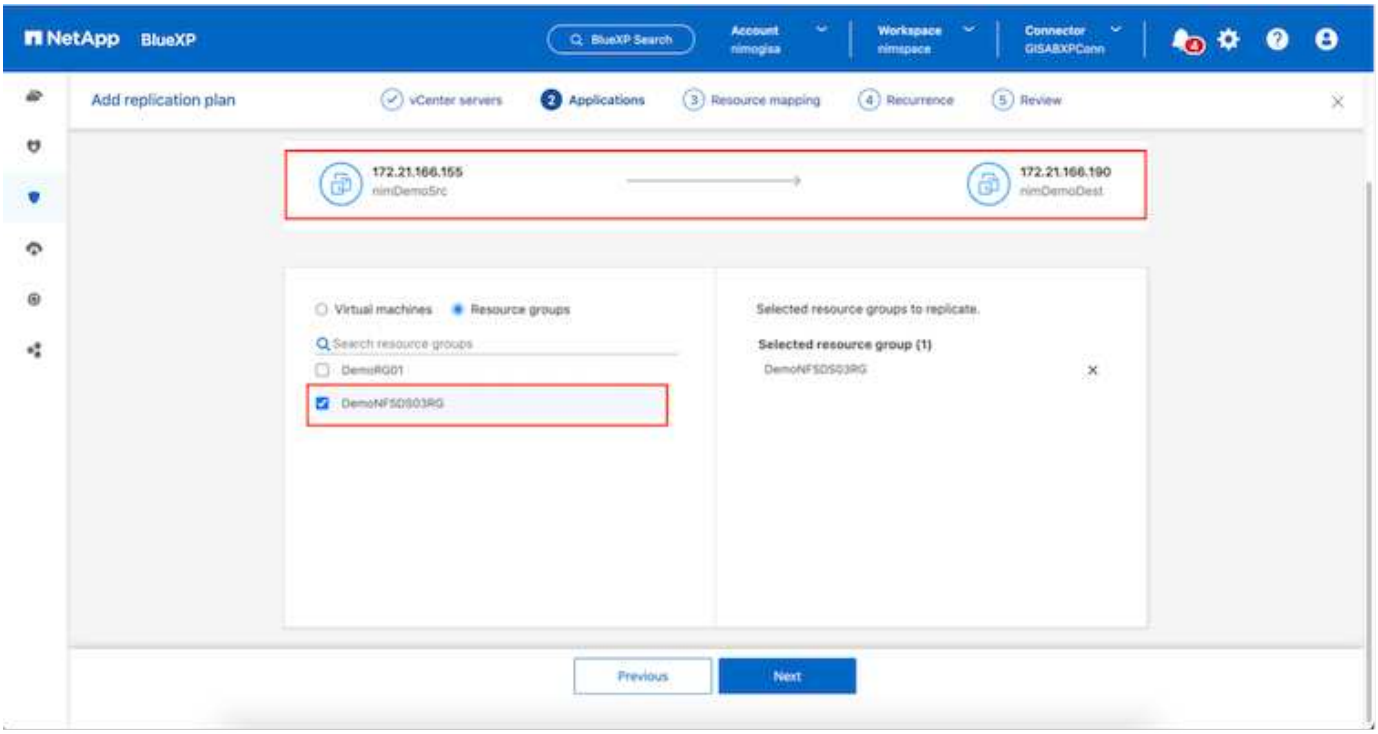
Configure o plano de replicação selecionando as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos no plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados e o mapeamento de clusters e redes. Para definir o plano de recuperação, navegue até a guia **Plano de Replicação** e clique em **Adicionar Plano**.

Primeiro, selecione o vCenter de origem e depois selecione o vCenter de destino.



O próximo passo é selecionar grupos de recursos existentes. Se nenhum grupo de recursos for criado, o assistente ajudará a agrupar as máquinas virtuais necessárias (basicamente, criar grupos de recursos funcionais) com base nos objetivos de recuperação. Isso também ajuda a definir a sequência de operação de

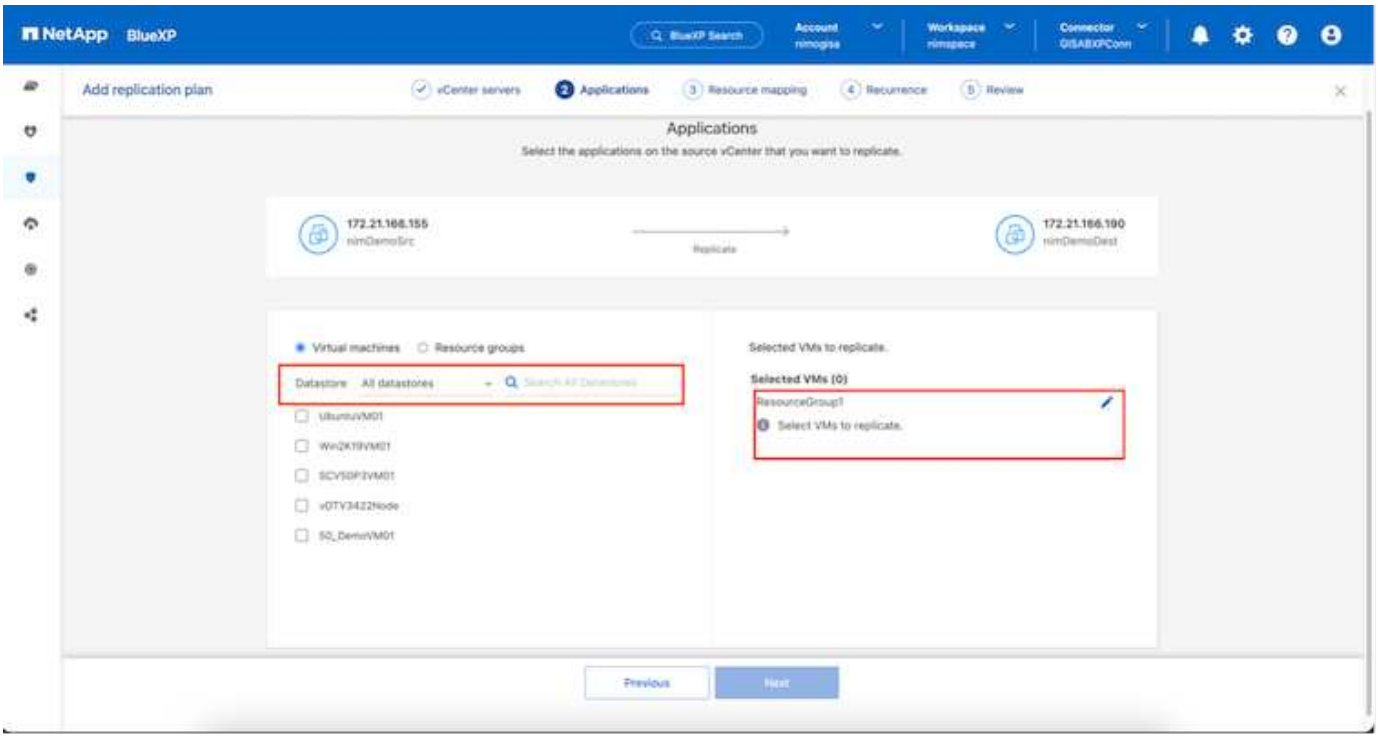
como as máquinas virtuais do aplicativo devem ser restauradas.



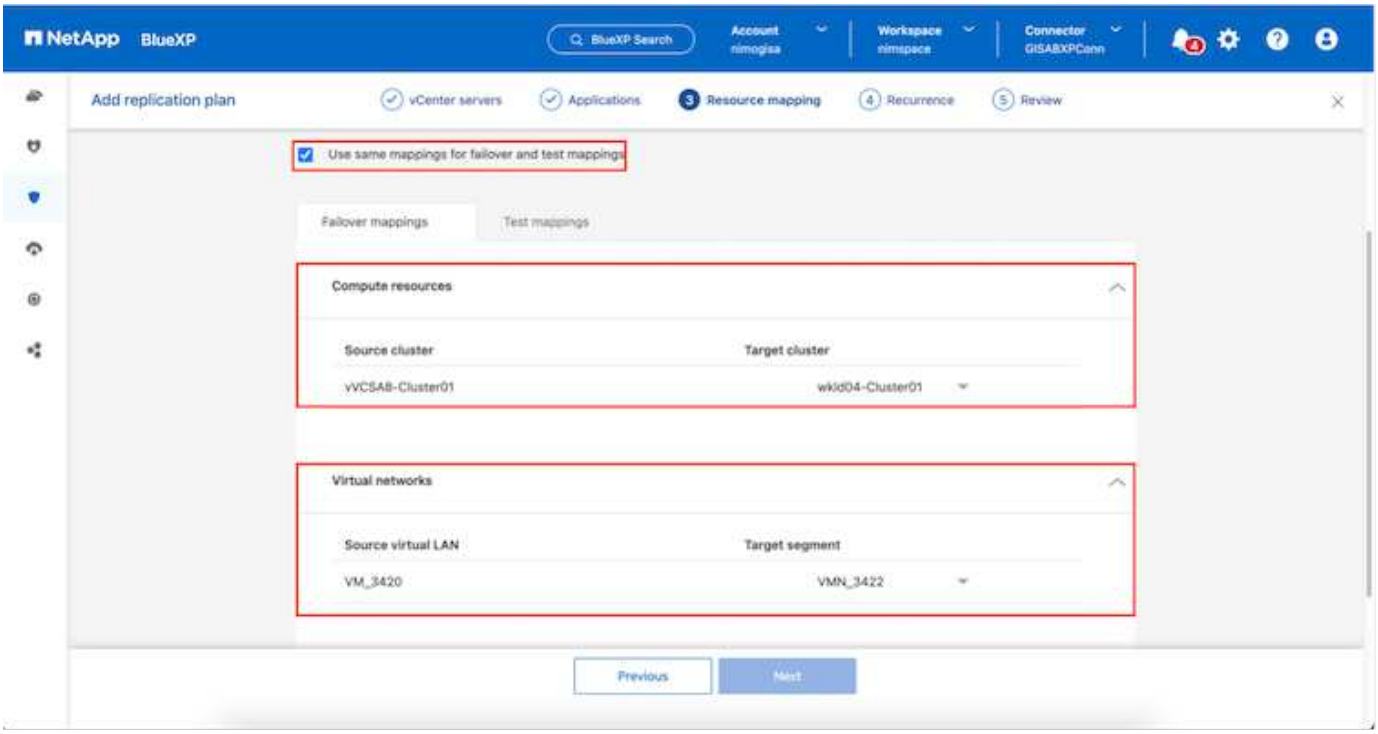
O grupo de recursos permite definir a ordem de inicialização usando a funcionalidade de arrastar e soltar. Ele pode ser usado para modificar facilmente a ordem em que as VMs serão ligadas durante o processo de recuperação.

Cada máquina virtual dentro de um grupo de recursos é iniciada em sequência com base na ordem. Dois grupos de recursos são iniciados em paralelo.

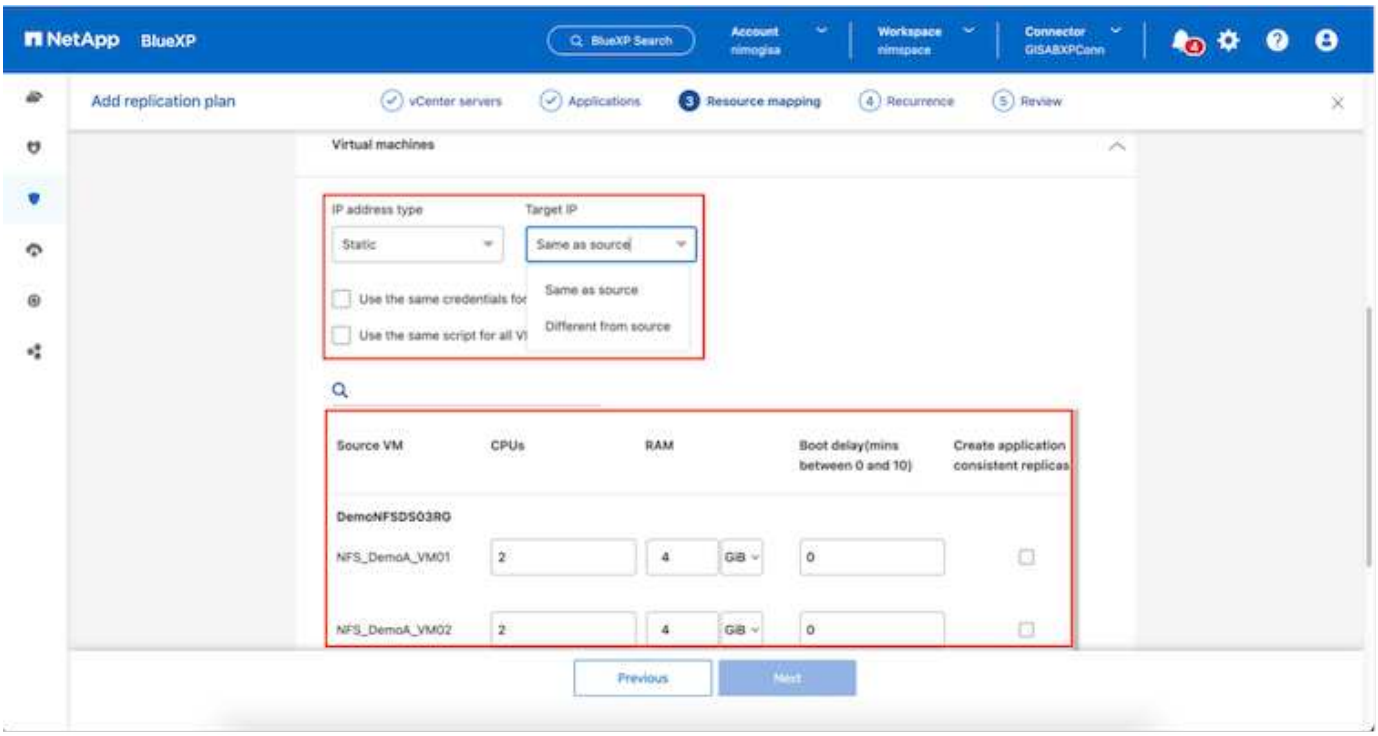
A captura de tela abaixo mostra a opção de filtrar máquinas virtuais ou armazenamentos de dados específicos com base em requisitos organizacionais, caso os grupos de recursos não sejam criados previamente.



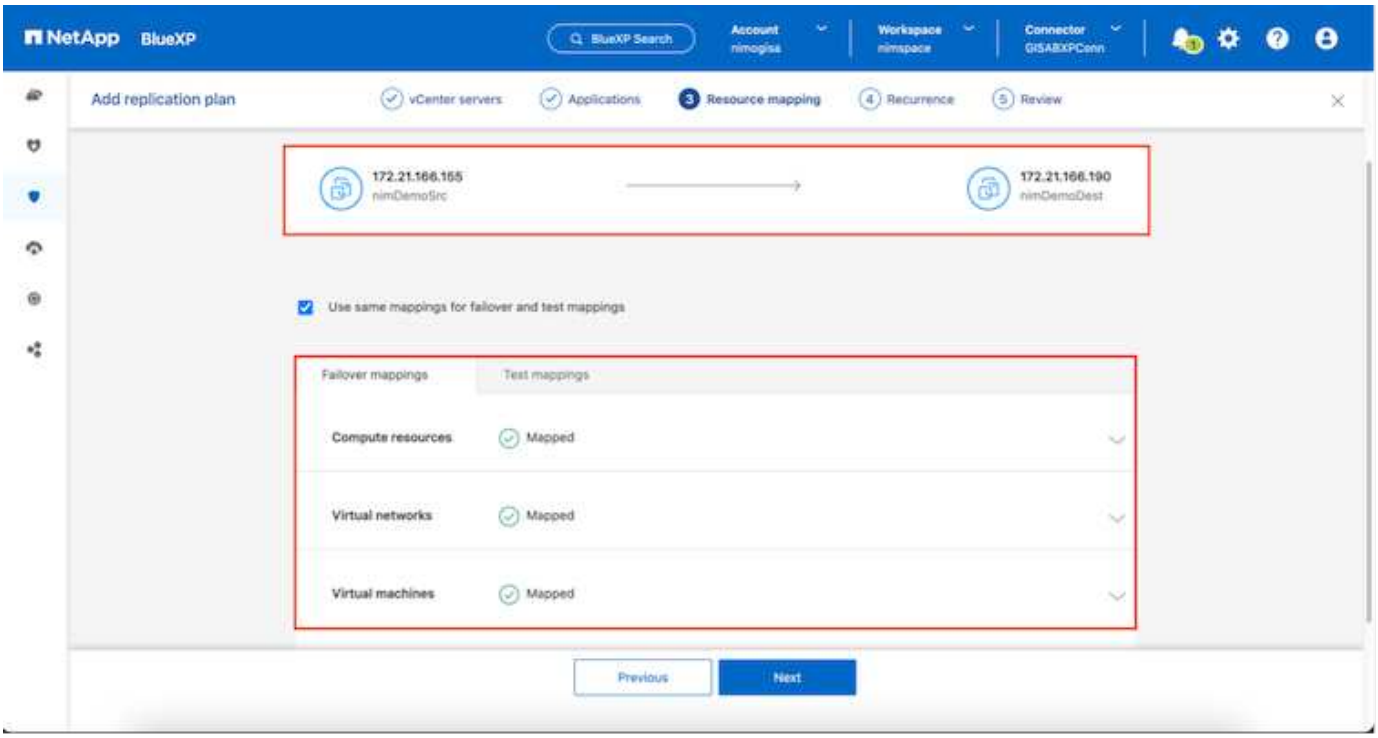
Depois que os grupos de recursos forem selecionados, crie os mapeamentos de failover. Nesta etapa, especifique como os recursos do ambiente de origem são mapeados para o destino. Isso inclui recursos de computação e redes virtuais. Personalização de IP, pré e pós-scripts, atrasos de inicialização, consistência de aplicativos e assim por diante. Para obter informações detalhadas, consulte"Crie um plano de replicação" .



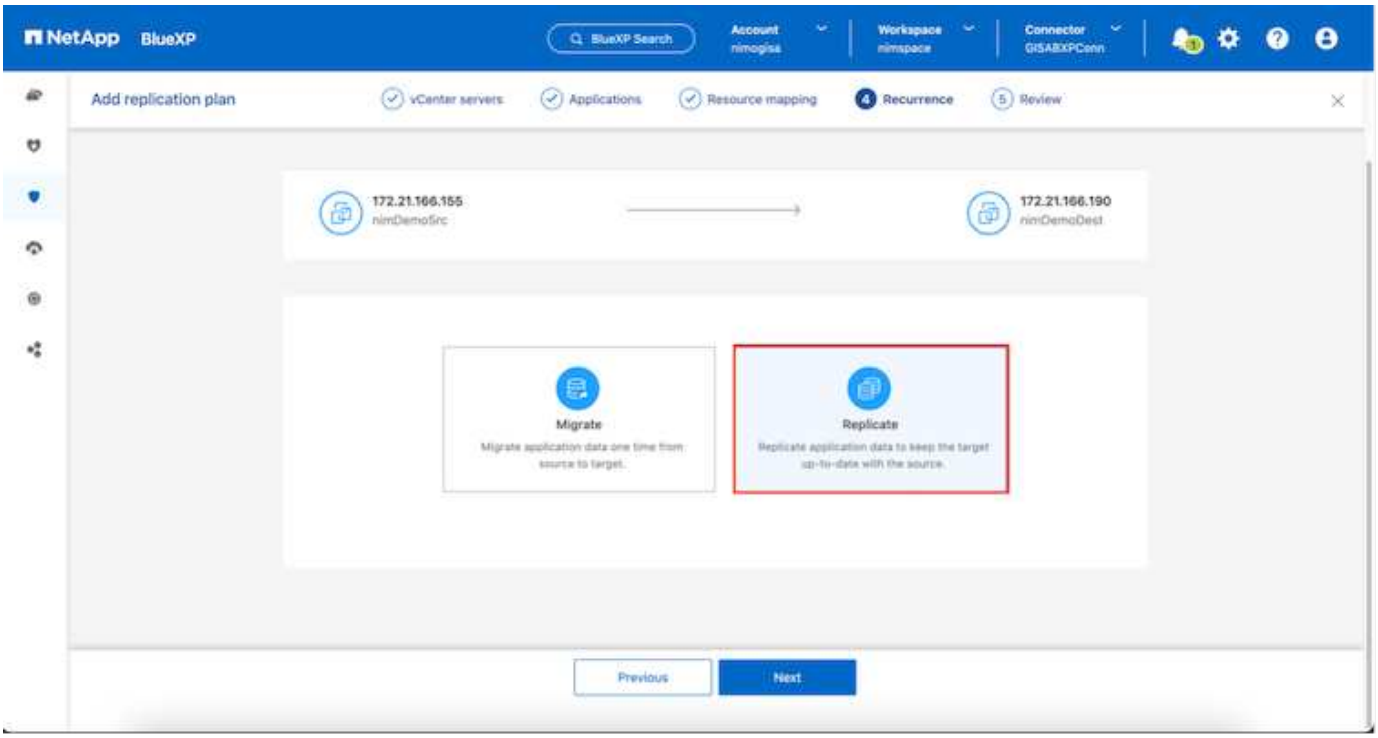
Por padrão, os mesmos parâmetros de mapeamento são usados para operações de teste e failover. Para definir mapeamentos diferentes para o ambiente de teste, selecione a opção Mapeamento de teste depois de desmarcar a caixa de seleção, conforme mostrado abaixo:



Quando o mapeamento de recursos estiver concluído, clique em Avançar.

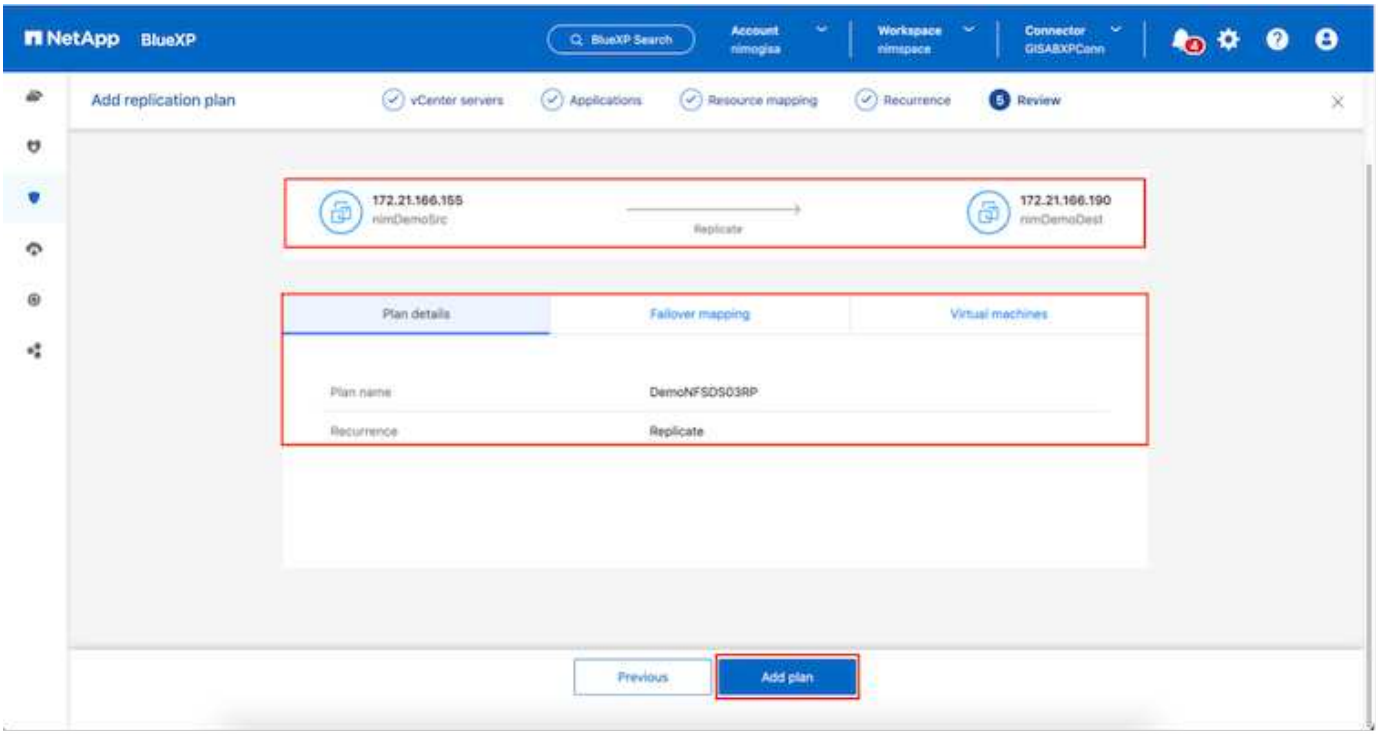


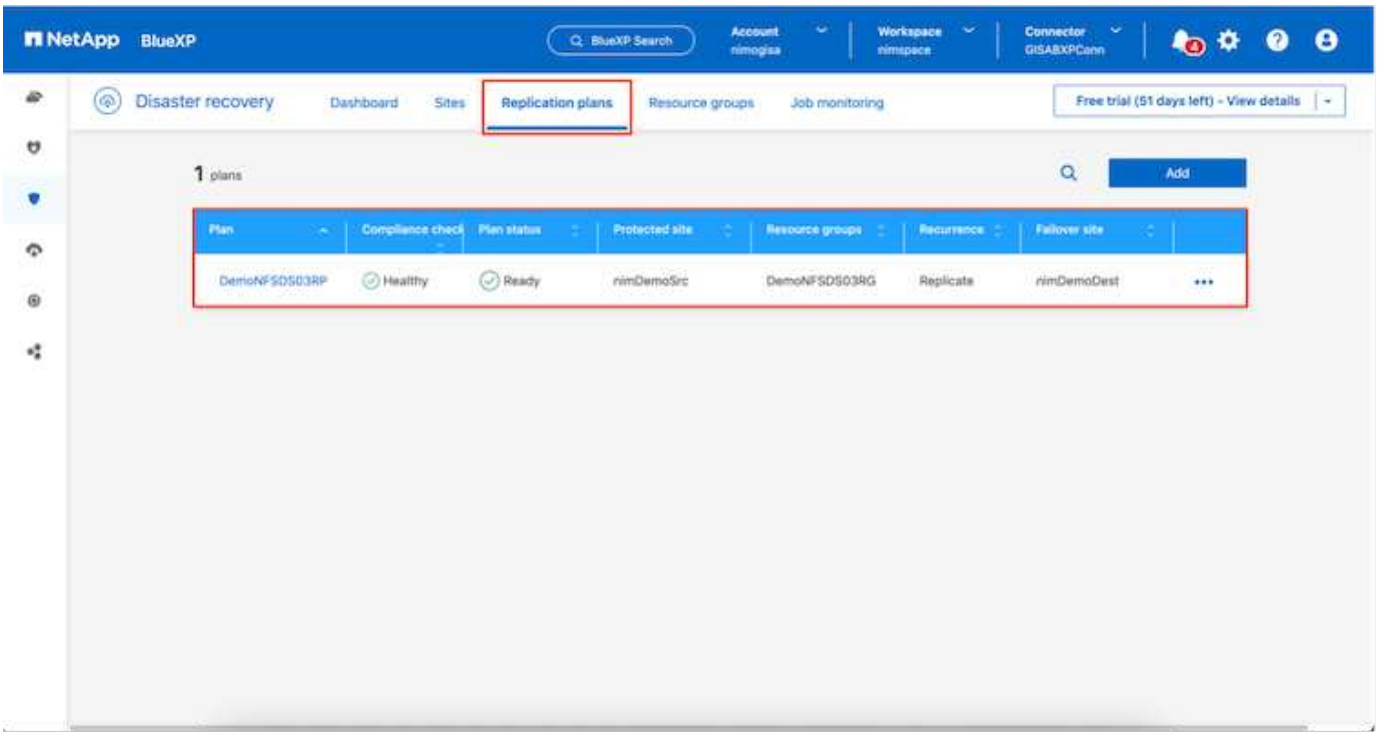
Selecione o tipo de recorrência. Em palavras simples, selecione Migrar (migração única usando failover) ou a opção de replicação contínua recorrente. Neste passo a passo, a opção Replicar está selecionada.



Uma vez concluído, revise os mapeamentos criados e clique em **Adicionar plano**.

> VMs de diferentes volumes e SVMs podem ser incluídas em um plano de replicação. Dependendo do posicionamento da VM (seja no mesmo volume ou em volumes separados dentro da mesma SVM, volumes separados em SVMs diferentes), a BlueXP disaster recovery cria um instantâneo de grupo de consistência.



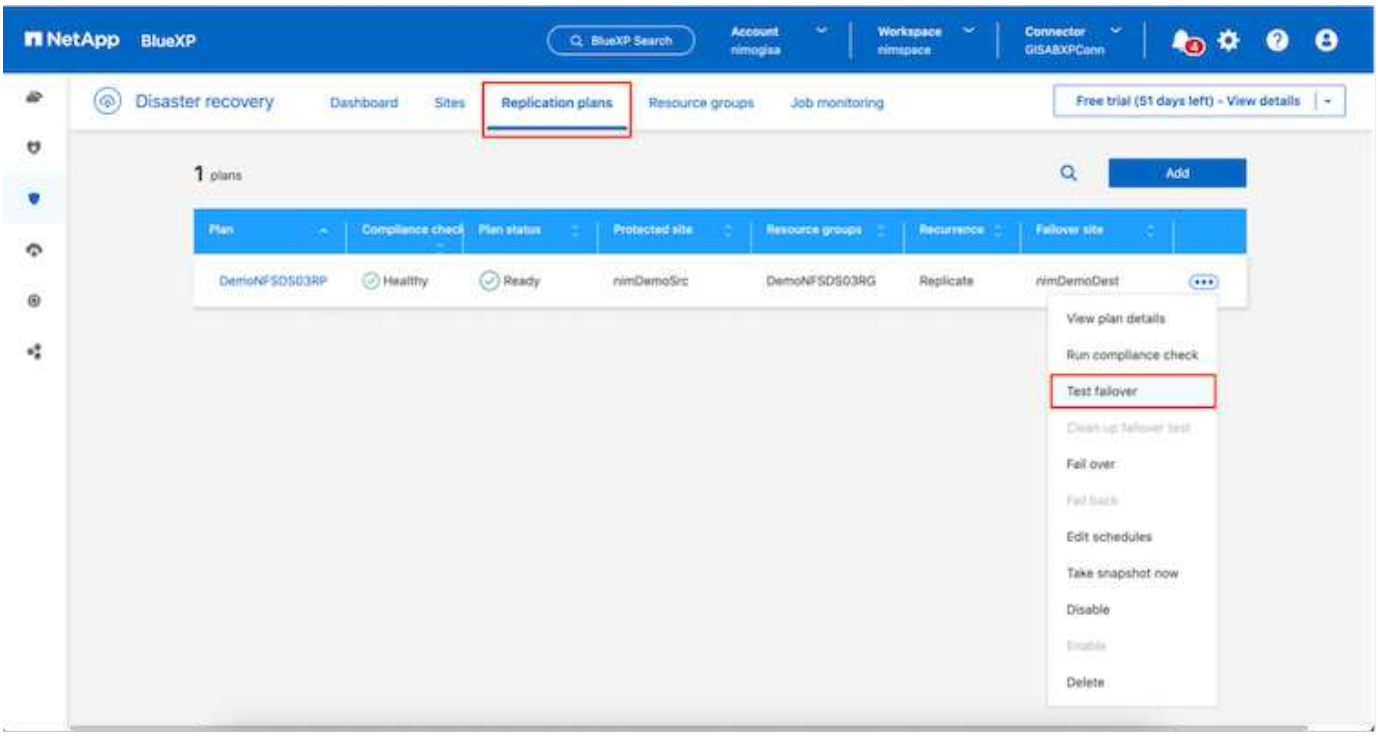


O BlueXP DRaaS consiste nos seguintes fluxos de trabalho:

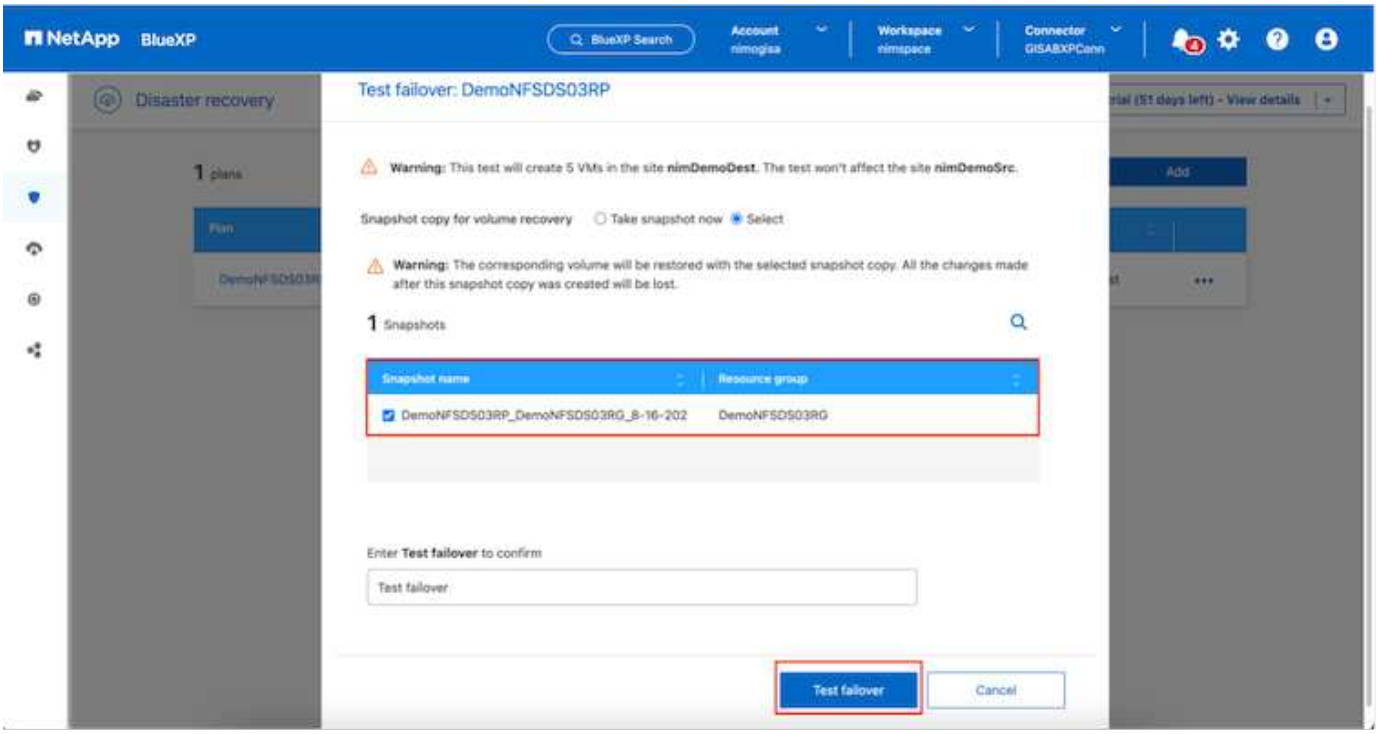
- Teste de failover (incluindo simulações automatizadas periódicas)
- Teste de failover de limpeza
- Failover
- Failback

Teste de failover

O failover de teste no BlueXP DRaaS é um procedimento operacional que permite que os administradores do VMware validem totalmente seus planos de recuperação sem interromper seus ambientes de produção.



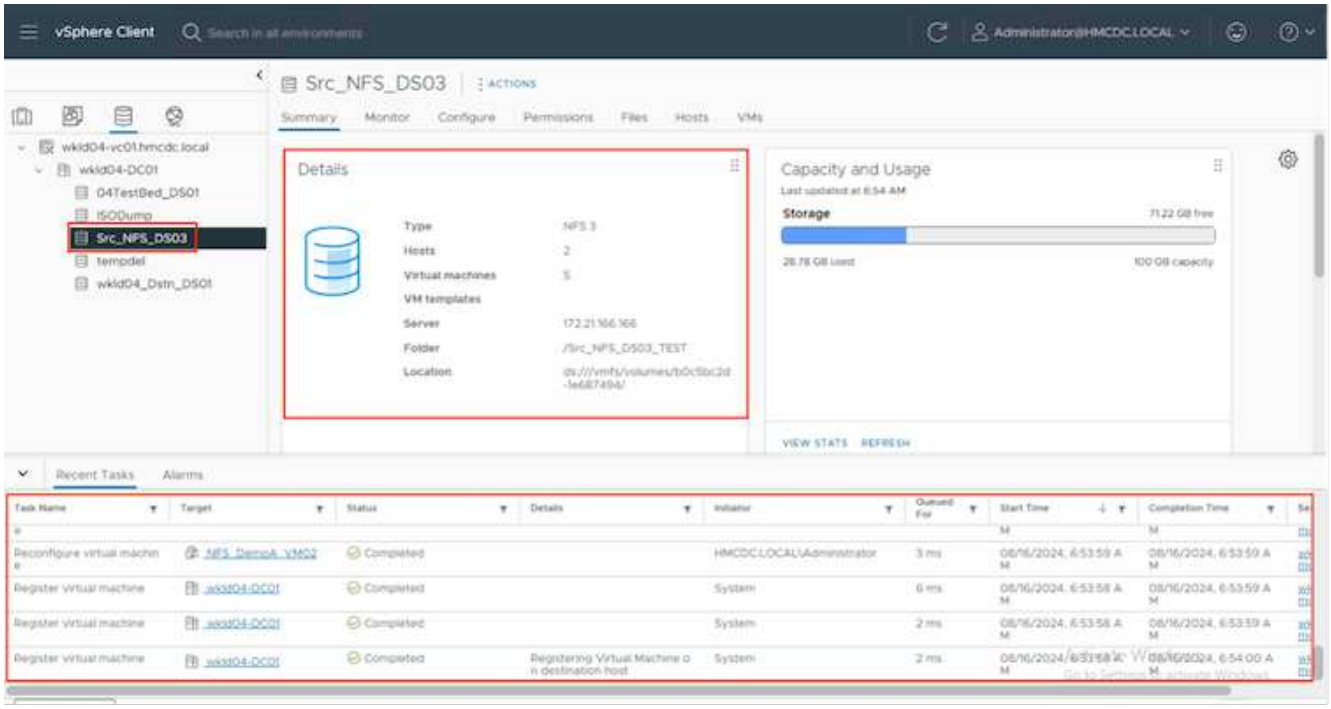
O BlueXP DRaaS incorpora a capacidade de selecionar o snapshot como um recurso opcional na operação de failover de teste. Esse recurso permite que o administrador do VMware verifique se quaisquer alterações feitas recentemente no ambiente são replicadas no site de destino e, portanto, estão presentes durante o teste. Essas mudanças incluem patches para o sistema operacional convidado da VM



Quando o administrador do VMware executa uma operação de failover de teste, o BlueXP DRaaS automatiza as seguintes tarefas:

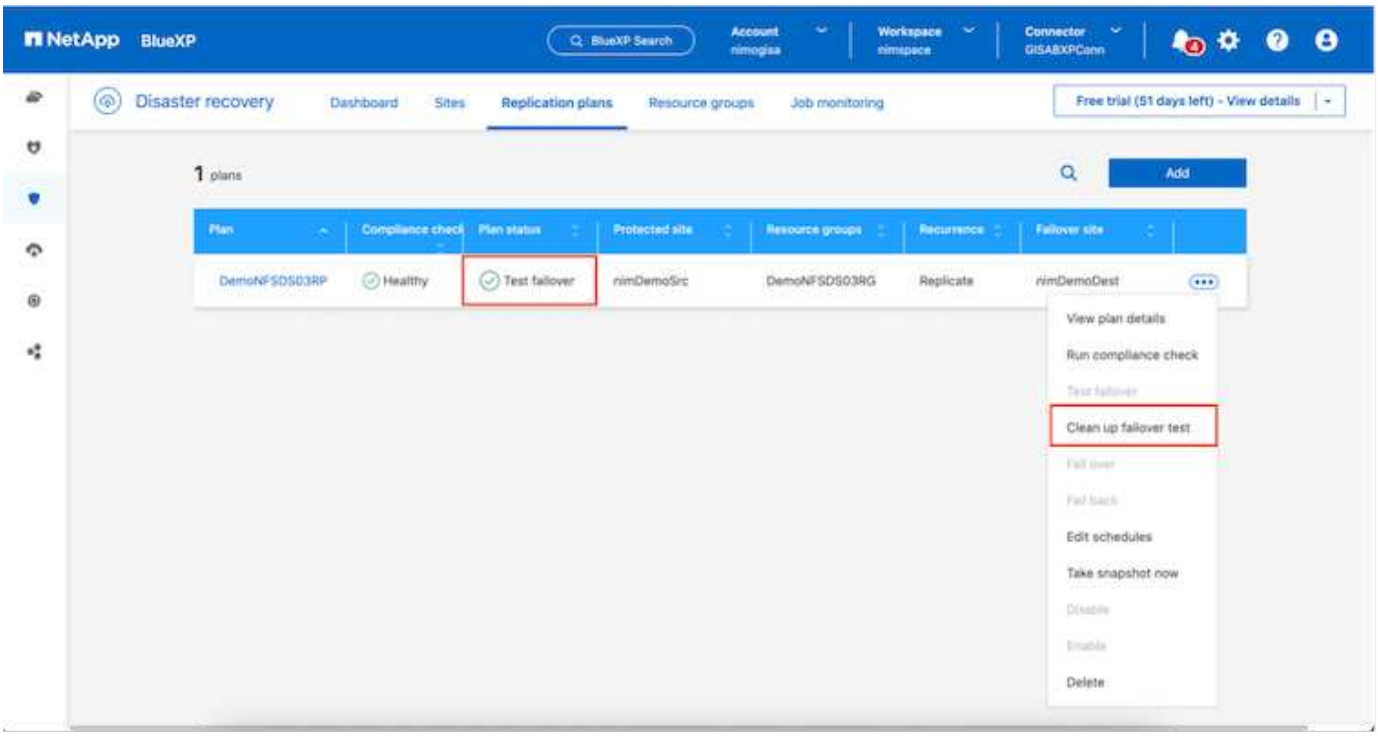
- Acionar relacionamentos do SnapMirror para atualizar o armazenamento no site de destino com quaisquer alterações recentes feitas no site de produção.

- Criação de volumes NetApp FlexClone dos volumes FlexVol no array de armazenamento DR.
- Conectando os datastores NFS nos volumes FlexClone aos hosts ESXi no site de DR.
- Conectando os adaptadores de rede da VM à rede de teste especificada durante o mapeamento.
- Reconfigurando as configurações de rede do sistema operacional convidado da VM, conforme definido para a rede no site de DR.
- Executar quaisquer comandos personalizados que tenham sido armazenados no plano de replicação.
- Ligar as VMs na ordem definida no plano de replicação.



Operação de teste de failover de limpeza

A operação de teste de failover de limpeza ocorre após a conclusão do teste do plano de replicação e o administrador do VMware responde ao prompt de limpeza.



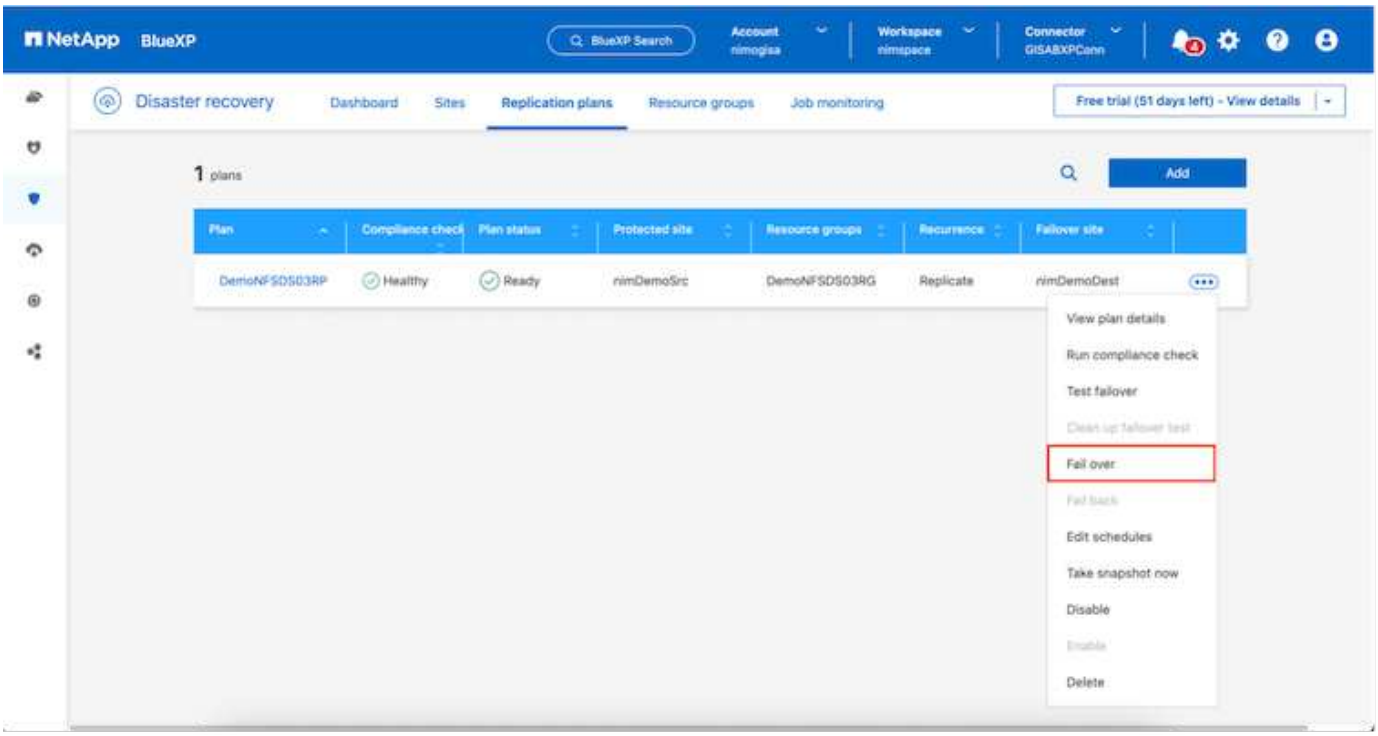
Esta ação redefinirá as máquinas virtuais (VMs) e o status do plano de replicação para o estado pronto.

Quando o administrador do VMware executa uma operação de recuperação, o BlueXP DRaaS conclui o seguinte processo:

1. Ele desliga cada VM recuperada na cópia do FlexClone que foi usada para teste.
2. Ele exclui o volume FlexClone que foi usado para apresentar as VMs recuperadas durante o teste.

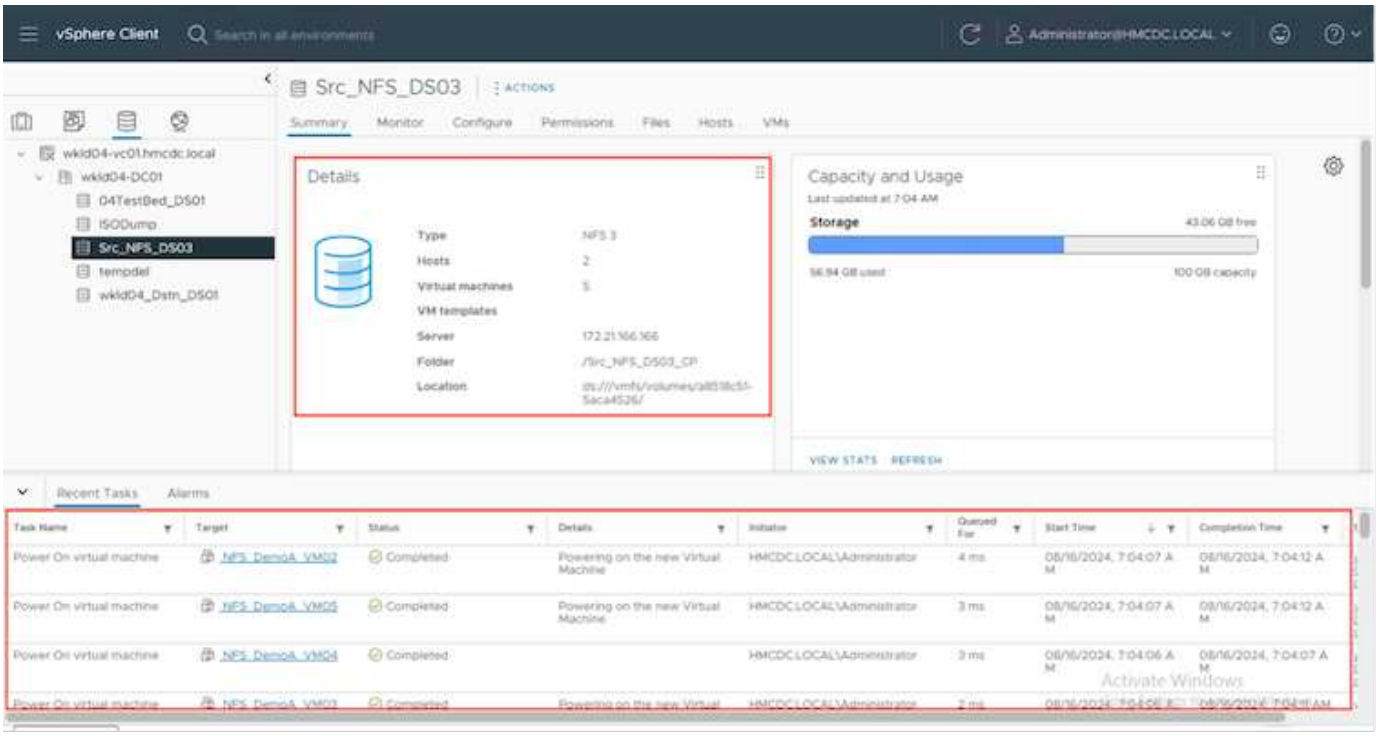
Migração planejada e failover

O BlueXP DRaaS tem dois métodos para executar um failover real: migração planejada e failover. O primeiro método, migração planejada, incorpora o desligamento da VM e a sincronização da replicação do armazenamento no processo para recuperar ou mover efetivamente as VMs para o site de destino. A migração planejada requer acesso ao site de origem. O segundo método, failover, é um failover planejado/não planejado no qual as VMs são recuperadas no site de destino a partir do último intervalo de replicação de armazenamento que foi concluído. Dependendo do RPO que foi projetado na solução, alguma perda de dados pode ser esperada no cenário de DR.



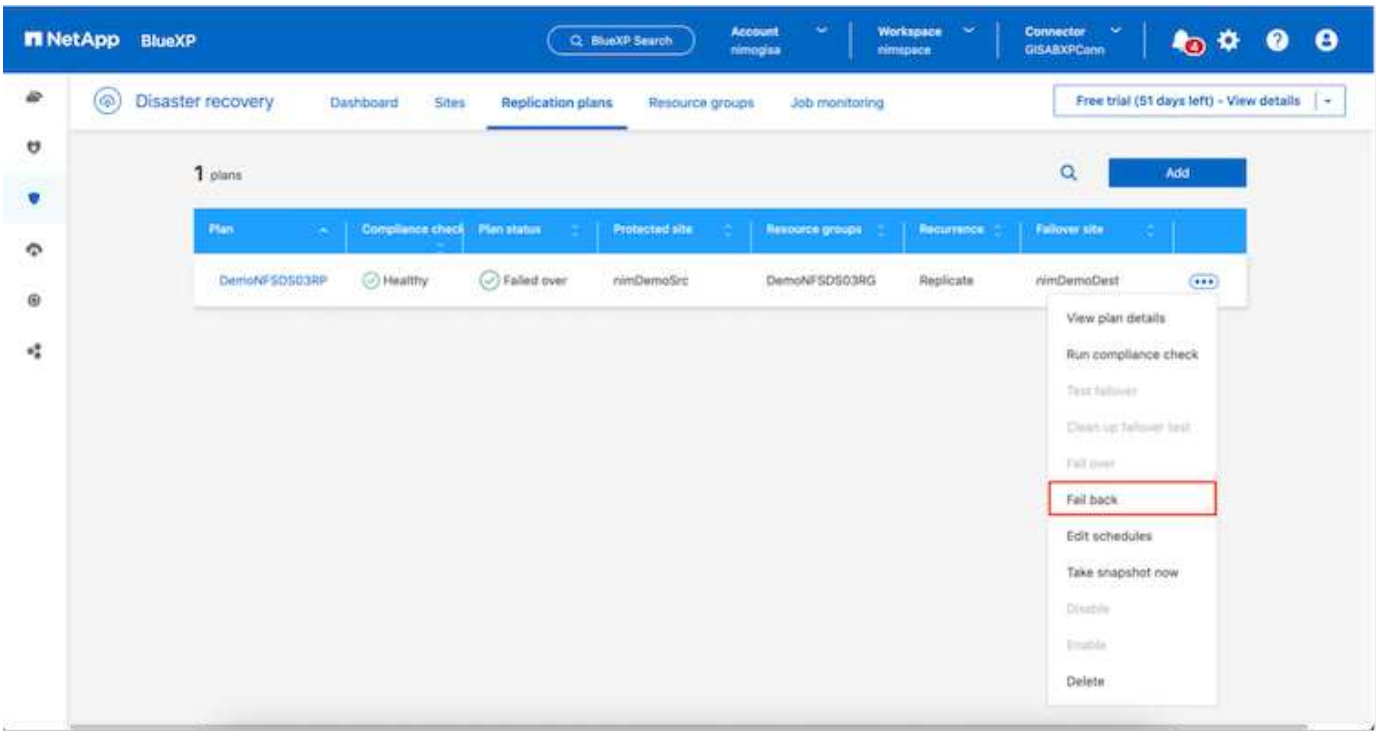
Quando o administrador do VMware executa uma operação de failover, o BlueXP DRaaS automatiza as seguintes tarefas:

- Interrompa e faça failover dos relacionamentos do NetApp SnapMirror .
- Conecte os datastores NFS replicados aos hosts ESXi no site de DR.
- Conecte os adaptadores de rede da VM à rede do site de destino apropriada.
- Reconfigure as configurações de rede do sistema operacional convidado da VM, conforme definido para a rede no site de destino.
- Execute quaisquer comandos personalizados (se houver) que tenham sido armazenados no plano de replicação.
- Ligue as VMs na ordem definida no plano de replicação.



Failback

Um failback é um procedimento opcional que restaura a configuração original dos sites de origem e destino após uma recuperação.



Os administradores do VMware podem configurar e executar um procedimento de failback quando estiverem prontos para restaurar serviços no site de origem original.

NOTA: O BlueXP DRaaS replica (ressincroniza) quaisquer alterações de volta para a máquina virtual de origem antes de reverter a direção da replicação. Esse processo começa com um relacionamento que

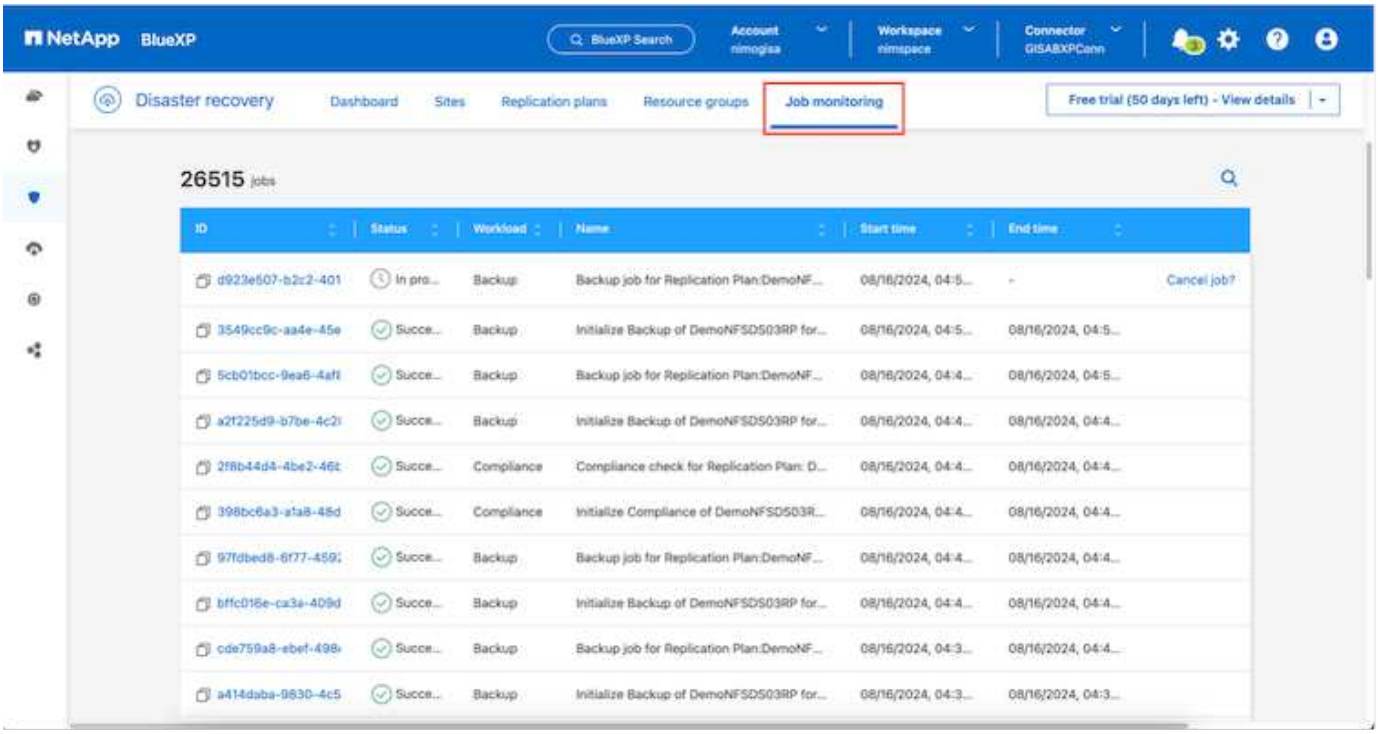
concluiu o failover para um alvo e envolve as seguintes etapas:

- Desligue e cancele o registro das máquinas virtuais e os volumes no site de destino serão desmontados.
- Interrompa o relacionamento SnapMirror na fonte original para torná-lo de leitura/gravação.
- Ressincronize o relacionamento do SnapMirror para reverter a replicação.
- Monte o volume na origem, ligue e registre as máquinas virtuais de origem.

Para obter mais detalhes sobre como acessar e configurar o BlueXP DRaaS, consulte o"Saiba mais sobre o BlueXP Disaster Recovery para VMware" .

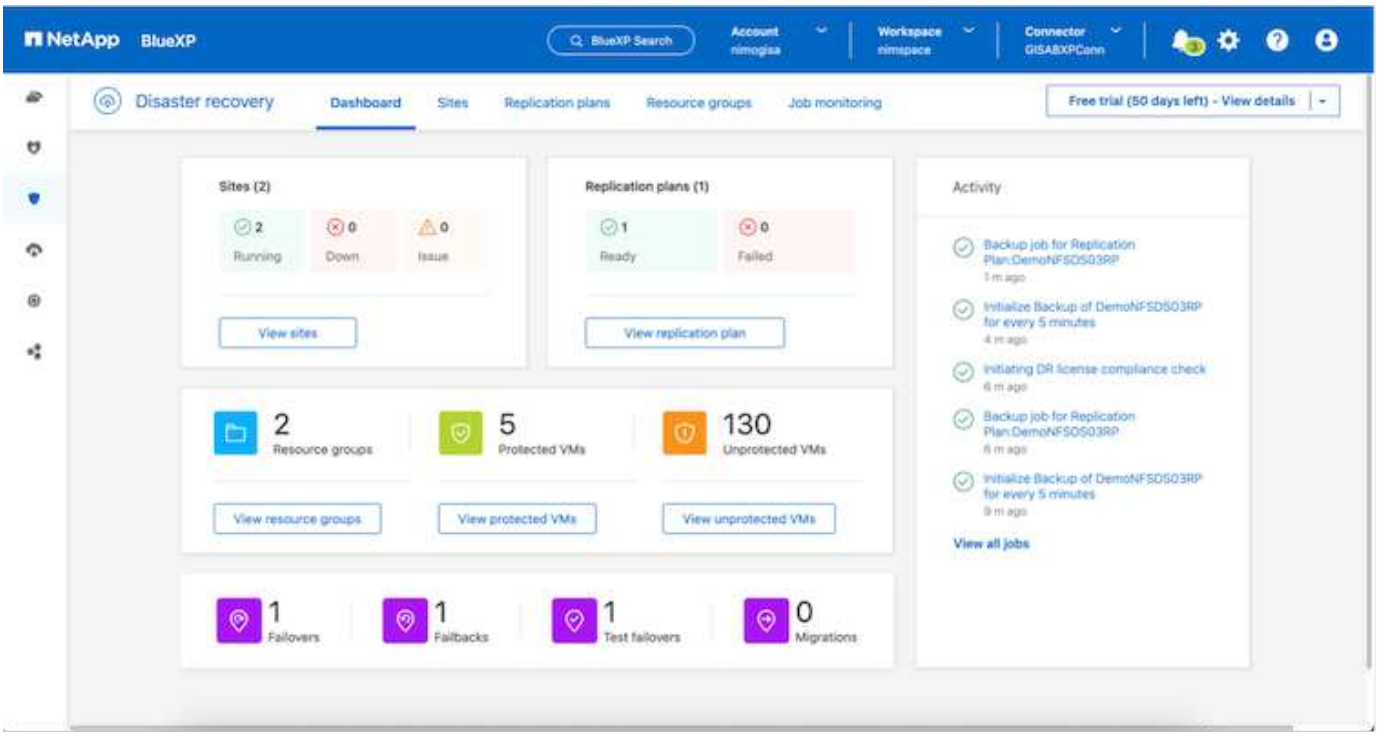
Monitoramento e Painel

No BlueXP ou no ONTAP CLI, você pode monitorar o status de integridade da replicação para os volumes de armazenamento de dados apropriados, e o status de um failover ou failover de teste pode ser rastreado por meio do Monitoramento de tarefas.



Se um trabalho estiver em andamento ou na fila e você desejar interrompê-lo, há uma opção para cancelá-lo.

Com o painel de BlueXP disaster recovery , avalie com confiança o status dos sites de recuperação de desastres e dos planos de replicação. Isso permite que os administradores identifiquem rapidamente sites e planos saudáveis, desconectados ou degradados.



Isso fornece uma solução poderosa para lidar com um plano de recuperação de desastres personalizado e personalizado. O failover pode ser feito como failover planejado ou failover com o clique de um botão quando ocorre um desastre e é tomada a decisão de ativar o site de DR.

Para saber mais sobre esse processo, fique à vontade para seguir o vídeo passo a passo detalhado ou usar o"simulador de soluções" .

Proteja as cargas de trabalho com o vSphere Metro Storage Cluster

Saiba mais sobre a integração de alta disponibilidade do ONTAP com o VMware vSphere Metro Storage Cluster (vMSC)

Saiba mais sobre as soluções NetApp que você pode usar para integrar a alta disponibilidade do NetApp ONTAP com o VMware vSphere Metro Storage Cluster (vMSC). Isso fornece soluções robustas para o gerenciamento do VMware Cloud Foundation (VCF) e domínios de carga de trabalho do VI.

Essa combinação garante disponibilidade contínua de dados, failover perfeito e recuperação de desastres em locais geograficamente dispersos, aumentando a resiliência e a continuidade operacional para cargas de trabalho críticas. O SnapMirror Active Sync permite que os serviços empresariais continuem operando mesmo durante uma falha completa do site, permitindo que os aplicativos executem failover de forma transparente usando uma cópia secundária. Com a sincronização ativa do SnapMirror , não é necessária intervenção manual ou script personalizado para acionar um failover.

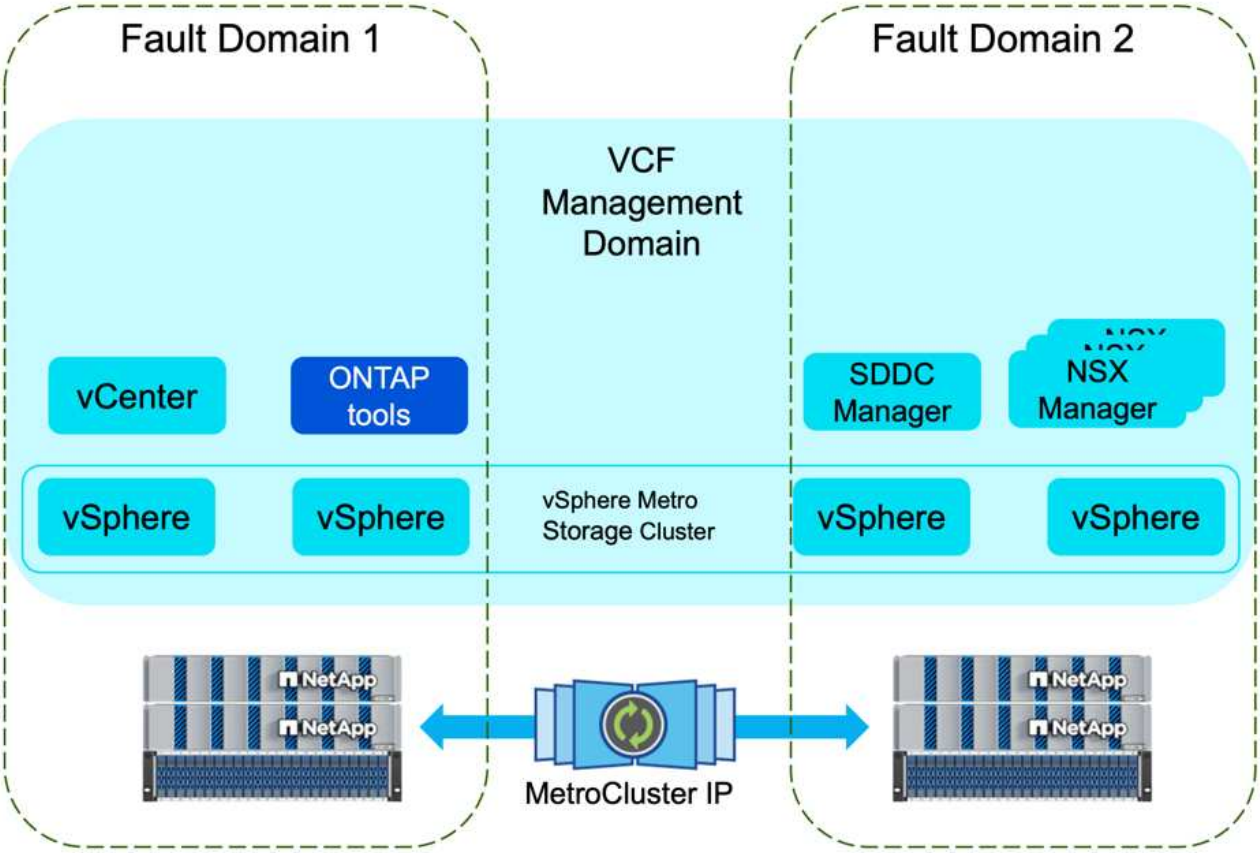
Consulte as soluções a seguir para obter mais detalhes.

- "Stretch Cluster para domínio de gerenciamento usando sincronização ativa do SnapMirror"
- "Stretch Cluster para Domínio de Gerenciamento usando MetroCluster"

- "Stretch Cluster para VI Workload Domain usando sincronização ativa do SnapMirror"
- "Stretch Cluster para Domínio de Carga de Trabalho VI usando MetroCluster"

Configurar um cluster de extensão para um domínio de gerenciamento VCF usando o MetroCluster

Neste caso de uso, descrevemos o procedimento para configurar um cluster estendido para o domínio de gerenciamento do VMware Cloud Foundation (VCF) usando o ONTAP MetroCluster com NFS como o armazenamento de dados primário. Este procedimento inclui a implantação de hosts vSphere e vCenter Server, o provisionamento de datastores NFS, a validação do cluster com a VCF Import Tool, a configuração das definições do NSX e a conversão do ambiente em um domínio de gerenciamento VCF.



Introdução

Nesta solução, demonstraremos como implementar o Domínio de Gerenciamento VCF Esticado com NFS como Datastore Principal usando o ONTAP MetroCluster.

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Implante hosts vSphere e o servidor vCenter.
- Provisione o armazenamento de dados NFS para hosts vSphere.

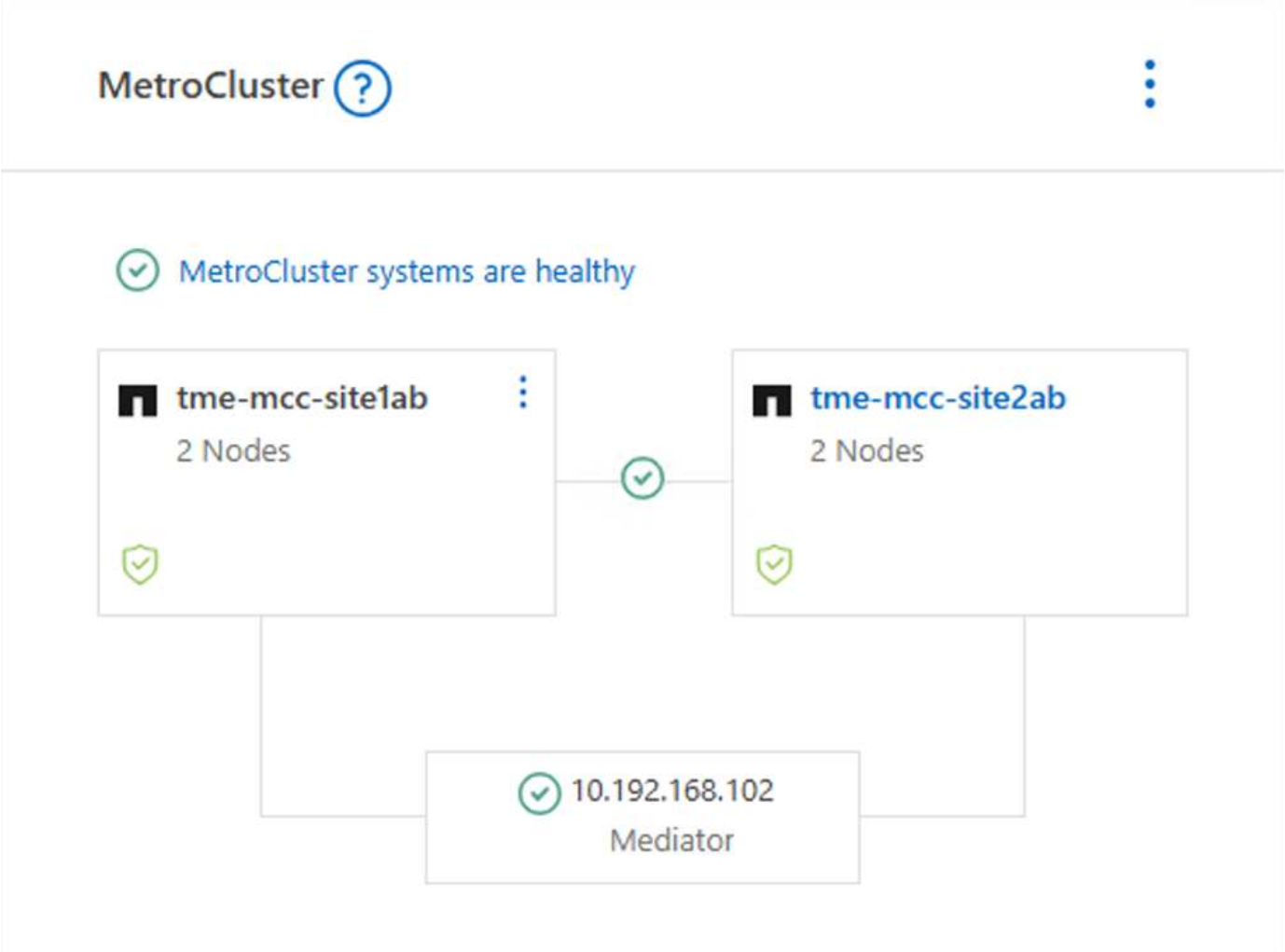
- Implante o SDDC Manager no cluster vSphere.
- Use a Ferramenta de Importação VCF para validar o cluster vSphere.
- Configure um arquivo JSON para criar um NSX durante a conversão de VCF.
- Use a Ferramenta de Importação VCF para converter o ambiente do vSphere 8 em domínio de gerenciamento VCF.

Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Configuração ONTAP MetroCluster suportada
- Máquina virtual de armazenamento (SVM) configurada para permitir tráfego NFS.
- A interface lógica (LIF) foi criada na rede IP que transportará o tráfego NFS e está associada ao SVM.
- Um cluster vSphere 8 com 4 hosts ESXi conectados ao switch de rede.
- Baixe o software necessário para a conversão de VCF.

Aqui está a captura de tela de exemplo do System Manager mostrando a configuração do MetroCluster
.



e aqui estão as interfaces de rede SVM de ambos os domínios de falha.

Network interfaces Subnets

+ Add

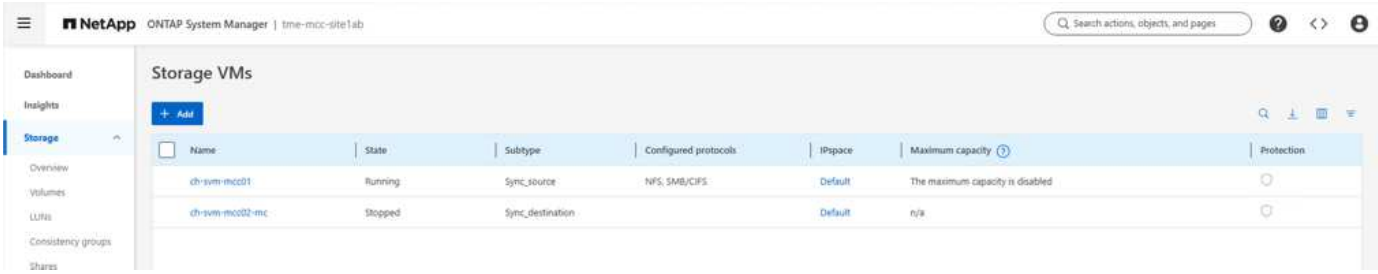
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

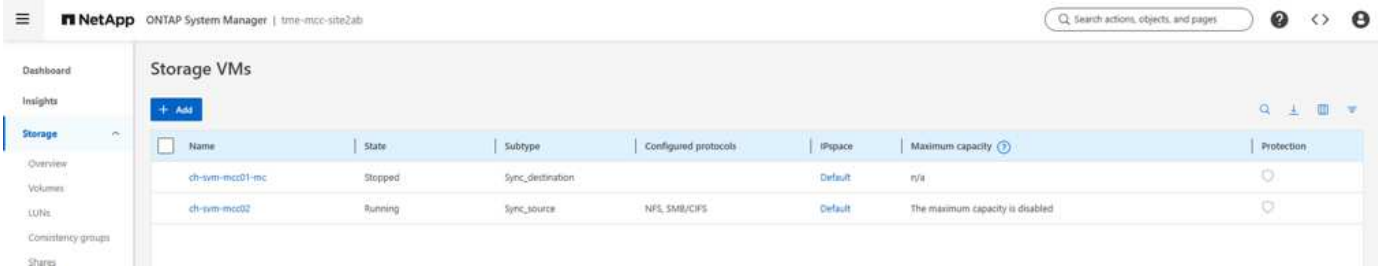
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] O SVM estará ativo em um dos domínios de falha no MetroCluster.





Referir "vMSC com MetroCluster" .

Para armazenamento suportado e outras considerações para conversão ou importação do vSphere para VCF 5.2, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

Antes de criar o vSphere Cluster que será convertido em VCF Management Domain, consulte "Consideração do NSX no vSphere Cluster"

Para o software necessário, consulte "Baixe o software para converter ou importar ambientes vSphere existentes" .

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Etapas de implantação

Para implantar o VCF Stretched Management Domain com NFS como armazenamento de dados principal,

Conclua as seguintes etapas:

- Implante hosts vSphere e vCenter.
- Crie um cluster do vSphere.
- Provisionar armazenamento de dados NFS.
- Copie a ferramenta de importação VCF para o dispositivo vCenter.
- Execute uma pré-verificação no dispositivo vCenter usando a Ferramenta de Importação VCF.
- Implante a VM do gerenciador do SDDC no cluster do vCenter.
- Crie um arquivo JSON para um cluster NSX a ser implantado durante o processo de conversão.
- Carregue o software necessário para o gerenciador do SDDC.
- Converta o cluster vSphere em VCF Management Domain.

Para uma visão geral do processo de conversão, consulte "Converter um ambiente vSphere em um domínio de gerenciamento ou importar um ambiente vSphere como um domínio de carga de trabalho VI no VMware Cloud Foundation" .

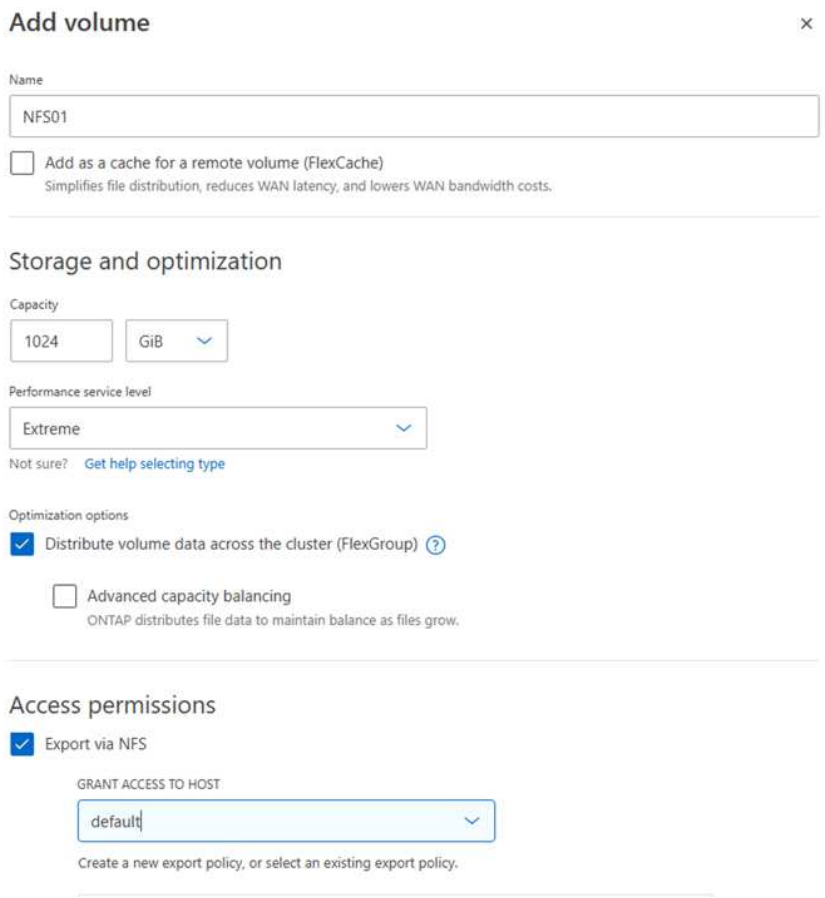
Implantar hosts vSphere e vCenter

Implante o vSphere em hosts usando o ISO baixado do portal de suporte da Broadcom ou use a opção de implantação existente para o host vSphere.

Monte o NFS Datastore para hospedar VMs

Nesta etapa, criamos o volume NFS e o montamos como Datastore para hospedar VMs.

1. Usando o Gerenciador do Sistema, crie um volume e anexe-o à política de exportação que inclui a sub-rede IP do host
vSphere.



2. Conecte-se via SSH ao host vSphere e monte o NFS
Datastore.

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Not Supported
[root@SiteA-vs01:~]
```

3. Repita as etapas acima para necessidades adicionais de armazenamento de dados e certifique-se de que a aceleração de hardware seja
suportada.

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS02        10.192.164.230  /NFS02  None          true     true            4      false  false  Supported
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Supported
[root@MCCA01:~]
```

Implante o vCenter no NFS Datastore. Certifique-se de que o SSH e o shell Bash estejam habilitados no dispositivo vCenter.

Criar cluster vSphere

1. Efetue login no cliente web do vSphere, crie o DataCenter e o Cluster do vSphere adicionando um dos hosts onde o NFS VAAI está implantado. Optamos por gerenciar todos os hosts no cluster com a opção de imagem única. [DICA] Não selecione Gerenciar configuração no nível do cluster. Para obter detalhes adicionais, consulte "Consideração do NSX no vSphere Cluster" . Para melhores práticas de vMSC com ONTAP MetroCluster, verifique "Diretrizes de design e implementação do vMSC"
2. Adicione outros hosts vSphere ao cluster.
3. Crie um Distributed Switch e adicione os grupos de portas.
4. "Migre a rede do vSwitch padrão para o switch distribuído."

Converter ambiente vSphere para domínio de gerenciamento VCF

A seção a seguir aborda as etapas para implantar o gerenciador SDDC e converter o cluster vSphere 8 em um domínio de gerenciamento VCF 5.2. Quando apropriado, a documentação da VMware será consultada para obter detalhes adicionais.

A VCF Import Tool, da VMware by Broadcom, é um utilitário usado no dispositivo vCenter e no gerenciador SDDC para validar configurações e fornecer serviços de conversão e importação para ambientes vSphere e VCF.

Para obter mais informações, consulte "Opções e parâmetros da ferramenta de importação VCF" .

Ferramenta de importação de VCF para copiar e extrair

A Ferramenta de Importação de VCF é usada no dispositivo vCenter para validar se o cluster vSphere está em um estado íntegro para o processo de conversão ou importação de VCF.

Conclua as seguintes etapas:

1. Siga os passos em "Copie a ferramenta de importação VCF para o dispositivo vCenter de destino" no VMware Docs para copiar a Ferramenta de Importação VCF para o local correto.
2. Extraia o pacote usando o seguinte comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar o dispositivo vCenter

Use a ferramenta de importação VCF para validar o dispositivo vCenter antes da conversão.

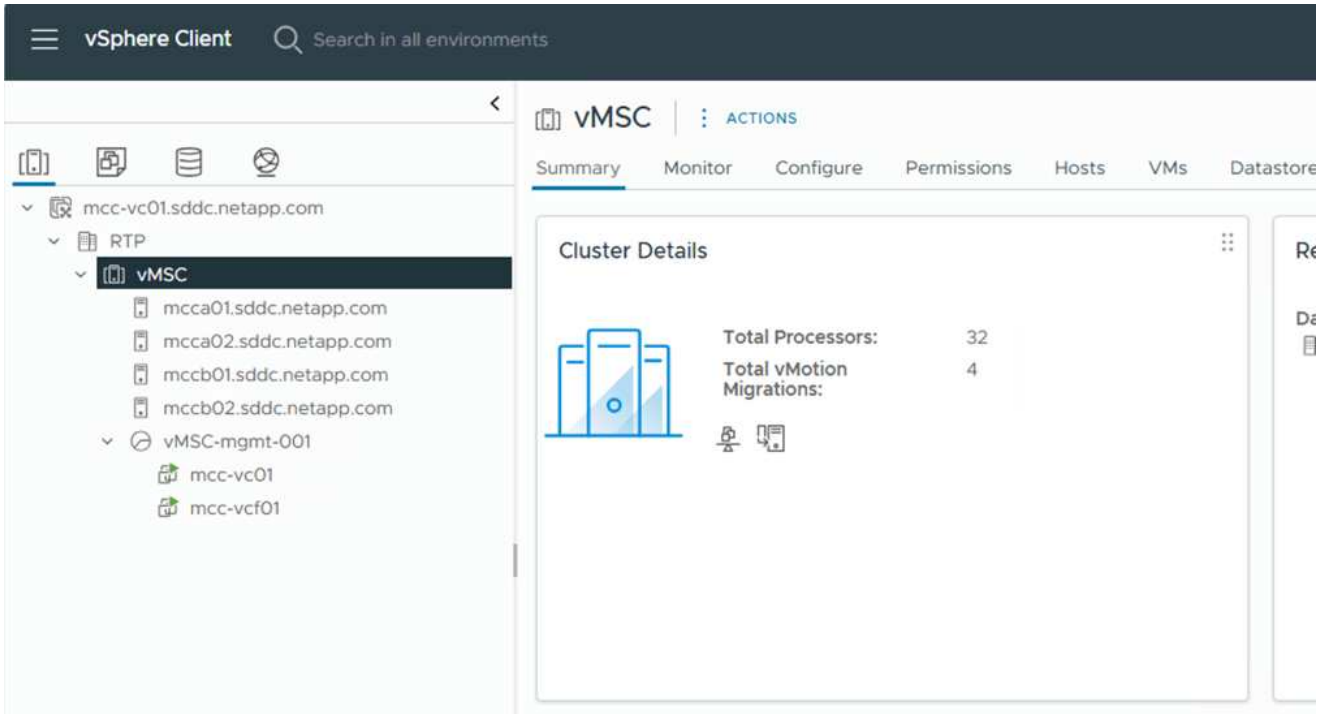
1. Siga os passos em "Execute uma pré-verificação no vCenter de destino antes da conversão" para executar a validação.
2. A saída a seguir mostra que o dispositivo vCenter passou na pré-verificação.

```
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2025-03-20 23:02:08,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

Implantar o Gerenciador do SDDC

O gerenciador do SDDC deve ser colocalizado no cluster vSphere que será convertido em um domínio de gerenciamento VCF.

Siga as instruções de implantação no VMware Docs para concluir a implantação.



Consulte "Implantar o SDDC Manager Appliance no vCenter de destino" .

Crie um arquivo JSON para implantação do NSX

Para implantar o NSX Manager ao importar ou converter um ambiente vSphere no VMware Cloud Foundation, crie uma especificação de implantação do NSX. A implantação do NSX requer um mínimo de 3 hosts.

> Ao implantar um cluster do NSX Manager em uma operação de conversão ou importação, o segmento com suporte da VLAN do NSX é usado. Para obter detalhes sobre as limitações do segmento com suporte NSX-VLAN, consulte a seção "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation". Para obter informações sobre as limitações de rede NSX-VLAN, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

A seguir está um exemplo de um arquivo JSON para implantação do NSX:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "******************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.114",
  "cluster_fqdn": "mcc-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-nsxa.sddc.netapp.com",
    "name": "mcc-nsxa",
    "ip_address": "10.61.185.111",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxb.sddc.netapp.com",
    "name": "mcc-nsxb",
    "ip_address": "10.61.185.112",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxc.sddc.netapp.com",
    "name": "mcc-nsxc",
    "ip_address": "10.61.185.113",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie o arquivo JSON para a pasta inicial do usuário vcf no SDDC Manager.

Carregar software para o SDDC Manager

Copie a Ferramenta de Importação VCF para a pasta inicial do usuário vcf e o pacote de implantação NSX para a pasta /nfs/vmware/vcf/nfs-mount/bundle/ no Gerenciador SDDC.

Ver "Carregue o software necessário para o SDDC Manager Appliance" para obter instruções detalhadas.

Verificação detalhada no vCenter antes da conversão

Antes de executar uma operação de conversão de domínio de gerenciamento ou uma operação de importação de domínio de carga de trabalho do VI, você deve executar uma verificação detalhada para garantir que a configuração do ambiente vSphere existente seja suportada para conversão ou importação. . SSH para o dispositivo SDDC Manager como usuário vcf. . Navegue até o diretório onde você copiou a Ferramenta de Importação VCF. . Execute o seguinte comando para verificar se o ambiente vSphere pode ser convertido

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```

Converter cluster vSphere em domínio de gerenciamento VCF

A ferramenta de importação VCF é usada para conduzir o processo de conversão.

O comando a seguir é executado para converter o cluster vSphere em um domínio de gerenciamento VCF e implantar o cluster NSX:

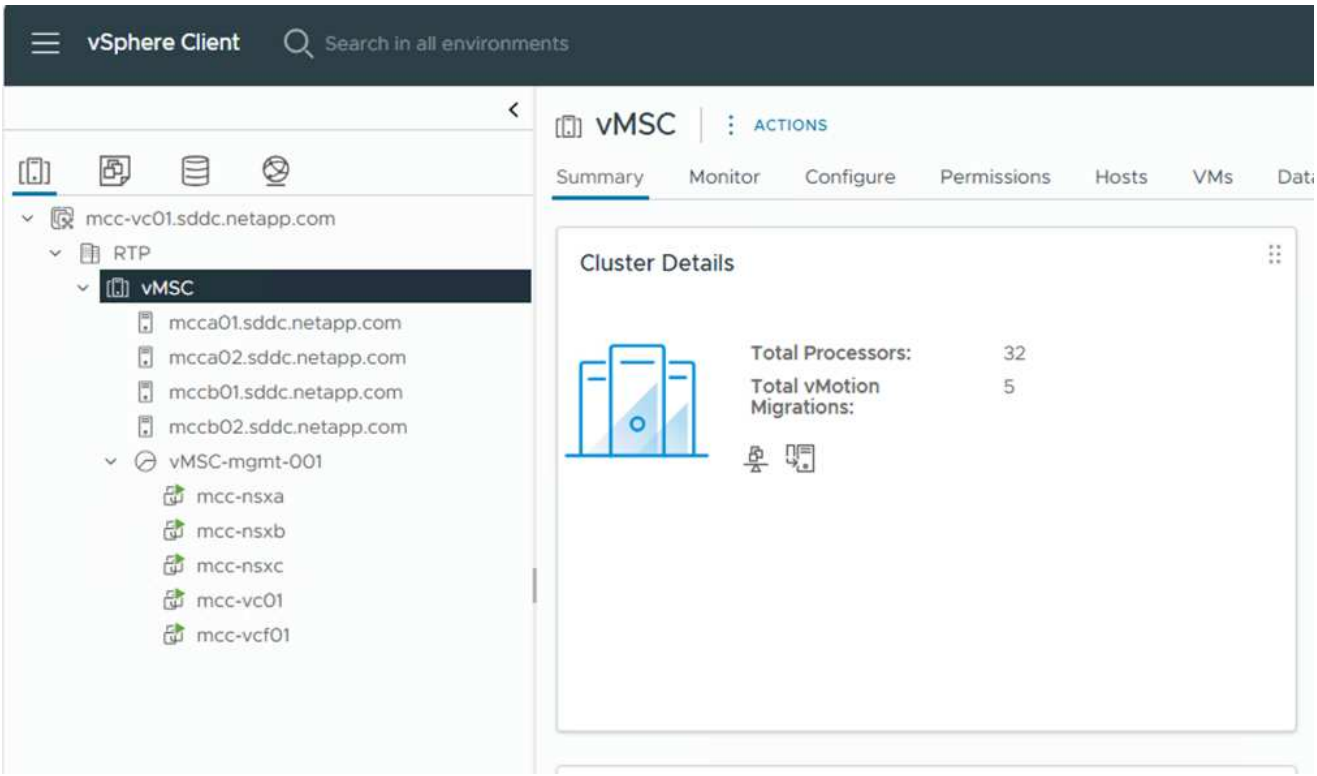
```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

Quando vários Datastores estão disponíveis no host vSphere, ele solicita qual Datastore precisa ser considerado como Datastore primário em quais VMs NSX serão implantadas por padrão.

```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: ==============================================================
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: ==============================================================
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
1) NFS01
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
```

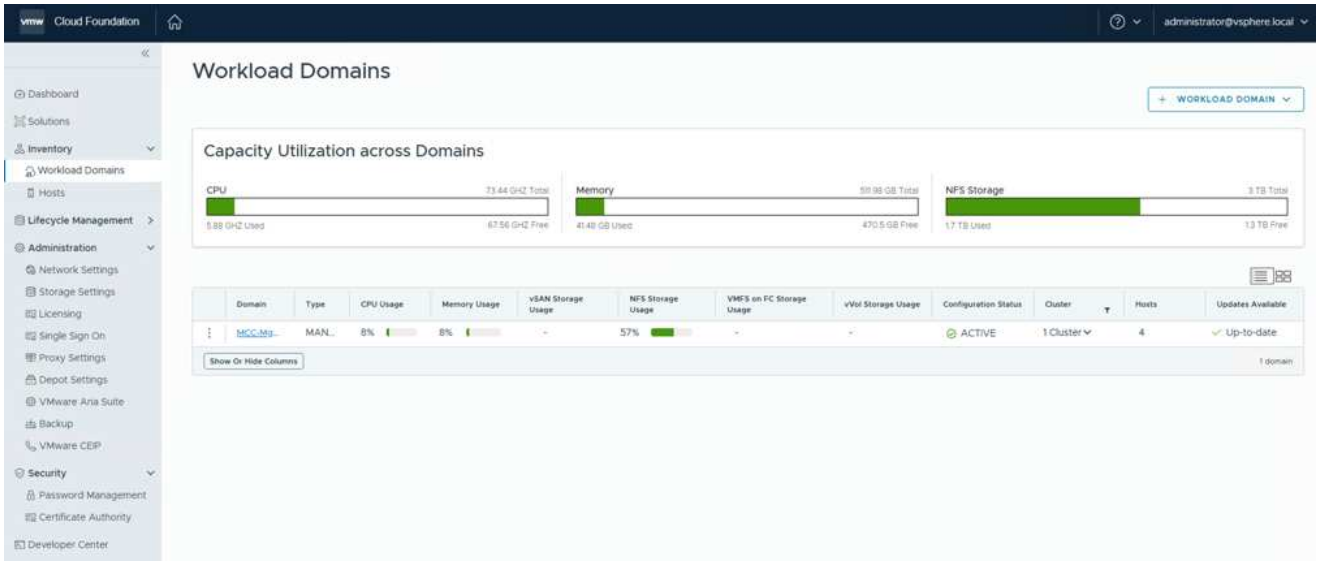
Para obter instruções completas, consulte "Procedimento de conversão VCF" .

As VMs do NSX serão implantadas no vCenter.

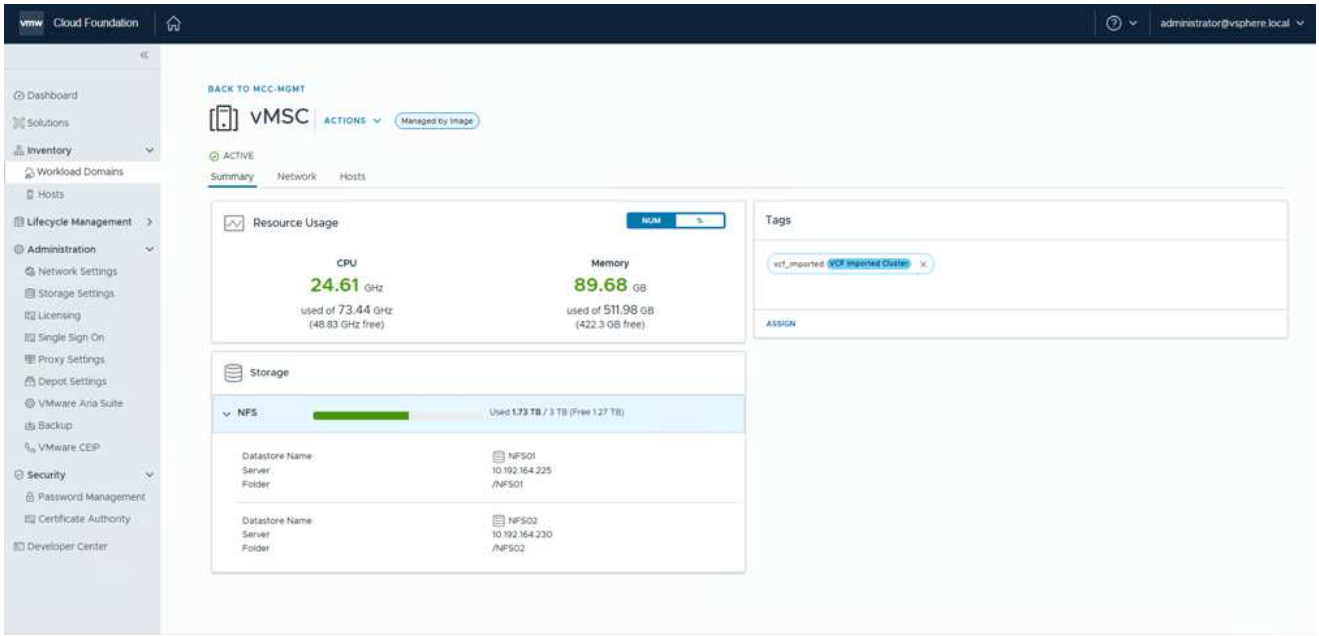


O SDDC Manager mostra o domínio de gerenciamento criado com o nome fornecido e o NFS como

Datastore.



Ao inspecionar o cluster, ele fornece as informações do NFS Datastore.



Adicionar licenciamento ao VCF

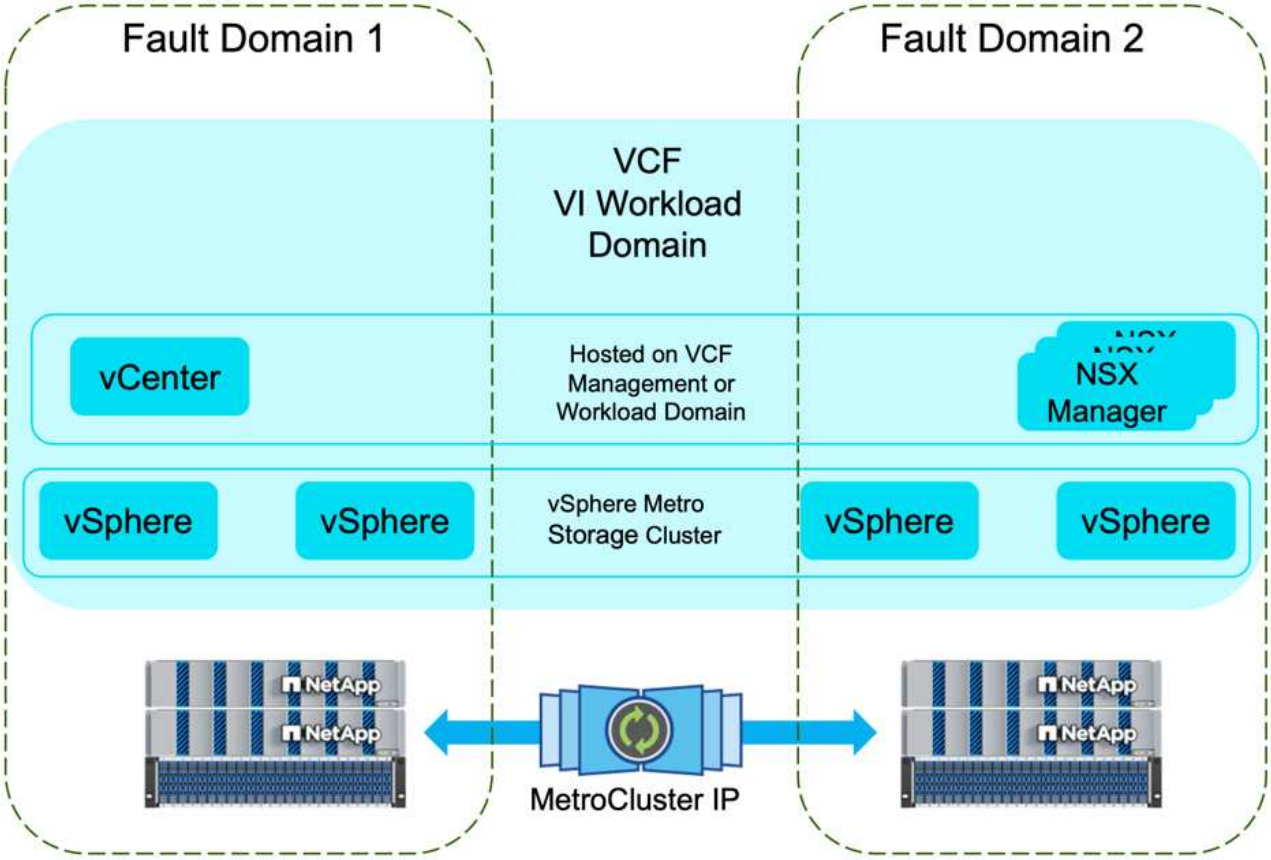
Após concluir a conversão, o licenciamento deve ser adicionado ao ambiente.

1. Efetue login na interface de usuário do SDDC Manager.
2. Navegue até **Administração > Licenciamento** no painel de navegação.
3. Clique em **+ Chave de licença**.
4. Escolha um produto no menu suspenso.
5. Digite a chave de licença.
6. Forneça uma descrição para a licença.
7. Clique em **Adicionar**.
8. Repita essas etapas para cada licença.

Configurar um cluster de extensão para um domínio de carga de trabalho VI usando o MetroCluster

Neste caso de uso, descrevemos o procedimento para configurar o domínio de carga de trabalho VCF VI estendido com NFS como armazenamento de dados principal usando o ONTAP MetroCluster. Este procedimento inclui a implantação de hosts vSphere e vCenter Server, o provisionamento de datastores NFS, a validação do cluster vSphere, a configuração do NSX durante a conversão do VCF e a importação do ambiente vSphere para um Domínio de Gerenciamento VCF existente.

As cargas de trabalho no VCF são protegidas pelo vSphere Metro Storage Cluster (vMSC). O ONTAP MetroCluster com implantação FC ou IP é normalmente utilizado para fornecer tolerância a falhas de datastores VMFS e NFS.



Introdução

Nesta solução, demonstraremos como implementar o Stetched VCF VI Workload Domain com NFS como Principal Datastore usando o ONTAP MetroCluster. O VI Workload Domain pode ser implantado usando o SDDC Manager ou importar um ambiente vSphere existente como VI Workload Domain.

Visão geral do cenário

Este cenário abrange as seguintes etapas de alto nível:

- Implante hosts vSphere e o servidor vCenter.
- Provisione o armazenamento de dados NFS para hosts vSphere.
- Use a Ferramenta de Importação VCF para validar o cluster vSphere.
- Configure um arquivo JSON para criar um NSX durante a conversão de VCF.
- Use a Ferramenta de Importação VCF para importar o ambiente vSphere 8 como domínio de carga de trabalho VCF VI para um Domínio de Gerenciamento VCF existente.

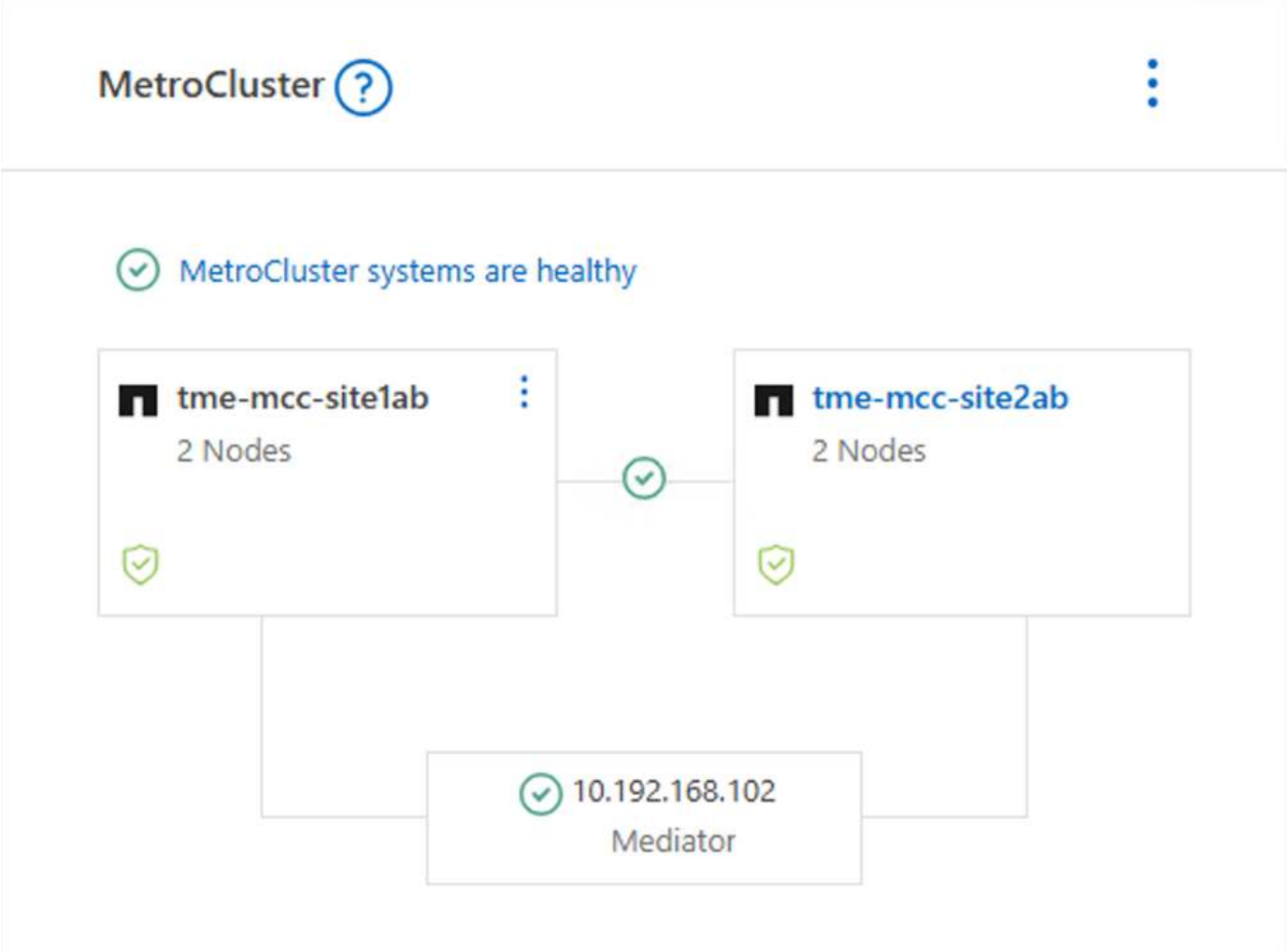
Pré-requisitos

Este cenário requer os seguintes componentes e configurações:

- Configuração ONTAP MetroCluster suportada
- Máquina virtual de armazenamento (SVM) configurada para permitir tráfego NFS.

- A interface lógica (LIF) foi criada na rede IP que transportará o tráfego NFS e está associada ao SVM.
- Um cluster vSphere 8 com 4 hosts ESXi conectados ao switch de rede.
- Baixe o software necessário para a conversão de VCF.

Aqui está a captura de tela de exemplo do System Manager mostrando a configuração do MetroCluster
.



e aqui estão as interfaces de rede SVM de ambos os domínios de falha.

Network interfaces Subnets

+ Add

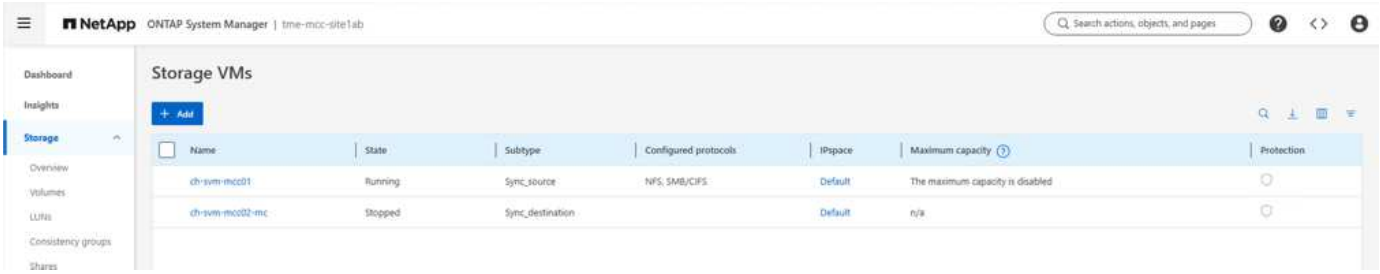
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

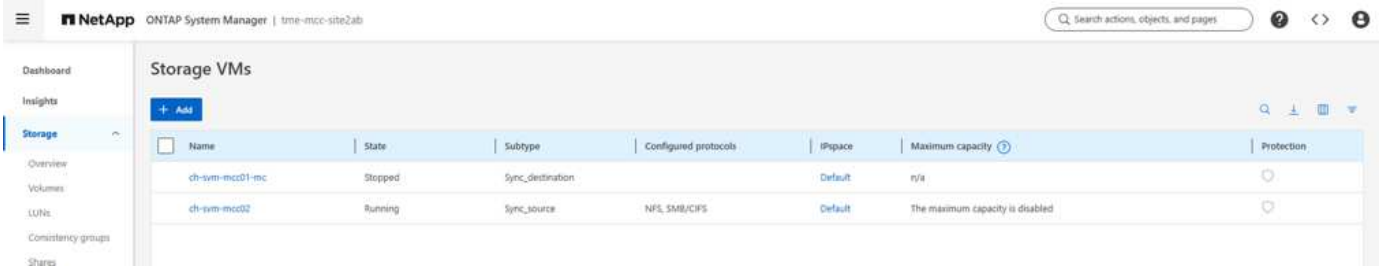
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[NOTA] O SVM estará ativo em um dos domínios de falha no MetroCluster.





Referir "vMSC com MetroCluster" .

Para armazenamento suportado e outras considerações para conversão ou importação do vSphere para VCF 5.2, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

Antes de criar o vSphere Cluster que será convertido em VCF Management Domain, consulte "Consideração do NSX no vSphere Cluster"

Para o software necessário, consulte "Baixe o software para converter ou importar ambientes vSphere existentes" .

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Etapas de implantação

Para implantar o VCF Stretched Management Domain com NFS como armazenamento de dados principal,

Conclua as seguintes etapas:

- Implante hosts vSphere e vCenter.
- Crie um cluster do vSphere.
- Provisionar armazenamento de dados NFS.
- Copie a ferramenta de importação VCF para o dispositivo vCenter.
- Execute uma pré-verificação no dispositivo vCenter usando a Ferramenta de Importação VCF.
- Crie um arquivo JSON para um cluster NSX a ser implantado durante o processo de importação.
- Carregue o software necessário para o gerenciador do SDDC.
- Converta o cluster vSphere em VCF VI Workload Domain.

Para uma visão geral do processo de conversão, consulte "Converter um ambiente vSphere em um domínio de gerenciamento ou importar um ambiente vSphere como um domínio de carga de trabalho VI no VMware Cloud Foundation" .

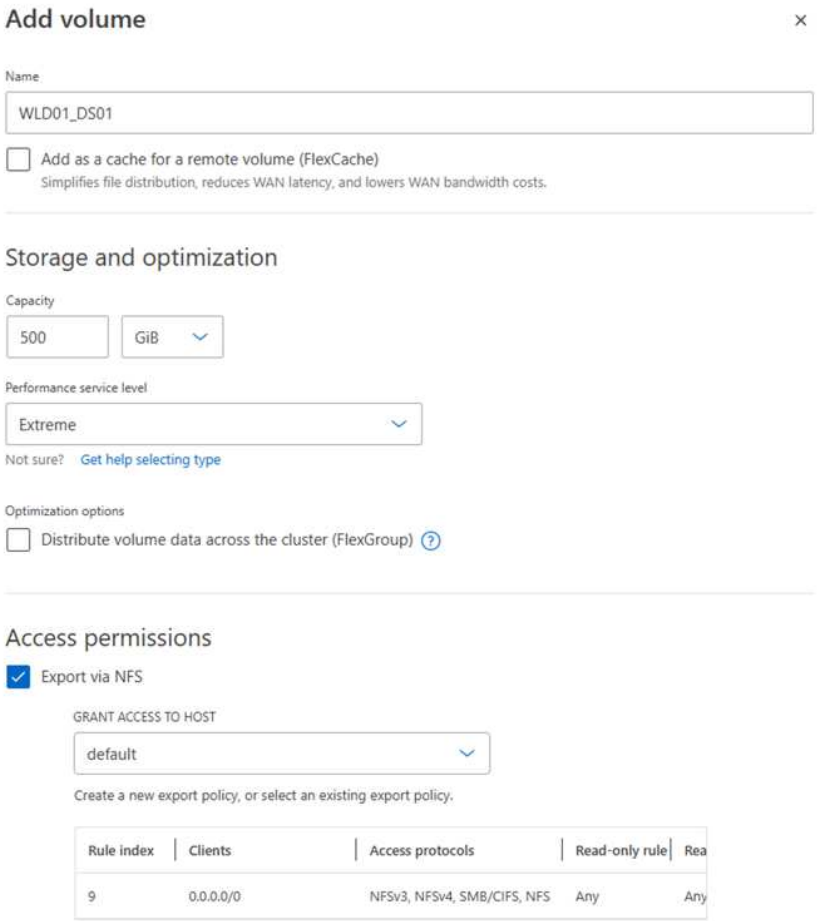
Implantar hosts vSphere e vCenter

Implante o vSphere em hosts usando o ISO baixado do portal de suporte da Broadcom ou use a opção de implantação existente para o host vSphere.

Monte o NFS Datastore para hospedar VMs

Nesta etapa, criamos o volume NFS e o montamos como Datastore para hospedar VMs.

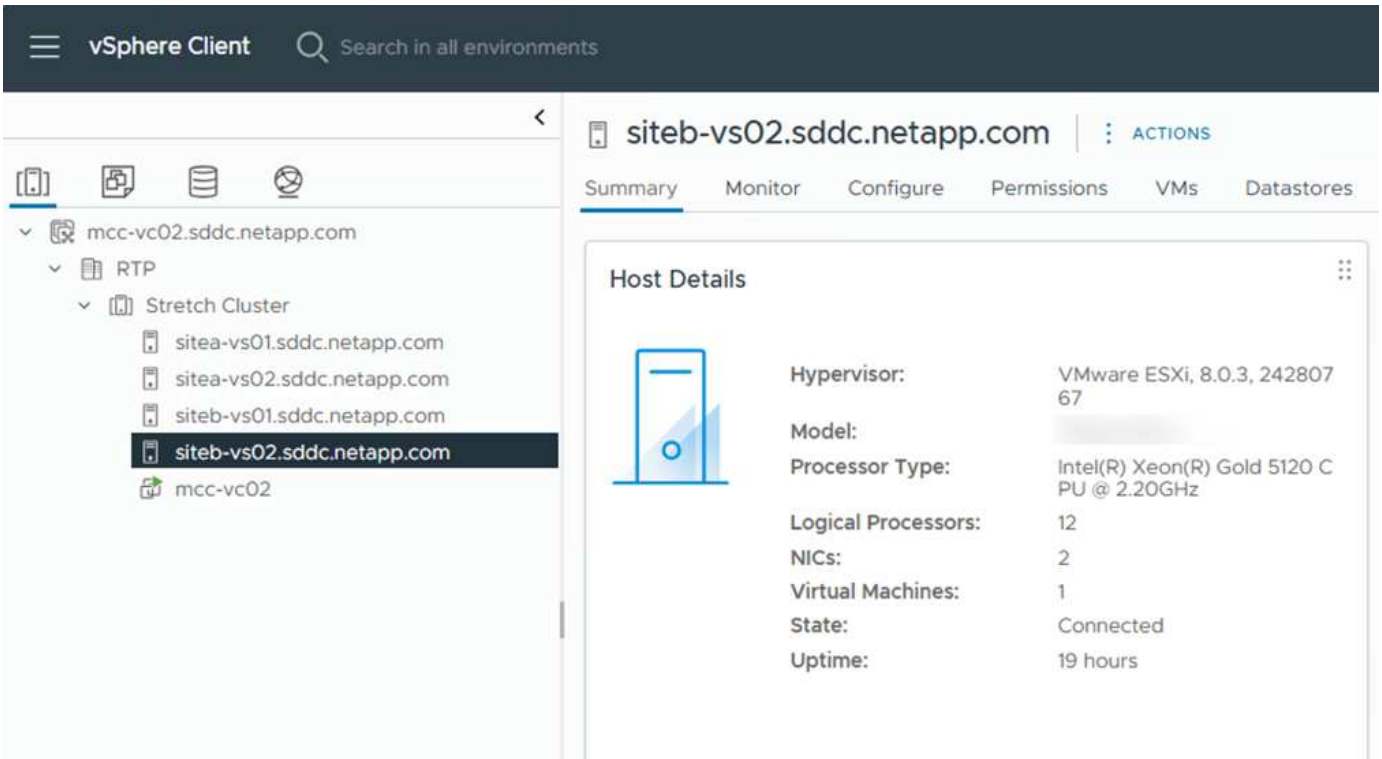
1. Usando o Gerenciador do Sistema, crie um volume e anexe-o à política de exportação que inclui a sub-rede IP do host
vSphere.



2. Conecte-se via SSH ao host vSphere e monte o NFS Datastore.

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

Implante o vCenter no NFS Datastore. Certifique-se de que o SSH e o shell Bash estejam habilitados no dispositivo
vCenter.



Criar cluster vSphere

1. Efetue login no vSphere webclient, crie o DataCenter e o vSphere Cluster adicionando um dos hosts onde o NFS VAAI está implantado. Optamos por gerenciar todos os hosts no cluster com a opção de imagem única. [DICA] Não selecione Gerenciar configuração no nível do cluster. Para obter detalhes adicionais, consulte "Consideração do NSX no vSphere Cluster" . Para melhores práticas de vMSC com ONTAP MetroCluster, verifique "Diretrizes de design e implementação do vMSC"
2. Adicione outros hosts vSphere ao cluster.
3. Crie um Distributed Switch e adicione os grupos de portas.
4. "Migre a rede do vSwitch padrão para o switch distribuído."

Converter ambiente vSphere para domínio de carga de trabalho VCF VI

A seção a seguir aborda as etapas para implantar o gerenciador SDDC e converter o cluster vSphere 8 em um domínio de gerenciamento VCF 5.2. Quando apropriado, a documentação da VMware será consultada para obter detalhes adicionais.

A VCF Import Tool, da VMware by Broadcom, é um utilitário usado no dispositivo vCenter e no gerenciador SDDC para validar configurações e fornecer serviços de conversão e importação para ambientes vSphere e VCF.

Para obter mais informações, consulte "Opções e parâmetros da ferramenta de importação VCF" .

Ferramenta de importação de VCF para copiar e extrair

A Ferramenta de Importação de VCF é usada no dispositivo vCenter para validar se o cluster vSphere está em um estado íntegro para o processo de conversão ou importação de VCF.

Conclua as seguintes etapas:

1. Siga os passos em "Copie a ferramenta de importação VCF para o dispositivo vCenter de destino" no VMware Docs para copiar a Ferramenta de Importação VCF para o local correto.
2. Extraia o pacote usando o seguinte comando:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validar o dispositivo vCenter

Use a ferramenta de importação VCF para validar o dispositivo vCenter antes da importação como domínio de carga de trabalho VI.

1. Siga os passos em "Execute uma pré-verificação no vCenter de destino antes da conversão" para executar a validação.

Crie um arquivo JSON para implantação do NSX

Para implantar o NSX Manager ao importar ou converter um ambiente vSphere no VMware Cloud Foundation, crie uma especificação de implantação do NSX. A implantação do NSX requer um mínimo de 3 hosts.

> Ao implantar um cluster do NSX Manager em uma operação de conversão ou importação, o segmento com suporte da VLAN do NSX é usado. Para obter detalhes sobre as limitações do segmento com suporte NSX-VLAN, consulte a seção "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation". Para obter informações sobre as limitações de rede NSX-VLAN, consulte "Considerações antes de converter ou importar ambientes vSphere existentes para o VMware Cloud Foundation" .

A seguir está um exemplo de um arquivo JSON para implantação do NSX:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "****************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.105",
  "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",
    "name": "mcc-wld01-nsxa",
    "ip_address": "10.61.185.106",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",
    "name": "mcc-wld01-nsxb",
    "ip_address": "10.61.185.107",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",
    "name": "mcc-wld01-nsxc",
    "ip_address": "10.61.185.108",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Copie o arquivo JSON para a pasta inicial do usuário vcf no SDDC Manager.

Carregar software para o SDDC Manager

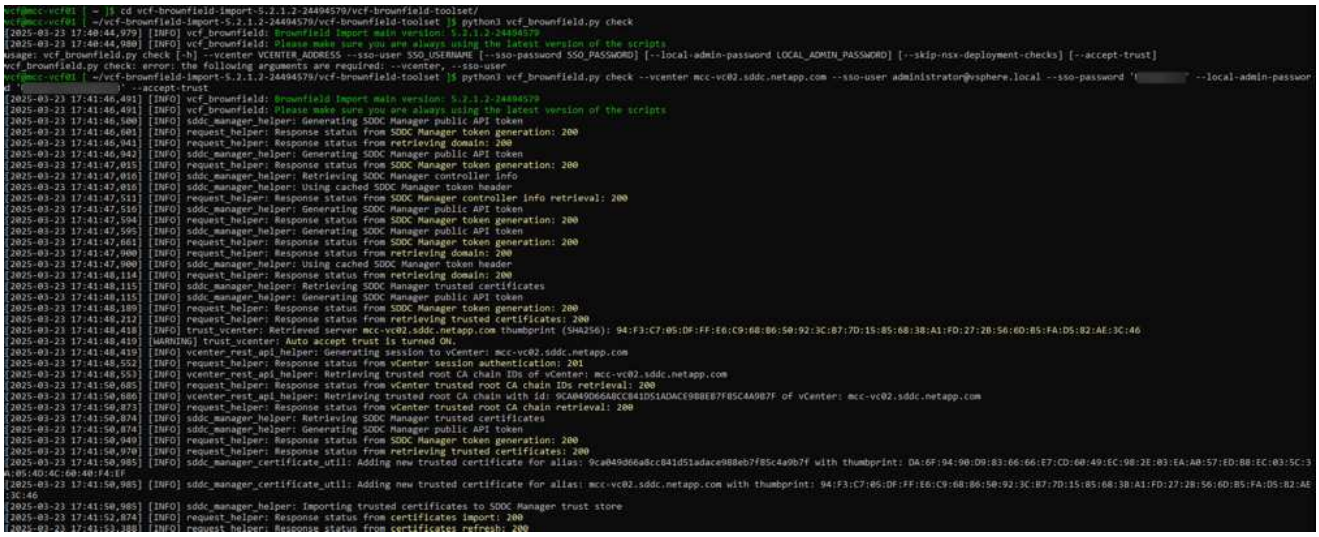
Copie a Ferramenta de Importação VCF para a pasta inicial do usuário vcf e o pacote de implantação NSX para a pasta /nfs/vmware/vcf/nfs-mount/bundle/ no Gerenciador SDDC.

Ver "Carregue o software necessário para o SDDC Manager Appliance" para obter instruções detalhadas.

Verificação detalhada no vCenter antes da conversão

Antes de executar uma operação de conversão de domínio de gerenciamento ou uma operação de importação de domínio de carga de trabalho do VI, você deve executar uma verificação detalhada para garantir que a configuração do ambiente vSphere existente seja suportada para conversão ou importação. . SSH para o dispositivo SDDC Manager como usuário vcf. . Navegue até o diretório onde você copiou a Ferramenta de Importação VCF. . Execute o seguinte comando para verificar se o ambiente vSphere pode ser convertido

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```



Converter cluster vSphere em domínio de carga de trabalho VCF VI

A ferramenta de importação VCF é usada para conduzir o processo de conversão.

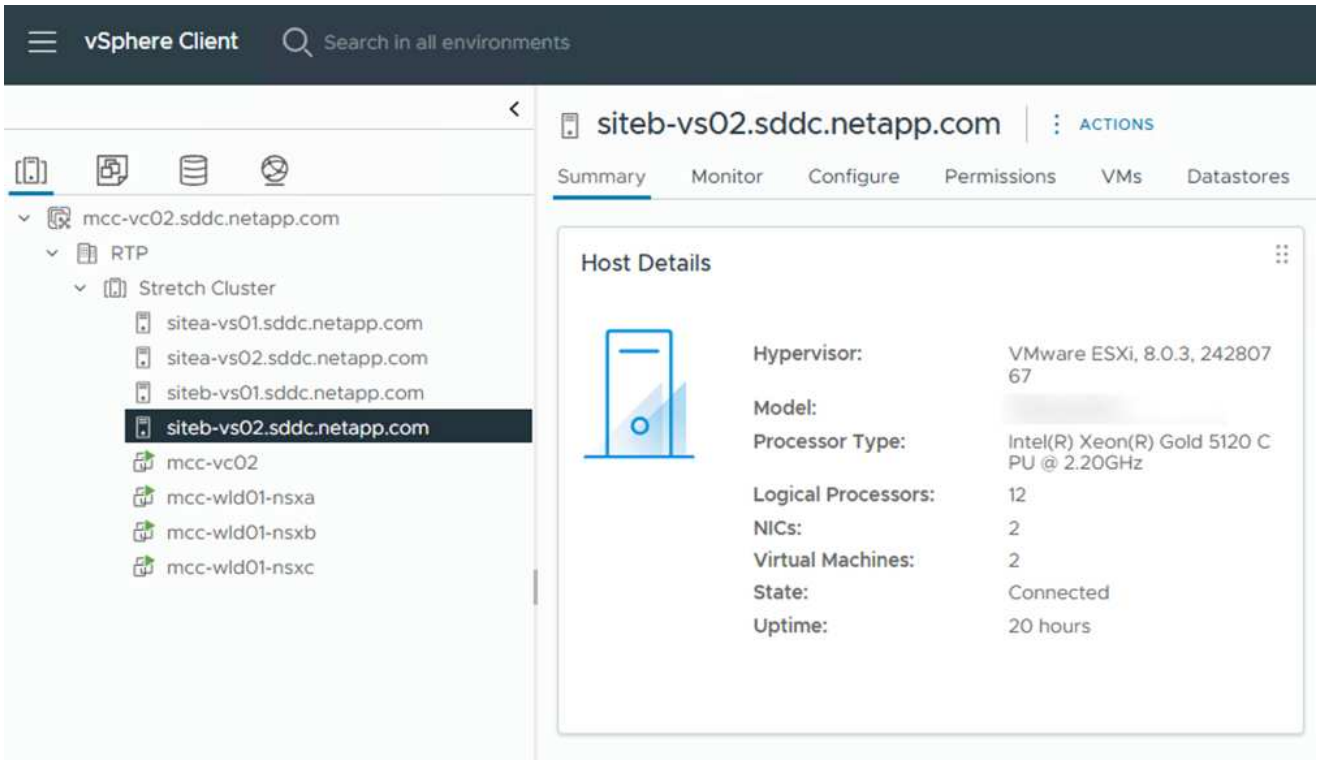
O comando a seguir é executado para converter o cluster vSphere em um domínio de gerenciamento VCF e implantar o cluster NSX:

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

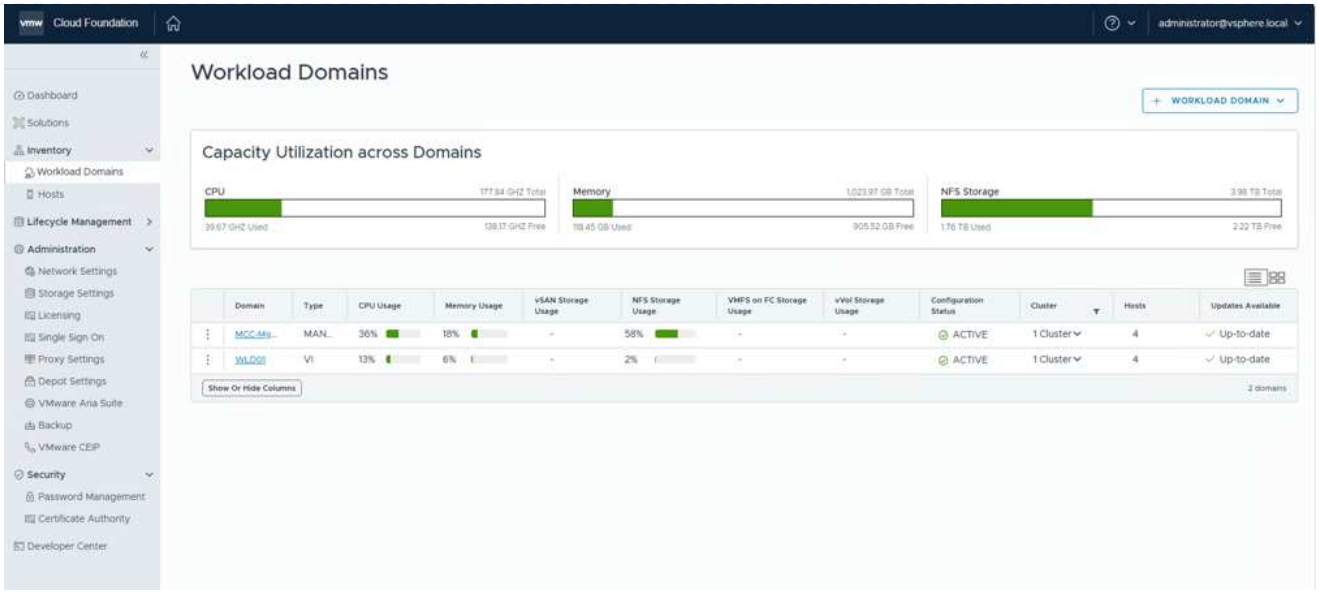
Mesmo que vários Datastores estejam disponíveis no host vSphere, não há necessidade de solicitar qual Datastore precisa ser considerado como Datastore Primário.

Para obter instruções completas, consulte "Procedimento de conversão VCF" .

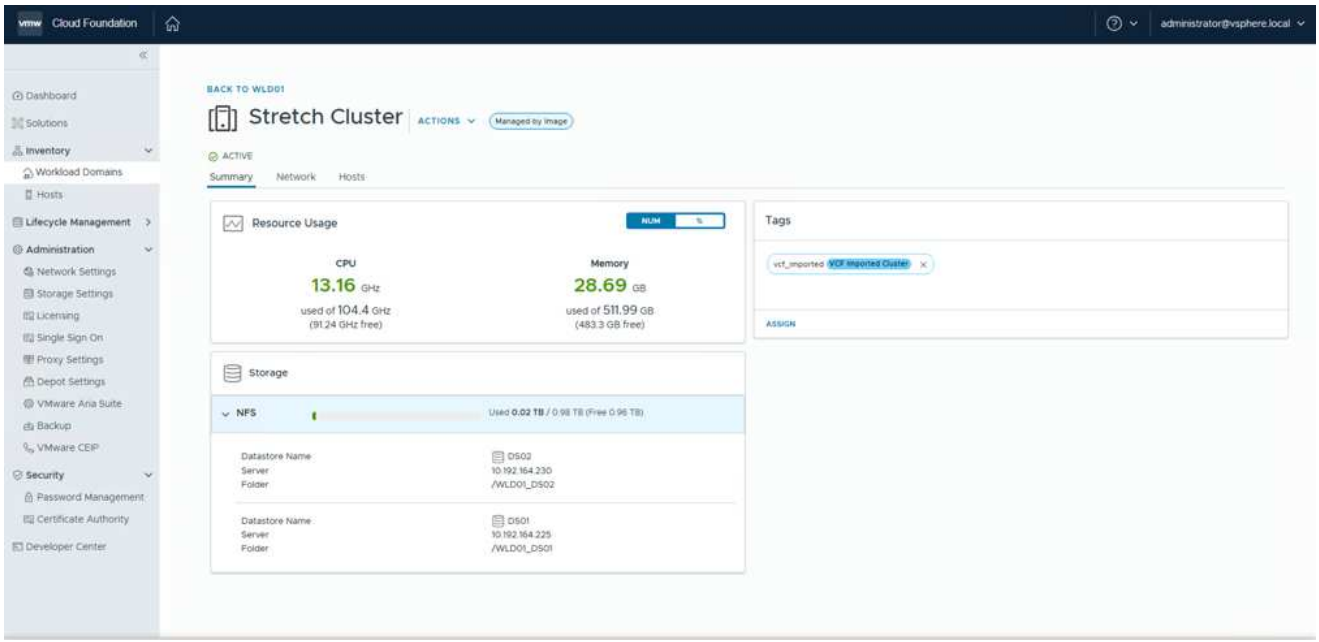
As VMs do NSX serão implantadas no vCenter.



O SDDC Manager mostra o domínio de carga de trabalho do VI criado com o nome fornecido e o NFS como Datastore.



Ao inspecionar o cluster, ele fornece as informações dos NFS Datastores.



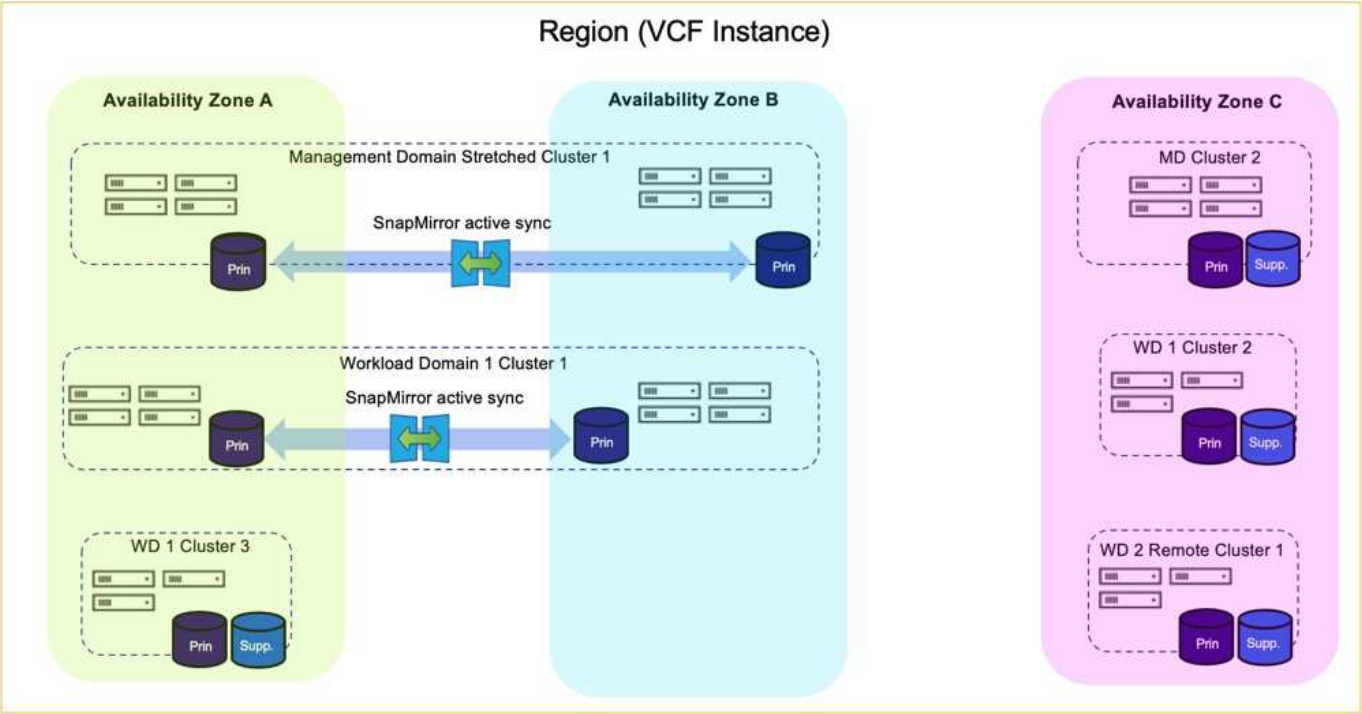
Adicionar licenciamento ao VCF

Após concluir a conversão, o licenciamento deve ser adicionado ao ambiente.

1. Efetue login na interface de usuário do SDDC Manager.
2. Navegue até **Administração > Licenciamento** no painel de navegação.
3. Clique em **+ Chave de licença**.
4. Escolha um produto no menu suspenso.
5. Digite a chave de licença.
6. Forneça uma descrição para a licença.
7. Clique em **Adicionar**.
8. Repita essas etapas para cada licença.

Configurar um cluster de extensão para um domínio de gerenciamento VCF usando o SnapMirror Active Sync

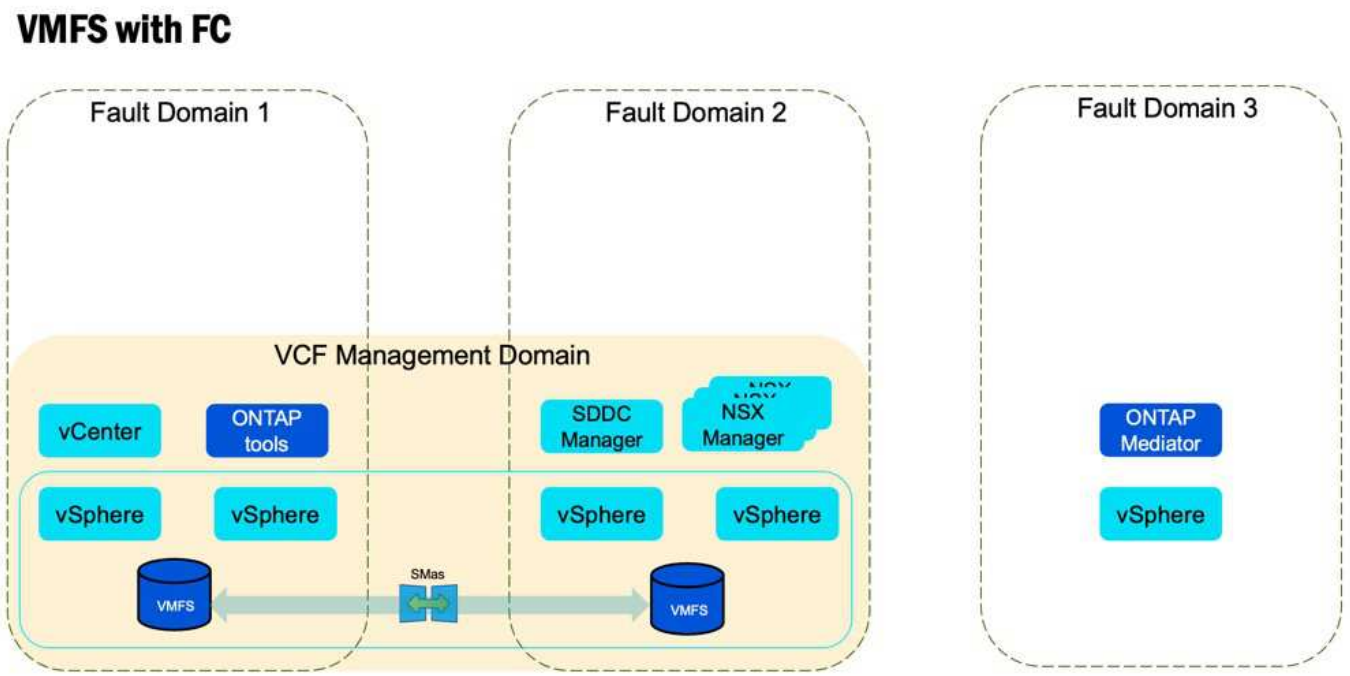
Neste caso de uso, descrevemos o procedimento para usar ONTAP tools for VMware vSphere para configurar um cluster estendido para um domínio de gerenciamento VCF. Este procedimento inclui a implantação de hosts vSphere e vCenter Server, a instalação de ferramentas ONTAP , a proteção de datastores com o SnapMirror Active Sync, a migração de VMs para datastores protegidos e a configuração de armazenamento suplementar.



Visão geral do cenário

A solução de cluster extensível pode ser implementada no cluster padrão ou em um cluster adicional em

domínios de gerenciamento ou carga de trabalho do VCF. O VMFS no FC é suportado tanto no armazenamento de dados principal quanto no armazenamento de dados suplementar. O VMFS no iSCSI só é suportado com armazenamentos de dados suplementares. Consulte o IMT para obter suporte de VMFS em NVMe-oF com sincronização ativa do SnapMirror .



Armazenamento principal no domínio de gerenciamento

A partir do VCF 5.2, o domínio de gerenciamento pode ser implantado sem VSAN usando a ferramenta de importação do VCF. A opção de conversão da ferramenta de importação VCF permite"uma implantação existente do vCenter em um domínio de gerenciamento" . Todos os clusters no vCenter se tornarão parte do domínio de gerenciamento.

1. Implantar hosts vSphere
2. Implantar o servidor vCenter no armazenamento de dados local (o vCenter precisa coexistir em hosts vSphere que serão convertidos em domínio de gerenciamento)
3. Implantar ONTAP tools for VMware vSphere
4. Implantar o plugin SnapCenter para VMware vSphere (opcional)
5. Criar armazenamento de dados (a configuração da zona FC deve estar em vigor)
6. Proteja o cluster vSphere
7. Migrar VMs para um armazenamento de dados recém-criado

> Sempre que o cluster for expandido ou reduzido, será necessário atualizar o relacionamento do cluster do host nas ferramentas ONTAP para que o cluster indique as alterações feitas na origem ou no destino.

Armazenamento suplementar no domínio de gerenciamento

Depois que o domínio de gerenciamento estiver instalado e funcionando, armazenamentos de dados adicionais poderão ser criados usando ferramentas ONTAP , o que acionará a expansão do grupo de consistência.

> Se um cluster vSphere estiver protegido, todos os armazenamentos de dados no cluster estarão protegidos.

Se o ambiente VCF for implantado com a ferramenta Cloud Builder, para criar o armazenamento suplementar com iSCSI, implante ferramentas ONTAP para criar o armazenamento de dados iSCSI e proteger o cluster vSphere.

> Sempre que o cluster for expandido ou reduzido, será necessário atualizar o relacionamento do cluster do host nas ferramentas ONTAP para que o cluster indique as alterações feitas na origem ou no destino.

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

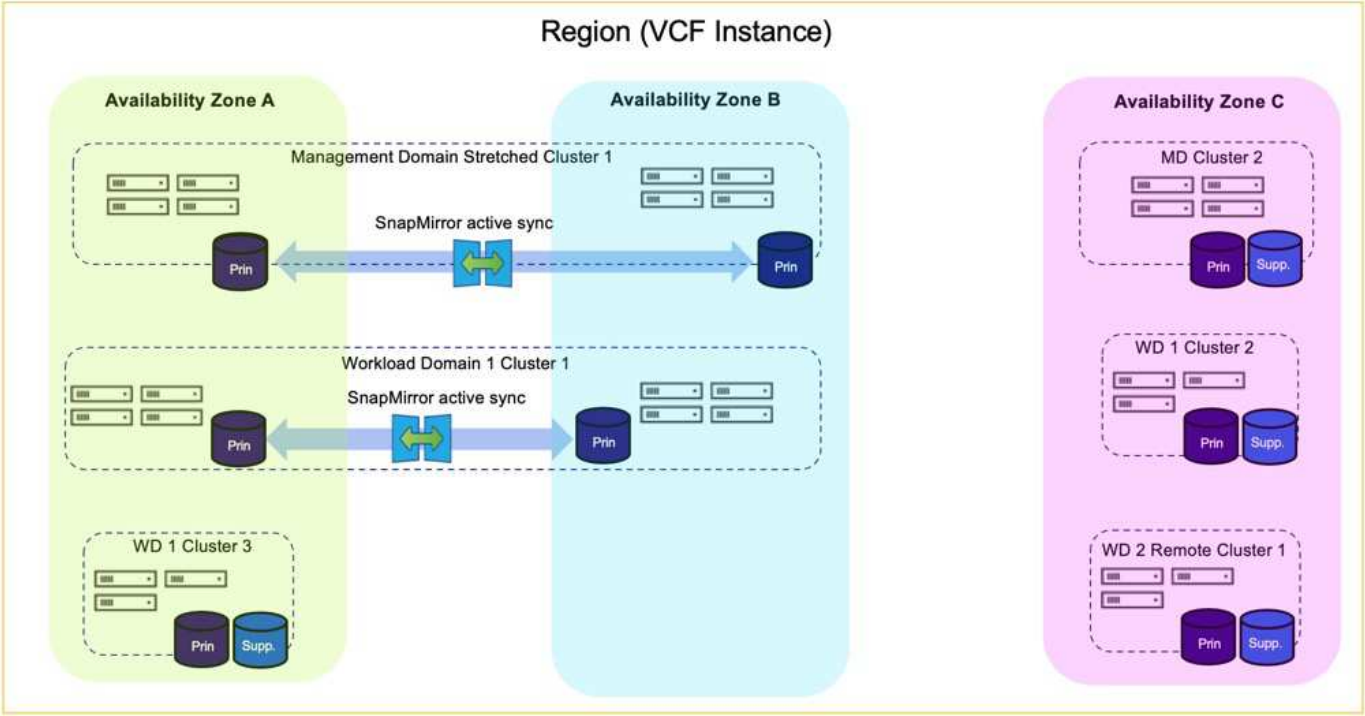
Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation 5.2" .

Demonstração em vídeo desta solução

Cluster de alongamento para VCF com ferramentas ONTAP

Configurar um cluster de extensão para um domínio de carga de trabalho de VI usando o SnapMirror Active Sync

Neste caso de uso, descrevemos o procedimento para configurar um cluster estendido para um domínio de carga de trabalho de infraestrutura virtual (VI) usando o SnapMirror Active Sync com ONTAP tools for VMware vSphere. Este procedimento inclui a criação de um domínio de carga de trabalho VCF com VMFS no Fibre Channel, o registro do vCenter com ferramentas ONTAP , o registro de sistemas de armazenamento e a proteção do cluster vSphere.



Visão geral do cenário

Os datastores no domínio de carga de trabalho do VCF podem ser protegidos com sincronização ativa do SnapMirror para fornecer uma solução de cluster expansível. A proteção é habilitada no nível do cluster do vSphere e todos os armazenamentos de dados do bloco ONTAP no cluster serão protegidos.

Armazenamento principal no domínio de carga de trabalho

O domínio de carga de trabalho pode ser criado importando usando a ferramenta de importação VCF ou implantando usando o gerenciador SDDC. A implantação com o gerenciador do SDDC fornecerá mais opções de rede do que importar um ambiente existente.

1. Criar domínio de carga de trabalho com VMFS no FC
2. "Registre o domínio de carga de trabalho vCenter no gerenciador de ferramentas ONTAP para implantar o plugin vCenter"
3. "Registre sistemas de armazenamento em ferramentas ONTAP"
4. "Proteja o cluster vSphere"

> Sempre que o cluster for expandido ou reduzido, será necessário atualizar o relacionamento do cluster do host nas ferramentas ONTAP para que o cluster indique as alterações feitas na origem ou no destino.

Armazenamento suplementar no domínio de carga de trabalho

Depois que o domínio da carga de trabalho estiver ativo e em execução, armazenamentos de dados adicionais poderão ser criados usando ferramentas ONTAP , o que acionará a expansão do grupo de consistência.

Se um cluster vSphere estiver protegido, todos os armazenamentos de dados no cluster estarão protegidos.

Informações adicionais

Para obter informações sobre como configurar sistemas de armazenamento ONTAP , consulte o"Documentação do ONTAP 9" centro.

Para obter informações sobre como configurar o VCF, consulte"Documentação do VMware Cloud Foundation" .

Demonstração em vídeo desta solução

Cluster de alongamento para VCF com ferramentas ONTAP

Migrar VMs do VMware vSphere para datastores ONTAP

Os ambientes VMware vSphere podem se beneficiar significativamente da migração de máquinas virtuais para armazenamentos de dados suportados NetApp ONTAP. Não importa se você está migrando do vSAN, de sistemas de armazenamento de terceiros ou atualizando sua infraestrutura existente, explore vários cenários e estratégias de migração do vMotion para fazer a transição perfeita de suas VMs para datastores ONTAP . Isso garante a continuidade dos negócios ao mesmo tempo em que aproveita os recursos de armazenamento de nível empresarial do ONTAP.

O VMware vSphere da Broadcom oferece suporte a datastores VMFS, NFS e vVol para hospedar máquinas virtuais. Os clientes têm a opção de criar esses armazenamentos de dados com infraestruturas hiperconvergentes ou com sistemas de armazenamento compartilhado centralizados.

Os clientes geralmente veem valor na hospedagem em sistemas de armazenamento baseados em ONTAP para fornecer snapshots e clones de máquinas virtuais com eficiência de espaço, flexibilidade para escolher vários modelos de implantação em data centers e nuvens, eficiência operacional com ferramentas de monitoramento e alerta, segurança, governança e ferramentas de conformidade opcionais para inspecionar dados de VM e assim por diante.

VMs hospedadas em datastores ONTAP podem ser protegidas usando o SnapCenter Plugin para VMware vSphere (SCV). O SCV cria instantâneos baseados em armazenamento e também replica para o sistema de armazenamento ONTAP remoto. As restaurações podem ser executadas em sistemas de armazenamento primário ou secundário.

Os clientes têm flexibilidade para escolher o Cloud Insights ou o Aria Operations ou uma combinação de ambos ou outras ferramentas de terceiros que usam a API ONTAP para solucionar problemas, monitorar desempenho, gerar relatórios e recursos de notificação de alertas.

Os clientes podem facilmente provisionar o armazenamento de dados usando o plug-in vCenter do ONTAP

Tools ou sua API, e as VMs podem ser migradas para os armazenamentos de dados do ONTAP mesmo enquanto ele estiver ligado.

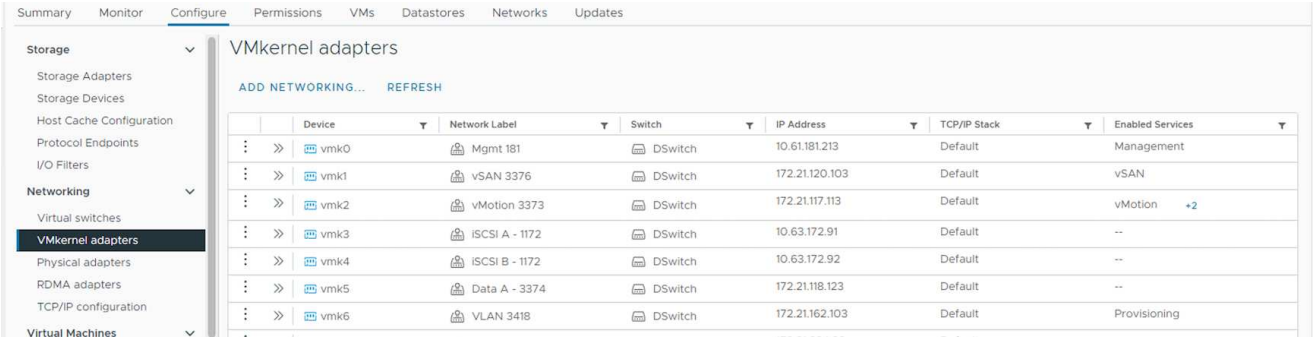
> Algumas VMs implantadas com ferramentas de gerenciamento externas, como Aria Automation, Tanzu (ou outras versões do Kubernetes), geralmente dependem da política de armazenamento da VM. A migração entre os armazenamentos de dados dentro da mesma política de armazenamento de VM deverá ter menos impacto nos aplicativos. Verifique com os proprietários do aplicativo para migrar adequadamente essas VMs para o novo armazenamento de dados. O vSphere 8 foi introduzido "Notificações vSphere vMotion para aplicativos sensíveis à latência" para preparar aplicações para o vMotion.

Requisitos de rede

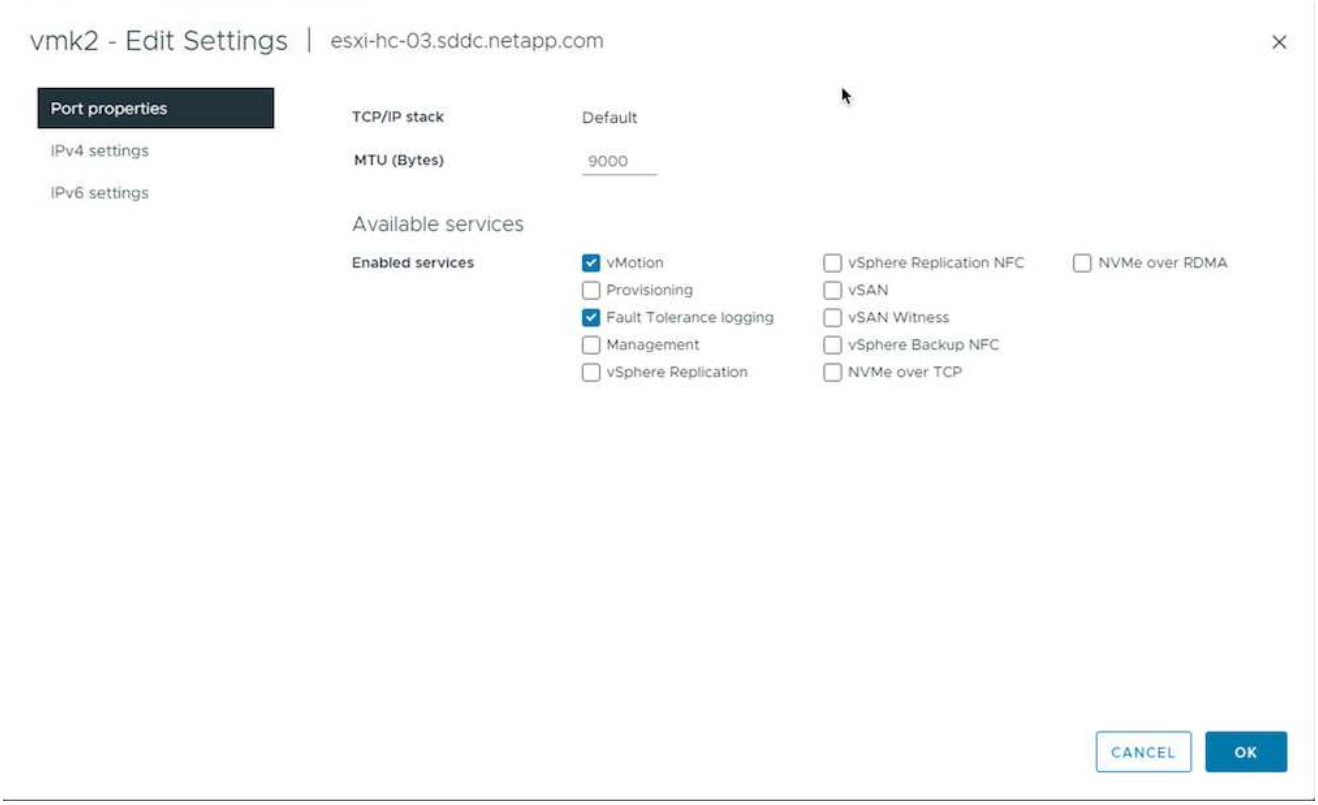
Migração de VM com vMotion

Presume-se que a rede de armazenamento dupla já esteja instalada para que o armazenamento de dados ONTAP forneça conectividade, tolerância a falhas e aumento de desempenho.

A migração de VMs entre hosts vSphere também é gerenciada pela interface VMKernel do host vSphere. Para migração a quente (ligadas em VMs), a interface VMKernel com o serviço vMotion habilitado é usada e para migração a frio (desligadas em VMs), a interface VMKernel com o serviço de provisionamento habilitado é consumida para mover os dados. Se nenhuma interface válida for encontrada, ele usará a interface de gerenciamento para mover os dados, o que pode não ser desejável para certos casos de uso.



Ao editar a interface VMKernel, aqui está a opção para habilitar os serviços necessários.



Certifique-se de que pelo menos duas placas de rede de uplink ativas de alta velocidade estejam disponíveis para o grupo de portas usado pelas interfaces vMotion e Provisioning VMkernel.

Cenários de migração de VM

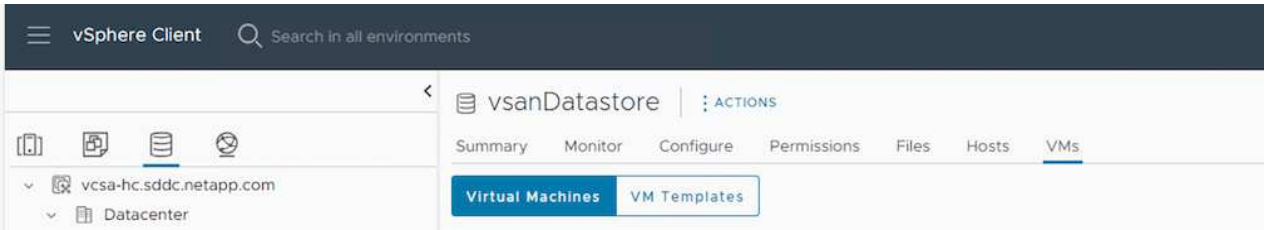
O vMotion é frequentemente usado para migrar VMs independentemente do seu estado de energia. Considerações adicionais e procedimentos de migração para cenários específicos estão disponíveis abaixo.

> Entender "Condições e limitações da VM do vSphere vMotion" antes de prosseguir com qualquer opção de migração de VM.

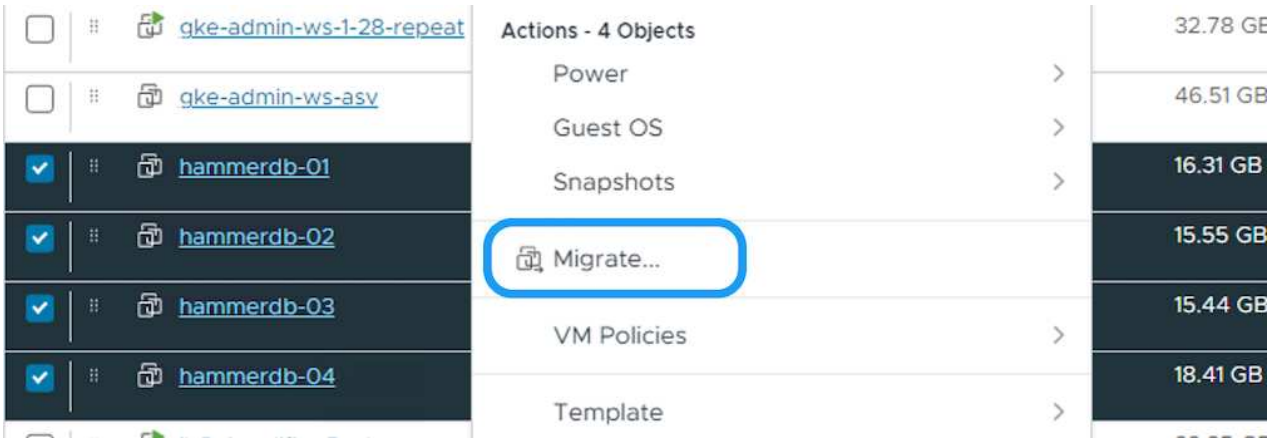
Migração de VMs de um vSphere Datastore específico

Siga o procedimento abaixo para migrar VMs para o novo Datastore usando a interface do usuário.

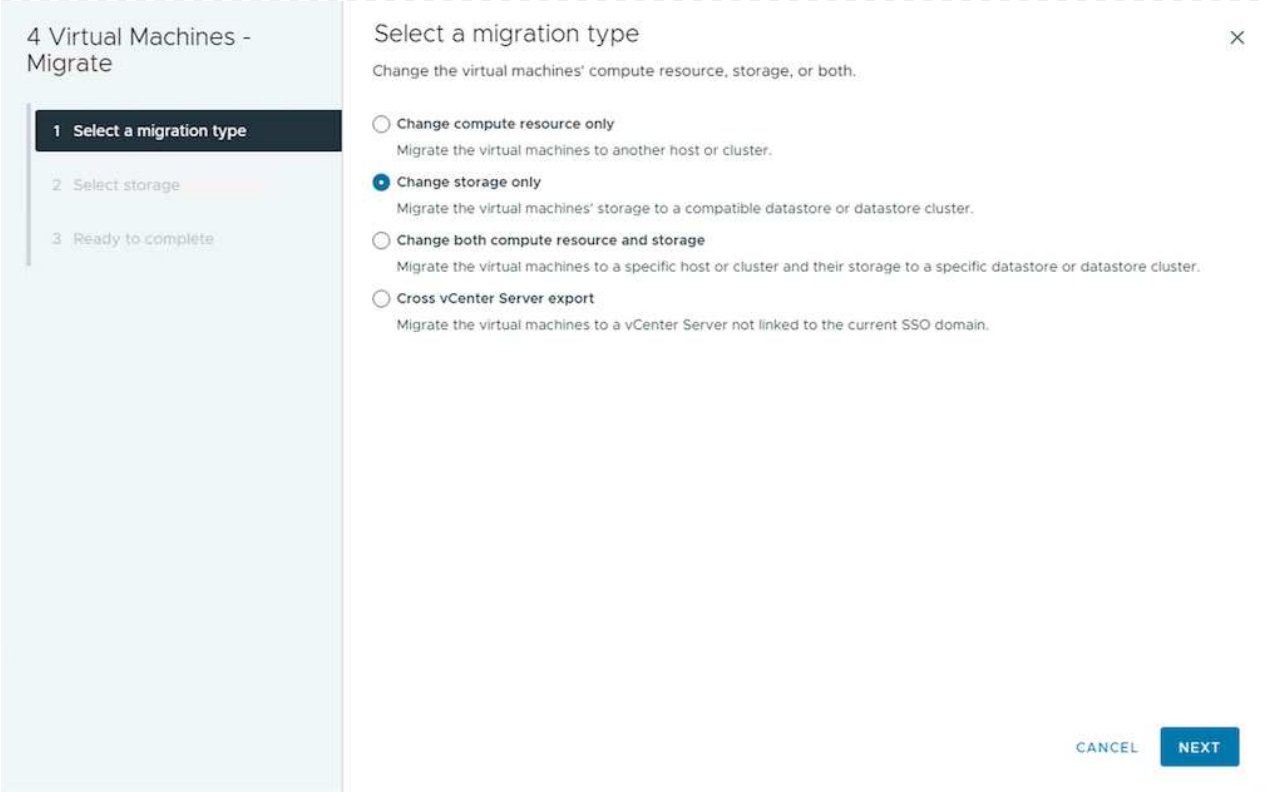
1. Com o vSphere Web Client, selecione o Datastore no inventário de armazenamento e clique na guia VMs.



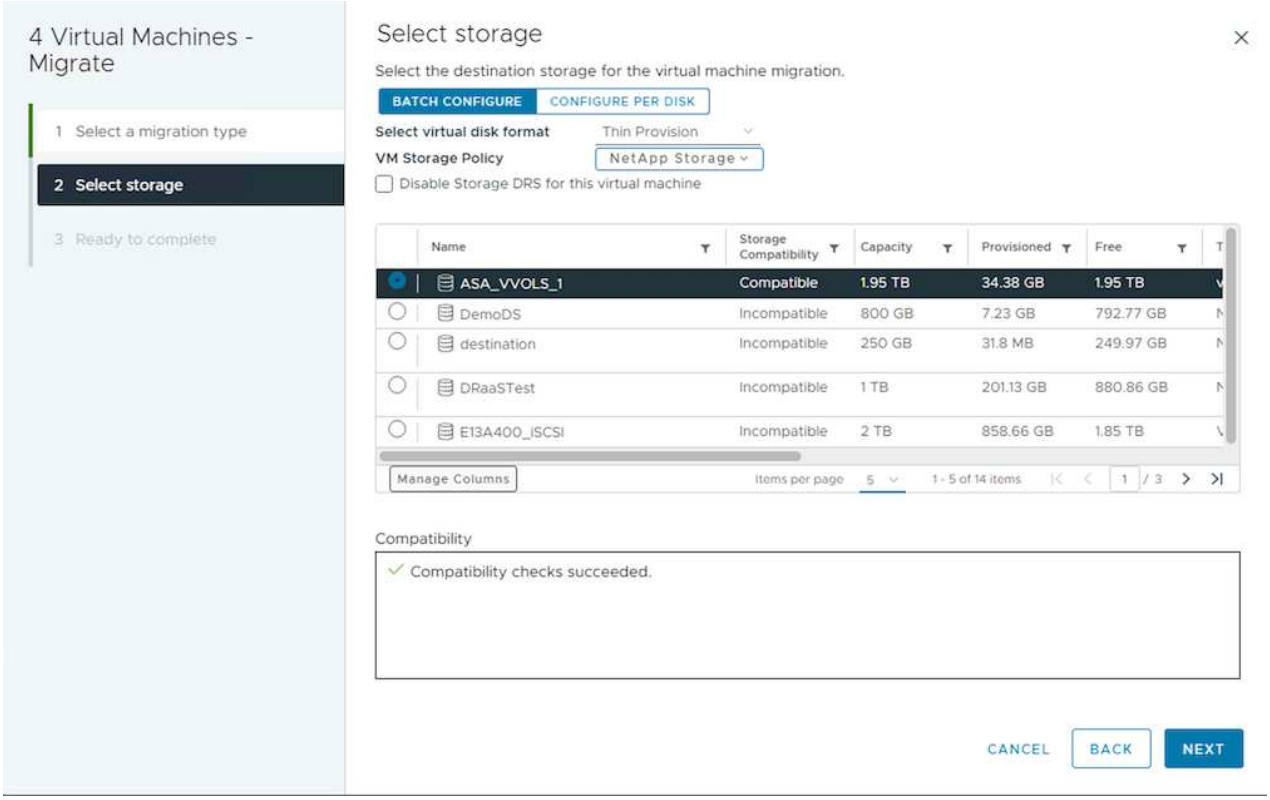
2. Selecione as VMs que precisam ser migradas e clique com o botão direito para selecionar a opção Migrar.



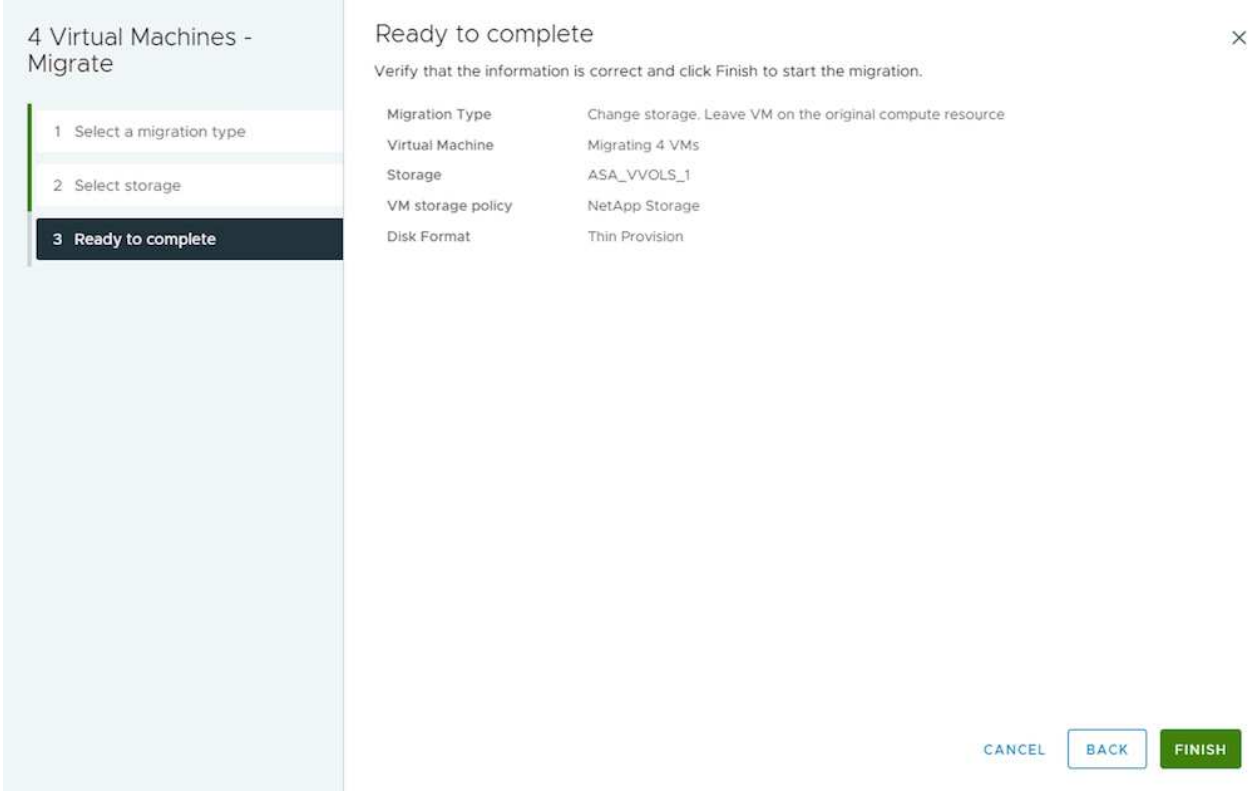
3. Escolha a opção para alterar apenas o armazenamento, clique em Avançar



4. Selecione a Política de Armazenamento de VM desejada e escolha o armazenamento de dados compatível. Clique em Avançar.



5. Revise e clique em Concluir.



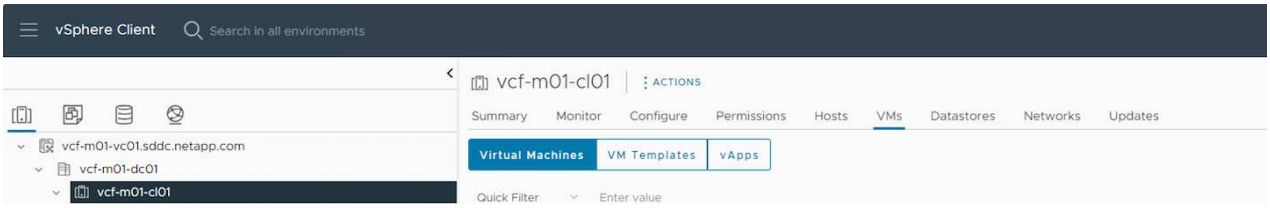
Para migrar VMs usando o PowerCLI, aqui está o script de exemplo.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

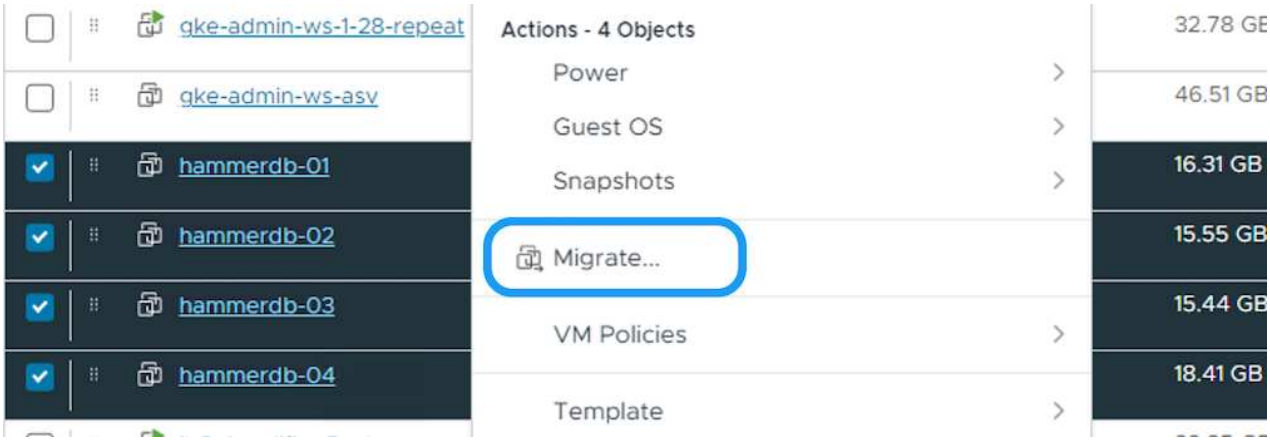
Migração de VMs no mesmo cluster vSphere

Siga o procedimento abaixo para migrar VMs para o novo Datastore usando a interface do usuário.

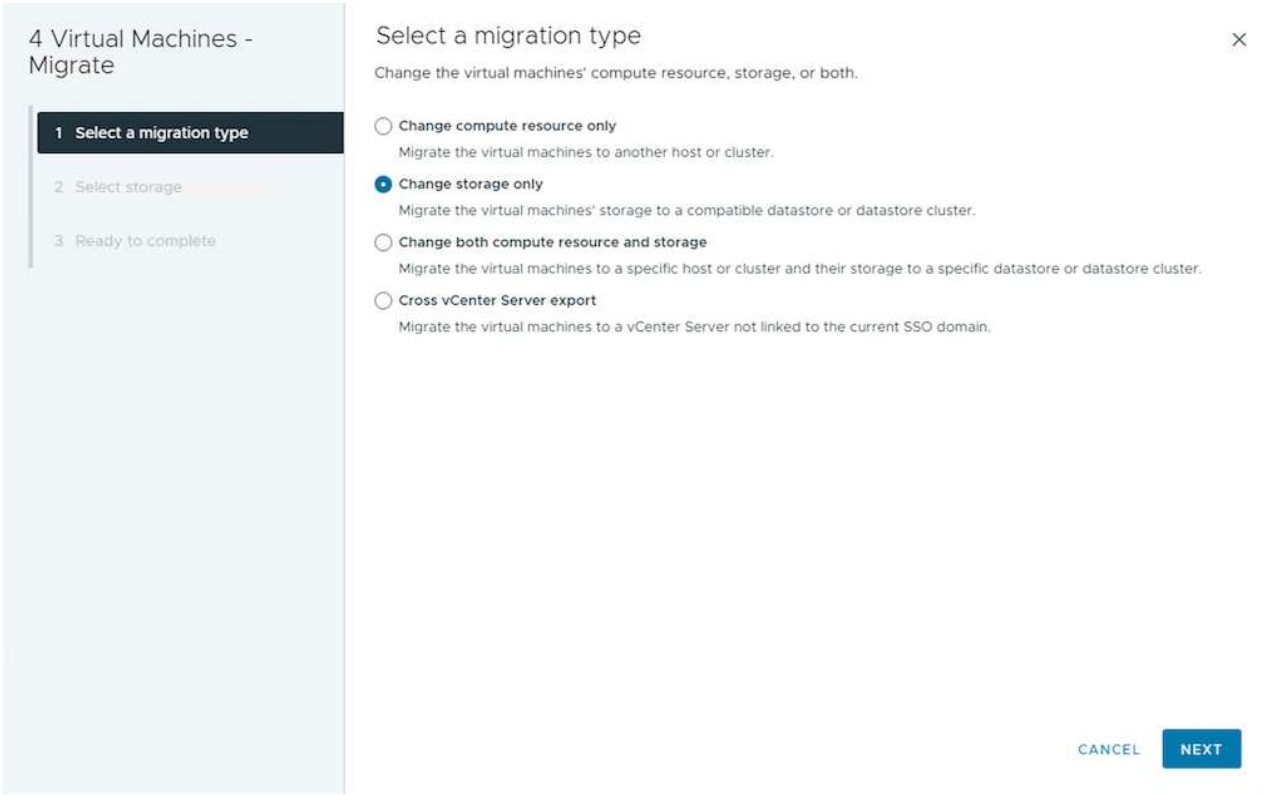
1. Com o vSphere Web Client, selecione o Cluster no inventário de Host e Cluster e clique na guia VMs.



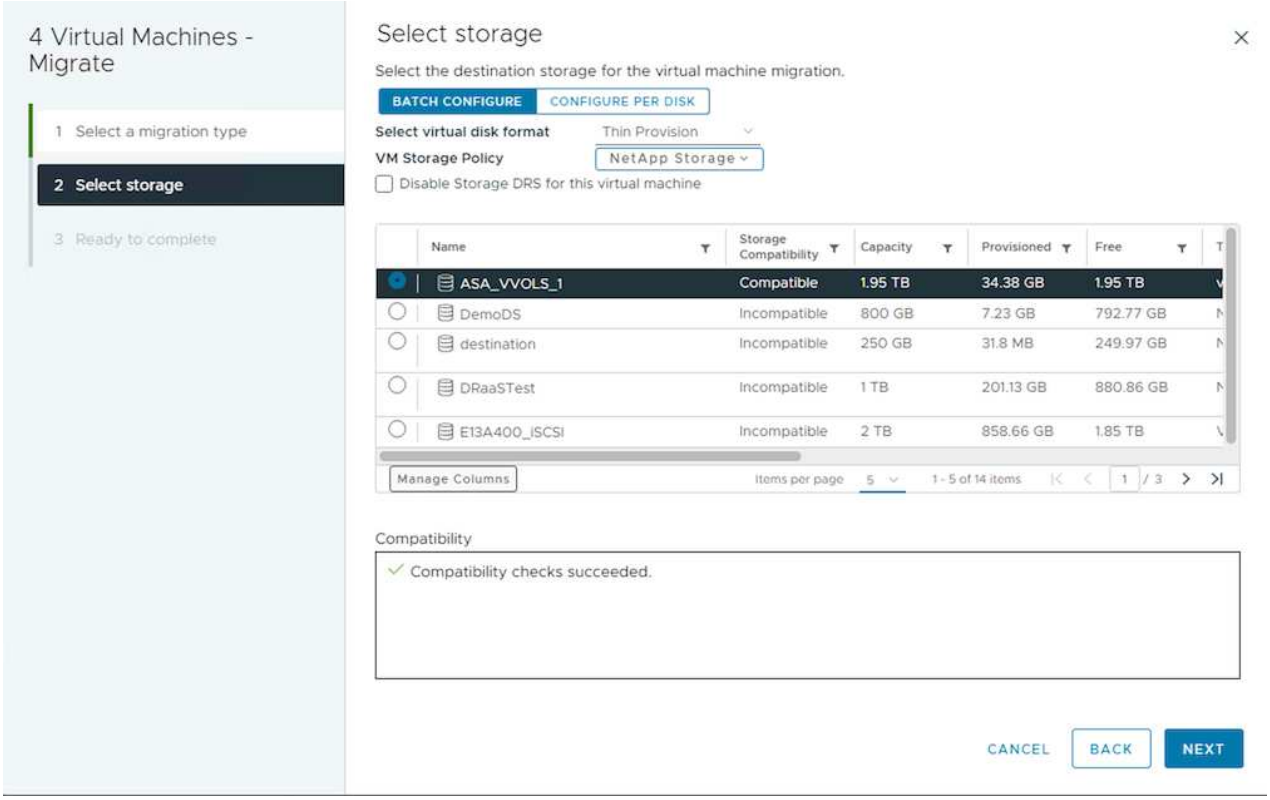
2. Selecione as VMs que precisam ser migradas e clique com o botão direito para selecionar a opção Migrar.



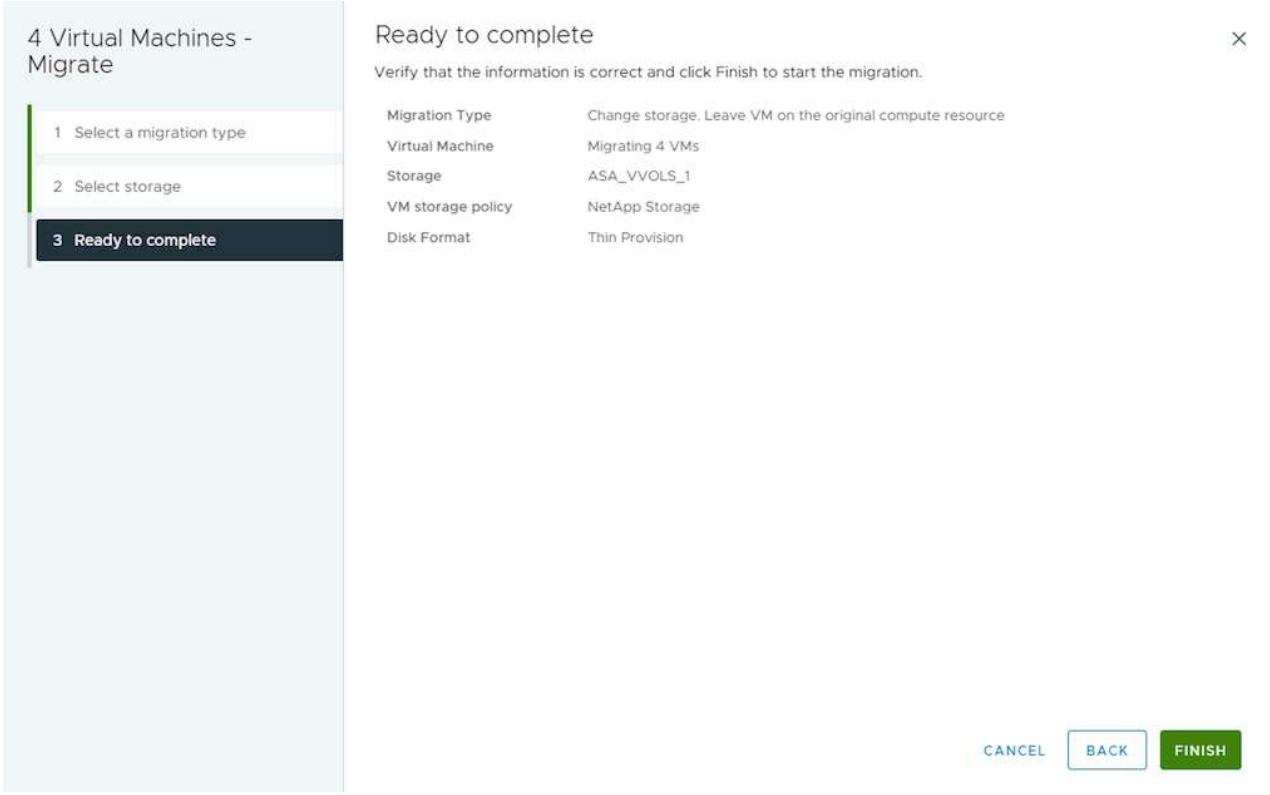
3. Escolha a opção para alterar apenas o armazenamento, clique em Avançar



4. Selecione a Política de Armazenamento de VM desejada e escolha o armazenamento de dados compatível. Clique em Avançar.



5. Revise e clique em Concluir.



Para migrar VMs usando o PowerCLI, aqui está o script de exemplo.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

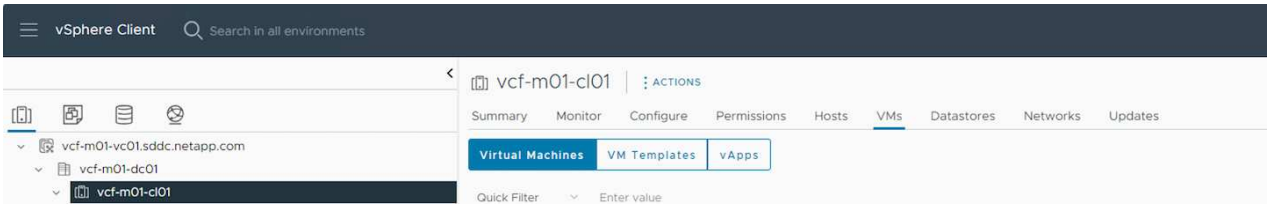
Quando o Cluster de Datastore estiver em uso com DRS (Agendamento Dinâmico de Recursos) de armazenamento totalmente automatizado e ambos os datastores (origem e destino) forem do mesmo tipo (VMFS/NFS/vVol), mantenha ambos os datastores no mesmo cluster de armazenamento e migre as VMs do datastore de origem habilitando o modo de manutenção na origem. A experiência será semelhante à forma como os hosts de computação são gerenciados para manutenção.

Migração de VMs entre vários clusters vSphere

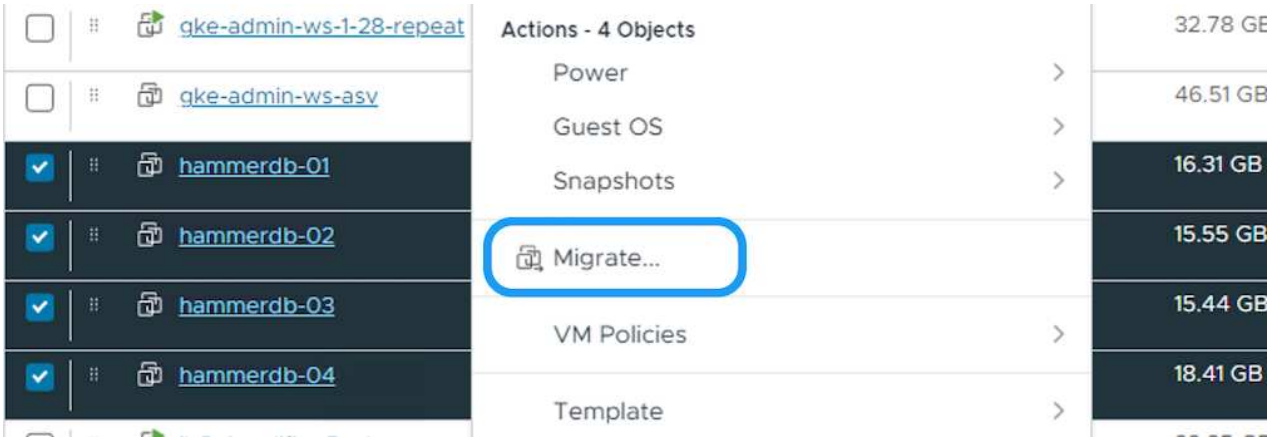
> Referir "Compatibilidade de CPU e compatibilidade aprimorada com vSphere vMotion" quando os hosts de origem e de destino são de famílias ou modelos de CPU diferentes.

Siga o procedimento abaixo para migrar VMs para o novo Datastore usando a interface do usuário.

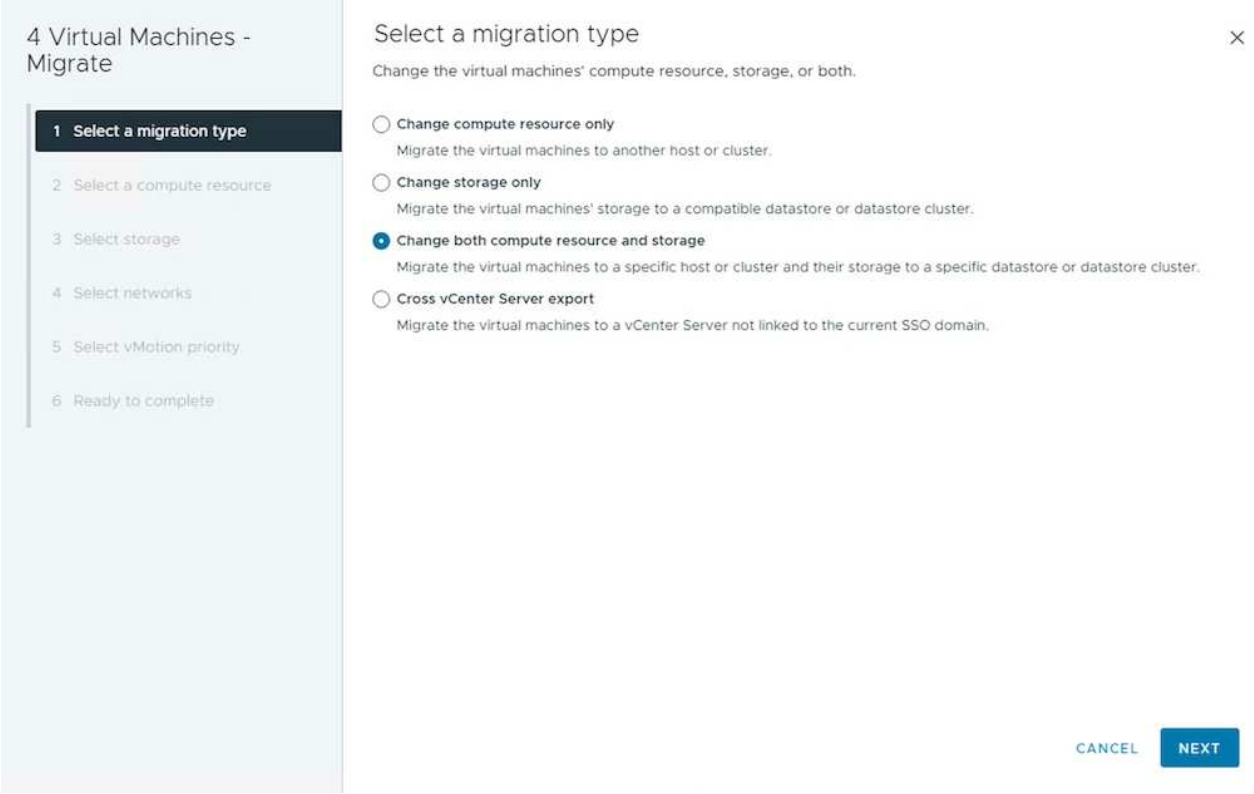
1. Com o vSphere Web Client, selecione o Cluster no inventário de Host e Cluster e clique na guia VMs.



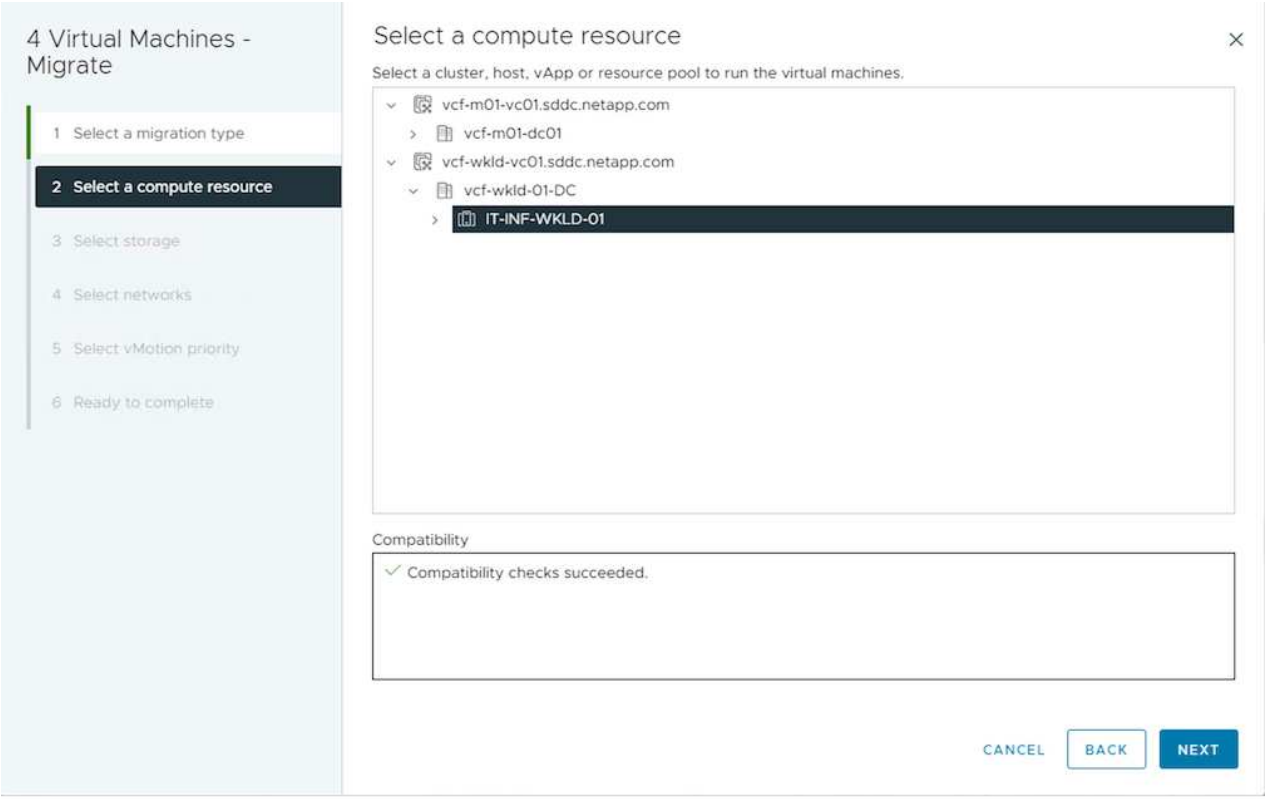
2. Selecione as VMs que precisam ser migradas e clique com o botão direito para selecionar a opção Migrar.



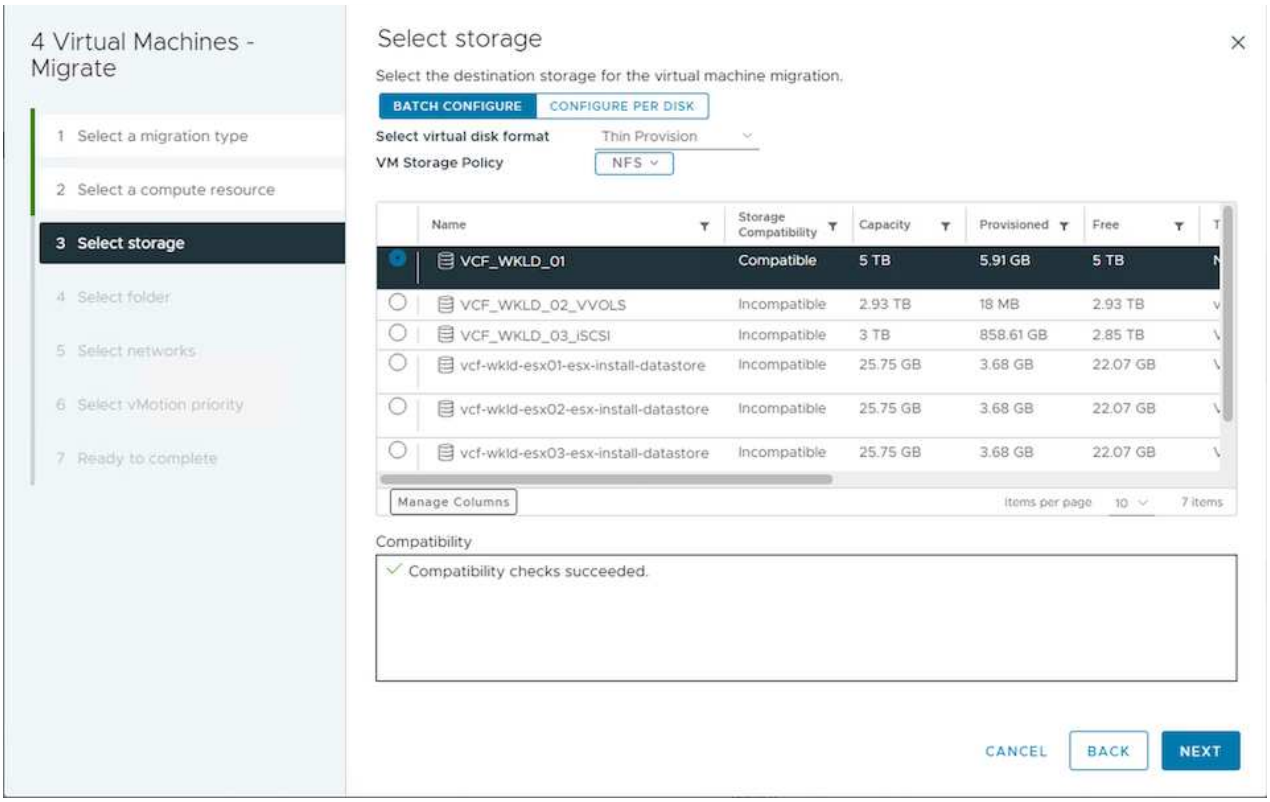
3. Escolha a opção para alterar o recurso de computação e armazenamento, clique em Avançar



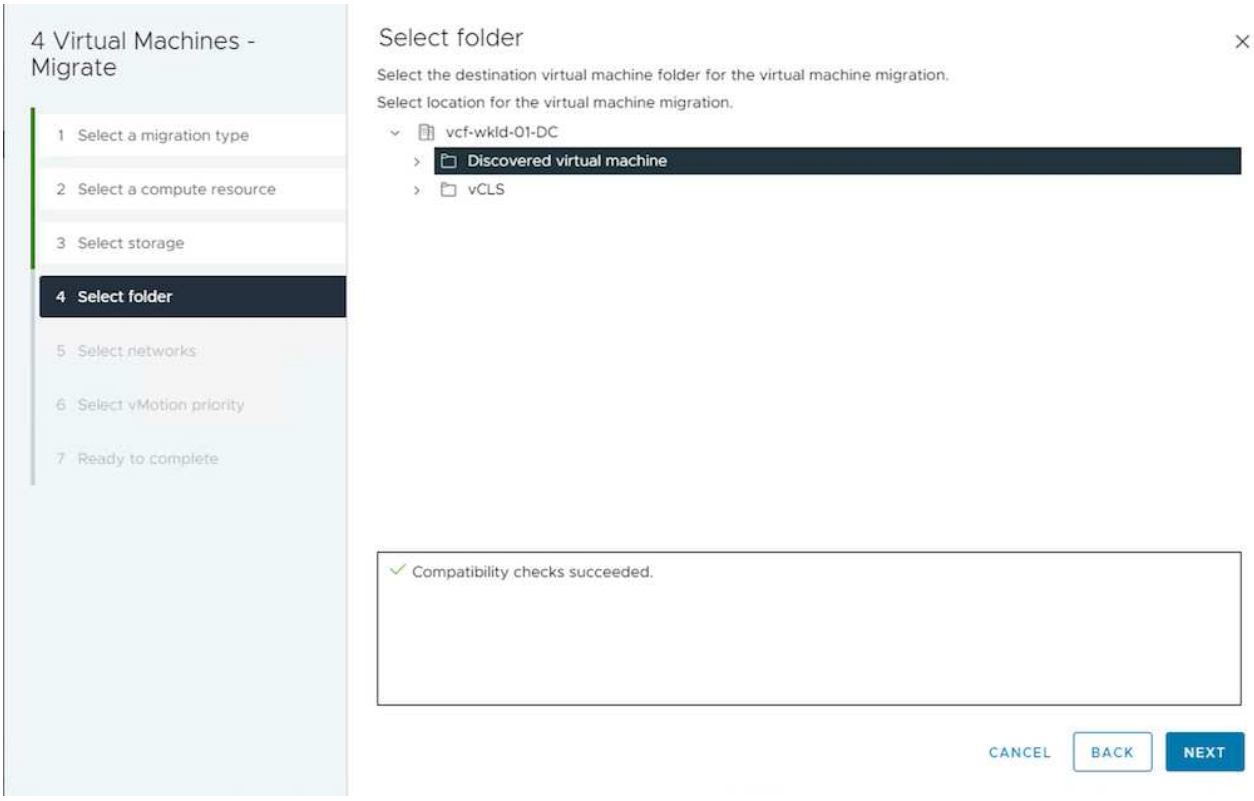
4. Navegue e escolha o cluster certo para migrar.



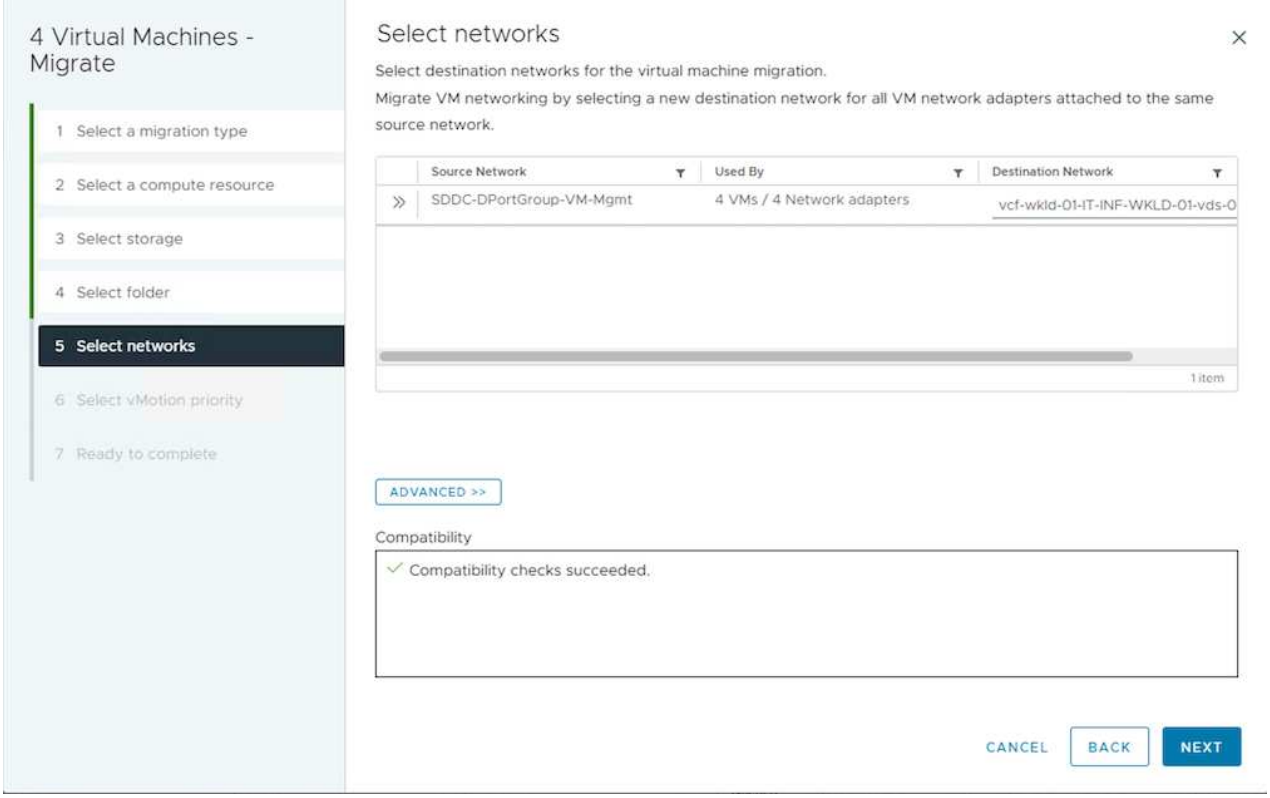
5. Selecione a Política de Armazenamento de VM desejada e escolha o armazenamento de dados compatível. Clique em Avançar.



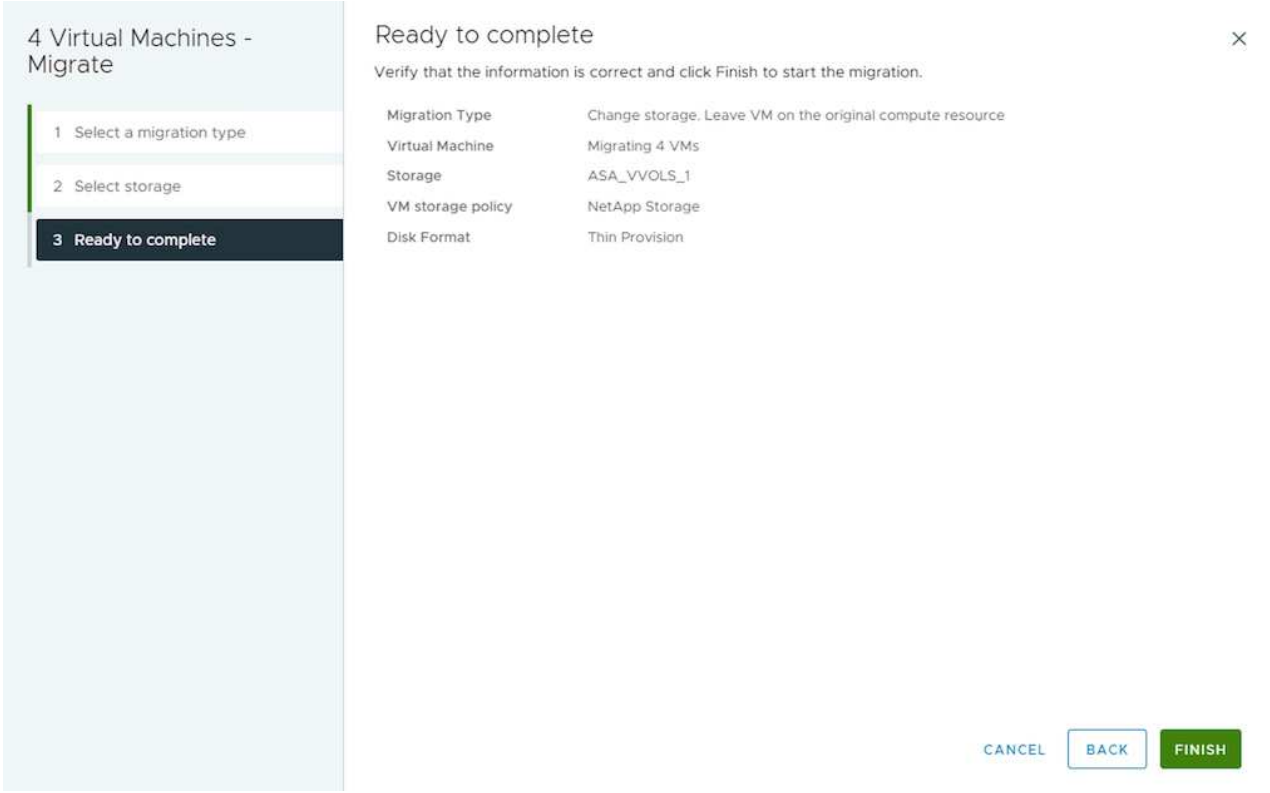
6. Selecione a pasta VM para colocar as VMs de destino.



7. Selecione o grupo de portas de destino.



8. Revise e clique em Concluir.



Para migrar VMs usando o PowerCLI, aqui está o script de exemplo.

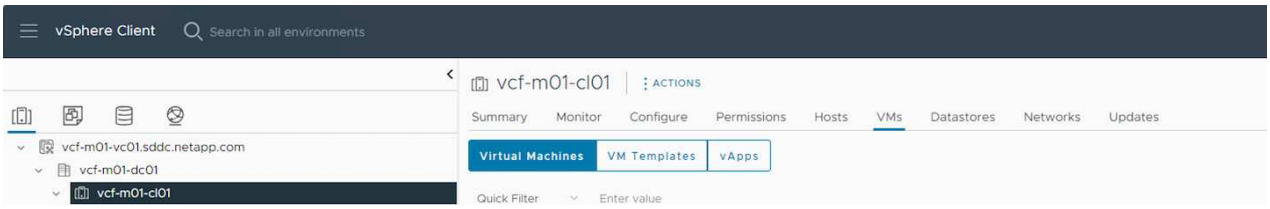
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migração de VMs entre servidores vCenter no mesmo domínio SSO

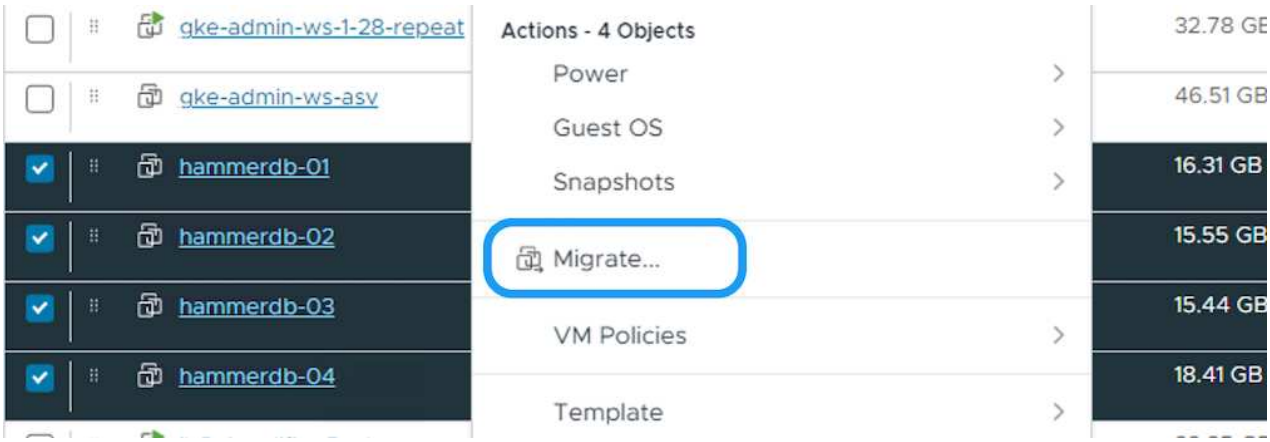
Siga o procedimento abaixo para migrar VMs para o novo servidor vCenter listado na mesma interface do usuário do vSphere Client.

> Para requisitos adicionais, como versões de origem e destino do vCenter, etc., verifique "Documentação do vSphere sobre requisitos para vMotion entre instâncias do servidor vCenter"

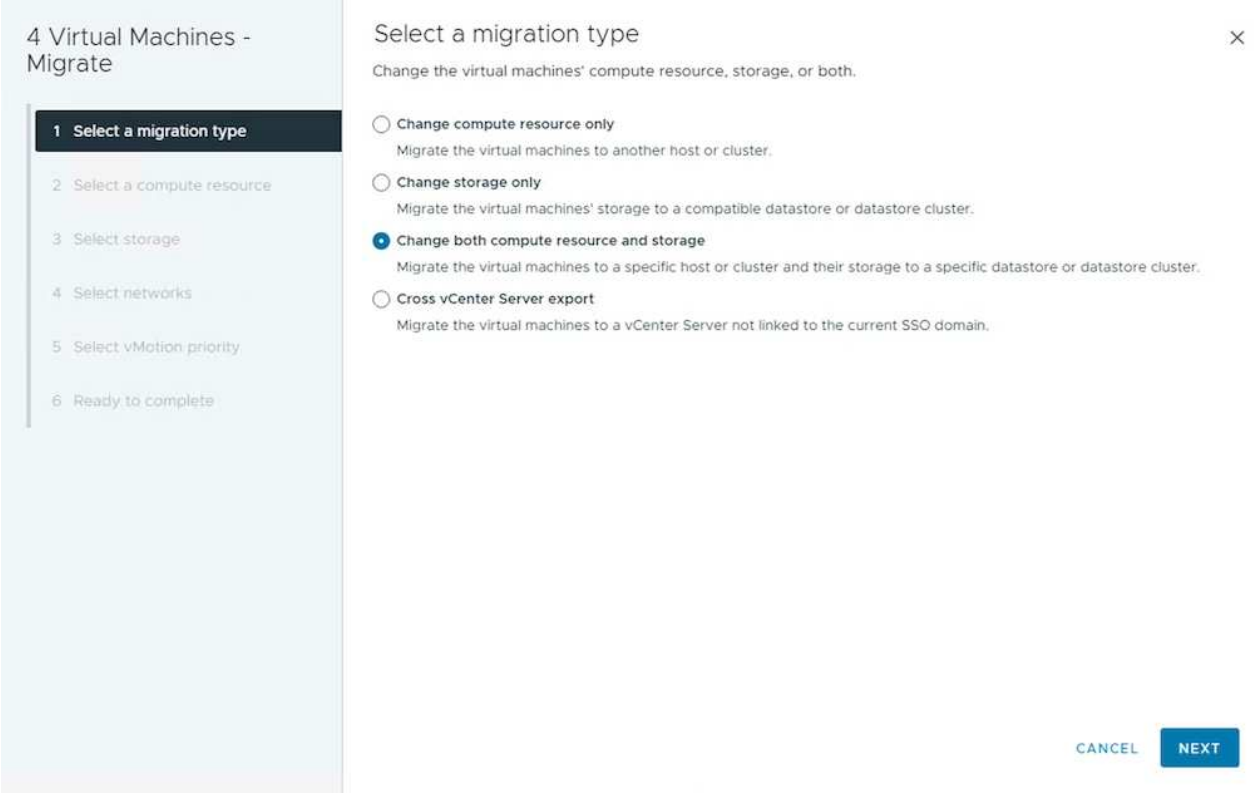
1. Com o vSphere Web Client, selecione o Cluster no inventário de Host e Cluster e clique na guia VMs.



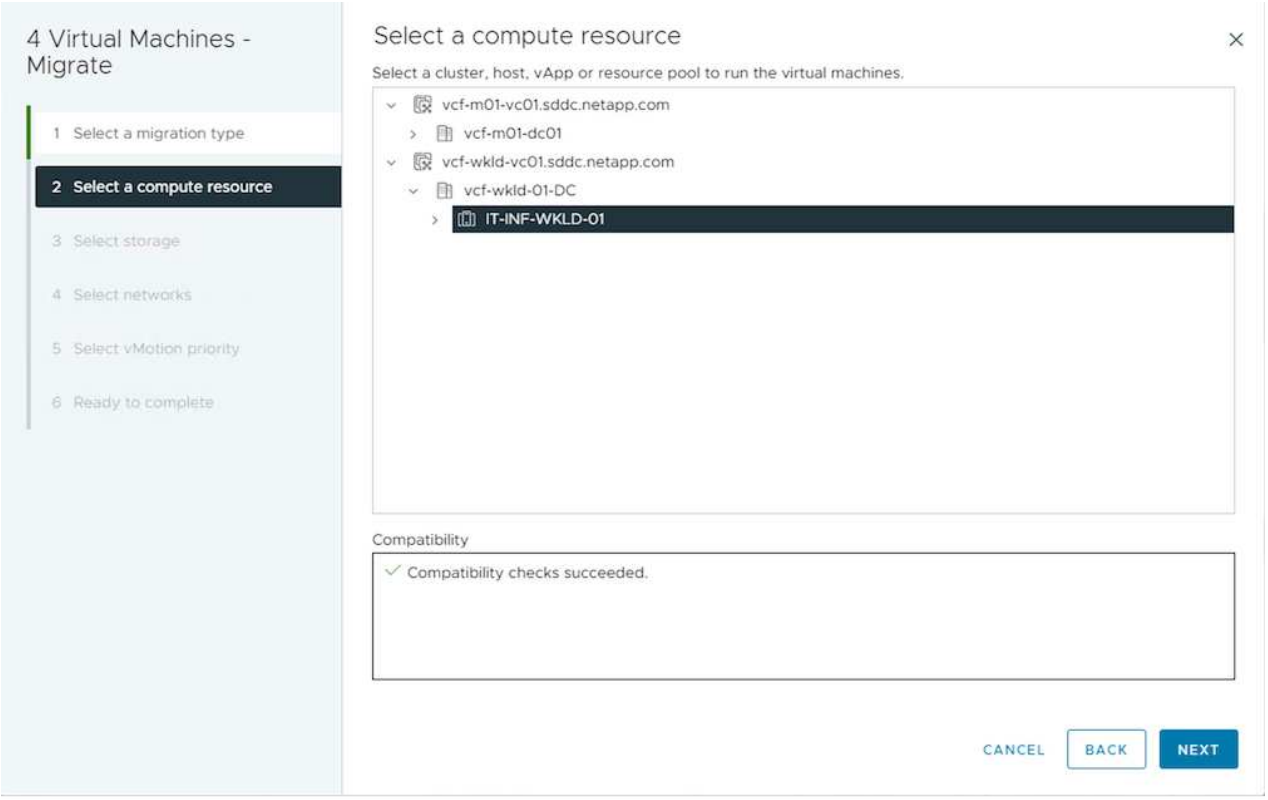
2. Selecione as VMs que precisam ser migradas e clique com o botão direito para selecionar a opção Migrar.



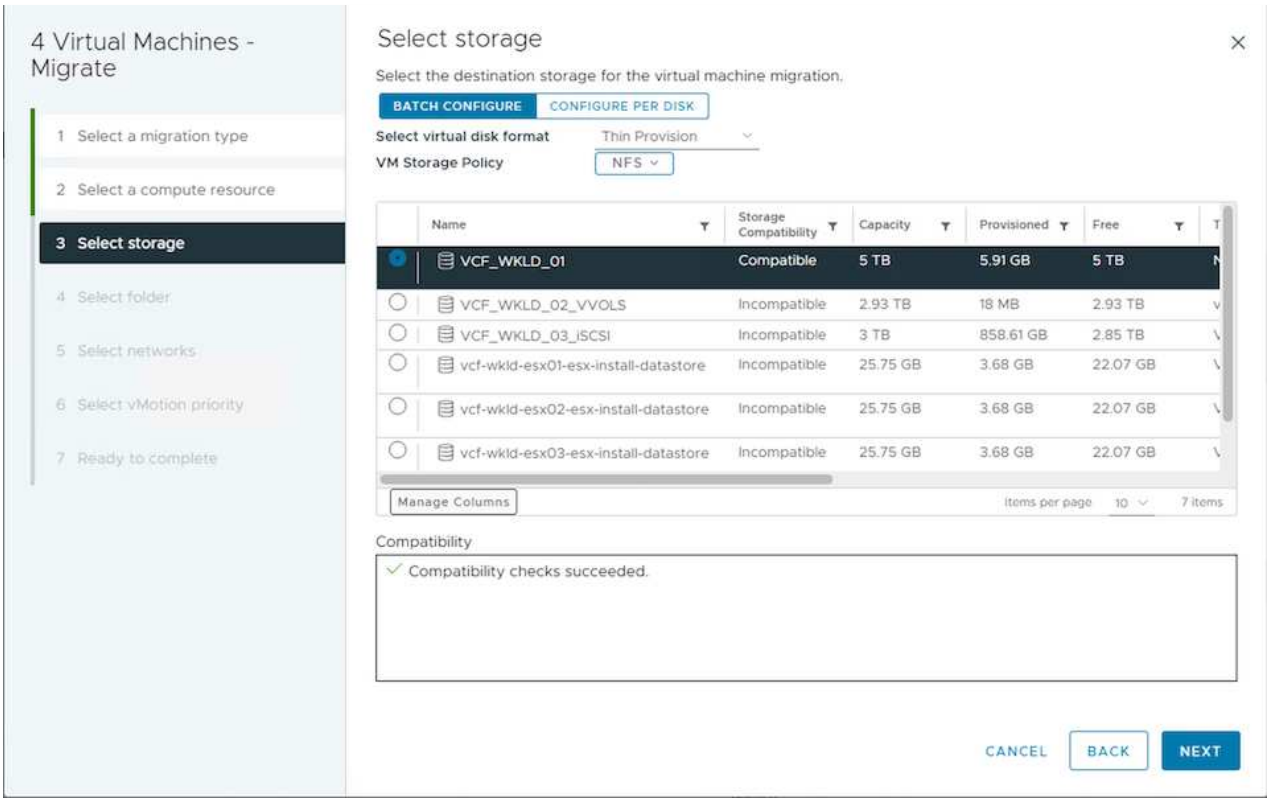
3. Escolha a opção para alterar o recurso de computação e armazenamento, clique em Avançar



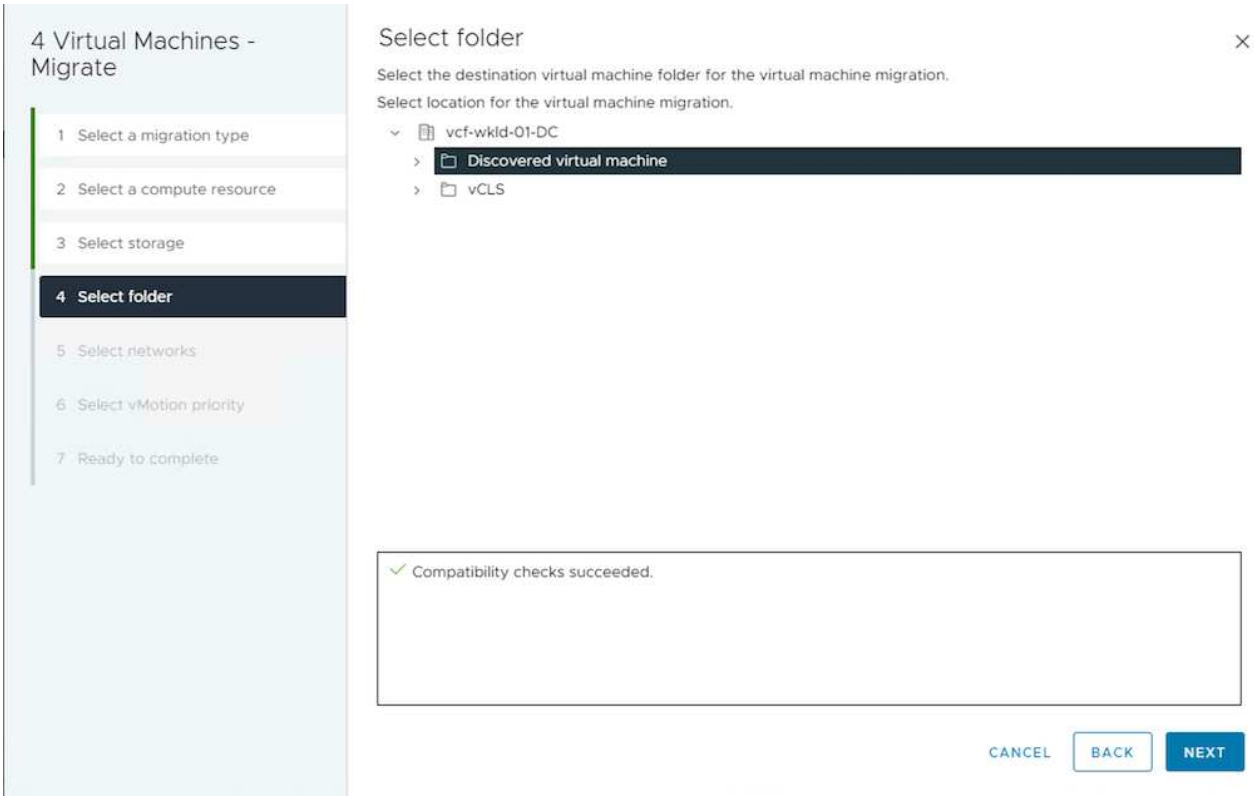
4. Selecione o cluster de destino no servidor vCenter de destino.



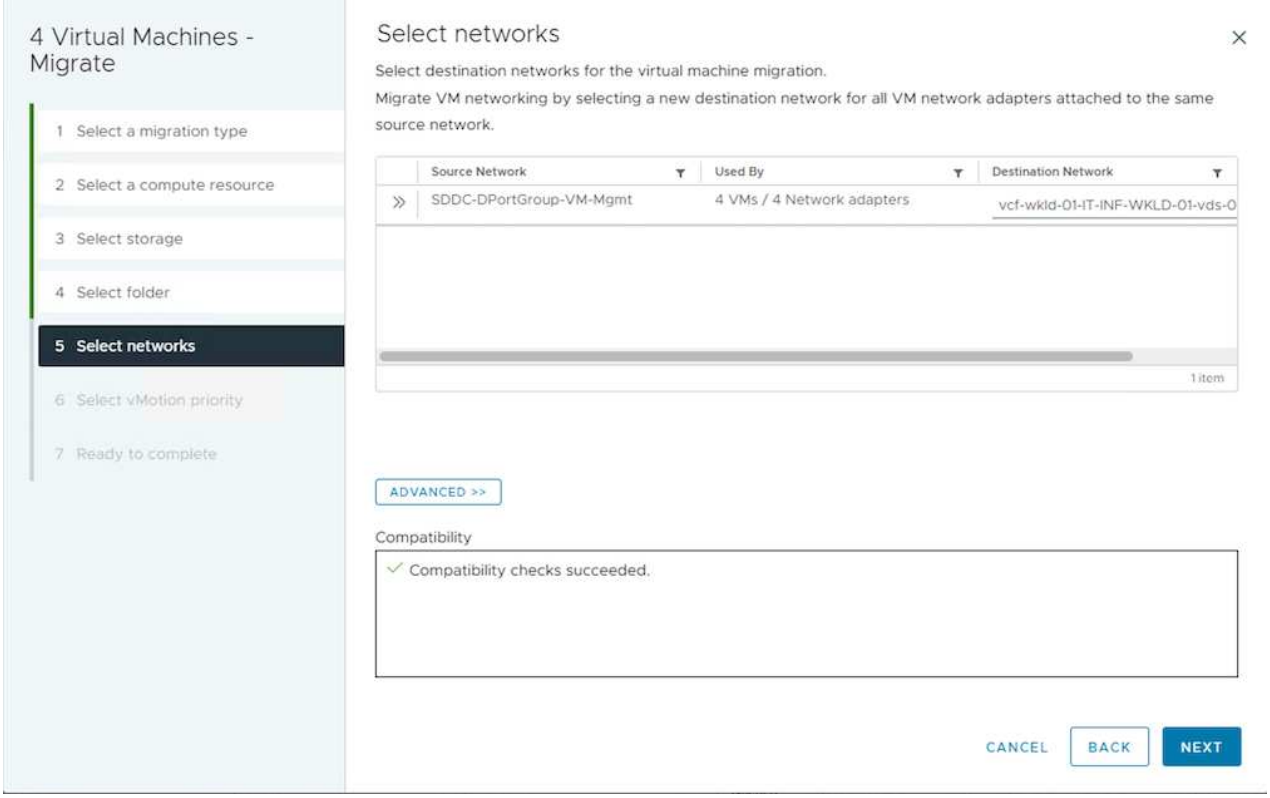
5. Selecione a Política de Armazenamento de VM desejada e escolha o armazenamento de dados compatível. Clique em Avançar.



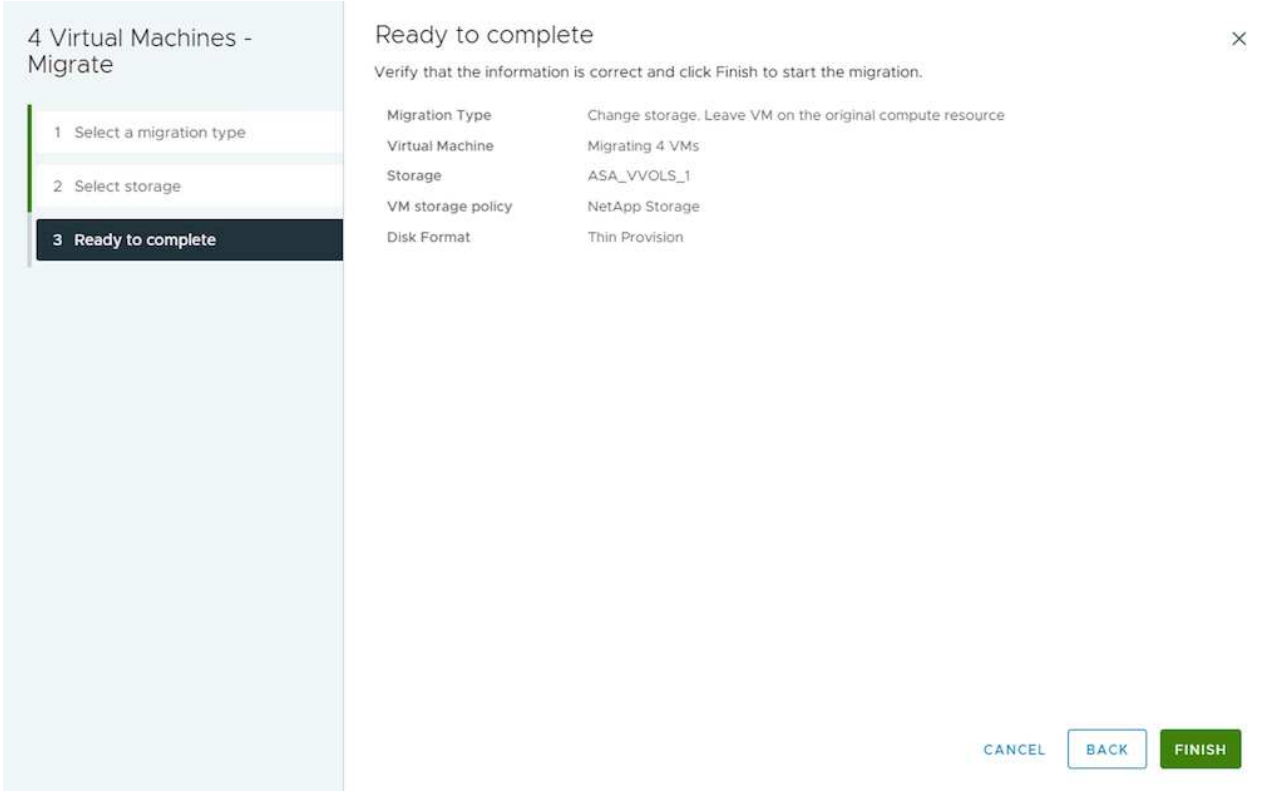
6. Selecione a pasta VM para colocar as VMs de destino.



7. Selecione o grupo de portas de destino.



8. Revise as opções de migração e clique em Concluir.



Para migrar VMs usando o PowerCLI, aqui está o script de exemplo.

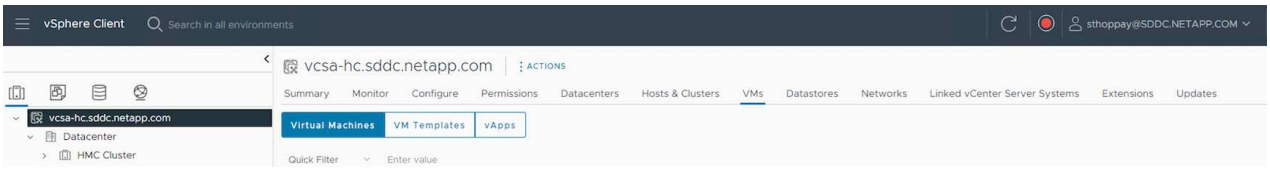
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migração de VMs entre servidores vCenter em diferentes domínios SSO

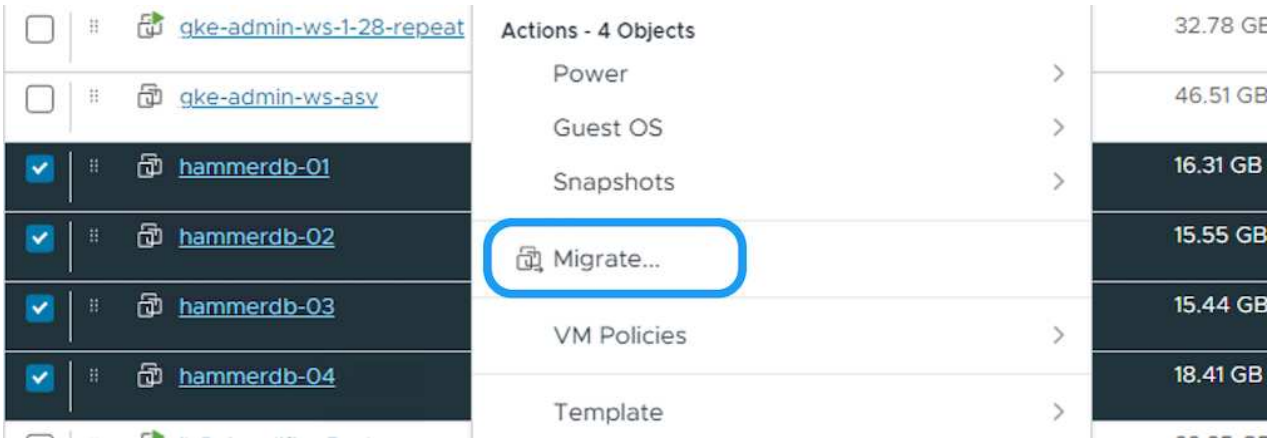
> Este cenário pressupõe que haja comunicação entre os servidores vCenter. Caso contrário, verifique o cenário de localização entre data centers listado abaixo. Para pré-requisitos, verifique "Documentação do vSphere sobre Advanced Cross vCenter vMotion"

Siga o procedimento abaixo para migrar VMs para diferentes servidores vCenter usando a interface do usuário.

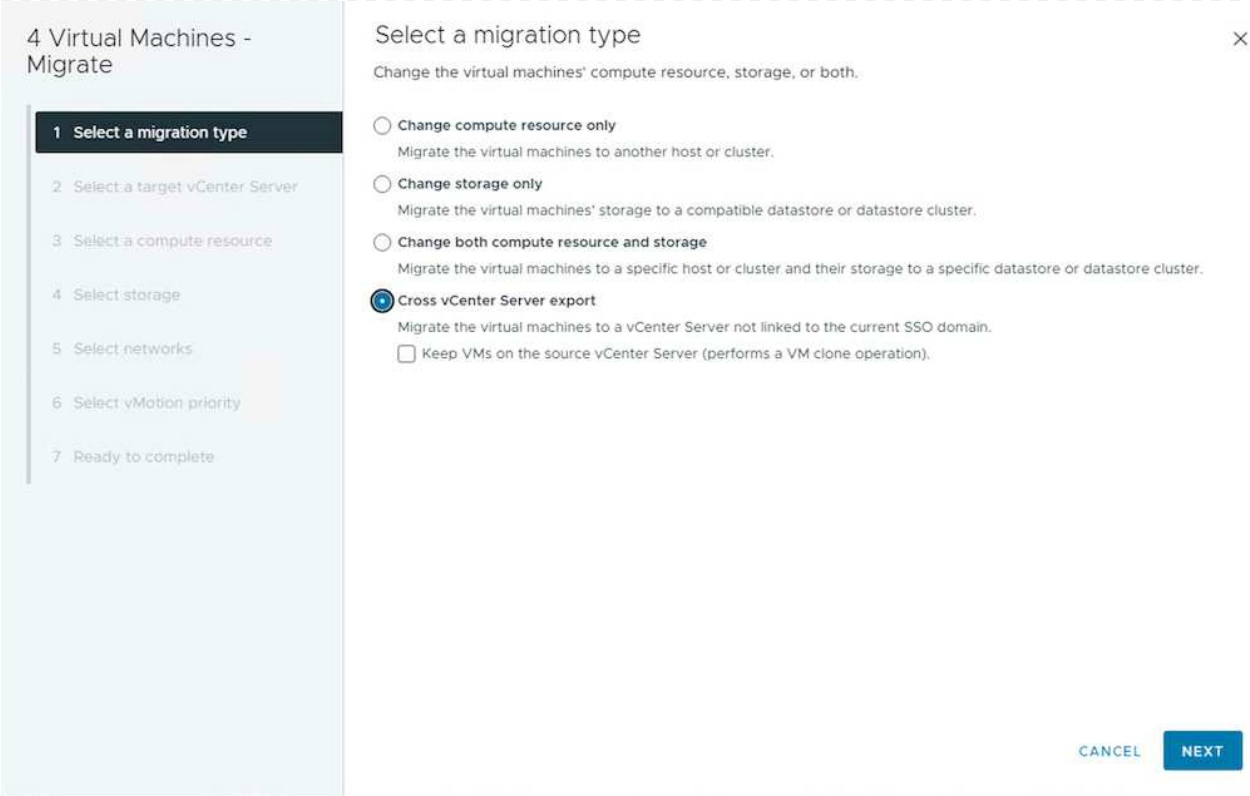
1. Com o vSphere Web Client, selecione o servidor vCenter de origem e clique na aba VMs.



2. Selecione as VMs que precisam ser migradas e clique com o botão direito para selecionar a opção Migrar.

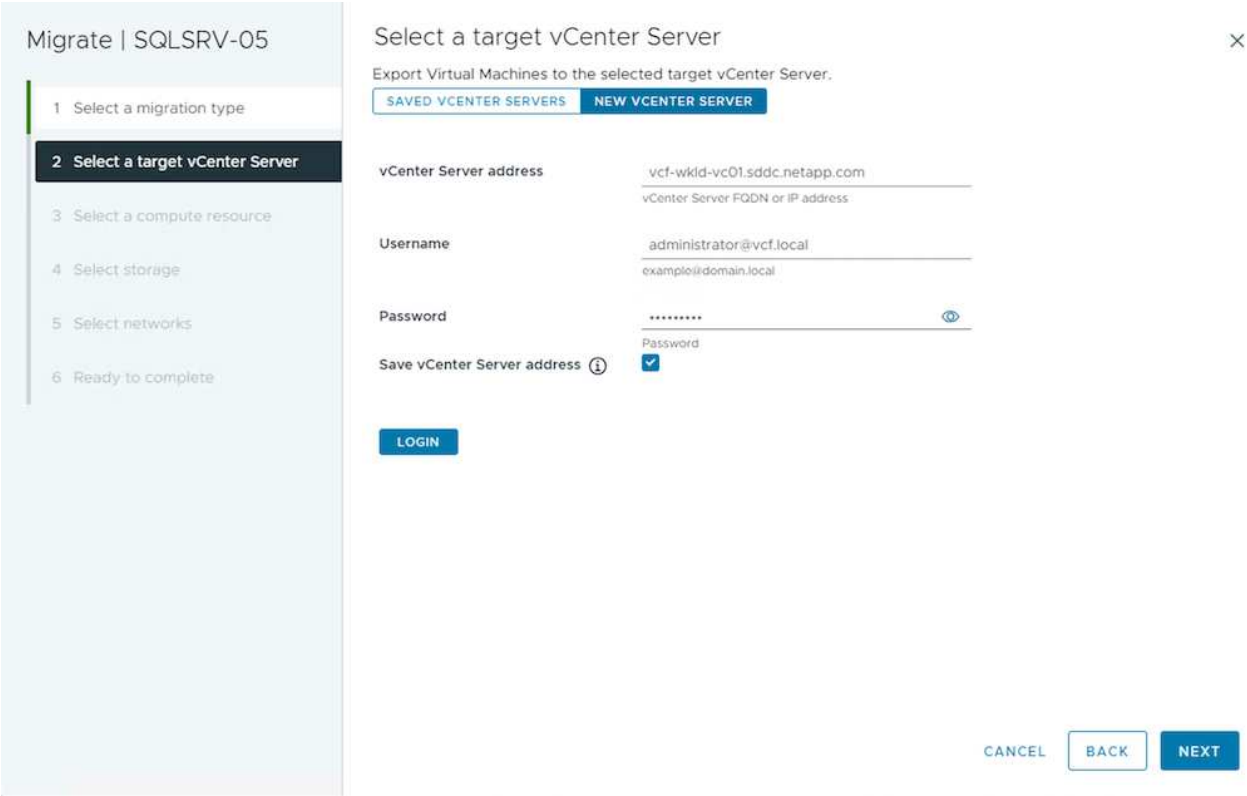


3. Escolha a opção Exportação entre vCenter Servers, clique em Avançar

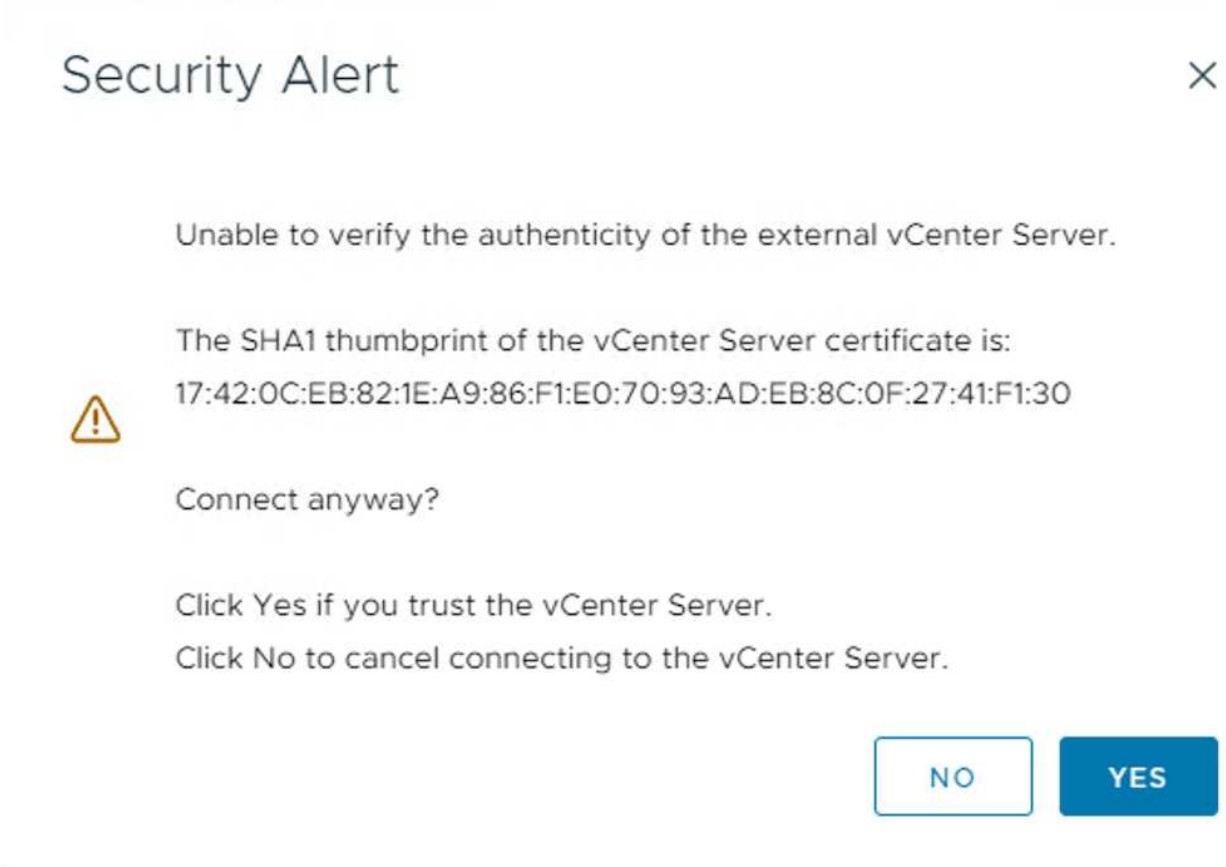


A VM também pode ser importada do servidor vCenter de destino. Para esse procedimento, verifique "Importar ou clonar uma máquina virtual com o Advanced Cross vCenter vMotion"

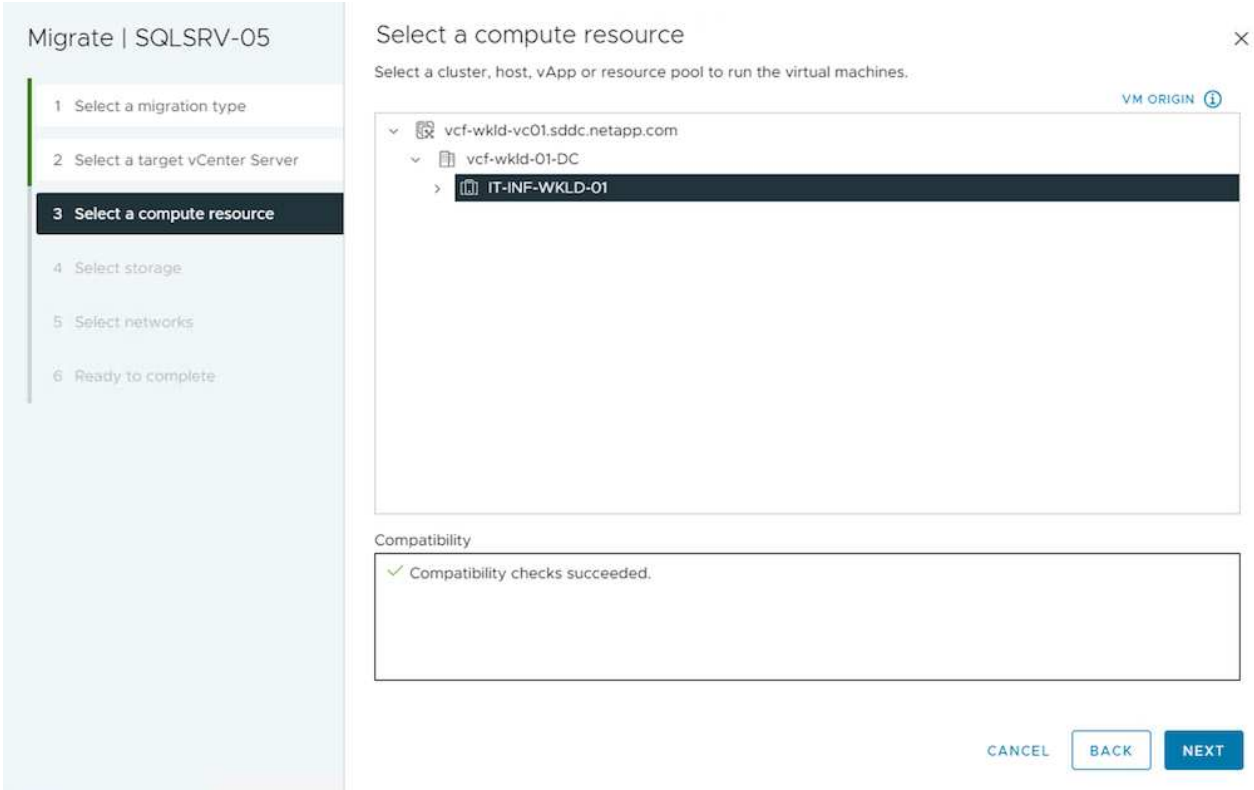
4. Forneça detalhes de credenciais do vCenter e clique em Login.



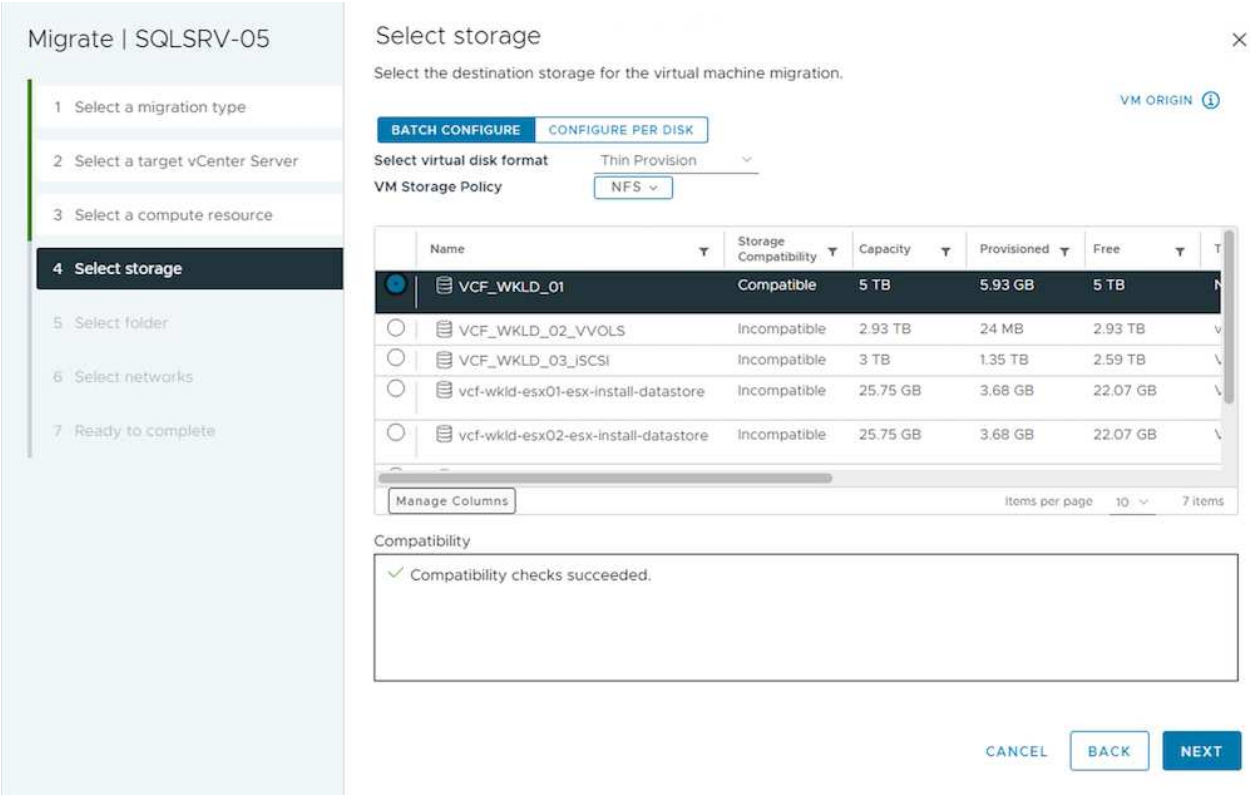
5. Confirme e aceite a impressão digital do certificado SSL do servidor vCenter



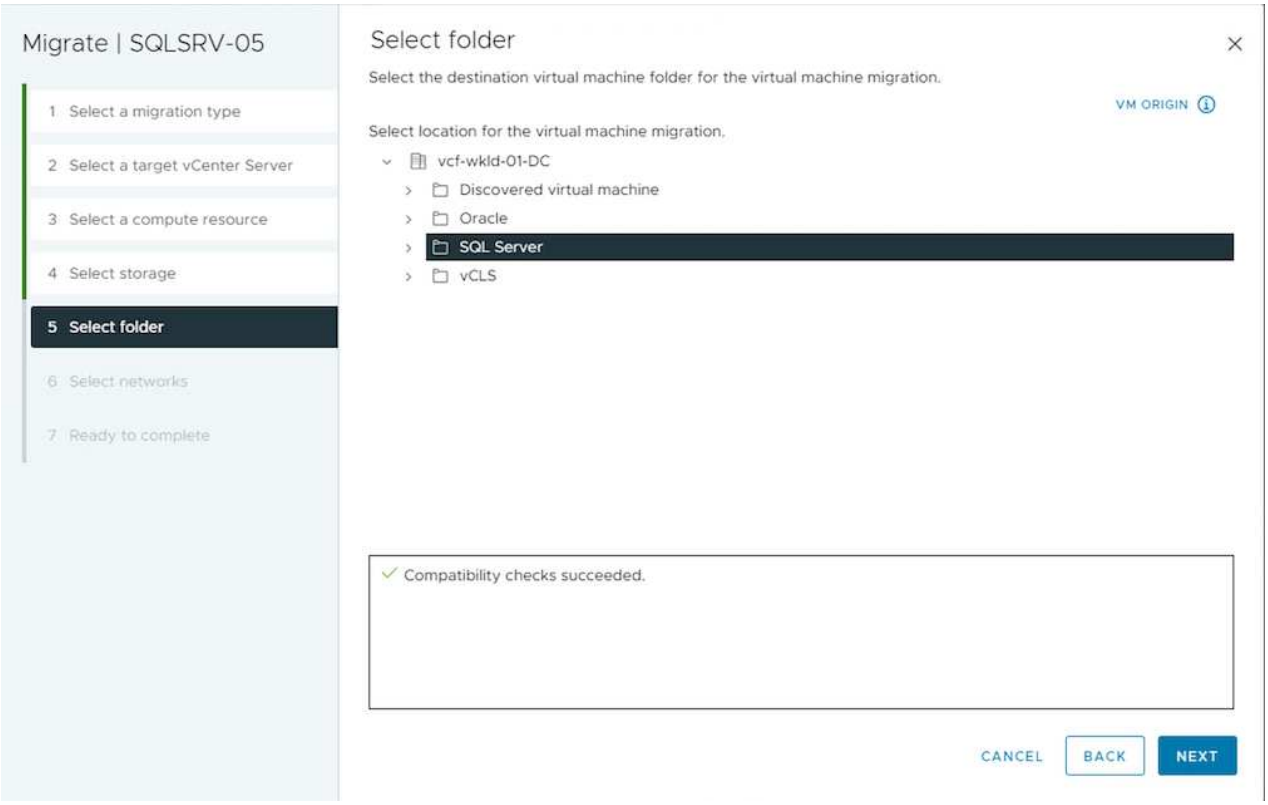
6. Expanda o vCenter de destino e selecione o cluster de computação de destino.



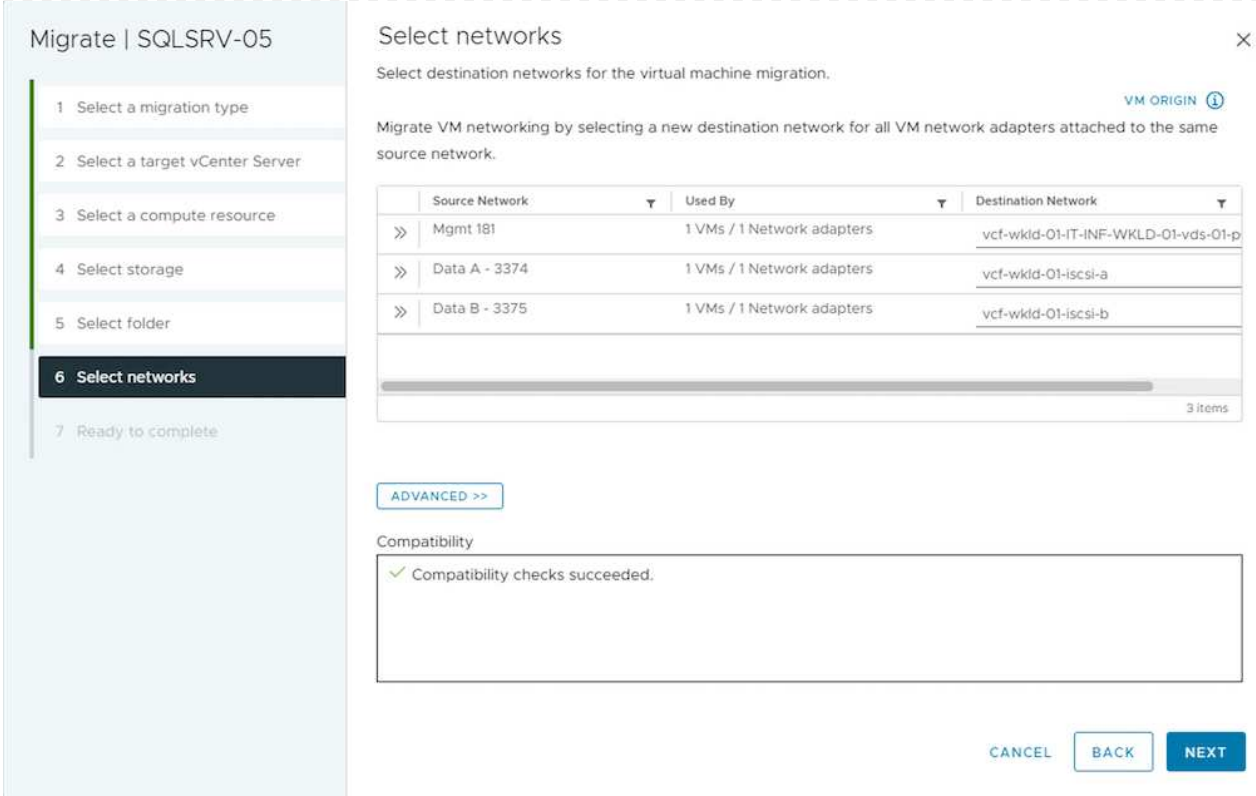
7. Selecione o armazenamento de dados de destino com base na Política de Armazenamento da VM.



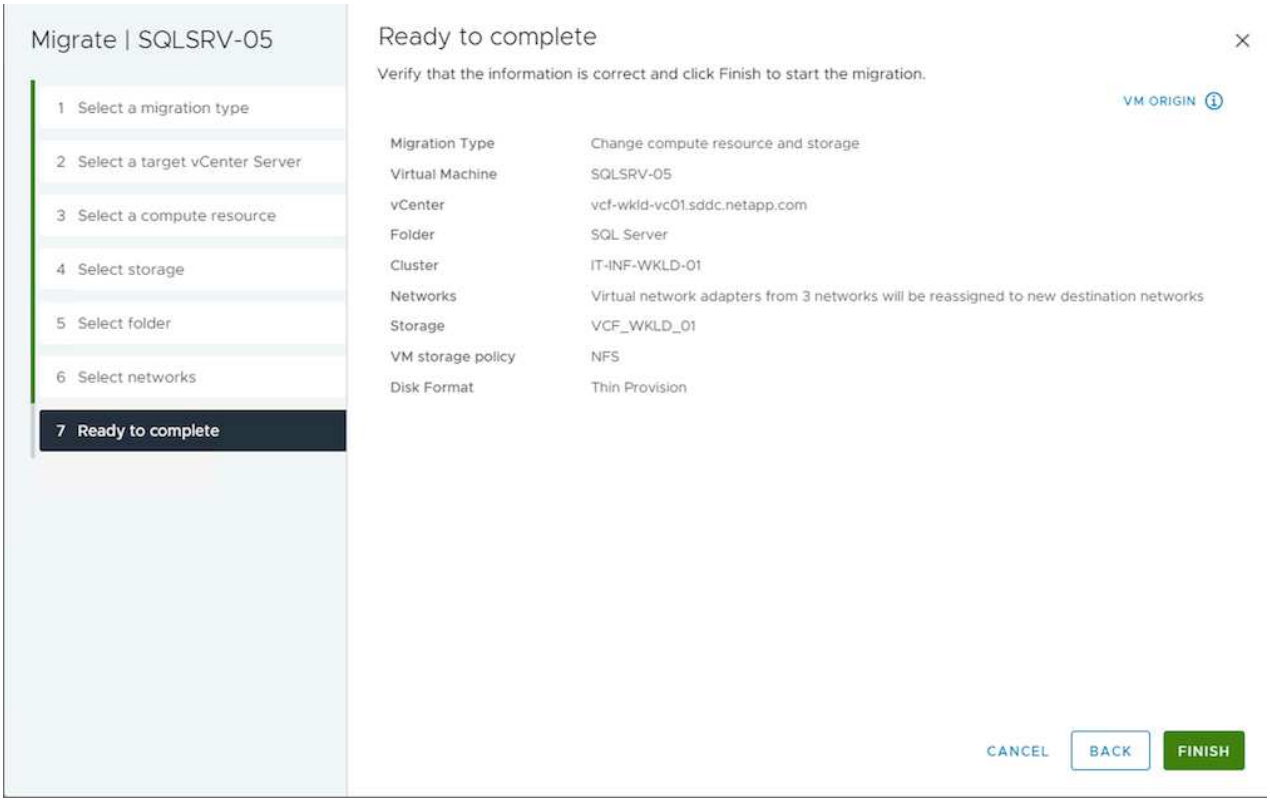
8. Selecione a pasta da VM de destino.



9. Selecione o grupo de portas da VM para cada mapeamento de placa de interface de rede.



10. Revise e clique em Concluir para iniciar o vMotion nos servidores vCenter.



Para migrar VMs usando o PowerCLI, aqui está o script de exemplo.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migração de VMs entre locais de datacenter

- Quando o tráfego da Camada 2 é estendido entre datacenters usando o NSX Federation ou outras opções, siga o procedimento para migrar VMs entre servidores vCenter.
- A HCX oferece vários "tipos de migração" incluindo Replication Assisted vMotion nos datacenters para mover a VM sem qualquer tempo de inatividade.
- "Gerenciador de Recuperação de Site (SRM)"é normalmente destinado a fins de recuperação de desastres e também frequentemente usado para migração planejada utilizando replicação baseada em matriz de armazenamento.
- Uso de produtos de Proteção Contínua de Dados (CDP) "API vSphere para E/S (VAIO)" para interceptar os dados e enviar uma cópia para um local remoto para uma solução de RPO próxima de zero.
- Produtos de backup e recuperação também podem ser utilizados. Mas muitas vezes resulta em um RTO mais longo.
- "Recuperação de Desastres BlueXP como Serviço (DRaaS)"utiliza replicação baseada em matriz de armazenamento e automatiza determinadas tarefas para recuperar as VMs no site de destino.

Migração de VMs em ambiente de nuvem híbrida

- "Configurar o Modo Híbrido Vinculado"e siga o procedimento de"Migração de VMs entre servidores vCenter no mesmo domínio SSO"
- A HCX oferece vários "tipos de migração" incluindo Replication Assisted vMotion nos datacenters para mover a VM enquanto ela estiver ligada.
  - "TR 4942: Migrar cargas de trabalho para o armazenamento de dados FSx ONTAP usando VMware HCX"
  - "TR-4940: Migrar cargas de trabalho para o repositório de dados do Azure NetApp Files usando o VMware HCX - Guia de início rápido"
  - "Migrar cargas de trabalho para o armazenamento de dados do Google Cloud NetApp Volumes no Google Cloud VMware Engine usando o VMware HCX - Guia de início rápido"
- "Recuperação de Desastres BlueXP como Serviço (DRaaS)"utiliza replicação baseada em matriz de armazenamento e automatiza determinadas tarefas para recuperar as VMs no site de destino.
- Com produtos de Proteção Contínua de Dados (CDP) suportados que usam "API vSphere para E/S (VAIO)" para interceptar os dados e enviar uma cópia para um local remoto para uma solução de RPO próxima de zero.

> Quando a VM de origem reside no armazenamento de dados vVol do bloco, ela pode ser replicada com o SnapMirror para o Amazon FSx ONTAP ou Cloud Volumes ONTAP (CVO) em outros provedores de nuvem compatíveis e consumida como volume iSCSI com VMs nativas da nuvem.

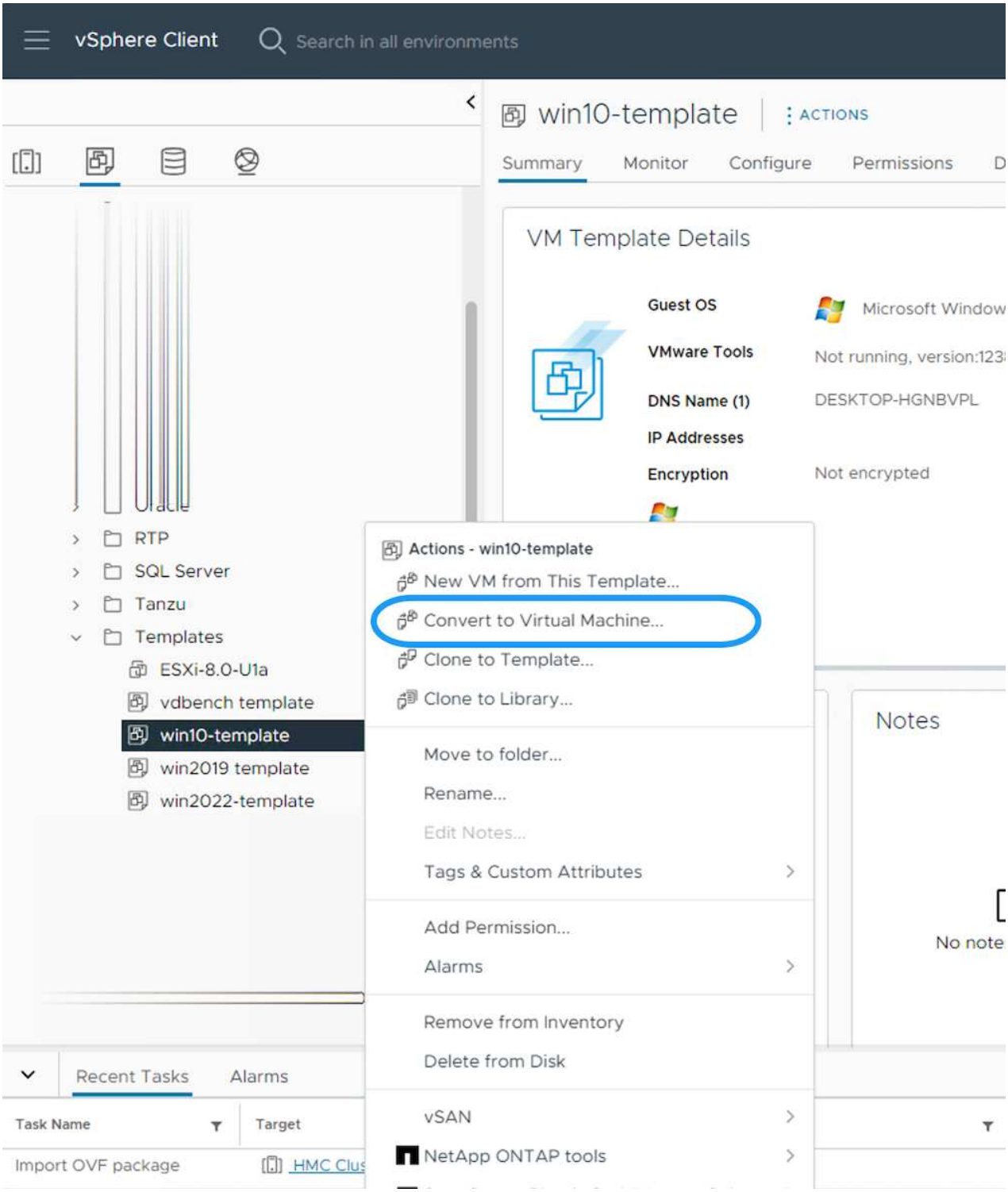
Cenários de migração de modelo de VM

Os modelos de VM podem ser gerenciados pelo vCenter Server ou por uma biblioteca de conteúdo. Distribuição de modelos de VM, modelos OVF e OVA, outros tipos de arquivos são gerenciados publicando-os na biblioteca de conteúdo local e bibliotecas de conteúdo remotas podem assiná-los.

- Os modelos de VM armazenados no inventário do vCenter podem ser convertidos em VM e usar as opções de migração de VM.
- Modelos OVF e OVA, outros tipos de arquivos armazenados na biblioteca de conteúdo podem ser clonados para outras bibliotecas de conteúdo.
- Os modelos de VM da biblioteca de conteúdo podem ser hospedados em qualquer armazenamento de dados e precisam ser adicionados à nova biblioteca de conteúdo.

Migração de modelos de VM hospedados no armazenamento de dados

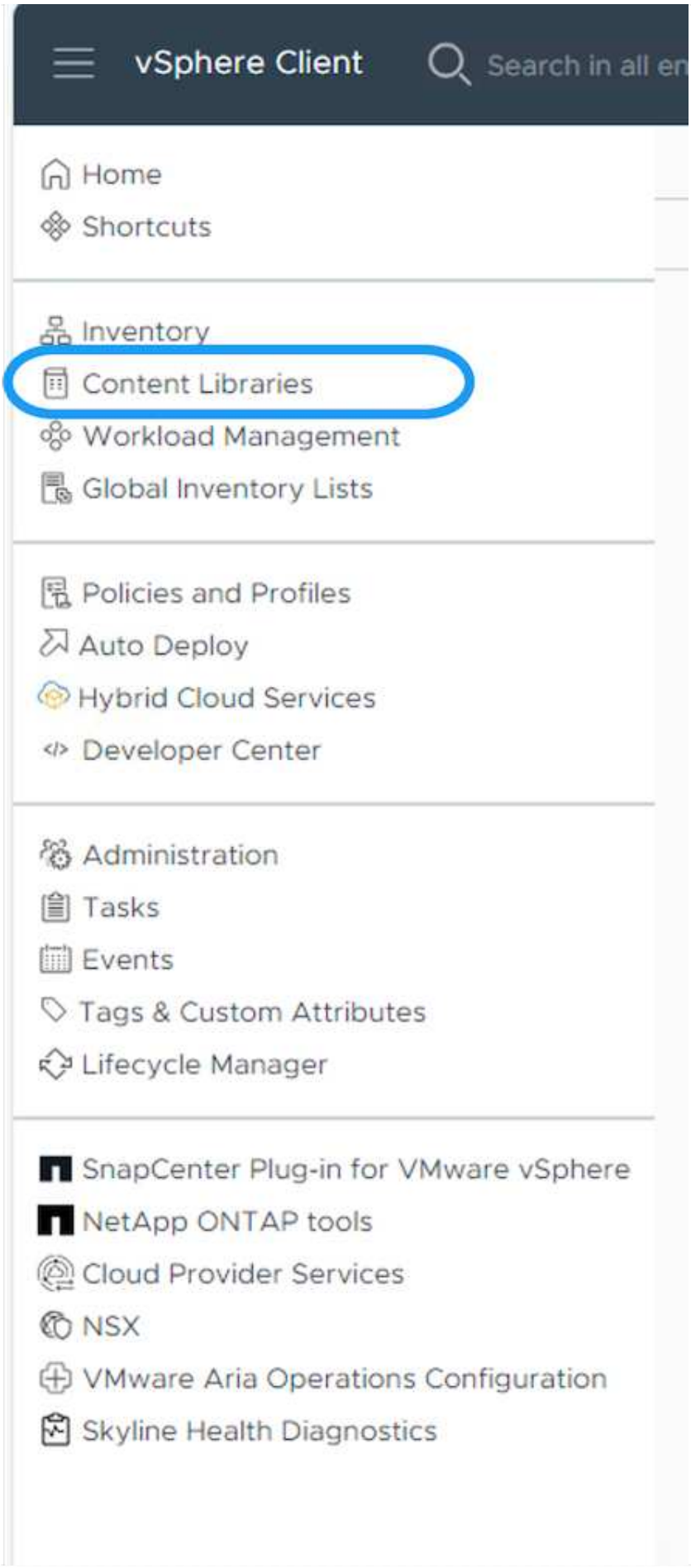
1. No vSphere Web Client, clique com o botão direito do mouse no modelo de VM na visualização da pasta VM e Modelos e selecione a opção para converter para VM.



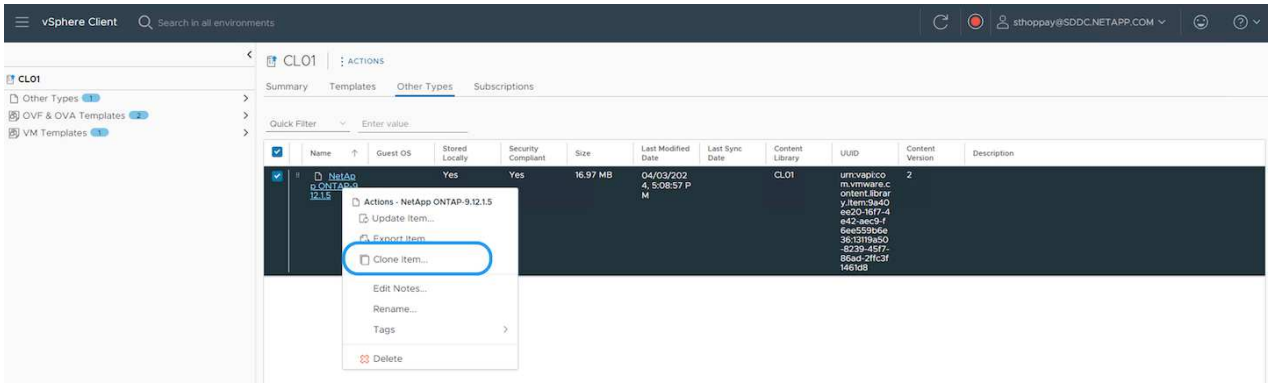
2. Após a conversão como VM, siga as opções de migração de VM.

Clone de itens da Biblioteca de Conteúdo

1. No vSphere Web Client, selecione Bibliotecas de conteúdo

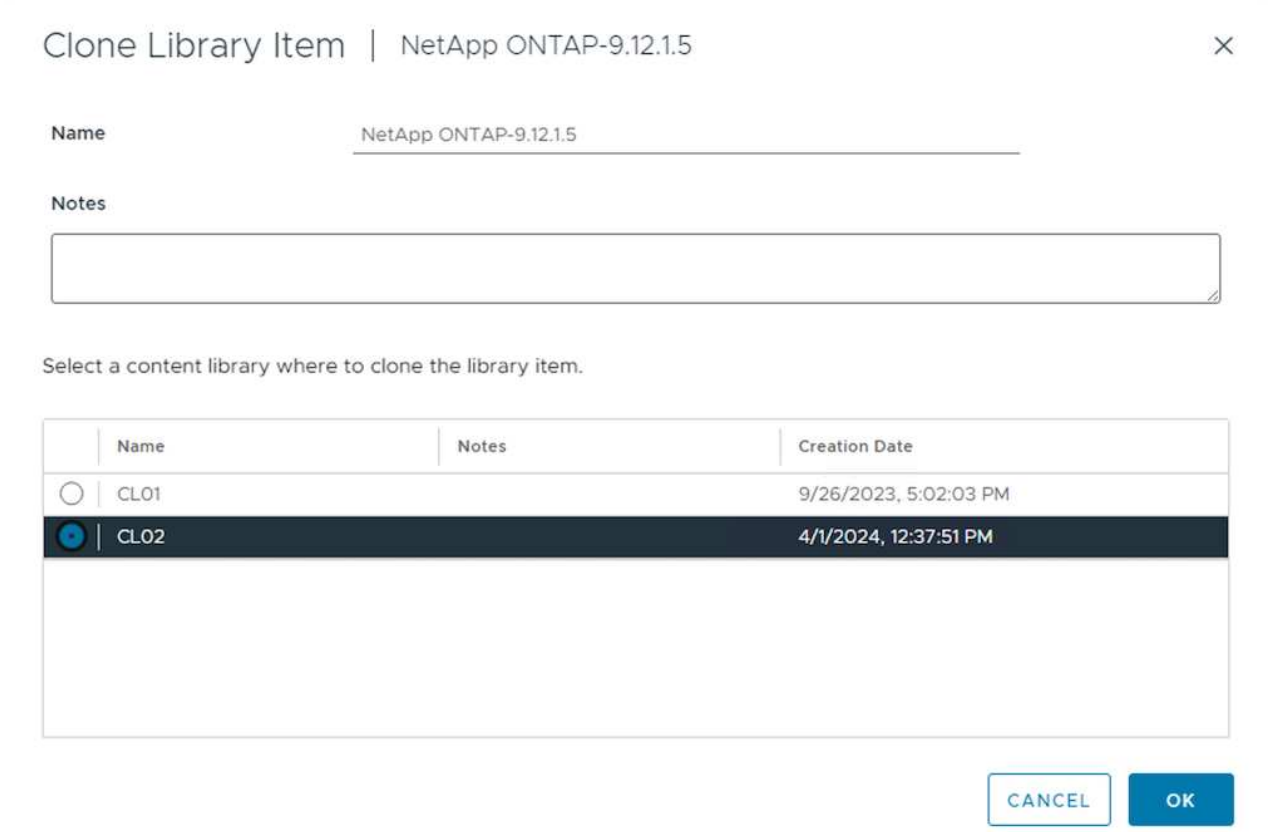

vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

2. Selecione a biblioteca de conteúdo na qual o item que você deseja clonar
3. Clique com o botão direito do mouse no item e clique em Clonar Item.

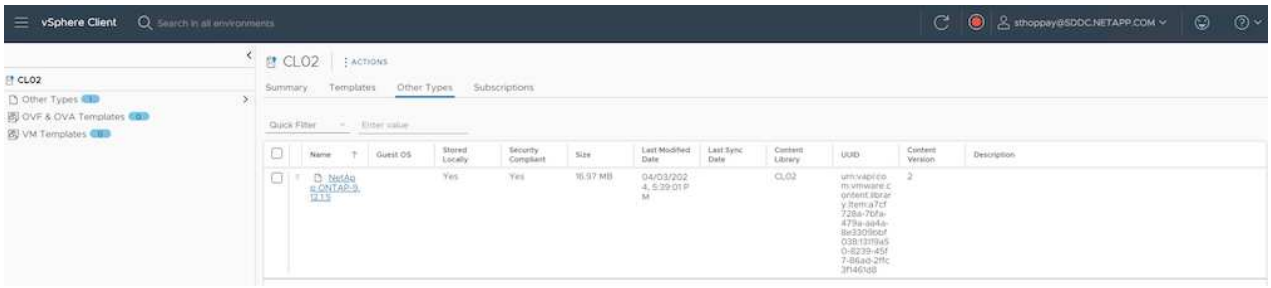


Se estiver usando o menu de ação, certifique-se de que o objeto de destino correto esteja listado para executar a ação.

4. Selecione a biblioteca de conteúdo de destino e clique em OK.



5. Valide se o item está disponível na biblioteca de conteúdo de destino.

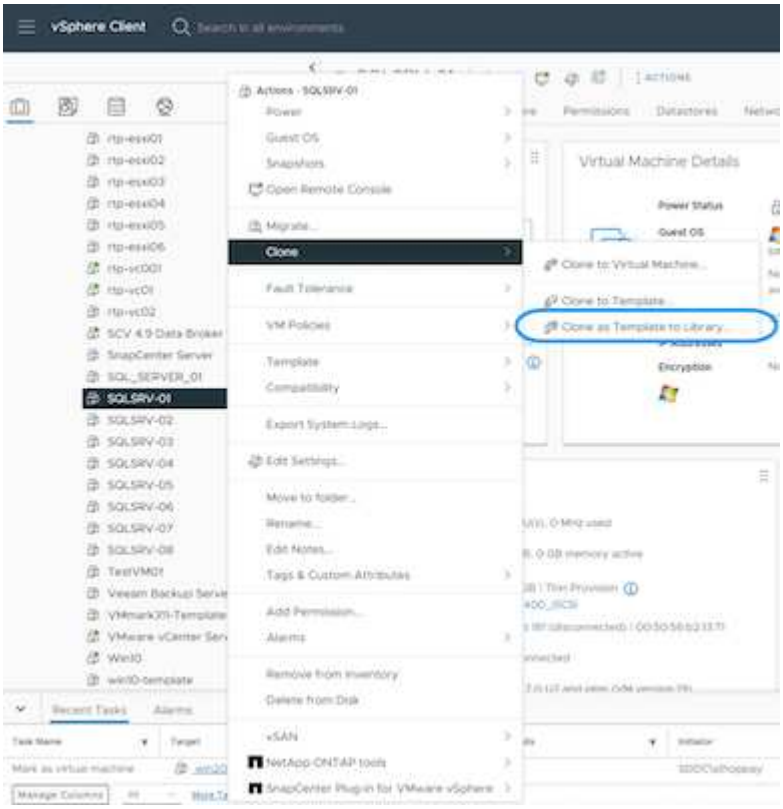


Aqui está o script de exemplo do PowerCLI para copiar os itens da biblioteca de conteúdo CL01 para CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

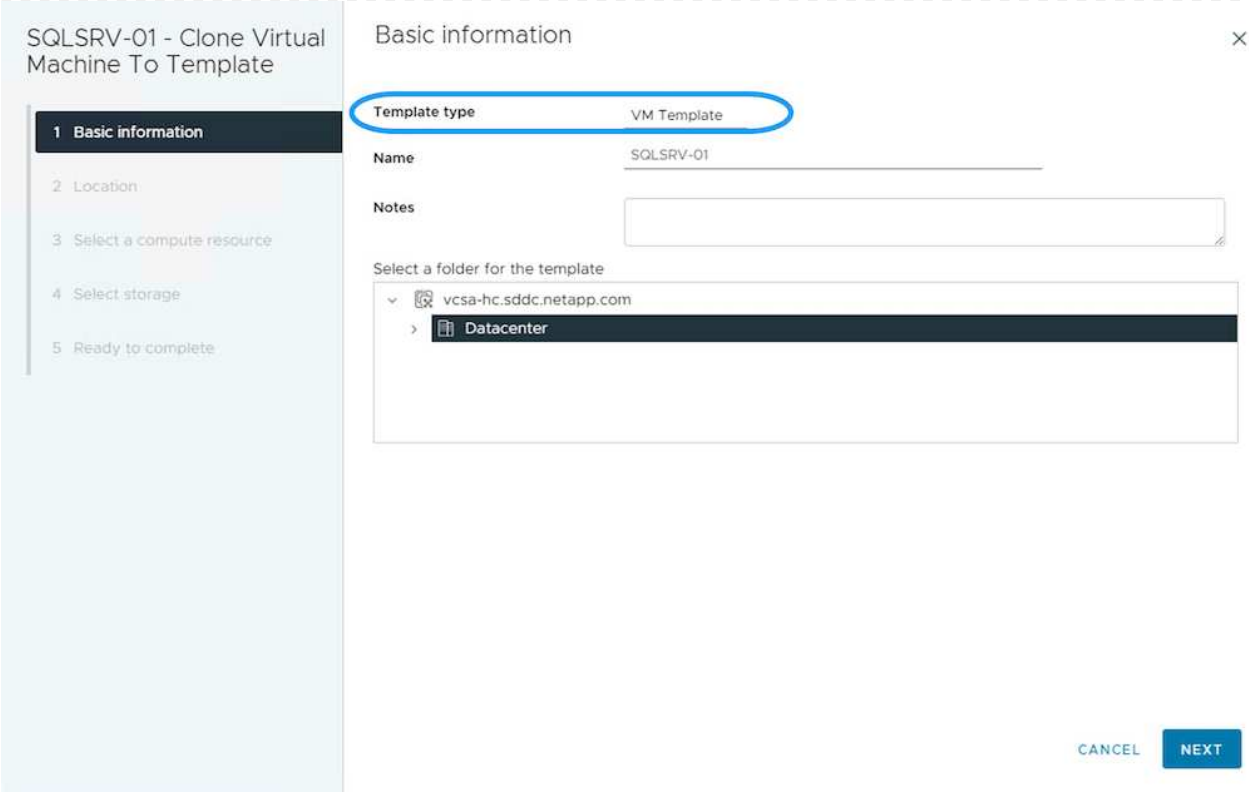
Adicionando VM como modelos na biblioteca de conteúdo

1. No vSphere Web Client, selecione a VM e clique com o botão direito para escolher Clonar como modelo na biblioteca



> Quando o modelo de VM é selecionado para clonar na biblioteca, ele só pode ser armazenado como modelo OVF e OVA e não como modelo de VM.

2. Confirme se o tipo de modelo está selecionado como Modelo de VM e siga as instruções do assistente para concluir a operação.



Para obter detalhes adicionais sobre modelos de VM na biblioteca de conteúdo, verifique "Guia de administração de VM do vSphere"

Casos de uso

Migração de sistemas de armazenamento de terceiros (incluindo vSAN) para datastores ONTAP .

- Com base em onde o armazenamento de dados ONTAP é provisionado, escolha as opções de migração de VM acima.

Migração da versão anterior para a versão mais recente do vSphere.

- Se a atualização local não for possível, você pode criar um novo ambiente e usar as opções de migração acima.

Na opção de migração entre vCenter, importe do destino se a opção de exportação não estiver disponível na origem. Para esse procedimento, verifique"Importar ou clonar uma máquina virtual com o Advanced Cross vCenter vMotion"

Migração para o domínio de carga de trabalho do VCF.

- Migre VMs de cada cluster do vSphere para o domínio de carga de trabalho de destino.

> Para permitir a comunicação de rede com VMs existentes em outros clusters no vCenter de origem, estenda o segmento NSX adicionando os hosts vSphere do vCenter de origem à zona de transporte ou use a ponte L2 na borda para permitir a comunicação L2 na VLAN. Verifique a documentação do NSX "Configurar uma VM de borda para ponte"

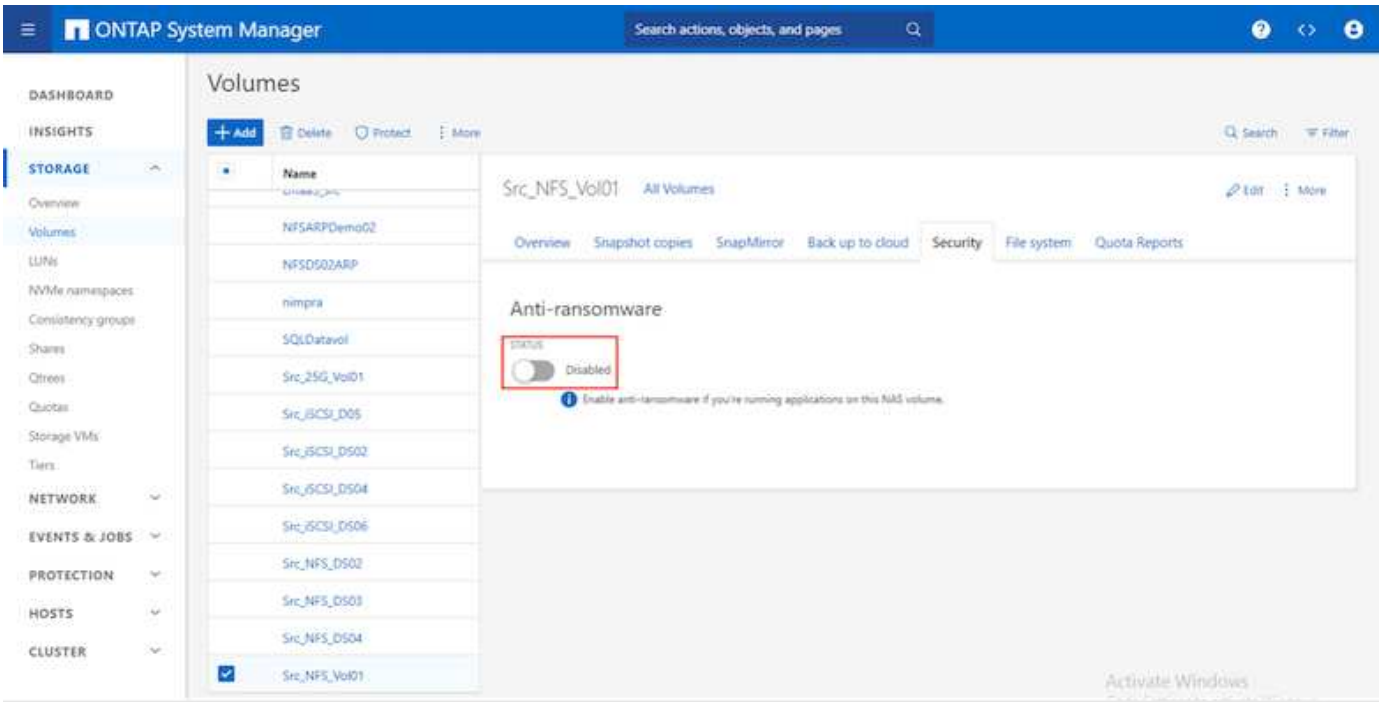
Recursos adicionais

- "Migração de Máquina Virtual vSphere"
- "Migrando máquinas virtuais com o vSphere vMotion"
- "Configurações de gateway de nível 0 na NSX Federation"
- "Guia do usuário do HCX 4.8"
- "Documentação do VMware Live Recovery"
- "BlueXP disaster recovery para VMware"

Proteção autônoma contra ransomware para armazenamento NFS

Detectar ransomware o mais cedo possível é crucial para impedir sua disseminação e evitar tempos de inatividade dispendiosos. Uma estratégia eficaz de detecção de ransomware deve incorporar várias camadas de proteção nos níveis de host ESXi e VM convidada. Embora diversas medidas de segurança sejam implementadas para criar uma defesa abrangente contra ataques de ransomware, o ONTAP permite adicionar mais camadas de proteção à abordagem geral de defesa. Para citar alguns recursos, ele começa com Snapshots, Proteção Autônoma contra Ransomware, snapshots à prova de violação e assim por diante.

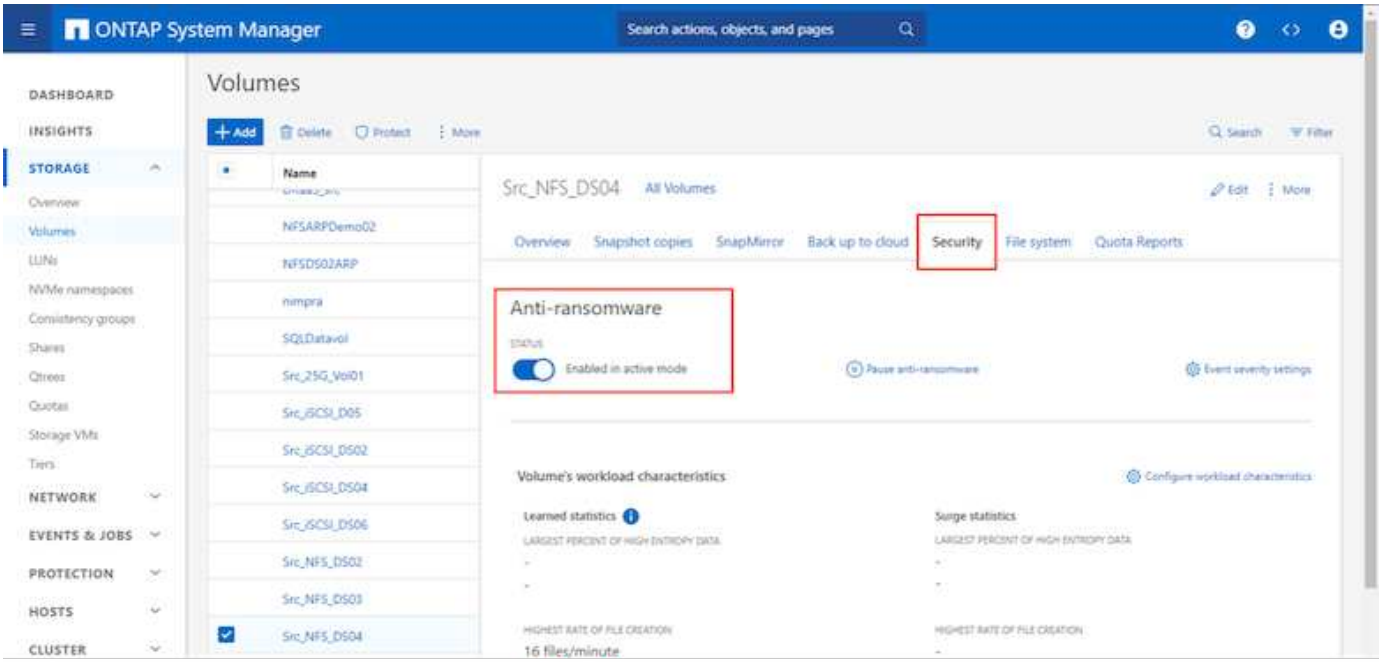
Vamos ver como os recursos mencionados acima funcionam com o VMware para proteger e recuperar dados contra ransomware. Para proteger o vSphere e as VMs convidadas contra ataques, é essencial tomar várias medidas, incluindo segmentação, utilização de EDR/XDR/SIEM para endpoints, instalação de atualizações de segurança e adesão às diretrizes de proteção apropriadas. Cada máquina virtual que reside em um armazenamento de dados também hospeda um sistema operacional padrão. Garanta que os conjuntos de produtos antimalware dos servidores corporativos estejam instalados e atualizados regularmente, o que é um componente essencial da estratégia de proteção contra ransomware em várias camadas. Junto com isso, habilite a Proteção Autônoma contra Ransomware (ARP) no volume NFS que alimenta o armazenamento de dados. O ARP utiliza o ML integrado que analisa a atividade da carga de trabalho em volume, além da entropia de dados, para detectar ransomware automaticamente. O ARP pode ser configurado por meio da interface de gerenciamento integrada do ONTAP ou do gerenciador do sistema e é ativado por volume.



Com o novo NetApp ARP/AI, que está atualmente em fase de pré-visualização tecnológica, não há necessidade de um modo de aprendizagem. Em vez disso, ele pode ir direto para o modo ativo com sua capacidade de detecção de ransomware alimentada por IA.

Com o ONTAP One, todos esses conjuntos de recursos são totalmente gratuitos. Acesse o robusto conjunto de proteção de dados, segurança e todos os recursos que o ONTAP oferece da NetApp sem se preocupar com barreiras de licenciamento.

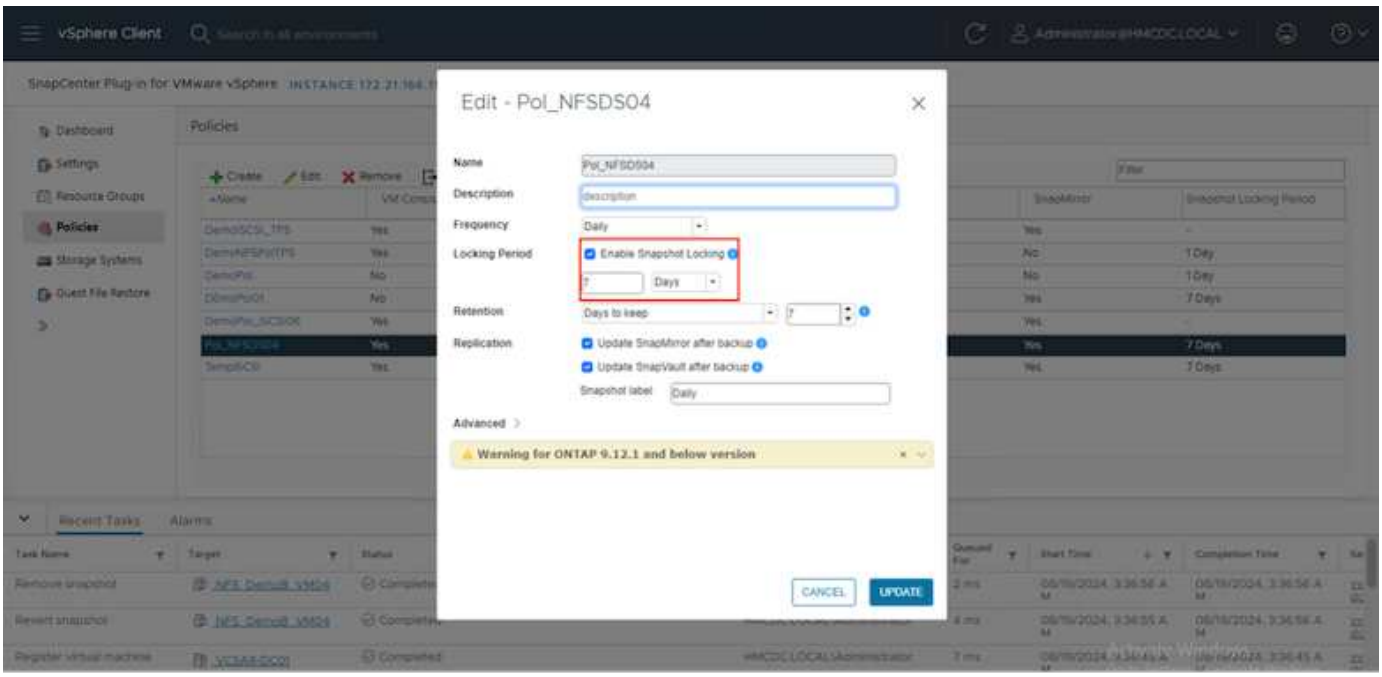
Uma vez no modo ativo, ele começa a procurar por atividades de volume anormal que podem ser potencialmente ransomware. Se atividade anormal for detectada, uma cópia automática do Snapshot é feita imediatamente, o que fornece um ponto de restauração o mais próximo possível da infecção do arquivo. O ARP pode detectar alterações em extensões de arquivo específicas da VM em um volume NFS localizado fora da VM quando uma nova extensão é adicionada ao volume criptografado ou a extensão de um arquivo é modificada.



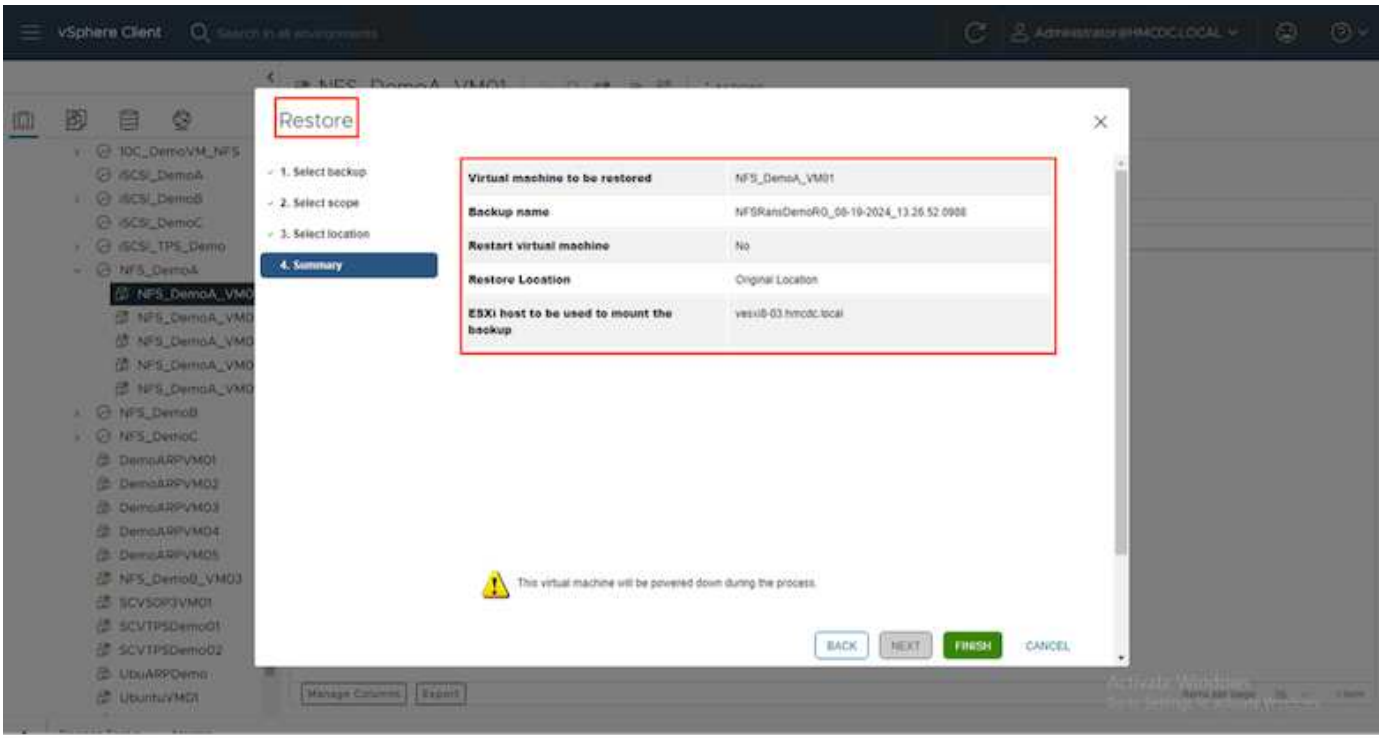
Se um ataque de ransomware tiver como alvo a máquina virtual (VM) e alterar arquivos dentro da VM sem fazer alterações fora dela, a Advanced Ransomware Protection (ARP) ainda detectará a ameaça se a entropia padrão da VM for baixa, por exemplo, para tipos de arquivo como .txt, .docx ou .mp4. Embora o ARP crie um snapshot de proteção neste cenário, ele não gera um alerta de ameaça porque as extensões de arquivo fora da VM não foram adulteradas. Nesses cenários, as camadas iniciais de defesa identificariam a anomalia, porém o ARP ajuda a criar um instantâneo com base na entropia.

Para obter informações detalhadas, consulte a seção "ARP e máquinas virtuais" em"Casos de uso e considerações do ARP" .

Passando de arquivos para dados de backup, os ataques de ransomware agora estão cada vez mais visando backups e pontos de recuperação de instantâneos, tentando excluí-los antes de começar a criptografar os arquivos. No entanto, com o ONTAP, isso pode ser evitado criando instantâneos à prova de violação em sistemas primários ou secundários com"Bloqueio de cópia do NetApp Snapshot" .



Essas cópias do Snapshot não podem ser excluídas ou alteradas por invasores de ransomware ou administradores desonestos, portanto, elas ficam disponíveis mesmo após um ataque. Se o armazenamento de dados ou máquinas virtuais específicas forem afetados, o SnapCenter poderá recuperar dados da máquina virtual em segundos, minimizando o tempo de inatividade da organização.

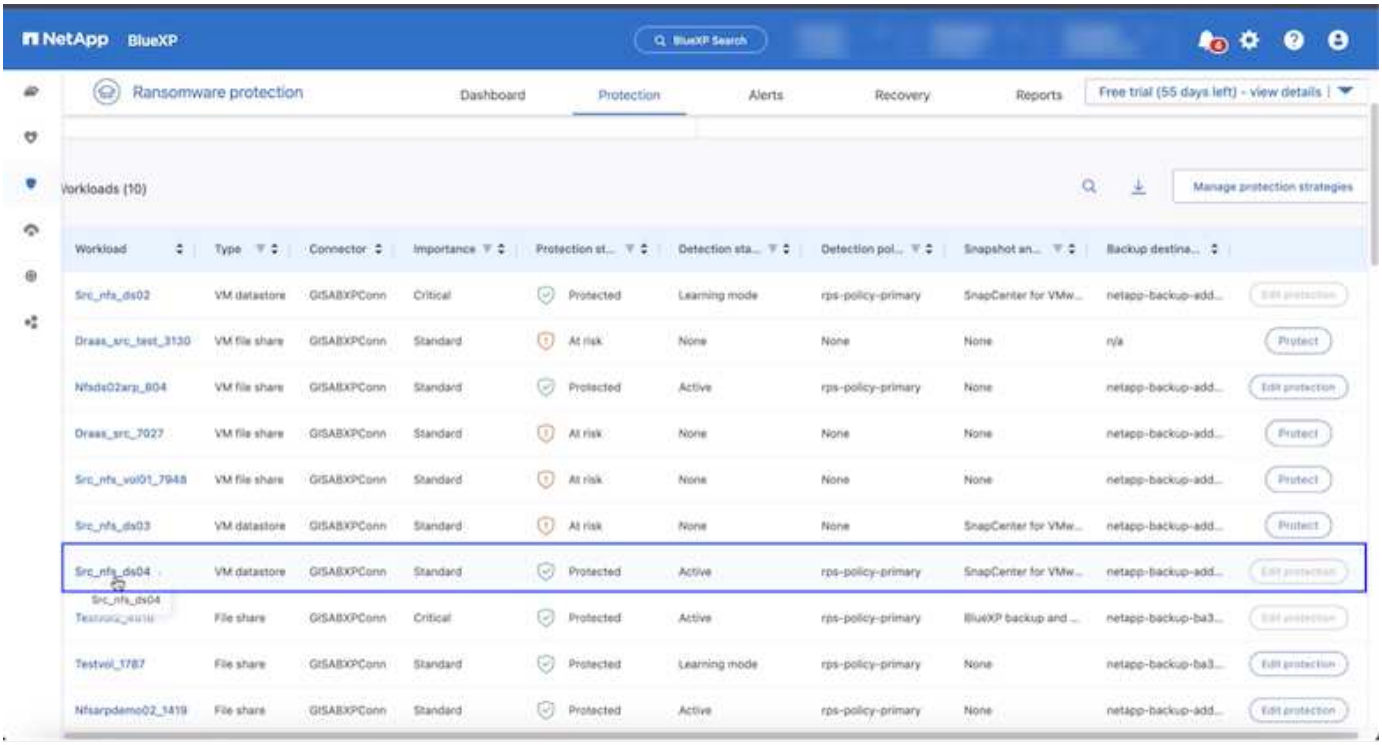


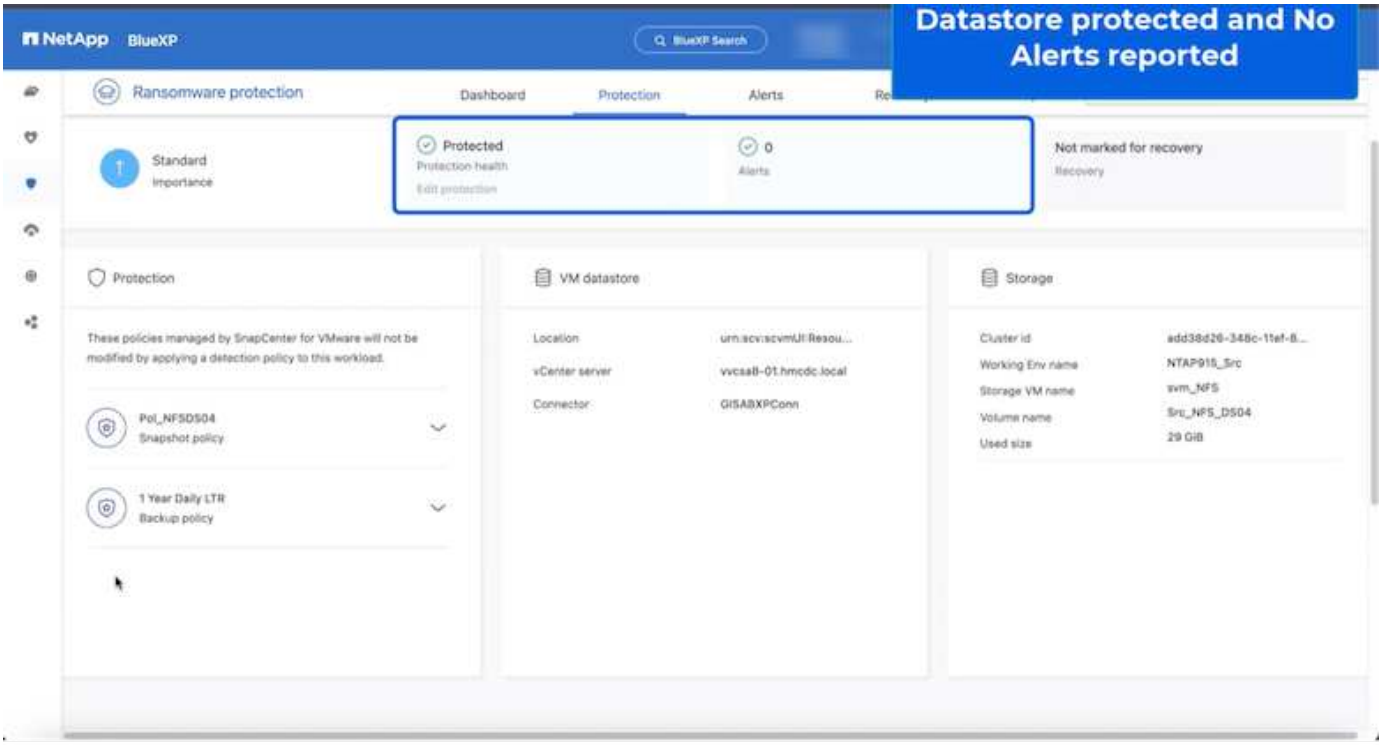
O texto acima demonstra como o armazenamento ONTAP acrescenta uma camada adicional às técnicas existentes, melhorando a proteção futura do ambiente.

Para obter informações adicionais, consulte as orientações para"Soluções NetApp para ransomware" .

Agora, se tudo isso precisar ser orquestrado e integrado com ferramentas SIEM, um serviço offtap como a BlueXP ransomware protection pode ser usado. É um serviço projetado para proteger dados contra ransomware. Este serviço oferece proteção para cargas de trabalho baseadas em aplicativos, como Oracle, MySQL, datastores de VM e compartilhamentos de arquivos em armazenamento NFS local.

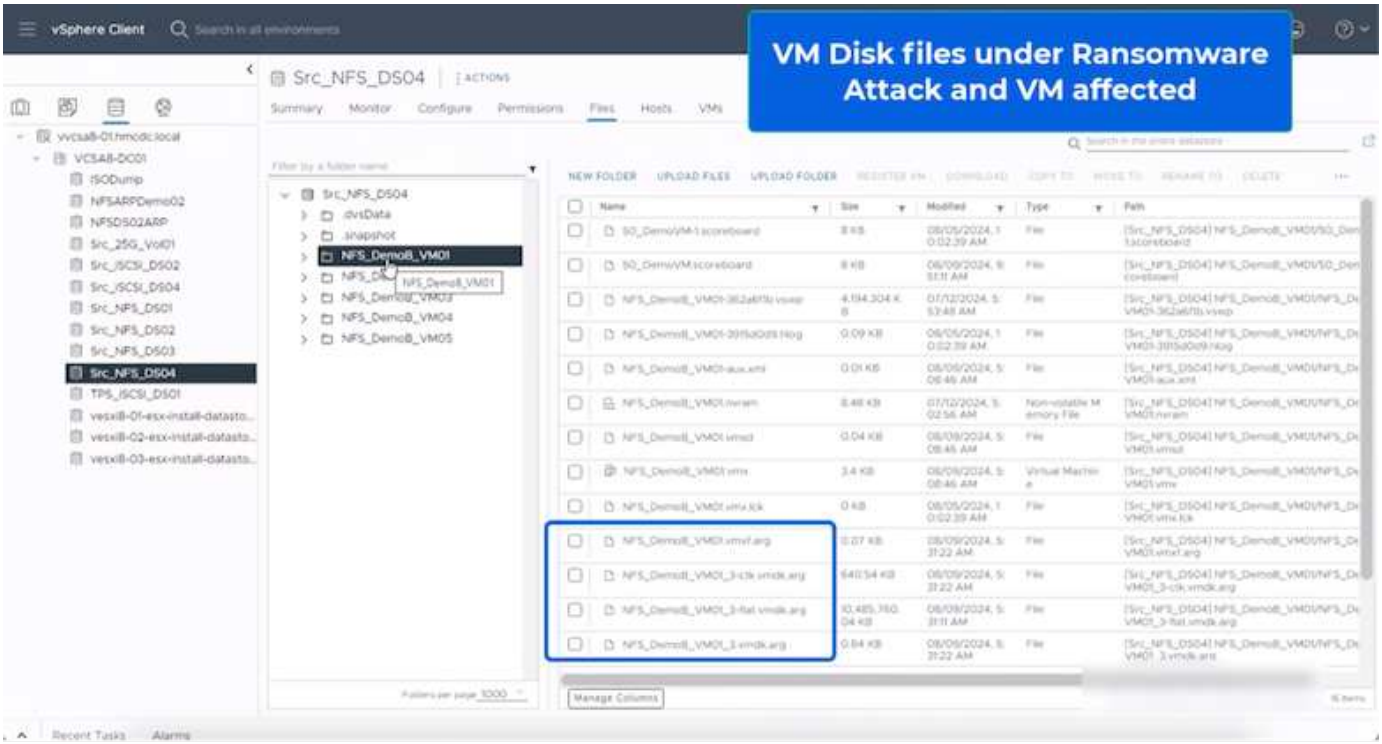
Neste exemplo, o armazenamento de dados NFS "Src_NFS_DS04" é protegido usando a BlueXP ransomware protection.



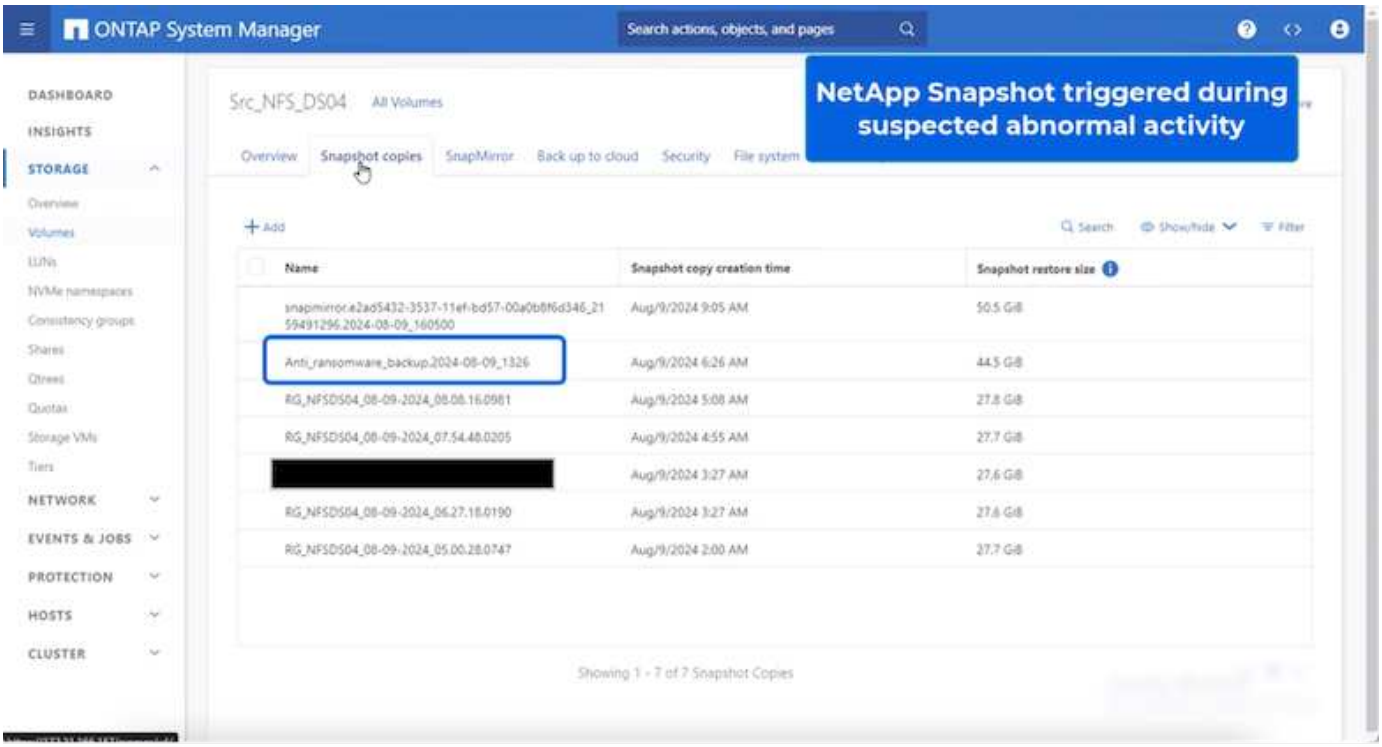


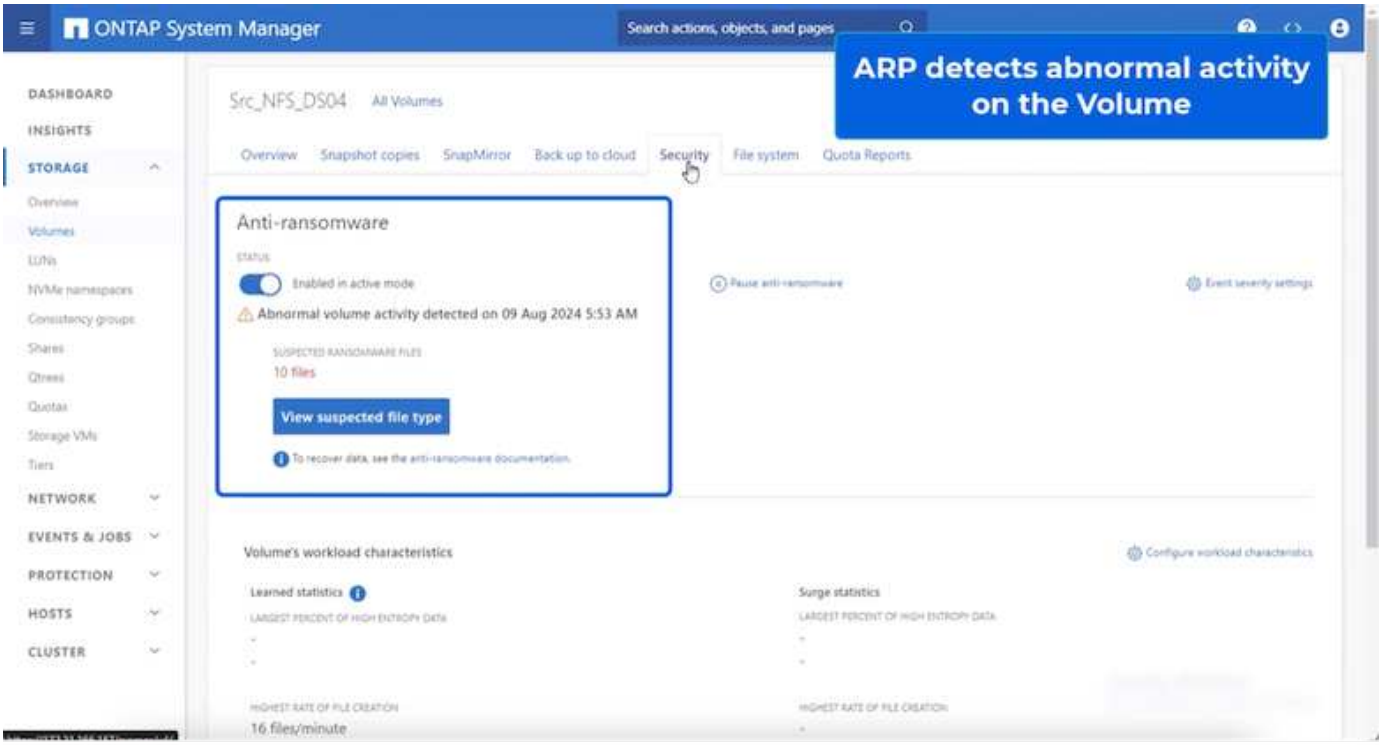
Para obter informações detalhadas sobre como configurar a BlueXP ransomware protection, consulte"Configurar a BlueXP ransomware protection" e"Configurar as definições de BlueXP ransomware protection" .

É hora de explicar isso com um exemplo. Neste passo a passo, o armazenamento de dados "Src_NFS_DS04" é afetado.

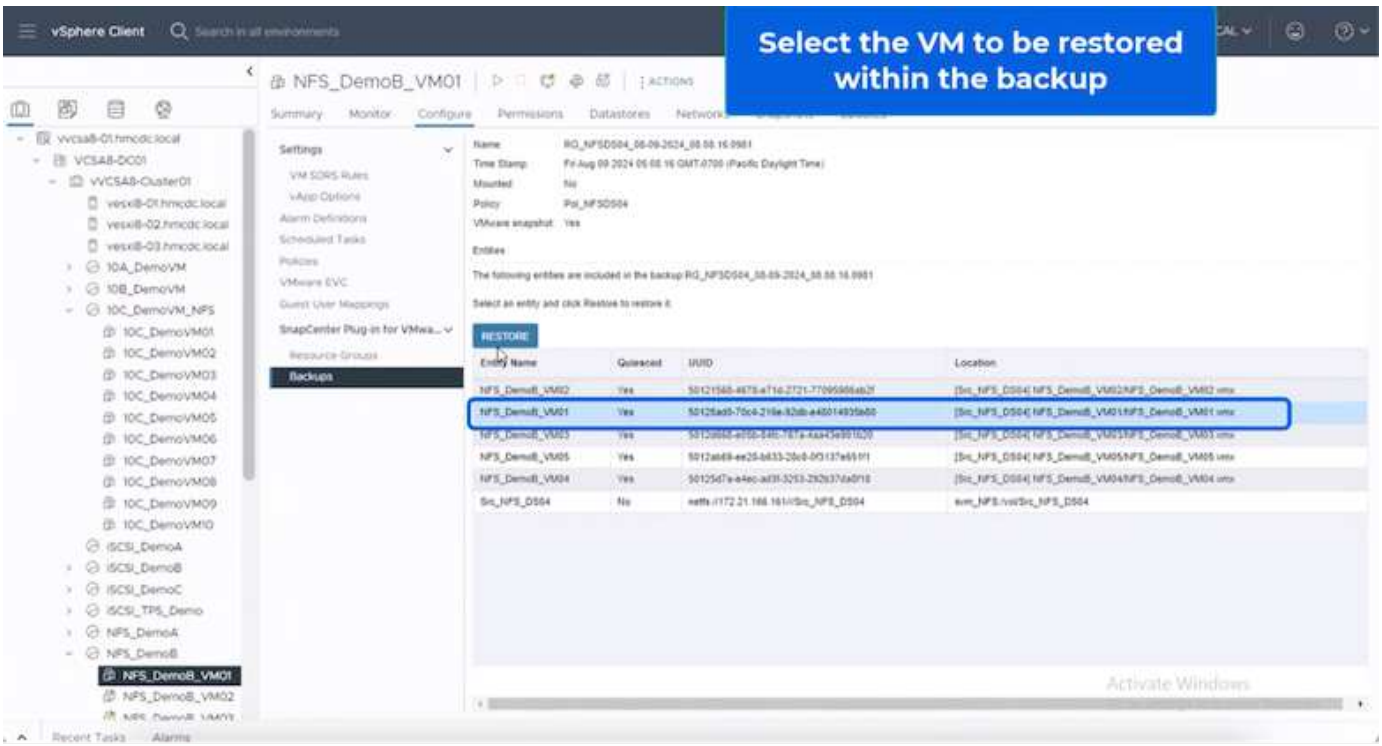


O ARP disparou imediatamente um instantâneo no volume após a detecção.





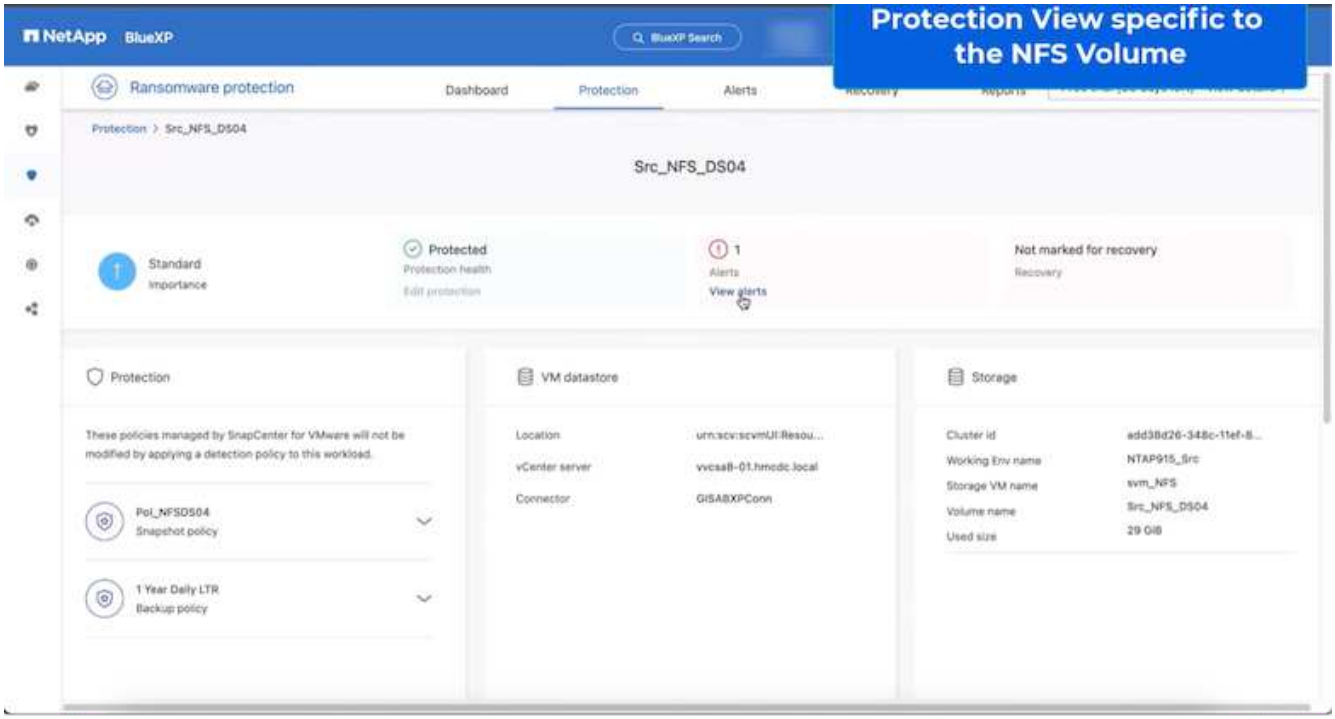
Após a conclusão da análise forense, as restaurações podem ser feitas de forma rápida e fácil usando a proteção contra ransomware SnapCenter ou BlueXP ransomware protection. Com o SnapCenter, acesse as máquinas virtuais afetadas e selecione o snapshot apropriado para restaurar.



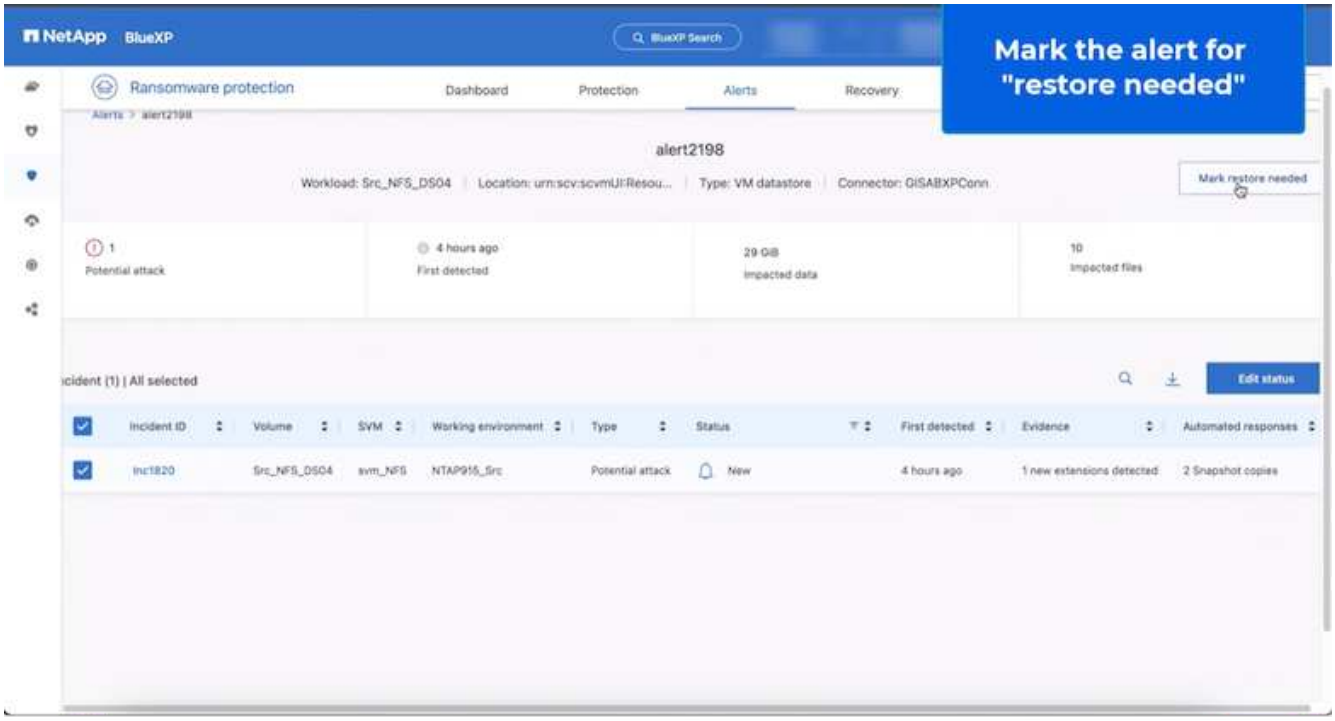
Esta seção analisa como a BlueXP ransomware protection orquestra a recuperação de um incidente de ransomware em que os arquivos da VM são criptografados.

> Se a VM for gerenciada pelo SnapCenter, a BlueXP ransomware protection restaurará a VM ao seu estado anterior usando o processo consistente com a VM.

1. Acesse a BlueXP ransomware protection e um alerta aparecerá no Painel de BlueXP ransomware protection .
2. Clique no alerta para revisar os incidentes naquele volume específico para o alerta gerado

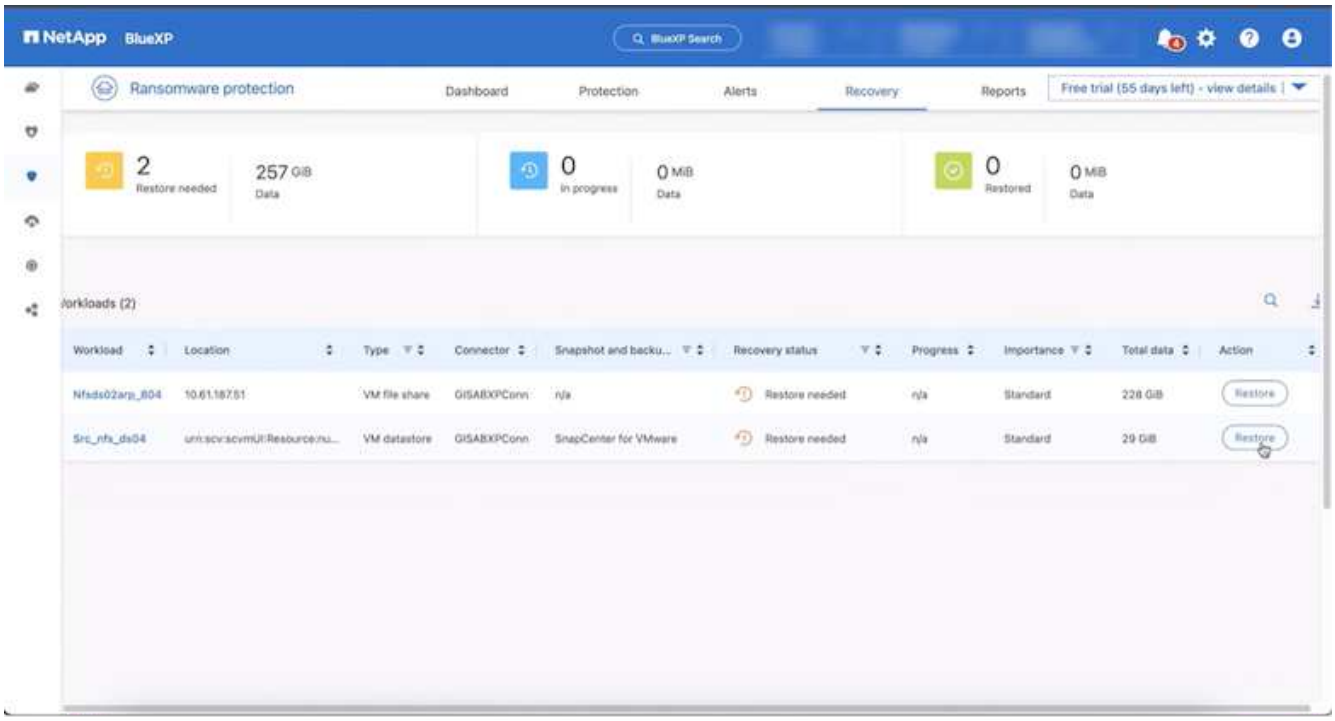


3. Marque o incidente de ransomware como pronto para recuperação (após os incidentes serem neutralizados) selecionando "Marcar restauração necessária"

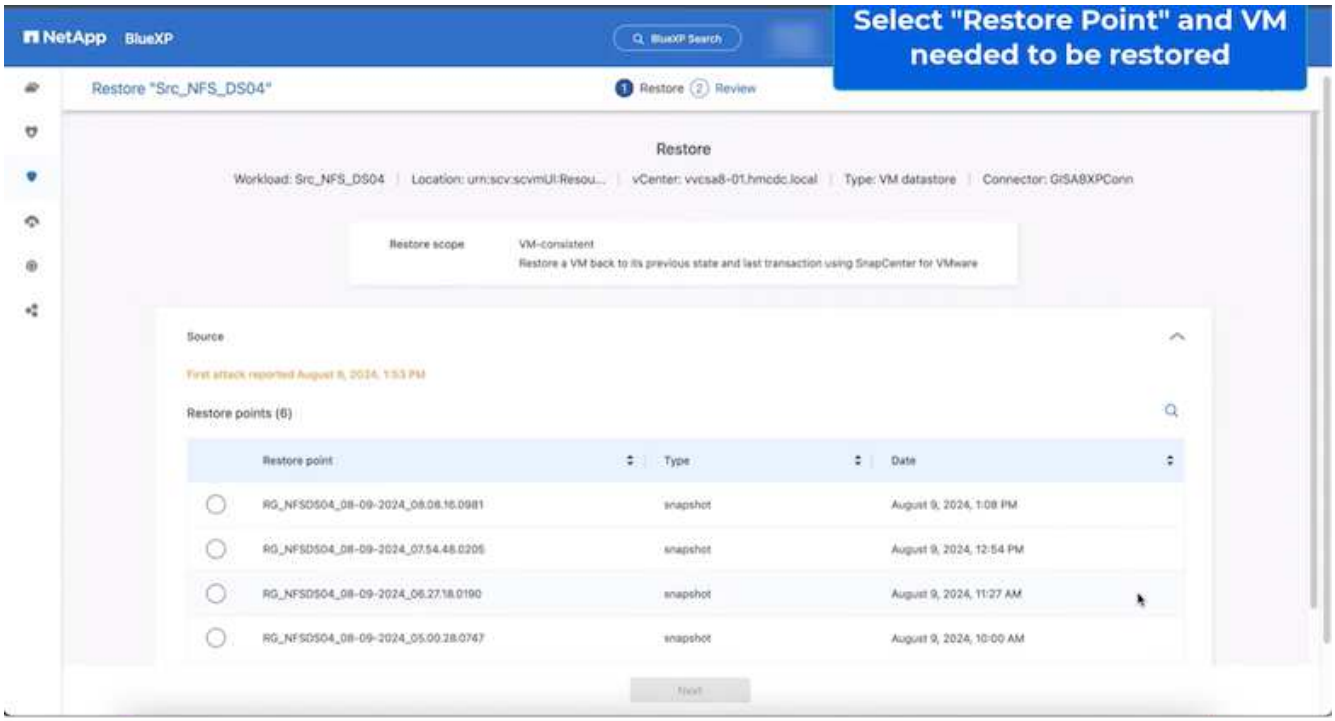


O alerta pode ser descartado se o incidente for um falso positivo.

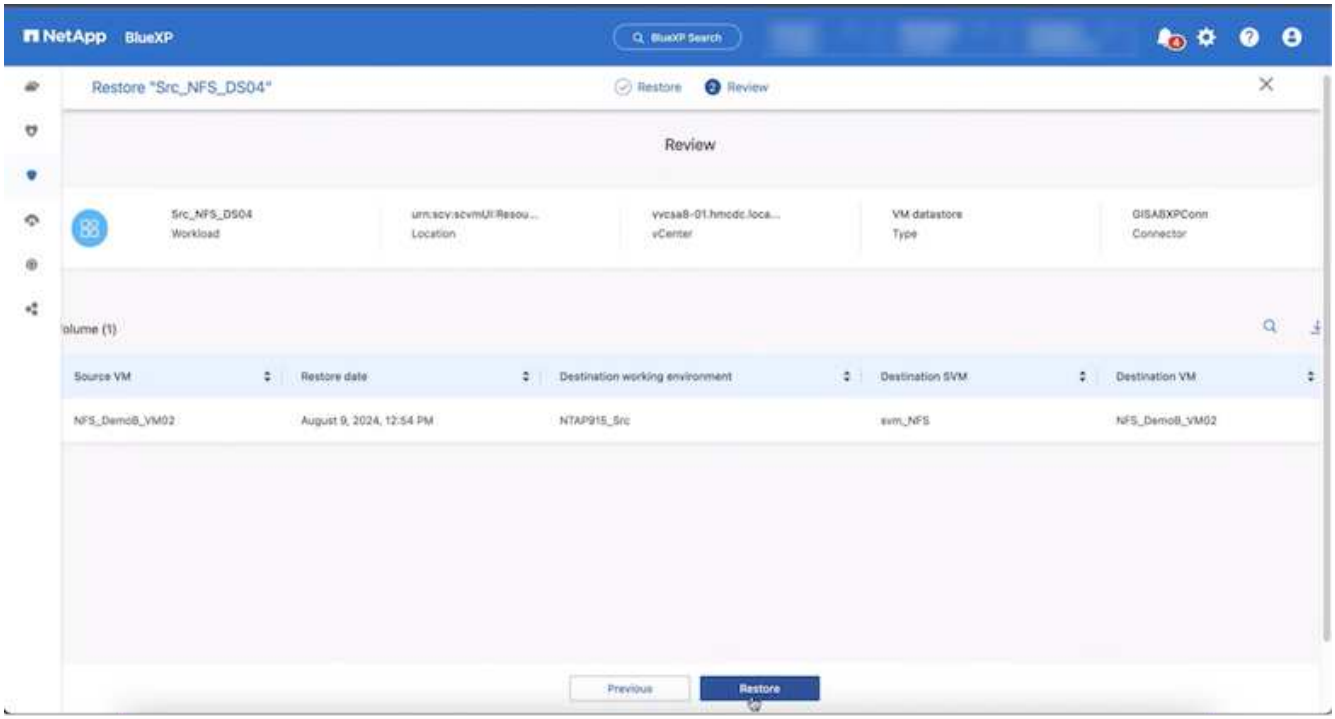
4. Acesse a guia Recuperação e revise as informações de carga de trabalho na página Recuperação e selecione o volume de armazenamento de dados que está no estado "Restauração necessária" e selecione Restaurar.



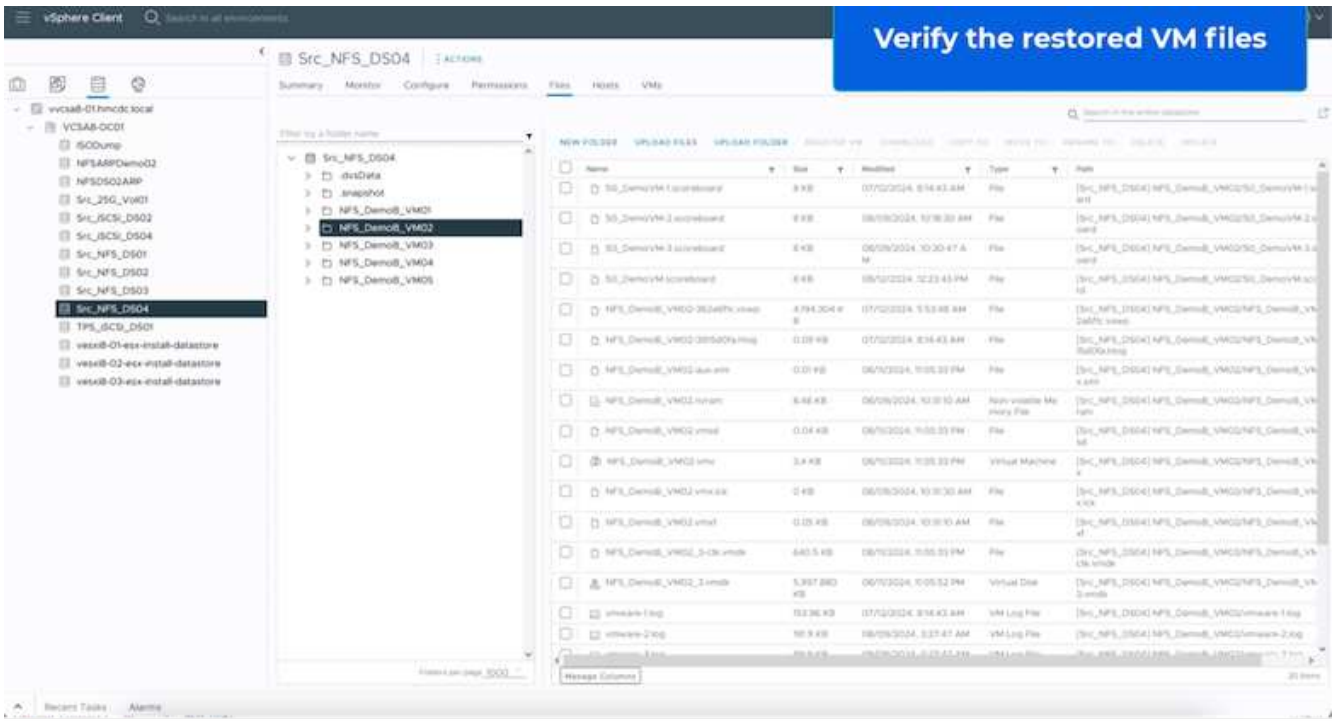
5. Neste caso, o escopo de restauração é "Por VM" (para SnapCenter para VMs, o escopo de restauração é "Por VM")



6. Escolha o ponto de restauração a ser usado para restaurar os dados, selecione Destino e clique em Restaurar.



7. No menu superior, selecione Recuperação para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados. Quando a restauração estiver concluída, os arquivos da VM serão restaurados conforme mostrado abaixo.



> A recuperação pode ser executada a partir do SnapCenter para VMware ou do plugin SnapCenter , dependendo do aplicativo.

A solução NetApp fornece várias ferramentas eficazes para visibilidade, detecção e correção, ajudando você a identificar ransomware precocemente, evitar sua disseminação e se recuperar rapidamente, se necessário, para evitar tempo de inatividade dispendioso. Soluções tradicionais de defesa em camadas continuam

prevalecendo, assim como soluções de terceiros e parceiros para visibilidade e detecção. A remediação eficaz continua sendo uma parte crucial da resposta a qualquer ameaça.

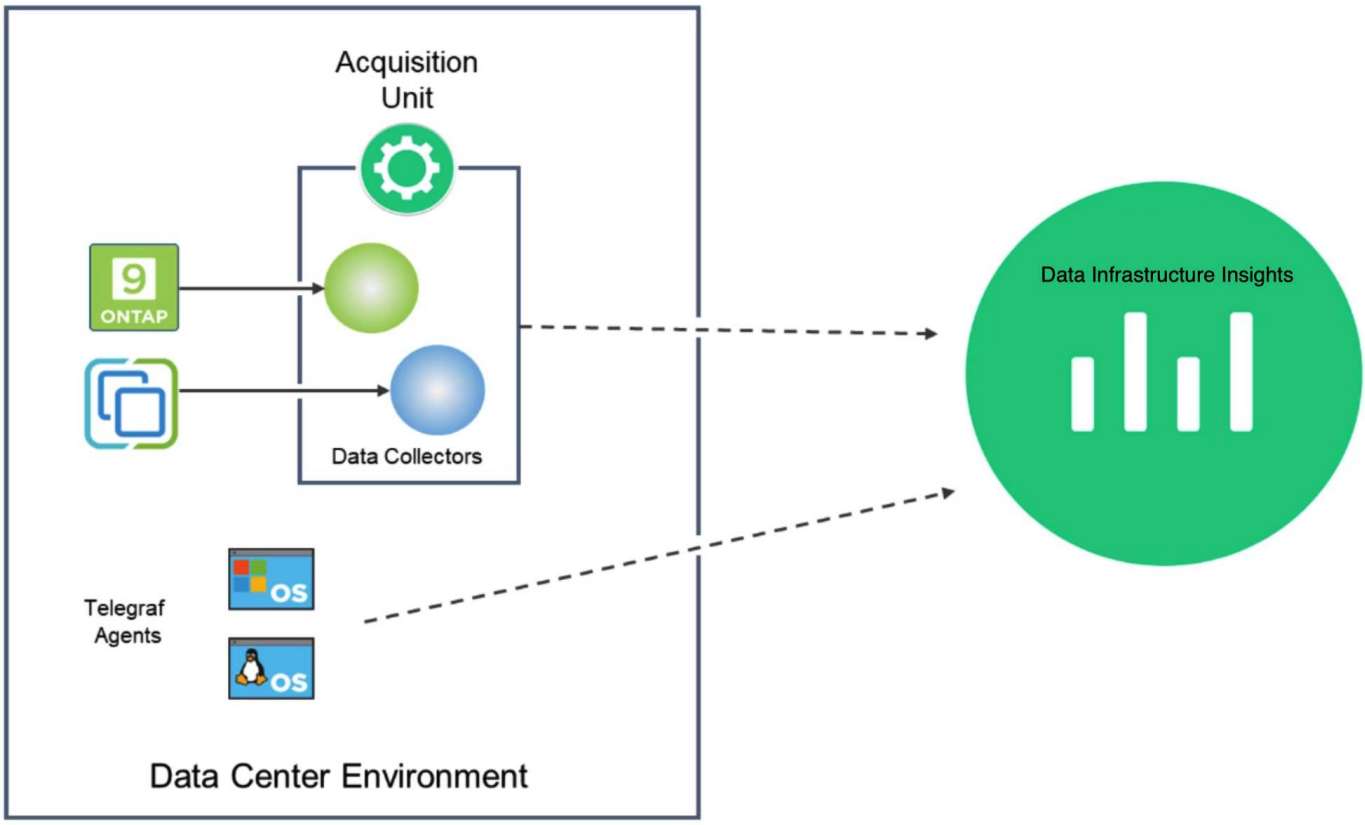
Monitore o armazenamento local com o Data Infrastructure Insights

O NetApp Data Infrastructure Insights (anteriormente Cloud Insights) é uma plataforma baseada em nuvem projetada para monitorar e analisar o desempenho, a integridade e os custos de infraestruturas de TI, tanto no local quanto na nuvem. Aprenda a implantar coletores de dados, analisar métricas de desempenho e usar painéis para identificar problemas e otimizar recursos.

Monitoramento de armazenamento local com Data Infrastructure Insights

O Data Infrastructure Insights opera por meio do software Acquisition Unit, que é configurado com coletores de dados para ativos como os sistemas de armazenamento VMware vSphere e NetApp ONTAP . Esses coletores reúnem dados e os transmitem ao Data Infrastructure Insights. A plataforma então utiliza uma variedade de painéis, widgets e consultas métricas para organizar os dados em análises perspicazes para os usuários interpretarem.

Diagrama de arquitetura do Data Infrastructure Insights :



Visão geral da implantação da solução

Esta solução fornece uma introdução ao monitoramento de sistemas de armazenamento VMware vSphere e ONTAP locais usando o Data Infrastructure Insights.

Esta lista fornece as etapas de alto nível abordadas nesta solução:

1. Configurar o Data Collector para um cluster vSphere.
2. Configurar o Data Collector para um sistema de armazenamento ONTAP .
3. Use regras de anotação para marcar ativos.
4. Explore e correlacione ativos.
5. Use um painel de latência de VM superior para isolar vizinhos barulhentos.
6. Identifique oportunidades para dimensionar corretamente as VMs.
7. Use consultas para isolar e classificar métricas.

Pré-requisitos

Esta solução utiliza os seguintes componentes:

1. Matriz SAN All-Flash A400 da NetApp com ONTAP 9.13.
2. Cluster do VMware vSphere 8.0.
3. Conta NetApp BlueXP .
4. Software NetApp Data Infrastructure Insights Acquisition Unit instalado em uma VM local com conectividade de rede aos ativos para coleta de dados.

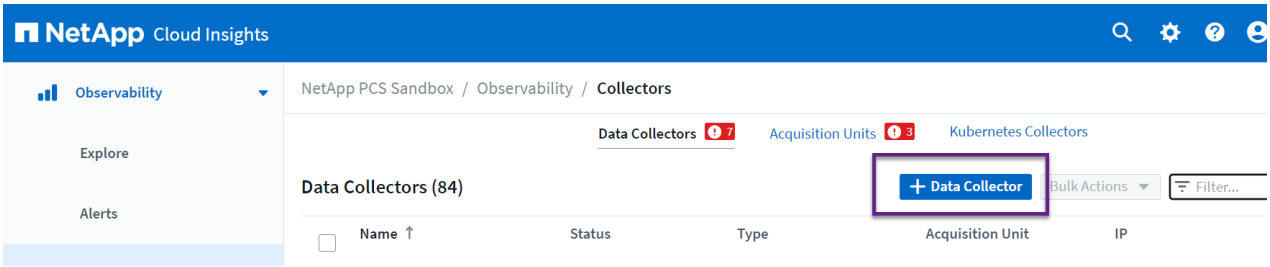
Implantação de solução

Configurar coletores de dados

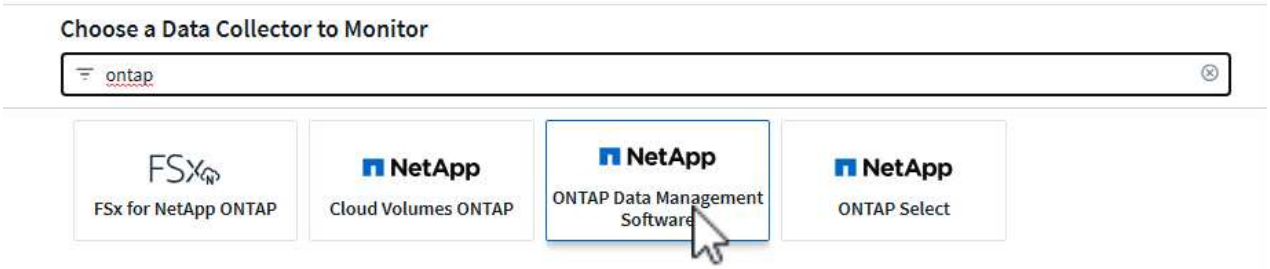
Para configurar os coletores de dados para sistemas de armazenamento VMware vSphere e ONTAP , conclua as seguintes etapas:

Adicionar um coletor de dados para sistemas de armazenamento ONTAP

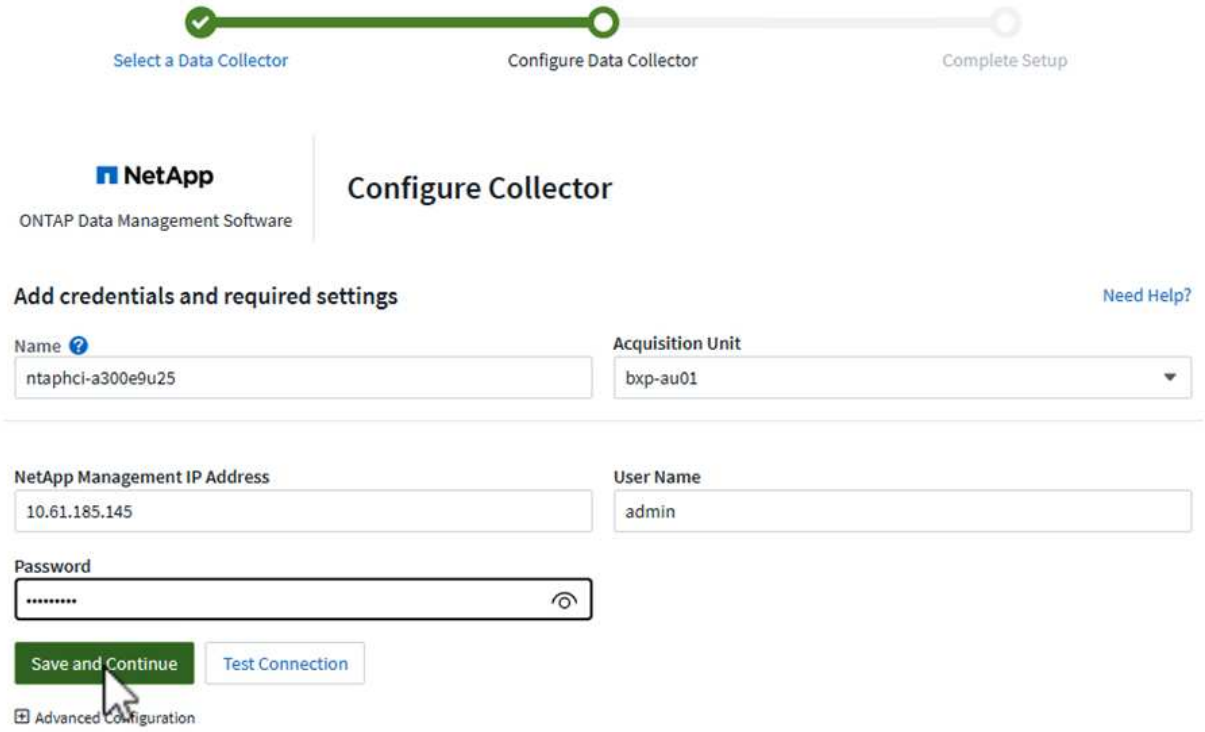
1. Depois de fazer login no Data Infrastructure Insights, navegue até **Observability > Collectors > Data Collectors** e pressione o botão para instalar um novo Data Collector.



2. A partir daqui, procure por * ONTAP* e clique em * Software de gerenciamento de dados ONTAP *.

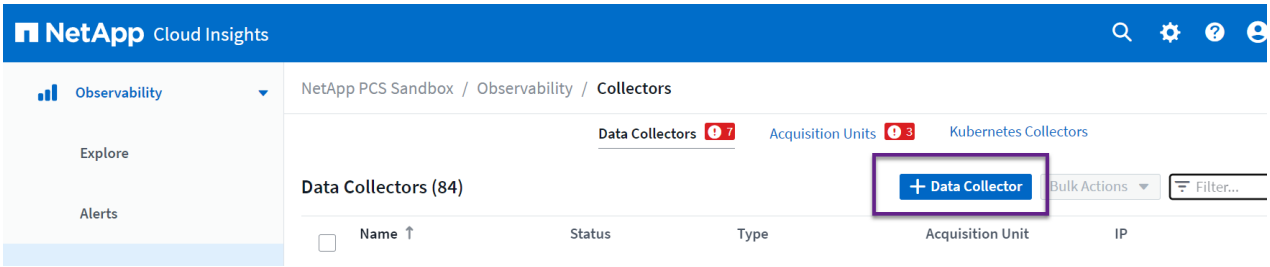


3. Na página **Configurar coletor**, preencha um nome para o coletor, especifique a **Unidade de aquisição** correta e forneça as credenciais para o sistema de armazenamento ONTAP . Clique em **Salvar e continuar** e depois em **Concluir configuração** na parte inferior da página para concluir a configuração.

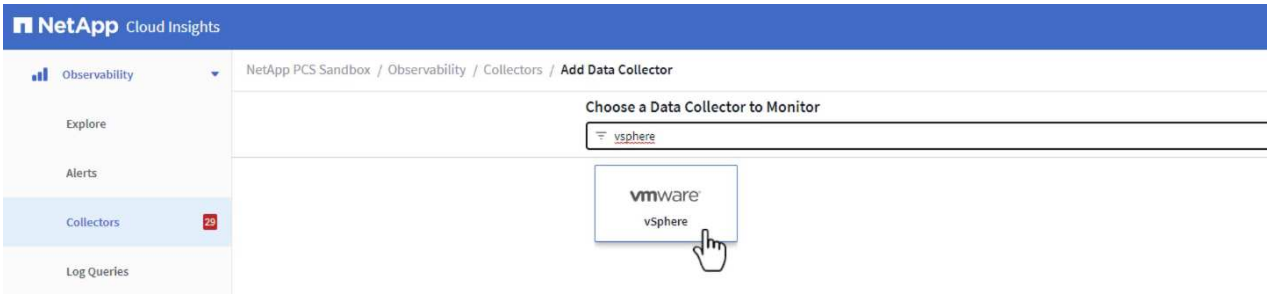


Adicionar um coletor de dados para um cluster VMware vSphere

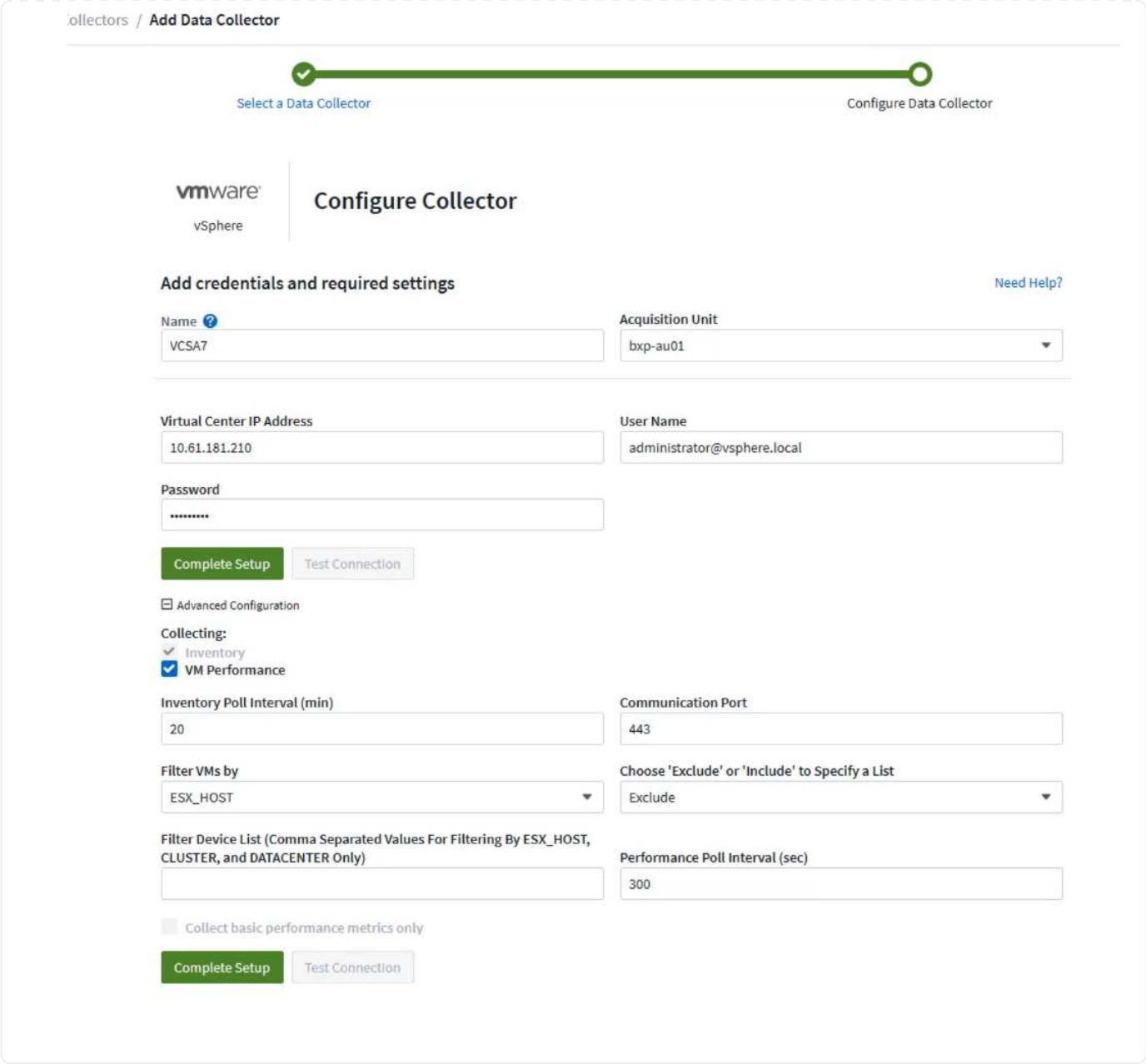
1. Mais uma vez, navegue até **Observabilidade > Coletores > Coletores de Dados** e pressione o botão para instalar um novo Coletor de Dados.



2. A partir daqui, procure por **vSphere** e clique em **VMware vSphere**.



3. Na página **Configurar coletor**, preencha um nome para o coletor, especifique a **Unidade de aquisição** correta e forneça as credenciais para o servidor vCenter. Clique em **Salvar e continuar** e depois em **Concluir configuração** na parte inferior da página para concluir a configuração.



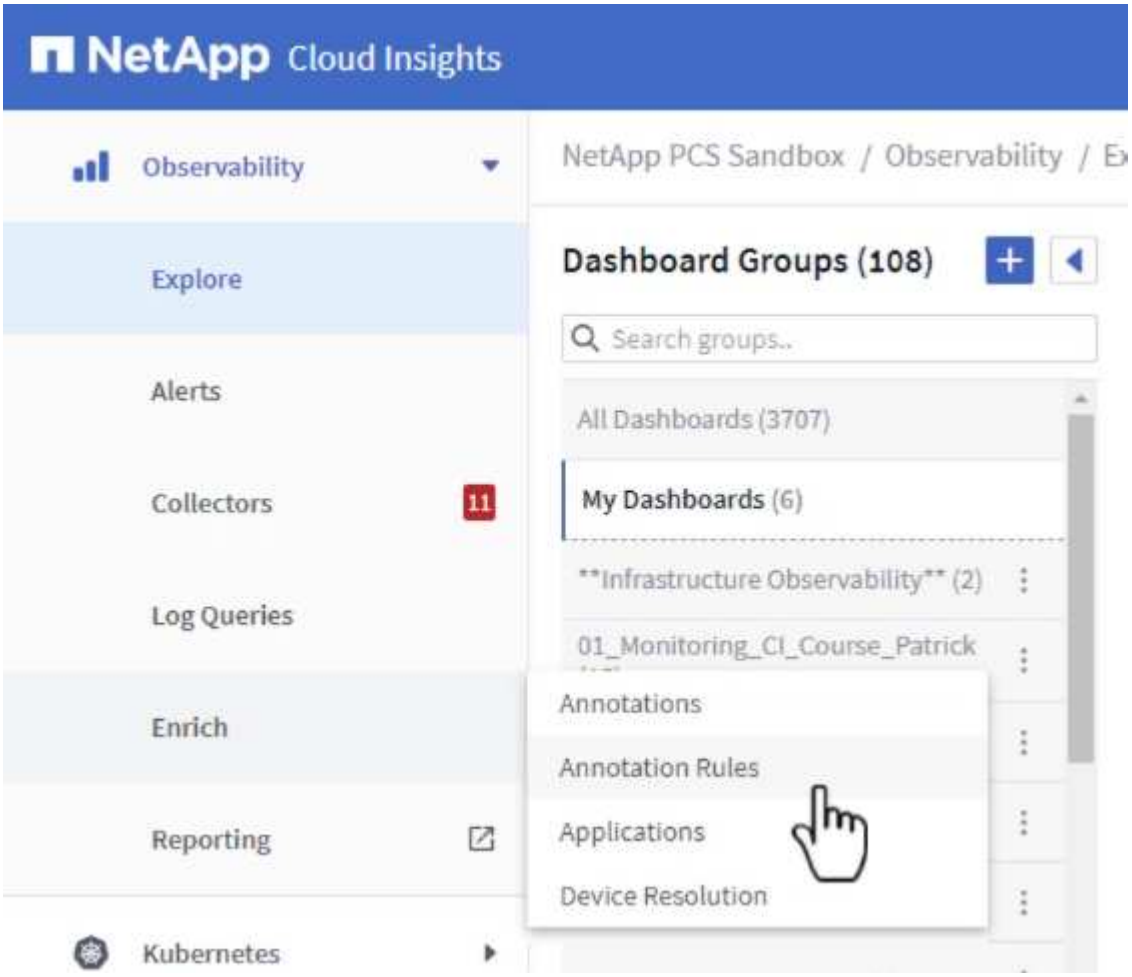
Adicionar anotações aos ativos

As anotações são um método útil de marcar ativos para que eles possam ser filtrados e identificados nas várias visualizações e consultas de métricas disponíveis no Cloud Insights.

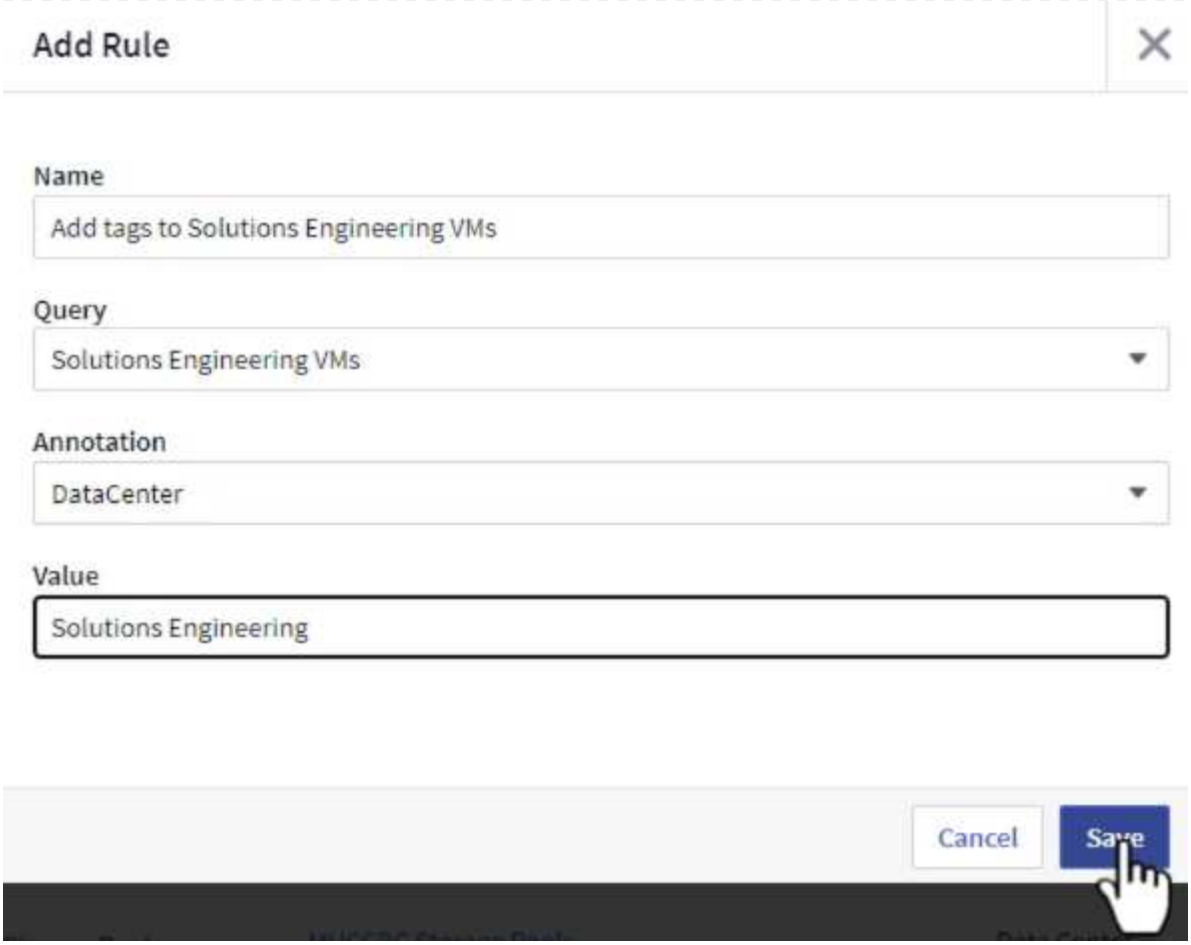
Nesta seção, anotações serão adicionadas aos ativos da máquina virtual para filtragem por **Data Center**.

Use regras de anotação para marcar ativos

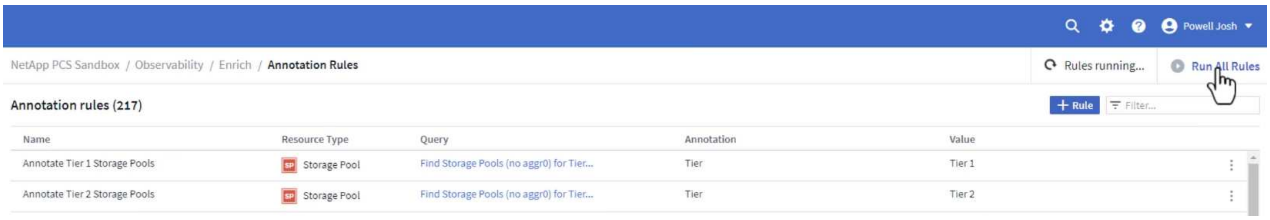
1. No menu à esquerda, navegue até **Observabilidade > Enriquecer > Regras de anotação** e clique no botão **+ Regra** no canto superior direito para adicionar uma nova regra.



2. Na caixa de diálogo **Adicionar regra**, preencha um nome para a regra, localize uma consulta à qual a regra será aplicada, o campo de anotação afetado e o valor a ser preenchido.



3. Por fim, no canto superior direito da página **Regras de anotação**, clique em **Executar todas as regras** para executar a regra e aplicar a anotação aos ativos.



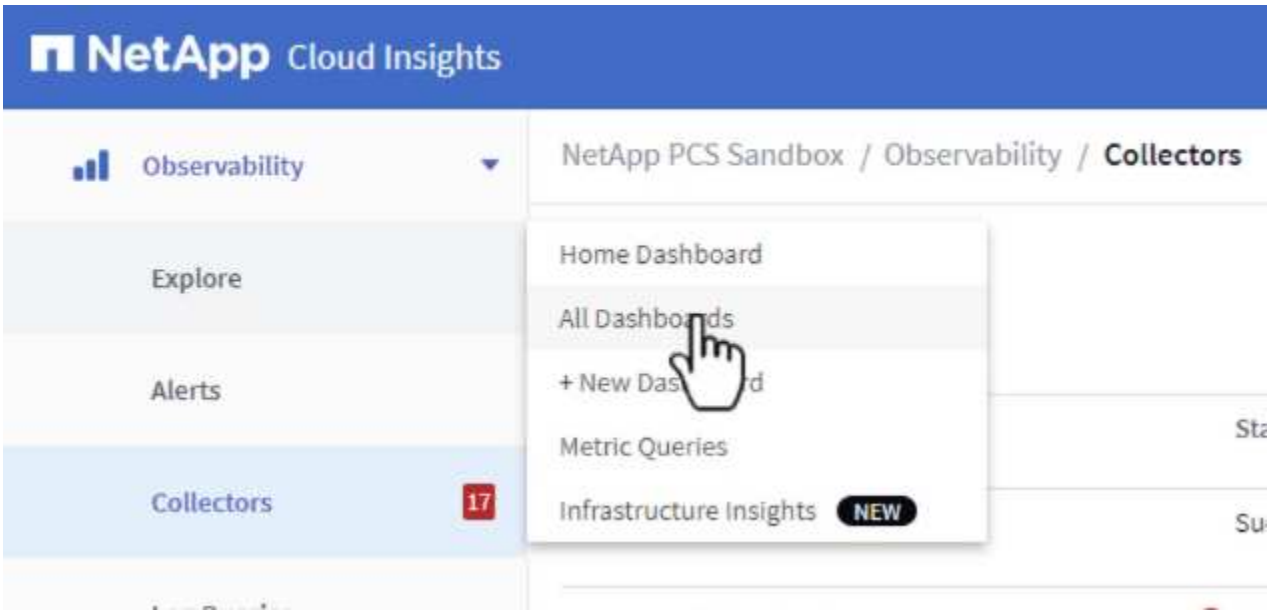
Explorar e correlacionar ativos

O Cloud Insights tira conclusões lógicas sobre os ativos que estão sendo executados juntos em seus sistemas de armazenamento e clusters do vSphere.

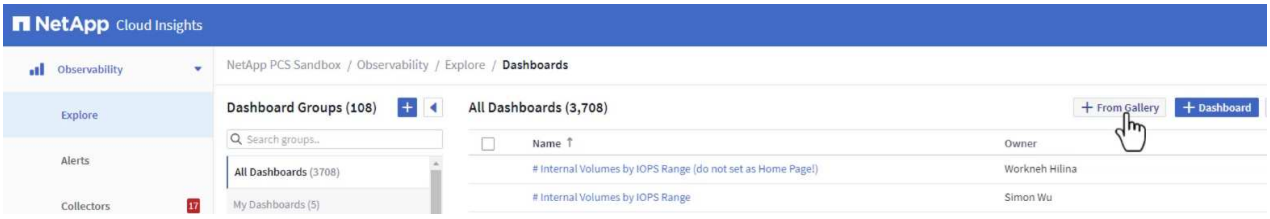
Esta seção ilustra como usar painéis para correlacionar ativos.

Correlacionando ativos de um painel de desempenho de armazenamento

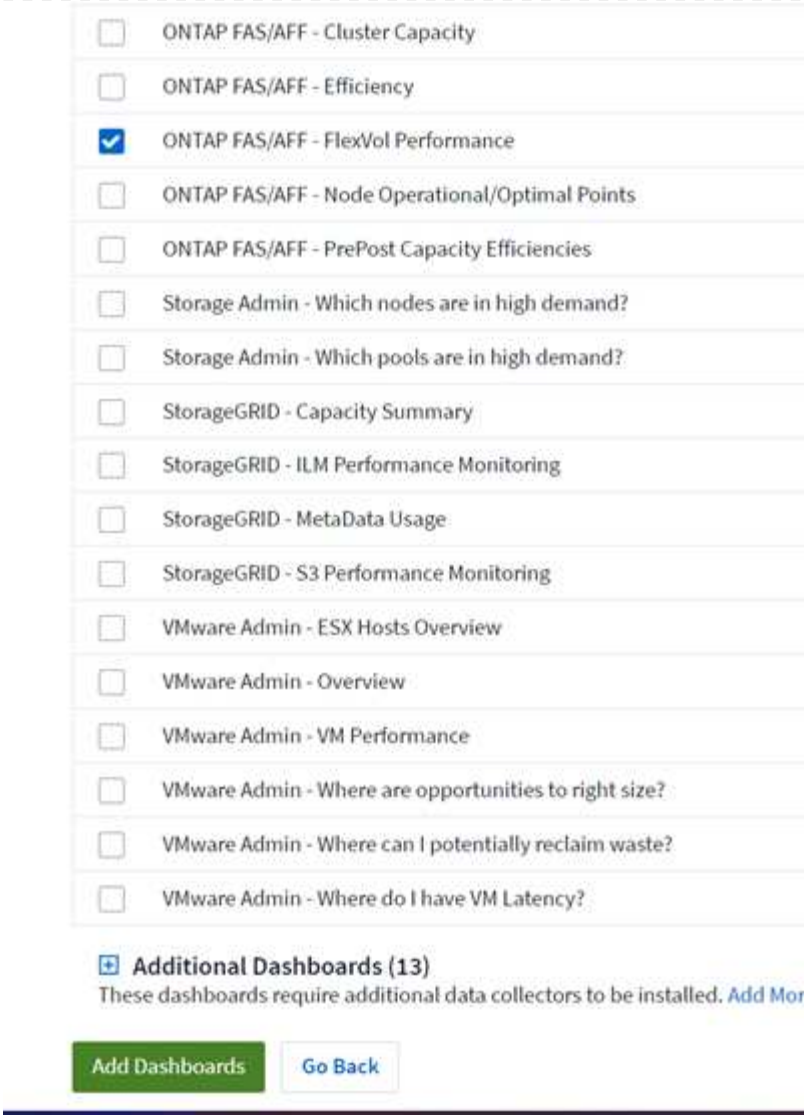
1. No menu à esquerda, navegue até **Observabilidade > Explorar > Todos os painéis**.



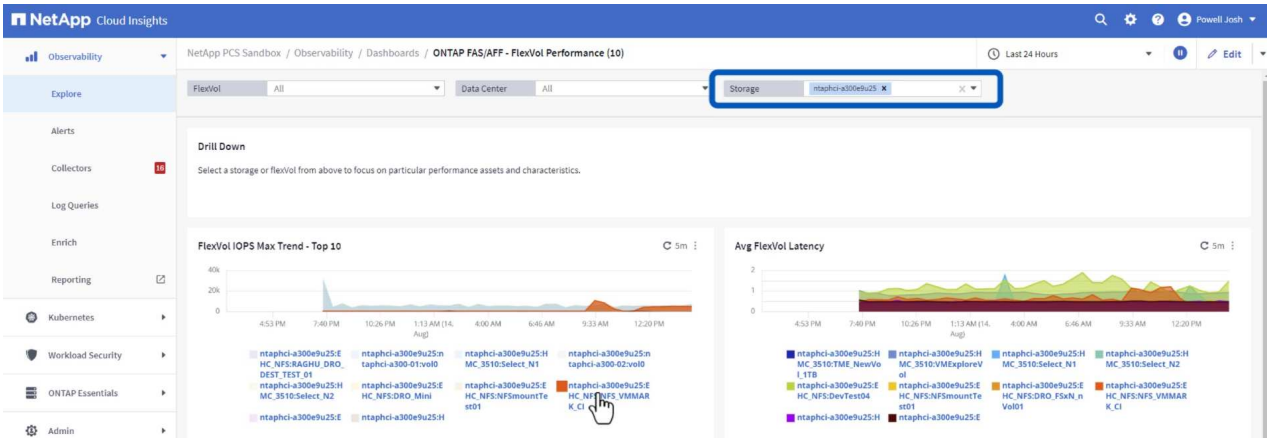
2. Clique no botão **+ Da Galeria** para ver uma lista de painéis prontos que podem ser importados.



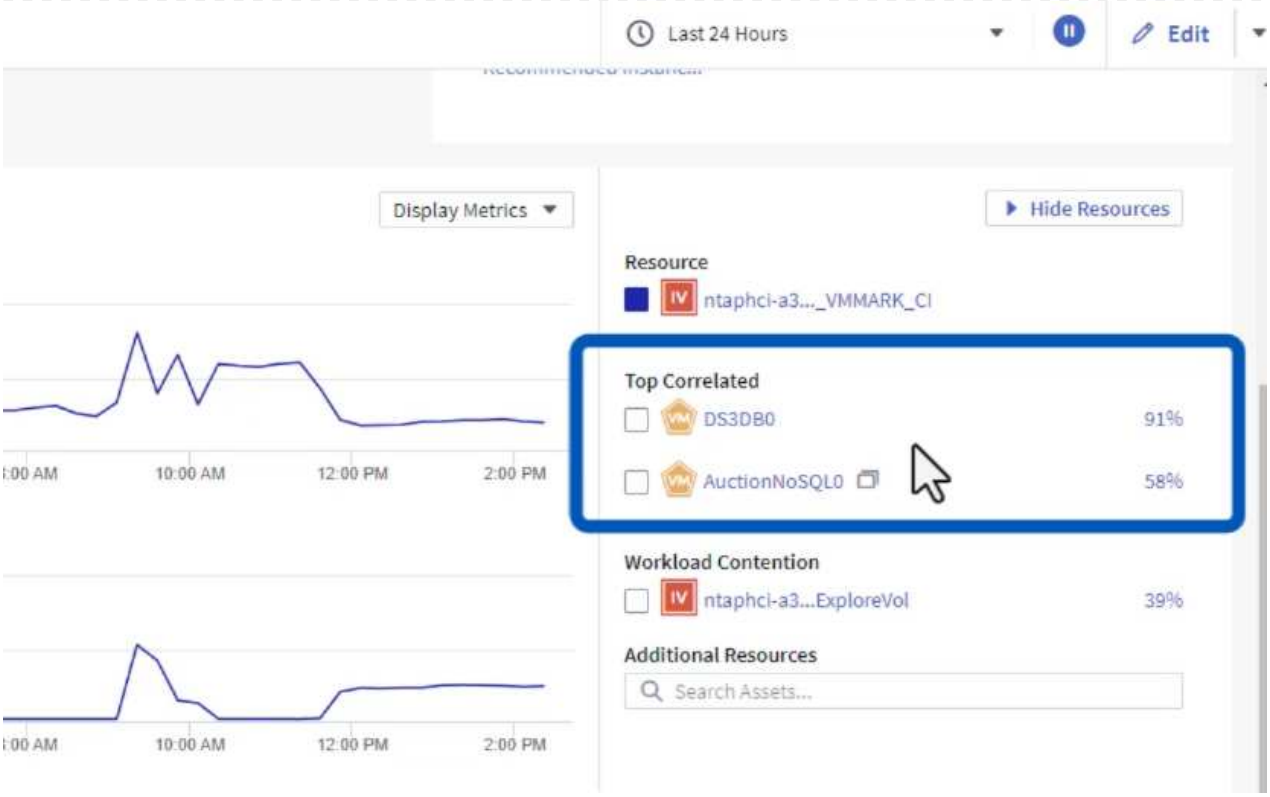
3. Escolha um painel para desempenho do FlexVol na lista e clique no botão **Adicionar painéis** na parte inferior da página.



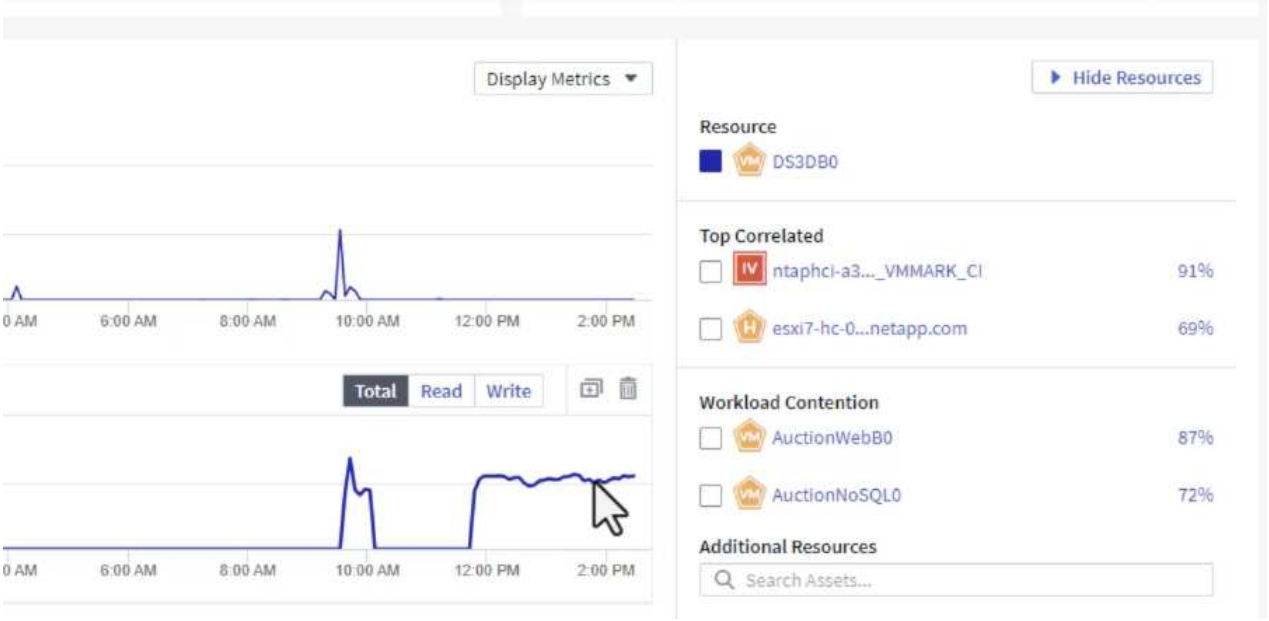
4. Após a importação, abra o painel. A partir daqui, você pode ver vários widgets com dados detalhados de desempenho. Adicione um filtro para visualizar um único sistema de armazenamento e selecione um volume de armazenamento para detalhar seus detalhes.



5. Nessa visualização, você pode ver várias métricas relacionadas a esse volume de armazenamento e as principais máquinas virtuais utilizadas e correlacionadas em execução no volume.



6. Clicar na VM com maior utilização detalha as métricas daquela VM para visualizar quaisquer problemas potenciais.



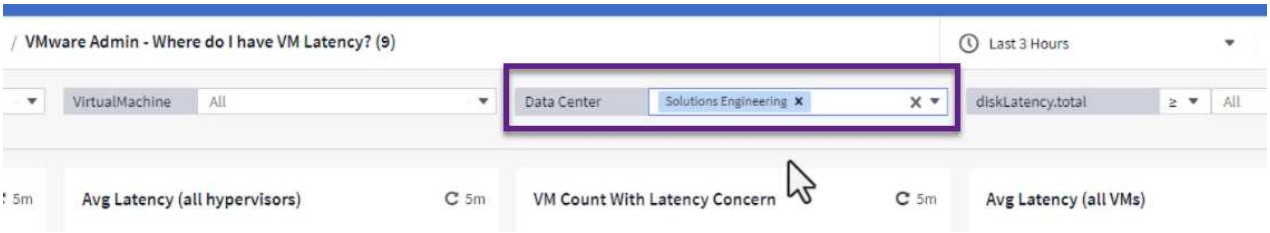
Use o Cloud Insights para identificar vizinhos barulhentos

O Cloud Insights apresenta painéis que podem isolar facilmente VMs pares que estão impactando negativamente outras VMs em execução no mesmo volume de armazenamento.

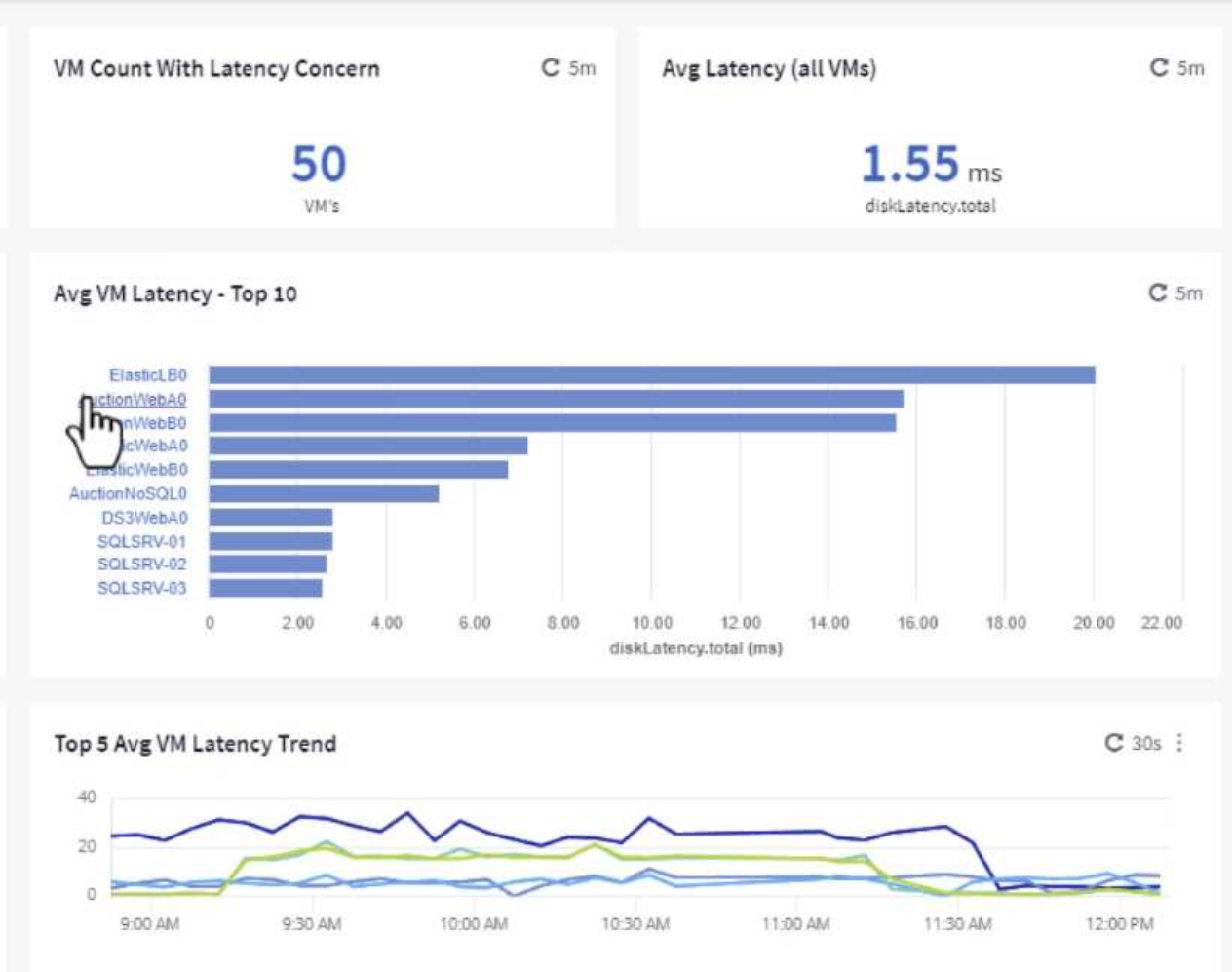
Use um painel de latência de VM superior para isolar vizinhos barulhentos

1. Neste exemplo, acesse um painel disponível na **Galeria** chamado **VMware Admin - Onde tenho latência de VM?**

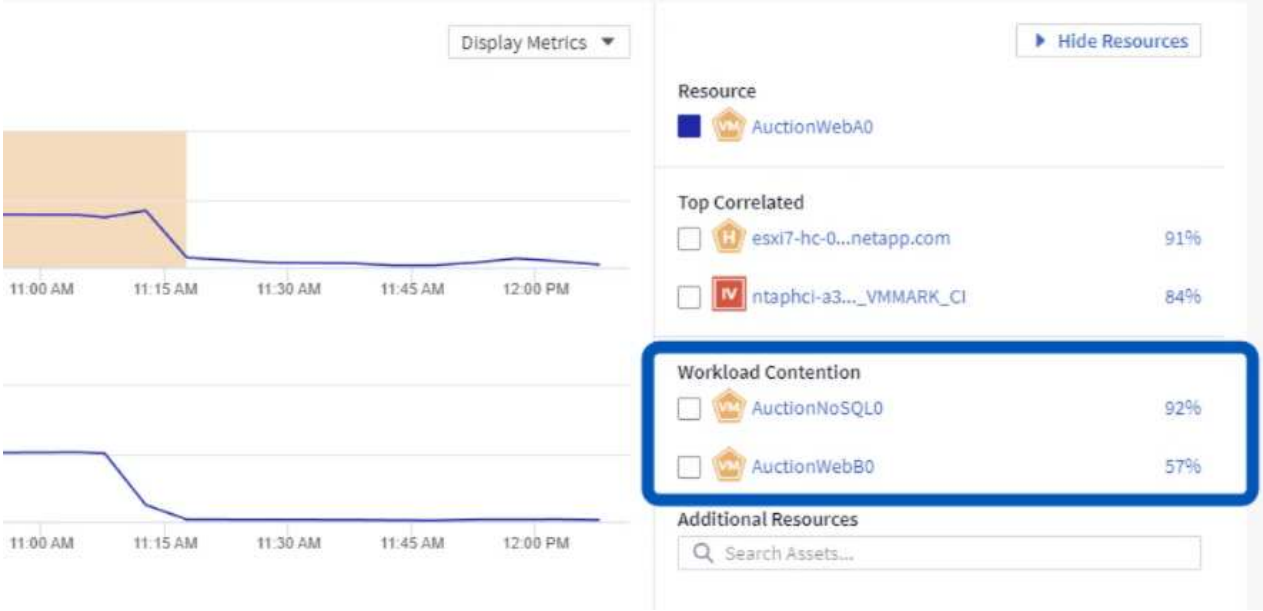
2. Em seguida, filtre pela anotação **Data Center** criada em uma etapa anterior para visualizar um subconjunto de ativos.



3. Este painel mostra uma lista das 10 principais VMs por latência média. A partir daqui, clique na VM em questão para ver seus detalhes.



4. As VMs que podem causar contenção de carga de trabalho estão listadas e disponíveis. Analise detalhadamente as métricas de desempenho dessas VMs para investigar possíveis problemas.

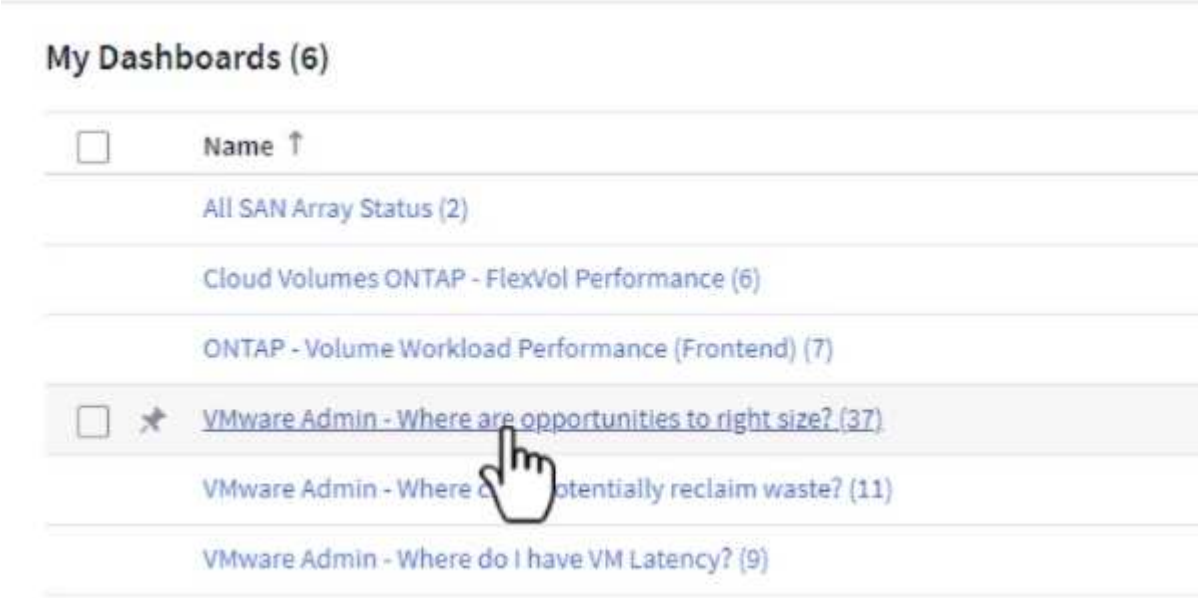


Visualize recursos super e subutilizados no Cloud Insights

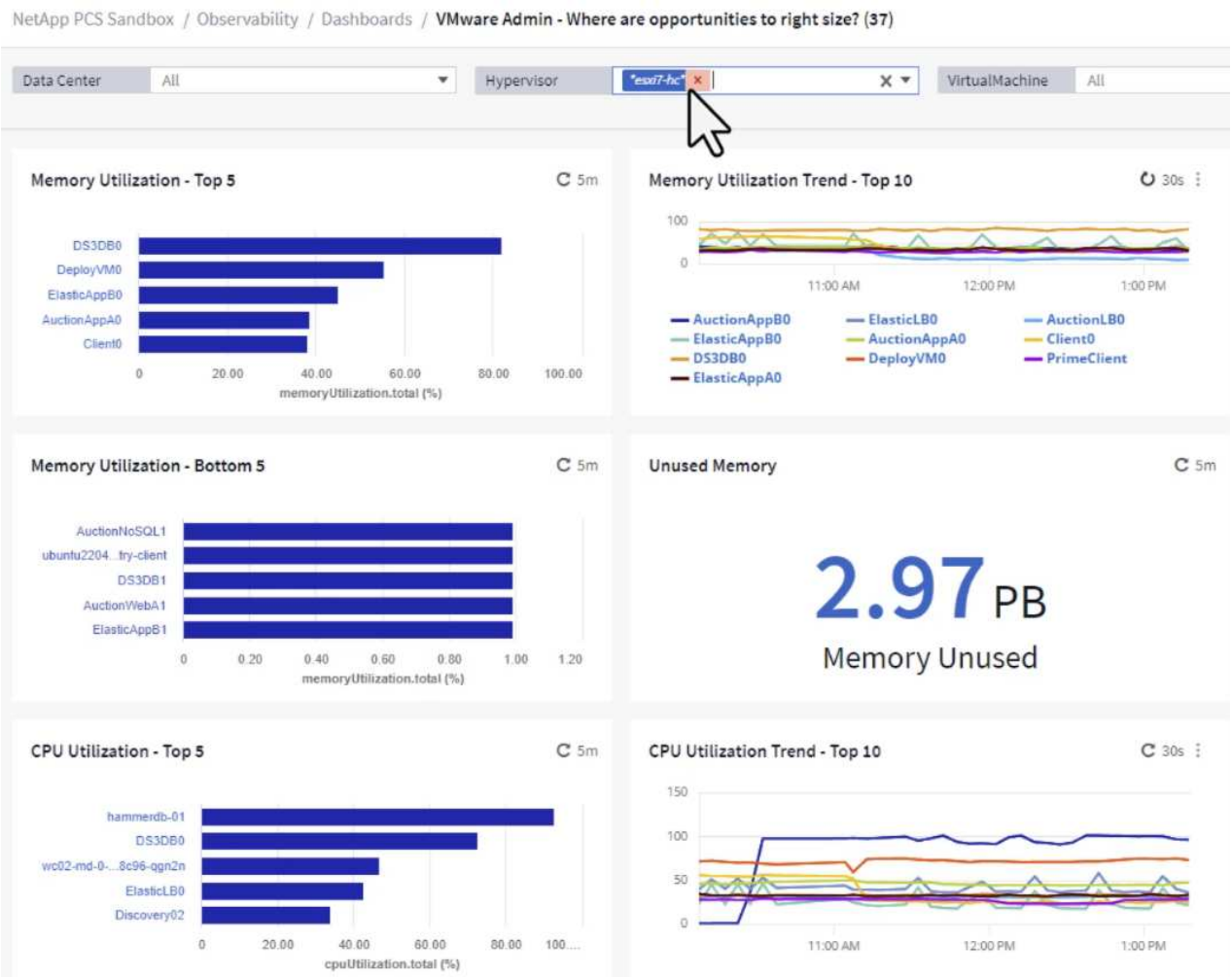
Ao combinar os recursos da VM com os requisitos reais da carga de trabalho, a utilização dos recursos pode ser otimizada, resultando em economia de custos em infraestrutura e serviços de nuvem. Os dados no Cloud Insights podem ser personalizados para exibir facilmente VMs super ou subutilizadas.

Identificar oportunidades para dimensionar corretamente as VMs

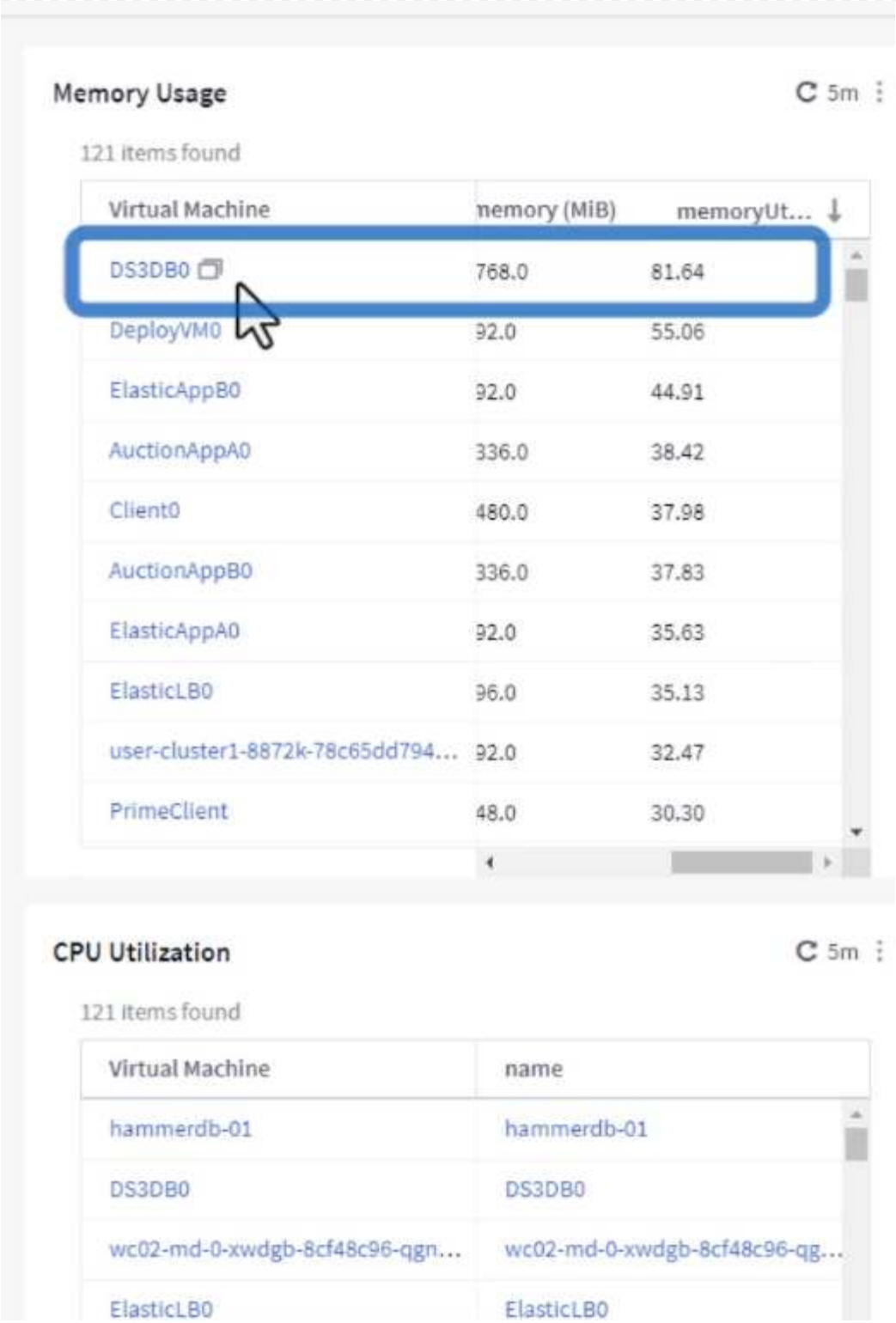
1. Neste exemplo, acesse um painel disponível na **Galeria** chamado **VMware Admin - Onde estão as oportunidades para dimensionar corretamente?**



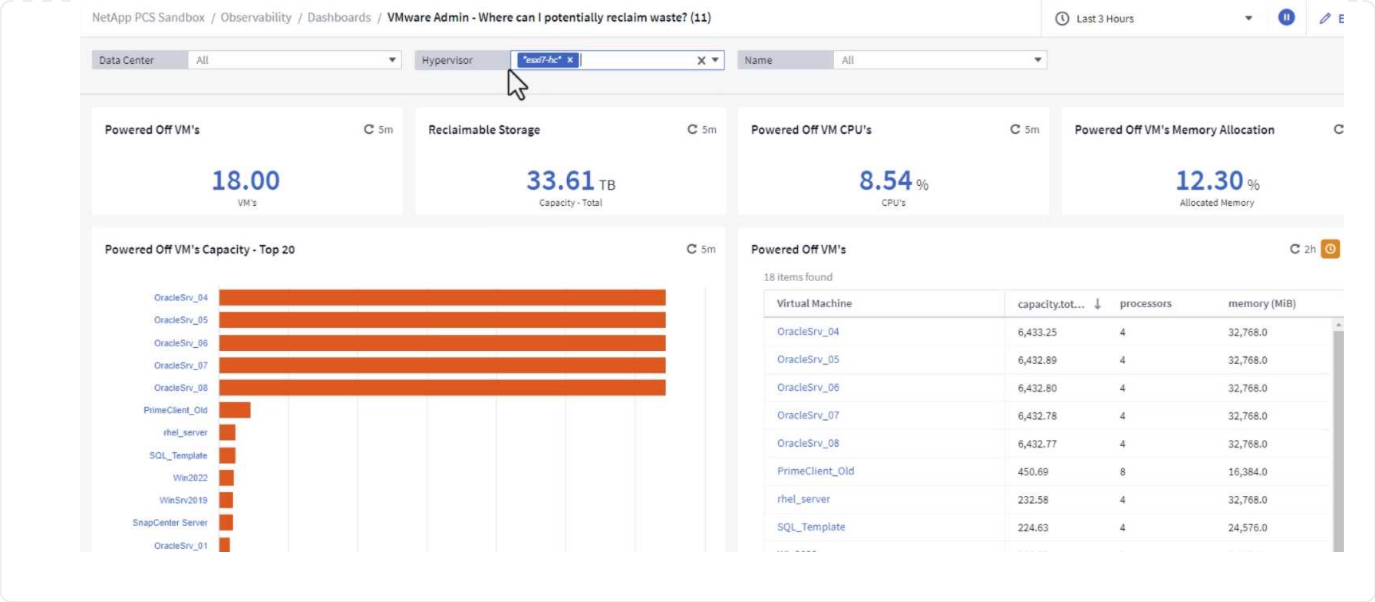
2. Primeiro filtre por todos os hosts ESXi no cluster. Você pode então ver a classificação das VMs superiores e inferiores por utilização de memória e CPU.



3. As tabelas permitem a classificação e fornecem mais detalhes com base nas colunas de dados escolhidas.



4. Outro painel chamado **VMware Admin - Onde posso potencialmente recuperar resíduos?** mostra as VMs desligadas classificadas por uso de capacidade.

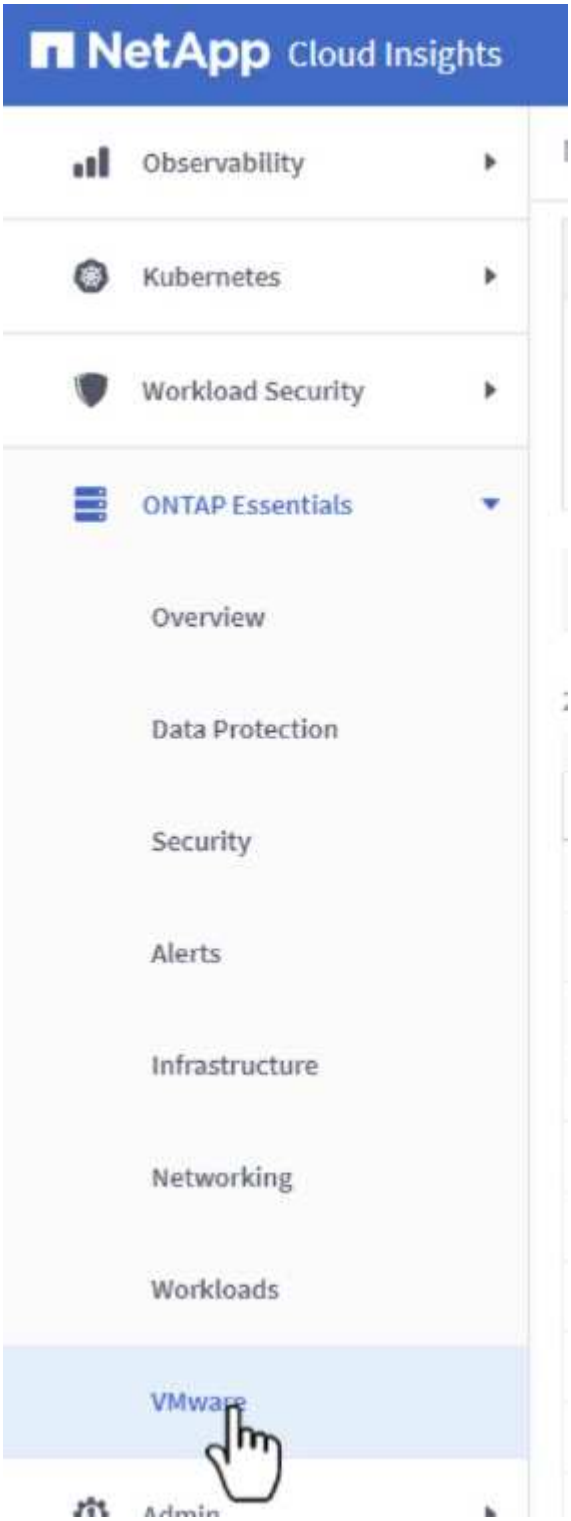


Use consultas para isolar e classificar métricas

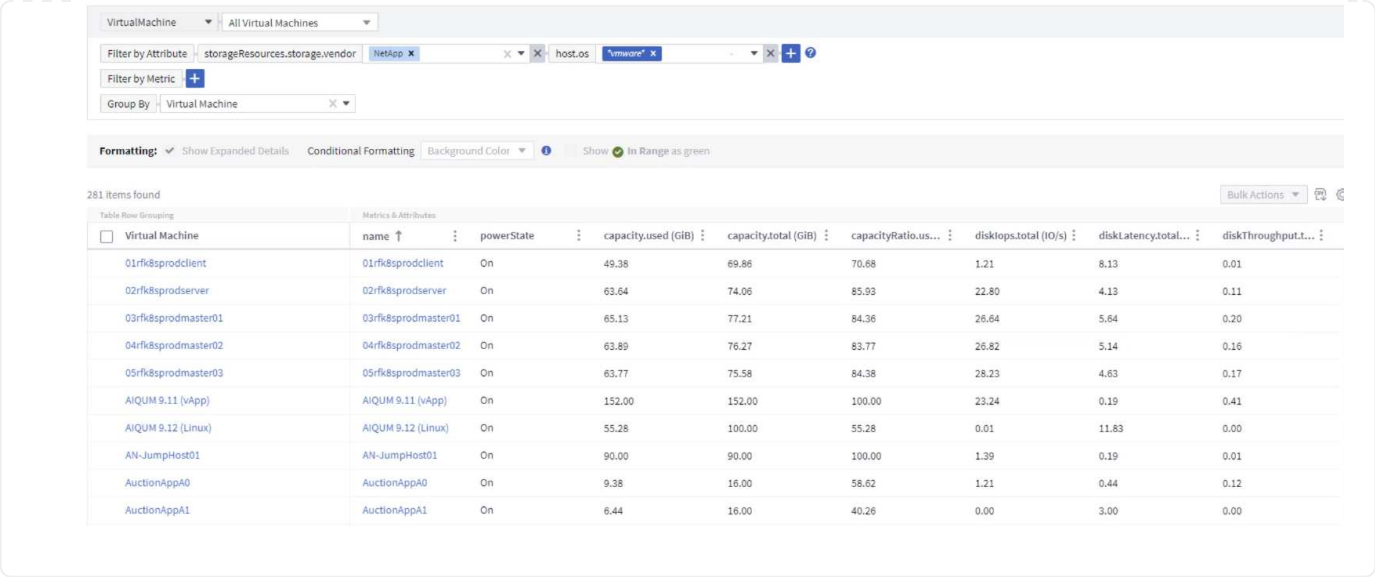
A quantidade de dados capturados pelo Cloud Insights é bastante abrangente. Consultas métricas fornecem uma maneira poderosa de classificar e organizar grandes quantidades de dados de maneiras úteis.

Veja uma consulta detalhada do VMware em ONTAP Essentials

1. Navegue até * ONTAP Essentials > VMware* para acessar uma consulta abrangente de métricas do VMware.



2. Nesta visualização, você verá várias opções para filtrar e agrupar os dados na parte superior. Todas as colunas de dados são personalizáveis e colunas adicionais podem ser facilmente adicionadas.



Conclusão

Esta solução foi projetada como uma introdução para aprender como começar a usar o NetApp Cloud Insights e mostrar alguns dos poderosos recursos que esta solução de observabilidade pode fornecer. Há centenas de painéis e consultas de métricas incorporados ao produto, o que facilita começar a usar imediatamente. A versão completa do Cloud Insights está disponível como teste de 30 dias e a versão básica está disponível gratuitamente para clientes da NetApp .

Informações adicionais

Para saber mais sobre as tecnologias apresentadas nesta solução, consulte as seguintes informações adicionais.

- "Página inicial do NetApp BlueXP e do Data Infrastructure Insights"
- "Documentação do NetApp Data Infrastructure Insights"

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.