Soluções de nuvem pública e híbrida da NetApp

NetApp public and hybrid cloud solutions

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/pt-br/netapp-solutions-cloud/index.html on November 11, 2026. Always check docs.netapp.com for the latest.

Índice

Soluções de nuvem pública e híbrida da NetApp . . . 1
Novidades nas soluções de nuvem pública e híbrida da NetApp . . . 2
NetApp Hybrid Multicloud com soluções VMware . . . 3
VMware para nuvem pública . . . 3
Visão geral do NetApp Hybrid Multicloud com VMware . . . 3
Soluções NetApp para VMware em Hyperscalers . . . 7
Configurações com suporte para NetApp Hybrid Multicloud com VMware . . . 10
VMware na configuração de hiperescaladores . . . 10
Armazenamento NetApp em nuvens públicas . . . 35
Resumo e conclusão: Por que NetApp Hybrid Multicloud com VMware . . . 137
Casos de uso da nuvem híbrida VMware . . . 139
Casos de uso para NetApp Hybrid Multicloud com VMware . . . 139
Soluções NetApp para VMware em Hyperscalers . . . 140
Soluções NetApp para Amazon VMware Managed Cloud (VMC) . . . 141
Soluções NetApp para Azure VMware Solution (AVS) . . . 141
Soluções NetApp para Google Cloud VMware Engine (GCVE) . . . 142
NetApp para AWS/VMC . . . 142
Recursos da NetApp para AWS VMC . . . 142
Proteja cargas de trabalho na AWS/VMC . . . 143
Migrar cargas de trabalho na AWS/VMC . . . 259
NetApp para AWS / EVS . . . 274
Monte o FSx ONTAP como armazenamento de dados externo para EVS . . . 274
Proteger o datastore FSx ONTAP para Exchange Virtual Server . . . 298
NetApp para Azure / AVS . . . 331
Recursos da NetApp para Azure AVS . . . 332
Proteja cargas de trabalho no Azure / AVS . . . 333
Migrar cargas de trabalho no Azure/AVS . . . 401
NetApp para GCP/GCVE . . . 415
Recursos da NetApp para o Google Cloud Platform GCVE . . . 415
Proteja cargas de trabalho no GCP/GCVE . . . 416
Migrar cargas de trabalho no GCP/GCVE . . . 448
Dados seguros com o Google Cloud NetApp Volumes no Google Cloud . . . 465
O NetApp Disaster Recovery . . . 534
Proteção de dados 3-2-1 para o VMware com o SnapCenter Plug-in e o NetApp Backup and Recovery para proteger cargas de trabalho do VMware . . . 534
O NetApp Disaster Recovery . . . 568
Multicloud híbrida NetApp com cargas de trabalho de contêiner Red Hat OpenShift . . . 610
Começar . . . 610
Soluções NetApp Hybrid Multicloud para cargas de trabalho do Red Hat OpenShift Container . . . 610
Propostas de valor das soluções NetApp Hybrid Multicloud para cargas de trabalho do Red Hat OpenShift Container . . . 612
Soluções suportadas do NetApp Hybrid Multicloud para cargas de trabalho do Red Hat OpenShift Container . . . 613

Versões de vários componentes usados na validação da solução . . . 617
Integrações do NetApp Storage com Red Hat OpenShift Containers . . . 618
Documentação adicional . . . 622
Openshift para instalações locais . . . 622
Solução NetApp com cargas de trabalho da plataforma Red Hat OpenShift Container no VMware . . . 622
Implantar e configurar a plataforma Red Hat OpenShift Container no VMware . . . 623
Proteção de dados usando Trident Protect . . . 625
Nuvem híbrida com componentes autogerenciados . . . 626
Solução NetApp com cargas de trabalho da plataforma Red Hat OpenShift Container em Nuvem Híbrida . . . 626
Implantar e configurar a plataforma Red Hat OpenShift Container na AWS . . . 628
Implantar e configurar o Red Hat OpenShift Container Platform no Google Cloud . . . 630
Implantar e configurar a plataforma Red Hat OpenShift Container no Azure . . . 632
Proteção de dados usando Trident Protect . . . 635
Nuvem híbrida com componentes gerenciados pelo provedor . . . 635
Solução NetApp com cargas de trabalho da plataforma Managed Red Hat OpenShift Container . . . 636
Implantar e configurar a plataforma Managed Red Hat OpenShift Container na AWS . . . 636
Implantar e configurar o OpenShift Dedicated no Google Cloud com o Google Cloud NetApp Volumes 639
Proteção de dados . . . 641
Soluções adicionais de multicloud híbrida da NetApp para cargas de trabalho do Red Hat OpenShift . 642
Proteja os dados usando o Trident Protect . . . 642
Proteção de dados para aplicativos em contêineres na OpenShift Container Platform usando Trident Protect . . . 642
Proteja VMs no Red Hat OpenShift Virtualization usando Trident Protect . . . 654
Proteja aplicativos de contêiner usando ferramentas de terceiros . . . 674
Proteção de dados para aplicativos de contêiner na plataforma de contêiner OpenShift usando a API OpenShift para proteção de dados (OADP) . . . 674
Instalação do Operador OpenShift API for Data Protection (OADP) . . . 676
Criação de backup sob demanda para aplicativos no OpenShift Container Platform . . . 685
Migrar um aplicativo de um cluster para outro . . . 688
Restaurar um aplicativo a partir de um backup . . . 692
Excluindo backups e restaurações usando Velero . . . 699
Assista a vídeos e demonstrações sobre soluções multicloud híbridas com a NetApp . . . 701
Assista a vídeos sobre soluções multicloud híbridas para Amazon Web Services com NetApp . . . 701
Armazenamento conectado ao convidado . . . 701
TCO e armazenamentos de dados suplementares . . . 701
Fluxos de trabalho de migração (HCX) . . . 701
Assista a vídeos sobre soluções multicloud híbridas para a nuvem Azure VMware com a NetApp . . . 701
Armazenamentos de dados suplementares . . . 701
Recuperação de desastres . . . 702
Fluxos de trabalho de migração (HCX) . . . 702
Assista a vídeos sobre soluções multicloud híbridas para Red Hat OpenShift com NetApp . . . 702
Snapshots e restauração . . . 702
Integração de armazenamento . . . 702
Failover e failback . . . 702

Automação de soluções . . . 702
Leia blogs sobre soluções em nuvem de especialistas da NetApp . . . 703
Integração do VMware com AWS e Amazon FSx para ONTAP . . . 703
Solução Azure VMware . . . 703
Google Cloud VMware Engine . . . 703
Proteção e gestão de dados . . . 703
Cargas de trabalho de contêiner NetApp para OpenShift . . . 703
Nuvem soberana da VMware . . . 703
Avisos legais . . . 704
Direitos autorais . . . 704
Marcas Registradas . . . 704
Patentes . . . 704
Política de Privacidade . . . 704

Soluções de nuvem pública e híbrida da NetApp

Novidades nas soluções de nuvem pública e híbrida da NetApp

Saiba o que há de novo em soluções de nuvem pública e híbrida.

[[18-august-2025]]
== 18 de agosto de 2025

O site da NetApp Solutions agora é o"Família de soluções NetApp" , que inclui os seguintes sites:

- "Soluções de inteligência artificial da NetApp"
- "Soluções de contêiner NetApp"
- "Soluções de gerenciamento de dados da NetApp"
- "Soluções de banco de dados NetApp"
- Soluções de nuvem pública e híbrida da NetApp
- "Soluções NetApp para SAP"
- "Soluções de virtualização da NetApp"

NetApp Hybrid Multicloud com soluções VMware

VMware para nuvem pública

Visão geral do NetApp Hybrid Multicloud com VMware

A maioria das organizações de TI segue a abordagem de nuvem híbrida em primeiro lugar. Essas organizações estão em uma fase de transformação e os clientes estão avaliando seu cenário atual de TI e, em seguida, migrando suas cargas de trabalho para a nuvem com base no exercício de avaliação e descoberta.

Os fatores que levam os clientes a migrarem para a nuvem podem incluir elasticidade e explosão, saída do data center, consolidação do data center, cenários de fim de vida útil, fusões, aquisições e assim por diante. O motivo dessa migração pode variar de acordo com cada organização e suas respectivas prioridades comerciais. Ao migrar para a nuvem híbrida, escolher o armazenamento certo na nuvem é muito importante para liberar o poder da implantação e da elasticidade da nuvem.

Opções do VMware Cloud na Nuvem Pública

Esta seção descreve como cada um dos provedores de nuvem oferece suporte a uma pilha VMware Software Defined Data Center (SDDC) e/ou VMware Cloud Foundation (VCF) em suas respectivas ofertas de nuvem pública.

Solução VMware do Azure

O Azure VMware Solution é um serviço de nuvem híbrida que permite SDDCs VMware totalmente funcionais dentro da nuvem pública do Microsoft Azure. O Azure VMware Solution é uma solução primária totalmente gerenciada e suportada pela Microsoft, verificada pela VMware e que aproveita a infraestrutura do Azure. Isso significa que, quando o Azure VMware Solution é implantado, os clientes obtêm o ESXi da VMware para virtualização de computação, o vSAN para armazenamento hiperconvergente e o NSX para rede e segurança, tudo isso aproveitando a presença global do Microsoft Azure, as instalações de data center líderes da categoria e a proximidade com o rico ecossistema de serviços e soluções nativos do Azure.

VMware Cloud na AWS

O VMware Cloud on AWS traz o software SDDC de nível empresarial da VMware para a AWS Cloud com acesso otimizado aos serviços nativos da AWS. Com a tecnologia VMware Cloud Foundation, o VMware Cloud on AWS integra os produtos de computação, armazenamento e virtualização de rede da VMware (VMware vSphere, VMware vSAN e VMware NSX) juntamente com o gerenciamento do VMware vCenter Server, otimizado para execução em infraestrutura AWS dedicada, elástica e bare-metal.

Google Cloud VMware Engine

O Google Cloud VMware Engine é uma oferta de infraestrutura como serviço (IaaS) desenvolvida com base na infraestrutura escalável de alto desempenho do Google Cloud e na pilha VMware Cloud Foundation – VMware vSphere, vCenter, vSAN e NSX-T. Este serviço permite um caminho rápido para a nuvem, migrando ou estendendo cargas de trabalho VMware existentes de ambientes locais para o Google Cloud Platform sem o custo, esforço ou risco de rearquitetar aplicativos ou reestruturar operações. É um serviço vendido e suportado pelo Google, trabalhando em estreita colaboração com a VMware.



A nuvem privada SDDC e a colocation do NetApp Cloud Volumes oferecem o melhor desempenho com latência de rede mínima.

Você sabia?

Independentemente da nuvem usada, quando um SDDC da VMware é implantado, o cluster inicial inclui os seguintes produtos:

- Hosts VMware ESXi para virtualização de computação com um dispositivo vCenter Server para gerenciamento
- Armazenamento hiperconvergente VMware vSAN incorporando os ativos de armazenamento físico de cada host ESXi
- VMware NSX para rede virtual e segurança com um cluster NSX Manager para gerenciamento

Configuração de armazenamento

Para clientes que planejam hospedar cargas de trabalho com uso intensivo de armazenamento e escalar em qualquer solução VMware hospedada na nuvem, a infraestrutura hiperconvergente padrão determina que a expansão deve ocorrer nos recursos de computação e armazenamento.

Ao integrar com o NetApp Cloud Volumes, como Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponível em todos os três principais hiperescaladores) e Google Cloud NetApp Volumes para Google Cloud, os clientes agora têm opções para dimensionar seu armazenamento separadamente de forma independente e adicionar nós de computação ao cluster SDDC somente quando necessário.

Observações:

- A VMware não recomenda configurações de cluster desbalanceadas, portanto, expandir o armazenamento significa adicionar mais hosts, o que implica em mais TCO.
- Somente um ambiente vSAN é possível. Portanto, todo o tráfego de armazenamento competirá diretamente com as cargas de trabalho de produção.
- Não há opção para fornecer vários níveis de desempenho para alinhar os requisitos do aplicativo, desempenho e custo.
- É muito fácil atingir os limites da capacidade de armazenamento do vSAN criado sobre os hosts do cluster. Use o NetApp Cloud Volumes para dimensionar o armazenamento para hospedar conjuntos de dados ativos ou armazenar dados mais frios em camadas para armazenamento persistente.

Azure NetApp Files, Amazon FSx ONTAP, Cloud Volumes ONTAP (disponível em todos os três principais hiperescaladores) e Google Cloud NetApp Volumes para Google Cloud podem ser usados em conjunto com VMs convidadas. Essa arquitetura de armazenamento híbrido consiste em um armazenamento de dados vSAN que contém os dados binários do aplicativo e do sistema operacional convidado. Os dados do aplicativo são anexados à VM por meio de um iniciador iSCSI baseado em convidado ou de montagens NFS/SMB que se comunicam diretamente com o Amazon FSx ONTAP, Cloud Volume ONTAP, Azure NetApp Files e Google Cloud NetApp Volumes para Google Cloud, respectivamente. Essa configuração permite que você supere facilmente os desafios com capacidade de armazenamento, pois com o vSAN o espaço livre disponível depende do espaço livre e das políticas de armazenamento usadas.

Vamos considerar um cluster SDDC de três nós no VMware Cloud na AWS:

- A capacidade bruta total para um SDDC de três nós = 31,1 TB (aproximadamente 10 TB para cada nó).
- O espaço de folga a ser mantido antes da inclusão de hosts adicionais = 25% = (0,25 x 31,1 TB) = 7,7 TB.
- Capacidade bruta utilizável após dedução do espaço livre = 23,4 TB
- O espaço livre efetivo disponível depende da política de armazenamento aplicada.

Por exemplo:

- RAID 0 = espaço livre efetivo = 23,4 TB (capacidade bruta utilizável/1)
- RAID 1 = espaço livre efetivo = 11,7 TB (capacidade bruta utilizável/2)
- RAID 5 = espaço livre efetivo = 17,5 TB (capacidade bruta utilizável/1,33)

Portanto, usar o NetApp Cloud Volumes como armazenamento conectado ao convidado ajudaria a expandir o armazenamento e otimizar o TCO, ao mesmo tempo em que atenderia aos requisitos de desempenho e proteção de dados.

> O armazenamento no local era a única opção disponível no momento em que este documento foi escrito.

Pontos a serem lembrados

- Em modelos de armazenamento híbrido, coloque cargas de trabalho de nível 1 ou de alta prioridade no armazenamento de dados vSAN para atender a quaisquer requisitos de latência específicos, porque elas fazem parte do próprio host e estão próximas. Use mecanismos no convidado para quaisquer VMs de carga de trabalho para as quais latências transacionais sejam aceitáveis.
- Use a tecnologia NetApp SnapMirror para replicar os dados da carga de trabalho do sistema ONTAP no local para o Cloud Volumes ONTAP ou o Amazon FSx ONTAP, para facilitar a migração usando mecanismos em nível de bloco. Isso não se aplica ao Azure NetApp Files nem ao Google Cloud NetApp Volumes. Para migrar dados para o Azure NetApp Files ou o Google Cloud NetApp Volumes, use NetApp XCP, NetApp Copy and Sync, rysnc ou robocopy, dependendo do protocolo de arquivo usado.
- Os testes mostram uma latência adicional de 2 a 4 ms ao acessar o armazenamento dos respectivos SDDCs. Considere essa latência adicional nos requisitos do aplicativo ao mapear o armazenamento.
- Para montar o armazenamento conectado ao convidado durante o failover de teste e o failover real, certifique-se de que os iniciadores iSCSI estejam reconfigurados, o DNS esteja atualizado para compartilhamentos SMB e os pontos de montagem NFS estejam atualizados no fstab.
- Certifique-se de que as configurações do registro de tempo limite de disco, firewall e Microsoft Multipath I/O (MPIO) no convidado estejam configuradas corretamente dentro da VM.

> Isso se aplica somente ao armazenamento conectado por convidado.

Benefícios do armazenamento em nuvem da NetApp

O armazenamento em nuvem da NetApp oferece os seguintes benefícios:

- Melhora a densidade da computação para armazenamento ao dimensionar o armazenamento independentemente da computação.
- Permite reduzir a contagem de hosts, reduzindo assim o TCO geral.
- Falha no nó de computação não afeta o desempenho do armazenamento.
- A remodelação de volume e a capacidade de nível de serviço dinâmico do Azure NetApp Files permitem otimizar custos por meio do dimensionamento para cargas de trabalho de estado estável, evitando assim o provisionamento excessivo.
- As eficiências de armazenamento, a divisão em camadas da nuvem e os recursos de modificação do tipo de instância do Cloud Volumes ONTAP permitem maneiras ideais de adicionar e dimensionar o armazenamento.

- Evita o excesso de provisionamento de recursos de armazenamento, que são adicionados somente quando necessário.
- Cópias e clones de Snapshot eficientes permitem que você crie cópias rapidamente sem nenhum impacto no desempenho.
- Ajuda a lidar com ataques de ransomware usando recuperação rápida de cópias de Snapshot.
- Fornece recuperação de desastres regional eficiente baseada em transferência de bloco incremental e nível de bloco de backup integrado entre regiões, proporcionando melhor RPO e RTOs.

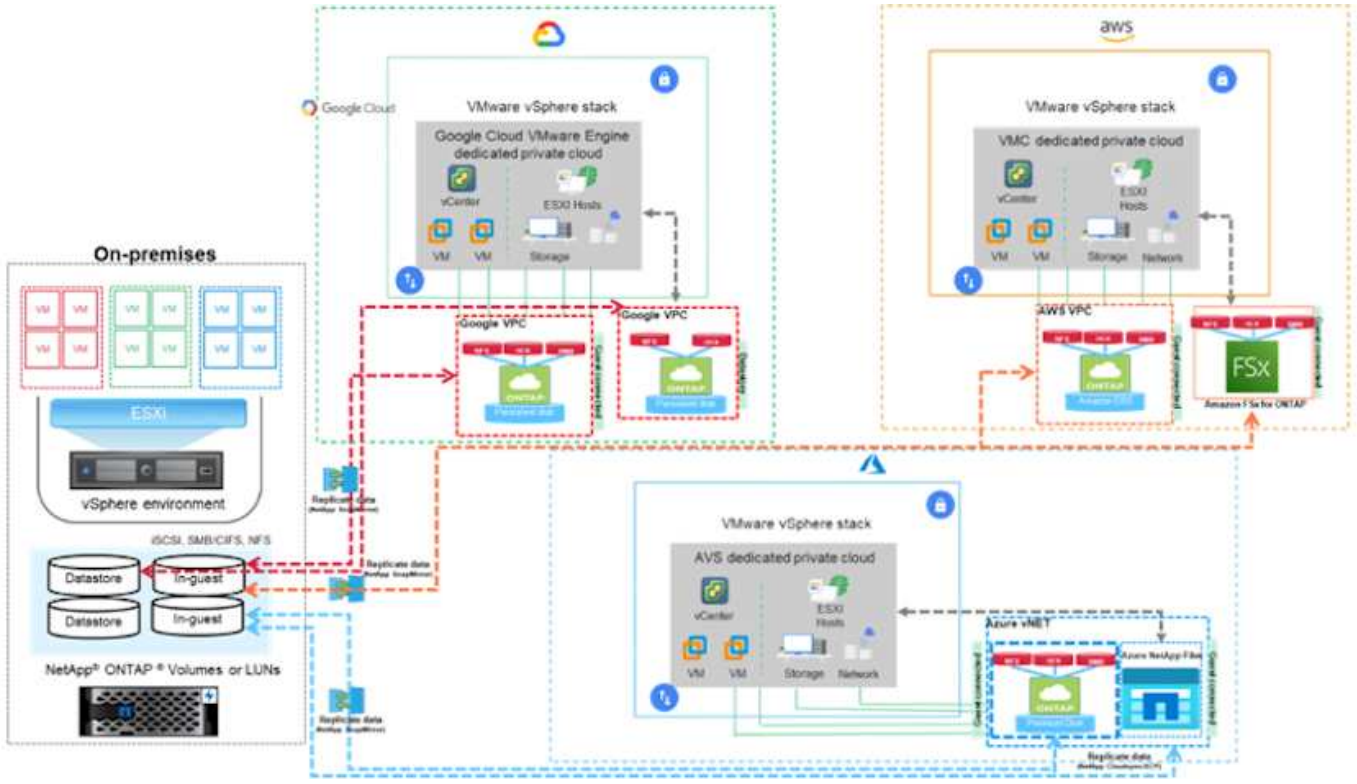
Suposições

- A tecnologia SnapMirror ou outros mecanismos relevantes de migração de dados estão habilitados. Há muitas opções de conectividade, desde locais até qualquer nuvem hiperescalável. Use o caminho apropriado e trabalhe com as equipes de rede relevantes.
- O armazenamento no local era a única opção disponível no momento em que este documento foi escrito.

> Contrate arquitetos de soluções da NetApp e os respectivos arquitetos de nuvem hiperescaladora para planejamento e dimensionamento do armazenamento e do número necessário de hosts. A NetApp recomenda identificar os requisitos de desempenho de armazenamento antes de usar o dimensionador Cloud Volumes ONTAP para finalizar o tipo de instância de armazenamento ou o nível de serviço apropriado com a taxa de transferência correta.

Arquitetura detalhada

De uma perspectiva de alto nível, esta arquitetura (mostrada na figura abaixo) aborda como obter conectividade multicloud híbrida e portabilidade de aplicativos entre vários provedores de nuvem usando o NetApp Cloud Volumes ONTAP, o Google Cloud NetApp Volumes para Google Cloud e o Azure NetApp Files como uma opção adicional de armazenamento no convidado.



Soluções NetApp para VMware em Hyperscalers

Saiba mais sobre os recursos que a NetApp oferece aos três (3) hiperescaladores principais — desde o NetApp como um dispositivo de armazenamento conectado a convidados ou um armazenamento de dados NFS suplementar até fluxos de trabalho de migração, extensão/estouro para a nuvem, backup/restauração e recuperação de desastres.

Escolha sua nuvem e deixe a NetApp fazer o resto!



Para ver os recursos de um hiperescalador específico, clique na guia apropriada para esse hiperescalador.

Vá para a seção do conteúdo desejado selecionando entre as seguintes opções:

- "VMware na configuração de hiperescaladores"
- "Opções de armazenamento da NetApp"
- "Soluções de nuvem NetApp /VMware"

VMware na configuração de hiperescaladores

Assim como no local, planejar um ambiente de virtualização baseado em nuvem é essencial para um ambiente de produção bem-sucedido, pronto para criação de VMs e migração.

AWS / VMC

Esta seção descreve como configurar e gerenciar o VMware Cloud on AWS SDDC e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP ao AWS VMC.

O processo de configuração pode ser dividido nas seguintes etapas:

- Implantar e configurar o VMware Cloud para AWS
- Conecte o VMware Cloud ao FSx ONTAP

Veja o detalhado"etapas de configuração para VMC" .

Azure / AVS

Esta seção descreve como configurar e gerenciar o Azure VMware Solution e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP ao Azure VMware Solution.

O processo de configuração pode ser dividido nas seguintes etapas:

- Registre o provedor de recursos e crie uma nuvem privada
- Conectar-se a um gateway de rede virtual ExpressRoute novo ou existente
- Valide a conectividade de rede e acesse a nuvem privada

Veja o detalhado"etapas de configuração para AVS" .

GCP / GCVE

Esta seção descreve como configurar e gerenciar o GCVE e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP e o Google Cloud NetApp Volumes ao GCVE.

O processo de configuração pode ser dividido nas seguintes etapas:

- Implantar e configurar o GCVE
- Habilitar acesso privado ao GCVE

Veja o detalhado"etapas de configuração para GCVE" .

Opções de armazenamento da NetApp

O armazenamento NetApp pode ser utilizado de diversas maneiras — como convidado conectado ou como um armazenamento de dados NFS suplementar — dentro de cada um dos três principais hiperescaladores.

Por favor visite"Opções de armazenamento NetApp suportadas" para maiores informações.

AWS / VMC

A AWS oferece suporte ao armazenamento NetApp nas seguintes configurações:

- FSx ONTAP como armazenamento conectado a convidados
- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados

- FSx ONTAP como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para VMC" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para VMC" .

Azure / AVS

O Azure oferece suporte ao armazenamento NetApp nas seguintes configurações:

- Azure NetApp Files (ANF) como armazenamento conectado a convidados
- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- Azure NetApp Files (ANF) como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para AVS" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para AVS" .

GCP / GCVE

O Google Cloud oferece suporte ao armazenamento NetApp nas seguintes configurações:

- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- Google Cloud NetApp Volumes (NetApp Volumes) como armazenamento conectado a convidados
- Google Cloud NetApp Volumes (NetApp Volumes) como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para GCVE" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para GCVE" .

Leia mais sobre"Suporte ao armazenamento de dados do Google Cloud NetApp Volumes para o Google Cloud VMware Engine (blog da NetApp)" ou"Como usar o Google Cloud NetApp Volumes como armazenamento de dados para o Google Cloud VMware Engine (blog do Google)"

Soluções de nuvem NetApp /VMware

Com as soluções de nuvem da NetApp e da VMware, muitos casos de uso são simples de implantar no hiperescalador de sua escolha. A VMware define os principais casos de uso de carga de trabalho na nuvem como:

- Proteger (inclui recuperação de desastres e backup/restauração)
- Migrar
- Estender

AWS / VMC

"Navegue pelas soluções NetApp para AWS / VMC"

Azure / AVS

"Navegue pelas soluções NetApp para Azure / AVS"

GCP / GCVE

"Navegue pelas soluções da NetApp para o Google Cloud Platform (GCP) / GCVE"

Configurações com suporte para NetApp Hybrid Multicloud com VMware

Entendendo as combinações para suporte de armazenamento NetApp nos principais hiperescaladores.

	Convidado conectado	Armazenamento de dados NFS suplementar
AWS	CVO FSx ONTAP"Detalhes"	FSx ONTAP"Detalhes"
Azul	CVO ANF"Detalhes"	ANF"Detalhes"
GCP	CVO NetApp Volumes"Detalhes"	Volumes NetApp"Detalhes"

VMware na configuração de hiperescaladores

Configurando o ambiente de virtualização no provedor de nuvem

Detalhes sobre como configurar o ambiente de virtualização em cada um dos hiperescaladores suportados são abordados aqui.

AWS / VMC

Esta seção descreve como configurar e gerenciar o VMware Cloud on AWS SDDC e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP ao AWS VMC.

O processo de configuração pode ser dividido nas seguintes etapas:

- Implantar e configurar o VMware Cloud para AWS
- Conecte o VMware Cloud ao FSx ONTAP

Veja o detalhado"etapas de configuração para VMC" .

Azure / AVS

Esta seção descreve como configurar e gerenciar o Azure VMware Solution e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP ao Azure VMware Solution.

O processo de configuração pode ser dividido nas seguintes etapas:

- Registre o provedor de recursos e crie uma nuvem privada
- Conectar-se a um gateway de rede virtual ExpressRoute novo ou existente
- Valide a conectividade de rede e acesse a nuvem privada

Veja o detalhado"etapas de configuração para AVS" .

GCP / GCVE

Esta seção descreve como configurar e gerenciar o GCVE e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP e o Google Cloud NetApp Volumes ao GCVE.

O processo de configuração pode ser dividido nas seguintes etapas:

- Implantar e configurar o GCVE
- Habilitar acesso privado ao GCVE

Veja o detalhado"etapas de configuração para GCVE" .

Implantar e configurar o ambiente de virtualização na AWS

Assim como no local, o planejamento do VMware Cloud on AWS é essencial para um ambiente de produção bem-sucedido, pronto para criação de VMs e migração.

Esta seção descreve como configurar e gerenciar o VMware Cloud on AWS SDDC e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é atualmente o único método suportado para conectar o Cloud Volumes ONTAP (CVO) ao AWS VMC.

O processo de configuração pode ser dividido nas seguintes etapas:

▼ **Implantar e configurar o VMware Cloud para AWS**

"VMware Cloud na AWS"fornece uma experiência nativa em nuvem para cargas de trabalho baseadas em VMware no ecossistema da AWS. Cada VMware Software-Defined Data Center (SDDC) é executado em uma Amazon Virtual Private Cloud (VPC) e fornece uma pilha VMware completa (incluindo o vCenter Server), rede definida por software NSX-T, armazenamento definido por software vSAN e um ou mais hosts ESXi que fornecem recursos de computação e armazenamento para suas cargas de trabalho.

Esta seção descreve como configurar e gerenciar o VMware Cloud on AWS e usá-lo em combinação com o Amazon FSx ONTAP e/ou Cloud Volumes ONTAP on AWS com armazenamento no guest.

> O armazenamento no convidado é atualmente o único método suportado para conectar o Cloud Volumes ONTAP (CVO) ao AWS VMC.

O processo de configuração pode ser dividido em três partes:

▼ **Registre-se para uma conta AWS**

Registre-se para um"Conta da Amazon Web Services" .

Você precisa de uma conta AWS para começar, supondo que ainda não haja uma criada. Nova ou existente, você precisa de privilégios administrativos na conta para muitas etapas deste procedimento. Veja isto"link" para obter mais informações sobre as credenciais da AWS.

▼ **Registre-se para uma conta My VMware**

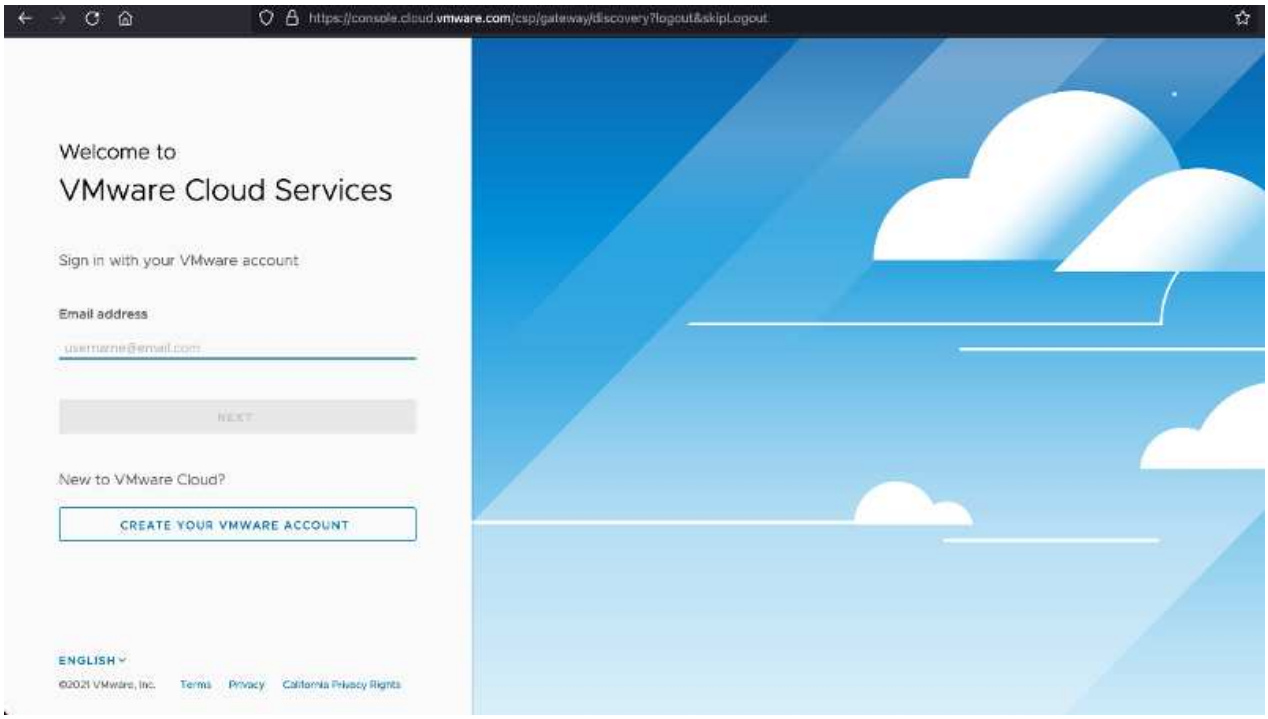
Registre-se para um"Meu VMware" conta.

Para acessar o portfólio de nuvem da VMware (incluindo o VMware Cloud on AWS), você precisa de uma conta de cliente VMware ou de uma conta My VMware. Se ainda não o fez, crie uma conta VMware"aqui" .

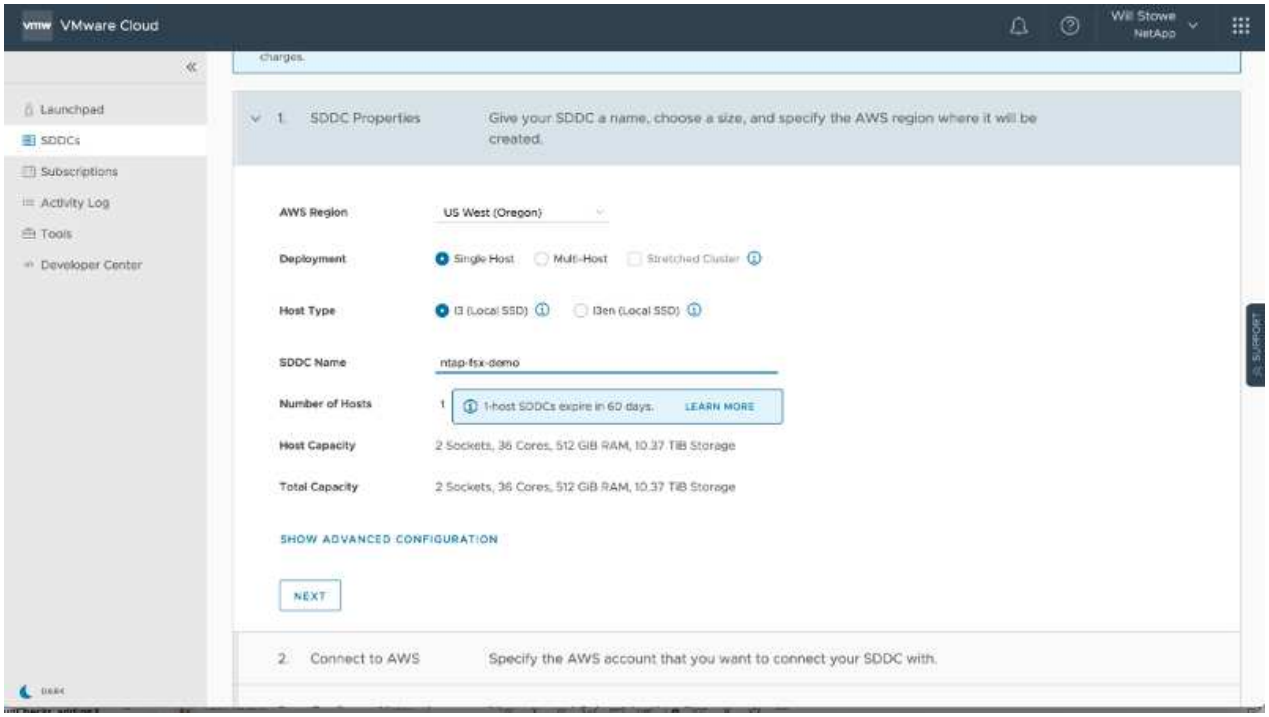
▼ **Provisionar SDDC no VMware Cloud**

Depois que a conta VMware for configurada e o dimensionamento adequado for realizado, a implantação de um Data Center definido por software é o próximo passo óbvio para usar o serviço VMware Cloud on AWS. Para criar um SDDC, escolha uma região da AWS para hospedá-lo, dê um nome ao SDDC e especifique quantos hosts ESXi você deseja que o SDDC contenha. Se você ainda não tiver uma conta na AWS, ainda poderá criar um SDDC de configuração inicial que contenha um único host ESXi.

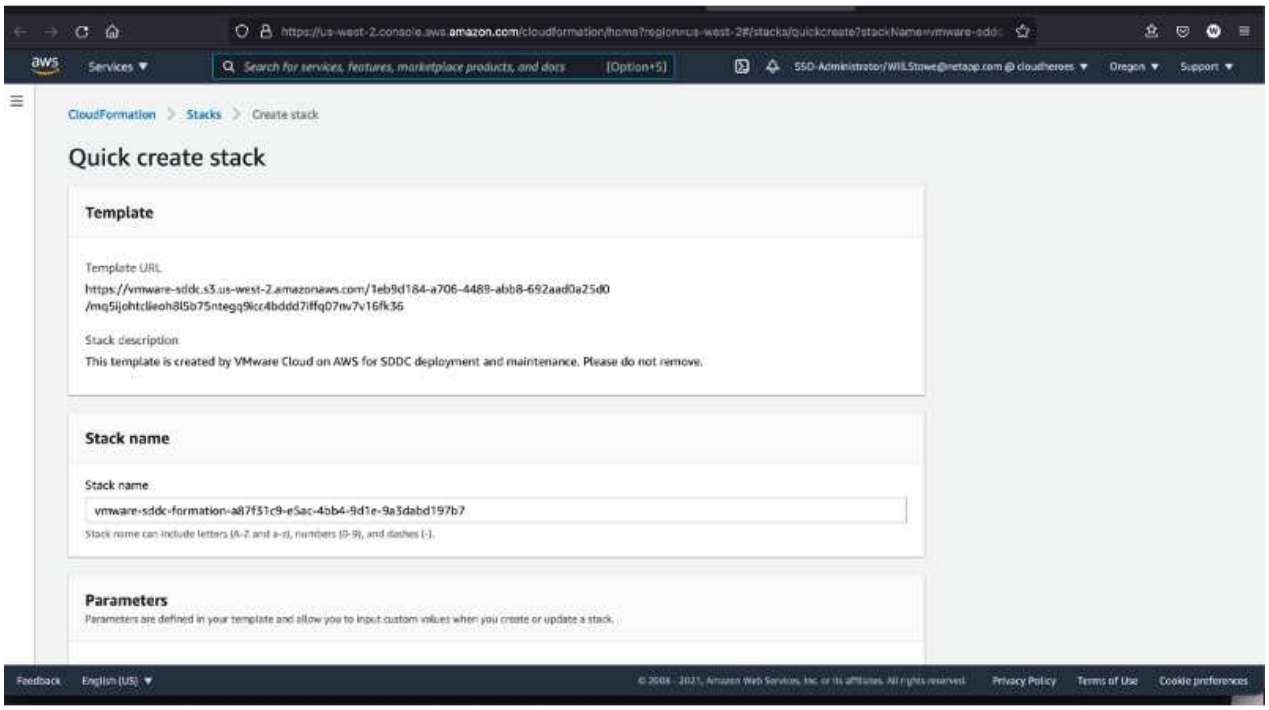
1. Efetue login no VMware Cloud Console usando suas credenciais VMware existentes ou recém-criadas.

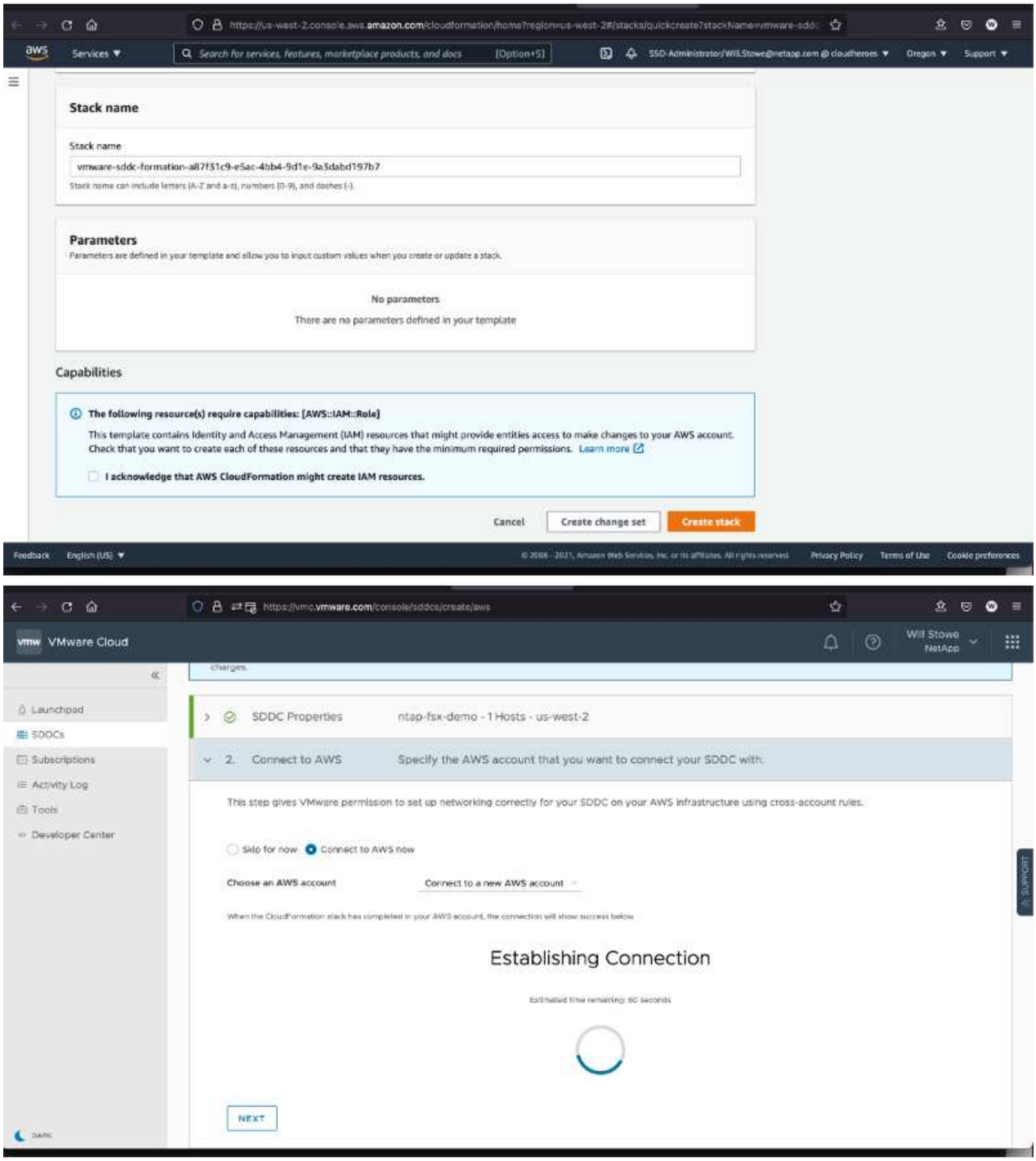


2. Configure a região da AWS, a implantação, o tipo de host e o nome do SDDC:

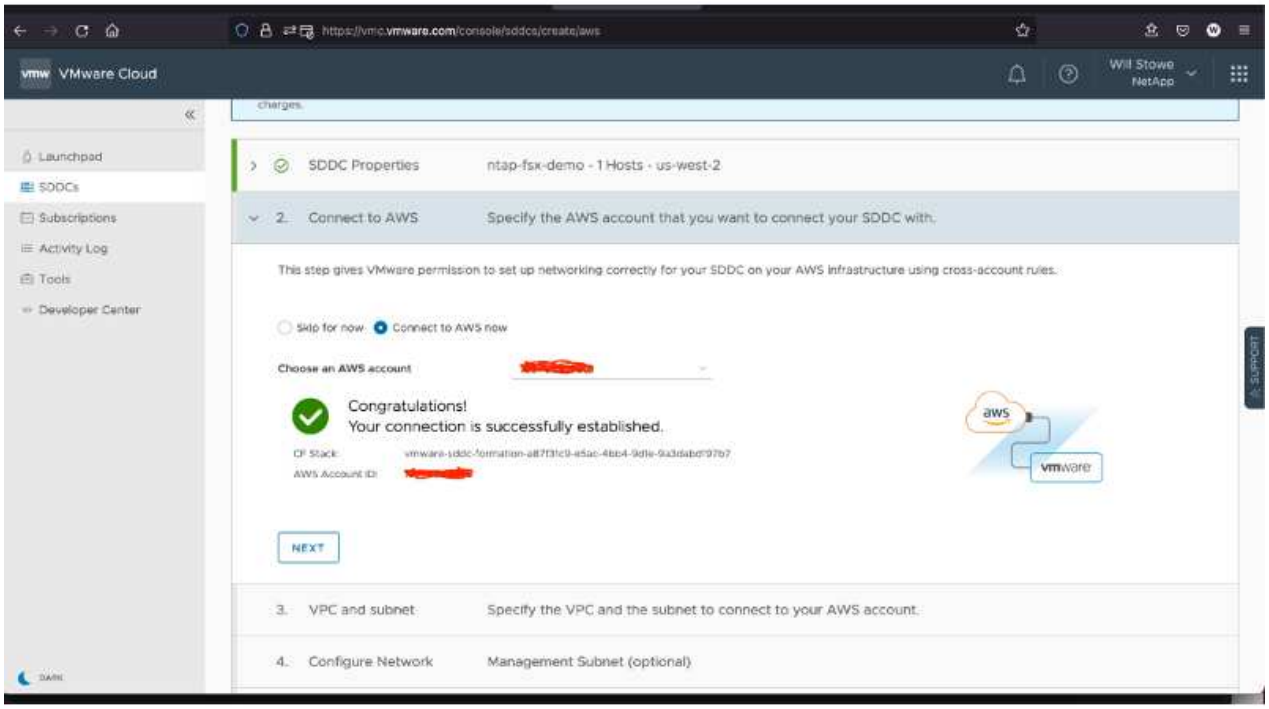


3. Conecte-se à conta AWS desejada e execute a pilha AWS Cloud Formation.



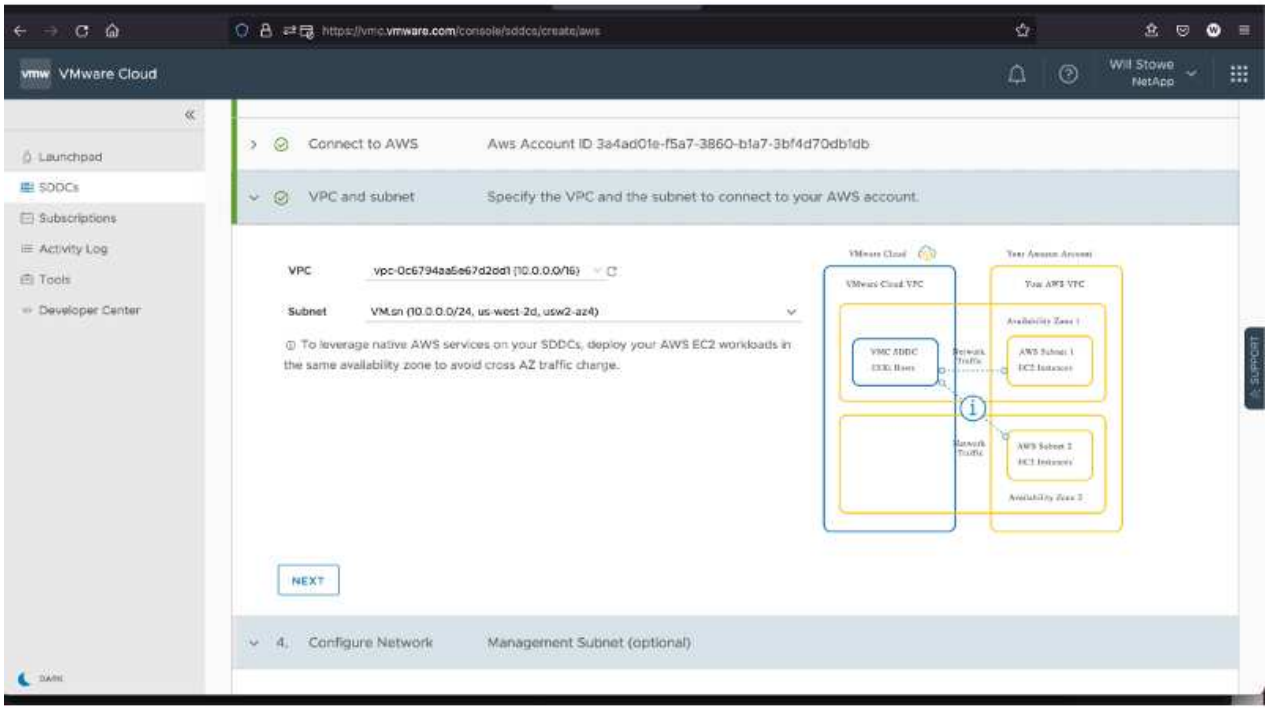

Stack name
Stack name
vmware-sddc-formation-a87f31c9-e5ac-4bb4-9d1e-9a3dabd197b7
Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.
No parameters
There are no parameters defined in your template
Capabilities
The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more
I acknowledge that AWS CloudFormation might create IAM resources.
Cancel
Create change set
Create stack
Feedback
English (US)
Privacy Policy
Terms of Use
Cookie preferences

VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
SDDC Properties
ntap-fsx-demo - 1 Hosts - us-west-2
2. Connect to AWS
Specify the AWS account that you want to connect your SDDC with.
This step gives VMware permission to set up networking correctly for your SDDC on your AWS infrastructure using cross-account rules.
Skip for now
Connect to AWS now
Choose an AWS account
Connect to a new AWS account
Establishing Connection
NEXT

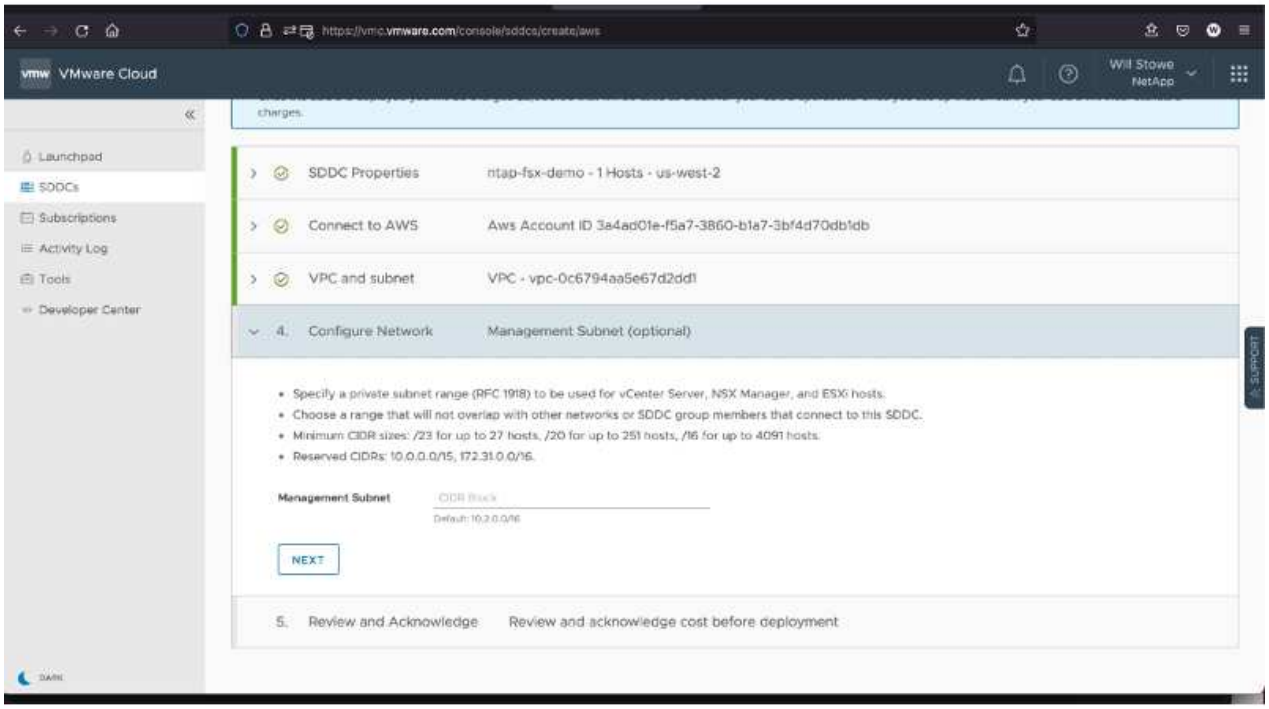


A configuração de host único é usada nesta validação.

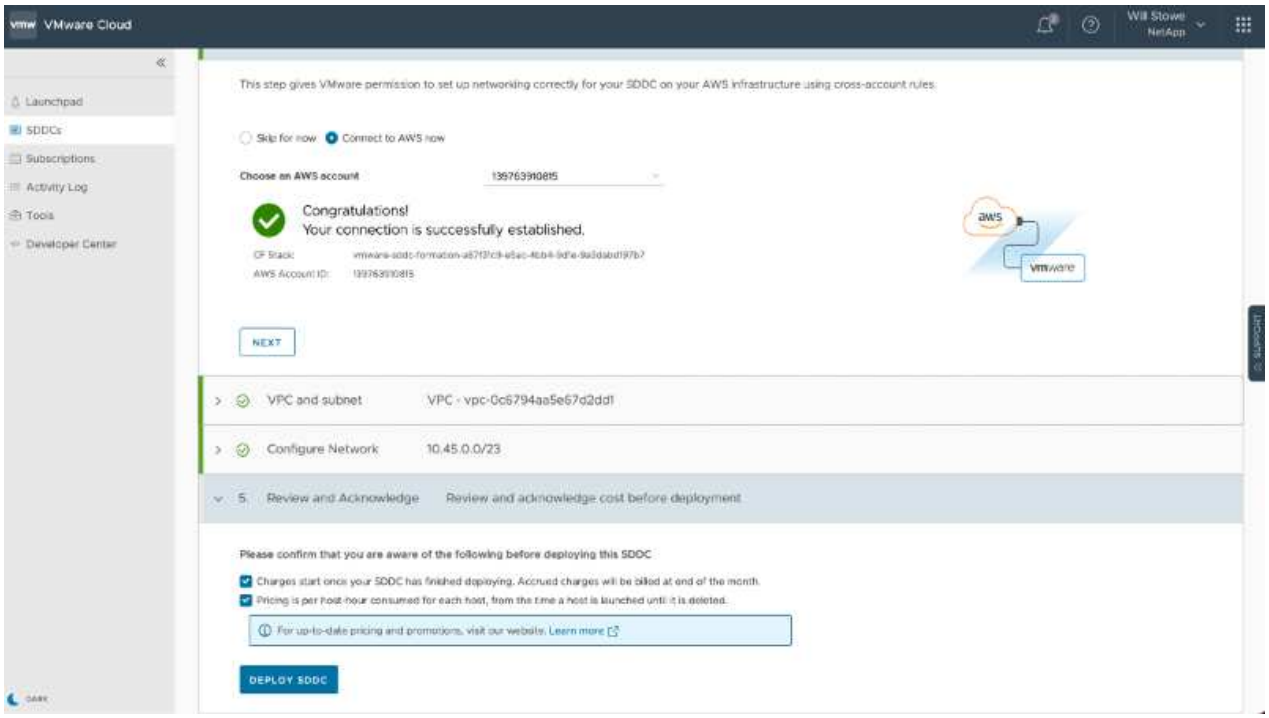
4. Selecione a AWS VPC desejada para conectar o ambiente VMC.



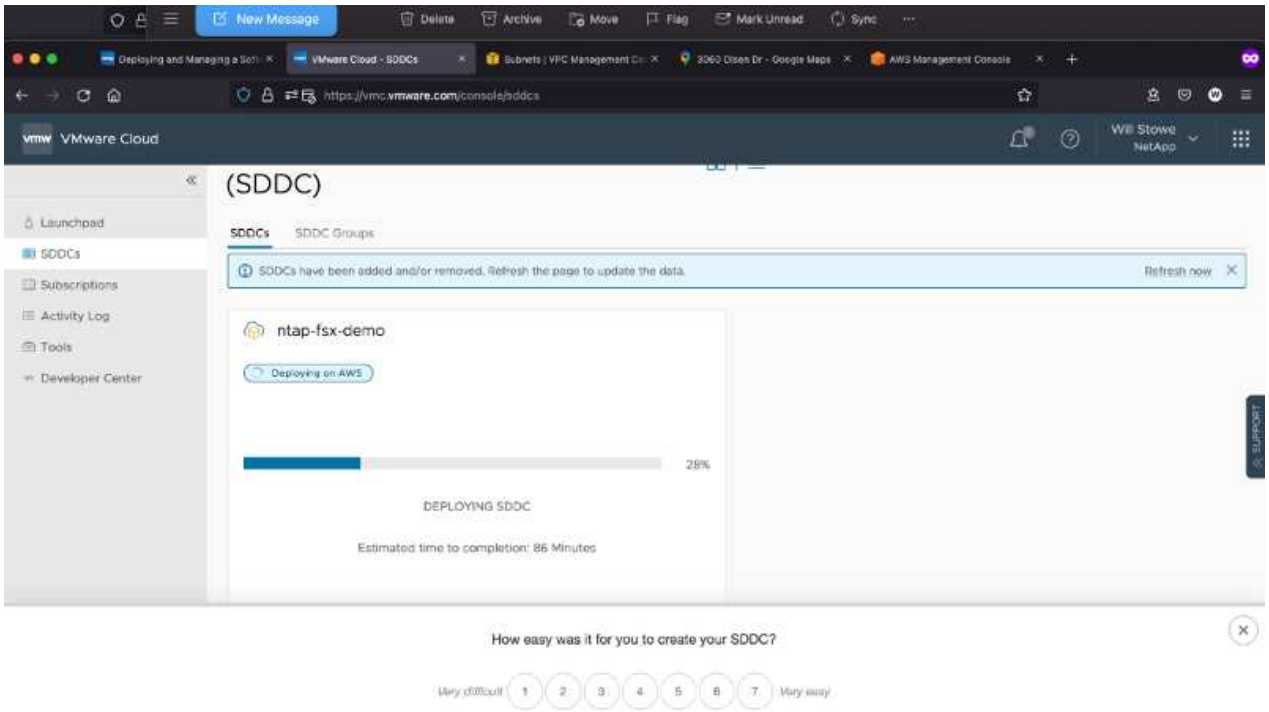
5. Configure a sub-rede de gerenciamento do VMC; esta sub-rede contém serviços gerenciados pelo VMC, como vCenter, NSX e assim por diante. Não escolha um espaço de endereço sobreposto com nenhuma outra rede que precise de conectividade com o ambiente SDDC. Por fim, siga as recomendações para o tamanho do CIDR indicadas abaixo.



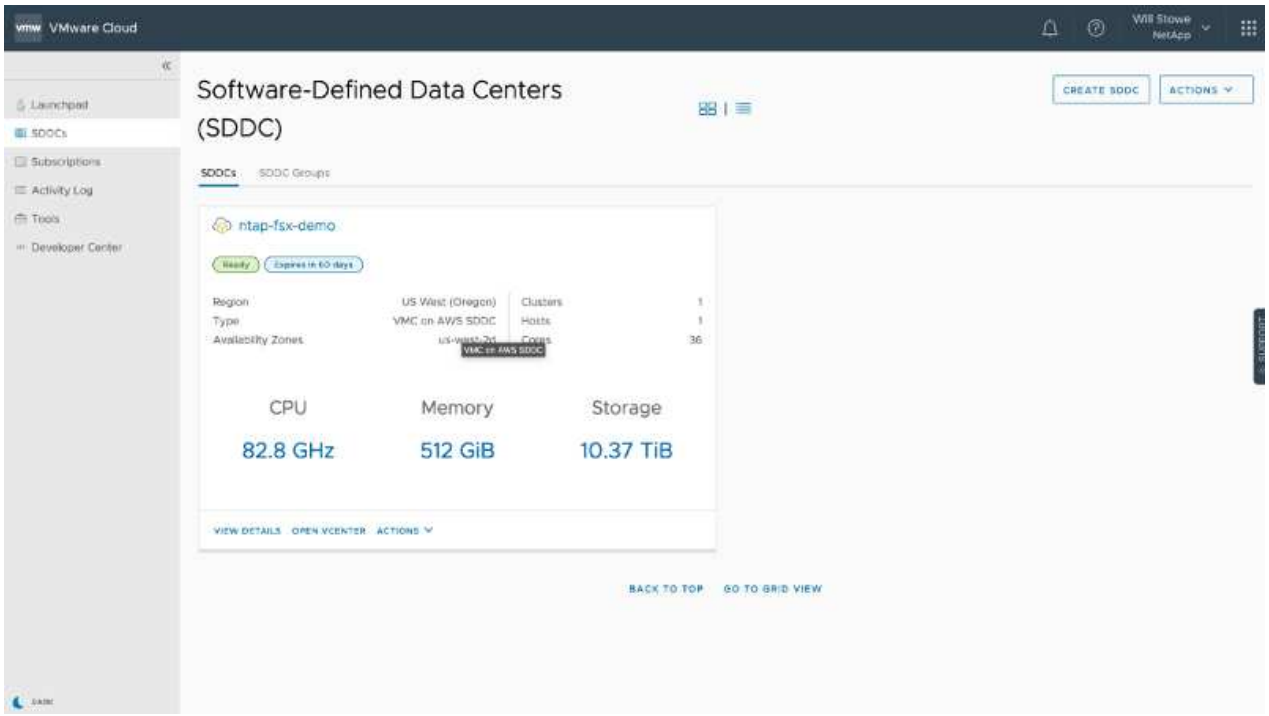
6. Revise e confirme a configuração do SDDC e clique em implantar o SDDC.



O processo de implantação normalmente leva aproximadamente duas horas para ser concluído.



7. Após a conclusão, o SDDC está pronto para uso.



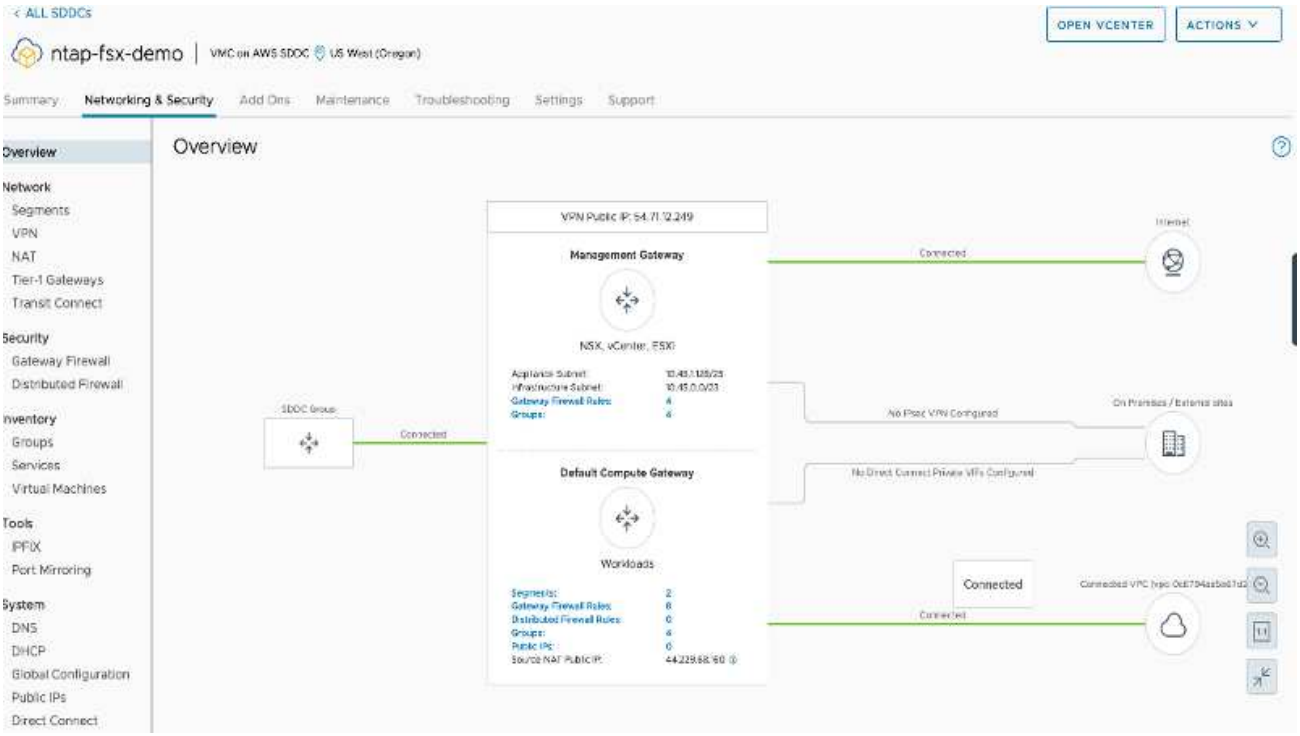
Para obter um guia passo a passo sobre a implantação do SDDC, consulte"Implantar um SDDC a partir do console do VMC" .

▼ Conecte o VMware Cloud ao FSx ONTAP

Para conectar o VMware Cloud ao FSx ONTAP, conclua as seguintes etapas:

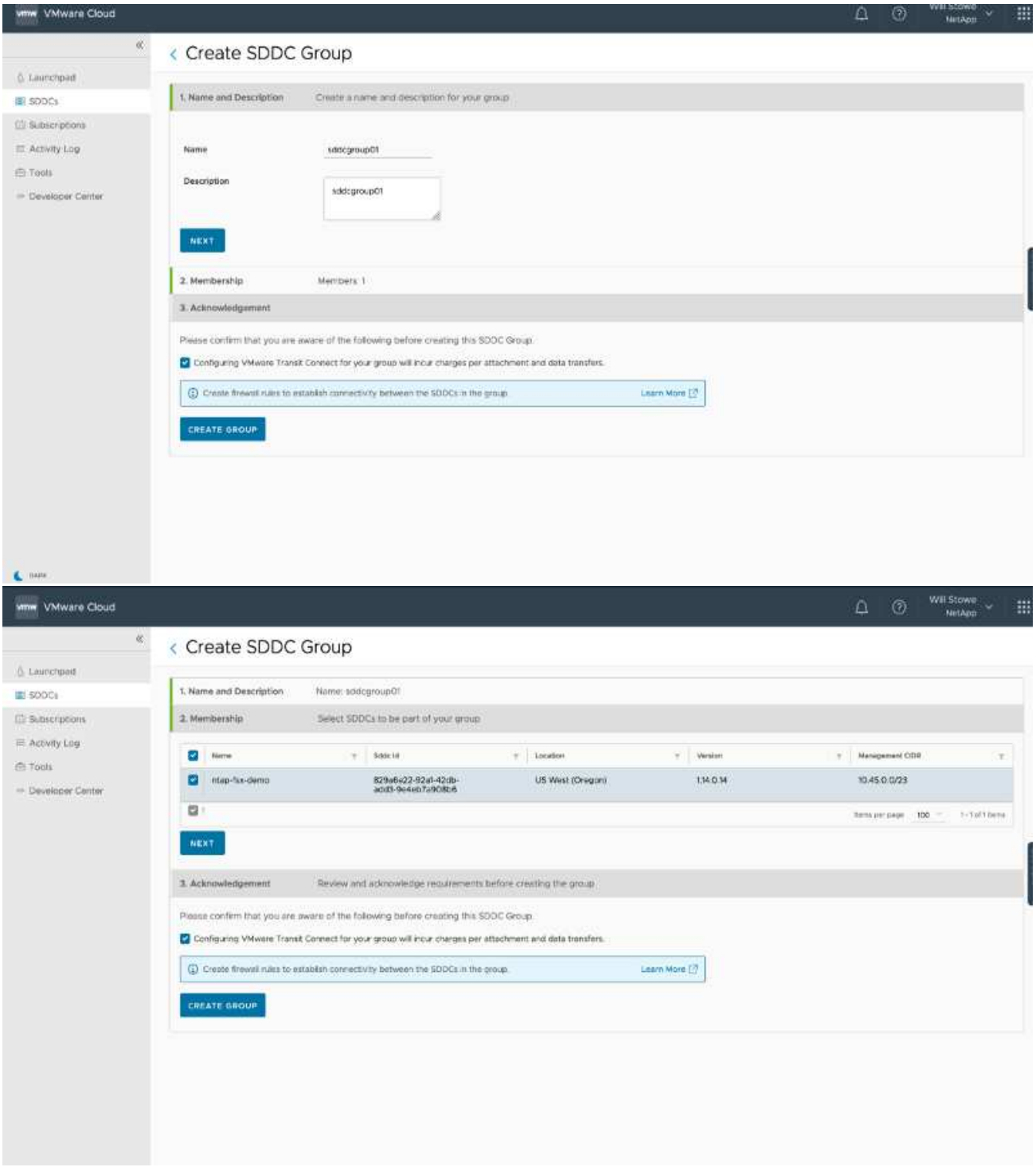
1. Com a implantação do VMware Cloud concluída e conectada ao AWS VPC, você deve implantar o Amazon FSx ONTAP em um novo VPC em vez do VPC conectado original (veja a captura de tela abaixo). O FSx (IPs flutuantes NFS e SMB) não estará acessível se for implantado na VPC conectada.

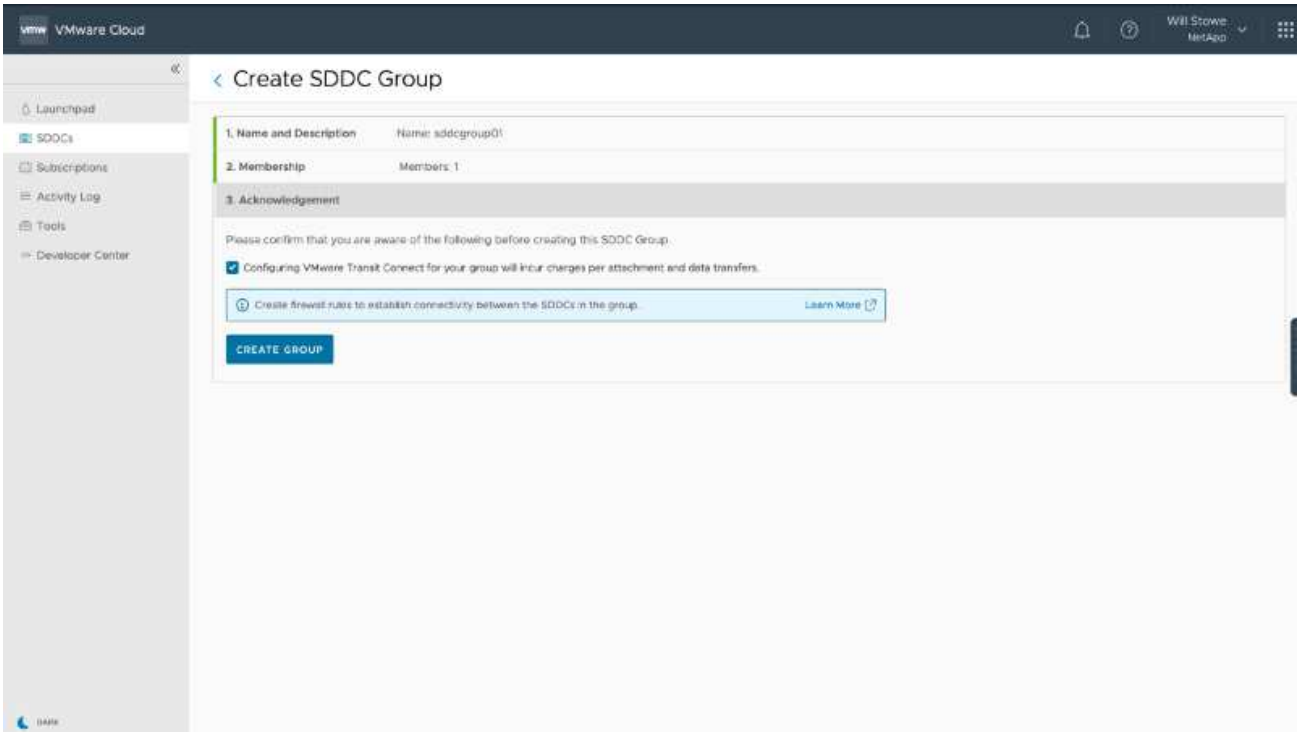
Tenha em mente que endpoints ISCSI como Cloud Volumes ONTAP funcionam perfeitamente na VPC conectada.



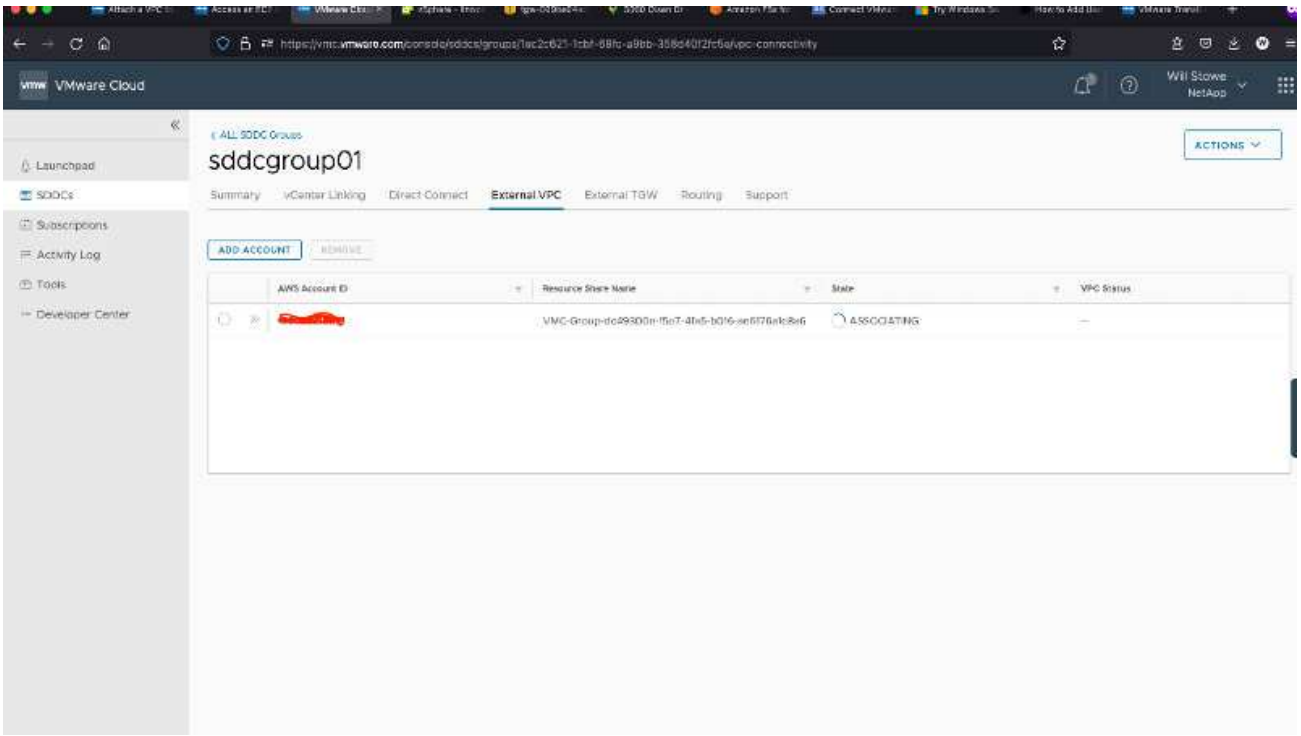
2. Implante uma VPC adicional na mesma região e, em seguida, implante o Amazon FSx ONTAP na nova VPC.

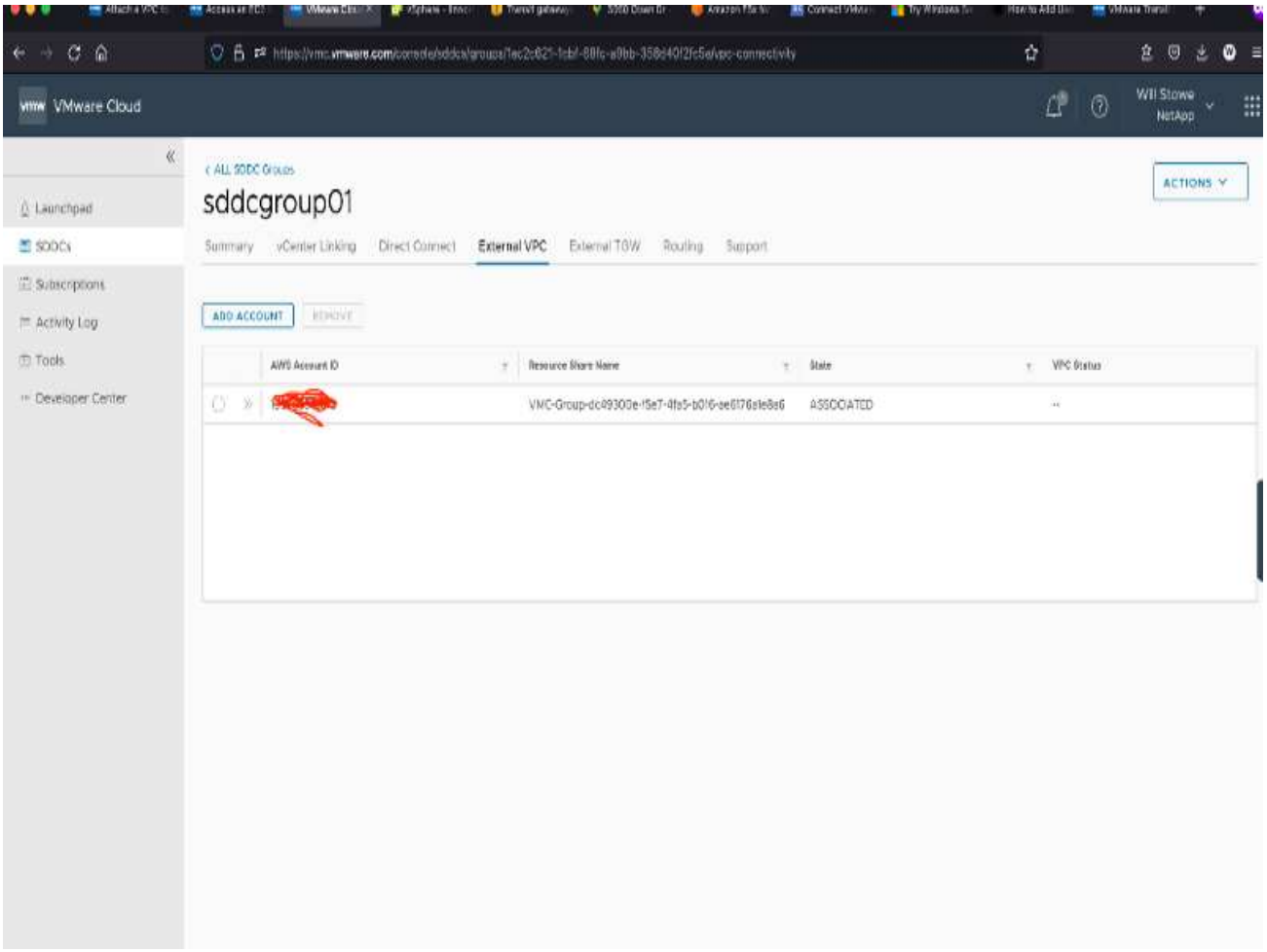
   A configuração de um grupo SDDC no console do VMware Cloud habilita as opções de configuração de rede necessárias para conectar-se à nova VPC onde o FSx está implantado. Na etapa 3, verifique se a opção "Configurar o VMware Transit Connect para seu grupo incorrerá em cobranças por anexo e transferências de dados" está marcada e escolha Criar grupo. O processo pode levar alguns minutos para ser concluído.


VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Create a name and description for your group
Name
sddcgroup01
Description
sddcgroup01
NEXT
2. Membership
Members: 1
3. Acknowledgement
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP
VMware Cloud
Will Stowe
NetApp
Launchpad
SDDCs
Subscriptions
Activity Log
Tools
Developer Center
Create SDDC Group
1. Name and Description
Name: sddcgroup01
2. Membership
Select SDDCs to be part of your group
Name
Sddc Id
Location
Version
Management CIDR
ntap-fsx-demo
829e6e22-92a1-42db-acd3-9e4eb7a90fb6
US West (Oregon)
1.14.0.14
10.45.0.0/23
Items per page: 100
1 - 1 of 1 items
NEXT
3. Acknowledgement
Review and acknowledge requirements before creating the group
Please confirm that you are aware of the following before creating this SDDC Group.
Configuring VMware Transit Connect for your group will incur charges per attachment and data transfers.
Create firewall rules to establish connectivity between the SDDCs in the group.
Learn More
CREATE GROUP

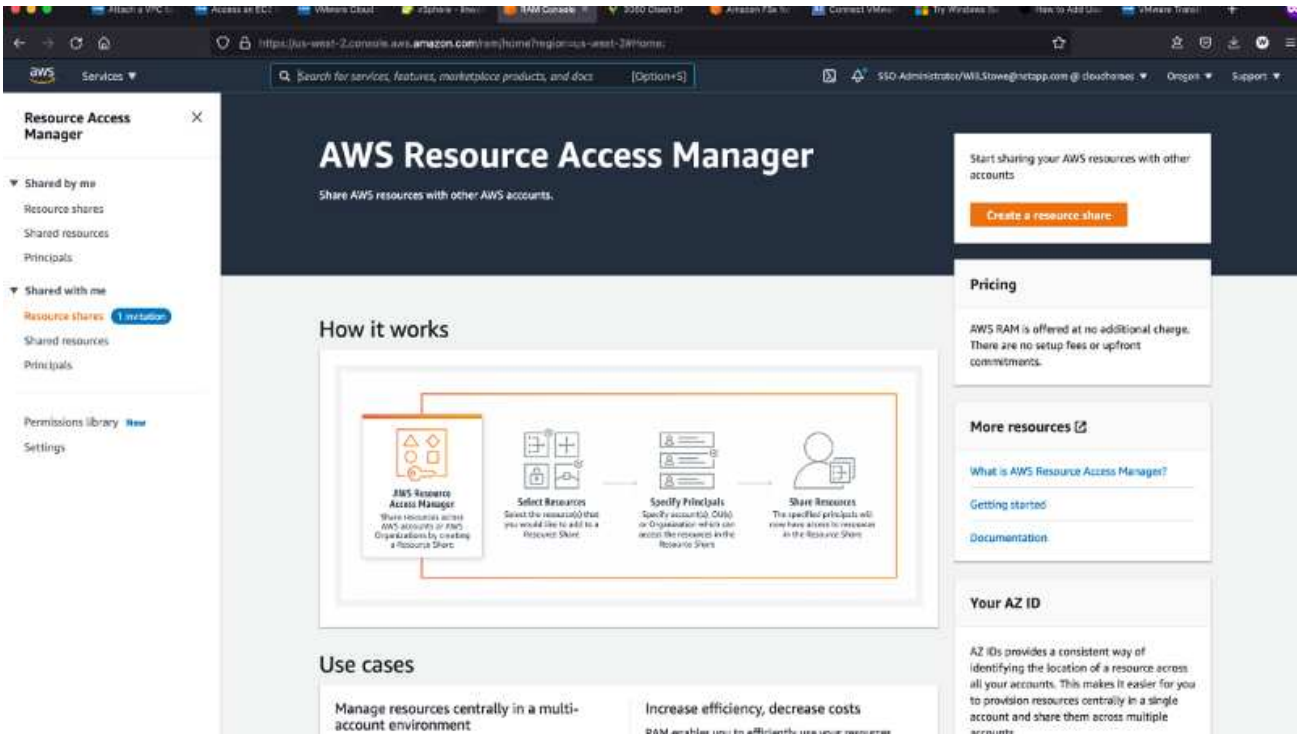


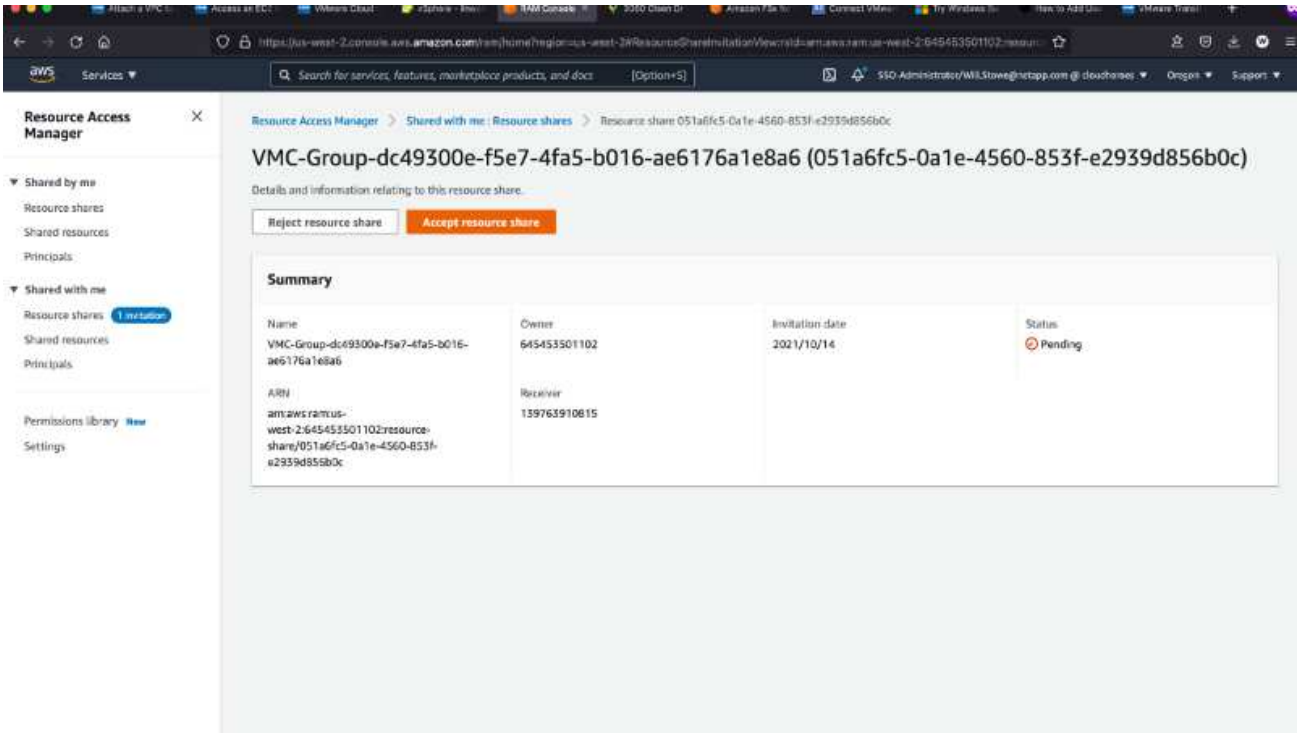
3. Anexe a VPC recém-criada ao grupo SDDC recém-criado. Selecione a aba VPC Externa e siga as instruções"instruções para anexar uma VPC externa" para o grupo. Esse processo pode levar de 10 a 15 minutos para ser concluído.



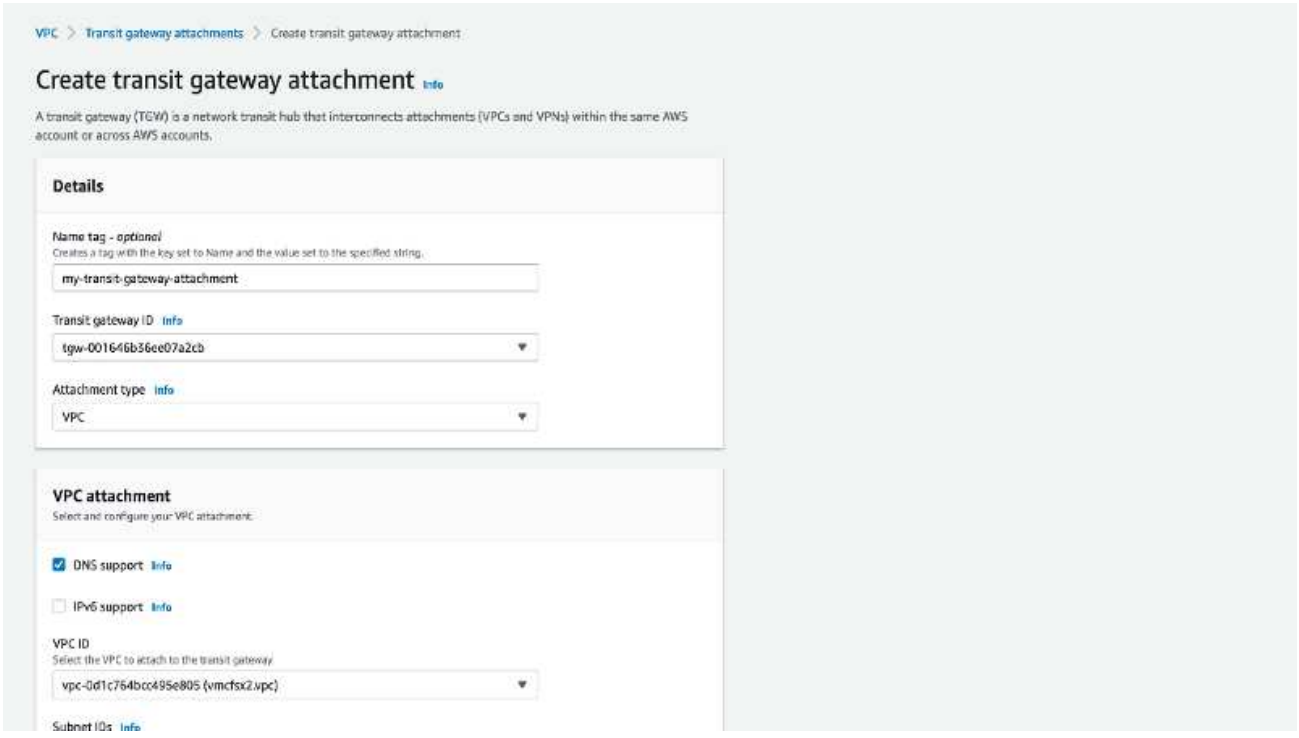


4. Como parte do processo de VPC externa, você é solicitado pelo console da AWS a acessar um novo recurso compartilhado por meio do Resource Access Manager. O recurso compartilhado é o"Gateway de trânsito da AWS" gerenciado pelo VMware Transit Connect.

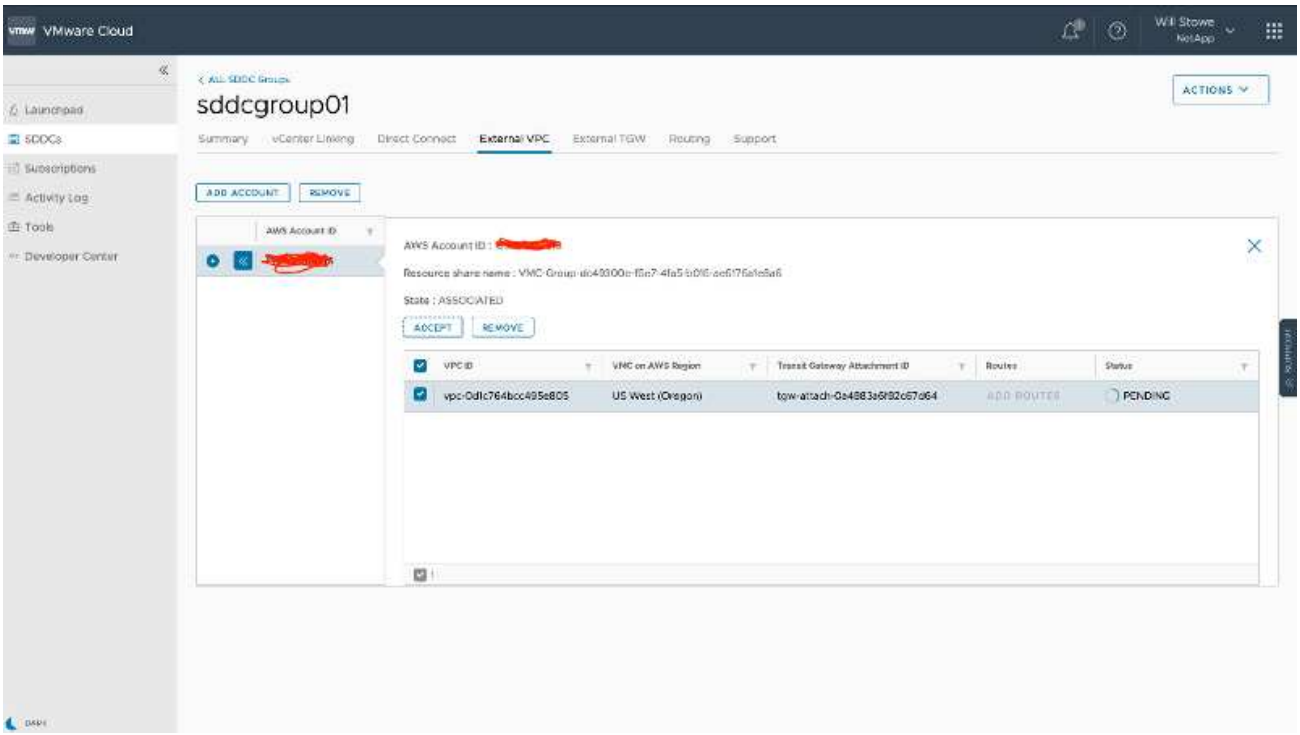




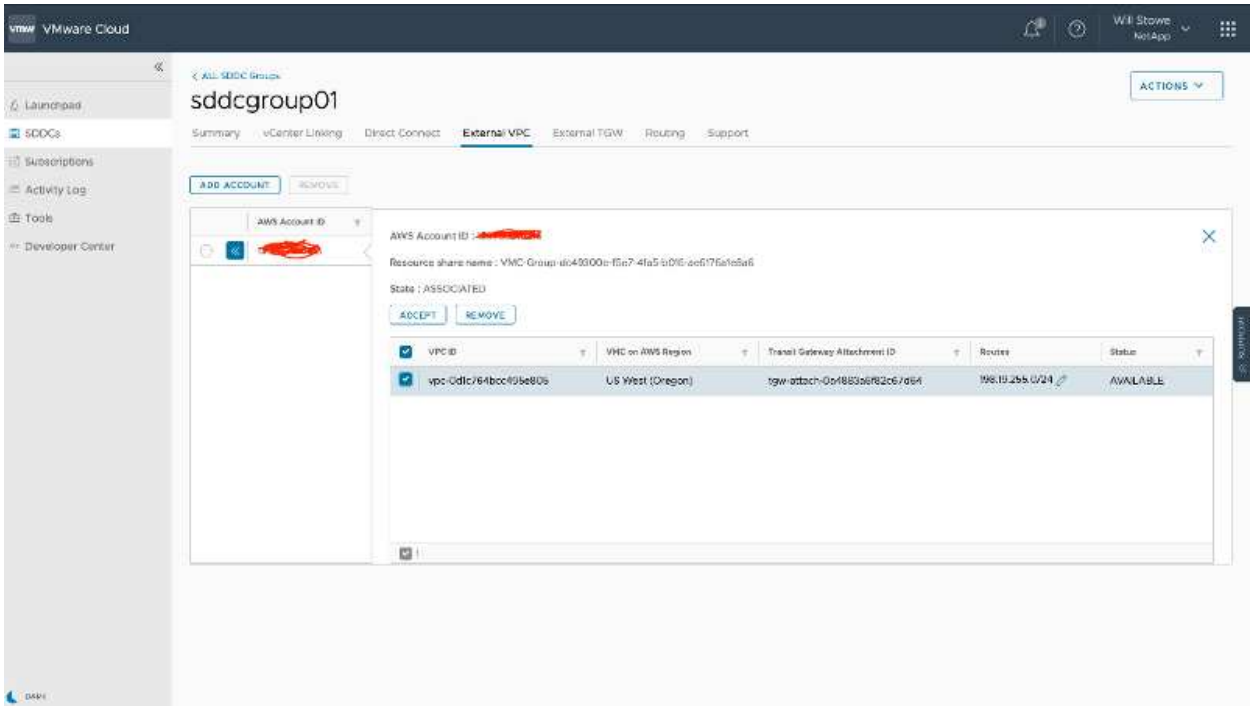
5. Crie o anexo do Transit Gateway.



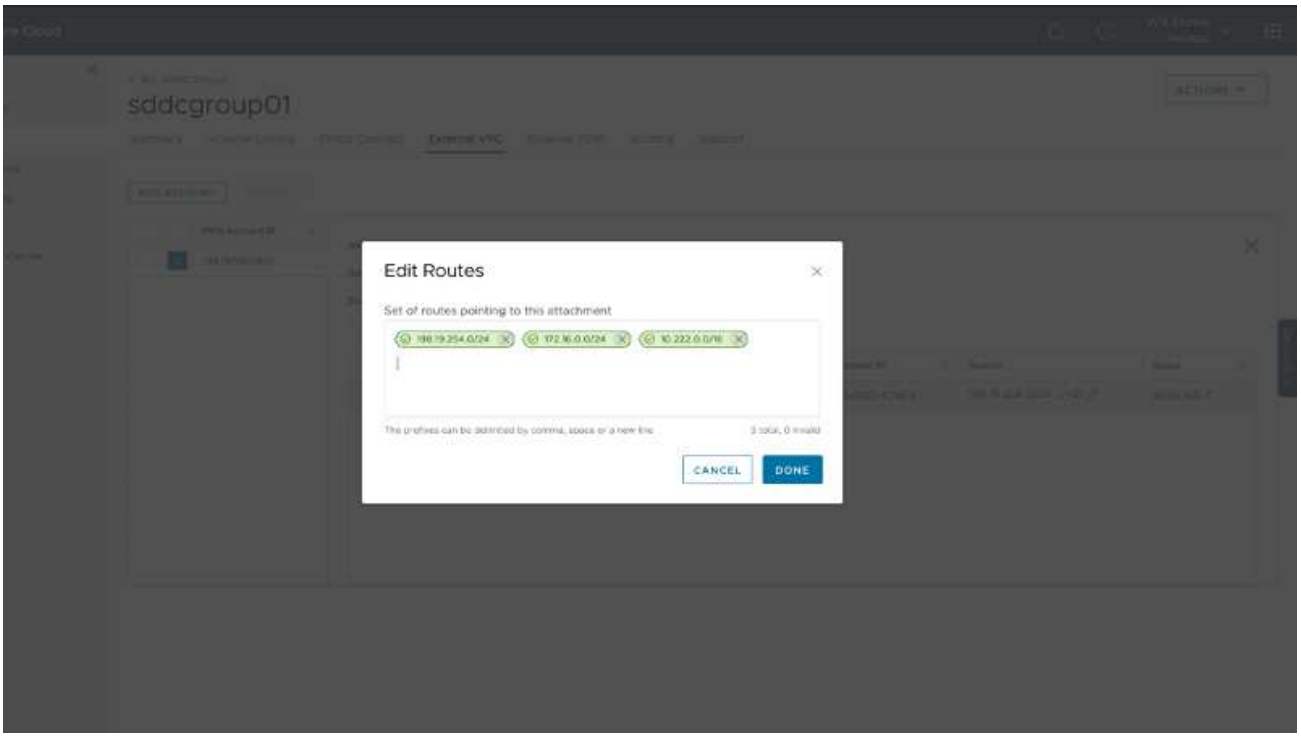
6. De volta ao console do VMC, aceite o anexo do VPC. Esse processo pode levar aproximadamente 10 minutos para ser concluído.



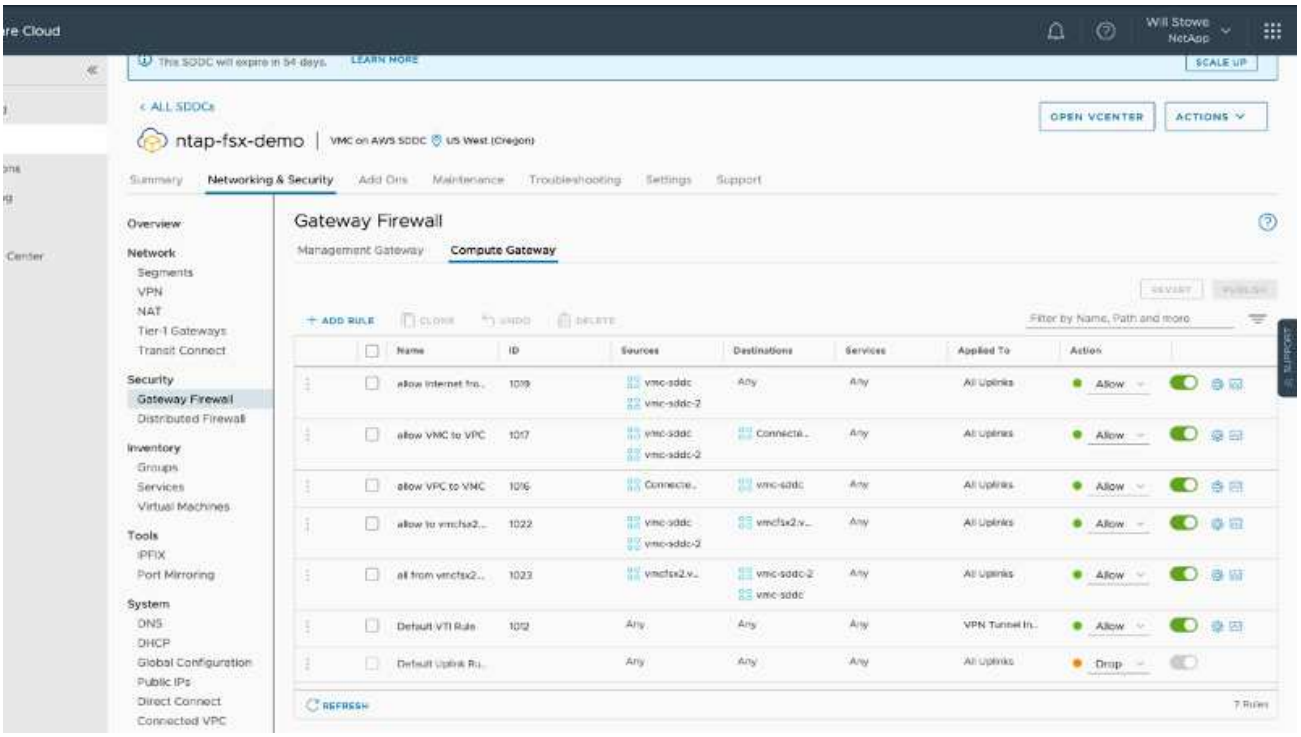
7. Na guia VPC externa, clique no ícone de edição na coluna Rotas e adicione as seguintes rotas necessárias:
   - Uma rota para o intervalo de IP flutuante para Amazon FSx ONTAP"IPs flutuantes" .
   - Uma rota para o intervalo de IP flutuante para o Cloud Volumes ONTAP (se aplicável).
   - Uma rota para o espaço de endereço VPC externo recém-criado.



8. Por fim, permita o tráfego bidirecional"regras de firewall" para acesso ao FSx/CVO. Siga estes"etapas detalhadas" para regras de firewall de gateway de computação para conectividade de carga de trabalho do SDDC.



9. Depois que os grupos de firewall forem configurados para o gateway de gerenciamento e de computação, o vCenter poderá ser acessado da seguinte maneira:



A próxima etapa é verificar se o Amazon FSx ONTAP ou o Cloud Volumes ONTAP está configurado dependendo dos seus requisitos e se os volumes estão provisionados para descarregar componentes de armazenamento do vSAN para otimizar a implantação.

Implantar e configurar o ambiente de virtualização no Azure

Assim como no local, o planejamento da Solução VMware no Azure é essencial para um ambiente de produção bem-sucedido, pronto para criação de VMs e migração.

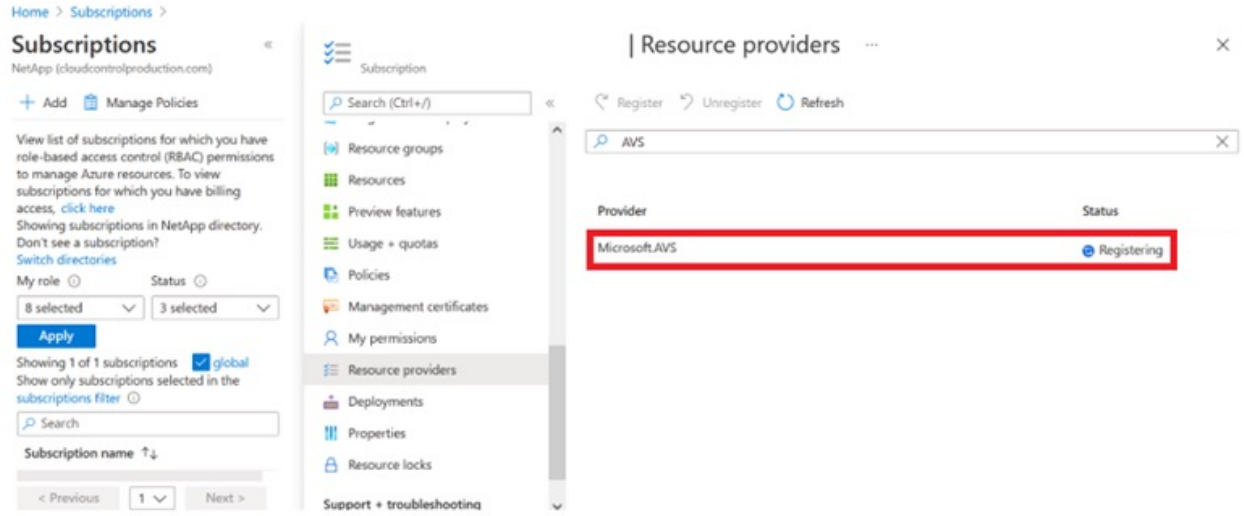
Esta seção descreve como configurar e gerenciar o Azure VMware Solution e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

O processo de configuração pode ser dividido nas seguintes etapas:

▼ **Registre o provedor de recursos e crie uma nuvem privada**

Para usar o Azure VMware Solution, primeiro registre o provedor de recursos na assinatura identificada:

1. Sign in no portal do Azure.
2. No menu do portal do Azure, selecione Todos os serviços.
3. Na caixa de diálogo Todos os serviços, insira a assinatura e selecione Assinaturas.
4. Para visualizar, selecione a assinatura na lista de assinaturas.
5. Selecione Provedores de Recursos e digite Microsoft.AVS na pesquisa.
6. Se o provedor de recursos não estiver registrado, selecione Registrar.

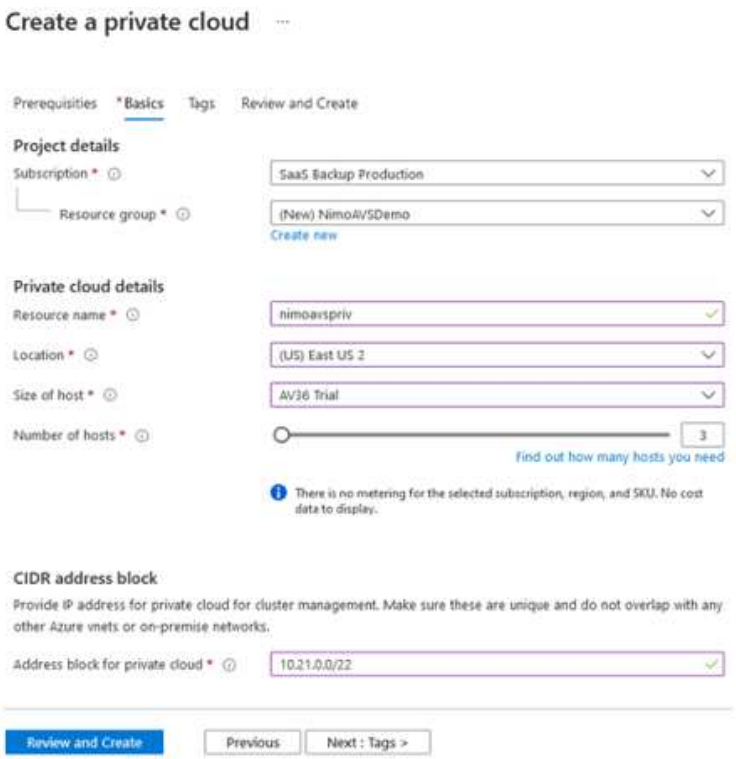




7. Depois que o provedor de recursos for registrado, crie uma nuvem privada do Azure VMware Solution usando o portal do Azure.
8. Sign in no portal do Azure.
9. Selecione Criar um novo recurso.
10. Na caixa de texto Pesquisar no Marketplace, insira Azure VMware Solution e selecione-o nos resultados.
11. Na página Solução VMware do Azure, selecione Criar.
12. Na guia Básico, insira os valores nos campos e selecione Revisar + Criar.

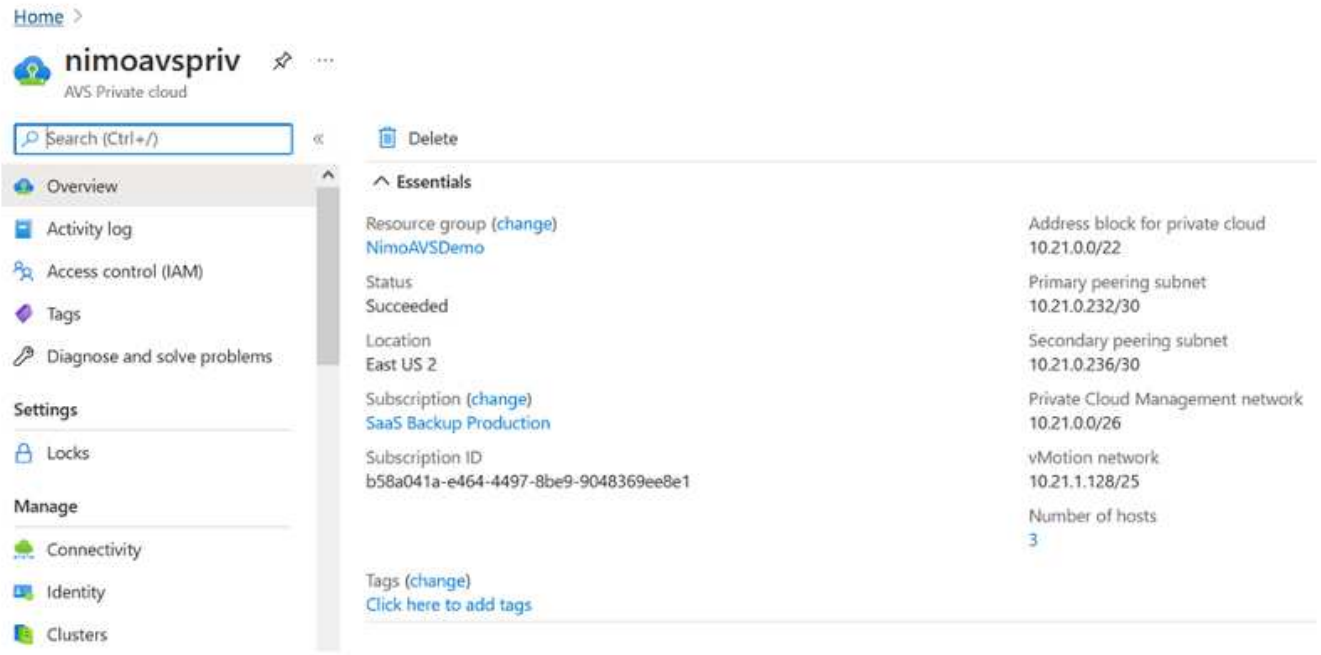
Observações:

- Para um início rápido, reúna as informações necessárias durante a fase de planejamento.
- Selecione um grupo de recursos existente ou crie um novo grupo de recursos para a nuvem privada. Um grupo de recursos é um contêiner lógico no qual os recursos do Azure são implantados e gerenciados.
- Certifique-se de que o endereço CIDR seja exclusivo e não se sobreponha a outras Redes Virtuais do Azure ou redes locais. O CIDR representa a rede de gerenciamento de nuvem privada e é usado para serviços de gerenciamento de cluster, como o vCenter Server e o NSX-T Manager. A NetApp recomenda usar um espaço de endereço /22. Neste exemplo, 10.21.0.0/22 é usado.



O processo de provisionamento leva aproximadamente de 4 a 5 horas. Após a conclusão do processo, verifique se a implantação foi bem-sucedida acessando a nuvem privada no portal do Azure. O status Bem-sucedido é exibido quando a implantação é concluída.

Uma nuvem privada do Azure VMware Solution requer uma Rede Virtual do Azure. Como o Azure VMware Solution não oferece suporte ao vCenter local, etapas adicionais são necessárias para integração com um ambiente local existente. Também é necessário configurar um circuito ExpressRoute e um gateway de rede virtual. Enquanto aguarda a conclusão do provisionamento do cluster, crie uma nova rede virtual ou use uma existente para se conectar ao Azure VMware Solution.



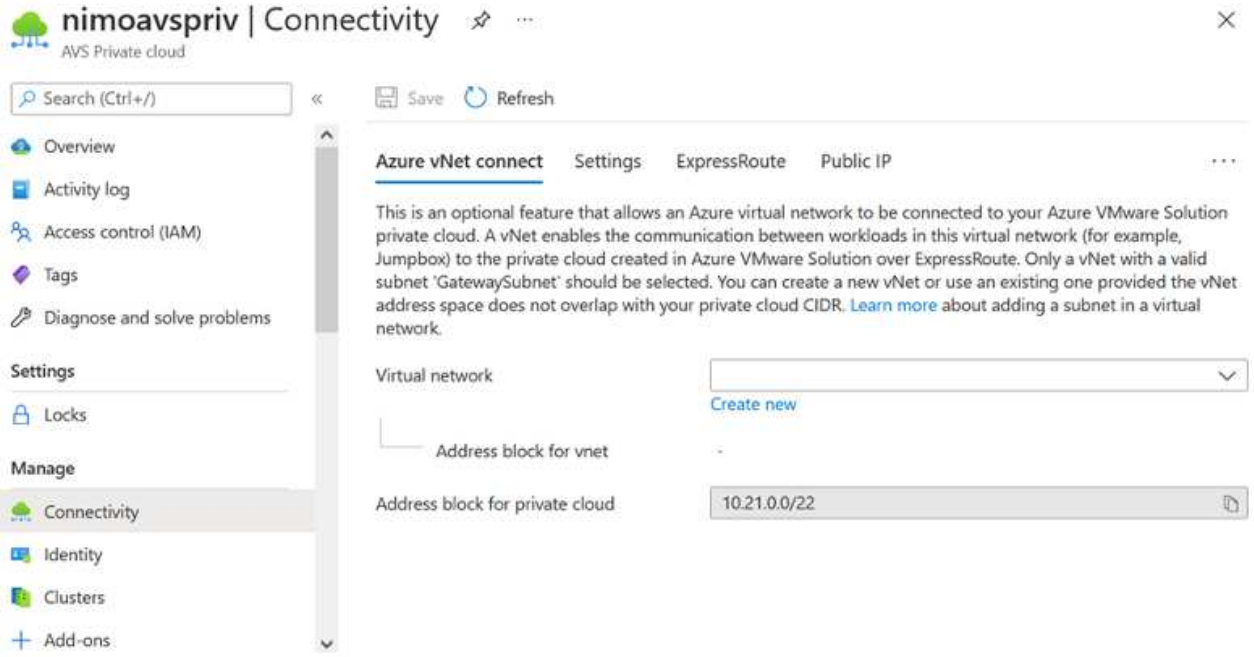
▼ **Conectar-se a um gateway de rede virtual ExpressRoute novo ou existente**

Para criar uma nova Rede Virtual do Azure (VNet), selecione a guia Conexão de VNet do Azure. Como alternativa, você pode criar uma manualmente no portal do Azure usando o assistente Criar Rede Virtual:

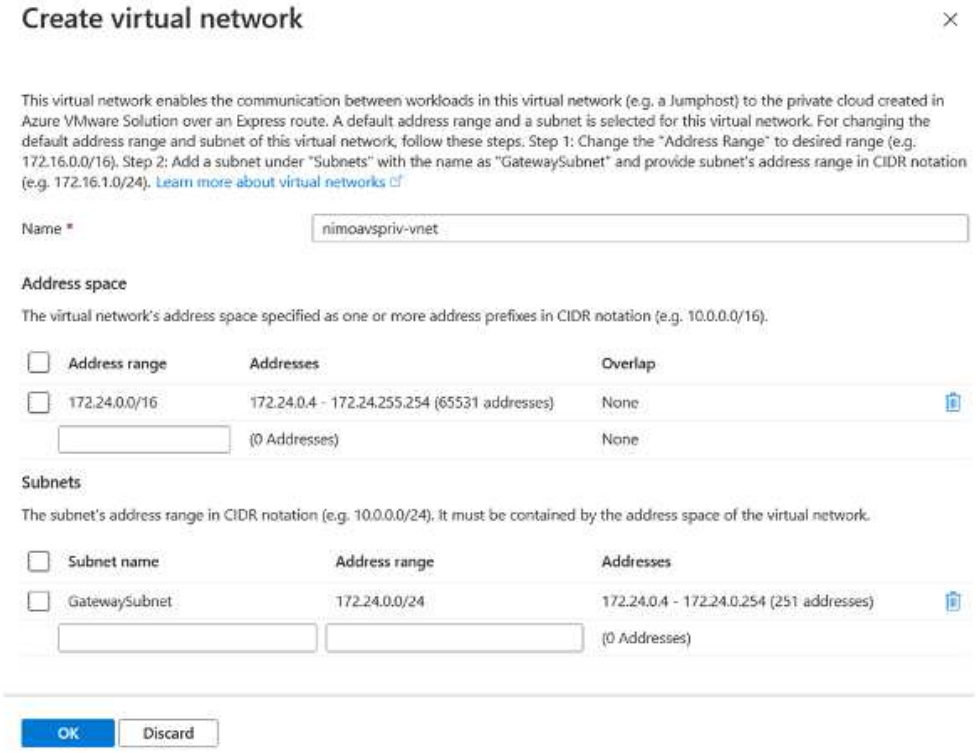
1. Acesse a nuvem privada do Azure VMware Solution e acesse Conectividade na opção Gerenciar.
2. Selecione Azure VNet Connect.
3. Para criar uma nova VNet, selecione a opção Criar nova.

   Este recurso permite que uma VNet seja conectada à nuvem privada do Azure VMware Solution. A VNet permite a comunicação entre cargas de trabalho nesta rede virtual criando automaticamente componentes necessários (por exemplo, jump box, serviços compartilhados como Azure NetApp Files e Cloud Volume ONTAP) para a nuvem privada criada no Azure VMware Solution via ExpressRoute.

   Observação: o espaço de endereço da VNet não deve se sobrepor ao CIDR da nuvem privada.



4. Forneça ou atualize as informações para a nova VNet e selecione OK.



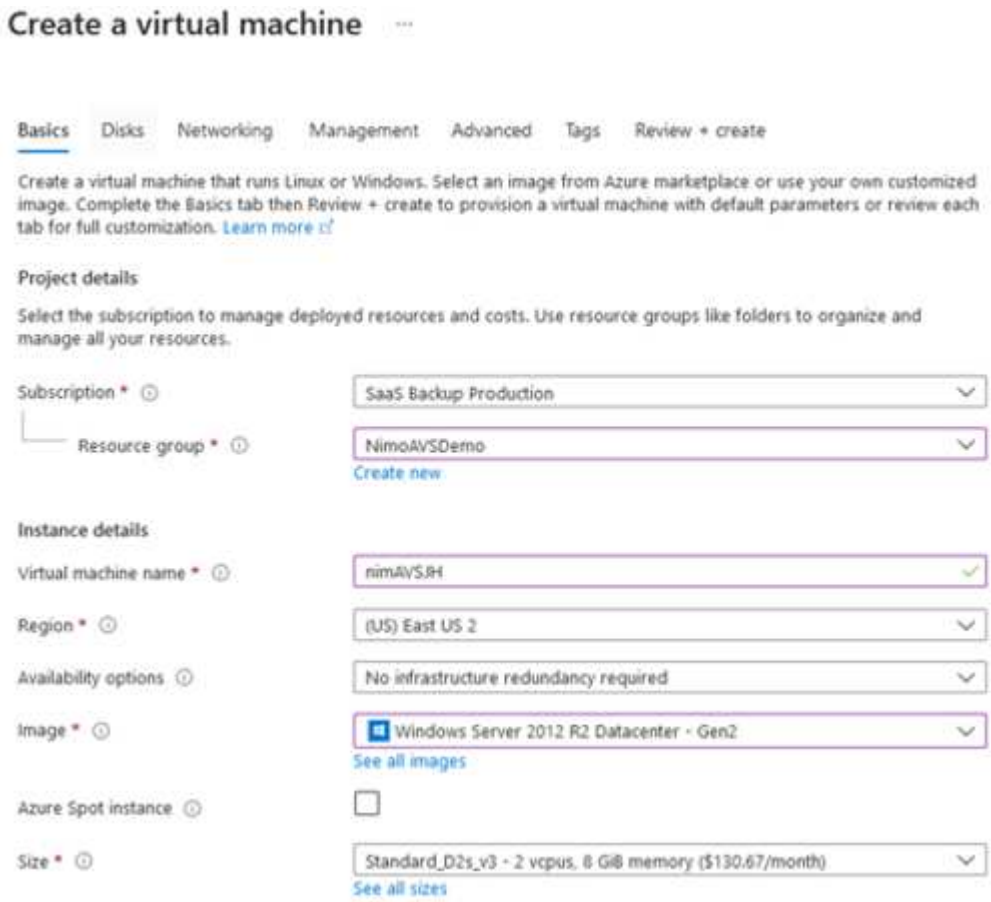
A VNet com o intervalo de endereços e a sub-rede de gateway fornecidos é criada na assinatura e no grupo de recursos designados.

Se você criar uma VNet manualmente, crie um gateway de rede virtual com o SKU apropriado e o ExpressRoute como o tipo de gateway. Após a conclusão da implantação, conecte a conexão do ExpressRoute ao gateway de rede virtual que contém a nuvem privada do Azure VMware Solution usando a chave de autorização. Para obter mais

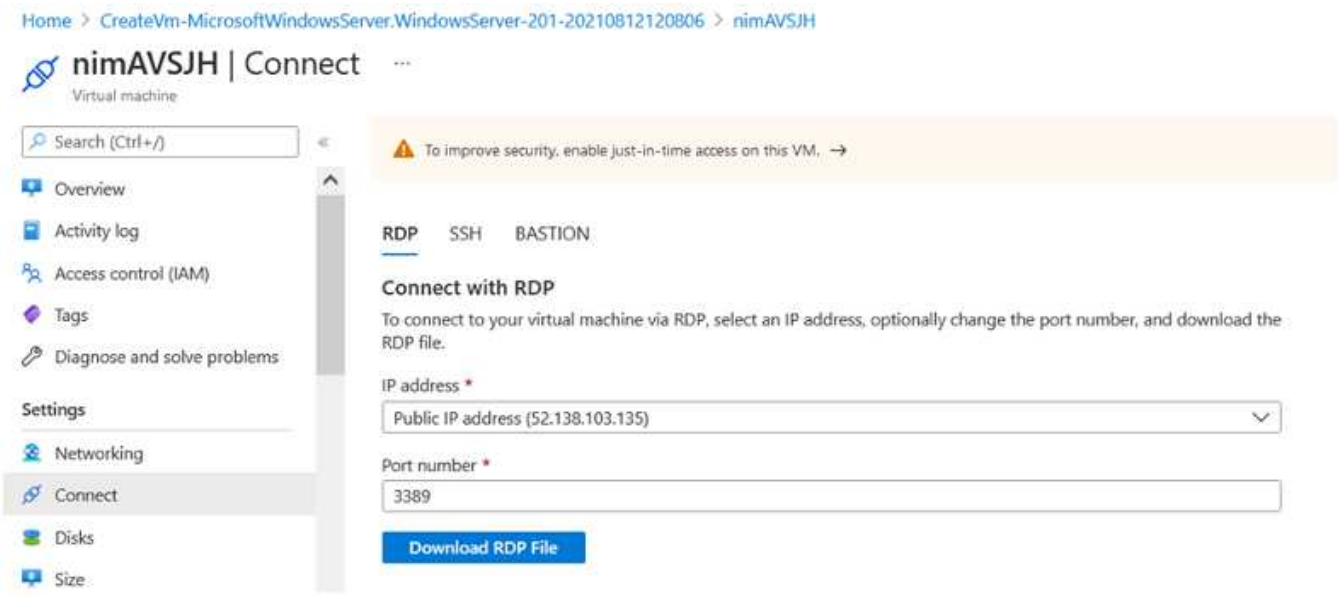
informações, consulte "Configurar a rede para sua nuvem privada VMware no Azure" .

▼ **Validar a conexão de rede e o acesso à nuvem privada do Azure VMware Solution**

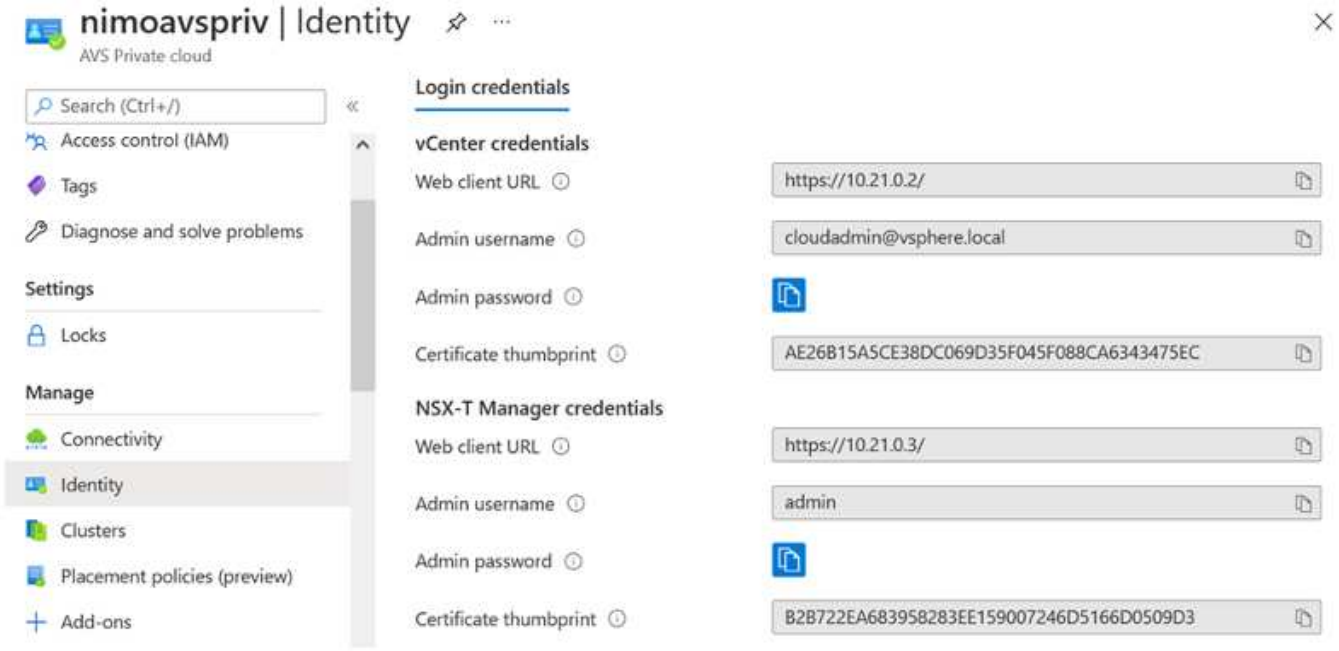
O Azure VMware Solution não permite que você gerencie uma nuvem privada com o VMware vCenter local. Em vez disso, o jump host é necessário para se conectar à instância do Azure VMware Solution vCenter. Crie um host de salto no grupo de recursos designado e entre no Azure VMware Solution vCenter. Este host de salto deve ser uma VM do Windows na mesma rede virtual que foi criada para conectividade e deve fornecer acesso ao vCenter e ao NSX Manager.



Após o provisionamento da máquina virtual, use a opção Conectar para acessar o RDP.



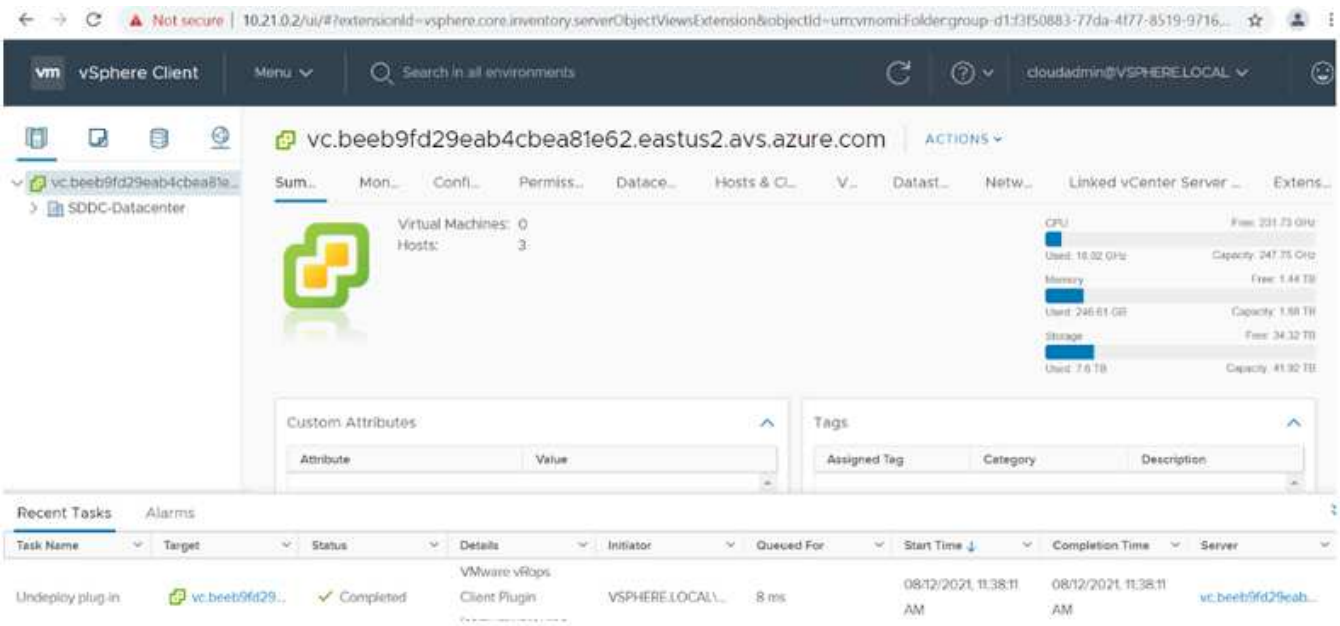
Sign in no vCenter a partir desta máquina virtual host de salto recém-criada usando o usuário administrador da nuvem. Para acessar as credenciais, acesse o portal do Azure e navegue até Identidade (na opção Gerenciar na nuvem privada). Os URLs e credenciais de usuário para a nuvem privada vCenter e o NSX-T Manager podem ser copiados aqui.



Na máquina virtual do Windows, abra um navegador e navegue até o URL do cliente web do vCenter(`"https://10.21.0.2/"`) e use o nome de usuário administrador como **cloudadmin@vsphere.local** e cole a senha copiada. Da mesma forma, o gerenciador NSX-T também pode ser acessado usando o URL do cliente web(`"https://10.21.0.3/"`) e use o nome de usuário administrador e cole a senha copiada para criar novos segmentos ou modificar os gateways de nível existentes.

Os URLs do cliente web são diferentes para cada SDDC provisionado.





O SDDC da Solução VMware do Azure agora está implantado e configurado. Aproveite o ExpressRoute Global Reach para conectar o ambiente local à nuvem privada do Azure VMware Solution. Para obter mais informações, consulte "Ambientes locais peer para a Solução VMware do Azure" .

Implantar e configurar o ambiente de virtualização no Google Cloud Platform (GCP)

Assim como no local, o planejamento do Google Cloud VMware Engine (GCVE) é essencial para um ambiente de produção bem-sucedido para criação de VMs e migração.

Esta seção descreve como configurar e gerenciar o GCVE e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

O processo de configuração pode ser dividido nas seguintes etapas:

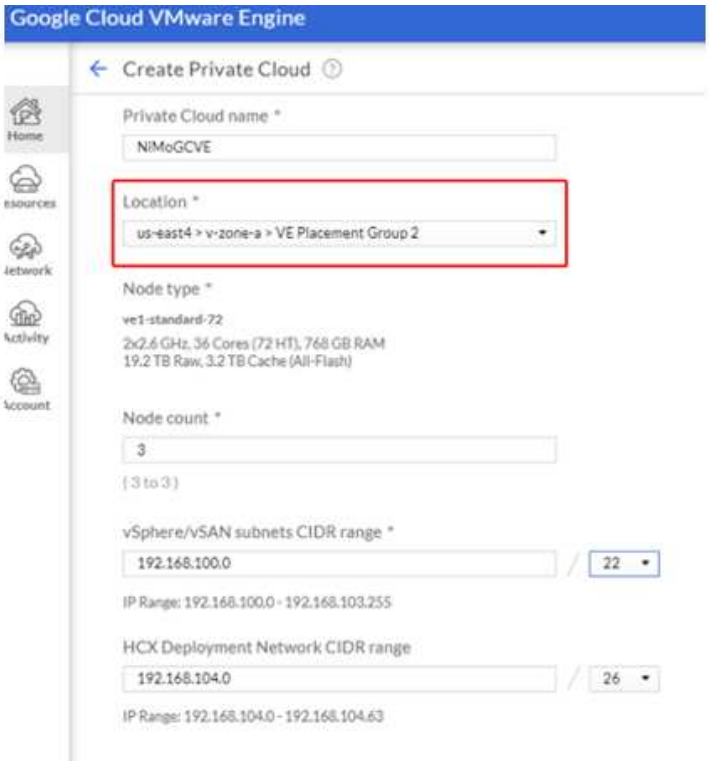
▼ Implantar e configurar o GCVE

Para configurar um ambiente GCVE no GCP, faça login no console do GCP e acesse o portal do VMware Engine.

Clique no botão "Nova Nuvem Privada" e insira a configuração desejada para a Nuvem Privada GCVE. Em "Localização", certifique-se de implantar a nuvem privada na mesma região/zona onde o NetApp Volumes/CVO está implantado, para garantir o melhor desempenho e a menor latência.

Pré-requisitos:

- Configurar a função IAM do administrador do serviço VMware Engine
- "Habilitar acesso à API do VMWare Engine e cota de nó"
- Certifique-se de que o intervalo CIDR não se sobreponha a nenhuma de suas sub-redes locais ou na nuvem. O intervalo CIDR deve ser /27 ou superior.



Observação: a criação de uma nuvem privada pode levar de 30 minutos a 2 horas.

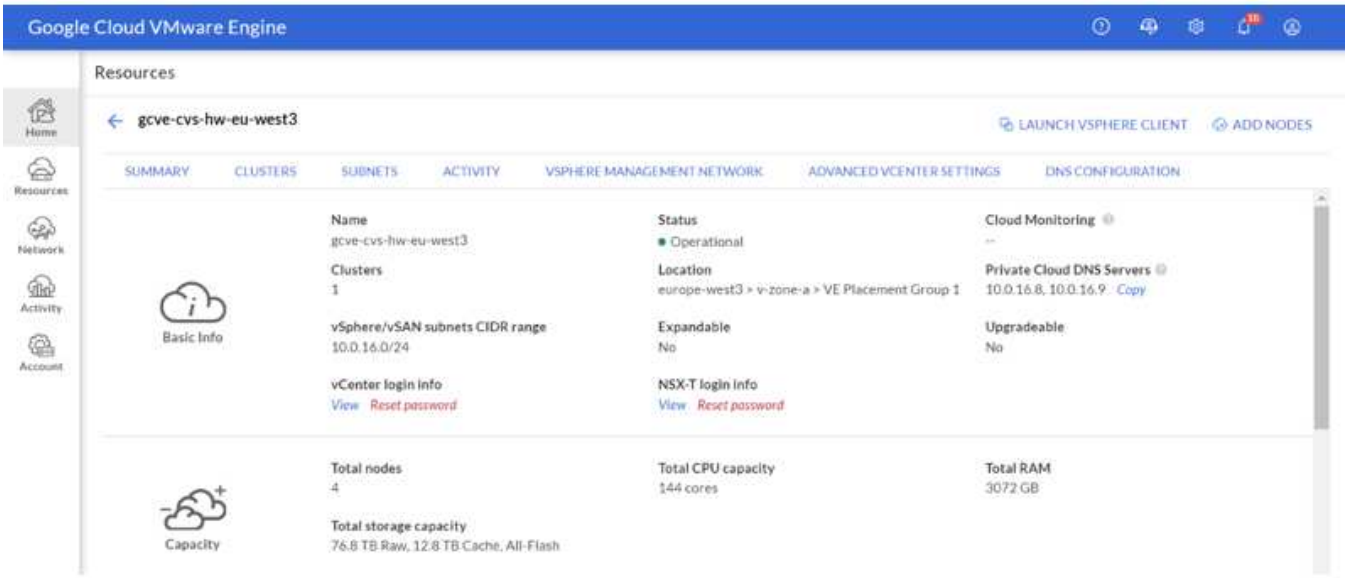
▼ Habilitar acesso privado ao GCVE

Depois que a Nuvem Privada for provisionada, configure o acesso privado à Nuvem Privada para conexão de caminho de dados de alta taxa de transferência e baixa latência.

Isso garantirá que a rede VPC em que as instâncias do Cloud Volumes ONTAP estão em execução consiga se comunicar com a Nuvem Privada do GCVE. Para isso, siga as instruções "Documentação do GCP". Para o Cloud Volume Service, estabeleça uma conexão entre o VMware Engine e o Google Cloud NetApp Volumes realizando um peering único entre os projetos de host do locatário. Para obter instruções detalhadas, siga este guia "link".

Tenant P	Service	Region	Routing Mode	Peered Project ID	Peered VPC	VPC Peering Sta...	Region Status
ke841388caa56b...	VPC Network	europe-west3	Global	cv-performance-te...	cloud-volumes-vpc	Active	Connected
jbd729510b3ebbf...	NetApp CVS	europe-west3	Global	y2b6c17202af6dc...	netapp-tenant-vpc	Active	Connected

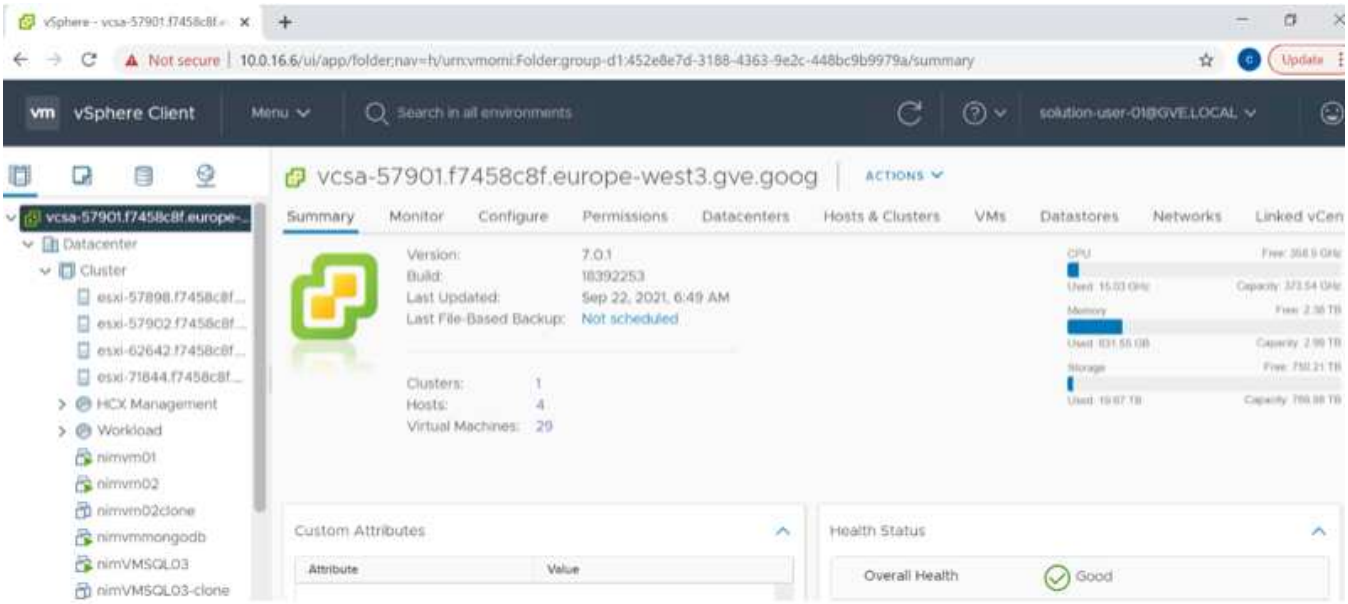
Sign in no vCenter usando o usuário CloudOwner@gve.local. Para acessar as credenciais, acesse o portal do VMware Engine, vá para Recursos e selecione a nuvem privada apropriada. Na seção Informações básicas, clique no link Exibir para obter informações de login do vCenter (vCenter Server, HCX Manager) ou informações de login do NSX-T (NSX Manager).



Em uma máquina virtual Windows, abra um navegador e navegue até o URL do cliente web vCenter(`"https://10.0.16.6/"`) e use o nome de usuário administrador como CloudOwner@gve.local e cole a senha copiada. Da mesma forma, o gerenciador NSX-T também pode ser acessado usando o URL do cliente web(`"https://10.0.16.11/"`) e use o nome de usuário administrador e cole a senha copiada para criar novos segmentos ou modificar os gateways de nível existentes.

Para conectar uma rede local à nuvem privada do VMware Engine, utilize a VPN na nuvem ou o Cloud Interconnect para obter a conectividade apropriada e certifique-se de que as portas necessárias estejam abertas. Para etapas detalhadas, siga estas"link" .





▼ **Implantar o armazenamento de dados suplementar do Google Cloud NetApp Volumes no GCVE**

Referir"Procedimento para implantar armazenamento de dados NFS suplementar com NetApp Volumes para GCVE"

Armazenamento NetApp em nuvens públicas

Opções de armazenamento da NetApp para provedores de nuvem pública

Explore as opções de armazenamento da NetApp nos três principais hiperescaladores.

AWS / VMC

A AWS oferece suporte ao armazenamento NetApp nas seguintes configurações:

- FSx ONTAP como armazenamento conectado a convidados
- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- FSx ONTAP como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para VMC" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para VMC" .

Azure / AVS

O Azure oferece suporte ao armazenamento NetApp nas seguintes configurações:

- Azure NetApp Files (ANF) como armazenamento conectado a convidados
- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- Azure NetApp Files (ANF) como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para AVS" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para AVS" .

GCP / GCVE

O Google Cloud oferece suporte ao armazenamento NetApp nas seguintes configurações:

- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- Google Cloud NetApp Volumes (NetApp Volumes) como armazenamento conectado a convidados
- Google Cloud NetApp Volumes (NetApp Volumes) como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para GCVE" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para GCVE" .

Leia mais sobre"Suporte ao armazenamento de dados do Google Cloud NetApp Volumes para o Google Cloud VMware Engine (blog da NetApp)" ou"Como usar o Google Cloud NetApp Volumes como armazenamento de dados para o Google Cloud VMware Engine (blog do Google)"

Amazon Web Services: opções para usar o armazenamento NetApp

O armazenamento NetApp pode ser anexado ao Amazon Web Services como armazenamento conectado a convidado ou suplementar.

Amazon FSx for NetApp ONTAP (FSx ONTAP) como um armazenamento de dados NFS suplementar

O Amazon FSx ONTAP oferece excelentes opções para implantar e gerenciar cargas de trabalho de aplicativos juntamente com serviços de arquivo, ao mesmo tempo em que reduz o TCO ao tornar os requisitos de dados integrados à camada de aplicativo. Seja qual for o caso de uso, escolha o VMware Cloud on AWS junto com o Amazon FSx ONTAP para rápida concretização dos benefícios da nuvem, infraestrutura consistente e operações do local para a AWS, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial. É o mesmo processo e procedimento familiar usado para conectar o armazenamento.

Para mais informações, visite:

- "FSx ONTAP como um Datastore NFS Suplementar: Visão Geral"
- "Amazon FSx para ONTAP como um datastore suplementar"

Amazon FSx for NetApp ONTAP como armazenamento conectado a convidados

O Amazon FSx ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, criado no popular sistema de arquivos ONTAP da NetApp. O FSx ONTAP combina os recursos familiares, o desempenho, as capacidades e as operações de API dos sistemas de arquivos NetApp com a agilidade, a escalabilidade e a simplicidade de um serviço AWS totalmente gerenciado.

O FSx ONTAP fornece armazenamento de arquivos compartilhados rápido, flexível e rico em recursos, amplamente acessível a partir de instâncias de computação Linux, Windows e macOS executadas na AWS ou no local. O FSx ONTAP oferece armazenamento de unidade de estado sólido (SSD) de alto desempenho com latências abaixo de milissegundos. Com o FSx ONTAP, você pode atingir níveis de desempenho de SSD para sua carga de trabalho pagando pelo armazenamento SSD apenas para uma pequena fração dos seus dados.

Gerenciar seus dados com o FSx ONTAP é mais fácil porque você pode criar snapshots, clonar e replicar seus arquivos com o clique de um botão. Além disso, o FSx ONTAP automaticamente classifica seus dados em armazenamento elástico de menor custo, diminuindo a necessidade de provisionar ou gerenciar capacidade.

O FSx ONTAP também fornece armazenamento altamente disponível e durável com backups totalmente

gerenciados e suporte para recuperação de desastres entre regiões. Para facilitar a proteção dos seus dados, o FSx ONTAP oferece suporte a aplicativos populares de segurança de dados e antivírus.

Para mais informações, visite"FSx ONTAP como armazenamento conectado para convidados"

Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados

O Cloud Volumes ONTAP, ou CVO, é a solução de gerenciamento de dados em nuvem líder do setor, desenvolvida no software de armazenamento ONTAP da NetApp, disponível nativamente na Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

É uma versão definida por software do ONTAP que consome armazenamento nativo da nuvem, permitindo que você tenha o mesmo software de armazenamento na nuvem e no local, reduzindo a necessidade de treinar novamente sua equipe de TI em métodos totalmente novos para gerenciar seus dados.

O CVO oferece aos clientes a capacidade de mover dados facilmente da borda para o data center, para a nuvem e vice-versa, reunindo sua nuvem híbrida — tudo gerenciado com um console de gerenciamento de painel único, o NetApp Cloud Manager.

Por design, o CVO oferece desempenho extremo e recursos avançados de gerenciamento de dados para satisfazer até mesmo seus aplicativos mais exigentes na nuvem.

Para mais informações, visite"CVO como armazenamento conectado a convidados" .

TR-4938: Monte o Amazon FSx ONTAP como um armazenamento de dados NFS com o VMware Cloud na AWS

Este documento descreve como montar o Amazon FSx ONTAP como um armazenamento de dados NFS com o VMware Cloud na AWS.

Introdução

Toda organização bem-sucedida está em um caminho de transformação e modernização. Como parte desse processo, as empresas normalmente usam seus investimentos existentes na VMware para aproveitar os benefícios da nuvem e explorar como migrar, expandir, estender e fornecer recuperação de desastres para processos da maneira mais perfeita possível. Os clientes que migram para a nuvem devem avaliar os casos de uso para elasticidade e pico, saída do data center, consolidação do data center, cenários de fim de vida, fusões, aquisições e assim por diante.

Embora o VMware Cloud on AWS seja a opção preferida pela maioria dos clientes porque oferece recursos híbridos exclusivos, as opções limitadas de armazenamento nativo restringiram sua utilidade para organizações com cargas de trabalho pesadas de armazenamento. Como o armazenamento está diretamente vinculado aos hosts, a única maneira de dimensioná-lo é adicionar mais hosts, o que pode aumentar os custos em 35-40% ou mais para cargas de trabalho com uso intensivo de armazenamento. Essas cargas de trabalho precisam de armazenamento adicional e desempenho segregado, não de potência adicional, mas isso significa pagar por hosts adicionais. É aqui que o "integração recente" do FSx ONTAP é útil para cargas de trabalho com uso intensivo de armazenamento e desempenho com o VMware Cloud na AWS.

Vamos considerar o seguinte cenário: um cliente precisa de oito hosts para potência (vCPU/vMem), mas também tem uma necessidade substancial de armazenamento. Com base na avaliação, eles precisam de 16 hosts para atender aos requisitos de armazenamento. Isso aumenta o TCO geral porque eles precisam comprar toda essa potência adicional quando tudo o que realmente precisam é de mais armazenamento. Isso é aplicável a qualquer caso de uso, incluindo migração, recuperação de desastres, bursting, desenvolvimento/teste e assim por diante.

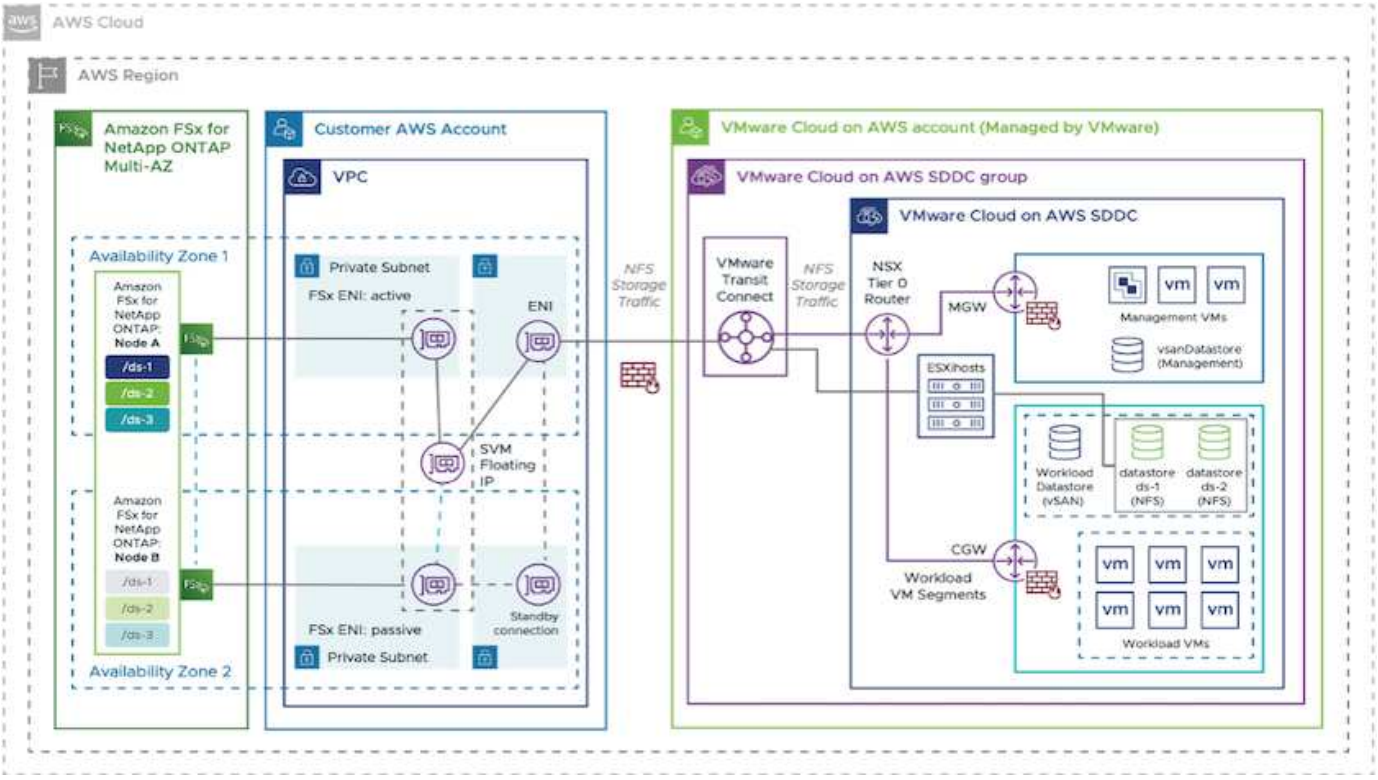
Este documento orienta você nas etapas necessárias para provisionar e anexar o FSx ONTAP como um armazenamento de dados NFS para o VMware Cloud na AWS.

Esta solução também está disponível na VMware. Por favor, visite o"Documentação do VMware Cloud na AWS" para maiores informações.

Opções de conectividade

O VMware Cloud on AWS oferece suporte a implantações de AZ único e de várias AZs do FSx ONTAP.

Esta seção descreve a arquitetura de conectividade de alto nível, juntamente com as etapas necessárias para implementar a solução para expandir o armazenamento em um cluster SDDC sem a necessidade de adicionar hosts adicionais.



As etapas de implantação de alto nível são as seguintes:

1. Crie o Amazon FSx ONTAP em uma nova VPC designada.
2. Crie um grupo SDDC.
3. Crie o VMware Transit Connect e um anexo TGW.
4. Configurar roteamento (AWS VPC e SDDC) e grupos de segurança.
5. Anexe um volume NFS como um armazenamento de dados ao cluster SDDC.

Antes de provisionar e anexar o FSx ONTAP como um armazenamento de dados NFS, você deve primeiro configurar um ambiente VMware on Cloud SDDC ou atualizar um SDDC existente para a versão 1.20 ou superior. Para obter mais informações, consulte o "Introdução ao VMware Cloud na AWS" .

O FSx ONTAP não é atualmente suportado com clusters estendidos.

Conclusão

Este documento aborda as etapas necessárias para configurar o Amazon FSx ONTAP com o VMware Cloud na AWS. O Amazon FSx ONTAP oferece excelentes opções para implantar e gerenciar cargas de trabalho de aplicativos juntamente com serviços de arquivo, ao mesmo tempo em que reduz o TCO ao tornar os requisitos de dados integrados à camada de aplicativo. Seja qual for o caso de uso, escolha o VMware Cloud on AWS junto com o Amazon FSx ONTAP para rápida concretização dos benefícios da nuvem, infraestrutura consistente e operações do local para a AWS, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial. É o mesmo processo e procedimento familiar usado para conectar o armazenamento. Lembre-se de que foi apenas a posição dos dados que mudou junto com os novos nomes; as ferramentas e os processos permanecem os mesmos, e o Amazon FSx ONTAP ajuda a otimizar a implantação geral.

Para saber mais sobre esse processo, fique à vontade para seguir o vídeo passo a passo detalhado.

Amazon FSx ONTAP VMware Cloud

Criando um armazenamento de dados NFS suplementar na AWS

Depois que o VMware Cloud estiver pronto e conectado ao AWS VPC, você deverá implantar o Amazon FSx ONTAP em um VPC recém-designado em vez do VPC padrão original conectado ou existente.

Para começar, implante uma VPC adicional na mesma região e zona de disponibilidade onde o SDDC reside e, em seguida, implante o Amazon FSx ONTAP na nova VPC. "Configuração de um grupo SDDC na nuvem VMware" O console habilita as opções de configuração de rede necessárias para conectar-se à VPC recém-designada onde o FSx ONTAP será implantado.

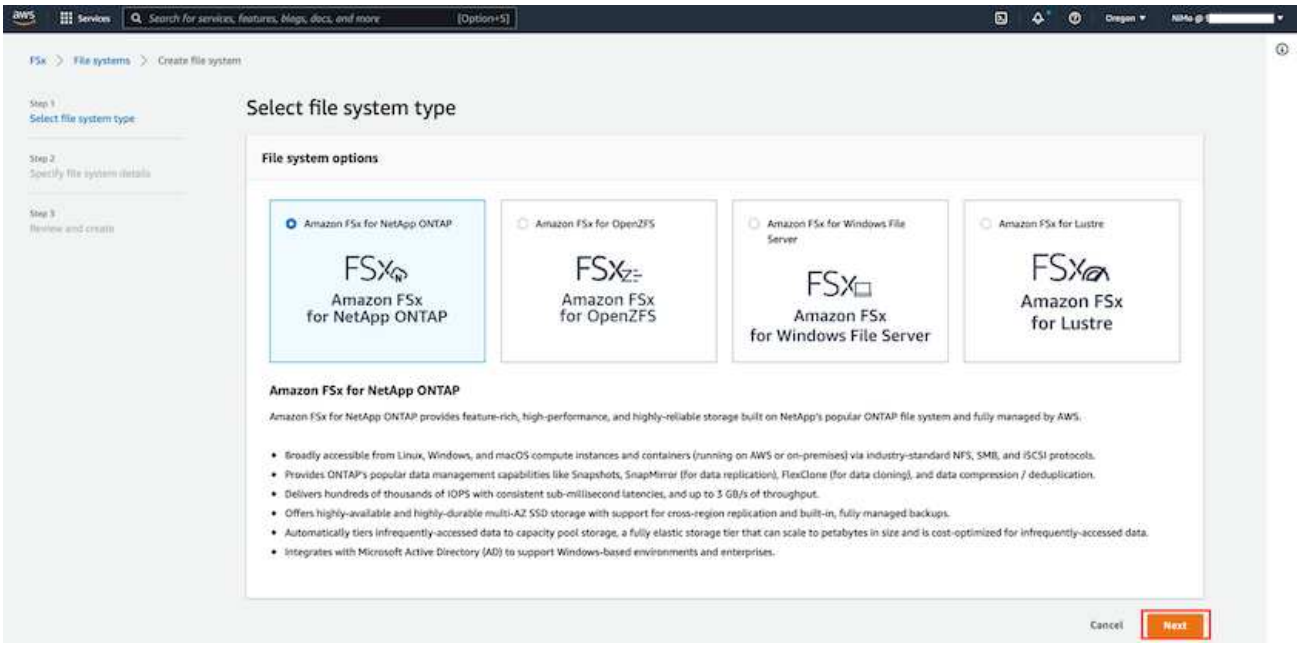
> Implante o FSx ONTAP na mesma zona de disponibilidade que o VMware Cloud no AWS SDDC.

> Não é possível implantar o FSx ONTAP na VPC conectada. Em vez disso, você deve implantá-lo em uma nova VPC designada e, em seguida, conectar a VPC a um VMware Managed Transit Gateway (vTGW) por meio de grupos SDDC.

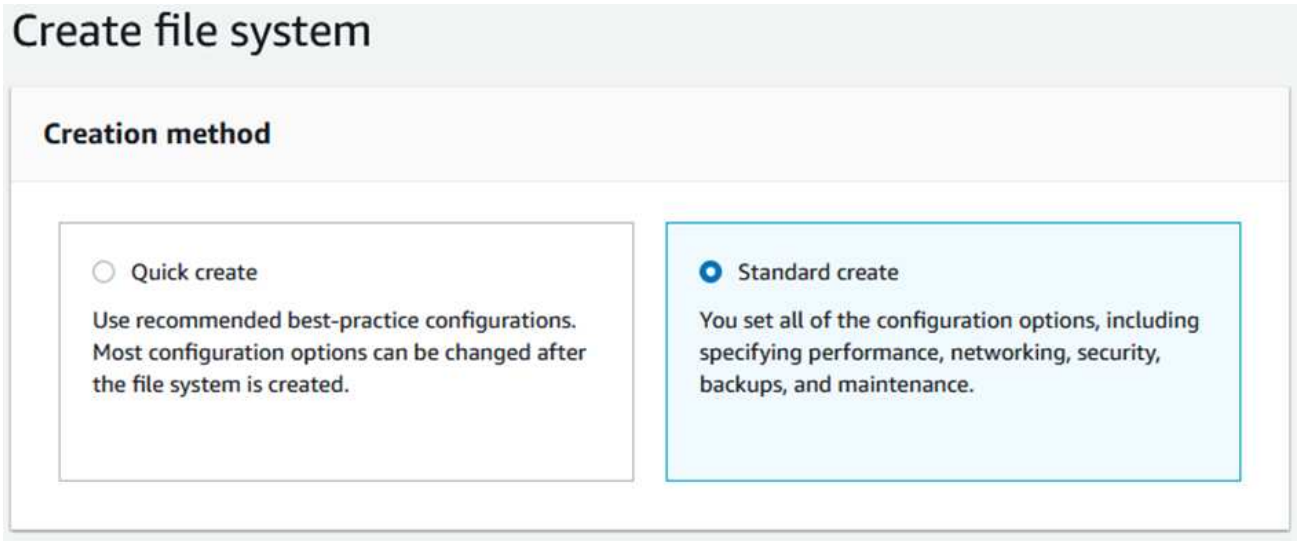
▼ **Etapa 1: criar o Amazon FSx ONTAP em uma nova VPC designada**

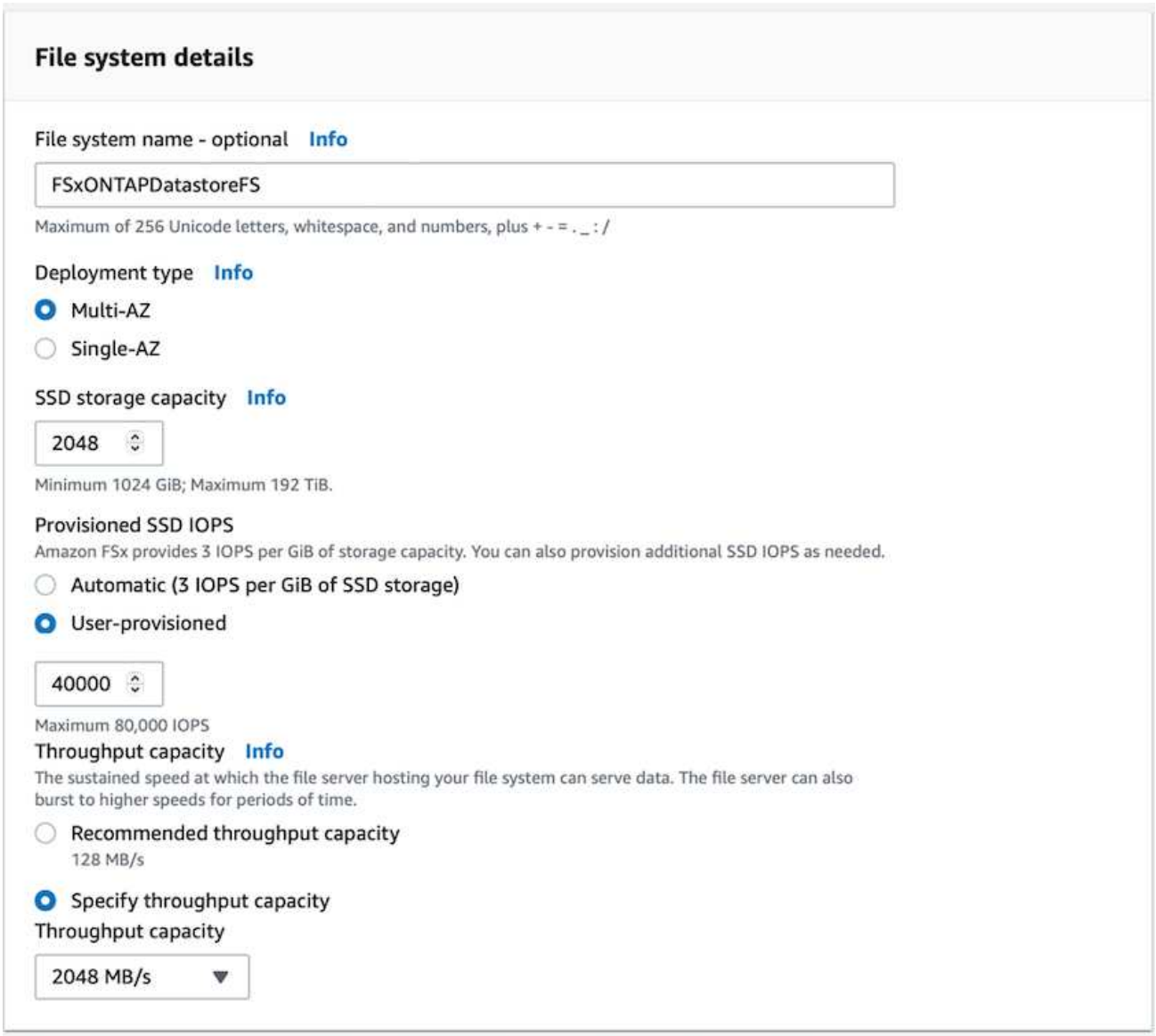
Para criar e montar o sistema de arquivos Amazon FSx ONTAP , conclua as seguintes etapas:

1. Abra o console do Amazon FSx em `https://console.aws.amazon.com/fsx/` e escolha **Criar sistema de arquivos** para iniciar o assistente **Criação de sistema de arquivos**.
2. Na página Selecionar tipo de sistema de arquivo, selecione * Amazon FSx ONTAP* e clique em **Avançar**. A página **Criar sistema de arquivos** é exibida.



3. Para o método de criação, escolha **Criação Padrão**.





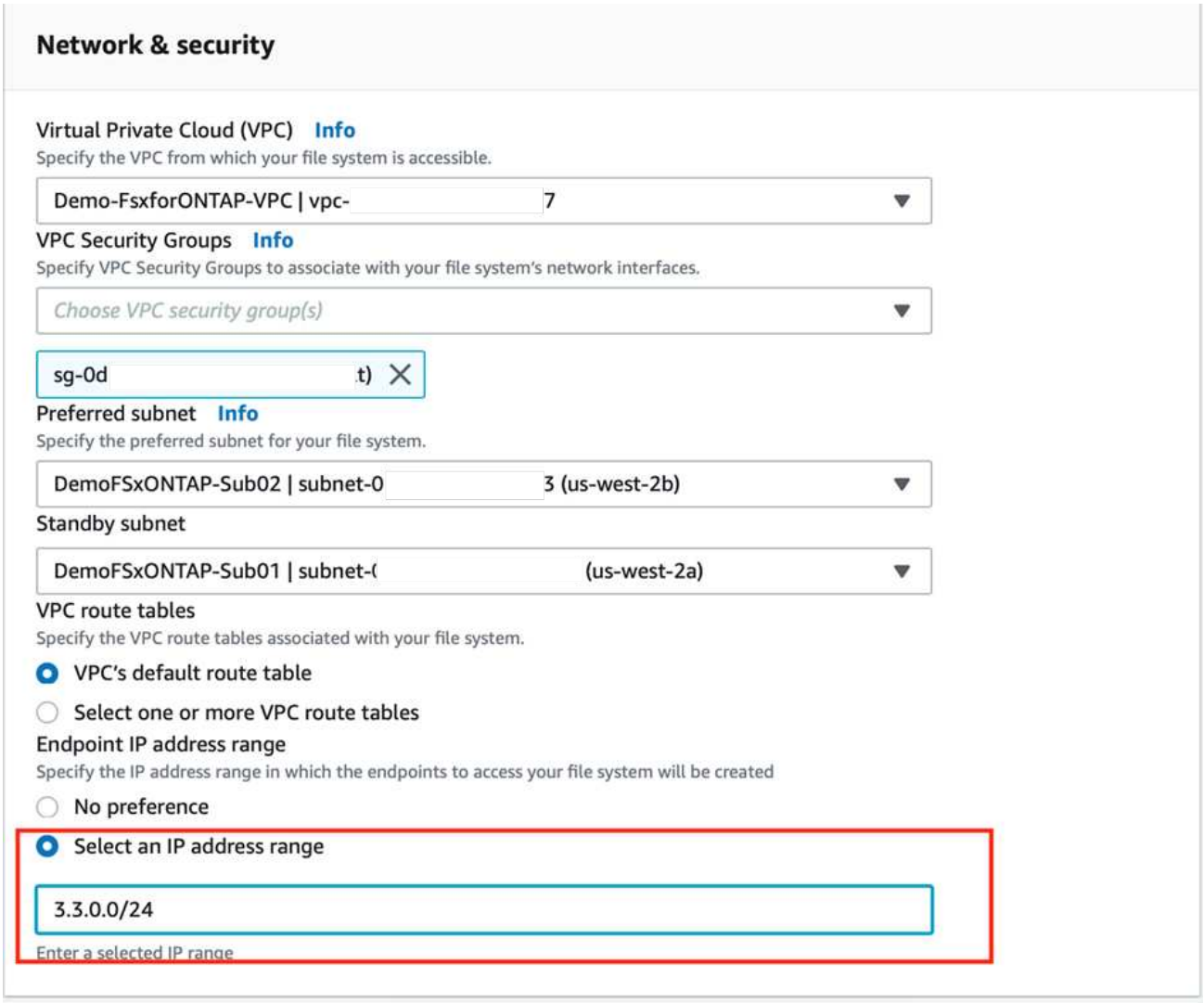
Os tamanhos do armazenamento de dados variam bastante de cliente para cliente. Embora o número recomendado de máquinas virtuais por armazenamento de dados NFS seja subjetivo, muitos fatores determinam o número ideal de VMs que podem ser colocadas em cada armazenamento de dados. Embora a maioria dos administradores considere apenas a capacidade, a quantidade de E/S simultânea enviada aos VMDKs é um dos fatores mais importantes para o desempenho geral. Use estatísticas de desempenho locais para dimensionar os volumes do armazenamento de dados adequadamente.

4. Na seção **Rede** da Nuvem Privada Virtual (VPC), escolha a VPC apropriada e as sub-redes preferenciais, juntamente com a tabela de rotas. Neste caso, Demo-FSxforONTAP-VPC é selecionado no menu suspenso.

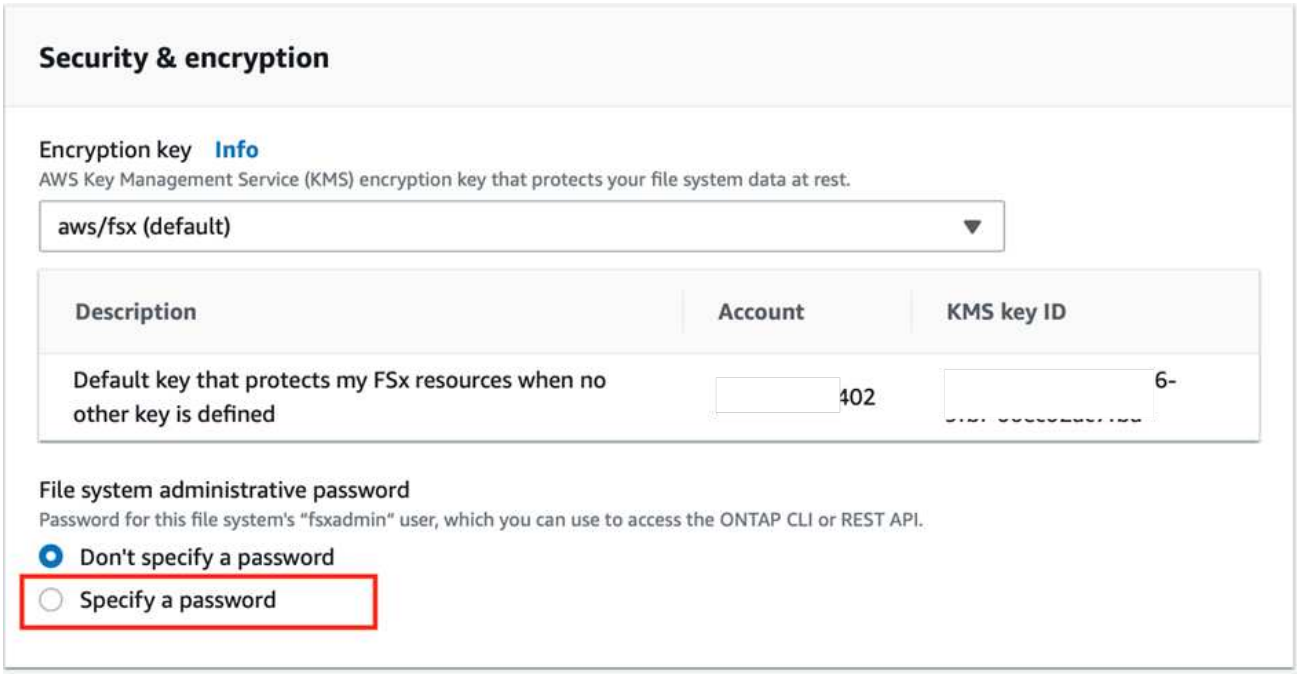
Certifique-se de que esta seja uma nova VPC designada e não a VPC conectada.

Por padrão, o FSx ONTAP usa 198.19.0.0/16 como o intervalo de endereço IP de ponto de extremidade padrão para o sistema de arquivos. Certifique-se de que o intervalo de endereços IP do endpoint não entre em conflito com o VMC no AWS SDDC, nas sub-

redes VPC associadas e na infraestrutura local. Se não tiver certeza, use um intervalo que não se sobreponha e não haja conflitos.

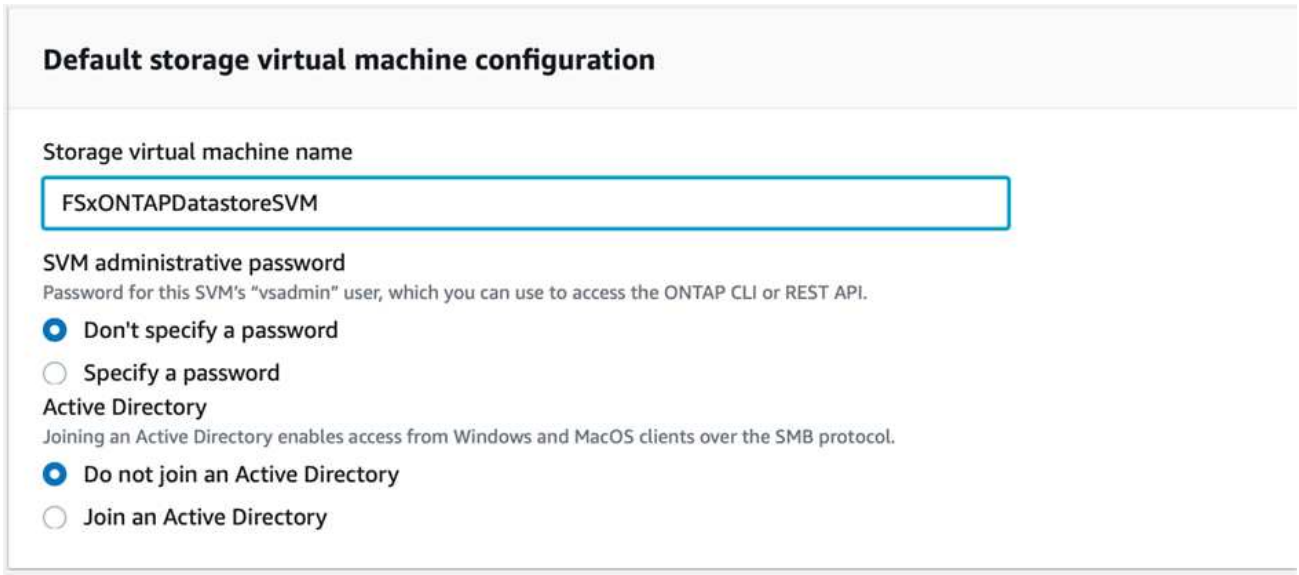


5. Na seção **Segurança e Criptografia** da chave de criptografia, escolha a chave de criptografia do AWS Key Management Service (AWS KMS) que protege os dados em repouso do sistema de arquivos. Para a **Senha administrativa do sistema de arquivos**, insira uma senha segura para o usuário fsxadmin.



6. Na seção **Configuração padrão da máquina virtual de armazenamento**, especifique o nome da SVM.

   A partir do GA, quatro armazenamentos de dados NFS são suportados.



7. Na seção **Configuração de volume padrão**, especifique o nome e o tamanho do volume necessário para o armazenamento de dados e clique em **Avançar**. Este deve ser um volume NFSv3. Para **Eficiência de armazenamento**, escolha **Ativado** para ativar os recursos de eficiência de armazenamento do ONTAP (compactação, desduplicação e compactação). Após a criação, use o shell para modificar os parâmetros do volume usando ***volume modify*** da seguinte maneira:

Contexto	Configuração
Garantia de volume (estilo de garantia de espaço)	Nenhum (thin provisioned) – definido por padrão
reserva_fracionária (reserva-fracionária)	0% – definido por padrão

Contexto	Configuração
snap_reserve (percentual de espaço para instantâneo)	0%
Dimensionamento automático (modo de dimensionamento automático)	crescer_encolher
Eficiência de armazenamento	Habilitado – definido por padrão
Excluir automaticamente	volume / mais antigo primeiro
Política de níveis de volume	Somente instantâneo – definido por padrão
tente_primeiro	Crescimento automático
Política de instantâneo	Nenhum

Use o seguinte comando SSH para criar e modificar volumes:

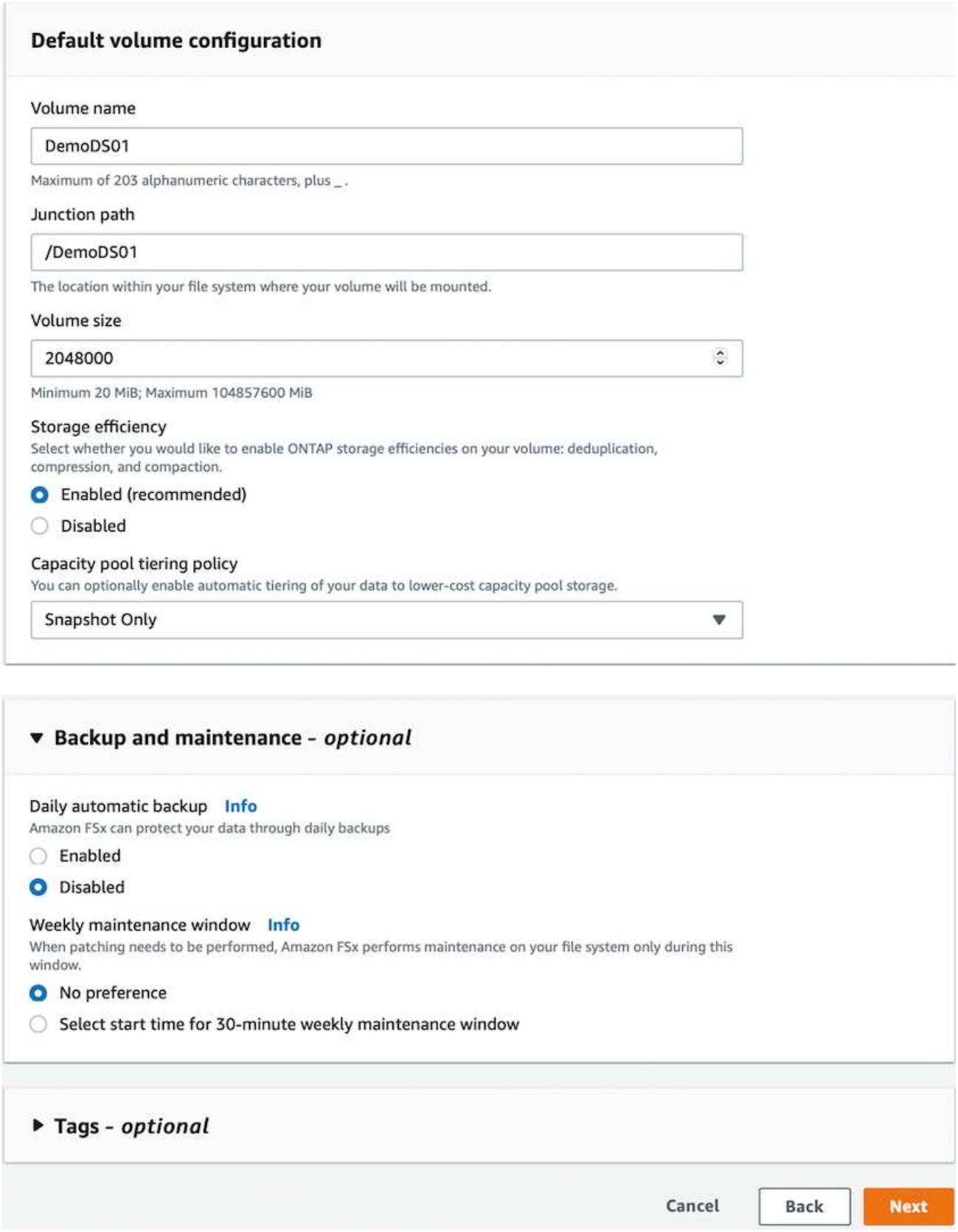
Comando para criar novo volume de armazenamento de dados a partir do shell:

```
volume create -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-aggregate aggr1 -size 1024GB -state online -tiering-policy snapshot-
only -percent-snapshot-space 0 -autosize-mode grow -snapshot-policy
none -junction-path /DemoDS002
```

Observação: Os volumes criados via shell levarão alguns minutos para aparecer no console da AWS.

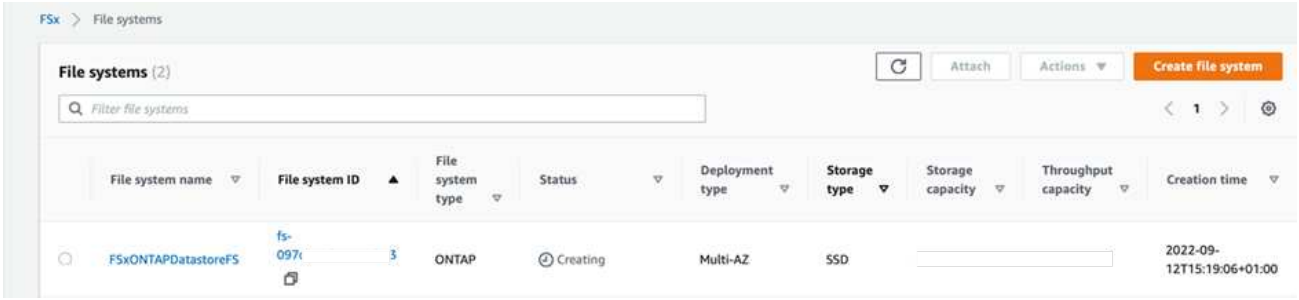
Comando para modificar parâmetros de volume que não são definidos por padrão:

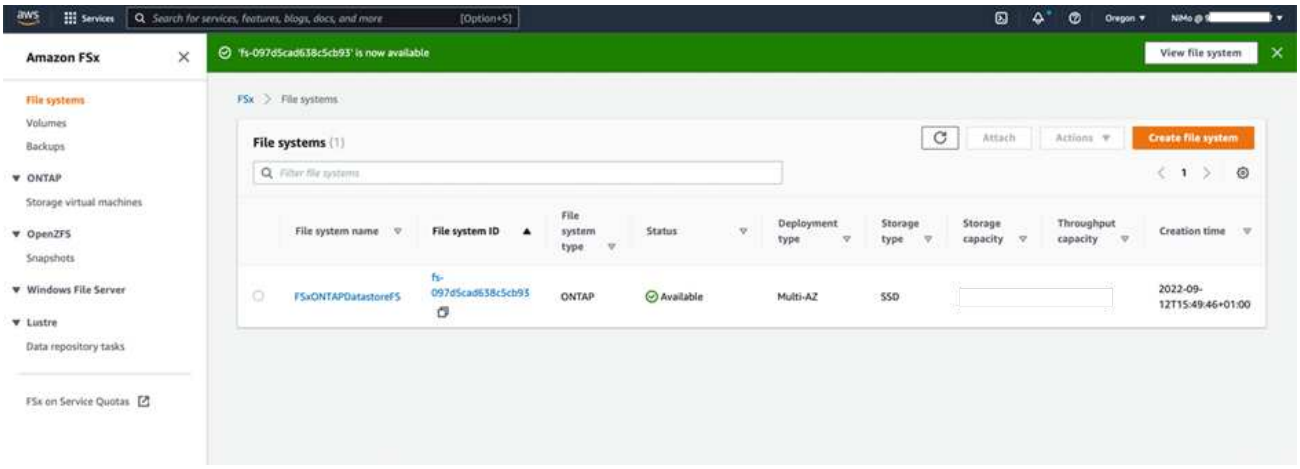
```
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-fractional-reserve 0
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002 -space
-mgmt-try-first vol_grow
volume modify -vserver FSxONTAPDatastoreSVM -volume DemoDS002
-autosize-mode grow
```



Durante o cenário de migração inicial, a política de snapshot padrão pode causar problemas de capacidade máxima do armazenamento de dados. Para superar isso, modifique a política de snapshot para atender às necessidades.

8. Revise a configuração do sistema de arquivos mostrada na página **Criar sistema de arquivos**.
9. Clique em **Criar sistema de arquivos**.





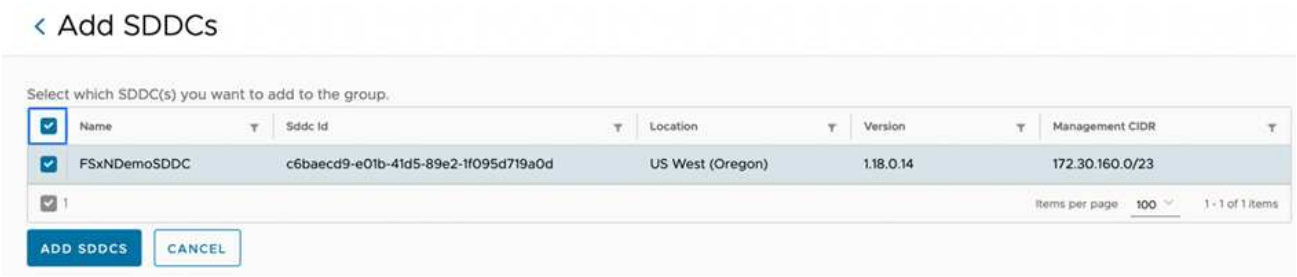
Repita as etapas anteriores para criar mais máquinas virtuais de armazenamento ou sistemas de arquivos e volumes de armazenamento de dados de acordo com os requisitos de capacidade e desempenho.

Para saber mais sobre o desempenho do Amazon FSx ONTAP , consulte "Desempenho do Amazon FSx ONTAP" .

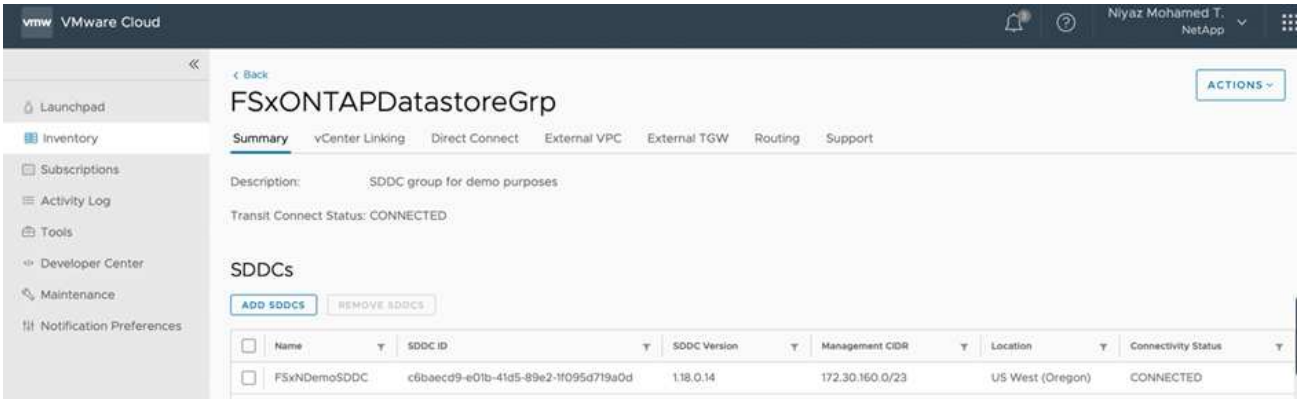
▼ Etapa 2: Criar grupo SDDC

Depois que os sistemas de arquivos e SVMs forem criados, use o VMware Console para criar um grupo SDDC e configurar o VMware Transit Connect. Para fazer isso, conclua as etapas a seguir e lembre-se de que você deve navegar entre o VMware Cloud Console e o AWS Console.

1. Faça login no console do VMC em `https://vmc.vmware.com` .
2. Na página **Inventário**, clique em **Grupos SDDC**.
3. Na aba **Grupos SDDC**, clique em **AÇÕES** e selecione **Criar Grupo SDDC**. Para fins de demonstração, o grupo SDDC é chamado `FSxONTAPDatastoreGrp` .
4. Na grade de Associação, selecione os SDDCs a serem incluídos como membros do grupo.

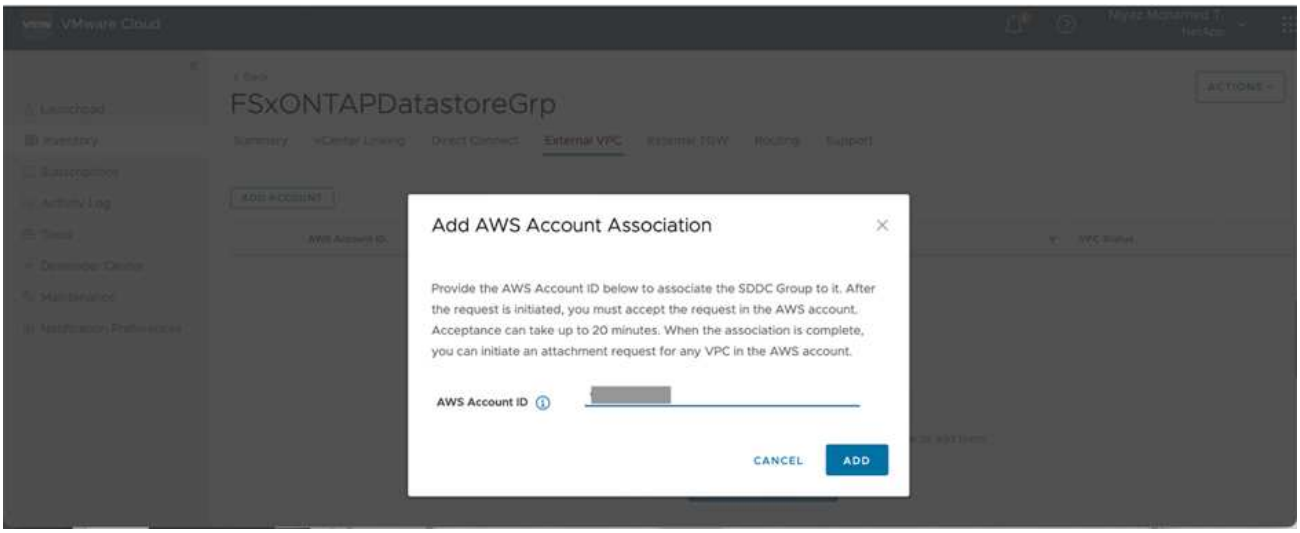


5. Verifique se a opção "Configurar o VMware Transit Connect para seu grupo incorrerá em cobranças por anexo e transferência de dados" está marcada e selecione **Criar grupo**. O processo pode levar alguns minutos para ser concluído.

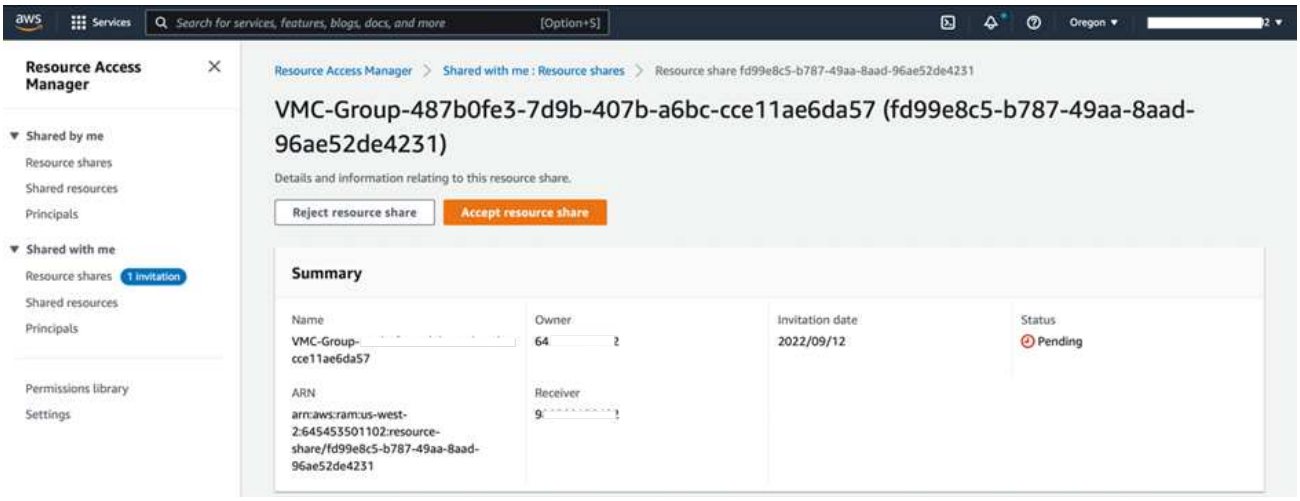


▼ **Etapa 3: Configurar a conexão do VMware Transit**

1. Anexe a VPC designada recém-criada ao grupo SDDC. Selecione a aba **VPC Externa** e siga as instruções "instruções para anexar uma VPC externa ao grupo" . Esse processo pode levar de 10 a 15 minutos para ser concluído.

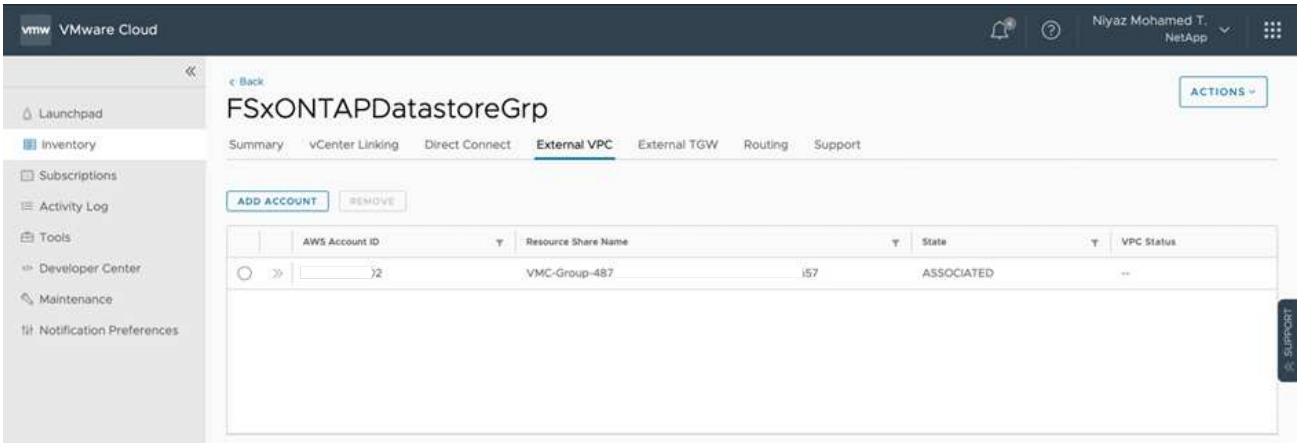


2. Clique em **Adicionar conta**.
   a. Forneça a conta da AWS que foi usada para provisionar o sistema de arquivos FSx ONTAP .
   b. Clique em **Adicionar**.
3. De volta ao console da AWS, faça login na mesma conta da AWS e navegue até a página de serviço **Resource Access Manager**. Há um botão para você aceitar o compartilhamento de recursos.



Como parte do processo de VPC externa, você será solicitado pelo console da AWS a acessar um novo recurso compartilhado por meio do Resource Access Manager. O recurso compartilhado é o AWS Transit Gateway gerenciado pelo VMware Transit Connect.

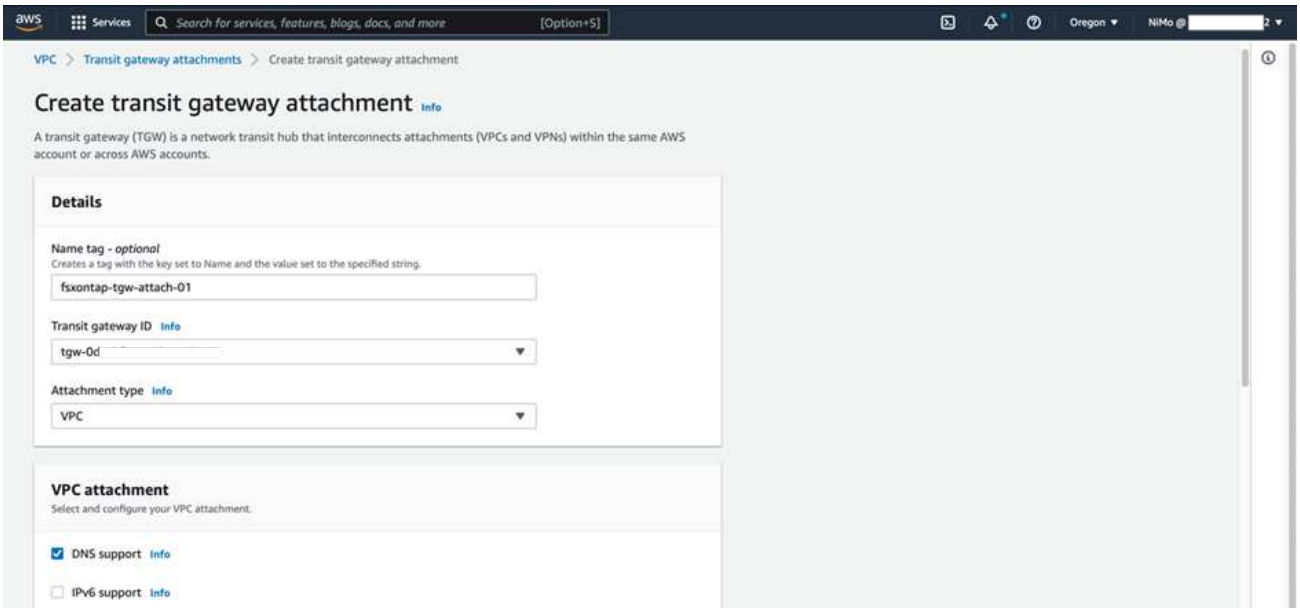
4. Clique em **Aceitar compartilhamento de recursos**.



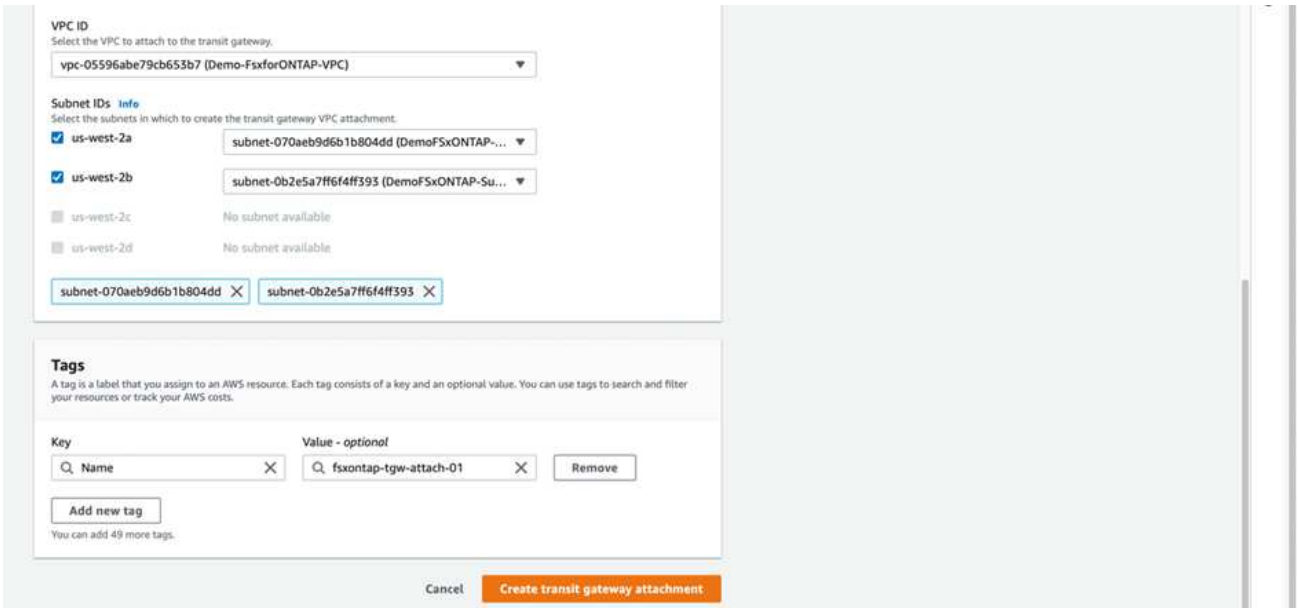
5. De volta ao Console do VMC, você vê que a VPC externa está em um estado associado. Isso pode levar vários minutos para aparecer.

▼ Etapa 4: criar anexo de gateway de trânsito

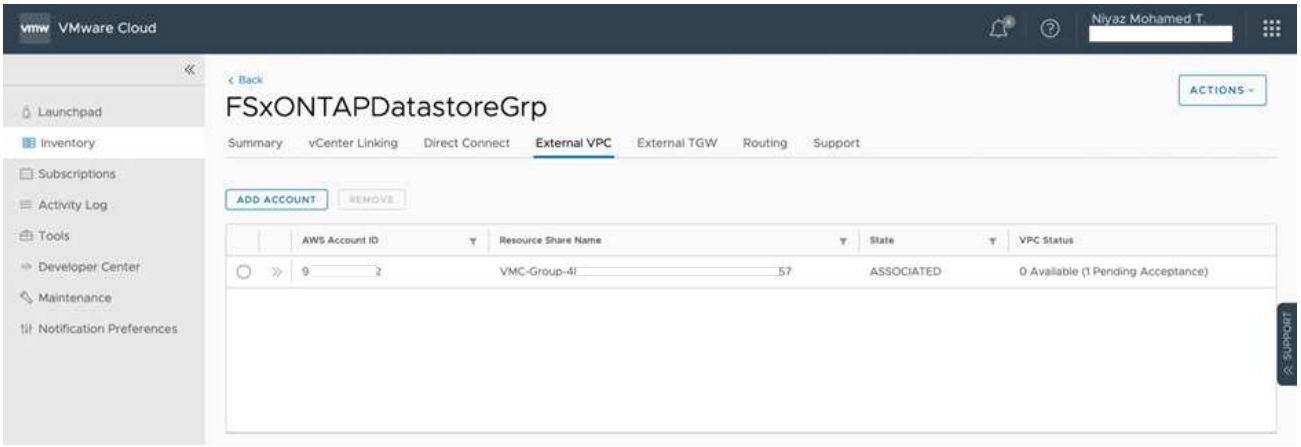
1. No console da AWS, acesse a página de serviço da VPC e navegue até a VPC que foi usada para provisionar o sistema de arquivos FSx. Aqui, você cria um anexo de gateway de trânsito clicando em **Anexo de gateway de trânsito** no painel de navegação à direita.
2. Em **Anexo de VPC**, certifique-se de que Suporte a DNS esteja marcado e selecione a VPC na qual o FSx ONTAP foi implantado.

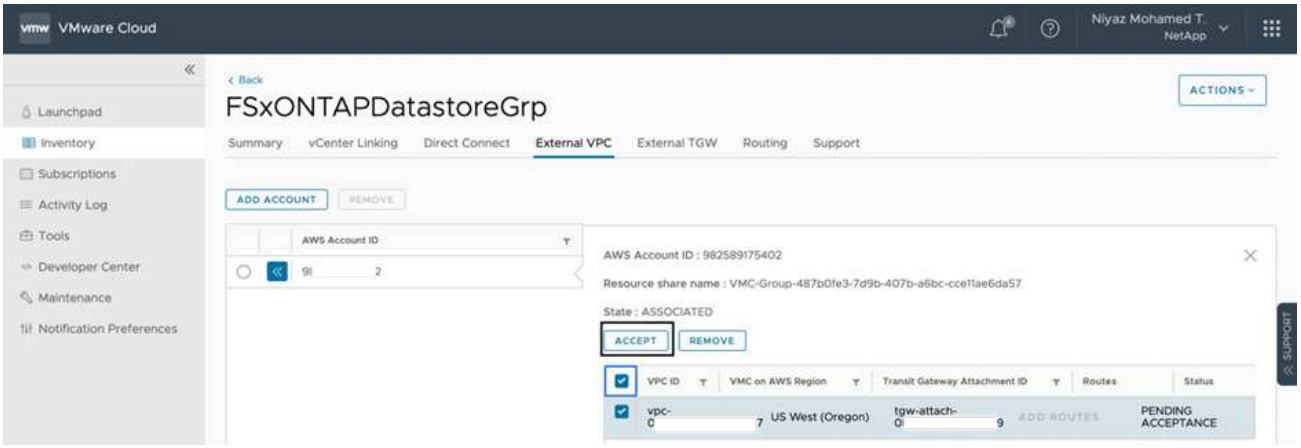


3. Clique em **Criar anexo de gateway de trânsito**.



4. De volta ao VMware Cloud Console, navegue de volta para a guia Grupo SDDC > VPC externa. Selecione o ID da conta AWS usado para o FSx, clique na VPC e clique em **Aceitar**.

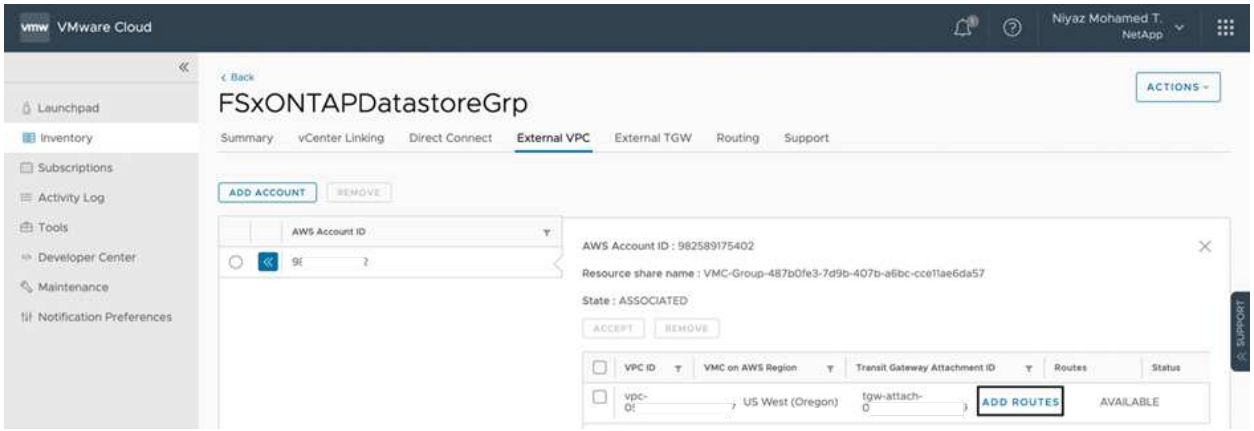


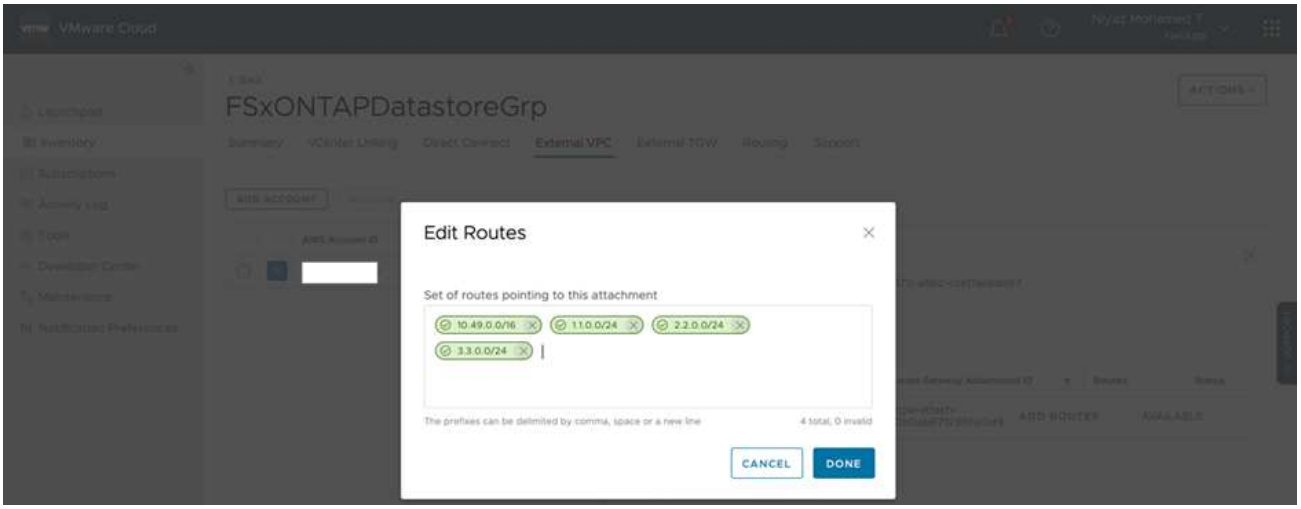


Esta opção pode levar alguns minutos para aparecer.

5. Em seguida, na aba **VPC externa** na coluna **Rotas**, clique na opção **Adicionar rotas** e adicione as rotas necessárias:

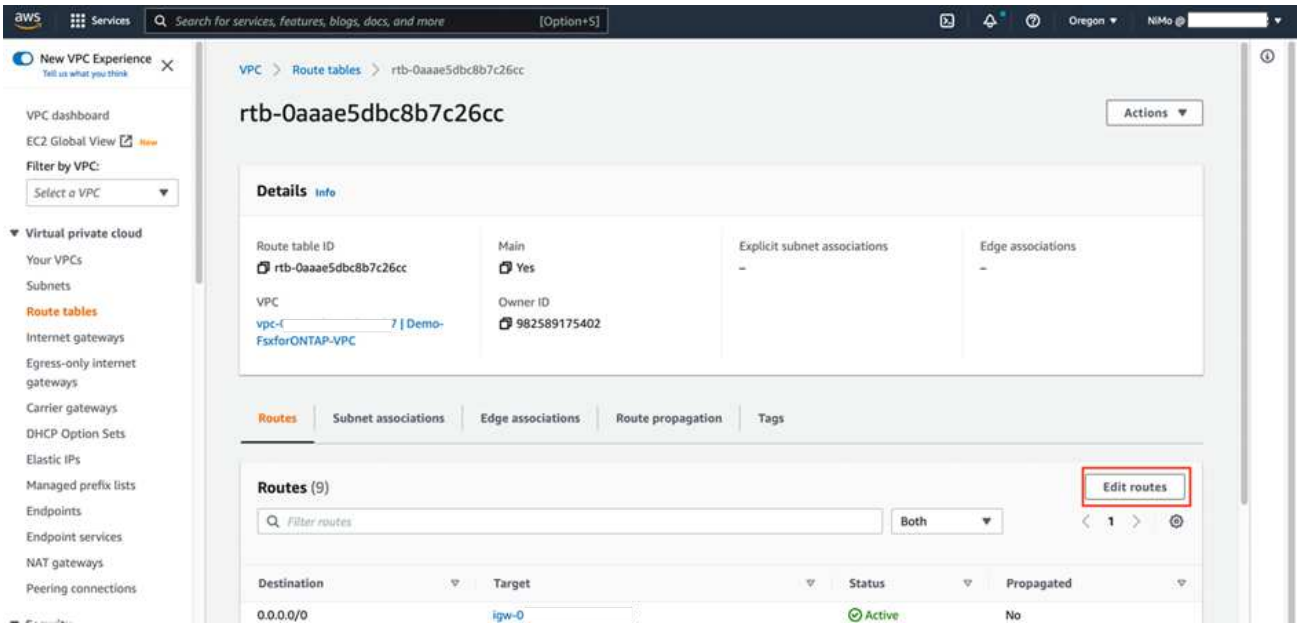
   - Uma rota para o intervalo de IP flutuante para IPs flutuantes do Amazon FSx ONTAP .
   - Uma rota para o espaço de endereço VPC externo recém-criado.



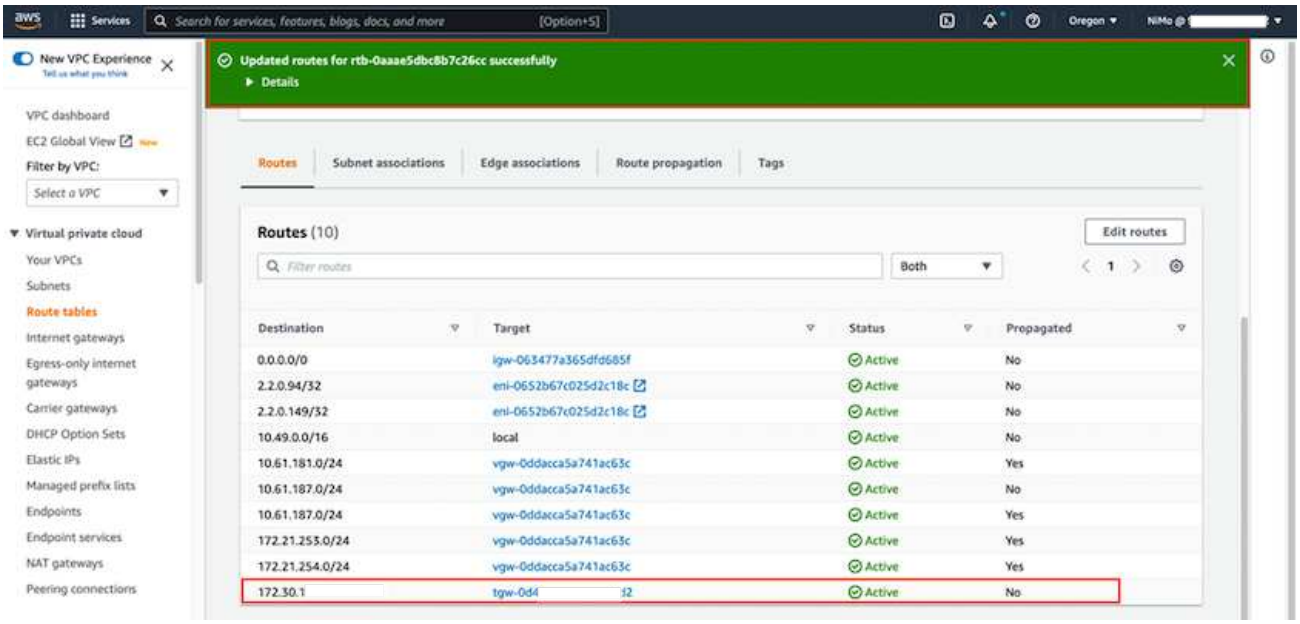


▼ **Etapa 5: configurar roteamento (AWS VPC e SDDC) e grupos de segurança**

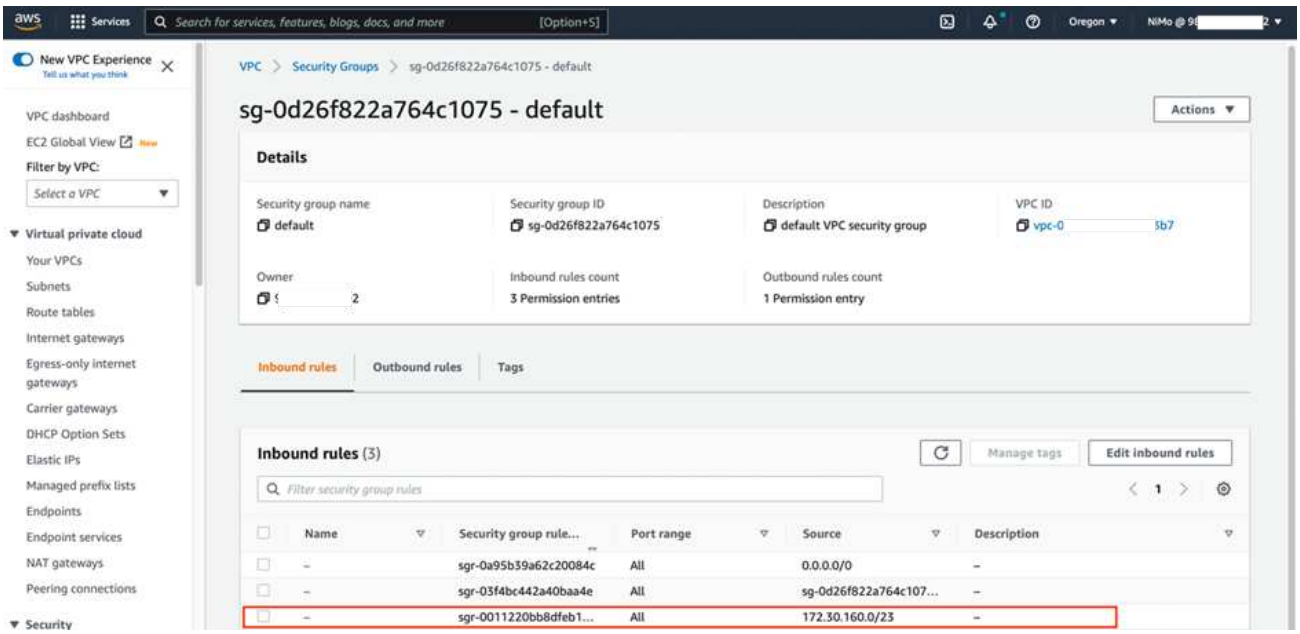
1. No console da AWS, crie a rota de volta para o SDDC localizando a VPC na página de serviço da VPC e selecione a tabela de rotas **principal** para a VPC.
2. Navegue até a tabela de rotas no painel inferior e clique em **Editar rotas**.



3. No painel **Editar rotas**, clique em **Adicionar rota** e insira o CIDR para a infraestrutura do SDDC selecionando **Transit Gateway** e o ID do TGW associado. Clique em **Salvar alterações**.



4. A próxima etapa é verificar se o grupo de segurança na VPC associada está atualizado com as regras de entrada corretas para o CIDR do grupo SDDC.
5. Atualize a regra de entrada com o bloco CIDR da infraestrutura do SDDC.



Verifique se a tabela de rotas da VPC (onde o FSx ONTAP reside) está atualizada para evitar problemas de conectividade.

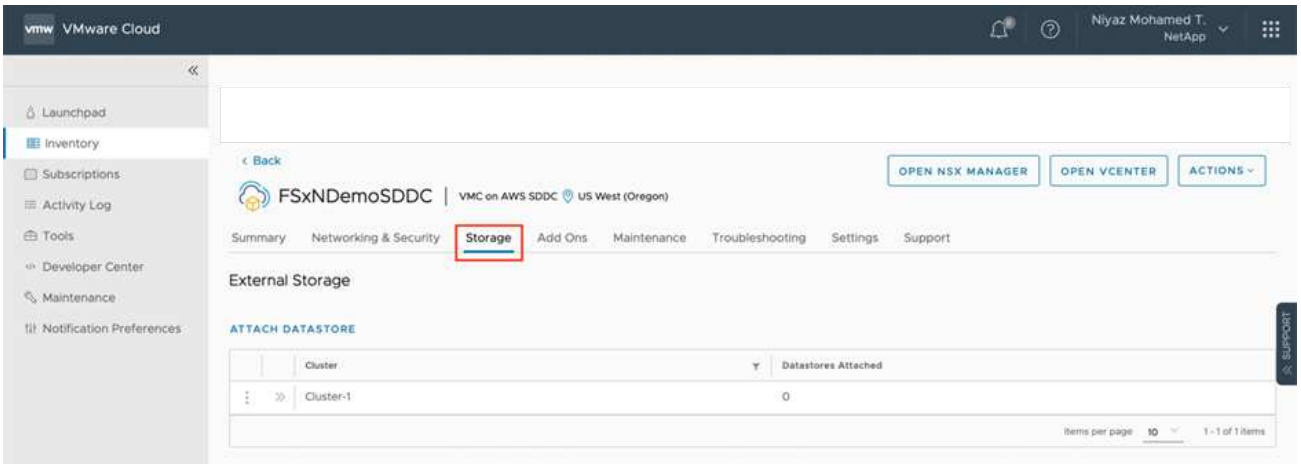
Atualize o grupo de segurança para aceitar tráfego NFS.

Esta é a etapa final na preparação da conectividade com o SDDC apropriado. Com o sistema de arquivos configurado, rotas adicionadas e grupos de segurança atualizados, é hora de montar o(s) armazenamento(s) de dados.

▼ **Etapa 6: anexar volume NFS como um armazenamento de dados ao cluster SDDC**

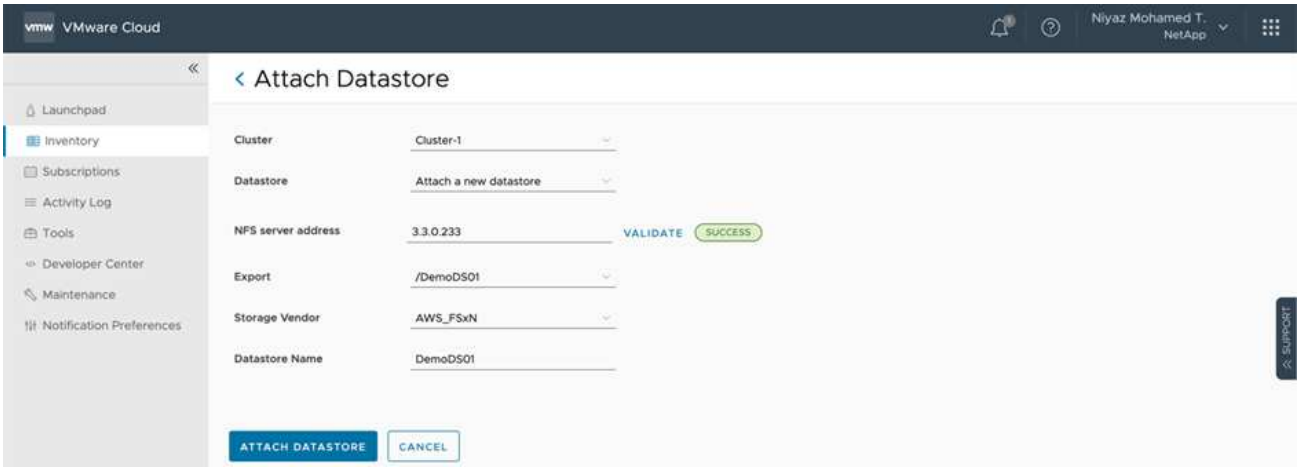
Depois que o sistema de arquivos for provisionado e a conectividade estiver estabelecida, acesse o VMware Cloud Console para montar o armazenamento de dados NFS.

1. No console do VMC, abra a guia **Armazenamento** do SDDC.

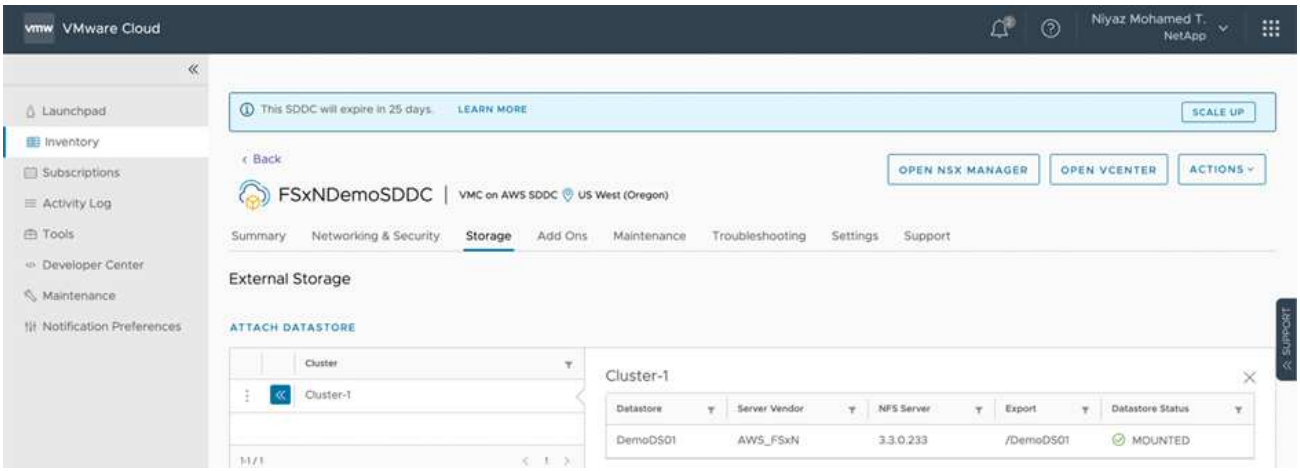


2. Clique em **ANEXAR DATASTORE** e preencha os valores necessários.

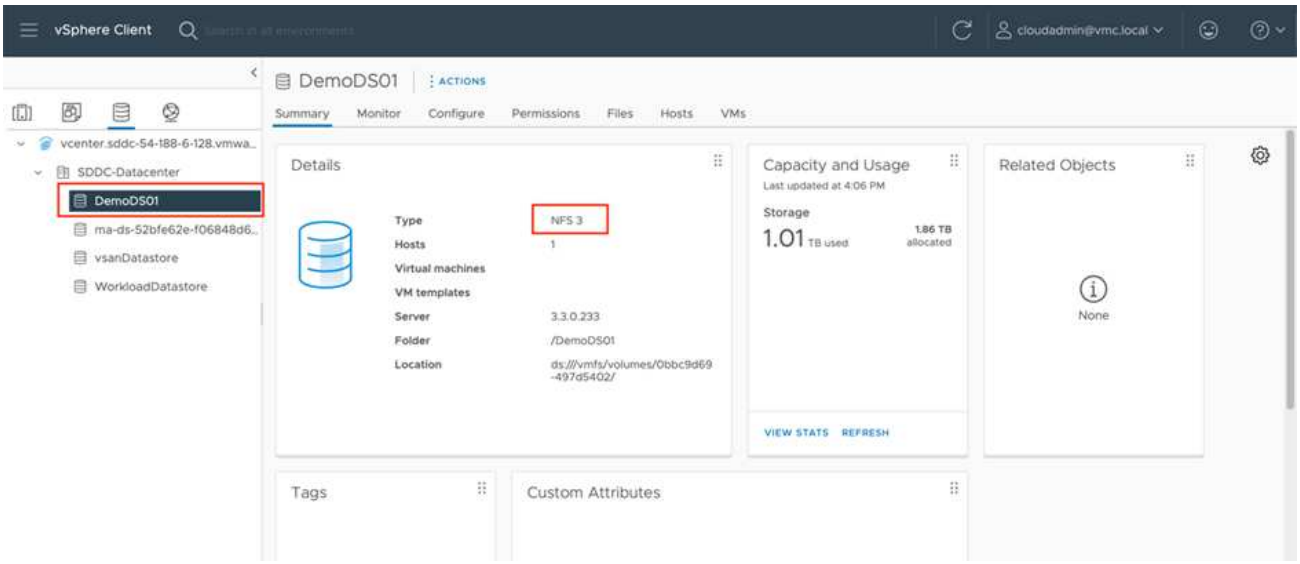
> O endereço do servidor NFS é o endereço IP NFS que pode ser encontrado em FSx > guia Máquinas virtuais de armazenamento > Endpoints no console da AWS.



3. Clique em **ATTACH DATASTORE** para anexar o armazenamento de dados ao cluster.



4. Valide o armazenamento de dados NFS acessando o vCenter conforme mostrado abaixo:



Opções de armazenamento conectado do NetApp Guest para AWS

A AWS oferece suporte ao armazenamento NetApp conectado a convidados com o serviço FSx nativo (FSx ONTAP) ou com o Cloud Volumes ONTAP (CVO).

FSx ONTAP

O Amazon FSx ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, criado no popular sistema de arquivos ONTAP da NetApp. O FSx ONTAP combina os recursos familiares, o desempenho, as capacidades e as operações de API dos sistemas de arquivos NetApp com a agilidade, a escalabilidade e a simplicidade de um serviço AWS totalmente gerenciado.

O FSx ONTAP fornece armazenamento de arquivos compartilhados rápido, flexível e rico em recursos, amplamente acessível a partir de instâncias de computação Linux, Windows e macOS executadas na AWS ou no local. O FSx ONTAP oferece armazenamento de unidade de estado sólido (SSD) de alto desempenho com latências abaixo de um milissegundo. Com o FSx ONTAP, você pode atingir níveis de desempenho de SSD para sua carga de trabalho pagando pelo armazenamento SSD apenas para uma pequena fração dos seus dados.

Gerenciar seus dados com o FSx ONTAP é mais fácil porque você pode criar snapshots, clonar e replicar seus arquivos com o clique de um botão. Além disso, o FSx ONTAP automaticamente classifica seus dados em armazenamento elástico de menor custo, diminuindo a necessidade de provisionar ou gerenciar capacidade.

O FSx ONTAP também fornece armazenamento altamente disponível e durável com backups totalmente gerenciados e suporte para recuperação de desastres entre regiões. Para facilitar a proteção dos seus dados, o FSx ONTAP oferece suporte a aplicativos populares de segurança de dados e antivírus.

FSx ONTAP como armazenamento conectado a convidados

▼ **Configurar o Amazon FSx ONTAP com o VMware Cloud na AWS**

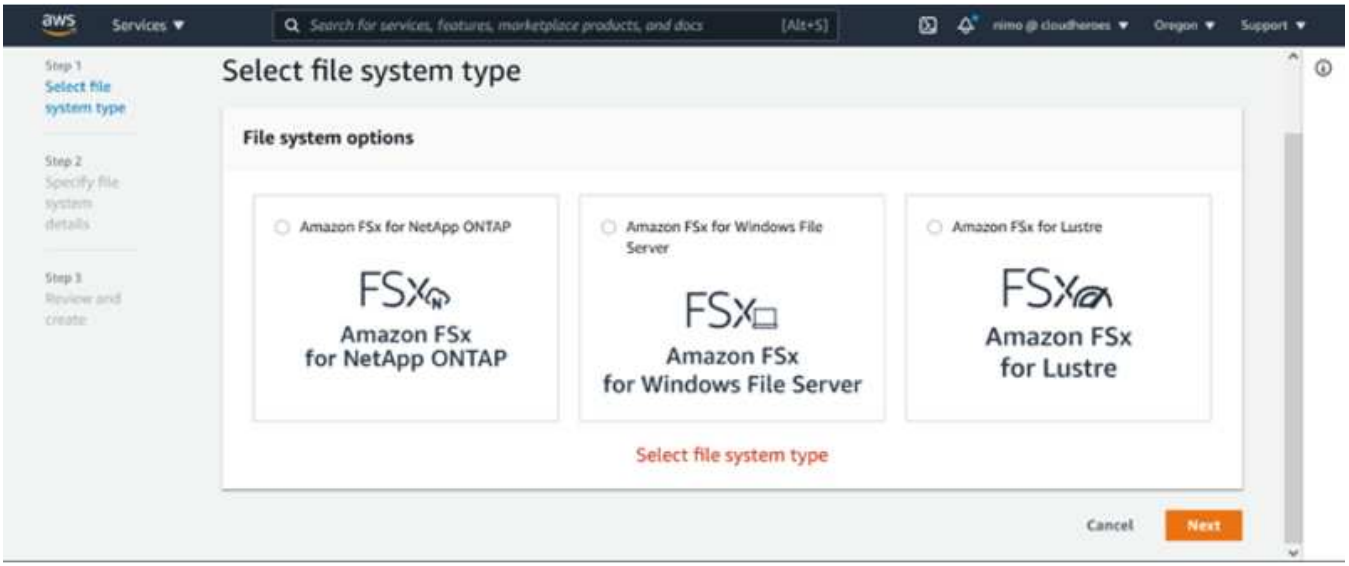
Os compartilhamentos de arquivos ONTAP e LUNs do Amazon FSx podem ser montados a partir de VMs criadas no ambiente VMware SDDC no VMware Cloud na AWS. Os volumes também podem ser montados no cliente Linux e mapeados no cliente Windows usando o protocolo NFS ou SMB, e os LUNS podem ser acessados em clientes Linux ou Windows como dispositivos de bloco quando montados via iSCSI. O Amazon FSx para o sistema de arquivos NetApp ONTAP pode ser configurado rapidamente com as seguintes etapas.

> ⓘ O Amazon FSx ONTAP e o VMware Cloud on AWS devem estar na mesma zona de disponibilidade para obter melhor desempenho e evitar cobranças de transferência de dados entre zonas de disponibilidade.

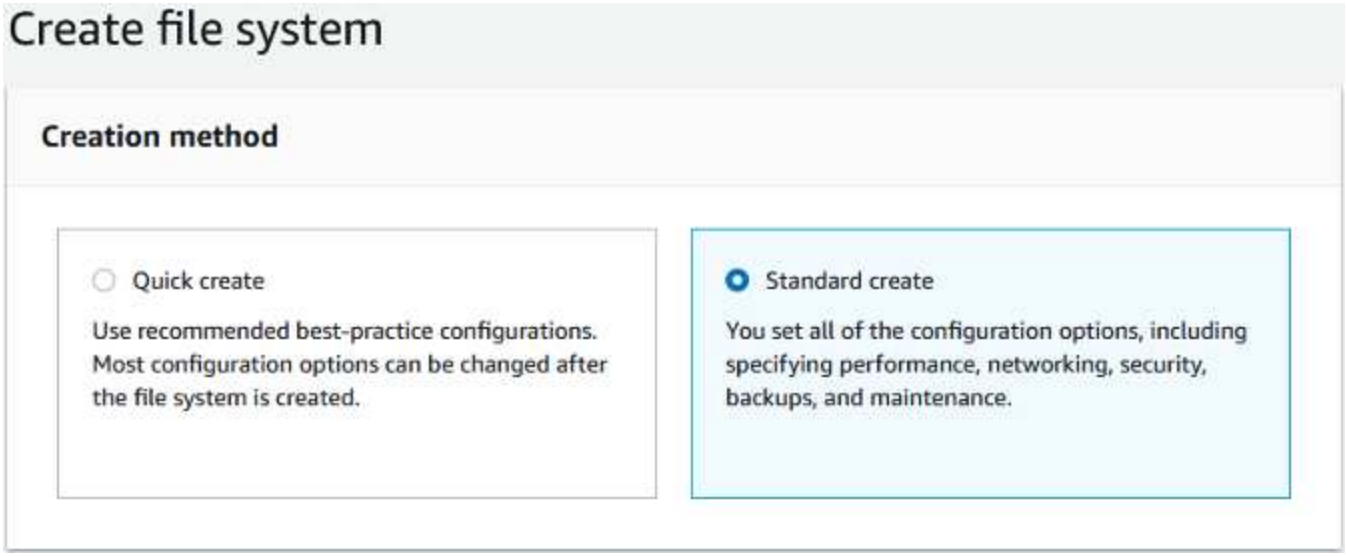
▼ **Criar e montar volumes Amazon FSx ONTAP**

Para criar e montar o sistema de arquivos Amazon FSx ONTAP , conclua as seguintes etapas:

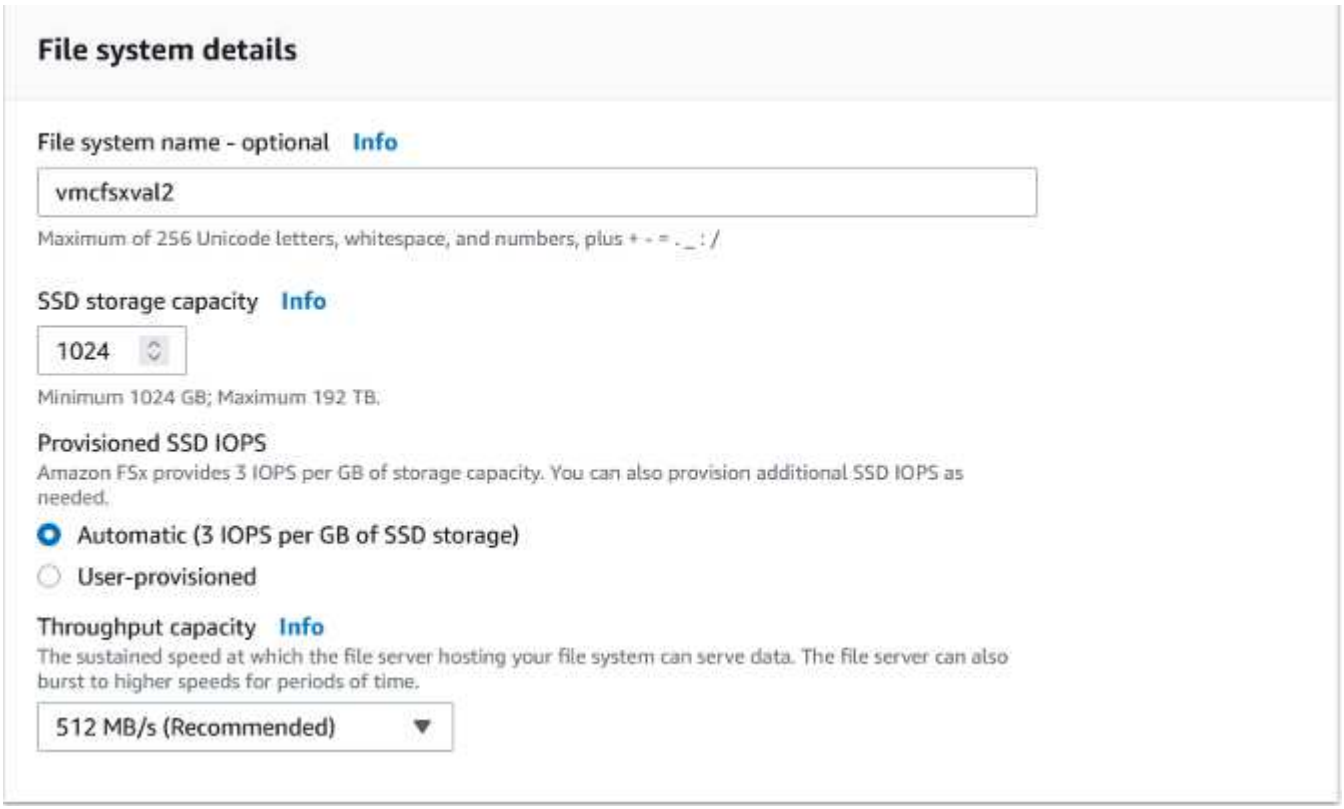
1. Abra o"Console Amazon FSx" e escolha Criar sistema de arquivos para iniciar o assistente de criação do sistema de arquivos.
2. Na página Selecionar tipo de sistema de arquivo, escolha Amazon FSx ONTAP e, em seguida, Avançar. A página Criar sistema de arquivos é exibida.



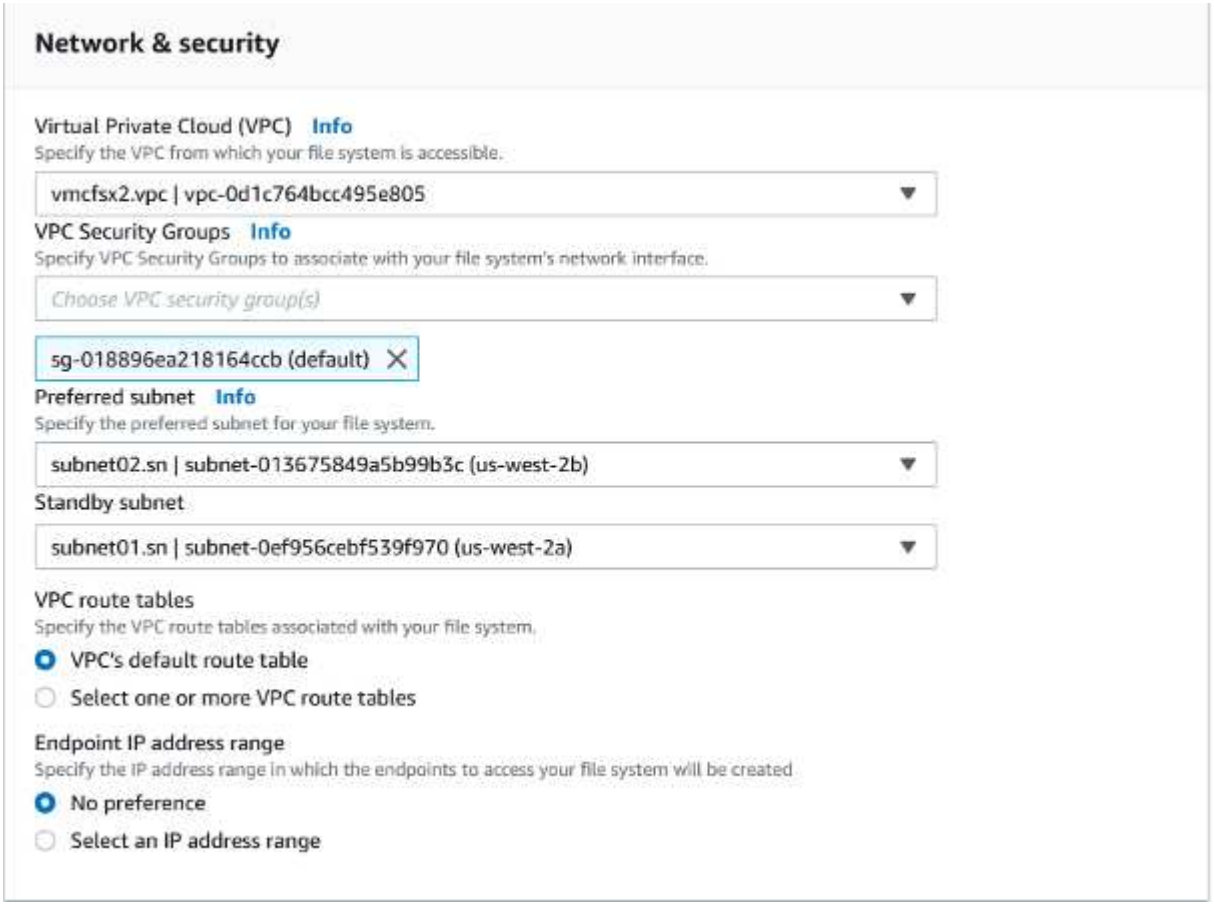
1. Na seção Rede, para Nuvem Privada Virtual (VPC), escolha a VPC apropriada e as sub-redes preferenciais, juntamente com a tabela de rotas. Neste caso, vmcfsx2.vpc é selecionado no menu suspenso.



1. Para o método de criação, escolha Criação Padrão. Você também pode escolher Criação rápida, mas este documento usa a opção de criação padrão.

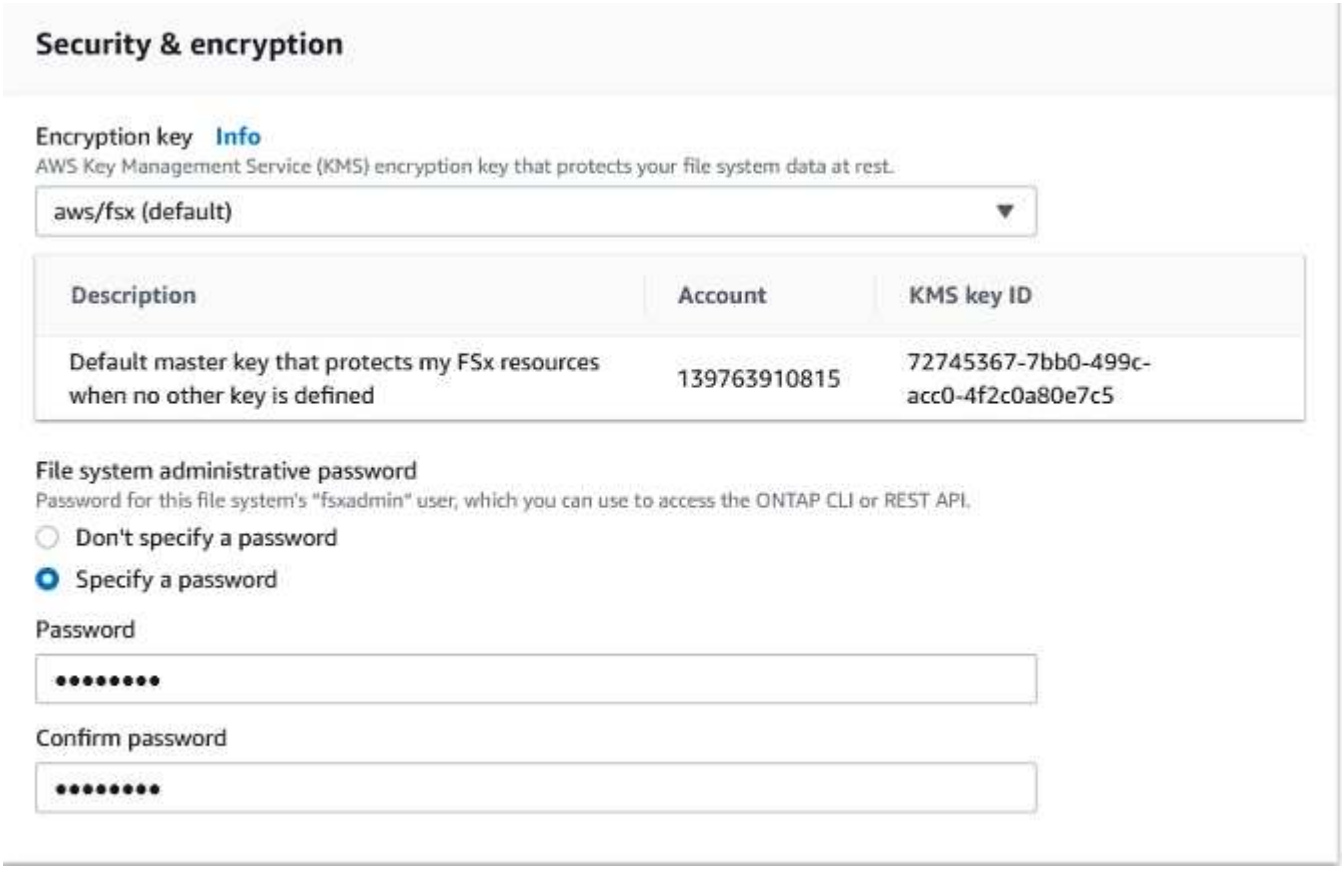


1. Na seção Rede, para Nuvem Privada Virtual (VPC), escolha a VPC apropriada e as sub-redes preferenciais, juntamente com a tabela de rotas. Neste caso, vmcfsx2.vpc é selecionado no menu suspenso.

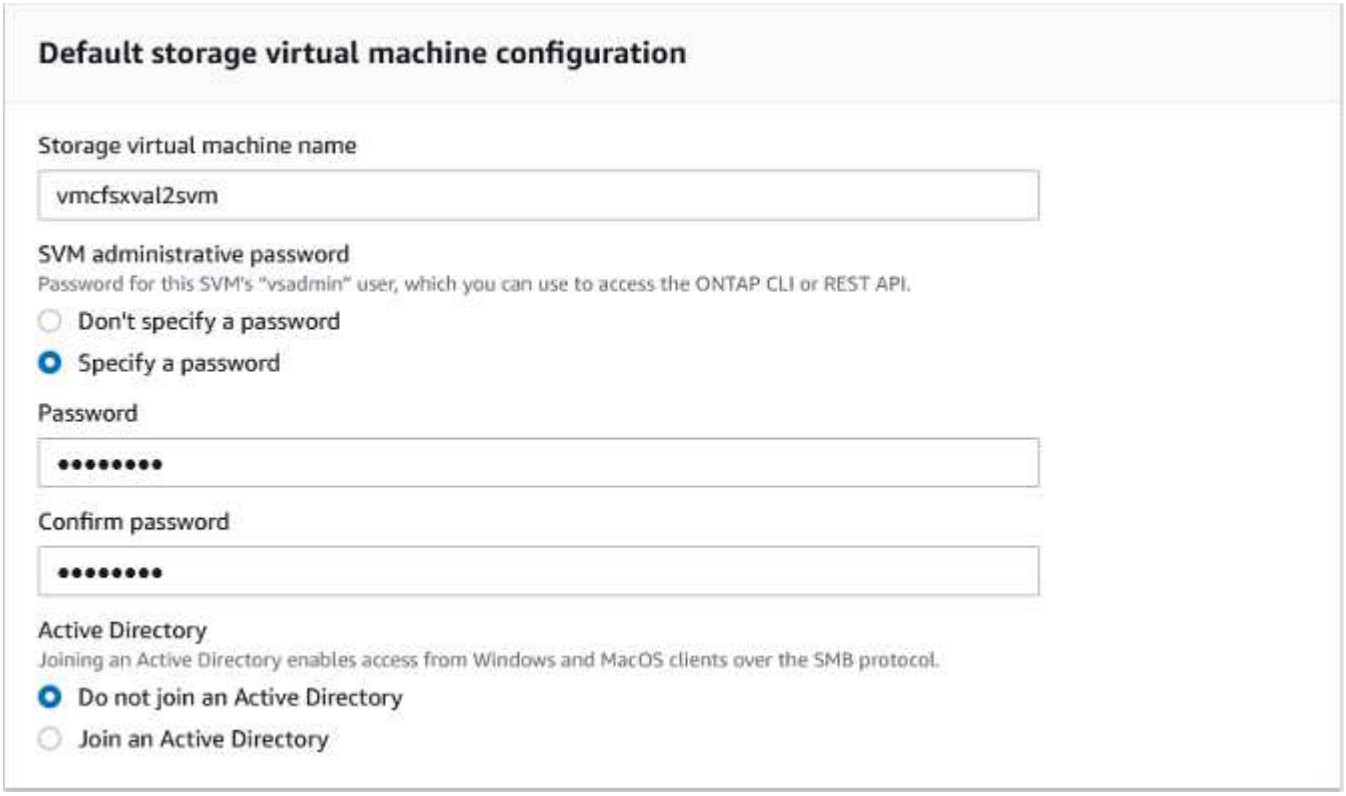


Na seção Rede, para Nuvem Privada Virtual (VPC), escolha a VPC apropriada e as sub-redes preferenciais, juntamente com a tabela de rotas. Neste caso, vmcfsx2.vpc é selecionado no menu suspenso.

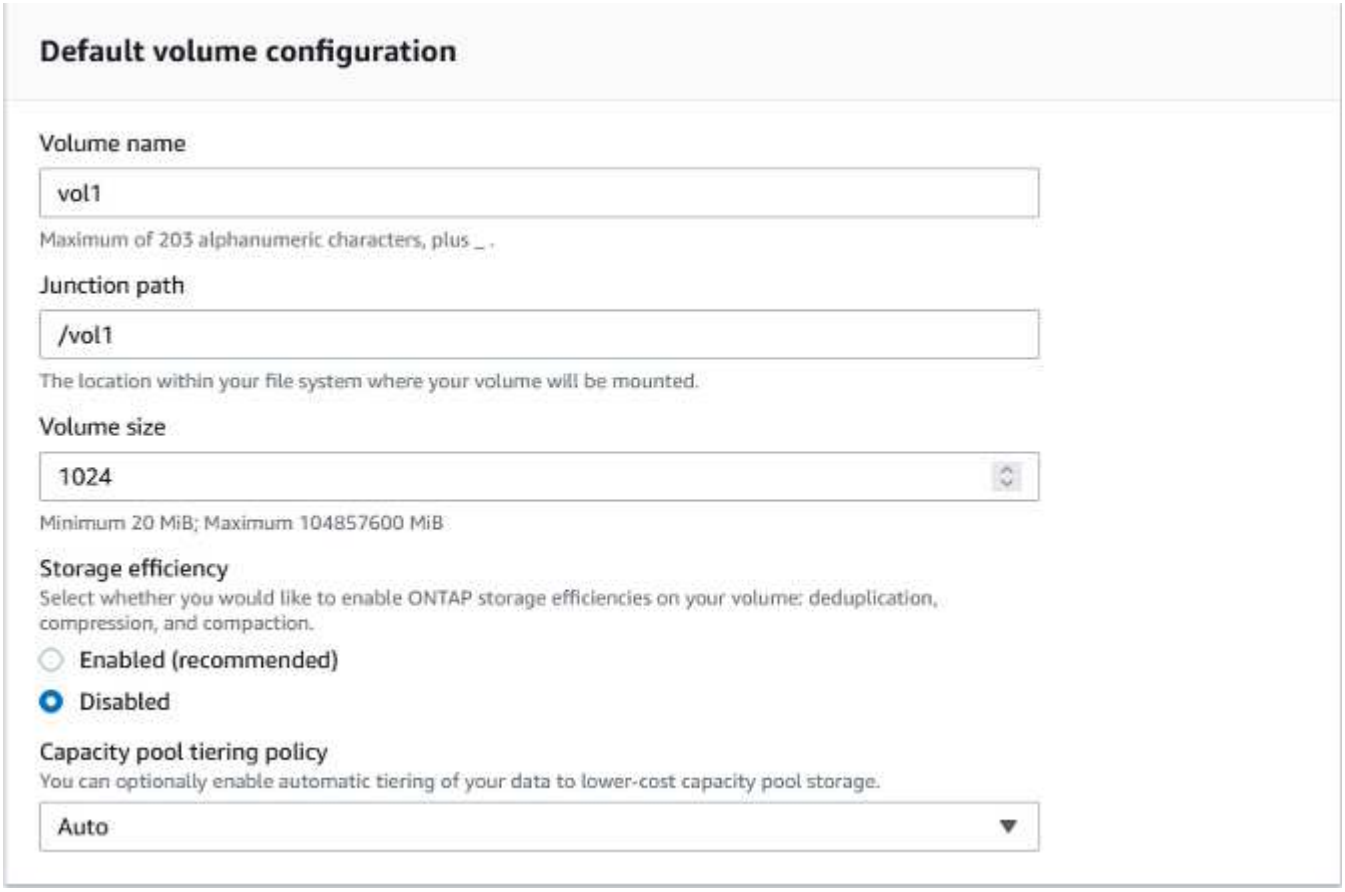
1. Na seção Segurança e Criptografia, para Chave de Criptografia, escolha a chave de criptografia do AWS Key Management Service (AWS KMS) que protege os dados em repouso do sistema de arquivos. Para a senha administrativa do sistema de arquivos, insira uma senha segura para o usuário fsxadmin.



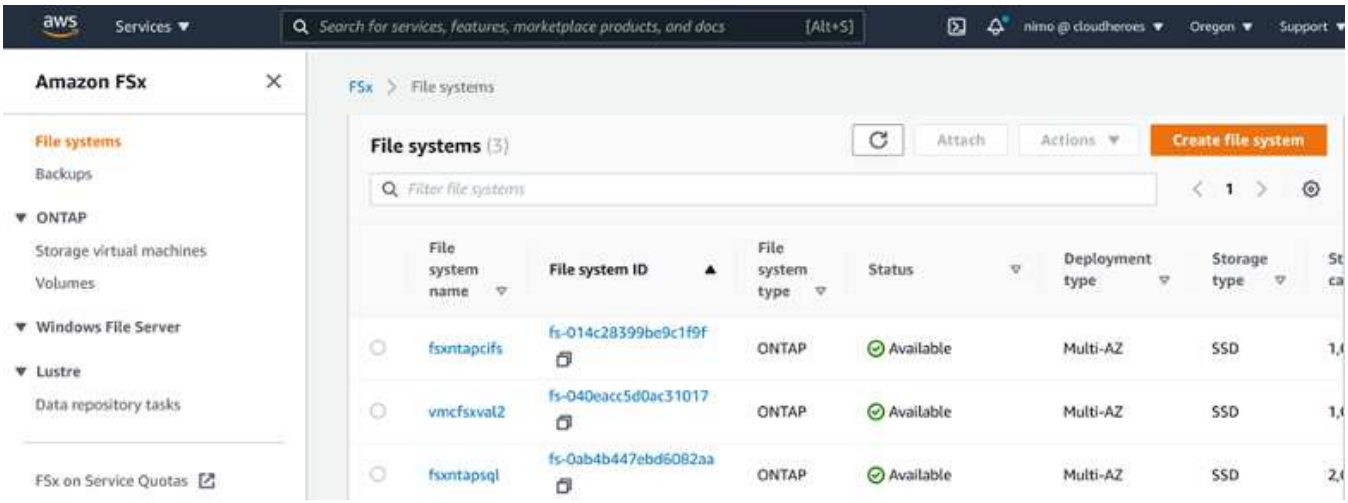
1. Na máquina virtual, especifique a senha a ser usada com vsadmin para administrar o ONTAP usando APIs REST ou a CLI. Se nenhuma senha for especificada, um usuário fsxadmin poderá ser usado para administrar o SVM. Na seção Active Directory, certifique-se de unir o Active Directory ao SVM para provisionar compartilhamentos SMB. Na seção Configuração da máquina virtual de armazenamento padrão, forneça um nome para o armazenamento nesta validação. Os compartilhamentos SMB são provisionados usando um domínio autogerenciado do Active Directory.

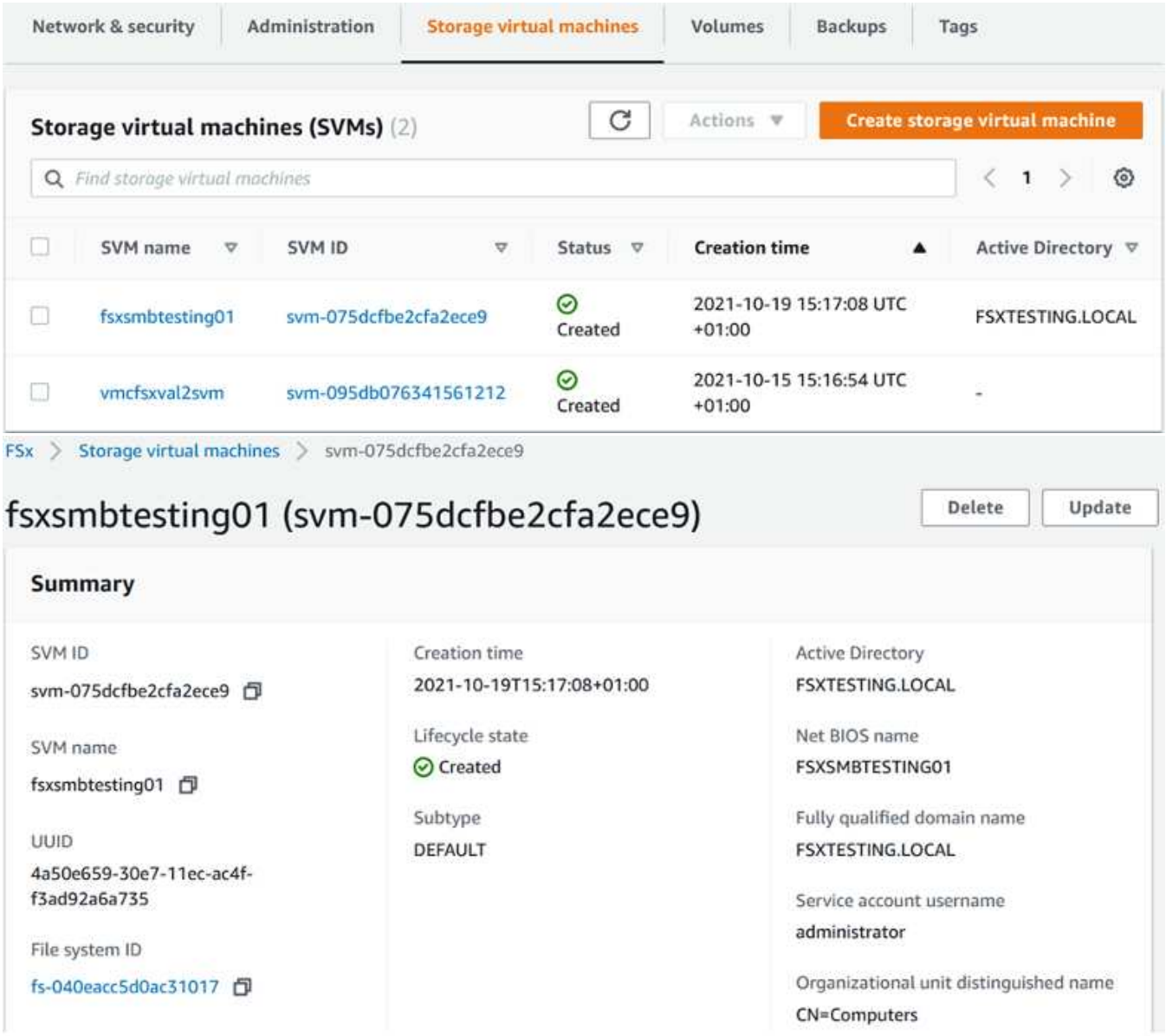


1. Na seção Configuração de volume padrão, especifique o nome e o tamanho do volume. Este é um volume NFS. Para Eficiência de armazenamento, escolha Habilitado para ativar os recursos de eficiência de armazenamento do ONTAP (compactação, desduplicação e compactação) ou Desabilitado para desativá-los.



1. Revise a configuração do sistema de arquivos mostrada na página Criar sistema de arquivos.
2. Clique em Criar sistema de arquivos.





Para obter informações mais detalhadas, consulte"Introdução ao Amazon FSx ONTAP" .

Depois que o sistema de arquivos for criado conforme acima, crie o volume com o tamanho e protocolo necessários.

1. Abra o"Console Amazon FSx" .
2. No painel de navegação esquerdo, escolha Sistemas de arquivos e, em seguida, escolha o sistema de arquivos ONTAP para o qual você deseja criar um volume.
3. Selecione a aba Volumes.
4. Selecione a aba Criar Volume.
5. A caixa de diálogo Criar volume é exibida.

Para fins de demonstração, um volume NFS é criado nesta seção e pode ser facilmente montado em VMs em execução na nuvem VMware na AWS. O nfsdemovol01 é criado conforme ilustrado abaixo:



▼ **Montar volume FSx ONTAP no cliente Linux**

Para montar o volume FSx ONTAP criado na etapa anterior a partir das VMs Linux dentro do VMC no AWS SDDC, conclua as seguintes etapas:

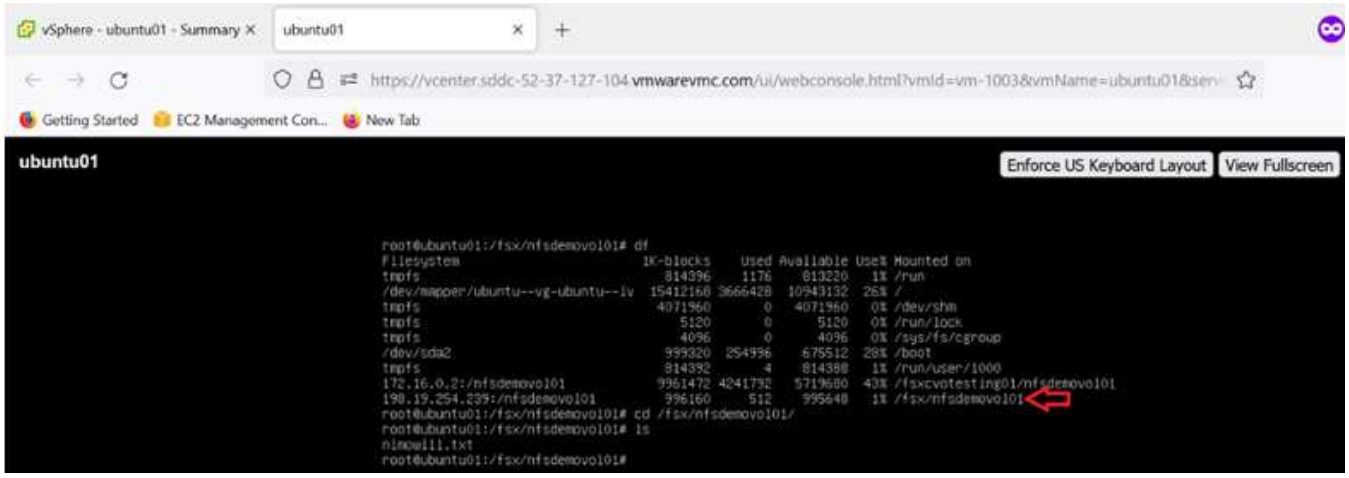
1. Conecte-se à instância Linux designada.
2. Abra um terminal na instância usando Secure Shell (SSH) e faça login com as credenciais apropriadas.
3. Crie um diretório para o ponto de montagem do volume com o seguinte comando:

```
 $ sudo mkdir /fsx/nfsdemovol01
. Monte o volume NFS do Amazon FSx ONTAP no diretório criado na etapa anterior.
```

```
sudo mount -t nfs nfsvers=4.1,198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

```
root@ubuntu01:/fsx/nfsdemovol01# mount -t nfs 198.19.254.239:/nfsdemovol01 /fsx/nfsdemovol01
```

1. Uma vez executado, execute o comando df para validar a montagem.



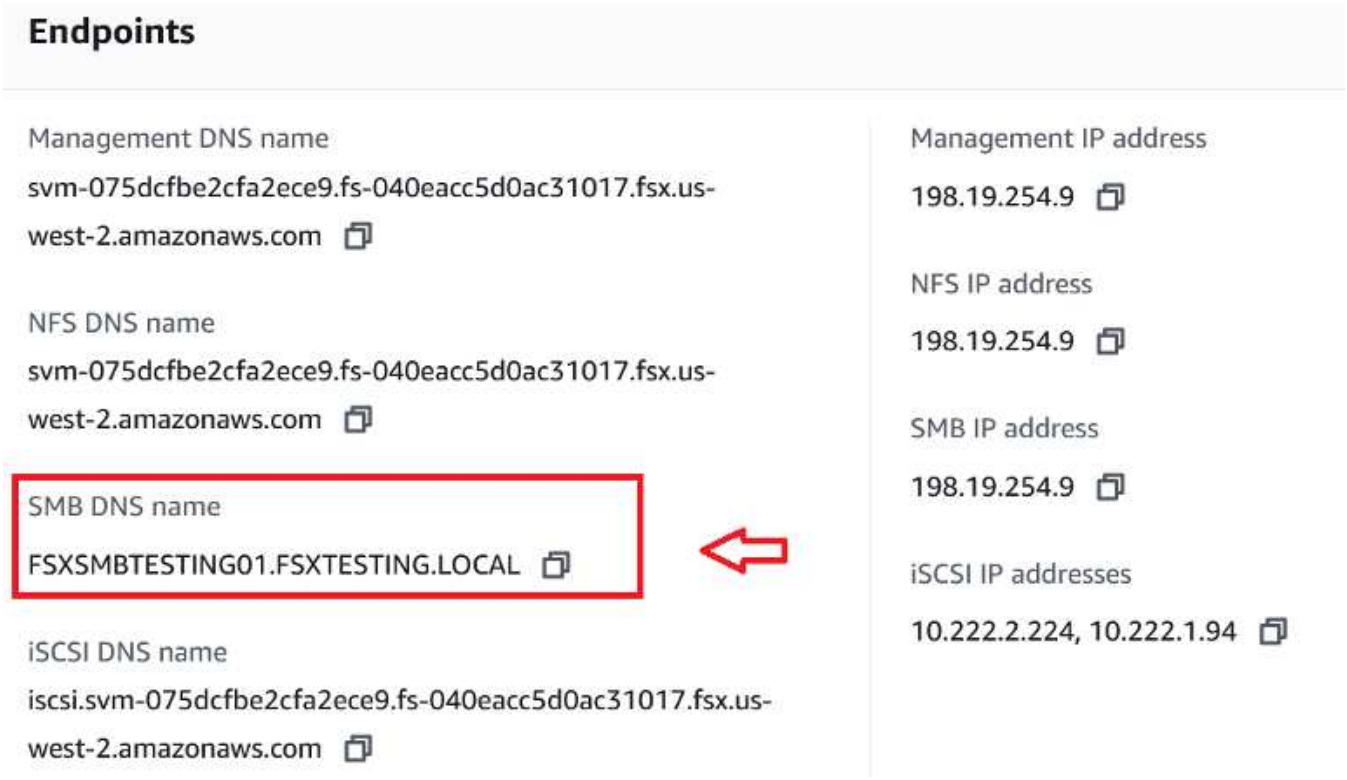
Montar volume FSx ONTAP no cliente Linux

▼ **Anexar volumes FSx ONTAP a clientes Microsoft Windows**

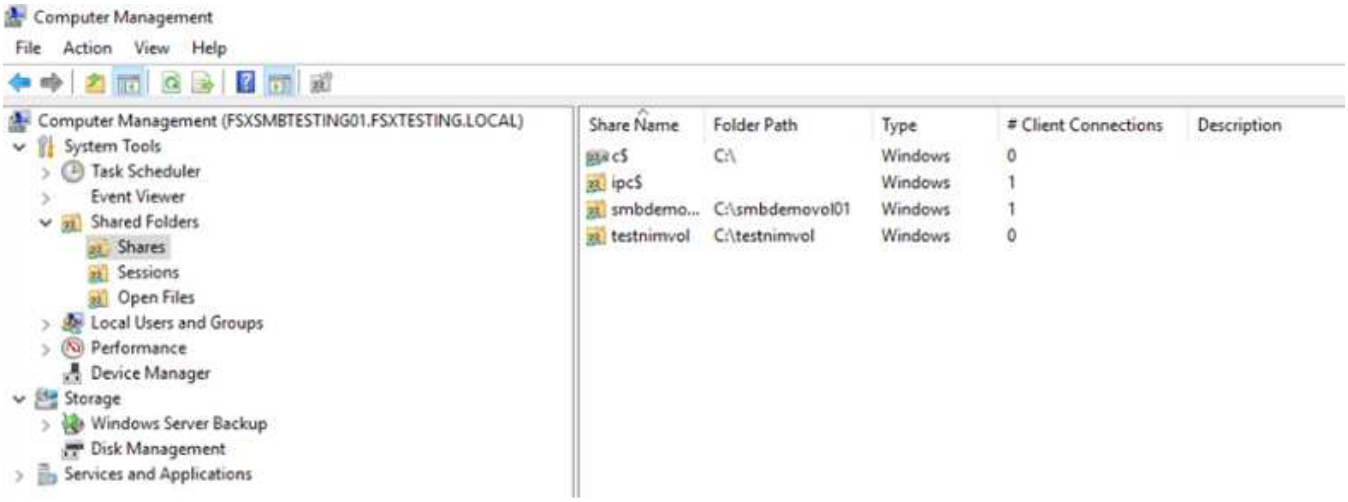
Para gerenciar e mapear compartilhamentos de arquivos em um sistema de arquivos Amazon FSx , a GUI de Pastas Compartilhadas deve ser usada.

1. Abra o menu Iniciar e execute fsmgmt.msc usando Executar como administrador. Isso abre a ferramenta GUI Pastas Compartilhadas.
2. Clique em Ação > Todas as tarefas e escolha Conectar a outro computador.
3. Para outro computador, insira o nome DNS da máquina virtual de armazenamento (SVM). Por exemplo, FSXSMBTESTING01.FSXTESTING.LOCAL é usado neste exemplo.

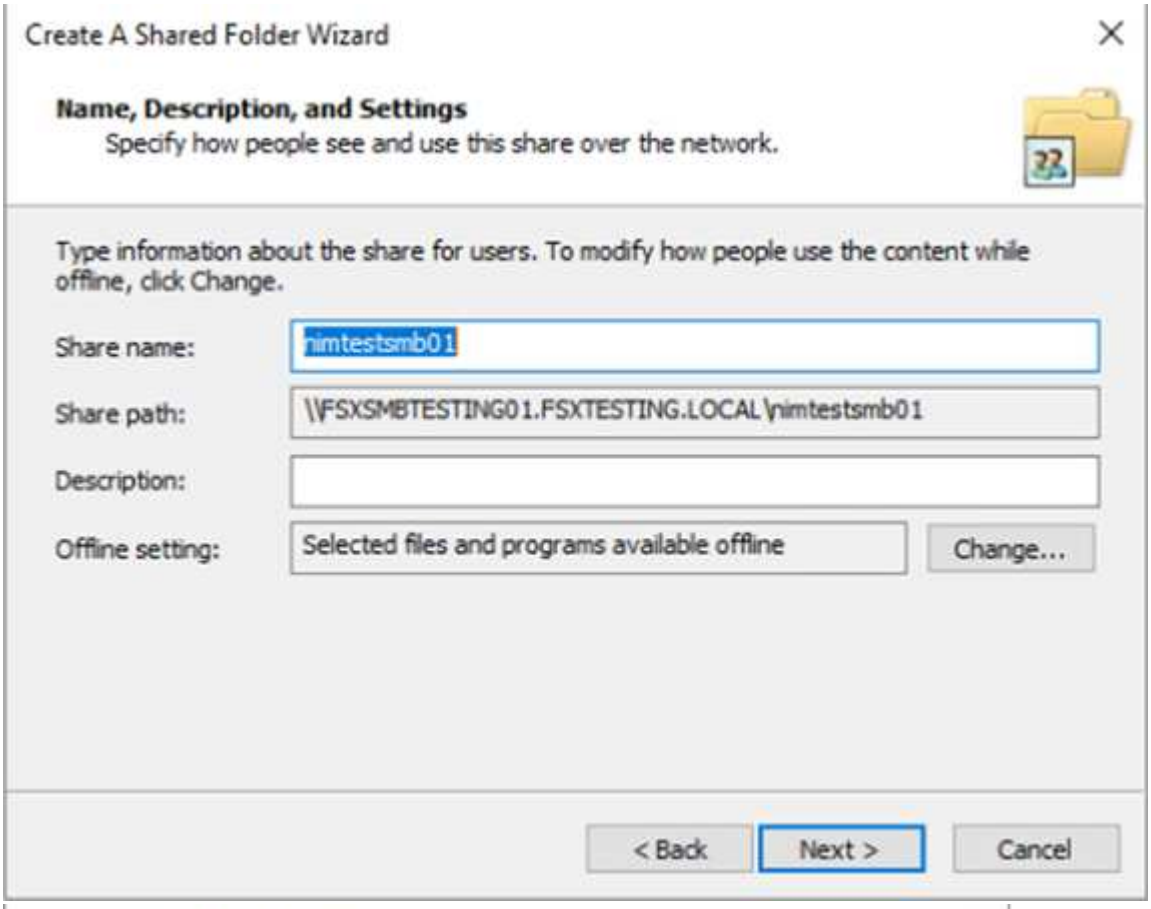
> ⓘ Para encontrar o nome DNS do SVM no console do Amazon FSx , escolha Máquinas Virtuais de Armazenamento, escolha SVM e role para baixo até Endpoints para encontrar o nome DNS do SMB. Clique em OK. O sistema de arquivos Amazon FSx aparece na lista de Pastas Compartilhadas.



1. Na ferramenta Pastas Compartilhadas, escolha Compartilhamentos no painel esquerdo para ver os compartilhamentos ativos do sistema de arquivos Amazon FSx .



1. Agora escolha um novo compartilhamento e conclua o assistente Criar uma pasta compartilhada.

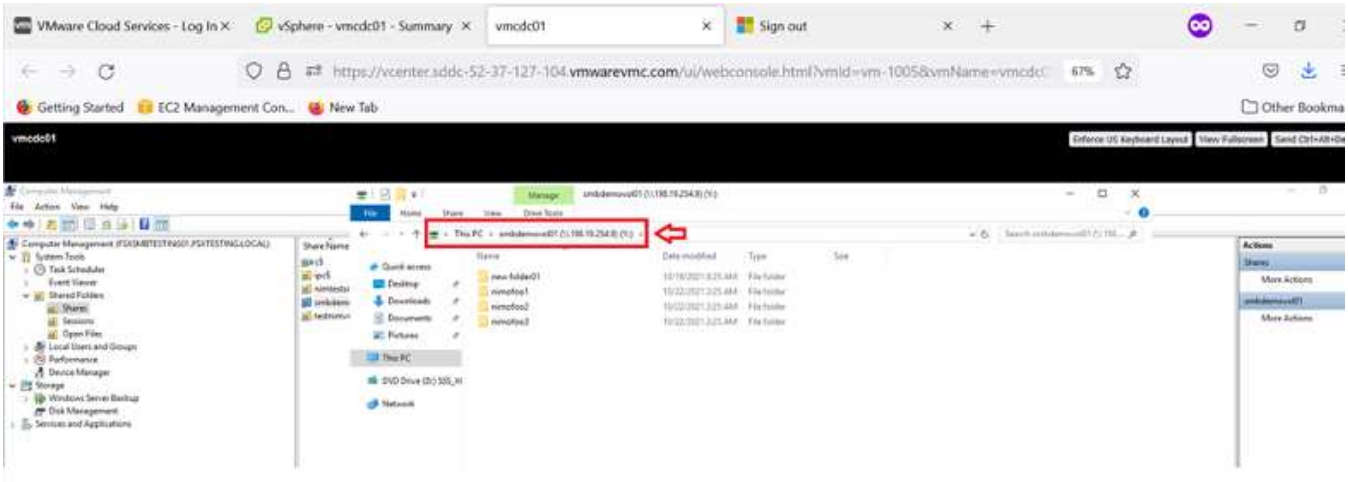




Para saber mais sobre como criar e gerenciar compartilhamentos SMB em um sistema de arquivos Amazon FSx , consulte"Criando compartilhamentos SMB" .

1. Após a conectividade estar estabelecida, o compartilhamento SMB pode ser anexado e usado para

dados do aplicativo. Para fazer isso, copie o caminho de compartilhamento e use a opção Mapear unidade de rede para montar o volume na VM em execução no VMware Cloud no AWS SDDC.



▼ **Conecte um FSx ONTAP LUN a um host usando iSCSI**

Conecte um FSx ONTAP LUN a um host usando iSCSI

O tráfego iSCSI para FSx atravessa o VMware Transit Connect/AWS Transit Gateway por meio das rotas fornecidas na seção anterior. Para configurar um LUN no Amazon FSx ONTAP, siga a documentação encontrada"aqui" .

Em clientes Linux, certifique-se de que o daemon iSCSI esteja em execução. Após o provisionamento dos LUNs, consulte as orientações detalhadas sobre a configuração do iSCSI com o Ubuntu (como exemplo)"aqui" .

Neste artigo, a conexão do iSCSI LUN a um host Windows é descrita:

▼ **Provisionar um LUN no FSx ONTAP:**

1. Acesse a CLI do NetApp ONTAP usando a porta de gerenciamento do FSx para o sistema de arquivos ONTAP .
2. Crie os LUNs com o tamanho necessário, conforme indicado pela saída de dimensionamento.

```
FsxId040eacc5d0ac31017::> lun create -vserver vmcfsxval2svm -volume
nimfsxscsivol -lun nimofsxlun01 -size 5gb -ostype windows -space
-reserve enabled
```

Neste exemplo, criamos um LUN de tamanho 5g (5368709120).

1. Crie os igroups necessários para controlar quais hosts têm acesso a LUNs específicos.

```
FsxId040eacc5d0ac31017::> igroup create -vserver vmcfsxval2svm -igroup
winIG -protocol iscsi -ostype windows -initiator iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local

FsxId040eacc5d0ac31017::> igroup show
```

```
Vserver   Igroup       Protocol OS Type  Initiators

--------- ------------ -------- --------
-----------------------------------

vmcfsxval2svm

          ubuntu01     iscsi    linux    iqn.2021-
10.com.ubuntu:01:initiator01

vmcfsxval2svm

          winIG        iscsi    windows  iqn.1991-
05.com.microsoft:vmcdc01.fsxtesting.local
```

Duas entradas foram exibidas.

1. Mapeie os LUNs para igroups usando o seguinte comando:

```
FsxId040eacc5d0ac31017::> lun map -vserver vmcfsxval2svm -path
/vol/nimfsxscsivol/nimofsxlun01 -igroup winIG

FsxId040eacc5d0ac31017::> lun show

Vserver   Path                            State   Mapped   Type
Size

--------- ------------------------------- ------- -------- --------
--------

vmcfsxval2svm

          /vol/blocktest01/lun01          online  mapped   linux
5GB

vmcfsxval2svm

          /vol/nimfsxscsivol/nimofsxlun01 online  mapped   windows
5GB
```

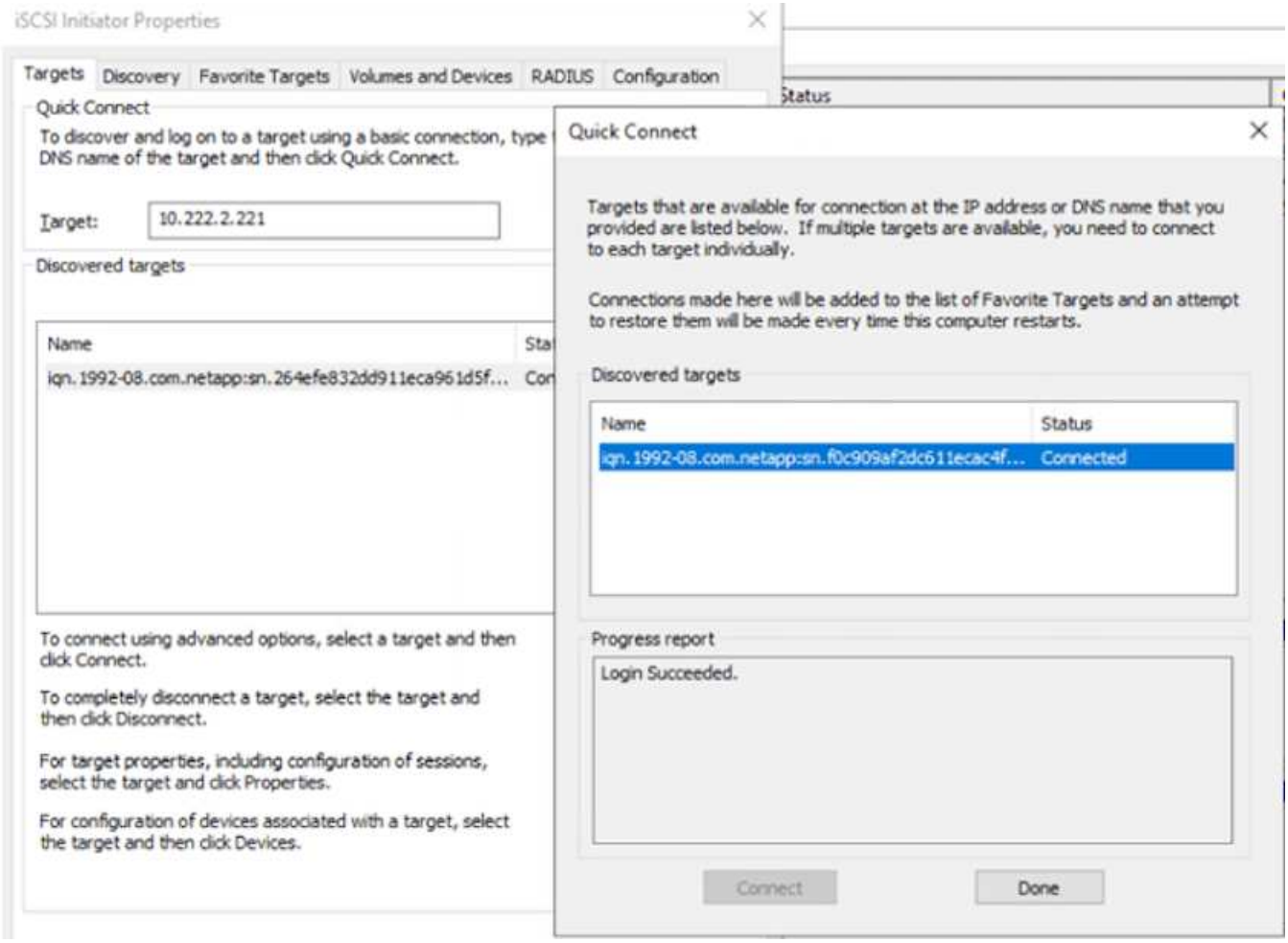
Duas entradas foram exibidas.

1. Conecte o LUN recém-provisionado a uma VM do Windows:

Para conectar o novo LUN a um host Windows residente na nuvem VMware no AWS SDDC, conclua as seguintes etapas:

1. RDP para a VM do Windows hospedada no VMware Cloud no AWS SDDC.
2. Navegue até Gerenciador do Servidor > Painel > Ferramentas > Iniciador iSCSI para abrir a caixa de diálogo Propriedades do Iniciador iSCSI.
3. Na guia Descoberta, clique em Descobrir Portal ou Adicionar Portal e insira o endereço IP da porta de destino iSCSI.
4. Na guia Destinos, selecione o alvo descoberto e clique em Fazer logon ou Conectar.
5. Selecione Habilitar multicaminho e, em seguida, selecione "Restaurar automaticamente esta conexão quando o computador iniciar" ou "Adicionar esta conexão à lista de destinos favoritos". Clique em Avançado.

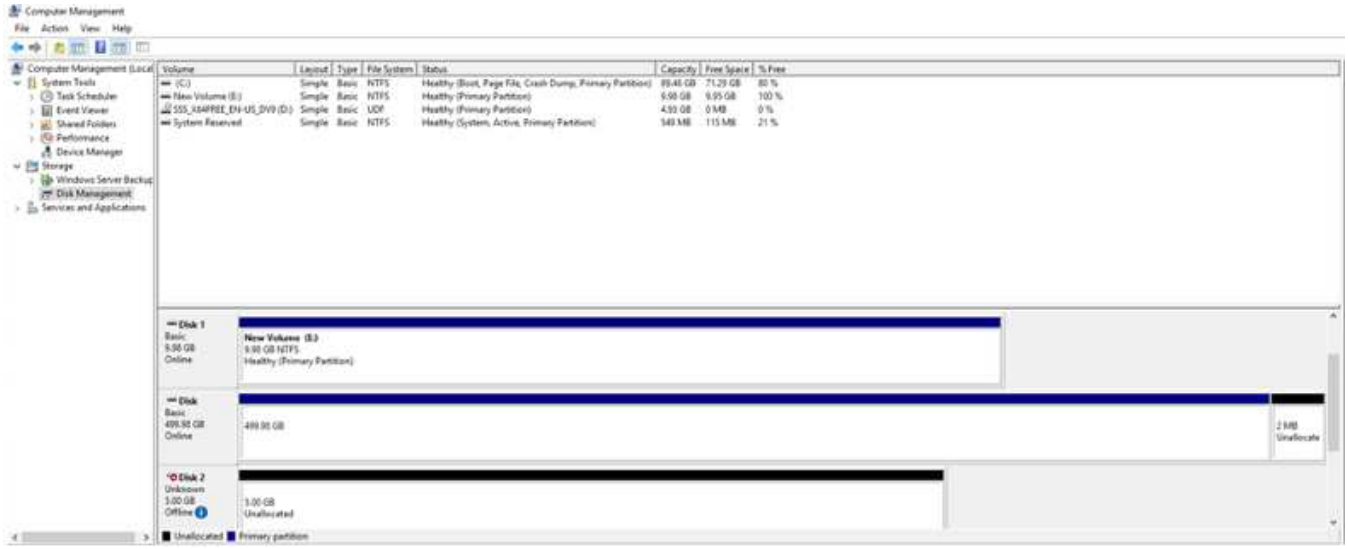
O host do Windows deve ter uma conexão iSCSI com cada nó no cluster. O DSM nativo seleciona os melhores caminhos a serem usados.



LUNs na máquina virtual de armazenamento (SVM) aparecem como discos para o host Windows. Nenhum novo disco adicionado é descoberto automaticamente pelo host. Inicie uma nova verificação manual para descobrir os discos concluindo as seguintes etapas:

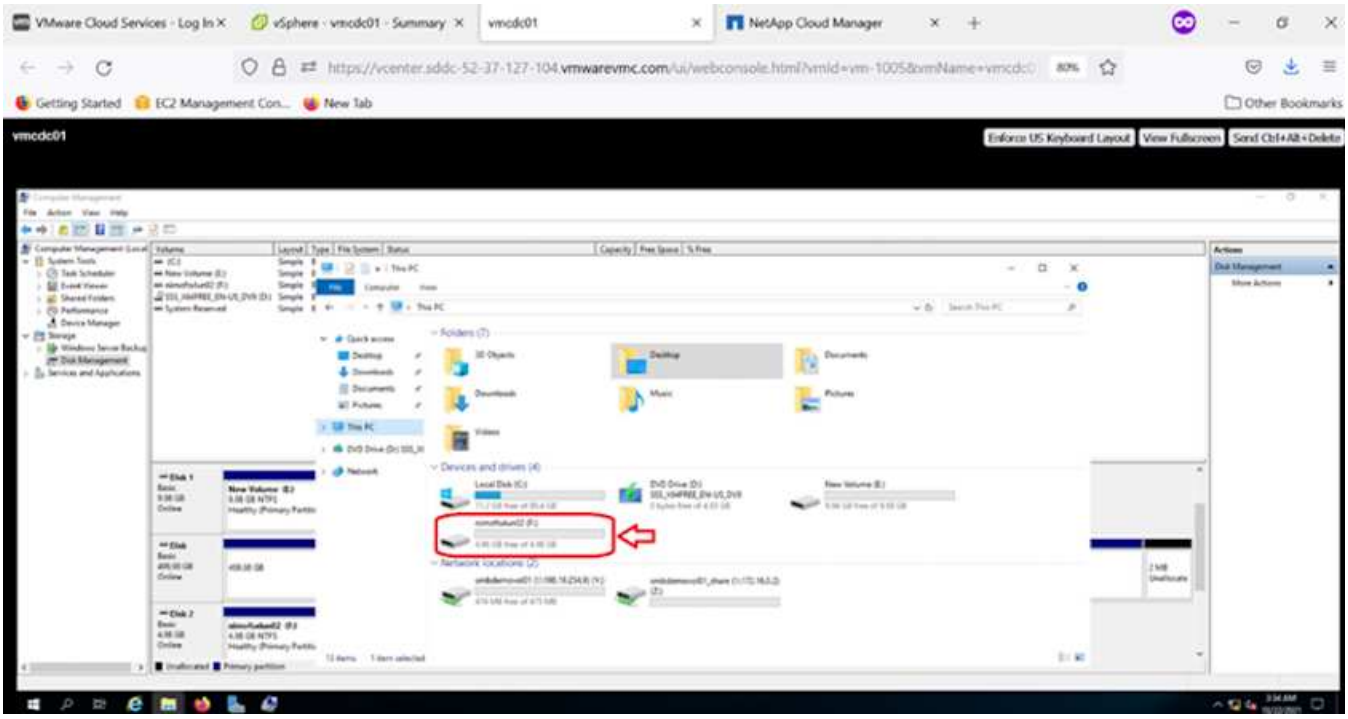
1. Abra o utilitário Gerenciamento do Computador do Windows: Iniciar > Ferramentas Administrativas > Gerenciamento do Computador.
2. Expanda o nó Armazenamento na árvore de navegação.
3. Clique em Gerenciamento de disco.

4. Clique em Ação > Reexaminar discos.



Quando um novo LUN é acessado pela primeira vez pelo host Windows, ele não tem partição ou sistema de arquivos. Inicialize o LUN e, opcionalmente, formate o LUN com um sistema de arquivos concluindo as seguintes etapas:

1. Inicie o Gerenciamento de Disco do Windows.
2. Clique com o botão direito do mouse no LUN e selecione o tipo de disco ou partição desejado.
3. Siga as instruções do assistente. Neste exemplo, a unidade F: está montada.



Cloud Volumes ONTAP (CVO)

O Cloud Volumes ONTAP, ou CVO, é a solução de gerenciamento de dados em nuvem líder do setor, desenvolvida no software de armazenamento ONTAP da NetApp, disponível nativamente na Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

É uma versão definida por software do ONTAP que consome armazenamento nativo da nuvem, permitindo que você tenha o mesmo software de armazenamento na nuvem e no local, reduzindo a necessidade de treinar novamente sua equipe de TI em métodos totalmente novos para gerenciar seus dados.

O CVO oferece aos clientes a capacidade de mover dados facilmente da borda para o data center, para a nuvem e vice-versa, reunindo sua nuvem híbrida — tudo gerenciado com um console de gerenciamento de painel único, o NetApp Cloud Manager.

Por design, o CVO oferece desempenho extremo e recursos avançados de gerenciamento de dados para satisfazer até mesmo seus aplicativos mais exigentes na nuvem

Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados

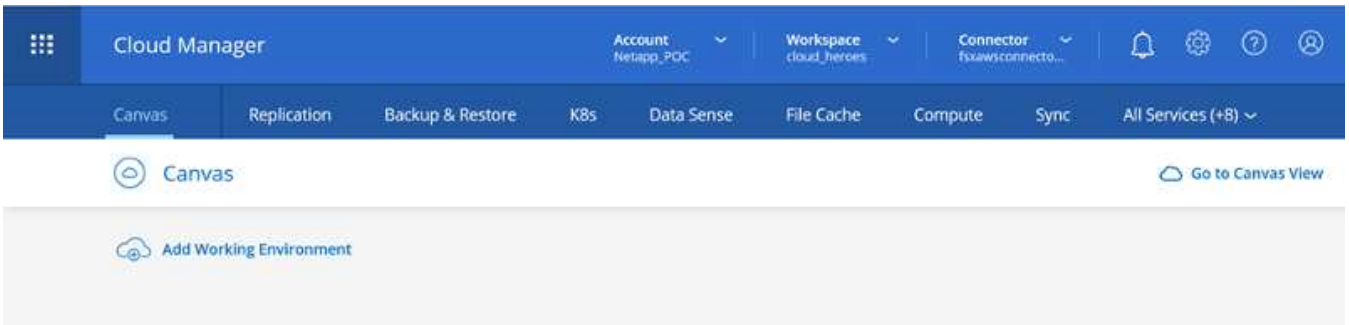
▼ **Implantar nova instância do Cloud Volumes ONTAP na AWS (faça você mesmo)**

Os compartilhamentos Cloud Volumes ONTAP podem ser montados a partir de VMs criadas no ambiente VMware Cloud on AWS SDDC. Os volumes também podem ser montados em clientes Linux Windows de VM da AWS nativa, e os LUNS podem ser acessados em clientes Linux ou Windows como dispositivos de bloco quando montados sobre iSCSI, porque o Cloud Volumes ONTAP oferece suporte aos protocolos iSCSI, SMB e NFS. Os volumes Cloud Volumes ONTAP podem ser configurados em algumas etapas simples.

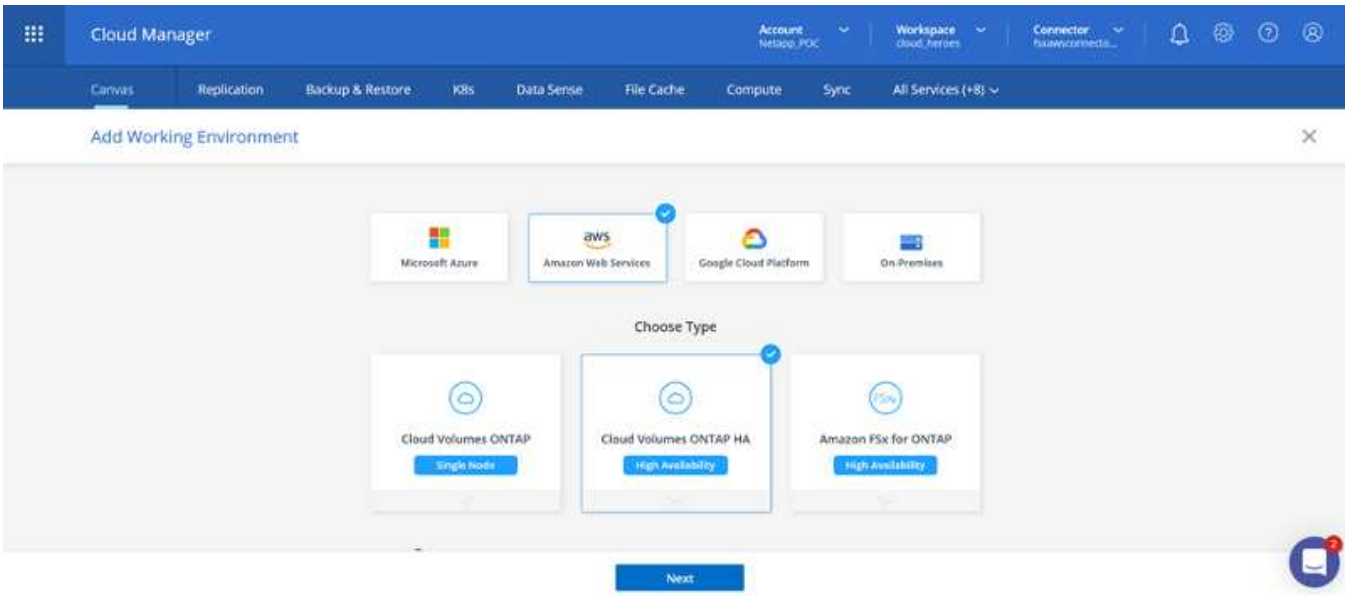
Para replicar volumes de um ambiente local para a nuvem para fins de recuperação de desastres ou migração, estabeleça conectividade de rede com a AWS, usando uma VPN site a site ou DirectConnect. A replicação de dados locais para o Cloud Volumes ONTAP está fora do escopo deste documento. Para replicar dados entre sistemas locais e Cloud Volumes ONTAP , consulte"Configurando a replicação de dados entre sistemas" .

Use a "Dimensionador Cloud Volumes ONTAP" para dimensionar com precisão as instâncias do Cloud Volumes ONTAP. Além disso, monitore o desempenho local para usar como entrada no dimensionador do Cloud Volumes ONTAP.

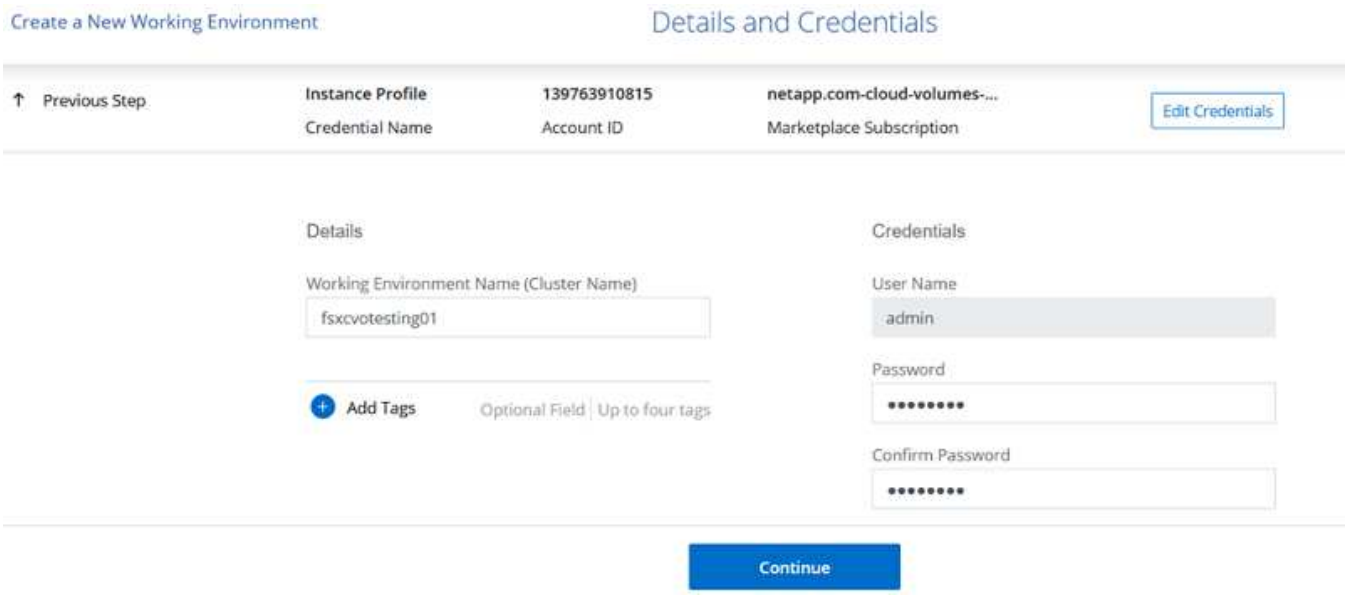
1. Efetue login no NetApp Cloud Central; a tela Fabric View é exibida. Localize a guia Cloud Volumes ONTAP e selecione Ir para o Cloud Manager. Após efetuar login, a tela Canvas será exibida.



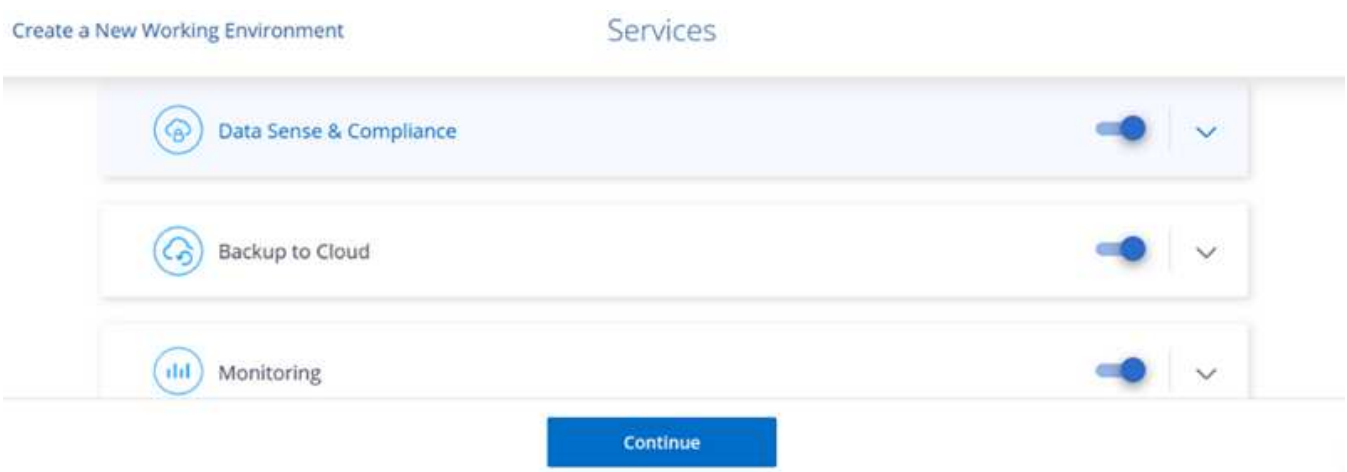
1. Na página inicial do Cloud Manager, clique em Adicionar um ambiente de trabalho e selecione AWS como a nuvem e o tipo de configuração do sistema.



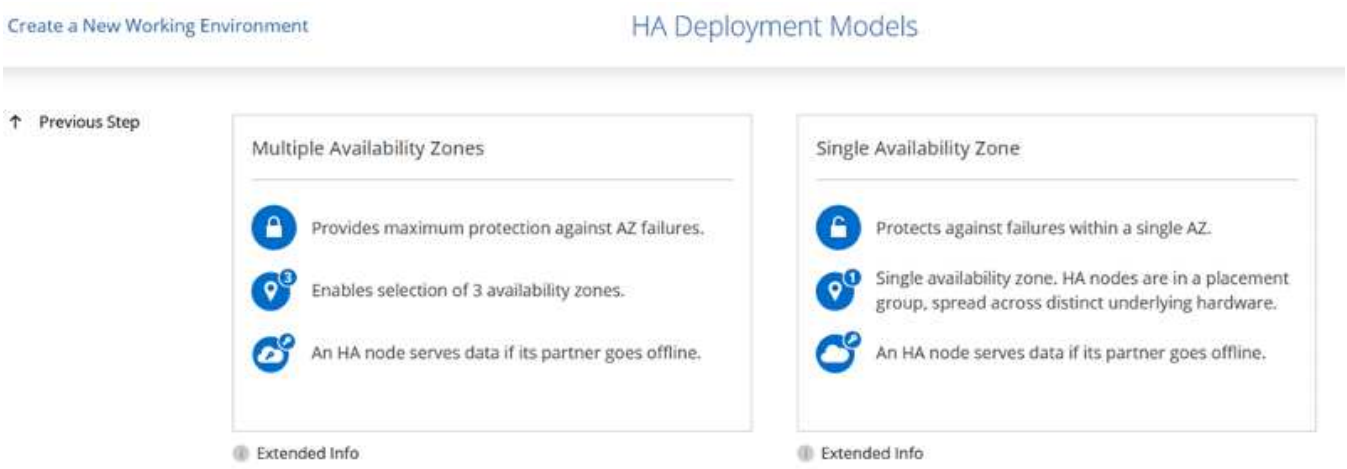
1. Forneça os detalhes do ambiente a ser criado, incluindo o nome do ambiente e as credenciais do administrador. Clique em Continuar.



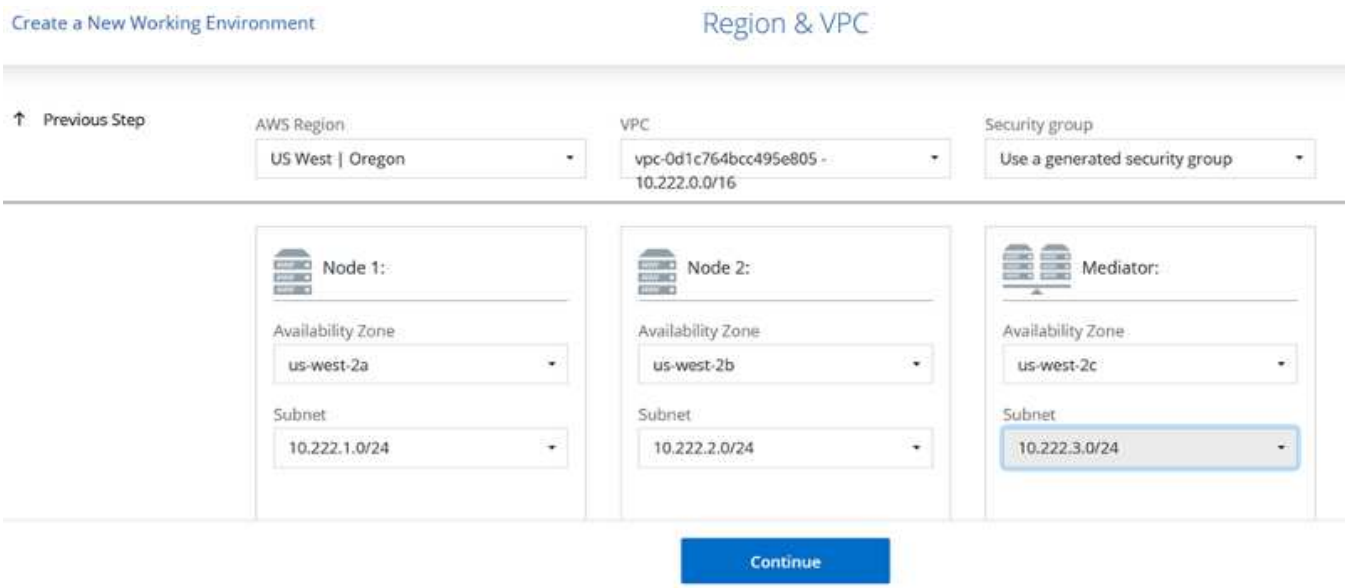
1. Selecione os serviços complementares para a implantação do Cloud Volumes ONTAP, incluindo o NetApp Data Classification, o NetApp Backup and Recovery e o Data Infrastructure Insights. Clique em Continue.



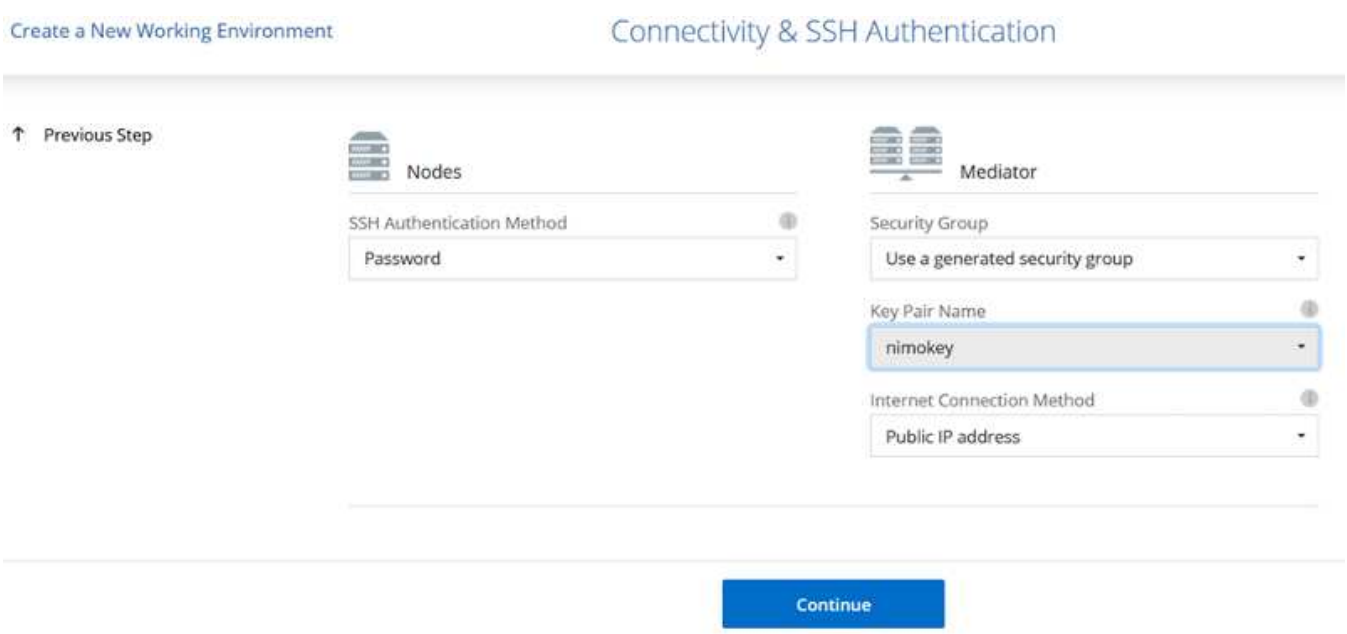
1. Na página Modelos de implantação de HA, escolha a configuração Várias zonas de disponibilidade.



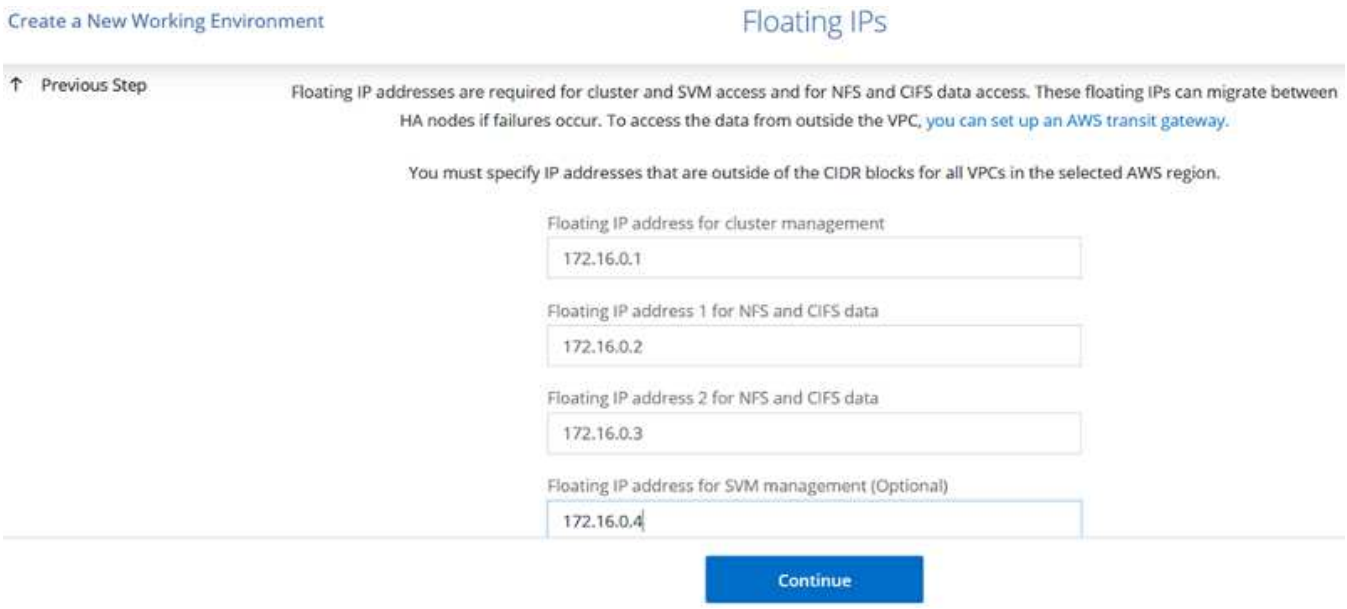
1. Na página Região e VPC, insira as informações de rede e clique em Continuar.



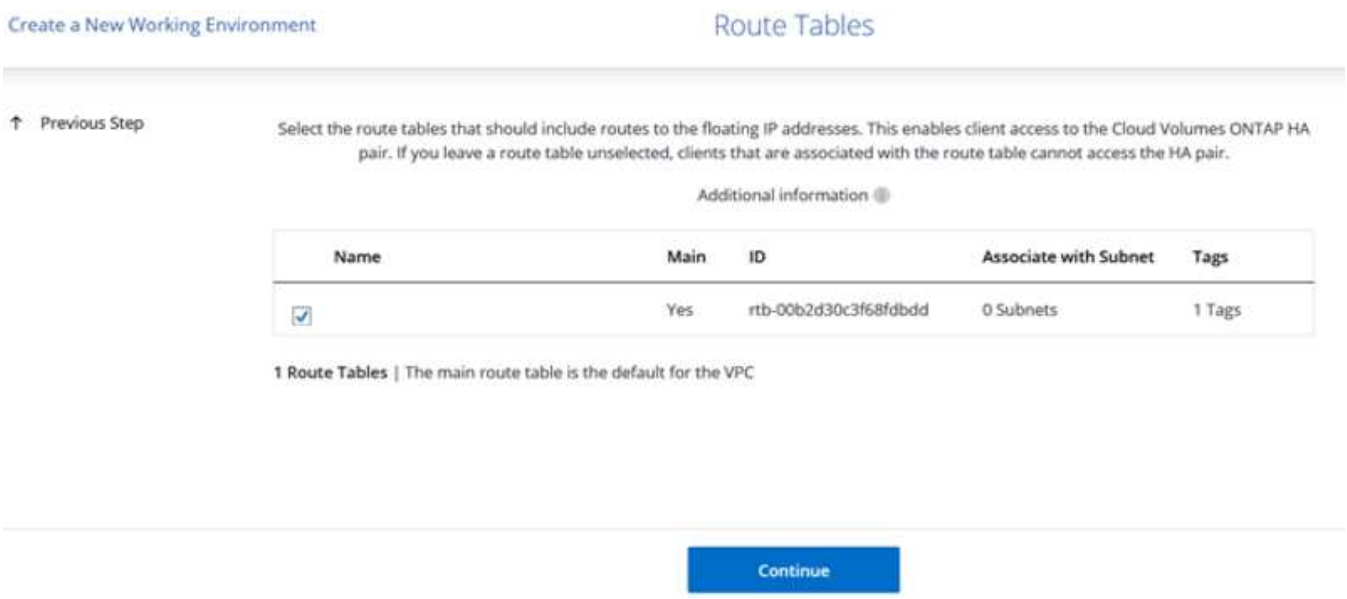
1. Na página Conectividade e Autenticação SSH, escolha os métodos de conexão para o par HA e o mediador.



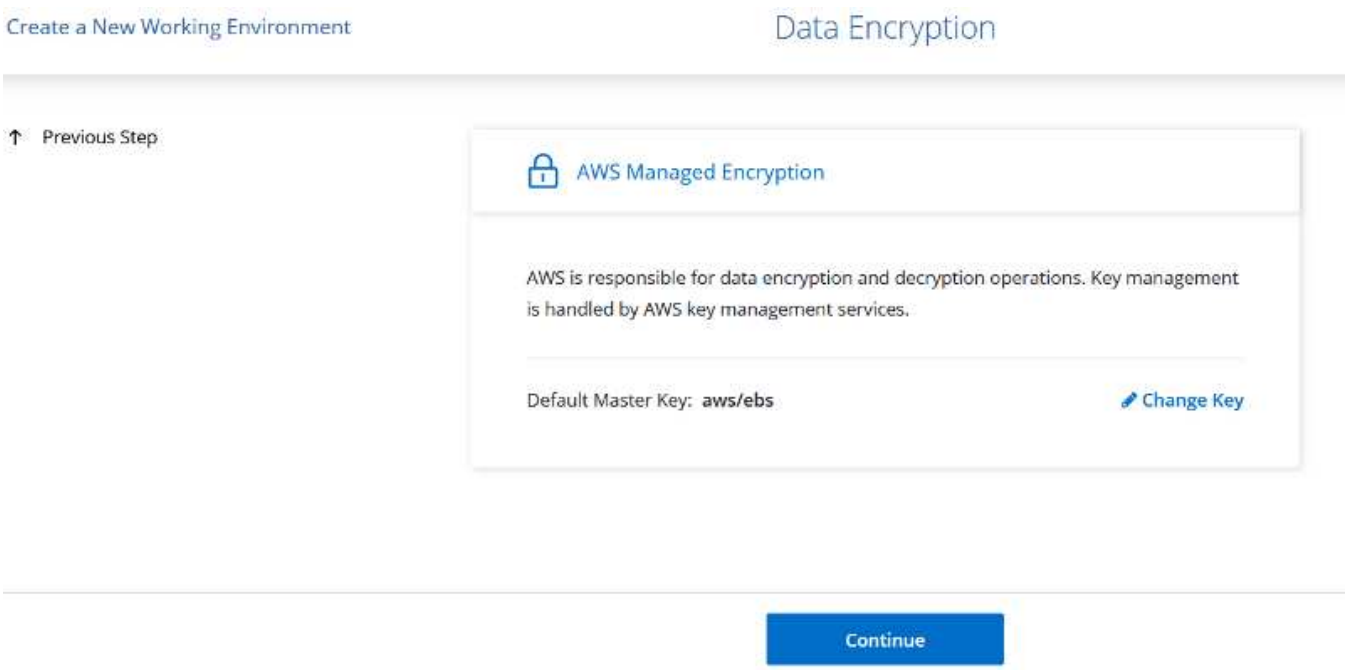
1. Especifique os endereços IP flutuantes e clique em Continuar.



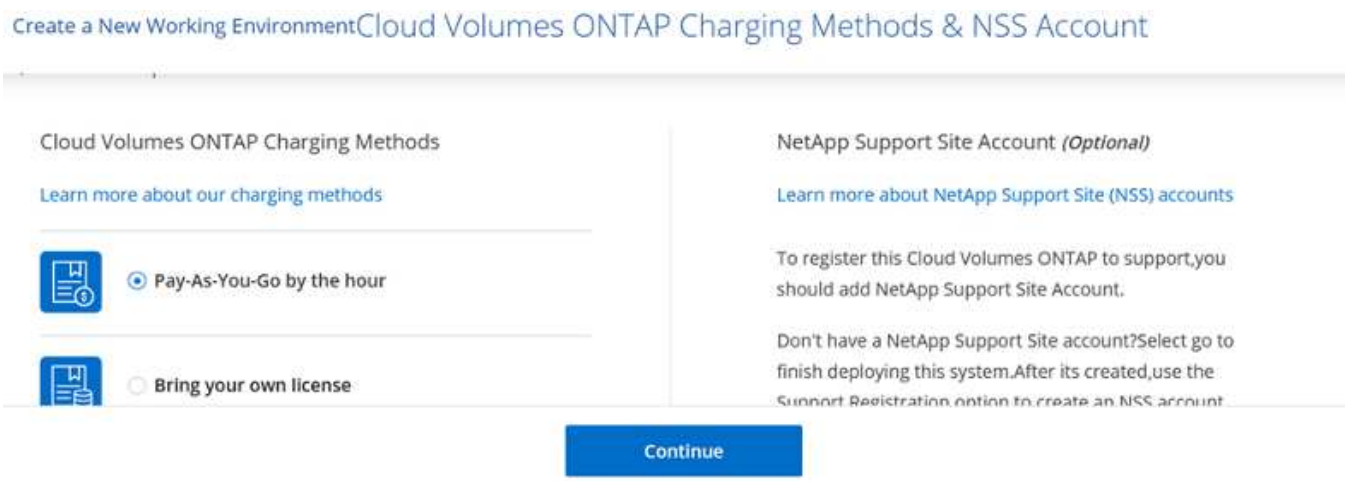
1. Selecione as tabelas de rotas apropriadas para incluir rotas para os endereços IP flutuantes e clique em Continuar.



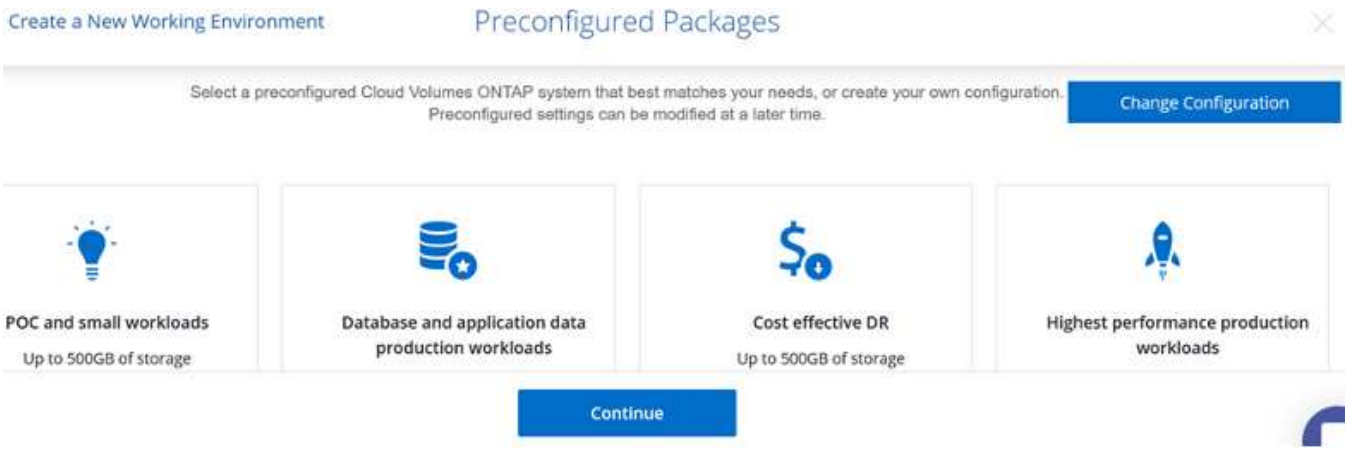
1. Na página Criptografia de dados, escolha Criptografia gerenciada pela AWS.



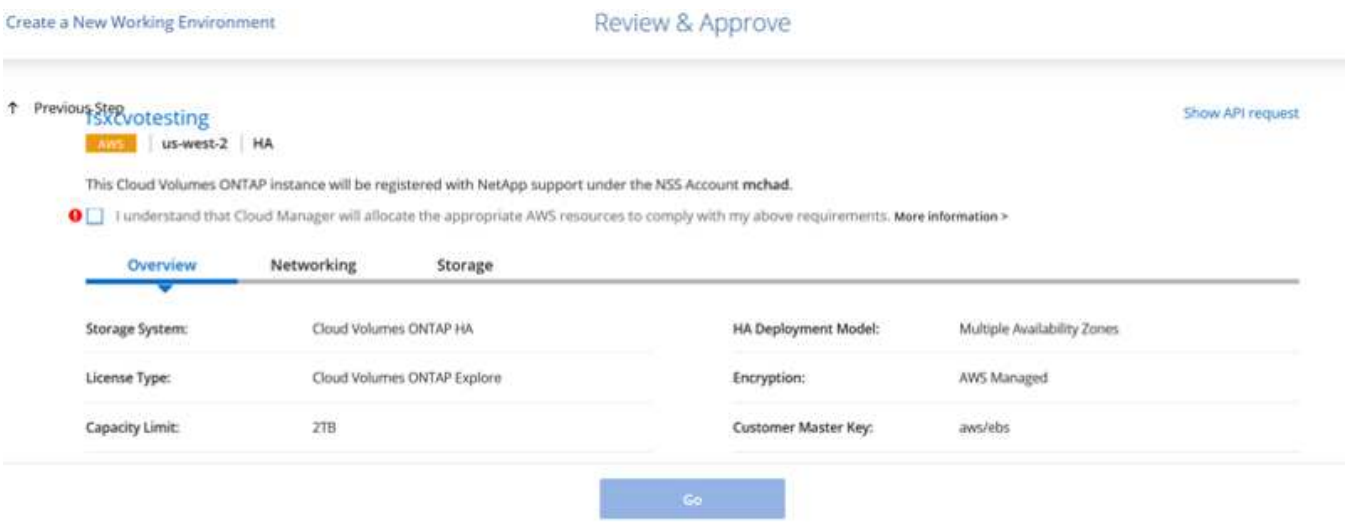
1. Selecione a opção de licença: Pague conforme o uso ou BYOL para usar uma licença existente. Neste exemplo, a opção Pague Conforme o Uso é usada.



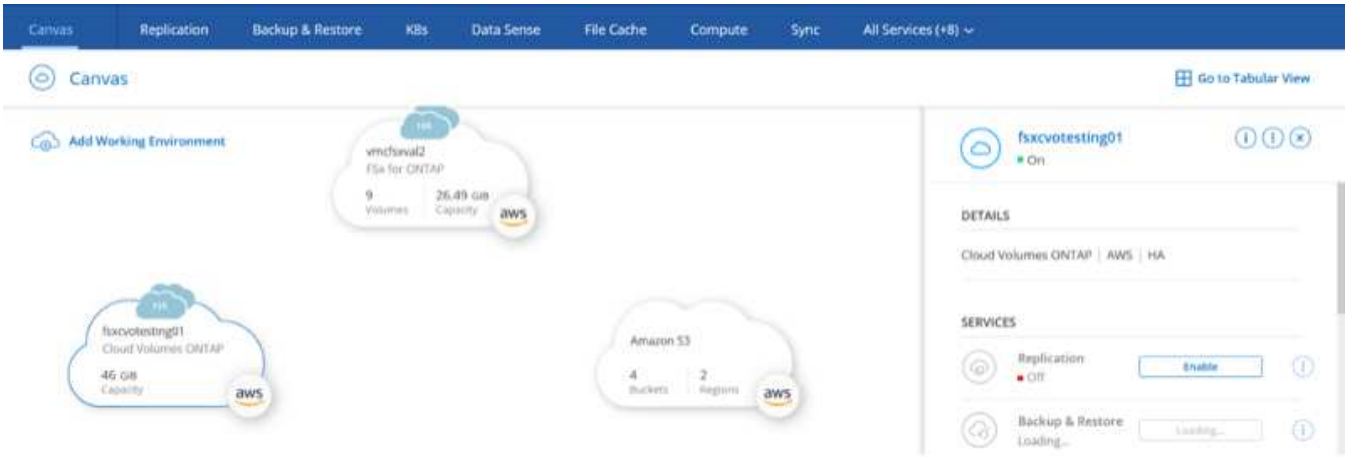
1. Selecione entre vários pacotes pré-configurados disponíveis com base no tipo de carga de trabalho a ser implantada nas VMs em execução na nuvem VMware no AWS SDDC.



1. Na página Revisar e aprovar, revise e confirme as seleções. Para criar a instância do Cloud Volumes ONTAP , clique em Ir.

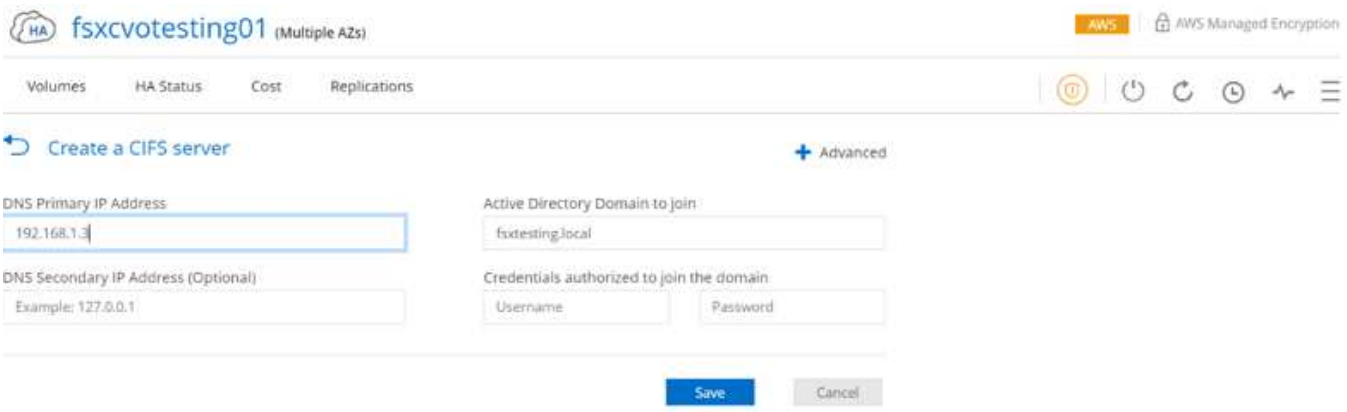


1. Depois que o Cloud Volumes ONTAP é provisionado, ele é listado nos ambientes de trabalho na página Canvas.

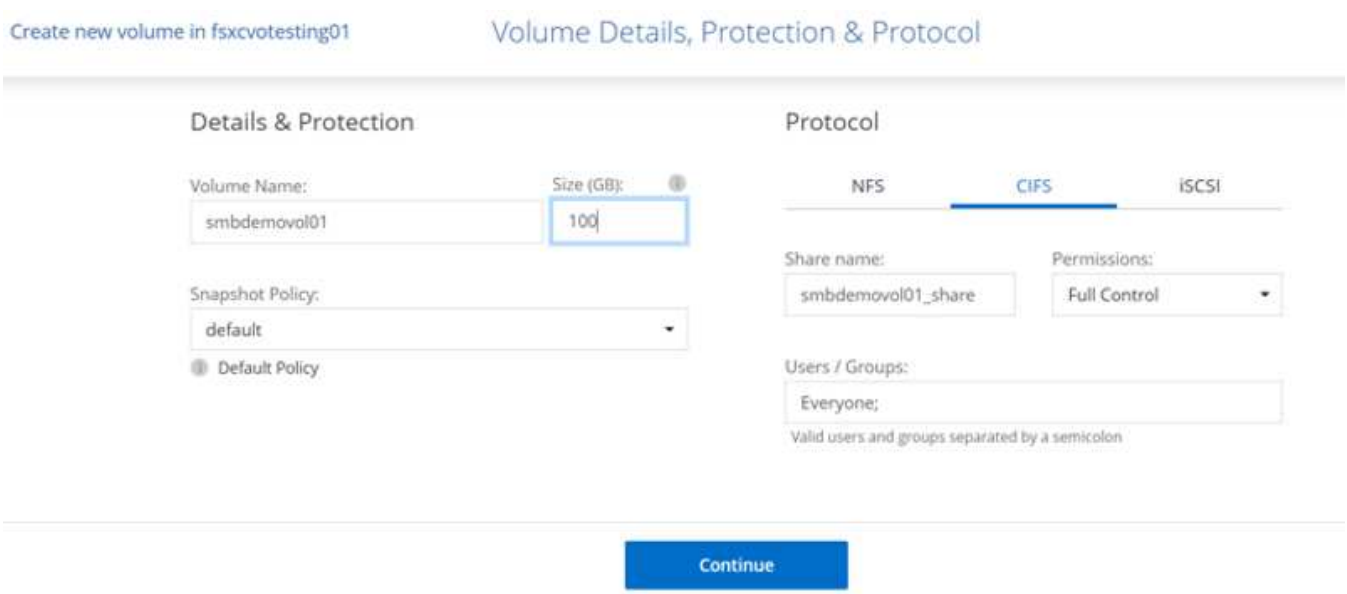


▼ **Configurações adicionais para volumes SMB**

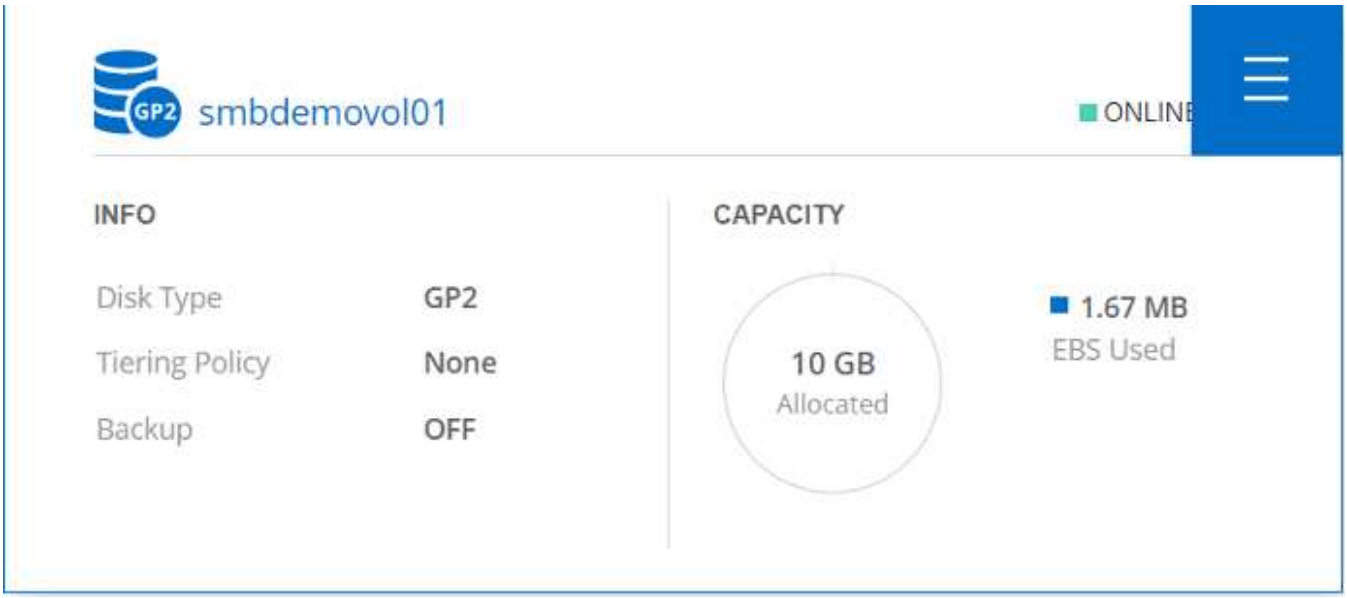
1. Depois que o ambiente de trabalho estiver pronto, certifique-se de que o servidor CIFS esteja configurado com os parâmetros de configuração de DNS e Active Directory apropriados. Esta etapa é necessária antes que você possa criar o volume SMB.



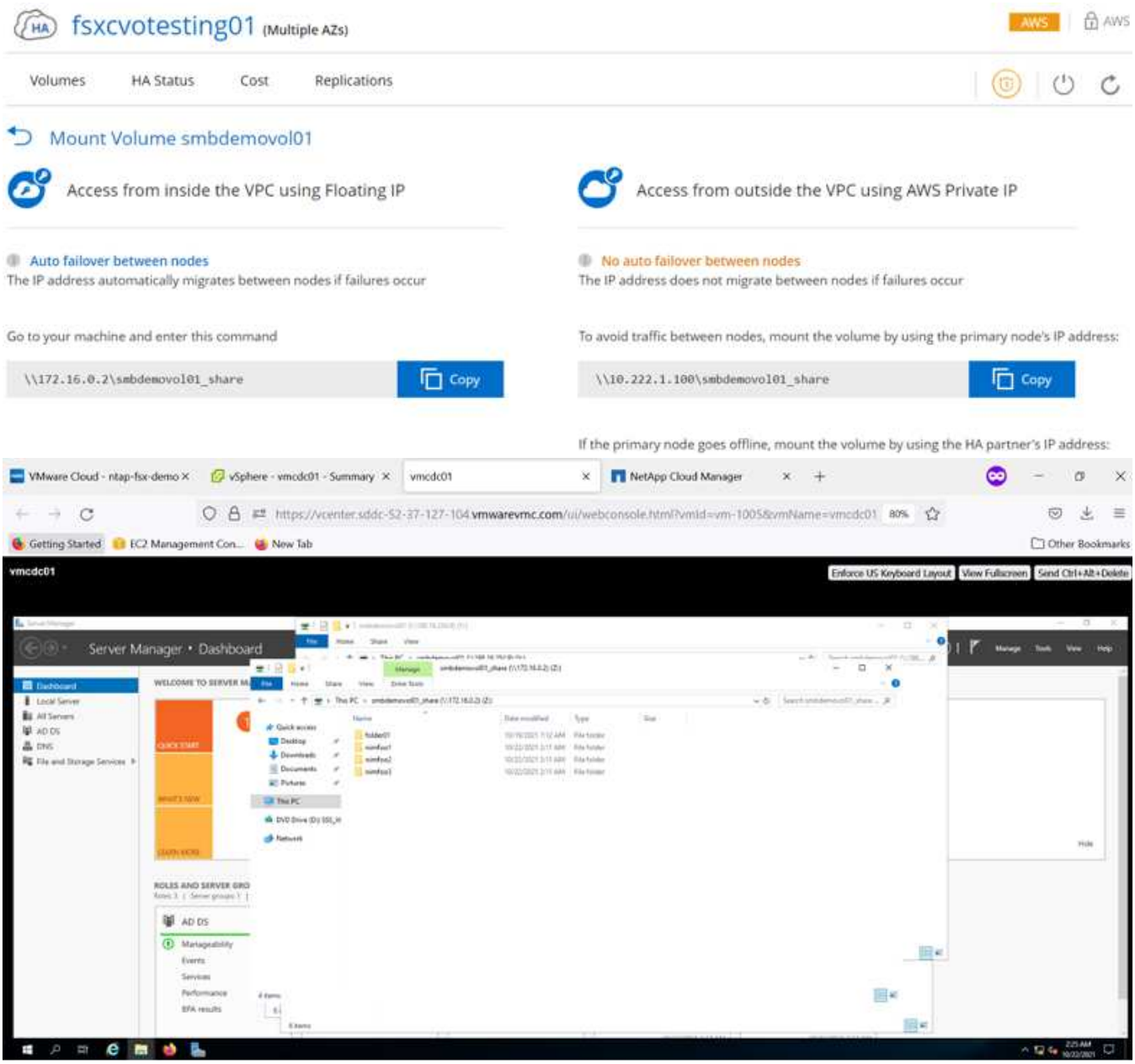
1. Selecione a instância CVO para criar o volume e clique na opção Criar Volume. Escolha o tamanho apropriado e o gerenciador de nuvem escolhe o agregado que o contém ou usa o mecanismo de alocação avançado para colocar em um agregado específico. Para esta demonstração, o SMB foi selecionado como protocolo.



1. Depois que o volume é provisionado, ele fica disponível no painel Volumes. Como um compartilhamento CIFS é provisionado, você deve dar aos seus usuários ou grupos permissão para os arquivos e pastas e verificar se esses usuários podem acessar o compartilhamento e criar um arquivo.



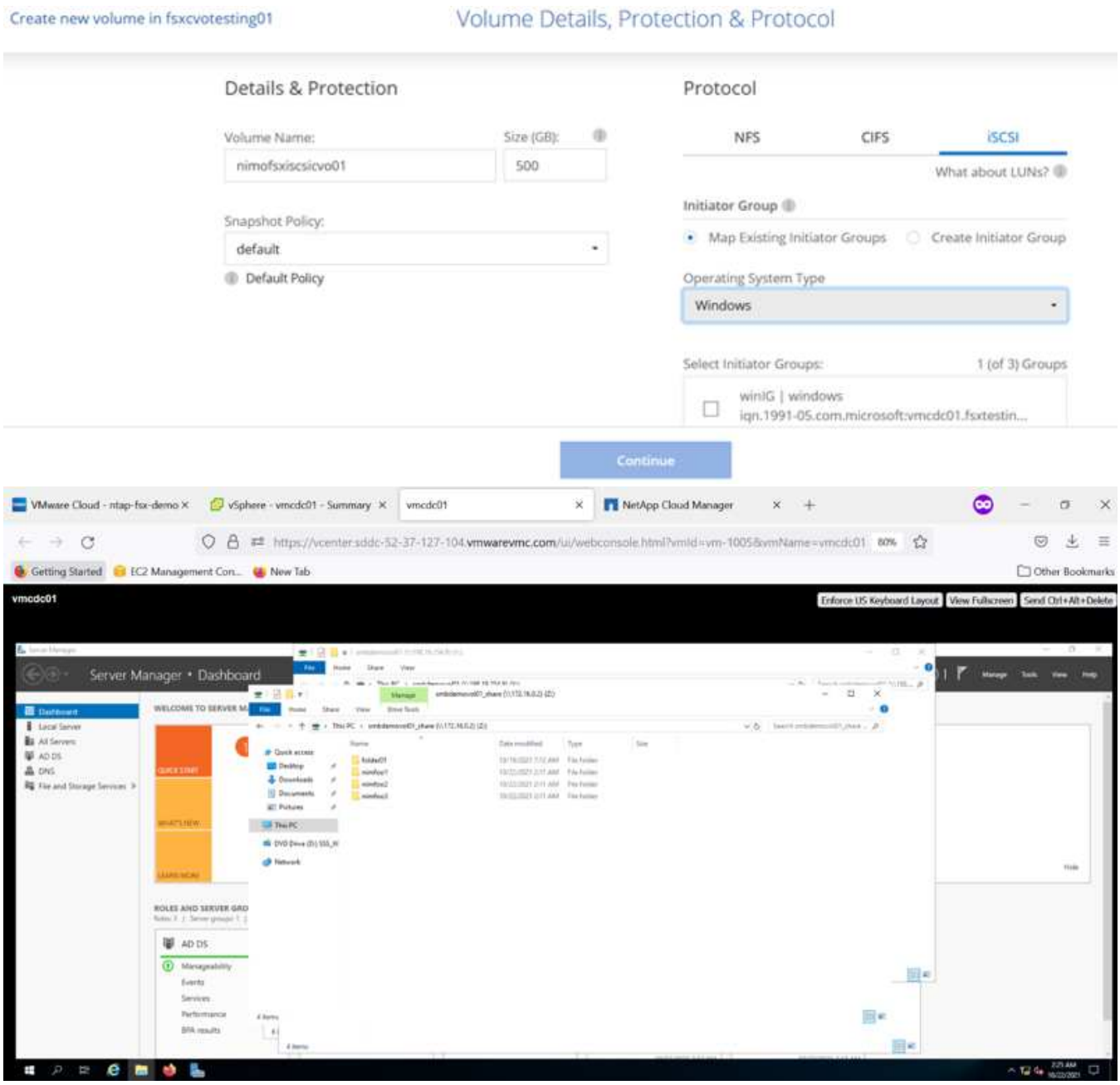
1. Após a criação do volume, use o comando mount para se conectar ao compartilhamento da VM em execução no VMware Cloud em hosts AWS SDDC.
2. Copie o caminho a seguir e use a opção Mapear unidade de rede para montar o volume na VM em execução no VMware Cloud no AWS SDDC.



▼ **Conecte o LUN a um host**

Para conectar o Cloud Volumes ONTAP LUN a um host, conclua as seguintes etapas:

1. Na página Cloud Manager Canvas, clique duas vezes no ambiente de trabalho Cloud Volumes ONTAP para criar e gerenciar volumes.
2. Clique em Adicionar volume > Novo volume, selecione iSCSI e clique em Criar grupo de iniciadores. Clique em Continuar.



1. Após o provisionamento do volume, selecione-o e clique em IQN de destino. Para copiar o Nome Qualificado iSCSI (IQN), clique em Copiar. Configure uma conexão iSCSI do host para o LUN.

Para fazer o mesmo para o host residente no VMware Cloud on AWS SDDC, conclua as seguintes etapas:

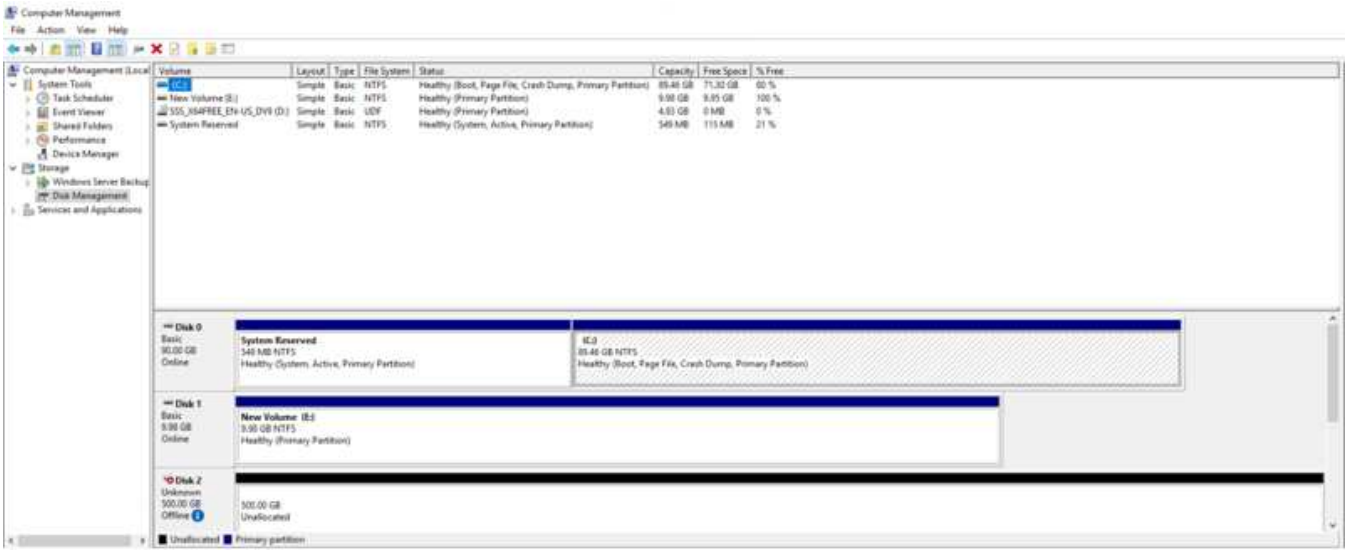
1. RDP para a VM hospedada na nuvem VMware na AWS.
2. Abra a caixa de diálogo Propriedades do Iniciador iSCSI: Gerenciador do Servidor > Painel > Ferramentas > Iniciador iSCSI.
3. Na guia Descoberta, clique em Descobrir Portal ou Adicionar Portal e insira o endereço IP da porta de destino iSCSI.
4. Na guia Destinos, selecione o alvo descoberto e clique em Fazer logon ou Conectar.
5. Selecione Habilitar multicaminho e, em seguida, selecione Restaurar automaticamente esta conexão quando o computador iniciar ou Adicionar esta conexão à lista de destinos favoritos. Clique em Avançado.

O host do Windows deve ter uma conexão iSCSI com cada nó no cluster. O DSM nativo seleciona os melhores caminhos a serem usados.



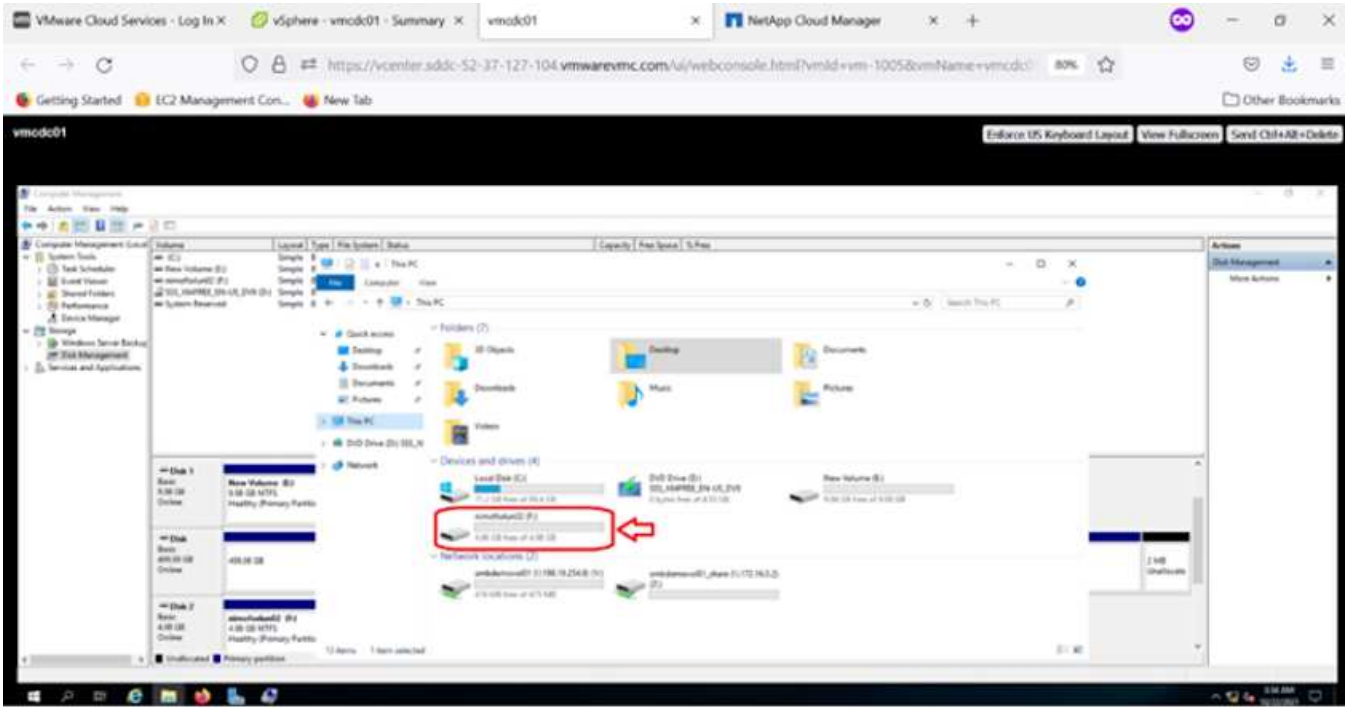
LUNs do SVM aparecem como discos para o host Windows. Nenhum novo disco adicionado é descoberto automaticamente pelo host. Inicie uma nova verificação manual para descobrir os discos concluindo as seguintes etapas:

1. Abra o utilitário Gerenciamento do Computador do Windows: Iniciar > Ferramentas Administrativas > Gerenciamento do Computador.
2. Expanda o nó Armazenamento na árvore de navegação.
3. Clique em Gerenciamento de disco.
4. Clique em Ação > Reexaminar discos.



Quando um novo LUN é acessado pela primeira vez pelo host Windows, ele não tem partição ou sistema de arquivos. Inicialize o LUN e, opcionalmente, formate o LUN com um sistema de arquivos concluindo as seguintes etapas:

1. Inicie o Gerenciamento de Disco do Windows.
2. Clique com o botão direito do mouse no LUN e selecione o tipo de disco ou partição desejado.
3. Siga as instruções do assistente. Neste exemplo, a unidade F: está montada.



Nos clientes Linux, certifique-se de que o daemon iSCSI esteja em execução. Depois que os LUNs forem provisionados, consulte as orientações detalhadas sobre a configuração do iSCSI para sua distribuição Linux. Por exemplo, a configuração iSCSI do Ubuntu pode ser encontrada"aqui" . Para verificar, execute lsblk cmd no shell.

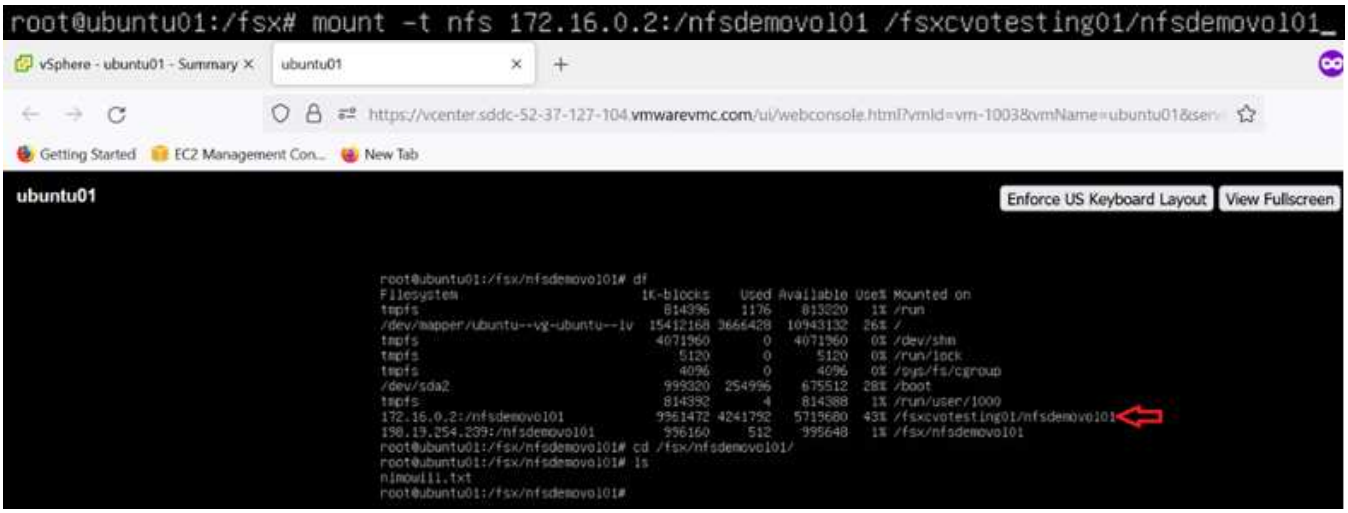
▼ **Montar Cloud Volumes ONTAP Volumes no cliente Linux**

Para montar o sistema de arquivos Cloud Volumes ONTAP (DIY) de VMs dentro do VMC no AWS SDDC, conclua as seguintes etapas:

1. Conecte-se à instância Linux designada.
2. Abra um terminal na instância usando shell seguro (SSH) e faça login com as credenciais apropriadas.
3. Crie um diretório para o ponto de montagem do volume com o seguinte comando.

```
 $ sudo mkdir /fsxcvotesting01/nfsdemovol01
. Monte o volume NFS do Amazon FSx ONTAP no diretório criado na etapa
anterior.
```

```
sudo mount -t nfs nfsvers=4.1,172.16.0.2:/nfsdemovol01
/fsxcvotesting01/nfsdemovol01
```



Serviço de Virtualização do Azure: Opções para usar o armazenamento NetApp

O armazenamento NetApp pode ser anexado ao Azure VMware Service como armazenamento conectado a convidado ou suplementar.

Azure NetApp Files (ANF) como um armazenamento de dados NFS suplementar

O suporte ao armazenamento de dados NFS foi introduzido com o ESXi versão 3 em implantações locais, o que ampliou muito os recursos de armazenamento do vSphere.

Executar o vSphere no NFS é uma opção amplamente adotada para implantações de virtualização no local porque oferece alto desempenho e estabilidade. Se você tiver um armazenamento conectado à rede (NAS) significativo em um datacenter local, considere implantar um SDDC de solução VMware no Azure com armazenamentos de dados do Azure NetApp File para superar desafios de capacidade e desempenho.

O Azure NetApp Files é criado com base no software de gerenciamento de dados NetApp ONTAP , líder do setor e altamente disponível. Os serviços do Microsoft Azure são agrupados em três categorias: básicos, principais e especializados. O Azure NetApp Files está na categoria especializada e é apoiado por hardware já implantado em muitas regiões. Com alta disponibilidade (HA) integrada, o Azure NetApp Files protege seus dados da maioria das interrupções e oferece um SLA líder do setor com 99,99% de tempo de atividade.

Para mais informações sobre o ANF como um armazenamento de dados NFS suplementar, visite:

- "ANF como um armazenamento de dados NFS suplementar: visão geral"
- "Opção suplementar de armazenamento de dados NFS no Azure"

Azure NetApp Files (ANF) como armazenamento conectado a convidados

O Azure NetApp Files traz gerenciamento e armazenamento de dados de nível empresarial para o Azure para que você possa gerenciar suas cargas de trabalho e aplicativos com facilidade. Migre suas cargas de trabalho para a nuvem e execute-as sem sacrificar o desempenho.

O Azure NetApp Files remove obstáculos para que você possa mover todos os seus aplicativos baseados em arquivos para a nuvem. Pela primeira vez, você não precisa reestruturar seus aplicativos e obtém armazenamento persistente para seus aplicativos sem complexidade.

Como o serviço é fornecido por meio do Portal do Microsoft Azure, os usuários experimentam um serviço totalmente gerenciado como parte do Contrato Corporativo da Microsoft. Suporte de classe mundial,

gerenciado pela Microsoft, lhe dá total tranquilidade. Esta solução única permite que você adicione cargas de trabalho multiprotocolo de forma rápida e fácil. Você pode criar e implantar aplicativos baseados em arquivos do Windows e do Linux, mesmo para ambientes legados.

Para mais informações, visite"ANF como armazenamento conectado para convidados" .

Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados

O Cloud Volumes ONTAP (CVO) é a solução de gerenciamento de dados em nuvem líder do setor, desenvolvida no software de armazenamento ONTAP da NetApp, disponível nativamente na Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

É uma versão definida por software do ONTAP que consome armazenamento nativo da nuvem, permitindo que você tenha o mesmo software de armazenamento na nuvem e no local, reduzindo a necessidade de treinar novamente sua equipe de TI em métodos totalmente novos para gerenciar seus dados.

O CVO oferece aos clientes a capacidade de mover dados facilmente da borda para o data center, para a nuvem e vice-versa, reunindo sua nuvem híbrida — tudo gerenciado com um console de gerenciamento de painel único, o NetApp Cloud Manager.

Por design, o CVO oferece desempenho extremo e recursos avançados de gerenciamento de dados para satisfazer até mesmo seus aplicativos mais exigentes na nuvem

Para mais informações, visite"CVO como armazenamento conectado a convidados" .

Visão geral das soluções de armazenamento de dados ANF

Toda organização bem-sucedida está em um caminho de transformação e modernização. Como parte desse processo, as empresas normalmente usam seus investimentos existentes na VMware enquanto aproveitam os benefícios da nuvem e exploram como tornar os processos de migração, expansão, extensão e recuperação de desastres o mais simples possível. Os clientes que migram para a nuvem devem avaliar os problemas de elasticidade e explosão, saída do data center, consolidação do data center, cenários de fim de vida, fusões, aquisições e assim por diante. A abordagem adotada por cada organização pode variar com base em suas respectivas prioridades de negócios. Ao escolher operações baseadas em nuvem, selecionar um modelo de baixo custo com desempenho apropriado e obstáculos mínimos é um objetivo crítico. Além de escolher a plataforma certa, a orquestração do armazenamento e do fluxo de trabalho é particularmente importante para liberar o poder da implantação e da elasticidade da nuvem.

Casos de uso

Embora a solução Azure VMware ofereça recursos híbridos exclusivos ao cliente, opções limitadas de armazenamento nativo restringiram sua utilidade para organizações com cargas de trabalho pesadas de armazenamento. Como o armazenamento está diretamente vinculado aos hosts, a única maneira de dimensioná-lo é adicionar mais hosts, o que pode aumentar os custos em 35-40% ou mais para cargas de trabalho com uso intensivo de armazenamento. Essas cargas de trabalho precisam de armazenamento adicional, não de potência adicional, mas isso significa pagar por hosts adicionais.

Vamos considerar o seguinte cenário: um cliente precisa de seis hosts para potência (vCPU/vMem), mas também tem uma necessidade substancial de armazenamento. Com base na avaliação, eles precisam de 12

hosts para atender aos requisitos de armazenamento. Isso aumenta o TCO geral porque eles precisam comprar toda essa potência adicional quando tudo o que realmente precisam é de mais armazenamento. Isso se aplica a qualquer caso de uso, incluindo migração, recuperação de desastres, bursting, desenvolvimento/teste e assim por diante.

Outro caso de uso comum do Azure VMware Solution é a recuperação de desastres (DR). A maioria das organizações não tem uma estratégia de DR infalível ou pode ter dificuldade para justificar a execução de um data center fantasma apenas para DR. Os administradores podem explorar opções de DR de pegada zero com um cluster piloto ou um cluster sob demanda. Eles poderiam então dimensionar o armazenamento sem adicionar hosts adicionais, o que pode ser uma opção atraente.

Então, para resumir, os casos de uso podem ser classificados de duas maneiras:

- Escalonamento da capacidade de armazenamento usando armazenamentos de dados ANF
- Usando datastores ANF como um destino de recuperação de desastres para um fluxo de trabalho de recuperação otimizado em termos de custo, no local ou em regiões do Azure entre os datacenters definidos por software (SDDCs). Este guia fornece insights sobre o uso do Azure NetApp Files para fornecer armazenamento otimizado para datastores (atualmente em versão prévia pública), juntamente com os melhores recursos de proteção de dados e DR em uma solução Azure VMware, o que permite que você descarregue a capacidade de armazenamento do armazenamento vSAN.



Entre em contato com os arquitetos de soluções da NetApp ou da Microsoft em sua região para obter informações adicionais sobre o uso de armazenamentos de dados ANF.

Opções do VMware Cloud no Azure

Solução VMware do Azure

O Azure VMware Solution (AVS) é um serviço de nuvem híbrida que fornece SDDCs VMware totalmente funcionais dentro de uma nuvem pública do Microsoft Azure. O AVS é uma solução própria totalmente gerenciada e suportada pela Microsoft e verificada pela VMware que usa a infraestrutura do Azure. Portanto, os clientes obtêm o VMware ESXi para virtualização de computação, o vSAN para armazenamento hiperconvergente e o NSX para rede e segurança, tudo isso enquanto aproveitam a presença global do Microsoft Azure, as instalações de data center líderes da categoria e a proximidade com o rico ecossistema de serviços e soluções nativos do Azure. Uma combinação do Azure VMware Solution SDDC e do Azure NetApp Files proporciona o melhor desempenho com latência de rede mínima.

Independentemente da nuvem usada, quando um SDDC da VMware é implantado, o cluster inicial inclui os seguintes componentes:

- Hosts VMware ESXi para virtualização de computação com um dispositivo de servidor vCenter para gerenciamento.
- Armazenamento hiperconvergente VMware vSAN incorporando os ativos de armazenamento físico de cada host ESXi.
- VMware NSX para rede virtual e segurança com um cluster NSX Manager para gerenciamento.

Conclusão

Não importa se você está visando a nuvem híbrida ou totalmente em nuvem, os arquivos do Azure NetApp oferecem excelentes opções para implantar e gerenciar cargas de trabalho de aplicativos junto com serviços de arquivo, ao mesmo tempo em que reduzem o TCO ao tornar os requisitos de dados integrados à camada de aplicativo. Seja qual for o caso de uso, escolha o Azure VMware Solution juntamente com o Azure NetApp Files para obter rapidamente os benefícios da nuvem, infraestrutura consistente e operações no local e em

várias nuvens, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial. É o mesmo processo e procedimento familiar usado para conectar o armazenamento. Lembre-se de que foi apenas a posição dos dados que mudou junto com os novos nomes; as ferramentas e os processos permanecem os mesmos, e o Azure NetApp Files ajuda a otimizar a implantação geral.

Takeaways

Os pontos principais deste documento incluem:

- Agora você pode usar o Azure NetApp Files como um armazenamento de dados no AVS SDDC.
- Aumente os tempos de resposta dos aplicativos e ofereça maior disponibilidade para fornecer acesso aos dados da carga de trabalho quando e onde forem necessários.
- Simplifique a complexidade geral do armazenamento vSAN com recursos de redimensionamento simples e instantâneos.
- Desempenho garantido para cargas de trabalho de missão crítica usando recursos de remodelação dinâmica.
- Se o Azure VMware Solution Cloud for o destino, o Azure NetApp Files é a solução de armazenamento certa para implantação otimizada.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes links do site:

- Documentação da solução Azure VMware

  "https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Documentação do Azure NetApp Files

  "https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Anexar repositórios de dados do Azure NetApp Files aos hosts do Azure VMware Solution (visualização)

  https://docs.microsoft.com/en-us/azure/azure-vmware/attach-azure-netapp-files-to-azure-vmware-solution-hosts?tabs=azure-portal/

Criando um armazenamento de dados NFS suplementar no Azure

O suporte ao armazenamento de dados NFS foi introduzido com o ESXi versão 3 em implantações locais, o que ampliou muito os recursos de armazenamento do vSphere.

Executar o vSphere no NFS é uma opção amplamente adotada para implantações de virtualização no local porque oferece alto desempenho e estabilidade. Se você tiver um armazenamento conectado à rede (NAS) significativo em um datacenter local, considere implantar um SDDC de solução VMware no Azure com armazenamentos de dados do Azure NetApp File para superar desafios de capacidade e desempenho.

O Azure NetApp Files é criado com base no software de gerenciamento de dados NetApp ONTAP , líder do setor e altamente disponível. Os serviços do Microsoft Azure são agrupados em três categorias: básicos, principais e especializados. O Azure NetApp Files está na categoria especializada e é apoiado por hardware já implantado em muitas regiões. Com alta disponibilidade (HA) integrada, o Azure NetApp Files protege seus dados da maioria das interrupções e oferece um SLA líder do setor de "99,99%" tempo de atividade.

Antes da introdução do recurso de armazenamento de dados do Azure NetApp Files , a operação de

expansão para clientes que planejavam hospedar cargas de trabalho com alto desempenho e armazenamento exigia a expansão da computação e do armazenamento.

Tenha em mente as seguintes questões:

- Configurações de cluster desbalanceadas não são recomendadas em um cluster SDDC. Portanto, expandir o armazenamento significa adicionar mais hosts, o que implica em mais TCO.
- Somente um ambiente vSAN é possível. Portanto, todo o tráfego de armazenamento compete diretamente com as cargas de trabalho de produção.
- Não há opção para fornecer vários níveis de desempenho para alinhar os requisitos do aplicativo, desempenho e custo.
- É fácil atingir os limites da capacidade de armazenamento do vSAN criado sobre hosts de cluster. Ao integrar ofertas de plataforma como serviço (PaaS) nativas do Azure, como o Azure NetApp Files , como um armazenamento de dados, os clientes têm a opção de dimensionar seu armazenamento separadamente e adicionar nós de computação ao cluster SDDC somente quando necessário. Essa capacidade supera os desafios mencionados acima.

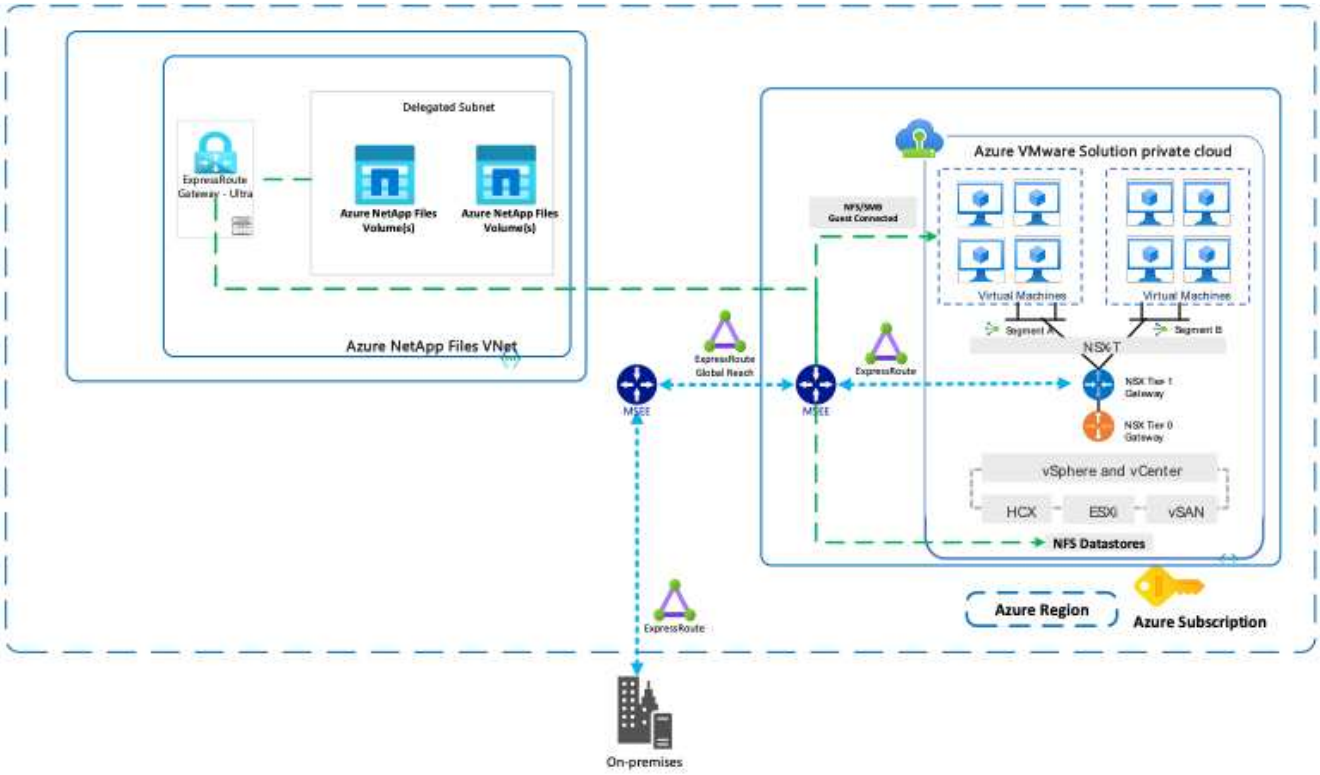
O Azure NetApp Files também permite que você implante vários armazenamentos de dados, o que ajuda a imitar um modelo de implantação local ao colocar máquinas virtuais no armazenamento de dados apropriado e ao atribuir o nível de serviço necessário para atender aos requisitos de desempenho da carga de trabalho. Com a capacidade exclusiva de suporte a vários protocolos, o armazenamento de convidados é uma opção adicional para cargas de trabalho de bancos de dados como SQL e Oracle, além de usar o recurso de armazenamento de dados NFS suplementar para abrigar os VMDKs restantes. Além disso, o recurso de snapshot nativo permite que você execute backups rápidos e restaurações granulares.



Entre em contato com a Azure e a NetApp Solution Architects para planejar e dimensionar o armazenamento e determinar o número necessário de hosts. A NetApp recomenda identificar os requisitos de desempenho de armazenamento antes de finalizar o layout do armazenamento de dados para implantações de teste, POC e produção.

Arquitetura detalhada

De uma perspectiva de alto nível, esta arquitetura descreve como obter conectividade de nuvem híbrida e portabilidade de aplicativos em ambientes locais e no Azure. Ele também descreve o uso do Azure NetApp Files como um armazenamento de dados NFS suplementar e como uma opção de armazenamento no convidado para máquinas virtuais convidadas hospedadas na solução Azure VMware.



Dimensionamento

O aspecto mais importante na migração ou recuperação de desastres é determinar o tamanho correto para o ambiente de destino. É muito importante entender quantos nós são necessários para acomodar um exercício de elevação e transferência do local para a Solução VMware no Azure.

Para dimensionamento, use dados históricos do ambiente local usando o RVTools (preferencial) ou outras ferramentas como Live Optics ou Azure Migrate. O RVTools é uma ferramenta ideal para capturar vCPU, vMem, vDisk e todas as informações necessárias, incluindo VMs ligadas ou desligadas, para caracterizar o ambiente de destino.

Para executar o RVtools, conclua as seguintes etapas:

1. Baixe e instale o RVTools.
2. Execute o RVTools, insira as informações necessárias para se conectar ao seu vCenter Server local e pressione Login.
3. Exporte o inventário para uma planilha do Excel.
4. Edite a planilha e remova quaisquer VMs que não sejam candidatas ideais da guia vInfo. Essa abordagem fornece uma saída clara sobre os requisitos de armazenamento que podem ser usados para dimensionar corretamente o cluster Azure VMware SDDC com o número necessário de hosts.

> As VMs convidadas usadas com armazenamento no convidado devem ser calculadas separadamente; no entanto, o Azure NetApp Files pode facilmente cobrir a capacidade de armazenamento adicional, mantendo assim o TCO geral baixo.

Implantando e configurando a solução Azure VMware

Assim como no local, planejar uma solução Azure VMware é essencial para um ambiente de produção bem-sucedido, pronto para criação de máquinas virtuais e migração.

Esta seção descreve como configurar e gerenciar o AVS para uso em combinação com o Azure NetApp Files como um armazenamento de dados com armazenamento no convidado também.

O processo de configuração pode ser dividido em três partes:

- Registre o provedor de recursos e crie uma nuvem privada.
- Conecte-se a um gateway de rede virtual ExpressRoute novo ou existente.
- Valide a conectividade de rede e acesse a nuvem privada. Consulte isto"link" para um passo a passo do processo de provisionamento do SDDC da solução Azure VMware.

Configurar o Azure NetApp Files com a Solução VMware no Azure

A nova integração entre o Azure NetApp Files permite que você crie datastores NFS por meio das APIs/CLI do provedor de recursos do Azure VMware Solution com volumes do Azure NetApp Files e monte os datastores nos clusters de sua escolha em uma nuvem privada. Além de abrigar os VMDKs de VM e aplicativo, os volumes de arquivo do Azure NetApp também podem ser montados a partir de VMs criadas no ambiente SDDC do Azure VMware Solution. Os volumes podem ser montados no cliente Linux e mapeados em um cliente Windows, porque o Azure NetApp Files oferece suporte aos protocolos Server Message Block (SMB) e Network File System (NFS).

Para um desempenho ideal, implante o Azure NetApp Files na mesma zona de disponibilidade que a nuvem privada. A colocation com o Express Route Fastpath proporciona o melhor desempenho, com latência de rede mínima.

Para anexar um volume do Azure NetApp File como o armazenamento de dados VMware de uma nuvem privada do Azure VMware Solution, certifique-se de que os seguintes pré-requisitos sejam atendidos.

▼ **Pré-requisitos**

1. Use o az login e valide se a assinatura está registrada no recurso CloudSanExperience no namespace Microsoft.AVS.

```
az login –tenant xcvxcvxc- vxcv- xcvx- cvxc- vxcvxcvxcv
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
```

1. Se não estiver registrado, registre-o.

```
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

O registro pode levar aproximadamente 15 minutos para ser concluído.

1. Para verificar o status do registro, execute o seguinte comando.

```
az feature show --name "CloudSanExperience" --namespace "Microsoft.AVS"
--query properties.state
```

1. Se o registro ficar preso em um estado intermediário por mais de 15 minutos, cancele o registro e registre a bandeira novamente.

```
az feature unregister --name "CloudSanExperience" --namespace
"Microsoft.AVS"
az feature register --name "CloudSanExperience" --namespace
"Microsoft.AVS"
```

1. Verifique se a assinatura está registrada no recurso AnfDatastoreExperience no namespace Microsoft.AVS.

```
az feature show --name "AnfDatastoreExperience" --namespace
"Microsoft.AVS" --query properties.state
```

1. Verifique se a extensão vmware está instalada.

```
az extension show --name vmware
```

1. Se a extensão já estiver instalada, verifique se a versão é 3.0.0. Se uma versão mais antiga estiver instalada, atualize a extensão.

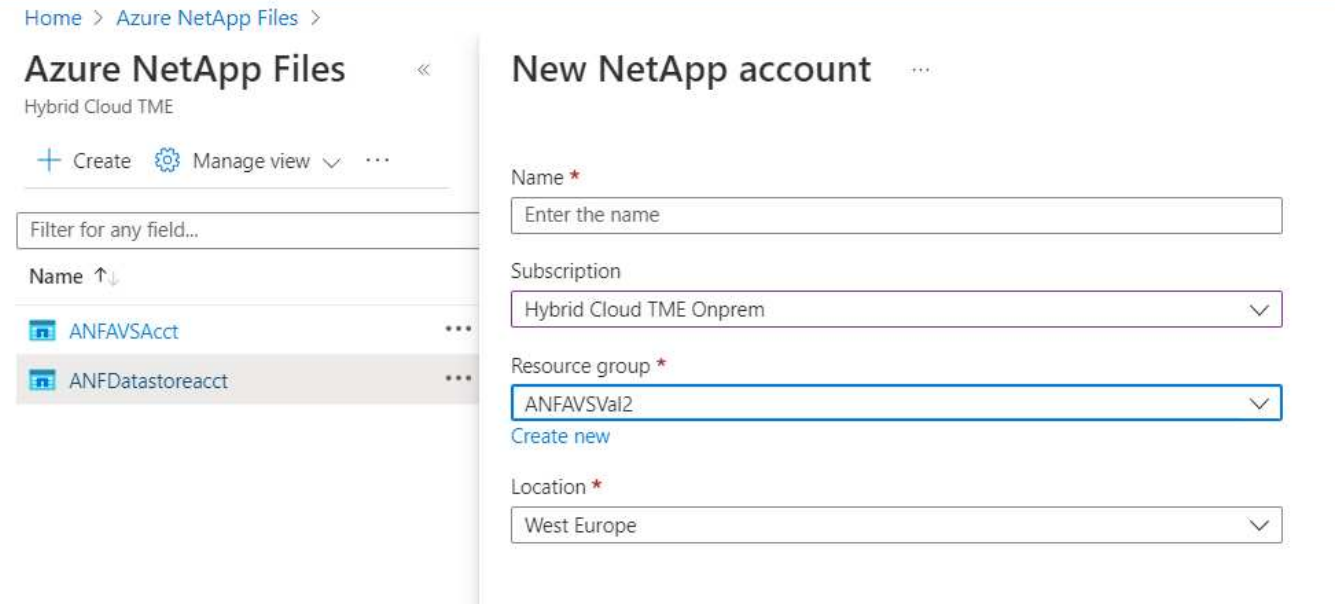
```
az extension update --name vmware
```

1. Se a extensão ainda não estiver instalada, instale-a.

```
az extension add --name vmware
```

▼ **Criar e montar volumes do Azure NetApp Files**

1. Efetue login no Portal do Azure e acesse o Azure NetApp Files. Verifique o acesso ao serviço Azure NetApp Files e registre o Provedor de Recursos do Azure NetApp Files usando o `az provider register --namespace Microsoft.NetApp –wait` comando. Após o registro, crie uma conta NetApp . Consulte isto "link" para etapas detalhadas.



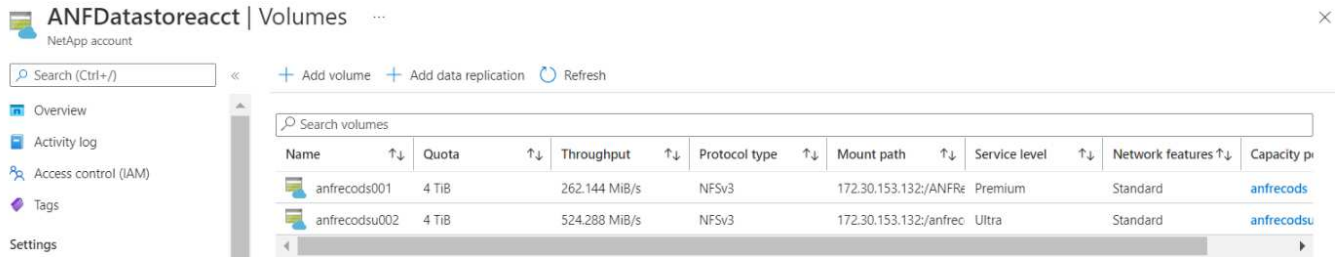
1. Depois que uma conta NetApp for criada, configure pools de capacidade com o nível de serviço e o tamanho necessários. Para obter informações detalhadas, consulte este "link" .



Pontos a serem lembrados

- O NFSv3 é suportado para armazenamentos de dados no Azure NetApp Files.
- Use o nível Premium ou padrão para cargas de trabalho com capacidade limitada e o nível Ultra para cargas de trabalho com desempenho limitado, quando necessário, complementando o armazenamento vSAN padrão.

1. Configure uma sub-rede delegada para o Azure NetApp Files e especifique essa sub-rede ao criar volumes. Para obter etapas detalhadas sobre como criar uma sub-rede delegada, consulte este "link" .
2. Adicione um volume NFS para o armazenamento de dados usando a lâmina Volumes na lâmina pools de capacidade.



Para saber mais sobre o desempenho do volume do Azure NetApp Files por tamanho ou cota,

consulte"Considerações de desempenho para o Azure NetApp Files" .

▼ **Adicionar armazenamento de dados de arquivos do Azure NetApp à nuvem privada**

O volume do Azure NetApp Files pode ser anexado à sua nuvem privada usando o Portal do Azure. Siga isto"link da Microsoft" para uma abordagem passo a passo de uso do portal do Azure para montar um armazenamento de dados de arquivos do Azure NetApp .

Para adicionar um armazenamento de dados do Azure NetApp Files a uma nuvem privada, conclua as seguintes etapas:

1. Depois que os recursos necessários forem registrados, anexe um armazenamento de dados NFS ao cluster de nuvem privada do Azure VMware Solution executando o comando apropriado.
2. Crie um armazenamento de dados usando um volume ANF existente no cluster de nuvem privada do Azure VMware Solution.

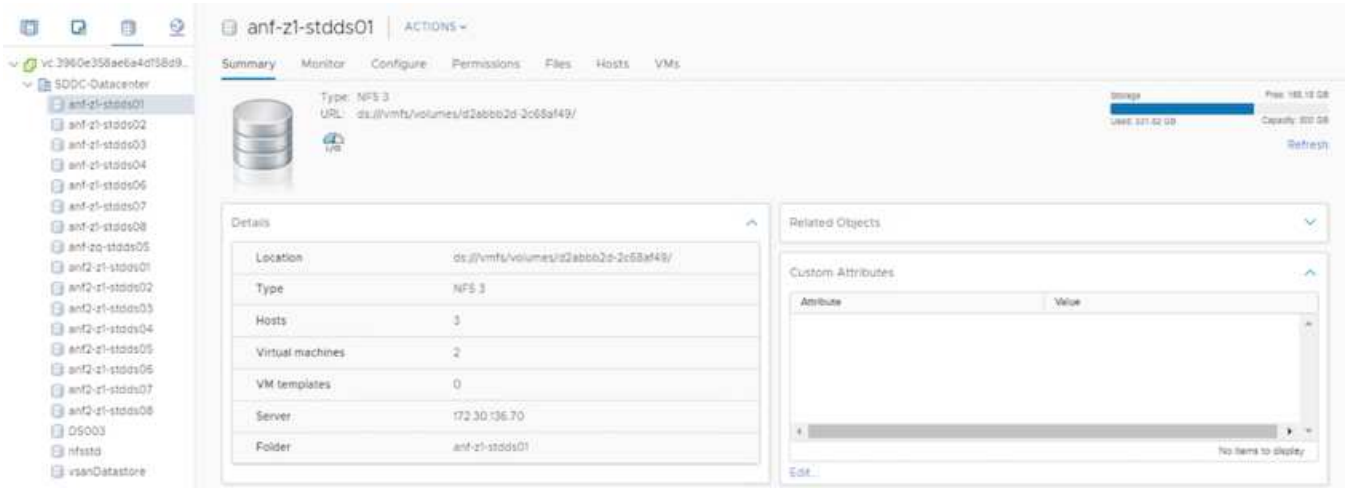
```
C:\Users\niyaz>az vmware datastore netapp-volume create --name
ANFRecoDSU002 --resource-group anfavsval2 --cluster Cluster-1 --private
-cloud ANFDataClus --volume-id /subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
{
  "diskPoolVolume": null,
  "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateCl
ouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002",
  "name": "ANFRecoDSU002",
  "netAppVolume": {
    "id": "/subscriptions/0efa2dfb-917c-4497-b56a-
b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netApp
Accounts/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002
",
    "resourceGroup": "anfavsval2"
  },
  "provisioningState": "Succeeded",
  "resourceGroup": "anfavsval2",
  "type": "Microsoft.AVS/privateClouds/clusters/datastores"
}

. List all the datastores in a private cloud cluster.
```

C:\Usuários\niyaz>lista de armazenamento de dados vmware az --grupo de recursos anfavsval2 --cluster Cluster-1 --nuvem-privada ANFDataClus [{ "diskPoolVolume": null, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDS001", "name": "ANFRecoDS001", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp/netAppAccounts/anfdatastoreacct/capacityPools/anfrecods/volumes/ANFRecoDS001",

"resourceGroup": "anfavsval2" }, "provisioningState": "Sucesso", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }, { "diskPoolVolume": nulo, "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.AVS/privateClouds/ANFDataClus/clusters/Cluster-1/datastores/ANFRecoDSU002", "name": "ANFRecoDSU002", "netAppVolume": { "id": "/subscriptions/0efa2dfb-917c-4497-b56a-b3f4eadb8111/resourceGroups/anfavsval2/providers/Microsoft.NetApp / NetApp/anfdatastoreacct/capacityPools/anfrecodsu/volumes/anfrecodsU002", "resourceGroup": "anfavsval2" }, "provisioningState": "Sucesso", "resourceGroup": "anfavsval2", "type": "Microsoft.AVS/privateClouds/clusters/datastores" }]

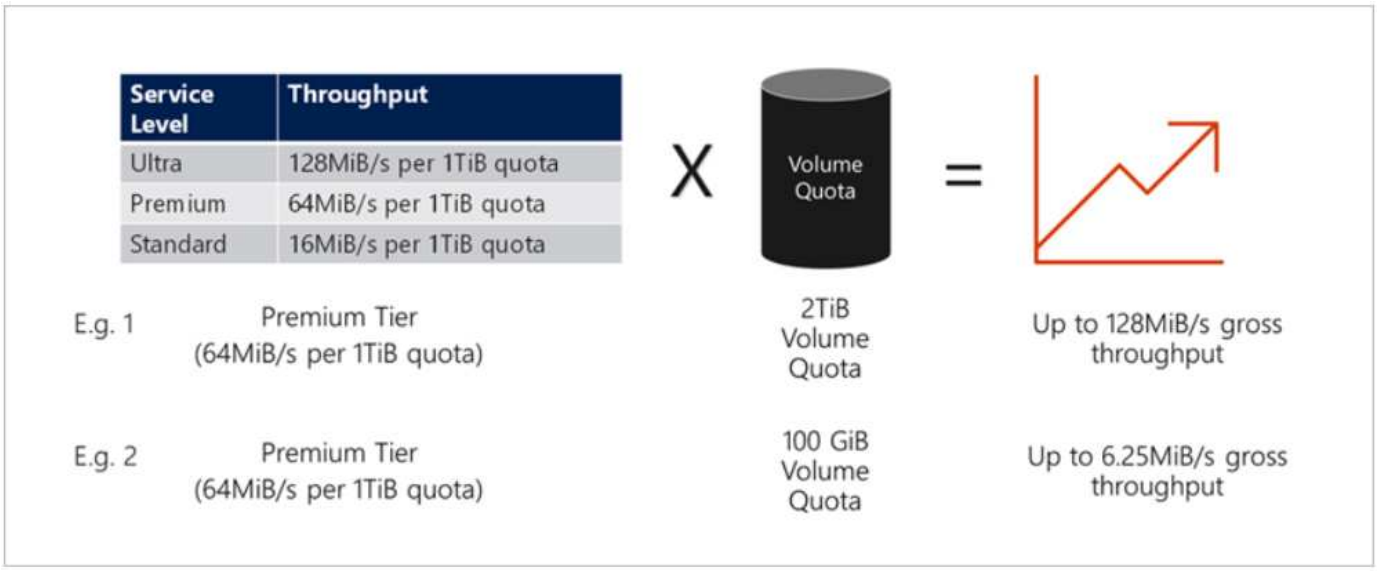
1. Depois que a conectividade necessária estiver estabelecida, os volumes serão montados como um armazenamento de dados.



Dimensionamento e otimização de desempenho

O Azure NetApp Files oferece suporte a três níveis de serviço: Standard (16 MBps por terabyte), Premium (64 MBps por terabyte) e Ultra (128 MBps por terabyte). Provisionar o tamanho correto do volume é importante para o desempenho ideal da carga de trabalho do banco de dados. Com o Azure NetApp Files, o desempenho do volume e o limite de taxa de transferência são determinados com base nos seguintes fatores:

- O nível de serviço do pool de capacidade ao qual o volume pertence
- A cota atribuída ao volume
- O tipo de qualidade de serviço (QoS) (automático ou manual) do pool de capacidade



Para obter mais informações, consulte "Níveis de serviço para Azure NetApp Files" .

Consulte isto"link da Microsoft" para benchmarks de desempenho detalhados que podem ser usados durante um exercício de dimensionamento.

Pontos a serem lembrados
• Use o nível Premium ou Standard para volumes de armazenamento de dados para capacidade e desempenho ideais. Se for necessário desempenho, o nível Ultra pode ser usado. • Para requisitos de montagem de convidado, use o nível Premium ou Ultra e para requisitos de compartilhamento de arquivos para VMs convidadas, use volumes de nível Standard ou Premium.

Considerações de desempenho

É importante entender que com o NFS versão 3 há apenas um pipe ativo para a conexão entre o host ESXi e um único destino de armazenamento. Isso significa que, embora possa haver conexões alternativas disponíveis para failover, a largura de banda de um único armazenamento de dados e o armazenamento subjacente são limitados ao que uma única conexão pode fornecer.

Para aproveitar mais largura de banda disponível com volumes do Azure NetApp Files , um host ESXi deve ter várias conexões com os destinos de armazenamento. Para resolver esse problema, você pode configurar vários armazenamentos de dados, com cada armazenamento de dados usando conexões separadas entre o host ESXi e o armazenamento.

Para maior largura de banda, como prática recomendada, crie vários armazenamentos de dados usando vários volumes ANF, crie VMDKs e distribua os volumes lógicos entre VMDKs.

Consulte isto"link da Microsoft" para benchmarks de desempenho detalhados que podem ser usados durante um exercício de dimensionamento.

Pontos a serem lembrados

- A solução Azure VMware permite oito armazenamentos de dados NFS por padrão. Isso pode ser aumentado por meio de uma solicitação de suporte.
- Aproveite o ER Fastpath junto com o Ultra SKU para maior largura de banda e menor latência. Mais informações
- Com os recursos de rede "Básicos" nos arquivos do Azure NetApp , a conectividade do Azure VMware Solution é limitada pela largura de banda do circuito do ExpressRoute e do ExpressRoute Gateway.
- Para volumes do Azure NetApp Files com recursos de rede "Padrão", o ExpressRoute FastPath é suportado. Quando habilitado, o FastPath envia tráfego de rede diretamente para volumes do Azure NetApp Files , ignorando o gateway, fornecendo maior largura de banda e menor latência.

Aumentando o tamanho do armazenamento de dados

A remodelação de volume e as mudanças dinâmicas no nível de serviço são completamente transparentes para o SDDC. No Azure NetApp Files, esses recursos fornecem otimizações contínuas de desempenho, capacidade e custo. Aumente o tamanho dos armazenamentos de dados NFS redimensionando o volume do Portal do Azure ou usando a CLI. Depois de terminar, acesse o vCenter, vá para a guia armazenamento de dados, clique com o botão direito do mouse no armazenamento de dados apropriado e selecione Atualizar informações de capacidade. Essa abordagem pode ser usada para aumentar a capacidade do armazenamento de dados e aumentar o desempenho do armazenamento de dados de forma dinâmica e sem tempo de inatividade. Esse processo também é completamente transparente para os aplicativos.

Pontos a serem lembrados

- A remodelação de volume e a capacidade de nível de serviço dinâmico permitem otimizar custos por meio do dimensionamento para cargas de trabalho de estado estável e, assim, evitar o provisionamento excessivo.
- O VAAI não está habilitado.

Cargas de trabalho

▼ **Migração**

Um dos casos de uso mais comuns é a migração. Use o VMware HCX ou o vMotion para mover VMs locais. Como alternativa, você pode usar o Rivermeadow para migrar VMs para armazenamentos de dados do Azure NetApp Files .

▼ **Proteção de Dados**

Fazer backup de VMs e recuperá-las rapidamente estão entre os grandes pontos fortes dos datastores ANF. Use cópias de instantâneo para fazer cópias rápidas da sua VM ou armazenamento de dados sem afetar o desempenho e, em seguida, envie-as para o armazenamento do Azure para proteção de dados de longo prazo ou para uma região secundária usando replicação entre regiões para fins de recuperação de desastres. Essa abordagem minimiza o espaço de armazenamento e a largura de banda da rede armazenando apenas as informações alteradas.

Use cópias de instantâneo do Azure NetApp Files para proteção geral e use ferramentas de aplicativo para proteger dados transacionais, como SQL Server ou Oracle, que residem nas VMs convidadas. Essas cópias de snapshot são diferentes dos snapshots do VMware (consistência) e são adequadas para proteção de longo prazo.



Com os datastores ANF, a opção Restaurar para novo volume pode ser usada para clonar um volume de datastore inteiro, e o volume restaurado pode ser montado como outro

datastore para hosts dentro do AVS SDDC. Depois que um armazenamento de dados é montado, as VMs dentro dele podem ser registradas, reconfiguradas e personalizadas como se fossem VMs clonadas individualmente.

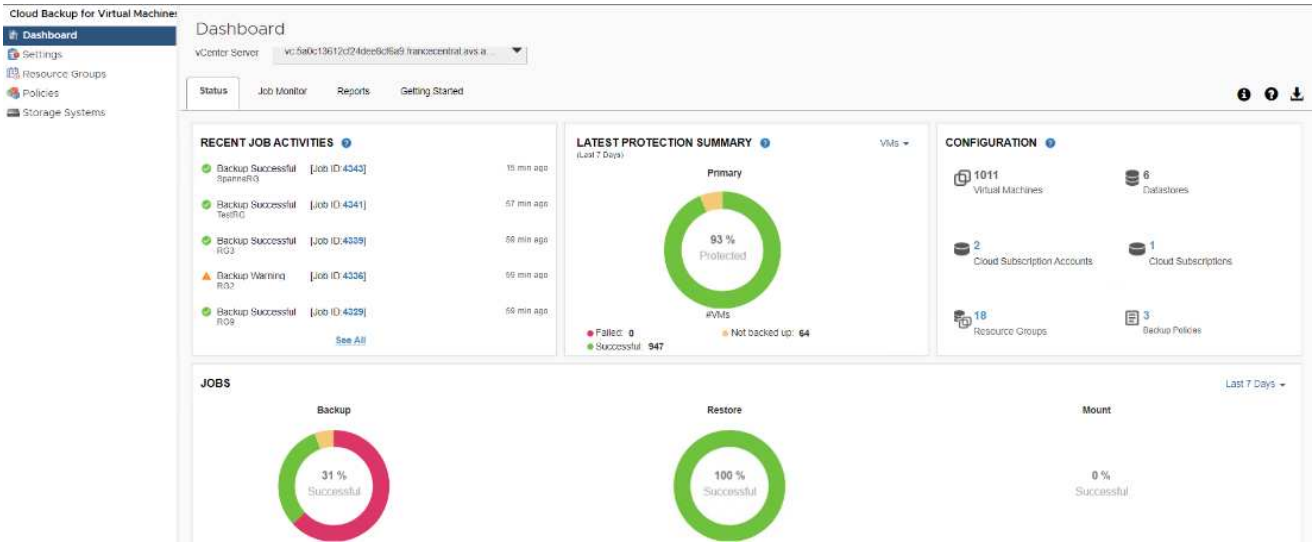
▼ **NetApp Backup e recuperação para máquinas virtuais**

O NetApp Backup and Recovery for Virtual Machines fornece uma GUI de cliente web do vSphere no vCenter para proteger máquinas virtuais do Azure VMware Solution e datastores do Azure NetApp files por meio de políticas de backup. Essas políticas podem definir agendamento, retenção e outros recursos. A funcionalidade do NetApp Backup and Recovery for Virtual Machines pode ser implantada usando o comando Run.

As políticas de configuração e proteção podem ser instaladas concluindo as seguintes etapas:

1. Instale o NetApp Backup and Recovery for Virtual Machine na nuvem privada do Azure VMware Solution usando o comando Run.
2. Adicione credenciais de assinatura de nuvem (cliente e valor secreto) e, em seguida, adicione uma conta de assinatura de nuvem (conta NetApp e grupo de recursos associado) que contenha os recursos que você deseja proteger.
3. Crie uma ou mais políticas de backup que gerenciem a retenção, a frequência e outras configurações para backups de grupos de recursos.
4. Crie um contêiner para adicionar um ou mais recursos que precisam ser protegidos com políticas de backup.
5. Em caso de falha, restaure a VM inteira ou VMDKs individuais específicos para o mesmo local.

Com a tecnologia Azure NetApp Files Snapshot, backups e restaurações são muito rápidos.



▼ **Recuperação de desastres com Azure NetApp Files, JetStream DR e Azure VMware Solution**

A recuperação de desastres na nuvem é uma maneira resiliente e econômica de proteger as cargas de trabalho contra interrupções do site e eventos de corrupção de dados (por exemplo, ransomware). Usando a estrutura VMware VAIO, as cargas de trabalho locais do VMware podem ser replicadas para o armazenamento de Blobs do Azure e recuperadas, permitindo perda de dados mínima ou quase nenhuma e RTO próximo de zero. O JetStream DR pode ser usado para recuperar perfeitamente as cargas de trabalho replicadas do local para o AVS e, especificamente, para o Azure NetApp Files. Ele permite uma recuperação de desastres econômica usando recursos mínimos no local de DR e

armazenamento em nuvem econômico. O JetStream DR automatiza a recuperação para armazenamentos de dados ANF por meio do Azure Blob Storage. O JetStream DR recupera VMs independentes ou grupos de VMs relacionadas na infraestrutura do site de recuperação de acordo com o mapeamento de rede e fornece recuperação pontual para proteção contra ransomware.

"Solução DR com ANF, JetStream e AVS" .

Opções de armazenamento conectado do NetApp Guest para Azure

O Azure oferece suporte ao armazenamento NetApp conectado a convidados com o serviço nativo Azure NetApp Files (ANF) ou com o Cloud Volumes ONTAP (CVO).

Azure NetApp Files (ANF)

O Azure netApp Files traz gerenciamento e armazenamento de dados de nível empresarial para o Azure para que você possa gerenciar suas cargas de trabalho e aplicativos com facilidade. Migre suas cargas de trabalho para a nuvem e execute-as sem sacrificar o desempenho.

O Azure netApp Files remove obstáculos para que você possa mover todos os seus aplicativos baseados em arquivos para a nuvem. Pela primeira vez, você não precisa reestruturar seus aplicativos e obtém armazenamento persistente para seus aplicativos sem complexidade.

Como o serviço é fornecido por meio do Portal do Microsoft Azure, os usuários experimentam um serviço totalmente gerenciado como parte do Contrato Corporativo da Microsoft. Suporte de classe mundial, gerenciado pela Microsoft, lhe dá total tranquilidade. Esta solução única permite que você adicione cargas de trabalho multiprotocolo de forma rápida e fácil. Você pode criar e implantar aplicativos baseados em arquivos do Windows e do Linux, mesmo para ambientes legados.

Azure NetApp Files (ANF) como armazenamento conectado a convidados

▼ **Configurar o Azure NetApp Files com o Azure VMware Solution (AVS)**

Os compartilhamentos do Azure NetApp Files podem ser montados a partir de VMs criadas no ambiente SDDC do Azure VMware Solution. Os volumes também podem ser montados no cliente Linux e mapeados no cliente Windows porque o Azure NetApp Files oferece suporte aos protocolos SMB e NFS. Os volumes do Azure NetApp Files podem ser configurados em cinco etapas simples.

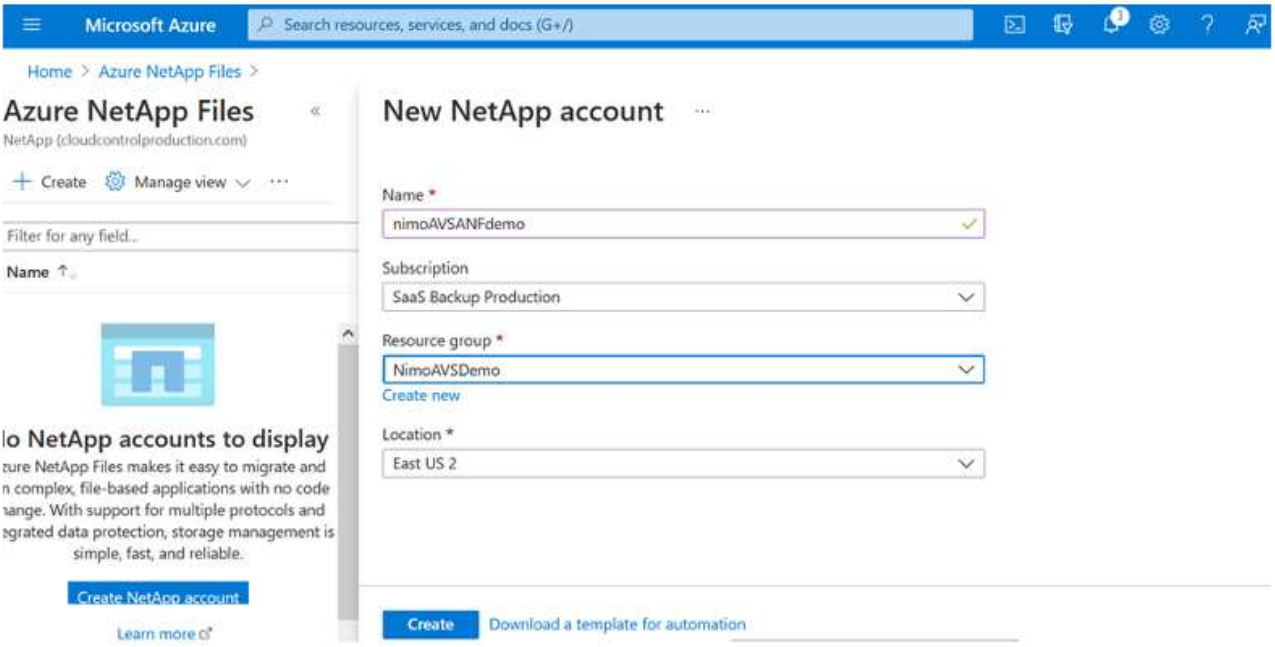
O Azure NetApp Files e o Azure VMware Solution devem estar na mesma região do Azure.

▼ **Criar e montar volumes do Azure NetApp Files**

Para criar e montar volumes do Azure NetApp Files , conclua as seguintes etapas:

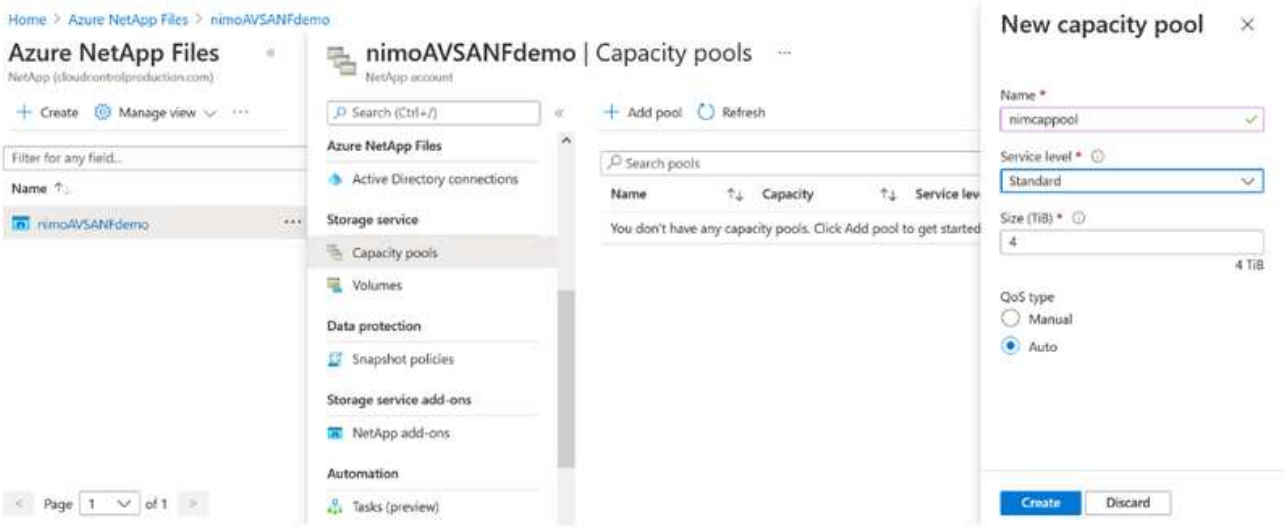
1. Efetue login no Portal do Azure e acesse o Azure NetApp Files. Verifique o acesso ao serviço Azure NetApp Files e registre o Provedor de Recursos do Azure NetApp Files usando o comando *az provider register --namespace NetApp –wait*. Após a conclusão do registro, crie uma conta NetApp .

   Para etapas detalhadas, consulte"Compartilhamentos do Azure NetApp Files" . Esta página guiará você pelo processo passo a passo.

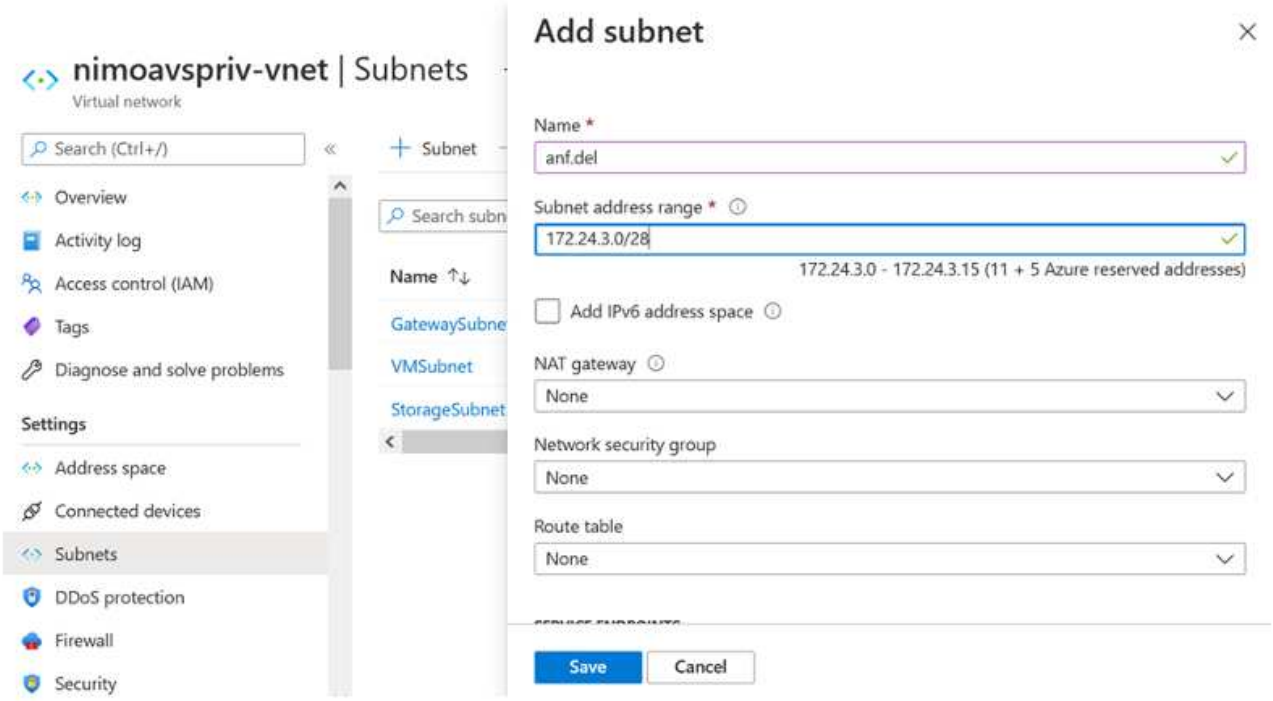


2. Após a criação da conta NetApp , configure os pools de capacidade com o nível de serviço e o tamanho necessários.

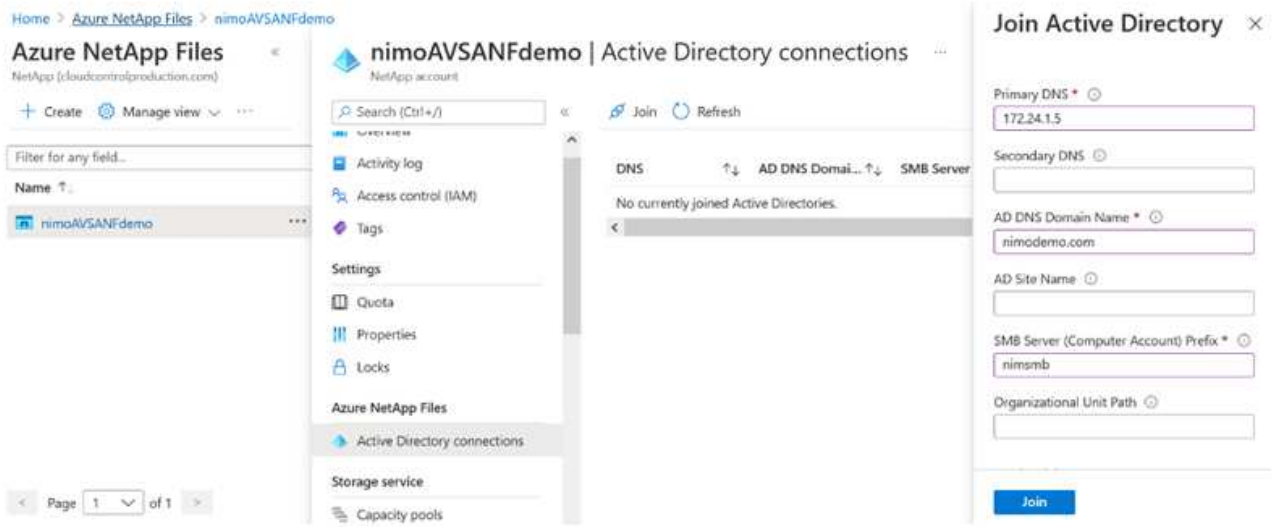
   Para obter mais informações, consulte "Configurar um pool de capacidade" .



3. Configure a sub-rede delegada para o Azure NetApp Files e especifique essa sub-rede ao criar os volumes. Para obter etapas detalhadas sobre como criar uma sub-rede delegada, consulte"Delegar uma sub-rede ao Azure NetApp Files" .

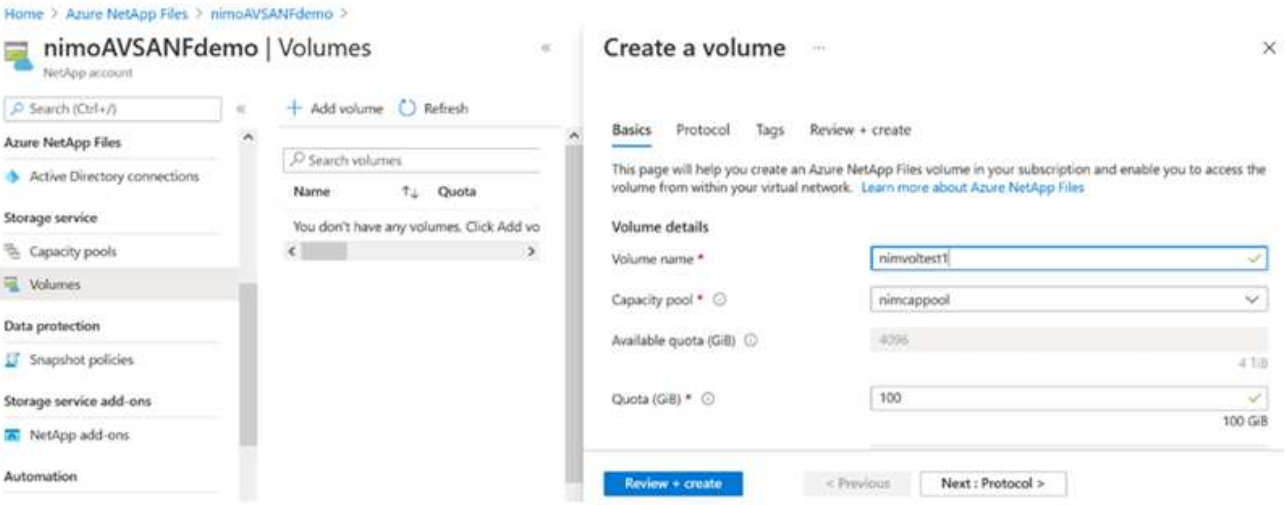


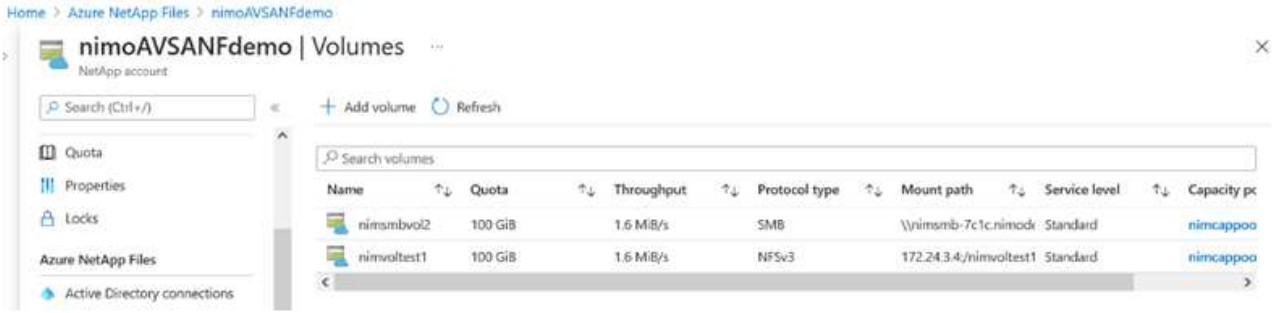
4. Adicione um volume SMB usando a lâmina Volumes na lâmina Pools de Capacidade. Certifique-se de que o conector do Active Directory esteja configurado antes de criar o volume SMB.



5. Clique em Revisar + Criar para criar o volume SMB.

   Se o aplicativo for SQL Server, habilite a disponibilidade contínua do SMB.

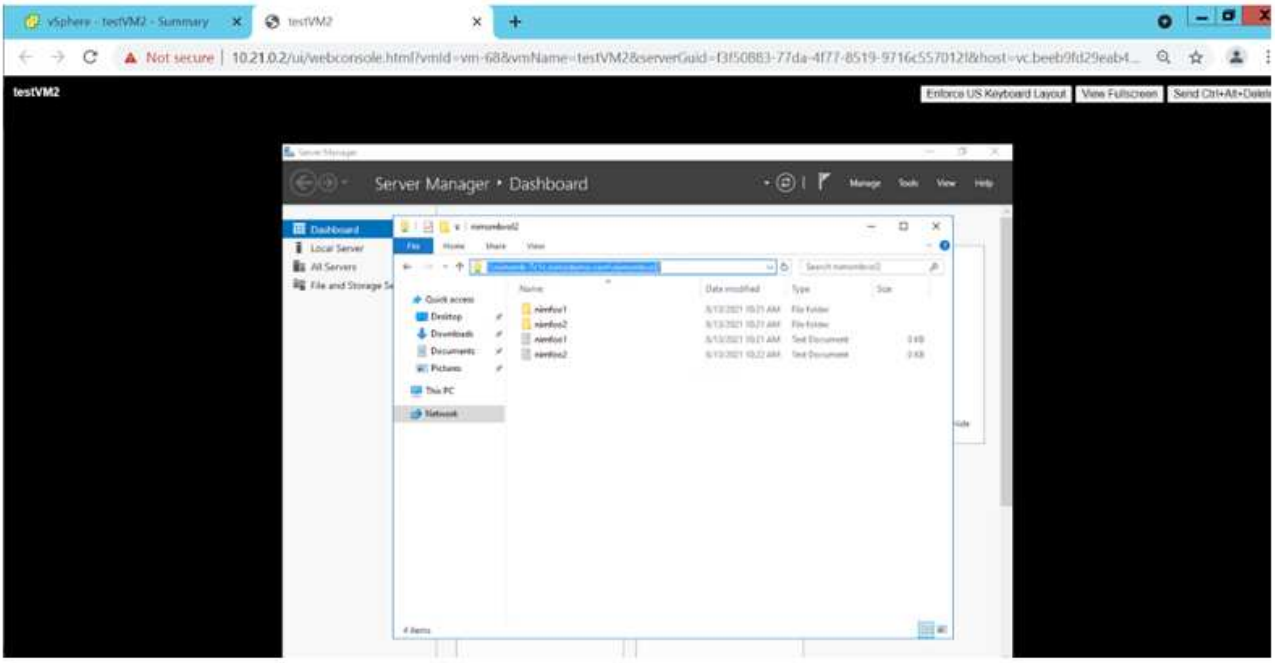


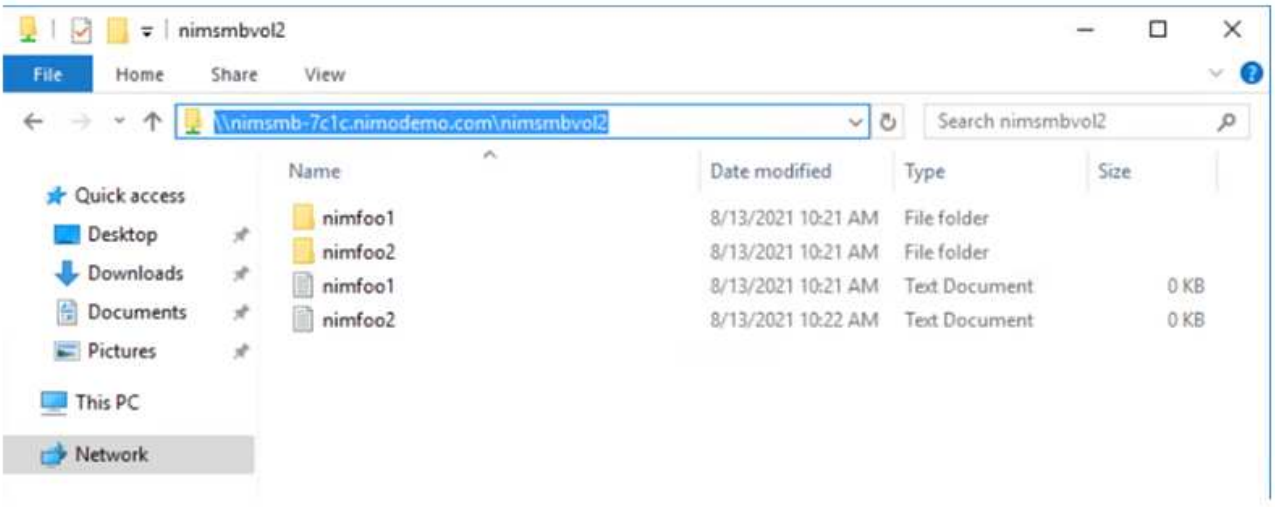


Para saber mais sobre o desempenho do volume do Azure NetApp Files por tamanho ou cota, consulte"Considerações de desempenho para o Azure NetApp Files" .

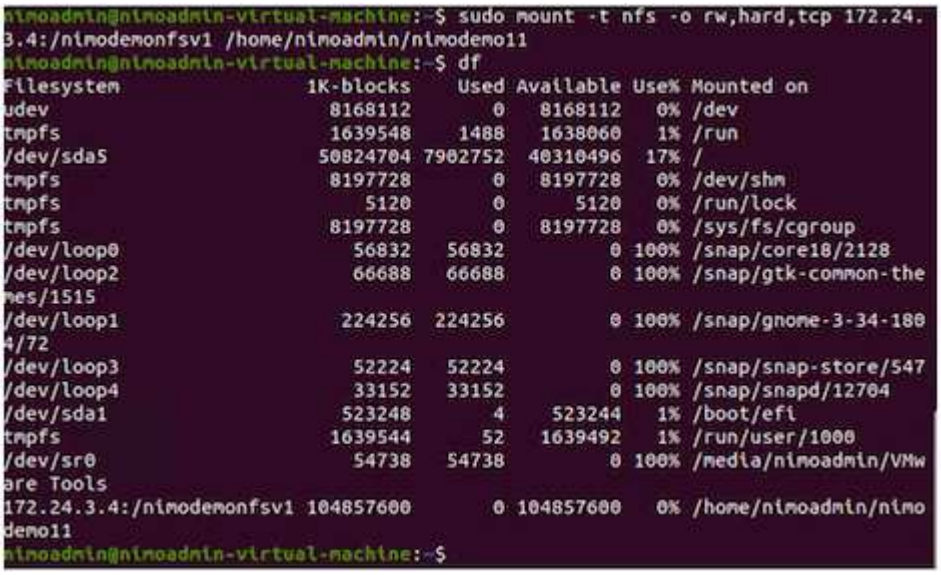
6. Depois que a conectividade estiver estabelecida, o volume poderá ser montado e usado para dados do aplicativo.

   Para fazer isso, no portal do Azure, clique na lâmina Volumes, selecione o volume a ser montado e acesse as instruções de montagem. Copie o caminho e use a opção Mapear unidade de rede para montar o volume na VM em execução no Azure VMware Solution SDDC.





7. Para montar volumes NFS em VMs Linux em execução no Azure VMware Solution SDDC, use este mesmo processo. Use a remodelação de volume ou a capacidade de nível de serviço dinâmico para atender às demandas da carga de trabalho.



Para obter mais informações, consulte "Alterar dinamicamente o nível de serviço de um volume" .

Cloud Volumes ONTAP (CVO)

O Cloud Volumes ONTAP, ou CVO, é a solução de gerenciamento de dados em nuvem líder do setor, desenvolvida no software de armazenamento ONTAP da NetApp, disponível nativamente na Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

É uma versão definida por software do ONTAP que consome armazenamento nativo da nuvem, permitindo que você tenha o mesmo software de armazenamento na nuvem e no local, reduzindo a necessidade de treinar novamente sua equipe de TI em métodos totalmente novos para gerenciar seus dados.

O CVO oferece aos clientes a capacidade de mover dados facilmente da borda para o data center, para a nuvem e vice-versa, reunindo sua nuvem híbrida — tudo gerenciado com um console de gerenciamento de painel único, o NetApp Cloud Manager.

Por design, o CVO oferece desempenho extremo e recursos avançados de gerenciamento de dados para satisfazer até mesmo seus aplicativos mais exigentes na nuvem

Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados

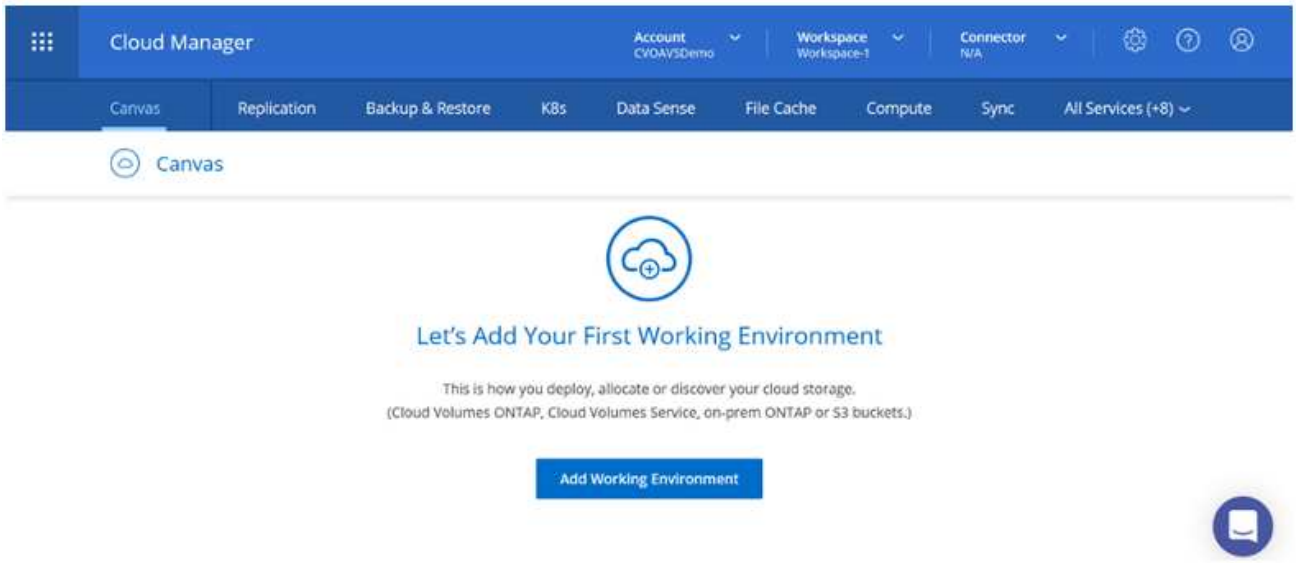
▼ Implantar novos Cloud Volumes ONTAP no Azure

Os compartilhamentos e LUNs do Cloud Volumes ONTAP podem ser montados a partir de VMs criadas no ambiente Azure VMware Solution SDDC. Os volumes também podem ser montados no cliente Linux e no cliente Windows porque o Cloud Volumes ONTAP oferece suporte aos protocolos iSCSI, SMB e NFS. Os volumes Cloud Volumes ONTAP podem ser configurados em algumas etapas simples.

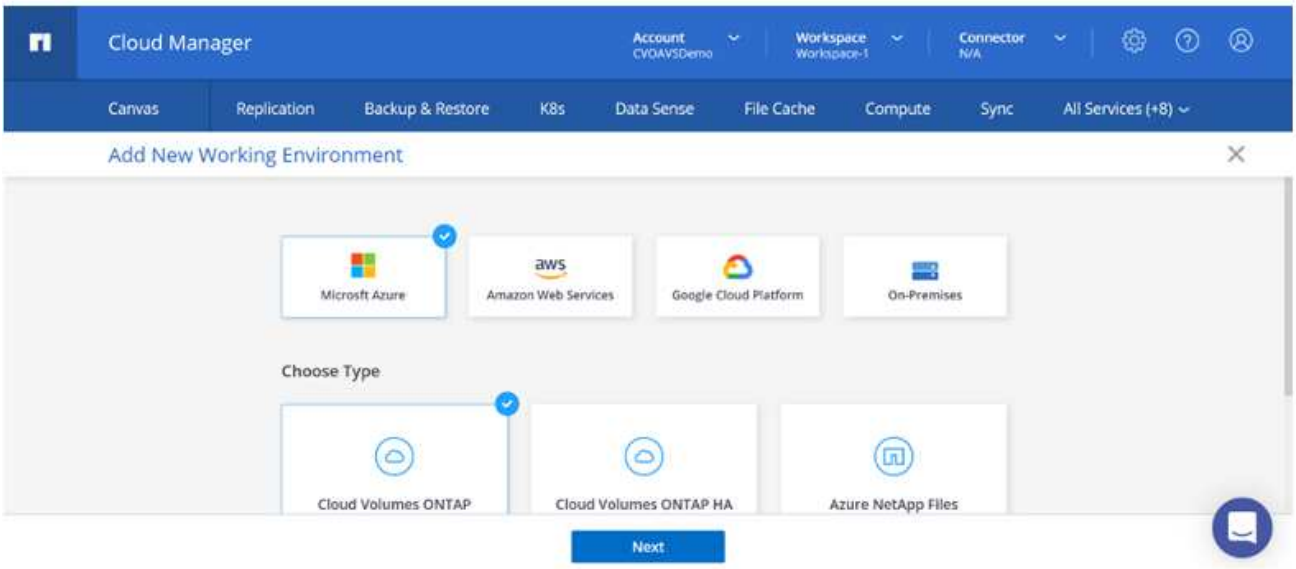
Para replicar volumes de um ambiente local para a nuvem para fins de recuperação de desastres ou migração, estabeleça conectividade de rede com o Azure, usando uma VPN site a site ou o ExpressRoute. A replicação de dados locais para o Cloud Volumes ONTAP está fora do escopo deste documento. Para replicar dados entre sistemas locais e Cloud Volumes ONTAP , consulte"Configurando a replicação de dados entre sistemas" .

Utilize "Dimensionador Cloud Volumes ONTAP" para dimensionar com precisão as instâncias do Cloud Volumes ONTAP. Monitore também o desempenho no local para usar como entrada no dimensionador do Cloud Volumes ONTAP.

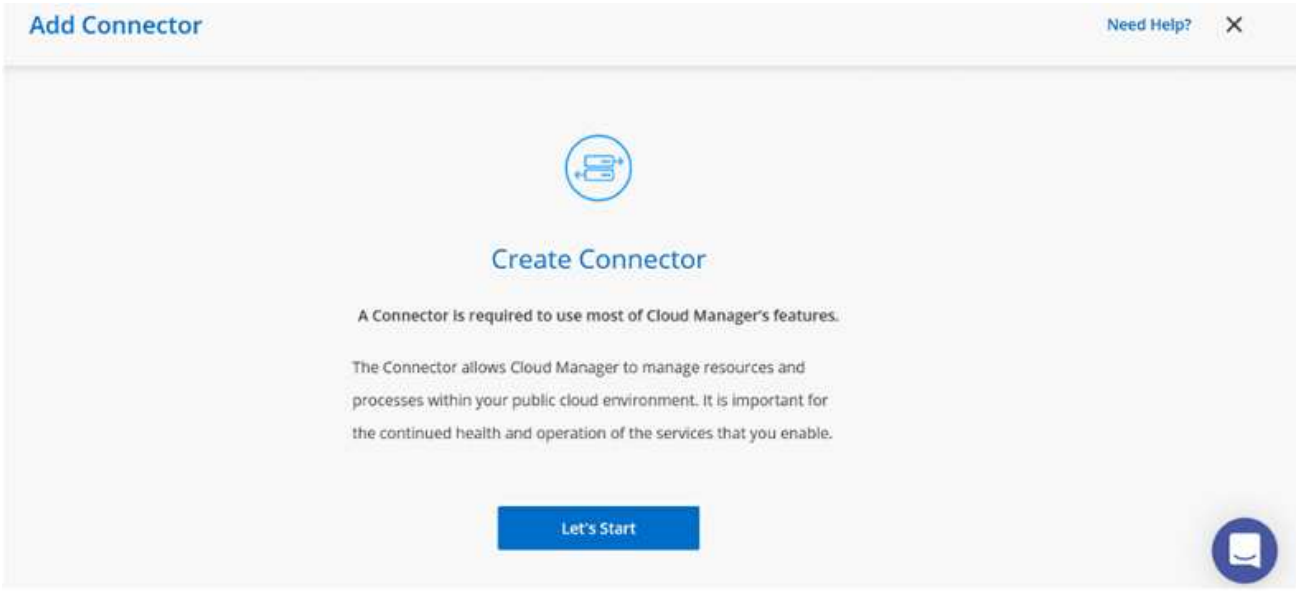
1. Efetue login no NetApp Cloud Central — a tela Fabric View é exibida. Localize a guia Cloud Volumes ONTAP e selecione Ir para o Cloud Manager. Após efetuar login, a tela Canvas será exibida.



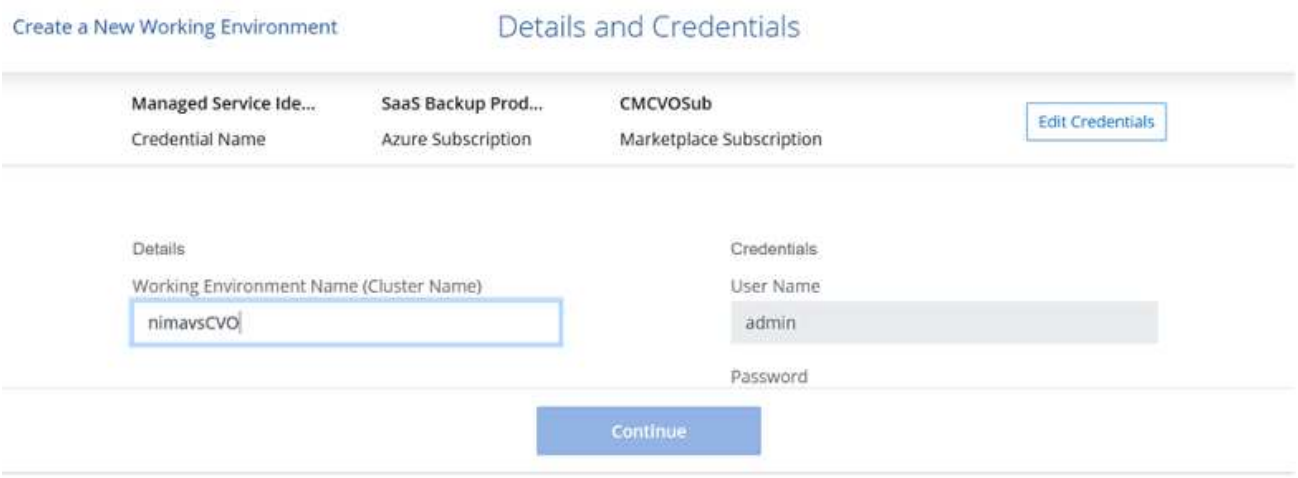
2. Na página inicial do Cloud Manager, clique em Adicionar um ambiente de trabalho e selecione Microsoft Azure como a nuvem e o tipo de configuração do sistema.



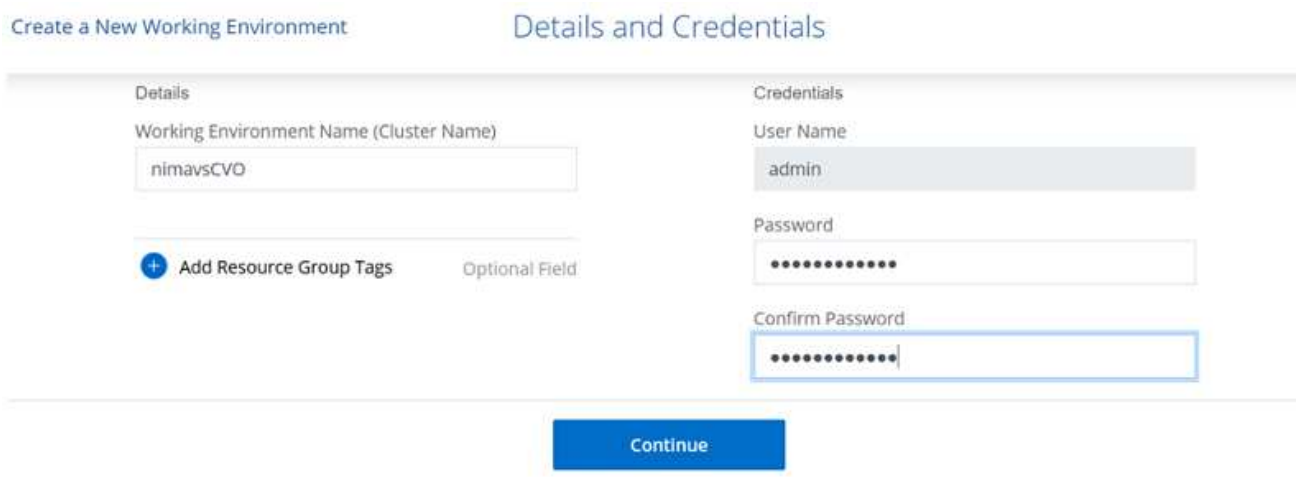
3. Ao criar o primeiro ambiente de trabalho do Cloud Volumes ONTAP , o Cloud Manager solicita que você implante um Conector.



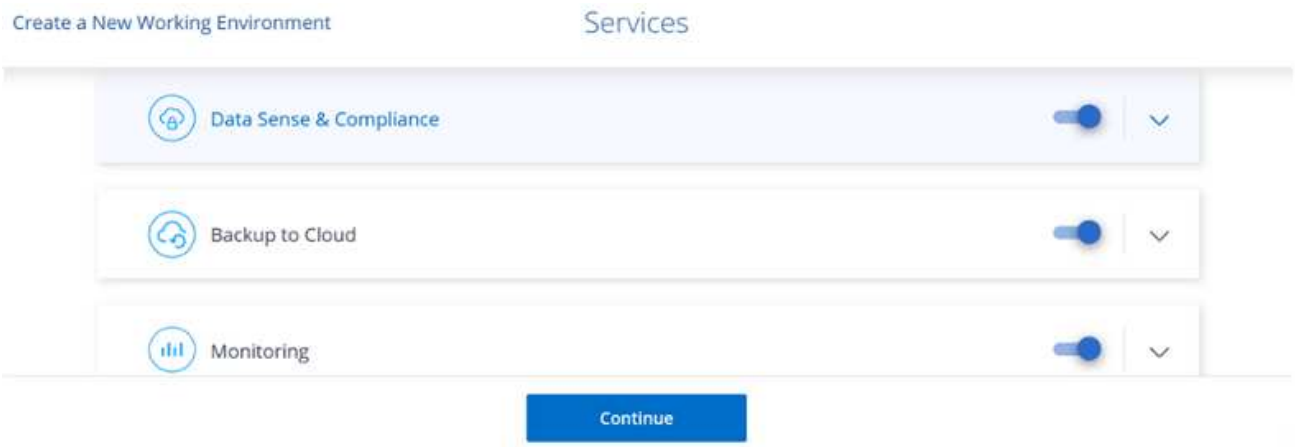
4. Após a criação do conector, atualize os campos Detalhes e Credenciais.



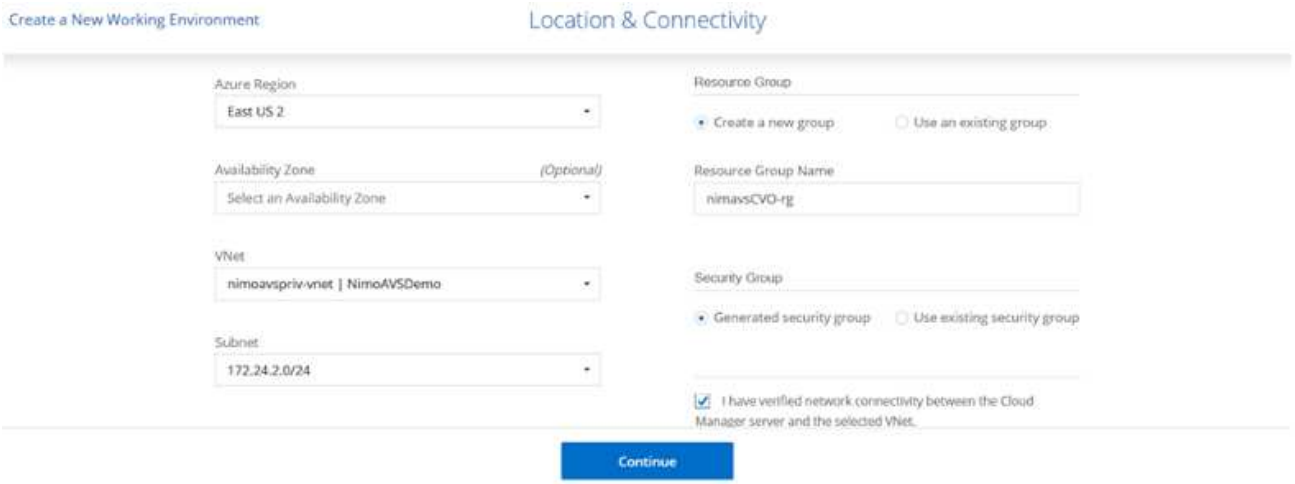
5. Forneça os detalhes do ambiente a ser criado, incluindo o nome do ambiente e as credenciais do administrador. Adicione tags de grupo de recursos para o ambiente do Azure como um parâmetro opcional. Após terminar, clique em Continuar.



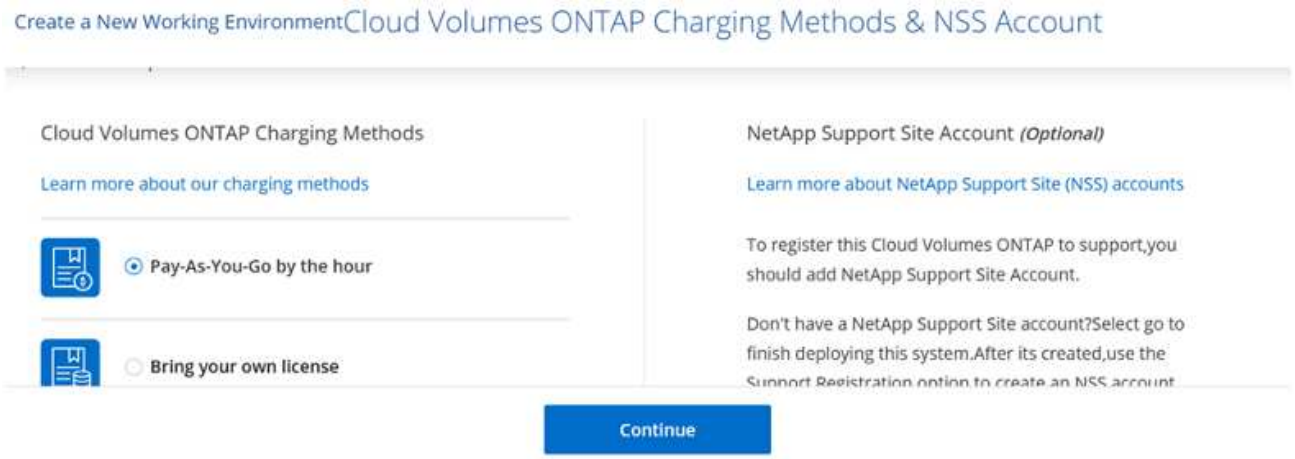
6. Selecione os serviços complementares para a implantação do Cloud Volumes ONTAP, incluindo o NetApp Data Classification, o NetApp Backup and Recovery e o Data Infrastructure Insights. Selecione os serviços e clique em Continue.



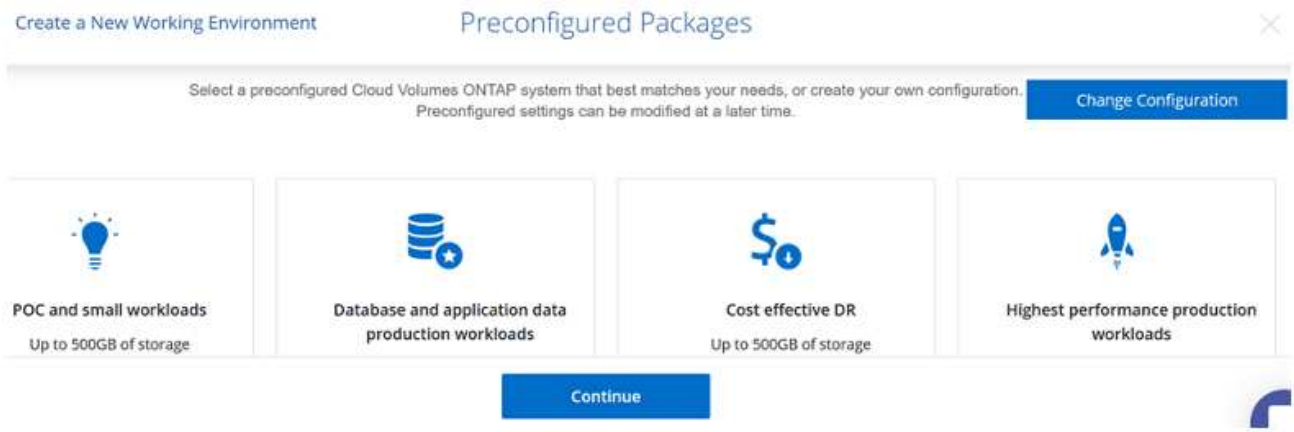
7. Configure a localização e a conectividade do Azure. Selecione a região do Azure, o grupo de recursos, a VNet e a sub-rede a serem usados.



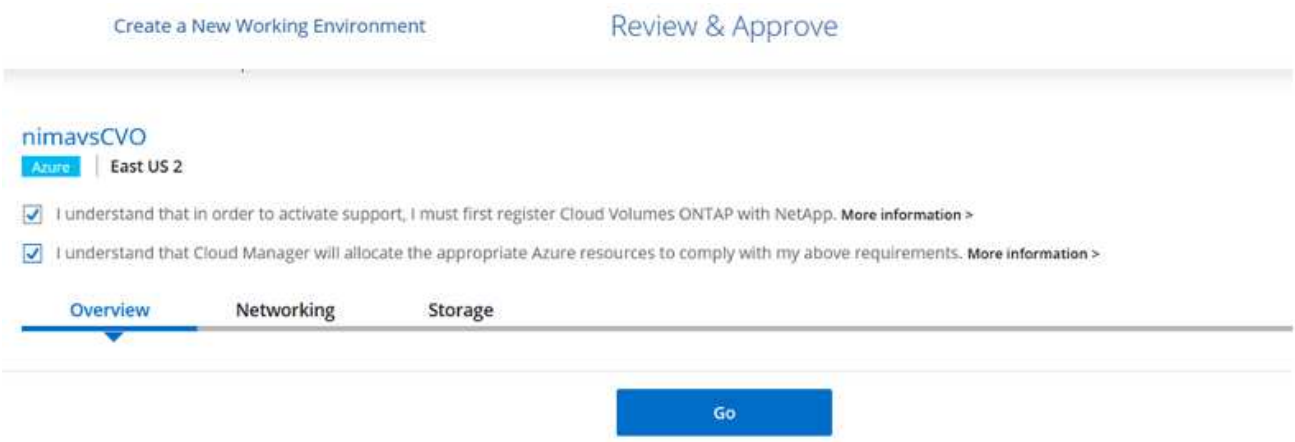
8. Selecione a opção de licença: Pague conforme o uso ou BYOL para usar a licença existente. Neste exemplo, a opção Pague Conforme o Uso é usada.



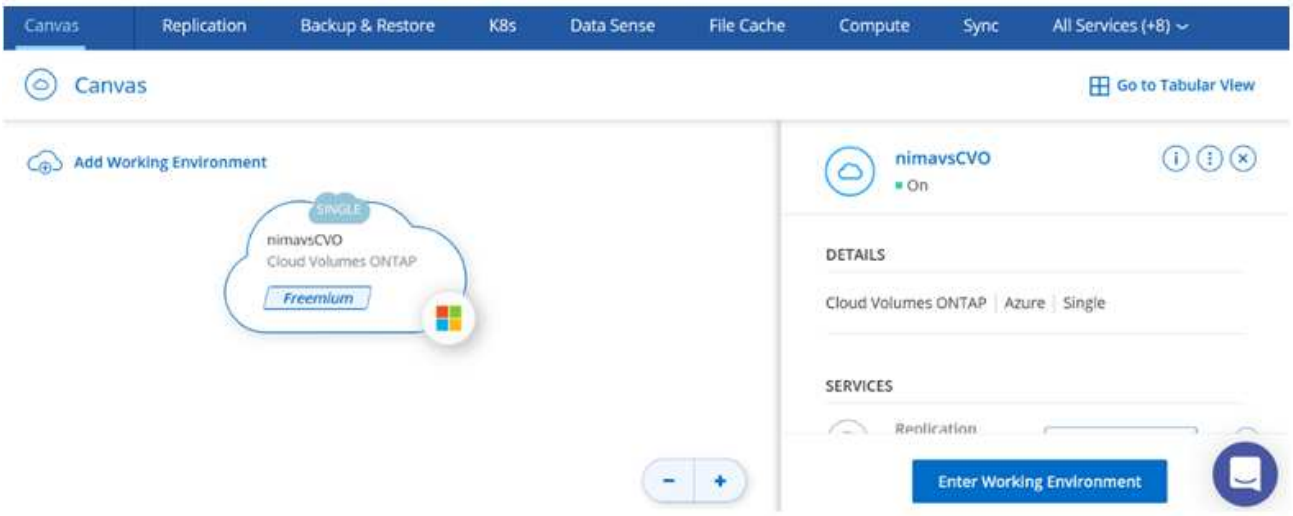
9. Selecione entre vários pacotes pré-configurados disponíveis para os vários tipos de cargas de trabalho.



10. Aceite os dois acordos sobre a ativação do suporte e a alocação de recursos do Azure. Para criar a instância do Cloud Volumes ONTAP , clique em Ir.

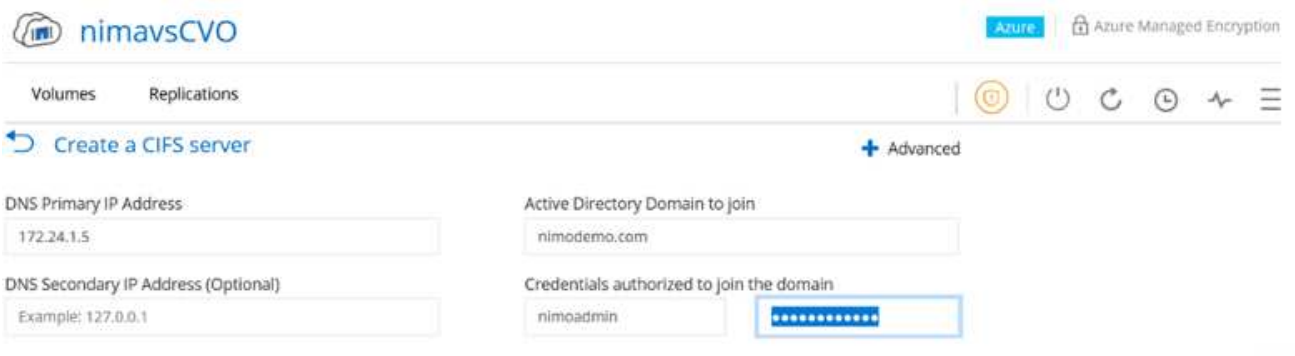


11. Depois que o Cloud Volumes ONTAP é provisionado, ele é listado nos ambientes de trabalho na página Canvas.

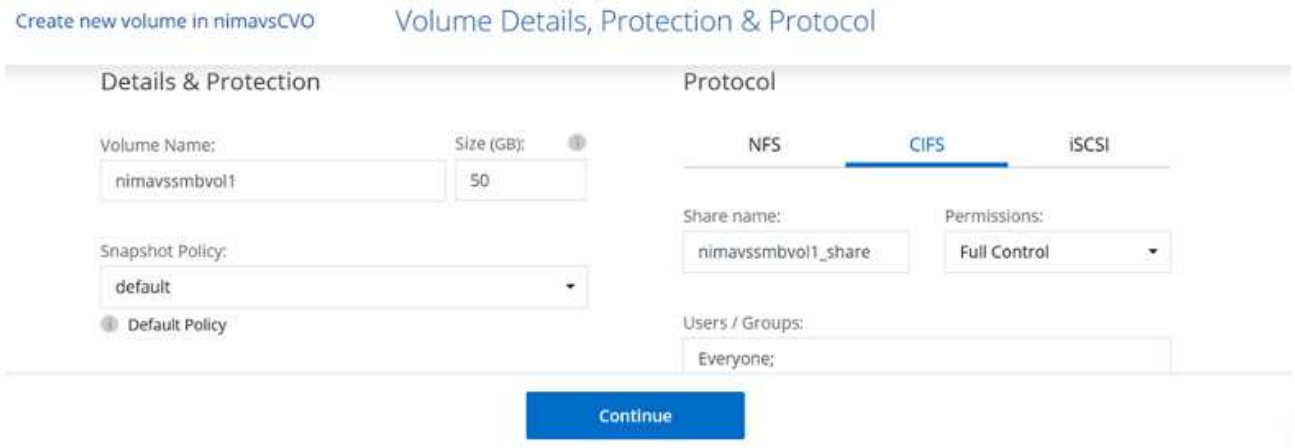


▼ Configurações adicionais para volumes SMB

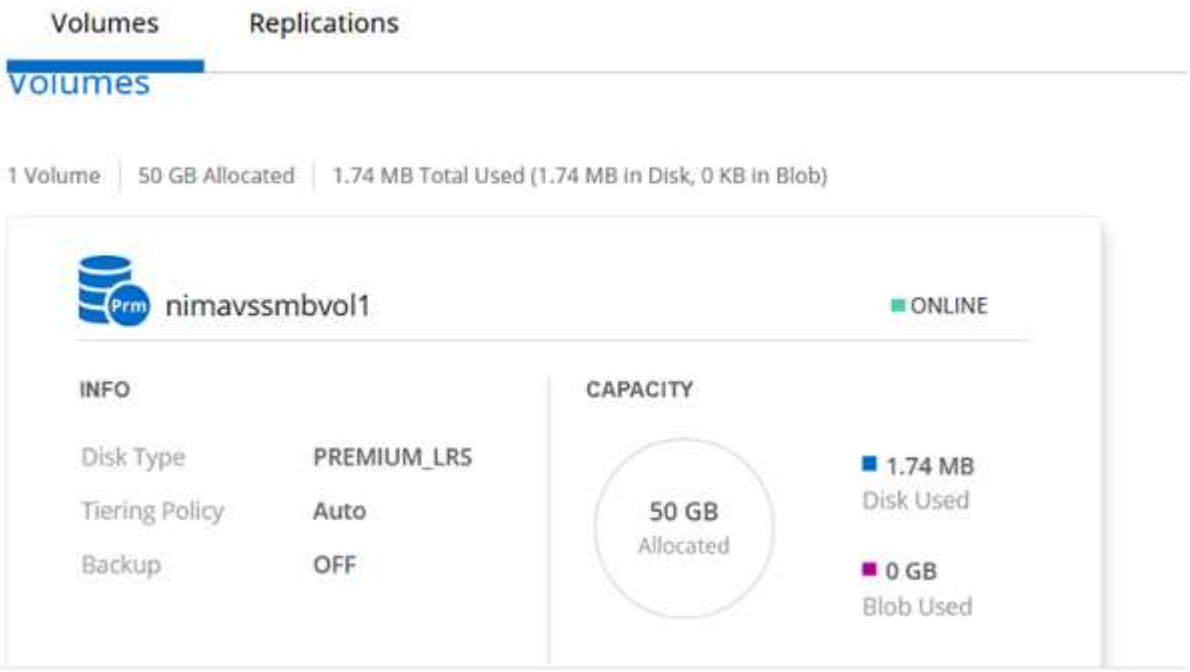
1. Depois que o ambiente de trabalho estiver pronto, certifique-se de que o servidor CIFS esteja configurado com os parâmetros de configuração de DNS e Active Directory apropriados. Esta etapa é necessária antes que você possa criar o volume SMB.



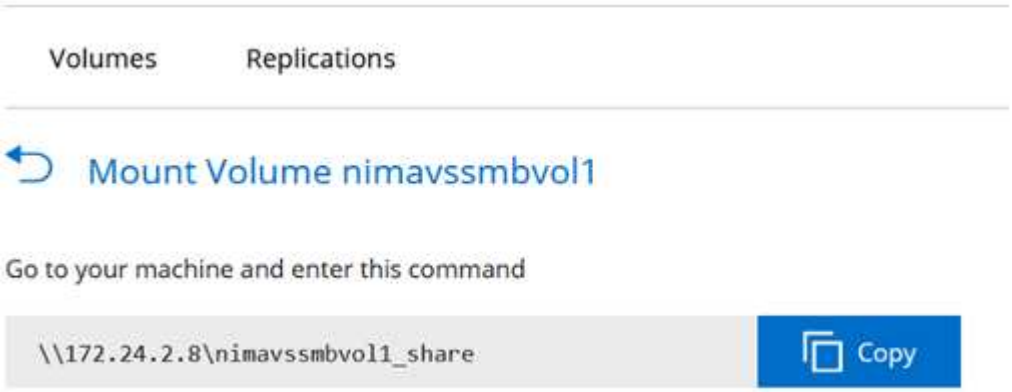
2. Criar o volume SMB é um processo fácil. Selecione a instância CVO para criar o volume e clique na opção Criar Volume. Escolha o tamanho apropriado e o gerenciador de nuvem escolhe o agregado que o contém ou usa o mecanismo de alocação avançado para colocar em um agregado específico. Para esta demonstração, o SMB foi selecionado como protocolo.

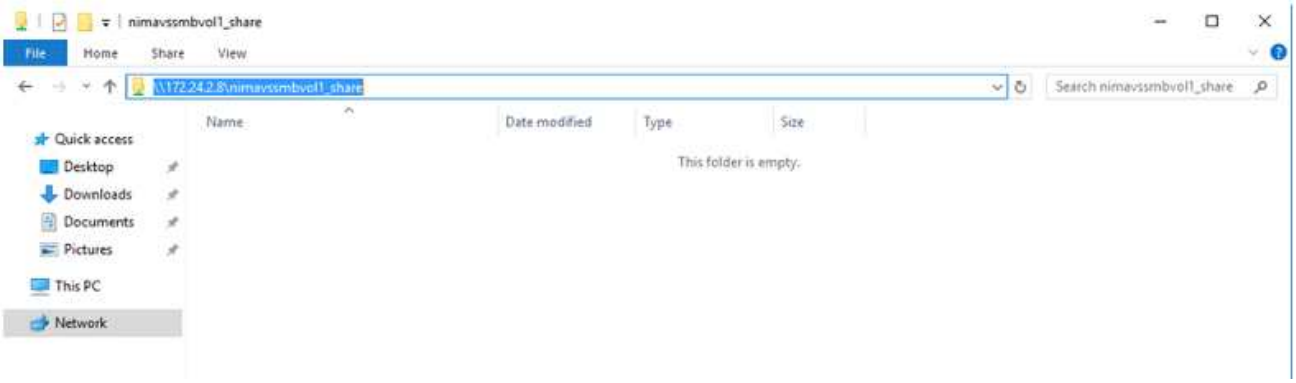


3. Depois que o volume for provisionado, ele ficará disponível no painel Volumes. Como um compartilhamento CIFS é provisionado, conceda aos seus usuários ou grupos permissão para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo. Esta etapa não é necessária se o volume for replicado de um ambiente local porque as permissões de arquivo e pasta são todas mantidas como parte da replicação do SnapMirror .



4. Após a criação do volume, use o comando mount para se conectar ao compartilhamento da VM em execução nos hosts SDDC do Azure VMware Solution.
5. Copie o caminho a seguir e use a opção Mapear unidade de rede para montar o volume na VM em execução no Azure VMware Solution SDDC.

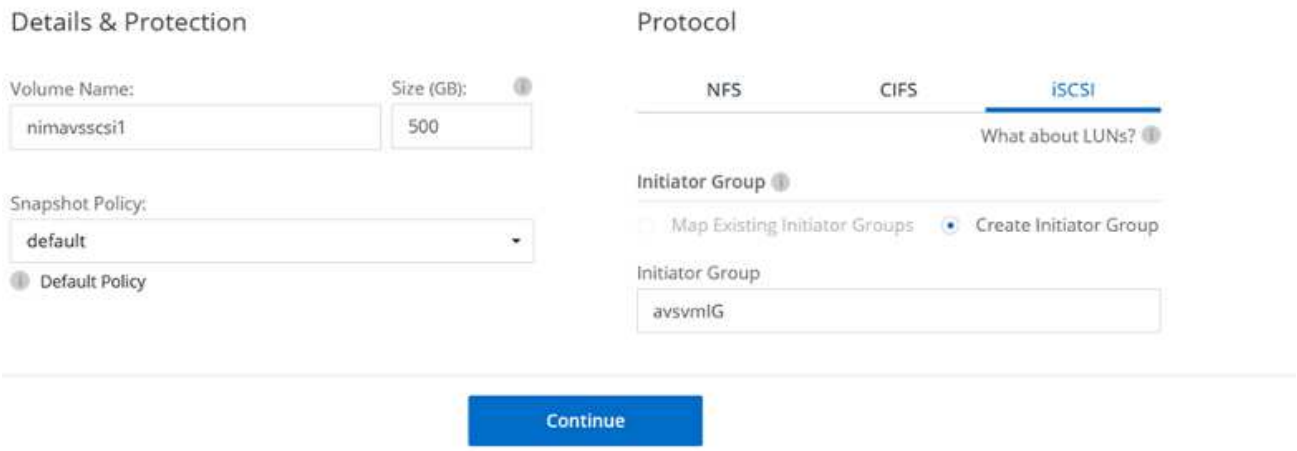




▼ **Conecte o LUN a um host**

Para conectar o LUN a um host, conclua as seguintes etapas:

1. Na página Canvas, clique duas vezes no ambiente de trabalho Cloud Volumes ONTAP para criar e gerenciar volumes.
2. Clique em Adicionar volume > Novo volume, selecione iSCSI e clique em Criar grupo de iniciadores. Clique em Continuar.



3. Após o provisionamento do volume, selecione-o e clique em IQN de destino. Para copiar o Nome Qualificado iSCSI (IQN), clique em Copiar. Configure uma conexão iSCSI do host para o LUN.

   Para fazer o mesmo para o host que reside no Azure VMware Solution SDDC:

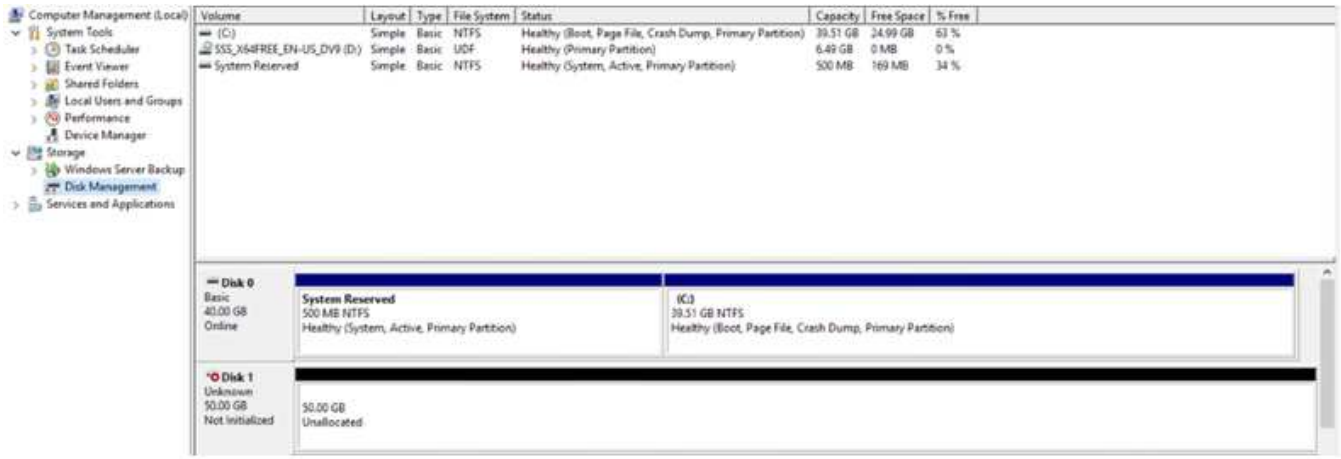
   a. RDP para a VM hospedada no Azure VMware Solution SDDC.
   b. Abra a caixa de diálogo Propriedades do Iniciador iSCSI: Gerenciador do Servidor > Painel > Ferramentas > Iniciador iSCSI.
   c. Na guia Descoberta, clique em Descobrir Portal ou Adicionar Portal e insira o endereço IP da porta de destino iSCSI.
   d. Na guia Destinos, selecione o alvo descoberto e clique em Fazer logon ou Conectar.
   e. Selecione Habilitar multicaminho e, em seguida, selecione Restaurar automaticamente esta conexão quando o computador iniciar ou Adicionar esta conexão à lista de destinos favoritos. Clique em Avançado.

      Observação: o host Windows deve ter uma conexão iSCSI com cada nó no cluster. O DSM nativo seleciona os melhores caminhos a serem usados.



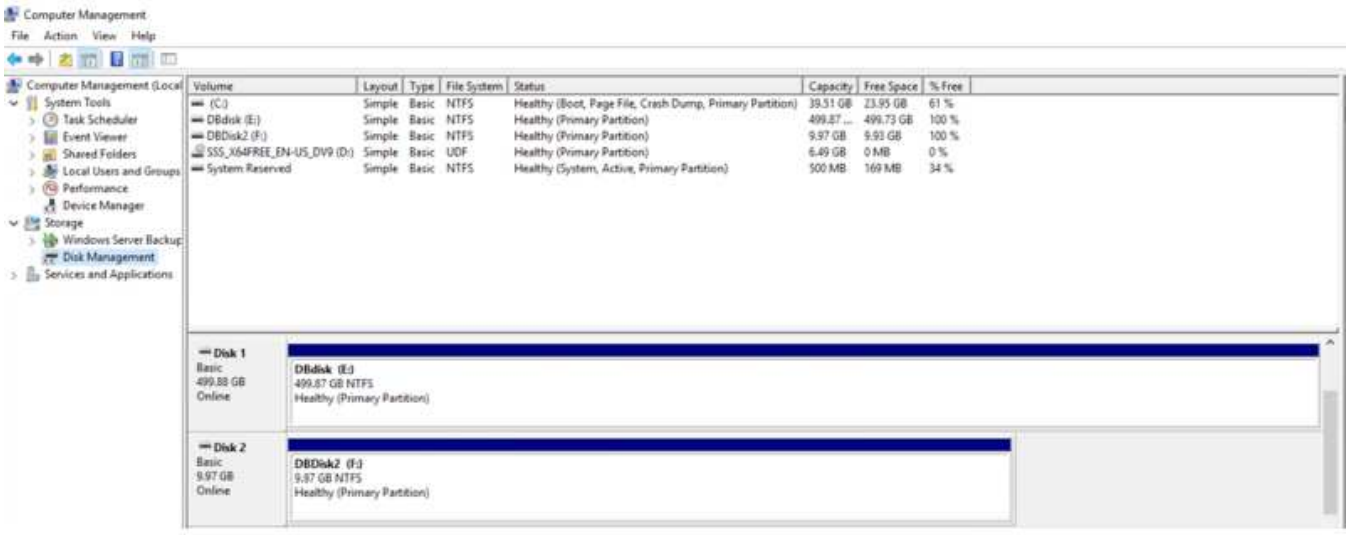
LUNs na máquina virtual de armazenamento (SVM) aparecem como discos para o host Windows. Nenhum novo disco adicionado é descoberto automaticamente pelo host. Inicie uma nova verificação manual para descobrir os discos concluindo as seguintes etapas:

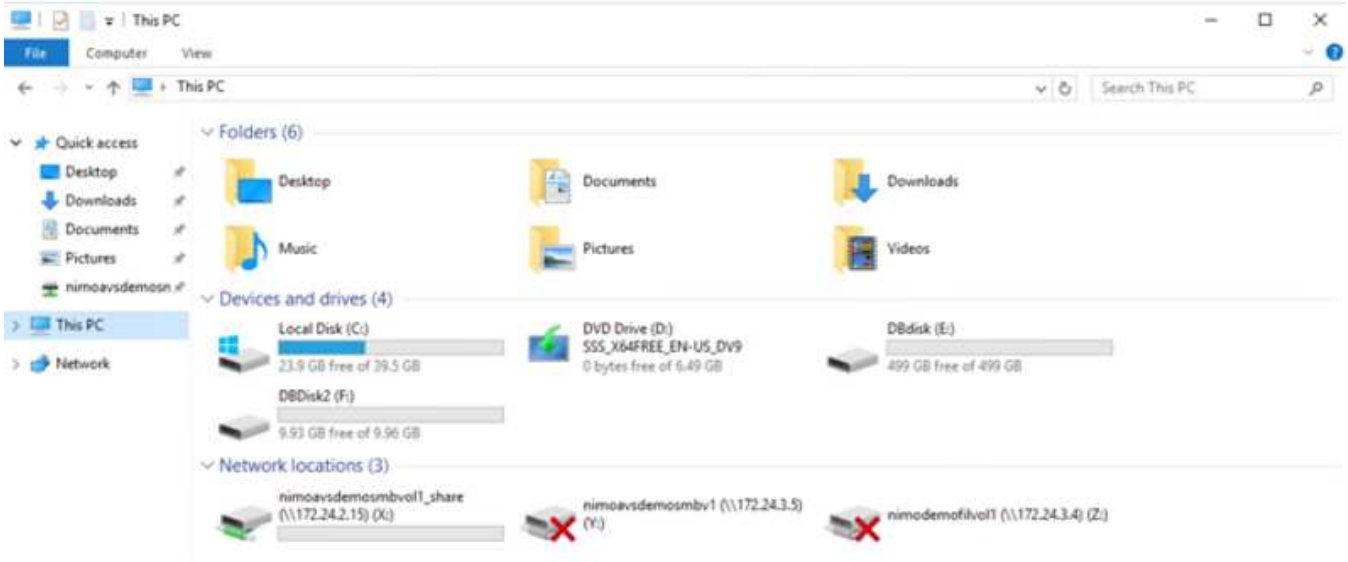
1. Abra o utilitário Gerenciamento do Computador do Windows: Iniciar > Ferramentas Administrativas > Gerenciamento do Computador.
2. Expanda o nó Armazenamento na árvore de navegação.
3. Clique em Gerenciamento de disco.
4. Clique em Ação > Reexaminar discos.



Quando um novo LUN é acessado pela primeira vez pelo host Windows, ele não tem partição ou sistema de arquivos. Inicialize o LUN e, opcionalmente, formate o LUN com um sistema de arquivos concluindo as seguintes etapas:

1. Inicie o Gerenciamento de Disco do Windows.
2. Clique com o botão direito do mouse no LUN e selecione o tipo de disco ou partição desejado.
3. Siga as instruções do assistente. Neste exemplo, a unidade E: está montada





Google Cloud VMware Engine: opções para usar o armazenamento NetApp

O armazenamento NetApp pode ser anexado ao Google Cloud Virtualization Engine como armazenamento conectado a convidado ou suplementar.

Google Cloud NetApp Volumes (NetApp Volumes) como um armazenamento de dados NFS suplementar

Os clientes que precisam de capacidade de armazenamento adicional em seu ambiente Google Cloud VMware Engine (GCVE) podem utilizar o Google Cloud NetApp Volumes para montar como armazenamento de dados NFS suplementar. Armazenar dados no Google Cloud NetApp Volumes permite que os clientes repliquem entre regiões para se protegerem de desastres.

Para mais informações, visite"Google Cloud NetApp Volumes (NetApp Volumes) como um armazenamento de dados NFS suplementar"

NetApp CVO como armazenamento conectado a convidados

O Cloud Volumes ONTAP, ou CVO, é a solução de gerenciamento de dados em nuvem líder do setor, desenvolvida no software de armazenamento ONTAP da NetApp, disponível nativamente na Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

É uma versão definida por software do ONTAP que consome armazenamento nativo da nuvem, permitindo que você tenha o mesmo software de armazenamento na nuvem e no local, reduzindo a necessidade de treinar novamente sua equipe de TI em métodos totalmente novos para gerenciar seus dados.

O CVO oferece aos clientes a capacidade de mover dados facilmente da borda para o data center, para a nuvem e vice-versa, reunindo sua nuvem híbrida — tudo gerenciado com um console de gerenciamento de painel único, o NetApp Cloud Manager.

Por design, o CVO oferece desempenho extremo e recursos avançados de gerenciamento de dados para satisfazer até mesmo seus aplicativos mais exigentes na nuvem.

Para mais informações, visite"NetApp CVO como armazenamento conectado a convidados"

Google Cloud NetApp Volumes (NetApp Volumes) como armazenamento conectado a convidados

Os compartilhamentos do Google Cloud NetApp Volumes podem ser montados a partir de VMs criadas no ambiente do VMware Engine. Os volumes também podem ser montados no cliente Linux e mapeados no cliente Windows porque o Google Cloud NetApp Volumes oferece suporte aos protocolos SMB e NFS. Os volumes do Google Cloud NetApp Volumes podem ser configurados em etapas simples.

O Google Cloud NetApp Volumes e a nuvem privada do Google Cloud VMware Engine devem estar na mesma região.

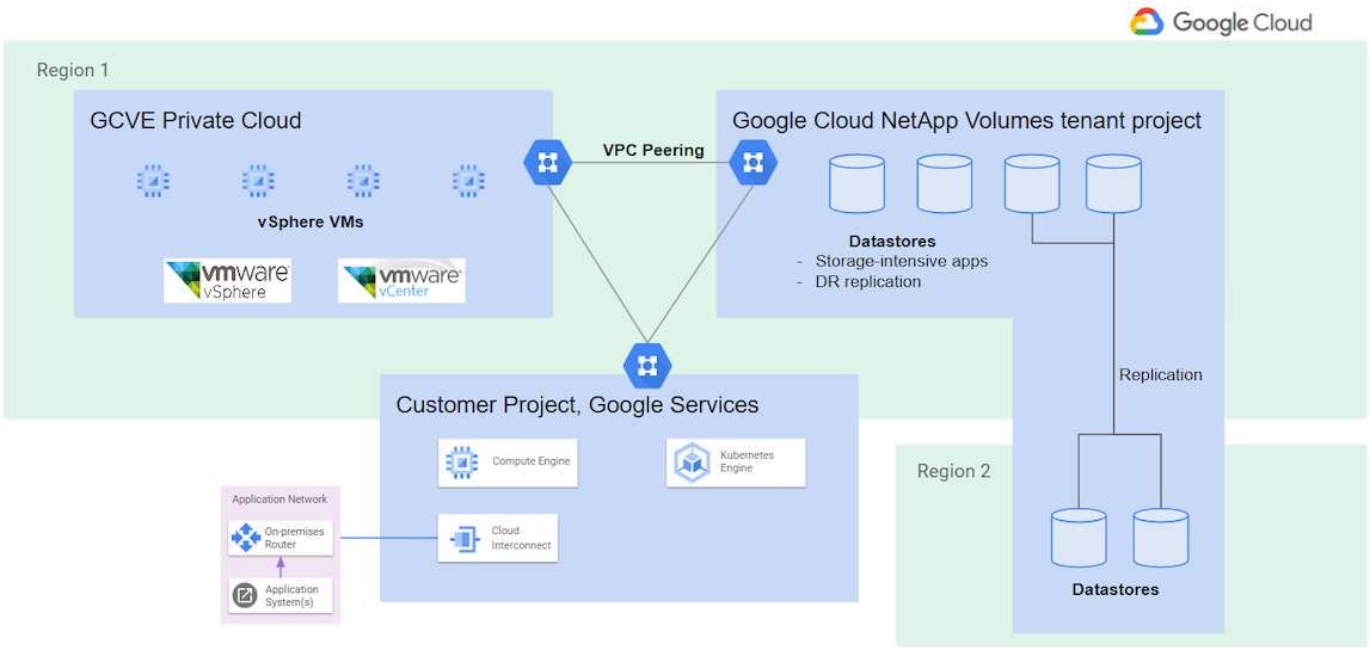
Para mais informações, visite"Google Cloud NetApp Volumes (NetApp Volumes) como armazenamento conectado a convidados"

Armazenamento de dados NFS suplementar do Google Cloud VMware Engine com Google Cloud NetApp Volumes

Os clientes podem expandir a capacidade de armazenamento no Google Cloud VMware Engine usando o armazenamento de dados suplementar NFS com o Google Cloud NetApp Volumes.

Visão geral

Os clientes que precisam de capacidade de armazenamento adicional em seu ambiente Google Cloud VMware Engine (GCVE) podem utilizar o Netapp Cloud Volume Service para montar como um armazenamento de dados NFS suplementar. Armazenar dados no Google Cloud NetApp Volumes permite que os clientes repliquem entre regiões para se protegerem de desastres.



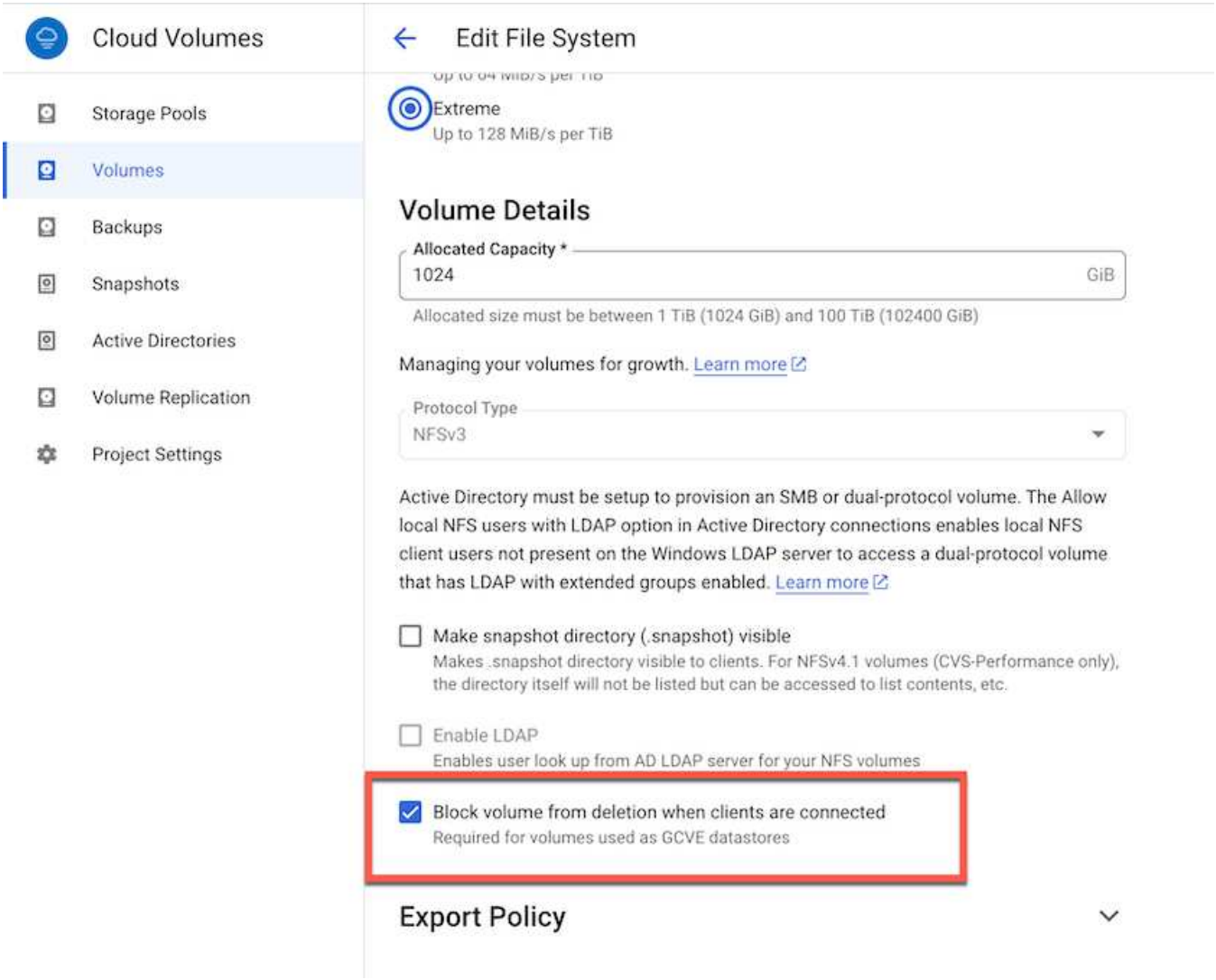
Etapas de implantação para montar o armazenamento de dados NFS do Google Cloud NetApp Volumes (NetApp Volumes) no GCVE

▼ **Provisionamento de volumes NetApp - Volume de desempenho**

O volume do Google Cloud NetApp Volumes pode ser provisionado por "Usando o Google Cloud Console" "Usando a CLI ou a API do Google Cloud"

▼ **Marque esse volume do NetApp Volumes como não excluível**

Para evitar a exclusão acidental do volume enquanto a máquina virtual estiver em execução, certifique-se de que o volume esteja marcado como não excluível conforme mostrado na captura de tela abaixo.



Para obter mais informações, consulte "Criando volume NFS" a documentação

▼ **Garanta que a Conexão Privada no GCVE exista para o NetApp Volumes Tenant VPC.**

Para montar o NFS Datastore, deve haver uma conexão privada entre o GCVE e o projeto NetApp Volumes. Para mais informações, consulte"Como configurar o acesso ao serviço privado"

▼ **Montar armazenamento de dados NFS**

Para obter instruções sobre como montar o armazenamento de dados NFS no GCVE, consulte"Como criar um armazenamento de dados NFS com o NetApp Volumes"

Como os hosts do vSphere são gerenciados pelo Google, você não tem acesso para instalar o NFS vSphere API for Array Integration (VAAI) vSphere Installation Bundle (VIB). Se precisar de suporte para Volumes Virtuais (vVol), avise-nos. Se você gosta de usar Jumbo Frames, consulte"Tamanhos máximos de MTU suportados no GCP"

Economias com o Google Cloud NetApp Volumes

Para saber mais sobre a economia potencial que você pode obter com o Google Cloud NetApp Volumes para suas necessidades de armazenamento no GCVE, consulte "Calculadora de ROI da NetApp"

Links de referência

- "Blog do Google - Como usar o NetApp Volumes como armazenamento de dados para o Google Cloud VMware Engine"
- "Blog da NetApp - Uma maneira melhor de migrar seus aplicativos com alto armazenamento para o Google Cloud"

Opções de armazenamento NetApp para GCP

O GCP oferece suporte ao armazenamento NetApp conectado a convidados com o Cloud Volumes ONTAP (CVO) ou o Google Cloud NetApp Volumes (NetApp Volumes).

Cloud Volumes ONTAP (CVO)

O Cloud Volumes ONTAP, ou CVO, é a solução de gerenciamento de dados em nuvem líder do setor, desenvolvida no software de armazenamento ONTAP da NetApp, disponível nativamente na Amazon Web Services (AWS), Microsoft Azure e Google Cloud Platform (GCP).

É uma versão definida por software do ONTAP que consome armazenamento nativo da nuvem, permitindo que você tenha o mesmo software de armazenamento na nuvem e no local, reduzindo a necessidade de treinar novamente sua equipe de TI em métodos totalmente novos para gerenciar seus dados.

O CVO oferece aos clientes a capacidade de mover dados facilmente da borda para o data center, para a nuvem e vice-versa, reunindo sua nuvem híbrida — tudo gerenciado com um console de gerenciamento de painel único, o NetApp Cloud Manager.

Por design, o CVO oferece desempenho extremo e recursos avançados de gerenciamento de dados para satisfazer até mesmo seus aplicativos mais exigentes na nuvem

Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados

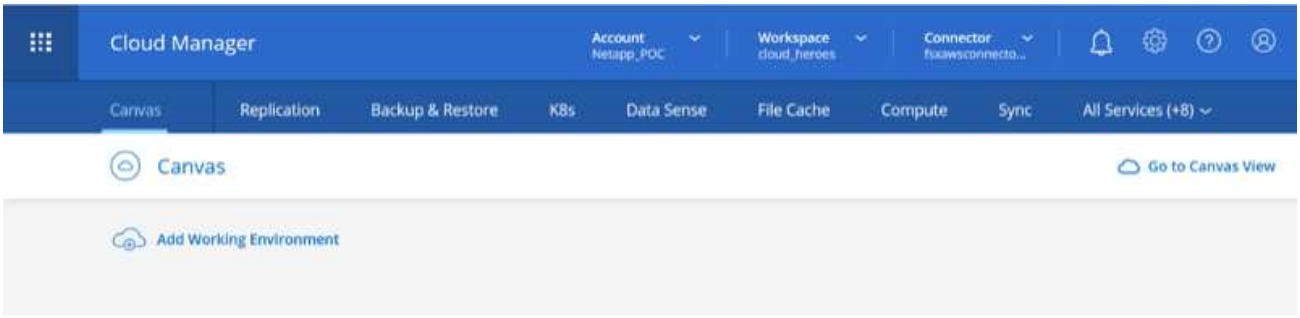
▼ **Implantar o Cloud Volumes ONTAP no Google Cloud (faça você mesmo)**

Os compartilhamentos Cloud Volumes ONTAP podem ser montados a partir de VMs criadas no ambiente de nuvem privada do GCVE. Os volumes também podem ser montados no cliente Linux e no cliente Windows, e os LUNS podem ser acessados em clientes Linux ou Windows como dispositivos de bloco quando montados sobre iSCSI, porque o Cloud Volumes ONTAP oferece suporte aos protocolos iSCSI, SMB e NFS. Os volumes Cloud Volumes ONTAP podem ser configurados em algumas etapas simples.

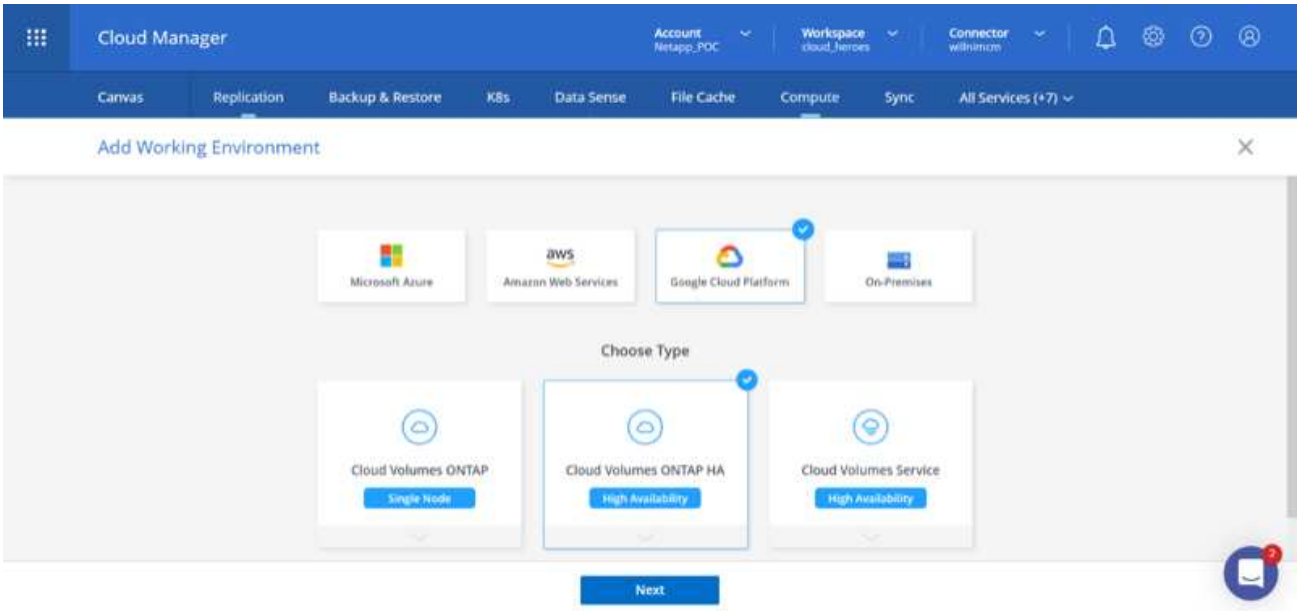
Para replicar volumes de um ambiente local para a nuvem para fins de recuperação de desastres ou migração, estabeleça conectividade de rede com o Google Cloud, usando uma VPN site a site ou o Cloud Interconnect. A replicação de dados locais para o Cloud Volumes ONTAP está fora do escopo deste documento. Para replicar dados entre sistemas locais e Cloud Volumes ONTAP , consulte"Configurando a replicação de dados entre sistemas" .

> Utilize "Dimensionador Cloud Volumes ONTAP" para dimensionar com precisão as instâncias do Cloud Volumes ONTAP. Monitore também o desempenho no local para usar como entrada no dimensionador do Cloud Volumes ONTAP.

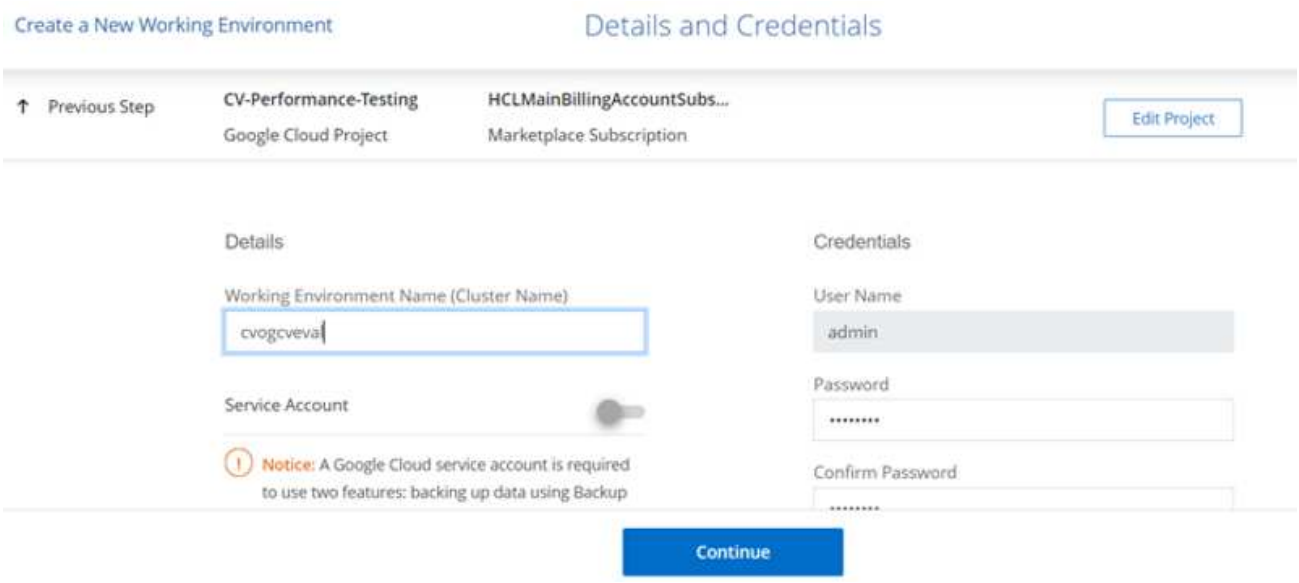
1. Efetue login no NetApp Cloud Central — a tela Fabric View é exibida. Localize a guia Cloud Volumes ONTAP e selecione Ir para o Cloud Manager. Após efetuar login, a tela Canvas será exibida.



2. Na guia Cloud Manager Canvas, clique em Adicionar um ambiente de trabalho e selecione Google Cloud Platform como a nuvem e o tipo de configuração do sistema. Em seguida, clique em Avançar.



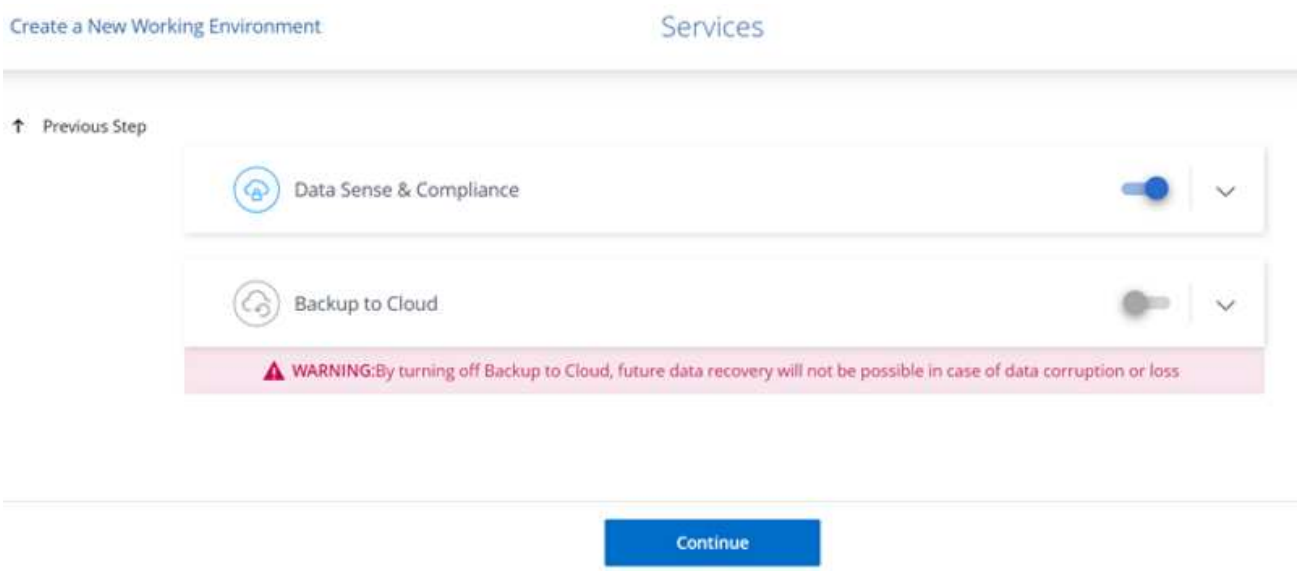
3. Forneça os detalhes do ambiente a ser criado, incluindo o nome do ambiente e as credenciais do administrador. Após terminar, clique em Continuar.



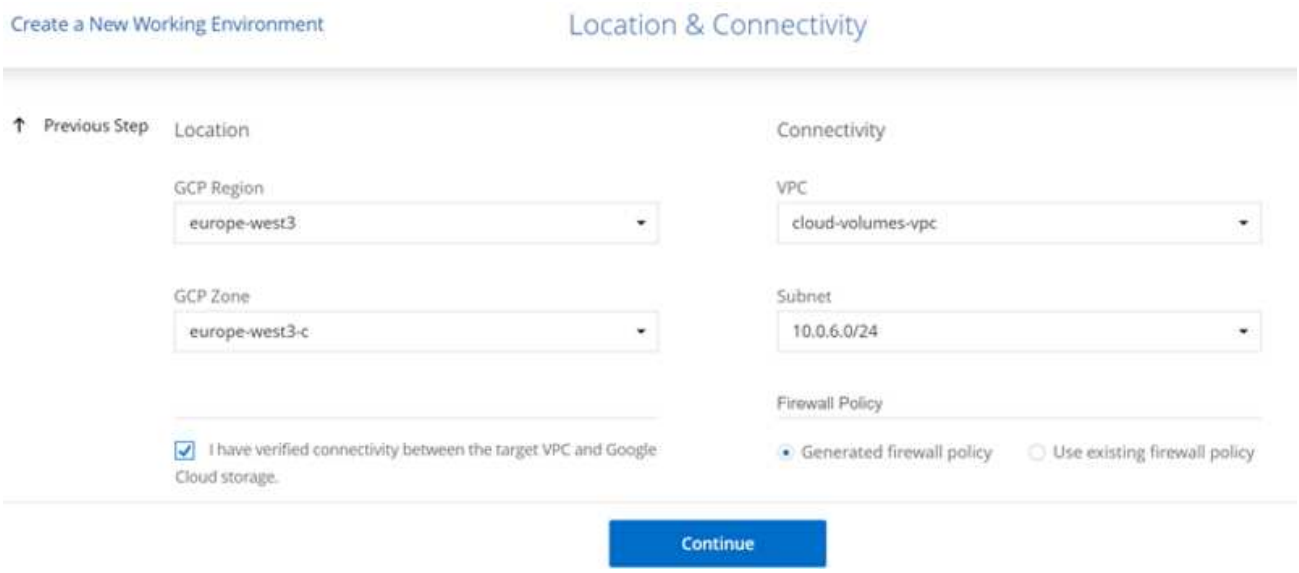
4. Selecione ou desmarque os serviços complementares para implantação do Cloud Volumes ONTAP ,

incluindo Data Sense & Compliance ou Backup to Cloud. Em seguida, clique em Continuar.

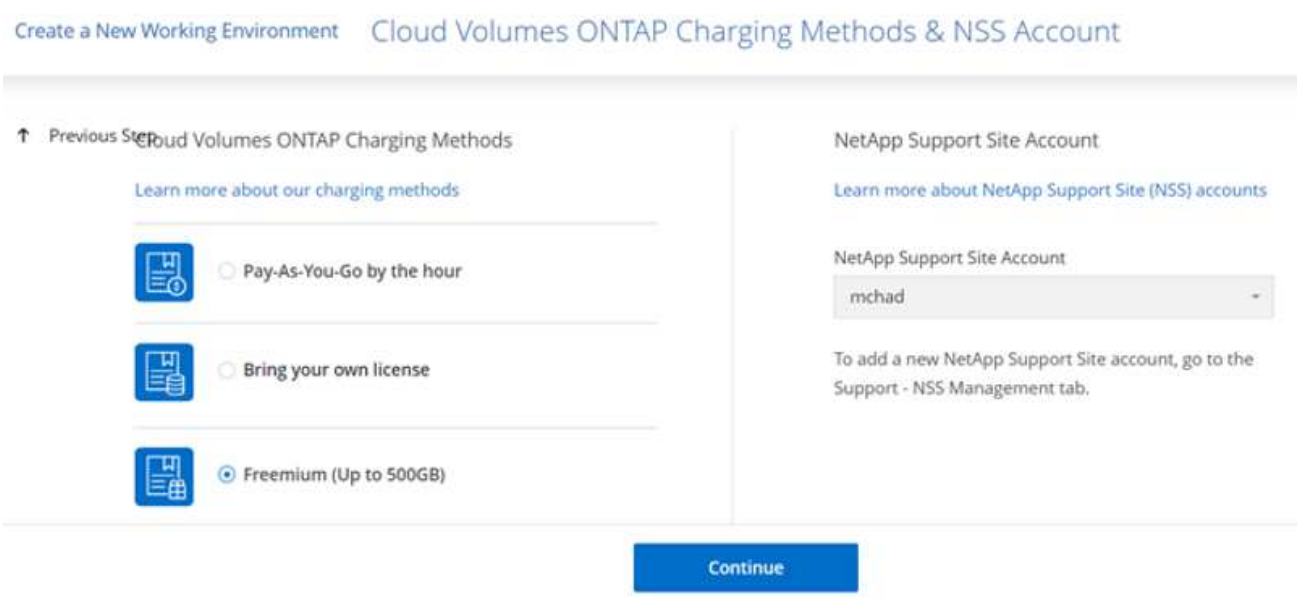
DICA: Uma mensagem pop-up de verificação será exibida ao desativar serviços complementares. Serviços complementares podem ser adicionados/removidos após a implantação do CVO. Considere desmarcá-los se não forem necessários desde o início para evitar custos.



5. Selecione um local, escolha uma política de firewall e marque a caixa de seleção para confirmar a conectividade de rede com o armazenamento do Google Cloud.

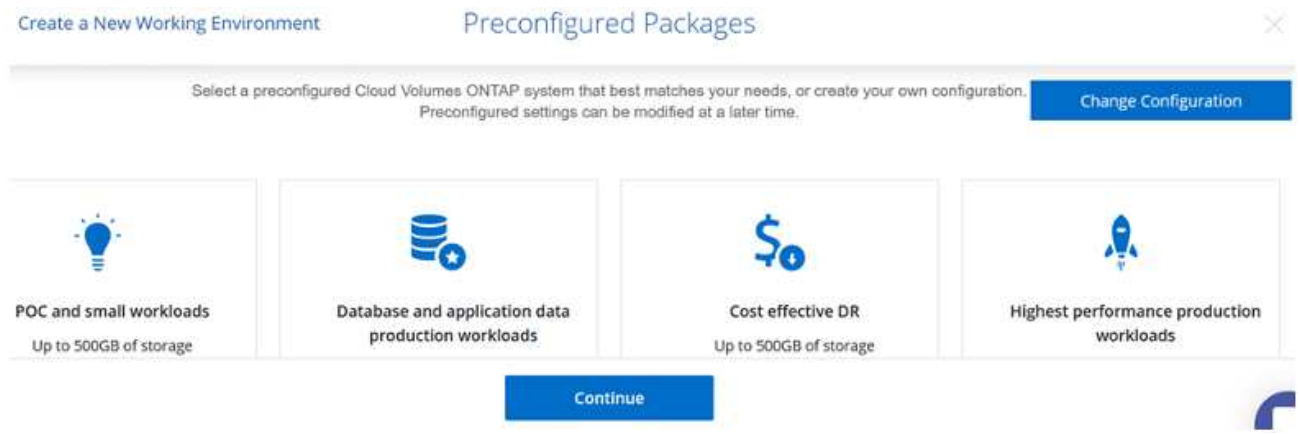


6. Selecione a opção de licença: Pague conforme o uso ou BYOL para usar a licença existente. Neste exemplo, a opção Freemium é usada. Em seguida, clique em Continuar.

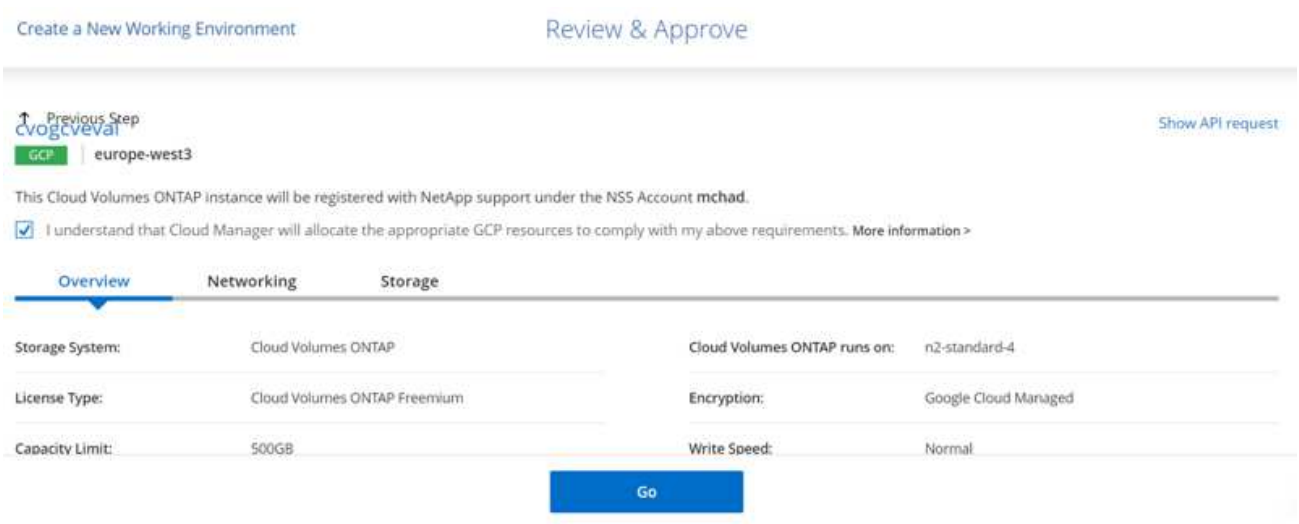


7. Selecione entre vários pacotes pré-configurados disponíveis com base no tipo de carga de trabalho que será implantada nas VMs em execução na nuvem VMware no AWS SDDC.

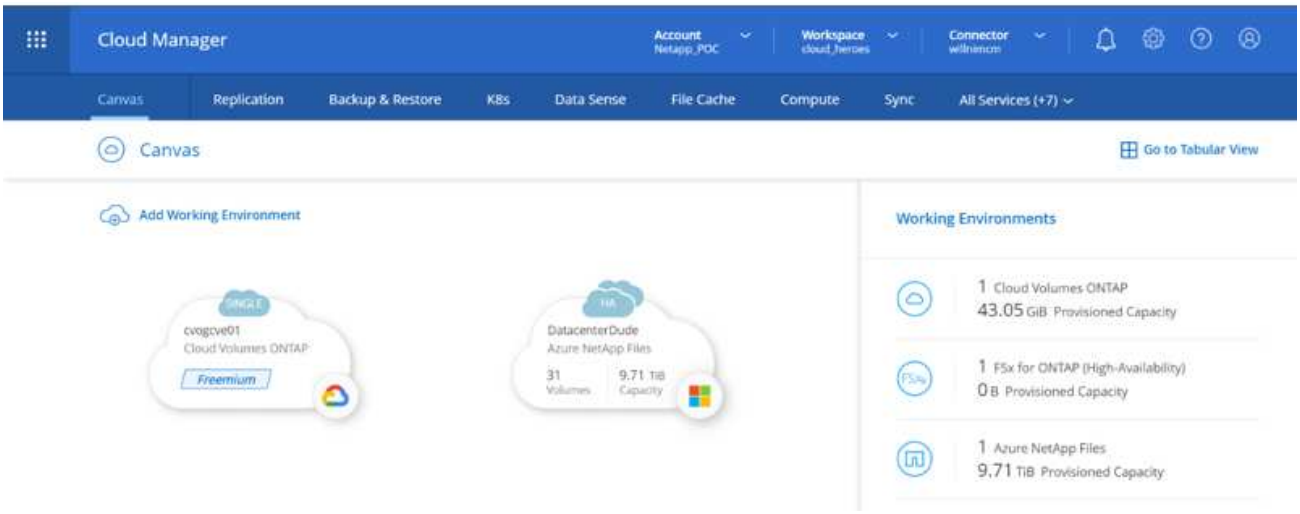
   DICA: Passe o mouse sobre os blocos para obter detalhes ou personalize os componentes do CVO e a versão do ONTAP clicando em Alterar configuração.



8. Na página Revisar e aprovar, revise e confirme as seleções. Para criar a instância do Cloud Volumes ONTAP , clique em Ir.



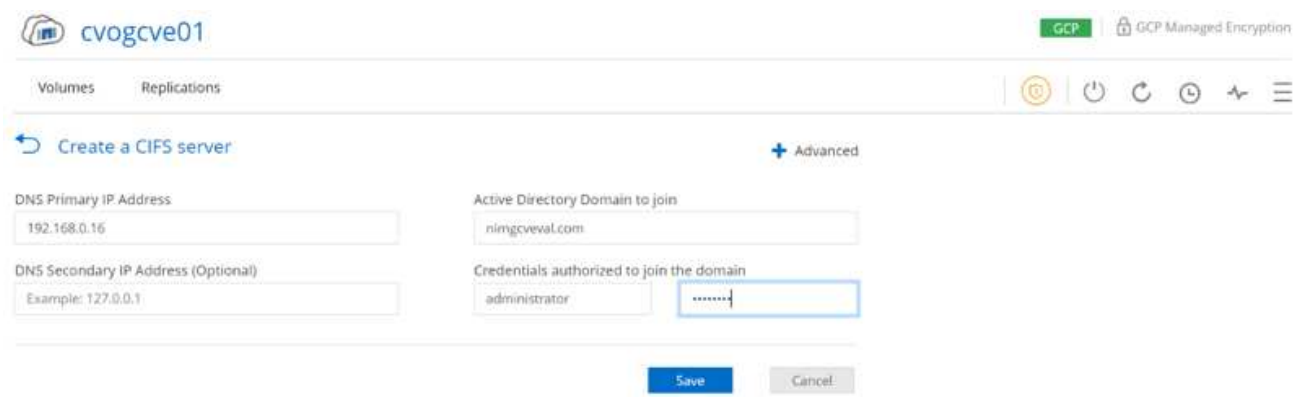
9. Depois que o Cloud Volumes ONTAP é provisionado, ele é listado nos ambientes de trabalho na página Canvas.



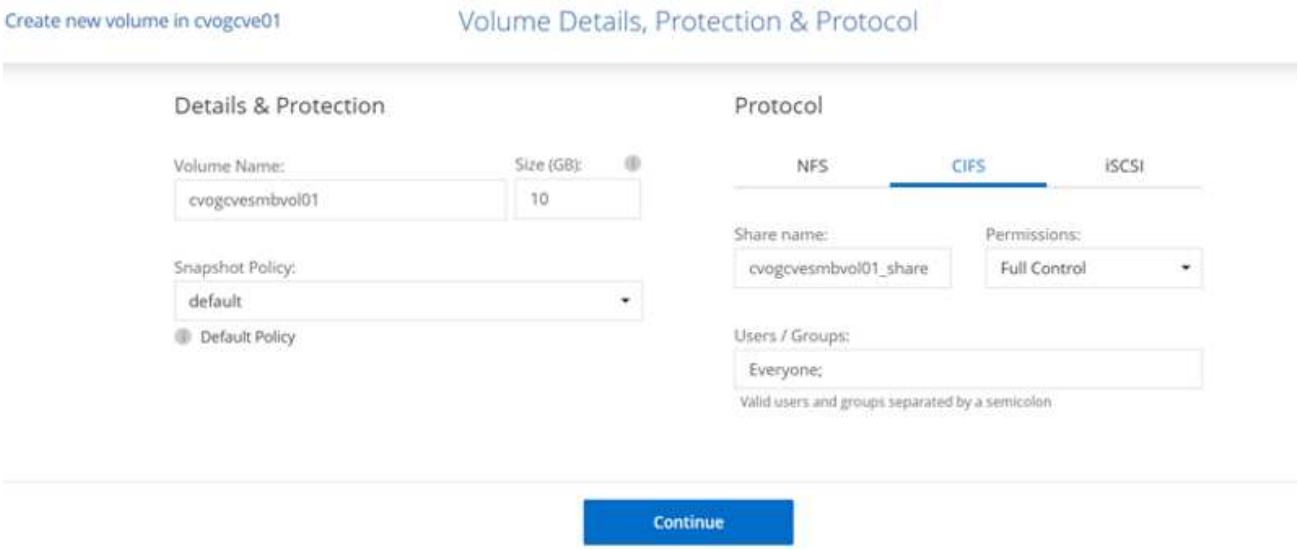
▼ **Configurações adicionais para volumes SMB**

1. Depois que o ambiente de trabalho estiver pronto, certifique-se de que o servidor CIFS esteja configurado com os parâmetros de configuração de DNS e Active Directory apropriados. Esta etapa é necessária antes que você possa criar o volume SMB.

   DICA: Clique no ícone Menu (º), selecione Avançado para exibir mais opções e selecione Configuração CIFS.



2. Criar o volume SMB é um processo fácil. No Canvas, clique duas vezes no ambiente de trabalho Cloud Volumes ONTAP para criar e gerenciar volumes e clique na opção Criar Volume. Escolha o tamanho apropriado e o gerenciador de nuvem escolhe o agregado que o contém ou usa o mecanismo de alocação avançado para colocar em um agregado específico. Para esta demonstração, CIFS/SMB foi selecionado como protocolo.



3. Depois que o volume for provisionado, ele ficará disponível no painel Volumes. Como um compartilhamento CIFS é provisionado, conceda aos seus usuários ou grupos permissão para os arquivos e pastas e verifique se esses usuários podem acessar o compartilhamento e criar um arquivo. Esta etapa não é necessária se o volume for replicado de um ambiente local porque as permissões de arquivo e pasta são todas mantidas como parte da replicação do SnapMirror .

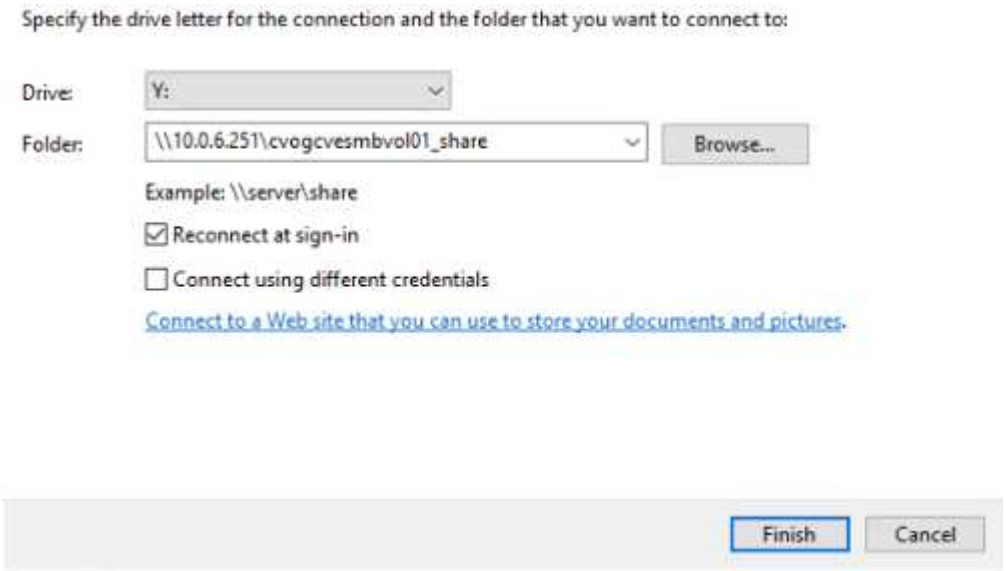
   DICA: Clique no menu de volume (º) para exibir suas opções.



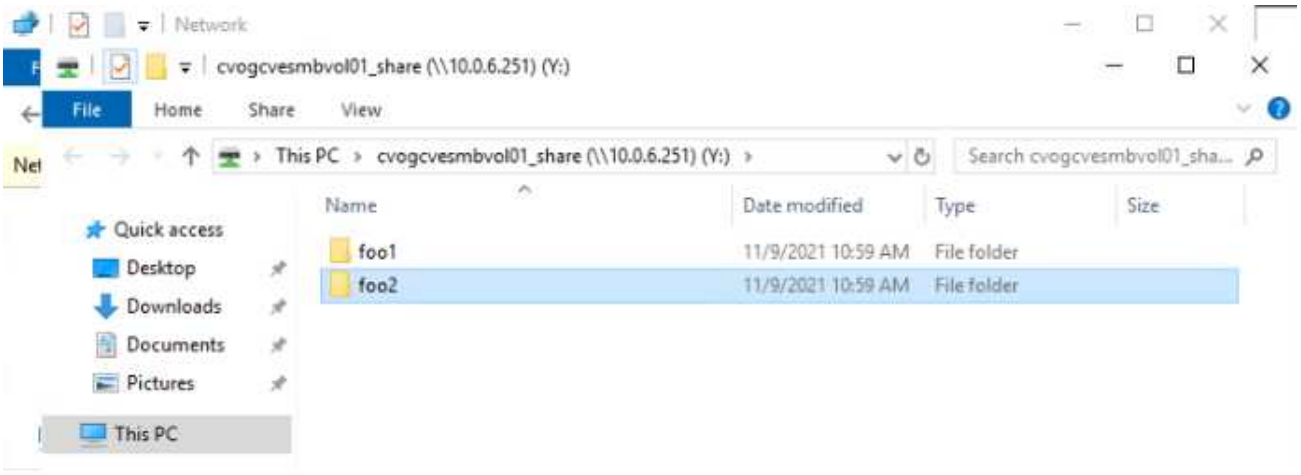
4. Após a criação do volume, use o comando mount para exibir as instruções de conexão do volume e, em seguida, conecte-se ao compartilhamento a partir das VMs no Google Cloud VMware Engine.



5. Copie o caminho a seguir e use a opção Mapear unidade de rede para montar o volume na VM em execução no Google Cloud VMware Engine.



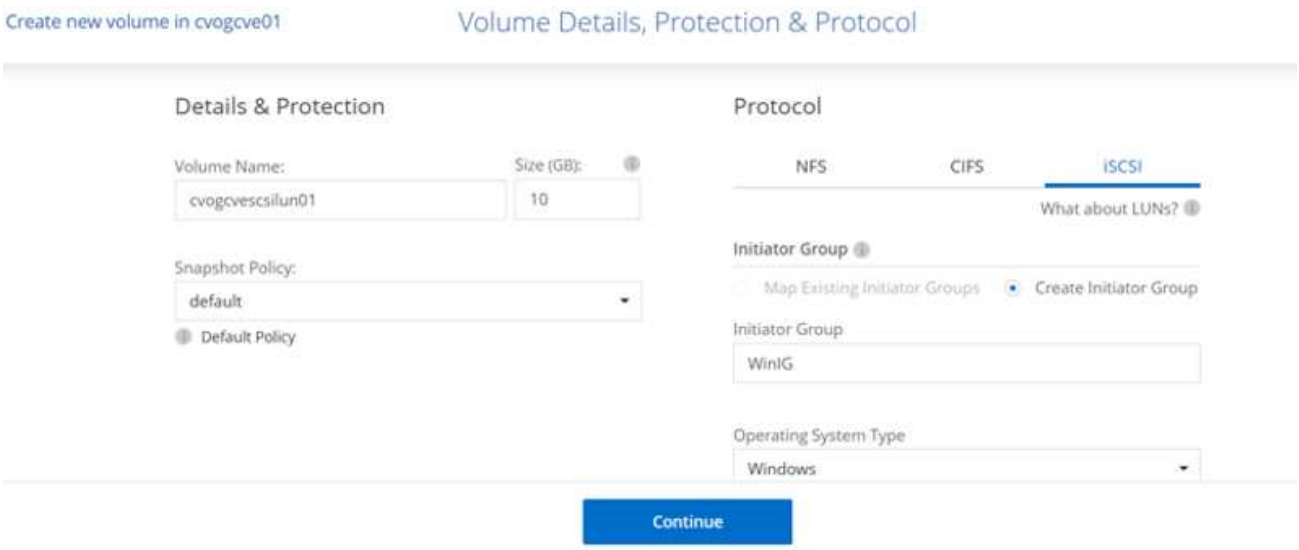
Uma vez mapeado, ele pode ser acessado facilmente, e as permissões NTFS podem ser definidas adequadamente.

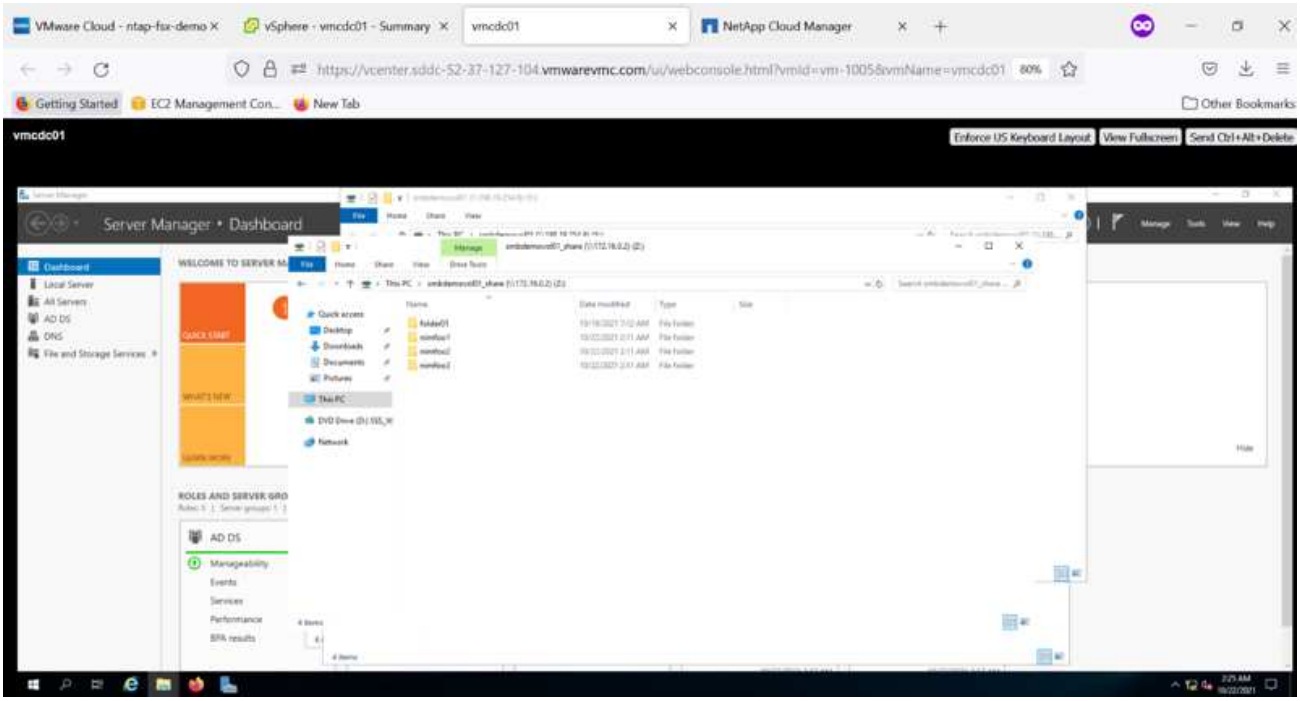


▼ Conecte o LUN no Cloud Volumes ONTAP a um host

Para conectar o LUN ONTAP dos volumes de nuvem a um host, conclua as seguintes etapas:

1. Na página Canvas, clique duas vezes no ambiente de trabalho Cloud Volumes ONTAP para criar e gerenciar volumes.
2. Clique em Adicionar volume > Novo volume, selecione iSCSI e clique em Criar grupo de iniciadores. Clique em Continuar.





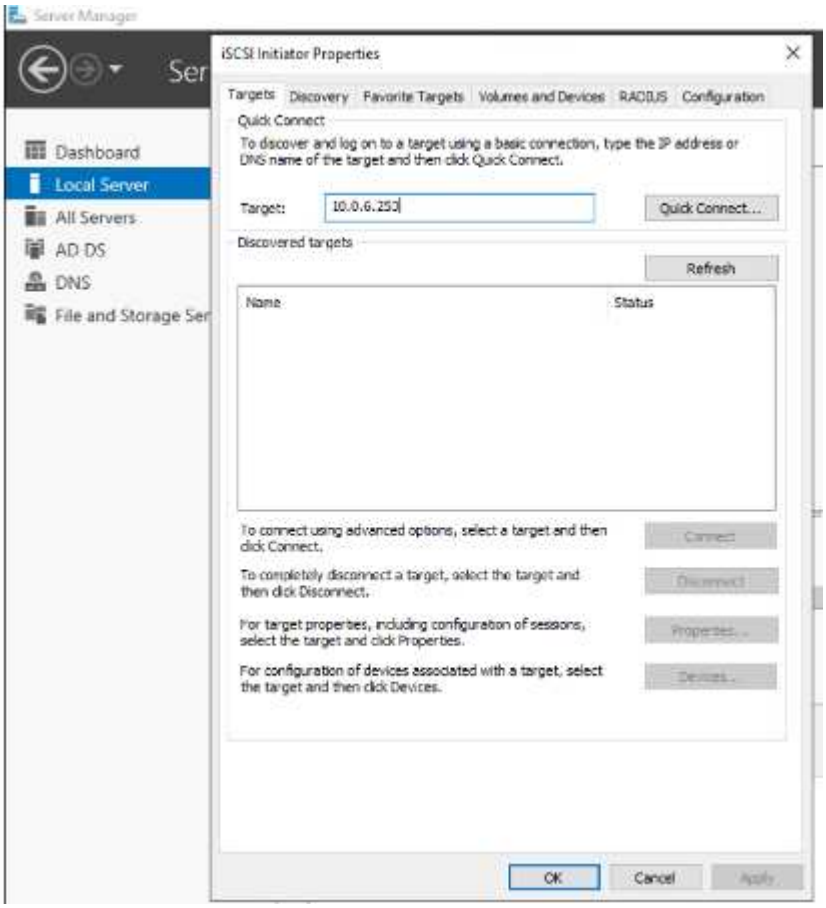
3. Após o provisionamento do volume, selecione o menu de volume (º) e clique em Target iQN. Para copiar o Nome Qualificado iSCSI (iQN), clique em Copiar. Configure uma conexão iSCSI do host para o LUN.

Para fazer o mesmo para o host residente no Google Cloud VMware Engine:

1. RDP para a VM hospedada no Google Cloud VMware Engine.
2. Abra a caixa de diálogo Propriedades do Iniciador iSCSI: Gerenciador do Servidor > Painel > Ferramentas > Iniciador iSCSI.

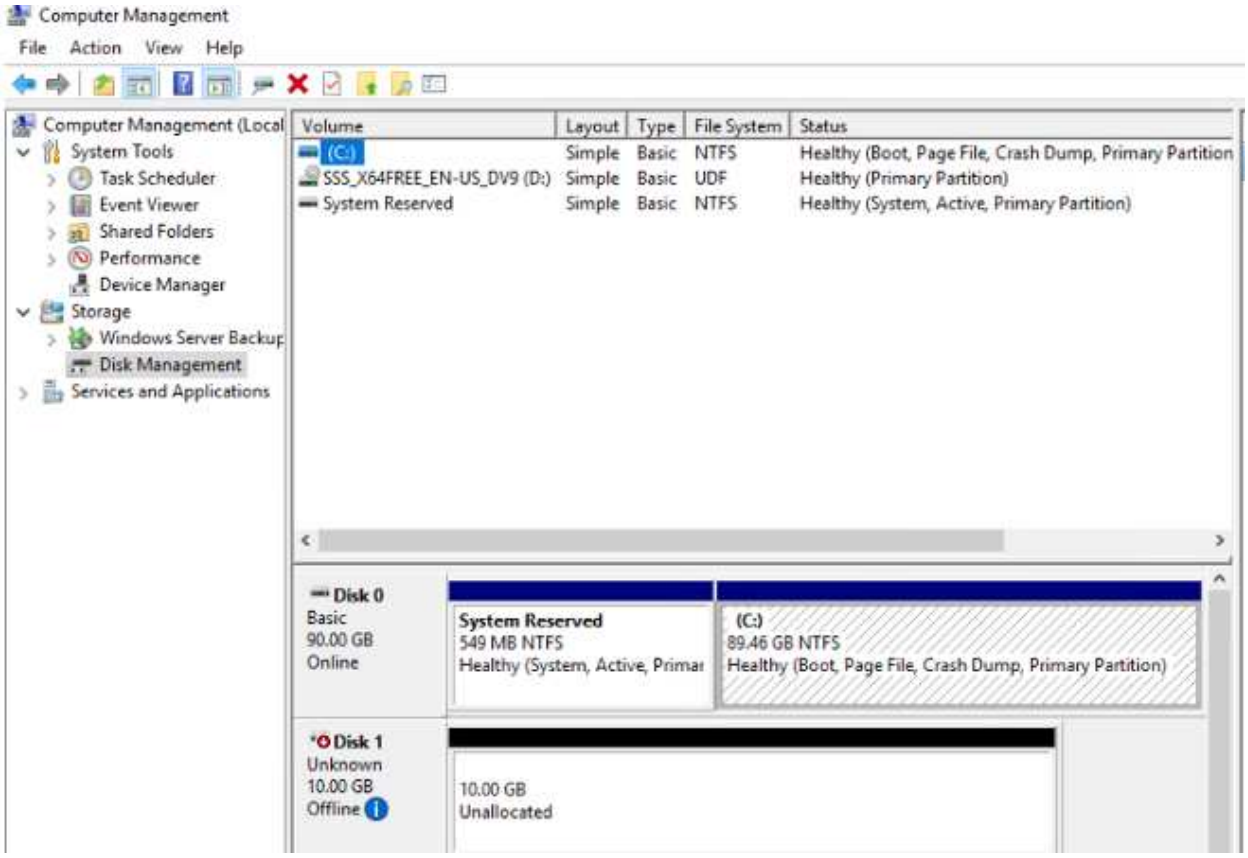
3. Na guia Descoberta, clique em Descobrir Portal ou Adicionar Portal e insira o endereço IP da porta de destino iSCSI.
4. Na guia Destinos, selecione o alvo descoberto e clique em Fazer logon ou Conectar.
5. Selecione Habilitar multicaminho e, em seguida, selecione Restaurar automaticamente esta conexão quando o computador iniciar ou Adicionar esta conexão à lista de destinos favoritos. Clique em Avançado.

> O host do Windows deve ter uma conexão iSCSI com cada nó no cluster. O DSM nativo seleciona os melhores caminhos a serem usados.



LUNs na máquina virtual de armazenamento (SVM) aparecem como discos para o host Windows. Nenhum novo disco adicionado é descoberto automaticamente pelo host. Inicie uma nova verificação manual para descobrir os discos concluindo as seguintes etapas:

a. Abra o utilitário Gerenciamento do Computador do Windows: Iniciar > Ferramentas Administrativas > Gerenciamento do Computador.
b. Expanda o nó Armazenamento na árvore de navegação.
c. Clique em Gerenciamento de disco.
d. Clique em Ação > Reexaminar discos.

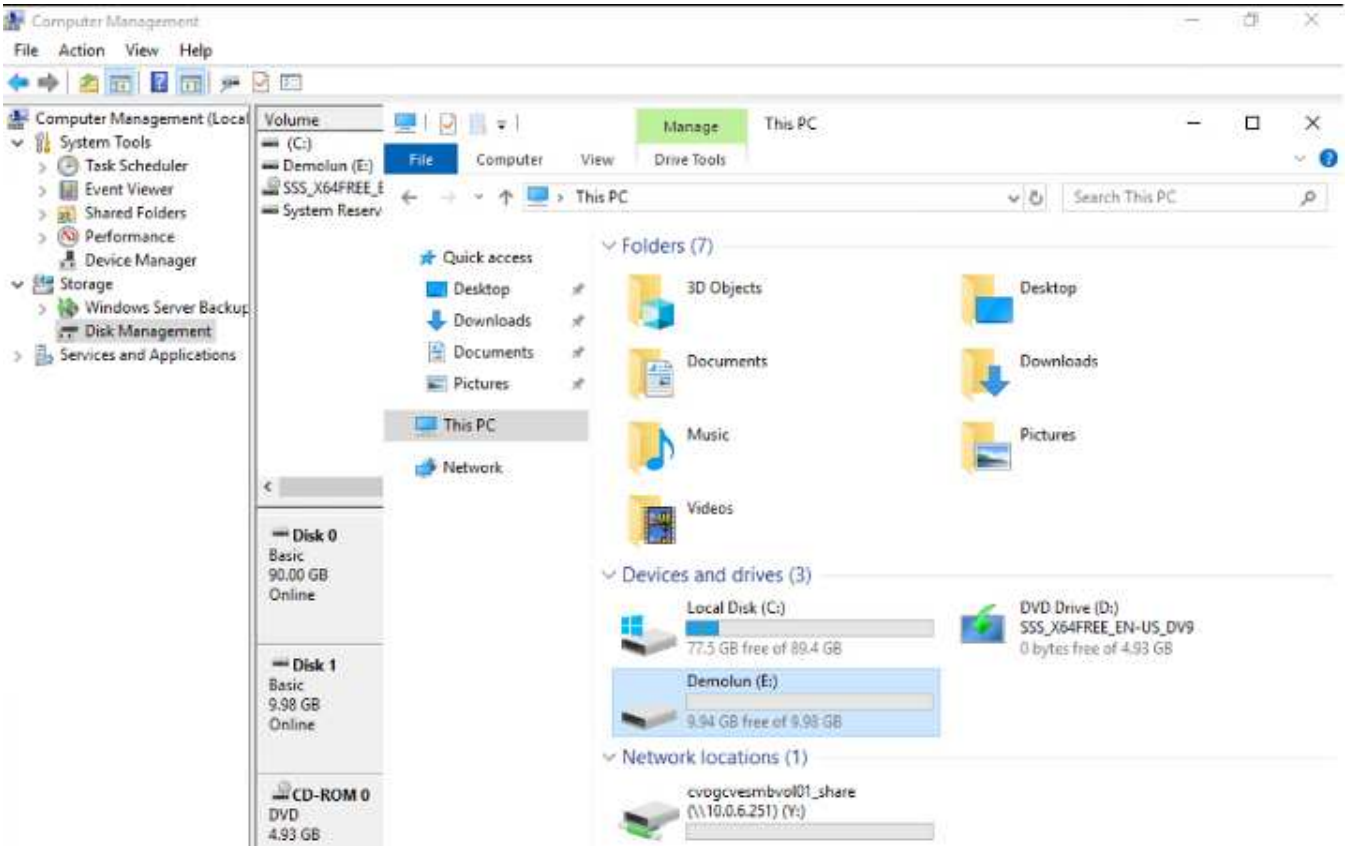


Quando um novo LUN é acessado pela primeira vez pelo host Windows, ele não tem partição ou sistema de arquivos. Inicialize o LUN e, opcionalmente, formate o LUN com um sistema de arquivos concluindo as seguintes etapas:

a. Inicie o Gerenciamento de Disco do Windows.

b. Clique com o botão direito do mouse no LUN e selecione o tipo de disco ou partição desejado.

c. Siga as instruções do assistente. Neste exemplo, a unidade F: está montada.



Nos clientes Linux, certifique-se de que o daemon iSCSI esteja em execução. Depois que os LUNs forem provisionados, consulte as orientações detalhadas sobre configuração de iSCSI com o Ubuntu como exemplo aqui. Para verificar, execute lsblk cmd no shell.

```
nlyaz@nlmubu01:~$ lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0    7:0    0 55.4M  1 loop /snap/core18/2128
loop1    7:1    0  219M  1 loop /snap/gnome-3-34-1804/72
loop2    7:2    0 65.1M  1 loop /snap/gtk-common-themes/1515
loop3    7:3    0   51M  1 loop /snap/snap-store/547
loop4    7:4    0 32.3M  1 loop /snap/snapd/12704
loop5    7:5    0 32.5M  1 loop /snap/snapd/13640
loop6    7:6    0 55.5M  1 loop /snap/core18/2246
loop7    7:7    0    4K  1 loop /snap/bare/5
loop8    7:8    0 65.2M  1 loop /snap/gtk-common-themes/1519
sda      8:0    0   16G  0 disk
├─sda1   8:1    0  512M  0 part /boot/efi
├─sda2   8:2    0    1K  0 part
└─sda5   8:5    0 15.5G  0 part /
sdb      8:16   0    1G  0 disk
```

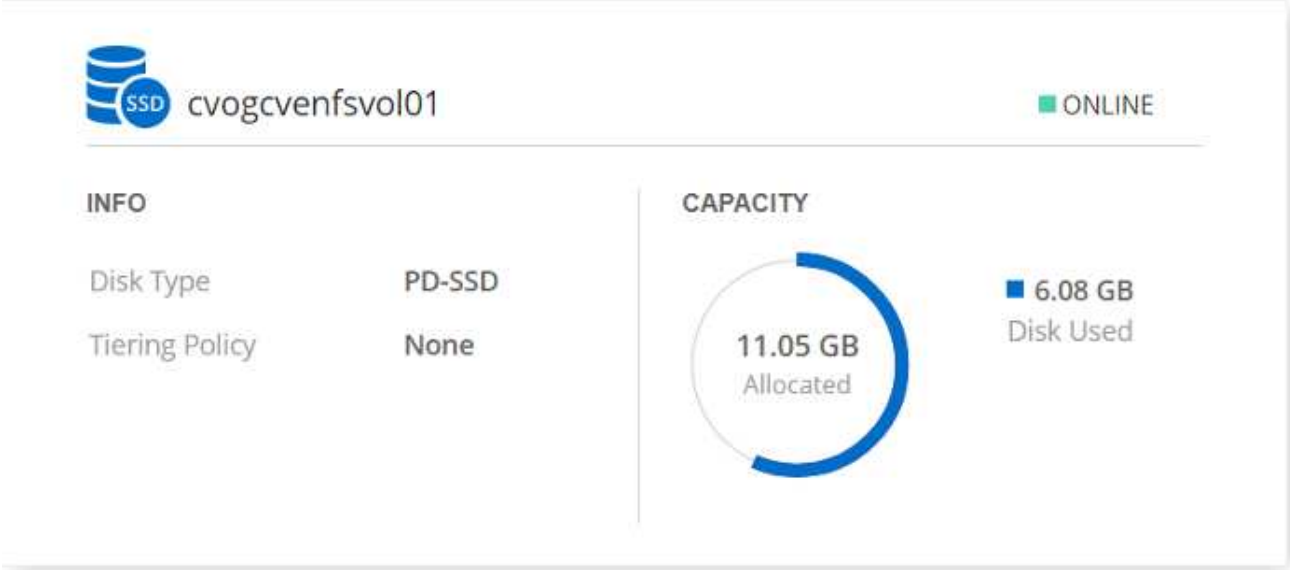
```
niyaz@nimubu01:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           394M  1.5M  392M   1% /run
/dev/sda5        16G  7.6G  6.9G  53% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M     0  5.0M   0% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop1      219M  219M     0 100% /snap/gnome-3-34-1804/72
/dev/loop2       66M   66M     0 100% /snap/gtk-common-themes/1515
/dev/loop3       51M   51M     0 100% /snap/snap-store/547
/dev/loop0       56M   56M     0 100% /snap/core18/2128
/dev/loop4       33M   33M     0 100% /snap/snapd/12704
/dev/sda1       511M  4.0K  511M   1% /boot/efi
tmpfs           394M   64K  394M   1% /run/user/1000
/dev/loop5       33M   33M     0 100% /snap/snapd/13640
/dev/loop6       56M   56M     0 100% /snap/core18/2246
/dev/loop7      128K  128K     0 100% /snap/bare/5
/dev/loop8       66M   66M     0 100% /snap/gtk-common-themes/1519
/dev/sdb        976M  2.6M  907M   1% /mnt
```

▼ **Montar Cloud Volumes ONTAP Volumes no cliente Linux**

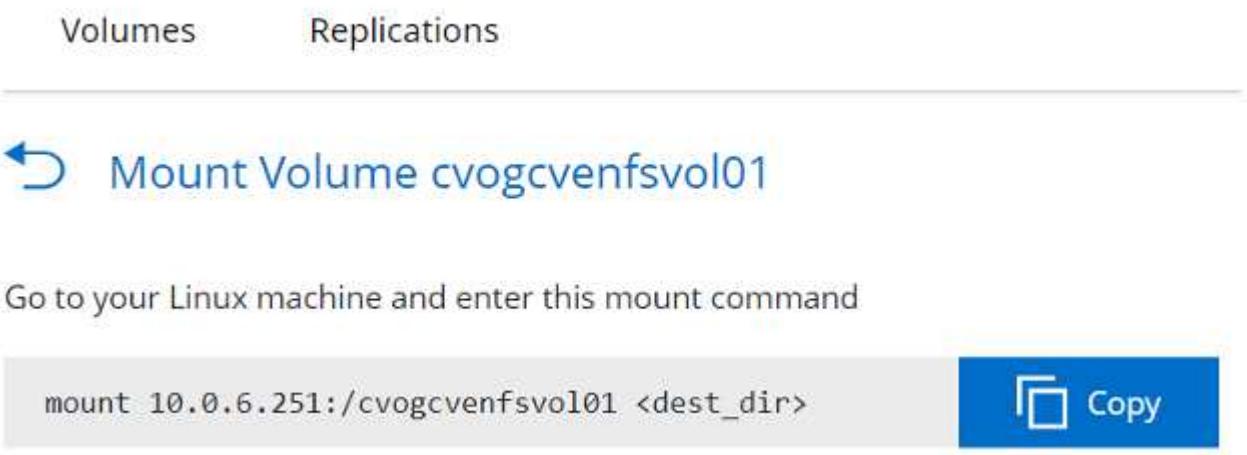
Para montar o sistema de arquivos Cloud Volumes ONTAP (DIY) de VMs no Google Cloud VMware Engine, siga as etapas abaixo:

Provisione o volume seguindo as etapas abaixo

1. Na guia Volumes, clique em Criar novo volume.
2. Na página Criar novo volume, selecione um tipo de volume:



3. Na aba Volumes, coloque o cursor do mouse sobre o volume, selecione o ícone de menu (º) e clique em Montar Comando.



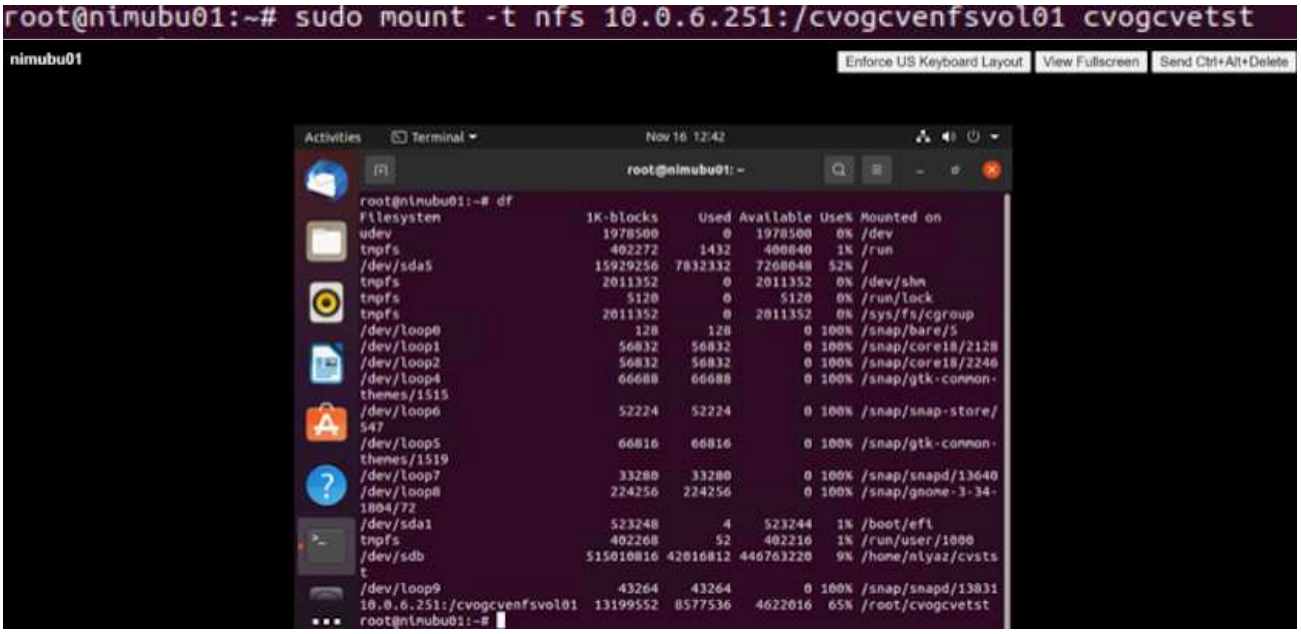
4. Clique em Copiar.
5. Conecte-se à instância Linux designada.
6. Abra um terminal na instância usando shell seguro (SSH) e faça login com as credenciais apropriadas.
7. Crie um diretório para o ponto de montagem do volume com o seguinte comando.

```
$ sudo mkdir /cvogcvetst
```

```
root@nimubu01:~# sudo mkdir cvogcvetst
```

8. Monte o volume NFS do Cloud Volumes ONTAP no diretório criado na etapa anterior.

```
sudo mount 10.0.6.251:/cvogcvenfsvol01 /cvogcvetst
```



Google Cloud NetApp Volumes (Volumes NetApp)

O Google Cloud NetApp Volumes (NetApp Volumes) é um portfólio completo de serviços de dados para fornecer soluções avançadas em nuvem. O NetApp Volumes oferece suporte a vários protocolos de acesso a arquivos para os principais provedores de nuvem (suporte a NFS e SMB).

Outros benefícios e recursos incluem: proteção e restauração de dados com Snapshot; recursos especiais para replicar, sincronizar e migrar destinos de dados no local ou na nuvem; e alto desempenho consistente no nível de um sistema de armazenamento flash dedicado.

Google Cloud NetApp Volumes (NetApp Volumes) como armazenamento conectado a convidados

▼ **Configurar volumes NetApp com o VMware Engine**

Os compartilhamentos do Google Cloud NetApp Volumes podem ser montados a partir de VMs criadas no ambiente do VMware Engine. Os volumes também podem ser montados no cliente Linux e mapeados no cliente Windows porque o Google Cloud NetApp Volumes oferece suporte aos protocolos SMB e NFS. Os volumes do Google Cloud NetApp Volumes podem ser configurados em etapas simples.

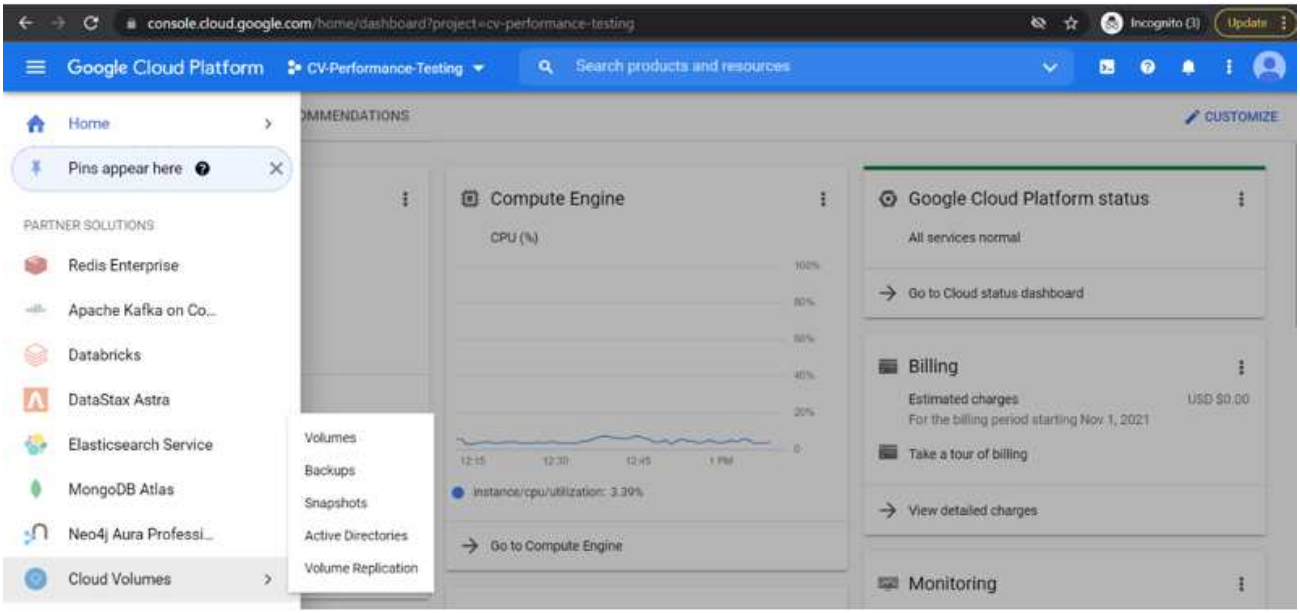
O Google Cloud NetApp Volumes e a nuvem privada do Google Cloud VMware Engine devem estar na mesma região.

Para comprar, habilitar e configurar o Google Cloud NetApp Volumes para Google Cloud no Google Cloud Marketplace, siga estas instruções detalhadas"guia" .

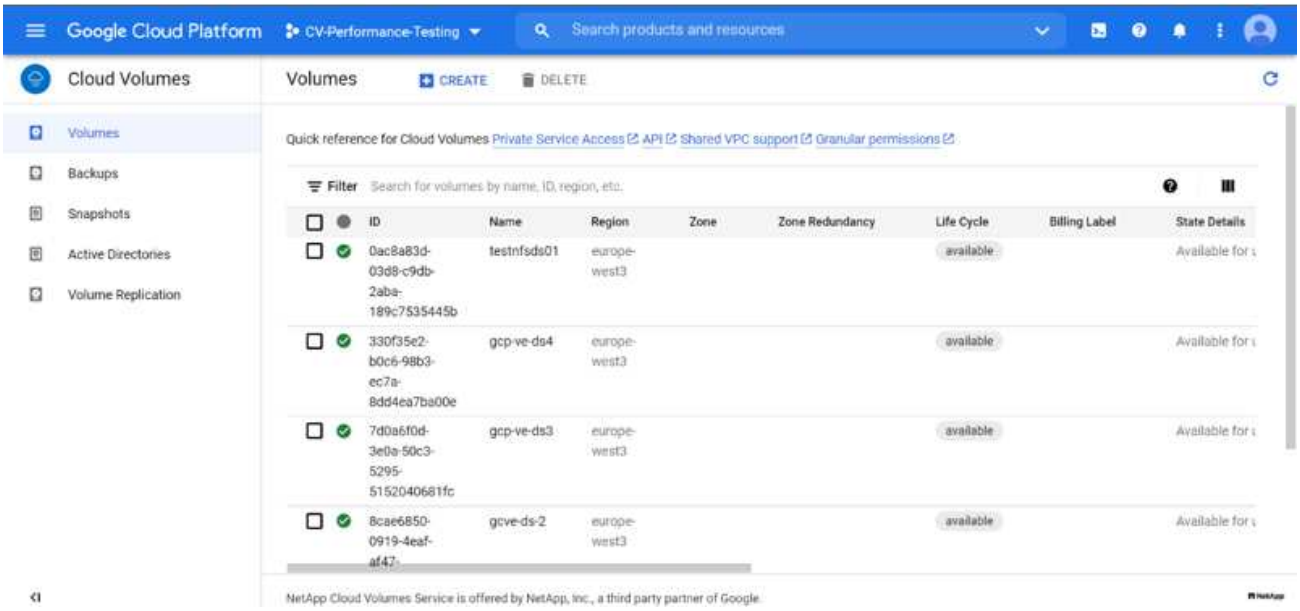
▼ **Crie um volume NFS do NetApp Volumes para a nuvem privada GCVE**

Para criar e montar volumes NFS, conclua as seguintes etapas:

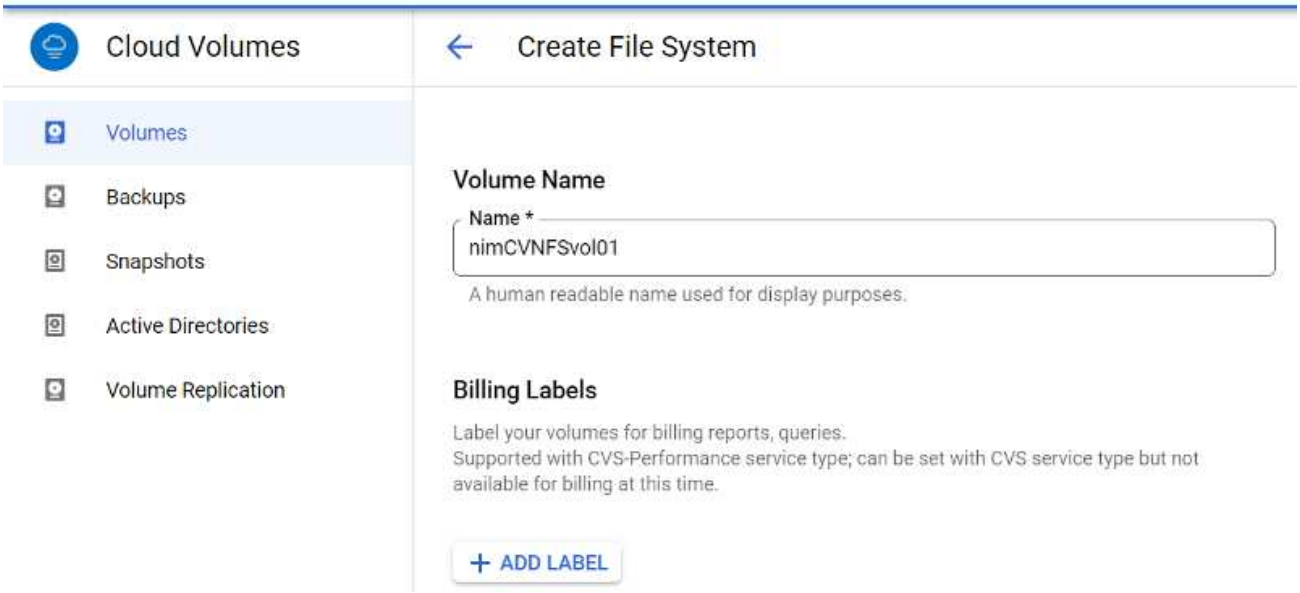
1. Acesse o Cloud Volumes a partir das Soluções de Parceiros no console do Google Cloud.



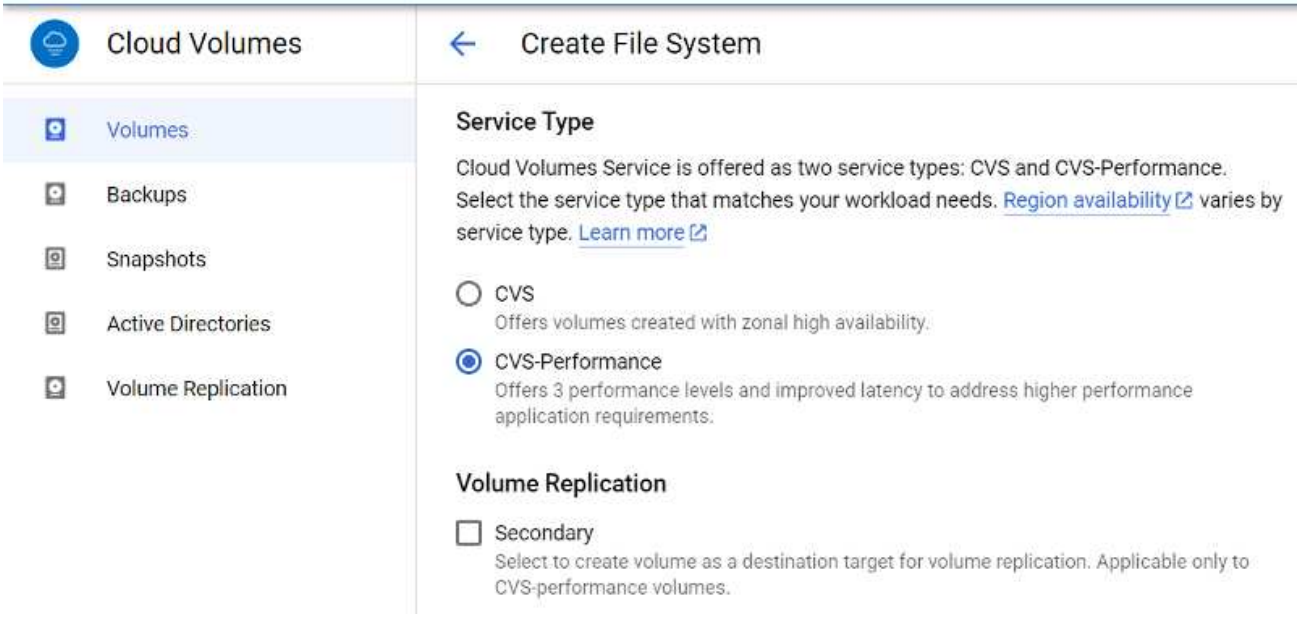
2. No Console do Cloud Volumes, acesse a página Volumes e clique em Criar.



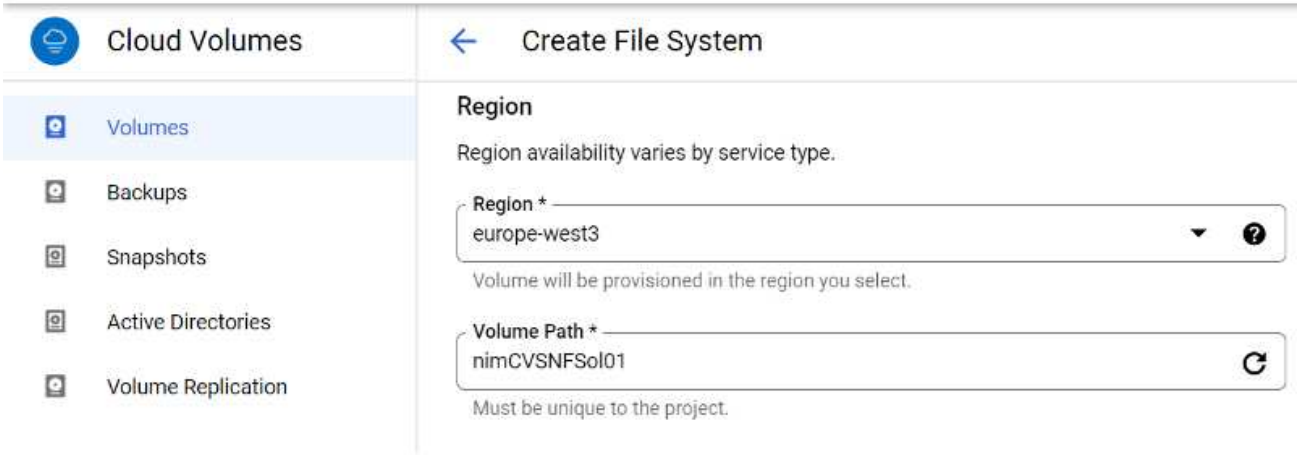
3. Na página Criar sistema de arquivos, especifique o nome do volume e os rótulos de cobrança, conforme necessário para mecanismos de estorno.



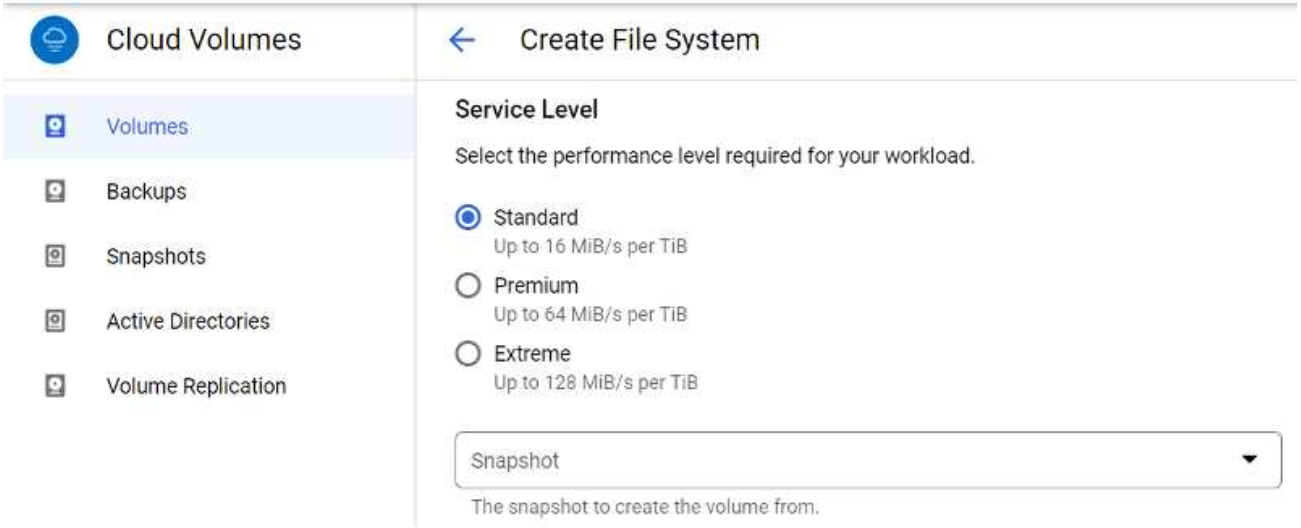
4. Selecione o serviço apropriado. Para GCVE, escolha NetApp Volumes-Desempenho e nível de serviço desejado para melhor latência e maior desempenho com base nos requisitos de carga de trabalho do aplicativo.



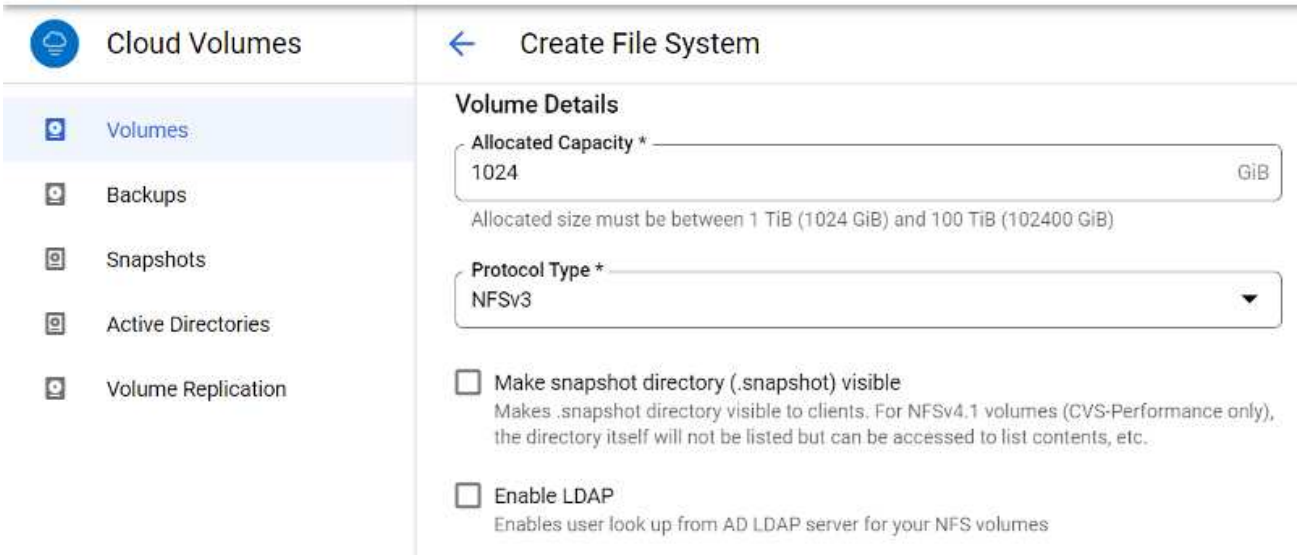
5. Especifique a região do Google Cloud para o volume e o caminho do volume (o caminho do volume deve ser exclusivo em todos os volumes de nuvem no projeto)



6. Selecione o nível de desempenho para o volume.

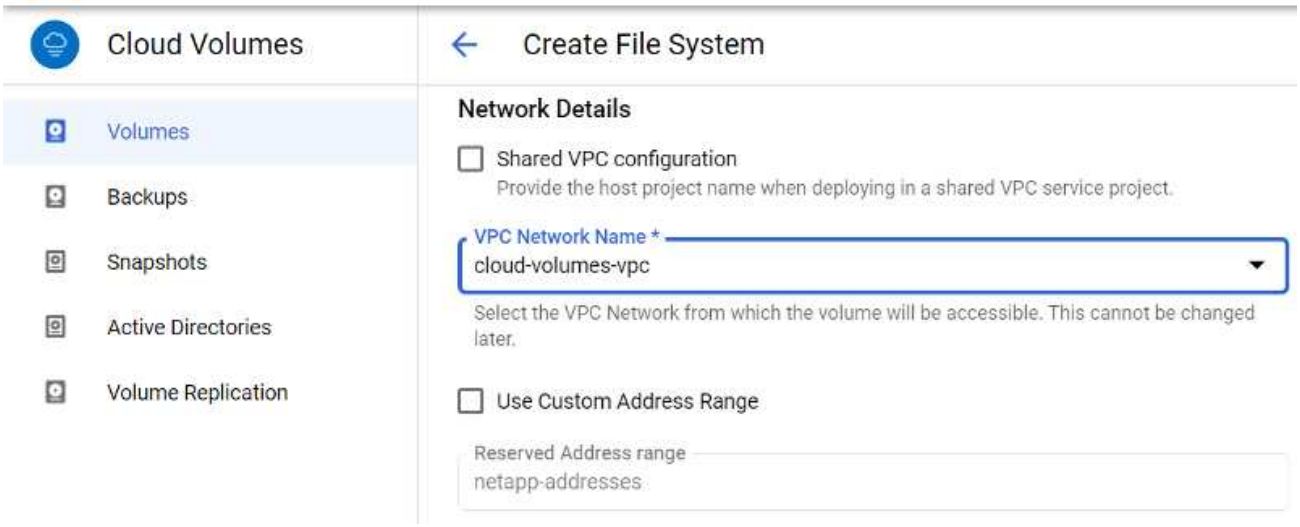


7. Especifique o tamanho do volume e o tipo de protocolo. Neste teste, o NFSv3 é usado.



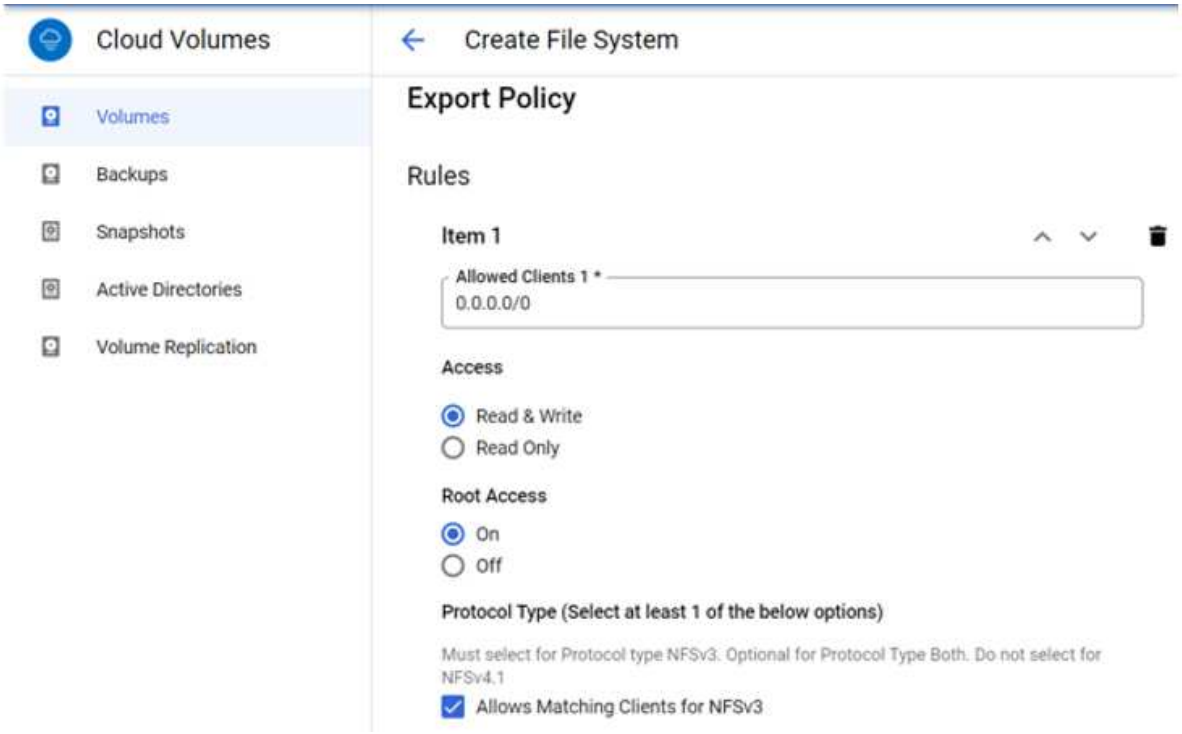
8. Nesta etapa, selecione a rede VPC da qual o volume estará acessível. Certifique-se de que o peering de VPC esteja em vigor.

   DICA: Se o peering de VPC não tiver sido feito, um botão pop-up será exibido para guiá-lo pelos comandos de peering. Abra uma sessão do Cloud Shell e execute os comandos apropriados para parear sua VPC com o produtor do Google Cloud NetApp Volumes . Caso você decida preparar o peering de VPC com antecedência, consulte estas instruções.



9. Gerencie as regras da política de exportação adicionando as regras apropriadas e marque a caixa de seleção para a versão do NFS correspondente.

   Observação: o acesso aos volumes NFS não será possível a menos que uma política de exportação seja adicionada.



10. Clique em Salvar para criar o volume.



▼ **Montando exportações NFS para VMs em execução no VMware Engine**

Antes de preparar a montagem do volume NFS, certifique-se de que o status de peering da conexão privada esteja listado como Ativo. Quando o status for Ativo, use o comando mount.

Para montar um volume NFS, faça o seguinte:

1. No Cloud Console, acesse Cloud Volumes > Volumes.
2. Vá para a página de volumes
3. Clique no volume NFS para o qual você deseja montar exportações NFS.
4. Role para a direita, em Mostrar mais, clique em Instruções de montagem.

Para executar o processo de montagem no sistema operacional convidado da VM VMware, siga as etapas abaixo:

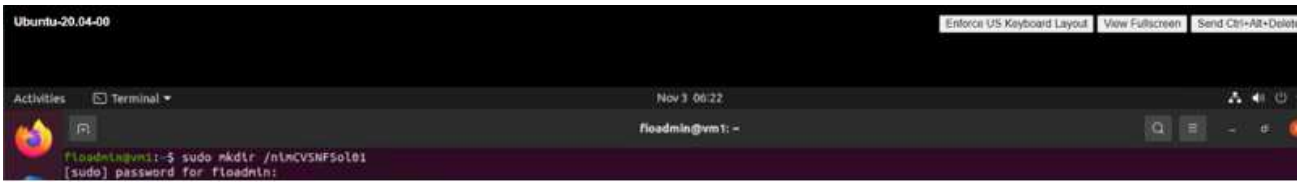
1. Use o cliente SSH e SSH para a máquina virtual.
2. Instale o cliente nfs na instância.
   a. Na instância do Red Hat Enterprise Linux ou SuSE Linux:

```
 sudo yum install -y nfs-utils
.. Em uma instância Ubuntu ou Debian:
```

```
sudo apt-get install nfs-common
```

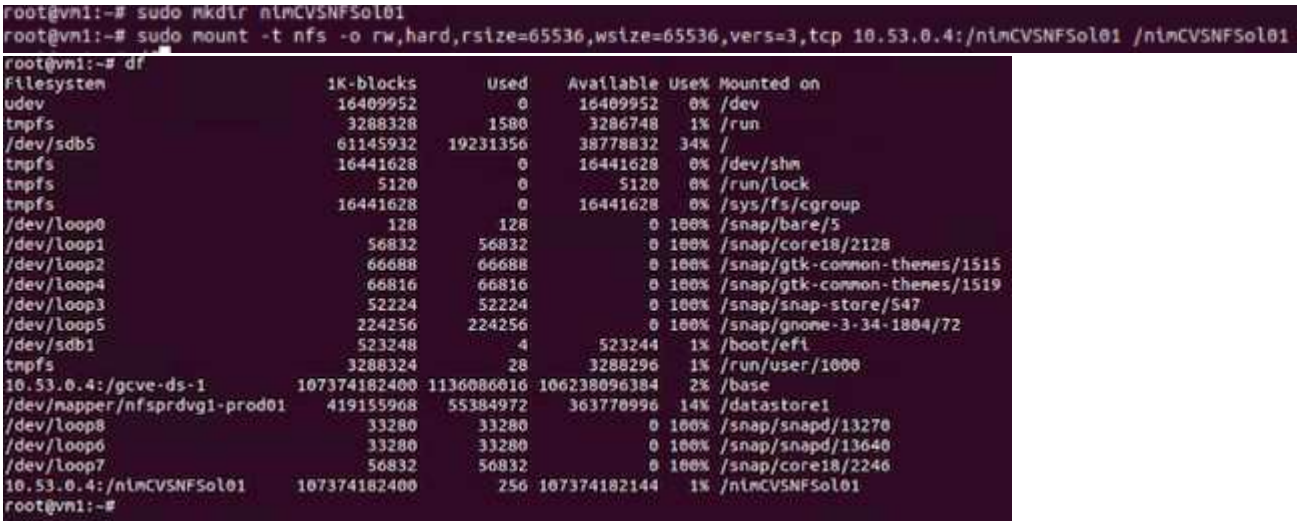
3. Crie um novo diretório na instância, como "/nimCVSNFSol01":

```
sudo mkdir /nimCVSNFSol01
```



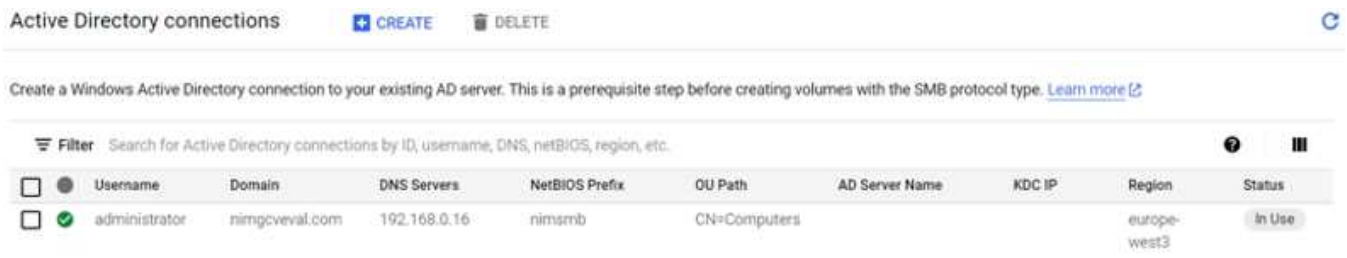
4. Monte o volume usando o comando apropriado. Exemplo de comando do laboratório abaixo:

```
sudo mount -t nfs -o rw,hard,rsize=65536,wsize=65536,vers=3,tcp
10.53.0.4:/nimCVSNFSol01 /nimCVSNFSol01
```



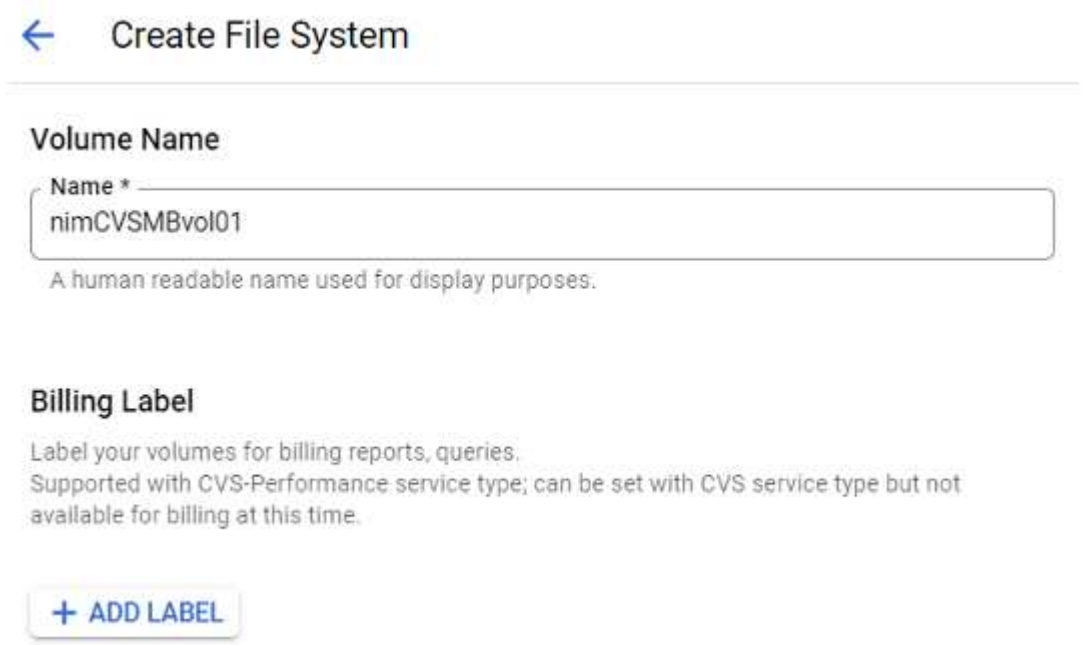
▼ **Criação e montagem de compartilhamento SMB em VMs em execução no VMware Engine**

Para volumes SMB, certifique-se de que as conexões do Active Directory estejam configuradas antes de criar o volume SMB.

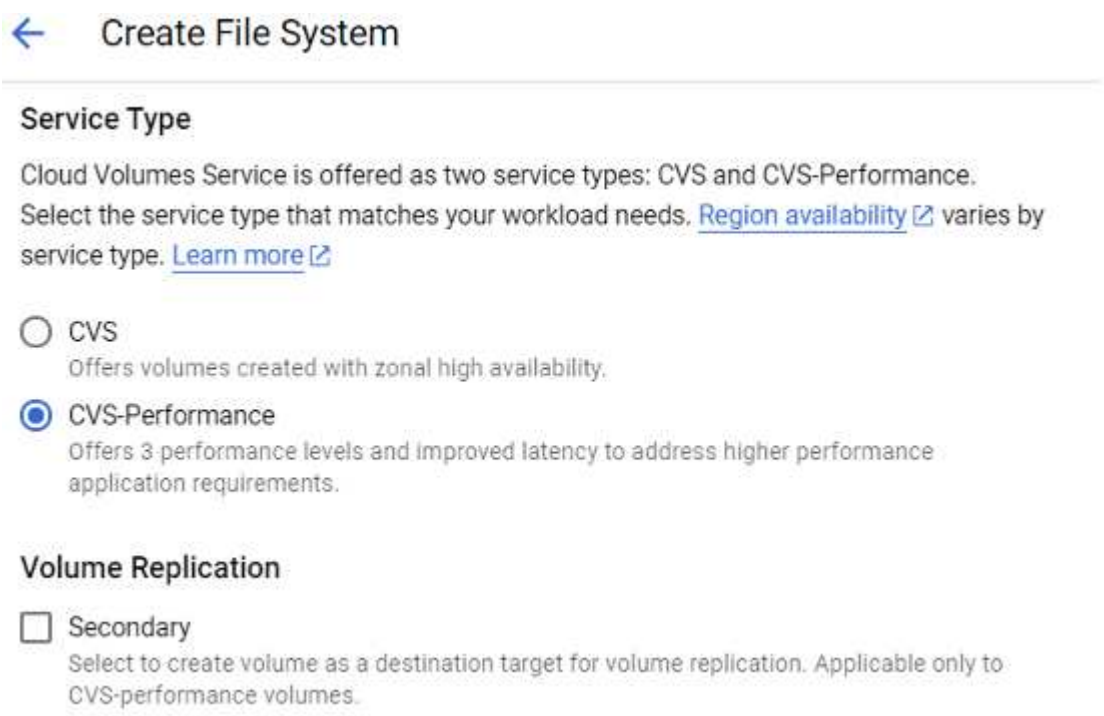


Depois que a conexão do AD estiver estabelecida, crie o volume com o nível de serviço desejado. As etapas são como a criação de um volume NFS, exceto pela seleção do protocolo apropriado.

1. No Console do Cloud Volumes, acesse a página Volumes e clique em Criar.
2. Na página Criar sistema de arquivos, especifique o nome do volume e os rótulos de cobrança, conforme necessário para mecanismos de estorno.



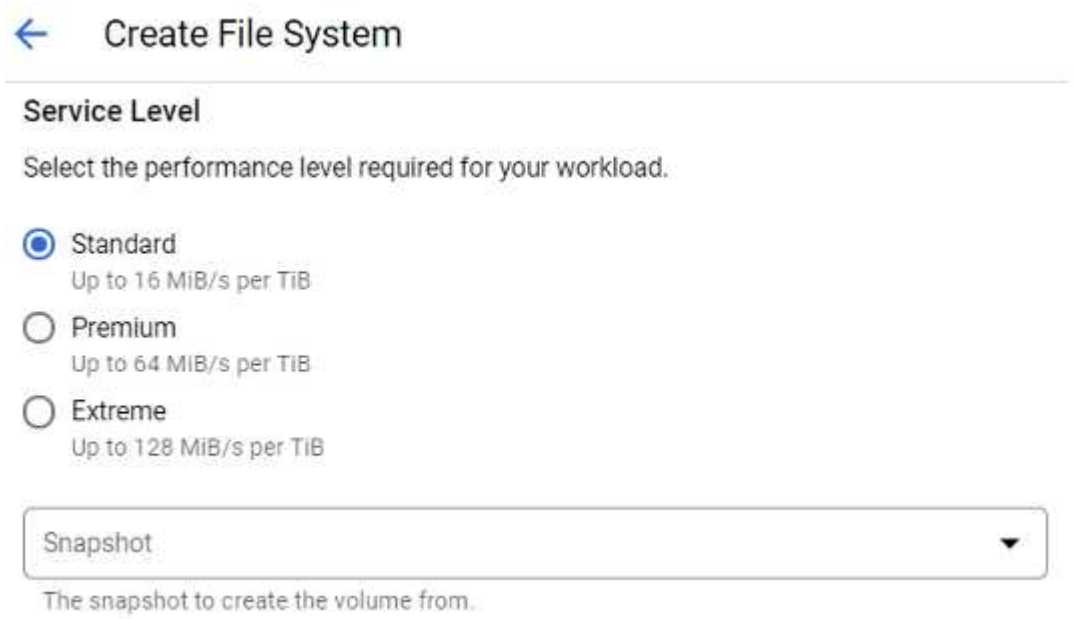
3. Selecione o serviço apropriado. Para GCVE, escolha NetApp Volumes-Desempenho e nível de serviço desejado para melhor latência e maior desempenho com base nos requisitos de carga de trabalho.



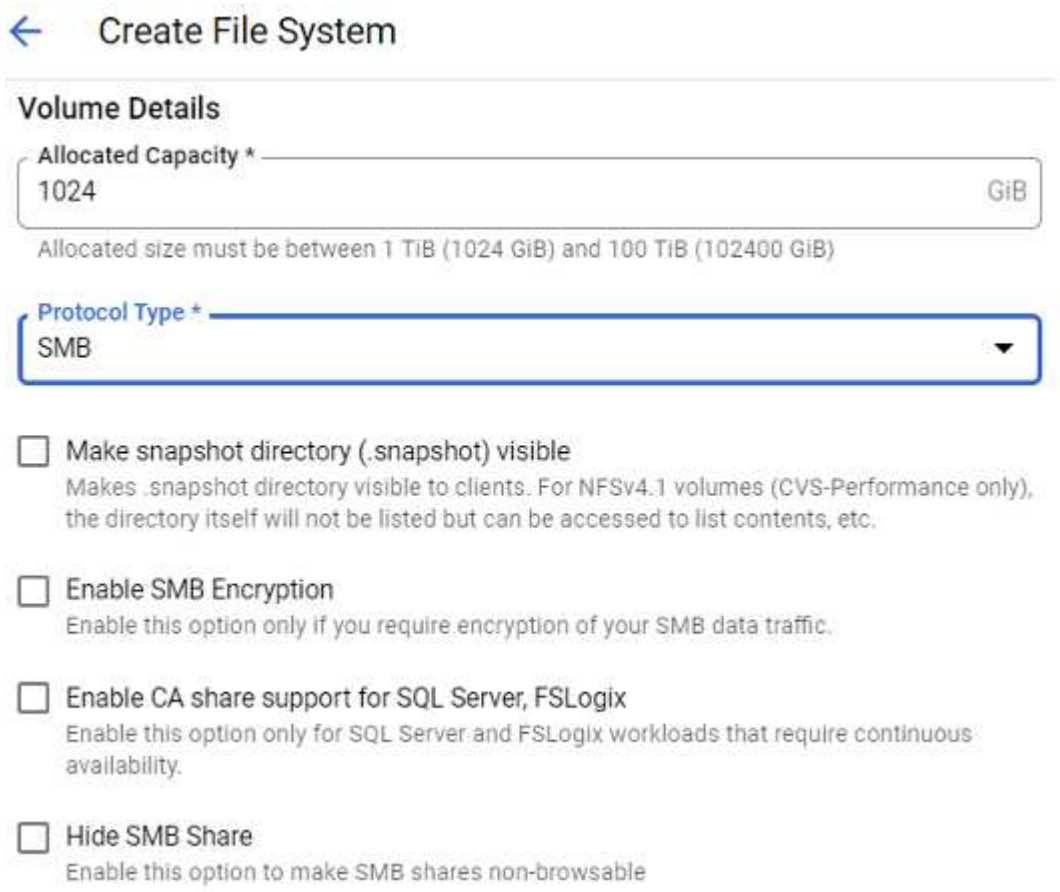
4. Especifique a região do Google Cloud para o volume e o caminho do volume (o caminho do volume deve ser exclusivo em todos os volumes de nuvem no projeto)



5. Selecione o nível de desempenho para o volume.

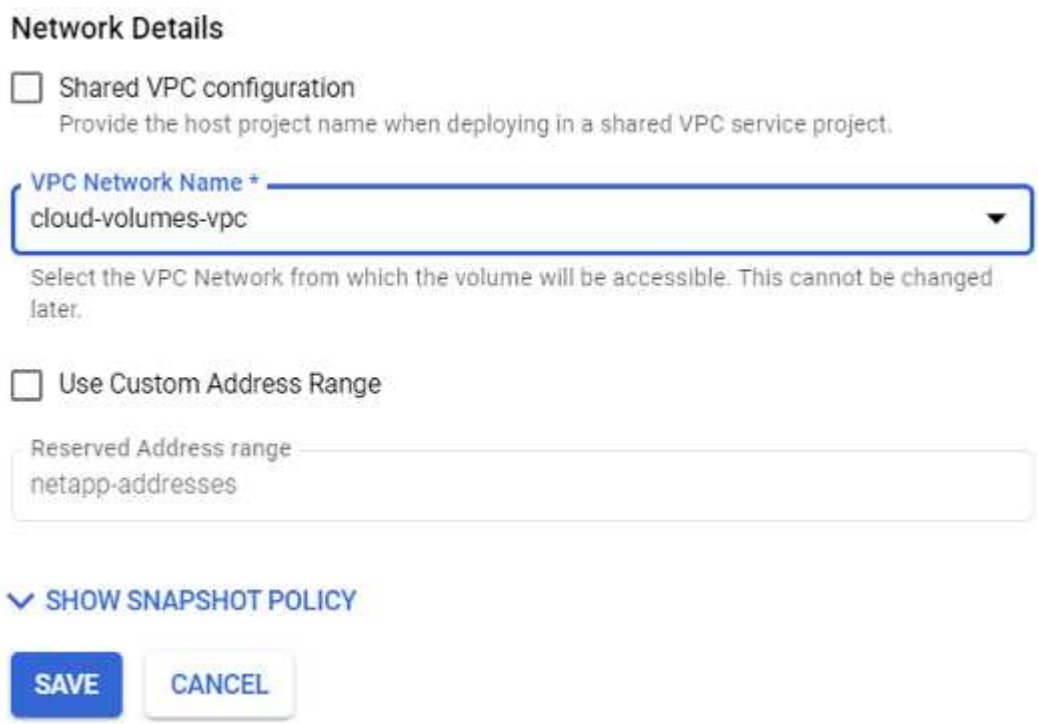


6. Especifique o tamanho do volume e o tipo de protocolo. Neste teste, o SMB é usado.



7. Nesta etapa, selecione a rede VPC da qual o volume estará acessível. Certifique-se de que o peering de VPC esteja em vigor.

   DICA: se o peering de VPC ainda não tiver sido configurado, um botão pop-up será exibido para orientar você nos comandos de peering. Abra uma sessão do Cloud Shell e execute os comandos apropriados para emparelhar sua VPC com o produtor do Google Cloud NetApp Volumes. Caso você decida preparar o peering de VPC antecipadamente, consulte estas "instruções".



8. Clique em Salvar para criar o volume.



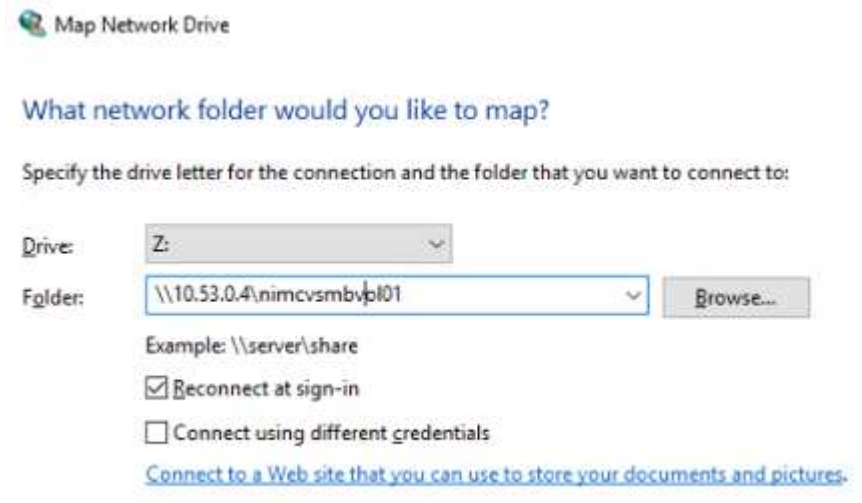
Para montar o volume SMB, faça o seguinte:

1. No Cloud Console, acesse Cloud Volumes > Volumes.
2. Vá para a página de volumes
3. Clique no volume SMB para o qual você deseja mapear um compartilhamento SMB.
4. Role para a direita, em Mostrar mais, clique em Instruções de montagem.

Para executar o processo de montagem no sistema operacional convidado Windows da VM VMware, siga as etapas abaixo:

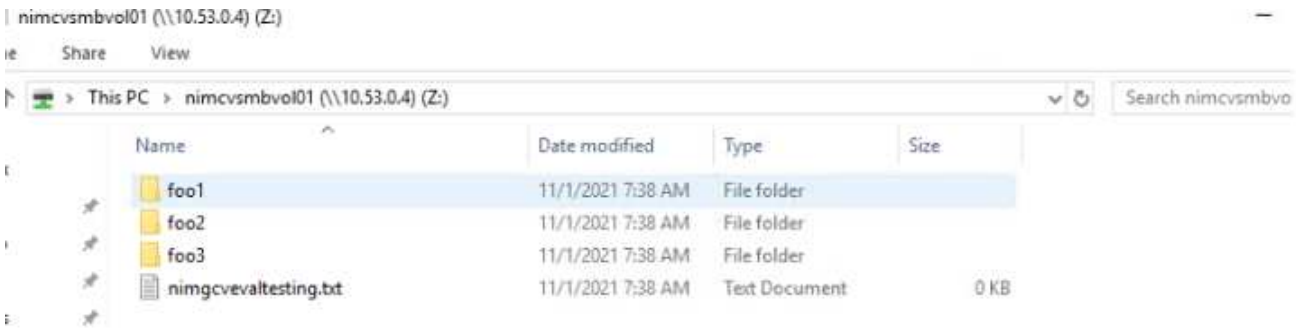
1. Clique no botão Iniciar e depois em Computador.
2. Clique em Mapear unidade de rede.
3. Na lista Unidades, clique em qualquer letra de unidade disponível.
4. Na caixa de pasta, digite:

```
\\nimsmb-3830.nimgcveval.com\nimCVSMBvol01
```



Para conectar-se sempre que fizer login no seu computador, marque a caixa de seleção Reconectar ao fazer login.

5. Clique em Concluir.



Resumo e conclusão: Por que NetApp Hybrid Multicloud com VMware

O NetApp Cloud Volumes, juntamente com as soluções VMware para os principais hiperescaladores, oferece grande potencial para organizações que buscam aproveitar a nuvem híbrida. O restante desta seção fornece os casos de uso que mostram que a integração do NetApp Cloud Volumes permite verdadeiros recursos de multinuvem híbrida.

Caso de uso nº 1: Otimização do armazenamento

Ao executar um exercício de dimensionamento usando a saída do RVtools, fica sempre evidente que a escala de potência (vCPU/vMem) é paralela ao armazenamento. Muitas vezes, as organizações se encontram em uma situação em que o espaço de armazenamento exige um tamanho de cluster muito maior do que o necessário em termos de potência.

Ao integrar o NetApp Cloud Volumes, as organizações podem obter uma solução de nuvem baseada no vSphere com uma abordagem de migração simples, sem necessidade de replataforma, sem alterações de IP e sem alterações arquitetônicas. Além disso, essa otimização permite que você dimensione a área de armazenamento enquanto mantém a contagem de hosts na menor quantidade necessária no vSphere, mas sem alterar a hierarquia de armazenamento, a segurança ou os arquivos disponibilizados. Isso permite que

você otimize a implantação e reduza o TCO geral em 35–45%. Essa integração também permite que você dimensione o armazenamento de armazenamento morno para desempenho de nível de produção em segundos.

Caso de uso nº 2: Migração para a nuvem

As organizações estão sob pressão para migrar aplicativos de data centers locais para a Nuvem Pública por vários motivos: uma expiração de concessão próxima; uma diretriz financeira para migrar gastos de capital (capex) para gastos operacionais (opex); ou simplesmente uma ordem de cima para baixo para mover tudo para a nuvem.

Quando a velocidade é crítica, somente uma abordagem de migração simplificada é viável, porque a reformulação de plataformas e a refatoração de aplicativos para adaptação à plataforma IaaS específica da nuvem são lentas e caras, muitas vezes levando meses. Ao combinar o NetApp Cloud Volumes com a replicação SnapMirror com eficiência de largura de banda para armazenamento conectado a convidados (incluindo RDMs em conjunto com cópias de Snapshot consistentes com aplicativos e HCX, migração específica para nuvem (por exemplo, Azure Migrate) ou produtos de terceiros para replicar VMs), essa transição é ainda mais fácil do que depender de mecanismos de filtros de E/S demorados.

Caso de uso nº 3: Expansão do data center

Quando um data center atinge limites de capacidade devido a picos sazonais de demanda ou apenas ao crescimento orgânico constante, migrar para o VMware hospedado na nuvem junto com o NetApp Cloud Volumes é uma solução fácil. O aproveitamento do NetApp Cloud Volumes permite a criação, replicação e expansão de armazenamento com muita facilidade, fornecendo alta disponibilidade em zonas de disponibilidade e recursos de dimensionamento dinâmico. Aproveitar o NetApp Cloud Volumes ajuda a minimizar a capacidade do cluster do host, superando a necessidade de clusters estendidos.

Caso de uso nº 4: Recuperação de desastres para a nuvem

Em uma abordagem tradicional, se ocorrer um desastre, as VMs replicadas para a nuvem precisarão ser convertidas para a plataforma de hipervisor da própria nuvem antes que possam ser restauradas — uma tarefa que não deve ser realizada durante uma crise.

Ao usar o NetApp Cloud Volumes para armazenamento conectado a convidados usando replicação do SnapCenter e do SnapMirror no local, juntamente com soluções de virtualização de nuvem pública, uma melhor abordagem para recuperação de desastres pode ser desenvolvida, permitindo que réplicas de VM sejam recuperadas em uma infraestrutura VMware SDDC totalmente consistente, juntamente com ferramentas de recuperação específicas da nuvem (por exemplo, Azure Site Recovery) ou ferramentas de terceiros equivalentes, como o Veeam. Essa abordagem também permite que você execute exercícios de recuperação de desastres e recuperação de ransomware rapidamente. Isso também permite que você dimensione para produção total para testes ou durante um desastre, adicionando hosts sob demanda.

Caso de uso nº 5: Modernização de aplicativos

Depois que os aplicativos estiverem na nuvem pública, as organizações desejarão aproveitar as centenas de serviços de nuvem poderosos para modernizá-los e estendê-los. Com o uso do NetApp Cloud Volumes, a modernização é um processo fácil porque os dados do aplicativo não ficam bloqueados no vSAN e permitem a mobilidade de dados para uma ampla variedade de casos de uso, incluindo o Kubernetes.

Conclusão

Não importa se você tem como alvo uma nuvem híbrida ou totalmente em nuvem, o NetApp Cloud Volumes oferece excelentes opções para implantar e gerenciar cargas de trabalho de aplicativos, juntamente com

serviços de arquivo e protocolos de bloco, ao mesmo tempo em que reduz o TCO ao tornar os requisitos de dados integrados à camada de aplicativo.

Seja qual for o caso de uso, escolha seu hiperescalador/nuvem favorito junto com o NetApp Cloud Volumes para rápida concretização dos benefícios da nuvem, infraestrutura consistente e operações em nuvens locais e múltiplas, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial.

É o mesmo processo e procedimento familiar usado para conectar o armazenamento. Lembre-se de que foi apenas a posição dos dados que mudou com os novos nomes; as ferramentas e os processos permanecem os mesmos e o NetApp Cloud Volumes ajuda a otimizar a implantação geral.

Casos de uso da nuvem híbrida VMware

Casos de uso para NetApp Hybrid Multicloud com VMware

Uma visão geral dos casos de uso importantes para a organização de TI ao planejar implantações de nuvem híbrida ou cloud-first.

Casos de uso populares

Os casos de uso incluem:

- Recuperação de desastres,
- Hospedagem de cargas de trabalho durante a manutenção do data center, * pico rápido no qual recursos adicionais são necessários além do que é provisionado no data center local,
- Expansão do site VMware,
- Migração rápida para a nuvem,
- Desenvolvedor/teste e
- Modernização de aplicativos aproveitando tecnologias suplementares de nuvem.

Ao longo desta documentação, as referências de carga de trabalho na nuvem serão detalhadas usando os casos de uso do VMware. Esses casos de uso são:

- Proteger (inclui recuperação de desastres e backup/restauração)
- Migrar
- Estender

Por dentro da jornada de TI

A maioria das organizações está em uma jornada de transformação e modernização. Como parte desse processo, as empresas estão tentando usar seus investimentos existentes na VMware enquanto aproveitam os benefícios da nuvem e exploram maneiras de tornar o processo de migração o mais tranquilo possível. Essa abordagem tornaria seus esforços de modernização muito mais fáceis porque os dados já estão na nuvem.

A resposta mais fácil para esse cenário são as ofertas da VMware em cada hiperescalador. Assim como o NetApp Cloud Volumes, o VMware oferece uma maneira de mover ou estender ambientes VMware locais para qualquer nuvem, permitindo que você retenha ativos, habilidades e ferramentas locais existentes enquanto executa cargas de trabalho nativamente na nuvem. Isso reduz os riscos porque não haverá interrupções de serviço nem necessidade de alterações de IP e fornece à equipe de TI a capacidade de operar da mesma

forma que opera no local, usando as habilidades e ferramentas existentes. Isso pode levar a migrações aceleradas para a nuvem e uma transição muito mais suave para uma arquitetura multicloud híbrida.

Compreendendo a importância das opções suplementares de armazenamento NFS

Embora o VMware em qualquer nuvem ofereça recursos híbridos exclusivos para cada cliente, opções limitadas de armazenamento NFS suplementar restringiram sua utilidade para organizações com cargas de trabalho pesadas de armazenamento. Como o armazenamento está diretamente vinculado aos hosts, a única maneira de dimensioná-lo é adicionar mais hosts, o que pode aumentar os custos em 35 a 40 por cento ou mais para cargas de trabalho com uso intensivo de armazenamento. Essas cargas de trabalho precisam apenas de armazenamento adicional, não de potência adicional. Mas isso significa pagar por hosts adicionais.

Vamos considerar este cenário:

Um cliente precisa de apenas cinco hosts para CPU e memória, mas tem muitas necessidades de armazenamento e precisa de 12 hosts para atender ao requisito de armazenamento. Essa exigência acaba desequilibrando a balança financeiramente, pois eles precisam comprar potência adicional, quando só precisam aumentar o armazenamento.

Ao planejar a adoção e as migrações para a nuvem, é sempre importante avaliar a melhor abordagem e seguir o caminho mais fácil que reduza os investimentos totais. A abordagem mais comum e fácil para qualquer migração de aplicativo é a rehospedagem (também conhecida como lift and shift), onde não há máquina virtual (VM) ou conversão de dados. Usar o NetApp Cloud Volumes com o data center definido por software (SDDC) da VMware, ao mesmo tempo em que complementa o vSAN, oferece uma opção fácil de elevação e transferência.

Soluções NetApp para VMware em Hyperscalers

Saiba mais sobre as soluções que a NetApp oferece ao ambiente VMware em cada um dos hiperescaladores — desde a migração de fluxos de trabalho, extensão/estouro para a nuvem, backup/restauração e recuperação de desastres.

Soluções NetApp para ambientes VMware

Não importa se você opera em um modelo de nuvem híbrida ou em um modelo "nuvem primeiro", a NetApp oferece uma ampla variedade de soluções para atender aos casos de uso mais comuns de gerenciamento de cargas de trabalho em um modelo de nuvem ou nuvem híbrida.

A NetApp também oferece soluções para armazenamento provisionado como armazenamento no convidado (conectado ao convidado) ou como um armazenamento de dados NFS suplementar em cada um dos hiperescaladores. Todas as soluções são categorizadas em uníssono com a classificação de cargas de trabalho em nuvem da VMware. Essas classificações incluem:

- Proteger (inclui recuperação de desastres e backup/restauração)
- Migrar
- Estender

Para mais detalhes sobre as soluções disponíveis para cada hiperescalador, visite:

- "Soluções para AWS / VMC"
- "Soluções para Azure / AVS"
- "Soluções para GCP / GCVE"

Soluções NetApp para Amazon VMware Managed Cloud (VMC)

Saiba mais sobre as soluções que a NetApp traz para a AWS.

A VMware define as cargas de trabalho na nuvem em uma das três categorias:

- Proteger (incluindo recuperação de desastres e backup/restauração)
- Migrar
- Estender

Navegue pelas soluções disponíveis nas seções a seguir.

Proteger

- "Recuperação de desastres com VMC na AWS (conectado por convidado)"
- "Veeam Backup Restore no VMC com FSx ONTAP"
- "Recuperação de Desastres (DRO) com FSx ONTAP e VMC"
- "Usando Veeam Replication e FSx ONTAP para recuperação de desastres no VMware Cloud na AWS"

Migrar

- "Migrar cargas de trabalho para o armazenamento de dados FSx ONTAP usando VMware HCX"

Estender

EM BREVE!!

Soluções NetApp para Azure VMware Solution (AVS)

Saiba mais sobre as soluções que a NetApp traz para o Azure.

A VMware define as cargas de trabalho na nuvem em uma das três categorias:

- Proteger (incluindo recuperação de desastres e backup/restauração)
- Migrar
- Estender

Navegue pelas soluções disponíveis nas seções a seguir.

Proteger

- "Recuperação de desastres com ANF e JetStream (armazenamento de dados NFS suplementar)"
- "Recuperação de desastres com ANF e CVO (armazenamento conectado a convidados)"
- "Recuperação de Desastres (DRO) com ANF e AVS"
- "Usando o Veeam Replication e o armazenamento de dados do Azure NetApp Files para recuperação de desastres no Azure VMware Solution"

Migrar

- "Migrar cargas de trabalho para o repositório de dados do Azure NetApp Files usando o VMware HCX"

Estender

EM BREVE!!

Soluções NetApp para Google Cloud VMware Engine (GCVE)

Saiba mais sobre as soluções que a NetApp traz para o GCP.

A VMware define as cargas de trabalho na nuvem em uma das três categorias:

- Proteger (incluindo recuperação de desastres e backup/restauração)
- Migrar
- Estender

Navegue pelas soluções disponíveis nas seções a seguir.

Proteger

- "Recuperação de desastres de aplicativos com SnapCenter, Cloud Volumes ONTAP e Veeam Replication"
- "Recuperação de desastres consistente com aplicativos com NetApp SnapCenter e Veeam Replication para volumes NetApp no GCVE"

Migrar

- "Migração de carga de trabalho usando VMware HCX para o armazenamento de dados NFS do Google Cloud NetApp Volumes"
- "Replicação de VM usando Veeam para armazenamento de dados NFS do Google Cloud NetApp Volumes"

Estender

EM BREVE!!

NetApp para AWS/VMC

Recursos da NetApp para AWS VMC

Saiba mais sobre os recursos que a NetApp oferece ao AWS VMware Cloud (VMC) - desde o NetApp como um dispositivo de armazenamento conectado a convidados ou um armazenamento de dados NFS suplementar até a migração de fluxos de trabalho, extensão/intermitência para a nuvem, backup/restauração e recuperação de desastres.

Vá para a seção do conteúdo desejado selecionando entre as seguintes opções:

- "Configurando o VMC na AWS"

- "Opções de armazenamento NetApp para VMC"
- "Soluções de nuvem NetApp /VMware"

Configurando o VMC na AWS

Assim como no local, planejar um ambiente de virtualização baseado em nuvem é essencial para um ambiente de produção bem-sucedido, pronto para criação de VMs e migração.

Esta seção descreve como configurar e gerenciar o VMware Cloud on AWS SDDC e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP ao AWS VMC.

O processo de configuração pode ser dividido nas seguintes etapas:

- Implantar e configurar o VMware Cloud para AWS
- Conecte o VMware Cloud ao FSx ONTAP

Veja o detalhado"etapas de configuração para VMC" .

Opções de armazenamento NetApp para VMC

O armazenamento NetApp pode ser utilizado de diversas maneiras — como um repositório de dados conectado ou como um repositório de dados NFS suplementar — dentro do AWS VMC.

Por favor visite"Opções de armazenamento NetApp suportadas" para maiores informações.

A AWS oferece suporte ao armazenamento NetApp nas seguintes configurações:

- FSx ONTAP como armazenamento conectado a convidados
- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- FSx ONTAP como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para VMC" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para VMC" .

Casos de uso da solução

Com as soluções de nuvem da NetApp e da VMware, muitos casos de uso são simples de implantar no seu AWS VMC. Os casos de uso são definidos para cada uma das áreas de nuvem definidas pela VMware:

- Proteger (inclui recuperação de desastres e backup/restauração)
- Estender
- Migrar

"Navegue pelas soluções NetApp para AWS VMC"

Proteja cargas de trabalho na AWS/VMC

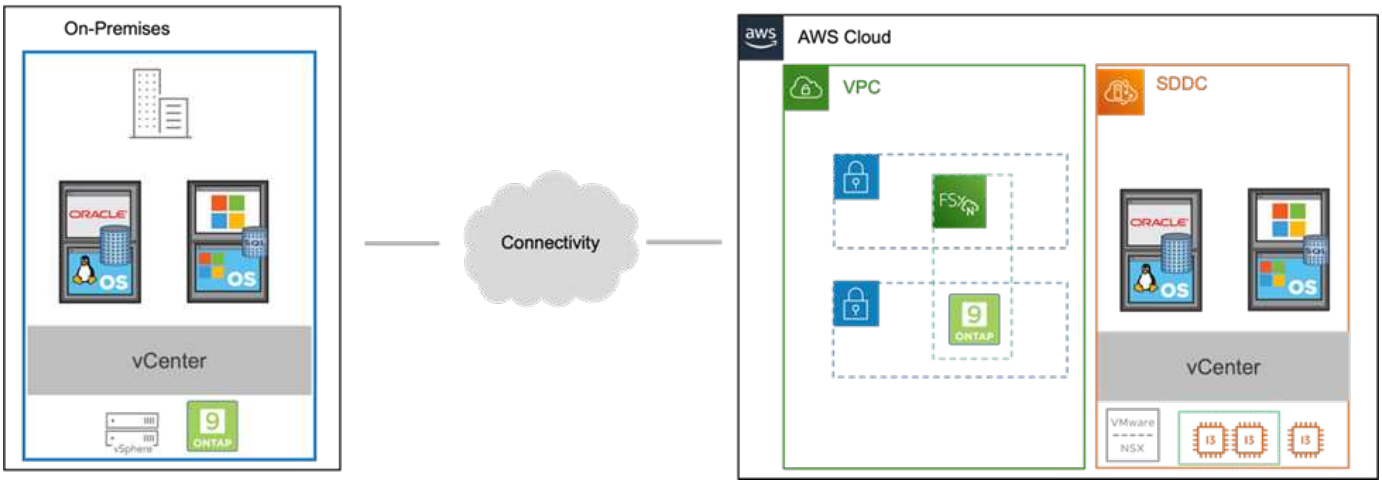
TR-4931: Recuperação de desastres com VMware Cloud na Amazon Web Services e Guest Connect

Um ambiente e um plano comprovados de recuperação de desastres (DR) são essenciais para que as organizações garantam que os aplicativos essenciais aos negócios possam ser restaurados rapidamente no caso de uma grande interrupção. Esta solução se concentra na demonstração de casos de uso de DR com foco nas tecnologias VMware e NetApp , tanto no local quanto com o VMware Cloud na AWS.

Visão geral

A NetApp tem um longo histórico de integração com a VMware, como evidenciado pelas dezenas de milhares de clientes que escolheram a NetApp como parceira de armazenamento para seus ambientes virtualizados. Essa integração continua com opções conectadas por convidados na nuvem e também integrações recentes com armazenamentos de dados NFS. Esta solução se concentra no caso de uso comumente conhecido como armazenamento conectado ao convidado.

No armazenamento conectado ao convidado, o VMDK convidado é implantado em um armazenamento de dados provisionado pela VMware, e os dados do aplicativo são armazenados no iSCSI ou NFS e mapeados diretamente para a VM. Os aplicativos Oracle e MS SQL são usados para demonstrar um cenário de DR, conforme mostrado na figura a seguir.



Suposições, pré-requisitos e visão geral dos componentes

Antes de implantar esta solução, revise a visão geral dos componentes, os pré-requisitos necessários para implantar a solução e as suposições feitas na documentação desta solução.

"Requisitos, pré-requisitos e planejamento da solução DR"

Executando DR com SnapCenter

Nesta solução, o SnapCenter fornece instantâneos consistentes de aplicativos para dados de aplicativos SQL Server e Oracle. Essa configuração, juntamente com a tecnologia SnapMirror , fornece replicação de dados de alta velocidade entre nosso AFF local e o cluster FSx ONTAP . Além disso, o Veeam Backup & Replication fornece recursos de backup e restauração para nossas máquinas virtuais.

Nesta seção, abordamos a configuração do SnapCenter, SnapMirror e Veeam para backup e restauração.

As seções a seguir abordam a configuração e as etapas necessárias para concluir um failover no site secundário:

Configurar relacionamentos e cronogramas de retenção do SnapMirror

O SnapCenter pode atualizar relacionamentos do SnapMirror dentro do sistema de armazenamento primário (primário > espelho) e para sistemas de armazenamento secundários (primário > cofre) para fins de arquivamento e retenção de longo prazo. Para fazer isso, você deve estabelecer e inicializar um relacionamento de replicação de dados entre um volume de destino e um volume de origem usando o SnapMirror.

Os sistemas ONTAP de origem e destino devem estar em redes pareadas usando o peering do Amazon VPC, um gateway de trânsito, o AWS Direct Connect ou uma VPN da AWS.

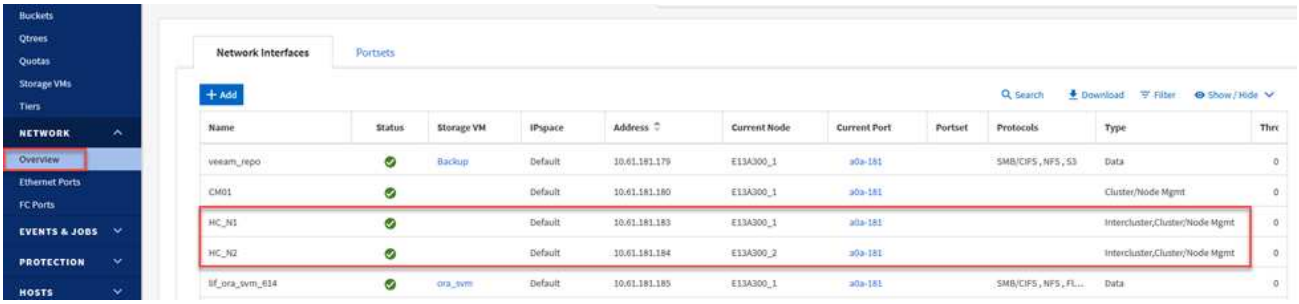
As etapas a seguir são necessárias para configurar relacionamentos SnapMirror entre um sistema ONTAP local e o FSx ONTAP:

Consulte o "FSx ONTAP – Guia do Usuário ONTAP" para obter mais informações sobre como criar relacionamentos SnapMirror com o FSx.

▼ **Registre as interfaces lógicas do Intercluster de origem e destino**

Para o sistema ONTAP de origem que reside no local, 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 para o FSx, faça login na CLI e execute o seguinte comando:

```
FSx-Dest::> network interface show -role intercluster
```

```
FsxId0ae40e08acc0dea67::> network interface show -role intercluster
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
FsxId0ae40e08acc0dea67
            inter_1      up/up    172.30.15.42/25    FsxId0ae40e08acc0dea67-01
                                                                   e0e     true
            inter_2      up/up    172.30.14.28/26    FsxId0ae40e08acc0dea67-02
                                                                   e0e     true
2 entries were displayed.
```

▼ **Estabelecer peering de cluster entre ONTAP e FSx**

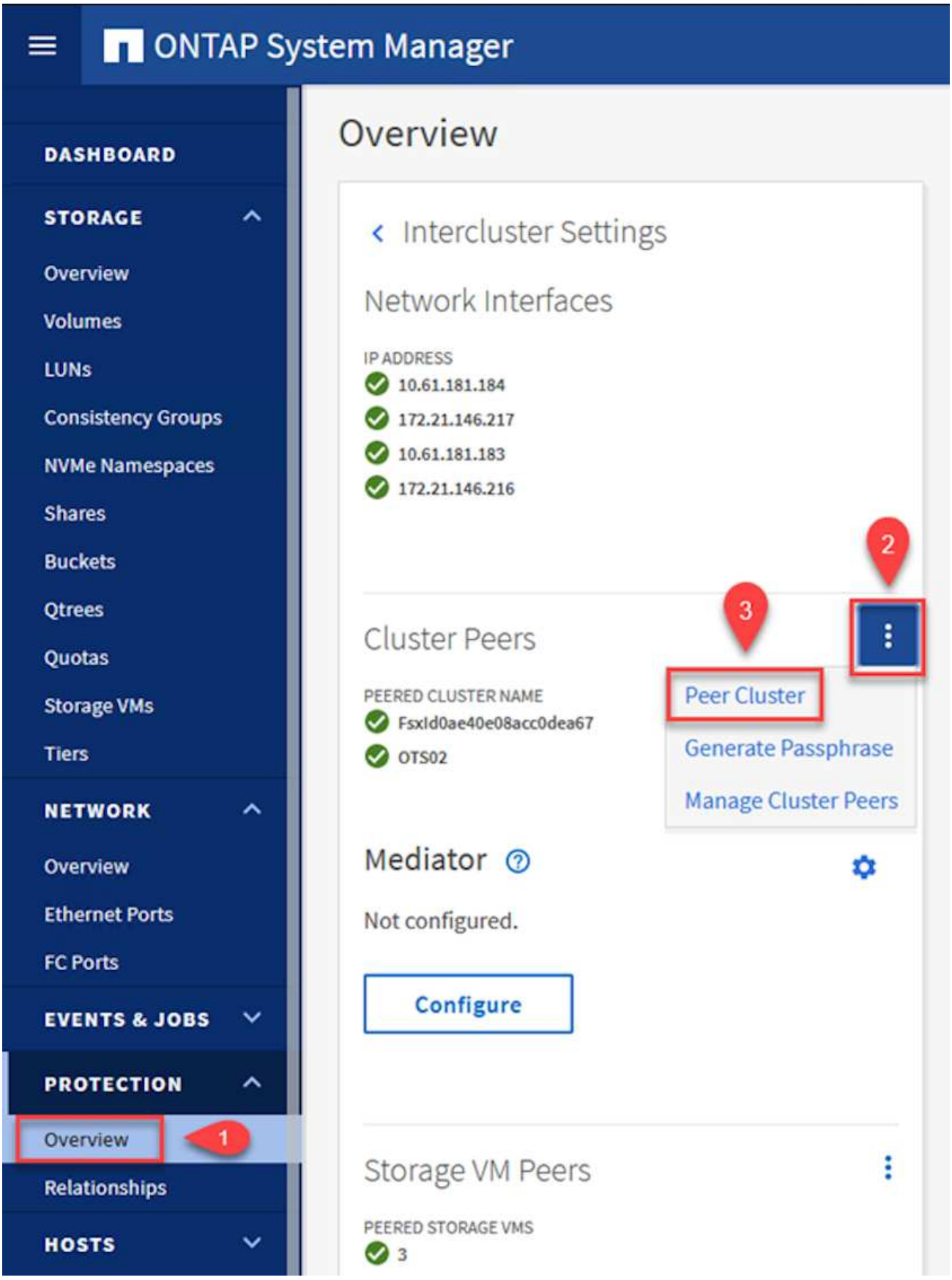
Para estabelecer o peering de cluster entre clusters ONTAP , uma senha exclusiva inserida no cluster

ONTAP inicial deve ser confirmada no outro cluster peer.

1. Configure o peering no cluster FSx 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.

```
FSx-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.



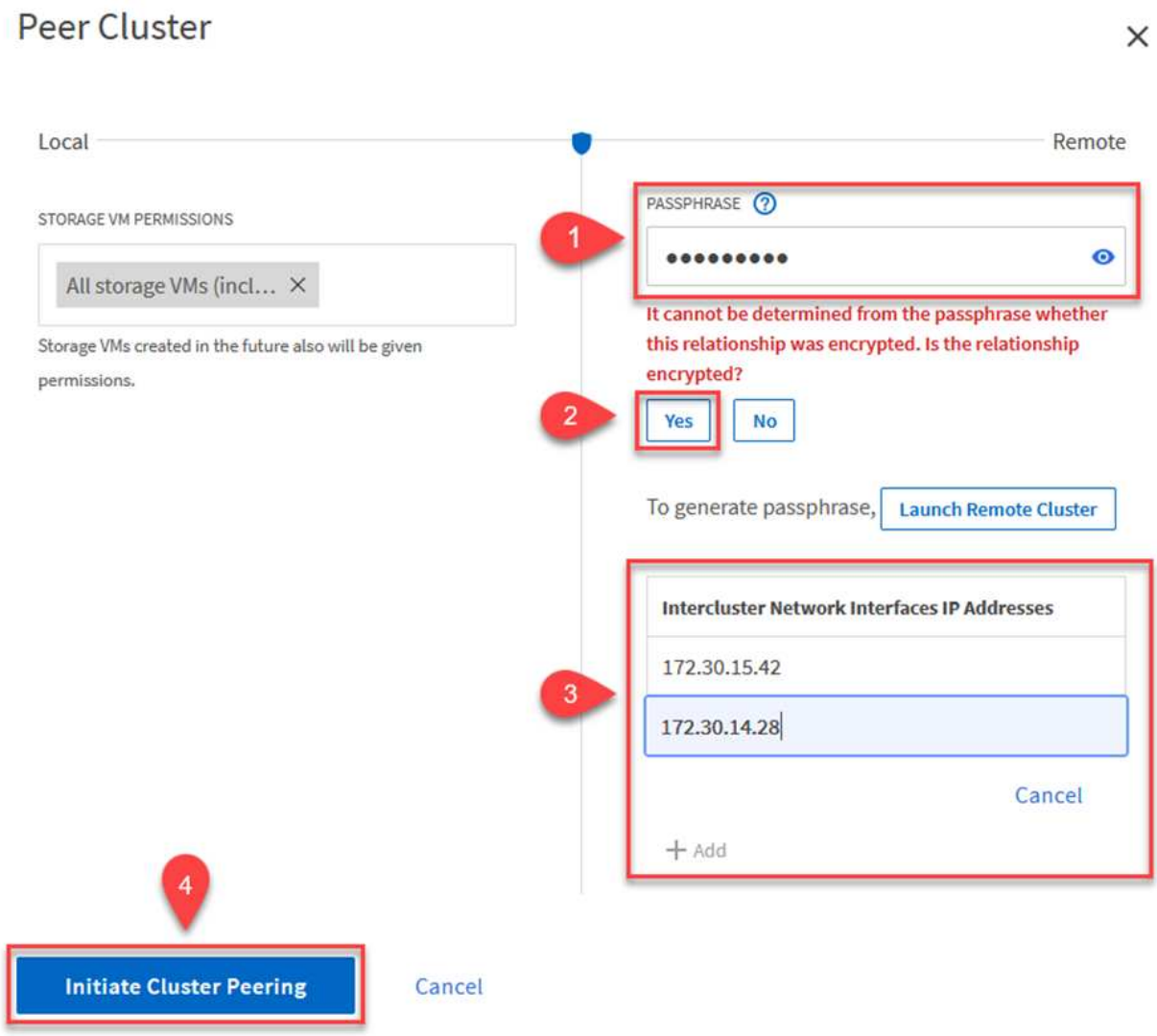
3. Na caixa de diálogo Cluster de Pares, preencha as informações necessárias:
   a. Digite a senha que foi usada para estabelecer o relacionamento do cluster de pares no cluster FSx

de destino.

b. Selecione `Yes` para estabelecer um relacionamento criptografado.

c. Insira o(s) endereço(s) IP do LIF intercluster do cluster FSx 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 FSx com o seguinte comando:

```
FSx-Dest::> cluster peer show
```

```
FsxId0ae40e08acc0dea67::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability   Authentication
------------------------- --------------------- -------------- --------------
E13A300                   1-80-000011           Available      ok
```

▼ **Estabelecer relacionamento de peering SVM**

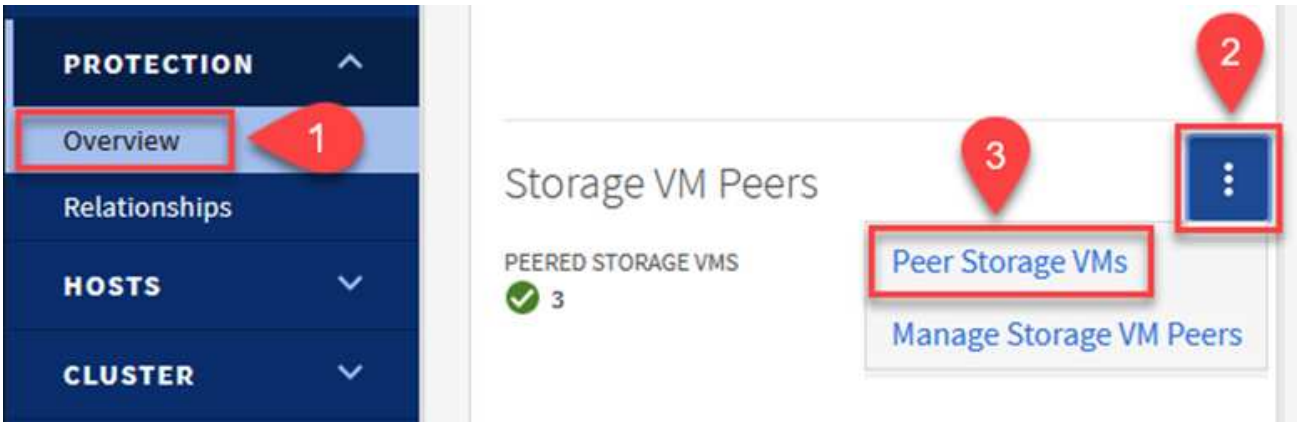
A próxima etapa é configurar um relacionamento SVM entre as máquinas virtuais de armazenamento de

destino e de origem que contêm os volumes que estarão nos relacionamentos SnapMirror .

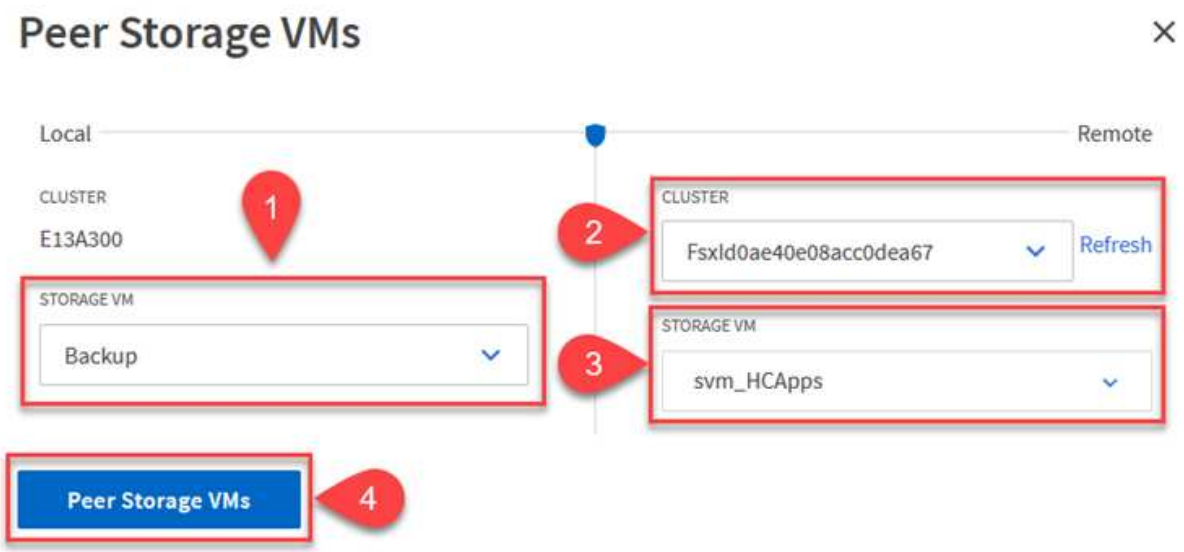
1. No cluster FSx de origem, use o seguinte comando da CLI para criar o relacionamento de pares SVM:

```
FSx-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.

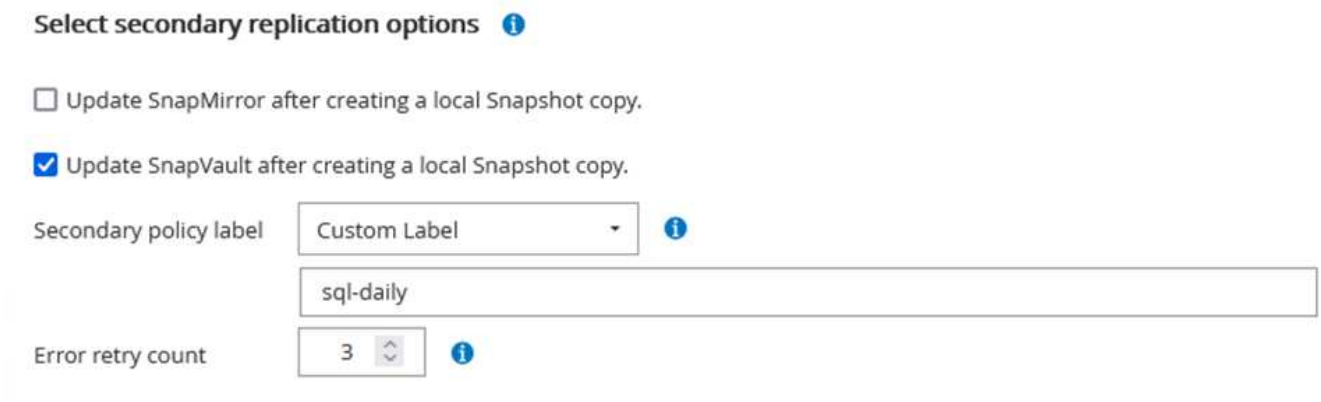
▼ **Crie uma política de retenção de instantâneos**

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.

```
FSx-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 .

```
FSx-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:

```
FSx-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 FSx que será o destinatário de cópias de instantâneos dos nossos volumes de origem, execute o seguinte comando no FSx ONTAP:

```
FSx-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 FSx ONTAP:

```
FSx-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.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Implante e configure o servidor Windows SnapCenter no local.

▼ **Implantar o Windows SnapCenter Server no local**

Esta solução usa o NetApp SnapCenter para fazer backups consistentes de aplicativos de bancos de dados SQL Server e Oracle. Em conjunto com o Veeam Backup & Replication para fazer backup de VMDKs de máquinas virtuais, isso fornece uma solução abrangente de recuperação de desastres para datacenters locais e baseados na nuvem.

O SnapCenter software está disponível no site de suporte da NetApp e pode ser instalado em sistemas Microsoft Windows que residam em um domínio ou grupo de trabalho. Um guia de planejamento detalhado e instruções de instalação podem ser encontrados em "Centro de documentação da NetApp" .

O SnapCenter software pode ser obtido em "este link" .

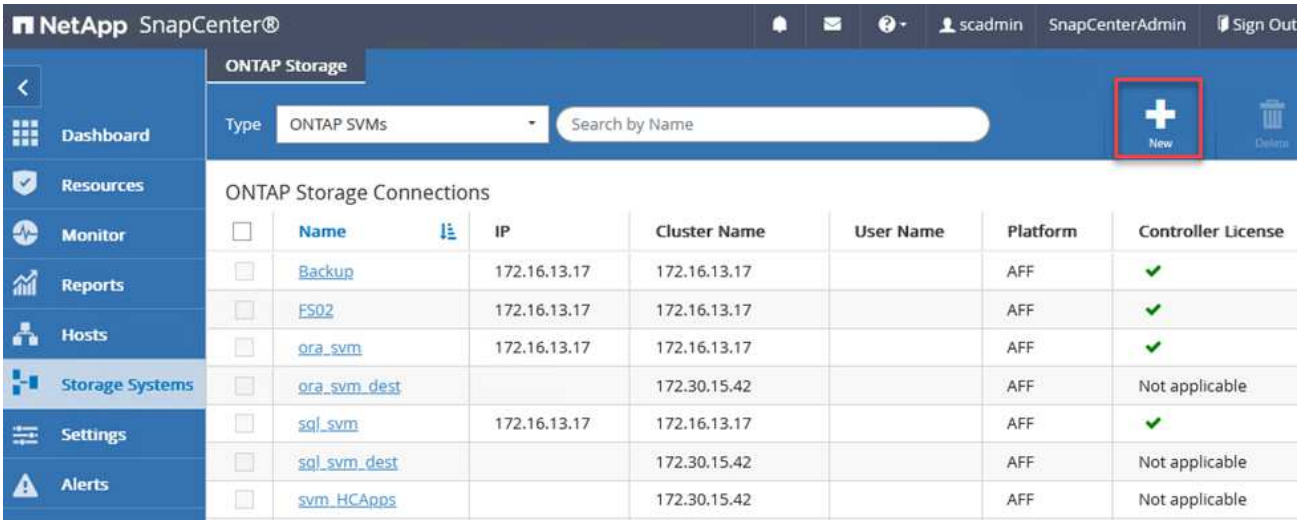
Após a instalação, você pode acessar o console do SnapCenter a partir de um navegador da web usando *https://Virtual_Cluster_IP_or_FQDN:8146*.

Depois de efetuar login no console, você deve configurar o SnapCenter para fazer backup dos bancos de dados SQL Server e Oracle.

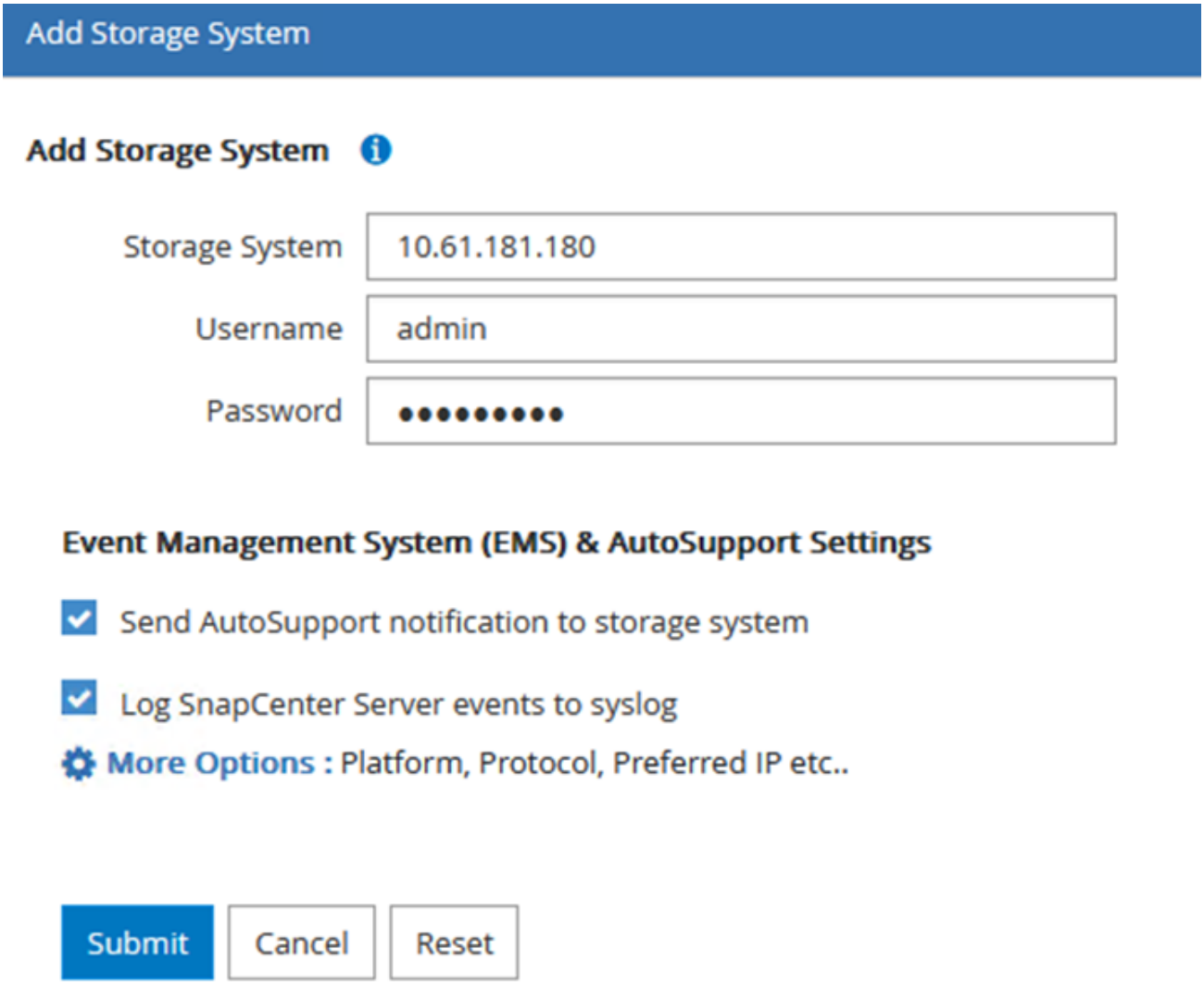
▼ **Adicionar controladores de armazenamento ao SnapCenter**

Para adicionar controladores de armazenamento ao SnapCenter, conclua as seguintes etapas:

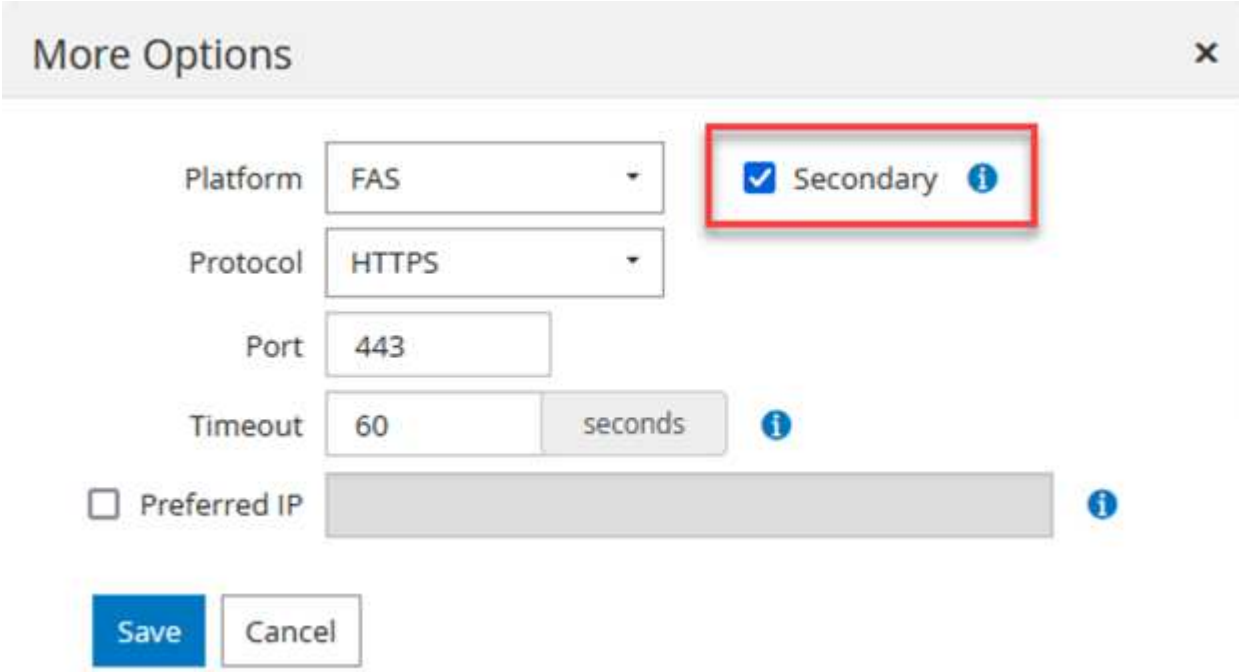
1. No menu à esquerda, selecione Sistemas de armazenamento e clique em Novo para iniciar o processo de adição de seus controladores de armazenamento ao SnapCenter.



2. Na caixa de diálogo Adicionar sistema de armazenamento, adicione o endereço IP de gerenciamento para o cluster ONTAP local, bem como o nome de usuário e a senha. Em seguida, clique em Enviar para iniciar a descoberta do sistema de armazenamento.



3. Repita esse processo para adicionar o sistema FSx ONTAP ao SnapCenter. Nesse caso, selecione Mais opções na parte inferior da janela Adicionar sistema de armazenamento e clique na caixa de seleção Secundário para designar o sistema FSx como o sistema de armazenamento secundário atualizado com cópias do SnapMirror ou nossos instantâneos de backup primários.

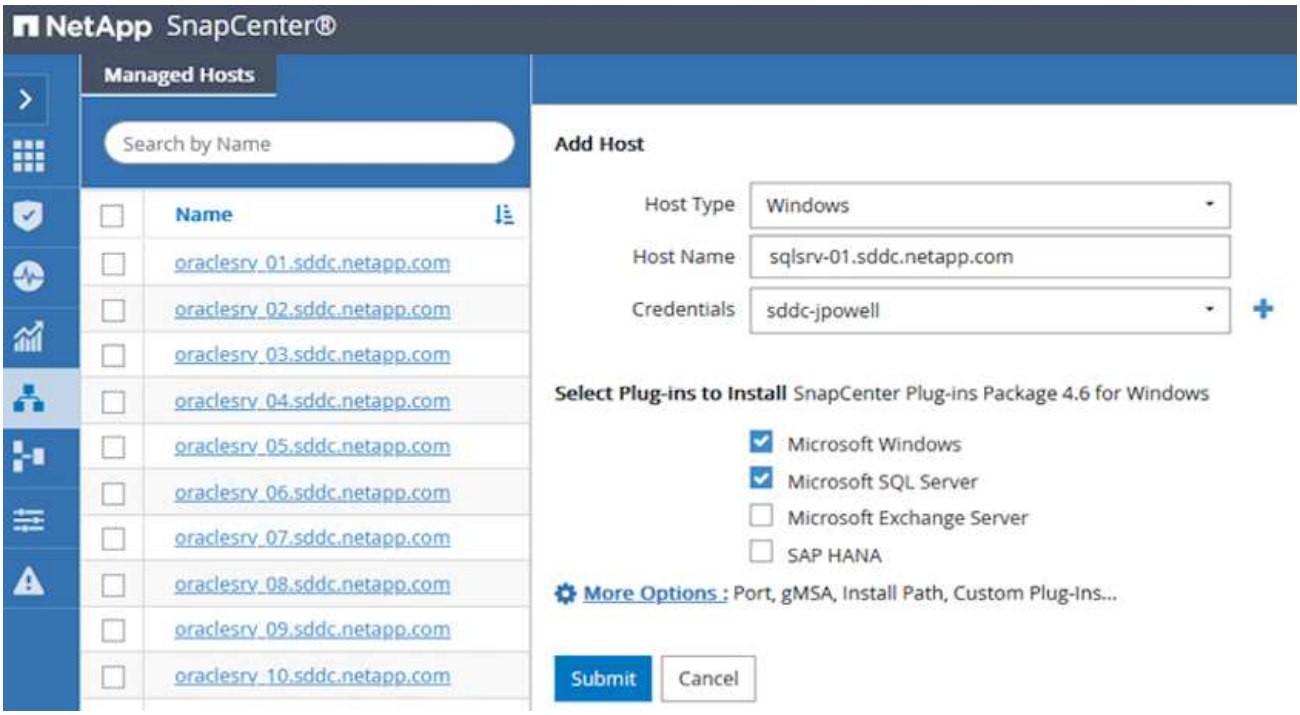


Para obter mais informações relacionadas à adição de sistemas de armazenamento ao SnapCenter, consulte a documentação em "este link" .

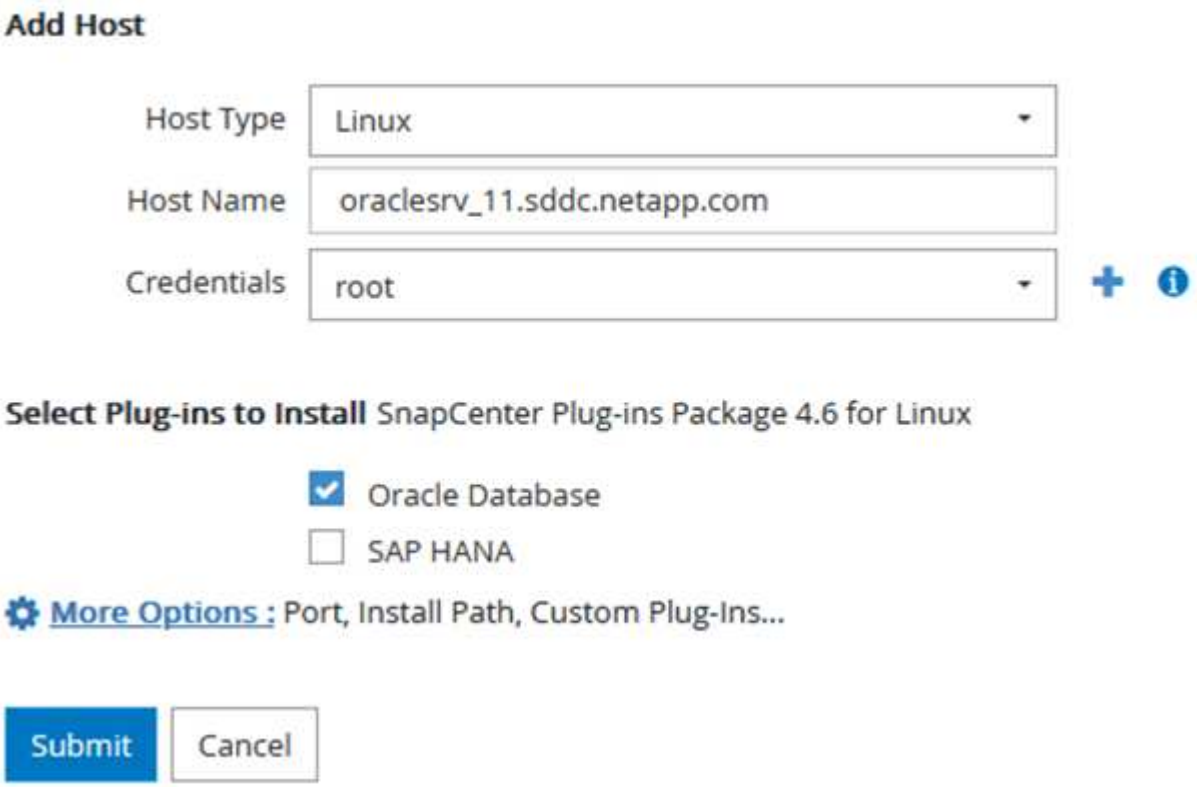
▼ **Adicionar hosts ao SnapCenter**

O próximo passo é adicionar servidores de aplicativos host ao SnapCenter. O processo é semelhante para SQL Server e Oracle.

1. No menu à esquerda, selecione Hosts e clique em Adicionar para iniciar o processo de adição de controladores de armazenamento ao SnapCenter.
2. Na janela Adicionar Hosts, adicione o Tipo de Host, o Nome do Host e as Credenciais do sistema host. Selecione o tipo de plug-in. Para o SQL Server, selecione o plug-in Microsoft Windows e Microsoft SQL Server.



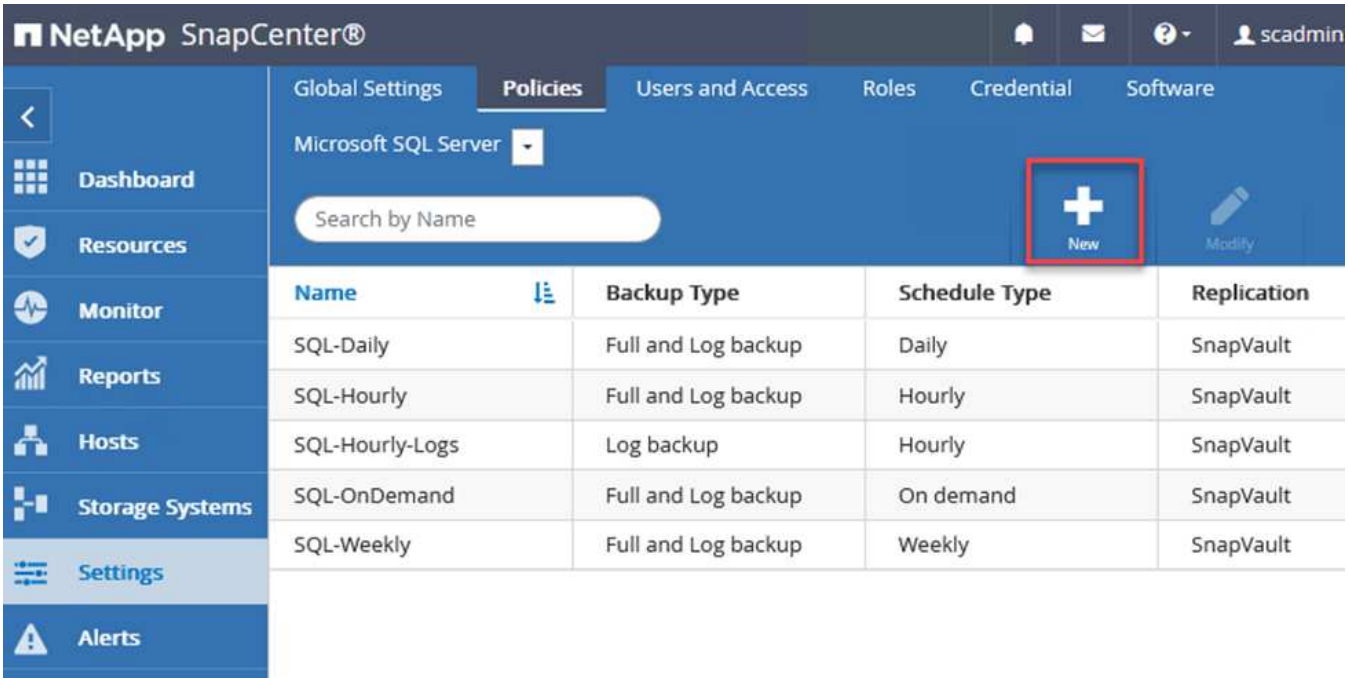
3. Para Oracle, preencha os campos obrigatórios na caixa de diálogo Adicionar Host e marque a caixa de seleção do plug-in do Oracle Database. Em seguida, clique em Enviar para iniciar o processo de descoberta e adicionar o host ao SnapCenter.



▼ **Criar políticas do SnapCenter**

As políticas estabelecem as regras específicas a serem seguidas para uma tarefa de backup. Eles incluem, mas não estão limitados a, o cronograma de backup, o tipo de replicação e como o SnapCenter lida com o backup e o truncamento de logs de transações.

Você pode acessar políticas na seção Configurações do cliente web SnapCenter .



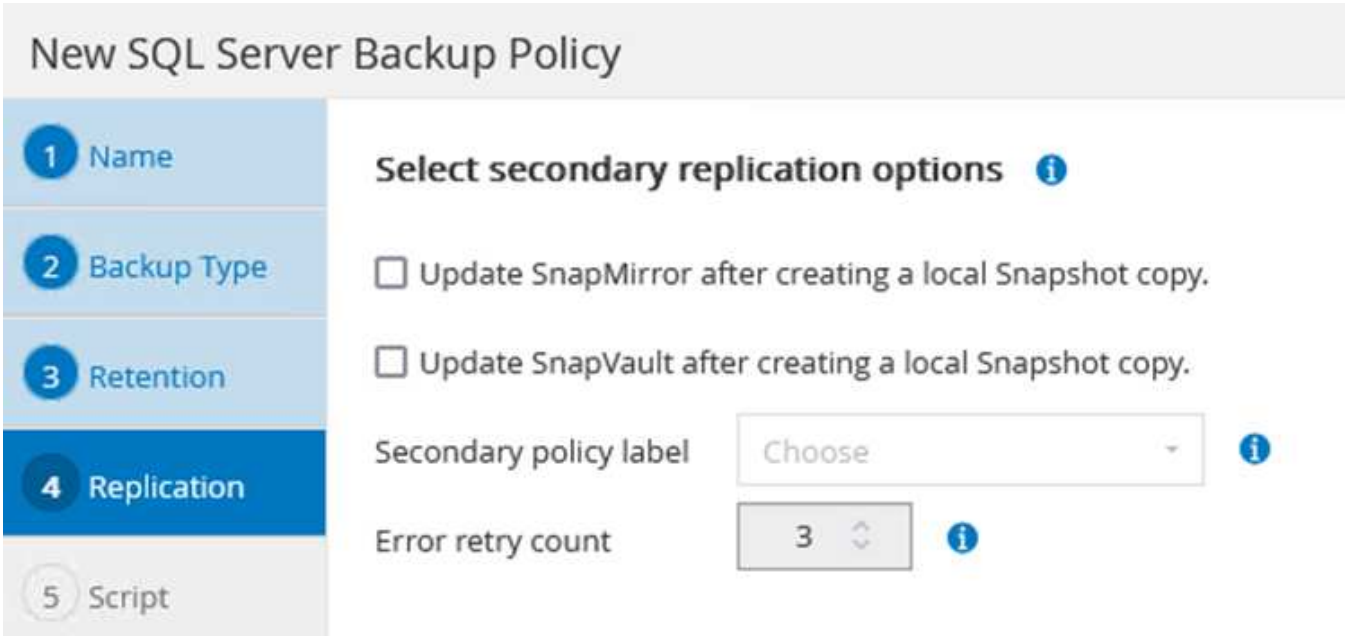
Para obter informações completas sobre a criação de políticas para backups do SQL Server, consulte o "Documentação do SnapCenter" .

Para obter informações completas sobre a criação de políticas para backups do Oracle, consulte o "Documentação do SnapCenter" .

Notas:

- À medida que você avança no assistente de criação de políticas, preste atenção especial à seção Replicação. Nesta seção você estipula os tipos de cópias secundárias do SnapMirror que deseja fazer durante o processo de backup.
- A configuração "Atualizar SnapMirror após criar uma cópia local do Snapshot" refere-se à atualização de um relacionamento SnapMirror quando esse relacionamento existe entre duas máquinas virtuais de armazenamento que residem no mesmo cluster.
- A configuração "Atualizar SnapVault após criar uma cópia local do SnapShot" é usada para atualizar um relacionamento SnapMirror que existe entre dois clusters separados e entre um sistema ONTAP local e o Cloud Volumes ONTAP ou FSx ONTAP.

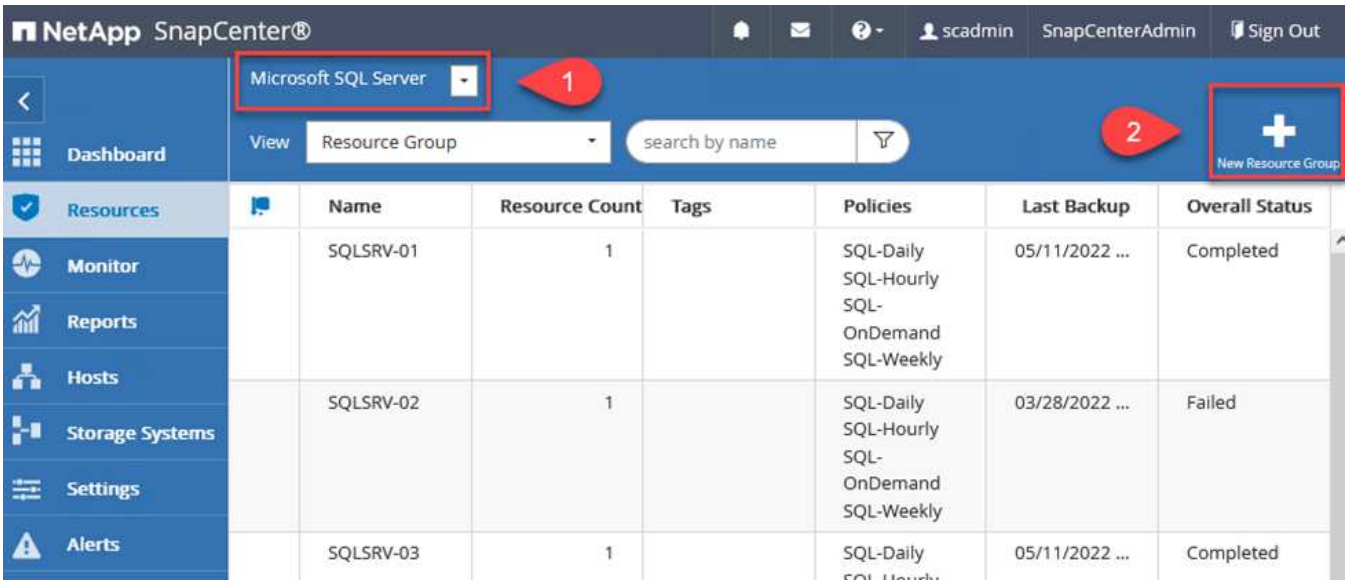
A imagem a seguir mostra as opções anteriores e como elas aparecem no assistente de política de backup.



▼ **Criar grupos de recursos do SnapCenter**

Os Grupos de Recursos permitem que você selecione os recursos de banco de dados que deseja incluir em seus backups e as políticas seguidas para esses recursos.

1. Acesse a seção Recursos no menu à esquerda.
2. Na parte superior da janela, selecione o tipo de recurso com o qual deseja trabalhar (neste caso, Microsoft SQL Server) e clique em Novo Grupo de Recursos.



A documentação do SnapCenter abrange detalhes passo a passo para a criação de Grupos de Recursos para bancos de dados SQL Server e Oracle.

Para fazer backup de recursos SQL, siga "este link" .

Para fazer backup de recursos Oracle, siga "este link" .

Implantar e configurar o Veeam Backup Server

O software Veeam Backup & Replication é usado na solução para fazer backup de nossas máquinas virtuais de aplicativos e arquivar uma cópia dos backups em um bucket do Amazon S3 usando um repositório de backup escalável da Veeam (SOBR). O Veeam é implantado em um servidor Windows nesta solução. Para obter orientações específicas sobre a implantação do Veeam, consulte o "Veeam Help Center Documentação técnica" .

▼ Configurar o repositório de backup de expansão do Veeam

Depois de implantar e licenciar o software, você pode criar um repositório de backup escalável (SOBR) como armazenamento de destino para tarefas de backup. Você também deve incluir um bucket S3 como backup de dados de VM externo para recuperação de desastres.

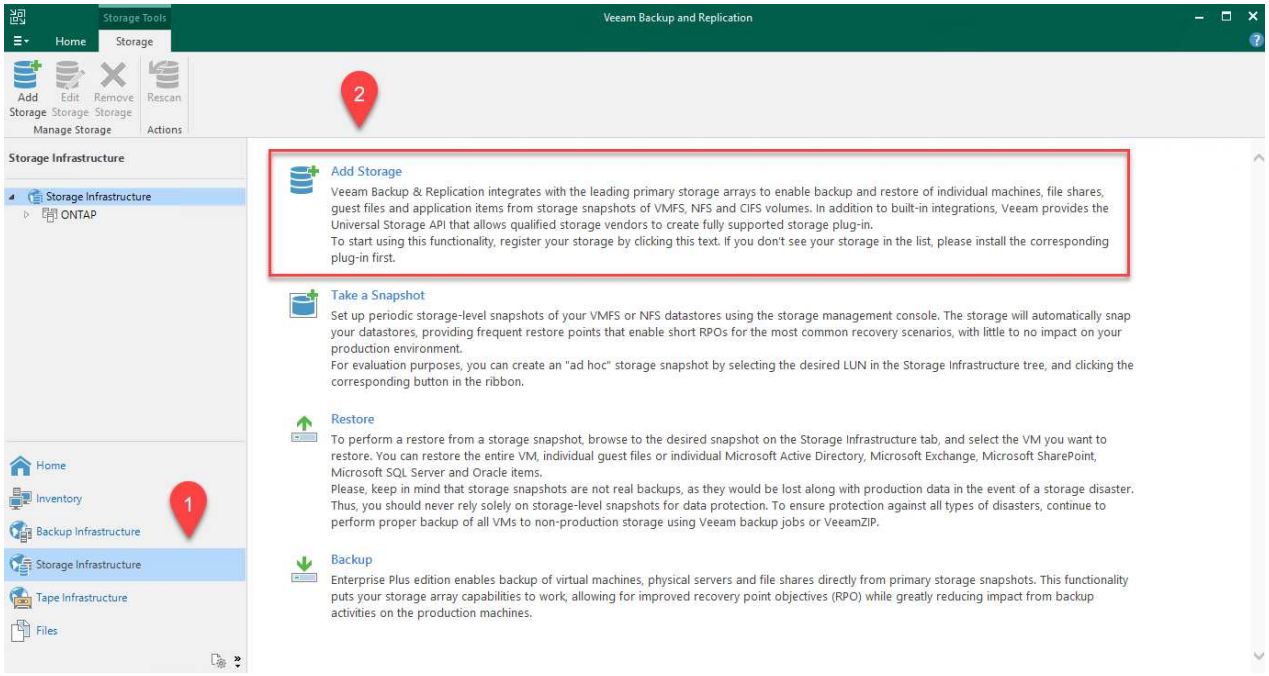
Veja os seguintes pré-requisitos antes de começar.

1. Crie um compartilhamento de arquivos SMB no seu sistema ONTAP local como armazenamento de destino para backups.
2. Crie um bucket do Amazon S3 para incluir no SOBR. Este é um repositório para backups externos.

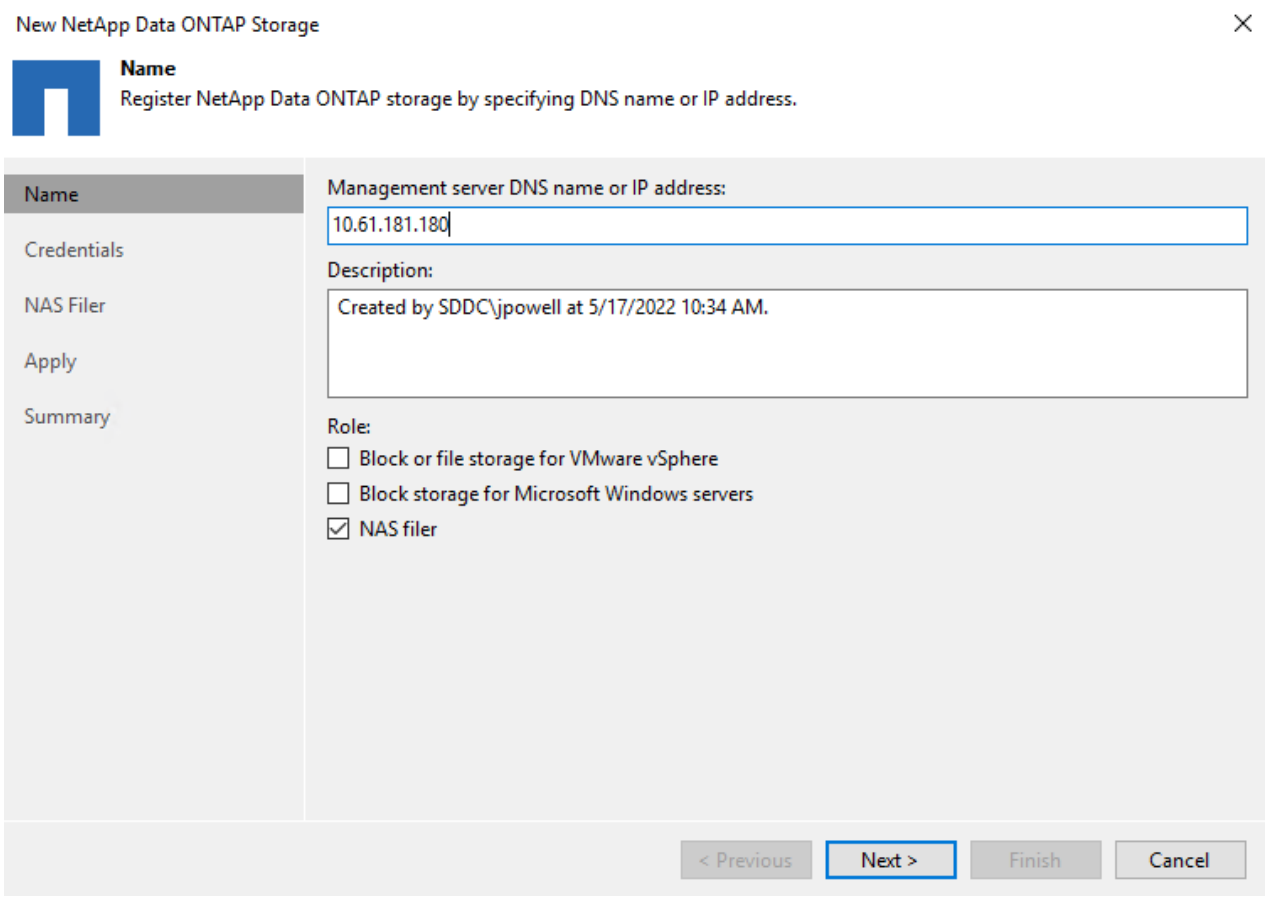
▼ Adicionar armazenamento ONTAP ao Veeam

Primeiro, adicione o cluster de armazenamento ONTAP e o sistema de arquivos SMB/NFS associado como infraestrutura de armazenamento no Veeam.

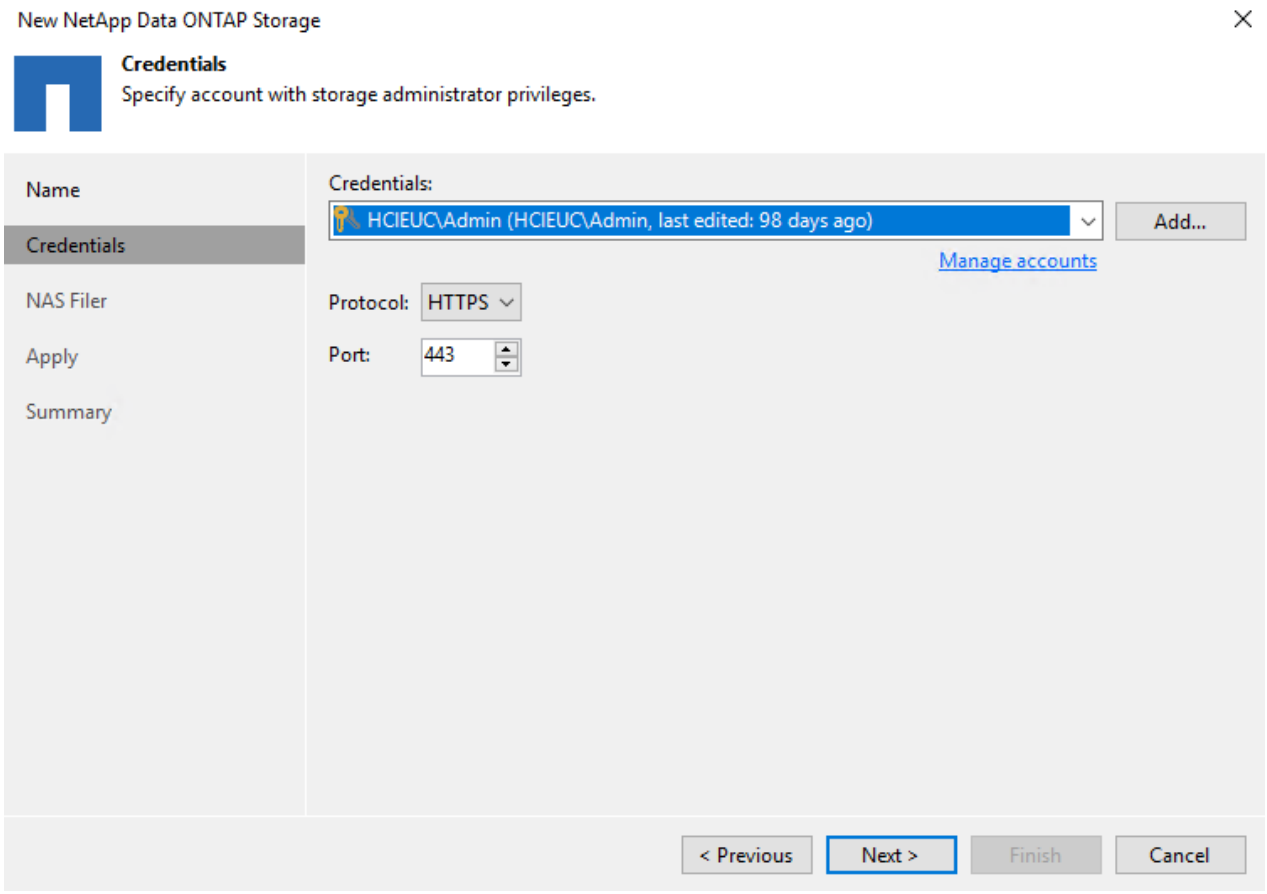
1. Abra o console do Veeam e faça login. Navegue até Infraestrutura de armazenamento e selecione Adicionar armazenamento.



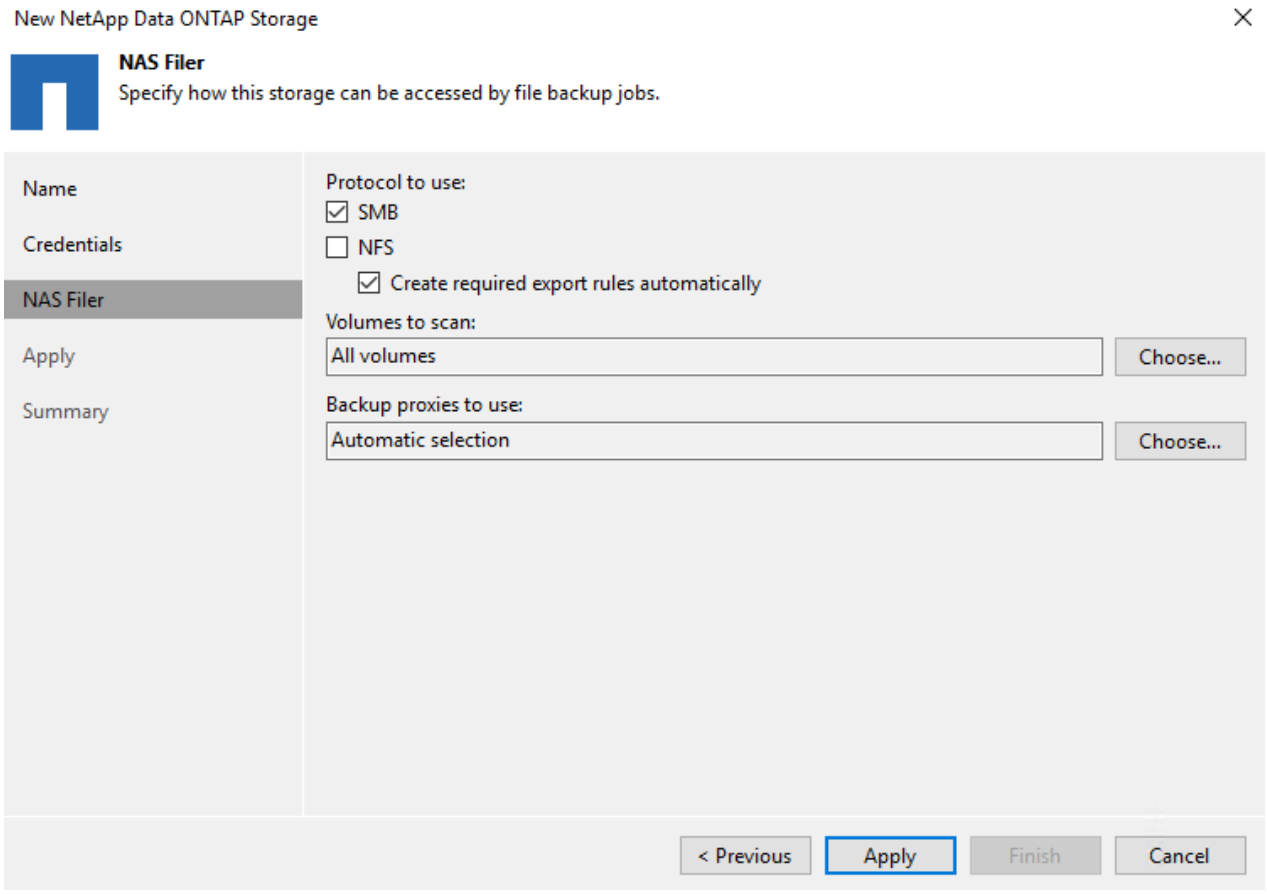
2. No assistente Adicionar armazenamento, selecione NetApp como o fornecedor de armazenamento e, em seguida, selecione Data ONTAP.
3. Digite o endereço IP de gerenciamento e marque a caixa NAS Filer. Clique em Avançar.



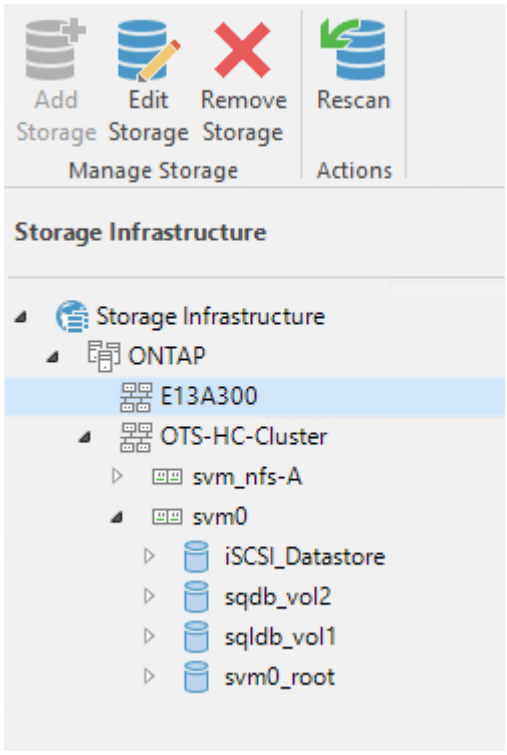
4. Adicione suas credenciais para acessar o cluster ONTAP .



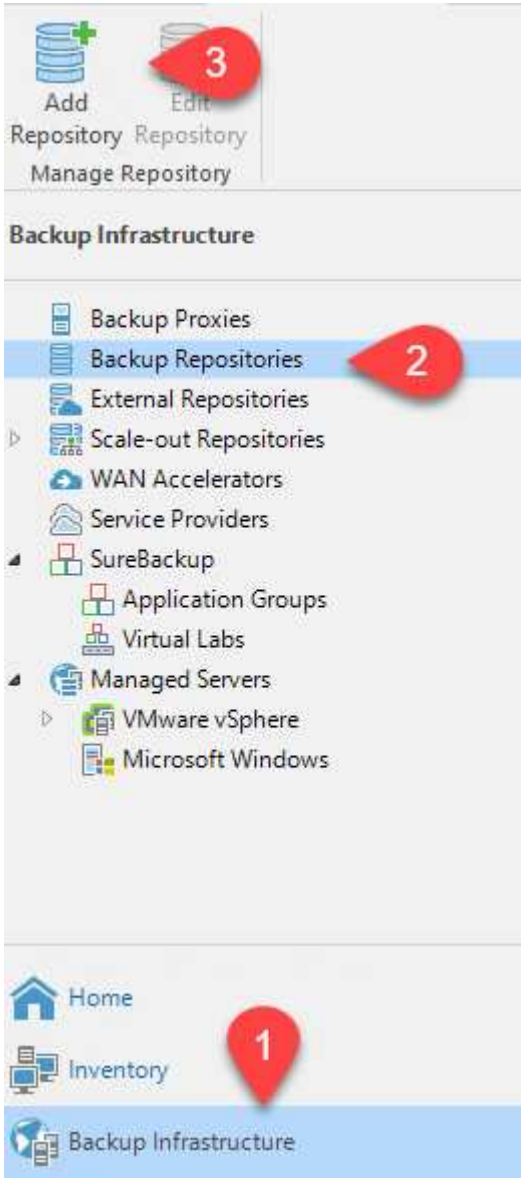
5. Na página NAS Filer, escolha os protocolos desejados para escanear e selecione Avançar.



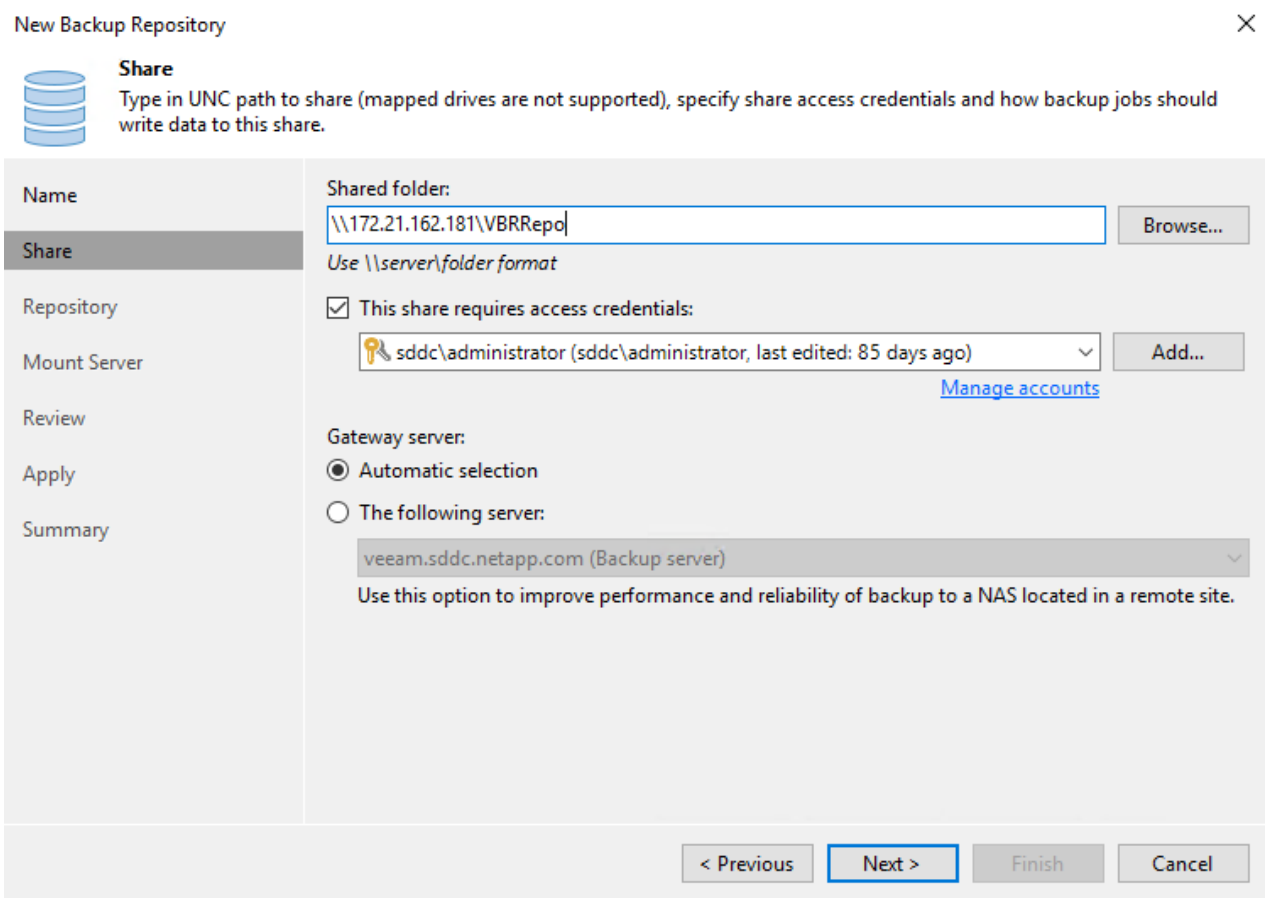
6. Preencha as páginas Aplicar e Resumo do assistente e clique em Concluir para iniciar o processo de descoberta de armazenamento. Após a conclusão da verificação, o cluster ONTAP é adicionado junto com os filtros NAS como recursos disponíveis.



7. Crie um repositório de backup usando os compartilhamentos NAS recém-descobertos. Em Infraestrutura de backup, selecione Repositórios de backup e clique no item de menu Adicionar repositório.



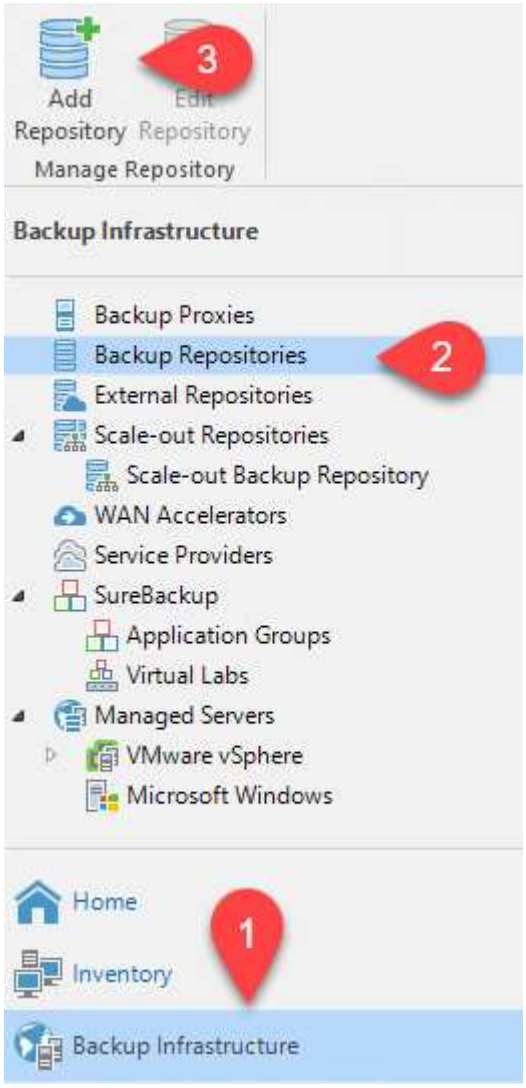
8. Siga todas as etapas do Assistente para Novo Repositório de Backup para criar o repositório. Para obter informações detalhadas sobre a criação de repositórios de backup do Veeam, consulte o "Documentação do Veeam" .



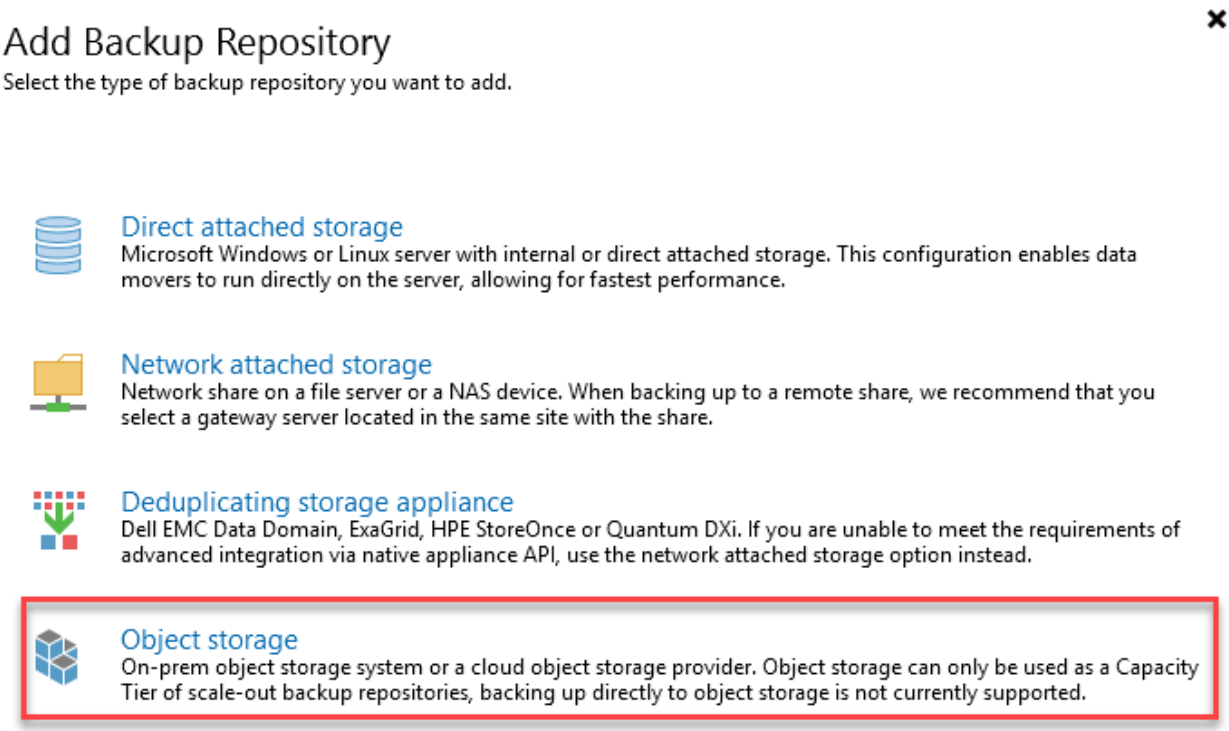
▼ **Adicione o bucket do Amazon S3 como um repositório de backup**

O próximo passo é adicionar o armazenamento do Amazon S3 como um repositório de backup.

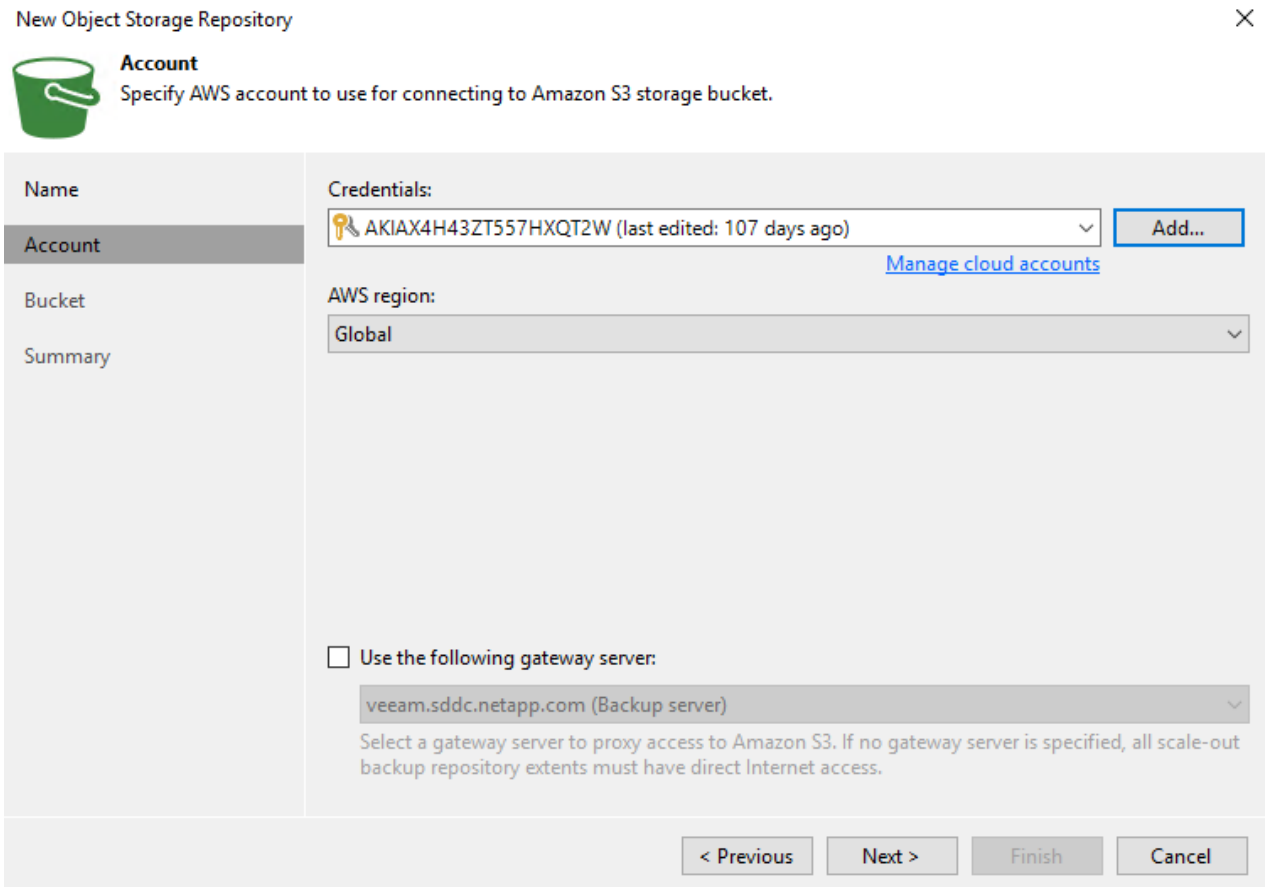
1. Navegue até Infraestrutura de backup > Repositórios de backup. Clique em Adicionar Repositório.



2. No assistente Adicionar repositório de backup, selecione Armazenamento de objetos e depois Amazon S3. Isso inicia o assistente Novo Repositório de Armazenamento de Objetos.



3. Forneça um nome para seu repositório de armazenamento de objetos e clique em Avançar.
4. Na próxima seção, forneça suas credenciais. Você precisa de uma chave de acesso e uma chave secreta da AWS.

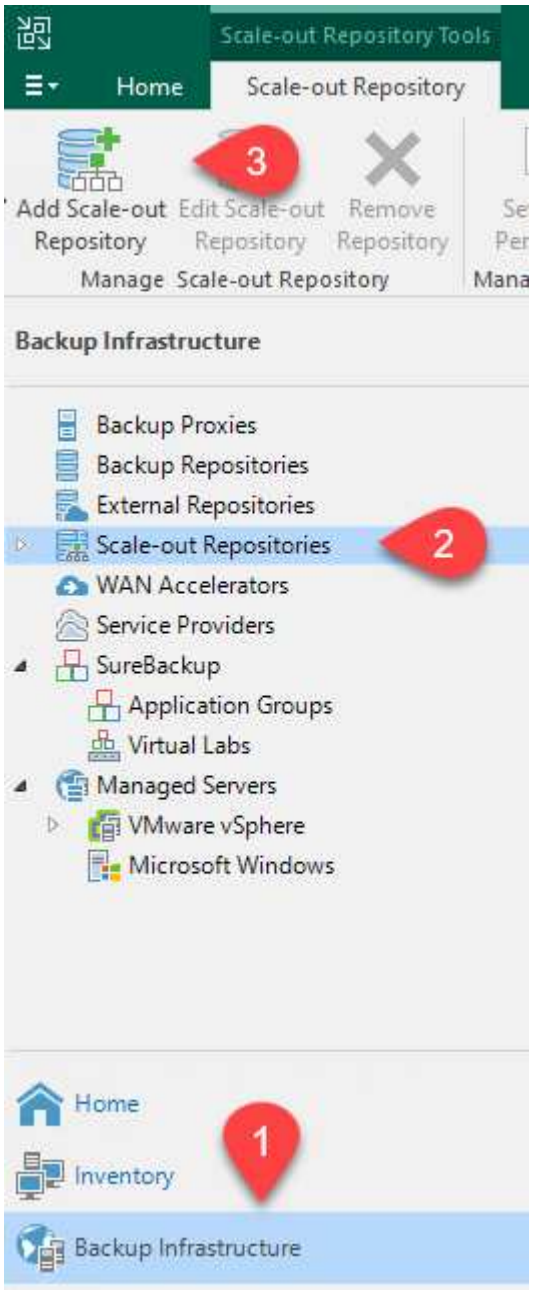


5. Após o carregamento da configuração da Amazon, escolha seu datacenter, bucket e pasta e clique em Aplicar. Por fim, clique em Concluir para fechar o assistente.

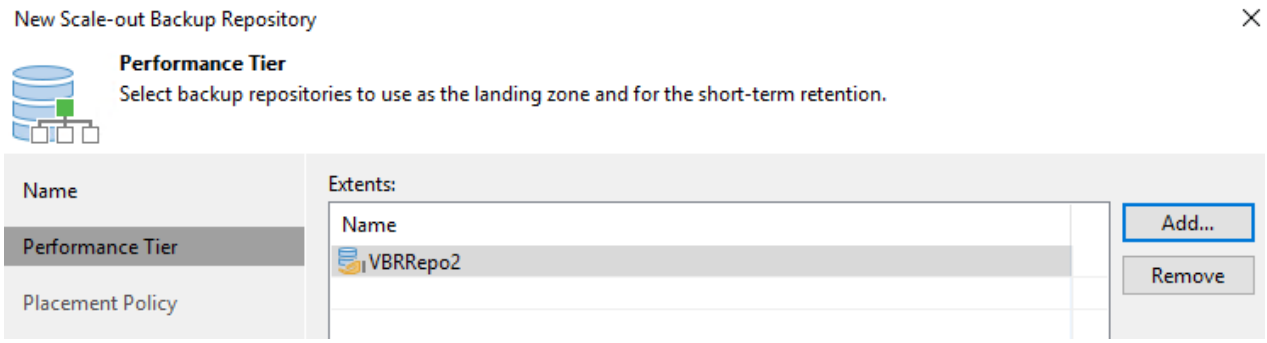
▼ **Criar repositório de backup de expansão**

Agora que adicionamos nossos repositórios de armazenamento ao Veeam, podemos criar o SOBR para automaticamente colocar cópias de backup em camadas em nosso armazenamento de objetos externo do Amazon S3 para recuperação de desastres.

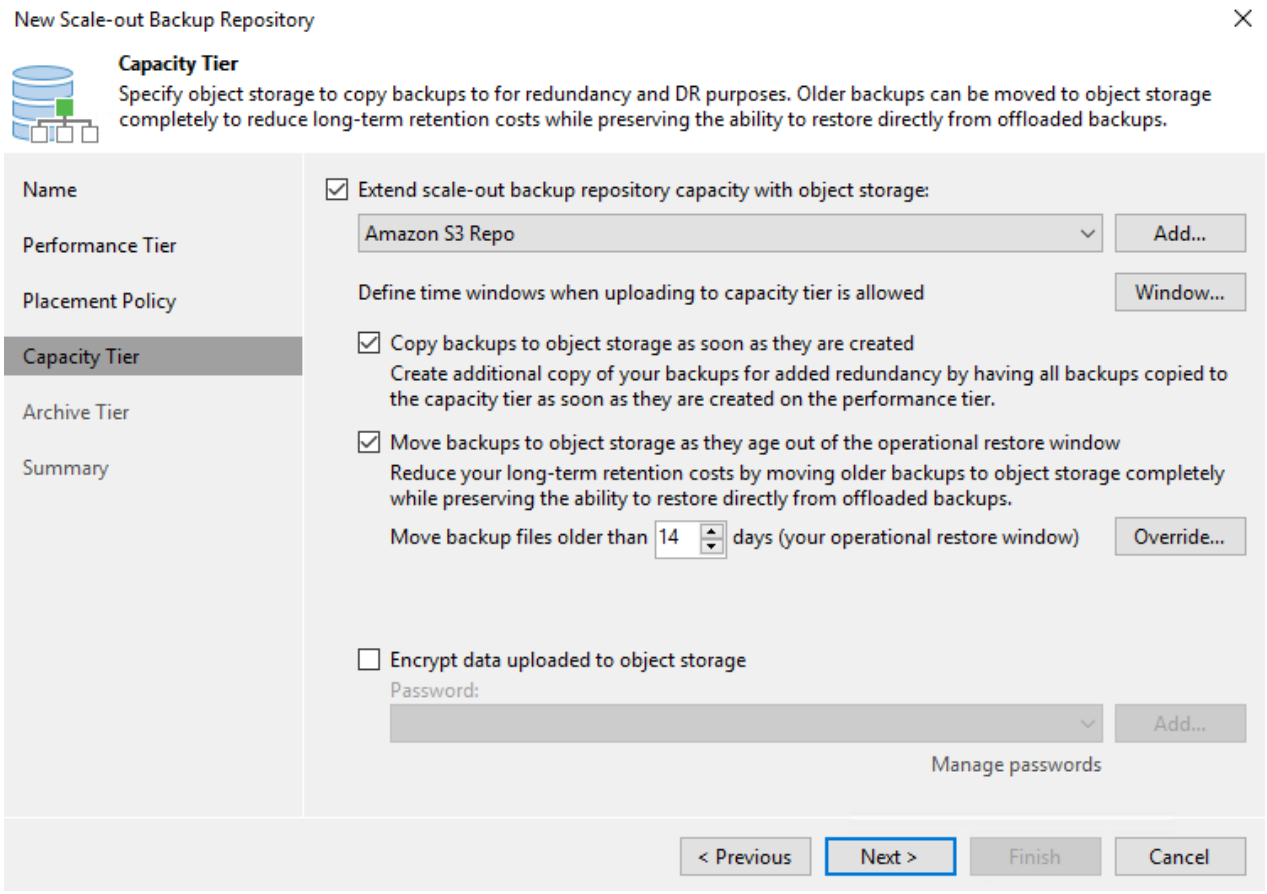
1. Em Infraestrutura de backup, selecione Repositórios de expansão e clique no item de menu Adicionar repositório de expansão.



2. No Novo repositório de backup de expansão, forneça um nome para o SOBR e clique em Avançar.
3. Para o nível de desempenho, escolha o repositório de backup que contém o compartilhamento SMB residente no seu cluster ONTAP local.



4. Para a Política de Posicionamento, escolha Localidade de Dados ou Desempenho com base em suas necessidades. Selecione próximo.
5. Para o nível de capacidade, estendemos o SOBR com o armazenamento de objetos do Amazon S3. Para fins de recuperação de desastres, selecione Copiar backups para o armazenamento de objetos assim que forem criados para garantir a entrega oportuna de nossos backups secundários.



6. Por fim, selecione Aplicar e Concluir para finalizar a criação do SOBR.

▼ Crie os trabalhos de repositório de backup de expansão

A etapa final para configurar o Veeam é criar tarefas de backup usando o SOBR recém-criado como destino de backup. A criação de tarefas de backup é uma parte normal do repertório de qualquer administrador de armazenamento e não abordaremos as etapas detalhadas aqui. Para obter informações mais completas sobre a criação de tarefas de backup no Veeam, consulte o "Documentação técnica da Central de Ajuda da Veeam" .

Ferramentas e configuração do NetApp Backup and Recovery

Para conduzir um failover de VMs de aplicativos e volumes de banco de dados para os serviços do VMware Cloud Volume em execução na AWS, você deve instalar e configurar uma instância em execução do SnapCenter Server e do Veeam Backup and Replication Server. Após a conclusão do failover, você também deve configurar essas ferramentas para retomar as operações normais de backup até que um failback para o datacenter local seja planejado e executado.

▼ **Implantar o Windows SnapCenter Server secundário**

O SnapCenter Server é implantado no VMware Cloud SDDC ou instalado em uma instância EC2 que reside em uma VPC com conectividade de rede com o ambiente VMware Cloud.

O SnapCenter software está disponível no site de suporte da NetApp e pode ser instalado em sistemas Microsoft Windows que residam em um domínio ou grupo de trabalho. Um guia de planejamento detalhado e instruções de instalação podem ser encontrados em "Centro de documentação da NetApp" .

Você pode encontrar o SnapCenter software em "este link" .

▼ **Configurar o Windows SnapCenter Server secundário**

Para executar uma restauração de dados do aplicativo espelhados no FSx ONTAP, você deve primeiro executar uma restauração completa do banco de dados SnapCenter local. Após a conclusão desse processo, a comunicação com as VMs será restabelecida e os backups de aplicativos agora poderão ser retomados usando o FSx ONTAP como armazenamento primário.

Para fazer isso, você deve concluir os seguintes itens no SnapCenter Server:

1. Configure o nome do computador para ser idêntico ao SnapCenter Server local original.
2. Configure a rede para se comunicar com o VMware Cloud e a instância do FSx ONTAP .
3. Conclua o procedimento para restaurar o banco de dados do SnapCenter .
4. Confirme se o SnapCenter está no modo de recuperação de desastres para garantir que o FSx agora seja o armazenamento principal para backups.
5. Confirme se a comunicação foi restabelecida com as máquinas virtuais restauradas.

▼ **Implantar servidor secundário Veeam Backup & Replication**

Você pode instalar o servidor Veeam Backup & Replication em um servidor Windows no VMware Cloud na AWS ou em uma instância EC2. Para obter orientações detalhadas sobre a implementação, consulte o "Documentação técnica da Central de Ajuda da Veeam" .

▼ **Configurar servidor secundário Veeam Backup & Replication**

Para executar uma restauração de máquinas virtuais que foram armazenadas em backup no armazenamento Amazon S3, você deve instalar o Veeam Server em um servidor Windows e configurá-lo para se comunicar com o VMware Cloud, o FSx ONTAP e o bucket S3 que contém o repositório de backup original. Ele também deve ter um novo repositório de backup configurado no FSx ONTAP para conduzir novos backups das VMs após elas serem restauradas.

Para realizar este processo, os seguintes itens devem ser preenchidos:

1. Configure a rede para se comunicar com o VMware Cloud, o FSx ONTAP e o bucket S3 que contém o repositório de backup original.
2. Configure um compartilhamento SMB no FSx ONTAP para ser um novo repositório de backup.
3. Monte o bucket S3 original que foi usado como parte do repositório de backup de expansão no local.

4. Após restaurar a VM, estabeleça novas tarefas de backup para proteger as VMs SQL e Oracle.

Para obter mais informações sobre como restaurar VMs usando o Veeam, consulte a seção"Restaurar VMs de aplicativos com o Veeam Full Restore" .

Backup de banco de dados SnapCenter para recuperação de desastres

O SnapCenter permite o backup e a recuperação do banco de dados MySQL subjacente e dos dados de configuração para fins de recuperação do servidor SnapCenter em caso de desastre. Para nossa solução, recuperamos o banco de dados e a configuração do SnapCenter em uma instância do AWS EC2 residente em nossa VPC. Para obter mais informações sobre a recuperação de desastres do SnapCenter, consulte "este link" .

▼ Pré-requisitos de backup do SnapCenter

Os seguintes pré-requisitos são necessários para o backup do SnapCenter :

- Um volume e compartilhamento SMB criados no sistema ONTAP local para localizar o banco de dados de backup e os arquivos de configuração.
- Um relacionamento SnapMirror entre o sistema ONTAP local e o FSx ou CVO na conta da AWS. Esse relacionamento é usado para transportar o snapshot que contém o banco de dados SnapCenter e os arquivos de configuração com backup.
- Windows Server instalado na conta de nuvem, em uma instância EC2 ou em uma VM no VMware Cloud SDDC.
- SnapCenter instalado na instância do Windows EC2 ou VM no VMware Cloud.

▼ Resumo do processo de backup e restauração do SnapCenter

- Crie um volume no sistema ONTAP local para hospedar o banco de dados de backup e os arquivos de configuração.
- Configure um relacionamento SnapMirror entre o ambiente local e o FSx/CVO.
- Monte o compartilhamento SMB.
- Recupere o token de autorização do Swagger para executar tarefas de API.
- Inicie o processo de restauração do banco de dados.
- Use o utilitário xcopy para copiar o banco de dados e o arquivo de configuração do diretório local para o compartilhamento SMB.
- No FSx, crie um clone do volume ONTAP (copiado via SnapMirror do local).
- Monte o compartilhamento SMB do FSx no EC2/VMware Cloud.
- Copie o diretório de restauração do compartilhamento SMB para um diretório local.
- Execute o processo de restauração do SQL Server pelo Swagger.

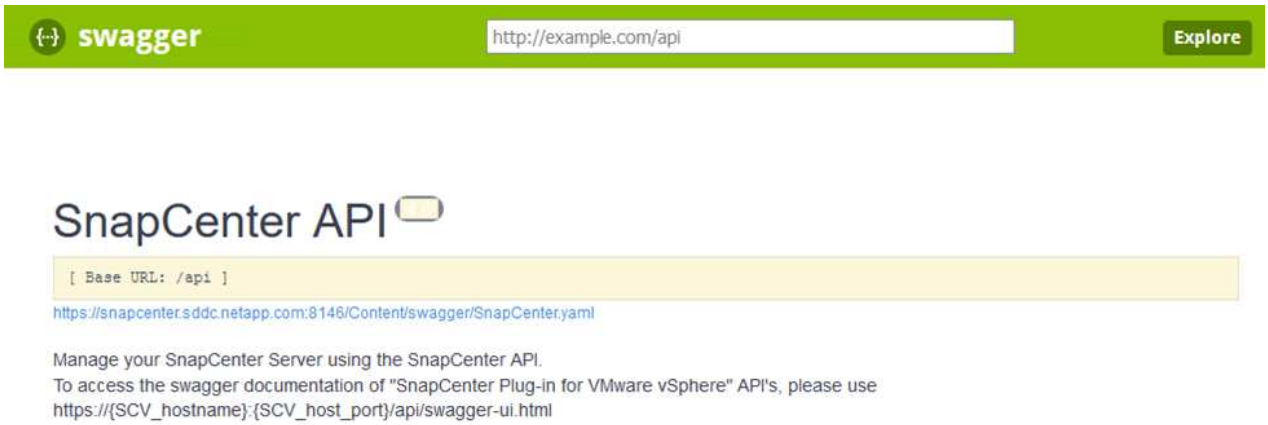
▼ Faça backup do banco de dados e da configuração do SnapCenter

O SnapCenter fornece uma interface de cliente web para executar comandos REST API. Para obter informações sobre como acessar as APIs REST por meio do Swagger, consulte a documentação do SnapCenter em "este link" .

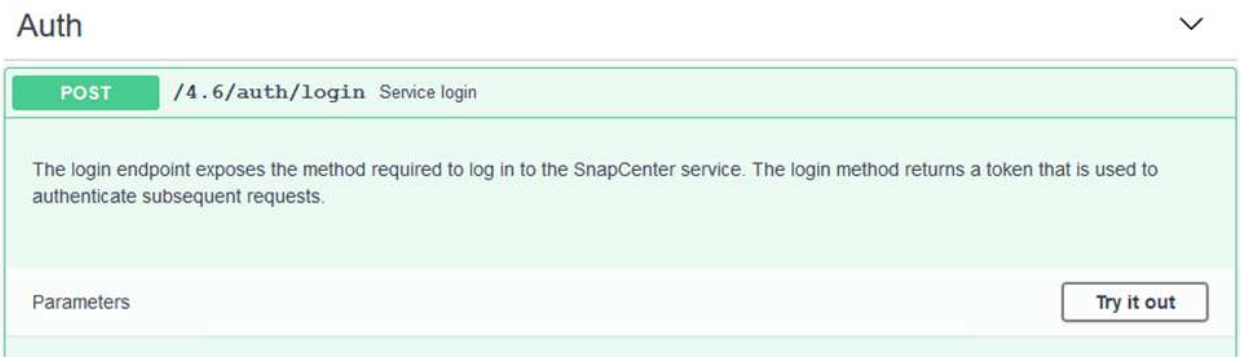
▼ Faça login no Swagger e obtenha o token de autorização

Depois de navegar até a página do Swagger, você deve recuperar um token de autorização para iniciar o processo de restauração do banco de dados.

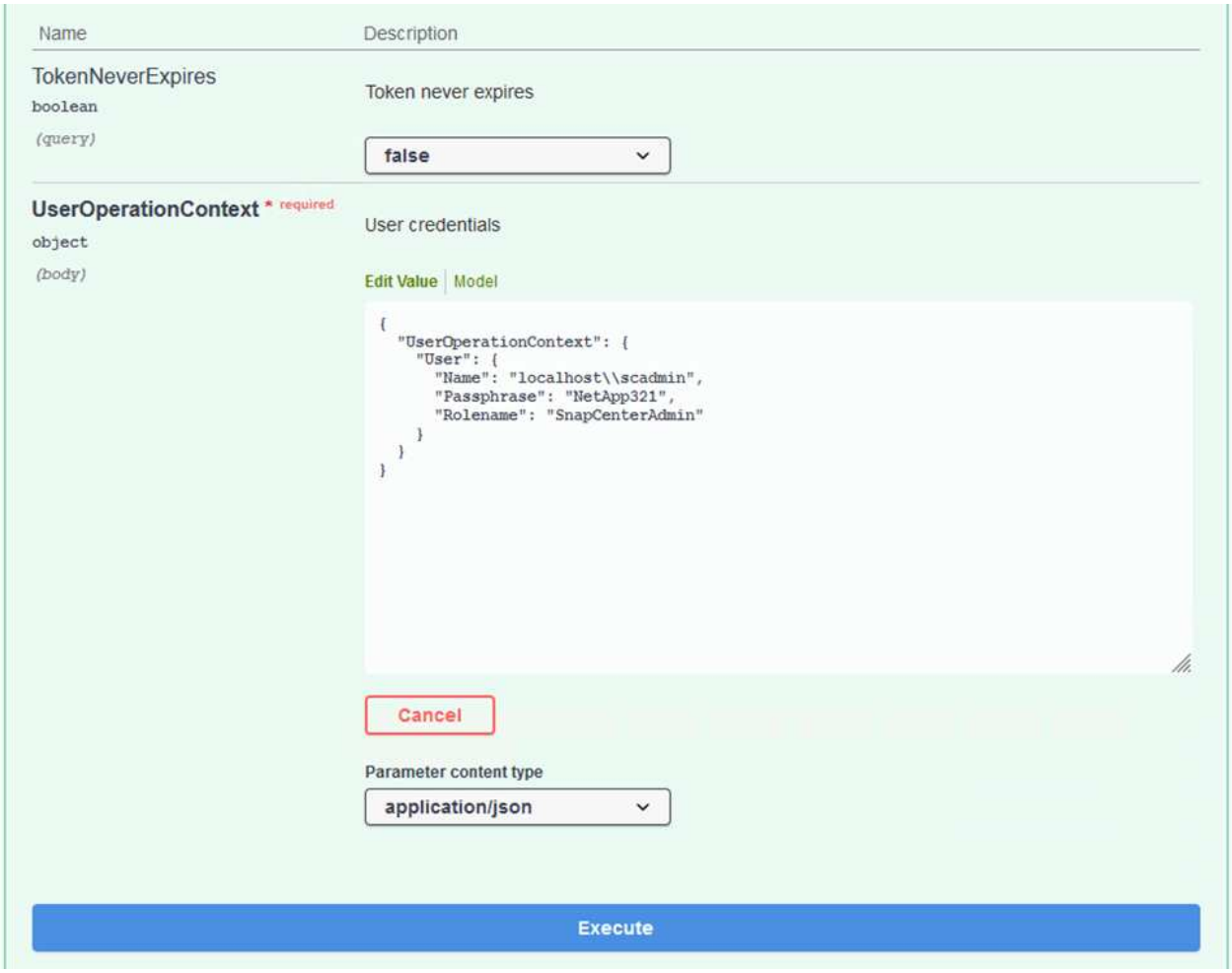
1. Acesse a página da API do SnapCenter Swagger em *https://< IP do servidor SnapCenter >:8146/swagger/*.



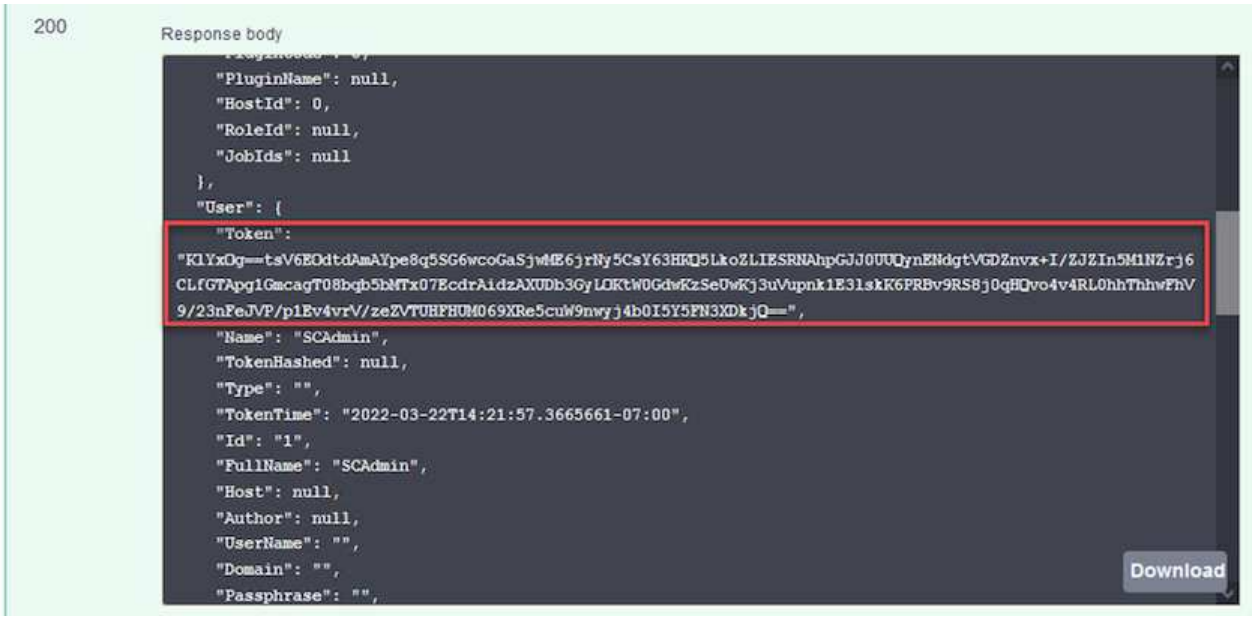
2. Expanda a seção Aut. e clique em Experimentar.



3. Na área UserOperationContext, preencha as credenciais e a função do SnapCenter e clique em Executar.



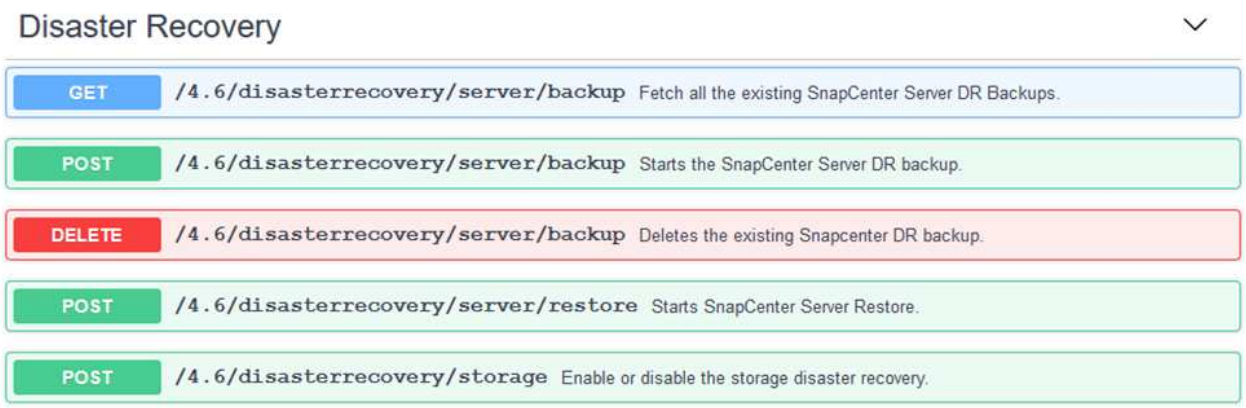
4. No corpo da resposta abaixo, você pode ver o token. Copie o texto do token para autenticação ao executar o processo de backup.



▼ **Executar um backup do banco de dados SnapCenter**

Em seguida, vá para a área Recuperação de desastres na página do Swagger para iniciar o processo de backup do SnapCenter .

1. Expanda a área Recuperação de Desastres clicando nela.

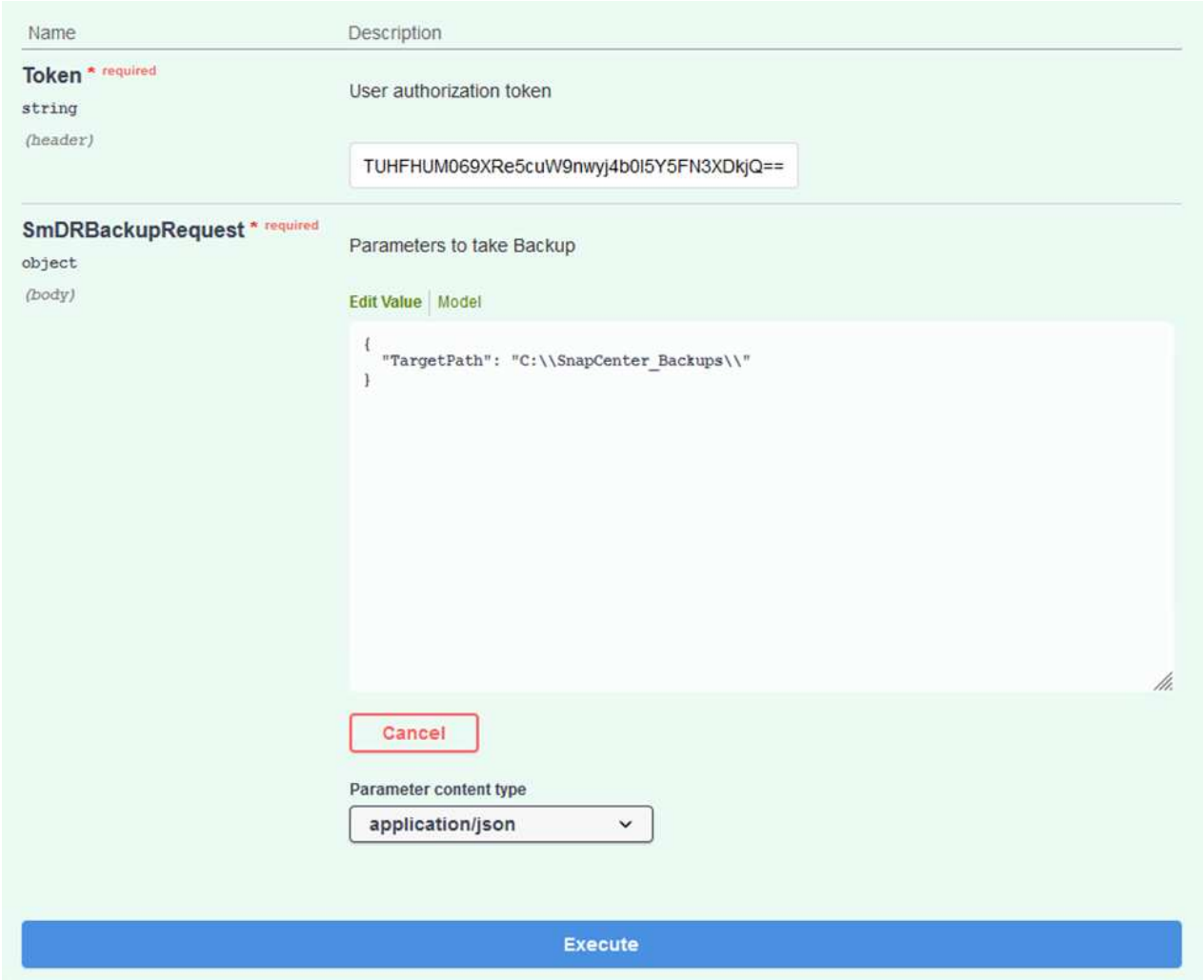


2. Expandir o `/4.6/disasterrecovery/server/backup` seção e clique em Experimentar.



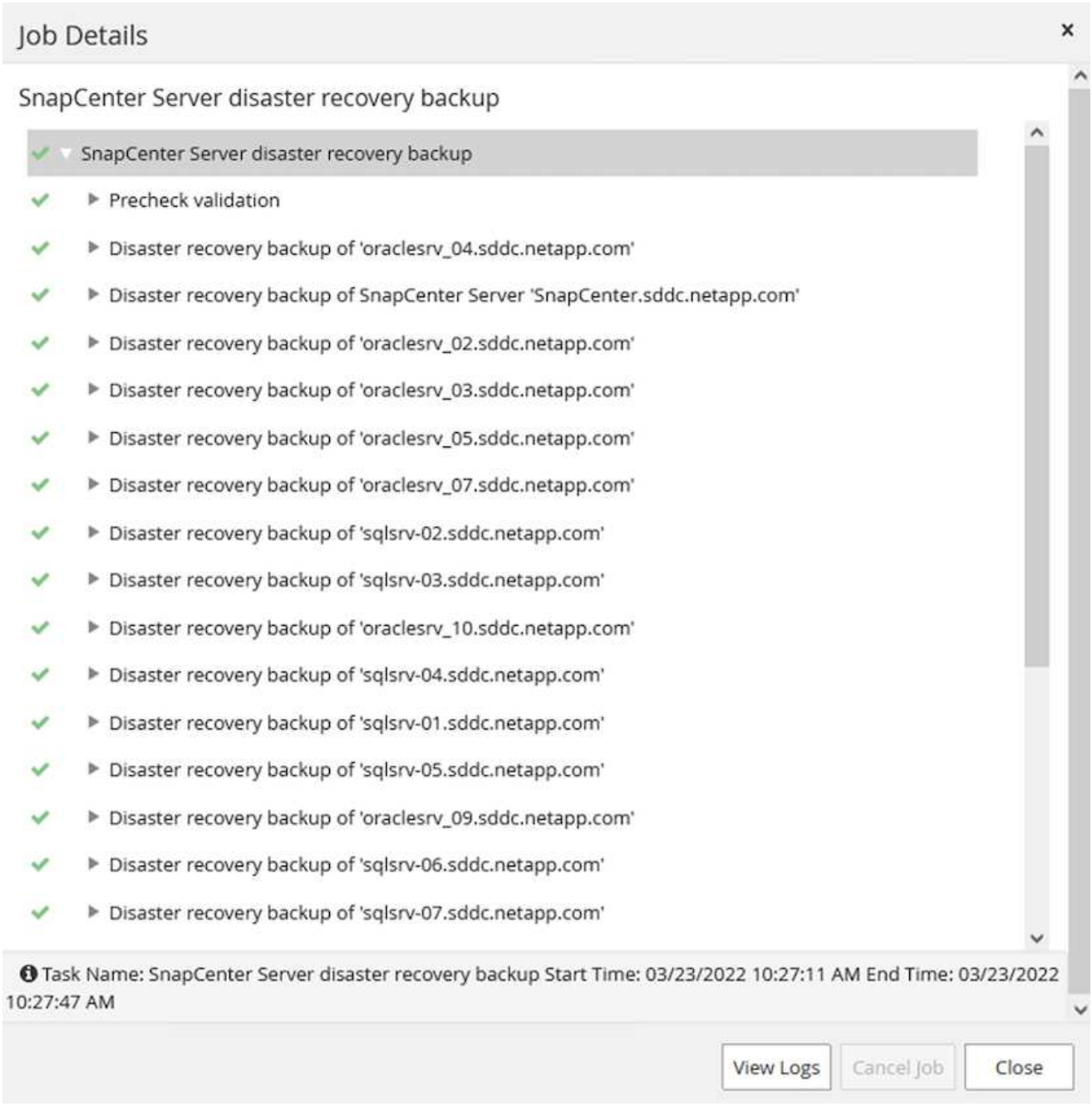
3. Na seção SmDRBackupRequest, adicione o caminho de destino local correto e selecione Executar para iniciar o backup do banco de dados e da configuração do SnapCenter .

> O processo de backup não permite fazer backup diretamente em um compartilhamento de arquivos NFS ou CIFS.



▼ **Monitore o trabalho de backup do SnapCenter**

Efetue login no SnapCenter para revisar os arquivos de log ao iniciar o processo de restauração do banco de dados. Na seção Monitor, você pode visualizar os detalhes do backup de recuperação de desastres do servidor SnapCenter .



▼ Use o utilitário XCOPY para copiar o arquivo de backup do banco de dados para o compartilhamento SMB

Em seguida, você deve mover o backup da unidade local no servidor SnapCenter para o compartilhamento CIFS que é usado para copiar os dados do SnapMirror para o local secundário localizado na instância do FSx na AWS. Use xcopy com opções específicas que retêm as permissões dos arquivos.

Abra um prompt de comando como Administrador. No prompt de comando, digite os seguintes comandos:

```
xcopy  <Source_Path>  \\<Destination_Server_IP>\<Folder_Path> /O /X /E
/H /K
xcopy c:\SC_Backups\SnapCenter_DR \\10.61.181.185\snapcenter_dr /O /X
```

```
/E /H /K
```

Failover

▼ O desastre ocorre no local primário

Para um desastre que ocorre no datacenter principal local, nosso cenário inclui failover para um site secundário que reside na infraestrutura da Amazon Web Services usando o VMware Cloud na AWS. Presumimos que as máquinas virtuais e nosso cluster ONTAP local não estão mais acessíveis. Além disso, as máquinas virtuais SnapCenter e Veeam não estão mais acessíveis e precisam ser reconstruídas em nosso site secundário.

Esta seção aborda o failover da nossa infraestrutura para a nuvem e abordamos os seguintes tópicos:

- Restauração de banco de dados SnapCenter . Depois que um novo servidor SnapCenter for estabelecido, restaure o banco de dados MySQL e os arquivos de configuração e coloque o banco de dados no modo de recuperação de desastres para permitir que o armazenamento FSx secundário se torne o dispositivo de armazenamento primário.
- Restaure as máquinas virtuais do aplicativo usando o Veeam Backup & Replication. Conecte o armazenamento S3 que contém os backups da VM, importe os backups e restaure-os no VMware Cloud na AWS.
- Restaure os dados do aplicativo SQL Server usando o SnapCenter.
- Restaure os dados do aplicativo Oracle usando o SnapCenter.

▼ Processo de restauração do banco de dados SnapCenter

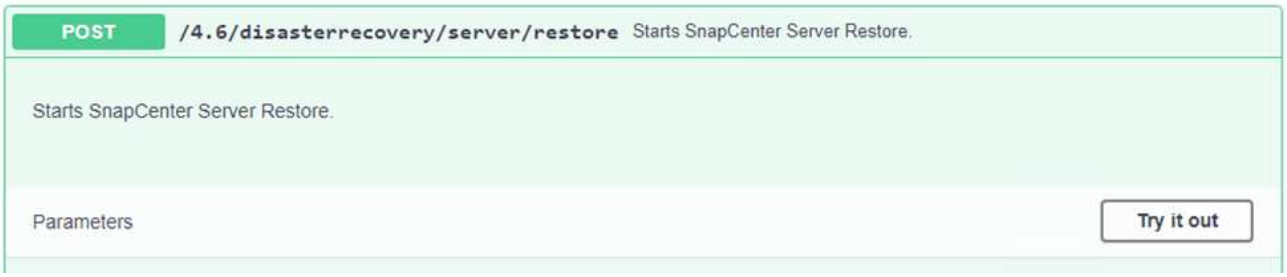
O SnapCenter oferece suporte a cenários de recuperação de desastres, permitindo o backup e a restauração de seu banco de dados MySQL e arquivos de configuração. Isso permite que um administrador mantenha backups regulares do banco de dados SnapCenter no datacenter local e depois restaure esse banco de dados em um banco de dados SnapCenter secundário.

Para acessar os arquivos de backup do SnapCenter no servidor SnapCenter remoto, conclua as seguintes etapas:

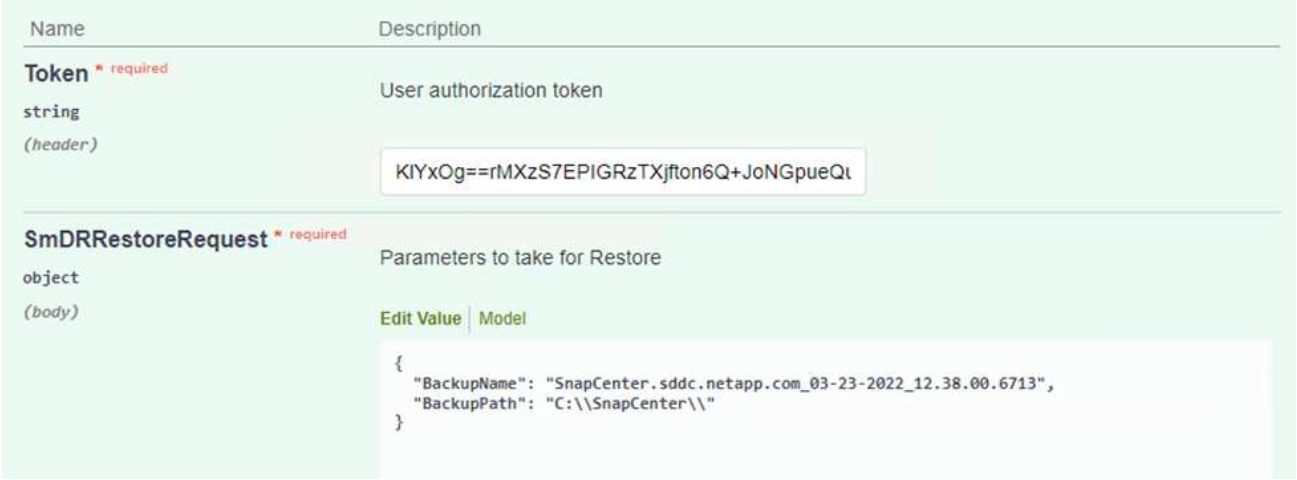
1. Interrompa o relacionamento do SnapMirror com o cluster FSx, o que torna o volume de leitura/gravação.
2. Crie um servidor CIFS (se necessário) e crie um compartilhamento CIFS apontando para o caminho de junção do volume clonado.
3. Use xcopy para copiar os arquivos de backup para um diretório local no sistema SnapCenter secundário.
4. Instale o SnapCenter v4.6.
5. Certifique-se de que o servidor SnapCenter tenha o mesmo FQDN do servidor original. Isso é necessário para que a restauração do banco de dados seja bem-sucedida.

Para iniciar o processo de restauração, conclua as seguintes etapas:

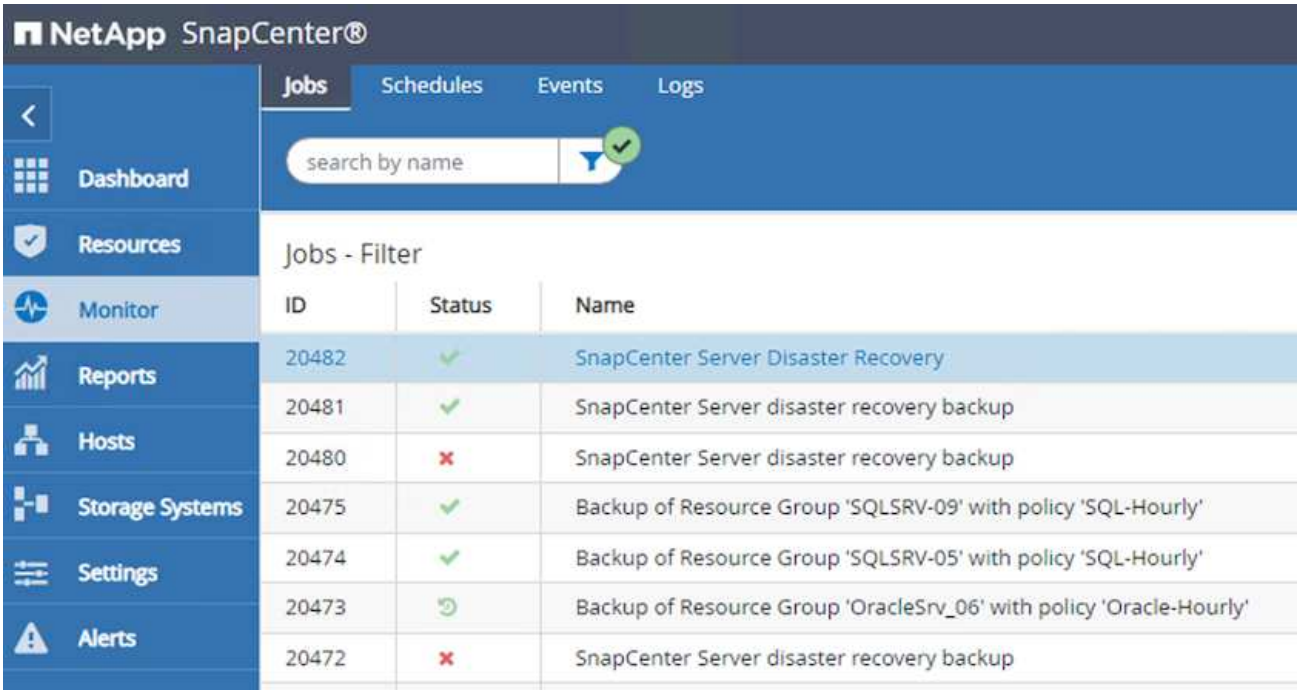
1. Navegue até a página da web da API do Swagger para o servidor SnapCenter secundário e siga as instruções anteriores para obter um token de autorização.
2. Navegue até a seção Recuperação de Desastres da página Swagger, selecione `/4.6/disasterrecovery/server/restore` e clique em Experimentar.

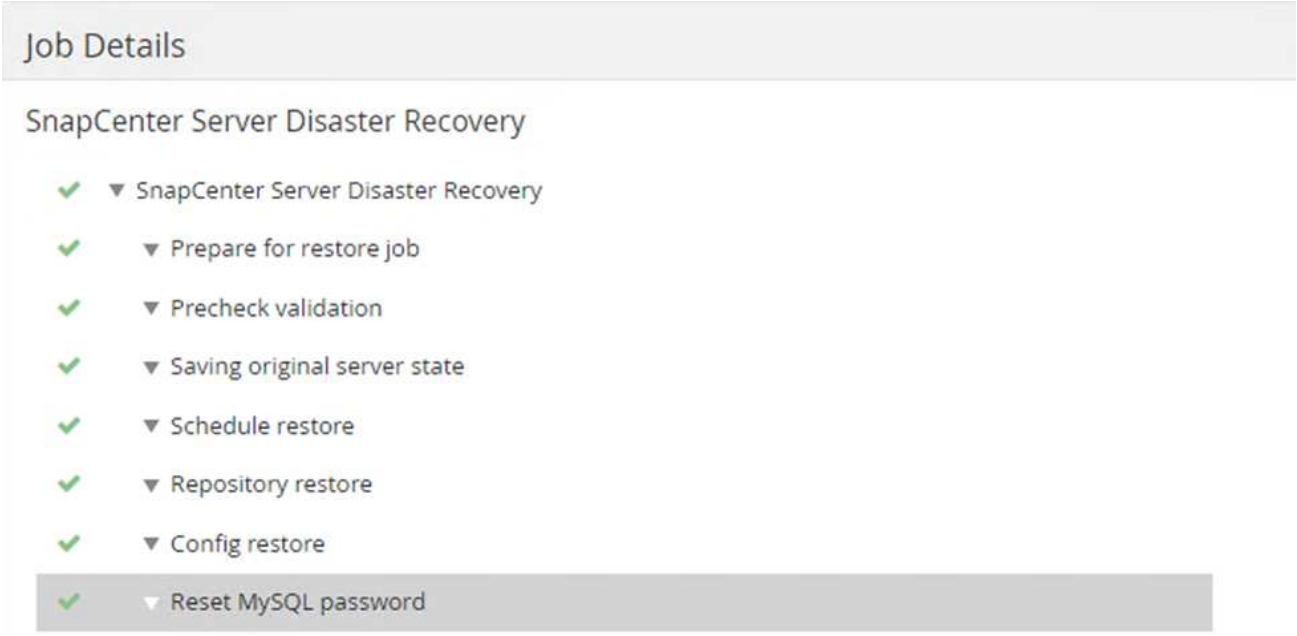


3. Cole seu token de autorização e, na seção SmDRResterRequest, cole o nome do backup e o diretório local no servidor SnapCenter secundário.



4. Selecione o botão Executar para iniciar o processo de restauração.
5. No SnapCenter, navegue até a seção Monitor para visualizar o progresso do trabalho de restauração.





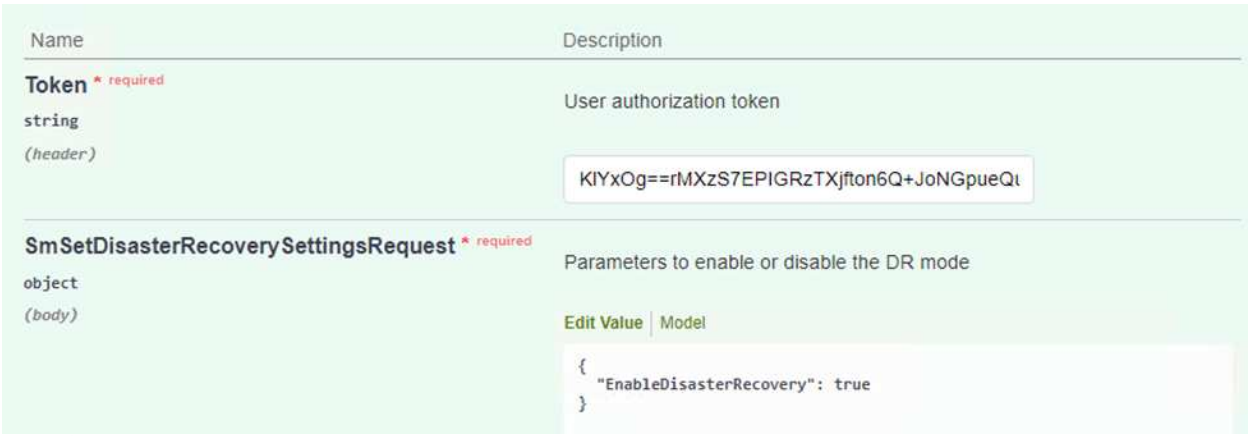
6. Para habilitar restaurações do SQL Server do armazenamento secundário, você deve alternar o banco de dados SnapCenter para o modo de recuperação de desastres. Isso é executado como uma operação separada e iniciada na página da web da API do Swagger.

   a. Navegue até a seção Recuperação de Desastres e clique em `/4.6/disasterrecovery/storage`.

   b. Cole o token de autorização do usuário.

   c. Na seção SmSetDisasterRecoverySettingsRequest, altere `EnableDisasterRecover` para `true`.

   d. Clique em Executar para habilitar o modo de recuperação de desastres para o SQL Server.



Veja comentários sobre procedimentos adicionais.

Restaurar VMs de aplicativos com restauração completa do Veeam

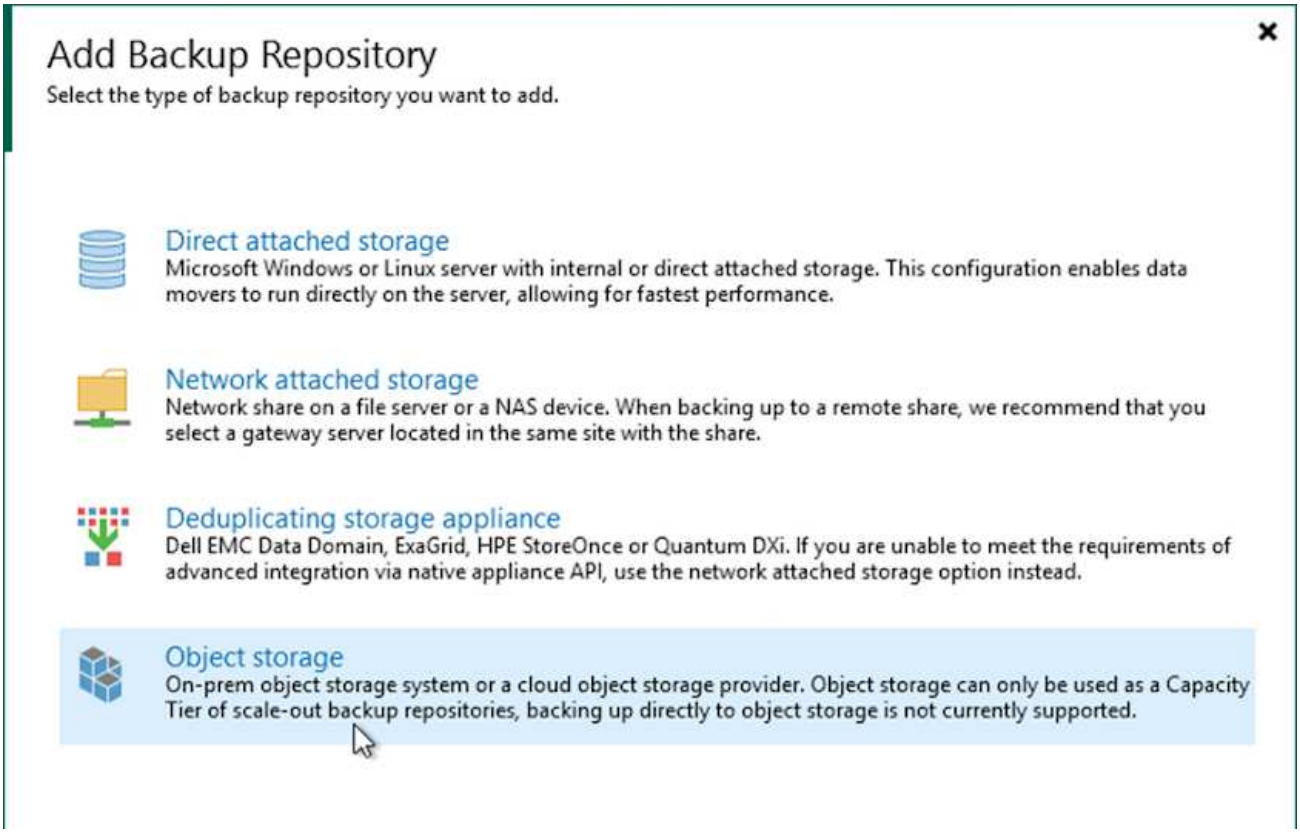
▼ Crie um repositório de backup e importe backups do S3

Do servidor Veeam secundário, importe os backups do armazenamento S3 e restaure as VMs do SQL Server e do Oracle para seu cluster do VMware Cloud.

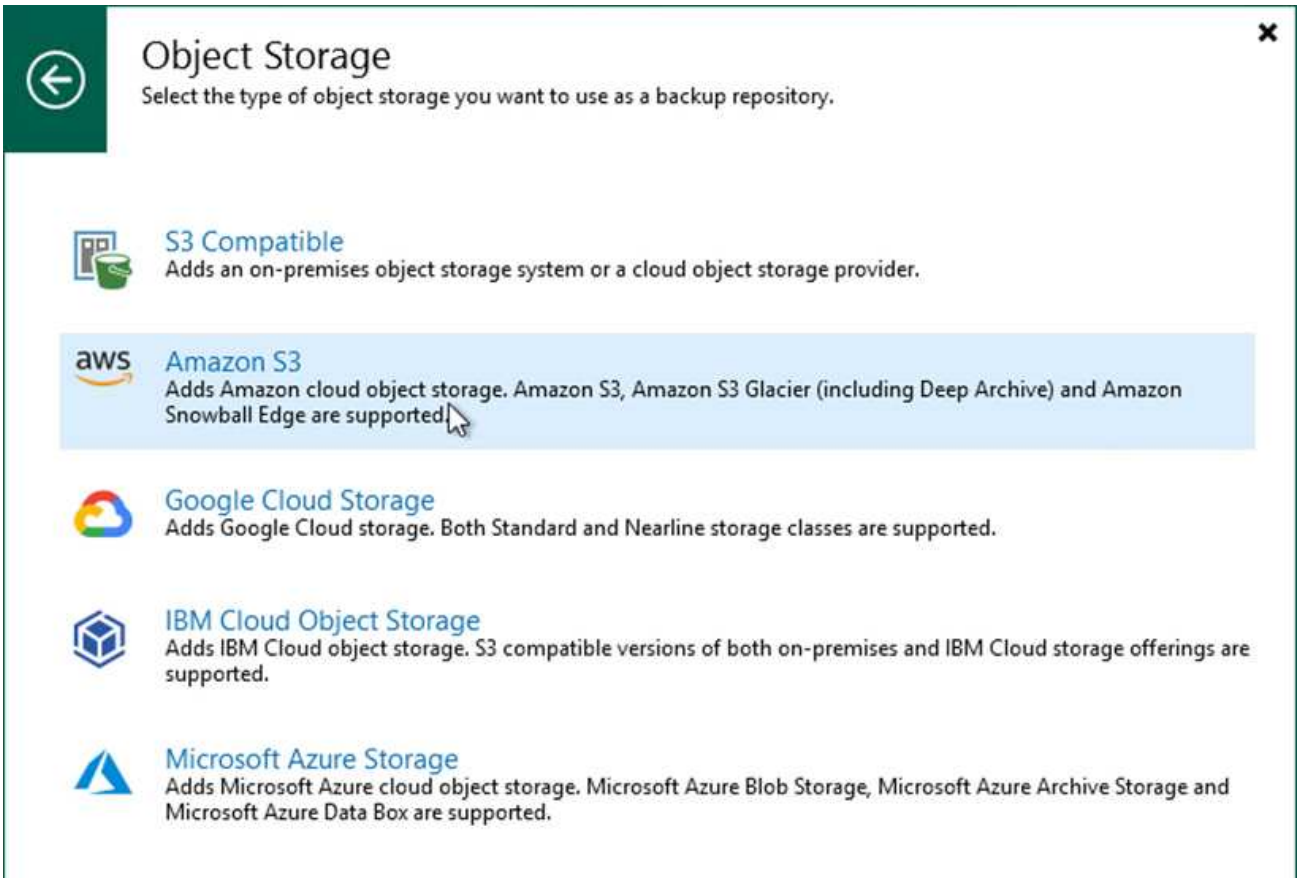
Para importar os backups do objeto S3 que fazia parte do repositório de backup de expansão local, conclua

as seguintes etapas:

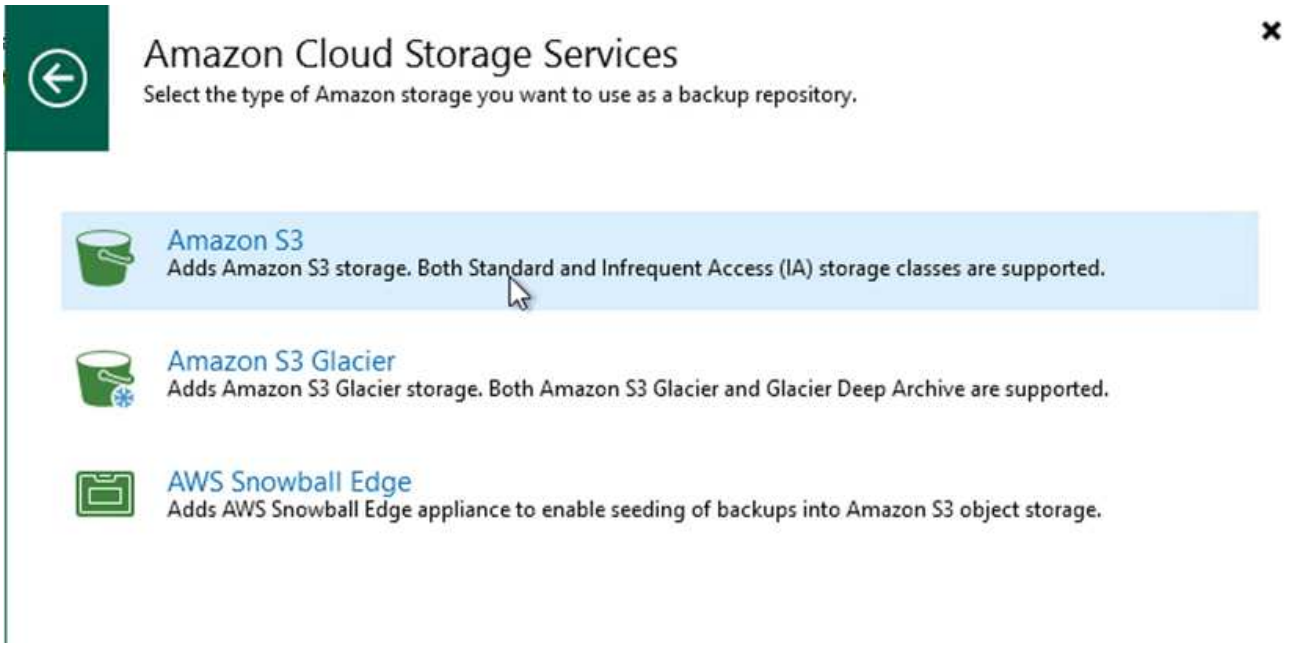
1. Vá para Repositórios de backup e clique em Adicionar repositório no menu superior para iniciar o assistente Adicionar repositório de backup. Na primeira página do assistente, selecione Armazenamento de Objetos como o tipo de repositório de backup.



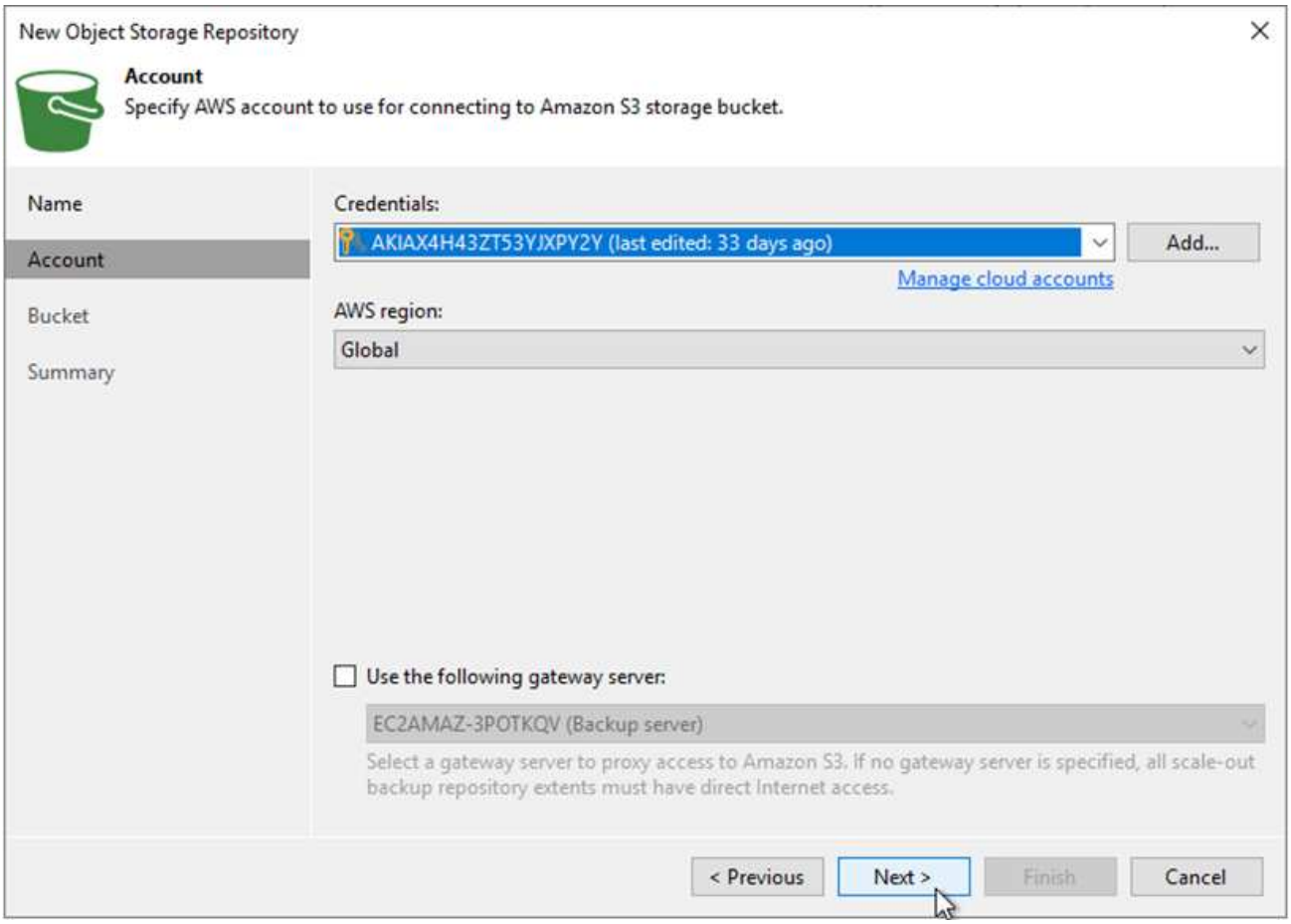
2. Selecione Amazon S3 como o tipo de armazenamento de objetos.



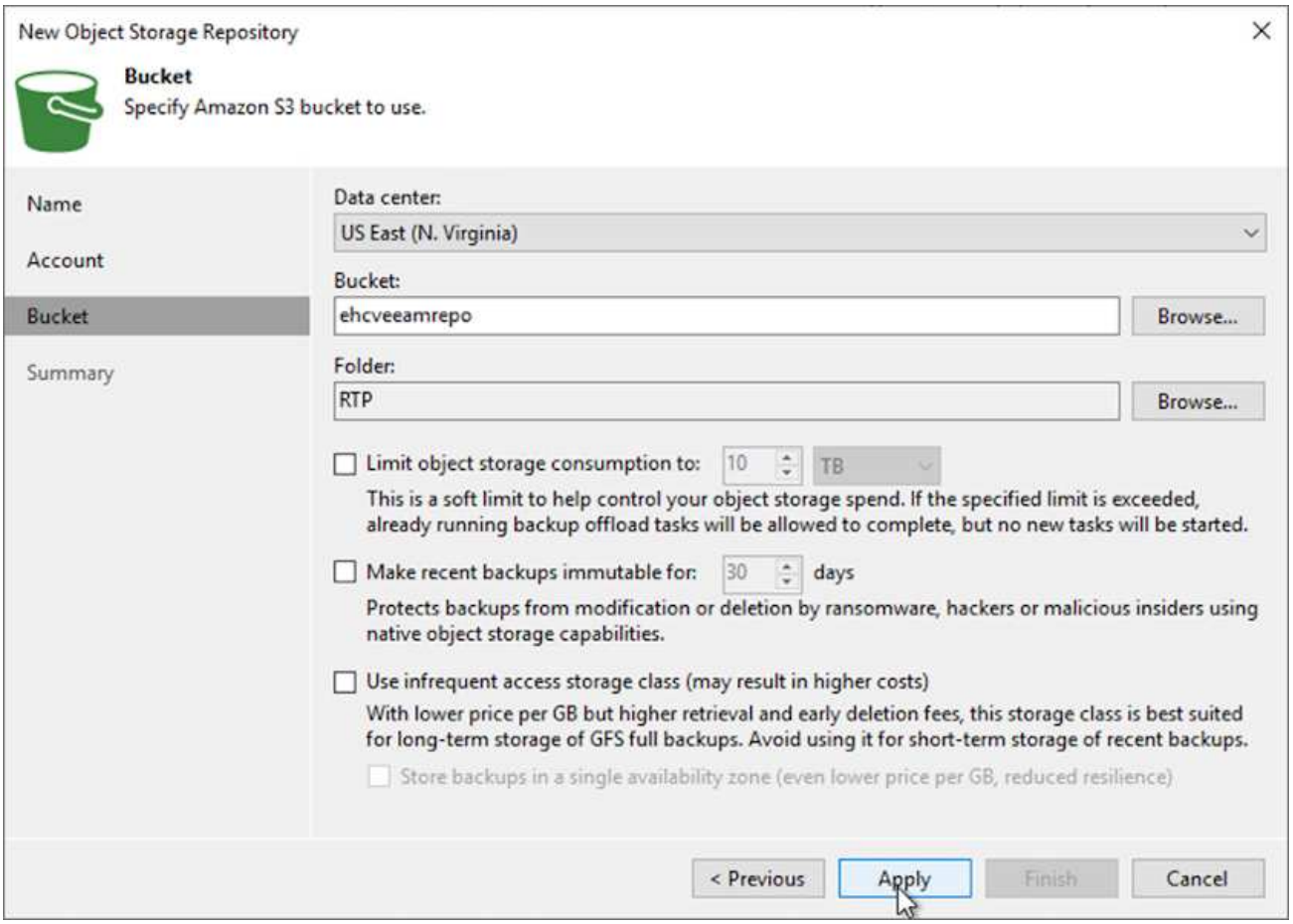
3. Na lista de serviços de armazenamento em nuvem da Amazon, selecione Amazon S3.



4. Selecione suas credenciais pré-inseridas na lista suspensa ou adicione uma nova credencial para acessar o recurso de armazenamento em nuvem. Clique em Avançar para continuar.



5. Na página Bucket, insira o data center, o bucket, a pasta e quaisquer opções desejadas. Clique em Aplicar.

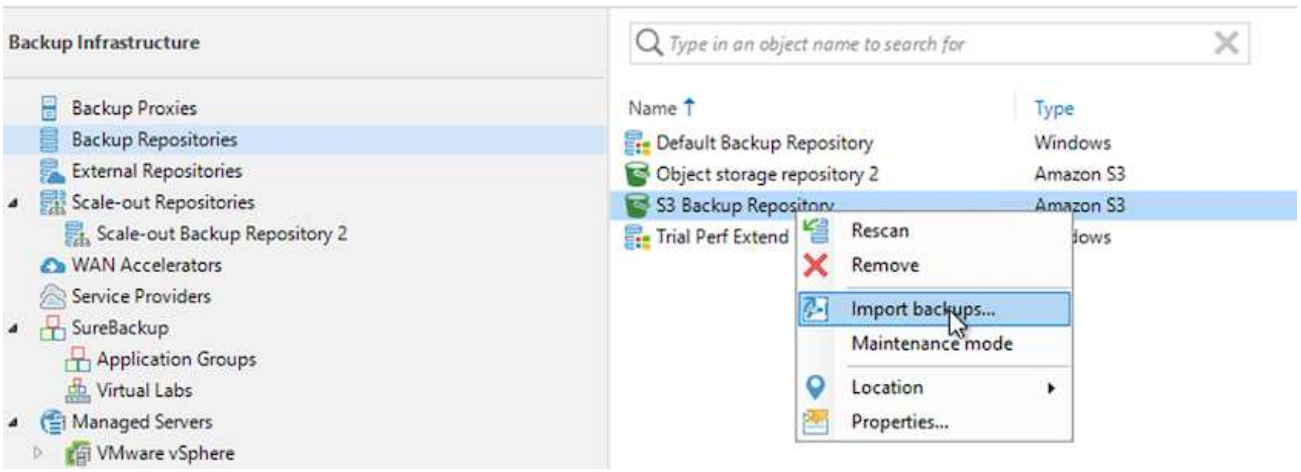


6. Por fim, selecione Concluir para finalizar o processo e adicionar o repositório.

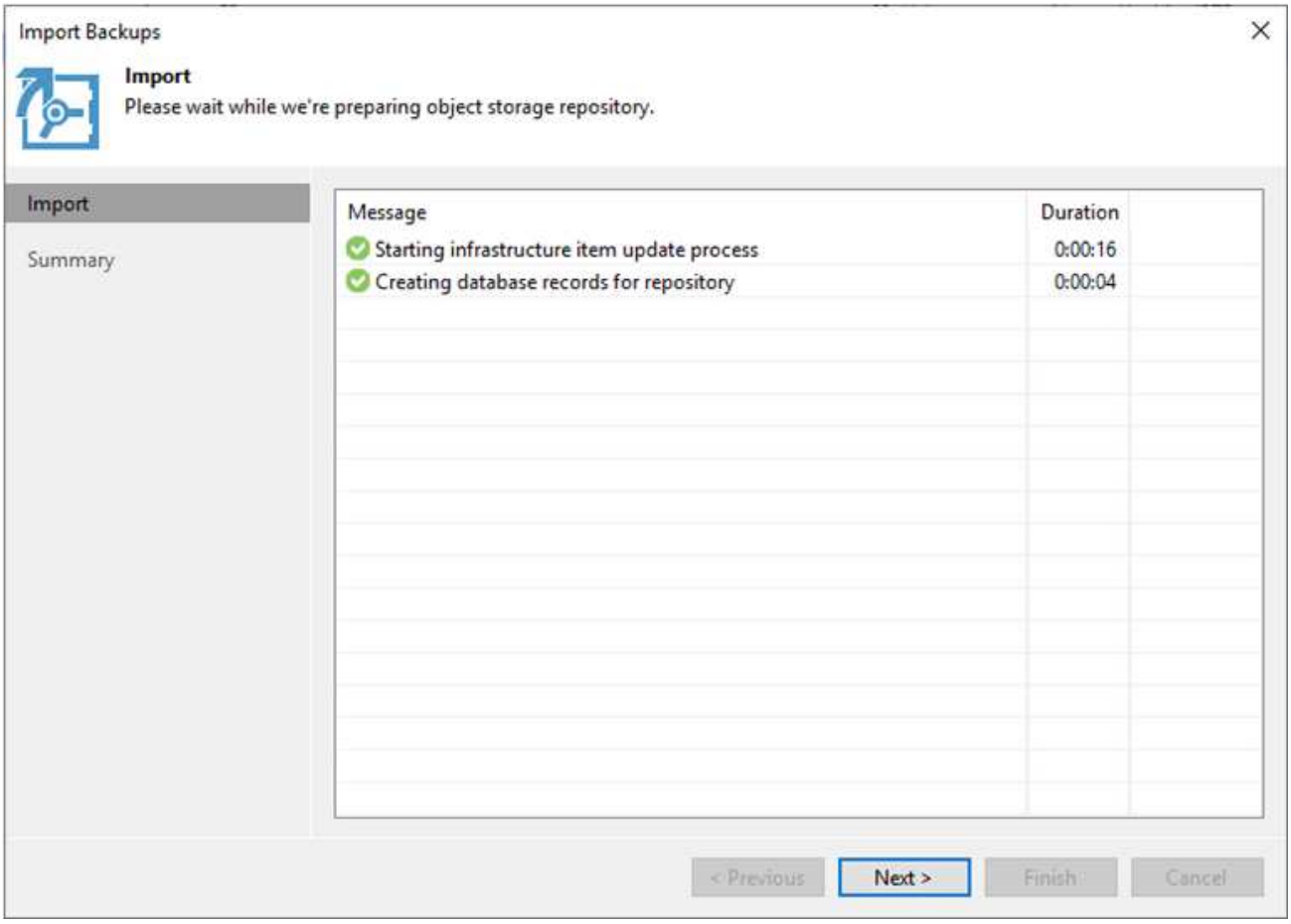
▼ **Importar backups do armazenamento de objetos S3**

Para importar os backups do repositório S3 adicionado na seção anterior, conclua as seguintes etapas.

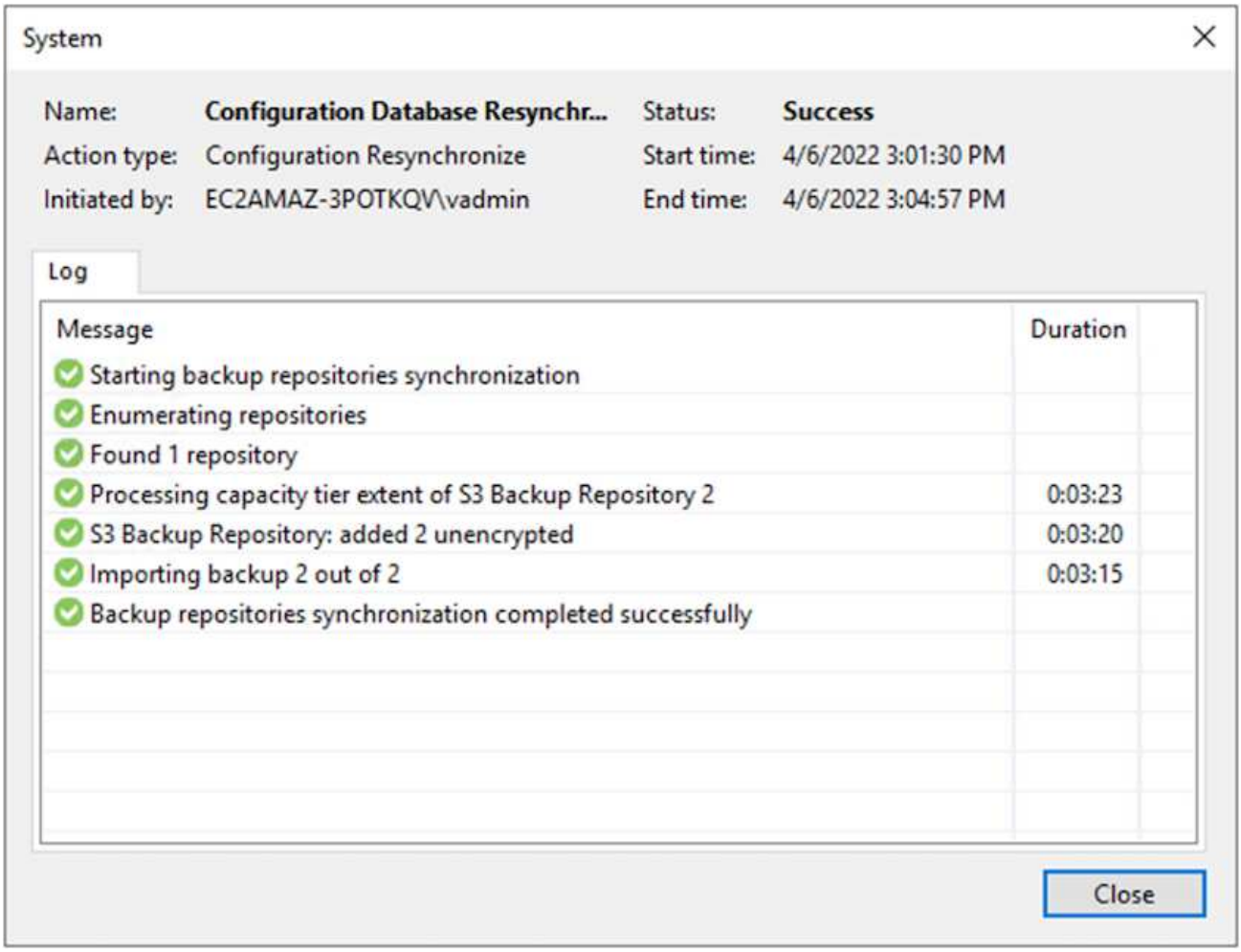
1. No repositório de backup do S3, selecione Importar backups para iniciar o assistente Importar backups.



2. Depois que os registros do banco de dados para importação forem criados, selecione Avançar e depois Concluir na tela de resumo para iniciar o processo de importação.



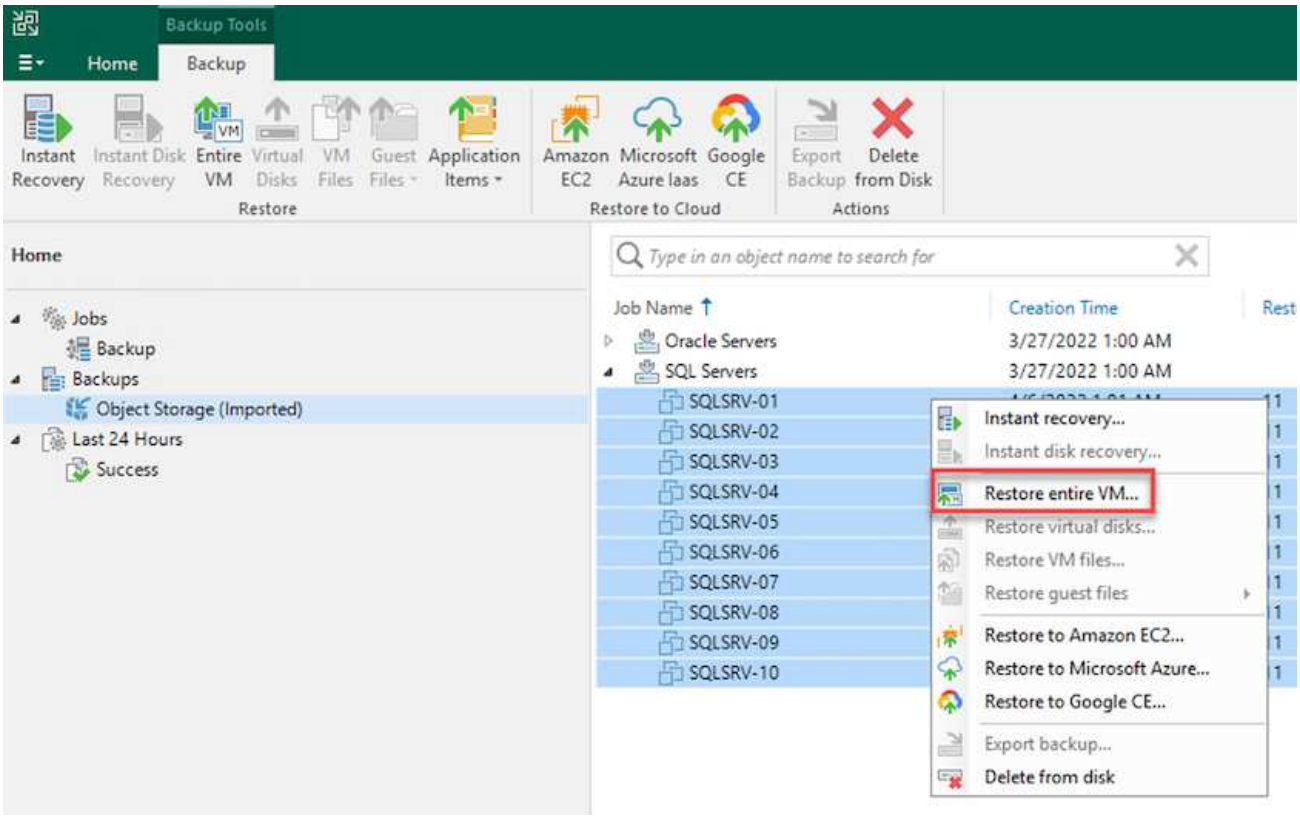
3. Após a conclusão da importação, você poderá restaurar as VMs no cluster do VMware Cloud.



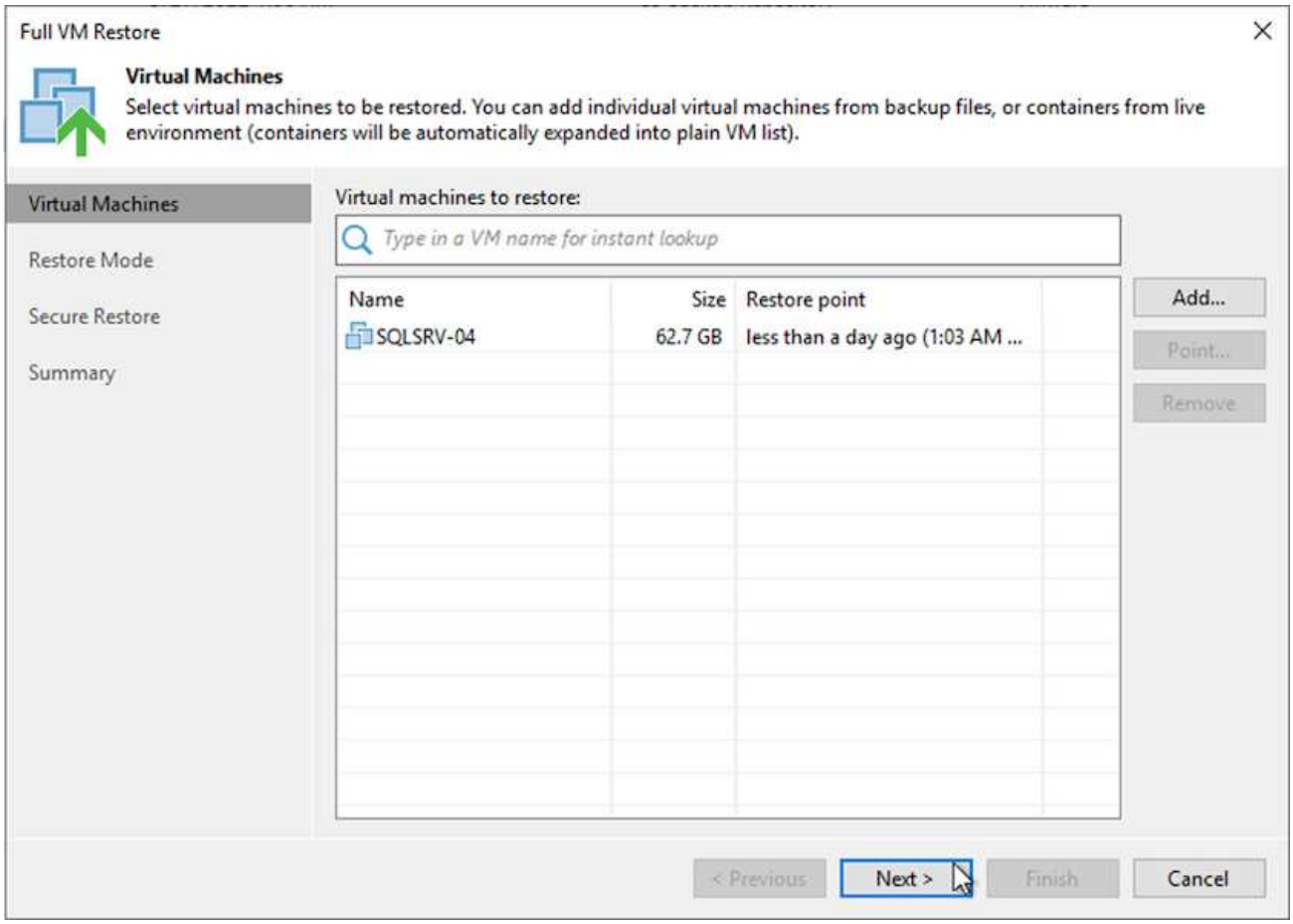
▼ **Restaurar VMs de aplicativos com restauração completa da Veeam para VMware Cloud**

Para restaurar máquinas virtuais SQL e Oracle para o domínio/cluster de carga de trabalho do VMware Cloud on AWS, conclua as seguintes etapas.

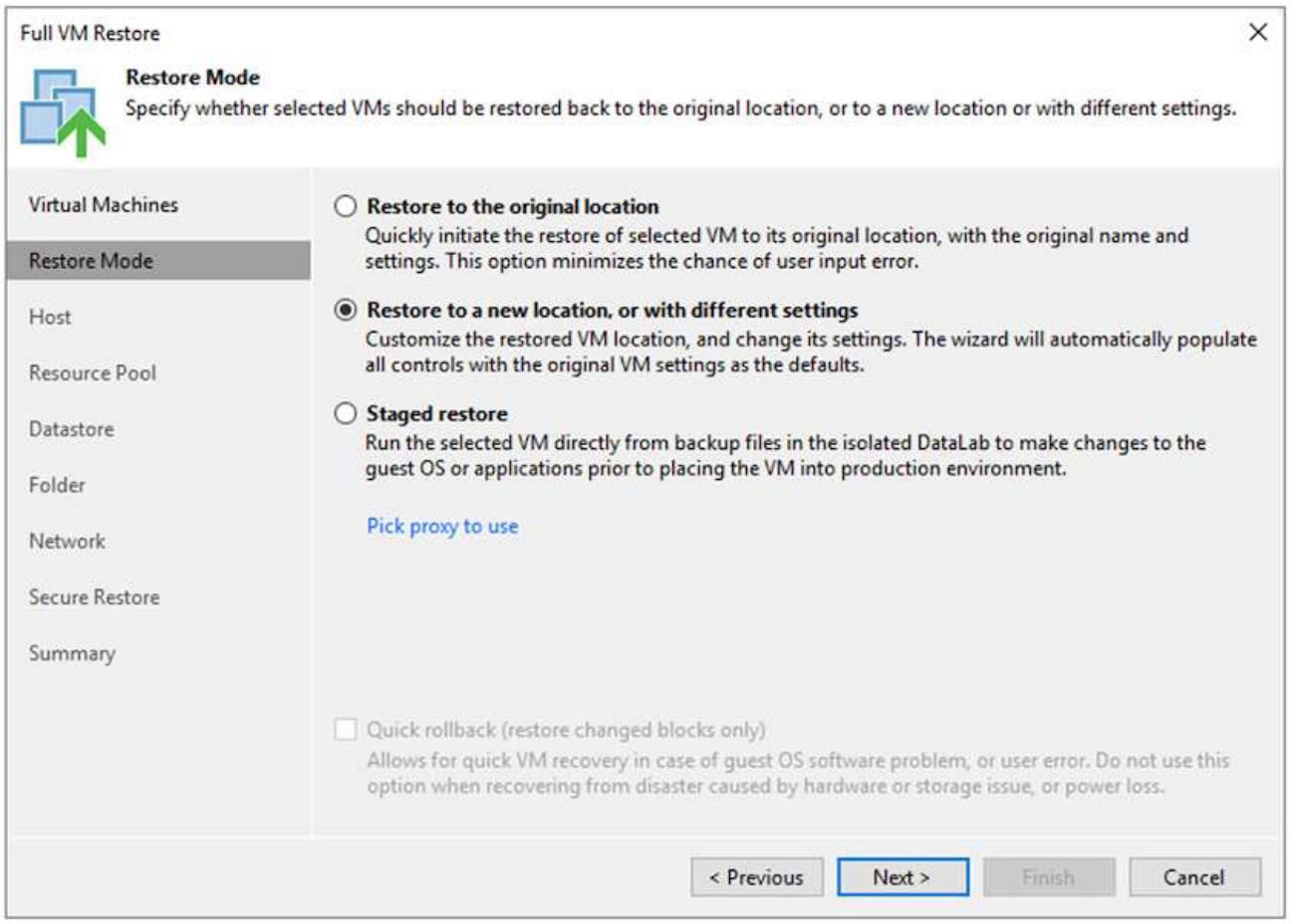
1. Na página inicial do Veeam, selecione o armazenamento de objetos que contém os backups importados, selecione as VMs a serem restauradas e, em seguida, clique com o botão direito e selecione Restaurar VM inteira.



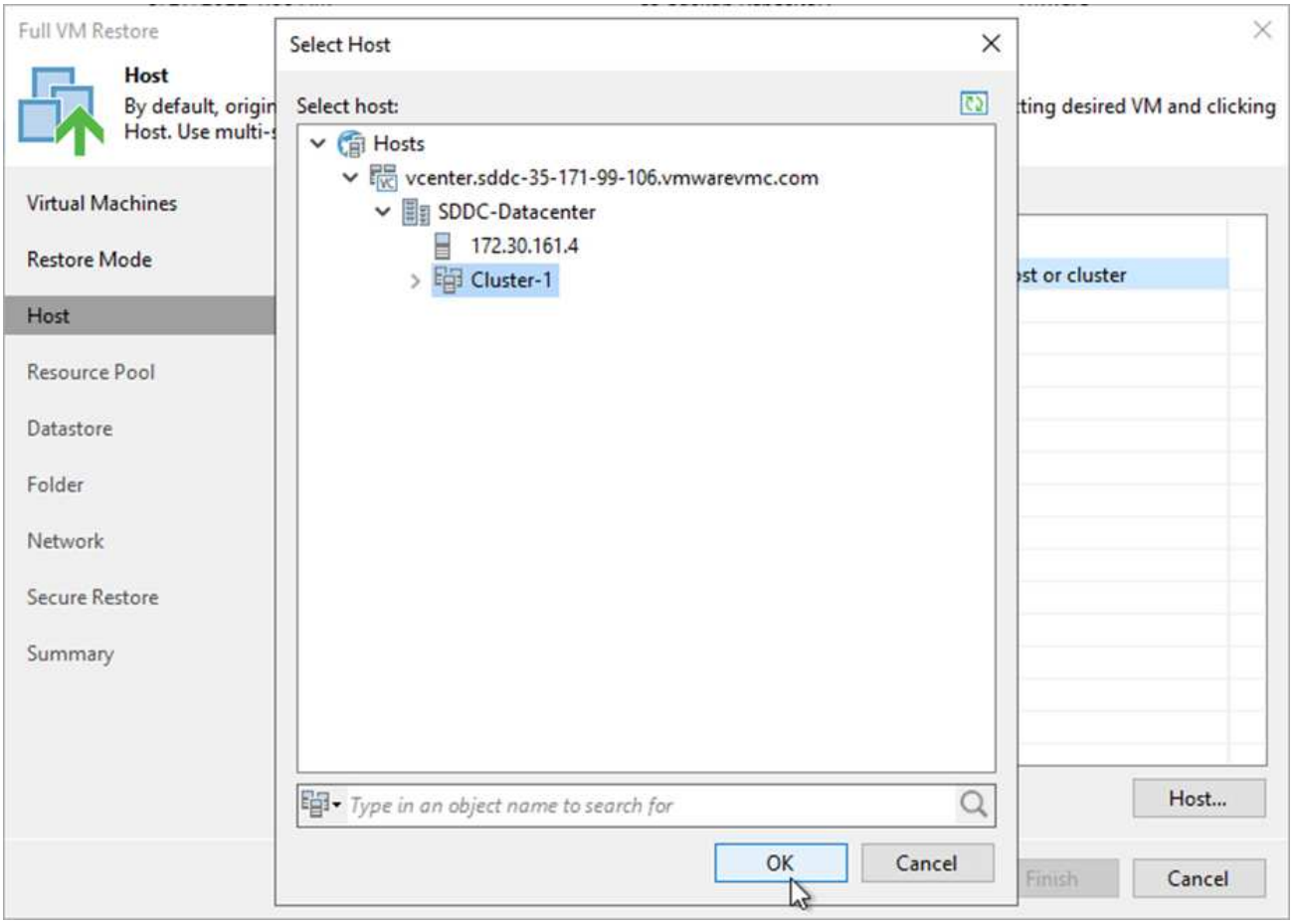
2. Na primeira página do assistente de Restauração completa de VM, modifique as VMs para backup, se desejar, e selecione Avançar.



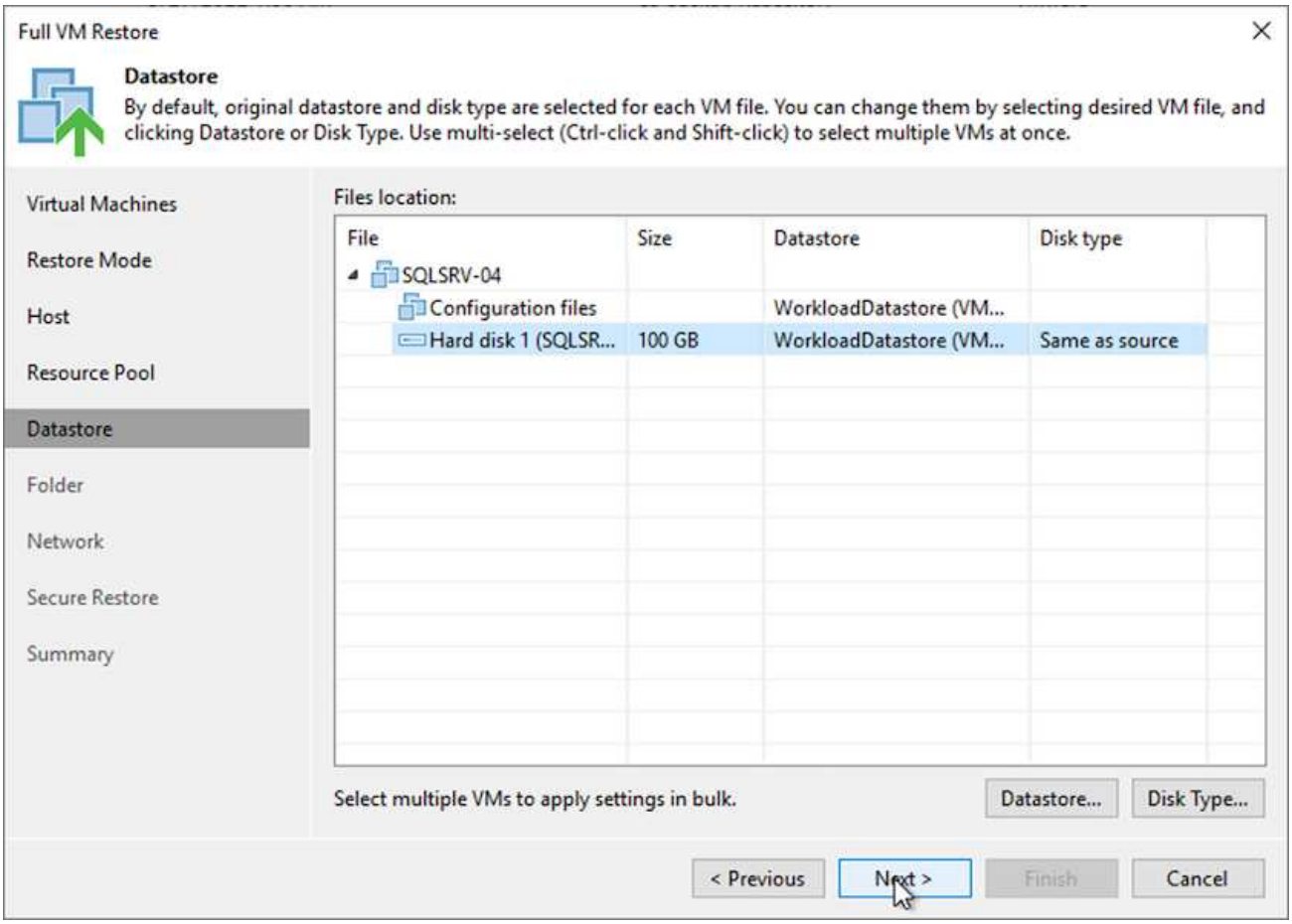
3. Na página Modo de restauração, selecione Restaurar para um novo local ou com configurações diferentes.



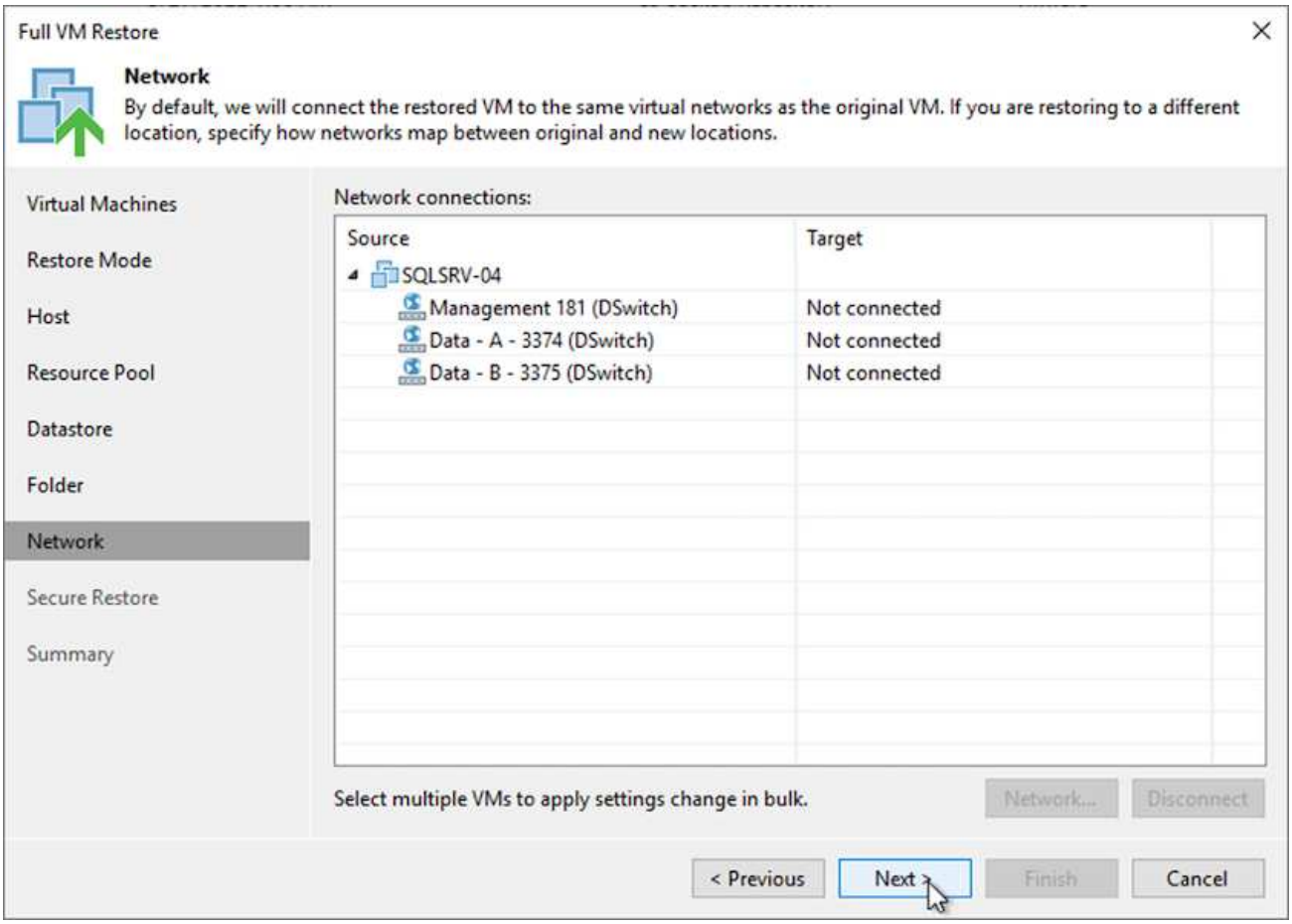
4. Na página do host, selecione o host ou cluster ESXi de destino para restaurar a VM.

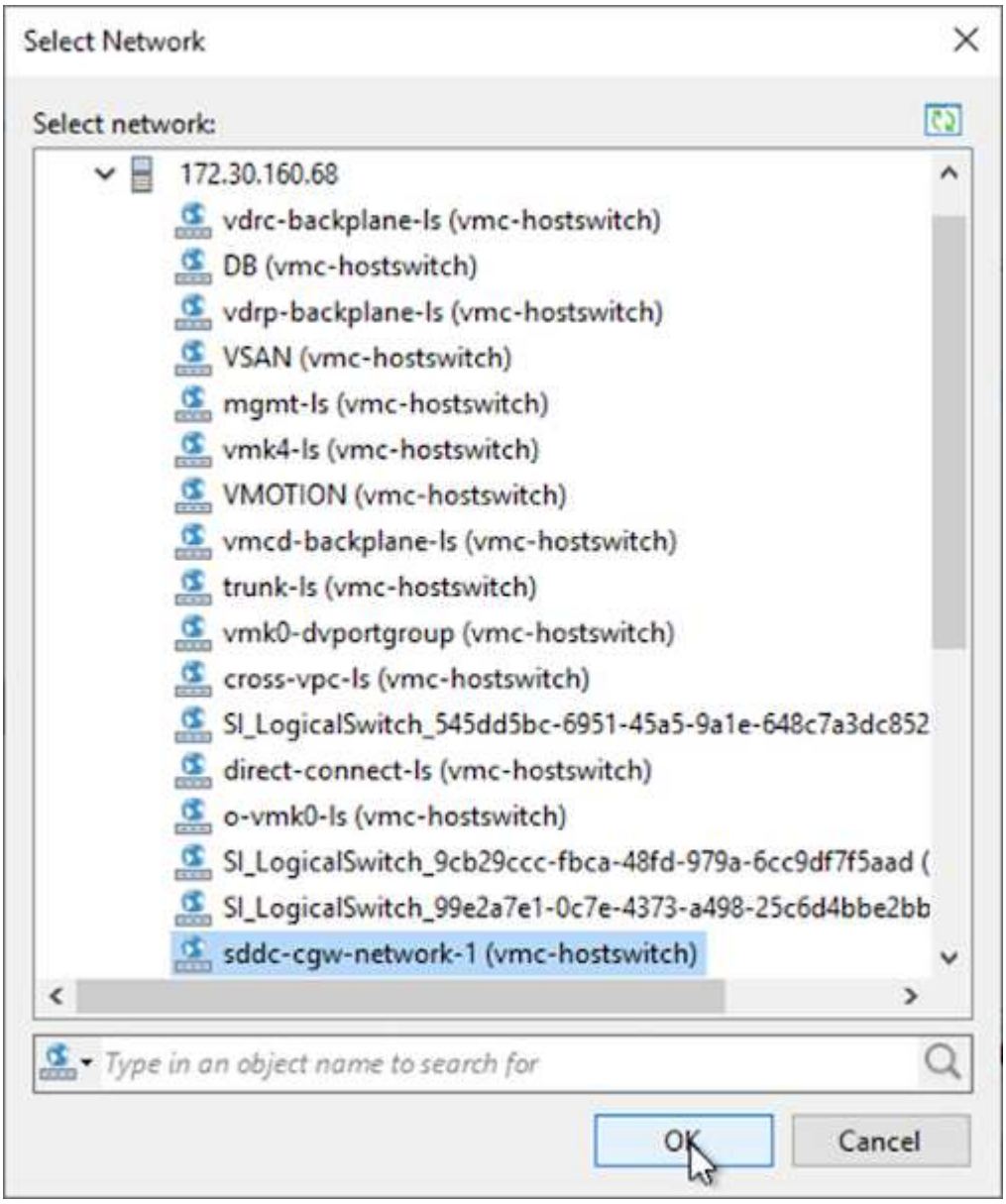


5. Na página Datastores, selecione o local do datastore de destino para os arquivos de configuração e o disco rígido.



6. Na página Rede, mapeie as redes originais na VM para as redes no novo local de destino.


Full VM Restore
Network
By default, we will connect the restored VM to the same virtual networks as the original VM. If you are restoring to a different location, specify how networks map between original and new locations.
Virtual Machines
Restore Mode
Host
Resource Pool
Datastore
Folder
Network
Secure Restore
Summary
Network connections:
Source
Target
SQLSRV-04
Management 181 (DSwitch)
Not connected
Data - A - 3374 (DSwitch)
Not connected
Data - B - 3375 (DSwitch)
Not connected
Select multiple VMs to apply settings change in bulk.
Network...
Disconnect
< Previous
Next >
Finish
Cancel



7. Selecione se deseja verificar se há malware na VM restaurada, revise a página de resumo e clique em Concluir para iniciar a restauração.

Restaurar dados do aplicativo SQL Server

O processo a seguir fornece instruções sobre como recuperar um SQL Server no VMware Cloud Services na AWS no caso de um desastre que torne o site local inoperante.

Os seguintes pré-requisitos devem ser atendidos para continuar com as etapas de recuperação:

1. A VM do Windows Server foi restaurada para o VMware Cloud SDDC usando o Veeam Full Restore.
2. Um servidor SnapCenter secundário foi estabelecido e a restauração e configuração do banco de dados SnapCenter foram concluídas usando as etapas descritas na seção"Resumo do processo de backup e restauração do SnapCenter ."

▼ **VM: Configuração pós-restauração para VM do SQL Server**

Após a conclusão da restauração da VM, você deve configurar a rede e outros itens em preparação para redescobrir a VM host no SnapCenter.

1. Atribua novos endereços IP para Gerenciamento e iSCSI ou NFS.
2. Ingresse o host no domínio do Windows.
3. Adicione os nomes de host ao DNS ou ao arquivo de hosts no servidor SnapCenter .

Se o plug-in SnapCenter foi implantado usando credenciais de domínio diferentes do domínio atual, você deve alterar a conta de logon do serviço Plug-in para Windows na VM do SQL Server. Após alterar a conta de logon, reinicie os serviços SnapCenter SMCore, Plug-in para Windows e Plug-in para SQL Server.

Para redescobrir automaticamente as VMs restauradas no SnapCenter, o FQDN deve ser idêntico à VM que foi adicionada originalmente ao SnapCenter local.

▼ Configurar o armazenamento FSx para restauração do SQL Server

Para realizar o processo de restauração de recuperação de desastres para uma VM do SQL Server, você deve interromper o relacionamento SnapMirror existente do cluster FSx e conceder acesso ao volume. Para fazer isso, siga os seguintes passos.

1. Para interromper o relacionamento SnapMirror existente para os volumes de log e banco de dados do SQL Server, execute o seguinte comando na CLI do FSx:

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

2. Conceda acesso ao LUN criando um grupo de iniciadores contendo o IQN iSCSI da VM Windows do SQL Server:

```
FSx-Dest::> igroup create -vserver DestSVM -igroup igroupName
-protocol iSCSI -ostype windows -initiator IQN
```

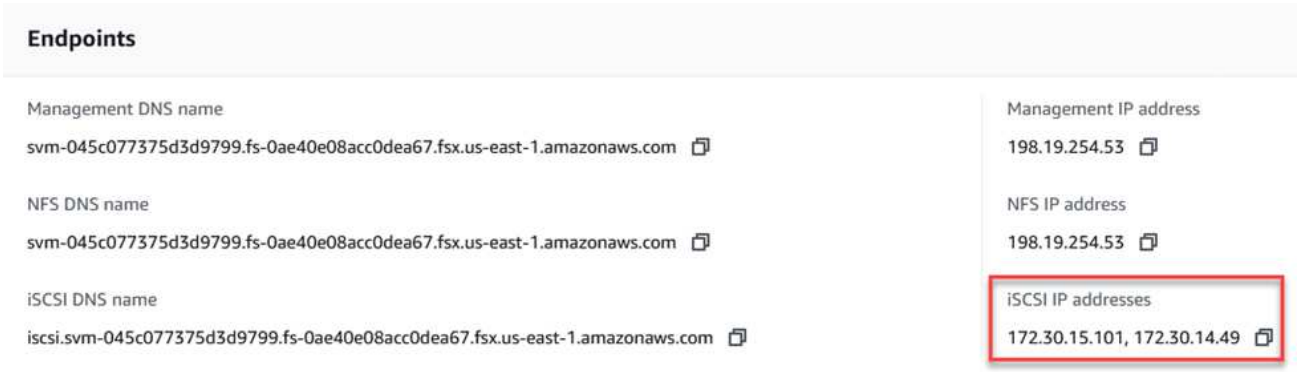
3. Por fim, mapeie os LUNs para o grupo iniciador que você acabou de criar:

```
FSx-Dest::> lun mapping create -vserver DestSVM -path LUNPath igroup
igroupName
```

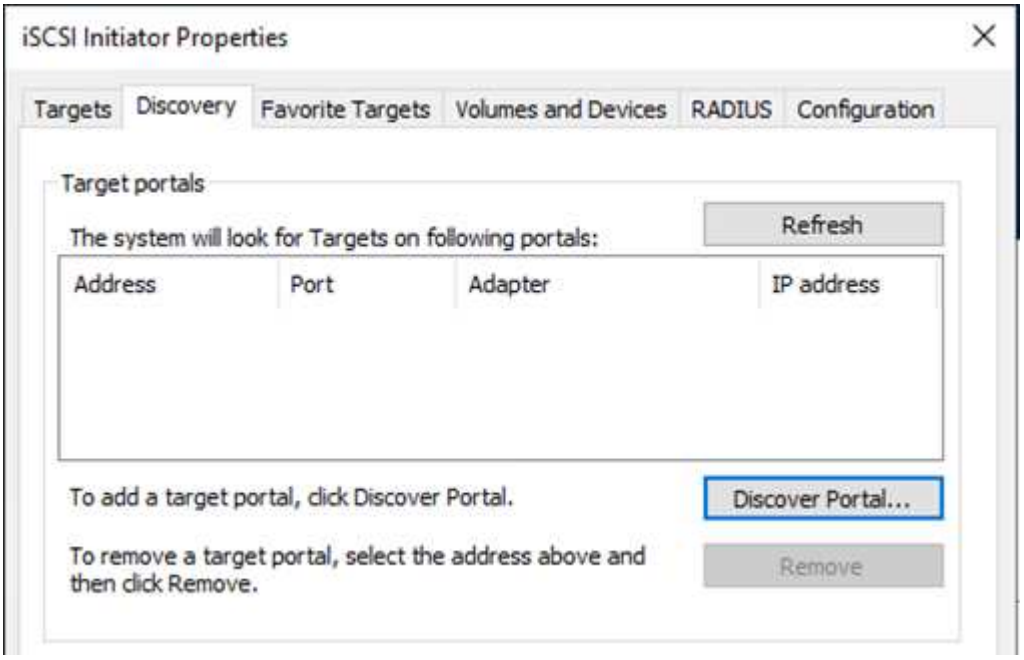
4. Para encontrar o nome do caminho, execute o `lun show` comando.

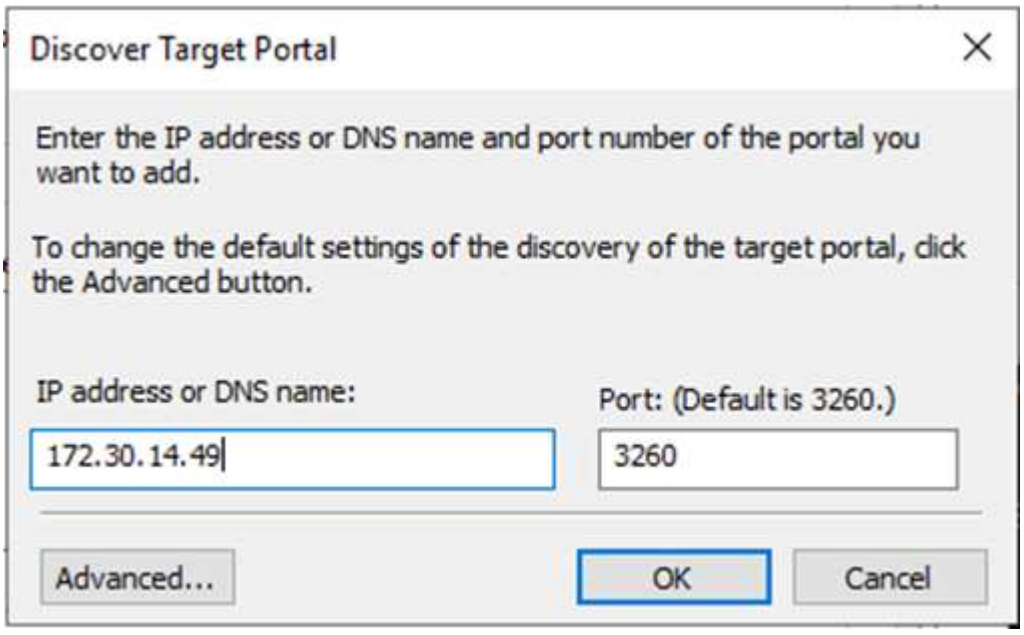
▼ Configurar a VM do Windows para acesso iSCSI e descobrir os sistemas de arquivos

1. Na VM do SQL Server, configure seu adaptador de rede iSCSI para se comunicar no grupo de portas VMware que foi estabelecido com conectividade com as interfaces de destino iSCSI na sua instância FSx.
2. Abra o utilitário Propriedades do Iniciador iSCSI e limpe as configurações de conectividade antigas nas guias Descoberta, Destinos Favoritos e Destinos.
3. Localize o(s) endereço(s) IP para acessar a interface lógica iSCSI na instância/cluster do FSx. Isso pode ser encontrado no console da AWS em Amazon FSx > ONTAP > Máquinas virtuais de armazenamento.



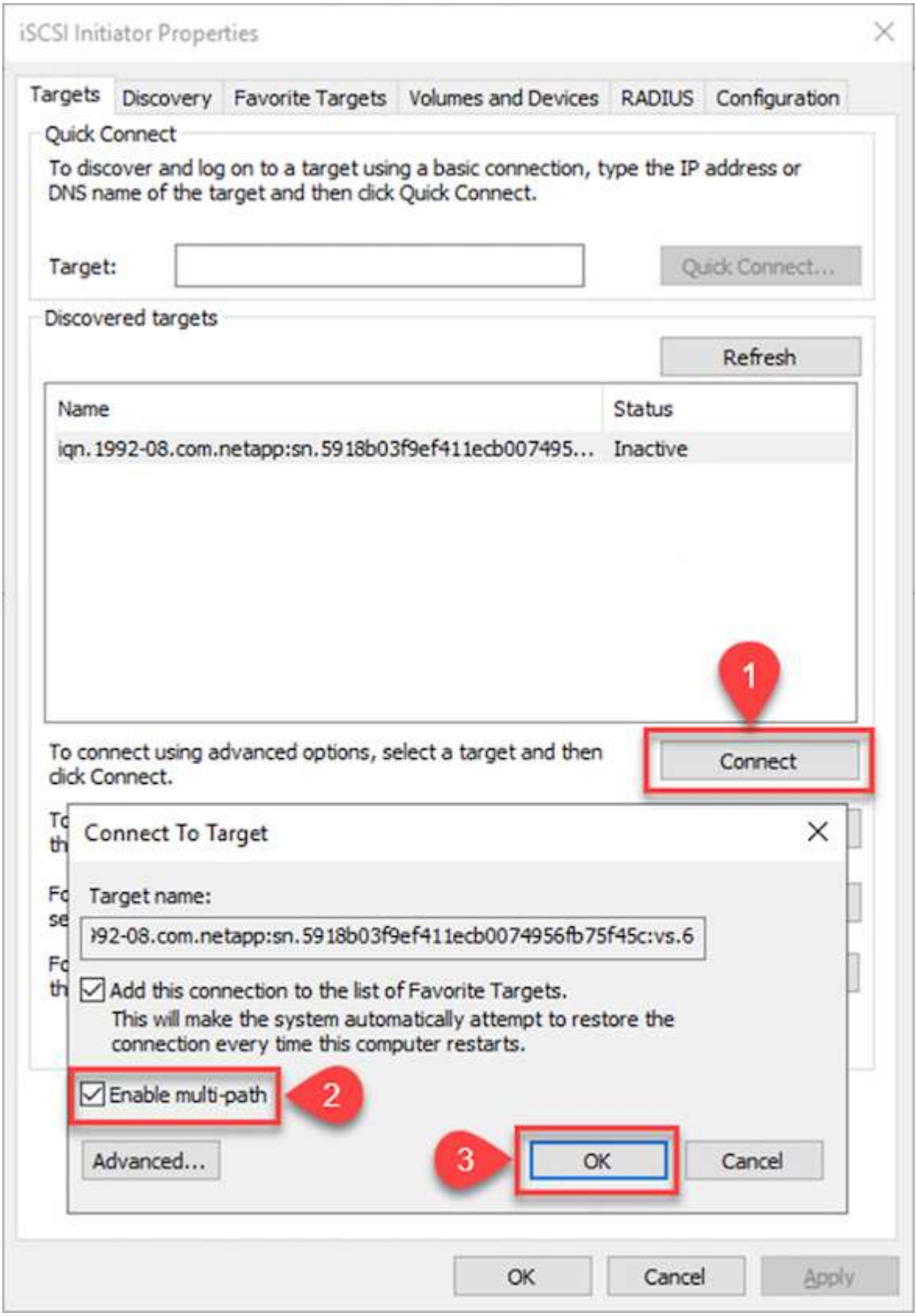
4. Na guia Descoberta, clique em Descobrir Portal e insira os endereços IP para seus destinos FSx iSCSI.



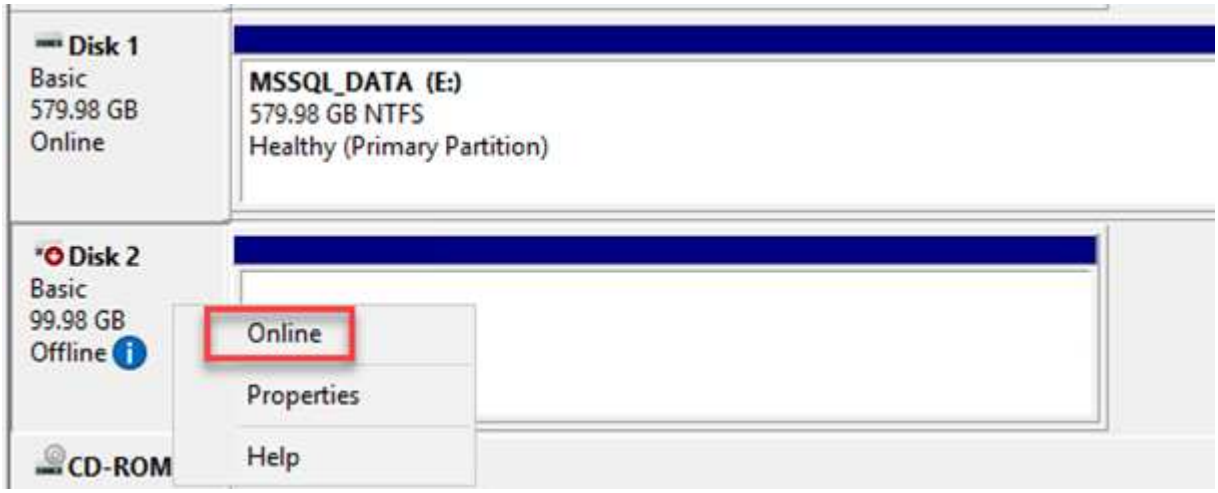


5. Na guia Destino, clique em Conectar, selecione Habilitar vários caminhos, se apropriado para sua

configuração, e clique em OK para se conectar ao destino.

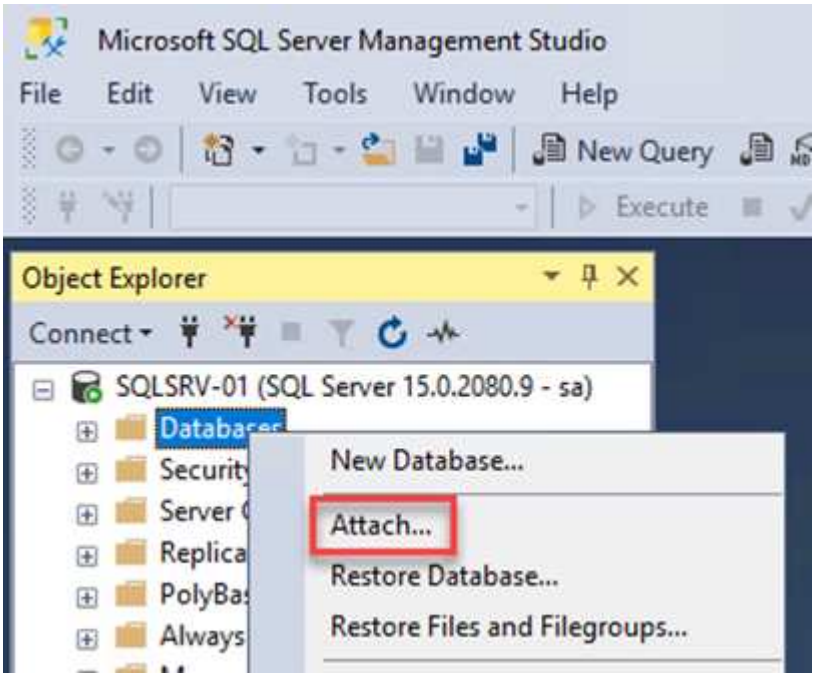


6. Abra o utilitário Gerenciamento do Computador e coloque os discos on-line. Verifique se eles mantêm as mesmas letras de unidade que tinham anteriormente.

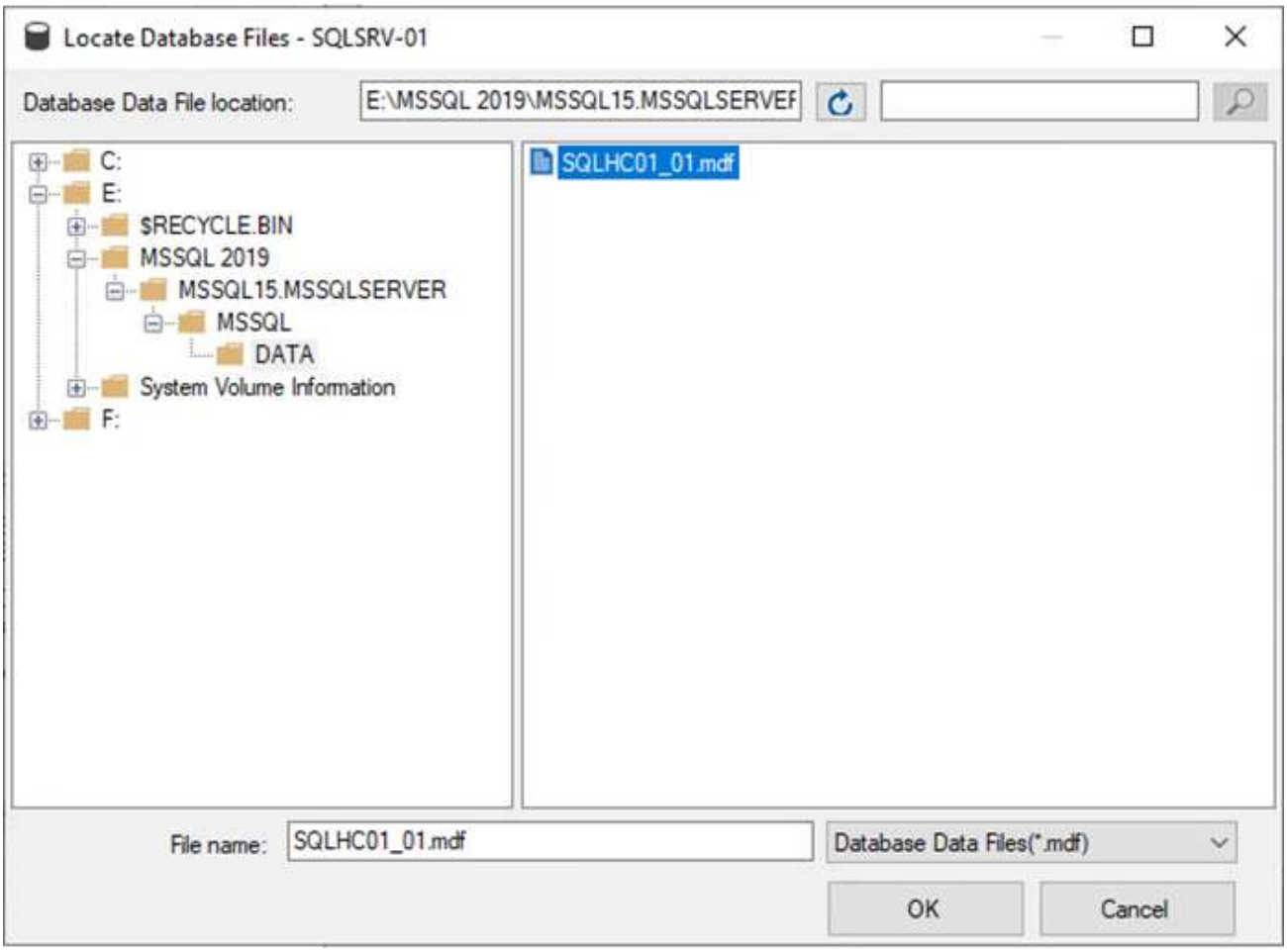


▼ **Anexar os bancos de dados do SQL Server**

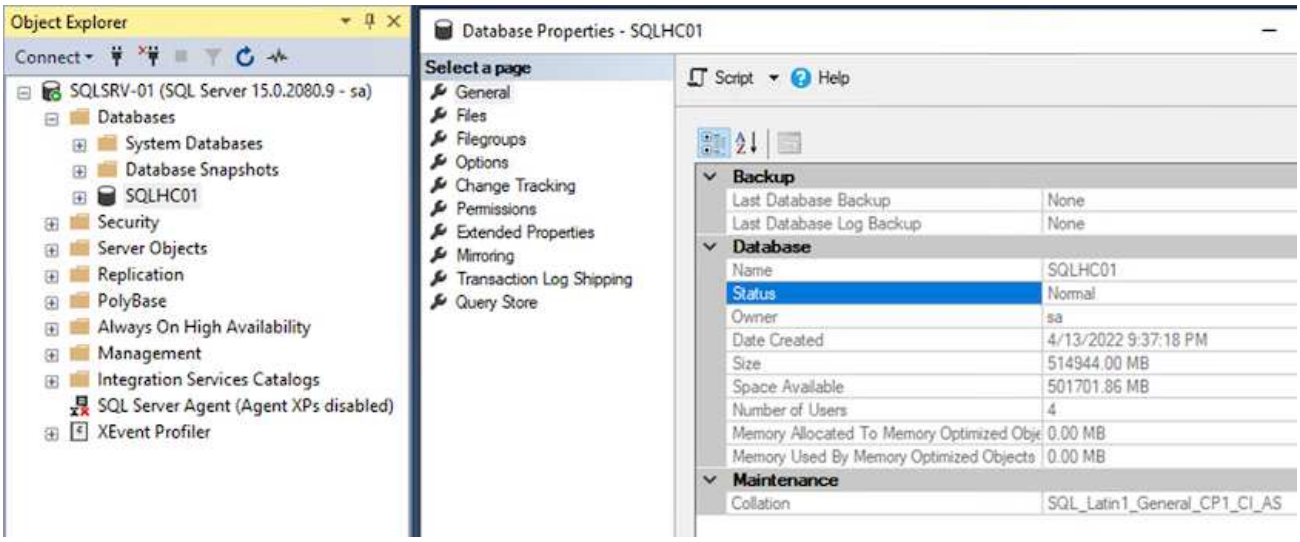
1. Na VM do SQL Server, abra o Microsoft SQL Server Management Studio e selecione Anexar para iniciar o processo de conexão ao banco de dados.



2. Clique em Adicionar e navegue até a pasta que contém o arquivo de banco de dados principal do SQL Server, selecione-o e clique em OK.



3. Se os logs de transações estiverem em uma unidade separada, escolha a pasta que contém o log de transações.
4. Quando terminar, clique em OK para anexar o banco de dados.

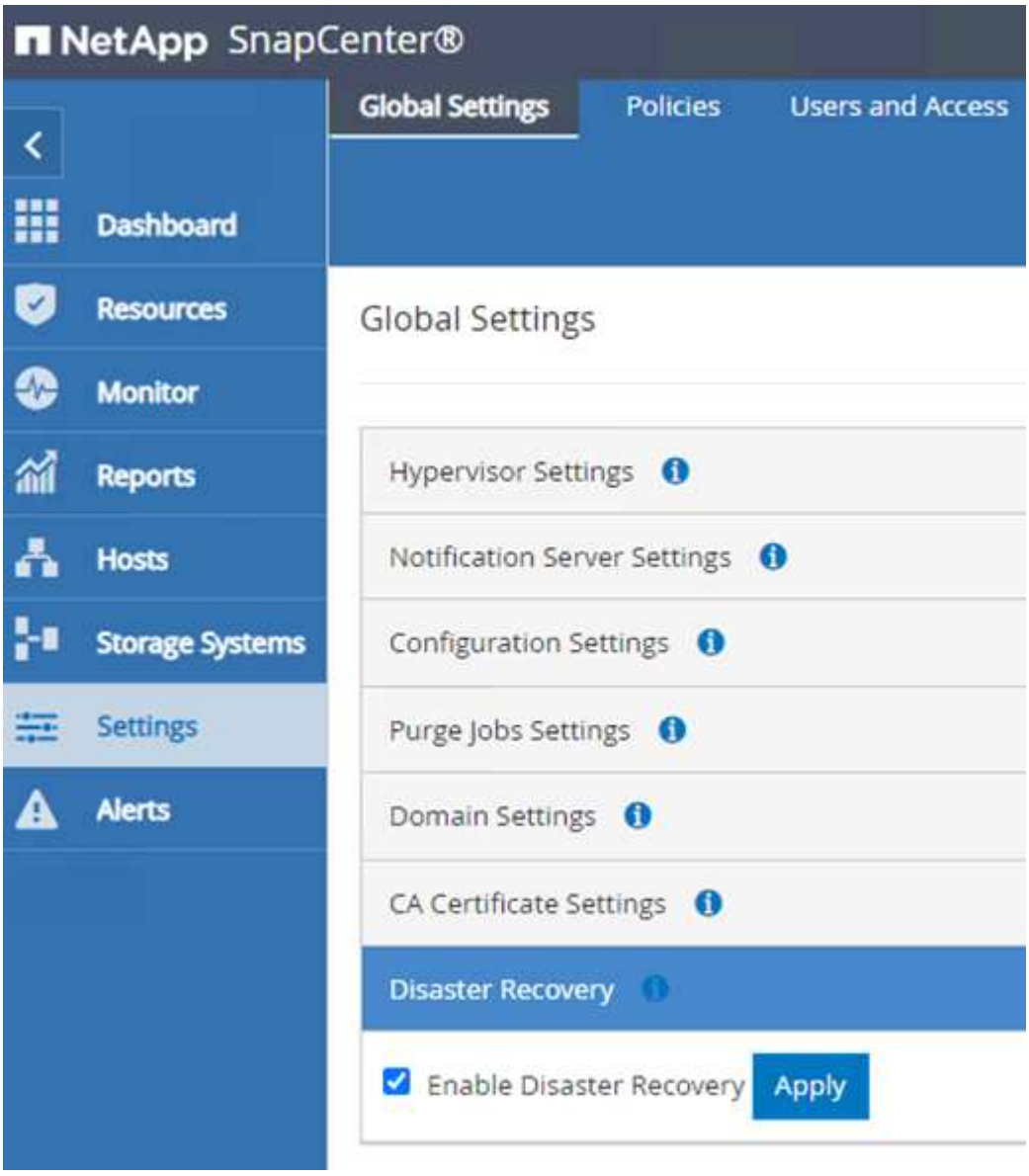


▼ **Confirme a comunicação do SnapCenter com o plug-in do SQL Server**

Com o banco de dados SnapCenter restaurado ao seu estado anterior, ele redescobre automaticamente os hosts do SQL Server. Para que isso funcione corretamente, tenha em mente os seguintes pré-requisitos:

- O SnapCenter deve ser colocado no modo de recuperação de desastres. Isso pode ser feito por meio da API do Swagger ou nas Configurações globais em Recuperação de desastres.
- O FQDN do SQL Server deve ser idêntico à instância que estava em execução no datacenter local.
- O relacionamento original do SnapMirror deve ser quebrado.
- Os LUNs que contêm o banco de dados devem ser montados na instância do SQL Server e o banco de dados deve ser anexado.

Para confirmar se o SnapCenter está no modo de recuperação de desastres, navegue até Configurações no cliente web do SnapCenter . Vá para a aba Configurações globais e clique em Recuperação de desastres. Certifique-se de que a caixa de seleção Habilitar recuperação de desastres esteja marcada.



Restaurar dados do aplicativo Oracle

O processo a seguir fornece instruções sobre como recuperar dados do aplicativo Oracle no VMware Cloud Services na AWS no caso de um desastre que torne o site local inoperante.

Conclua os seguintes pré-requisitos para continuar com as etapas de recuperação:

1. A VM do servidor Oracle Linux foi restaurada para o VMware Cloud SDDC usando o Veeam Full Restore.
2. Um servidor SnapCenter secundário foi estabelecido e o banco de dados SnapCenter e os arquivos de configuração foram restaurados usando as etapas descritas nesta seção"Resumo do processo de backup e restauração do SnapCenter ."

▼ **Configurar o FSx para restauração do Oracle – Interromper o relacionamento do SnapMirror**

Para tornar os volumes de armazenamento secundário hospedados na instância do FSx ONTAP acessíveis aos servidores Oracle, você deve primeiro quebrar o relacionamento SnapMirror existente.

1. Após efetuar login no FSx CLI, execute o seguinte comando para visualizar os volumes filtrados pelo nome correto.

```
FSx-Dest::> volume show -volume VolumeName*
```

```
FsxId0ae40e08acc0dea67::> volume show -volume oraclesrv_03*
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
ora_svm_dest
          oraclesrv_03_u01_dest
                       aggr1        online     DP        100GB    93.12GB    6%
ora_svm_dest
          oraclesrv_03_u02_dest
                       aggr1        online     DP        200GB    34.98GB   82%
ora_svm_dest
          oraclesrv_03_u03_dest
                       aggr1        online     DP        150GB    33.37GB   77%
3 entries were displayed.

FsxId0ae40e08acc0dea67::>
```

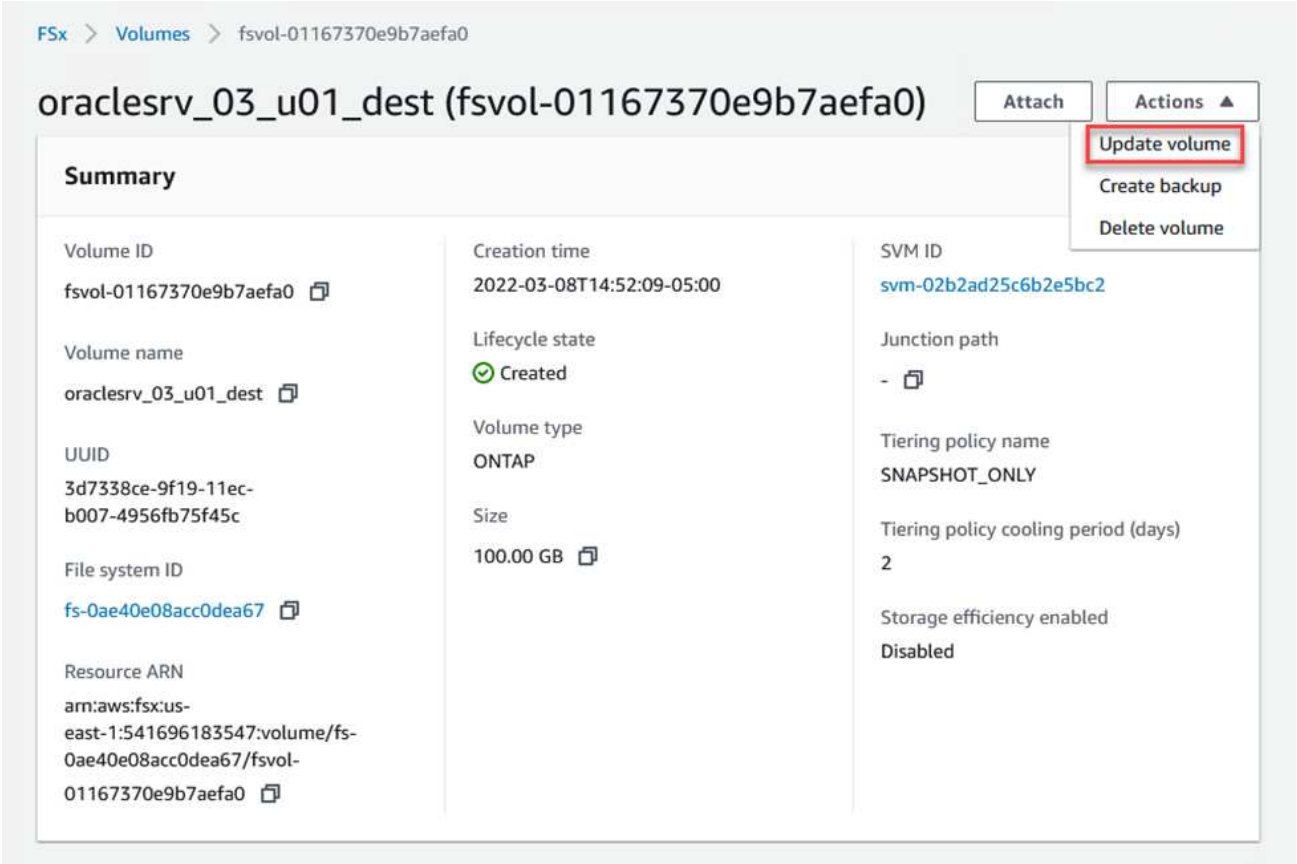
2. Execute o seguinte comando para quebrar os relacionamentos SnapMirror existentes.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:DestVolName
```

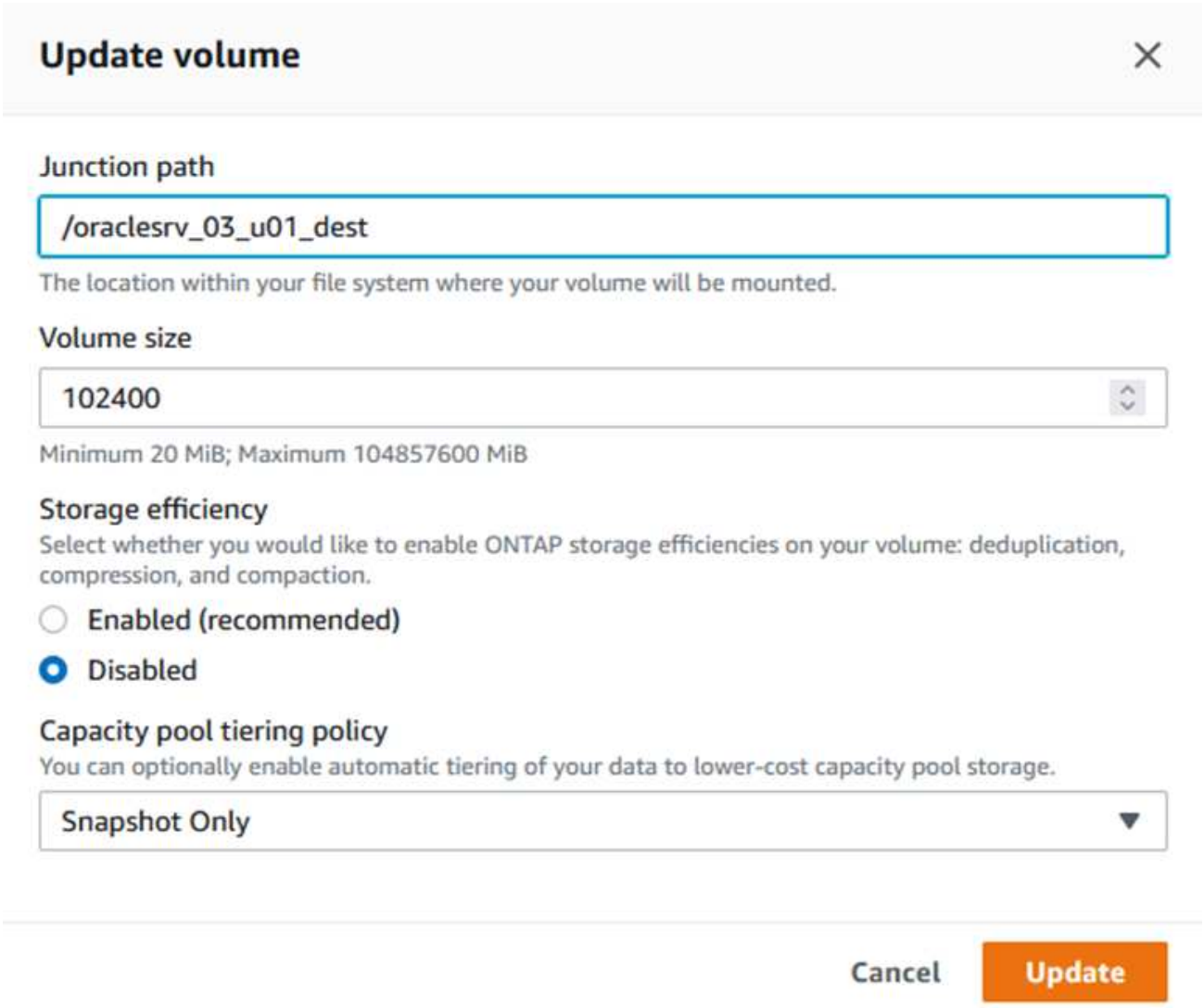
```
FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u02_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u02_dest".

FsxId0ae40e08acc0dea67::> snapmirror break -destination-path ora_svm_dest:oraclesrv_03_u03_dest
Operation succeeded: snapmirror break for destination "ora_svm_dest:oraclesrv_03_u03_dest".
```

3. Atualize o caminho de junção no cliente web do Amazon FSx :



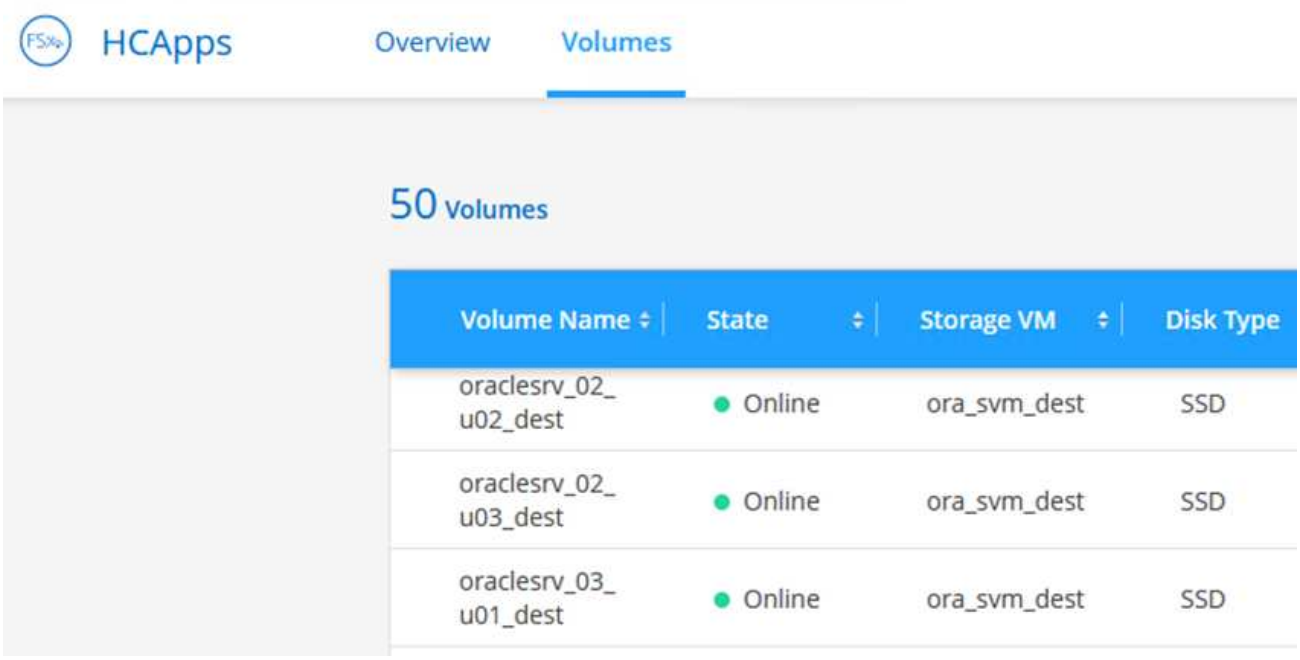
4. Adicione o nome do caminho de junção e clique em Atualizar. Especifique este caminho de junção ao montar o volume NFS do servidor Oracle.



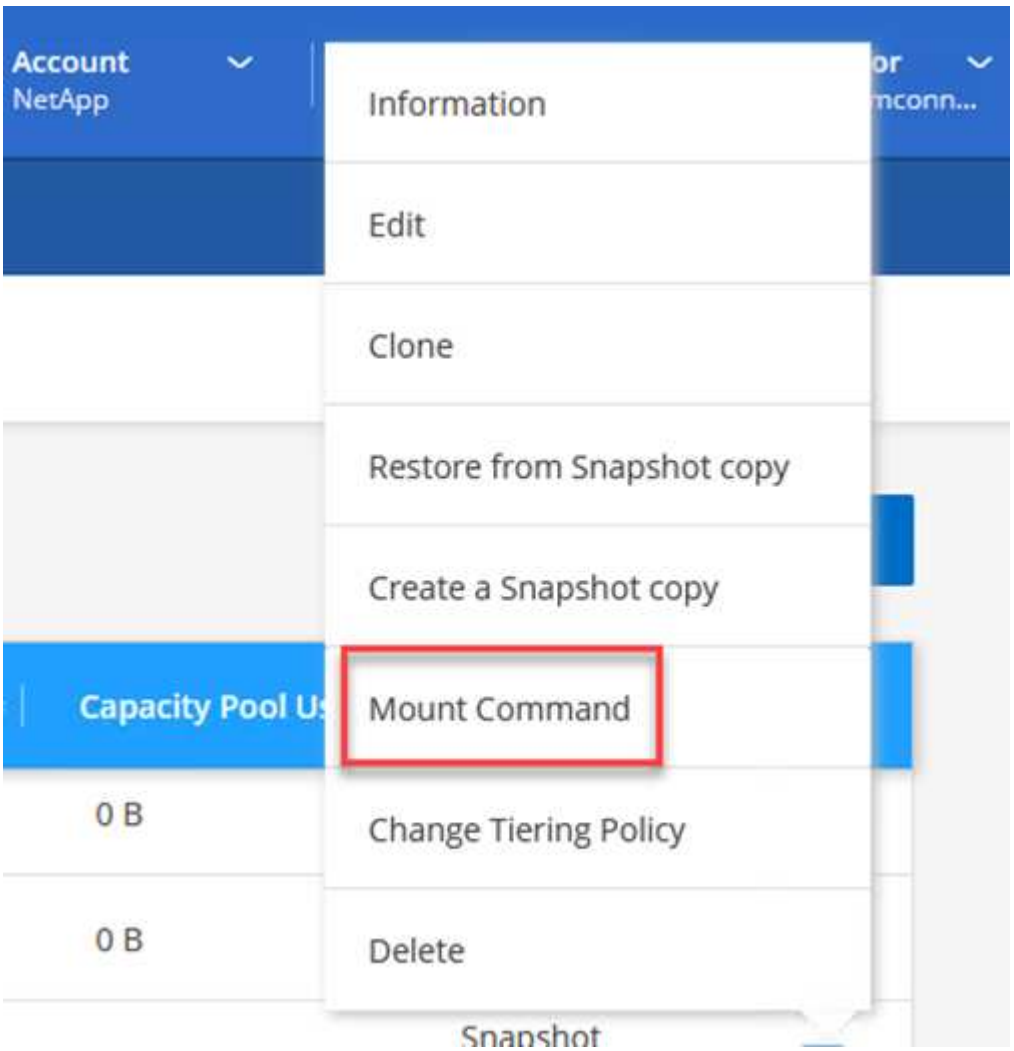
▼ **Montar volumes NFS no Oracle Server**

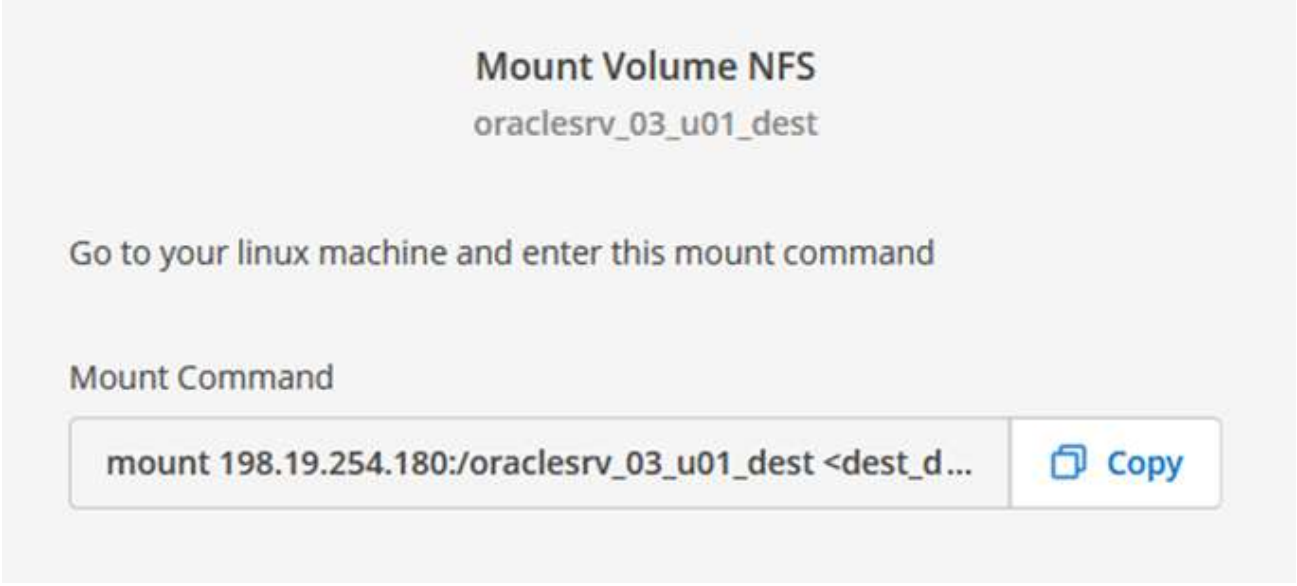
No Cloud Manager, você pode obter o comando mount com o endereço IP do NFS LIF correto para montar os volumes NFS que contêm os arquivos e logs do banco de dados Oracle.

1. No Cloud Manager, acesse a lista de volumes do seu cluster FSx.



2. No menu de ação, selecione Comando de montagem para visualizar e copiar o comando de montagem a ser usado em nosso servidor Oracle Linux.





3. Monte o sistema de arquivos NFS no Oracle Linux Server. Os diretórios para montar o compartilhamento NFS já existem no host Oracle Linux.
4. No servidor Oracle Linux, use o comando mount para montar os volumes NFS.

```
FSx-Dest::> mount -t oracle_server_ip:/junction-path
```

Repita esta etapa para cada volume associado aos bancos de dados Oracle.

Para tornar a montagem NFS persistente após a reinicialização, edite o `/etc/fstab` arquivo para incluir os comandos de montagem.

5. Reinicie o servidor Oracle. Os bancos de dados Oracle devem iniciar normalmente e estar disponíveis para uso.

Failback

Após a conclusão bem-sucedida do processo de failover descrito nesta solução, o SnapCenter e o Veeam retomam suas funções de backup em execução na AWS, e o FSx ONTAP agora é designado como armazenamento primário, sem relacionamentos SnapMirror existentes com o datacenter local original. Após a função normal ser retomada no local, você pode usar um processo idêntico ao descrito nesta documentação para espelhar dados de volta para o sistema de armazenamento ONTAP local.

Conforme também descrito nesta documentação, você pode configurar o SnapCenter para espelhar os volumes de dados do aplicativo do FSx ONTAP para um sistema de armazenamento ONTAP residente no local. Da mesma forma, você pode configurar o Veeam para replicar cópias de backup para o Amazon S3 usando um repositório de backup escalável para que esses backups sejam acessíveis a um servidor de backup do Veeam residente no datacenter local.

O failback está fora do escopo desta documentação, mas o failback difere pouco do processo detalhado descrito aqui.

Conclusão

O caso de uso apresentado nesta documentação se concentra em tecnologias comprovadas de recuperação de desastres que destacam a integração entre a NetApp e a VMware. Os sistemas de armazenamento NetApp ONTAP fornecem tecnologias comprovadas de espelhamento de dados que permitem que as organizações projetem soluções de recuperação de desastres que abrangem tecnologias locais e ONTAP residentes nos principais provedores de nuvem.

O FSx ONTAP na AWS é uma dessas soluções que permite integração perfeita com o SnapCenter e o SyncMirror para replicar dados de aplicativos na nuvem. O Veeam Backup & Replication é outra tecnologia bem conhecida que se integra bem aos sistemas de armazenamento NetApp ONTAP e pode fornecer failover para armazenamento nativo do vSphere.

Esta solução apresentou uma solução de recuperação de desastres usando armazenamento de conexão de convidado de um sistema ONTAP que hospeda dados de aplicativos SQL Server e Oracle. O SnapCenter com SnapMirror fornece uma solução fácil de gerenciar para proteger volumes de aplicativos em sistemas ONTAP e replicá-los para FSx ou CVO residentes na nuvem. O SnapCenter é uma solução habilitada para DR para failover de todos os dados do aplicativo para o VMware Cloud na AWS.

Veeam Backup e Restauração na VMware Cloud, com Amazon FSx ONTAP

O Veeam Backup & Replication é uma solução eficaz e confiável para proteger dados no VMware Cloud. Esta solução demonstra a configuração e a instalação corretas para usar o Veeam Backup and Replication para fazer backup e restaurar VMs de aplicativos que residem em datastores FSx ONTAP NFS no VMware Cloud.

Visão geral

O VMware Cloud (na AWS) oferece suporte ao uso de datastores NFS como armazenamento suplementar, e o FSx ONTAP é uma solução segura para clientes que precisam armazenar grandes quantidades de dados para seus aplicativos de nuvem que podem ser dimensionados independentemente do número de hosts ESXi no cluster SDDC. Este serviço de armazenamento integrado da AWS oferece armazenamento altamente eficiente com todos os recursos tradicionais do NetApp ONTAP .

Casos de uso

Esta solução aborda os seguintes casos de uso:

- Backup e restauração de máquinas virtuais Windows e Linux hospedadas no VMC usando o FSx ONTAP como repositório de backup.
- Backup e restauração de dados de aplicativos do Microsoft SQL Server usando o FSx ONTAP como repositório de backup.
- Backup e restauração de dados de aplicativos Oracle usando o FSx ONTAP como repositório de backup.

Armazenamentos de dados NFS usando Amazon FSx ONTAP

Todas as máquinas virtuais nesta solução residem em armazenamentos de dados NFS suplementares do FSx ONTAP . Usar o FSx ONTAP como um armazenamento de dados NFS suplementar tem vários benefícios. Por exemplo, permite que você:

- Crie um sistema de arquivos escalável e altamente disponível na nuvem sem a necessidade de configuração e gerenciamento complexos.

- Integre-se ao seu ambiente VMware existente, permitindo que você use ferramentas e processos familiares para gerenciar seus recursos de nuvem.
- Aproveite os recursos avançados de gerenciamento de dados fornecidos pelo ONTAP, como snapshots e replicação, para proteger seus dados e garantir sua disponibilidade.

▼ **Visão geral da implantação da solução**

Esta lista fornece as etapas de alto nível necessárias para configurar o Veeam Backup & Replication, executar tarefas de backup e restauração usando o FSx ONTAP como um repositório de backup e realizar restaurações de VMs e bancos de dados SQL Server e Oracle:

1. Crie o sistema de arquivos FSx ONTAP para ser usado como repositório de backup iSCSI para o Veeam Backup & Replication.
2. Implante o Veeam Proxy para distribuir cargas de trabalho de backup e montar repositórios de backup iSCSI hospedados no FSx ONTAP.
3. Configure tarefas de backup do Veeam para fazer backup de máquinas virtuais SQL Server, Oracle, Linux e Windows.
4. Restaure máquinas virtuais do SQL Server e bancos de dados individuais.
5. Restaure máquinas virtuais Oracle e bancos de dados individuais.

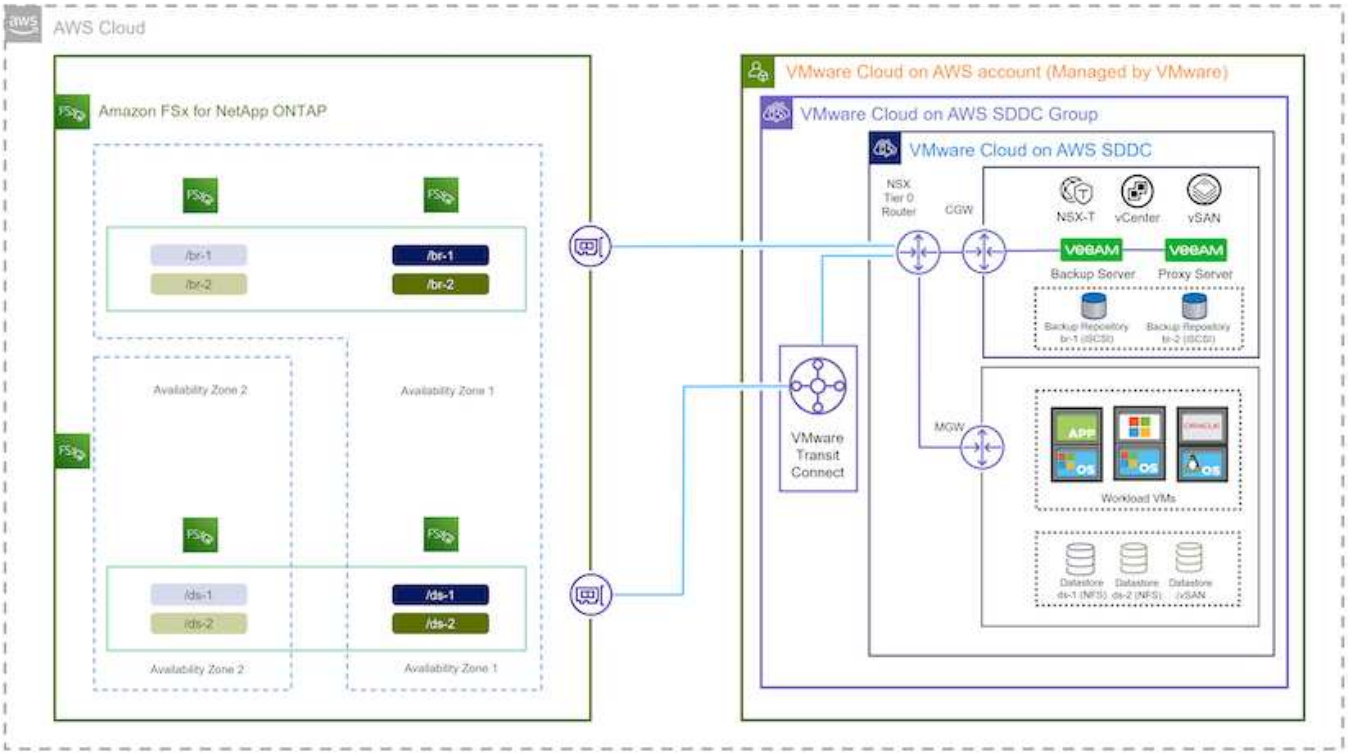
▼ **Pré-requisitos**

O objetivo desta solução é demonstrar a proteção de dados de máquinas virtuais em execução no VMware Cloud e localizadas em NFS Datastores hospedados pelo FSx ONTAP. Esta solução pressupõe que os seguintes componentes estejam configurados e prontos para uso:

1. Sistema de arquivos FSx ONTAP com um ou mais armazenamentos de dados NFS conectados ao VMware Cloud.
2. VM do Microsoft Windows Server com o software Veeam Backup & Replication instalado.
    - O servidor vCenter foi descoberto pelo servidor Veeam Backup & Replication usando seu endereço IP ou nome de domínio totalmente qualificado.
3. VM do Microsoft Windows Server a ser instalada com componentes do Veeam Backup Proxy durante a implantação da solução.
4. VMs do Microsoft SQL Server com VMDKs e dados de aplicativos residindo em armazenamentos de dados FSx ONTAP NFS. Para esta solução, tínhamos dois bancos de dados SQL em dois VMDKs separados.
    - Observação: como prática recomendada, os arquivos de banco de dados e de log de transações são colocados em unidades separadas, pois isso melhora o desempenho e a confiabilidade. Isso se deve em parte ao fato de que os logs de transações são gravados sequencialmente, enquanto os arquivos de banco de dados são gravados aleatoriamente.
5. VMs do Oracle Database com VMDKs e dados de aplicativos residindo em datastores FSx ONTAP NFS.
6. VMs de servidores de arquivos Linux e Windows com VMDKs residindo em armazenamentos de dados FSx ONTAP NFS.
7. O Veeam requer portas TCP específicas para comunicação entre servidores e componentes no ambiente de backup. Nos componentes de infraestrutura de backup da Veeam, as regras de firewall necessárias são criadas automaticamente. Para obter uma lista completa dos requisitos de porta de rede, consulte a seção Portas do "Guia do usuário de backup e replicação do Veeam para VMware vSphere" .

Arquitetura de Alto Nível

O teste/validação desta solução foi realizado em um laboratório que pode ou não corresponder ao ambiente de implantação final. Para mais informações, consulte as seções a seguir.



▼ **Componentes de hardware/software**

O objetivo desta solução é demonstrar a proteção de dados de máquinas virtuais em execução no VMware Cloud e localizadas em NFS Datastores hospedados pelo FSx ONTAP. Esta solução pressupõe que os seguintes componentes já estejam configurados e prontos para uso:

- VMs do Microsoft Windows localizadas em um armazenamento de dados FSx ONTAP NFS
- VMs Linux (CentOS) localizadas em um Datastore FSx ONTAP NFS
- VMs do Microsoft SQL Server localizadas em um armazenamento de dados FSx ONTAP NFS
  - Dois bancos de dados hospedados em VMDKs separados
- Oracle VMs localizadas em um FSx ONTAP NFS Datastore

Implantação de solução

Nesta solução, fornecemos instruções detalhadas para implantar e validar uma solução utilizando o software Veeam Backup and Replication para executar backup e recuperação de máquinas virtuais de servidores de arquivos SQL Server, Oracle e Windows e Linux em um VMware Cloud SDDC na AWS. As máquinas virtuais nesta solução residem em um armazenamento de dados NFS suplementar hospedado pelo FSx ONTAP. Além disso, um sistema de arquivos FSx ONTAP separado é usado para hospedar volumes iSCSI que serão usados para repositórios de backup do Veeam.

Abordaremos a criação do sistema de arquivos FSx ONTAP , a montagem de volumes iSCSI para serem usados como repositórios de backup, a criação e execução de tarefas de backup e a execução de restaurações de VM e banco de dados.

Para obter informações detalhadas sobre o FSx ONTAP, consulte o "Guia do usuário do FSx ONTAP" .

Para obter informações detalhadas sobre o Veeam Backup and Replication, consulte o "Documentação técnica da Central de Ajuda da Veeam" site.

Para considerações e limitações ao usar o Veeam Backup and Replication com o VMware Cloud na AWS, consulte "Suporte do VMware Cloud na AWS e VMware Cloud na Dell EMC. Considerações e Limitações" .

Implantar servidor proxy Veeam

Um servidor proxy Veeam é um componente do software Veeam Backup & Replication que atua como um intermediário entre a origem e o destino de backup ou replicação. O servidor proxy ajuda a otimizar e acelerar a transferência de dados durante tarefas de backup, processando dados localmente e pode usar diferentes modos de transporte para acessar dados usando APIs do VMware vStorage para proteção de dados ou por meio de acesso direto ao armazenamento.

Ao escolher um design de servidor proxy Veeam, é importante considerar o número de tarefas simultâneas e o modo de transporte ou tipo de acesso ao armazenamento desejado.

Para dimensionar o número de servidores proxy e seus requisitos de sistema, consulte o "Guia de boas práticas do Veeam VMware vSphere" .

O Veeam Data Mover é um componente do Veeam Proxy Server e utiliza um Modo de Transporte como método para obter dados de VM da origem e transferi-los para o destino. O modo de transporte é especificado durante a configuração da tarefa de backup. É possível aumentar a eficiência dos backups de armazenamentos de dados NFS usando acesso direto ao armazenamento.

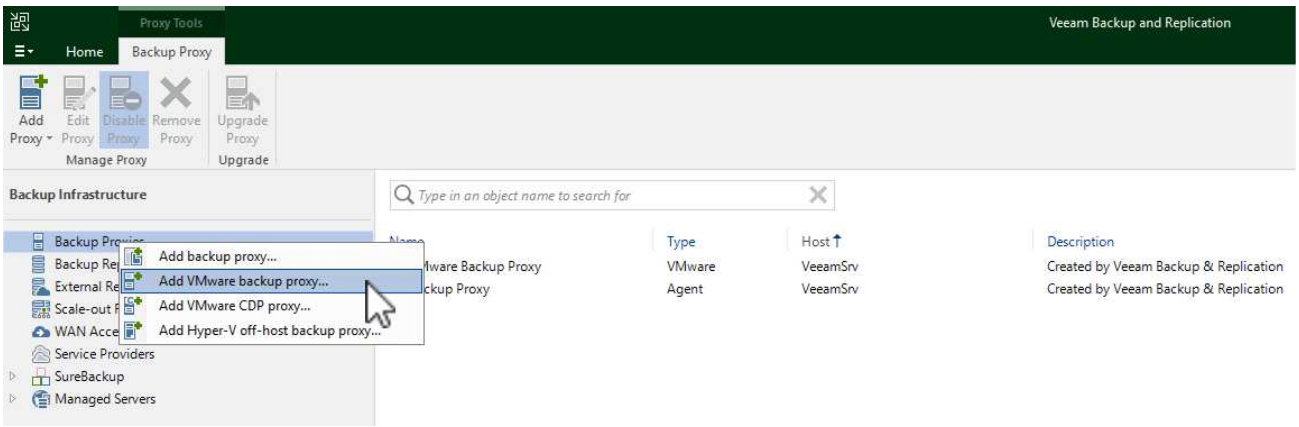
Para mais informações sobre os modos de transporte, consulte o "Guia do usuário de backup e replicação do Veeam para VMware vSphere" .

Na etapa a seguir, abordaremos a implantação do Veeam Proxy Server em uma VM Windows no VMware Cloud SDDC.

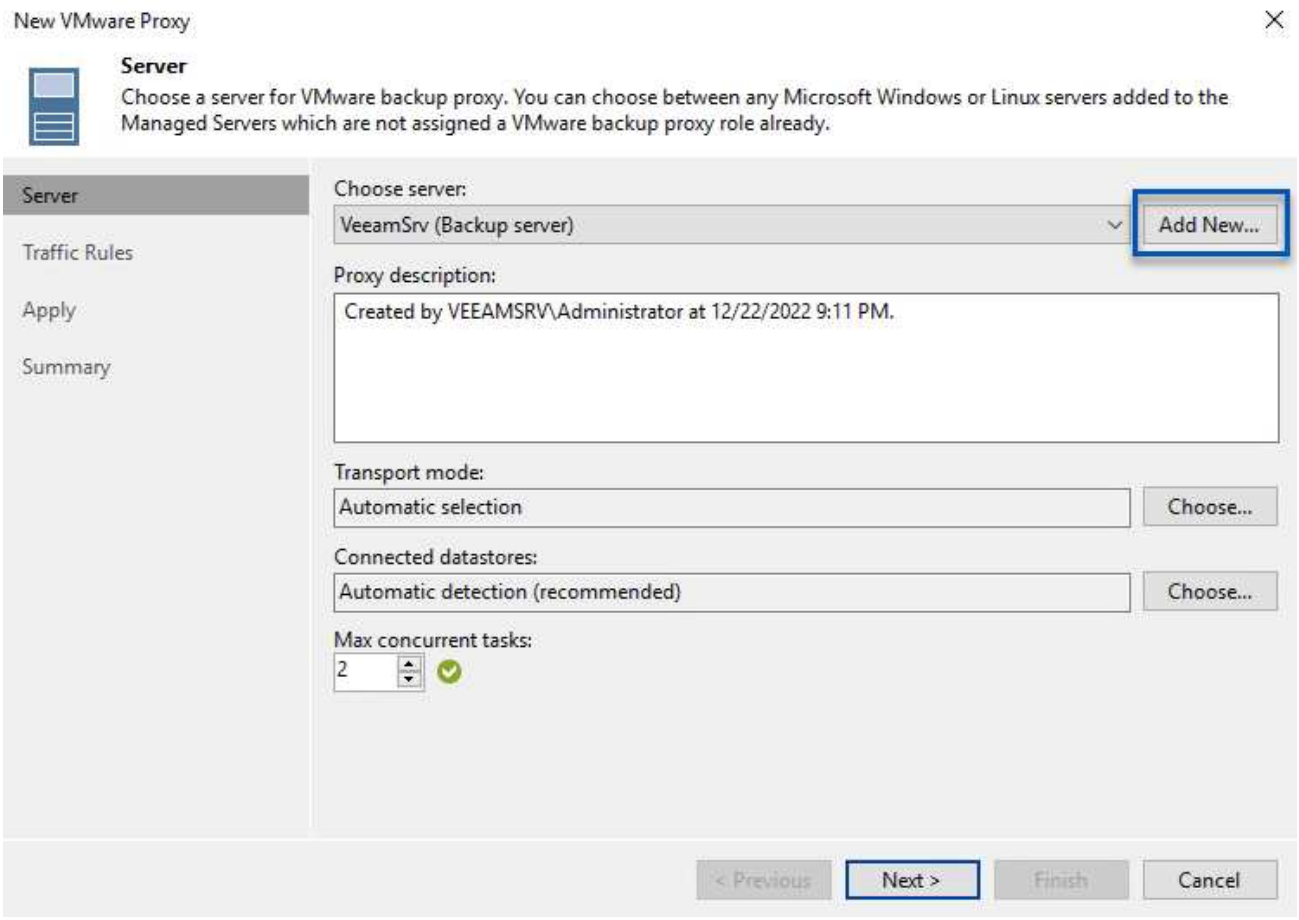
▼ **Implante o Veeam Proxy para distribuir cargas de trabalho de backup**

Nesta etapa, o Veeam Proxy é implantado em uma VM Windows existente. Isso permite que os trabalhos de backup sejam distribuídos entre o Veeam Backup Server principal e o Veeam Proxy.

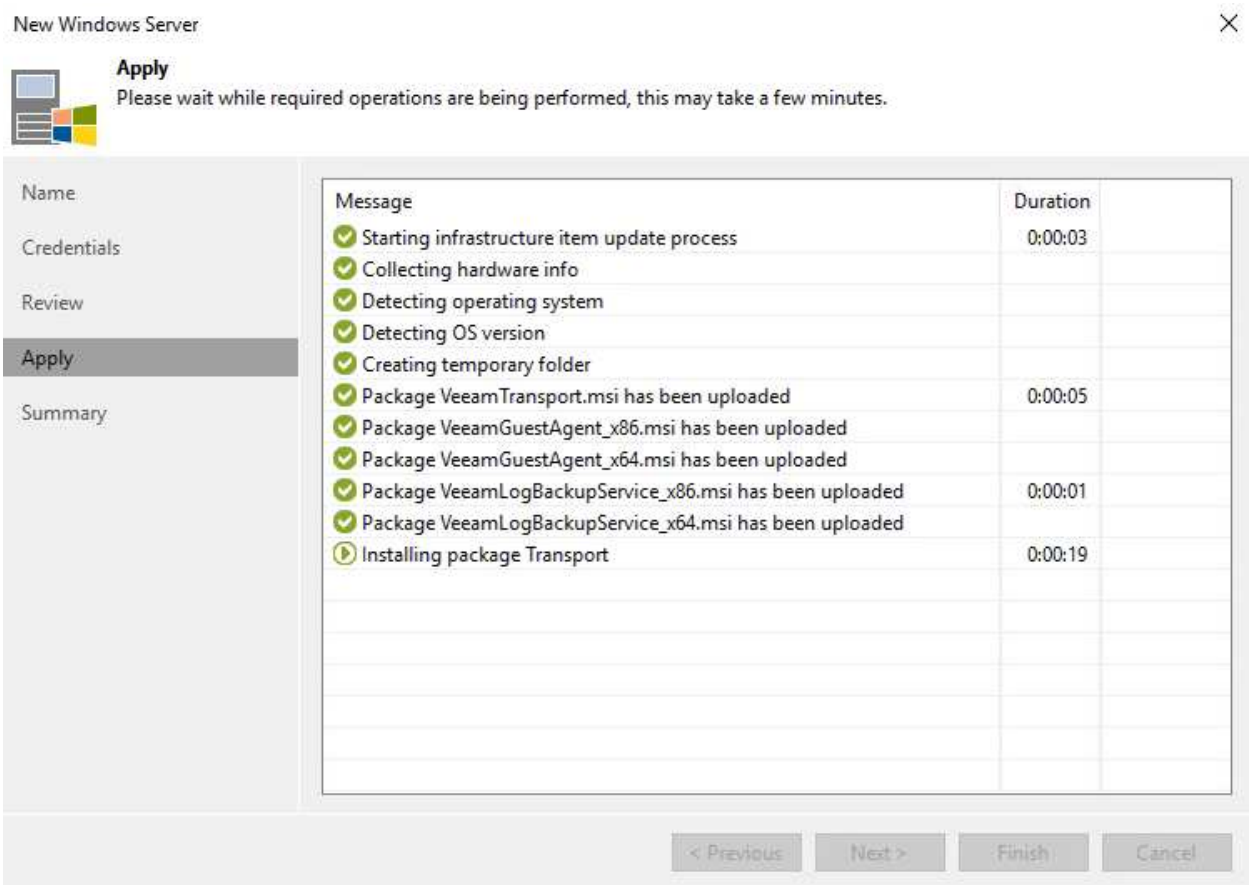
1. No servidor Veeam Backup and Replication, abra o console de administração e selecione **Infraestrutura de backup** no menu inferior esquerdo.
2. Clique com o botão direito do mouse em **Proxies de backup** e clique em **Adicionar proxy de backup VMware…** para abrir o assistente.



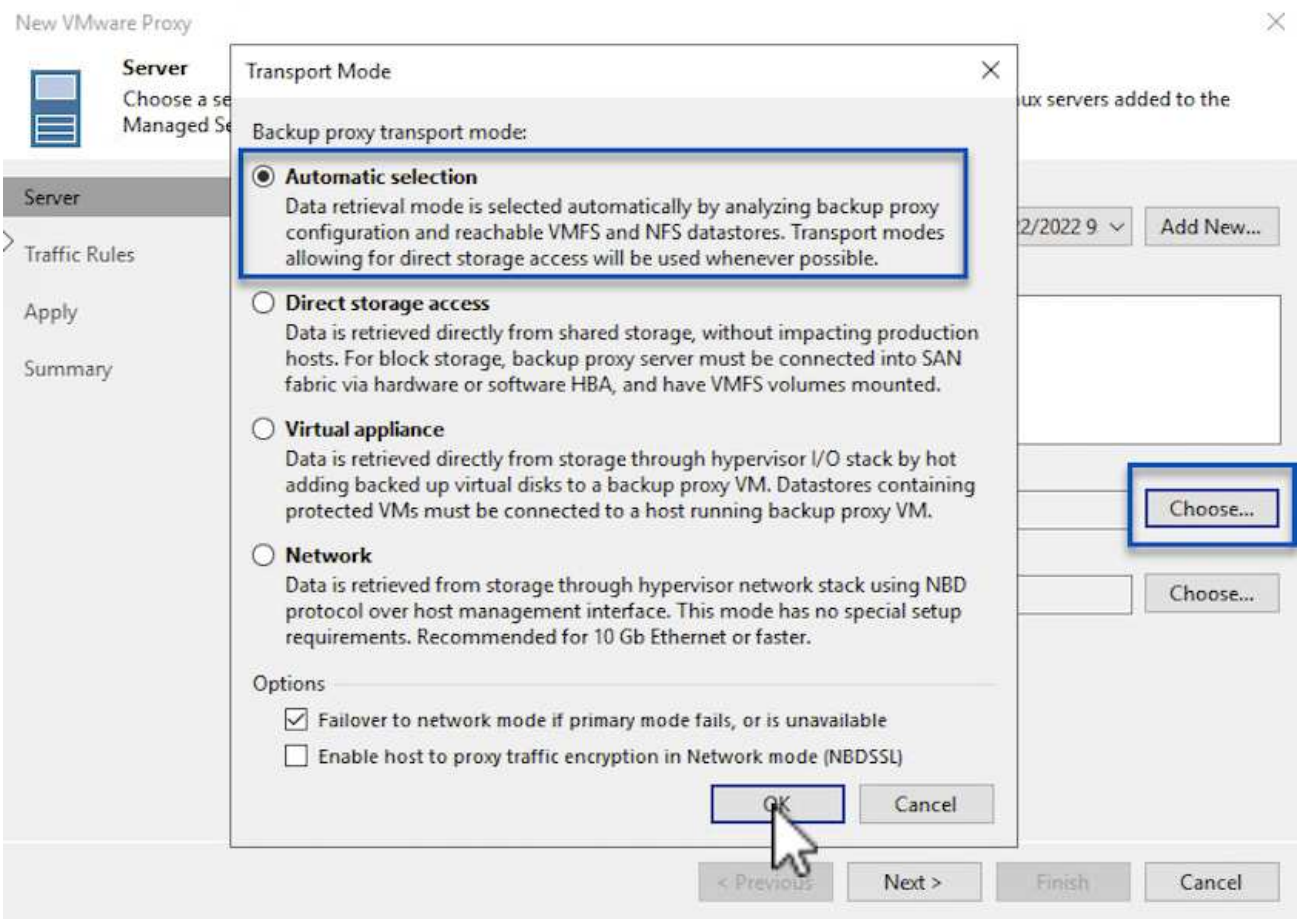
3. No assistente **Adicionar proxy VMware**, clique no botão **Adicionar novo…** para adicionar um novo servidor proxy.



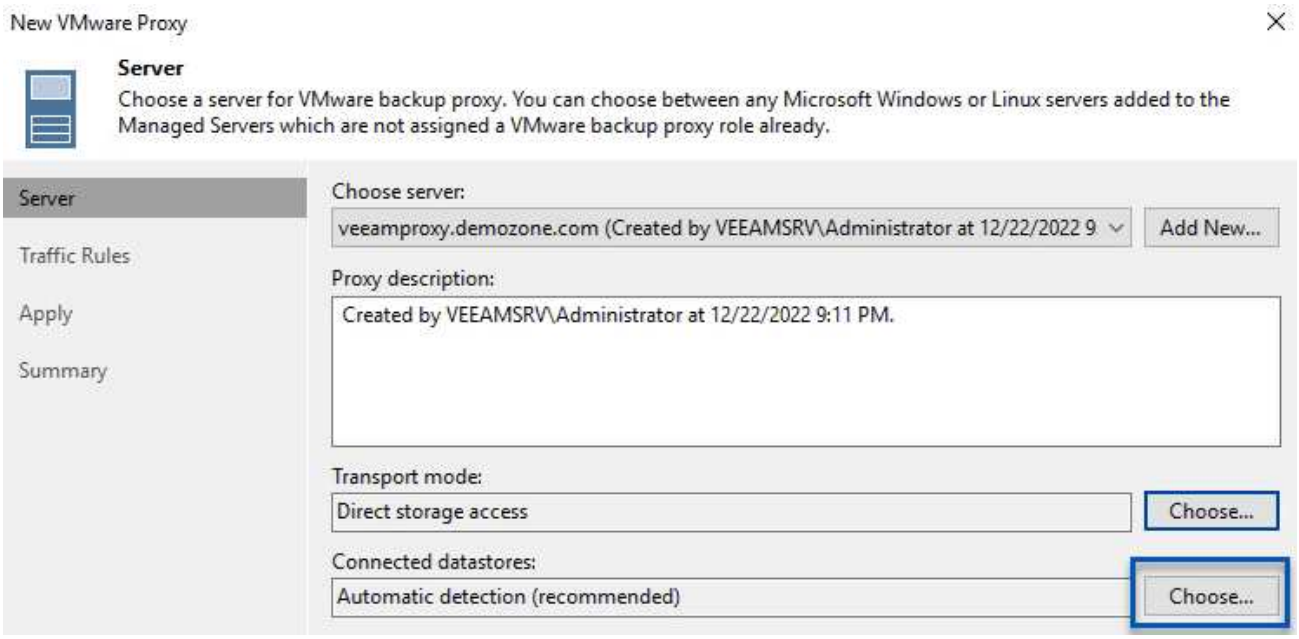
4. Selecione para adicionar o Microsoft Windows e siga as instruções para adicionar o servidor:
   - Preencha o nome DNS ou endereço IP
   - Selecione uma conta para usar para credenciais no novo sistema ou adicione novas credenciais
   - Revise os componentes a serem instalados e clique em **Aplicar** para iniciar a implantação

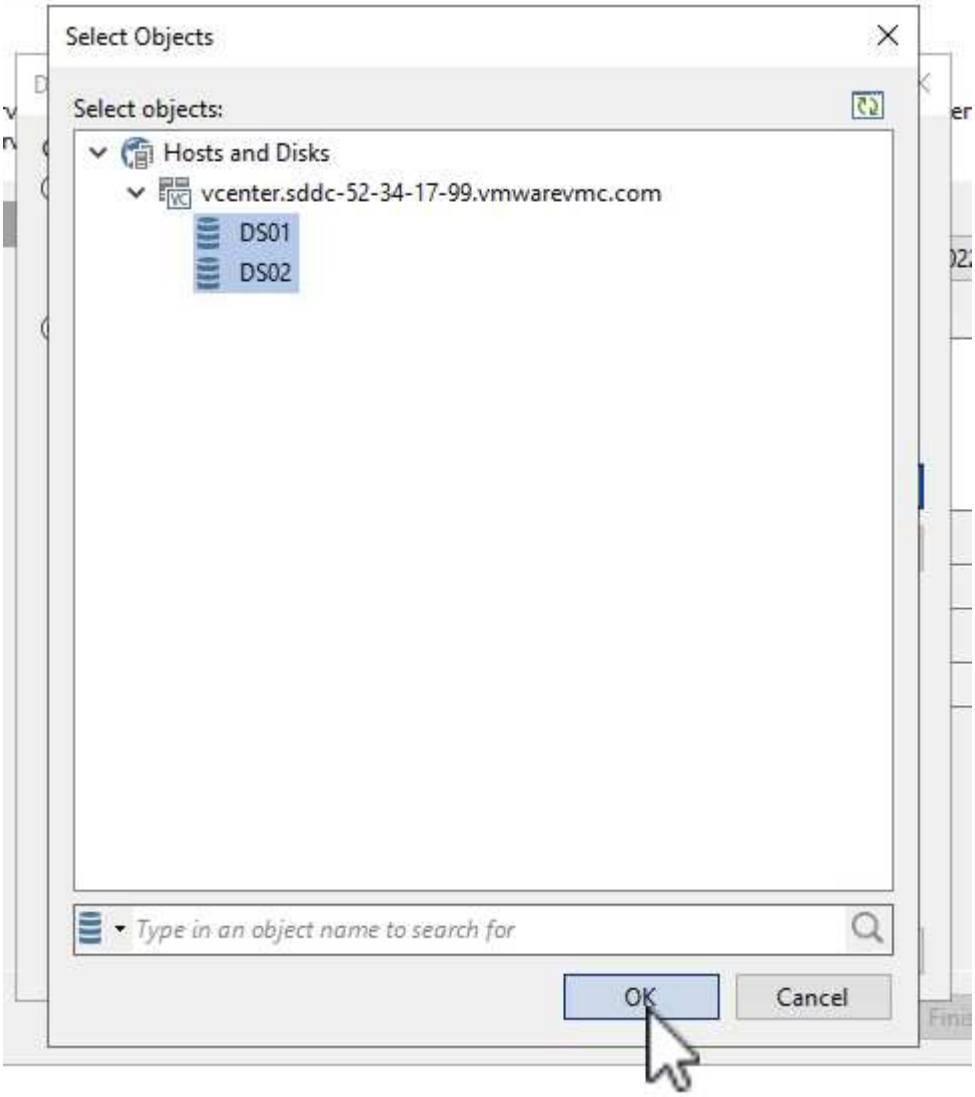


5. De volta ao assistente **Novo Proxy VMware**, escolha um Modo de Transporte. No nosso caso, escolhemos **Seleção Automática**.

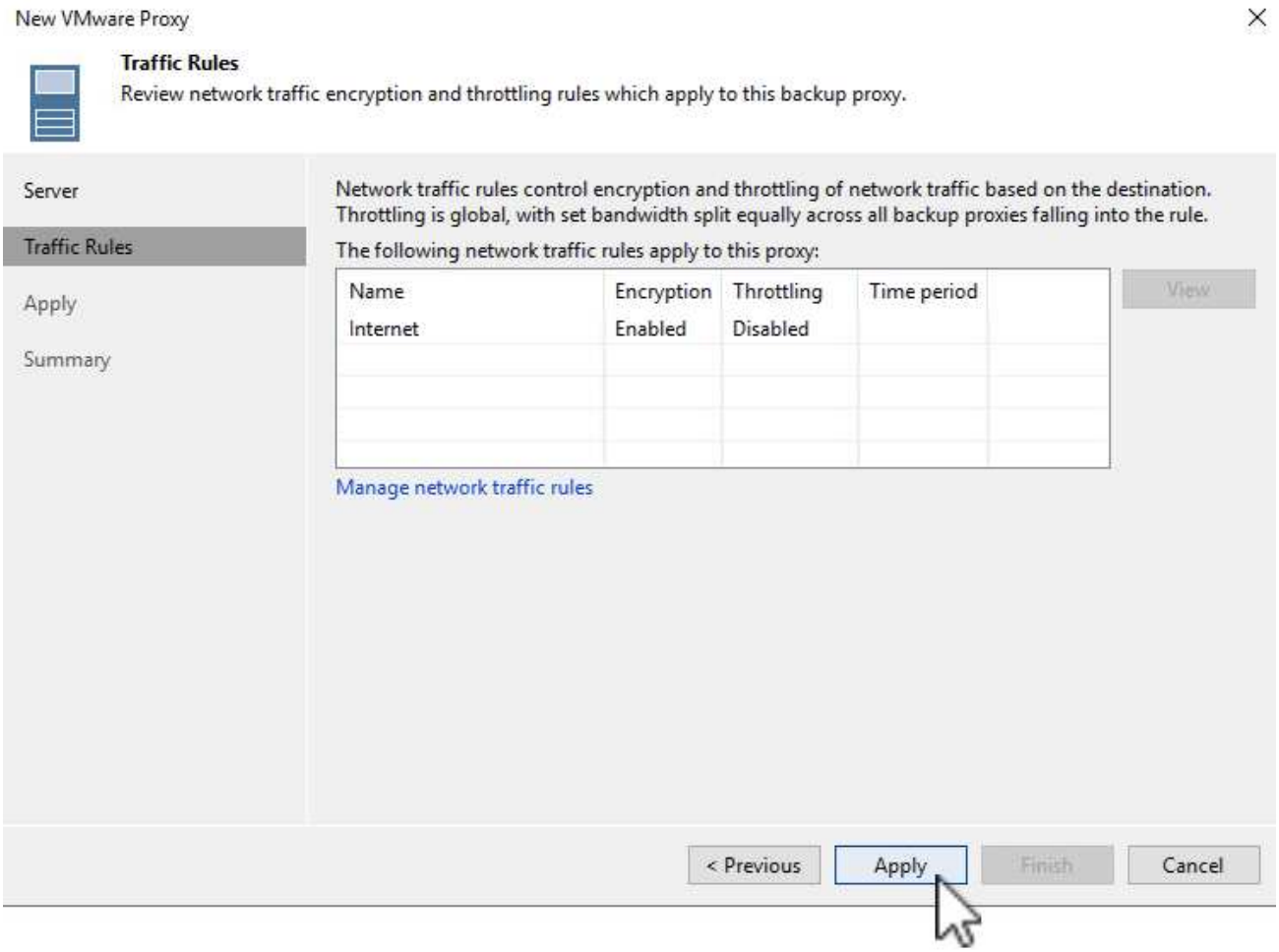


6. Selecione os datastores conectados aos quais você deseja que o VMware Proxy tenha acesso direto.





7. Configure e aplique quaisquer regras específicas de tráfego de rede, como criptografia ou limitação, que sejam desejadas. Quando terminar, clique no botão **Aplicar** para finalizar a implantação.



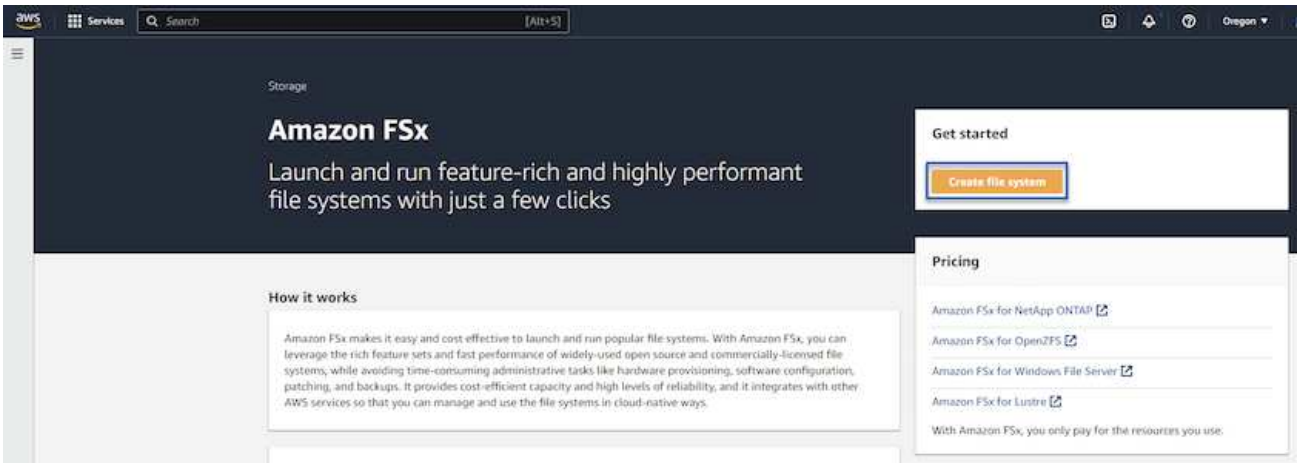
Configurar repositórios de armazenamento e backup

O servidor Veeam Backup principal e o servidor Veeam Proxy têm acesso a um repositório de backup na forma de armazenamento conectado diretamente. Nesta seção, abordamos a criação de um sistema de arquivos FSx ONTAP , a montagem de LUNs iSCSI nos servidores Veeam e a criação de repositórios de backup.

▼ Criar sistema de arquivos FSx ONTAP

Crie um sistema de arquivos FSx ONTAP que será usado para hospedar os volumes iSCSI para os Repositórios de Backup do Veeam.

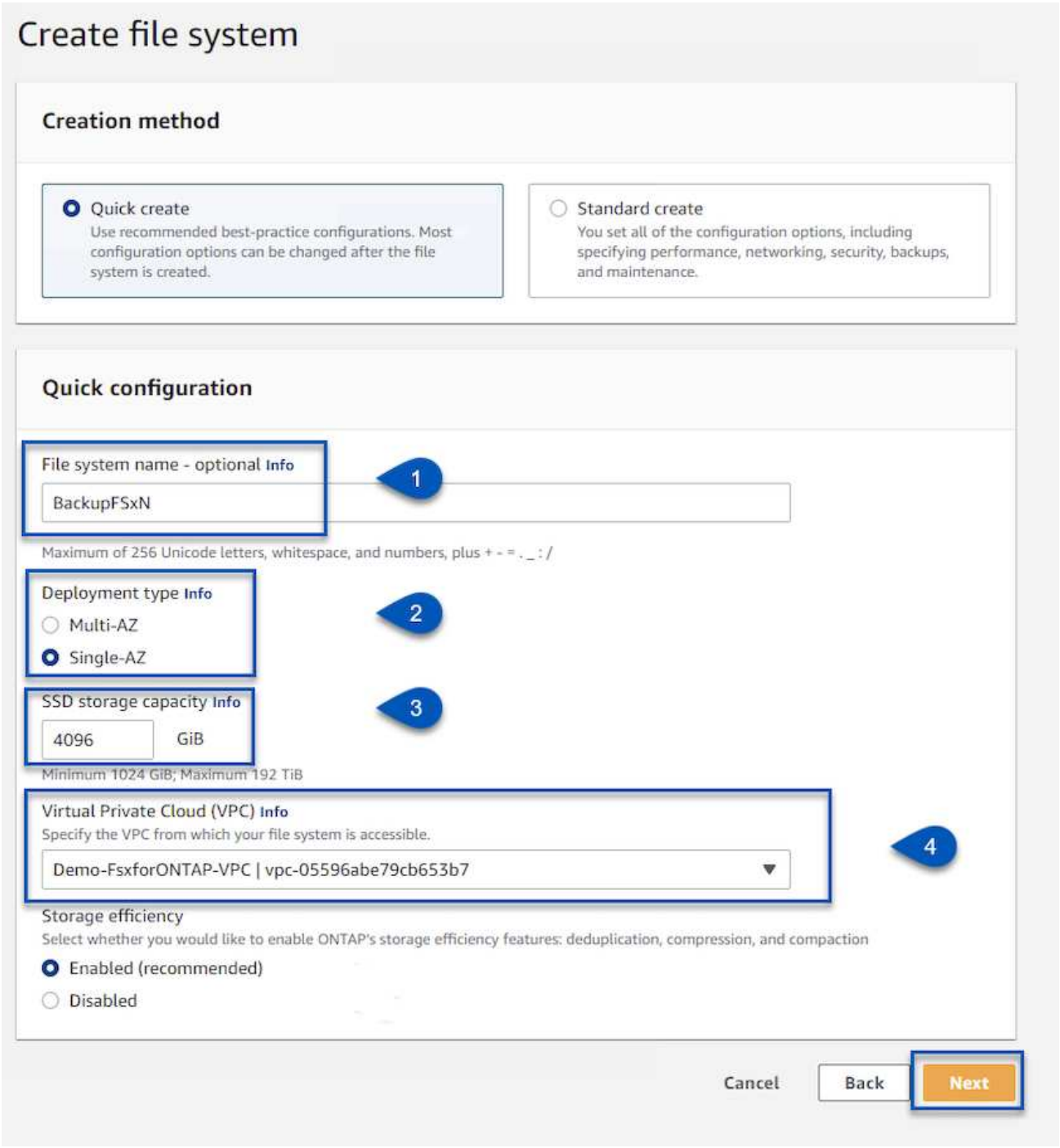
1. No console da AWS, vá para FSx e depois **Criar sistema de arquivos**



2. Selecione * Amazon FSx ONTAP* e depois **Avançar** para continuar.



3. Preencha o nome do sistema de arquivos, o tipo de implantação, a capacidade de armazenamento SSD e a VPC na qual o cluster FSx ONTAP residirá. Esta deve ser uma VPC configurada para se comunicar com a rede de máquinas virtuais no VMware Cloud. Clique em **Avançar**.



4. Revise as etapas de implantação e clique em **Criar sistema de arquivos** para iniciar o processo de criação do sistema de arquivos.

▼ **Configurar e montar LUNs iSCSI**

Crie e configure os LUNs iSCSI no FSx ONTAP e monte-os nos servidores proxy e de backup da Veeam. Esses LUNs serão usados posteriormente para criar repositórios de backup do Veeam.

ⓘ Criar um iSCSI LUN no FSx ONTAP é um processo de várias etapas. A primeira etapa da criação dos volumes pode ser realizada no Amazon FSx Console ou com o NetApp ONTAP CLI.

ⓘ Para obter mais informações sobre o uso do FSx ONTAP, consulte o "Guia do usuário do

FSx ONTAP" .

1. Na CLI do NetApp ONTAP, crie os volumes iniciais usando o seguinte comando:

```
FSx-Backup::> volume create -vserver svm_name -volume vol_name
-aggregate aggregate_name -size vol_size -type RW
```

2. Crie LUNs usando os volumes criados na etapa anterior:

```
FSx-Backup::> lun create -vserver svm_name -path
/vol/vol_name/lun_name -size size -ostype windows -space-allocation
enabled
```

3. Conceda acesso aos LUNs criando um grupo iniciador contendo o IQN iSCSI dos servidores proxy e de backup da Veeam:

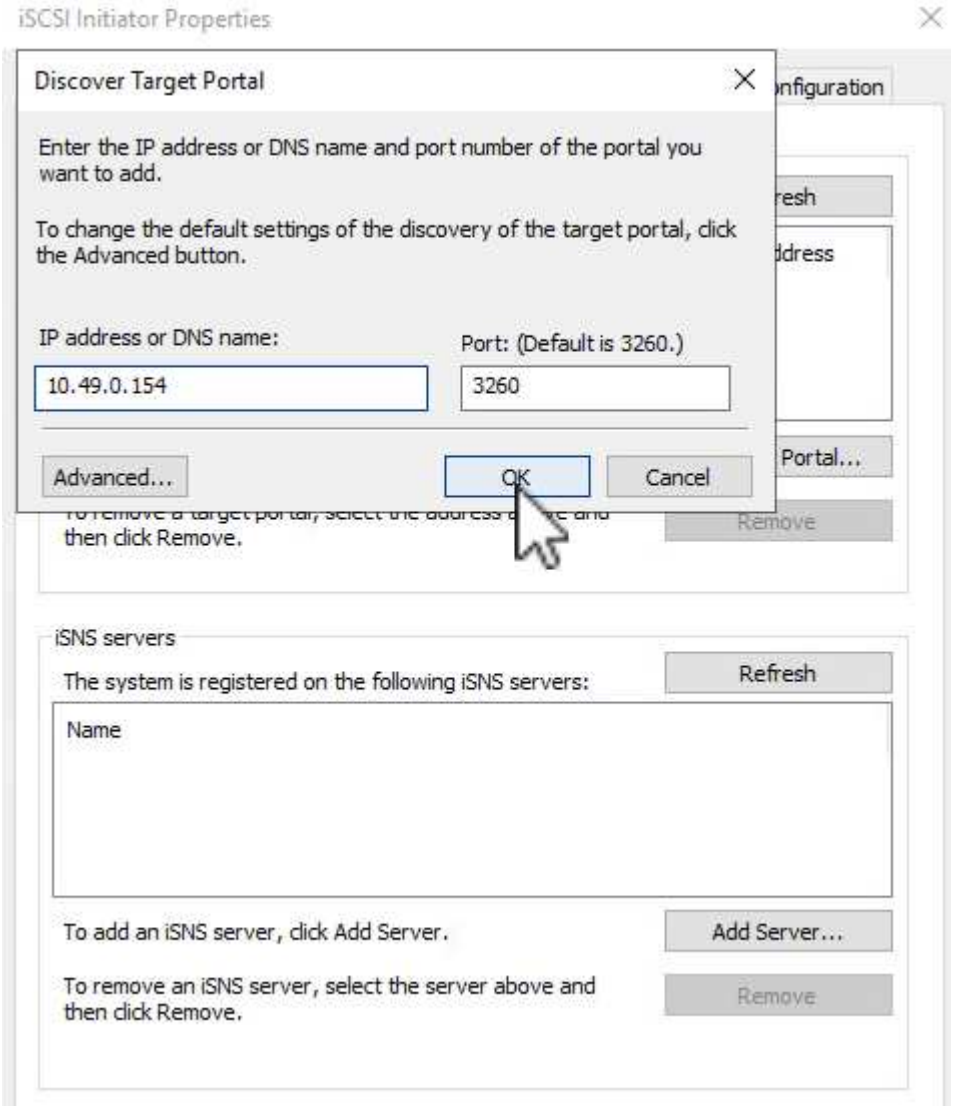
```
FSx-Backup::> igroup create -vserver svm_name -igroup igroup_name
-protocol iSCSI -ostype windows -initiator IQN
```

Para concluir a etapa anterior, você precisará primeiro recuperar o IQN das propriedades do iniciador iSCSI nos servidores Windows.

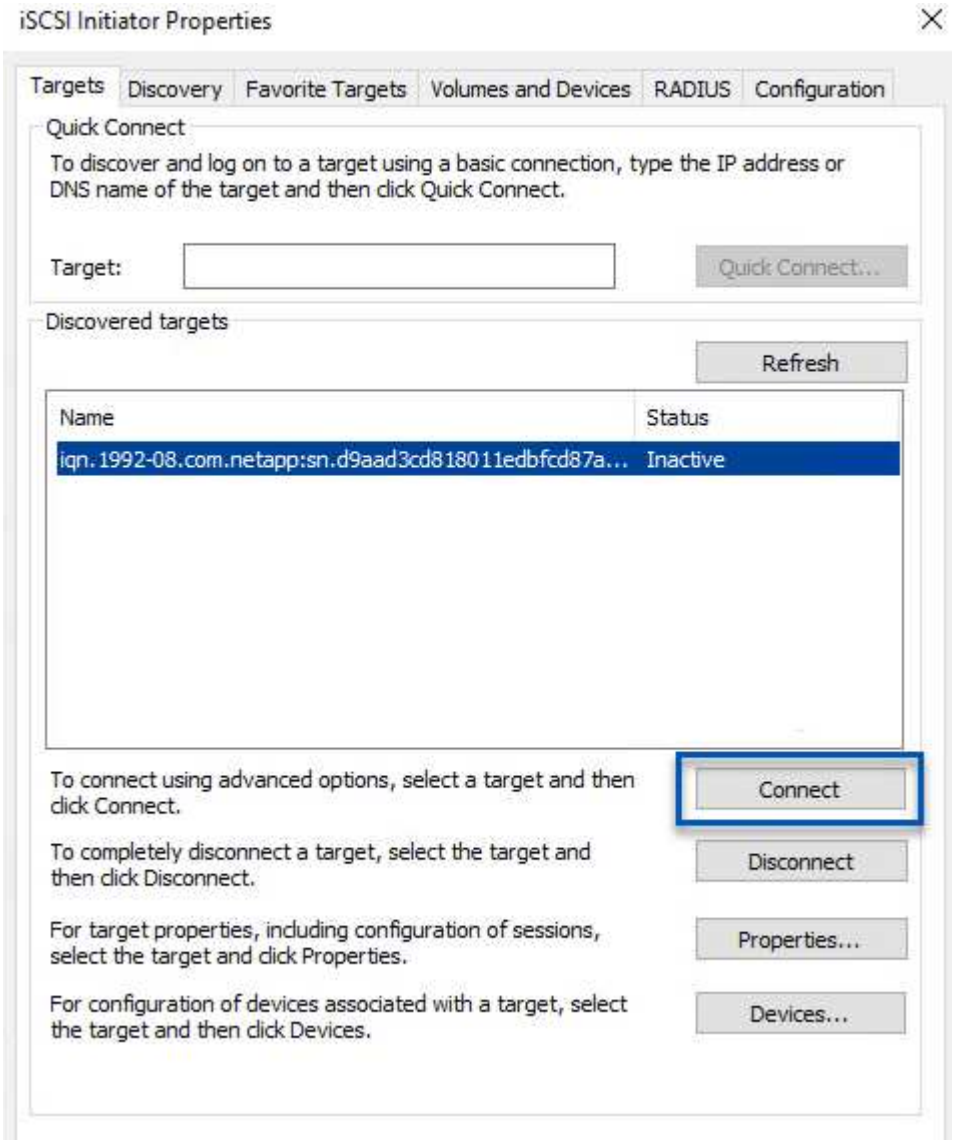
4. Por fim, mapeie os LUNs para o grupo iniciador que você acabou de criar:

```
FSx-Backup::> lun mapping create -vserver svm_name -path
/vol/vol_name/lun_name igroup igroup_name
```

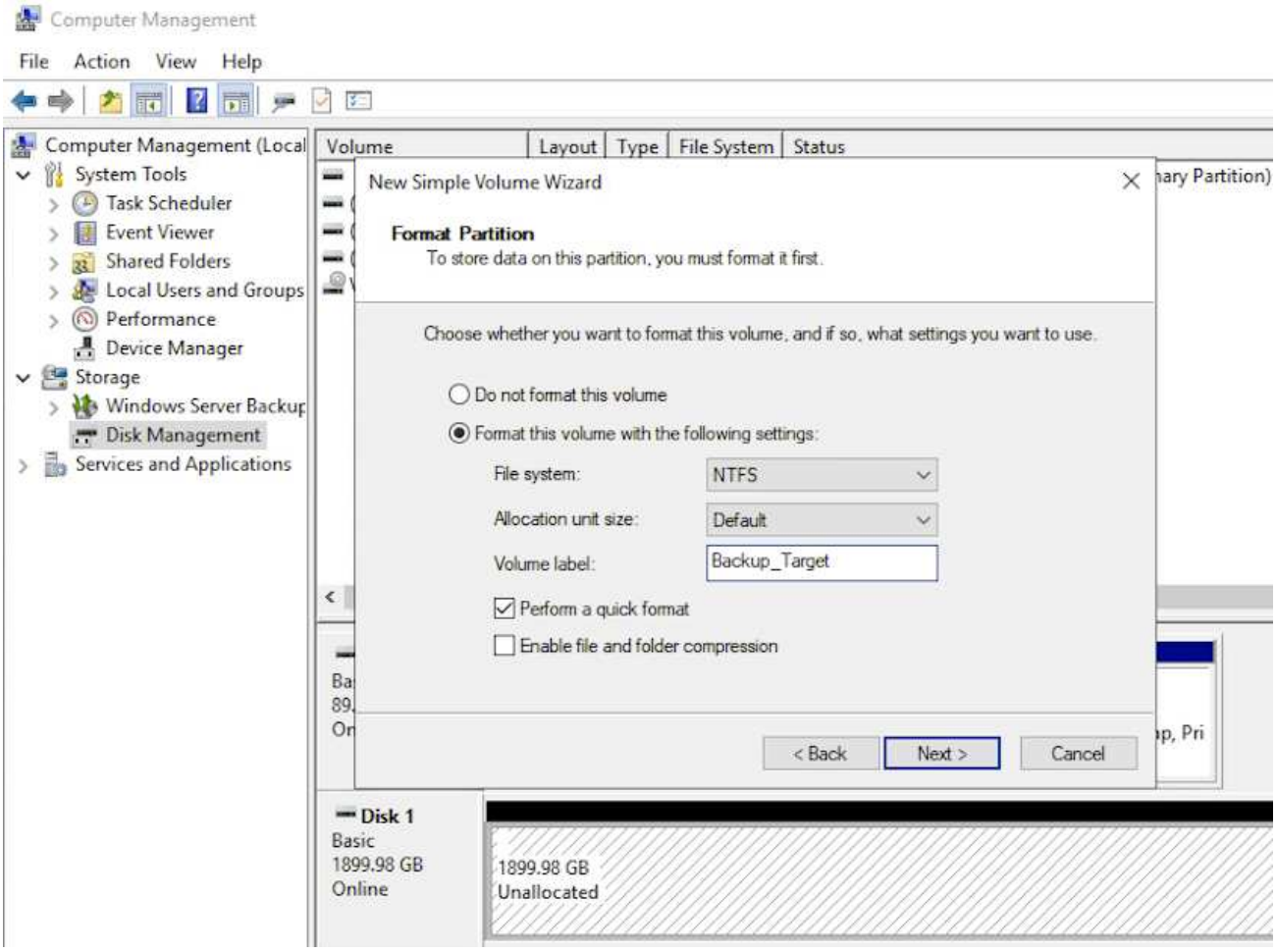
5. Para montar os LUNs iSCSI, faça login no Veeam Backup & Replication Server e abra as Propriedades do Iniciador iSCSI. Vá para a aba **Descobrir** e insira o endereço IP de destino iSCSI.



6. Na aba **Destinos**, realce o LUN inativo e clique em **Conectar**. Marque a caixa **Ativar múltiplos caminhos** e clique em **OK** para conectar ao LUN.



7. No utilitário Gerenciamento de Disco, inicialize o novo LUN e crie um volume com o nome e a letra de unidade desejados. Marque a caixa **Ativar múltiplos caminhos** e clique em **OK** para conectar ao LUN.

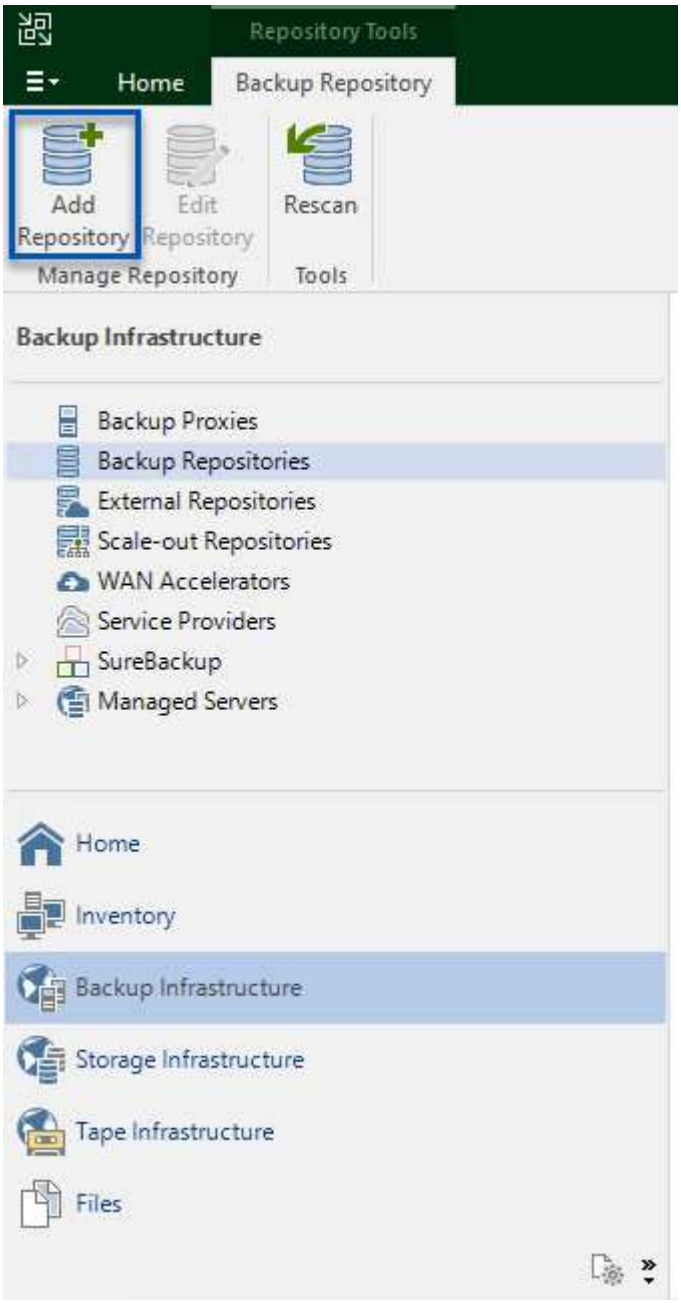


8. Repita essas etapas para montar os volumes iSCSI no servidor Veeam Proxy.

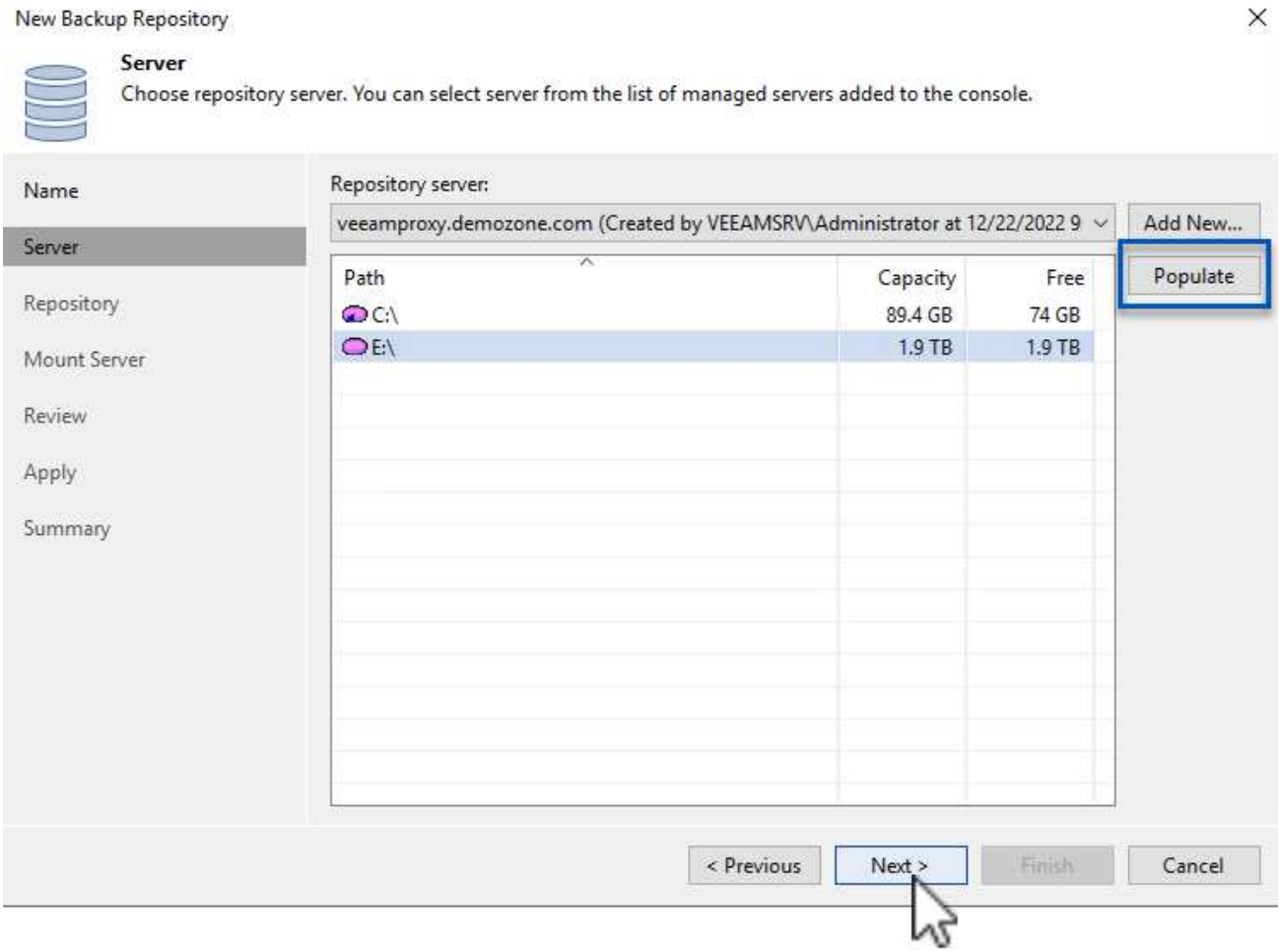
▼ **Criar repositórios de backup do Veeam**

No console do Veeam Backup and Replication, crie repositórios de backup para os servidores Veeam Backup e Veeam Proxy. Esses repositórios serão usados como destinos de backup para os backups das máquinas virtuais.

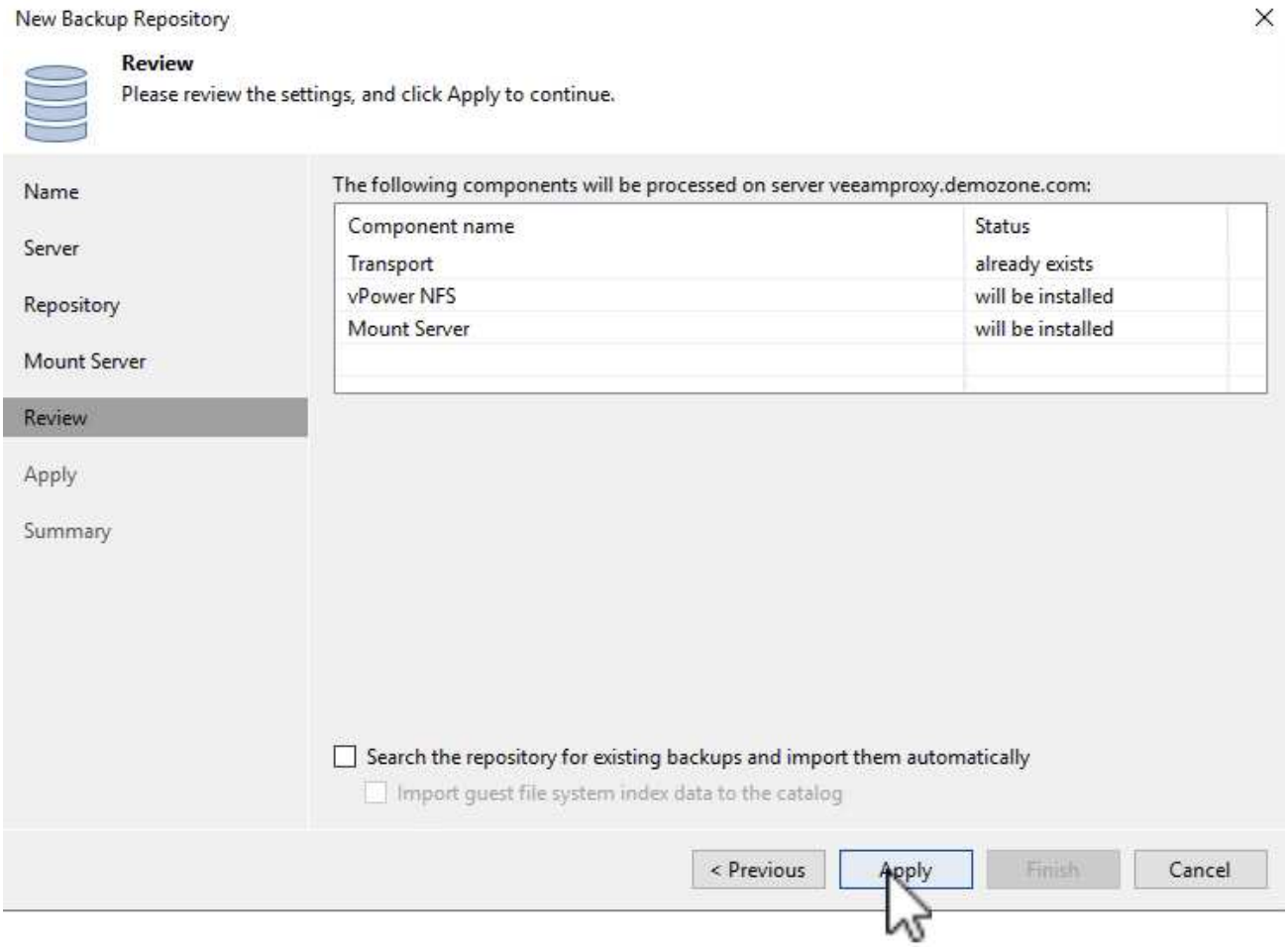
1. No console do Veeam Backup and Replication, clique em **Infraestrutura de backup** no canto inferior esquerdo e selecione **Adicionar repositório**



2. No assistente Novo Repositório de Backup, insira um nome para o repositório, selecione o servidor na lista suspensa e clique no botão **Preencher** para escolher o volume NTFS que será usado.



3. Na próxima página, escolha um servidor de montagem que será usado para montar backups ao executar restaurações avançadas. Por padrão, este é o mesmo servidor que tem o armazenamento do repositório conectado.
4. Revise suas seleções e clique em **Aplicar** para iniciar a criação do repositório de backup.



5. Repita essas etapas para quaisquer servidores proxy adicionais.

Configurar tarefas de backup do Veeam

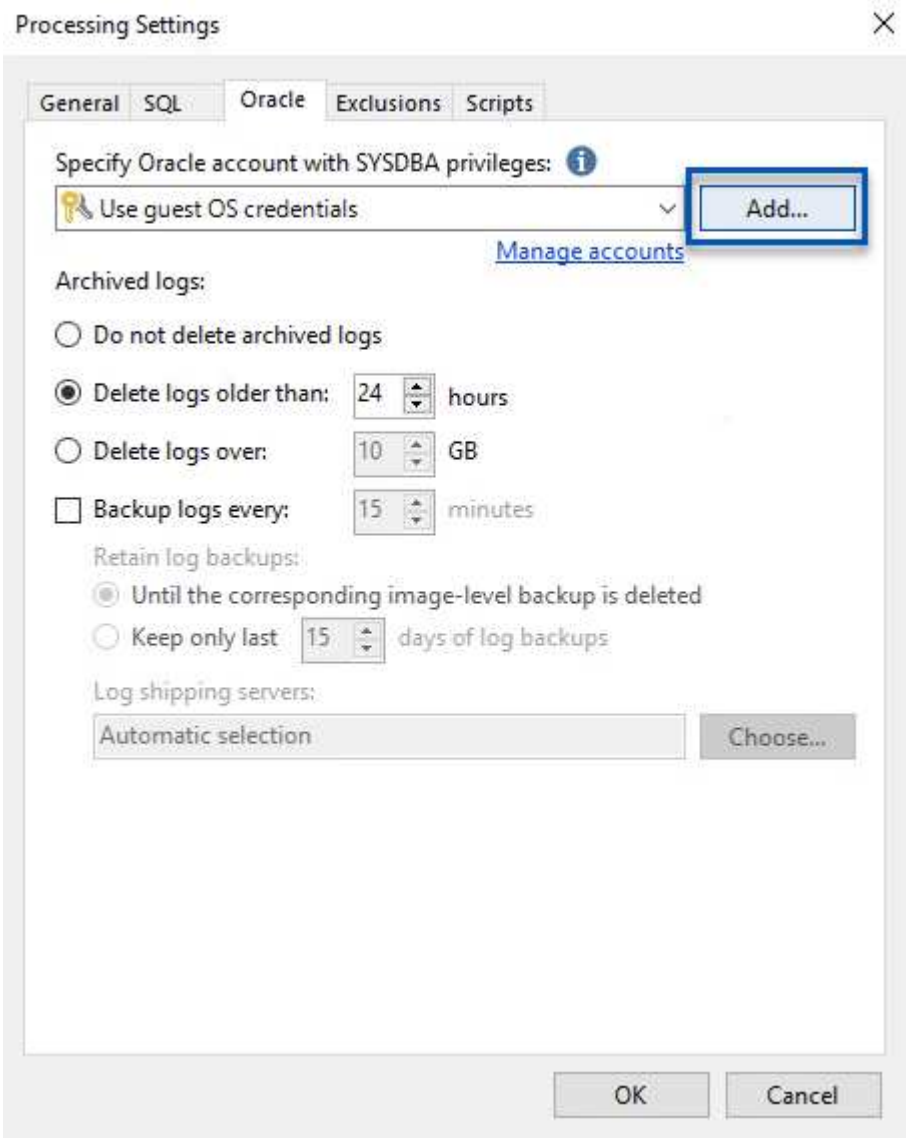
Os trabalhos de backup devem ser criados utilizando os Repositórios de Backup da seção anterior. A criação de tarefas de backup é uma parte normal do repertório de qualquer administrador de armazenamento e não abordaremos todas as etapas aqui. Para obter informações mais completas sobre a criação de tarefas de backup no Veeam, consulte o "Documentação técnica da Central de Ajuda da Veeam" .

Nesta solução, foram criados trabalhos de backup separados para:

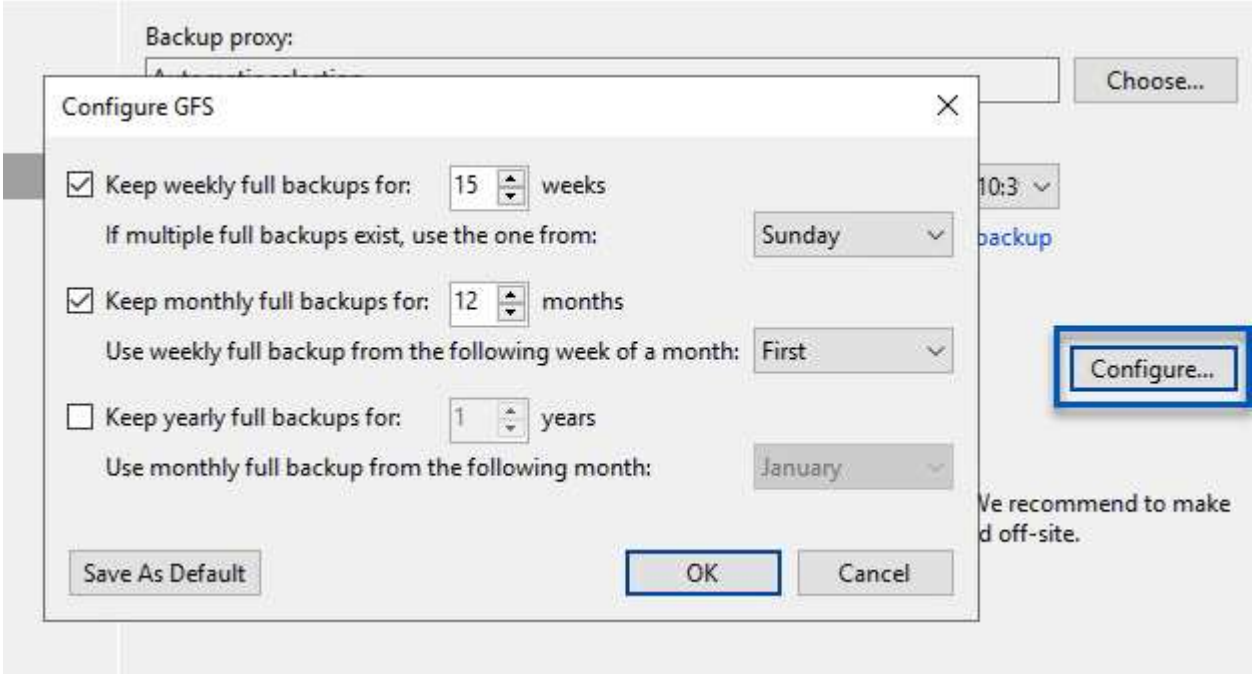
- Servidores SQL do Microsoft Windows
- Servidores de banco de dados Oracle
- Servidores de arquivos do Windows
- Servidores de arquivos Linux

▼ Considerações gerais ao configurar tarefas de backup do Veeam

1. Habilite o processamento com reconhecimento de aplicativo para criar backups consistentes e executar o processamento de log de transações.
2. Depois de habilitar o processamento com reconhecimento de aplicativo, adicione as credenciais corretas com privilégios de administrador ao aplicativo, pois elas podem ser diferentes das credenciais do sistema operacional convidado.



3. Para gerenciar a política de retenção do backup, marque a opção **Manter determinados backups completos por mais tempo para fins de arquivamento** e clique no botão **Configurar…** para configurar a política.



Restaurar VMs de aplicativos com restauração completa do Veeam

Executar uma restauração completa com o Veeam é o primeiro passo para executar uma restauração de aplicativo. Validamos que restaurações completas de nossas VMs estavam ligadas e todos os serviços estavam funcionando normalmente.

Restaurar servidores é uma parte normal do repertório de qualquer administrador de armazenamento e não abordaremos todas as etapas aqui. Para obter informações mais completas sobre como executar restaurações completas no Veeam, consulte o "Documentação técnica da Central de Ajuda da Veeam" .

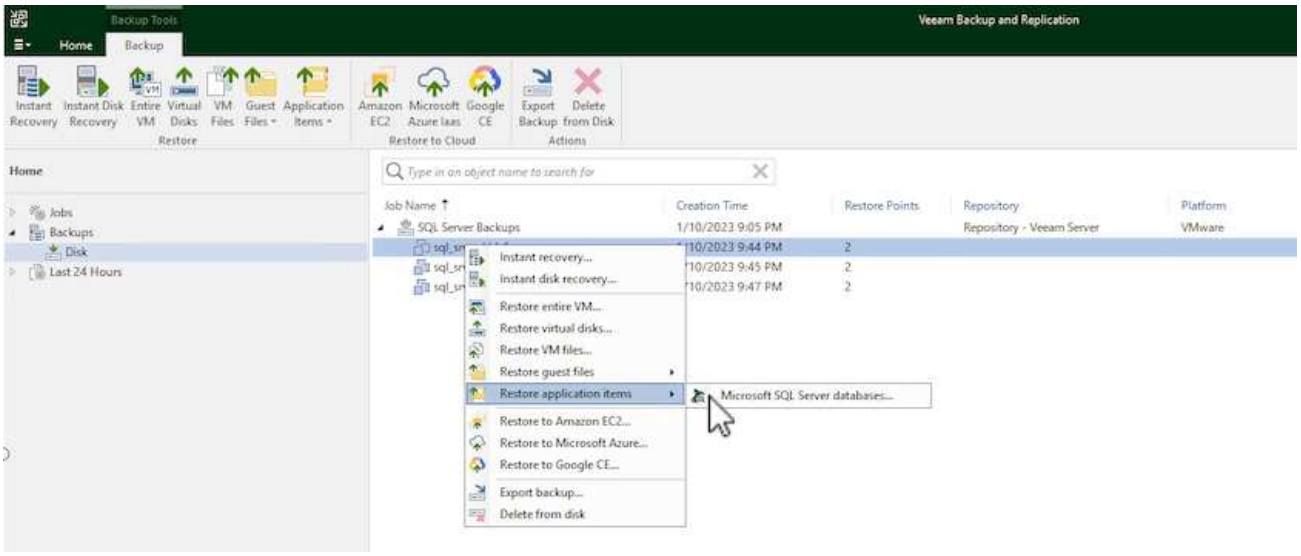
Restaurar bancos de dados do SQL Server

O Veeam Backup & Replication oferece diversas opções para restaurar bancos de dados do SQL Server. Para esta validação, usamos o Veeam Explorer para SQL Server com Instant Recovery para executar restaurações de nossos bancos de dados SQL Server. O SQL Server Instant Recovery é um recurso que permite restaurar rapidamente bancos de dados do SQL Server sem precisar esperar por uma restauração completa do banco de dados. Esse processo de recuperação rápida minimiza o tempo de inatividade e garante a continuidade dos negócios. Veja como funciona:

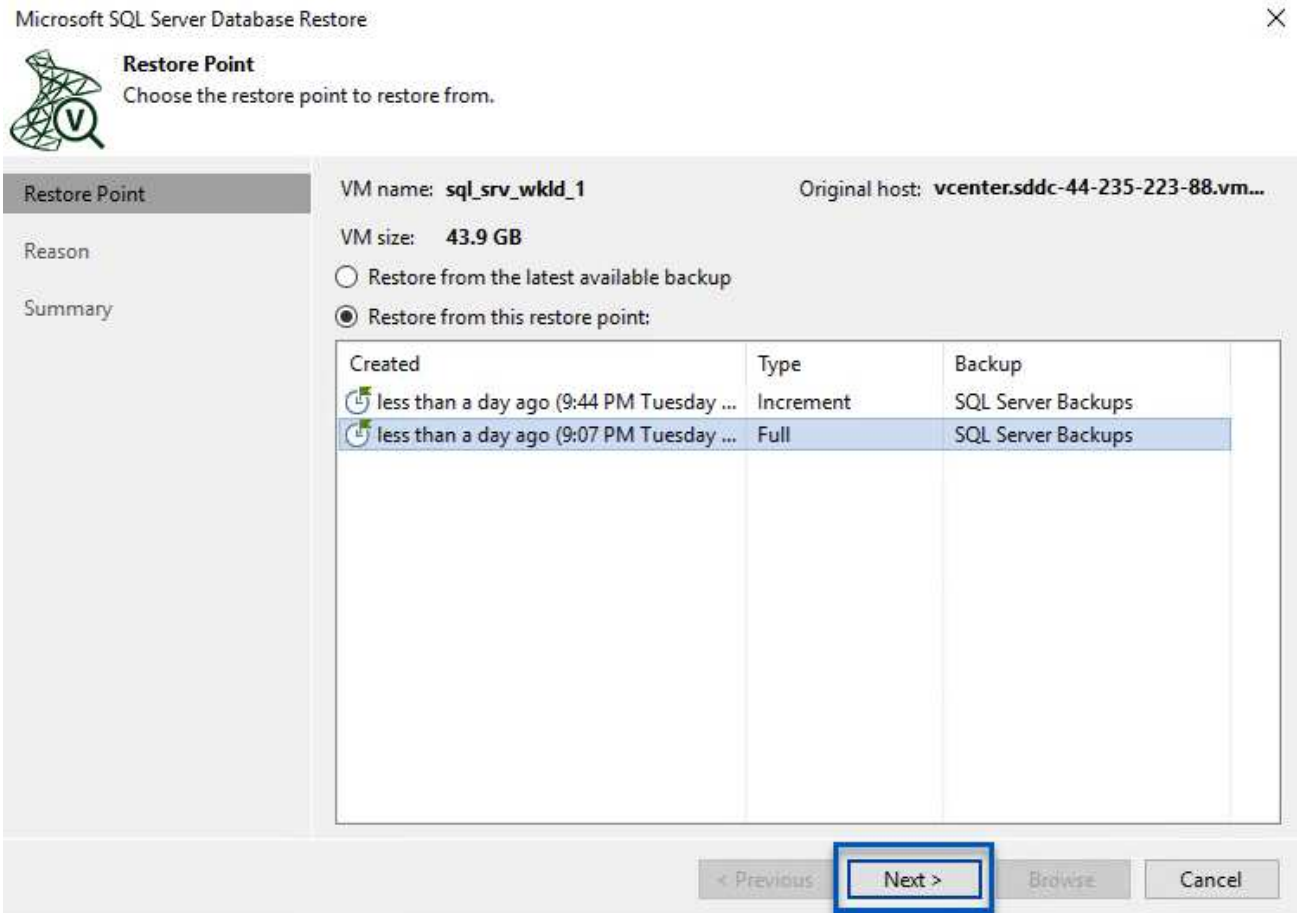
- O Veeam Explorer **monta o backup** contendo o banco de dados SQL Server a ser restaurado.
- O software **publica o banco de dados** diretamente dos arquivos montados, tornando-o acessível como um banco de dados temporário na instância de destino do SQL Server.
- Enquanto o banco de dados temporário estiver em uso, o Veeam Explorer **redireciona as consultas dos usuários** para esse banco de dados, garantindo que os usuários possam continuar acessando e trabalhando com os dados.
- Em segundo plano, a Veeam **executa uma restauração completa do banco de dados**, transferindo dados do banco de dados temporário para o local original do banco de dados.
- Após a restauração completa do banco de dados ser concluída, o Veeam Explorer **muda as consultas do usuário de volta para o banco de dados original** e remove o banco de dados temporário.

▼ Restaurar banco de dados SQL Server com o Veeam Explorer Instant Recovery

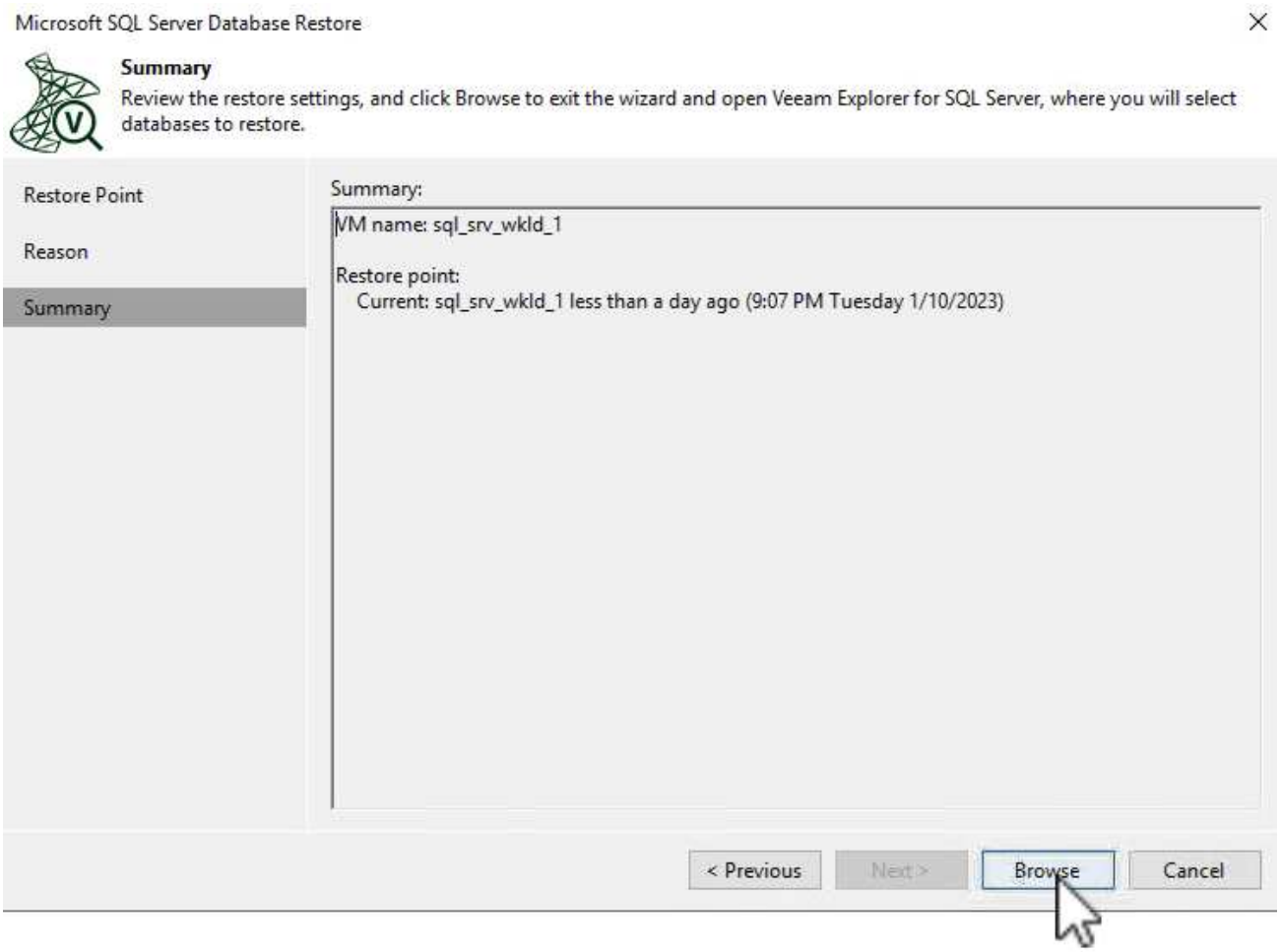
1. No console do Veeam Backup and Replication, navegue até a lista de backups do SQL Server, clique com o botão direito do mouse em um servidor e selecione **Restaurar itens do aplicativo** e depois **Bancos de dados do Microsoft SQL Server…**.



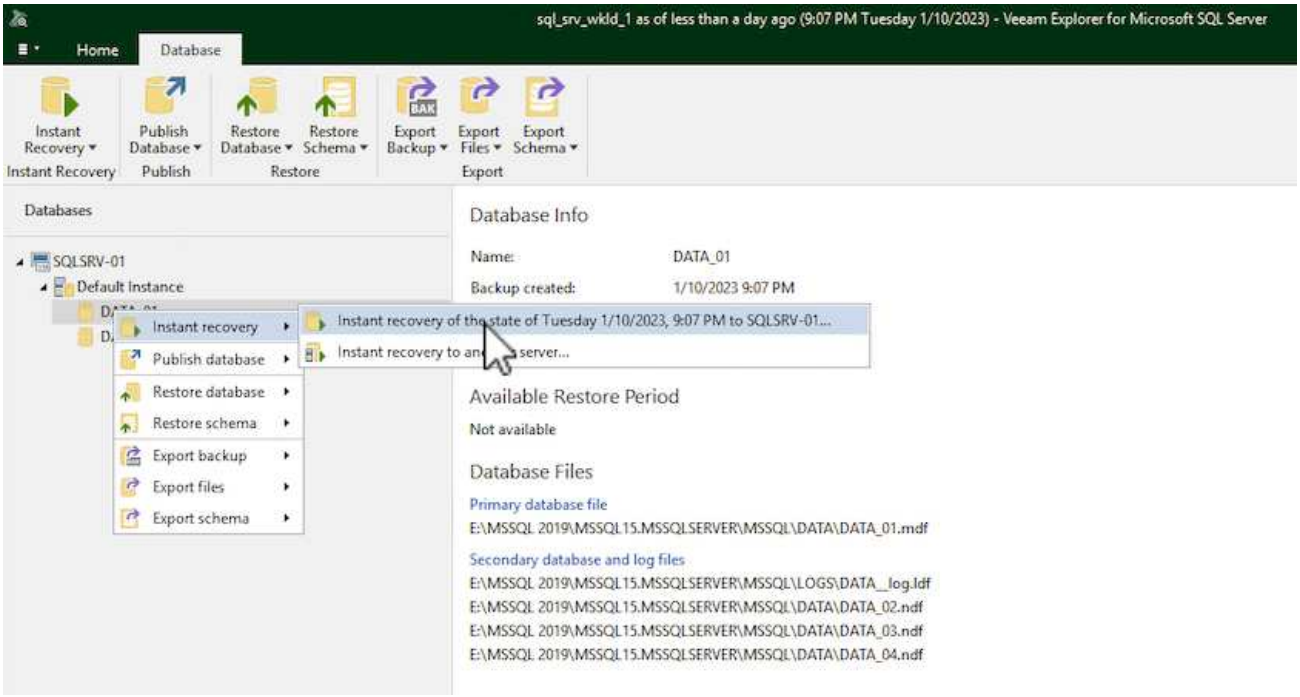
2. No Assistente de Restauração de Banco de Dados do Microsoft SQL Server, selecione um ponto de restauração na lista e clique em **Avançar**.



3. Insira um **Motivo da restauração**, se desejar, e então, na página Resumo, clique no botão **Procurar** para iniciar o Veeam Explorer para Microsoft SQL Server.

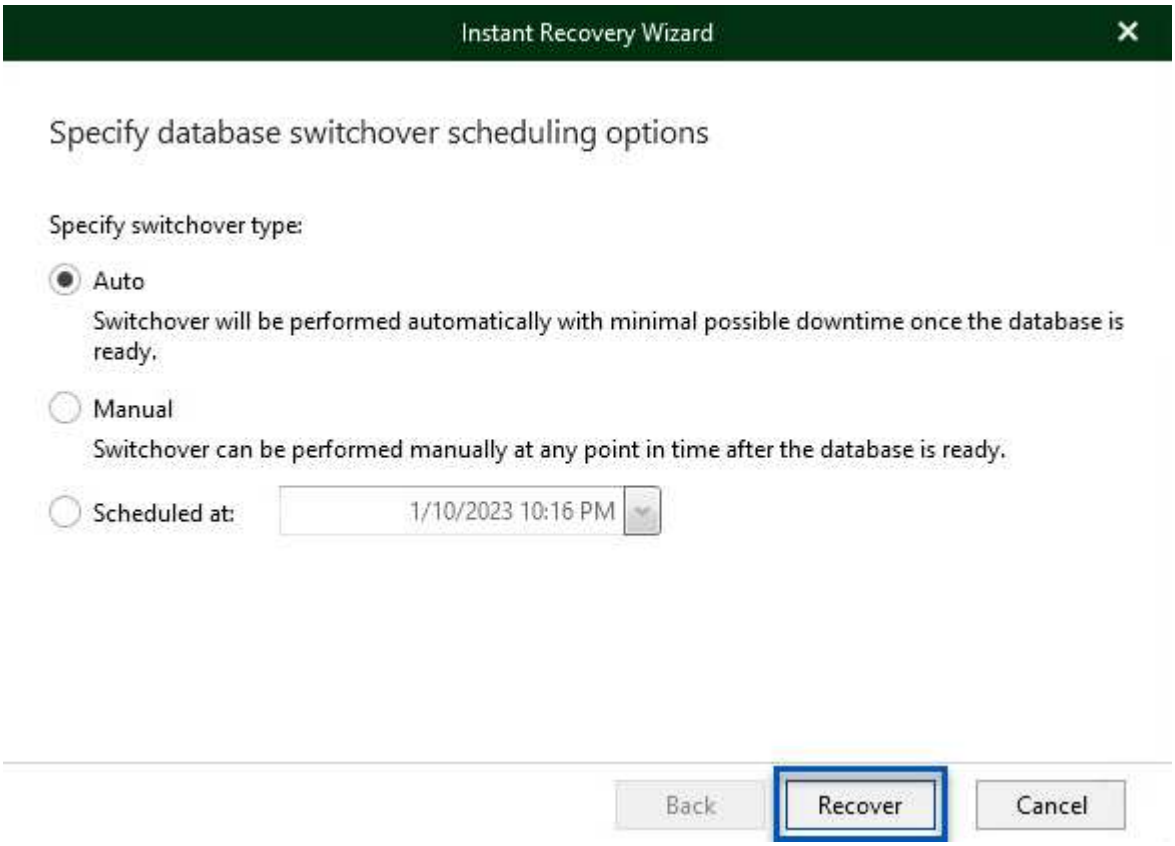


4. No Veeam Explorer, expanda a lista de instâncias de banco de dados, clique com o botão direito e selecione **Recuperação instantânea** e, em seguida, o ponto de restauração específico para recuperar.

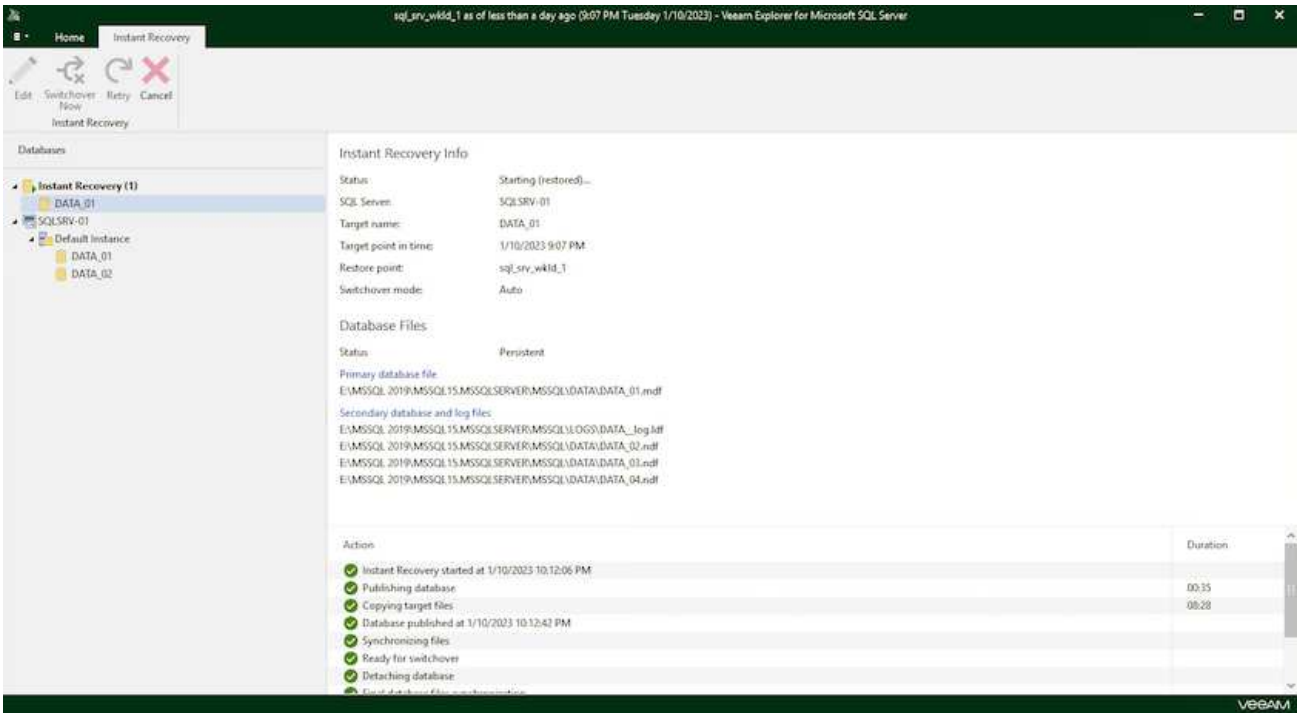


5. No Assistente de Recuperação Instantânea, especifique o tipo de alternância. Isso pode ser feito

automaticamente com tempo de inatividade mínimo, manualmente ou em um horário específico. Em seguida, clique no botão **Recuperar** para iniciar o processo de restauração.



6. O processo de recuperação pode ser monitorado pelo Veeam Explorer.



Para obter informações mais detalhadas sobre como executar operações de restauração do SQL Server com o Veeam Explorer, consulte a seção Microsoft SQL Server no "Guia do usuário do Veeam Explorers" .

Restaurar bancos de dados Oracle com o Veeam Explorer

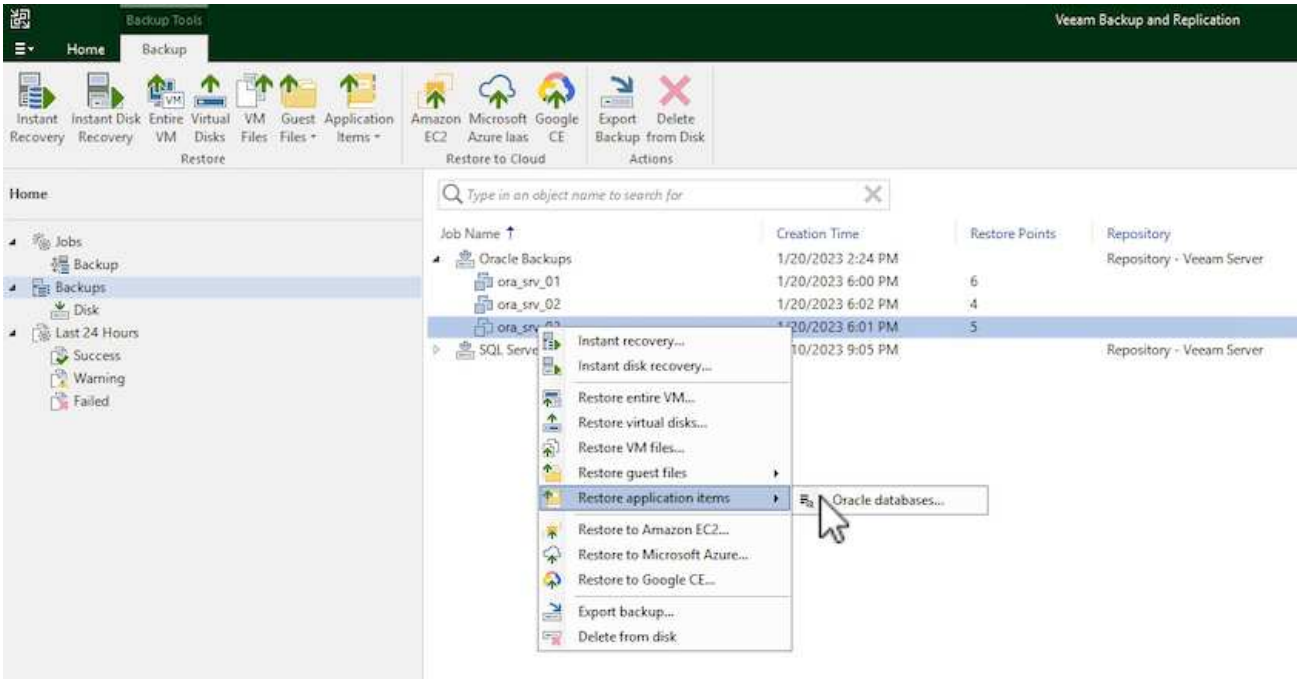
O Veeam Explorer para banco de dados Oracle oferece a capacidade de executar uma restauração padrão do banco de dados Oracle ou uma restauração ininterrupta usando a Recuperação Instantânea. Ele também oferece suporte à publicação de bancos de dados para acesso rápido, recuperação de bancos de dados do Data Guard e restaurações de backups RMAN.

Para obter informações mais detalhadas sobre como executar operações de restauração de banco de dados Oracle com o Veeam Explorer, consulte a seção Oracle no "Guia do usuário do Veeam Explorers" .

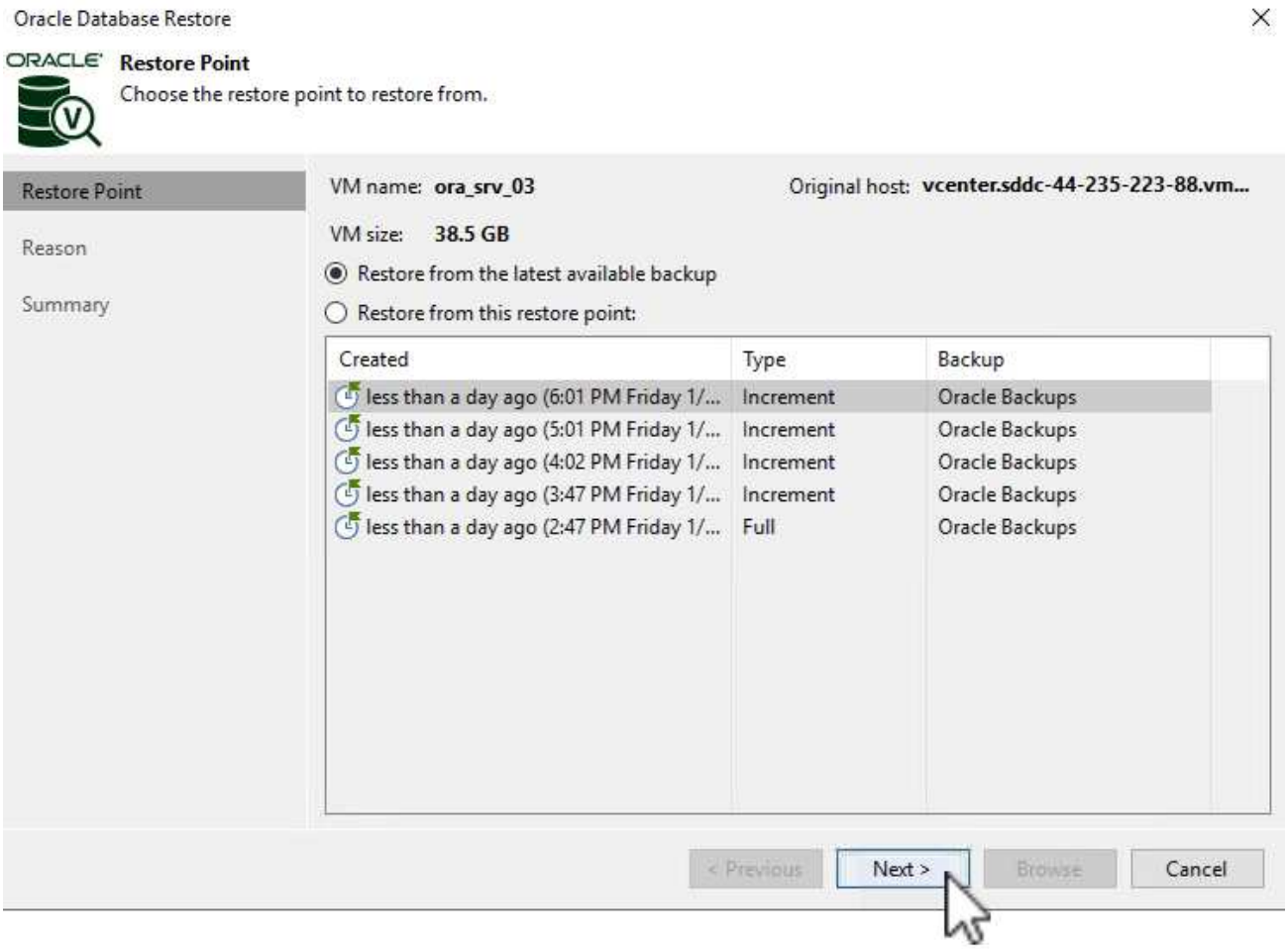
▼ **Restaurar banco de dados Oracle com o Veeam Explorer**

Nesta seção, uma restauração de banco de dados Oracle para um servidor diferente é abordada usando o Veeam Explorer.

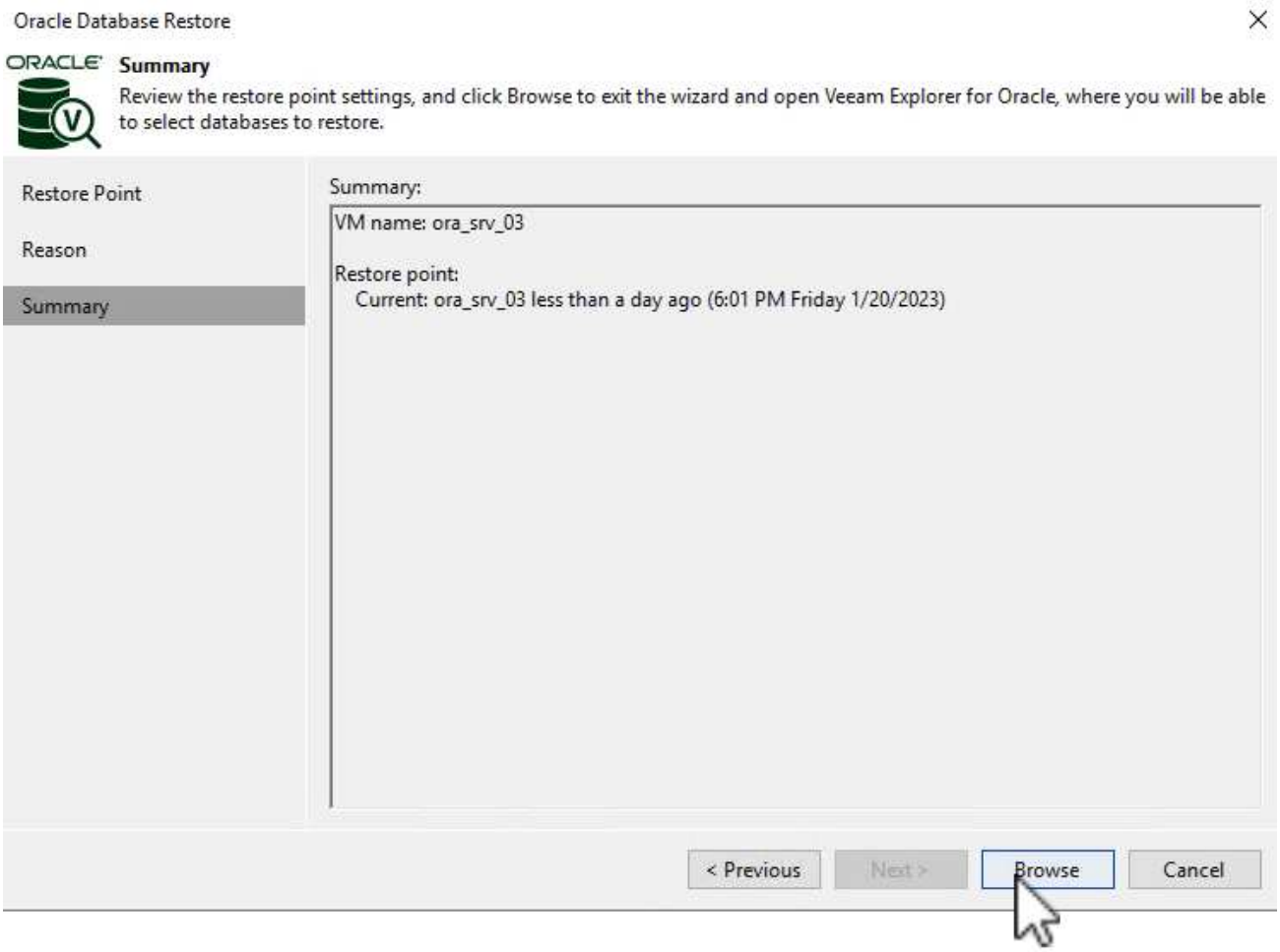
1. No console do Veeam Backup and Replication, navegue até a lista de backups do Oracle, clique com o botão direito do mouse em um servidor e selecione **Restaurar itens do aplicativo** e depois **Bancos de dados Oracle…**.



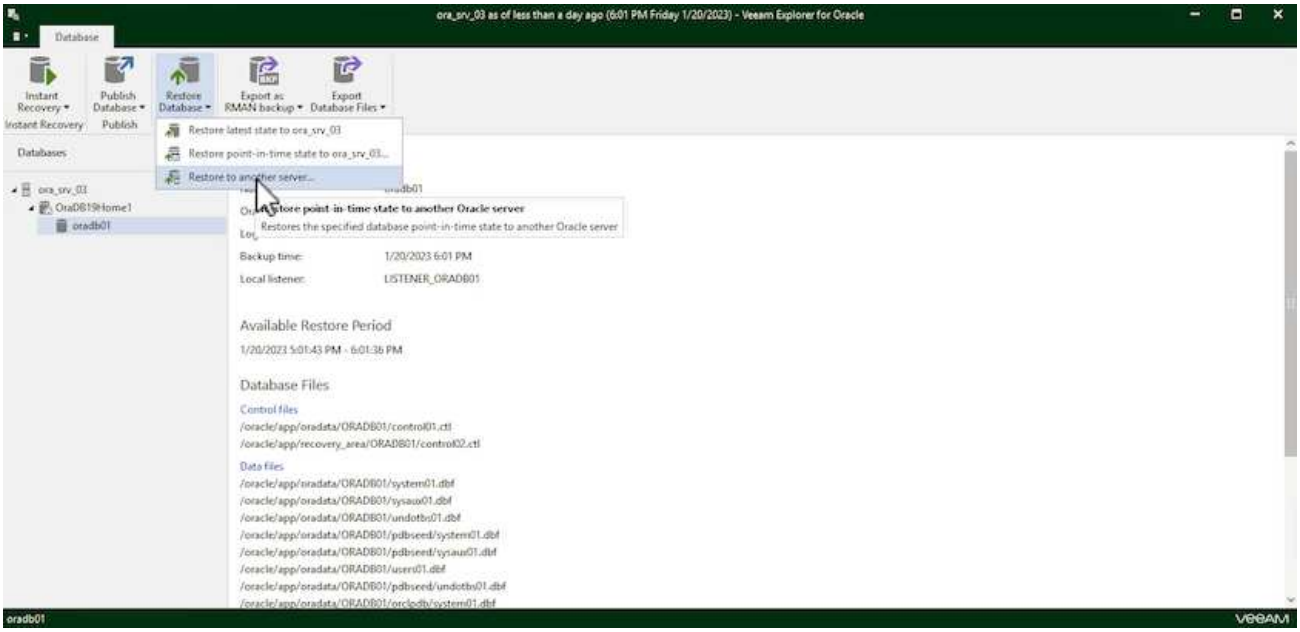
2. No Assistente de Restauração do Banco de Dados Oracle, selecione um ponto de restauração na lista e clique em **Avançar**.



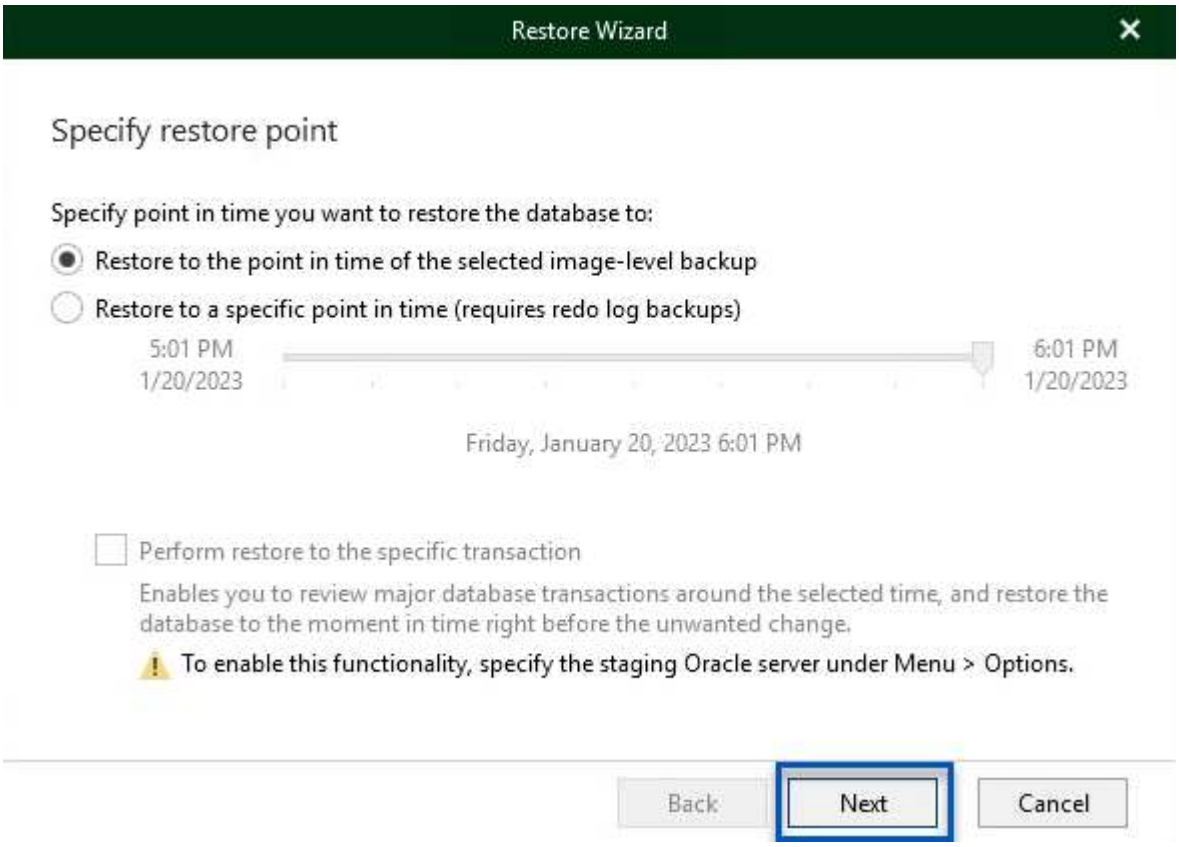
3. Insira um **Motivo da restauração**, se desejar, e então, na página Resumo, clique no botão **Procurar** para iniciar o Veeam Explorer para Oracle.



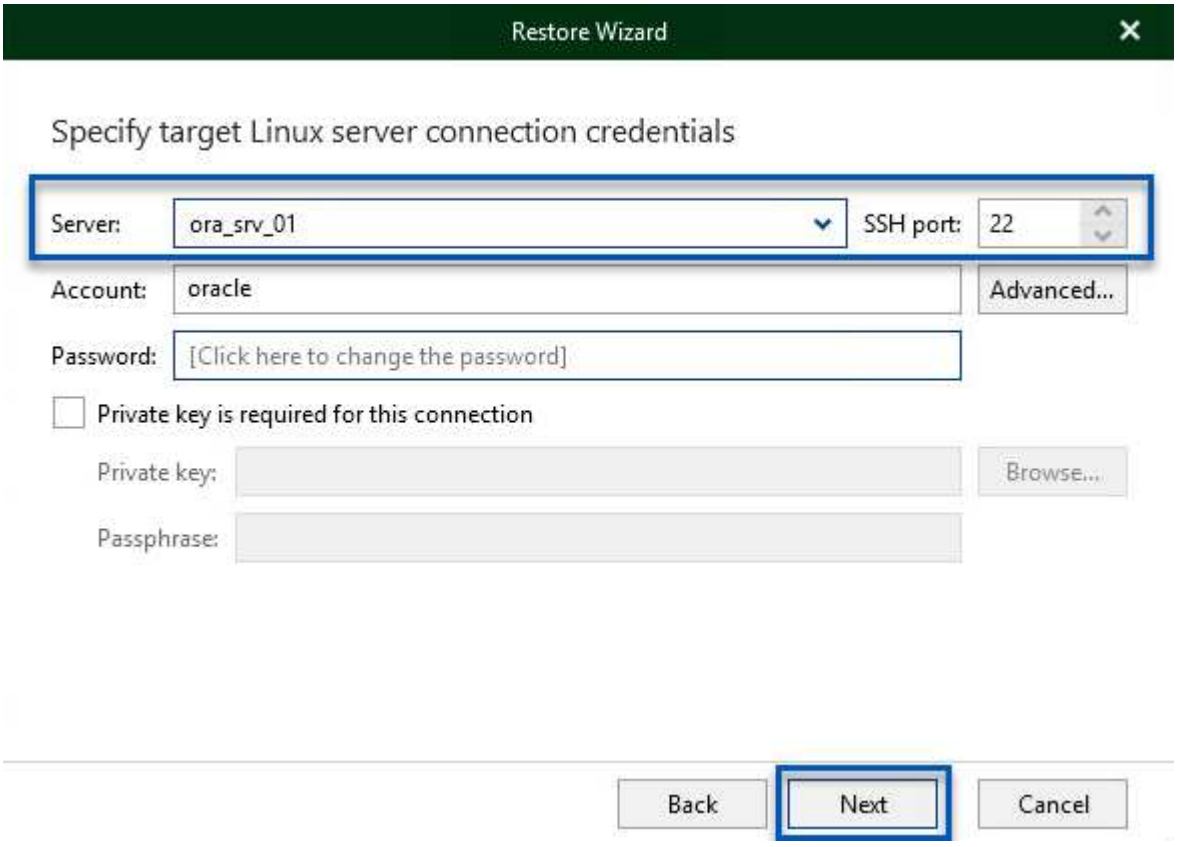
4. No Veeam Explorer, expanda a lista de instâncias de banco de dados, clique no banco de dados a ser restaurado e, no menu suspenso **Restaurar banco de dados** na parte superior, selecione **Restaurar para outro servidor…**.



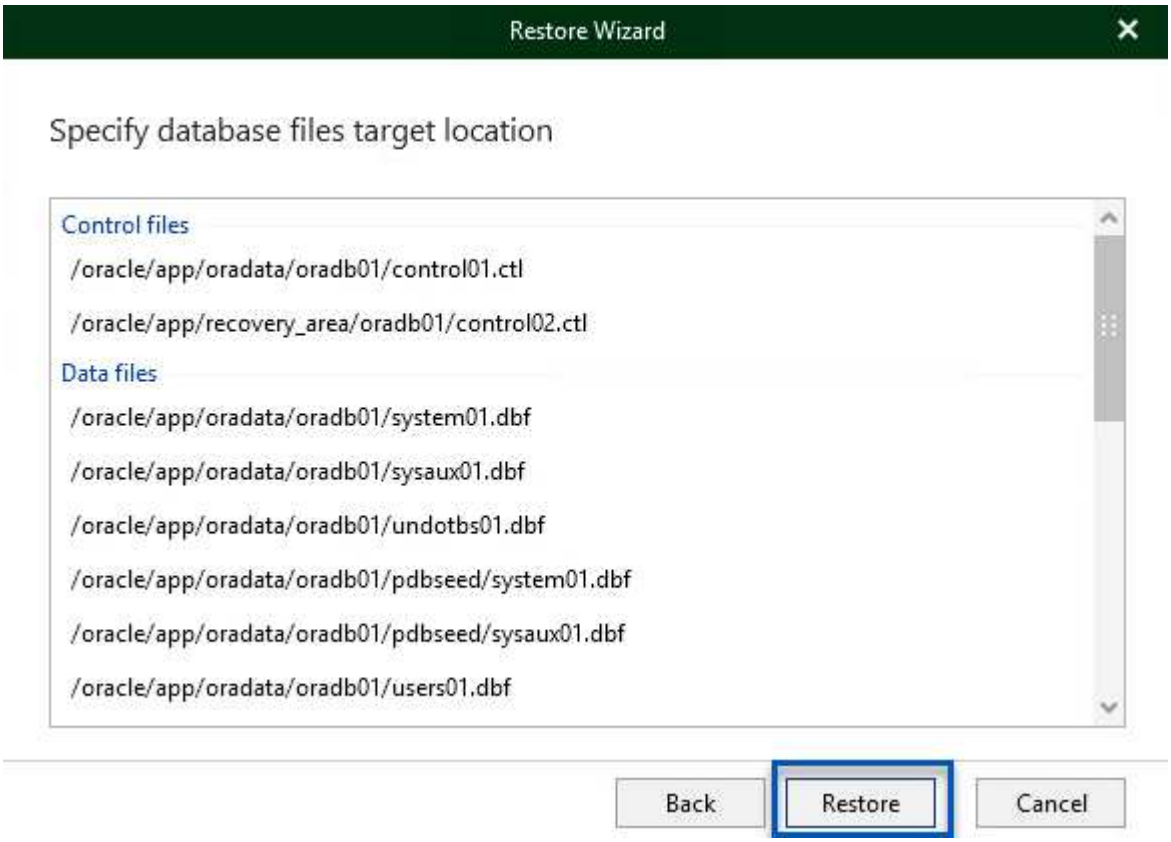
5. No Assistente de Restauração, especifique o ponto de restauração a ser restaurado e clique em **Avançar**.



6. Especifique o servidor de destino para o qual o banco de dados será restaurado, as credenciais da conta e clique em **Avançar**.



7. Por fim, especifique o local de destino dos arquivos do banco de dados e clique no botão **Restaurar** para iniciar o processo de restauração.

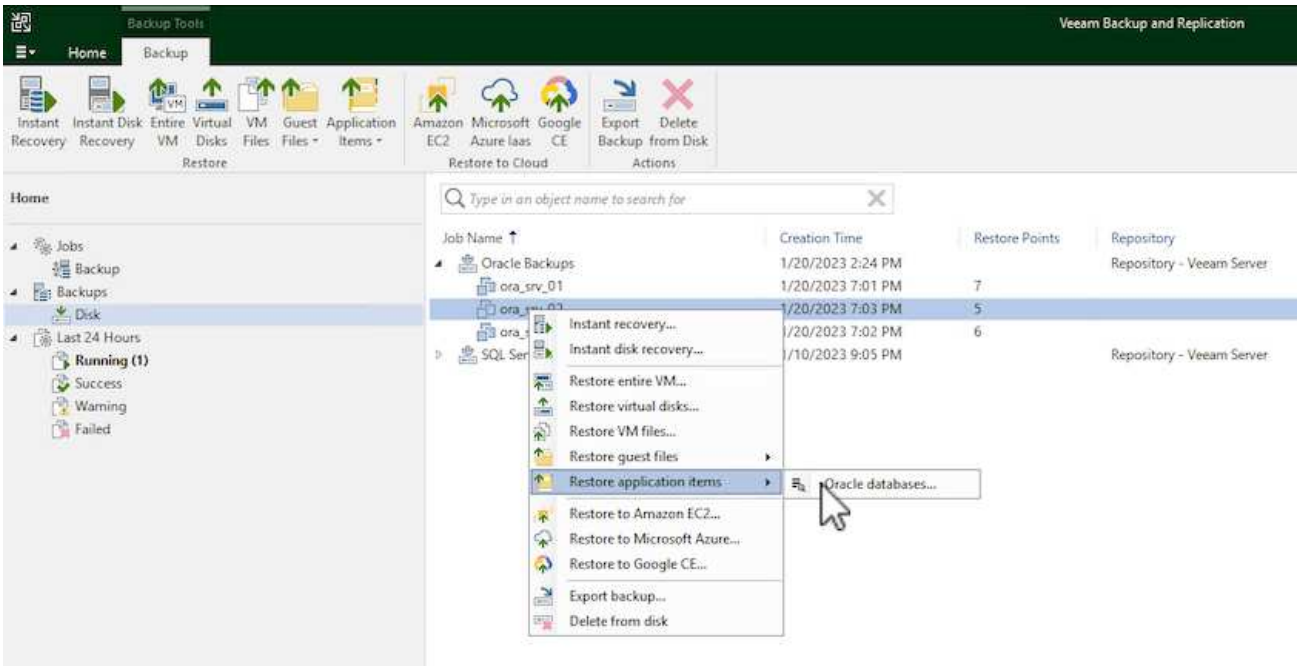


8. Após a conclusão da recuperação do banco de dados, verifique se o banco de dados Oracle inicia corretamente no servidor.

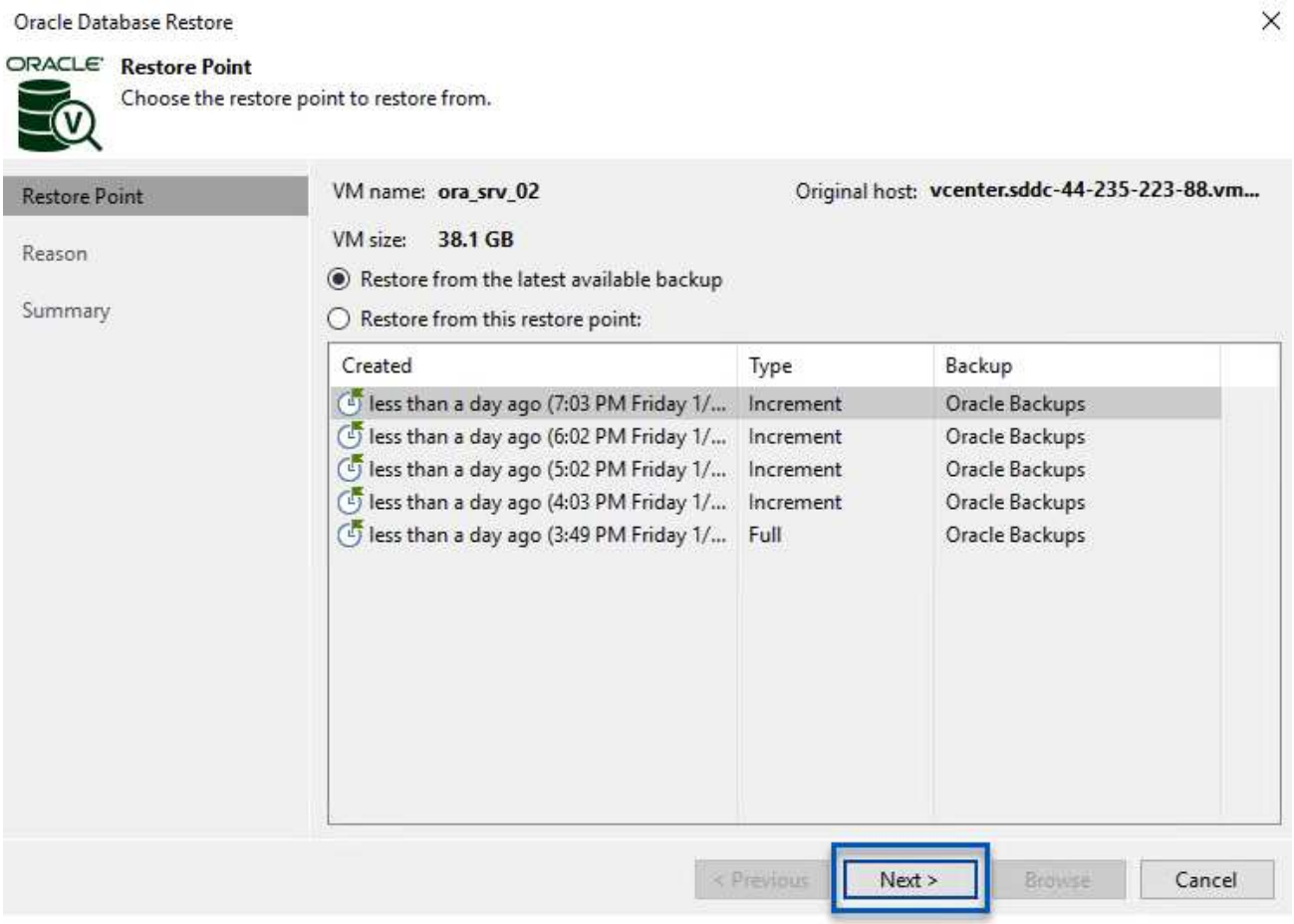
▼ **Publicar banco de dados Oracle em servidor alternativo**

Nesta seção, um banco de dados é publicado em um servidor alternativo para acesso rápido sem iniciar uma restauração completa.

1. No console do Veeam Backup and Replication, navegue até a lista de backups do Oracle, clique com o botão direito do mouse em um servidor e selecione **Restaurar itens do aplicativo** e depois **Bancos de dados Oracle…**.

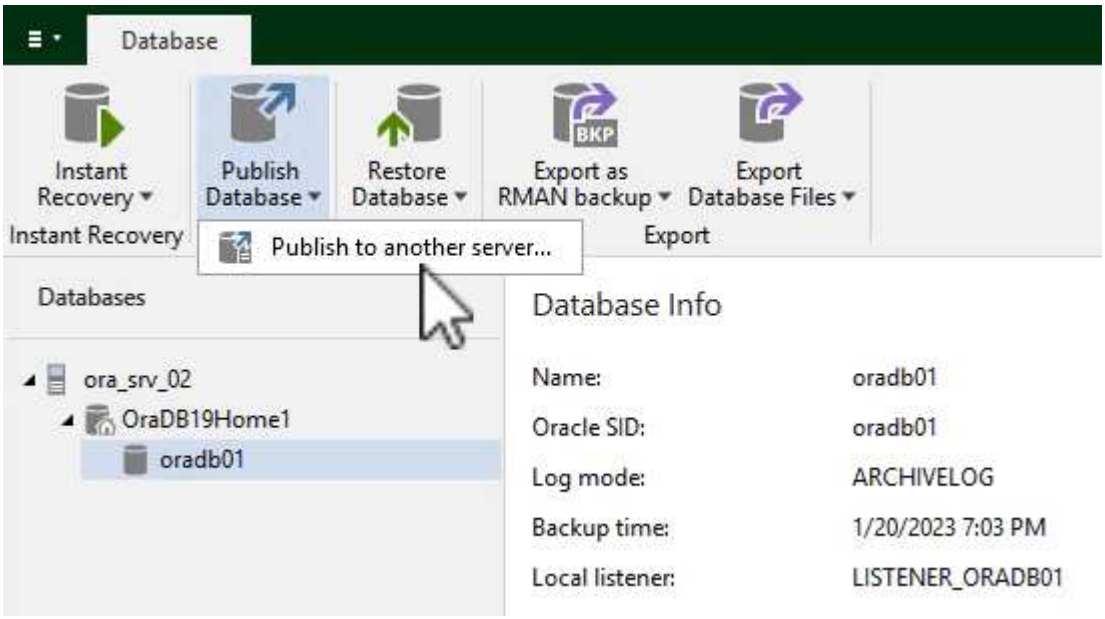


2. No Assistente de Restauração do Banco de Dados Oracle, selecione um ponto de restauração na lista e clique em **Avançar**.

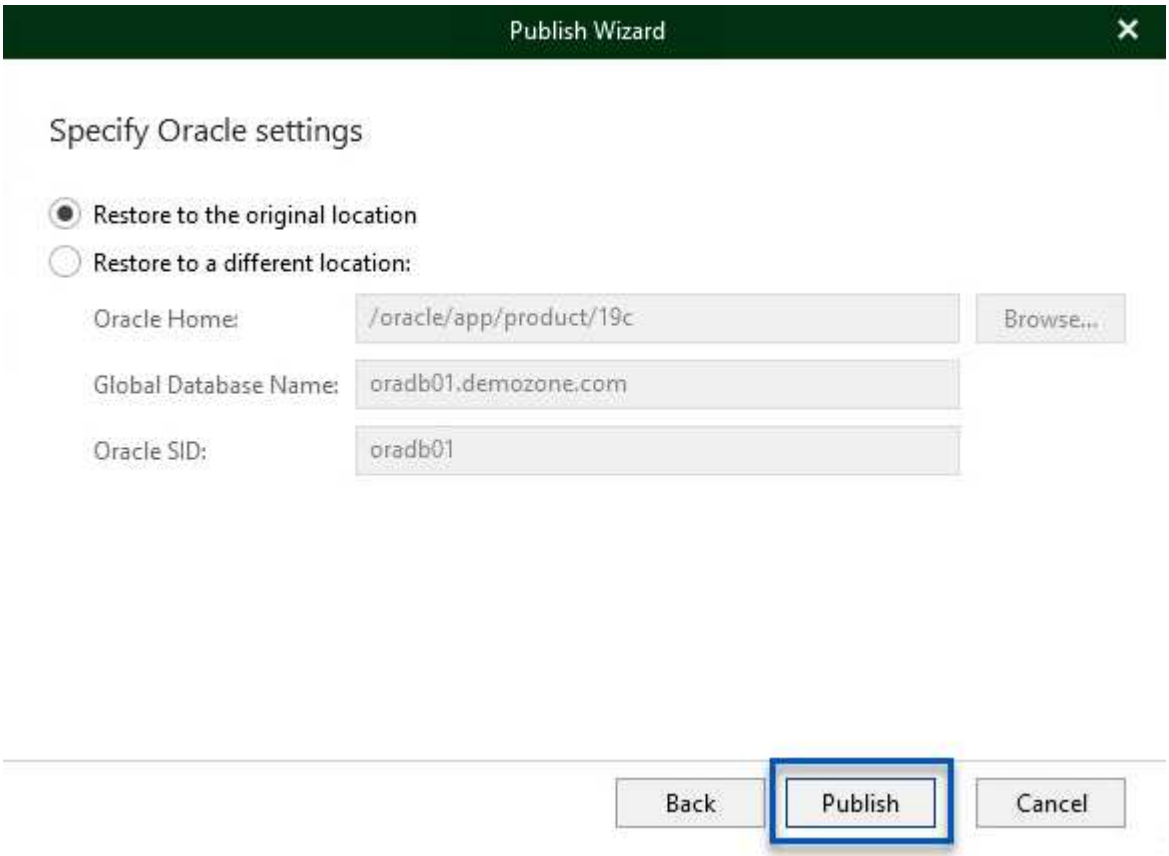


3. Insira um **Motivo da restauração**, se desejar, e então, na página Resumo, clique no botão **Procurar** para iniciar o Veeam Explorer para Oracle.

4. No Veeam Explorer, expanda a lista de instâncias de banco de dados, clique no banco de dados a ser restaurado e, no menu suspenso **Publicar banco de dados** na parte superior, selecione **Publicar em outro servidor…**.



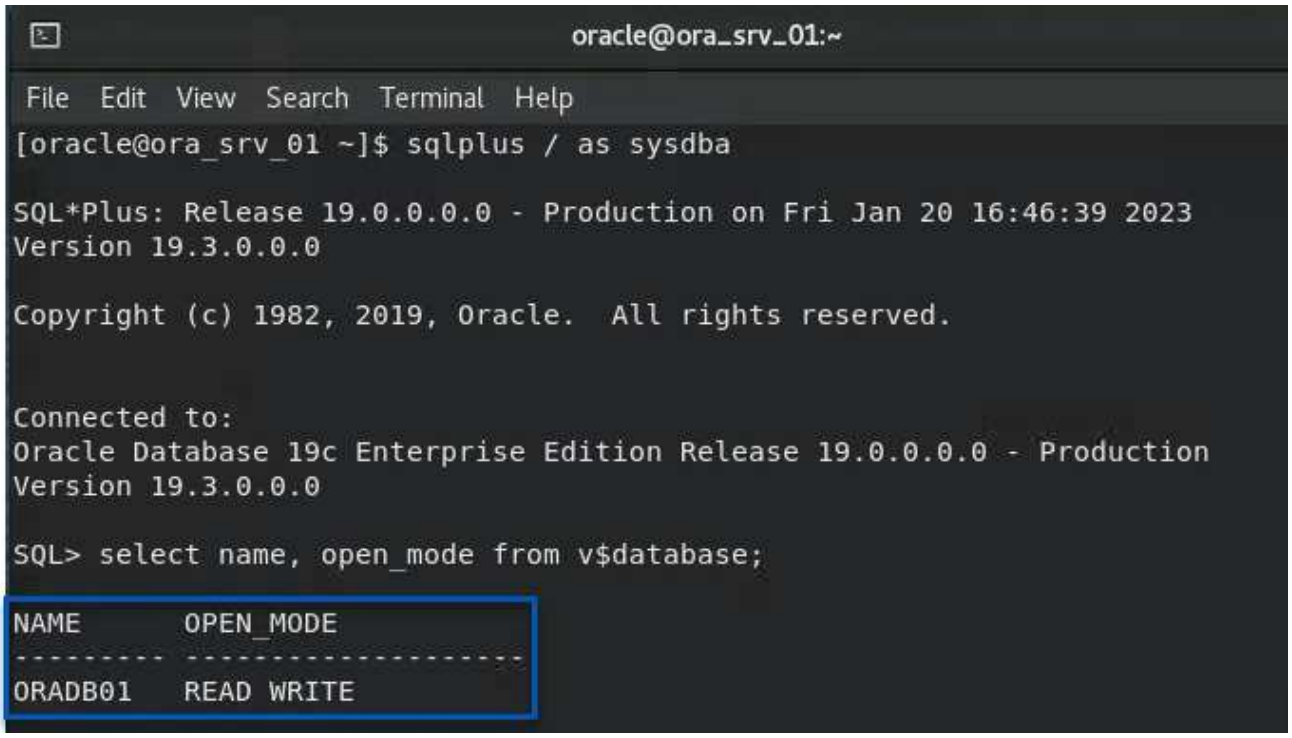
5. No assistente de publicação, especifique o ponto de restauração no qual o banco de dados será publicado e clique em **Avançar**.
6. Por fim, especifique o local do sistema de arquivos Linux de destino e clique em **Publicar** para iniciar o processo de restauração.



7. Após a conclusão da publicação, efetue login no servidor de destino e execute os seguintes comandos para garantir que o banco de dados esteja em execução:

```
oracle@ora_srv_01> sqlplus / as sysdba
```

```
SQL> select name, open_mode from v$database;
```



Conclusão

O VMware Cloud é uma plataforma poderosa para executar aplicativos essenciais aos negócios e armazenar dados confidenciais. Uma solução segura de proteção de dados é essencial para empresas que dependem do VMware Cloud para garantir a continuidade dos negócios e ajudar a proteger contra ameaças cibernéticas e perda de dados. Ao escolher uma solução de proteção de dados confiável e robusta, as empresas podem ter certeza de que seus dados críticos estarão seguros e protegidos, não importa o que aconteça.

O caso de uso apresentado nesta documentação se concentra em tecnologias comprovadas de proteção de dados que destacam a integração entre NetApp, VMware e Veeam. O FSx ONTAP é suportado como armazenamento de dados NFS suplementar para o VMware Cloud na AWS e é usado para todos os dados de aplicativos e máquinas virtuais. O Veeam Backup & Replication é uma solução abrangente de proteção de dados projetada para ajudar empresas a melhorar, automatizar e otimizar seus processos de backup e recuperação. O Veeam é usado em conjunto com volumes de destino de backup iSCSI, hospedados no FSx ONTAP, para fornecer uma solução de proteção de dados segura e fácil de gerenciar para dados de aplicativos que residem no VMware Cloud.

Informações adicionais

Para saber mais sobre as tecnologias apresentadas nesta solução, consulte as seguintes informações adicionais.

- "Guia do usuário do FSx ONTAP"
- "Documentação técnica da Central de Ajuda da Veeam"
- "Suporte do VMware Cloud na AWS. Considerações e Limitações"

TR-4955: Recuperação de desastres com FSx ONTAP e VMC (AWS VMware Cloud)

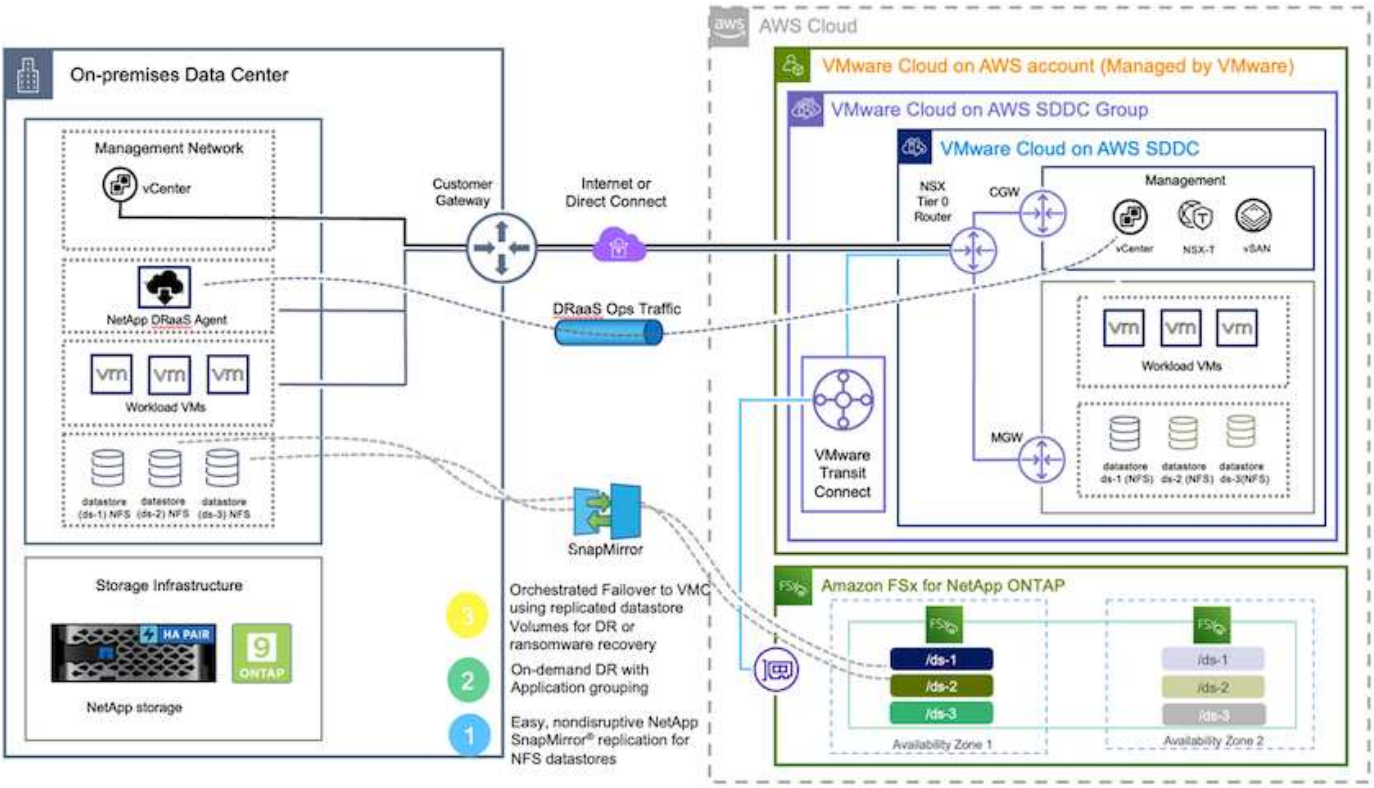
O Disaster Recovery Orchestrator (DRO; uma solução com script e interface de usuário) pode ser usado para recuperar facilmente cargas de trabalho replicadas do local para o FSx ONTAP. O DRO automatiza a recuperação do nível do SnapMirror , passando pelo registro da VM no VMC, até os mapeamentos de rede diretamente no NSX-T. Este recurso está incluído em todos os ambientes VMC.

Niyaz Mohamed, NetApp

Visão geral

A recuperação de desastres na nuvem é uma maneira resiliente e econômica de proteger as cargas de trabalho contra interrupções do site e eventos de corrupção de dados (por exemplo, ransomware). Com a tecnologia NetApp SnapMirror , as cargas de trabalho locais do VMware podem ser replicadas para o FSx ONTAP em execução na AWS.

O Disaster Recovery Orchestrator (DRO; uma solução com script e interface de usuário) pode ser usado para recuperar facilmente cargas de trabalho replicadas do local para o FSx ONTAP. O DRO automatiza a recuperação do nível do SnapMirror , passando pelo registro da VM no VMC, até os mapeamentos de rede diretamente no NSX-T. Este recurso está incluído em todos os ambientes VMC.



Implantar e configurar o VMware Cloud na AWS

"VMware Cloud na AWS"fornece uma experiência nativa em nuvem para cargas de trabalho baseadas em VMware no ecossistema da AWS. Cada VMware Software-Defined Data Center (SDDC) é executado em uma Amazon Virtual Private Cloud (VPC) e fornece uma pilha VMware completa (incluindo o vCenter Server), rede definida por software NSX-T, armazenamento definido por software vSAN e um ou mais hosts ESXi que fornecem recursos de computação e armazenamento para as cargas de trabalho. Para configurar um ambiente VMC na AWS, siga as etapas neste"link" . Um conjunto de luz piloto também pode ser usado para fins de DR.

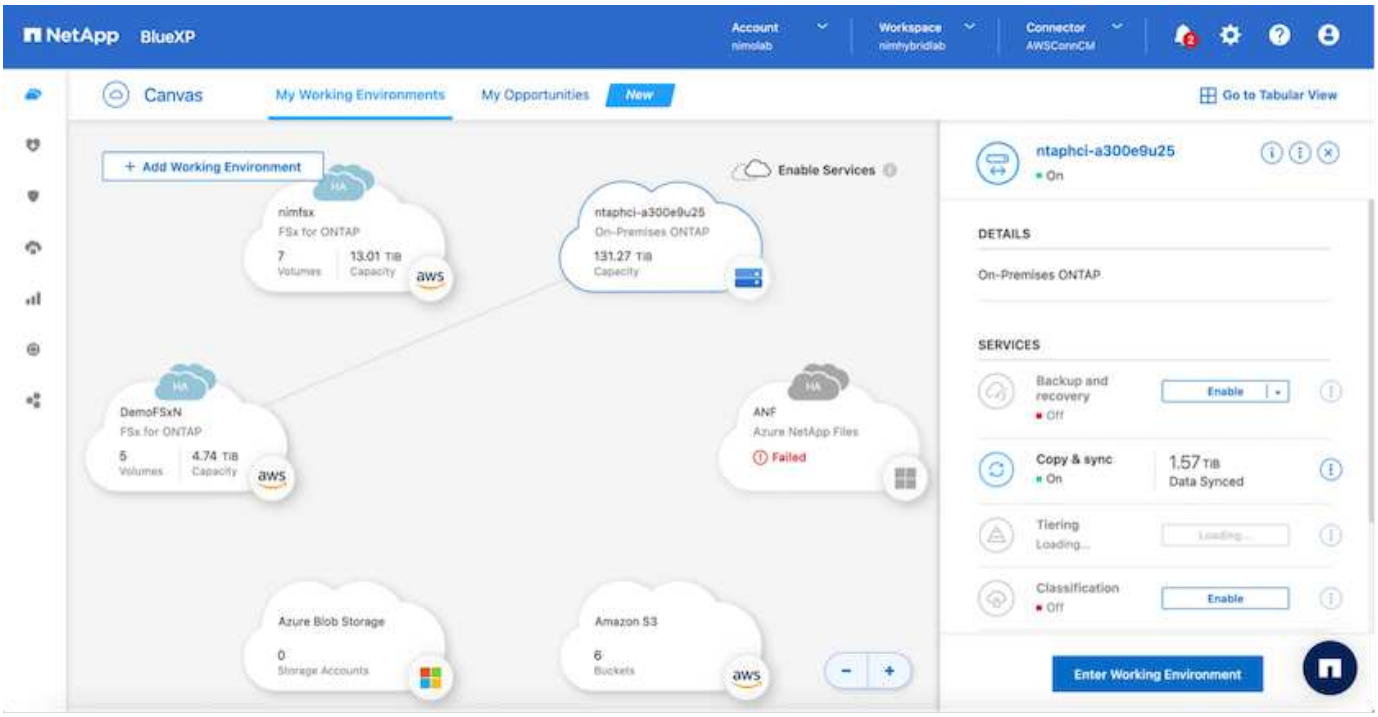
Na versão inicial, o DRO dá suporte a um cluster piloto existente. A criação de SDDC sob demanda estará disponível em uma próxima versão.

Provisionar e configurar o FSx ONTAP

O Amazon FSx ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, criado no popular sistema de arquivos NetApp ONTAP . Siga os passos aqui"link" para provisionar e configurar o FSx ONTAP.

Implantar e configurar o SnapMirror no FSx ONTAP

O próximo passo é usar o NetApp Console e descobrir a instância do FSx ONTAP na AWS provisionada, além de replicar os volumes de datastore desejados de um ambiente local para o FSx ONTAP com a frequência apropriada e a retenção de cópias Snapshot do NetApp:



Siga os passos neste link para configurar o DRO. Você também pode usar a CLI do ONTAP da NetApp para agendar a replicação seguindo este link.

Um relacionamento SnapMirror é um pré-requisito e deve ser criado previamente.

Instalação DRO

Para começar a usar o DRO, use o sistema operacional Ubuntu em uma instância EC2 ou máquina virtual designada para garantir que você atenda aos pré-requisitos. Em seguida, instale o pacote.

Pré-requisitos

- Certifique-se de que haja conectividade com os sistemas de armazenamento e vCenter de origem e destino.
- A resolução de DNS deve estar em vigor se você estiver usando nomes DNS. Caso contrário, você deve usar endereços IP para os sistemas vCenter e de armazenamento.
- Crie um usuário com permissões de root. Você também pode usar sudo com uma instância EC2.

Requisitos do OS

- Ubuntu 20.04 (LTS) com mínimo de 2 GB e 4 vCPUs
- Os seguintes pacotes devem ser instalados na VM do agente designado:
  - Docker
  - Docker-compose
  - Jq

Alterar permissões em `docker.sock` : `sudo chmod 666 /var/run/docker.sock` .

O `deploy.sh` O script executa todos os pré-requisitos necessários.

Instalar o pacote

1. Baixe o pacote de instalação na máquina virtual designada:

```
git clone https://github.com/NetApp/DRO-AWS.git
```

   O agente pode ser instalado no local ou em uma VPC da AWS.

2. Descompacte o pacote, execute o script de implantação e insira o IP do host (por exemplo, 10.10.10.10).

```
tar xvf DRO-prereq.tar
```

3. Navegue até o diretório e execute o script de implantação da seguinte maneira:

```
sudo sh deploy.sh
```

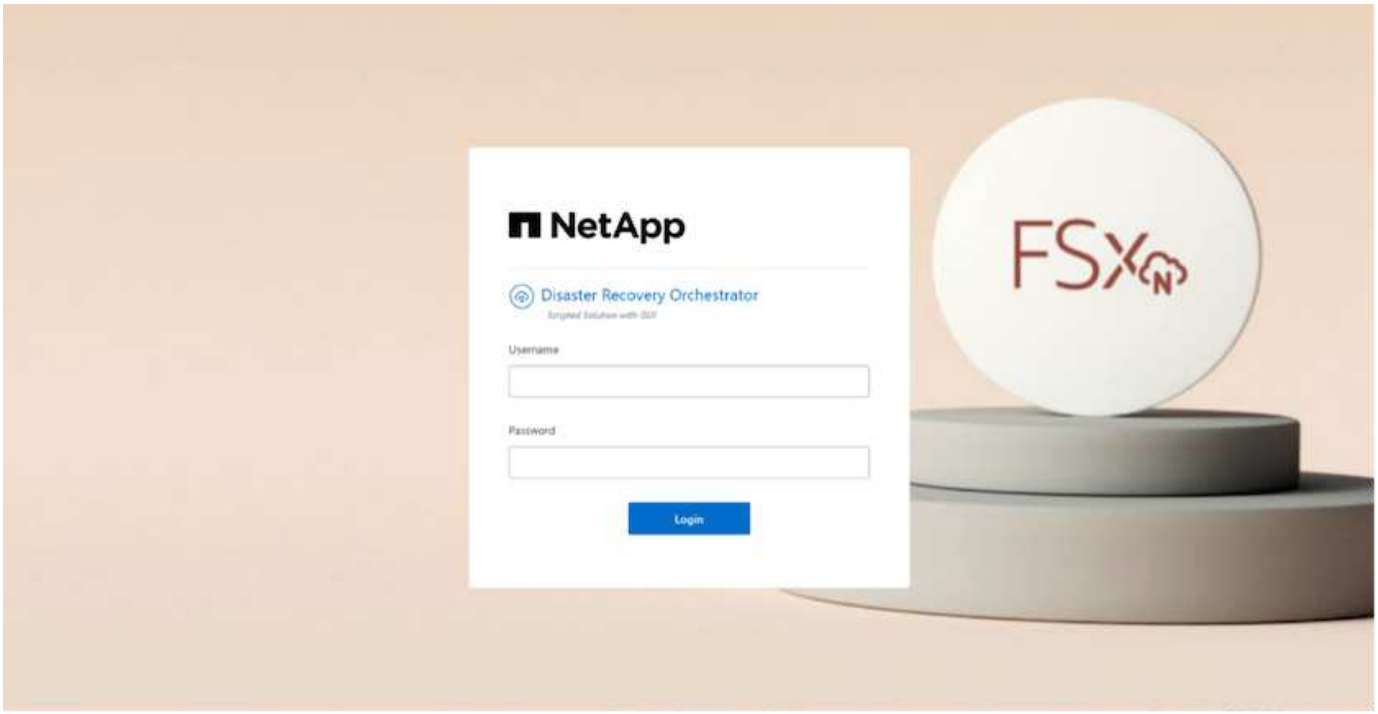
4. Acesse a interface do usuário usando:

```
https://<host-ip-address>
```

com as seguintes credenciais padrão:

```
Username: admin
Password: admin
```

A senha pode ser alterada usando a opção "Alterar senha".



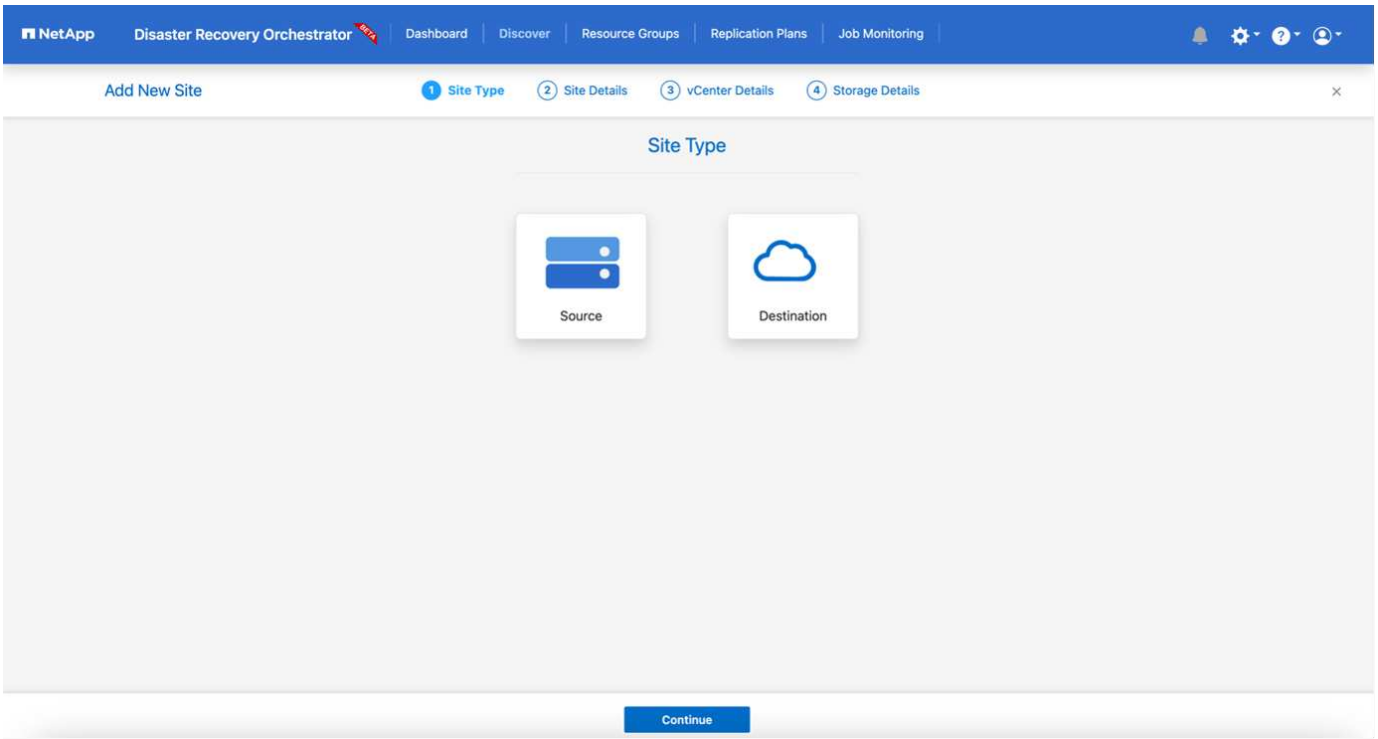
Configuração DRO

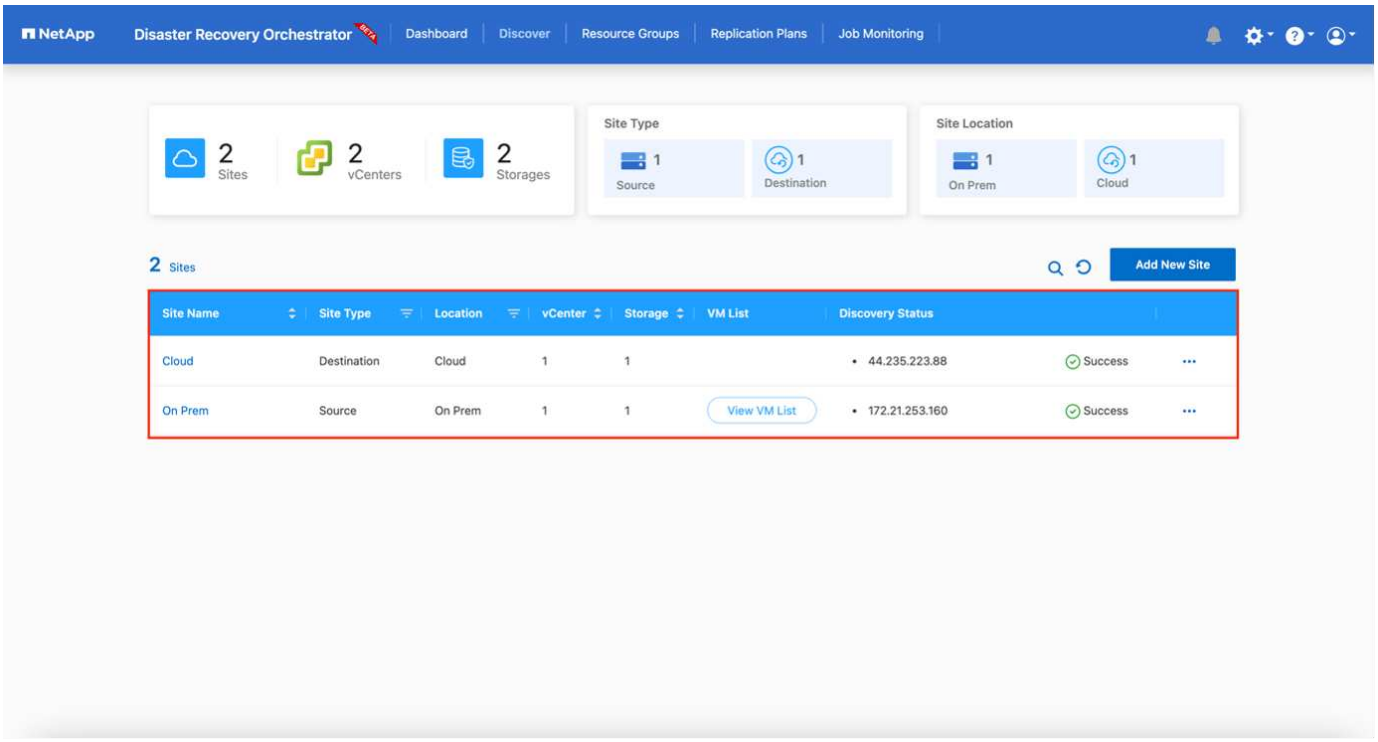
Depois que o FSx ONTAP e o VMC forem configurados corretamente, você poderá começar a configurar o DRO para automatizar a recuperação de cargas de trabalho locais para o VMC usando cópias somente leitura do SnapMirror no FSx ONTAP.

A NetApp recomenda implantar o agente DRO na AWS e também na mesma VPC onde o FSx ONTAP está implantado (ele também pode ser conectado por pares), para que o agente DRO possa se comunicar pela rede com seus componentes locais, bem como com os recursos do FSx ONTAP e VMC.

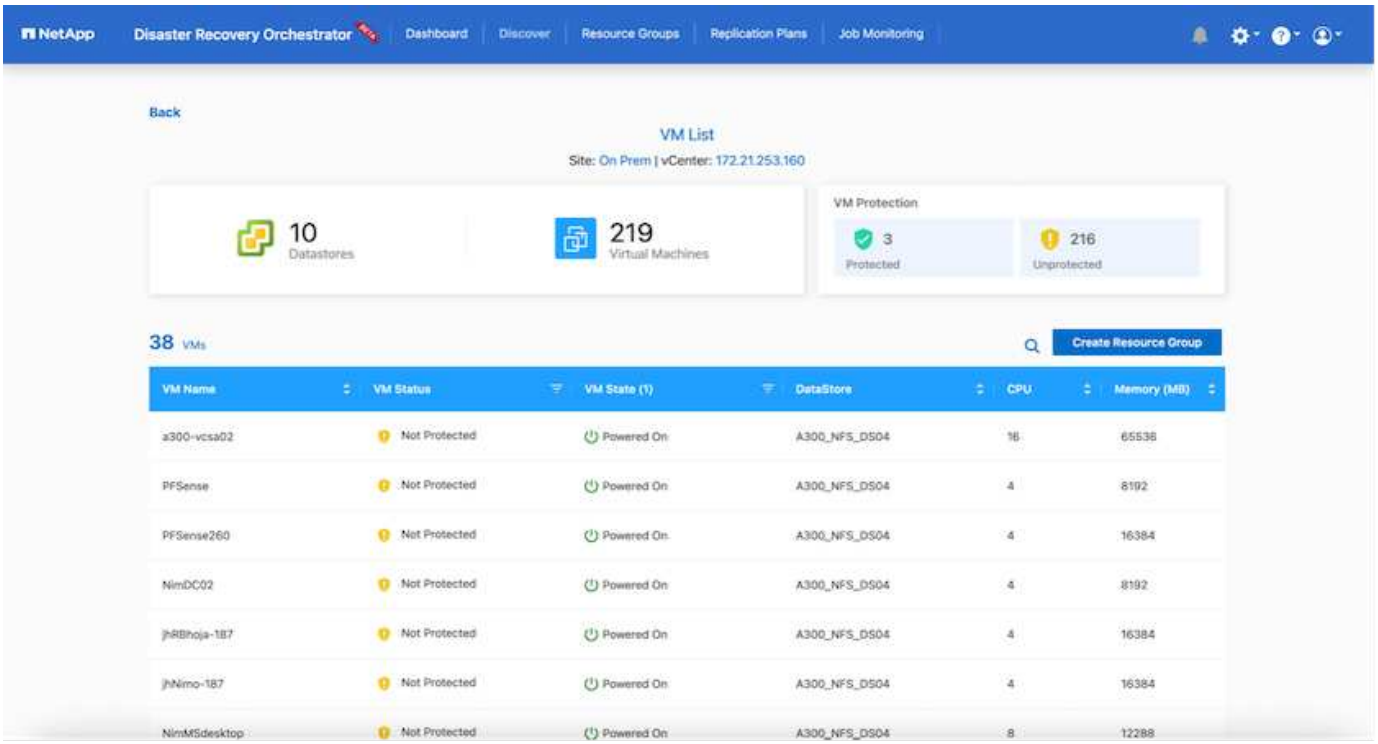
O primeiro passo é descobrir e adicionar os recursos locais e na nuvem (vCenter e armazenamento) ao DRO. Abra o DRO em um navegador compatível e use o nome de usuário e a senha padrão (admin/admin) e adicione sites. Os sites também podem ser adicionados usando a opção Descobrir. Adicione as seguintes plataformas:

- No local
  - vCenter local
  - Sistema de armazenamento ONTAP
- Nuvem
  - VMC vCenter
  - FSx ONTAP





Uma vez adicionado, o DRO executa a descoberta automática e exibe as VMs que têm réplicas SnapMirror correspondentes do armazenamento de origem para o FSx ONTAP. O DRO detecta automaticamente as redes e grupos de portas usados pelas VMs e os preenche.



A próxima etapa é agrupar as VMs necessárias em grupos funcionais para servir como grupos de recursos.

Agrupamentos de recursos

Depois que as plataformas forem adicionadas, você pode agrupar as VMs que deseja recuperar em grupos de recursos. Os grupos de recursos de DRO permitem que você agrupe um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização, atrasos de inicialização e validações de aplicativos opcionais que podem ser executadas na recuperação.

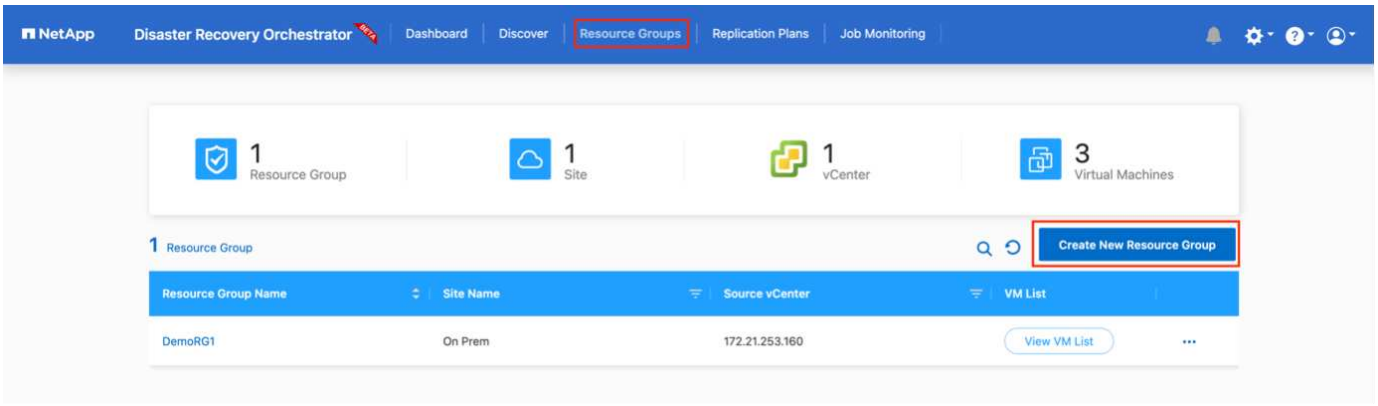
Para começar a criar grupos de recursos, conclua as seguintes etapas:

1. Acesse **Grupos de Recursos** e clique em **Criar Novo Grupo de Recursos**.
2. Em **Novo grupo de recursos**, selecione o site de origem no menu suspenso e clique em **Criar**.
3. Forneça **Detalhes do grupo de recursos** e clique em **Continuar**.
4. Selecione as VMs apropriadas usando a opção de pesquisa.
5. Selecione a ordem de inicialização e o atraso de inicialização (segs) para as VMs selecionadas. Defina a ordem da sequência de inicialização selecionando cada VM e definindo a prioridade para ela. Três é o valor padrão para todas as VMs.

   As opções são as seguintes:

   1 – A primeira máquina virtual a ligar 3 – Padrão 5 – A última máquina virtual a ligar

6. Clique em **Criar grupo de recursos**.

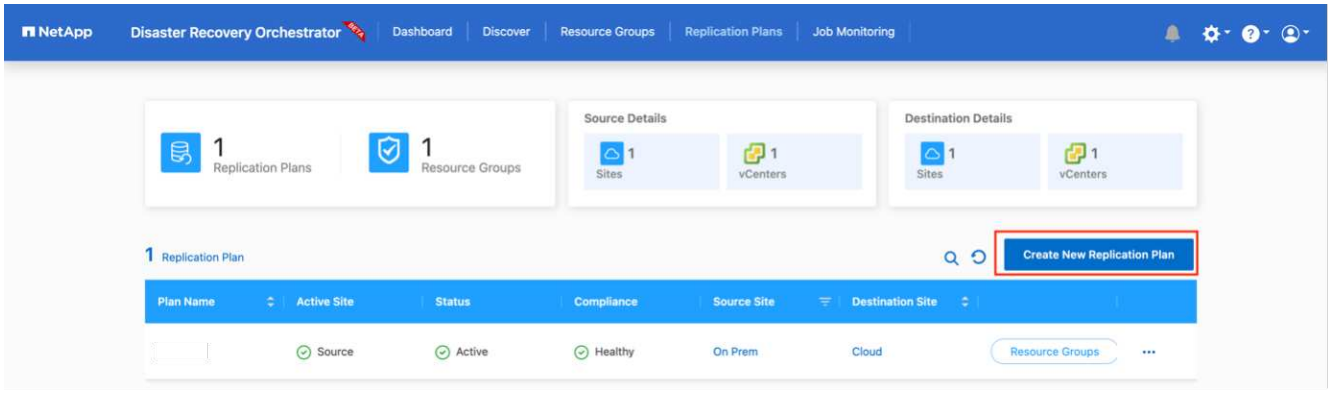


Planos de replicação

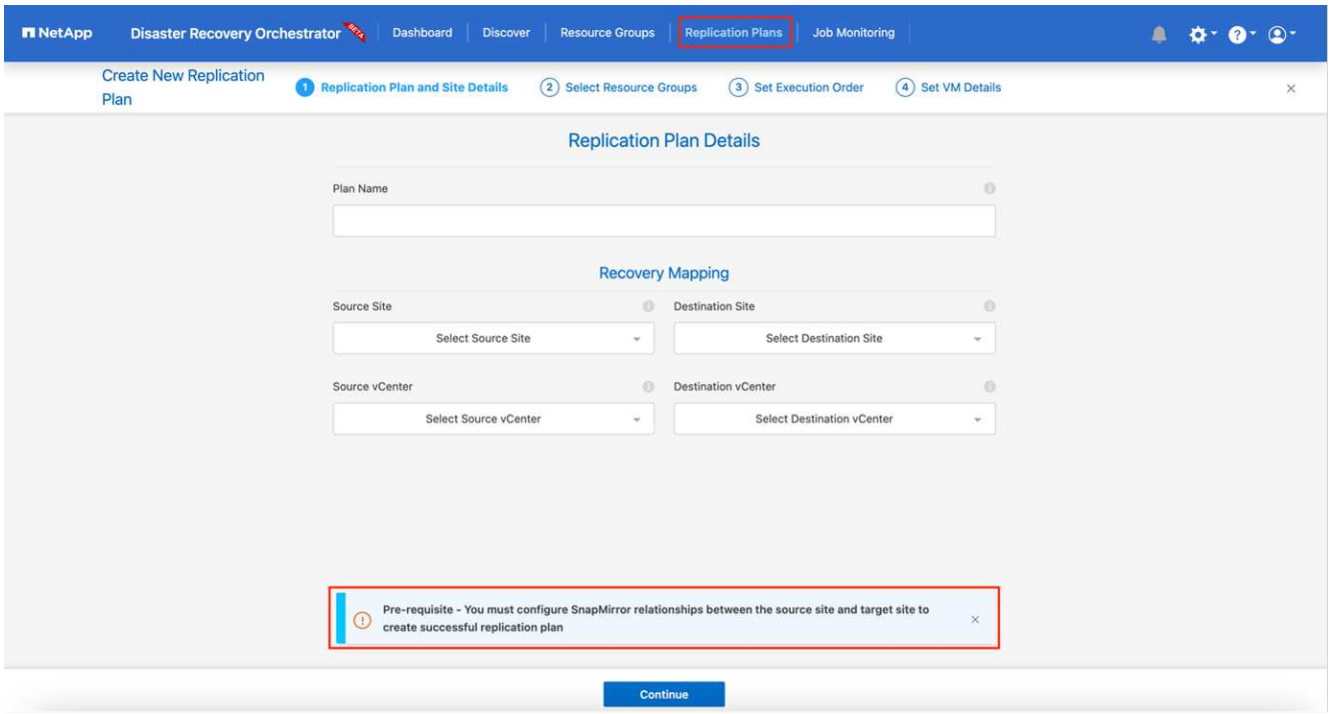
Você precisa de um plano para recuperar aplicativos em caso de desastre. Selecione as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos neste plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados (por exemplo, controladores de domínio, depois nível 1, depois nível 2 e assim por diante). Esses planos às vezes também são chamados de projetos. Para definir o plano de recuperação, navegue até a guia **Plano de Replicação** e clique em **Novo Plano de Replicação**.

Para começar a criar um plano de replicação, conclua as seguintes etapas:

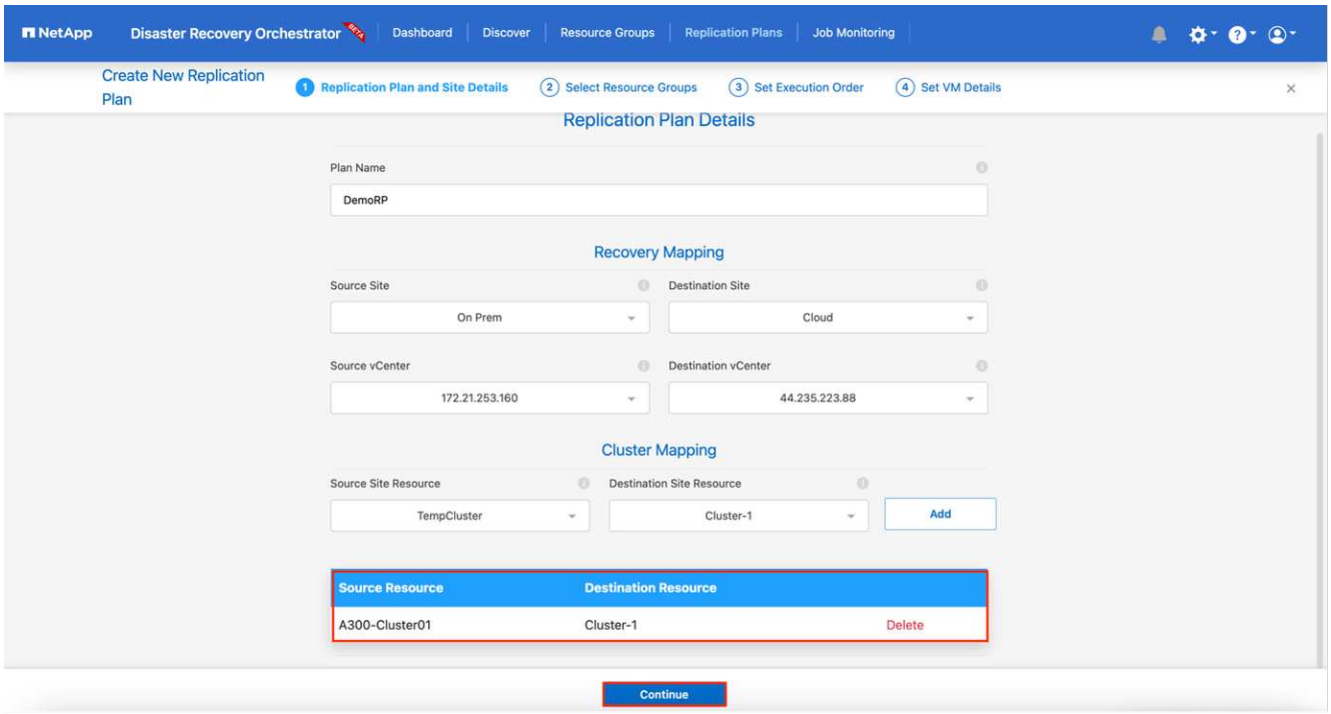
1. Acesse **Planos de Replicação** e clique em **Criar Novo Plano de Replicação**.



2. Em **Novo Plano de Replicação**, forneça um nome para o plano e adicione mapeamentos de recuperação selecionando o site de origem, o vCenter associado, o site de destino e o vCenter associado.

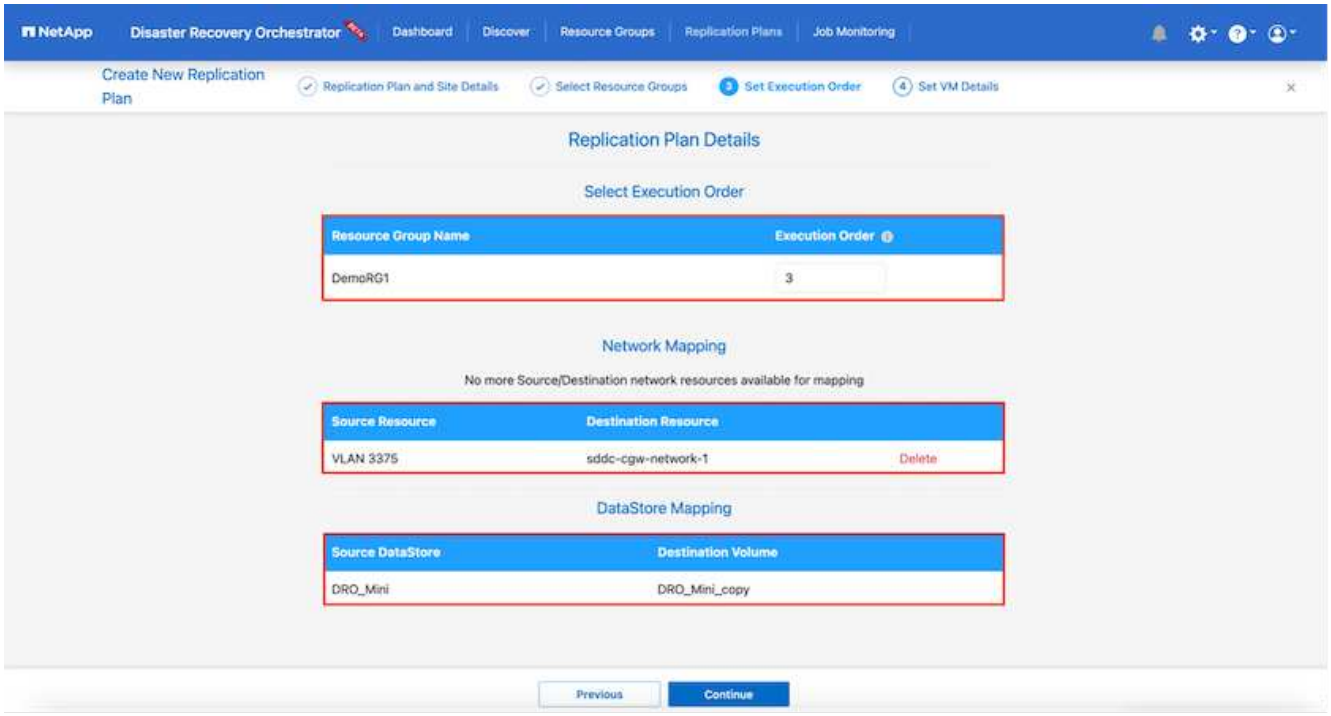


3. Após a conclusão do mapeamento de recuperação, selecione o mapeamento do cluster.

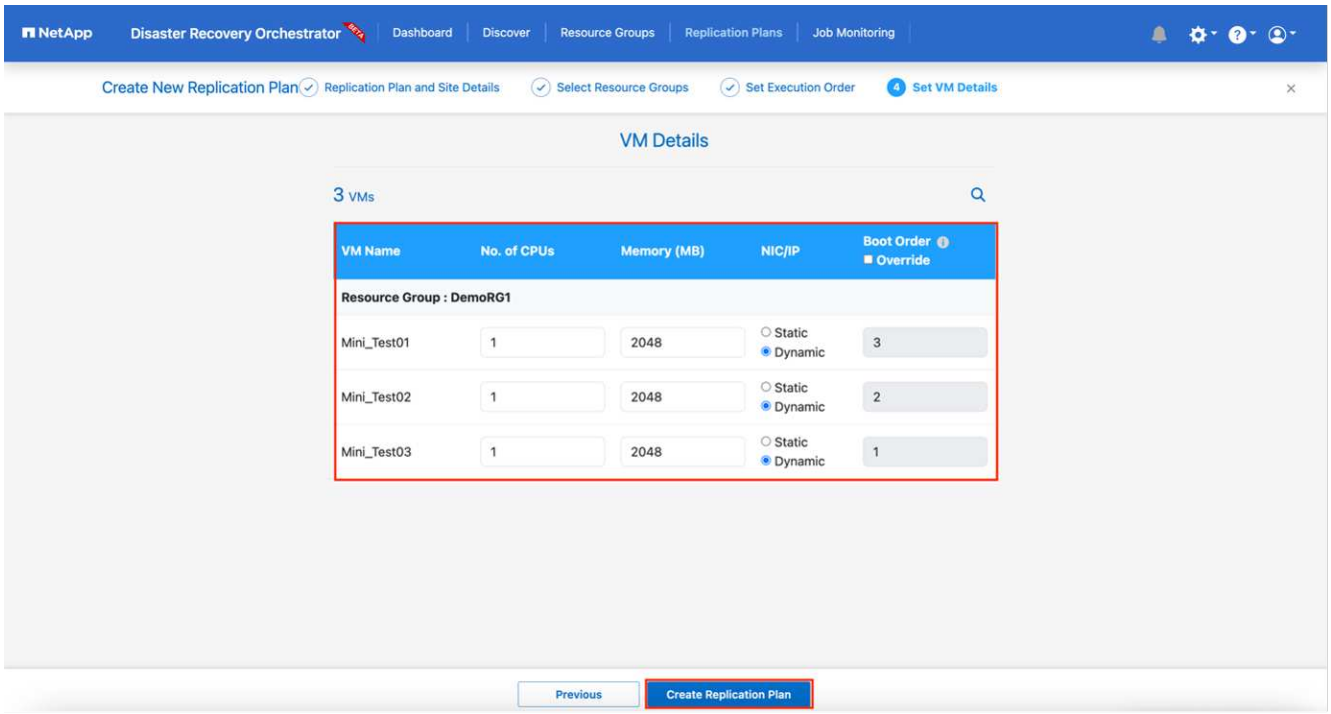


4. Selecione **Detalhes do grupo de recursos** e clique em **Continuar**.
5. Defina a ordem de execução para o grupo de recursos. Esta opção permite que você selecione a sequência de operações quando existem vários grupos de recursos.
6. Após terminar, selecione o mapeamento de rede para o segmento apropriado. Os segmentos já devem estar provisionados no VMC, então selecione o segmento apropriado para mapear a VM.
7. Com base na seleção de VMs, os mapeamentos de armazenamento de dados são selecionados automaticamente.

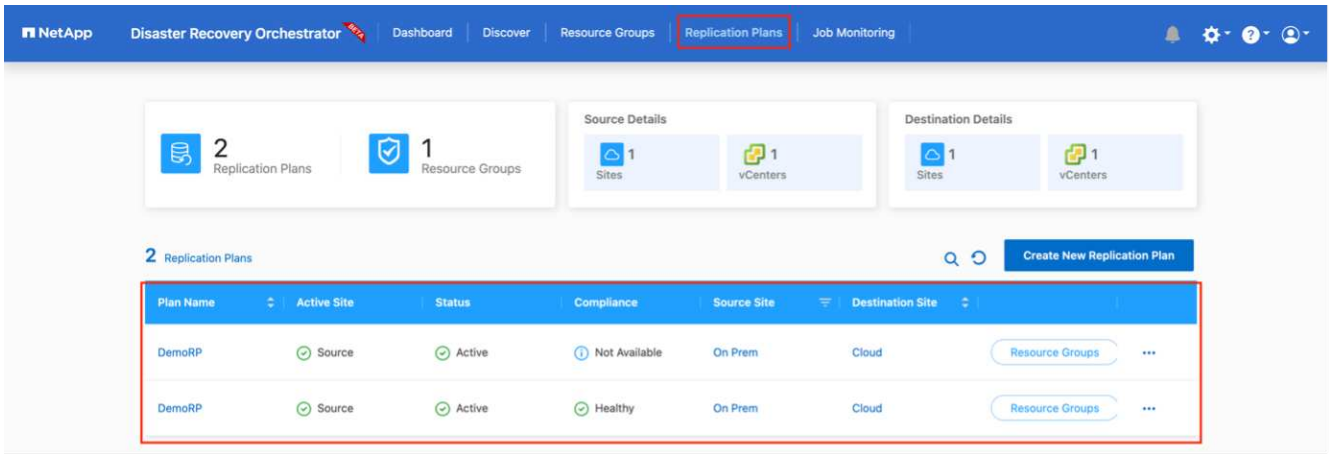
SnapMirror está no nível de volume. Portanto, todas as VMs são replicadas para o destino de replicação. Certifique-se de selecionar todas as VMs que fazem parte do armazenamento de dados. Se não forem selecionadas, somente as VMs que fazem parte do plano de replicação serão processadas.



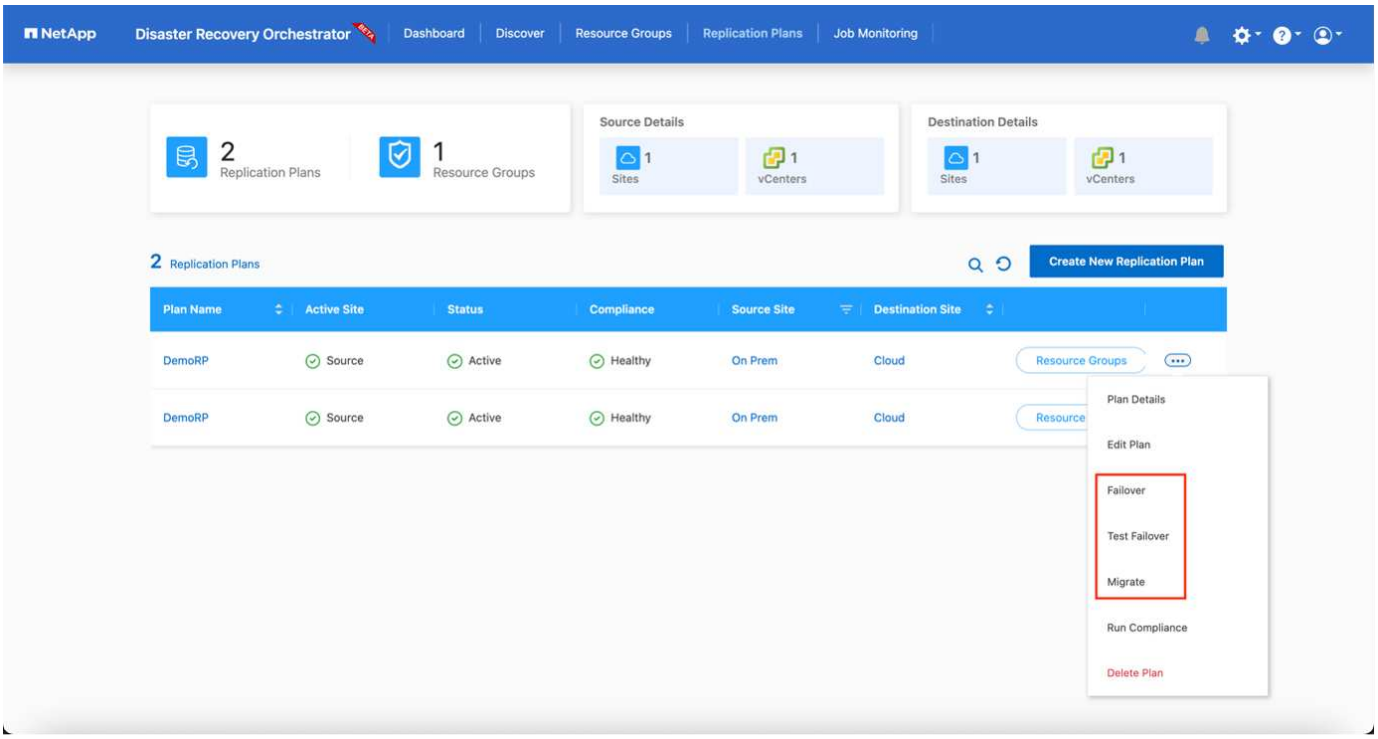
8. Nos detalhes da VM, você pode, opcionalmente, redimensionar os parâmetros de CPU e RAM da VM; isso pode ser muito útil ao recuperar ambientes grandes para clusters de destino menores ou para conduzir testes de DR sem precisar provisionar uma infraestrutura física VMware individual. Além disso, você pode modificar a ordem de inicialização e o atraso de inicialização (segundos) para todas as VMs selecionadas nos grupos de recursos. Há uma opção adicional para modificar a ordem de inicialização caso sejam necessárias alterações em relação às selecionadas durante a seleção da ordem de inicialização do grupo de recursos. Por padrão, a ordem de inicialização selecionada durante a seleção do grupo de recursos é usada; no entanto, qualquer modificação pode ser realizada nesta fase.

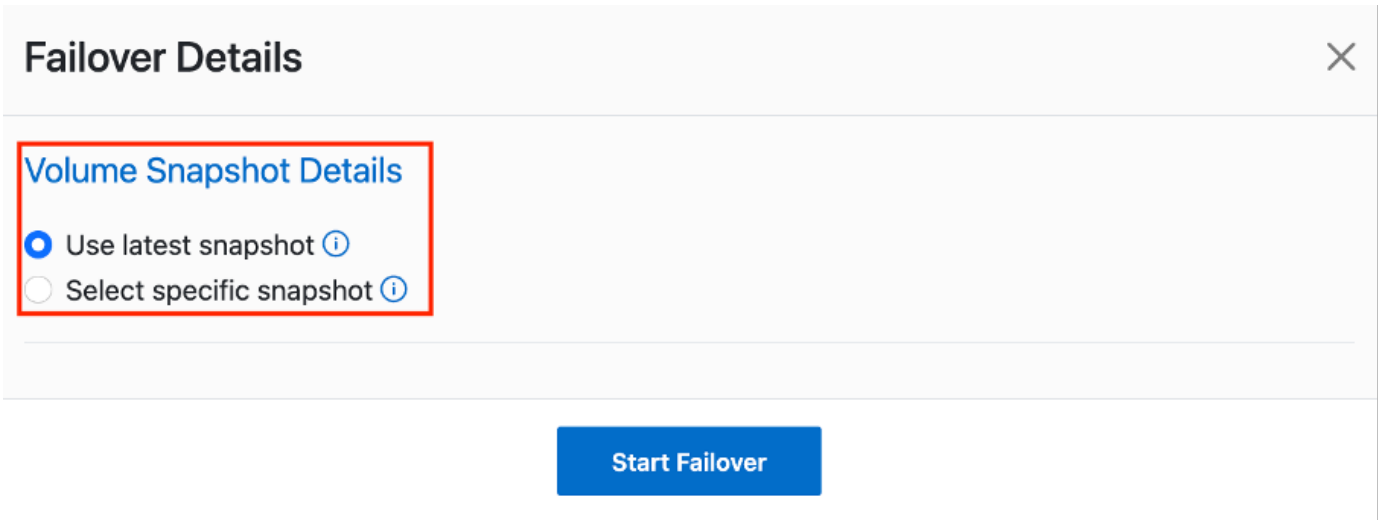


9. Clique em **Criar plano de replicação**.

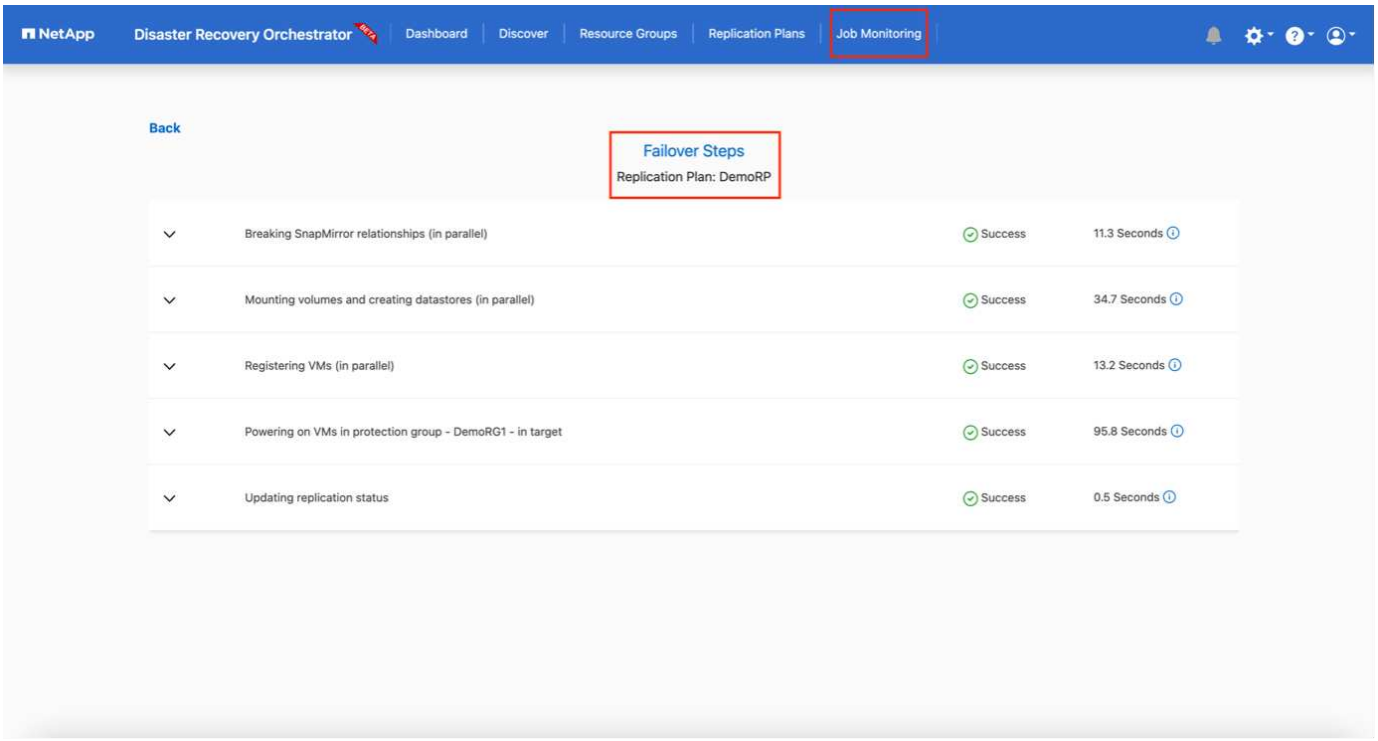


Após a criação do plano de replicação, a opção de failover, a opção de failover de teste ou a opção de migração podem ser exercidas dependendo dos requisitos. Durante as opções de failover e teste-failover, a cópia mais recente do SnapMirror Snapshot é usada, ou uma cópia específica do Snapshot pode ser selecionada de uma cópia do Snapshot de um momento específico (conforme a política de retenção do SnapMirror). A opção de momento específico pode ser muito útil se você estiver enfrentando um evento de corrupção como um ransomware, em que as réplicas mais recentes já estão comprometidas ou criptografadas. O DRO mostra todos os pontos disponíveis no tempo. Para acionar o failover ou testar o failover com a configuração especificada no plano de replicação, você pode clicar em **Failover** ou **Testar failover**.

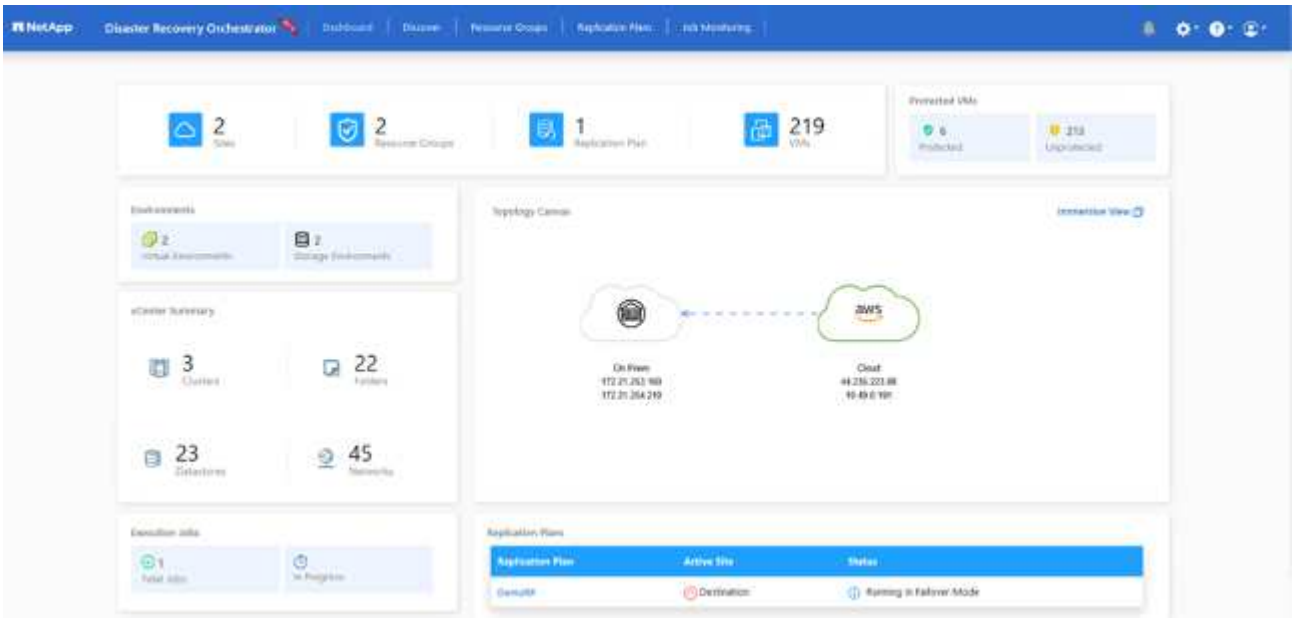




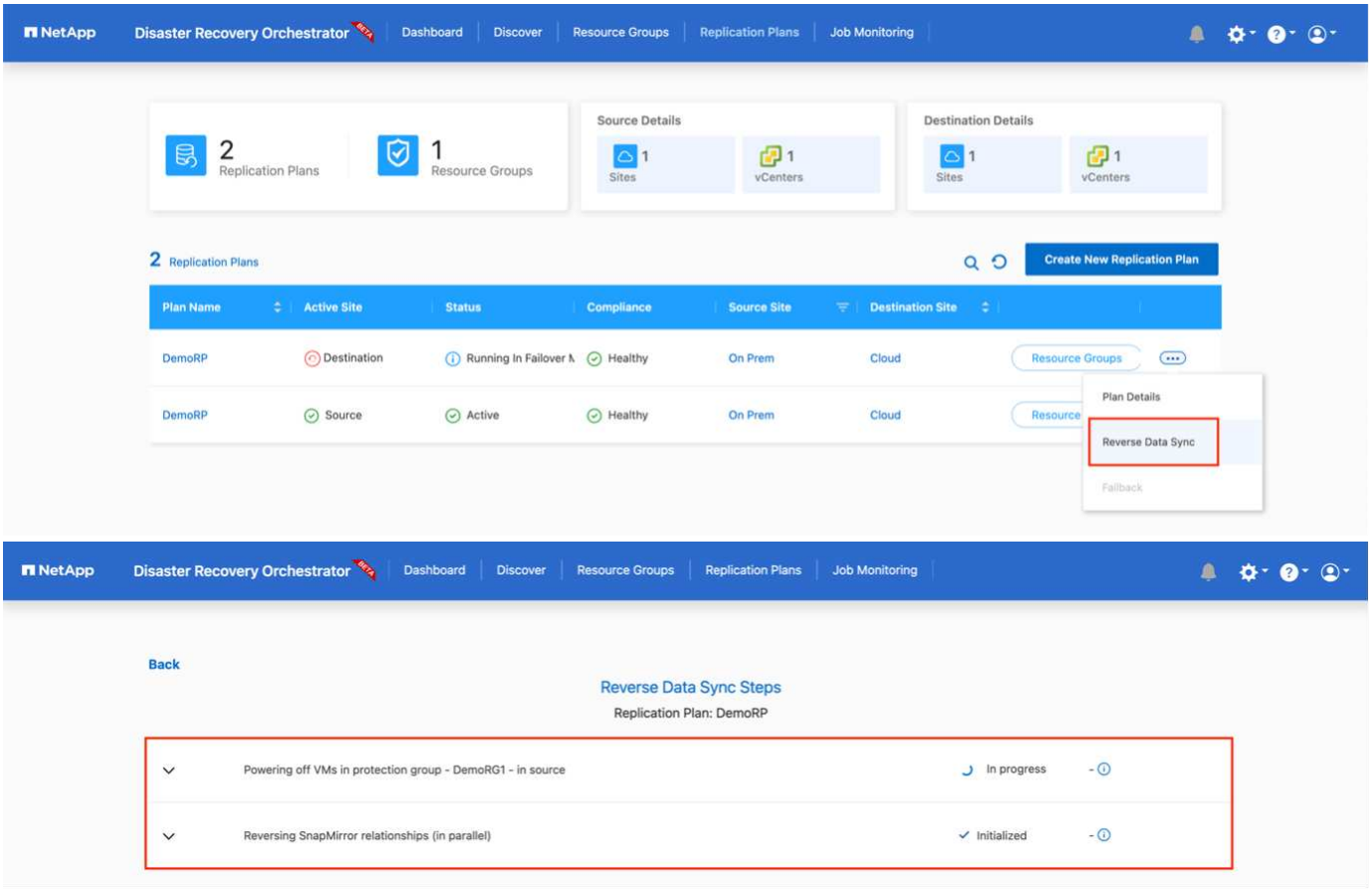
O plano de replicação pode ser monitorado no menu de tarefas:



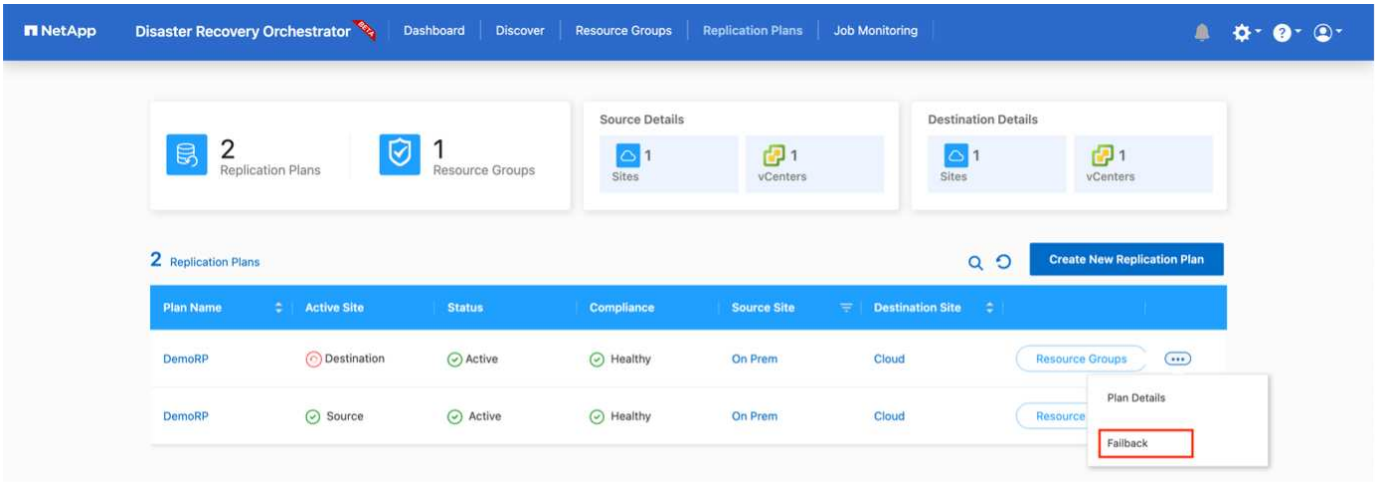
Após o failover ser acionado, os itens recuperados podem ser vistos no VMC vCenter (VMs, redes, armazenamentos de dados). Por padrão, as VMs são recuperadas para a pasta Carga de trabalho.

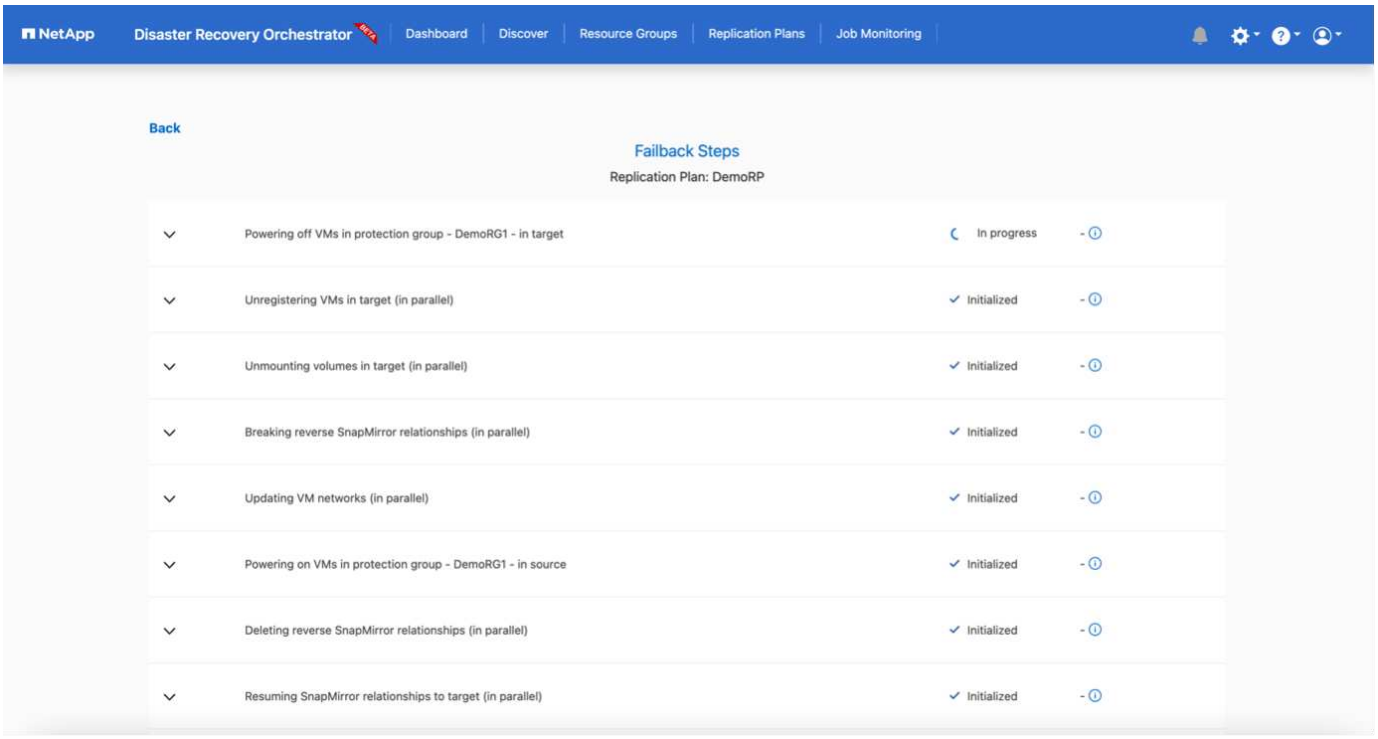


O failback pode ser acionado no nível do plano de replicação. Para um failover de teste, a opção tear-down pode ser usada para reverter as alterações e remover o relacionamento FlexClone . O failback relacionado ao failover é um processo de duas etapas. Selecione o plano de replicação e selecione **Sincronização reversa de dados**.

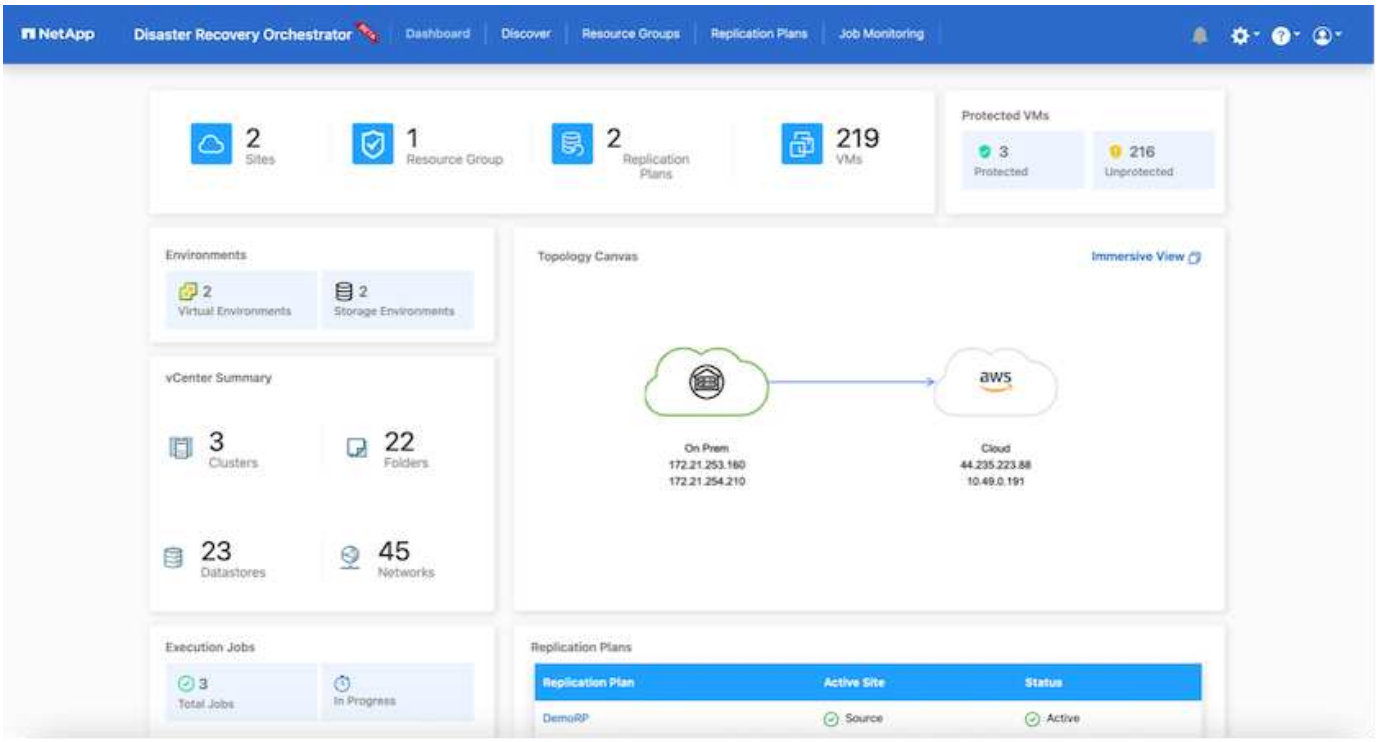


Após a conclusão, você pode acionar o failback para retornar ao site de produção original.





No NetApp Console, podemos ver que a integridade da replicação foi interrompida para os volumes apropriados (aqueles que foram mapeados para o VMC como volumes de leitura e gravação). Durante o failover de teste, o DRO não mapeia o volume de destino nem o de réplica. Em vez disso, ele cria uma cópia FlexClone da instância necessária do SnapMirror (ou Snapshot) e expõe a instância FlexClone, que não consome capacidade física adicional para o FSx ONTAP. Esse processo garante que o volume não seja modificado e que os trabalhos de replicação possam continuar mesmo durante testes de DR ou fluxos de trabalho de triagem. Além disso, esse processo garante que, se ocorrerem erros ou se dados corrompidos forem recuperados, a recuperação possa ser limpa sem o risco de a réplica ser destruída.



Recuperação de ransomware

Recuperar-se de um ransomware pode ser uma tarefa assustadora. Especificamente, pode ser difícil para organizações de TI identificar onde está o ponto de retorno seguro e, uma vez determinado, proteger cargas de trabalho recuperadas de ataques recorrentes de, por exemplo, malware inativo ou aplicativos vulneráveis.

O DRO resolve essas preocupações permitindo que você recupere seu sistema a partir de qualquer ponto disponível no tempo. Você também pode recuperar cargas de trabalho para redes funcionais, porém isoladas, para que os aplicativos possam funcionar e se comunicar entre si em um local onde não estejam expostos ao tráfego norte-sul. Isso dá à sua equipe de segurança um lugar seguro para conduzir análises forenses e garantir que não haja malware oculto ou adormecido.

Benefícios

- Uso da replicação eficiente e resiliente do SnapMirror .
- Recuperação para qualquer ponto disponível no tempo com retenção de cópia do Snapshot.
- Automação completa de todas as etapas necessárias para recuperar centenas a milhares de VMs das etapas de armazenamento, computação, rede e validação de aplicativos.
- Recuperação de carga de trabalho com tecnologia ONTAP FlexClone usando um método que não altera o volume replicado.
  - Evita risco de corrupção de dados para volumes ou cópias de Snapshot.
  - Evita interrupções de replicação durante fluxos de trabalho de teste de DR.
  - Uso potencial de dados de DR com recursos de computação em nuvem para fluxos de trabalho além de DR, como DevTest, testes de segurança, testes de patch ou atualização e testes de remediação.
- Otimização de CPU e RAM para ajudar a reduzir os custos da nuvem, permitindo a recuperação para clusters de computação menores.

Usando Veeam Replication e FSx ONTAP para recuperação de desastres no VMware Cloud na AWS

A integração do Amazon FSx ONTAP com o VMware Cloud on AWS é um armazenamento de dados NFS externo gerenciado pela AWS criado no sistema de arquivos ONTAP da NetApp que pode ser anexado a um cluster no SDDC. Ela fornece aos clientes uma infraestrutura de armazenamento virtualizada flexível e de alto desempenho que pode ser dimensionada independentemente dos recursos de computação.

Visão geral

Para os clientes que buscam usar o VMware Cloud on AWS SDDC como destino de recuperação de desastres, os datastores FSx ONTAP podem ser usados para replicar dados locais usando qualquer solução de terceiros validada que forneça capacidade de replicação de VM. Ao adicionar o datastore FSx ONTAP , será possível uma implantação com custo otimizado em vez de construir o VMware Cloud no AWS SDDC com uma quantidade enorme de hosts ESXi apenas para acomodar o armazenamento.

Essa abordagem também ajuda os clientes a usar o cluster de luz piloto no VMC junto com os armazenamentos de dados FSx ONTAP para hospedar as réplicas de VM. O mesmo processo também pode ser estendido como uma opção de migração para o VMware Cloud na AWS por meio de failover suave do plano de replicação.

Declaração do Problema

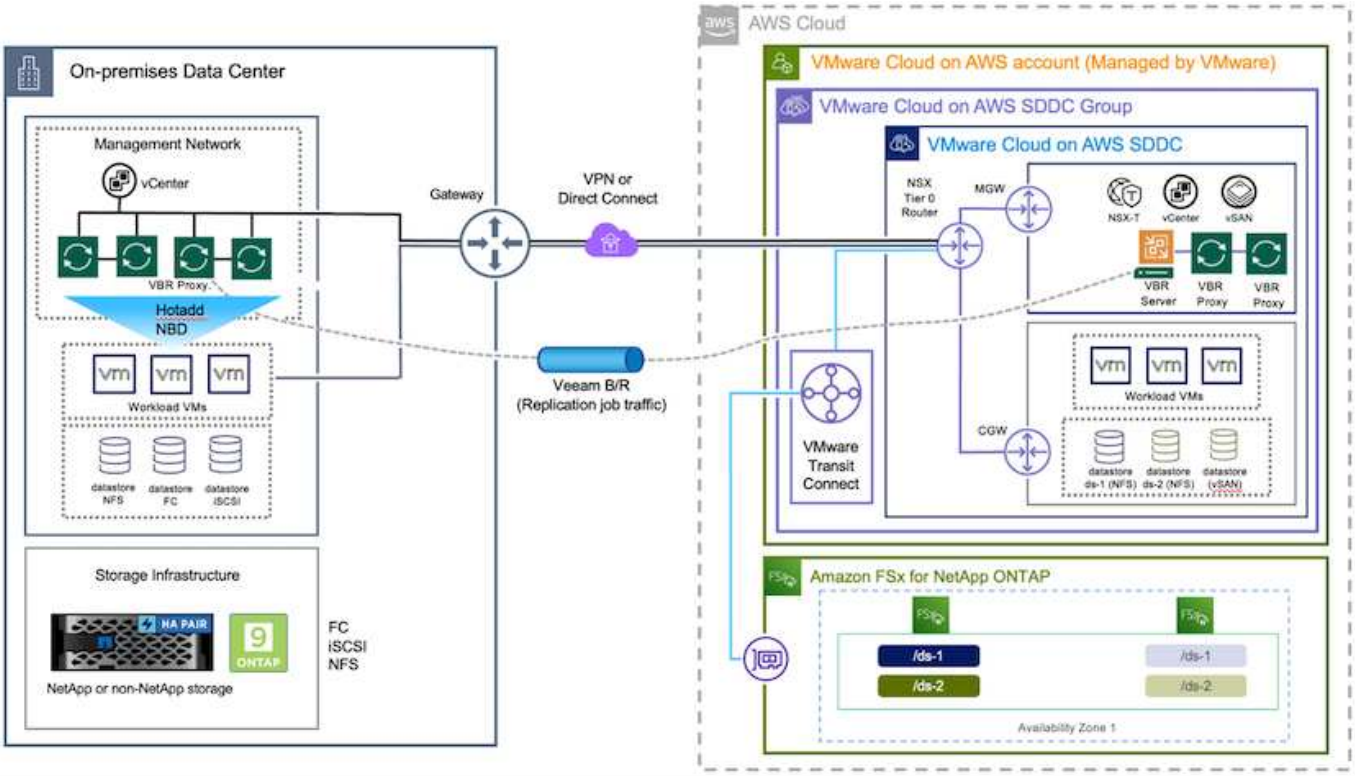
Este documento descreve como usar o armazenamento de dados FSx ONTAP e o Veeam Backup and Replication para configurar a recuperação de desastres para VMs VMware locais para o VMware Cloud na AWS usando a funcionalidade de replicação de VM.

O Veeam Backup & Replication permite replicação local e remota para recuperação de desastres (DR). Quando as máquinas virtuais são replicadas, o Veeam Backup & Replication cria uma cópia exata das VMs no formato nativo do VMware vSphere no cluster SDDC de destino do VMware Cloud on AWS e mantém a cópia sincronizada com a VM original.

A replicação fornece os melhores valores de objetivo de tempo de recuperação (RTO), pois há uma cópia de uma VM no estado pronto para iniciar. Esse mecanismo de replicação garante que as cargas de trabalho possam iniciar rapidamente no VMware Cloud on AWS SDDC em caso de um evento de desastre. O software Veeam Backup & Replication também otimiza a transmissão de tráfego para replicação via WAN e conexões lentas. Além disso, ele também filtra blocos de dados duplicados, blocos de dados zero, arquivos de swap e arquivos de sistema operacional convidado de VM excluídos, além de compactar o tráfego de réplica.

Para evitar que trabalhos de replicação consumam toda a largura de banda da rede, aceleradores de WAN e regras de limitação de rede podem ser implementados. O processo de replicação no Veeam Backup & Replication é orientado por tarefas, o que significa que a replicação é realizada configurando tarefas de replicação. Em caso de desastre, o failover pode ser acionado para recuperar as VMs por meio de failover para sua cópia de réplica.

Quando o failover é executado, uma VM replicada assume a função da VM original. O failover pode ser executado no estado mais recente de uma réplica ou em qualquer um dos seus pontos de restauração conhecidos. Isso permite a recuperação de ransomware ou testes isolados, conforme necessário. No Veeam Backup & Replication, failover e failback são etapas intermediárias temporárias que devem ser finalizadas posteriormente. O Veeam Backup & Replication oferece diversas opções para lidar com diferentes cenários de recuperação de desastres.



Degraus altos

1. O software Veeam Backup and Replication está sendo executado em um ambiente local com conectividade de rede apropriada.
2. Configure o VMware Cloud on AWS, consulte o artigo do VMware Cloud Tech Zone "Guia de implantação de integração do VMware Cloud on AWS com o Amazon FSx ONTAP" para implantar e configurar o VMware Cloud on AWS SDDC e o FSx ONTAP como datastore NFS. (Um ambiente pilot-light configurado com uma configuração mínima pode ser usado para fins de DR. As VMs farão failover para esse cluster em caso de incidente, e você pode adicionar nós adicionais).
3. Configure trabalhos de replicação para criar réplicas de VM usando o Veeam Backup and Replication.
4. Crie um plano de failover e execute o failover.
5. Retorne para as VMs de produção quando o evento de desastre for concluído e o site principal estiver ativo.

Pré-requisitos para replicação de VM Veeam para datastores VMC e FSx ONTAP

1. Certifique-se de que a VM de backup do Veeam Backup & Replication esteja conectada ao vCenter de origem, bem como aos clusters SDDC de destino do VMware Cloud on AWS.
2. O servidor de backup deve ser capaz de resolver nomes curtos e se conectar aos vCenters de origem e de destino.
3. O armazenamento de dados FSx ONTAP de destino deve ter espaço livre suficiente para armazenar VMDKs de VMs replicadas

Para obter informações adicionais, consulte “Considerações e Limitações” abordado"aqui" .

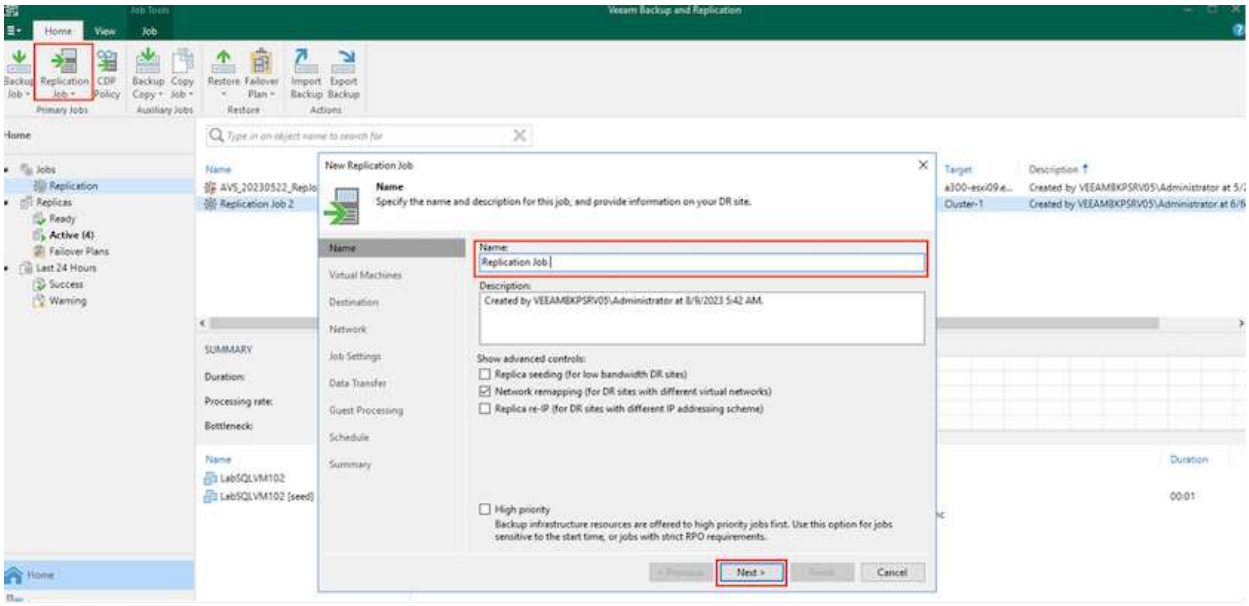
Detalhes da implantação

▼ **Etapa 1: replicar VMs**

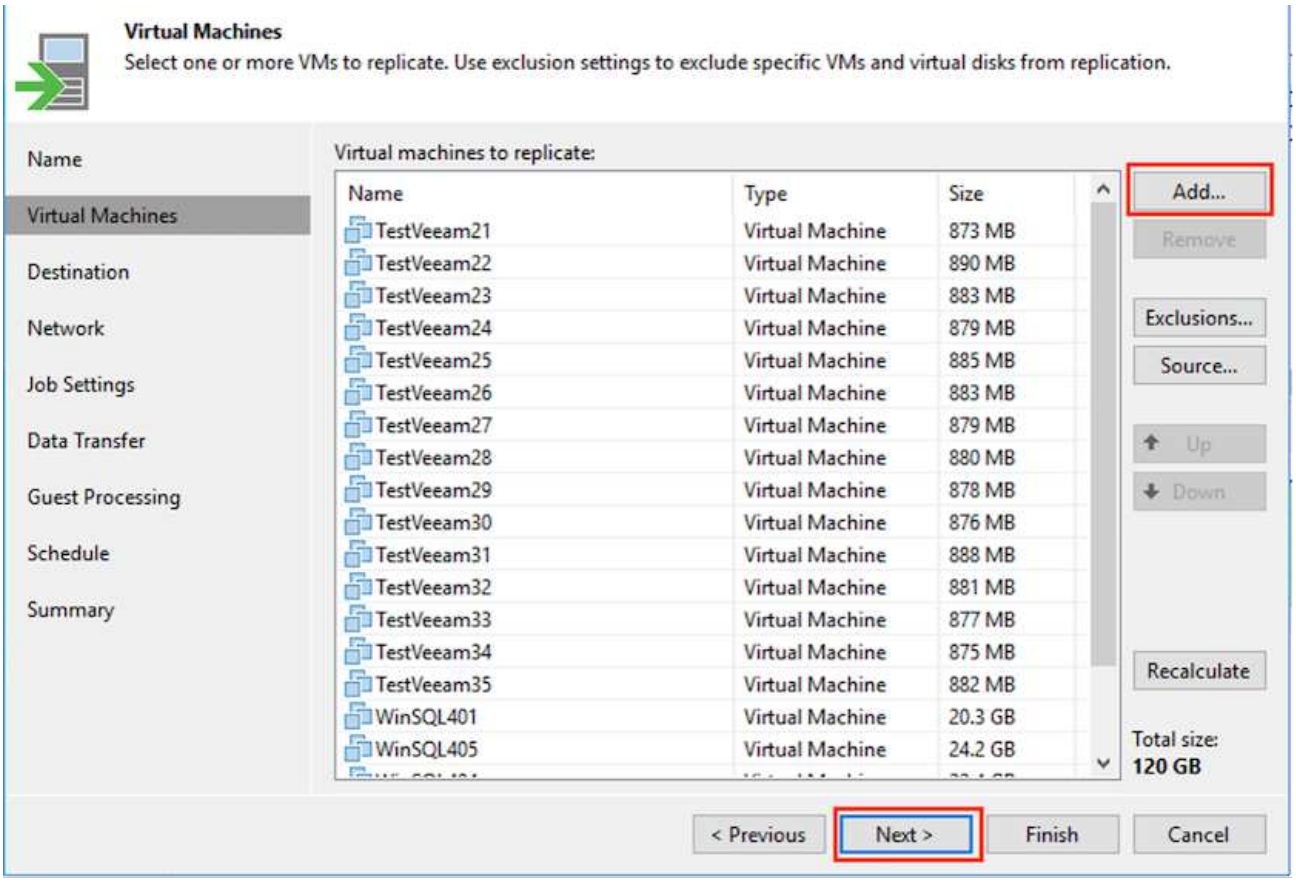
O Veeam Backup & Replication aproveita os recursos de snapshot do VMware vSphere e, durante a replicação, o Veeam Backup & Replication solicita que o VMware vSphere crie um snapshot de VM. O snapshot da VM é a cópia de um momento específico de uma VM que inclui discos virtuais, estado do sistema, configuração e assim por diante. O Veeam Backup & Replication usa o snapshot como uma fonte de dados para replicação.

Para replicar VMs, siga as etapas abaixo:

1. Abra o Veeam Backup & Replication Console.
2. Na exibição Início, selecione Trabalho de replicação > Máquina virtual > VMware vSphere.
3. Especifique um nome de tarefa e selecione a caixa de seleção de controle avançado apropriada. Clique em Avançar.
   - Marque a caixa de seleção Semeadura de réplica se a conectividade entre o local e a AWS tiver largura de banda restrita.
   - Marque a caixa de seleção Remapeamento de rede (para sites do AWS VMC com redes diferentes) se os segmentos no VMware Cloud on AWS SDDC não corresponderem às redes de sites locais.
   - Se o esquema de endereçamento IP no site de produção local for diferente do esquema no site do AWS VMC, marque a caixa de seleção Replica re-IP (para sites de DR com esquema de endereçamento IP diferente).

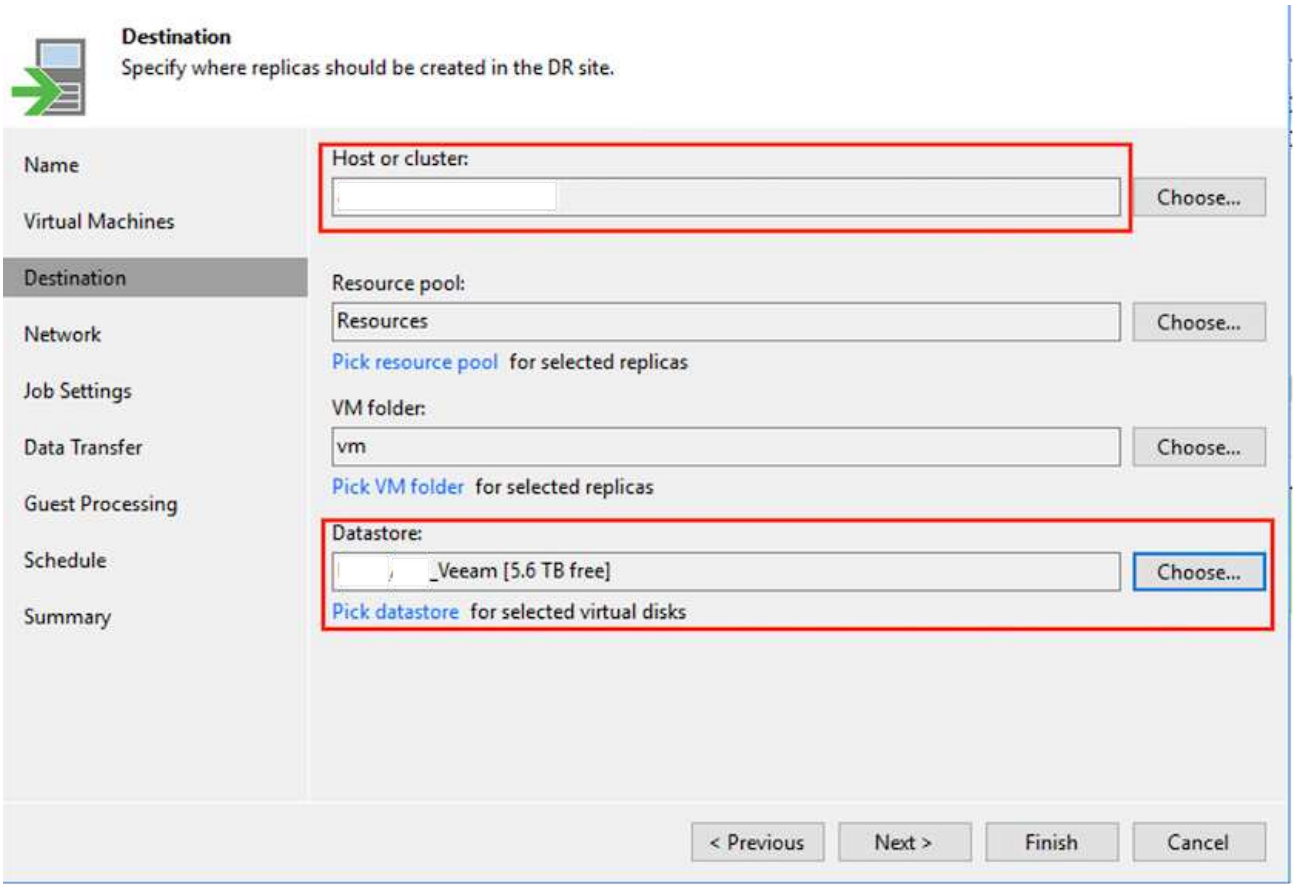


4. Selecione as VMs que precisam ser replicadas para o armazenamento de dados FSx ONTAP anexado ao VMware Cloud on AWS SDDC na etapa **Máquinas virtuais**. As máquinas virtuais podem ser colocadas no vSAN para preencher a capacidade disponível do armazenamento de dados do vSAN. Em um cluster de luz piloto, a capacidade utilizável de um cluster de 3 nós será limitada. O restante dos dados pode ser replicado nos armazenamentos de dados FSx ONTAP . Clique em **Adicionar**, então na janela **Adicionar Objeto** selecione as VMs ou contêineres de VM necessários e clique em **Adicionar**. Clique em **Avançar**.

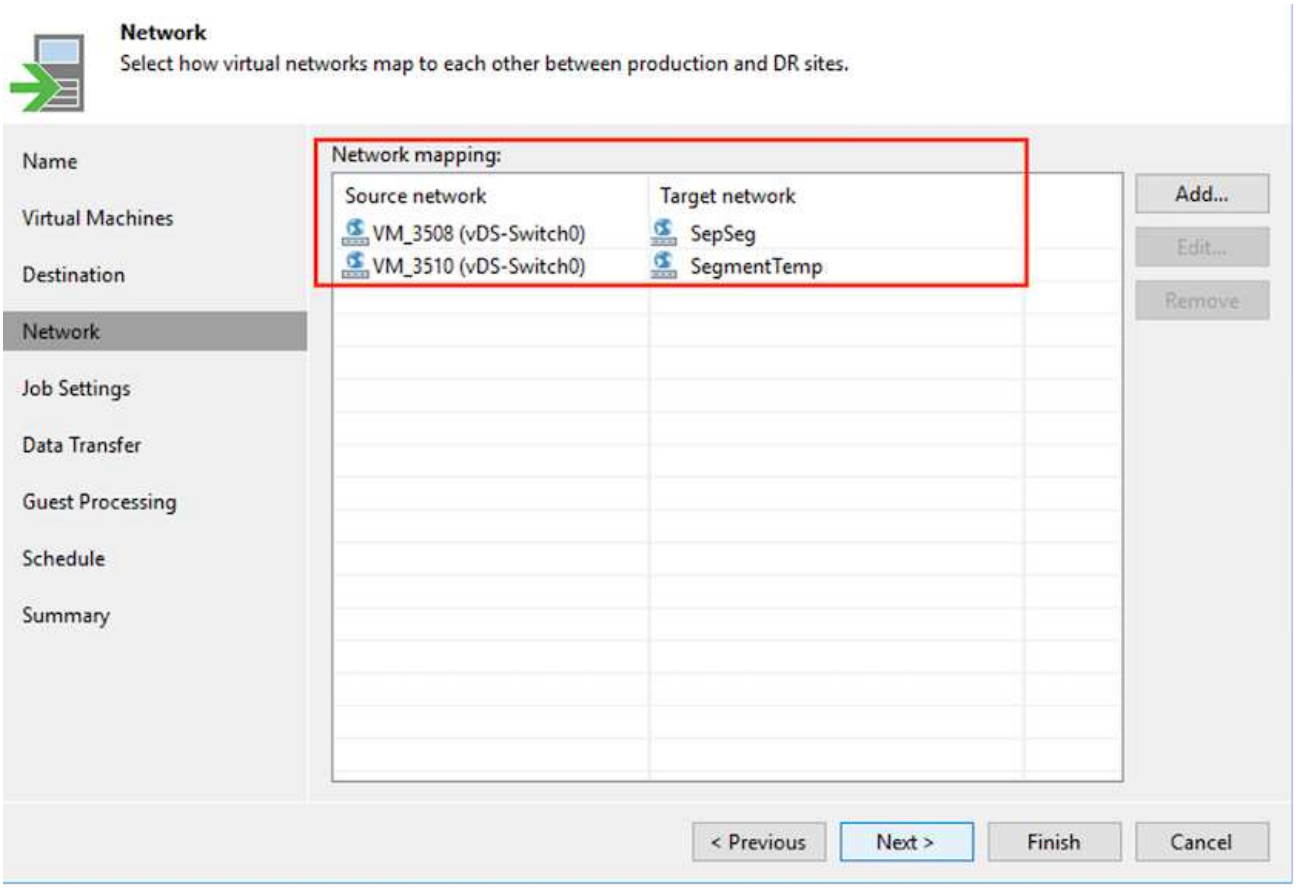


5. Depois disso, selecione o destino como cluster/host SDDC do VMware Cloud on AWS e o pool de

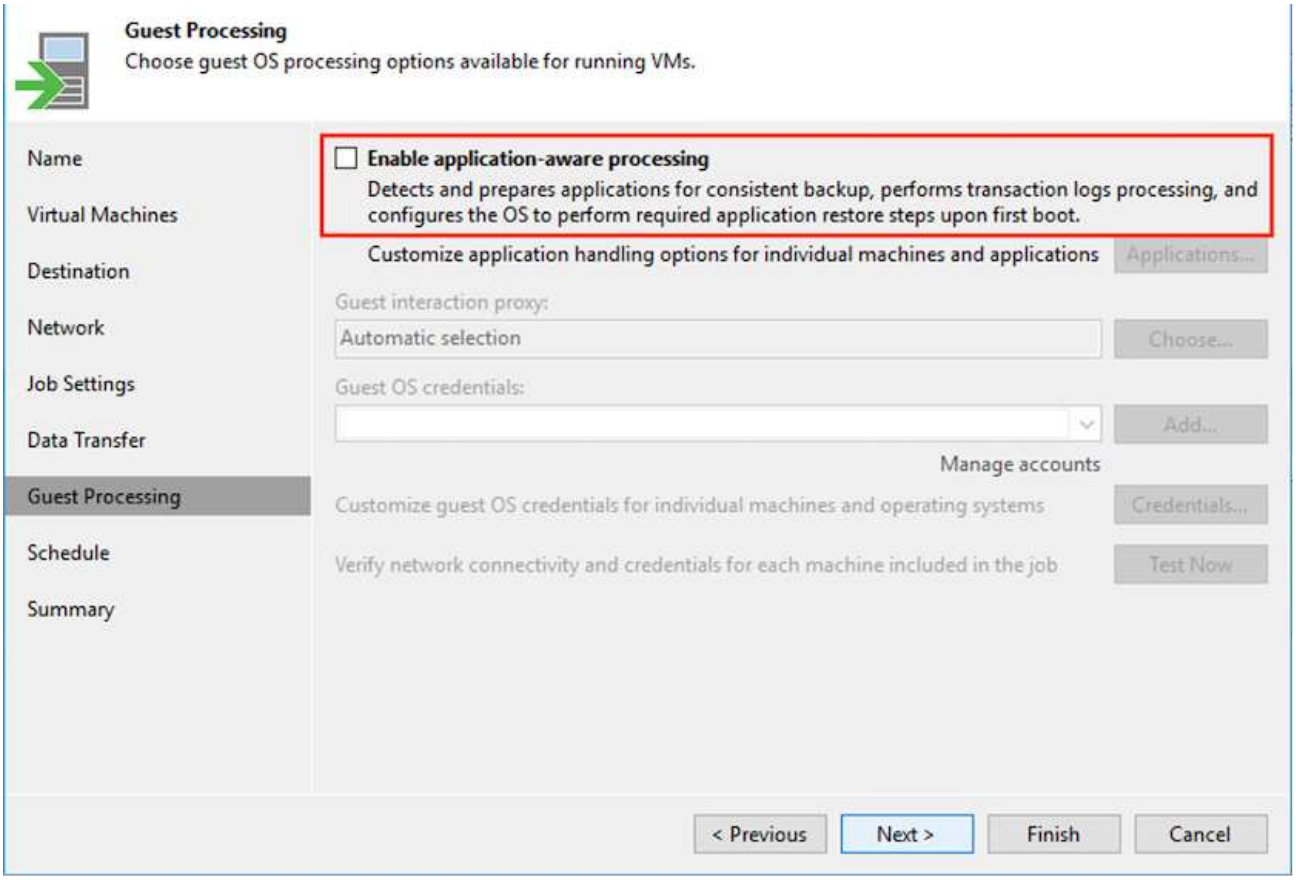
recursos apropriado, a pasta da VM e o armazenamento de dados FSx ONTAP para réplicas da VM. Em seguida, clique em **Avançar**.



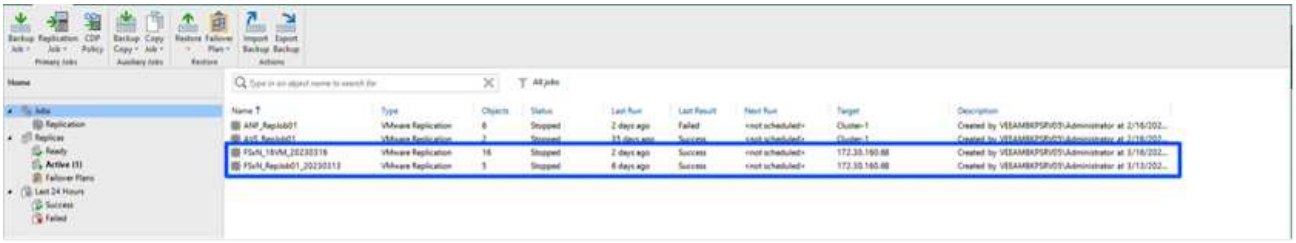
6. Na próxima etapa, crie o mapeamento entre a rede virtual de origem e de destino, conforme necessário.



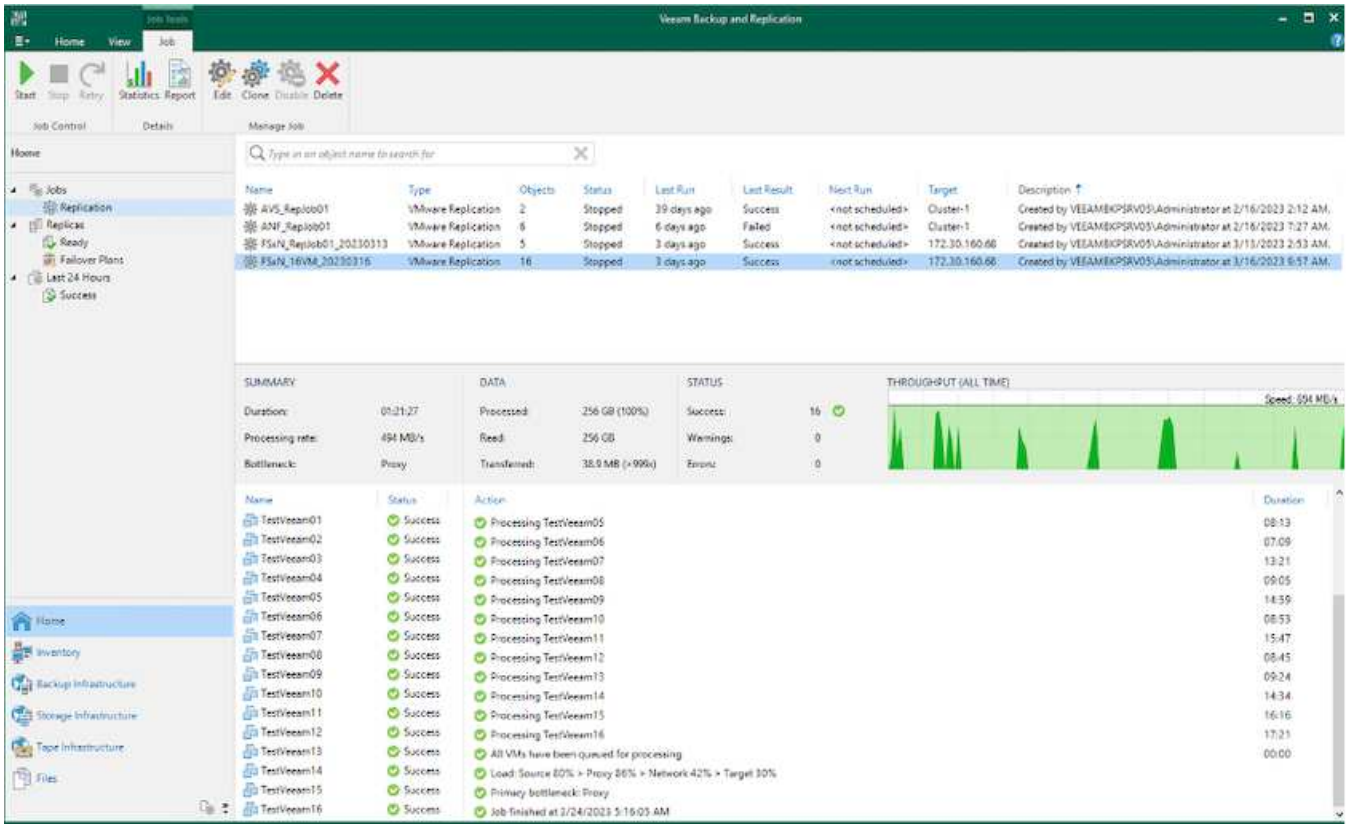
7. Na etapa **Configurações da tarefa**, especifique o repositório de backup que armazenará metadados para réplicas de VM, política de retenção e assim por diante.
8. Atualize os servidores proxy **Origem** e **Destino** na etapa **Transferência de dados** e deixe a seleção **Automático** (padrão) e mantenha a opção **Direto** selecionada e clique em **Avançar**.
9. Na etapa **Processamento de Convidado**, selecione a opção **Ativar processamento com reconhecimento de aplicativo** conforme necessário. Clique em **Avançar**.



10. Escolha o agendamento de replicação para executar o trabalho de replicação regularmente.
11. Na etapa **Resumo** do assistente, revise os detalhes do trabalho de replicação. Para iniciar o trabalho logo após o assistente ser fechado, marque a caixa de seleção **Executar o trabalho quando eu clicar em Concluir**; caso contrário, deixe a caixa de seleção desmarcada. Em seguida, clique em **Concluir** para fechar o assistente.



Assim que o trabalho de replicação começar, as VMs com o sufixo especificado serão preenchidas no cluster/host do SDDC do VMC de destino.



Para obter informações adicionais sobre a replicação do Veeam, consulte"Como funciona a replicação" .

▼ **Etapa 2: Crie um plano de failover**

Quando a replicação ou propagação inicial estiver concluída, crie o plano de failover. O plano de failover ajuda a executar o failover para VMs dependentes, uma por uma ou como um grupo, automaticamente. O plano de failover é o modelo para a ordem em que as VMs são processadas, incluindo os atrasos de inicialização. O plano de failover também ajuda a garantir que as VMs dependentes críticas já estejam em execução.

Para criar o plano, navegue até a nova subseção chamada Réplicas e selecione Plano de Failover. Escolha as VMs apropriadas. O Veeam Backup & Replication procurará os pontos de restauração mais próximos desse momento e os usará para iniciar réplicas de VM.

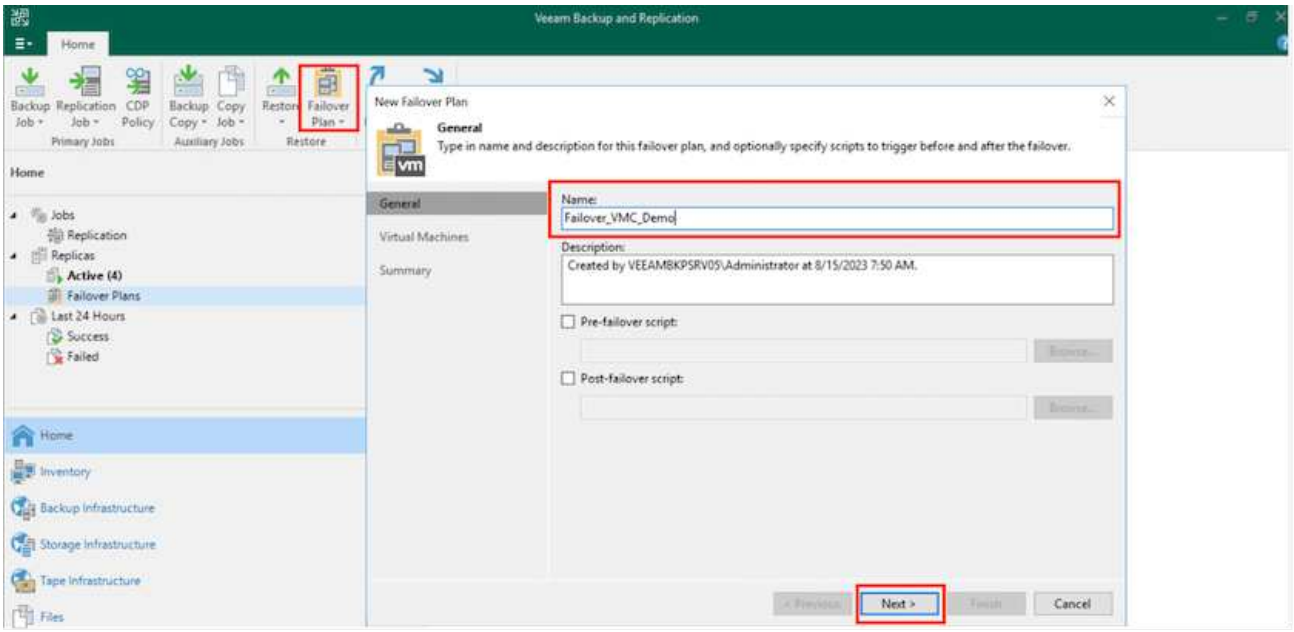
ⓘ O plano de failover só pode ser adicionado quando a replicação inicial estiver concluída e as réplicas da VM estiverem no estado Pronto.

ⓘ O número máximo de VMs que podem ser iniciadas simultaneamente ao executar um plano de failover é 10.

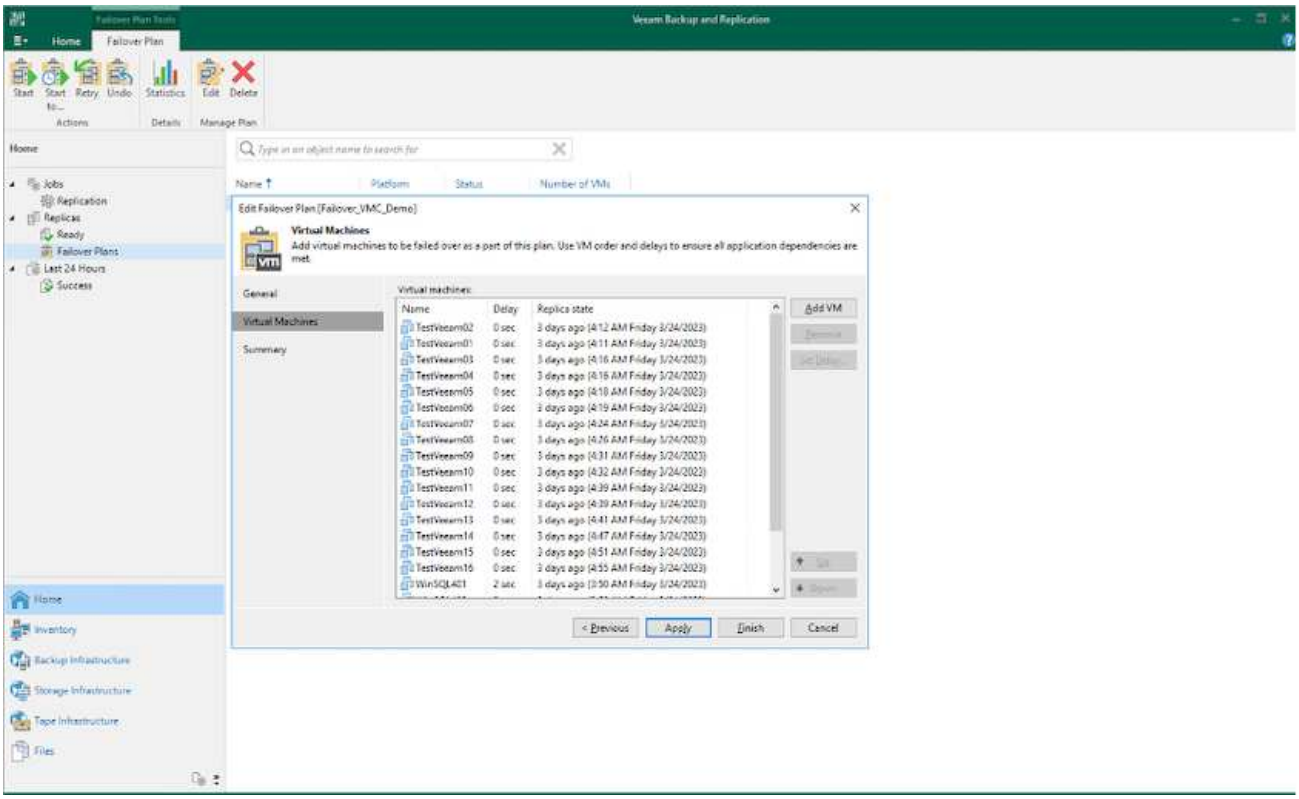
ⓘ Durante o processo de failover, as VMs de origem não serão desligadas.

Para criar o **Plano de Failover**, faça o seguinte:

1. Na exibição inicial, selecione **Plano de failover > VMware vSphere**.
2. Em seguida, forneça um nome e uma descrição para o plano. Scripts pré e pós-failover podem ser adicionados conforme necessário. Por exemplo, execute um script para desligar as VMs antes de iniciar as VMs replicadas.



3. Adicione as VMs ao plano e modifique a ordem de inicialização das VMs e os atrasos de inicialização para atender às dependências do aplicativo.



Para obter informações adicionais sobre a criação de trabalhos de replicação, consulte"Criando trabalhos de replicação" .

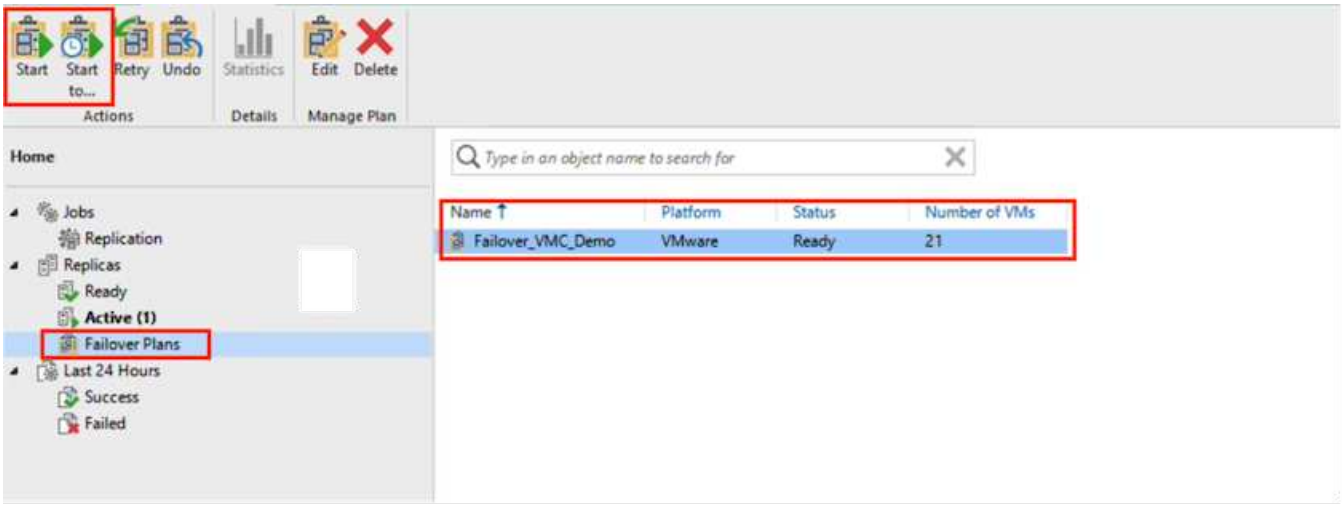
▼ **Etapa 3: execute o plano de failover**

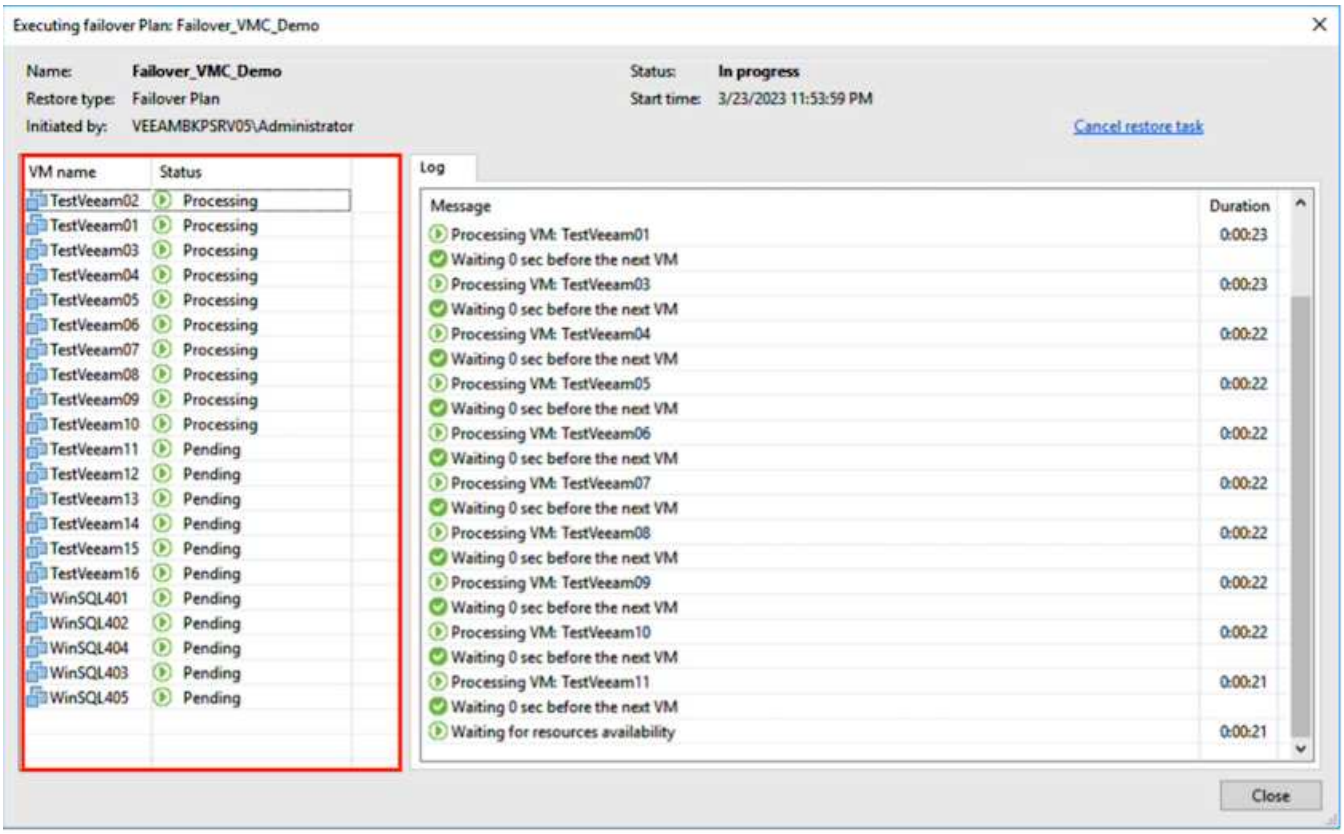
Durante o failover, a VM de origem no site de produção é alternada para sua réplica no site de recuperação de desastres. Como parte do processo de failover, o Veeam Backup & Replication restaura a réplica da VM para o ponto de restauração necessário e move todas as atividades de E/S da VM de origem para sua réplica. As réplicas podem ser usadas não apenas em caso de desastre, mas também para simular

exercícios de DR. Durante a simulação de failover, a VM de origem permanece em execução. Depois que todos os testes necessários forem realizados, você poderá desfazer o failover e retornar às operações normais.

Certifique-se de que a segmentação de rede esteja em vigor para evitar conflitos de IP durante simulações de DR.

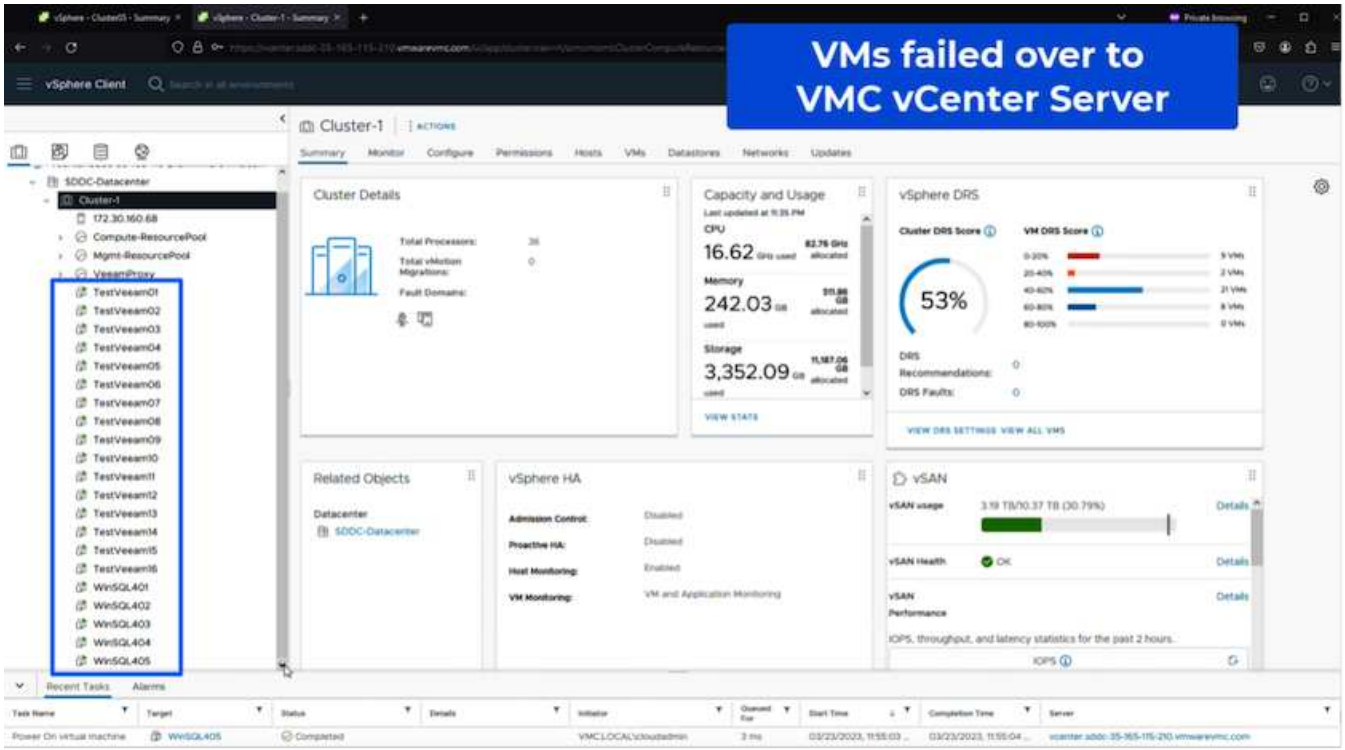
Para iniciar o plano de failover, basta clicar na aba **Planos de failover** e clicar com o botão direito do mouse no plano de failover. Selecione **Iniciar**. Isso fará failover usando os pontos de restauração mais recentes das réplicas de VM. Para fazer failover para pontos de restauração específicos de réplicas de VM, selecione **Iniciar para**.



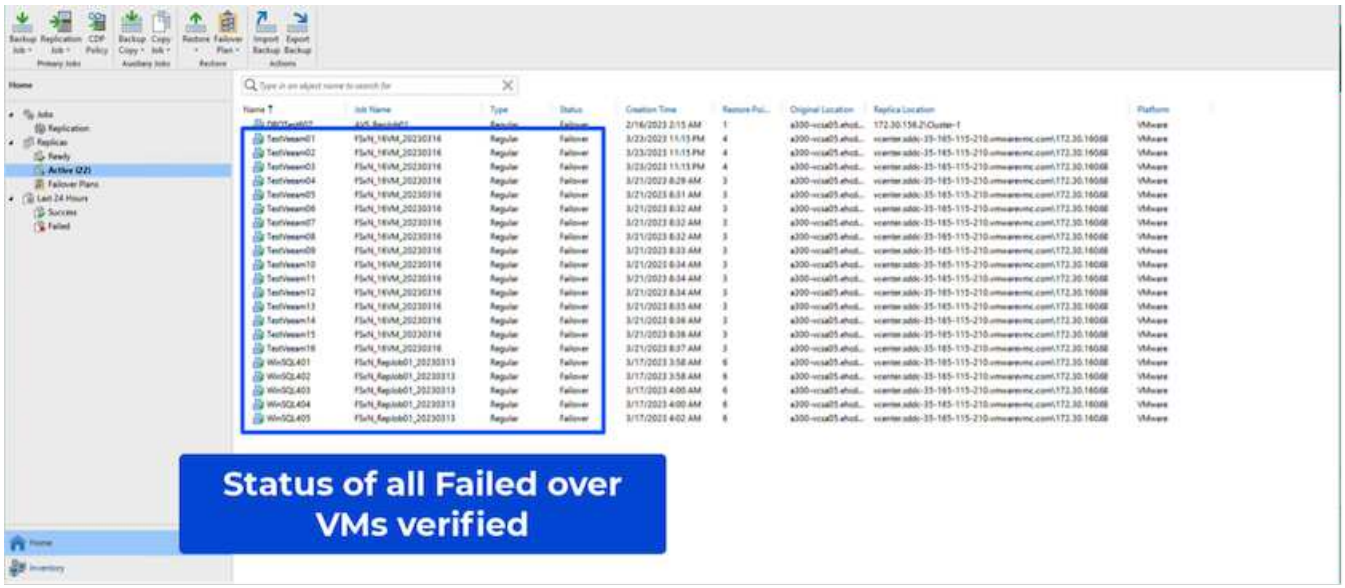


O estado da réplica da VM muda de Pronto para Failover e as VMs serão iniciadas no cluster/host SDDC

do VMware Cloud on AWS de destino.



Quando o failover estiver concluído, o status das VMs mudará para "Failover".



> O Veeam Backup & Replication interrompe todas as atividades de replicação da VM de origem até que sua réplica retorne ao estado Pronto.

Para obter informações detalhadas sobre planos de failover, consulte"Planos de Failover" .

▼ **Etapa 4: Failback para o site de produção**

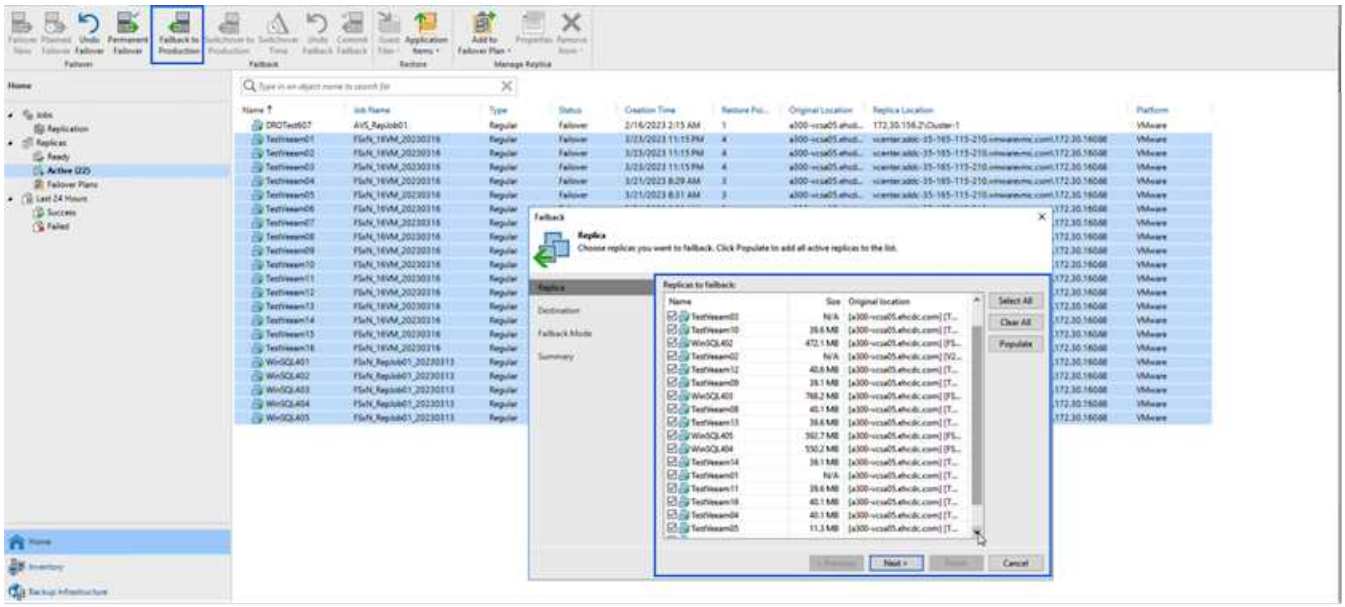
Quando o plano de failover está em execução, ele é considerado uma etapa intermediária e precisa ser finalizado com base no requisito. As opções incluem o seguinte:

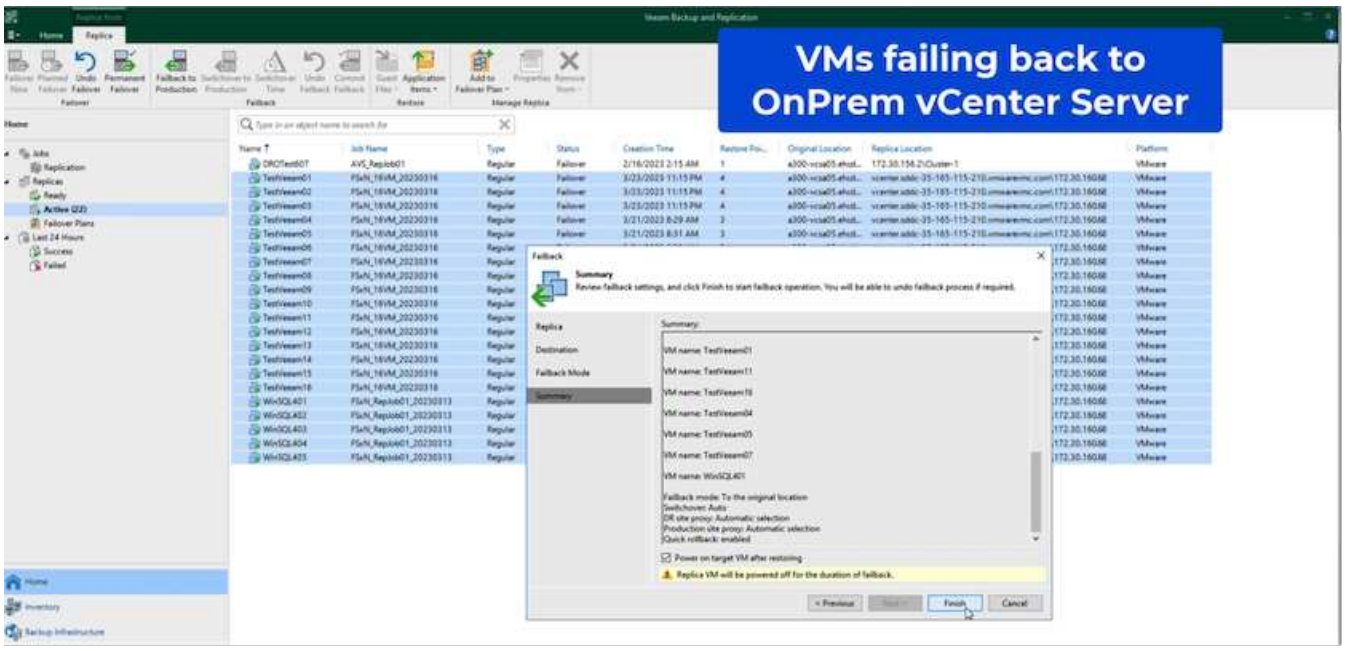
- **Failback para produção** - retorne para a VM original e transfira todas as alterações que ocorreram enquanto a réplica da VM estava em execução para a VM original.

> Quando você executa o failback, as alterações são apenas transferidas, mas não publicadas. Escolha **Confirmar failback** (assim que a VM original for confirmada como funcionando conforme o esperado) ou **Desfazer failback** para retornar à réplica da VM se a VM original não estiver funcionando conforme o esperado.

- **Desfazer failover** - retorne à VM original e descarte todas as alterações feitas na réplica da VM enquanto ela estava em execução.
- **Failover permanente** - alterna permanentemente da VM original para uma réplica da VM e usa essa réplica como a VM original.

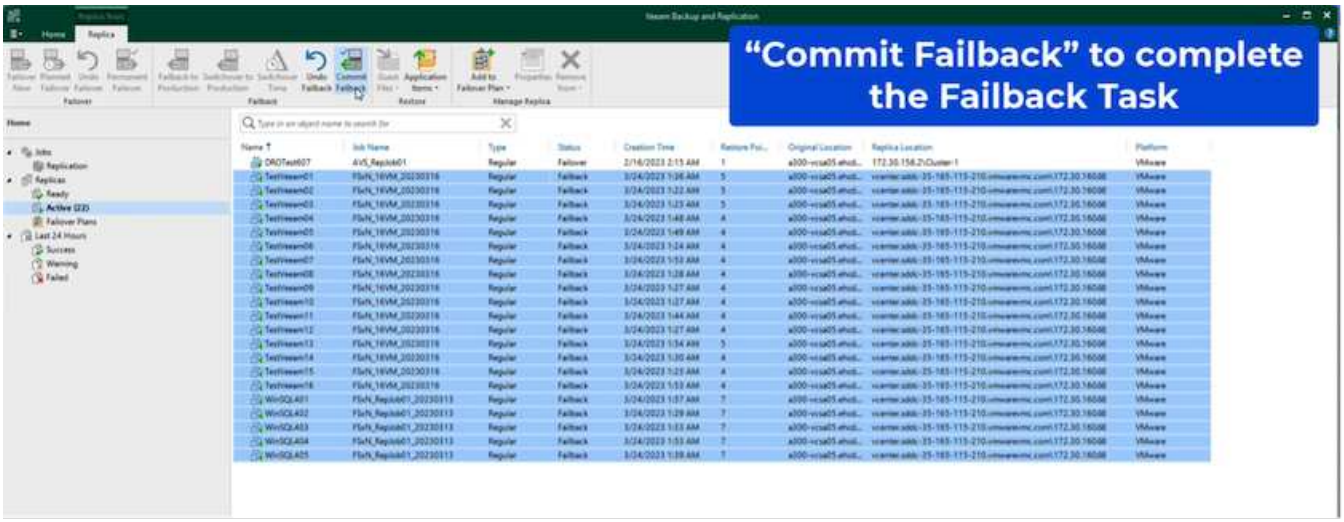
Nesta demonstração, foi escolhido Failback para produção. O failback para a VM original foi selecionado durante a etapa Destino do assistente e a caixa de seleção "Ligar a VM após a restauração" foi marcada.

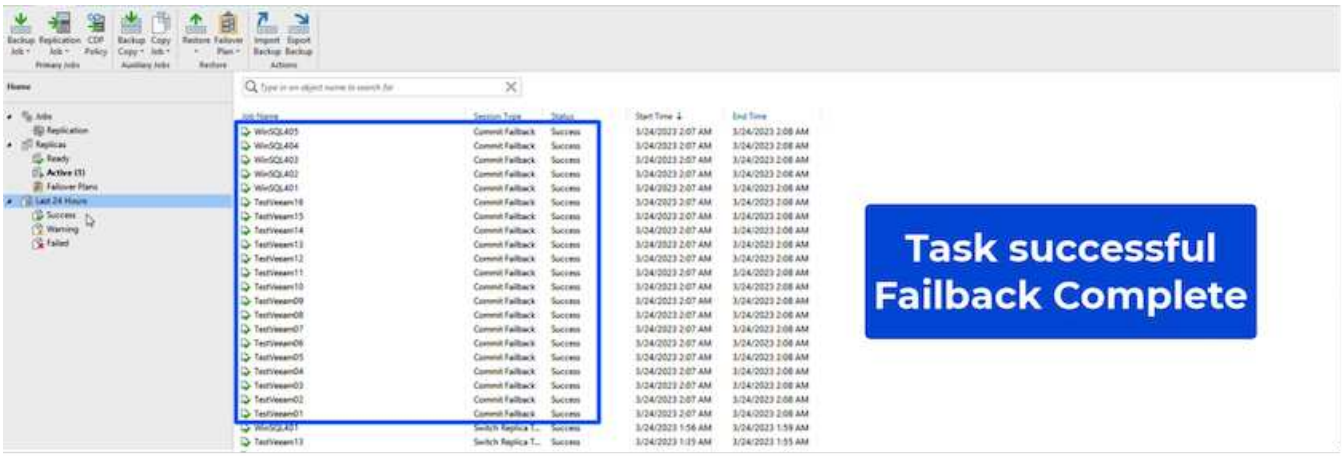




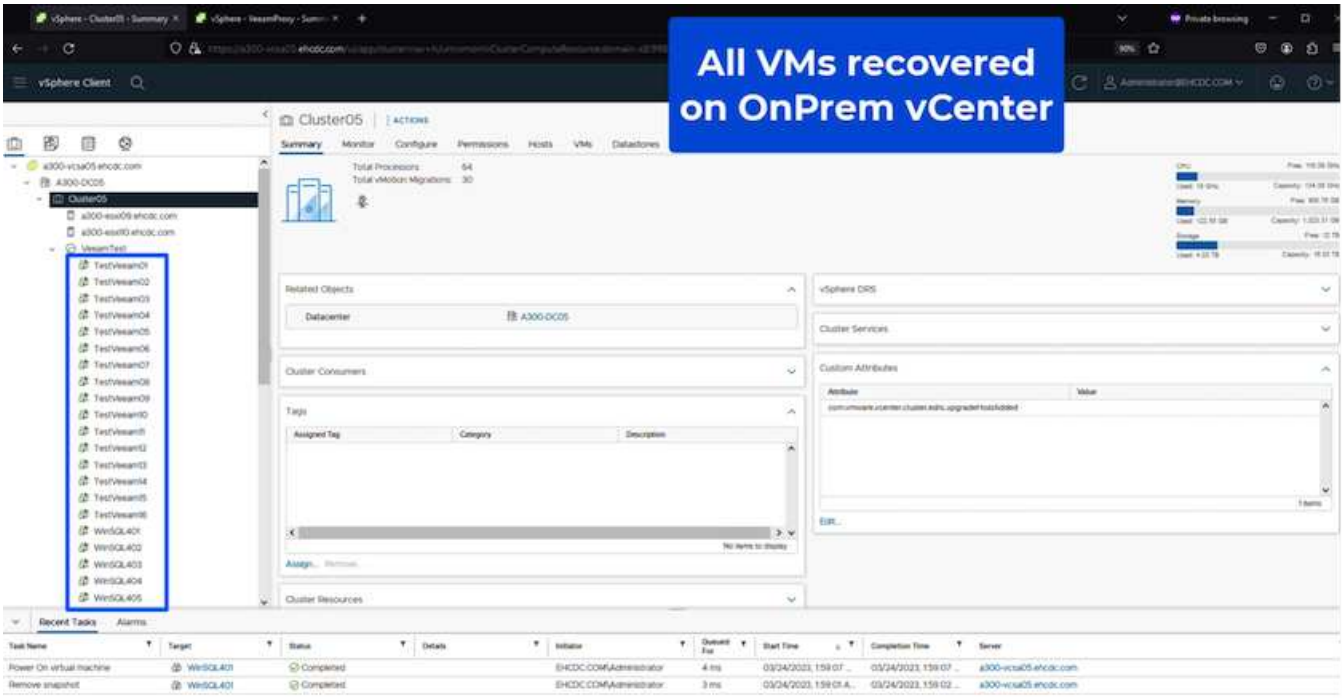
A confirmação de failback é uma das maneiras de finalizar a operação de failback. Quando o failback é confirmado, ele confirma que as alterações enviadas para a VM que sofreu failback (a VM de produção) estão funcionando conforme o esperado. Após a operação de confirmação, o Veeam Backup & Replication retoma as atividades de replicação para a VM de produção.

Para obter informações detalhadas sobre o processo de failback, consulte a documentação do Veeam para"Failover e Failback para replicação" .





Após o failback para produção ser bem-sucedido, todas as VMs serão restauradas para o site de produção original.



Conclusão

O recurso de armazenamento de dados FSx ONTAP permite que a Veeam ou qualquer ferramenta de terceiros validada forneça uma solução de DR de baixo custo usando o cluster Pilot Light e sem criar um grande número de hosts no cluster apenas para acomodar a cópia da réplica da VM. Isso fornece uma solução poderosa para lidar com um plano de recuperação de desastres personalizado e personalizado e também permite reutilizar produtos de backup existentes internamente para atender às necessidades de DR, permitindo assim a recuperação de desastres baseada em nuvem ao sair dos data centers de DR locais. 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.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=15fed205-8614-4ef7-b2d0-b061015e925a

Migrar cargas de trabalho na AWS/VMC

TR 4942: Migrar cargas de trabalho para o armazenamento de dados FSx ONTAP usando VMware HCX

Um caso de uso comum para o VMware Cloud (VMC) na Amazon Web Services (AWS), com seu armazenamento de dados NFS suplementar no Amazon FSx ONTAP, é a migração de cargas de trabalho do VMware. O VMware HCX é uma opção preferencial e fornece vários métodos de migração para mover máquinas virtuais (VMs) locais e seus dados, em execução em qualquer repositório de dados compatível com VMware, para repositórios de dados VMC, o que inclui repositórios de dados NFS suplementares no FSx ONTAP.

Visão geral: Migrando máquinas virtuais com VMware HCX, armazenamentos de dados suplementares FSx ONTAP e VMware Cloud

O VMware HCX é principalmente uma plataforma de mobilidade projetada para simplificar a migração de carga de trabalho, o rebalanceamento de carga de trabalho e a continuidade dos negócios entre nuvens. Ele

está incluído como parte do VMware Cloud on AWS e oferece muitas maneiras de migrar cargas de trabalho e pode ser usado para operações de recuperação de desastres (DR).

Este documento fornece orientação passo a passo para implantar e configurar o VMware HCX, incluindo todos os seus principais componentes, no local e no data center na nuvem, o que permite vários mecanismos de migração de VM.

Para mais informações, consulte "Guia do usuário do VMware HCX" e "Lista de verificação de instalação B - HCX com um ambiente de destino SDDC do VMware Cloud on AWS" .

▼ Etapas de alto nível

Esta lista fornece as etapas de alto nível para instalar e configurar o VMware HCX:

1. Ative o HCX para o data center definido por software (SDDC) do VMC por meio do VMware Cloud Services Console.
2. Baixe e implante o instalador OVA do HCX Connector no vCenter Server local.
3. Ative o HCX com uma chave de licença.
4. Emparelhe o VMware HCX Connector local com o VMC HCX Cloud Manager.
5. Configure o perfil de rede, o perfil de computação e a malha de serviço.
6. (Opcional) Execute a extensão de rede para estender a rede e evitar a redefinição de IP.
7. Valide o status do dispositivo e garanta que a migração seja possível.
8. Migre as cargas de trabalho da VM.

▼ Pré-requisitos

Antes de começar, certifique-se de que os seguintes pré-requisitos sejam atendidos. Para obter mais informações, consulte "Preparando para instalação" . Depois que os pré-requisitos estiverem prontos, incluindo a conectividade, configure e ative o HCX gerando uma chave de licença no VMware HCX Console no VMC. Após a ativação do HCX, o plug-in do vCenter é implantado e pode ser acessado usando o vCenter Console para gerenciamento.

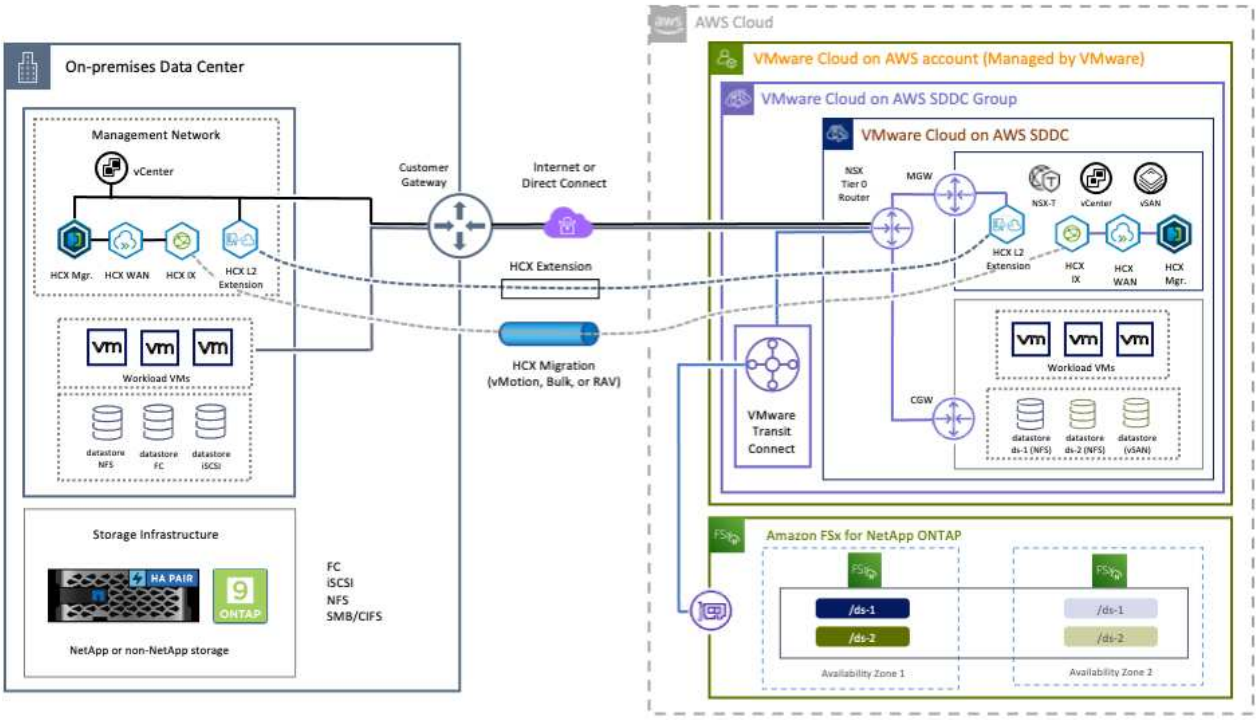
As seguintes etapas de instalação devem ser concluídas antes de prosseguir com a ativação e implantação do HCX:

1. Use um VMC SDDC existente ou crie um novo SDDC seguindo este"Link da NetApp" ou isto "Link VMware" .
2. O caminho de rede do ambiente vCenter local para o VMC SDDC deve oferecer suporte à migração de VMs usando o vMotion.
3. Certifique-se de que o necessário "regras e portas de firewall" são permitidos para tráfego vMotion entre o vCenter Server local e o SDDC vCenter.
4. O volume FSx ONTAP NFS deve ser montado como um armazenamento de dados suplementar no VMC SDDC. Para anexar os datastores NFS ao cluster apropriado, siga as etapas descritas neste"Link da NetApp" ou isto "Link VMware" .

▼ Arquitetura de Alto Nível

Para fins de teste, o ambiente de laboratório local usado para esta validação foi conectado por meio de uma VPN site a site ao AWS VPC, o que permitiu conectividade local ao AWS e ao VMware Cloud SDDC por meio do gateway de trânsito externo. O tráfego de migração HCX e extensão de rede flui pela internet entre o SDDC local e o destino de nuvem VMware. Esta arquitetura pode ser modificada para usar interfaces virtuais privadas do Direct Connect.

A imagem a seguir descreve a arquitetura de alto nível.



Implantação de solução

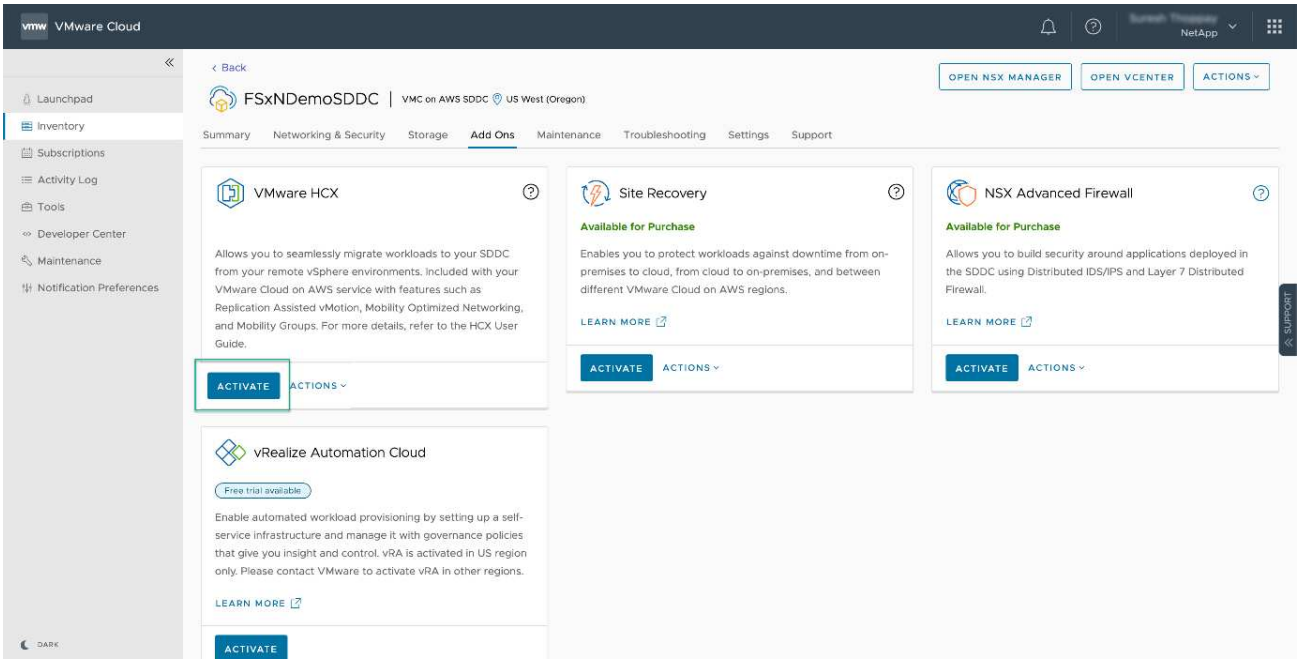
Siga a série de etapas para concluir a implantação desta solução:

▼ **Etapa 1: ativar o HCX por meio do VMC SDDC usando a opção Add-ons**

Para executar a instalação, siga os seguintes passos:

1. Faça login no console do VMC em "vmc.vmware.com" e acessar o inventário.
2. Para selecionar o SDDC apropriado e acessar os complementos, clique em Exibir detalhes no SDDC e selecione a guia Complementos.
3. Clique em Ativar para VMware HCX.

Esta etapa leva até 25 minutos para ser concluída.

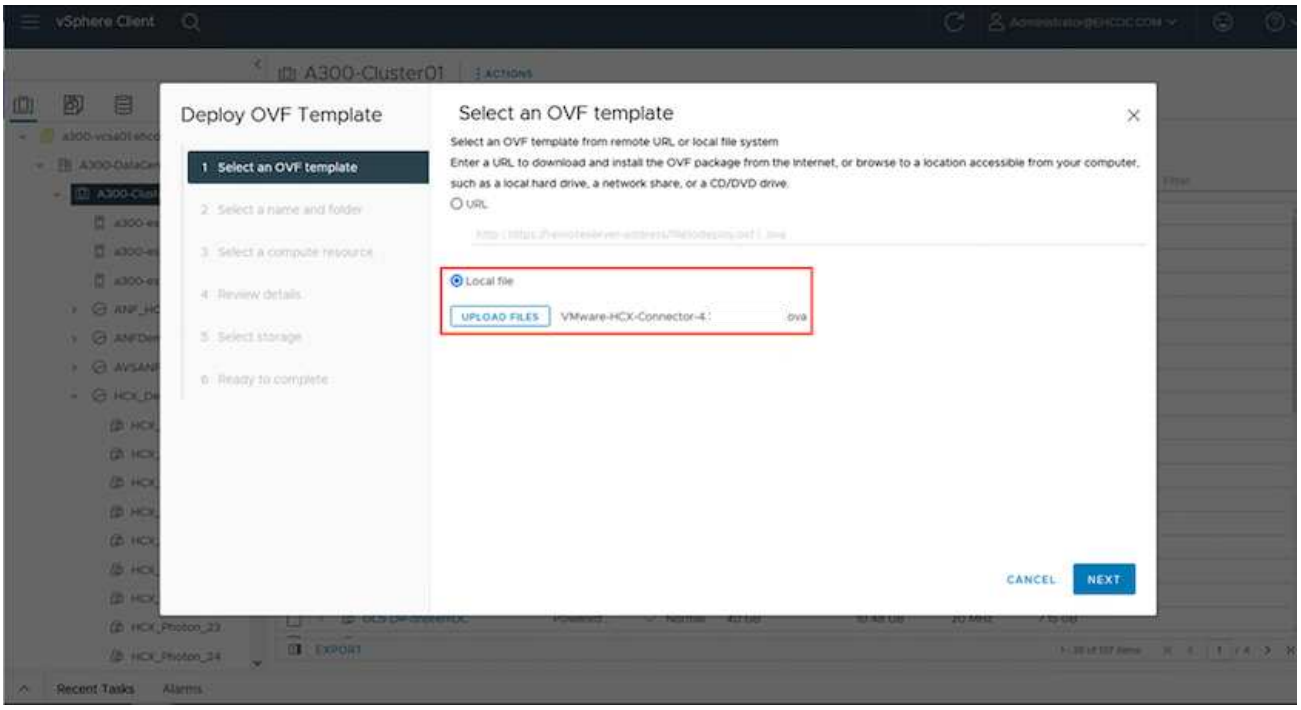


4. Após a conclusão da implantação, valide-a confirmando se o HCX Manager e seus plug-ins associados estão disponíveis no vCenter Console.
5. Crie os firewalls do Management Gateway apropriados para abrir as portas necessárias para acessar o HCX Cloud Manager. O HCX Cloud Manager agora está pronto para as operações do HCX.

▼ **Etapa 2: implantar o instalador OVA no vCenter Server local**

Para que o Conector local se comunique com o Gerenciador HCX no VMC, certifique-se de que as portas de firewall apropriadas estejam abertas no ambiente local.

1. No Console do VMC, navegue até o Painel do HCX, vá para Administração e selecione a guia Atualização de sistemas. Clique em Solicitar um link de download para a imagem OVA do conector HCX.
2. Com o conector HCX baixado, implante o OVA no vCenter Server local. Clique com o botão direito do mouse em vSphere Cluster e selecione a opção Implantar modelo OVF.

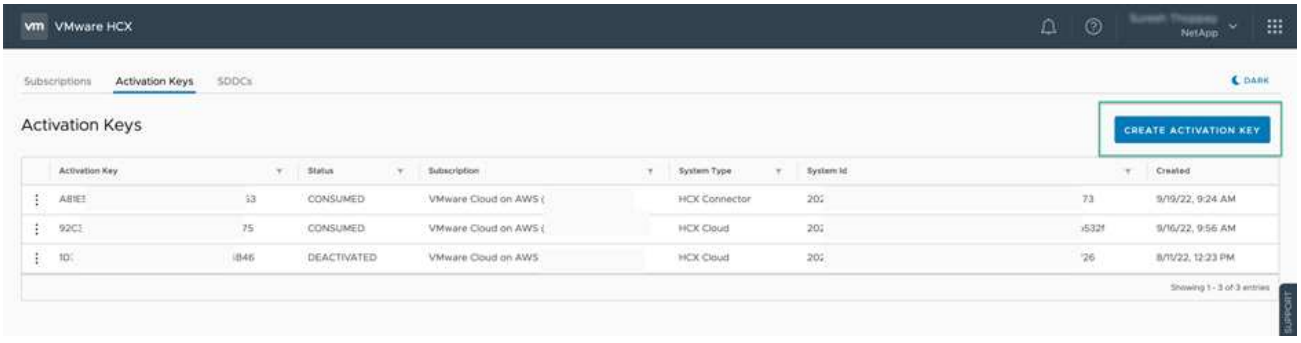


3. Insira as informações necessárias no assistente Implantar modelo OVF, clique em Avançar e depois Concluir para implantar o VMware HCX Connector OVA.
4. Ligue o dispositivo virtual manualmente. Para obter instruções passo a passo, acesse "Guia do usuário do VMware HCX" .

▼ **Etapa 3: Ative o HCX Connector com a chave de licença**

Depois de implantar o VMware HCX Connector OVA no local e iniciar o dispositivo, conclua as seguintes etapas para ativar o HCX Connector. Gere a chave de licença do VMware HCX Console no VMC e insira a licença durante a configuração do VMware HCX Connector.

1. No VMware Cloud Console, acesse Inventário, selecione o SDDC e clique em Exibir detalhes. Na guia Complementos, no bloco VMware HCX, clique em Abrir HCX.
2. Na aba Chaves de ativação, clique em Criar chave de ativação. Selecione o Tipo de Sistema como Conector HCX e clique em Confirmar para gerar a chave. Copie a chave de ativação.



Uma chave separada é necessária para cada conector HCX implantado no local.

3. Efetue login no VMware HCX Connector local em "`https://hcxconnectorIP:9443`" usando credenciais de administrador.

Use a senha definida durante a implantação do OVA.

4. Na seção Licenciamento, insira a chave de ativação copiada da etapa 2 e clique em Ativar.

O conector HCX local deve ter acesso à Internet para que a ativação seja concluída com sucesso.

5. Em Local do datacenter, forneça o local desejado para instalar o VMware HCX Manager no local. Clique em Continuar.
6. Em Nome do sistema, atualize o nome e clique em Continuar.
7. Selecione Sim e depois Continuar.
8. Em Conectar seu vCenter, forneça o endereço IP ou nome de domínio totalmente qualificado (FQDN) e as credenciais para o vCenter Server e clique em Continuar.

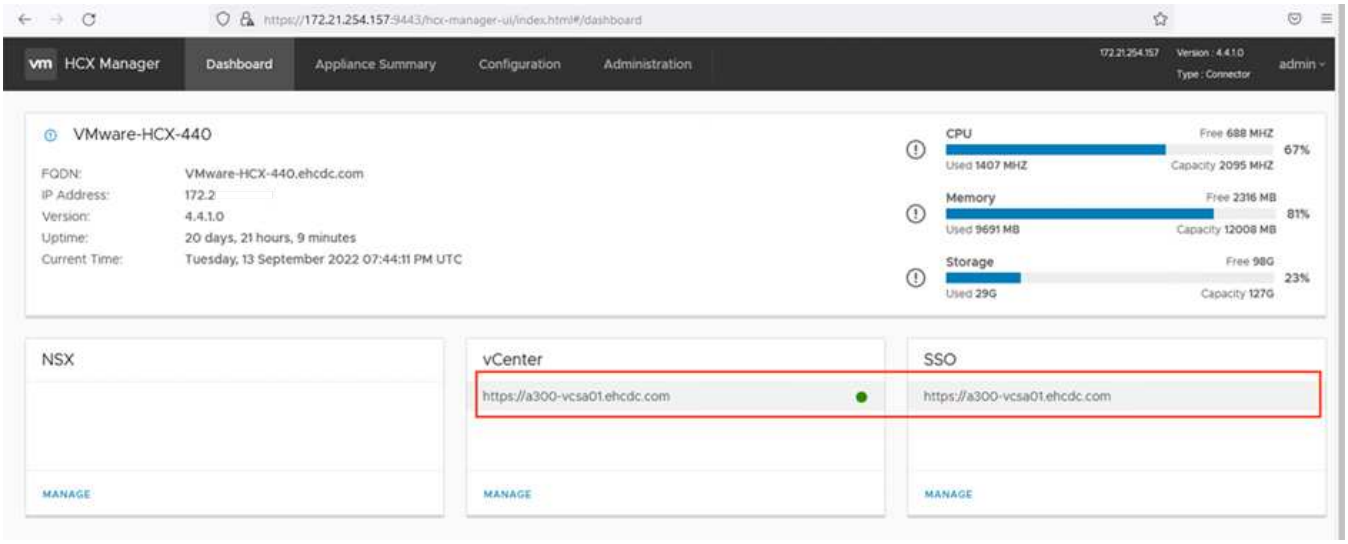
Use o FQDN para evitar problemas de comunicação mais tarde.

9. Em Configurar SSO/PSC, forneça o FQDN ou endereço IP do Platform Services Controller e clique em Continuar.

Digite o endereço IP ou FQDN do vCenter Server.

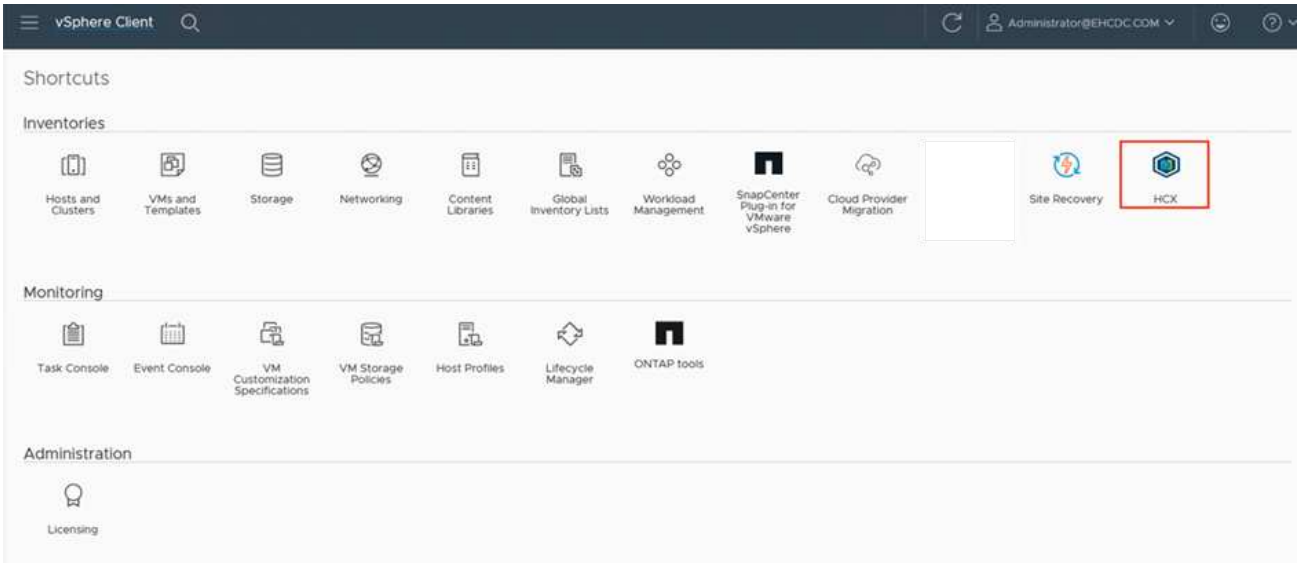
10. Verifique se as informações foram inseridas corretamente e clique em Reiniciar.
11. Após a conclusão, o vCenter Server é exibido em verde. Tanto o vCenter Server quanto o SSO devem ter os parâmetros de configuração corretos, que devem ser os mesmos da página anterior.

Esse processo deve levar aproximadamente 10 a 20 minutos para que o plug-in seja adicionado ao vCenter Server.

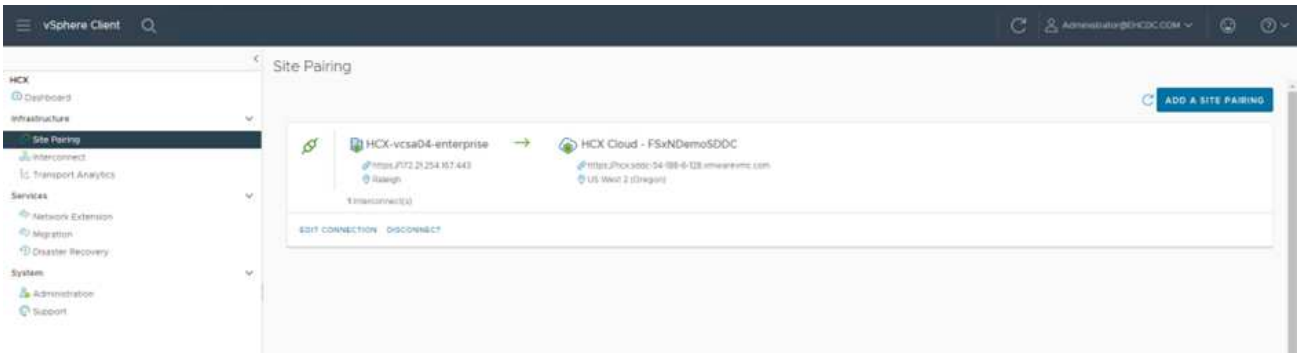


▼ **Etapa 4: Emparelhe o VMware HCX Connector local com o VMC HCX Cloud Manager**

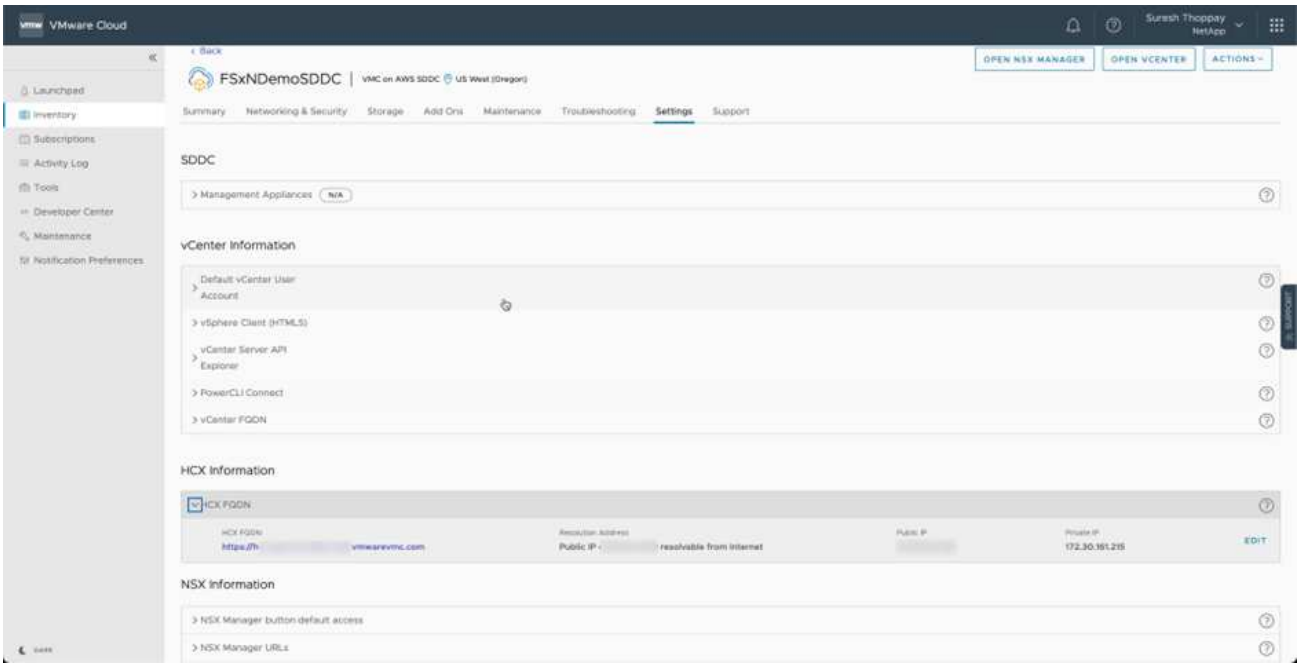
1. Para criar um par de sites entre o vCenter Server local e o VMC SDDC, faça login no vCenter Server local e acesse o HCX vSphere Web Client Plug-in.

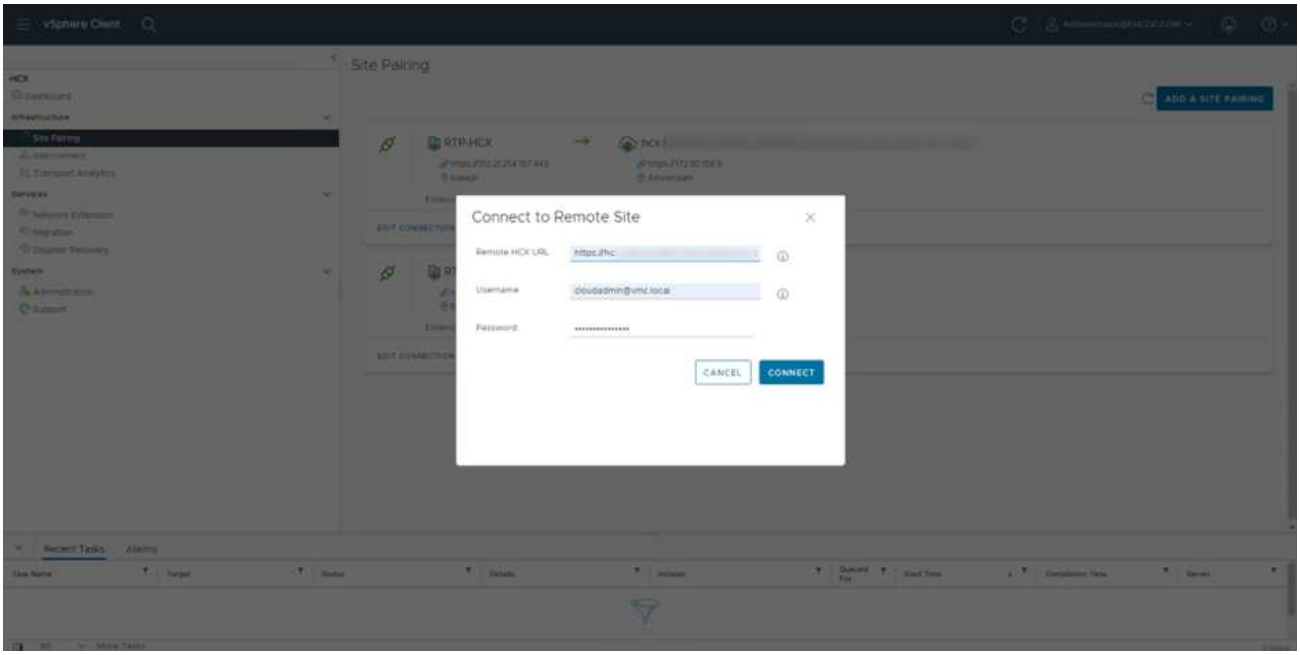


2. Em Infraestrutura, clique em Adicionar um pareamento de sites. Para autenticar o site remoto, insira o URL ou endereço IP do VMC HCX Cloud Manager e as credenciais para a função CloudAdmin.



As informações do HCX podem ser recuperadas na página Configurações do SDDC.





3. Para iniciar o pareamento do site, clique em Conectar.

> O VMware HCX Connector deve ser capaz de se comunicar com o IP do HCX Cloud Manager pela porta 443.

4. Após a criação do pareamento, o pareamento do site recém-configurado fica disponível no Painel do HCX.

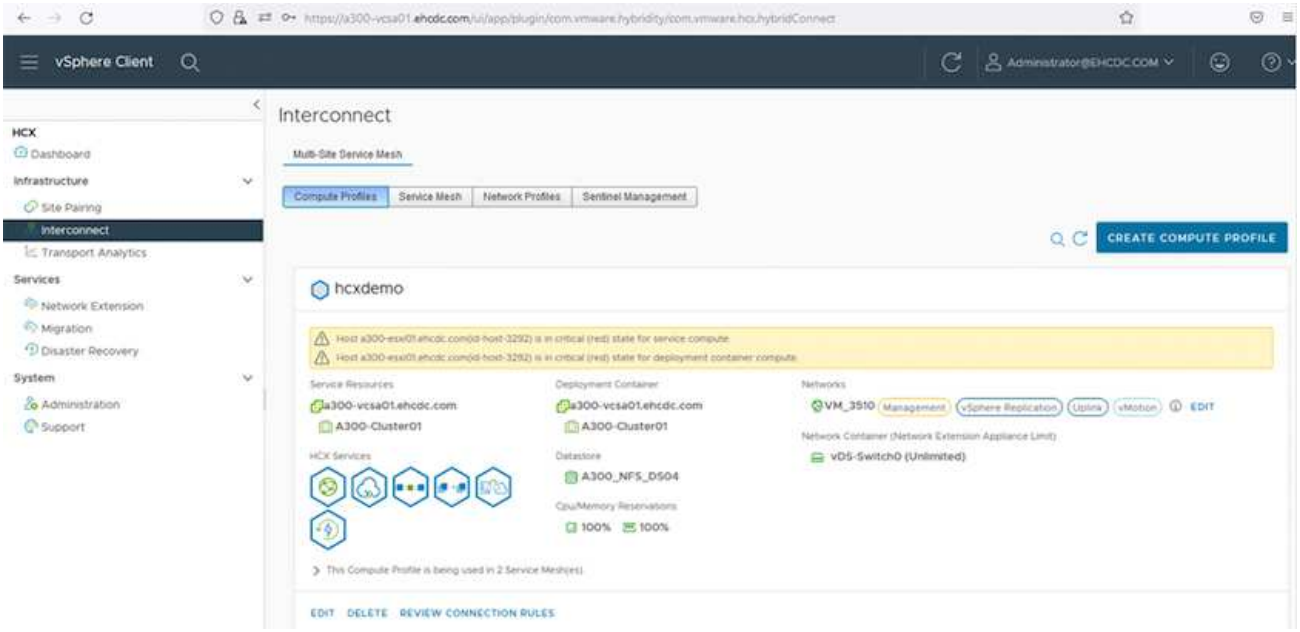
▼ **Etapa 5: configurar o perfil de rede, o perfil de computação e a malha de serviço**

O dispositivo VMware HCX Interconnect (HCX-IX) fornece recursos de túnel seguro pela Internet e conexões privadas com o site de destino que permitem replicação e recursos baseados em vMotion. A interconexão fornece criptografia, engenharia de tráfego e uma SD-WAN. Para criar o HCI-IX Interconnect Appliance, conclua as seguintes etapas:

1. Em Infraestrutura, selecione Interconexão > Malha de serviços multisite > Perfis de computação > Criar perfil de computação.

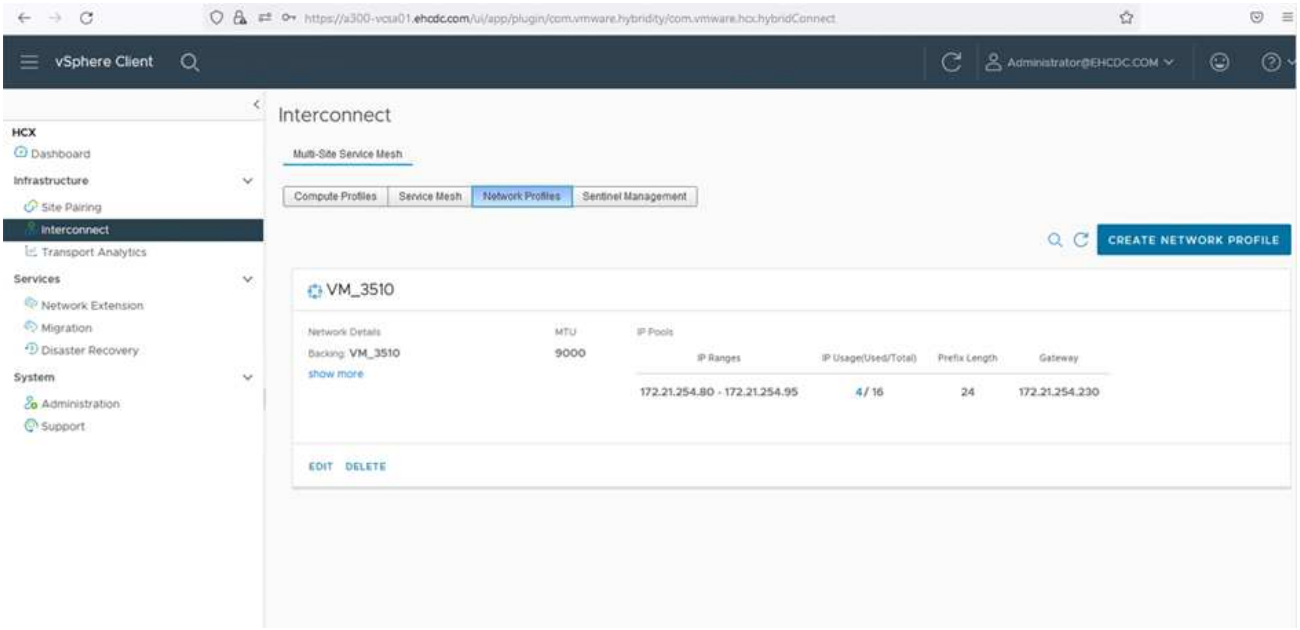
> Os perfis de computação contêm os parâmetros de computação, armazenamento e implantação de rede necessários para implantar um dispositivo virtual de interconexão. Eles também especificam qual parte do data center VMware estará acessível ao serviço HCX.

Para obter instruções detalhadas, consulte "Criando um Perfil de Computação" .



2. Após a criação do perfil de computação, crie o perfil de rede selecionando Multi-Site Service Mesh > Perfis de rede > Criar perfil de rede.
3. O perfil de rede define um intervalo de endereços IP e redes que serão usados pelo HCX para seus dispositivos virtuais.

> Isso exigirá dois ou mais endereços IP. Esses endereços IP serão atribuídos pela rede de gerenciamento aos dispositivos virtuais.



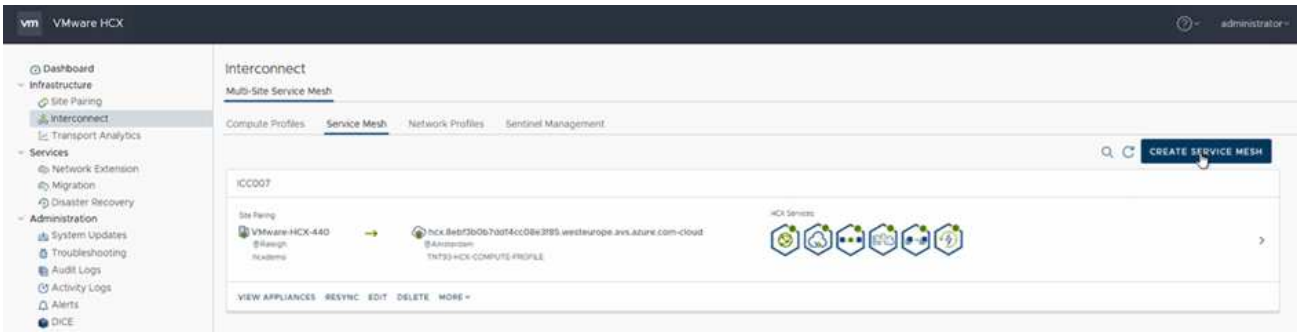
Para obter instruções detalhadas, consulte "Criando um perfil de rede" .

> Se você estiver se conectando a uma SD-WAN pela Internet, precisará reservar IPs públicos na seção Rede e Segurança.

4. Para criar uma malha de serviço, selecione a guia Malha de serviço na opção Interconexão e selecione

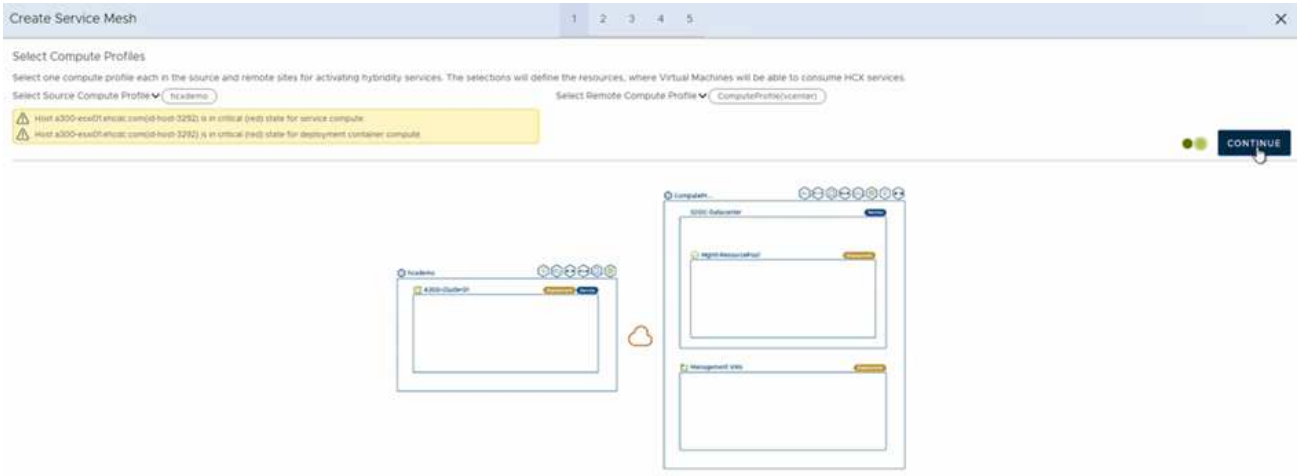
sites locais e VMC SDDC.

A malha de serviço estabelece um par de perfis de computação e rede locais e remotos.

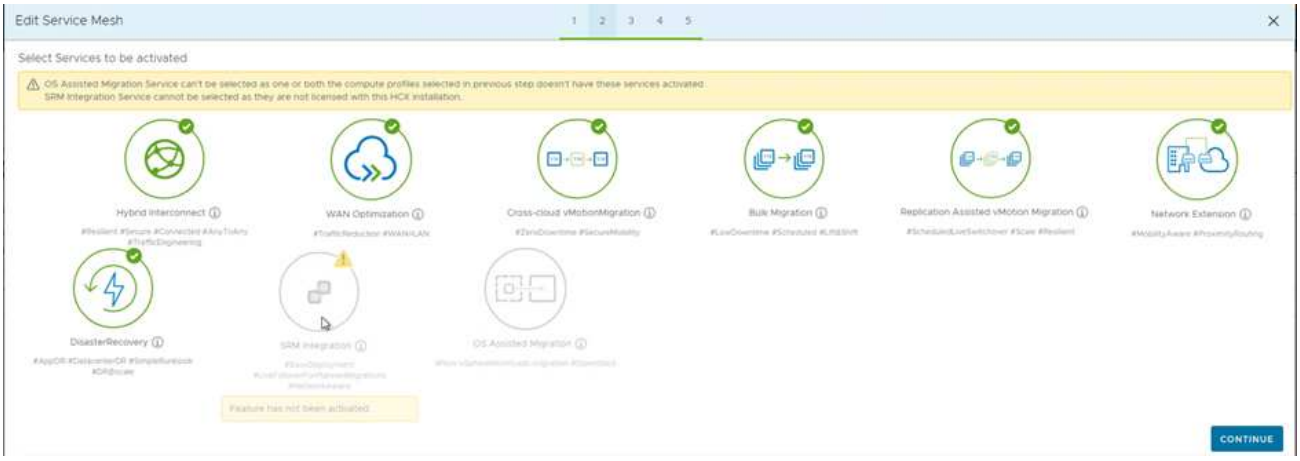


Parte desse processo envolve a implantação de dispositivos HCX que serão configurados automaticamente nos sites de origem e de destino, criando uma estrutura de transporte segura.

5. Selecione os perfis de computação de origem e remota e clique em Continuar.

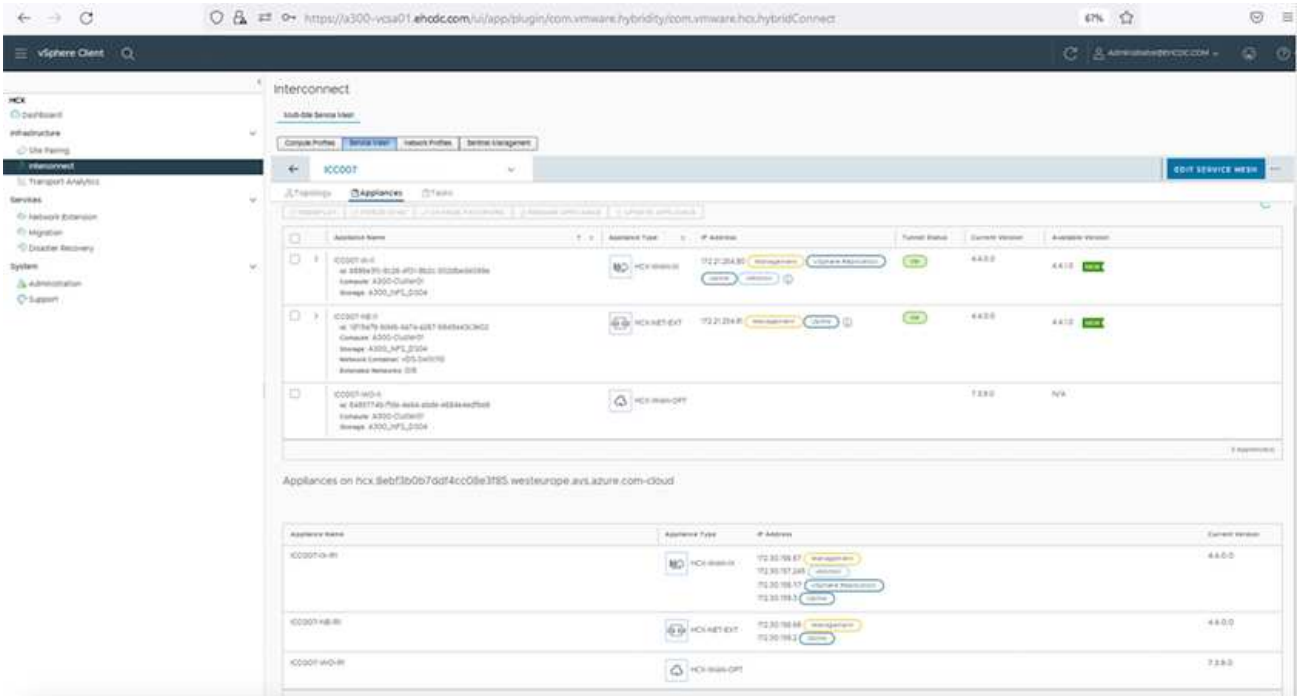


6. Selecione o serviço a ser ativado e clique em Continuar.



Uma licença HCX Enterprise é necessária para migração vMotion assistida por replicação, integração com SRM e migração assistida por sistema operacional.

7. Crie um nome para a malha de serviço e clique em Concluir para iniciar o processo de criação. A implantação deve levar aproximadamente 30 minutos para ser concluída. Após a configuração da malha de serviço, a infraestrutura virtual e a rede necessárias para migrar as VMs de carga de trabalho foram criadas.



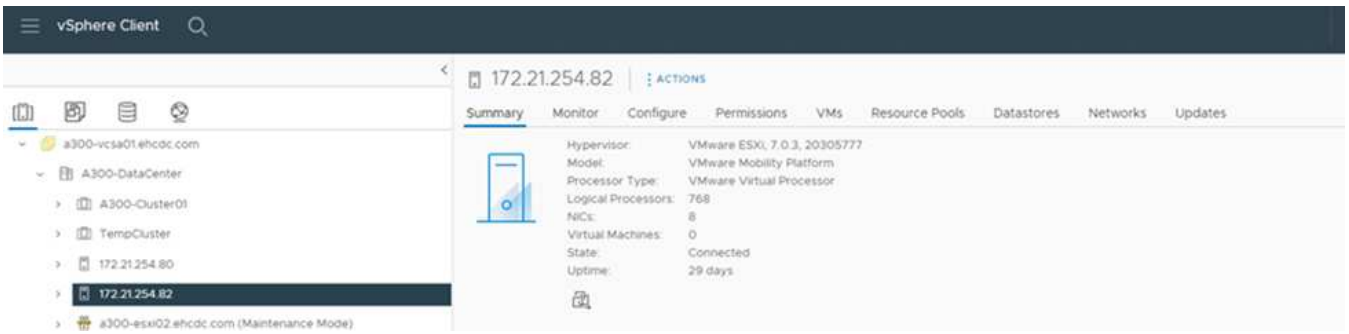
▼ Etapa 6: Migrando cargas de trabalho

O HCX fornece serviços de migração bidirecional entre dois ou mais ambientes distintos, como SDDCs locais e VMC. As cargas de trabalho de aplicativos podem ser migradas de e para sites ativados pelo HCX usando uma variedade de tecnologias de migração, como migração em massa do HCX, HCX vMotion, migração a frio do HCX, HCX Replication Assisted vMotion (disponível com a edição HCX Enterprise) e HCX OS Assisted Migration (disponível com a edição HCX Enterprise).

Para saber mais sobre as tecnologias de migração HCX disponíveis, consulte "Tipos de migração do VMware HCX"

O dispositivo HCX-IX usa o serviço Mobility Agent para executar migrações vMotion, Cold e Replication Assisted vMotion (RAV).

O dispositivo HCX-IX adiciona o serviço Mobility Agent como um objeto de host no vCenter Server. Os recursos de processador, memória, armazenamento e rede exibidos neste objeto não representam o consumo real no hipervisor físico que hospeda o dispositivo IX.

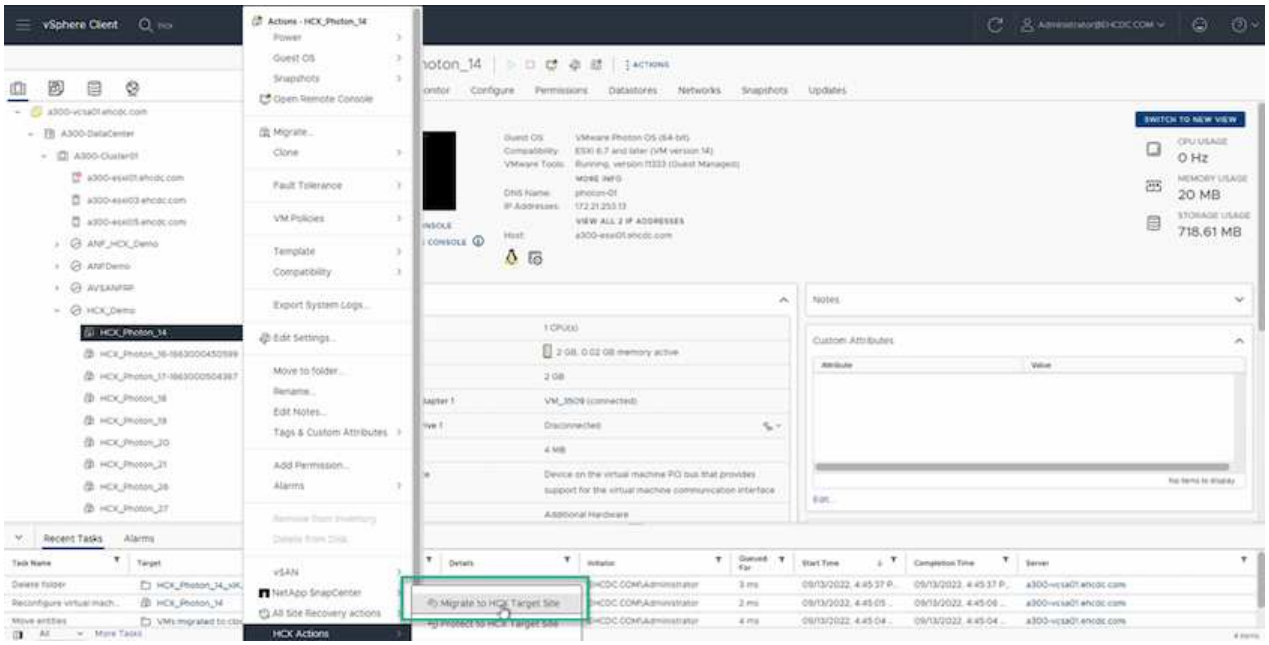


▼ VMware HCX vMotion

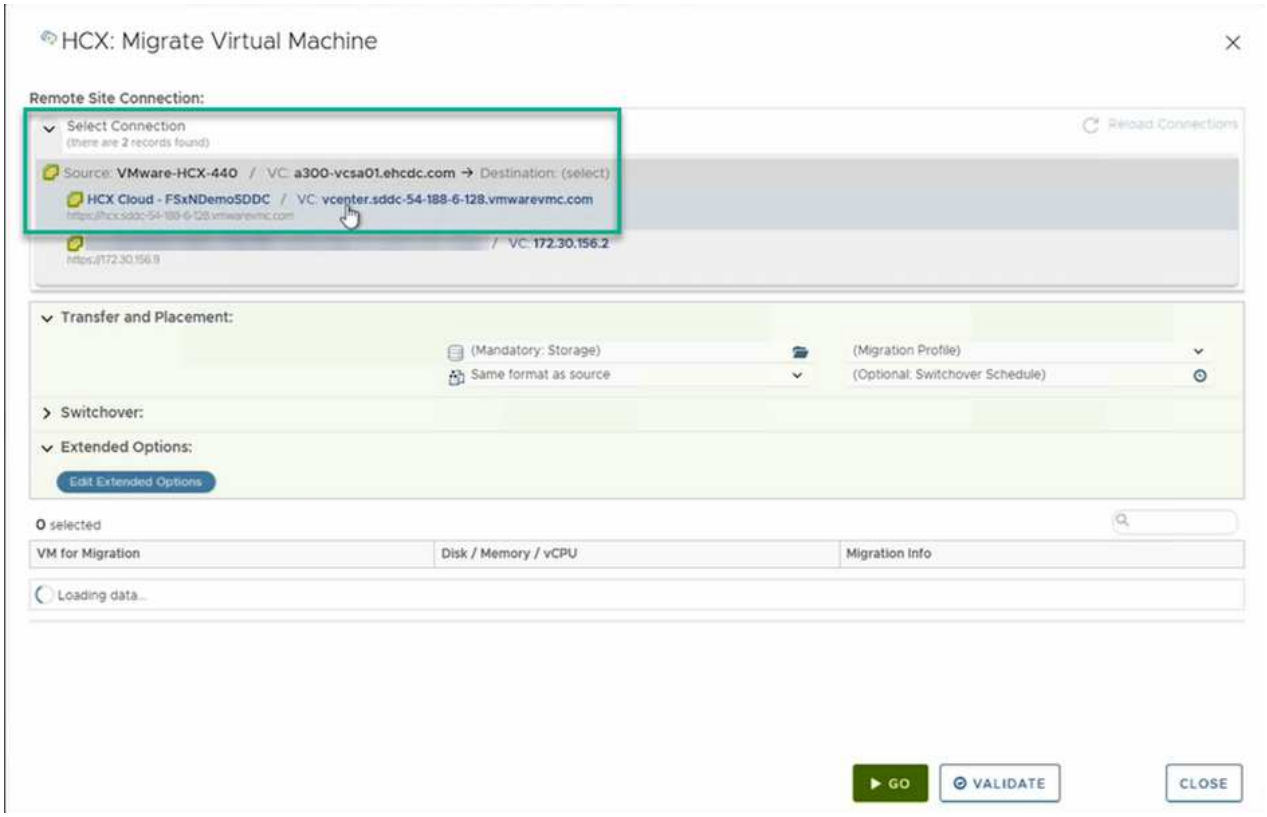
Esta seção descreve o mecanismo HCX vMotion. Esta tecnologia de migração usa o protocolo VMware vMotion para migrar uma VM para o VMC SDDC. A opção de migração vMotion é usada para migrar o estado de uma única VM por vez. Não há interrupção de serviço durante este método de migração.

> ⓘ A extensão de rede deve estar em vigor (para o grupo de portas no qual a VM está conectada) para migrar a VM sem a necessidade de fazer uma alteração de endereço IP.

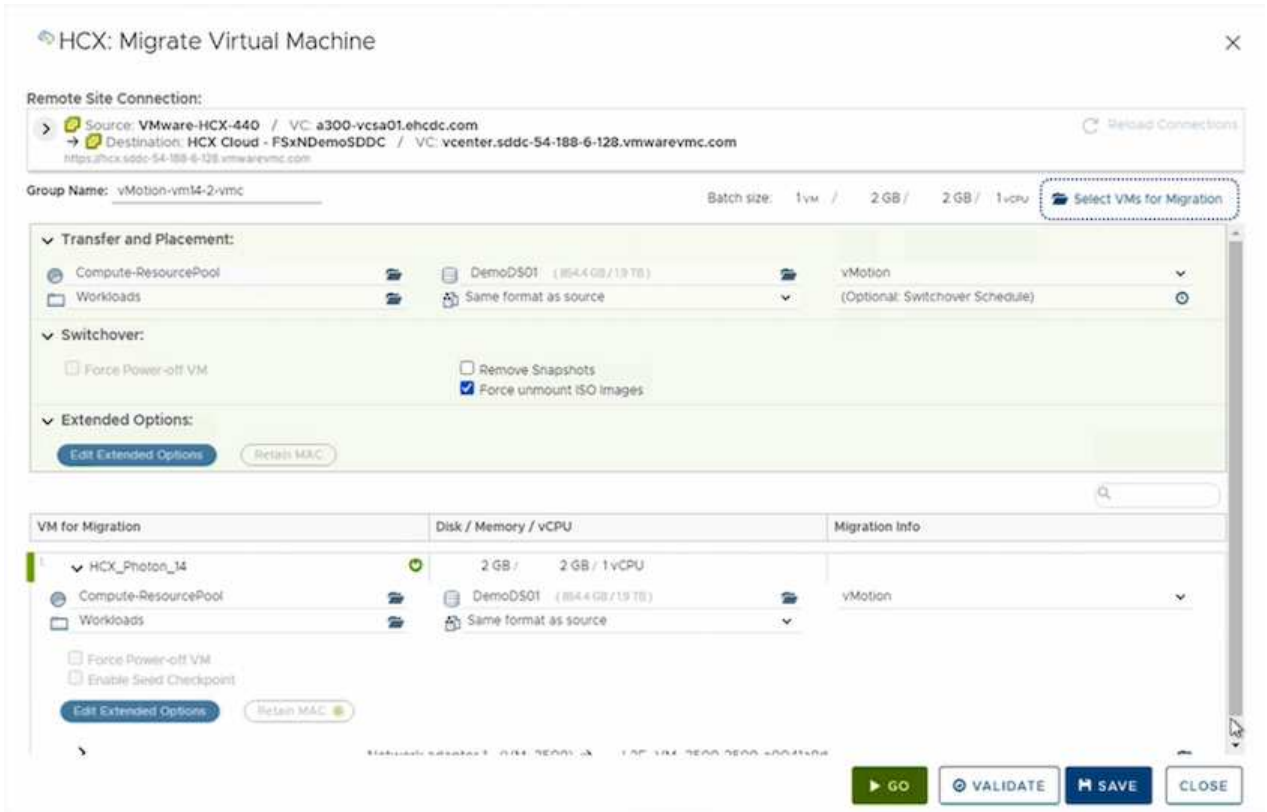
1. No cliente vSphere local, acesse Inventário, clique com o botão direito do mouse na VM a ser migrada e selecione Ações do HCX > Migrar para o site de destino do HCX.



2. No assistente Migrar Máquina Virtual, selecione Conexão de Site Remoto (VMC de destino SDDC).



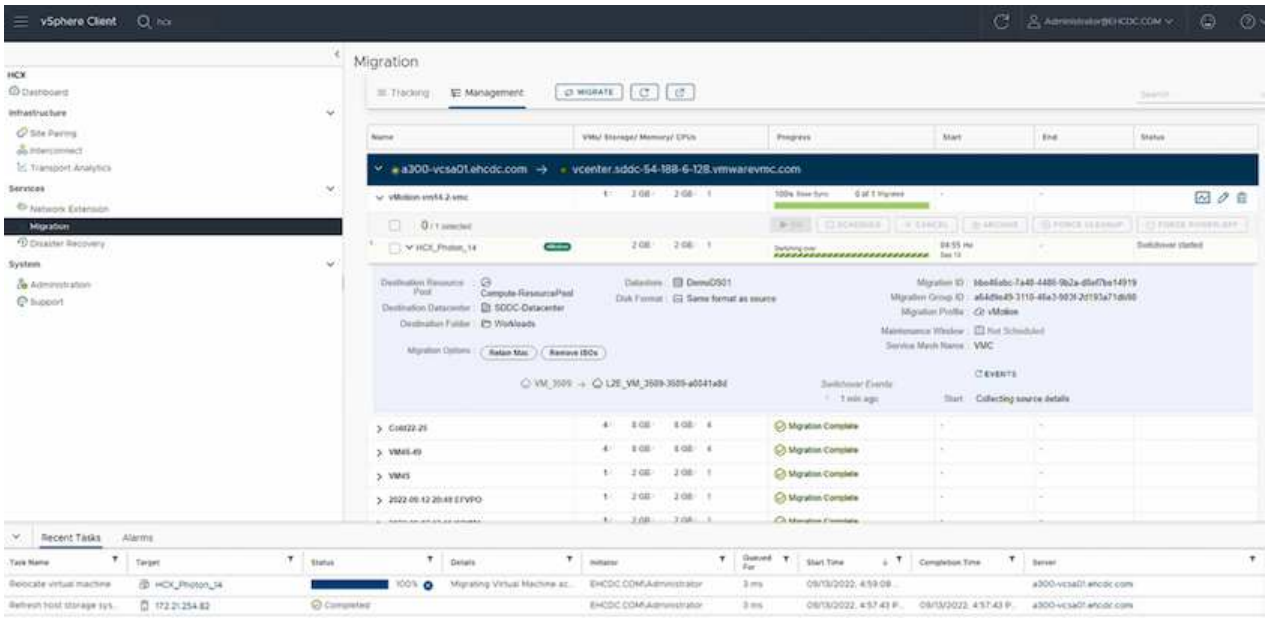
3. Adicione um nome de grupo e, em Transferência e posicionamento, atualize os campos obrigatórios (Cluster, Armazenamento e Rede de destino). Clique em Validar.



4. Após a conclusão das verificações de validação, clique em Ir para iniciar a migração.

A transferência vMotion captura a memória ativa da VM, seu estado de execução, seu endereço IP e seu endereço MAC. Para obter mais informações sobre os requisitos e limitações do HCX vMotion, consulte "Compreendendo o VMware HCX vMotion e a migração a frio" .

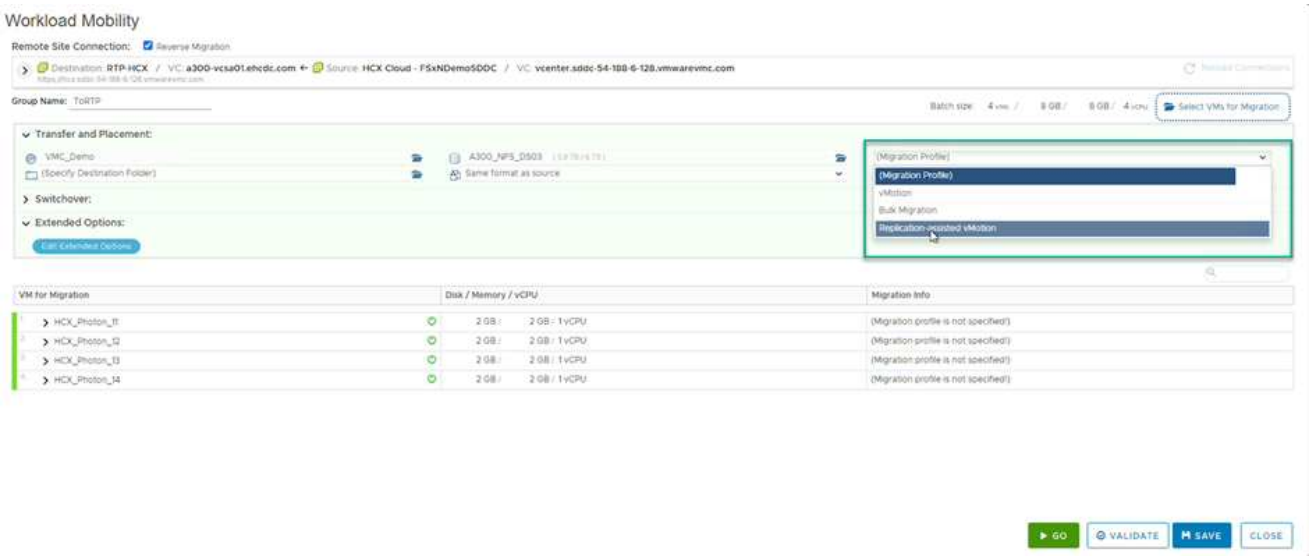
5. Você pode monitorar o progresso e a conclusão do vMotion no painel HCX > Migração.



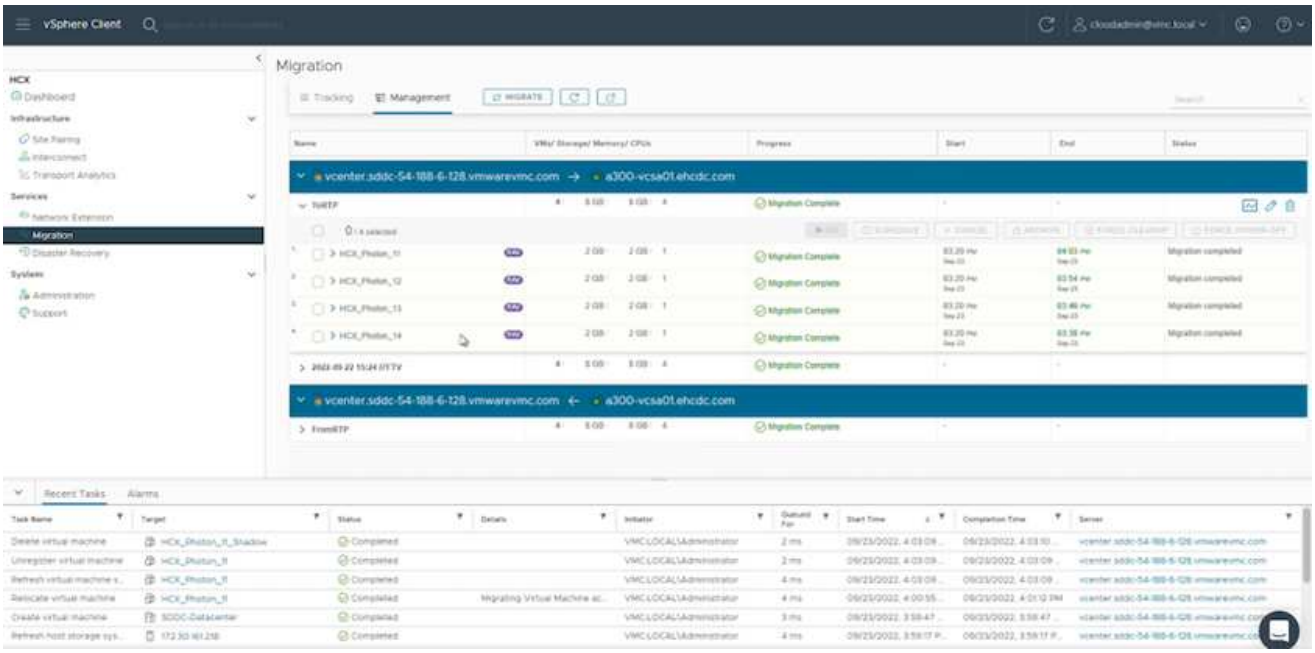
▼ **VMware Replication Assisted vMotion**

Como você deve ter notado na documentação da VMware, o VMware HCX Replication Assisted vMotion (RAV) combina os benefícios da migração em massa e do vMotion. A migração em massa usa o vSphere Replication para migrar várias VMs em paralelo — a VM é reinicializada durante a alternância. O HCX vMotion migra sem tempo de inatividade, mas é executado em série, uma VM por vez em um grupo de replicação. O RAV replica a VM em paralelo e a mantém sincronizada até a janela de alternância. Durante o processo de troca, ele migra uma VM por vez, sem tempo de inatividade para a VM.

A captura de tela a seguir mostra o perfil de migração como Replication Assisted vMotion.



A duração da replicação pode ser maior em comparação ao vMotion de um pequeno número de VMs. Com RAV, sincronize apenas os deltas e inclua o conteúdo da memória. A seguir está uma captura de tela do status da migração — ela mostra como o horário de início da migração é o mesmo e o horário de término é diferente para cada VM.



Para obter informações adicionais sobre as opções de migração do HCX e sobre como migrar cargas de trabalho do local para o VMware Cloud na AWS usando o HCX, consulte o "Guia do usuário do VMware HCX" .

O VMware HCX vMotion requer capacidade de transferência de 100 Mbps ou superior.

O armazenamento de dados VMC FSx ONTAP de destino deve ter espaço suficiente para acomodar a migração.

Conclusão

Não importa se você está mirando em nuvem completa ou híbrida e dados residindo em qualquer tipo/fornecedor de armazenamento no local, o Amazon FSx ONTAP junto com o HCX oferecem excelentes opções para implantar e migrar as cargas de trabalho, ao mesmo tempo em que reduzem o TCO ao tornar os requisitos de dados integrados à camada de aplicativo. Seja qual for o caso de uso, escolha o VMC junto com o datastore FSx ONTAP para rápida concretização dos benefícios da nuvem, infraestrutura consistente e operações no local e em várias nuvens, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial. É o mesmo processo e procedimento familiar usado para conectar o armazenamento e migrar VMs usando replicação VMware vSphere, VMware vMotion ou até mesmo cópia NFC.

Takeaways

Os pontos principais deste documento incluem:

- Agora você pode usar o Amazon FSx ONTAP como um armazenamento de dados com o VMC SDDC.
- Você pode migrar facilmente dados de qualquer datacenter local para o VMC em execução com o armazenamento de dados FSx ONTAP

- Você pode facilmente aumentar e diminuir o armazenamento de dados do FSx ONTAP para atender aos requisitos de capacidade e desempenho durante a atividade de migração.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes links do site:

- Documentação do VMware Cloud

  "https://docs.vmware.com/en/VMware-Cloud-on-AWS/"

- Documentação do Amazon FSx ONTAP

  "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide"

  Guia do usuário do VMware HCX

- "https://techdocs.broadcom.com/us/en/vmware-cis/hcx/vmware-hcx/4-10/vmware-hcx-user-guide-4-10.html"

NetApp para AWS / EVS

Monte o FSx ONTAP como armazenamento de dados externo para EVS

Como montar o Amazon FSx for NetApp ONTAP como um armazenamento de dados externo para o Amazon Elastic VMware Service

Este documento apresentará etapas detalhadas para criar um FSx para sistema de arquivos ONTAP e anexá-lo para uso como um armazenamento de dados de interface de sistema de computadores pequenos da Internet (iSCSI) ou de sistema de arquivos de rede (NFS) para uso com o Amazon EVS.

Introdução

Organizações com investimentos existentes em VMware local que buscam maneiras eficientes e econômicas de modernizar suas implantações migrando, distribuindo, estendendo ou protegendo (backup, recuperação de desastres) cópias na AWS enfrentaram vários desafios. Com o lançamento do Amazon Elastic VMware Service (Amazon EVS), agora há um serviço nativo da AWS que possibilita executar o VMware Cloud Foundation (VCF) diretamente em uma Amazon Virtual Private Cloud (VPC).

O Amazon EVS possibilita estender implantações de VCF existentes para a AWS, expandir na AWS para aumentar o desempenho durante o pico de uso e executar cargas de trabalho de VCF inteiramente na AWS para facilitar modernizações, saídas de data centers, consolidações e outros casos de uso.

Embora o Amazon EVS ofereça grandes benefícios, a arquitetura hiperconvergente padrão acopla computação e armazenamento, impedindo a escala independente de um ou outro conforme as necessidades do negócio. No mundo atual centrado em dados, as demandas de armazenamento em muitas organizações são maiores do que as de computação. No entanto, com a arquitetura hiperconvergente da VMware, os recursos de armazenamento são acoplados aos recursos de computação. Isso significa que o dimensionamento do armazenamento só pode ser feito adicionando hosts de computação que nunca serão usados. É uma situação que pode aumentar os custos consideravelmente, especialmente em cargas de trabalho com uso intenso de armazenamento.

Para resolver esse problema, a AWS e a NetApp oferecem o Amazon FSx for NetApp ONTAP (FSx para ONTAP) como serviço de armazenamento externo para o Amazon EVS. O FSx for ONTAP é um serviço de armazenamento nativo da AWS que oferece alto desempenho, resiliência de dados e recursos de custo-benefício do software NetApp ONTAP . Ao usar o FSx for ONTAP como armazenamento externo, os usuários do Amazon EVS podem dimensionar recursos de computação e armazenamento de forma independente, permitindo um custo total de propriedade (TCO) ideal.

Visão geral

Este documento apresentará etapas detalhadas para criar um FSx para sistema de arquivos ONTAP e anexá-lo para uso como um armazenamento de dados de interface de sistema de computadores pequenos da Internet (iSCSI) ou de sistema de arquivos de rede (NFS) para uso com o Amazon EVS.

Objetivo deste Guia

Este guia fornece instruções sobre como configurar um armazenamento de dados FSx for ONTAP para o Amazon EVS, bem como práticas recomendadas, requisitos de suporte, considerações de dimensionamento e outras informações para ajudar você a planejar, projetar e implementar a integração.

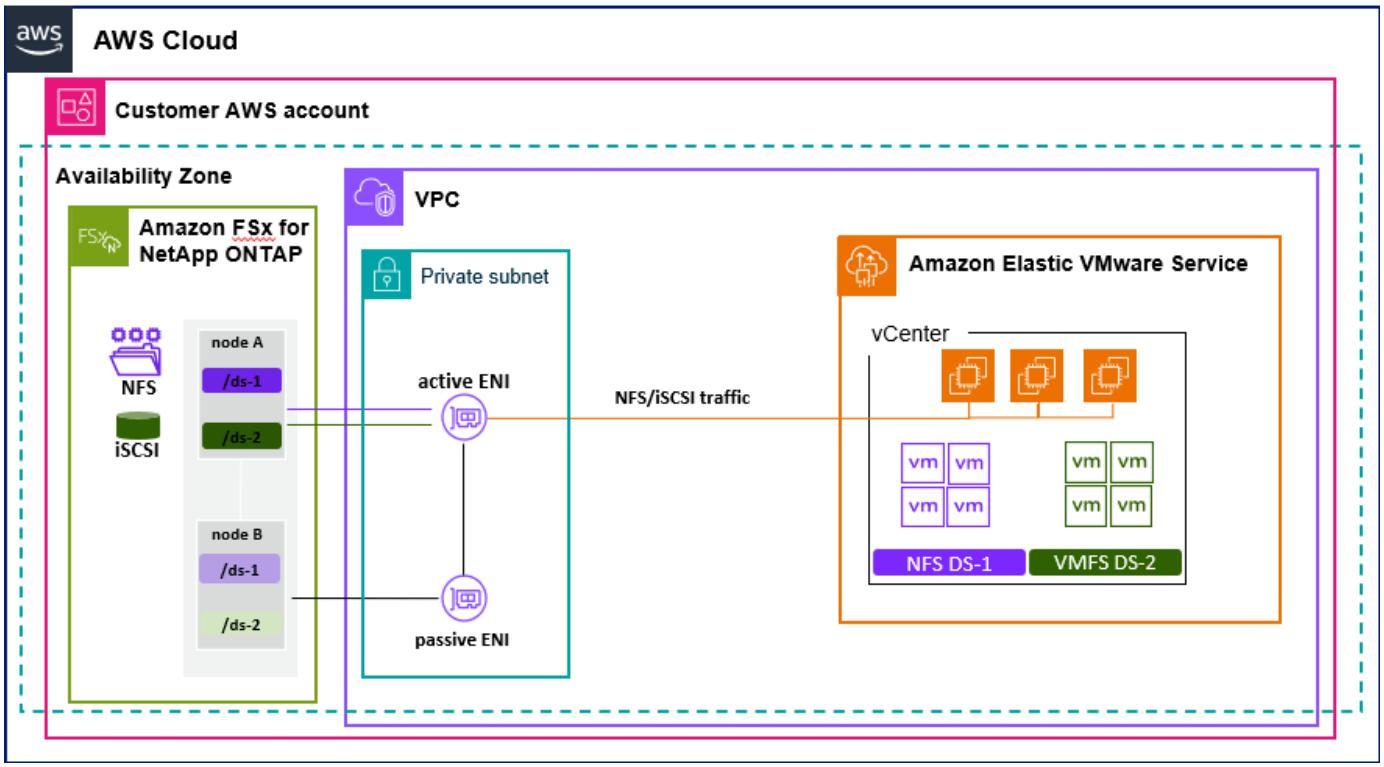
Público

Este tutorial é destinado a arquitetos e administradores de nuvem familiarizados com VMware vSphere, Amazon EVS, AWS Console e FSx for ONTAP.

Arquitetura de alto nível

Nesta seção, daremos uma visão geral da arquitetura da solução para usar o FSx for ONTAP como um armazenamento de dados para o Amazon EVS.

Abaixo você pode ver uma visão geral da arquitetura do armazenamento de dados FSx for ONTAP com um ambiente Amazon EVS dentro de uma VPC AWS.



Procedimento de implantação para usar FSx para ONTAP como um armazenamento de dados NFS

Esta seção mostrará as etapas sobre como implantar o FSx para ONTAP como um armazenamento de dados NFS. As etapas para implantar um armazenamento de dados iSCSI são detalhadas na próxima seção.

Etapas de implantação de alto nível

A implantação do sistema de arquivos FSx para ONTAP para uso como um armazenamento de dados NFS para o Amazon EVS e o estabelecimento de conectividade entre os dois serviços incluirão as seguintes etapas:

- Configurando um FSx para o sistema de arquivos ONTAP na mesma VPC onde o ambiente Amazon EVS VCF está localizado.
- Validando os grupos de segurança e a tabela de roteamento.
- Anexando um volume de armazenamento FSx para ONTAP para uso como um armazenamento de dados NFS para Amazon EVS.

Pré-requisitos

Os seguintes pré-requisitos devem estar em vigor antes de você iniciar o processo de configuração de um FSx para ONTAP como um armazenamento de dados NFS para o Amazon EVS:

- Um ambiente de virtualização Amazon EVS. Para obter mais informações sobre como fazer isso, consulte a documentação em"Guia de introdução ao Amazon EVS" .
- Crie uma Zona de Disponibilidade Única (AZ) FSx para ONTAP com capacidade de armazenamento SSD apropriada, IOPS provisionados e taxa de transferência.
- Para um desempenho ideal, coloque o FSx para o sistema de arquivos ONTAP na mesma VPC que a instância do Amazon EVS. Observe que o VPC Peering também é suportado nos casos em que o FSx for ONTAP é implantado em um VPC diferente.
- Com base nos requisitos de desempenho, selecione o IOPS e a taxa de transferência corretos necessários para um FSx Single-AZ para sistema de arquivos ONTAP . Ver"detalhes de especificação de desempenho para FSx para ONTAP" para entender a taxa de transferência e o IOPS que cada opção disponível fornece.



Neste guia, implantaremos o sistema de arquivos FSx para ONTAP na mesma sub-rede que a sub-rede de acesso ao serviço.

Depois que o ambiente de virtualização do Amazon EVS for implantado na VPC, você poderá prosseguir com a configuração do sistema de arquivos Single-AZ FSx para ONTAP que será usado como um armazenamento de dados NFS.



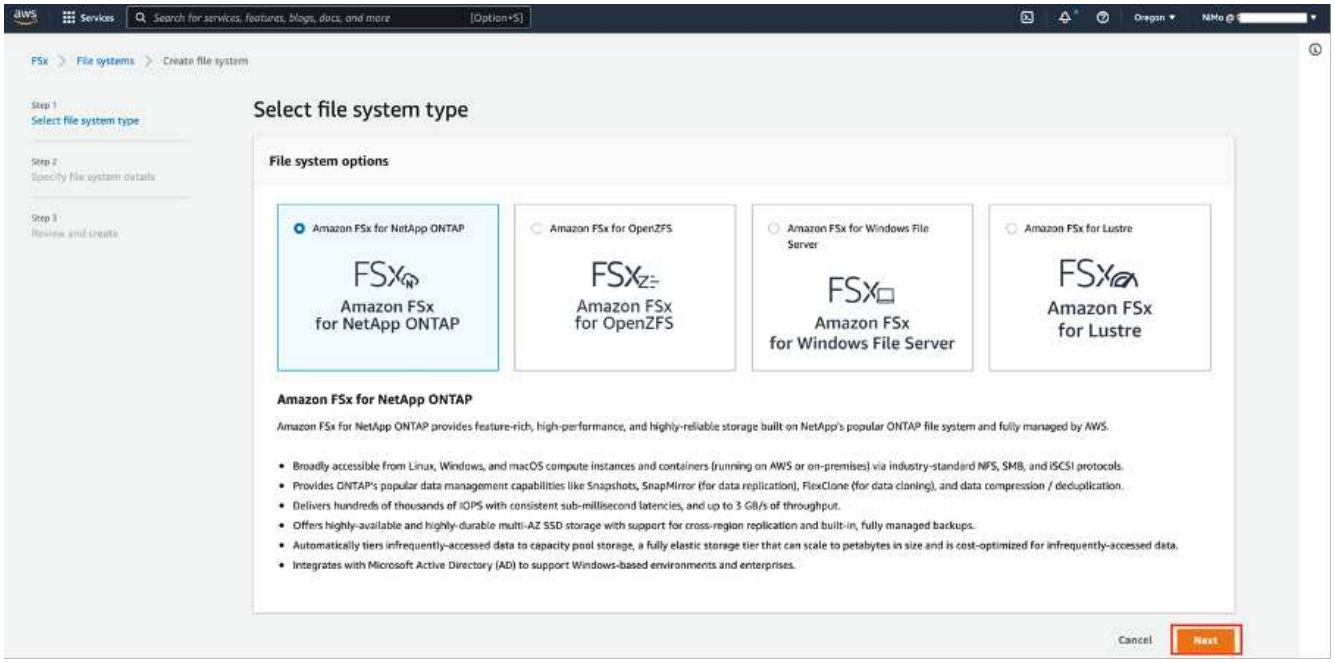
Seu sistema de arquivos FSx para ONTAP deve ser implantado na mesma AZ que o Amazon EVS SDDC.

Crie um FSx para o sistema de arquivos ONTAP

As etapas a seguir mostrarão como provisionar e montar um FSx para o sistema de arquivos ONTAP :

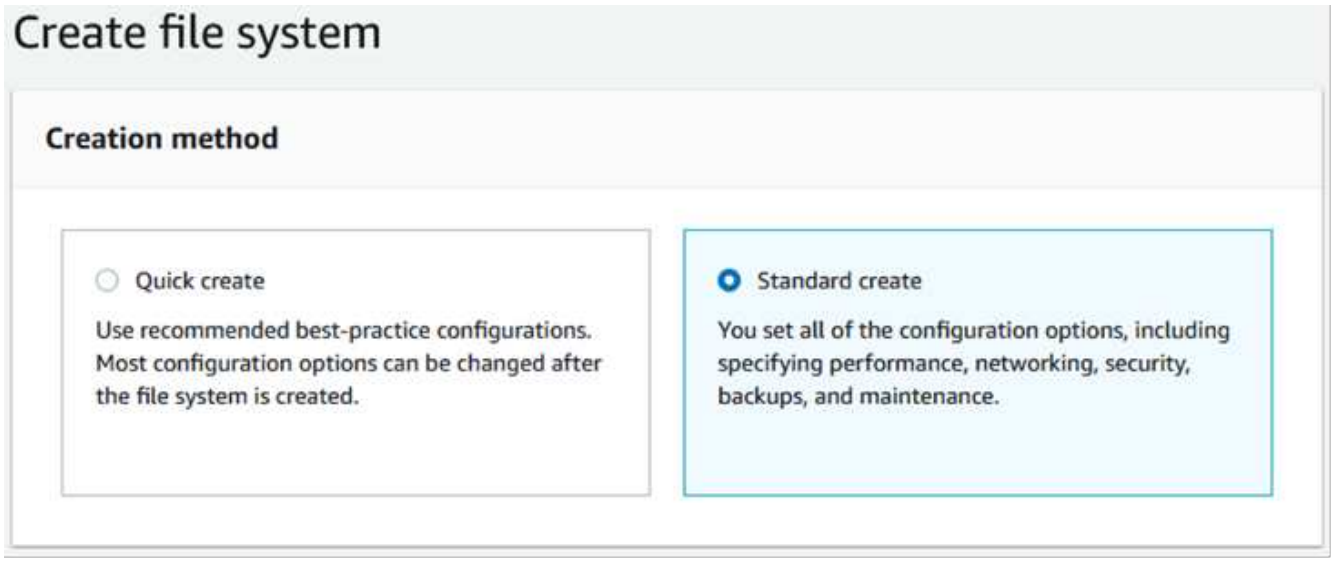
1. Acesse o Amazon FSx Console em `https://console.aws.amazon.com/fsx/` usando seu navegador de internet e faça login com suas credenciais.

2. No console, selecione Criar sistema de arquivos. Isso iniciará o assistente de configuração para criar um FSx para o sistema de arquivos ONTAP .
3. Primeiro, selecione o tipo de sistema de arquivos. Nas opções de sistema de arquivos disponíveis, selecione "Amazon FSx for NetApp ONTAP" e prossiga clicando no botão "Avançar".

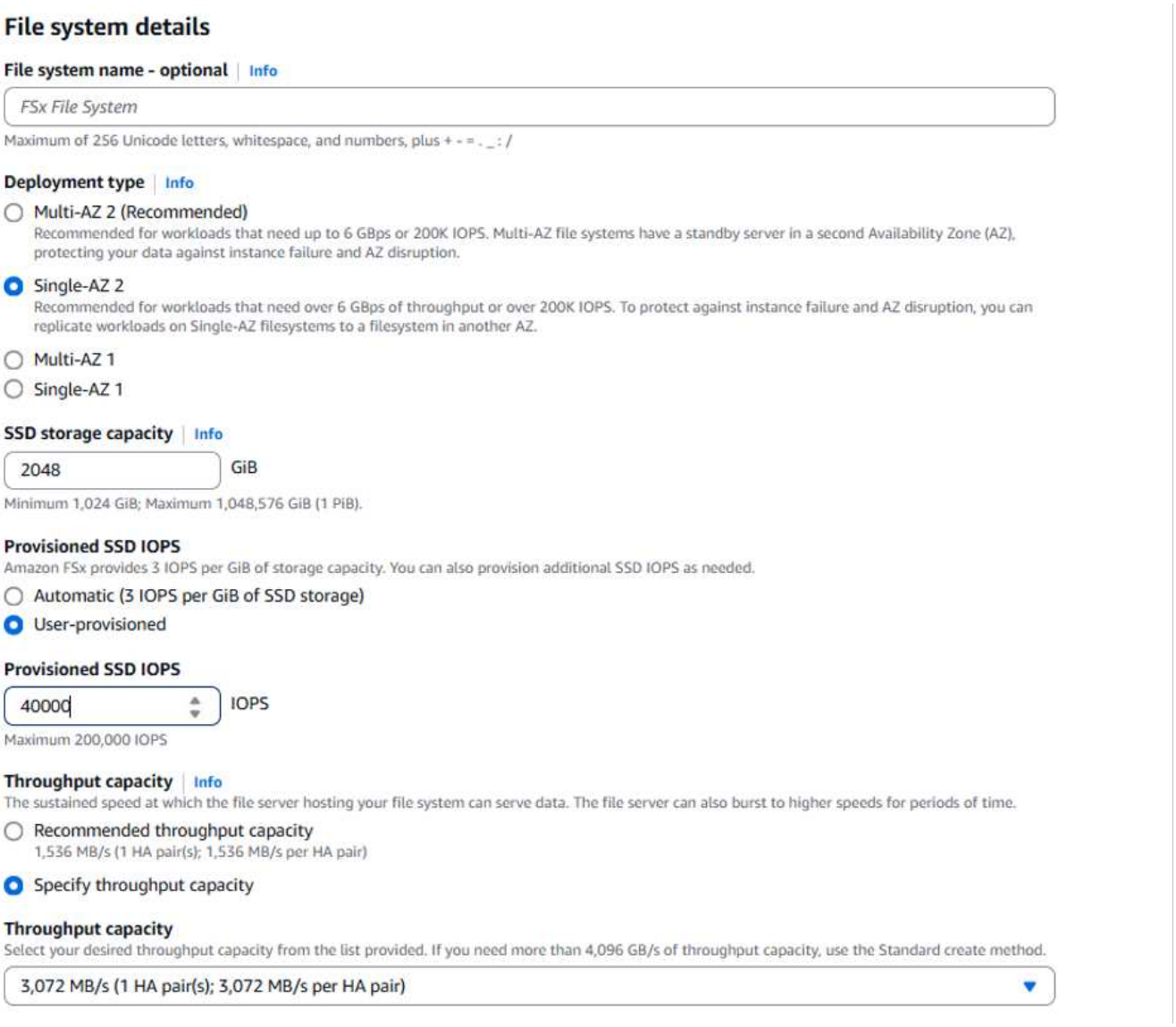


4. Você poderá escolher entre as opções Criação rápida e Criação padrão. A criação rápida oferece configurações predefinidas e a criação padrão permite que você defina suas próprias configurações.

   Selecione a opção "Criação padrão".

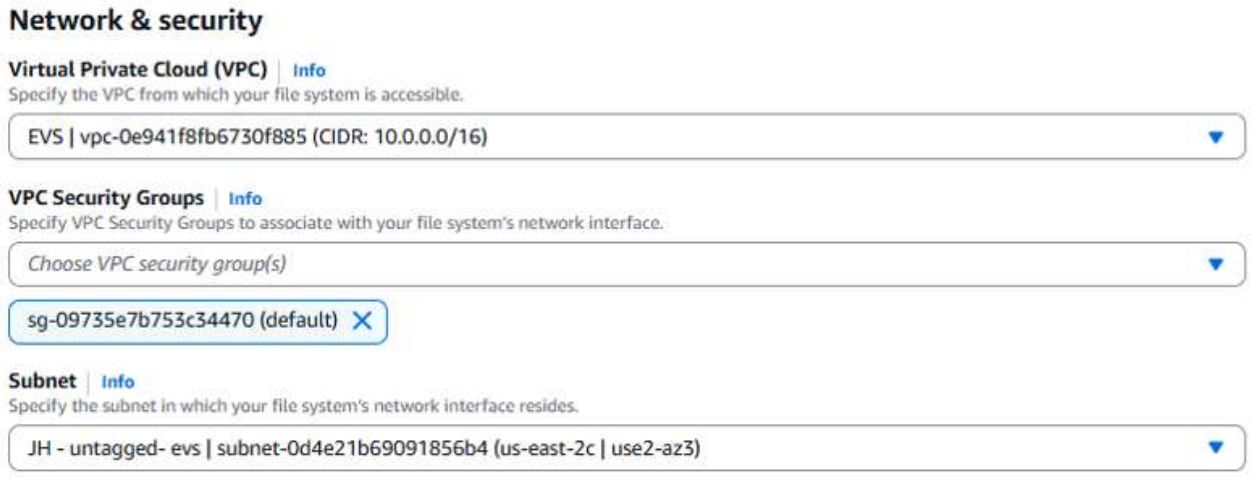


   Agora você estará no assistente de configuração do sistema de arquivos padrão. Na página de detalhes do sistema de arquivos, escolha e insira as mesmas informações mostradas na imagem abaixo:



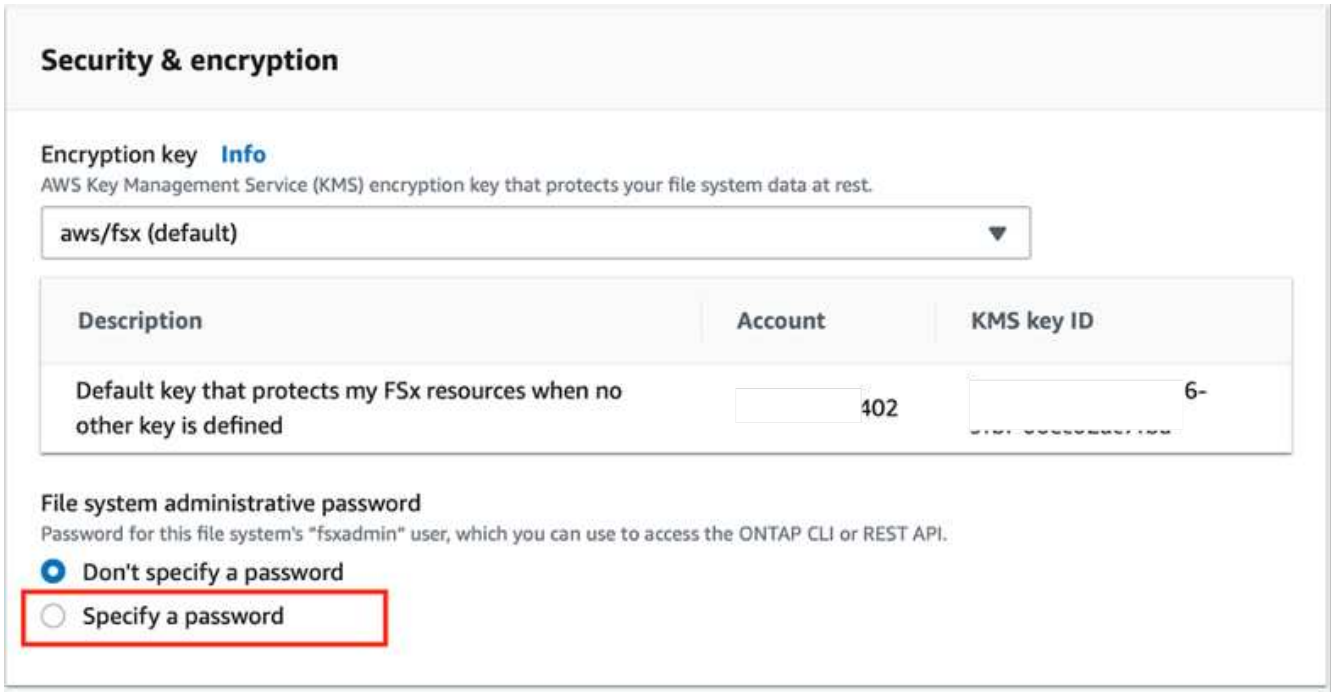
5. Role para baixo até encontrar uma seção chamada "Rede e segurança". Nesta seção, você definirá os detalhes da sub-rede e da VPC. Para os propósitos deste guia, selecionamos "EVS-VPC" no menu suspenso e selecionamos a sub-rede de acesso ao serviço (VLAN não marcada) como a sub-rede para o ambiente virtual EVS.

> ⓘ A sub-rede pode ser qualquer sub-rede privada não marcada na VPC. Ele também pode estar em uma VPC/sub-rede diferente conectada via VPC Peering, desde que o roteamento adequado tenha sido configurado.

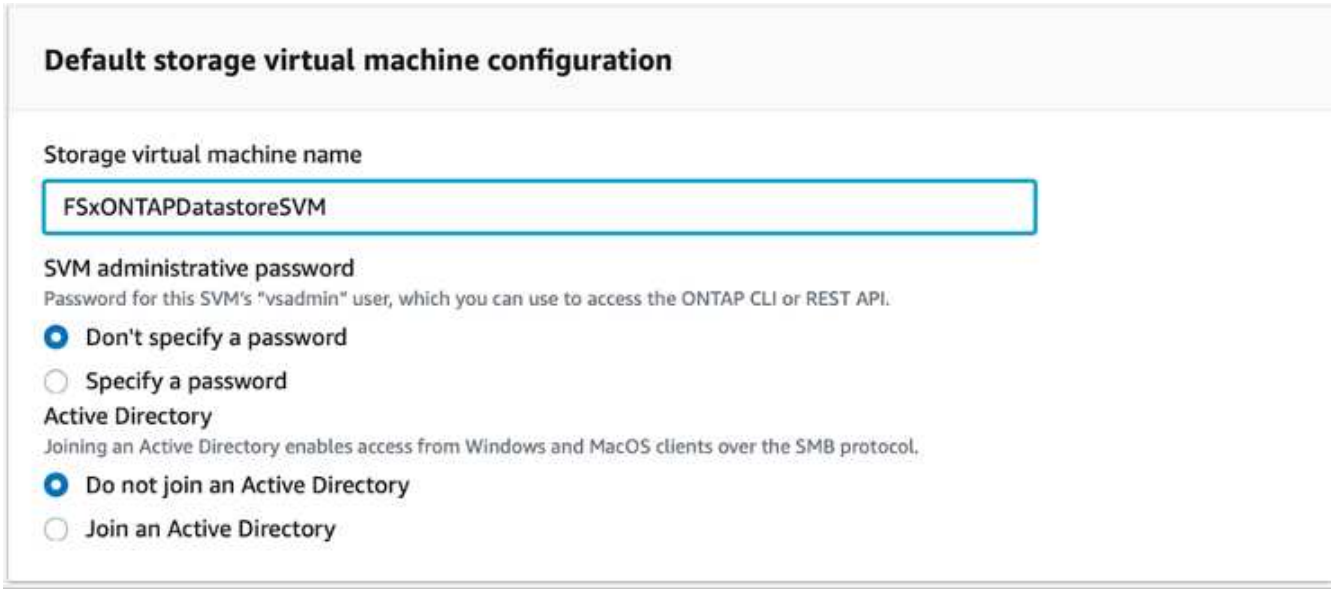


6. Rolando para baixo, você encontrará a seção "Segurança e criptografia". Aqui, selecione a chave de criptografia no menu suspenso. Essas chaves são fornecidas pelo AWS Key Management Service (AWS KMS) e protegerão os dados em repouso no seu sistema de arquivos FSx for ONTAP .

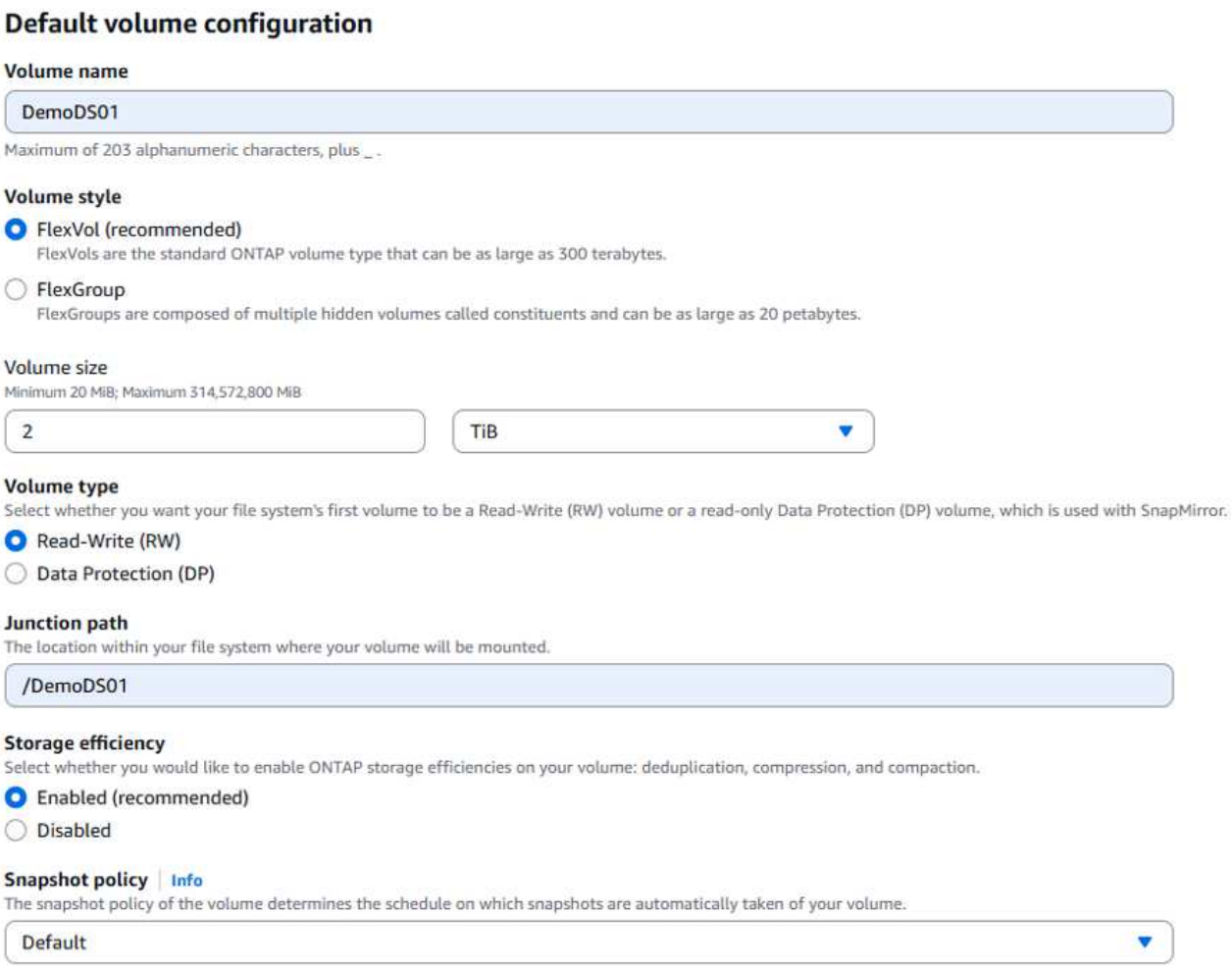
   Em seguida, na configuração "Senha administrativa do sistema de arquivos", especifique uma senha exclusiva para o usuário fsxadmin que administrará o sistema de arquivos.



7. Em seguida, role para baixo até uma seção intitulada "Configuração padrão da máquina virtual de armazenamento". Aqui, você precisará fornecer um nome para a máquina virtual de armazenamento (SVM).

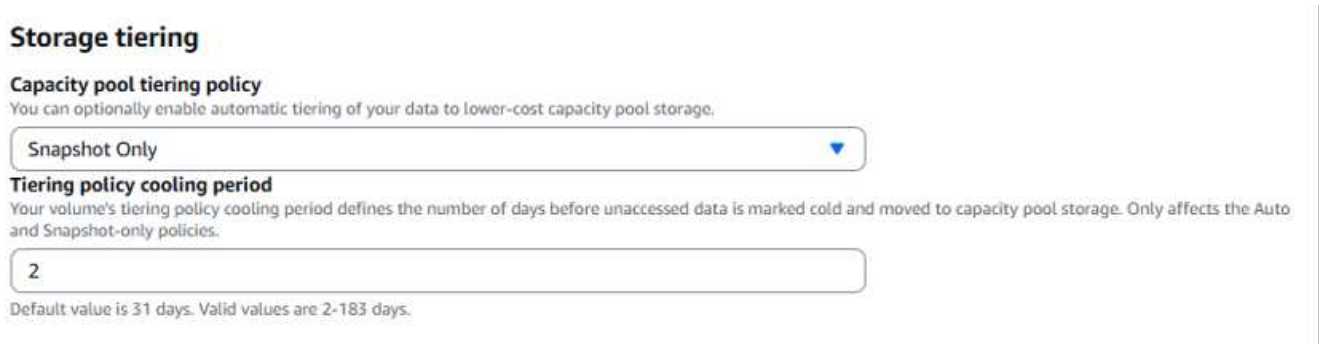


8. Em seguida, role para baixo até a seção intitulada "Configuração de volume padrão". Aqui você fornecerá um nome para o volume e definirá o tamanho do volume. O protocolo de volume deve ser NFS v3 (habilitado por padrão). Clique na opção para habilitar recursos de eficiência de armazenamento (compactação, desduplicação e compactação) para reduzir o uso geral de armazenamento e os custos.



9. Para a opção de níveis de armazenamento, selecione "Somente instantâneo" no menu suspenso e defina

um período de resfriamento da política de níveis. O padrão é 31 dias, mas para este exemplo definimos um período de resfriamento de dois dias.

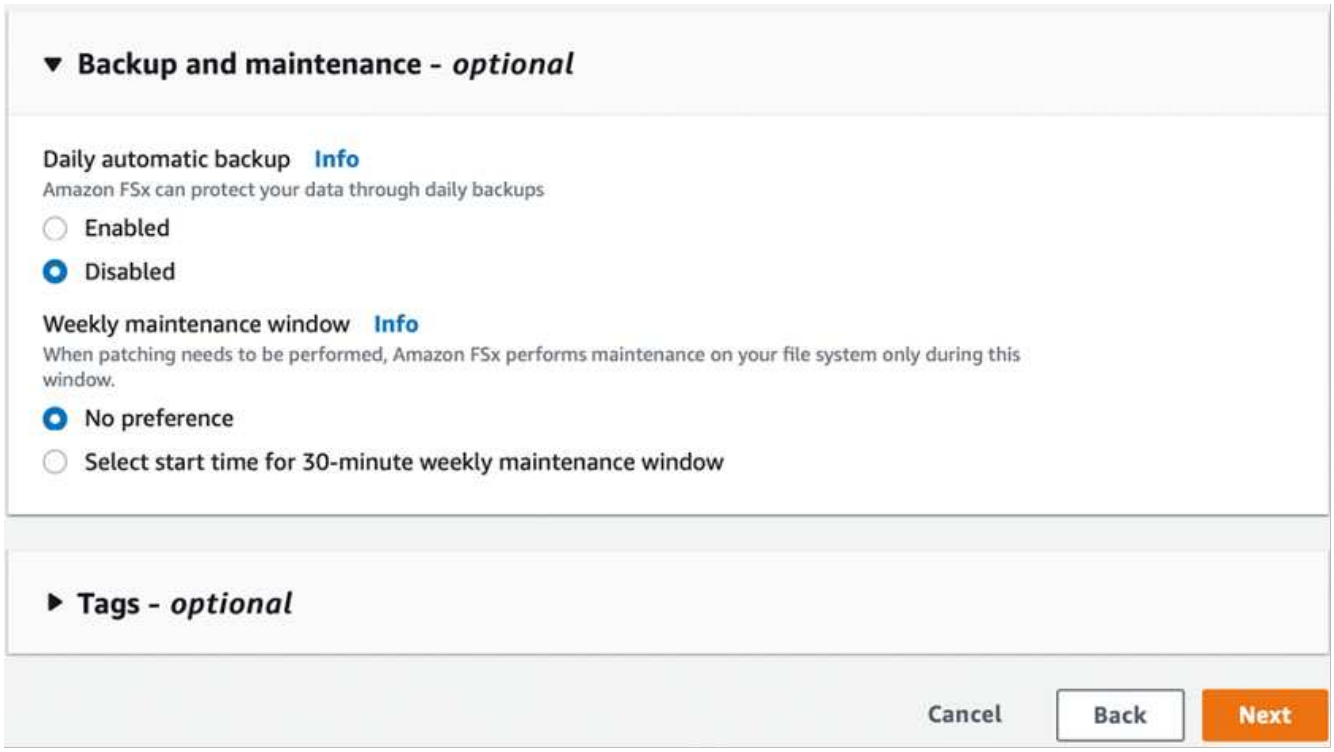


10. Depois de criar o volume, modifique os seguintes parâmetros usando a interface de linha de comando do ONTAP (ONTAP CLI):

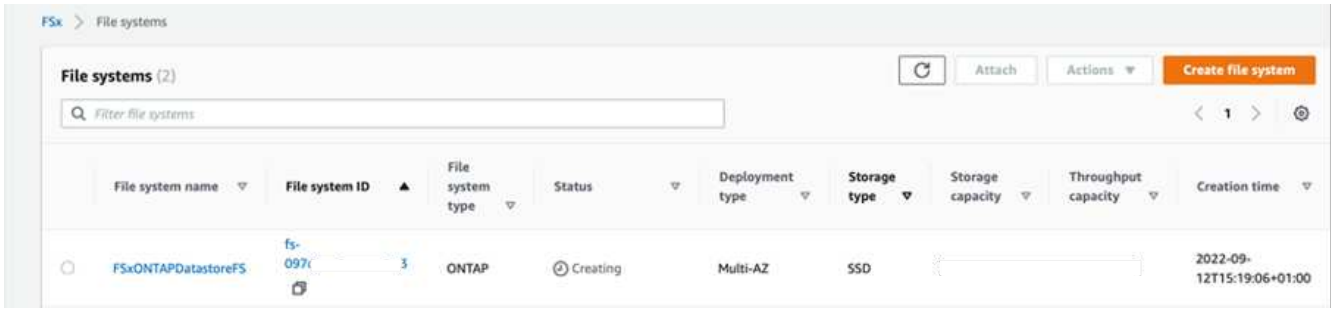
Contexto	Configuração
Garantia de volume	Nenhum (thin provisioned)
reserva_fracionária	0%
reserva instantânea	0%
Dimensionamento automático	crescer_encolher
Eficiência de armazenamento	Habilitado
Política de níveis de volume	Apenas instantâneo
Atualização de tempo de acesso (-atime-update)	Falso
Leitura mínima à frente (-min-readahead)	Falso
Política de instantâneo	Nenhum

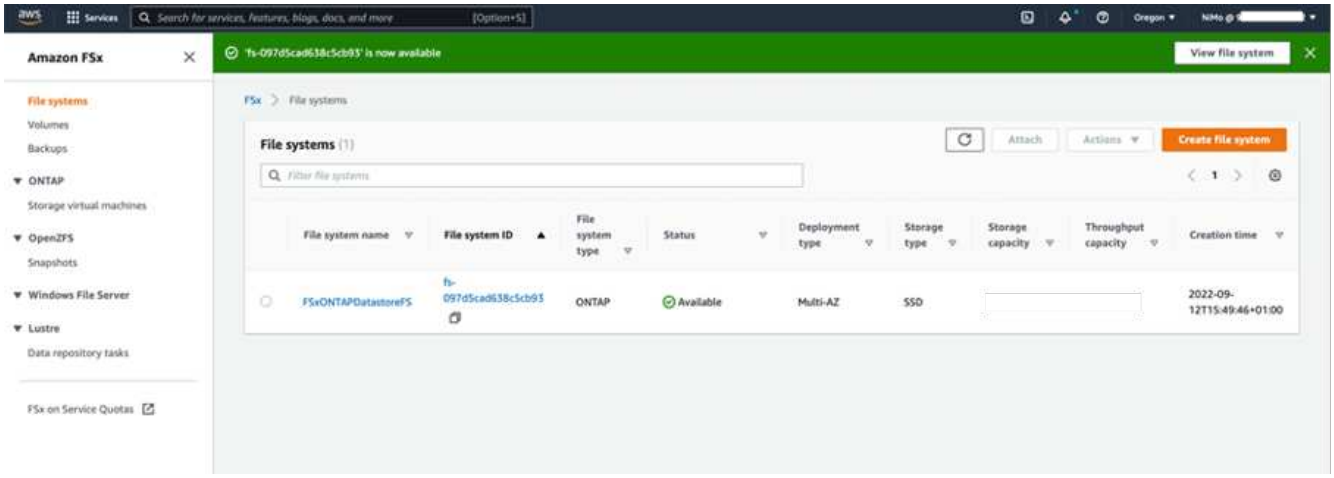
11. Na etapa opcional "Backup e manutenção", desative os backups automáticos diários e selecione "Sem preferência" para a janela de manutenção semanal.

    Clique em "Avançar" quando terminar.



12. Agora você receberá uma revisão de toda a configuração do sistema de arquivos que você definiu seguindo as etapas anteriores. Verifique se todos os parâmetros estão corretos e clique no botão "Criar sistema de arquivos" para concluir a configuração.





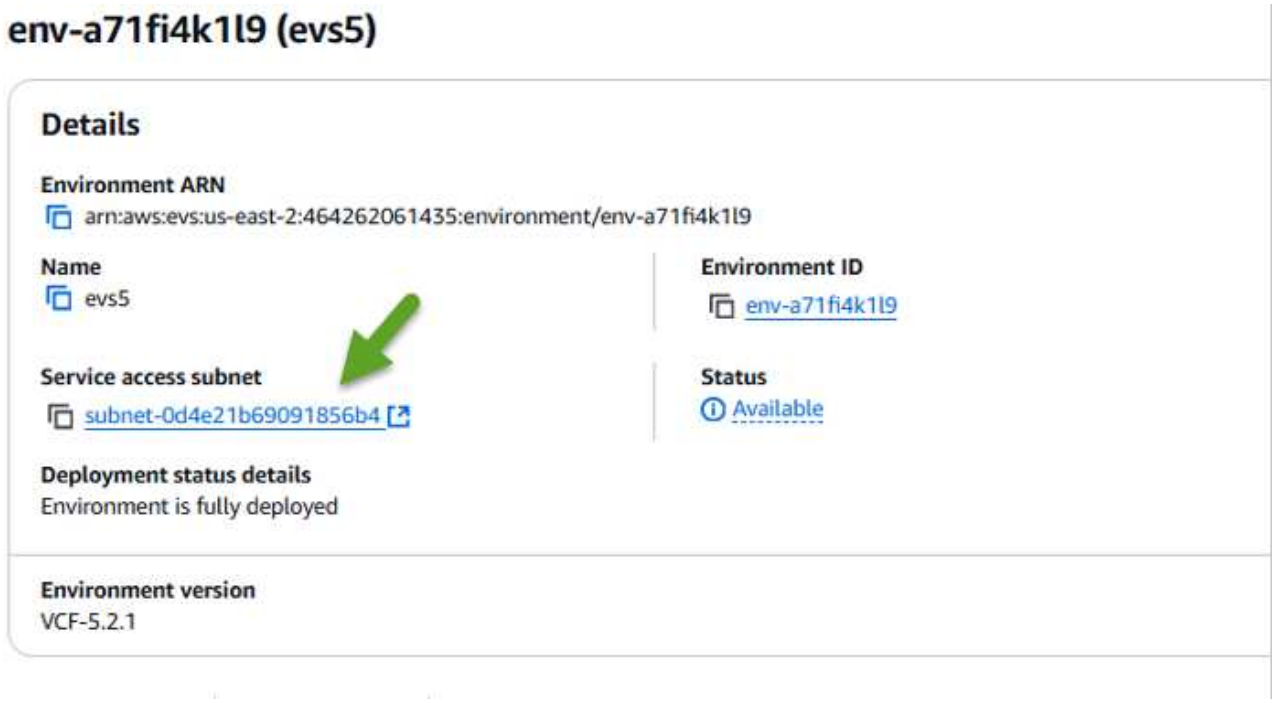
Para criar FSx adicionais para sistemas de arquivos ONTAP , você pode seguir as etapas detalhadas acima, ajustando os valores que afetam o desempenho e a capacidade do disco conforme necessário. Para saber mais sobre as opções de desempenho do FSx para

ONTAP, consulte"esta página de documentação" .

Validando grupos de roteamento e segurança de VPC e ambiente de virtualização

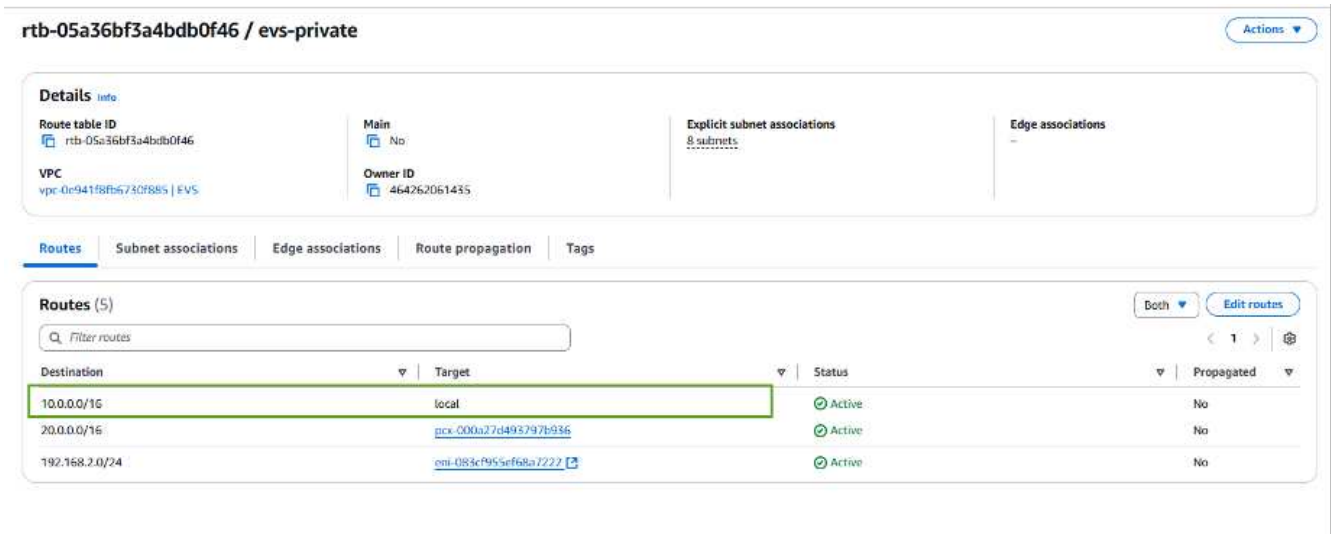
Validar os grupos de roteamento e segurança do VPC e do SDDC é importante para garantir que o ambiente de virtualização do Amazon EVS e os componentes do sistema de arquivos FSx for ONTAP possam funcionar juntos corretamente.

1. Navegue até Elastic VMware Service > Virtualization Environments > [seu ambiente Amazon EVS] e selecione a sub-rede de acesso ao serviço, conforme indicado pela seta verde abaixo:



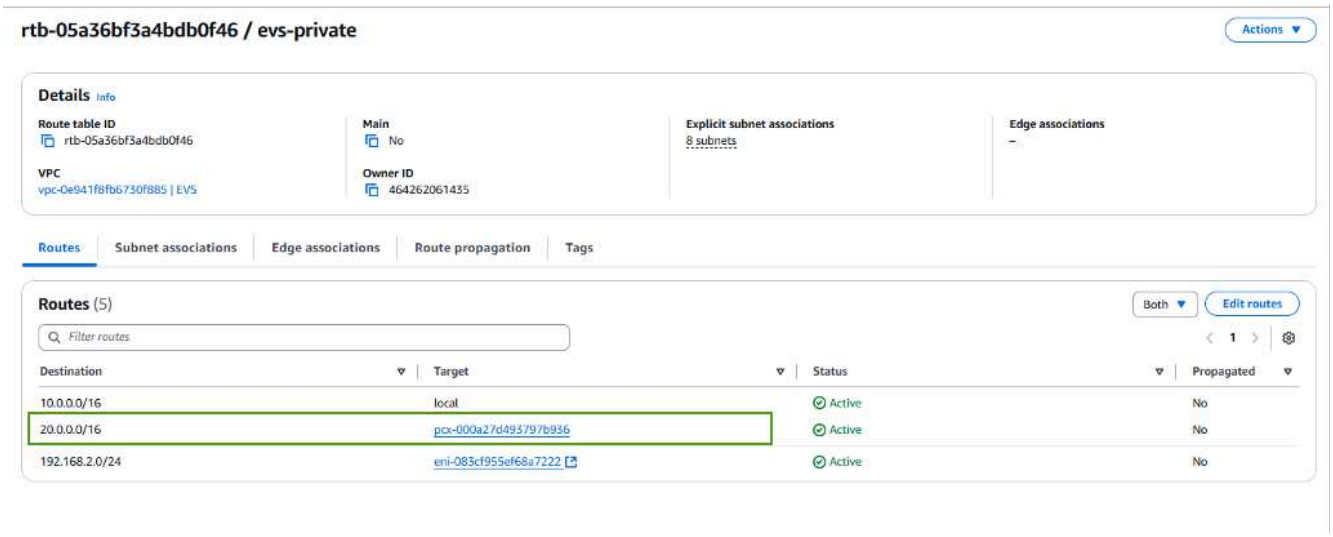
2. Isso abrirá o painel de sub-rede. Encontre a tabela Rotas neste painel e clique nela.

   Neste exemplo, o sistema de arquivos FSxN ONTAP está na mesma VPC que o ambiente Amazon EVS VCF, portanto, as rotas padrão são suficientes.



   Se o sistema de arquivos FSx para ONTAP estiver em uma VPC diferente, verifique se as rotas para essa

VPC foram adicionadas. Neste exemplo, foram adicionadas rotas para VPC Peering para a VPC onde o sistema FSx for ONTAP reside.

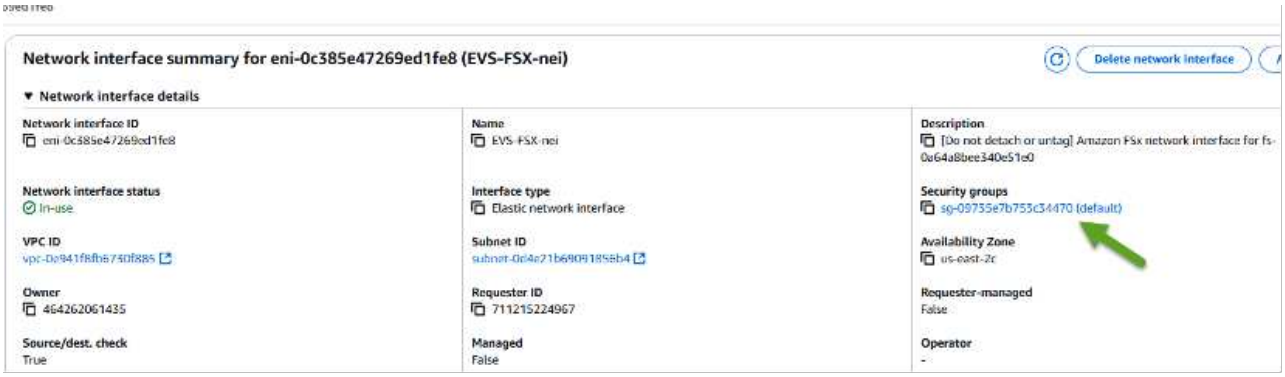


3. Em seguida, você precisará verificar se o grupo de segurança conectado ao sistema de arquivos FSx para ONTAP (ou seja, aquele conectado à interface de rede elástica (ENI) — permite acesso às portas NFS).

   Para obter uma lista completa de portas de protocolo NFS e iSCSI, consulte o xref:./vmware/ https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/limit-access-security-groups.html]Documentação do Controle de Acesso ao Sistema de Arquivos com Amazon VPC].

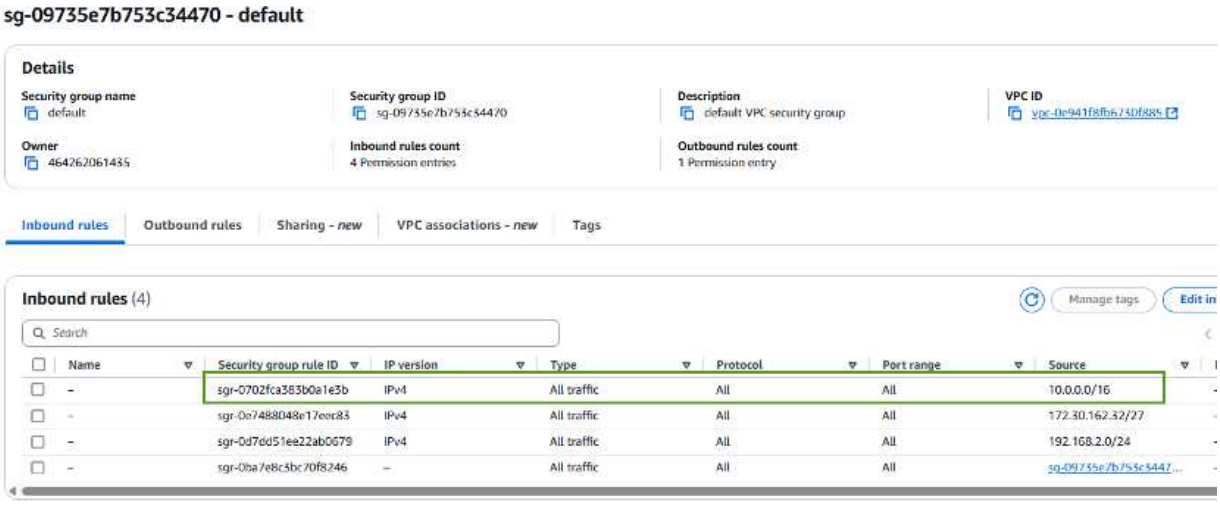
   Para verificar se o seu sistema de arquivos FSx para ONTAP está associado ao grupo de segurança:

   a. No console da AWS, navegue até FSx > Sistemas de arquivos > [seu sistema de arquivos FSx para ONTAP].
   b. Na aba Rede e Segurança, clique em ENI.
   c. Encontre o grupo de segurança listado nos detalhes da interface de rede associado à ENI (indicado pela seta verde na imagem abaixo).



   d. Valide as portas. Neste exemplo mostrado na tela a seguir, todo o tráfego é permitido. No entanto, você pode limitá-los somente às portas NFS. Aqui está a lista dos portos:
      - Porta 111 TCP: Portmapper, usado para negociar quais portas são usadas em solicitações NFS.
      - Porta 635 TCP: Mountd, que é para receber solicitações de montagem de entrada.
      - Porta 2049 TCP: NFS, que manipula o tráfego NFS.

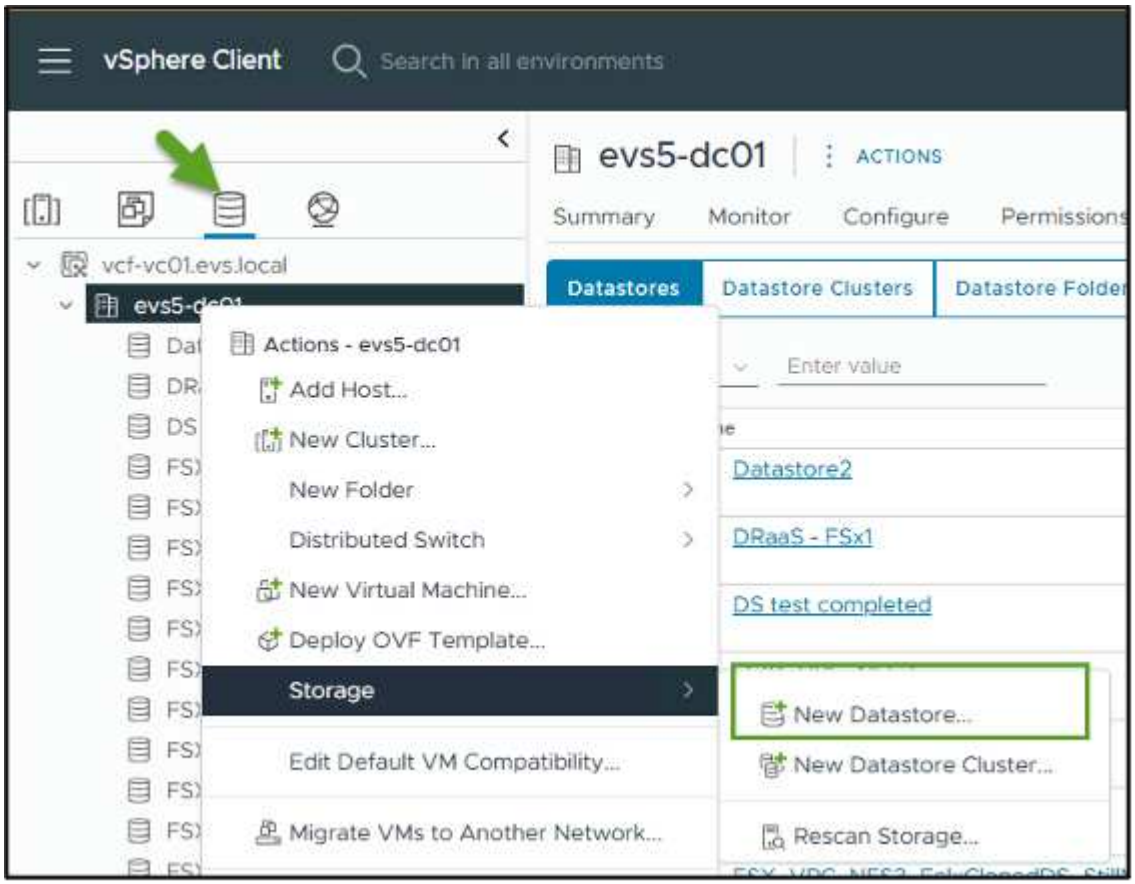
- Porta 4045 TCP: Network Lock Manager (NLM), que lida com solicitações de bloqueio.
- Porta 4046 TCP: Monitor de status de rede (NSM), que envia notificações aos clientes NFS quando o servidor é reinicializado para gerenciamento de bloqueio.



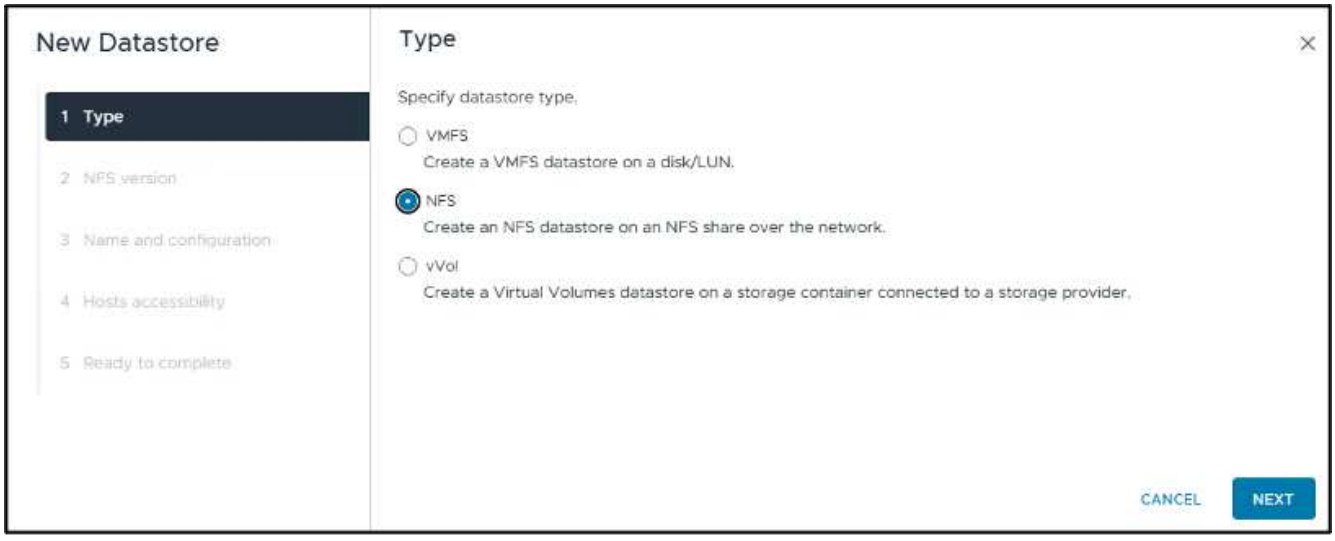
Anexando um volume FSx para ONTAP NFS ao Amazon EVS para uso como um armazenamento de dados

Agora que seu sistema de arquivos FSx para ONTAP foi provisionado e todos os parâmetros de conectividade adequados foram validados, é hora de anexar um volume de armazenamento FSx para ONTAP ao Amazon EVS. As etapas a seguir mostrarão como acessar o vCenter e montar o volume FSx para ONTAP como um armazenamento de dados NFS:

1. No cliente vSphere, vá para a aba "Datastore". Localize o Datacenter e navegue até Armazenamento > Novo Datastore, conforme mostrado abaixo:

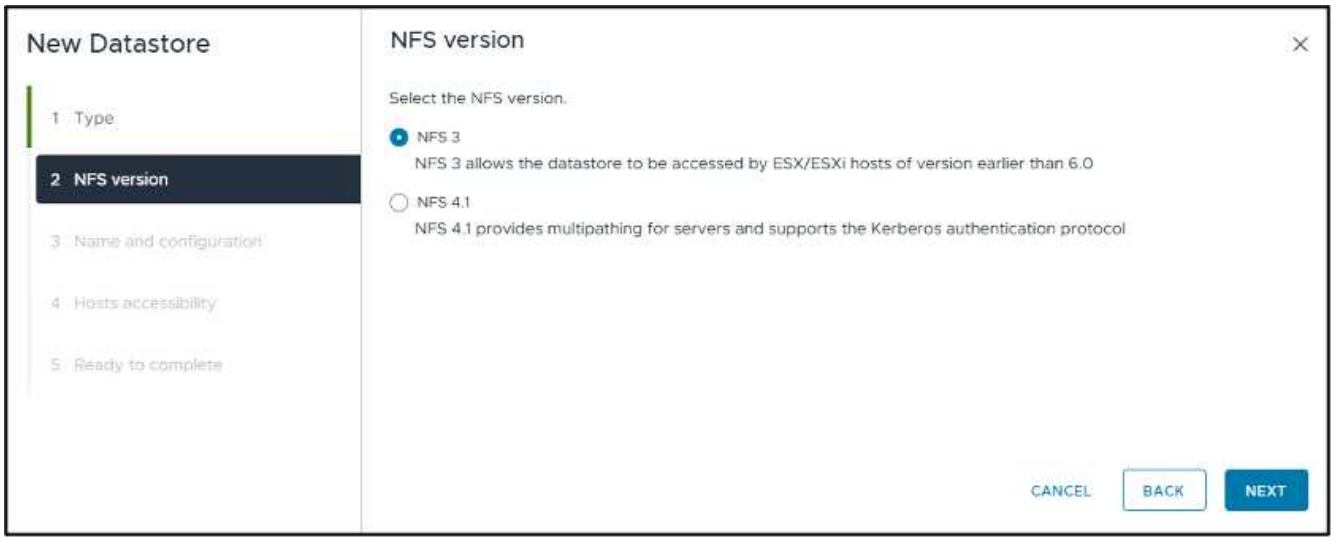


2. Agora você estará no assistente Novo armazenamento de dados. Na etapa "Tipo", você escolherá um tipo de armazenamento de dados. Selecione "NFS" e clique em "PRÓXIMO" para prosseguir.



3. Na etapa "Versão do NFS", você selecionará uma versão do NFS.

   Para os propósitos deste exemplo, escolheremos "NFS 3", mas observe que o NFS v4.1 também pode ser usado.



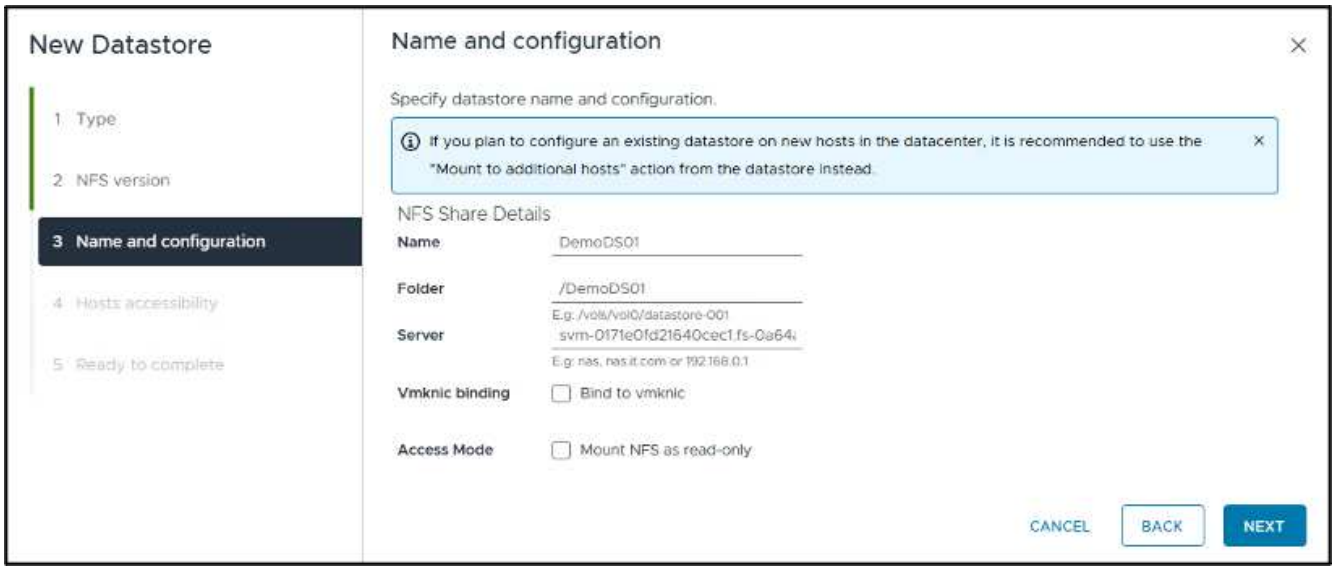
4. Na etapa "Nome e configuração", você irá:

   a. Dê um nome ao armazenamento de dados.

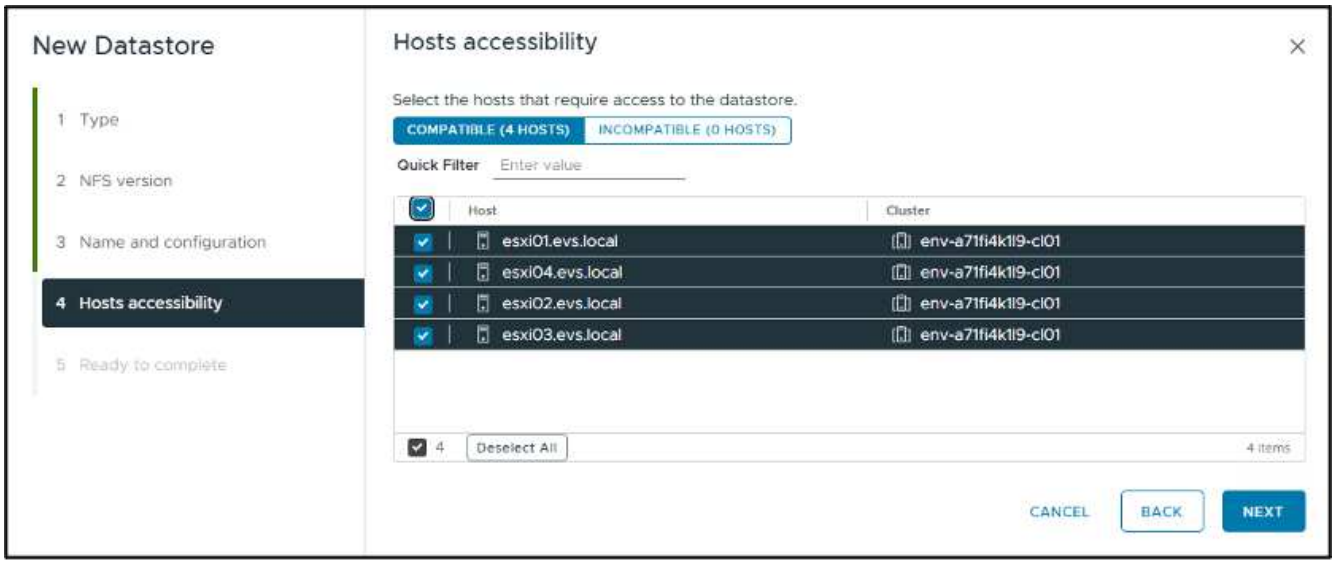
   b. Dê um nome à pasta. Use o caminho de junção para seu volume NFS.

   c. Dê um nome ao servidor. Use o nome DNS do NFS do seu SVM ou o endereço IP do NFS.

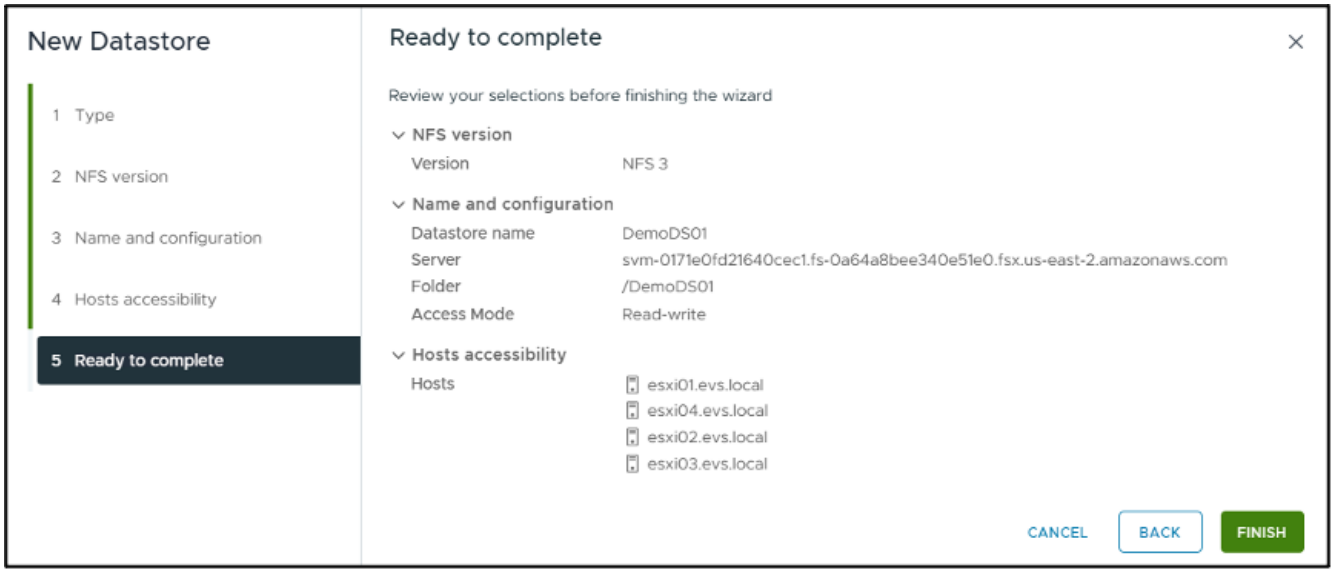
   Clique em "PRÓXIMO" para continuar.



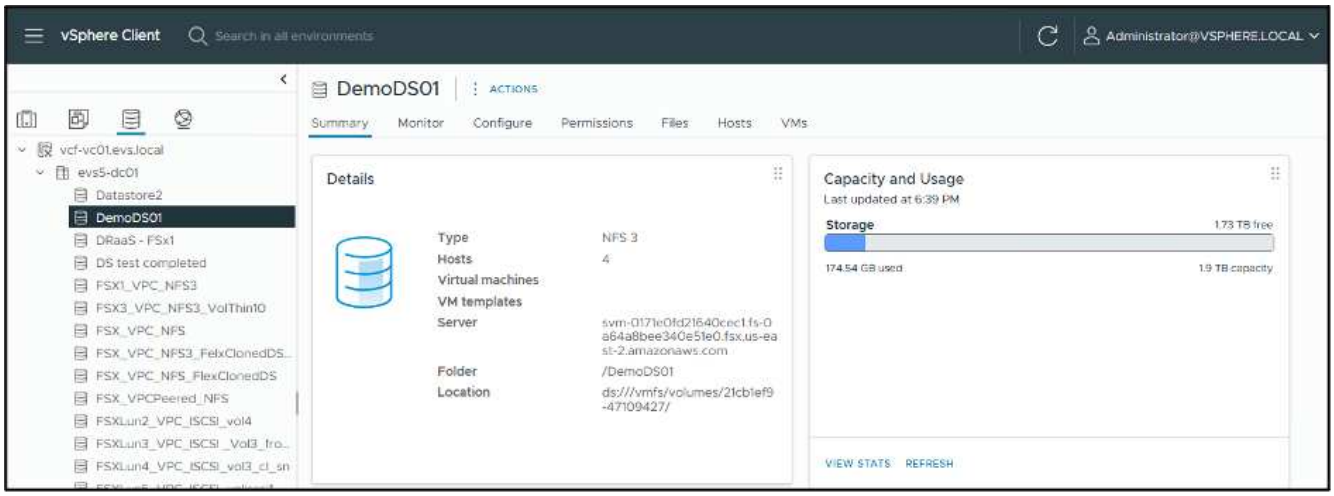
5. Na etapa "Acessibilidade do host", selecione todos os hosts que exigem acesso ao armazenamento de dados e clique em "PRÓXIMO" para continuar.



6. Na etapa "Pronto para concluir", revise os dados e clique em "CONCLUIR" para concluir a configuração.



7. Valide se o armazenamento de dados NFS foi conectado acessando o vCenter, conforme mostrado abaixo:



Procedimento de implantação para usar FSx para ONTAP como um armazenamento de dados iSCSI

Esta seção aborda as etapas para configurar um armazenamento de dados iSCSI usando o FSx para ONTAP.

Pré-requisitos

Antes de provisionar e anexar o FSx para ONTAP como um armazenamento de dados iSCSI, você deve primeiro implantar um ambiente de virtualização Amazon EVS. Para obter mais informações, consulte a documentação no guia Introdução ao Amazon EVS. Esta seção também pressupõe que você tenha implantado um FSx para o sistema de arquivos ONTAP . Consulte a seção Abordagem detalhada acima para obter as etapas apropriadas.

Etapas de implantação de alto nível

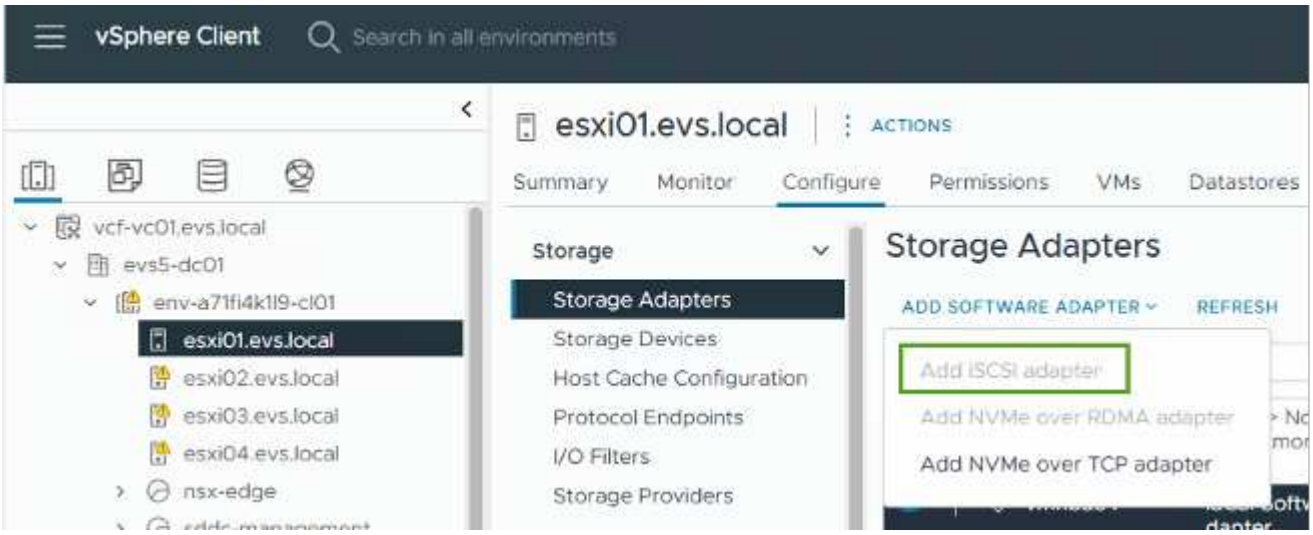
A implantação do sistema de arquivos FSx para ONTAP para uso como um armazenamento de dados iSCSI para o Amazon EVS e o estabelecimento de conectividade entre os dois serviços incluirão as seguintes etapas:

- Configurando um adaptador de rede iSCSI para cada host ESXi.
- Criação e configuração do FSx para sistema de arquivos ONTAP , volume, LUN, etc.
- Conectando os hosts ESXi ao servidor do sistema de arquivos FSx para ONTAP .
- Criação de um sistema de arquivos de máquina virtual (VMFS) de armazenamento de dados iSCSI.

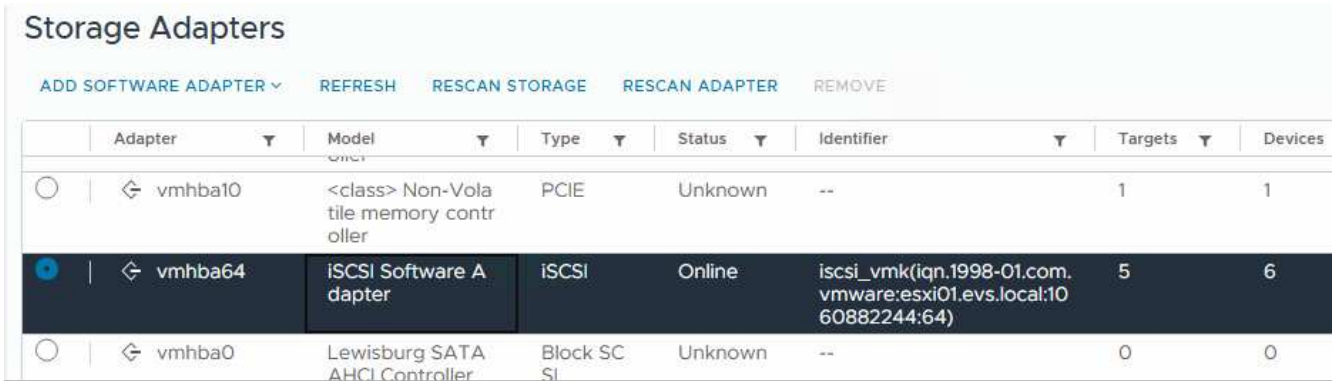
Adicionar adaptador de rede iSCSI

As etapas a seguir precisam ser executadas em cada host ESXi em seu ambiente.

1. Entre no cliente vSphere e selecione o host ESXi. Na aba Configurar, escolha "Adicionar adaptador de software" e selecione "Adicionar adaptador iSCSI" no menu suspenso, conforme mostrado aqui:

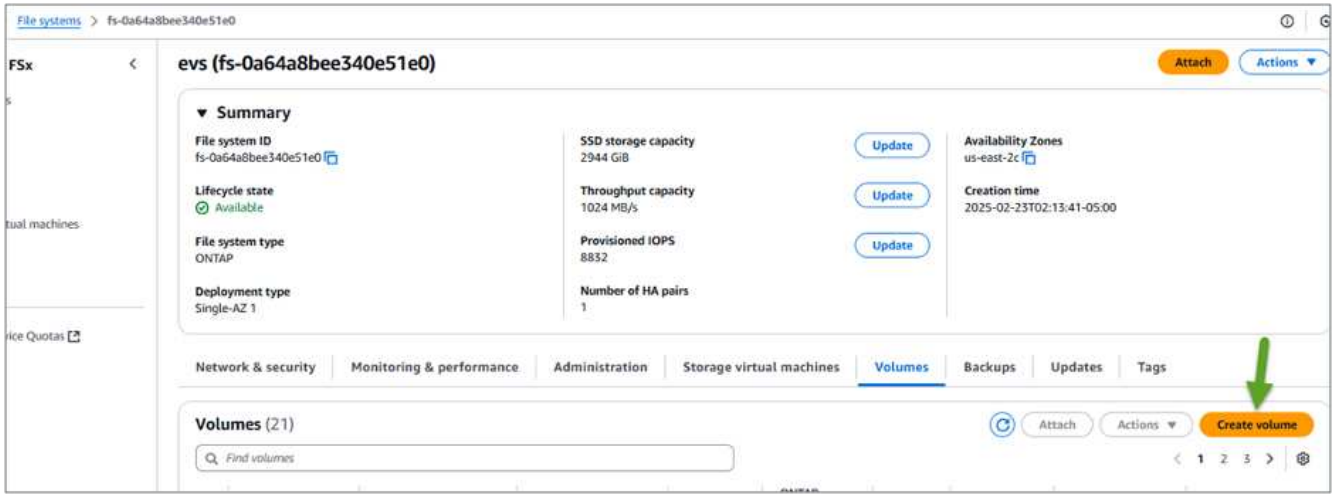


2. Quando a instalação estiver concluída, você estará na tela Adaptadores de Armazenamento. Selecione "Redigitalizar adaptador" na barra de menu. Registre o IQN do adaptador iSCSI: iqn.xxxx. Este valor será usado na etapa de mapeamento de LUN posteriormente.



Crie um FSx para volume ONTAP

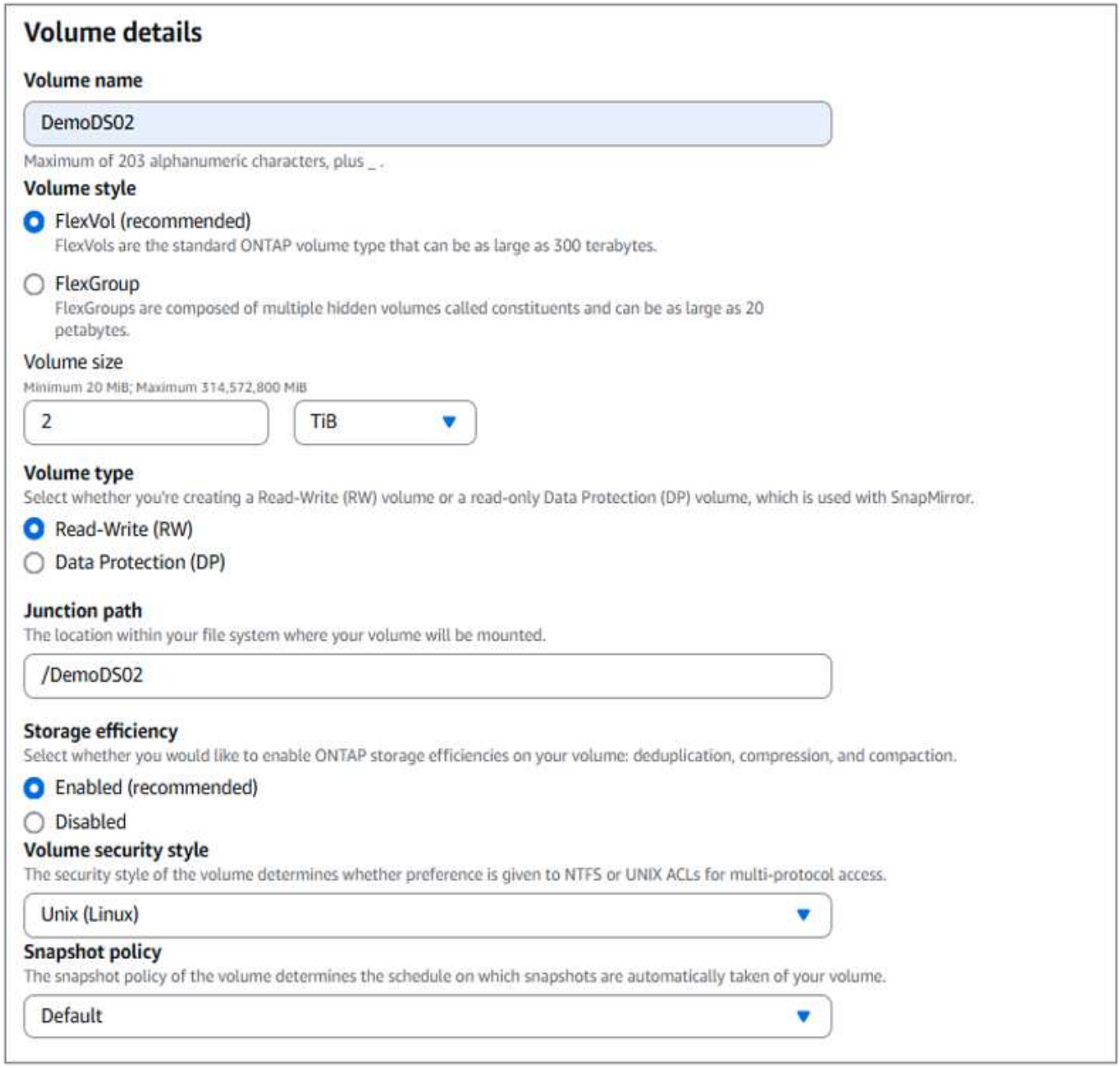
1. Acesse o Console da AWS e entre na página do seu sistema de arquivos FSx para ONTAP e clique em "Criar volume".



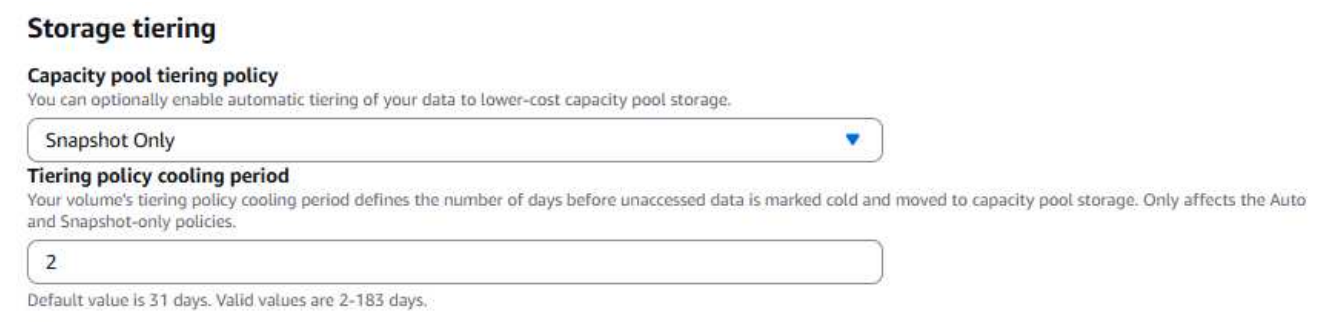
2. Selecione o SVM onde você deseja criar o volume.



3. Na página "Detalhes do volume", insira os detalhes conforme mostrado na captura de tela abaixo. Quando terminar, clique em "Criar" para configurar o volume. Selecione "Ativado" para ativar os recursos de eficiência de armazenamento do ONTAP (compressão, desduplicação e compactação).



4. Para a opção de níveis de armazenamento, selecione "Somente instantâneo" no menu suspenso e defina um período de resfriamento da política de níveis. O padrão é 31 dias, mas para este exemplo definimos um período de resfriamento de dois dias.



5. Depois que o volume for criado, use o ONTAP CLI para definir os seguintes valores:

Contexto	Configuração
Garantia de volume	Nenhum (thin provisioned)
reserva_fracionária	0%
reserva instantânea	0%
Dimensionamento automático	crescer_encolher
Eficiência de armazenamento	Habilitado
Política de níveis de volume	Apenas instantâneo
Atualização de tempo de acesso (-atime-update)	Falso
Leitura mínima à frente (-min-readahead)	Falso
Política de instantâneo	Nenhum
Reserva de espaço LUN	Desabilitado
Alocação de espaço LUN	Habilitado

Crie um LUN, um igroup e mapeie o LUN

Nesta seção, mostramos como criar o LUN que aparecerá como um disco no vSphere. Também mostraremos como criar um grupo de iniciadores (igroup), que é a lista dos iniciadores que têm acesso ao LUN. O igroup permitirá acesso ao LUN a partir dos hosts vSphere ESXi. Por fim, mostraremos como mapear o igroup para o LUN.

1. Para acessar o ONTAP CLI, estabeleça uma sessão SSH na porta de gerenciamento do sistema de arquivos FSx para ONTAP ou SVM executando o seguinte comando:

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

2. Crie o LUN. Certifique-se de definir alocação de espaço e reserva de espaço como habilitados. O tamanho deve ser de até 90% do tamanho do volume:

```
Fsxid::> lun create -vserver fsx -path /vol/DemoDS02/lun_name -size 1.8T
-ostype vmware -space-allocation enabled -space-reservation disabled
```

3. Crie o igroup e adicione o IQN de todos os hosts ESXi dentro do cluster.

```
Fsxid::> lun igroup create -vserver fsx -igroup evs1 -protocol iscsi
-ostype vmware -initiator iqn.1998-
01.com.vmware:esxi01.evs.local:1060882244:64,iqn.1998-
01.com.vmware:esxi02.evs.local:1911302492:64,iqn.1998-
01.com.vmware:esxi03.evs.local:2069609753:64,iqn.1998-
01.com.vmware:esxi04.evs.local:1165297648:64
```

4. Mapeie o LUN com o seguinte código:

```
Fsxid::> lun mapping create -vserver fsx -path /vol/DemoDS02/lun1
-igroup evs1 -lun-id 2
```

5. Revise o mapeamento do LUN e verifique se o estado foi alterado para "mapeado". Esta é uma verificação dupla necessária para garantir que o LUN esteja em um estado mapeado:

```
Fsxid::> lun show
Vserver   Path                            State   Mapped   Type
Size
--------- ------------------------------- ------- -------- --------
--------
fsx       /vol/DemoDS02/lun1              online  mapped   vmware
1.80TB
```

Obter informações de configuração iSCSI do SVM

1. Execute o iSCSI show e registre o nome do alvo. Isso será usado na descoberta do vSphere do FSx para discos ONTAP (Observação: esse nome de destino é exclusivo do seu SVM):

```
Fsxid::> iscsi show -vserver fsx
                 Vserver: fsx
             Target Name: iqn.1992-
08.com.netapp:sn.c083e374f1b711ef9d9f8123a3ebcf46:vs.3
            Target Alias: fsx
   Administrative Status: up
```

2. Registre os endereços IP iSCSI:

```
Fsxid::> network interface show -vserver fsx -data-protocol iscsi
-fields address
vserver lif       address
------- -------   -----------
fsx     iscsi_1   10.0.10.134
fsx     iscsi_2   10.0.10.227
```

Descubra o servidor FSx para ONTAP iSCSI

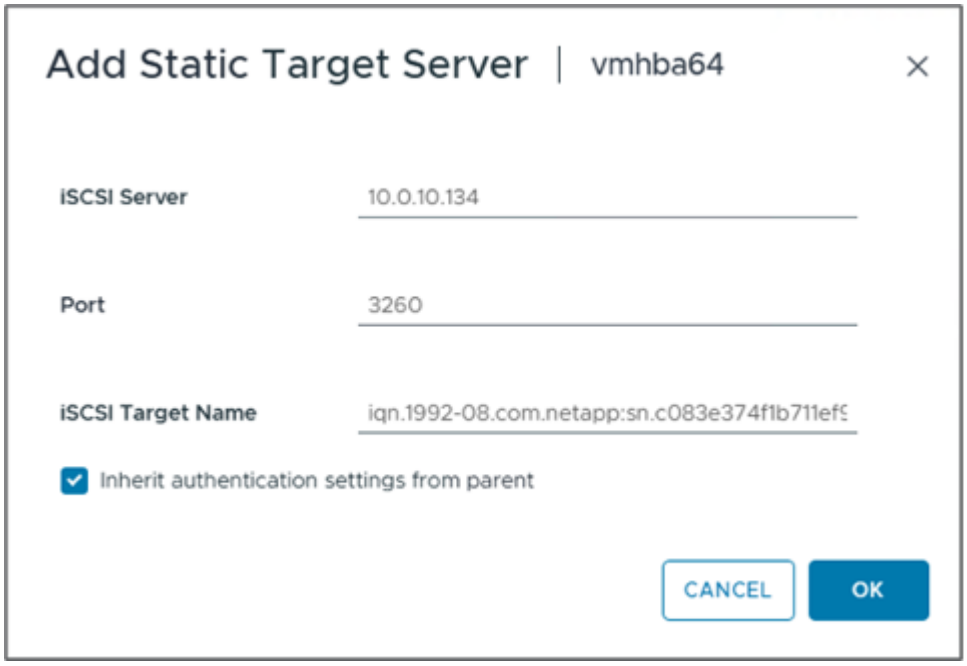
Agora que mapeamos o LUN, podemos descobrir o servidor FSx para ONTAP iSCSI para o SVM. Observe que para cada host ESXi existente no seu SDDC, você precisará repetir as etapas listadas aqui.

1. Primeiro, certifique-se de que o grupo de segurança vinculado ao sistema de arquivos FSx para ONTAP (ou seja, aquele conectado ao ENI) permite portas iSCSI.

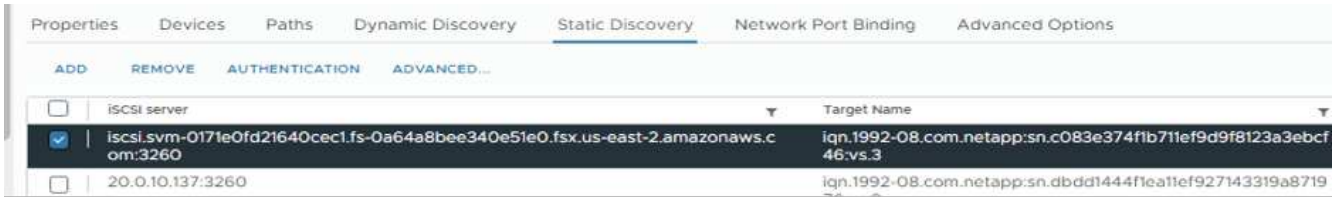
   Para obter uma lista completa de portas do protocolo iSCSI e como aplicá-las, consulte"Controle de

acesso ao sistema de arquivos com Amazon VPC" .

2. No vSphere Client, acesse ESXi Host > Adaptadores de Armazenamento > Descoberta Estática e clique em "Adicionar".
3. Digite o endereço IP do servidor iSCSI acima (a porta é 3260). O nome do destino iSCSI é o IQN do comando iSCSI show. Clique em "OK" para prosseguir.



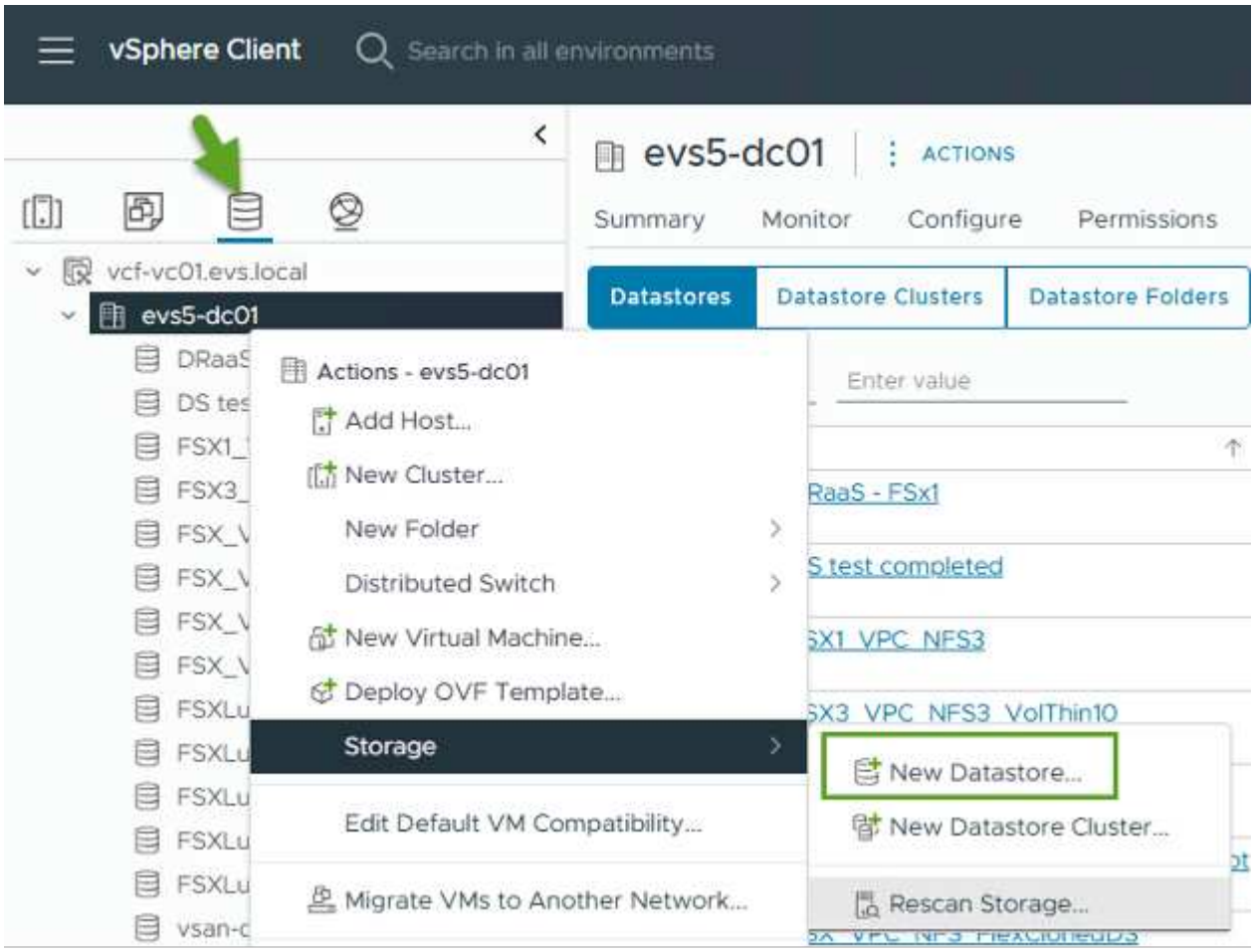
4. O assistente será fechado e você estará na tela Descoberta estática do armazenamento de dados. Na tabela desta página você poderá verificar se o alvo foi descoberto.



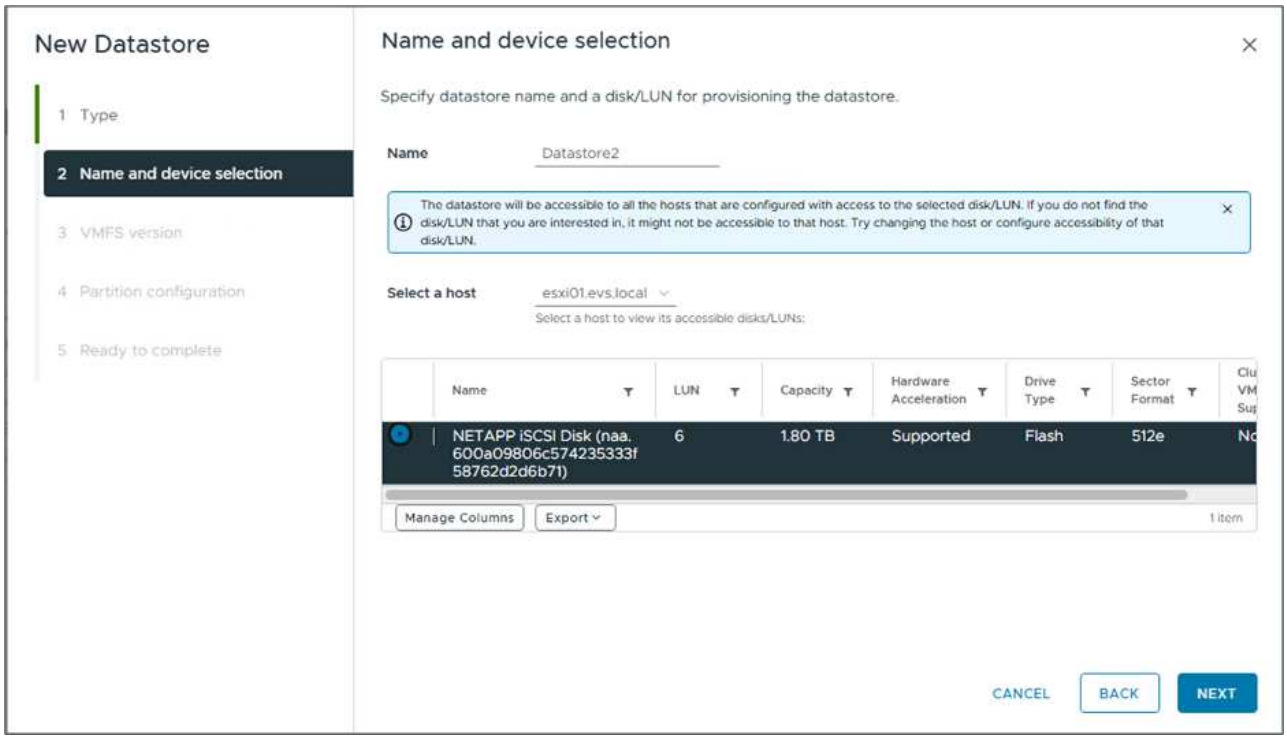
Criar um armazenamento de dados iSCSI

Agora que descobrimos o servidor iSCSI, podemos criar um armazenamento de dados iSCSI.

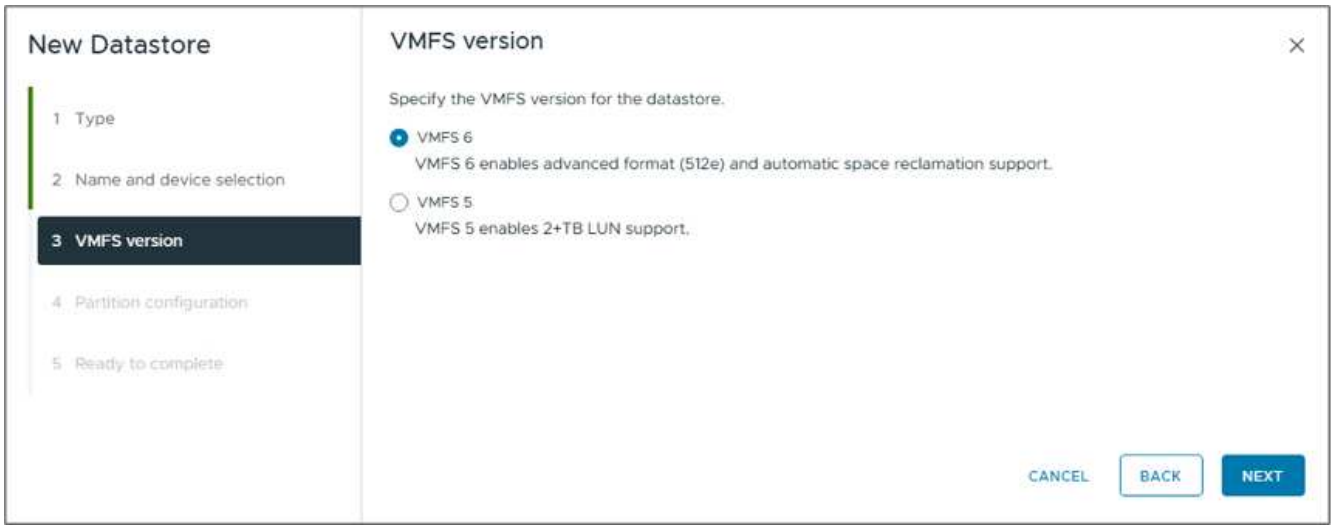
1. No cliente vSphere, vá para a guia Datastore e selecione o SDDC onde deseja implantar o datastore. Clique com o botão direito e selecione o ícone Armazenamento (indicado pela seta verde na captura de tela abaixo) e, em seguida, selecione "Novo armazenamento de dados" no menu suspenso:



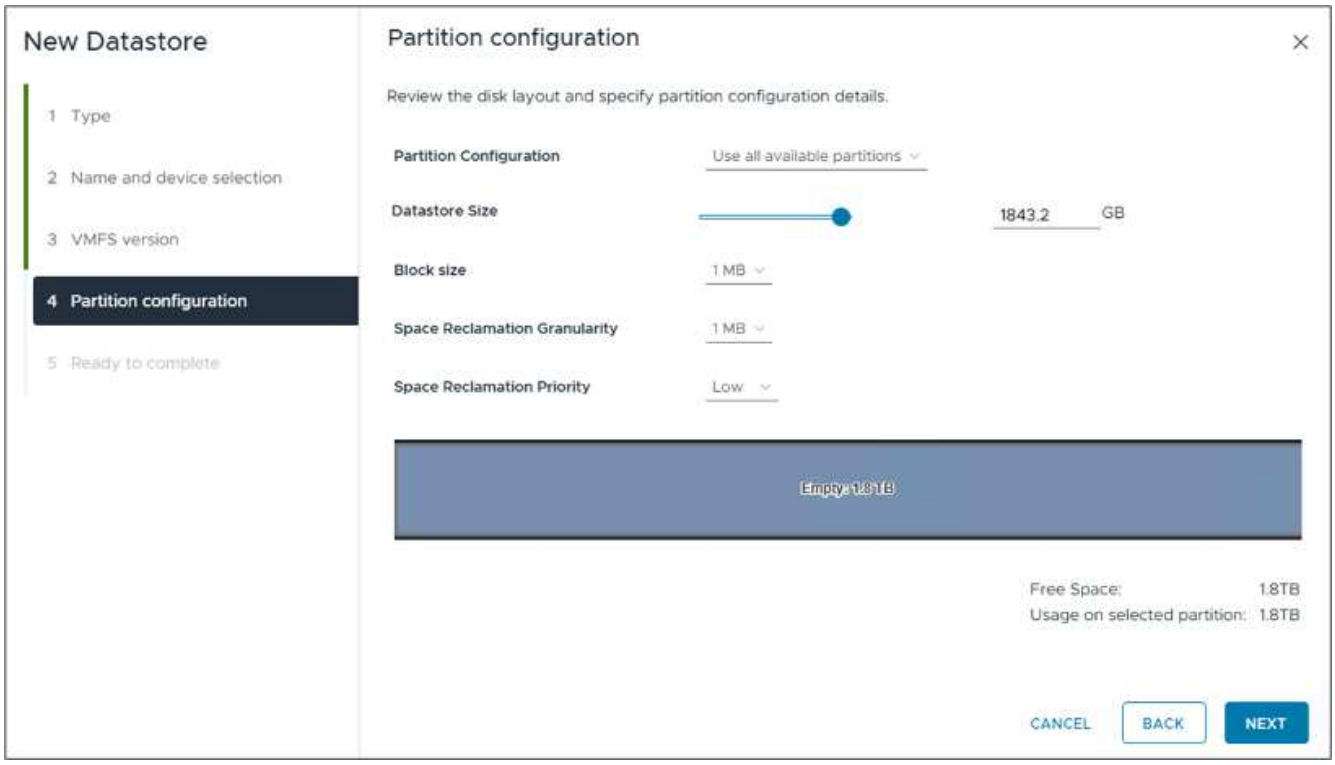
2. Agora você estará no assistente Novo armazenamento de dados. Na etapa "Tipo", selecione a opção VMFS.
3. Na etapa "Seleção de nome e dispositivo":
   a. Forneça um nome para seu armazenamento de dados.
   b. Selecione qual host ESXi você deseja conectar ao armazenamento de dados.
   c. Selecione o disco descoberto (LUN) e clique em "Avançar".



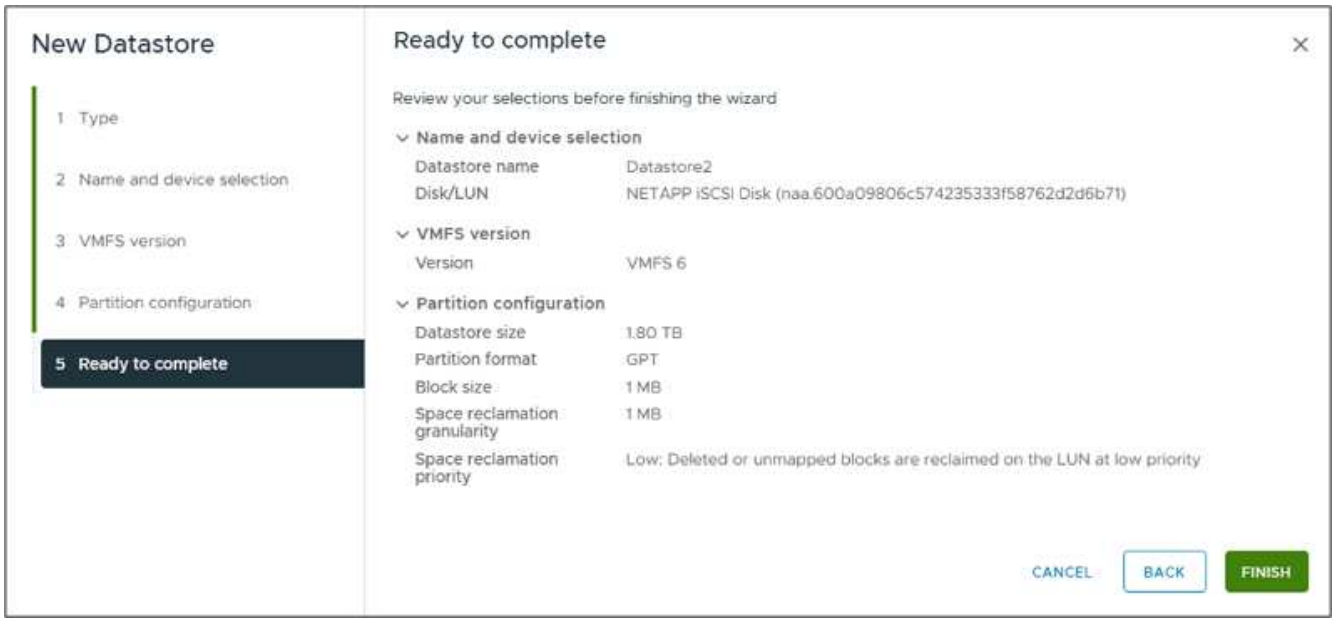
4. Na etapa "Versão do VMFS", selecione "VMFS 6".



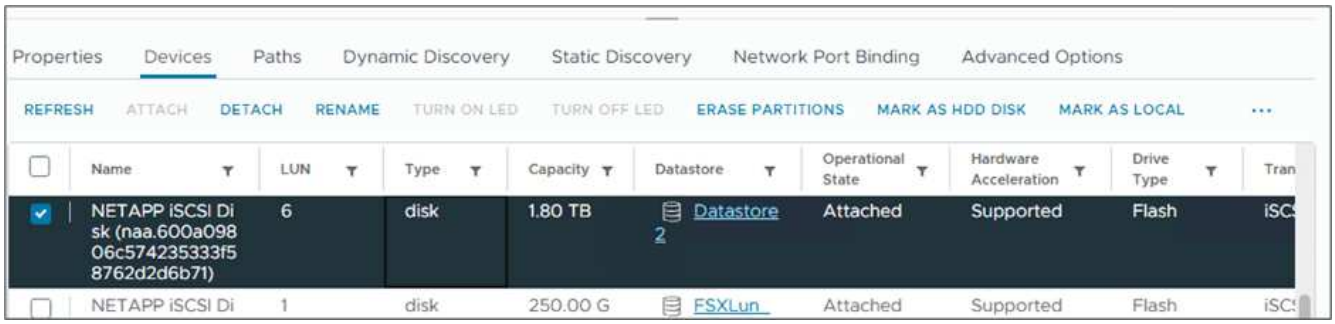
5. Na etapa "Configuração da partição", deixe as configurações padrão como estão, incluindo a opção "Usar todas as partições disponíveis". Clique em "Avançar" para prosseguir.



6. Na etapa "Pronto para concluir", certifique-se de que as configurações estejam corretas. Quando terminar, clique em "CONCLUIR" para finalizar a configuração.



7. Retorne à página Dispositivos e verifique se o armazenamento de dados foi anexado.



Conclusão

Este documento fornece instruções sobre como configurar o FSx para ONTAP como um armazenamento externo para o Amazon EVS para uso com os protocolos NFS e iSCSI.

Usar o FSx for ONTAP como armazenamento externo para o Amazon EVS fornece valores operacionais e comerciais claros. Ele fornece melhor resiliência de dados, proteção, replicação e eficiência de custos por meio da tecnologia ONTAP e mantém o TCO otimizado graças ao desacoplamento da arquitetura hiperconvergente da VMware. Com o FSx para ONTAP, os usuários do Amazon EVS podem dimensionar o armazenamento sem adicionar recursos de computação e sem inflar os custos. Isso abre todo o potencial de elasticidade e escala apresentado pela Nuvem AWS.

Para saber mais, leia o anúncio de novidades da Amazon:"Amazon EVS agora se integra com FSx para ONTAP" , e o blog da NetApp :"Amazon EVS anuncia suporte para FSx para ONTAP" .

Proteger o datastore FSx ONTAP para Exchange Virtual Server

Como proteger Amazon FSx for NetApp ONTAP datastores com Amazon Elastic VMware Service usando NetApp SnapCenter Plug-in for VMware

Este guia demonstrará uma abordagem de implantação simples para proteger FSx for ONTAP Network File System (NFS) e iSCSI Amazon Exchange Virtual Server datastores e VMs associadas usando a NetApp SnapCenter® Plug-in for VMware vSphere solução de backup e recuperação para VMs.

Introdução

Amazon FSx for NetApp ONTAP (FSx for ONTAP)-based datastores suplementares para Amazon Elastic VMware Service (Amazon Exchange Virtual Server) oferecem uma excelente solução para executar tanto cargas de trabalho que exigem alto desempenho — como aproveitar nConnect, o peering do Amazon Virtual Private Cloud (Amazon VPC) e usar várias conexões de rede por montagem de datastore — quanto cargas de trabalho com uso intensivo de armazenamento.

Essa capacidade permite que os clientes superem as limitações do armazenamento de instâncias locais fornecido por uma storage virtual area network (vSAN), dimensionem o armazenamento independentemente da computação e reduzam o custo total de propriedade. Além dos benefícios de custo total de propriedade (TCO), o FSx for ONTAP oferece Amazon Exchange Virtual Server com recursos de nível empresarial já conhecidos pelos clientes de ONTAP on-premises, ajudando a otimizar e simplificar as implantações. O uso do FSx for ONTAP fornece acesso às tecnologias NetApp® Snapshot™, SnapMirror® e SnapVault® que oferecem suporte a operações de backup e restauração para máquinas virtuais (VMs), datastores e discos de máquinas virtuais (VMDKs). Um recurso fundamental é a proteção baseada em Snapshot.

Visão geral

À medida que as organizações expandem e consolidam ambientes, a necessidade de proteger essas cargas de trabalho e o storage subjacente torna-se cada vez mais importante. O SCV pode ser usado para fazer backup de datastores e máquinas virtuais diretamente do Amazon EVS vSphere cliente.

Objetivo deste Guia

Este guia fornece instruções sobre como proteger um Amazon FSx for NetApp ONTAP datastore para Amazon EVS usando o SCV. Exemplos de cenários de proteção de máquinas virtuais e bancos de dados são fornecidos, assim como de restauração.

Público

Este tutorial é destinado a arquitetos e administradores de nuvem familiarizados com VMware vSphere, Amazon EVS, AWS Console e FSx for ONTAP.

Etapas de alto nível para implantação e configuração

A seguir estão os passos de alto nível para implantar e configurar o SCV para proteger suas máquinas virtuais e datastores no Amazon Exchange Virtual Server:

1. Baixe o SCV Open Virtual Appliance (OVA).
2. Faça login com as credenciais do vSphere Client no Amazon Exchange Virtual Server.
3. Implante um modelo Open Virtualization Format (OVF) para iniciar o assistente de implantação do VMware.
4. Para acessar o plug-in, selecione SnapCenter Plug-in for VMware no menu.
5. Adicionar storage.
6. Crie políticas de backup.
7. Crie grupos de recursos.
8. Backup de grupos de recursos.
9. Restaure toda a máquina virtual ou um disco virtual específico ou arquivos do convidado.

Procedimento de configuração do SnapCenter Plug-in para VMware

Esta seção aborda os passos para configurar o SnapCenter Plug-in para VMware.

Pré-requisitos

Os seguintes pré-requisitos são necessários antes de começar:

1. Para registrar o servidor vCenter durante a implantação do OVA, especifique o domínio totalmente qualificado (FQDN) ou o endereço IP do vCenter.
2. Para as credenciais do vCenter, use uma conta com os privilégios mínimos necessários
3. Abra as portas do firewall para acesso ao vCenter Server.
4. Atualize o grupo de segurança da Amazon VPC onde o FSx for ONTAP está em execução para permitir o acesso do SCV ao FSx for ONTAP.

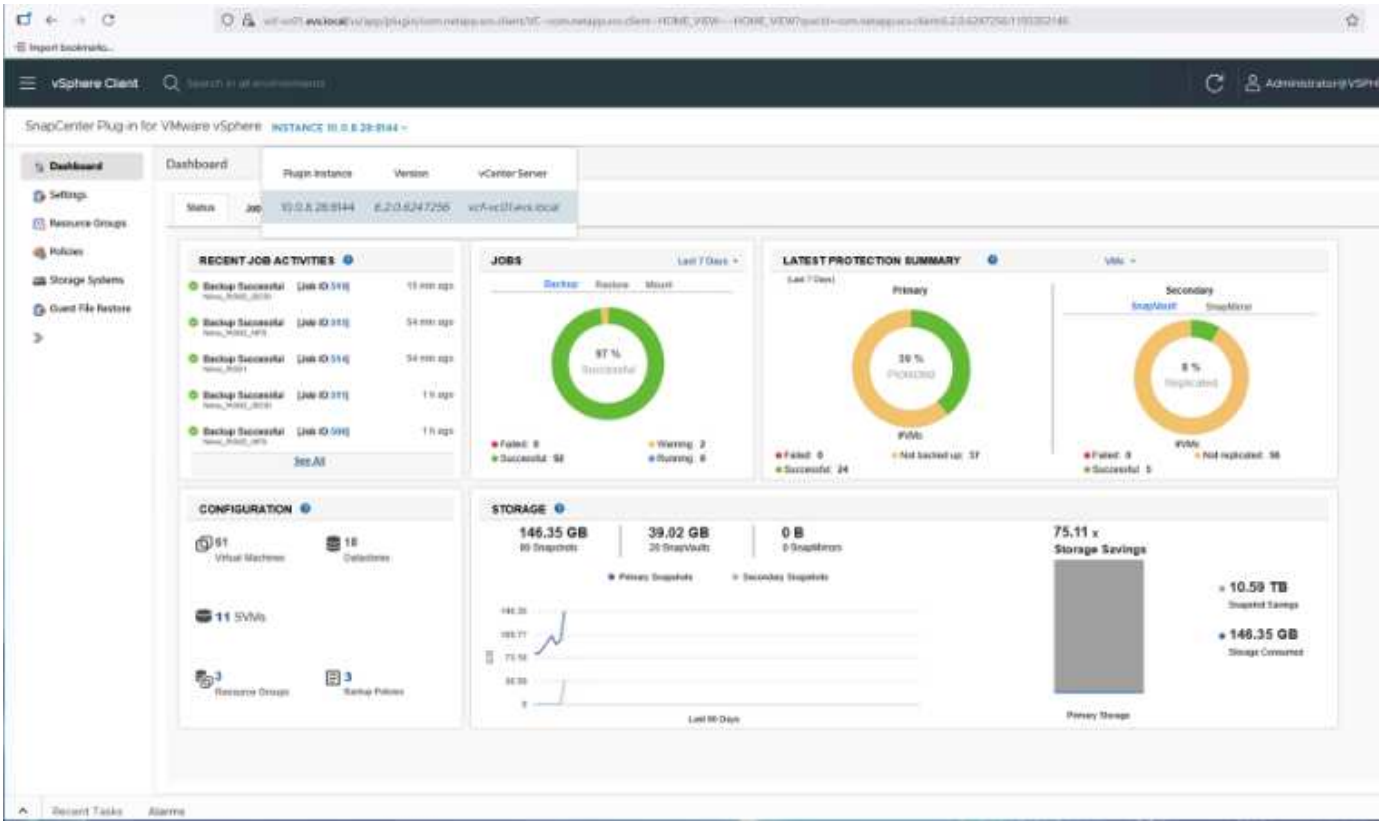
SCV está disponível gratuitamente.

Configurando o SnapCenter Plug-in para VMware

Para proteger as VMs e os datastores baseados em NFS/iSCSI que as hospedam, o SCV deve ser implantado. É uma simples importação de OVF.

As etapas para a implementação são as seguintes:

1. Baixe o OVA em "NetApp site de suporte".
2. Faça login no Amazon Exchange Virtual Server vCenter.
3. Dentro do vCenter, clique com o botão direito em qualquer objeto do inventário, como um data center, pasta, cluster ou host e selecione "Implantar modelo OVF".
4. Selecione as configurações corretas, incluindo armazenamento, segmento e personalize o modelo para atualizar o vCenter e suas credenciais, criar credenciais SCV e detalhes de endereço IP. Após a revisão, selecione "Concluir".
5. Aguarde as tarefas de importação e implantação do OVF serem concluídas.
6. Assim que o SCV for implantado com sucesso, ele será registrado dentro do vCenter.
7. Para acessar o plug-in, navegue até a barra lateral esquerda da página do cliente web vCenter e selecione "SnapCenter Plug-in for VMware".



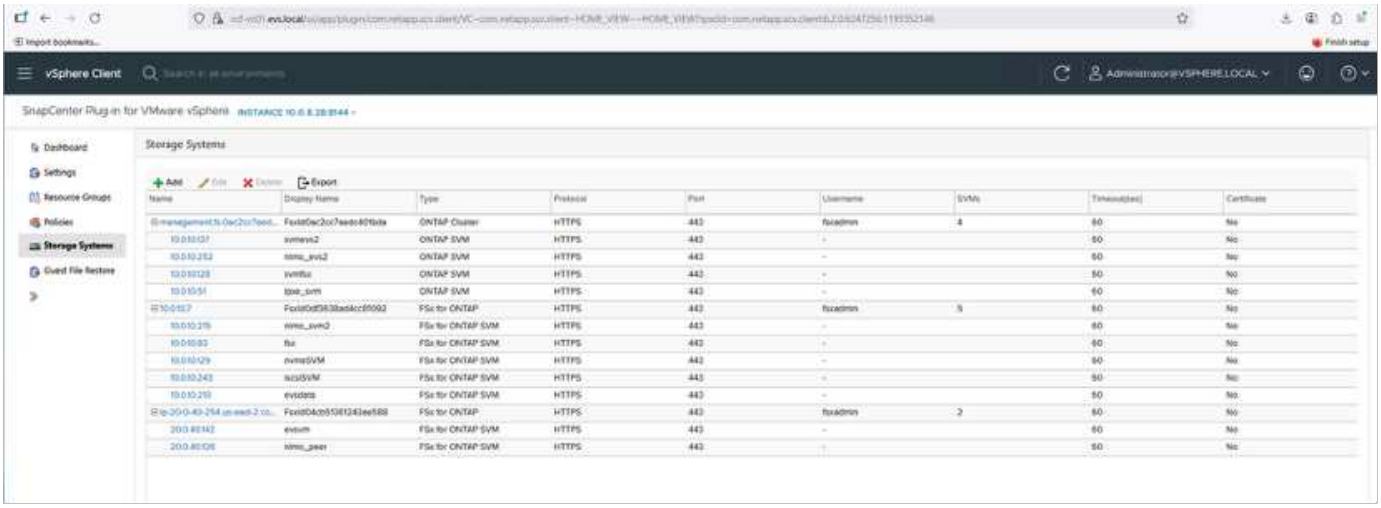
Procedimento de configuração do SnapCenter Plug-in para VMware

Esta seção aborda as etapas para configurar o SnapCenter Plug-in for VMware. As seções a seguir detalharão como adicionar storage, criar uma política de backup e como criar grupos de recursos.

Adicionando o sistema de storage

O próximo passo na proteção de cargas de trabalho com o SVC é adicionar o "sistema de storage". Adicionar armazenamento permite que o SCV detecte e gerencie operações de backup e restauração dentro do vCenter. Inclua o endpoint de gerenciamento do FSx for NetApp ONTAP ou o endereço IP do endpoint de administração da máquina virtual de armazenamento (SVM) como um sistema de storage para habilitar o backup e a restauração de máquinas virtuais.

1. No menu de navegação à esquerda do Exchange Virtual Server vCenter, selecione "SnapCenter Plug-in for VMware".
2. Selecione "sistema de storage".
3. Selecione "Adicionar" para adicionar os detalhes do FSx for ONTAP.
4. Utilize o método "Credenciais como autenticação" e insira FSxadmin como nome de usuário e senha. Em seguida, selecione "Adicionar" para salvar as configurações.



Todas as SVMs são adicionadas automaticamente quando o sistema de arquivos é adicionado.

Se a versão do SCV for 6.2, acesse "a página de suporte do SCV" e faça o download do SCV 6.2P1 release.

Criar uma política de backup

Uma estratégia de backup robusta deve definir fatores-chave como a programação de backup, os dados a serem copiados e o período de retenção dos backups. Cópias Snapshot podem ser agendadas em intervalos de hora em hora ou diariamente para proteger datastores inteiros. Agendar backups dessa forma não só protege os datastores, mas também suporta as operações de backup e restauração das VMs e VMDKs contidos nesses datastores.

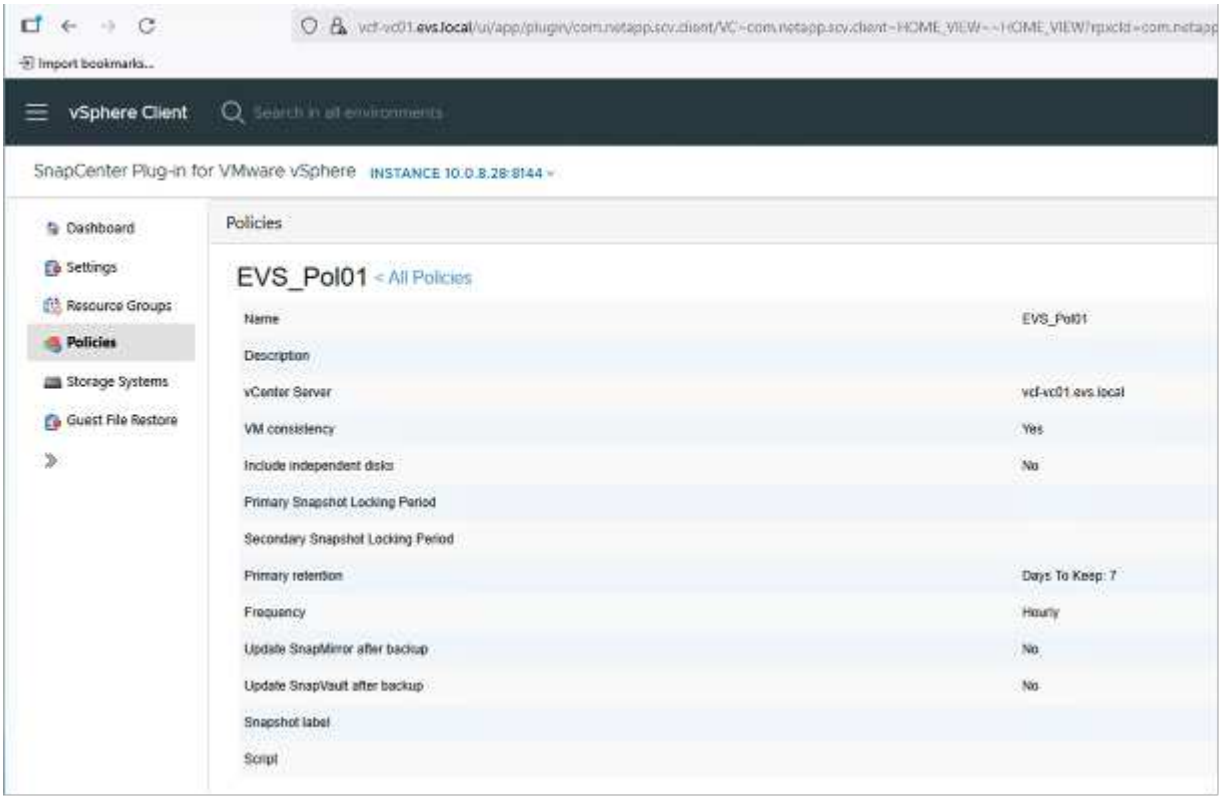
Antes de iniciar backups para VMs e datastores, crie uma "política de backup" política de backup e um grupo de recursos. A política de backup especifica parâmetros como o agendamento de backup e as configurações de retenção.

Aqui estão as etapas para criar uma política de backup:

1. Acesse o menu de navegação à esquerda no SCV e selecione "Policies".
2. Na página Policies, selecione "Create" para iniciar o assistente.
3. Na página "New Backup Policy", insira um nome para a política.

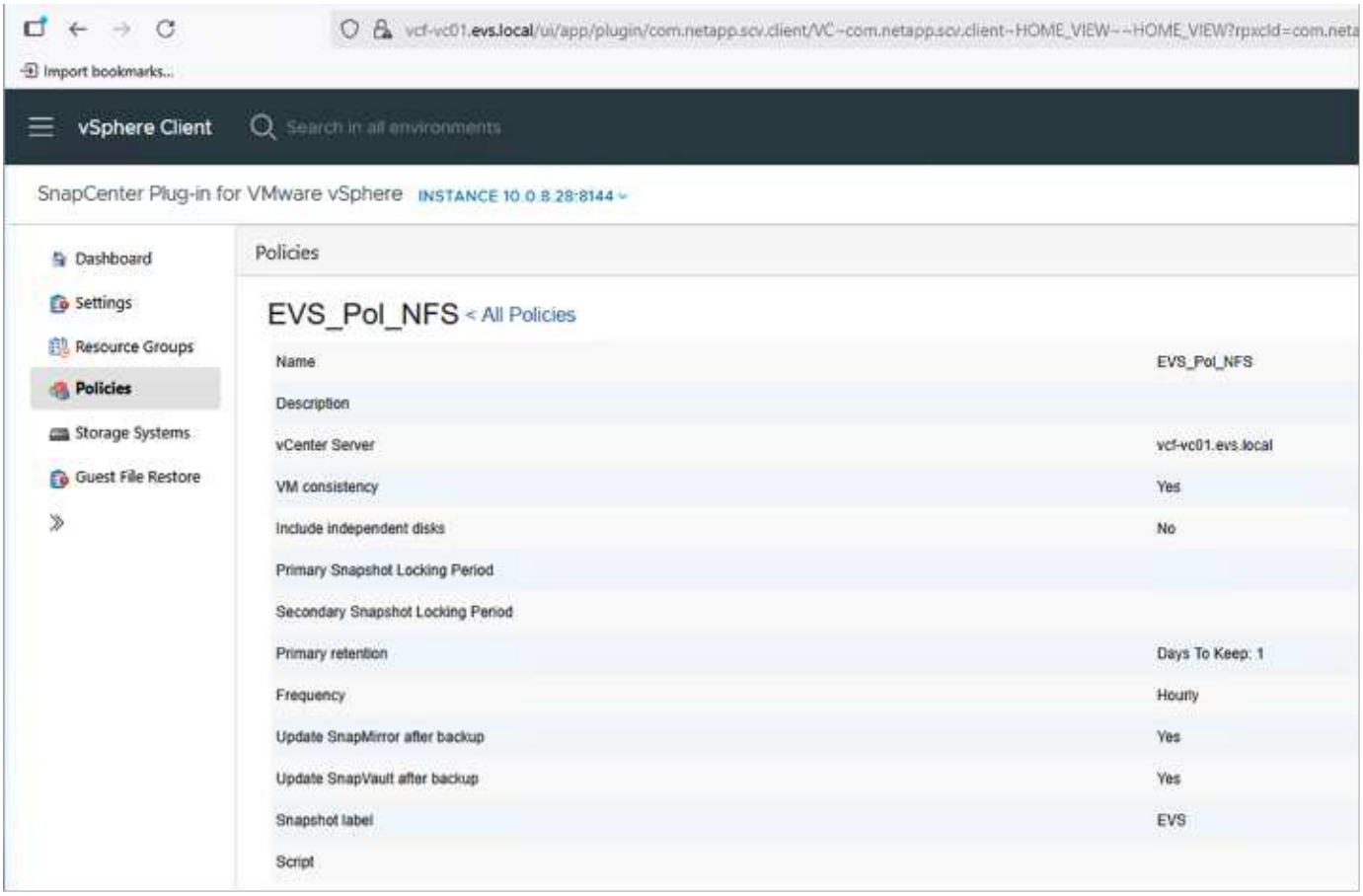
4. Especifique o período de retenção, a frequência de backup e as configurações de replicação.
5. Selecione a caixa de seleção "Período de Bloqueio" para ativar o bloqueio de Snapshot. Você pode selecionar os períodos de bloqueio de Snapshot primário e secundário como Dias/Meses/Anos.

Independentemente do valor de retenção definido na política SnapMirror, a cópia Snapshot secundária permanece intacta até que o período de bloqueio do Snapshot secundário especificado expire.



Para habilitar backups consistentes com a VM, as ferramentas VMware devem estar instaladas e em execução. Quando a caixa de consistência da VM está marcada, as VMs são primeiro colocadas em estado quiescente, em seguida o VMware realiza um snapshot consistente com a VM (excluindo memória), depois o SCV executa sua operação de backup, e então as operações da VM são retomadas.

Para replicar cópias Snapshot para um sistema de arquivos de espelho ou vault secundário, os relacionamentos devem ser configurados previamente.



Após a criação da política, o próximo passo é criar o grupo de recursos que definirá os datastores NFS ou iSCSI e as máquinas virtuais apropriadas que devem ser backup.

Criar um grupo de recursos

Um grupo de recursos serve como um contêiner para máquinas virtuais e datastores que precisam de proteção. Recursos podem ser adicionados ou removidos de um grupo de recursos a qualquer momento, proporcionando flexibilidade no gerenciamento das configurações de backup.

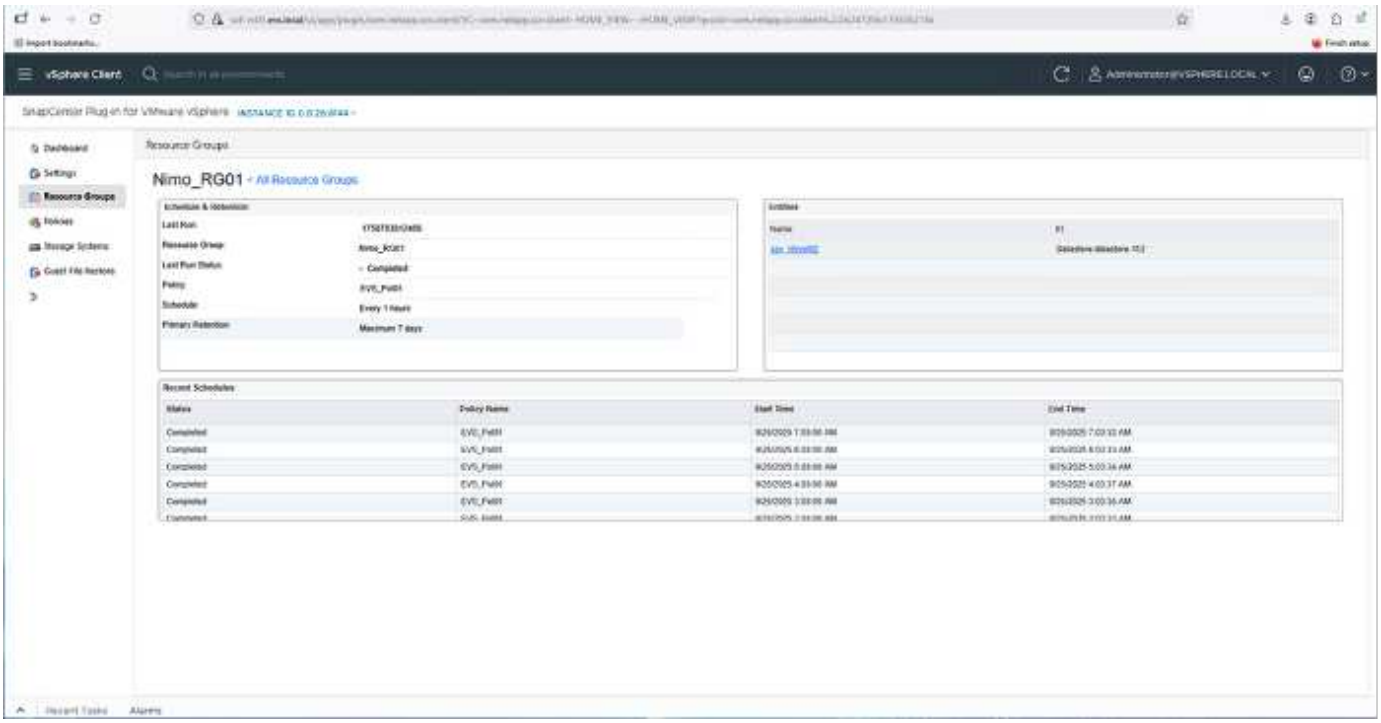
Você pode criar um "grupo de recursos" usando as etapas a seguir:

1. Vá para o painel de navegação à esquerda no SCV e selecione "Resource Groups".
2. Na página Grupos de Recursos, selecione "Criar" para iniciar o assistente de criação de grupo de recursos.

> Outra opção para criar grupos de recursos é selecionar uma máquina virtual ou um datastore individual e criar um grupo de recursos que contenha apenas esse recurso.

3. Na página "Resources", selecione o escopo (VMs ou datastores) e o data center.
4. Na página "Spanning disks", selecione a opção "Virtual Machines with multiple VMDKs across multiple datastores".
5. Em seguida, associe uma política de backup. Selecione uma política existente ou crie uma nova política de backup.
6. Na página "Agendamentos", configure o agendamento de backup para cada política selecionada.

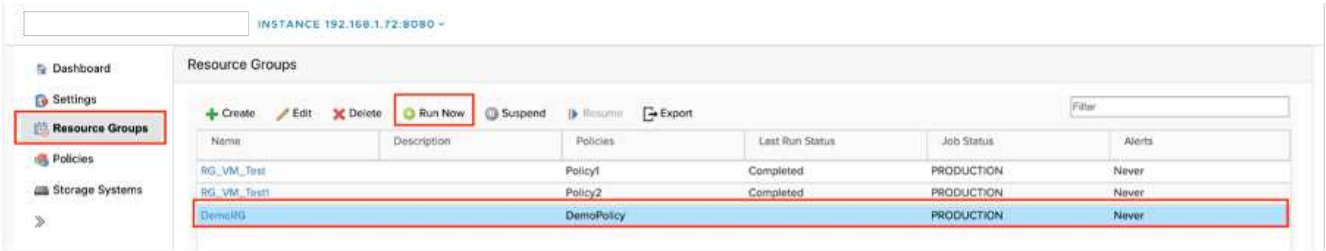
7. Após selecionar as opções adequadas, clique em "Concluir". Isso criará um novo grupo de recursos e o adicionará à lista de grupos de recursos.



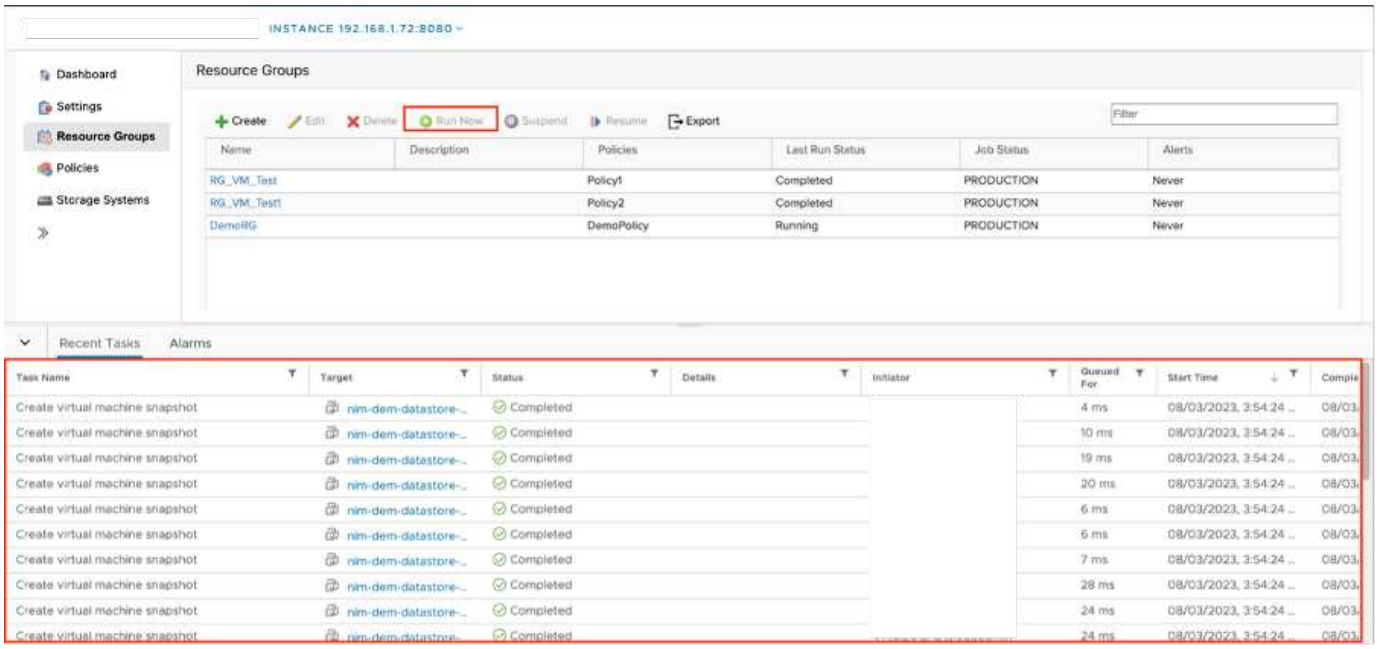
Backup de grupos de recursos

As operações de backup são executadas em todos os recursos definidos dentro de um grupo de recursos. Se um grupo de recursos tiver uma política associada e um agendamento configurado, os backups ocorrem automaticamente de acordo com o agendamento.

1. Na navegação à esquerda da página do cliente web vCenter, selecione "SnapCenter Plug-in for VMware" e depois "Resource Groups".
2. Na página Grupos de Recursos, encontre o grupo de recursos designado e selecione "Executar agora" para iniciar o backup manual.



3. Se o grupo de recursos tiver várias políticas configuradas, selecione a política para a operação de backup na caixa de diálogo "Backup Now".
4. Selecione "OK" para iniciar o backup.

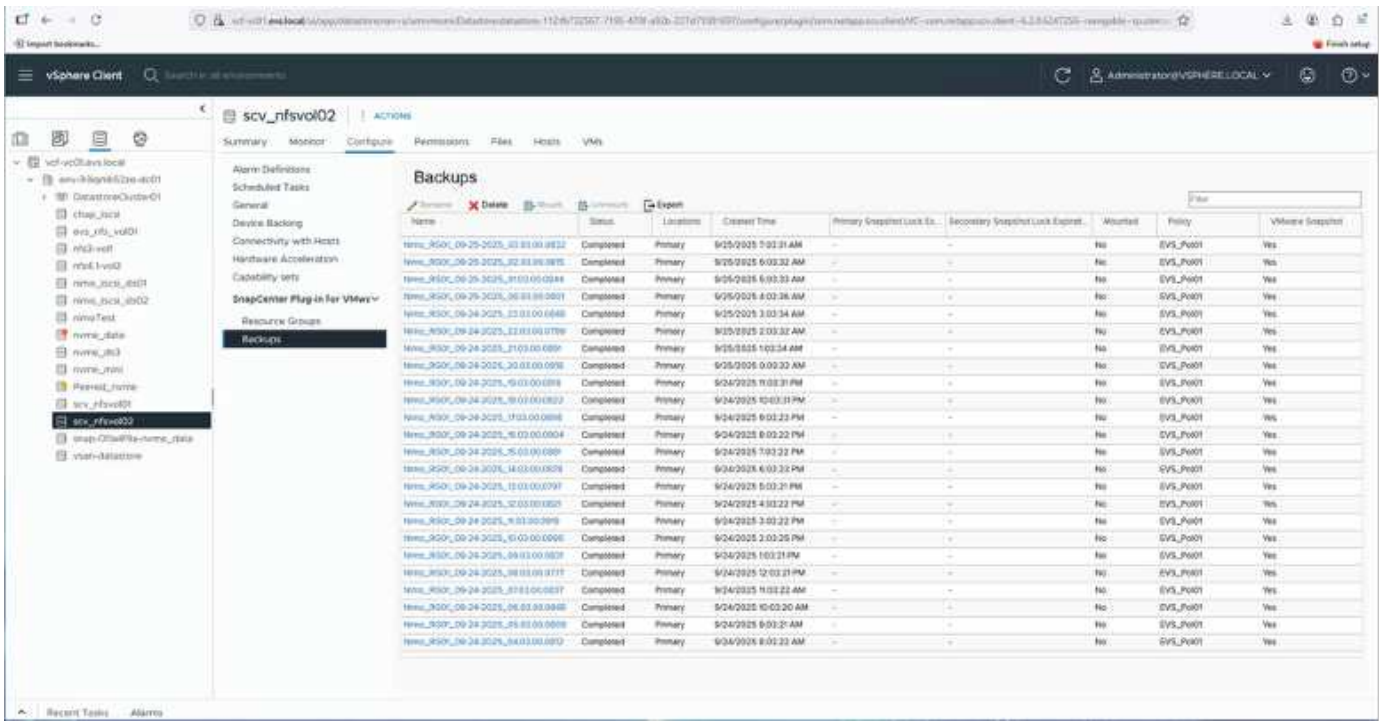


Monitore o progresso da operação selecionando "Tarefas Recentes" na parte inferior da janela ou, para mais detalhes, selecionando "Monitor de Tarefas" no painel.

O processo para criar políticas de backup, configurar grupos de recursos e executar operações de backup é consistente em diferentes protocolos de storage, incluindo NFS e iSCSI.

Os backups são realizados de acordo com o cronograma definido na política.

Após a conclusão do backup, ele pode ser visualizado no nível do datastore ou para máquinas virtuais individuais, selecionando "SnapCenter Plug-in for VMware vSphere" na lista suspensa e, em seguida, escolhendo "Restaurar".



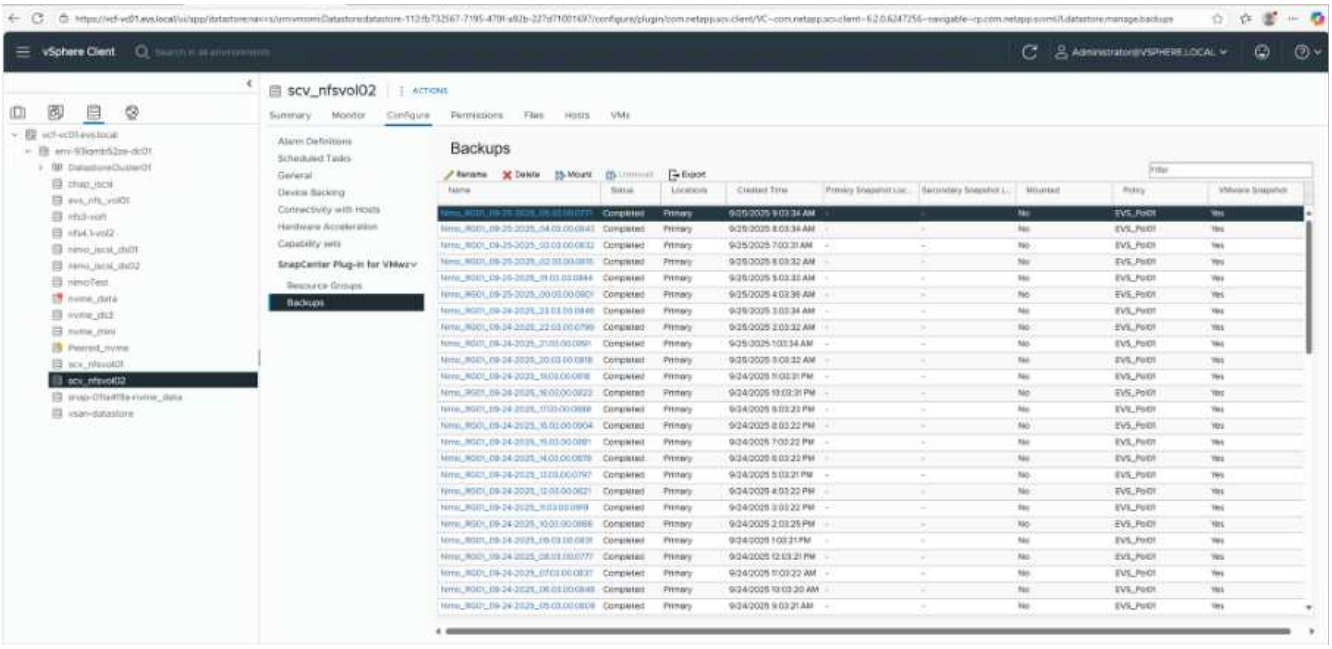
Procedimento de restauração para VMs protegidas pelo SnapCenter Plug-in for VMware

Esta seção aborda os passos para restaurar VMs a partir de backups. O SCV pode ser usado para restaurar VMs dentro do vCenter, permitindo que elas sejam recuperadas para o datastore original no host ESXi original (sobrescrevendo o conteúdo existente), para restaurar VMs excluídas ou renomeadas a partir de uma cópia de backup, para um datastore diferente no host ESXi original, para o datastore original em um host ESXi diferente gerenciado pelo mesmo vCenter, ou para um datastore diferente em outro host ESXi dentro do mesmo vCenter environment.

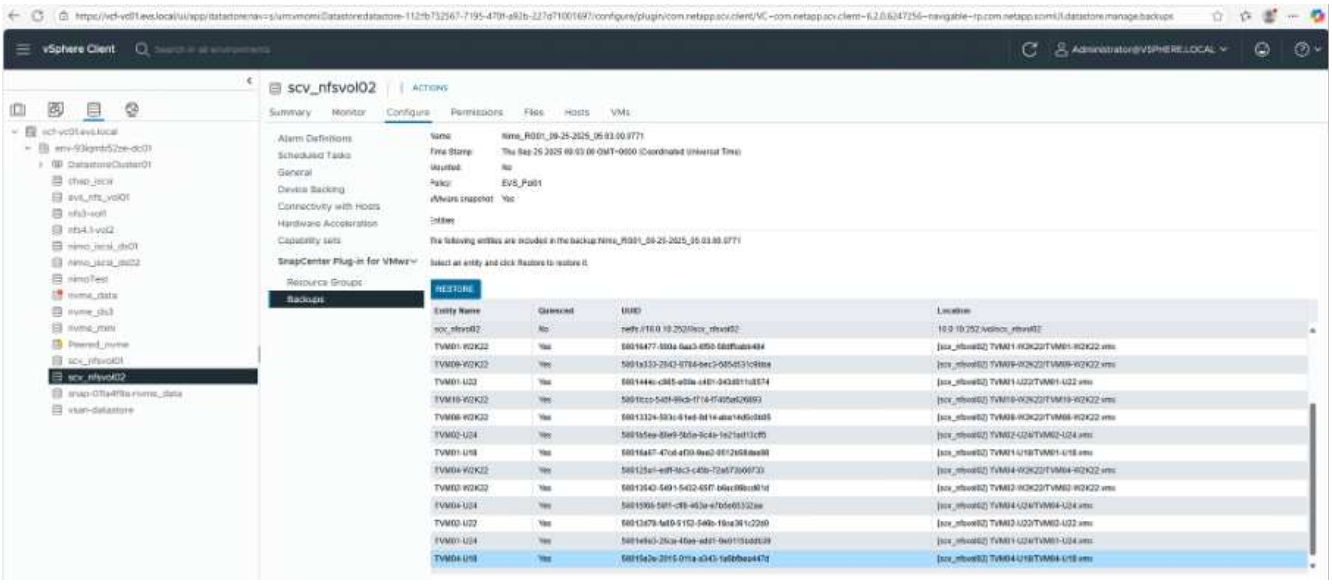
Etapas para realizar a operação de restauração

Para realizar a operação de restauração, siga estes passos:

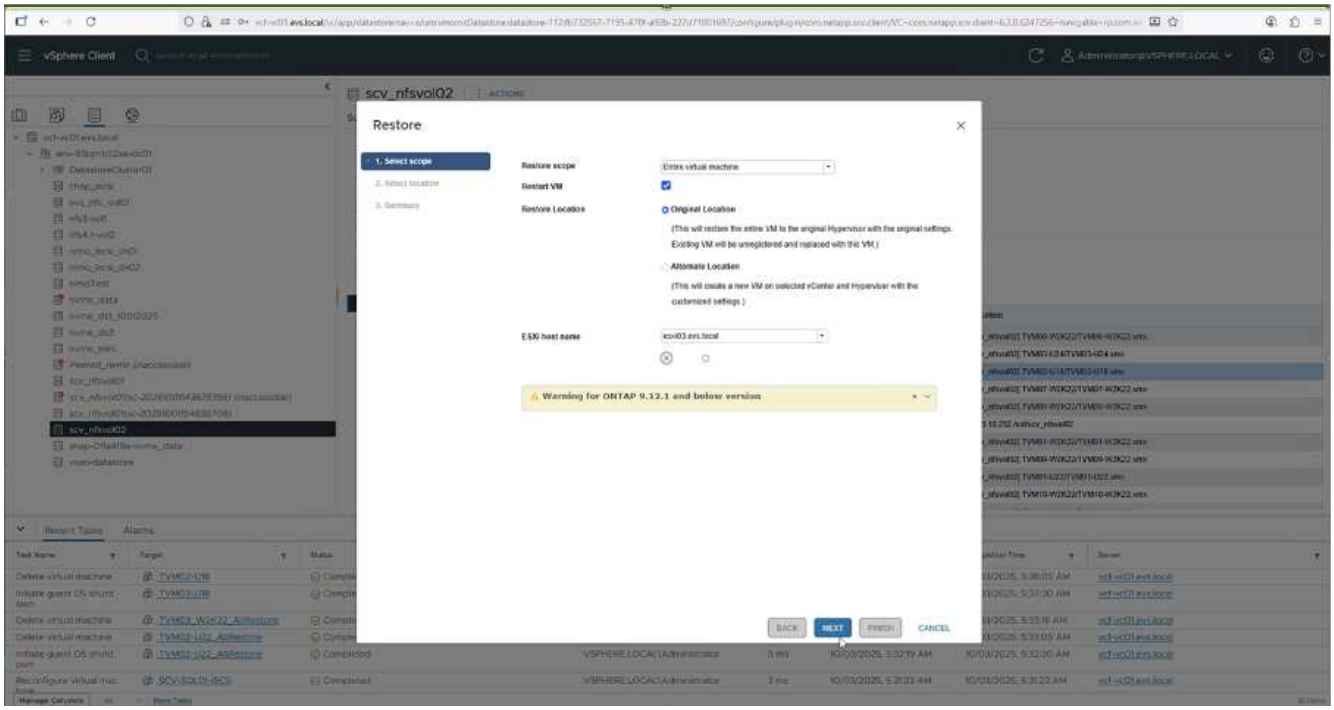
1. No cliente web do Exchange Virtual Server vSphere, vá para **Inventory › Datastores** e selecione o datastore desejado. Em seguida, navegue até **Configure › Backups** na seção "SnapCenter Plug-in for VMware vSphere".



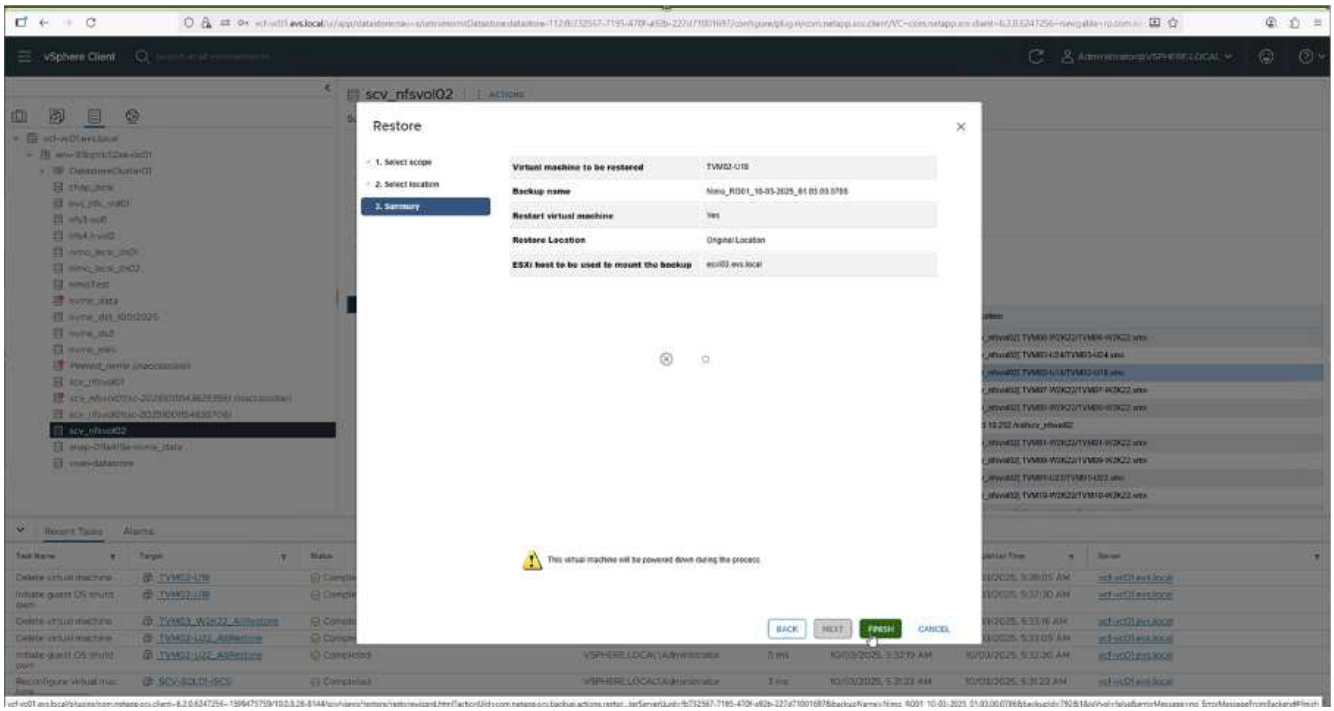
2. Clique duas vezes em um backup para visualizar todas as VMs incluídas nesse backup. Encontre a VM que deseja restaurar na lista e selecione "Restaurar".



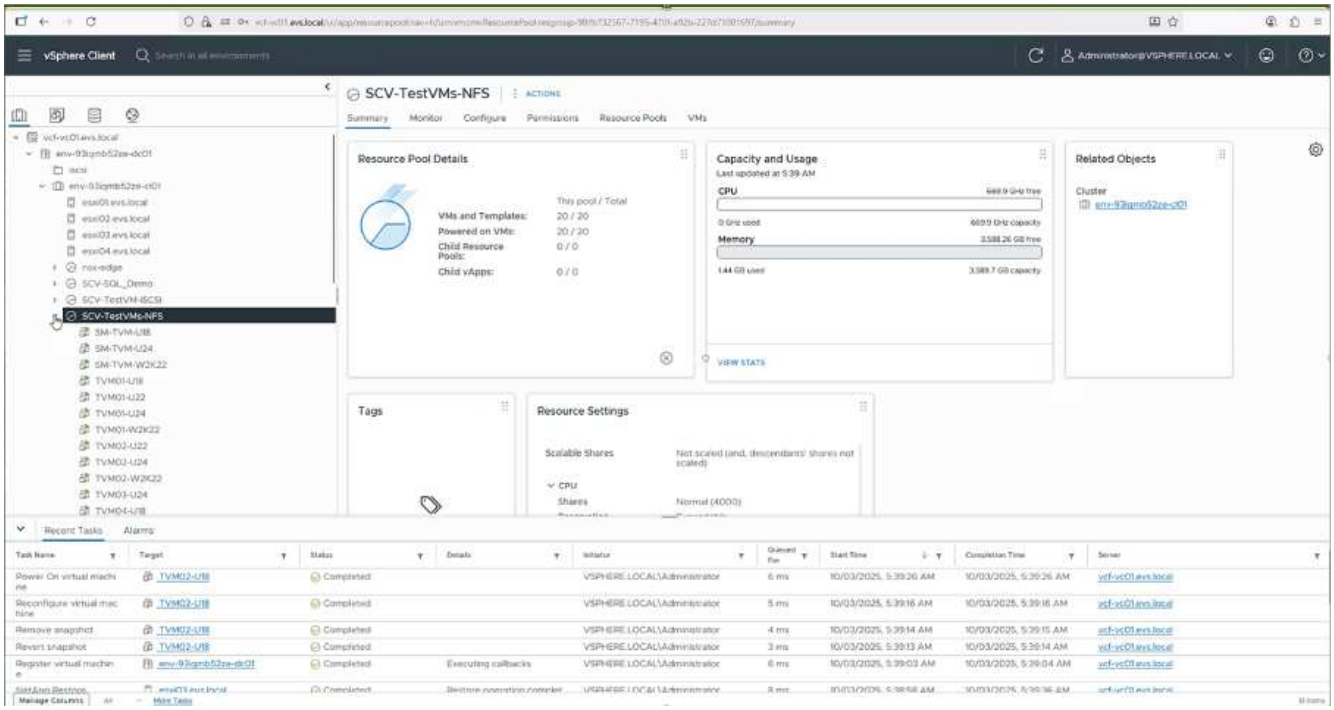
3. Na página "Selecionar Escopo", selecione "Máquina Virtual Inteira" no campo "Escopo de Restauração", depois selecione "Local de Restauração" e insira as informações do ESXi de destino onde o backup deve ser montado.
4. Marque a caixa de seleção "Restart VM" se a máquina virtual precisar ser ligada após a operação de restauração.
5. Na página "Select Location", selecione um local principal.



6. Revise a página "Resumo" e, em seguida, selecione "Concluir".



7. Monitore o progresso da operação selecionando "Tarefas recentes" na parte inferior da tela.



Embora as VMs sejam restauradas, elas não são adicionadas automaticamente aos seus grupos de recursos anteriores. Se você quiser proteger essas VMs, adicione-as manualmente aos grupos de recursos apropriados.

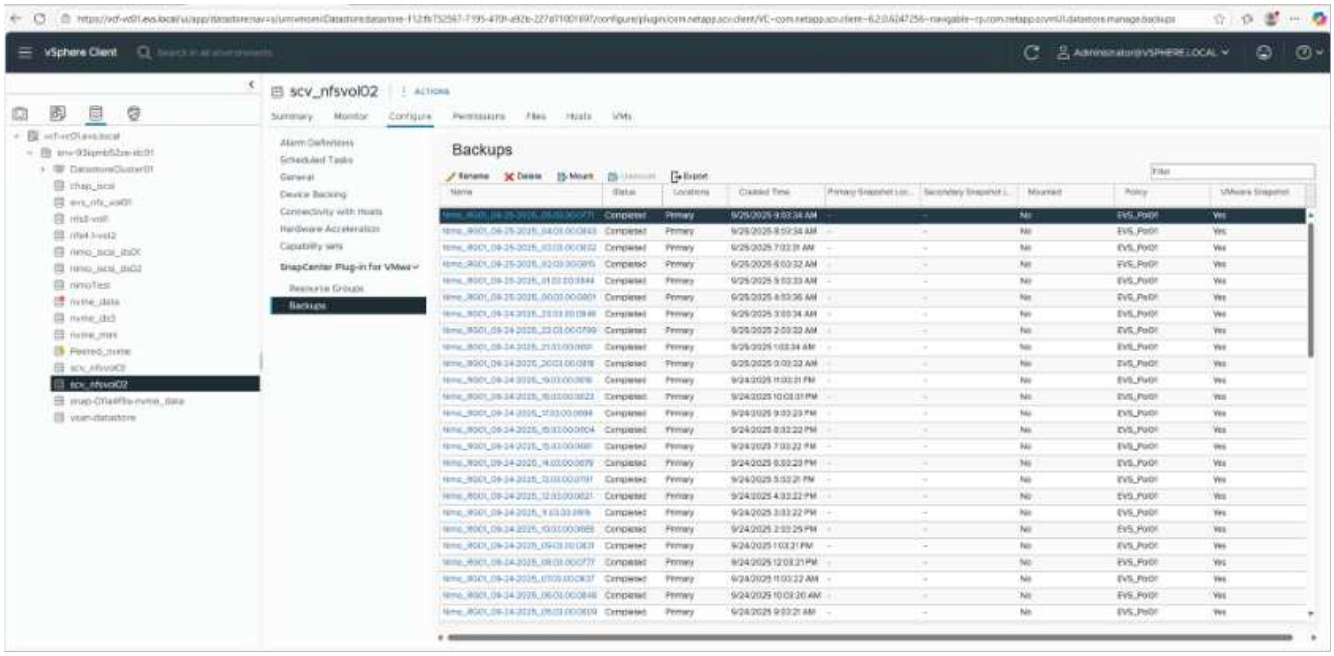
A operação de restauração também pode ser acionada a partir do nível de máquina virtual individual.

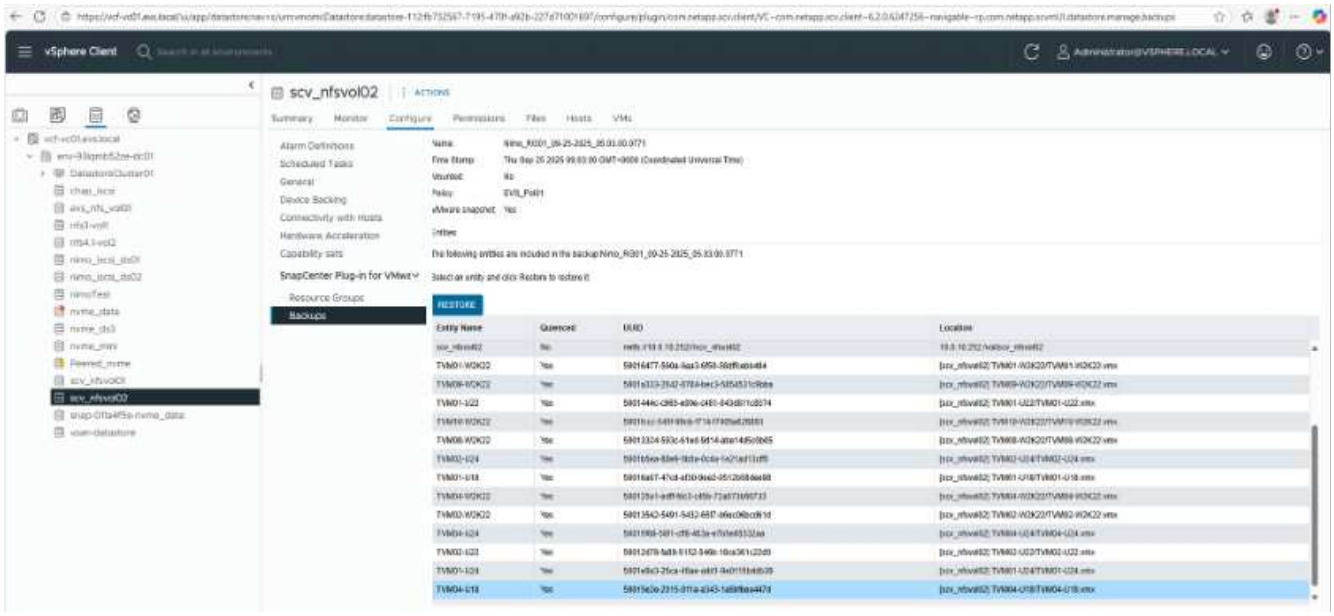
Passos para restaurar uma máquina virtual excluída

Restaurar uma máquina virtual excluída é um processo simples com SCV.

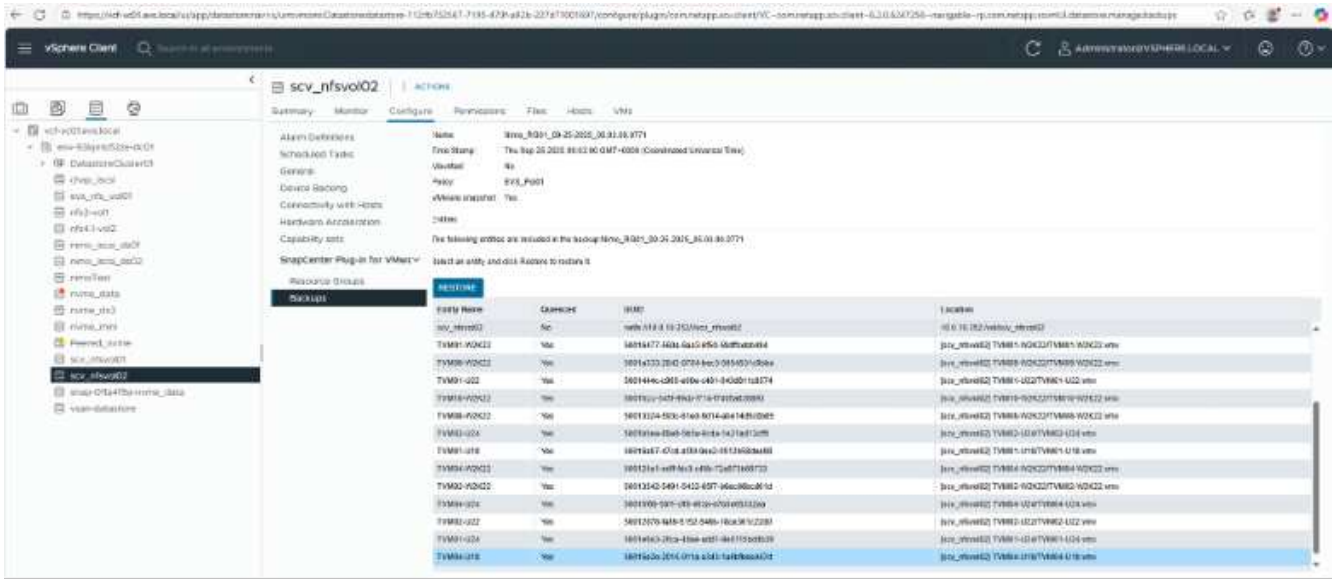
A operação de restauração de uma máquina virtual excluída pode ser realizada a partir do nível do datastore.

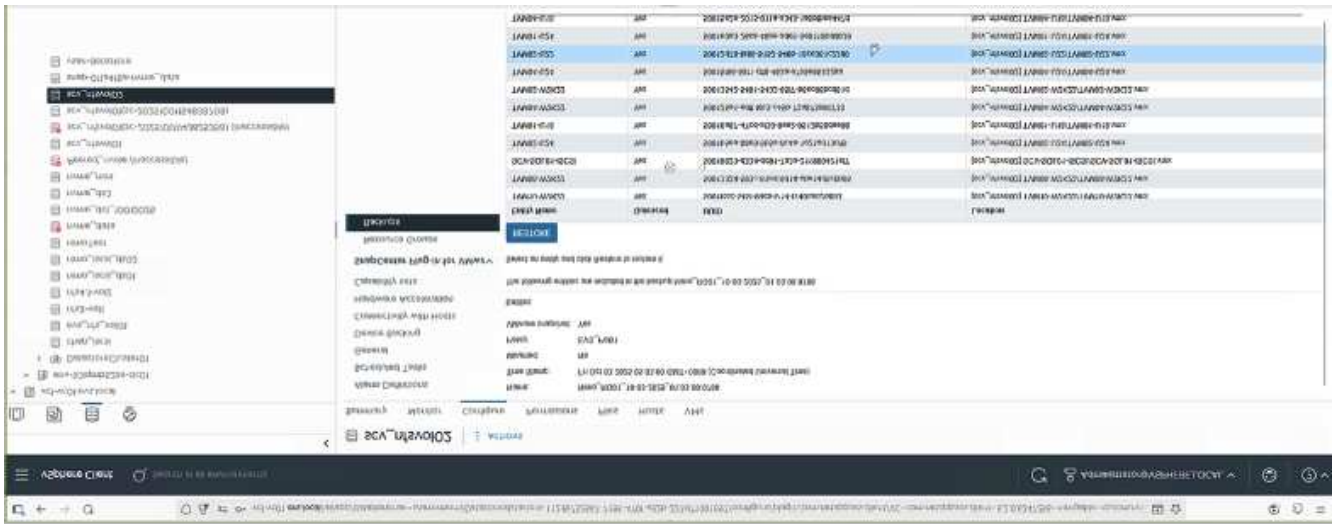
1. Acesse o Datastore correspondente > Configurar > Backups. Lá, selecione a máquina virtual excluída e selecione "Restaurar".

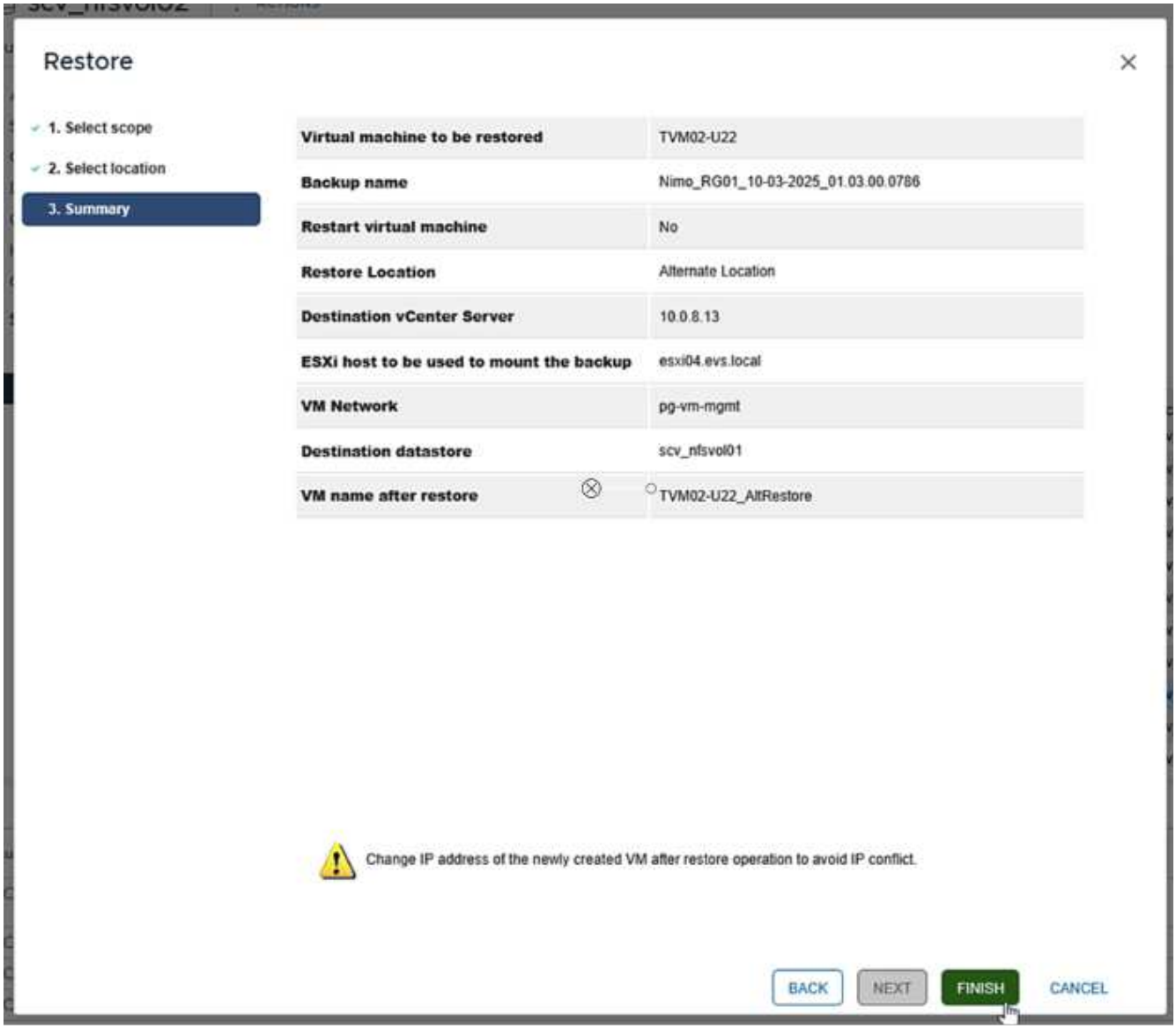


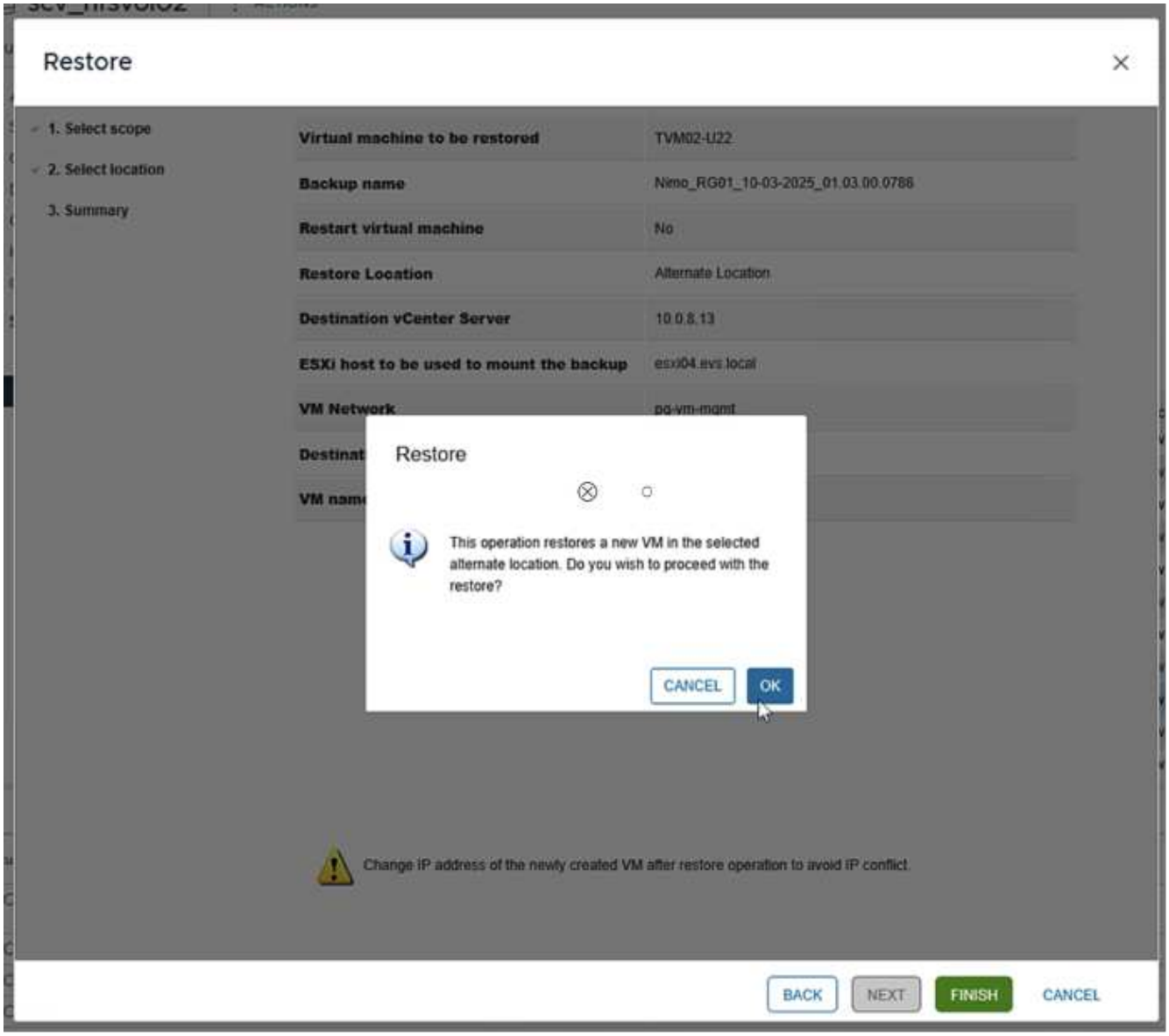


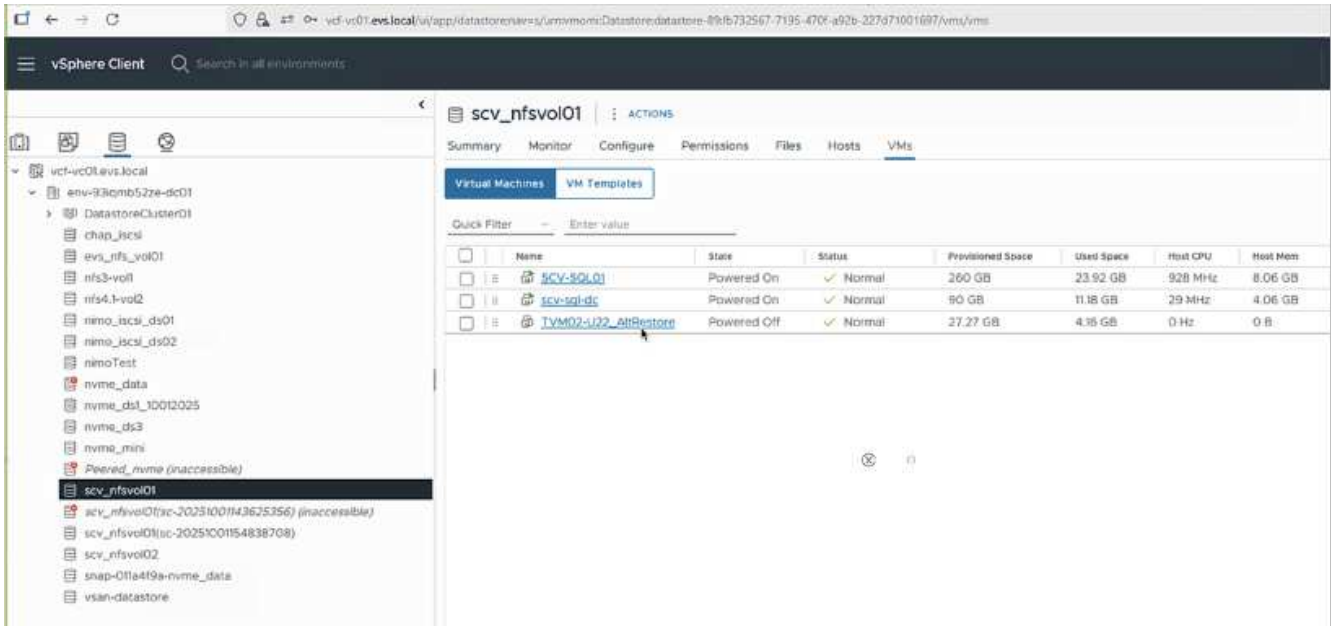
2. O fluxo de capturas de tela a seguir abrange a restauração de uma máquina virtual para um host ESXi alternativo e um datastore diferente.


vSphere Client
scv_nfsvol02
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
SnapCenter Plug-in for VMware
Resource Groups
Backups
RESTORE


vSphere Client
scv_nfsvol02
RESTORE


Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Destination datastore
scv_nfsvol01
VM name after restore
TVM02-U22_AltRestore
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL

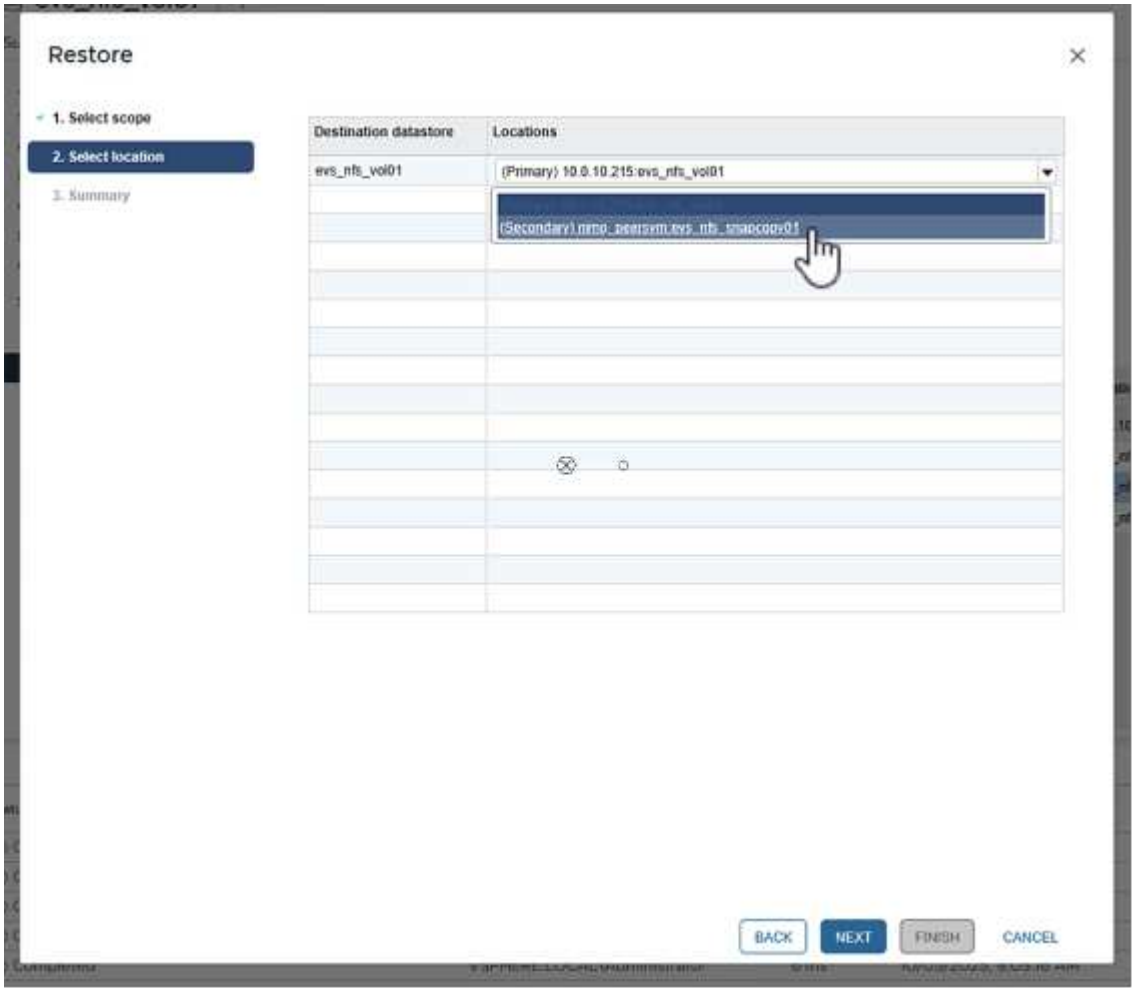

Restore
1. Select scope
2. Select location
3. Summary
Virtual machine to be restored
TVM02-U22
Backup name
Nimo_RG01_10-03-2025_01.03.00.0786
Restart virtual machine
No
Restore Location
Alternate Location
Destination vCenter Server
10.0.8.13
ESXi host to be used to mount the backup
esxi04.evs.local
VM Network
pg-vm-mgmt
Restore
This operation restores a new VM in the selected alternate location. Do you wish to proceed with the restore?
CANCEL
OK
Change IP address of the newly created VM after restore operation to avoid IP conflict.
BACK
NEXT
FINISH
CANCEL


vSphere Client
scv_nfsvol01
ACTIONS
Summary
Monitor
Configure
Permissions
Files
Hosts
VMs
Virtual Machines
VM Templates
Quick Filter
Enter value
Name
State
Status
Provisioned Space
Used Space
Host CPU
Host Mem
SCV-SQL01
Powered On
Normal
260 GB
23.92 GB
928 MHz
8.06 GB
scv-sql-dc
Powered On
Normal
90 GB
11.18 GB
29 MHz
4.06 GB
TVM02-U22_AltRestore
Powered Off
Normal
27.27 GB
4.16 GB
0 Hz
0 B
vcf-vc01.evs.local
env-93ojmb52ze-dc01
DatastoreCluster01
chap_iscsi
evs_nfs_vol01
nfs3-vol1
nfs4.1-vol2
nimo_iscsi_ds01
nimo_iscsi_ds02
nimoTest
nvme_data
nvme_ds1_10012025
nvme_ds3
nvme_mini
Peered_nvme (inaccessible)
scv_nfsvol01
scv_nfsvol01(sc-20251001154838708)
scv_nfsvol02
snap-011a4f9a-nvme_data
vsan-datastore

O datastore de destino deve ter espaço livre adequado e o vCenter especificado no campo "Restaurar para local alternativo" deve ser resolvível por DNS.

Para uma melhor eficiência de restauração em ambientes NFS, ative a API vStorage da VMware para Integração de Arrays (VAAI).

As restaurações também podem ser realizadas a partir de locais secundários, como um destino do SnapMirror.



+

Procedimento de restauração para arquivos e pastas convidados protegidos pelo SnapCenter Plug-in for VMware

A seção a seguir mostra como restaurar arquivos e pastas de guest a partir de VMDKs.

SnapCenter suporta a restauração de arquivos e pastas de VMDKs somente quando o sistema operacional convidado é Windows.

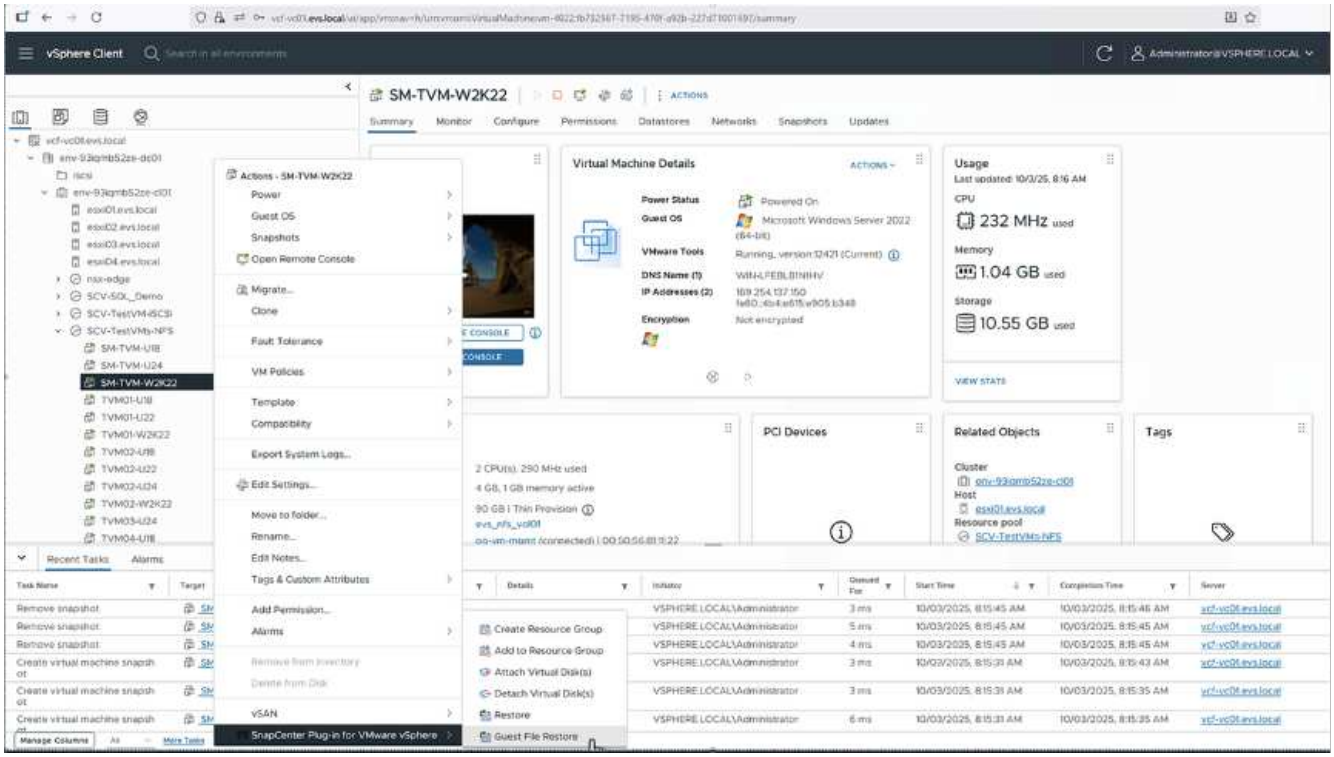
Considerações sobre a restauração de arquivos e pastas de convidados com SCV:

- VMware tools devem estar em execução na máquina virtual.
- O VMDK anexado fica acessível por 24 horas por padrão.

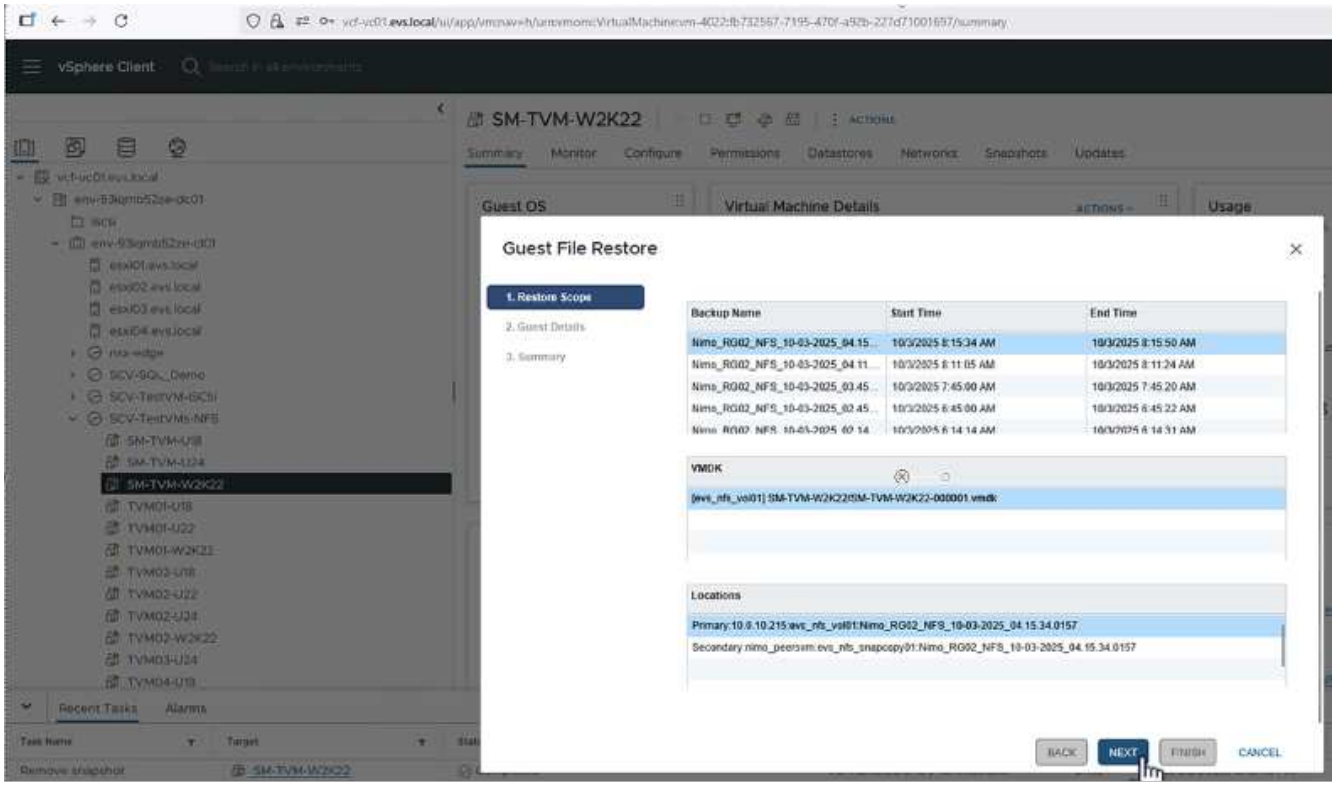
- Apenas uma operação de restauração ou de conexão pode ser realizada em uma máquina virtual por vez.
- Arquivos de sistema, ocultos e criptografados podem ser restaurados; no entanto, seus atributos originais não serão preservados.
- Evite restaurar arquivos criptografados para pastas criptografadas ou sobrescrever arquivos do sistema.

Etapas para a restauração de arquivos e pastas do guest:

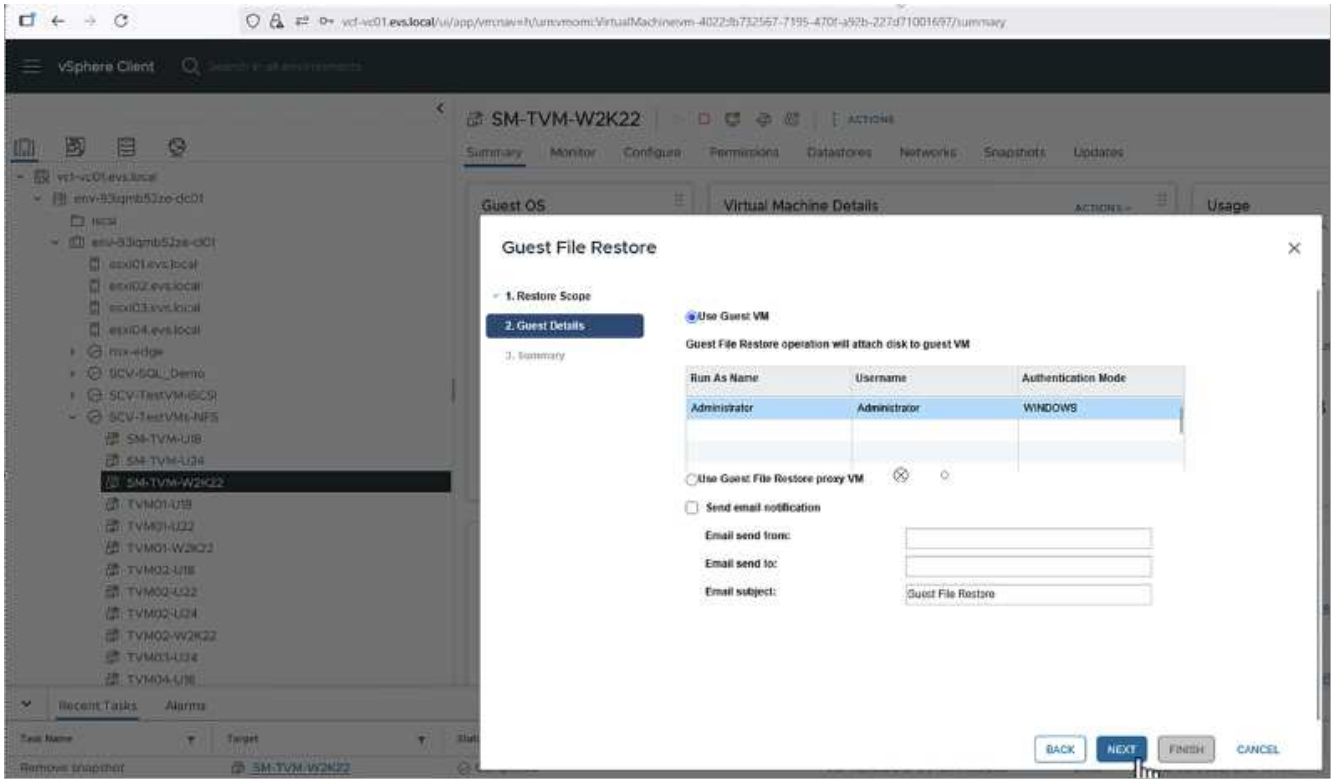
1. Clique com o botão direito do mouse na máquina virtual de destino e selecione "**NetApp SnapCenter › Guest File Restore**.



2. Escolha o backup que contém o VMDK necessário. Especifique o VMDK e sua localização (primário ou secundário).

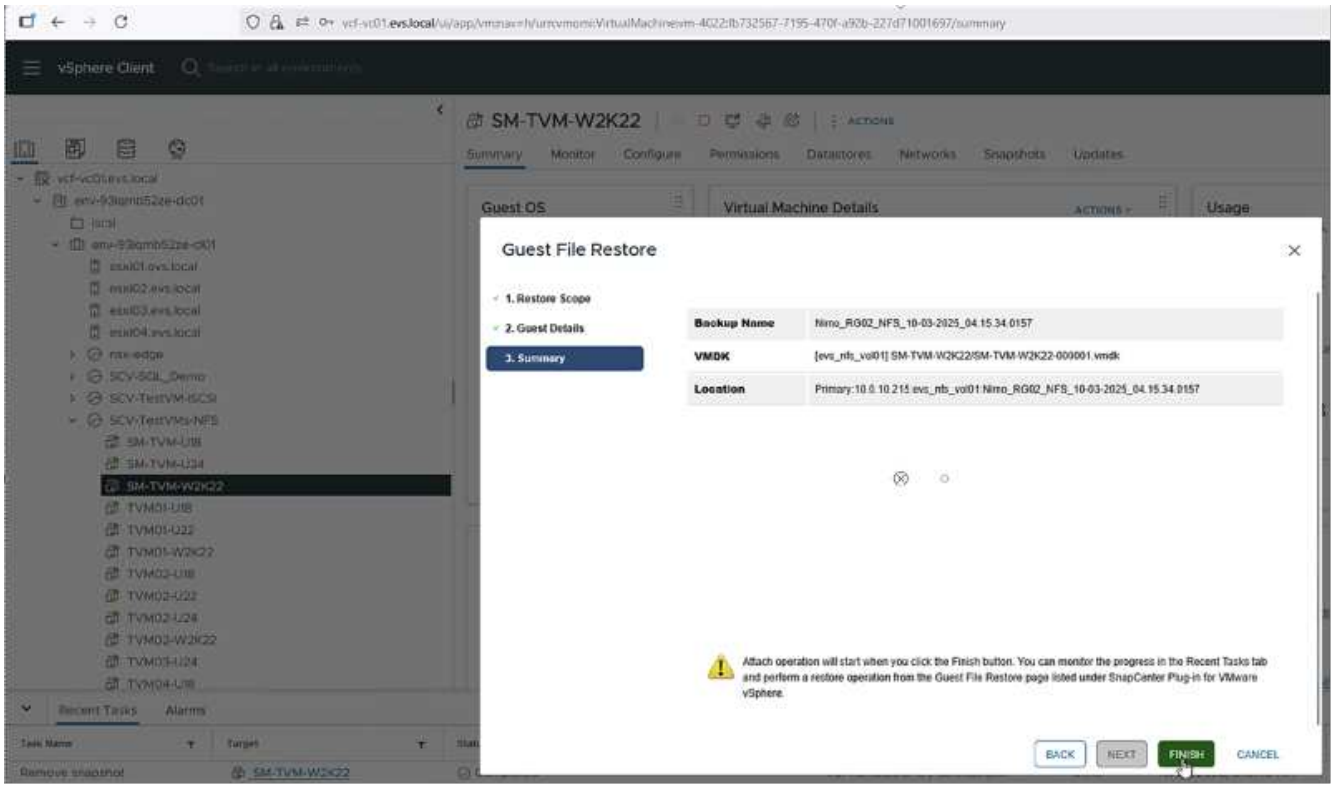


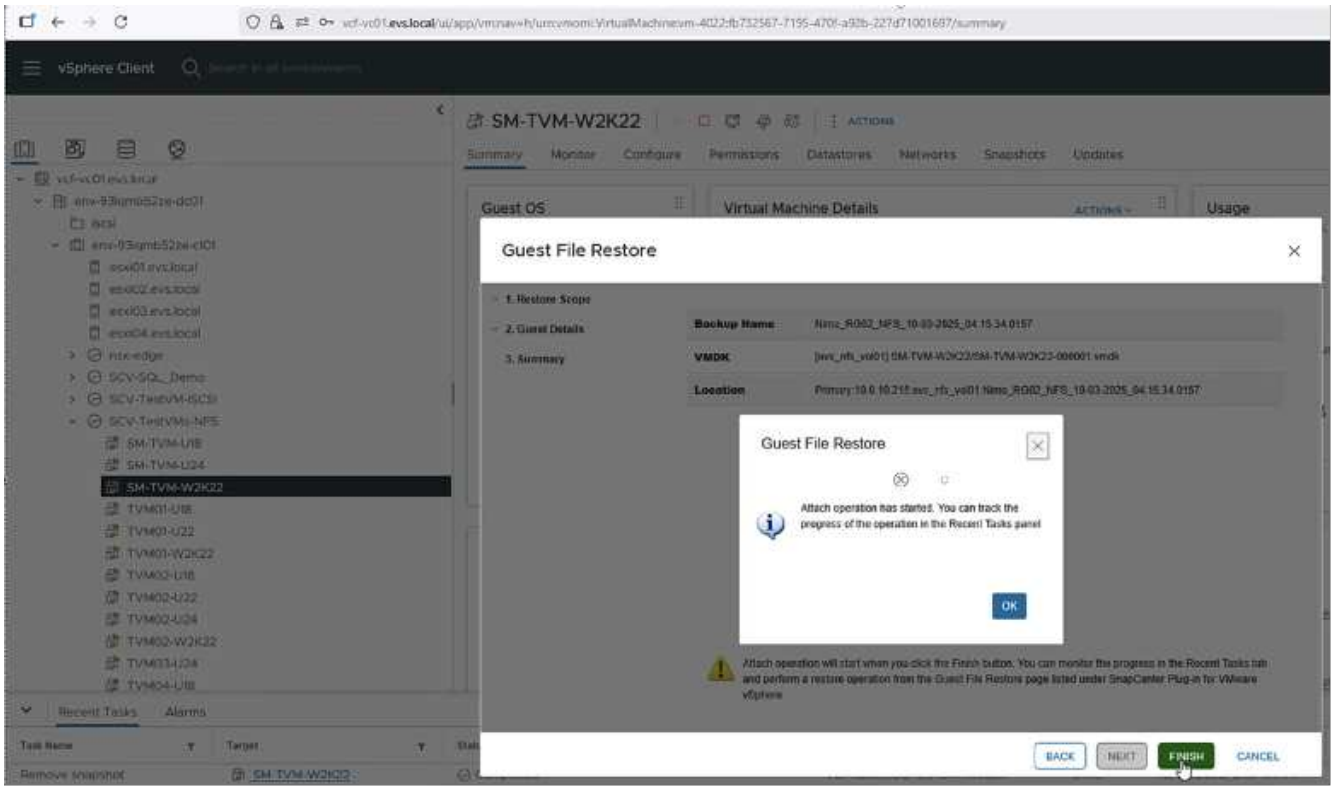
3. Escolha "Disk Attachment Method".



- Opção de VM convidada: anexe o disco à VM original (requer credenciais pré-configuradas). Esta é a opção usada nesta demonstração.
- Opção de VM proxy: anexe o disco a uma VM proxy designada (deve ser configurada com antecedência).

4. Aguarde a conclusão da operação de anexação antes de navegar e restaurar arquivos. Assim que a operação for concluída, SnapCenter cria automaticamente uma sessão de restauração de arquivos do convidado.





5. Navegue até o VMDK na sessão de Guest File Restore, selecione os arquivos ou pastas necessários e restaure-os para o local especificado.

Procedimentos de proteção para bancos de dados executados em VMDKs da VMware com SnapCenter for SQL (SCSQL)

A seção a seguir mostra como proteger bancos de dados em execução em VMDKs da VMware com SnapCenter para SQL (SCSQL).

Configurando o SCSQL

A configuração para usar SCSQL para proteger bancos de dados em VMDKs é a seguinte:

1. "Instale e configure" Servidor SnapCenter.
2. Faça login no SnapCenter.
3. Configurar o ambiente SnapCenter:
   - "Adicionar ou atribuir" conexões do sistema de storage.
   - "Criar" credenciais.
4. Para bancos de dados Microsoft SQL Server em VMDKs da VMware:
   - "Implantar SCV" (já abordado na seção de configuração).
   - Registre o plug-in com SnapCenter.
5. Adicionar "Hosts do SQL Server e instalam plug-ins":
   - "Configurar os plug-ins SQL".
   - "Configure o plano de proteção e os agendamentos para o banco de dados e os logs".

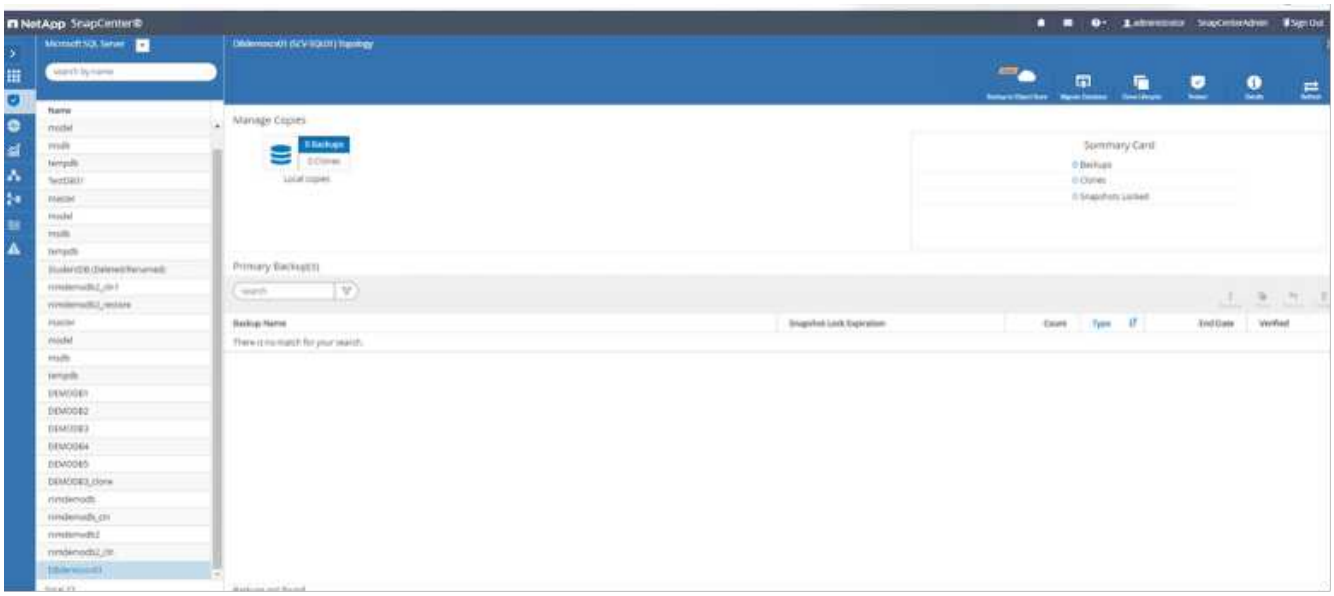


Configuração de uma política de backup

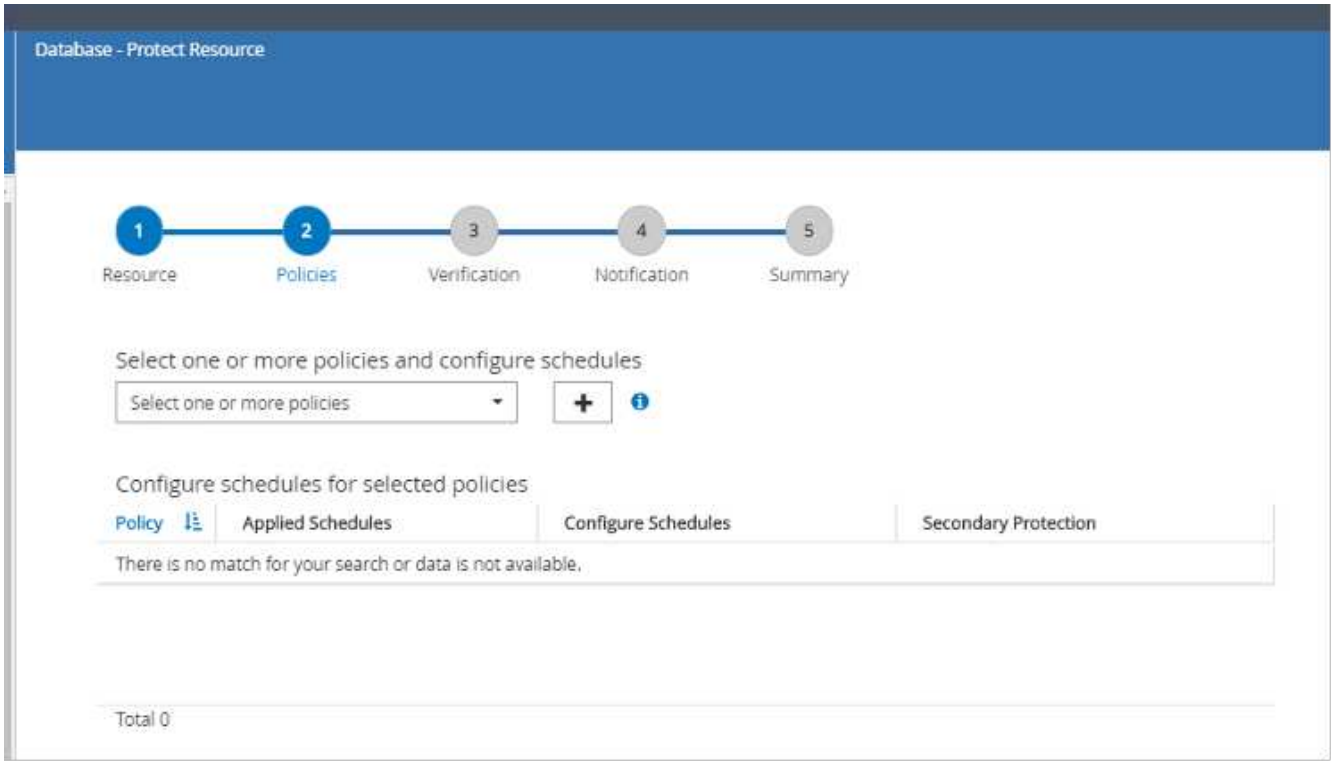
As etapas a seguir mostrarão como configurar uma política de backup.

1. Selecione o banco de dados na guia de recursos e selecione "Proteger" no canto superior direito.

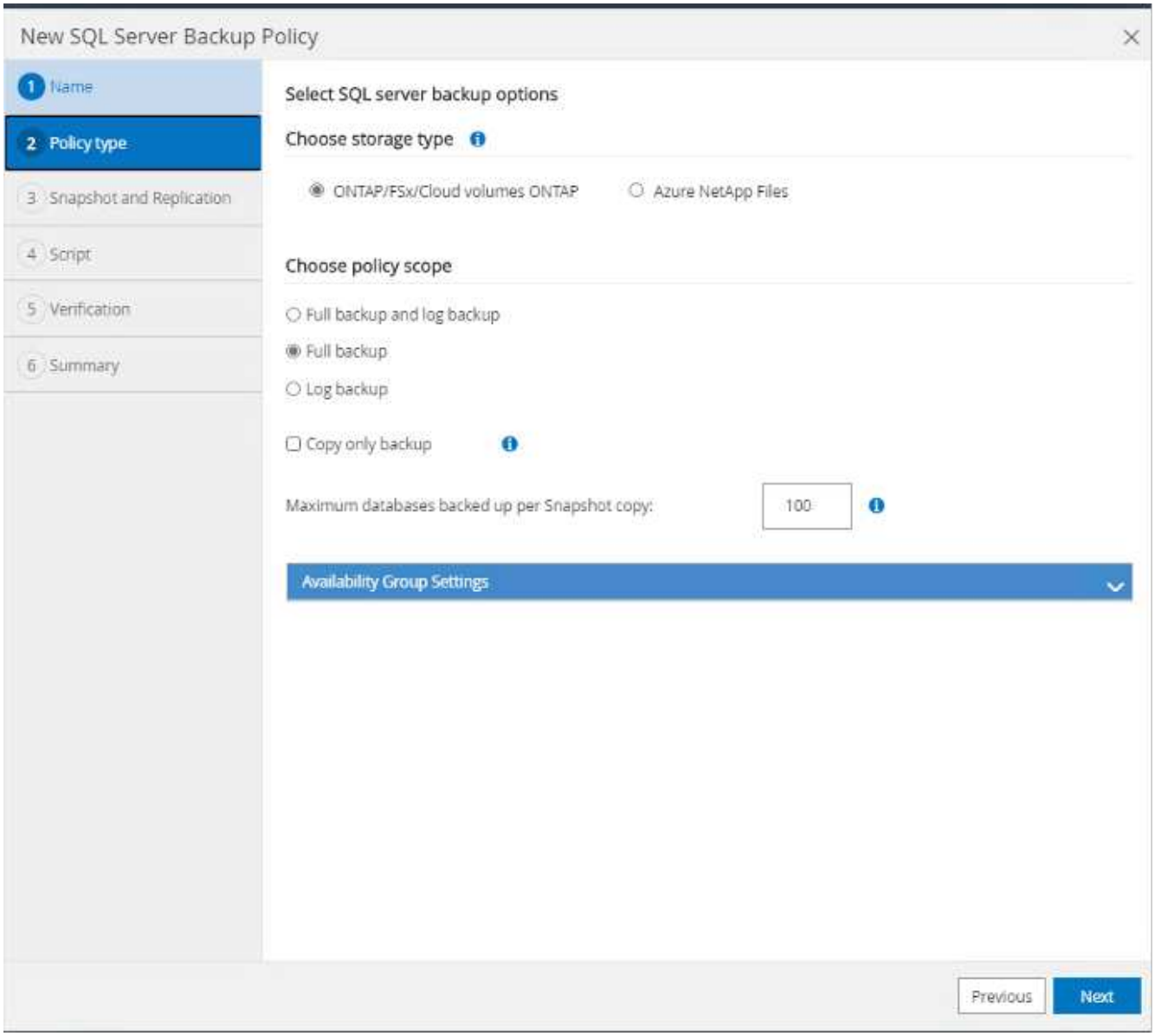
> As validações são realizadas em um banco de dados Microsoft SQL Server em execução na máquina virtual convidada.



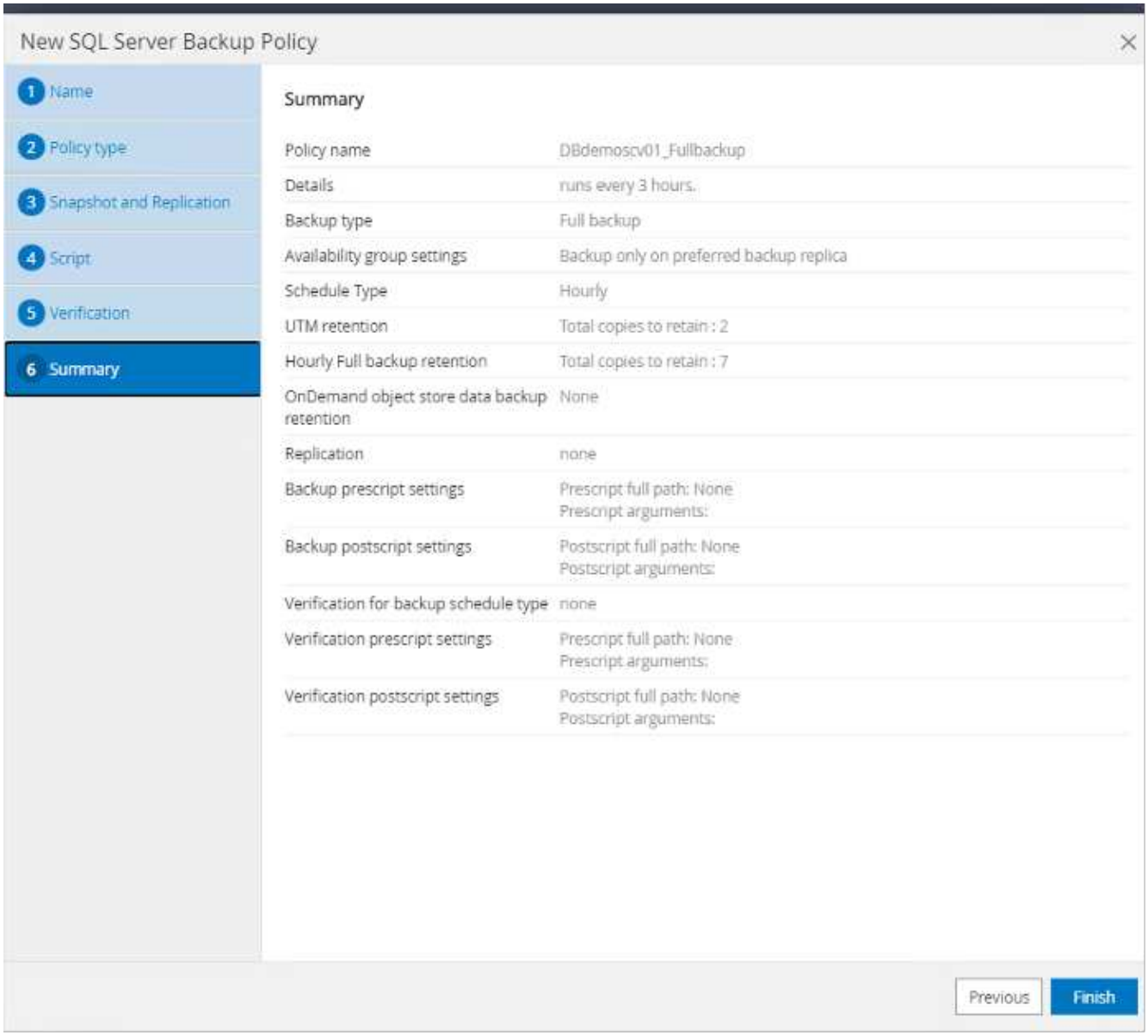
2. Clique no ícone de sinal de mais para configurar uma política de backup do SQL Server.



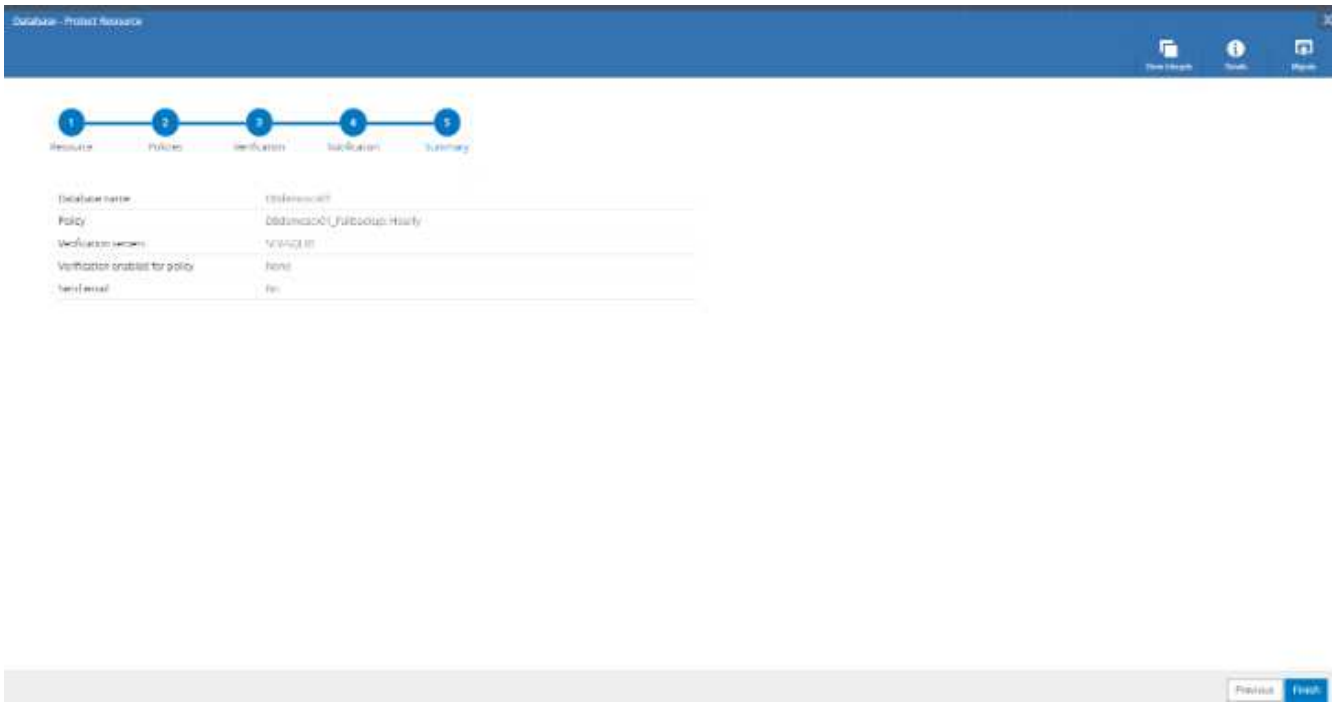
3. Nesta demonstração, "Full backup" está selecionado. Selecione "Next" para continuar.



4. Na página Summary, selecione "Finish".



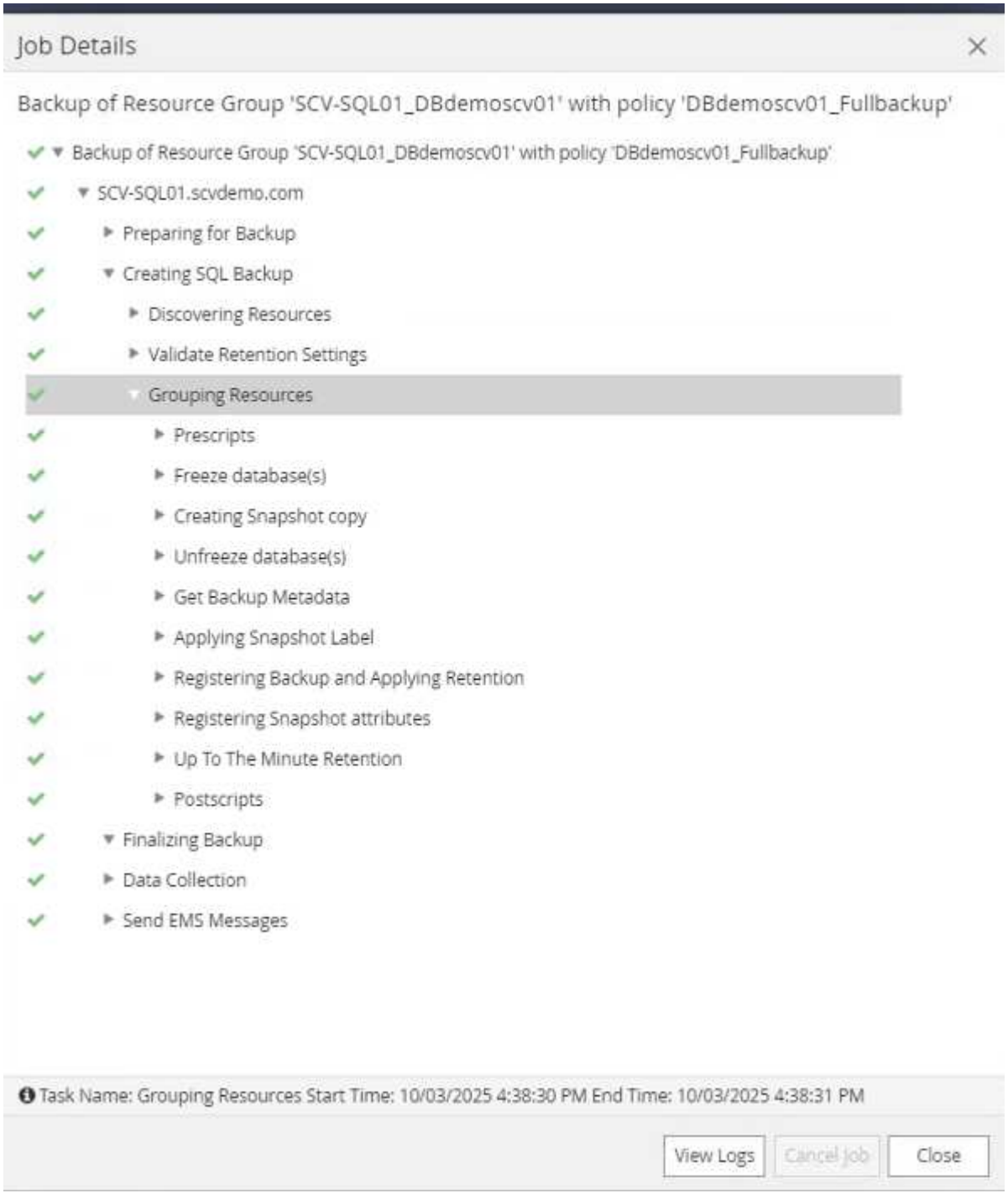
5. Prossiga para "Finish".



Monitorando um backup

Após configurar uma política de backup, você pode monitorar suas operações de backup à medida que ocorrem. Você pode fazer isso clicando em Backup now para acionar uma operação de backup sob demanda ou aguardando a sua política de backup agendada entrar em vigor.

1. Monitore o progresso do trabalho usando **Monitor › Jobs**.
2. Selecione a tarefa de backup e clique em "Detalhes" para visualizar as informações da tarefa, conforme mostrado abaixo.

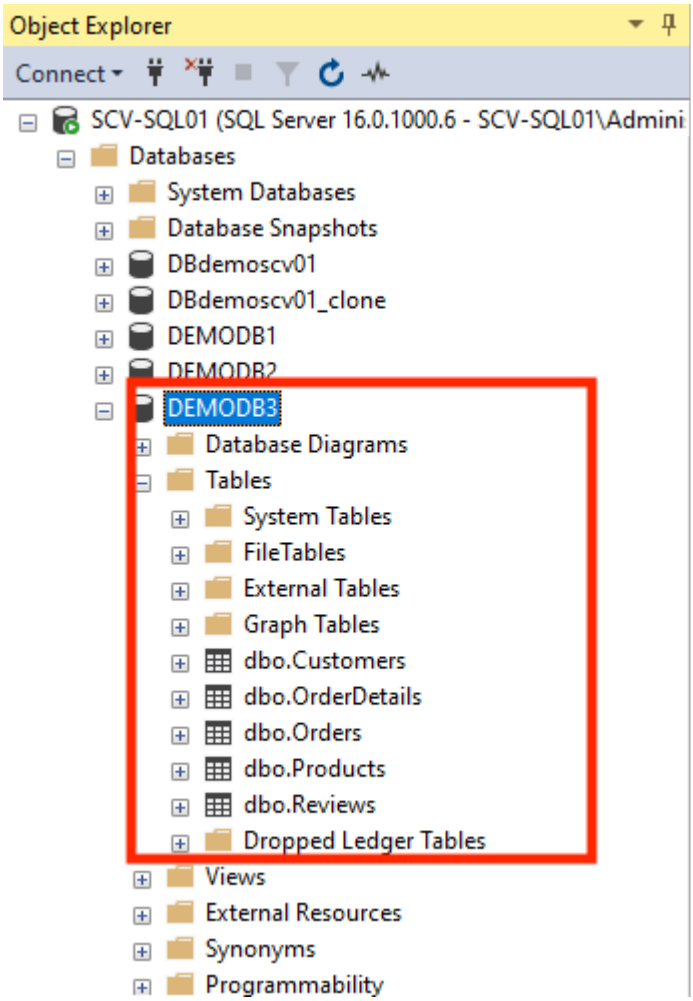


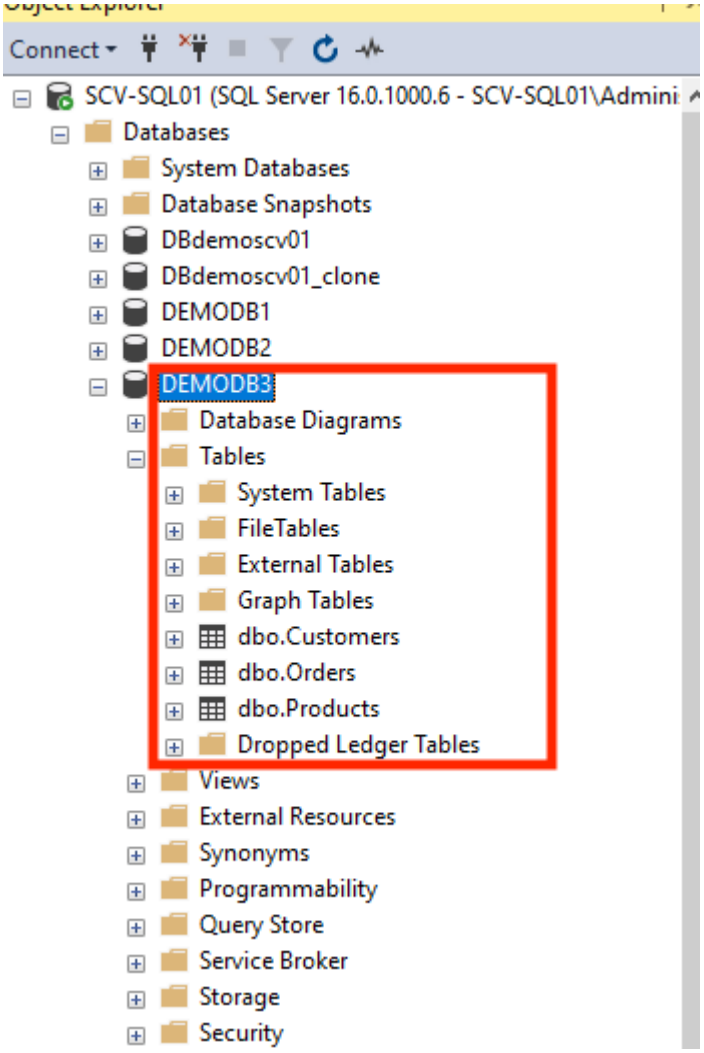
Restauração de bancos de dados residentes nos VMDKs

O banco de dados no VMDK pode ser restaurado para um ponto específico no tempo.

Podemos simular a importância disso excluindo algumas tabelas do seu banco de dados, que serão então corrigidas ao realizar uma restauração pontual.

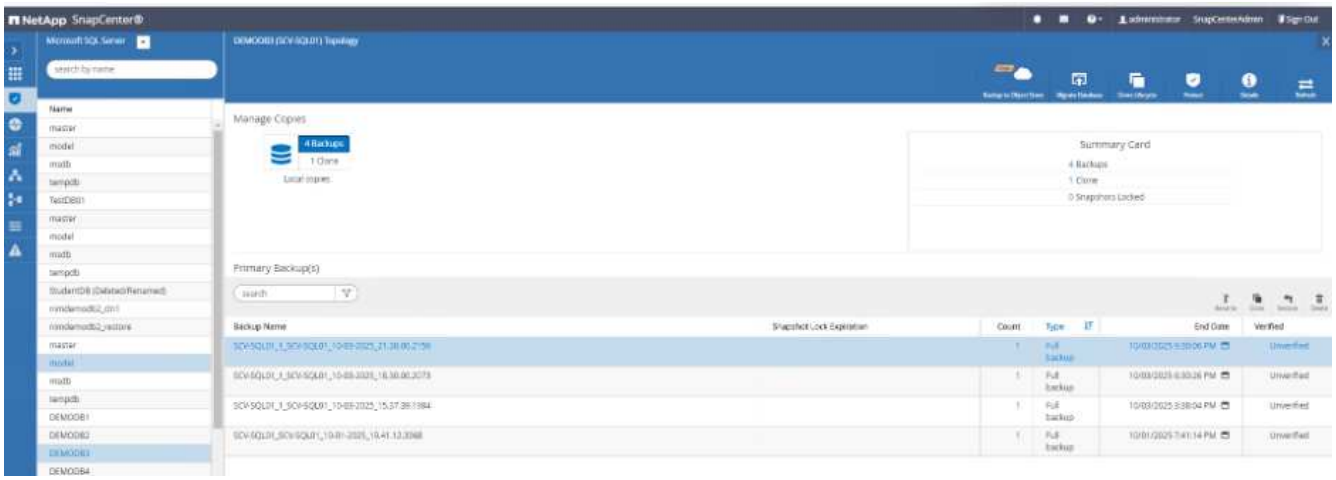
Abaixo, você pode ver que várias tabelas do nosso banco de dados mostradas na primeira captura de tela foram excluídas na segunda captura de tela:


Object Explorer
Connect
SCV-SQL01 (SQL Server 16.0.1000.6 - SCV-SQL01\Admini
Databases
System Databases
Database Snapshots
DBdemoscv01
DBdemoscv01_clone
DEMODB1
DEMODB2
DEMODB3
Database Diagrams
Tables
System Tables
FileTables
External Tables
Graph Tables
dbo.Customers
dbo.OrderDetails
dbo.Orders
dbo.Products
dbo.Reviews
Dropped Ledger Tables
Views
External Resources
Synonyms
Programmability

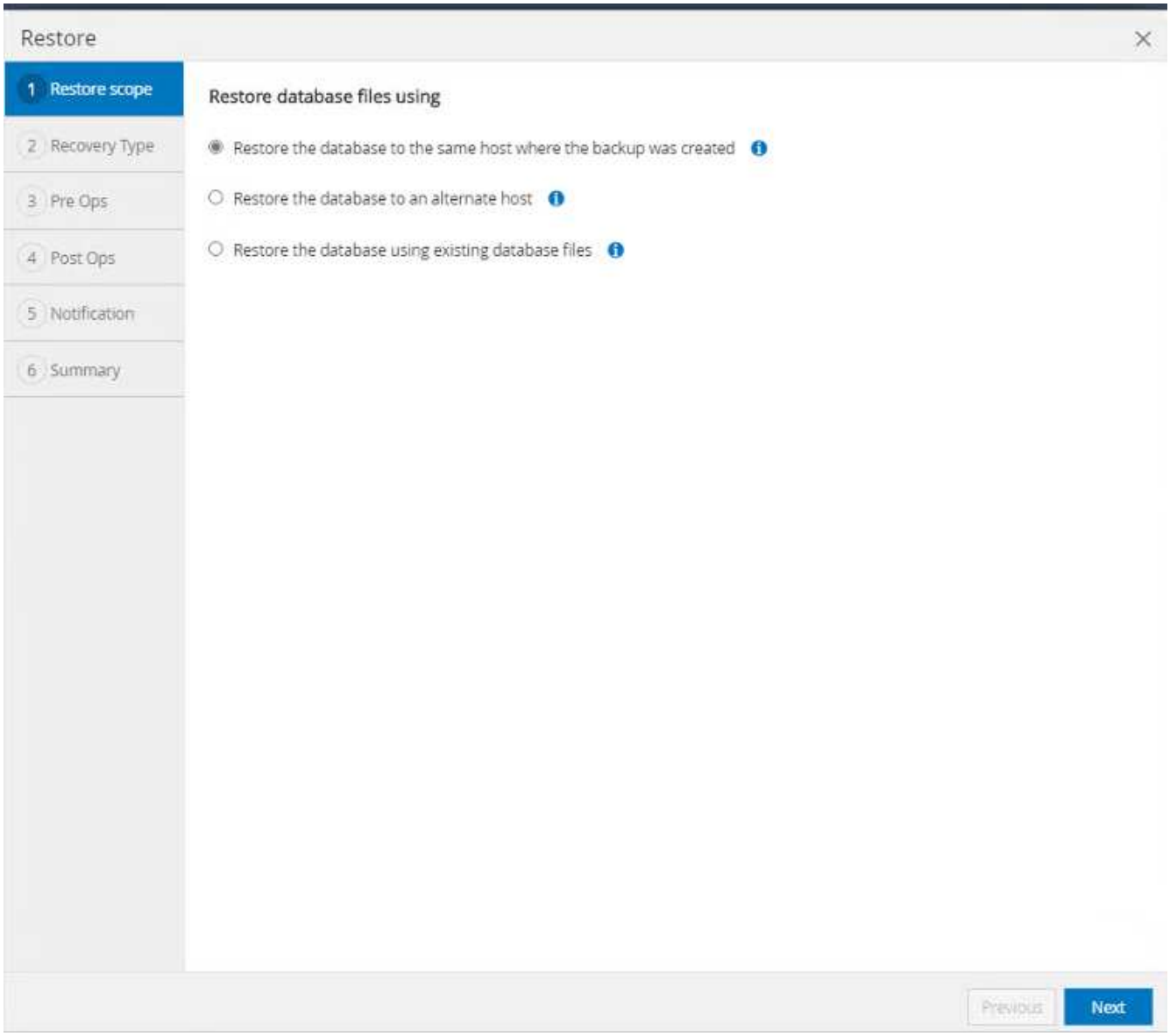


As etapas a seguir mostram como realizar uma restauração para recuperar essas tabelas excluídas:

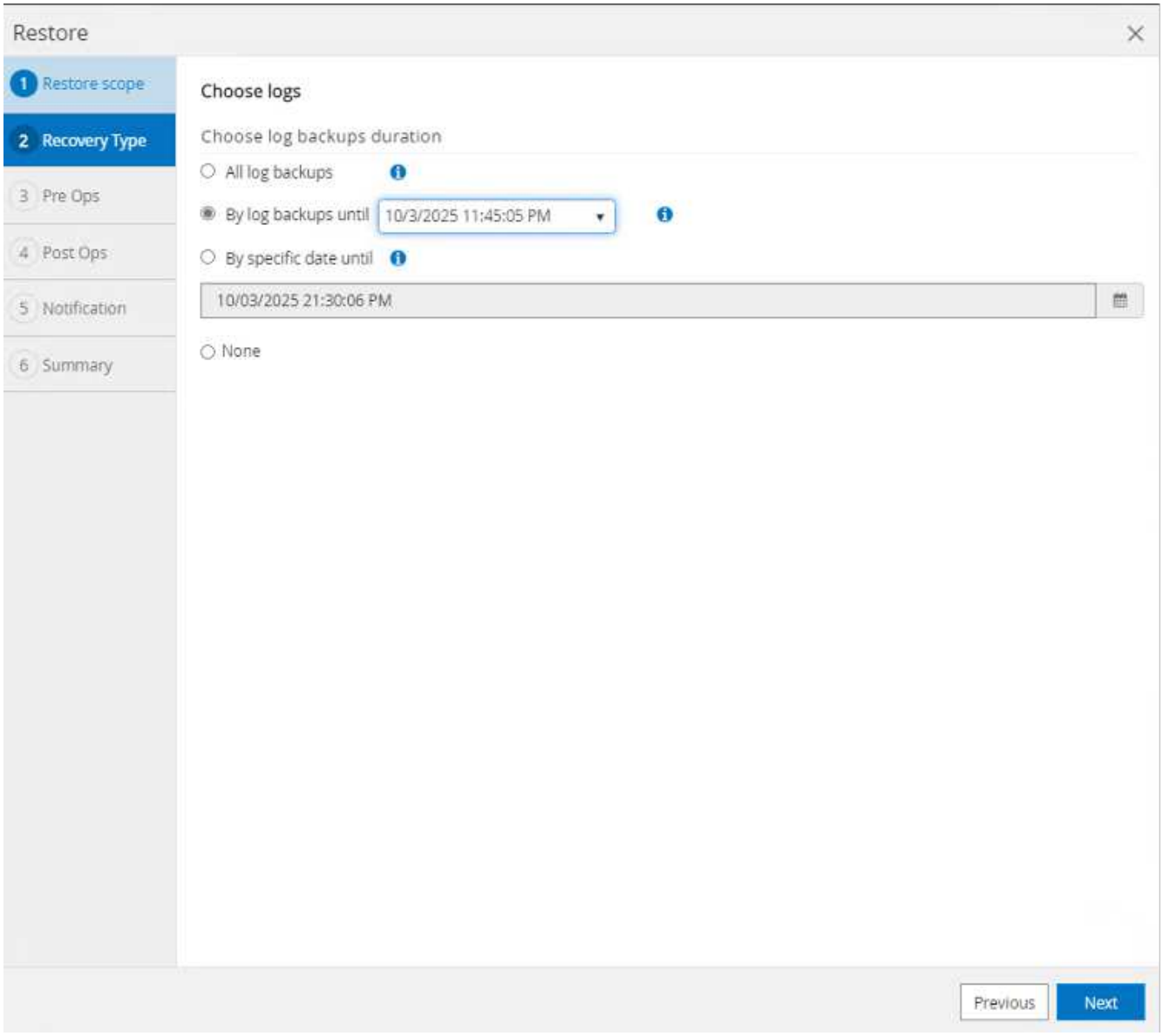
1. Selecione o banco de dados do grupo de recursos.



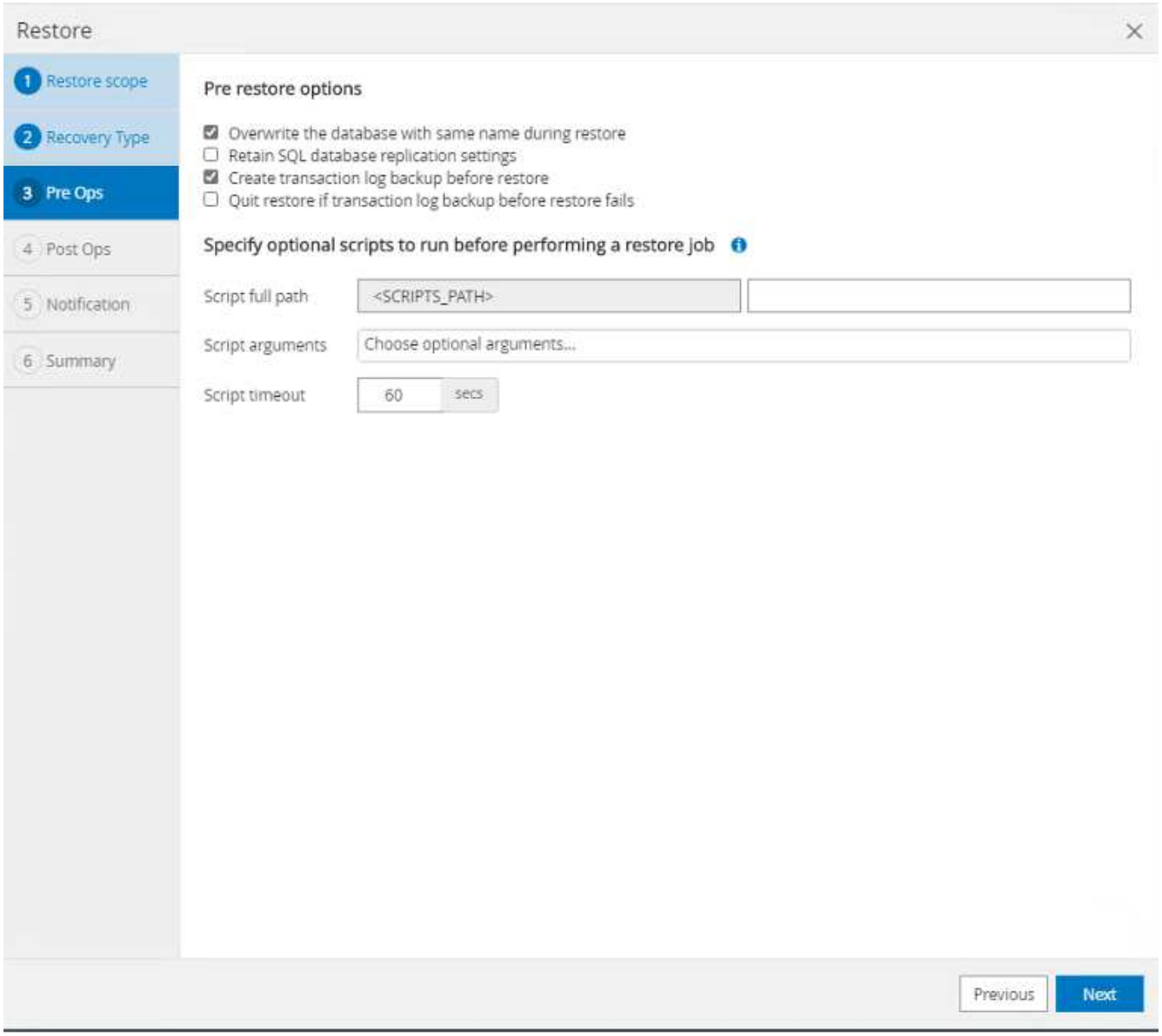
2. Na página Restore, selecione a opção "Restore the database to the same host where the backup was created".



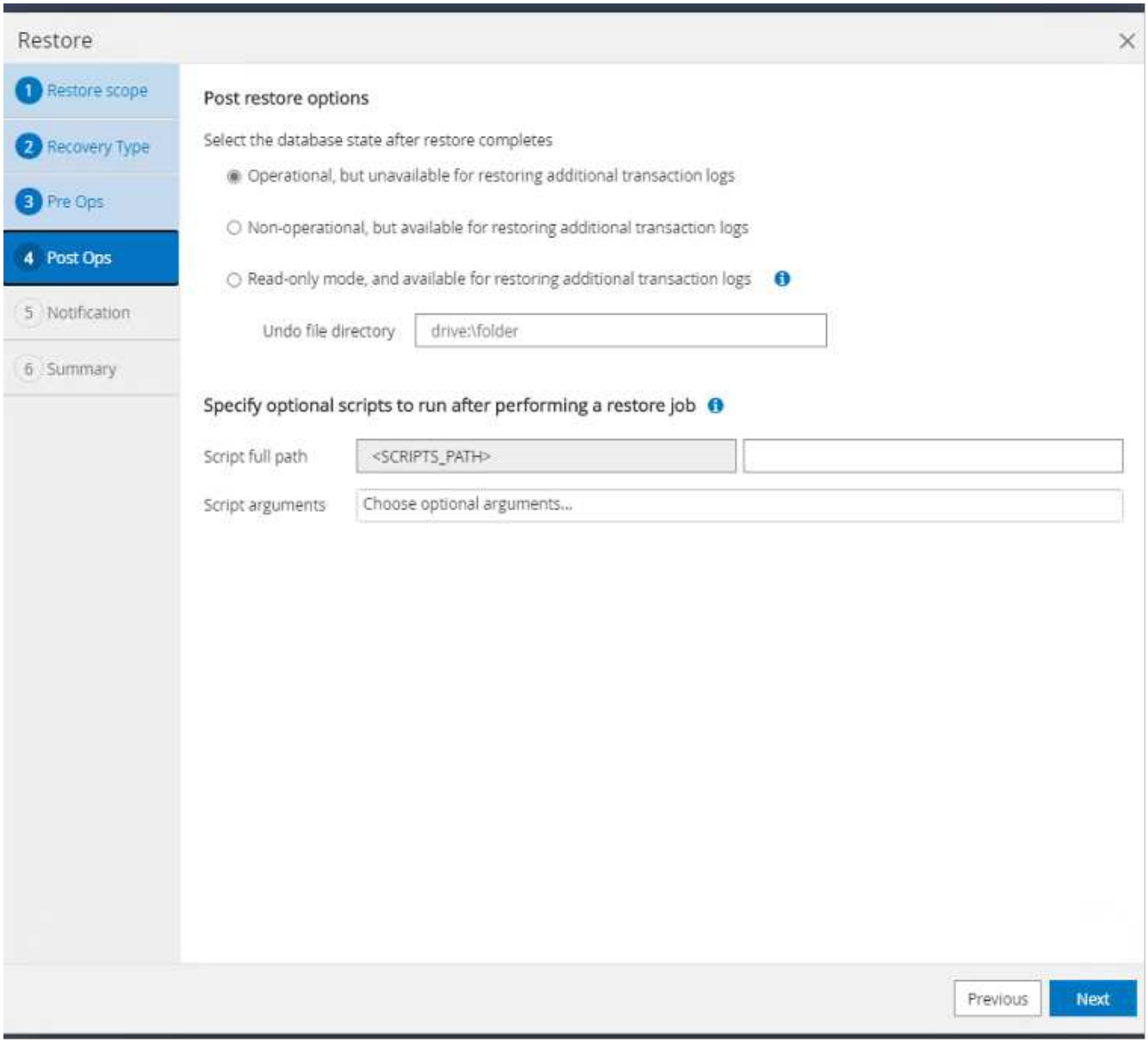
3. Selecione a opção para usar um backup de log para um ponto específico no tempo.



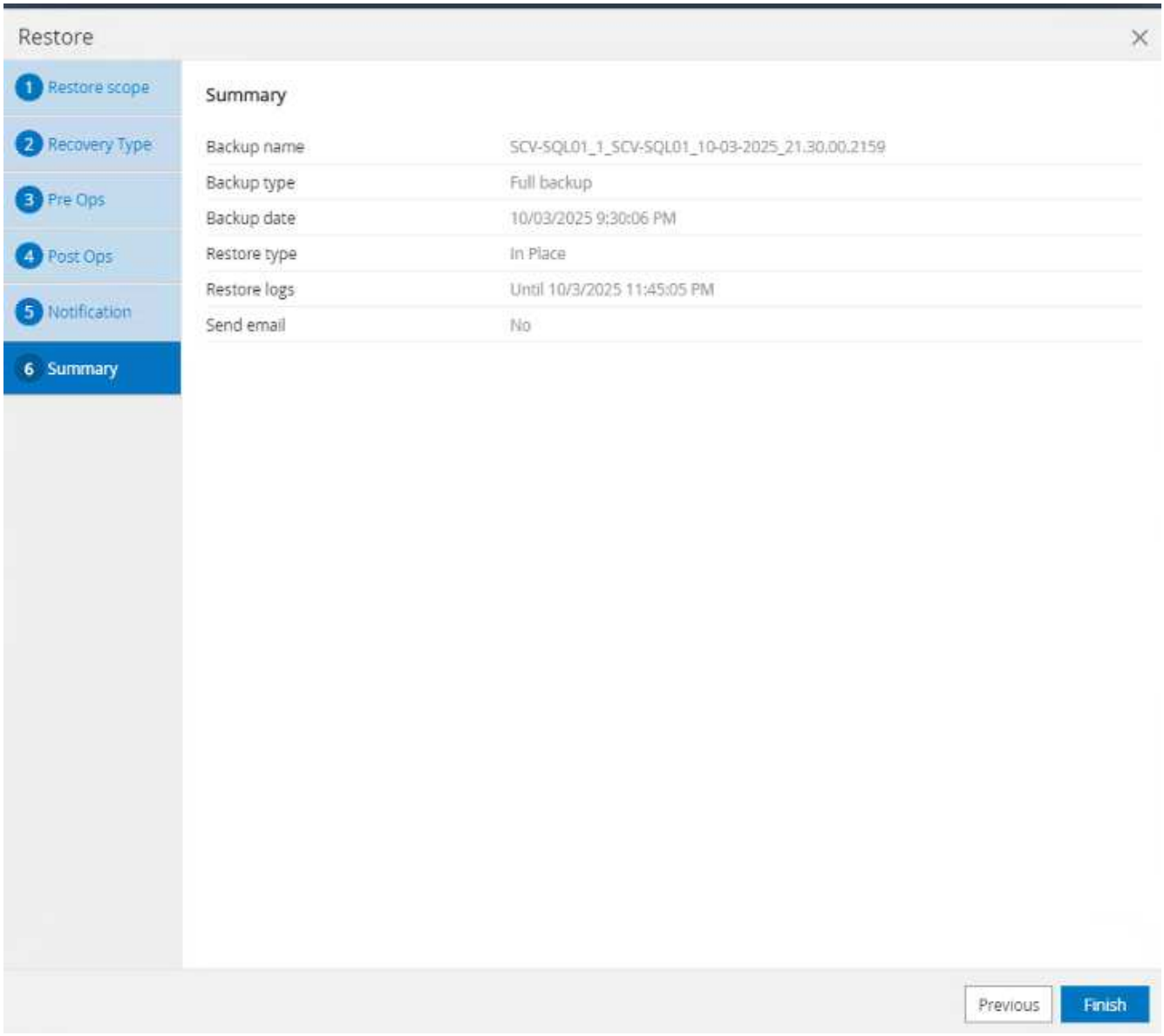
4. Selecione "Sobrescrever banco de dados com o mesmo nome durante a restauração, criar backup do log de transações antes da restauração" e selecione "Avançar".



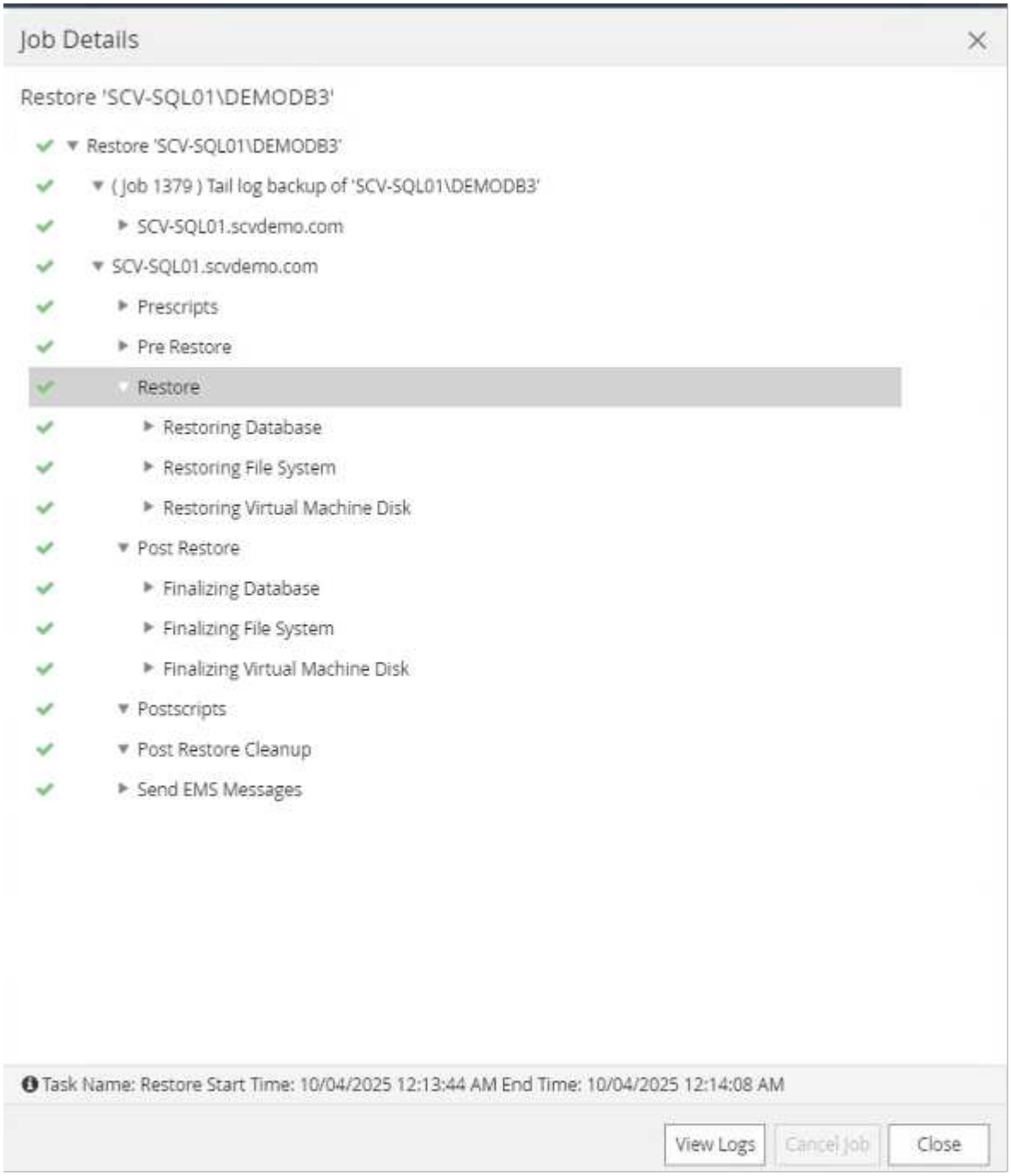
5. Selecione o estado pós-restauração que deseja que o banco de dados assuma nas opções da lista e selecione "Next".



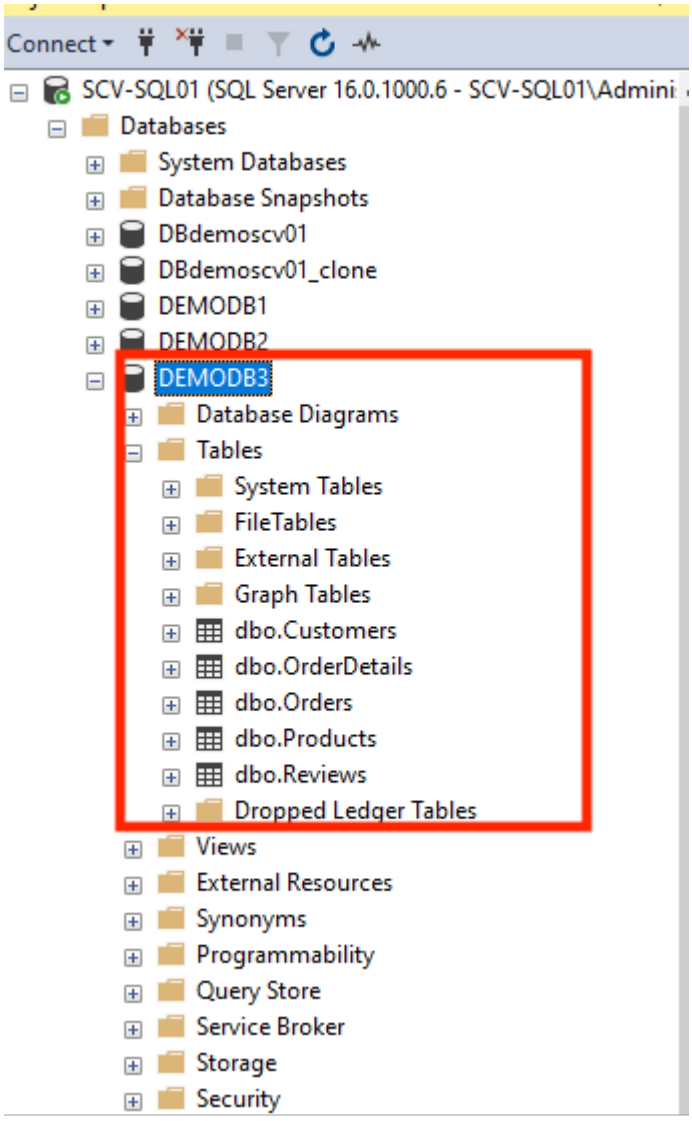
6. Na página de resumo, selecione "Finish".



7. Monitore o trabalho até a conclusão.



8. Verifique se as tabelas excluídas foram restauradas com sucesso.



Conclusão

Neste documento, fornecemos orientações detalhadas passo a passo sobre como implantar, configurar e usar o SCV e "SnapCenter Plug-in para SQL Server (SCSQL)" ao utilizar o FSx for ONTAP como datastore suplementar com clusters Amazon EVS.

Conclusão

Em resumo, ao usar FSx for ONTAP para otimizar o TCO em uma implantação do Amazon EVS, o SCV oferece um método simples e eficiente para fazer backup de máquinas virtuais. Ele pode fazer backup e restaurar máquinas virtuais de maneira rápida e integrada, pois depende de cópias Snapshot, que levam literalmente segundos para serem concluídas.

"Experimente o SnapCenter plug-in para VMware agora gratuitamente".

NetApp para Azure / AVS

Recursos da NetApp para Azure AVS

Saiba mais sobre os recursos que a NetApp traz para o Azure VMware Solution (AVS) - desde o NetApp como um dispositivo de armazenamento conectado a convidados ou um armazenamento de dados NFS suplementar até a migração de fluxos de trabalho, extensão/intermitência para a nuvem, backup/restauração e recuperação de desastres.

Vá para a seção do conteúdo desejado selecionando entre as seguintes opções:

- "Configurando o AVS no Azure"
- "Opções de armazenamento NetApp para AVS"
- "Soluções de nuvem NetApp /VMware"

Configurando o AVS no Azure

Assim como no local, planejar um ambiente de virtualização baseado em nuvem é essencial para um ambiente de produção bem-sucedido, pronto para criação de VMs e migração.

Esta seção descreve como configurar e gerenciar o Azure VMware Solution e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP ao Azure VMware Solution.

O processo de configuração pode ser dividido nas seguintes etapas:

- Registre o provedor de recursos e crie uma nuvem privada
- Conectar-se a um gateway de rede virtual ExpressRoute novo ou existente
- Valide a conectividade de rede e acesse a nuvem privada

Veja o detalhado"etapas de configuração para AVS" .

Opções de armazenamento NetApp para AVS

O armazenamento NetApp pode ser utilizado de diversas maneiras — como um repositório de dados NFS conectado ou suplementar — dentro do Azure AVS.

Por favor visite"Opções de armazenamento NetApp suportadas" para maiores informações.

O Azure oferece suporte ao armazenamento NetApp nas seguintes configurações:

- Azure NetApp Files (ANF) como armazenamento conectado a convidados
- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- Azure NetApp Files (ANF) como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para AVS" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para AVS" .

Casos de uso da solução

Com as soluções de nuvem da NetApp e da VMware, muitos casos de uso são simples de implantar no Azure AVS. Esses casos são definidos para cada uma das áreas de nuvem definidas pela VMware:

- Proteger (inclui recuperação de desastres e backup/restauração)
- Estender
- Migrar

"Navegue pelas soluções da NetApp para o Azure AVS"

Proteja cargas de trabalho no Azure / AVS

Recuperação de desastres com ANF e JetStream

A recuperação de desastres na nuvem é uma maneira resiliente e econômica de proteger as cargas de trabalho contra interrupções do site e eventos de corrupção de dados (por exemplo, ransomware). Usando a estrutura VMware VAIO, as cargas de trabalho locais do VMware podem ser replicadas para o armazenamento de Blobs do Azure e recuperadas, permitindo perda de dados mínima ou quase nenhuma e RTO próximo de zero.

O JetStream DR pode ser usado para recuperar perfeitamente as cargas de trabalho replicadas do local para o AVS e, especificamente, para o Azure NetApp Files. Ele permite uma recuperação de desastres econômica usando recursos mínimos no local de DR e armazenamento em nuvem econômico. O JetStream DR automatiza a recuperação para armazenamentos de dados ANF por meio do Azure Blob Storage. O JetStream DR recupera VMs independentes ou grupos de VMs relacionadas na infraestrutura do site de recuperação de acordo com o mapeamento de rede e fornece recuperação pontual para proteção contra ransomware.

Este documento fornece uma compreensão dos princípios de operações do JetStream DR e seus principais componentes.

▼ Visão geral da implantação da solução

1. Instale o software JetStream DR no data center local.
    a. Baixe o pacote de software JetStream DR do Azure Marketplace (ZIP) e implante o JetStream DR MSA (OVA) no cluster designado.
    b. Configure o cluster com o pacote de filtro de E/S (instale o JetStream VIB).
    c. Provisione o Blob do Azure (Conta de Armazenamento do Azure) na mesma região que o cluster DR AVS.
    d. Implante dispositivos DRVA e atribua volumes de log de replicação (VMDK de armazenamento de dados existente ou armazenamento iSCSI compartilhado).
    e. Crie domínios protegidos (grupos de VMs relacionadas) e atribua DRVAs e Azure Blob Storage/ANF.
    f. Inicie a proteção.
2. Instale o software JetStream DR na nuvem privada do Azure VMware Solution.
    a. Use o comando Executar para instalar e configurar o JetStream DR.
    b. Adicione o mesmo contêiner de Blobs do Azure e descubra domínios usando a opção Verificar

Domínios.

c. Implante os dispositivos DRVA necessários.

d. Crie volumes de log de replicação usando armazenamentos de dados vSAN ou ANF disponíveis.

e. Importe domínios protegidos e configure o RocVA (VA de recuperação) para usar o armazenamento de dados ANF para posicionamentos de VM.

f. Selecione a opção de failover apropriada e inicie a reidratação contínua para domínios ou VMs com RTO próximo de zero.

3. Durante um evento de desastre, acione o failover para os repositórios de dados do Azure NetApp Files no site de DR do AVS designado.
4. Invoque o failback para o site protegido após a recuperação do site protegido. Antes de começar, certifique-se de que os pré-requisitos sejam atendidos conforme indicado neste "link" e também executar a Ferramenta de Teste de Largura de Banda (BWT) fornecida pela JetStream Software para avaliar o desempenho potencial do armazenamento de Blobs do Azure e sua largura de banda de replicação quando usada com o software JetStream DR. Depois que os pré-requisitos, incluindo conectividade, estiverem prontos, configure e assine o JetStream DR para AVS a partir do "Mercado do Azure" . Após o download do pacote de software, prossiga com o processo de instalação descrito acima.

Ao planejar e iniciar a proteção para um grande número de VMs (por exemplo, mais de 100), use a Ferramenta de Planejamento de Capacidade (CPT) do JetStream DR Automation Toolkit. Forneça uma lista de VMs a serem protegidas, juntamente com suas preferências de RTO e grupo de recuperação, e então execute o CPT.

O CPT desempenha as seguintes funções:

- Combinando VMs em domínios de proteção de acordo com seu RTO.
- Definir o número ideal de DRVAs e seus recursos.
- Estimando a largura de banda de replicação necessária.
- Identificar características do volume do log de replicação (capacidade, largura de banda e assim por diante).
- Estimativa da capacidade de armazenamento de objetos necessária e muito mais.

> O número e o conteúdo dos domínios prescritos dependem de várias características da VM, como IOPS médio, capacidade total, prioridade (que define a ordem de failover), RTO e outros.

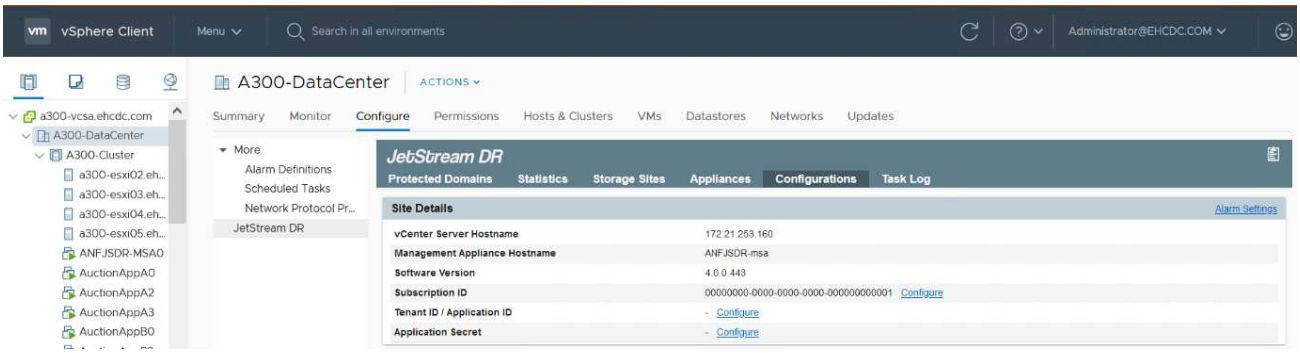
Instalar o JetStream DR no datacenter local

O software JetStream DR consiste em três componentes principais: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) e componentes de host (pacotes de filtro de E/S). O MSA é usado para instalar e configurar componentes do host no cluster de computação e, em seguida, para administrar o software JetStream DR. A lista a seguir fornece uma descrição de alto nível do processo de instalação:

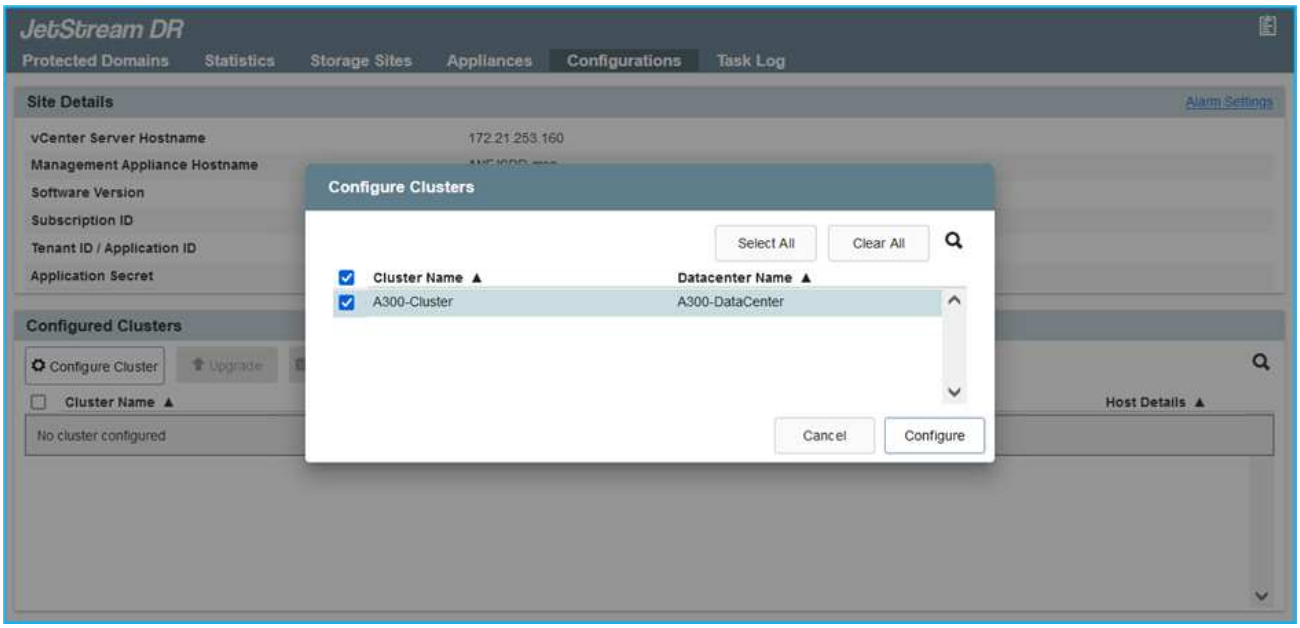
▼ Como instalar o JetStream DR no local

1. Verifique os pré-requisitos.
2. Execute a Ferramenta de Planejamento de Capacidade para obter recomendações de recursos e configuração (opcional, mas recomendado para testes de prova de conceito).
3. Implante o MSA do JetStream DR em um host vSphere no cluster designado.

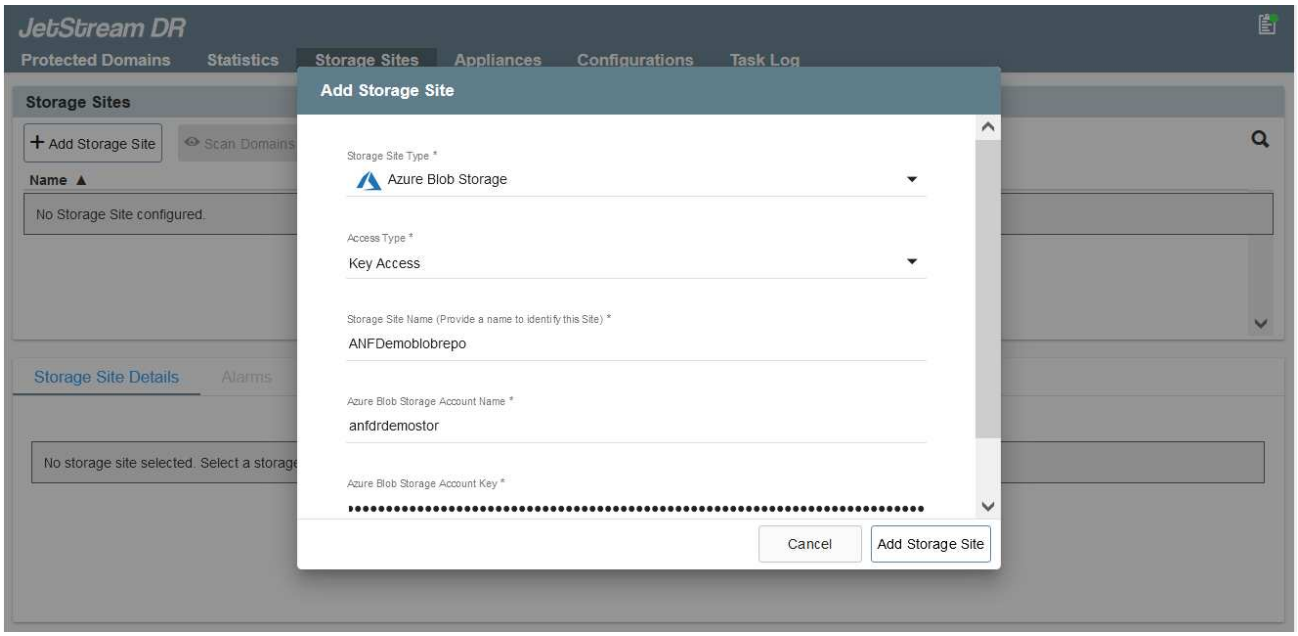
4. Inicie o MSA usando seu nome DNS em um navegador.
5. Registre o servidor vCenter com o MSA. Para executar a instalação, conclua as seguintes etapas detalhadas:
6. Depois que o JetStream DR MSA for implantado e o vCenter Server for registrado, acesse o plug-in JetStream DR usando o vSphere Web Client. Isso pode ser feito navegando até Datacenter > Configurar > JetStream DR.



7. Na interface do JetStream DR, selecione o cluster apropriado.



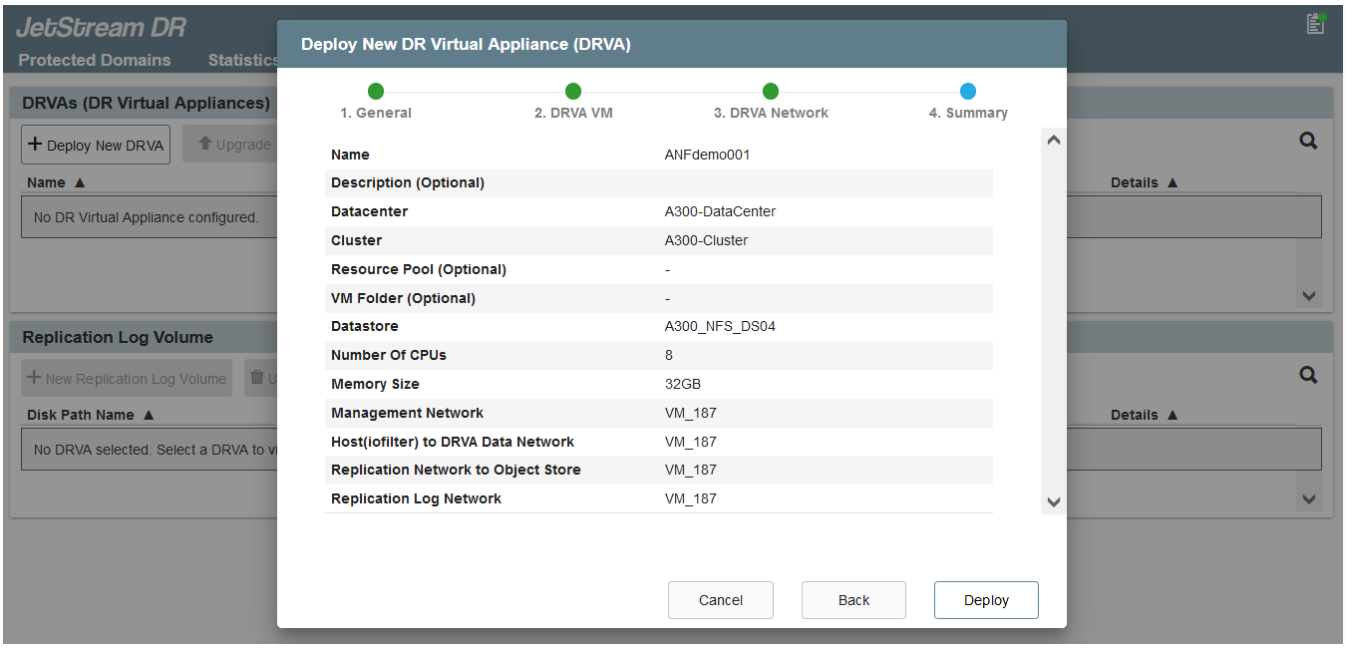
8. Configure o cluster com o pacote de filtro de E/S.



9. Adicione o Armazenamento de Blobs do Azure localizado no site de recuperação.
10. Implante um DR Virtual Appliance (DRVA) na guia Appliances.

> Os DRVAs podem ser criados automaticamente pelo CPT, mas para testes de POC, recomendamos configurar e executar o ciclo de DR manualmente (iniciar proteção > failover > failback).

O JetStream DRVA é um dispositivo virtual que facilita funções essenciais no processo de replicação de dados. Um cluster protegido deve conter pelo menos um DRVA e, normalmente, um DRVA é configurado por host. Cada DRVA pode gerenciar vários domínios protegidos.

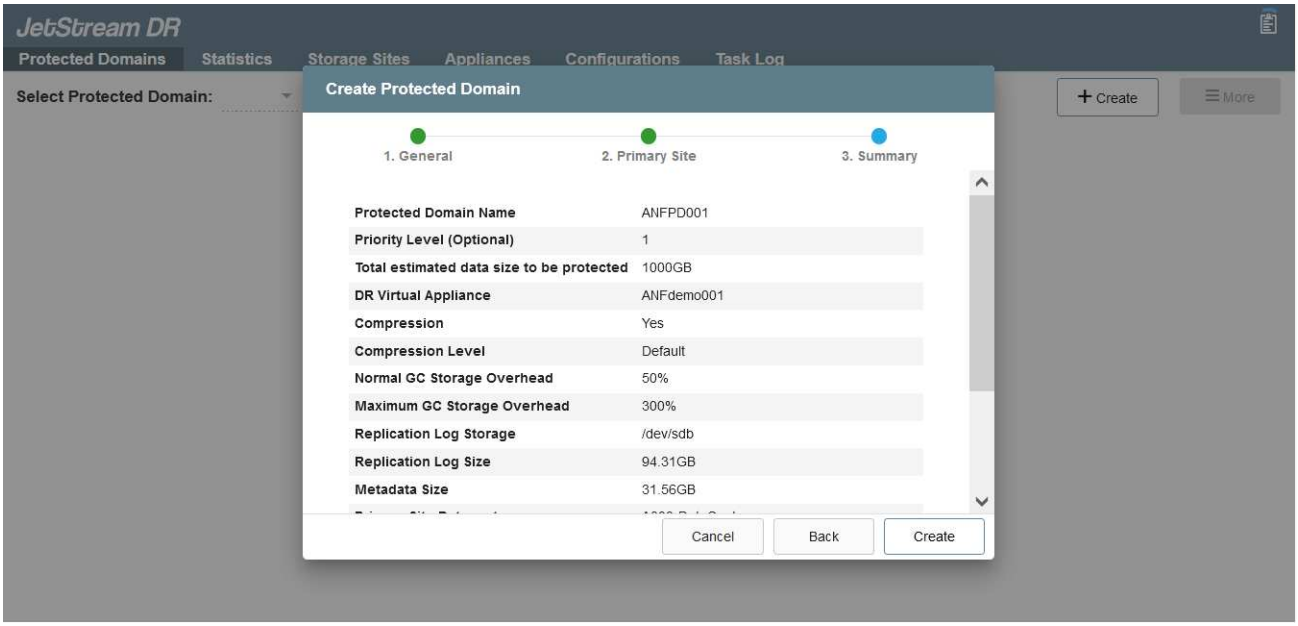


Neste exemplo, quatro DRVAs foram criados para 80 máquinas virtuais.

1. Crie volumes de log de replicação para cada DRVA usando VMDK a partir dos armazenamentos de

dados disponíveis ou de pools de armazenamento iSCSI compartilhados independentes.

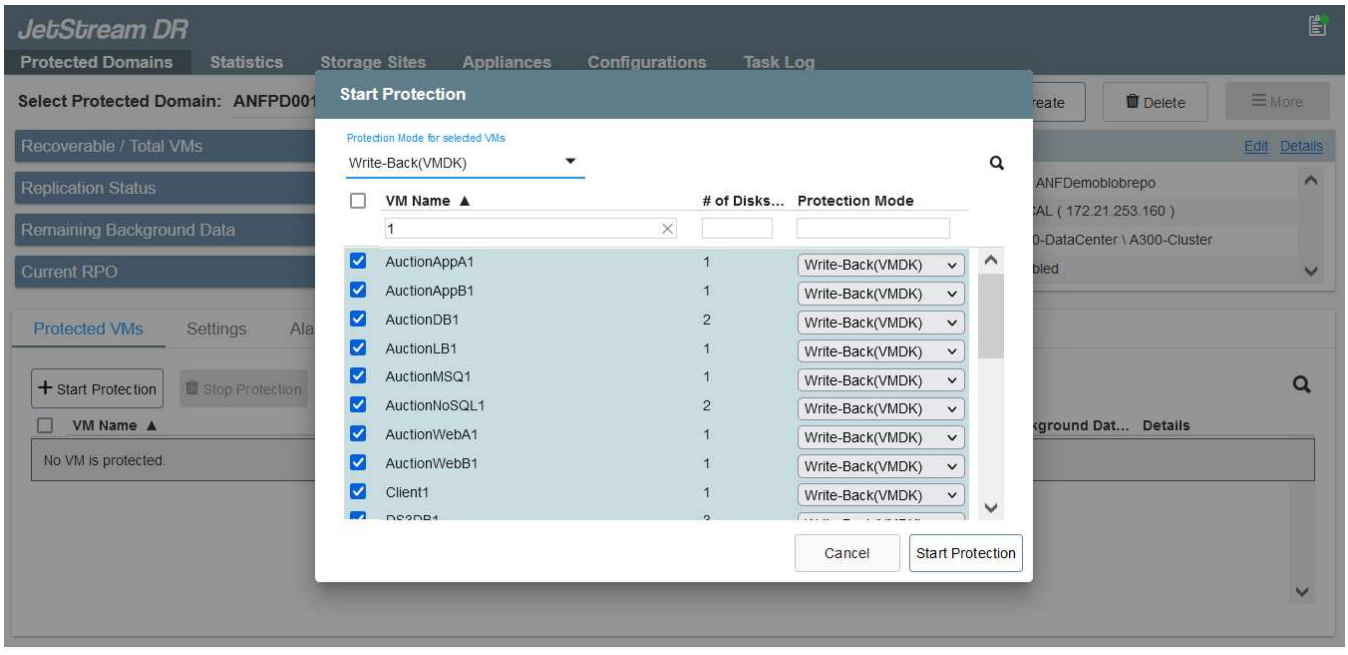
2. Na guia Domínios Protegidos, crie o número necessário de domínios protegidos usando informações sobre o site do Armazenamento de Blobs do Azure, a instância do DRVA e o log de replicação. Um domínio protegido define uma VM específica ou um conjunto de VMs dentro do cluster que são protegidas em conjunto e recebem uma ordem de prioridade para operações de failover/failback.



3. Selecione as VMs que você deseja proteger e inicie a proteção da VM do domínio protegido. Isso inicia a replicação de dados para o Blob Store designado.

Verifique se o mesmo modo de proteção é usado para todas as VMs em um domínio protegido.

O modo Write-Back (VMDK) pode oferecer maior desempenho.



Verifique se os volumes de log de replicação são colocados no armazenamento de alto desempenho.

> Os runbooks de failover podem ser configurados para agrupar as VMs (chamado de Grupo de Recuperação), definir a sequência da ordem de inicialização e modificar as configurações de CPU/memória, juntamente com as configurações de IP.

Instalar o JetStream DR para AVS em uma nuvem privada do Azure VMware Solution usando o comando Executar

Uma prática recomendada para um site de recuperação (AVS) é criar um cluster de luz piloto de três nós com antecedência. Isso permite que a infraestrutura do site de recuperação seja pré-configurada, incluindo os seguintes itens:

- Segmentos de rede de destino, firewalls, serviços como DHCP e DNS e assim por diante.
- Instalação do JetStream DR para AVS
- Configuração de volumes ANF como armazenamentos de dados e muito maisO JetStream DR oferece suporte ao modo RTO quase zero para domínios de missão crítica. Para esses domínios, o armazenamento de destino deve ser pré-instalado. ANF é um tipo de armazenamento recomendado neste caso.

> A configuração de rede, incluindo a criação de segmentos, deve ser configurada no cluster AVS para atender aos requisitos locais.

Dependendo dos requisitos de SLA e RTO, o failover contínuo ou o modo de failover regular (padrão) podem ser usados. Para um RTO próximo de zero, a reidratação contínua deve ser iniciada no local de recuperação.

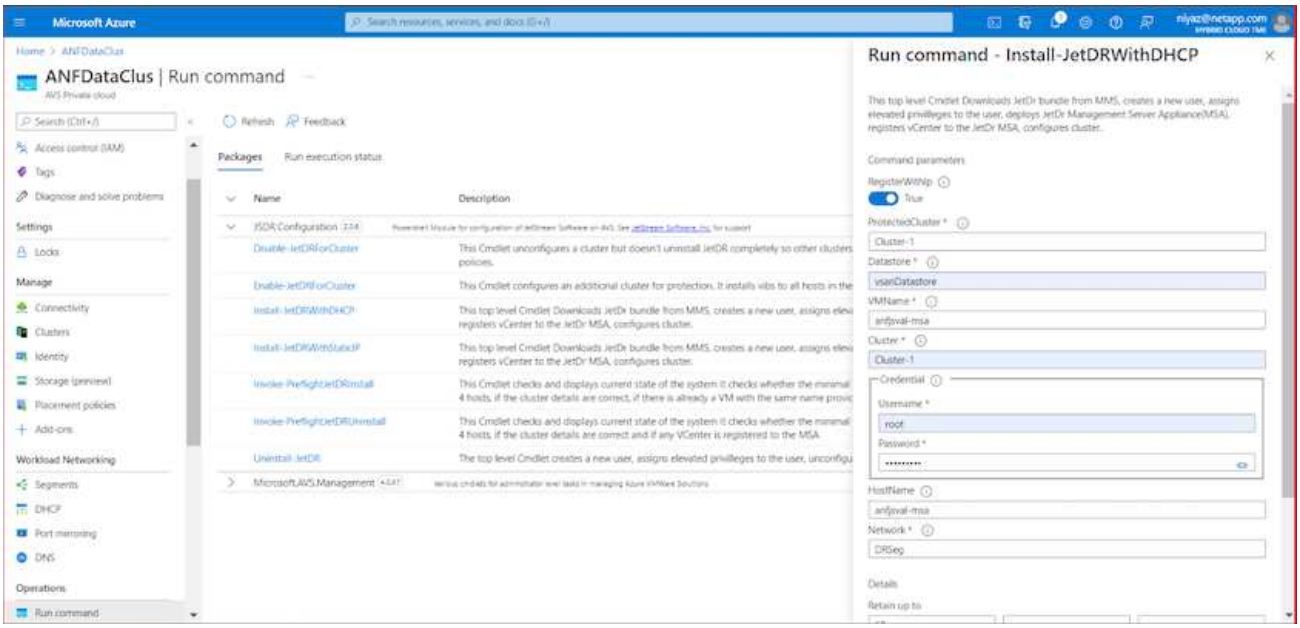
▼ **Como instalar o JetStream DR para AVS em uma nuvem privada**

Para instalar o JetStream DR para AVS em uma nuvem privada do Azure VMware Solution, conclua as seguintes etapas:

1. No portal do Azure, acesse a solução Azure VMware, selecione a nuvem privada e selecione Executar comando > Pacotes > JSDR.Configuration.

> O usuário padrão do CloudAdmin no Azure VMware Solution não tem privilégios suficientes para instalar o JetStream DR para AVS. O Azure VMware Solution permite a instalação simplificada e automatizada do JetStream DR invocando o comando Azure VMware Solution Run para o JetStream DR.

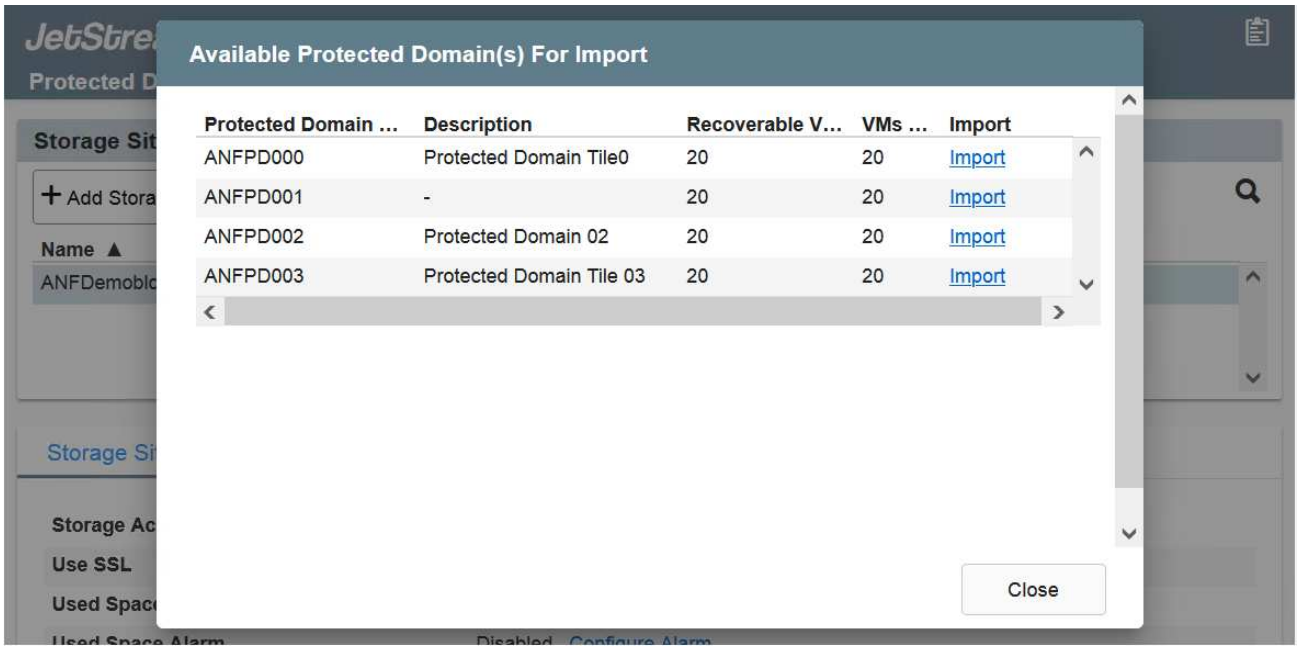
A captura de tela a seguir mostra a instalação usando um endereço IP baseado em DHCP.



2. Após a conclusão da instalação do JetStream DR para AVS, atualize o navegador. Para acessar a interface do usuário do JetStream DR, vá para SDDC Datacenter > Configurar > JetStream DR.



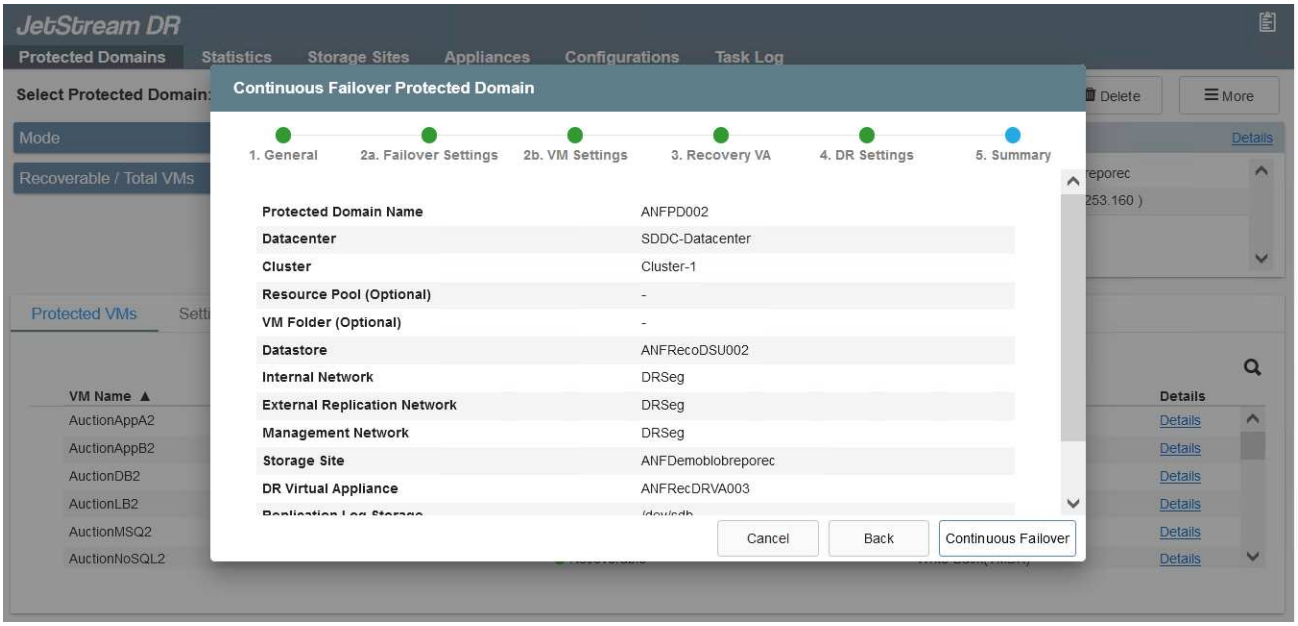
3. Na interface do JetStream DR, adicione a conta do Azure Blob Storage que foi usada para proteger o cluster local como um site de armazenamento e execute a opção Verificar Domínios.



4. Depois que os domínios protegidos forem importados, implante os dispositivos DRVA. Neste exemplo, a reidratação contínua é iniciada manualmente no local de recuperação usando a interface de usuário do JetStream DR.

> Essas etapas também podem ser automatizadas usando planos criados pela CPT.

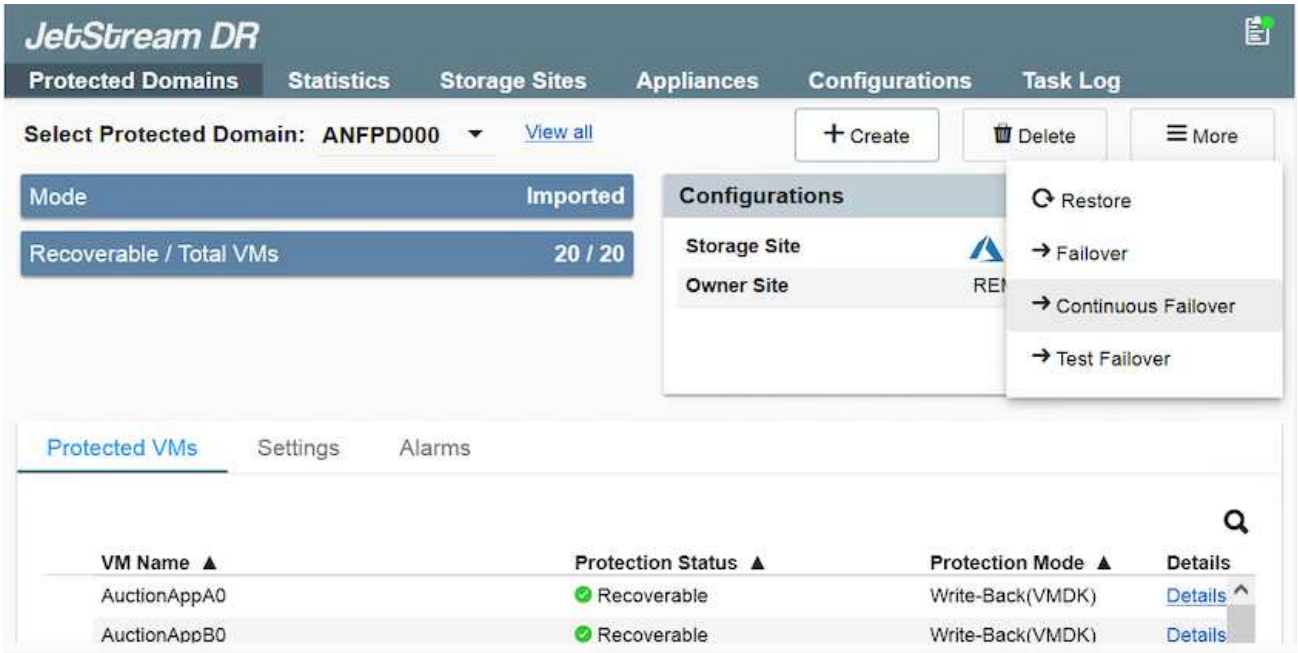
5. Crie volumes de log de replicação usando armazenamentos de dados vSAN ou ANF disponíveis.
6. Importe os domínios protegidos e configure o VA de recuperação para usar o armazenamento de dados ANF para posicionamentos de VM.



> Certifique-se de que o DHCP esteja habilitado no segmento selecionado e que haja IPs suficientes disponíveis. IPs dinâmicos são usados temporariamente enquanto os domínios estão se recuperando. Cada VM em recuperação (incluindo reidratação contínua) requer um IP dinâmico individual. Após a recuperação ser concluída, o IP é

liberado e pode ser reutilizado.

7. Selecione a opção de failover apropriada (failover contínuo ou failover). Neste exemplo, a reidratação contínua (failover contínuo) é selecionada.



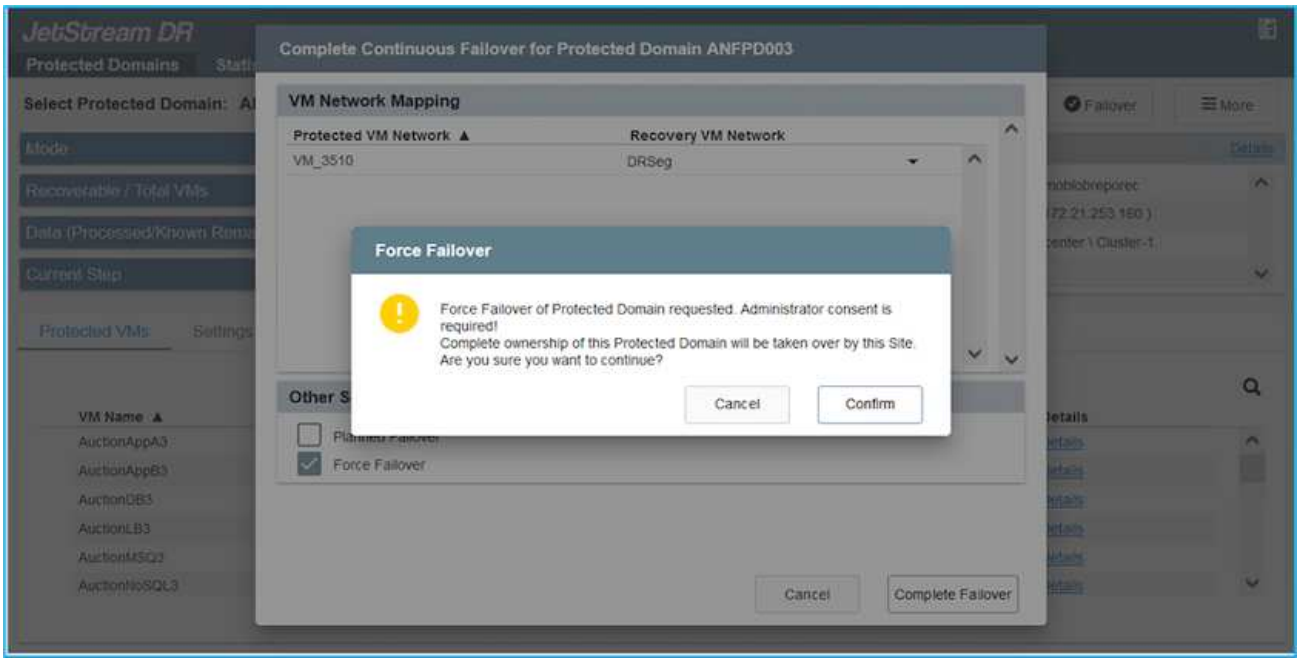
Executando Failover/Failback

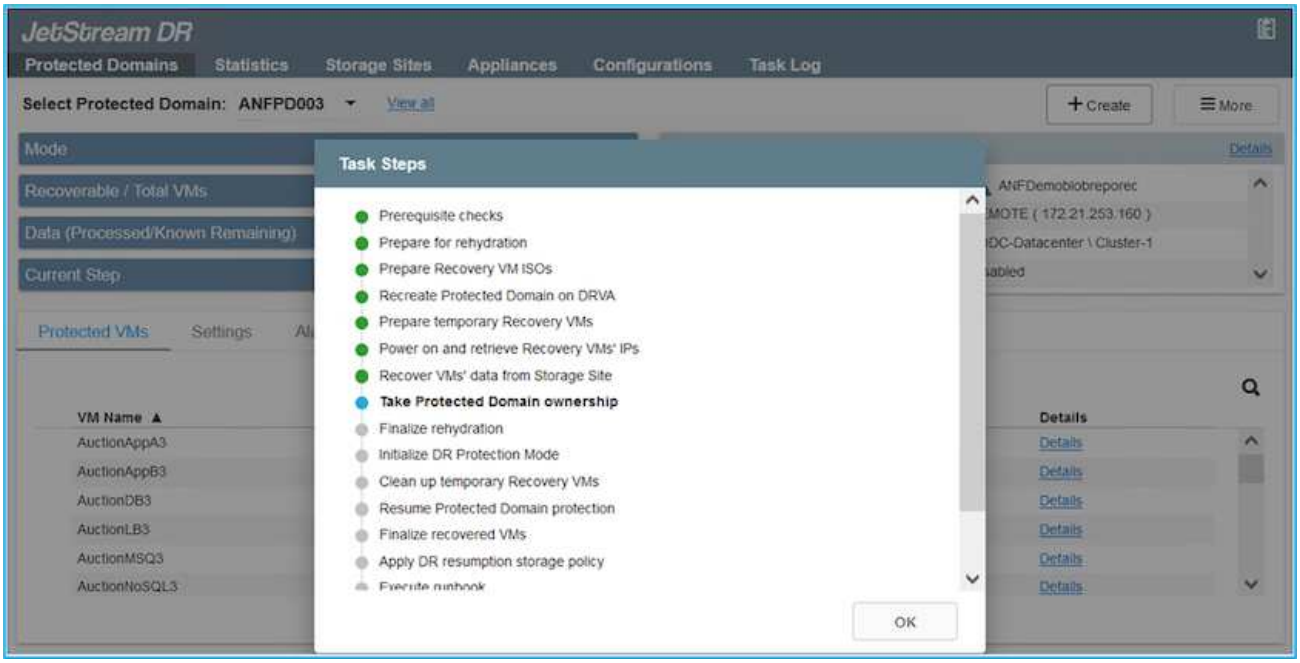
▼ Como executar um Failover / Failback

1. Após ocorrer um desastre no cluster protegido do ambiente local (falha parcial ou total), acione o failover.

O CPT pode ser usado para executar o plano de failover para recuperar as VMs do Armazenamento de Blobs do Azure para o site de recuperação do cluster AVS.

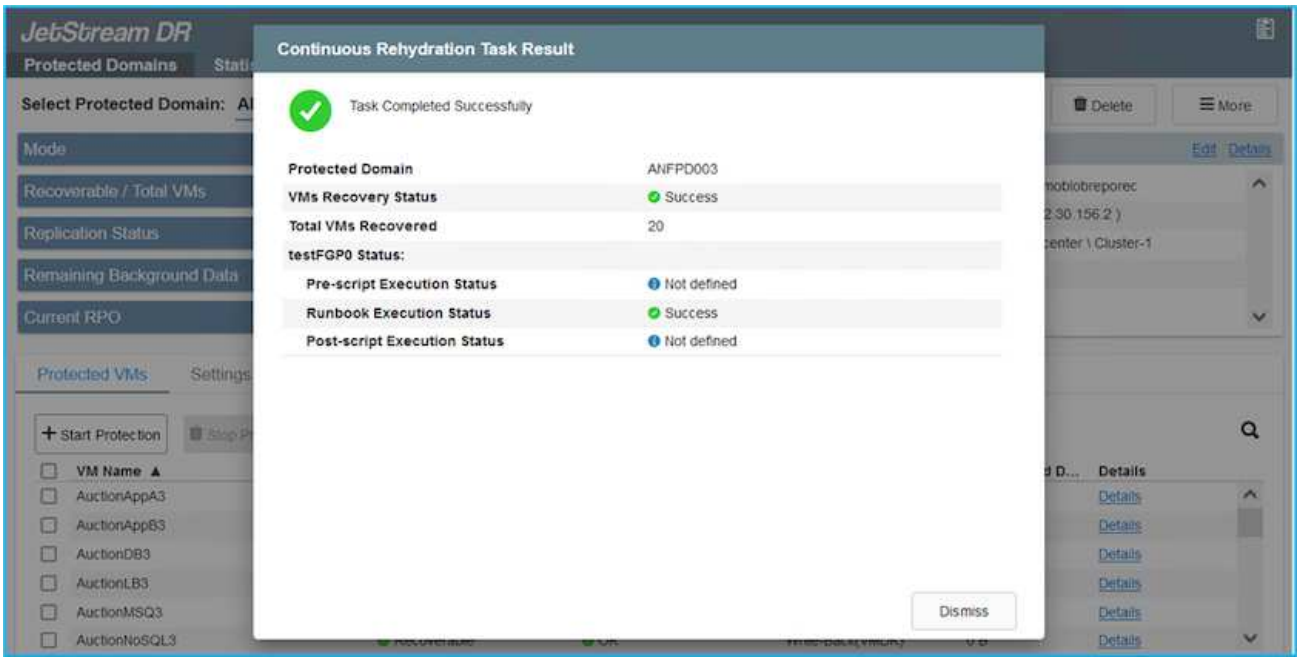
Após o failover (para reidratação contínua ou padrão), quando as VMs protegidas são iniciadas no AVS, a proteção é retomada automaticamente e o JetStream DR continua a replicar seus dados nos contêineres apropriados/originais no Azure Blob Storage.





A barra de tarefas mostra o progresso das atividades de failover.

2. Quando a tarefa estiver concluída, acesse as VMs recuperadas e os negócios continuarão normalmente.

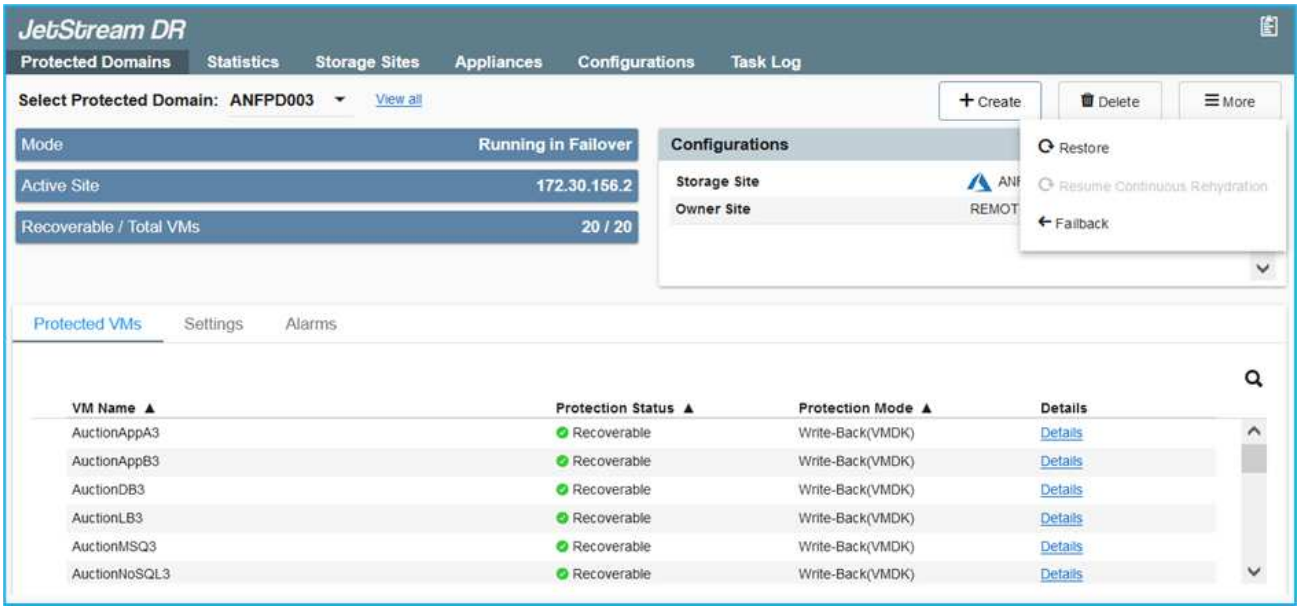


Depois que o site principal estiver funcionando novamente, o failback poderá ser executado. A proteção da VM é retomada e a consistência dos dados deve ser verificada.

3. Restaure o ambiente local. Dependendo do tipo de incidente de desastre, pode ser necessário restaurar e/ou verificar a configuração do cluster protegido. Se necessário, o software JetStream DR pode precisar ser reinstalado.

> Nota: O `recovery_utility_prepare_failback` O script fornecido no Automation Toolkit pode ser usado para ajudar a limpar o site protegido original de quaisquer VMs obsoletas, informações de domínio e assim por diante.

4. Acesse o ambiente local restaurado, vá para a interface do usuário do Jetstream DR e selecione o domínio protegido apropriado. Depois que o site protegido estiver pronto para failback, selecione a opção Failback na interface do usuário.



O plano de failback gerado pelo CPT também pode ser usado para iniciar o retorno das VMs e seus dados do armazenamento de objetos para o ambiente VMware original.

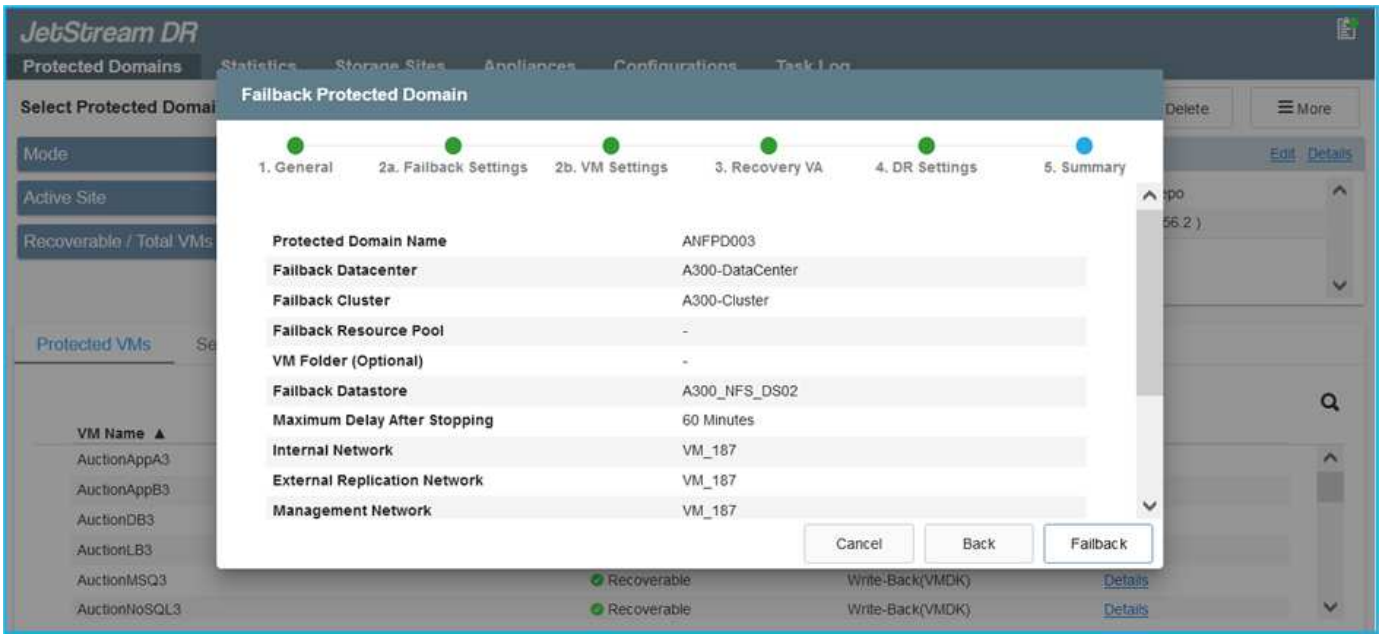
Especifique o atraso máximo após pausar VMs no site de recuperação e reiniciar no site protegido. Esse tempo inclui a conclusão da replicação após interromper as VMs de failover, o tempo para limpar o site de recuperação e o tempo para recriar as VMs no site protegido. O valor recomendado pela NetApp é 10 minutos.

Conclua o processo de failback e confirme a retomada da proteção da VM e da consistência dos dados.

Recuperação de Ransomeware

Recuperar-se de um ransomware pode ser uma tarefa assustadora. Especificamente, pode ser difícil para organizações de TI determinar o ponto de retorno seguro e, uma vez determinado, como garantir que as cargas de trabalho recuperadas estejam protegidas contra ataques recorrentes (de malware inativo ou por meio de aplicativos vulneráveis).

O JetStream DR para AVS, juntamente com os armazenamentos de dados do Azure NetApp Files, pode resolver essas preocupações permitindo que as organizações se recuperem de pontos disponíveis no tempo, para que as cargas de trabalho sejam recuperadas para uma rede funcional e isolada, se necessário. A recuperação permite que os aplicativos funcionem e se comuniquem entre si sem expô-los ao tráfego norte-sul, dando assim às equipes de segurança um local seguro para realizar análises forenses e outras remediações necessárias.

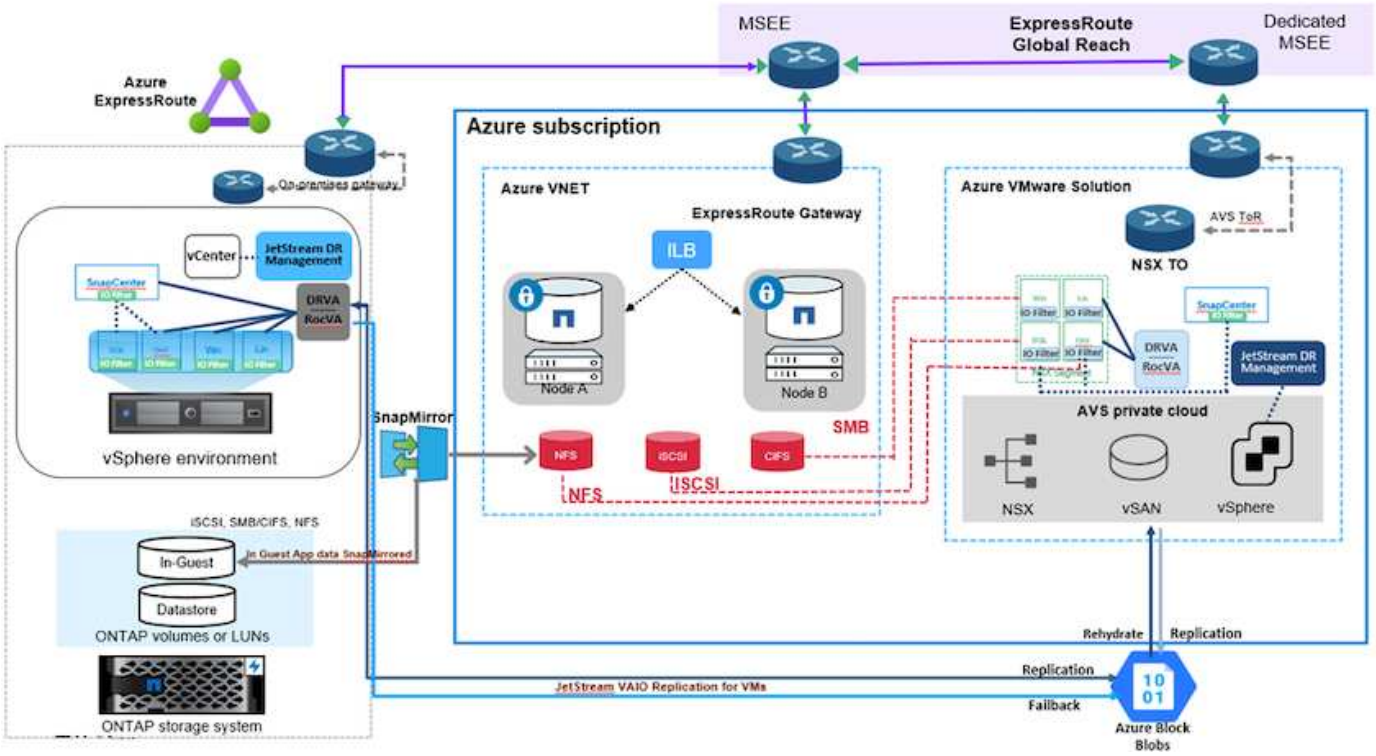


Recuperação de desastres com CVO e AVS (armazenamento conectado ao convidado)

A recuperação de desastres na nuvem é uma maneira resiliente e econômica de proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados, como ransomware. Com o NetApp SnapMirror, as cargas de trabalho locais do VMware que usam armazenamento conectado ao convidado podem ser replicadas para o NetApp Cloud Volumes ONTAP em execução no Azure.

Visão geral

This covers application data; however, what about the actual VMs themselves. Disaster recovery should cover all dependent components, including virtual machines, VMDKs, application data, and more. To accomplish this, SnapMirror along with Jetstream can be used to seamlessly recover workloads replicated from on-premises to Cloud Volumes ONTAP while using vSAN storage for VM VMDKs.
Este documento fornece uma abordagem passo a passo para configurar e executar a recuperação de desastres que usa o NetApp SnapMirror, o JetStream e o Azure VMware Solution (AVS).



Suposições

Este documento se concentra no armazenamento no convidado para dados de aplicativos (também conhecido como convidado conectado), e presumimos que o ambiente local esteja usando o SnapCenter para backups consistentes com aplicativos.

> Este documento se aplica a qualquer solução de backup ou recuperação de terceiros. Dependendo da solução usada no ambiente, siga as práticas recomendadas para criar políticas de backup que atendam aos SLAs organizacionais.

Para conectividade entre o ambiente local e a rede virtual do Azure, use o Express Route Global Reach ou uma WAN virtual com um gateway VPN. Os segmentos devem ser criados com base no design da vLAN local.

> Há várias opções para conectar datacenters locais ao Azure, o que nos impede de descrever

um fluxo de trabalho específico neste documento. Consulte a documentação do Azure para obter o método apropriado de conectividade local com o Azure.

Implementando a solução de DR

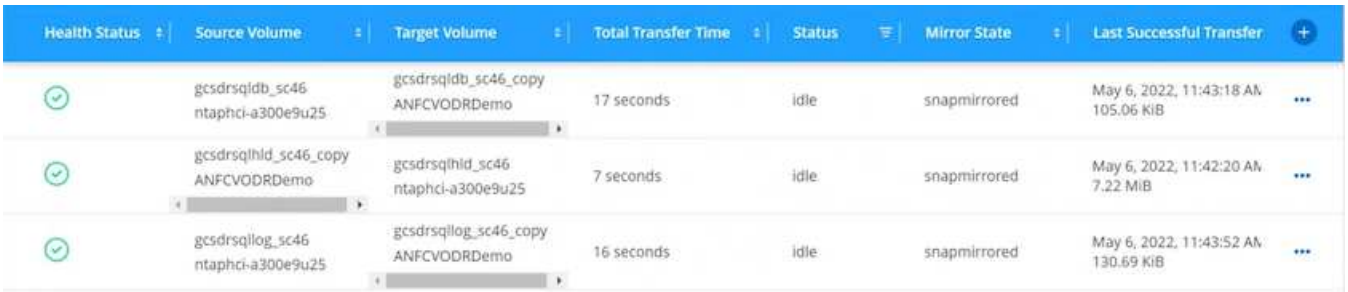
Visão geral da implantação da solução

1. Certifique-se de que os dados do aplicativo sejam copiados usando o SnapCenter com os requisitos de RPO necessários.
2. Provisione o Cloud Volumes ONTAP com o tamanho de instância correto usando o Cloud Manager dentro da assinatura e rede virtual apropriadas.
   a. Configure o SnapMirror para os volumes de aplicativos relevantes.
   b. Atualize as políticas de backup no SnapCenter para acionar atualizações do SnapMirror após os trabalhos agendados.
3. Instale o software JetStream DR no data center local e inicie a proteção para máquinas virtuais.
4. Instale o software JetStream DR na nuvem privada do Azure VMware Solution.
5. Durante um evento de desastre, interrompa o relacionamento do SnapMirror usando o Cloud Manager e acione o failover de máquinas virtuais para o Azure NetApp Files ou para armazenamentos de dados vSAN no site de DR do AVS designado.
   a. Reconecte os LUNs ISCSI e as montagens NFS para as VMs do aplicativo.
6. Invoque o failback para o site protegido por meio da ressincronização reversa do SnapMirror após a recuperação do site primário.

Detalhes da implantação

▼ Configurar o CVO no Azure e replicar volumes para o CVO

O primeiro passo é configurar o Cloud Volumes ONTAP no Azure ("Link") e replicar os volumes desejados para o Cloud Volumes ONTAP com as frequências e retenções de snapshots desejadas.



▼ Configurar hosts AVS e acesso a dados CVO

Dois fatores importantes a serem considerados ao implantar o SDDC são o tamanho do cluster SDDC na solução Azure VMware e por quanto tempo manter o SDDC em serviço. Essas duas considerações importantes para uma solução de recuperação de desastres ajudam a reduzir os custos operacionais gerais. O SDDC pode ter apenas três hosts ou até mesmo um cluster de vários hosts em uma implantação em grande escala.

A decisão de implantar um cluster AVS é baseada principalmente nos requisitos de RPO/RTO. Com a solução Azure VMware, o SDDC pode ser provisionado na hora certa em preparação para testes ou para um evento de desastre real. Um SDDC implantado just in time economiza em custos de host ESXi quando você não está lidando com um desastre. No entanto, essa forma de implantação afeta o RTO por algumas

horas enquanto o SDDC está sendo provisionado.

A opção mais comumente implantada é ter o SDDC em execução em um modo de operação piloto sempre ativo. Essa opção fornece uma pequena área de cobertura de três hosts que estão sempre disponíveis e também acelera as operações de recuperação ao fornecer uma linha de base em execução para atividades de simulação e verificações de conformidade, evitando assim o risco de desvio operacional entre os sites de produção e DR. O cluster de luz piloto pode ser ampliado rapidamente para o nível desejado quando necessário para lidar com um evento de DR real.

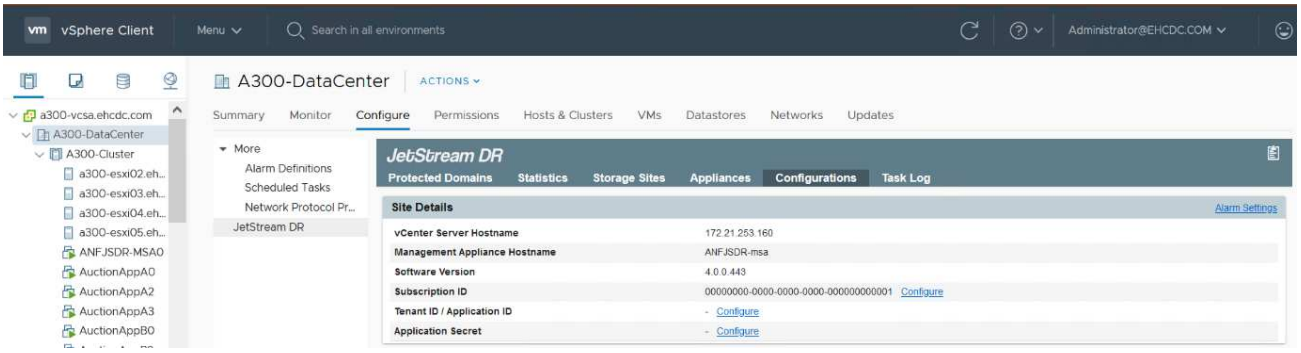
Para configurar o AVS SDDC (seja sob demanda ou no modo piloto), consulte"Implantar e configurar o ambiente de virtualização no Azure" . Como pré-requisito, verifique se as VMs convidadas que residem nos hosts AVS conseguem consumir dados do Cloud Volumes ONTAP depois que a conectividade for estabelecida.

Depois que o Cloud Volumes ONTAP e o AVS forem configurados corretamente, comece a configurar o Jetstream para automatizar a recuperação de cargas de trabalho locais para o AVS (VMs com VMDKs de aplicativo e VMs com armazenamento no convidado) usando o mecanismo VAIO e aproveitando o SnapMirror para cópias de volumes de aplicativo para o Cloud Volumes ONTAP.

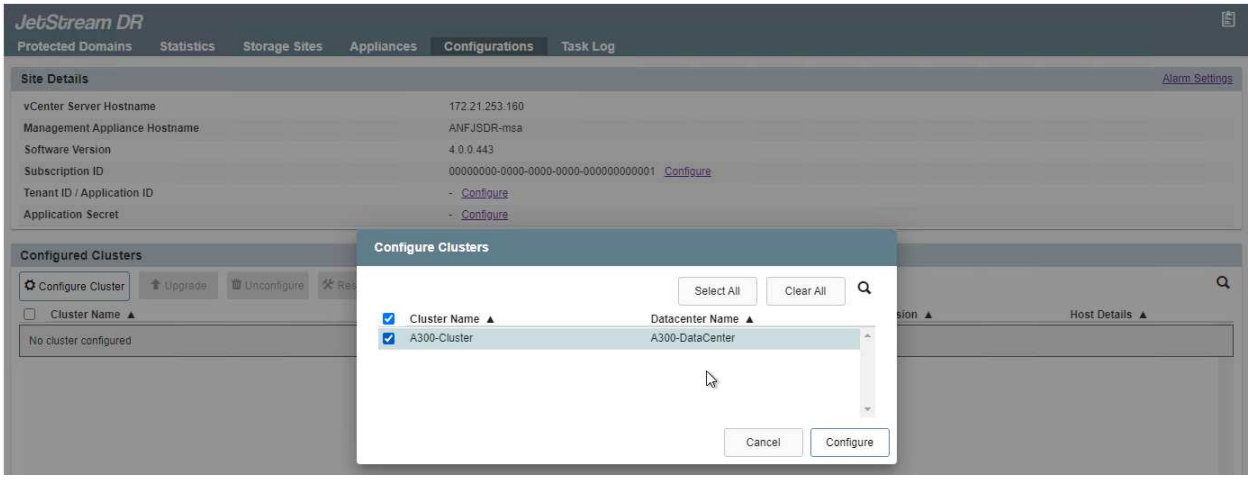
▼ Instalar o JetStream DR no datacenter local

O software JetStream DR consiste em três componentes principais: o JetStream DR Management Server Virtual Appliance (MSA), o DR Virtual Appliance (DRVA) e componentes de host (pacotes de filtros de E/S). O MSA é usado para instalar e configurar componentes do host no cluster de computação e, em seguida, para administrar o software JetStream DR. O processo de instalação é o seguinte:

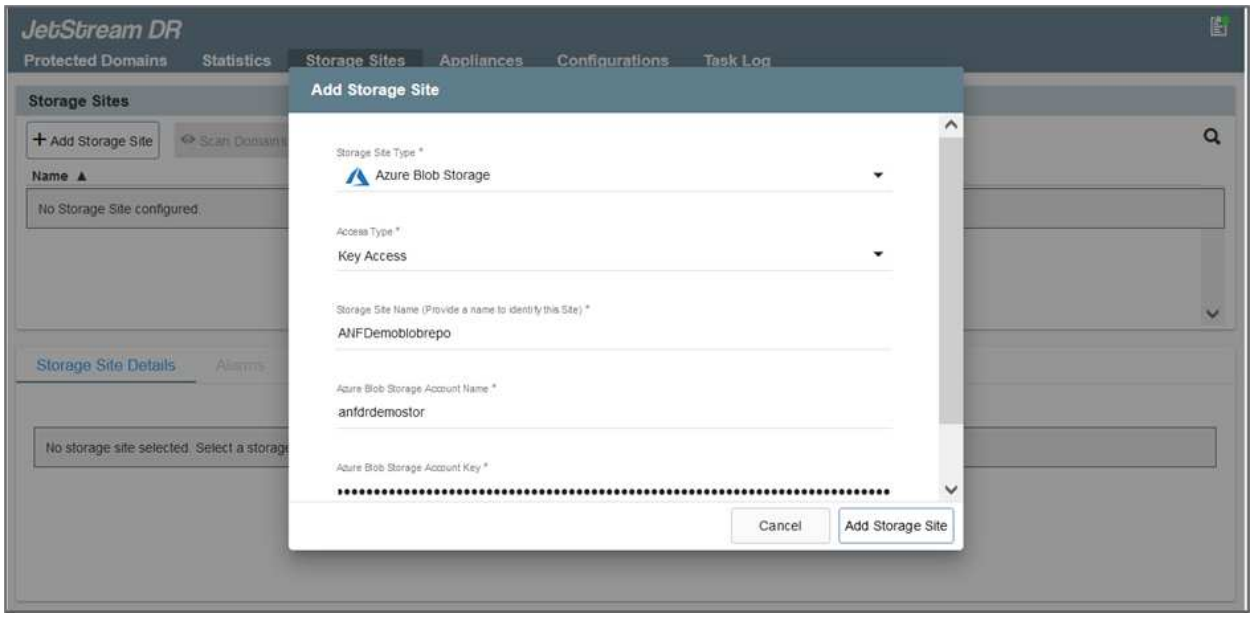
1. Verifique os pré-requisitos.
2. Execute a Ferramenta de Planejamento de Capacidade para obter recomendações de recursos e configuração.
3. Implante o JetStream DR MSA em cada host vSphere no cluster designado.
4. Inicie o MSA usando seu nome DNS em um navegador.
5. Registre o servidor vCenter com o MSA.
6. Depois que o JetStream DR MSA for implantado e o vCenter Server for registrado, navegue até o plug-in JetStream DR com o vSphere Web Client. Isso pode ser feito navegando até Datacenter > Configurar > JetStream DR.



7. Na interface do JetStream DR, conclua as seguintes tarefas:
   a. Configure o cluster com o pacote de filtro de E/S.

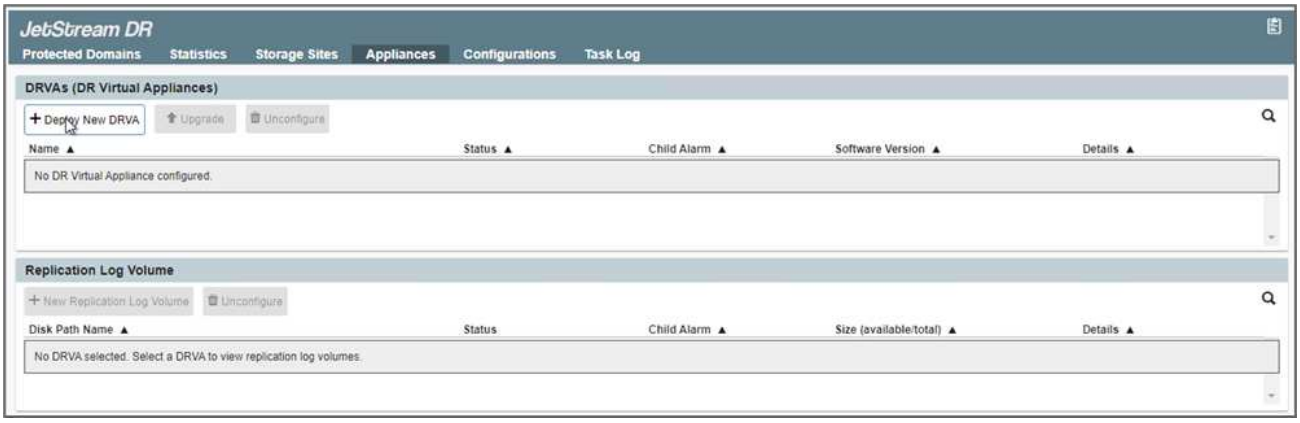


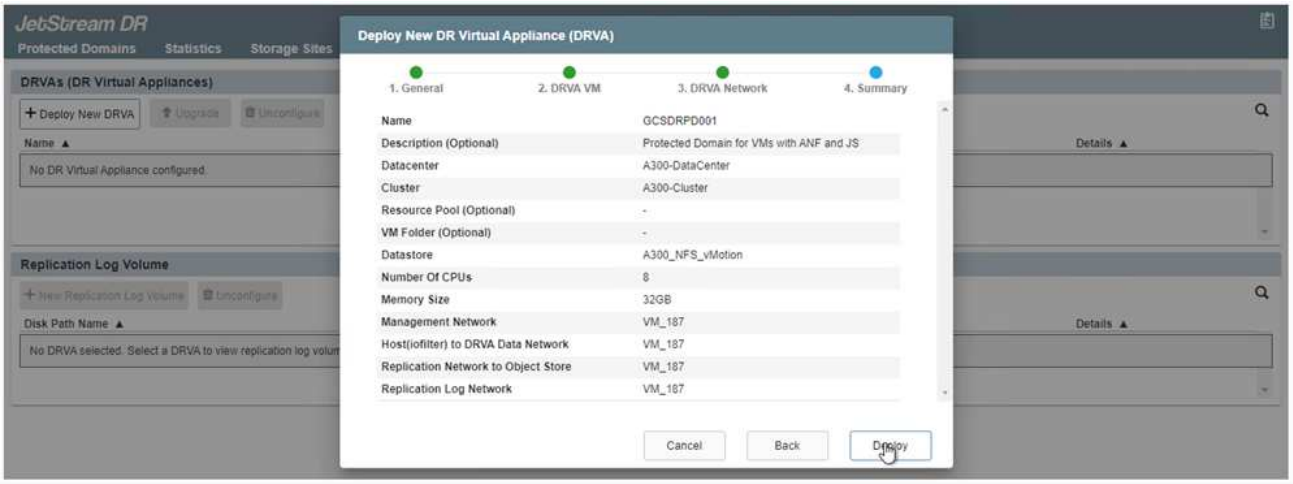
b. Adicione o armazenamento de Blobs do Azure localizado no site de recuperação.



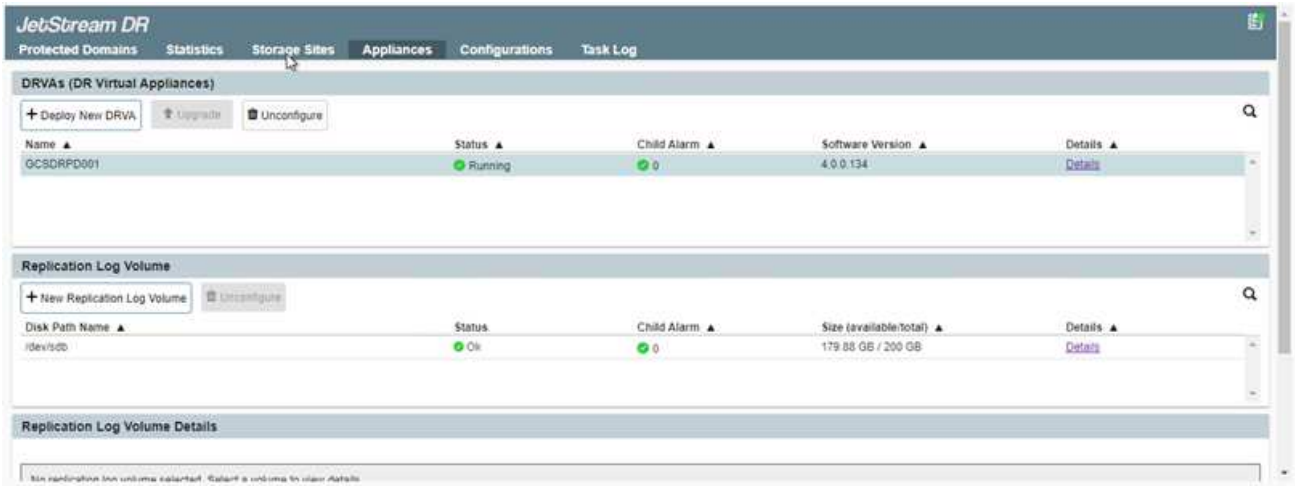
8. Implante o número necessário de DR Virtual Appliances (DRVAs) na guia Appliances.

Use a ferramenta de planejamento de capacidade para estimar o número de DRVAs necessários.

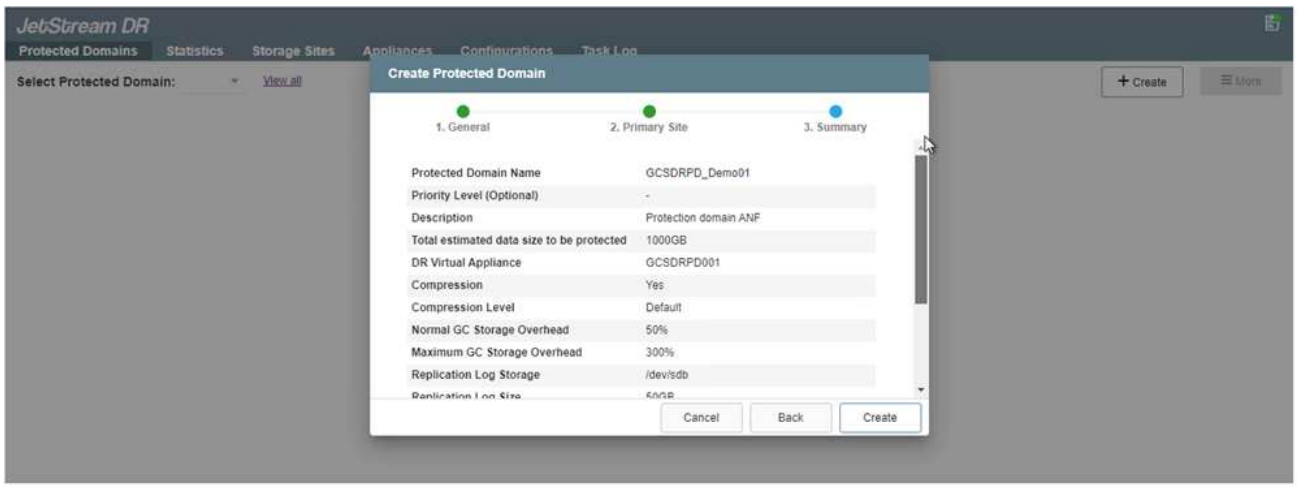


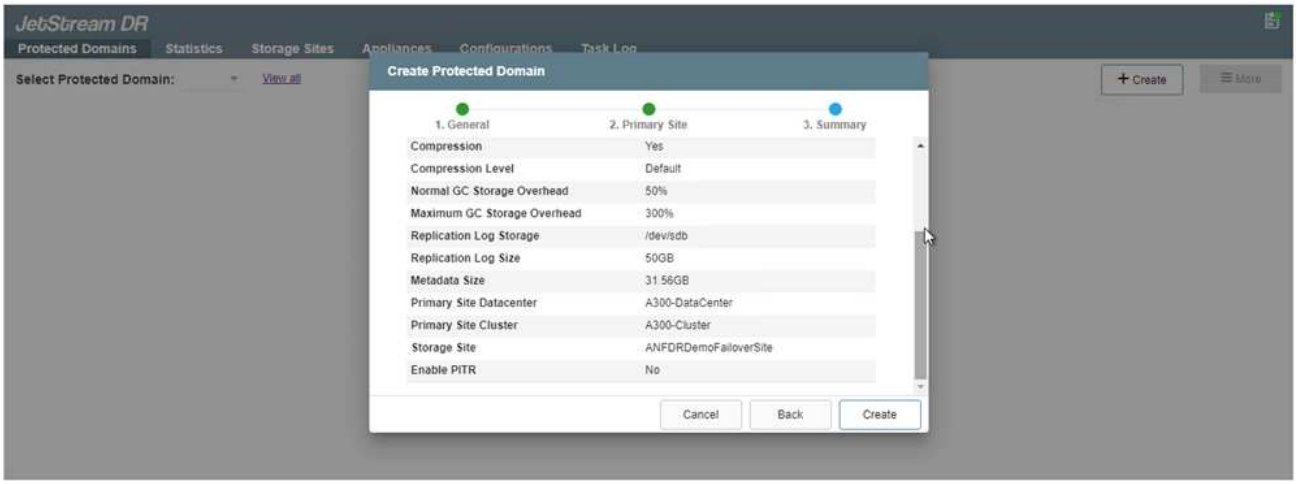


9. Crie volumes de log de replicação para cada DRVA usando o VMDK dos armazenamentos de dados disponíveis ou do pool de armazenamento iSCSI compartilhado independente.



10. Na guia Domínios Protegidos, crie o número necessário de domínios protegidos usando informações sobre o site do Armazenamento de Blobs do Azure, a instância do DRVA e o log de replicação. Um domínio protegido define uma VM específica ou um conjunto de VMs de aplicativos dentro do cluster que são protegidas em conjunto e recebem uma ordem de prioridade para operações de failover/failback.

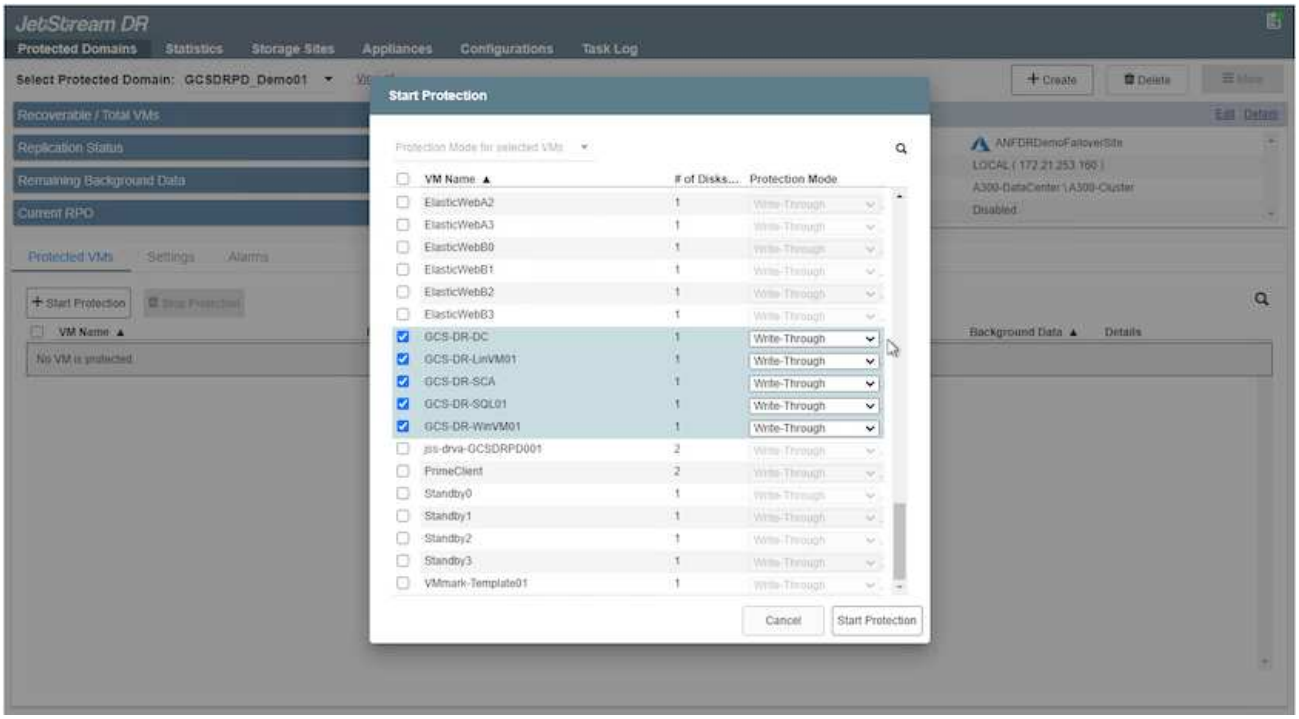




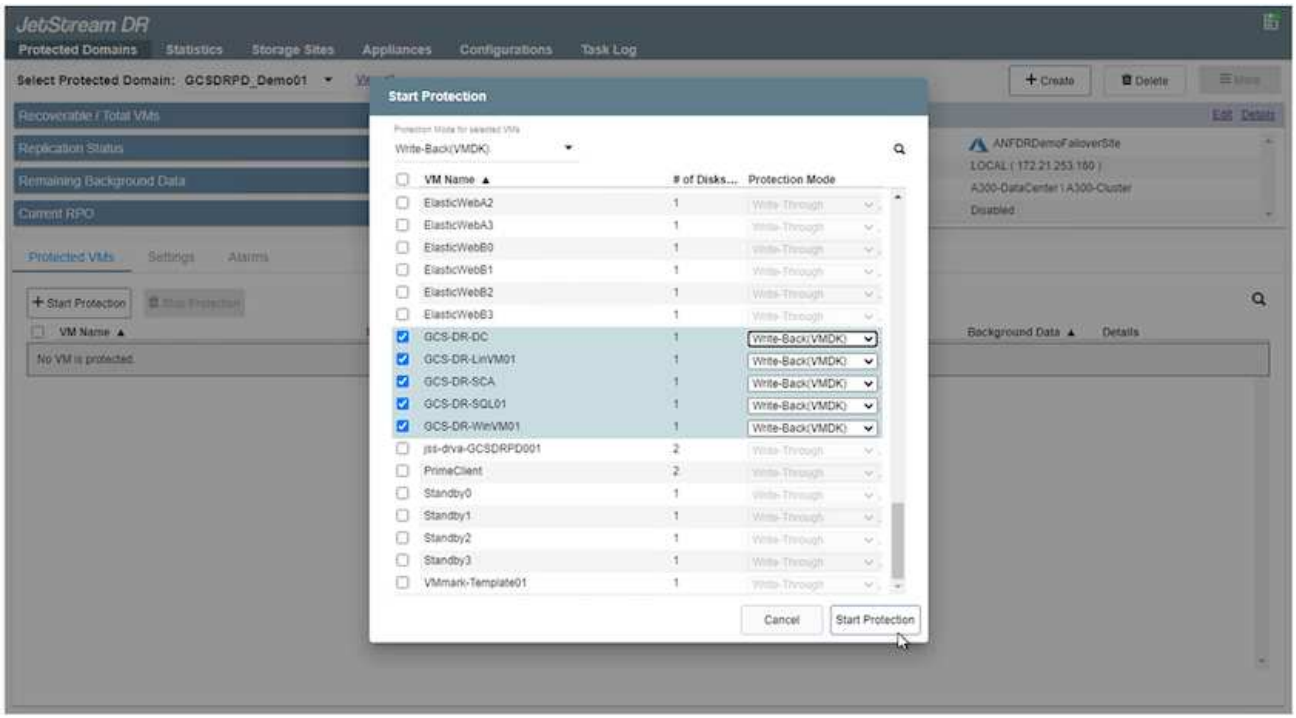
11. Selecione as VMs a serem protegidas e agrupe-as em grupos de aplicativos com base na dependência. As definições de aplicativo permitem agrupar conjuntos de VMs em grupos lógicos que contêm suas ordens de inicialização, atrasos de inicialização e validações de aplicativo opcionais que podem ser executadas na recuperação.

Certifique-se de que o mesmo modo de proteção seja usado para todas as VMs em um domínio protegido.

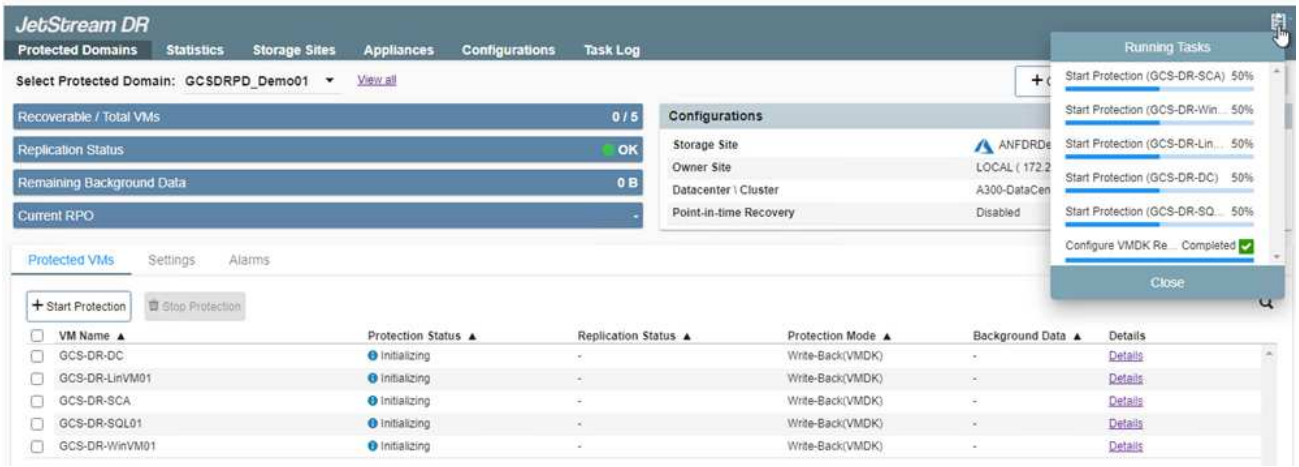
O modo Write-Back (VMDK) oferece maior desempenho.



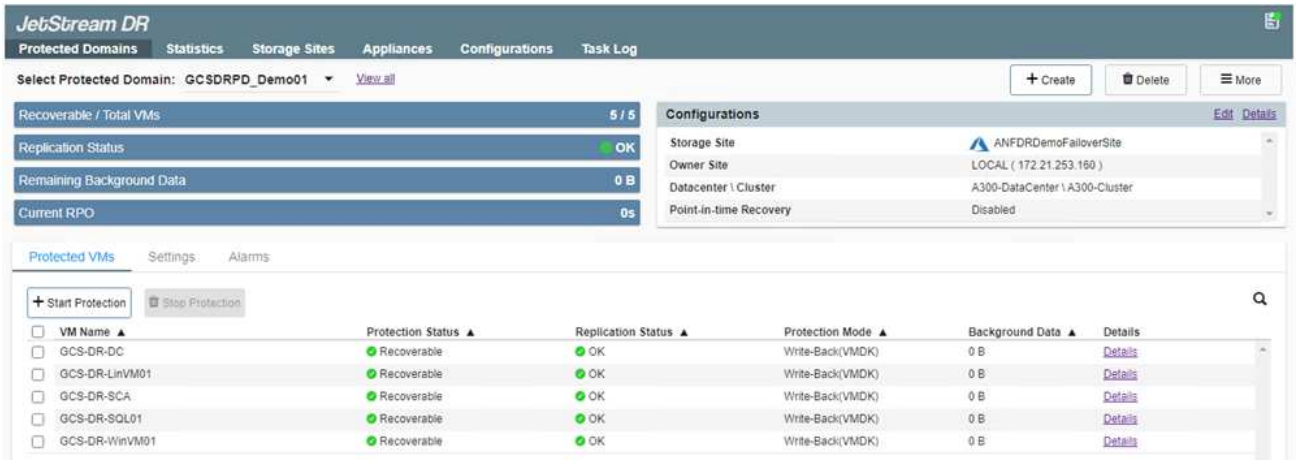
12. Certifique-se de que os volumes de log de replicação sejam colocados em armazenamento de alto desempenho.



13. Após terminar, clique em Iniciar proteção para o domínio protegido. Isso inicia a replicação de dados das VMs selecionadas para o repositório de Blobs designado.



14. Após a conclusão da replicação, o status de proteção da VM é marcado como Recuperável.



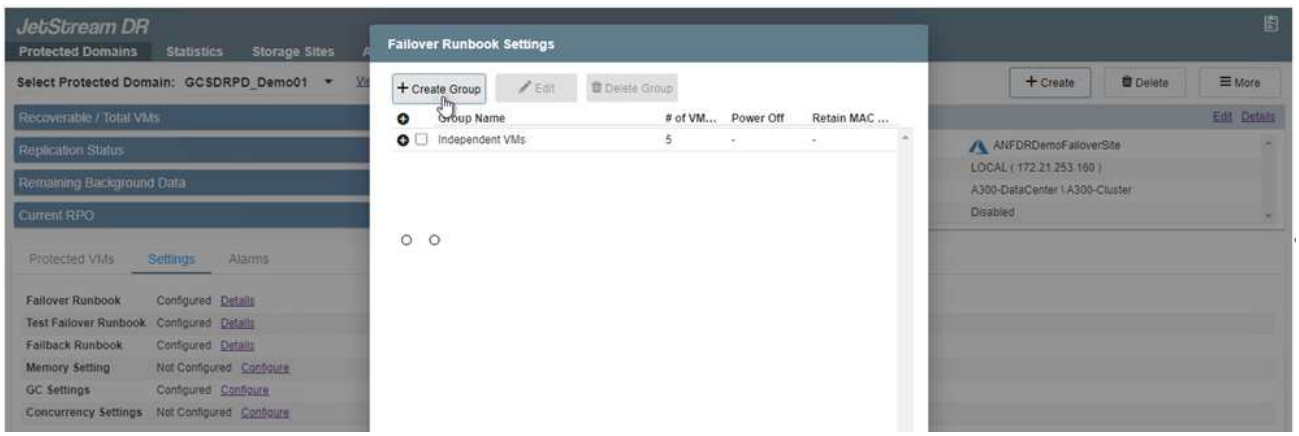
Os runbooks de failover podem ser configurados para agrupar as VMs (chamado de grupo de recuperação), definir a sequência da ordem de inicialização e modificar as configurações de CPU/memória, juntamente com as configurações de IP.

15. Clique em Configurações e depois no link Configurar runbook para configurar o grupo de runbooks.

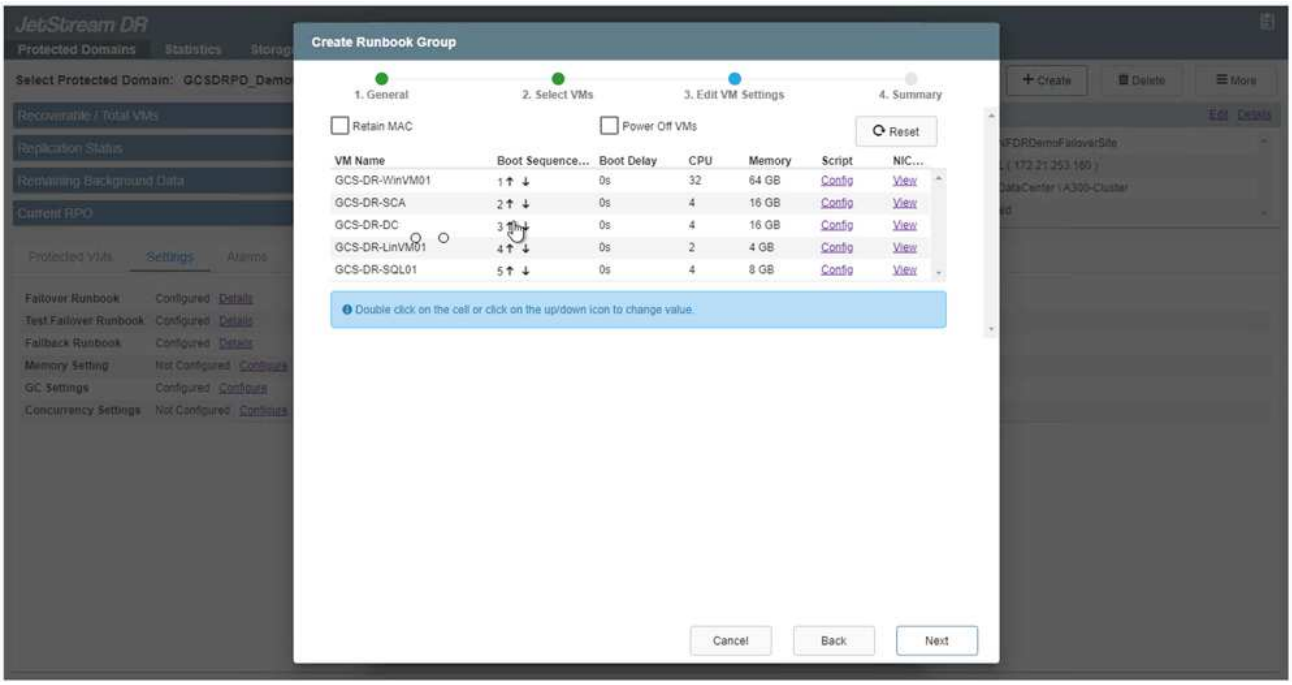


16. Clique no botão Criar grupo para começar a criar um novo grupo de runbook.

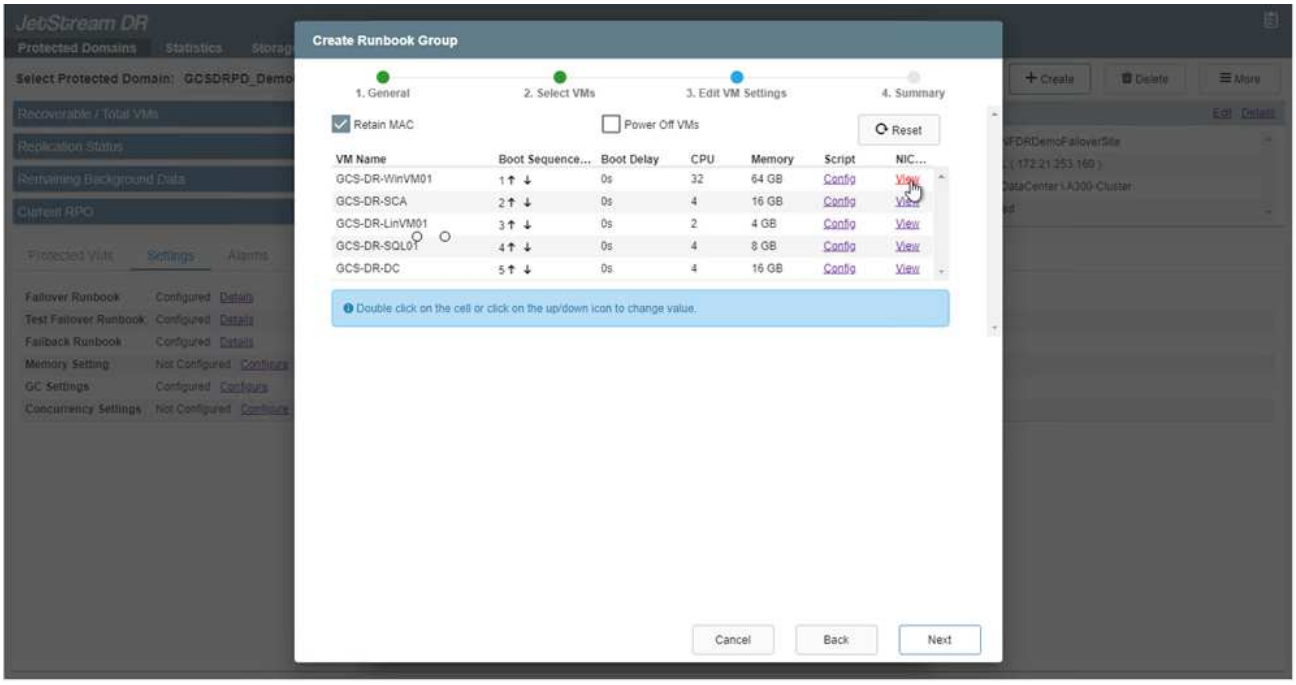
Se necessário, na parte inferior da tela, aplique pré-scripts e pós-scripts personalizados para serem executados automaticamente antes e depois da operação do grupo de runbooks. Certifique-se de que os scripts do Runbook estejam residindo no servidor de gerenciamento.



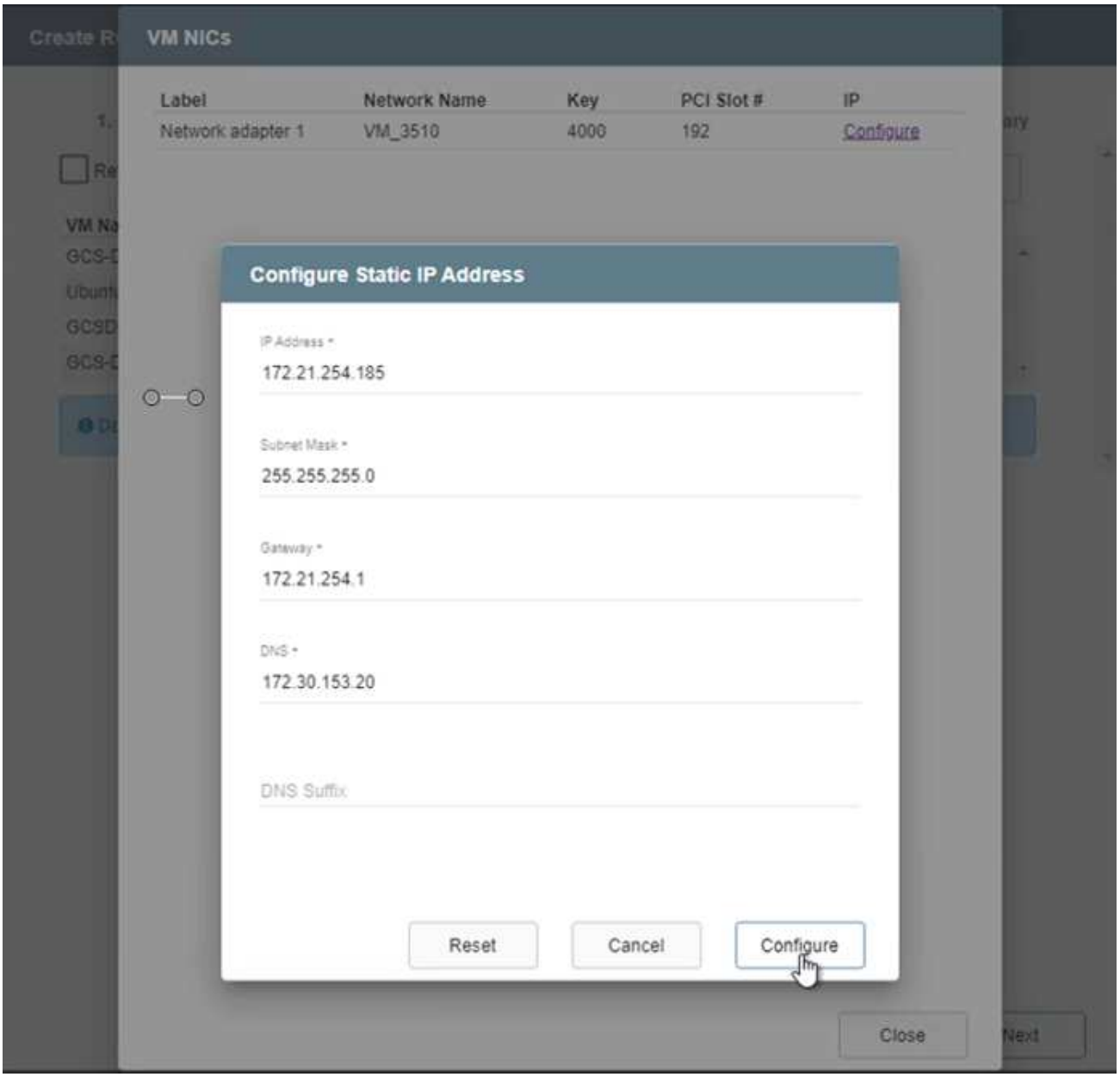
17. Edite as configurações da VM conforme necessário. Especifique os parâmetros para recuperar as VMs, incluindo a sequência de inicialização, o atraso de inicialização (especificado em segundos), o número de CPUs e a quantidade de memória a ser alocada. Altere a sequência de inicialização das VMs clicando nas setas para cima ou para baixo. Também são fornecidas opções para manter o MAC.

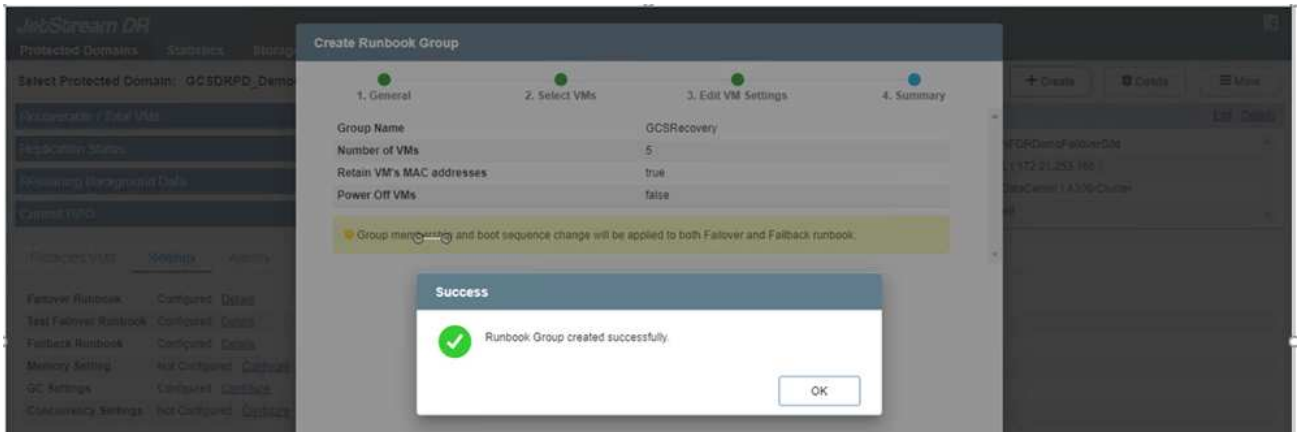


18. Endereços IP estáticos podem ser configurados manualmente para as VMs individuais do grupo. Clique no link Visualização da NIC de uma VM para configurar manualmente suas configurações de endereço IP.



19. Clique no botão Configurar para salvar as configurações de NIC para as respectivas VMs.





O status dos runbooks de failover e failback agora está listado como Configurado. Os grupos de runbooks de failover e failback são criados em pares usando o mesmo grupo inicial de VMs e configurações. Se necessário, as configurações de qualquer grupo de runbooks podem ser personalizadas individualmente clicando no respectivo link Detalhes e fazendo alterações.

▼ Instalar JetStream DR para AVS em nuvem privada

Uma prática recomendada para um site de recuperação (AVS) é criar um cluster de luz piloto de três nós com antecedência. Isso permite que a infraestrutura do site de recuperação seja pré-configurada, incluindo o seguinte:

- Segmentos de rede de destino, firewalls, serviços como DHCP e DNS e assim por diante
- Instalação do JetStream DR para AVS
- Configuração de volumes ANF como datastores e muito mais

O JetStream DR suporta um modo RTO próximo de zero para domínios de missão crítica. Para esses domínios, o armazenamento de destino deve ser pré-instalado. ANF é um tipo de armazenamento recomendado neste caso.

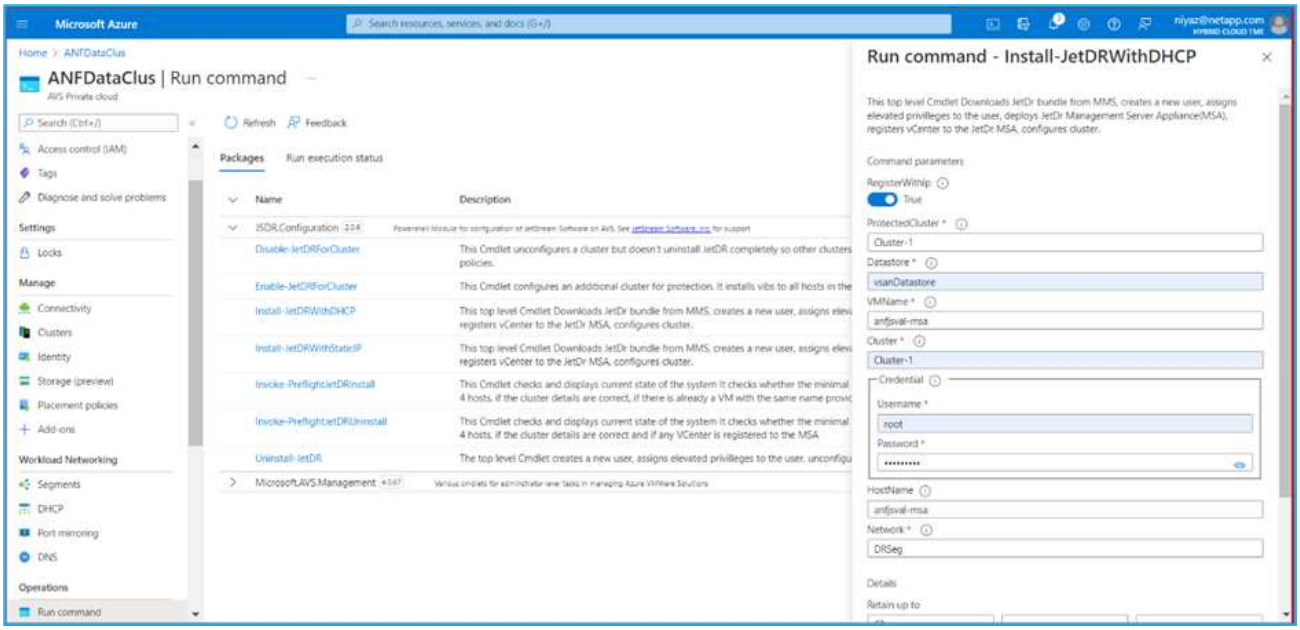
> ⓘ A configuração de rede, incluindo a criação de segmentos, deve ser configurada no cluster AVS para atender aos requisitos locais.

> ⓘ Dependendo dos requisitos de SLA e RTO, você pode usar o failover contínuo ou o modo de failover regular (padrão). Para um RTO próximo de zero, você deve iniciar a reidratação contínua no local de recuperação.

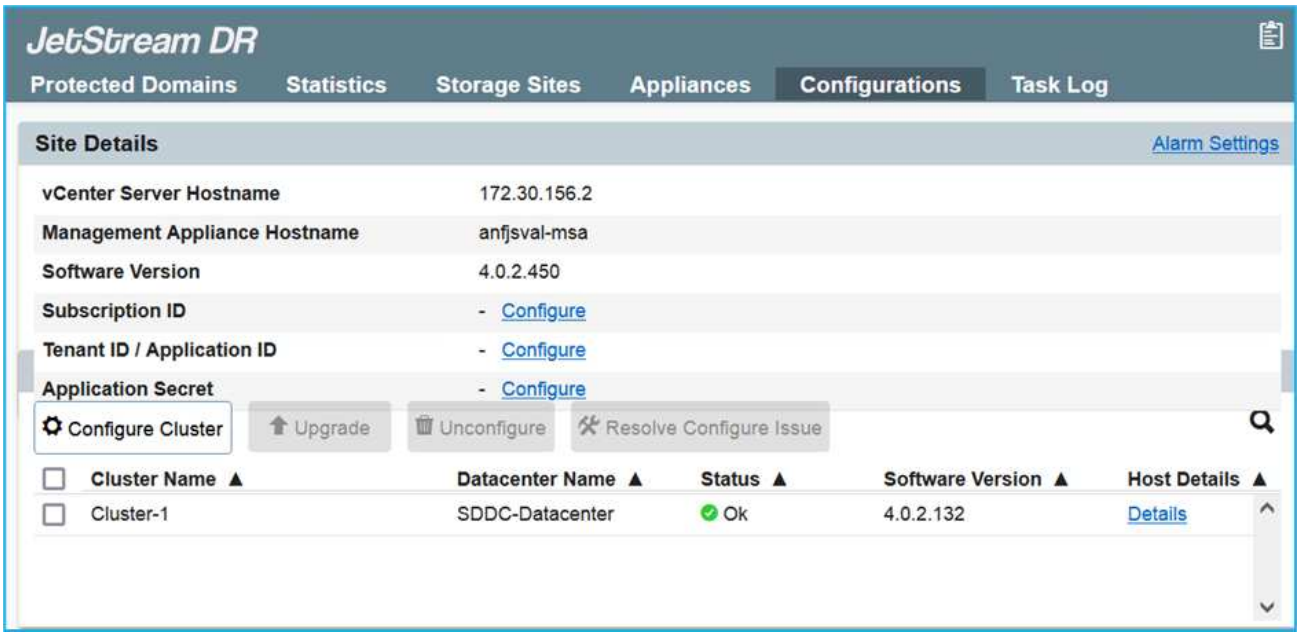
1. Para instalar o JetStream DR para AVS em uma nuvem privada do Azure VMware Solution, use o comando Executar. No portal do Azure, acesse a solução Azure VMware, selecione a nuvem privada e selecione Executar comando > Pacotes > JSDR.Configuration.

> ⓘ O usuário padrão do CloudAdmin do Azure VMware Solution não tem privilégios suficientes para instalar o JetStream DR para AVS. A Solução VMware do Azure permite a instalação simplificada e automatizada do JetStream DR invocando o comando Executar Solução VMware do Azure para o JetStream DR.

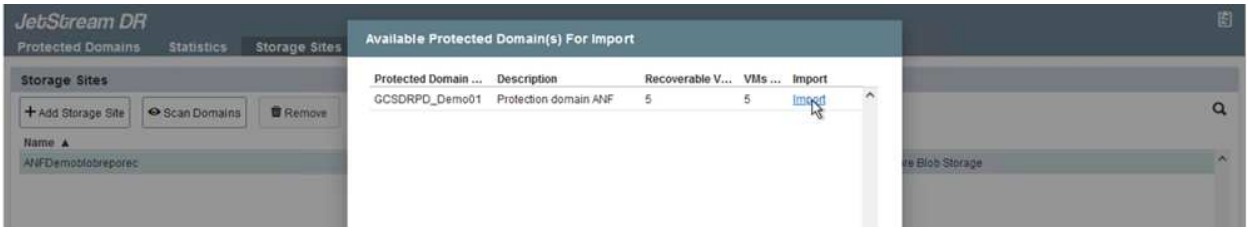
A captura de tela a seguir mostra a instalação usando um endereço IP baseado em DHCP.



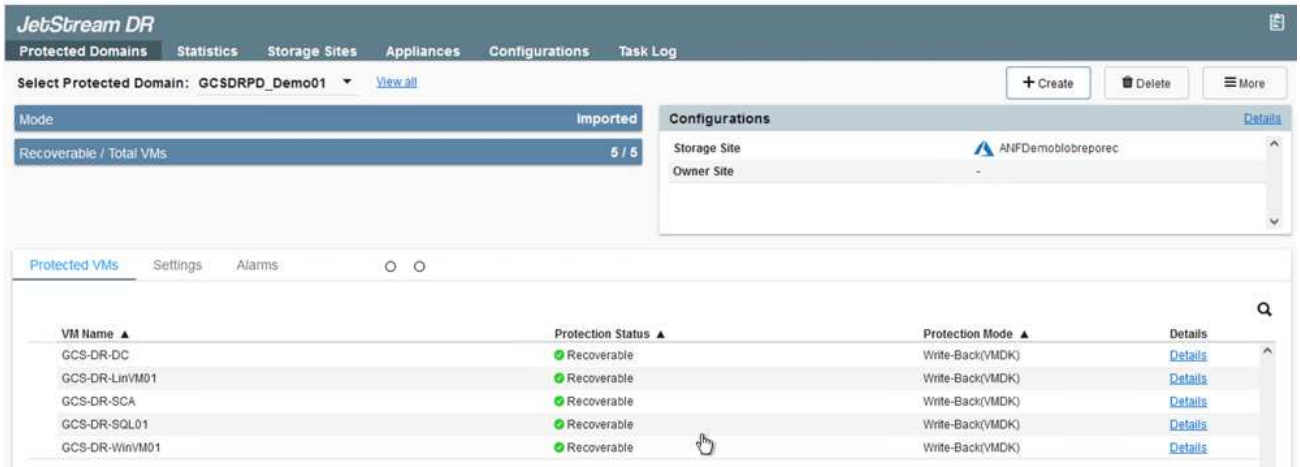
2. Após a conclusão da instalação do JetStream DR para AVS, atualize o navegador. Para acessar a interface do usuário do JetStream DR, vá para SDDC Datacenter > Configurar > JetStream DR.



3. Na interface do JetStream DR, conclua as seguintes tarefas:
   a. Adicione a conta do Armazenamento de Blobs do Azure que foi usada para proteger o cluster local como um site de armazenamento e execute a opção Verificar Domínios.
   b. Na janela de diálogo pop-up que aparece, selecione o domínio protegido a ser importado e clique no link Importar.



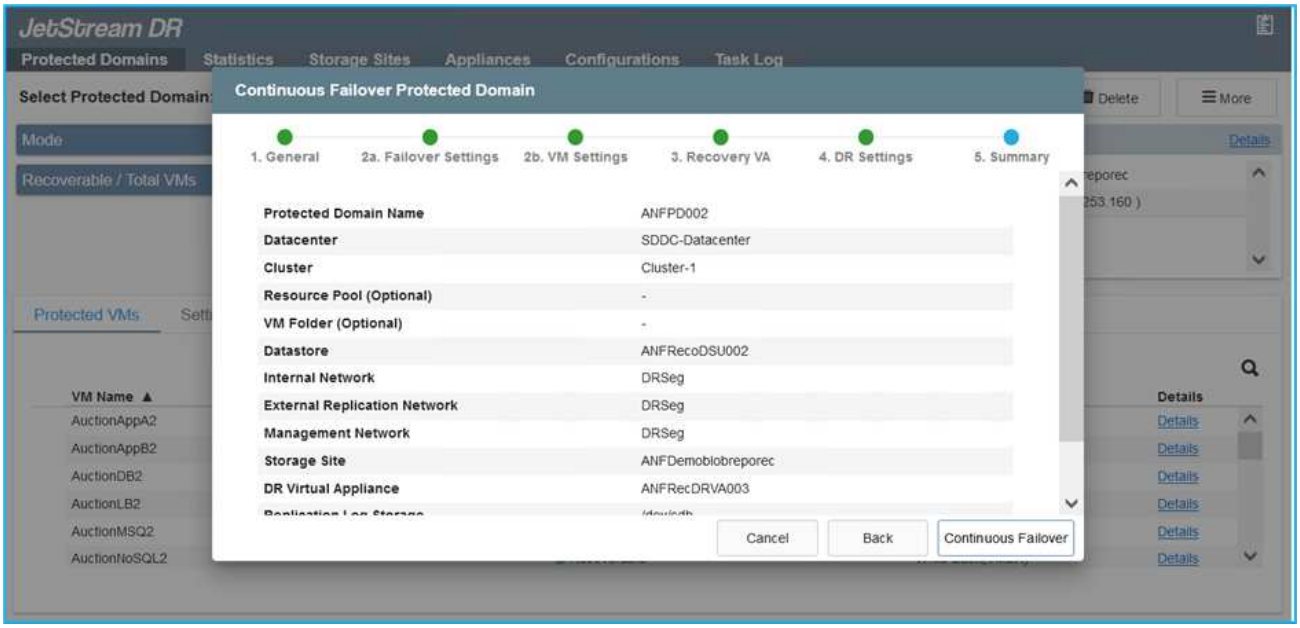
4. O domínio é importado para recuperação. Vá para a aba Domínios Protegidos e verifique se o domínio pretendido foi selecionado ou escolha o desejado no menu Selecionar Domínio Protegido. Uma lista de VMs recuperáveis no domínio protegido é exibida.



5. Depois que os domínios protegidos forem importados, implante os dispositivos DRVA.

Essas etapas também podem ser automatizadas usando planos criados pela CPT.

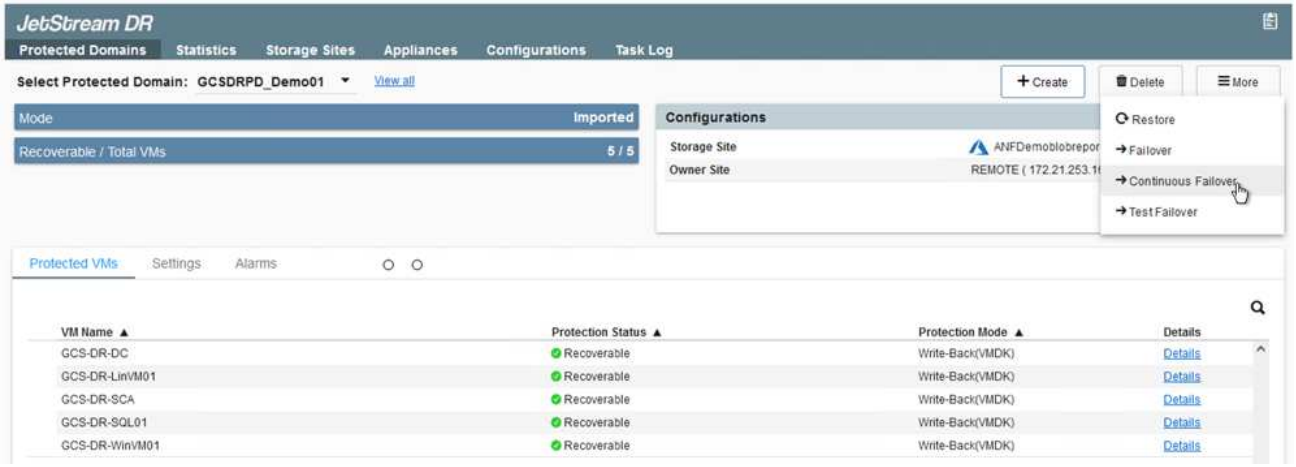
6. Crie volumes de log de replicação usando armazenamentos de dados vSAN ou ANF disponíveis.
7. Importe os domínios protegidos e configure a VA de recuperação para usar um armazenamento de dados ANF para posicionamentos de VM.



Certifique-se de que o DHCP esteja habilitado no segmento selecionado e que haja IPs suficientes disponíveis. IPs dinâmicos são usados temporariamente enquanto os domínios estão se recuperando. Cada VM em recuperação (incluindo reidratação contínua) requer um IP dinâmico individual. Após a recuperação ser concluída, o IP é liberado e pode ser reutilizado.

8. Selecione a opção de failover apropriada (failover contínuo ou failover). Neste exemplo, a reidratação contínua (failover contínuo) é selecionada.

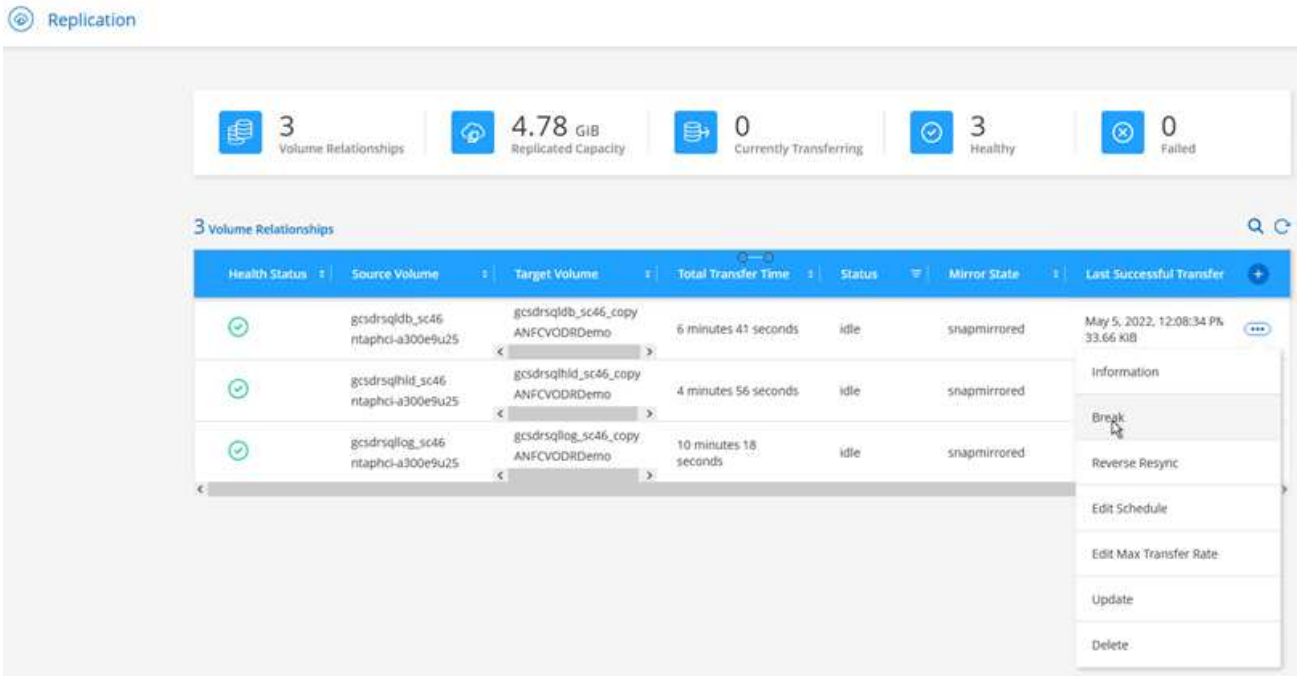
Embora os modos Failover Contínuo e Failover sejam diferentes em quando a configuração é realizada, ambos os modos de failover são configurados usando as mesmas etapas. As etapas de failover são configuradas e executadas juntas em resposta a um evento de desastre. O failover contínuo pode ser configurado a qualquer momento e então executado em segundo plano durante a operação normal do sistema. Após a ocorrência de um evento de desastre, o failover contínuo é concluído para transferir imediatamente a propriedade das VMs protegidas para o site de recuperação (RTO próximo de zero).

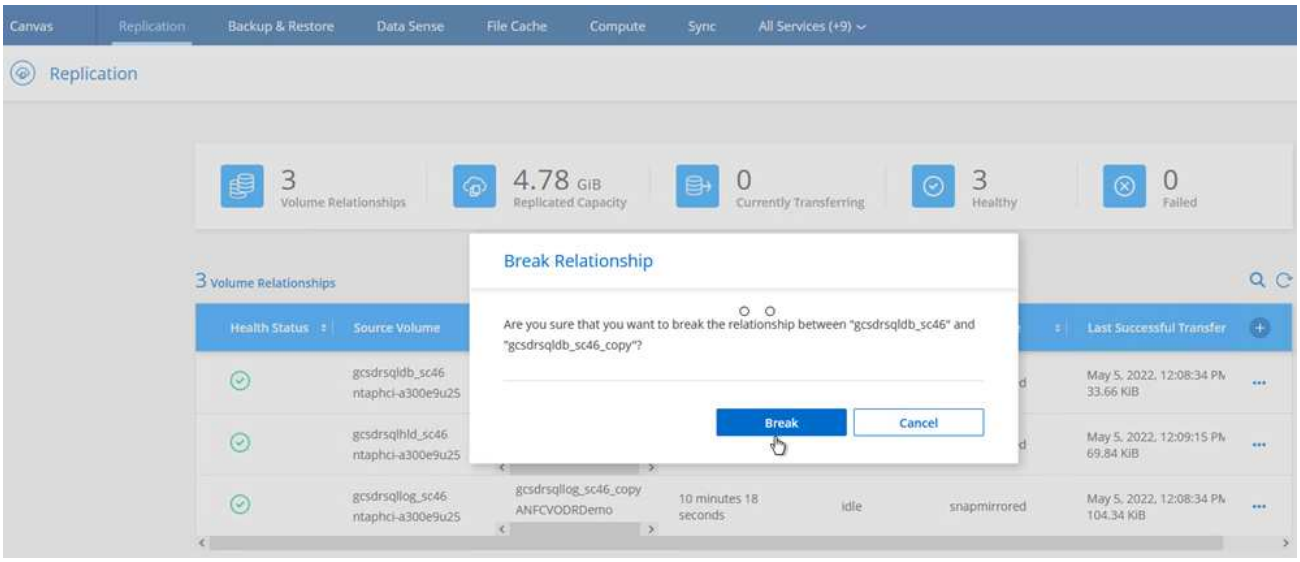


O processo de failover contínuo é iniciado e seu progresso pode ser monitorado pela interface do usuário. Clicar no ícone azul na seção Etapa atual expõe uma janela pop-up mostrando detalhes da etapa atual do processo de failover.

▼ **Failover e Failback**

1. Após ocorrer um desastre no cluster protegido do ambiente local (falha parcial ou completa), você pode acionar o failover para VMs usando o Jetstream após interromper o relacionamento do SnapMirror para os respectivos volumes de aplicativo.

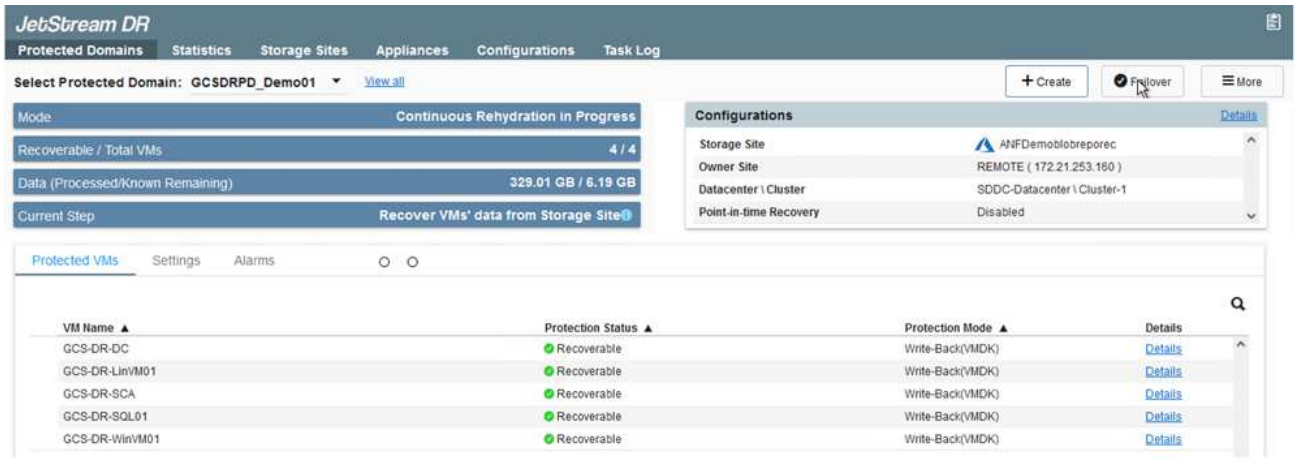


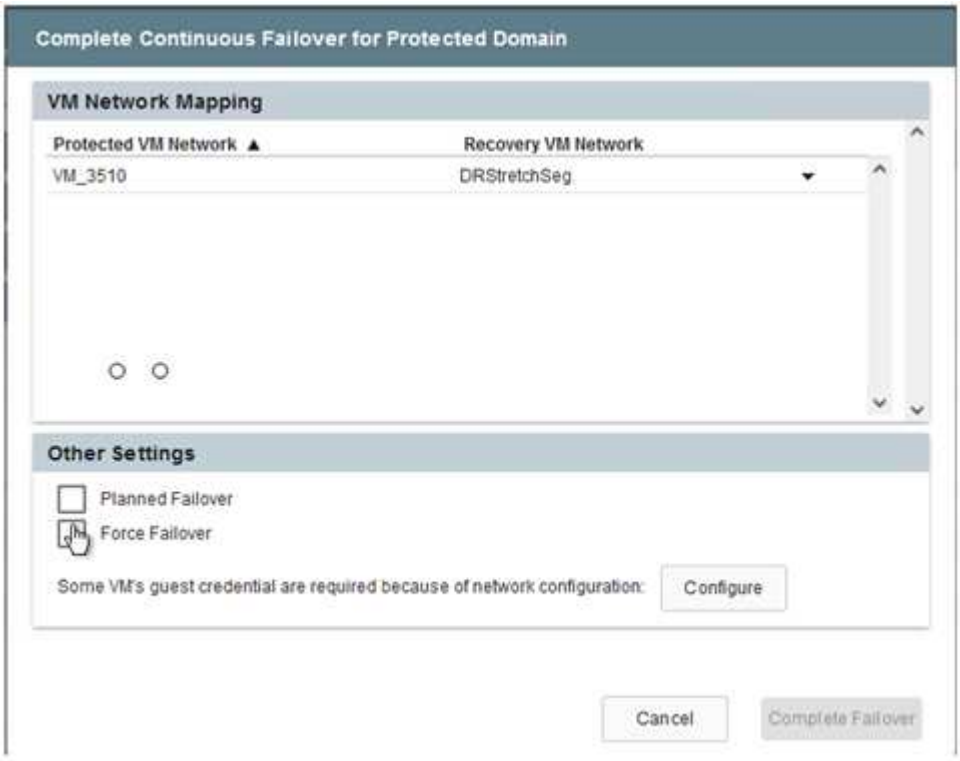


Esta etapa pode ser facilmente automatizada para facilitar o processo de recuperação.

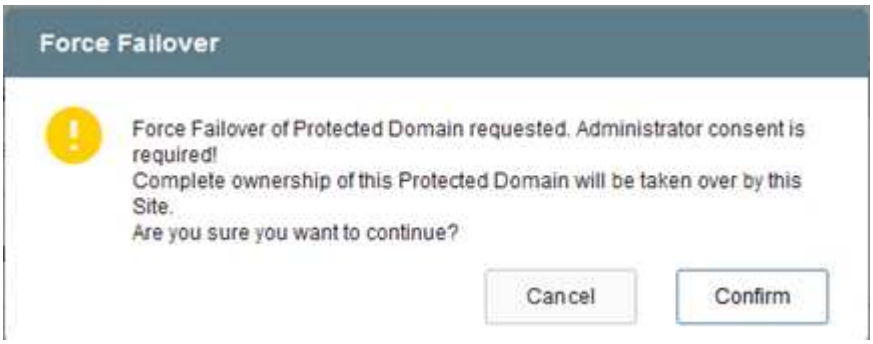
2. Acesse a interface do usuário do Jetstream no AVS SDDC (lado de destino) e acione a opção de failover para concluir o failover. A barra de tarefas mostra o progresso das atividades de failover.

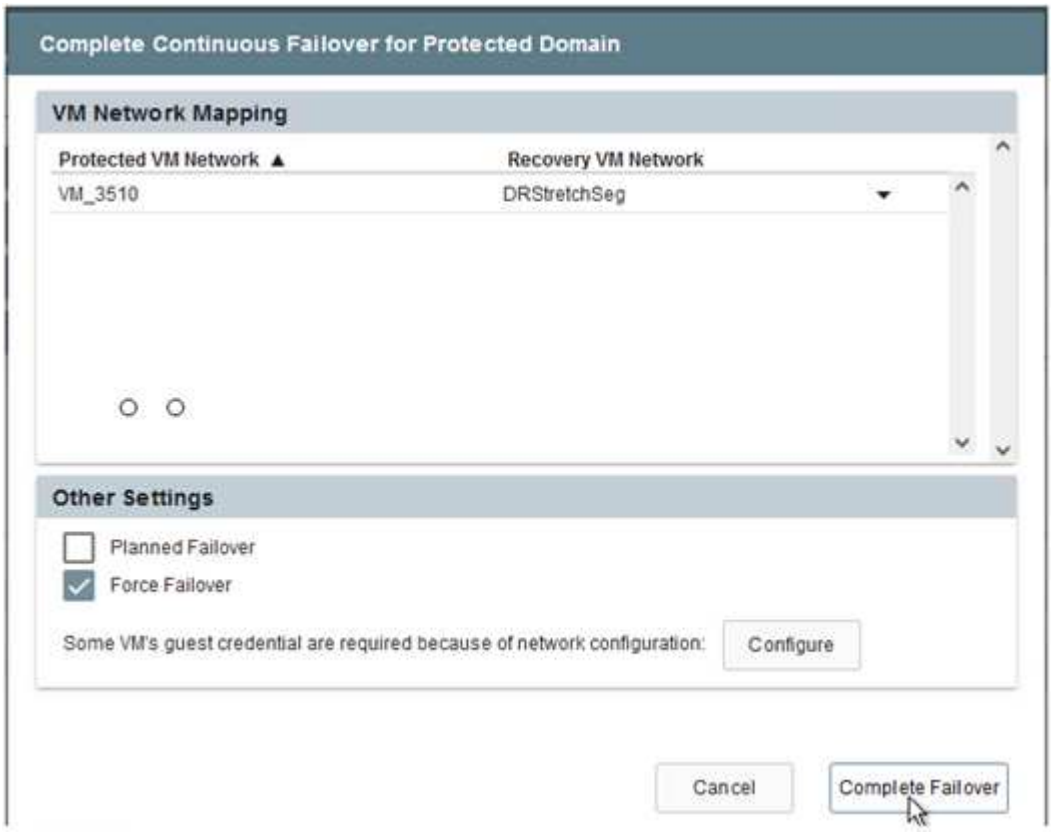
   Na janela de diálogo que aparece ao concluir o failover, a tarefa de failover pode ser especificada como planejada ou assumida como forçada.





O failover forçado pressupõe que o site principal não está mais acessível e a propriedade do domínio protegido deve ser assumida diretamente pelo site de recuperação.





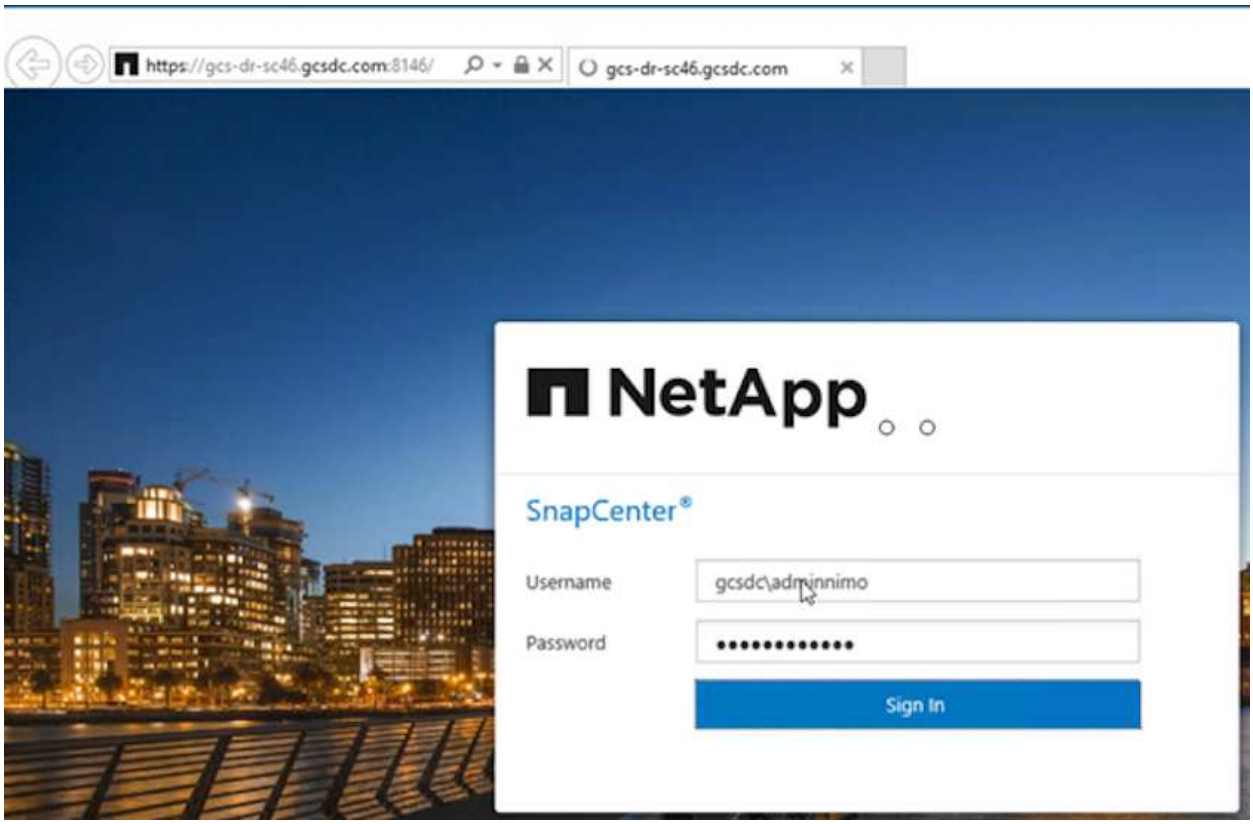
3. Após a conclusão do failover contínuo, uma mensagem será exibida confirmando a conclusão da tarefa. Quando a tarefa estiver concluída, acesse as VMs recuperadas para configurar sessões ISCSI ou NFS.

O modo de failover muda para Em execução no failover e o status da VM é Recuperável. Todas as VMs do domínio protegido agora estão em execução no site de recuperação no estado especificado pelas configurações do runbook de failover.

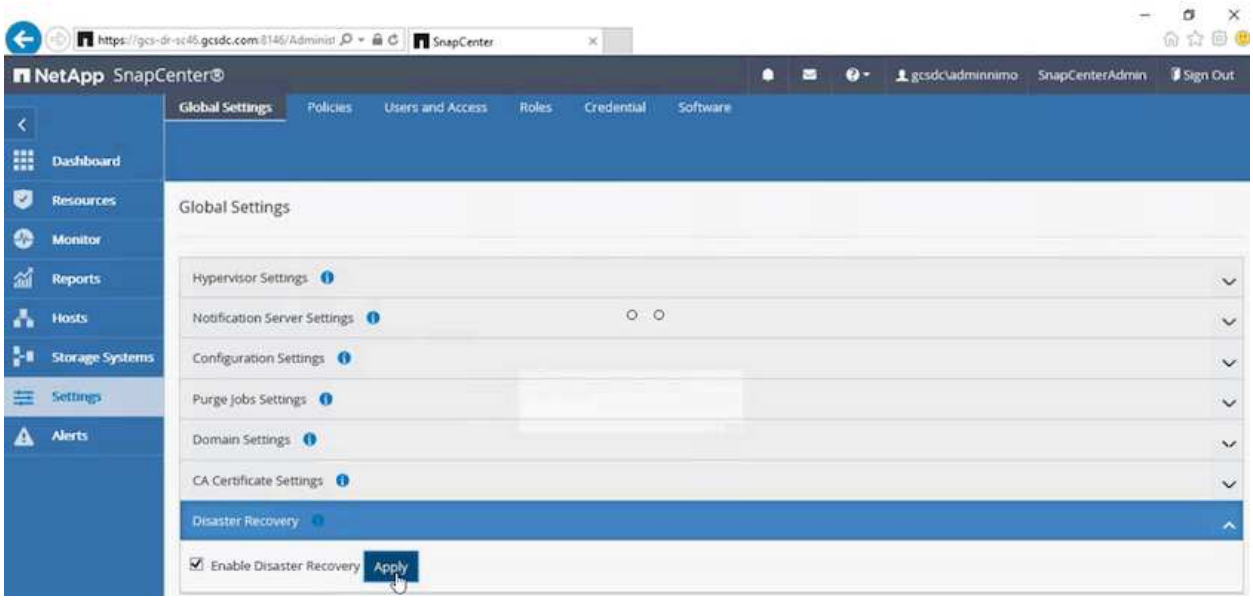
Para verificar a configuração e a infraestrutura de failover, o JetStream DR pode ser operado no modo de teste (opção Test Failover) para observar a recuperação de máquinas virtuais e seus dados do armazenamento de objetos em um ambiente de recuperação de teste. Quando um procedimento de failover é executado no modo de teste, sua operação se assemelha a um processo de failover real.



4. Depois que as máquinas virtuais forem recuperadas, use a recuperação de desastres de armazenamento para armazenamento no convidado. Para demonstrar esse processo, o servidor SQL é usado neste exemplo.
5. Efetue login na VM SnapCenter recuperada no AVS SDDC e ative o modo DR.
   a. Acesse a interface do usuário do SnapCenter usando o navegadorN.



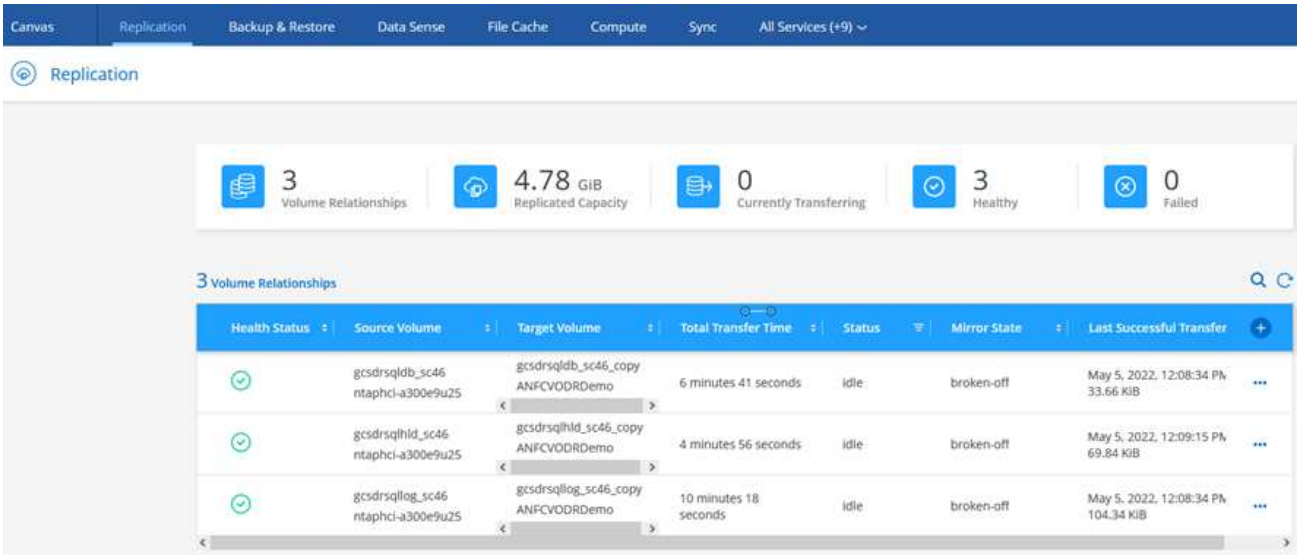
   b. Na página Configurações, navegue até Configurações > Configurações globais > Recuperação de desastres.
   c. Selecione Habilitar recuperação de desastres.
   d. Clique em Aplicar.



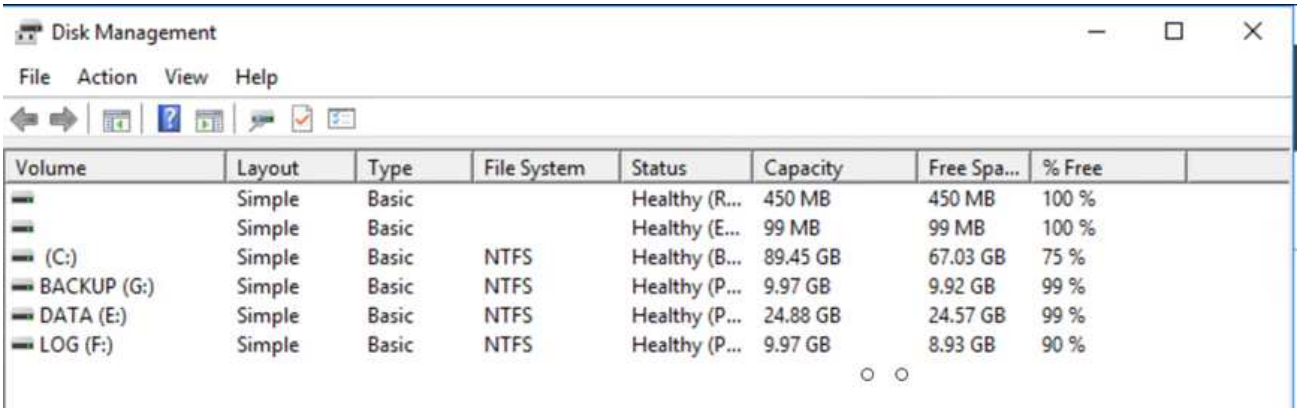
e. Verifique se o trabalho de DR está habilitado clicando em Monitor > Trabalhos.

> O NetApp SnapCenter 4.6 ou posterior deve ser usado para recuperação de desastres de armazenamento. Para versões anteriores, snapshots consistentes com o aplicativo (replicados usando SnapMirror) devem ser usados e a recuperação manual deve ser executada caso backups anteriores precisem ser recuperados no site de recuperação de desastres.

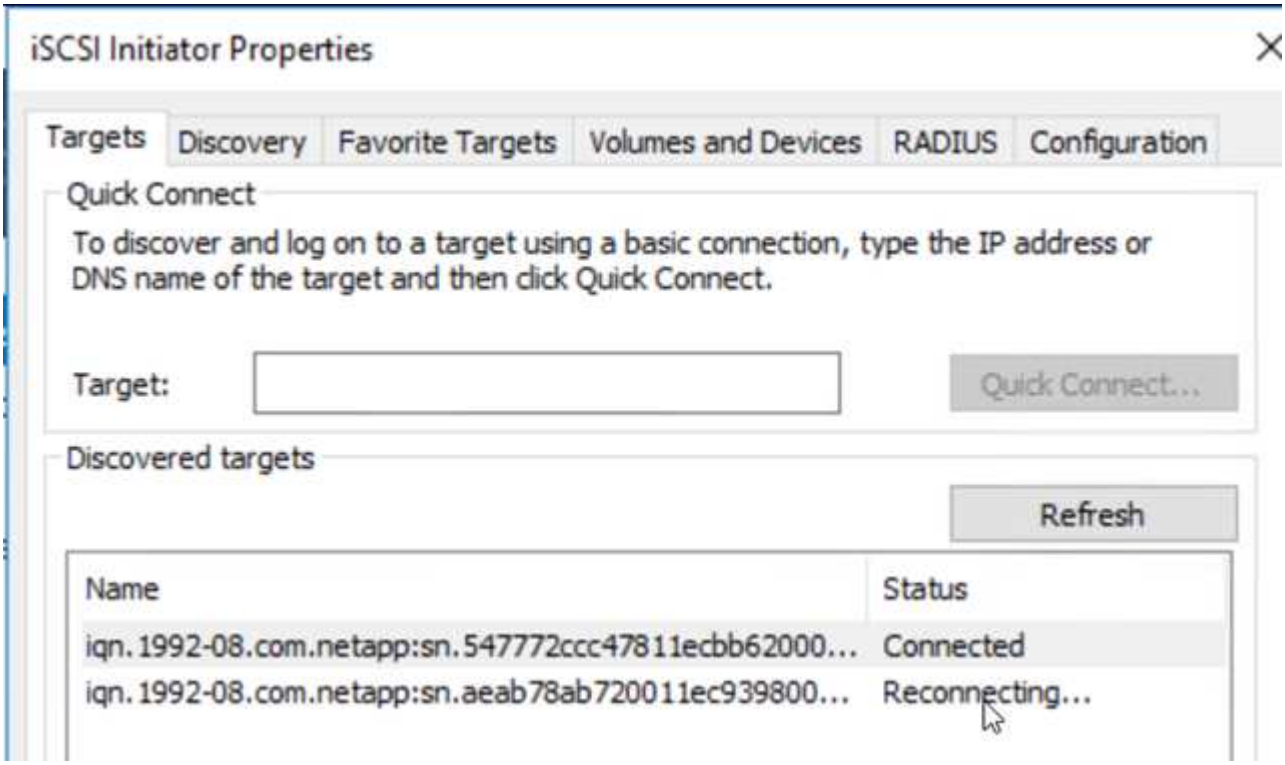
6. Certifique-se de que o relacionamento SnapMirror esteja quebrado.



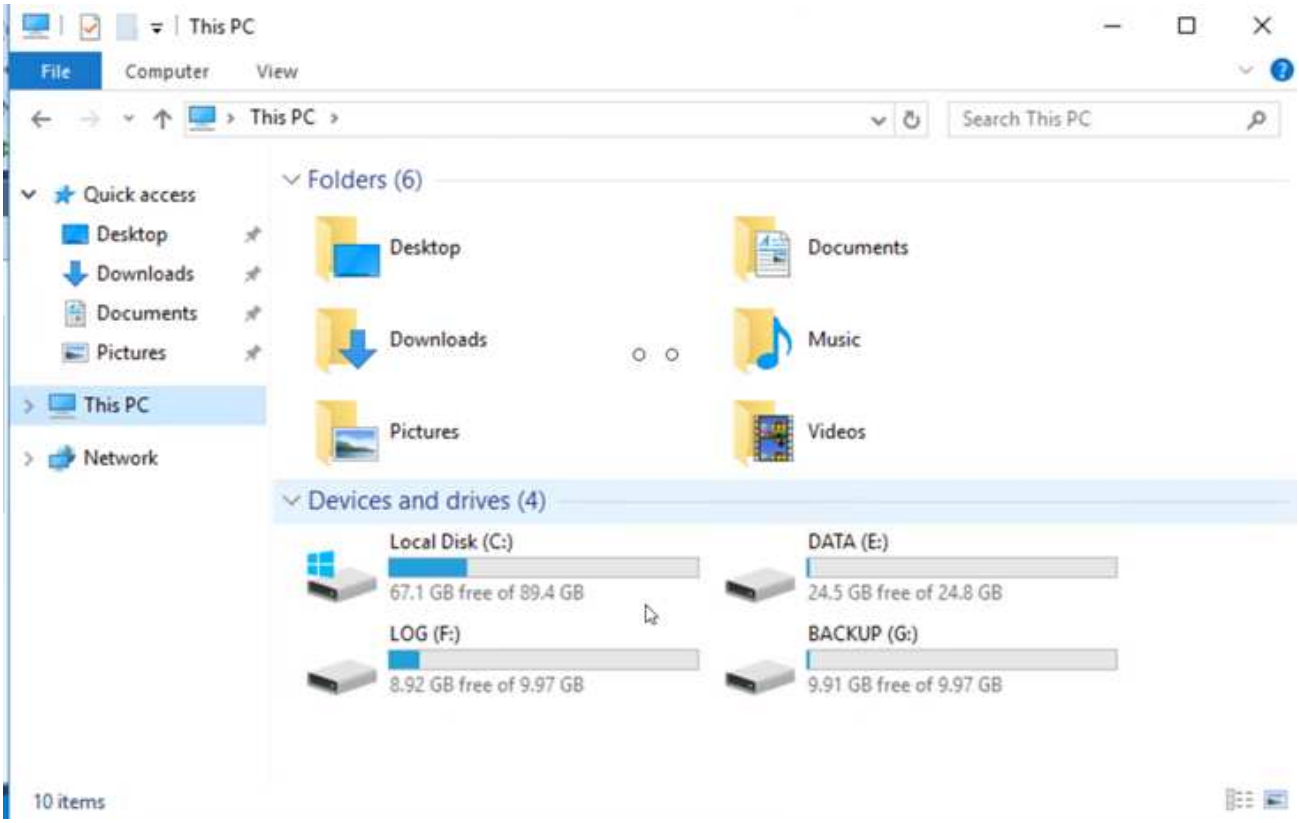
7. Anexe o LUN do Cloud Volumes ONTAP à VM convidada do SQL recuperada com as mesmas letras de unidade.



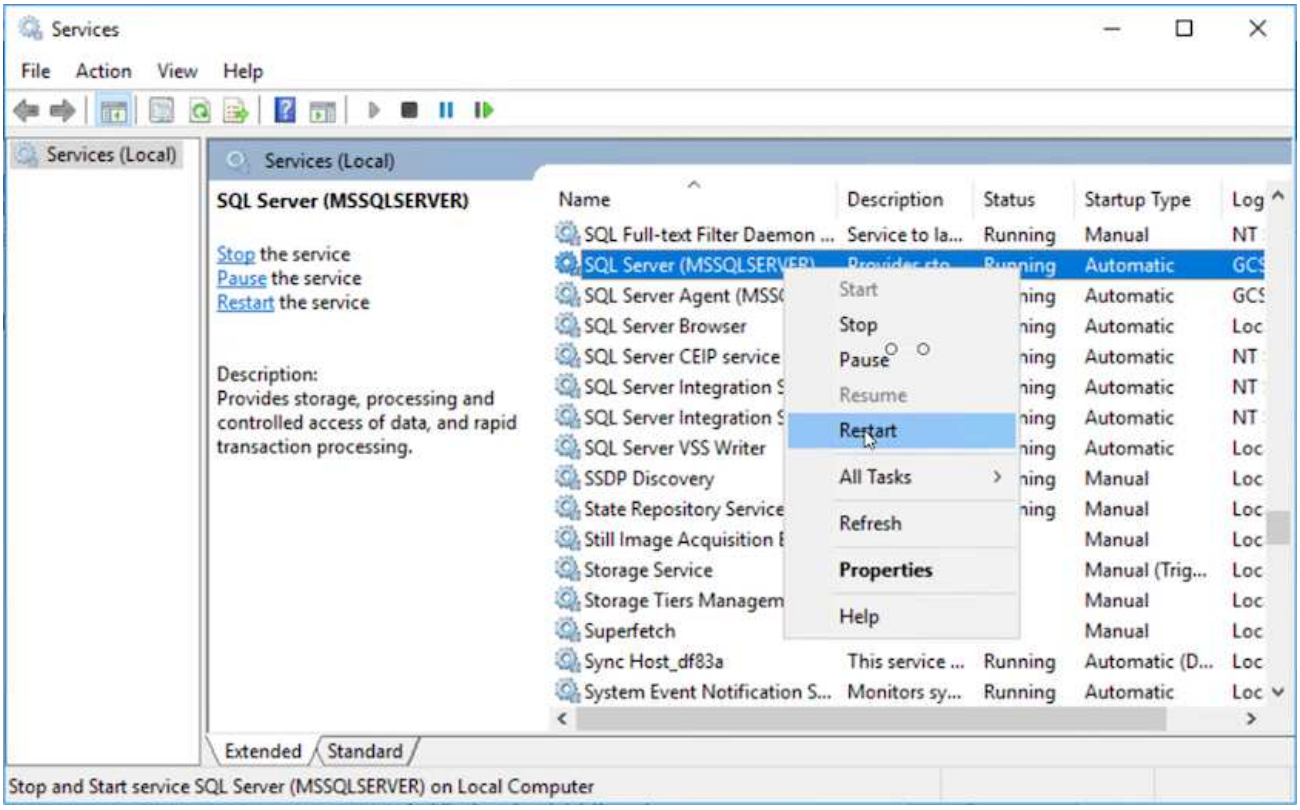
8. Abra o iSCSI Initiator, limpe a sessão desconectada anterior e adicione o novo destino junto com o multipath para os volumes Cloud Volumes ONTAP replicados.



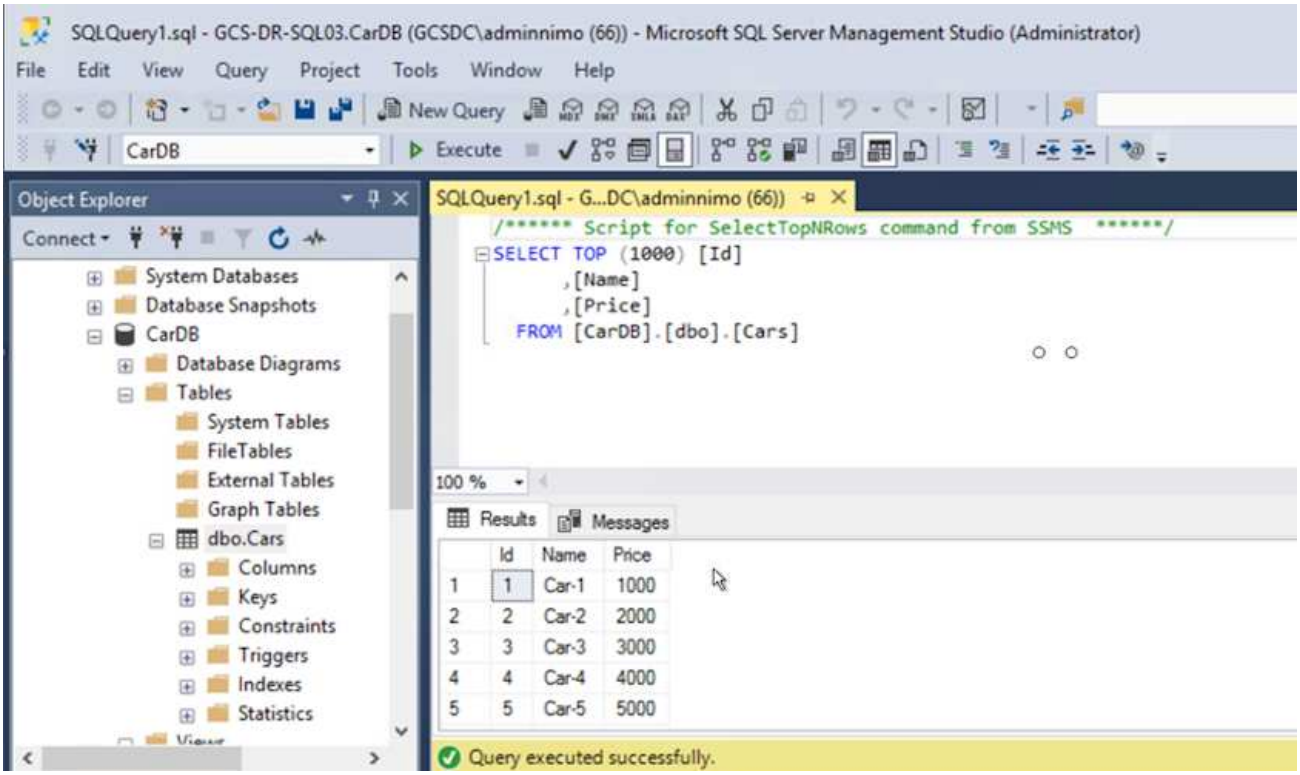
9. Certifique-se de que todos os discos estejam conectados usando as mesmas letras de unidade que eram usadas antes do DR.



10. Reinicie o serviço do servidor MSSQL.



11. Certifique-se de que os recursos SQL estejam online novamente.



No caso do NFS, anexe os volumes usando o comando mount e atualize o `/etc/fstab` entradas.

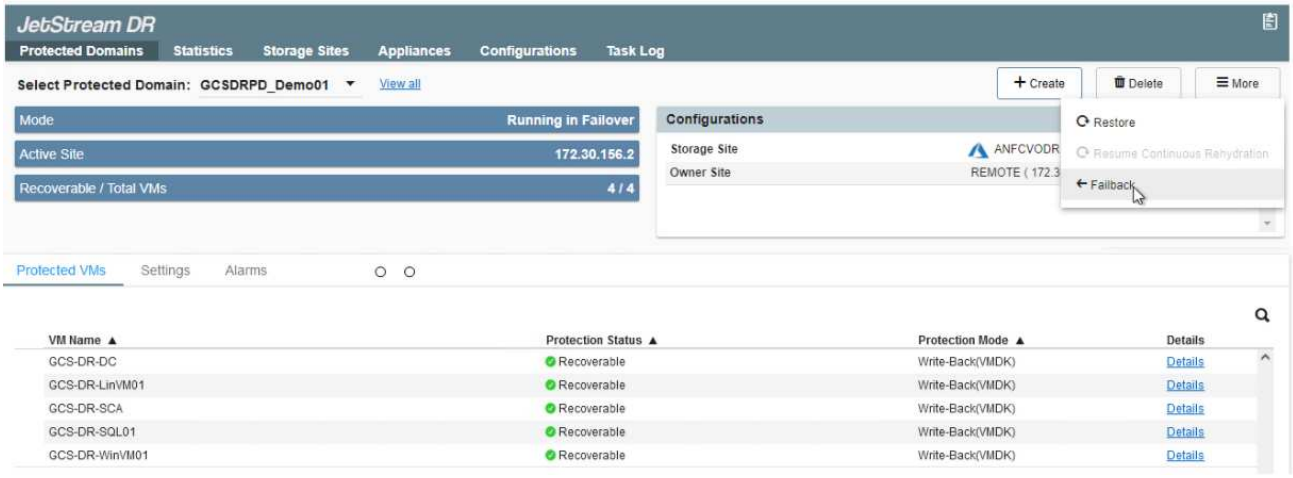
Neste ponto, as operações podem ser executadas e os negócios continuam normalmente.

No final do NSX-T, um gateway de nível 1 dedicado separado pode ser criado para simular cenários de failover. Isso garante que todas as cargas de trabalho possam se comunicar entre si, mas que nenhum tráfego possa entrar ou sair do ambiente, de modo que qualquer tarefa de triagem, contenção ou proteção possa ser executada sem risco de contaminação cruzada. Esta operação está fora do escopo deste documento, mas pode ser facilmente realizada para simular isolamento.

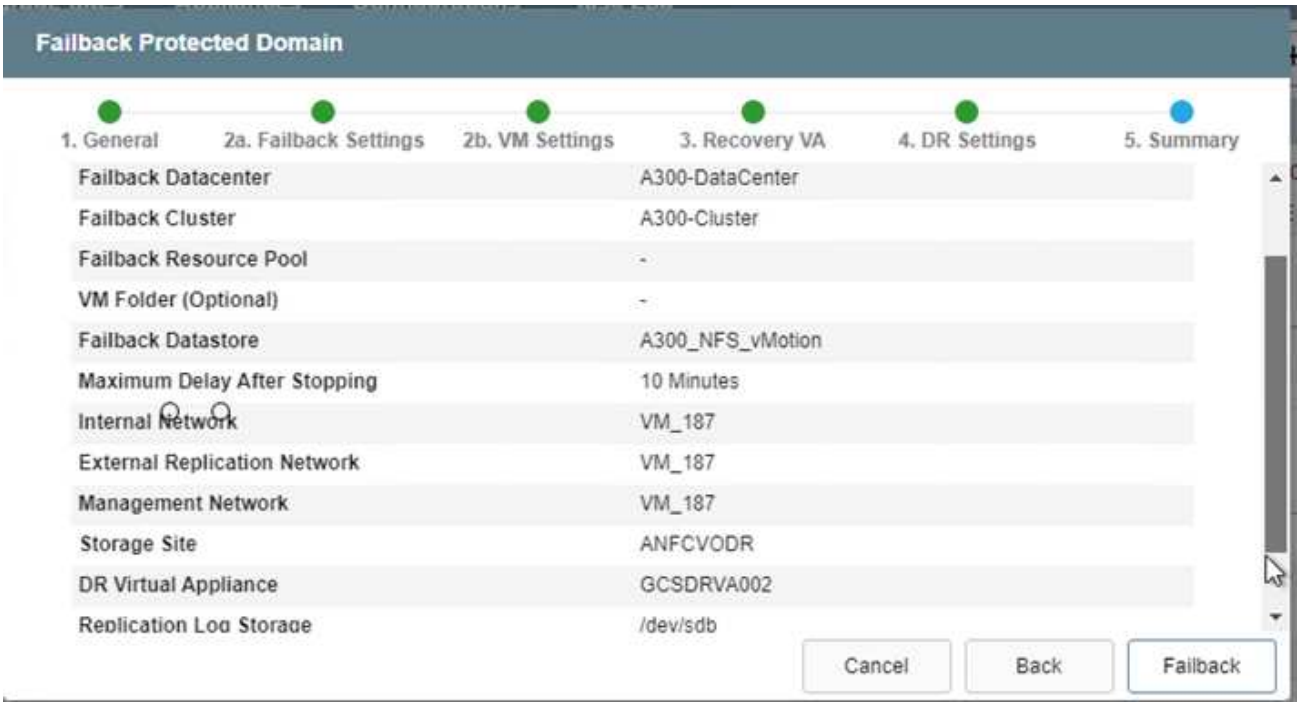
Depois que o site principal estiver funcionando novamente, você poderá executar o failback. A proteção da VM é retomada pelo Jetstream e o relacionamento do SnapMirror deve ser revertido.

1. Restaure o ambiente local. Dependendo do tipo de incidente de desastre, pode ser necessário restaurar e/ou verificar a configuração do cluster protegido. Se necessário, o software JetStream DR pode precisar ser reinstalado.
2. Acesse o ambiente local restaurado, vá para a interface do usuário do Jetstream DR e selecione o domínio protegido apropriado. Depois que o site protegido estiver pronto para failback, selecione a opção Failback na interface do usuário.

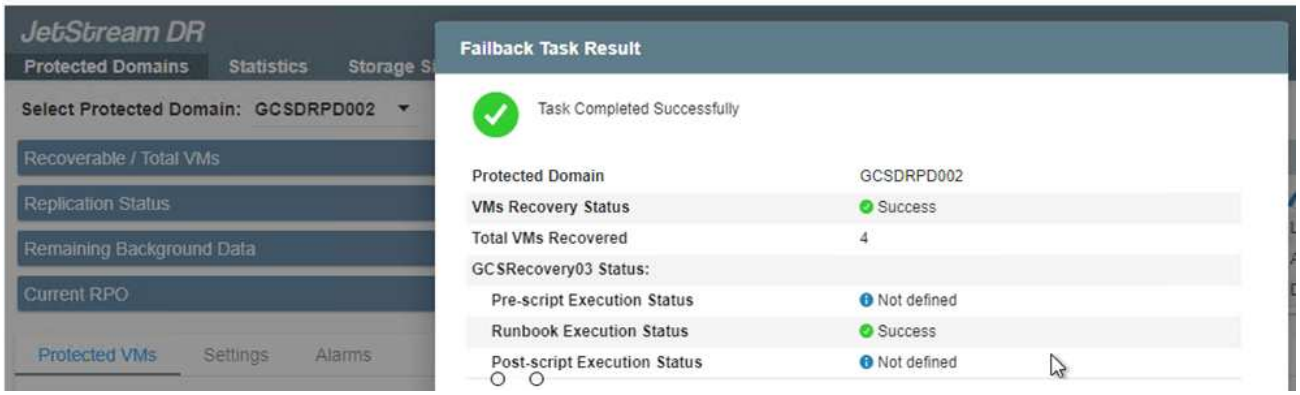
O plano de failback gerado pelo CPT também pode ser usado para iniciar o retorno das VMs e seus dados do armazenamento de objetos para o ambiente VMware original.



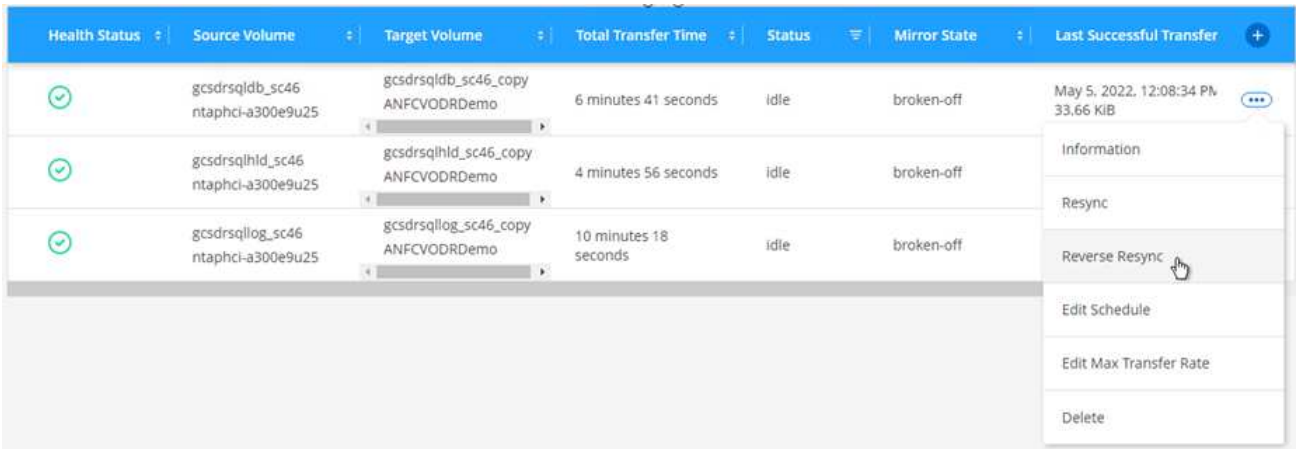
Especifique o atraso máximo após pausar as VMs no site de recuperação e reiniciá-las no site protegido. O tempo necessário para concluir esse processo inclui a conclusão da replicação após interromper as VMs de failover, o tempo necessário para limpar o site de recuperação e o tempo necessário para recriar as VMs no site protegido. A NetApp recomenda 10 minutos.

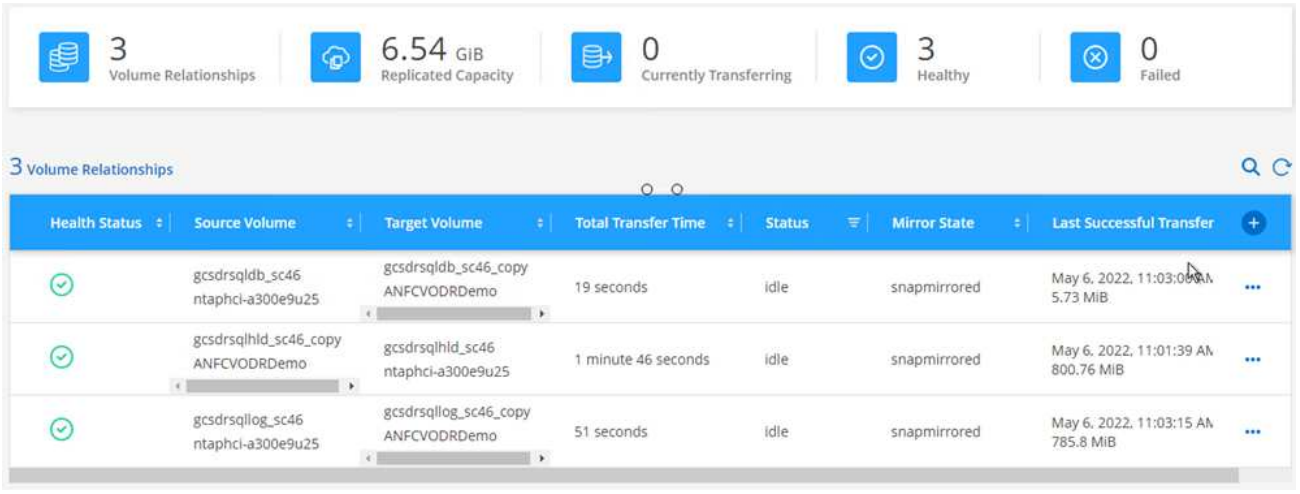


3. Conclua o processo de failback e confirme a retomada da proteção da VM e da consistência dos dados.

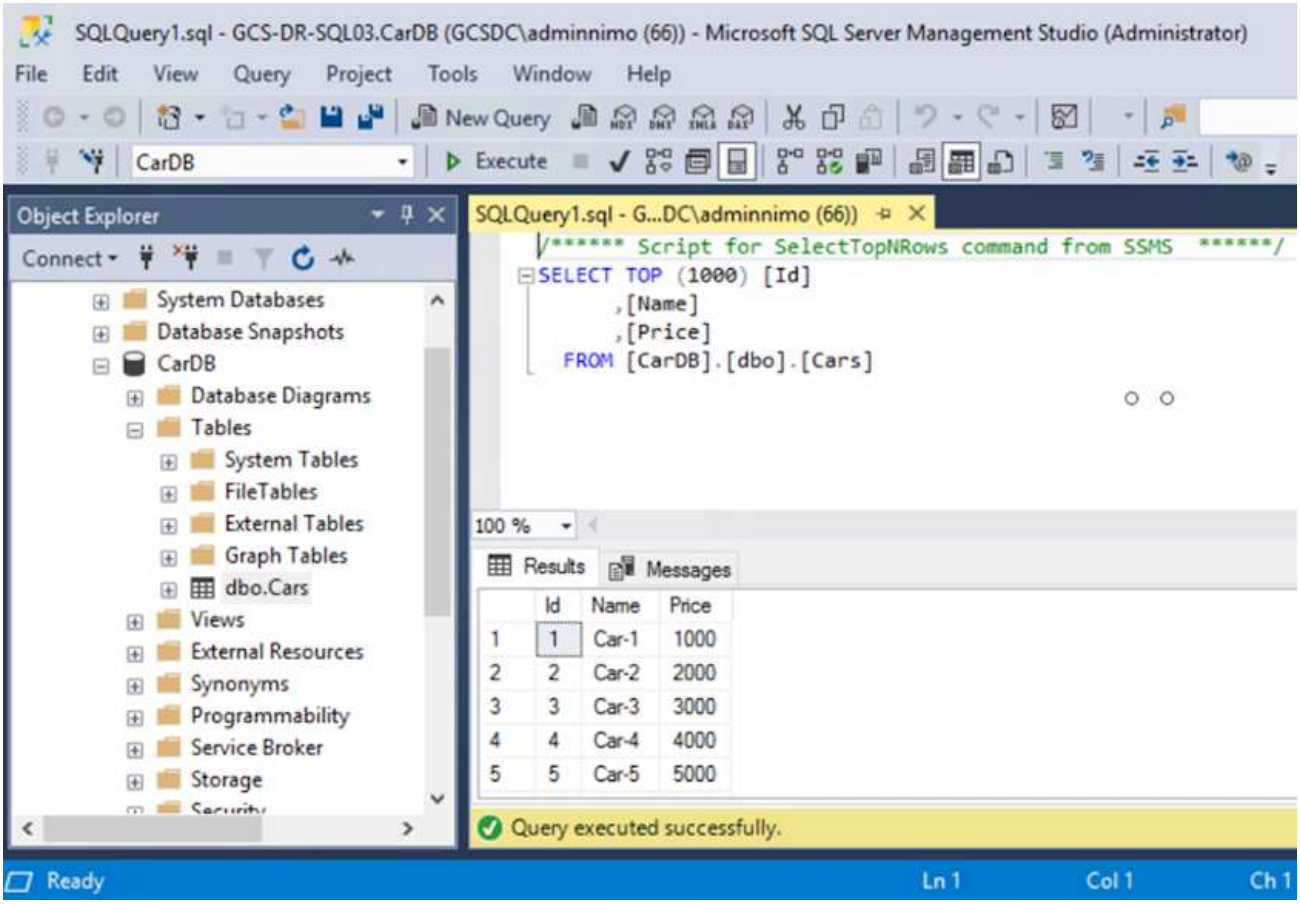


4. Depois que as VMs forem recuperadas, desconecte o armazenamento secundário do host e conecte-o ao armazenamento primário.





5. Reinicie o serviço do servidor MSSQL.
6. Verifique se os recursos SQL estão online novamente.



Para fazer failback para o armazenamento primário, certifique-se de que a direção do relacionamento permaneça a mesma de antes do failover, executando uma operação de ressincronização reversa.

Para manter as funções de armazenamento primário e secundário após a operação de ressincronização reversa, execute a operação de ressincronização reversa novamente.

Esse processo é aplicável a outros aplicativos como Oracle, bancos de dados semelhantes e quaisquer outros aplicativos que usem armazenamento conectado a convidados.

Como sempre, teste as etapas envolvidas para recuperar as cargas de trabalho críticas antes de portá-las para produção.

Benefícios desta solução

- Utiliza a replicação eficiente e resiliente do SnapMirror.
- Recupera para quaisquer pontos disponíveis no tempo com retenção de instantâneos ONTAP .
- A automação completa está disponível para todas as etapas necessárias para recuperar centenas a milhares de VMs, desde as etapas de armazenamento, computação, rede e validação de aplicativos.
- O SnapCenter usa mecanismos de clonagem que não alteram o volume replicado.
  - Isso evita o risco de corrupção de dados para volumes e instantâneos.
  - Evita interrupções de replicação durante fluxos de trabalho de teste de DR.
  - Aproveita os dados de DR para fluxos de trabalho além de DR, como desenvolvimento/teste, testes de

segurança, testes de patch e atualização e testes de remediação.

- A otimização da CPU e da RAM pode ajudar a reduzir os custos da nuvem ao permitir a recuperação para clusters de computação menores.

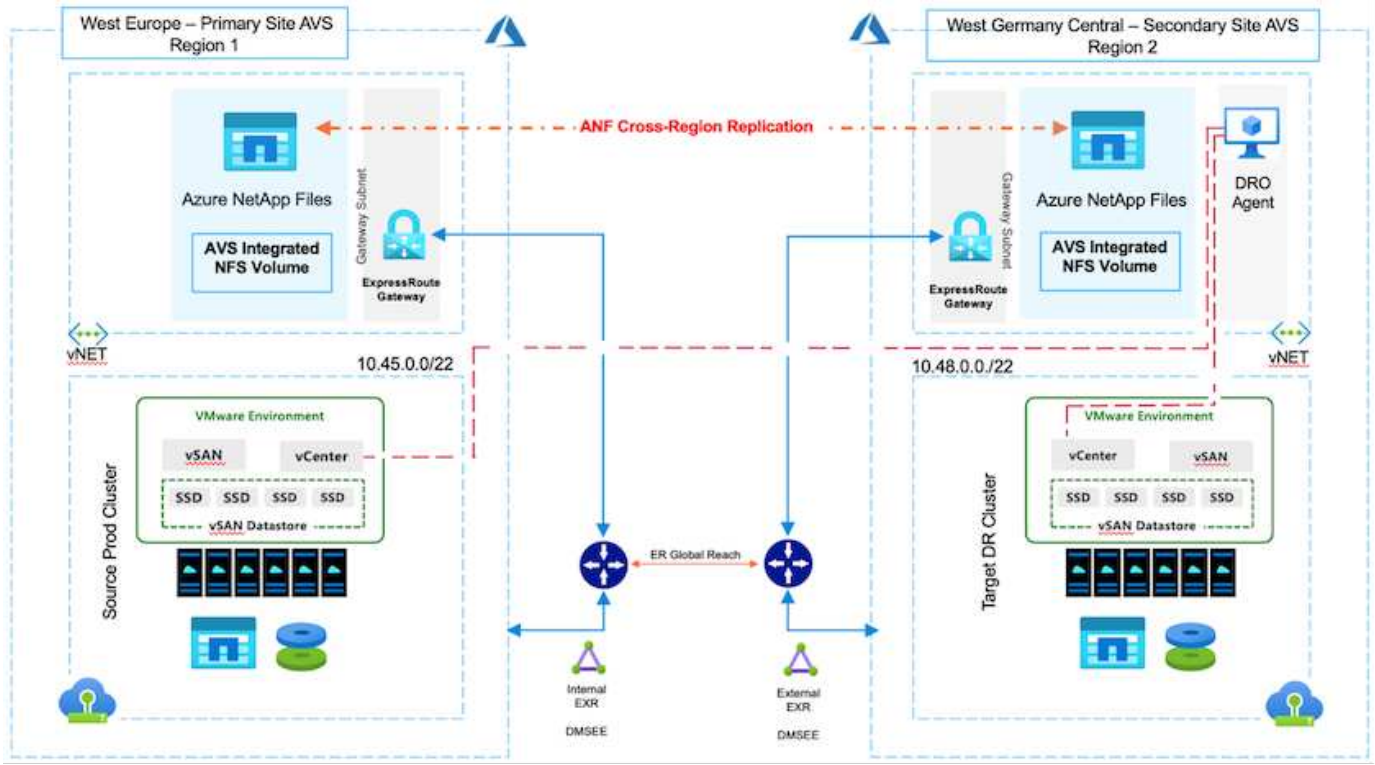
TR-4955: Recuperação de desastres com Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

A recuperação de desastres usando replicação em nível de bloco entre regiões dentro da nuvem é uma maneira resiliente e econômica de proteger as cargas de trabalho contra interrupções do site e eventos de corrupção de dados (por exemplo, ransomware).

Visão geral

Com a replicação de volume entre regiões do Azure NetApp Files (ANF), as cargas de trabalho do VMware em execução em um site SDDC do Azure VMware Solution (AVS) usando volumes do Azure NetApp Files como um armazenamento de dados NFS no site AVS principal podem ser replicadas para um site AVS secundário designado na região de recuperação de destino.

O Disaster Recovery Orchestrator (DRO) (uma solução com script e uma interface de usuário) pode ser usado para recuperar perfeitamente cargas de trabalho replicadas de um AVS SDDC para outro. O DRO automatiza a recuperação interrompendo o peering de replicação e, em seguida, montando o volume de destino como um armazenamento de dados, por meio do registro de VM no AVS, para mapeamentos de rede diretamente no NSX-T (incluído em todas as nuvens privadas do AVS).



Pré-requisitos e recomendações gerais

- Verifique se você habilitou a replicação entre regiões criando o peering de replicação. Ver "Criar replicação de volume para o Azure NetApp Files" .
- Você deve configurar o ExpressRoute Global Reach entre as nuvens privadas de origem e de destino do Azure VMware Solution.

- Você deve ter uma entidade de serviço que possa acessar recursos.
- A seguinte topologia é suportada: site AVS primário para site AVS secundário.
- Configurar o "replicação" programe cada volume adequadamente com base nas necessidades do negócio e na taxa de alteração de dados.

Topologias em cascata e fan-in e fan-out não são suportadas.

Começando

Implantar a solução Azure VMware

O "Solução VMware do Azure" (AVS) é um serviço de nuvem híbrida que fornece SDDCs VMware totalmente funcionais dentro de uma nuvem pública do Microsoft Azure. O AVS é uma solução própria totalmente gerenciada e suportada pela Microsoft e verificada pela VMware que usa a infraestrutura do Azure. Portanto, os clientes obtêm o VMware ESXi para virtualização de computação, o vSAN para armazenamento hiperconvergente e o NSX para rede e segurança, tudo isso aproveitando a presença global do Microsoft Azure, as instalações de data center líderes da categoria e a proximidade com o rico ecossistema de serviços e soluções nativos do Azure. Uma combinação do Azure VMware Solution SDDC e do Azure NetApp Files proporciona o melhor desempenho com latência de rede mínima.

Para configurar uma nuvem privada AVS no Azure, siga as etapas neste"link" para documentação da NetApp e neste "link" para documentação da Microsoft. Um ambiente de luz piloto configurado com uma configuração mínima pode ser usado para fins de DR. Esta configuração contém apenas componentes principais para dar suporte a aplicativos críticos e pode ser dimensionada e gerar mais hosts para assumir a maior parte da carga se ocorrer um failover.

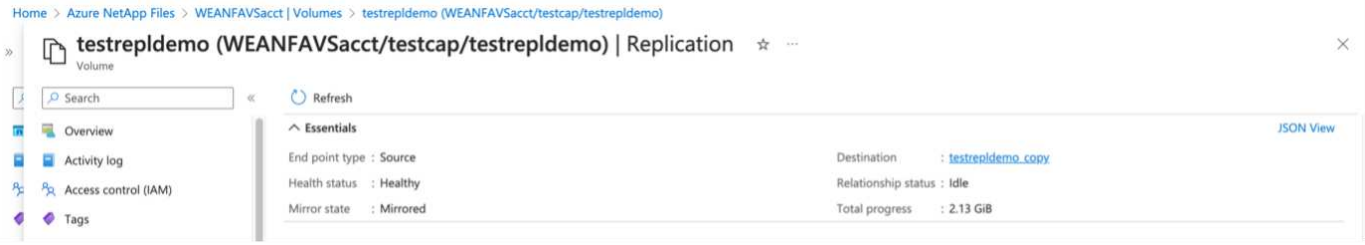
Na versão inicial, o DRO oferece suporte a um cluster AVS SDDC existente. A criação de SDDC sob demanda estará disponível em uma próxima versão.

Provisionar e configurar o Azure NetApp Files

"Azure NetApp Files"é um serviço de armazenamento de arquivos medido, de alto desempenho e de nível empresarial. Siga os passos deste "link" para provisionar e configurar o Azure NetApp Files como um armazenamento de dados NFS para otimizar implantações de nuvem privada do AVS.

Criar replicação de volume para volumes de armazenamento de dados com tecnologia Azure NetApp Files

A primeira etapa é configurar a replicação entre regiões para os volumes de armazenamento de dados desejados do site primário do AVS para o site secundário do AVS com as frequências e retenções apropriadas.



Siga os passos deste "link" para configurar a replicação entre regiões criando peering de replicação. O nível de serviço do pool de capacidade de destino pode corresponder ao do pool de capacidade de origem. No

entanto, para este caso de uso específico, você pode selecionar o nível de serviço padrão e então "modificar o nível de serviço" no caso de um desastre real ou simulações de DR.

> Um relacionamento de replicação entre regiões é um pré-requisito e deve ser criado previamente.

Instalação DRO

Para começar a usar o DRO, use o sistema operacional Ubuntu na máquina virtual do Azure designada e certifique-se de atender aos pré-requisitos. Em seguida, instale o pacote.

Pré-requisitos:

- Principal de serviço que pode acessar recursos.
- Certifique-se de que haja conectividade apropriada com as instâncias de origem e destino do SDDC e do Azure NetApp Files .
- A resolução de DNS deve estar em vigor se você estiver usando nomes DNS. Caso contrário, use endereços IP para o vCenter.

Requisitos do sistema operacional:

- Ubuntu Focal 20.04 (LTS)Os seguintes pacotes devem ser instalados na máquina virtual do agente designado:
- Docker
- Docker- compose
- JqChange `docker.sock` para esta nova permissão: `sudo chmod 666 /var/run/docker.sock` .

> O `deploy.sh` O script executa todos os pré-requisitos necessários.

Os passos são os seguintes:

1. Baixe o pacote de instalação na máquina virtual designada:

```
git clone https://github.com/NetApp/DRO-Azure.git
```

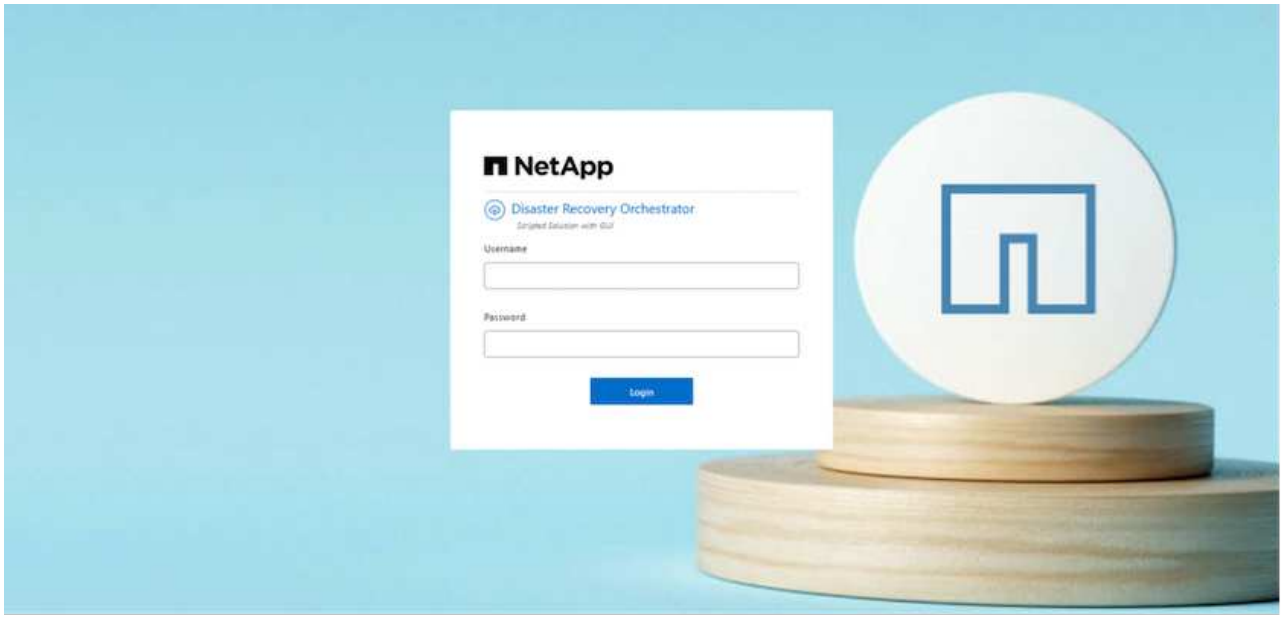
> O agente deve ser instalado na região do site AVS secundário ou na região do site AVS primário em uma AZ separada do SDDC.

2. Descompacte o pacote, execute o script de implantação e insira o IP do host (por exemplo, `10.10.10.10`).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Acesse a interface do usuário usando as seguintes credenciais:

- Nome de usuário: `admin`
- Senha: `admin`



Configuração DRO

Depois que o Azure NetApp Files e o AVS forem configurados corretamente, você poderá começar a configurar o DRO para automatizar a recuperação de cargas de trabalho do site AVS principal para o site AVS secundário. A NetApp recomenda implantar o agente DRO no site AVS secundário e configurar a conexão do gateway ExpressRoute para que o agente DRO possa se comunicar pela rede com os componentes AVS e Azure NetApp Files apropriados.

O primeiro passo é adicionar credenciais. O DRO requer permissão para descobrir o Azure NetApp Files e a Azure VMware Solution. Você pode conceder as permissões necessárias a uma conta do Azure criando e configurando um aplicativo do Azure Active Directory (AD) e obtendo as credenciais do Azure necessárias para o DRO. Você deve vincular a entidade de serviço à sua assinatura do Azure e atribuir a ela uma função personalizada que tenha as permissões necessárias relevantes. Ao adicionar ambientes de origem e destino, você será solicitado a selecionar as credenciais associadas à entidade de serviço. Você precisa adicionar essas credenciais ao DRO antes de clicar em Adicionar novo site.

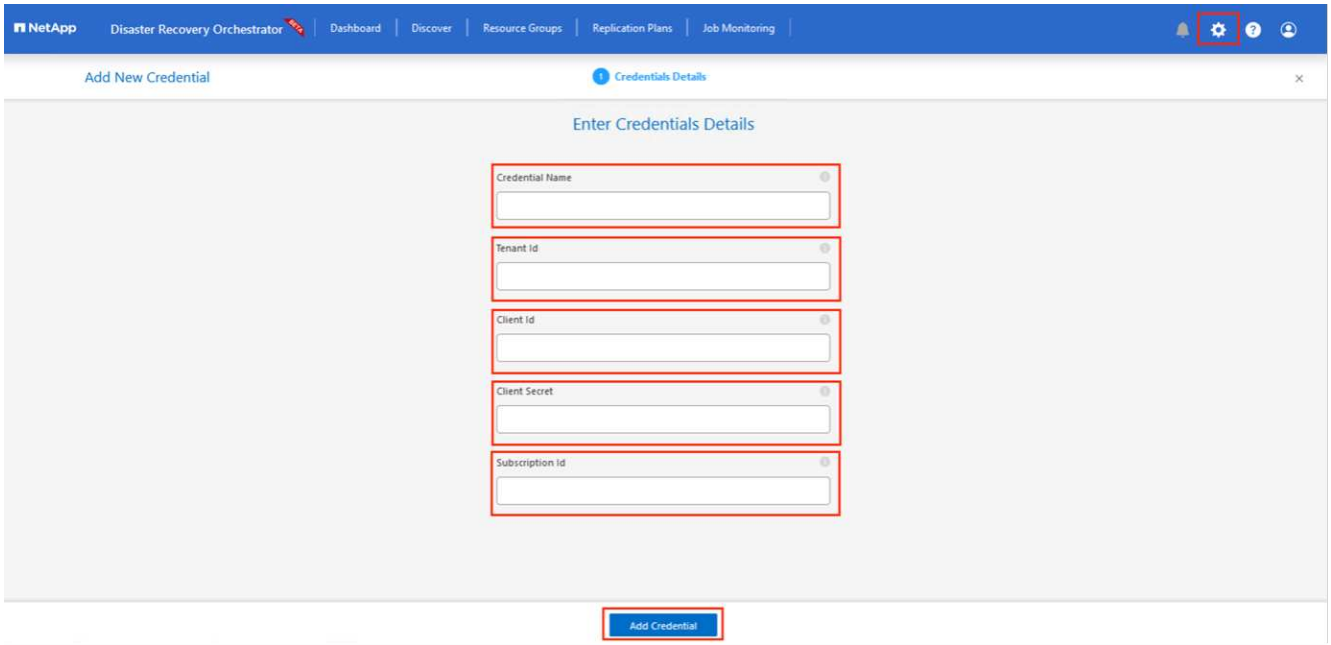
Para executar esta operação, siga os seguintes passos:

1. Abra o DRO em um navegador compatível e use o nome de usuário e a senha padrão/`admin`/`admin`). A senha pode ser redefinida após o primeiro login usando a opção Alterar senha.
2. No canto superior direito do console do DRO, clique no ícone **Configurações** e selecione **Credenciais**.
3. Clique em Adicionar nova credencial e siga as etapas do assistente.
4. Para definir as credenciais, insira informações sobre a entidade de serviço do Azure Active Directory que concede as permissões necessárias:
   - Nome da credencial
   - ID do inquilino
   - ID do cliente
   - Segredo do cliente

- ID da assinatura

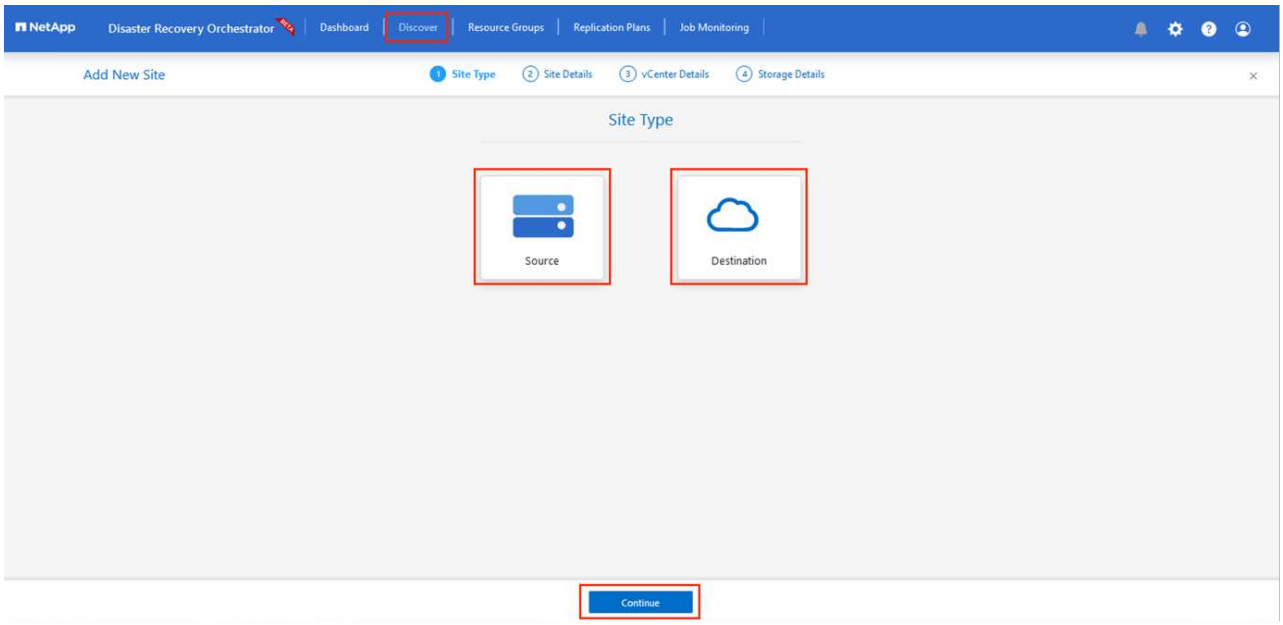
  Você deveria ter capturado essas informações ao criar o aplicativo AD.

5. Confirme os detalhes sobre as novas credenciais e clique em Adicionar credencial.



Depois de adicionar as credenciais, é hora de descobrir e adicionar os sites AVS primário e secundário (vCenter e a conta de armazenamento de arquivos do Azure NetApp) ao DRO. Para adicionar o site de origem e de destino, conclua as seguintes etapas:

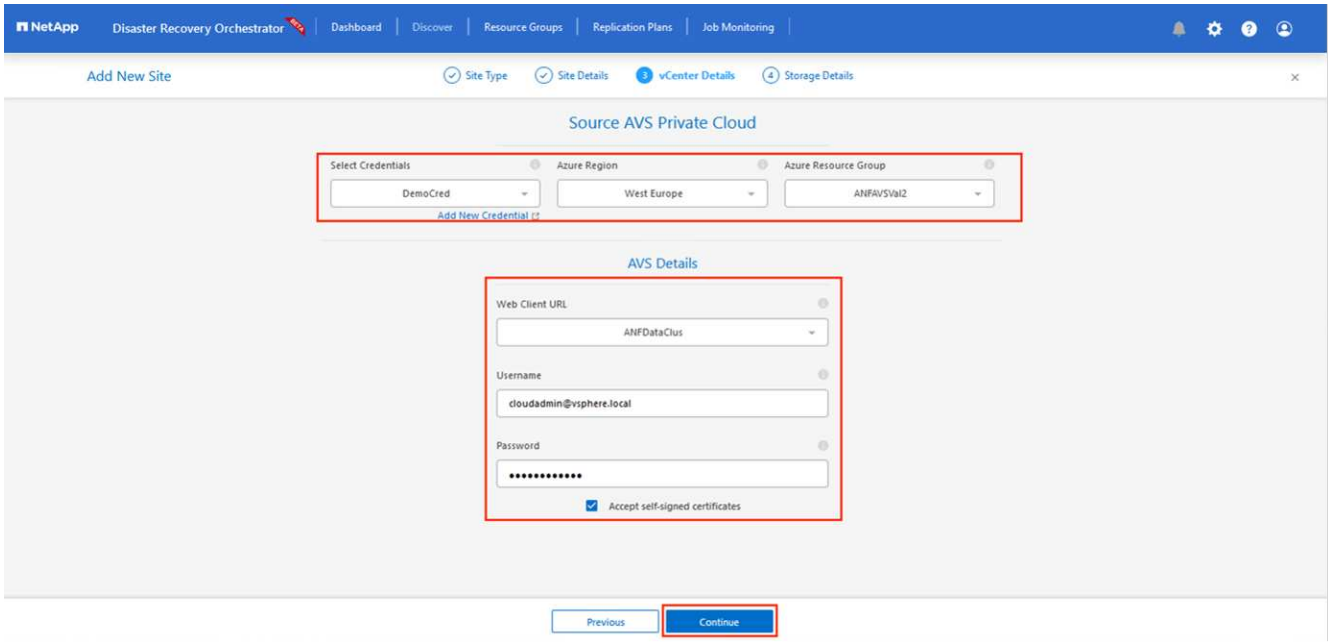
6. Acesse a aba **Descobrir**.
7. Clique em **Adicionar novo site**.
8. Adicione o seguinte site AVS primário (designado como **Fonte** no console).
   - SDDC vCenter
   - Conta de armazenamento do Azure NetApp Files
9. Adicione o seguinte site AVS secundário (designado como **Destino** no console).
   - SDDC vCenter
   - Conta de armazenamento do Azure NetApp Files



10. Adicione detalhes do site clicando em **Fonte**, inserindo um nome de site amigável e selecionando o conector. Em seguida, clique em **Continuar**.

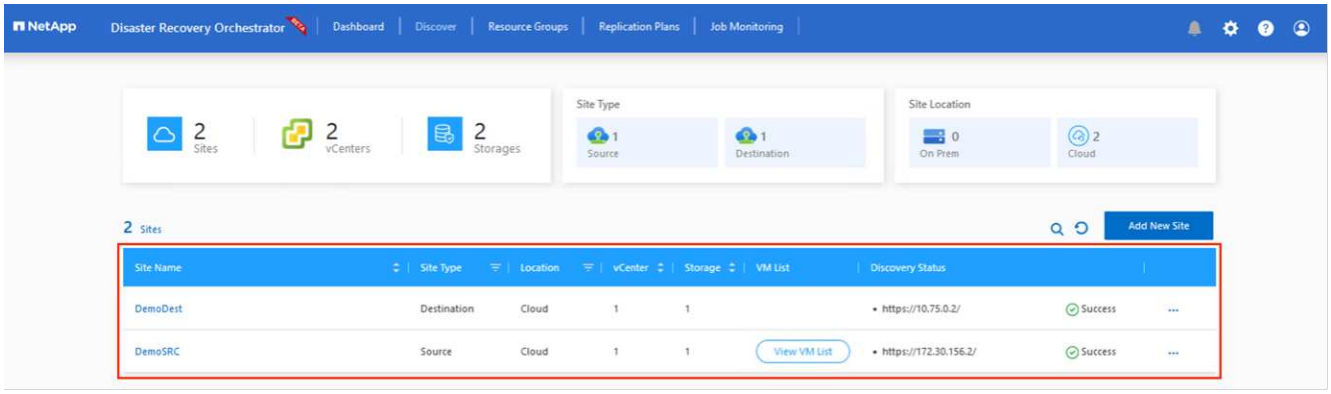
> Para fins de demonstração, a adição de um site de origem é abordada neste documento.

11. Atualize os detalhes do vCenter. Para fazer isso, selecione as credenciais, a região do Azure e o grupo de recursos no menu suspenso do SDDC do AVS principal.
12. O DRO lista todos os SDDCs disponíveis na região. Selecione a URL da nuvem privada designada no menu suspenso.
13. Entre no `cloudadmin@vsphere.local` credenciais do usuário. Isso pode ser acessado no Portal do Azure. Siga os passos mencionados neste "link" . Quando terminar, clique em **Continuar**.

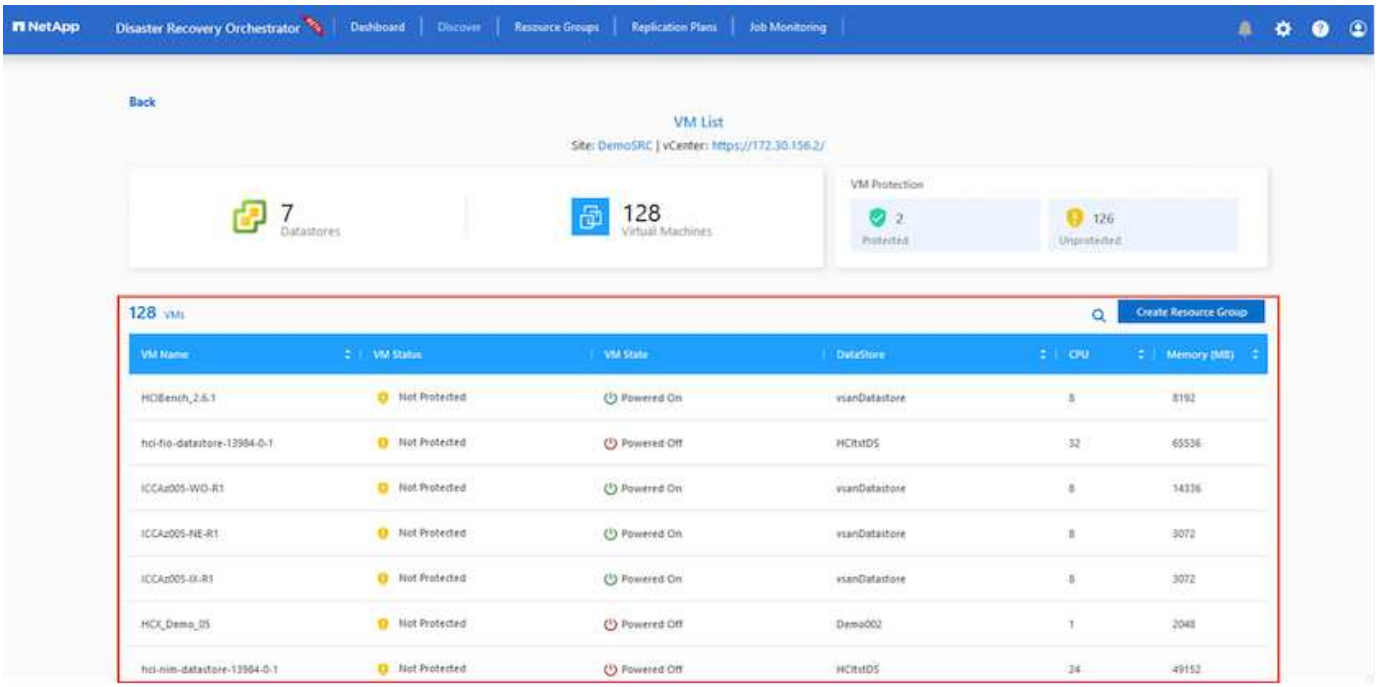


14. Selecione os detalhes do Source Storage (ANF) selecionando o grupo de recursos do Azure e a conta do NetApp .

15. Clique em **Criar site**.



Uma vez adicionado, o DRO executa a descoberta automática e exibe as VMs que têm réplicas entre regiões correspondentes do site de origem para o site de destino. O DRO detecta automaticamente as redes e os segmentos usados pelas VMs e os preenche.



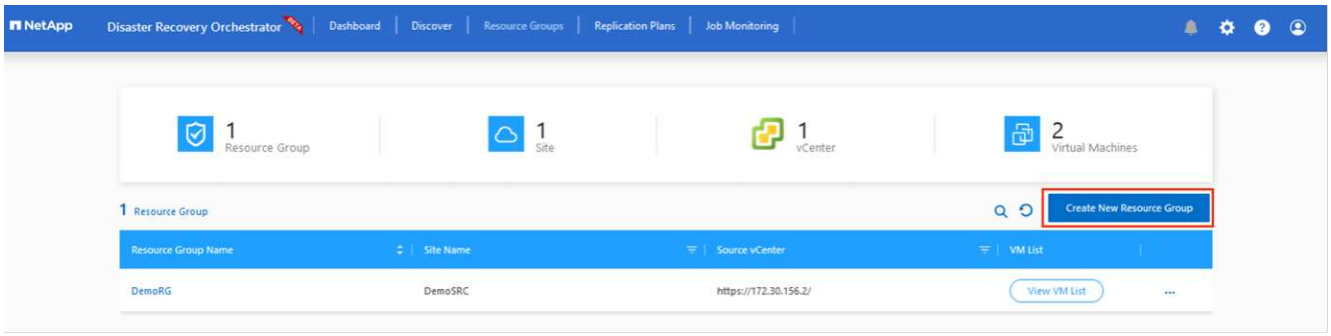
A próxima etapa é agrupar as VMs necessárias em seus grupos funcionais como grupos de recursos.

Agrupamentos de recursos

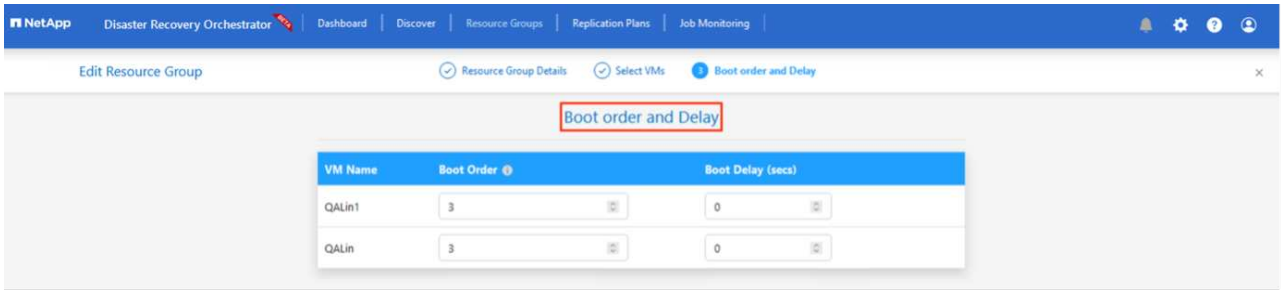
Depois que as plataformas forem adicionadas, agrupe as VMs que você deseja recuperar em grupos de recursos. Os grupos de recursos de DRO permitem que você agrupe um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização, atrasos de inicialização e validações de aplicativos opcionais que podem ser executadas na recuperação.

Para começar a criar grupos de recursos, clique no item de menu **Criar novo grupo de recursos**.

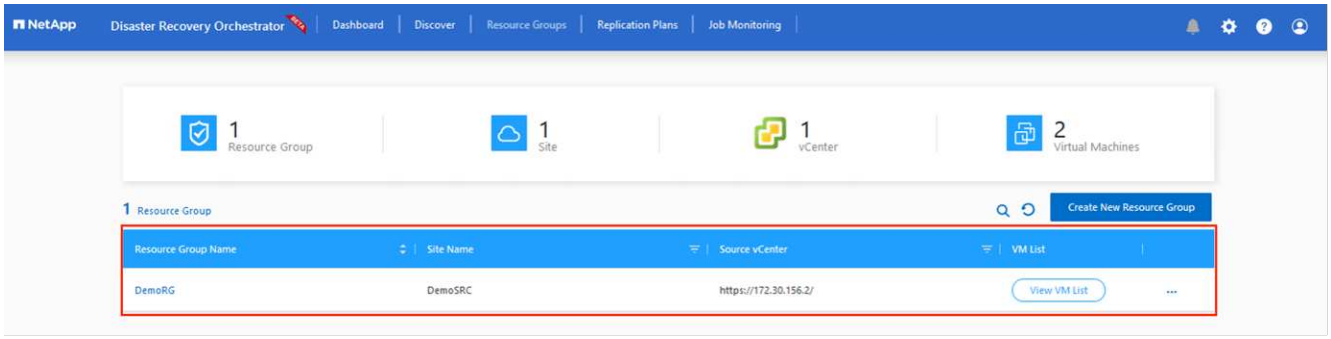
1. Acesse **Grupos de Recursos** e clique em **Criar Novo Grupo de Recursos**.



2. Em Novo grupo de recursos, selecione o site de origem no menu suspenso e clique em **Criar**.
3. Forneça os detalhes do grupo de recursos e clique em **Continuar**.
4. Selecione as VMs apropriadas usando a opção de pesquisa.
5. Selecione a **Ordem de inicialização** e o **Atraso de inicialização** (segs) para todas as VMs selecionadas. Defina a ordem da sequência de inicialização selecionando cada máquina virtual e definindo a prioridade para ela. O valor padrão para todas as máquinas virtuais é 3. As opções são as seguintes:
   - A primeira máquina virtual a ligar
   - Padrão
   - A última máquina virtual a ser ligada



6. Clique em **Criar grupo de recursos**.

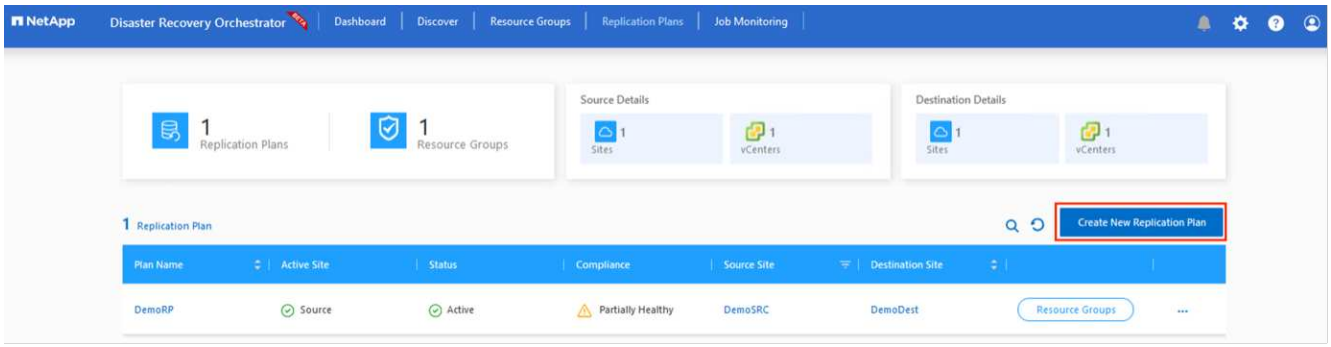


Planos de replicação

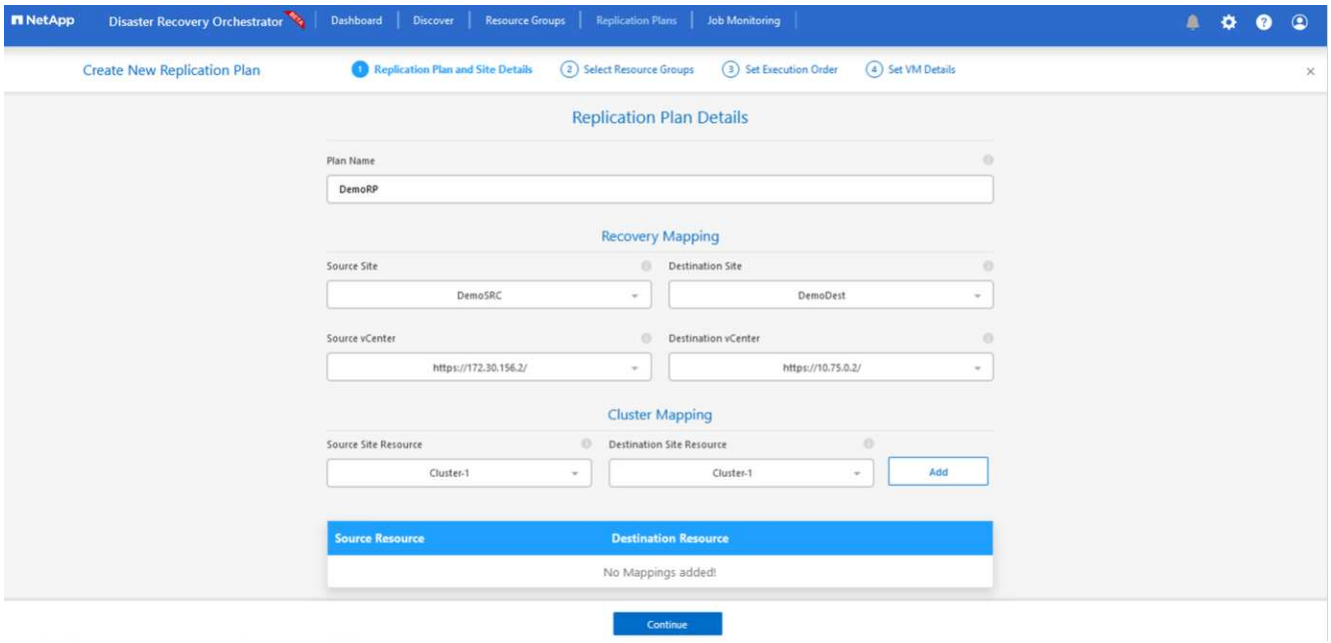
Você deve ter um plano para recuperar aplicativos em caso de desastre. Selecione as plataformas vCenter de origem e destino no menu suspenso, escolha os grupos de recursos a serem incluídos neste plano e inclua também o agrupamento de como os aplicativos devem ser restaurados e ligados (por exemplo, controladores de domínio, nível 1, nível 2 e assim por diante). Os planos também são frequentemente chamados de projetos. Para definir o plano de recuperação, navegue até a guia Plano de Replicação e clique em **Novo Plano de Replicação**.

Para começar a criar um plano de replicação, conclua as seguintes etapas:

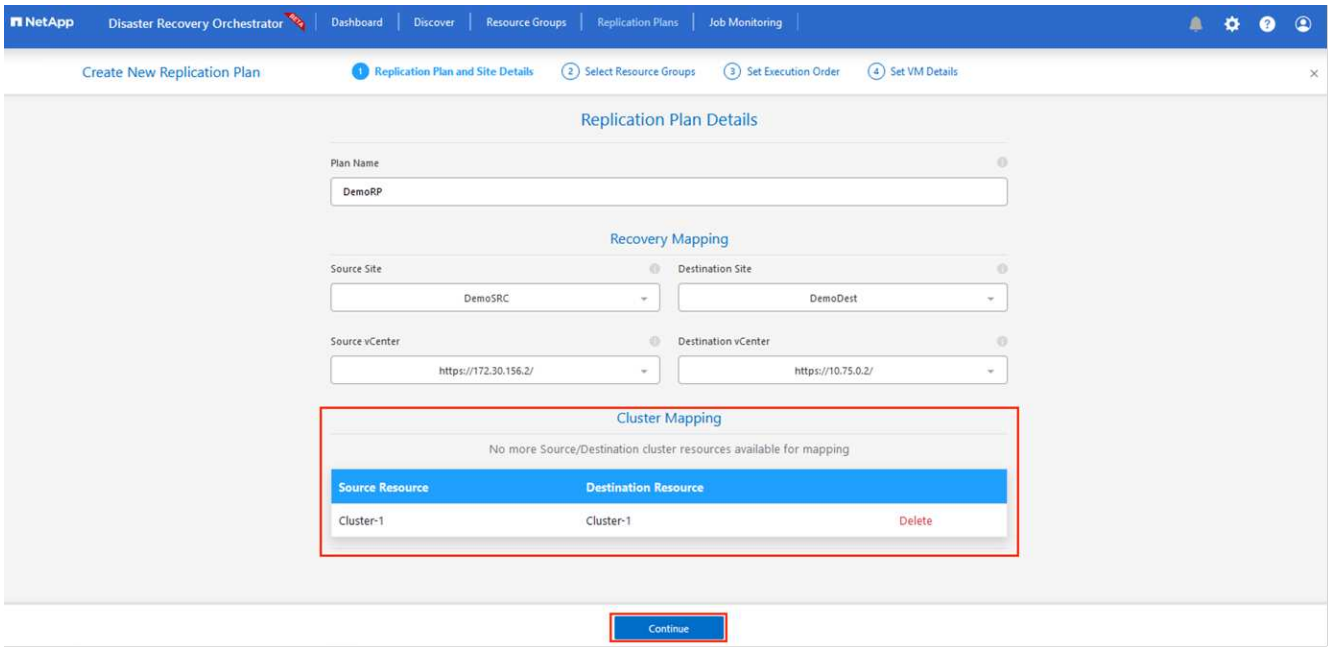
1. Navegue até **Planos de Replicação** e clique em **Criar Novo Plano de Replicação**.



2. No **Novo Plano de Replicação**, forneça um nome para o plano e adicione mapeamentos de recuperação selecionando o Site de Origem, o vCenter associado, o Site de Destino e o vCenter associado.

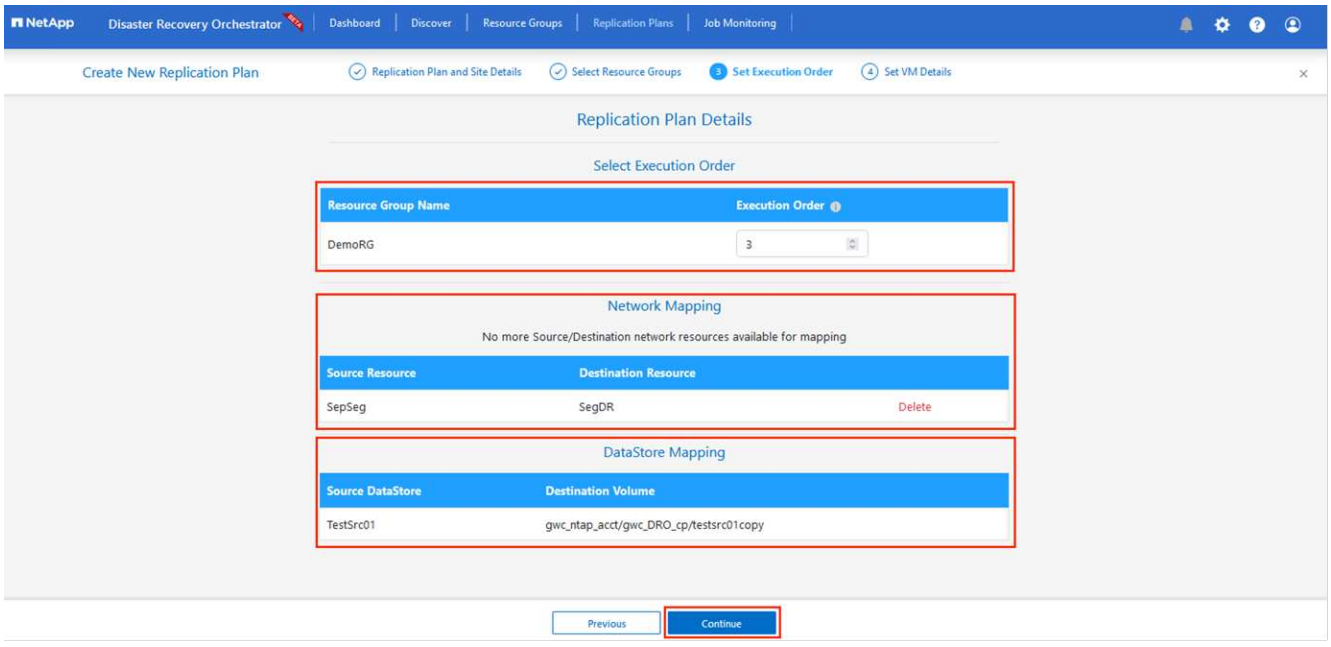


3. Após a conclusão do mapeamento de recuperação, selecione **Mapeamento de Cluster**.

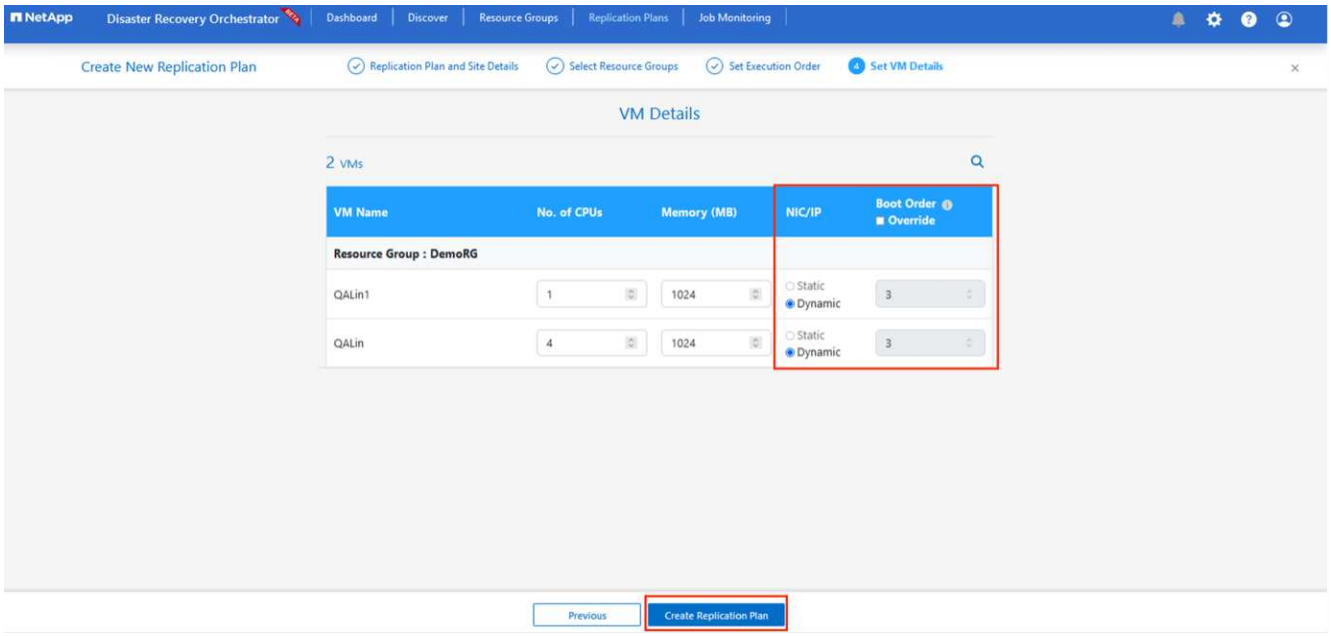


4. Selecione **Detalhes do grupo de recursos** e clique em **Continuar**.
5. Defina a ordem de execução para o grupo de recursos. Esta opção permite que você selecione a sequência de operações quando existem vários grupos de recursos.
6. Uma vez feito isso, defina o mapeamento de rede para o segmento apropriado. Os segmentos já devem estar provisionados no cluster AVS secundário e, para mapear as VMs para eles, selecione o segmento apropriado.
7. Os mapeamentos de armazenamento de dados são selecionados automaticamente com base na seleção de VMs.

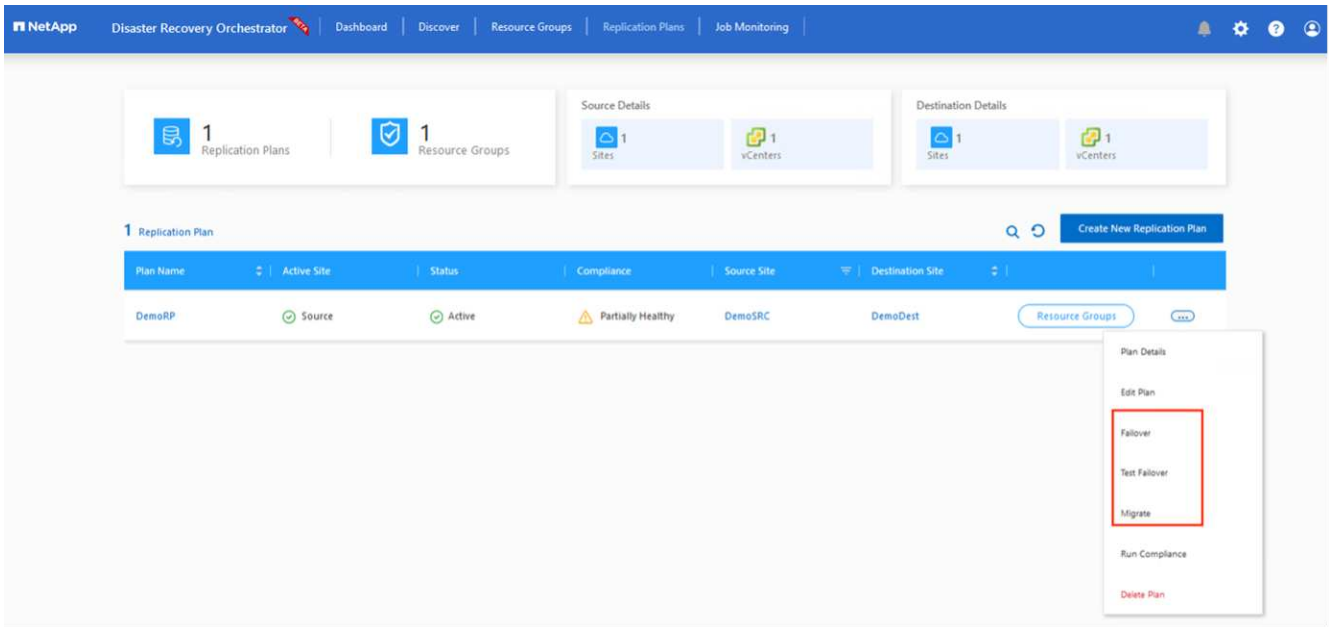
> A replicação entre regiões (CRR) ocorre no nível de volume. Portanto, todas as VMs que residem no respectivo volume são replicadas para o destino CRR. Certifique-se de selecionar todas as VMs que fazem parte do armazenamento de dados, porque somente as máquinas virtuais que fazem parte do plano de replicação são processadas.



8. Em detalhes da VM, você pode redimensionar opcionalmente os parâmetros de CPU e RAM da VM. Isso pode ser muito útil quando você estiver recuperando grandes ambientes para clusters de destino menores ou quando estiver conduzindo testes de DR sem precisar provisionar uma infraestrutura física VMware individual. Além disso, modifique a ordem de inicialização e o atraso de inicialização (seg.) para todas as VMs selecionadas nos grupos de recursos. Há uma opção adicional para modificar a ordem de inicialização caso sejam necessárias alterações em relação ao que você selecionou durante a seleção da ordem de inicialização do grupo de recursos. Por padrão, a ordem de inicialização selecionada durante a seleção do grupo de recursos é usada, no entanto, quaisquer modificações podem ser realizadas nesta fase.

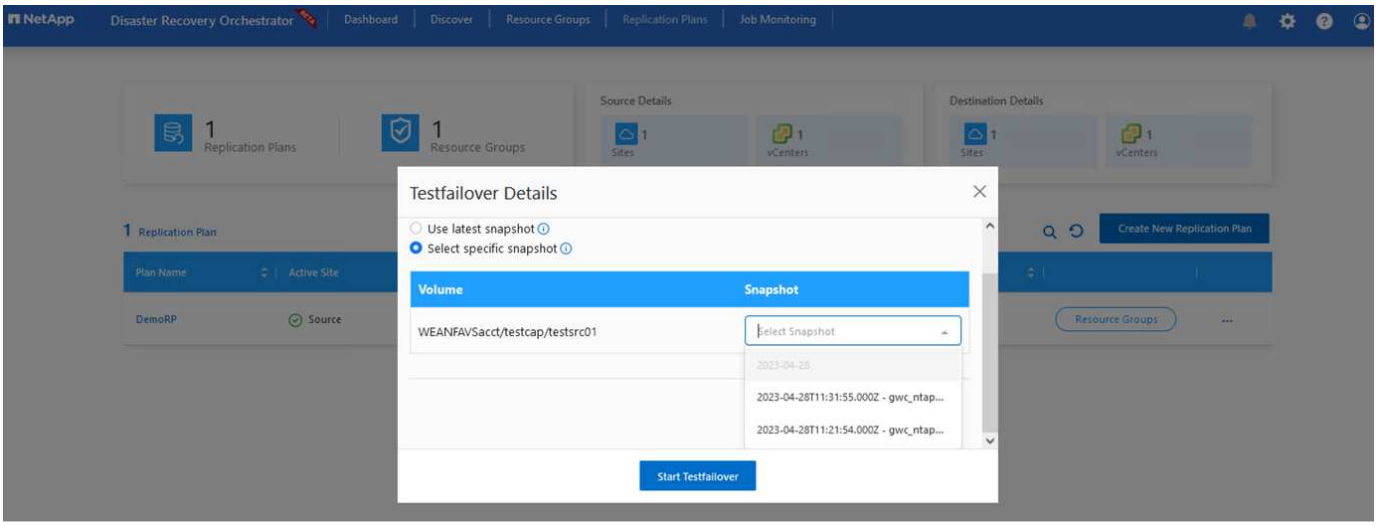


9. Clique em **Criar Plano de Replicação**. Após a criação do plano de replicação, você pode exercer as opções de failover, failover de teste ou migrar, dependendo de suas necessidades.

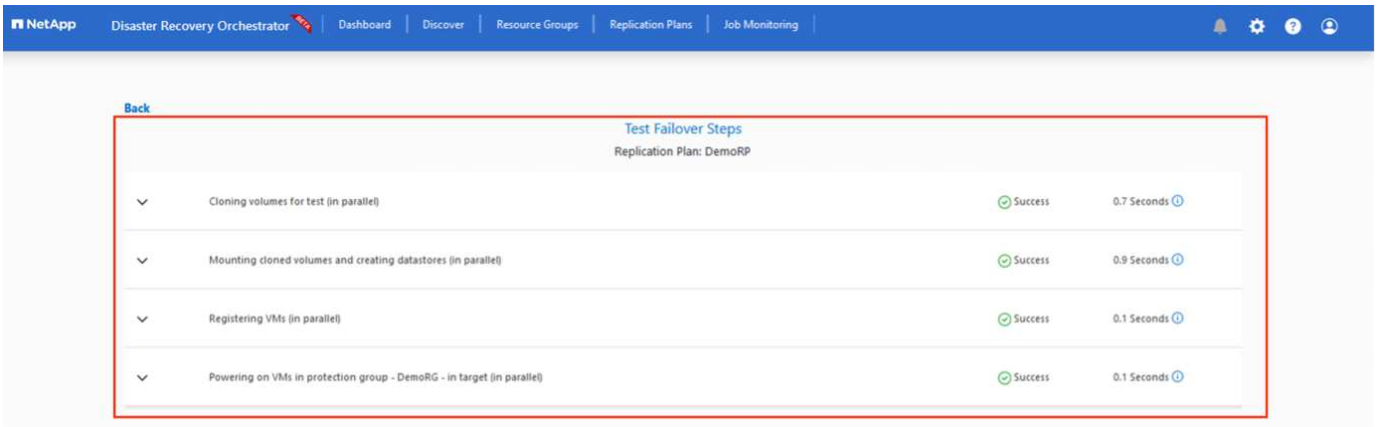


Durante as opções de failover e failover de teste, o snapshot mais recente é usado, ou um snapshot específico pode ser selecionado de um snapshot de momento específico. A opção de ponto no tempo pode ser muito benéfica se você estiver enfrentando um evento de corrupção como um ransomware, em que as

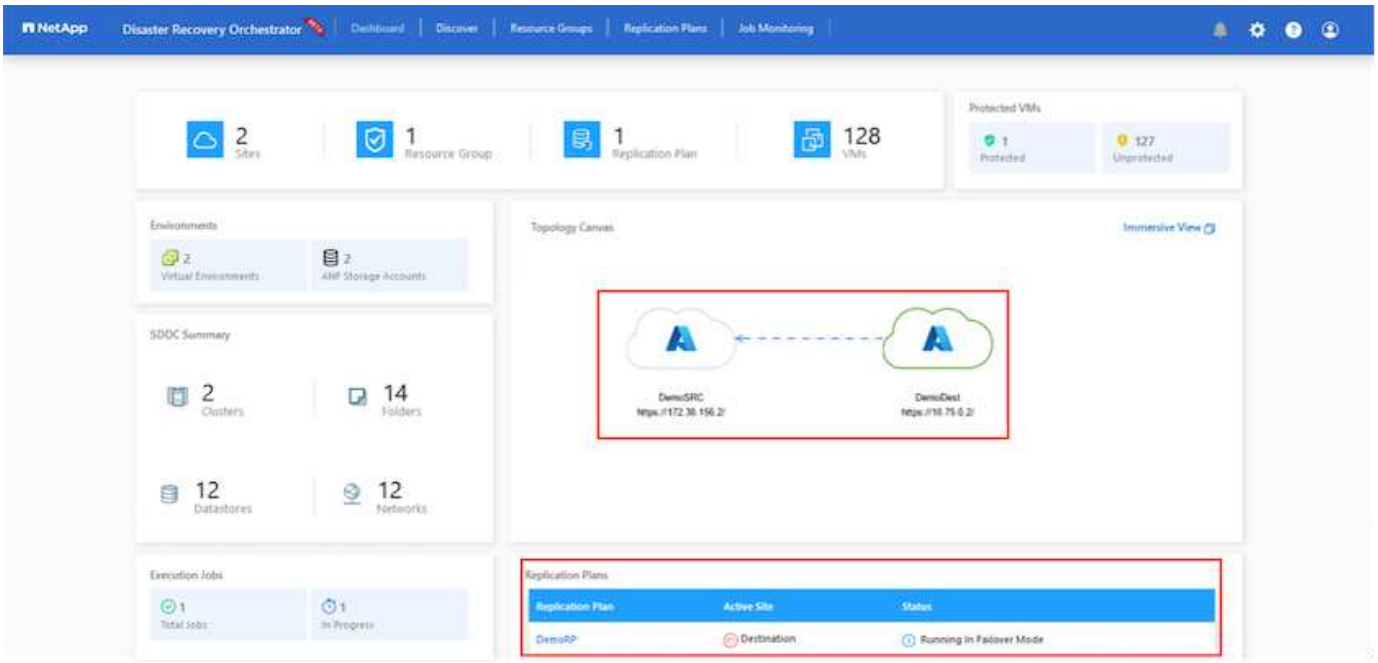
réplicas mais recentes já estão comprometidas ou criptografadas. O DRO mostra todos os pontos de tempo disponíveis.



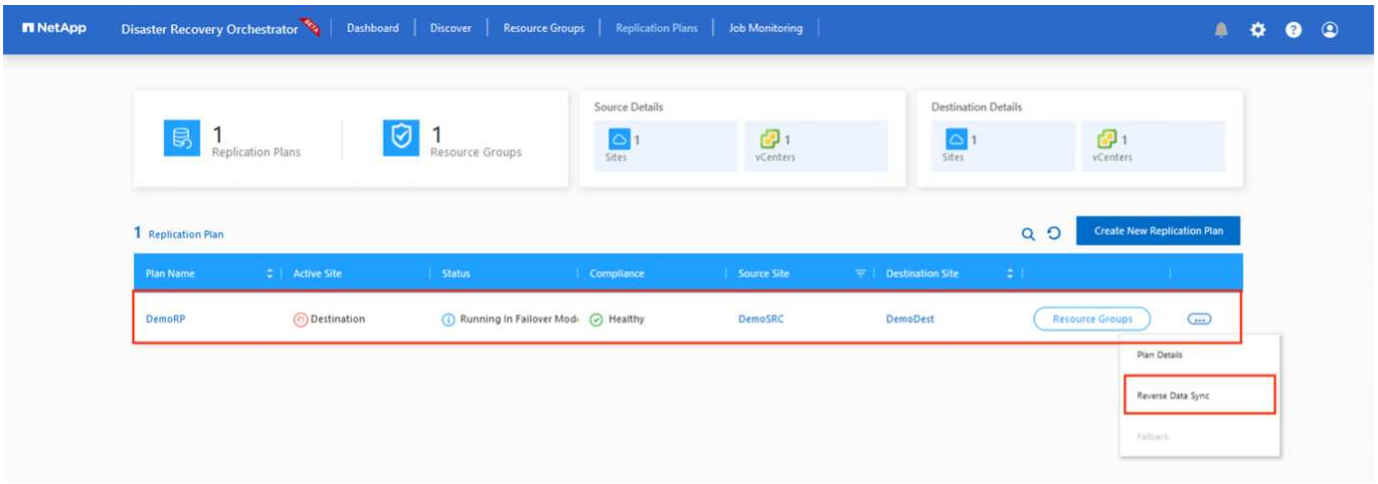
Para acionar o failover ou testar o failover com a configuração especificada no plano de replicação, você pode clicar em **Failover** ou **Testar failover**. Você pode monitorar o plano de replicação no menu de tarefas.



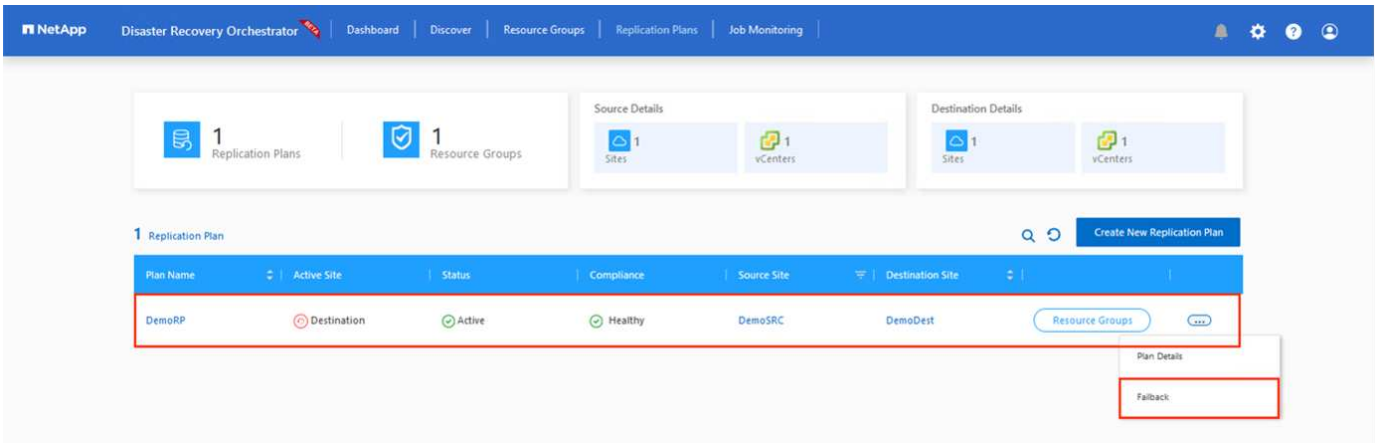
Após o failover ser acionado, os itens recuperados podem ser vistos no site secundário AVS SDDC vCenter (VMs, redes e armazenamentos de dados). Por padrão, as VMs são recuperadas para a pasta Carga de trabalho.

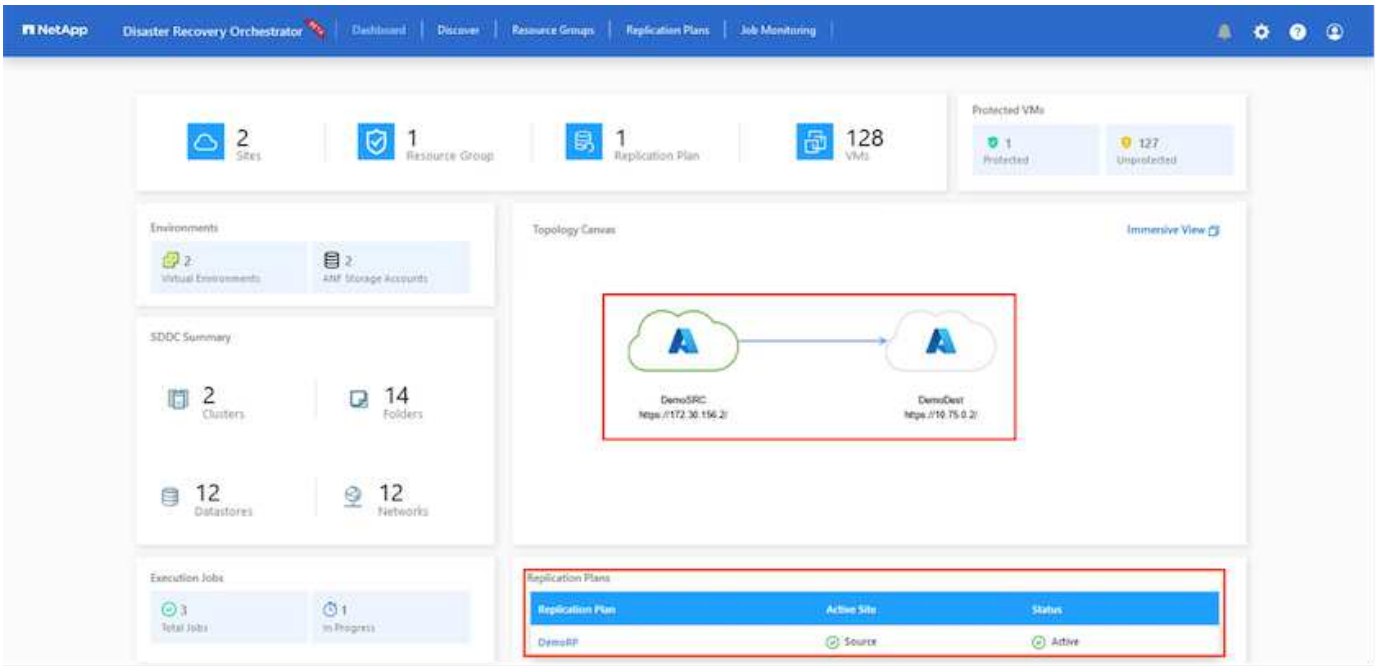


O failback pode ser acionado no nível do plano de replicação. Em caso de falha de teste, a opção de desmontagem pode ser usada para reverter as alterações e remover o volume recém-criado. Failbacks relacionados a failover são um processo de duas etapas. Selecione o plano de replicação e selecione **Sincronização reversa de dados**.



Após a conclusão desta etapa, acione o failback para retornar ao site AVS principal.





No portal do Azure, podemos ver que a integridade da replicação foi interrompida para os volumes apropriados que foram mapeados para o AVS SDDC do site secundário como volumes de leitura/gravação. Durante o failover de teste, o DRO não mapeia o volume de destino ou de réplica. Em vez disso, ele cria um novo volume do instantâneo de replicação entre regiões necessário e expõe o volume como um armazenamento de dados, o que consome capacidade física adicional do pool de capacidade e garante que o volume de origem não seja modificado. Notavelmente, os trabalhos de replicação podem continuar durante testes de DR ou fluxos de trabalho de triagem. Além disso, esse processo garante que a recuperação possa ser limpa sem o risco de a réplica ser destruída caso ocorram erros ou dados corrompidos sejam recuperados.

Recuperação de ransomware

Recuperar-se de um ransomware pode ser uma tarefa assustadora. Especificamente, pode ser difícil para organizações de TI identificar qual é o ponto de retorno seguro e, uma vez determinado, como garantir que as cargas de trabalho recuperadas estejam protegidas contra ataques recorrentes (por exemplo, de malware inativo ou por meio de aplicativos vulneráveis).

O DRO aborda essas preocupações permitindo que as organizações se recuperem de qualquer momento disponível. As cargas de trabalho são então recuperadas para redes funcionais, porém isoladas, para que os aplicativos possam funcionar e se comunicar entre si, mas não sejam expostos a nenhum tráfego norte-sul.

Esse processo oferece às equipes de segurança um local seguro para realizar análises forenses e identificar qualquer malware oculto ou adormecido.

Conclusão

A solução de recuperação de desastres do Azure NetApp Files e do Azure VMware oferece os seguintes benefícios:

- Aproveite a replicação eficiente e resiliente entre regiões do Azure NetApp Files .
- Recupere para qualquer ponto no tempo disponível com retenção de instantâneos.
- Automatize totalmente todas as etapas necessárias para recuperar centenas a milhares de VMs das etapas de armazenamento, computação, rede e validação de aplicativos.
- A recuperação de carga de trabalho aproveita o processo "Criar novos volumes a partir dos instantâneos mais recentes", que não manipula o volume replicado.
- Evite qualquer risco de corrupção de dados nos volumes ou snapshots.
- Evite interrupções de replicação durante fluxos de trabalho de teste de DR.
- Aproveite os dados de DR e os recursos de computação em nuvem para fluxos de trabalho além de DR, como desenvolvimento/teste, testes de segurança, testes de patches e atualizações e testes de remediação.
- A otimização da CPU e da RAM pode ajudar a reduzir os custos da nuvem, permitindo a recuperação em clusters de computação menores.

Onde encontrar informações adicionais

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

- Criar replicação de volume para o Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"

- Replicação entre regiões de volumes do Azure NetApp Files

  "https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"

- "Solução VMware do Azure"

  "https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"

- Implantar e configurar o ambiente de virtualização no Azure

  "Configurar o AVS no Azure"

- Implantar e configurar a solução VMware do Azure

  https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal

Usando o Veeam Replication e o armazenamento de dados do Azure NetApp Files para recuperação de desastres no Azure VMware Solution

Os armazenamentos de dados do Azure NetApp Files (ANF) separam o armazenamento da computação e desbloqueiam a flexibilidade necessária para qualquer organização

levar suas cargas de trabalho para a nuvem. Ela fornece aos clientes uma infraestrutura de armazenamento flexível e de alto desempenho que pode ser dimensionada independentemente dos recursos de computação. O armazenamento de dados do Azure NetApp Files simplifica e otimiza a implantação junto com o Azure VMware Solution (AVS) como um site de recuperação de desastres para ambientes VMWare locais.

Visão geral

Os armazenamentos de dados NFS baseados em volume do Azure NetApp Files (ANF) podem ser usados para replicar dados locais usando qualquer solução de terceiros validada que forneça capacidade de replicação de VM. Ao adicionar os datastores do Azure NetApp Files , será possível otimizar custos de implantação em vez de criar um SDDC do Azure VMware Solution com uma quantidade enorme de hosts ESXi para acomodar o armazenamento. Essa abordagem é chamada de "Pilot Light Cluster". Um cluster de luz piloto é uma configuração mínima de host AVS (3 nós AVS) junto com capacidade de armazenamento de dados do Azure NetApp Files .

O objetivo é manter uma infraestrutura de baixo custo com todos os componentes principais para lidar com um failover. Um cluster de luz piloto pode ser dimensionado e provisionado mais hosts AVS se ocorrer um failover. E quando o failover estiver concluído e as operações normais forem restauradas, o cluster de luz piloto pode retornar ao modo de operações de baixo custo.

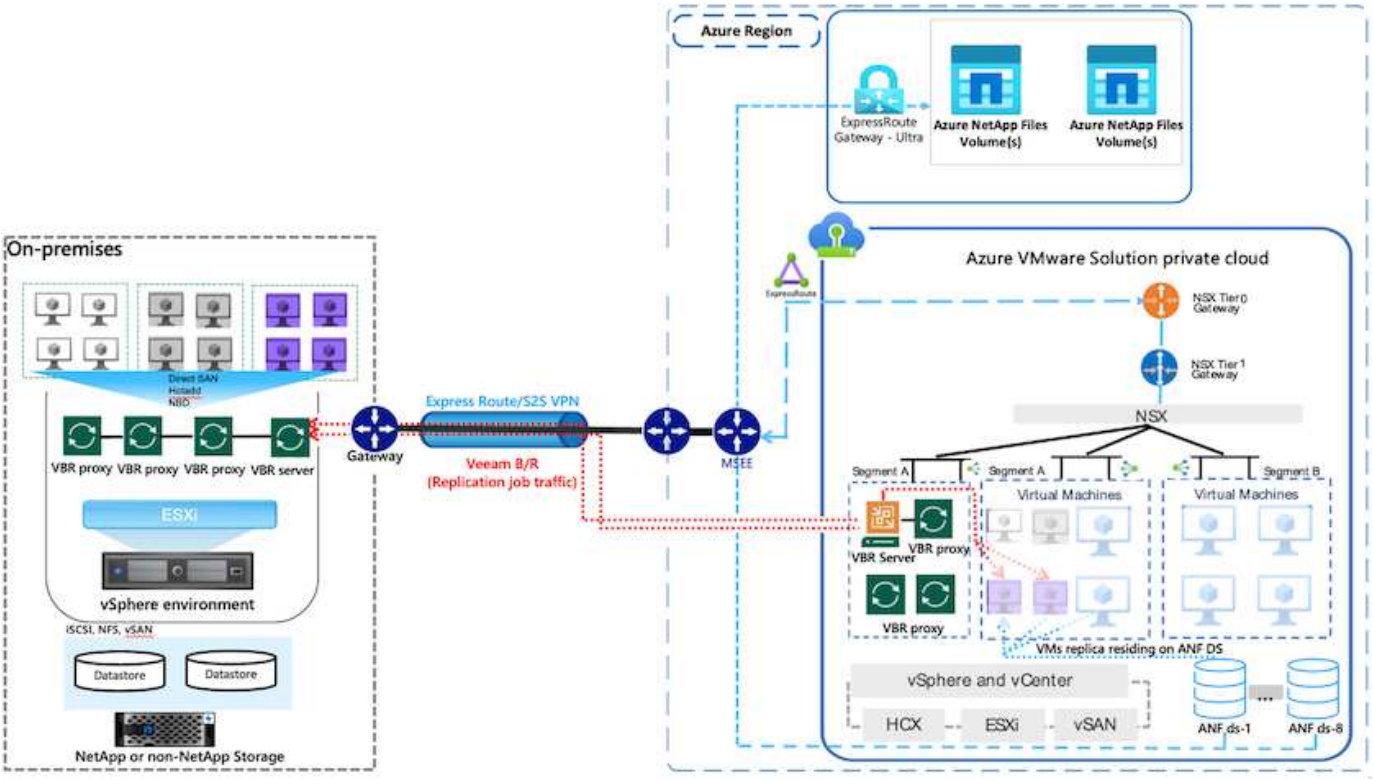
Finalidades deste documento

Este artigo descreve como usar o armazenamento de dados do Azure NetApp Files com o Veeam Backup and Replication para configurar a recuperação de desastres para VMs VMware locais (AVS) usando a funcionalidade do software de replicação de VMs da Veeam.

O Veeam Backup & Replication é um aplicativo de backup e replicação para ambientes virtuais. Quando as máquinas virtuais são replicadas, o Veeam Backup & Replication é replicado no AVS, o software cria uma cópia exata das VMs no formato nativo do VMware vSphere no cluster SDDC do AVS de destino. O Veeam Backup & Replication manterá a cópia sincronizada com a VM original. A replicação fornece o melhor objetivo de tempo de recuperação (RTO), pois há uma cópia montada de uma VM no site de DR em um estado pronto para iniciar.

Esse mecanismo de replicação garante que as cargas de trabalho possam iniciar rapidamente em um SDDC do AVS no caso de um evento de desastre. O software Veeam Backup & Replication também otimiza a transmissão de tráfego para replicação via WAN e conexões lentas. Além disso, ele também filtra blocos de dados duplicados, blocos de dados zero, arquivos de troca e "arquivos de sistema operacional convidado de VM excluídos". O software também compactará o tráfego de réplica. Para evitar que trabalhos de replicação consumam toda a largura de banda da rede, aceleradores de WAN e regras de limitação de rede podem ser utilizados.

O processo de replicação no Veeam Backup & Replication é orientado por tarefas, o que significa que a replicação é realizada configurando tarefas de replicação. No caso de um evento de desastre, o failover pode ser acionado para recuperar as VMs por meio de failover para sua cópia de réplica. Quando o failover é executado, uma VM replicada assume a função da VM original. O failover pode ser executado no estado mais recente de uma réplica ou em qualquer um dos seus pontos de restauração conhecidos. Isso permite a recuperação de ransomware ou testes isolados, conforme necessário. O Veeam Backup & Replication oferece diversas opções para lidar com diferentes cenários de recuperação de desastres.



Implantação de solução

Degraus altos

1. O software Veeam Backup and Replication está sendo executado em um ambiente local com conectividade de rede apropriada.
2. "Implantar a Solução VMware do Azure (AVS)"nuvem privada e"anexar armazenamentos de dados do Azure NetApp Files" para hosts da Solução VMware do Azure.

   Um ambiente de luz piloto configurado com uma configuração mínima pode ser usado para fins de DR. As VMs farão failover para esse cluster no caso de um incidente, e nós adicionais podem ser adicionados).
3. Configure a tarefa de replicação para criar réplicas de VM usando o Veeam Backup and Replication.
4. Crie um plano de failover e execute o failover.
5. Retorne para as VMs de produção quando o evento de desastre for concluído e o site principal estiver ativo.

Pré-requisitos para replicação de VM Veeam para datastores AVS e ANF

1. Certifique-se de que a VM de backup do Veeam Backup & Replication esteja conectada aos clusters AVS SDDC de origem e de destino.
2. O servidor de backup deve ser capaz de resolver nomes curtos e se conectar aos vCenters de origem e de destino.
3. O armazenamento de dados de destino do Azure NetApp Files deve ter espaço livre suficiente para armazenar VMDKs de VMs replicadas.

Para obter informações adicionais, consulte “Considerações e Limitações” abordado"aqui" .

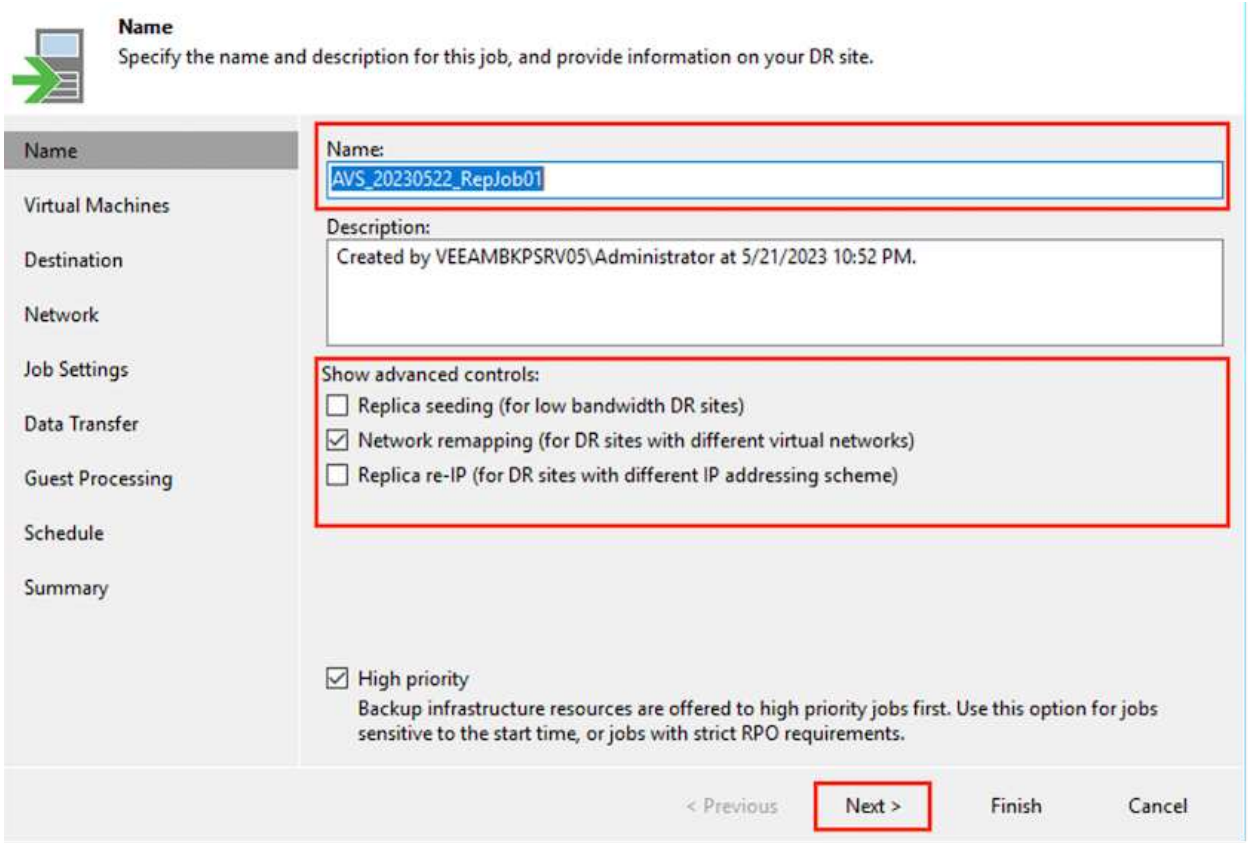
Detalhes da implantação

▼ **Etapa 1: replicar VMs**

O Veeam Backup & Replication aproveita os recursos de snapshot do VMware vSphere/Durante a replicação, o Veeam Backup & Replication solicita que o VMware vSphere crie um snapshot de VM. O snapshot da VM é a cópia de um momento específico de uma VM que inclui discos virtuais, estado do sistema, configuração e metadados. O Veeam Backup & Replication usa o snapshot como uma fonte de dados para replicação.

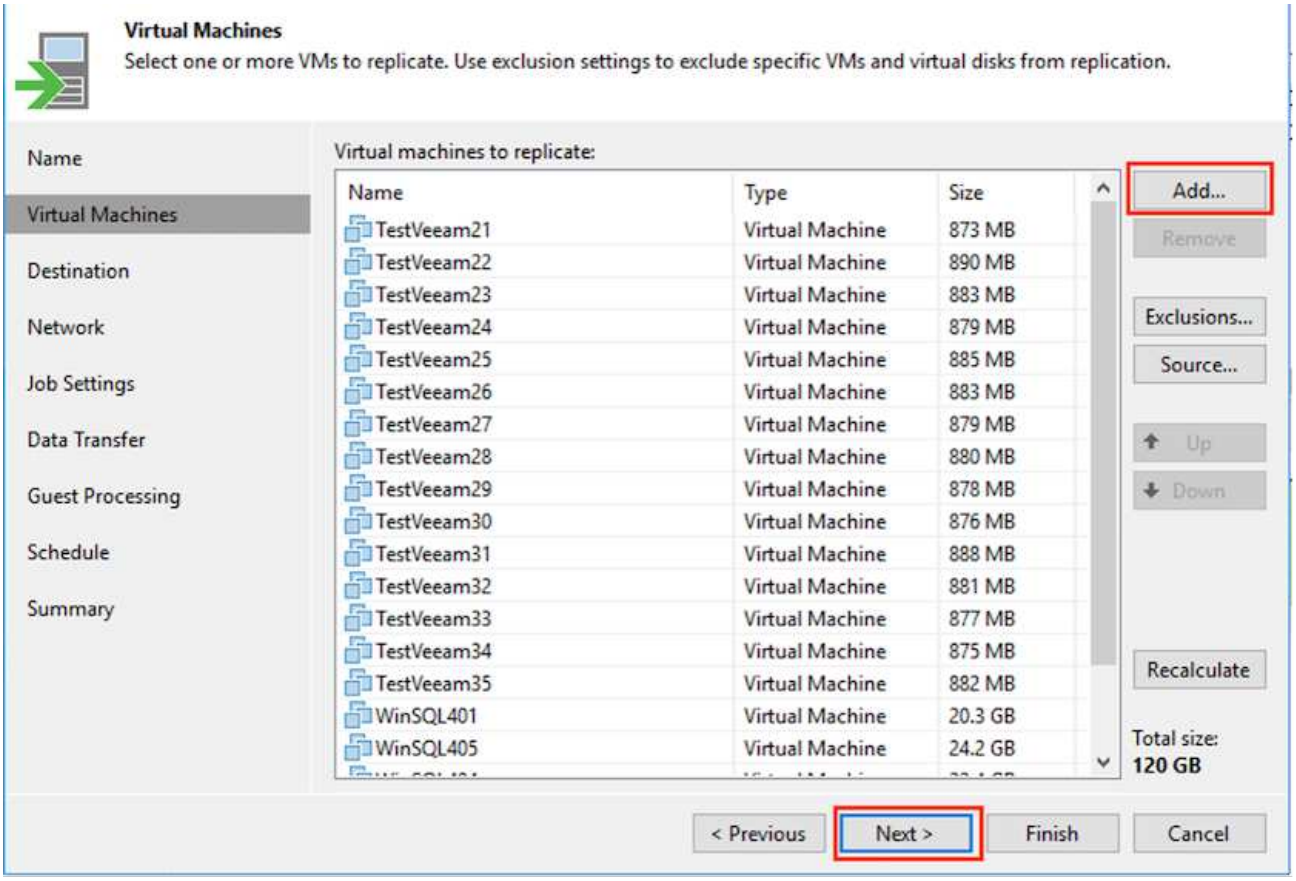
Para replicar VMs, siga as etapas abaixo:

1. Abra o Veeam Backup & Replication Console.
2. Na visualização inicial. Clique com o botão direito do mouse no nó de trabalhos e selecione Trabalho de replicação > Máquina virtual.
3. Especifique um nome de tarefa e selecione a caixa de seleção de controle avançado apropriada. Clique em Avançar.
   - Marque a caixa de seleção Semeadura de réplica se a conectividade entre o local e o Azure tiver largura de banda restrita. *Selecione a caixa de seleção Remapeamento de rede (para sites AVS SDDC com redes diferentes) se os segmentos no Azure VMware Solution SDDC não corresponderem aos das redes de sites locais.
   - Se o esquema de endereçamento IP no site de produção local for diferente do esquema no site do AVS de destino, marque a caixa de seleção Replicar re-IP (para sites de DR com esquema de endereçamento IP diferente).

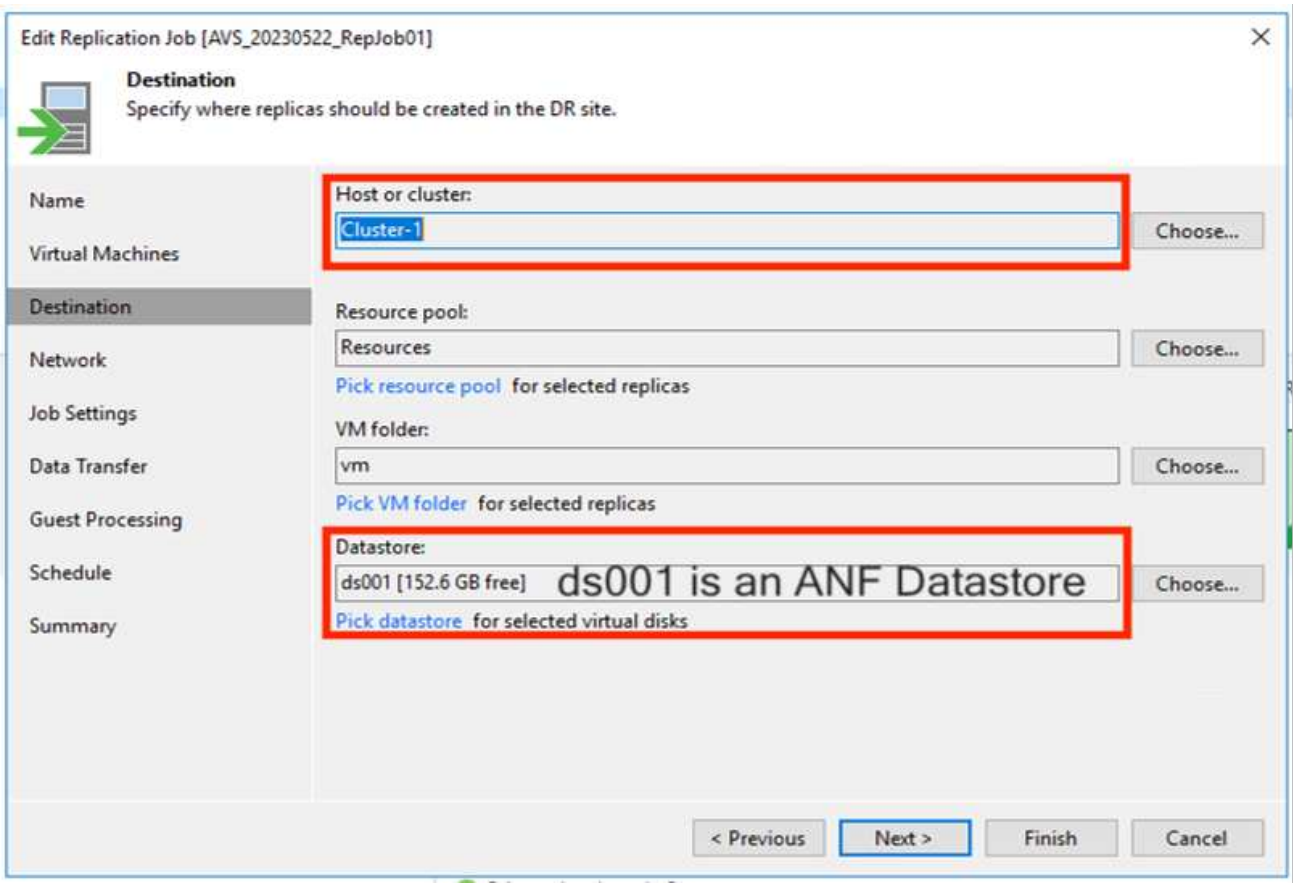


4. Selecione as VMs a serem replicadas no armazenamento de dados do Azure NetApp Files anexado a um SDDC da Solução VMware do Azure na etapa **Máquinas** Virtuais*. As máquinas virtuais podem ser colocadas no vSAN para preencher a capacidade disponível do armazenamento de dados do vSAN.

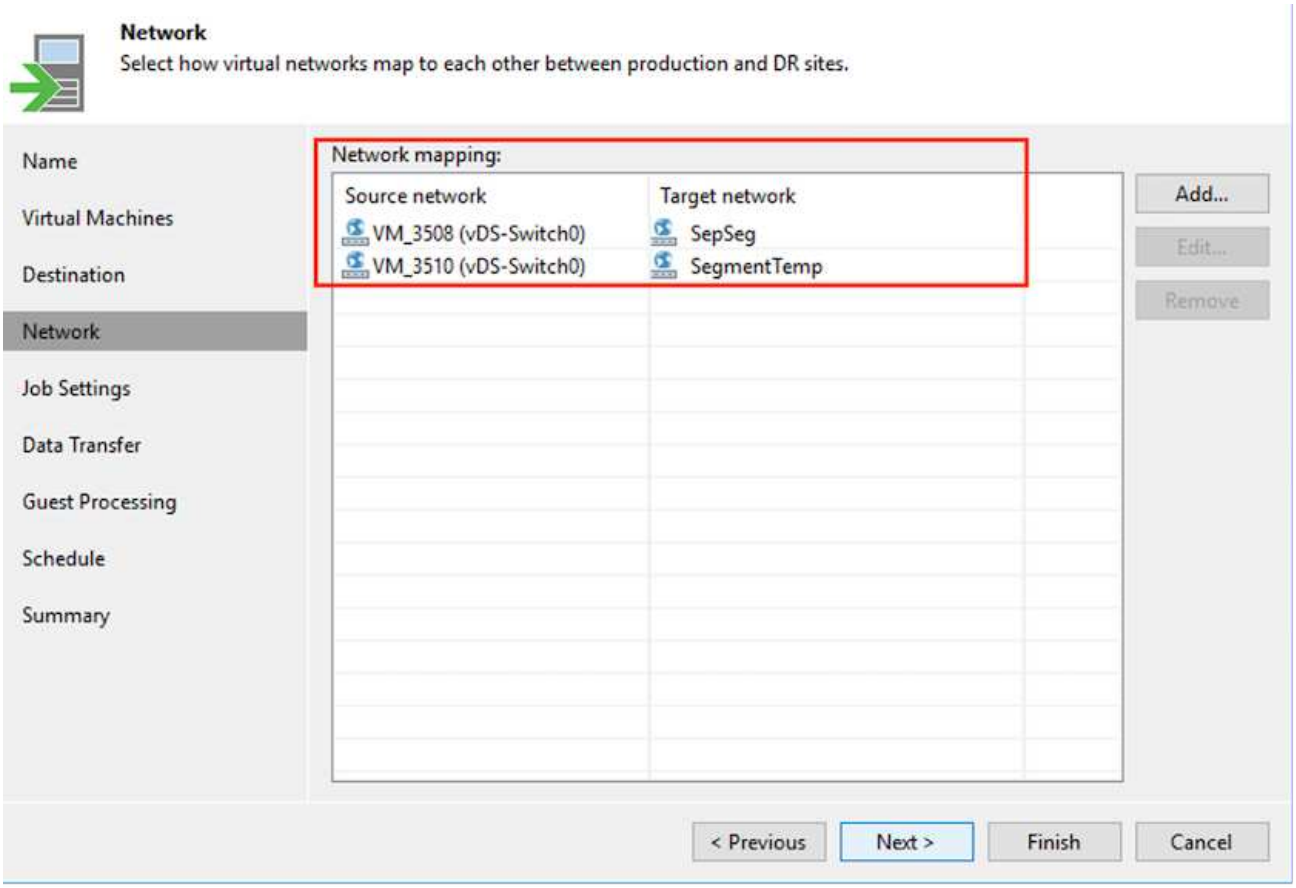
Em um cluster de luz piloto, a capacidade utilizável de um cluster de 3 nós será limitada. O restante dos dados pode ser facilmente colocado nos armazenamentos de dados do Azure NetApp Files para que as VMs possam ser recuperadas, e o cluster pode ser expandido para atender aos requisitos de CPU/memória. Clique em **Adicionar**, então na janela **Adicionar Objeto** selecione as VMs ou contêineres de VM necessários e clique em **Adicionar**. Clique em **Avançar**.



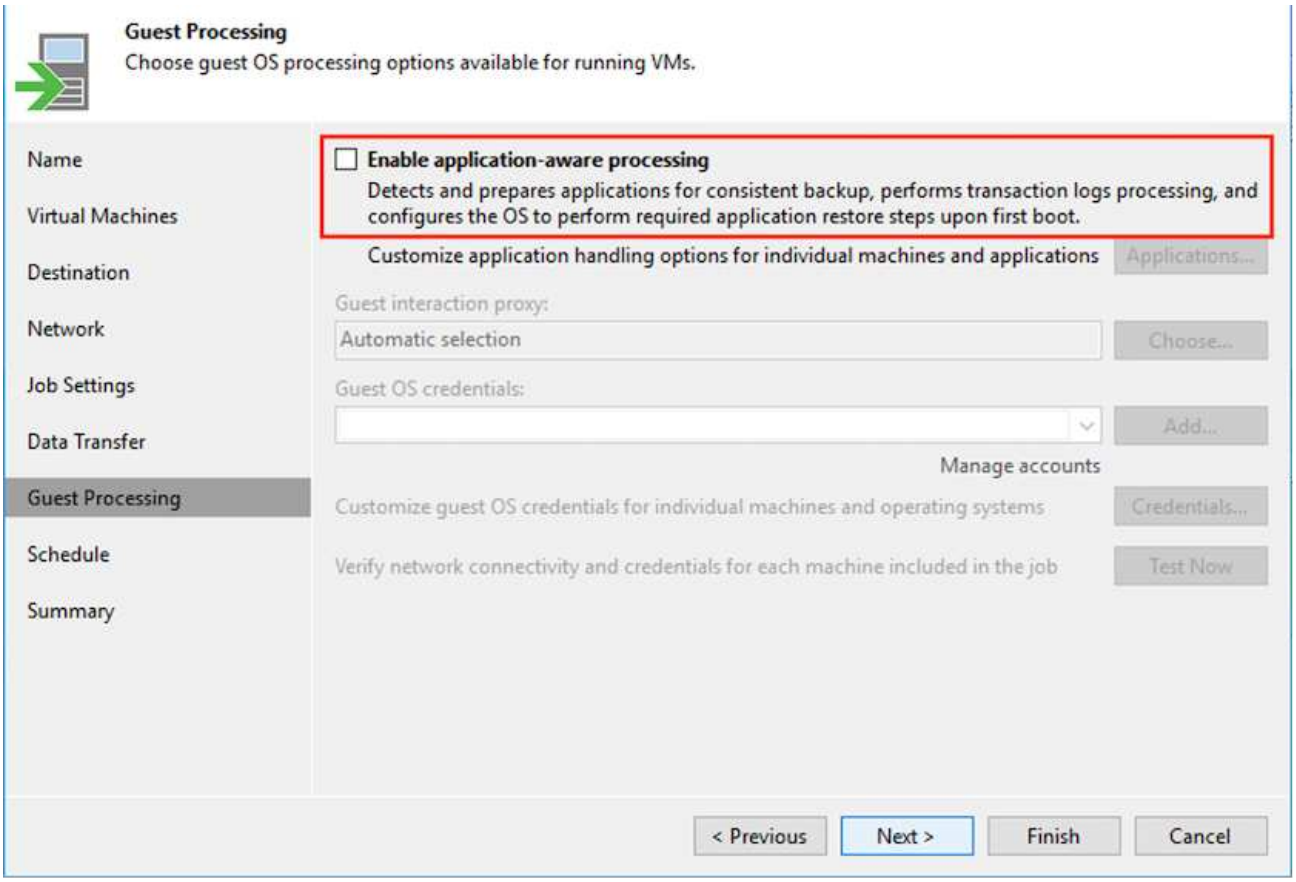
5. Depois disso, selecione o destino como cluster/host do Azure VMware Solution SDDC e o pool de recursos apropriado, a pasta da VM e o armazenamento de dados FSx ONTAP para réplicas da VM. Em seguida, clique em **Avançar**.



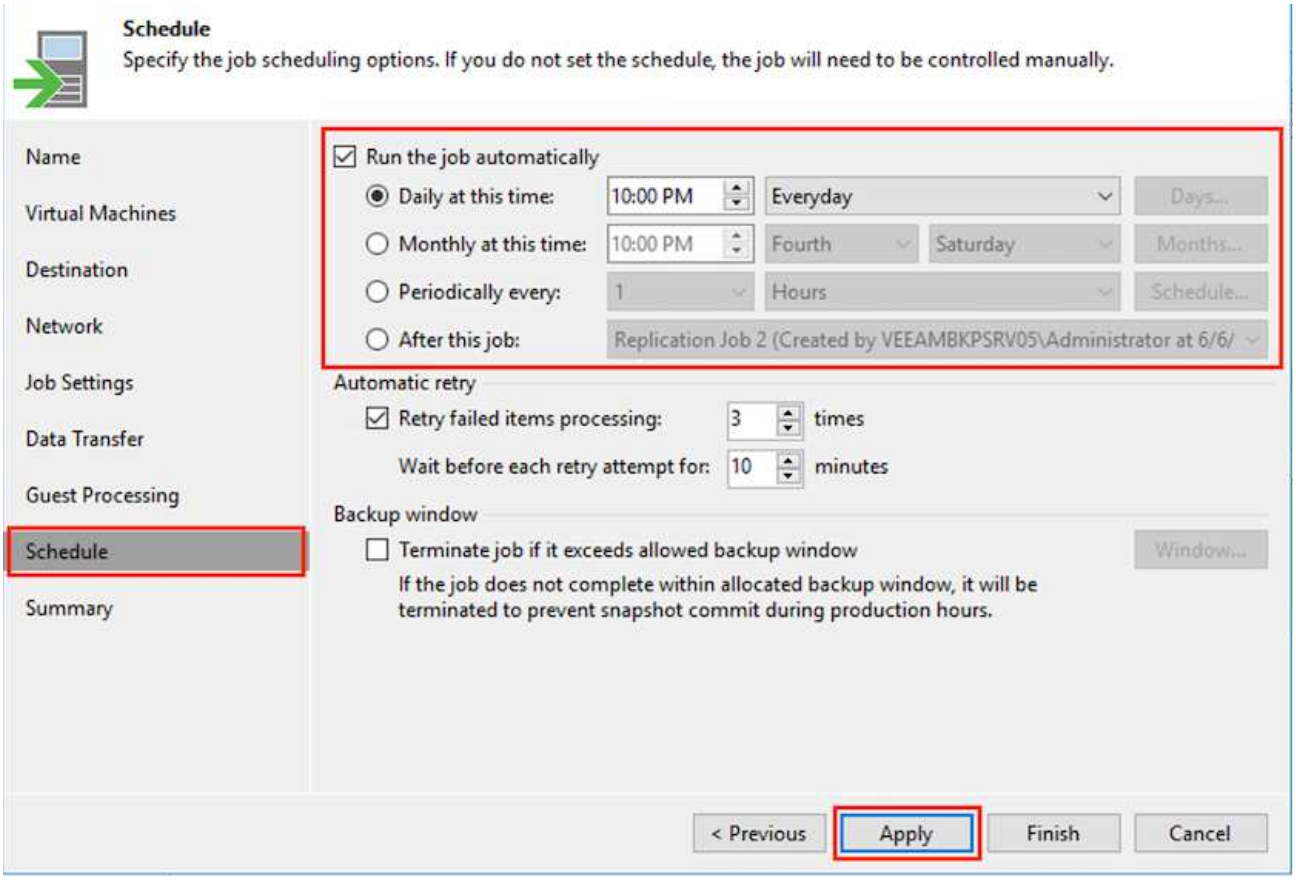
6. Na próxima etapa, crie o mapeamento entre a rede virtual de origem e de destino, conforme necessário.



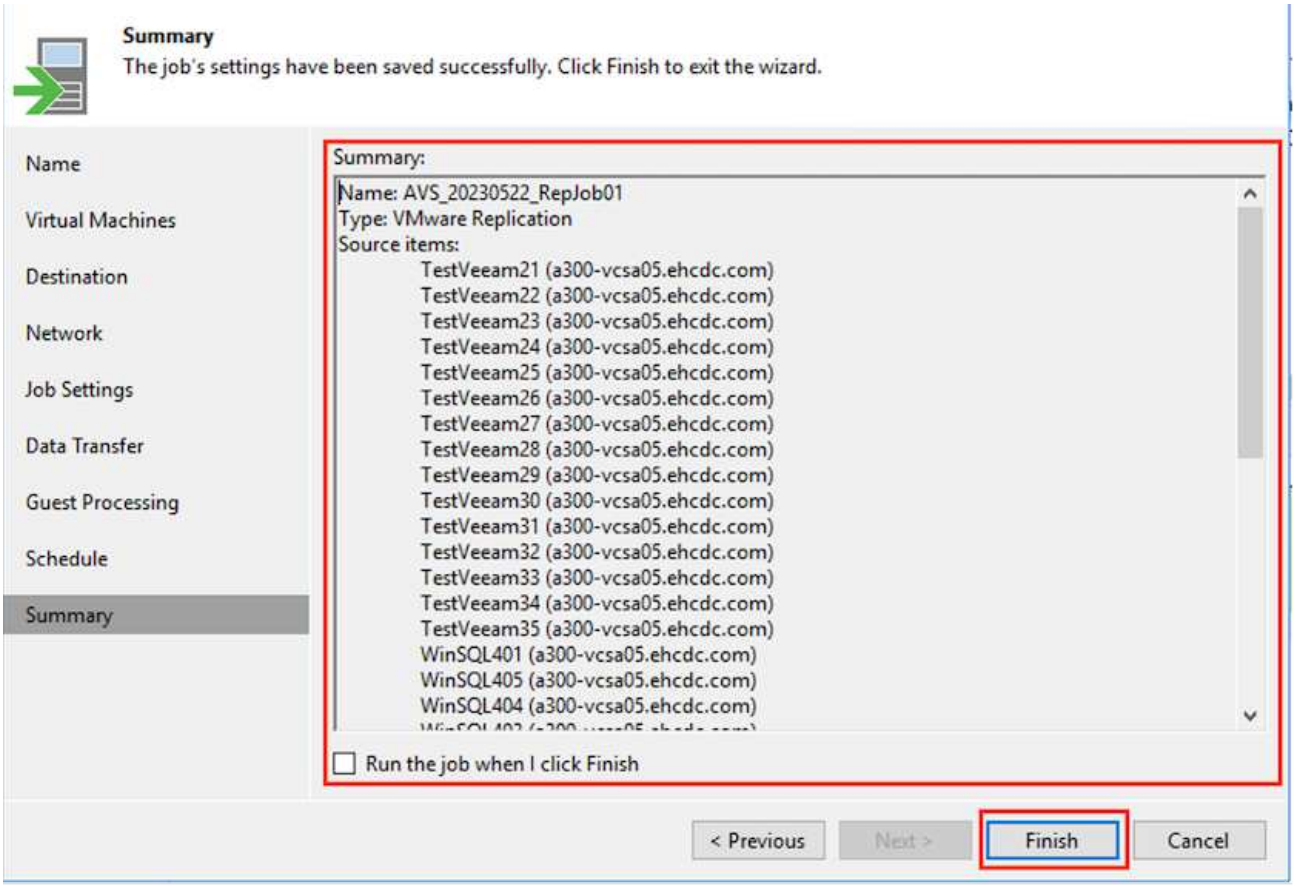
7. Na etapa **Configurações da tarefa**, especifique o repositório de backup que armazenará metadados para réplicas de VM, política de retenção e assim por diante.
8. Atualize os servidores proxy **Origem** e **Destino** na etapa **Transferência de dados** e deixe a seleção **Automático** (padrão) e mantenha a opção **Direto** selecionada e clique em **Avançar**.
9. Na etapa **Processamento de Convidado**, selecione a opção **Ativar processamento com reconhecimento de aplicativo** conforme necessário. Clique em **Avançar**.



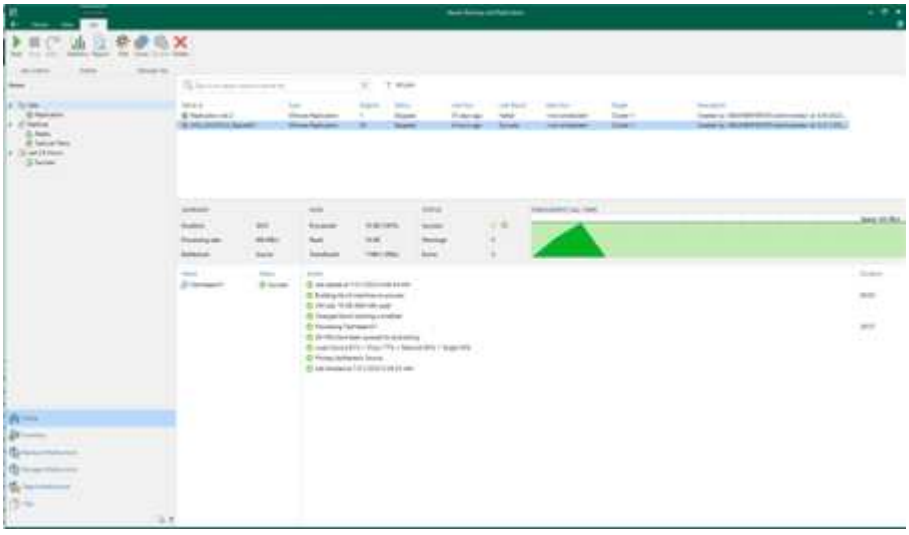
10. Escolha o agendamento de replicação para executar o trabalho de replicação regularmente.



11. Na etapa **Resumo** do assistente, revise os detalhes do trabalho de replicação. Para iniciar o trabalho logo após o assistente ser fechado, marque a caixa de seleção **Executar o trabalho quando eu clicar em Concluir**; caso contrário, deixe a caixa de seleção desmarcada. Em seguida, clique em **Concluir** para fechar o assistente.



Assim que o trabalho de replicação começar, as VMs com o sufixo especificado serão preenchidas no cluster/host do AVS SDDC de destino.



Para obter informações adicionais sobre a replicação do Veeam, consulte"Como funciona a replicação"

▼ **Etapa 2: Crie um plano de failover**

Quando a replicação ou propagação inicial estiver concluída, crie o plano de failover. O plano de failover ajuda a executar o failover para VMs dependentes, uma por uma ou como um grupo, automaticamente. O plano de failover é o modelo para a ordem em que as VMs são processadas, incluindo os atrasos de inicialização. O plano de failover também ajuda a garantir que as VMs dependentes críticas já estejam em execução.

Para criar o plano, navegue até a nova subseção chamada **Réplicas** e selecione **Plano de Failover**. Escolha as VMs apropriadas. O Veeam Backup & Replication procurará os pontos de restauração mais próximos desse momento e os usará para iniciar réplicas de VM.

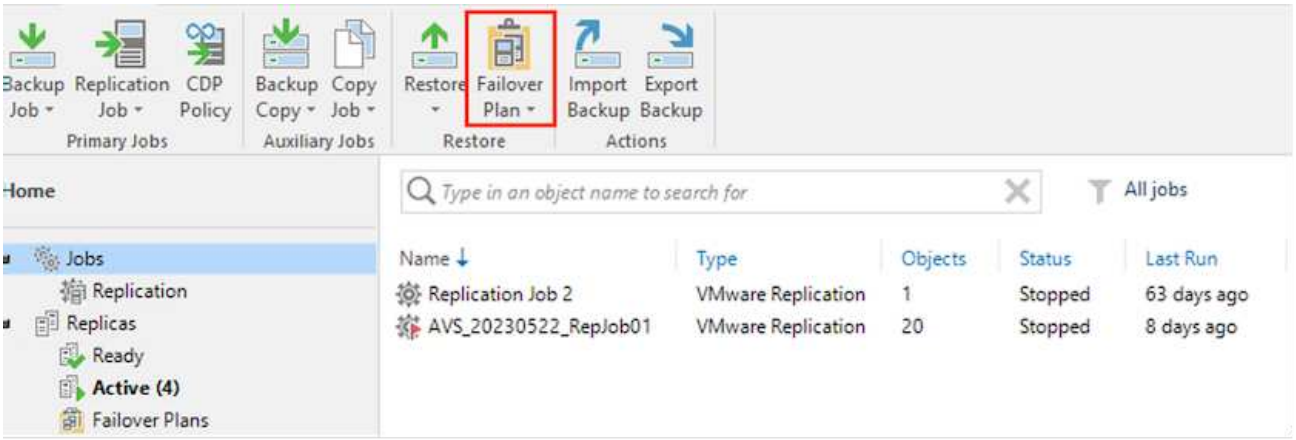
O plano de failover só pode ser adicionado quando a replicação inicial estiver concluída e as réplicas da VM estiverem no estado Pronto.

O número máximo de VMs que podem ser iniciadas simultaneamente ao executar um plano de failover é 10

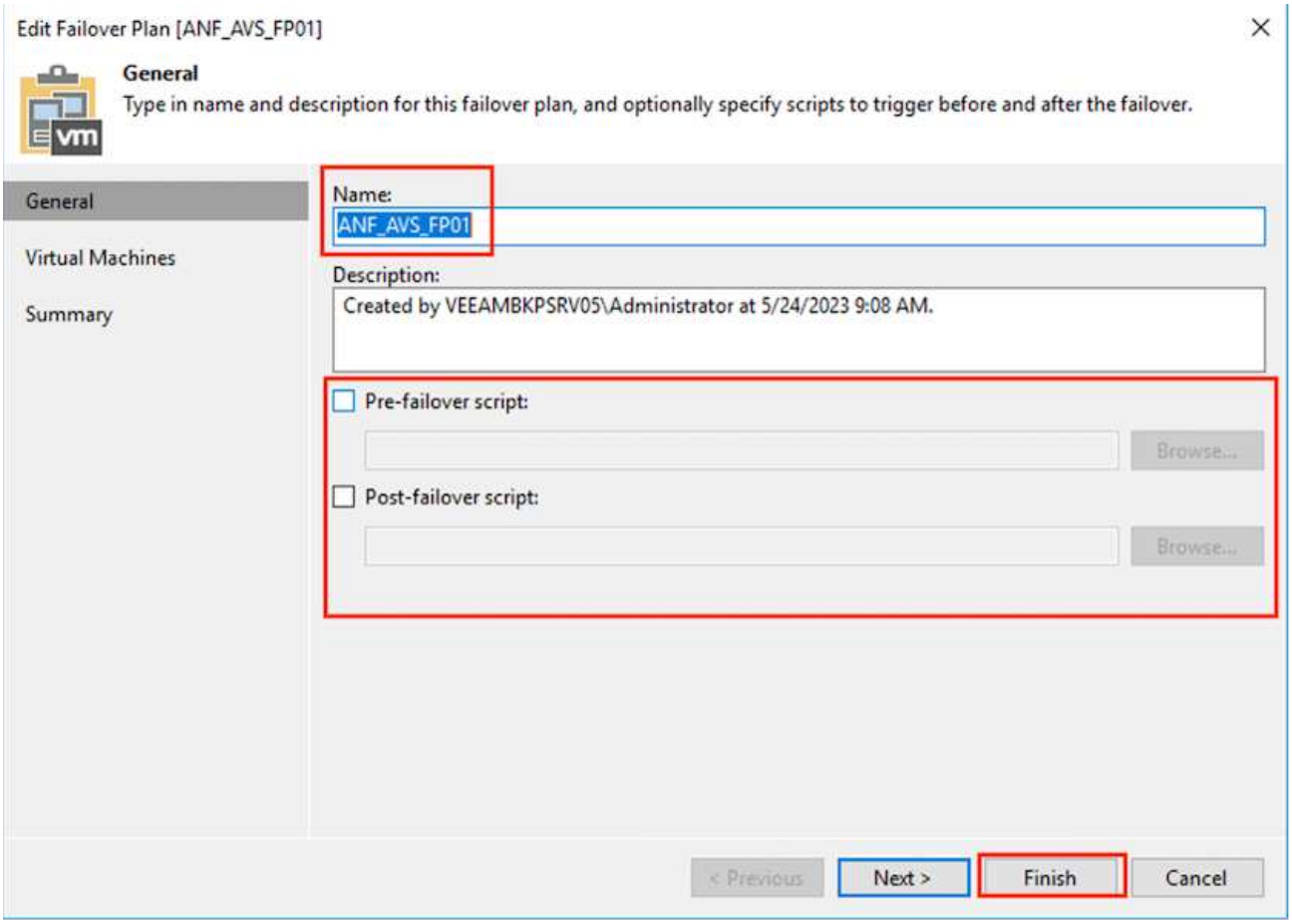
Durante o processo de failover, as VMs de origem não serão desligadas

Para criar o **Plano de Failover**, faça o seguinte:

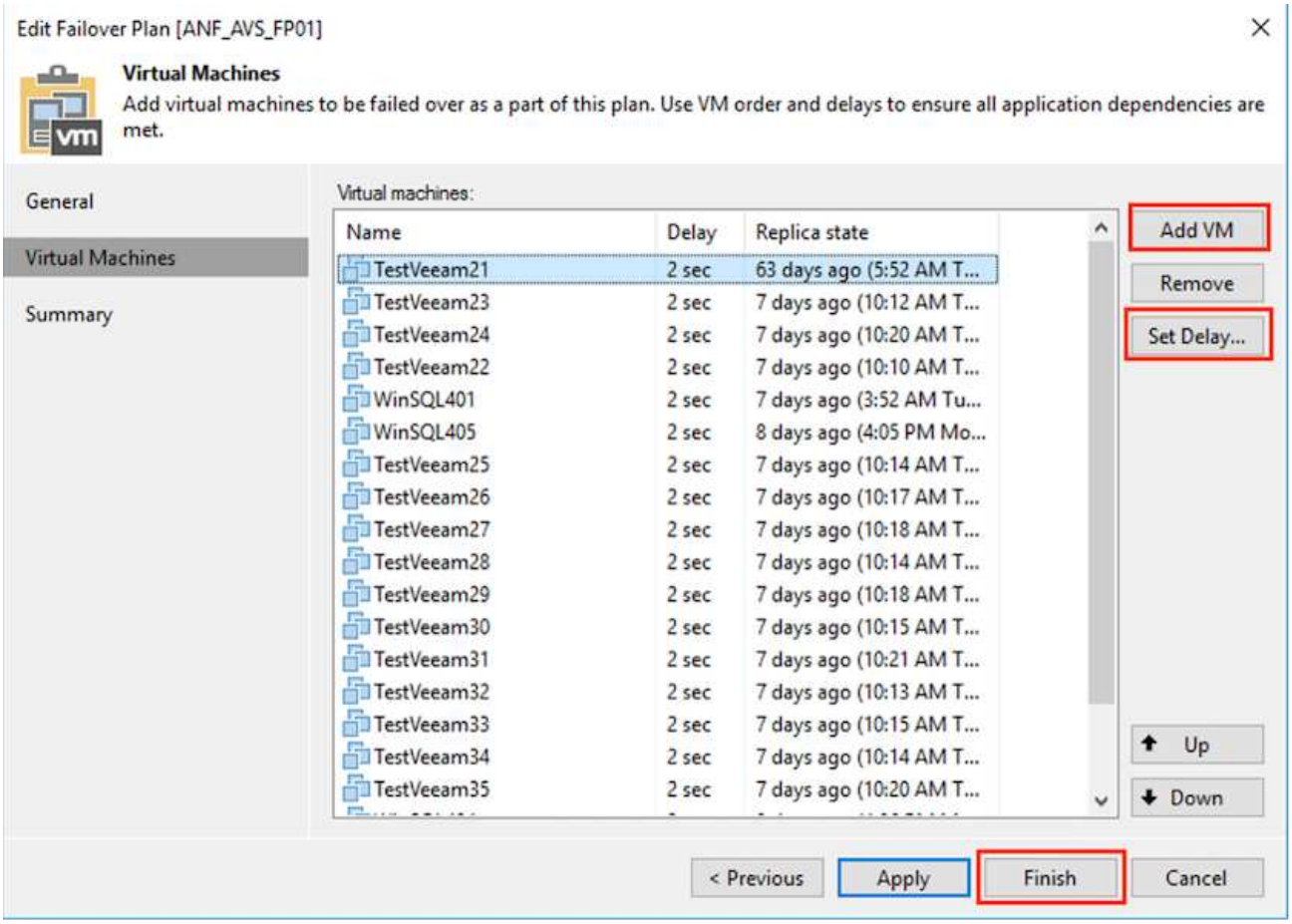
1. Na visualização inicial. Clique com o botão direito do mouse no nó Réplicas e selecione Planos de Failover > Plano de Failover > VMware vSphere.



2. Em seguida, forneça um nome e uma descrição para o plano. Scripts pré e pós-failover podem ser adicionados conforme necessário. Por exemplo, execute um script para desligar as VMs antes de iniciar as VMs replicadas.



3. Adicione as VMs ao plano e modifique a ordem de inicialização das VMs e os atrasos de inicialização para atender às dependências do aplicativo.



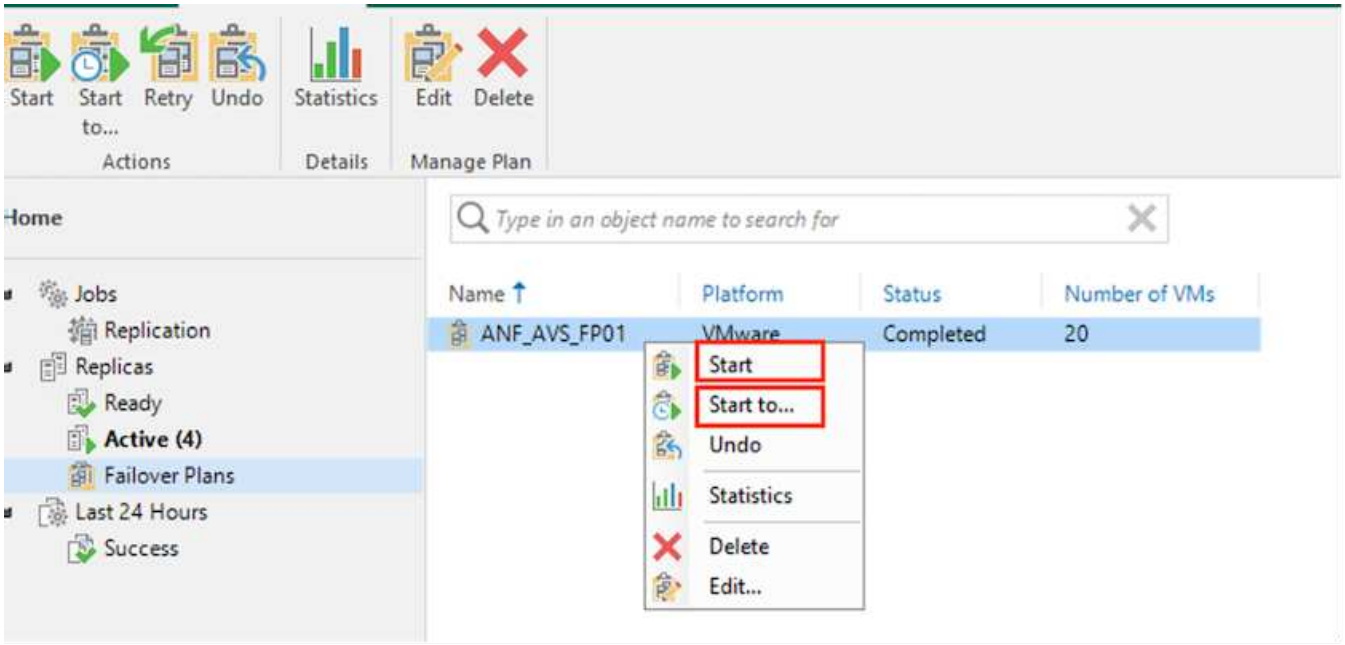
Para obter informações adicionais sobre a criação de trabalhos de replicação, consulte"Criando trabalhos de replicação" .

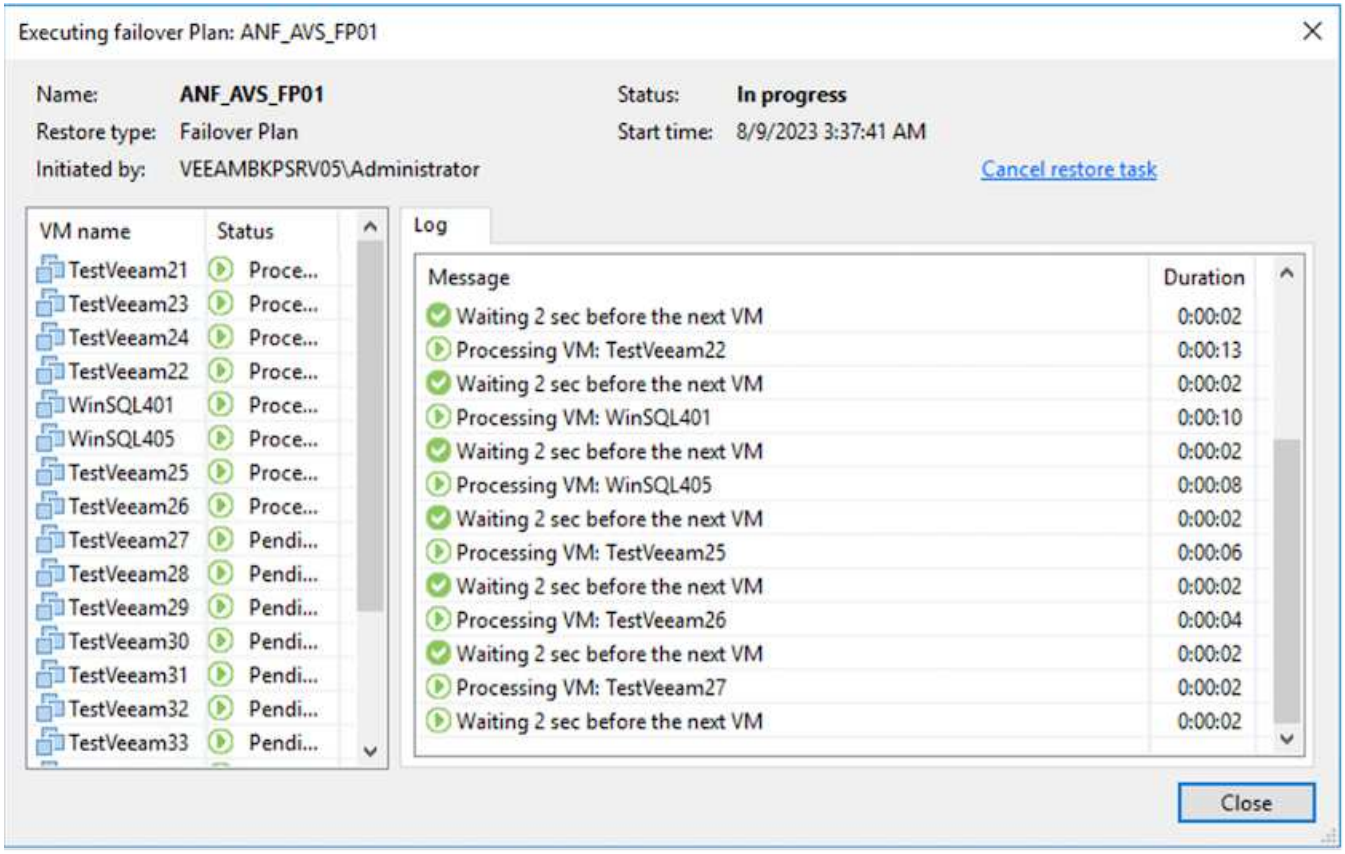
▼ **Etapa 3: execute o plano de failover**

Durante o failover, a VM de origem no site de produção é alternada para sua réplica no site de recuperação de desastres. Como parte do processo de failover, o Veeam Backup & Replication restaura a réplica da VM para o ponto de restauração necessário e move todas as atividades de E/S da VM de origem para sua réplica. As réplicas podem ser usadas não apenas em caso de desastre, mas também para simular exercícios de DR. Durante a simulação de failover, a VM de origem permanece em execução. Depois que todos os testes necessários forem realizados, você poderá desfazer o failover e retornar às operações normais.

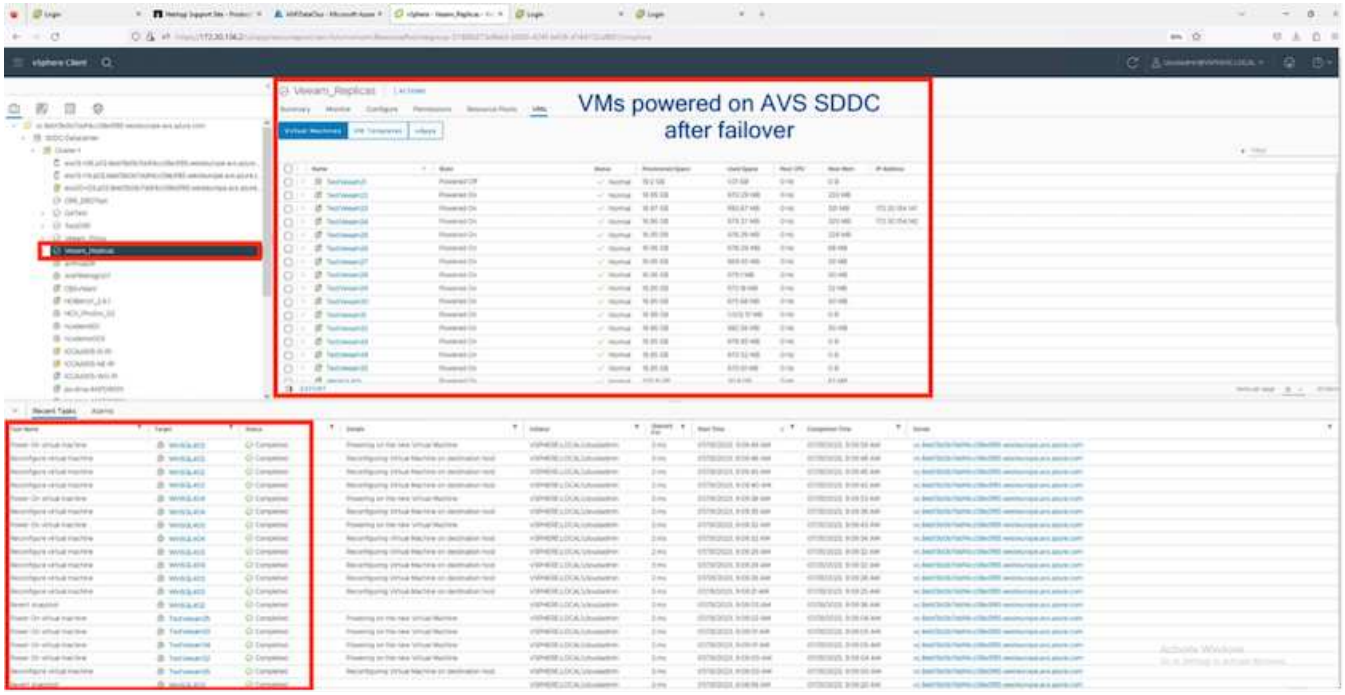
ⓘ Certifique-se de que a segmentação de rede esteja em vigor para evitar conflitos de IP durante o failover.

Para iniciar o plano de failover, basta clicar na aba **Planos de failover** e clicar com o botão direito no seu plano de failover. Selecione ***Iniciar**. Isso fará failover usando os pontos de restauração mais recentes das réplicas de VM. Para fazer failover para pontos de restauração específicos de réplicas de VM, selecione **Iniciar para**.

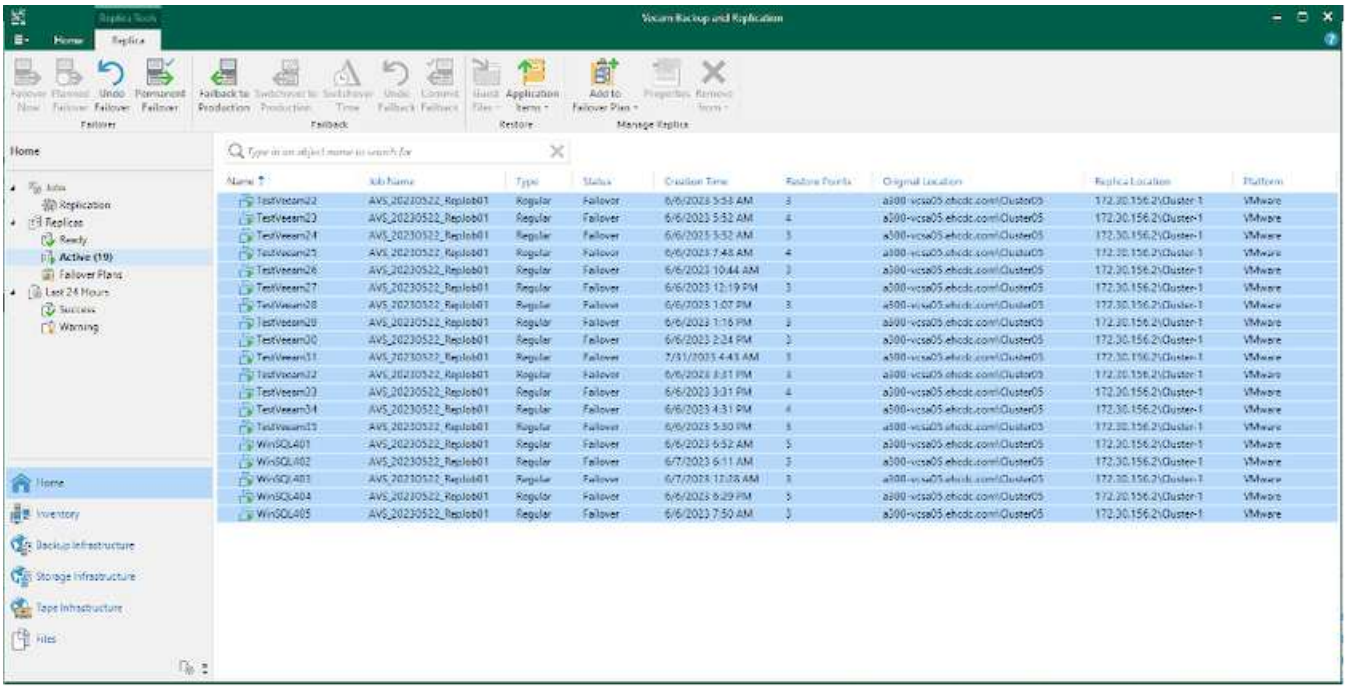




O estado da réplica da VM muda de Pronto para Failover e as VMs serão iniciadas no cluster/host SDDC do Azure VMware Solution (AVS) de destino.



Quando o failover estiver concluído, o status das VMs mudará para "Failover".



O Veeam Backup & Replication interrompe todas as atividades de replicação da VM de origem até que sua réplica retorne ao estado Pronto.

Para obter informações detalhadas sobre planos de failover, consulte"Planos de Failover" .

▼ **Etapa 4: Failback para o site de produção**

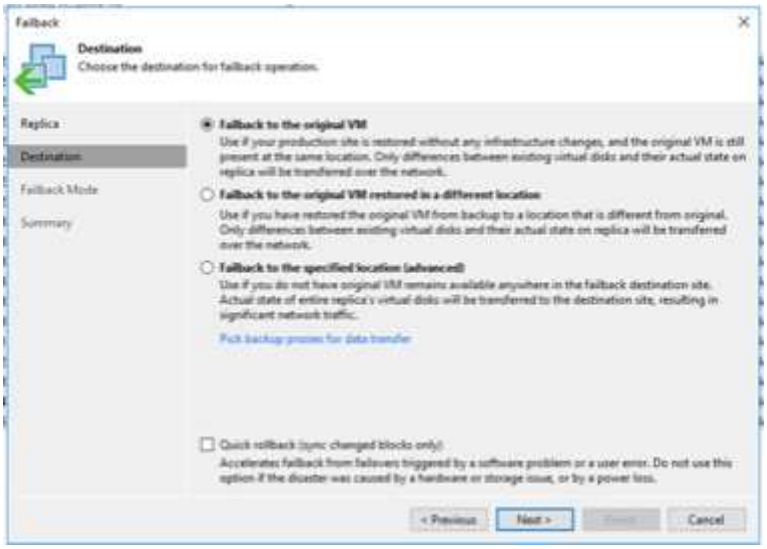
Quando o plano de failover está em execução, ele é considerado uma etapa intermediária e precisa ser finalizado com base no requisito. As opções incluem o seguinte:

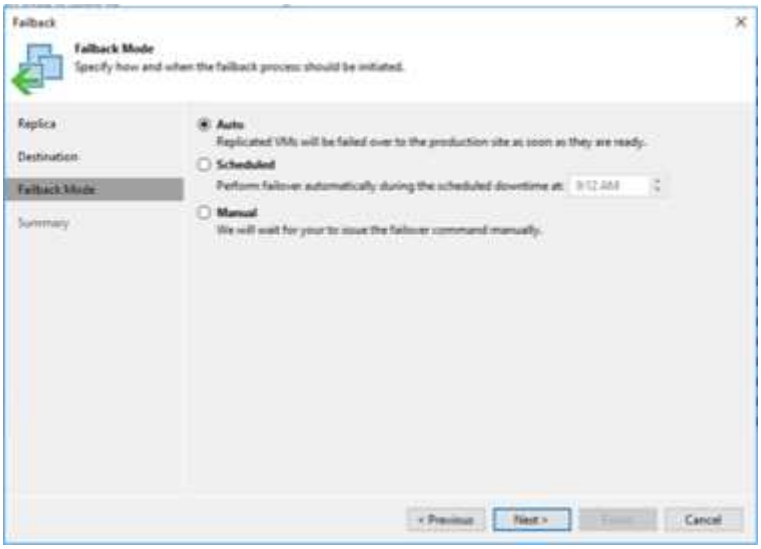
- **Failback para produção** - retorne para a VM original e transfira todas as alterações que ocorreram enquanto a réplica da VM estava em execução para a VM original.

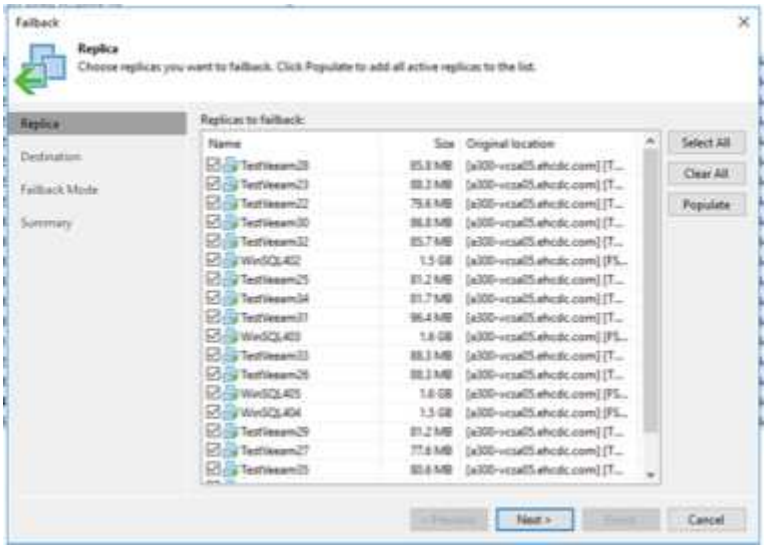
> Quando você executa o failback, as alterações são apenas transferidas, mas não publicadas. Selecione **Confirmar failback** (assim que a VM original for confirmada como funcionando conforme o esperado) ou Desfazer failback para retornar à réplica da VM se a VM original não estiver funcionando conforme o esperado.

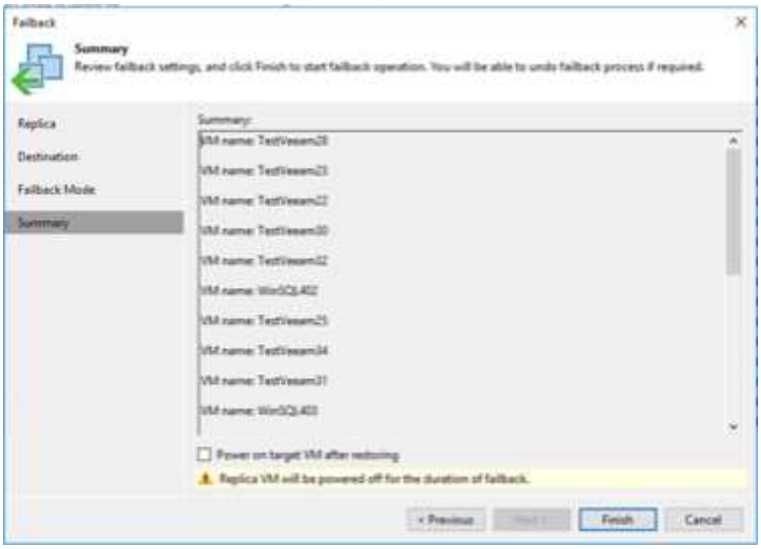
- **Desfazer failover** - retorne à VM original e descarte todas as alterações feitas na réplica da VM enquanto ela estava em execução.
- **Failover permanente** - alterna permanentemente da VM original para uma réplica da VM e usa essa réplica como a VM original.

Nesta demonstração, foi escolhido Failback para produção. O failback para a VM original foi selecionado durante a etapa Destino do assistente e a caixa de seleção "Ligar a VM após a restauração" foi marcada.



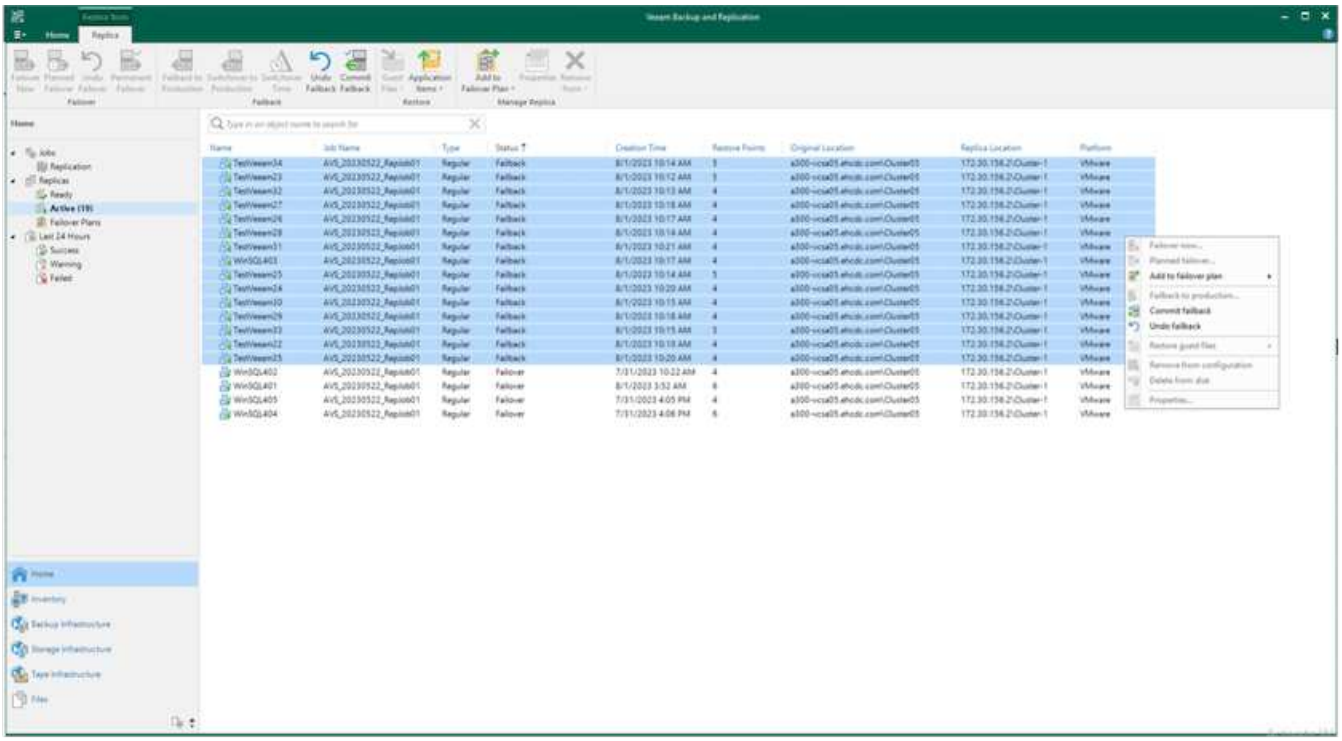




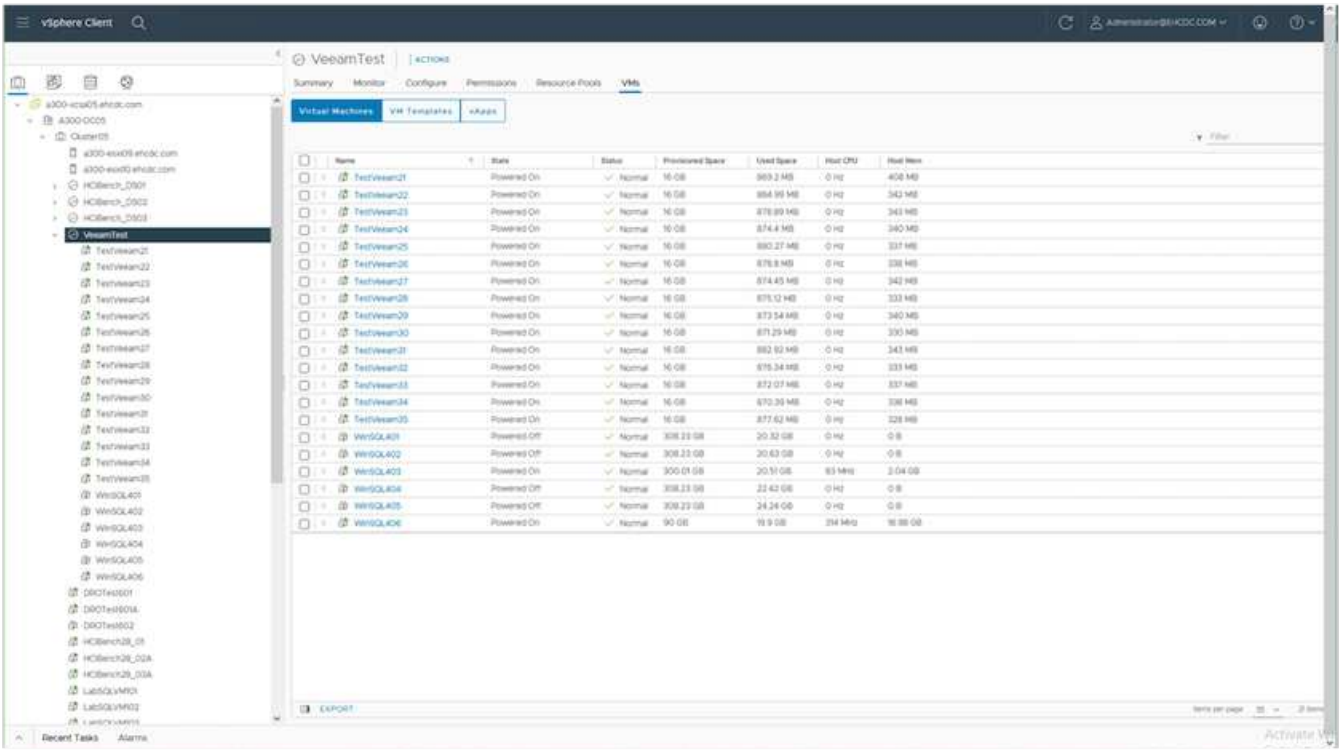


A confirmação de failback é uma das maneiras de finalizar a operação de failback. Quando o failback é confirmado, ele confirma que as alterações enviadas para a VM que sofreu failback (a VM de produção) estão funcionando conforme o esperado. Após a operação de confirmação, o Veeam Backup & Replication retoma as atividades de replicação para a VM de produção.

Para obter informações detalhadas sobre o processo de failback, consulte a documentação do Veeam para"Failover e Failback para replicação" .



Após o failback para produção ser bem-sucedido, todas as VMs serão restauradas para o site de produção original.



Conclusão

O recurso de armazenamento de dados do Azure NetApp Files permite que a Veeam ou qualquer ferramenta de terceiros validada forneça uma solução de DR de baixo custo aproveitando clusters Pilot Light em vez de criar um cluster grande apenas para acomodar réplicas de VM. Isso fornece uma maneira eficaz de lidar com um plano de recuperação de desastres personalizado e personalizado e de reutilizar produtos de backup

existentes internamente para DR, permitindo a recuperação de desastres baseada em nuvem ao sair dos datacenters de DR locais. É possível fazer failover clicando em um botão em caso de desastre ou fazer failover automaticamente se ocorrer um desastre.

Para saber mais sobre esse processo, fique à vontade para seguir o vídeo passo a passo detalhado.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278

Migrar cargas de trabalho no Azure/AVS

TR-4940: Migrar cargas de trabalho para o repositório de dados do Azure NetApp Files usando o VMware HCX - Guia de início rápido

Um dos casos de uso mais comuns para o Azure VMware Solution e o armazenamento de dados do Azure NetApp Files é a migração de cargas de trabalho do VMware. O VMware HCX é uma opção preferencial e fornece vários mecanismos de migração para mover máquinas virtuais (VMs) locais e seus dados para armazenamentos de dados do Azure NetApp Files .

Visão geral: Migrando máquinas virtuais com VMware HCX, repositórios de dados do Azure NetApp Files e solução Azure VMware

O VMware HCX é principalmente uma plataforma de migração projetada para simplificar a migração de aplicativos, o rebalanceamento de carga de trabalho e até mesmo a continuidade dos negócios entre nuvens. Ele está incluído como parte do Azure VMware Solution Private Cloud e oferece muitas maneiras de migrar cargas de trabalho e pode ser usado para operações de recuperação de desastres (DR).

Este documento fornece orientação passo a passo para provisionar o armazenamento de dados do Azure NetApp Files, seguido pelo download, implantação e configuração do VMware HCX, incluindo todos os seus principais componentes no local e no lado da solução VMware do Azure, incluindo interconexão, extensão de rede e otimização de WAN para habilitar vários mecanismos de migração de VM.

> O VMware HCX funciona com qualquer tipo de armazenamento de dados, pois a migração ocorre no nível da VM. Portanto, este documento é aplicável a clientes atuais da NetApp e clientes não pertencentes à NetApp que planejam implantar o Azure NetApp Files com o Azure VMware Solution para uma implantação de nuvem VMware econômica.

▼ **Etapas de alto nível**

Esta lista fornece as etapas gerais necessárias para instalar e configurar o HCX Cloud Manager no lado da nuvem do Azure e instalar o HCX Connector no local:

1. Instale o HCX por meio do portal do Azure.
2. Baixe e implante o instalador do HCX Connector Open Virtualization Appliance (OVA) no VMware vCenter Server local.
3. Ative o HCX com a chave de licença.
4. Emparelhe o VMware HCX Connector local com o Azure VMware Solution HCX Cloud Manager.
5. Configure o perfil de rede, o perfil de computação e a malha de serviço.
6. (Opcional) Execute a extensão da rede para evitar a troca de IP durante migrações.
7. Valide o status do dispositivo e garanta que a migração seja possível.

8. Migre as cargas de trabalho da VM.

▼ Pré-requisitos

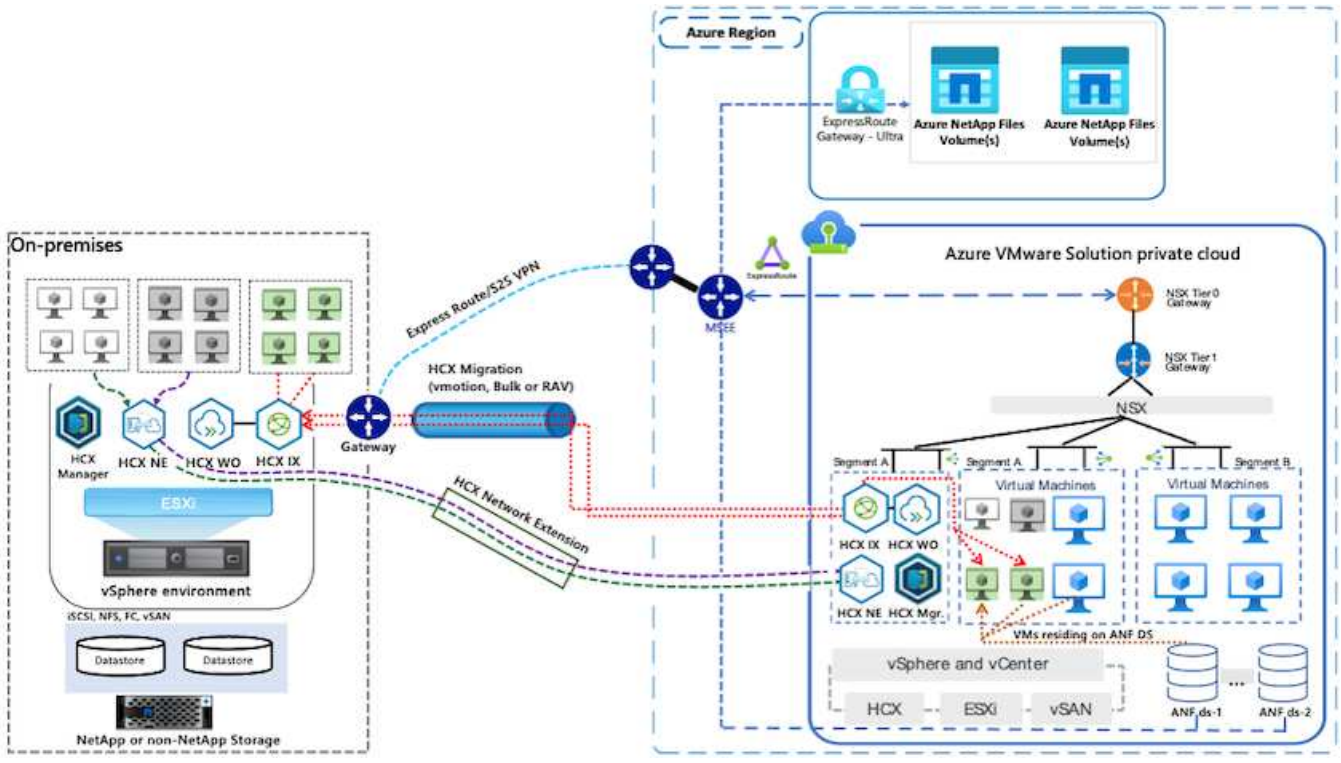
Antes de começar, certifique-se de que os seguintes pré-requisitos sejam atendidos. Para mais informações, consulte isto "link" . Depois que os pré-requisitos, incluindo conectividade, estiverem prontos, configure e ative o HCX gerando a chave de licença no portal do Azure VMware Solution. Após o download do instalador do OVA, prossiga com o processo de instalação conforme descrito abaixo.

> ⓘ O HCX Advanced é a opção padrão e a edição VMware HCX Enterprise também está disponível por meio de um tíquete de suporte e tem suporte sem custo adicional.

- Use um data center definido por software (SDDC) de solução VMware do Azure existente ou crie uma nuvem privada usando este"Link da NetApp" ou isto "Link da Microsoft" .
- A migração de VMs e dados associados do data center habilitado para VMware vSphere local requer conectividade de rede do data center para o ambiente SDDC. Antes de migrar cargas de trabalho, "configurar uma conexão VPN site a site ou uma conexão de alcance global de rota expressa" entre o ambiente local e a respectiva nuvem privada.
- O caminho de rede do ambiente VMware vCenter Server local para a nuvem privada do Azure VMware Solution deve dar suporte à migração de VMs usando o vMotion.
- Certifique-se de que o necessário "regras e portas de firewall" são permitidos para tráfego vMotion entre o vCenter Server local e o SDDC vCenter. Na nuvem privada, o roteamento na rede vMotion é configurado por padrão.
- O volume NFS do Azure NetApp Files deve ser montado como um armazenamento de dados no Azure VMware Solution. Siga os passos detalhados neste "link" para anexar armazenamentos de dados do Azure NetApp Files aos hosts do Azure VMware Solutions.

▼ Arquitetura de Alto Nível

Para fins de teste, o ambiente de laboratório local usado para esta validação foi conectado por meio de uma VPN site a site, que permite conectividade local com o Azure VMware Solution.



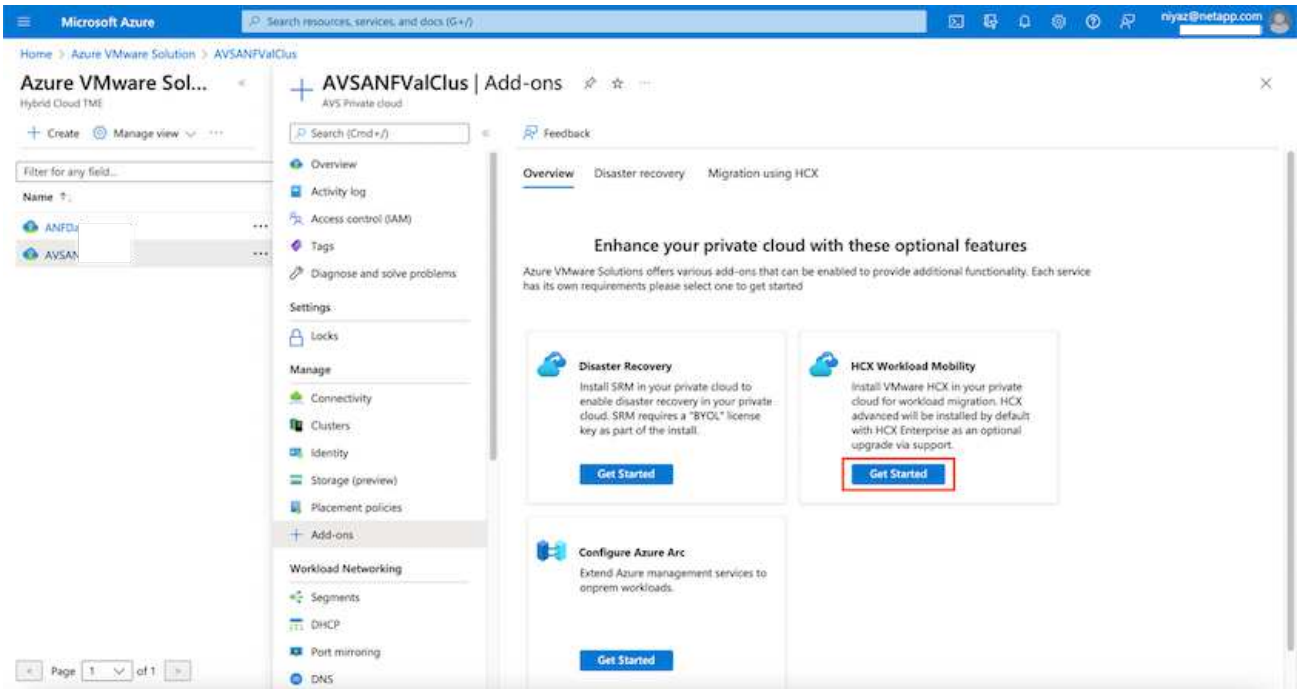
Implantação de solução

Siga a série de etapas para concluir a implantação desta solução:

▼ **Etapa 1: instalar o HCX por meio do Portal do Azure usando a opção Complementos**

Para executar a instalação, siga os seguintes passos:

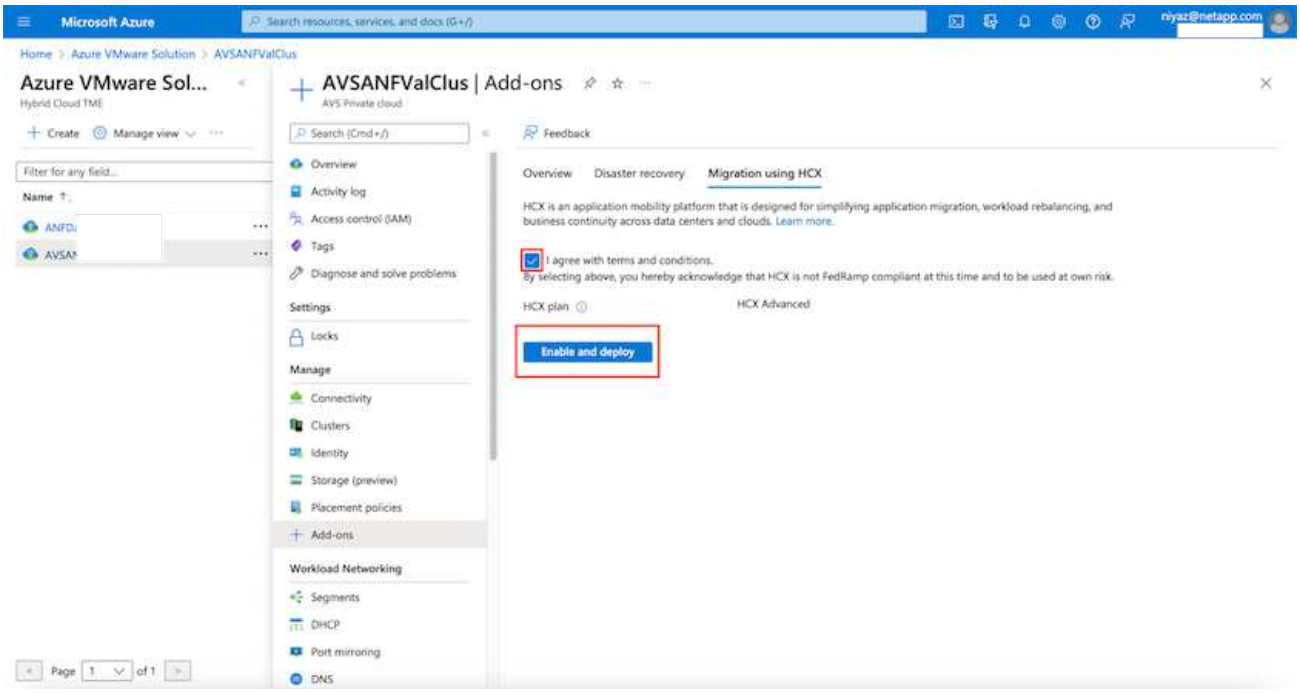
1. Efetue login no Portal do Azure e acesse a nuvem privada do Azure VMware Solution.
2. Selecione a nuvem privada apropriada e acesse os complementos. Isso pode ser feito navegando até **Gerenciar > Complementos**.
3. Na seção Mobilidade de carga de trabalho do HCX, clique em **Começar**.



4. Selecione a opção **Concordo com os Termos e Condições** e clique em **Ativar e Implantar**.

> ⓘ A implantação padrão é o HCX Advanced. Abra uma solicitação de suporte para habilitar a edição Enterprise.

> ⓘ A implantação leva aproximadamente de 25 a 30 minutos.



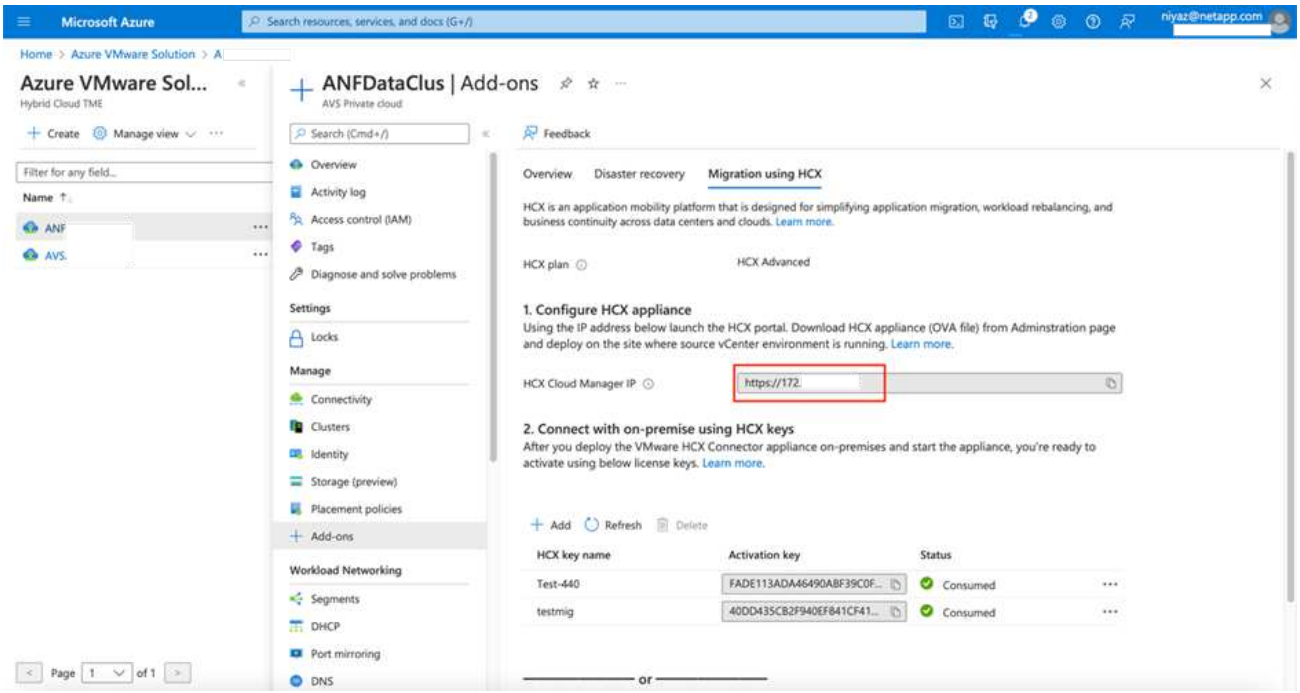
▼ **Etapa 2: implantar o instalador OVA no vCenter Server local**

Para que o conector local se conecte ao HCX Manager no Azure VMware Solution, certifique-se de que as portas de firewall apropriadas estejam abertas no ambiente local.

Para baixar e instalar o HCX Connector no vCenter Server local, conclua as seguintes etapas:

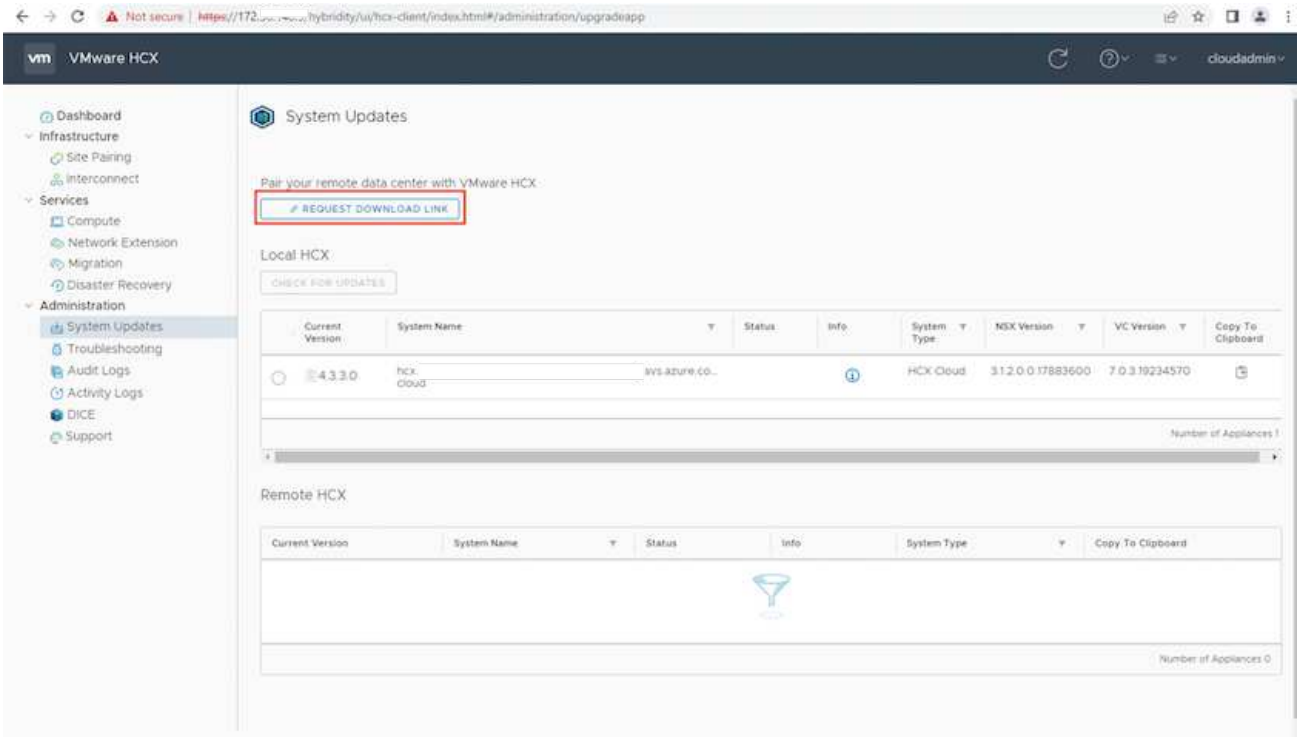
1. No portal do Azure, acesse a Solução VMware do Azure, selecione a nuvem privada e selecione **Gerenciar > Complementos > Migração** usando HCX e copie o portal do HCX Cloud Manager para baixar o arquivo OVA.

   Use as credenciais de usuário padrão do CloudAdmin para acessar o portal HCX.

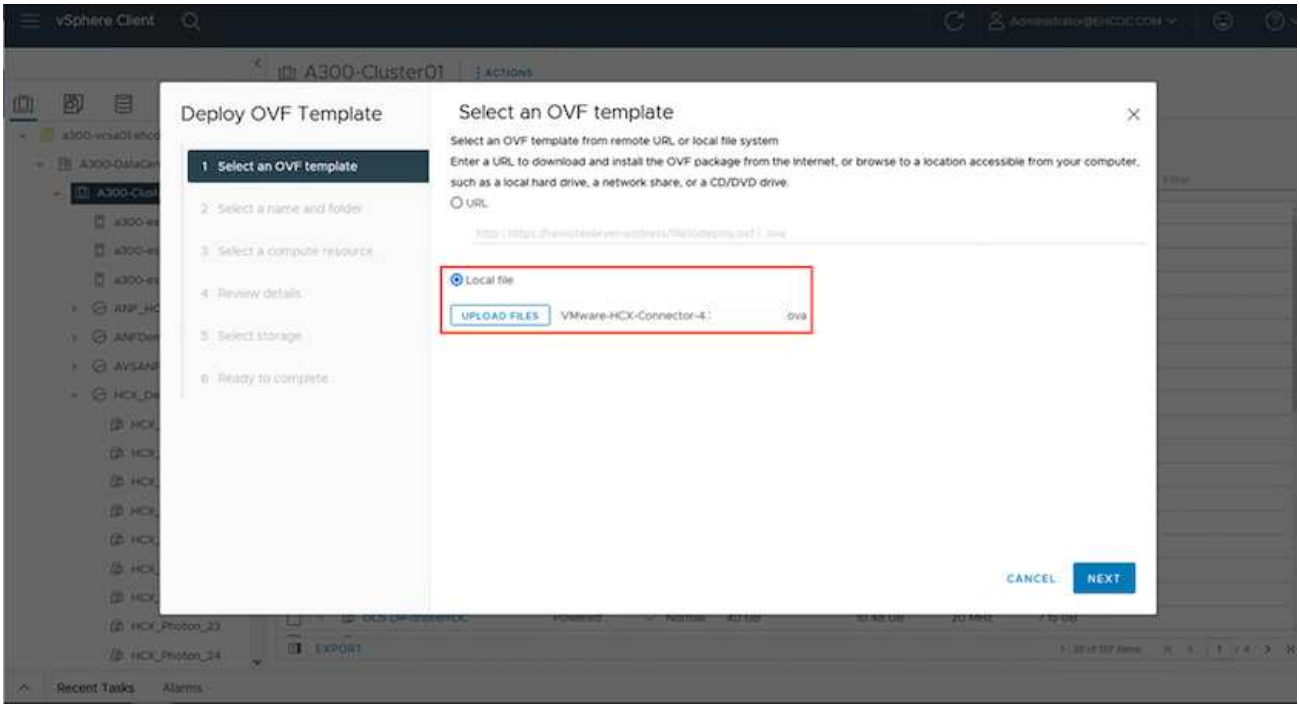


2. Depois de acessar o portal HCX com cloudadmin@vsphere.local usando o jumphost, navegue até **Administração > Atualizações do sistema** e clique em **Solicitar link de download**.

Baixe ou copie o link para o OVA e cole-o em um navegador para iniciar o processo de download do arquivo OVA do VMware HCX Connector para implantação no vCenter Server local.



3. Após o download do OVA, implante-o no ambiente VMware vSphere local usando a opção **Implantar modelo OVF**.



4. Insira todas as informações necessárias para a implantação do OVA, clique em **Avançar** e, em seguida, clique em **Concluir** para implantar o OVA do conector VMware HCX.

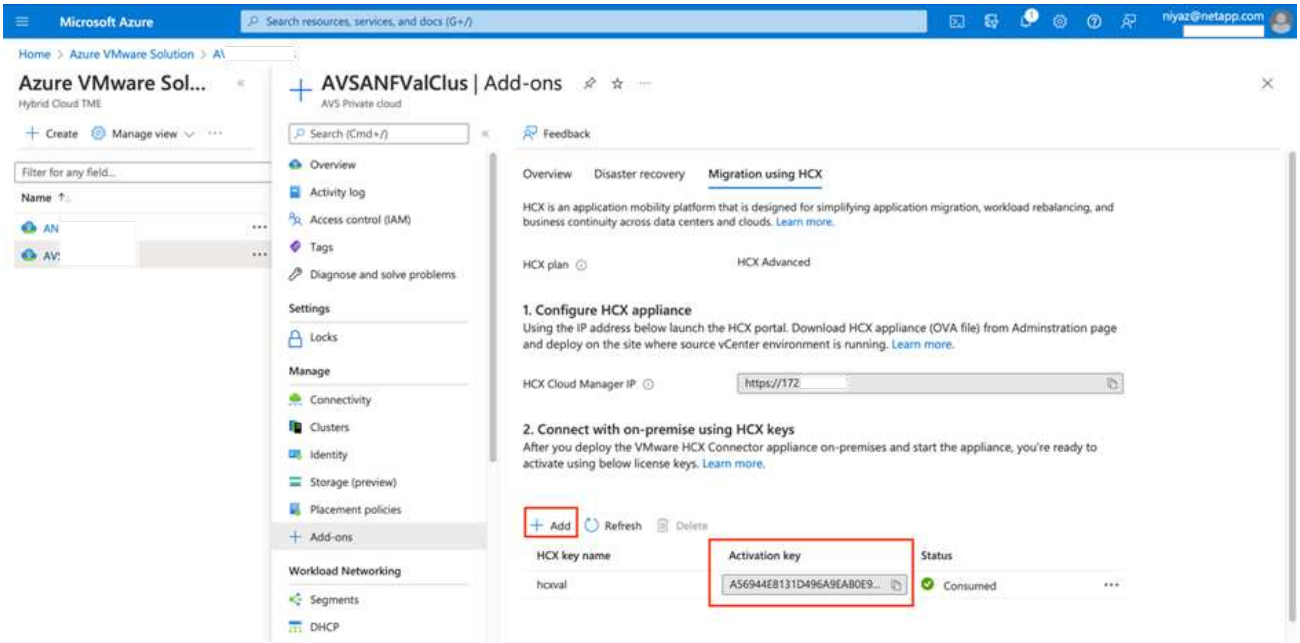
   Ligue o dispositivo virtual manualmente.

Para obter instruções passo a passo, consulte o "Guia do usuário do VMware HCX" .

▼ **Etapa 3: Ative o HCX Connector com a chave de licença**

Depois de implantar o VMware HCX Connector OVA no local e iniciar o dispositivo, conclua as seguintes etapas para ativar o HCX Connector. Gere a chave de licença no portal do Azure VMware Solution e ative-a no VMware HCX Manager.

1. No portal do Azure, acesse a Solução VMware do Azure, selecione a nuvem privada e selecione **Gerenciar > Complementos > Migração usando HCX**.
2. Em **Conectar com chaves HCX locais**, clique em **Adicionar** e copie a chave de ativação.



   Uma chave separada é necessária para cada conector HCX local implantado.

3. Efetue login no VMware HCX Manager local em "`https://hcxmanagerIP:9443`" usando credenciais de administrador.

   Use a senha definida durante a implantação do OVA.

4. No licenciamento, insira a chave copiada do passo 3 e clique em **Ativar**.

   O conector HCX local deve ter acesso à Internet.

5. Em **Local do datacenter**, forneça o local mais próximo para instalar o VMware HCX Manager no local. Clique em **Continuar**.
6. Em **Nome do sistema**, atualize o nome e clique em **Continuar**.
7. Clique em **Sim, Continuar**.

8. Em **Conectar seu vCenter**, forneça o nome de domínio totalmente qualificado (FQDN) ou endereço IP do vCenter Server e as credenciais apropriadas e clique em **Continuar**.

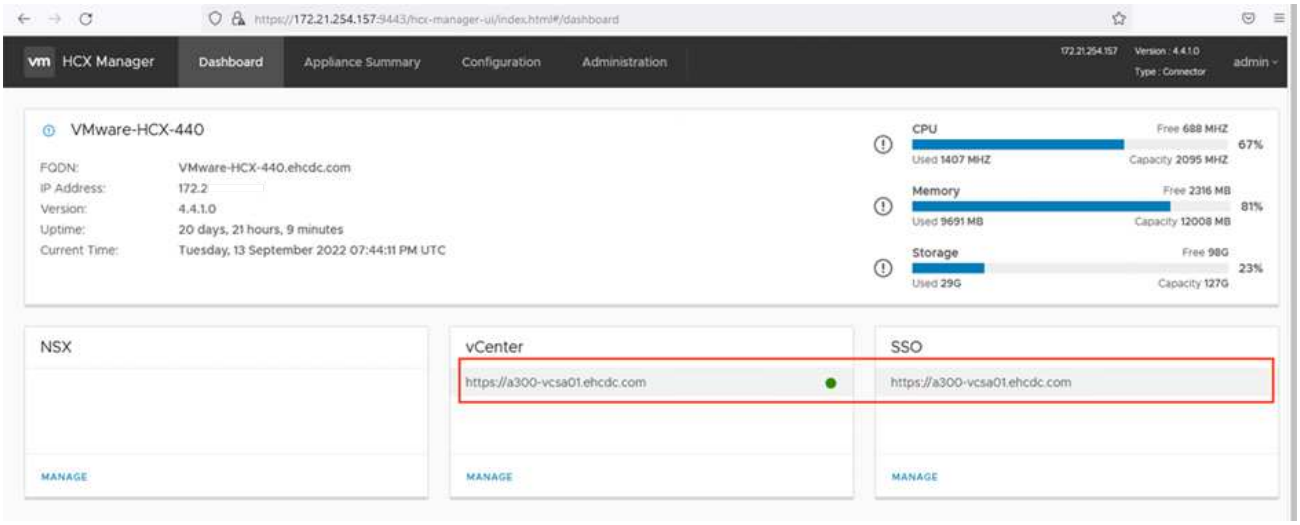
   Use o FQDN para evitar problemas de conectividade mais tarde.

9. Em **Configurar SSO/PSC**, forneça o FQDN ou endereço IP do Platform Services Controller e clique em **Continuar**.

   Digite o FQDN ou endereço IP do VMware vCenter Server.

10. Verifique se as informações inseridas estão corretas e clique em **Reiniciar**.
11. Após a reinicialização dos serviços, o vCenter Server é exibido em verde na página que aparece. Tanto o vCenter Server quanto o SSO devem ter os parâmetros de configuração apropriados, que devem ser os mesmos da página anterior.

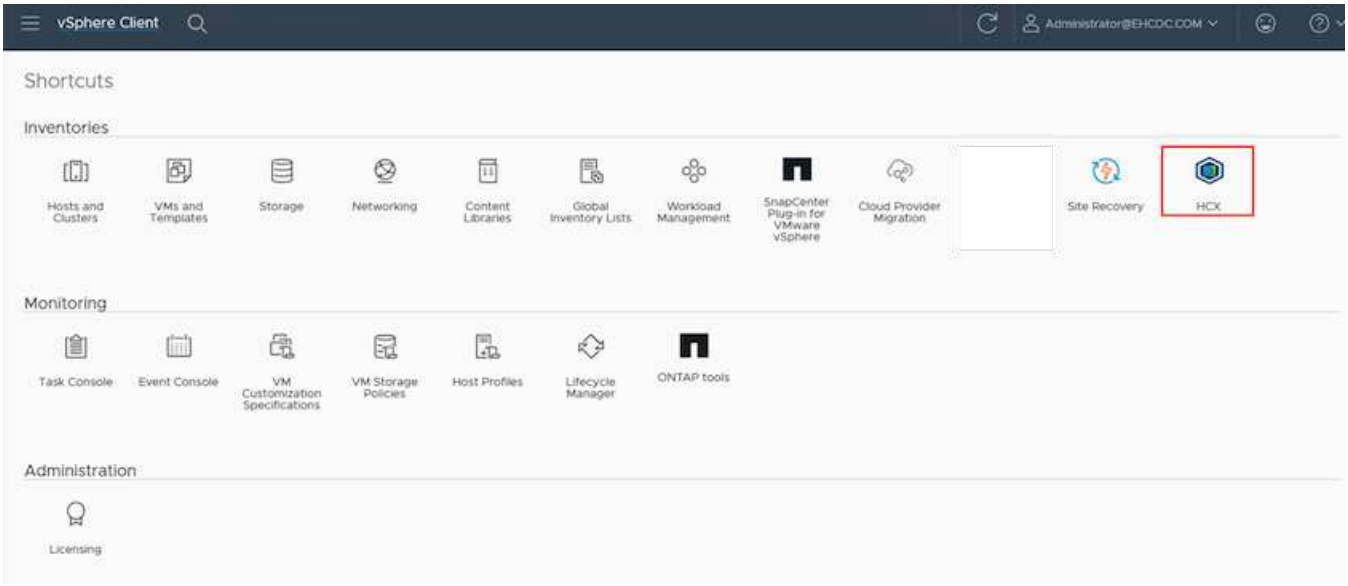
    Esse processo deve levar aproximadamente de 10 a 20 minutos para que o plug-in seja adicionado ao vCenter Server.



▼ **Etapa 4: emparelhe o VMware HCX Connector local com o Azure VMware Solution HCX Cloud Manager**

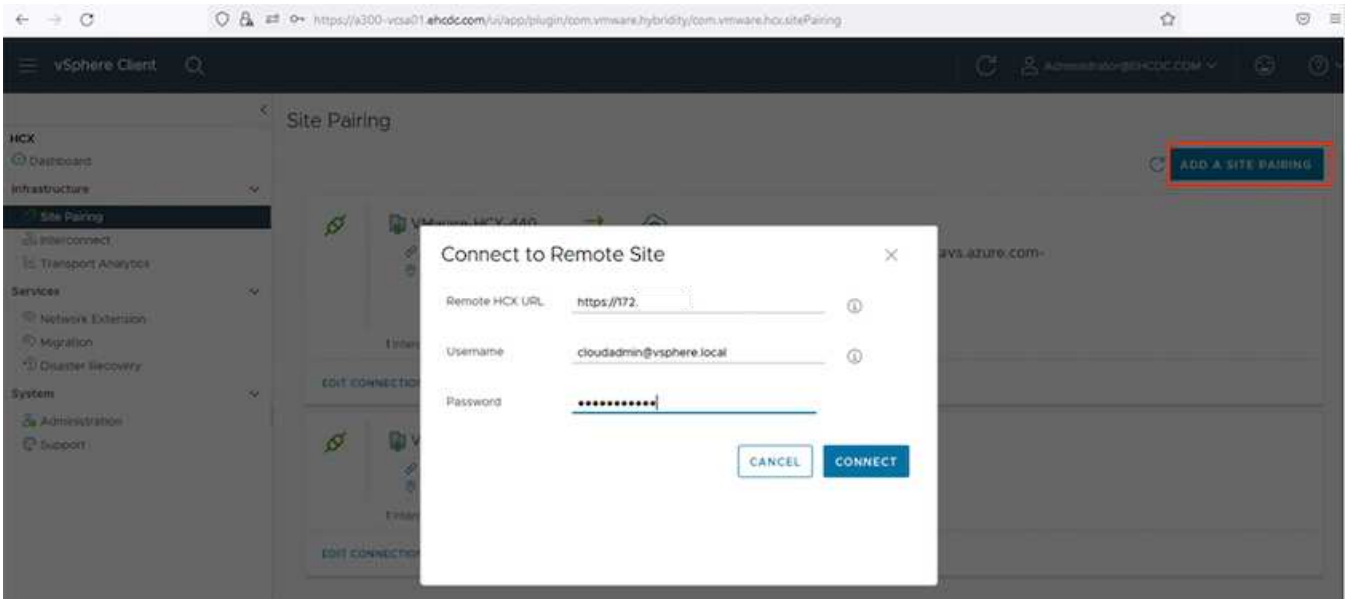
Depois que o HCX Connector for instalado no local e no Azure VMware Solution, configure o VMware HCX Connector local para a nuvem privada do Azure VMware Solution adicionando o emparelhamento. Para configurar o pareamento de sites, conclua as seguintes etapas:

1. Para criar um par de sites entre o ambiente vCenter local e o Azure VMware Solution SDDC, faça logon no vCenter Server local e acesse o novo plug-in HCX vSphere Web Client.



1. Em Infraestrutura, clique em **Adicionar um pareamento de sites**.

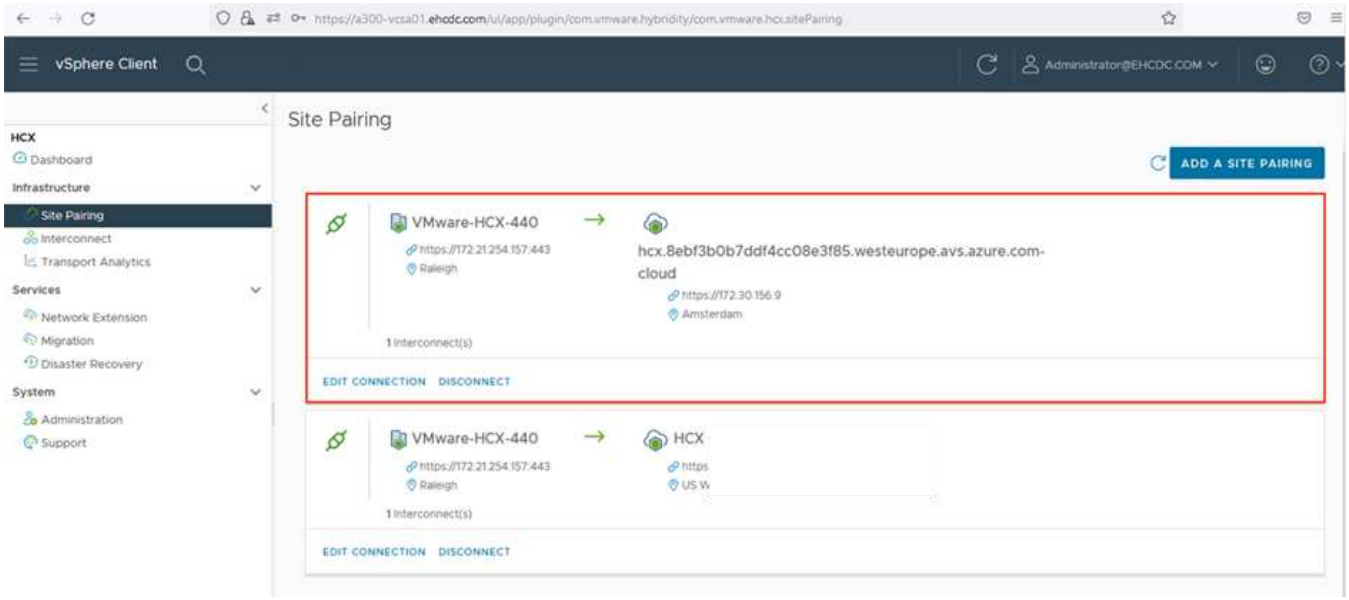
Insira a URL ou o endereço IP do Azure VMware Solution HCX Cloud Manager e as credenciais da função CloudAdmin para acessar a nuvem privada.



1. Clique em **Conectar**.

O VMware HCX Connector deve ser capaz de rotear para o IP do HCX Cloud Manager pela porta 443.

1. Após a criação do pareamento, o pareamento do site recém-configurado fica disponível no Painel do HCX.

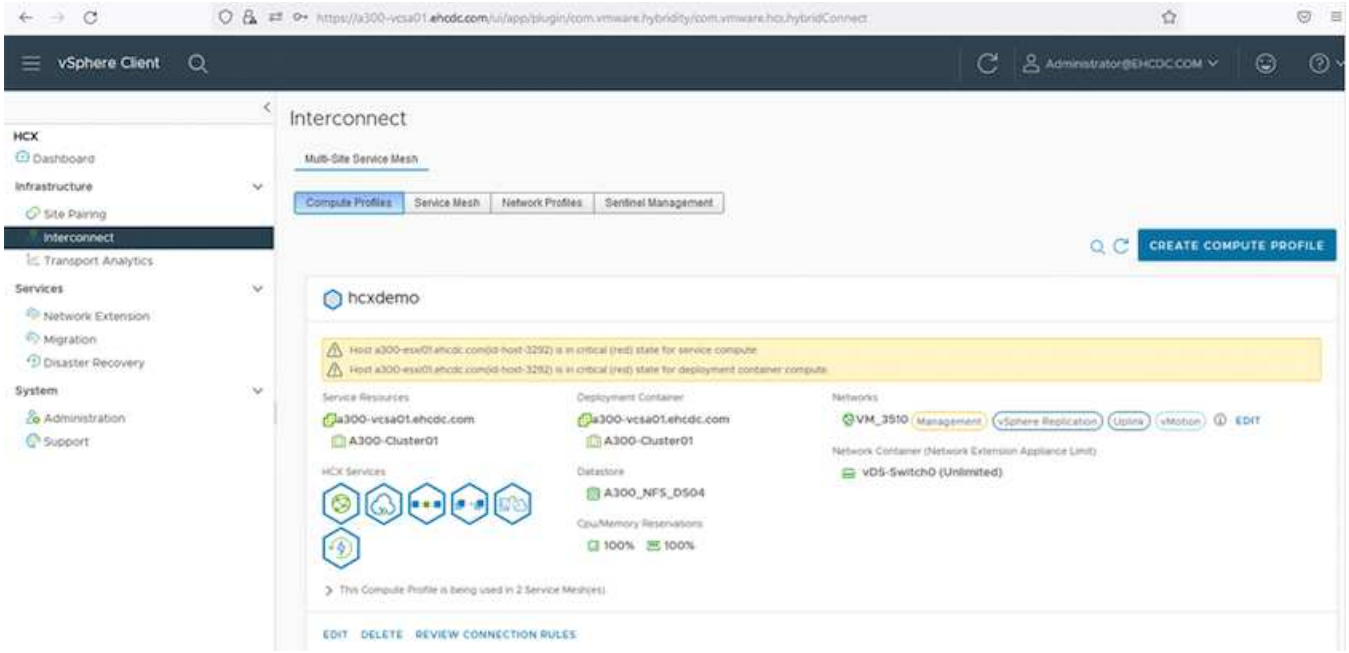


▼ **Etapa 5: configurar o perfil de rede, o perfil de computação e a malha de serviço**

O dispositivo de serviço VMware HCX Interconnect fornece recursos de replicação e migração baseados em vMotion pela Internet e conexões privadas com o site de destino. A interconexão fornece criptografia, engenharia de tráfego e mobilidade de VM. Para criar um dispositivo de serviço de interconexão, conclua as seguintes etapas:

1. Em Infraestrutura, selecione **Interconexão > Malha de serviço multisite > Perfis de computação > Criar perfil de computação**.

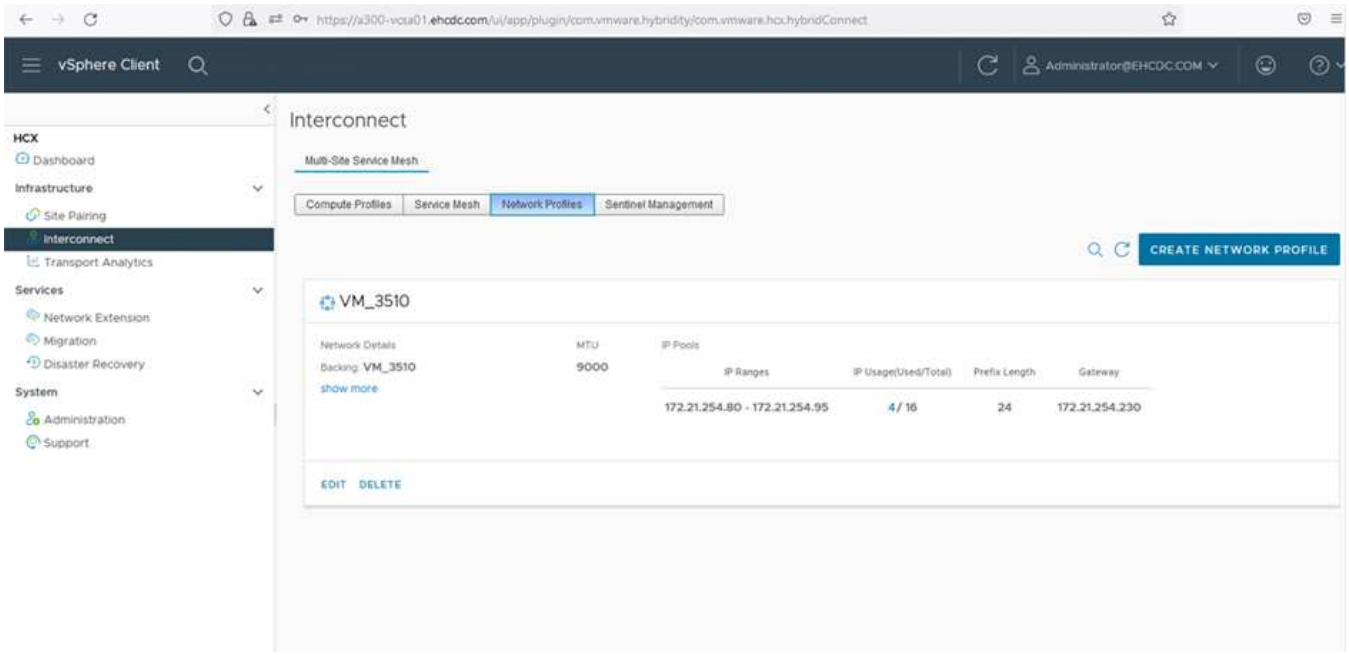
Os perfis de computação definem os parâmetros de implantação, incluindo os dispositivos que são implantados e quais partes do data center VMware são acessíveis ao serviço HCX.



1. Após a criação do perfil de computação, crie os perfis de rede selecionando **Multi-Site Service Mesh > Perfis de rede > Criar perfil de rede**.

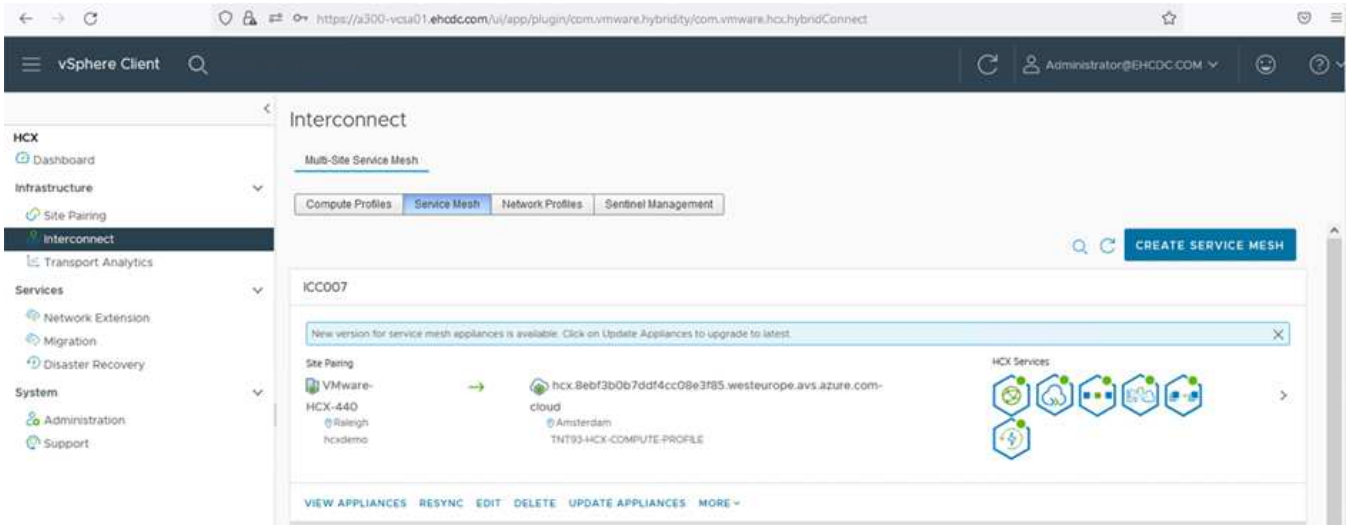
O perfil de rede define um intervalo de endereços IP e redes que são usados pelo HCX para seus dispositivos virtuais.

Esta etapa requer dois ou mais endereços IP. Esses endereços IP são atribuídos pela rede de gerenciamento aos dispositivos de interconexão.



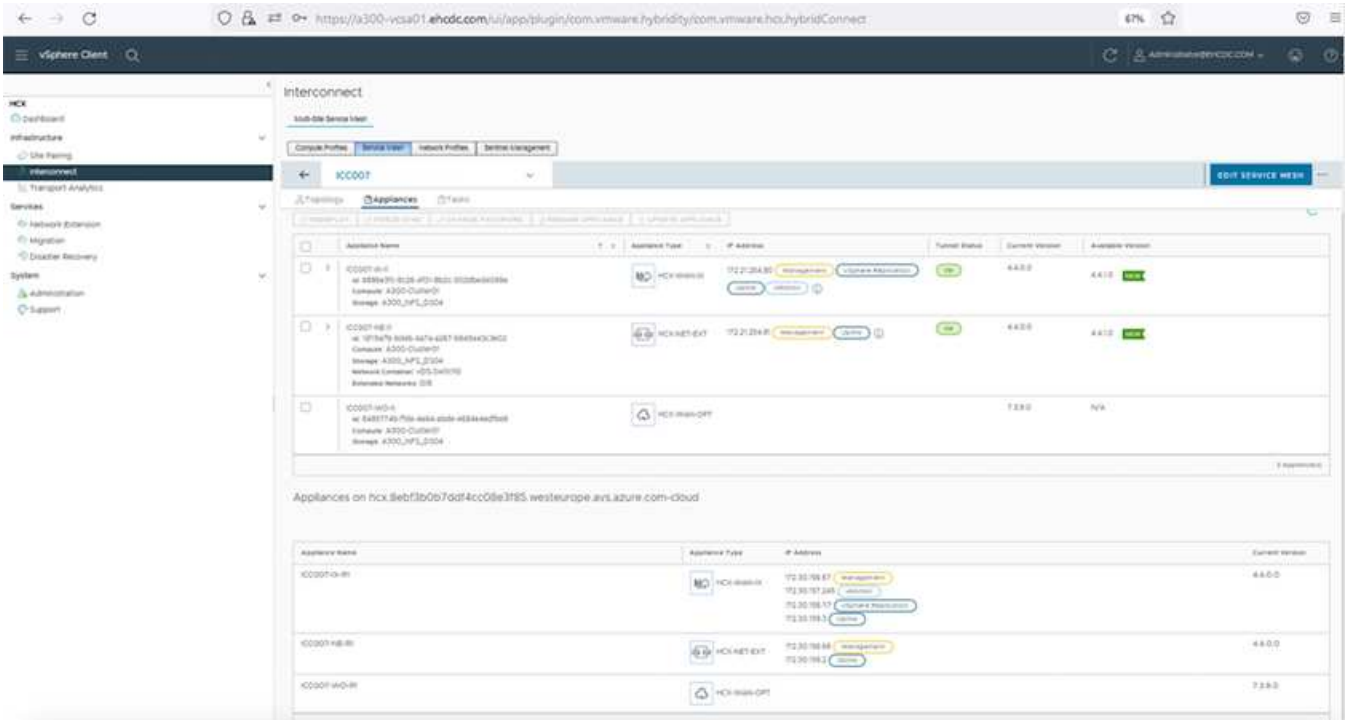
1. Neste momento, os perfis de computação e rede foram criados com sucesso.
2. Crie o Service Mesh selecionando a aba **Service Mesh** dentro da opção **Interconnect** e selecione os sites locais e do Azure SDDC.
3. O Service Mesh especifica um par de perfis de computação e rede locais e remotos.

Como parte desse processo, os dispositivos HCX são implantados e configurados automaticamente nos sites de origem e de destino para criar uma estrutura de transporte segura.



1. Esta é a etapa final da configuração. A implantação deve levar cerca de 30 minutos para ser concluída.

Após a configuração da malha de serviço, o ambiente estará pronto com os túneis IPsec criados com sucesso para migrar as VMs de carga de trabalho.



▼ **Etapa 6: migrar cargas de trabalho**

As cargas de trabalho podem ser migradas bidirecionalmente entre SDDCs locais e do Azure usando várias tecnologias de migração do VMware HCX. As VMs podem ser movidas de e para entidades ativadas pelo VMware HCX usando diversas tecnologias de migração, como migração em massa do HCX, HCX vMotion, migração a frio do HCX, HCX Replication Assisted vMotion (disponível com a edição HCX Enterprise) e HCX OS Assisted Migration (disponível com a edição HCX Enterprise).

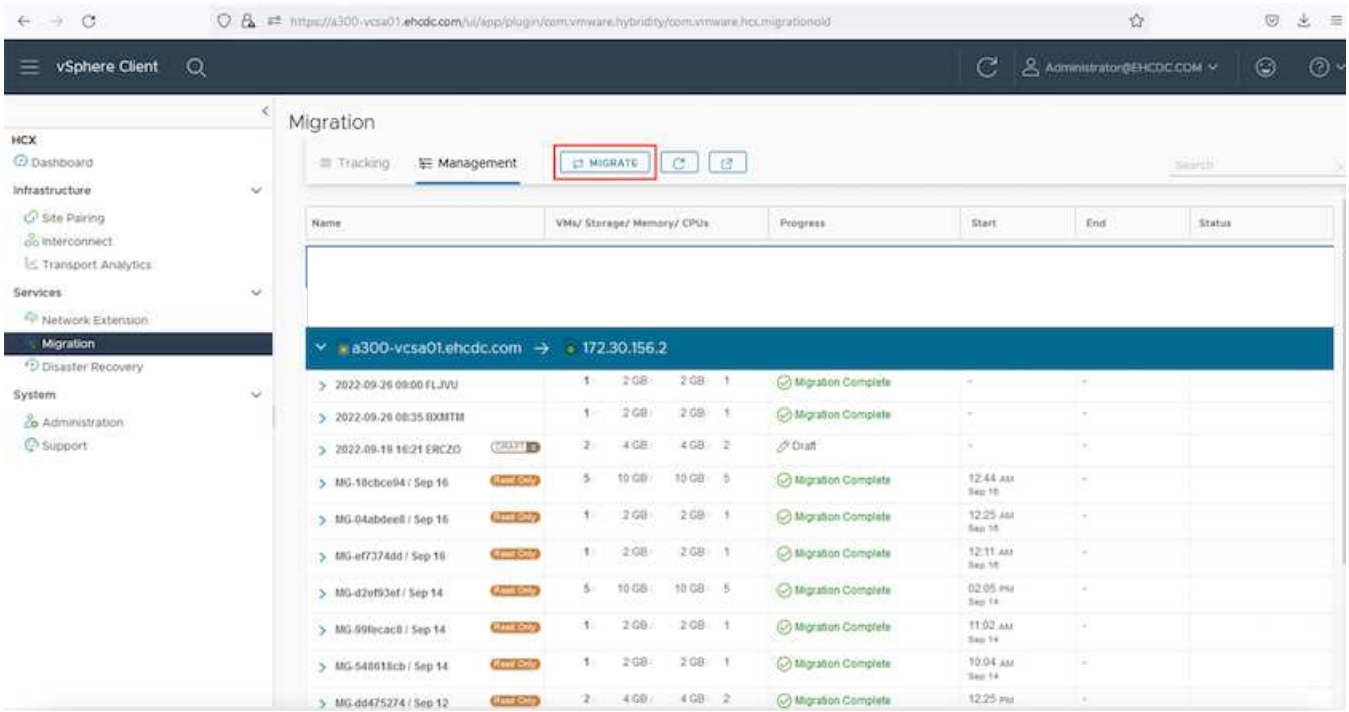
Para saber mais sobre os vários mecanismos de migração do HCX, consulte "Tipos de migração do VMware HCX" .

Migração em massa

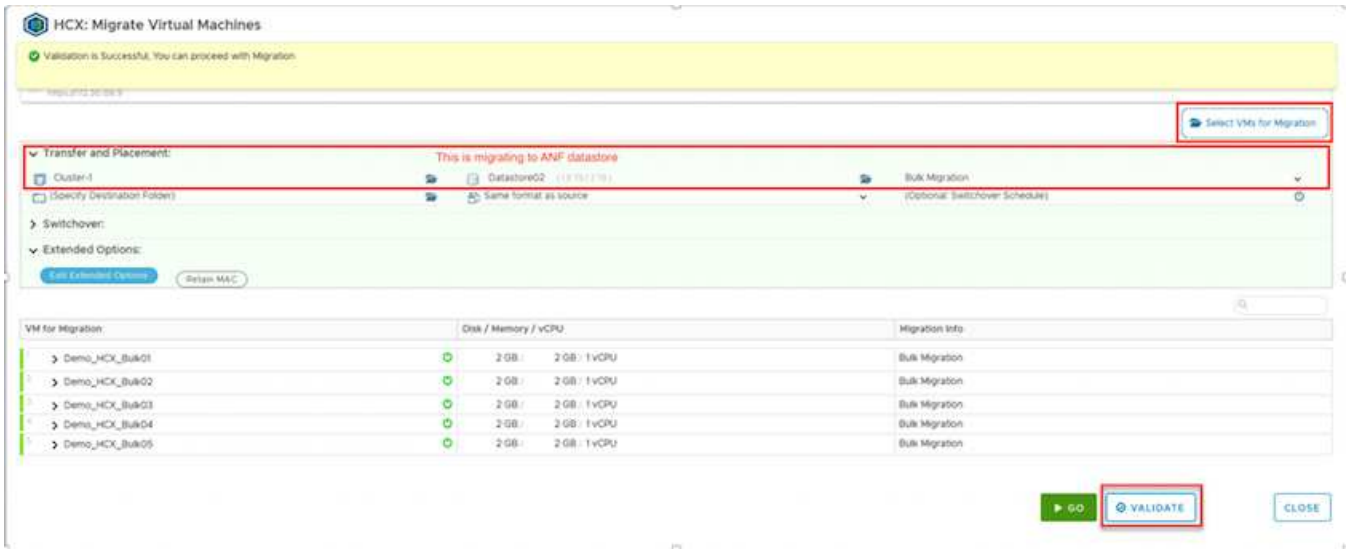
Esta seção detalha o mecanismo de migração em massa. Durante uma migração em massa, o recurso de migração em massa do HCX usa o vSphere Replication para migrar arquivos de disco enquanto recria a VM na instância do vSphere HCX de destino.

Para iniciar migrações em massa de VMs, conclua as seguintes etapas:

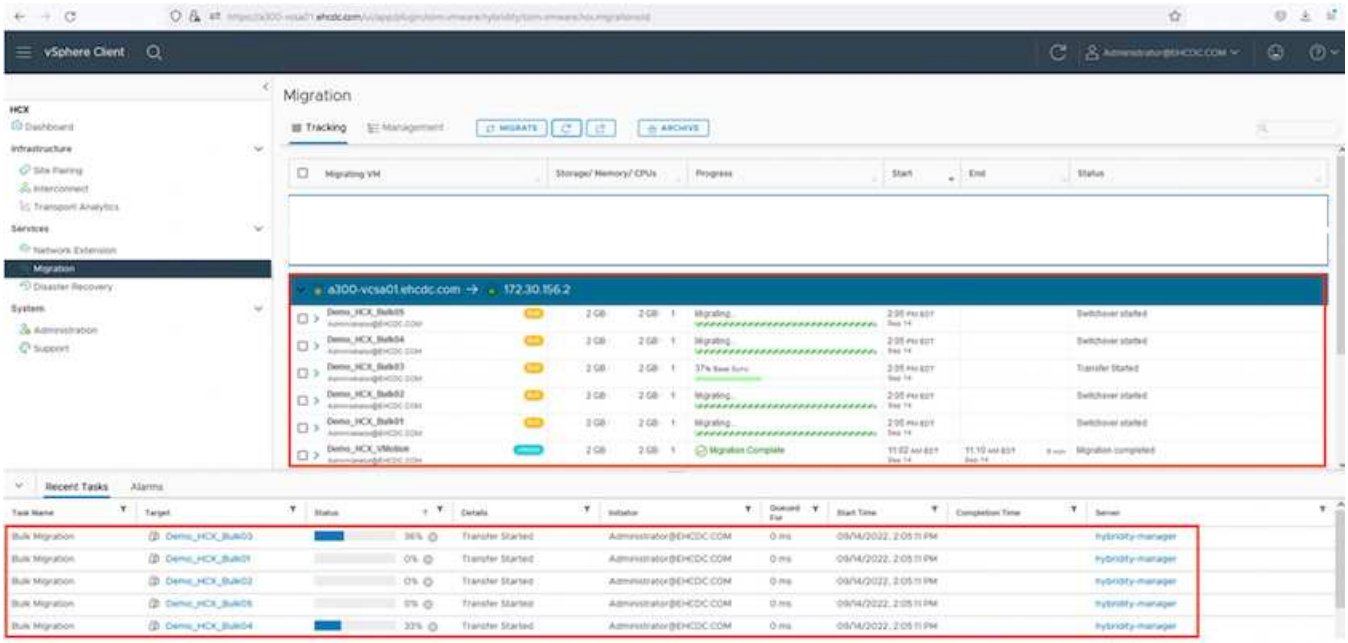
1. Acesse a aba **Migrar** em **Serviços > Migração**.



1. Em **Conexão de site remoto**, selecione a conexão de site remoto e selecione a origem e o destino. Neste exemplo, o destino é o ponto de extremidade SDDC HCX do Azure VMware Solution.
2. Clique em **Selecionar VMs para migração**. Isso fornece uma lista de todas as VMs locais. Selecione as VMs com base na expressão match:value e clique em **Adicionar**.
3. Na seção **Transferência e posicionamento**, atualize os campos obrigatórios (**Cluster**, **Armazenamento**, **Destino** e **Rede**), incluindo o perfil de migração, e clique em **Validar**.

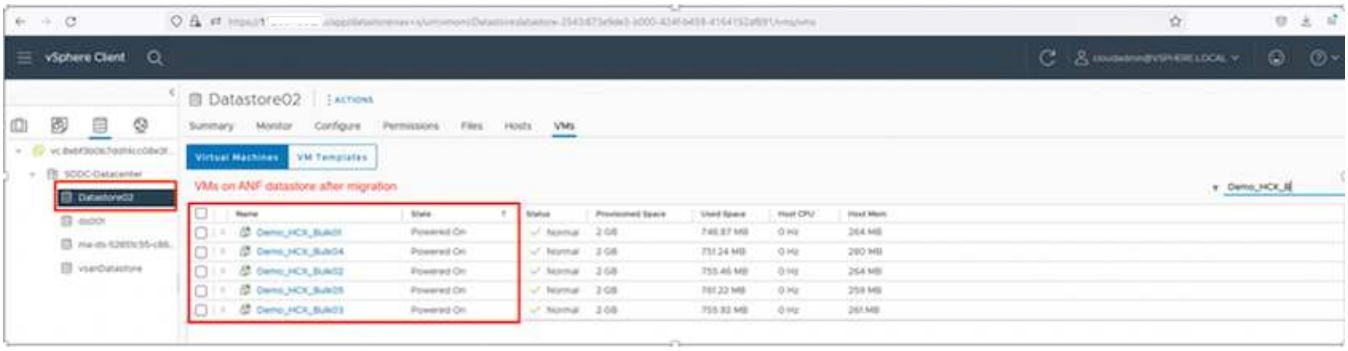


1. Após a conclusão das verificações de validação, clique em **Ir** para iniciar a migração.



Durante essa migração, um disco de espaço reservado é criado no armazenamento de dados especificado do Azure NetApp Files dentro do vCenter de destino para permitir a replicação dos dados do disco da VM de origem para os discos de espaço reservado. O HBR é acionado para uma sincronização completa com o alvo e, após a conclusão da linha de base, uma sincronização incremental é executada com base no ciclo do objetivo do ponto de recuperação (RPO). Após a conclusão da sincronização completa/incremental, a alternância é acionada automaticamente, a menos que uma programação específica seja definida.

1. Após a conclusão da migração, valide-a acessando o SDDC vCenter de destino.

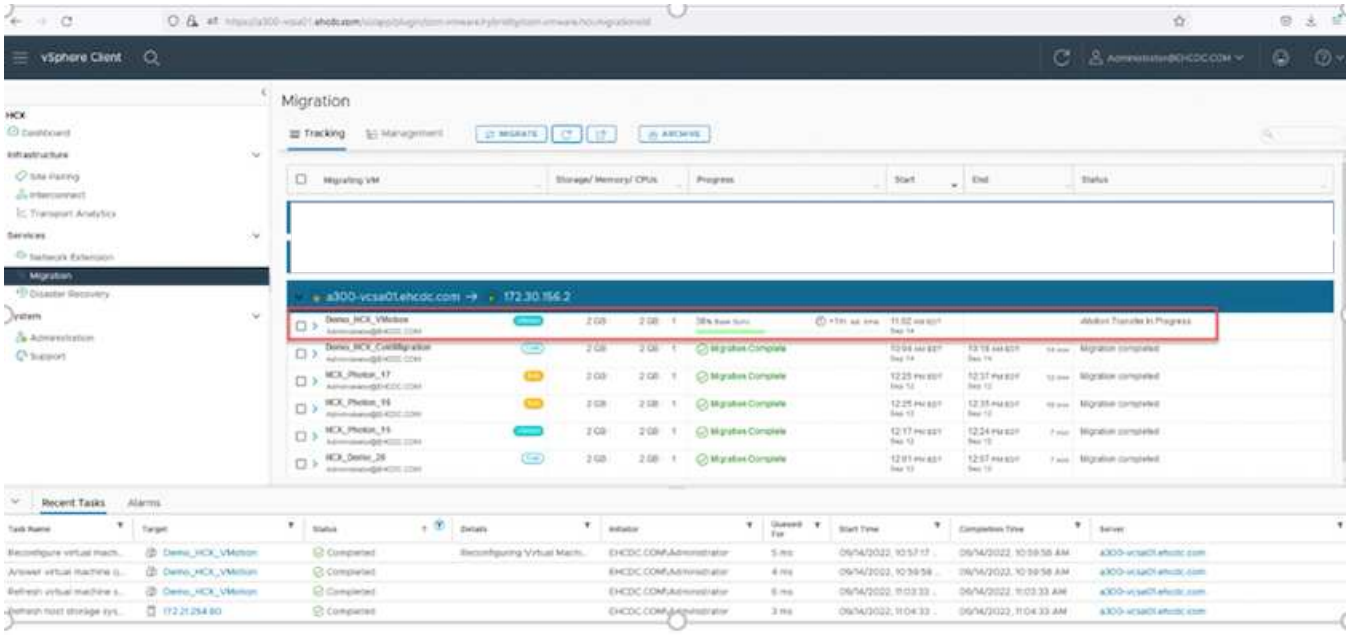


Para obter informações adicionais e detalhadas sobre várias opções de migração e sobre como migrar cargas de trabalho do local para o Azure VMware Solution usando HCX, consulte "Considerações sobre a migração do VMware HCX" .

Para saber mais sobre esse processo, assista ao vídeo a seguir:

Migração de carga de trabalho usando HCX

Aqui está uma captura de tela da opção HCX vMotion.



Para saber mais sobre esse processo, assista ao vídeo a seguir:

HCX vMotion

Certifique-se de que haja largura de banda suficiente disponível para lidar com a migração.

O armazenamento de dados ANF de destino deve ter espaço suficiente para lidar com a migração.

Conclusão

Não importa se você tem como alvo a nuvem híbrida ou totalmente em nuvem e dados residindo em qualquer tipo/fornecedor de armazenamento no local, o Azure NetApp Files e o HCX oferecem excelentes opções para implantar e migrar as cargas de trabalho do aplicativo, ao mesmo tempo em que reduzem o TCO ao tornar os requisitos de dados integrados à camada do aplicativo. Seja qual for o caso de uso, escolha o Azure VMware Solution juntamente com o Azure NetApp Files para rápida concretização dos benefícios da nuvem, infraestrutura consistente e operações em nuvens locais e múltiplas, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial. É o mesmo processo e procedimento familiar usado para conectar o armazenamento e migrar VMs usando VMware vSphere Replication, VMware vMotion ou até mesmo cópia de arquivo de rede (NFC).

Takeaways

Os pontos principais deste documento incluem:

- Agora você pode usar o Azure NetApp Files como um armazenamento de dados no Azure VMware Solution SDDC.
- Você pode migrar facilmente dados do local para o armazenamento de dados do Azure NetApp Files .
- Você pode facilmente aumentar e diminuir o armazenamento de dados do Azure NetApp Files para atender aos requisitos de capacidade e desempenho durante a atividade de migração.

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes links do site:

- Documentação da solução Azure VMware

"https://docs.microsoft.com/en-us/azure/azure-vmware/"

- Documentação do Azure NetApp Files

"https://docs.microsoft.com/en-us/azure/azure-netapp-files/"

- Considerações sobre a migração do VMware HCX

"https://learn.microsoft.com/en-us/azure/azure-vmware/architecture-migrate"

NetApp para GCP/GCVE

Recursos da NetApp para o Google Cloud Platform GCVE

Saiba mais sobre os recursos que a NetApp oferece ao Google Cloud VMware Engine (GCVE) do Google Cloud Platform (GCP) - desde o NetApp como um dispositivo de armazenamento conectado a convidados ou um armazenamento de dados NFS suplementar até a migração de fluxos de trabalho, extensão/intermitência para a nuvem, backup/restauração e recuperação de desastres.

Vá para a seção do conteúdo desejado selecionando entre as seguintes opções:

- "Configurando o GCVE no GCP"
- "Opções de armazenamento NetApp para GCVE"
- "Soluções de nuvem NetApp /VMware"

Configurando o GCVE no GCP

Assim como no local, planejar um ambiente de virtualização baseado em nuvem é essencial para um ambiente de produção bem-sucedido, pronto para criação de VMs e migração.

Esta seção descreve como configurar e gerenciar o GCVE e usá-lo em combinação com as opções disponíveis para conectar o armazenamento NetApp .

> O armazenamento no convidado é o único método suportado para conectar o Cloud Volumes ONTAP e o Google Cloud NetApp Volumes ao GCVE.

O processo de configuração pode ser dividido nas seguintes etapas:

- Implantar e configurar o GCVE
- Habilitar acesso privado ao GCVE

Veja o detalhado"etapas de configuração para GCVE" .

Opções de armazenamento NetApp para GCVE

O armazenamento NetApp pode ser utilizado de diversas maneiras — como um repositório de dados conectado ou como um repositório de dados NFS suplementar — dentro do GCP GCVE.

Por favor visite"Opções de armazenamento NetApp suportadas" para maiores informações.

O Google Cloud oferece suporte ao armazenamento NetApp nas seguintes configurações:

- Cloud Volumes ONTAP (CVO) como armazenamento conectado a convidados
- Google Cloud NetApp Volumes (NetApp Volumes) como armazenamento conectado a convidados
- Google Cloud NetApp Volumes (NetApp Volumes) como um armazenamento de dados NFS suplementar

Veja o detalhado"opções de armazenamento de conexão de convidado para GCVE" . Veja o detalhado"opções suplementares de armazenamento de dados NFS para GCVE" .

Leia mais sobre"Suporte ao armazenamento de dados do Google Cloud NetApp Volumes para o Google Cloud VMware Engine (blog da NetApp)" ou"Como usar o Google Cloud NetApp Volumes como armazenamento de dados para o Google Cloud VMware Engine (blog do Google)"

Casos de uso da solução

Com as soluções de nuvem da NetApp e da VMware, muitos casos de uso são simples de implantar no Azure AVS. Esses casos são definidos para cada uma das áreas de nuvem definidas pela VMware:

- Proteger (inclui recuperação de desastres e backup/restauração)
- Estender
- Migrar

"Navegue pelas soluções da NetApp para o Google Cloud GCVE"

Proteja cargas de trabalho no GCP/GCVE

Recuperação de desastres consistente com aplicativos com NetApp SnapCenter e Veeam Replication

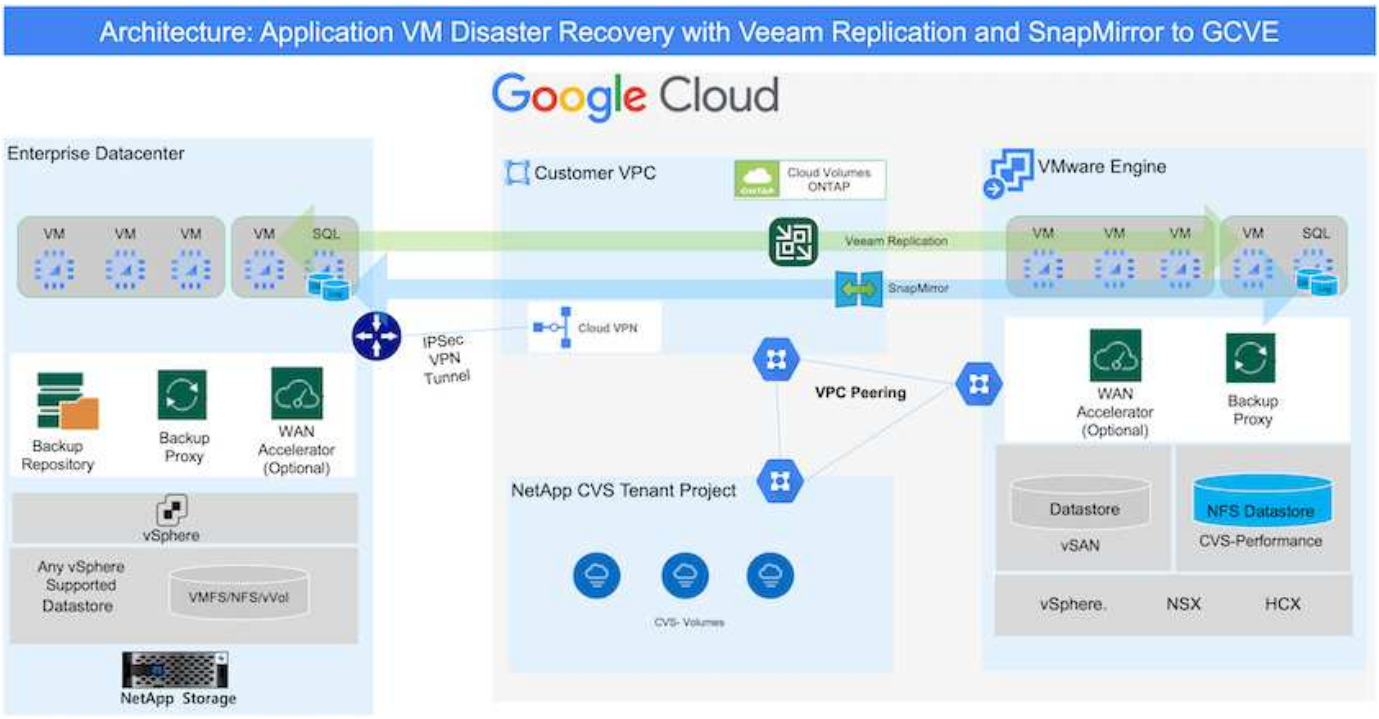
A recuperação de desastres na nuvem é uma maneira resiliente e econômica de proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados, como ransomware. Com o NetApp SnapMirror, as cargas de trabalho locais do VMware que usam armazenamento conectado ao convidado podem ser replicadas para o NetApp Cloud Volumes ONTAP em execução no Google Cloud.

Visão geral

Muitos clientes procuram uma solução eficaz de recuperação de desastres para suas VMs de aplicativos hospedadas no VMware vSphere. Muitos deles usam sua solução de backup existente para executar a recuperação durante desastres. Muitas vezes essa solução aumenta o RTO e não atende às expectativas. Para reduzir o RPO e o RTO, a replicação de VM da Veeam pode ser utilizada até mesmo do local para o GCVE, desde que a conectividade de rede e o ambiente com permissões apropriadas estejam disponíveis. OBSERVAÇÃO: O Veeam VM Replication não protege dispositivos de armazenamento conectados a VMs convidadas, como montagens iSCSI ou NFS dentro da VM convidada. É preciso proteger cada um separadamente.

Para replicação consistente de aplicativos para SQL VM e para reduzir o RTO, usamos o SnapCenter para orquestrar operações do SnapMirror de volumes de log e banco de dados SQL.

Este documento fornece uma abordagem passo a passo para configurar e executar a recuperação de desastres que usa o NetApp SnapMirror, o Veeam e o Google Cloud VMware Engine (GCVE).



Suposições

Este documento se concentra no armazenamento no convidado para dados de aplicativos (também conhecido como convidado conectado), e presumimos que o ambiente local esteja usando o SnapCenter para backups consistentes com aplicativos.

> Este documento se aplica a qualquer solução de backup ou recuperação de terceiros. Dependendo da solução usada no ambiente, siga as práticas recomendadas para criar políticas de backup que atendam aos SLAs organizacionais.

Para conectividade entre o ambiente local e a rede do Google Cloud, use opções de conectividade como interconexão dedicada ou Cloud VPN. Os segmentos devem ser criados com base no design da VLAN local.

> Há várias opções para conectar datacenters locais ao Google Cloud, o que nos impede de descrever um fluxo de trabalho específico neste documento. Consulte a documentação do Google Cloud para saber o método apropriado de conectividade local com o Google.

Implementando a solução de DR

Visão geral da implantação da solução

1. Certifique-se de que os dados do aplicativo sejam copiados usando o SnapCenter com os requisitos de RPO necessários.
2. Provisione o Cloud Volumes ONTAP com o tamanho de instância correto usando o NetApp Console na assinatura e na rede virtual apropriadas.

a. Configure o SnapMirror para os volumes de aplicativos relevantes.

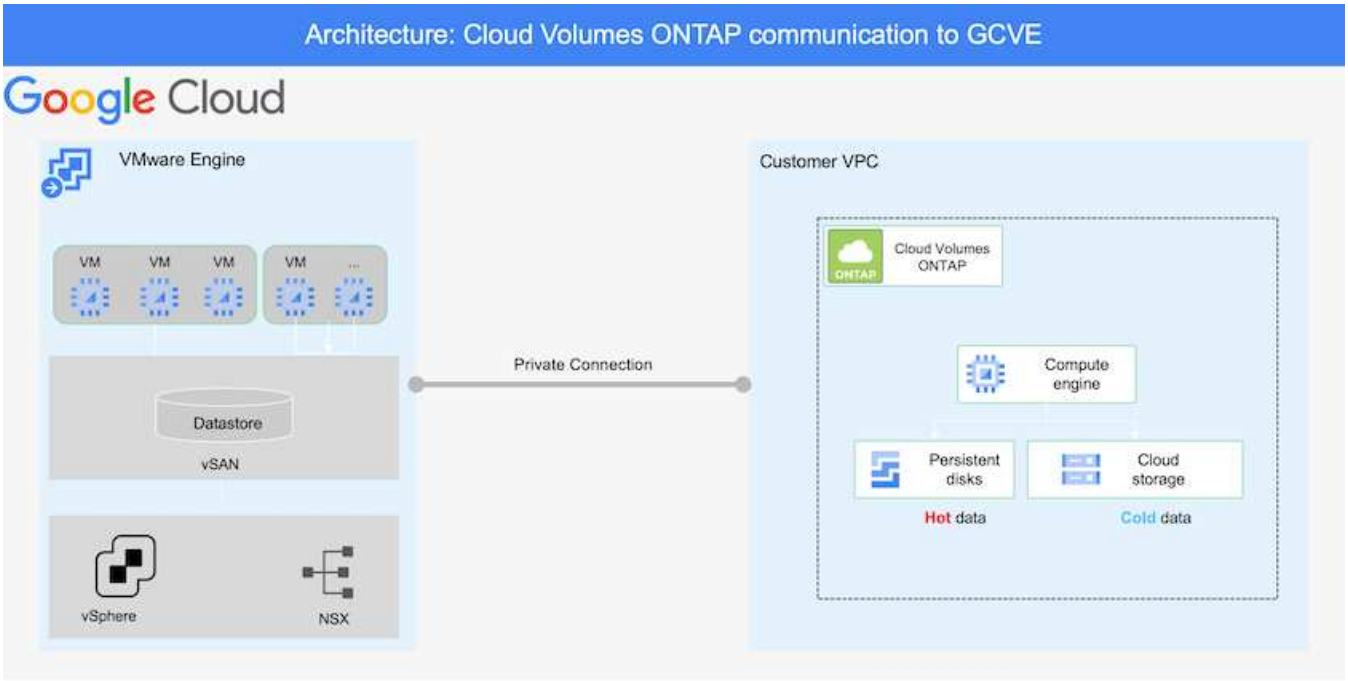
b. Atualize as políticas de backup no SnapCenter para acionar atualizações do SnapMirror após os trabalhos agendados.

3. Instale o software Veeam e comece a replicar máquinas virtuais para a instância do Google Cloud VMware Engine.
4. Durante um evento de desastre, interrompa a relação do SnapMirror usando o NetApp Console e acione o failover das máquinas virtuais com o Veeam.
   a. Reconecte os LUNs ISCSI e as montagens NFS para as VMs do aplicativo.
   b. Abra inscrições on-line.
5. Invoque o failback para o site protegido por meio da ressincronização reversa do SnapMirror após a recuperação do site primário.

Detalhes da implantação

▼ **Configurar o CVO no Google Cloud e replicar volumes para o CVO**

O primeiro passo é configurar o Cloud Volumes ONTAP no Google Cloud ("cvo") e replicar os volumes desejados para o Cloud Volumes ONTAP com as frequências e retenções de snapshots desejadas.



Para obter instruções passo a passo sobre como configurar o SnapCenter e replicar os dados, consulte"Configurar replicação com SnapCenter"

Revisão da proteção de VM SQL com SnapCenter

▼ **Configurar hosts GCVE e acesso a dados CVO**

Dois fatores importantes a serem considerados ao implantar o SDDC são o tamanho do cluster SDDC na solução GCVE e por quanto tempo o SDDC será mantido em serviço. Essas duas considerações importantes para uma solução de recuperação de desastres ajudam a reduzir os custos operacionais gerais. O SDDC pode ter apenas três hosts ou até mesmo um cluster de vários hosts em uma implantação em grande escala.

O Google Cloud NetApp Volumes para NFS Datastore e o Cloud Volumes ONTAP para bancos de dados e logs SQL podem ser implantados em qualquer VPC e o GCVE deve ter conexão privada com essa VPC para montar o NFS Datastore e fazer com que a VM se conecte aos LUNs iSCSI.

Para configurar o GCVE SDDC, consulte"Implantar e configurar o ambiente de virtualização no Google Cloud Platform (GCP)" . Como pré-requisito, verifique se as VMs convidadas que residem nos hosts GCVE conseguem consumir dados do Cloud Volumes ONTAP depois que a conectividade for estabelecida.

Depois que o Cloud Volumes ONTAP e o GCVE forem configurados corretamente, comece a configurar o Veeam para automatizar a recuperação de cargas de trabalho locais para o GCVE (VMs com VMDKs de aplicativo e VMs com armazenamento no guest) usando o recurso Veeam Replication e aproveitando o SnapMirror para cópias de volumes de aplicativo para o Cloud Volumes ONTAP.

▼ **Instalar componentes Veeam**

Com base no cenário de implantação, o servidor de backup, o repositório de backup e o proxy de backup da Veeam precisam ser implantados. Para este caso de uso, não há necessidade de implantar o repositório de objetos para o Veeam e o repositório de escalonamento também não é obrigatório. "Consulte a documentação do Veeam para o procedimento de instalação" Para obter informações adicionais, consulte"Migração com Veeam Replication"

▼ **Configurar replicação de VM com Veeam**

Tanto o vCenter local quanto o vCenter GCVE precisam ser registrados no Veeam. "Configurar tarefa de replicação de VM do vSphere" Na etapa Processamento de Convidado do assistente, selecione desabilitar processamento de aplicativo, pois utilizaremos o SnapCenter para backup e recuperação com reconhecimento de aplicativo.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=8b7e4a9b-7de1-4d48-a8e2-b01200f00692

▼ **Failover da VM do Microsoft SQL Server**

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=9762dc99-081b-41a2-ac68-b01200f00ac0

Benefícios desta solução

- Utiliza a replicação eficiente e resiliente do SnapMirror.
- Recupera para quaisquer pontos disponíveis no tempo com retenção de instantâneos ONTAP .
- A automação completa está disponível para todas as etapas necessárias para recuperar centenas a milhares de VMs, desde as etapas de armazenamento, computação, rede e validação de aplicativos.
- O SnapCenter usa mecanismos de clonagem que não alteram o volume replicado.
  - Isso evita o risco de corrupção de dados para volumes e instantâneos.
  - Evita interrupções de replicação durante fluxos de trabalho de teste de DR.
  - Aproveita os dados de DR para fluxos de trabalho além de DR, como desenvolvimento/teste, testes de segurança, testes de patch e atualização e testes de remediação.
- O Veeam Replication permite alterar endereços IP de VM no site de DR.

Recuperação de desastres de aplicativos com SnapCenter, Cloud Volumes ONTAP e Veeam Replication

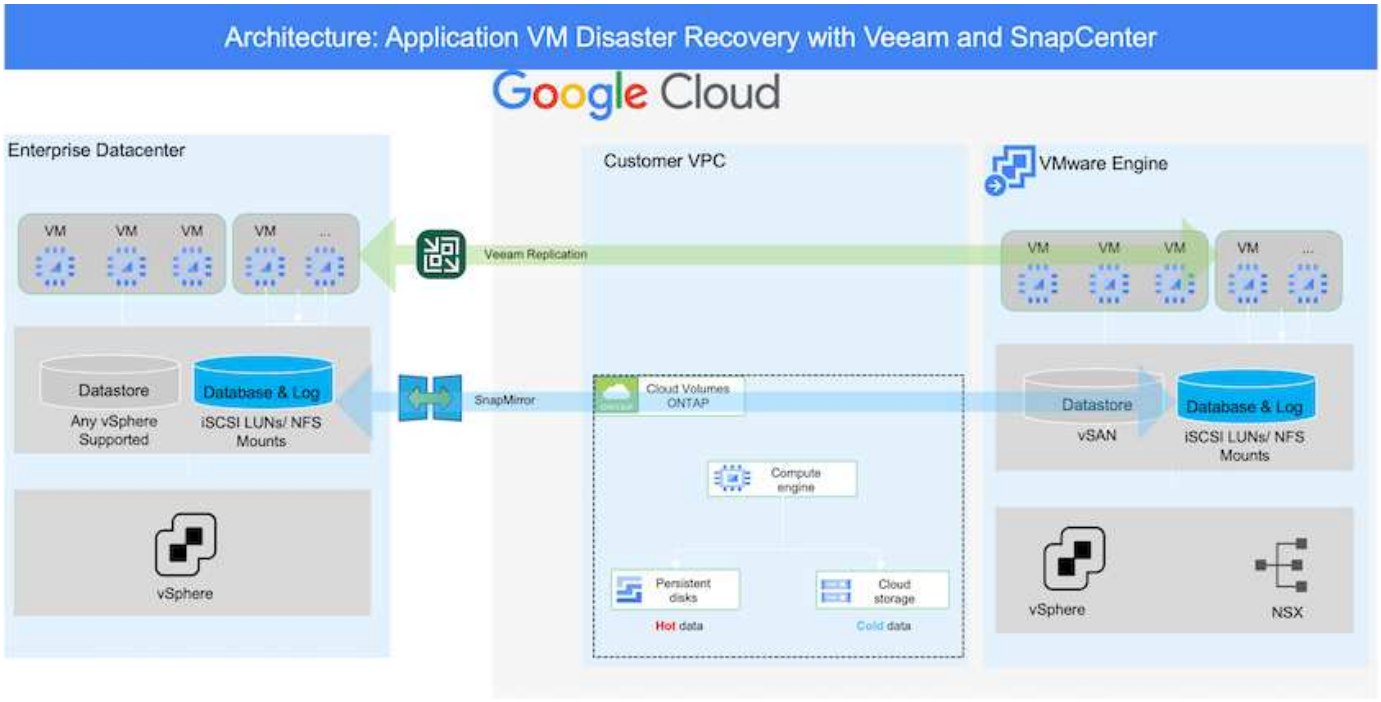
A recuperação de desastres na nuvem é uma maneira resiliente e econômica de

proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados, como ransomware. Com o NetApp SnapMirror, as cargas de trabalho locais do VMware que usam armazenamento conectado ao convidado podem ser replicadas para o NetApp Cloud Volumes ONTAP em execução no Google Cloud.

Visão geral

Isso abrange dados de aplicativos; no entanto, e as VMs em si? A recuperação de desastres deve abranger todos os componentes dependentes, incluindo máquinas virtuais, VMDKs, dados de aplicativos e muito mais. Para fazer isso, o SnapMirror junto com o Veeam pode ser usado para recuperar perfeitamente cargas de trabalho replicadas do local para o Cloud Volumes ONTAP enquanto usa armazenamento vSAN para VMDKs de VM.

Este documento fornece uma abordagem passo a passo para configurar e executar a recuperação de desastres que usa o NetApp SnapMirror, o Veeam e o Google Cloud VMware Engine (GCVE).



Suposições

Este documento se concentra no armazenamento no convidado para dados de aplicativos (também conhecido como convidado conectado), e presumimos que o ambiente local esteja usando o SnapCenter para backups consistentes com aplicativos.

Este documento se aplica a qualquer solução de backup ou recuperação de terceiros. Dependendo da solução usada no ambiente, siga as práticas recomendadas para criar políticas de backup que atendam aos SLAs organizacionais.

Para conectividade entre o ambiente local e a rede do Google Cloud, use opções de conectividade como interconexão dedicada ou Cloud VPN. Os segmentos devem ser criados com base no design da VLAN local.

Há várias opções para conectar datacenters locais ao Google Cloud, o que nos impede de descrever um fluxo de trabalho específico neste documento. Consulte a documentação do

Google Cloud para saber o método apropriado de conectividade local com o Google.

Implementando a solução de DR

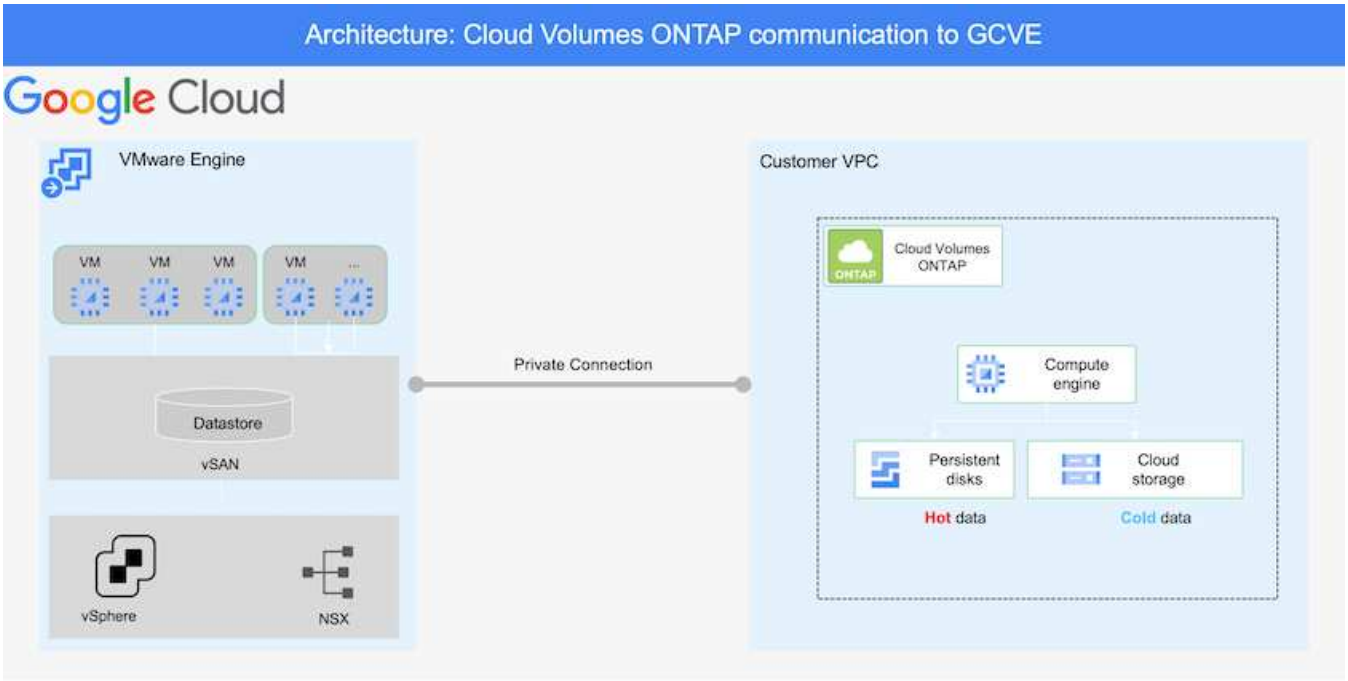
Visão geral da implantação da solução

1. Certifique-se de que os dados do aplicativo sejam copiados usando o SnapCenter com os requisitos de RPO necessários.
2. Provisione o Cloud Volumes ONTAP com o tamanho de instância correto usando o Cloud Manager dentro da assinatura e rede virtual apropriadas.
   a. Configure o SnapMirror para os volumes de aplicativos relevantes.
   b. Atualize as políticas de backup no SnapCenter para acionar atualizações do SnapMirror após os trabalhos agendados.
3. Instale o software Veeam e comece a replicar máquinas virtuais para a instância do Google Cloud VMware Engine.
4. Durante um evento de desastre, interrompa o relacionamento do SnapMirror usando o Cloud Manager e acione o failover de máquinas virtuais com o Veeam.
   a. Reconecte os LUNs ISCSI e as montagens NFS para as VMs do aplicativo.
   b. Abra inscrições on-line.
5. Invoque o failback para o site protegido por meio da ressincronização reversa do SnapMirror após a recuperação do site primário.

Detalhes da implantação

▼ **Configurar o CVO no Google Cloud e replicar volumes para o CVO**

O primeiro passo é configurar o Cloud Volumes ONTAP no Google Cloud ("cvo") e replicar os volumes desejados para o Cloud Volumes ONTAP com as frequências e retenções de snapshots desejadas.



Para obter instruções passo a passo sobre como configurar o SnapCenter e replicar os dados,

consulte"Configurar replicação com SnapCenter"

Configurar replicação com SnapCenter

▼ **Configurar hosts GCVE e acesso a dados CVO**

Dois fatores importantes a serem considerados ao implantar o SDDC são o tamanho do cluster SDDC na solução GCVE e por quanto tempo o SDDC será mantido em serviço. Essas duas considerações importantes para uma solução de recuperação de desastres ajudam a reduzir os custos operacionais gerais. O SDDC pode ter apenas três hosts ou até mesmo um cluster de vários hosts em uma implantação em grande escala.

O Cloud Volumes ONTAP pode ser implantado em qualquer VPC e o GCVE deve ter conexão privada com essa VPC para que a VM se conecte aos LUNs iSCSI.

Para configurar o GCVE SDDC, consulte"Implantar e configurar o ambiente de virtualização no Google Cloud Platform (GCP)" . Como pré-requisito, verifique se as VMs convidadas que residem nos hosts GCVE conseguem consumir dados do Cloud Volumes ONTAP depois que a conectividade for estabelecida.

Depois que o Cloud Volumes ONTAP e o GCVE forem configurados corretamente, comece a configurar o Veeam para automatizar a recuperação de cargas de trabalho locais para o GCVE (VMs com VMDKs de aplicativo e VMs com armazenamento no guest) usando o recurso Veeam Replication e aproveitando o SnapMirror para cópias de volumes de aplicativo para o Cloud Volumes ONTAP.

▼ **Instalar componentes Veeam**

Com base no cenário de implantação, o servidor de backup, o repositório de backup e o proxy de backup da Veeam precisam ser implantados. Para este caso de uso, não há necessidade de implantar o repositório de objetos para o Veeam e o repositório de escalonamento também não é obrigatório.https://helpcenter.veeam.com/docs/backup/qsg_vsphere/deployment_scenarios.html["Consulte a documentação do Veeam para o procedimento de instalação"]

▼ **Configurar replicação de VM com Veeam**

Tanto o vCenter local quanto o vCenter GCVE precisam ser registrados no Veeam. "Configurar tarefa de replicação de VM do vSphere" Na etapa Processamento de Convidado do assistente, selecione desabilitar processamento de aplicativo, pois utilizaremos o SnapCenter para backup e recuperação com reconhecimento de aplicativo.

Configurar tarefa de replicação de VM do vSphere

▼ **Failover da VM do Microsoft SQL Server**

Failover da VM do Microsoft SQL Server

Benefícios desta solução

- Utiliza a replicação eficiente e resiliente do SnapMirror.
- Recupera para quaisquer pontos disponíveis no tempo com retenção de instantâneos ONTAP .
- A automação completa está disponível para todas as etapas necessárias para recuperar centenas a milhares de VMs, desde as etapas de armazenamento, computação, rede e validação de aplicativos.
- O SnapCenter usa mecanismos de clonagem que não alteram o volume replicado.
  - Isso evita o risco de corrupção de dados para volumes e instantâneos.
  - Evita interrupções de replicação durante fluxos de trabalho de teste de DR.
  - Aproveita os dados de DR para fluxos de trabalho além de DR, como desenvolvimento/teste, testes de

segurança, testes de patch e atualização e testes de remediação.

- O Veeam Replication permite alterar endereços IP de VM no site de DR.

Usando o Veeam Replication e o armazenamento de dados do Google Cloud NetApp Volumes para recuperação de desastres no Google Cloud VMware Engine

Um plano abrangente de recuperação de desastres é essencial para empresas em tempos de crise. Muitas organizações utilizam a computação em nuvem para operações diárias e recuperação de desastres. Essa abordagem proativa pode reduzir ou eliminar interrupções comerciais dispendiosas.

Este artigo descreve como usar o Veeam Backup & Replication para configurar a recuperação de desastres para VMs VMware locais no Google Cloud VMware Engine (GCVE) com o Google Cloud NetApp Volumes (NetApp Volumes).

Visão geral

O Google Cloud NetApp Volumes é um serviço de armazenamento do Google e da NetApp que está disponível para o Google Cloud. O serviço NetApp Volumes fornece armazenamento NFS/SMB de alto desempenho. O armazenamento NFS NetApp Volumes certificado pela VMware pode ser usado como um armazenamento de dados externo para hosts ESXi no GCVE. Os usuários precisam fazer uma conexão de peering entre sua nuvem privada GCVE e o projeto NetApp Volumes. Não há cobranças de rede resultantes do acesso ao armazenamento dentro de uma região. Os usuários podem criar volumes do NetApp Volumes no console do Google Cloud e habilitar a proteção contra exclusão antes de montar volumes como armazenamentos de dados em seus hosts ESXi.

Os datastores NFS baseados no NetApp Volumes podem ser usados para replicar dados locais usando qualquer solução de terceiros validada que forneça capacidade de replicação de VM. Ao adicionar datastores do NetApp Volumes, é possível uma implantação com custo otimizado em vez de criar um SDDC baseado no Google Cloud VMware Engine (GCVE) com um grande número de hosts ESXi para acomodar o armazenamento. Essa abordagem é chamada de "Pilot Light Cluster". Um cluster de luz piloto é uma configuração mínima de host GCVE (3 hosts GCVE ESXi) junto com capacidade de armazenamento de dados do NetApp Volumes para permitir dimensionamento independente para atender aos requisitos de capacidade.

O objetivo é sustentar uma infraestrutura econômica com apenas os componentes principais para gerenciar um failover. Um cluster de luz piloto pode expandir e adicionar mais hosts GCVE no caso de um failover. Depois que o failover for resolvido e as operações normais forem retomadas, o cluster de luz piloto pode reduzir sua escala, retornando a um modo operacional de baixo custo.

Finalidades deste documento

Este artigo descreve como usar um armazenamento de dados do Google Cloud NetApp Volumes com o Veeam Backup & Replication para configurar a recuperação de desastres para VMs VMware locais para GCVE usando a funcionalidade do software de replicação de VMs Veeam.

O Veeam Backup & Replication é um aplicativo de backup e replicação para ambientes virtuais. Quando as máquinas virtuais são replicadas, o Veeam Backup & Replication cria uma cópia exata das VMs no formato nativo do VMware vSphere no cluster GCVE SDDC de destino. O Veeam Backup & Replication manterá a cópia sincronizada com a VM original. A replicação fornece o melhor objetivo de tempo de recuperação (RTO), pois há uma cópia montada de uma VM no site de DR em um estado pronto para iniciar.

Esse mecanismo de replicação garante que as cargas de trabalho possam iniciar rapidamente no GCVE no caso de um evento de desastre. O software Veeam Backup & Replication também otimiza a transmissão de tráfego para replicação via WAN e conexões lentas. Além disso, ele também filtra blocos de dados duplicados,

blocos de dados zero, arquivos de troca e "arquivos de sistema operacional convidado de VM excluídos". O software também compactará o tráfego de réplica. Para evitar que trabalhos de replicação consumam toda a largura de banda da rede, aceleradores de WAN e regras de limitação de rede podem ser utilizados.

O processo de replicação no Veeam Backup & Replication é orientado por tarefas, o que significa que a replicação é realizada configurando tarefas de replicação. No caso de um evento de desastre, o failover pode ser acionado para recuperar as VMs por meio de failover para sua cópia de réplica. Quando o failover é executado, uma VM replicada assume a função da VM original. O failover pode ser executado no estado mais recente de uma réplica ou em qualquer um dos seus pontos de restauração conhecidos. Isso permite a recuperação de ransomware ou testes isolados, conforme necessário. O Veeam Backup & Replication oferece diversas opções para lidar com diferentes cenários de recuperação de desastres.

Visão geral da solução

Esta solução abrange as seguintes etapas de alto nível:

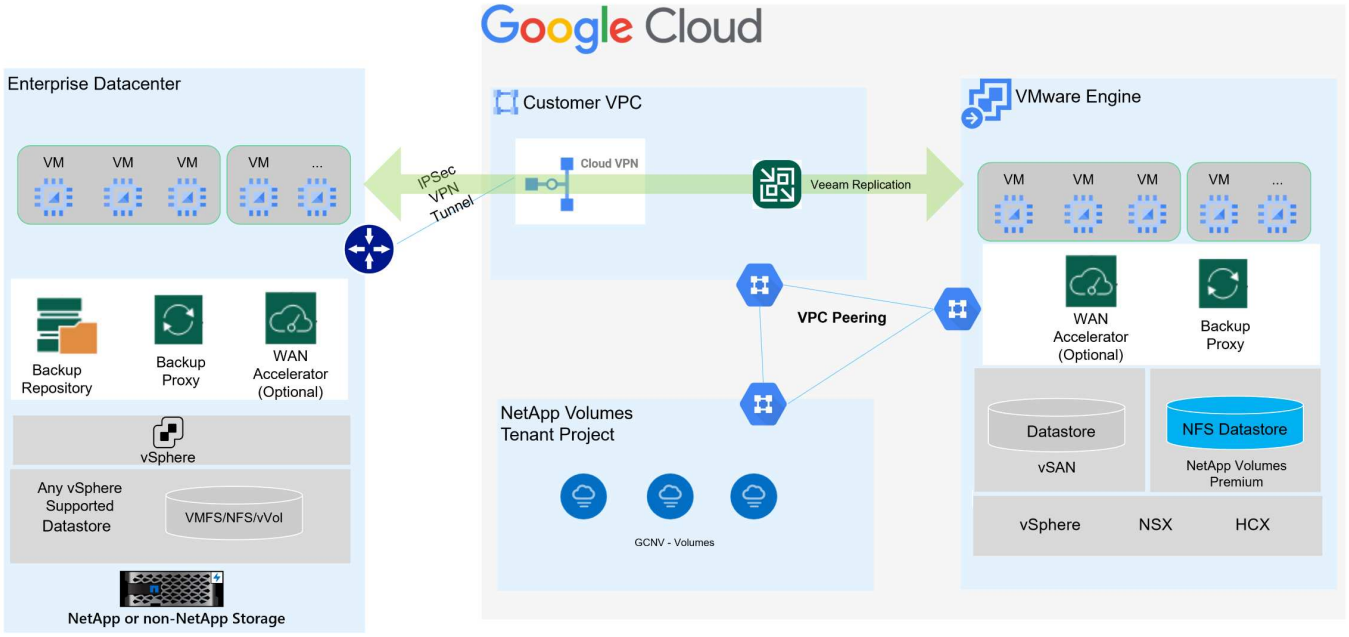
1. Crie um volume NFS usando o Google Cloud NetApp Volumes
2. Siga o processo do GCP para criar um armazenamento de dados GCVE a partir do volume NFS do NetApp Volumes.
3. Configure uma tarefa de replicação para criar réplicas de VM usando o Veeam Backup & Replication.
4. Crie um plano de failover e execute o failover.
5. Retorne para as VMs de produção quando o evento de desastre for concluído e o site principal estiver ativo.

> Ao criar um volume no NetApp Volumes, para uso como um armazenamento de dados GCVE, somente o NFS v3 é suportado.

Para obter mais informações sobre o uso de volumes NFS do NetApp Volumes como armazenamentos de dados para GCVE, consulte "Usando o volume NFS como armazenamento de dados do vSphere hospedado pelo Google Cloud NetApp Volumes" .

Arquitetura

O diagrama a seguir mostra a arquitetura da solução apresentada nesta documentação. Uma prática recomendada é ter um servidor Veeam Backup & Replication localizado no site local e no SDDC do GCVE. O backup e a recuperação são executados e gerenciados pelo servidor Veeam local, e a replicação é gerenciada pelo servidor Veeam no SDDC do GCVE. Essa arquitetura fornece a mais alta disponibilidade quando ocorre uma falha no datacenter principal.



Pré-requisitos para Veeam Replication para datastores GCVE e NetApp Volumes

Esta solução requer os seguintes componentes e configurações:

1. O NetApp Volumes tem um pool de armazenamento disponível com capacidade livre suficiente para acomodar o volume NFS a ser criado.
2. O software Veeam Backup and Replication está sendo executado em um ambiente local com conectividade de rede apropriada.
3. Certifique-se de que a VM de backup do Veeam Backup & Replication esteja conectada aos clusters GCVE SDDC de origem e de destino.
4. Certifique-se de que a VM de backup do Veeam Backup & Replication esteja conectada às VMs do servidor Veeam Proxy nos clusters GCVE de origem e de destino.
5. O servidor de backup deve ser capaz de resolver nomes curtos e se conectar aos vCenters de origem e de destino.

Os usuários precisam fazer uma conexão de peering entre sua nuvem privada GCVE e o projeto do NetApp Volumes usando as páginas de peering de rede VPC ou conexões privadas na interface de usuário do console do VMware Engine Cloud.

> O Veeam exige uma conta de usuário da solução GCVE com privilégios elevados ao adicionar o servidor GCVE vCenter ao inventário do Veeam Backup and Replication. Para obter mais informações, consulte a documentação do Google Cloud Platform (GCP), "Elevando privilégios do VMware Engine".

Para obter informações adicionais, consulte "Considerações e Limitações" na documentação do Veeam Backup & Replication.

Etapas de implantação

As seções a seguir descrevem as etapas de implantação para criar e montar um armazenamento de dados NFS usando o Google Cloud NetApp Volumes e usar o Veeam Backup and Replication para implementar uma solução completa de recuperação de desastres entre um datacenter local e o Google Cloud VMware Engine.

Crie um volume NFS e um armazenamento de dados do NetApp Volumes para GCVE

Consulte "Usando o volume NFS como armazenamento de dados do vSphere hospedado pelo Google Cloud NetApp Volumes" para uma visão geral de como usar o Google Cloud NetApp Volumes como um armazenamento de dados para GCVE.

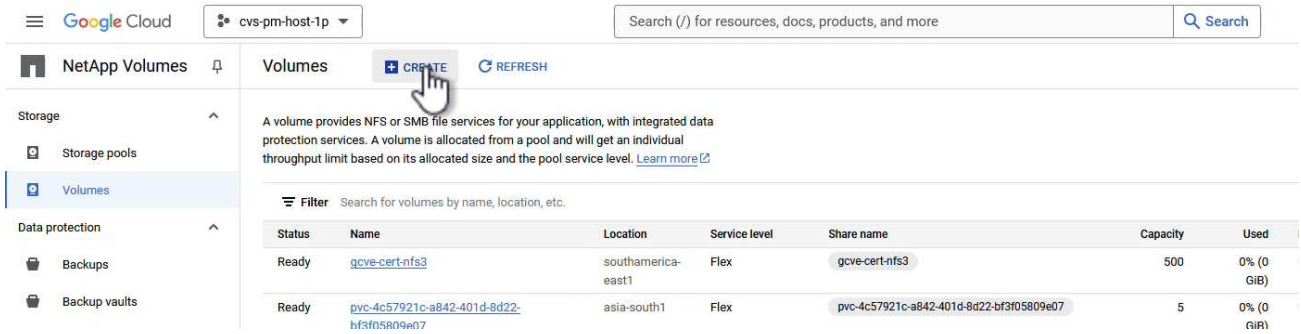
Conclua as seguintes etapas para criar e usar um armazenamento de dados NFS para GCVE usando o NetApp Volumes:

▼ **Criar volume NFS do NetApp Volumes**

O Google Cloud NetApp Volumes é acessado pelo console do Google Cloud Platform (GCP).

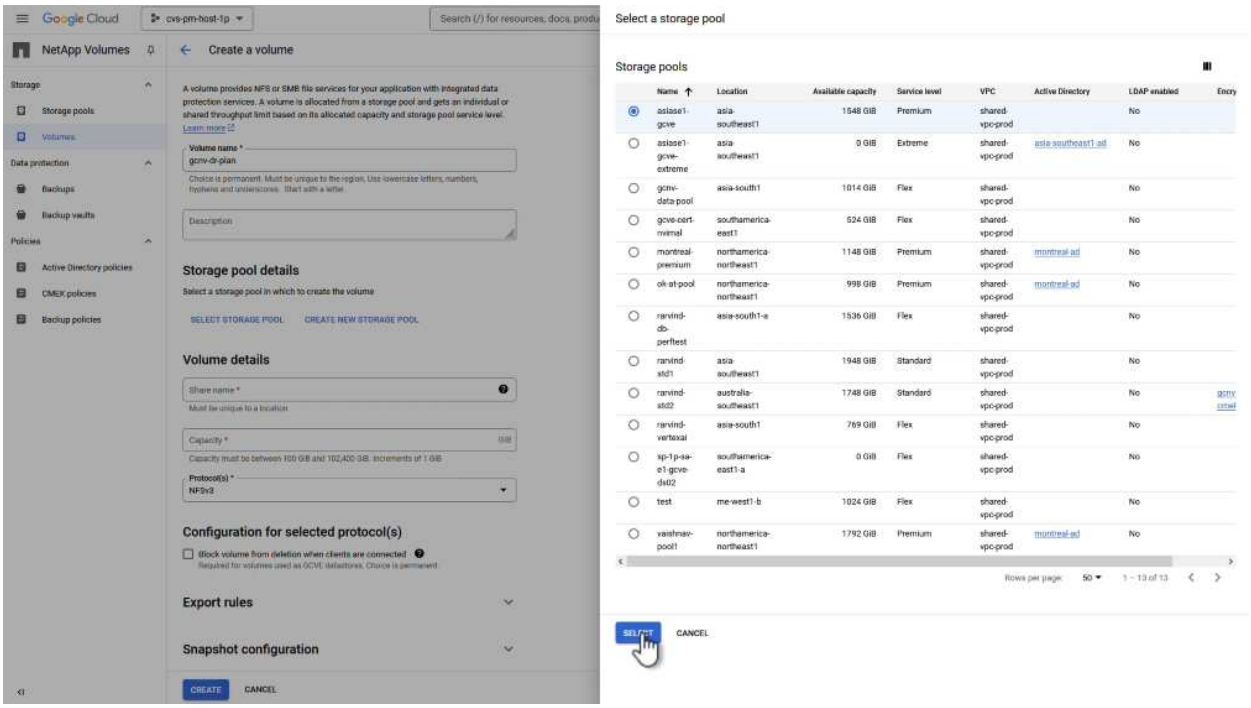
Consulte "Criar um volume" na documentação do Google Cloud NetApp Volumes para obter informações detalhadas sobre esta etapa.

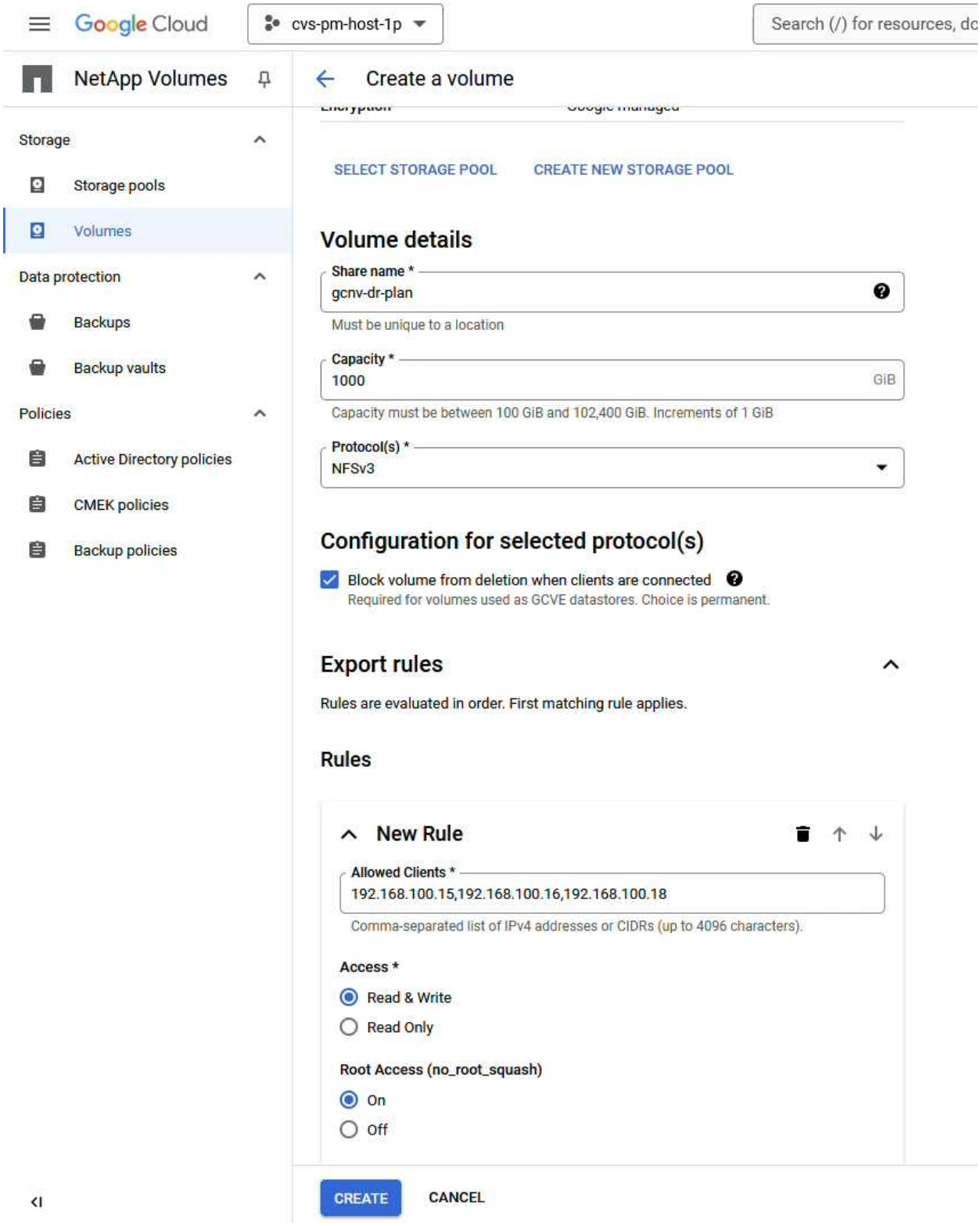
1. Em um navegador da web, navegue até https://console.cloud.google.com/ e faça login no console do GCP. Pesquise por * NetApp Volumes* para começar.
2. Na interface de gerenciamento * NetApp Volumes **, clique em *Criar** para começar a criar um volume NFS.



3. No assistente **Criar um volume**, preencha todas as informações necessárias:
   - Um nome para o volume.
   - O pool de armazenamento no qual o volume será criado.
   - Um nome de compartilhamento usado ao montar o volume NFS.
   - A capacidade do volume em GiB.
   - O protocolo de armazenamento a ser usado.
   - Marque a caixa para **Bloquear a exclusão do volume quando os clientes estiverem conectados** (exigido pelo GCVE ao montar como um armazenamento de dados).
   - As regras de exportação para acessar o volume. Estes são os endereços IP dos adaptadores ESXi na rede NFS.
   - Um agendamento de snapshot usado para proteger o volume usando snapshots locais.
   - Opcionalmente, escolha fazer backup do volume e/ou criar rótulos para o volume.

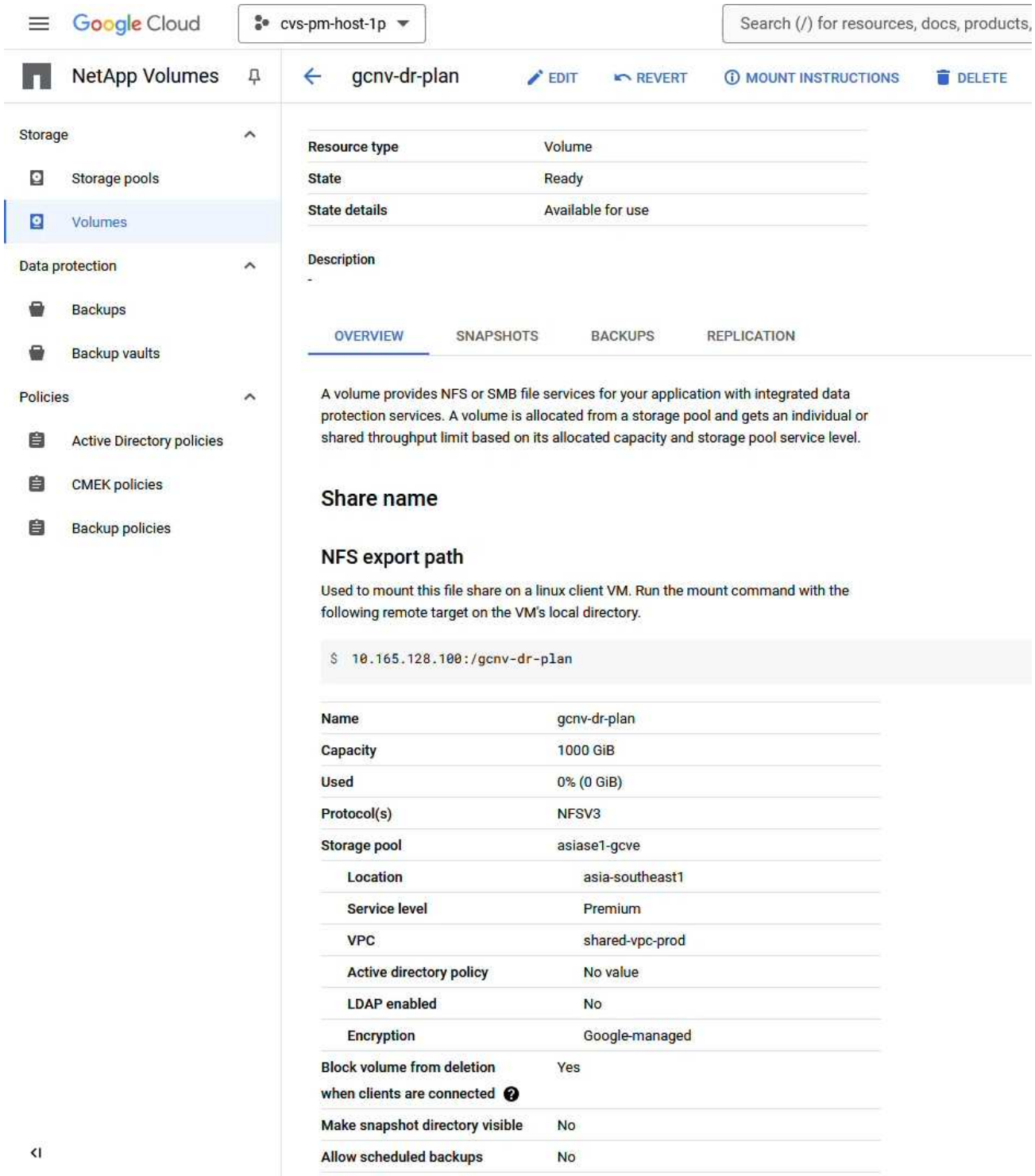
> Ao criar um volume no NetApp Volumes, para uso como um armazenamento de dados GCVE, somente o NFS v3 é suportado.


Google Cloud
cvs-pm-host-1p
Search (/) for resources, docs, produ
NetApp Volumes
Create a volume
Storage
Storage pools
Volumes
Data protection
Backups
Backup vaults
Policies
Active Directory policies
CMEK policies
Backup policies
A volume provides NFS or SMB file services for your application with integrated data protection services. A volume is allocated from a storage pool and gets an individual or shared throughput limit based on its allocated capacity and storage pool service level.
Learn more
Volume name *
gcnv-dr-plan
Choice is permanent. Must be unique to the region. Use lowercase letters, numbers, hyphens and underscores. Start with a letter.
Description
Storage pool details
Select a storage pool in which to create the volume
SELECT STORAGE POOL
CREATE NEW STORAGE POOL
Volume details
Share name *
Must be unique to a location
Capacity *
GiB
Capacity must be between 100 GiB and 102,400 GiB. Increments of 1 GiB
Protocol(s) *
NFSv3
Configuration for selected protocol(s)
Block volume from deletion when clients are connected
Required for volumes used as GCVE datastores. Choice is permanent.
Export rules
Snapshot configuration
CREATE
CANCEL
Select a storage pool
Storage pools
Name
Location
Available capacity
Service level
VPC
Active Directory
LDAP enabled
Encry
asiase1-gcve
asia-southeast1
1548 GiB
Premium
shared-vpc-prod
No
asiase1-gcve-extreme
asia-southeast1
0 GiB
Extreme
shared-vpc-prod
asia-southeast1-ad
No
gcnv-data-pool
asia-south1
1014 GiB
Flex
shared-vpc-prod
No
gcve-cert-nvmal
southamerica-east1
524 GiB
Flex
shared-vpc-prod
No
montreal-premium
northamerica-northeast1
1148 GiB
Premium
shared-vpc-prod
montreal-ad
No
ok-at-pool
northamerica-northeast1
998 GiB
Premium
shared-vpc-prod
montreal-ad
No
ranvind-db-perftest
asia-south1-a
1536 GiB
Flex
shared-vpc-prod
No
ranvind-std1
asia-southeast1
1948 GiB
Standard
shared-vpc-prod
No
ranvind-std2
australia-southeast1
1748 GiB
Standard
shared-vpc-prod
No
gcnv cmek
ranvind-vertexai
asia-south1
769 GiB
Flex
shared-vpc-prod
No
sp-1p-sa-e1-gcve-ds02
southamerica-east1-a
0 GiB
Flex
shared-vpc-prod
No
test
me-west1-b
1024 GiB
Flex
shared-vpc-prod
No
vaishnav-pool1
northamerica-northeast1
1792 GiB
Premium
shared-vpc-prod
montreal-ad
No
Rows per page: 50
1 – 13 of 13
SELECT
CANCEL



Clique em **Criar** para finalizar a criação do volume.

4. Depois que o volume é criado, o caminho de exportação NFS necessário para montá-lo pode ser visualizado na página de propriedades do volume.



▼ **Monte o armazenamento de dados NFS no GCVE**

No momento em que este artigo foi escrito, o processo para montar um armazenamento de dados no GCVE exigia a abertura de um tíquete de suporte do GCP para que o volume fosse montado como um armazenamento de dados NFS.

Consulte "Usando o volume NFS como armazenamento de dados do vSphere hospedado pelo Google Cloud NetApp Volumes" para maiores informações.

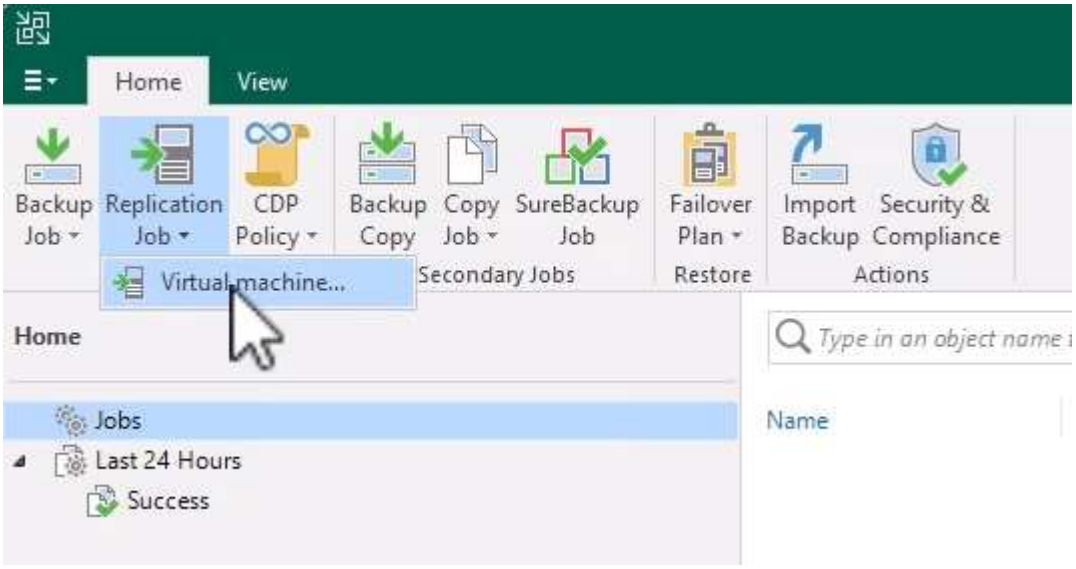
Replique VMs para GCVE e execute o plano de failover e failback

▼ Replicar VMs para o armazenamento de dados NFS no GCVE

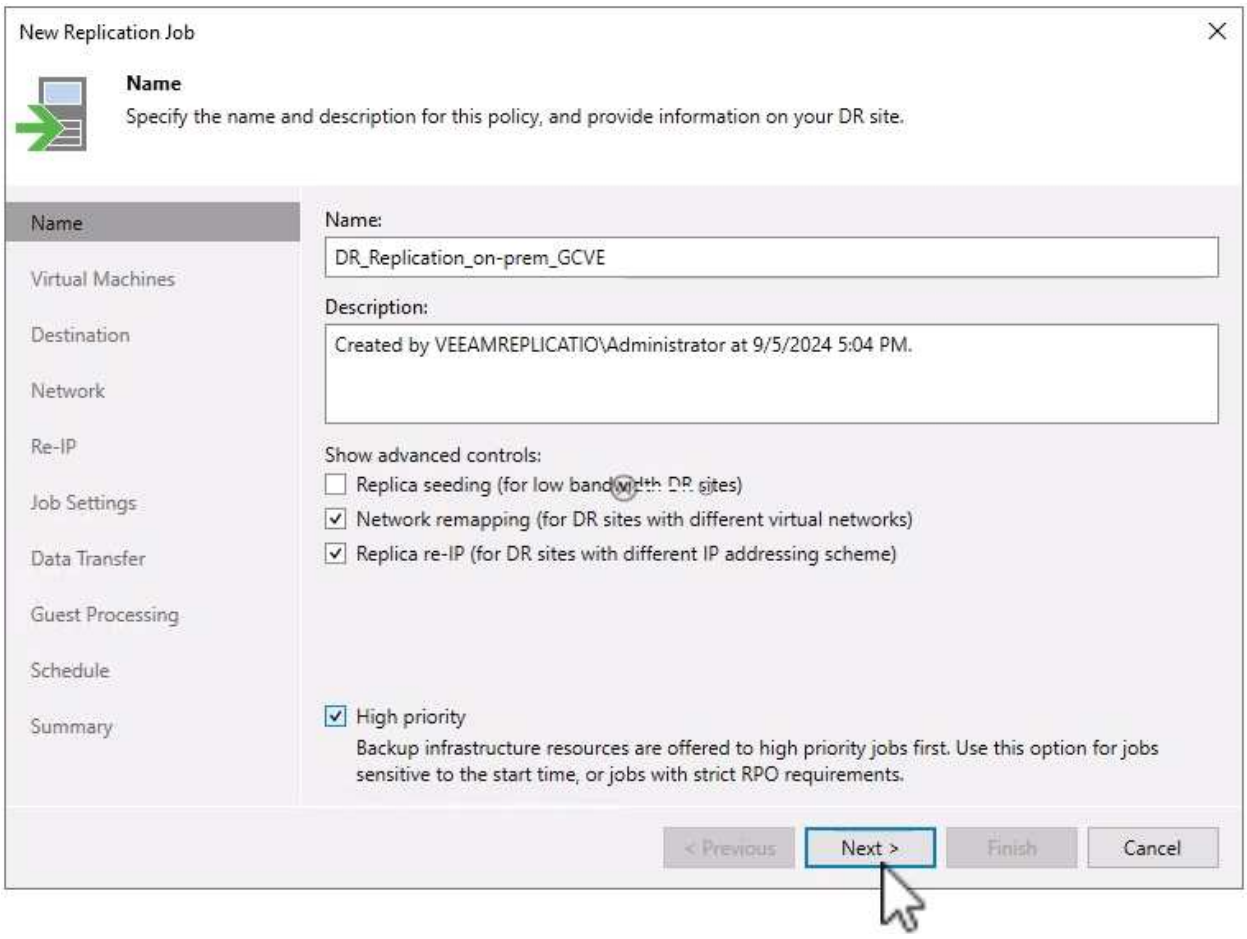
O Veeam Backup & Replication aproveita os recursos de snapshot do VMware vSphere. Durante a replicação, o Veeam Backup & Replication solicita que o VMware vSphere crie um snapshot da VM. O snapshot da VM é a cópia de um momento específico de uma VM que inclui discos virtuais, estado do sistema, configuração e metadados. O Veeam Backup & Replication usa o snapshot como uma fonte de dados para replicação.

Para replicar VMs, conclua as seguintes etapas:

1. Abra o Veeam Backup & Replication Console.
2. Na guia **Início**, clique em **Trabalho de replicação > Máquina virtual…**

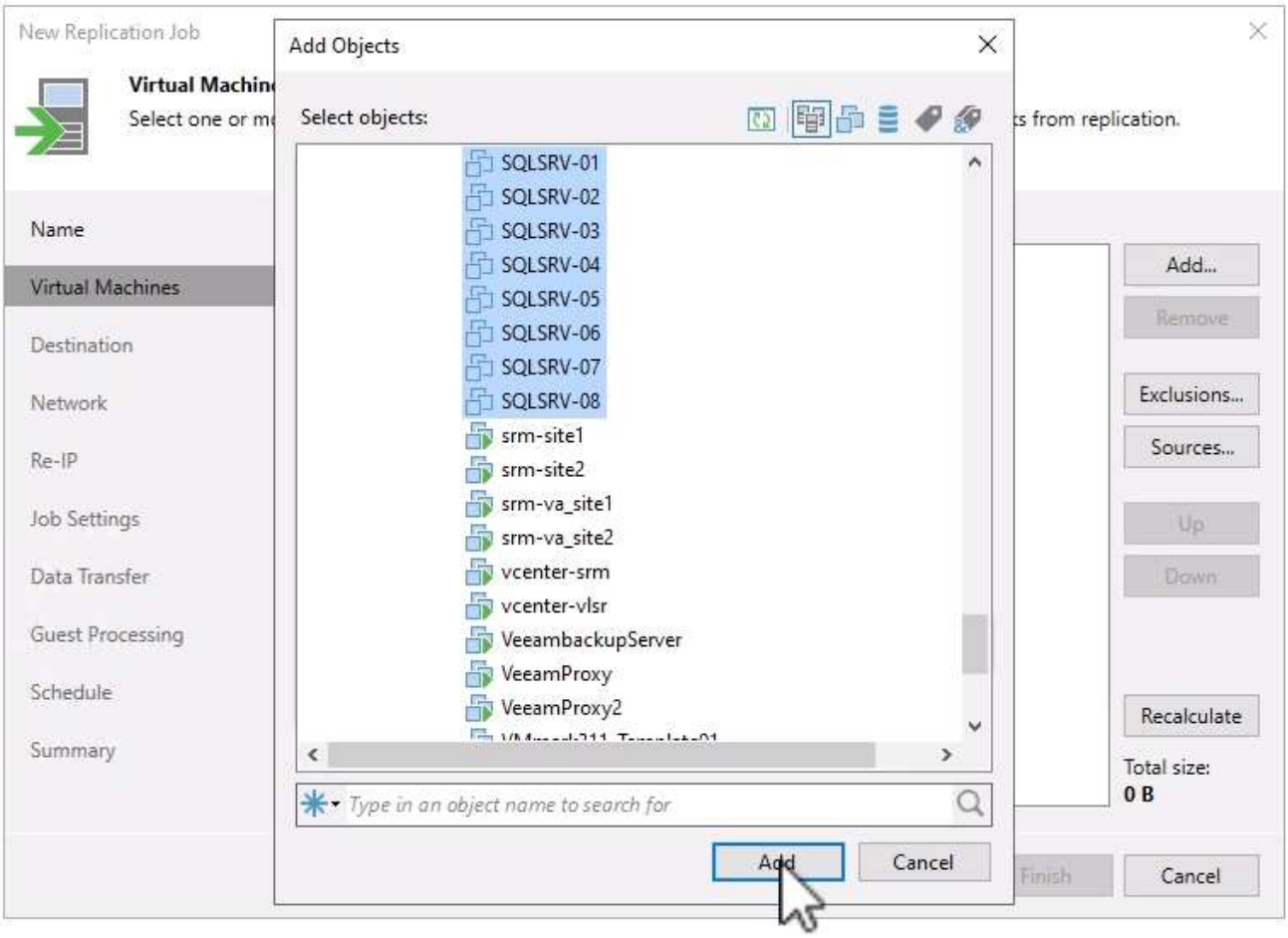


3. Na página **Nome** do assistente **Novo trabalho de replicação**, especifique um nome de trabalho e marque as caixas de seleção de controle avançado apropriadas.
   - Marque a caixa de seleção Semeadura de réplica se a conectividade entre o local e o GCP tiver largura de banda restrita.
   - Marque a caixa de seleção Remapeamento de rede (para sites GCVE SDDC com redes diferentes) se os segmentos no GCVE SDDC não corresponderem às redes do site local.
   - Marque a caixa de seleção Replica re-IP (para sites de DR com esquema de endereçamento IP diferente) se o esquema de endereçamento IP no site de produção local for diferente do esquema no site GCVE de destino.

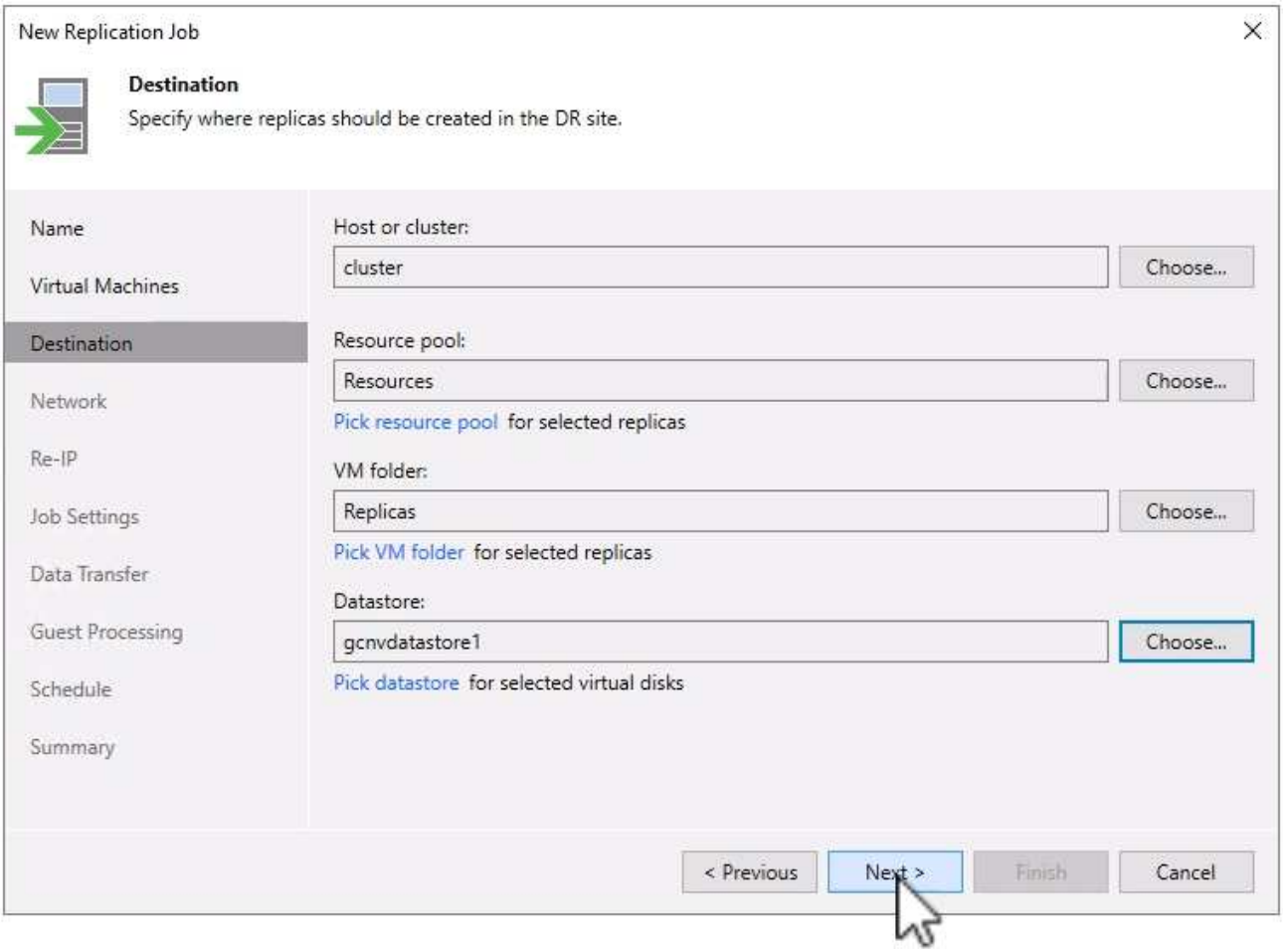


4. Na página **Máquinas Virtuais**, selecione as VMs a serem replicadas para o armazenamento de dados do NetApp Volumes anexado a um SDDC GCVE. Clique em **Adicionar**, então na janela **Adicionar Objeto** selecione as VMs ou contêineres de VM necessários e clique em **Adicionar**. Clique em **Avançar**.

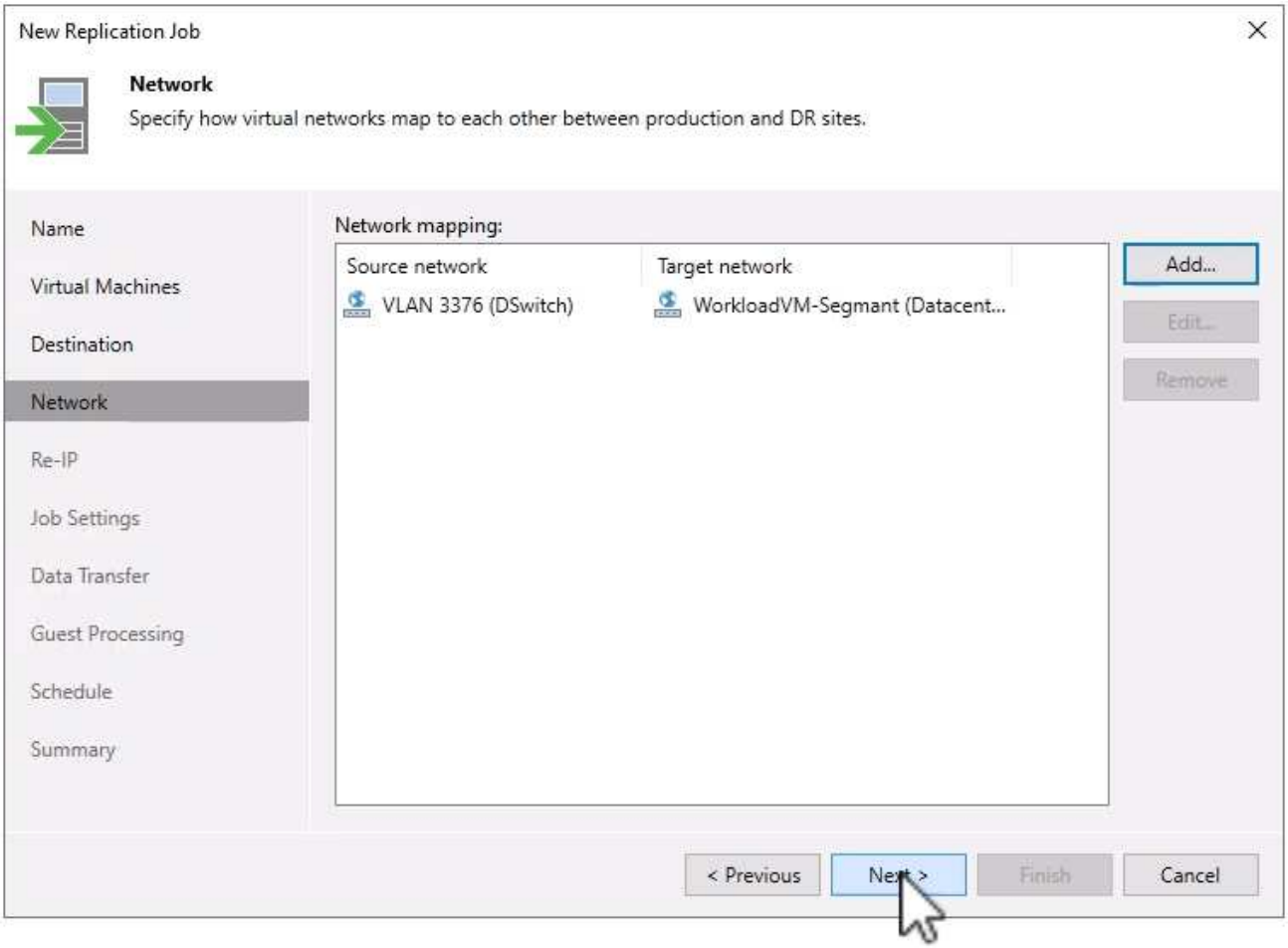
> As máquinas virtuais podem ser colocadas no vSAN para preencher a capacidade disponível do armazenamento de dados do vSAN. Em um cluster piloto, a capacidade utilizável de um cluster vSAN de 3 nós será limitada. O restante dos dados pode ser facilmente colocado nos armazenamentos de dados do Google Cloud NetApp Volumes para que as VMs possam ser recuperadas e o cluster possa ser expandido posteriormente para atender aos requisitos de CPU/memória.



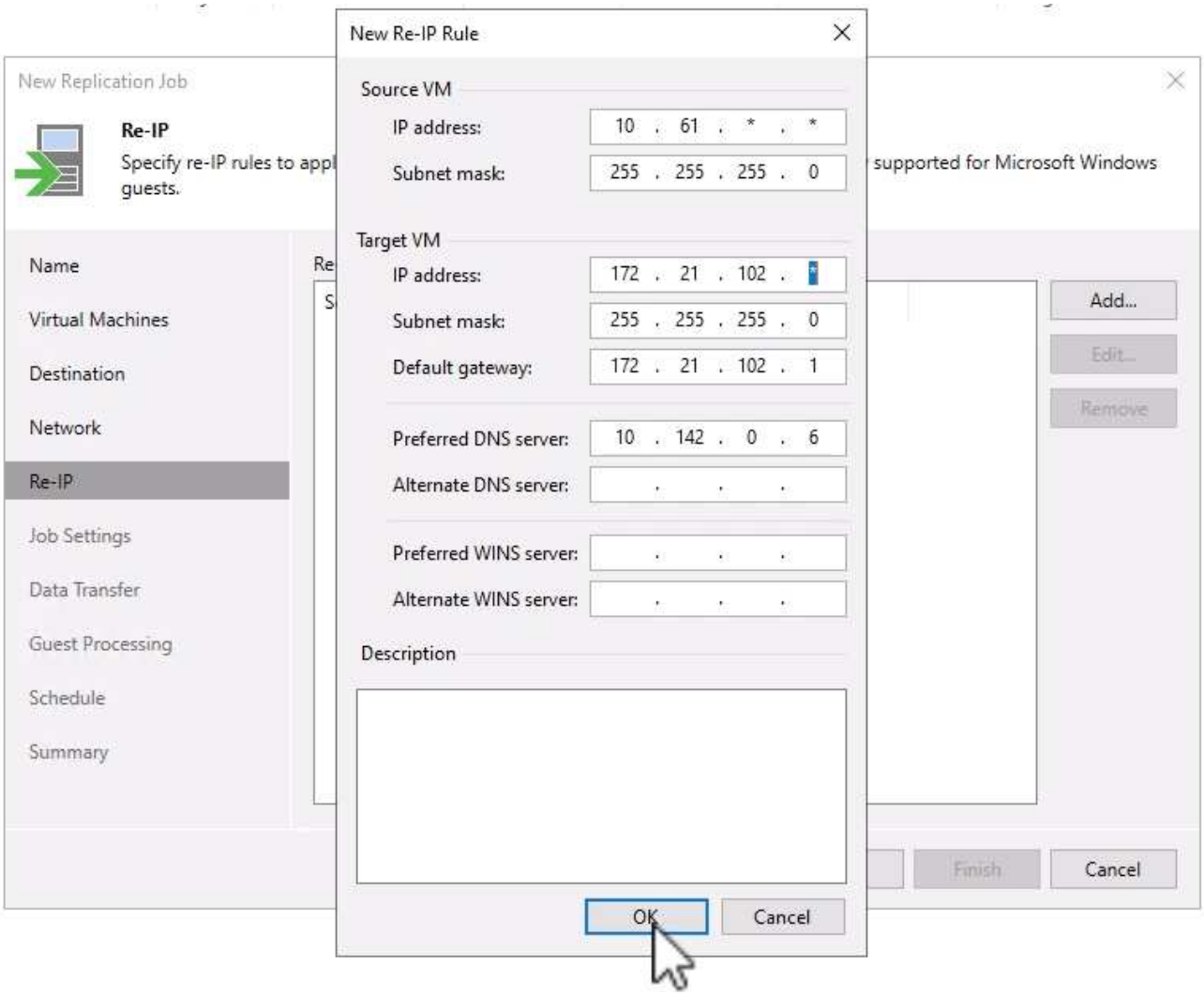
5. Na página **Destino**, selecione o destino como o cluster/hosts do SDDC do GCVE e o pool de recursos apropriado, a pasta da VM e o armazenamento de dados do NetApp Volumes para as réplicas da VM. Clique em **Avançar** para continuar.



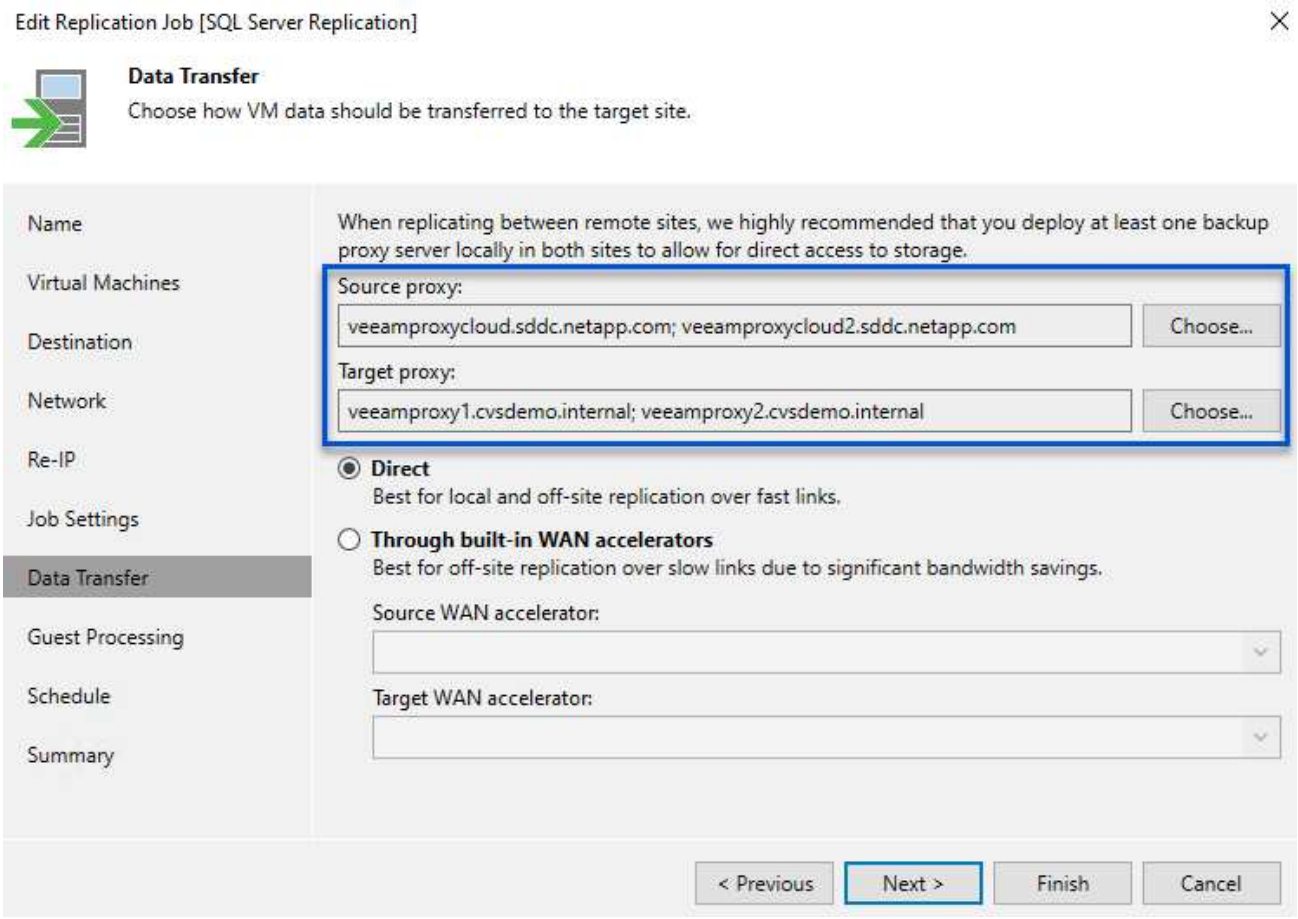
6. Na página **Rede**, crie o mapeamento entre as redes virtuais de origem e de destino, conforme necessário. Clique em **Avançar** para continuar.



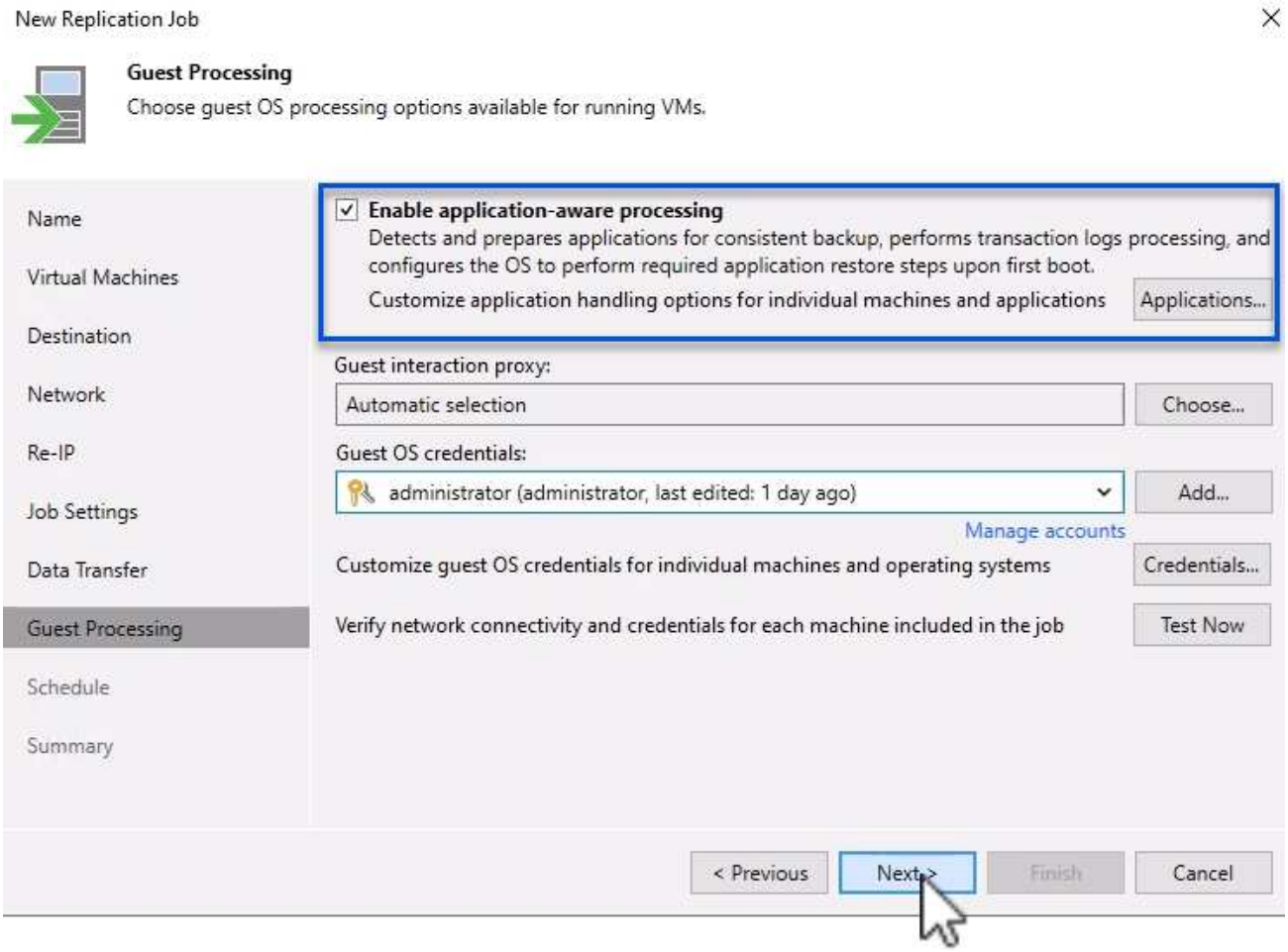
7. Na página **Re-IP**, clique no botão **Adicionar…** para adicionar uma nova regra de re-IP. Preencha os intervalos de IP das VMs de origem e de destino para especificar a rede que será aplicada às VMs de origem no caso de um failover. Use asteriscos para especificar um intervalo de endereços indicado para esse octeto. Clique em **Avançar** para continuar.



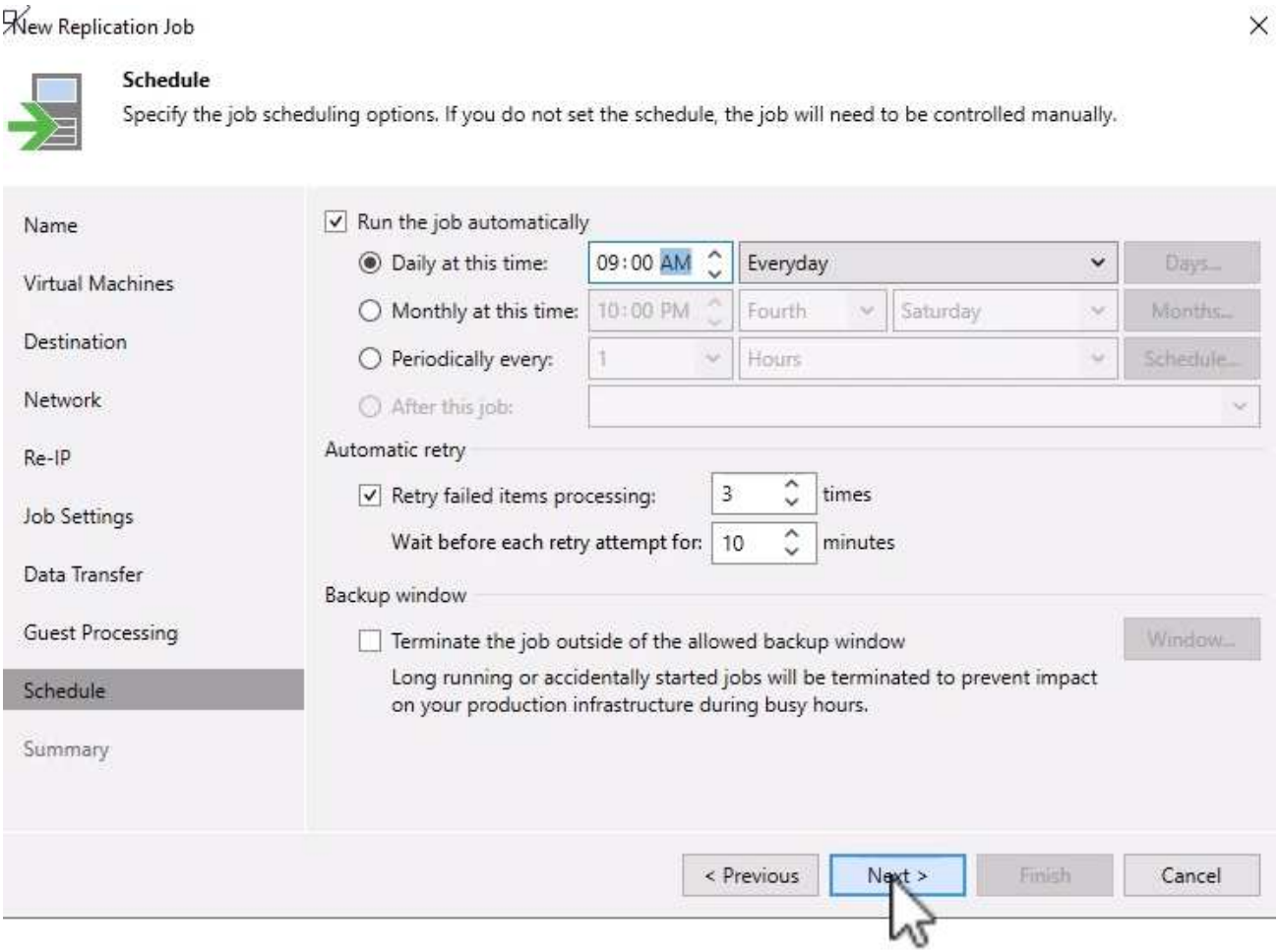
8. Na página **Configurações do trabalho**, especifique o repositório de backup que armazenará metadados para réplicas de VM, a política de retenção e selecione o botão na parte inferior para **Avançado…** para configurações adicionais do trabalho. Clique em **Avançar** para continuar.
9. Em **Transferência de dados**, selecione os servidores proxy que residem nos sites de origem e de destino e mantenha a opção Direto selecionada. Aceleradores WAN também podem ser selecionados aqui, se configurados. Clique em **Avançar** para continuar.



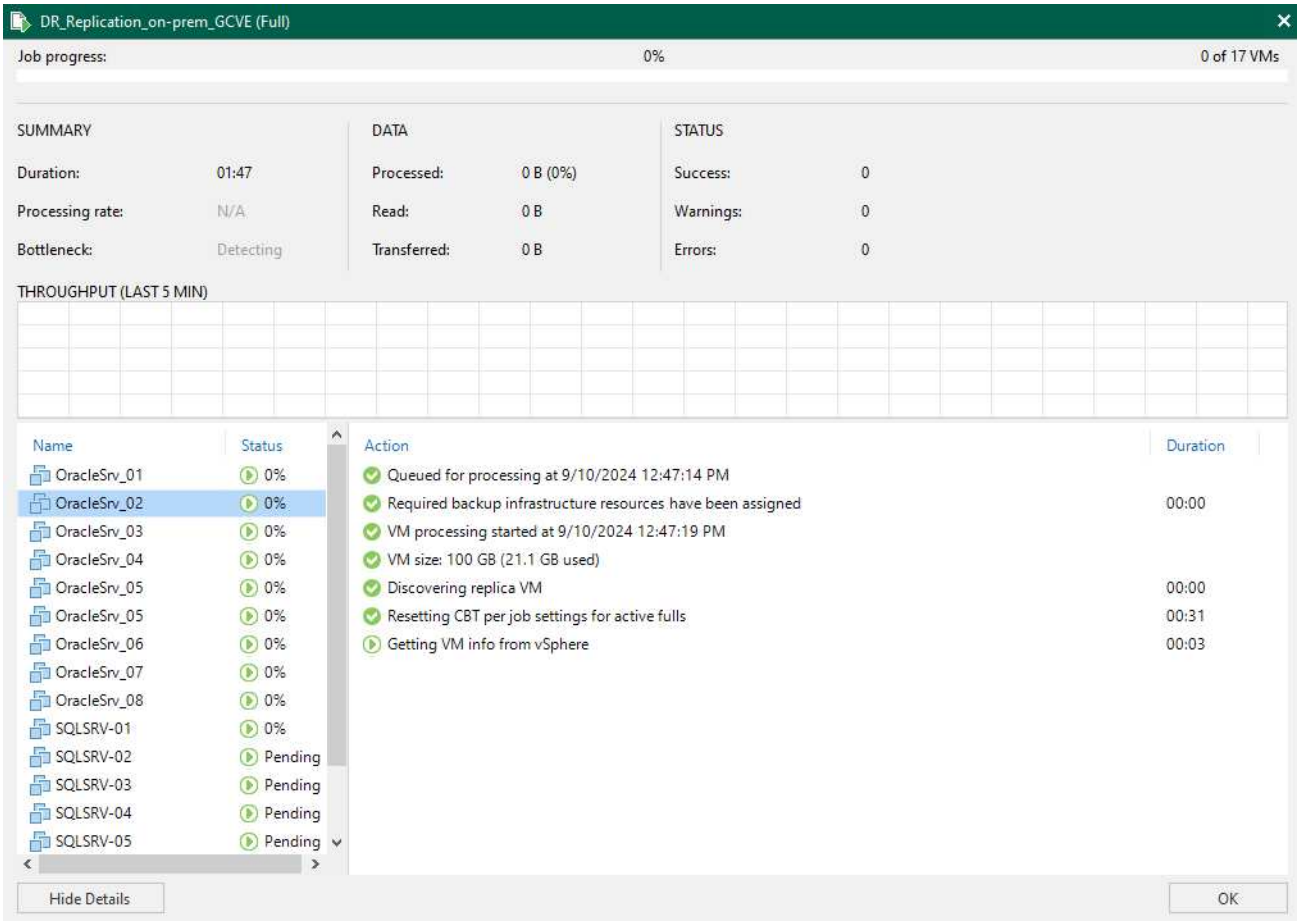
10. Na página **Processamento de Convidado**, marque a caixa **Ativar processamento com reconhecimento de aplicativo** conforme necessário e selecione as **Credenciais do SO Convidado**. Clique em **Avançar** para continuar.



11. Na página **Agendar**, defina os horários e a frequência em que o trabalho de replicação será executado. Clique em **Avançar** para continuar.



12. Por fim, revise a configuração do trabalho na página **Resumo**. Marque a caixa para **Executar o trabalho quando eu clicar em Concluir** e clique em **Concluir** para concluir a criação do trabalho de replicação.
13. Uma vez executado, o trabalho de replicação pode ser visualizado na janela de status do trabalho.



Para obter informações adicionais sobre a replicação do Veeam, consulte"Como funciona a replicação"

▼ **Crie um plano de failover**

Quando a replicação ou propagação inicial estiver concluída, crie o plano de failover. O plano de failover ajuda a executar o failover para VMs dependentes, uma por uma ou como um grupo, automaticamente. O plano de failover é o modelo para a ordem em que as VMs são processadas, incluindo os atrasos de inicialização. O plano de failover também ajuda a garantir que as VMs dependentes críticas já estejam em execução.

Após concluir a replicação ou propagação inicial, crie um plano de failover. Este plano serve como um modelo estratégico para orquestrar o failover de VMs dependentes, individualmente ou em grupo. Ele define a ordem de processamento das VMs, incorpora atrasos de inicialização necessários e garante que as VMs dependentes críticas estejam operacionais antes das outras. Ao implementar um plano de failover bem estruturado, as organizações podem otimizar seu processo de recuperação de desastres, minimizando o tempo de inatividade e mantendo a integridade dos sistemas interdependentes durante um evento de failover.

Ao criar o plano, o Veeam Backup & Replication identifica e usa automaticamente os pontos de restauração mais recentes para iniciar as réplicas de VM.

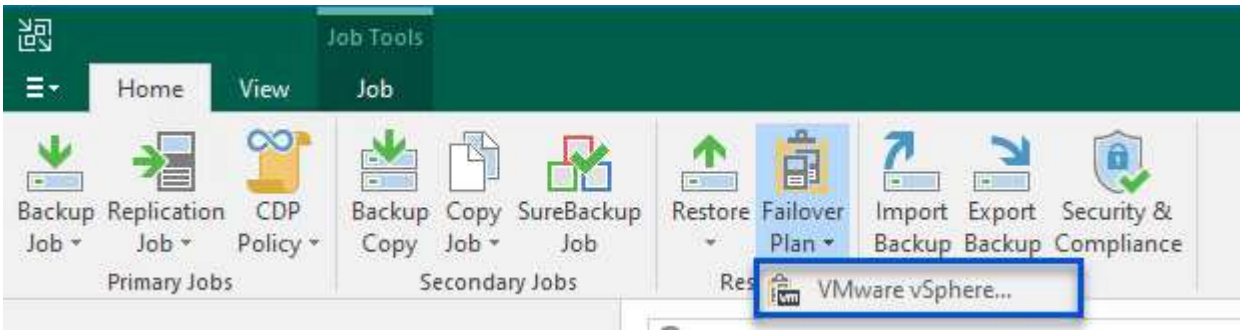
ⓘ O plano de failover só pode ser criado quando a replicação inicial estiver concluída e as réplicas da VM estiverem no estado Pronto.

ⓘ O número máximo de VMs que podem ser iniciadas simultaneamente ao executar um plano de failover é 10.

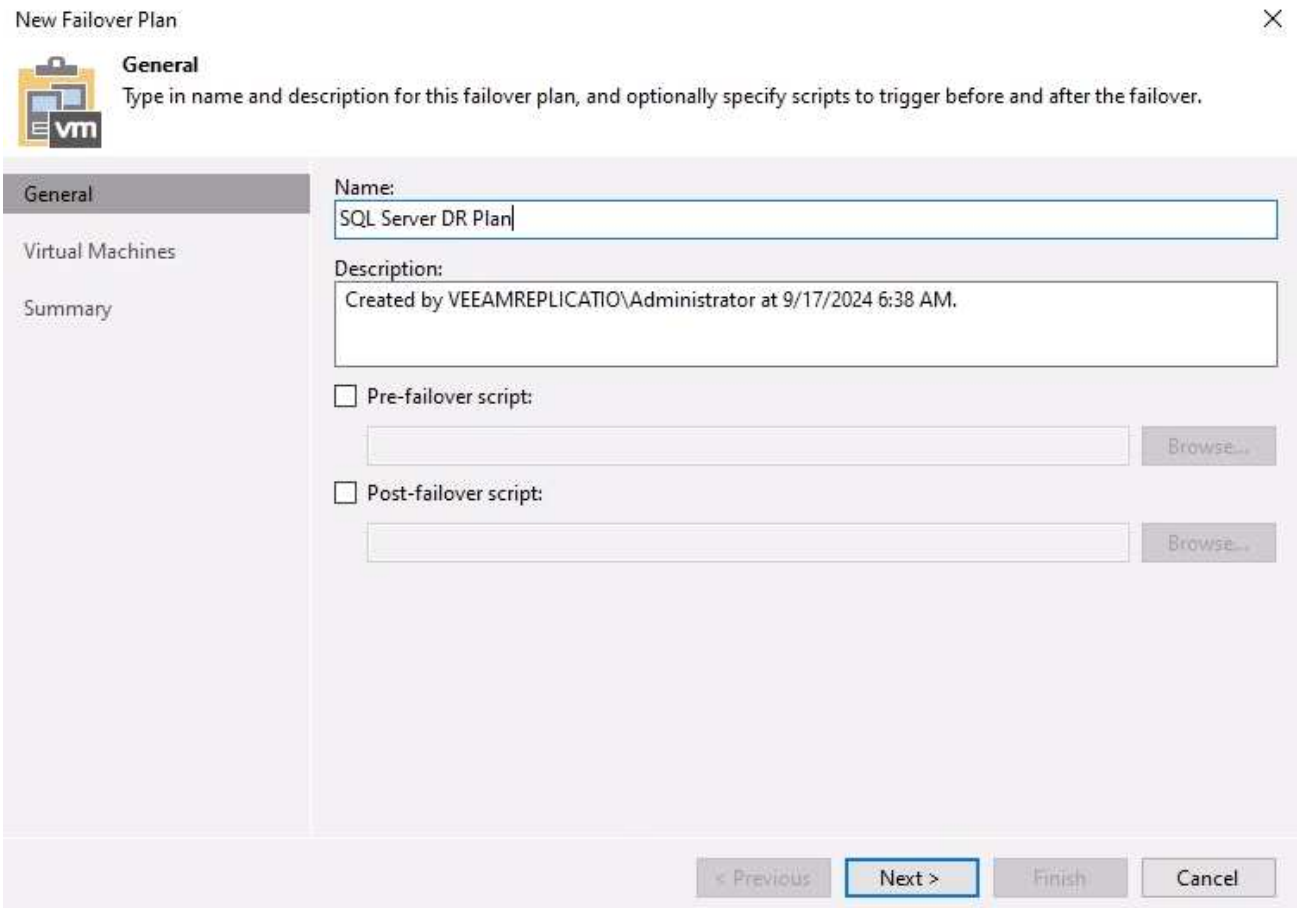
Durante o processo de failover, as VMs de origem não serão desligadas.

Para criar o **Plano de Failover**, conclua as seguintes etapas:

1. Na visualização **Início**, clique no botão **Plano de Failover** na seção **Restaurar**. No menu suspenso, selecione **VMware vSphere…**

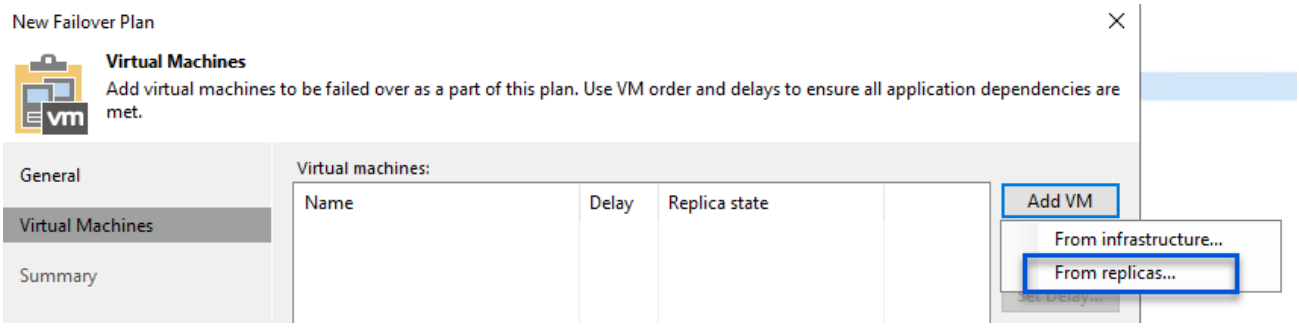


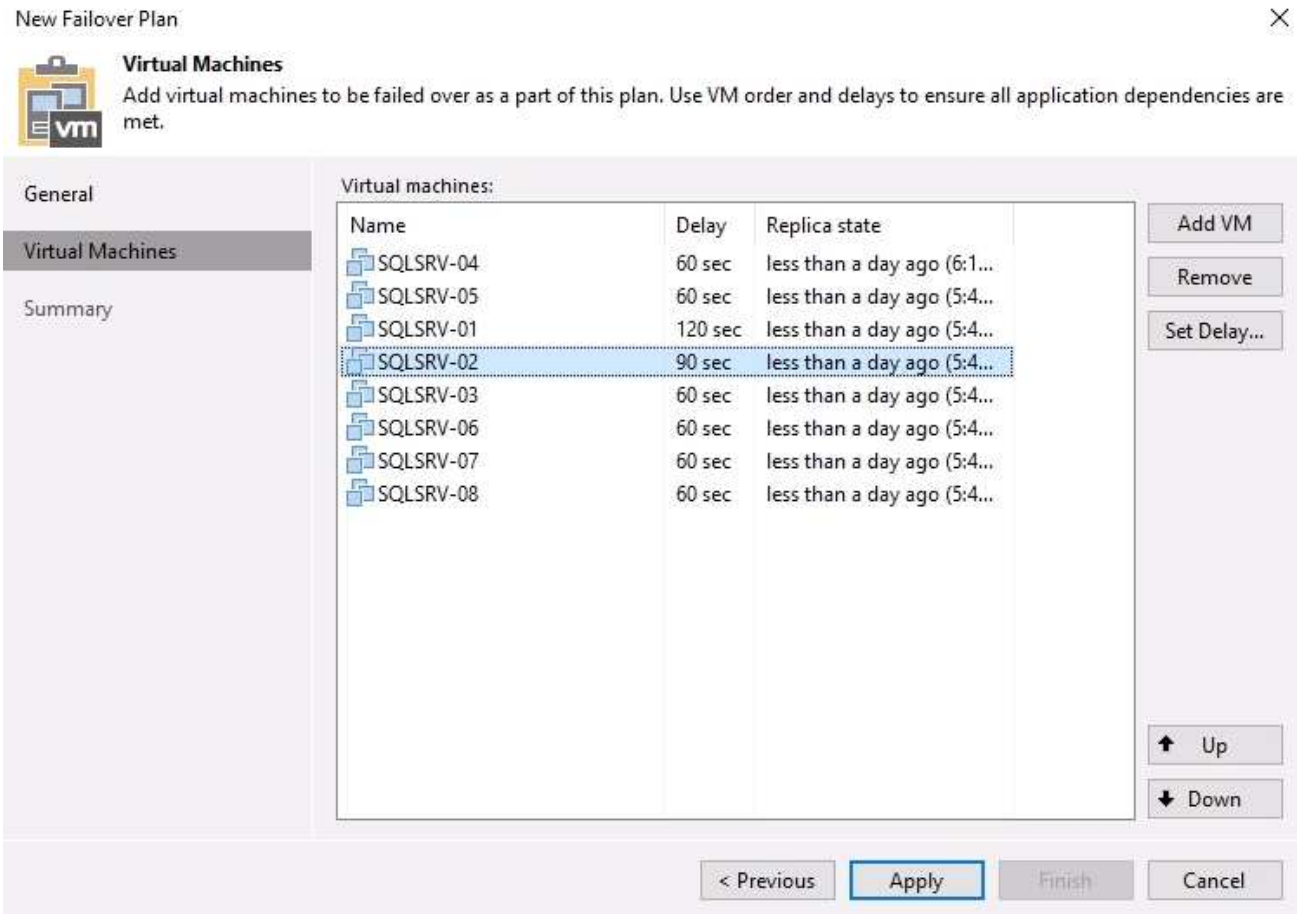
2. Na página **Geral** do assistente **Novo Plano de Failover**, forneça um nome e uma descrição para o plano. Scripts pré e pós-failover podem ser adicionados conforme necessário. Por exemplo, execute um script para desligar as VMs antes de iniciar as VMs replicadas.



3. Na página **Máquinas Virtuais**, clique no botão **Adicionar VM** e selecione **De réplicas…**. Escolha as

VMs que farão parte do plano de failover e modifique a ordem de inicialização das VMs e quaisquer atrasos de inicialização necessários para atender às dependências do aplicativo.





Clique em **Aplicar** para continuar.

4. Por fim, revise todas as configurações do plano de failover e clique em **Concluir** para criar o plano de failover.

Para obter informações adicionais sobre a criação de trabalhos de replicação, consulte"Criando trabalhos de replicação" .

▼ **Execute o plano de failover**

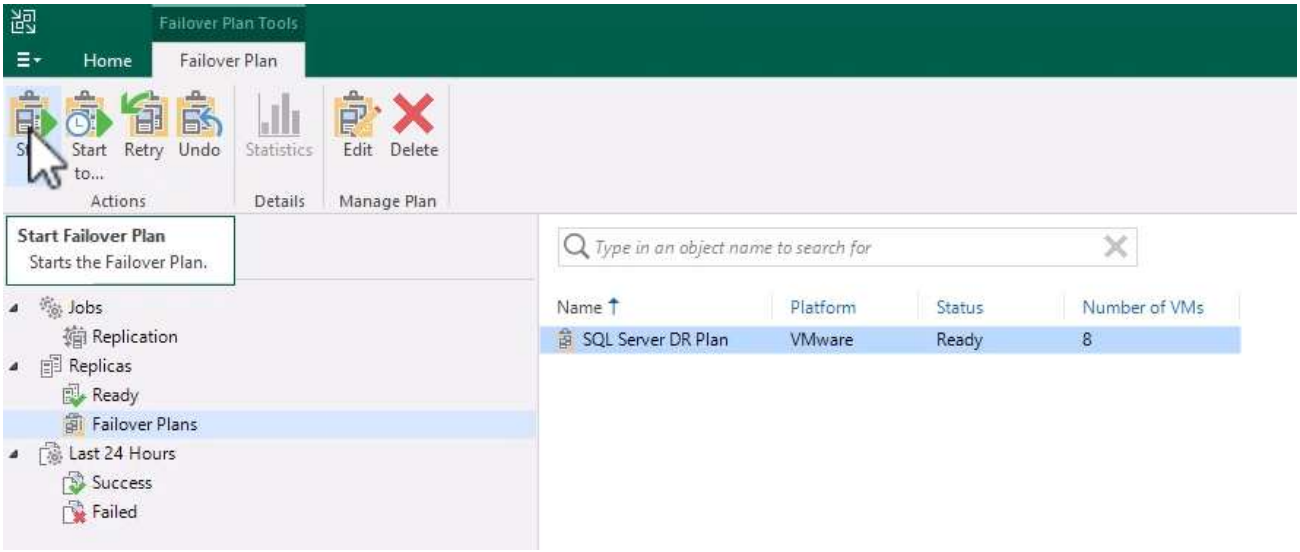
Durante o failover, a VM de origem no site de produção alterna para sua réplica no site de recuperação de

desastres. Como parte do processo, o Veeam Backup & Replication restaura a réplica da VM para o ponto de restauração necessário e transfere todas as atividades de E/S da VM de origem para sua réplica. As réplicas servem não apenas para desastres reais, mas também para simular exercícios de DR. Na simulação de failover, a VM de origem continua em execução. Após a conclusão dos testes necessários, o failover pode ser desfeito, retornando as operações ao normal.

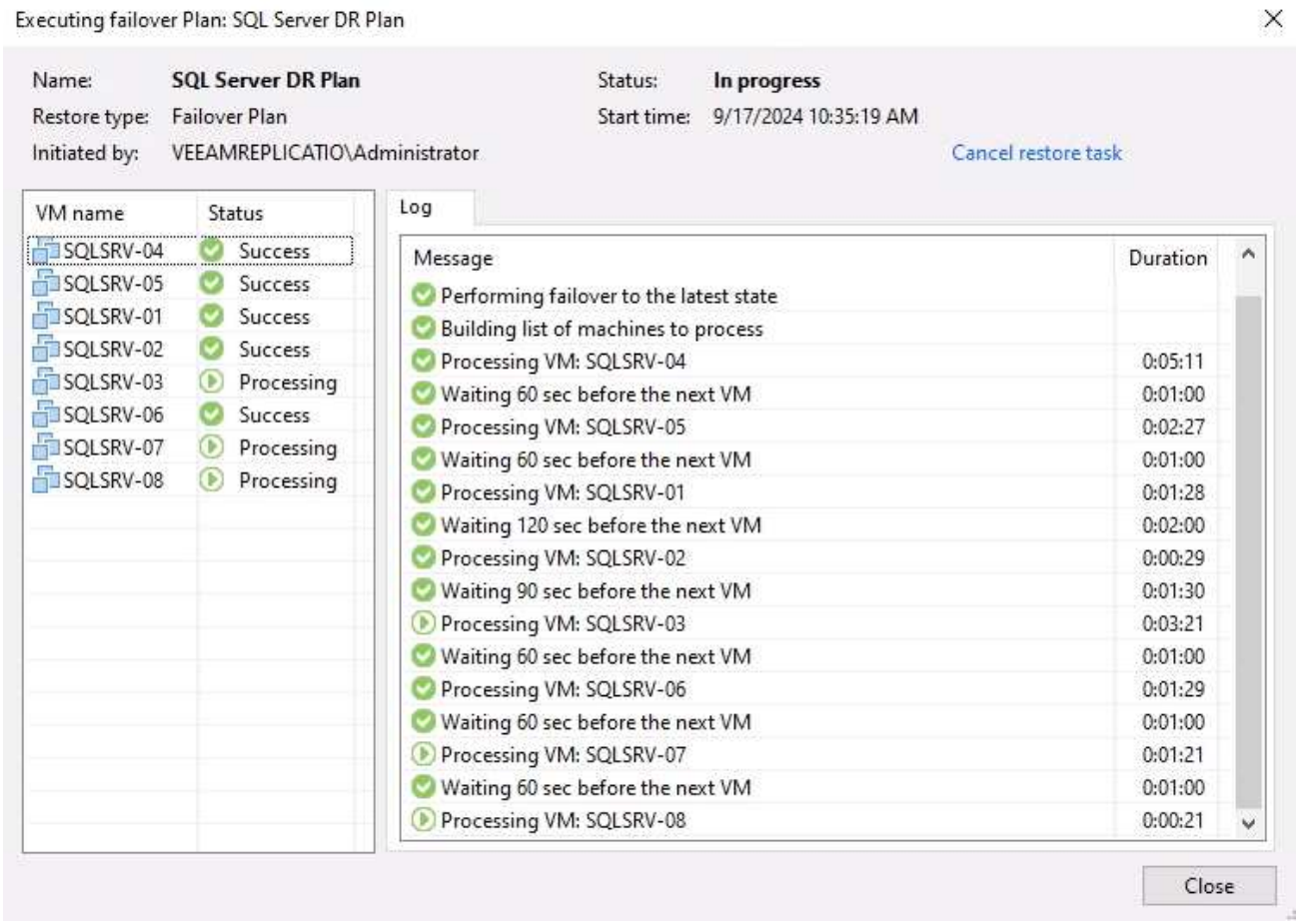
Certifique-se de que a segmentação de rede esteja em vigor para evitar conflitos de IP durante o failover.

Conclua as seguintes etapas para iniciar o plano de failover:

1. Para começar, na visualização **Início**, clique em **Réplicas > Planos de Failover** no menu à esquerda e depois no botão **Iniciar**. Como alternativa, o botão **Iniciar para…** pode ser usado para fazer failover para um ponto de restauração anterior.



2. Monitore o progresso do failover na janela **Executando plano de failover**.



O Veeam Backup & Replication interrompe todas as atividades de replicação da VM de origem até que sua réplica retorne ao estado Pronto.

Para obter informações detalhadas sobre planos de failover, consulte"Planos de Failover" .

▼ **Failback para o site de produção**

A realização de um failover é considerada uma etapa intermediária e precisa ser finalizada com base no requisito. As opções incluem o seguinte:

- **Failback para produção** - Reverta para a VM original e sincronize todas as modificações feitas durante o período ativo da réplica de volta para a VM de origem.

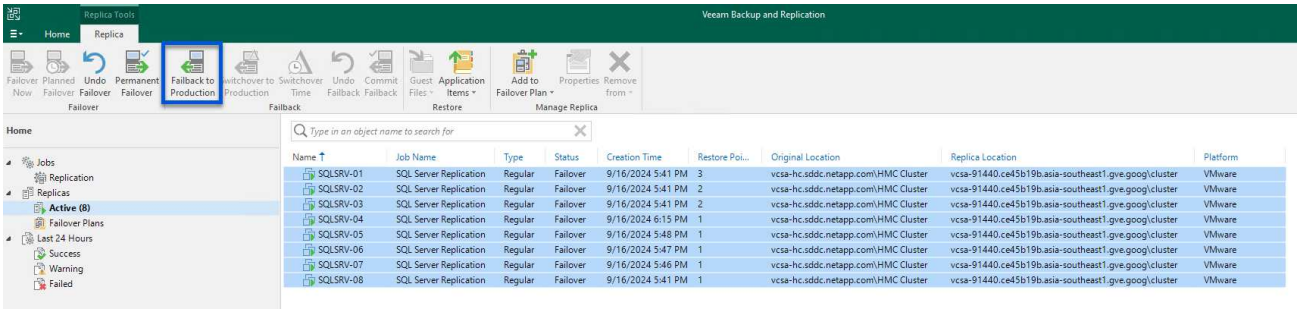
Durante o failback, as alterações são transferidas, mas não aplicadas imediatamente. Selecione **Confirmar failback** depois que a funcionalidade da VM original for verificada. Como alternativa, escolha **Desfazer failback** para reverter para a réplica da VM se a VM original apresentar comportamento inesperado.

- **Desfazer failover** - Reverta para a VM original, descartando todas as alterações feitas na réplica da VM durante seu período operacional.
- **Failover permanente** - Alterne permanentemente da VM original para sua réplica, estabelecendo a réplica como a nova VM primária para operações em andamento.

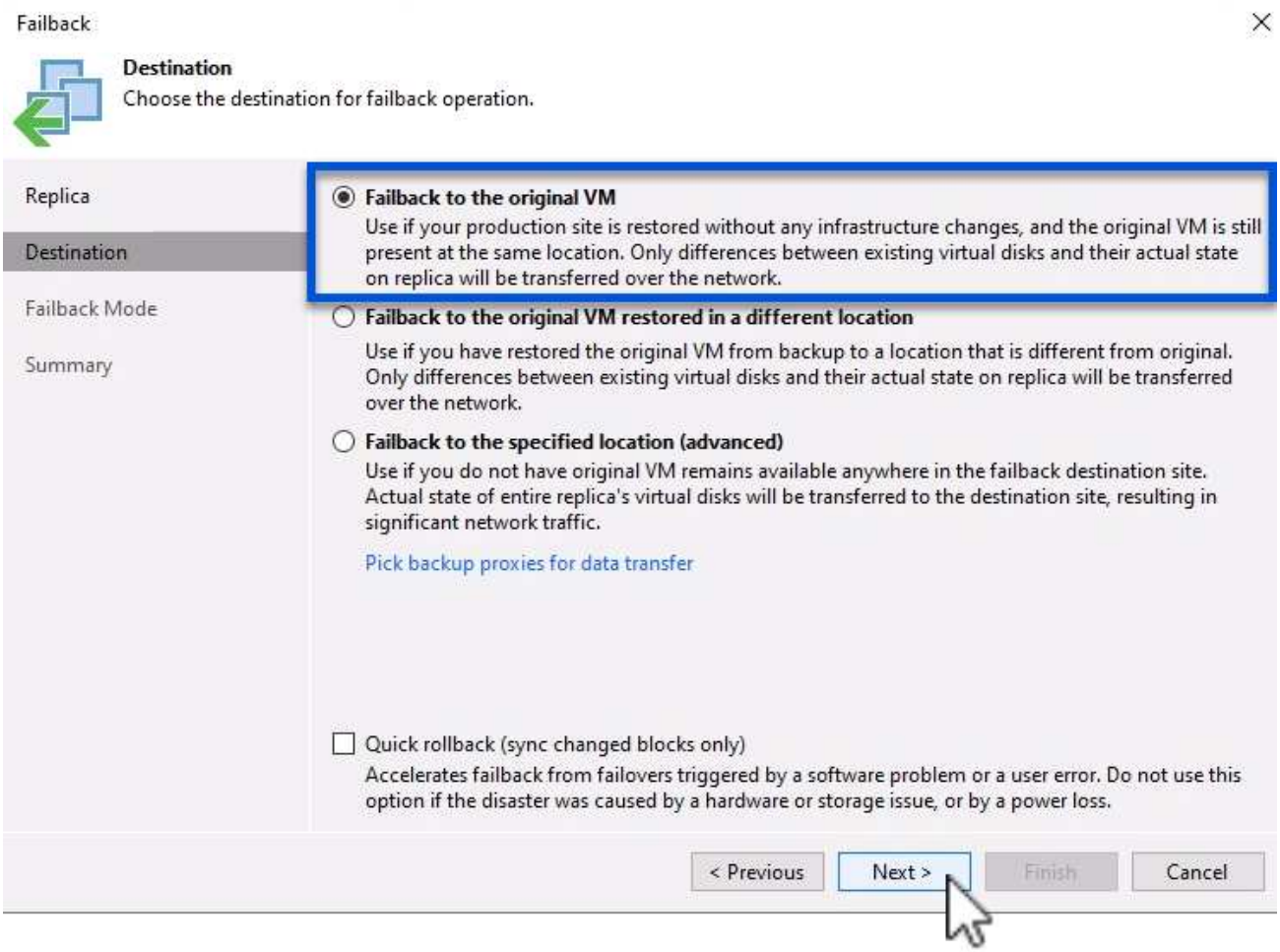
Neste cenário, a opção "Failback para produção" foi selecionada.

Conclua as seguintes etapas para executar um failback para o site de produção:

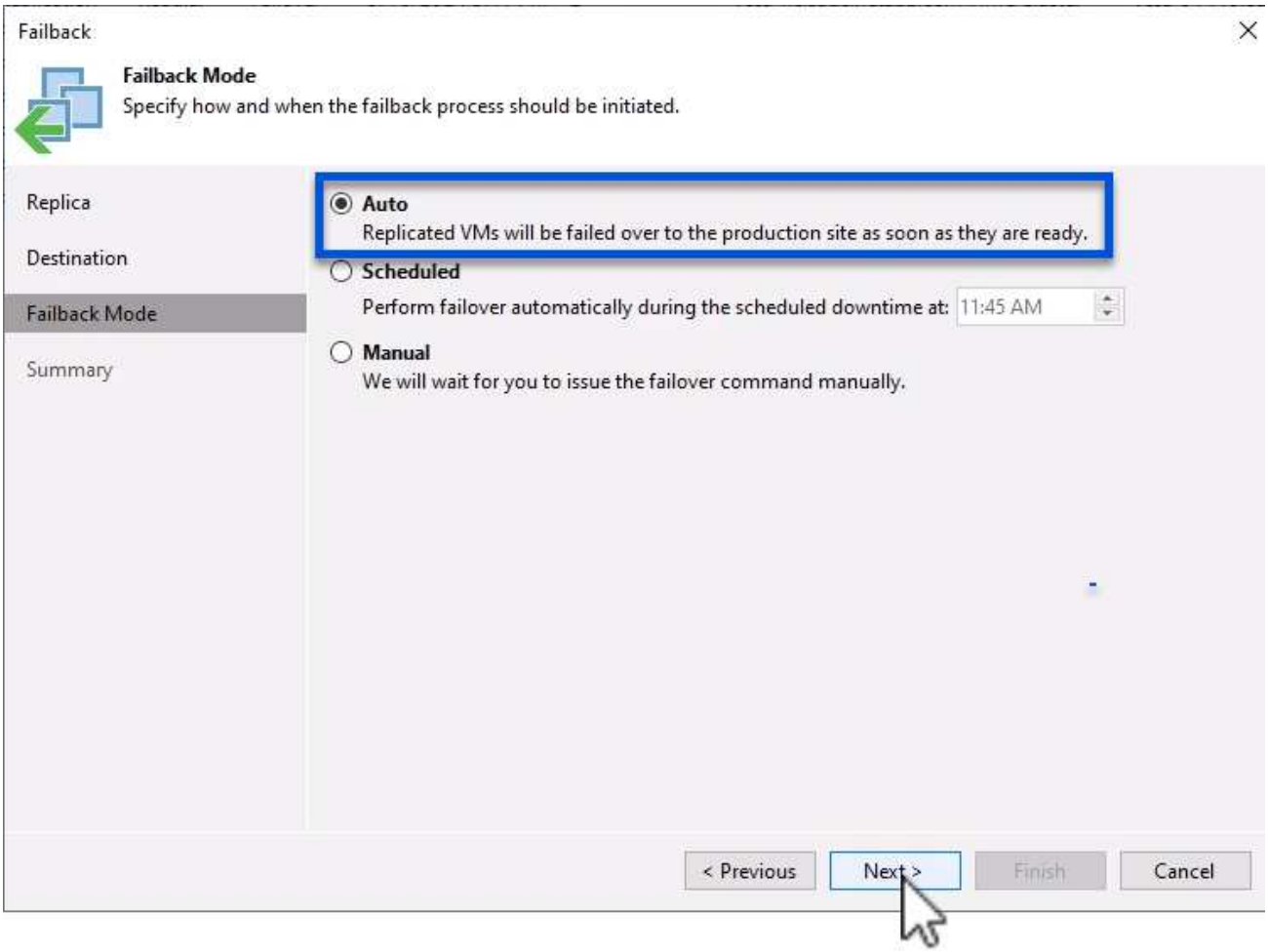
1. Na visualização **Início**, clique em **Réplicas > Ativas** no menu à esquerda. Selecione as VMs a serem incluídas e clique no botão **Failback para produção** no menu superior.



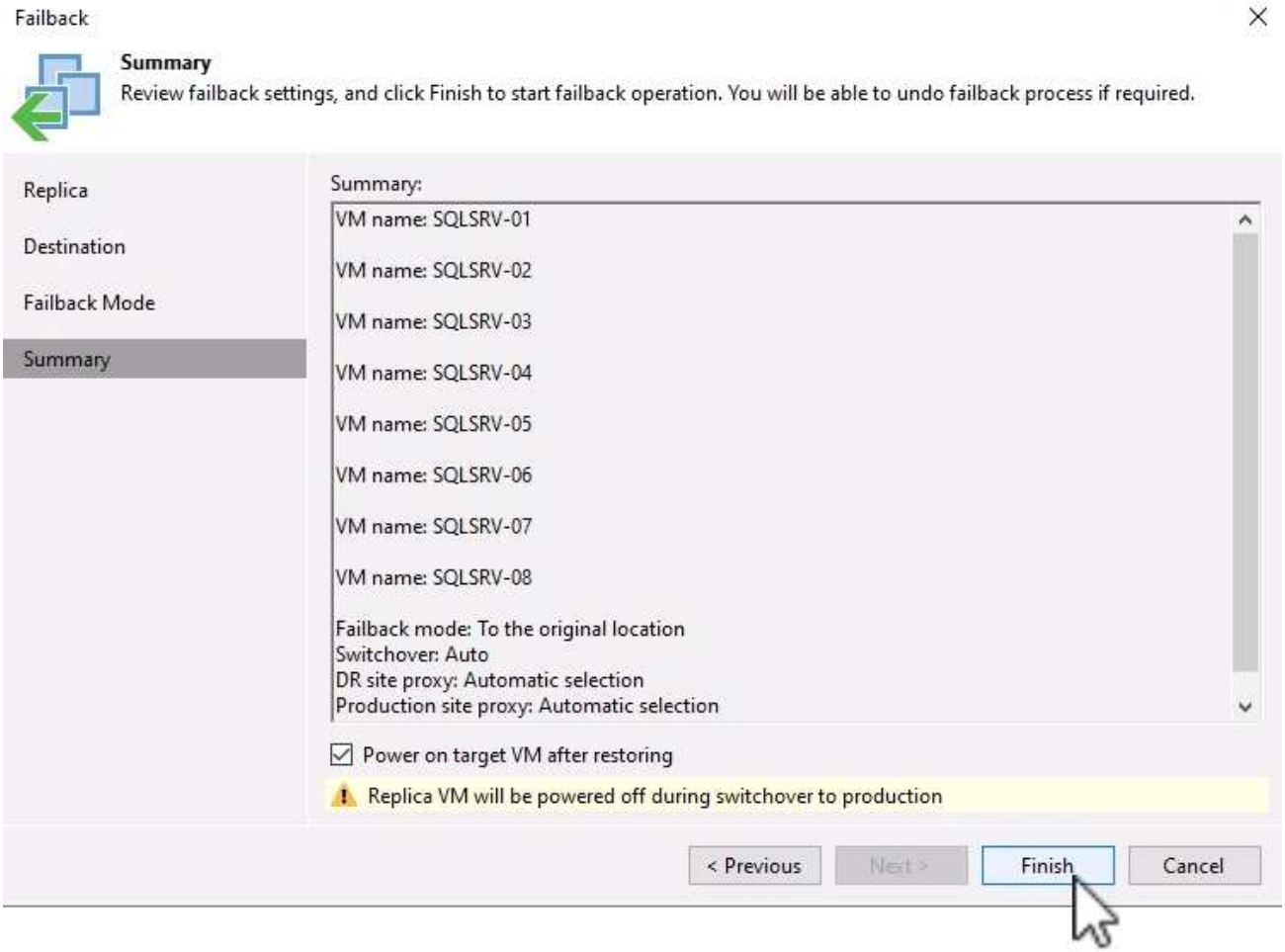
2. Na página **Réplica** do assistente **Failback**, selecione as réplicas a serem incluídas no trabalho de failback.
3. Na página **Destino**, selecione **Failback para a VM original** e clique em **Avançar** para continuar.



4. Na página **Modo de failback**, selecione **Automático** para iniciar o failback o mais rápido possível.

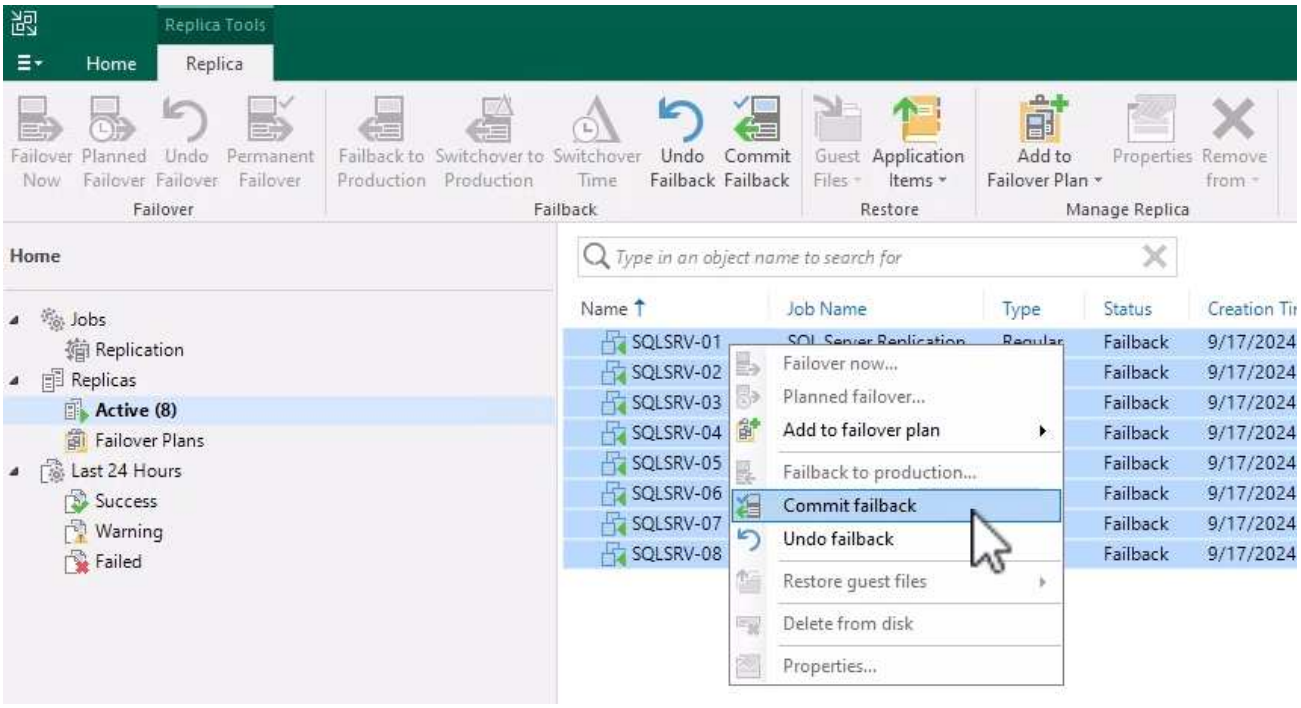


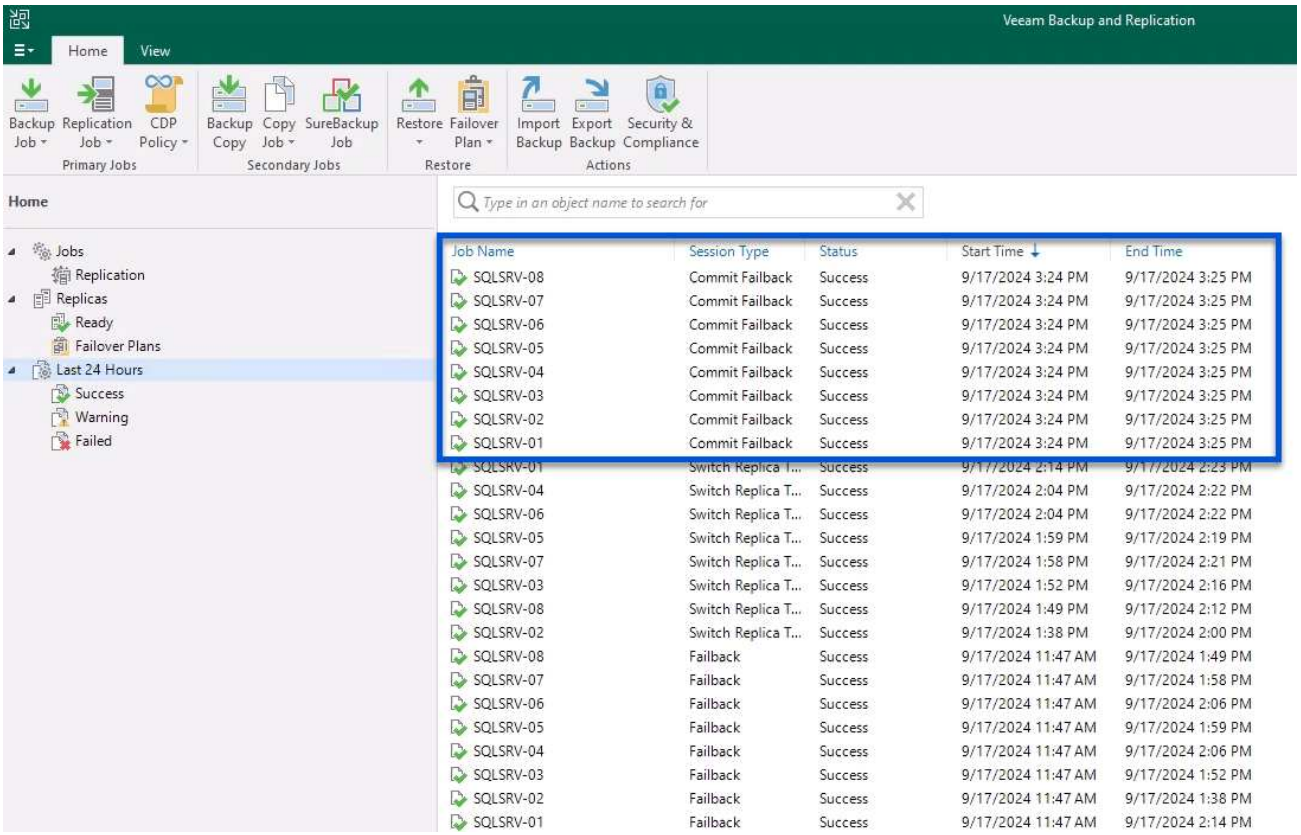
5. Na página **Resumo**, escolha se deseja **Ligar a VM de destino após a restauração** e clique em Concluir para iniciar o trabalho de failback.



A confirmação de failback finaliza a operação de failback, confirmando a integração bem-sucedida das alterações na VM de produção. Após a confirmação, o Veeam Backup & Replication retoma as atividades regulares de replicação para a VM de produção restaurada. Isso altera o status da réplica restaurada de *Failback* para *Pronto*.

1. Para confirmar o failback, navegue até **Réplicas > Ativo**, selecione as VMs a serem confirmadas, clique com o botão direito e selecione **Confirmar failback**.





Após o failback para produção ser bem-sucedido, todas as VMs serão restauradas para o site de produção original.

Para obter informações detalhadas sobre o processo de failback, consulte a documentação do Veeam para"Failover e Failback para replicação" .

Conclusão

A funcionalidade de armazenamento de dados do Google Cloud NetApp Volumes capacita a Veeam e outras ferramentas de terceiros validadas a fornecer soluções de recuperação de desastres (DR) econômicas. Ao utilizar clusters Pilot Light em vez de grandes clusters dedicados para réplicas de VM, as organizações podem reduzir significativamente as despesas. Essa abordagem permite estratégias de DR personalizadas que aproveitam soluções de backup internas existentes para recuperação de desastres baseada em nuvem, eliminando a necessidade de datacenters locais adicionais. Em caso de desastre, o failover pode ser iniciado com um único clique ou configurado para ocorrer automaticamente, garantindo a continuidade dos negócios com tempo de inatividade mínimo.

Para saber mais sobre esse processo, fique à vontade para seguir o vídeo passo a passo detalhado.

https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=b2fb8597-c3fe-49e2-8a84-b1f10118db6d

Migrar cargas de trabalho no GCP/GCVE

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

Um dos casos de uso mais comuns para o armazenamento de dados do Google Cloud VMware Engine e do Cloud Volume Service é a migração de cargas de trabalho do VMware. O VMware HCX é uma opção preferencial e fornece vários mecanismos de migração para mover máquinas virtuais (VMs) locais e seus dados para armazenamentos de dados NFS do Cloud Volume Service.

Visão geral: Migrando máquinas virtuais com VMware HCX, datastores do Google Cloud NetApp Volumes e Google Cloud VMware Engine (GCVE)

O VMware HCX é principalmente uma plataforma de migração projetada para simplificar a migração de aplicativos, o rebalanceamento de carga de trabalho e até mesmo a continuidade dos negócios entre nuvens. Ele está incluído como parte do Google Cloud VMware Engine Private Cloud e oferece muitas maneiras de migrar cargas de trabalho e pode ser usado para operações de recuperação de desastres (DR).

Este documento fornece orientação passo a passo para provisionar o armazenamento de dados do Cloud Volume Service, seguido pelo download, implantação e configuração do VMware HCX, incluindo todos os seus principais componentes no local e no Google Cloud VMware Engine, incluindo interconexão, extensão de rede e otimização de WAN para habilitar vários mecanismos de migração de VM.

> ⓘ O VMware HCX funciona com qualquer tipo de armazenamento de dados, pois a migração ocorre no nível da VM. Portanto, este documento é aplicável a clientes atuais da NetApp e clientes não pertencentes à NetApp que planejam implantar o Cloud Volume Service com o Google Cloud VMware Engine para uma implantação de nuvem VMware econômica.

▼ **Etapas de alto nível**

Esta lista fornece as etapas de alto nível necessárias para emparelhar e migrar as VMs para o HCX Cloud Manager no lado do Google Cloud VMware Engine a partir do HCX Connector local:

1. Prepare o HCX por meio do portal do Google VMware Engine.
2. Baixe e implante o instalador do HCX Connector Open Virtualization Appliance (OVA) no VMware vCenter Server local.
3. Ative o HCX com a chave de licença.

4. Emparelhe o VMware HCX Connector local com o Google Cloud VMware Engine HCX Cloud Manager.
5. Configure o perfil de rede, o perfil de computação e a malha de serviço.
6. (Opcional) Execute a extensão da rede para evitar a troca de IP durante migrações.
7. Valide o status do dispositivo e garanta que a migração seja possível.
8. Migre as cargas de trabalho da VM.

▼ Pré-requisitos

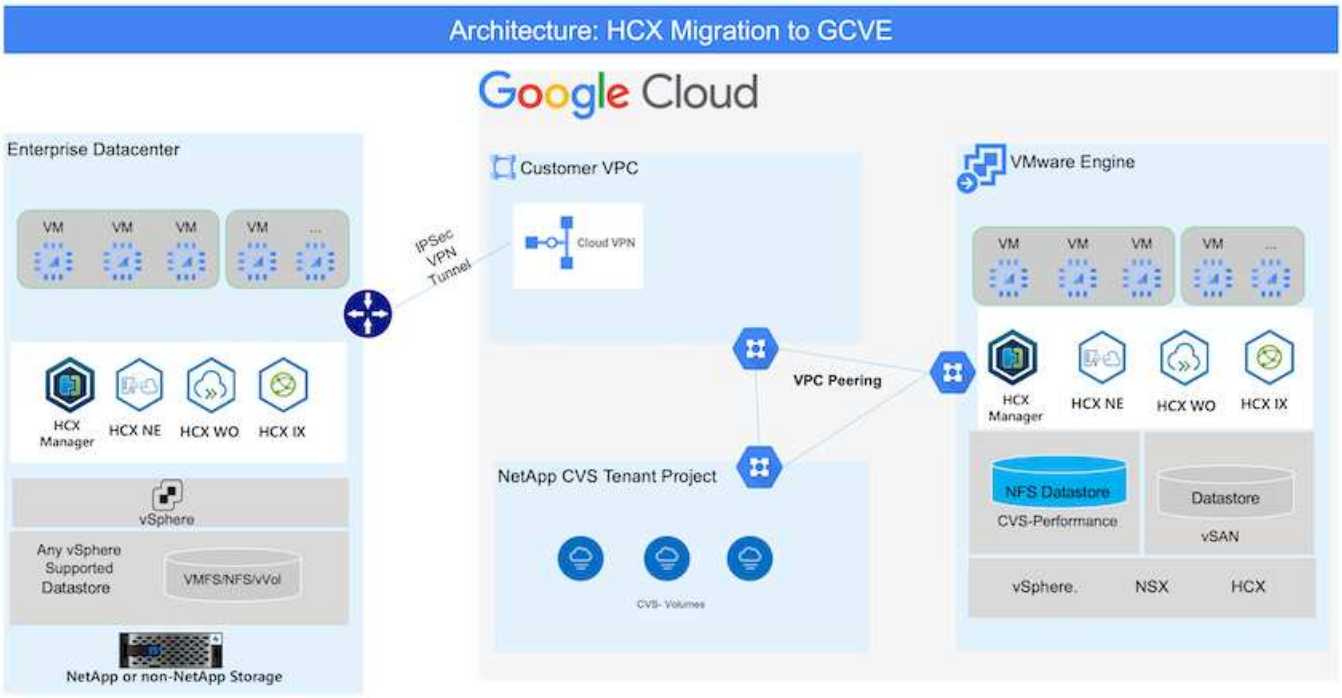
Antes de começar, certifique-se de que os seguintes pré-requisitos sejam atendidos. Para mais informações, consulte isto "link" . Depois que os pré-requisitos, incluindo conectividade, estiverem prontos, baixe a chave de licença do HCX no portal do Google Cloud VMware Engine. Após o download do instalador do OVA, prossiga com o processo de instalação conforme descrito abaixo.

> ⓘ O HCX Advanced é a opção padrão e a edição VMware HCX Enterprise também está disponível por meio de um tíquete de suporte e tem suporte sem custo adicional. Referir "este link"

- Use um data center definido por software (SDDC) do Google Cloud VMware Engine existente ou crie uma nuvem privada usando este"Link da NetApp" ou isto "Link do Google" .
- A migração de VMs e dados associados do data center habilitado para VMware vSphere local requer conectividade de rede do data center para o ambiente SDDC. Antes de migrar cargas de trabalho, "configurar uma conexão Cloud VPN ou Cloud Interconnect" entre o ambiente local e a respectiva nuvem privada.
- O caminho de rede do ambiente VMware vCenter Server local para a nuvem privada do Google Cloud VMware Engine deve oferecer suporte à migração de VMs usando o vMotion.
- Certifique-se de que o necessário "regras e portas de firewall" são permitidos para tráfego vMotion entre o vCenter Server local e o SDDC vCenter.
- O volume NFS do Cloud Volume Service deve ser montado como um armazenamento de dados no Google Cloud VMware Engine. Siga os passos detalhados neste "link" para anexar armazenamentos de dados do Cloud Volume Service aos hosts do Google Cloud VMware Engines.

▼ Arquitetura de Alto Nível

Para fins de teste, o ambiente de laboratório local usado para esta validação foi conectado por meio de uma VPN na nuvem, que permite conectividade local com o Google Cloud VPC.



Para obter mais detalhes sobre o uso do VMware HCX com o Google, consulte "Link VMware"

Implantação de solução

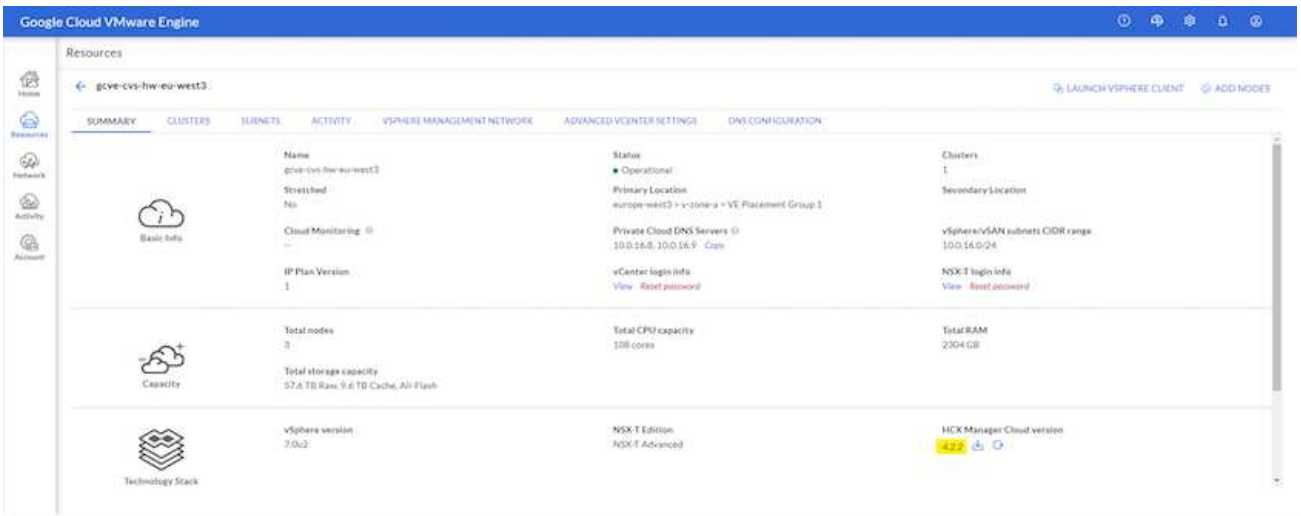
Siga a série de etapas para concluir a implantação desta solução:

▼ **Etapa 1: preparar o HCX por meio do portal do Google VMware Engine**

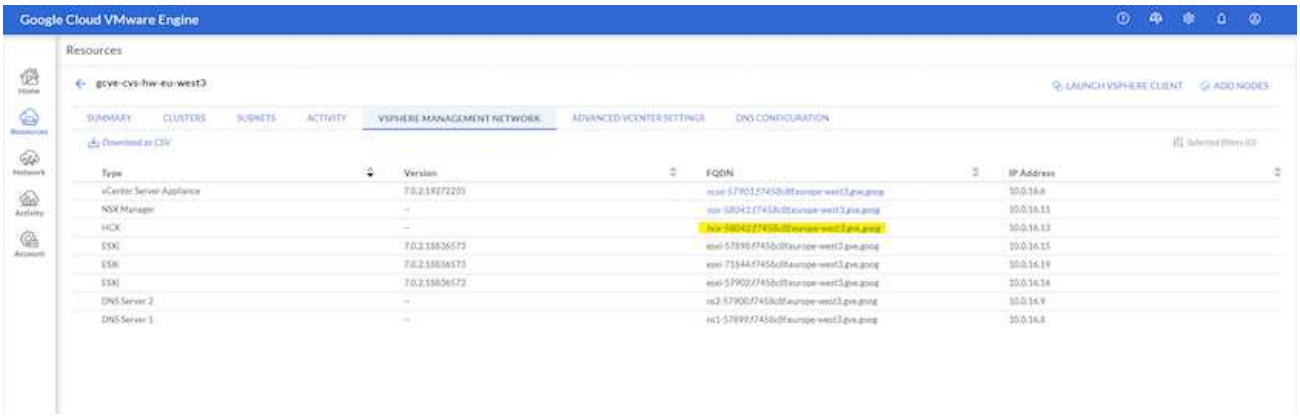
O componente HCX Cloud Manager é instalado automaticamente conforme você provisiona a nuvem privada com o VMware Engine. Para se preparar para o pareamento do site, conclua as seguintes etapas:

1. Faça login no Google VMware Engine Portal e entre no HCX Cloud Manager.

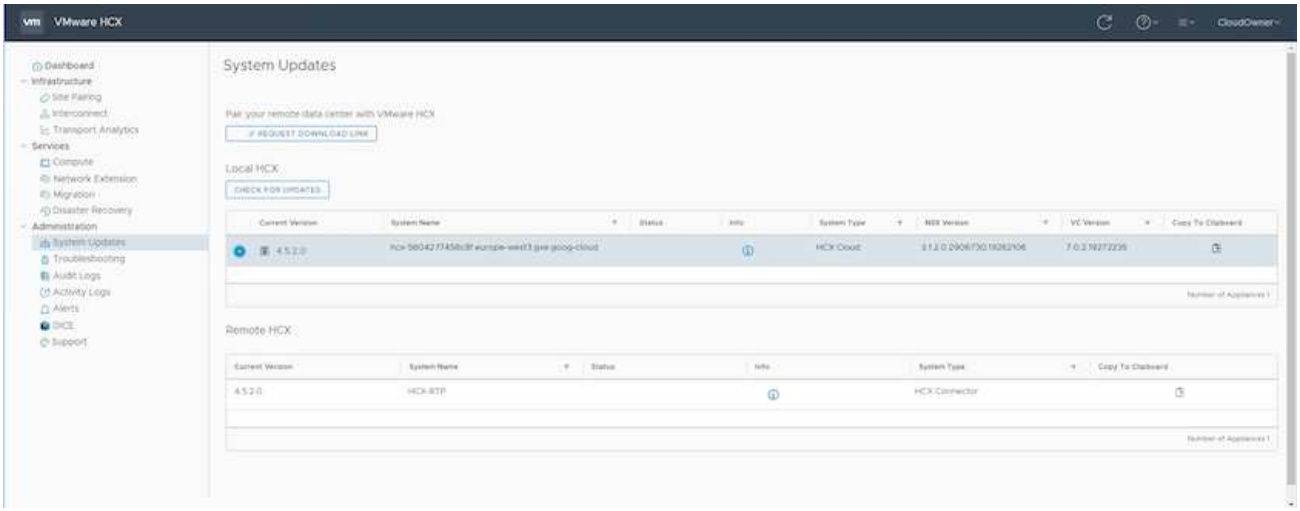
   Você pode fazer login no HCX Console clicando no link da versão HCX



   ou clicando em HCX FQDN na guia vSphere Management Network.



2. No HCX Cloud Manager, acesse **Administração > Atualizações do sistema**.
3. Clique em **Solicitar link de download** e baixe o arquivo OVA.



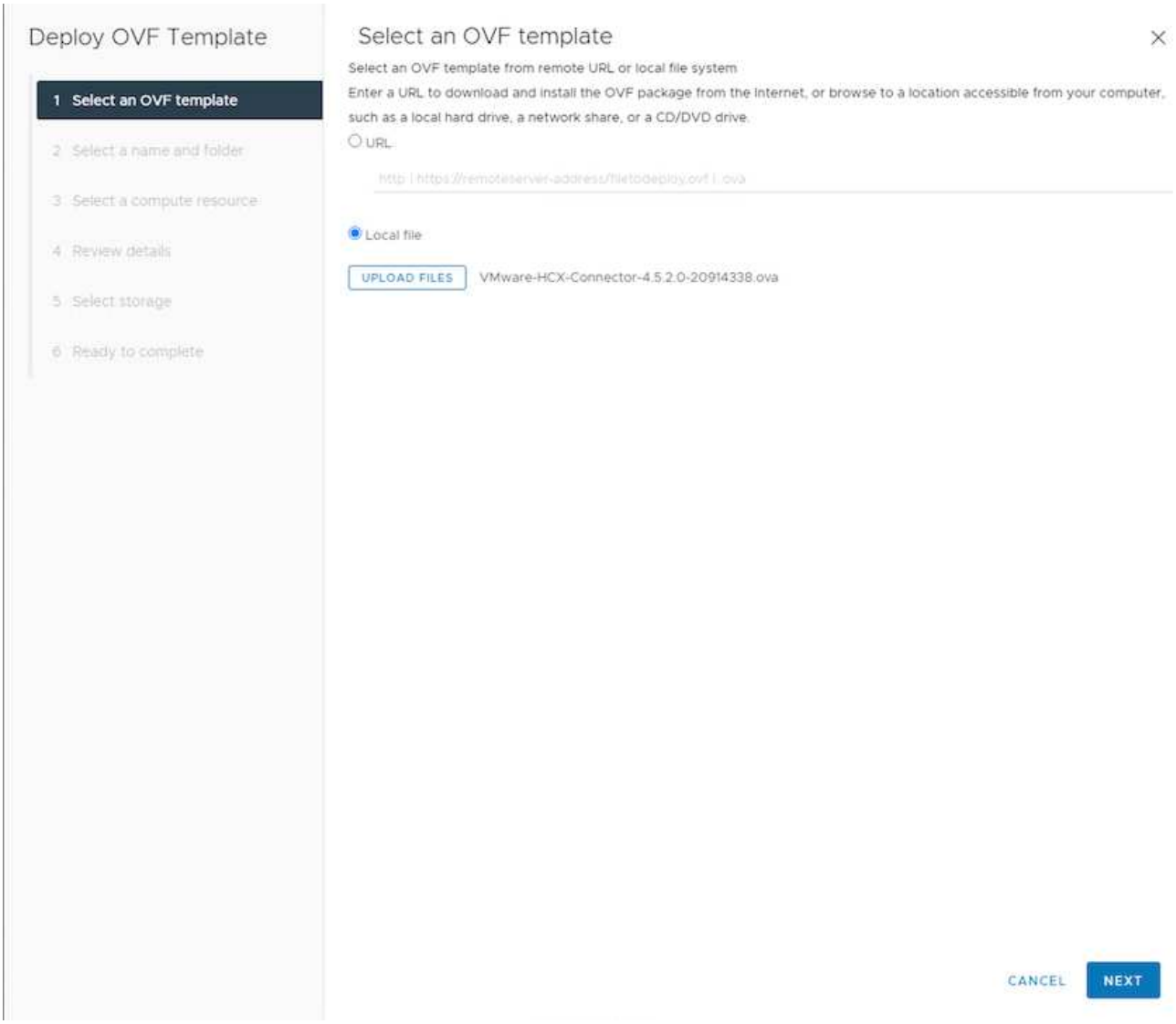
4. Atualize o HCX Cloud Manager para a versão mais recente disponível na interface do usuário do HCX Cloud Manager.

▼ **Etapa 2: implantar o instalador OVA no vCenter Server local**

Para que o conector local se conecte ao HCX Manager no Google Cloud VMware Engine, certifique-se de que as portas de firewall apropriadas estejam abertas no ambiente local.

Para baixar e instalar o HCX Connector no vCenter Server local, conclua as seguintes etapas:

1. Faça o download dos ova do Console HCX no Google Cloud VMware Engine, conforme indicado na etapa anterior.
2. Após o download do OVA, implante-o no ambiente VMware vSphere local usando a opção **Implantar modelo OVF**.



3. Insira todas as informações necessárias para a implantação do OVA, clique em **Avançar** e, em seguida, clique em **Concluir** para implantar o OVA do conector VMware HCX.

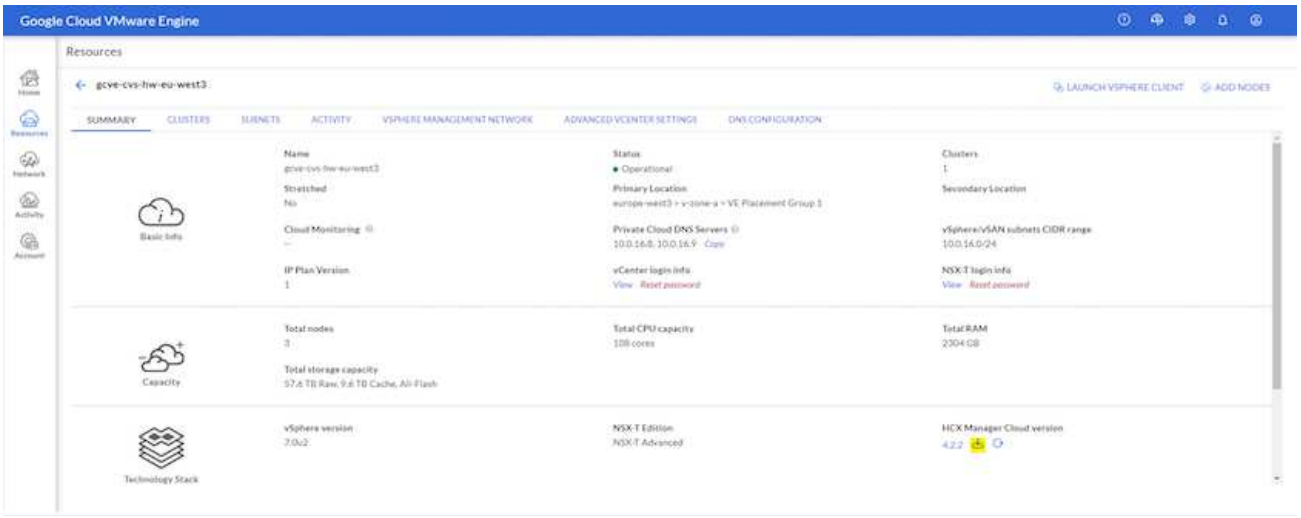
   Ligue o dispositivo virtual manualmente.

Para obter instruções passo a passo, consulte o "Documentação do Google HCX" .

▼ **Etapa 3: Ative o HCX Connector com a chave de licença**

Depois de implantar o VMware HCX Connector OVA no local e iniciar o dispositivo, conclua as seguintes etapas para ativar o HCX Connector. Gere a chave de licença no portal do Google Cloud VMware Engine e ative-a no VMware HCX Manager.

1. No portal do VMware Engine, clique em Recursos, selecione a nuvem privada e **clique no ícone de download em Versão da nuvem do HCX Manager**.



Abra o arquivo baixado e copie a sequência da chave de licença.

2. Efetue login no VMware HCX Manager local em `"https://hcxmanagerIP:9443"` usando credenciais de administrador.

   Use o hcxmanagerIP e a senha definidos durante a implantação do OVA.

3. No licenciamento, insira a chave copiada do passo 3 e clique em **Ativar**.

   O conector HCX local deve ter acesso à Internet.

4. Em **Local do datacenter**, forneça o local mais próximo para instalar o VMware HCX Manager no local. Clique em **Continuar**.
5. Em **Nome do sistema**, atualize o nome e clique em **Continuar**.
6. Clique em **Sim, Continuar**.
7. Em **Conectar seu vCenter**, forneça o nome de domínio totalmente qualificado (FQDN) ou endereço IP do vCenter Server e as credenciais apropriadas e clique em **Continuar**.

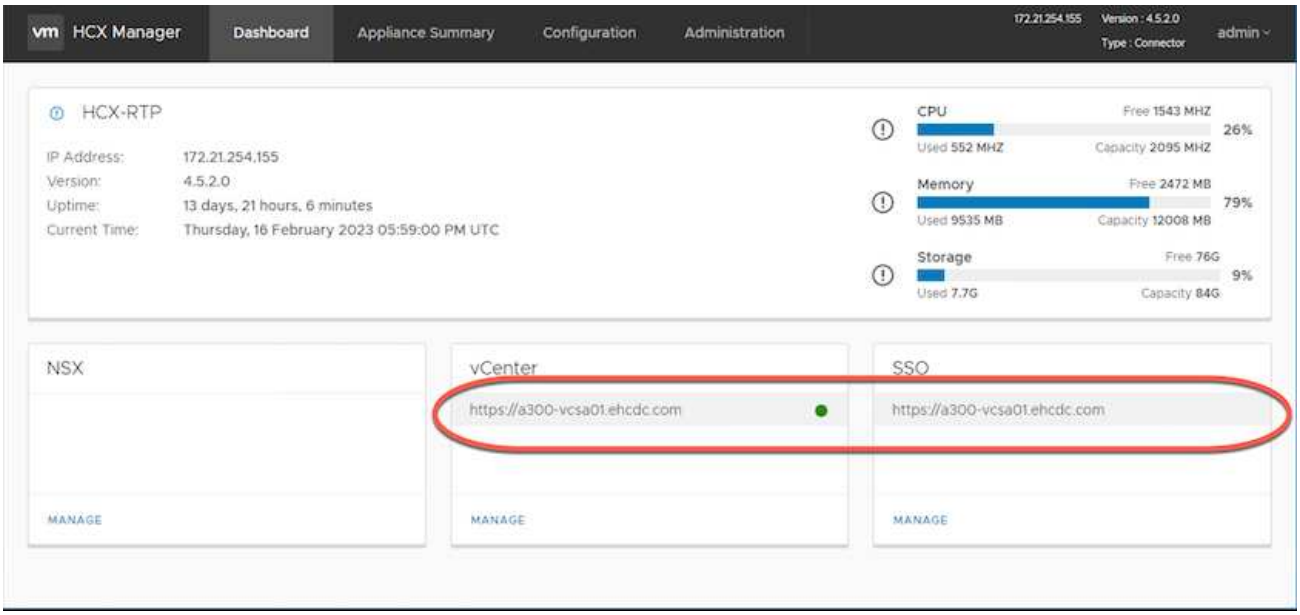
   Use o FQDN para evitar problemas de conectividade mais tarde.

8. Em **Configurar SSO/PSC**, forneça o FQDN ou endereço IP do Controlador de Serviços de Plataforma (PSC) e clique em **Continuar**.

   Para PSC incorporado, insira o FQDN ou endereço IP do VMware vCenter Server.

9. Verifique se as informações inseridas estão corretas e clique em **Reiniciar**.
10. Após a reinicialização dos serviços, o vCenter Server é exibido em verde na página que aparece. Tanto o vCenter Server quanto o SSO devem ter os parâmetros de configuração apropriados, que devem ser os mesmos da página anterior.

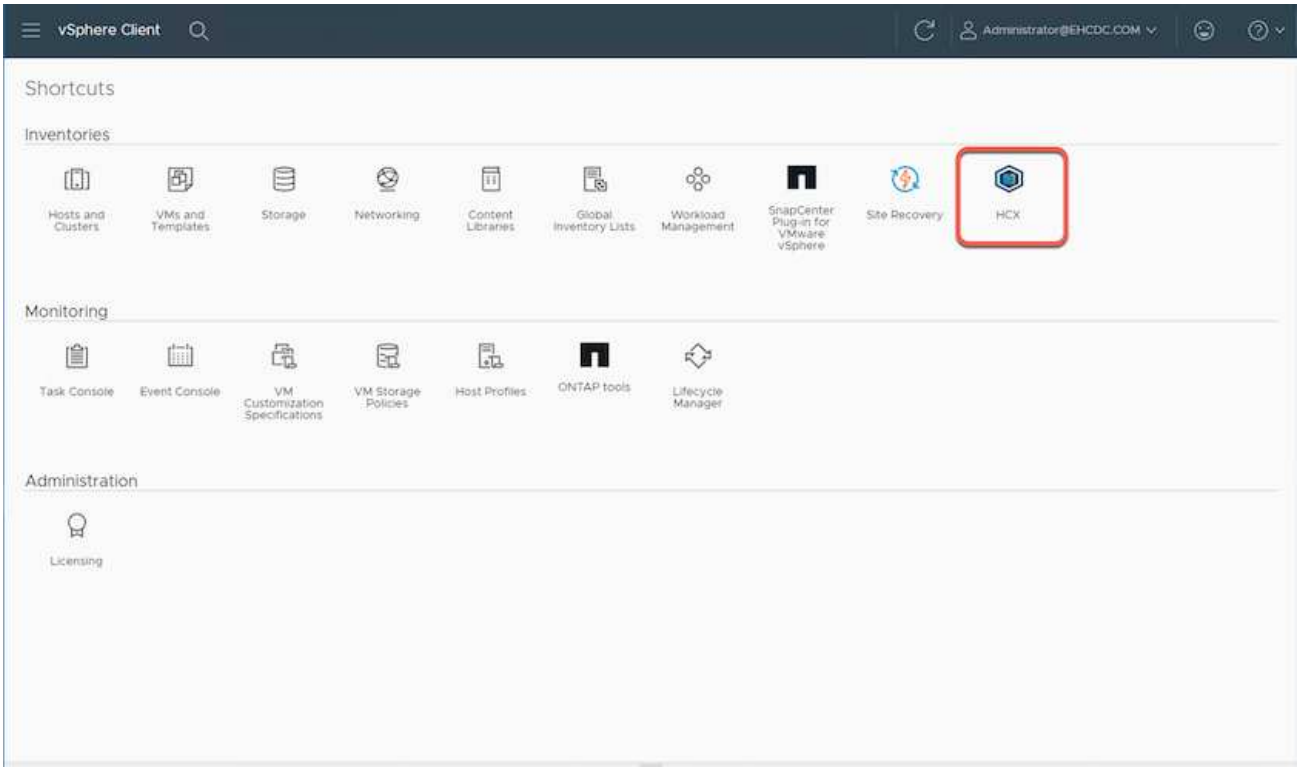
    Esse processo deve levar aproximadamente de 10 a 20 minutos para que o plug-in seja adicionado ao vCenter Server.



▼ Etapa 4: emparelhe o VMware HCX Connector local com o Google Cloud VMware Engine HCX Cloud Manager

Depois que o HCX Connector for implantado e configurado no vCenter local, estabeleça a conexão com o Cloud Manager adicionando o emparelhamento. Para configurar o pareamento de sites, conclua as seguintes etapas:

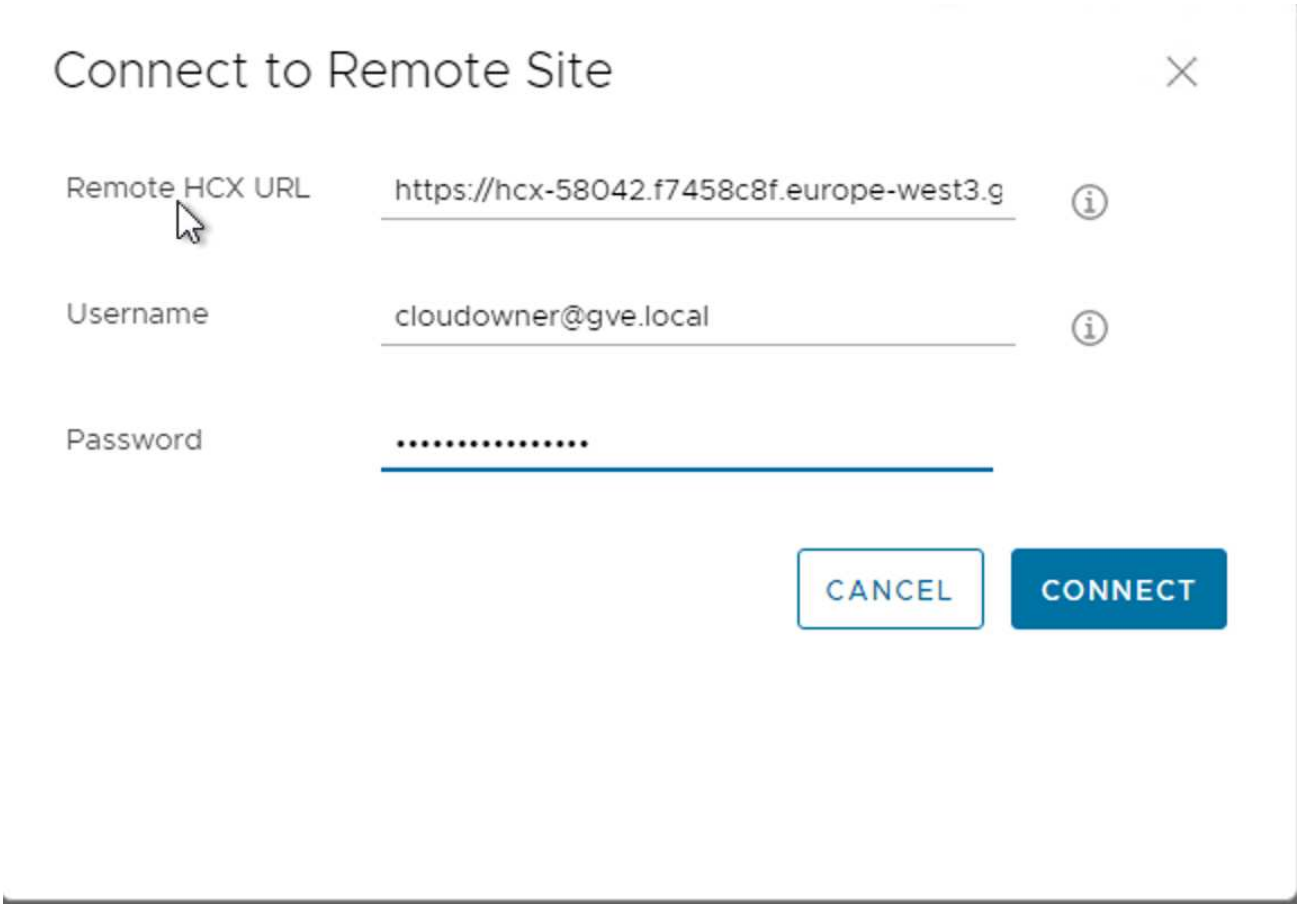
1. Para criar um par de sites entre o ambiente vCenter local e o Google Cloud VMware Engine SDDC, faça login no vCenter Server local e acesse o novo plug-in HCX vSphere Web Client.



2. Em Infraestrutura, clique em **Adicionar um pareamento de sites**.

Insira o URL ou endereço IP do Google Cloud VMware Engine HCX Cloud Manager e as

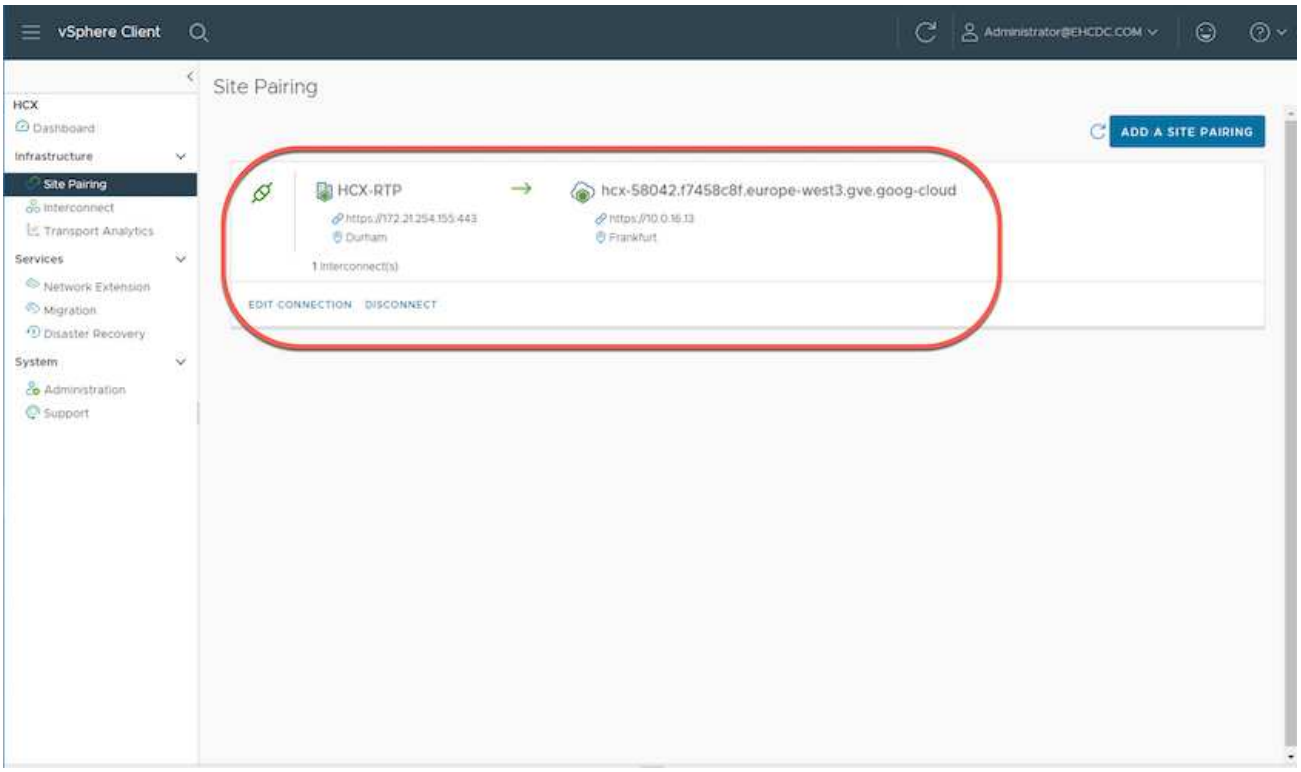
credenciais do usuário com privilégios Cloud-Owner-Role para acessar a nuvem privada.



3. Clique em **Conectar**.

O VMware HCX Connector deve ser capaz de rotear para o IP do HCX Cloud Manager pela porta 443.

4. Após a criação do pareamento, o pareamento do site recém-configurado fica disponível no Painel do HCX.

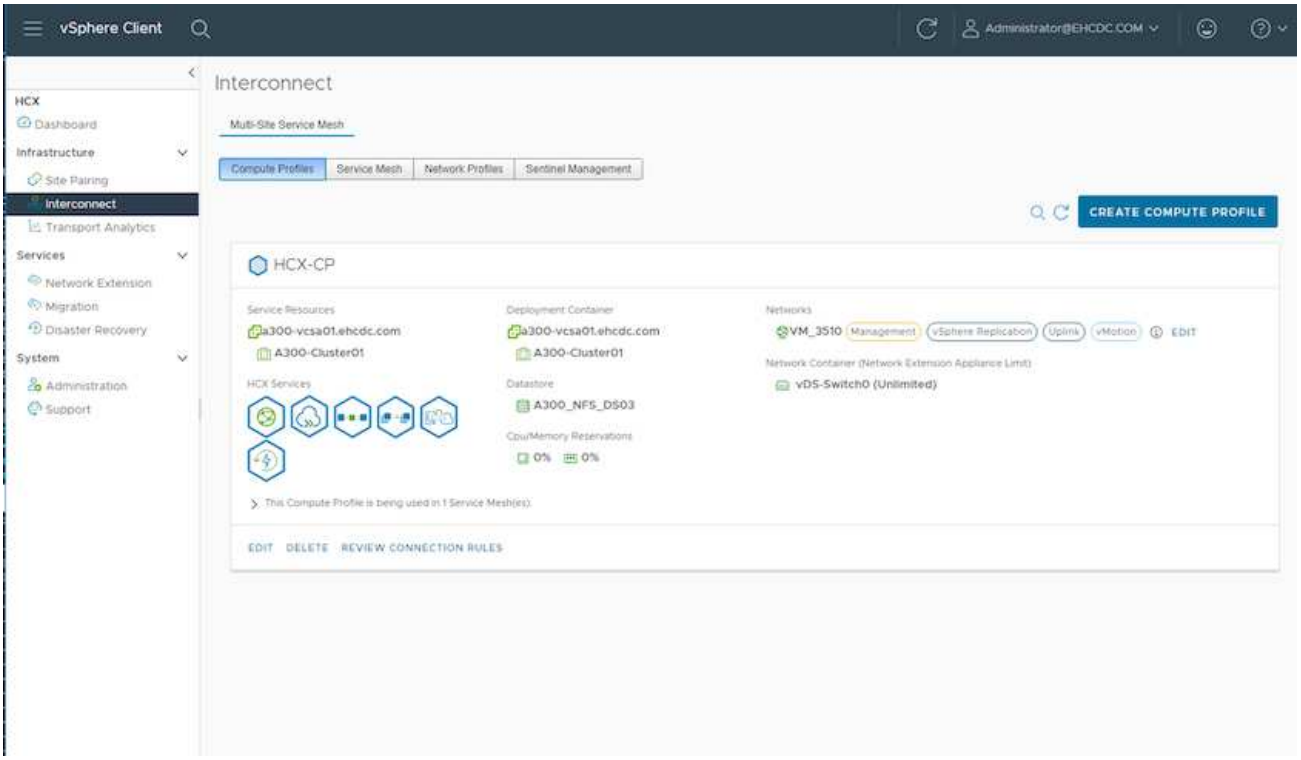


▼ **Etapa 5: configurar o perfil de rede, o perfil de computação e a malha de serviço**

O dispositivo de serviço VMware HCX Interconnect fornece recursos de replicação e migração baseados em vMotion pela Internet e conexões privadas com o site de destino. A interconexão fornece criptografia, engenharia de tráfego e mobilidade de VM. Para criar um dispositivo de serviço de interconexão, conclua as seguintes etapas:

1. Em Infraestrutura, selecione **Interconexão > Malha de serviço multisite > Perfis de computação > Criar perfil de computação**.

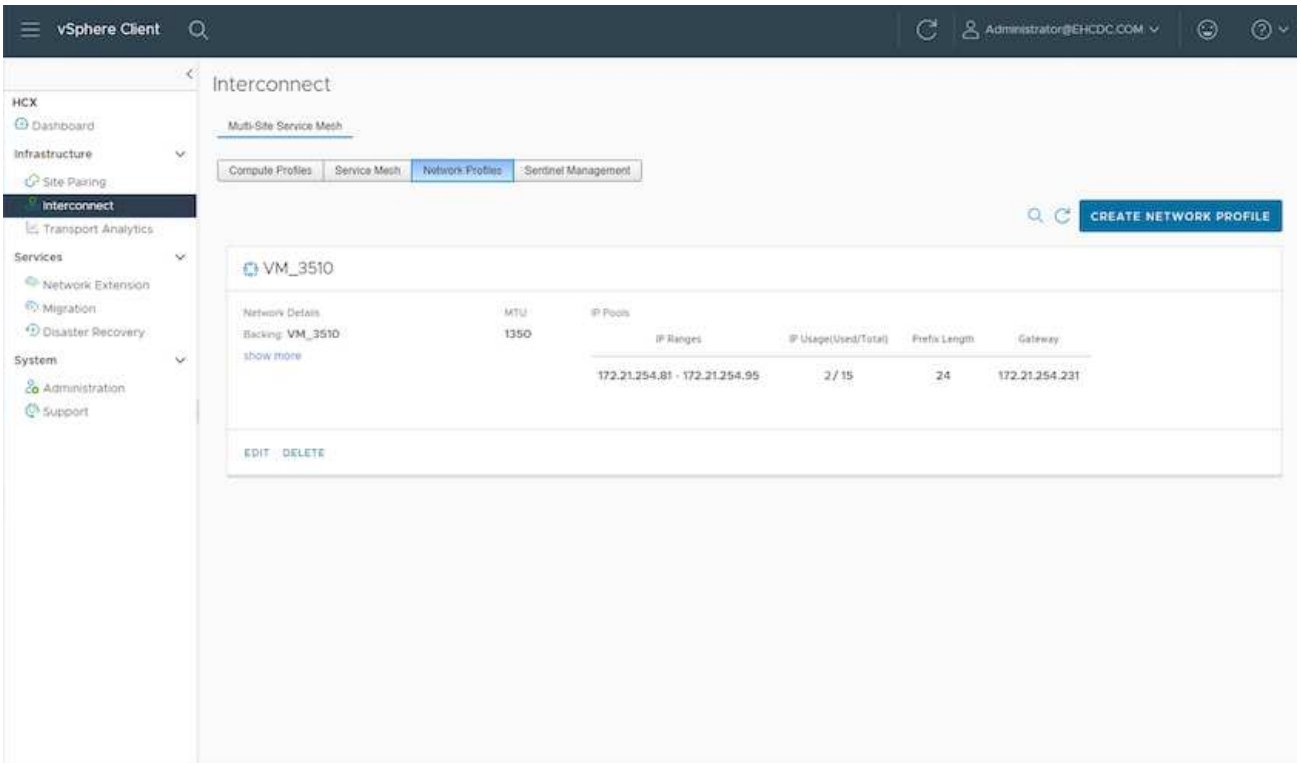
Os perfis de computação definem os parâmetros de implantação, incluindo os dispositivos que são implantados e quais partes do data center VMware são acessíveis ao serviço HCX.



2. Após a criação do perfil de computação, crie os perfis de rede selecionando **Multi-Site Service Mesh > Perfis de rede > Criar perfil de rede**.

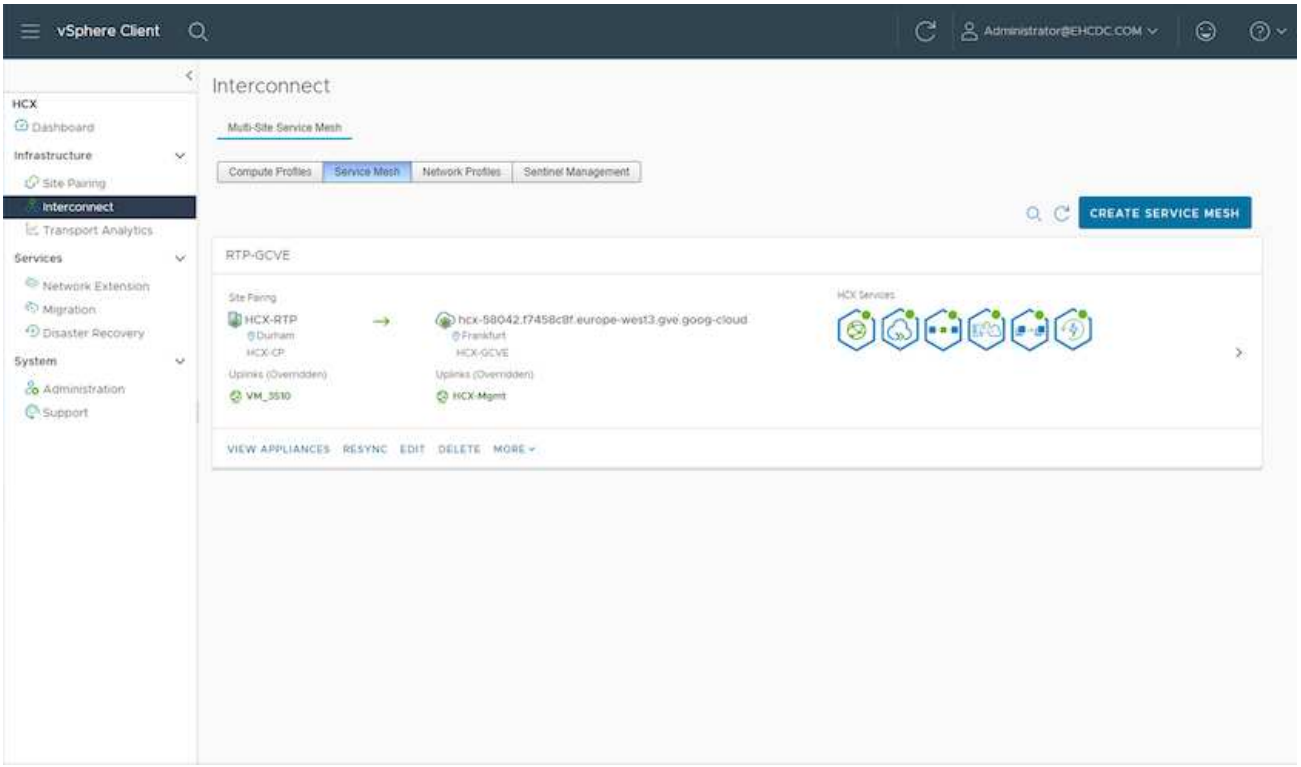
   O perfil de rede define um intervalo de endereços IP e redes que são usados pelo HCX para seus dispositivos virtuais.

   Esta etapa requer dois ou mais endereços IP. Esses endereços IP são atribuídos pela rede de gerenciamento aos dispositivos de interconexão.

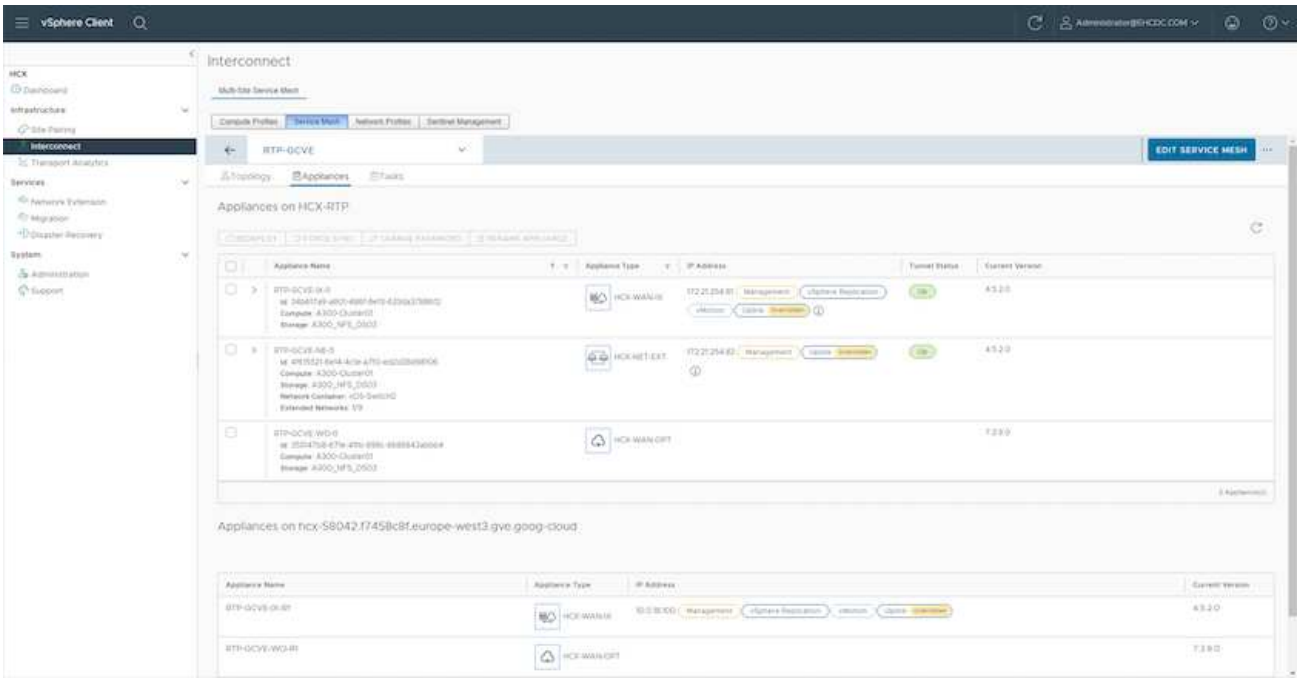


3. Neste momento, os perfis de computação e rede foram criados com sucesso.
4. Crie o Service Mesh selecionando a aba **Service Mesh** dentro da opção **Interconnect** e selecione os sites SDDC locais e GCVE.
5. O Service Mesh especifica um par de perfis de computação e rede locais e remotos.

> Como parte desse processo, os dispositivos HCX são implantados e configurados automaticamente nos sites de origem e de destino para criar uma estrutura de transporte segura.



6. Esta é a etapa final da configuração. A implantação deve levar cerca de 30 minutos para ser concluída. Após a configuração da malha de serviço, o ambiente estará pronto com os túneis IPsec criados com sucesso para migrar as VMs de carga de trabalho.



▼ **Etapa 6: migrar cargas de trabalho**

As cargas de trabalho podem ser migradas bidirecionalmente entre SDDCs locais e GCVE usando várias tecnologias de migração do VMware HCX. As VMs podem ser movidas de e para entidades ativadas pelo VMware HCX usando diversas tecnologias de migração, como migração em massa do HCX, HCX vMotion, migração a frio do HCX, HCX Replication Assisted vMotion (disponível com a edição HCX Enterprise) e HCX OS Assisted Migration (disponível com a edição HCX Enterprise).

Para saber mais sobre os vários mecanismos de migração do HCX, consulte "Migrando VMs VMware usando a documentação do VMware HCX" .

O dispositivo HCX-IX usa o serviço Mobility Agent para executar migrações vMotion, Cold e Replication Assisted vMotion (RAV).

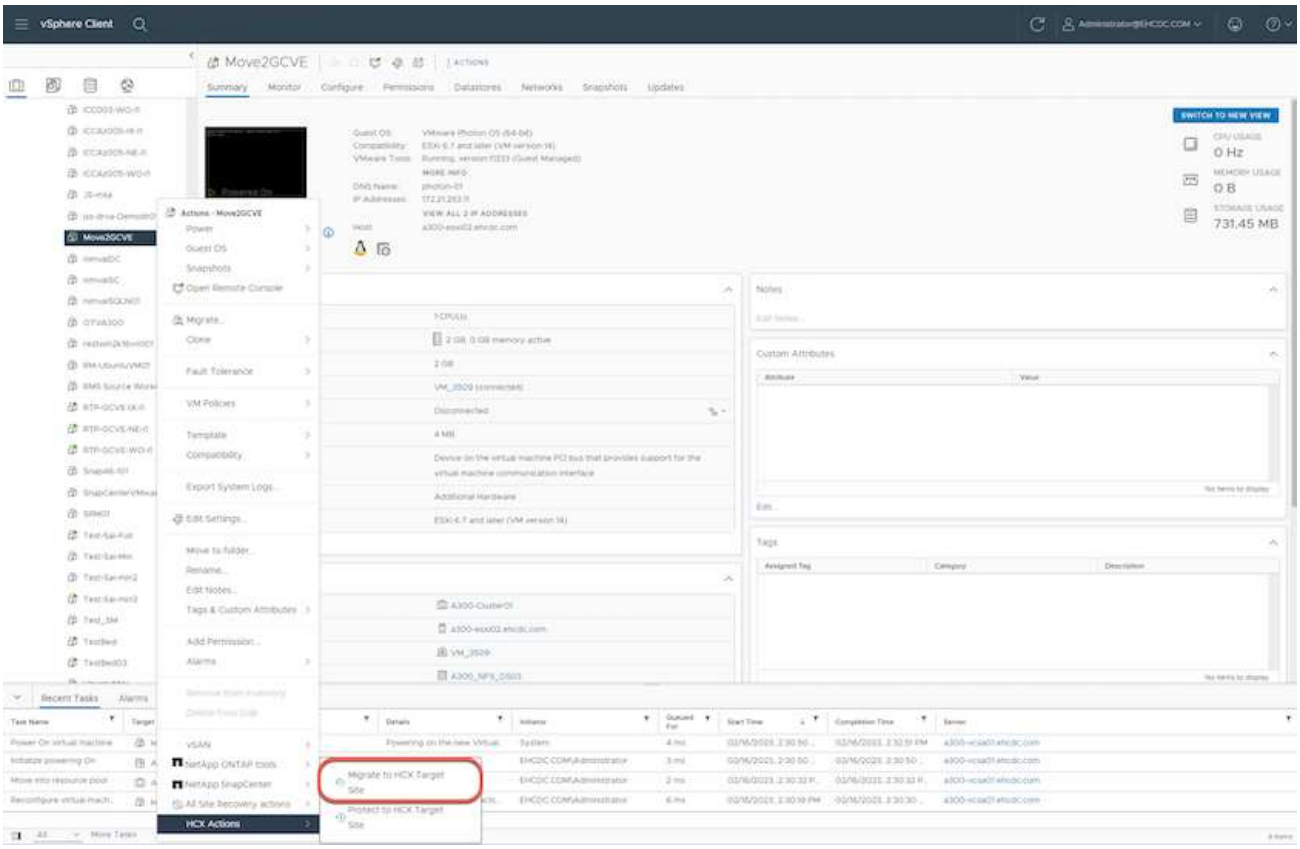
> ⓘ O dispositivo HCX-IX adiciona o serviço Mobility Agent como um objeto de host no vCenter Server. Os recursos de processador, memória, armazenamento e rede exibidos neste objeto não representam o consumo real no hipervisor físico que hospeda o dispositivo IX.

HCX vMotion

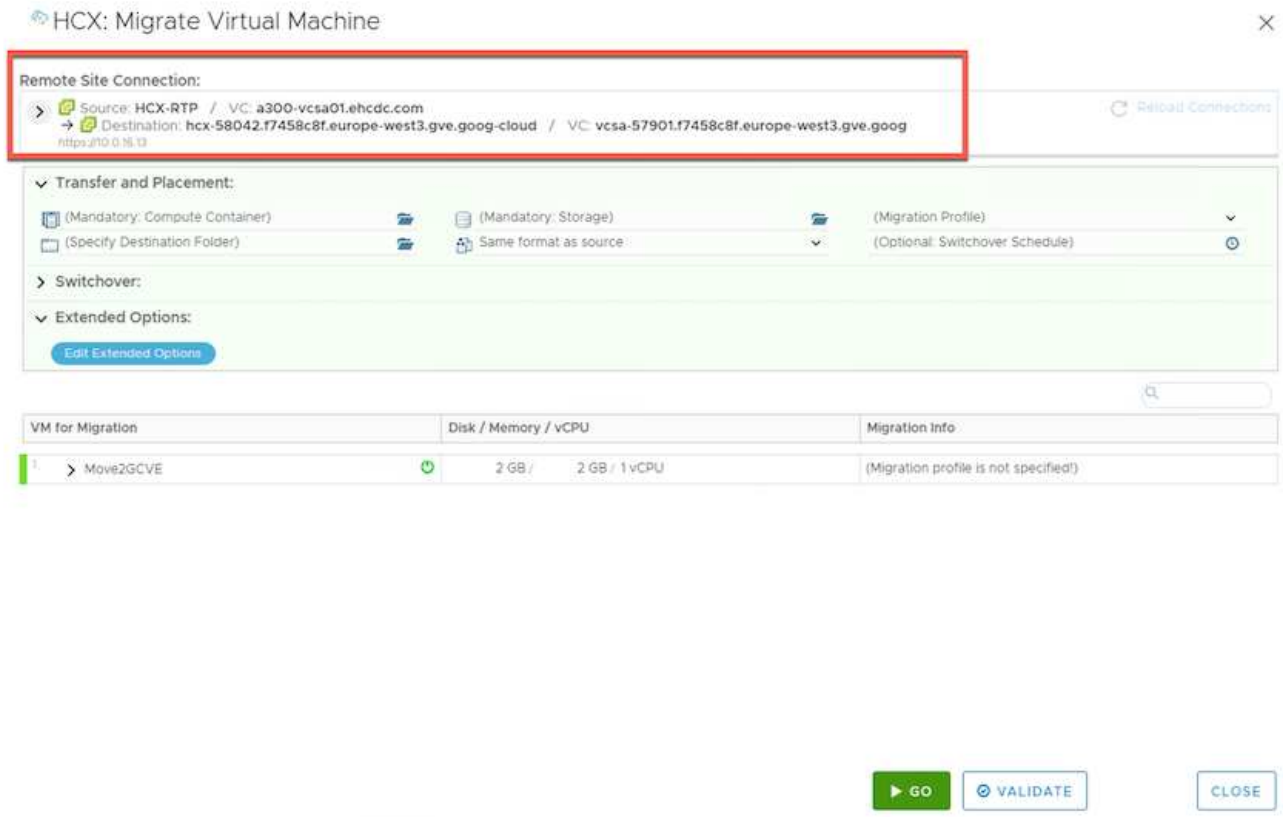
Esta seção descreve o mecanismo HCX vMotion. Esta tecnologia de migração usa o protocolo VMware vMotion para migrar uma VM para o GCVE. A opção de migração vMotion é usada para migrar o estado de uma única VM por vez. Não há interrupção de serviço durante este método de migração.

> ⓘ A extensão de rede deve estar em vigor (para o grupo de portas no qual a VM está conectada) para migrar a VM sem a necessidade de fazer uma alteração de endereço IP.

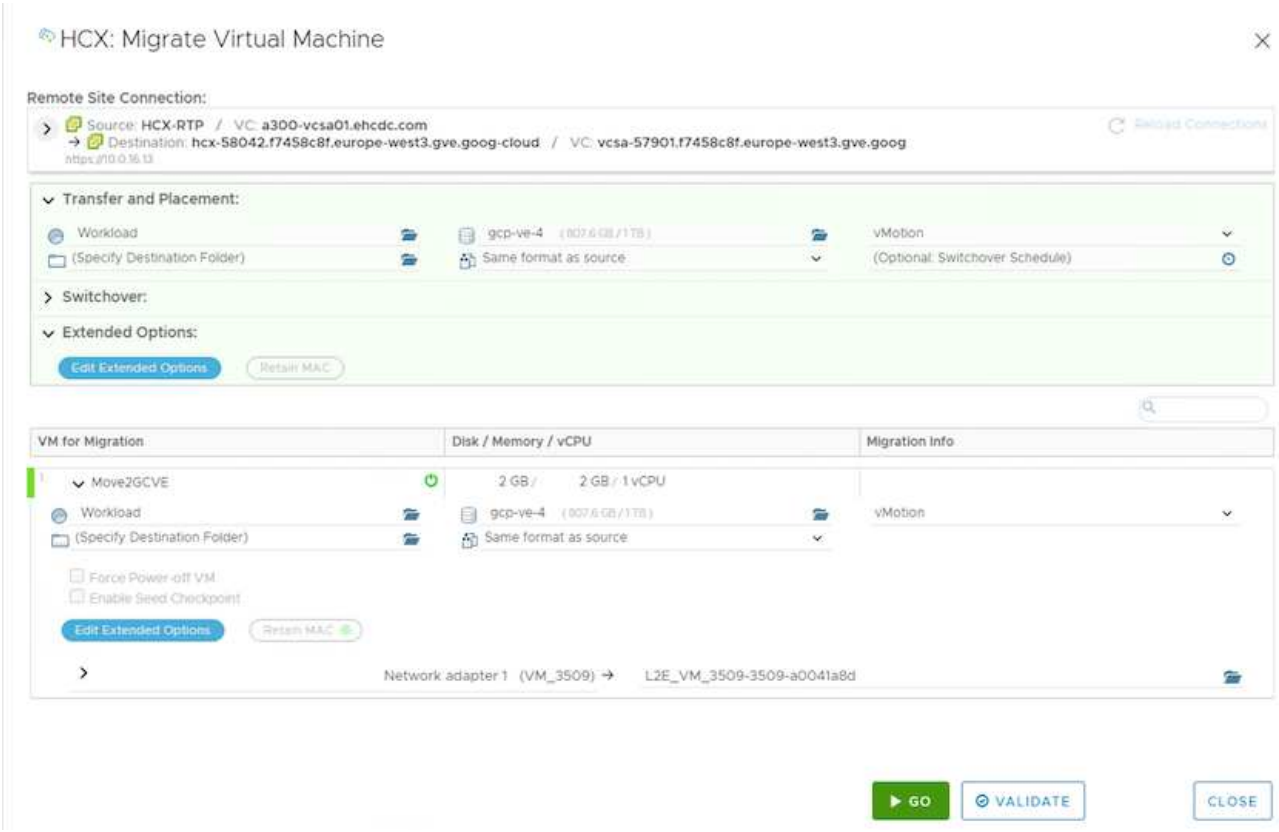
1. No cliente vSphere local, acesse Inventário, clique com o botão direito do mouse na VM a ser migrada e selecione Ações do HCX > Migrar para o site de destino do HCX.



2. No assistente Migrar Máquina Virtual, selecione Conexão de Site Remoto (GCVE de destino).



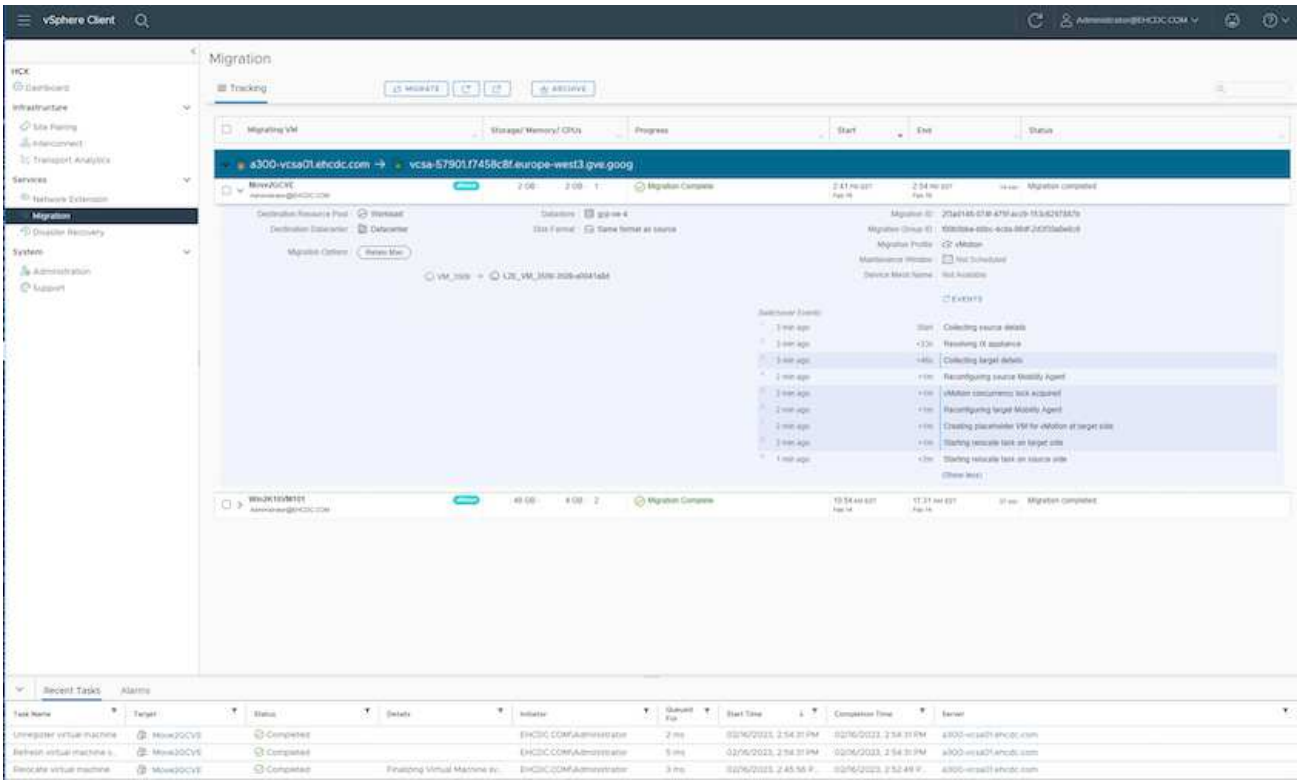
3. Atualize os campos obrigatórios (Cluster, Armazenamento e Rede de Destino), clique em Validar.



4. Após a conclusão das verificações de validação, clique em Ir para iniciar a migração.

> A transferência vMotion captura a memória ativa da VM, seu estado de execução, seu endereço IP e seu endereço MAC. Para obter mais informações sobre os requisitos e limitações do HCX vMotion, consulte "Compreendendo o VMware HCX vMotion e a migração a frio" .

5. Você pode monitorar o progresso e a conclusão do vMotion no painel HCX > Migração.



O armazenamento de dados NFS do Google Cloud NetApp Volumes (NetApp Volumes) de destino deve ter espaço suficiente para lidar com a migração.

Conclusão

Não importa se você está visando nuvem híbrida ou totalmente em nuvem e dados residindo em qualquer tipo/fornecedor de armazenamento no local, o Cloud Volume Service e o HCX oferecem excelentes opções para implantar e migrar as cargas de trabalho do aplicativo, ao mesmo tempo em que reduzem o TCO ao tornar os requisitos de dados integrados à camada do aplicativo. Seja qual for o caso de uso, escolha o Google Cloud VMware Engine junto com o Cloud Volume Service para rápida concretização dos benefícios da nuvem, infraestrutura consistente e operações em nuvens locais e múltiplas, portabilidade bidirecional de cargas de trabalho e capacidade e desempenho de nível empresarial. É o mesmo processo e procedimento familiar usado para conectar o armazenamento e migrar VMs usando VMware vSphere Replication, VMware vMotion ou até mesmo cópia de arquivo de rede (NFC).

Takeaways

Os pontos principais deste documento incluem:

- Agora você pode usar o Cloud Volume Service como um armazenamento de dados no Google Cloud VMware Engine SDDC.
- Você pode migrar facilmente dados do local para o armazenamento de dados do Cloud Volume Service.
- Você pode facilmente aumentar e diminuir o armazenamento de dados do Cloud Volume Service para atender aos requisitos de capacidade e desempenho durante a atividade de migração.

Vídeos do Google e VMware para referência

▼ **Do Google**

- "Implantar o conector HCX com GCVE"

- "Configurar o HCX ServiceMesh com GCVE"
- "Migrar VM com HCX para GCVE"

▼ **Da VMware**

- "Implantação do conector HCX para GCVE"
- "Configuração do HCX ServiceMesh para GCVE"
- "Migração de carga de trabalho do HCX para o GCVE"

Onde encontrar informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes links do site:

- Documentação do Google Cloud VMware Engine

  "https://cloud.google.com/vmware-engine/docs/overview"

- Documentação do Cloud Volume Service

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Guia do usuário do VMware HCX

  "https://docs.vmware.com/en/VMware-HCX/index.html"

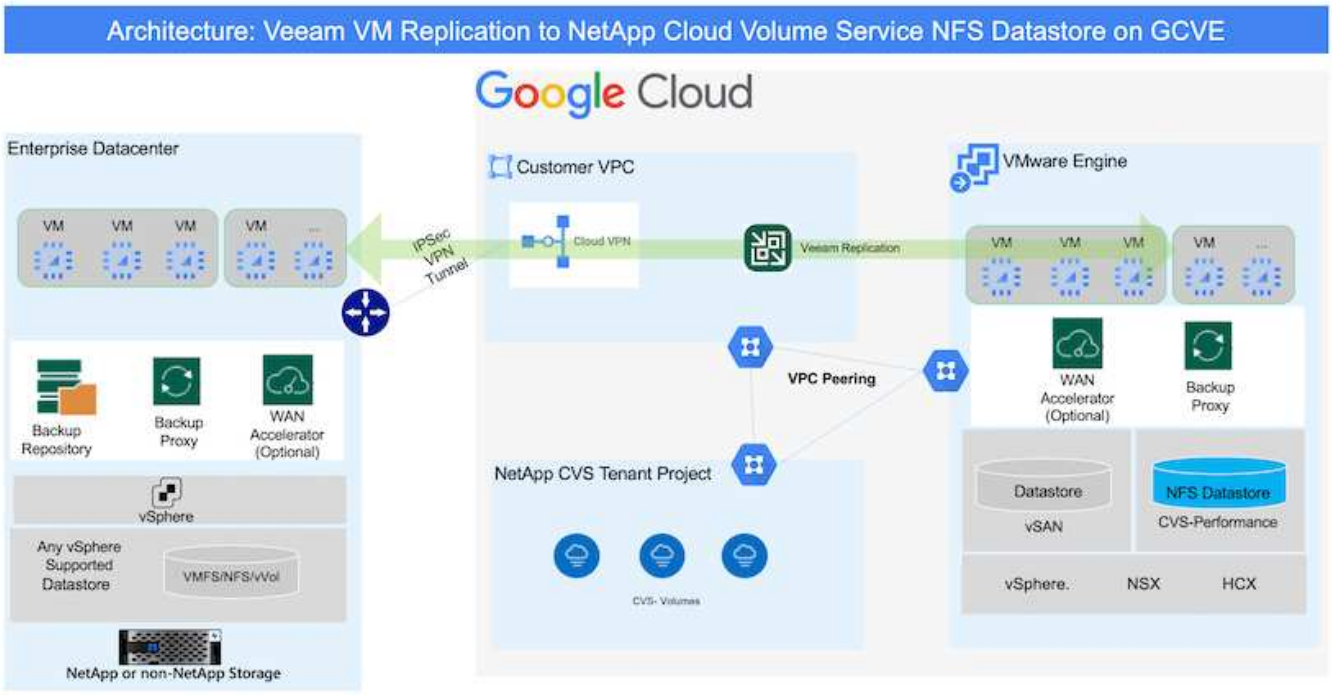
Migração de VM para o Google Cloud NetApp Volumes NFS Datastore no Google Cloud VMware Engine usando o recurso Veeam Replication

Os clientes que atualmente usam o Veeam para atender às suas necessidades de proteção de dados continuam usando essa solução para migrar as cargas de trabalho para o GCVE e aproveitar os benefícios dos armazenamentos de dados NFS do Google Cloud NetApp Volumes .

Visão geral

Cargas de trabalho de VM em execução no VMware vSphere podem ser migradas para o Google Cloud VMware Engine (GCVE) utilizando o recurso Veeam Replication.

Este documento fornece uma abordagem passo a passo para configurar e executar a migração de VM que usa o Google Cloud NetApp Volumes, o Veeam e o Google Cloud VMware Engine (GCVE).



Suposições

Este documento pressupõe que você tenha o Google Cloud VPN, o Cloud Interconnect ou outra opção de rede para estabelecer conectividade de rede dos servidores vSphere existentes com o Google Cloud VMware Engine.

> Há várias opções para conectar datacenters locais ao Google Cloud, o que nos impede de descrever um fluxo de trabalho específico neste documento. Consulte o"Documentação do Google Cloud" para o método de conectividade local apropriado com o Google.

Implementando a solução de migração

Visão geral da implantação da solução

1. Certifique-se de que o armazenamento de dados NFS do Google Cloud NetApp Volumes esteja montado no GCVE vCenter.
2. Garanta que o Veeam Backup Recovery esteja implantado no ambiente VMware vSphere existente
3. Crie um trabalho de replicação para iniciar a replicação de máquinas virtuais para a instância do Google Cloud VMware Engine.
4. Executar failover do trabalho de replicação do Veeam.
5. Execute failover permanente no Veeam.

Detalhes da implantação

Certifique-se de que o armazenamento de dados NFS do Google Cloud NetApp Volumes esteja montado no GCVE vCenter

Efetue login no GCVE vCenter e verifique se há um armazenamento de dados NFS com espaço suficiente disponível. Caso contrário, consulte"Montar volumes NetApp como armazenamento de dados NFS no GCVE"

Garanta que o Veeam Backup Recovery esteja implantado no ambiente VMware vSphere existente

Por favor consulte"Componentes de replicação Veeam" documentação para instalar os componentes necessários.

Crie um trabalho de replicação para iniciar a replicação de máquinas virtuais para a instância do Google Cloud VMware Engine.

Tanto o vCenter local quanto o vCenter GCVE precisam ser registrados no Veeam. "Configurar tarefa de replicação de VM do vSphere" Aqui está um vídeo explicando como"Configurar trabalho de replicação" .

> ⓘ A VM de réplica pode ter IP diferente da VM de origem e também pode ser conectada a um grupo de portas diferente. Para mais detalhes, assista ao vídeo acima.

Executar failover do trabalho de replicação do Veeam

Para migrar VMs, execute"Executar failover"

Execute failover permanente no Veeam.

Para tratar o GCVE como seu novo ambiente de origem, execute"Failover permanente"

Benefícios desta solução

- A infraestrutura de backup existente da Veeam pode ser utilizada para migração.
- O Veeam Replication permite alterar endereços IP de VM no site de destino.
- Possui a capacidade de remapear dados existentes replicados fora do Veeam (como dados replicados do sistema NetApp)
- Tem a capacidade de especificar diferentes grupos de portas de rede no site de destino.
- Pode especificar a ordem em que as VMs serão ligadas.
- Utiliza o VMware Change Block Tracking para minimizar a quantidade de dados a serem enviados pela WAN.
- Capacidade de executar pré e pós scripts para replicação.
- Capacidade de executar pré e pós scripts para snapshots.

Dados seguros com o Google Cloud NetApp Volumes no Google Cloud

TR-4918: Visão geral de segurança - Google Cloud NetApp Volumes no Google Cloud

Oliver Krause, Justin Parisi, NetApp

A segurança, especialmente na nuvem, onde a infraestrutura está fora do controle dos administradores de armazenamento, é fundamental para confiar seus dados às ofertas de serviços fornecidas pelos provedores de nuvem. Este documento apresenta uma visão geral das ofertas de segurança que "O Google Cloud NetApp Volumes fornece no Google Cloud".

Público-alvo

O público-alvo deste documento inclui, mas não está limitado às seguintes funções:

- Provedores de nuvem
- Administradores de armazenamento
- Arquitetos de armazenamento
- Recursos de campo
- Tomadores de decisões empresariais

Caso tenha dúvidas sobre o conteúdo deste relatório técnico, consulte a seção"Contate-nos."

Abreviação	Definição
Volumes NetApp -SW	Google Cloud NetApp Volumes, Tipo de serviço NetApp Volumes
Volumes NetApp -Desempenho	Serviço de Volume em Nuvem, Tipo de Serviço NetApp Volumes-Desempenho
PSA	

Como o Google Cloud NetApp Volumes no Google Cloud protege seus dados

O Google Cloud NetApp Volumes no Google Cloud oferece diversas maneiras de proteger seus dados nativamente.

Arquitetura segura e modelo de locação

O Google Cloud NetApp Volumes fornece uma arquitetura segura no Google Cloud segmentando o gerenciamento de serviços (plano de controle) e o acesso a dados (plano de dados) em diferentes pontos de extremidade para que nenhum possa impactar o outro (consulte a seção"Arquitetura do Google Cloud NetApp Volumes"). Ele usa o Google "acesso a serviços privados" (PSA) estrutura para fornecer o serviço. Esta estrutura distingue entre o produtor de serviço, que é fornecido e operado pela NetApp, e o consumidor de serviço, que é uma Nuvem Privada Virtual (VPC) em um projeto de cliente, hospedando os clientes que desejam acessar compartilhamentos de arquivos do Google Cloud NetApp Volumes .

Nesta arquitetura, os inquilinos (veja a seção"Modelo de locação") são definidos como projetos do Google Cloud que são completamente isolados uns dos outros, a menos que sejam explicitamente conectados pelo usuário. Os locatários permitem o isolamento completo de volumes de dados, serviços de nomes externos e outras partes essenciais da solução de outros locatários usando a plataforma de volume Google Cloud NetApp Volumes . Como a plataforma Google Cloud NetApp Volumes é conectada por meio de peering de VPC, esse isolamento também se aplica a ela. Você pode habilitar o compartilhamento de volumes do Google Cloud NetApp Volumes entre vários projetos usando uma VPC compartilhada (consulte a seção"VPCs compartilhadas"). Você pode aplicar controles de acesso a compartilhamentos SMB e exportações NFS para limitar quem ou o que pode visualizar ou modificar conjuntos de dados.

Gerenciamento de identidade forte para o plano de controle

No plano de controle onde a configuração do Google Cloud NetApp Volumes ocorre, o gerenciamento de identidade é gerenciado usando "Gerenciamento de acesso de identidade (IAM)" . O IAM é um serviço padrão que permite controlar a autenticação (logins) e a autorização (permissões) para instâncias de projetos do Google Cloud. Toda a configuração é realizada com as APIs do Google Cloud NetApp Volumes por meio de um transporte HTTPS seguro usando criptografia TLS 1.2, e a autenticação é realizada usando tokens JWT

para maior segurança. A interface do usuário do console do Google para o Google Cloud NetApp Volumes traduz a entrada do usuário em chamadas de API do Google Cloud NetApp Volumes .

Reforço da segurança - Limitando superfícies de ataque

Parte da segurança eficaz é limitar o número de superfícies de ataque disponíveis em um serviço. As superfícies de ataque podem incluir uma variedade de coisas, incluindo dados em repouso, transferências em andamento, logins e os próprios conjuntos de dados.

Um serviço gerenciado remove algumas das superfícies de ataque inerentes ao seu design. Gestão de infraestrutura, conforme descrito na seção"Operação de serviço," é gerenciado por uma equipe dedicada e é automatizado para reduzir o número de vezes que um humano realmente toca nas configurações, o que ajuda a reduzir o número de erros intencionais e não intencionais. A rede é isolada para que somente os serviços necessários possam acessar uns aos outros. A criptografia é incorporada ao armazenamento de dados e somente o plano de dados precisa de atenção de segurança dos administradores do Google Cloud NetApp Volumes . Ao ocultar a maior parte do gerenciamento por trás de uma interface de API, a segurança é alcançada limitando as superfícies de ataque.

Modelo Zero Trust

Historicamente, a filosofia de segurança de TI tem sido confiar, mas verificar, e se manifesta na dependência exclusiva de mecanismos externos (como firewalls e sistemas de detecção de intrusão) para mitigar ameaças. No entanto, ataques e violações evoluíram para contornar a verificação em ambientes por meio de phishing, engenharia social, ameaças internas e outros métodos que fornecem a verificação para entrar em redes e causar estragos.

Zero Trust se tornou uma nova metodologia em segurança, com o mantra atual sendo "não confiar em nada e ainda assim verificar tudo". Portanto, nada tem acesso permitido por padrão. Esse mantra é aplicado de várias maneiras, incluindo firewalls padrão e sistemas de detecção de intrusão (IDS), e também com os seguintes métodos:

- Métodos de autenticação fortes (como tokens Kerberos ou JWT criptografados em AES)
- Fontes únicas e fortes de identidades (como Windows Active Directory, Lightweight Directory Access Protocol (LDAP) e Google IAM)
- Segmentação de rede e multilocação segura (somente locatários têm acesso permitido por padrão)
- Controles de acesso granulares com políticas de acesso menos privilegiado
- Pequenas listas exclusivas de administradores dedicados e confiáveis com auditoria digital e registros em papel

O Google Cloud NetApp Volumes em execução no Google Cloud adere ao modelo Zero Trust ao implementar a postura "não confie em nada, verifique tudo".

Criptografia

Criptografar dados em repouso (consulte a seção"Criptografia de dados em repouso") usando cifras XTS-AES-256 com NetApp Volume Encryption (NVE) e em voo com"Criptografia SMB" ou suporte NFS Kerberos 5p. Fique tranquilo sabendo que as transferências de replicação entre regiões são protegidas pela criptografia TLS 1.2 (consulte o link da seção:gcp-gcnv-security-considerations.html#Detecção, prevenção e mitigação de ransomware, malware e vírus#cross-region-replication["Replicação entre regiões"]). Além disso, a rede do Google também fornece comunicações criptografadas (consulte a seção"Criptografia de dados em trânsito") para uma camada adicional de proteção contra ataques. Para obter mais informações sobre criptografia de transporte, consulte a seção"Rede Google Cloud" .

Proteção de dados e backups

Segurança não se trata apenas de prevenção de ataques. Também se trata de como nos recuperamos de ataques, se ou quando eles ocorrem. Esta estratégia inclui proteção de dados e backups. O Google Cloud NetApp Volumes fornece métodos para replicar para outras regiões em caso de interrupções (consulte a seção"Replicação entre regiões") ou se um conjunto de dados for afetado por um ataque de ransomware. Ele também pode executar backups assíncronos de dados em locais fora da instância do Google Cloud NetApp Volumes usando"Backup de Google Cloud NetApp Volumes" . Com backups regulares, a mitigação de eventos de segurança pode levar menos tempo e economizar dinheiro e angústia para os administradores.

Mitigação rápida de ransomware com cópias Snapshot líderes do setor

Além da proteção de dados e backups, o Google Cloud NetApp Volumes oferece suporte para cópias imutáveis do Snapshot (consulte a seção"Cópias de Snapshot imutáveis") de volumes que permitem a recuperação de ataques de ransomware (consulte a seção"Operação de serviço") em segundos após a descoberta do problema e com interrupção mínima. O tempo de recuperação e os efeitos dependem do cronograma do Snapshot, mas você pode criar cópias do Snapshot que fornecem deltas de apenas uma hora em ataques de ransomware. Cópias de instantâneos têm um efeito insignificante no desempenho e no uso da capacidade e são uma abordagem de baixo risco e alta recompensa para proteger seus conjuntos de dados.

Considerações de segurança e superfícies de ataque

O primeiro passo para entender como proteger seus dados é identificar os riscos e as potenciais superfícies de ataque.

Isso inclui (mas não está limitado a) o seguinte:

- Administração e logins
- Dados em repouso
- Dados em voo
- Rede e firewalls
- Ransomware, malware e vírus

Entender as superfícies de ataque pode ajudar você a proteger melhor seus ambientes. O Google Cloud NetApp Volumes no Google Cloud já considera muitos desses tópicos e implementa a funcionalidade de segurança por padrão, sem qualquer interação administrativa.

Garantindo logins seguros

Ao proteger seus componentes críticos de infraestrutura, é fundamental garantir que somente usuários aprovados possam efetuar login e gerenciar seus ambientes. Se pessoas mal-intencionadas violarem suas credenciais administrativas, elas terão as chaves do castelo e poderão fazer o que quiserem: alterar configurações, excluir volumes e backups, criar backdoors ou desabilitar agendamentos de Snapshots.

O Google Cloud NetApp Volumes para Google Cloud oferece proteção contra logins administrativos não autorizados por meio da ofuscação do armazenamento como serviço (StaaS). O Google Cloud NetApp Volumes é totalmente mantido pelo provedor de nuvem, sem disponibilidade para login externo. Todas as operações de instalação e configuração são totalmente automatizadas, de modo que um administrador humano nunca precisa interagir com os sistemas, exceto em circunstâncias muito raras.

Se for necessário login, o Google Cloud NetApp Volumes no Google Cloud protege os logins mantendo uma lista muito curta de administradores confiáveis que têm acesso para fazer login nos sistemas. Essa proteção ajuda a reduzir o número de possíveis criminosos com acesso. Além disso, a rede do Google Cloud oculta os

sistemas atrás de camadas de segurança de rede e expõe apenas o que é necessário para o mundo externo. Para obter informações sobre a arquitetura do Google Cloud, Google Cloud NetApp Volumes , consulte a seção"Arquitetura do Google Cloud NetApp Volumes ."

Administração e atualizações de cluster

Duas áreas com potenciais riscos de segurança incluem administração de cluster (o que acontece se um invasor tiver acesso de administrador) e atualizações (o que acontece se uma imagem de software for comprometida).

Proteção de administração de armazenamento

O armazenamento fornecido como serviço elimina o risco adicional de exposição dos administradores, removendo esse acesso aos usuários finais fora do data center na nuvem. Em vez disso, a única configuração feita é para o plano de acesso a dados pelos clientes. Cada locatário gerencia seus próprios volumes, e nenhum locatário pode acessar outras instâncias do Google Cloud NetApp Volumes . O serviço é gerenciado por automação, com uma lista muito pequena de administradores confiáveis que têm acesso aos sistemas por meio dos processos abordados na seção"Operação de serviço."

O tipo de serviço NetApp Volumes-Performance oferece replicação entre regiões como uma opção para fornecer proteção de dados a uma região diferente no caso de uma falha regional. Nesses casos, o Google Cloud NetApp Volumes pode ser transferido para a região não afetada para manter o acesso aos dados.

Atualizações de serviço

As atualizações ajudam a proteger sistemas vulneráveis. Cada atualização fornece melhorias de segurança e correções de bugs que minimizam as superfícies de ataque. As atualizações de software são baixadas de repositórios centralizados e validadas antes que as atualizações sejam permitidas, para verificar se as imagens oficiais são usadas e se as atualizações não são comprometidas por agentes mal-intencionados.

Com o Google Cloud NetApp Volumes, as atualizações são gerenciadas pelas equipes do provedor de nuvem, o que elimina a exposição a riscos para as equipes de administradores ao fornecer especialistas bem versados em configuração e atualizações que automatizaram e testaram completamente o processo. As atualizações não causam interrupções, e o Google Cloud NetApp Volumes mantém as atualizações mais recentes para melhores resultados gerais.

Para obter informações sobre a equipe de administradores que executa essas atualizações de serviço, consulte a seção"Operação de serviço."

Protegendo dados em repouso

A criptografia de dados em repouso é importante para proteger dados confidenciais no caso de um disco ser roubado, devolvido ou reutilizado. Os dados no Google Cloud NetApp Volumes são protegidos em repouso usando criptografia baseada em software.

- As chaves geradas pelo Google são usadas para o NetApp Volumes-SW.
- Para o NetApp Volumes-Performance, as chaves por volume são armazenadas em um gerenciador de chaves integrado ao Google Cloud NetApp Volumes, que usa o NetApp ONTAP CryptoMod para gerar chaves de criptografia AES-256. O CryptoMod está listado na lista de módulos validados pelo CMVP FIPS 140-2. Ver "Certificado FIPS 140-2 nº 4144" .

A partir de novembro de 2021, a funcionalidade de visualização de Criptografia gerenciada pelo cliente (CMEK) foi disponibilizada para o NetApp Volumes-Performance. Essa funcionalidade permite criptografar as chaves por volume com chaves mestras por projeto e por região hospedadas no Google Key Management

Service (KMS). O KMS permite que você anexe gerenciadores de chaves externos.

Para obter detalhes sobre como configurar o KMS para NetApp Volumes-Performance, "consulte a documentação do Google Cloud NetApp Volumes".

Para mais informações sobre arquitetura, consulte a seção"Arquitetura do Google Cloud NetApp Volumes ."

Protegendo dados durante o voo

Além de proteger dados em repouso, você também deve ser capaz de proteger dados quando eles estiverem em trânsito entre a instância do Google Cloud NetApp Volumes e um cliente ou destino de replicação. O Google Cloud NetApp Volumes fornece criptografia para dados em trânsito por meio de protocolos NAS usando métodos de criptografia como criptografia SMB usando Kerberos, assinatura/selagem de pacotes e NFS Kerberos 5p para criptografia de ponta a ponta de transferências de dados.

A replicação de volumes do Google Cloud NetApp Volumes usa TLS 1.2, que aproveita os métodos de criptografia AES-GCM.

A maioria dos protocolos inseguros de bordo, como telnet, NDMP e outros, são desabilitados por padrão. No entanto, o DNS não é criptografado pelo Google Cloud NetApp Volumes (sem suporte a DNS Sec) e deve ser criptografado usando criptografia de rede externa quando possível. Veja a seção"Criptografia de dados em trânsito" para obter mais informações sobre como proteger dados durante o voo.

Para obter informações sobre a criptografia do protocolo NAS, consulte a seção"Protocolos NAS."

Usuários e grupos para permissões NAS

Parte da proteção dos seus dados na nuvem envolve a autenticação adequada de usuários e grupos, onde os usuários que acessam os dados são verificados como usuários reais no ambiente e os grupos contêm usuários válidos. Esses usuários e grupos fornecem acesso inicial de compartilhamento e exportação, bem como validação de permissão para arquivos e pastas no sistema de armazenamento.

O Google Cloud NetApp Volumes usa autenticação padrão de usuários e grupos do Windows baseada no Active Directory para compartilhamentos SMB e permissões no estilo do Windows. O serviço também pode aproveitar provedores de identidade UNIX, como LDAP para usuários e grupos UNIX para exportações NFS, validação de ID NFSv4, autenticação Kerberos e ACLs NFSv4.

> Atualmente, apenas o Active Directory LDAP é compatível com o Google Cloud NetApp Volumes para funcionalidade LDAP.

Detecção, prevenção e mitigação de ransomware, malware e vírus

Ransomware, malware e vírus são uma ameaça persistente aos administradores, e a detecção, a prevenção e a mitigação dessas ameaças são sempre prioridades para organizações empresariais. Um único evento de ransomware em um conjunto de dados crítico pode custar milhões de dólares, então é benéfico fazer o que puder para minimizar o risco.

Embora o Google Cloud NetApp Volumes atualmente não inclua medidas nativas de detecção ou prevenção, como proteção antivírus ou "detecção automática de ransomware", há maneiras de se recuperar rapidamente de um evento de ransomware ativando programações regulares de Snapshot. As cópias de Snapshot são imutáveis e contêm ponteiros somente leitura para blocos alterados no sistema de arquivos, são quase instantâneas, têm impacto mínimo no desempenho e só ocupam espaço quando os dados são alterados ou excluídos. Você pode definir programações para cópias de Snapshot de acordo com seu objetivo aceitável de ponto de recuperação (RPO)/objetivo de tempo de recuperação (RTO) e pode manter até 1.024 cópias de Snapshot por volume.

O suporte a Snapshot está incluído sem custo adicional (além das taxas de armazenamento de dados para blocos alterados/dados retidos por cópias de Snapshot) com o Google Cloud NetApp Volumes e, no caso de um ataque de ransomware, pode ser usado para reverter para uma cópia de Snapshot antes do ataque ocorrer. As restaurações de instantâneos levam apenas alguns segundos para serem concluídas e você pode então voltar a servir dados normalmente. Para obter mais informações, consulte "A solução da NetApp para ransomware" .

Impedir que o ransomware afete seu negócio requer uma abordagem em várias camadas que inclui um ou mais dos seguintes:

- Proteção de endpoint
- Proteção contra ameaças externas por meio de firewalls de rede
- Detecção de anomalias de dados
- Vários backups (no local e fora do local) de conjuntos de dados críticos
- Testes regulares de restauração de backups
- Cópias imutáveis somente leitura do NetApp Snapshot
- Autenticação multifatorial para infraestrutura crítica
- Auditorias de segurança de logins de sistema

Esta lista está longe de ser exaustiva, mas é um bom modelo a seguir ao lidar com o potencial de ataques de ransomware. O Google Cloud NetApp Volumes no Google Cloud oferece diversas maneiras de proteção contra eventos de ransomware e reduzir seus efeitos.

Cópias de Snapshot imutáveis

O Google Cloud NetApp Volumes fornece nativamente cópias de instantâneos somente leitura e imutáveis que são feitas em um cronograma personalizável para recuperação rápida em um ponto específico no tempo em caso de exclusão de dados ou se um volume inteiro tiver sido vítima de um ataque de ransomware. As restaurações de instantâneos para cópias anteriores boas do Snapshot são rápidas e minimizam a perda de dados com base no período de retenção de suas programações de Snapshot e RTO/RPO. O efeito no desempenho com a tecnologia Snapshot é insignificante.

Como as cópias de instantâneo no Google Cloud NetApp Volumes são somente leitura, elas não podem ser infectadas por ransomware, a menos que o ransomware tenha proliferado no conjunto de dados sem ser notado e cópias de instantâneo tenham sido feitas dos dados infectados pelo ransomware. É por isso que você também deve considerar a detecção de ransomware com base em anomalias de dados. Atualmente, o Google Cloud NetApp Volumes não fornece detecção nativamente, mas você pode usar um software de monitoramento externo.

Backups e restaurações

O Google Cloud NetApp Volumes fornece recursos padrão de backup de cliente NAS (como backups por NFS ou SMB).

- O NetApp Volumes-Performance oferece replicação de volumes entre regiões para outros volumes do NetApp Volumes-Performance. Para obter mais informações, consulte "replicação de volume" na documentação do Google Cloud NetApp Volumes.
- O NetApp Volumes-SW oferece recursos nativos do serviço para backup e restauração de volumes. Para obter mais informações, consulte "backup em nuvem" a documentação do Google Cloud NetApp Volumes.

A replicação de volume fornece uma cópia exata do volume de origem para failover rápido em caso de

desastre, incluindo eventos de ransomware.

Replicação entre regiões

O NetApp Volumes-Performance permite que você replique volumes com segurança em regiões do Google Cloud para proteção de dados e casos de uso de arquivamento usando criptografia TLS1.2 AES 256 GCM em uma rede de serviço de back-end controlada pela NetApp usando interfaces específicas usadas para replicação em execução na rede do Google. Um volume primário (origem) contém os dados de produção ativos e é replicado para um volume secundário (destino) para fornecer uma réplica exata do conjunto de dados primário.

A replicação inicial transfere todos os blocos, mas as atualizações transmitem apenas os blocos alterados em um volume primário. Por exemplo, se um banco de dados de 1 TB que reside em um volume primário for replicado para o volume secundário, 1 TB de espaço será transferido na replicação inicial. Se esse banco de dados tiver algumas centenas de linhas (hipoteticamente, alguns MB) que mudam entre a inicialização e a próxima atualização, somente os blocos com as linhas alteradas são replicados para o secundário (alguns MB). Isso ajuda a garantir que os tempos de transferência permaneçam baixos e reduz os custos de replicação.

Todas as permissões em arquivos e pastas são replicadas para o volume secundário, mas as permissões de acesso compartilhado (como políticas e regras de exportação ou compartilhamentos SMB e ACLs de compartilhamento) devem ser tratadas separadamente. No caso de failover de um site, o site de destino deve aproveitar os mesmos serviços de nomes e conexões de domínio do Active Directory para fornecer tratamento consistente de identidades e permissões de usuários e grupos. Você pode usar um volume secundário como um destino de failover no caso de um desastre, interrompendo o relacionamento de replicação, o que converte o volume secundário para leitura e gravação.

As réplicas de volume são somente leitura, o que fornece uma cópia imutável dos dados fora do local para recuperação rápida de dados em casos em que um vírus infectou os dados ou um ransomware criptografou o conjunto de dados primário. Dados somente leitura não serão criptografados, mas, se o volume primário for afetado e a replicação ocorrer, os blocos infectados também serão replicados. Você pode usar cópias mais antigas e não afetadas do Snapshot para recuperar, mas os SLAs podem ficar fora do alcance do RTO/RPO prometido, dependendo da rapidez com que um ataque é detectado.

Além disso, você pode impedir ações administrativas maliciosas, como exclusões de volumes, exclusões de Snapshot ou alterações no agendamento do Snapshot, com o gerenciamento da replicação entre regiões (CRR) no Google Cloud. Isso é feito criando funções personalizadas que separam os administradores de volume, que podem excluir volumes de origem, mas não podem interromper espelhamentos e, portanto, não podem excluir volumes de destino, dos administradores de CRR, que não podem executar nenhuma operação de volume. Consulte "Considerações de segurança" na documentação do Google Cloud NetApp Volumes as permissões permitidas para cada grupo de administradores.

Backup de Google Cloud NetApp Volumes

Embora o Google Cloud NetApp Volumes ofereça alta durabilidade de dados, eventos externos podem causar perda de dados. No caso de um evento de segurança, como um vírus ou ransomware, backups e restaurações se tornam essenciais para retomar o acesso aos dados em tempo hábil. Um administrador pode excluir acidentalmente um volume do Google Cloud NetApp Volumes . Ou os usuários simplesmente querem manter versões de backup de seus dados por muitos meses e manter o espaço extra de cópia do Snapshot dentro do volume se torna um desafio de custo. Embora as cópias de instantâneo devam ser a maneira preferida de manter versões de backup das últimas semanas para restaurar dados perdidos, elas ficam dentro do volume e serão perdidas se o volume for desativado.

Por todos esses motivos, o Google Cloud NetApp Volumes oferece serviços de backup por meio de "Backup de Google Cloud NetApp Volumes".

O backup do Google Cloud NetApp Volumes gera uma cópia do volume no Google Cloud Storage (GCS). Ele só faz backup dos dados armazenados no volume, não do espaço livre. Ele funciona como incremental para sempre, o que significa que transfere o conteúdo do volume uma vez e, a partir daí, continua fazendo backup apenas dos dados alterados. Comparado aos conceitos clássicos de backup com vários backups completos, ele economiza grandes quantidades de armazenamento de backup, reduzindo custos. Como o preço mensal do espaço de backup é menor quando comparado a um volume, é um local ideal para manter versões de backup por mais tempo.

Os usuários podem usar um backup do Google Cloud NetApp Volumes para restaurar qualquer versão de backup para o mesmo volume ou para um volume diferente dentro da mesma região. Se o volume de origem for excluído, os dados de backup serão retidos e precisarão ser gerenciados (por exemplo, excluídos) de forma independente.

O backup do Google Cloud NetApp Volumes é incorporado ao Google Cloud NetApp Volumes como opção. Os usuários podem decidir quais volumes proteger ativando o backup do Google Cloud NetApp Volumes por volume. Consulte a "Documentação de backup do Google Cloud NetApp Volumes" para obter informações sobre backups, o "número máximo de versões de backup suportadas", o agendamento e a "preços".

Todos os dados de backup de um projeto são armazenados em um bucket do GCS, que é gerenciado pelo serviço e não é visível ao usuário. Cada projeto usa um bucket diferente. Atualmente, os buckets estão na mesma região que os volumes do Google Cloud NetApp Volumes , mas mais opções estão sendo discutidas. Consulte a documentação para saber o status mais recente.

O transporte de dados de um bucket do Google Cloud NetApp Volumes para o GCS usa redes internas do serviço do Google com HTTPS e TLS1.2. Os dados são criptografados em repouso com chaves gerenciadas pelo Google.

Para gerenciar o backup do Google Cloud NetApp Volumes (criar, excluir e restaurar backups), o usuário deve ter a "roles/netapp.admin" função.

Visão geral

Parte de confiar em uma solução de nuvem é entender a arquitetura e como ela é protegida. Esta seção destaca diferentes aspectos da arquitetura do Google Cloud NetApp Volumes no Google para ajudar a aliviar possíveis preocupações sobre como os dados são protegidos, bem como destacar áreas onde etapas de configuração adicionais podem ser necessárias para obter a implantação mais segura.

A arquitetura geral do Google Cloud NetApp Volumes pode ser dividida em dois componentes principais: o plano de controle e o plano de dados.

Plano de controle

O plano de controle no Google Cloud NetApp Volumes é a infraestrutura de back-end gerenciada pelos administradores do Google Cloud NetApp Volumes e pelo software de automação nativo da NetApp . Este plano é completamente transparente para os usuários finais e inclui rede, hardware de armazenamento, atualizações de software e assim por diante para ajudar a agregar valor a uma solução residente na nuvem, como o Google Cloud NetApp Volumes.

Plano de dados

O plano de dados no Google Cloud NetApp Volumes inclui os volumes de dados reais e a configuração geral do Google Cloud NetApp Volumes (como controle de acesso, autenticação Kerberos e assim por diante). O plano de dados está inteiramente sob o controle dos usuários finais e consumidores da plataforma Google

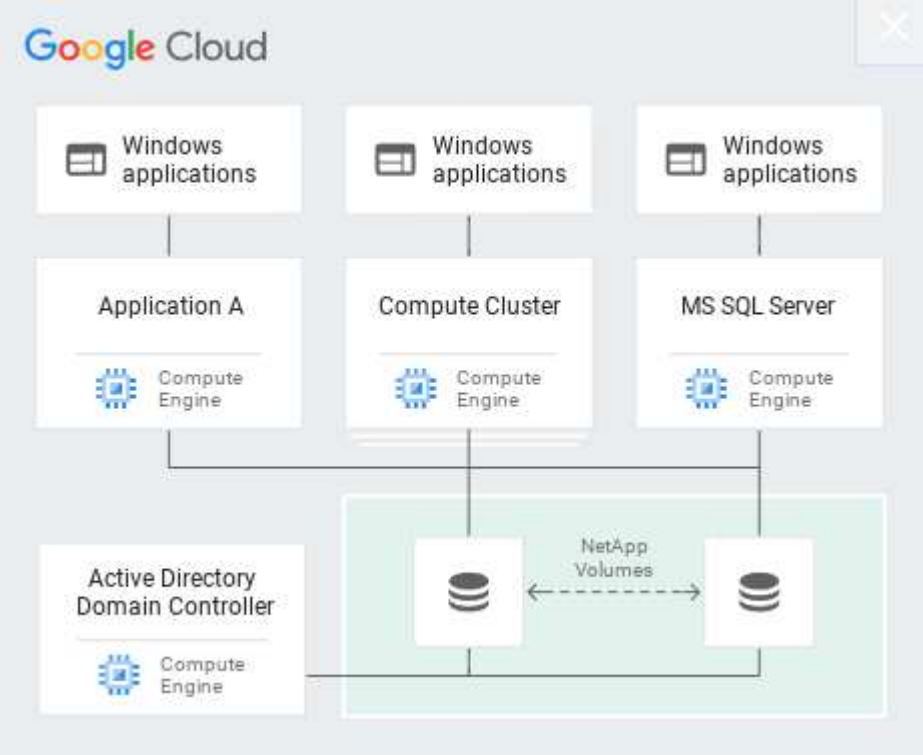
Cloud NetApp Volumes .

Há diferenças distintas em como cada avião é protegido e gerenciado. As seções a seguir abordam essas diferenças, começando com uma visão geral da arquitetura do Google Cloud NetApp Volumes .

Arquitetura do Google Cloud NetApp Volumes

De maneira semelhante a outros serviços nativos do Google Cloud, como CloudSQL, Google Cloud VMware Engine (GCVE) e FileStore, o Google Cloud NetApp Volumes usa "Google PSA" para prestar o serviço. No PSA, os serviços são construídos dentro de um projeto de produtor de serviços, que usa "Peering de rede VPC" para se conectar ao consumidor do serviço. O produtor do serviço é fornecido e operado pela NetApp, e o consumidor do serviço é uma VPC em um projeto do cliente, hospedando os clientes que desejam acessar os compartilhamentos de arquivos do Google Cloud NetApp Volumes .

A figura a seguir, referenciada a partir da "Documentação do Google Cloud NetApp Volumes", apresenta uma visão geral de alto nível.



A parte acima da linha pontilhada mostra o plano de controle do serviço, que controla o ciclo de vida do volume. A parte abaixo da linha pontilhada mostra o plano de dados. A caixa azul à esquerda representa o VPC do usuário (consumidor de serviço), a caixa azul à direita representa o produtor de serviço fornecido pela NetApp. Ambos estão conectados por meio de peering de VPC.

Modelo de locação

No Google Cloud NetApp Volumes, projetos individuais são considerados locatários exclusivos. Isso significa que a manipulação de volumes, cópias de Snapshot e assim por diante são realizadas por projeto. Em outras palavras, todos os volumes são de propriedade do projeto no qual foram criados e somente esse projeto pode gerenciar e acessar os dados dentro deles por padrão. Esta é considerada a visão do plano de controle do serviço.

VPCs compartilhadas

Na exibição do plano de dados, o Google Cloud NetApp Volumes pode se conectar a uma VPC compartilhada. Você pode criar volumes no projeto de hospedagem ou em um dos projetos de serviço conectados à VPC compartilhada. Todos os projetos (host ou serviço) conectados a essa VPC compartilhada podem acessar os volumes na camada de rede (TCP/IP). Como todos os clientes com conectividade de rede na VPC compartilhada podem potencialmente acessar os dados por meio de protocolos NAS, o controle de acesso no volume individual (como listas de controle de acesso (ACLs) de usuário/grupo e nomes de host/endereços IP para exportações NFS) deve ser usado para controlar quem pode acessar os dados.

Você pode conectar o Google Cloud NetApp Volumes a até cinco VPCs por projeto de cliente. No plano de controle, o projeto permite que você gerencie todos os volumes criados, independentemente da VPC à qual eles estejam conectados. No plano de dados, as VPCs são isoladas umas das outras e cada volume só pode ser conectado a uma VPC.

O acesso aos volumes individuais é controlado por mecanismos de controle de acesso específicos do protocolo (NFS/SMB).

Em outras palavras, na camada de rede, todos os projetos conectados à VPC compartilhada conseguem ver o volume, enquanto, no lado de gerenciamento, o plano de controle permite que apenas o projeto proprietário veja o volume.

Controles de serviço VPC

Os VPC Service Controls estabelecem um perímetro de controle de acesso em torno dos serviços do Google Cloud que estão conectados à Internet e são acessíveis em todo o mundo. Esses serviços fornecem controle de acesso por meio de identidades de usuários, mas não podem restringir a origem das solicitações de localização de rede. Os VPC Service Controls preenchem essa lacuna introduzindo recursos para restringir o acesso a redes definidas.

O plano de dados do Google Cloud NetApp Volumes não está conectado à Internet externa, mas a VPCs privadas com limites de rede bem definidos (perímetros). Dentro dessa rede, cada volume usa controle de acesso específico do protocolo. Qualquer conectividade de rede externa é criada explicitamente pelos administradores de projetos do Google Cloud. O plano de controle, no entanto, não fornece as mesmas proteções que o plano de dados e pode ser acessado por qualquer pessoa de qualquer lugar com credenciais válidas ("Tokens JWT").

Resumindo, o plano de dados do Google Cloud NetApp Volumes fornece o recurso de controle de acesso à rede, sem a necessidade de oferecer suporte a VPC Service Controls e não usa explicitamente VPC Service Controls.

Considerações sobre rastreamento/farejamento de pacotes

As capturas de pacotes podem ser úteis para solucionar problemas de rede ou outros problemas (como permissões de NAS, conectividade LDAP e assim por diante), mas também podem ser usadas maliciosamente para obter informações sobre endereços IP de rede, endereços MAC, nomes de usuários e grupos e qual nível de segurança está sendo usado nos endpoints. Devido à forma como a rede do Google Cloud, VPCs e regras de firewall são configuradas, o acesso indesejado aos pacotes de rede deve ser difícil de obter sem credenciais de login do usuário ou"Tokens JWT" nas instâncias da nuvem. As capturas de pacotes só são possíveis em endpoints (como máquinas virtuais (VMs)) e somente em endpoints internos à VPC, a menos que uma VPC compartilhada e/ou um túnel de rede externo/encaminhamento de IP estejam em uso para permitir explicitamente o tráfego externo para endpoints. Não há como farejar o tráfego fora dos clientes.

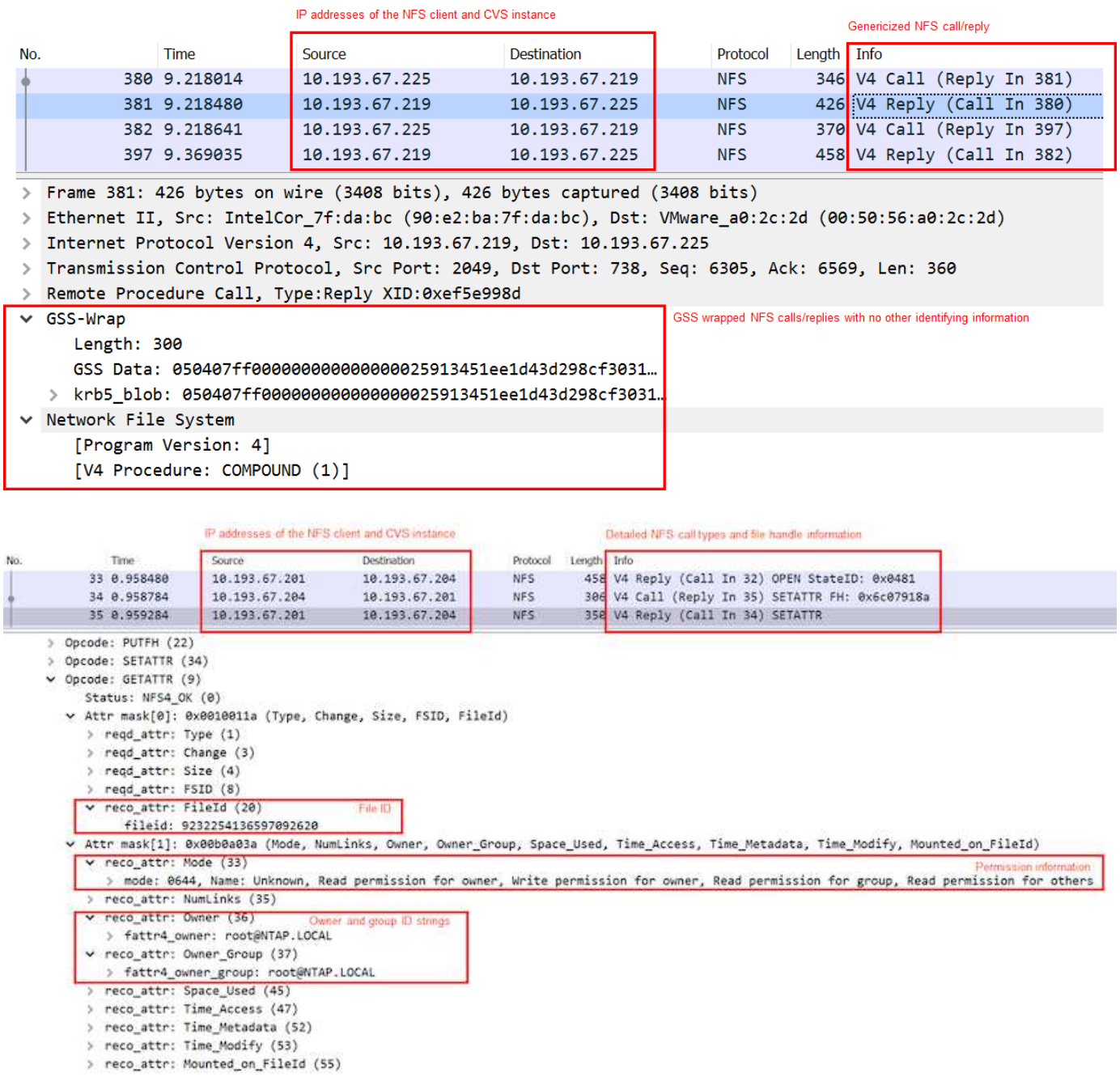
Quando VPCs compartilhados são usados, a criptografia em voo com NFS Kerberos e/ou"Criptografia SMB"

pode mascarar muitas das informações coletadas dos rastros. No entanto, algum tráfego ainda é enviado em texto simples, como"DNS" e"Consultas LDAP" . A figura a seguir mostra uma captura de pacote de uma consulta LDAP de texto simples originada do Google Cloud NetApp Volumes e as possíveis informações de identificação que são expostas. As consultas LDAP no Google Cloud NetApp Volumes atualmente não oferecem suporte a criptografia ou LDAP sobre SSL. O NetApp Volumes-Performance oferece suporte à assinatura LDAP, se solicitado pelo Active Directory. O NetApp Volumes-SW não oferece suporte à assinatura LDAP.



> unixUserPassword é consultado pelo LDAP e não é enviado em texto simples, mas sim em um hash salgado. Por padrão, o Windows LDAP não preenche os campos unixUserPassword. Este campo só é necessário se você precisar aproveitar o Windows LDAP para logins interativos por meio do LDAP para clientes. O Google Cloud NetApp Volumes não oferece suporte a logins LDAP interativos nas instâncias.

A figura a seguir mostra uma captura de pacote de uma conversa NFS Kerberos ao lado de uma captura de NFS sobre AUTH_SYS. Observe como as informações disponíveis em um rastreamento diferem entre os dois e como habilitar a criptografia em andamento oferece maior segurança geral para o tráfego NAS.



Interfaces de rede de VM

Um truque que os invasores podem tentar é adicionar uma nova placa de interface de rede (NIC) a uma VM em "modo promíscuo" (espelhamento de porta) ou habilitar o modo promíscuo em uma NIC existente para detectar todo o tráfego. No Google Cloud, adicionar uma nova NIC exige que uma VM seja desligada completamente, o que cria alertas para que os invasores não possam fazer isso despercebidos.

Além disso, as NICs não podem ser definidas para o modo promíscuo e dispararão alertas no Google Cloud.

Arquitetura do plano de controle

Todas as ações de gerenciamento do Google Cloud NetApp Volumes são feitas por meio da API. O gerenciamento do Google Cloud NetApp Volumes integrado ao GCP Cloud Console também usa a API do Google Cloud NetApp Volumes .

Gerenciamento de Identidade e Acesso

Gerenciamento de Identidade e Acesso("EU SOU") é um serviço padrão que permite controlar a autenticação (logins) e a autorização (permissões) para instâncias de projetos do Google Cloud. O Google IAM fornece uma trilha de auditoria completa de autorização e remoção de permissões. Atualmente, o Google Cloud NetApp Volumes não fornece auditoria de plano de controle.

Visão geral de autorização/permissão

O IAM oferece permissões granulares incorporadas para o Google Cloud NetApp Volumes. Você pode encontrar um "lista completa de permissões granulares aqui".

O IAM também oferece duas funções predefinidas chamadas `netappcloudvolumes.admin` e `netappcloudvolumes.viewer` . Essas funções podem ser atribuídas a usuários ou contas de serviço específicos.

Atribua funções e permissões apropriadas para permitir que usuários do IAM gerenciem o Google Cloud NetApp Volumes.

Exemplos de uso de permissões granulares incluem o seguinte:

- Crie uma função personalizada com apenas permissões obter/listar/criar/atualizar para que os usuários não possam excluir volumes.
- Use uma função personalizada com apenas `snapshot.*` permissões para criar uma conta de serviço que é usada para criar integração de Snapshot consistente com o aplicativo.
- Crie uma função personalizada para delegar `volumereplication.*` para usuários específicos.

Contas de serviço

Para fazer chamadas de API do Google Cloud NetApp Volumes por meio de scripts ou "Terraform" , você deve criar uma conta de serviço com o `roles/netappcloudvolumes.admin` papel. Você pode usar esta conta de serviço para gerar os tokens JWT necessários para autenticar solicitações da API do Google Cloud NetApp Volumes de duas maneiras diferentes:

- Gere uma chave JSON e use as APIs do Google para derivar um token JWT dela. Esta é a abordagem mais simples, mas envolve gerenciamento manual de segredos (a chave JSON).
- Usar "Representação de conta de serviço" com `roles/iam.serviceAccountTokenCreator` . O código (script, Terraform e assim por diante) é executado com "Credenciais padrão do aplicativo" e representa a conta de serviço para obter suas permissões. Essa abordagem reflete as práticas recomendadas de segurança do Google.

Consulte "Criando sua conta de serviço e chave privada" na documentação do Google cloud para obter mais informações.

API de Google Cloud NetApp Volumes

A API do Google Cloud NetApp Volumes usa uma API baseada em REST, usando HTTPS (TLSv1.2) como o transporte de rede subjacente. Você pode encontrar a definição mais recente da API e informações sobre como usar a API em "APIs do Cloud Volumes na documentação do Google Cloud".

O ponto de extremidade da API é operado e protegido pela NetApp usando a funcionalidade HTTPS padrão (TLSv1.2).

Tokens JWT

A autenticação na API é realizada com tokens portadores JWT("RFC-7519"). Tokens JWT válidos devem ser obtidos usando a autenticação do Google Cloud IAM. Isso deve ser feito buscando um token do IAM, fornecendo uma chave JSON da conta de serviço.

Registro de auditoria

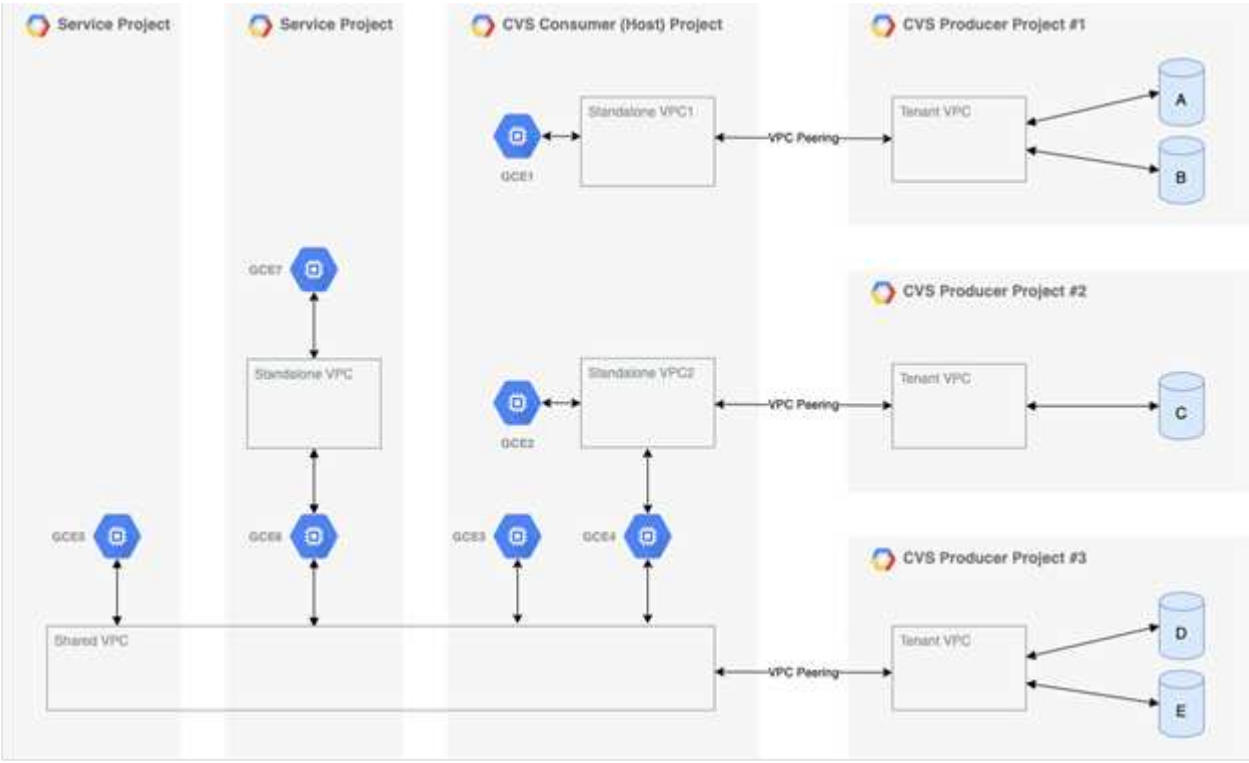
Atualmente, não há logs de auditoria de plano de controle acessíveis ao usuário disponíveis.

Arquitetura do plano de dados

O Google Cloud NetApp Volumes para Google Cloud aproveita o Google Cloud "acesso a serviços privados" estrutura. Nessa estrutura, os usuários podem se conectar ao Google Cloud NetApp Volumes. Esta estrutura usa construções de Service Networking e peering de VPC como outros serviços do Google Cloud, garantindo isolamento completo entre locatários.

Para obter uma visão geral da arquitetura do Google Cloud NetApp Volumes para Google Cloud, consulte "Arquitetura para Google Cloud NetApp Volumes".

As VPCs de usuário (autônomas ou compartilhadas) são pareadas com VPCs dentro de projetos de locatários gerenciados do Google Cloud NetApp Volumes , que hospedam os volumes.



A figura anterior mostra um projeto (o projeto do consumidor do NetApp Volumes no meio) com três redes VPC conectadas ao Google Cloud NetApp Volumes e várias VMs do Compute Engine (GCE1-7) compartilhando volumes:

- O VPC1 permite que o GCE1 acesse os volumes A e B.
- O VPC2 permite que GCE2 e GCE4 acessem o volume C.

- A terceira rede VPC é uma VPC compartilhada, compartilhada com dois projetos de serviço. Ele permite que GCE3, GCE4, GCE5 e GCE6 acessem os volumes D e E. Redes VPC compartilhadas são suportadas somente para volumes do tipo de serviço NetApp Volumes-Performance.

> O GCE7 não pode acessar nenhum volume.

Os dados podem ser criptografados em trânsito (usando criptografia Kerberos e/ou SMB) e em repouso no Google Cloud NetApp Volumes.

Criptografia de dados em trânsito

Os dados em trânsito podem ser criptografados na camada do protocolo NAS, e a própria rede do Google Cloud é criptografada, conforme descrito nas seções a seguir.

Rede Google Cloud

O Google Cloud criptografa o tráfego no nível da rede, conforme descrito em "Criptografia em trânsito" na documentação do Google. Conforme mencionado na seção "Arquitetura do Google Cloud NetApp Volumes" , o Google Cloud NetApp Volumes é entregue a partir de um projeto de produtor PSA controlado pela NetApp.

No caso do NetApp Volumes-SW, o locatário produtor executa VMs do Google para fornecer o serviço. O tráfego entre as VMs do usuário e as VMs do Google Cloud NetApp Volumes é criptografado automaticamente pelo Google.

Embora o caminho de dados para o NetApp Volumes-Performance não seja totalmente criptografado na camada de rede, a NetApp e o Google usam uma combinação "de criptografia IEEE 802.1AE (MACSec)" , "encapsulamento" (criptografia de dados) e redes fisicamente restritas para proteger dados em trânsito entre o tipo de serviço NetApp Google Cloud NetApp Volumes e o Google Cloud.

Protocolos NAS

Os protocolos NFS e SMB NAS fornecem criptografia de transporte opcional na camada de protocolo.

Criptografia SMB

"Criptografia SMB"fornece criptografia de ponta a ponta de dados de SMB e protege os dados contra ocorrências de espionagem em redes não confiáveis. Você pode habilitar a criptografia para a conexão de dados cliente/servidor (disponível somente para clientes compatíveis com SMB3.x) e a autenticação do servidor/controlador de domínio.

Quando a criptografia SMB está habilitada, os clientes que não oferecem suporte à criptografia não podem acessar o compartilhamento.

O Google Cloud NetApp Volumes oferece suporte às cifras de segurança RC4-HMAC, AES-128-CTS-HMAC-SHA1 e AES-256-CTS-HMAC-SHA1 para criptografia SMB. O SMB negocia com o tipo de criptografia mais alto suportado pelo servidor.

NFSv4.1 Kerberos

Para NFSv4.1, o NetApp Volumes-Performance oferece autenticação Kerberos conforme descrito em "RFC7530" . Você pode habilitar o Kerberos por volume.

O tipo de criptografia mais forte disponível atualmente para Kerberos é AES-256-CTS-HMAC-SHA1. O Google Cloud NetApp Volumes é compatível com AES-256-CTS-HMAC-SHA1, AES-128-CTS-HMAC-SHA1, DES3 e

DES para NFS. Ele também suporta ARCFOUR-HMAC (RC4) para tráfego CIFS/SMB, mas não para NFS.

O Kerberos fornece três níveis de segurança diferentes para montagens NFS que oferecem opções de quão forte a segurança do Kerberos deve ser.

De acordo com a RedHat "Opções de montagem comuns" documentação:

```
sec=krb5 uses Kerberos V5 instead of local UNIX UIDs and GIDs to
authenticate users.
sec=krb5i uses Kerberos V5 for user authentication and performs integrity
checking of NFS operations using secure checksums to prevent data
tampering.
sec=krb5p uses Kerberos V5 for user authentication, integrity checking,
and encrypts NFS traffic to prevent traffic sniffing. This is the most
secure setting, but it also involves the most performance overhead.
```

Como regra geral, quanto mais o nível de segurança do Kerberos precisa fazer, pior é o desempenho, pois o cliente e o servidor gastam tempo criptografando e descriptografando operações NFS para cada pacote enviado. Muitos clientes e servidores NFS oferecem suporte para descarregamento AES-NI para as CPUs para uma melhor experiência geral, mas o impacto do Kerberos 5p (criptografia completa de ponta a ponta) no desempenho é significativamente maior que o impacto do Kerberos 5 (autenticação do usuário).

A tabela a seguir mostra as diferenças no que cada nível faz pela segurança e desempenho.

Nível de segurança	Segurança	Desempenho
NFSv3—sistema	• Menos seguro; texto simples com IDs de usuário/grupo numéricos • Capaz de visualizar UID, GID, endereços IP do cliente, caminhos de exportação, nomes de arquivos, permissões em capturas de pacotes	• Melhor para a maioria dos casos
NFSv4.x—sistema	• Mais seguro que o NFSv3 (IDs de cliente, correspondência de string de nome/string de domínio), mas ainda texto simples • Capaz de visualizar UID, GID, endereços IP de clientes, sequências de nomes, IDs de domínio, caminhos de exportação, nomes de arquivos, permissões em capturas de pacotes	• Bom para cargas de trabalho sequenciais (como VMs, bancos de dados, arquivos grandes) • Ruim com alta contagem de arquivos/altos metadados (30-50% pior)

Nível de segurança	Segurança	Desempenho
NFS—krb5	• Criptografia Kerberos para credenciais em cada pacote NFS — envolve UID/GID de usuários/grupos em chamadas RPC no wrapper GSS • O usuário que solicita acesso à montagem precisa de um tíquete Kerberos válido (por meio de nome de usuário/senha ou troca manual de chave); o tíquete expira após um período de tempo especificado e o usuário deve se autenticar novamente para obter acesso • Nenhuma criptografia para operações NFS ou protocolos auxiliares como mount/portmapper/nlm (pode ver caminhos de exportação, endereços IP, identificadores de arquivo, permissões, nomes de arquivo, atime/mtime em capturas de pacotes)	• Melhor na maioria dos casos para Kerberos; pior que AUTH_SYS

Nível de segurança	Segurança	Desempenho
NFS—krb5i	• Criptografia Kerberos para credenciais em cada pacote NFS — envolve UID/GID de usuários/grupos em chamadas RPC no wrapper GSS • O usuário que solicita acesso à montagem precisa de um tíquete Kerberos válido (por meio de nome de usuário/senha ou troca manual de chave); o tíquete expira após um período de tempo especificado e o usuário deve se autenticar novamente para obter acesso • Nenhuma criptografia para operações NFS ou protocolos auxiliares como mount/portmapper/nlm (pode ver caminhos de exportação, endereços IP, identificadores de arquivo, permissões, nomes de arquivo, atime/mtime em capturas de pacotes) • A soma de verificação Kerberos GSS é adicionada a cada pacote para garantir que nada intercepte os pacotes. Se as somas de verificação corresponderem, a conversa será permitida.	• Melhor que o krb5p porque a carga útil do NFS não é criptografada; a única sobrecarga adicionada em comparação ao krb5 é a soma de verificação de integridade. O desempenho do krb5i não será muito pior que o do krb5, mas sofrerá alguma degradação.

Nível de segurança	Segurança	Desempenho
NFS – krb5p	• Criptografia Kerberos para credenciais em cada pacote NFS — envolve UID/GID de usuários/grupos em chamadas RPC no wrapper GSS • O usuário que solicita acesso à montagem precisa de um tíquete Kerberos válido (por meio de nome de usuário/senha ou troca manual de keytab); o tíquete expira após um período de tempo especificado e o usuário deve se autenticar novamente para obter acesso • Todas as cargas de pacotes NFS são criptografadas com o wrapper GSS (não é possível ver identificadores de arquivos, permissões, nomes de arquivos, atime/mtime em capturas de pacotes). • Inclui verificação de integridade. • O tipo de operação NFS é visível (FSINFO, ACCESS, GETATTR e assim por diante). • Protocolos auxiliares (mount, portmap, nlm e assim por diante) não são criptografados - (pode ver caminhos de exportação, endereços IP)	• Pior desempenho dos níveis de segurança; o krb5p precisa criptografar/descriptografar mais. • Melhor desempenho que krb5p com NFSv4.x para cargas de trabalho com alta contagem de arquivos.

No Google Cloud NetApp Volumes, um servidor Active Directory configurado é usado como servidor Kerberos e servidor LDAP (para pesquisar identidades de usuários em um esquema compatível com RFC2307). Nenhum outro servidor Kerberos ou LDAP é suportado. A NetApp recomenda fortemente que você use o LDAP para gerenciamento de identidade no Google Cloud NetApp Volumes. Para obter informações sobre como o NFS Kerberos é exibido em capturas de pacotes, consulte a seção "Considerações sobre detecção/rastreamento de pacotes."

Criptografia de dados em repouso

Todos os volumes no Google Cloud NetApp Volumes são criptografados em repouso usando criptografia AES-256, o que significa que todos os dados do usuário gravados na mídia são criptografados e só podem ser descriptografados com uma chave por volume.

- Para o NetApp Volumes-SW, são usadas chaves geradas pelo Google.
- Para o NetApp Volumes-Performance, as chaves por volume são armazenadas em um gerenciador de chaves integrado ao Google Cloud NetApp Volumes.

A partir de novembro de 2021, a funcionalidade de chaves de criptografia gerenciadas pelo cliente (CMEK) foi disponibilizada. Isso permite que você criptografe as chaves por volume com uma chave mestra por projeto e por região hospedada em "Serviço de gerenciamento de chaves do Google (KMS)." O KMS permite que você anexe gerenciadores de chaves externos.

Para obter informações sobre como configurar o KMS para o NetApp Volumes-Performance, consulte "Configurando chaves de criptografia gerenciadas pelo cliente".

Firewall

O Google Cloud NetApp Volumes expõe várias portas TCP para atender compartilhamentos NFS e SMB:

- "Portas necessárias para acesso NFS"
- "Portas necessárias para acesso SMB"

Além disso, as configurações de SMB, NFS com LDAP, incluindo Kerberos, e de protocolo duplo exigem acesso a um domínio do Windows Active Directory. As conexões do Active Directory devem ser "configurado" feitas por região. Os controladores de domínio (DCs) do Active Directory são identificados usando "Descoberta de DC baseada em DNS" os servidores DNS especificados. Qualquer um dos DCs retornados será usado. A lista de DCs elegíveis pode ser limitada pela especificação de um site do Active Directory.

O Google Cloud NetApp Volumes se comunica usando endereços IP do intervalo CIDR alocado com o comando `gcloud compute address` enquanto "integração do Google Cloud NetApp Volumes". Você pode usar esse CIDR como endereços de origem para configurar firewalls de entrada para seus controladores de domínio do Active Directory.

Os controladores de domínio do Active Directory devem "expor portas para os CIDRs do Google Cloud NetApp Volumes, conforme mencionado aqui".

Visão geral dos protocolos NAS

Os protocolos NAS incluem NFS (v3 e v4.1) e SMB/CIFS (2.x e 3.x). Esses protocolos são como o NetApp Volumes permite acesso compartilhado a dados entre vários clientes NAS. Além disso, o Google Cloud NetApp Volumes pode fornecer acesso a clientes NFS e SMB/CIFS simultaneamente (protocolo duplo), respeitando todas as configurações de identidade e permissão em arquivos e pastas nos compartilhamentos NAS. Para manter a mais alta segurança possível na transferência de dados, o Google Cloud NetApp Volumes oferece suporte à criptografia de protocolo em trânsito usando criptografia SMB e NFS Kerberos 5p.

> O protocolo duplo está disponível somente com o NetApp Volumes-Performance.

Noções básicas de protocolos NAS

Os protocolos NAS são maneiras de vários clientes em uma rede acessarem os mesmos dados em um sistema de armazenamento, como o Google Cloud NetApp Volumes no GCP. NFS e SMB são os protocolos NAS definidos e operam em uma base cliente/servidor, onde o Google Cloud NetApp Volumes atua como servidor. Os clientes enviam solicitações de acesso, leitura e gravação ao servidor, e o servidor é responsável

por coordenar os mecanismos de bloqueio de arquivos, armazenar permissões e manipular solicitações de identidade e autenticação.

Por exemplo, o seguinte processo geral é seguido se um cliente NAS quiser criar um novo arquivo em uma pasta.

1. O cliente solicita ao servidor informações sobre o diretório (permissões, proprietário, grupo, ID do arquivo, espaço disponível e assim por diante); o servidor responde com as informações se o cliente e o usuário solicitantes têm as permissões necessárias na pasta pai.
2. Se as permissões no diretório permitirem acesso, o cliente perguntará ao servidor se o nome do arquivo que está sendo criado já existe no sistema de arquivos. Se o nome do arquivo já estiver em uso, a criação falhará. Se o nome do arquivo não existir, o servidor informa ao cliente que ele pode prosseguir.
3. O cliente emite uma chamada ao servidor para criar o arquivo com o identificador do diretório e o nome do arquivo e define os horários de acesso e modificação. O servidor emite um ID de arquivo exclusivo para o arquivo para garantir que nenhum outro arquivo seja criado com o mesmo ID de arquivo.
4. O cliente envia uma chamada para verificar os atributos do arquivo antes da operação WRITE. Se as permissões permitirem, o cliente grava o novo arquivo. Se o bloqueio for usado pelo protocolo/aplicativo, o cliente solicitará um bloqueio ao servidor para impedir que outros clientes acessem o arquivo enquanto ele estiver bloqueado, para evitar corrupção de dados.

NFS

NFS é um protocolo de sistema de arquivos distribuído que é um padrão IETF aberto definido em Request for Comments (RFC) que permite que qualquer pessoa implemente o protocolo.

Os volumes no Google Cloud NetApp Volumes são compartilhados com clientes NFS exportando um caminho que pode ser acessado por um cliente ou conjunto de clientes. As permissões para montar essas exportações são definidas por políticas e regras de exportação, que podem ser configuradas pelos administradores do Google Cloud NetApp Volumes .

A implementação do NetApp NFS é considerada um padrão ouro para o protocolo e é usada em inúmeros ambientes NAS empresariais. As seções a seguir abordam o NFS e os recursos de segurança específicos disponíveis no Google Cloud NetApp Volumes e como eles são implementados.

Usuários e grupos UNIX locais padrão

O Google Cloud NetApp Volumes contém vários usuários e grupos UNIX padrão para diversas funcionalidades básicas. Esses usuários e grupos não podem ser modificados ou excluídos no momento. No momento, não é possível adicionar novos usuários e grupos locais ao Google Cloud NetApp Volumes. Usuários e grupos UNIX fora dos usuários e grupos padrão precisam ser fornecidos por um serviço de nomes LDAP externo.

A tabela a seguir mostra os usuários e grupos padrão e seus IDs numéricos correspondentes. A NetApp recomenda não criar novos usuários ou grupos no LDAP ou nos clientes locais que reutilizam essas IDs numéricas.

Usuários padrão: IDs numéricos	Grupos padrão: IDs numéricos
• raiz:0 • usuário do computador:65534 • ninguém:65535	• raiz:0 • daemon:1 • usuário do computador:65534 • ninguém:65535

Ao usar o NFSv4.1, o usuário root pode ser exibido como ninguém ao executar comandos de listagem de diretórios em clientes NFS. Isso ocorre devido à configuração de mapeamento de domínio de ID do cliente. Veja a seção chamadaNFSv4.1 e o usuário/grupo nobody para obter detalhes sobre esse problema e como resolvê-lo.

O usuário root

No Linux, a conta root tem acesso a todos os comandos, arquivos e pastas em um sistema de arquivos baseado em Linux. Devido ao poder dessa conta, as práticas recomendadas de segurança geralmente exigem que o usuário root seja desabilitado ou restringido de alguma forma. Nas exportações NFS, o poder que um usuário root tem sobre os arquivos e pastas pode ser controlado no Google Cloud NetApp Volumes por meio de políticas e regras de exportação e um conceito conhecido como root squash.

O root squashing garante que o usuário root que acessa uma montagem NFS seja compactado para o usuário numérico anônimo 65534 (consulte a seção "O usuário anônimo ") e atualmente está disponível somente ao usar o NetApp Volumes-Desempenho selecionando Desativado para acesso root durante a criação da regra de política de exportação. Se o usuário root for espremido para o usuário anônimo, ele não terá mais acesso para executar chown ou "comandos setuid/setgid (a parte pegajosa)" em arquivos ou pastas na montagem NFS, e arquivos ou pastas criados pelo usuário root mostram o UID anônimo como proprietário/grupo. Além disso, as ACLs do NFSv4 não podem ser modificadas pelo usuário root. Entretanto, o usuário root ainda tem acesso ao chmod e aos arquivos excluídos para os quais não tem permissões explícitas. Se você quiser limitar o acesso às permissões de arquivo e pasta de um usuário root, considere usar um volume com ACLs NTFS, criando um usuário do Windows chamado `root` , e aplicando as permissões desejadas aos arquivos ou pastas.

O usuário anônimo

O ID de usuário anônimo (anon) especifica um ID de usuário UNIX ou nome de usuário que é mapeado para solicitações de cliente que chegam sem credenciais NFS válidas. Isso pode incluir o usuário root quando o root squashing for usado. O usuário anônimo no Google Cloud NetApp Volumes é 65534.

Este UID normalmente está associado ao nome de usuário `nobody` ou `nfsnobody` em ambientes Linux. O Google Cloud NetApp Volumes também usa 65534 como o usuário UNIX local `pcuser` (consulte a seção "Usuários e grupos UNIX locais padrão "), que também é o usuário de fallback padrão para mapeamentos de nomes do Windows para o UNIX quando nenhum usuário UNIX correspondente válido pode ser encontrado no LDAP.

Devido às diferenças nos nomes de usuário entre o Linux e o Google Cloud NetApp Volumes para o UID 65534, a sequência de nomes para usuários mapeados para 65534 pode não corresponder ao usar o NFSv4.1. Como resultado, você pode ver `nobody` como o usuário em alguns arquivos e pastas. Veja a seção "NFSv4.1 e o usuário/grupo nobody " para obter informações sobre esse problema e como resolvê-lo.

Controle de acesso/exportações

O acesso inicial de exportação/compartilhamento para montagens NFS é controlado por meio de regras de política de exportação baseadas em host contidas em uma política de exportação. Um IP de host, nome de

host, sub-rede, grupo de rede ou domínio é definido para permitir acesso para montar o compartilhamento NFS e o nível de acesso permitido ao host. As opções de configuração da regra de política de exportação dependem do nível do Google Cloud NetApp Volumes .

Para o NetApp Volumes-SW, as seguintes opções estão disponíveis para configuração de política de exportação:

- **Correspondência de clientes.** Lista separada por vírgulas de endereços IP, lista separada por vírgulas de nomes de host, sub-redes, grupos de rede, nomes de domínio.
- **Regras de acesso RO/RW.** Selecione leitura/gravação ou somente leitura para controlar o nível de acesso à exportação. O NetApp Volumes-Performance oferece as seguintes opções:
- **Correspondência de clientes.** Lista separada por vírgulas de endereços IP, lista separada por vírgulas de nomes de host, sub-redes, grupos de rede, nomes de domínio.
- **Regras de acesso RO/RW.** Selecione leitura/gravação ou somente leitura para controlar o nível de acesso à exportação.
- **Acesso root (ligado/desligado).** Configura o root squash (veja a seção "O usuário root " para mais detalhes).
- **Tipo de protocolo.** Isso limita o acesso à montagem NFS a uma versão de protocolo específica. Ao especificar NFSv3 e NFSv4.1 para o volume, deixe ambos em branco ou marque ambas as caixas.
- **Nível de segurança Kerberos (quando Ativar Kerberos estiver selecionado).** Fornece as opções de krb5, krb5i e/ou krb5p para acesso somente leitura ou leitura-gravação.

Alterar propriedade (chown) e alterar grupo (chgrp)

O NFS no Google Cloud NetApp Volumes permite que somente o usuário root execute chown/chgrp em arquivos e pastas. Outros usuários veem um `Operation not permitted` erro — mesmo em arquivos que eles possuem. Se você usar raiz de abóbora (conforme abordado na seção "O usuário root "), o root é repassado a um usuário não root e não tem permissão para acessar chown e chgrp. Atualmente, não há soluções alternativas no Google Cloud NetApp Volumes para permitir chown e chgrp para usuários não root. Se forem necessárias alterações de propriedade, considere usar volumes de protocolo duplo e defina o estilo de segurança como NTFS para controlar as permissões do lado do Windows.

Gerenciamento de permissões

O Google Cloud NetApp Volumes oferece suporte a bits de modo (como 644, 777 e assim por diante para rwx) e ACLs NFSv4.1 para controlar permissões em clientes NFS para volumes que usam o estilo de segurança UNIX. O gerenciamento de permissões padrão é usado para eles (como chmod, chown ou nfs4_setfacl) e funciona com qualquer cliente Linux que os suporte.

Além disso, ao usar volumes de protocolo duplo definidos como NTFS, os clientes NFS podem aproveitar o mapeamento de nomes do Google Cloud NetApp Volumes para usuários do Windows, que são usados para resolver as permissões NTFS. Isso requer uma conexão LDAP com o Google Cloud NetApp Volumes para fornecer traduções de ID numérico para nome de usuário, porque o Google Cloud NetApp Volumes requer um nome de usuário UNIX válido para mapear corretamente para um nome de usuário do Windows.

Fornecendo ACLs granulares para NFSv3

As permissões de bits de modo abrangem apenas o proprietário, o grupo e todos os outros na semântica, o que significa que não há controles granulares de acesso de usuário para o NFSv3 básico. O Google Cloud NetApp Volumes não oferece suporte a ACLs POSIX nem a atributos estendidos (como chattr), portanto, ACLs granulares só são possíveis nos seguintes cenários com NFSv3:

- Volumes de estilo de segurança NTFS (servidor CIFS necessário) com mapeamentos de usuários válidos do UNIX para o Windows.
- ACLs do NFSv4.1 aplicadas usando um cliente de administração montando o NFSv4.1 para aplicar ACLs.

Ambos os métodos exigem uma conexão LDAP para gerenciamento de identidade UNIX e informações válidas de usuário e grupo UNIX preenchidas (consulte a seção"LDAP") e estão disponíveis somente com instâncias do NetApp Volumes-Performance. Para usar volumes de estilo de segurança NTFS com NFS, você deve usar protocolo duplo (SMB e NFSv3) ou protocolo duplo (SMB e NFSv4.1), mesmo que nenhuma conexão SMB seja feita. Para usar ACLs NFSv4.1 com montagens NFSv3, você deve selecionar `Both (NFSv3/NFSv4.1)` como o tipo de protocolo.

Os bits regulares do modo UNIX não fornecem o mesmo nível de granularidade em permissões que as ACLs NTFS ou NFSv4.x fornecem. A tabela a seguir compara a granularidade de permissão entre bits do modo NFSv3 e ACLs do NFSv4.1. Para obter informações sobre ACLs NFSv4.1, consulte "nfs4_acl - Listas de controle de acesso NFSv4" .

Bits do modo NFSv3	ACLs do NFSv4.1
• Definir ID do usuário na execução • Definir ID do grupo na execução • Salvar texto trocado (não definido em POSIX) • Permissão de leitura para o proprietário • Permissão de escrita para o proprietário • Permissão de execução para o proprietário em um arquivo; ou procurar (pesquisar) permissão para o proprietário no diretório • Permissão de leitura para grupo • Permissão de escrita para grupo • Permissão de execução para grupo em um arquivo; ou procurar (pesquisar) permissão para grupo no diretório • Permissão de leitura para outros • Permissão de escrita para outros • Permissão de execução para outros em um arquivo; ou procurar (pesquisar) permissão para outros no diretório	Tipos de entrada de controle de acesso (ACE) (Permitir/Negar/Auditar) * Sinalizadores de herança * herança de diretório * herança de arquivo * herança sem propagação * somente herança Permissões * ler-dados (arquivos) / listar-diretórios (diretórios) * gravar-dados (arquivos) / criar-arquivo (diretórios) * anexar-dados (arquivos) / criar-subdiretório (diretórios) * executar (arquivos) / alterar-diretório (diretórios) * excluir * excluir-filho * ler-atributos * gravar-atributos * ler-atributos-nomeados * gravar-atributos-nomeados * ler-ACL * gravar-ACL * gravar-proprietário * Sincronizar

Por fim, a associação ao grupo NFS (tanto no NFSv3 quanto no NFSV4.x) é limitada a um máximo padrão de 16 para AUTH_SYS, conforme os limites de pacotes RPC. O NFS Kerberos fornece até 32 grupos e as ACLs NFSv4 removem a limitação por meio de ACLs granulares de usuários e grupos (até 1.024 entradas por ACE).

Além disso, o Google Cloud NetApp Volumes oferece suporte estendido a grupos, ampliando o número máximo de grupos suportados para até 32. Isso requer uma conexão LDAP com um servidor LDAP que contenha identidades válidas de usuários e grupos UNIX. Para obter mais informações sobre como configurar isso, consulte "Criação e gerenciamento de volumes NFS" a documentação do Google.

IDs de usuários e grupos NFSv3

Os IDs de usuários e grupos do NFSv3 chegam como IDs numéricos em vez de nomes. O Google Cloud

NetApp Volumes não faz resolução de nome de usuário para essas IDs numéricas com NFSv3, com volumes de estilo de segurança UNIX usando apenas bits de modo. Quando ACLs do NFSv4.1 estão presentes, uma consulta de ID numérica e/ou consulta de sequência de nomes é necessária para resolver a ACL corretamente, mesmo ao usar o NFSv3. Com volumes de estilo de segurança NTFS, o Google Cloud NetApp Volumes deve resolver uma ID numérica para um usuário UNIX válido e, em seguida, mapear para um usuário Windows válido para negociar direitos de acesso.

Limitações de segurança de IDs de usuários e grupos NFSv3

Com o NFSv3, o cliente e o servidor nunca precisam confirmar se o usuário que tenta uma leitura ou gravação com uma ID numérica é um usuário válido; ele é apenas implicitamente confiável. Isso expõe o sistema de arquivos a possíveis violações simplesmente falsificando qualquer ID numérica. Para evitar falhas de segurança como essa, há algumas opções disponíveis para o Google Cloud NetApp Volumes.

- A implementação do Kerberos para NFS força os usuários a se autenticarem com um nome de usuário e senha ou um arquivo keytab para obter um tíquete Kerberos para permitir acesso a uma montagem. O Kerberos está disponível com instâncias do NetApp Volumes-Performance e somente com o NFSv4.1.
- Limitar a lista de hosts em suas regras de política de exportação limita quais clientes NFSv3 têm acesso ao volume do Google Cloud NetApp Volumes .
- O uso de volumes de protocolo duplo e a aplicação de ACLs NTFS ao volume força os clientes NFSv3 a resolver IDs numéricos para nomes de usuários UNIX válidos para autenticação adequada para acessar montagens. Isso requer a ativação do LDAP e a configuração de identidades de usuários e grupos do UNIX.
- Eliminar o usuário root limita os danos que um usuário root pode causar a uma montagem NFS, mas não remove completamente o risco. Para mais informações, consulte a seção "O usuário root ."

Em última análise, a segurança do NFS é limitada ao que a versão do protocolo que você está usando oferece. O NFSv3, embora tenha melhor desempenho em geral que o NFSv4.1, não oferece o mesmo nível de segurança.

NFSv4.1

O NFSv4.1 oferece maior segurança e confiabilidade em comparação ao NFSv3, pelos seguintes motivos:

- Bloqueio integrado por meio de um mecanismo baseado em arrendamento
- Sessões com estado
- Toda a funcionalidade NFS em uma única porta (2049)
- Somente TCP
- Mapeamento de domínio de ID
- Integração Kerberos (NFSv3 pode usar Kerberos, mas apenas para NFS, não para protocolos auxiliares como NLM)

Dependências do NFSv4.1

Devido aos recursos de segurança adicionais no NFSv4.1, há algumas dependências externas envolvidas que não eram necessárias para usar o NFSv3 (semelhante a como o SMB requer dependências como o Active Directory).

ACLs do NFSv4.1

O Google Cloud NetApp Volumes oferece suporte para ACLs NFSv4.x, que oferecem vantagens distintas sobre as permissões normais no estilo POSIX, como as seguintes:

- Controle granular do acesso do usuário a arquivos e diretórios
- Melhor segurança NFS
- Interoperabilidade aprimorada com CIFS/SMB
- Remoção da limitação do NFS de 16 grupos por usuário com segurança AUTH_SYS
- As ACLs ignoram a necessidade de resolução de ID de grupo (GID), o que efetivamente remove o limite de GID. As ACLs do NFSv4.1 são controladas por clientes NFS, não pelo Google Cloud NetApp Volumes. Para usar ACLs do NFSv4.1, certifique-se de que a versão do software do seu cliente seja compatível com elas e que os utilitários NFS adequados estejam instalados.

Compatibilidade entre ACLs NFSv4.1 e clientes SMB

As ACLs do NFSv4 são diferentes das ACLs de nível de arquivo do Windows (ACLs do NTFS), mas têm funcionalidade semelhante. No entanto, em ambientes NAS multiprotocolo, se as ACLs NFSv4.1 estiverem presentes e você estiver usando acesso de protocolo duplo (NFS e SMB nos mesmos conjuntos de dados), os clientes que usam SMB2.0 e versões posteriores não poderão visualizar ou gerenciar ACLs nas guias de segurança do Windows.

Como funcionam as ACLs do NFSv4.1

Para referência, os seguintes termos são definidos:

- **Lista de controle de acesso (ACL).** Uma lista de entradas de permissões.
- **Entrada de controle de acesso (ACE).** Uma entrada de permissão na lista.

Quando um cliente define uma ACL NFSv4.1 em um arquivo durante uma operação SETATTR, o Google Cloud NetApp Volumes define essa ACL no objeto, substituindo qualquer ACL existente. Se não houver ACL em um arquivo, as permissões de modo no arquivo serão calculadas a partir de OWNER@, GROUP@ e EVERYONE@. Se houver algum bit SUID/SGID/STICKY existente no arquivo, eles não serão afetados.

Quando um cliente obtém uma ACL NFSv4.1 em um arquivo durante uma operação GETATTR, o Google Cloud NetApp Volumes lê a ACL NFSv4.1 associada ao objeto, constrói uma lista de ACEs e retorna a lista ao cliente. Se o arquivo tiver uma ACL NT ou bits de modo, uma ACL será construída a partir de bits de modo e retornada ao cliente.

O acesso será negado se uma DENY ACE estiver presente na ACL; o acesso será concedido se uma ALLOW ACE existir. Entretanto, o acesso também será negado se nenhuma das ACEs estiver presente na ACL.

Um descritor de segurança consiste em uma ACL de segurança (SACL) e uma ACL discricionária (DACL). Quando o NFSv4.1 interopera com o CIFS/SMB, o DACL é mapeado um-para-um com o NFSv4 e o CIFS. O DACL consiste em ALLOW e DENY ACEs.

Se um básico `chmod` é executado em um arquivo ou pasta com ACLs NFSv4.1 definidas, as ACLs de usuário e grupo existentes são preservadas, mas as ACLs padrão OWNER@, GROUP@, EVERYONE@ são modificadas.

Um cliente que usa ACLs do NFSv4.1 pode definir e visualizar ACLs para arquivos e diretórios no sistema. Quando um novo arquivo ou subdiretório é criado em um diretório que possui uma ACL, esse objeto herda todas as ACEs na ACL que foram marcadas com o apropriado "sinalizadores de herança" .

Se um arquivo ou diretório tiver uma ACL NFSv4.1, essa ACL será usada para controlar o acesso, independentemente do protocolo usado para acessar o arquivo ou diretório.

Arquivos e diretórios herdam ACEs de ACLs NFSv4 em diretórios pais (possivelmente com modificações apropriadas), desde que as ACEs tenham sido marcadas com os sinalizadores de herança corretos.

Quando um arquivo ou diretório é criado como resultado de uma solicitação NFSv4, a ACL no arquivo ou diretório resultante depende se a solicitação de criação de arquivo inclui uma ACL ou apenas permissões de acesso a arquivos UNIX padrão. A ACL também depende se o diretório pai tem uma ACL.

- Se a solicitação incluir uma ACL, essa ACL será usada.
- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão e o diretório pai não tiver uma ACL, o modo de arquivo do cliente será usado para definir permissões de acesso a arquivos UNIX padrão.
- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão e o diretório pai tiver uma ACL não herdável, uma ACL padrão com base nos bits de modo passados na solicitação será definida no novo objeto.
- Se a solicitação incluir apenas permissões de acesso a arquivos UNIX padrão, mas o diretório pai tiver uma ACL, as ACEs na ACL do diretório pai serão herdadas pelo novo arquivo ou diretório, desde que as ACEs tenham sido marcadas com os sinalizadores de herança apropriados.

Permissões da ACE

As permissões ACLs do NFSv4.1 usam uma série de valores de letras maiúsculas e minúsculas (como `rxtncy`) para controlar o acesso. Para obter mais informações sobre esses valores de letras, consulte "COMO: Usar a ACL do NFSv4" .

Comportamento da ACL do NFSv4.1 com umask e herança de ACL

"As ACLs do NFSv4 oferecem a capacidade de oferecer herança de ACL" . Herança de ACL significa que arquivos ou pastas criados abaixo de objetos com ACLs NFSv4.1 definidos podem herdar as ACLs com base na configuração do "Sinalizador de herança ACL" .

"Umask"é usado para controlar o nível de permissão no qual arquivos e pastas são criados em um diretório sem interação do administrador. Por padrão, o Google Cloud NetApp Volumes permite que o umask substitua ACLs herdados, o que é o comportamento esperado de acordo com "RFC 5661" .

Formatação ACL

As ACLs do NFSv4.1 têm formatação específica. O exemplo a seguir é um conjunto ACE em um arquivo:

```
A::ldapuser@domain.netapp.com:rwatTnNcCy
```

O exemplo anterior segue as diretrizes de formato ACL de:

```
type:flags:principal:permissions
```

Um tipo de `A` significa "permitir". Os sinalizadores de herança não são definidos neste caso, porque o principal não é um grupo e não inclui herança. Além disso, como o ACE não é uma entrada de AUDITORIA, não há necessidade de definir sinalizadores de auditoria. Para obter mais informações sobre ACLs do NFSv4.1,

consulte "http://linux.die.net/man/5/nfs4_acl" .

Se a ACL do NFSv4.1 não estiver definida corretamente (ou uma sequência de nomes não puder ser resolvida pelo cliente e pelo servidor), a ACL poderá não se comportar conforme o esperado, ou a alteração da ACL poderá não ser aplicada e gerar um erro.

Erros de amostra incluem:

```
Failed setxattr operation: Invalid argument
Scanning ACE string 'A:: user@rwaDxtTnNcCy' failed.
```

NEGAÇÃO explícita

As permissões do NFSv4.1 podem incluir atributos DENY explícitos para PROPRIETÁRIO, GRUPO e TODOS. Isso ocorre porque as ACLs do NFSv4.1 são negadas por padrão, o que significa que se uma ACL não for explicitamente concedida por uma ACE, ela será negada. Atributos DENY explícitos substituem quaisquer ACEs de ACESSO, explícitos ou não.

DENY ACEs são definidos com uma tag de atributo de `D` .

No exemplo abaixo, GROUP@ tem todas as permissões de leitura e execução, mas não tem acesso de gravação.

```
sh-4.1$ nfs4_getfacl /mixed
A::ldapuser@domain.netapp.com:ratTnNcCy
A::OWNER@:rwaDxtTnNcCy
D::OWNER@:
A:g:GROUP@:rxtncy
D:g:GROUP@:waDTC
A::EVERYONE@:rxtncy
D::EVERYONE@:waDTC
```

DENY ACEs devem ser evitadas sempre que possível porque podem ser confusas e complicadas; ALLOW ACLs que não são explicitamente definidas são implicitamente negadas. Quando DENY ACEs são definidos, os usuários podem ter acesso negado quando esperam que o acesso seja concedido.

O conjunto anterior de ACEs é equivalente a 755 bits de modo, o que significa:

- O proprietário tem todos os direitos.
- Os grupos têm permissão somente para leitura.
- Outros somente leram.

Entretanto, mesmo que as permissões sejam ajustadas para o equivalente a 775, o acesso pode ser negado devido ao DENY explícito definido em EVERYONE.

Dependências de mapeamento de domínio de ID NFSv4.1

O NFSv4.1 utiliza a lógica de mapeamento de domínio de ID como uma camada de segurança para ajudar a verificar se um usuário que tenta acessar uma montagem NFSv4.1 é realmente quem ele afirma ser. Nesses

casos, o nome de usuário e o nome do grupo provenientes do cliente NFSv4.1 anexam uma sequência de nome e a enviam para a instância do Google Cloud NetApp Volumes . Se a combinação de nome de usuário/grupo e ID não corresponder, o usuário e/ou grupo será reduzido ao usuário padrão ninguém especificado no `/etc/idmapd.conf` arquivo no cliente.

Esta sequência de ID é um requisito para a adesão adequada às permissões, especialmente quando ACLs NFSv4.1 e/ou Kerberos estão em uso. Como resultado, dependências do servidor de serviço de nomes, como servidores LDAP, são necessárias para garantir a consistência entre clientes e Google Cloud NetApp Volumes para resolução adequada de identidade de nomes de usuários e grupos.

O Google Cloud NetApp Volumes usa um valor de nome de domínio de ID padrão estático de `defaultv4iddomain.com` . Os clientes NFS usam como padrão o nome de domínio DNS para suas configurações de nome de domínio de ID, mas você pode ajustar manualmente o nome de domínio de ID em `/etc/idmapd.conf` .

Se o LDAP estiver habilitado no Google Cloud NetApp Volumes, o Google Cloud NetApp Volumes automatizará o domínio do ID NFS para alterar o que está configurado para o domínio de pesquisa no DNS e os clientes não precisarão ser modificados, a menos que usem nomes de pesquisa de domínio DNS diferentes.

Quando o Google Cloud NetApp Volumes consegue resolver um nome de usuário ou nome de grupo em arquivos locais ou LDAP, a sequência de caracteres de domínio é usada e IDs de domínio não correspondentes são compactados para ninguém. Se o Google Cloud NetApp Volumes não conseguir encontrar um nome de usuário ou nome de grupo em arquivos locais ou LDAP, o valor de ID numérico será usado e o cliente NFS resolverá o nome corretamente (isso é semelhante ao comportamento do NFSv3).

Sem alterar o domínio do ID NFSv4.1 do cliente para corresponder ao que o volume do Google Cloud NetApp Volumes está usando, você verá o seguinte comportamento:

- Usuários e grupos UNIX com entradas locais no Google Cloud NetApp Volumes (como root, conforme definido em usuários e grupos UNIX locais) são compactados para o valor nobody.
- Usuários e grupos UNIX com entradas no LDAP (se o Google Cloud NetApp Volumes estiver configurado para usar LDAP) serão compactados para ninguém se os domínios DNS forem diferentes entre clientes NFS e o Google Cloud NetApp Volumes.
- Usuários e grupos UNIX sem entradas locais ou entradas LDAP usam o valor de ID numérico e resolvem para o nome especificado no cliente NFS. Se não houver nenhum nome no cliente, somente o ID numérico será exibido.

A seguir são mostrados os resultados do cenário anterior:

```
# ls -la /mnt/home/prof1/nfs4/
total 8
drwxr-xr-x 2 nobody nobody 4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root   4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835   9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 nobody nobody    0 Feb  3 12:06 root-user-file
```

Quando os domínios de ID do cliente e do servidor correspondem, a mesma listagem de arquivos fica assim:

```
# ls -la
total 8
drwxr-xr-x 2 root   root         4096 Feb  3 12:07 .
drwxrwxrwx 7 root   root         4096 Feb  3 12:06 ..
-rw-r--r-- 1   9835         9835    0 Feb  3 12:07 client-user-no-name
-rw-r--r-- 1 apache apache-group    0 Feb  3 12:07 ldap-user-file
-rw-r--r-- 1 root   root            0 Feb  3 12:06 root-user-file
```

Para obter mais informações sobre esse problema e como resolvê-lo, consulte a seção "NFSv4.1 e o usuário/grupo nobody ."

Dependências do Kerberos

Se você planeja usar o Kerberos com NFS, deverá ter o seguinte com o Google Cloud NetApp Volumes:

- Domínio do Active Directory para serviços do Kerberos Distribution Center (KDC)
- Domínio do Active Directory com atributos de usuário e grupo preenchidos com informações do UNIX para funcionalidade LDAP (o NFS Kerberos no Google Cloud NetApp Volumes requer um SPN de usuário para mapeamento de usuário do UNIX para funcionalidade adequada).
- LDAP habilitado na instância do Google Cloud NetApp Volumes
- Domínio do Active Directory para serviços DNS

NFSv4.1 e o usuário/grupo nobody

Um dos problemas mais comuns observados com uma configuração NFSv4.1 é quando um arquivo ou pasta é mostrado em uma lista usando `ls` como sendo propriedade do `user:group` combinação de `nobody:nobody` .

Por exemplo:

```
sh-4.2$ ls -la | grep prof1-file
-rw-r--r-- 1 nobody nobody    0 Apr 24 13:25 prof1-file
```

E o ID numérico é `99` .

```
sh-4.2$ ls -lan | grep prof1-file
-rw-r--r-- 1 99 99    0 Apr 24 13:25 prof1-file
```

Em alguns casos, o arquivo pode mostrar o proprietário correto, mas `nobody` como o grupo.

```
sh-4.2$ ls -la | grep newfile1
-rw-r--r-- 1 prof1  nobody    0 Oct  9  2019 newfile1
```

Quem é ninguém?

O `nobody` usuário no NFSv4.1 é diferente do `nfsnobody` usuário. Você pode visualizar como um cliente NFS vê cada usuário executando o `id` comando:

```
# id nobody
uid=99(nobody) gid=99(nobody) groups=99(nobody)
# id nfsnobody
uid=65534(nfsnobody) gid=65534(nfsnobody) groups=65534(nfsnobody)
```

Com o NFSv4.1, o `nobody` usuário é o usuário padrão definido pelo `idmapd.conf` arquivo e pode ser definido como qualquer usuário que você queira usar.

```
# cat /etc/idmapd.conf | grep nobody
#Nobody-User = nobody
#Nobody-Group = nobody
```

Por que isso acontece?

Como a segurança por meio do mapeamento de sequências de nomes é um princípio fundamental das operações do NFSv4.1, o comportamento padrão quando uma sequência de nomes não corresponde corretamente é restringir esse usuário a um que normalmente não terá acesso a arquivos e pastas pertencentes a usuários e grupos.

Quando você vê `nobody` para o usuário e/ou grupo nas listagens de arquivos, isso geralmente significa que algo no NFSv4.1 está mal configurado. A diferenciação entre maiúsculas e minúsculas pode ser importante aqui.

Por exemplo, se user1@CVSDEMO.LOCAL (uid 1234, gid 1234) estiver acessando uma exportação, o Google Cloud NetApp Volumes deverá conseguir encontrar user1@CVSDEMO.LOCAL (uid 1234, gid 1234). Se o usuário no Google Cloud NetApp Volumes for USER1@CVSDEMO.LOCAL, não haverá correspondência (USER1 maiúsculo versus user1 minúsculo). Em muitos casos, você pode ver o seguinte no arquivo de mensagens no cliente:

```
May 19 13:14:29 centos7 nfsidmap[17481]: nss_getpwnam: name
'root@defaultv4iddomain.com' does not map into domain 'CVSDEMO.LOCAL'
May 19 13:15:05 centos7 nfsidmap[17534]: nss_getpwnam: name 'nobody' does
not map into domain 'CVSDEMO.LOCAL'
```

O cliente e o servidor devem concordar que um usuário é realmente quem ele afirma ser, então você deve verificar o seguinte para garantir que o usuário que o cliente vê tenha as mesmas informações que o usuário que o Google Cloud NetApp Volumes vê.

- **ID de domínio NFSv4.x.** Cliente: `idmapd.conf` arquivo; O Google Cloud NetApp Volumes usa `defaultv4iddomain.com` e não pode ser alterado manualmente. Se estiver usando LDAP com NFSv4.1, o Google Cloud NetApp Volumes altera o domínio de ID para o que o domínio de pesquisa de DNS está usando, que é o mesmo que o domínio do AD.
- **Nome de usuário e IDs numéricos.** Isso determina onde o cliente está procurando por nomes de usuário e aproveita a configuração do switch de serviço de nomes — cliente: `nsswitch.conf` e/ou arquivos de

senha e grupo locais; o Google Cloud NetApp Volumes não permite modificações nisso, mas adiciona automaticamente o LDAP à configuração quando ele é ativado.

- **Nome do grupo e IDs numéricos.** Isso determina onde o cliente está procurando por nomes de grupos e aproveita a configuração do switch de serviço de nomes — cliente: `nsswitch.conf` e/ou arquivos de senha e grupo locais; o Google Cloud NetApp Volumes não permite modificações nisso, mas adiciona automaticamente o LDAP à configuração quando ele é ativado.

Em quase todos os casos, se você ver `nobody` nas listagens de usuários e grupos de clientes, o problema é a tradução do ID de domínio do nome do usuário ou grupo entre o Google Cloud NetApp Volumes e o cliente NFS. Para evitar esse cenário, use o LDAP para resolver informações de usuários e grupos entre clientes e o Google Cloud NetApp Volumes.

Visualizando sequências de ID de nome para NFSv4.1 em clientes

Se você estiver usando o NFSv4.1, há um mapeamento de nome-string que ocorre durante as operações do NFS, conforme descrito anteriormente.

Além de usar `/var/log/messages` para encontrar um problema com IDs NFSv4, você pode usar o "nfsidmap -l" comando no cliente NFS para visualizar quais nomes de usuários foram mapeados corretamente para o domínio NFSv4.

Por exemplo, esta é a saída do comando depois que um usuário que pode ser encontrado pelo cliente e Google Cloud NetApp Volumes acessa uma montagem NFSv4.x:

```
# nfsidmap -l
4 .id_resolver keys found:
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

Quando um usuário não mapeia corretamente no domínio de ID NFSv4.1 (neste caso, `netapp-user`) tenta acessar a mesma montagem e toca em um arquivo, eles são atribuídos `nobody:nobody` , como esperado.

```
# su netapp-user
sh-4.2$ id
uid=482600012(netapp-user), 2000(secondary)
sh-4.2$ cd /mnt/nfs4/
sh-4.2$ touch newfile
sh-4.2$ ls -la
total 16
drwxrwxrwx  5 root   root   4096 Jan 14 17:13 .
drwxr-xr-x. 8 root   root     81 Jan 14 10:02 ..
-rw-r--r--  1 nobody nobody    0 Jan 14 17:13 newfile
drwxrwxrwx  2 root   root   4096 Jan 13 13:20 qtree1
drwxrwxrwx  2 root   root   4096 Jan 13 13:13 qtree2
drwxr-xr-x  2 nfs4   daemon 4096 Jan 11 14:30 testdir
```

O `nfsidmap -l` a saída mostra o usuário `pcuser` na exibição, mas não `netapp-user` ; este é o usuário anônimo em nossa regra de política de exportação(`65534`).

```
# nfsidmap -l
6 .id_resolver keys found:
  gid:pcuser@CVSDEMO.LOCAL
  uid:pcuser@CVSDEMO.LOCAL
  gid:daemon@CVSDEMO.LOCAL
  uid:nfs4@CVSDEMO.LOCAL
  gid:root@CVSDEMO.LOCAL
  uid:root@CVSDEMO.LOCAL
```

PMEs

"PMEs" SMB é um protocolo de compartilhamento de arquivos em rede desenvolvido pela Microsoft que fornece autenticação centralizada de usuário/grupo, permissões, bloqueio e compartilhamento de arquivos para vários clientes SMB em uma rede Ethernet. Arquivos e pastas são apresentados aos clientes por meio de compartilhamentos, que podem ser configurados com diversas propriedades de compartilhamento e oferecem controle de acesso por meio de permissões em nível de compartilhamento. O SMB pode ser apresentado a qualquer cliente que ofereça suporte ao protocolo, incluindo clientes Windows, Apple e Linux.

O Google Cloud NetApp Volumes oferece suporte para as versões SMB 2.1 e 3.x do protocolo.

Controle de acesso/compartilhamentos SMB

- Quando um nome de usuário do Windows solicita acesso ao volume do Google Cloud NetApp Volumes , o Google Cloud NetApp Volumes procura um nome de usuário do UNIX usando os métodos configurados pelos administradores do Google Cloud NetApp Volumes .
- Se um provedor de identidade UNIX externo (LDAP) estiver configurado e os nomes de usuário do Windows/UNIX forem idênticos, os nomes de usuário do Windows serão mapeados 1:1 para os nomes de usuário do UNIX sem necessidade de nenhuma configuração adicional. Quando o LDAP está habilitado, o Active Directory é usado para hospedar esses atributos UNIX para objetos de usuário e grupo.
- Se os nomes do Windows e os nomes do UNIX não corresponderem de forma idêntica, o LDAP deverá ser configurado para permitir que o Google Cloud NetApp Volumes use a configuração de mapeamento de nomes LDAP (consulte a seção"Usando LDAP para mapeamento de nomes assimétricos").
- Se o LDAP não estiver em uso, os usuários do Windows SMB serão mapeados para um usuário UNIX local padrão chamado `pcuser` no Google Cloud NetApp Volumes. Isso significa arquivos escritos no Windows por usuários que mapeiam para o `pcuser` mostrar a propriedade do UNIX como `pcuser` em ambientes NAS multiprotocolo. `pcuser` aqui está efetivamente o `nobody` usuário em ambientes Linux (UID 65534).

Em implantações somente com SMB, o `pcuser` O mapeamento ainda ocorre, mas não importa, porque a propriedade de usuários e grupos do Windows é exibida corretamente e o acesso NFS ao volume somente SMB não é permitido. Além disso, os volumes somente SMB não oferecem suporte à conversão para volumes NFS ou de protocolo duplo após serem criados.

O Windows utiliza o Kerberos para autenticação de nome de usuário com os controladores de domínio do Active Directory, o que requer uma troca de nome de usuário/senha com os DCs do AD, que é externo à instância do Google Cloud NetApp Volumes . A autenticação Kerberos é usada quando o `\\SERVERNAME` O caminho UNC é usado pelos clientes SMB e o seguinte é verdadeiro:

- Existe uma entrada DNS A/AAAA para SERVERNAME
- Existe um SPN válido para acesso SMB/CIFS para SERVERNAME

Quando um volume SMB do Google Cloud NetApp Volumes é criado, o nome da conta da máquina é criado conforme definido na seção"Como o Google Cloud NetApp Volumes aparece no Active Directory." O nome da conta da máquina também se torna o caminho de acesso do compartilhamento SMB porque o Google Cloud NetApp Volumes utiliza o DNS dinâmico (DDNS) para criar as entradas A/AAAA e PTR necessárias no DNS e as entradas SPN necessárias na entidade de conta da máquina.

Para que entradas PTR sejam criadas, a zona de pesquisa reversa para o endereço IP da instância do Google Cloud NetApp Volumes deve existir no servidor DNS.

Por exemplo, este volume do Google Cloud NetApp Volumes usa o seguinte caminho de compartilhamento UNC: `\\cvs-east- 433d.cvsdemo.local` .

No Active Directory, estas são as entradas SPN geradas Google Cloud NetApp Volumes:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Este é o resultado da pesquisa direta/reversa de DNS:

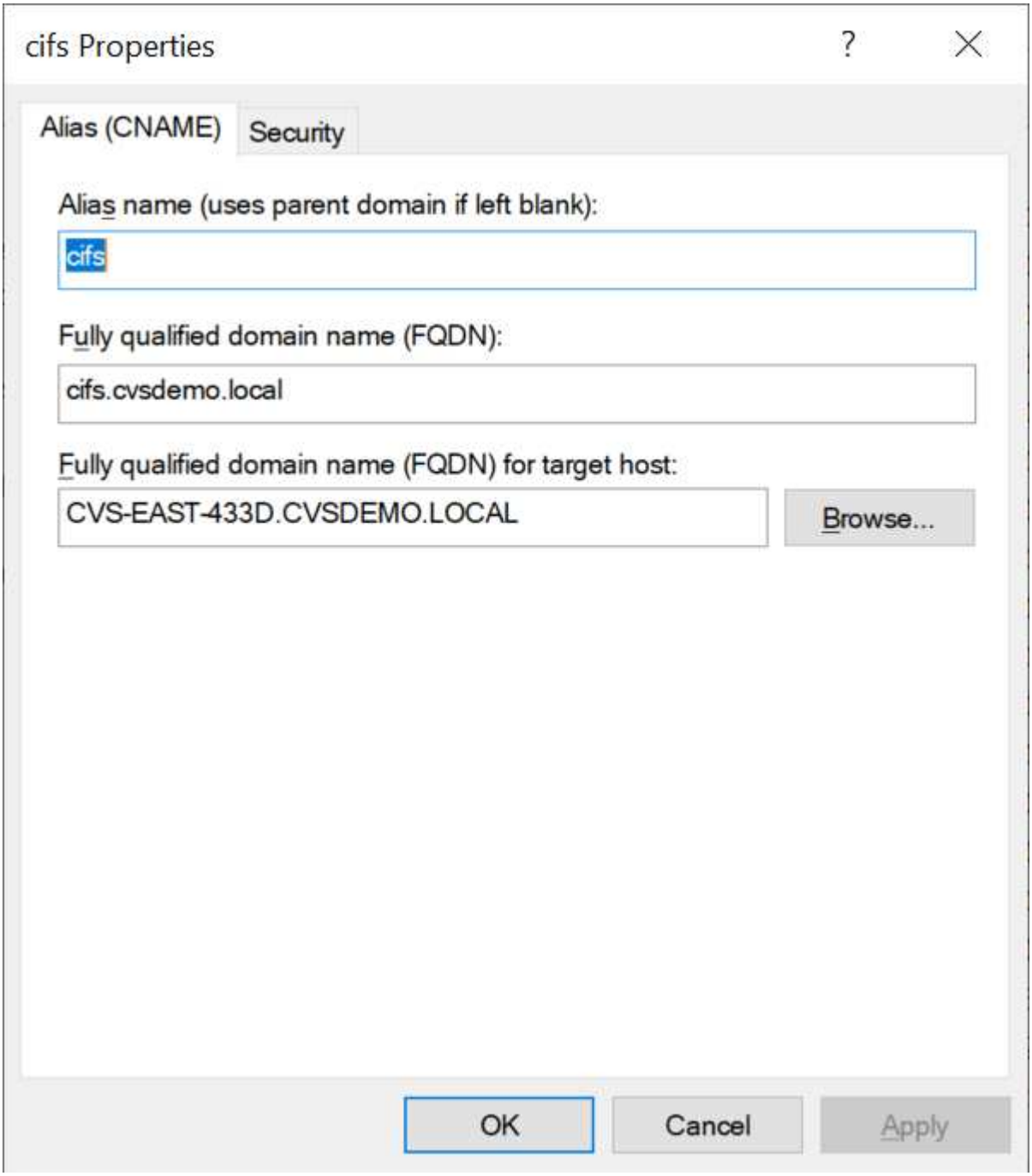
```
PS C:\> nslookup NetApp Volumes-EAST-433D
Server:  activedirectory. region. lab. internal
Address:  10. xx.0. xx
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
PS C:\> nslookup 10. xxx.0. x
Server:  activedirectory.region.lab.internal
Address:  10.xx.0.xx
Name:    NetApp Volumes-EAST-433D.CVSDEMO.LOCAL
Address:  10. xxx.0. x
```

Opcionalmente, mais controle de acesso pode ser aplicado habilitando/exigindo criptografia SMB para compartilhamentos SMB no Google Cloud NetApp Volumes. Se a criptografia SMB não for suportada por um dos endpoints, o acesso não será permitido.

Usando aliases de nomes SMB

Em alguns casos, pode ser uma preocupação de segurança para os usuários finais saberem o nome da conta da máquina em uso para o Google Cloud NetApp Volumes. Em outros casos, você pode simplesmente querer fornecer um caminho de acesso mais simples aos seus usuários finais. Nesses casos, você pode criar aliases SMB.

Se quiser criar aliases para o caminho de compartilhamento SMB, você pode aproveitar o que é conhecido como registro CNAME no DNS. Por exemplo, se você quiser usar o nome `\\CIFS` para acessar ações em vez de `\\cvs-east- 433d.cvsdemo.local` , mas você ainda deseja usar a autenticação Kerberos, um CNAME no DNS que aponta para o registro A/AAAA existente e um SPN adicional adicionado à conta da máquina existente fornece acesso Kerberos.



Este é o resultado da pesquisa direta de DNS após adicionar um CNAME:

```
PS C:\> nslookup cifs
Server:  ok-activedirectory.us-east4-a.c.cv-solution-architect-
lab.internal
Address:  10. xx.0. xx
```

```
Name:    NetApp Volumes-EAST-433D.cvsdemo.local
Address:  10. xxx.0. x
Aliases:  cifs.cvsdemo.local
```

Esta é a consulta SPN resultante após adicionar novos SPNs:

```
PS C:\> setspn /L CVS-EAST-433D
Registered ServicePrincipalNames for CN=CVS-EAST-433D,CN=Computers,DC=cvsdemo,DC=local:
        cifs/cifs.cvsdemo.local
        cifs/cifs
        HOST/cvs-east-433d.cvsdemo.local
        HOST/CVS-EAST-433D
```

Em uma captura de pacotes, podemos ver a solicitação de configuração de sessão usando o SPN vinculado ao CNAME.

```
431 4.156722                                    SMB2     308 Negotiate Protocol Response
432 4.156785                                    SMB2     232 Negotiate Protocol Request
434 4.158108                                    SMB2     374 Negotiate Protocol Response
435 4.160977                                    SMB2    1978 Session Setup Request
437 4.166224                                    SMB2     322 Session Setup Response
438 4.166891                                    SMB2     152 Tree Connect Request Tree: \\cifs\IPC$
439 4.168063                                    SMB2     138 Tree Connect Response
```

```
realm: CVSDEMO.LOCAL
sname
   name-type: kRB5-NT-SRV-INST (2)
   sname-string: 2 items
      SNameString: cifs
      SNameString: cifs
enc-part
   etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

Dialetos de autenticação SMB

O Google Cloud NetApp Volumes oferece suporte ao seguinte "dialetos" para autenticação SMB:

- LM
- NTLM
- NTLMv2
- Kerberos

A autenticação Kerberos para acesso ao compartilhamento SMB é o nível de autenticação mais seguro que você pode usar. Com a criptografia AES e SMB habilitada, o nível de segurança aumenta ainda mais.

O Google Cloud NetApp Volumes também oferece suporte à compatibilidade com versões anteriores para autenticação LM e NTLM. Quando o Kerberos está configurado incorretamente (como ao criar aliases SMB), o acesso compartilhado recorre a métodos de autenticação mais fracos (como NTLMv2). Como esses mecanismos são menos seguros, eles são desabilitados em alguns ambientes do Active Directory. Se métodos de autenticação mais fracos estiverem desabilitados e o Kerberos não estiver configurado corretamente, o acesso compartilhado falhará porque não há um método de autenticação válido para recorrer.

Para obter informações sobre como configurar/visualizar seus níveis de autenticação suportados no Active Directory, consulte "Segurança de rede: nível de autenticação do LAN Manager" .

Permissões de NTFS/Arquivo

Permissões NTFS são as permissões aplicadas a arquivos e pastas em sistemas de arquivos que aderem à lógica NTFS. Você pode aplicar permissões NTFS em `Basic` ou `Advanced` e pode ser configurado para `Allow` ou `Deny` para controle de acesso.

As permissões básicas incluem o seguinte:

- Controle total
- Modificar
- Ler e Executar
- Ler
- Escrever

Quando você define permissões para um usuário ou grupo, conhecido como ACE, ele reside em uma ACL. As permissões NTFS usam os mesmos princípios básicos de leitura/gravação/execução dos bits do modo UNIX, mas também podem se estender a controles de acesso mais granulares e estendidos (também conhecidos como Permissões Especiais), como Assumir Propriedade, Criar Pastas/Acrescentar Dados, Gravar Atributos e muito mais.

Os bits do modo UNIX padrão não fornecem o mesmo nível de granularidade que as permissões NTFS (como poder definir permissões para objetos de usuários e grupos individuais em uma ACL ou definir atributos estendidos). No entanto, as ACLs do NFSv4.1 fornecem a mesma funcionalidade que as ACLs do NTFS.

As permissões NTFS são mais específicas do que as permissões de compartilhamento e podem ser usadas em conjunto com as permissões de compartilhamento. Com estruturas de permissão NTFS, a mais restritiva se aplica. Dessa forma, negações explícitas a um usuário ou grupo substituem até mesmo o Controle Total ao definir direitos de acesso.

As permissões NTFS são controladas por clientes SMB do Windows.

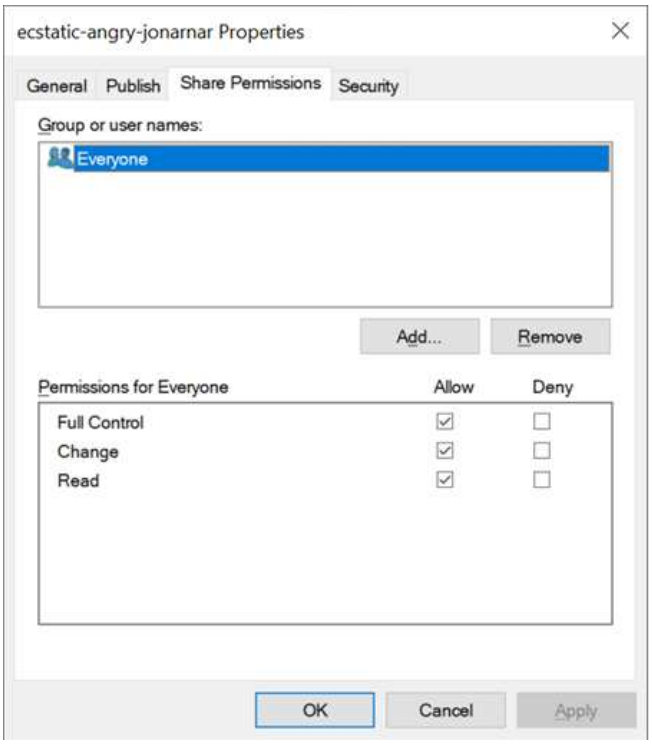
Permissões de compartilhamento

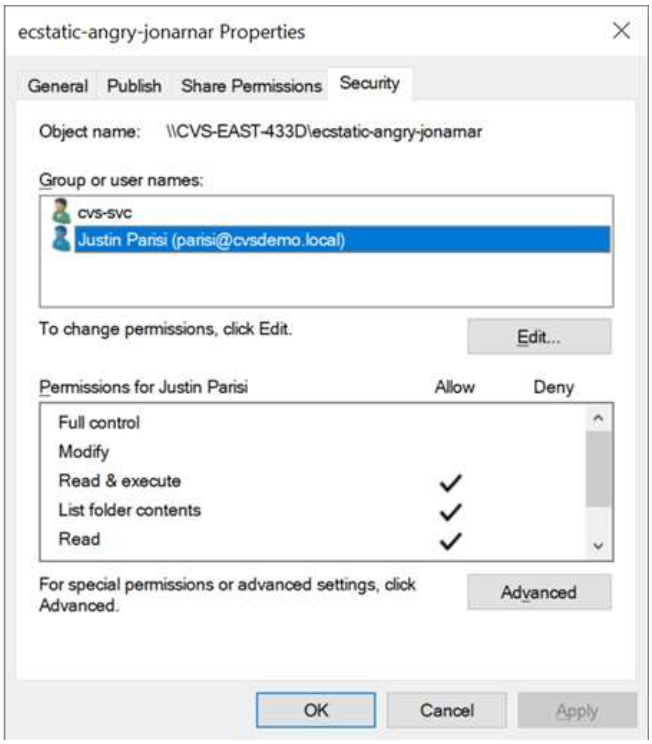
As permissões de compartilhamento são mais gerais do que as permissões NTFS (somente Leitura/Alteração/Controle Total) e controlam a entrada inicial em um compartilhamento SMB, semelhante ao funcionamento das regras de política de exportação NFS.

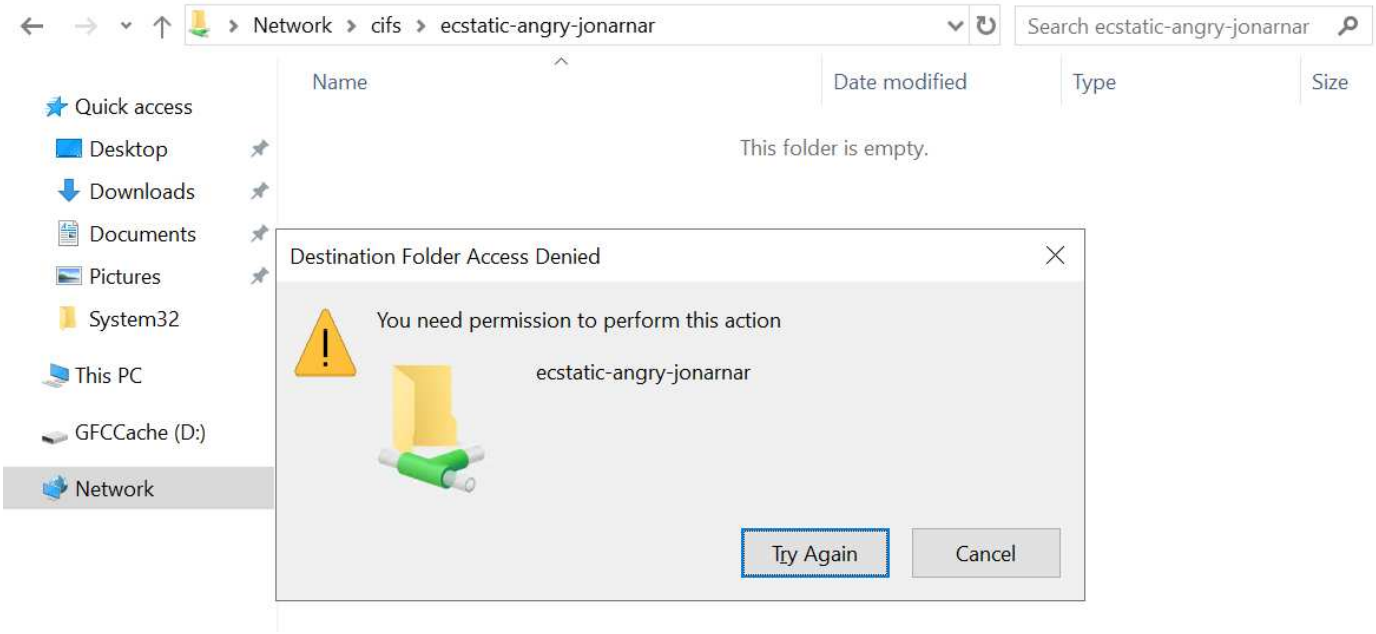
Embora as regras de política de exportação do NFS controlem o acesso por meio de informações baseadas em host, como endereços IP ou nomes de host, as permissões de compartilhamento SMB podem controlar o acesso usando ACEs de usuário e grupo em uma ACL de compartilhamento. Você pode definir ACLs de compartilhamento no cliente Windows ou na interface de gerenciamento do Google Cloud NetApp Volumes .

Por padrão, as ACLs de compartilhamento e as ACLs de volume inicial incluem Todos com Controle Total. As ACLs do arquivo devem ser alteradas, mas as permissões de compartilhamento são substituídas pelas permissões de arquivo em objetos no compartilhamento.

Por exemplo, se um usuário tiver permissão somente para acesso de Leitura à ACL do arquivo de volume do Google Cloud NetApp Volumes , ele terá o acesso negado para criar arquivos e pastas, mesmo que a ACL de compartilhamento esteja definida como Todos com Controle Total, conforme mostrado na figura a seguir.







Para melhores resultados de segurança, faça o seguinte:

- Remova Todos das ACLs de compartilhamento e arquivo e, em vez disso, defina o acesso de compartilhamento para usuários ou grupos.
- Use grupos para controle de acesso em vez de usuários individuais para facilitar o gerenciamento e remover/adicionar usuários mais rapidamente para compartilhar ACLs por meio do gerenciamento de grupos.
- Permita acesso de compartilhamento menos restritivo e mais geral aos ACEs nas permissões de compartilhamento e bloqueie o acesso a usuários e grupos com permissões de arquivo para um controle de acesso mais granular.
- Evite o uso geral de ACLs de negação explícitas, porque elas substituem ACLs de permissão. Limite o uso

de ACLs de negação explícita para usuários ou grupos que precisam ter o acesso a um sistema de arquivos restringido rapidamente.

- Certifique-se de prestar atenção ao "Herança ACL" configurações ao modificar permissões; definir o sinalizador de herança no nível superior de um diretório ou volume com altas contagens de arquivos significa que cada arquivo abaixo desse diretório ou volume herdou permissões adicionadas a ele, o que pode criar comportamento indesejado, como acesso/negação não intencional e longa rotatividade de modificação de permissão à medida que cada arquivo é ajustado.

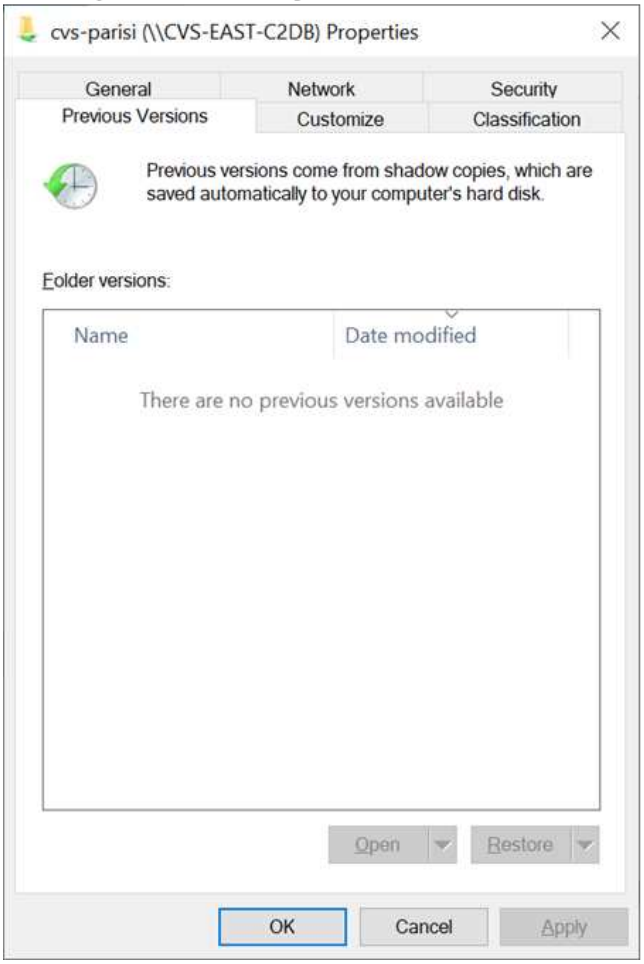
Recursos de segurança de compartilhamento de PMEs

Ao criar um volume com acesso SMB pela primeira vez no Google Cloud NetApp Volumes, você verá uma série de opções para proteger esse volume.

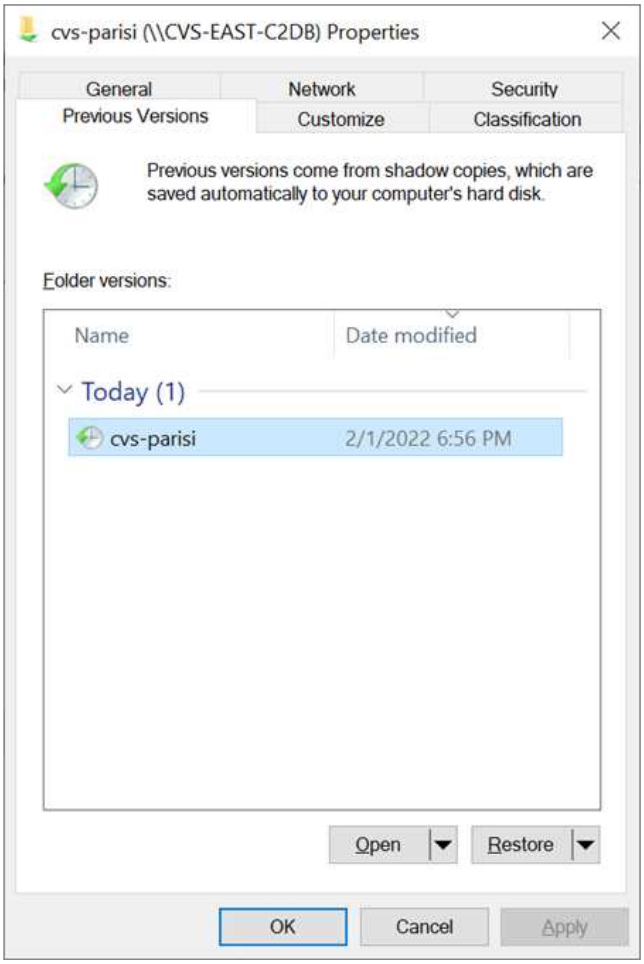
Algumas dessas opções dependem do nível do Google Cloud NetApp Volumes (desempenho ou software) e as opções incluem:

- **Tornar o diretório de snapshot visível (disponível para NetApp Volumes-Performance e NetApp Volumes-SW).** Esta opção controla se os clientes SMB podem ou não acessar o diretório Snapshot em um compartilhamento SMB(`\\server\share\~snapshot` e/ou guia Versões Anteriores). A configuração padrão é Não Verificado, o que significa que o volume é ocultado por padrão e não permite o acesso ao `~snapshot` diretório e nenhuma cópia do Snapshot aparece na guia Versões anteriores do volume.

Snapshot directory visible: Unchecked



Snapshot directory visible: Checked



Ocultar cópias de Snapshot dos usuários finais pode ser desejado por motivos de segurança, desempenho

(ocultar essas pastas de verificações de antivírus) ou preferência. Os Snapshots do Google Cloud NetApp Volumes são somente leitura, portanto, mesmo que estejam visíveis, os usuários finais não podem excluir ou modificar arquivos no diretório Snapshot. As permissões de arquivo nos arquivos ou pastas no momento em que a cópia do Snapshot foi feita se aplicam. Se as permissões de um arquivo ou pasta forem alteradas entre cópias do Snapshot, as alterações também se aplicarão aos arquivos ou pastas no diretório do Snapshot. Usuários e grupos podem obter acesso a esses arquivos ou pastas com base em permissões. Embora não seja possível excluir ou modificar arquivos no diretório Snapshot, é possível copiar arquivos ou pastas do diretório Snapshot.

- **Habilite a criptografia SMB (disponível para NetApp Volumes-Performance e NetApp Volumes-SW).** A criptografia SMB é desabilitada no compartilhamento SMB por padrão (desmarcada). Marcar a caixa ativa a criptografia SMB, o que significa que o tráfego entre o cliente e o servidor SMB é criptografado em trânsito com os mais altos níveis de criptografia suportados negociados. O Google Cloud NetApp Volumes oferece suporte à criptografia de até AES-256 para PMEs. Habilitar a criptografia SMB acarreta uma perda de desempenho que pode ou não ser perceptível para seus clientes SMB, em torno de 10-20%. A NetApp recomenda fortemente testes para verificar se essa perda de desempenho é aceitável.
- **Ocultar compartilhamento SMB (disponível para NetApp Volumes-Performance e NetApp Volumes-SW).** Definir esta opção oculta o caminho do compartilhamento SMB da navegação normal. Isso significa que os clientes que não conhecem o caminho do compartilhamento não podem ver os compartilhamentos ao acessar o caminho UNC padrão (como `\\NetApp Volumes-SMB`). Quando a caixa de seleção é marcada, somente clientes que conhecem explicitamente o caminho do compartilhamento SMB ou têm o caminho do compartilhamento definido por um Objeto de Política de Grupo podem acessá-lo (segurança por ofuscação).
- **Habilite a enumeração baseada em acesso (ABE) (somente NetApp Volumes-SW).** Isso é semelhante a ocultar o compartilhamento SMB, exceto que os compartilhamentos ou arquivos são ocultados somente de usuários ou grupos que não têm permissões para acessar os objetos. Por exemplo, se o usuário do Windows `joe` não é permitido pelo menos acesso de leitura através das permissões, então o usuário do Windows `joe` não é possível ver o compartilhamento SMB ou os arquivos. Isso é desabilitado por padrão, mas você pode habilitá-lo marcando a caixa de seleção. Para obter mais informações sobre o ABE, consulte o artigo da Base de conhecimento da NetApp "Como funciona a Enumeração Baseada em Acesso (ABE)?"
- **Habilite o suporte de compartilhamento continuamente disponível (CA) (somente NetApp Volumes-Performance).** "Ações SMB continuamente disponíveis" fornece uma maneira de minimizar interrupções de aplicativos durante eventos de failover replicando estados de bloqueio entre nós no sistema de back-end do Google Cloud NetApp Volumes . Este não é um recurso de segurança, mas oferece melhor resiliência geral. Atualmente, apenas aplicativos SQL Server e FSLogix são suportados para essa funcionalidade.

Compartilhamentos ocultos padrão

Quando um servidor SMB é criado no Google Cloud NetApp Volumes, há "compartilhamentos administrativos ocultos" (usando a convenção de nomenclatura $) que são criados além do compartilhamento SMB do volume de dados. Isso inclui C$ (acesso ao namespace) e IPC$ (compartilhamento de pipes nomeados para comunicação entre programas, como chamadas de procedimento remoto (RPC) usadas para acesso ao Microsoft Management Console (MMC)).

O compartilhamento IPC$ não contém ACLs de compartilhamento e não pode ser modificado - é usado estritamente para chamadas RPC e "O Windows não permite acesso anônimo a esses compartilhamentos por padrão" .

O compartilhamento C$ permite acesso de BUILTIN/Administradores por padrão, mas a automação do Google Cloud NetApp Volumes remove a ACL do compartilhamento e não permite acesso a ninguém porque o acesso ao compartilhamento C$ permite visibilidade de todos os volumes montados nos sistemas de arquivos do

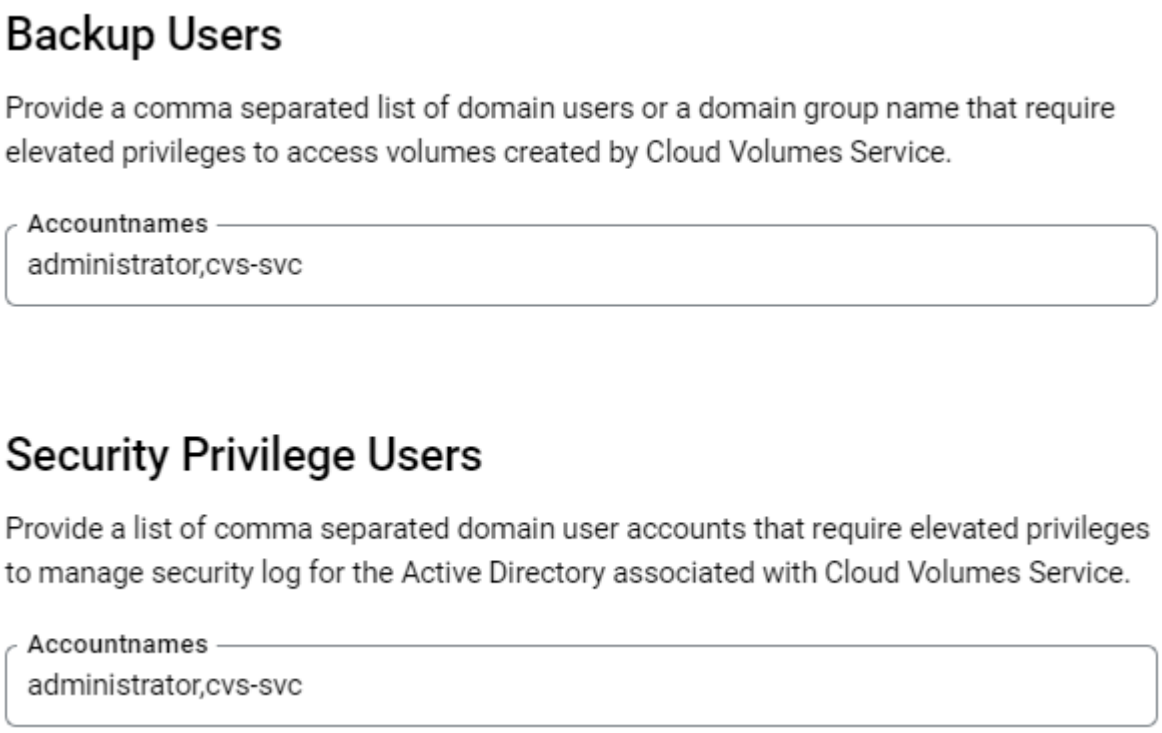
Google Cloud NetApp Volumes . Como resultado, as tentativas de navegar para `\\SERVER\C$` falhar.

Contas com direitos de administrador/backup locais/INCLUÍDOS

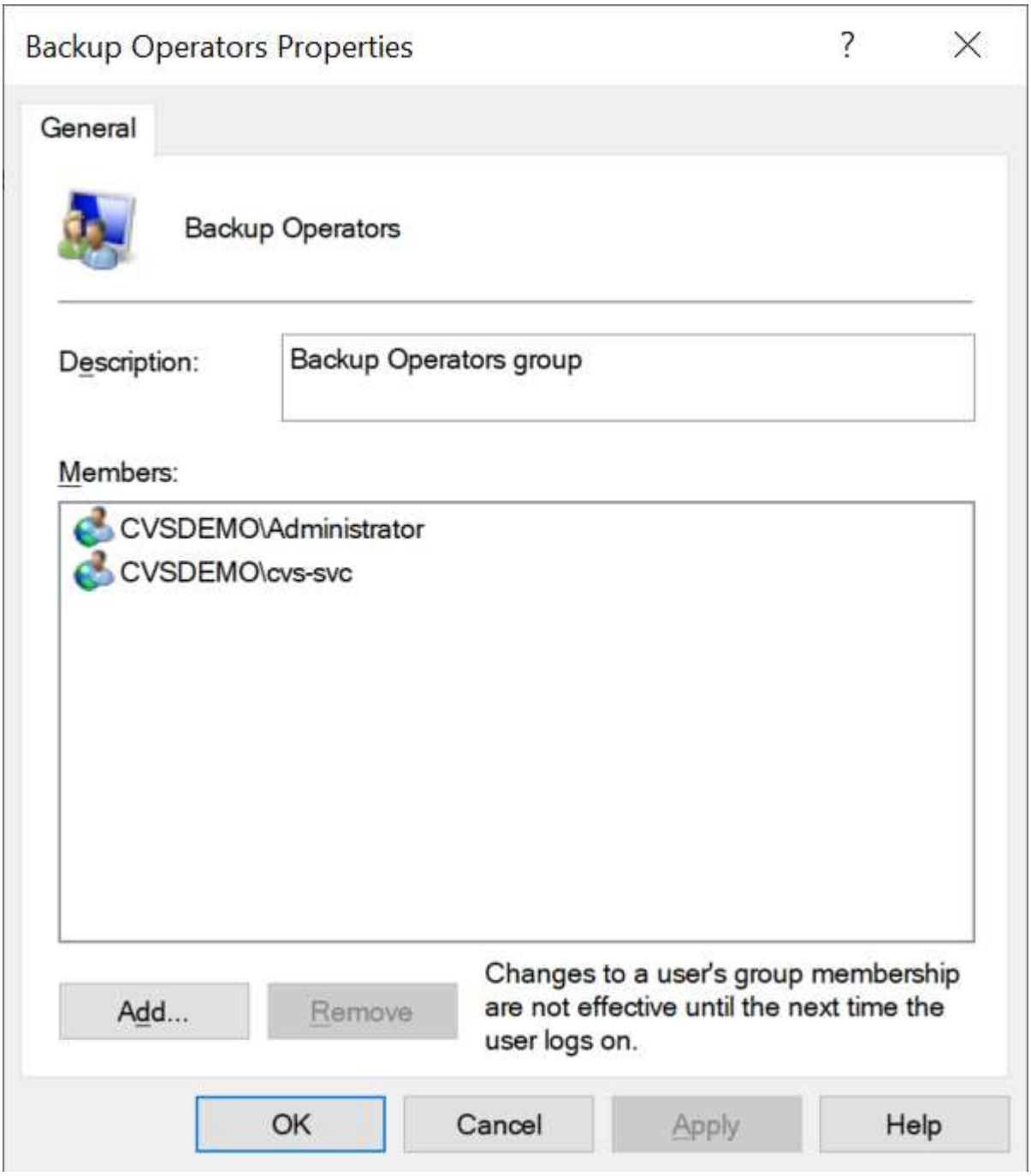
Os servidores SMB do Google Cloud NetApp Volumes mantêm funcionalidade semelhante aos servidores SMB comuns do Windows, pois há grupos locais (como BUILTIN\Administradores) que aplicam direitos de acesso para selecionar usuários e grupos de domínio.

Quando você especifica um usuário a ser adicionado aos Usuários de backup, o usuário é adicionado ao grupo BUILTIN\Operadores de backup na instância do Google Cloud NetApp Volumes que usa essa conexão do Active Directory, que então obtém o "SeBackupPrivilege e SeRestorePrivilege" .

Quando você adiciona um usuário aos Usuários com Privilégio de Segurança, o usuário recebe o SeSecurityPrivilege, que é útil em alguns casos de uso de aplicativos, como "SQL Server em compartilhamentos SMB" .



Você pode visualizar as associações de grupos locais do Google Cloud NetApp Volumes por meio do MMC com os privilégios adequados. A figura a seguir mostra os usuários que foram adicionados usando o console do Google Cloud NetApp Volumes .

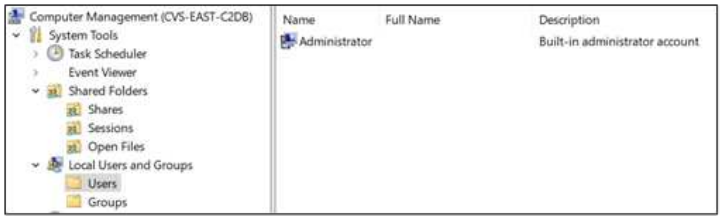


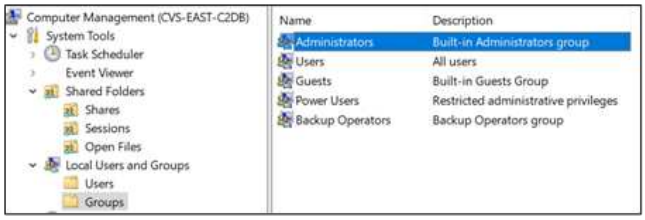
A tabela a seguir mostra a lista de grupos BUILTIN padrão e quais usuários/grupos são adicionados por padrão.

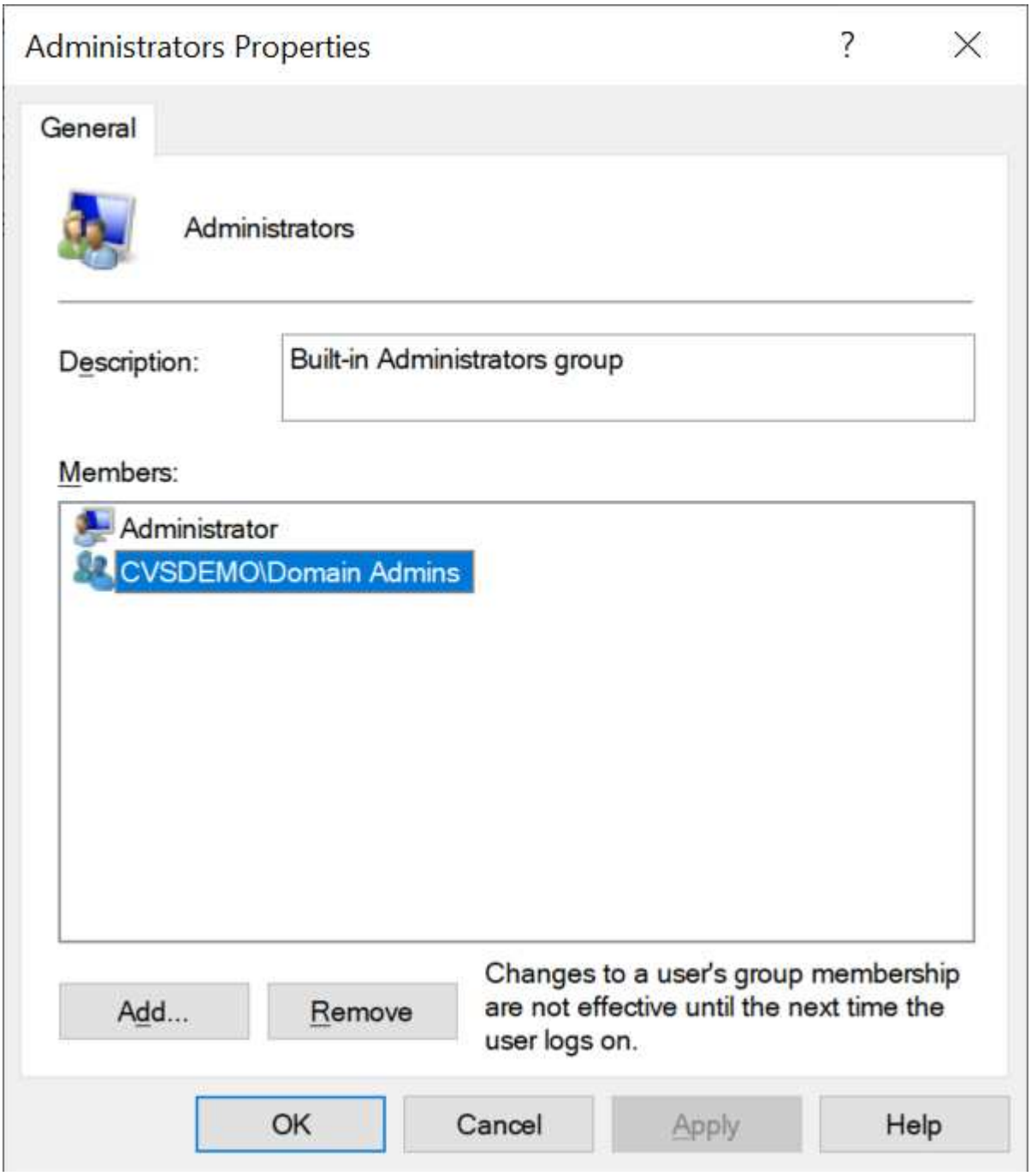
Grupo local/BUILTIN	Membros padrão
BUILTIN\Administradores*	DOMÍNIO\Administradores de Domínio
BUILTIN\Operadores de backup*	Nenhum
CONSTRUÇÃO\Convidados	DOMÍNIO\Convidados do Domínio
BUILTIN\Usuários avançados	Nenhum
BUILTIN\Usuários do Domínio	DOMÍNIO\Usuários do Domínio

*Associação de grupo controlada na configuração de conexão do Google Cloud NetApp Volumes Active Directory.

Você pode visualizar usuários e grupos locais (e membros do grupo) na janela do MMC, mas não pode adicionar ou excluir objetos ou alterar associações de grupo neste console. Por padrão, somente o grupo Administradores de domínio e Administrador são adicionados ao grupo BUILTIN\Administradores no Google Cloud NetApp Volumes. Atualmente, você não pode modificar isso.







Acesso MMC/Gerenciamento de Computador

O acesso SMB no Google Cloud NetApp Volumes fornece conectividade ao MMC de gerenciamento do computador, o que permite que você visualize compartilhamentos, gerencie ACLs de compartilhamento, bem como visualize/gerencie sessões SMB e abra arquivos.

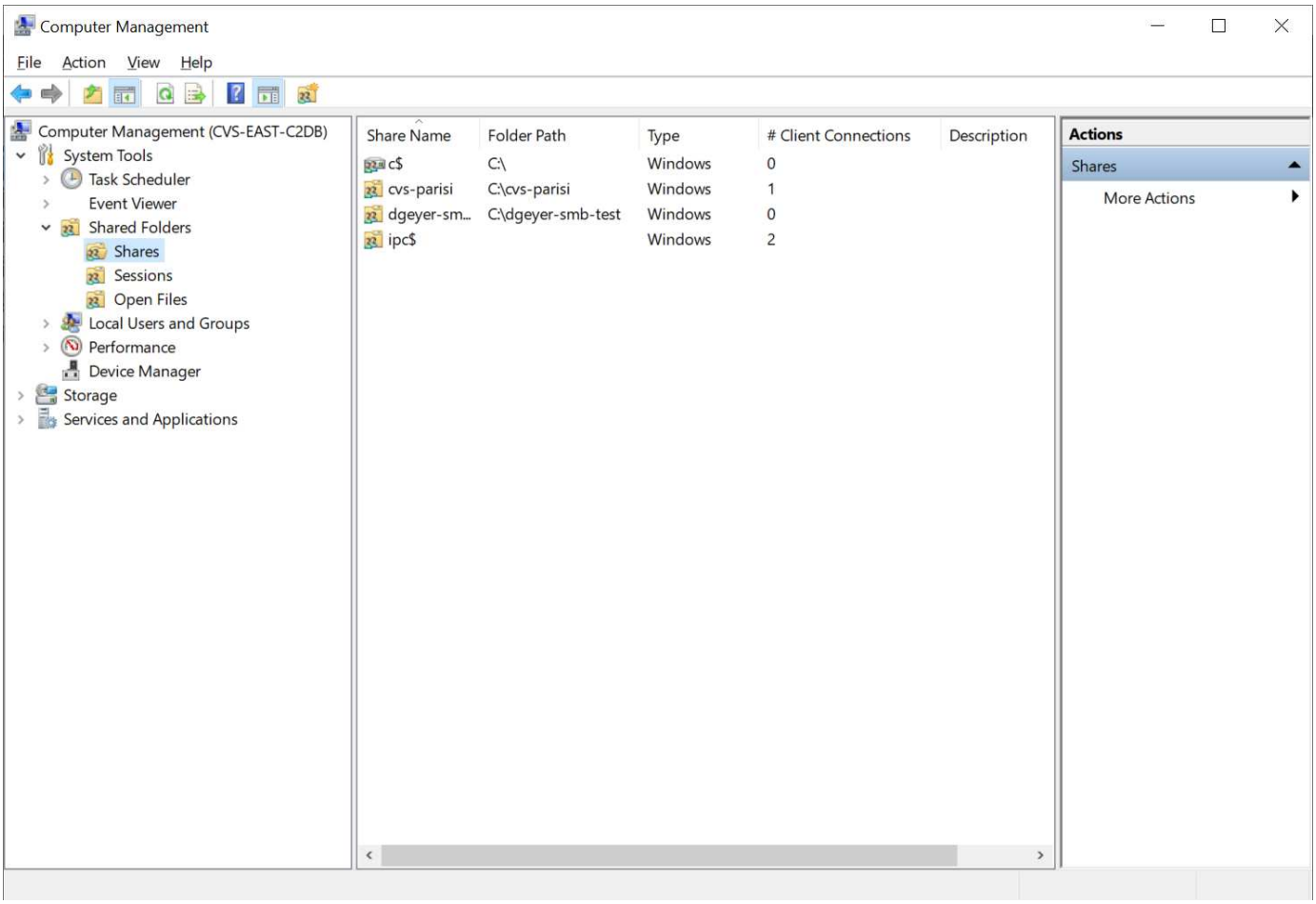
Para usar o MMC para visualizar compartilhamentos e sessões SMB no Google Cloud NetApp Volumes, o usuário conectado no momento deve ser um administrador de domínio. Outros usuários têm permissão para visualizar ou gerenciar o servidor SMB do MMC e recebem uma caixa de diálogo Você não tem permissões ao tentar visualizar compartilhamentos ou sessões na instância SMB do Google Cloud NetApp Volumes .

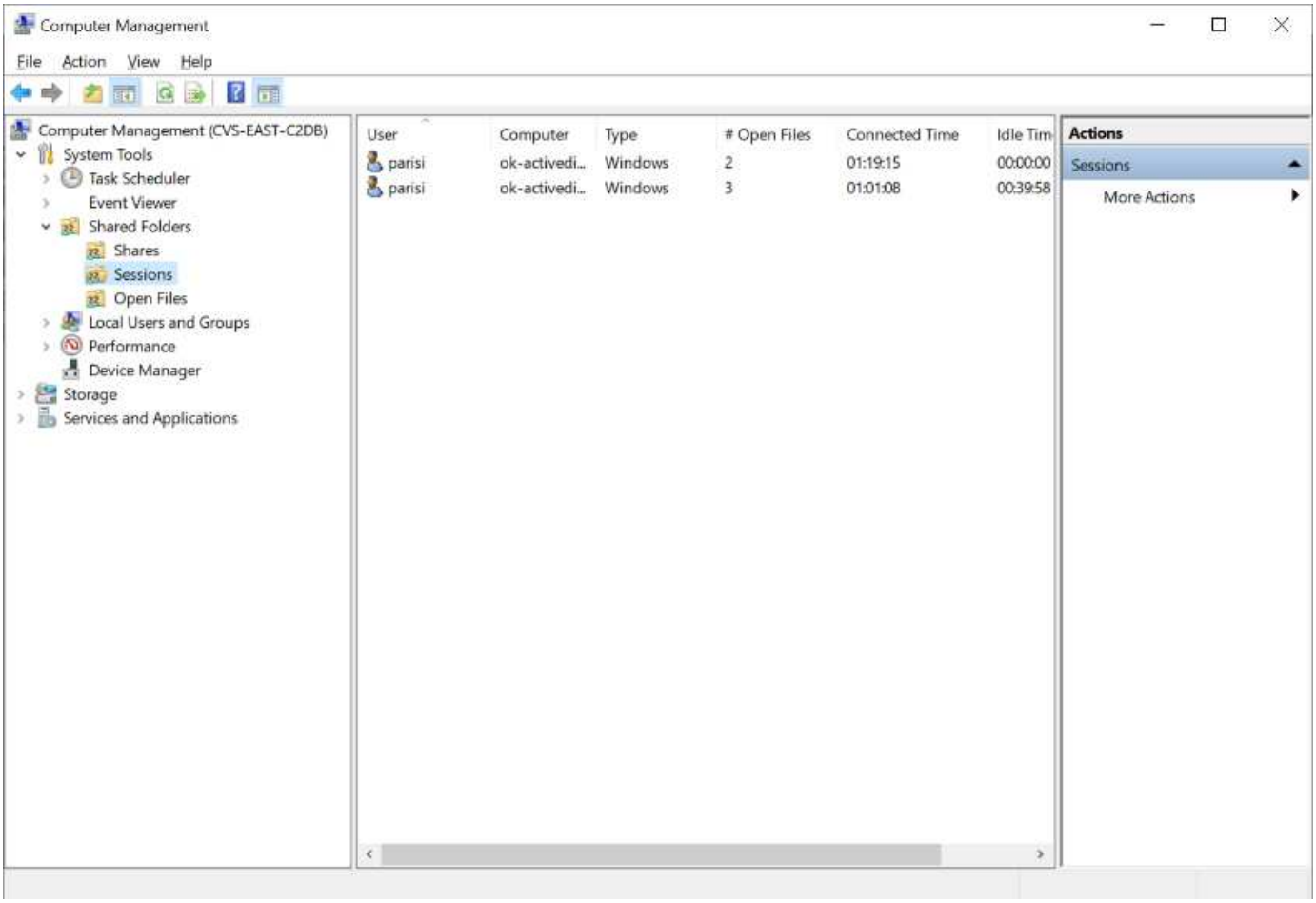
Para se conectar ao servidor SMB, abra o Gerenciamento do Computador, clique com o botão direito do mouse em Gerenciamento do Computador e selecione Conectar a Outro Computador. Isso abre a caixa de diálogo Selecionar computador, onde você pode inserir o nome do servidor SMB (encontrado nas informações

de volume do Google Cloud NetApp Volumes).

Ao visualizar compartilhamentos SMB com as permissões adequadas, você verá todos os compartilhamentos disponíveis na instância do Google Cloud NetApp Volumes que compartilham a conexão do Active Directory. Para controlar esse comportamento, defina a opção Ocultar compartilhamentos SMB na instância de volume do Google Cloud NetApp Volumes .

Lembre-se de que apenas uma conexão do Active Directory é permitida por região.





A tabela a seguir mostra uma lista de funcionalidades suportadas/não suportadas para o MMC.

Funções suportadas	Funções não suportadas
• Ver compartilhamentos • Ver sessões SMB ativas • Ver arquivos abertos • Ver usuários e grupos locais • Ver associações de grupos locais • Enumerar a lista de sessões, arquivos e conexões de árvore no sistema • Feche os arquivos abertos no sistema • Fechar sessões abertas • Criar/gerenciar compartilhamentos	• Criação de novos usuários/grupos locais • Gerenciando/visualizando usuários/grupos locais existentes • Ver eventos ou registros de desempenho • Gerenciando armazenamento • Gerenciando serviços e aplicativos

Informações de segurança do servidor SMB

O servidor SMB no Google Cloud NetApp Volumes usa uma série de opções que definem políticas de segurança para conexões SMB, incluindo coisas como distorção do relógio Kerberos, idade do tíquete, criptografia e muito mais.

A tabela a seguir contém uma lista dessas opções, o que elas fazem, as configurações padrão e se elas

podem ser modificadas com o Google Cloud NetApp Volumes. Algumas opções não se aplicam ao Google Cloud NetApp Volumes.

Opção de segurança	O que ele faz	Valor padrão	Pode mudar?
Desvio máximo do relógio Kerberos (minutos)	Disparidade máxima de tempo entre o Google Cloud NetApp Volumes e os controladores de domínio. Se o desvio de tempo exceder 5 minutos, a autenticação Kerberos falhará. Isso é definido como o valor padrão do Active Directory.	5	Não
Tempo de vida do tíquete Kerberos (horas)	Tempo máximo que um tíquete Kerberos permanece válido antes de precisar ser renovado. Caso não haja renovação antes das 10 horas, será necessário adquirir um novo ingresso. O Google Cloud NetApp Volumes executa essas renovações automaticamente. 10 horas é o valor padrão do Active Directory.	10	Não
Renovação máxima do tíquete Kerberos (dias)	Número máximo de dias que um tíquete Kerberos pode ser renovado antes que uma nova solicitação de autorização seja necessária. O Google Cloud NetApp Volumes renova automaticamente os tíquetes para conexões SMB. Sete dias é o valor padrão do Active Directory.	7	Não
Tempo limite de conexão do Kerberos KDC (segs)	O número de segundos antes que o tempo limite da conexão KDC seja atingido.	3	Não
Exigir assinatura para tráfego SMB de entrada	Configuração para exigir assinatura para tráfego SMB. Se definido como verdadeiro, os clientes que não oferecem suporte à assinatura falham na conectividade.	Falso	

Opção de segurança	O que ele faz	Valor padrão	Pode mudar?
Exigir complexidade de senha para contas de usuários locais	Usado para senhas de usuários SMB locais. O Google Cloud NetApp Volumes não oferece suporte à criação de usuários locais, portanto, esta opção não se aplica ao Google Cloud NetApp Volumes.	Verdadeiro	Não
Use start_tls para conexões LDAP do Active Directory	Usado para habilitar o início de conexões TLS para o LDAP do Active Directory. O Google Cloud NetApp Volumes não oferece suporte para essa ativação no momento.	Falso	Não
A criptografia AES-128 e AES-256 para Kerberos está habilitada?	Isso controla se a criptografia AES é usada para conexões do Active Directory e é controlada com a opção Habilitar criptografia AES para autenticação do Active Directory ao criar/modificar a conexão do Active Directory.	Falso	Sim
Nível de compatibilidade LM	Nível de dialetos de autenticação suportados para conexões do Active Directory. Veja a seção "Dialetos de autenticação SMB " para mais informações.	ntlmv2-krb	Não
Exigir criptografia SMB para tráfego CIFS de entrada	Requer criptografia SMB para todos os compartilhamentos. Isso não é usado pelo Google Cloud NetApp Volumes; em vez disso, defina a criptografia por volume (consulte a seção "Recursos de segurança de compartilhamento de PMEs ").	Falso	Não

Opção de segurança	O que ele faz	Valor padrão	Pode mudar?
Segurança da sessão do cliente	Define assinatura e/ou selagem para comunicação LDAP. Isso não está definido atualmente no Google Cloud NetApp Volumes, mas pode ser necessário em versões futuras para resolver o problema. A correção para problemas de autenticação LDAP devido ao patch do Windows é abordada na seção"Ligação de canal LDAP." .	Nenhum	Não
Habilitação SMB2 para conexões DC	Usa SMB2 para conexões DC. Ativado por padrão.	Padrão do sistema	Não
Busca de referência LDAP	Ao usar vários servidores LDAP, a busca de referência permite que o cliente consulte outros servidores LDAP na lista quando uma entrada não for encontrada no primeiro servidor. Atualmente, isso não é suportado pelo Google Cloud NetApp Volumes.	Falso	Não
Use LDAPS para conexões seguras do Active Directory	Permite o uso de LDAP sobre SSL. Atualmente não é compatível com o Google Cloud NetApp Volumes.	Falso	Não
A criptografia é necessária para conexão DC	Requer criptografia para conexões DC bem-sucedidas. Desativado por padrão no Google Cloud NetApp Volumes.	Falso	Não

Protocolo duplo/multiprotocolo

O Google Cloud NetApp Volumes oferece a capacidade de compartilhar os mesmos conjuntos de dados com clientes SMB e NFS, mantendo as permissões de acesso adequadas ("protocolo duplo"). Isso é feito coordenando o mapeamento de identidades entre os protocolos e usando um servidor LDAP de back-end centralizado para fornecer as identidades UNIX ao Google Cloud NetApp Volumes. Você pode usar o Active Directory do Windows para fornecer usuários do Windows e UNIX, facilitando o uso.

Controle de acesso

- **Compartilhe controles de acesso.** Determine quais clientes e/ou usuários e grupos podem acessar um compartilhamento NAS. Para o NFS, as políticas e regras de exportação controlam o acesso do cliente às exportações. As exportações do NFS são gerenciadas a partir da instância do Google Cloud NetApp Volumes . O SMB usa compartilhamentos CIFS/SMB e ACLs de compartilhamento para fornecer controle mais granular no nível de usuário e grupo. Você só pode configurar ACLs em nível de compartilhamento de clientes SMB usando https://library.netapp.com/ecmdocs/ECMP1401220/html/GUID-C1772CDF-8AEE-422B-AB87-CFCB7E50FF94.html [MMC/Gerenciamento de Computadores^] com uma conta que tenha direitos de administrador na instância do Google Cloud NetApp Volumes (consulte a seção "Contas com direitos de administrador/backup locais/INTEGRADOS.").
- **Controles de acesso a arquivos.** Controle as permissões no nível de arquivo ou pasta e elas são sempre gerenciadas pelo cliente NAS. Os clientes NFS podem usar bits de modo tradicional (rwx) ou ACLs NFSv4. Clientes SMB aproveitam permissões NTFS.

O controle de acesso para volumes que fornecem dados para NFS e SMB depende do protocolo em uso. Para obter informações sobre permissões com protocolo duplo, consulte a seção "Modelo de permissão ."

Mapeamento de usuários

Quando um cliente acessa um volume, o Google Cloud NetApp Volumes tenta mapear o usuário de entrada para um usuário válido na direção oposta. Isso é necessário para que o acesso adequado seja determinado entre os protocolos e para garantir que o usuário que solicita acesso é realmente quem ele afirma ser.

Por exemplo, se um usuário do Windows chamado `joe` tenta acessar um volume com permissões UNIX por meio de SMB, então o Google Cloud NetApp Volumes executa uma pesquisa para encontrar um usuário UNIX correspondente chamado `joe` . Se existir, os arquivos que são gravados em um compartilhamento SMB como usuário do Windows `joe` aparece como usuário UNIX `joe` de clientes NFS.

Alternativamente, se um usuário UNIX chamado `joe` tenta acessar um volume do Google Cloud NetApp Volumes com permissões do Windows, então o usuário UNIX deve ser capaz de mapear para um usuário válido do Windows. Caso contrário, o acesso ao volume será negado.

Atualmente, apenas o Active Directory é compatível com o gerenciamento de identidades UNIX externas via LDAP. Para obter mais informações sobre como configurar o acesso a esse serviço, consulte "Criando uma conexão AD".

Modelo de permissão

Ao usar configurações de protocolo duplo, o Google Cloud NetApp Volumes usa estilos de segurança para volumes para determinar o tipo de ACL. Esses estilos de segurança são definidos com base no protocolo NAS especificado ou, no caso de protocolo duplo, é uma escolha feita no momento da criação do volume do Google Cloud NetApp Volumes .

- Se você estiver usando apenas NFS, os volumes do Google Cloud NetApp Volumes usarão permissões UNIX.
- Se você estiver usando apenas SMB, os volumes do Google Cloud NetApp Volumes usarão permissões NTFS.

Se estiver criando um volume de protocolo duplo, você pode escolher o estilo ACL na criação do volume. Esta decisão deve ser tomada com base no gerenciamento de permissões desejado. Se seus usuários gerenciam permissões de clientes Windows/SMB, selecione NTFS. Se seus usuários preferirem usar clientes NFS e chmod/chown, use estilos de segurança UNIX.

Considerações para criar conexões do Active Directory

O Google Cloud NetApp Volumes oferece a capacidade de conectar sua instância do Google Cloud NetApp Volumes a um servidor externo do Active Directory para gerenciamento de identidade para usuários de SMB e UNIX. É necessário criar uma conexão com o Active Directory para usar o SMB no Google Cloud NetApp Volumes.

A configuração para isso fornece diversas opções que exigem alguma consideração por questões de segurança. O servidor externo do Active Directory pode ser uma instância local ou nativa da nuvem. Se você estiver usando um servidor Active Directory local, não exponha o domínio à rede externa (como com uma DMZ ou um endereço IP externo). Em vez disso, use túneis privados seguros ou VPNs, trusts de floresta unidirecionais ou conexões de rede dedicadas às redes locais com "Acesso privado ao Google" . Consulte a documentação do Google Cloud para obter mais informações sobre "melhores práticas usando o Active Directory no Google Cloud" .

> O NetApp Volumes-SW exige que os servidores do Active Directory estejam localizados na mesma região. Se uma conexão DC for tentada no NetApp Volumes-SW para outra região, a tentativa falhará. Ao usar o NetApp Volumes-SW, crie sites do Active Directory que incluam os DCs do Active Directory e especifique sites no Google Cloud NetApp Volumes para evitar tentativas de conexão de DC entre regiões.

Credenciais do Active Directory

Quando o SMB ou o LDAP para NFS está habilitado, o Google Cloud NetApp Volumes interage com os controladores do Active Directory para criar um objeto de conta de máquina a ser usado para autenticação. Isso não é diferente de como um cliente SMB do Windows ingressa em um domínio e requer os mesmos direitos de acesso às Unidades Organizacionais (UOs) no Active Directory.

Em muitos casos, os grupos de segurança não permitem o uso de uma conta de administrador do Windows em servidores externos, como o Google Cloud NetApp Volumes. Em alguns casos, o usuário Administrador do Windows é desabilitado completamente como prática recomendada de segurança.

Permissões necessárias para criar contas de máquina SMB

Para adicionar objetos de máquina do Google Cloud NetApp Volumes a um Active Directory, uma conta que tenha direitos administrativos no domínio ou tenha "permissões delegadas para criar e modificar objetos de conta de máquina" para uma UO especificada é necessário. Você pode fazer isso com o Assistente de Delegação de Controle no Active Directory criando uma tarefa personalizada que fornece ao usuário acesso à criação/exclusão de objetos de computador com as seguintes permissões de acesso fornecidas:

- Ler/Escrever
- Criar/Excluir todos os objetos filho
- Ler/Escrever todas as propriedades
- Alterar/Redefinir senha

Isso adiciona automaticamente uma ACL de segurança para o usuário definido na UO no Active Directory e minimiza o acesso ao ambiente do Active Directory. Depois que um usuário for delegado, esse nome de usuário e senha podem ser fornecidos como Credenciais do Active Directory nesta janela.

> O nome de usuário e a senha passados ao domínio do Active Directory utilizam a criptografia Kerberos durante a consulta e a criação do objeto de conta da máquina para maior segurança.

Detalhes de conexão do Active Directory

Os "Detalhes da conexão do Active Directory" fornecem orientações para administradores indicarem informações específicas do esquema do Active Directory para o posicionamento de contas de máquina, como as seguintes:

- **Tipo de conexão do Active Directory.** Usado para especificar se a conexão do Active Directory em uma região é usada para volumes do tipo de serviço Google Cloud NetApp Volumes ou NetApp Volumes-Performance. Se isso for definido incorretamente em uma conexão existente, ele poderá não funcionar corretamente quando usado ou editado.
- **Domínio.** O nome de domínio do Active Directory.
- **Site.** Limita os servidores Active Directory a um site específico para segurança e desempenho "considerações". Isso é necessário quando vários servidores Active Directory abrangem regiões porque o Google Cloud NetApp Volumes atualmente não oferece suporte para permitir solicitações de autenticação Active Directory para servidores Active Directory em uma região diferente da instância do Google Cloud NetApp Volumes. (Por exemplo, o controlador de domínio Active Directory está em uma região que apenas o NetApp Volumes-Performance oferece suporte, mas você deseja um compartilhamento SMB em uma instância NetApp Volumes-SW.)
- **Servidores DNS.** Servidores DNS para usar em pesquisas de nomes.
- **Nome NetBIOS (opcional).** Se desejar, o nome NetBIOS do servidor. Isso é usado quando novas contas de máquina são criadas usando a conexão do Active Directory. Por exemplo, se o nome NetBIOS estiver definido como NetApp Volumes-EAST, os nomes das contas da máquina serão NetApp Volumes-EAST-{1234}. Veja a seção"Como o Google Cloud NetApp Volumes aparece no Active Directory" para maiores informações.
- **Unidade Organizacional (UO).** A UO específica para criar a conta de computador. Isso é útil se você estiver delegando o controle de contas de máquina a um usuário em uma UO específica.
- **Criptografia AES.** Você também pode marcar ou desmarcar a caixa de seleção Habilitar criptografia AES para autenticação do AD. Habilitar a criptografia AES para autenticação do Active Directory fornece segurança extra para a comunicação do Google Cloud NetApp Volumes com o Active Directory durante pesquisas de usuários e grupos. Antes de habilitar esta opção, verifique com o administrador do seu domínio para confirmar se os controladores de domínio do Active Directory suportam autenticação AES.

> Por padrão, a maioria dos servidores Windows não desabilita cifras mais fracas (como DES ou RC4-HMAC), mas se você optar por desabilitar cifras mais fracas, confirme se a conexão do Google Cloud NetApp Volumes Active Directory foi configurada para habilitar o AES. Caso contrário, ocorrerão falhas de autenticação. Habilitar a criptografia AES não desabilita cifras mais fracas, mas adiciona suporte para cifras AES à conta da máquina SMB do Google Cloud NetApp Volumes .

Detalhes do reino Kerberos

Esta opção não se aplica a servidores SMB. Em vez disso, ele é usado ao configurar o NFS Kerberos para o sistema Google Cloud NetApp Volumes . Quando esses detalhes são preenchidos, o domínio NFS Kerberos é configurado (semelhante a um arquivo krb5.conf no Linux) e é usado quando o NFS Kerberos é especificado na criação do volume do Google Cloud NetApp Volumes , pois a conexão do Active Directory atua como o Centro de Distribuição NFS Kerberos (KDC).

> Atualmente, KDCs que não sejam Windows não têm suporte para uso com o Google Cloud NetApp Volumes.

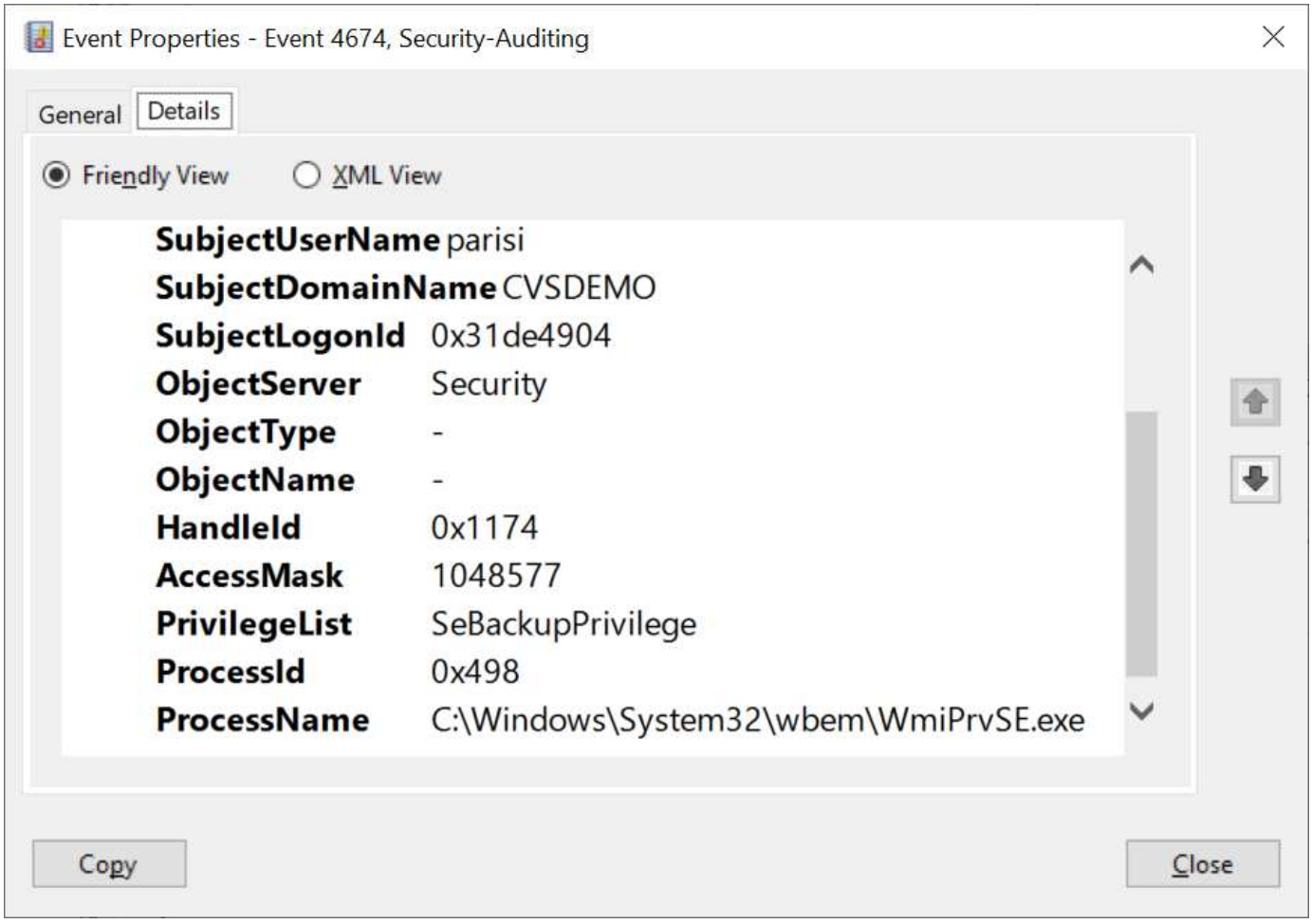
Região

Uma região permite que você especifique o local onde a conexão do Active Directory reside. Esta região deve ser a mesma região que o volume do Google Cloud NetApp Volumes .

- **Usuários NFS locais com LDAP.** Nesta seção, também há uma opção para Permitir usuários NFS locais com LDAP. Esta opção deve ser deixada desmarcada se você quiser estender seu suporte de associação ao grupo de usuários do UNIX além da limitação de 16 grupos do NFS (grupos estendidos). No entanto, o uso de grupos estendidos requer um servidor LDAP configurado para identidades UNIX. Se você não tiver um servidor LDAP, deixe esta opção desmarcada. Se você tiver um servidor LDAP e quiser usar também usuários UNIX locais (como root), selecione esta opção.

Usuários de backup

Esta opção permite que você especifique usuários do Windows que tenham permissões de backup para o volume do Google Cloud NetApp Volumes . Privilégios de backup (SeBackupPrivilege) são necessários para que alguns aplicativos façam backup e restaurem dados adequadamente em volumes NAS. Este usuário tem um alto nível de acesso aos dados no volume, então você deve considerar "permitindo a auditoria do acesso desse usuário" . Após a ativação, os eventos de auditoria são exibidos em Visualizador de Eventos > Logs do Windows > Segurança.



Usuários com privilégios de segurança

Esta opção permite que você especifique usuários do Windows que tenham permissões de modificação de segurança para o volume do Google Cloud NetApp Volumes . Privilégios de segurança (SeSecurityPrivilege) são necessários para alguns aplicativos("como o SQL Server") para definir permissões corretamente durante

a instalação. Este privilégio é necessário para gerenciar o log de segurança. Embora esse privilégio não seja tão poderoso quanto o SeBackupPrivilege, a NetApp recomenda "auditoria de acesso de usuários" com este nível de privilégio, se necessário.

Para obter mais informações, consulte "Privilégios especiais atribuídos ao novo logon" .

Como o Google Cloud NetApp Volumes aparece no Active Directory

O Google Cloud NetApp Volumes aparece no Active Directory como um objeto de conta de máquina normal. As convenções de nomenclatura são as seguintes.

- CIFS/SMB e NFS Kerberos criam objetos de conta de máquina separados.
- O NFS com LDAP habilitado cria uma conta de máquina no Active Directory para vinculações LDAP do Kerberos.
- Volumes de protocolo duplo com LDAP compartilham a conta da máquina CIFS/SMB para LDAP e SMB.
- Contas de máquina CIFS/SMB usam uma convenção de nomenclatura NAME-1234 (ID aleatório de quatro dígitos com hífen anexado ao nome de <10 caracteres) para a conta de máquina. Você pode definir NAME pela configuração do nome NetBIOS na conexão do Active Directory (consulte a seção "Detalhes de conexão do Active Directory ").
- O NFS Kerberos usa NFS-NAME-1234 como convenção de nomenclatura (até 15 caracteres). Se mais de 15 caracteres forem usados, o nome será NFS-TRUNCATED-NAME-1234.
- Instâncias do NetApp Volumes-Performance somente NFS com LDAP habilitado criam uma conta de máquina SMB para vinculação ao servidor LDAP com a mesma convenção de nomenclatura das instâncias CIFS/SMB.
- Quando uma conta de máquina SMB é criada, compartilhamentos administrativos ocultos padrão (consulte a seção"Compartilhamentos ocultos padrão") também são criados (c$, admin$, ipc$), mas esses compartilhamentos não têm ACLs atribuídos e são inacessíveis.
- Os objetos de conta de máquina são colocados em CN=Computadores por padrão, mas você pode especificar uma UO diferente quando necessário. Veja a seção "Permissões necessárias para criar contas de máquina SMB " para obter informações sobre quais direitos de acesso são necessários para adicionar/remover objetos de conta de máquina para o Google Cloud NetApp Volumes.

Quando o Google Cloud NetApp Volumes adiciona a conta da máquina SMB ao Active Directory, os seguintes campos são preenchidos:

- cn (com o nome do servidor SMB especificado)
- dNSHostName (com SMBserver.domain.com)
- msDS-SupportedEncryptionTypes (permite DES_CBC_MD5, RC4_HMAC_MD5 se a criptografia AES não estiver habilitada; se a criptografia AES estiver habilitada, DES_CBC_MD5, RC4_HMAC_MD5, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96 são permitidos para troca de tíquetes Kerberos com a conta da máquina para SMB)
- nome (com o nome do servidor SMB)
- sAMAccountName (com SMBserver$)
- servicePrincipalName (com SPNs host/smbserver.domain.com e host/smbserver para Kerberos)

Se quiser desabilitar tipos de criptografia Kerberos mais fracos (enctype) na conta da máquina, você pode alterar o valor msDS-SupportedEncryptionTypes na conta da máquina para um dos valores na tabela a seguir para permitir somente AES.

Valor msDS-SupportedEncryptionTypes	Enctype habilitado
2	DES_CBC_MD5
4	RC4_HMAC
8	Somente AES128_CTS_HMAC_SHA1_96
16	Somente AES256_CTS_HMAC_SHA1_96
24	AES128_CTS_HMAC_SHA1_96 e AES256_CTS_HMAC_SHA1_96
30	DES_CBC_MD5, RC4_HMAC, AES128_CTS_HMAC_SHA1_96 e AES256_CTS_HMAC_SHA1_96

Para habilitar a criptografia AES para contas de máquinas SMB, clique em Habilitar criptografia AES para autenticação do AD ao criar a conexão do Active Directory.

Para habilitar a criptografia AES para NFS Kerberos, "consulte a documentação do Google Cloud NetApp Volumes".

Outras dependências de serviço de infraestrutura NAS (KDC, LDAP e DNS)

Ao usar o Google Cloud NetApp Volumes para compartilhamentos NAS, pode haver dependências externas necessárias para a funcionalidade adequada. Essas dependências estão em jogo em circunstâncias específicas. A tabela a seguir mostra várias opções de configuração e quais dependências, se houver, são necessárias.

Configuração	Dependências necessárias
Somente NFSv3	Nenhum
Somente NFSv3 Kerberos	Diretório ativo do Windows: * KDC * DNS * LDAP
Somente NFSv4.1	Configuração de mapeamento de ID do cliente (/etc/idmap.conf)
Somente NFSv4.1 Kerberos	• Configuração de mapeamento de ID do cliente (/etc/idmap.conf) • Diretório Ativo do Windows: KDC DNS LDAP
Somente PMEs	Diretório ativo: * KDC * DNS
NAS multiprotocolo (NFS e SMB)	• Configuração de mapeamento de ID do cliente (somente NFSv4.1; /etc/idmap.conf) • Diretório Ativo do Windows: KDC DNS LDAP

Rotação de keytabs do Kerberos/redefinições de senhas para objetos de conta de máquina

Com contas de máquina SMB, o Google Cloud NetApp Volumes agenda redefinições periódicas de senha para a conta de máquina SMB. Essas redefinições de senha ocorrem usando a criptografia Kerberos e operam em um cronograma de cada quarto domingo em um horário aleatório entre 23h e 1h. Essas redefinições de senha alteram as versões da chave Kerberos, giram as keytabs armazenadas no sistema Google Cloud NetApp Volumes e ajudam a manter um maior nível de segurança para servidores SMB em execução no Google Cloud NetApp Volumes. As senhas das contas de máquina são aleatórias e não são

conhecidas pelos administradores.

Para contas de máquina NFS Kerberos, as redefinições de senha ocorrem somente quando um novo keytab é criado/trocado com o KDC. Atualmente, isso não é possível fazer no Google Cloud NetApp Volumes.

Portas de rede para uso com LDAP e Kerberos

Ao usar LDAP e Kerberos, você deve determinar as portas de rede usadas por esses serviços. Você pode encontrar uma lista completa das portas usadas pelo Google Cloud NetApp Volumes no "Documentação do Google Cloud NetApp Volumes sobre considerações de segurança".

LDAP

O Google Cloud NetApp Volumes atua como um cliente LDAP e usa consultas de pesquisa LDAP padrão para pesquisas de usuários e grupos para identidades UNIX. O LDAP é necessário se você pretende usar usuários e grupos fora dos usuários padrão fornecidos pelo Google Cloud NetApp Volumes. O LDAP também é necessário se você planeja usar o NFS Kerberos com entidades de usuário (como user1@domain.com). Atualmente, somente o LDAP usando o Microsoft Active Directory é suportado.

Para usar o Active Directory como um servidor LDAP UNIX, você deve preencher os atributos UNIX necessários nos usuários e grupos que pretende usar para identidades UNIX. O Google Cloud NetApp Volumes usa um modelo de esquema LDAP padrão que consulta atributos com base em "RFC-2307-bis" . Como resultado, a tabela a seguir mostra os atributos mínimos necessários do Active Directory a serem preenchidos para usuários e grupos e para que cada atributo é usado.

Para obter mais informações sobre como configurar atributos LDAP no Active Directory, consulte "Gerenciando acesso de protocolo duplo."

Atributo	O que ele faz
uid*	Especifica o nome do usuário UNIX
Número uid*	Especifica o ID numérico do usuário UNIX
gidNumber*	Especifica o ID numérico do grupo primário do usuário UNIX
objectClass*	Especifica qual tipo de objeto está sendo usado; o Google Cloud NetApp Volumes exige que "usuário" seja incluído na lista de classes de objeto (está incluído na maioria das implantações do Active Directory por padrão).
nome	Informações gerais sobre a conta (nome real, número de telefone e assim por diante — também conhecido como gecos)
Senha de Usuário unix	Não é necessário definir isso; não é usado em pesquisas de identidade do UNIX para autenticação NAS. Definir isso coloca o valor unixUserPassword configurado em texto simples.
diretório inicial unix	Define o caminho para os diretórios pessoais do UNIX quando um usuário se autentica no LDAP de um cliente Linux. Defina isso se quiser usar o LDAP para a funcionalidade de diretório inicial do UNIX.

Atributo	O que ele faz
loginShell	Define o caminho para o shell bash/profile para clientes Linux quando um usuário se autentica no LDAP.

*Indica que o atributo é necessário para a funcionalidade adequada com o Google Cloud NetApp Volumes. Os atributos restantes são somente para uso do lado do cliente.

Atributo	O que ele faz
cn*	Especifica o nome do grupo UNIX. Ao usar o Active Directory para LDAP, isso é definido quando o objeto é criado pela primeira vez, mas pode ser alterado posteriormente. Este nome não pode ser o mesmo de outros objetos. Por exemplo, se o seu usuário UNIX chamado user1 pertencer a um grupo chamado user1 no seu cliente Linux, o Windows não permitirá dois objetos com o mesmo atributo cn. Para contornar isso, renomeie o usuário do Windows para um nome exclusivo (como user1-UNIX); o LDAP no Google Cloud NetApp Volumes usa o atributo uid para nomes de usuário do UNIX.
gidNumber*	Especifica o ID numérico do grupo UNIX.
objectClass*	Especifica qual tipo de objeto está sendo usado; o Google Cloud NetApp Volumes exige que o grupo seja incluído na lista de classes de objeto (esse atributo é incluído na maioria das implantações do Active Directory por padrão).
ID do membro	Especifica quais usuários UNIX são membros do grupo UNIX. Com o Active Directory LDAP no Google Cloud NetApp Volumes, este campo não é necessário. O esquema LDAP do Google Cloud NetApp Volumes usa o campo Membro para associações de grupo.
Membro*	Obrigatório para associações de grupo/grupos UNIX secundários. Este campo é preenchido adicionando usuários do Windows aos grupos do Windows. Entretanto, se os grupos do Windows não tiverem atributos UNIX preenchidos, eles não serão incluídos nas listas de associação de grupos do usuário UNIX. Todos os grupos que precisam estar disponíveis no NFS devem preencher os atributos de grupo UNIX necessários listados nesta tabela.

*Indica que o atributo é necessário para a funcionalidade adequada com o Google Cloud NetApp Volumes. Os atributos restantes são somente para uso do lado do cliente.

Informações de ligação LDAP

Para consultar usuários no LDAP, o Google Cloud NetApp Volumes deve se vincular (fazer login) ao serviço LDAP. Este login tem permissões somente leitura e é usado para consultar atributos LDAP UNIX para

pesquisas de diretório. Atualmente, as vinculações LDAP só são possíveis usando uma conta de máquina SMB.

Você só pode habilitar o LDAP para `NetApp Volumes-Performance` instâncias e usá-lo para volumes NFSv3, NFSv4.1 ou de protocolo duplo. Uma conexão do Active Directory deve ser estabelecida na mesma região que o volume do Google Cloud NetApp Volumes para uma implantação bem-sucedida do volume habilitado para LDAP.

Quando o LDAP está habilitado, o seguinte ocorre em cenários específicos.

- Se apenas NFSv3 ou NFSv4.1 for usado para o projeto do Google Cloud NetApp Volumes , uma nova conta de máquina será criada no controlador de domínio do Active Directory, e o cliente LDAP no Google Cloud NetApp Volumes será vinculado ao Active Directory usando as credenciais da conta da máquina. Nenhum compartilhamento SMB é criado para o volume NFS e compartilhamentos administrativos ocultos padrão (consulte a seção"Compartilhamentos ocultos padrão") têm ACLs de compartilhamento removidos.
- Se volumes de protocolo duplo forem usados para o projeto do Google Cloud NetApp Volumes , somente a conta de máquina única criada para acesso SMB será usada para vincular o cliente LDAP no Google Cloud NetApp Volumes ao Active Directory. Nenhuma conta de máquina adicional é criada.
- Se volumes SMB dedicados forem criados separadamente (antes ou depois de volumes NFS com LDAP serem habilitados), a conta da máquina para vinculações LDAP será compartilhada com a conta da máquina SMB.
- Se o NFS Kerberos também estiver habilitado, duas contas de máquina serão criadas: uma para compartilhamentos SMB e/ou vinculações LDAP e uma para autenticação NFS Kerberos.

Consultas LDAP

Embora as vinculações LDAP sejam criptografadas, as consultas LDAP são passadas pela rede em texto simples usando a porta LDAP comum 389. Esta porta conhecida não pode ser alterada no momento no Google Cloud NetApp Volumes. Como resultado, alguém com acesso à detecção de pacotes na rede pode ver nomes de usuários e grupos, IDs numéricos e associações a grupos.

No entanto, as VMs do Google Cloud não podem detectar o tráfego unicast de outras VMs. Somente VMs que participam ativamente do tráfego LDAP (ou seja, que conseguem se vincular) podem ver o tráfego do servidor LDAP. Para obter mais informações sobre a detecção de pacotes no Google Cloud NetApp Volumes, consulte a seção"Considerações sobre rastreamento/farejamento de pacotes."

Padrões de configuração do cliente LDAP

Quando o LDAP é habilitado em uma instância do Google Cloud NetApp Volumes , uma configuração de cliente LDAP é criada com detalhes de configuração específicos por padrão. Em alguns casos, as opções não se aplicam ao Google Cloud NetApp Volumes (não são compatíveis) ou não são configuráveis.

Opção de cliente LDAP	O que ele faz	Valor padrão	Pode mudar?
Lista de servidores LDAP	Define nomes de servidores LDAP ou endereços IP a serem usados para consultas. Isso não é usado para o Google Cloud NetApp Volumes. Em vez disso, o Domínio do Active Directory é usado para definir servidores LDAP.	Não definido	Não
Domínio do Active Directory	Define o domínio do Active Directory a ser usado para consultas LDAP. O Google Cloud NetApp Volumes utiliza registros SRV para LDAP no DNS para encontrar servidores LDAP no domínio.	Defina como o domínio do Active Directory especificado na conexão do Active Directory.	Não
Servidores do Active Directory preferenciais	Define os servidores do Active Directory preferenciais a serem usados para LDAP. Não compatível com o Google Cloud NetApp Volumes. Em vez disso, use sites do Active Directory para controlar a seleção do servidor LDAP.	Não definido.	Não
Vincular usando credenciais do servidor SMB	Vincula-se ao LDAP usando a conta da máquina SMB. Atualmente, o único método de vinculação LDAP suportado no Google Cloud NetApp Volumes.	Verdadeiro	Não
Modelo de esquema	O modelo de esquema usado para consultas LDAP.	MS-AD-BIS	Não
Porta do servidor LDAP	O número da porta usada para consultas LDAP. Atualmente, o Google Cloud NetApp Volumes usa apenas a porta LDAP padrão 389. LDAPS/porta 636 não é suportado atualmente.	389	Não

Opção de cliente LDAP	O que ele faz	Valor padrão	Pode mudar?
O LDAPS está habilitado?	Controla se o LDAP sobre Secure Sockets Layer (SSL) é usado para consultas e vinculações. Atualmente não é compatível com o Google Cloud NetApp Volumes.	Falso	Não
Tempo limite de consulta (seg)	Tempo limite para consultas. Se as consultas demorarem mais que o valor especificado, elas falharão.	3	Não
Nível mínimo de autenticação de ligação	O nível de vinculação mínimo suportado. Como o Google Cloud NetApp Volumes usa contas de máquina para vinculações LDAP e o Active Directory não oferece suporte a vinculações anônimas por padrão, essa opção não entra em jogo por questões de segurança.	Anônimo	Não
Vincular DN	O nome de usuário/distinguido (DN) usado para vinculações quando a vinculação simples é usada. O Google Cloud NetApp Volumes usa contas de máquina para vinculações LDAP e atualmente não oferece suporte à autenticação de vinculação simples.	Não definido	Não
DN base	O DN base usado para pesquisas LDAP.	O uso do domínio do Windows para a conexão do Active Directory, no formato DN (ou seja, DC=domínio, DC=local).	Não
Escopo de pesquisa base	O escopo de pesquisa para pesquisas de DN base. Os valores podem incluir base, um nível ou subárvore. O Google Cloud NetApp Volumes oferece suporte apenas a pesquisas de subárvore.	Subárvore	Não

Opção de cliente LDAP	O que ele faz	Valor padrão	Pode mudar?
DN do usuário	Define o DN onde as pesquisas do usuário começam para consultas LDAP. Atualmente não há suporte para o Google Cloud NetApp Volumes, portanto todas as pesquisas de usuários começam no DN base.	Não definido	Não
Escopo de pesquisa do usuário	O escopo de pesquisa para pesquisas de DN do usuário. Os valores podem incluir base, um nível ou subárvore. O Google Cloud NetApp Volumes não oferece suporte à definição do escopo de pesquisa do usuário.	Subárvore	Não
Grupo DN	Define o DN onde as pesquisas de grupo começam para consultas LDAP. Atualmente não há suporte para o Google Cloud NetApp Volumes, portanto todas as pesquisas de grupo começam no DN base.	Não definido	Não
Escopo de pesquisa de grupo	O escopo de pesquisa para pesquisas de DN de grupo. Os valores podem incluir base, um nível ou subárvore. O Google Cloud NetApp Volumes não oferece suporte à definição do escopo de pesquisa de grupo.	Subárvore	Não
DN do grupo de rede	Define o DN onde as pesquisas de netgroup começam para consultas LDAP. Atualmente não há suporte para o Google Cloud NetApp Volumes, portanto todas as pesquisas de netgroup começam no DN base.	Não definido	Não

Opção de cliente LDAP	O que ele faz	Valor padrão	Pode mudar?
Escopo de pesquisa do Netgroup	O escopo de pesquisa para pesquisas de DN do netgroup. Os valores podem incluir base, um nível ou subárvore. O Google Cloud NetApp Volumes não oferece suporte à definição do escopo de pesquisa do netgroup.	Subárvore	Não
Use start_tls sobre LDAP	Aproveita o Start TLS para conexões LDAP baseadas em certificados na porta 389. Atualmente não é compatível com o Google Cloud NetApp Volumes.	Falso	Não
Habilitar pesquisa de grupo de rede por host	Permite pesquisas de netgroups por nome de host em vez de expandir netgroups para listar todos os membros. Atualmente não é compatível com o Google Cloud NetApp Volumes.	Falso	Não
DN do grupo de rede por host	Define o DN onde as pesquisas netgroup-by-host começam para consultas LDAP. Atualmente, o Netgroup-by-host não é compatível com o Google Cloud NetApp Volumes.	Não definido	Não
Escopo de pesquisa de grupo de rede por host	O escopo de pesquisa para pesquisas de DN de grupo de rede por host. Os valores podem incluir base, um nível ou subárvore. Atualmente, o Netgroup-by-host não é compatível com o Google Cloud NetApp Volumes.	Subárvore	Não

Opção de cliente LDAP	O que ele faz	Valor padrão	Pode mudar?
Segurança da sessão do cliente	Define qual nível de segurança de sessão é usado pelo LDAP (assinatura, selo ou nenhum). A assinatura LDAP é suportada pelo NetApp Volumes-Performance, se solicitada pelo Active Directory. O NetApp Volumes-SW não oferece suporte à assinatura LDAP. Para ambos os tipos de serviço, a selagem não é suportada atualmente.	Nenhum	Não
Busca de referência LDAP	Ao usar vários servidores LDAP, a busca de referência permite que o cliente consulte outros servidores LDAP na lista quando uma entrada não for encontrada no primeiro servidor. Atualmente, isso não é suportado pelo Google Cloud NetApp Volumes.	Falso	Não
Filtro de associação de grupo	Fornece um filtro de pesquisa LDAP personalizado a ser usado ao consultar associação de grupo em um servidor LDAP. Atualmente não compatível com o Google Cloud NetApp Volumes.	Não definido	Não

Usando LDAP para mapeamento de nomes assimétricos

O Google Cloud NetApp Volumes, por padrão, mapeia usuários do Windows e usuários do UNIX com nomes de usuário idênticos bidirecionalmente, sem configuração especial. Desde que o Google Cloud NetApp Volumes consiga encontrar um usuário UNIX válido (com LDAP), ocorrerá o mapeamento de nomes 1:1. Por exemplo, se o usuário do Windows `johnsmith` é usado, então, se o Google Cloud NetApp Volumes puder encontrar um usuário UNIX chamado `johnsmith` no LDAP, o mapeamento de nomes é bem-sucedido para esse usuário, todos os arquivos/pastas criados por `johnsmith` mostrar a propriedade correta do usuário e todas as ACLs que afetam `johnsmith` são honrados independentemente do protocolo NAS em uso. Isso é conhecido como mapeamento simétrico de nomes.

O mapeamento de nomes assimétrico ocorre quando a identidade do usuário do Windows e do usuário do UNIX não correspondem. Por exemplo, se o usuário do Windows `johnsmith` tem uma identidade UNIX de `jsmith` O Google Cloud NetApp Volumes precisa de uma maneira de ser informado sobre a variação. Como o Google Cloud NetApp Volumes atualmente não oferece suporte à criação de regras de mapeamento de nomes estáticos, o LDAP deve ser usado para consultar a identidade dos usuários para identidades do

Windows e do UNIX para garantir a propriedade adequada de arquivos e pastas e as permissões esperadas.

Por padrão, o Google Cloud NetApp Volumes inclui `LDAP` no ns-switch da instância do banco de dados de mapa de nomes, para fornecer a funcionalidade de mapeamento de nomes usando LDAP para nomes assimétricos, você só precisa modificar alguns dos atributos de usuário/grupo para refletir o que o Google Cloud NetApp Volumes procura.

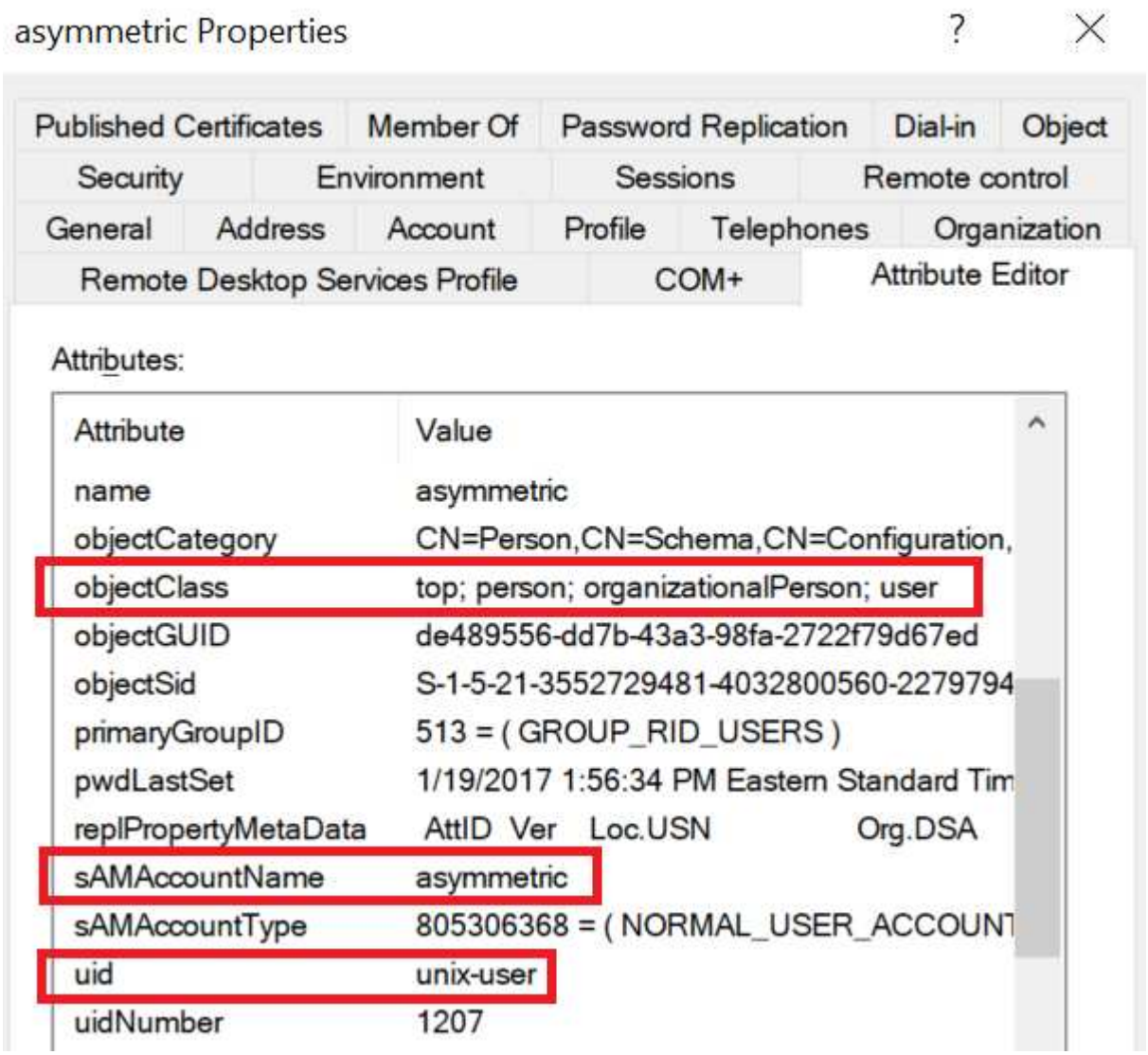
A tabela a seguir mostra quais atributos devem ser preenchidos no LDAP para a funcionalidade de mapeamento de nomes assimétricos. Na maioria dos casos, o Active Directory já está configurado para fazer isso.

Atributo de Google Cloud NetApp Volumes	**O que ele faz**	**Valor usado pelo Google Cloud NetApp Volumes para mapeamento de nomes**
ObjectClass do Windows para UNIX	Especifica o tipo de objeto que está sendo usado. (Ou seja, usuário, grupo, posixAccount e assim por diante)	Deve incluir o usuário (pode conter vários outros valores, se desejado).
Atributo Windows para UNIX	que define o nome de usuário do Windows na criação. O Google Cloud NetApp Volumes usa isso para pesquisas do Windows para o UNIX.	Nenhuma alteração necessária aqui; sAMAccountName é o mesmo que o nome de login do Windows.
UID	Define o nome de usuário do UNIX.	Nome de usuário UNIX desejado.

Atualmente, o Google Cloud NetApp Volumes não usa prefixos de domínio em pesquisas LDAP, portanto, ambientes LDAP com vários domínios não funcionam corretamente com pesquisas de mapa de nomes LDAP.

O exemplo a seguir mostra um usuário com o nome Windows `asymmetric` , o nome UNIX `unix-user` , e o comportamento que ele segue ao gravar arquivos de SMB e NFS.

A figura a seguir mostra a aparência dos atributos LDAP no servidor Windows.



De um cliente NFS, você pode consultar o nome UNIX, mas não o nome Windows:

```
# id unix-user
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
# id asymmetric
id: asymmetric: no such user
```

Quando um arquivo é gravado do NFS como `unix-user` , o seguinte é o resultado do cliente NFS:

```
sh-4.2$ pwd
/mnt/home/ntfssh-4.2$ touch unix-user-file
sh-4.2$ ls -la | grep unix-user
-rwx------  1 unix-user sharedgroup     0 Feb 28 12:37 unix-user-nfs
sh-4.2$ id
uid=1207(unix-user) gid=1220(sharedgroup) groups=1220(sharedgroup)
```

Em um cliente Windows, você pode ver que o proprietário do arquivo está definido como o usuário apropriado do Windows:

```
PS C:\ > Get-Acl \\demo\home\ntfs\unix-user-nfs | select Owner
Owner
-----
NTAP\asymmetric
```

Por outro lado, os arquivos criados pelo usuário do Windows `asymmetric` de um cliente SMB mostra o proprietário UNIX apropriado, conforme mostrado no texto a seguir.

PME:

```
PS Z:\ntfs> echo TEXT > asymmetric-user-smb.txt
```

NFS:

```
sh-4.2$ ls -la | grep asymmetric-user-smb.txt
-rwx------  1 unix-user         sharedgroup   14 Feb 28 12:43 asymmetric-
user-smb.txt
sh-4.2$ cat asymmetric-user-smb.txt
TEXT
```

Ligação de canal LDAP

Devido a uma vulnerabilidade nos controladores de domínio do Windows Active Directory, "Aviso de segurança da Microsoft ADV190023" altera como os DCs permitem vinculações LDAP.

O impacto para o Google Cloud NetApp Volumes é o mesmo que para qualquer cliente LDAP. O Google Cloud NetApp Volumes não oferece suporte à vinculação de canais no momento. Como o Google Cloud NetApp Volumes oferece suporte à assinatura LDAP por padrão por meio de negociação, a vinculação de canal LDAP não deve ser um problema. Se você tiver problemas para vincular ao LDAP com a vinculação de canal habilitada, siga as etapas de correção em ADV190023 para permitir que as vinculações LDAP do Google Cloud NetApp Volumes sejam bem-sucedidas.

DNS

O Active Directory e o Kerberos têm dependências no DNS para resolução de nome de host para IP/IP para nome de host. O DNS exige que a porta 53 esteja aberta. O Google Cloud NetApp Volumes não faz nenhuma modificação nos registros DNS, nem atualmente oferece suporte ao uso de "DNS dinâmico" em interfaces de rede.

Você pode configurar o DNS do Active Directory para restringir quais servidores podem atualizar registros DNS. Para obter mais informações, consulte "DNS seguro do Windows" .

Observe que os recursos dentro de um projeto do Google usam por padrão o Google Cloud DNS, que não está conectado ao DNS do Active Directory. Clientes que usam o Cloud DNS não conseguem resolver caminhos UNC retornados pelo Google Cloud NetApp Volumes. Os clientes Windows associados ao domínio

do Active Directory são configurados para usar o DNS do Active Directory e podem resolver esses caminhos UNC.

Para adicionar um cliente ao Active Directory, você deve configurar a configuração de DNS dele para usar o DNS do Active Directory. Opcionalmente, você pode configurar o Cloud DNS para encaminhar as solicitações para o DNS do Active Directory. Consulte "Por que meu cliente não consegue resolver o nome NetBIOS do SMB?"para obter mais informações.

Atualmente, o Google Cloud NetApp Volumes não oferece suporte a DNSSEC e as consultas DNS são realizadas em texto simples.

Auditoria de acesso a arquivos

Atualmente sem suporte para Google Cloud NetApp Volumes.

Proteção antivírus

Você deve executar uma verificação antivírus no Google Cloud NetApp Volumes no cliente para um compartilhamento NAS. Atualmente, não há integração antivírus nativa com o Google Cloud NetApp Volumes.

Operação de serviço

A equipe do Google Cloud NetApp Volumes gerencia os serviços de back-end no Google Cloud e usa várias estratégias para proteger a plataforma e evitar acesso indesejado.

Cada cliente obtém sua própria sub-rede exclusiva, cujo acesso é isolado de outros clientes por padrão, e cada locatário no Google Cloud NetApp Volumes obtém seu próprio namespace e VLAN para isolamento total de dados. Depois que um usuário é autenticado, o Service Delivery Engine (SDE) só pode ler dados de configuração específicos daquele locatário.

Segurança física

Com a pré-aprovação adequada, apenas engenheiros no local e engenheiros de suporte de campo (FSEs) com o selo NetApp têm acesso ao cage e aos racks para trabalho físico. Não é permitido armazenamento e gerenciamento de rede. Somente esses recursos no local são capazes de executar tarefas de manutenção de hardware.

Para engenheiros no local, um tíquete é gerado para a declaração de trabalho (SOW) que inclui o ID do rack e a localização do dispositivo (RU), e todos os outros detalhes estão incluídos no tíquete. Para FSEs da NetApp , um tíquete de visita ao site deve ser gerado com o COLO e o tíquete inclui os detalhes do visitante, data e hora para fins de auditoria. O SOW para o FSE é comunicado internamente à NetApp.

Equipe de operações

A equipe de operações do Google Cloud NetApp Volumes é composta por engenheiros de produção e um engenheiro de confiabilidade do site (SRE) para o Google Cloud NetApp Volumes , além de engenheiros e parceiros de suporte de campo da NetApp para hardware. Todos os membros da equipe de operações são credenciados para trabalhar no Google Cloud e registros detalhados do trabalho são mantidos para cada ticket gerado. Além disso, há um rigoroso processo de controle e aprovação de mudanças para garantir que cada decisão seja devidamente examinada.

A equipe de SRE gerencia o plano de controle e como os dados são roteados das solicitações de interface do usuário para o hardware e software de back-end no Google Cloud NetApp Volumes. A equipe SRE também gerencia recursos do sistema, como volume e máximos de inodes. Os SREs não têm permissão para interagir

ou ter acesso aos dados do cliente. Os SREs também fornecem coordenação com Autorizações de Devolução de Material (RMAs), como novas solicitações de substituição de disco ou memória para o hardware de backend.

Responsabilidades do cliente

Os clientes do Google Cloud NetApp Volumes gerenciam o Active Directory e o gerenciamento de funções de usuário de suas organizações, bem como as operações de volume e dados. Os clientes podem ter funções administrativas e delegar permissões a outros usuários finais dentro do mesmo projeto do Google Cloud usando as duas funções predefinidas que a NetApp e o Google Cloud fornecem (Administrador e Visualizador).

O administrador pode conectar qualquer VPC dentro do projeto do cliente ao Google Cloud NetApp Volumes que o cliente determinar ser apropriado. É responsabilidade do cliente gerenciar o acesso à sua assinatura do Google Cloud Marketplace e gerenciar as VPCs que têm acesso ao plano de dados.

Proteção SRE maliciosa

Uma preocupação que pode surgir é como o Google Cloud NetApp Volumes protege contra cenários em que há um SRE malicioso ou quando as credenciais do SRE foram comprometidas?

O acesso ao ambiente de produção é restrito a um número limitado de profissionais de SRE. Os privilégios administrativos são ainda mais restritos a um punhado de administradores experientes. Todas as ações executadas por qualquer pessoa no ambiente de produção do Google Cloud NetApp Volumes são registradas e quaisquer anomalias na linha de base ou atividades suspeitas são detectadas por nossa plataforma de inteligência de ameaças de gerenciamento de eventos e informações de segurança (SIEM). Como resultado, ações maliciosas podem ser rastreadas e mitigadas antes que muitos danos sejam causados ao backend do Google Cloud NetApp Volumes .

Ciclo de vida do volume

O Google Cloud NetApp Volumes gerencia apenas os objetos dentro do serviço, não os dados dentro dos volumes. Somente clientes que acessam os volumes podem gerenciar os dados, as ACLs, os proprietários dos arquivos e assim por diante. Os dados nesses volumes são criptografados em repouso e o acesso é limitado aos locatários da instância do Google Cloud NetApp Volumes .

O ciclo de vida do volume do Google Cloud NetApp Volumes é criar-atualizar-excluir. Os volumes retêm cópias de instantâneo dos volumes até que eles sejam excluídos, e somente administradores validados do Google Cloud NetApp Volumes podem excluir volumes no Google Cloud NetApp Volumes. Quando a exclusão de um volume é solicitada por um administrador, uma etapa adicional de inserção do nome do volume é necessária para verificar a exclusão. Depois que um volume é excluído, ele desaparece e não pode ser recuperado.

Nos casos em que um contrato do Google Cloud NetApp Volumes é rescindido, a NetApp marca os volumes para exclusão após um período de tempo específico. Antes que esse período expire, você pode recuperar volumes a pedido do cliente.

Certificações

O Google Cloud NetApp Volumes para Google Cloud está atualmente certificado de acordo com os padrões ISO/IEC 27001:2013 e ISO/IEC 27018:2019. O serviço também recebeu recentemente seu relatório de atestado SOC2 Tipo I. Para obter informações sobre o compromisso da NetApp com a segurança e privacidade dos dados, consulte "Conformidade: Segurança de dados e privacidade de dados" .

RGPD

Nossos compromissos com a privacidade e a conformidade com o GDPR estão disponíveis em vários de nossos "contratos com clientes", como a nossa "Adendo de Data Processing do Cliente", que inclui o "Cláusulas contratuais padrão" fornecido pela Comissão Europeia. Também assumimos esses compromissos em nossa Política de Privacidade, respaldada pelos valores fundamentais estabelecidos em nosso Código de Conduta corporativo.

Informações adicionais e informações de contato

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

- Documentação do Google Cloud para o Google Cloud NetApp Volumes

  "https://docs.cloud.google.com/netapp/volumes/docs/discover/overview"

- Acesso ao serviço privado do Google

  https://cloud.google.com/vpc/docs/private-services-access?hl=en_US

- Documentação do produto NetApp

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

- Programa de Módulo de Validação Criptográfica — NetApp CryptoMod

  "https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4144"

- A solução da NetApp para ransomware

  https://www.netapp.com/pdf.html?item=/media/16716-sb-3938pdf.pdf&v=202093745

- TR-4616: NFS Kerberos em ONTAP

  https://www.netapp.com/pdf.html?item=/media/19384-tr-4616.pdf

Contate-nos

Deixe-nos saber como podemos melhorar este relatório técnico.

Entre em contato conosco pelo e-mail doccomments@netapp.com. Inclua RELATÓRIO TÉCNICO 4918 no assunto.

O NetApp Disaster Recovery

Proteção de dados 3-2-1 para o VMware com o SnapCenter Plug-in e o NetApp Backup and Recovery para proteger cargas de trabalho do VMware

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 aborda uma solução de backup 3-2-1 usando o SnapCenter Plug-in for VMware vSphere (SCV) para criar backups primários e secundários das suas máquinas virtuais no local e o NetApp Backup and Recovery para máquinas virtuais para fazer backup de uma cópia dos seus dados em storage de nuvem ou no StorageGRID.

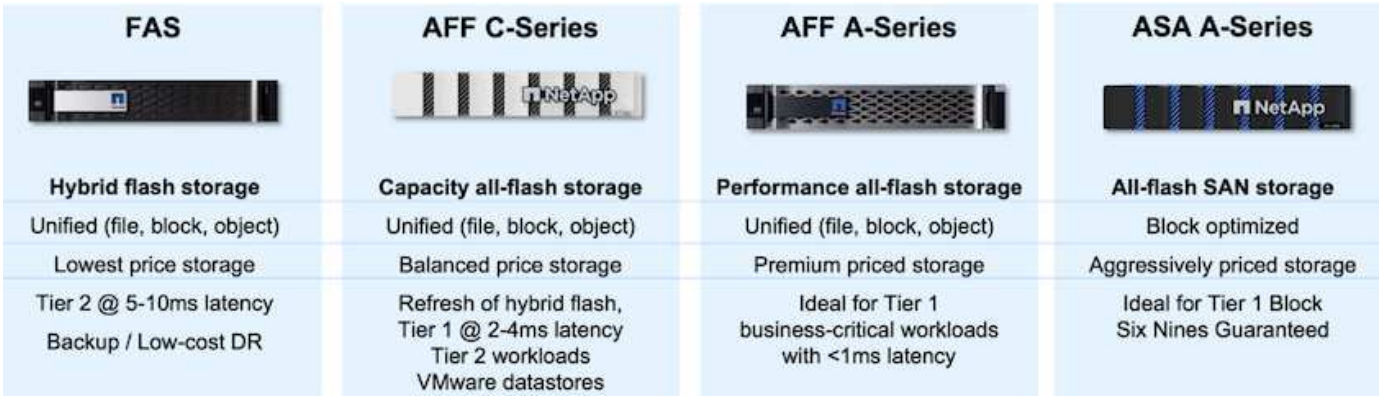
Casos de uso

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 do ONTAP e com backup em storage de objetos usando o NetApp 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.



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.

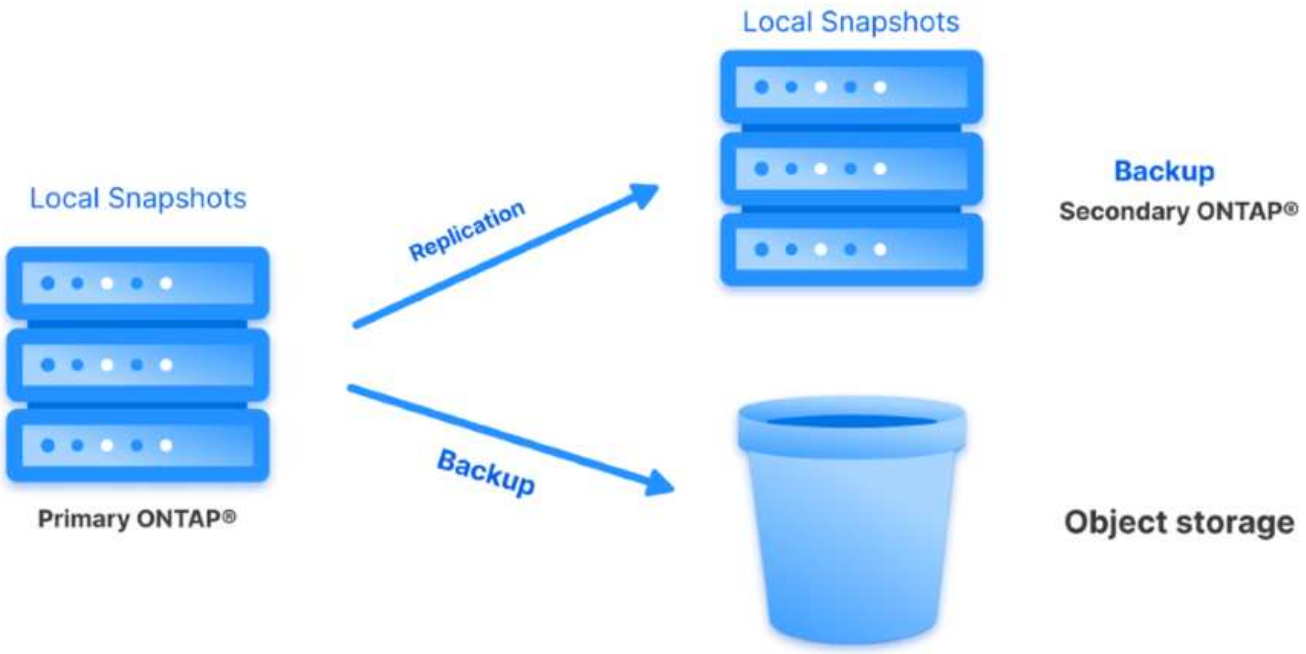
Para obter informações detalhadas sobre SCV, consulte "Documentação do SnapCenter Plug-in for VMware vSphere" .

NetApp Backup and Recovery para proteger cargas de trabalho do VMware

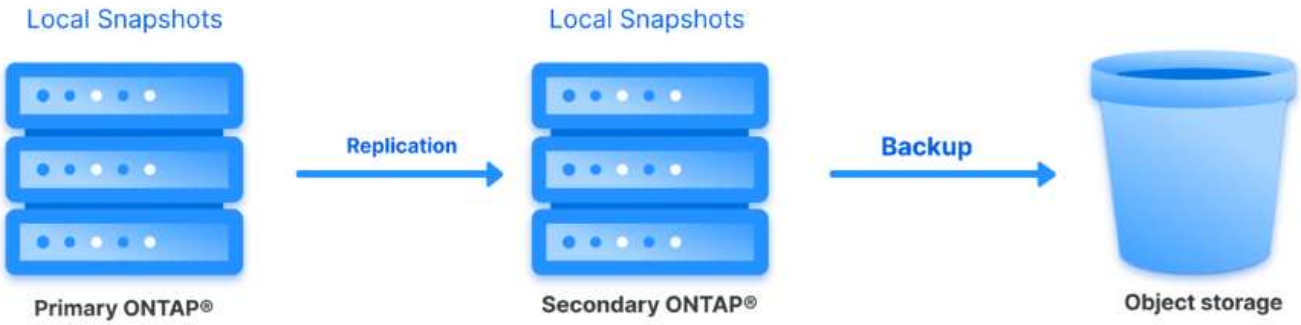
O NetApp Backup and Recovery é uma ferramenta baseada na nuvem para gerenciamento de dados que fornece um único plano de controle para uma ampla variedade de operações de backup e recuperação em ambientes locais e na nuvem. Parte do pacote do NetApp Backup and Recovery para VMs é um recurso que se integra ao SnapCenter Plug-in for VMware vSphere (local) para estender uma cópia dos dados para o storage de objetos na nuvem. Isso estabelece uma terceira cópia dos dados fora do local, originada dos backups no storage primário ou no storage secundário. O NetApp Backup and Recovery para VMs facilita a configuração de políticas de storage que transferem cópias dos seus dados de qualquer um desses dois locais locais.

A escolha entre os backups primário e secundário como origem no NetApp Backup and Recovery resultará na implementação de uma das duas topologias a seguir:

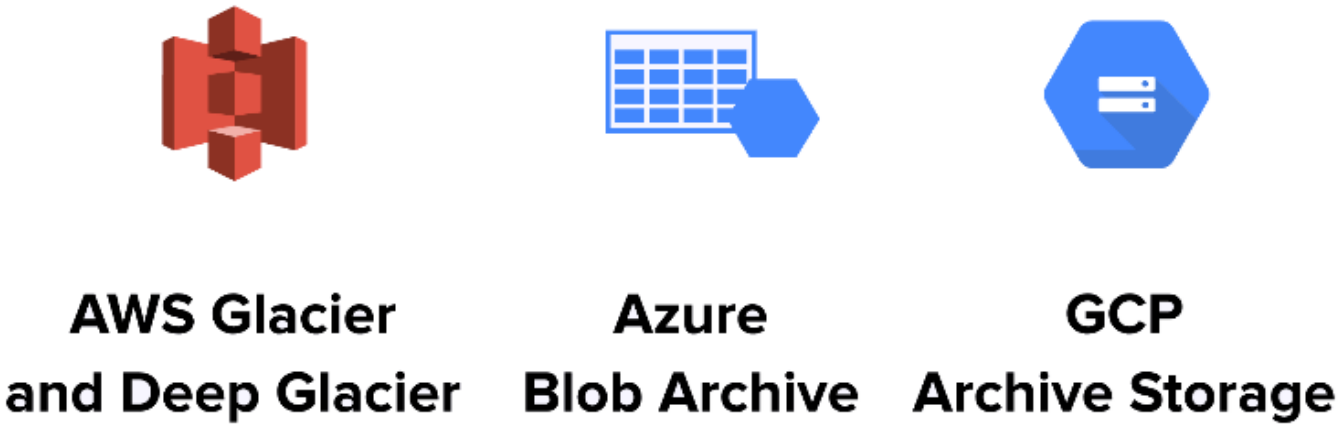
Topologia fan-out: quando um backup é iniciado pelo SnapCenter Plug-in for VMware vSphere, uma cópia Snapshot local é feita imediatamente. O SCV então inicia uma operação do SnapMirror que replica a cópia Snapshot mais recente para o cluster ONTAP secundário. No NetApp Backup and Recovery, uma política especifica o cluster ONTAP primário como a origem de uma cópia Snapshot dos dados a serem transferidos para o storage de objetos no provedor de nuvem de sua escolha.



Topologia em cascata: criar as cópias de dados primária e secundária usando o SCV é idêntico à topologia fan-out mencionada acima. No entanto, desta vez, uma política é criada no NetApp Backup and Recovery, especificando que o backup para storage de objetos terá origem no cluster ONTAP secundário.



O NetApp Backup and Recovery pode criar cópias de backup de Snapshots do ONTAP no local para o storage 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 a partir do SCV e do NetApp Console:

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. Configure o NetApp 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. Restaurar máquinas virtuais do storage de objetos usando a NetApp Console.

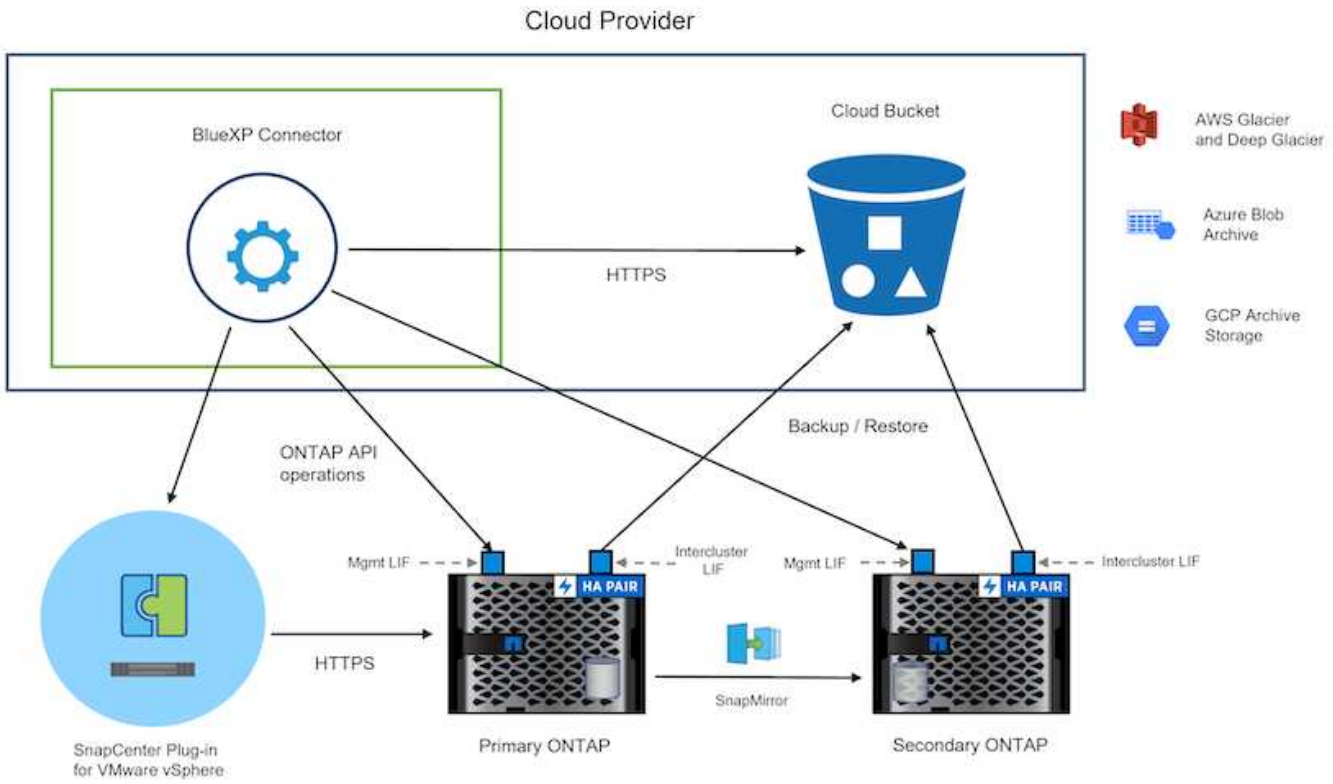
▼ **Pré-requisitos**

O objetivo desta solução é demonstrar a proteção de dados de máquinas virtuais em execução no VMware vSphere e localizadas em NFS Datastores hospedados 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. Agente do console instalado para o provedor de nuvem usado para backups de storage 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 agente do Console e as interfaces de gerenciamento do cluster de storage ONTAP local.
6. Conectividade de rede entre o agente do Console e a VM do dispositivo SCV local e entre o agente do Console e 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 implementar e validar uma solução que utiliza o SnapCenter Plug-in for VMware vSphere, juntamente com o Backup and Recovery, para realizar 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 nessa configuração são armazenadas em datastores NFS hospedados por um cluster de storage ONTAP A300. Além disso, um cluster de storage ONTAP A300 separado serve como destino secundário para volumes replicados usando o SnapMirror. Além disso, o storage de objetos hospedado na Amazon Web Services e no Azure Blob foi utilizado como destino para uma terceira cópia dos dados.

Vamos abordar a criação de relações do SnapMirror para cópias secundárias de nossos backups gerenciados pelo SCV e a configuração de tarefas de backup tanto no SCV quanto no NetApp Console.

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 backup e recuperação consulte o "Documentação de backup e recuperação".

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 NetApp Console, onde muitas das etapas são automatizadas, ou pode ser feita usando o System Manager e a ONTAP CLI. Todos esses métodos são discutidos abaixo.

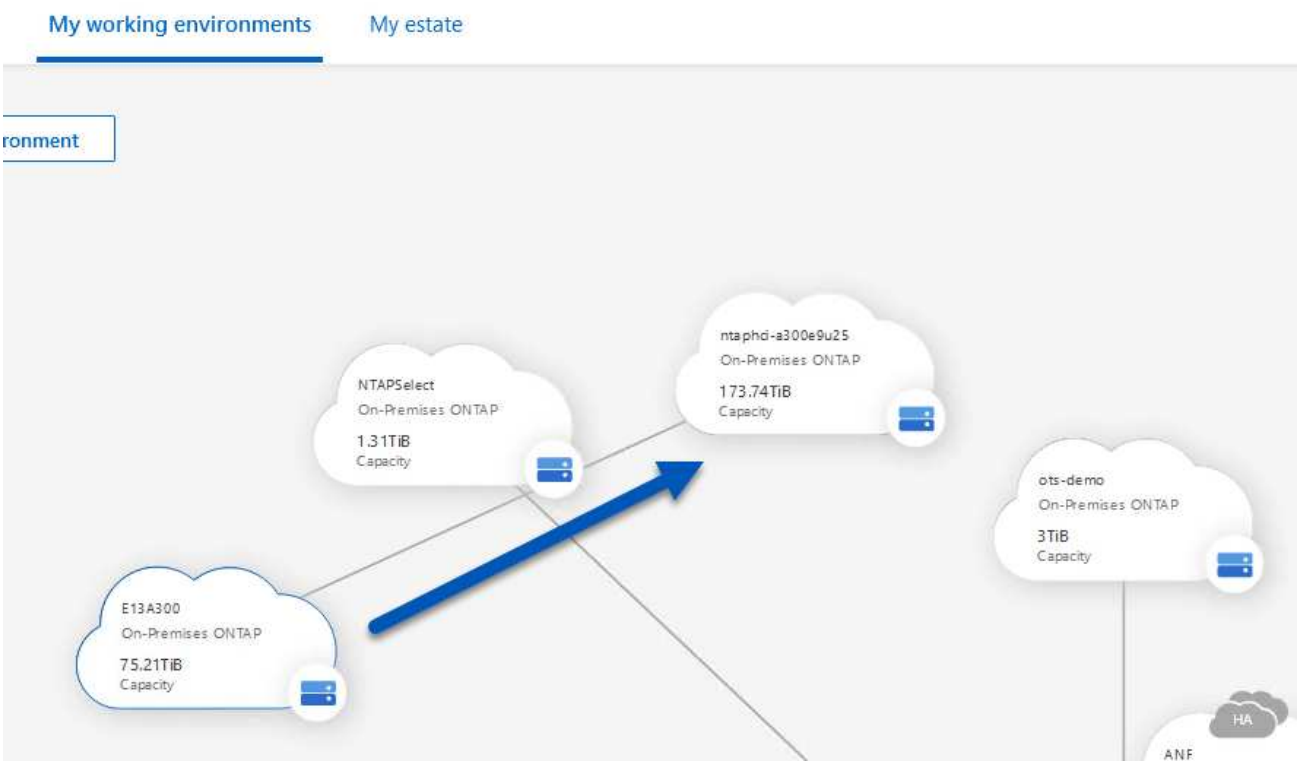
Estabeleça relações do SnapMirror com o NetApp Console

As etapas a seguir devem ser concluídas a partir do NetApp Console:

▼ **Configuração de replicação para sistemas de armazenamento ONTAP primário e secundário**

Comece fazendo login no NetApp Console e navegue até Sistemas.

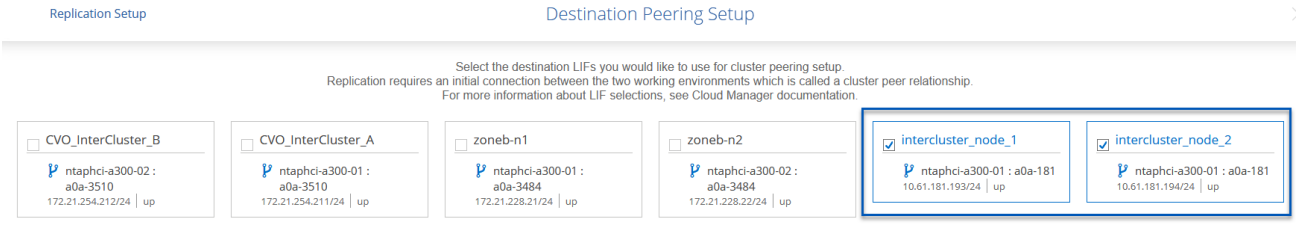
1. Arraste e solte o sistema de armazenamento ONTAP de origem (primário) no sistema de armazenamento ONTAP de destino (secundário).



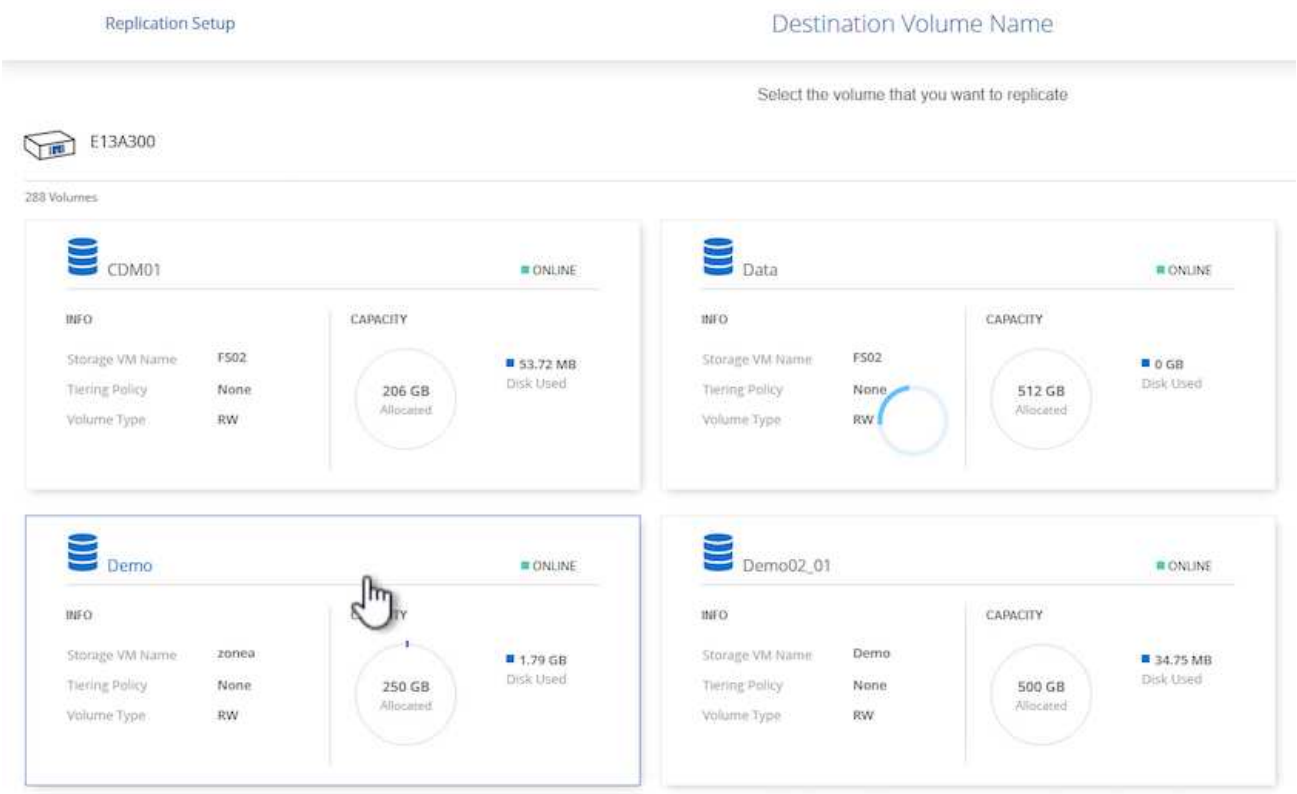
2. No menu que aparece, selecione **Replicação**.



3. Na página **Configuração de peering de destino**, selecione os LIFs Intercluster de destino a serem usados para a conexão entre sistemas de armazenamento.

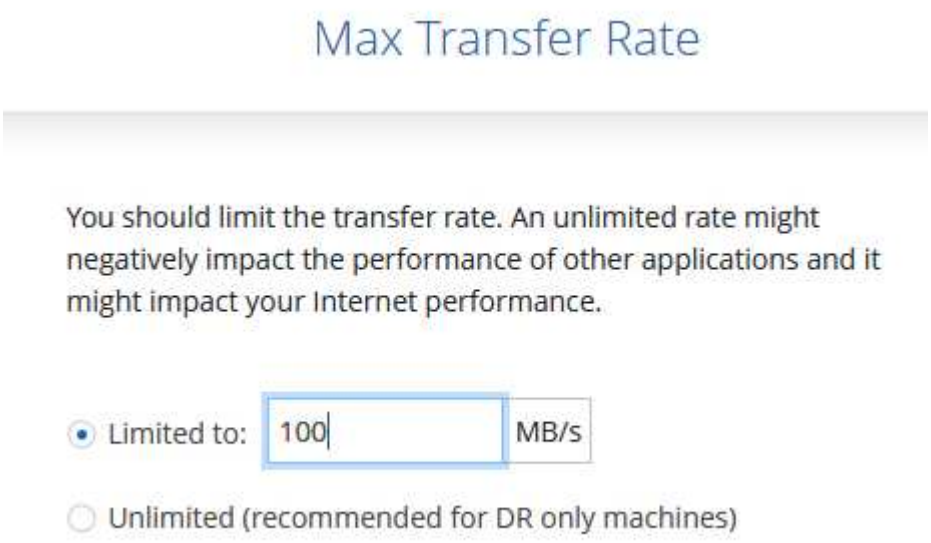


4. Na página **Nome do volume de destino**, primeiro selecione o volume de origem, depois preencha o nome do volume de destino e selecione o SVM de destino e o agregado. Clique em **Avançar** para continuar.

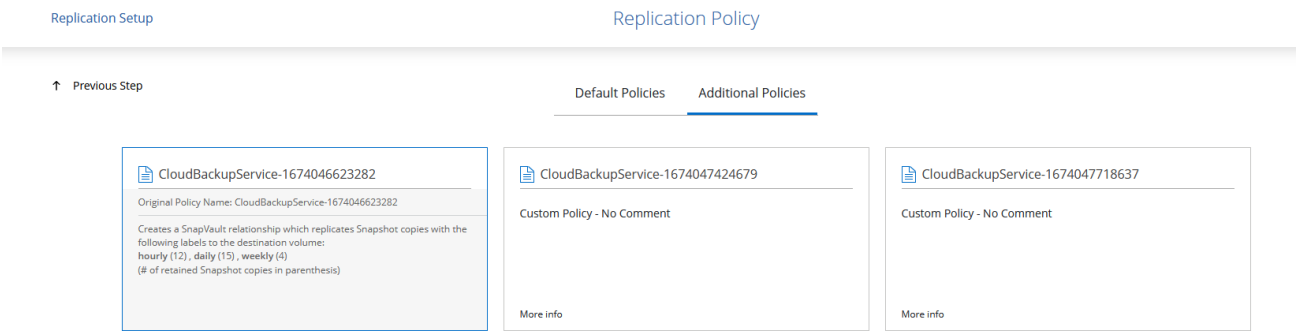




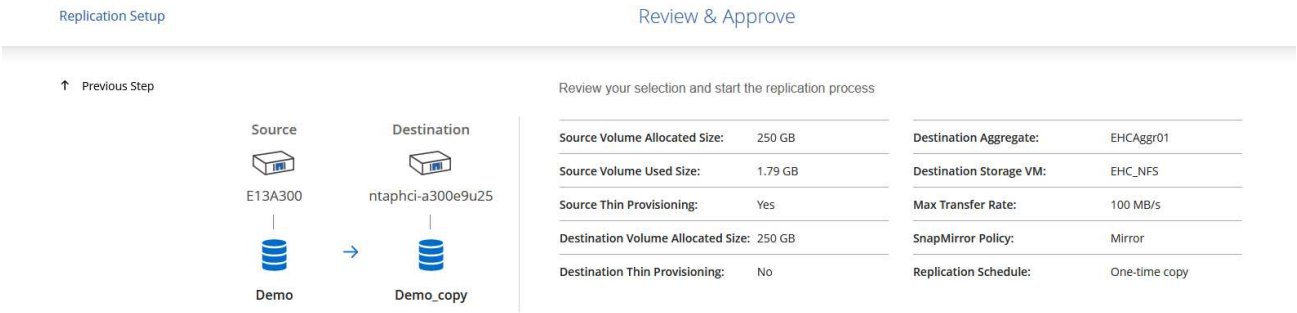
5. Escolha a taxa máxima de transferência para que a replicação ocorra.



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.



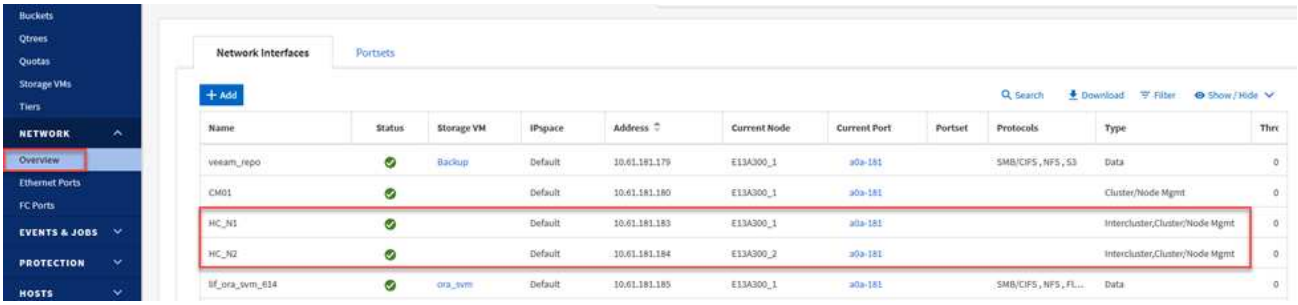
Estabelecer relacionamentos do SnapMirror com o System Manager e o ONTAP CLI

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
```

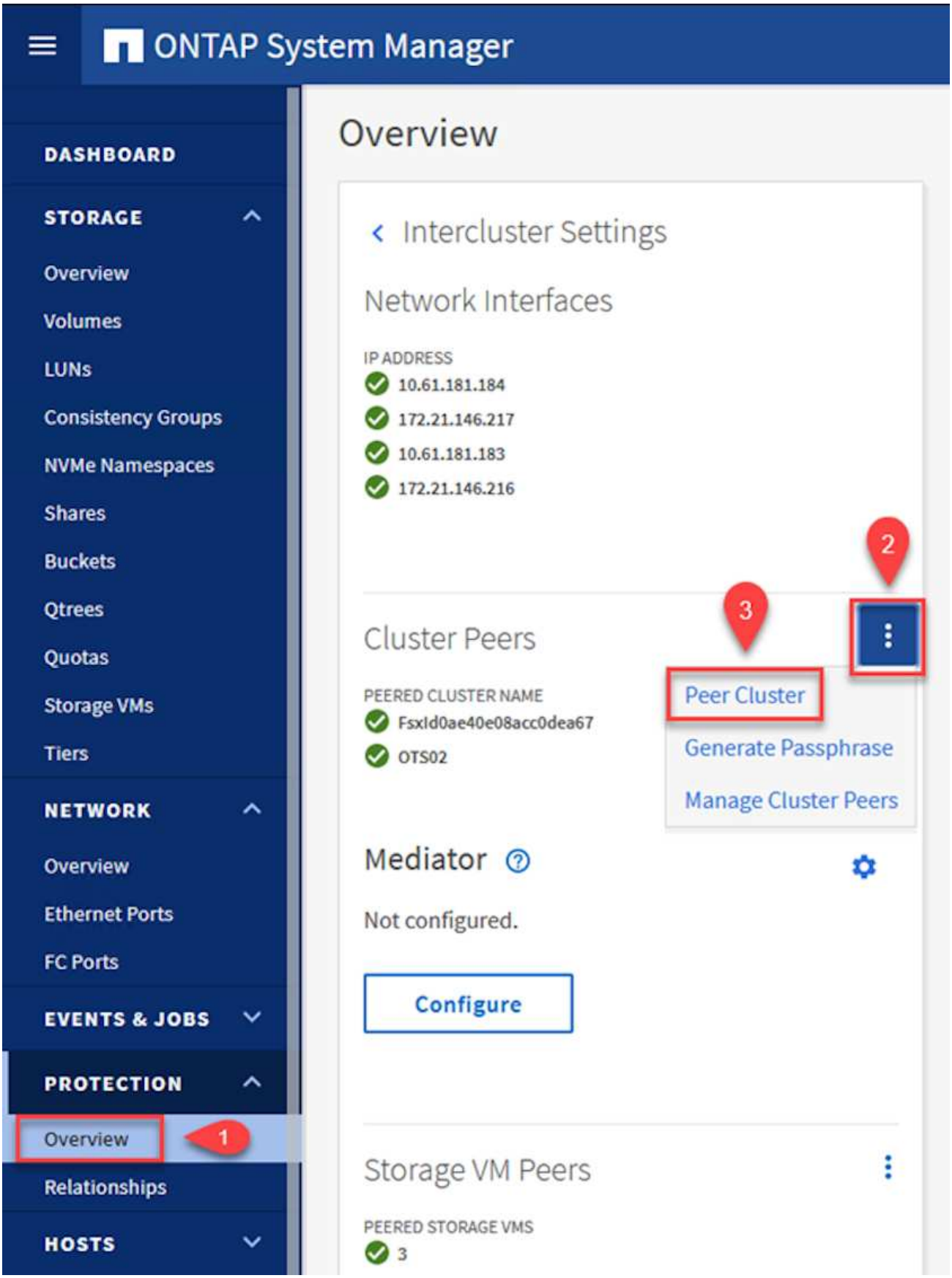
▼ **Estabelecer peering de cluster entre clusters ONTAP**

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.



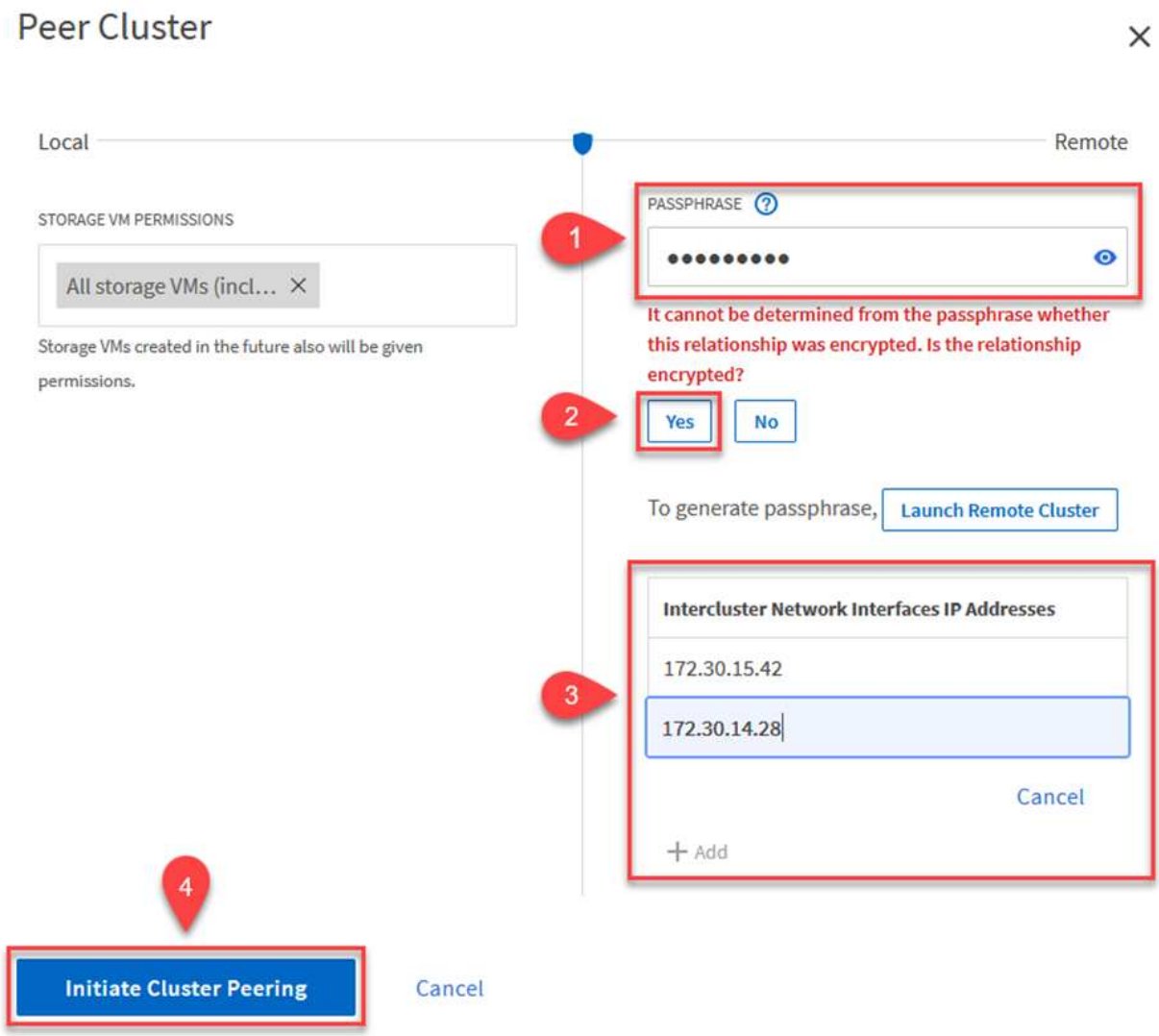
3. Na caixa de diálogo Cluster de Pares, preencha as informações necessárias:
   a. Digite a senha que foi usada para estabelecer o relacionamento do cluster de pares no cluster

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
```

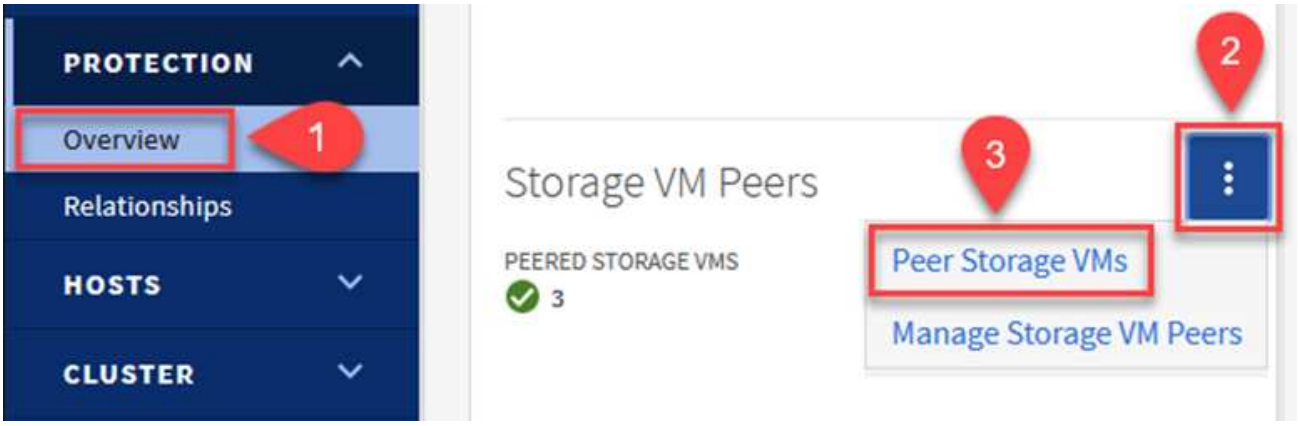
▼ **Estabelecer relacionamento de peering SVM**

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 .

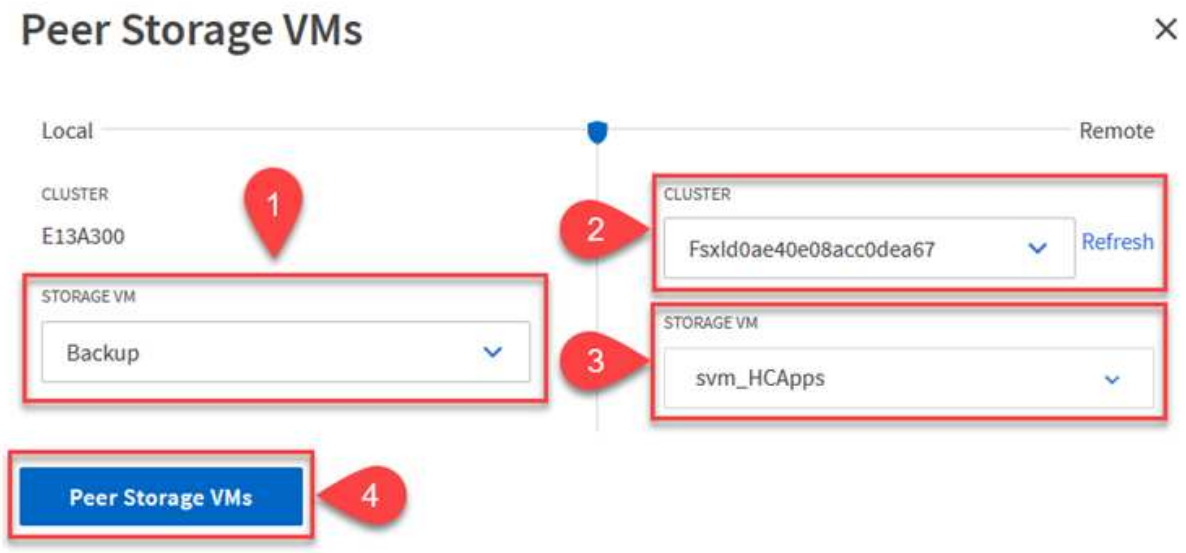
1. No cluster ONTAP de destino, use o seguinte comando da CLI para criar o relacionamento de peer SVM:

```
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**

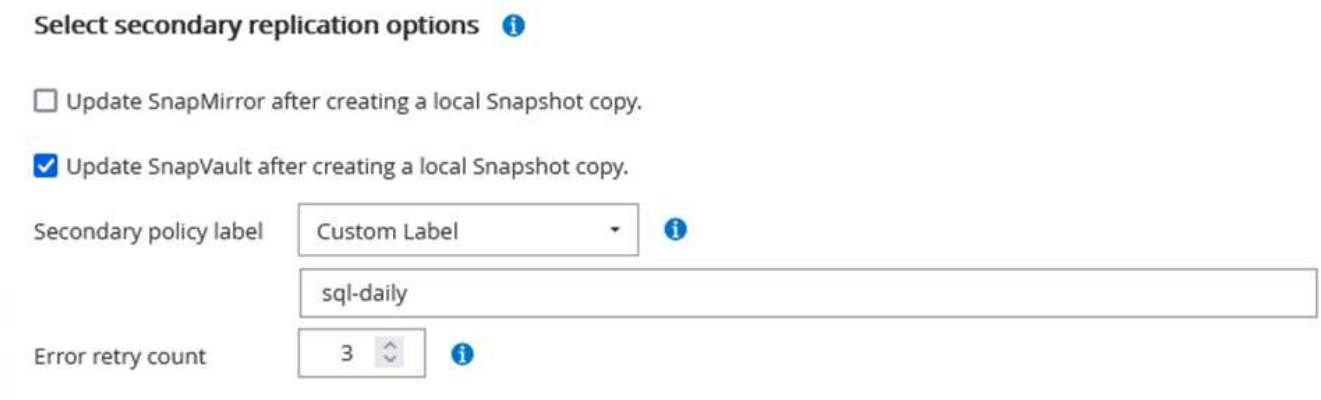
O SnapCenter gerencia agendamentos de retenção para backups que existem como cópias instantâneas no sistema de armazenamento primário. Isso é estabelecido ao criar uma política no SnapCenter. O SnapCenter não gerencia políticas de retenção para backups retidos em sistemas de armazenamento

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.

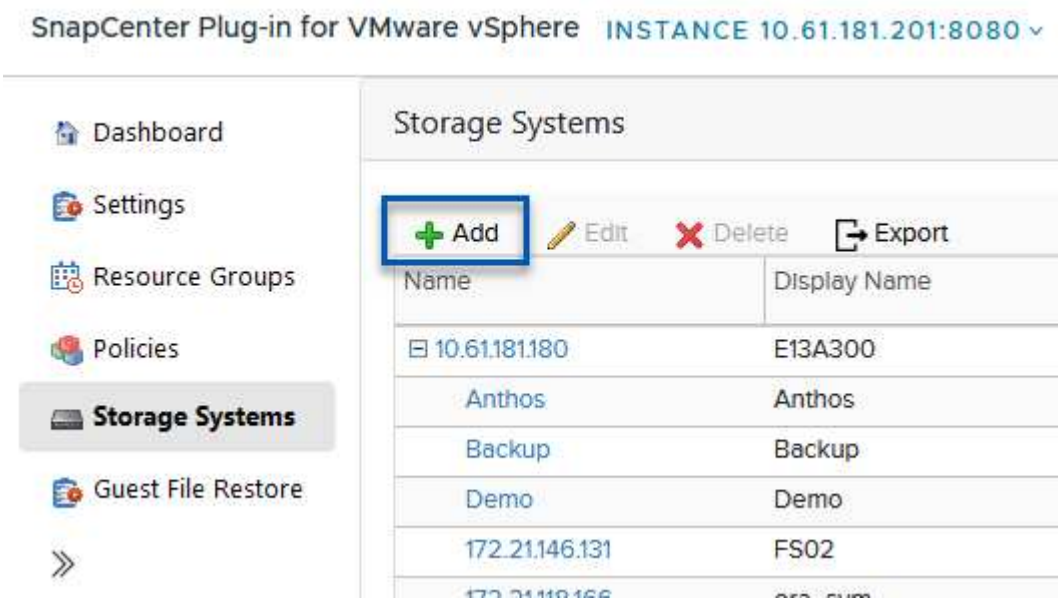
Revise o "Fluxo de trabalho de proteção de dados" seção da documentação do SCV para obter mais informações sobre as etapas envolvidas na configuração de backups.

Para configurar backups de suas máquinas virtuais e armazenamentos de dados, as seguintes etapas precisarão ser concluídas na interface do plug-in.

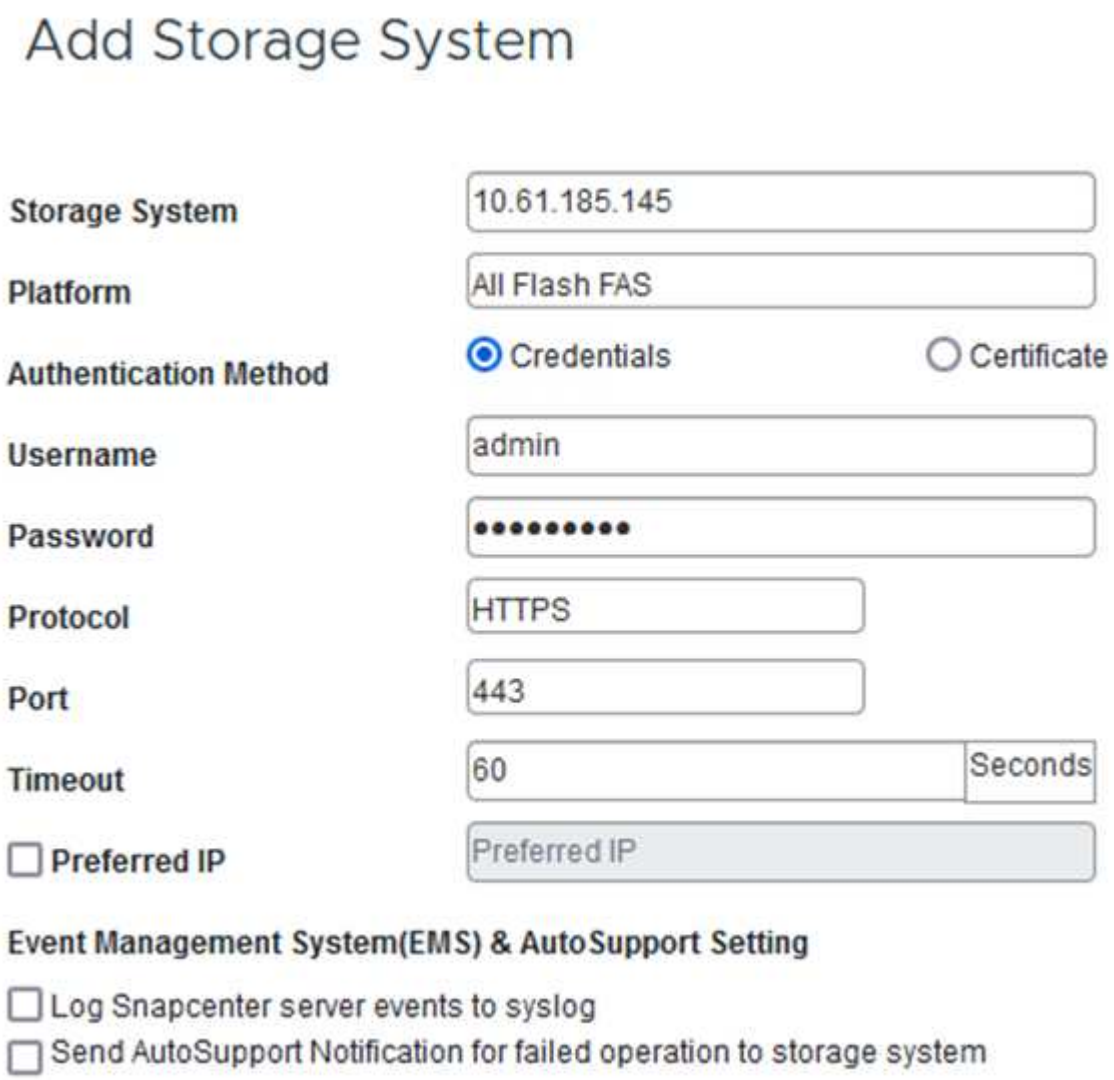
▼ **Sistemas de armazenamento Discovery ONTAP**

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.

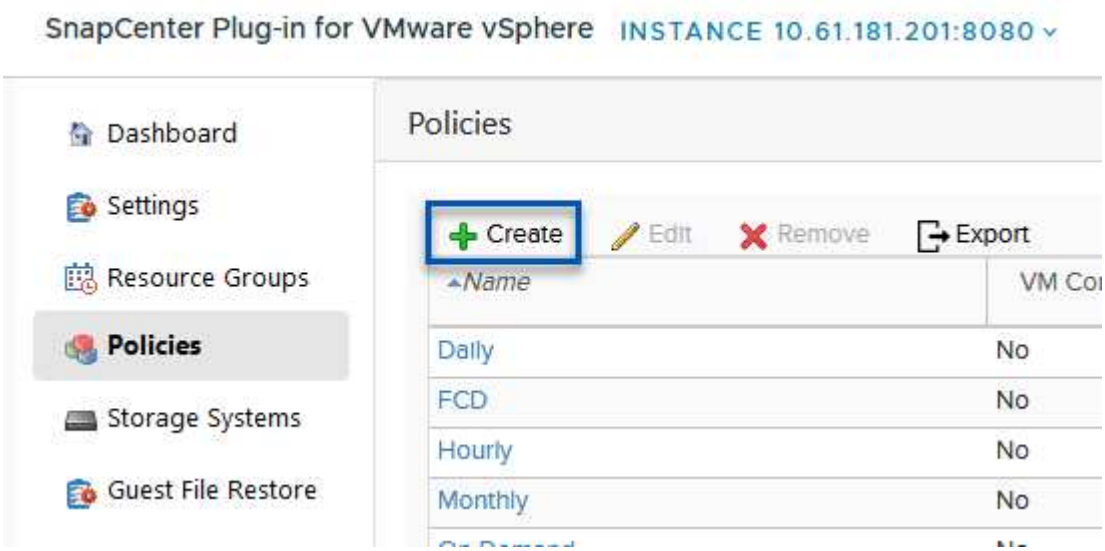
▼ **Criar políticas de backup do SCV**

As políticas especificam o período de retenção, a frequência e as opções de replicação para os backups gerenciados pelo SCV.

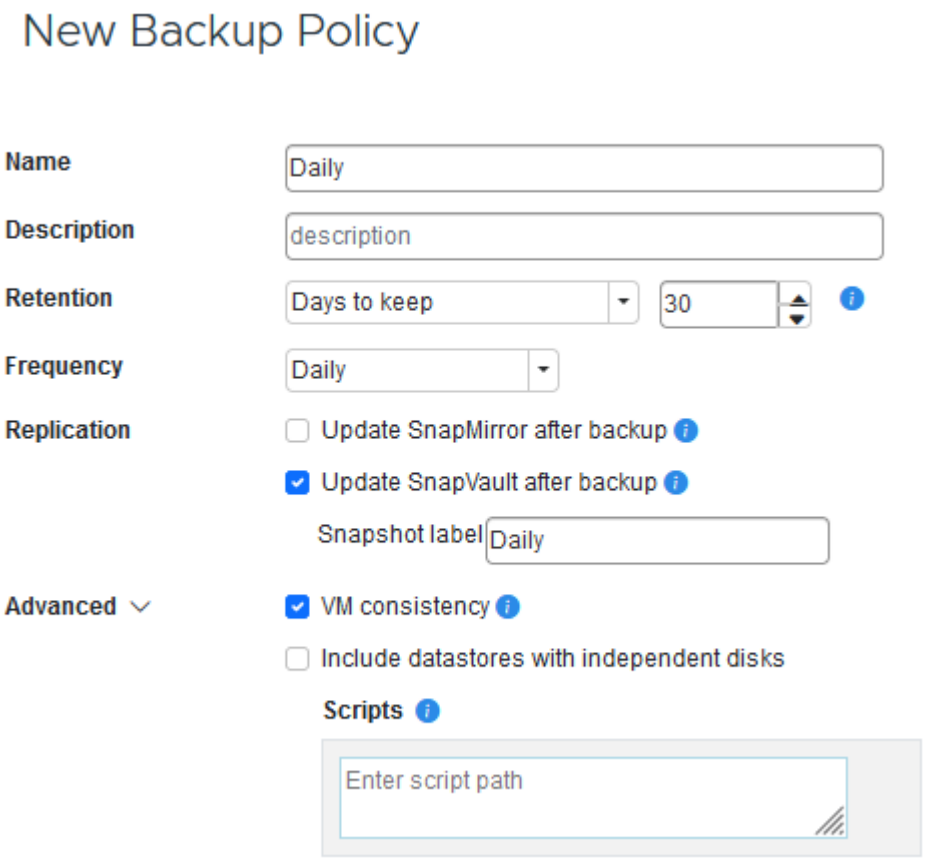
Revise o "Crie políticas de backup para VMs e armazenamentos de dados" seção da documentação para mais informações.

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 Snapshot são úteis porque podem ser usados para implementar políticas com um período de retenção específico para as cópias do SnapVault replicadas para o cluster secundário do ONTAP. Quando o SCV é usado com o NetApp Data Services, o campo de rótulo de Snapshot deve ficar em branco ou corresponder ao rótulo especificado na política de backup.

3. Repita o procedimento para cada política necessária. Por exemplo, políticas separadas para backups diários, semanais e mensais.

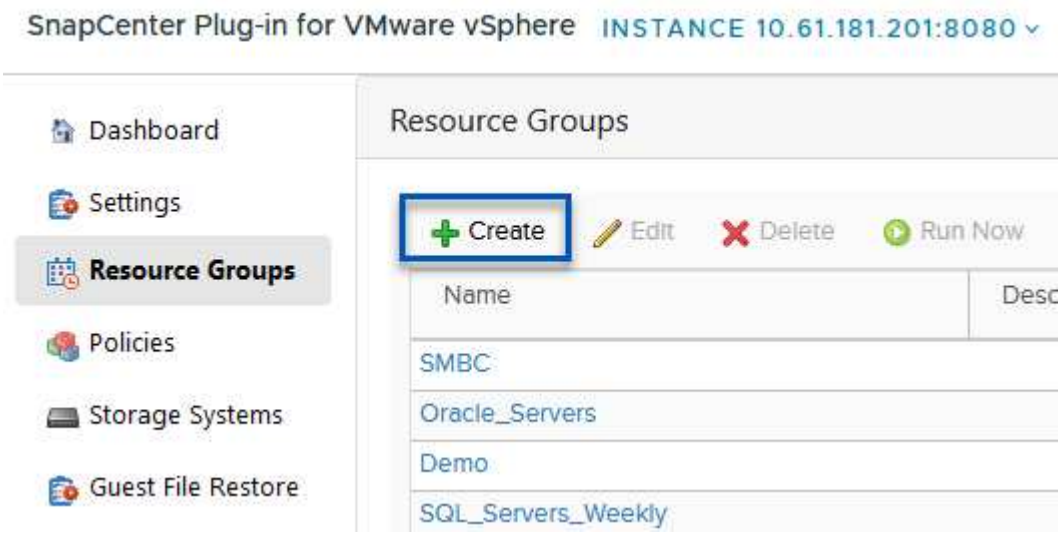
▼ **Criar grupos de recursos**

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.

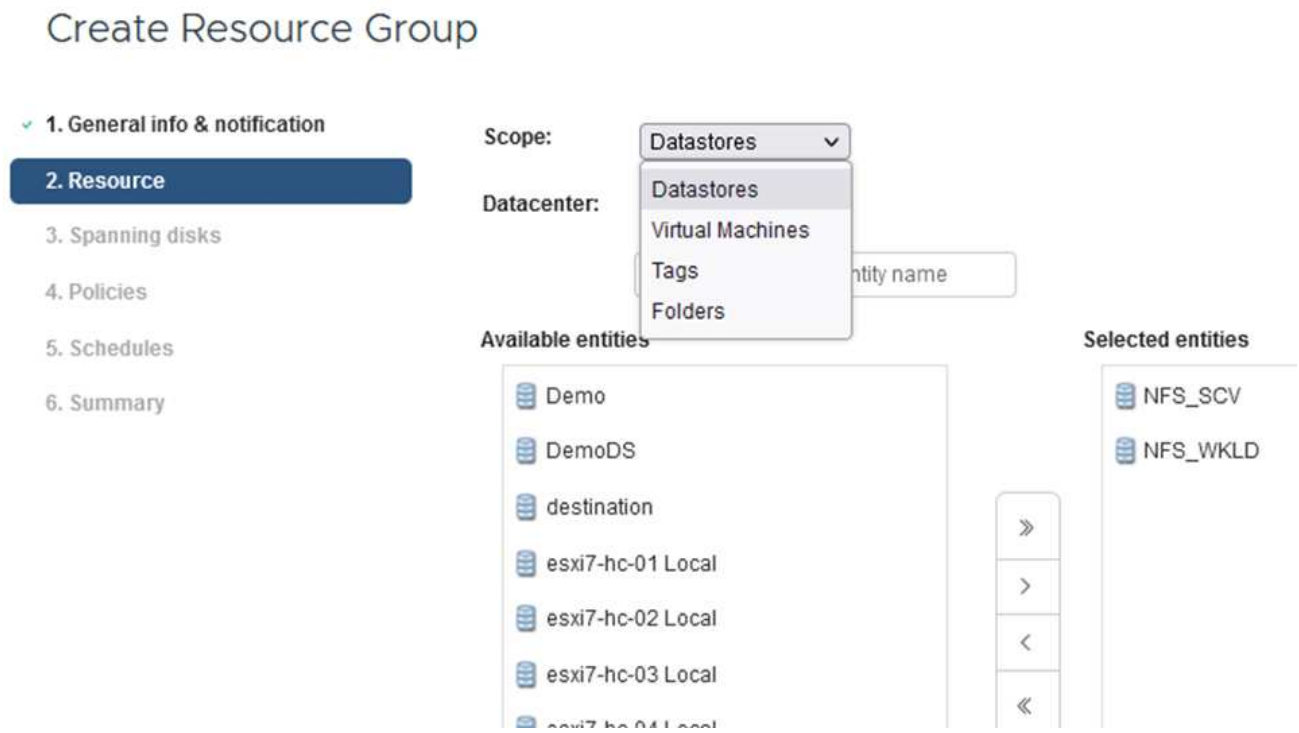
Revise o "Criar grupos de recursos" seção da documentação para mais informações.

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**.

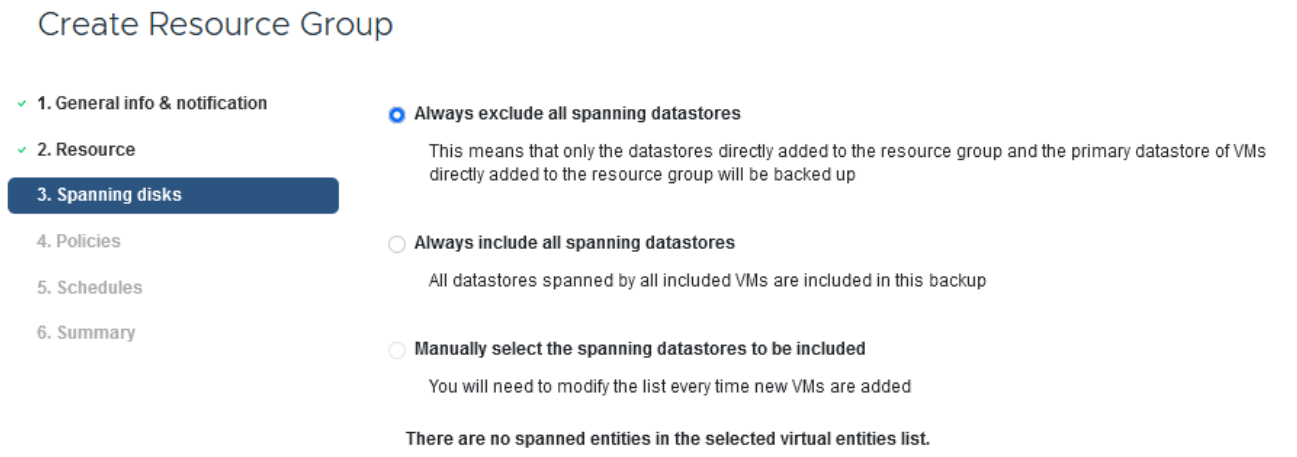


2. No assistente Criar grupo de recursos, insira um nome e uma descrição para o grupo, bem como as informações necessárias para receber notificações. Clique em **Avançar**
3. Na próxima página, selecione os armazenamentos de dados e máquinas virtuais que desejam ser incluídos na tarefa de backup e clique em **Avançar**.



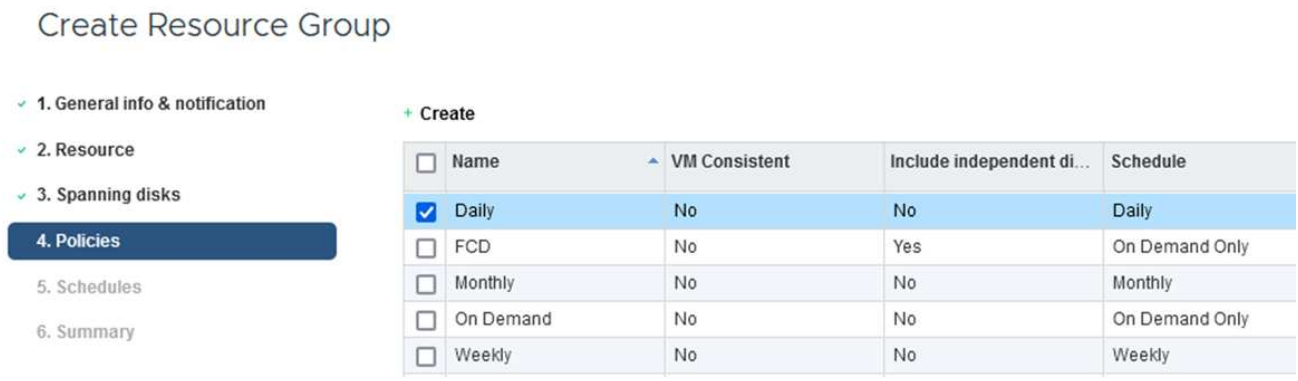
Você tem a opção de selecionar VMs específicas ou armazenamentos de dados inteiros. Independentemente de qual você escolher, todo o volume (e armazenamento de dados) será copiado, pois o backup é o resultado da criação de um instantâneo do volume subjacente. Na maioria dos casos, é mais fácil escolher 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**.



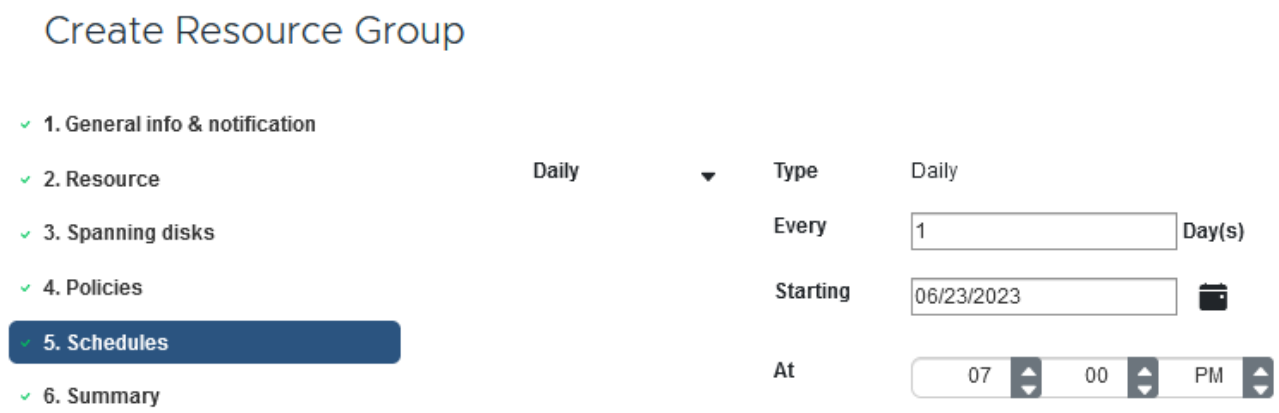
Atualmente, o backup e recuperação para proteger cargas de trabalho do VMware não oferece suporte ao backup de VMs com VMDKs que abrangem vários datastores.

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 storage de objetos usando o 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**.

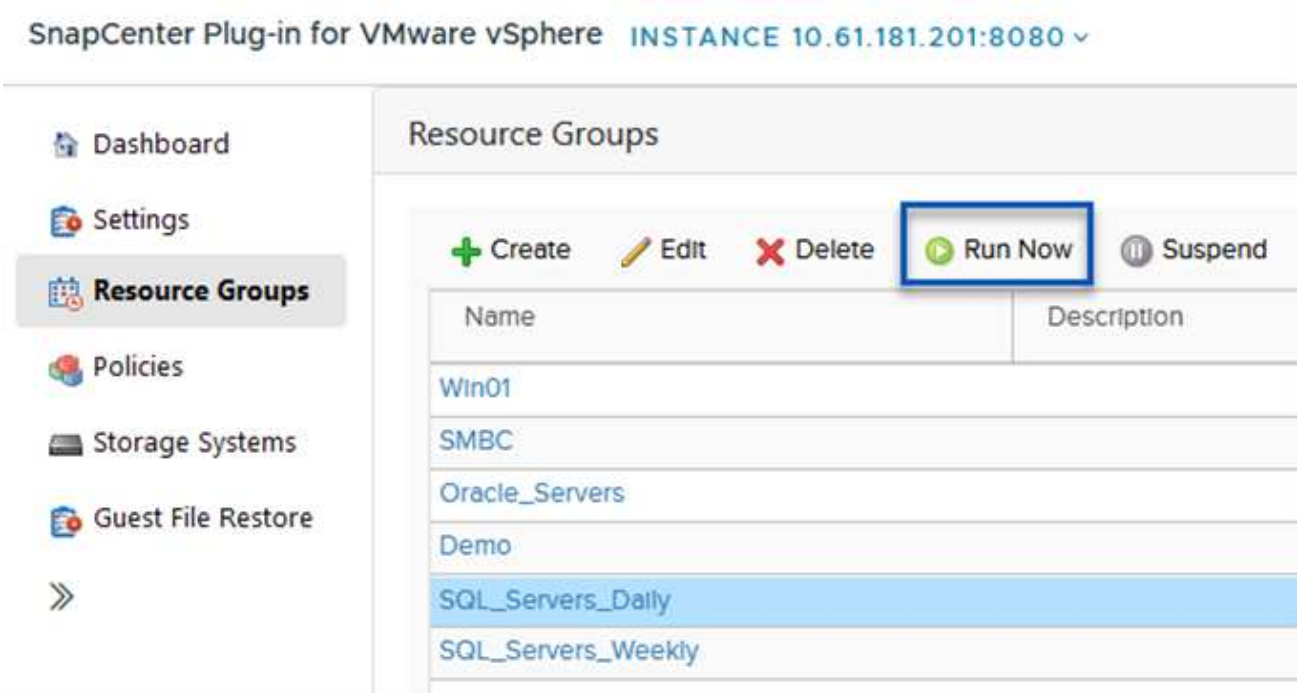


7. Por fim, revise a página de resumo e clique em **Concluir** para finalizar a criação do grupo de recursos.

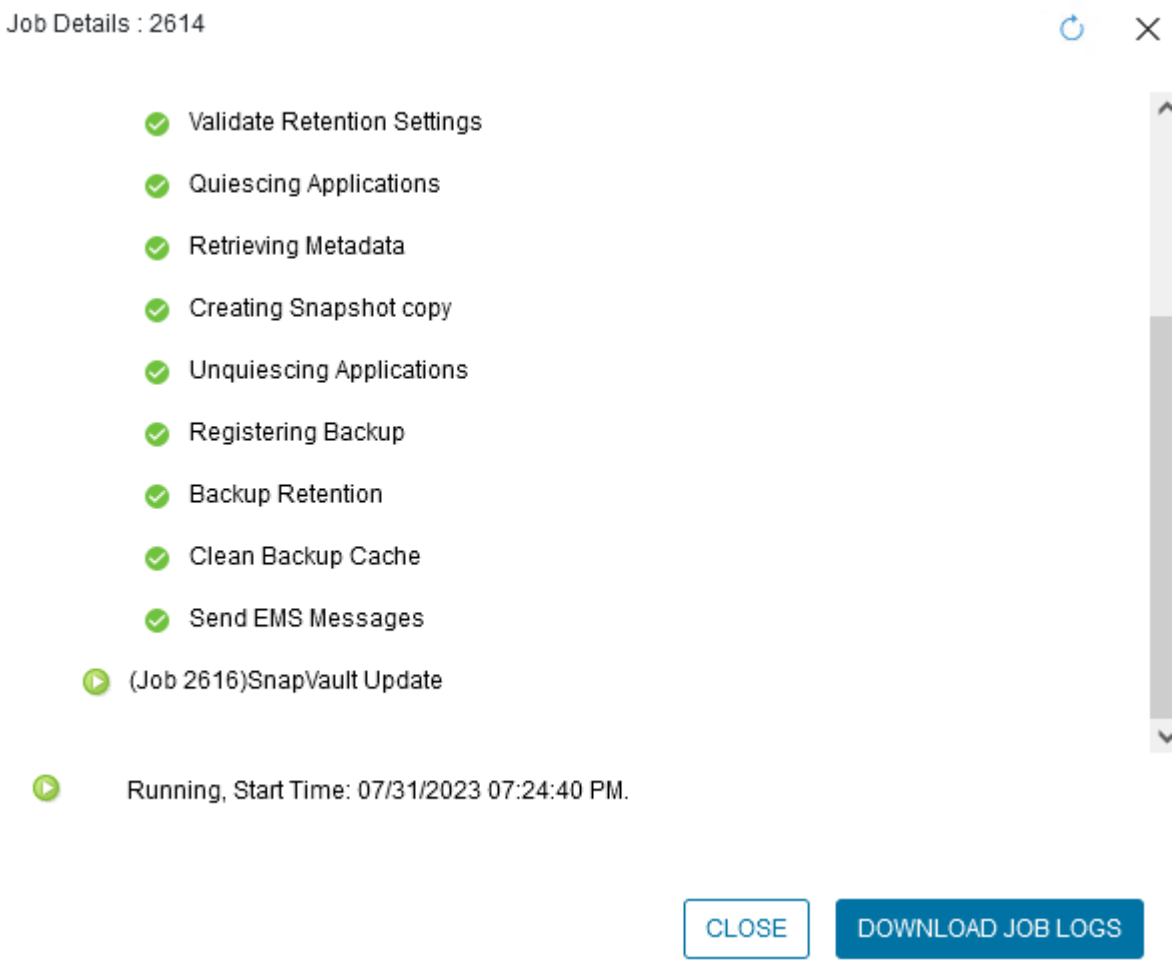
▼ **Executar uma tarefa de backup**

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 a partir do NetApp Console.

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.



Configure backups para storage de objetos no NetApp Console

Para que o NetApp Console gerencie a infraestrutura de dados de forma eficaz, ele requer a instalação prévia de um agente do Console. O agente do Console executa as ações envolvidas na descoberta de recursos e no gerenciamento de operações de dados.

Para obter mais informações sobre o agente do Console, consulte "Saiba mais sobre os agentes do Console" na documentação do NetApp Console.

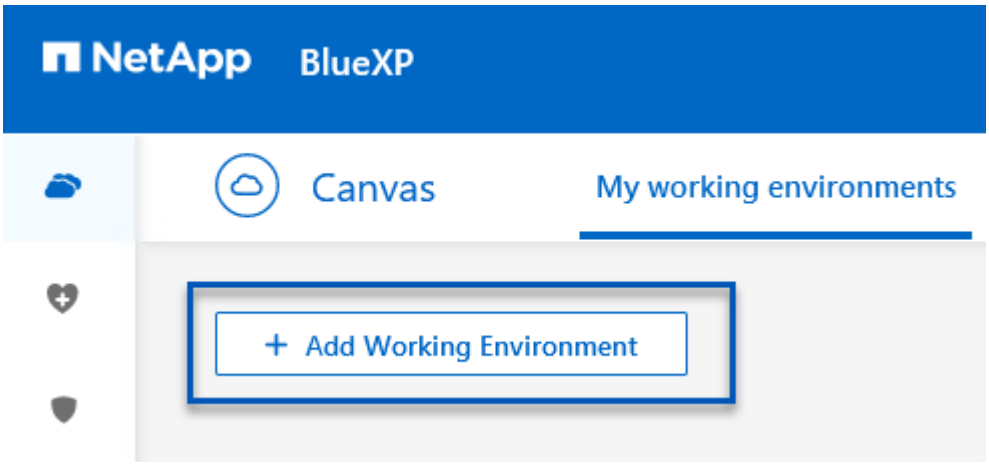
Após instalar o agente do provedor de nuvem utilizado, você poderá ver uma representação gráfica do storage de objetos em Systems.

Para configurar o Backup and Recovery para fazer backup de dados gerenciados pelo SCV no local, siga estas etapas:

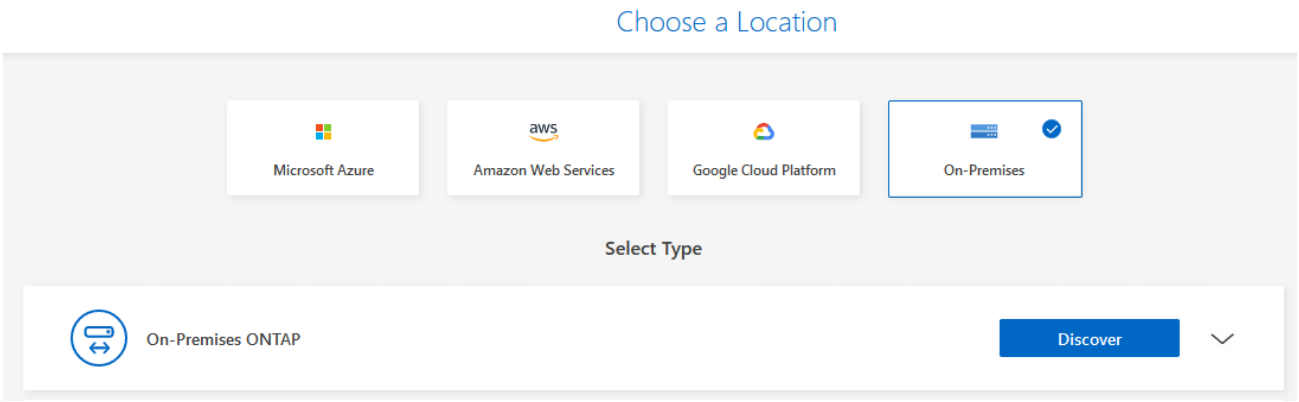
▼ **Adicionar o sistema de storage ONTAP ao Systems**

O primeiro passo é adicionar os sistemas de storage ONTAP locais ao NetApp Console.

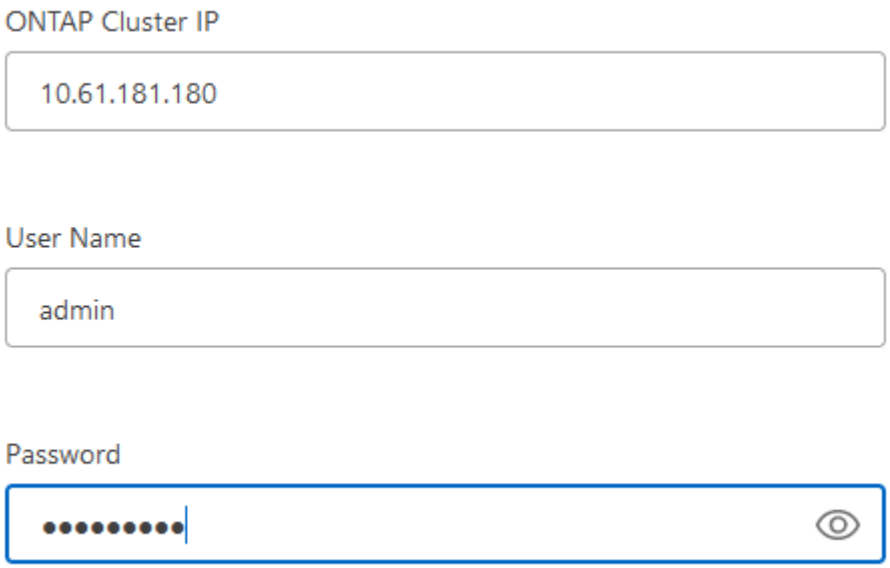
1. Na seção Systems, clique em **+ Add** para começar.



2. Selecione **No local** entre as opções de locais e clique no botão **Descobrir**.



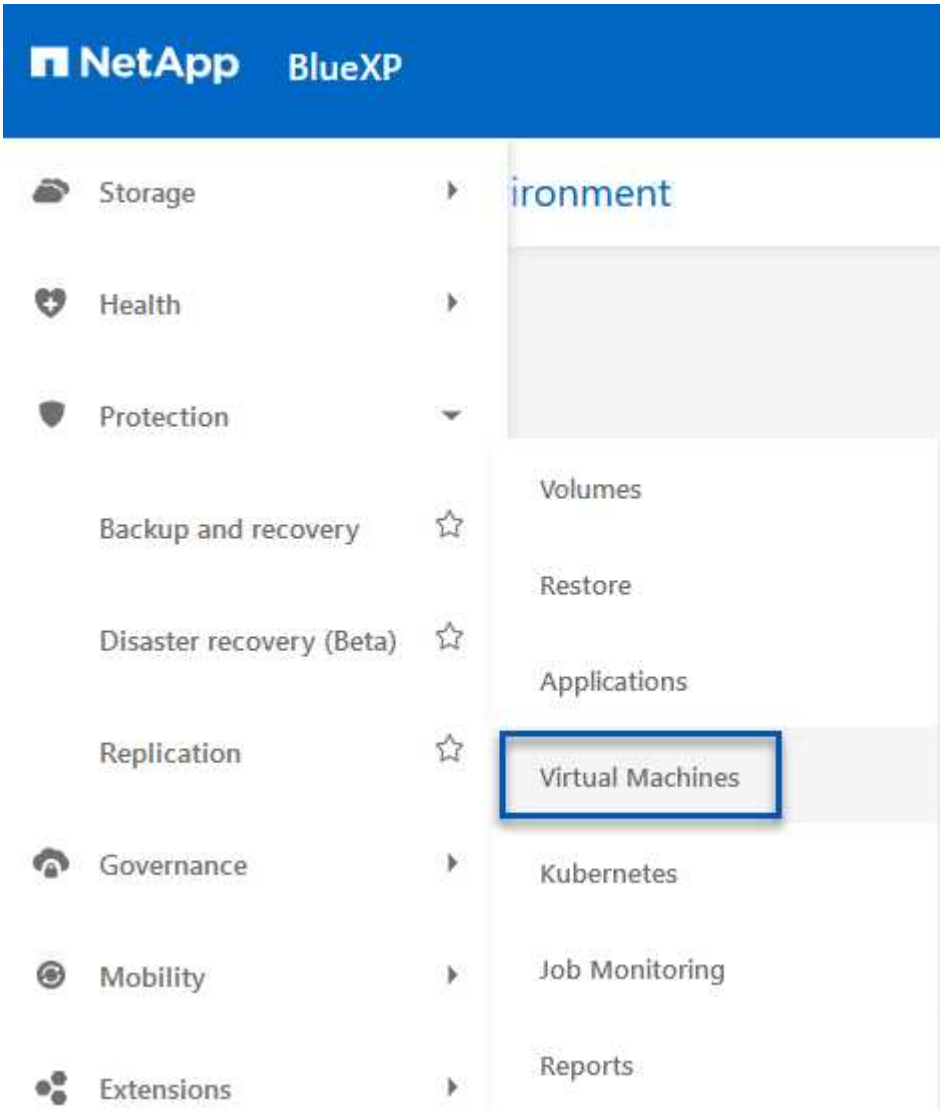
3. Preencha as credenciais do sistema de armazenamento ONTAP e clique no botão **Descobrir** para adicionar o ambiente de trabalho.



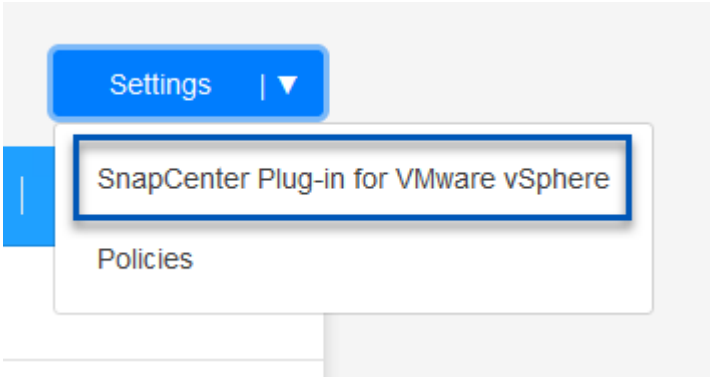
▼ Descubra o dispositivo SCV local e o vCenter

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.

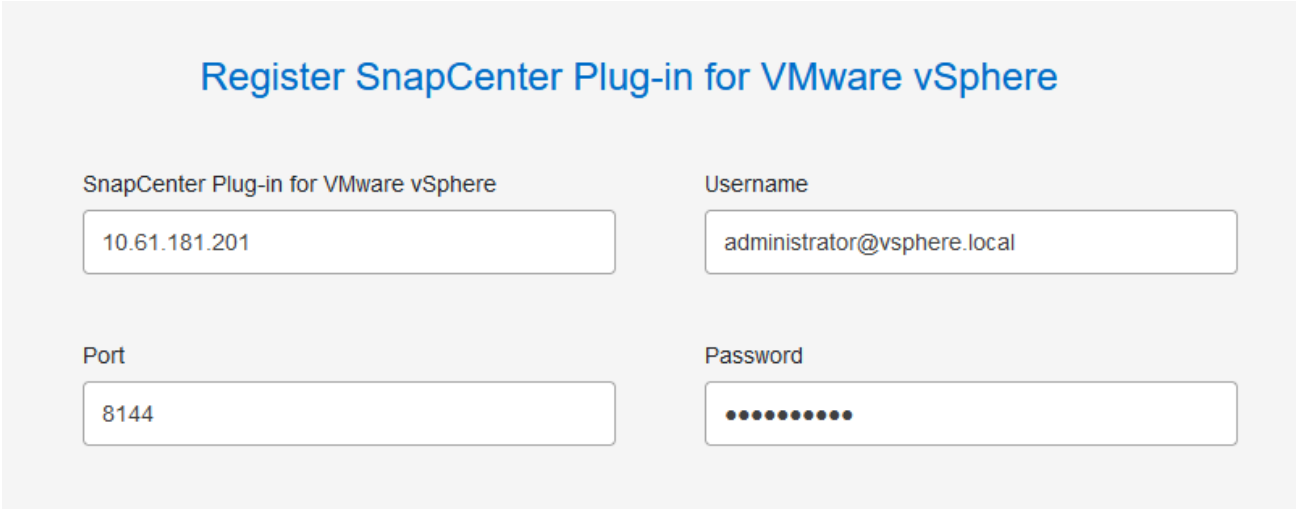
1. No menu à esquerda do NetApp Console, selecione **Proteção > Backup e recuperação > Cargas de trabalho > VMware**.



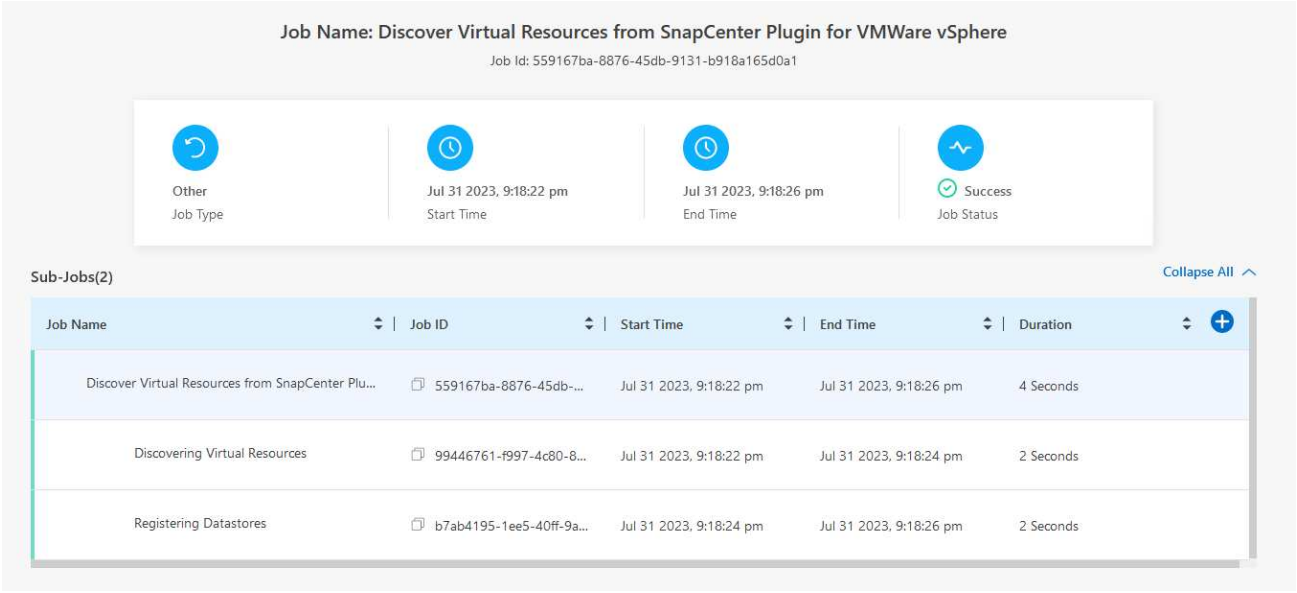
2. Na tela principal Máquinas Virtuais, acesse o menu suspenso **Configurações** e selecione * SnapCenter Plug-in for VMware vSphere*.



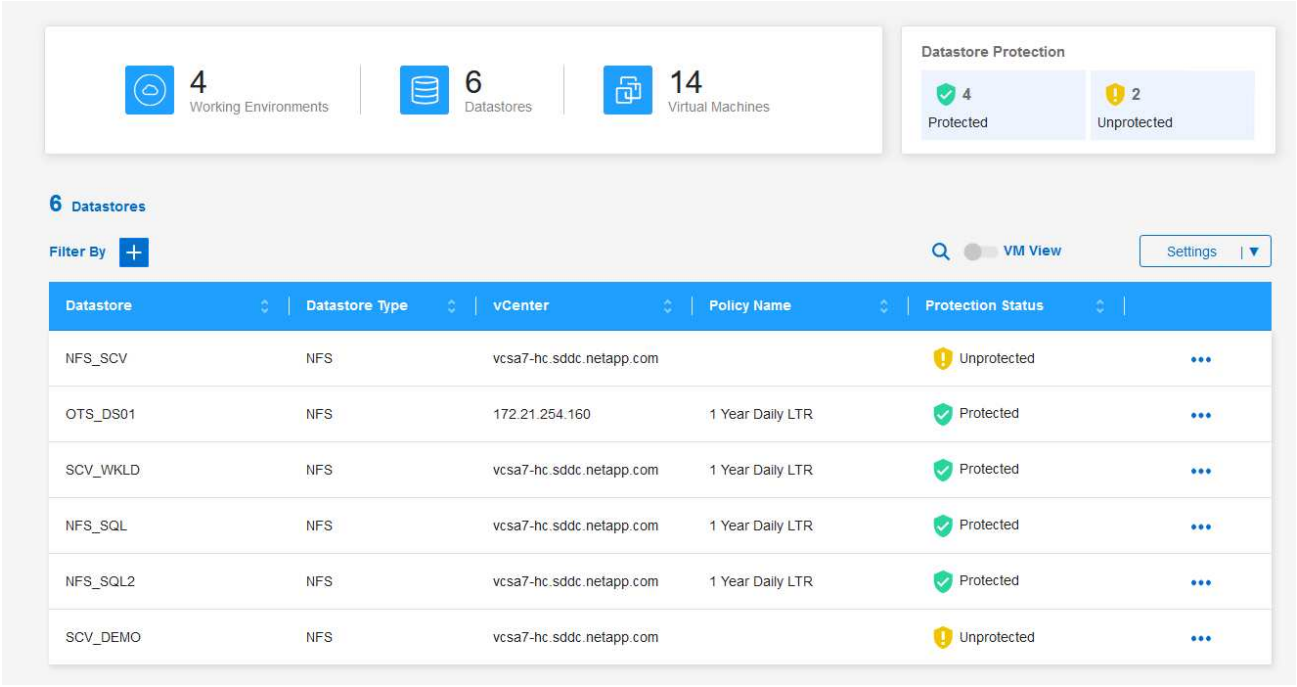
3. Clique no botão **Registrar** e insira o endereço IP e o número da porta do dispositivo SnapCenter Plug-in e o nome de usuário e a senha do dispositivo de gerenciamento vCenter. Clique no botão **Registrar** para iniciar o processo de descoberta.



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.

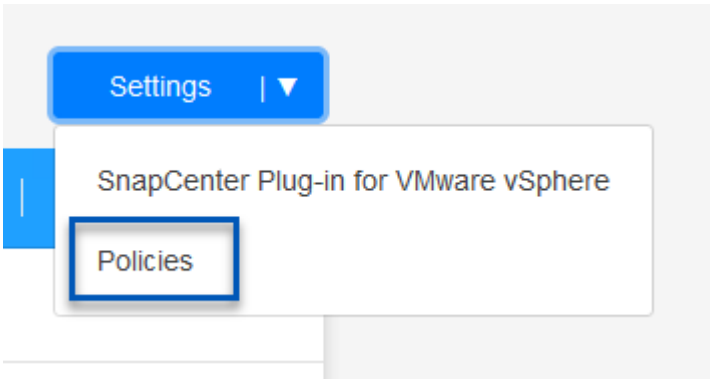


▼ Criar políticas de backup

No NetApp Backup and Recovery for Virtual Machines, 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 grupos de proteção, consulte "Criar um grupo de proteção".

1. Na página principal do NetApp Backup and Recovery for Virtual Machines, acesse o menu suspenso **Settings** e selecione **Policies**.



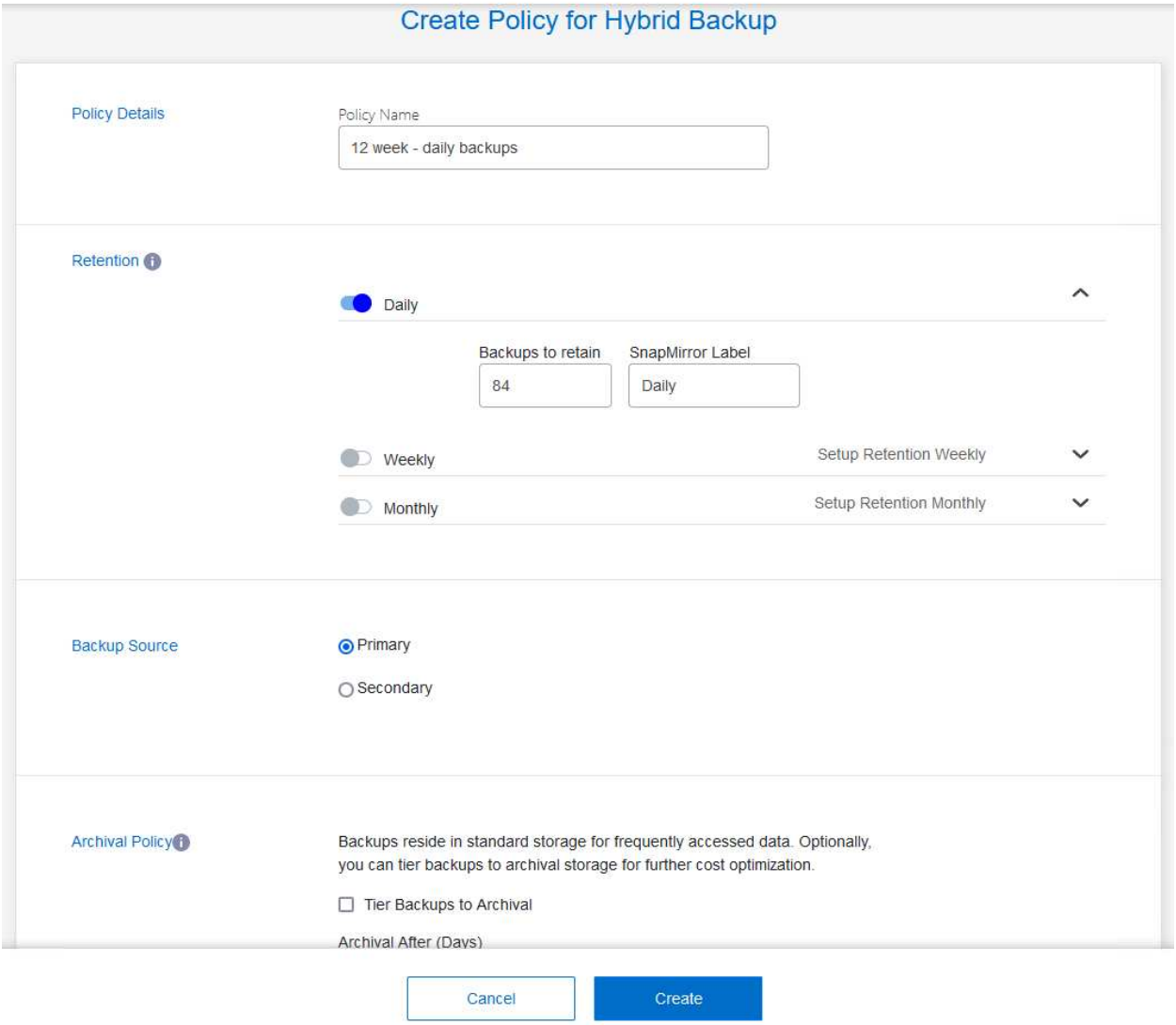
2. Clique em **Criar política** para acessar a janela **Criar política para backup híbrido**.

   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.

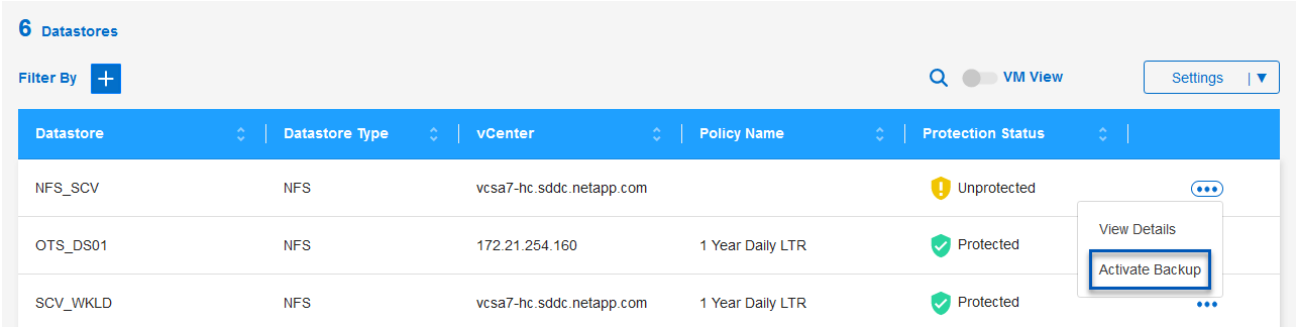
3. Clique em **Criar** para concluir a criação da política.

▼ **Fazer backup de datastores para Amazon Web Services**

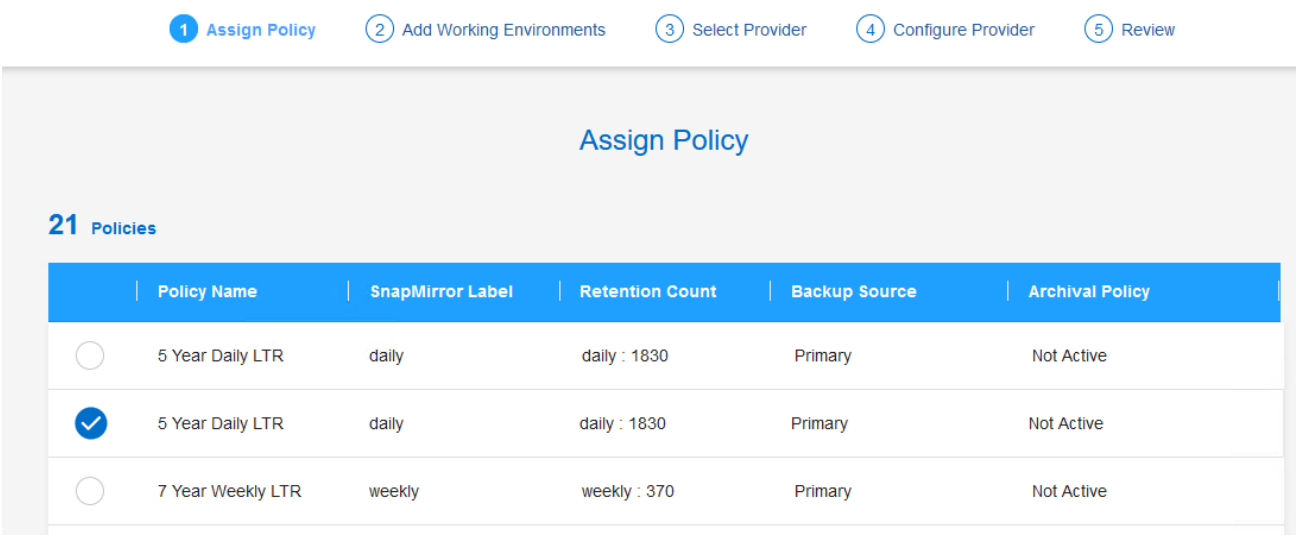
A etapa final é ativar a proteção de dados para os armazenamentos de dados e máquinas virtuais individuais. As etapas a seguir descrevem como ativar backups na AWS.

Para obter mais informações, consulte "Faça backup das cargas de trabalho do VMware".

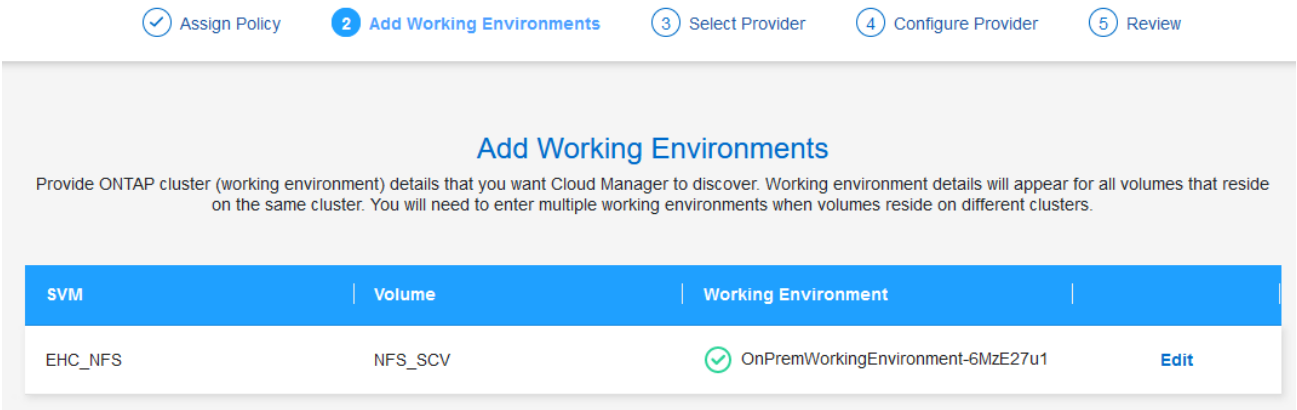
1. Na página principal do NetApp Backup and Recovery for Virtual Machines, acesse o menu suspenso de configurações do datastore para o qual você deseja fazer backup e selecione **Activate Backup**.



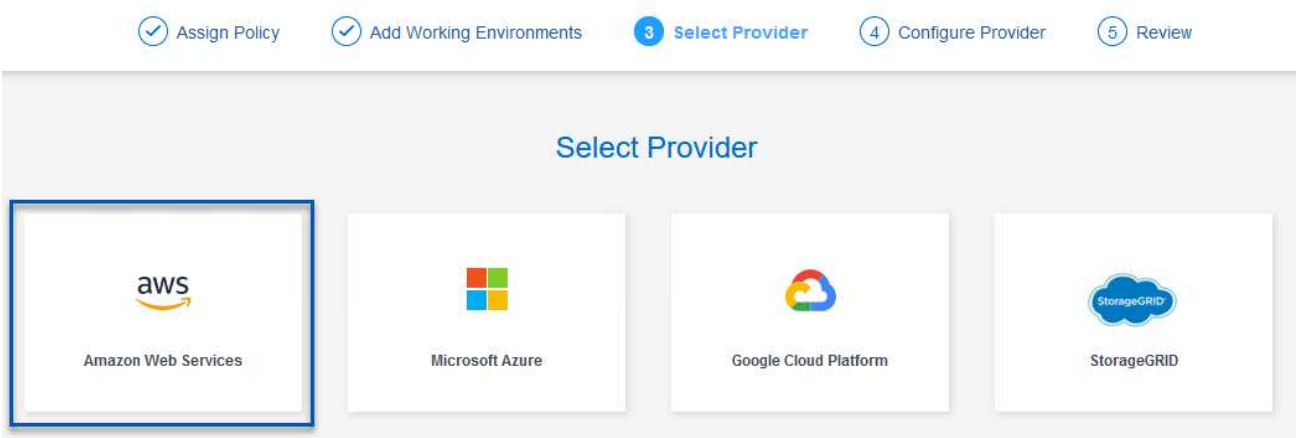
2. Atribua a política a ser usada para a operação de proteção de dados e clique em **Avançar**.



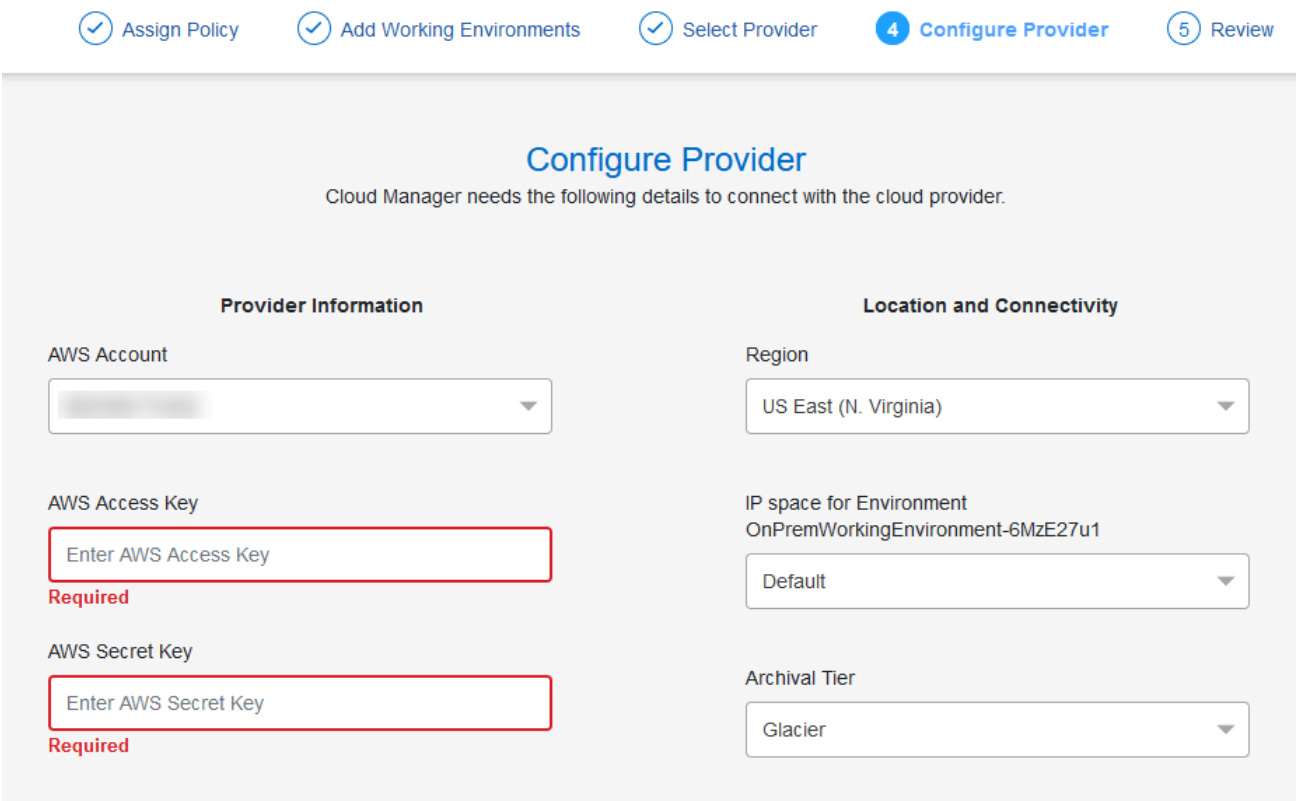
3. Na página **Adicionar ambientes de trabalho**, o armazenamento de dados e o ambiente de trabalho com uma marca de seleção devem aparecer se o ambiente de trabalho já tiver sido descoberto anteriormente. Se o ambiente de trabalho não tiver sido descoberto anteriormente, você pode adicioná-lo aqui. Clique em **Avançar** para continuar.



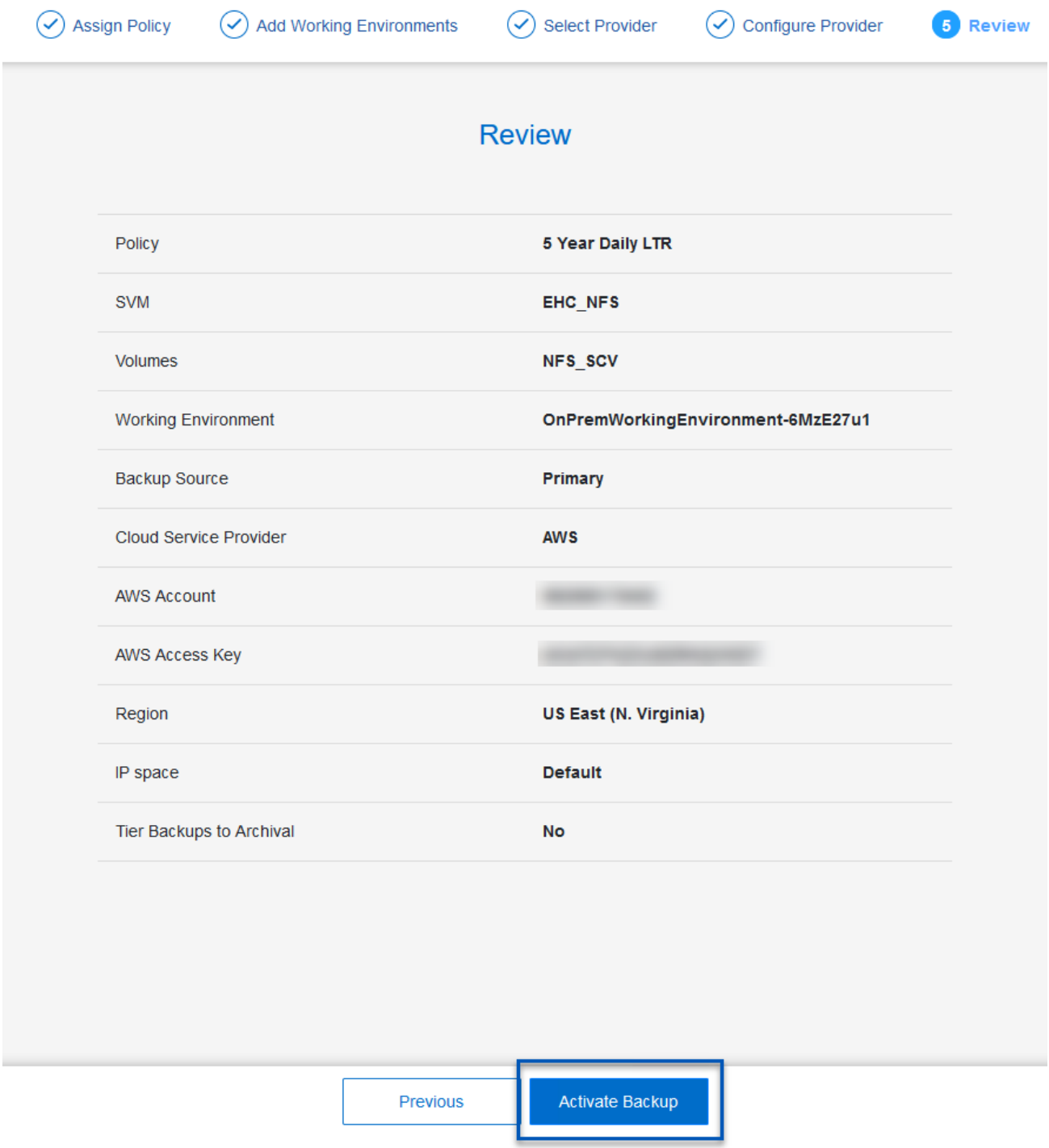
4. Na página **Selecionar provedor**, clique em AWS e depois clique no botão **Avançar** para continuar.



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 NetApp Backup and Recovery verifica a cada hora se há snapshots pendentes e, em seguida, os transfere para o storage 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 tanto do SnapCenter Plug-in for VMware vSphere quanto do NetApp Backup and Recovery para máquinas virtuais.

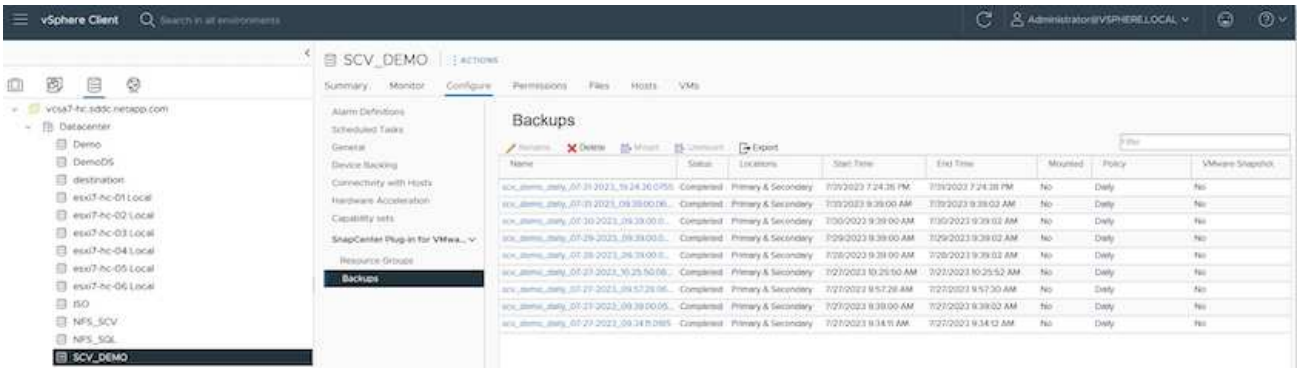
Restaurando máquinas virtuais do SnapCenter Plug-in for VMware vSphere

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.

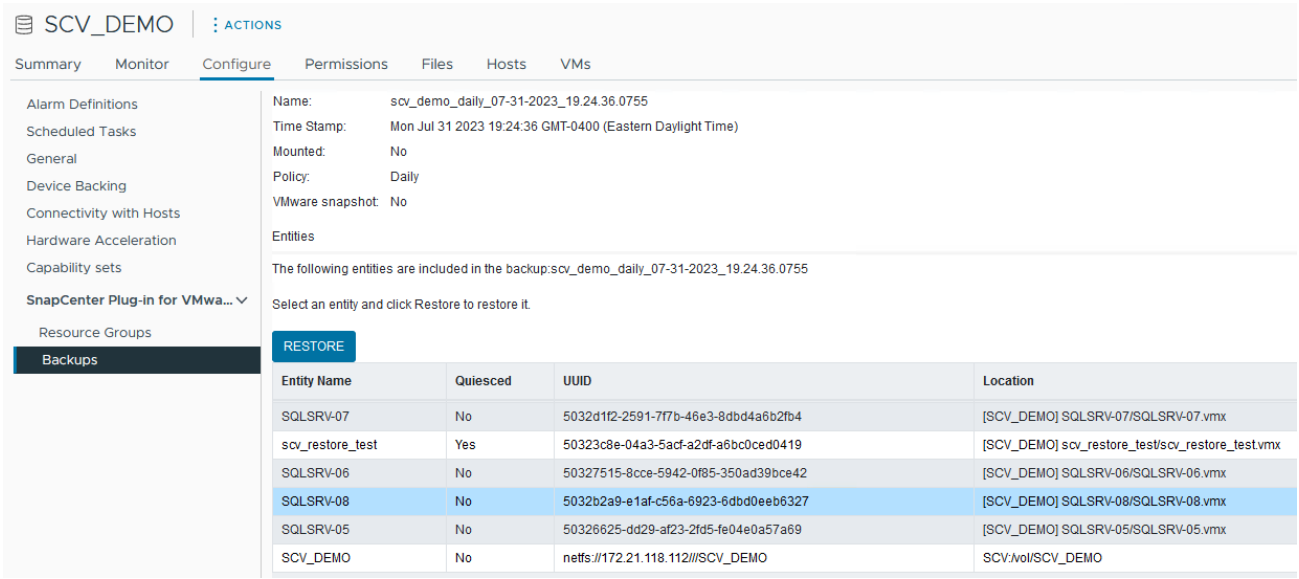
▼ Restaurar máquinas virtuais do SCV

Conclua as etapas a seguir para restaurar uma máquina virtual do armazenamento primário ou secundário.

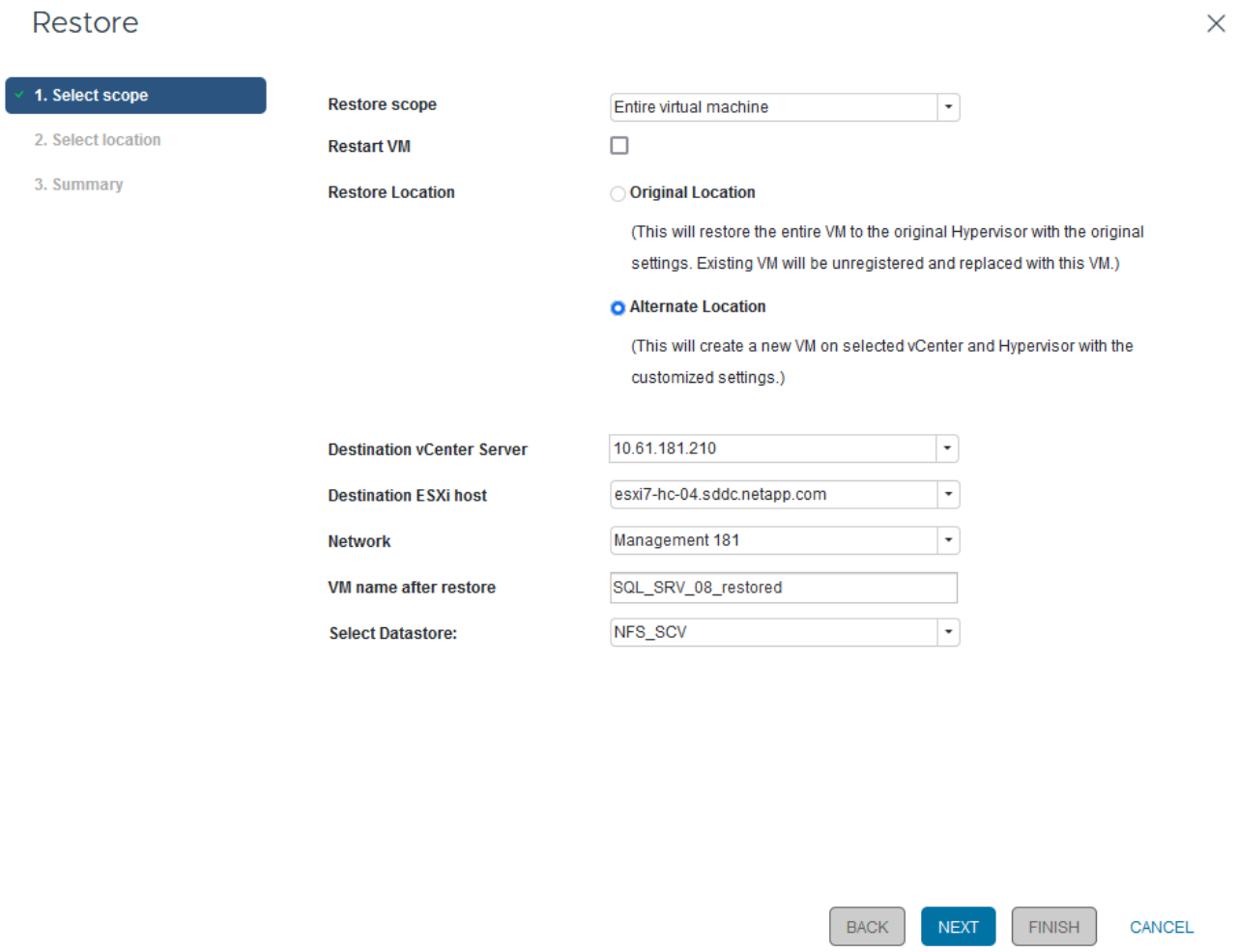
1. No cliente vCenter, navegue até **Inventário > Armazenamento** e clique no armazenamento de dados que contém as máquinas virtuais que você deseja restaurar.
2. Na aba **Configurar** clique em **Backups** para acessar a lista de backups disponíveis.



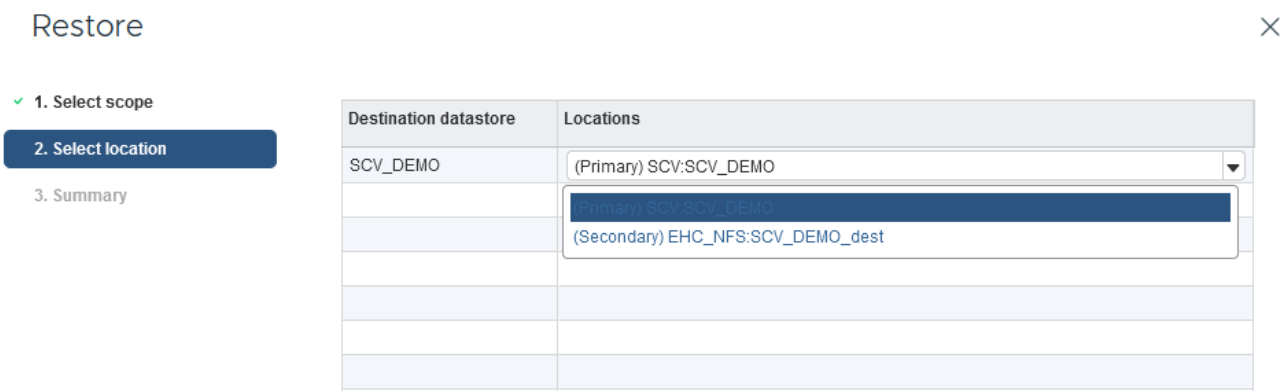
3. Clique em um backup para acessar a lista de VMs e selecione uma VM para restaurar. Clique em **Restaurar**.



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.

Restauração de máquinas virtuais do NetApp Backup and Recovery for Virtual Machines

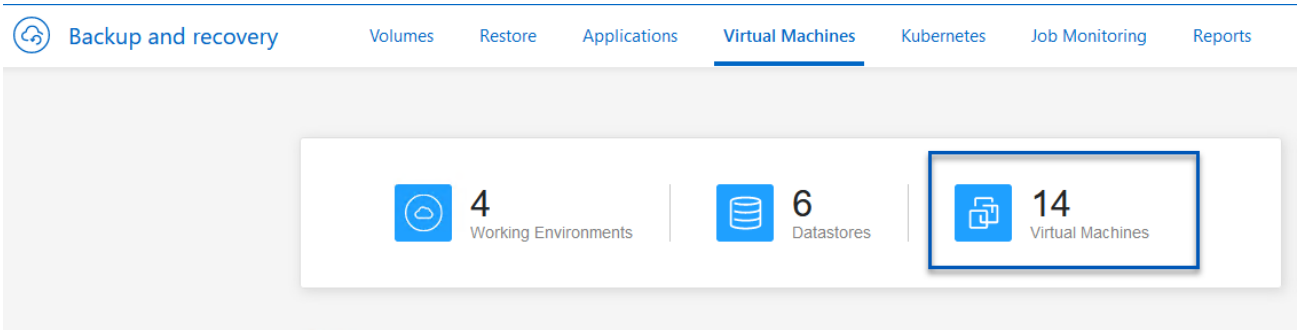
O NetApp Backup and Recovery for Virtual Machines permite restaurar máquinas virtuais para seu local original. As funções de restauração são acessadas por meio do console web do NetApp Backup and Recovery.

Para obter mais informações consulte "Restaurar dados de máquinas virtuais da nuvem".

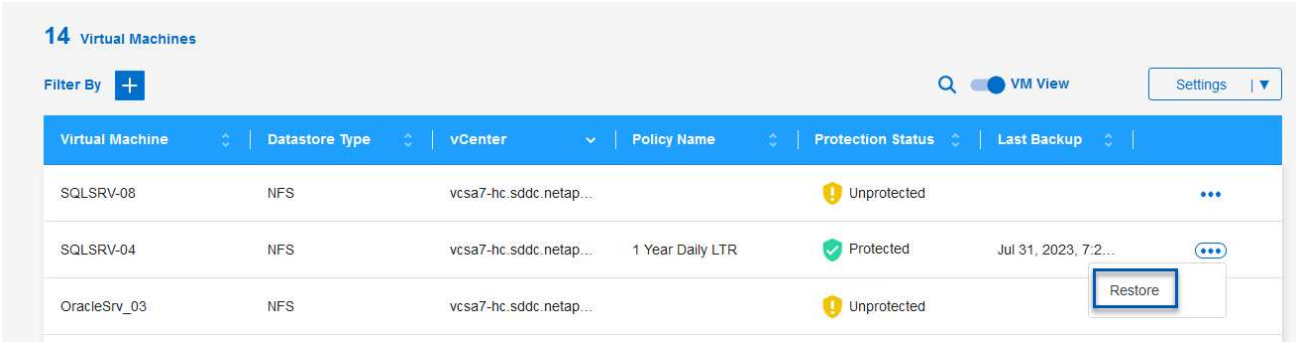
▼ **Restaurar máquinas virtuais do NetApp Backup and Recovery**

Para restaurar uma máquina virtual do NetApp Backup and Recovery, conclua as etapas a seguir.

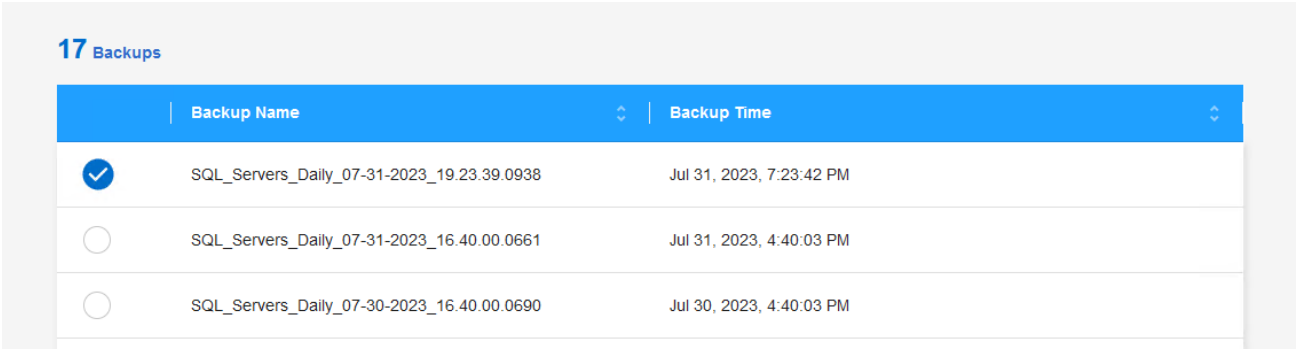
1. Navegue até **Proteção > Backup e recuperação > Máquinas virtuais** e clique em Máquinas virtuais para visualizar a lista de máquinas virtuais disponíveis para restauração.



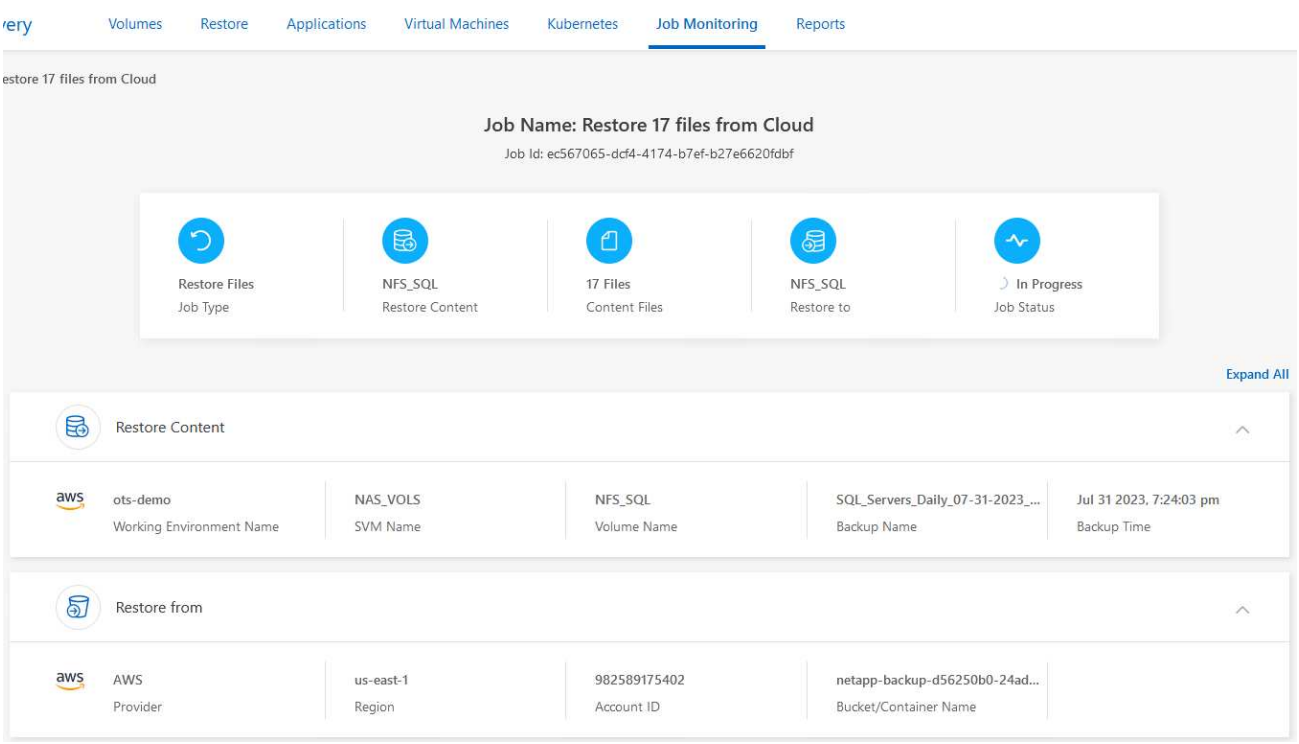
2. Acesse o menu suspenso de configurações da VM a ser restaurada e selecione



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 NetApp 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 dos dados, mas também oferece a flexibilidade de restaurar dados de qualquer local e tanto de sistemas de storage ONTAP locais quanto de storage de objetos baseado na nuvem.

O caso de uso apresentado nesta documentação concentra-se em tecnologias comprovadas de proteção de dados que destacam a integração entre NetApp, 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, monitoramento e operações de restauração flexíveis no ecossistema VMware. O NetApp Backup and Recovery para máquinas virtuais oferece o um (1) em 3-2-1 ao fornecer backups seguros, air-gapped, de dados de máquinas virtuais para storage de objetos baseado em nuvem. A interface intuitiva e o fluxo de trabalho lógico fornecem uma plataforma segura para o 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"
- "NetApp Console documentação"

O NetApp Disaster Recovery

Visão geral

A recuperação de desastres é uma preocupação primordial na mente de todos os

administradores do VMware. Como o VMware encapsula servidores inteiros em uma série de arquivos que compõem a máquina virtual, os administradores aproveitam técnicas baseadas em armazenamento em bloco, como clones, snapshots e réplicas, para proteger essas VMs. Os arrays do ONTAP oferecem replicação incorporada para transferir dados de volume e, portanto, as máquinas virtuais residentes nos LUNs de datastore designados, de um site para outro. O NetApp Disaster Recovery integra-se ao vSphere e automatiza todo o fluxo de trabalho para failover e failback contínuos em caso de desastre. Ao combinar a replicação de storage com a automação inteligente, os administradores agora têm uma maneira gerenciável não apenas de configurar, automatizar e testar planos de recuperação de desastres, mas também os meios para executá-los facilmente em caso de desastre.

As partes mais demoradas de um failover de DR em um ambiente VMware vSphere são a execução das etapas necessárias para inventariar, registrar, reconfigurar e ligar as VMs no site de DR. Uma solução ideal tem um RPO baixo (medido em minutos) e um RTO baixo (medido em minutos a horas). Um fator que muitas vezes é negligenciado em uma solução de DR é a capacidade de testar a solução de DR de forma eficiente em um intervalo periódico.

Para arquitetar uma solução de DR, tenha em mente os seguintes fatores:

- O objetivo do tempo de recuperação (RTO). O RTO é a rapidez com que uma empresa pode se recuperar de um desastre ou, mais especificamente, quanto tempo leva para executar o processo de recuperação para tornar os serviços empresariais disponíveis novamente.
- O objetivo do ponto de recuperação (RPO). O RPO é a idade dos dados recuperados depois de terem sido disponibilizados, em relação ao momento em que o desastre ocorreu.
- Escalabilidade e adaptabilidade. Esse fator inclui a capacidade de aumentar os recursos de armazenamento gradualmente conforme a demanda aumenta.

Para mais informações técnicas sobre as soluções disponíveis, consulte:

- "NetApp Disaster Recovery para Datastores NFS"
- "NetApp Disaster Recovery para datastores VMFS"

NetApp Disaster Recovery para Datastores NFS

NetApp Disaster Recovery para Datastores NFS

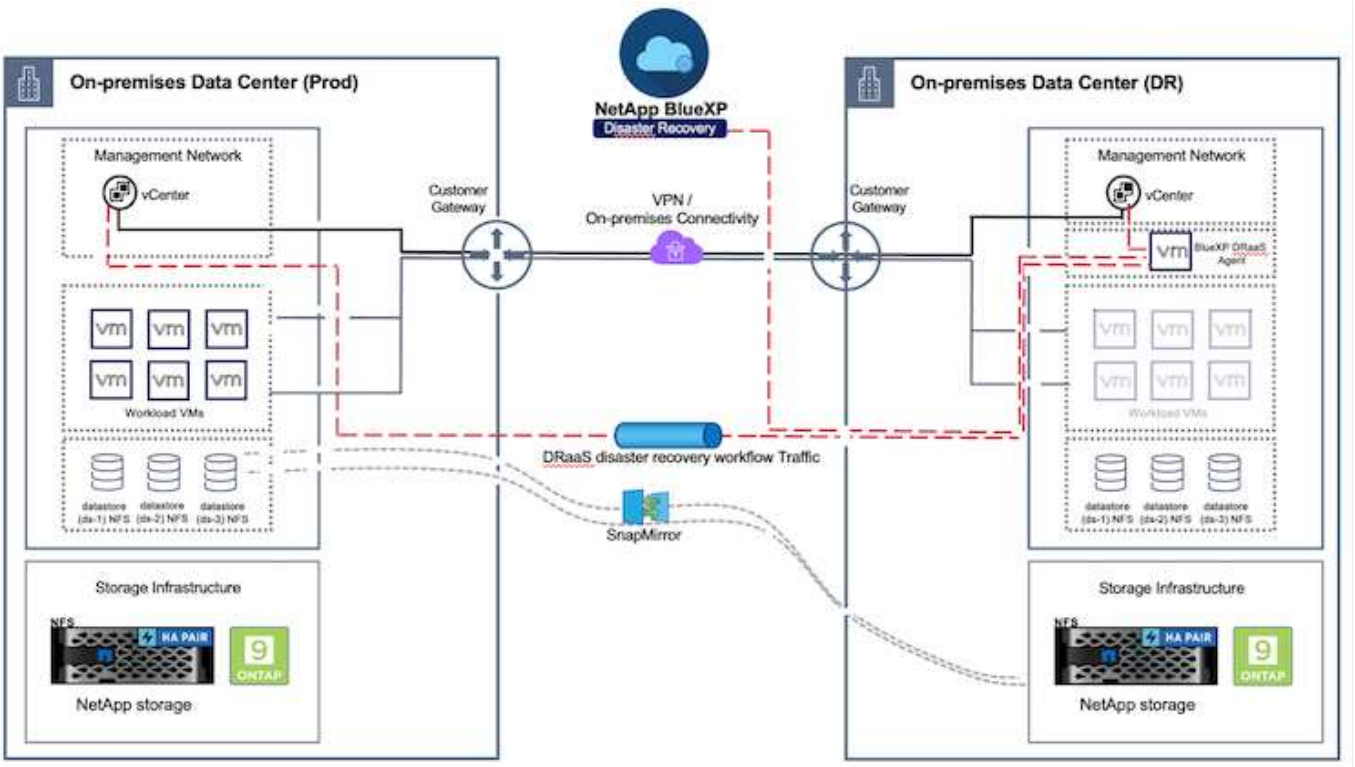
Implementar a recuperação de desastres por meio de replicação em nível de bloco do site de produção para o site de recuperação de desastres é um método resiliente e econômico para proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados, como ataques de ransomware. Usando 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.

Esta seção do documento descreve a configuração do NetApp Disaster Recovery para configurar a recuperação de desastres de VMs VMware no local para outro site designado. Como parte dessa configuração, o Console agent, o onboarding dos arrays ONTAP, o Defining Sites e a associação do VMware

vCenter. 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 realizar um failover completo do site e como fazer o failback quando o site primário for recuperado e colocado online.

Utilizando o Disaster Recovery, parte do NetApp Data Services, as empresas podem descobrir facilmente seus VMware vCenters locais e o storage ONTAP. As organizações podem então criar grupos de recursos, criar um plano de recuperação de desastres, associá-lo aos grupos de recursos e testar ou executar failover e failback. SnapMirror fornece replicação de blocos no nível de storage para manter os dois sites atualizados com mudanças incrementais, resultando em um Recovery Point Objective (RPO) de até 5 minutos. Além disso, é possível simular procedimentos de recuperação de desastres sem afetar a produção nem gerar custos adicionais de storage.

O Disaster Recovery utiliza a tecnologia FlexClone do ONTAP para criar uma cópia com uso eficiente de espaço do datastore NFS a partir da última cópia Snapshot replicada 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 Disaster Recovery orquestra todas as etapas necessárias para ativar automaticamente as máquinas virtuais protegidas no site de recuperação de desastres designado com apenas alguns cliques. O serviço também reverterá a relação do SnapMirror para o site primário e replicará quaisquer alterações do secundário para o primário para uma operação de failback, quando necessário. Todos esses recursos têm um custo muito menor em comparação com outras alternativas bem conhecidas.

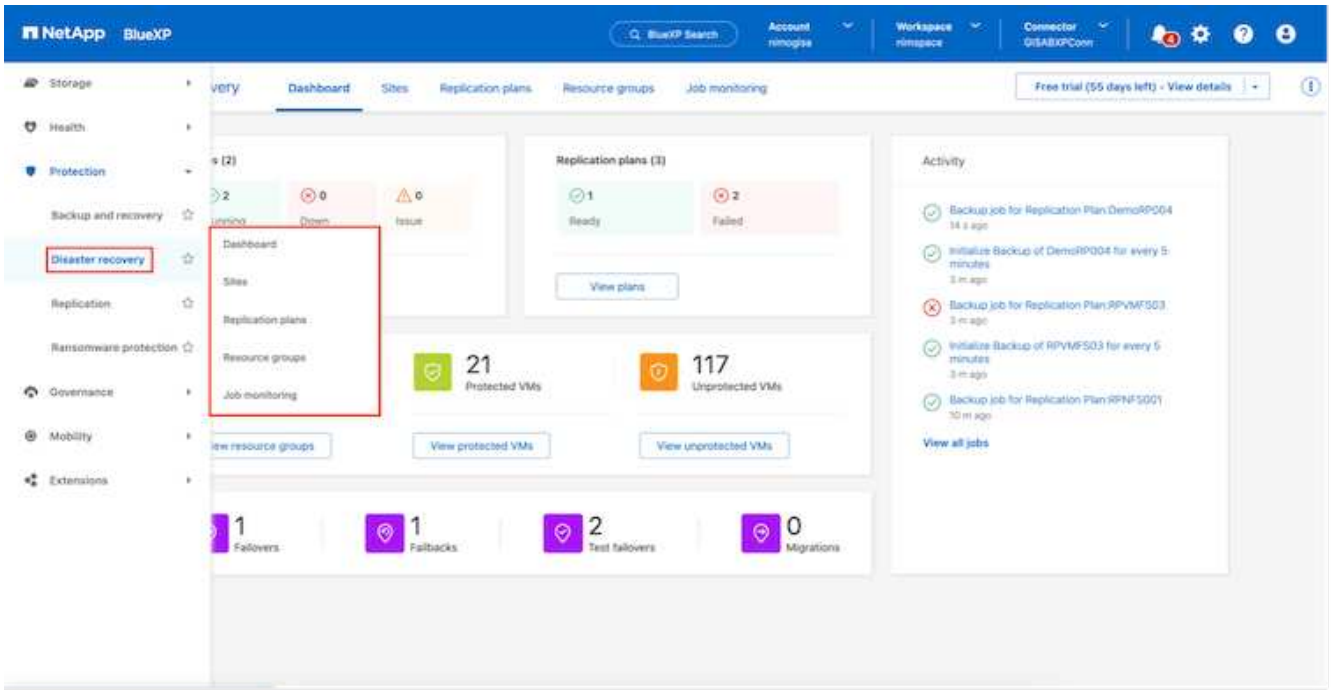


Para obter informações atualizadas e versões compatíveis do vCenter Server, do ESXi e do ONTAP for Disaster Recovery, consulte o "Configurações suportadas para recuperação de desastres".

Começando

Para começar a usar o NetApp Disaster Recovery, use o console da NetApp e acesse o serviço.

1. Faça login no Console.
2. Na navegação à esquerda do Console, selecione Protection > Disaster Recovery.
3. O painel de recuperação de desastres é exibido.

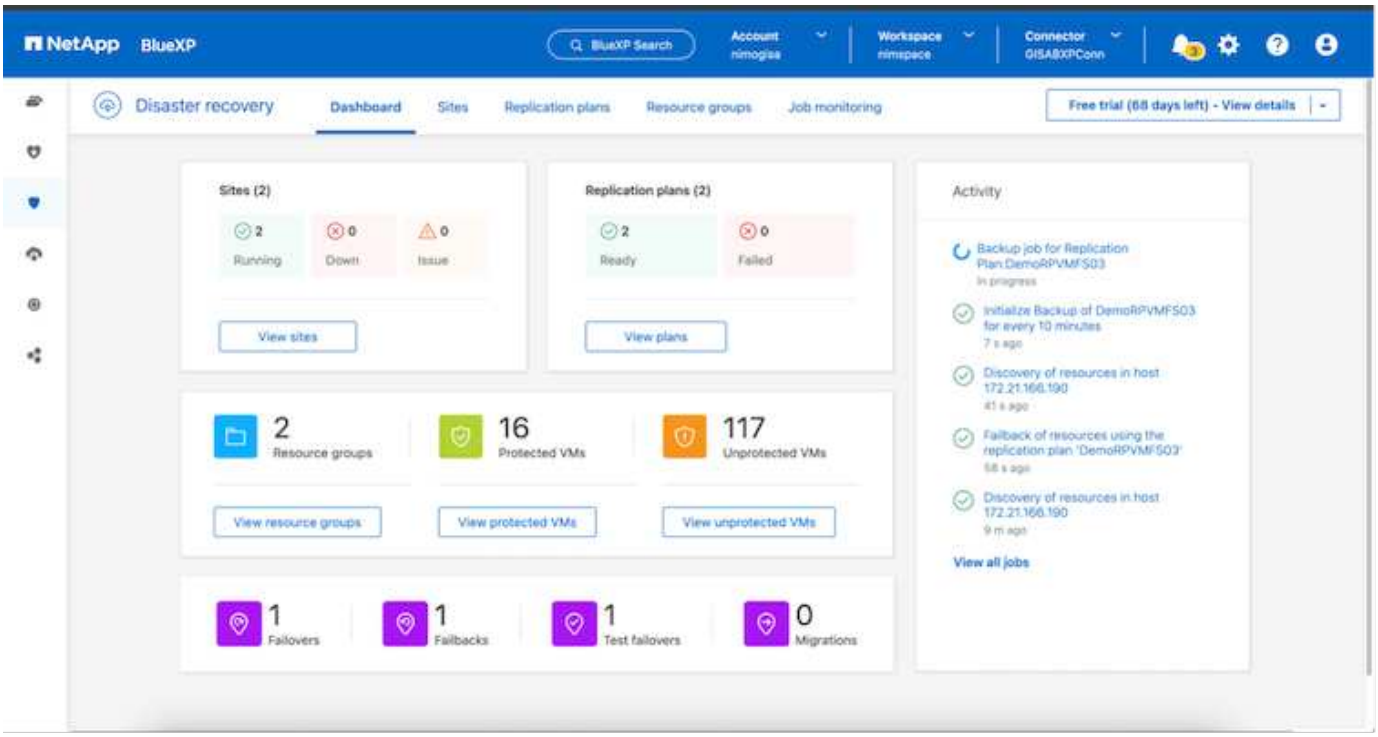


Antes de configurar o plano de recuperação de desastres, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O agente do Console está implantado.
- O agente tem conectividade com o vCenter de origem e de destino e os sistemas de storage.
- O cluster ONTAP com SVM com serviço NFS habilitado está disponível.
- Os sistemas de storage locais da NetApp que hospedam datastores NFS para VMware são adicionados no Console.
- 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.

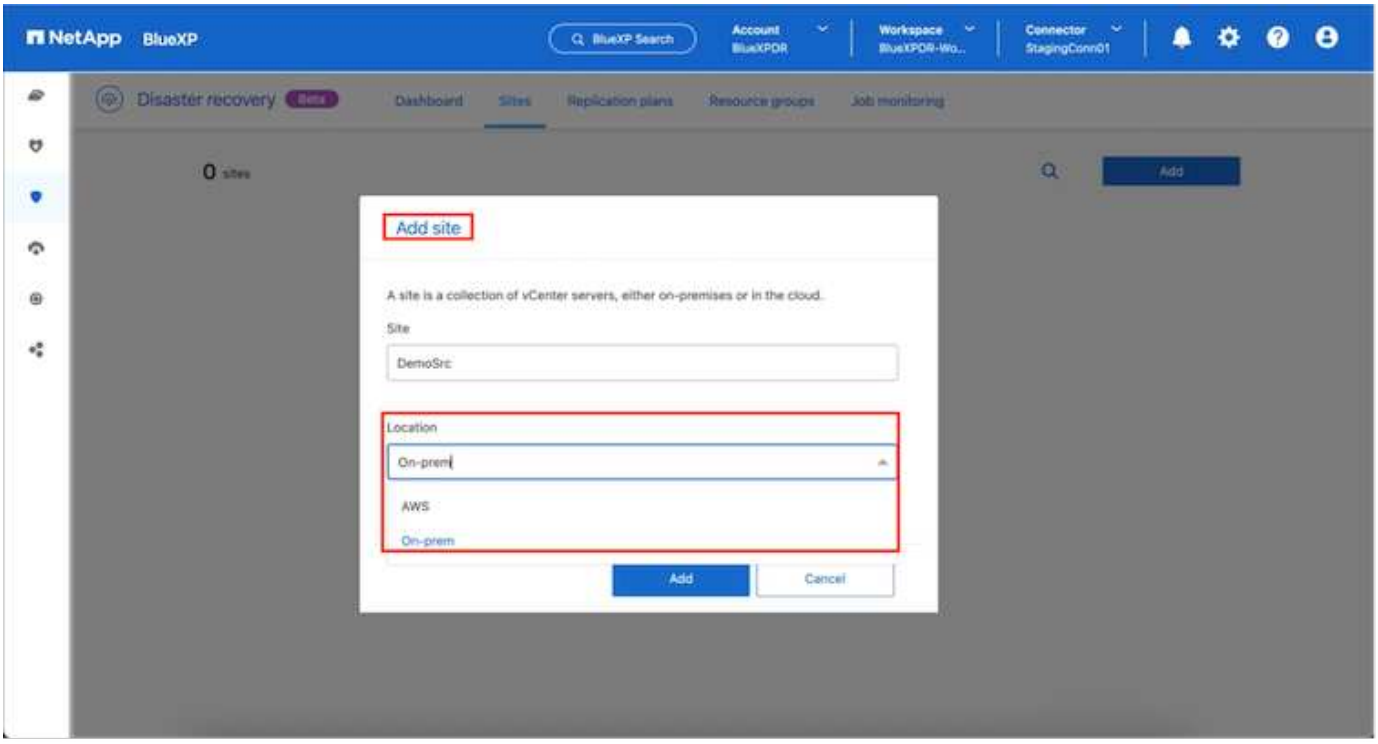
NetApp recomenda implantar o agente do Console no site de destino ou em um terceiro site, para que o agente do Console possa se comunicar pela rede com os recursos de origem e destino.



Configuração do NetApp Disaster Recovery

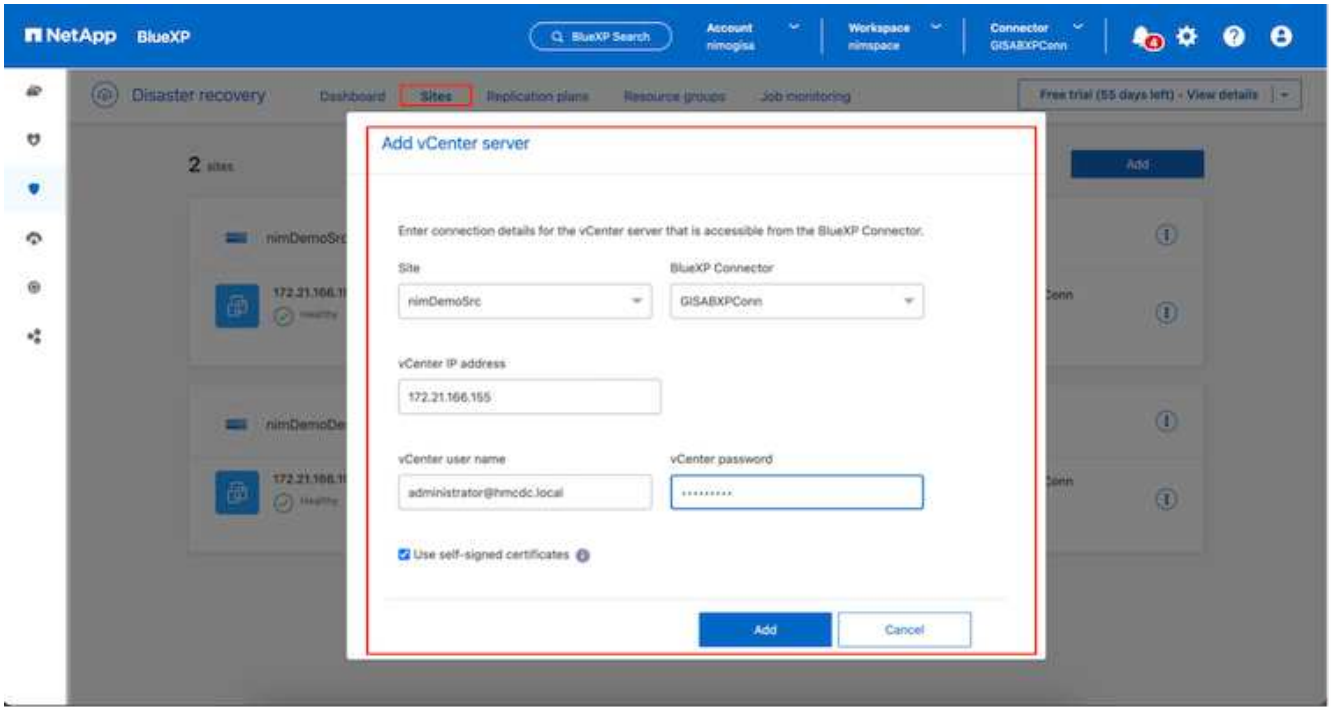
O primeiro passo na preparação para a recuperação de desastres é descobrir e adicionar o vCenter local e os recursos de storage ao NetApp Disaster Recovery.

Abra o Console e selecione **Proteção > Recuperação de Desastres** na navegação à esquerda. Clique em **Sites**, forneça um nome e escolha o tipo de local. Em seguida, clique no botão **Adicionar vCenter**.

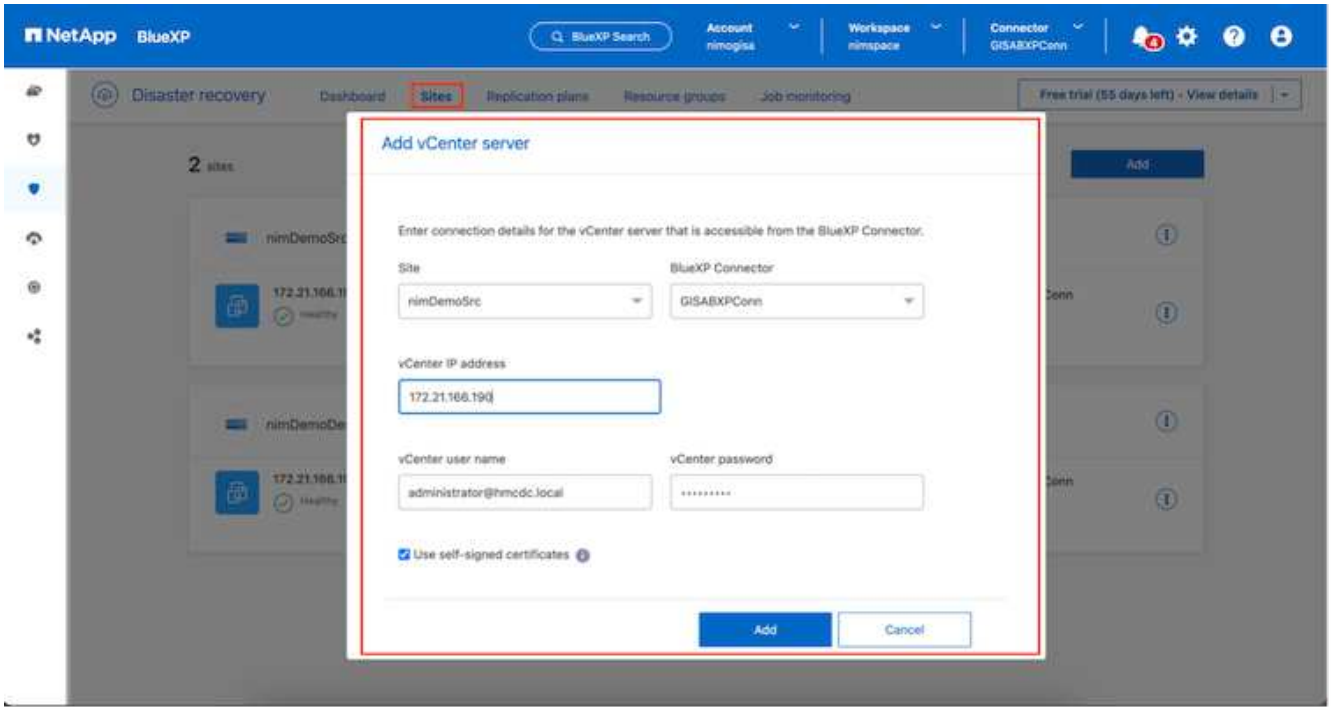


Adicione as seguintes plataformas:

- **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. Baseada na tecnologia Snapshot da NetApp, a replicação do SnapMirror é extremamente eficiente, pois replica apenas os blocos que foram

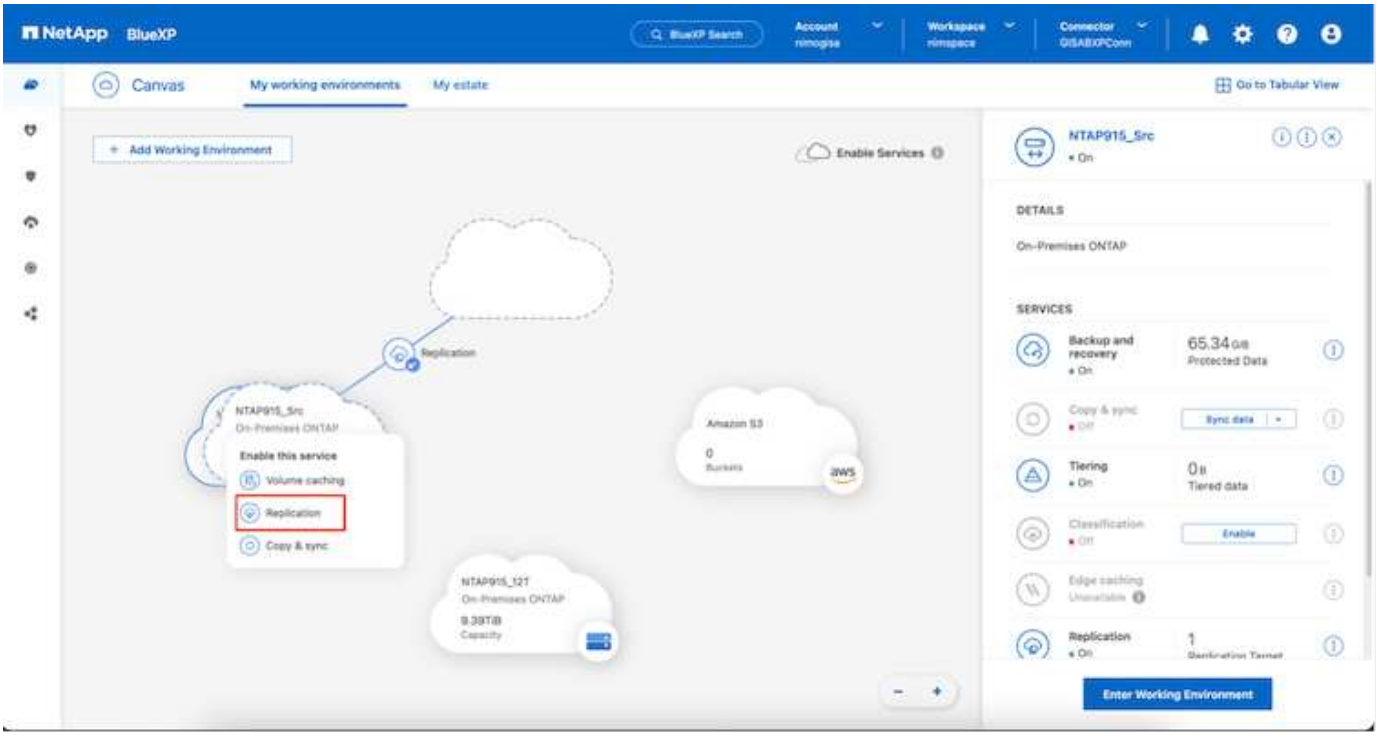
alterados ou adicionados desde a atualização anterior. O SnapMirror é facilmente configurado usando o NetApp OnCommand System Manager ou a CLI do ONTAP. O NetApp Data Services também cria a relação do SnapMirror, desde que o peering de cluster e de SVM tenha sido configurado previamente.

Para os casos em que o storage primário não se perde completamente, o SnapMirror oferece um meio eficiente de ressincronizar os sites primário e de DR. O SnapMirror pode ressincronizar os dois sites, transferindo de volta para o site primário, a partir do site de DR, apenas os dados alterados ou novos, simplesmente invertendo as relações do SnapMirror. Isso significa que os planos de replicação na recuperação de desastres podem ser ressincronizados em qualquer direção após um failover, sem copiar novamente o volume inteiro. Se uma relação for ressincronizada na direção inversa, apenas os novos dados gravados desde a última sincronização bem-sucedida da cópia Snapshot serão enviados de volta para o destino.

Se a relação do SnapMirror já estiver configurada para o volume via CLI ou o System Manager, o NetApp Data Services reconhecerá a relação e continuará com o restante das operações do fluxo de trabalho.

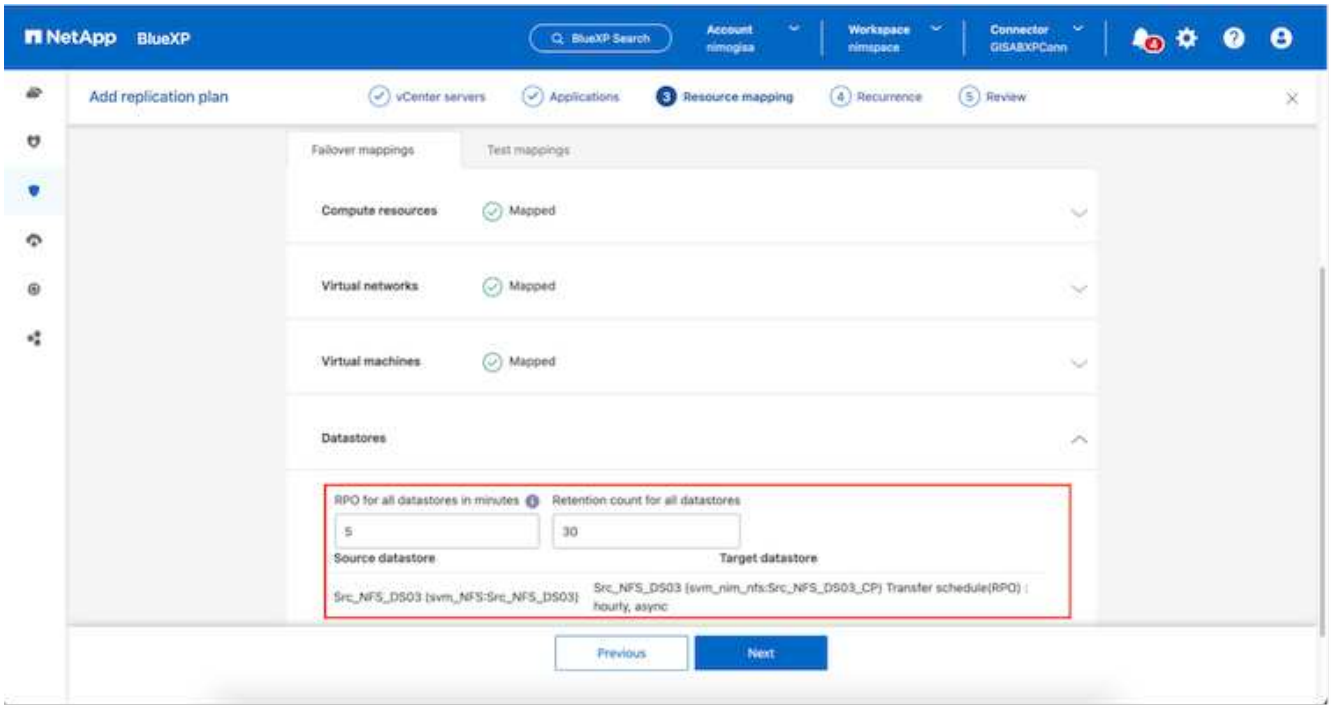
Como configurá-lo para recuperação de desastres do VMware

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 usar o NetApp Console para configurar a replicação do SnapMirror usando um simples recurso de arrastar e soltar do sistema ONTAP de origem no ambiente até o destino para acionar o assistente que orienta você pelo restante do processo.



A recuperação de desastres também pode automatizar esse processo, desde que você atenda aos dois critérios a seguir:

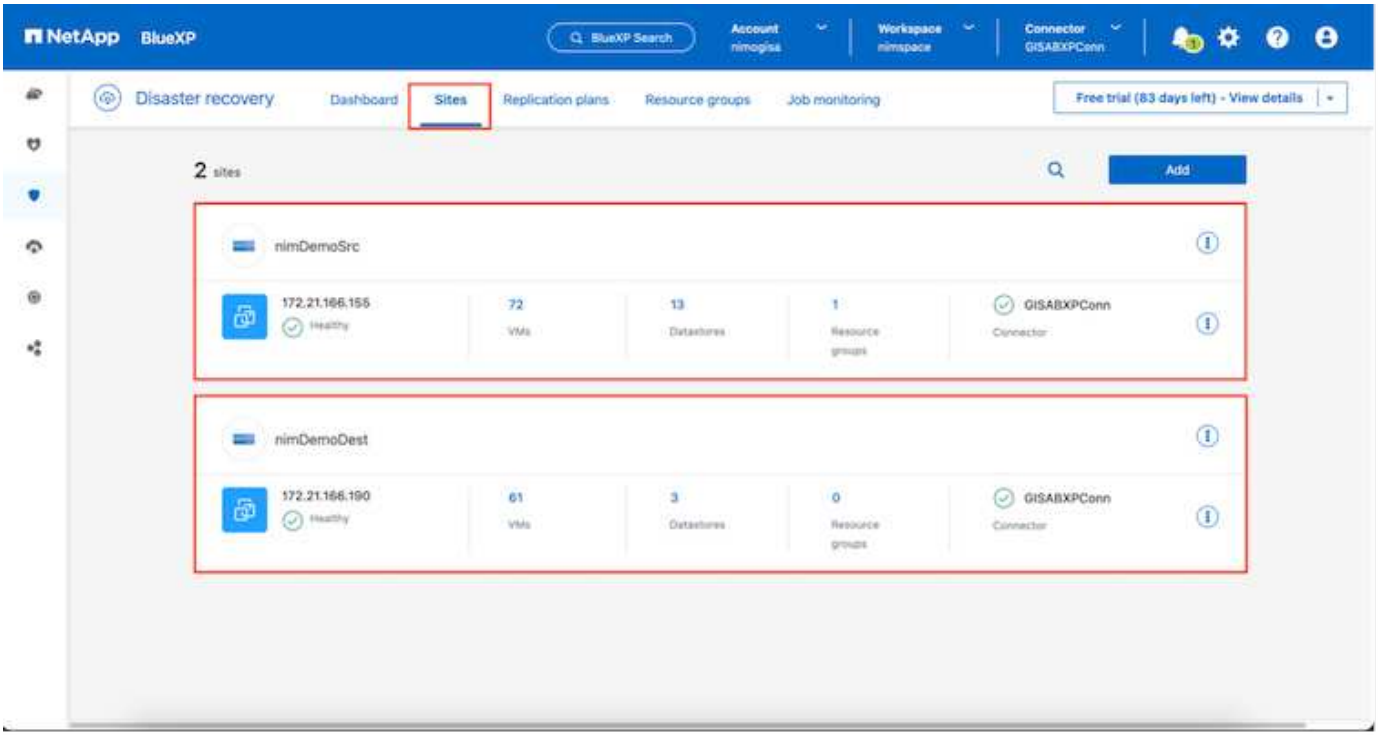
- Os clusters de origem e destino têm um relacionamento de pares.
- O SVM de origem e o SVM de destino têm um relacionamento de mesmo nível.



Se a relação do SnapMirror já estiver configurada para o volume via CLI, o Disaster Recovery reconhece a relação e continua com o restante das operações do fluxo de trabalho.

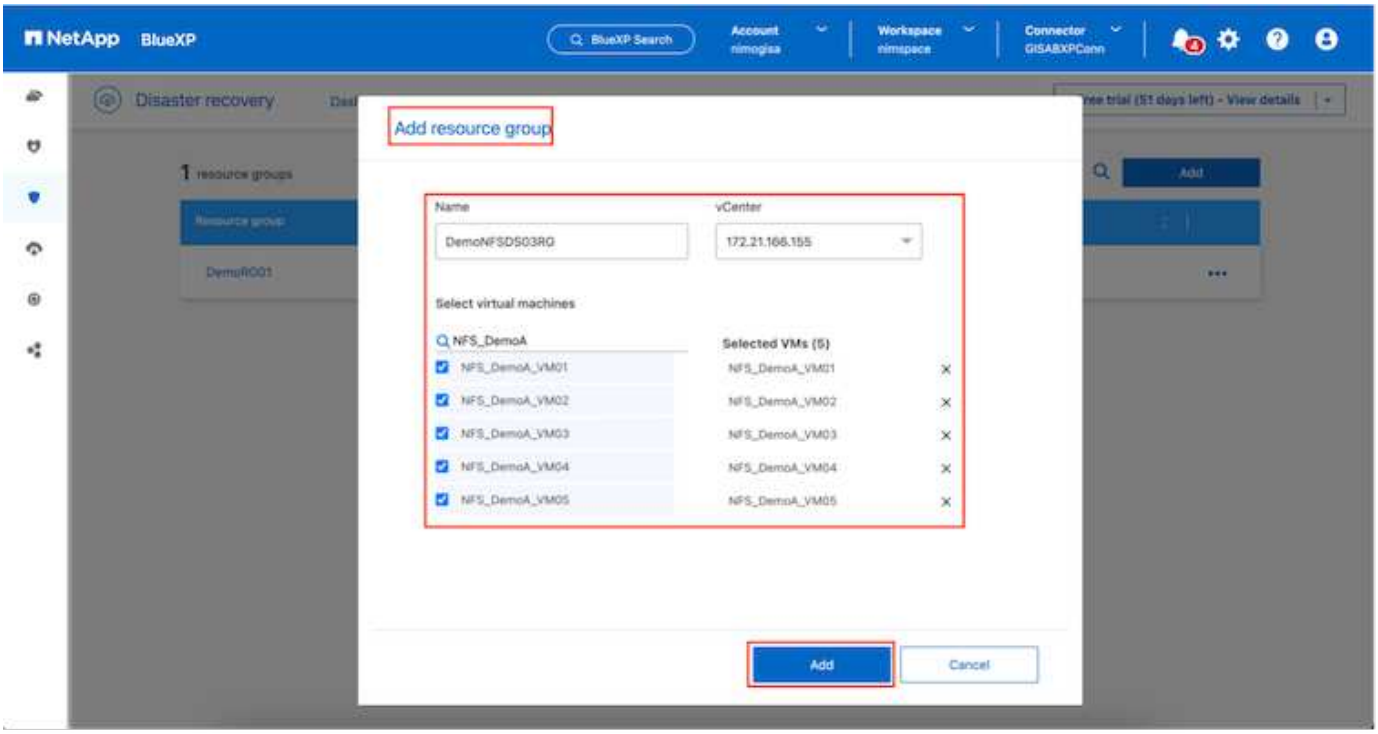
O que o Disaster Recovery pode fazer por você?

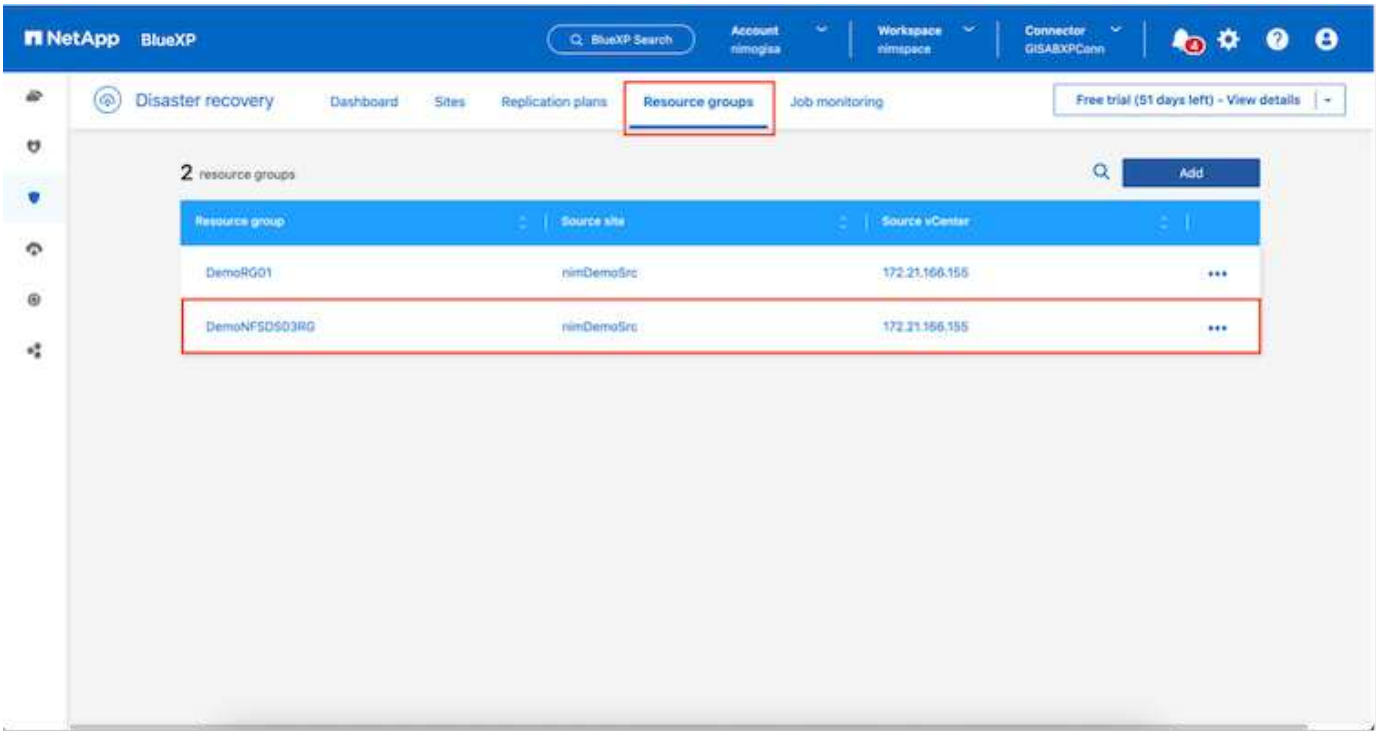
Após a adição dos sites de origem e destino, o Disaster Recovery realiza uma descoberta profunda automática e exibe as VMs juntamente com os metadados associados. O Disaster Recovery também detecta automaticamente as redes e os grupos de portas usados pelas VMs e os preenche.



Após a adição dos sites, as VMs podem ser agrupadas em grupos de recursos. Os grupos de recursos do

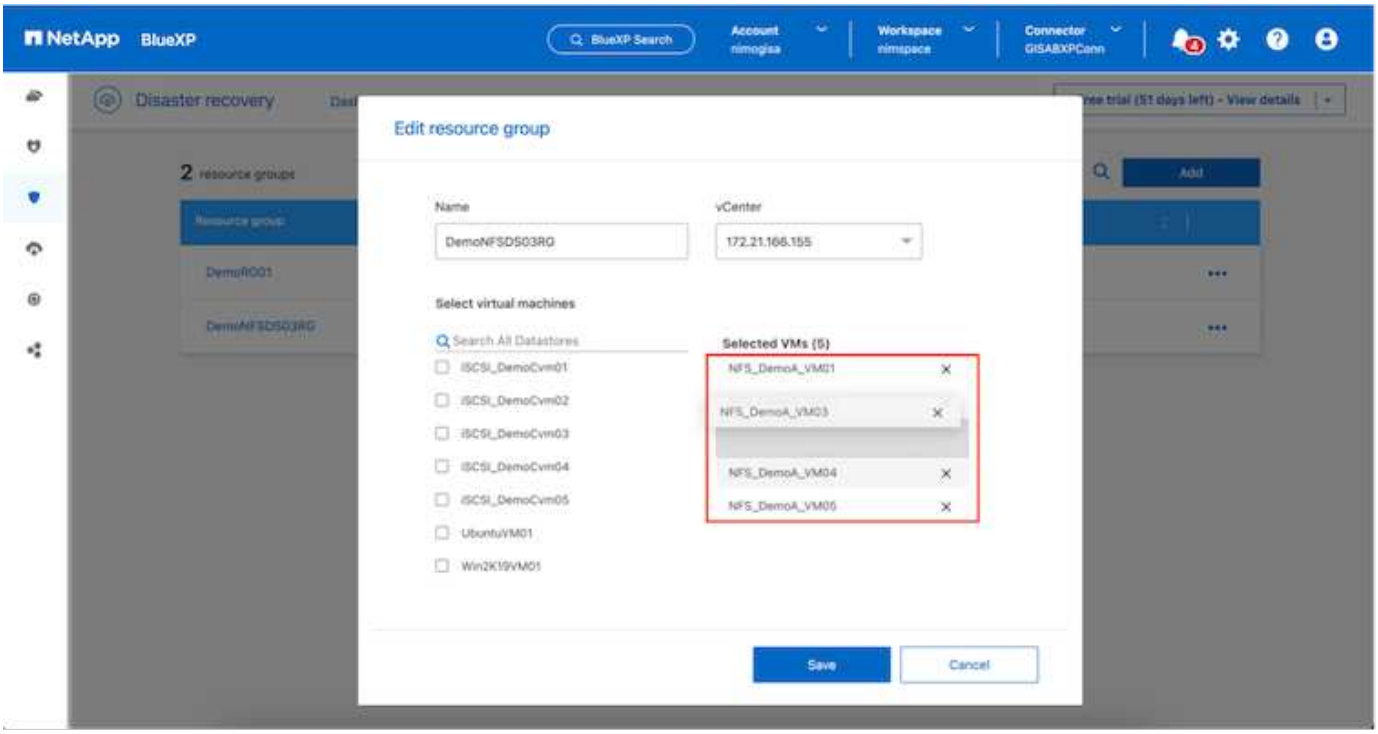
Disaster Recovery permitem agrupar um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização e atrasos de inicialização, que podem ser executados na recuperação. Para começar a criar grupos de recursos, acesse **Grupos de Recursos** e clique em **Criar Novo Grupo de Recursos**.



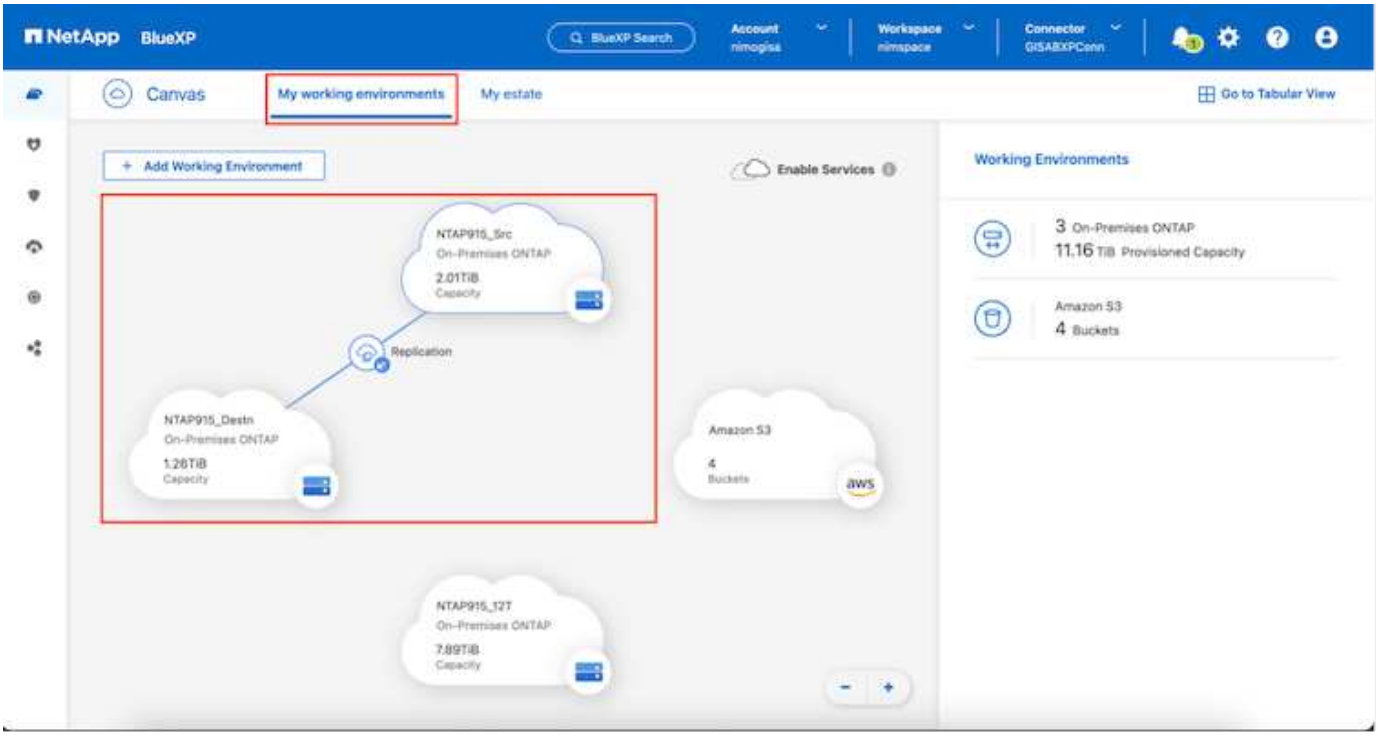


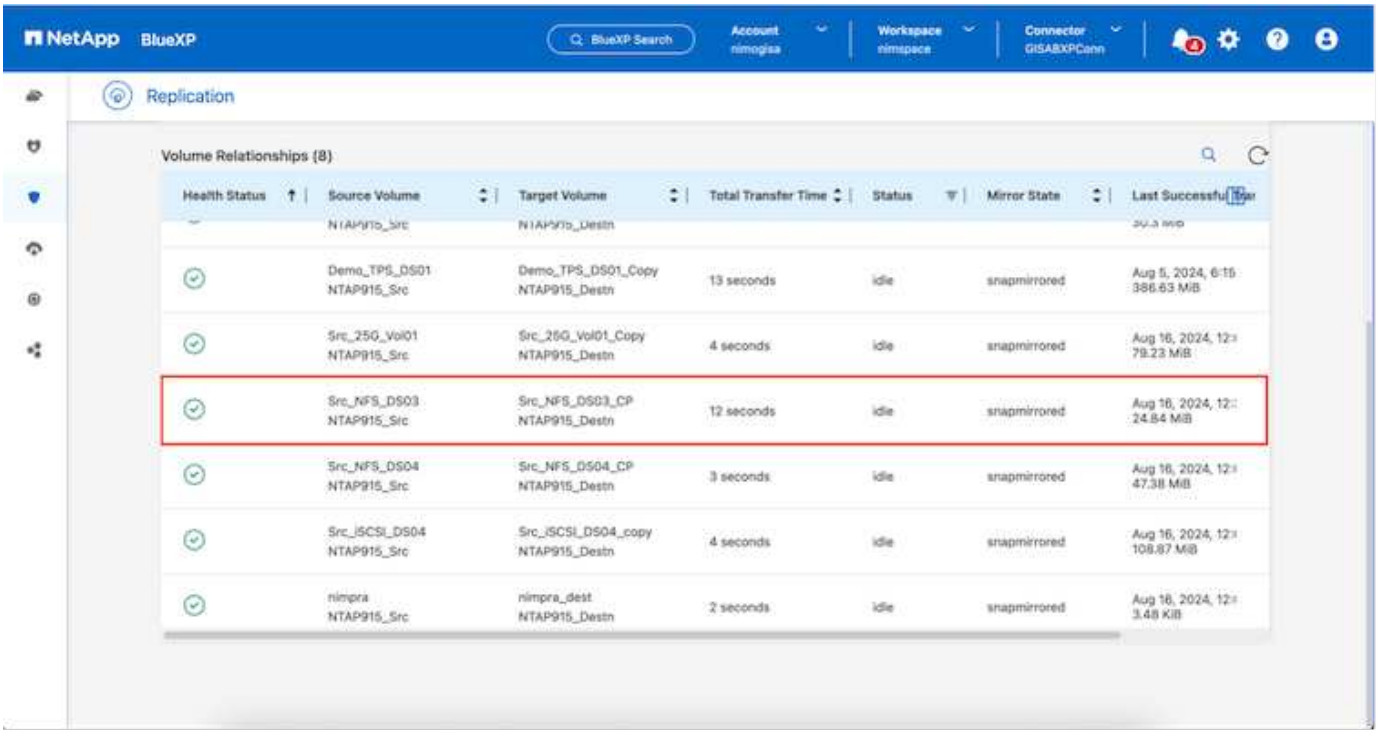
O grupo de recursos também pode ser criado durante a criação de um plano de replicação.

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.



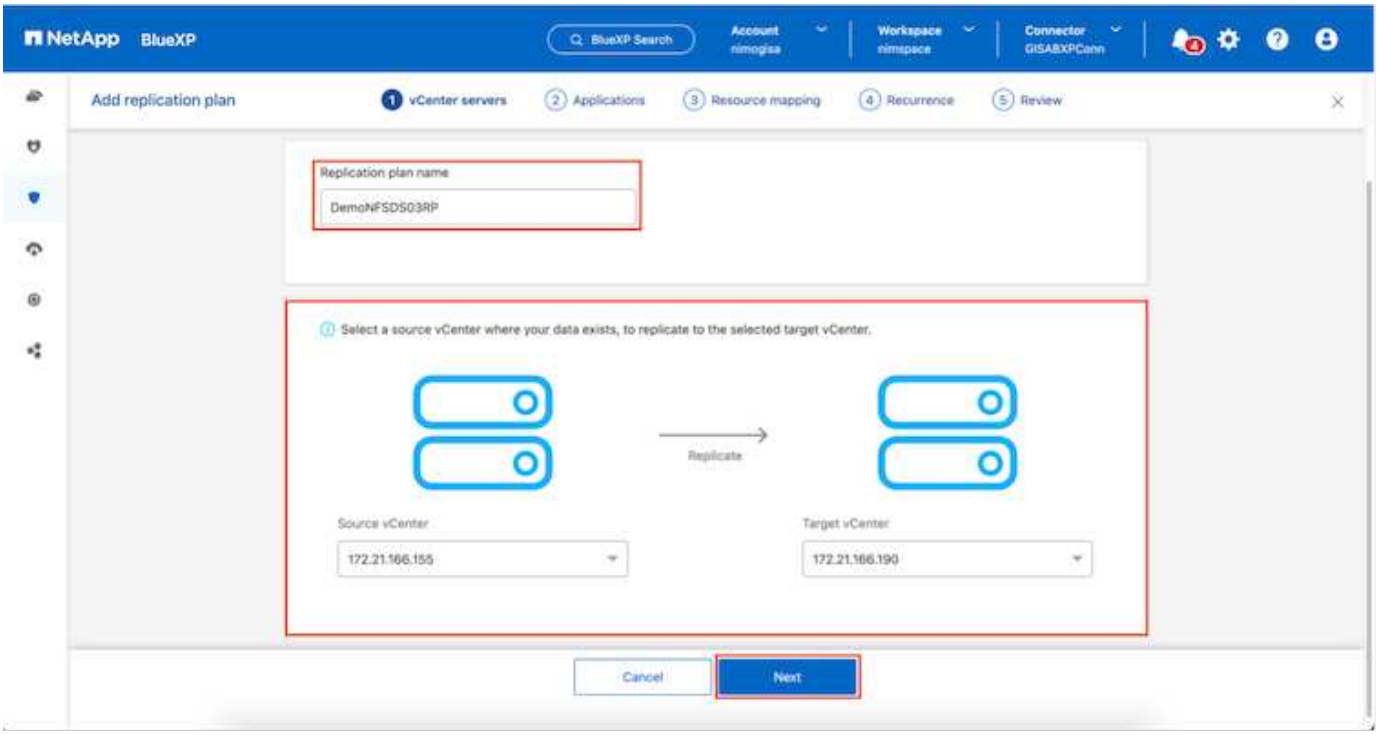
Depois que os grupos de recursos forem criados, a próxima etapa é criar o projeto de execução ou um plano para recuperar máquinas virtuais e aplicativos em caso de desastre. Conforme mencionado nos pré-requisitos, a replicação do SnapMirror pode ser configurada antecipadamente ou o DRaaS pode configurá-la usando o RPO e a contagem de retenção especificados durante a criação do plano de replicação.





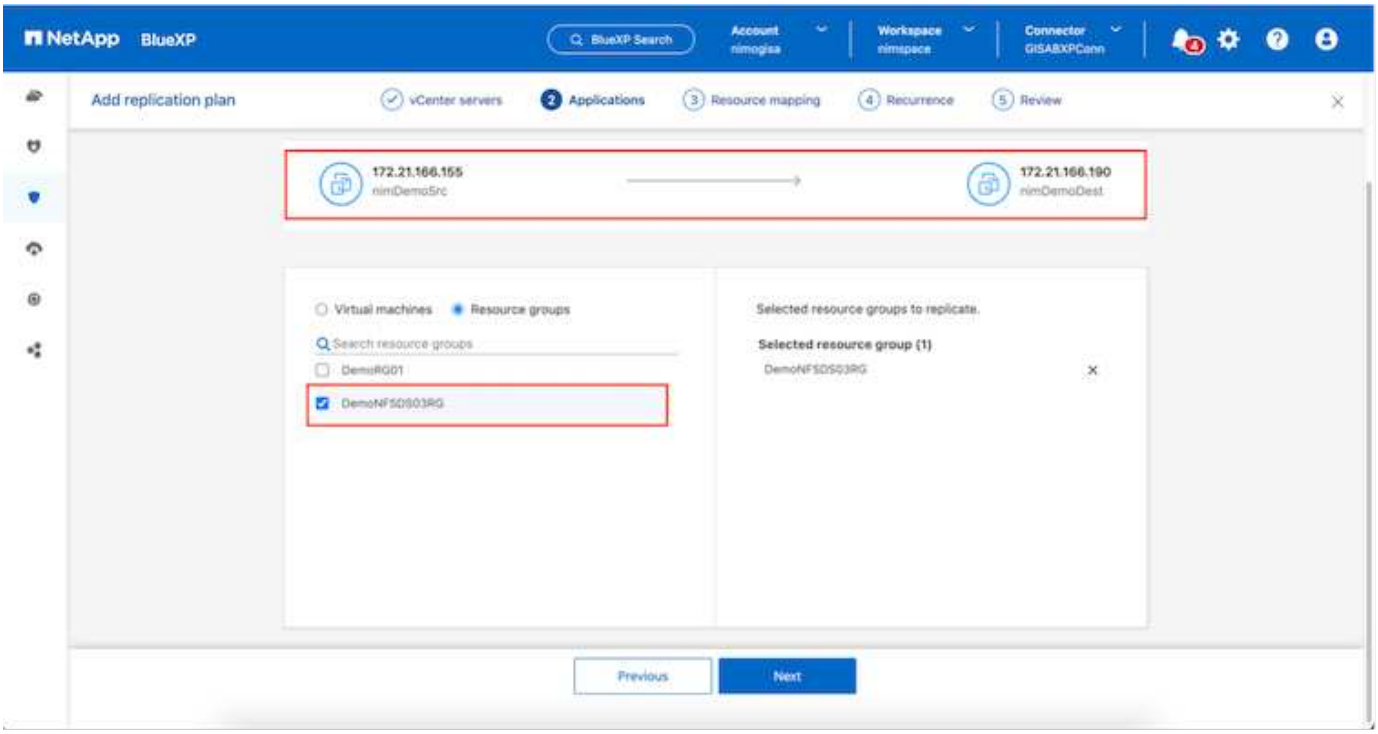
Configure o plano de replicação selecionando as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos no plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados e o mapeamento de clusters e redes. Para definir o plano 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

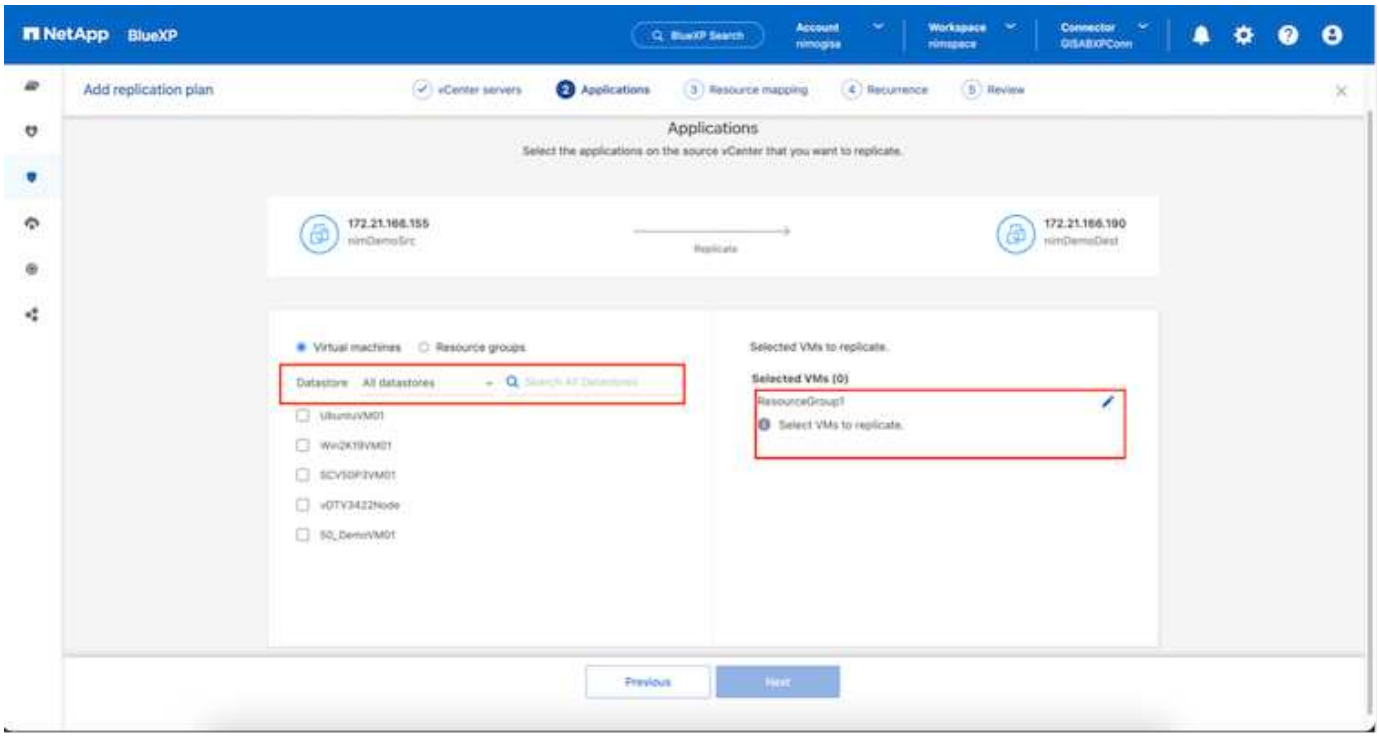
como as máquinas virtuais do aplicativo devem ser restauradas.



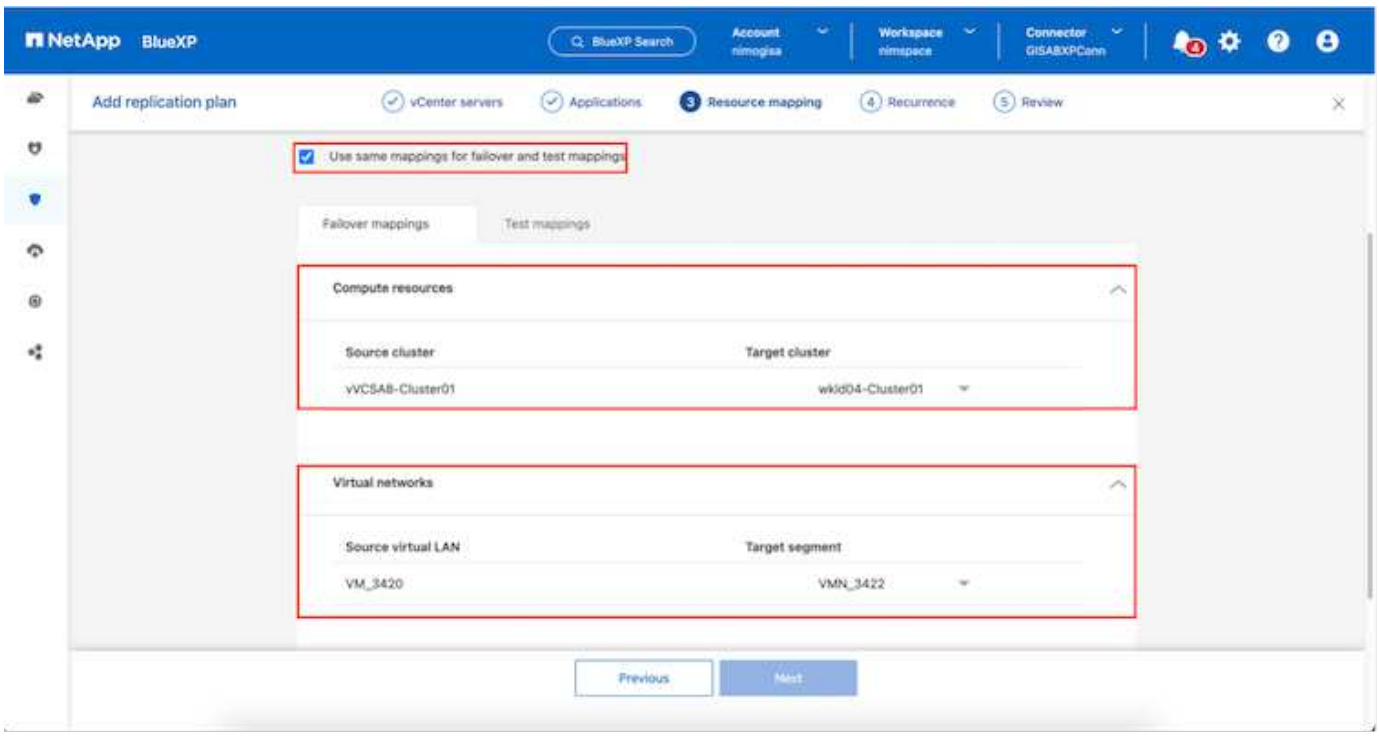
O grupo de recursos permite definir a ordem de inicialização usando a funcionalidade de arrastar e soltar. Ele pode ser usado para modificar facilmente a ordem em que as VMs serão ligadas durante o processo de recuperação.

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.

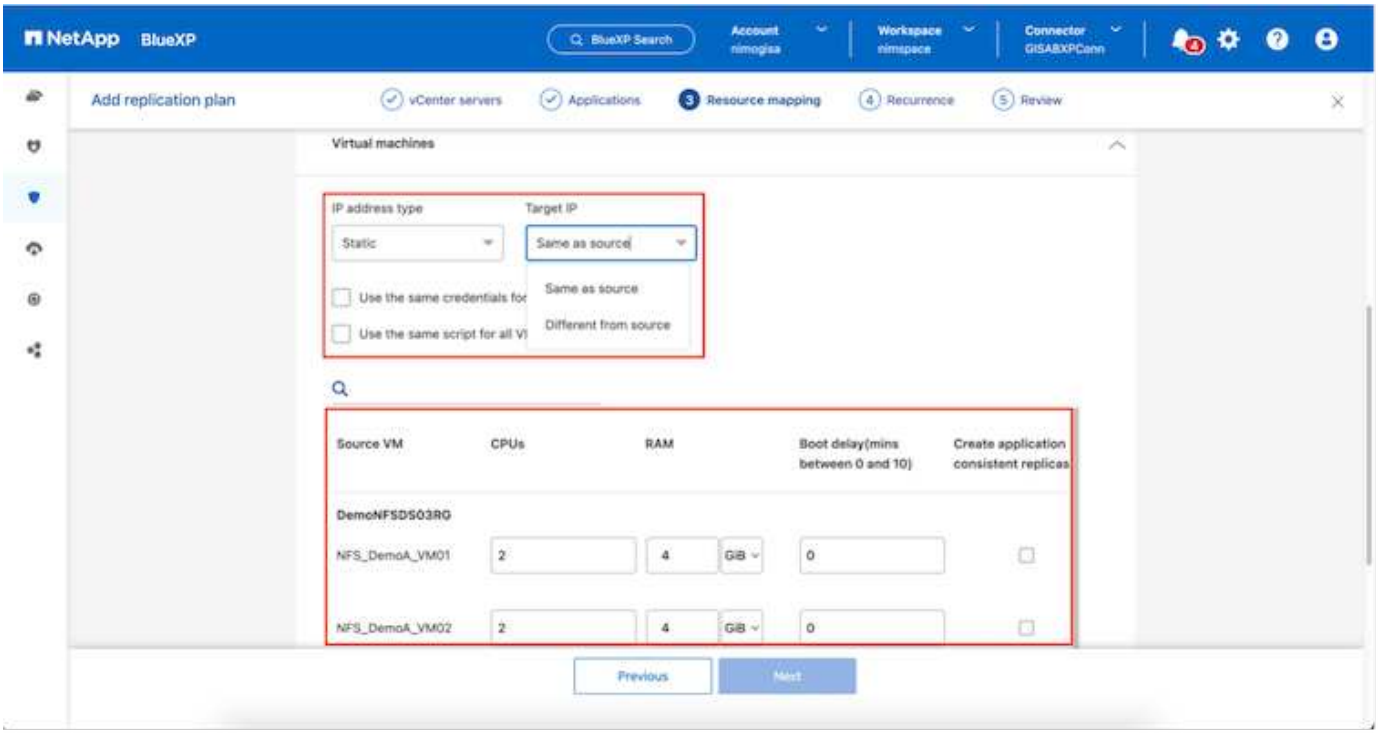
A captura de tela abaixo mostra a opção de filtrar máquinas virtuais ou armazenamentos de dados específicos com base em requisitos organizacionais, caso os grupos de recursos não sejam criados previamente.



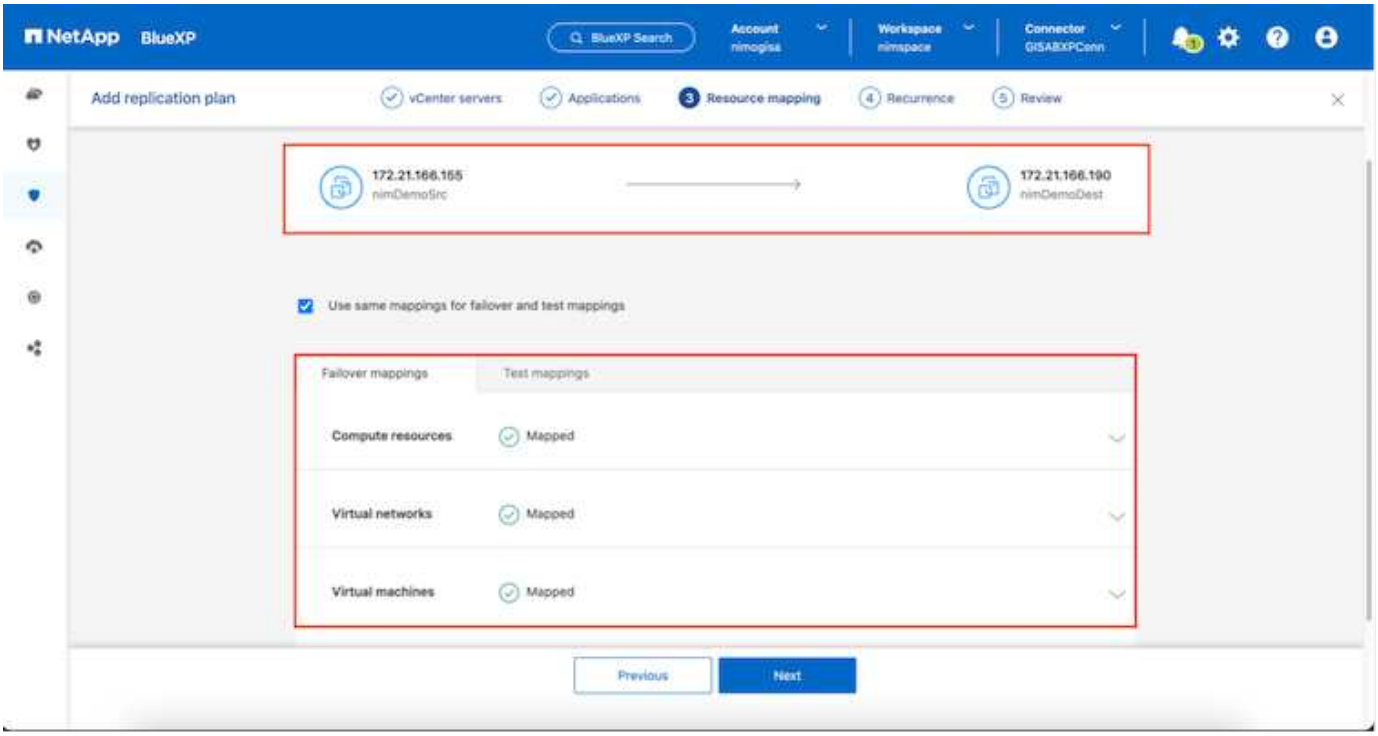
Após selecionar os grupos de recursos, crie os mapeamentos de failover. Nesta etapa, especifique como os recursos do ambiente de origem são mapeados para o destino. Isso inclui recursos de computação e redes virtuais. Personalização de IP, scripts de pré e pós-inicialização, atrasos de inicialização, consistência de aplicativos e assim por diante. Para obter informações detalhadas, consulte "Crie um plano de replicação".



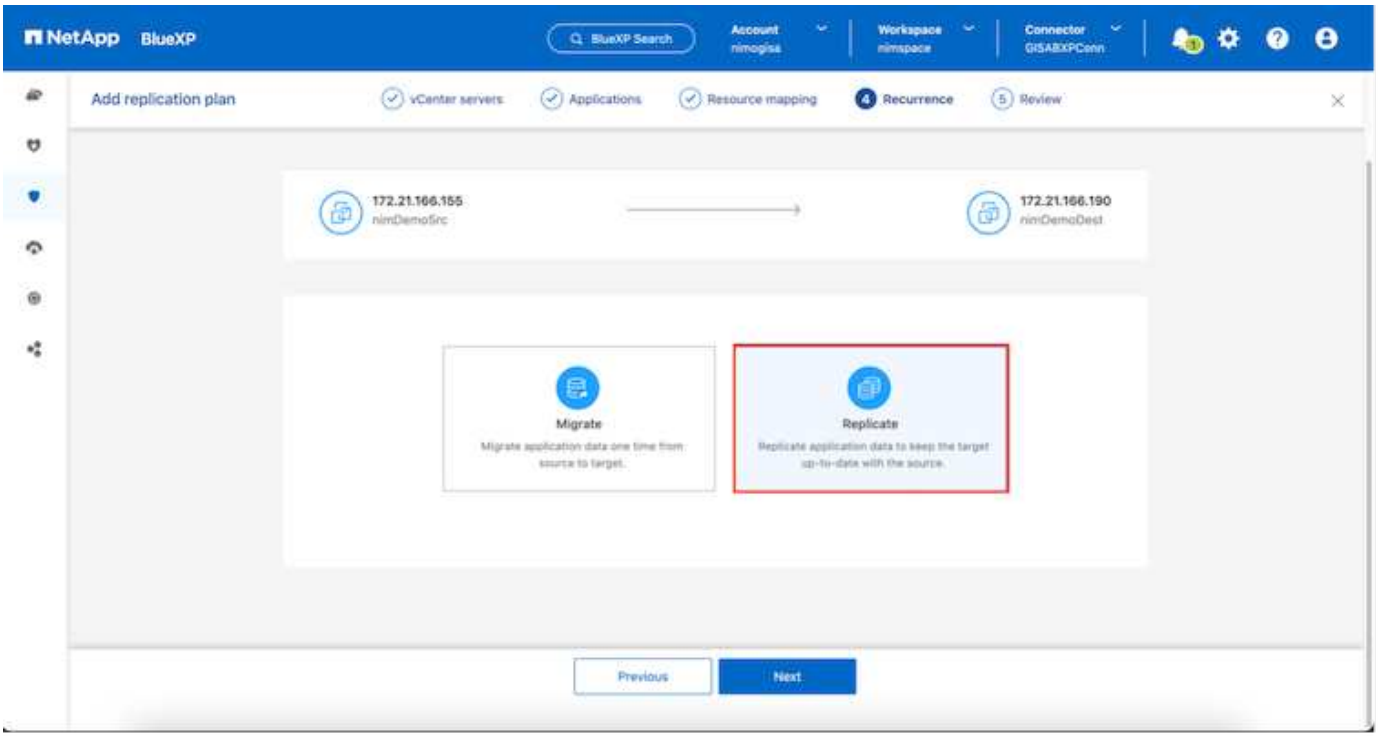
Por padrão, os mesmos parâmetros de mapeamento são usados para operações de teste e failover. Para definir mapeamentos diferentes para o ambiente de teste, selecione a opção Mapeamento de teste depois de desmarcar a caixa de seleção, conforme mostrado abaixo:



Quando o mapeamento de recursos estiver concluído, clique em Avançar.

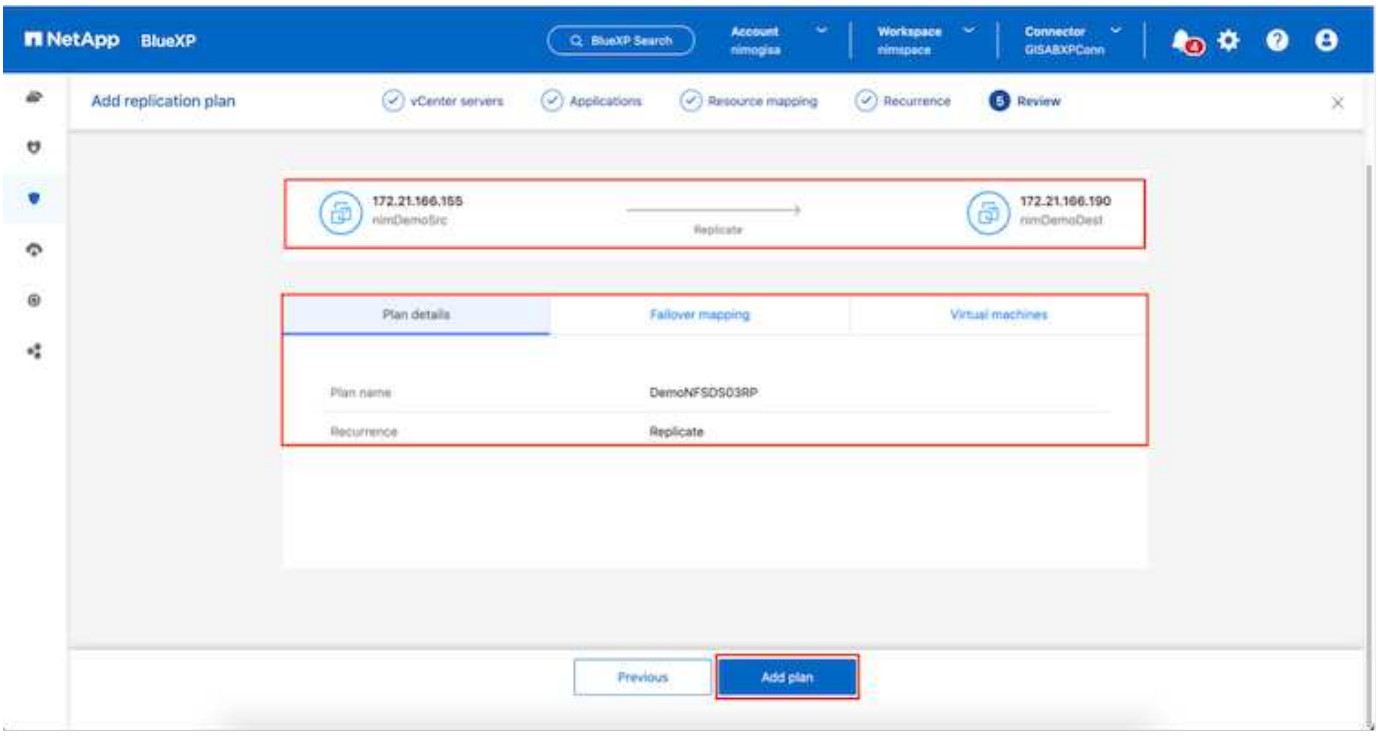


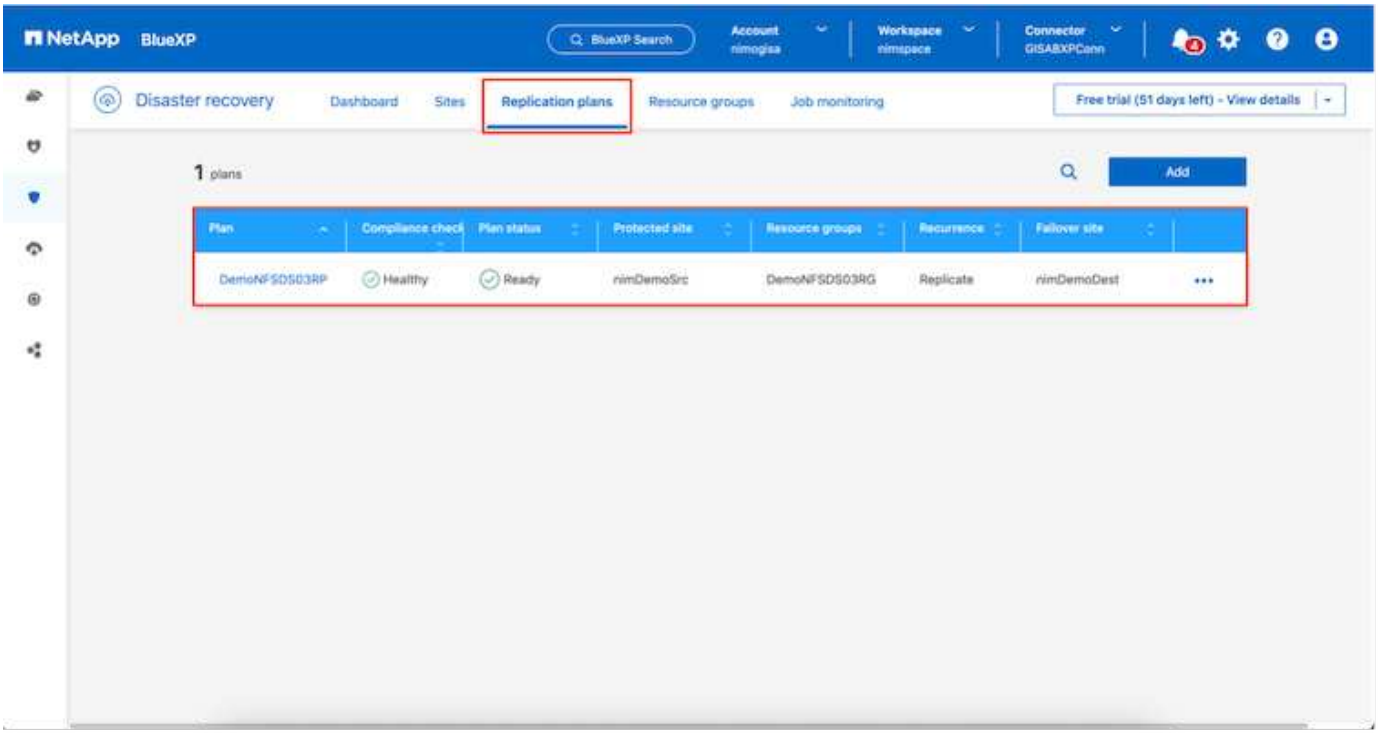
Selecione o tipo de recorrência. Em palavras simples, selecione Migrar (migração única usando failover) ou a opção de replicação contínua recorrente. Neste passo a passo, a opção Replicar está selecionada.



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

É possível incluir máquinas virtuais (VMs) de diferentes volumes e SVMs em um plano de replicação. Dependendo da localização da VM (seja no mesmo volume ou em volumes separados dentro da mesma SVM, ou em volumes separados em SVMs diferentes), o Disaster Recovery cria um Snapshot de grupo de consistência.



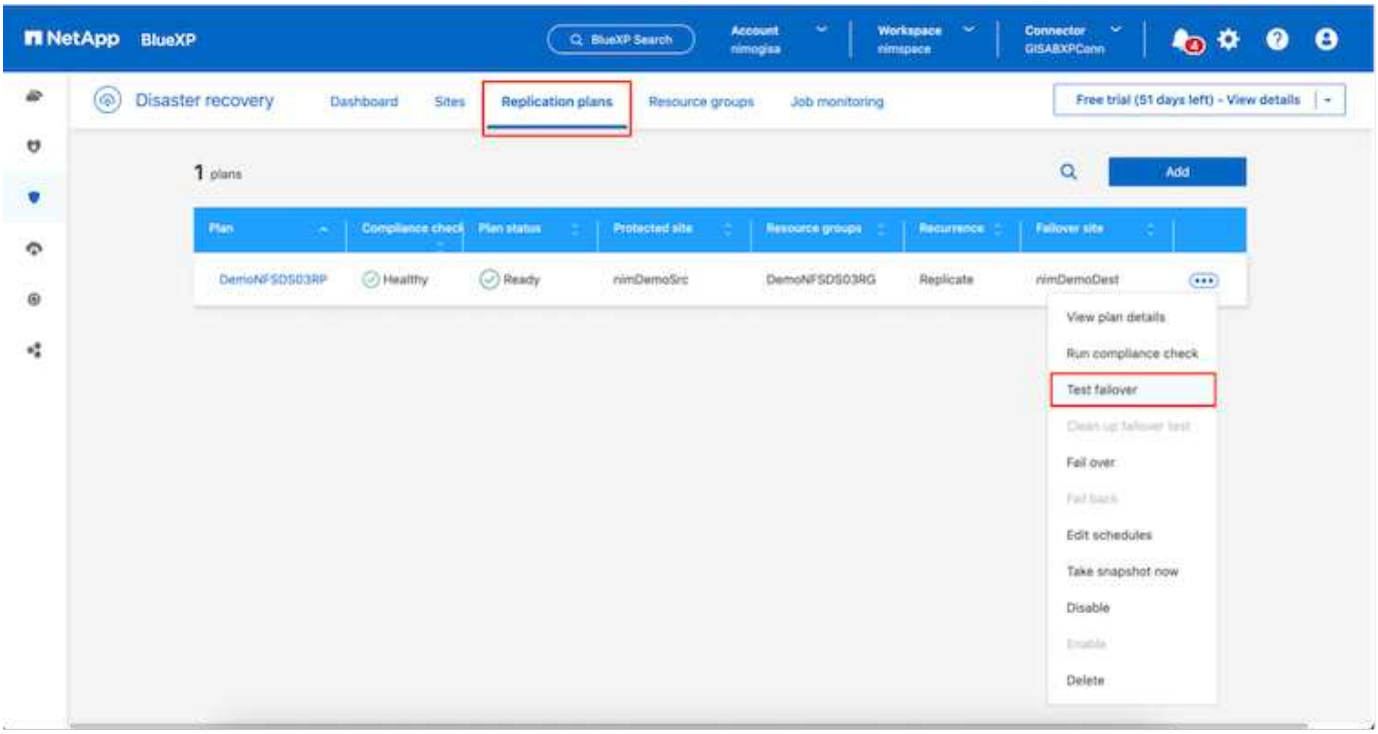


A recuperação de desastres consiste nos seguintes fluxos de trabalho:

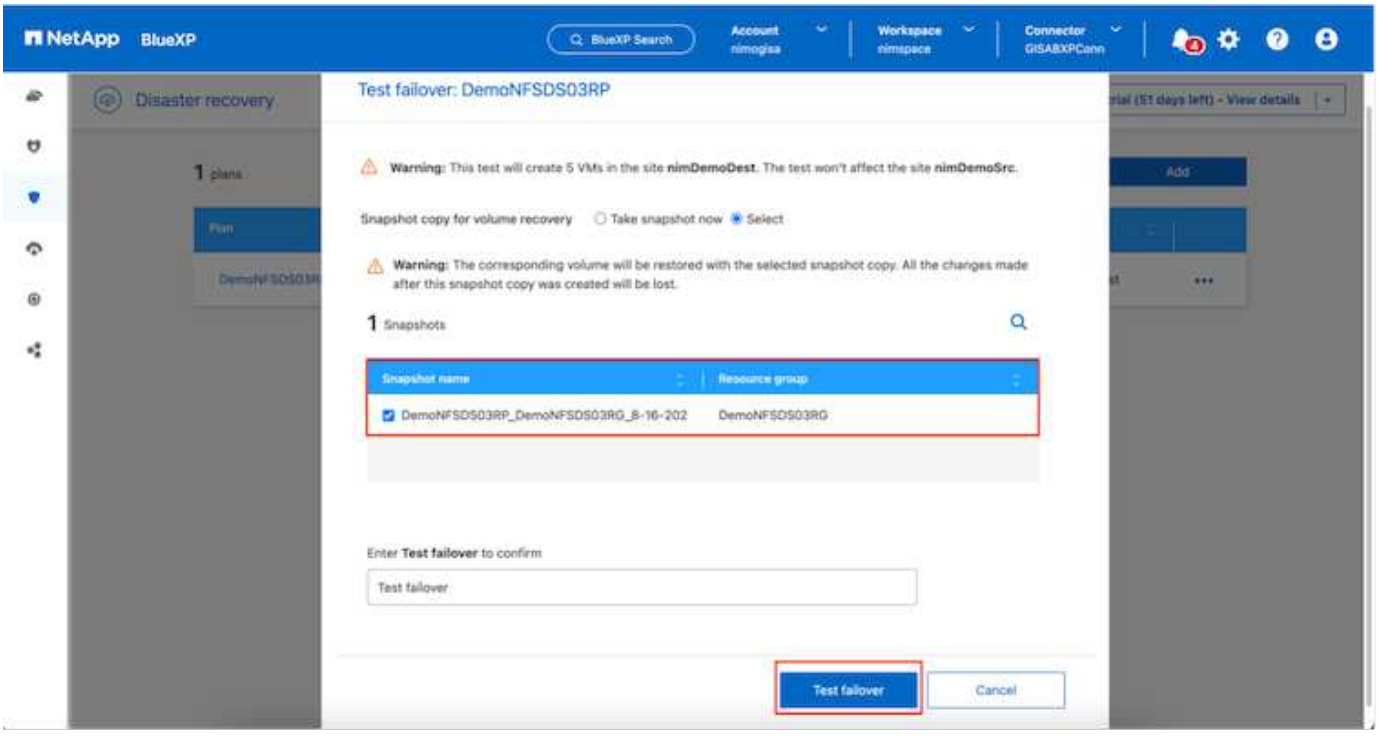
- Teste de failover (incluindo simulações automatizadas periódicas)
- Teste de failover de limpeza
- Failover
- Failback

Teste de failover

O teste de failover no o Disaster Recovery é um procedimento operacional que permite aos administradores do VMware validar completamente seus planos de recuperação sem interromper seus ambientes de produção. Durante um teste de failover, o Disaster Recovery cria cópias NetApp FlexClone com uso eficiente de espaço dos volumes de datastore NFS replicados no sistema de storage de DR. Esses volumes FlexClone são então montados nos hosts ESXi no site de DR, e as máquinas virtuais são ligadas em uma rede de teste isolada. Esse processo permite que os administradores verifiquem se seus planos de recuperação de desastres funcionarão como pretendido no caso de um desastre real.



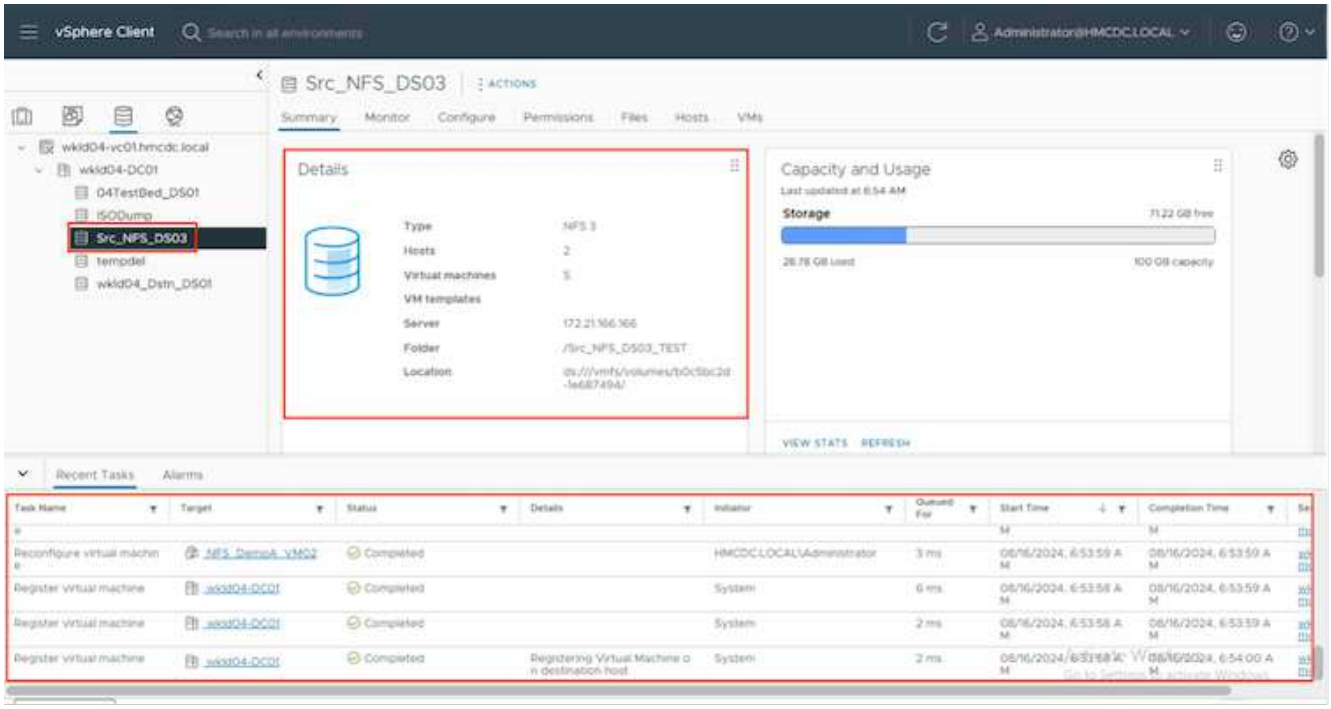
A recuperação de desastres incorpora a capacidade de selecionar o snapshot como um recurso opcional na operação de failover de teste. Esse recurso permite que o administrador do VMware verifique se quaisquer alterações feitas recentemente no ambiente foram replicadas para o site de destino e, portanto,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



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

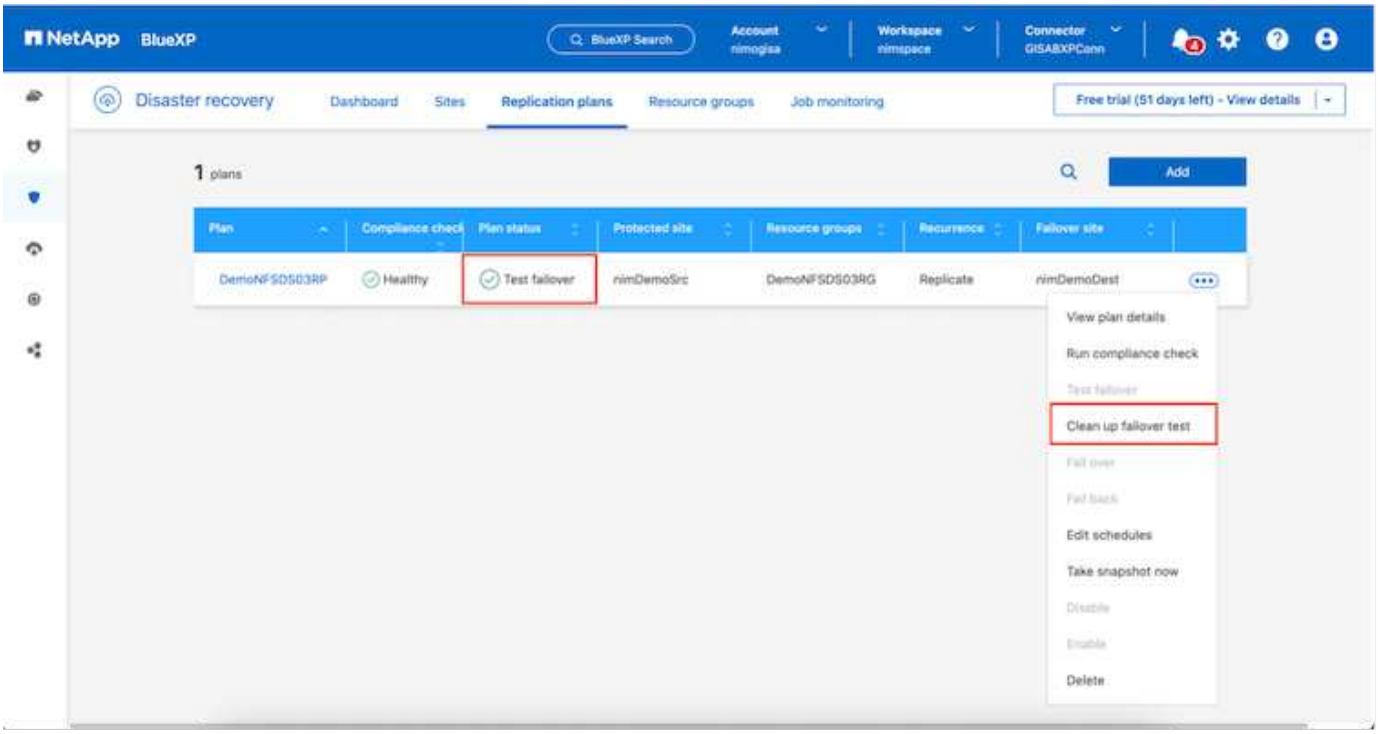
- Acionar relacionamentos do SnapMirror para atualizar o armazenamento no site de destino com quaisquer alterações recentes feitas no site de produção.

- 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.



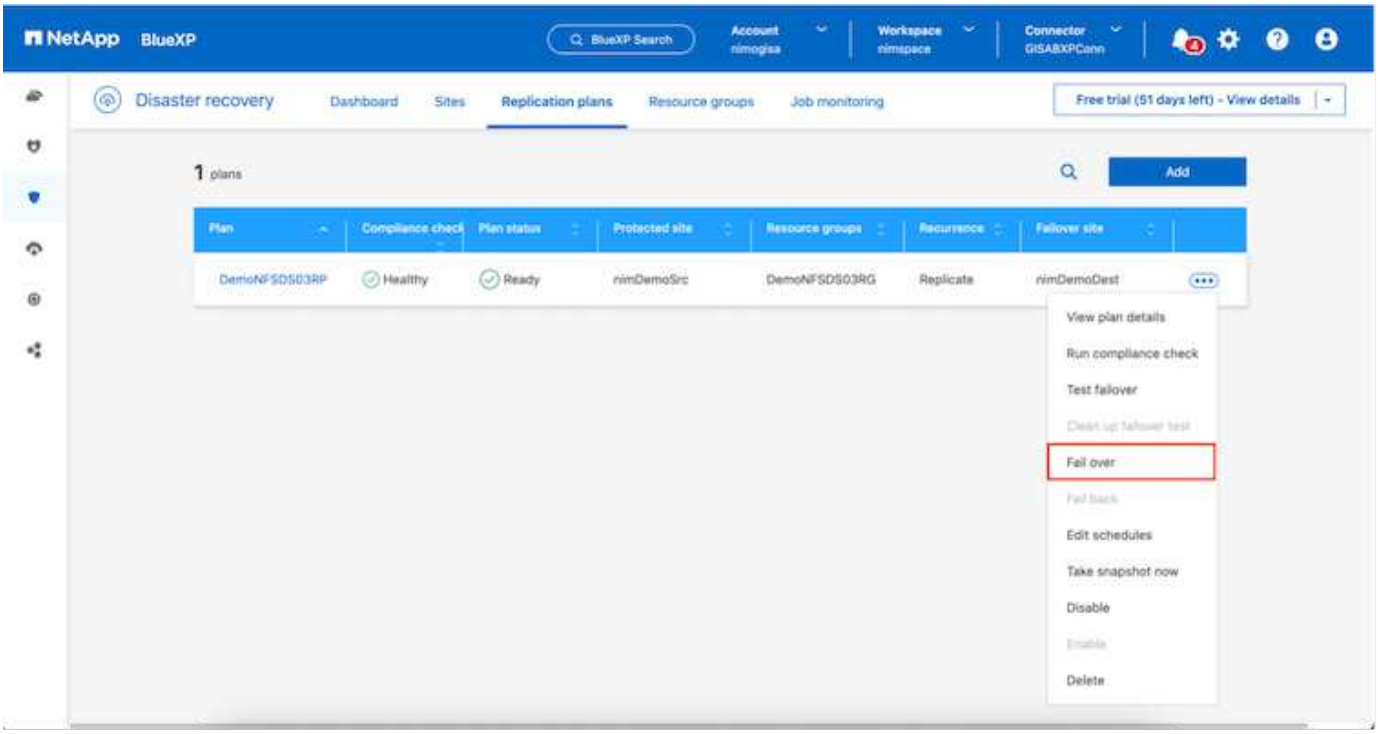
Esta ação redefinirá as máquinas virtuais (VMs) e o status do plano de replicação para o estado pronto.

Quando o administrador do VMware executa uma operação de recuperação, o Disaster Recovery completa 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.

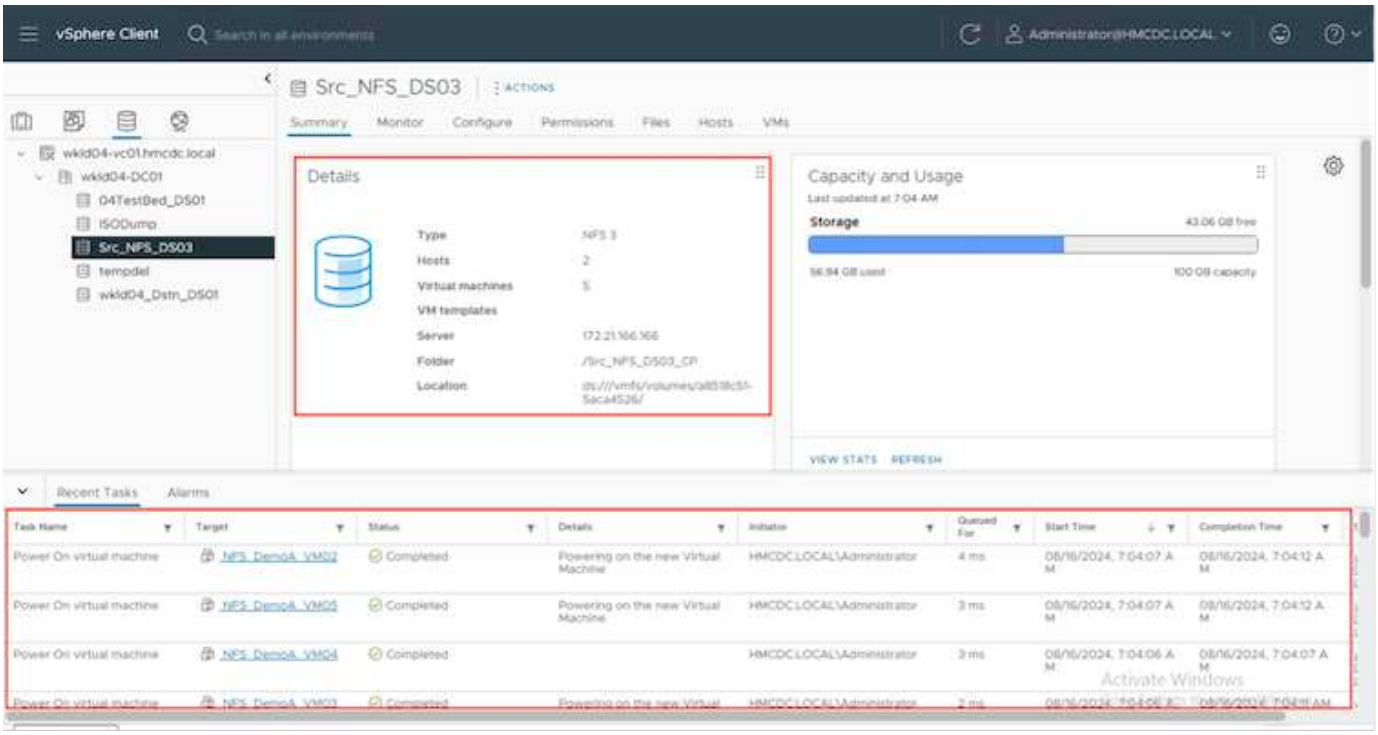
Migração planejada e failover

O Disaster Recovery tem dois métodos para realizar um failover real: migração planejada e failover. O primeiro método, migração planejada, incorpora o desligamento das VMs e a sincronização da replicação de storage ao 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 storage que pôde ser concluído. Dependendo do RPO definido na solução, alguma perda de dados pode ser esperada no cenário de DR.



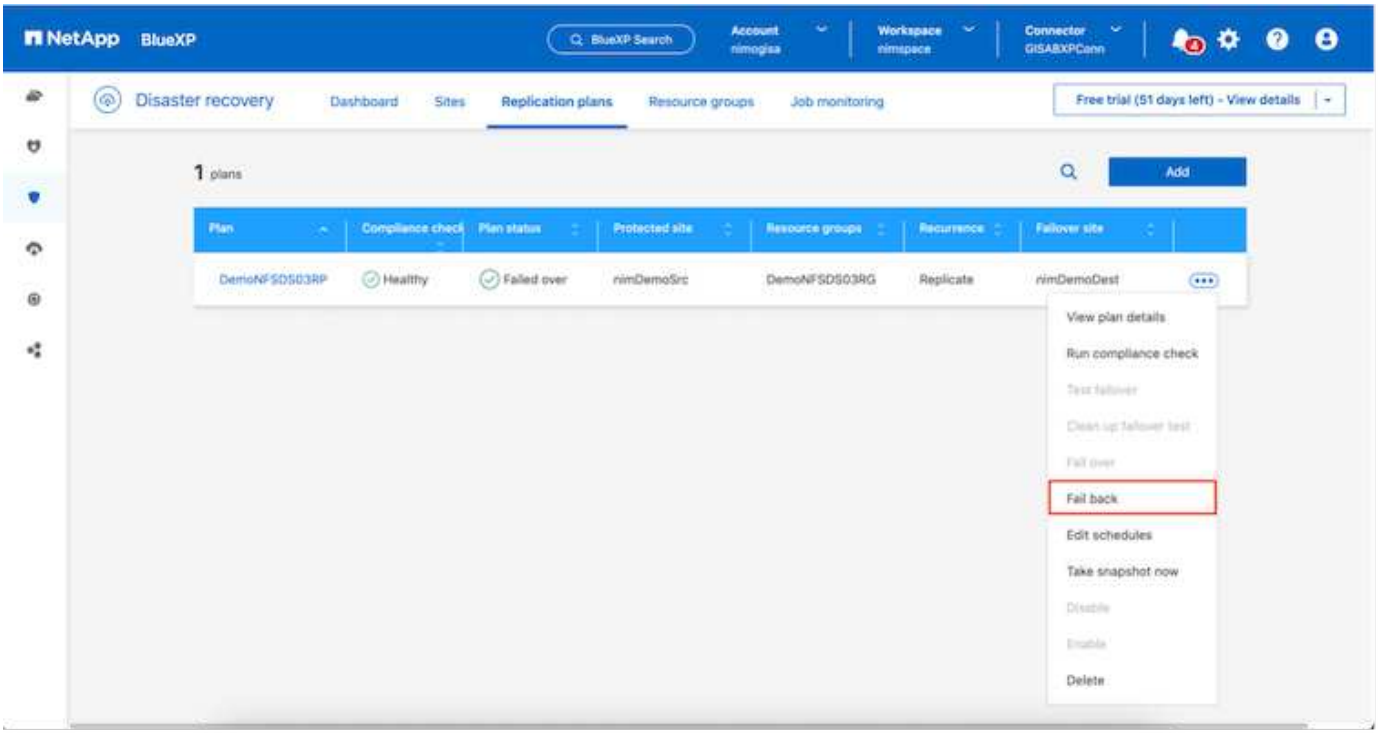
Quando o administrador do VMware executa uma operação de failover, o Disaster Recovery automatiza as seguintes tarefas:

- 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 Disaster Recovery replica (ressincroniza) quaisquer alterações de volta para a máquina virtual de origem original antes de inverter a direção da replicação. Esse processo começa a partir de uma relação que

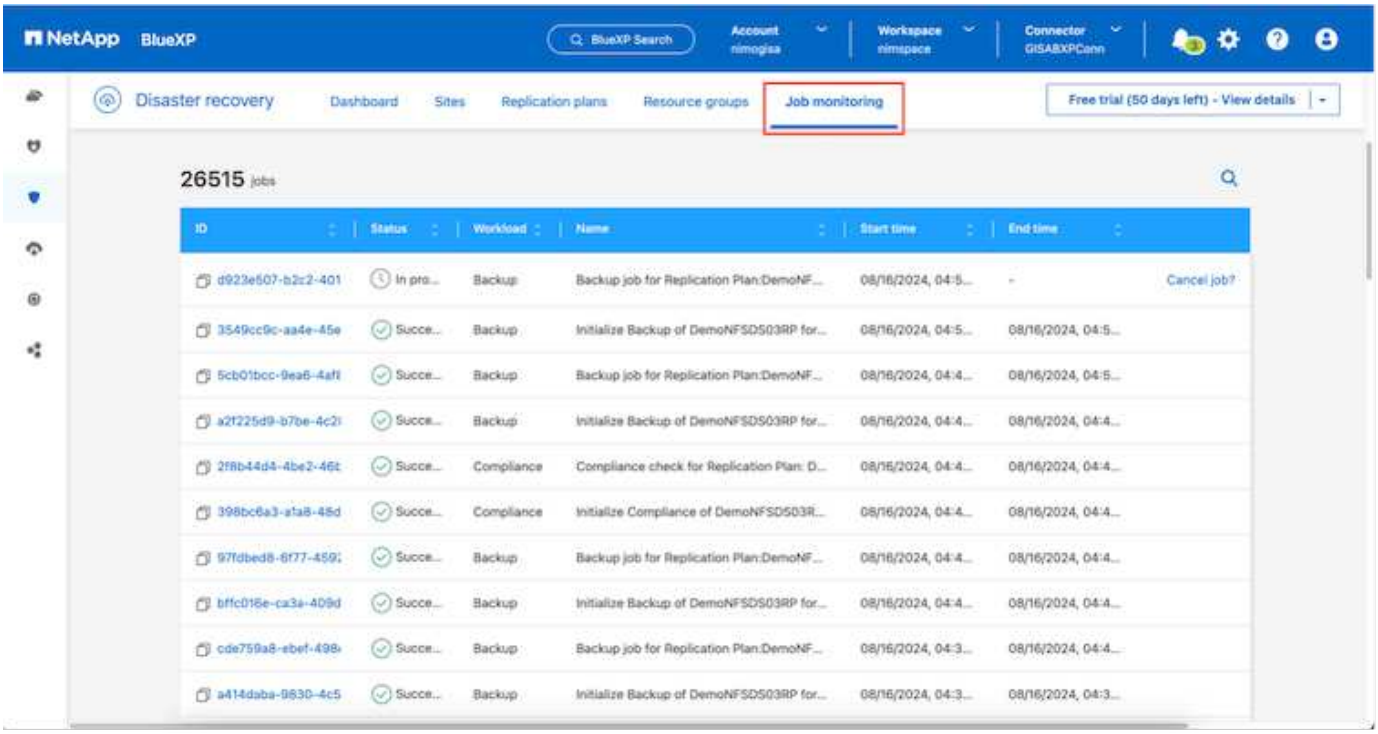
concluiu o failover para um destino e envolve as seguintes etapas:

- 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 Disaster Recovery, consulte "Saiba mais sobre o NetApp Disaster Recovery for VMware".

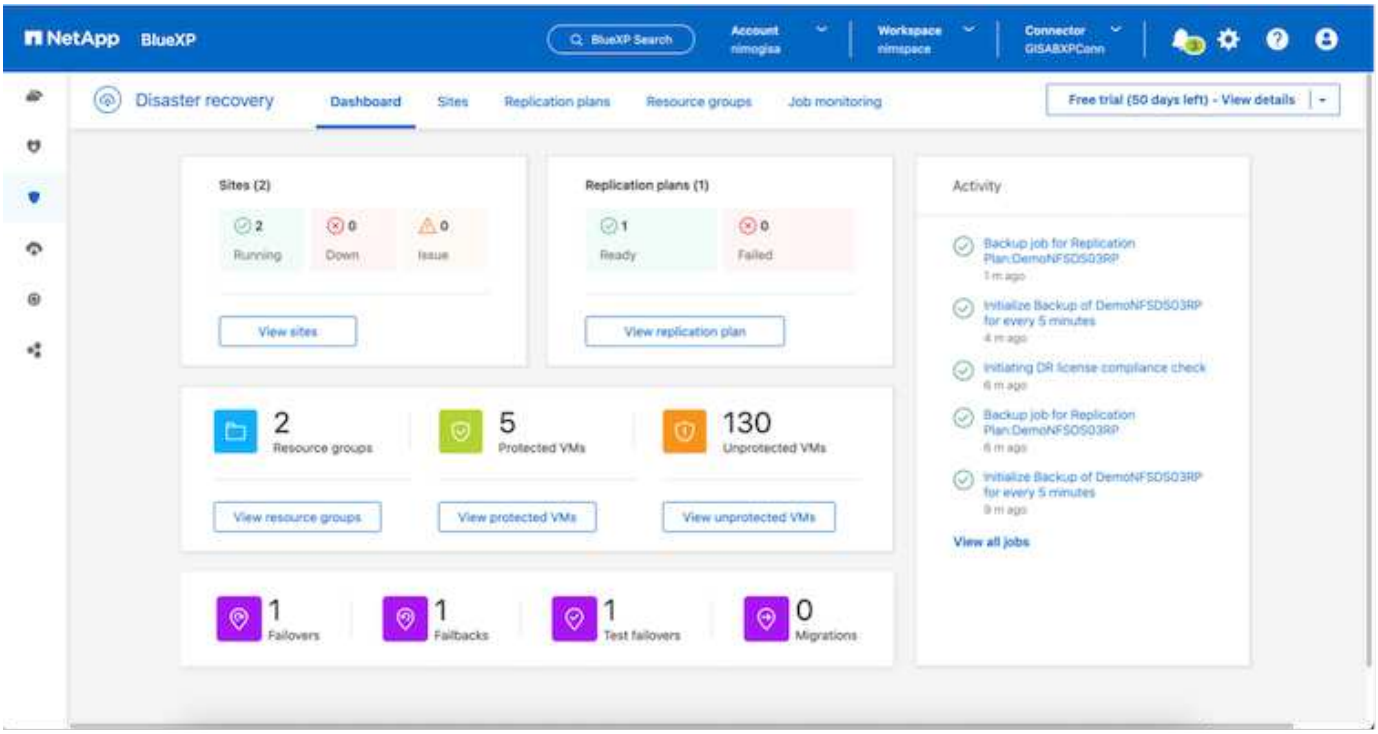
Monitoramento e Painel

A partir do Console ou da ONTAP CLI, você pode monitorar o status de integridade da replicação dos volumes do datastore apropriados, e o status de um failover ou failover de teste pode ser acompanhado por meio do Job Monitoring.



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

Com o painel do 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 íntegros, 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" .

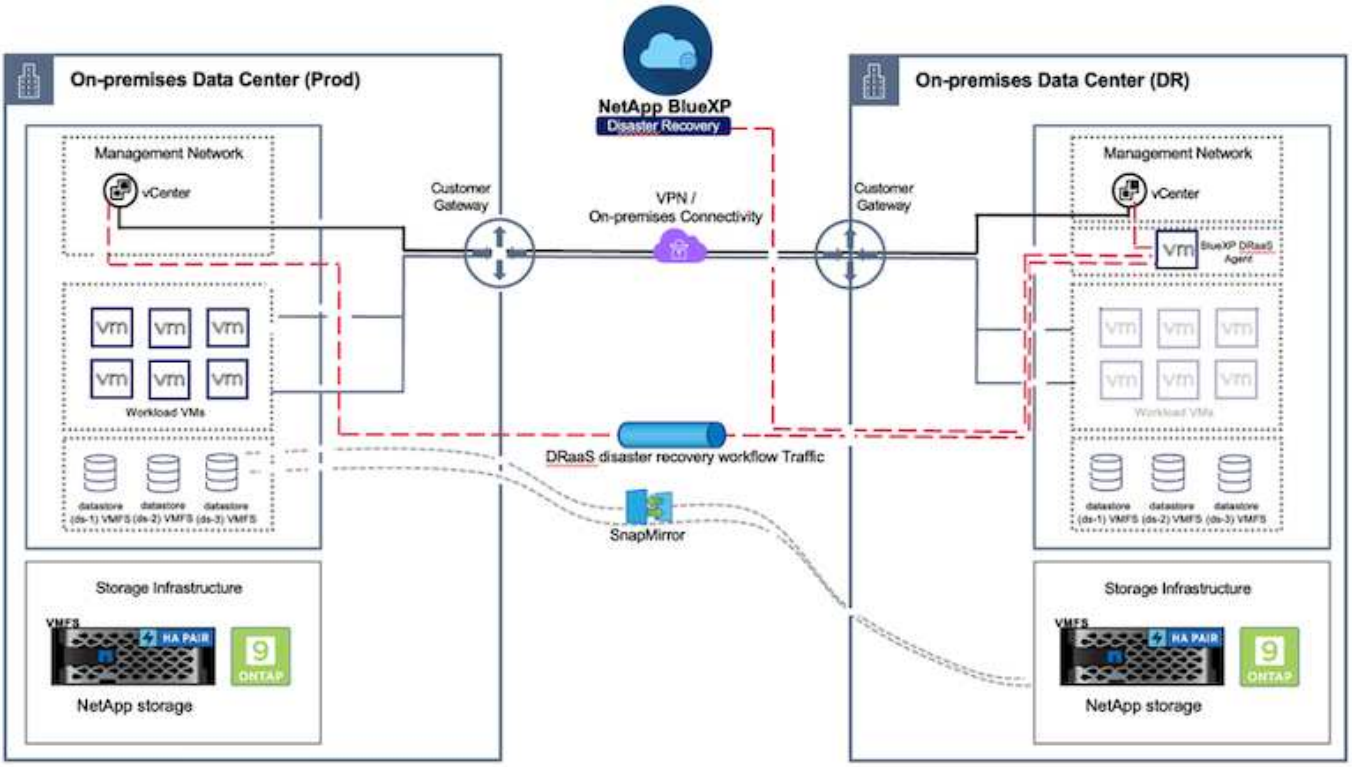
NetApp Disaster Recovery para datastores VMFS

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.

Esta seção do documento descreve a configuração do NetApp Diaster Recovery para configurar a recuperação de desastres de VMs VMware locais para outro site designado. Como parte dessa configuração, o Console agent, a integração dos arrays ONTAP, a definição de sites e a associação do VMware vCenter. 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 realizar um failover completo do site e como fazer o failback quando o site primário for recuperado e ficar online.

Utilizando o Disaster Recovery, parte do NetApp Data Services, os clientes podem descobrir seus vCenters VMware no local junto com o storage do 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. SnapMirror fornece replicação de blocos no nível de storage 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 afetar os datastores de produção e replicados nem gerar custos adicionais de storage. NetApp Data Services aproveita a tecnologia FlexClone do ONTAP para criar uma cópia com uso

eficiente de espaço do datastore VMFS a partir da última cópia Snapshot replicada no site de DR. Quando o teste de DR estiver concluído, os clientes poderão simplesmente excluir o ambiente de teste, novamente sem qualquer impacto nos recursos de produção replicados reais. Quando houver necessidade, planejada ou não, de um failover real, com alguns cliques, o Disaster Recovery orquestrará todas as etapas necessárias para ativar automaticamente as máquinas virtuais protegidas no site de recuperação de desastres designado. O serviço também reverterá a relação do SnapMirror para o site primário e replicará quaisquer alterações do secundário para o primário em uma operação de failback, quando necessário. Tudo isso pode ser alcançado com uma fração do custo em comparação com outras alternativas bem conhecidas.

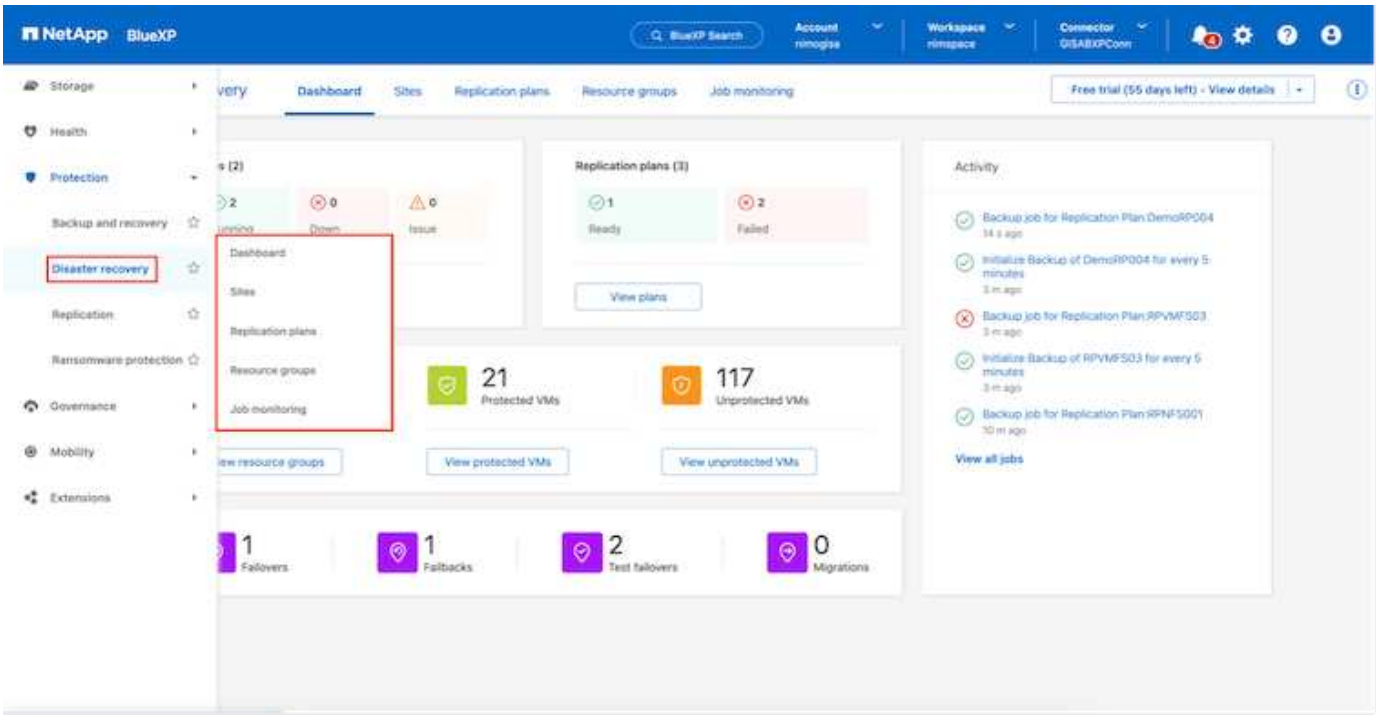


Para obter informações atualizadas e versões compatíveis do vCenter Server, do ESXi e do ONTAP for Disaster Recovery, consulte o "Configurações suportadas para recuperação de desastres".

Começando

Para começar a usar o Disaster Recovery, use o NetApp Console e depois acesse o serviço.

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

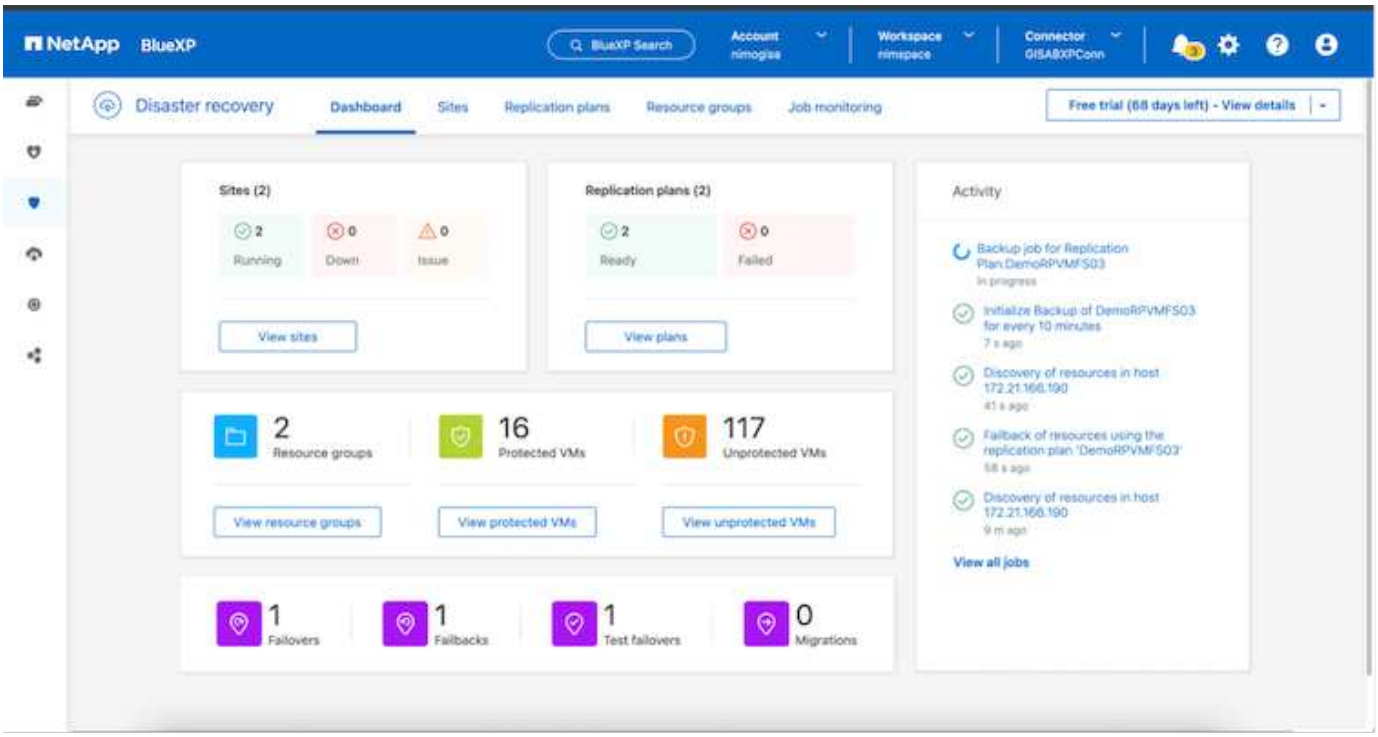


Antes de configurar o plano de recuperação de desastres, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- O agente do console está implantado na AWS VPC.
- A instância do agente do console tem conectividade com o vCenter de origem e de destino e com os sistemas de storage.
- Os sistemas de storage locais da NetApp que hospedam datastores VMFS para VMware são adicionados no Console.
- 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.

NetApp recomenda implantar o agente do Console no site de recuperação de desastres ou em um terceiro site, para que o agente do Console possa se comunicar pela rede com os recursos de origem e destino durante interrupções reais ou desastres naturais.

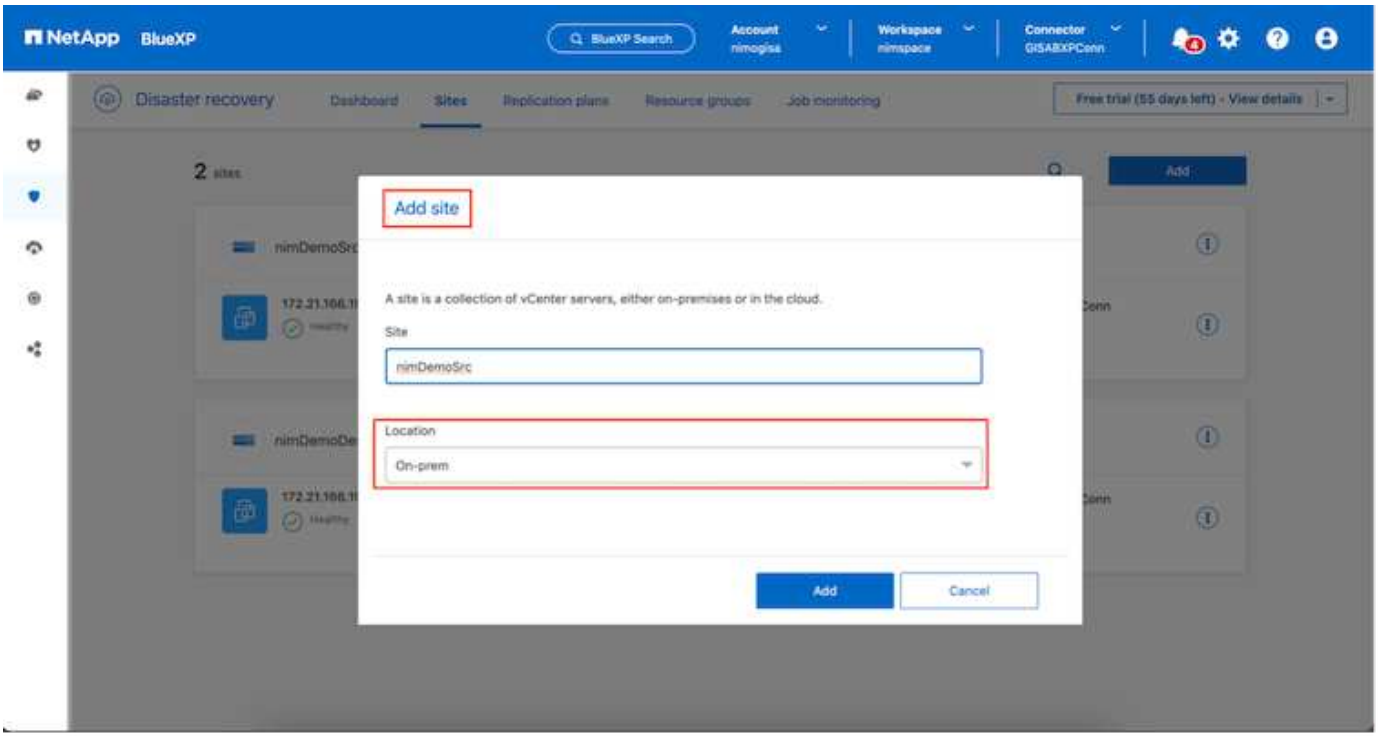


O suporte para datastores VMFS locais para locais está em fase de pré-visualização de tecnologia no momento da redação deste documento. O recurso é suportado por armazenamentos de dados VMFS baseados nos protocolos FC e ISCSI.

Configuração de recuperação de desastres

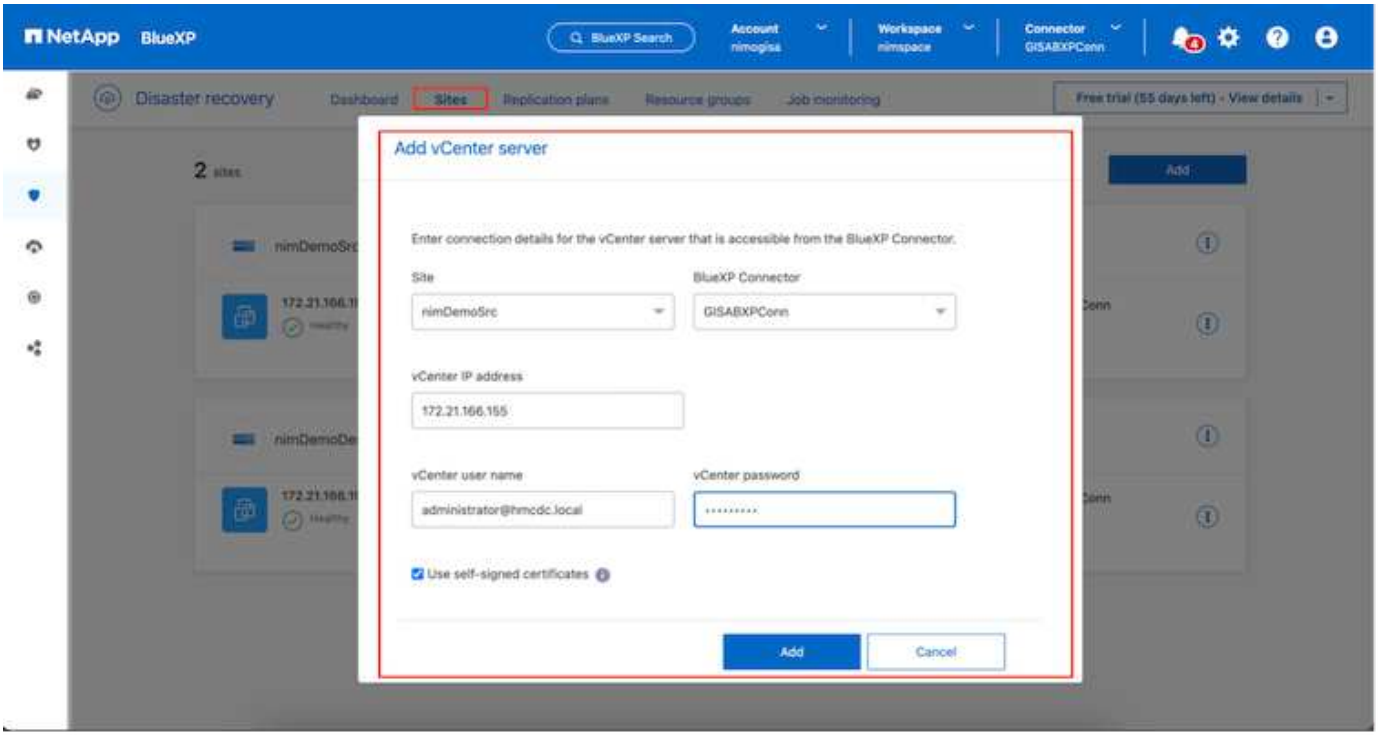
O primeiro passo na preparação para a recuperação de desastres é descobrir e adicionar o vCenter local e os recursos de storage ao Disaster Recovery.

Certifique-se de que os sistemas de storage ONTAP foram adicionados ao ambiente de trabalho no canvas. Abra o Console e selecione **Proteção > Recuperação de Desastres** na navegação à esquerda. Selecione **Descobrir servidores vCenter** ou use o menu superior e selecione **Sites > Adicionar > Adicionar vCenter**.

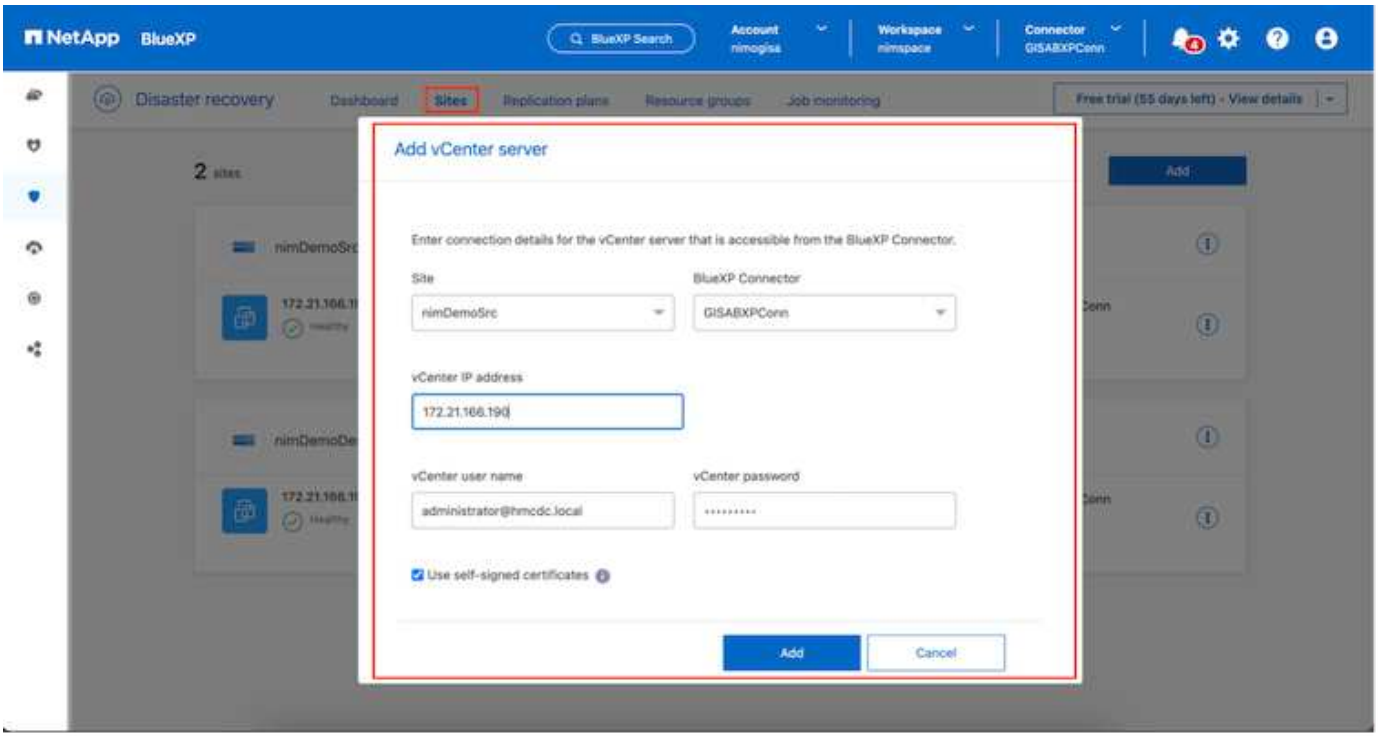


Adicione as seguintes plataformas:

- **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

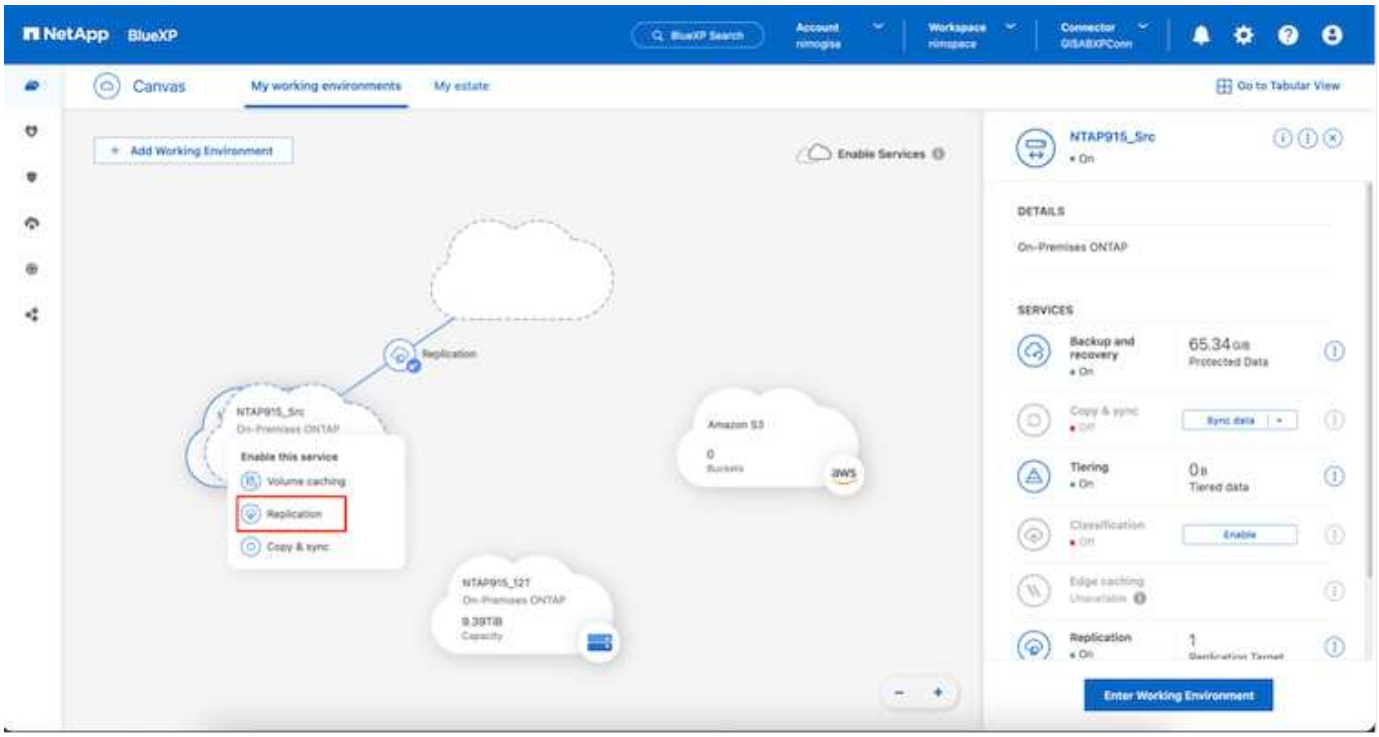
O SnapMirror usa snapshots ONTAP para gerenciar a transferência de dados de um local para outro. Inicialmente, uma cópia completa baseada em um instantâneo do volume de origem é copiada para o destino para executar uma sincronização de linha de base. À medida que ocorrem alterações de dados na origem, 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.

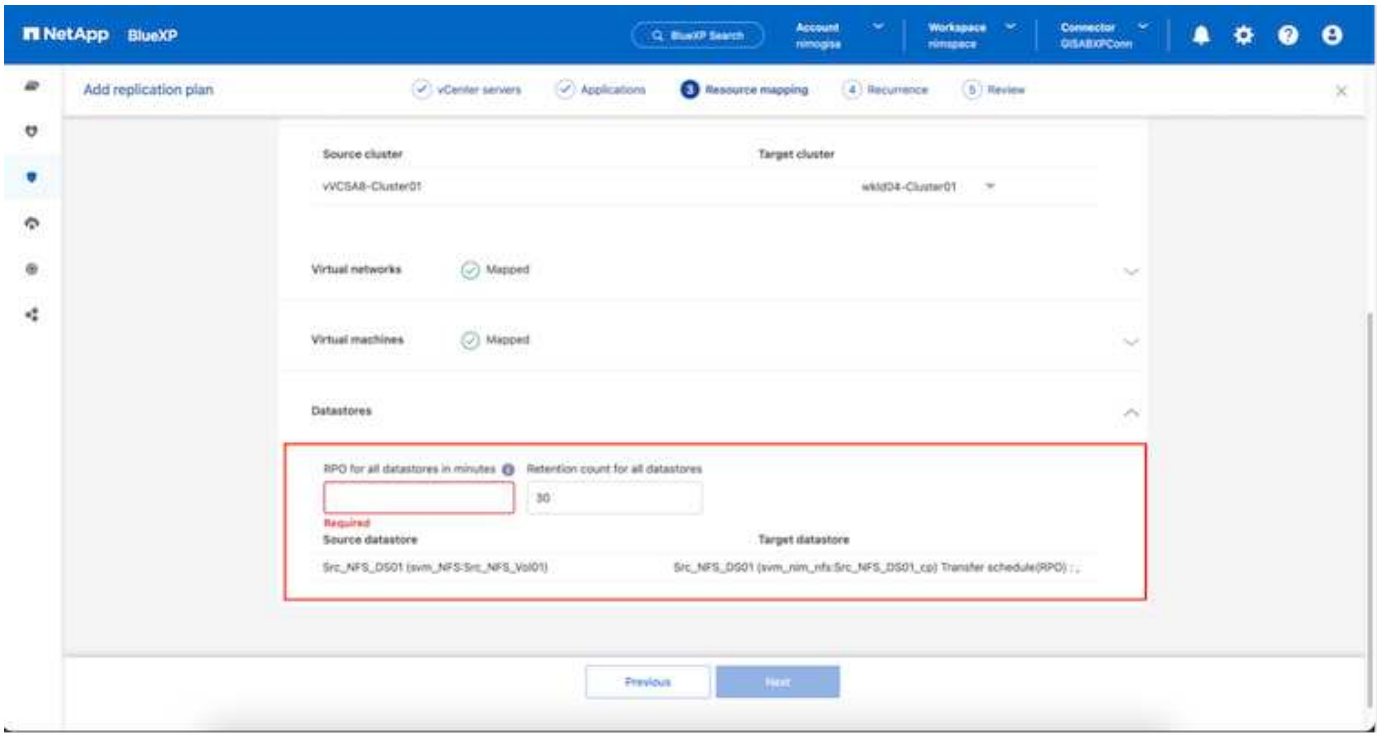
Como configurá-lo para recuperação de desastres do VMware

O processo para criar a replicação do SnapMirror permanece o mesmo para qualquer aplicação. O processo pode ser manual ou automatizado. A maneira mais fácil é usar o Console para configurar a replicação do SnapMirror, usando o recurso simples de arrastar e soltar o sistema ONTAP de origem no ambiente sobre o destino para acionar o assistente que guia você pelo restante do processo.



Os NetApp Data Services também podem 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.

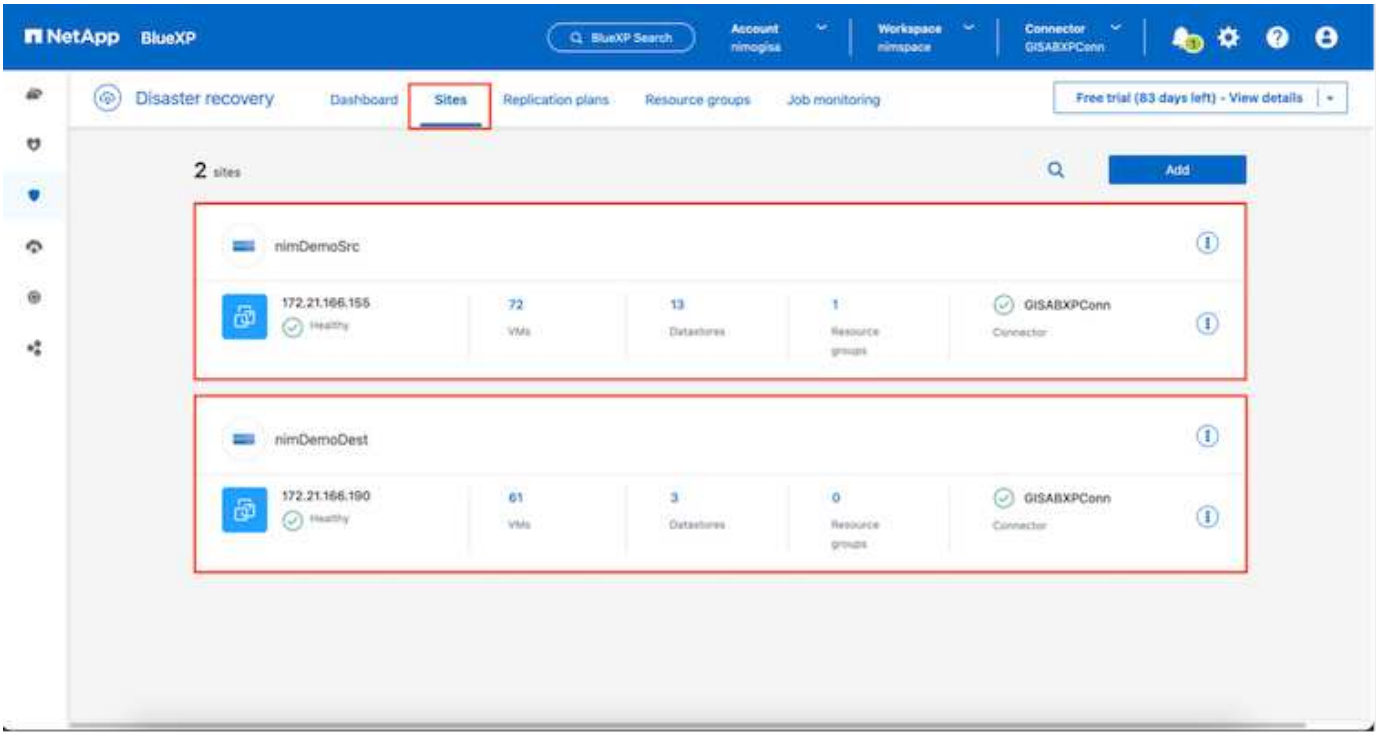


Se a relação do SnapMirror já estiver configurada para o volume via CLI, o Console reconhecerá a relação e continuará com o restante das operações do fluxo de trabalho.

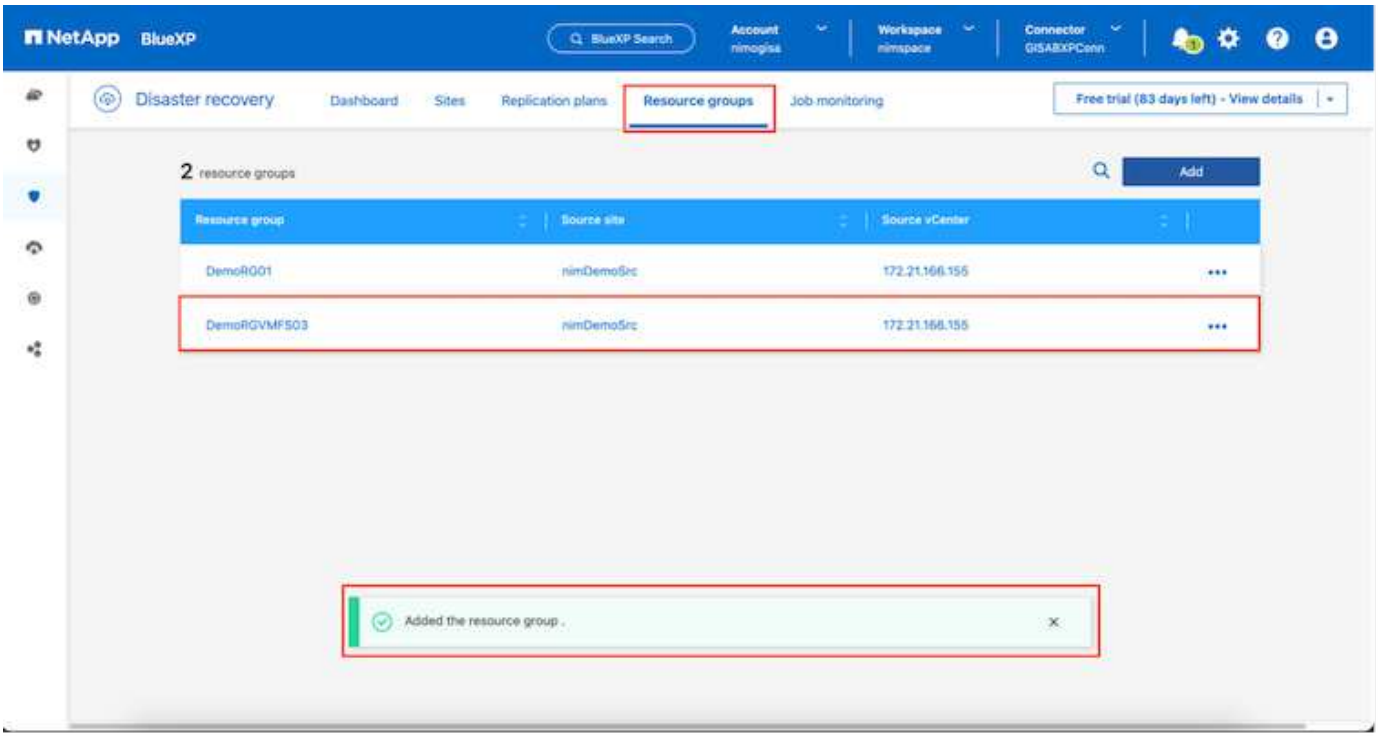
Além das abordagens acima, a replicação do SnapMirror também pode ser criada por meio da ONTAP CLI ou do System Manager. Independentemente da abordagem usada para sincronizar os dados usando SnapMirror, o Disaster Recovery orquestra o fluxo de trabalho para operações de recuperação de desastres contínuas e eficientes.

O que o Disaster Recovery pode fazer por você?

Após a adição dos sites de origem e destino, o Disaster Recovery realiza uma descoberta profunda automática e exibe as VMs juntamente com os metadados associados. O Disaster Recovery também detecta automaticamente as redes e os grupos de portas usados pelas VMs e os preenche.

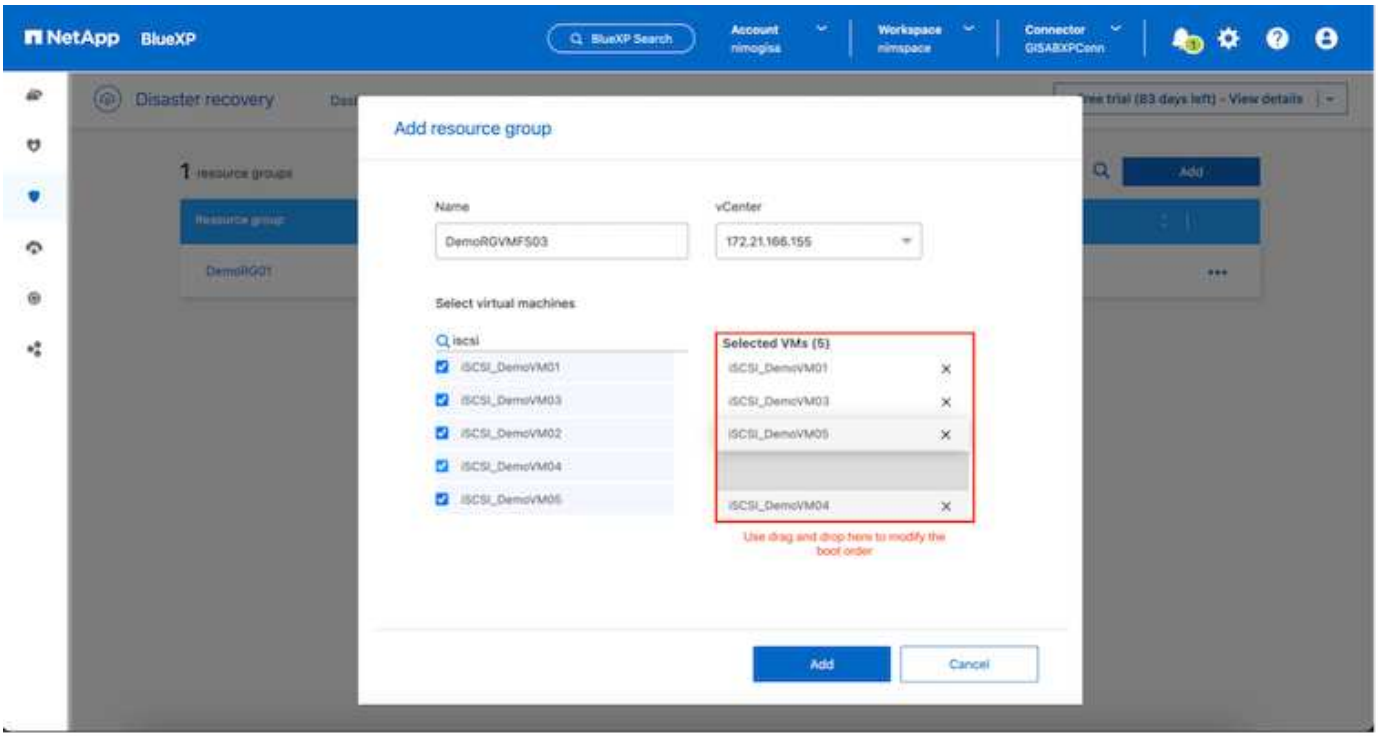


Após a adição dos sites, as VMs podem ser agrupadas em grupos de recursos. Os grupos de recursos do Disaster Recovery permitem agrupar um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização e atrasos de inicialização, que podem ser executados na recuperação. Para começar a criar grupos de recursos, acesse **Grupos de Recursos** e clique em **Criar Novo Grupo de Recursos**.

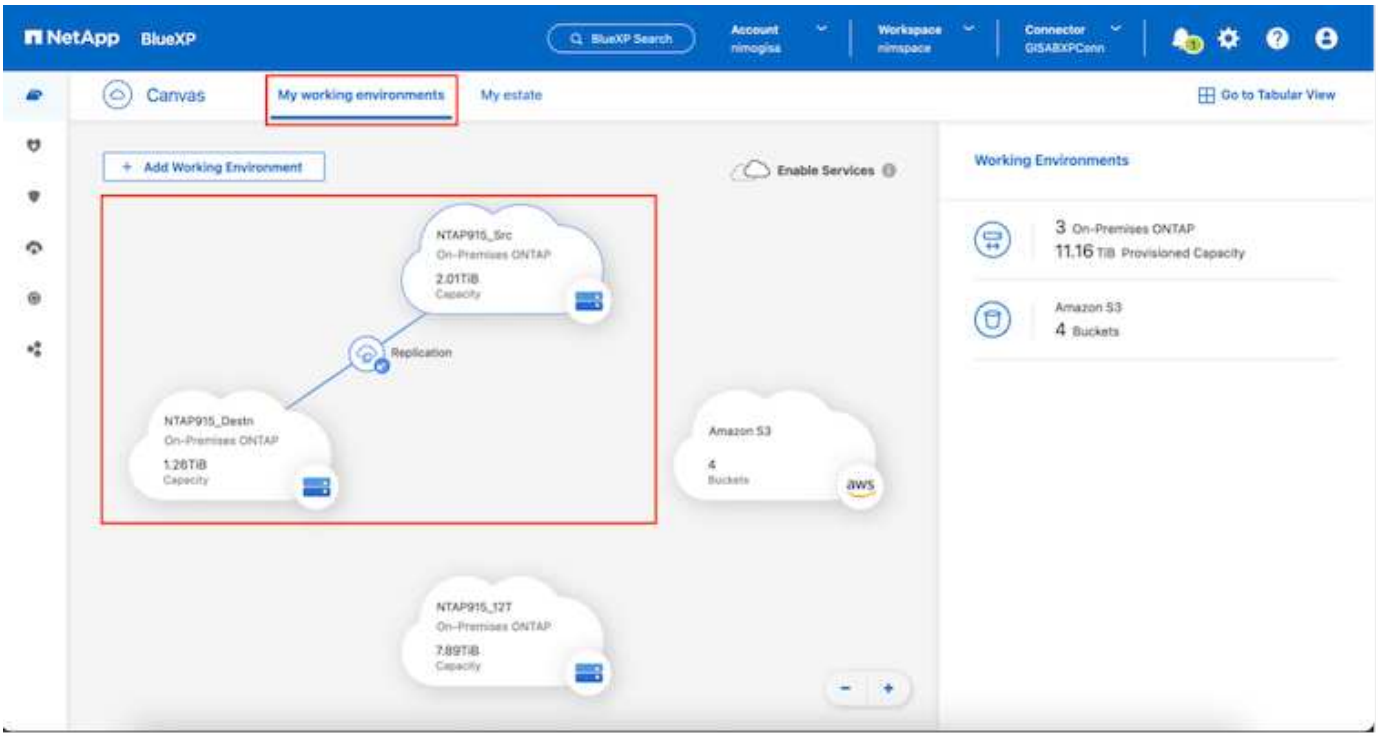


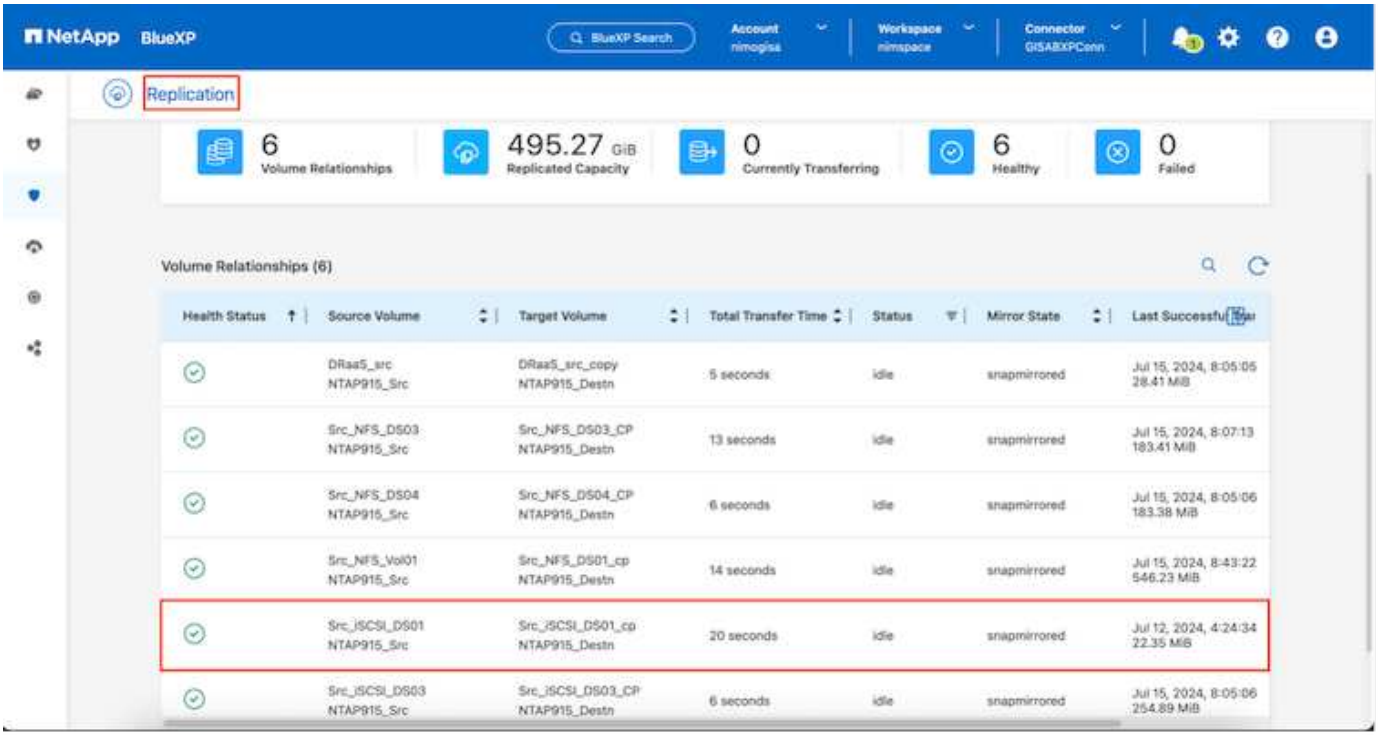
O grupo de recursos também pode ser criado durante a criação de um plano de replicação.

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.



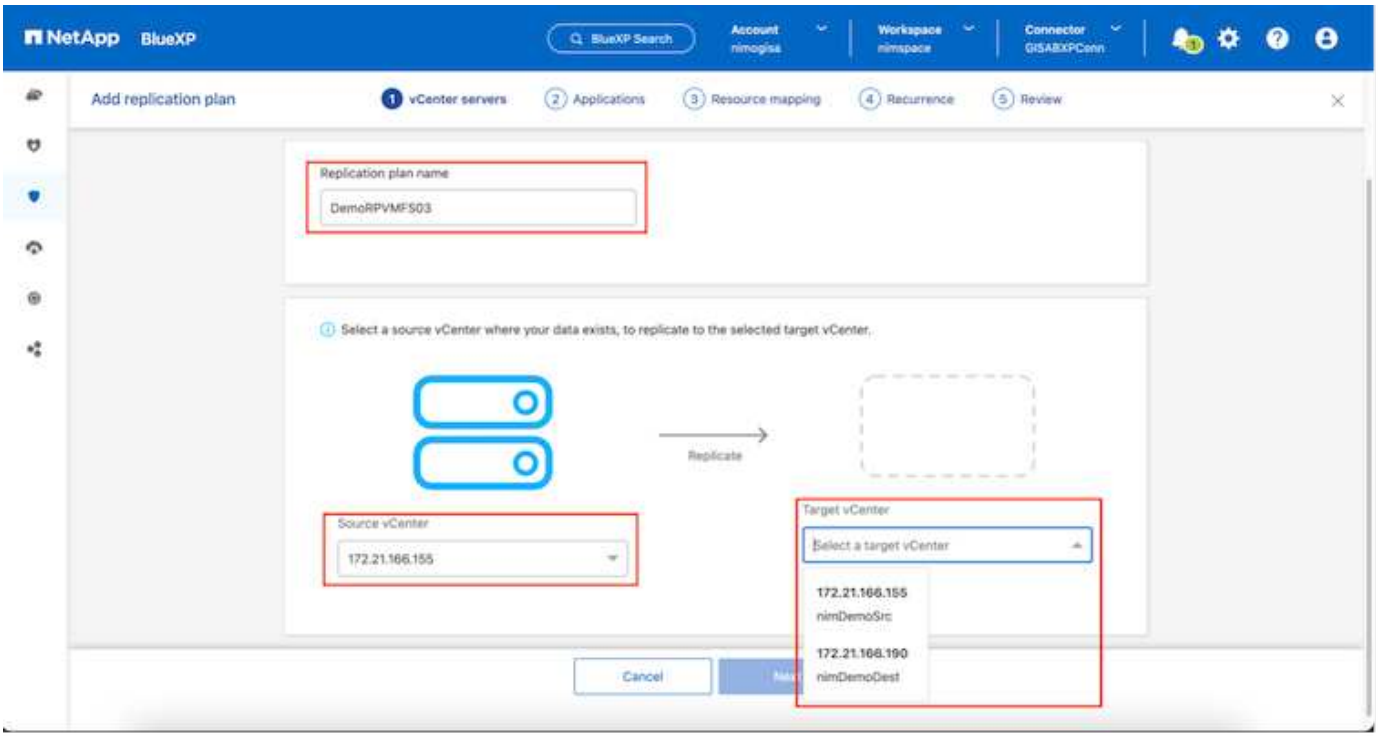
Depois que os grupos de recursos forem criados, a próxima etapa é criar o projeto de execução ou um plano para recuperar máquinas virtuais e aplicativos em caso de desastre. Conforme mencionado nos pré-requisitos, a replicação do SnapMirror pode ser configurada antecipadamente ou o DRaaS pode configurá-la usando o RPO e a contagem de retenção especificados durante a criação do plano de replicação.



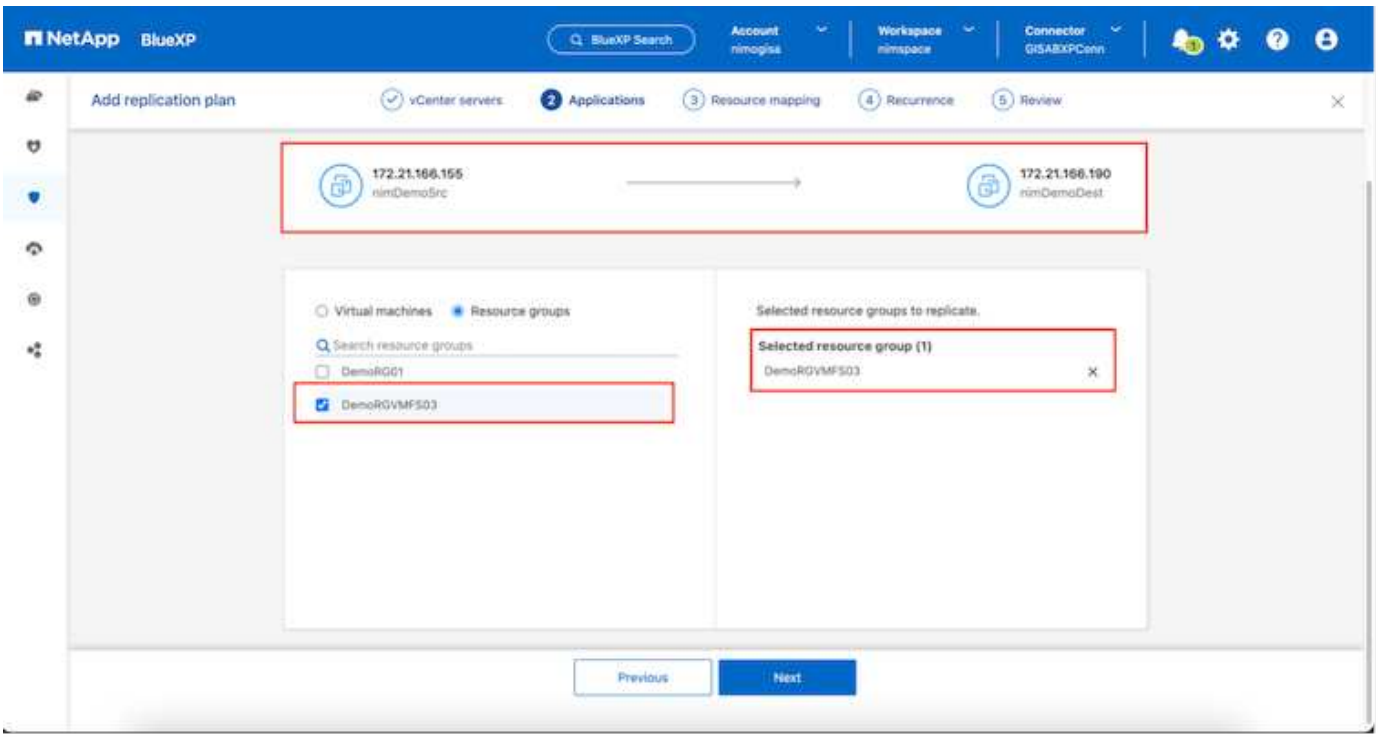


Configure o plano de replicação selecionando as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos no plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados e o mapeamento de clusters e redes. Para definir o plano 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.



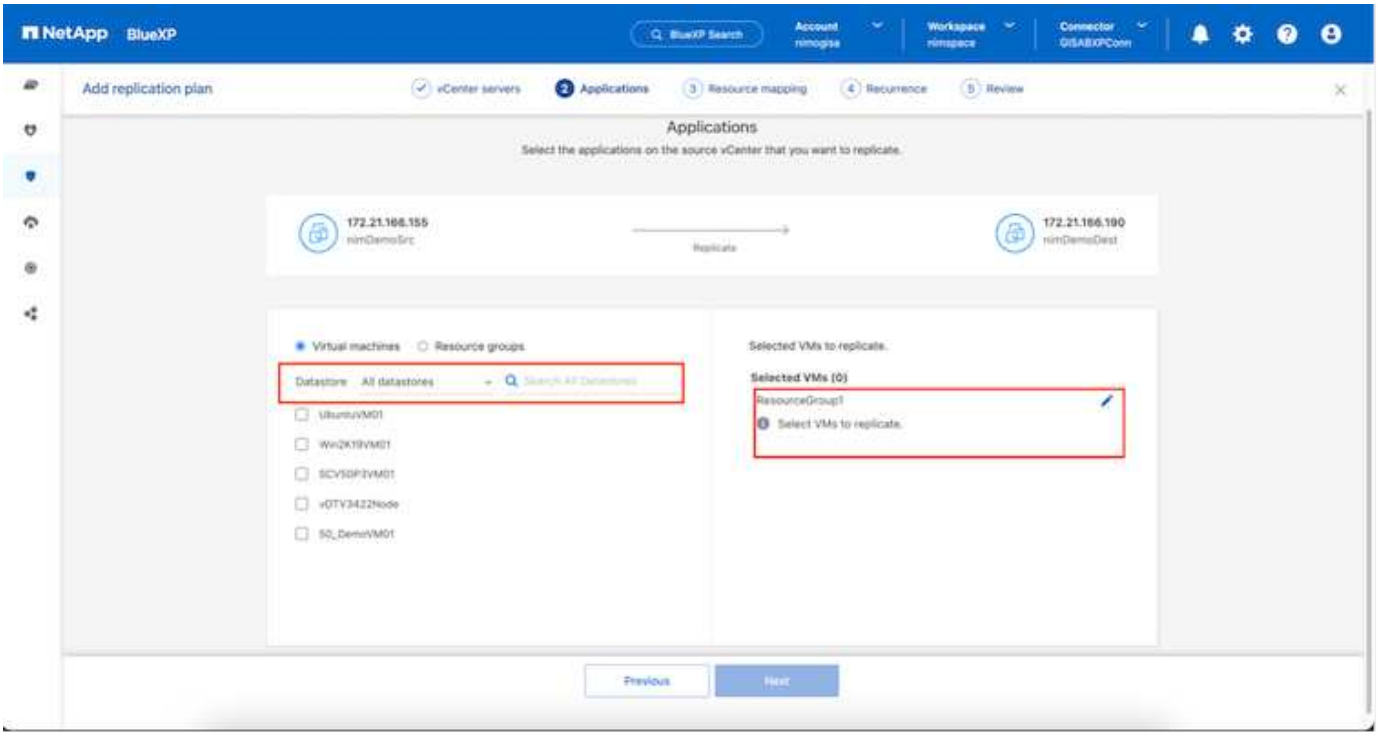
O próximo passo é selecionar grupos de recursos existentes. Se nenhum grupo de recursos for criado, o assistente ajudará a agrupar as máquinas virtuais necessárias (basicamente, criar grupos de recursos funcionais) com base nos objetivos de recuperação. Isso também ajuda a definir a sequência de operação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



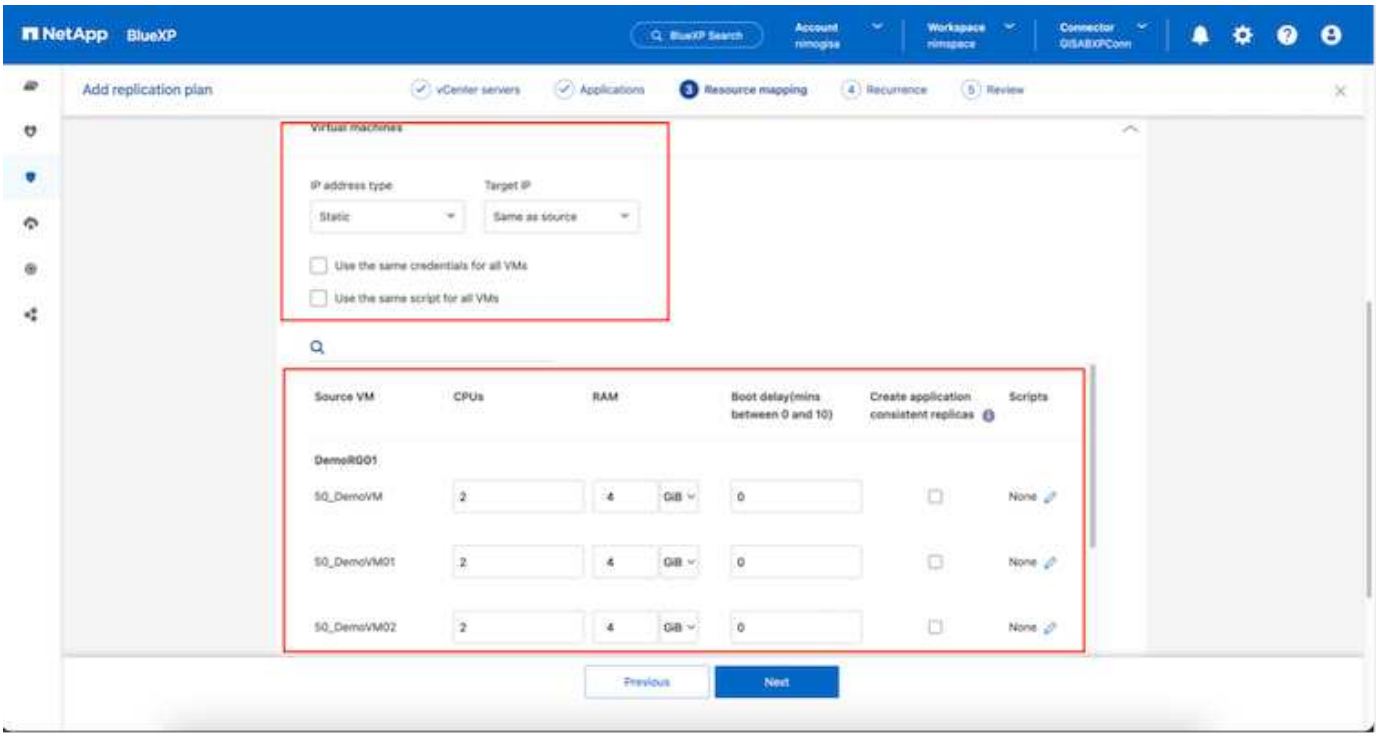
O grupo de recursos permite definir a ordem de inicialização usando a funcionalidade de arrastar e soltar. Ele pode ser usado para modificar facilmente a ordem em que as VMs serão ligadas durante o processo de recuperação.

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.

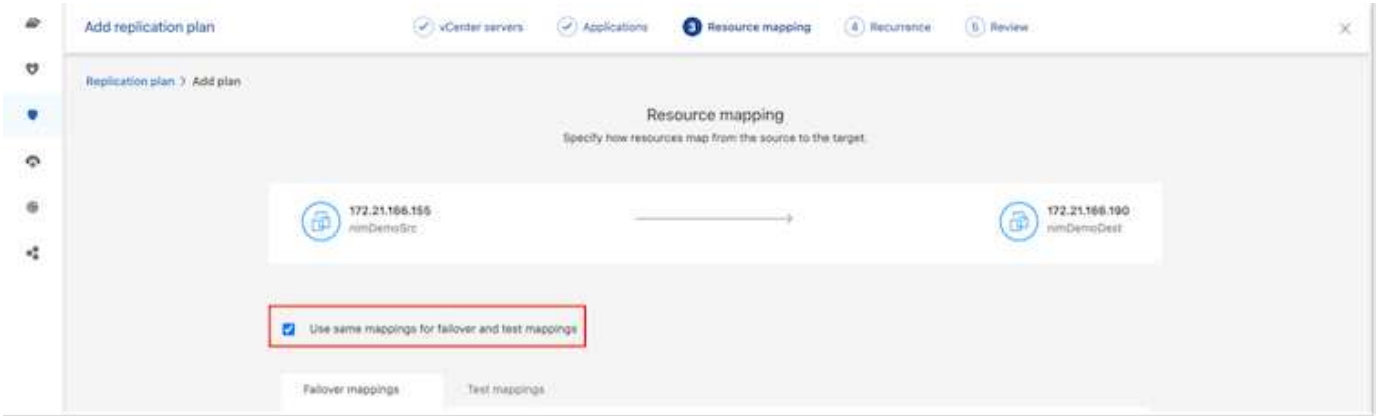
A captura de tela abaixo mostra a opção de filtrar máquinas virtuais ou armazenamentos de dados específicos com base em requisitos organizacionais, caso os grupos de recursos não sejam criados previamente.



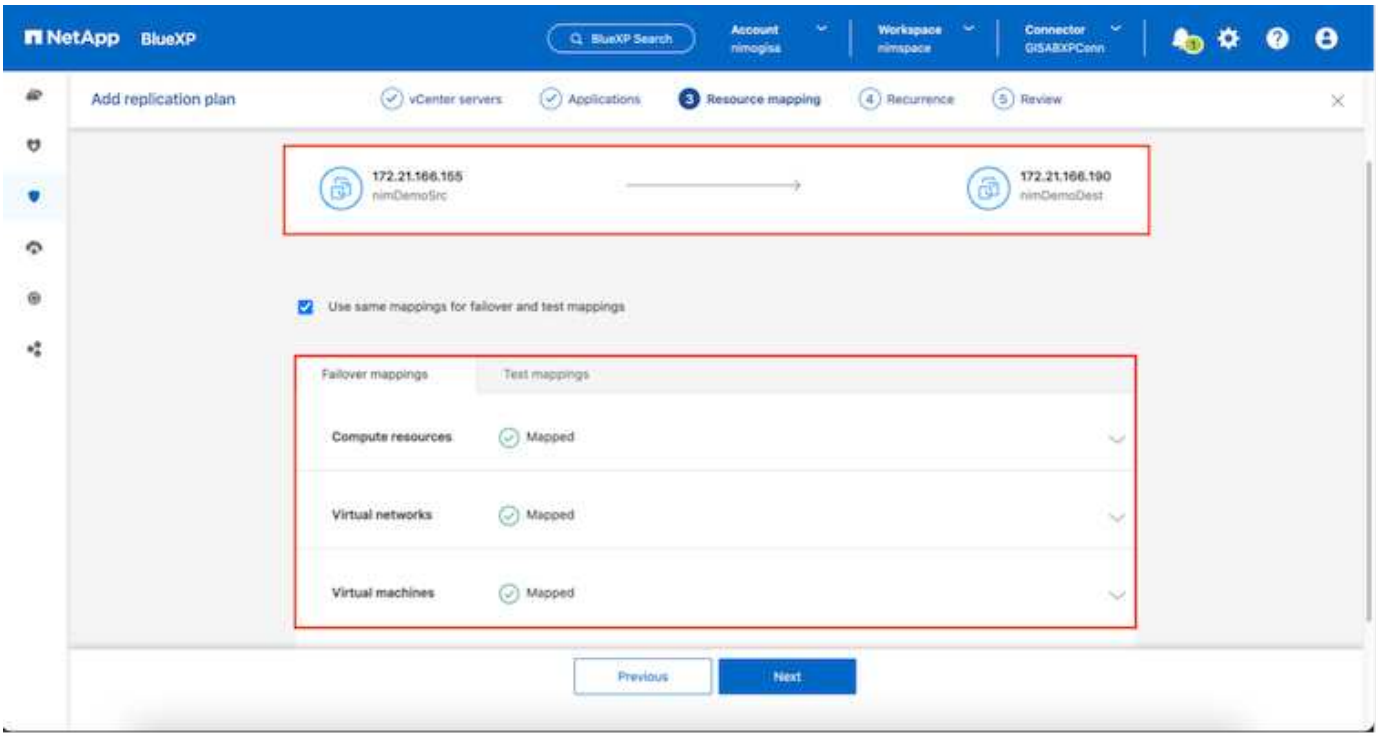
Após selecionar os grupos de recursos, crie os mapeamentos de failover. Nesta etapa, especifique como os recursos do ambiente de origem são mapeados para o destino. Isso inclui recursos de computação e redes virtuais. Personalização de IP, scripts pré e pós, atrasos de inicialização, consistência de aplicativos e assim por diante. Para obter informações detalhadas, consulte "Crie um plano de replicação".



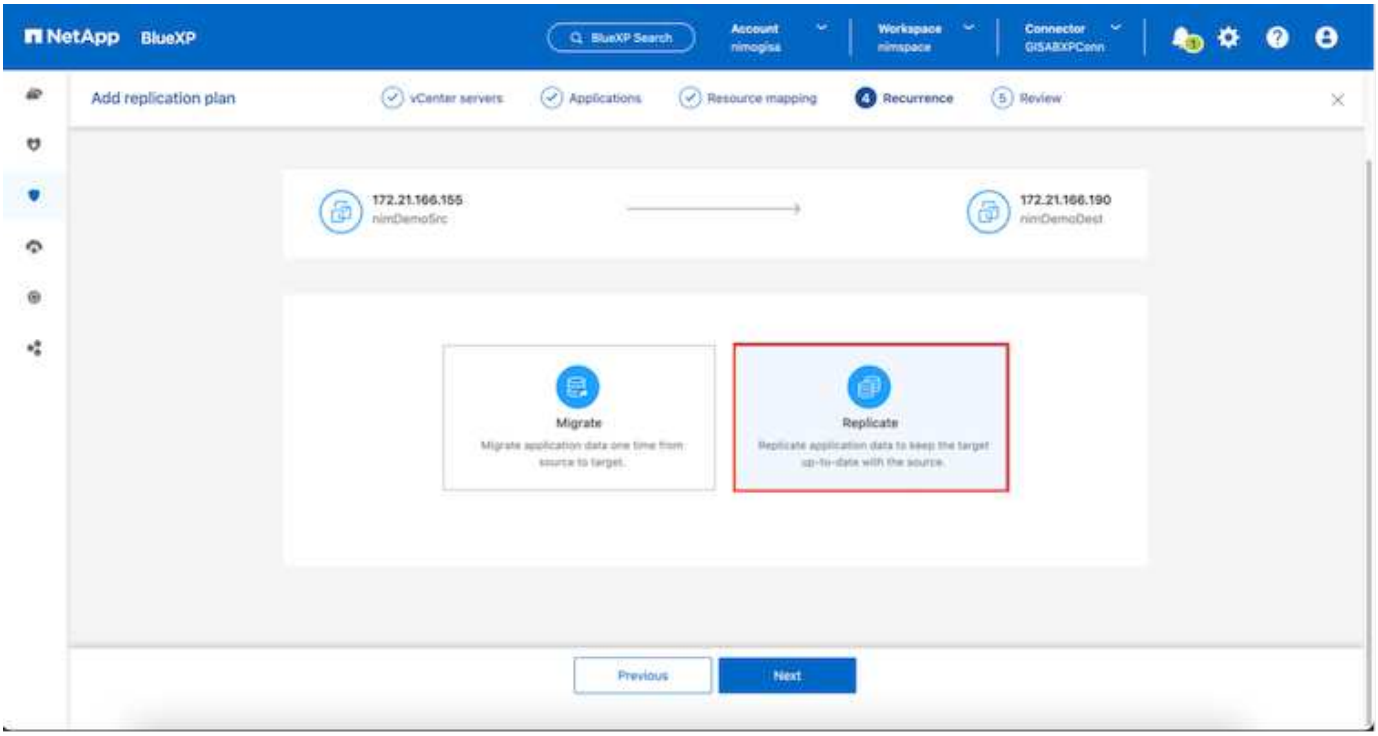
Por padrão, os mesmos parâmetros de mapeamento são usados para operações de teste e failover. Para aplicar mapeamentos diferentes para o ambiente de teste, selecione a opção Mapeamento de teste depois de desmarcar a caixa de seleção, conforme mostrado abaixo:



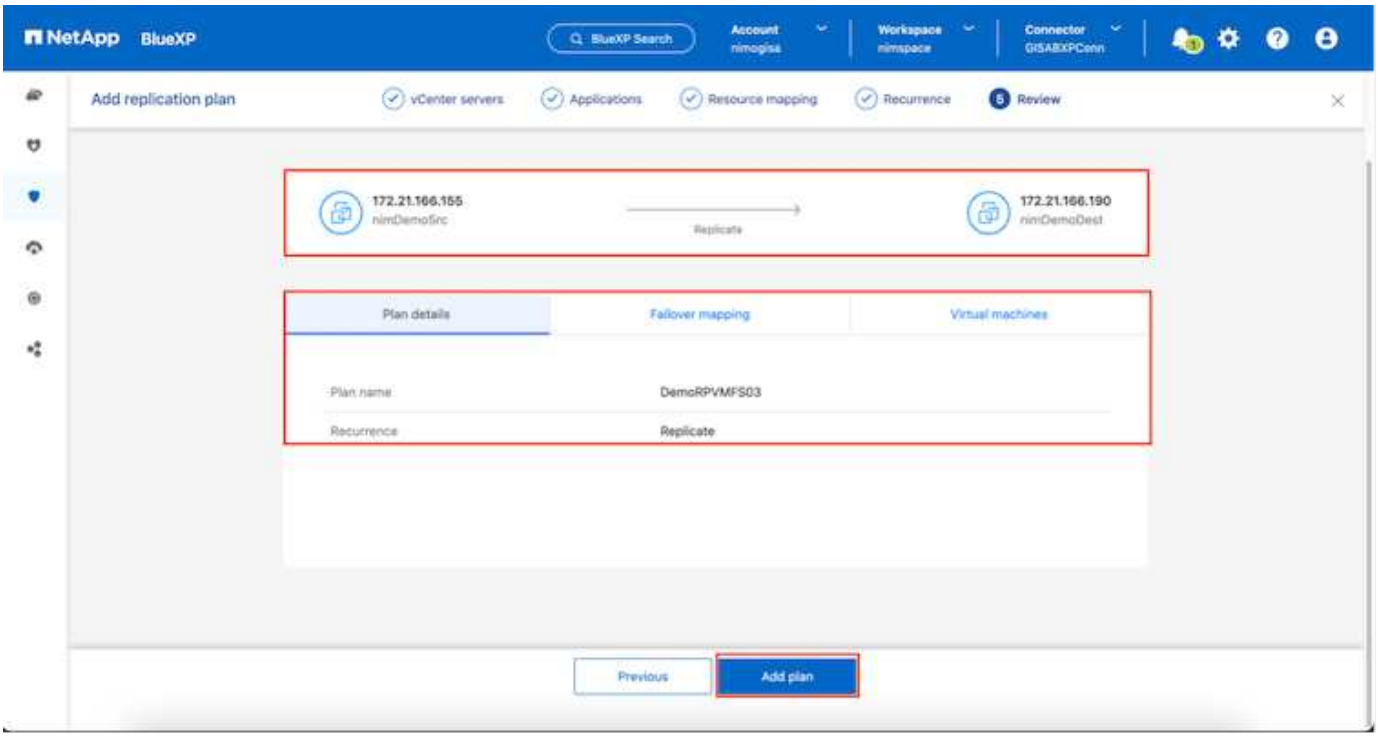
Quando o mapeamento de recursos estiver concluído, clique em Avançar.

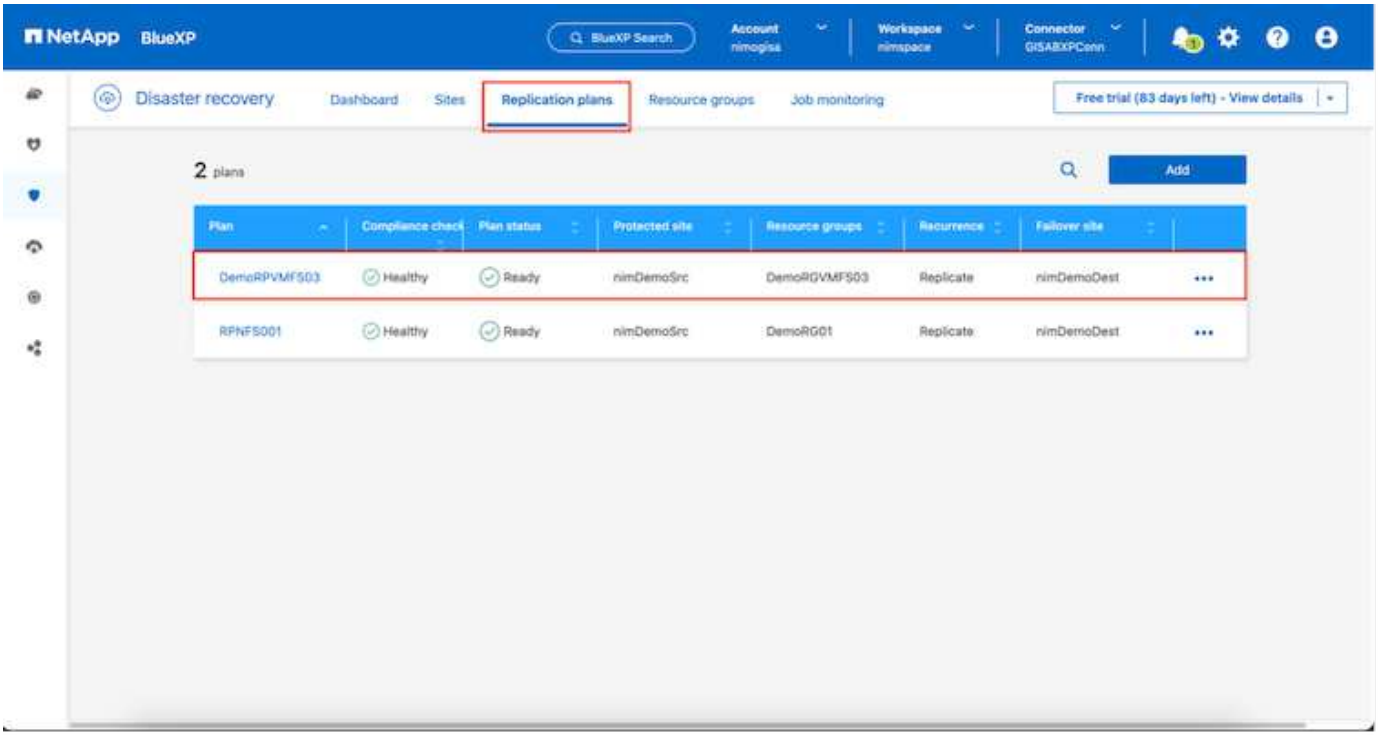


Selecione o tipo de recorrência. Em palavras simples, selecione Migrar (migração única usando failover) ou a opção de replicação contínua recorrente. Neste passo a passo, a opção Replicar está selecionada.

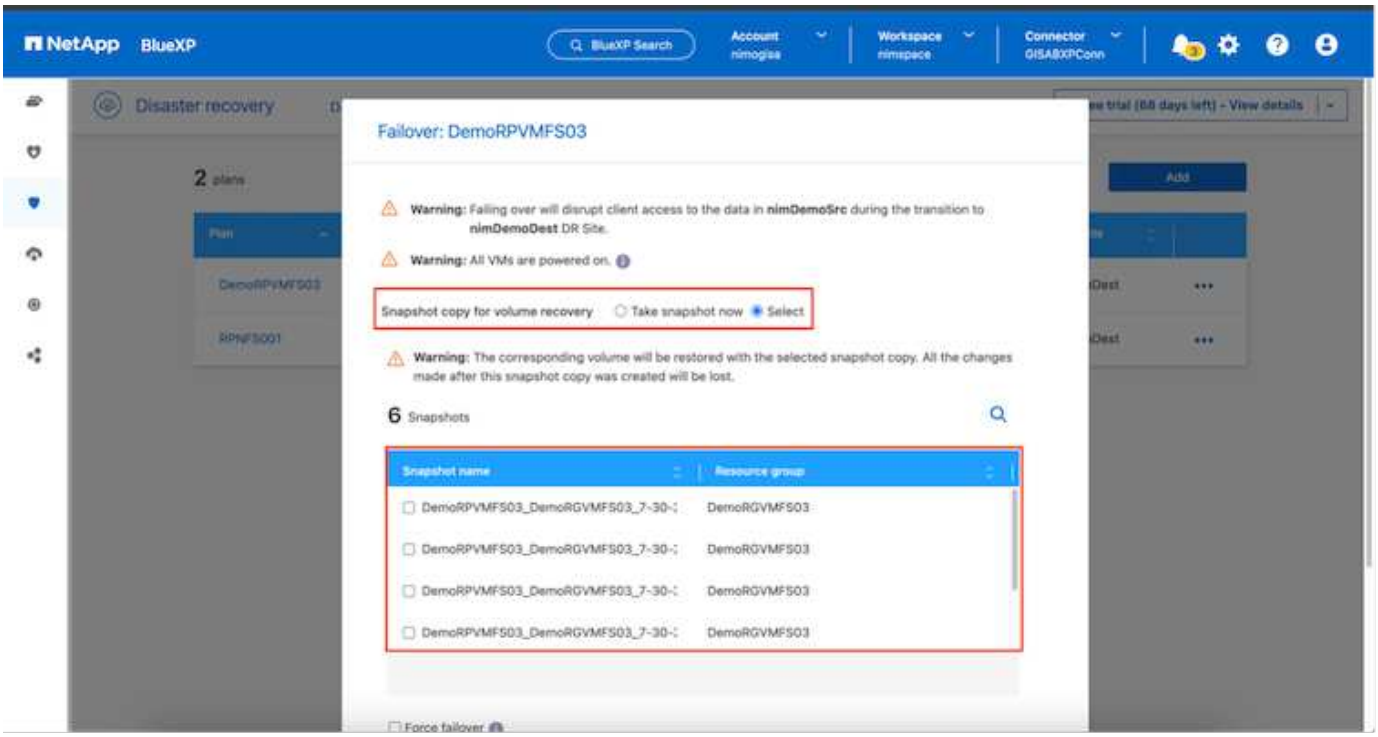


Uma vez concluído, revise os mapeamentos criados e clique em Adicionar plano.

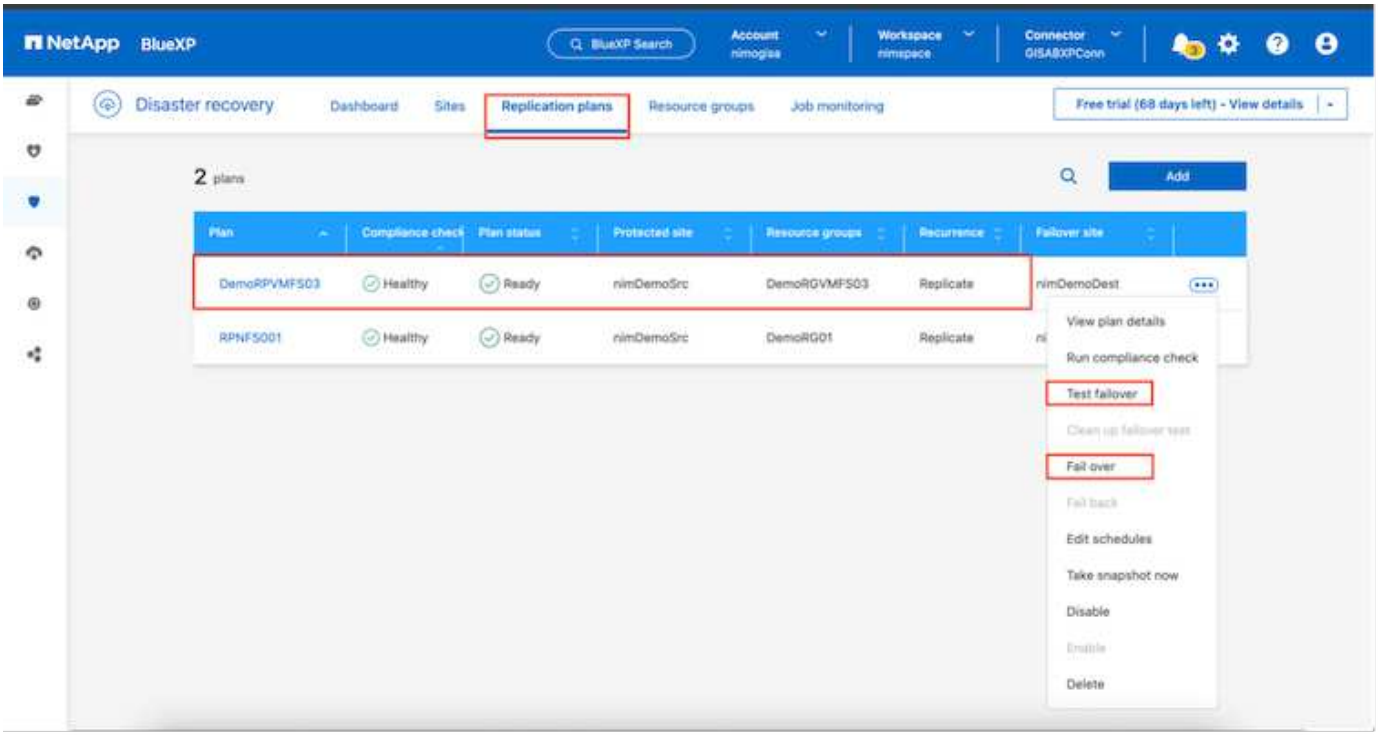




Após a criação do plano de replicação, o failover pode ser executado de acordo com os requisitos, selecionando a opção de failover, a opção de teste de failover ou a opção de migração. O Disaster Recovery garante que o processo de replicação seja executado de acordo com o plano a cada 30 minutos. Durante as opções de failover e teste de failover, você pode usar a cópia Snapshot mais recente do SnapMirror ou selecionar uma cópia Snapshot específica de uma cópia Snapshot de ponto no tempo (de acordo com a política de retenção do SnapMirror). A opção de ponto no tempo pode ser muito útil se ocorrer um evento de corrupção, como ransomware, em que as réplicas mais recentes já estejam comprometidas ou criptografadas. O Disaster Recovery exibe 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**.

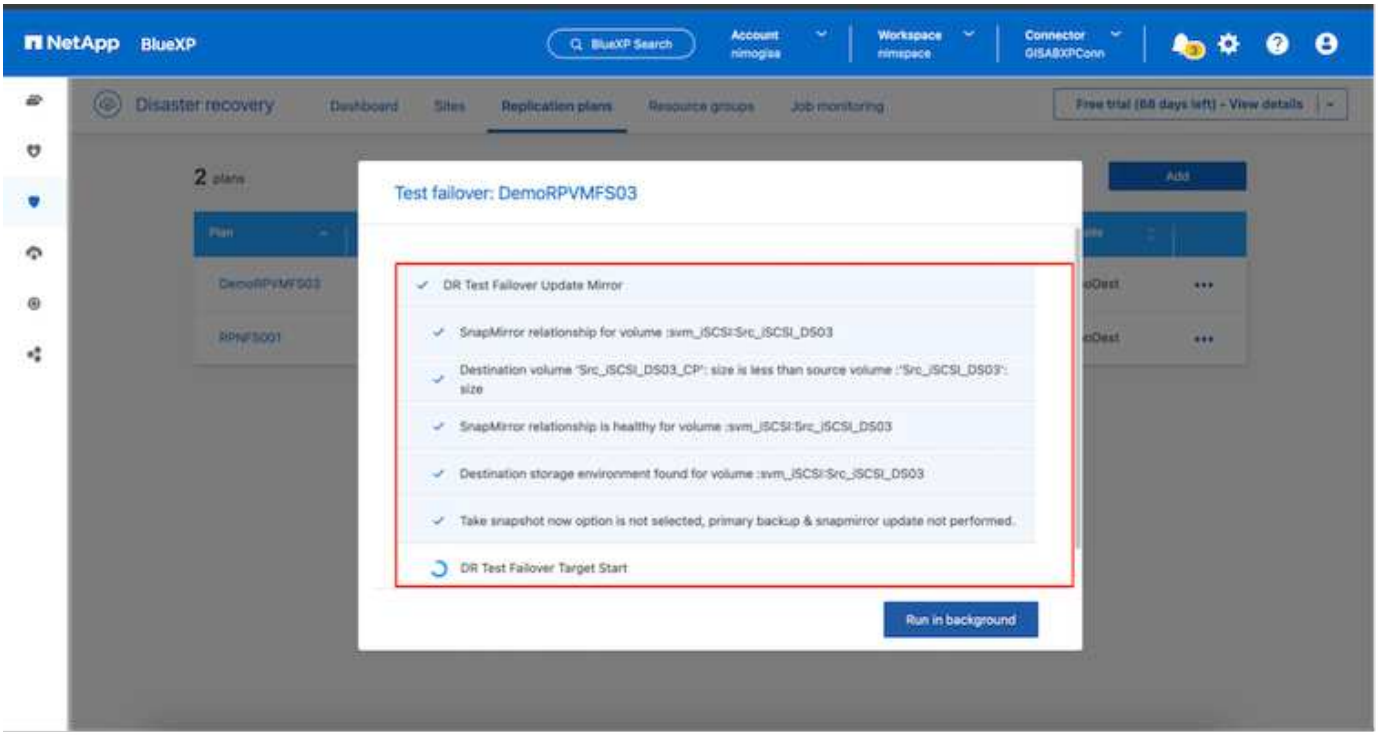


O que acontece durante uma operação de failover ou failover de teste?

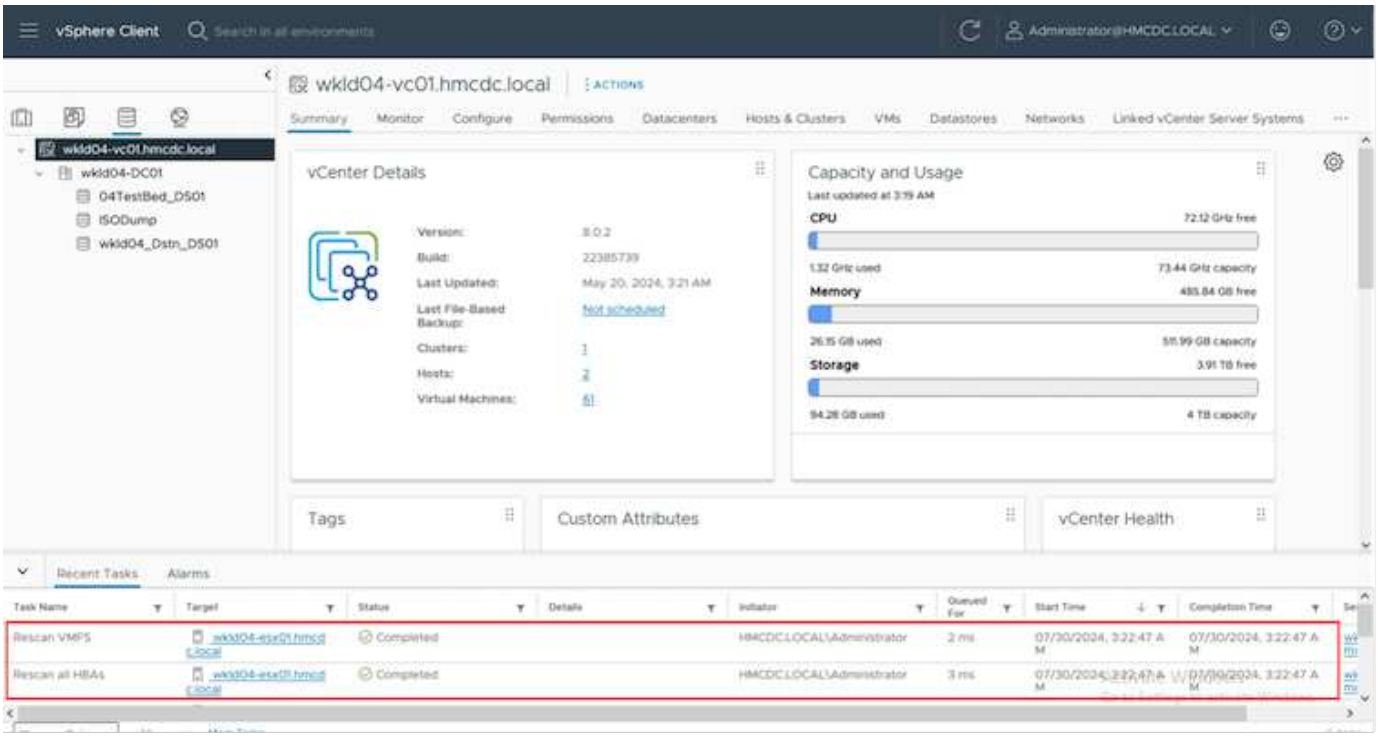
Durante uma operação de failover de teste, o Disaster Recovery cria um volume FlexClone no sistema de storage ONTAP de destino usando a cópia Snapshot mais recente ou um snapshot selecionado do volume de destino.

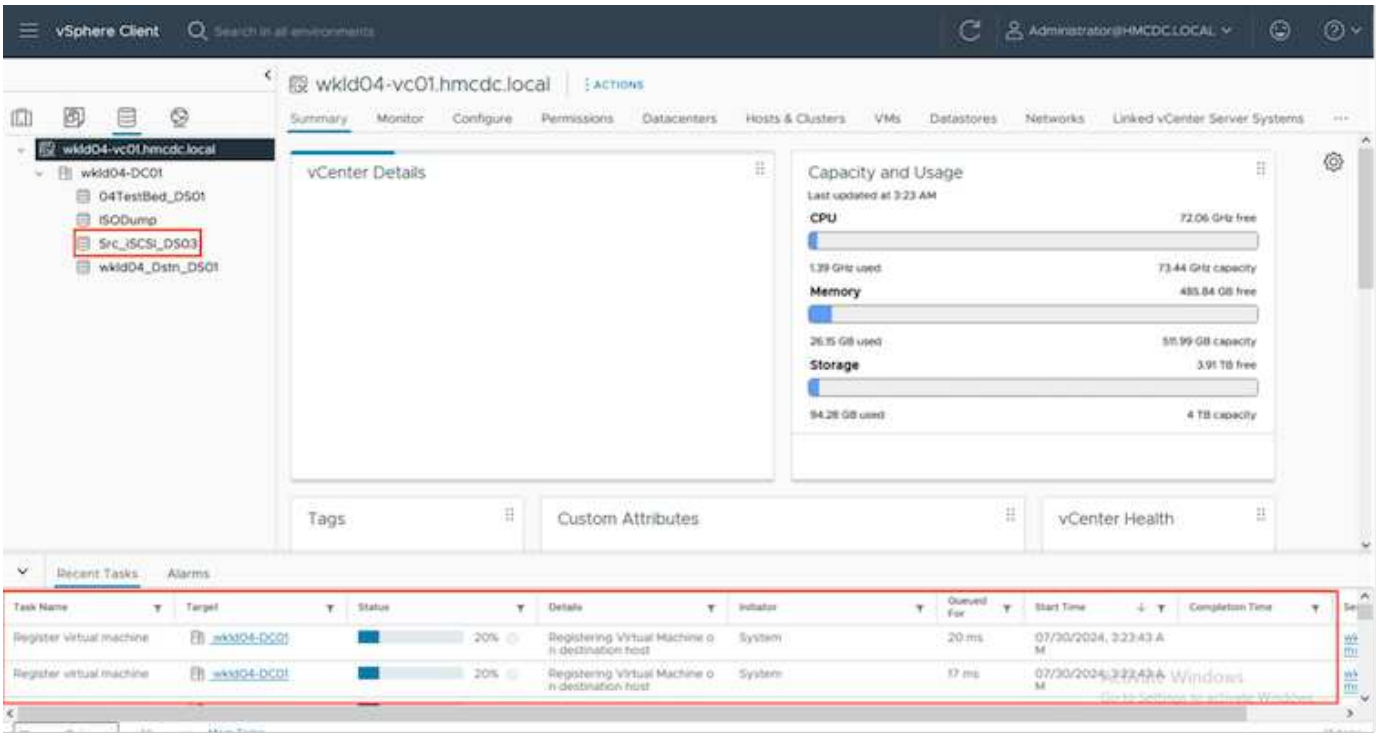
Uma operação de failover de teste cria um volume clonado no sistema de armazenamento ONTAP de destino.

Executar uma operação de recuperação de teste não afeta a replicação do SnapMirror .



Durante o processo, o 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 dá suporte ao volume FlexClone é mapeado para os hosts ESXi.

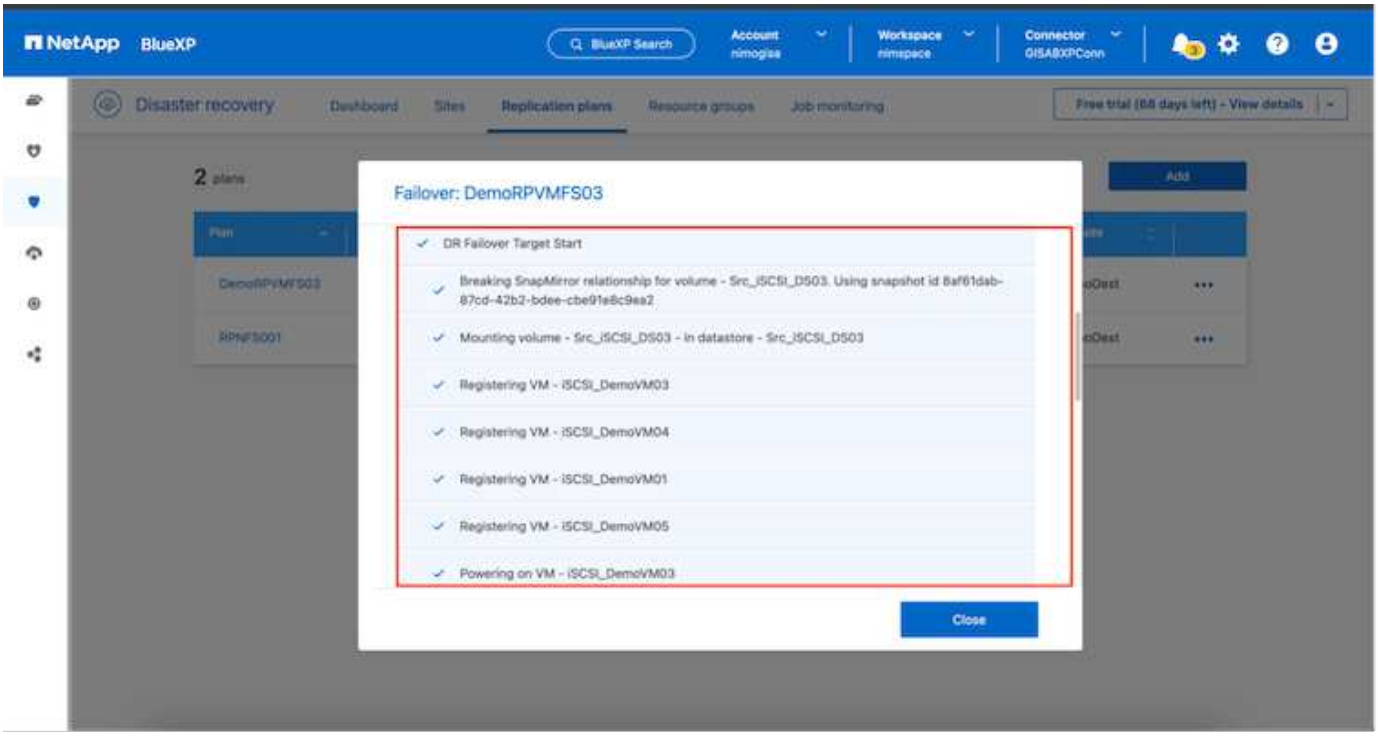




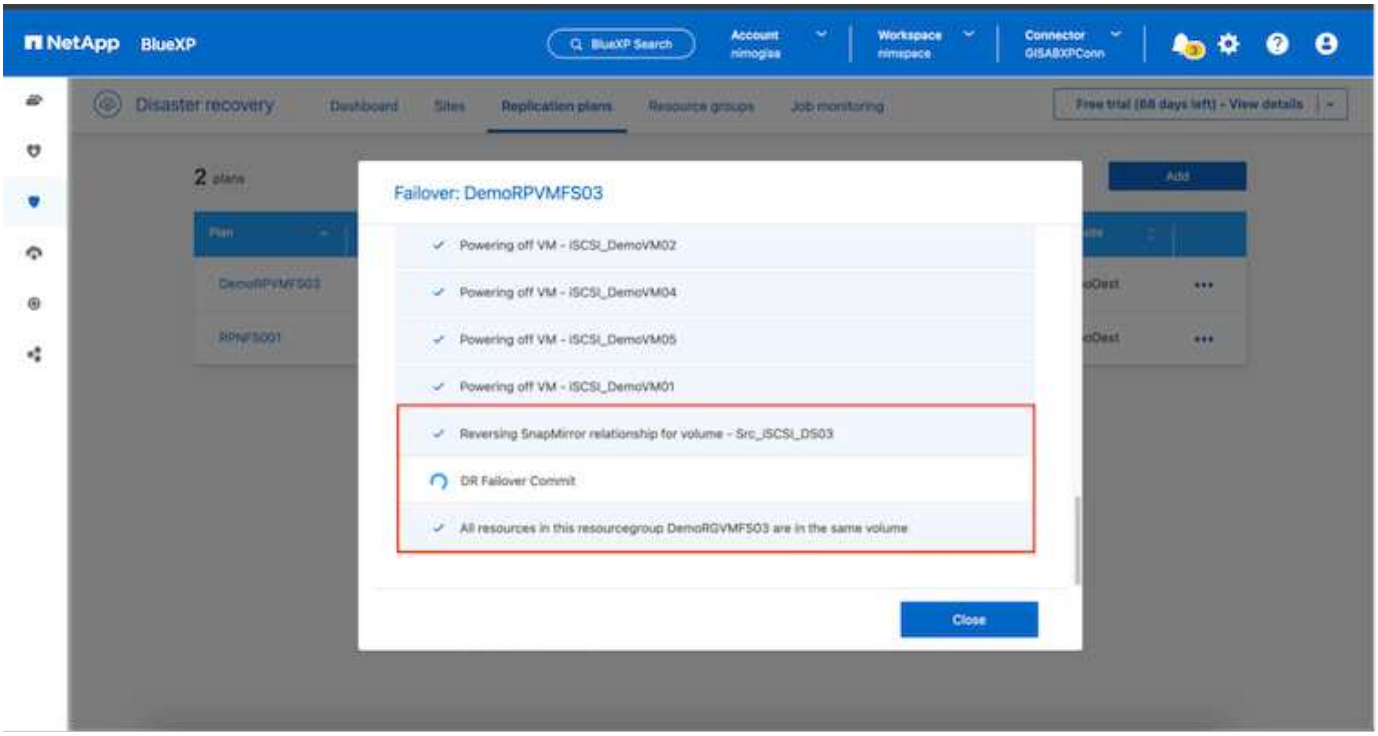
Quando a operação de failover de teste for concluída, a operação de limpeza poderá ser acionada usando **"Clean Up failover test"**. Durante essa operação, o Disaster Recovery destrói o volume FlexClone que foi usado na operação.

Em caso de um desastre real, o Disaster Recovery executa as etapas a seguir:

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

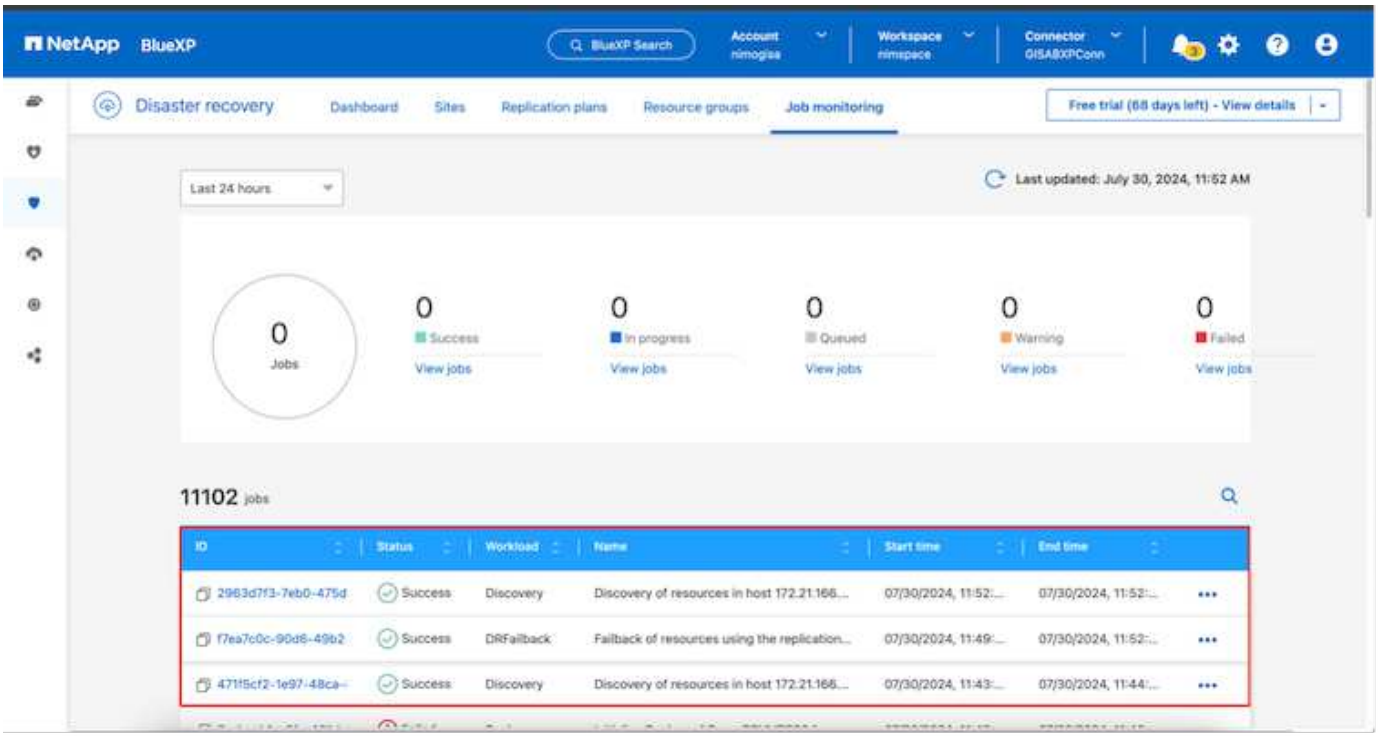


Assim que o site principal estiver operacional, o Disaster Recovery permite a ressincronização reversa do SnapMirror e permite o failback, que novamente pode ser realizado com um simples clique.



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.

A partir do Console ou da ONTAP CLI, você pode monitorar o status de integridade da replicação dos volumes do datastore apropriados, e o status de um failover ou failover de teste pode ser acompanhado por meio do Job Monitoring.



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" .

Multicloud híbrida NetApp com cargas de trabalho de contêiner Red Hat OpenShift

Começar

Soluções NetApp Hybrid Multicloud para cargas de trabalho do Red Hat OpenShift Container

A NetApp está observando um aumento significativo de clientes modernizando seus aplicativos empresariais legados e criando novos aplicativos usando contêineres e plataformas de orquestração criadas em torno do Kubernetes. O Red Hat OpenShift Container Platform é um exemplo que vemos adotado por muitos de nossos clientes.

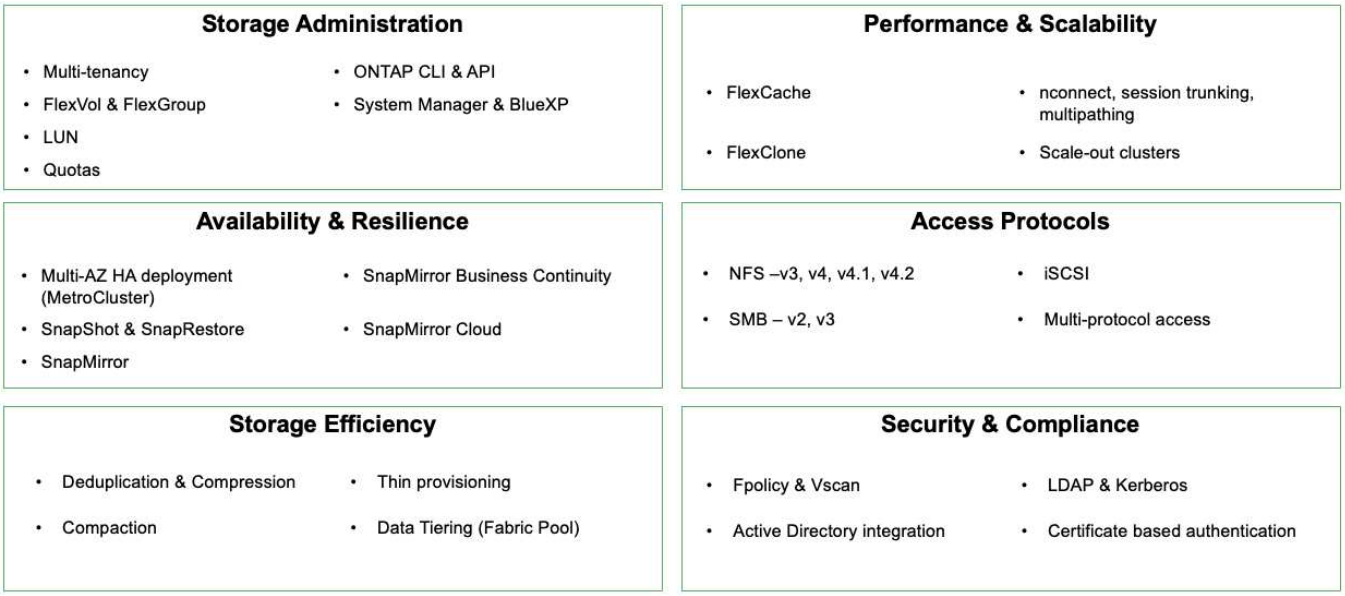
Visão geral

À medida que mais e mais clientes começam a adotar contêineres em suas empresas, a NetApp está perfeitamente posicionada para ajudar a atender às necessidades de armazenamento persistente de seus aplicativos com estado e às necessidades clássicas de gerenciamento de dados, como proteção de dados, segurança de dados e migração de dados. No entanto, essas necessidades são atendidas por meio de diferentes estratégias, ferramentas e métodos.

As opções de armazenamento baseadas em **NetApp ONTAP** listadas abaixo oferecem segurança, proteção de dados, confiabilidade e flexibilidade para contêineres e implantações do Kubernetes.

- Armazenamento autogerenciado no local:
  - Armazenamento conectado à estrutura NetApp (FAS), matrizes FAS All Flash NetApp (AFF), matriz All SAN NetApp (ASA) e ONTAP Select
- Armazenamento gerenciado pelo provedor no local:
  - O NetApp Keystone fornece armazenamento como serviço (STaaS)
- Armazenamento autogerenciado na nuvem:
  - O NetApp Cloud Volumes ONTAP(CVO) fornece armazenamento autogerenciado em hiperescaladores
- Armazenamento gerenciado pelo provedor na nuvem:
  - Amazon FSx for NetApp ONTAP, Azure NetApp Files e Google Cloud NetApp Volumes fornecem armazenamento baseado em arquivos na nuvem.

ONTAP feature highlights

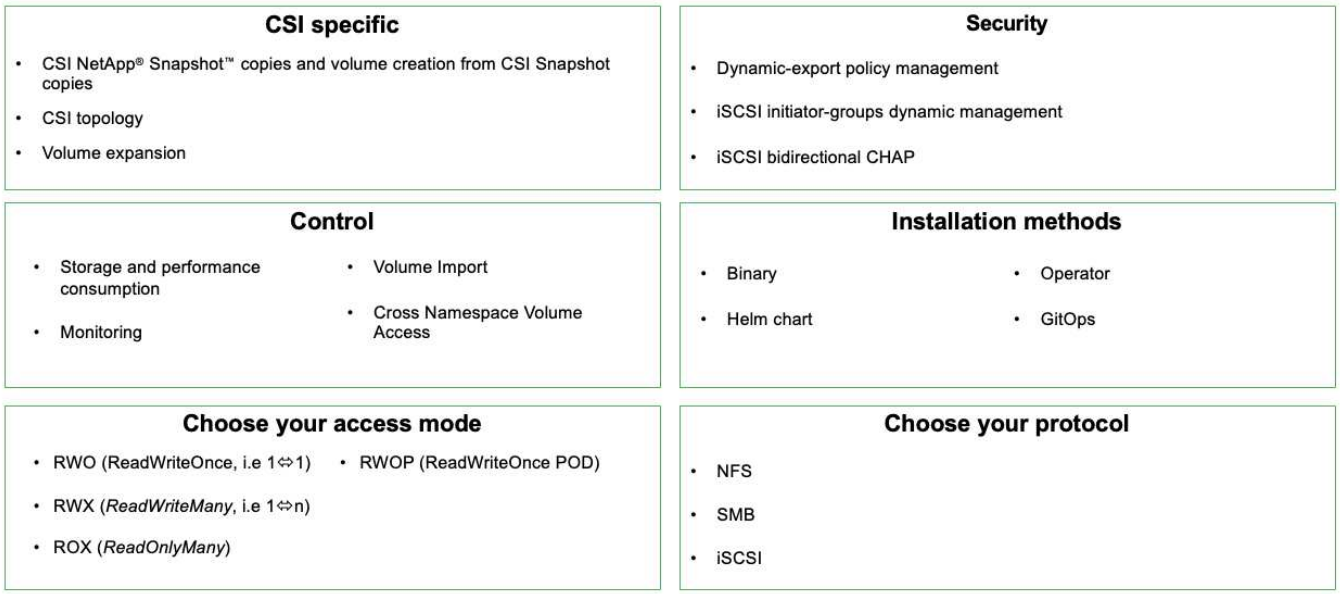


O **NetApp Console** permite gerenciar todos os seus ativos de storage e dados a partir de um único plano de controle/interface.

Você pode usar o NetApp Console para criar e administrar storage de nuvem (por exemplo, o Cloud Volumes ONTAP e o Azure NetApp Files), para mover, proteger e analisar dados e para controlar diversos dispositivos de storage locais e de borda.

- NetApp Trident** é um orquestrador de armazenamento compatível com CSI que permite o consumo rápido e fácil de armazenamento persistente apoiado por uma variedade de opções de armazenamento NetApp mencionadas acima. É um software de código aberto mantido e suportado pela NetApp.

Astra Trident CSI feature highlights



Cargas de trabalho de contêineres críticas aos negócios precisam de mais do que apenas volumes persistentes. Seus requisitos de gerenciamento de dados também exigem proteção e migração dos objetos do aplicativo Kubernetes.

> Os dados do aplicativo incluem objetos do Kubernetes, além dos dados do usuário. Alguns exemplos são os seguintes: - objetos do Kubernetes, como especificações de pods, PVCs, implantações, serviços - objetos de configuração personalizados, como mapas de configuração e segredos - dados persistentes, como cópias de snapshot, backups, clones - recursos personalizados, como CRs e CRDs

NetApp Trident Protect, disponível como um complemento gratuito para NetApp Trident, oferece recursos avançados de gerenciamento de dados de aplicativos que aprimoram a funcionalidade e a disponibilidade de aplicativos Kubernetes com estado suportados por sistemas de armazenamento NetApp ONTAP. Trident Protect simplifica o gerenciamento, a proteção e a movimentação de cargas de trabalho conteinerizadas em nuvens públicas e ambientes locais. Ele também oferece recursos robustos de automação por meio de sua API e CLI.

Esta documentação de referência fornece validação da proteção de dados de aplicativos baseados em contêineres, implantados na plataforma RedHat OpenShift usando o Trident Protect. Além disso, a solução fornece detalhes de alto nível para a implantação e o uso do Red Hat Advanced Cluster Management (ACM) para gerenciar as plataformas de contêineres. O documento também destaca os detalhes para a integração do armazenamento NetApp com plataformas de contêiner Red Hat OpenShift usando o provisionador Trident CSI.

Propostas de valor das soluções NetApp Hybrid Multicloud para cargas de trabalho do Red Hat OpenShift Container

A maioria dos clientes não começa a criar ambientes baseados em Kubernetes sem nenhuma infraestrutura existente. Talvez eles sejam uma loja de TI tradicional executando a maioria de seus aplicativos corporativos em máquinas virtuais (em grandes ambientes VMware, por exemplo). Em seguida, eles começam a construir pequenos ambientes baseados em contêineres para satisfazer as necessidades de suas equipes modernas de desenvolvimento de aplicativos. Essas iniciativas geralmente começam pequenas e se tornam mais difundidas à medida que as equipes aprendem essas novas tecnologias e habilidades e começam a reconhecer os muitos benefícios de adotá-las. A boa notícia para os clientes é que a NetApp pode atender às necessidades de ambos os ambientes. Este conjunto de soluções para multicloud híbrida com Red Hat OpenShift capacitará os clientes da NetApp a adotar tecnologias e serviços de nuvem modernos sem precisar reformular toda a sua infraestrutura e organização. Não importa se os aplicativos e dados do cliente são hospedados no local, na nuvem, executados em máquinas virtuais ou em contêineres, a NetApp pode fornecer gerenciamento de dados consistente, proteção, segurança e portabilidade. Com essas novas soluções, o mesmo valor que a NetApp oferece em ambientes de data center locais há décadas estará disponível em todo o horizonte de dados da empresa, sem exigir investimentos significativos para reequipar, adquirir novas habilidades ou formar novas equipes. A NetApp está bem posicionada para ajudar os clientes a resolver esses desafios de negócios, independentemente da fase da jornada para a nuvem em que estejam.

NetApp Hybrid Multi-Cloud com Red Hat Openshift:

- Oferece aos clientes designs e práticas validados que demonstram as melhores maneiras para os clientes gerenciarem, protegerem, garantirem e migrarem seus dados e aplicativos ao usar o Red Hat OpenShift com soluções de armazenamento baseadas em NetApp .
- Apresentar as melhores práticas para clientes que executam o Red Hat OpenShift com armazenamento NetApp em ambientes VMware, infraestrutura bare metal ou uma combinação de ambos.
- Demonstre estratégias e opções para ambientes locais e na nuvem, bem como ambientes híbridos onde ambos são usados.

Soluções suportadas do NetApp Hybrid Multicloud para cargas de trabalho do Red Hat OpenShift Container

A solução testa e valida a migração e a proteção centralizada de dados com a OpenShift Container Platform (OCP), o OpenShift Advanced Cluster Manager (ACM), o NetApp ONTAP, o NetApp Console e o NetApp Trident Protect.

Para esta solução, os seguintes cenários são testados e validados pela NetApp. A solução é separada em vários cenários com base nas seguintes características:

- no local
- nuvem
  - clusters OpenShift autogerenciados e armazenamento NetApp autogerenciado
  - clusters OpenShift gerenciados pelo provedor e armazenamento NetApp gerenciado pelo provedor

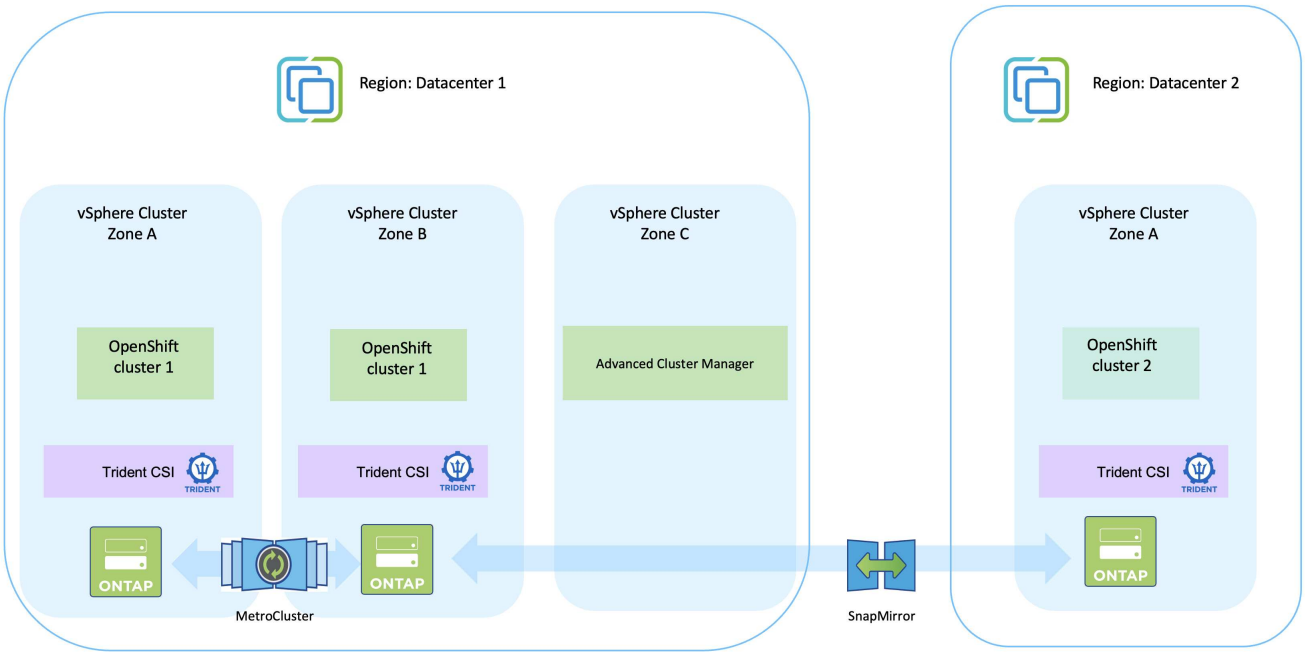
Desenvolveremos soluções e casos de uso adicionais no futuro.

Cenário 1: Proteção de dados e migração no ambiente local usando o Trident Protect

No local: clusters OpenShift autogerenciados e armazenamento NetApp autogerenciado

- Utilize Trident Protect para proteger aplicativos e dar suporte à migração entre os clusters locais.

Cenário 1

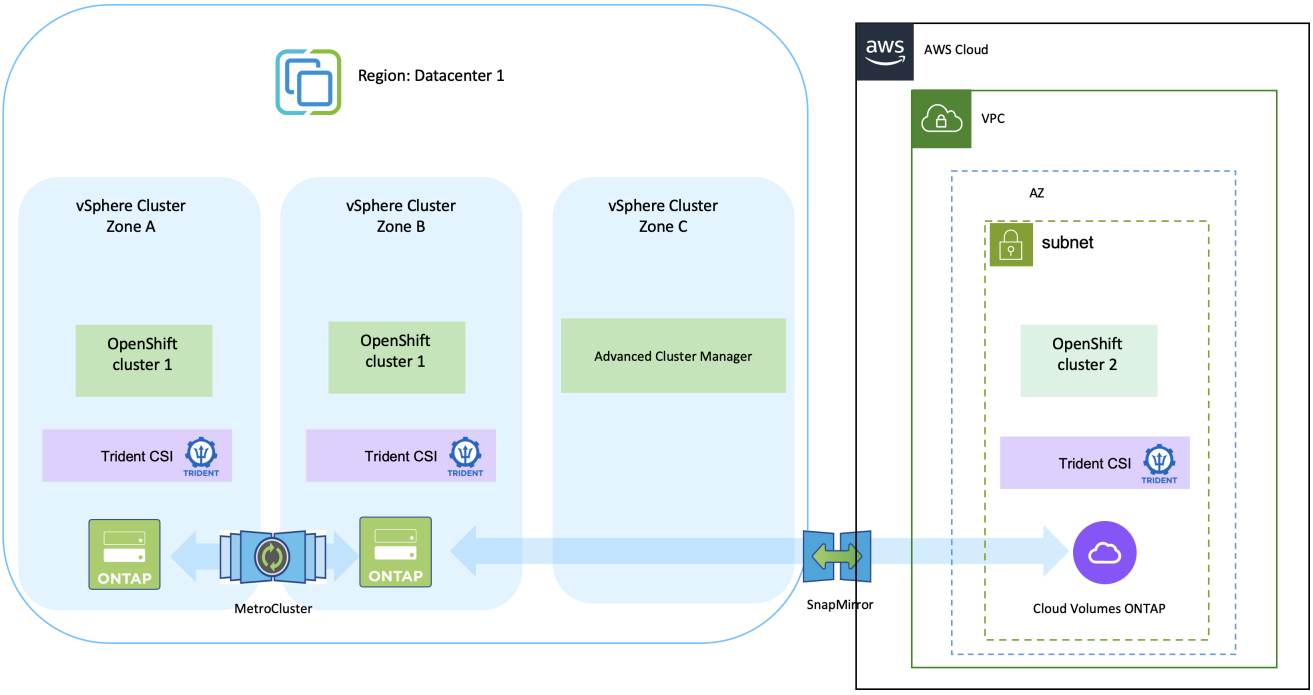


Cenário 2: Proteção de dados e migração do ambiente local para o ambiente AWS usando o Trident Protect

No local: cluster OpenShift autogerenciado e armazenamento autogerenciado Nuvem AWS: cluster OpenShift autogerenciado e armazenamento autogerenciado

- Utilize Trident Protect para proteger aplicações e dar suporte à migração entre os clusters locais e os clusters OpenShift autogerenciados na AWS.

Cenário 2

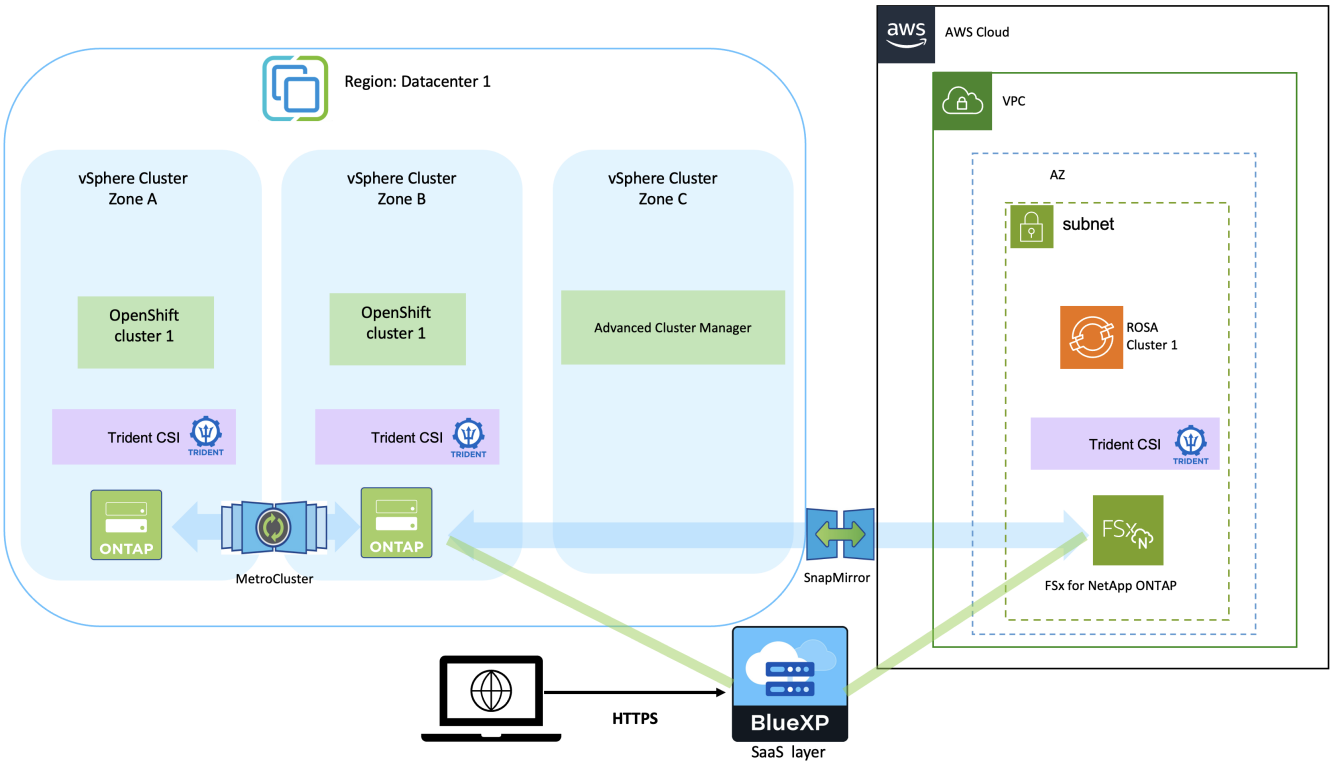


Cenário 3: Proteção de dados e migração do ambiente local para o ambiente AWS

No local: cluster OpenShift autogerenciado e armazenamento autogerenciado Nuvem AWS: cluster OpenShift gerenciado pelo provedor (ROSA) e armazenamento gerenciado pelo provedor (FSx ONTAP)

- Usando o NetApp Console, execute a replicação de volumes persistentes (FSx ONTAP).
- Usando o OpenShift GitOps, recrie metadados do aplicativo.

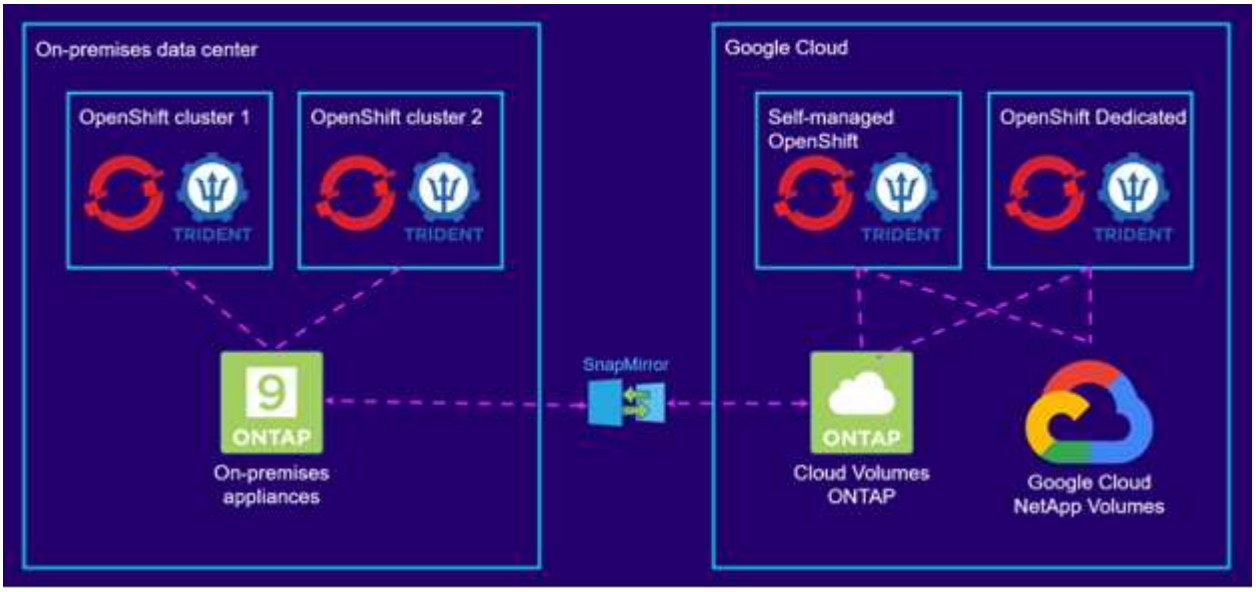
Cenário 3



Cenário 4: Proteção de dados e migração do ambiente local para o ambiente GCP usando o Trident Protect

No local: cluster OpenShift autogerenciado e armazenamento autogerenciado Google Cloud: cluster OpenShift autogerenciado e armazenamento autogerenciado

- Use Trident Protect para proteger aplicativos e dar suporte à migração entre os clusters locais e do Google Cloud OpenShift.

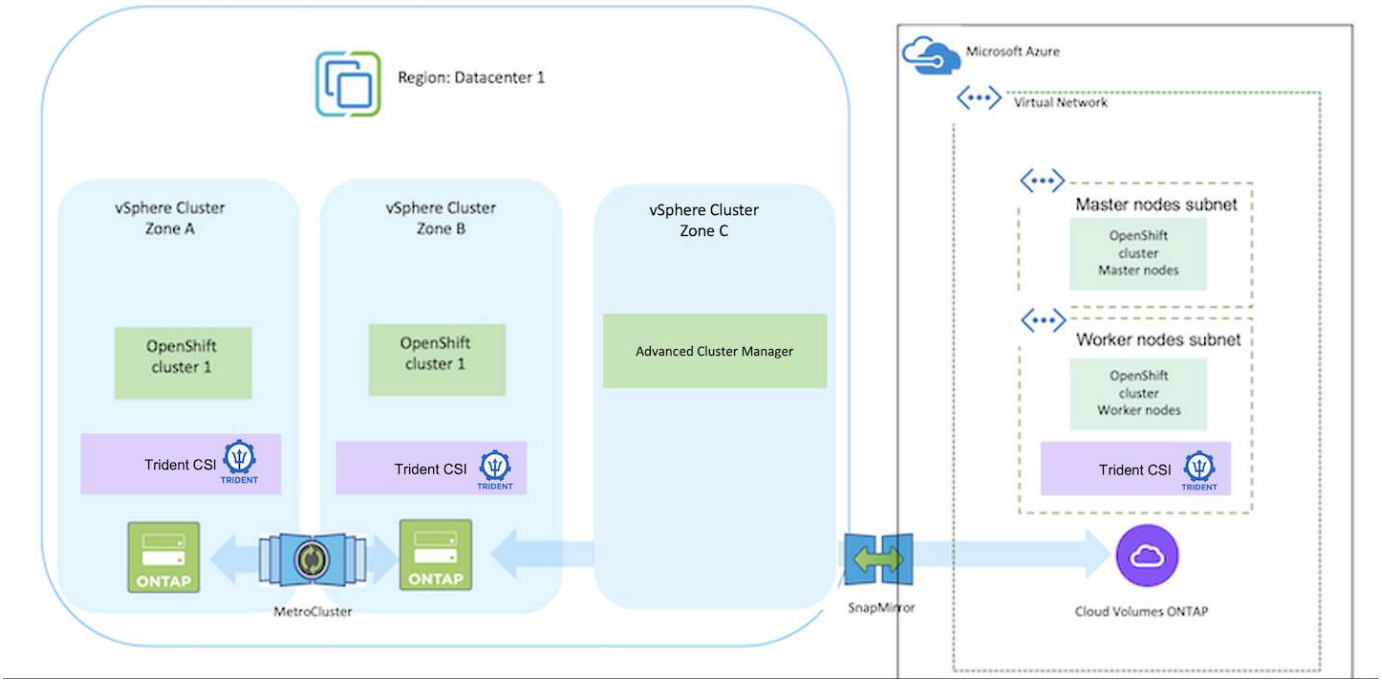


Para considerações ao usar o ONTAP em uma configuração MetroCluster , consulte"aqui" .

Cenário 5: Proteção de dados e migração do ambiente local para o ambiente do Azure usando o Trident Protect

No local: cluster OpenShift autogerenciado e armazenamento autogerenciado Azure Cloud: cluster OpenShift autogerenciado e armazenamento autogerenciado

- Use Trident Protect para proteger aplicativos e dar suporte à migração entre os ambientes locais e os clusters OpenShift no Azure.



Para considerações ao usar o ONTAP em uma configuração MetroCluster , consulte"aqui" .

Versões de vários componentes usados na validação da solução

A solução testa e valida a migração e a proteção centralizada de dados com a plataforma de contêiner OpenShift, OpenShift Advanced Cluster Manager, NetApp ONTAP e NetApp Trident Protect.

Os cenários 1, 2 e 3 da solução foram validados utilizando as versões conforme tabela abaixo:

Componente	Versão
VMware	vSphere Client versão 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Cluster Hub	OpenShift 4.11.34
Clusters de Origem e Destino	OpenShift 4.12.9 local e na AWS
* NetApp Trident*	Servidor e Cliente Trident 23.04.0
* NetApp Trident Protect*	Trident Protect 22.11.0-82
* NetApp ONTAP*	ONTAP 9.12.1
AWS FSx ONTAP	Único AZ

O cenário 4 da solução foi validado utilizando as versões conforme mostrado na tabela abaixo:

Componente	Versão
VMware	vSphere Client versão 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Cluster Hub	OpenShift 4.13.13
Clusters de Origem e Destino	OpenShift 4.13.12 local e no Google Cloud
* NetApp Trident*	Servidor e Cliente Trident 23.07.0
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Único AZ, nó único, 9.14.0

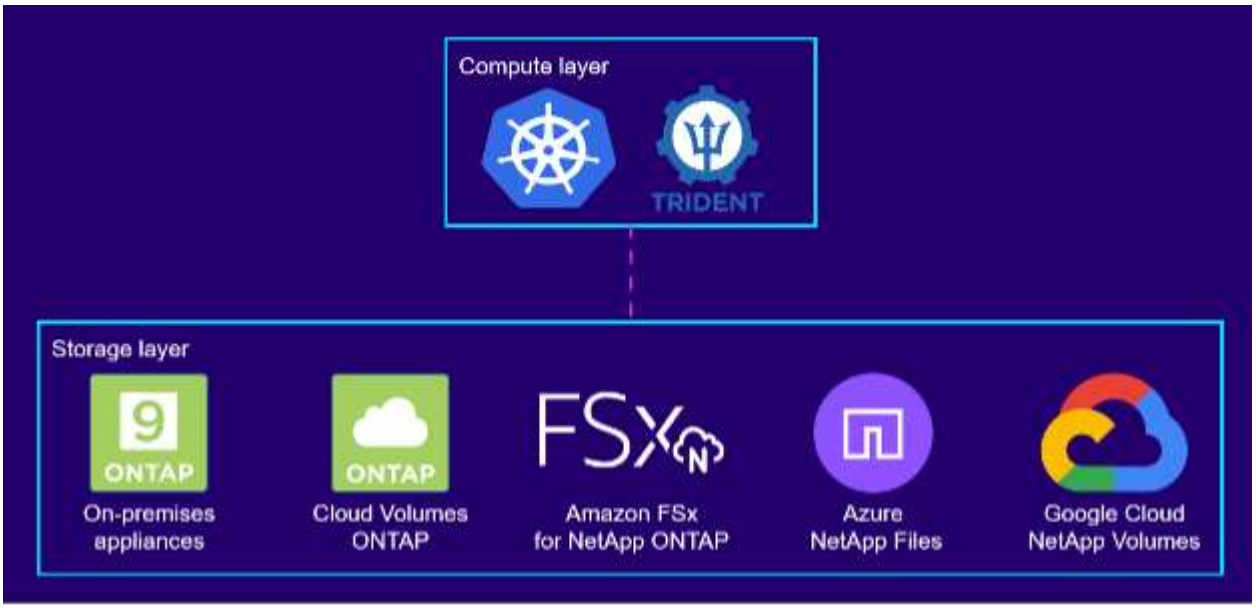
O cenário 5 da solução foi validado utilizando as versões conforme mostrado na tabela abaixo:

Componente	Versão
VMware	vSphere Client versão 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Clusters de Origem e Destino	OpenShift 4.13.25 local e no Azure
* NetApp Trident*	Trident Server e Client 23.10.0
* NetApp Trident Protect*	Trident Protect 23.10
* NetApp ONTAP*	ONTAP 9.12.1
* Cloud Volumes ONTAP*	Único AZ, nó único, 9.14.0

Integrações do NetApp Storage com Red Hat OpenShift Containers

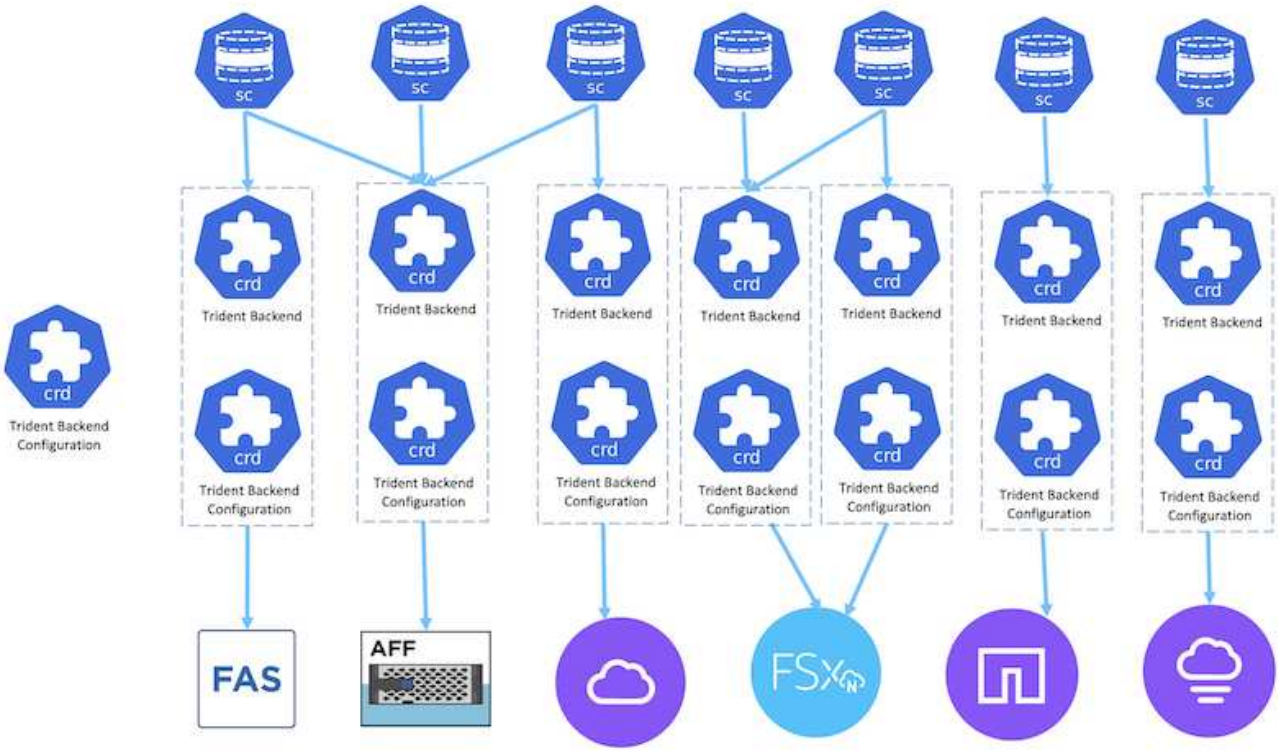
Não importa se os contêineres do Red Hat OpenShift estão em execução no VMware ou nos hiperescaladores, o NetApp Trident pode ser usado como o provisionador CSI para os vários tipos de armazenamento NetApp de backend que ele suporta.

O diagrama a seguir descreve os vários armazenamentos de backend da NetApp que podem ser integrados aos clusters OpenShift usando o NetApp Trident.



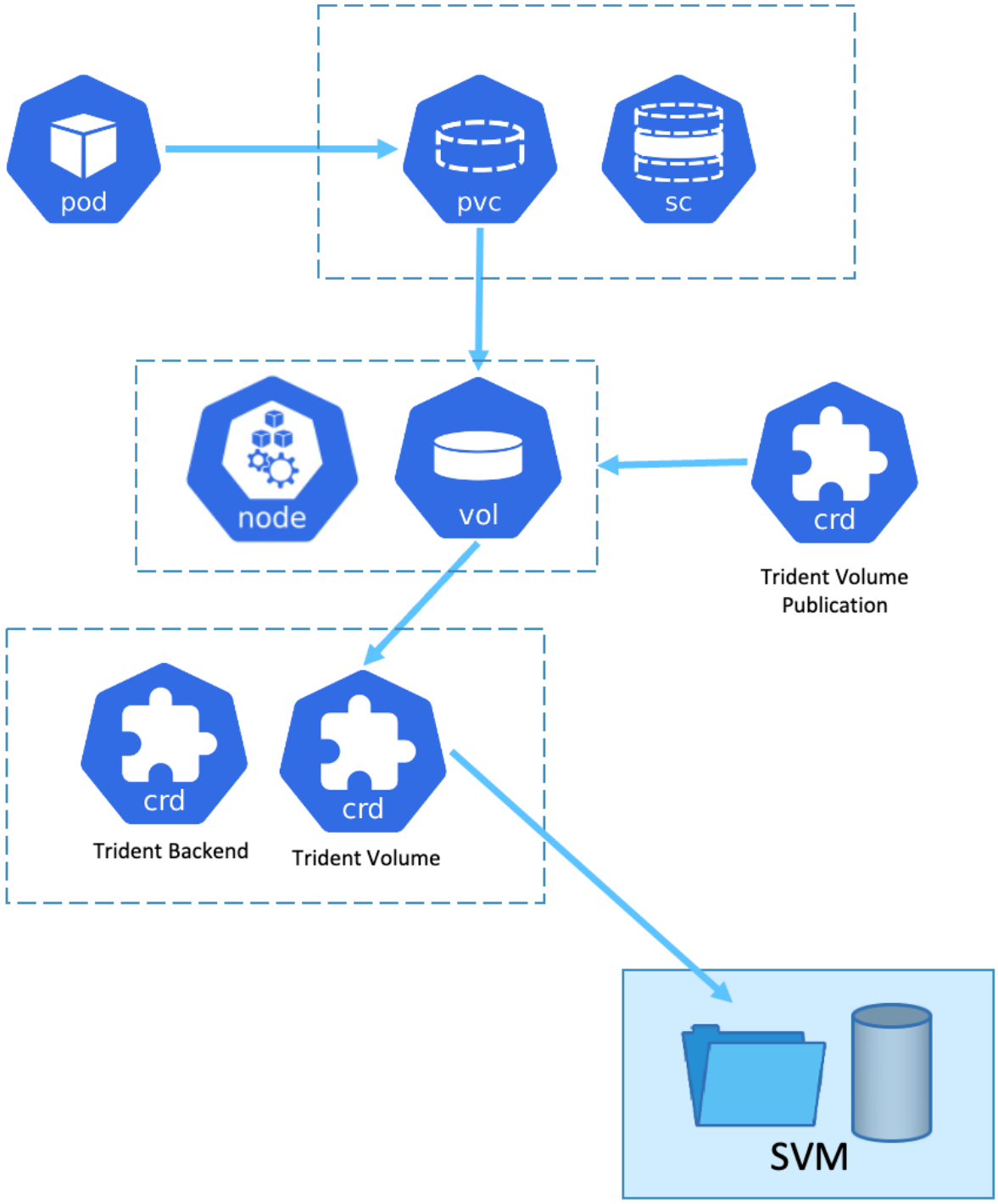
A Máquina Virtual de Armazenamento ONTAP (SVM) fornece multilocação segura. Um único cluster OpenShift pode se conectar a uma única SVM ou a várias SVMs ou até mesmo a vários clusters ONTAP . A classe de armazenamento filtra o armazenamento de backend com base em parâmetros ou rótulos. Os administradores de armazenamento definem os parâmetros para conectar ao sistema de armazenamento usando a configuração de backend do Trident. Após o estabelecimento da conexão bem-sucedido, ele cria o backend trident e preenche as informações que a classe de armazenamento pode filtrar.

O relacionamento entre a classe de armazenamento e o backend é mostrado abaixo.



O proprietário do aplicativo solicita um volume persistente usando uma classe de armazenamento. A classe de armazenamento filtra o armazenamento de backend.

A relação entre o pod e o armazenamento de backend é mostrada abaixo.



Opções de interface de armazenamento de contêiner (CSI)

Em ambientes vSphere, os clientes podem escolher o driver VMware CSI e/ou Trident CSI para integrar com o ONTAP. Com o VMware CSI, os volumes persistentes são consumidos como discos SCSI locais, enquanto com o Trident, eles são consumidos com a rede.

Como o VMware CSI não oferece suporte aos modos de acesso RWX com ONTAP, os aplicativos precisam usar o Trident CSI se o modo RWX for necessário. Com implantações baseadas em FC, o VMware CSI é o

preferido e o SnapMirror Business Continuity (SMBC) fornece alta disponibilidade em nível de zona.

Suporte VMware CSI

- Armazenamentos de dados baseados em blocos principais (FC, FCoE, iSCSI, NVMeoF)
- Armazenamentos de dados baseados em arquivos principais (NFS v3, v4)
- Armazenamentos de dados vVol (bloco e arquivo)

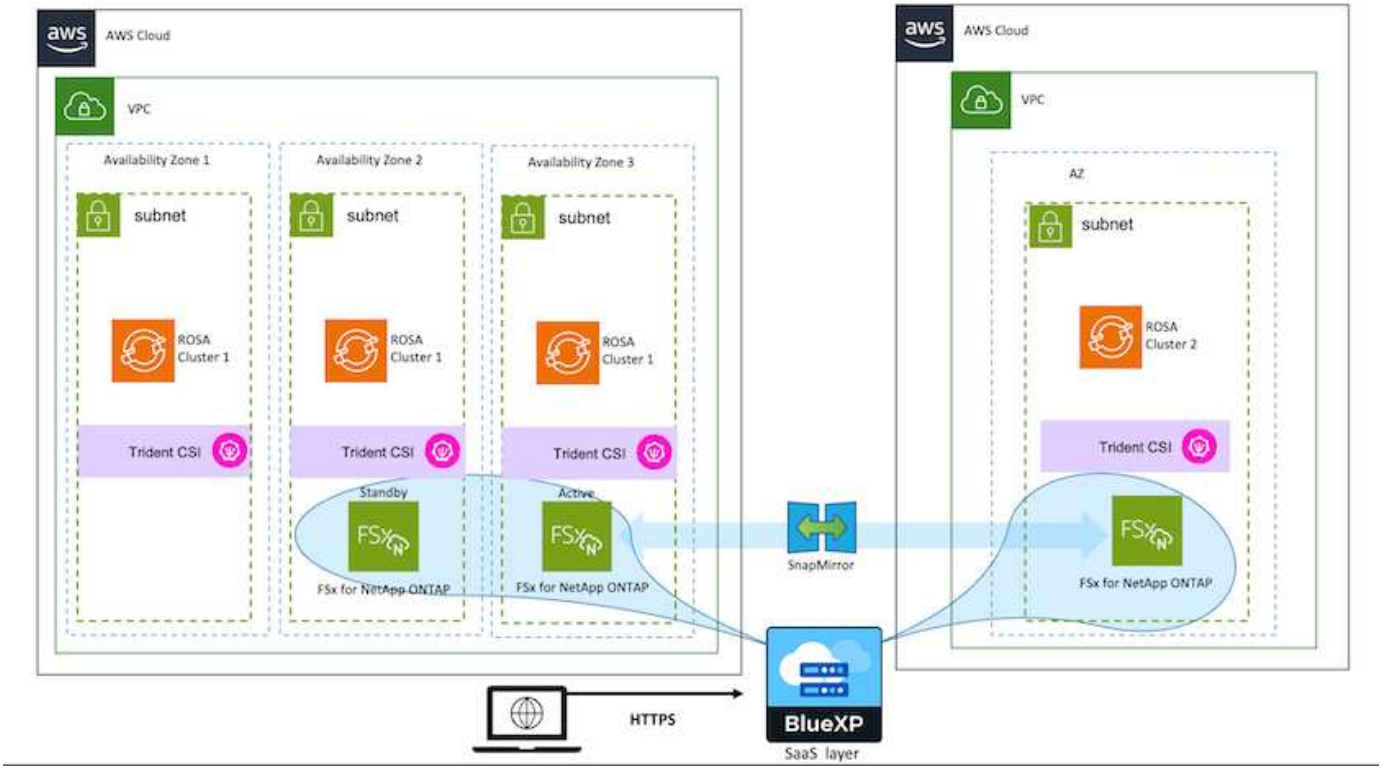
A Trident conta com os seguintes drivers para oferecer suporte ao ONTAP

- ontap-san (volume dedicado)
- ontap-san-economy (volume compartilhado)
- ontap-nas (volume dedicado)
- ontap-nas-economy (volume compartilhado)
- ontap-nas-flexgroup (volume dedicado em grande escala)

Tanto para VMware CSI quanto para Trident CSI, o ONTAP oferece suporte a nconnect, entroncamento de sessão, kerberos, etc. para NFS e multipathing, autenticação chap, etc. para protocolos de bloco.

Na AWS, o Amazon FSx for NetApp ONTAP (FSx ONTAP) pode ser implantado em uma única Zona de Disponibilidade (AZ) ou em várias AZs. Para cargas de trabalho de produção que exigem alta disponibilidade, o multi-AZ fornece tolerância a falhas em nível zonal e tem melhor cache de leitura NVMe em comparação ao AZ único. Para mais informações, consulte"Diretrizes de desempenho da AWS" .

Para economizar custos no local de recuperação de desastres, um único AZ FSx ONTAP pode ser utilizado.



Para o número de SVMs suportados pelo FSx ONTAP, consulte"gerenciando máquina virtual de armazenamento FSx ONTAP"

Documentação adicional

Aqui está alguma documentação adicional para referência:

1. "VMware vSphere"
2. "Documentação do produto da plataforma OpenShift Container"
3. "Instalando clusters de plataforma de contêiner OpenShift"
4. "Documentação avançada do produto de gerenciamento de cluster"
5. "Criando um cluster usando o ACM"
6. "Implantando o Red Hat Quay no OpenShift"
7. "Trident"
8. "ONTAP 9"
9. "NetApp Verda" - O Verda (código aberto) possui uma coleção de hooks de execução de referência para aplicações populares nativas da nuvem com uso intensivo de dados
10. "NetApp serviços de dados"
11. "Arquitetura clássica do Red Hat OpenShift Service on AWS"
12. "Amazon FSx ONTAP"
13. "Instalando clusters OpenShift no GCP"
14. "Instalando Clusters OpenShift no Azure"

Openshift para instalações locais

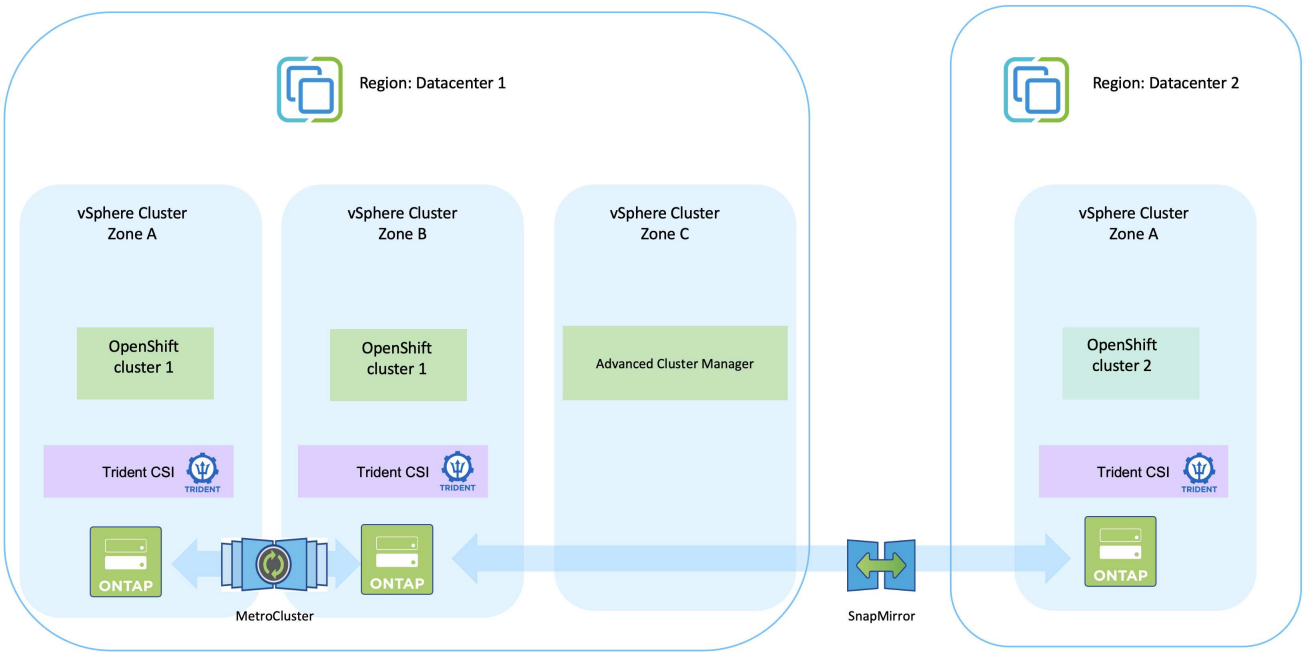
Solução NetApp com cargas de trabalho da plataforma Red Hat OpenShift Container no VMware

Se os clientes precisarem executar seus aplicativos modernos em contêineres na infraestrutura de seus data centers privados, eles poderão fazê-lo. Eles devem planejar e implantar a plataforma de contêiner Red Hat OpenShift (OCP) para um ambiente de produção bem-sucedido e pronto para implantar suas cargas de trabalho de contêiner. Seus clusters OCP podem ser implantados no VMware ou bare metal.

O armazenamento NetApp ONTAP oferece proteção de dados, confiabilidade e flexibilidade para implantações de contêineres. O Trident atua como um provedor de armazenamento dinâmico para consumir armazenamento ONTAP persistente para aplicativos com estado dos clientes. O NetApp Trident Protect pode ser usado para atender a muitos requisitos de gerenciamento de dados de aplicativos com estado, como proteção de dados, migração e continuidade de negócios.

Com o VMware vSphere, as ferramentas NetApp ONTAP fornecem um plug-in vCenter que pode ser utilizado para provisionar armazenamentos de dados. Aplique tags e use-as com o OpenShift para armazenar a configuração e os dados do nó. O armazenamento baseado em NVMe oferece menor latência e alto desempenho.

Solução de proteção e migração de dados para cargas de trabalho de contêiner OpenShift usando Trident Protect

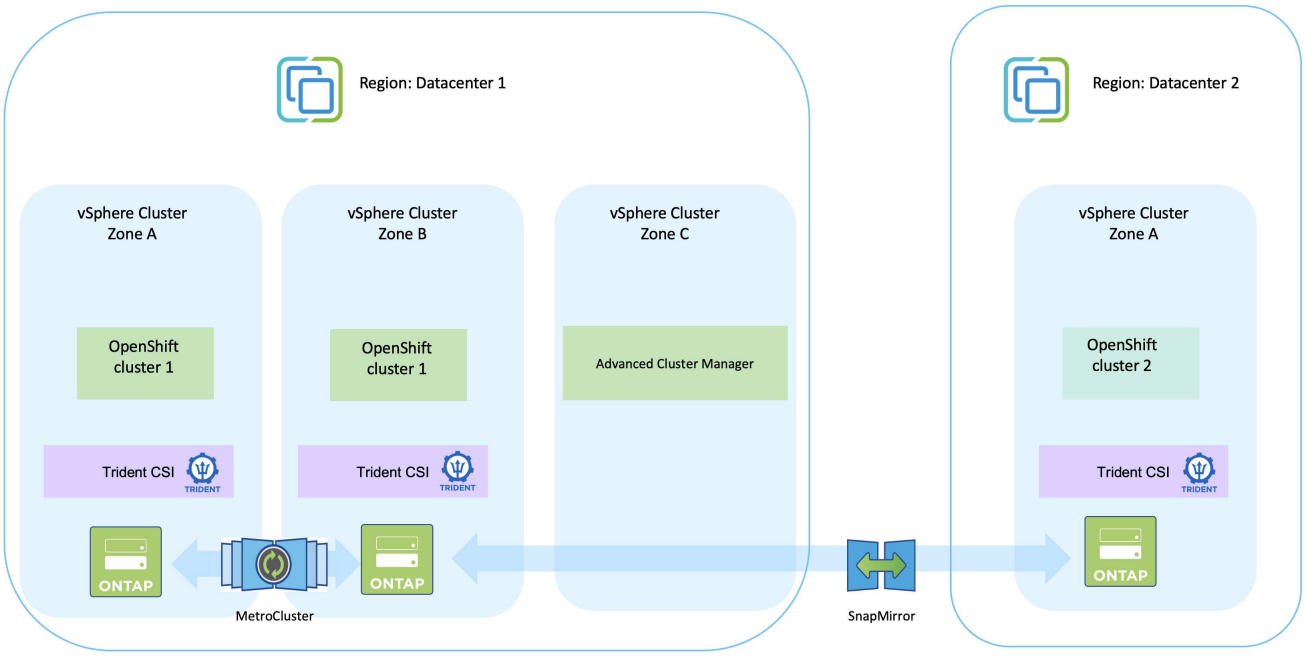


Implantar e configurar a plataforma Red Hat OpenShift Container no VMware

Esta seção descreve um fluxo de trabalho de alto nível sobre como configurar e gerenciar clusters OpenShift e gerenciar aplicativos com estado neles. Ele mostra o uso de matrizes de armazenamento NetApp ONTAP com a ajuda do Trident para fornecer volumes persistentes.

> Há várias maneiras de implantar clusters da plataforma Red Hat OpenShift Container. Esta descrição de alto nível da configuração fornece links de documentação para o método específico que foi usado. Você pode consultar os outros métodos nos links relevantes fornecidos no"seção de recursos" .

Aqui está um diagrama que descreve os clusters implantados no VMware em um data center.



O processo de configuração pode ser dividido nas seguintes etapas:

▼ **Implantar e configurar uma VM CentOS**

- Ele é implantado no ambiente VMware vSphere.
- Esta VM é usada para implantar alguns componentes, como o NetApp Trident e o NetApp Trident Protect, para a solução.
- Um usuário root é configurado nesta VM durante a instalação.

▼ **Implantar e configurar um cluster do OpenShift Container Platform no VMware vSphere (Hub Cluster)**

Consulte as instruções sobre o "Implantação assistida"método para implantar um cluster OCP.

Lembre-se do seguinte: - Crie uma chave ssh pública e privada para fornecer ao instalador. Essas chaves serão usadas para fazer login nos nós mestre e de trabalho, se necessário. - Baixe o programa instalador do instalador assistido. Este programa é usado para inicializar as VMs que você cria no ambiente VMware vSphere para os nós mestre e de trabalho. - As VMs devem ter os requisitos mínimos de CPU, memória e disco rígido. (Consulte os comandos vm create em"esse" página para os nós mestre e de trabalho que fornecem essas informações) - O diskUUID deve ser habilitado em todas as VMs. - Crie no mínimo 3 nós para o mestre e 3 nós para o trabalhador. - Assim que forem descobertos pelo instalador, ative o botão de alternância de integração do VMware vSphere.

▼ **Instalar o Advanced Cluster Management no cluster Hub**

Ele é instalado usando o Advanced Cluster Management Operator no Hub Cluster. Consulte as instruções"aqui" .

▼ **Instalar dois clusters OCP adicionais (Origem e Destino)**

- Os clusters adicionais podem ser implantados usando o ACM no Hub Cluster.
- Consulte as instruções "aqui".

▼ **Configurar o armazenamento NetApp ONTAP**

- Instale um cluster ONTAP com conectividade com as VMs OCP no ambiente VMWare.
- Crie uma SVM.
- Configure o data life do NAS para acessar o armazenamento no SVM.

▼ **Instalar o NetApp Trident nos clusters OCP**

- Instale o NetApp Trident em todos os três clusters: clusters de hub, de origem e de destino
- Consulte as instruções "aqui".
- Crie um backend de armazenamento para ontap-nas .
- Crie uma classe de armazenamento para ontap-nas.
- Consulte as instruções"aqui" .

▼ **Implantar um aplicativo no cluster de origem**

Use o OpenShift GitOps para implantar um aplicativo. (por exemplo, Postgres, Ghost)

O próximo passo é usar o Trident Protect para proteção de dados e migração de dados do cluster de origem para o de destino. Referir"aqui" para obter instruções.

Proteção de dados usando Trident Protect

Esta página mostra as opções de proteção de dados para aplicativos baseados em contêineres Red Hat OpenShift executados no VMware vSphere usando Trident Protect.

À medida que os usuários avançam em sua jornada de modernização de aplicativos com Red Hat OpenShift, uma estratégia de proteção de dados deve ser implementada para protegê-los contra exclusão acidental ou qualquer outro erro humano. Muitas vezes, uma estratégia de proteção também é exigida para fins regulatórios ou de conformidade para proteger seus dados contra um desastre.

Os requisitos de proteção de dados variam desde a reversão para uma cópia de um ponto no tempo até o failover automático para um domínio de falha diferente, sem qualquer intervenção humana. Muitos clientes escolhem o ONTAP como sua plataforma de armazenamento preferida para seus aplicativos Kubernetes por causa de seus recursos avançados, como multilocação, multiprotocolo, ofertas de alto desempenho e capacidade, replicação e armazenamento em cache para locais de vários sites, segurança e flexibilidade.

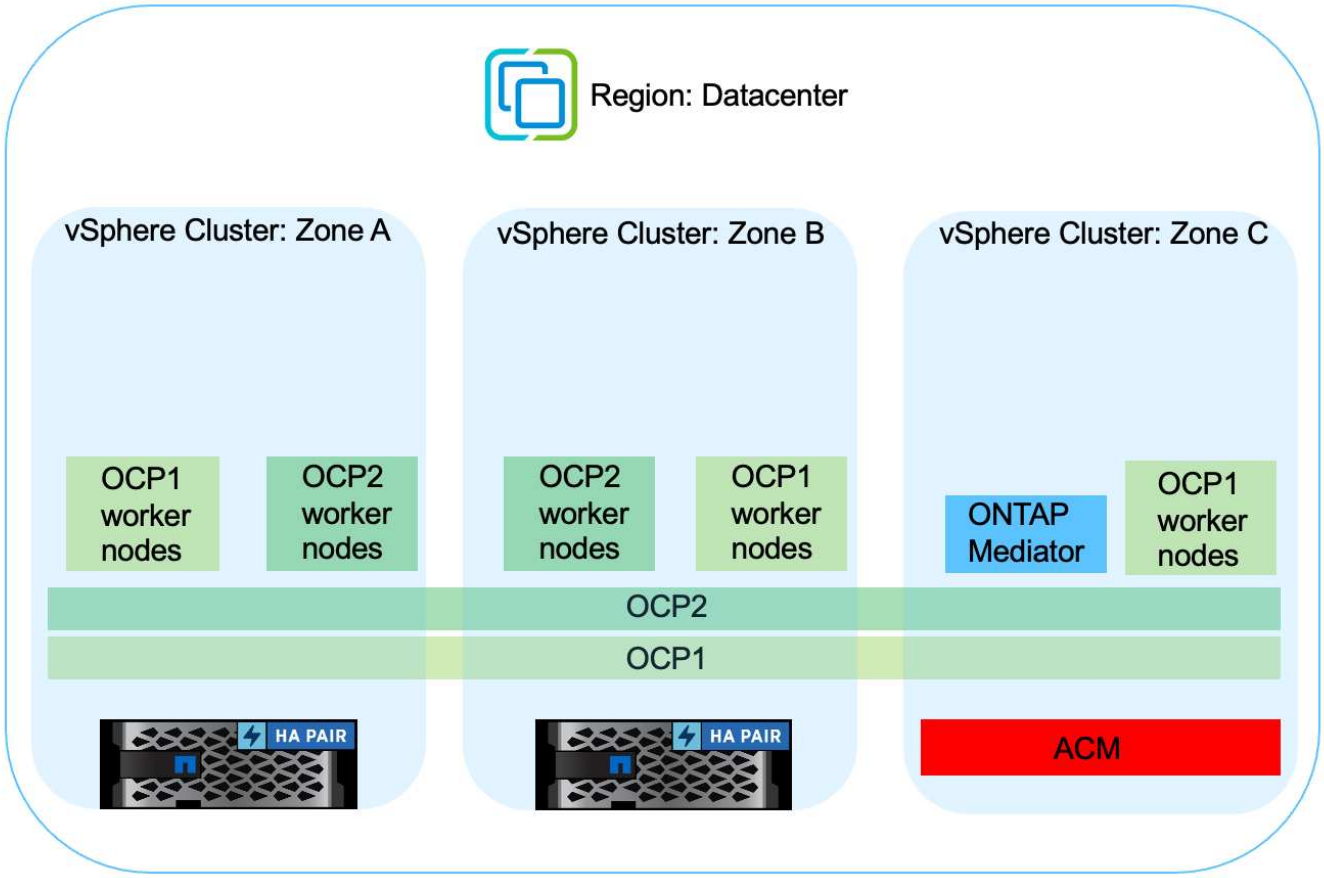
Para obter detalhes sobre como proteger e migrar cargas de trabalho de contêineres usando Trident Protect, consulte a seção a seguir: - "Proteja e migre aplicativos de contêiner usando Trident Protect"

Continuidade de negócios com MetroCluster

A maior parte da nossa plataforma de hardware para ONTAP tem recursos de alta disponibilidade para proteger contra falhas de dispositivos, evitando a necessidade de executar recuperação de desastres. Mas para proteger contra incêndios ou qualquer outro desastre e continuar o negócio com RPO zero e RTO baixo, muitas vezes é usada uma solução MetroCluster .

Os clientes que atualmente têm um sistema ONTAP podem estender para o MetroCluster adicionando sistemas ONTAP suportados dentro das limitações de distância para fornecer recuperação de desastres em nível de zona. O Trident, o CSI (Container Storage Interface), oferece suporte ao NetApp ONTAP , incluindo a configuração do MetroCluster , bem como outras opções como Cloud Volumes ONTAP, Azure NetApp Files, AWS FSx ONTAP, etc. O Trident fornece cinco opções de driver de armazenamento para ONTAP e todas são suportadas para a configuração do MetroCluster . Referir"aqui" para obter detalhes adicionais sobre drivers de armazenamento ONTAP suportados pelo Trident.

A solução MetroCluster requer extensão de rede de camada 2 ou capacidade de acessar o mesmo endereço de rede de ambos os domínios de falha. Depois que a configuração do MetroCluster estiver pronta, a solução será transparente para os proprietários dos aplicativos, pois todos os volumes no svm do MetroCluster serão protegidos e obterão os benefícios do SyncMirror (RPO zero).



Para a configuração de backend do Trident (TBC), não especifique o dataLIF e o SVM ao usar a configuração do MetroCluster . Especifique o IP de gerenciamento do SVM para managementLIF e use as credenciais da função vsadmin.

Detalhes sobre os recursos de proteção de dados do Trident Protect estão disponíveis "aqui".

Nuvem híbrida com componentes autogerenciados

Solução NetApp com cargas de trabalho da plataforma Red Hat OpenShift Container em Nuvem Híbrida

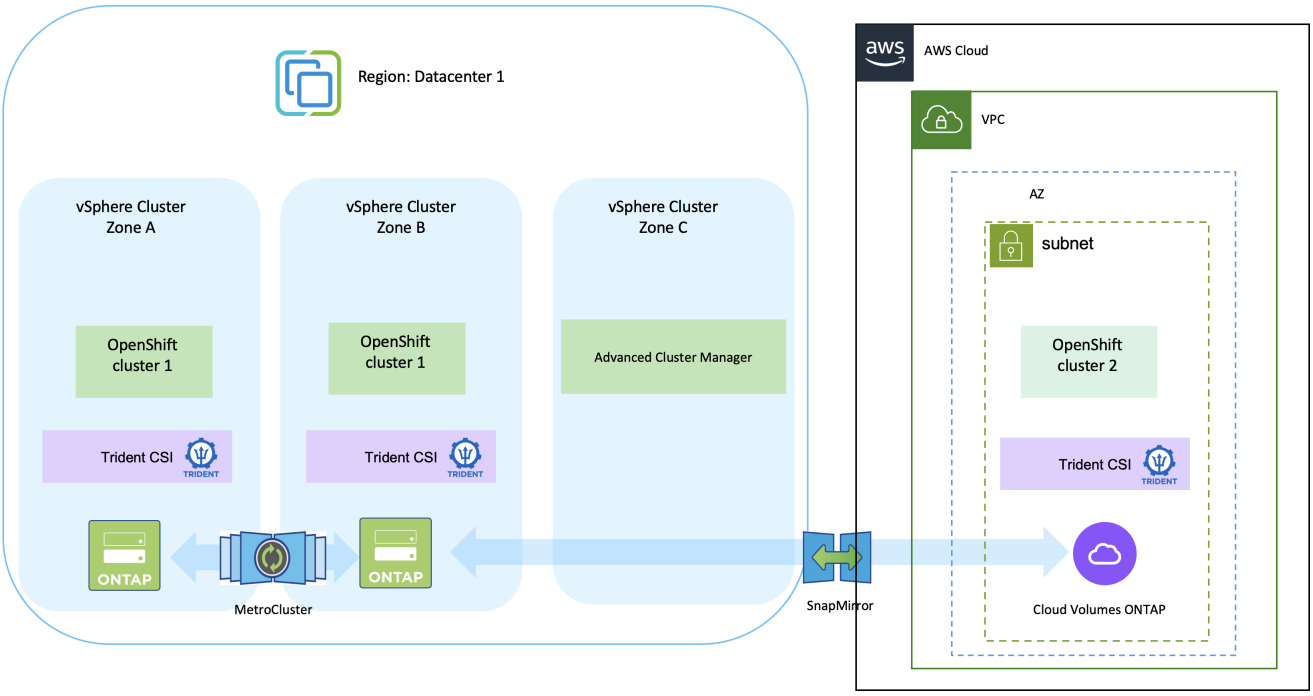
Os clientes podem estar em um ponto em sua jornada de modernização em que estão prontos para mover algumas cargas de trabalho selecionadas ou todas as cargas de trabalho de seus data centers para a nuvem. Eles podem optar por usar contêineres OpenShift autogerenciados e armazenamento NetApp autogerenciado na nuvem por vários motivos. Eles devem planejar e implantar a plataforma de contêiner Red Hat OpenShift (OCP) na nuvem para um ambiente pronto para produção bem-sucedido para migrar suas cargas de trabalho de contêiner de seus data centers. Seus clusters OCP podem ser implantados em VMware ou Bare Metal em seus data centers e em AWS,

Azure ou Google Cloud no ambiente de nuvem.

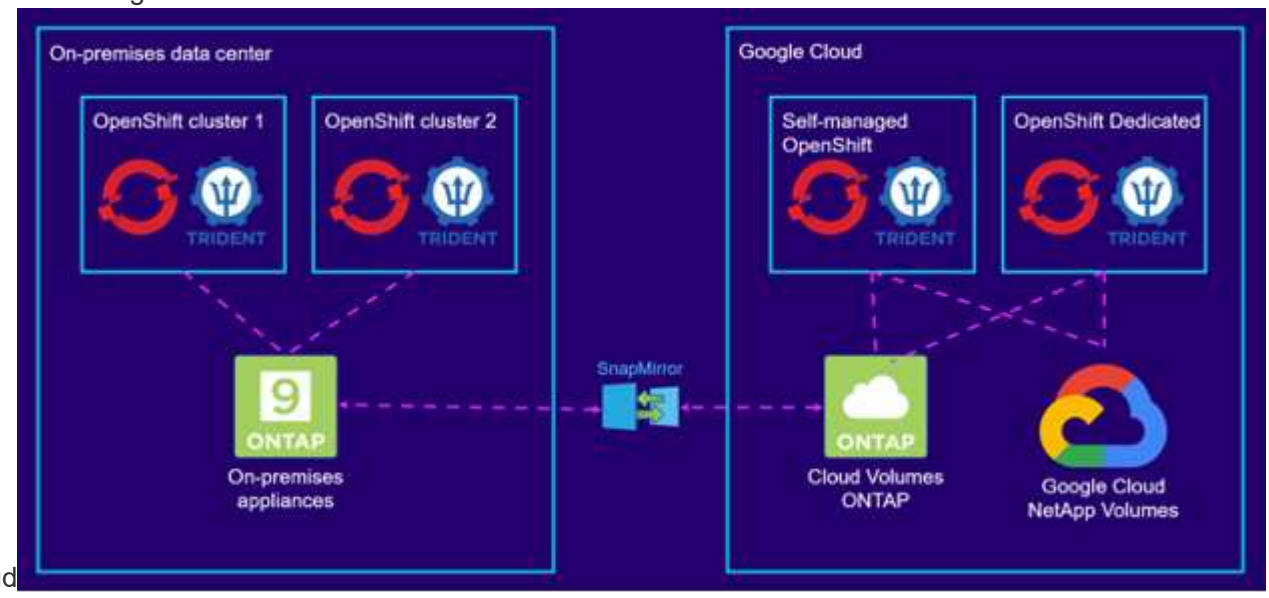
NetApp Cloud Volumes ONTAP storage oferece proteção de dados, confiabilidade e flexibilidade para implantações de contêineres na AWS, Azure e Google Cloud. Trident atua como o provisionador de armazenamento dinâmico para consumir o armazenamento persistente Cloud Volumes ONTAP para aplicações com estado dos clientes. Trident Protect pode ser usado para os requisitos de gerenciamento de dados de aplicações com estado, como proteção de dados, migração e continuidade dos negócios.

Solução de proteção e migração de dados para cargas de trabalho de contêiner OpenShift em uma nuvem híbrida usando Trident Protect

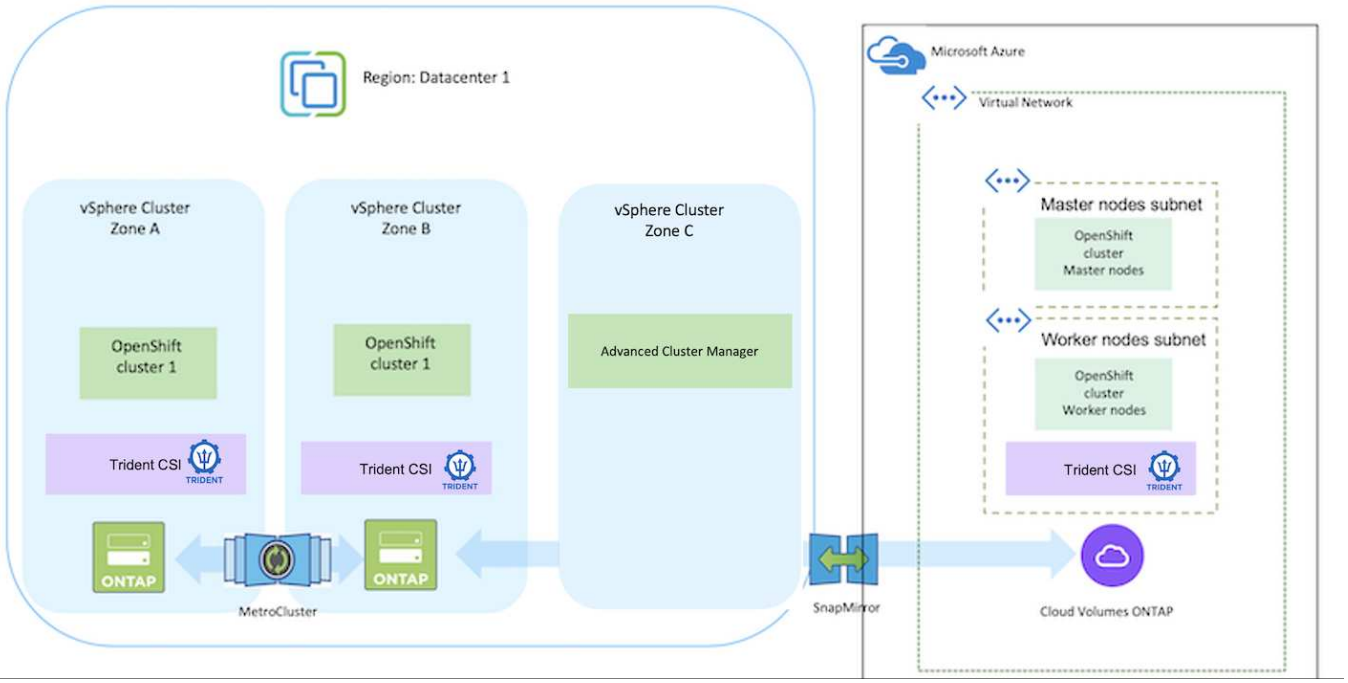
No local e
AWS



No local e Google
Cloud



No local e na nuvem do
Azure

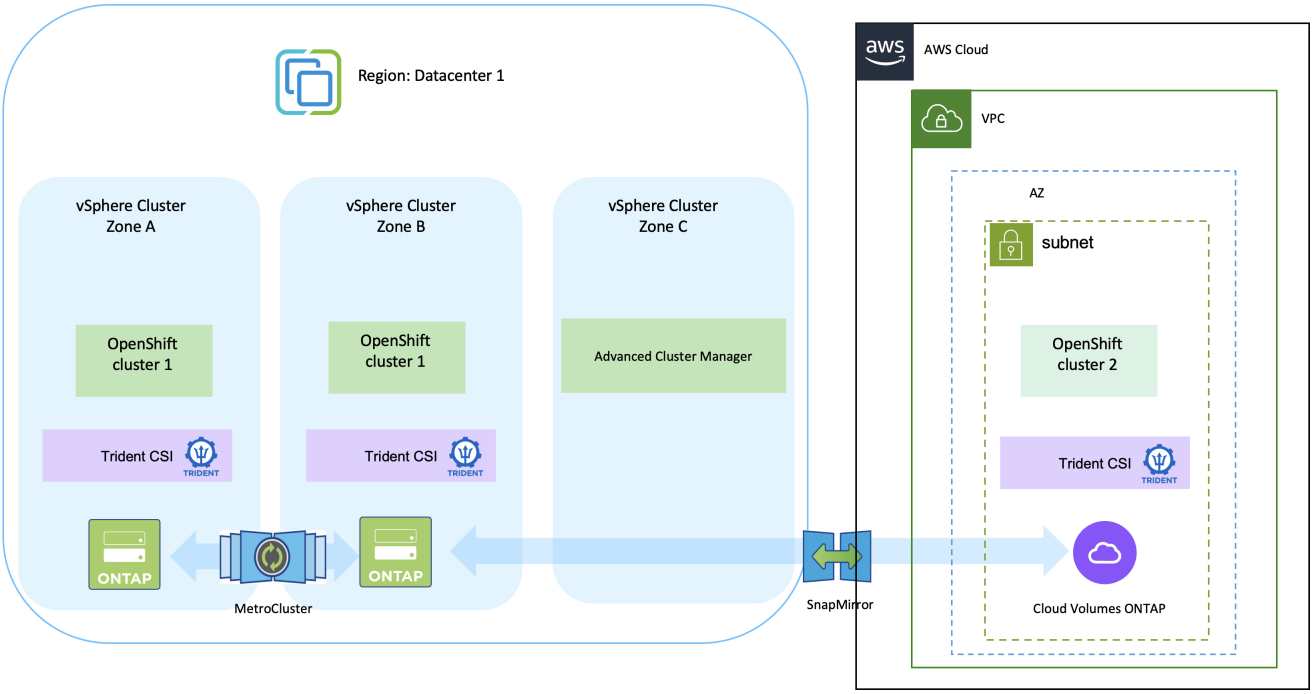


Implantar e configurar a plataforma Red Hat OpenShift Container na AWS

Esta seção descreve um fluxo de trabalho de alto nível sobre como configurar e gerenciar clusters OpenShift na AWS e implantar aplicativos com estado neles. Ele mostra o uso do armazenamento NetApp Cloud Volumes ONTAP com a ajuda do Trident para fornecer volumes persistentes. São fornecidos detalhes sobre o uso do Trident Protect para executar atividades de proteção e migração de dados para aplicativos com estado.

Há várias maneiras de implantar clusters da plataforma Red Hat OpenShift Container na AWS. Esta descrição de alto nível da configuração fornece links de documentação para o método específico que foi usado. Você pode consultar os outros métodos nos links relevantes fornecidos no"seção de recursos" .

Aqui está um diagrama que descreve os clusters implantados na AWS e conectados ao data center usando uma VPN.



O processo de configuração pode ser dividido nas seguintes etapas:

▼ **Instale um cluster OCP na AWS a partir do Advanced Cluster Management.**

- Crie uma VPC com uma conexão VPN site a site (usando o pfsense) para se conectar à rede local.
- A rede local tem conectividade com a Internet.
- Crie 3 sub-redes privadas em 3 AZs diferentes.
- Crie uma zona hospedada privada do Route 53 e um resolvedor de DNS para a VPC.

Crie um cluster OpenShift na AWS usando o assistente do Advanced Cluster Management (ACM). Consulte as instruções "aqui".

Você também pode criar o cluster na AWS a partir do console Hybrid Cloud do OpenShift. Consulte "aqui" para obter instruções.

Ao criar o cluster usando o ACM, você pode personalizar a instalação editando o arquivo yaml depois de preencher os detalhes na visualização do formulário. Após a criação do cluster, você pode fazer login via SSH nos nós do cluster para solução de problemas ou configuração manual adicional. Use a chave SSH fornecida durante a instalação e o nome de usuário core para fazer login.

▼ **Implante o Cloud Volumes ONTAP na AWS usando o NetApp Console.**

- Instale o conector no ambiente VMware local. Consulte as instruções"aqui" .
- Implante uma instância CVO na AWS usando o conector. Consulte as instruções"aqui" .

O conector também pode ser instalado no ambiente de nuvem. Referir"aqui" para obter informações adicionais.

▼ **Instalar o Trident no cluster OCP**

- Implante o Trident Operator usando o Helm. Consulte as instruções "aqui"
- Crie um backend e uma classe de armazenamento. Consulte as instruções"aqui" .

Usando o recurso de topologia CSI do Trident para arquiteturas multizona

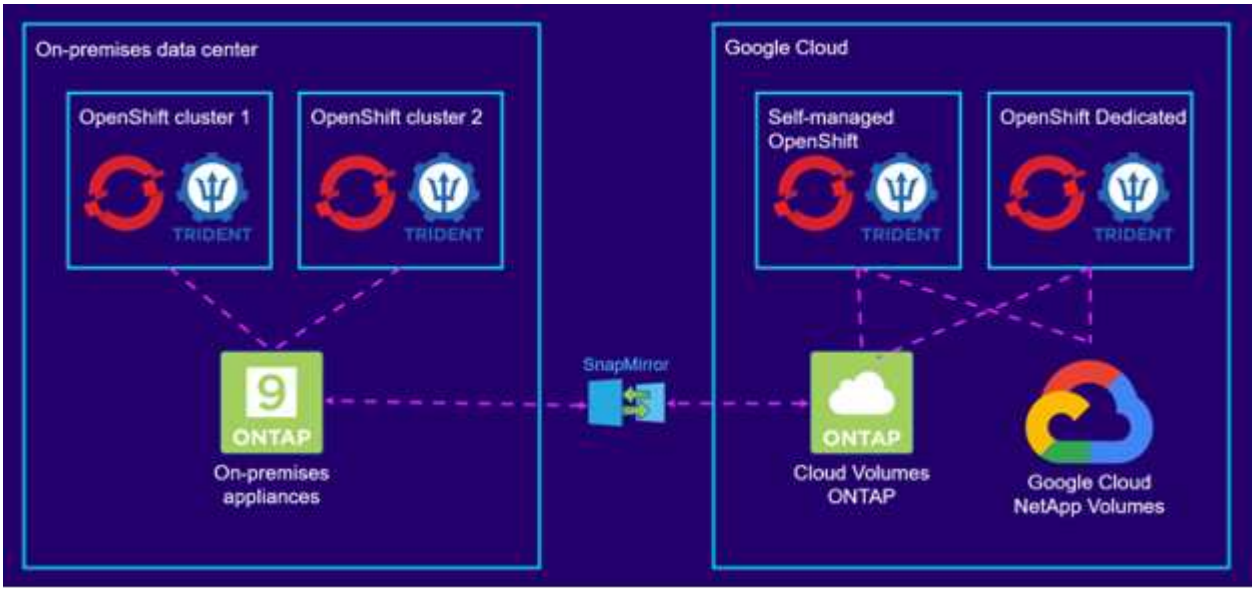
Os provedores de nuvem, hoje, permitem que os administradores de cluster do Kubernetes/OpenShift gerem nós dos clusters baseados em zonas. Os nós podem estar localizados em diferentes zonas de disponibilidade dentro de uma região ou em várias regiões. Para facilitar o provisionamento de volumes para cargas de trabalho em uma arquitetura multizona, o Trident usa a topologia CSI. Usando o recurso Topologia CSI, o acesso aos volumes pode ser limitado a um subconjunto de nós, com base em regiões e zonas de disponibilidade. Referir"aqui" para obter detalhes adicionais.

> O Kubernetes oferece suporte a dois modos de vinculação de volume: - Quando ***VolumeBindingMode* é definido como *Immediate*** (padrão), o Trident cria o volume sem qualquer reconhecimento de topologia. Volumes persistentes são criados sem qualquer dependência dos requisitos de agendamento do pod solicitante. - Quando ***VolumeBindingMode* definido como *WaitForFirstConsumer***, a criação e a vinculação de um Volume Persistente para um PVC são atrasadas até que um pod que usa o PVC seja agendado e criado. Dessa forma, os volumes são criados para atender às restrições de agendamento impostas pelos requisitos de topologia. Os backends de armazenamento Trident podem ser projetados para provisionar volumes seletivamente com base em zonas de disponibilidade (backend com reconhecimento de topologia). Para StorageClasses que fazem uso desse backend, um volume só seria criado se solicitado por um aplicativo agendado em uma região/zona suportada. (Classe de armazenamento com reconhecimento de topologia) Consulte"aqui" para obter detalhes adicionais.

Implantar e configurar o Red Hat OpenShift Container Platform no Google Cloud

Esta seção descreve um fluxo de trabalho de alto nível sobre como configurar e gerenciar clusters OpenShift no GCP e implantar aplicativos com estado neles. Ele mostra o uso do armazenamento Google Cloud NetApp Volumes e NetApp Cloud Volumes ONTAP com a ajuda do Trident para fornecer volumes persistentes.

Aqui está um diagrama que mostra os clusters implantados no GCP e conectados ao data center usando uma VPN.



Há várias maneiras de implantar clusters da plataforma Red Hat OpenShift Container no GCP. Esta descrição de alto nível da configuração fornece links de documentação para o método específico que foi usado. Você pode consultar os outros métodos nos links relevantes fornecidos no"seção de recursos" .

O processo de configuração pode ser dividido nas seguintes etapas:

Instalar um cluster OCP no GCP a partir da CLI

- Certifique-se de ter cumprido todos os pré-requisitos indicados "aqui".
- Para a conectividade VPN entre o ambiente local e o GCP, uma VM pfsense foi criada e configurada. Para obter instruções, consulte "aqui" .
  - O endereço do gateway remoto no pfsense só pode ser configurado depois de criar um gateway VPN no Google Cloud Platform.
  - Os endereços IP de rede remota para a Fase 2 podem ser configurados somente depois que o programa de instalação do cluster OpenShift for executado e criar os componentes de infraestrutura para o cluster.
  - A VPN no Google Cloud só pode ser configurada depois que os componentes de infraestrutura do cluster forem criados pelo programa de instalação.
- Agora instale o cluster OpenShift no GCP.
  - Obtenha o programa de instalação e o pull secret e implante o cluster seguindo as etapas fornecidas na documentação "aqui".
  - A instalação cria uma rede VPC no Google Cloud Platform. Ele também cria uma zona privada no Cloud DNS e adiciona registros A.
    - Use o endereço do bloco CIDR da rede VPC para configurar o pfsense e estabelecer a conexão VPN. Certifique-se de que os firewalls estejam configurados corretamente.
    - Adicione registros A no DNS do ambiente local usando o endereço IP nos registros A do DNS do Google Cloud.
  - A instalação do cluster será concluída e fornecerá um arquivo kubeconfig, nome de usuário e senha para efetuar login no console do cluster.

Implantar o Google Cloud NetApp Volumes

- Os Google Cloud NetApp Volumes podem ser adicionados aos seus projetos conforme descrito"aqui" .

Implante o Cloud Volumes ONTAP no GCP usando o NetApp Console

- Instale um agente do Console no Google Cloud. Consulte as instruções "aqui".
- Implante uma instância do CVO no Google Cloud usando o agente. Consulte as instruções "aqui".

Instalar o Trident no cluster OCP no GCP

- Existem muitos métodos para implantar o Trident, como mostrado "aqui".
- Para este projeto, o Trident foi instalado com a implantação manual do Trident Operator, seguindo as instruções "aqui".
- Crie classes de backend e armazenamento. Consulte as instruções"aqui" .

Usando o recurso de topologia CSI do Trident para arquiteturas multizona

Os provedores de nuvem, hoje, permitem que os administradores de cluster do Kubernetes/OpenShift gerem nós dos clusters baseados em zonas. Os nós podem estar localizados em diferentes zonas de disponibilidade dentro de uma região ou em várias regiões. Para facilitar o provisionamento de volumes para cargas de trabalho em uma arquitetura multizona, o Trident usa a topologia CSI. Usando o recurso Topologia CSI, o acesso aos volumes pode ser limitado a um subconjunto de nós, com base em regiões e zonas de disponibilidade. Referir"aqui" para obter detalhes adicionais.

> O Kubernetes oferece suporte a dois modos de vinculação de volume: - Quando ***VolumeBindingMode* é definido como *Immediate*** (padrão), o Trident cria o volume sem qualquer reconhecimento de topologia. Volumes persistentes são criados sem qualquer dependência dos requisitos de agendamento do pod solicitante. - Quando ***VolumeBindingMode* definido como *WaitForFirstConsumer***, a criação e a vinculação de um Volume Persistente para um PVC são atrasadas até que um pod que usa o PVC seja agendado e criado. Dessa forma, os volumes são criados para atender às restrições de agendamento impostas pelos requisitos de topologia. Os backends de armazenamento Trident podem ser projetados para provisionar volumes seletivamente com base em zonas de disponibilidade (backend com reconhecimento de topologia). Para StorageClasses que fazem uso desse backend, um volume só seria criado se solicitado por um aplicativo agendado em uma região/zona suportada. (Classe de armazenamento com reconhecimento de topologia) Consulte"aqui" para obter detalhes adicionais.

Vídeo de demonstração

Instalação do OpenShift Cluster no Google Cloud Platform

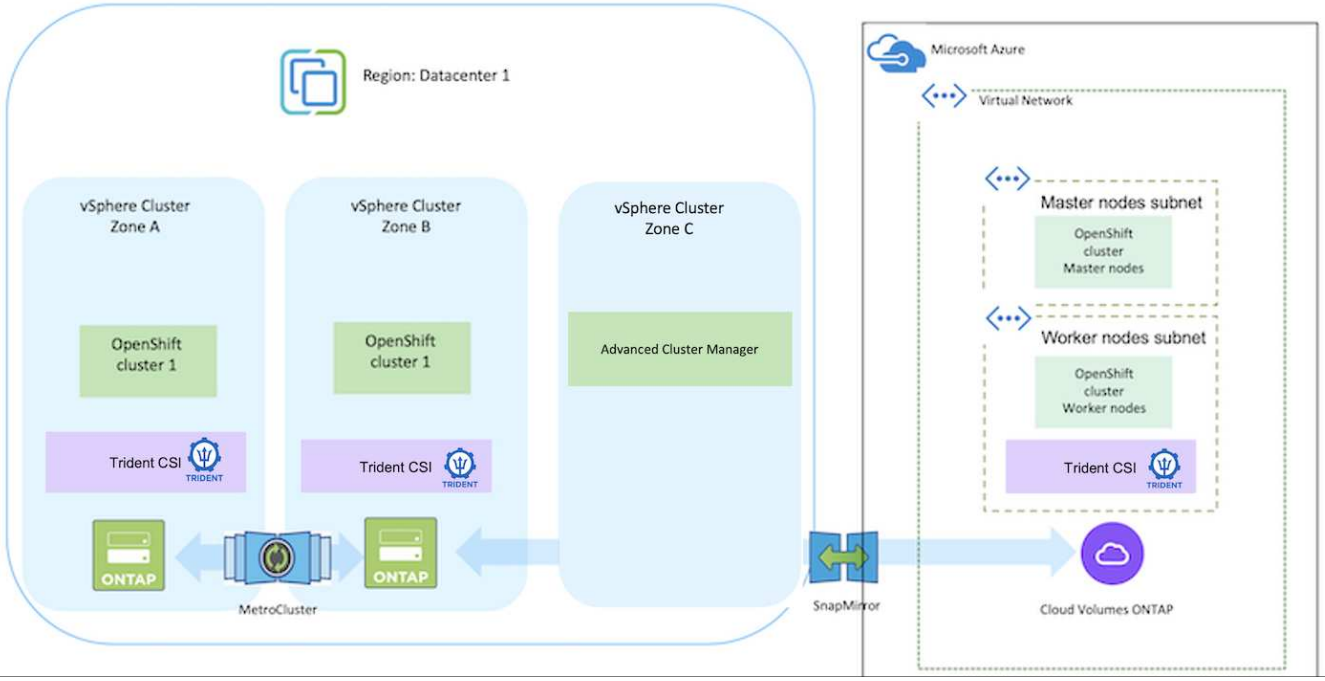
Importando clusters OpenShift para o Trident Protect

Implantar e configurar a plataforma Red Hat OpenShift Container no Azure

Esta seção descreve um fluxo de trabalho de alto nível sobre como configurar e gerenciar clusters OpenShift no Azure e implantar aplicativos com estado neles. Ele mostra o uso do armazenamento NetApp Cloud Volumes ONTAP com a ajuda do Trident para fornecer volumes persistentes. São fornecidos detalhes sobre o uso do Trident Protect para executar atividades de proteção e migração de dados para aplicativos com estado.

Aqui está um diagrama que mostra os clusters implantados no Azure e conectados ao data center usando

uma VPN.



Há várias maneiras de implantar clusters da plataforma Red Hat OpenShift Container no Azure. Esta descrição de alto nível da configuração fornece links de documentação para o método específico que foi usado. Você pode consultar os outros métodos nos links relevantes fornecidos no"seção de recursos" .

O processo de configuração pode ser dividido nas seguintes etapas:

▼ **Instale um cluster OCP no Azure a partir da CLI.**

- Certifique-se de ter cumprido todos os pré-requisitos indicados "aqui".
- Crie uma VPN, sub-redes e grupos de segurança de rede e uma zona DNS privada. Crie um gateway VPN e uma conexão VPN site a site.
- Para a conectividade VPN entre o ambiente local e o Azure, uma VM pfsense foi criada e configurada. Para obter instruções, consulte"aqui" .
- Obtenha o programa de instalação e o segredo de pull e implante o cluster seguindo os passos fornecidos na documentação "aqui".
- A instalação do cluster será concluída e fornecerá um arquivo kubeconfig, nome de usuário e senha para efetuar login no console do cluster.

Um exemplo de arquivo install-config.yaml é fornecido abaixo.

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
```

```
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
```

```
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

▼ **Implante o Cloud Volumes ONTAP no Azure usando o NetApp Console.**

- Instale um agente do NetApp Console no Azure. Consulte as instruções "aqui".
- Implante uma instância do CVO no Azure usando o agente. Consulte as instruções "aqui".

Usando o recurso de topologia CSI do Trident para arquiteturas multizona

Os provedores de nuvem, hoje, permitem que os administradores de cluster do Kubernetes/OpenShift gerem nós dos clusters baseados em zonas. Os nós podem estar localizados em diferentes zonas de disponibilidade dentro de uma região ou em várias regiões. Para facilitar o provisionamento de volumes para cargas de trabalho em uma arquitetura multizona, o Trident usa a topologia CSI. Usando o recurso Topologia CSI, o acesso aos volumes pode ser limitado a um subconjunto de nós, com base em regiões e zonas de disponibilidade. Referir"aqui" para obter detalhes adicionais.

> O Kubernetes oferece suporte a dois modos de vinculação de volume: - Quando ***VolumeBindingMode* é definido como *Immediate*** (padrão), o Trident cria o volume sem qualquer reconhecimento de topologia. Volumes persistentes são criados sem qualquer dependência dos requisitos de agendamento do pod solicitante. - Quando ***VolumeBindingMode* definido como *WaitForFirstConsumer***, a criação e a vinculação de um Volume Persistente para um PVC são atrasadas até que um pod que usa o PVC seja agendado e criado. Dessa forma, os volumes são criados para atender às restrições de agendamento impostas pelos requisitos de topologia. Os backends de armazenamento Trident podem ser projetados para provisionar volumes seletivamente com base em zonas de disponibilidade (backend com reconhecimento de topologia). Para StorageClasses que fazem uso desse backend, um volume só seria criado se solicitado por um aplicativo agendado em uma região/zona suportada. (Classe de armazenamento com reconhecimento de topologia) Consulte"aqui" para obter detalhes adicionais.

Proteção de dados usando Trident Protect

Para obter detalhes sobre como proteger e migrar cargas de trabalho de contêineres usando Trident Protect, consulte a seção a seguir: - "Proteja e migre aplicativos de contêiner usando Trident Protect"

Nuvem híbrida com componentes gerenciados pelo provedor

Solução NetApp com cargas de trabalho da plataforma Managed Red Hat OpenShift Container

Os clientes podem ter "nascido na nuvem" ou podem estar em um ponto em sua jornada de modernização em que estão prontos para mover algumas cargas de trabalho selecionadas ou todas as cargas de trabalho de seus data centers para a nuvem. Eles podem optar por usar contêineres OpenShift gerenciados pelo provedor e armazenamento NetApp gerenciado pelo provedor na nuvem para executar suas cargas de trabalho. Eles devem planejar e implantar os clusters de contêineres do Managed Red Hat OpenShift na nuvem para um ambiente pronto para produção para suas cargas de trabalho de contêiner. A NetApp fornece ofertas de armazenamento totalmente gerenciadas para soluções Managed Red Hat em todas as três principais nuvens públicas.

- Amazon FSx for NetApp ONTAP (FSx ONTAP)*

O FSx ONTAP oferece proteção de dados, confiabilidade e flexibilidade para implantações de contêineres na AWS. O Trident atua como um provisionador de armazenamento dinâmico para consumir o armazenamento persistente FSx ONTAP para aplicativos com estado dos clientes.

Como o ROSA pode ser implantado no modo HA com nós do plano de controle distribuídos em várias zonas de disponibilidade, o FSx ONTAP também pode ser provisionado com a opção Multi-AZ, que fornece alta disponibilidade e proteção contra falhas de AZ.

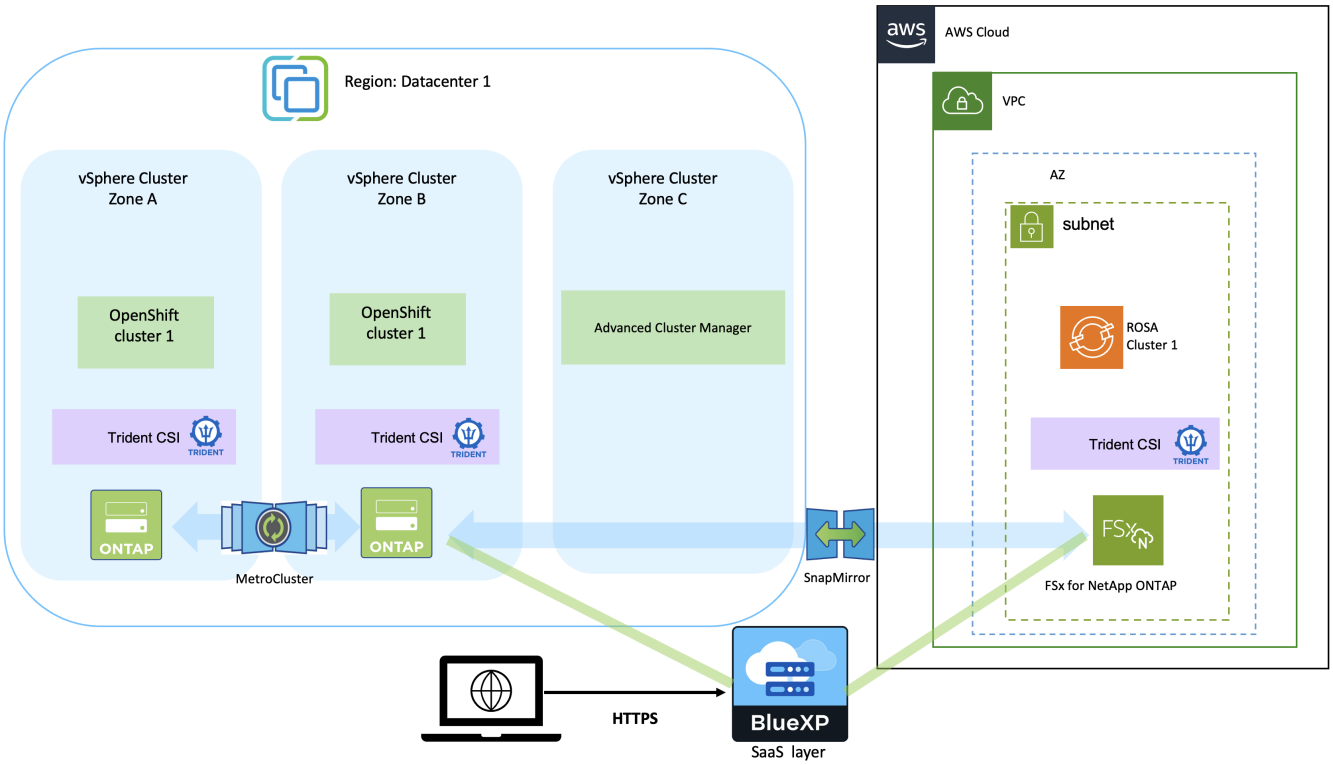
- Google Cloud NetApp Volumes*

O Red Hat OpenShift Dedicated é uma plataforma de aplicativos totalmente gerenciada que permite que você crie, implante e dimensione aplicativos rapidamente na nuvem híbrida. O Google Cloud NetApp Volumes fornece volumes persistentes, trazendo o conjunto completo de recursos de gerenciamento de dados empresariais do ONTAP para implantações do OpenShift no Google Cloud.

Implantar e configurar a plataforma Managed Red Hat OpenShift Container na AWS

Esta seção descreve um fluxo de trabalho de alto nível para configurar os clusters Managed Red Hat OpenShift na AWS (ROSA). Ela mostra o uso do Amazon FSx for NetApp ONTAP (FSx ONTAP) gerenciado como backend de storage pelo Trident para fornecer volumes persistentes. São fornecidos detalhes sobre a implantação do FSx ONTAP na AWS usando o NetApp Console. Além disso, são fornecidos detalhes sobre o uso do NetApp Console e do OpenShift GitOps (Argo CD) para executar atividades de proteção e migração de dados para as aplicações com estado nos clusters ROSA.

Aqui está um diagrama que descreve os clusters ROSA implantados na AWS e usando o FSx ONTAP como armazenamento de backend.



Esta solução foi verificada usando dois clusters ROSA em duas VPCs na AWS. Cada cluster ROSA foi integrado ao FSx ONTAP usando Trident. Existem várias maneiras de implantar clusters ROSA e FSx ONTAP na AWS. Esta descrição de alto nível da configuração fornece links de documentação para o método específico que foi usado. Você pode consultar os outros métodos nos links relevantes fornecidos no"seção de recursos" .

O processo de configuração pode ser dividido nas seguintes etapas:

Instalar clusters ROSA

- Crie duas VPCs e configure a conectividade de peering de VPC entre elas.
- Consulte "aqui" para obter instruções sobre como instalar clusters ROSA.

Instalar FSx ONTAP

- Instale o FSx ONTAP nas VPCs a partir do NetApp Console. Consulte "aqui" para criar uma conta no NetApp Console e começar a usar. Consulte "aqui" para instalar o FSx ONTAP. Consulte "aqui" para criar um conector na AWS para gerenciar o FSx ONTAP.
- Implante o FSx ONTAP usando a AWS. Referir"aqui" para implantação usando o console da AWS.

Instalar o Trident em clusters ROSA (usando o gráfico Helm)

- Use o gráfico Helm para instalar o Trident em clusters ROSA. Consulte o link da documentação: aqui.

Integração do FSx ONTAP com Trident para clusters ROSA

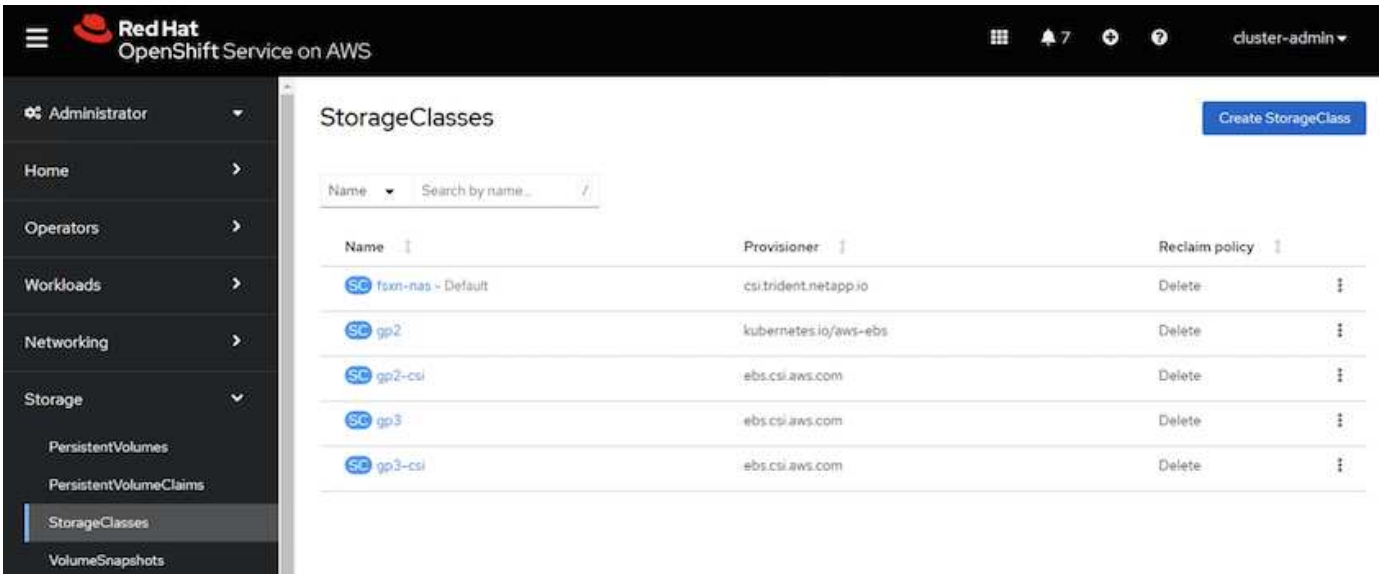
O OpenShift GitOps pode ser utilizado para implantar o Trident CSI em todos os clusters gerenciados à medida que eles são registrados no ArgoCD usando o ApplicationSet.

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```



Crie classes de backend e armazenamento usando Trident (para FSx ONTAP)

- Referir"aqui" para obter detalhes sobre a criação de classes de backend e armazenamento.
- Defina a classe de armazenamento criada para FsxN com Trident CSI como padrão no OpenShift Console. Veja a captura de tela abaixo:



Implantar um aplicativo usando OpenShift GitOps (Argo CD)

- Instale o operador OpenShift GitOps no cluster. Consulte as instruções "aqui".
- SetUp uma nova instância do Argo CD para o cluster. Consulte as instruções "aqui".

Abra o console do Argo CD e implante um aplicativo. Como exemplo, você pode implantar um aplicativo Jenkins usando o Argo CD com um Helm Chart. Ao criar o aplicativo, os seguintes detalhes foram fornecidos:

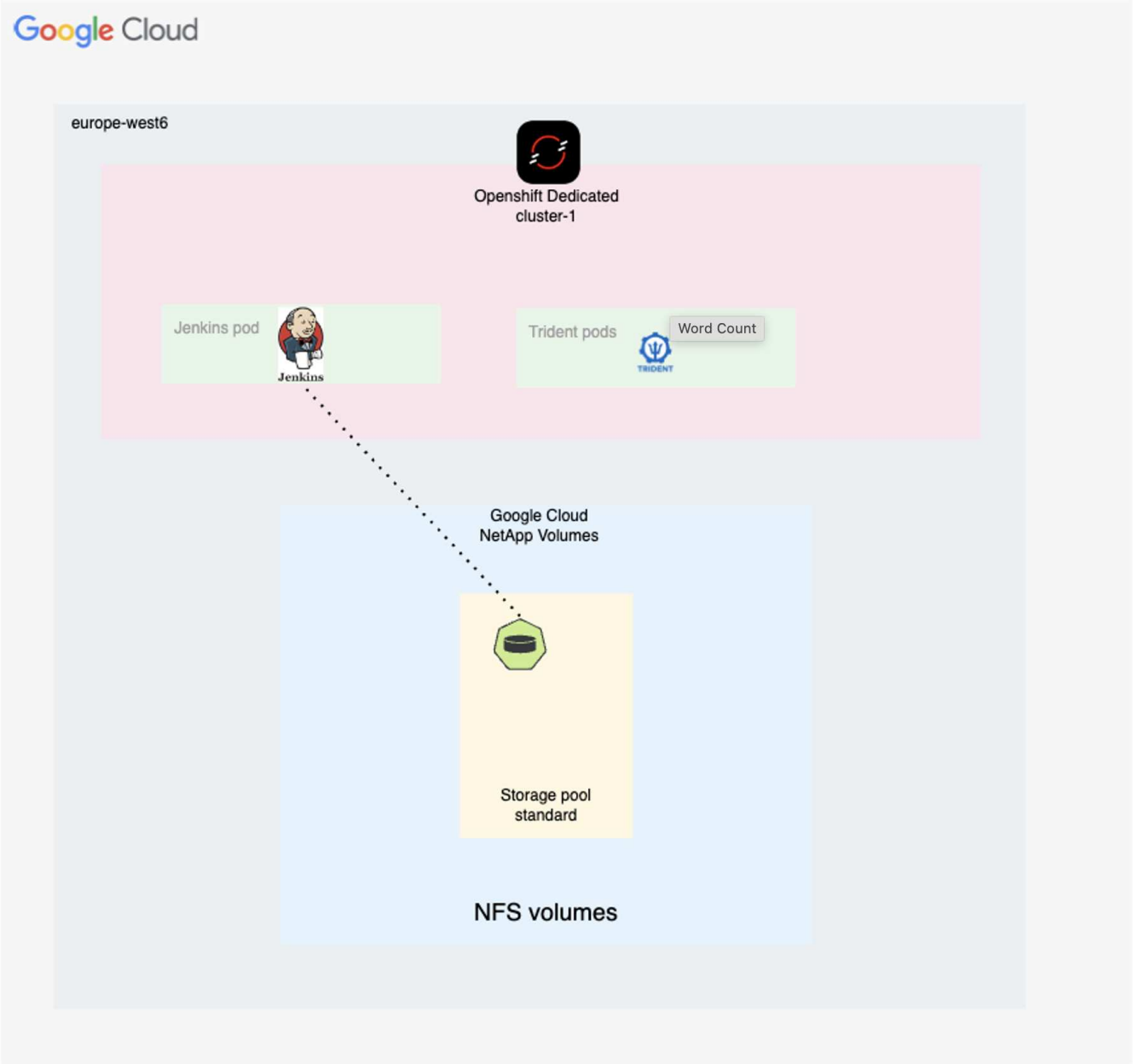
Projeto: default cluster: 'https://kubernetes.default.svc'[] (sem as aspas) Namespace: Jenkins A url do Helm Chart: 'https://charts.bitnami.com/bitnami'[] (sem as aspas)

Parâmetros do Helm: global.storageClass: fsxn-nas

Implantar e configurar o OpenShift Dedicated no Google Cloud com o Google Cloud NetApp Volumes

Esta seção descreve um fluxo de trabalho de alto nível de configuração de clusters OpenShift Dedicated (OSD) na plataforma Google Cloud. Ele mostra o NetApp Trident usando o Google Cloud NetApp Volumes como backend de armazenamento para fornecer volumes persistentes para aplicativos com estado em execução com o Kubernetes.

Aqui está um diagrama que descreve um cluster OSD implantado no Google Cloud e usando o NetApp Volumes como armazenamento de back-end.



O processo de configuração pode ser dividido nas seguintes etapas:

Instalar clusters OSD no Google Cloud

- Se desejar usar uma VPC existente para o cluster, você deverá criar a VPC, duas sub-redes, um roteador de nuvem e dois NATs de nuvem do GCP para o cluster OSD. Referir"aqui" para obter instruções.
- Consulte "aqui" para obter instruções sobre como instalar clusters do OSD no GCP usando o modelo de faturamento Customer Cloud Subscription (CCS). O OSD também está incluído no Google Cloud Marketplace. Um vídeo que mostra como instalar o OSD usando a solução do Google Cloud Marketplace está disponível "aqui".

Habilitar Google Cloud NetApp Volumes

- Referir"aqui" para obter informações sobre como configurar o acesso ao Google Cloud NetApp Volumes. Siga todos os passos até e incluindo
- Crie um pool de armazenamento. Referir"aqui" para obter informações sobre como configurar um pool de armazenamento no Google Cloud NetApp Volumes. Os volumes para os aplicativos Kubernetes com

estado em execução no OSD serão criados dentro do pool de armazenamento.

Instalar o Trident em clusters OSD (usando o gráfico Helm)

- Use um gráfico Helm para instalar Trident em clusters OSD. Consulte "aqui" para obter instruções sobre como instalar o gráfico Helm.

Integração do NetApp Volumes com o NetApp Trident para clusters OSD

Crie classes de backend e armazenamento usando o Trident (para Google Cloud NetApp Volumes)

- Consulte aqui para obter detalhes sobre a criação do backend.
- Se alguma das classes de armazenamento atuais no Kubernetes estiver marcada como padrão, remova essa anotação editando a classe de armazenamento.
- Crie pelo menos uma classe de armazenamento para volumes NetApp com o provisionador Trident CSI. Defina exatamente uma das classes de armazenamento como padrão usando uma anotação. Isso permitirá que um PVC use essa classe de armazenamento quando ela não for explicitamente chamada no manifesto do PVC. Um exemplo com a anotação é mostrado abaixo.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: gcnv-standard-k8s
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.trident.netapp.io
parameters:
  backendType: "google-cloud-netapp-volumes"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: true
```

Implantar um aplicativo usando OpenShift GitOps (Argo CD)

- Instale o operador OpenShift GitOps no cluster. Consulte as instruções "aqui".
- SetUp uma nova instância do Argo CD para o cluster. Consulte as instruções "aqui".

Abra o console do Argo CD e implante um aplicativo. Como exemplo, você pode implantar um aplicativo Jenkins usando o Argo CD com um Helm Chart. Ao criar o aplicativo, os seguintes detalhes foram fornecidos: Projeto: default cluster: 'https://kubernetes.default.svc'[] (sem as aspas) Namespace: Jenkins A url do Helm Chart: 'https://charts.bitnami.com/bitnami'[] (sem as aspas)

Proteção de dados

Para obter detalhes sobre como proteger e migrar cargas de trabalho de contêineres usando Trident Protect, consulte a seção a seguir: - "Proteja e migre aplicativos de contêiner usando Trident Protect"

Soluções adicionais de multicloud híbrida da NetApp para cargas de trabalho do Red Hat OpenShift

Veja as seguintes soluções adicionais:

- "Solução de contêineres Red Hat OpenShift on-premises"
- "Solução de contêineres do serviço Red Hat OpenShift na AWS"
- "Solução de virtualização Red Hat OpenShift on-premises"
- "Solução de virtualização do Red Hat OpenShift Service on AWS"

Proteja os dados usando o Trident Protect

Proteção de dados para aplicativos em contêineres na OpenShift Container Platform usando Trident Protect

Esta seção do documento de referência fornece detalhes sobre a criação de snapshots e backups de Container Apps usando Trident Protect. NetApp Trident Protect oferece recursos avançados de gerenciamento de dados de aplicativos que aprimoram a funcionalidade e a disponibilidade de aplicativos Kubernetes com estado, com suporte pelos sistemas de armazenamento NetApp ONTAP e pelo provisionador de armazenamento NetApp Trident CSI. Trident Protect cria snapshots e backups de aplicativos. Isso significa que snapshots e backups são criados não apenas para os dados do aplicativo em volumes persistentes, mas também para metadados do aplicativo. Os snapshots e backups criados pelo Trident Protect podem ser armazenados em qualquer um dos seguintes storage de objetos e restaurados a partir deles posteriormente.

- AWS S3
- Armazenamento de Blobs do Azure
- Armazenamento em nuvem do Google
- ONTAP S3
- StorageGrid
- Qualquer outro storage compatível com S3

Trident Protect utiliza o modelo Kubernetes de controle de acesso baseado em funções (RBAC). Por padrão, Trident Protect fornece um único namespace de sistema chamado trident-protect e sua conta de serviço padrão associada. Se você tem uma organização com muitos usuários ou necessidades de segurança específicas, pode usar os recursos de RBAC do Trident Protect para obter um controle mais granular sobre o acesso a recursos e namespaces.

Informações adicionais sobre RBAC no Trident Protect podem ser encontradas no "Documentação do Trident Protect"



O administrador do cluster tem acesso aos recursos no namespace padrão trident-protect e também pode acessar recursos em todos os outros namespaces. Os usuários não podem criar recursos personalizados (CRs) de gerenciamento de dados de aplicativos, como CRs de instantâneo e backup, no namespace trident-protect. Como prática recomendada, os usuários

precisarão criar essas CRs no namespace do aplicativo.

Trident Protect pode ser instalado seguindo as instruções fornecidas na documentação "aqui". Esta seção mostrará o fluxo de trabalho para a proteção de dados de aplicações em contêineres e a restauração das aplicações usando Trident Protect. 1. Criação de Snapshot (sob demanda ou agendada) 2. Restauração a partir do Snapshot (restaurar para o mesmo ou para um namespace diferente) 3. Criação de backup 4. Restauração a partir do backup

▼ **Pré-requisito**

Antes de criar os snapshots e backups para um aplicativo, o storage de objetos deve ser configurado no Trident Protect para armazenar os snapshots e backups. Isso é feito usando o bucket CR. Somente administradores podem criar um bucket CR e configurá-lo. O bucket CR é conhecido como AppVault no Trident Protect. Os objetos AppVault são a representação declarativa do fluxo de trabalho do Kubernetes de um bucket de armazenamento. Um CR AppVault contém as configurações necessárias para que um bucket seja usado em operações de proteção, como backups, snapshots, operações de restauração e replicação SnapMirror.

Neste exemplo, mostraremos o uso do ONTAP S3 como storage de objetos. Aqui está o fluxo de trabalho para criar AppVault CR para ONTAP S3: 1. Crie um servidor de armazenamento de objetos S3 na SVM no cluster ONTAP. 2. Crie um bucket no servidor de armazenamento de objetos. 3. Crie um usuário S3 na SVM. Guarde a chave de acesso e a chave secreta em um local seguro. 4. No OpenShift, crie um segredo para armazenar as credenciais do ONTAP S3. 5. Crie um objeto AppVault para ONTAP S3

Configurar Trident Protect AppVault para ONTAP S3

Arquivo YAML de exemplo para configurar Trident Protect com ONTAP S3 como o AppVault

```
# alias tp='tridentctl-protect'

appvault-secret.yaml

apiVersion: v1
stringData:
  accessKeyID: "<access key id created for a user to access ONTAP S3
bucket>"
  secretAccessKey: "corresponding Secret Access Key"
#data:
# base 64 encoded values
#  accessKeyID: <base64 access key id created for a user to access ONTAP
S3 bucket>
#  secretAccessKey: <base 64  Secret Access Key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

appvault.yaml
```

```
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: <bucket-name for storing the snapshots and backups>
      endpoint: <endpoint IP for S3>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost openshift-benchmark]#
[root@localhost openshift-benchmark]# tp get appvault -n trident-protect
+-------------------+----------+-----------+------+-------+
|       NAME        | PROVIDER |   STATE   | AGE  | ERROR |
+-------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 2d2h |       |
+-------------------+----------+-----------+------+-------+
[root@localhost openshift-benchmark]#
```

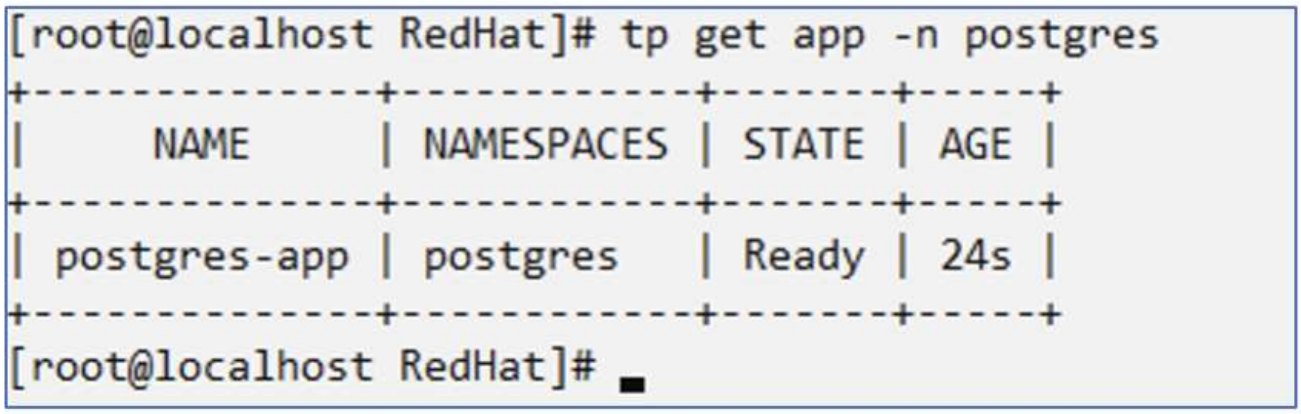
Arquivo yaml de exemplo para instalar o aplicativo postgresql

```
postgres.yaml
```

```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: postgres
spec:
  replicas: 1
  selector:
    matchLabels:
      app: postgres
  template:
    metadata:
      labels:
        app: postgres
    spec:
      containers:
      - name: postgres
        image: postgres:14
        env:
        - name: POSTGRES_USER
          #value: "myuser"
          value: "admin"
        - name: POSTGRES_PASSWORD
          #value: "mypassword"
          value: "adminpass"
        - name: POSTGRES_DB
          value: "mydb"
        - name: PGDATA
          value: "/var/lib/postgresql/data/pgdata"
        ports:
        - containerPort: 5432
        volumeMounts:
        - name: postgres-storage
          mountPath: /var/lib/postgresql/data
      volumes:
      - name: postgres-storage
        persistentVolumeClaim:
          claimName: postgres-pvc
---
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: postgres-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
```

```
    requests:
      storage: 5Gi
---
apiVersion: v1
kind: Service
metadata:
  name: postgres
spec:
  selector:
    app: postgres
  ports:
  - protocol: TCP
    port: 5432
    targetPort: 5432
  type: ClusterIP

Now create the Trident Protect application CR for the postgres app.
Include the objects in the namespace postgres and create it in the
postgres namespace.
# tp create app postgres-app --namespaces postgres -n postgres
```



▼ **Criar instantâneos**

Criando um snapshot sob demanda

```
# tp create snapshot postgres-snap1 --app postgres-app --appvault ontap-
s3-appvault -n postgres
Snapshot "postgres-snap1" created.
```

```
[root@localhost RedHat]# tp get snapshot -n postgres
+-----------------+--------------+-----------+-----+-------+
|      NAME       |   APP REF    |   STATE   | AGE | ERROR |
+-----------------+--------------+-----------+-----+-------+
| postgres-snap1 | postgres-app | Completed | 19s |       |
+-----------------+--------------+-----------+-----+-------+
[root@localhost RedHat]#
```

```
[root@localhost DataProtection]# oc get all,pvc,volumesnapshot -n postgres
Warning: apps.openshift.io/v1 DeploymentConfig is deprecated in v4.14+, unavailable in v4.10000+
Warning: kubevirt.io/v1 VirtualMachineInstancePresets is now deprecated and will be removed in v2.
NAME                            READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-jfx49     1/1     Running   0          3h47m

NAME               TYPE        CLUSTER-IP       EXTERNAL-IP   PORT(S)    AGE
service/postgres   ClusterIP   172.30.132.112   <none>        5432/TCP   3h47m

NAME                       READY   UP-TO-DATE   AVAILABLE   AGE
deployment.apps/postgres   1/1     1            1           3h47m

NAME                                  DESIRED   CURRENT   READY   AGE
replicaset.apps/postgres-cd9d6ccb     1         1         1       3h47m

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAG
ECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0    Bound    pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   8Gi        RWO            sc-zon
ea-nas   <unset>                 4h40m
persistentvolumeclaim/postgres-pvc                  Bound    pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   5Gi        RWO            sc-zon
ea-nas   <unset>                 3h47m

NAME                                                                                                                                READYTO
USE   SOURCEPVC                  SOURCESNAPSHOTCONTENT   RESTORESIZE   SNAPSHOTCLASS           SNAPSHOTCONTENT
          CREATIONTIME   AGE
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true
      postgres-pvc                                      53676Ki       trident-snapshotclass   snapcontent-796ea7f8-59a0-493e-bbd8-3a
e76fe9036c   13m            13m
volumesnapshot.snapshot.storage.k8s.io/snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true
      data-postgres-postgresql-0                        368Ki         trident-snapshotclass   snapcontent-86a464d4-ffd8-4279-9cf7-88
88a097c001   13m            13m
```

Criando um agendamento Usando o comando a seguir, os snapshots serão criados diariamente às 15:33 e dois snapshots e backups serão mantidos.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+-----+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE | ERROR |
+-----------+--------------+----------------------+---------+-------+-----+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 17s |       |
+-----------+--------------+----------------------+---------+-------+-----+-------+
[root@localhost DataProtection]#
```

Criando uma programação usando yaml

```
# tp create schedule schedule2 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres --dry-run >
hourly-snapshotschedule.yaml

cat hourly-snapshotschedule.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: schedule2
  namespace: postgres
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: postgres-app
  backupRetention: "2"
  dataMover: Restic
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  #hour: "15"
  minute: "33"
  recurrenceRule: ""
  snapshotRetention: "2"
status: {}
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 8d7h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 8d7h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
[root@localhost DataProtection]#
```

Você pode ver instantâneos criados nesta programação.

```
[root@localhost DataProtection]# tp get snap -n postgres
+-----------------------------+--------------+-----------+-------+-------+
|            NAME             |   APP REF    |   STATE   |  AGE  | ERROR |
+-----------------------------+--------------+-----------+-------+-------+
| hourly-3f1ee-20250214183300 | postgres-app | Completed | 19s   |       |
| postgres-snap1              | postgres-app | Completed | 1h25m |       |
+-----------------------------+--------------+-----------+-------+-------+
[root@localhost DataProtection]#
```

Snapshots de volume também são criados.

```
[root@localhost DataProtection]# oc get volumesnapshots -n postgres
NAME                                                                                                READYTOUSE   SOURCEPVC
                          CREATIONTIME   AGE
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-59a0-493e-bbd8-3ae76fe9036c   114m           114m
snapshot-2e94d04c-c8ea-446a-8d47-64b0bee67107-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-ffd8-4279-9cf7-8888a097c001   114m           114m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-951a9910-9edb-48ae-898a-1aed9aa25dc3   true         postgres-pvc
-7adc-4042-a8c9-7606d1103ead   30m            30m
snapshot-ce75a274-ecb2-48c9-a0a5-94c10f8e6cb1-pvc-9f89514e-3f2c-41ad-b7a3-792cea503f00   true         data-postgres-postgresql-0
-3a82-43f6-9868-dcadd2cc04e2   30m            30m
```

▼ **Excluir o aplicativo para simular a perda do aplicativo**

```
# oc delete deployment/postgres -n postgres
# oc get pod,pvc -n postgres
No resources found in postgres namespace.
```

▼ **Restaurar do Snapshot para o mesmo namespace**

```
# tp create sir postgres-sir --snapshot postgres/hourly-3f1ee-
20250214183300 -n postgres
SnapshotInplaceRestore "postgres-sir" created.
```

```
[root@localhost DataProtection]# tp get sir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-sir | ontap-s3-appvault | Completed | 2m39s |       |
+--------------+--------------------+-----------+-------+-------+
```

O aplicativo e seus PVCis são restaurados para o mesmo namespace.

```
[root@localhost DataProtection]# oc get pods,pvc -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-x85tg   1/1     Running   0          98s

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>                 105s
persistentvolumeclaim/postgres-pvc                 Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>                 105s
[root@localhost DataProtection]#
```

▼ **Restaurar do Snapshot para um namespace diferente**

```
# tp create snapshotrestore postgres-restore --snapshot postgres/hourly-3f1ee-20250214183300 --namespace-mapping postgres:postgres-restore -n postgres-restore
SnapshotRestore "postgres-restore" created.
```

```
[root@localhost DataProtection]# tp get snapshotrestore -n postgres-restore
+------------------+--------------------+-----------+-------+-------+
|       NAME       |     APPVAULT       |   STATE   |  AGE  | ERROR |
+------------------+--------------------+-----------+-------+-------+
| postgres-restore | ontap-s3-appvault | Completed | 1m15s |       |
+------------------+--------------------+-----------+-------+-------+
```

Você pode ver que o aplicativo foi restaurado para um novo namespace.

```
[root@localhost DataProtection]#
[root@localhost DataProtection]# oc get pods,pvc -n postgres-restore
NAME                         READY   STATUS    RESTARTS   AGE
pod/postgres-cd9d6ccb-pfxw9   1/1     Running   0          8d

NAME                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/data-postgres-postgresql-0   Bound    pvc-3dff4e42-828d-49f9-84e9-4daf75479292   8Gi        RWO            sc-zonea-nas
persistentvolumeclaim/postgres-pvc                 Bound    pvc-f57321b2-f21f-4eb7-8f86-4a17f915318b   5Gi        RWO            sc-zonea-nas
[root@localhost DataProtection]#
```

▼ **Criar backups**

Criando um backup sob demanda

```
# tp create backup postgres-backup1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup1" created.
```

```
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d12h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d10h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 10h36m |       |
| hourly-3f1ee-20250224003300 | postgres-app | Completed | 1h36m  |       |
| hourly-3f1ee-20250224013300 | postgres-app | Completed | 36m27s |       |
| postgres-backup1             | postgres-app | Completed | 6m19s  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Criando agendamento para backup

Os backups diários e horários na lista acima são criados a partir da programação configurada anteriormente.

```
# tp create schedule schedule1 --app postgres-app --appvault ontap-s3-
appvault --backup-retention 2 --snapshot-retention 2 --granularity Daily
--hour 15 --minute 33 --data-mover Restic -n postgres
Schedule "schedule1" created.
```

```
[root@localhost DataProtection]# tp get schedule -n postgres
+-----------+--------------+----------------------+---------+-------+------+-------+
|   NAME    |     APP      |       SCHEDULE       | ENABLED | STATE | AGE  | ERROR |
+-----------+--------------+----------------------+---------+-------+------+-------+
| schedule1 | postgres-app | Daily:hour=15,min=33 | true    |       | 9d8h |       |
| schedule2 | postgres-app | Hourly:min=33        | true    |       | 9d8h |       |
+-----------+--------------+----------------------+---------+-------+------+-------+
```

▼ **Restaurar do backup**

Exclua o aplicativo e os PVCs para simular uma perda de dados.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-dftkt     1/1     Running   0          11s
[root@localhost DataProtection]# oc get deployment -n postgres
NAME       READY   UP-TO-DATE   AVAILABLE   AGE
postgres   1/1     1            1           20s
[root@localhost DataProtection]# oc delete deployment/postgres -n postgres
deployment.apps "postgres" deleted
[root@localhost DataProtection]# oc get pods -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTE
SCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-b2cd67fd-fe4d-49b1-9e06-a53bf7be575e   8Gi        RWO            sc-zonea-nas   <unset>
         5d13h
postgres-pvc                  Bound    pvc-2d549395-0cc6-4529-b2b9-7361bfb14fa8   5Gi        RWO            sc-zonea-nas   <unset>
         5d13h
[root@localhost DataProtection]# oc delete pvc/data-postgres-postgresql-0  -n postgres
persistentvolumeclaim "data-postgres-postgresql-0" deleted
[root@localhost DataProtection]# oc delete pvc/postgres-pvc -n postgres
persistentvolumeclaim "postgres-pvc" deleted
[root@localhost DataProtection]# oc get pvc -n postgres
No resources found in postgres namespace.
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Restaurar para o mesmo namespace #tp create bir postgres-bir --backup postgres/hourly-3f1ee-20250224023300 -n postgres BackupInplaceRestore "postgres-bir" criado.

```
[root@localhost DataProtection]# tp get bir -n postgres
+--------------+--------------------+-----------+-------+-------+
|     NAME     |      APPVAULT      |   STATE   |  AGE  | ERROR |
+--------------+--------------------+-----------+-------+-------+
| postgres-bir | ontap-s3-appvault | Completed | 2m19s |       |
+--------------+--------------------+-----------+-------+-------+
```

O aplicativo e os PVCs são restaurados no mesmo namespace.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-t857w     1/1     Running   0          10m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-0a849c19-16fe-466f-9733-85e82a8b1677   8Gi        RWO            sc-zonea-nas   <unset>
          10m
postgres-pvc                  Bound    pvc-ded304ea-02d4-4225-b606-63007666ad66   5Gi        RWO            sc-zonea-nas   <unset>
          10m
```

Restaurar para um namespace diferente Criar um novo namespace. Restaurar de um backup para o novo namespace.

```
[root@localhost DataProtection]# oc create ns postgres-restore-from-backup
namespace/postgres-restore-from-backup created
[root@localhost DataProtection]# tp create backuprestore postgres-restore-from-backup --backup postgres/postgres-backup1 --namespace-map
ping postgres:postgres-restore-from-backup -n postgres-restore-from-backup
BackupRestore "postgres-restore-from-backup" created.
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           37s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE     ERROR   AGE
postgres-restore-from-backup   Running           56s
[root@localhost DataProtection]# oc get backuprestore -n postgres-restore-from-backup
NAME                           STATE       ERROR   AGE
postgres-restore-from-backup   Completed           2m52s
[root@localhost DataProtection]# oc get pods -n postgres-restore-from-backup
NAME                        READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-p659p     1/1     Running   0          2m9s
[root@localhost DataProtection]# oc get pvc -n postgres-restore-from-backup
NAME                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0    Bound    pvc-36df7399-95da-4c67-a621-af9434015bdb   8Gi        RWO            sc-zonea-nas   <unset>
          2m18s
postgres-pvc                  Bound    pvc-633de3aa-a4f9-4f3b-93cc-e91afbd4fe02   5Gi        RWO            sc-zonea-nas   <unset>
          2m18s
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

▼ **Migrar aplicativos**

Para clonar ou migrar um aplicativo para um cluster diferente (realizar uma clonagem entre clusters), crie um backup no cluster de origem e, em seguida, restaure o backup em um cluster diferente. Certifique-se de que Trident Protect esteja instalado no cluster de destino.

No cluster de origem, execute as etapas conforme mostrado na imagem abaixo:

```
[root@localhost DataProtection]# tp create backup postgres-backup-cluster1 --app postgres-app --appvault ontap-s3-appvault -n postgres
Backup "postgres-backup-cluster1" created.
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h18m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h18m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 18m26s |       |
| postgres-backup-cluster1     | postgres-app | Running   | 35s    |       |
| postgres-backup1             | postgres-app | Completed | 1h48m  |       |
+------------------------------+--------------+-----------+--------+-------+
[root@localhost DataProtection]# tp get backup -n postgres
+------------------------------+--------------+-----------+--------+-------+
|             NAME             |   APP REF    |   STATE   |  AGE   | ERROR |
+------------------------------+--------------+-----------+--------+-------+
| backup1                      | postgres-app | Completed | 5d14h  |       |
| daily-feac1-20250222153300   | postgres-app | Completed | 1d12h  |       |
| daily-feac1-20250223153300   | postgres-app | Completed | 12h19m |       |
| hourly-3f1ee-20250224023300  | postgres-app | Completed | 1h19m  |       |
| hourly-3f1ee-20250224033300  | postgres-app | Completed | 19m41s |       |
| postgres-backup-cluster1     | postgres-app | Completed | 1m50s  |       |
| postgres-backup1             | postgres-app | Completed | 1h49m  |       |
+------------------------------+--------------+-----------+--------+-------+
```

Activate Windows
Go to Settings to activate Windows.

Do cluster de origem, alterne o contexto para o cluster de destino. Em seguida, certifique-se de que o

AppVault esteja acessível a partir do contexto do cluster de destino e obtenha o conteúdo do AppVault do cluster de destino.

```
[root@localhost DataProtection]# kubectl config use-context default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin
Switched to context "default/api-bm-cluster5-min-ocpv-sddc-netapp-com:6443/kube:admin".
[root@localhost DataProtection]# tp get appvault -n trident-protect
+------------------+----------+-----------+------+-------+
|       NAME       | PROVIDER |   STATE   | AGE  | ERROR |
+------------------+----------+-----------+------+-------+
| ontap-s3-appvault | OntapS3  | Available | 3d6h |       |
+------------------+----------+-----------+------+-------+
[root@localhost DataProtection]# tp get appvaultcontent ontap-s3-appvault --show-resources backup --show-paths
+--------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
----------------------------------------------------------------------------+
|    CLUSTER   |     APP     |  TYPE  |            NAME             |        TIMESTAMP        |
                  PATH                                                                        |
+--------------+-------------+--------+-----------------------------+-------------------------+-----------------------------------
----------------------------------------------------------------------------+
| ocp-cluster11 | bbox        | backup | bboxbackup1                 | 2025-01-17 15:57:49 (UTC) | bbox_68b4f05f-d5f1-4304-8c69-ad67514
fe393/backups/bboxbackup1_3960c945-8ee0-42fe-945c-c57bb0a3af6f                                                                  |
| ocp-cluster11 | postgres-app | backup | backup1                     | 2025-02-18 13:31:50 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/backup1_28e1bd9a-9b04-4412-8b96-811f9b62e2e3                                                               |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250222153300  | 2025-02-22 15:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250222153300_23d1386b-09f0-456f-aa49-a5865fd48abd  |
| ocp-cluster11 | postgres-app | backup | daily-feac1-20250223153300  | 2025-02-23 15:34:42 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/daily-feac1-20250223153300_c492a4d1-38a9-4472-9684-4705c12a206d  |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224033300 | 2025-02-24 03:34:44 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224033300_3d09ab81-f6fe-47fa-a699-28006160cdbc |
| ocp-cluster11 | postgres-app | backup | hourly-3f1ee-20250224043300 | 2025-02-24 04:34:47 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/hourly-3f1ee-20250224043300_66805e4f-7631-48a6-98f7-d34bb8626031 |
| ocp-cluster11 | postgres-app | backup | postgres-backup-cluster1    | 2025-02-24 03:52:36 (UTC) | postgres-app_4d798ed5-cfa8-49ff-a5b6
-c5e2d89aeb89/backups/postgres-backup-cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3    |
```

Use o caminho de backup da lista e crie um objeto CR de backuprestore, conforme mostrado no comando abaixo.

```
# tp create backuprestore backup-restore-cluster2 --namespace-mapping
postgres:postgres --appvault ontap-s3-appvault --path postgres-
app_4d798ed5-cfa8-49ff-a5b6-c5e2d89aeb89/backups/postgres-backup-
cluster1_ec0ed3f3-5500-4e72-afa8-117a04a0b1c3 -n postgres
BackupRestore "backup-restore-cluster2" created.
```

```
[root@localhost DataProtection]# tp get backuprestore -n postgres
+--------------------------+--------------------+-----------+--------+-------+
|           NAME           |      APPVAULT      |   STATE   |  AGE   | ERROR |
+--------------------------+--------------------+-----------+--------+-------+
| backup-restore-cluster2 | ontap-s3-appvault | Completed | 12m41s |       |
+--------------------------+--------------------+-----------+--------+-------+
```

Agora você pode ver que os pods do aplicativo e os pvcs são criados no cluster de destino.

```
[root@localhost DataProtection]# oc get pods -n postgres
NAME                     READY   STATUS    RESTARTS   AGE
postgres-cd9d6ccb-2lvcq   1/1     Running   0          13m
[root@localhost DataProtection]# oc get pvc -n postgres
NAME                       STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUT
ESCLASS   AGE
data-postgres-postgresql-0   Bound    pvc-872a5182-601b-4848-b410-fef368337d07   8Gi        RWO            sc-zoneb-san   <unset>
          13m
postgres-pvc                 Bound    pvc-caf9fa71-76a8-4645-9bb5-2ed72e72948b   5Gi        RWO            sc-zoneb-san   <unset>
          13m
[root@localhost DataProtection]#
```

Activate Windows
Go to Settings to activate Windows.

Proteja VMs no Red Hat OpenShift Virtualization usando Trident Protect

Proteja VMs em OpenShift Virtualization usando snapshots e backups. Este procedimento inclui a criação de um AppVault usando ONTAP S3 storage de objetos, configurar o Trident Protect para capturar dados da VM, incluindo objetos de recursos do Kubernetes, volumes persistentes e imagens internas, e restaurar os dados quando necessário.

As máquinas virtuais no ambiente de virtualização OpenShift são aplicativos em contêineres executados nos nós de trabalho da sua plataforma OpenShift Container. É importante proteger os metadados da VM, bem como os discos persistentes das VMs, para que, quando eles forem perdidos ou corrompidos, você possa recuperá-los.

Os discos persistentes das VMs de Virtualização OpenShift podem ser suportados pelo armazenamento ONTAP integrado ao cluster OpenShift usando "Trident CSI". Nesta seção, usamos "Trident Protect" para criar snapshots e backups das VMs, incluindo seus volumes de dados, no storage de objetos ONTAP.

Em seguida, restauramos a partir de um snapshot ou de um backup quando necessário.

Trident Protect permite snapshots, backups, restaurações e recuperação de desastres de aplicações e VMs em um OpenShift cluster. Para VMs de OpenShift Virtualization, os dados que podem ser protegidos com Trident Protect incluem objetos de recursos do Kubernetes associados às VMs, volumes persistentes e imagens internas.

A seguir estão as versões dos vários componentes usados nos exemplos desta seção

- "Cluster OpenShift 4.17"
- "OpenShift Virtualization instalado via OpenShift Virtualization Operator fornecido pela Red Hat"
- "Trident 25.02"
- "Trident Protect 25.02"
- "ONTAP 9.16"

Criar AppVault para storage de objetos

▼ **Criar AppVault**

Antes de criar snapshots e backups para um aplicativo ou uma máquina virtual, o storage de objetos deve ser configurado no Trident Protect para armazenar os snapshots e backups. Isso é feito usando o bucket CR. Somente administradores podem criar um bucket CR e configurá-lo. O bucket CR é conhecido como AppVault no Trident Protect. Os objetos AppVault são a representação declarativa do fluxo de trabalho do Kubernetes de um bucket de armazenamento. Um CR AppVault contém as configurações necessárias para que um bucket seja usado em operações de proteção, como backups, snapshots, operações de restauração e replicação SnapMirror.

Neste exemplo, mostraremos o uso do ONTAP S3 como storage de objetos. A seguir está o fluxo de trabalho para criar AppVault CR para ONTAP S3: 1. Crie um servidor de armazenamento de objetos S3 na SVM no cluster ONTAP. 2. Crie um bucket no servidor de armazenamento de objetos. 3. Crie um usuário S3 na SVM. Guarde a chave de acesso e a chave secreta em um local seguro. 4. No OpenShift, crie um segredo para armazenar as credenciais do ONTAP S3. 5. Crie um objeto AppVault para ONTAP S3

Configurar Trident Protect AppVault para ONTAP S3

```
# alias tp='tridentctl-protect'

# cat appvault-secret.yaml
apiVersion: v1
stringData:
  accessKeyID: "<access key of S3>"
  secretAccessKey: "<secret access key of S3>"
# you can also provide base 64 encoded values instead of string values
#data:
# base 64 encoded values
#  accessKeyID: < base 64 encoded access key>
#  secretAccessKey: <base 64 encoded secretAccess key>
kind: Secret
metadata:
  name: appvault-secret
  namespace: trident-protect
type: Opaque

# cat appvault.yaml
apiVersion: protect.trident.netapp.io/v1
kind: AppVault
metadata:
  name: ontap-s3-appvault
  namespace: trident-protect
spec:
  providerConfig:
    azure:
      accountName: ""
      bucketName: ""
      endpoint: ""
    gcp:
      bucketName: ""
      projectID: ""
    s3:
      bucketName: trident-protect
      endpoint: <lif for S3 access>
      secure: "false"
      skipCertValidation: "true"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        key: accessKeyID
        name: appvault-secret
    secretAccessKey:
      valueFromSecret:
```

```
        key: secretAccessKey
        name: appvault-secret
  providerType: OntapS3

# oc create -f appvault-secret.yaml -n trident-protect
# oc create -f appvault.yaml -n trident-protect
```

```
[root@localhost VM-DataProtection]# tp get appvault
+-------------------+----------+-----------+-------+---------+-------+
|       NAME        | PROVIDER |   STATE   | ERROR | MESSAGE |  AGE  |
+-------------------+----------+-----------+-------+---------+-------+
| ontap-s3-appvault | OntapS3  | Available |       |         | 8d17h |
+-------------------+----------+-----------+-------+---------+-------+
[root@localhost VM-DataProtection]#
```

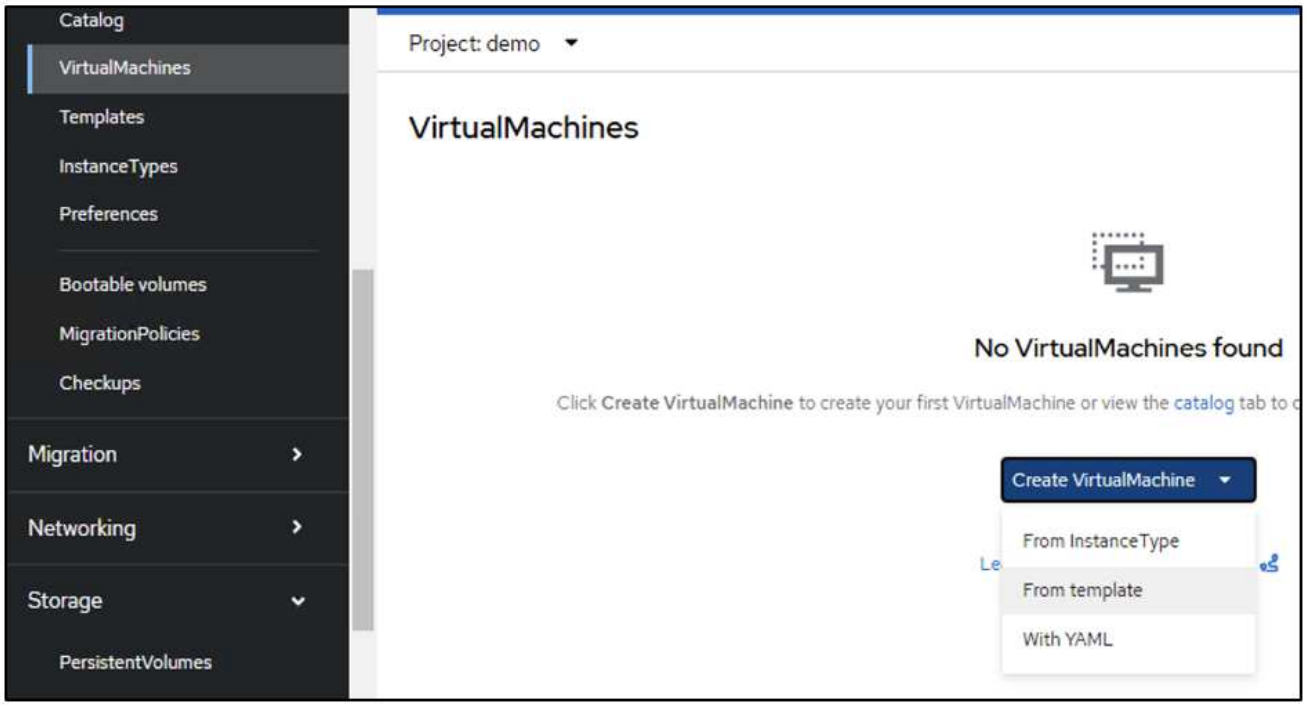
Criar uma VM no OpenShift Virtualization

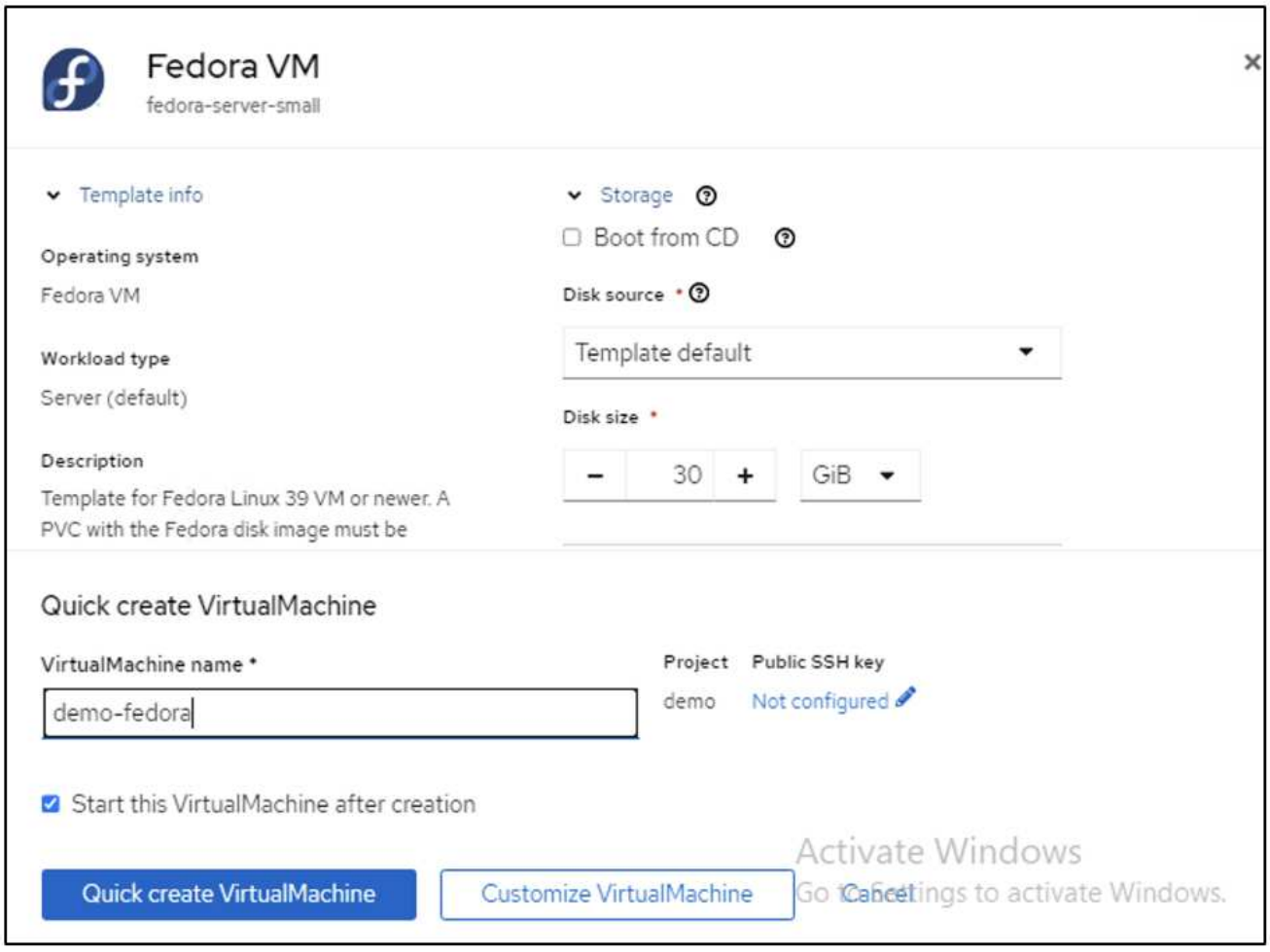
▼ **Criar uma VM no OpenShift Virtualization**

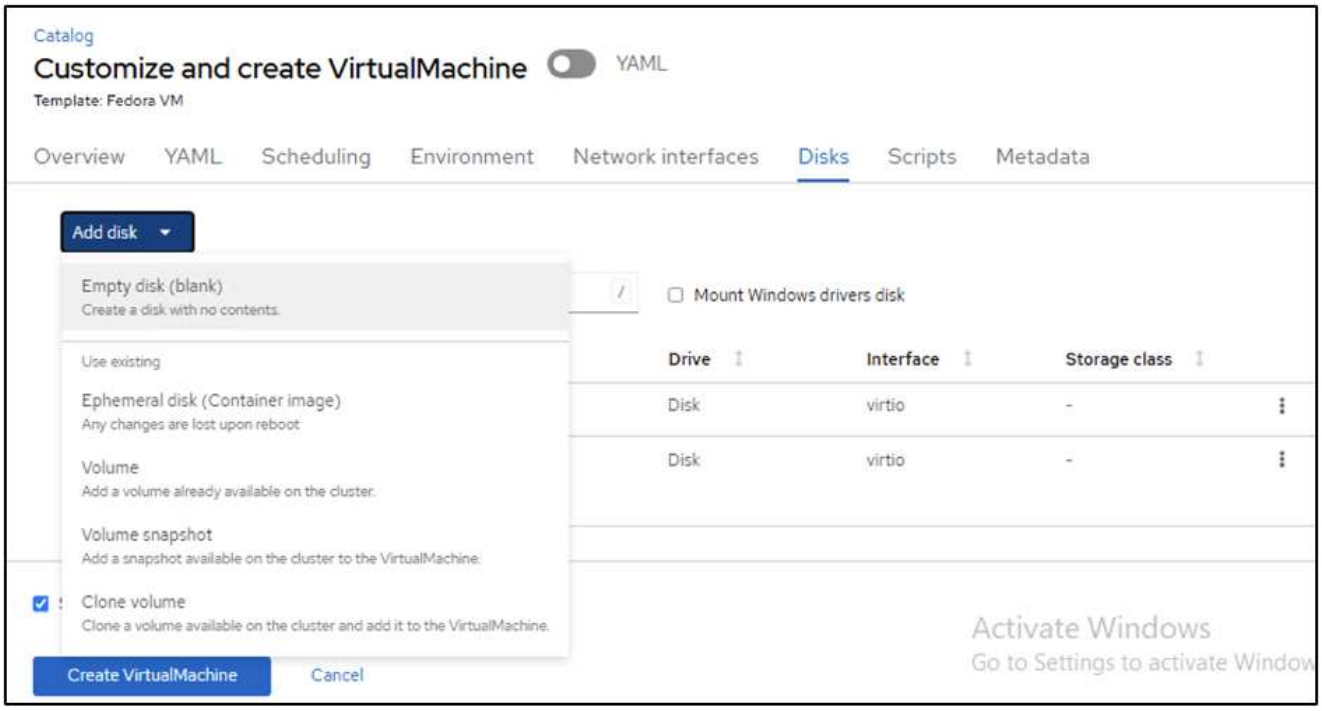
As capturas de tela a seguir mostram a criação da VM (demo-fedora no namespace demo) a partir do console usando o modelo. O disco raiz escolhe a classe de armazenamento padrão automaticamente, portanto, verifique se a classe de armazenamento padrão está definida corretamente. Nesta configuração, a classe de armazenamento padrão é **sc-zonea-san**. Ao criar o disco adicional, certifique-se de escolher a classe de armazenamento sc-zonea-san e marcar a caixa de seleção "**Aplicar configurações de armazenamento otimizadas**". Isso definirá os modos de acesso como RWX e o modo de volume como Bloqueio.

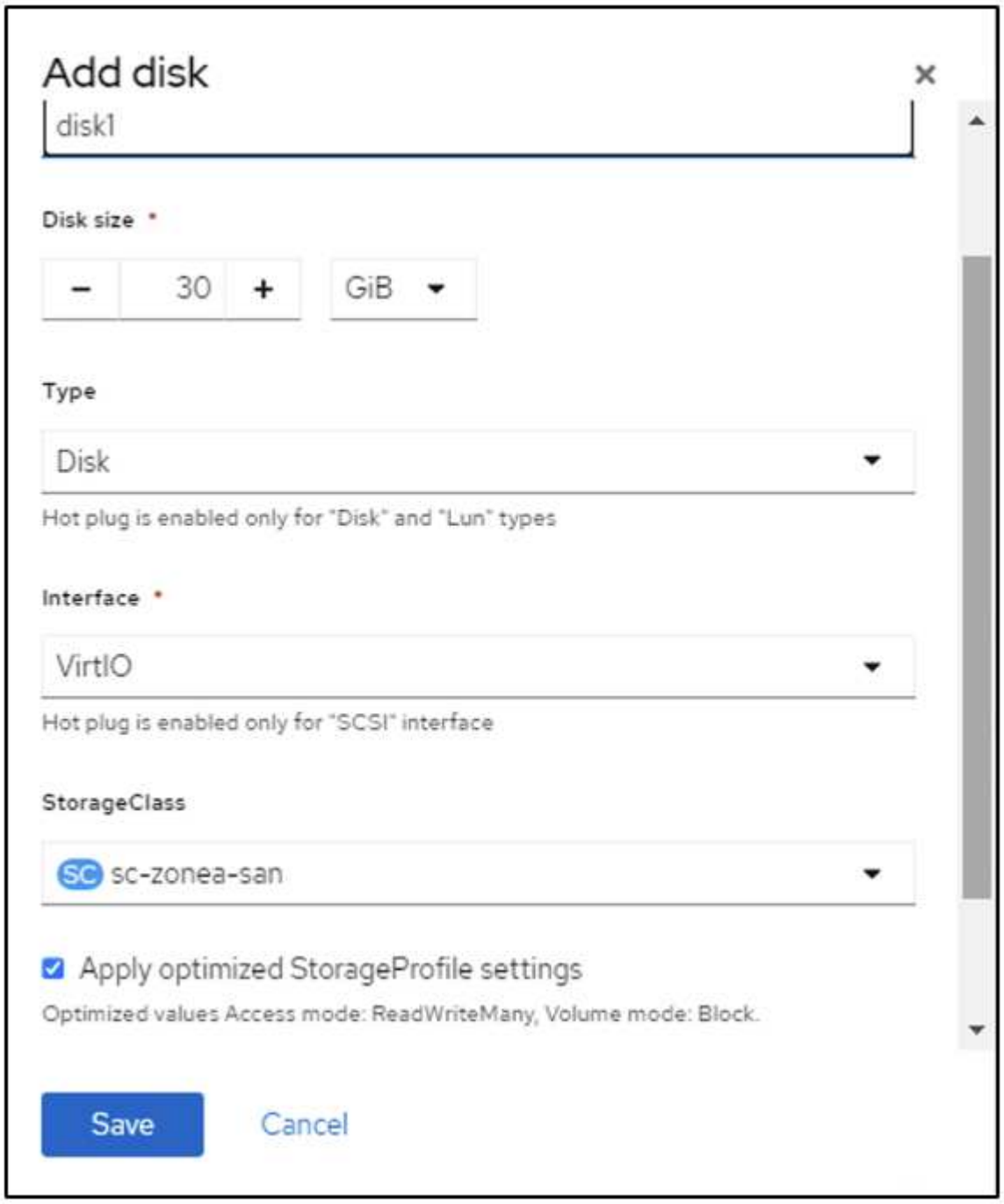
> ⓘ O Trident suporta o modo de acesso RWX no modo Block Volume para SAN (iSCSI, NVMe/TCP e FC). (É o modo de acesso padrão para NAS). O modo de acesso RWX é necessário se você precisar fazer a migração ao vivo das VMs posteriormente.

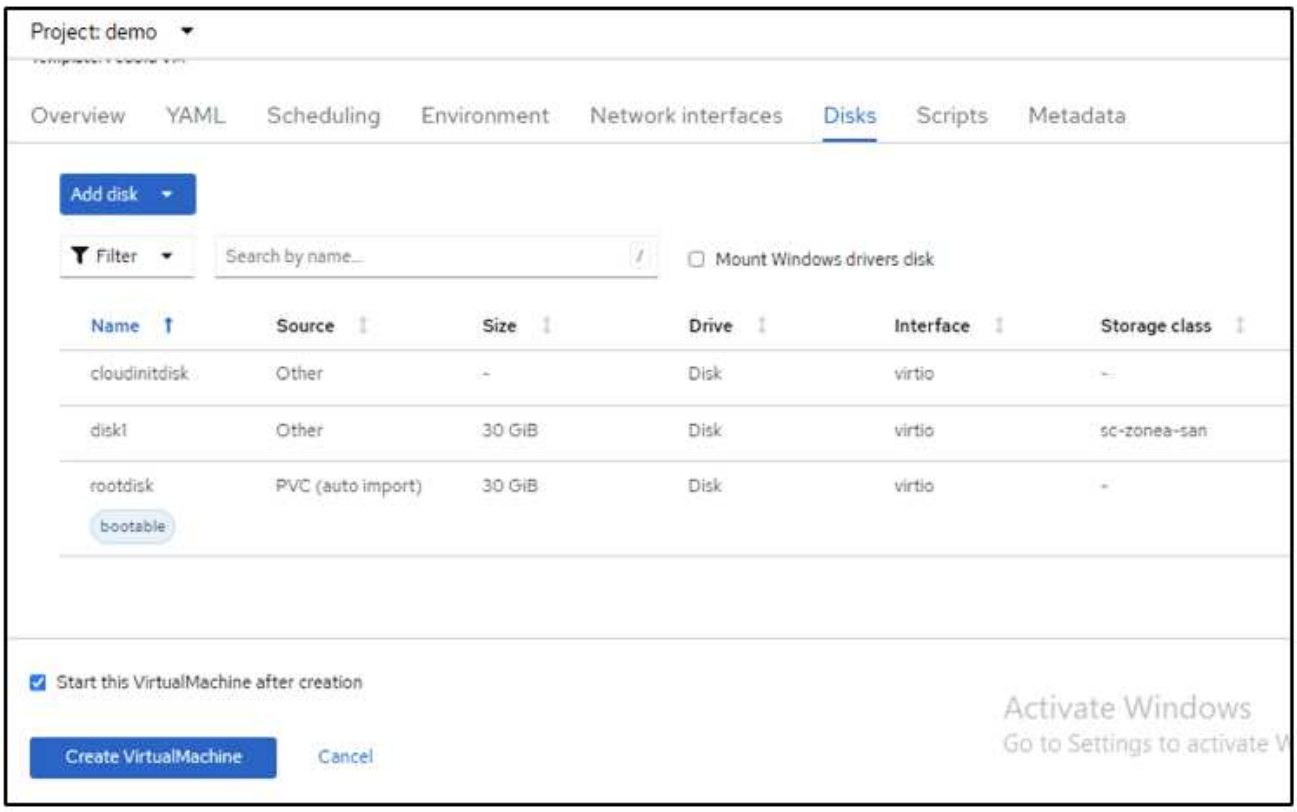



Catalog
VirtualMachines
Templates
InstanceTypes
Preferences
Bootable volumes
MigrationPolicies
Checkups
Migration
Networking
Storage
PersistentVolumes
Project: demo
VirtualMachines
No VirtualMachines found
Click Create VirtualMachine to create your first VirtualMachine or view the catalog tab to
Create VirtualMachine
From InstanceType
From template
With YAML


Fedora VM
fedora-server-small
Template info
Operating system
Fedora VM
Workload type
Server (default)
Description
Template for Fedora Linux 39 VM or newer. A PVC with the Fedora disk image must be
Storage
Boot from CD
Disk source *
Template default
Disk size *
30
GiB
Quick create VirtualMachine
VirtualMachine name *
demo-fedora
Project
demo
Public SSH key
Not configured
Start this VirtualMachine after creation
Activate Windows
Go to Settings to activate Windows.
Quick create VirtualMachine
Customize VirtualMachine
Cancel


Catalog
Customize and create VirtualMachine
YAML
Template: Fedora VM
Overview
YAML
Scheduling
Environment
Network interfaces
Disks
Scripts
Metadata
Add disk
Empty disk (blank)
Create a disk with no contents.
Use existing
Ephemeral disk (Container image)
Any changes are lost upon reboot
Volume
Add a volume already available on the cluster.
Volume snapshot
Add a snapshot available on the cluster to the VirtualMachine.
Clone volume
Clone a volume available on the cluster and add it to the VirtualMachine.
Mount Windows drivers disk
Drive
Interface
Storage class
Disk
virtio
-
Disk
virtio
-
Create VirtualMachine
Cancel
Activate Windows
Go to Settings to activate Windows


Add disk
disk1
Disk size *
30
GiB
Type
Disk
Hot plug is enabled only for "Disk" and "Lun" types
Interface *
VirtIO
Hot plug is enabled only for "SCSI" interface
StorageClass
SC sc-zonea-san
Apply optimized StorageProfile settings
Optimized values Access mode: ReadWriteMany, Volume mode: Block.
Save
Cancel




```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   2m54s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          110s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Criar um aplicativo

▼ **Criar aplicativo**

Crie um aplicativo Trident Protect para a VM

No exemplo, o namespace demo possui uma VM e todos os recursos do namespace são incluídos ao criar o app.

```
# alias tp='tridentctl-protect'
# tp create app demo-vm --namespaces demo -n demo --dry-run > app.yaml

# cat app.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-vm
```

```
  namespace: demo
spec:
  includedNamespaces:
  - namespace: demo
# oc create -f app.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+---------+------------+-------+-----+
|  NAME   | NAMESPACES | STATE | AGE |
+---------+------------+-------+-----+
| demo-vm | demo       | Ready | 45s |
+---------+------------+-------+-----+
[root@localhost VM-DataProtection]#
```

Proteja o aplicativo criando um backup

▼ **Criar backups**

Criar um backup sob demanda

Crie um backup para o aplicativo (demo-vm) criado anteriormente que inclua todos os recursos no namespace demo. Forneça o nome do appvault onde os backups serão armazenados.

```
# tp create backup demo-vm-backup-on-demand --app demo-vm --appvault
ontap-s3-appvault -n demo
Backup "demo-vm-backup-on-demand" created.
```

```
[root@localhost VM-DataProtection]# tp get backup -n demo
+--------------------------+---------+----------------+-----------+-------+--------+
|           NAME           |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+--------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand | demo-vm | Retain         | Completed |       | 12m53s |
+--------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Crie backups conforme uma programação

Crie um cronograma para os backups especificando a granularidade e o número de backups a serem mantidos.

```
# tp create schedule backup-schedule1 --app demo-vm --appvault ontap-s3-
appvault --granularity Hourly --minute 45 --backup-retention 1 -n demo
--dry-run>backup-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/backup-schedule1 created
```

```
#cat backup-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: backup-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "1"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "45"
  recurrenceRule: ""
  snapshotRetention: "0"
status: {}
# oc create -f backup-schedule-demo-vm.yaml -n demo
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+------------------+---------+---------------+---------+-------+-------+-----+
|       NAME       |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR | AGE |
+------------------+---------+---------------+---------+-------+-------+-----+
| backup-schedule1 | demo-vm | Hourly:min=45 | true    |       |       | 9s  |
+------------------+---------+---------------+---------+-------+-------+-----+
```

```
[root@localhost VM-DataProtection]# tp get backups -n demo
+-----------------------------+---------+----------------+-----------+-------+--------+
|            NAME             |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------+---------+----------------+-----------+-------+--------+
| demo-vm-backup-on-demand    | demo-vm | Retain         | Completed |       | 44m4s  |
| hourly-4c094-20250312144500 | demo-vm | Retain         | Completed |       | 20m34s |
+-----------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Restaurar do backup

▼ **Restaurar de backups**

Restaurar a VM para o mesmo namespace

No exemplo, o backup demo-vm-backup-on-demand contém o backup com o demo-app para a VM do Fedora.

Primeiro, exclua a VM e certifique-se de que os PVCs, o pod e os objetos da VM sejam excluídos do namespace "demo".

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                   AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   59m   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-69cts   1/1     Running   0          58m

NAME                                                  STATUS   VOLUME                                     CAPACITY
CLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                     Bound    pvc-406d9d57-4a5e-4123-93c1-13070b7b0140   30Gi
a-san   <unset>                 59m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-311f2f81-1d25-4a9a-b0cb-836b4e702f04   30Gi
a-san   <unset>                 59m
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc delete vm demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
No resources found in demo namespace.
[root@localhost VM-DataProtection]#
```

Agora, crie um objeto de restauração de backup no local.

```
# tp create bir demo-fedora-restore --backup demo/demo-vm-backup-on-
demand -n demo --dry-run>vm-demo-bir.yaml

# cat vm-demo-bir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo-fedora-restore
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/demo-vm-backup-on-demand_f6af3513-9739-480e-88c7-
4cca45808a80
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-bir.yaml -n demo
backupinplacerestore.protect.trident.netapp.io/demo-fedora-restore
created
```

```
[root@localhost VM-DataProtection]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 28m17s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Verifique se a VM, os pods e os PVCs foram restaurados

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo
NAME                                        AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora      116s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-9kfxh  1/1     Running   0          116s

NAME                                                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                    Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Restaurar a VM para um namespace diferente

Primeiro, crie um novo namespace para o qual você deseja restaurar o aplicativo, neste exemplo, demo2. Em seguida, crie um objeto de restauração de backup

```
# tp create br demo2-fedora-restore --backup demo/hourly-4c094-
20250312154500 --namespace-mapping demo:demo2 -n demo2 --dry-run>vm
-demo2-br.yaml

# cat vm-demo2-br.yaml
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  annotations:
    protect.trident.netapp.io/max-parallel-restore-jobs: "25"
  creationTimestamp: null
  name: demo2-fedora-restore
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/backups/hourly-4c094-20250312154500_aaa14543-a3fa-41f1-
a04c-44b1664d0f81
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
```

```
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""
# oc create -f vm-demo2-br.yaml -n demo2
```

```
[root@localhost VM-DataProtection]# tp get br -n demo2
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-fedora-restore | ontap-s3-appvault | Completed |       | 38m52s |
+----------------------+--------------------+-----------+-------+--------+
```

Verifique se a VM, os pods e os pvcs foram criados no novo namespace demo2.

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                   AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Proteja o aplicativo usando Snapshots

▼ Criar instantâneos

Crie um snapshot sob demanda Crie um snapshot para o aplicativo e especifique o appvault onde ele precisa ser armazenado.

```
# tp create snapshot demo-vm-snapshot-ondemand --app demo-vm --appvault
ontap-s3-appvault -n demo --dry-run
# cat demo-vm-snapshot-on-demand.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  creationTimestamp: null
  name: demo-vm-snapshot-ondemand
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  completionTimeout: 0s
  volumeSnapshotsCreatedTimeout: 0s
  volumeSnapshotsReadyToUseTimeout: 0s
status:
  conditions: null
```

```
  postSnapshotExecHooksRunResults: null
  preSnapshotExecHooksRunResults: null
  state: ""

# oc create -f demo-vm-snapshot-on-demand.yaml
snapshot.protect.trident.netapp.io/demo-vm-snapshot-ondemand created
```

```
[root@localhost VM-DataProtection]#
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE    STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m8s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-fedora-c7xc6   1/1     Running   0          5m7s

NAME                                                STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-fedora                   Bound    pvc-4d278ae2-76cc-46f1-bbf8-071ae75e4a82   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-9b96d09c-7226-4ffc-829b-2cee88e7a117   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Crie um cronograma para instantâneos Crie um cronograma para os instantâneos. Especifique a granularidade e o número de instantâneos a serem retidos.

```
# tp create Schedule snapshot-schedule1 --app demo-vm --appvault ontap-
s3-appvault --granularity Hourly --minute 50 --snapshot-retention 1 -n
demo --dry-run>snapshot-schedule-demo-vm.yaml

# cat snapshot-schedule-demo-vm.yaml
apiVersion: protect.trident.netapp.io/v1
kind: Schedule
metadata:
  creationTimestamp: null
  name: snapshot-schedule1
  namespace: demo
spec:
  appVaultRef: ontap-s3-appvault
  applicationRef: demo-vm
  backupRetention: "0"
  dayOfMonth: ""
  dayOfWeek: ""
  enabled: true
  granularity: Hourly
  hour: ""
  minute: "50"
  recurrenceRule: ""
  snapshotRetention: "1"
status: {}

# oc create -f snapshot-schedule-demo-vm.yaml
schedule.protect.trident.netapp.io/snapshot-schedule1 created
```

```
[root@localhost VM-DataProtection]# tp get schedule -n demo
+--------------------+---------+---------------+---------+-------+-------+-------+
|        NAME        |   APP   |   SCHEDULE    | ENABLED | STATE | ERROR |  AGE  |
+--------------------+---------+---------------+---------+-------+-------+-------+
| backup-schedule1   | demo-vm | Hourly:min=45 | true    |       |       | 5d23h |
| snapshot-schedule1 | demo-vm | Hourly:min=50 | true    |       |       | 12s   |
+--------------------+---------+---------------+---------+-------+-------+-------+
[root@localhost VM-DataProtection]#
```

```
[root@localhost VM-DataProtection]# tp get snapshots -n demo
+-----------------------------------------+---------+----------------+-----------+-------+--------+
|                  NAME                   |   APP   | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
| backup-39b67e1c-f875-4045-93df-78634bae9dfb | demo-vm | Delete         | Completed |       | 6m29s  |
| demo-vm-snapshot-ondemand               | demo-vm | Delete         | Completed |       | 21m30s |
| hourly-51839-20250318135000             | demo-vm | Delete         | Completed |       | 1m29s  |
+-----------------------------------------+---------+----------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Restaurar do Snapshot

▼ Restaurar do Snapshot

Restaurar a VM do snapshot para o mesmo namespace Exclua a VM demo-fedora do namespace demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   28h   Running   True

NAME                                                    STATUS   VOLUME
ORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                       Bound    pvc-e0d5f79d-dff9-450d-be0e-90ab6880b7af
-zonea-san   <unset>                 28h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-e6f7890a-70c7-4538-9035-5e2e9379511d
-zonea-san   <unset>                 28h
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo
virtualmachine.kubevirt.io "demo-fedora" deleted
[root@localhost RedHat]#
```

Crie um objeto de restauração de snapshot no local a partir do snapshot da VM.

```
# tp create sir demo-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand -n demo --dry-run>vm-demo-sir.yaml

# cat vm-demo-sir.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  creationTimestamp: null
  name: demo-fedora-restore-from-snapshot
  namespace: demo
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
```

```
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  resourceFilter: {}
status:
  conditions: null
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo-sir.yaml
snapshotinplacerestore.protect.trident.netapp.io/demo-fedora-restore-
from-snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sir -n demo
+----------------------------------+-------------------+-----------+-------+--------+
|               NAME               |     APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------------------+-------------------+-----------+-------+--------+
| demo-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 58m17s |
+----------------------------------+-------------------+-----------+-------+--------+
[root@localhost VM-DataProtection]#
```

Verifique se a VM e seus PVCs foram criados no namespace demo.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora   5m17s   Running   True

NAME                                                STATUS   VOLUME
persistentvolumeclaim/demo-fedora                   Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
[root@localhost RedHat]#
```

Restaurar a VM do snapshot para um namespace diferente

Exclua a VM no namespace demo2 restaurada anteriormente do backup.

```
[root@localhost VM-DataProtection]# oc get vm,pods,pvc -n demo2
NAME                                  AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos   3m12s   Running   True
virtualmachine.kubevirt.io/demo-fedora   3m11s   Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-w77rr   1/1     Running   0          3m11s
pod/virt-launcher-demo-fedora-wwdtc   1/1     Running   0          3m11s

NAME                                                  STATUS   VOLUME                                     CAPACITY   ACCESS MODES
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                     Bound    pvc-7aafd5e2-d4cf-4af6-a259-c68e016ec6cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m26s
persistentvolumeclaim/demo-fedora                     Bound    pvc-c1f8145a-56ea-42c5-abb4-6457b6853e1c   30Gi       RWX
  sc-zonea-san   <unset>                 3m25s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-e82b6d98-6762-4473-9bb8-7e98efcb7987   30Gi       RWX
  sc-zonea-san   <unset>                 3m20s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-ee13cfbc-2921-4129-a214-a0f6b10335cd   30Gi       RWX
  sc-zonea-san   <unset>                 3m16s
[root@localhost VM-DataProtection]# oc delete virtualmachine.kubevirt.io/demo-fedora -n demo2
virtualmachine.kubevirt.io "demo-fedora" deleted
```

Crie o objeto de restauração de snapshot a partir do snapshot e forneça o mapeamento de namespace.

```
# tp create sr demo2-fedora-restore-from-snapshot --snapshot demo/demo-
vm-snapshot-ondemand --namespace-mapping demo:demo2 -n demo2 --dry
-run>vm-demo2-sr.yaml

# cat vm-demo2-sr.yaml
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  creationTimestamp: null
  name: demo2-fedora-restore-from-snapshot
  namespace: demo2
spec:
  appArchivePath: demo-vm_cc8adc7a-0c28-460b-a32f-
0a7b3d353e13/snapshots/20250318132959_demo-vm-snapshot-
ondemand_e3025972-30c0-4940-828a-47c276d7b034
  appVaultRef: ontap-s3-appvault
  namespaceMapping:
  - destination: demo2
    source: demo
  resourceFilter: {}
status:
  postRestoreExecHooksRunResults: null
  state: ""

# oc create -f vm-demo2-sr.yaml
snapshotrestore.protect.trident.netapp.io/demo2-fedora-restore-from-
snapshot created
```

```
[root@localhost VM-DataProtection]# tp get sr -n demo2
+-----------------------------------+------------------+-----------+-------+--------+
|               NAME                |     APPVAULT     |   STATE   | ERROR |  AGE   |
+-----------------------------------+------------------+-----------+-------+--------+
| demo2-fedora-restore-from-snapshot | ontap-s3-appvault | Completed |       | 15m22s |
+-----------------------------------+------------------+-----------+-------+--------+
```

Verifique se a VM e seus PVCs foram restaurados no novo namespace demo2.

```
[root@localhost RedHat]# oc get vm,pvc -n demo2
NAME                                      AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    29h   Running   True

NAME                                                          STATUS   VOLUME
STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-fedora                             Bound    pvc-35dcd9b2-4fca-486c-af9e-596bc5b4dc15
-zonea-san     <unset>                 29h
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-575a3111-382f-4933-a778-0089fa1ea2af
-zonea-san     <unset>                 29h
[root@localhost RedHat]#
```

Restaurar uma VM específica

▼ Selecionando VMs específicas em um namespace para criar snapshots/backups e restaurar

No exemplo anterior, tínhamos uma única VM dentro de um namespace. Ao incluir todo o namespace no backup, todos os recursos associados a essa VM foram capturados. No exemplo a seguir, adicionamos outra VM ao mesmo namespace e criamos um aplicativo apenas para essa nova VM usando um seletor de rótulos.

Crie uma nova VM (demo-centos vm) no namespace demo

```
[root@localhost VM-DataProtection]# oc get vm,pod,pvc -n demo
NAME                                    AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos  2m47s   Running   True
virtualmachine.kubevirt.io/demo-fedora  81m     Running   True

NAME                                 READY   STATUS    RESTARTS   AGE
pod/virt-launcher-demo-centos-2nq6g  1/1     Running   0          113s
pod/virt-launcher-demo-fedora-9kfxh  1/1     Running   0          81m

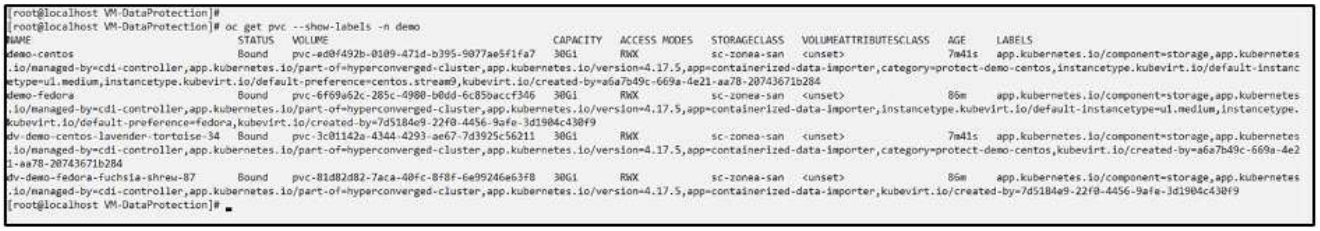
NAME                                                          STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS
persistentvolumeclaim/demo-centos                             Bound    pvc-ed0f492b-0109-471d-b395-9077ae5f1fa7   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/demo-fedora                             Bound    pvc-6f69a62c-285c-4980-b0dd-6c85baccf346   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34     Bound    pvc-3c01142a-4344-4293-ae67-7d3925c56211   30Gi       RWX            sc-zonea-san
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87         Bound    pvc-81d82d82-7aca-40fc-8f8f-6e99246e63f8   30Gi       RWX            sc-zonea-san
[root@localhost VM-DataProtection]#
```

Rotule a VM demo-centos e seus recursos associados

```
[root@localhost VM-DataProtection]# oc label vm demo-centos category=protect-demo-centos -n demo
virtualmachine.kubevirt.io/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc demo-centos category=protect-demo-centos -n demo
persistentvolumeclaim/demo-centos labeled
[root@localhost VM-DataProtection]# oc label pvc dv-demo-centos-lavender-tortoise-34 category=protect-demo-centos -n demo
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34 labeled
[root@localhost VM-DataProtection]#
```

Verifique se a VM demo-centos e os pvcs receberam os rótulos

```
[root@localhost VM-DataProtection]# oc get vm --show-labels -n demo
NAME          AGE     STATUS    READY   LABELS
demo-centos   6m31s   Running   True    app=demo-centos,category=protect-demo-centos,kubevirt.io/dynamic-credentials-support=true,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=centos-stream9-server-small
demo-fedora   85m     Running   True    app=demo-fedora,vm.kubevirt.io/template.namespace=openshift,vm.kubevirt.io/template.revision=1,vm.kubevirt.io/template.version=v0.31.1,vm.kubevirt.io/template=fedora-server-small
[root@localhost VM-DataProtection]#
```



Crie um aplicativo apenas para uma VM específica (demo-centos) usando o seletor de rótulos

```
# tp create app demo-centos-app --namespaces 'demo(category=protect-
demo-centos)' -n demo --dry-run>demo-centos-app.yaml

# cat demo-centos-app.yaml

apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  creationTimestamp: null
  name: demo-centos-app
  namespace: demo
spec:
  includedNamespaces:
  - labelSelector:
      matchLabels:
        category: protect-demo-centos
    namespace: demo
status:
  conditions: null

# oc create -f demo-centos-app.yaml -n demo
application.protect.trident.netapp.io/demo-centos-app created
```

```
[root@localhost VM-DataProtection]# tp get app -n demo
+-----------------+------------+-------+------+
|      NAME       | NAMESPACES | STATE | AGE  |
+-----------------+------------+-------+------+
| demo-centos-app | demo       | Ready | 56s  |
| demo-vm         | demo       | Ready | 4h6m |
+-----------------+------------+-------+------+
```

O método de criação de backups e snapshots sob demanda e conforme agendamento é o mesmo mostrado anteriormente. Como o aplicativo trident-protect que está sendo usado para criar os snapshots ou backups contém apenas a VM específica do namespace, a restauração a partir deles restaura apenas uma VM específica. Um exemplo de operação de backup/restauração é mostrado abaixo.

Crie um backup de uma VM específica em um namespace usando seu aplicativo correspondente

Nas etapas anteriores, um aplicativo foi criado usando seletores de rótulos para incluir apenas a VM centos no namespace demo. Crie um backup (backup sob demanda, neste exemplo) para este aplicativo.

```
# tp create backup demo-centos-backup-on-demand --app demo-centos-app
--appvault ontap-s3-appvault -n demo
Backup "demo-centos-backup-on-demand" created.
```

```
+------------------------------+----------------+----------------+-----------+-------+--------+
|             NAME             |       APP      | RECLAIM POLICY |   STATE   | ERROR |  AGE   |
+------------------------------+----------------+----------------+-----------+-------+--------+
| demo-centos-backup-on-demand | demo-centos-app | Retain         | Completed |       | 13m22s |
| demo-vm-backup-on-demand     | demo-vm         | Retain         | Completed |       | 4h19m  |
| hourly-4c094-20250312174500  | demo-vm         | Retain         | Completed |       | 56m17s |
+------------------------------+----------------+----------------+-----------+-------+--------+
```

Restaurar uma VM específica para o mesmo namespace O backup de uma VM específica (centos) foi criado usando o aplicativo correspondente. Se um backup-in-loco-restauração ou um backup-restauração for criado a partir disso, somente essa VM específica será restaurada. Exclua a VM Centos.

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-centos    4m27s   Running   True
virtualmachine.kubevirt.io/demo-fedora    4m27s   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-e8faeaf8-fc0c-4d92-96de-c83a335a7a17
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-66eb7996-1420-4513-a67c-2824f08534da
  sc-zonea-san   <unset>                 4m33s
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
  sc-zonea-san   <unset>                 4m32s
```

```
[root@localhost RedHat]# oc delete virtualmachine.kubevirt.io/demo-centos -n demo
virtualmachine.kubevirt.io "demo-centos" deleted
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                      AGE     STATUS    READY
virtualmachine.kubevirt.io/demo-fedora    5m17s   Running   True

NAME                                                    STATUS   VOLUME
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87   Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c
[root@localhost RedHat]#
```

Crie uma restauração de backup no local a partir do demo-centos-backup-on-demand e verifique se a VM centos foi recriada.

```
#tp create bir demo-centos-restore --backup demo/demo-centos-backup-on-
demand -n demo
BackupInplaceRestore "demo-centos-restore" created.
```

```
[root@localhost RedHat]# tp get bir -n demo
+----------------------+--------------------+-----------+-------+-------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE  |
+----------------------+--------------------+-----------+-------+-------+
| demo-centos-restore | ontap-s3-appvault | Completed |       | 57m9s |
| demo-fedora-restore | ontap-s3-appvault | Completed |       | 7d5h  |
+----------------------+--------------------+-----------+-------+-------+
```

```
[root@localhost RedHat]# oc get vm,pvc -n demo
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   29m   Running   True
virtualmachine.kubevirt.io/demo-fedora   85m   Running   True

NAME                                                    STATUS   VOLUME                                     C
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-82954bf7-4a7e-4e0c-9a04-4fa152e1b0ef   1
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/demo-fedora                       Bound    pvc-e2f418b0-1b97-40fc-9cb8-943b370d85bc   1
  sc-zonea-san   <unset>                 85m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-2a8d4eb5-ed6d-4408-b85d-e218e9a5d4b0   1
  sc-zonea-san   <unset>                 29m
persistentvolumeclaim/dv-demo-fedora-fuchsia-shrew-87       Bound    pvc-db085154-079f-45ad-9e62-9656e913d01c   1
  sc-zonea-san   <unset>                 85m
[root@localhost RedHat]#
```

Restaurar uma VM específica para um namespace diferente Crie uma restauração de backup para um namespace diferente (demo3) de demo-centos-backup-on-demand e verifique se a VM centos foi recriada.

```
# tp create br demo2-centos-restore --backup demo/demo-centos-backup-on-demand --namespace-mapping demo:demo3 -n demo3
BackupRestore "demo2-centos-restore" created.
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# tp get br -n demo3
+----------------------+--------------------+-----------+-------+--------+
|         NAME         |      APPVAULT      |   STATE   | ERROR |  AGE   |
+----------------------+--------------------+-----------+-------+--------+
| demo2-centos-restore | ontap-s3-appvault | Completed |       | 52m57s |
+----------------------+--------------------+-----------+-------+--------+
[root@localhost RedHat]#
```

```
[root@localhost RedHat]#
[root@localhost RedHat]# oc get vm,pvc -n demo3
NAME                                    AGE   STATUS    READY
virtualmachine.kubevirt.io/demo-centos   19m   Running   True

NAME                                                    STATUS   VOLUME
  STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
persistentvolumeclaim/demo-centos                       Bound    pvc-0a14e38f-07de-4e09-8f88-14a9a8bb45c2
  sc-zonea-san   <unset>                 19m
persistentvolumeclaim/dv-demo-centos-lavender-tortoise-34   Bound    pvc-d4f9cf2f-264c-4d02-94bf-0db28b427acc
  sc-zonea-san   <unset>                 19m
[root@localhost RedHat]#
```

Demonstração em vídeo

O vídeo a seguir mostra uma demonstração de proteção de uma VM usando Snapshots

Protegendo uma VM

Proteja aplicativos de contêiner usando ferramentas de terceiros

Proteção de dados para aplicativos de contêiner na plataforma de contêiner OpenShift usando a API OpenShift para proteção de dados (OADP)

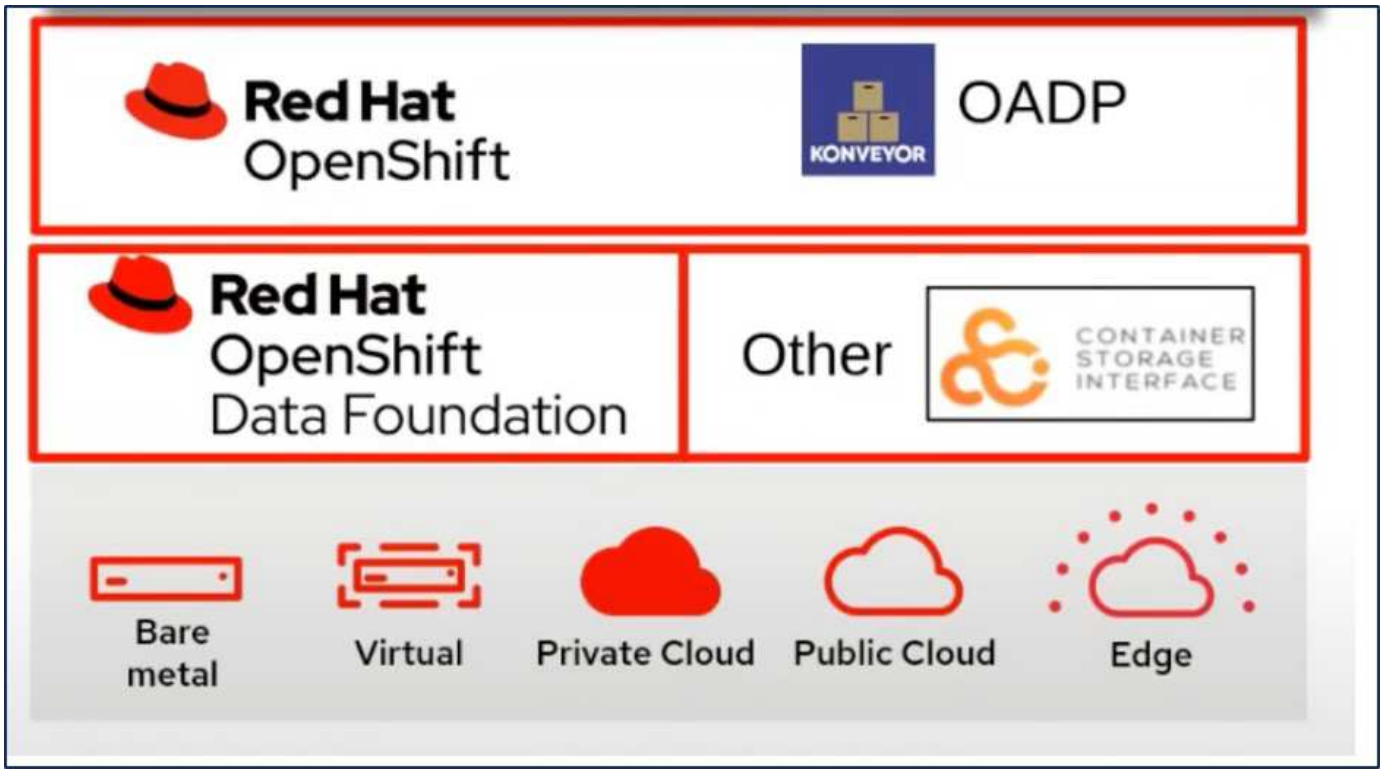
Esta seção do documento de referência fornece detalhes para criar backups de aplicativos de contêiner usando a API OpenShift para proteção de dados (OADP) com o Velero no NetApp ONTAP S3 ou NetApp StorageGRID S3. Os backups de recursos com escopo de namespace, incluindo Volumes Persistentes (PVs) do aplicativo, são criados usando CSI Trident Snapshots.

O storage persistente para aplicativos em contêineres pode ter como suporte o storage do ONTAP integrado ao cluster OpenShift usando "Trident CSI". Nesta seção, usamos "API OpenShift para Proteção de Dados (OADP)" para realizar backup de aplicativos, incluindo seus volumes de dados, para

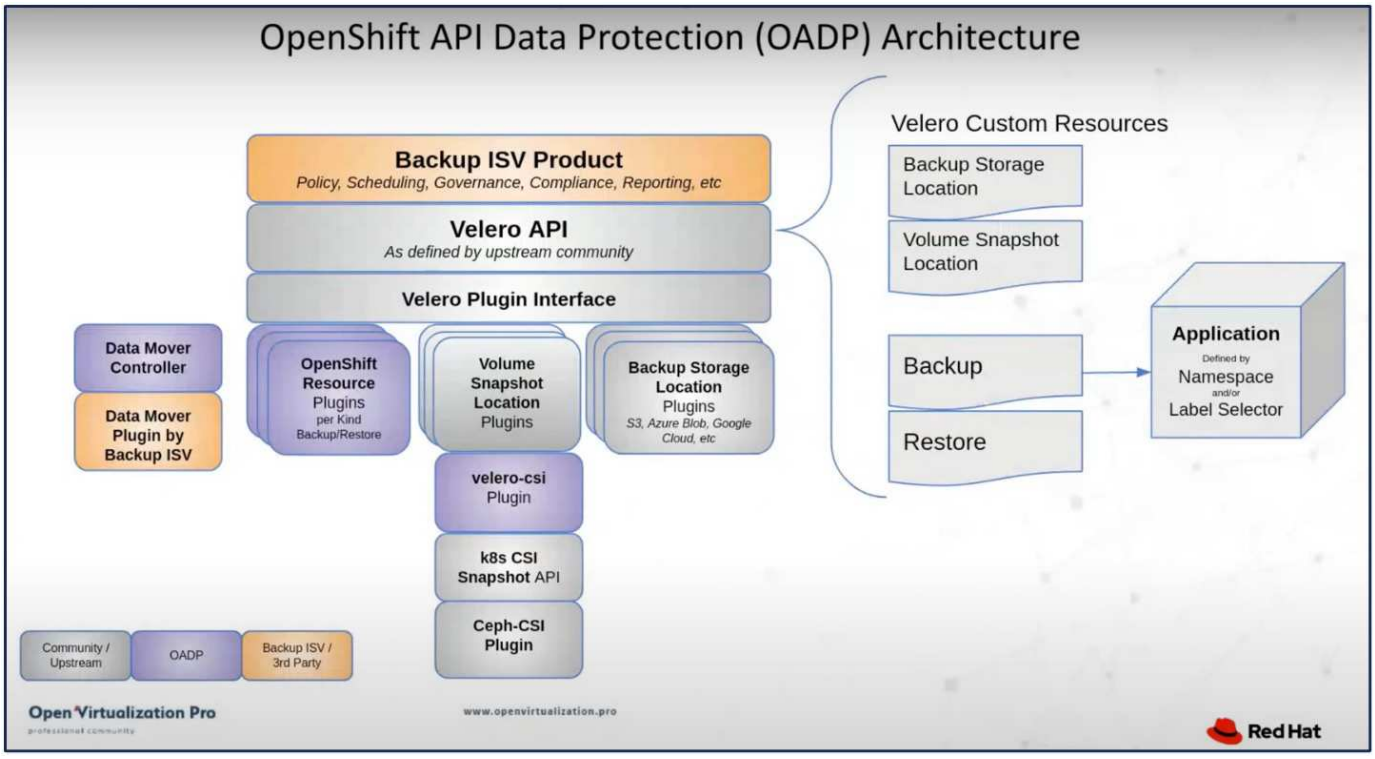
- Armazenamento de objetos ONTAP
- StorageGrid

Em seguida, restauramos a partir do backup quando necessário. Observe que o aplicativo só pode ser restaurado no cluster de onde o backup foi criado.

O OADP permite backup, restauração e recuperação de desastres de aplicativos em um cluster OpenShift. Os dados que podem ser protegidos com OADP incluem objetos de recursos do Kubernetes, volumes persistentes e imagens internas.



O Red Hat OpenShift aproveitou as soluções desenvolvidas pelas comunidades OpenSource para proteção de dados. "Velero" é uma ferramenta de código aberto para fazer backup e restaurar com segurança, executar recuperação de desastres e migrar recursos de cluster e volumes persistentes do Kubernetes. Para usar o Velero facilmente, a OpenShift desenvolveu o operador OADP e o plugin Velero para integração com os drivers de armazenamento CSI. O núcleo das APIs OADP expostas são baseadas nas APIs Velero. Após instalar o operador OADP e configurá-lo, as operações de backup/restauração que podem ser executadas são baseadas nas operações expostas pela API do Velero.



O OADP 1.3 está disponível no hub do operador do cluster OpenShift 4.12 e posteriores. Ele tem um Data Mover integrado que pode mover instantâneos de volume CSI para um armazenamento de objetos remoto. Isso proporciona portabilidade e durabilidade ao mover instantâneos para um local de armazenamento de objetos durante o backup. Os instantâneos ficam então disponíveis para restauração após desastres.

A seguir estão as versões dos vários componentes usados nos exemplos desta seção

- Cluster OpenShift 4.14
- Operador OADP 1.13 fornecido pela Red Hat
- Velero CLI 1.13 para Linux
- Trident 24.02
- ONTAP 9.12
- postgresql instalado usando helm.

"Trident CSI" "API OpenShift para Proteção de Dados (OADP)" "Velero"

Instalação do Operador OpenShift API for Data Protection (OADP)

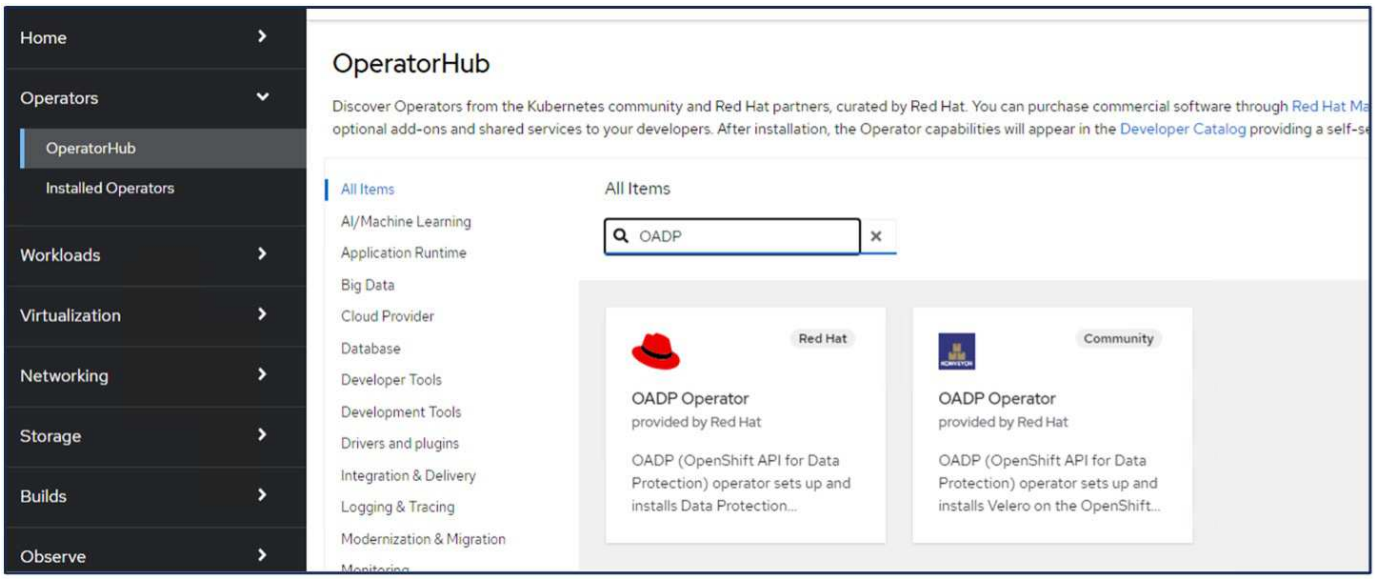
Esta seção descreve a instalação do Operador OpenShift API for Data Protection (OADP).

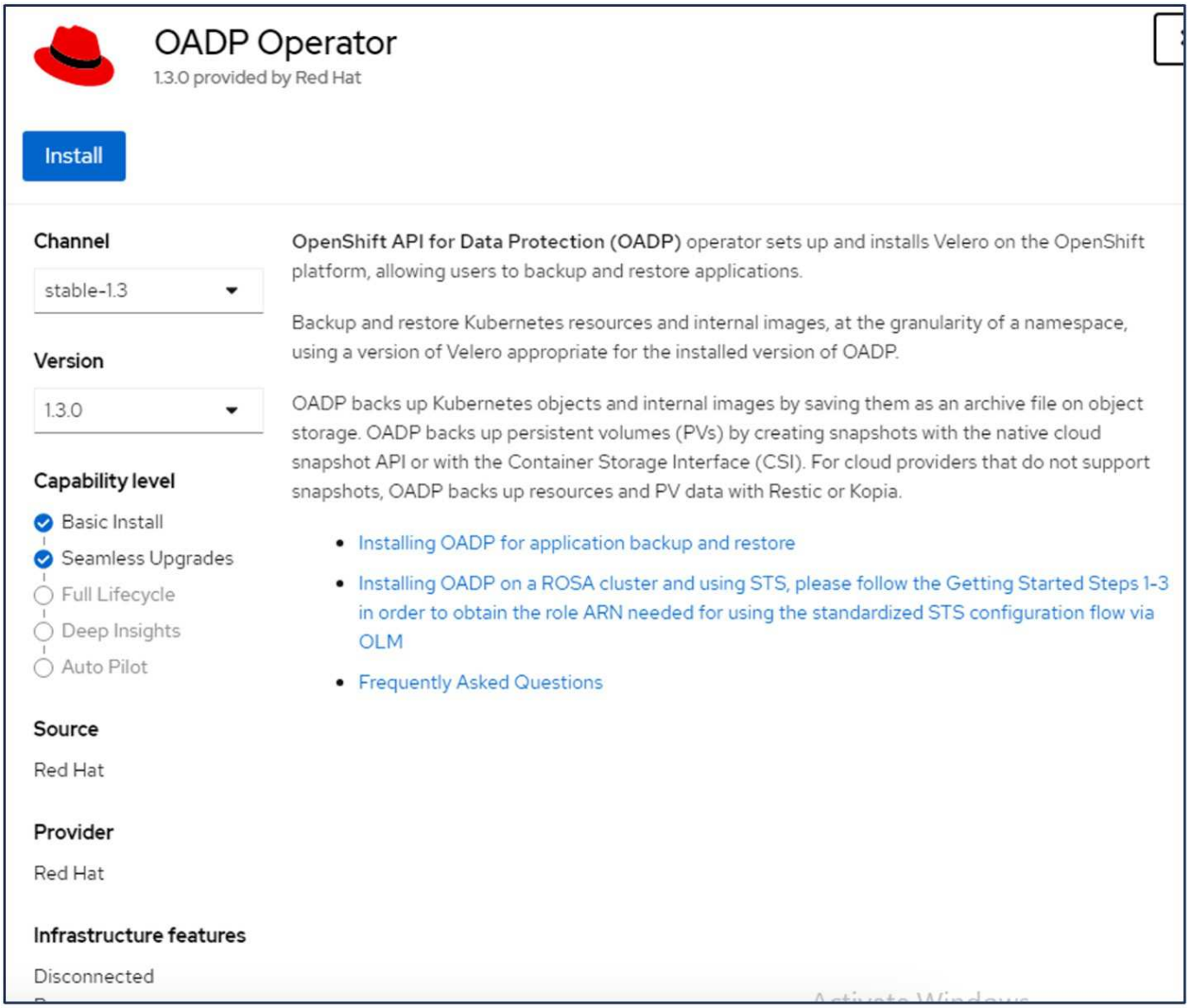
Pré-requisitos

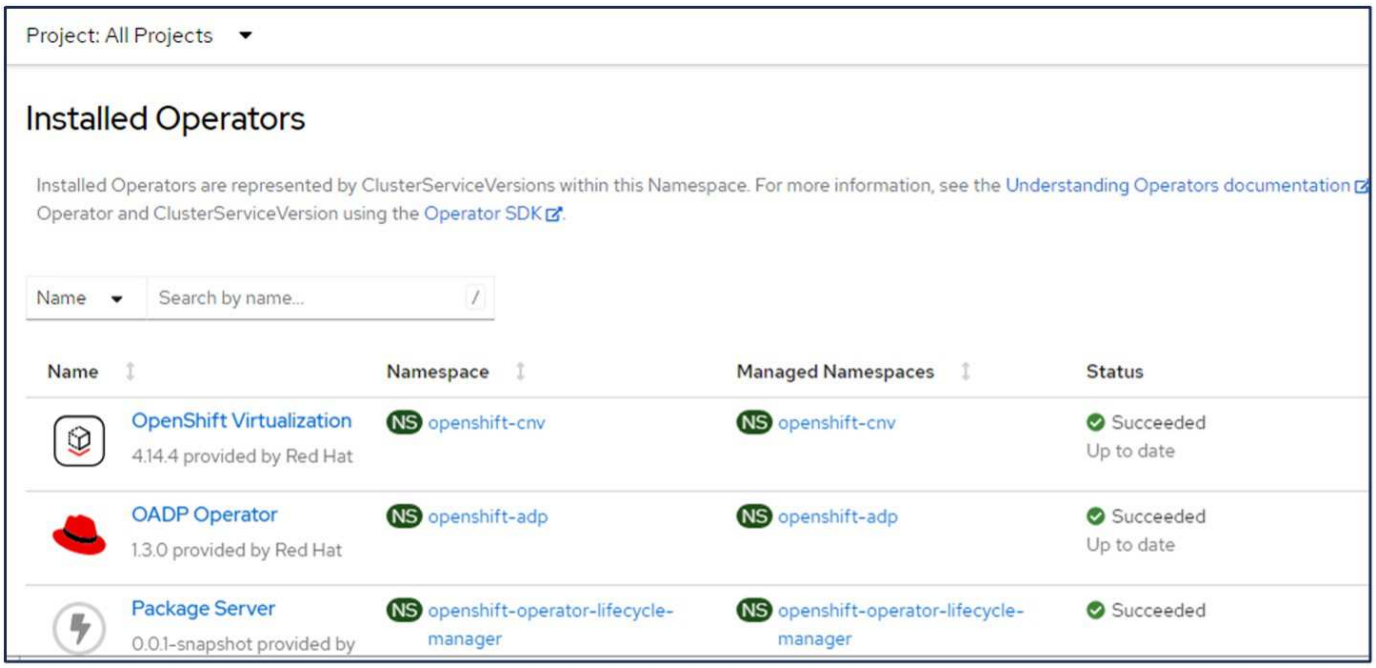
- Um cluster Red Hat OpenShift (posterior à versão 4.12) instalado em infraestrutura bare-metal com nós de trabalho RHCOS
- Um cluster NetApp ONTAP integrado ao cluster usando Trident
- Um backend Trident configurado com um SVM no cluster ONTAP
- Um StorageClass configurado no cluster OpenShift com Trident como provisionador
- Classe Trident Snapshot criada no cluster
- Acesso de administrador de cluster ao cluster Red Hat OpenShift
- Acesso de administrador ao cluster NetApp ONTAP
- Um aplicativo, por exemplo, postgresql implantado no cluster
- Uma estação de trabalho de administração com as ferramentas tridentctl e oc instaladas e adicionadas ao $PATH

Etapas para instalar o operador OADP

1. Acesse o Operator Hub do cluster e selecione o operador Red Hat OADP. Na página Instalar, use todas as seleções padrões e clique em instalar. Na próxima página, use novamente todos os padrões e clique em Instalar. O operador OADP será instalado no namespace openshift-adp.


Home
Operators
OperatorHub
Installed Operators
Workloads
Virtualization
Networking
Storage
Builds
Observe
OperatorHub
Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through Red Hat Ma
optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the Developer Catalog providing a self-se
All Items
AI/Machine Learning
Application Runtime
Big Data
Cloud Provider
Database
Developer Tools
Development Tools
Drivers and plugins
Integration & Delivery
Logging & Tracing
Modernization & Migration
All Items
OADP
Red Hat
OADP Operator
provided by Red Hat
OADP (OpenShift API for Data Protection) operator sets up and installs Data Protection...
Community
OADP Operator
provided by Red Hat
OADP (OpenShift API for Data Protection) operator sets up and installs Velero on the OpenShift...


OADP Operator
1.3.0 provided by Red Hat
Install
Channel
stable-1.3
Version
1.3.0
Capability level
Basic Install
Seamless Upgrades
Full Lifecycle
Deep Insights
Auto Pilot
Source
Red Hat
Provider
Red Hat
Infrastructure features
Disconnected
OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.
Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.
OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.
Installing OADP for application backup and restore
Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM
Frequently Asked Questions



Pré-requisitos para configuração do Velero com detalhes do Ontap S3

Após a instalação bem-sucedida do operador, configure a instância do Velero. O Velero pode ser configurado para usar o Object Storage compatível com S3. Configure o ONTAP S3 usando os procedimentos mostrados no"Seção de gerenciamento de armazenamento de objetos da documentação do ONTAP" . Você precisará das seguintes informações da sua configuração do ONTAP S3 para integrar com o Velero.

- Uma interface lógica (LIF) que pode ser usada para acessar o S3
- Credenciais do usuário para acessar o S3 que incluem a chave de acesso e a chave de acesso secreta
- Um nome de bucket no S3 para backups com permissões de acesso para o usuário
- Para acesso seguro ao armazenamento de objetos, o certificado TLS deve ser instalado no servidor de armazenamento de objetos.

Pré-requisitos para configuração do Velero com detalhes do StorageGrid S3

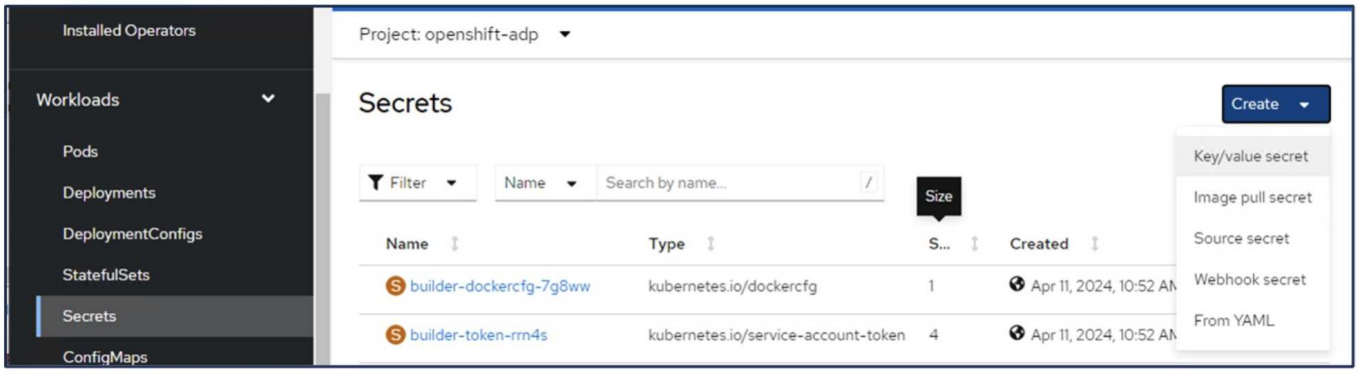
O Velero pode ser configurado para usar o Object Storage compatível com S3. Você pode configurar o StorageGrid S3 usando os procedimentos mostrados no"Documentação do StorageGrid" . Você precisará das seguintes informações da configuração do StorageGrid S3 para integrar com o Velero.

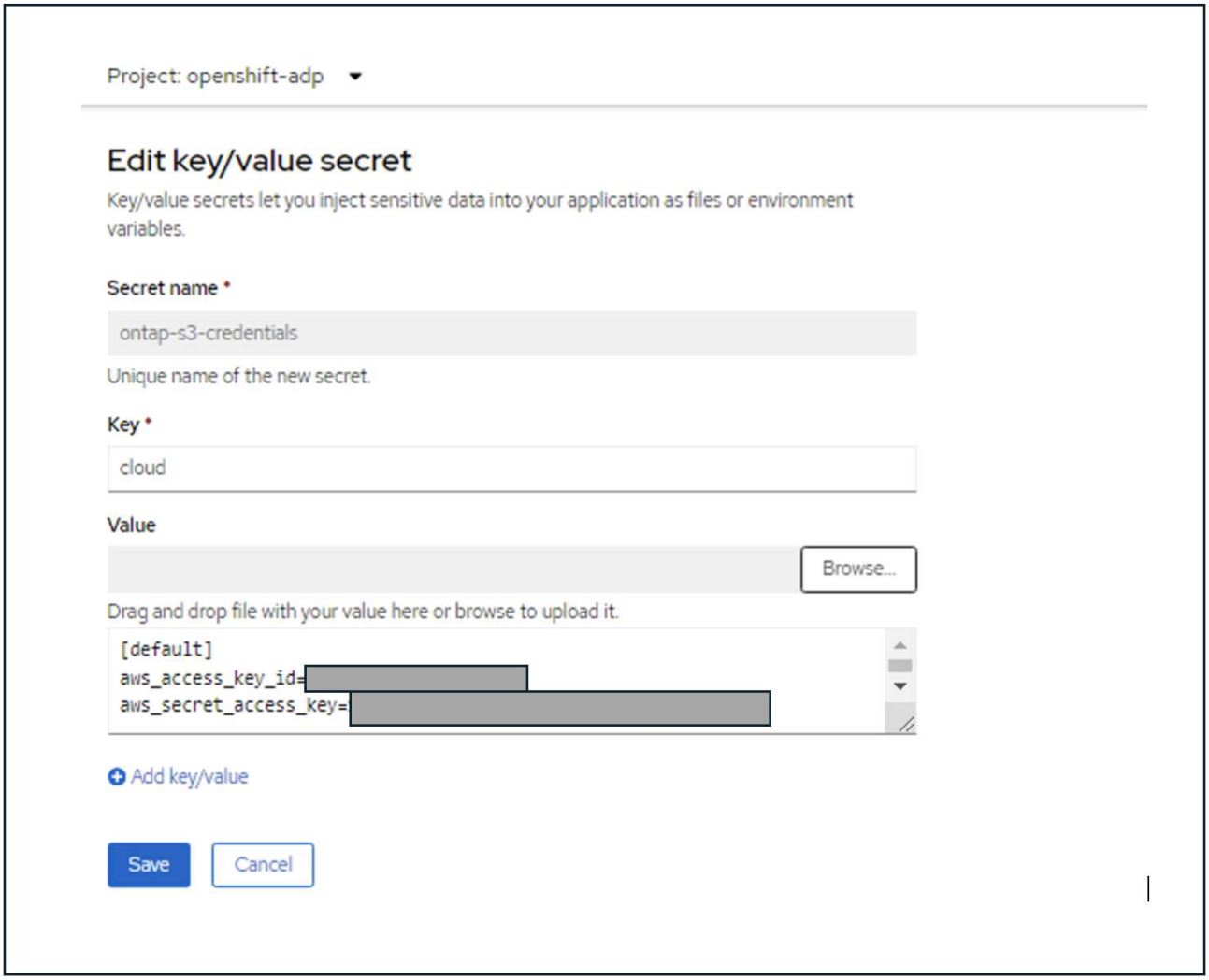
- O ponto de extremidade que pode ser usado para acessar o S3
- Credenciais do usuário para acessar o S3 que incluem a chave de acesso e a chave de acesso secreta
- Um nome de bucket no S3 para backups com permissões de acesso para o usuário
- Para acesso seguro ao armazenamento de objetos, o certificado TLS deve ser instalado no servidor de armazenamento de objetos.

Etapas para configurar o Velero

- Primeiro, crie um segredo para uma credencial de usuário do ONTAP S3 ou credenciais de usuário do StorageGrid Tenant. Isso será usado para configurar o Velero mais tarde. Você pode criar um segredo a partir da CLI ou do console da web. Para criar um segredo no console da web, selecione Segredos e clique em Segredo de chave/valor. Forneça os valores para o nome da credencial, a chave e o valor, conforme mostrado. Certifique-se de usar o ID da chave de acesso e a chave de acesso secreta do seu

usuário do S3. Dê um nome apropriado ao segredo. No exemplo abaixo, um segredo com credenciais de usuário do ONTAP S3 chamado ontap-s3-credentials é criado.





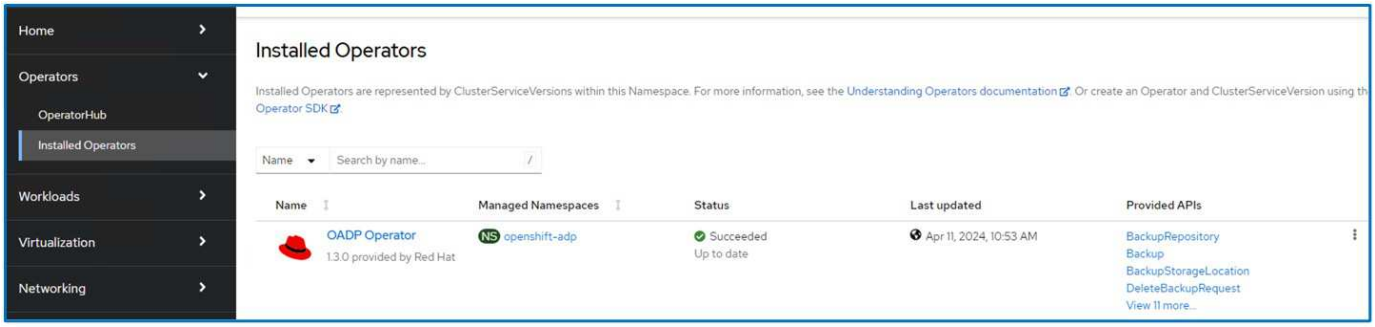
Para criar um segredo chamado sg-s3-credentials na CLI, você pode usar o seguinte comando.

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt

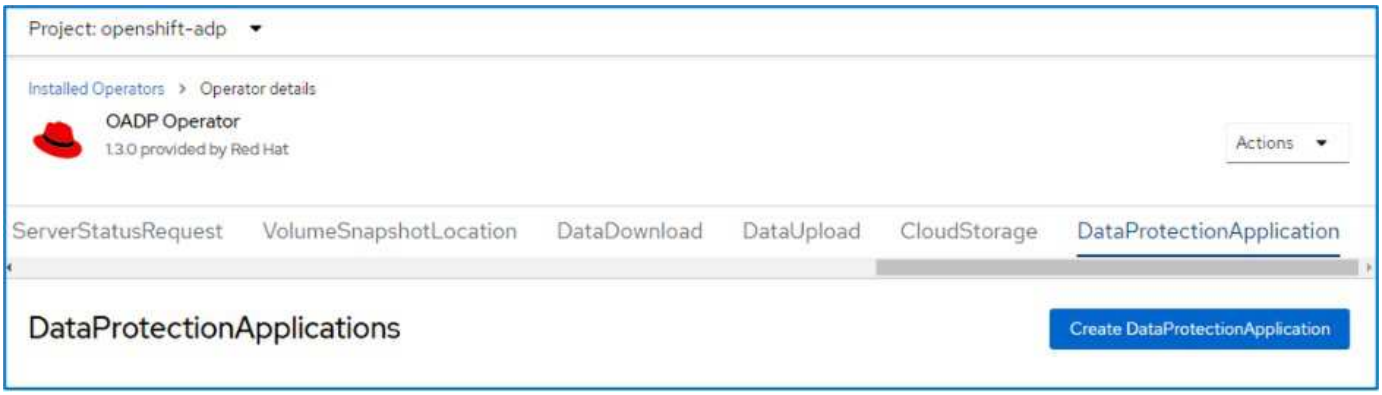
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3
user in the following format:

[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- Em seguida, para configurar o Velero, selecione Operadores instalados no item de menu em Operadores, clique no operador OADP e selecione a guia **DataProtectionApplication**.



Clique em Criar DataProtectionApplication. Na visualização de formulário, forneça um nome para o aplicativo DataProtection ou use o nome padrão.



Agora vá para a visualização YAML e substitua as informações de especificação conforme mostrado nos exemplos de arquivo yaml abaixo.

Arquivo yaml de exemplo para configurar o Velero com o ONTAP S3 como backupLocation

```
spec:
  backupLocations:
    - velero:
        config:
```

```
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'  ->This allows use of IP in s3URL
          s3Url: 'https://10.61.181.161' ->Ensure TLS certificate for S3
is configured
        credential:
          key: cloud
          name: ontap-s3-credentials -> previously created secret
        default: true
        objectStorage:
          bucket: velero -> Your bucket name previously created in S3 for
backups
          prefix: container-demo-backup ->The folder that will be created
in the bucket
          caCert: <base64 encoded CA Certificate installed on ONTAP
Cluster with the SVM Scope where the bucker exists>
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
      #default Data Mover uses Kopia to move snapshots to Object Storage
    velero:
      defaultPlugins:
        - csi ->This plugin to use CSI snapshots
        - openshift
        - aws
        - kubevirt -> This plugin to use Velero with OIpenShift
Virtualization
```

Arquivo yaml de exemplo para configurar o Velero com o StorageGrid S3 como backupLocation

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
```

```
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

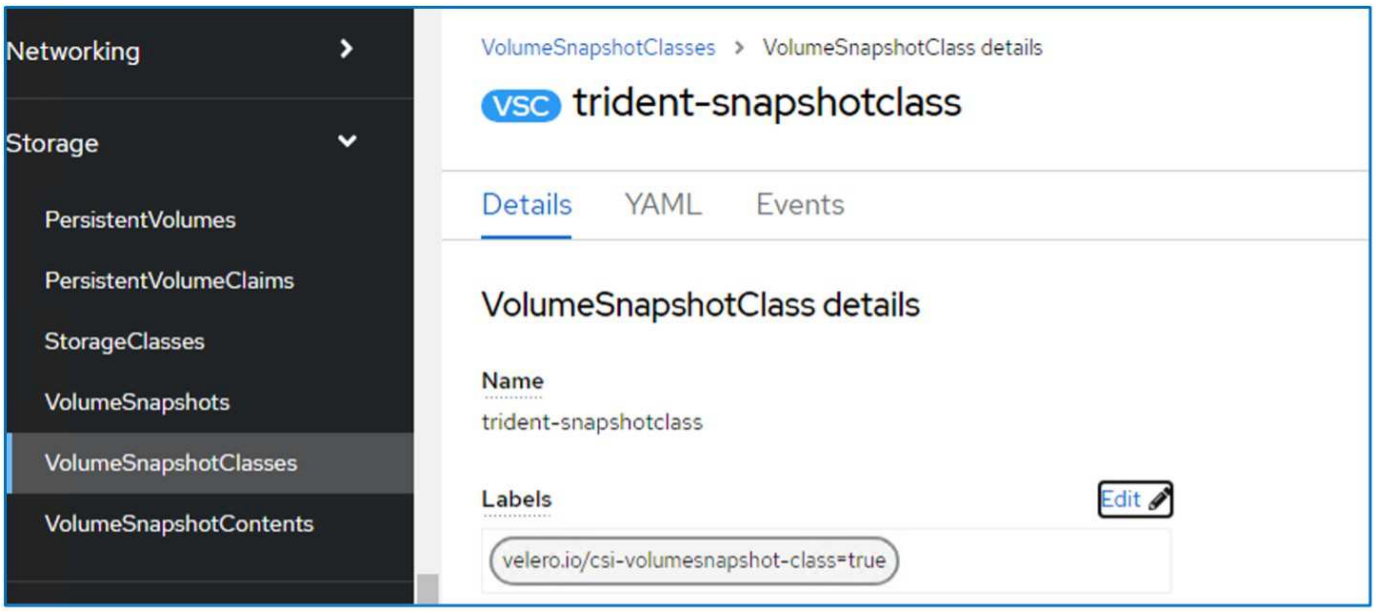
A seção de especificações no arquivo yaml deve ser configurada apropriadamente para os seguintes parâmetros, semelhante ao exemplo acima

backupLocations ONTAP S3 ou StorageGrid S3 (com suas credenciais e outras informações conforme mostrado no yaml) é configurado como o BackupLocation padrão para o velero.

snapshotLocations Se você usar snapshots da Container Storage Interface (CSI), não precisará especificar um local de snapshot porque você criará um VolumeSnapshotClass CR para registrar o driver CSI. Em nosso exemplo, você usa o Trident CSI e criou anteriormente o VolumeSnapShotClass CR usando o driver Trident CSI.

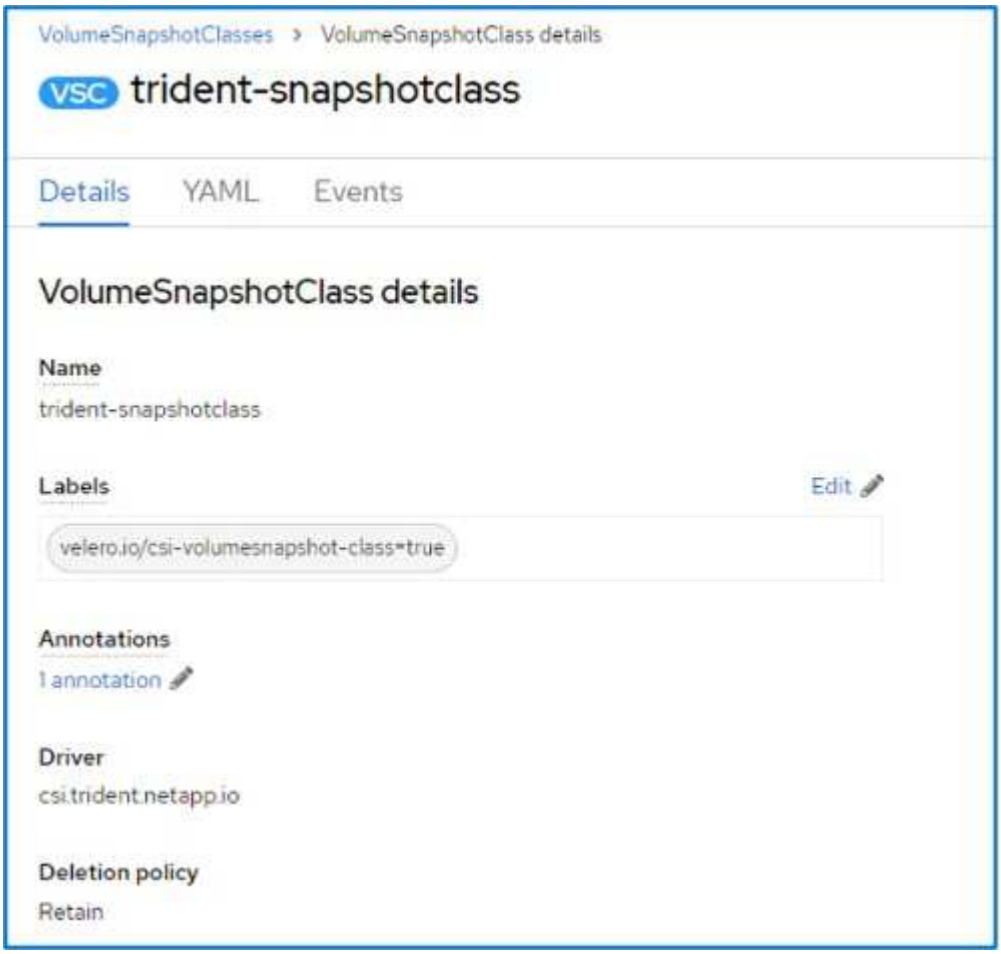
Habilitar plugin CSI Adicione csi aos defaultPlugins para que o Velero faça backup de volumes persistentes com snapshots CSI. Os plug-ins Velero CSI, para fazer backup de PVCs com suporte a CSI, escolherão o VolumeSnapshotClass no cluster que tem o rótulo **velero.io/csi-volumesnapshot-class** definido. Por esta

- Você deve ter o trident VolumeSnapshotClass criado.
- Edite o rótulo da classe trident-snapshot e defina-o como **velero.io/csi-volumesnapshot-class=true** conforme mostrado abaixo.

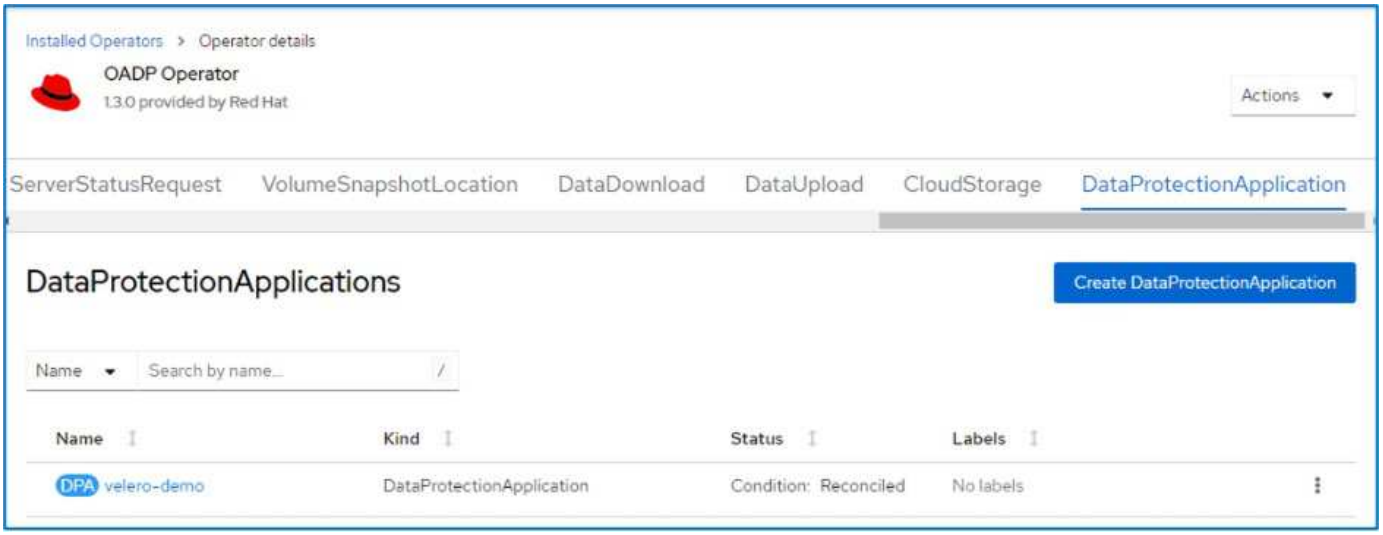


Garanta que os snapshots possam persistir mesmo se os objetos VolumeSnapshot forem excluídos. Isso pode ser feito definindo **deletionPolicy** como Retain. Caso contrário, a exclusão de um namespace perderá completamente todos os PVCs já armazenados em backup nele.

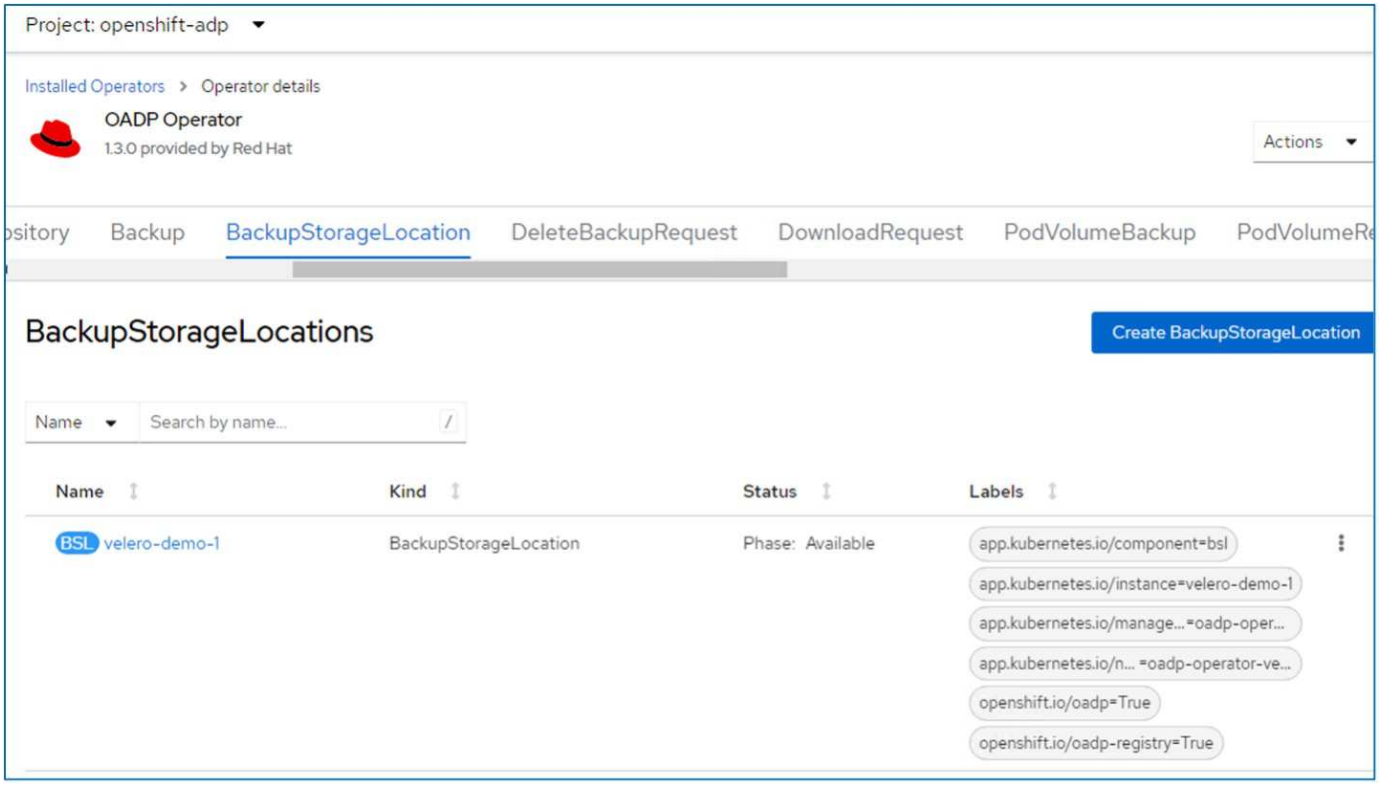
```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```



Certifique-se de que o DataProtectionApplication foi criado e está na condição:Reconciliado.



O operador OADP criará um BackupStorageLocation correspondente. Ele será usado ao criar um backup.



Criação de backup sob demanda para aplicativos no OpenShift Container Platform

Esta seção descreve como criar backup sob demanda para VMs no OpenShift Virtualization.

Etapas para criar um backup de um aplicativo

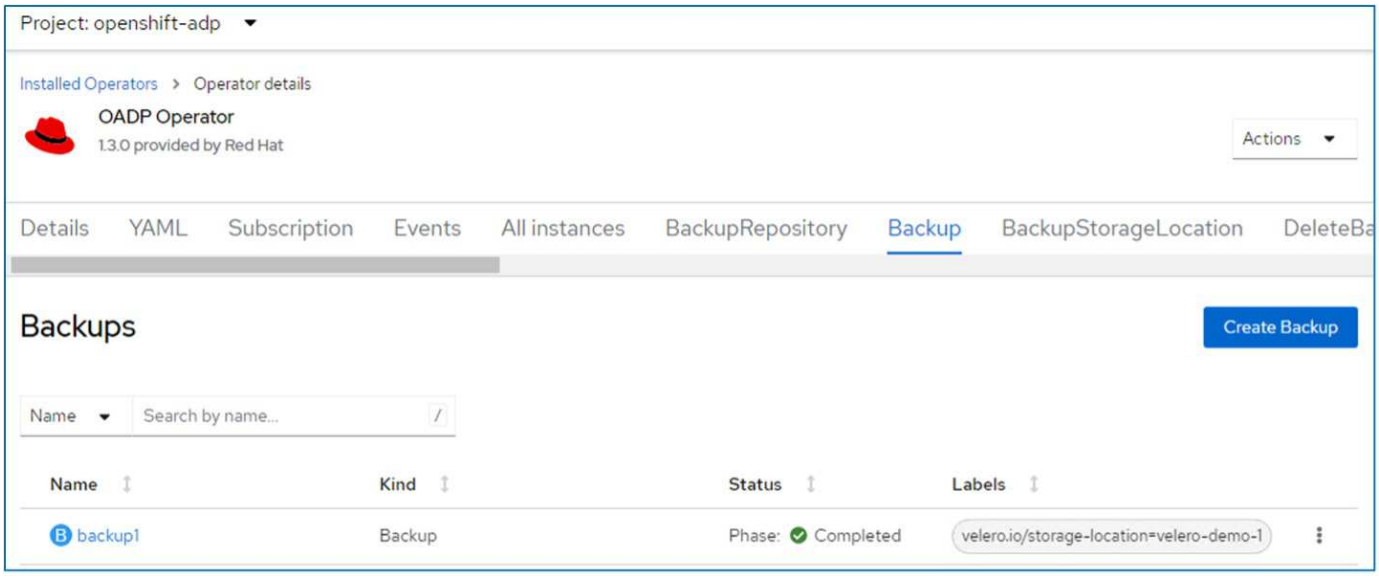
Para criar um backup sob demanda de um aplicativo (metadados do aplicativo e volumes persistentes do aplicativo), clique na guia **Backup** para criar um Recurso Personalizado (CR) de Backup. Um exemplo de arquivo YAML é fornecido para criar o CR de Backup. Usando este arquivo YAML, será feito backup do aplicativo e do seu storage persistente no namespace especificado. Parâmetros adicionais podem ser definidos, conforme mostrado no "documentação".

Um instantâneo dos volumes persistentes e dos recursos do aplicativo no namespace especificado será criado pelo CSI. Este instantâneo será armazenado no local de backup especificado no yaml. O backup permanecerá no sistema por 30 dias, conforme especificado no ttl.

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql ->namespace of the app
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: false
  storageLocation: velero-container-backup-ontap-1 -->this is the
backupStorageLocation previously created when Velero is configured.
```

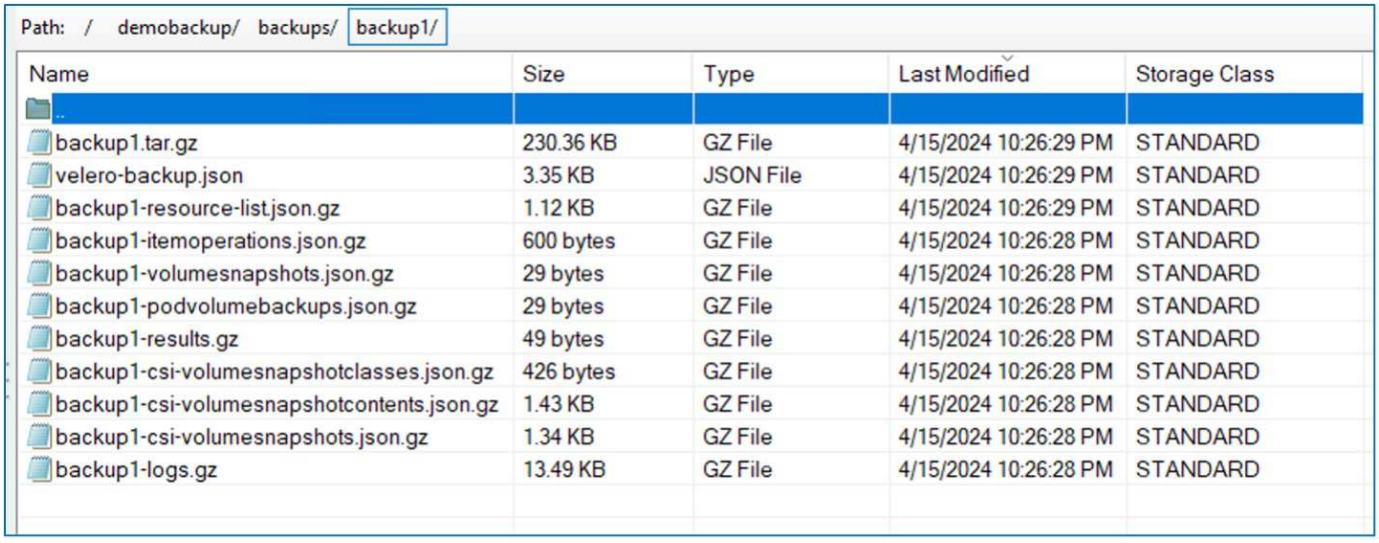
```
  ttl: 720h0m0s
```

Quando o backup for concluído, sua Fase será exibida como concluída.



Você pode inspecionar o backup no armazenamento de objetos com a ajuda de um aplicativo de navegador S3. O caminho do backup aparece no bucket configurado com o nome do prefixo (velero/container-demo-backup). Você pode ver que o conteúdo do backup inclui instantâneos de volume, logs e outros metadados do aplicativo.

No StorageGrid, você também pode usar o console S3 disponível no Tenant Manager para visualizar os objetos de backup.



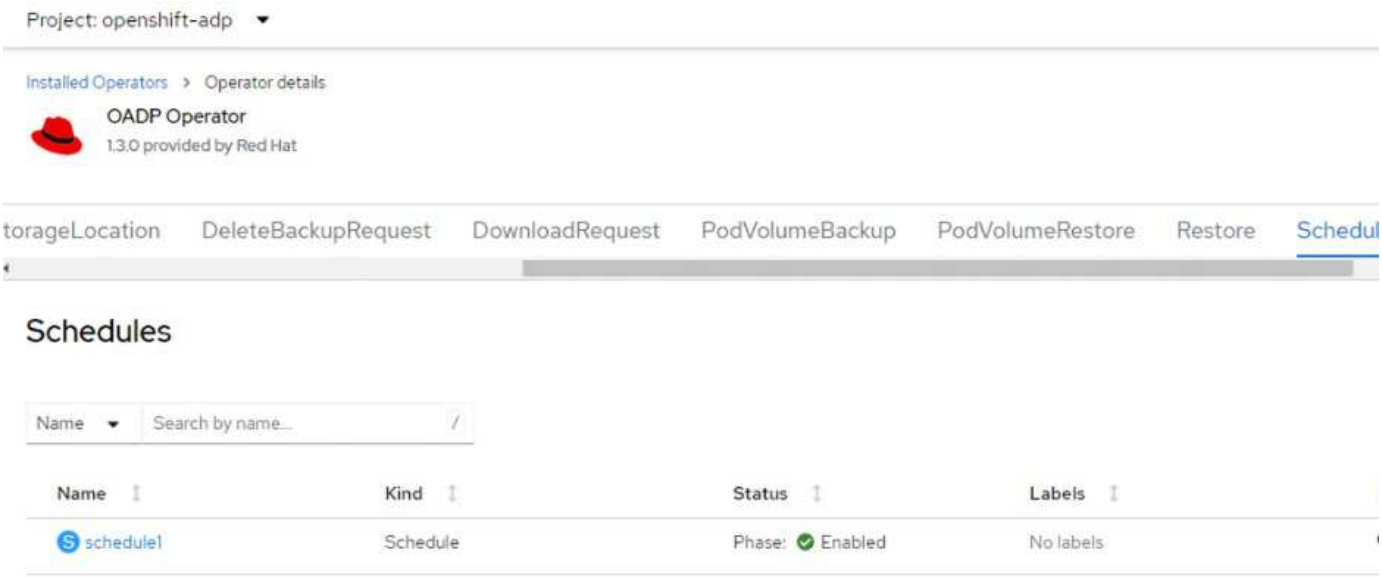
Criação de backups agendados para aplicativos

Para criar backups agendados, você precisa criar uma CR agendada. O agendamento é simplesmente uma expressão Cron que permite que você especifique o horário em que deseja criar o backup. Um exemplo de yaml para criar um Schedule CR é mostrado abaixo.

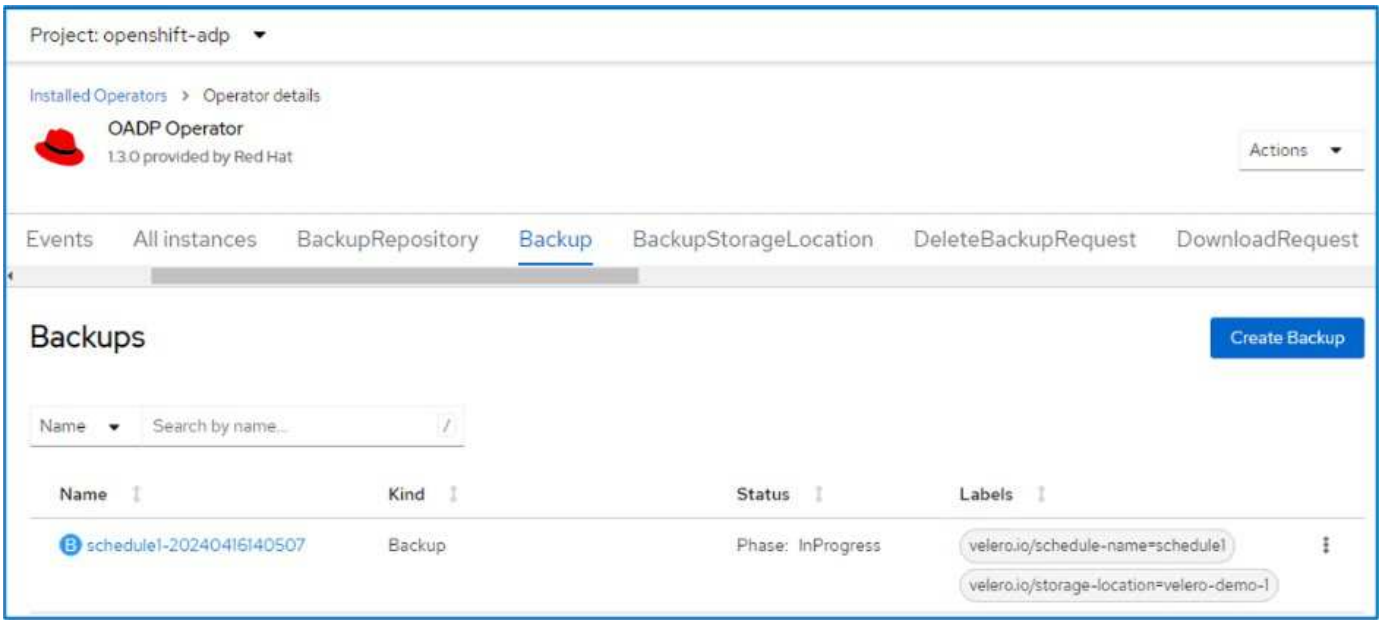
```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: schedule1
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    includedNamespaces:
      - postgresql
    storageLocation: velero-container-backup-ontap-1
```

A expressão Cron 0 7 * * * significa que um backup será criado às 7:00 todos os dias. Os namespaces a serem incluídos no backup e o local de armazenamento do backup também são especificados. Então, em vez de um CR de backup, o CR agendado é usado para criar um backup no horário e na frequência especificados.

Depois que o agendamento for criado, ele será habilitado.



Os backups serão criados de acordo com esta programação e podem ser visualizados na aba Backup.



Migrar um aplicativo de um cluster para outro

Os recursos de backup e restauração do Velero o tornam uma ferramenta valiosa para migrar seus dados entre clusters. Esta seção descreve como migrar aplicativos de um cluster para outro criando um backup do aplicativo no Armazenamento de objetos de um cluster e, em seguida, restaurando o aplicativo do mesmo armazenamento de objetos para outro cluster. .

▼ **Backup do primeiro cluster**

Pré-requisitos no Cluster 1

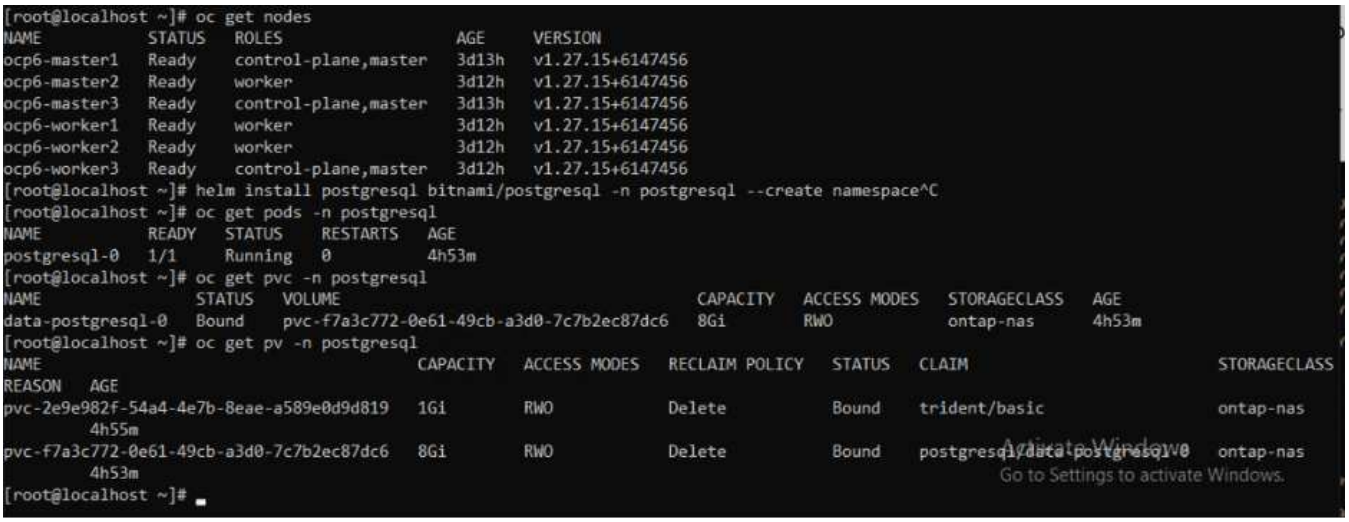
- O Trident deve ser instalado no cluster.
- Um backend trident e uma classe de armazenamento devem ser criados.
- O operador OADP deve ser instalado no cluster.
- O DataProtectionApplication deve ser configurado.

Use a seguinte especificação para configurar o objeto DataProtectionApplication.

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false'
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'true'
          s3Url: 'https://10.61.181.161'
        credential:
          key: cloud
          name: ontap-s3-credentials
```

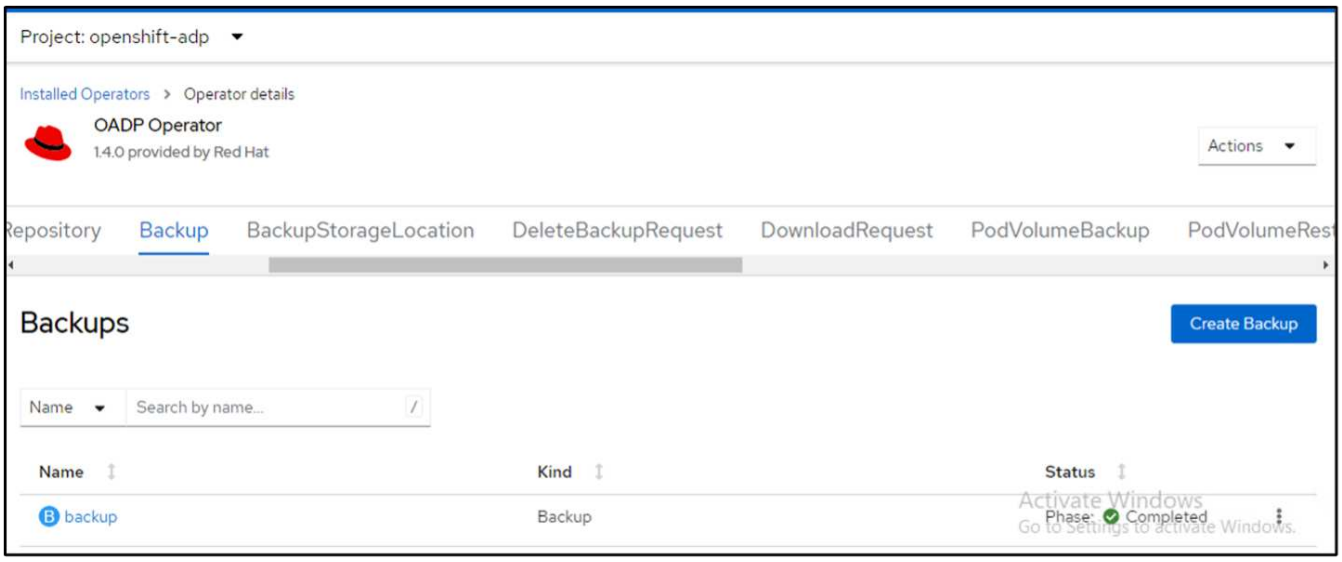
```
        default: true
        objectStorage:
          bucket: velero
          caCert: <base-64 encoded tls certificate>
          prefix: container-backup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

- Crie um aplicativo no cluster e faça um backup desse aplicativo. Por exemplo, instale um aplicativo postgres.



- Use a seguinte especificação para o CR de backup:

```
spec:
  csiSnapshotTimeout: 10m0s
  defaultVolumesToFsBackup: false
  includedNamespaces:
    - postgresql
  itemOperationTimeout: 4h0m0s
  snapshotMoveData: true
  storageLocation: velero-sample-1
  ttl: 720h0m0s
```



Você pode clicar na aba **Todas as instâncias** para ver os diferentes objetos sendo criados e passando por diferentes fases até finalmente chegar à fase de backup **concluído**.

Um backup dos recursos no namespace postgresql será armazenado no local de armazenamento de objetos (ONTAP S3) especificado em backupLocation na especificação OADP.

▼ **Restaurar para um segundo cluster**

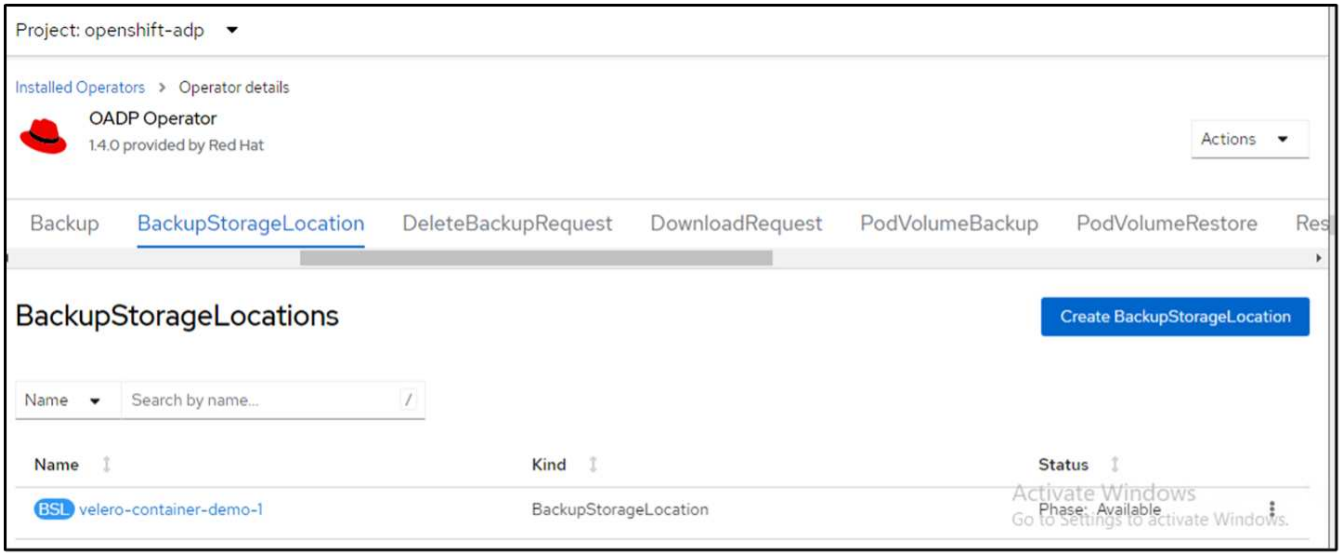
Pré-requisitos no Cluster 2

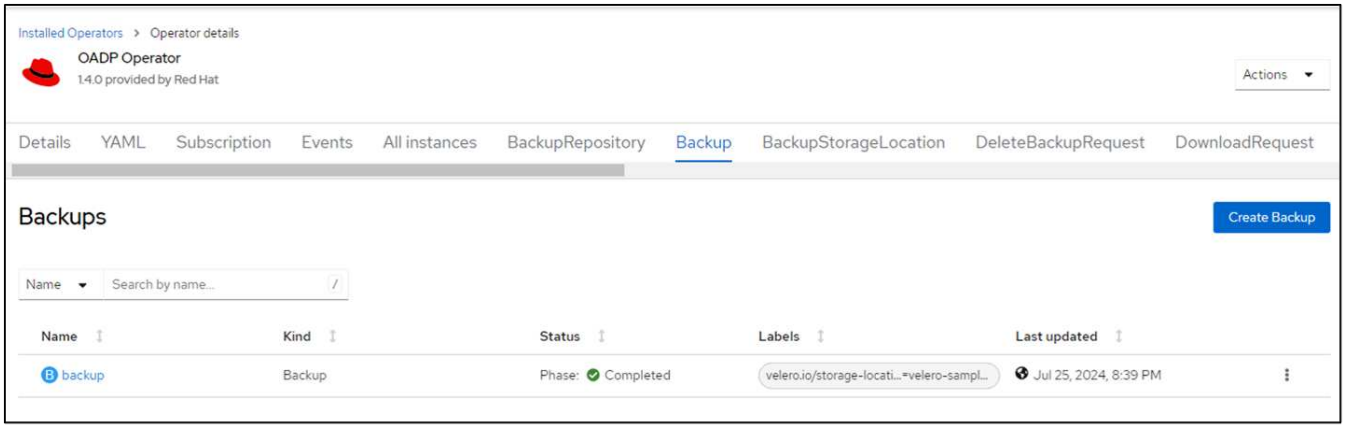
- O Trident deve ser instalado no cluster 2.
- O aplicativo postgresql NÃO deve estar instalado no namespace postgresql.
- O operador OADP deve ser instalado no cluster 2, e o BackupStorage Location deve apontar para o mesmo local de armazenamento de objetos onde o backup foi armazenado do primeiro cluster.
- O CR de backup deve estar visível no segundo cluster.

```
[root@localhost ~]# oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-controller-6799cfb77f-8rzvk   6/6     Running   6          2d7h
trident-node-linux-7wvjz            2/2     Running   2          2d7h
trident-node-linux-8vvm2            2/2     Running   0          2d7h
trident-node-linux-bgs6f            2/2     Running   2          2d7h
trident-node-linux-njwb8            2/2     Running   0          2d7h
trident-node-linux-scqjl            2/2     Running   0          2d7h
trident-node-linux-swr69            2/2     Running   2          2d7h
trident-operator-b88b86fc8-7fk68    1/1     Running   1          2d7h
[root@localhost ~]#
```

```
[root@localhost ~]# oc get nodes
NAME           STATUS   ROLES                  AGE   VERSION
ocp7-master1   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master2   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-master3   Ready    control-plane,master   3d    v1.27.15+6147456
ocp7-worker1   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker2   Ready    worker                 3d    v1.27.15+6147456
ocp7-worker3   Ready    worker                 3d    v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pvc -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pv -n postgresql
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                STORAGECLASS   REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic        ontap-nas               11m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc     vsphere-sc              2d7
h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.



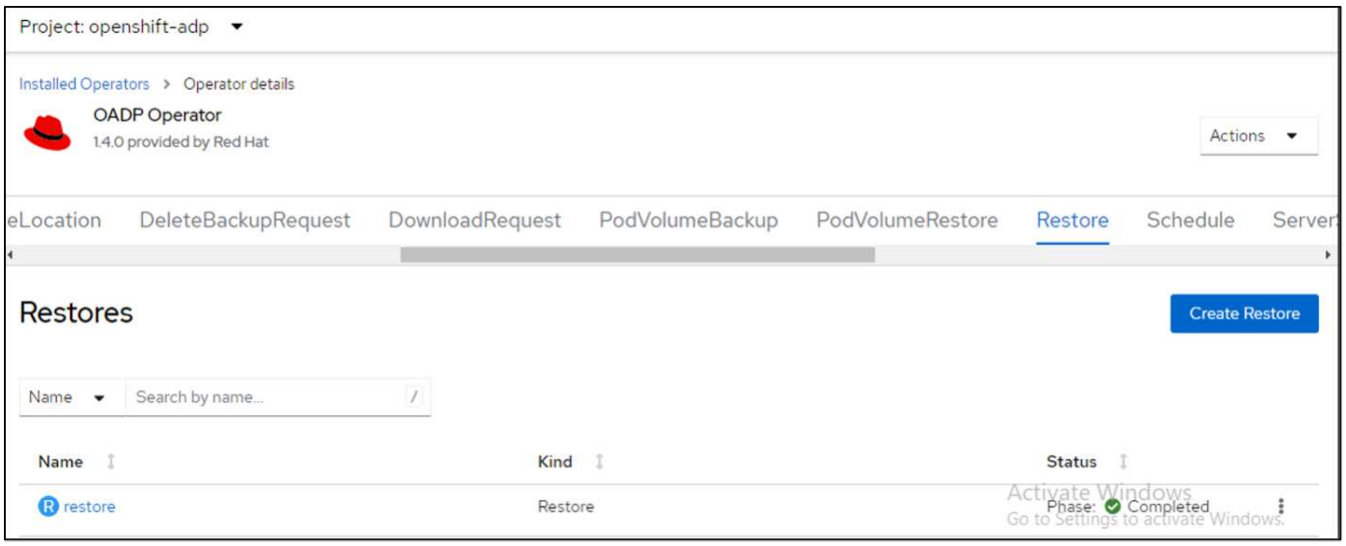


Restaure o aplicativo neste cluster a partir do backup. Use o seguinte yaml para criar o Restore CR.

```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
```

```
  backupName: backup
  restorePVs: true
```

Quando a restauração estiver concluída, você verá que o aplicativo postgresql está em execução neste cluster e está associado ao pvc e a um pv correspondente. O estado do aplicativo é o mesmo de quando o backup foi feito.




```
[root@localhost ~]# export KUBECONFIG=ocp-cluster7/kubeconfig-ocp-cluster7
[root@localhost ~]# oc get nodes
NAME          STATUS   ROLES                  AGE    VERSION
ocp7-master1  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master2  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-master3  Ready    control-plane,master   3d3h   v1.27.15+6147456
ocp7-worker1  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker2  Ready    worker                 3d3h   v1.27.15+6147456
ocp7-worker3  Ready    worker                 3d3h   v1.27.15+6147456
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          31m
[root@localhost ~]# oc get pvc -n postgresql
NAME                 STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0    Bound    pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            ontap-nas      31m
[root@localhost ~]# oc get pv
NAME                                       CAPACITY   ACCESS MODES   RECLAIM POLICY   STATUS   CLAIM                          STORAGECLASS
REASON   AGE
pvc-c6660630-0cfe-484b-aaa3-5ada54c8b9a7   1Gi        RWO            Delete           Bound    trident/basic                  ontap-nas
         3h27m
pvc-ce7044e3-2ba5-4934-8bad-553fa7d35128   8Gi        RWO            Delete           Bound    postgresql/data-postgresql-0   ontap-nas
         31m
pvc-edcc6551-81b0-40b4-8547-e9df70c1740d   10Gi       RWO            Delete           Bound    default/test-pvc               vsphere-sc
         2d10h
[root@localhost ~]#
```

Activate Windows
Go to Settings to activate Windows.

Restaurar um aplicativo a partir de um backup

Esta seção descreve como restaurar aplicativos de um backup.

Pré-requisitos

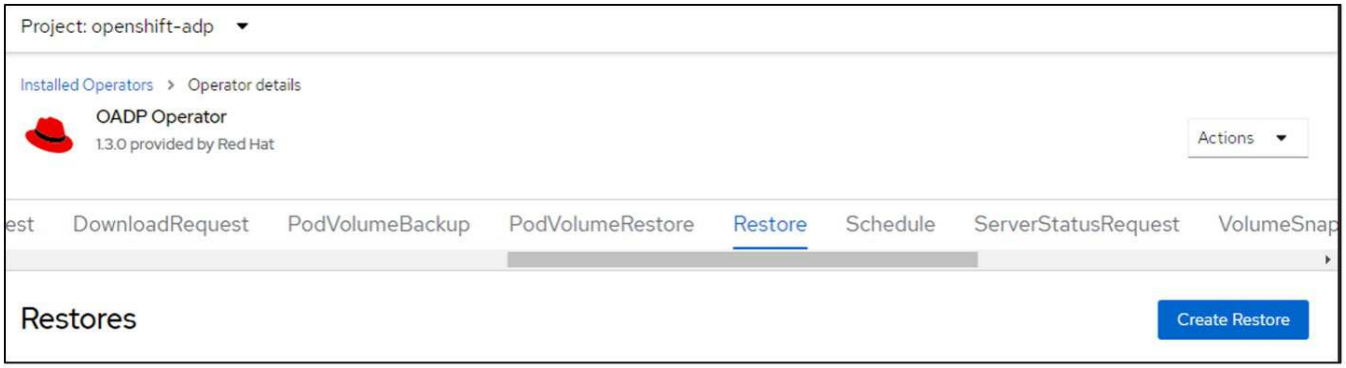
Para restaurar a partir de um backup, vamos supor que o namespace onde o aplicativo existia foi excluído acidentalmente.

```
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          102s
[root@localhost ~]# oc delete ns postgresql
namespace "postgresql" deleted

[root@localhost ~]#
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]#
```

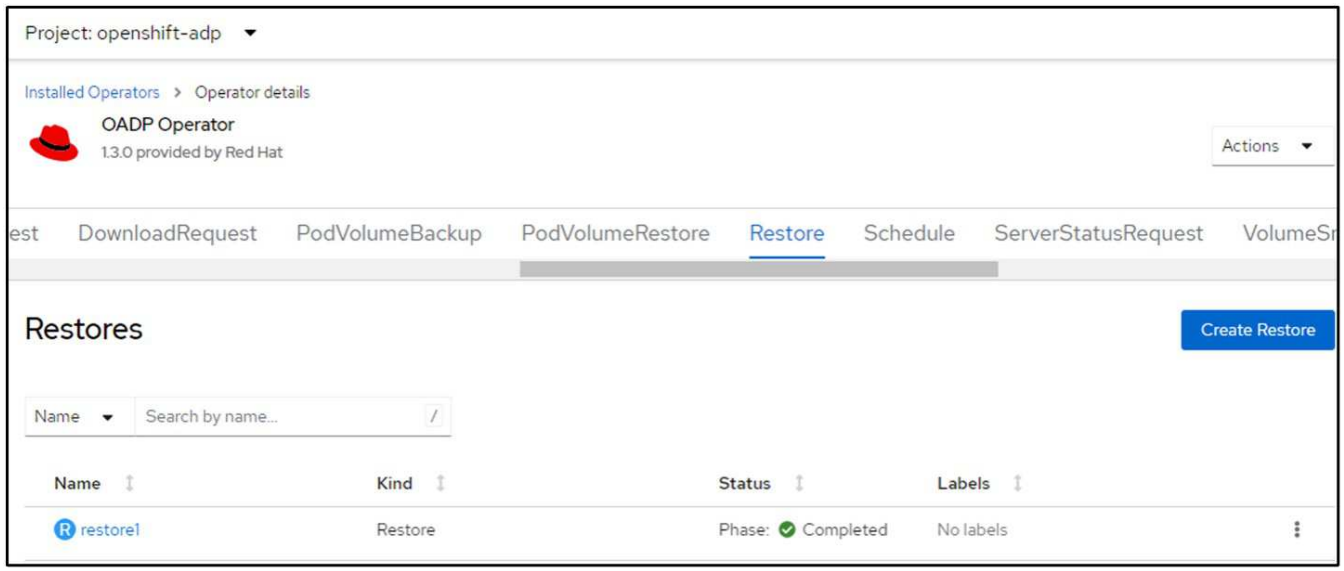
▼ **Restaurar para o mesmo namespace**

Para restaurar a partir do backup que acabamos de criar, precisamos criar um Recurso Personalizado de Restauração (CR). Precisamos fornecer um nome para ele, o nome do backup do qual queremos restaurar e definir o parâmetro restorePVs como true. Parâmetros adicionais podem ser definidos como mostrado em "documentação". Clique no botão Create.




```
apiVersion: velero.io/v1
kind: Restore
apiVersion: velero.io/v1
metadata:
  name: restore
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
  restorePVs: true
```

Quando a fase for exibida como concluída, você poderá ver que o aplicativo foi restaurado ao estado em que o instantâneo foi tirado. O aplicativo é restaurado para o mesmo namespace.




```
[root@localhost ~]#
[root@localhost ~]# oc get pods -n postgresql
No resources found in postgresql namespace.
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS              RESTARTS   AGE
postgresql-0   0/1     ContainerCreating   0          16s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          22s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   0/1     Running   0          29s
[root@localhost ~]# oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          37s
[root@localhost ~]#
```

▼ **Restaurar para um namespace diferente**

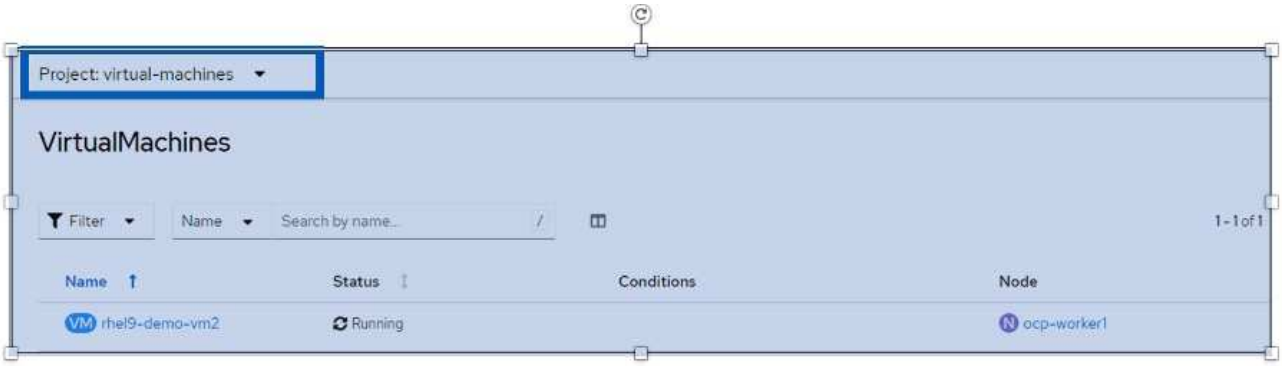
Para restaurar o aplicativo para um namespace diferente, você pode fornecer um namespaceMapping na definição yaml do CR de restauração.

O arquivo yaml de exemplo a seguir cria um CR de restauração para restaurar um aplicativo e seu armazenamento persistente do namespace postgresql para o novo namespace postgresql-restored.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup-postgresql-ontaps3
```

```
  restorePVs: true
  includedNamespaces:
  - postgresql
  namespaceMapping:
    postgresql: postgresql-restored
```

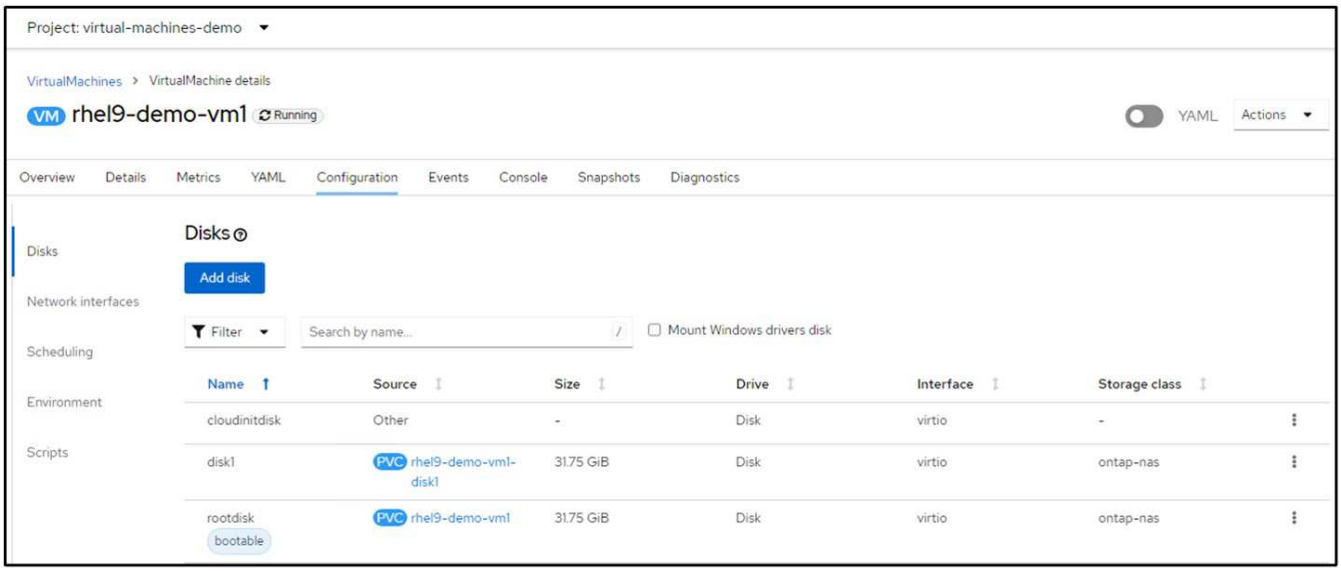
Quando a fase for exibida como concluída, você poderá ver que o aplicativo foi restaurado ao estado em que o instantâneo foi tirado. O aplicativo é restaurado para um namespace diferente, conforme especificado no yaml.

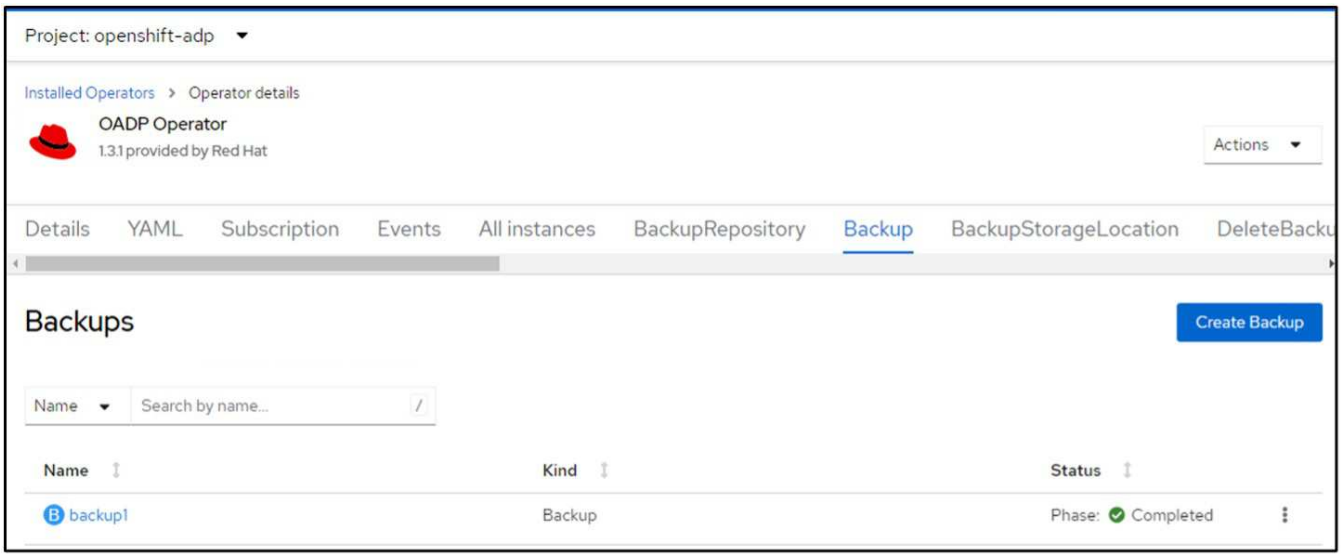


▼ **Restaurar para uma classe de armazenamento diferente**

O Velero fornece uma capacidade genérica de modificar os recursos durante a restauração especificando patches json. Os patches json são aplicados aos recursos antes de serem restaurados. Os patches json são especificados em um configmap e o configmap é referenciado no comando restore. Este recurso permite que você restaure usando diferentes classes de armazenamento.

No exemplo abaixo, o aplicativo, durante a implantação, usa ontap-nas como classe de armazenamento para seus volumes persistentes. Um backup do aplicativo chamado backup-postgresql-ontaps3 é criado.





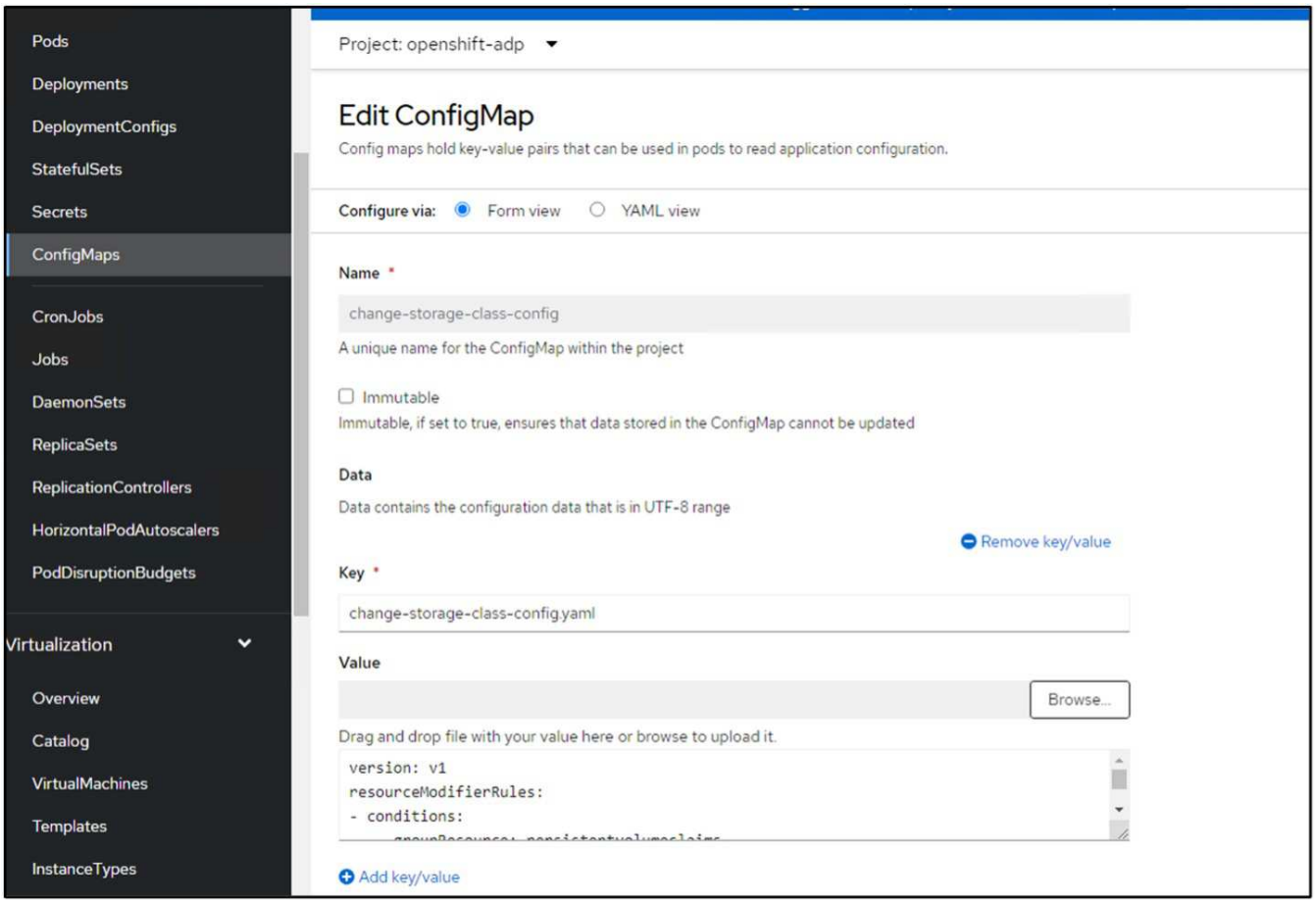
Simule a perda do aplicativo desinstalando-o.

Para restaurar a VM usando uma classe de armazenamento diferente, por exemplo, classe de armazenamento ontap-nas-eco, você precisa seguir estas duas etapas:

Passo 1

Crie um mapa de configuração (console) no namespace openshift-adp da seguinte maneira: Preencha os detalhes conforme mostrado na captura de tela: Selecione o namespace: openshift-adp Nome: change-ontap-sc (pode ser qualquer nome) Chave: change-ontap-sc-config.yaml: Valor:

```
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "data-postgresql*"
     namespaces:
     - postgresql
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"
```



O objeto do mapa de configuração resultante deve ter esta aparência (CLI):

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:         change-storage-class-config
Namespace:    openshift-adp
Labels:       velero.io/change-storage-class=RestoreItemAction
              velero.io/plugin-config=
Annotations:  <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
     groupResource: persistentvolumeclaims
     resourceNameRegex: "^rhel*"
     namespaces:
     - virtual-machines-demo
  patches:
  - operation: replace
    path: "/spec/storageClassName"
    value: "ontap-nas-eco"


BinaryData
====

Events:  <none>
```

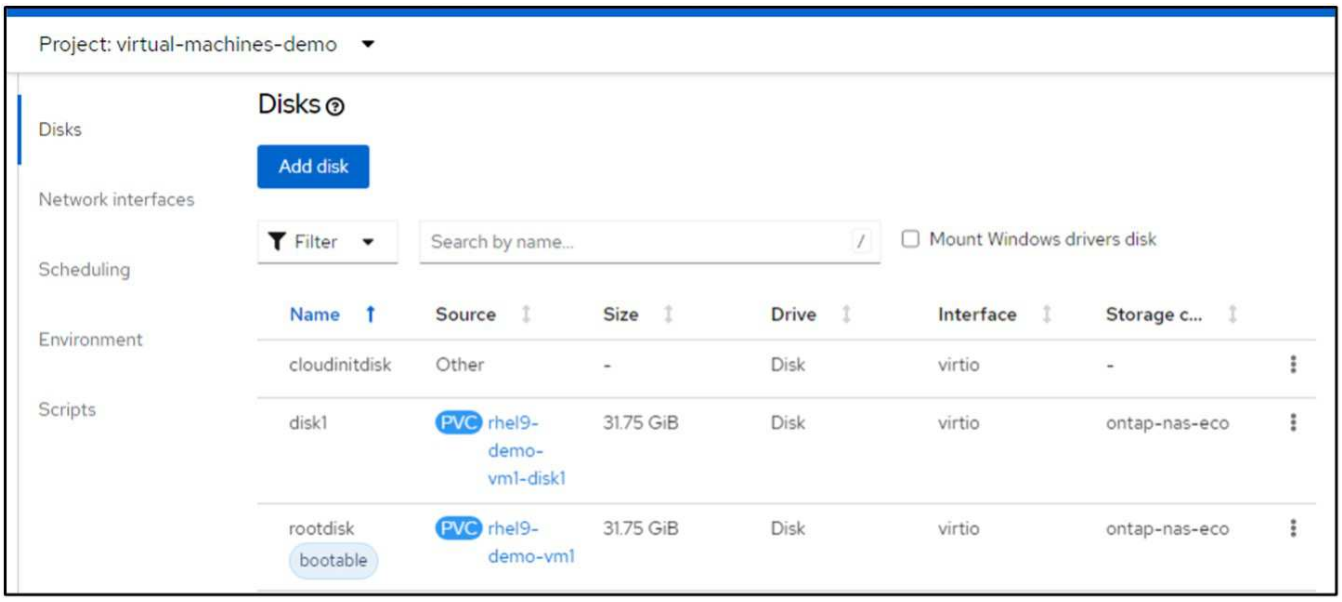
Este mapa de configuração aplicará a regra do modificador de recursos quando a restauração for criada. Um patch será aplicado para substituir o nome da classe de armazenamento para ontap-nas-eco para todas as declarações de volume persistentes que começam com rhel.

Etapa 2

Para restaurar a VM, use o seguinte comando do Velero CLI:

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

O aplicativo é restaurado no mesmo namespace com as reivindicações de volume persistentes criadas usando a classe de armazenamento ontap-nas-eco.



Excluindo backups e restaurações usando Velero

Esta seção descreve como excluir backups e restaurações de aplicativos na plataforma de contêiner OpenShift usando o Velero.

Listar todos os backups

Você pode listar todos os CRs de backup usando a ferramenta OC CLI ou a ferramenta Velero CLI. Baixe o Velero CLI conforme as instruções no"Documentação do Velero" .

```
[root@localhost ~]# oc get backups -n openshift-adp
NAME                        AGE
backup-postgresql-ontaps3   23h
backup2                     26s
schedule1-20240717070005    6h42m
[root@localhost ~]# velero get backups -n openshift-adp
NAME                        STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                SELECTOR
backup-postgresql-ontaps3   Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                     Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005    Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Excluindo um backup

Você pode excluir um CR de backup sem excluir os dados do Object Storage usando a ferramenta OC CLI. O backup será removido da saída CLI/Console. Entretanto, como o backup correspondente não é removido do armazenamento de objetos, ele reaparecerá na saída da CLI/console.

```
[root@localhost ~]# oc delete backup backup2 -n openshift-adp
backup.velero.io "backup2" deleted
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
schedule1-20240717070005      6h49m
[root@localhost ~]# oc get backups -n openshift-adp
NAME                          AGE
backup-postgresql-ontaps3     23h
backup2                       24s
schedule1-20240717070005      6h50m
[root@localhost ~]#
```

Se você quiser excluir o Backup CR E os dados de armazenamento de objetos associados, poderá fazer isso usando a ferramenta Velero CLI.

```
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
backup2                       Completed   0        0          2024-07-17 09:42:32 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]# velero delete backup backup2 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete backup "backup2" submitted successfully.
The backup will be fully deleted after all associated data (disk snapshots, backup files, restores) are removed.
[root@localhost ~]# velero get backups -n openshift-adp
NAME                          STATUS      ERRORS   WARNINGS   CREATED                         EXPIRES   STORAGE LOCATION                 SELECTOR
backup-postgresql-ontaps3     Completed   0        0          2024-07-16 10:01:08 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
schedule1-20240717070005      Completed   0        0          2024-07-17 03:00:05 -0400 EDT   29d       velero-container-backup-ontap-1   <none>
[root@localhost ~]#
```

Excluindo a restauração

Você pode excluir o objeto CR de restauração usando o OC CLI ou o Velero CLI

```
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
restore1   backup-postgresql-ontaps3   Completed   2024-07-16 16:36:37 -0400 EDT   2024-07-16 16:36:59 -0400 EDT   0        9          2024-07-16 16:36:37 -0400 EDT   <none>
[root@localhost ~]# velero restore delete restore1 -n openshift-adp
Are you sure you want to continue (Y/N)? Y
Request to delete restore "restore1" submitted successfully.
The restore will be fully deleted after all associated data (restore files in object storage) are removed.
[root@localhost ~]# velero get restore -n openshift-adp
NAME       BACKUP                    STATUS      STARTED                         COMPLETED                       ERRORS   WARNINGS   CREATED                         SELECTOR
restore    backup-postgresql-ontaps3   Completed   2024-07-16 14:59:22 -0400 EDT   2024-07-16 14:59:45 -0400 EDT   0        10         2024-07-16 14:59:22 -0400 EDT   <none>
[root@localhost ~]#
[root@localhost ~]# oc delete restore restore -n openshift-adp
restore.velero.io "restore" deleted
[root@localhost ~]# oc get restore -n openshift-adp
No resources found in openshift-adp namespace.
[root@localhost ~]# velero get restore -n openshift-adp
[root@localhost ~]#
```

Activate Windows

Assista a vídeos e demonstrações sobre soluções multicloud híbridas com a NetApp

Assista a vídeos sobre soluções multicloud híbridas para Amazon Web Services com NetApp

Explore a abrangente biblioteca de vídeos da NetApp apresentando soluções multicloud híbridas para AWS com NetApp. Assista a vídeos sobre armazenamento conectado a convidados, economia de TCO, armazenamentos de dados suplementares e fluxos de trabalho de migração para VMware Cloud on AWS e Amazon FSx for ONTAP, incluindo cenários Windows e Linux.

Armazenamento conectado ao convidado

Armazenamento conectado de convidado do Windows com FSx ONTAP usando iSCSI

Armazenamento conectado para convidados Linux com FSx ONTAP usando NFS

TCO e armazenamentos de dados suplementares

Economia de TCO do VMware Cloud na AWS com o Amazon FSx ONTAP

Armazenamento de dados suplementar do VMware Cloud on AWS com Amazon FSx ONTAP

Fluxos de trabalho de migração (HCX)

Implantação e configuração do VMware HCX para VMC

Demonstração de migração do vMotion com VMware HCX para VMC e FSx ONTAP

Demonstração de migração a frio com VMware HCX para VMC e FSx ONTAP

Assista a vídeos sobre soluções multicloud híbridas para a nuvem Azure VMware com a NetApp

Explore a abrangente biblioteca de vídeos da NetApp apresentando soluções multicloud híbridas para o Azure VMware Solution (AVS) com NetApp. Esta coleção inclui vídeos sobre armazenamentos de dados suplementares, recuperação de desastres e fluxos de trabalho de migração.

Armazenamentos de dados suplementares

Visão geral do armazenamento de dados suplementar da solução VMware do Azure com o Azure NetApp Files

Recuperação de desastres

Solução Azure VMware DR com Cloud Volumes ONTAP, SnapCenter e JetStream

Fluxos de trabalho de migração (HCX)

Demonstração de migração a frio com VMware HCX para AVS e ANF

Demonstração do vMotion com VMware HCX para AVS e ANF

Demonstração de migração em massa com VMware HCX para AVS e ANF

Assista a vídeos sobre soluções multicloud híbridas para Red Hat OpenShift com NetApp

Explore a abrangente biblioteca de vídeos da NetApp apresentando soluções multicloud híbridas para Red Hat OpenShift com NetApp. Esta coleção inclui demonstrações de snapshots e restauração para OpenShift na AWS (ROSA) com FSx ONTAP, integração com Trident, failover e fail-back para aplicativos e implantação automatizada do Oracle RAC no FlexPod com Ansible.

Snapshots e restauração

Snapshot/Restauração para aplicativos em clusters do Red Hat OpenShift Service on AWS (ROSA) com armazenamento Amazon FSx ONTAP

Integração de armazenamento

Integração do FSx ONTAP com o Trident

Failover e failback

Failover e Fail-back de aplicativos no ROSA com FSx ONTAP

Automação de soluções



Implantação automatizada do Oracle 19c RAC no FlexPod com Ansible

Leia blogs sobre soluções em nuvem de especialistas da NetApp

Leia os blogs que oferecem orientações práticas e práticas recomendadas para integrar o armazenamento ONTAP com as soluções de nuvem da NetApp .

Integração do VMware com AWS e Amazon FSx para ONTAP

- "Migrar VMs VMware para AWS usando o Amazon EC2 e o protocolo Amazon FSx ONTAP iSCSI"
- "Amazon EVS agora se integra com FSx para ONTAP"
- "Amazon EVS anuncia suporte para FSx para ONTAP"
- "Configurar Nuvem Híbrida com FSx ONTAP e VMware Cloud na AWS SDDC usando VMware HCX"

Solução Azure VMware

- "Otimize o armazenamento e as cargas de trabalho VMware com uso intensivo de dados em qualquer nuvem"
- "Migrar cargas de trabalho VMware para Azure VMware Solution? Leia isto primeiro."

Google Cloud VMware Engine

- "Suporte ao armazenamento de dados do Google Cloud NetApp Volumes para o Google Cloud VMware Engine (NetApp)"
- "Como usar o NetApp Volumes como armazenamento de dados para o Google Cloud VMware Engine (Google)"
- "Blog da NetApp - Uma maneira melhor de migrar seus aplicativos com alto armazenamento para o Google Cloud"

Proteção e gestão de dados

- "Proteção de dados 3-2-1 para o VMware com o SnapCenter Plug-in e o NetApp Backup and Recovery for VMs"
- "Observabilidade para o data center moderno com o NetApp Cloud Insights"

Cargas de trabalho de contêiner NetApp para OpenShift

- "O NetApp ONTAP também funciona como armazenamento para logs na plataforma de contêineres Red Hat OpenShift"

Nuvem soberana da VMware

- "Apresentando a nova iniciativa Sovereign Cloud"

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de Privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Informações sobre direitos autorais

Copyright © 2026 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.