TR-4955: Recuperação de desastres com Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/pt-br/netapp-solutions-cloud/vmware/vmw-azure-avs-dro.html on August 18, 2025. Always check docs.netapp.com for the latest.

Índice

TR-4955: Recuperação de desastres com Azure NetApp Files (ANF) e Azure VMware Solution (AVS) 1
Visão geral 1
Pré-requisitos e recomendações gerais 1
Começando 2
Implantar a solução Azure VMware 2
Provisionar e configurar o Azure NetApp Files 2
Instalação DRO 3
Configuração DRO 4
Agrupamentos de recursos 7
Planos de replicação 8
Recuperação de ransomware 14
Conclusão 15
Onde encontrar informações adicionais 15

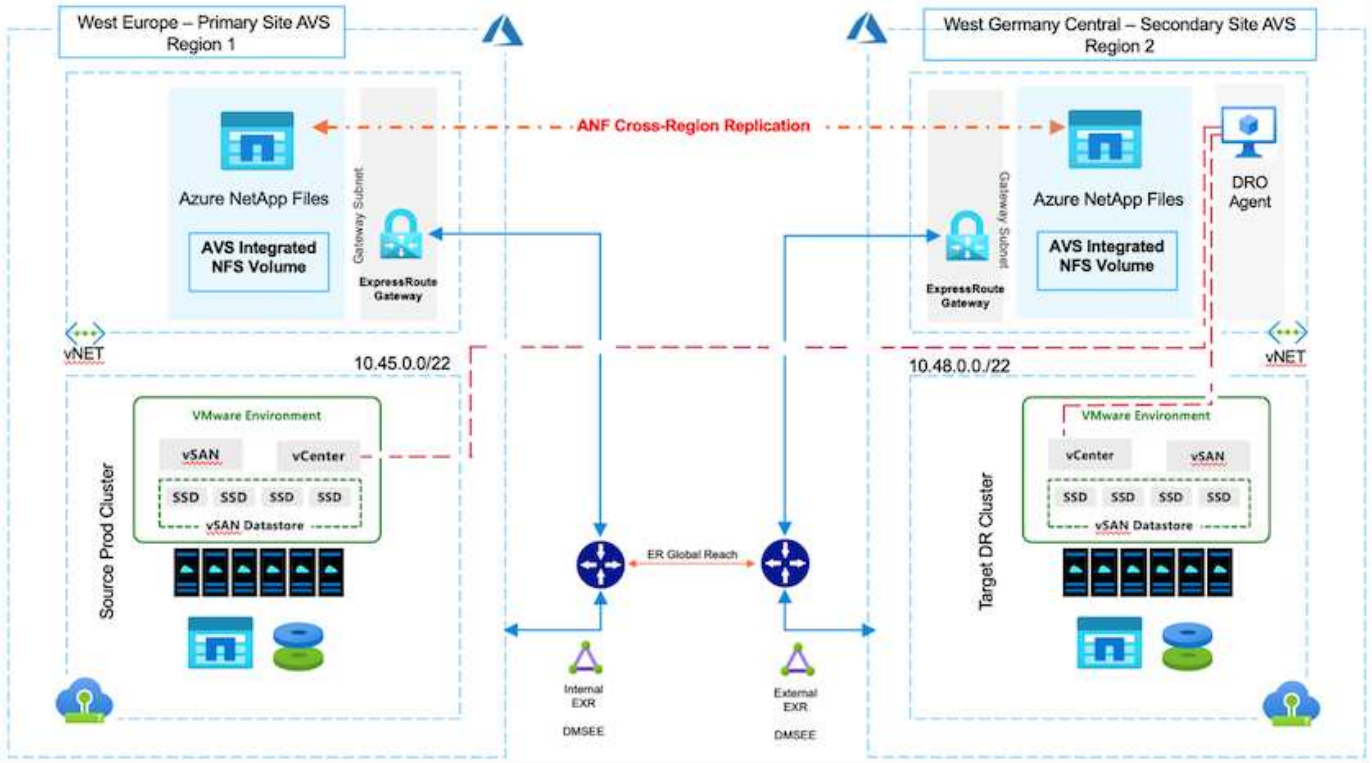
TR-4955: Recuperação de desastres com Azure NetApp Files (ANF) e Azure VMware Solution (AVS)

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.

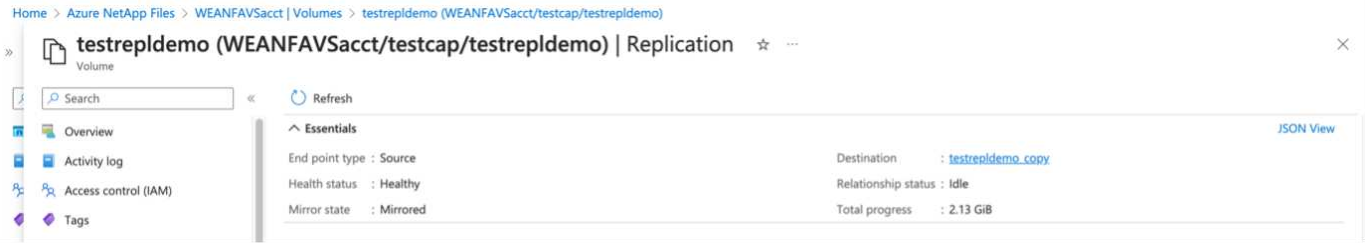
> Na versão inicial, o DRO oferece suporte a um cluster AVS SDDC existente. A criação de SDDC sob demanda estará disponível em uma próxima versão.

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:

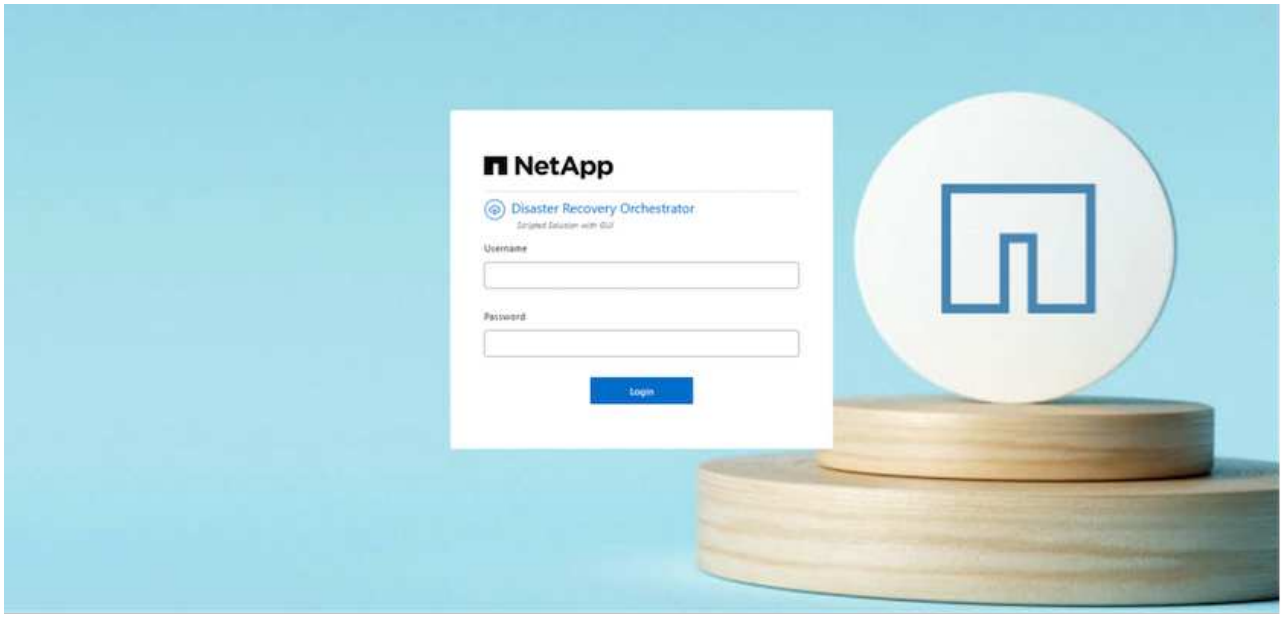
```
git clone https://github.com/NetApp/DRO-Azure.git
```

> 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.

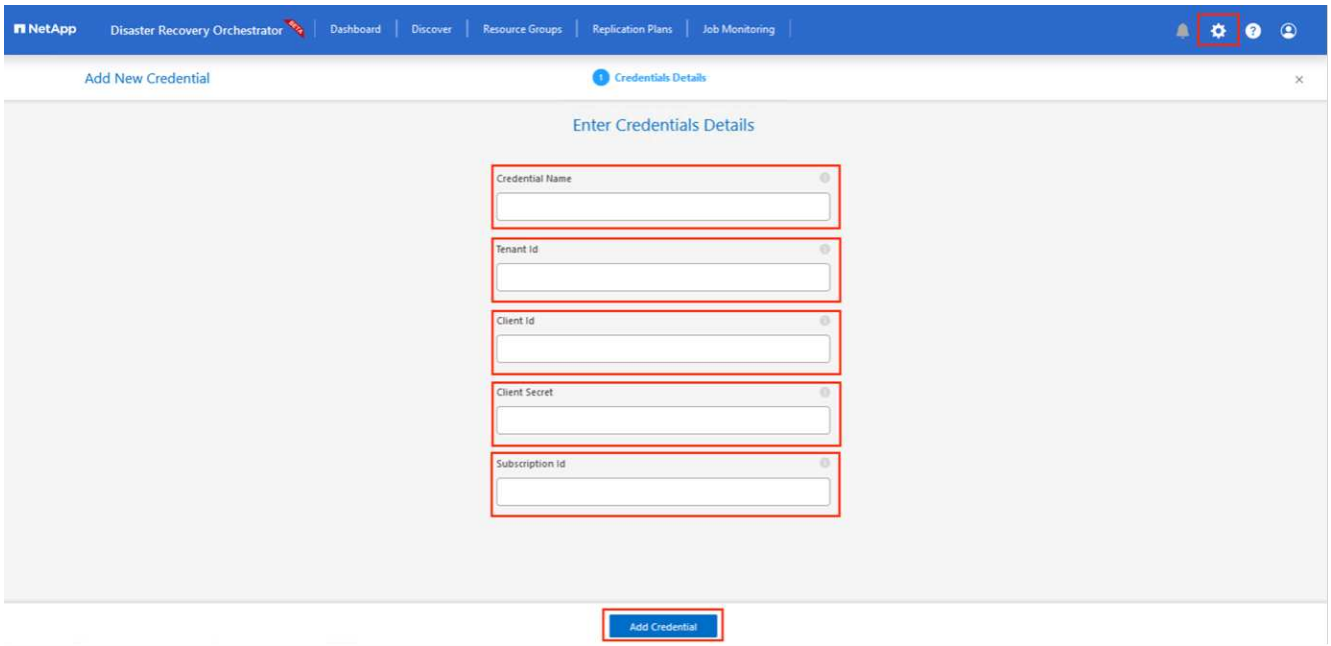
Para executar esta operação, siga os seguintes passos:

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

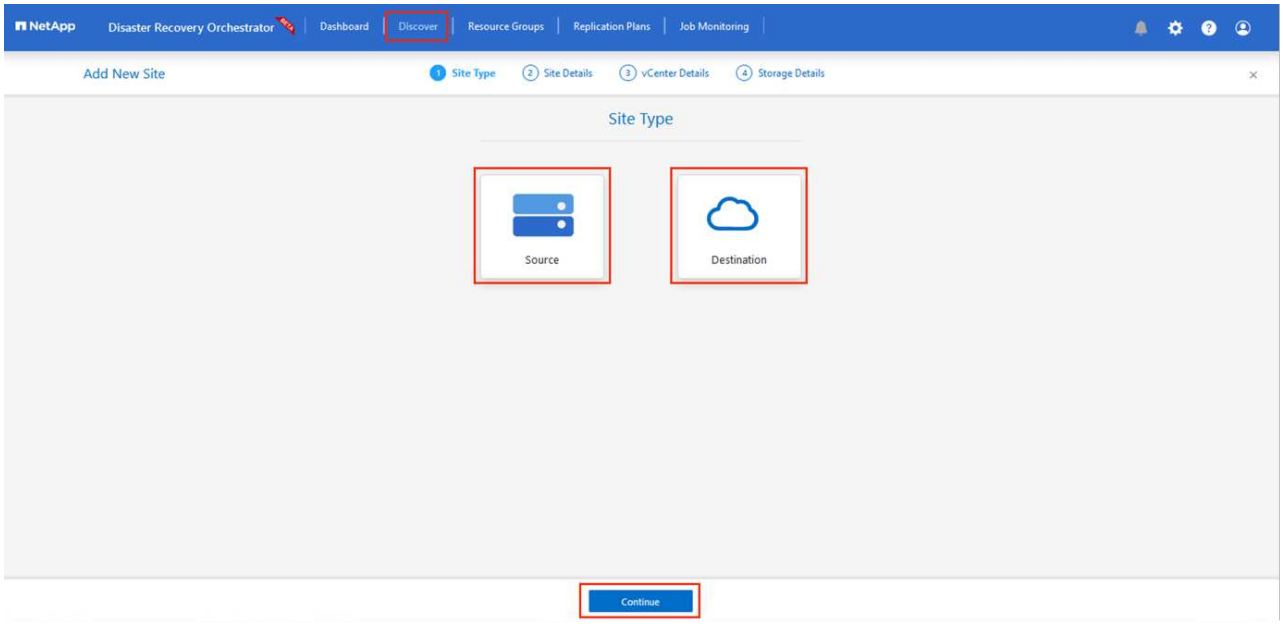
  Você deveria ter capturado essas informações ao criar o aplicativo AD.

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:

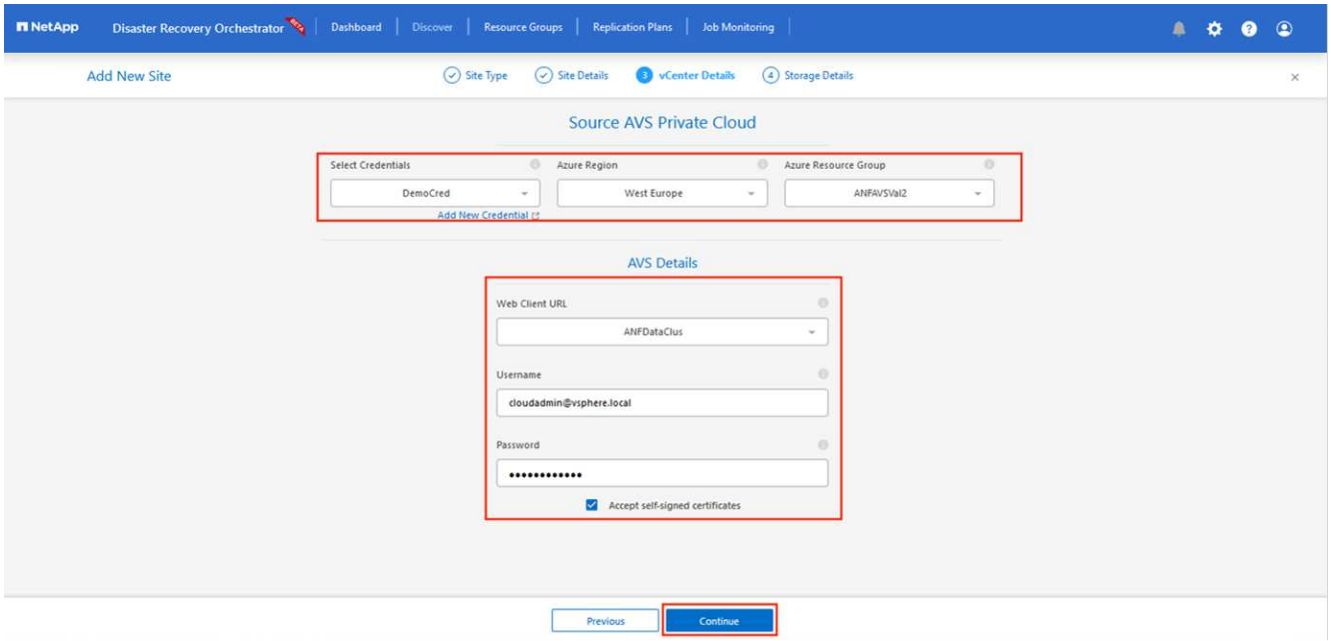
6. Acesse a aba **Descobrir**.
7. Clique em **Adicionar novo site**.
8. Adicione o seguinte site AVS primário (designado como **Fonte** no console).
   - SDDC vCenter
   - Conta de armazenamento do Azure NetApp Files
9. Adicione o seguinte site AVS secundário (designado como **Destino** no console).
   - 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**.

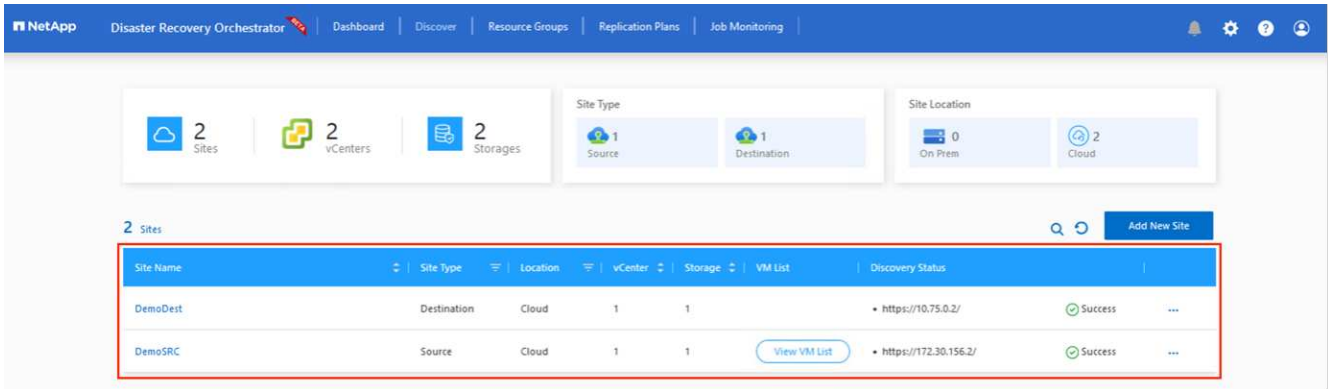
> Para fins de demonstração, a adição de um site de origem é abordada neste documento.

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**.

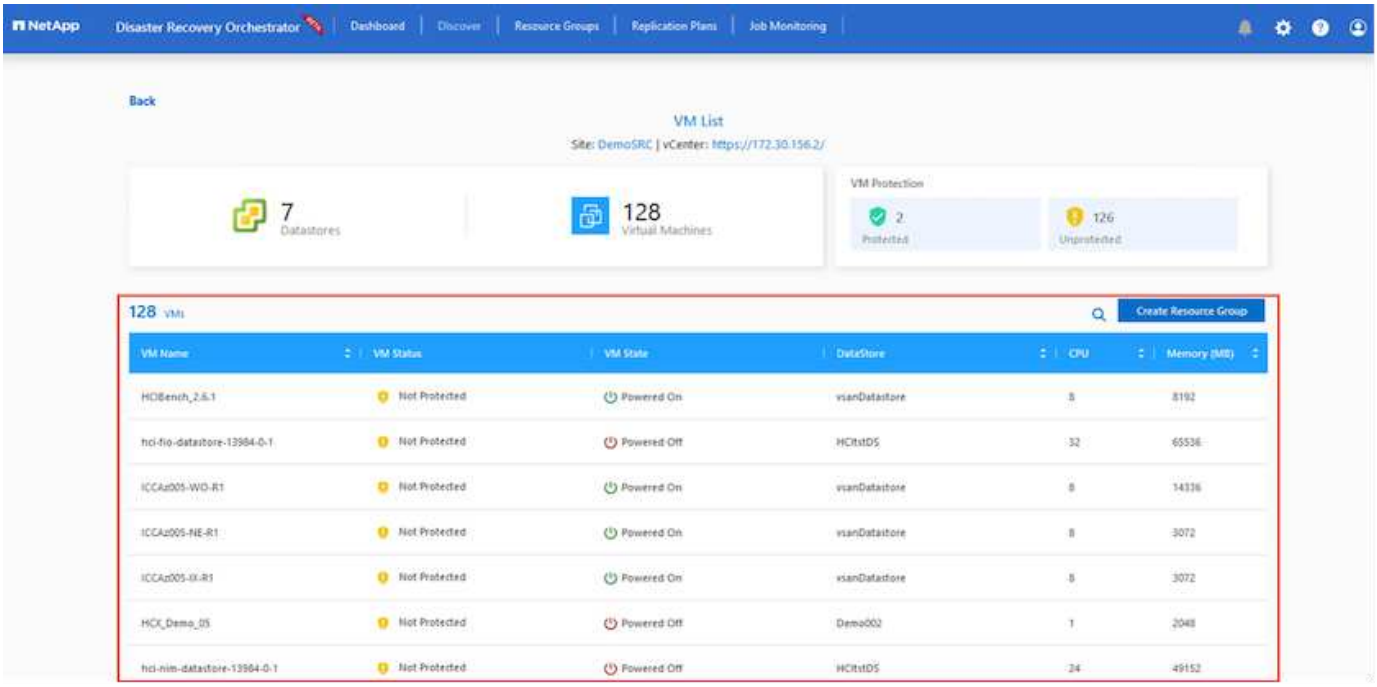


14. Selecione os detalhes do Source Storage (ANF) selecionando o grupo de recursos do Azure e a conta do NetApp .

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.



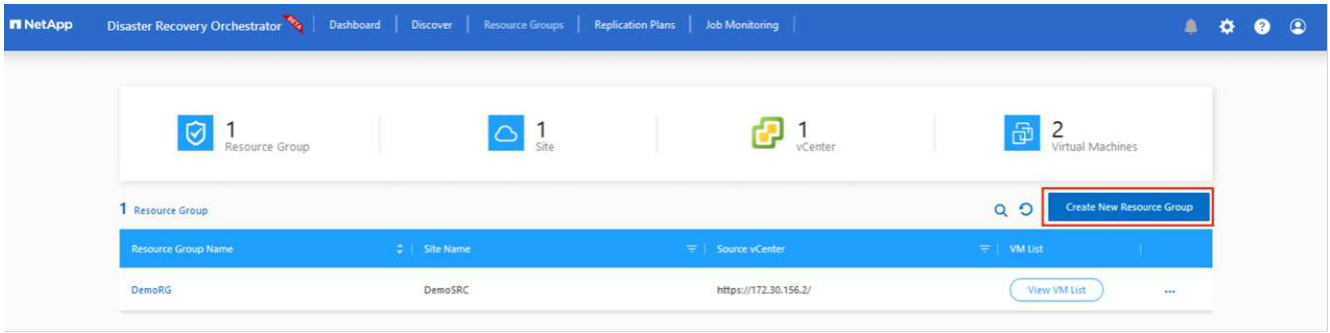
A próxima etapa é agrupar as VMs necessárias em seus grupos funcionais como grupos de recursos.

Agrupamentos de recursos

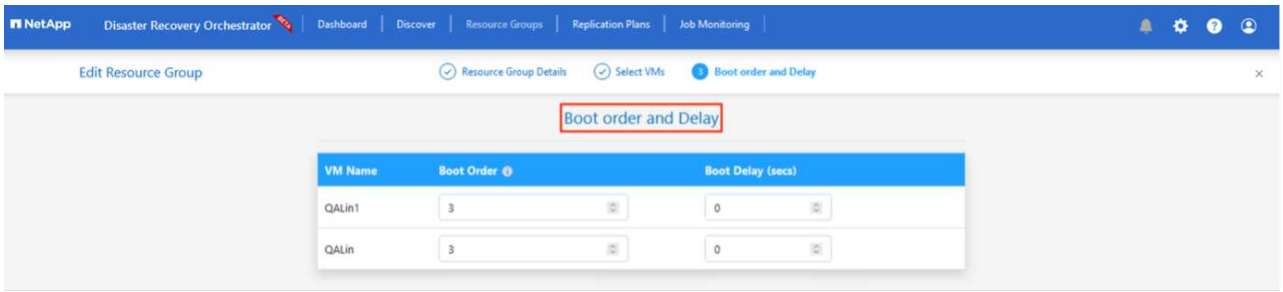
Depois que as plataformas forem adicionadas, agrupe as VMs que você deseja recuperar em grupos de recursos. Os grupos de recursos de DRO permitem que você agrupe um conjunto de VMs dependentes em grupos lógicos que contêm suas ordens de inicialização, atrasos de inicialização e validações de aplicativos opcionais que podem ser executadas na recuperação.

Para começar a criar grupos de recursos, clique no item de menu **Criar novo grupo de recursos**.

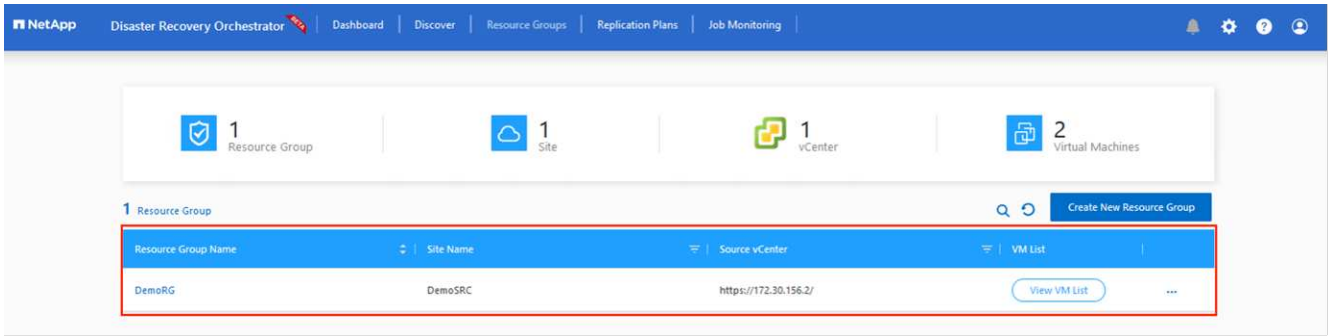
1. Acesse **Grupos de Recursos** e clique em **Criar Novo Grupo de Recursos**.



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**.

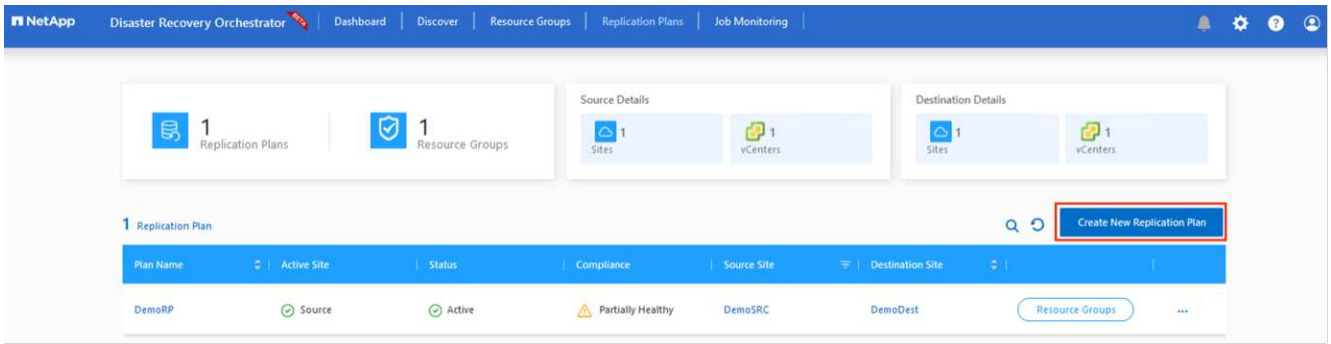


Planos de replicação

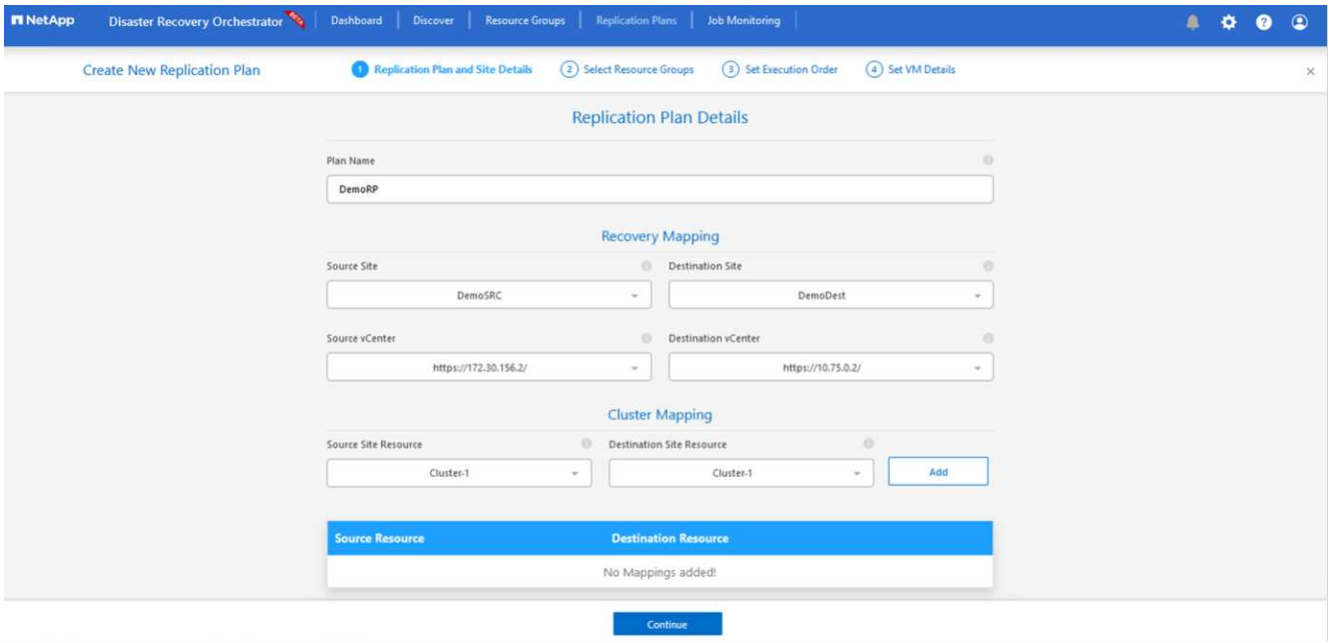
Você deve ter um plano para recuperar aplicativos em caso de desastre. Selecione as plataformas vCenter de origem e destino no menu suspenso, escolha os grupos de recursos a serem incluídos neste plano e inclua também o agrupamento de como os aplicativos devem ser restaurados e ligados (por exemplo, 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:

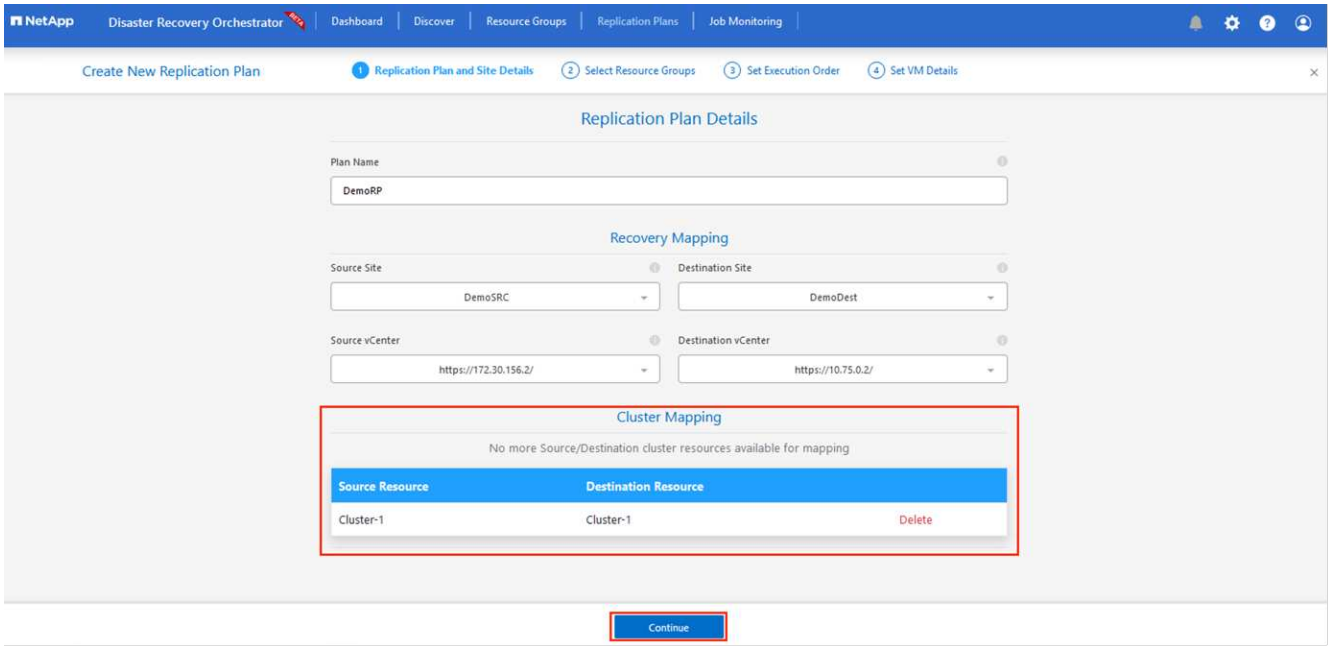
1. Navegue até **Planos de Replicação** e clique em **Criar Novo Plano de Replicação**.



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.

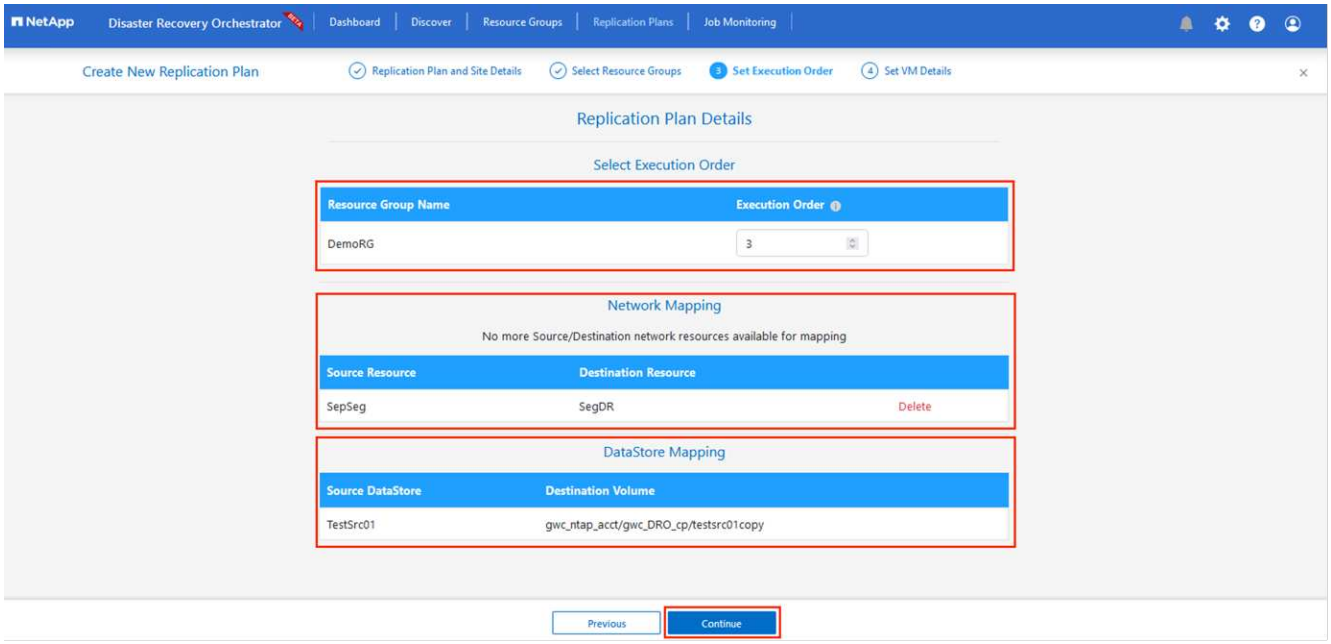


3. Após a conclusão do mapeamento de recuperação, selecione **Mapeamento de Cluster**.

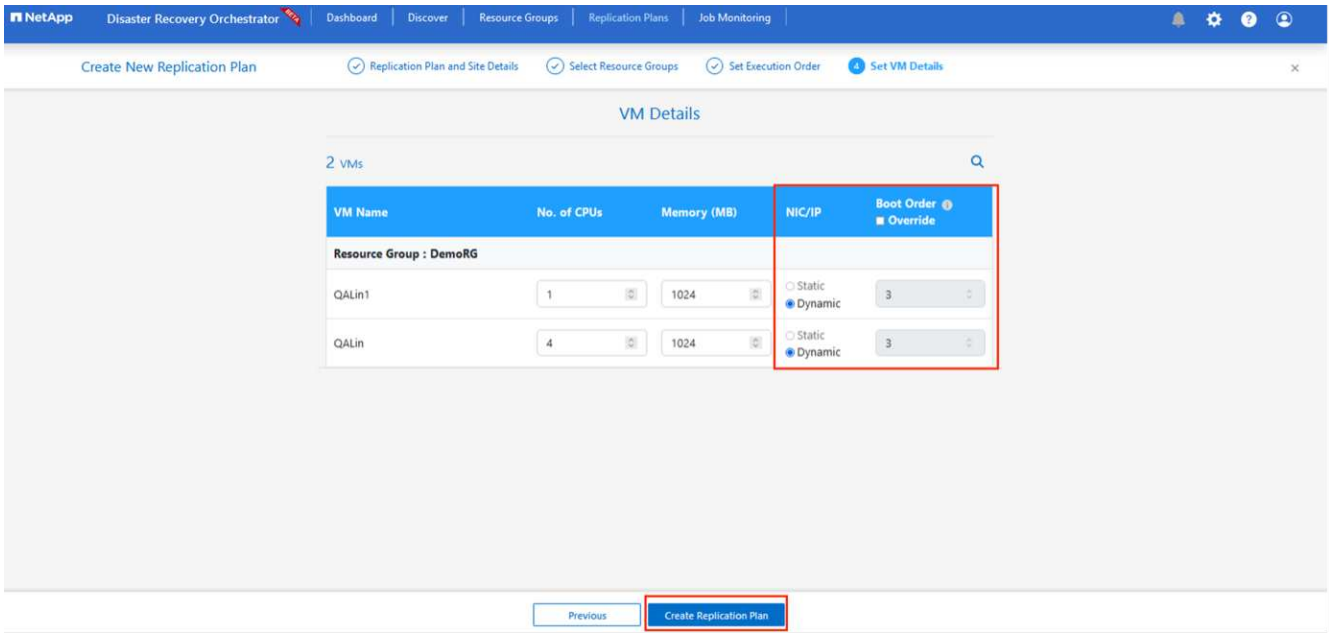


4. Selecione **Detalhes do grupo de recursos** e clique em **Continuar**.
5. Defina a ordem de execução para o grupo de recursos. Esta opção permite que você selecione a sequência de operações quando existem vários grupos de recursos.
6. Uma vez feito isso, defina o mapeamento de rede para o segmento 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.

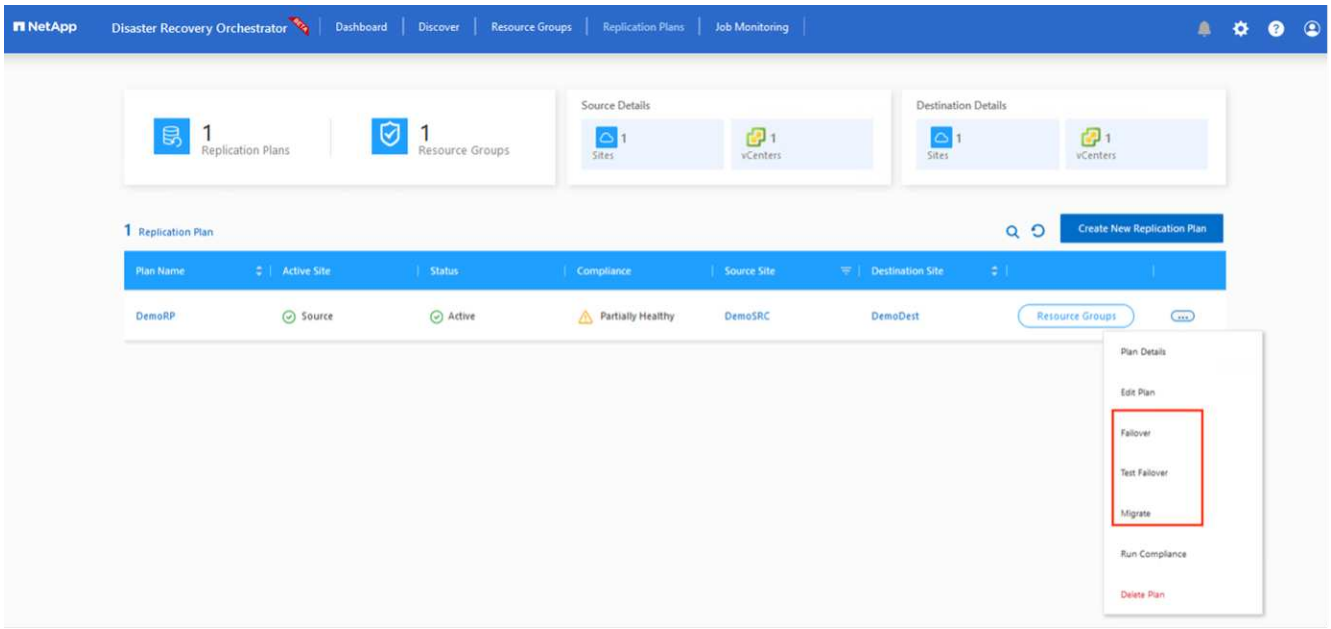
> A replicação entre regiões (CRR) ocorre no nível de volume. Portanto, todas as VMs que residem no respectivo volume são replicadas para o destino CRR. Certifique-se de selecionar todas as VMs que fazem parte do armazenamento de dados, porque somente as máquinas virtuais que fazem parte do plano de 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.

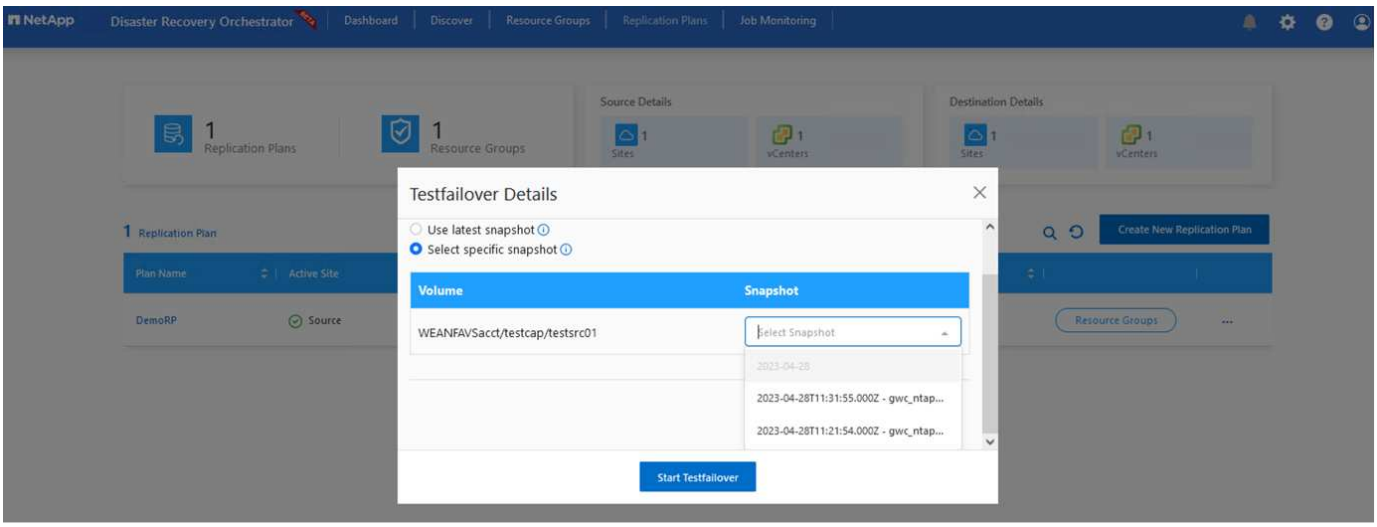


9. Clique em **Criar Plano de Replicação**. Após a criação do plano de replicação, você pode exercer as opções de failover, failover de teste ou migrar, dependendo de suas necessidades.

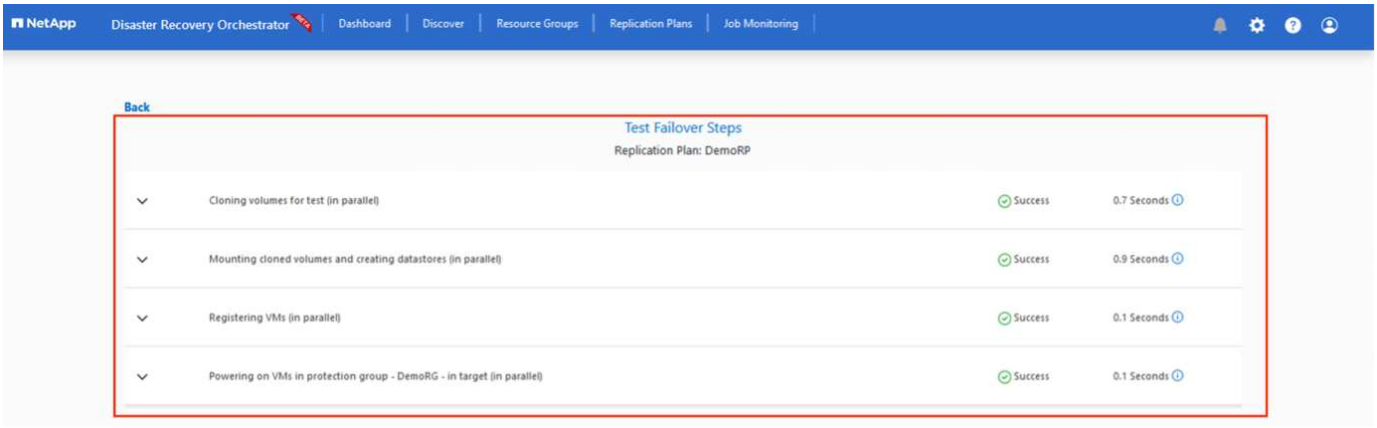


Durante as opções de failover e failover de teste, o snapshot mais recente é usado, ou um snapshot específico pode ser selecionado de um snapshot de momento específico. A opção de ponto no tempo pode

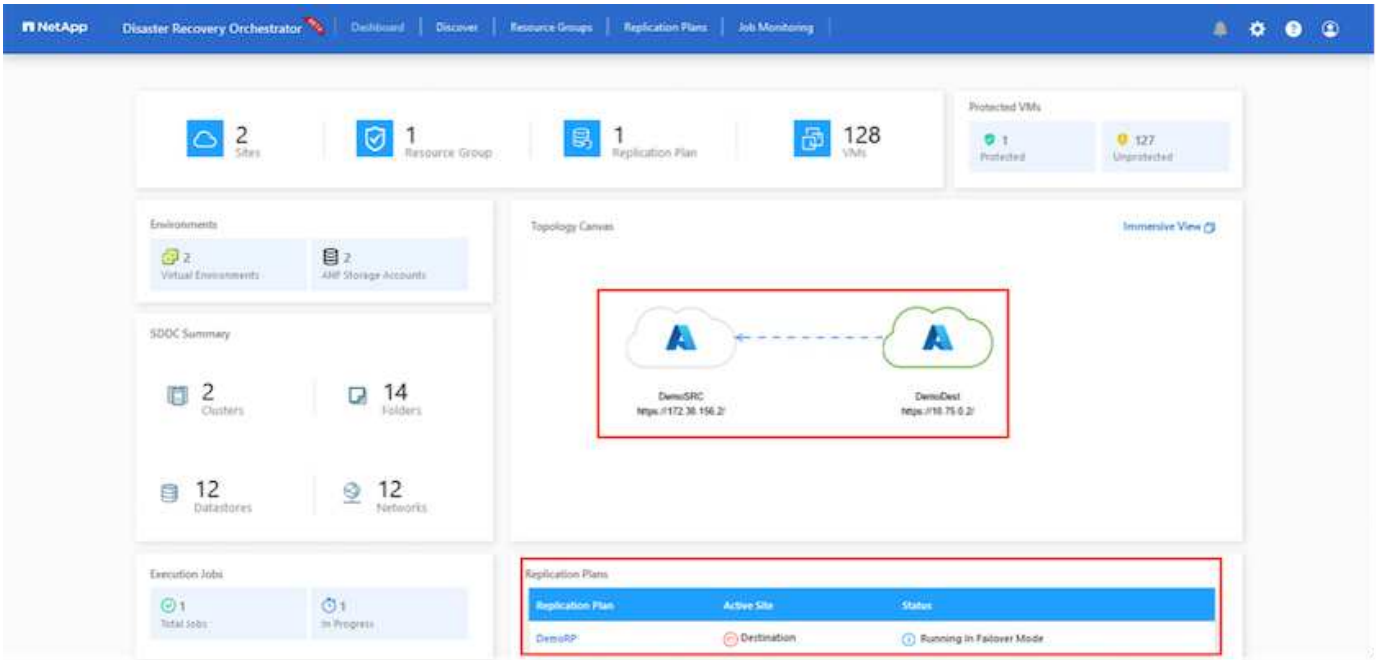
ser muito benéfica se você estiver enfrentando um evento de corrupção como um ransomware, em que as réplicas mais recentes já estão comprometidas ou criptografadas. O DRO mostra todos os pontos de tempo disponíveis.



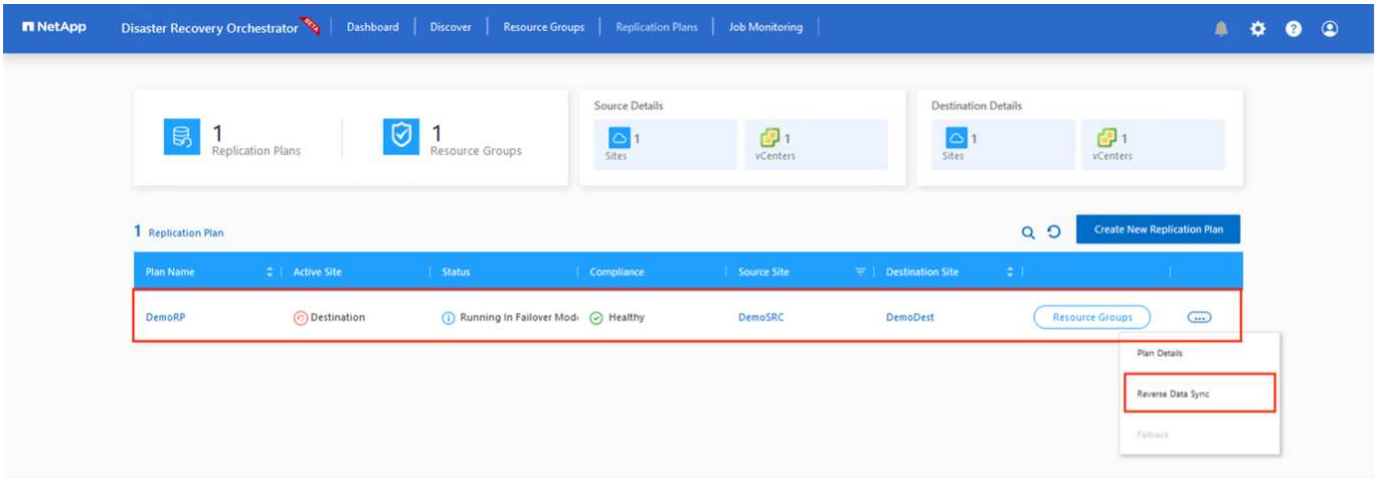
Para acionar o failover ou testar o failover com a configuração especificada no plano de replicação, você pode clicar em **Failover** ou **Testar failover**. Você pode monitorar o plano de replicação no menu de tarefas.



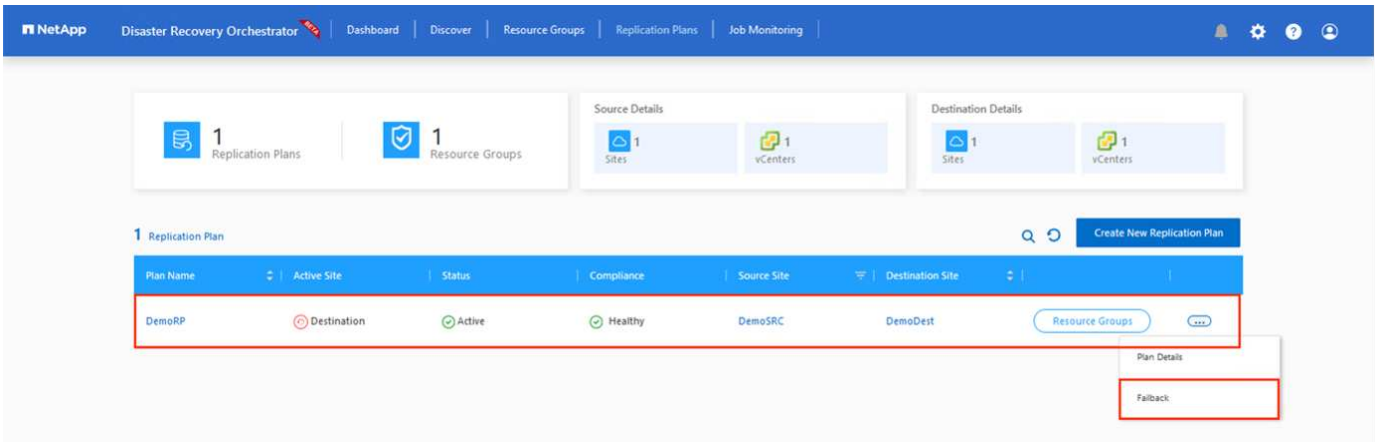
Após o failover ser acionado, os itens recuperados podem ser vistos no site secundário AVS SDDC vCenter (VMs, redes e armazenamentos de dados). Por padrão, as VMs são recuperadas para a pasta Carga de trabalho.

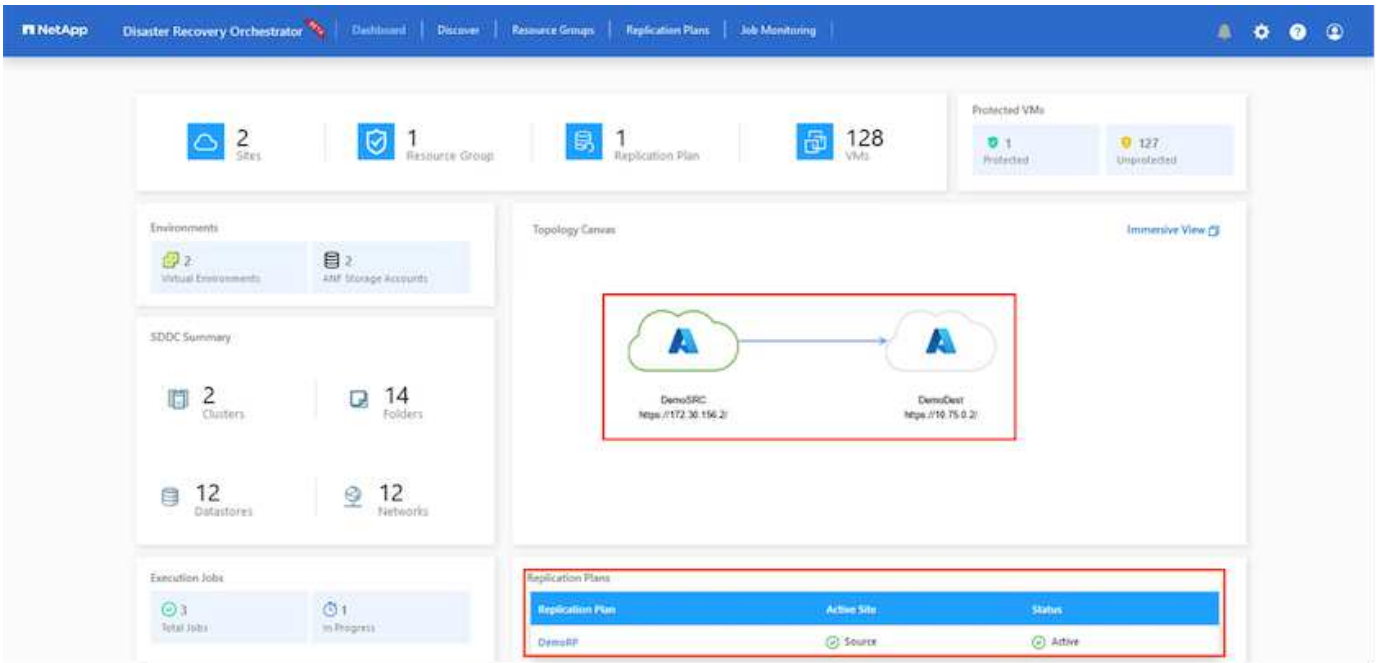


O failback pode ser acionado no nível do plano de replicação. Em caso de falha de teste, a opção de desmontagem pode ser usada para reverter as alterações e remover o volume recém-criado. Failbacks relacionados a failover são um processo de duas etapas. Selecione o plano de replicação e selecione **Sincronização 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

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em http://www.netapp.com/TM são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.