



TR-4955: Recuperação de desastres com FSx ONTAP e VMC (AWS VMware Cloud)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Índice

- TR-4955: Recuperação de desastres com FSx ONTAP e VMC (AWS VMware Cloud) 1
 - Visão geral 1
 - Começando 1
 - Implantar e configurar o VMware Cloud na AWS 2
 - Provisionar e configurar o FSx ONTAP 2
 - Implantar e configurar o SnapMirror no FSx ONTAP 2
 - Instalação DRO 3
 - Pré-requisitos 3
 - Requisitos do OS 3
 - Instalar o pacote 3
 - Configuração DRO 4
 - Agrupamentos de recursos 6
 - Planos de replicação 7
 - Recuperação de ransomware 15
 - Benefícios 15

TR-4955: Recuperação de desastres com FSx ONTAP e VMC (AWS VMware Cloud)

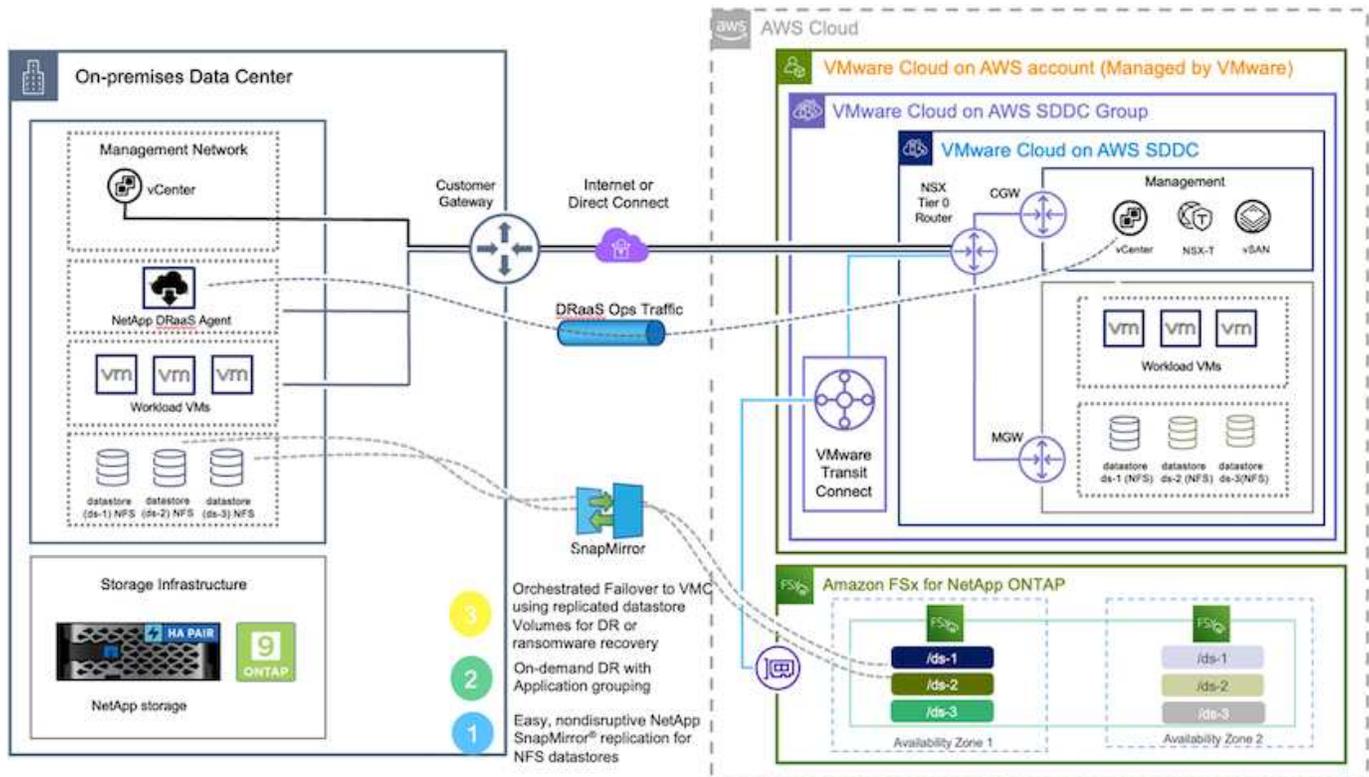
O Disaster Recovery Orchestrator (DRO; uma solução com script e interface de usuário) pode ser usado para recuperar facilmente cargas de trabalho replicadas do local para o FSx ONTAP. O DRO automatiza a recuperação do nível do SnapMirror, passando pelo registro da VM no VMC, até os mapeamentos de rede 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.



Começando

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 VM na AWS, siga as etapas neste [link](#) . Um conjunto de luz piloto também pode ser usado para fins de DR.



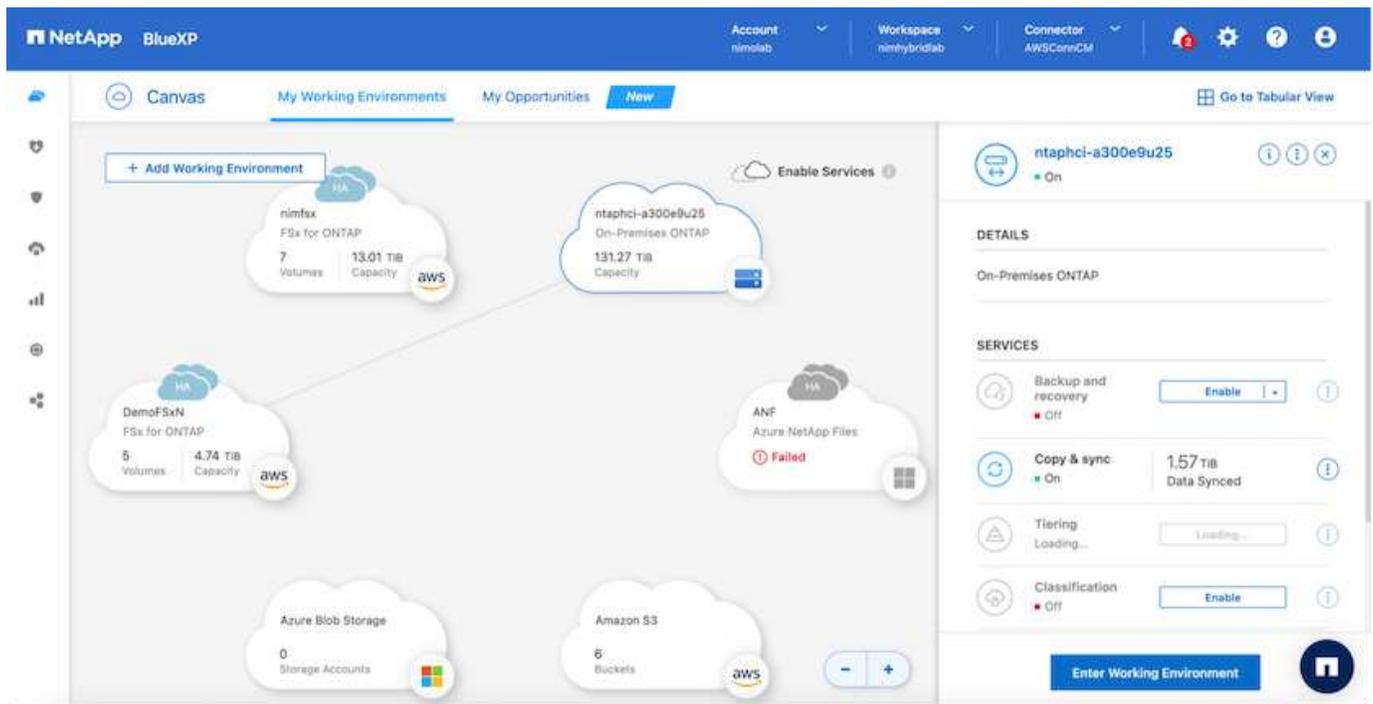
Na versão inicial, o DRO dá suporte a um cluster piloto existente. A criação de SDDC sob demanda estará disponível em uma próxima versão.

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

A próxima etapa é usar o NetApp BlueXP e descobrir o FSx ONTAP provisionado na instância da AWS e replicar os volumes de armazenamento de dados desejados de um ambiente local para o FSx ONTAP com a frequência apropriada e retenção de cópia do NetApp Snapshot:



Siga os passos neste [link](#) para configurar o BlueXP. Você também pode usar o NetApp ONTAP CLI 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:

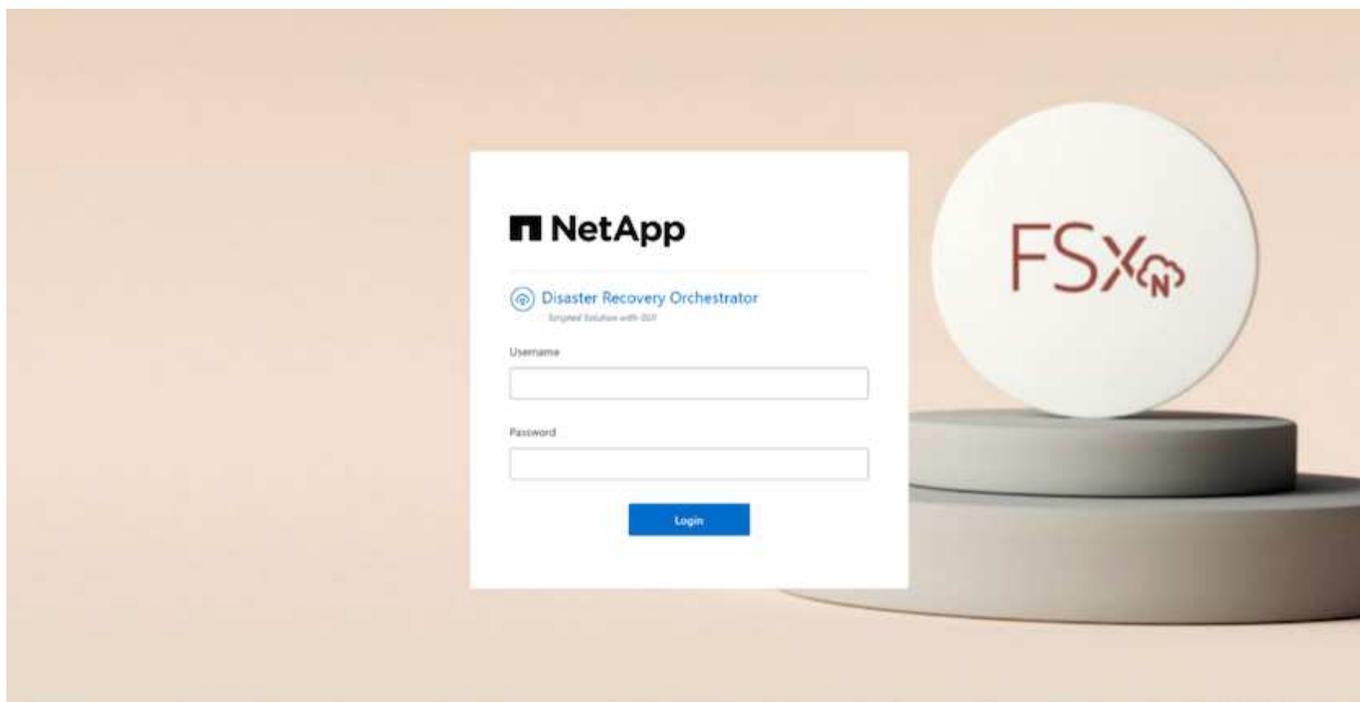
```
https://<host-ip-address>
```

com as seguintes credenciais padrão:

```
Username: admin  
Password: admin
```



A senha pode ser alterada usando a opção "Alterar senha".



Configuração DRO

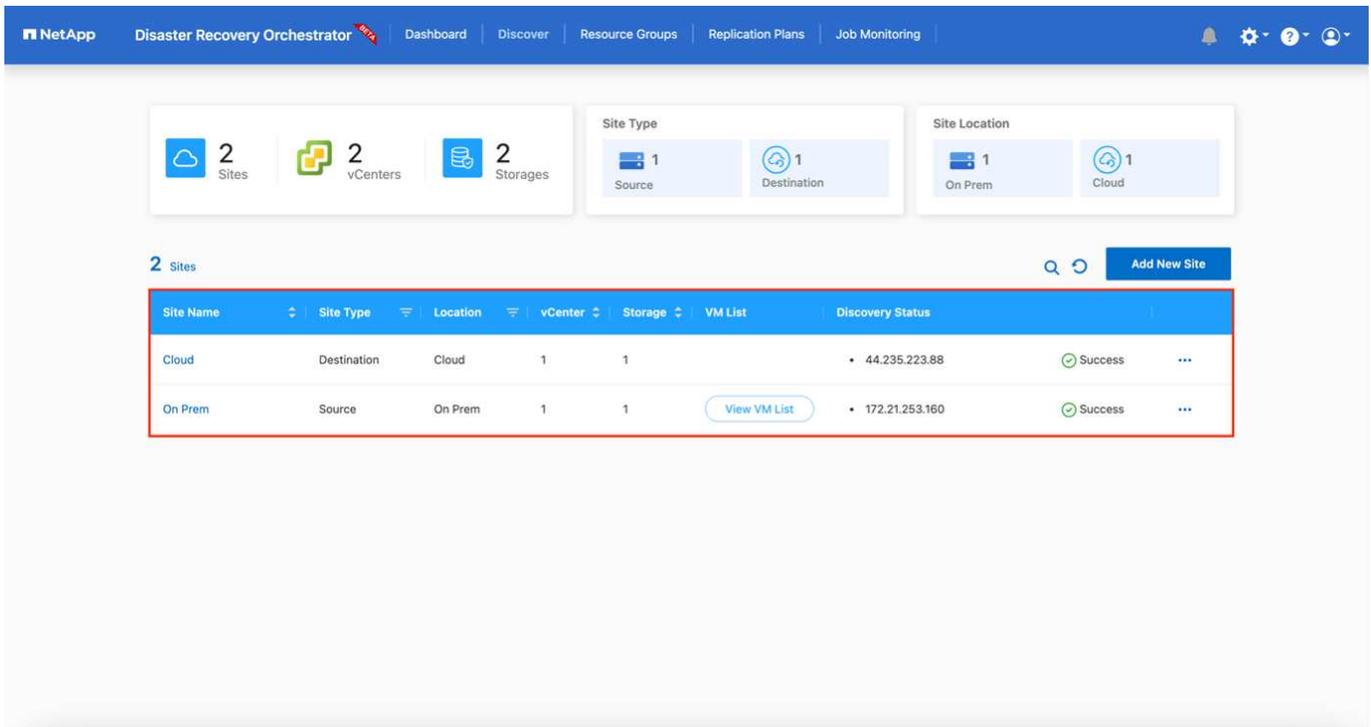
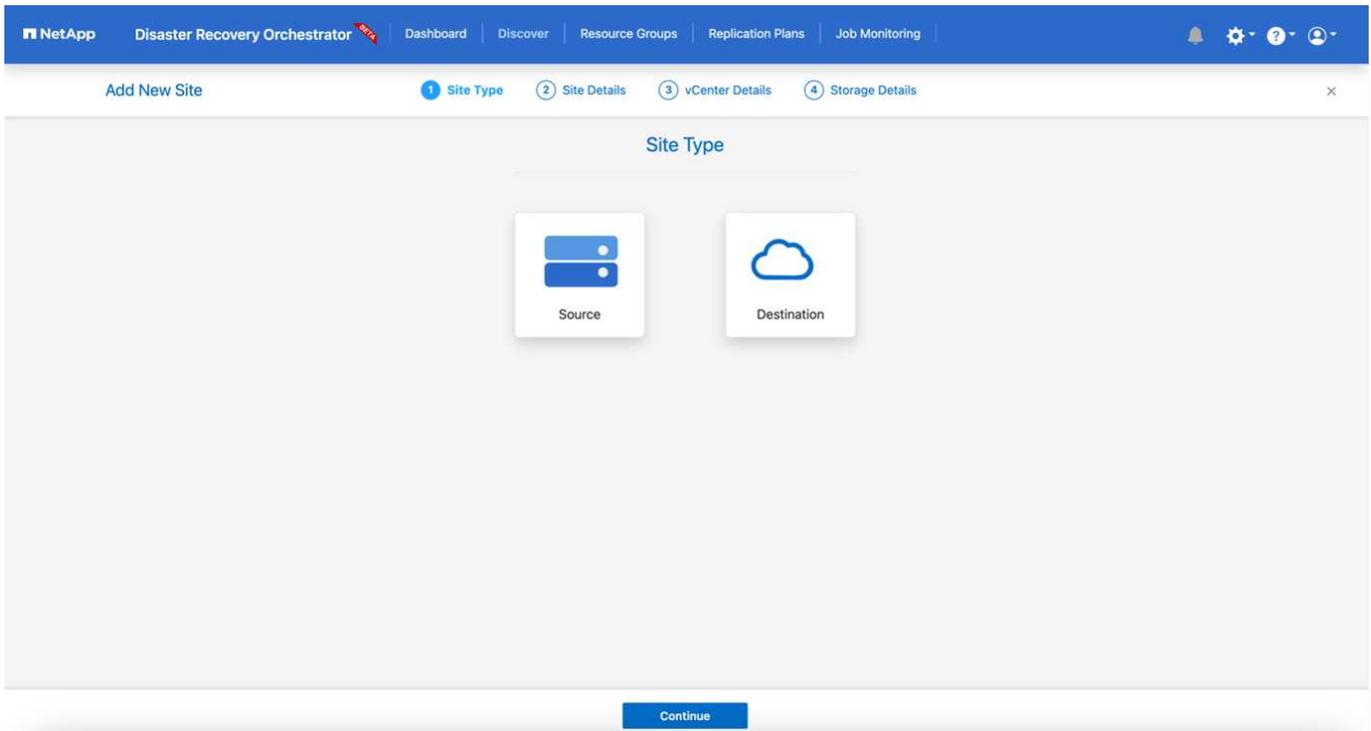
Depois que o FSx ONTAP e o VMC forem configurados corretamente, você poderá começar a configurar o DRO para automatizar a recuperação de cargas de trabalho locais para o VMC usando cópias somente leitura do SnapMirror no FSx ONTAP.

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.

NetApp Disaster Recovery Orchestrator Dashboard Discover Resource Groups Replication Plans Job Monitoring

Back VM List Site: On Prem | vCenter: 172.21.253.160

10 Datastores 219 Virtual Machines

VM Protection 3 Protected 216 Unprotected

38 VMs Create Resource Group

VM Name	VM Status	VM State (1)	DataStore	CPU	Memory (MB)
a300-vcsa02	Not Protected	Powered On	A300_NFS_DS04	16	65536
PFSense	Not Protected	Powered On	A300_NFS_DS04	4	8192
PFSense260	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimDC02	Not Protected	Powered On	A300_NFS_DS04	4	8192
jRBhaja-1B7	Not Protected	Powered On	A300_NFS_DS04	4	16384
jNimo-1B7	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimMSdesktop	Not Protected	Powered On	A300_NFS_DS04	8	12288

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.

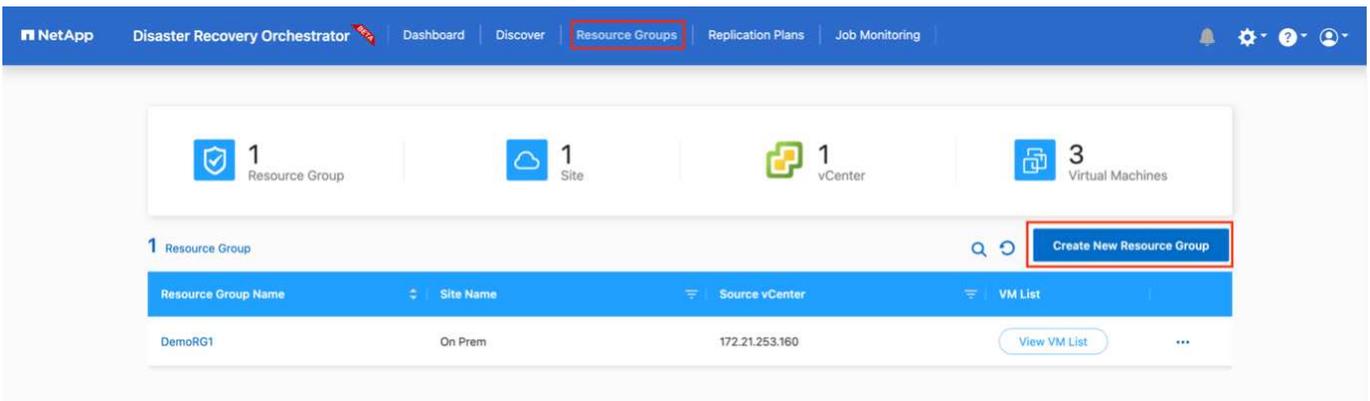
Para começar a criar grupos de recursos, conclua as seguintes etapas:

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**.

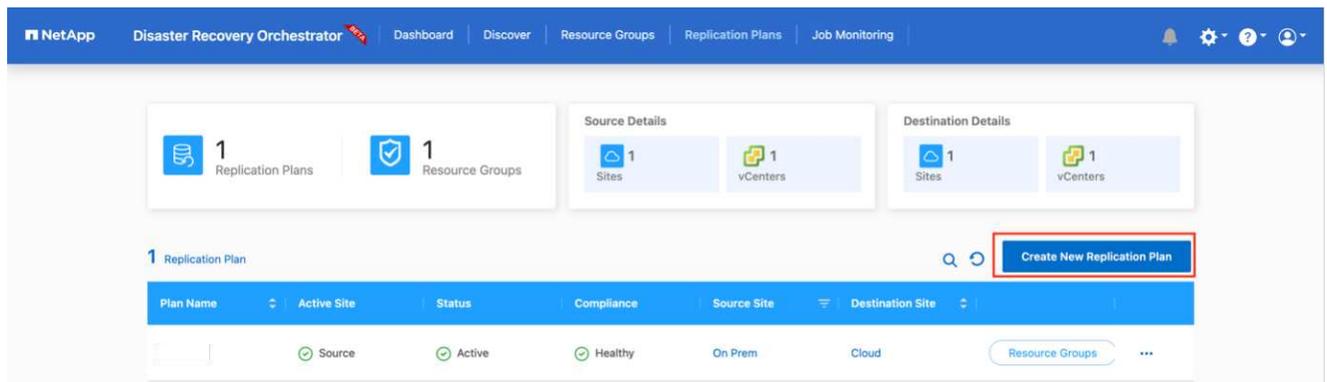


Planos de replicação

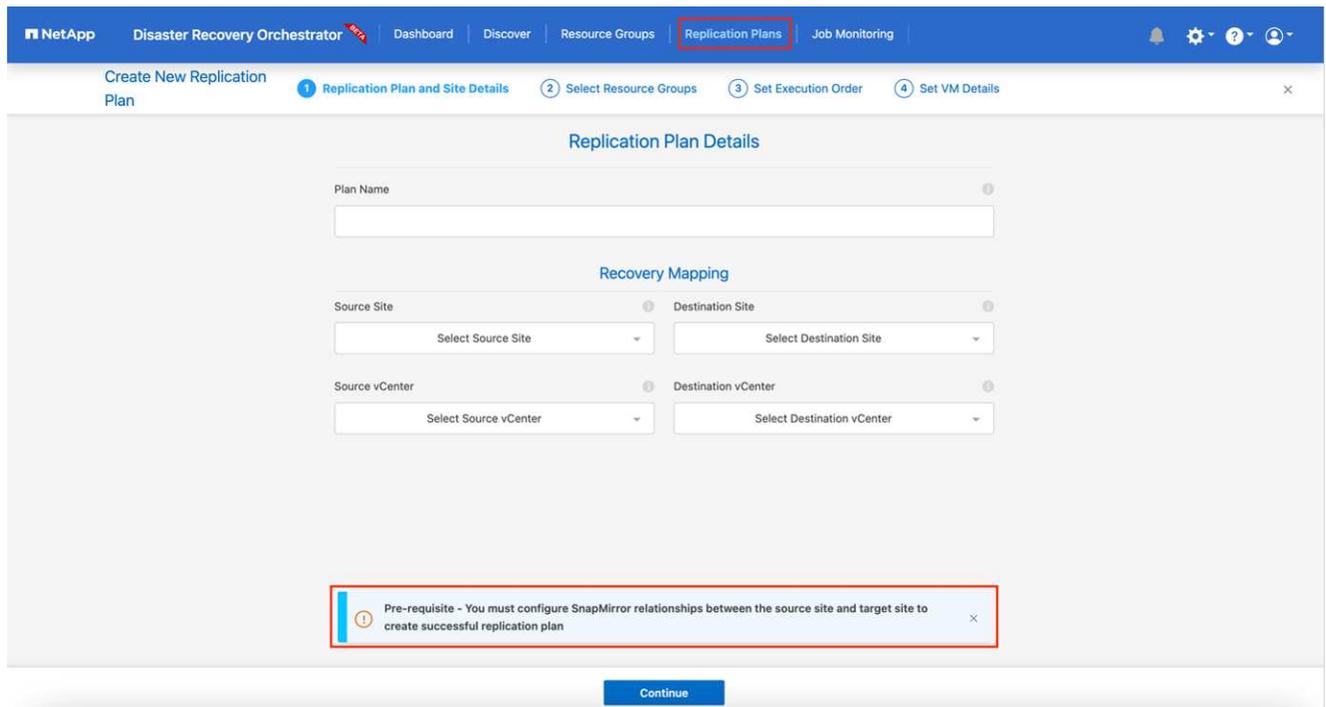
Você precisa de um plano para recuperar aplicativos em caso de desastre. Selecione as plataformas vCenter de origem e destino no menu suspenso e escolha os grupos de recursos a serem incluídos neste plano, juntamente com o agrupamento de como os aplicativos devem ser restaurados e ligados (por exemplo,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

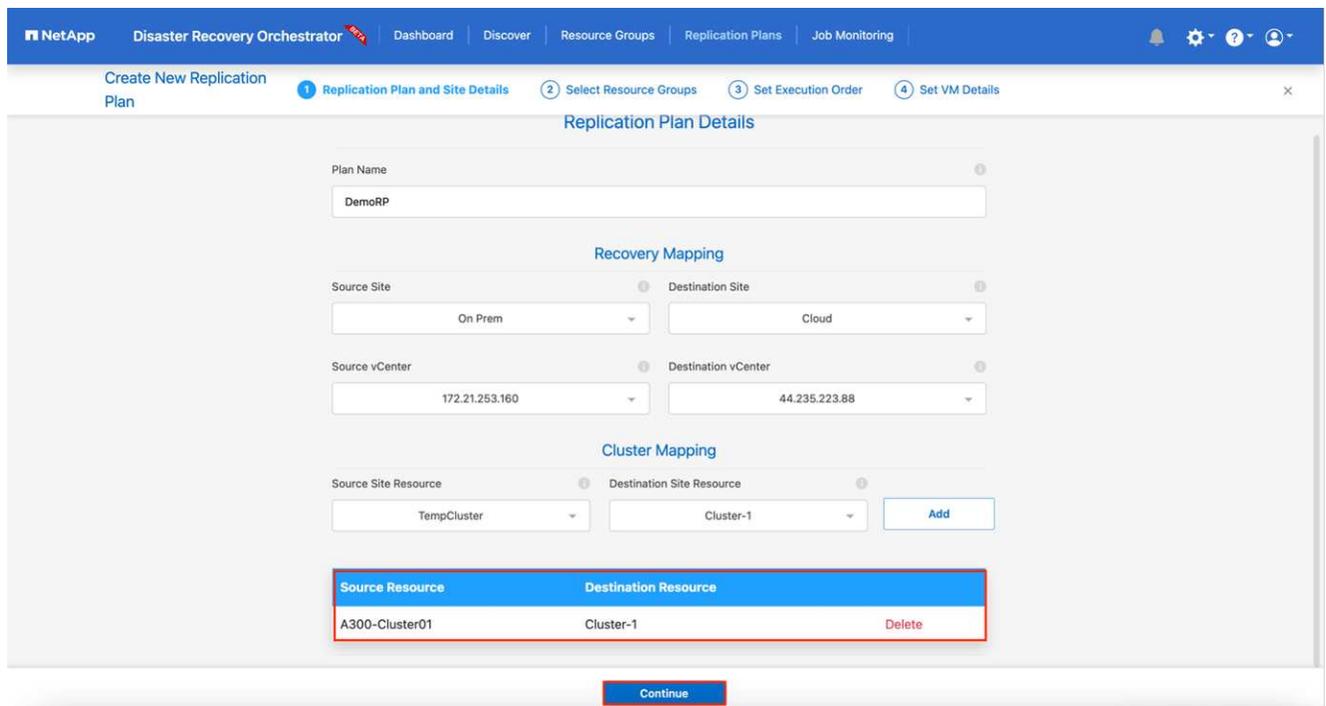
1. Acesse **Planos de Replicação** e clique em **Criar Novo Plano de Replicação**.



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.

The screenshot shows the 'Replication Plan Details' page in the NetApp Disaster Recovery Orchestrator. The page is divided into three main sections: 'Select Execution Order', 'Network Mapping', and 'DataStore Mapping'. Each section contains a table with resource details.

Select Execution Order:

Resource Group Name	Execution Order
DemoRG1	3

Network Mapping:

No more Source/Destination network resources available for mapping

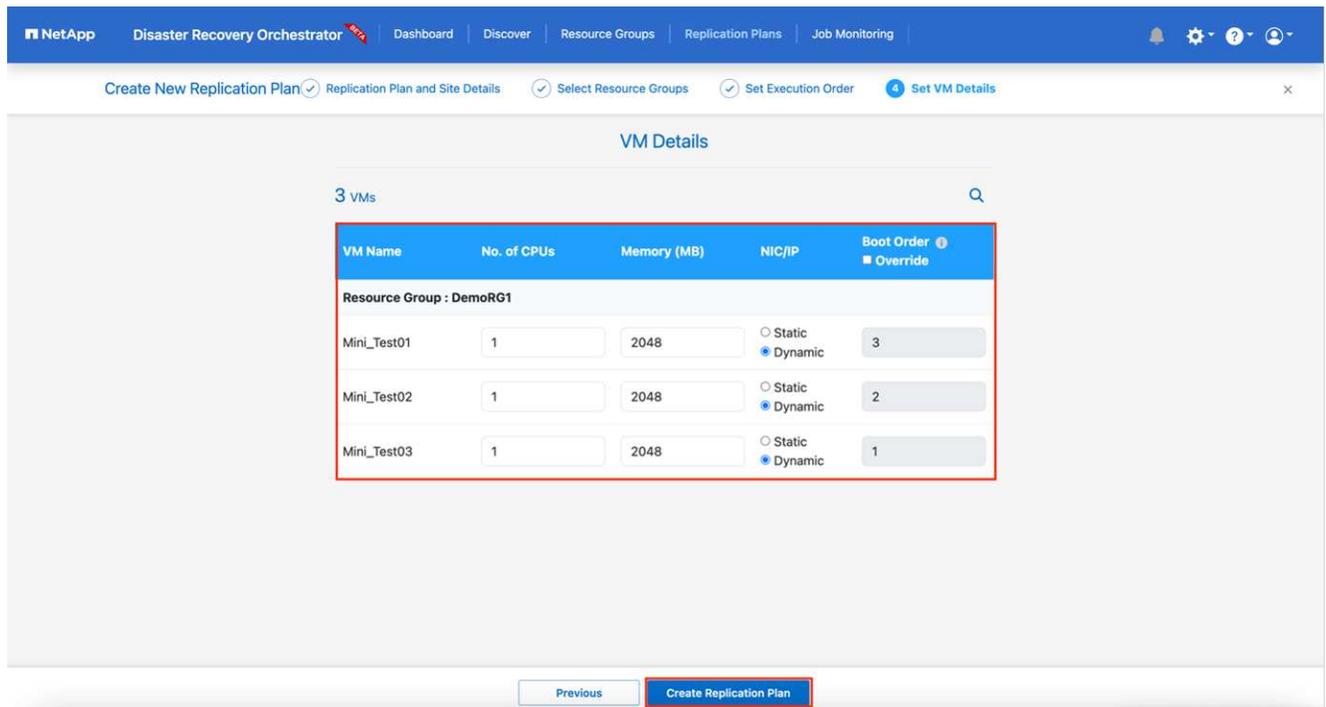
Source Resource	Destination Resource	
VLAN 3375	sddc-cgw-network-1	Delete

DataStore Mapping:

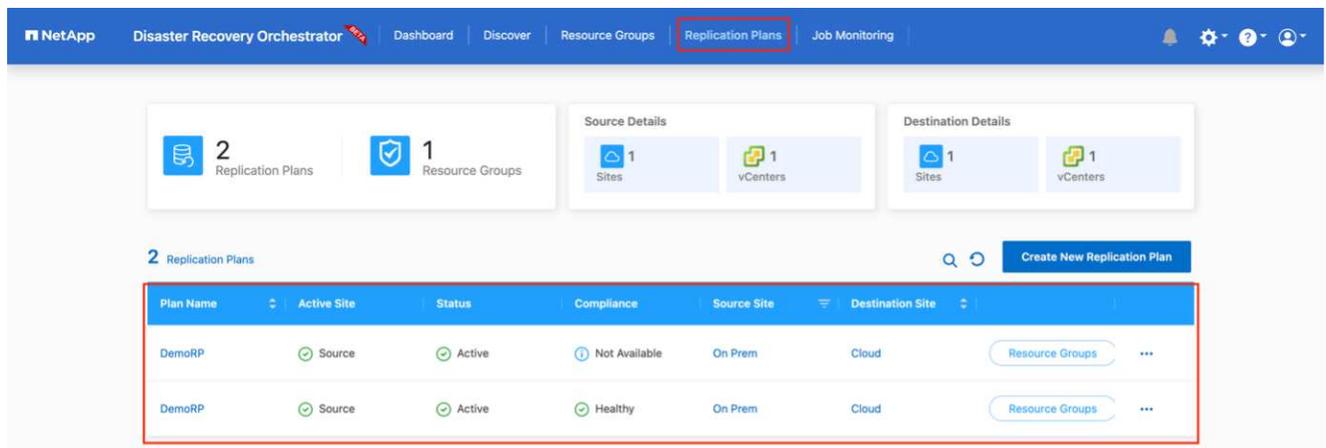
Source DataStore	Destination Volume
DRO_Mini	DRO_Mini_copy

At the bottom of the page, there are 'Previous' and 'Continue' buttons.

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**.

NetApp Disaster Recovery Orchestrator **NEW** Dashboard Discover Resource Groups Replication Plans Job Monitoring

2 Replication Plans 1 Resource Groups

Source Details: 1 Sites, 1 vCenters

Destination Details: 1 Sites, 1 vCenters

2 Replication Plans Create New Replication Plan

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource

- Plan Details
- Edit Plan
- Failover**
- Test Failover
- Migrate
- Run Compliance
- Delete Plan

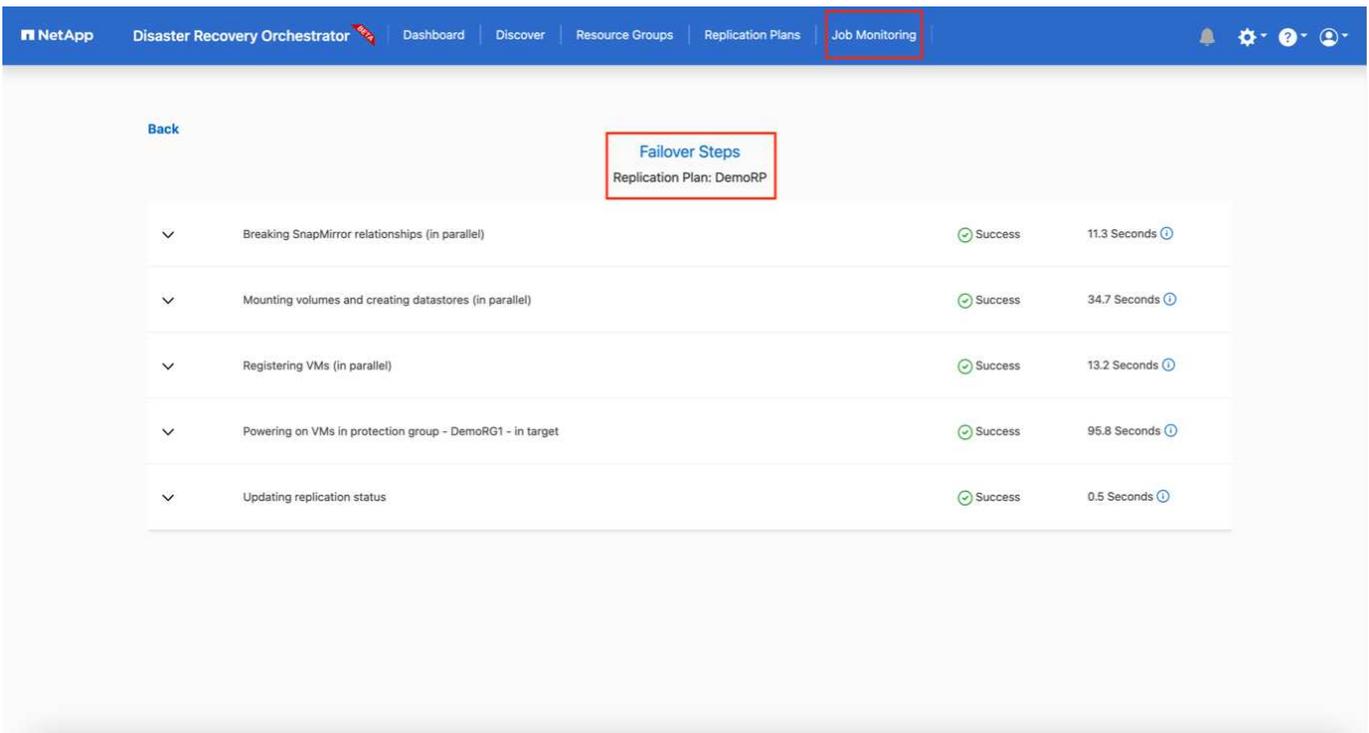
Failover Details

Volume Snapshot Details

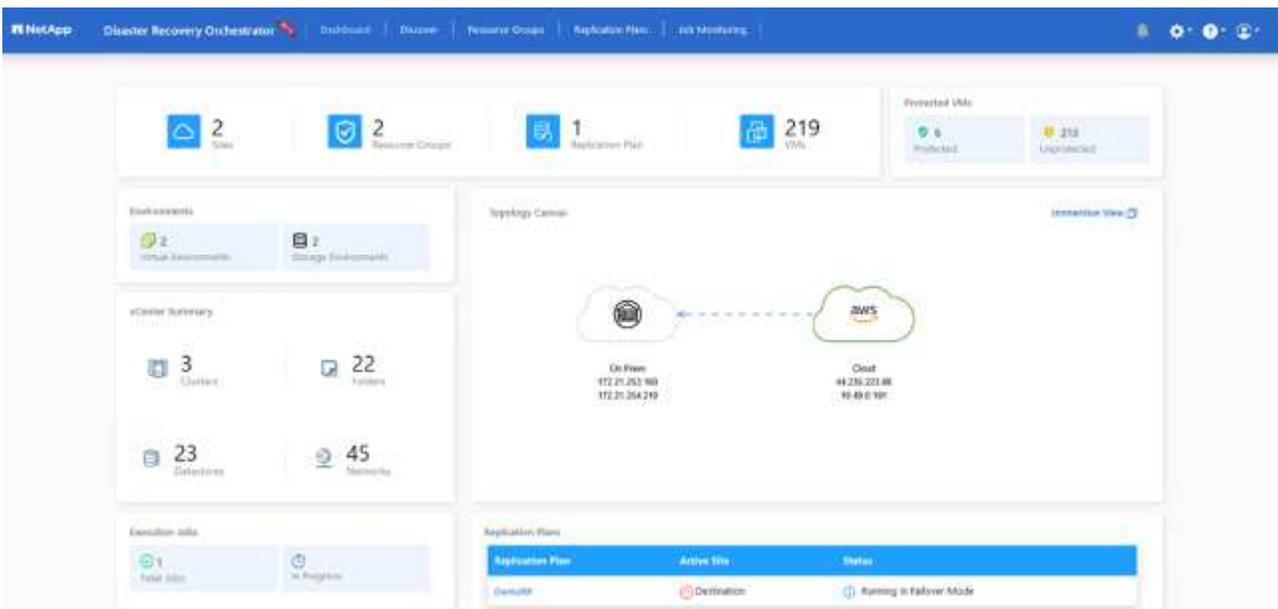
- Use latest snapshot i
- Select specific snapshot i

Start 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**.

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Destination	Running in Failover h	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details

- Reverse Data Sync
- Failback

Back

Reverse Data Sync Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in source	In progress
Reversing SnapMirror relationships (in parallel)	Initialized

Após a conclusão, você pode acionar o failback para retornar ao site de produção original.

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Destination	Active	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details

- Failback

NetApp Disaster Recovery Orchestrator Dashboard

Failback Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in target	In progress
Unregistering VMs in target (in parallel)	Initialized
Unmounting volumes in target (in parallel)	Initialized
Breaking reverse SnapMirror relationships (in parallel)	Initialized
Updating VM networks (in parallel)	Initialized
Powering on VMs in protection group - DemoRG1 - in source	Initialized
Deleting reverse SnapMirror relationships (in parallel)	Initialized
Resuming SnapMirror relationships to target (in parallel)	Initialized

No NetApp BlueXP, 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 ou de réplica. Em vez disso, ele faz uma cópia FlexClone da instância SnapMirror (ou Snapshot) necessária 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 réplica possam continuar mesmo durante testes de DR ou fluxos de trabalho de triagem. Além disso, esse processo garante que, se ocorrerem erros ou dados corrompidos forem recuperados, a recuperação poderá ser limpa sem o risco de a réplica ser destruída.

NetApp Disaster Recovery Orchestrator Dashboard

2 Sites

1 Resource Group

2 Replication Plans

219 VMs

Protected VMs

3 Protected

216 Unprotected

Environments

2 Virtual Environments

2 Storage Environments

Topology Canvas

vCenter Summary

3 Clusters

22 Folders

23 Datastores

45 Networks

Execution Jobs

3 Total Jobs

In Progress

Replication Plans

Replication Plan	Active Site	Status
DemoRP	Source	Active

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.

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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; 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 DESTES SOFTWARES, 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.