



Referência

NetApp Disaster Recovery

NetApp

February 04, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/data-services-disaster-recovery/reference/vcenter-privileges.html> on February 04, 2026. Always check docs.netapp.com for the latest.

Índice

Referência	1
Privilégios necessários do vCenter para NetApp Disaster Recovery	1
Alternar agentes do Console ao usar o NetApp Disaster Recovery	4
Antes de começar	4
Passos	4
Mais informações	5
Use a NetApp Disaster Recovery com o Amazon EVS	5
Introdução ao NetApp Disaster Recovery usando o Amazon Elastic VMware Service e o Amazon FSx for NetApp ONTAP	5
Visão geral da solução de NetApp Disaster Recovery usando Amazon EVS e Amazon FSs para NetApp ONTAP	6
Instalar o agente do NetApp Console para NetApp Disaster Recovery	8
Configurar o NetApp Disaster Recovery para Amazon EVS	8
Crie planos de replicação para o Amazon EVS	21
Execute operações de plano de replicação com o NetApp Disaster Recovery	34

Referência

Privilégios necessários do vCenter para NetApp Disaster Recovery

Para que o NetApp Disaster Recovery execute seus serviços, a conta vCenter deve ter um conjunto mínimo de privilégios vCenter. Esses privilégios incluem registrar e cancelar o registro de datastores, iniciar e parar máquinas virtuais (VMs) e reconfigurar VMs.

A tabela a seguir lista todos os privilégios necessários para que o NetApp Disaster Recovery interfira com um cluster vCenter.

Tipo	Nome do privilégio (vSphere cliente)	Nome do privilégio (API)	Descrição
Datastore	Datastore.Config	Configurar datastore	Permite configurar um datastore.
	Datastore.Delete	Remover datastore	Permite remover um repositório de dados.
	Datastore.Rename	Renomear datastore	Permite renomear um datastore.
Pasta	Folder.Create	Criar pasta	Permite criar uma nova pasta.
	Pasta.Delete	Excluir pasta	Permite excluir uma pasta. Requer privilégio tanto no objeto quanto em seu pai.
	Folder.Rename	Renomear pasta	Permite modificar o nome de uma pasta.
Rede	Network.Assign	Atribuir rede	Permite atribuir uma rede a uma VM.
	Network.Config	Configurar	Permite configurar uma rede.

Tipo	Nome do privilégio (vSphere cliente)	Nome do privilégio (API)	Descrição
Configuração de máquina virtual	VirtualMachine.Config.AdvancedConfig	Configuração avançada	Permite adicionar ou modificar parâmetros avançados no arquivo de configuração da VM.
	VirtualMachine.Config.Settings	Alterar configurações	Permite alterar as configurações gerais da máquina virtual.
	VirtualMachine.Config.CPUCount	Alterar contagem de CPU	Permite alterar o número de CPUs virtuais.
	VirtualMachine.Config.Memory	Alterar memória	Permite alterar a quantidade de memória alocada à VM.
	VirtualMachine.Config.Resource	Alterar recurso	Permite alterar a configuração de recursos dos nós de VM em um pool de recursos.
	VirtualMachine.Config.Rename	Renomear	Permite renomear uma VM ou modificar suas notas.
	VirtualMachine.Config.EditDevice	Modificar configurações do dispositivo	Permite alterar as propriedades de um dispositivo existente.
	VirtualMachine.Config.ReloadFromPath	Recarregar do caminho	Permite alterar o caminho de configuração de uma VM, preservando sua identidade.
	VirtualMachine.Config.ResetGuestInfo	Redefinir informações do convidado	Permite editar as informações do sistema operacional convidado para uma VM.
Convidado da máquina virtual	VirtualMachine.GuestOperations.ModifyAliases	Modificação do alias da operação guest	Permite modificar o alias da VM.
	VirtualMachine.GuestOperations.QueryAliases	Consulta de alias de operação de guest	Permite consultar o alias de uma VM.
	VirtualMachine.GuestOperations.Modificar	Modificações na operação do guest	Permite operações de modificação, incluindo transferir um arquivo para a VM.
	VirtualMachine.GuestOperations.Executar	Execução do programa de operação guest	Permite executar um aplicativo dentro da VM.
	VirtualMachine.GuestOperations.Consulta	Consultas de operações de guest	Permite consultar o sistema operacional convidado. As operações incluem listar arquivos.

Tipo	Nome do privilégio (vSphere cliente)	Nome do privilégio (API)	Descrição
Interação com máquina virtual	VirtualMachine.Interact.AnswerQuestion	Responder à pergunta	Permite resolver problemas durante transições de estado da máquina virtual ou erros de tempo de execução.
	VirtualMachine.Interact.PowerOff	Desligar	Permite desligar uma máquina virtual ligada.
	VirtualMachine.Interact.PowerOn	Ligar	Permite ligar ou retomar uma VM.
	VirtualMachine.Interact.ToolsInstall	Instalação do VMware Tools	Permite montar/desmontar o instalador do VMware Tools.
	VirtualMachine.Inventory.CreateFromExisting	Criar a partir de existente	Permite clonagem ou implantação de uma máquina virtual a partir de um modelo.
	VirtualMachine.Inventory.Create	Criar novo	Permite criar uma VM e alocar recursos.
	VirtualMachine.Inventory.Register	Cadastre-se	Permite adicionar uma VM existente a um inventário.
	VirtualMachine.Inventory.Delete	Remover	Permite excluir uma máquina virtual e seus arquivos. Requer privilégios tanto no objeto quanto em seu pai.
	VirtualMachine.Inventory.Unregister	Cancelar registro	Permite cancelar o registro de uma máquina virtual. Essa permissão requer privilégios tanto no objeto quanto em seu pai.
Provisionamento de máquina virtual	VirtualMachine.Provisioning.Clone	Clonagem de máquina virtual	Permite a clonagem de uma máquina virtual e a alocação de recursos.
	VirtualMachine.Provisioning.Personalização	Personalizar convidado	Permite a personalização do sistema operacional convidado da máquina virtual.
	VirtualMachine.Provisionamento.ModifyCustSpecs	Modificar especificação de personalização	Permite criar, modificar ou excluir especificações de personalização.
	VirtualMachine.Provisionamento.ReadCustSpecs	Leia as especificações de personalização	Permite a leitura de uma especificação de personalização para uma máquina virtual.
Configuração do serviço de máquina virtual	VirtualMachine.NameSpace.Query	Consultar configurações de serviço	Permite recuperar uma lista de serviços de VM.
	VirtualMachine.NameSpace.ReadContent	Leia a configuração do serviço	Permite recuperar a configuração de serviço da máquina virtual existente.

Tipo	Nome do privilégio (vSphere cliente)	Nome do privilégio (API)	Descrição
Instantâneo da máquina virtual	VirtualMachine.State.CreateSnapshot	Criar instantâneo	Permite criar um instantâneo do estado atual da máquina virtual.
	VirtualMachine.State.RemoveSnapshot	Remover snapshot	Permite remover um instantâneo.
	VirtualMachine.State.RenameSnapshot	Renomear snapshot	Permite renomear um snapshot ou atualizar sua descrição.
	VirtualMachine.State.RevertToSnapshot	Reverter para o snapshot	Permite reverter a máquina virtual para o estado de um determinado snapshot.

Alternar agentes do Console ao usar o NetApp Disaster Recovery

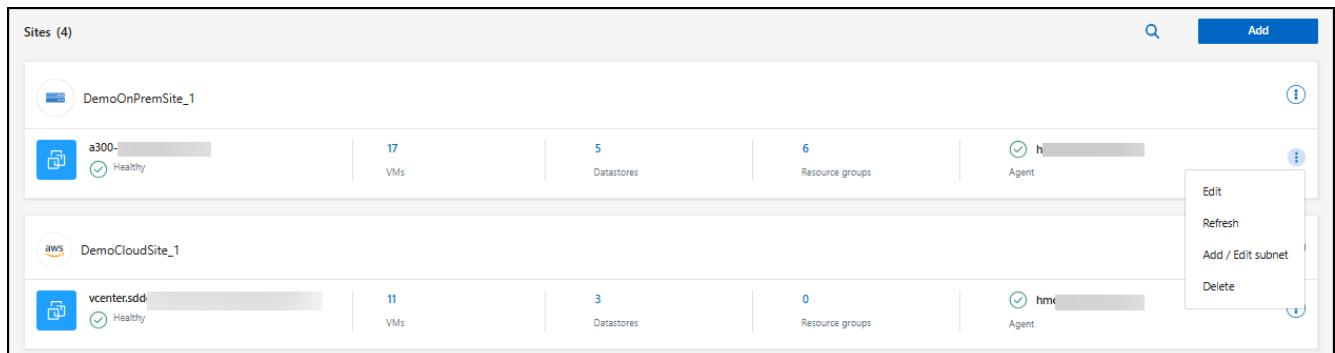
O NetApp Console suporta o uso de vários agentes de console em um único ambiente de trabalho. Utilizar vários agentes de console pode ser útil para manter o acesso aos recursos enquanto se realiza manutenção em outro agente de console ou caso um agente de console apresente falha. Como cada agente do Console possui um identificador único, a troca inadequada de agentes do Console pode comprometer a disponibilidade de recursos em um ambiente de trabalho.

Antes de começar

- Você deve ter [Adicionou pelo menos dois agentes de console ao seu ambiente de trabalho](#) .
- Ambos os agentes do Console devem conter os mesmos clusters ONTAP .

Passos

1. Em Recuperação de Desastres, selecione **Sites**.
2. Você precisa alterar o agente do console tanto para o vCenter de origem quanto para o de destino. Identifique os vCenters que deseja modificar. Selecione o menu de ações do vCenter e, em seguida, **Editar**.



3. Selecione o agente do console que deseja usar no menu suspenso e insira novamente seu nome de usuário e senha do vCenter. Selecione **Salvar**.

Edit vCenter server

Enter connection details for the vCenter server that is accessible from the Console Agent.

Site	Console Agent
DemoOnPremSite_1	hmcdraasconnector4
	ShivaOnPremConnDemo
	hmcdraasconnector4
	DRaaSTest
vCenter IP address	a300-vcsa06.ehcde.com
vCenter user name	
	vCenter password
<input checked="" type="checkbox"/> Use self-signed certificates <small>?</small>	
<input type="checkbox"/> Enable scheduled discovery	

Save **Cancel**

4. Repita os passos 2 e 3 para cada vCenter adicional que você deseja modificar.
5. No vCenter que você modificou, atualize-o para que o novo agente do Console seja detectado. Repita este passo para cada vCenter que você modificou.
6. Em Recuperação de Desastres, navegue até **Planos de replicação**.
7. Identifique os planos de replicação que deseja usar para retomar os fluxos de trabalho. Selecione o menu de ações ... Em seguida, **atualize os recursos**. Você pode acompanhar o status das tarefas em **Monitoramento de tarefas**.

Mais informações

- ["Saiba mais sobre os agentes do Console"](#)

Use a NetApp Disaster Recovery com o Amazon EVS

Introdução ao NetApp Disaster Recovery usando o Amazon Elastic VMware Service e o Amazon FSx for NetApp ONTAP

Cada vez mais, os clientes têm se tornado mais dependentes de infraestruturas virtualizadas para cargas de trabalho de computação de produção, como aquelas baseadas no VMware vSphere. À medida que essas máquinas virtuais (VMs) se

tornaram mais críticas para seus negócios, os clientes precisam protegê-las dos mesmos tipos de desastres que seus recursos de computação física. As soluções de recuperação de desastres (DR) oferecidas atualmente são complexas, caras e exigem muitos recursos. A NetApp, maior provedora de armazenamento usada para infraestruturas virtualizadas, tem interesse em garantir que as VMs de seus clientes sejam protegidas da mesma forma que protegemos dados hospedados em armazenamento ONTAP de qualquer tipo. Para atingir esse objetivo, a NetApp criou o serviço NetApp Disaster Recovery .

Um dos principais desafios de qualquer solução de DR é gerenciar o custo incremental de compra, configuração e manutenção de recursos adicionais de computação, rede e armazenamento apenas para fornecer uma infraestrutura de replicação e recuperação de DR. Uma opção popular para proteger recursos virtuais críticos no local é usar recursos virtuais hospedados na nuvem como infraestrutura de replicação e recuperação de DR. A Amazon é um exemplo de uma solução que pode fornecer recursos econômicos e compatíveis com infraestruturas de VM hospedadas NetApp ONTAP .

A Amazon lançou seu Amazon Elastic VMware Service (Amazon EVS), que habilita o VMware Cloud Foundation dentro de sua nuvem privada virtual (VPC). O Amazon EVS oferece a resiliência e o desempenho da AWS, juntamente com o software e as ferramentas familiares da VMware, permitindo que os Amazon EVS vCenters sejam integrados como uma extensão da sua infraestrutura virtualizada local.

Embora o Amazon EVS venha com recursos de armazenamento incluídos, o uso de armazenamento nativo pode reduzir sua eficácia para organizações com cargas de trabalho pesadas de armazenamento. Nesses casos, a combinação do Amazon EVS com o Amazon FSx for NetApp ONTAP (Amazon FSxN) pode fornecer uma solução de armazenamento mais flexível. Além disso, ao usar soluções de armazenamento NetApp ONTAP no local para hospedar sua infraestrutura VMware, usar o Amazon EVS com o FSx para ONTAP significa que você obtém os melhores recursos de proteção e interoperabilidade de dados entre suas infraestruturas no local e hospedadas na nuvem.

Para obter informações sobre o Amazon FSx for NetApp ONTAP, consulte "[Introdução ao Amazon FSx for NetApp ONTAP](#)" .

Visão geral da solução de NetApp Disaster Recovery usando Amazon EVS e Amazon FSs para NetApp ONTAP

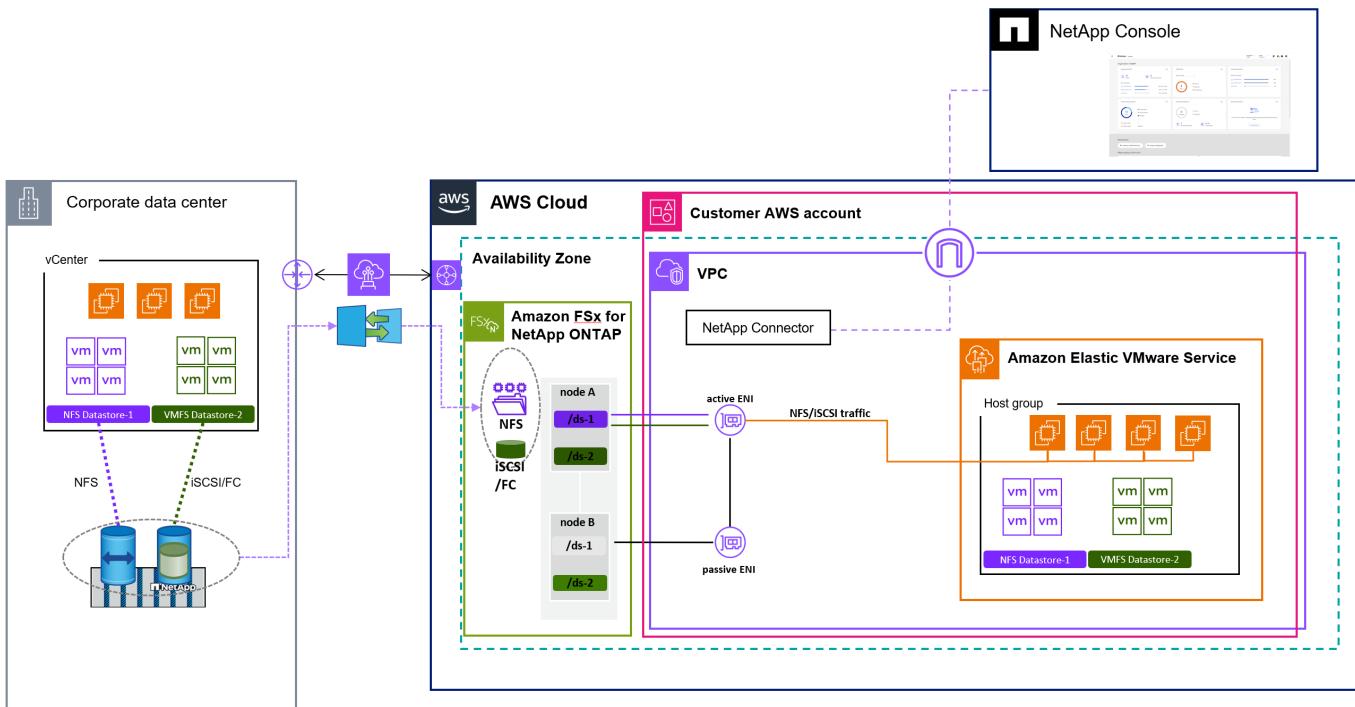
O NetApp Disaster Recovery é um serviço de valor agregado hospedado no ambiente de software como serviço do NetApp Console , que depende da arquitetura principal do NetApp Console . Vários componentes principais compõem o serviço DR para proteção do VMware no Console.

Para uma visão geral completa da solução NetApp Disaster Recovery , consulte "[Saiba mais sobre o NetApp Disaster Recovery para VMware](#)" .

Se você quiser proteger suas máquinas virtuais VMware locais hospedadas no Amazon AWS, use o serviço para fazer backup no Amazon EVS com o Amazon FSx for NetApp ONTAP .

A figura a seguir mostra como o serviço funciona para proteger suas VMs com o Amazon EVS.

Visão geral da NetApp Disaster Recovery usando Amazon EVS e FSx para ONTAP



1. O Amazon EVS é implantado em sua conta em uma única configuração de Zona de Disponibilidade (AZ) e dentro da sua Nuvem Privada Virtual (VPC).
2. Um sistema de arquivos FSx para ONTAP é implantado na mesma AZ que a implantação do Amazon EVS. O sistema de arquivos se conecta ao Amazon EVS diretamente por meio de uma Elastic Network Interface (ENI), uma conexão de peer VPC ou um AmazonTransit Gateway.
3. O agente do NetApp Console está instalado na sua VPC. O agente do NetApp Console hospeda vários serviços de gerenciamento de dados (chamados agentes), incluindo o agente NetApp Disaster Recovery que gerencia a recuperação de desastres da infraestrutura VMware em seus datacenters físicos locais e em seus recursos hospedados na Amazon AWS.
4. O agente NetApp Disaster Recovery se comunica com segurança com o serviço hospedado na nuvem do NetApp Console para receber tarefas e distribuir essas tarefas para as instâncias de armazenamento vCenter e ONTAP apropriadas no local e hospedadas na AWS.
5. Crie um plano de replicação usando o console de interface do usuário hospedado na nuvem do NetApp Console, indicando as VMs que devem ser protegidas, a frequência com que essas VMs devem ser protegidas e os procedimentos que precisam ser executados para reiniciar essas VMs no caso de um failover do site local.
6. O plano de replicação determina quais datastores do vCenter estão hospedando as VMs protegidas e os volumes ONTAP que estão hospedando esses datastores. Se ainda não houver volumes no cluster FSx for ONTAP, o NetApp Disaster Recovery os criará automaticamente.
7. Um relacionamento SnapMirror é criado para cada volume ONTAP de origem identificado para cada FSx de destino para o volume ONTAP hospedado no ONTAP e um cronograma de replicação é criado com base no RPO fornecido pelo usuário no plano de replicação.
8. Em caso de falha do site principal, um administrador inicia um processo de failover manual no NetApp Console e seleciona um backup para usar como ponto de restauração.
9. O agente NetApp Disaster Recovery ativa o FSx para volumes de proteção de dados hospedados no ONTAP.
10. O agente registra cada volume FSx for ONTAP ativado no Amazon EVS vCenter, registra cada VM protegida no Amazon EVS vCenter e inicia cada uma de acordo com as regras predefinidas contidas no

plano de replicação.

Instalar o agente do NetApp Console para NetApp Disaster Recovery

Um agente do NetApp Console permite que você conecte suas implantações do NetApp Console à sua infraestrutura para orquestrar soluções com segurança em ambientes AWS, Azure, Google Cloud ou locais. O agente do Console executa as ações que o NetApp Console precisa realizar para gerenciar sua infraestrutura de dados. O agente do Console consulta constantemente a camada de software como serviço NetApp Disaster Recovery em busca de quaisquer ações que precise executar.

Para NetApp Disaster Recovery, as ações executadas orquestram clusters VMware vCenter e instâncias de armazenamento ONTAP usando APIs nativas para cada serviço respectivo, a fim de fornecer proteção para VMs de produção em execução em um local on-premises. Embora o agente do Console possa ser instalado em qualquer local da sua rede, recomenda-se instalar o agente do Console no site de recuperação de desastres para NetApp Disaster Recovery. A instalação no site de recuperação de desastres garante que, em caso de falha do site primário, a interface do usuário do NetApp Console mantenha sua conexão com o agente do Console e possa orquestrar o processo de recuperação dentro desse site de recuperação de desastres.

Instalação

- Para usar o NetApp Disaster Recovery, instale o agente do NetApp Console no modo padrão. Para saber mais sobre os tipos de instalação do agente do NetApp Console, visite "[Saiba mais sobre os modos de implantação do NetApp Console](#)".

Os passos específicos de instalação do agente do Console dependem do seu tipo de implantação. Consulte "[Saiba mais sobre os agentes do Console](#)" para mais informações.



O método mais simples para instalar o agente do Console com Amazon AWS é usar o AWS Marketplace. Para obter detalhes sobre a instalação do agente do Console usando o AWS Marketplace, consulte "[Crie um agente do NetApp Console a partir do AWS Marketplace](#)".

Configurar o NetApp Disaster Recovery para Amazon EVS

Visão geral da configuração do NetApp Disaster Recovery para Amazon EVS

Depois de instalar o agente do NetApp Console, você precisa integrar todos os recursos de armazenamento ONTAP e VMware vCenter que participarão do processo de recuperação de desastres com o NetApp Disaster Recovery.

- "[Pré-requisitos para Amazon EVS com NetApp Disaster Recovery](#)"
- "[Adicionar matrizes de armazenamento ONTAP ao NetApp Disaster Recovery](#)"
- "[Habilitar a NetApp Disaster Recovery para Amazon EVS](#)"
- "[Adicionar sites do vCenter ao NetApp Disaster Recovery](#)"
- "[Adicionar clusters do vCenter ao NetApp Disaster Recovery](#)"

Pré-requisitos para Amazon EVS com NetApp Disaster Recovery

Certifique-se de revisar e atender aos requisitos para configurar Amazon EVS com NetApp Disaster Recovery.

Pré-requisitos

- Revise o "[Pré-requisitos gerais para NetApp Disaster Recovery](#)".
- Crie uma conta de usuário do vCenter com os privilégios específicos do VMware necessários para que o NetApp Disaster Recovery execute as operações necessárias.



É recomendável que você **não** utilize a conta de administrador padrão "administrator@vsphere.com". Em vez disso, você deve criar uma conta de usuário específica do NetApp Disaster Recovery em todos os clusters vCenter que participarão do processo de recuperação de desastres. Para obter uma lista dos privilégios específicos necessários, consulte "[Privilégios do vCenter necessários para NetApp Disaster Recovery](#)".

- Certifique-se de que todos os datastores do vCenter que hospedarão VMs protegidas pela NetApp Disaster Recovery estejam localizados em recursos de storage NetApp ONTAP.

O Disaster Recovery oferece suporte a NFS e VMFS em iSCSI (e não FC) ao usar Amazon FSx no NetApp ONTAP. Embora o Disaster Recovery ofereça suporte a FC, Amazon FSx for NetApp ONTAP não oferece.

- Certifique-se de que seu Amazon Exchange Virtual Server vCenter está conectado a um Amazon FSx for NetApp ONTAP storage cluster.
- Certifique-se de que as ferramentas VMware estejam instaladas em todas as VMs protegidas.
- Certifique-se de que sua rede local esteja conectada à sua rede VPC da AWS usando um método de conexão aprovado pela Amazon. Recomenda-se o uso de AWS Direct Connect, AWS Private Link ou AWS Site-to-Site VPN.
- Analisar e garantir a conformidade com os requisitos de conexão e porta para Exchange Virtual Server com NetApp Disaster Recovery:

Fonte	Destino	Porta	Detalhes
Amazon FSxN	ONTAP local	TCP 11104, 11105, ICMP	SnapMirror
ONTAP local	Amazon FSxN	TCP 11104, 11105, ICMP	SnapMirror
Agente do NetApp Console	ONTAP local	TCP 443, somente ICMP	Chamadas de API
Agente do NetApp Console	Amazon FSxN	TCP 441, somente ICMP	Chamadas de API
Agente do NetApp Console	vCenter (local, Exchange Virtual Server), host ESXi (local, Exchange Virtual Server)	443	Chamadas de API, execução de script

Adicione matrizes locais ao sistema NetApp Console para Amazon EVS com NetApp Disaster Recovery

Antes de usar o NetApp Disaster Recovery, você deve adicionar instâncias de

armazenamento locais e hospedadas na nuvem ao sistema NetApp Console .

Você precisa fazer o seguinte:

- Adicione matrizes locais ao seu sistema NetApp Console .
- Adicione instâncias do Amazon FSx for NetApp ONTAP (FSx para ONTAP) ao seu sistema NetApp Console .

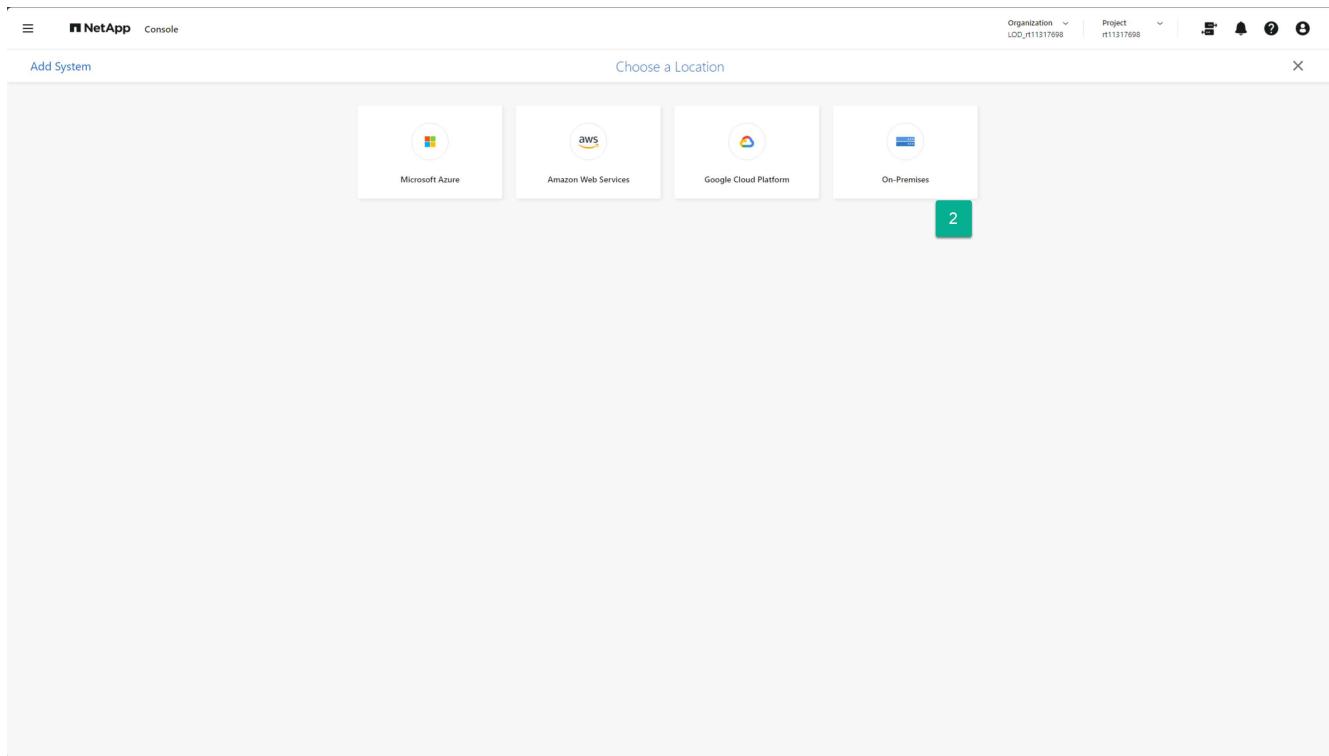
Adicionar matrizes de armazenamento locais ao sistema NetApp Console

Adicione recursos de armazenamento ONTAP local ao seu sistema NetApp Console .

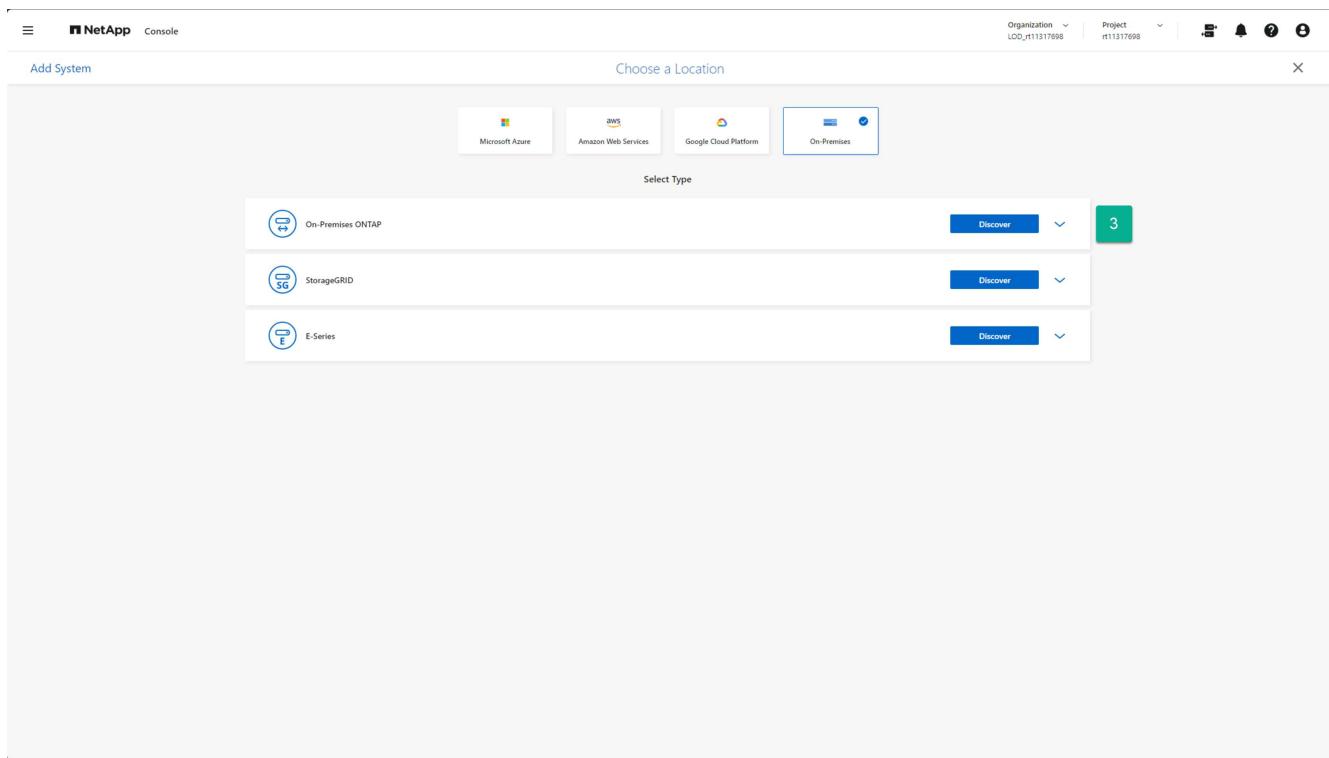
1. Na página Sistemas do NetApp Console , selecione **Adicionar sistema**.

The screenshot shows the 'Systems' page in the NetApp Console. On the left, there's a sidebar with 'Management' and 'Discoverable systems' sections, and a central area with a '+ Add' button and a count of '1'. Below this, two cloud icons represent clusters: 'cluster2' (On-Premises ONTAP, 210.23GB Capacity) and 'cluster1' (On-Premises ONTAP, 210.23GB Capacity). On the right, a table view shows a single row for 'cluster1' with a count of '2', '420.47 GiB' capacity, and 'On-Premises ONTAP' type. The top right corner shows 'Organization: LDD_r11317698' and 'Project: rt11317698'.

2. Na página Adicionar sistema, selecione o cartão **On-Premises**.



3. Selecione **Discover** no cartão On-Premises ONTAP .



4. Na página Descobrir Cluster, insira as seguintes informações:

- O endereço IP da porta de gerenciamento do cluster do array ONTAP
- O nome de usuário do administrador
- A senha do administrador

5. Selecione **Descobrir** na parte inferior da página.

ONTAP Cluster IP

User Name

Password

Discover

6. Repita as etapas 1 a 5 para cada matriz ONTAP que hospedará os armazenamentos de dados do vCenter.

Adicionar instâncias de armazenamento do Amazon FSx for NetApp ONTAP ao sistema NetApp Console

Em seguida, adicione um Amazon FSx for NetApp ONTAP ao seu sistema NetApp Console .

1. Na página Sistemas do NetApp Console , selecione **Adicionar sistema**.

Systems	Enable Services
2 On-Premises ONTAP	420.47 GiB Provisioned Capacity

cluster2
On-Premises ONTAP
210.23GiB
Capacity

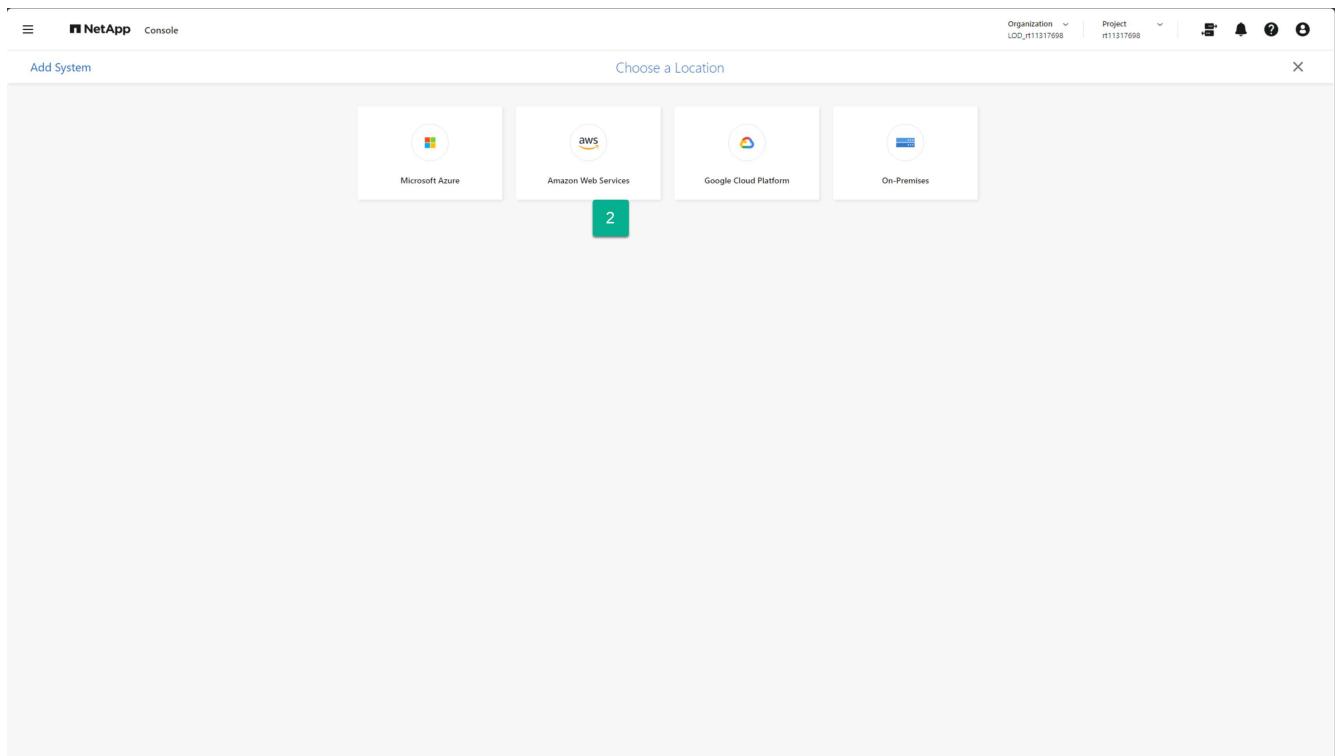
cluster1
On-Premises ONTAP
210.23GiB
Capacity

Table view

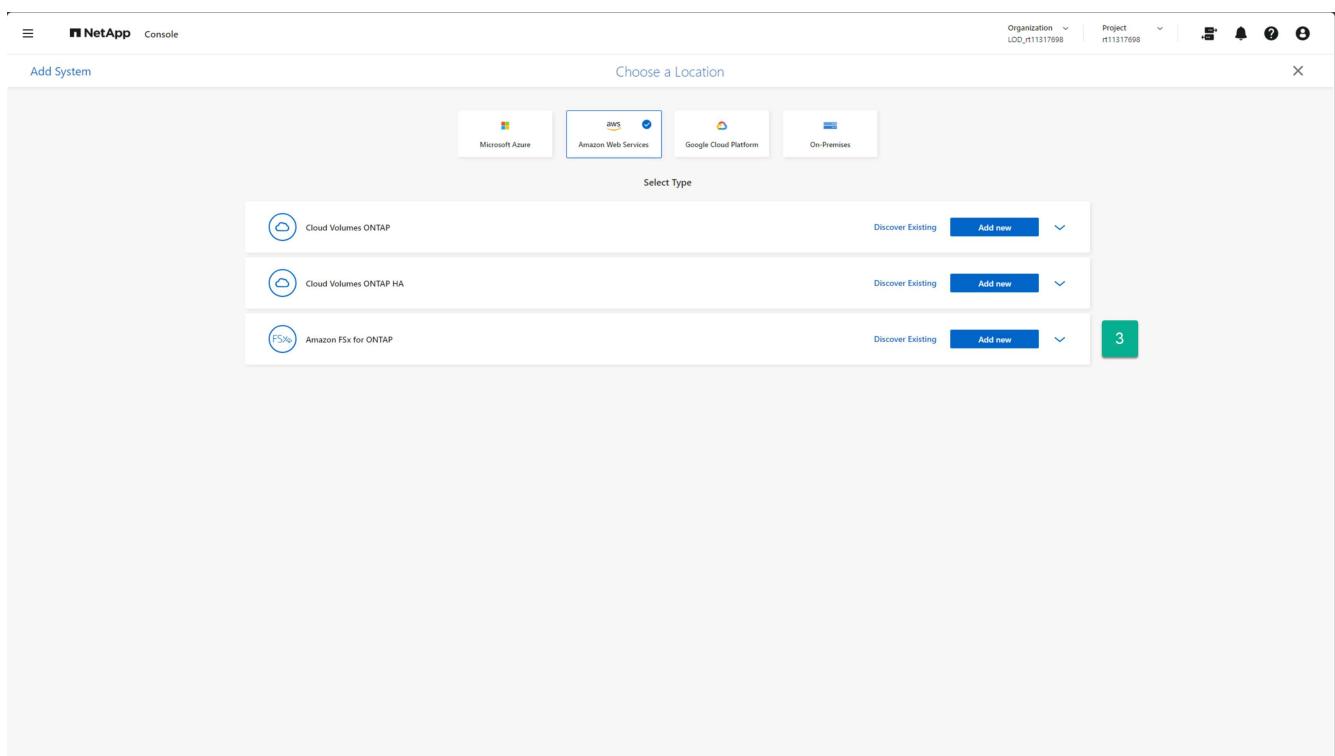
List view

+

2. Na página Adicionar sistema, selecione o cartão **Amazon Web Services**.



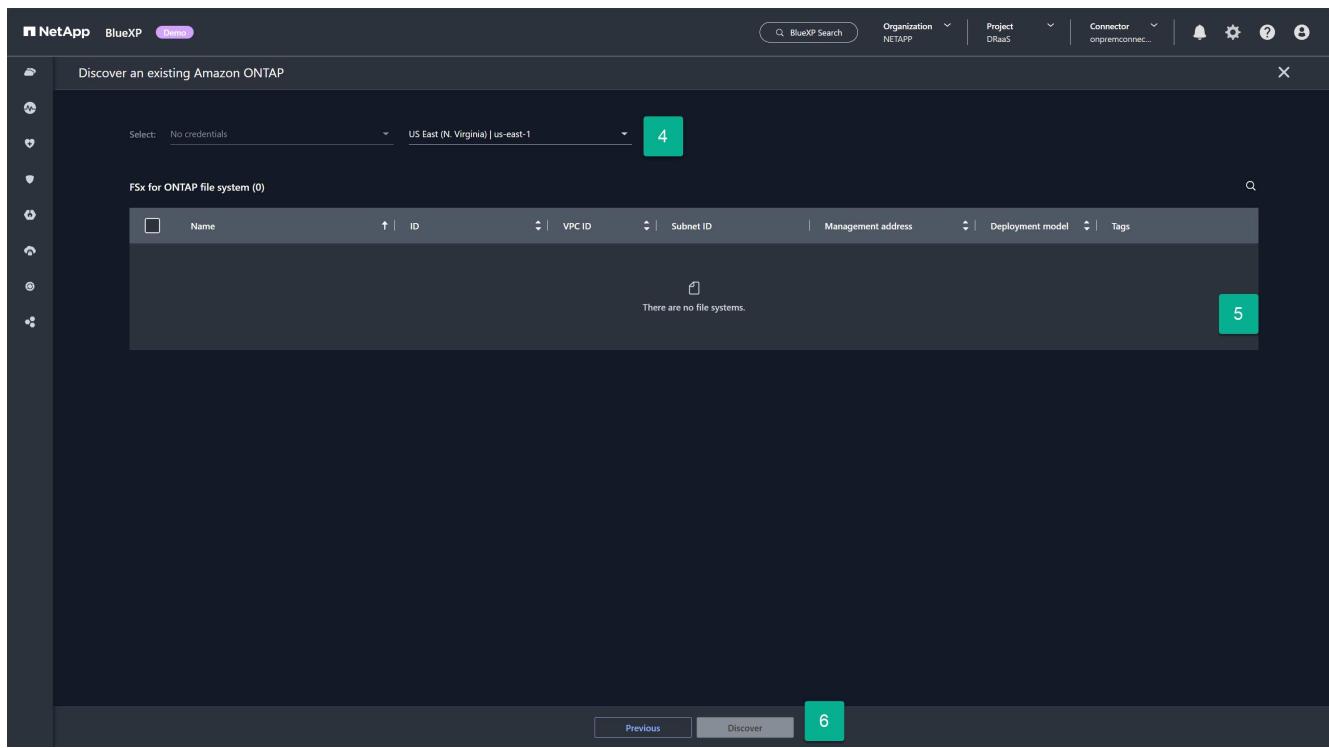
3. Selecione o link **Descobrir existente** no cartão Amazon FSx para ONTAP .



4. Selecione as credenciais e a região da AWS que hospeda a instância do FSx para ONTAP .

5. Selecione um ou mais sistemas de arquivos FSx para ONTAP a serem adicionados.

6. Selecione **Descobrir** na parte inferior da página.



7. Repita as etapas 1 a 6 para cada instância do FSx for ONTAP que hospedará os armazenamentos de dados do vCenter.

Adicione o serviço NetApp Disaster Recovery à sua conta do NetApp Console para Amazon EVS

O NetApp Disaster Recovery é um produto licenciado que deve ser adquirido antes de poder ser usado. Existem vários tipos de licenças e várias maneiras de adquiri-las. Uma licença lhe dá o direito de proteger uma quantidade específica de dados por um período de tempo específico.

Para obter mais informações sobre as licenças do NetApp Disaster Recovery , consulte "[Configurar licenciamento para NetApp Disaster Recovery](#)" .

Tipos de licença

Existem dois tipos principais de licença:

- A NetApp oferece uma "[Licença de teste de 30 dias](#)" que você pode usar para avaliar o NetApp Disaster Recovery usando seus recursos ONTAP e VMware. Esta licença fornece 30 dias de uso para uma quantidade ilimitada de capacidade protegida.
- Compre uma licença de produção se quiser proteção de DR além do período de teste de 30 dias. Esta licença pode ser adquirida nos marketplaces de qualquer um dos parceiros de nuvem da NetApp, mas para este guia, recomendamos que você compre sua licença de marketplace para o NetApp Disaster Recovery usando o Amazon AWS Marketplace. Para saber mais sobre como comprar uma licença através do Amazon Marketplace, consulte "[Assine pelo AWS Marketplace](#)" .

Dimensione suas necessidades de capacidade de recuperação de desastres

Antes de comprar sua licença, você deve entender quanta capacidade de armazenamento ONTAP você precisa proteger. Uma das vantagens de usar o armazenamento NetApp ONTAP é a alta eficiência com que a NetApp armazena seus dados. Todos os dados armazenados em um volume ONTAP — como VMs que

hospedam datastore VMware — são armazenados de maneira altamente eficiente. O ONTAP adota três tipos de eficiência de armazenamento por padrão ao gravar dados no armazenamento físico: compactação, desduplicação e compressão. O resultado líquido é uma eficiência de armazenamento entre 1,5:1 e 4:1, dependendo dos tipos de dados armazenados. Na verdade, a NetApp oferece uma "[garantia de eficiência de armazenamento](#)" para determinadas cargas de trabalho.

Isso pode ser benéfico para você porque o NetApp Disaster Recovery calcula a capacidade para fins de licenciamento depois que todas as eficiências de armazenamento do ONTAP são aplicadas. Por exemplo, digamos que você provisionou um armazenamento de dados NFS de 100 terabytes (TiB) no vCenter para hospedar 100 VMs que você deseja proteger usando o serviço. Além disso, vamos supor que quando os dados são gravados no volume ONTAP, as técnicas de eficiência de armazenamento aplicadas automaticamente resultam no consumo de apenas 33 TiB por essas VMs (eficiência de armazenamento de 3:1). O NetApp Disaster Recovery precisa ser licenciado apenas para 33 TiB, não 100 TiB. Isso pode ser um benefício muito grande para o custo total de propriedade da sua solução de DR quando comparado a outras soluções de DR.

Passos

1. Para determinar a quantidade de dados que está sendo consumida em cada volume que hospeda um armazenamento de dados VMware a ser protegido, determine o consumo de capacidade no disco executando o comando ONTAP CLI para cada volume: `volume show-space -volume < volume name > -vserver < SVM name >`.

Por exemplo:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature           Used      Used%
-----  -----
User Data          163.4MB   3%
Filesystem Metadata    172KB   0%
Inodes             2.93MB   0%
Snapshot Reserve   292.9MB   5%
Total Metadata     185KB   0%
Total Used         459.4MB   8%
Total Physical Used 166.4MB   3%
```

2. Anote o valor **Total Físico Usado** para cada volume. Essa é a quantidade de dados que o NetApp Disaster Recovery precisa proteger e é o valor que você usará para determinar quanta capacidade precisa licenciar.

Adicionar sites no NetApp Disaster Recovery para Amazon EVS

Antes de proteger sua infraestrutura de VM, identifique quais clusters do VMware vCenter estão hospedando as VMs a serem protegidas e onde esses vCenters estão localizados. O primeiro passo é criar um site para representar os datacenters de origem e destino. Um site é um domínio de falha ou um domínio de recuperação.

Você precisa criar o seguinte:

- Um site para representar cada datacenter de produção onde seus clusters vCenter de produção residem
- Um site para seu datacenter em nuvem Amazon EVS/ Amazon FSx for NetApp ONTAP

Crie sites locais

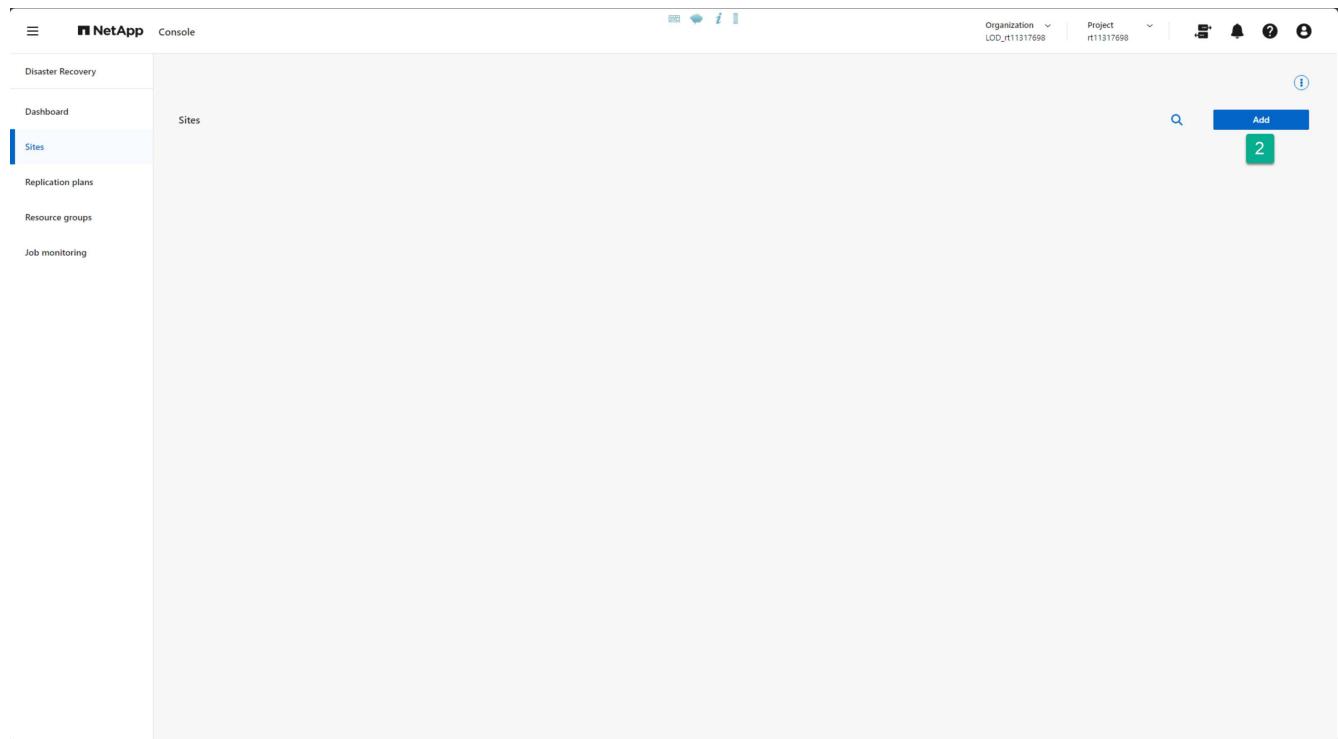
Crie um site de produção do vCenter.

Passos

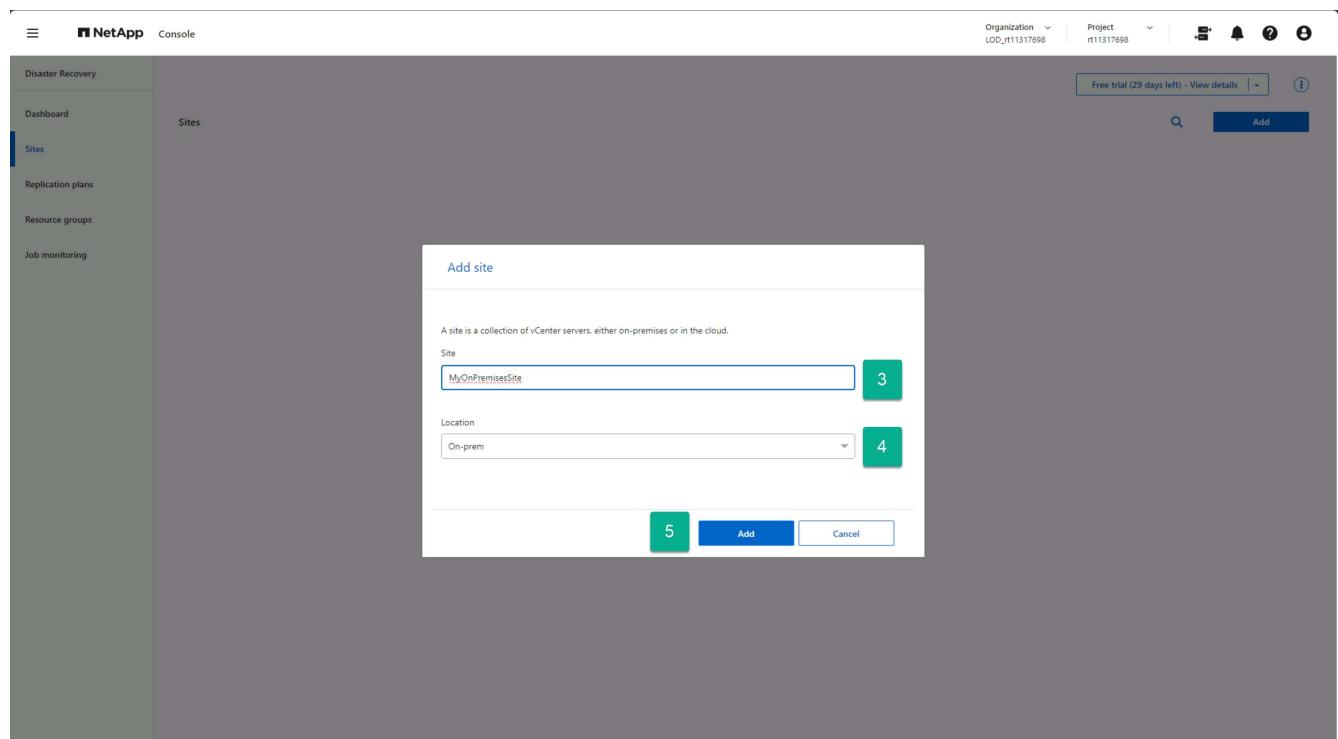
1. Na barra de navegação esquerda do NetApp Console , selecione **Proteção > Recuperação de desastres**.
2. Em qualquer página do NetApp Disaster Recovery, selecione a opção **Sites**.

The screenshot shows the NetApp Disaster Recovery console interface. On the left, a vertical sidebar lists navigation options: Dashboard (selected), Sites (highlighted with a green box), Replication plans, Resource groups, and Job monitoring. The main content area is titled 'Sites (0)' and includes sections for 'View sites', 'Replication plans (0)', and 'Activity (Last 12 hours)'. Below these are detailed counts for various states: Running (0), Down (0), Issue (0) for sites; Ready (0), Failed (0) for replication plans; and 0 for Resource groups, Protected VMs, Unprotected VMs, Failovers, Failbacks, Test failovers, and Migrations.

3. Na opção Sites, selecione **Adicionar**.



4. Na caixa de diálogo Adicionar site, forneça um nome de site.
5. Selecione “No local” como local.
6. Selecione **Adicionar**.



Se você tiver outros sites de produção do vCenter, poderá adicioná-los usando as mesmas etapas.

Crie sites na nuvem da Amazon

Crie um site de DR para o Amazon EVS usando o Amazon FSx for NetApp ONTAP .

1. Em qualquer página do NetApp Disaster Recovery, selecione a opção **Sites**.

The screenshot shows the NetApp Disaster Recovery console interface. On the left, a sidebar menu includes 'Dashboard', 'Sites' (which is selected and highlighted with a green box labeled '1'), 'Replication plans', 'Resource groups', and 'Job monitoring'. The main content area is divided into several sections: 'Sites (0)' with 'View sites' button, 'Replication plans (0)' with 'View plans' button, and 'Activity (Last 12 hours)' with 'View all jobs' button. Below these are three rows of status indicators: 'Running' (0), 'Down' (0), 'Issue' (0) under 'Sites'; 'Ready' (0), 'Failed' (0) under 'Replication plans'; and 'Resource groups' (0), 'Protected VMs' (0), 'Unprotected VMs' (0) under 'Activity'.

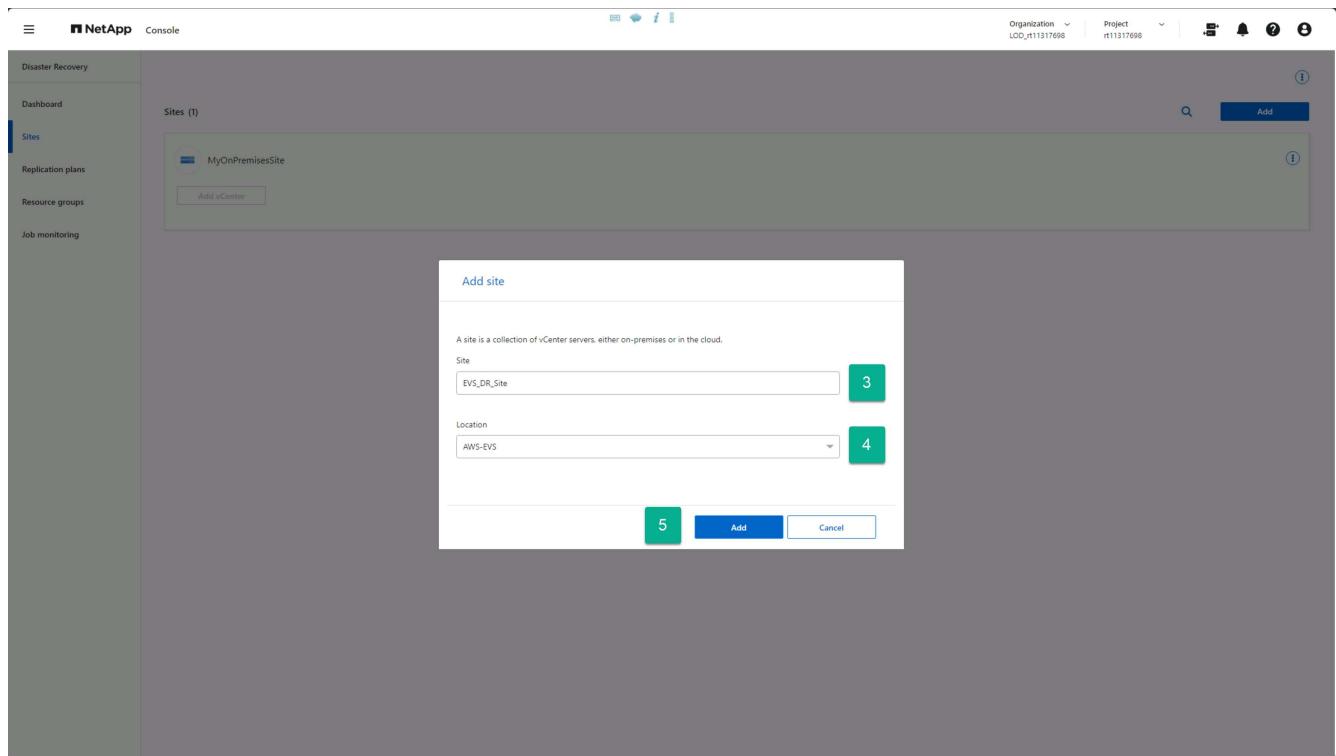
2. Na opção Sites, selecione **Adicionar**.

The screenshot shows the 'Add Site' dialog box. It has a search bar at the top right and a large blue 'Add' button on the right side. In the center, there is a list with one item: 'MyOnPremisesSite'. Below the list is a button labeled 'Add vCenter'.

3. Na caixa de diálogo Adicionar site, forneça um nome de site.

4. Selecione "AWS-EVS" como Local.

5. Selecione **Adicionar**.



Resultado

Agora você tem um site de produção (origem) e um site de DR (destino) criados.

Adicionar clusters locais e do Amazon EVS vCenter no NetApp Disaster Recovery

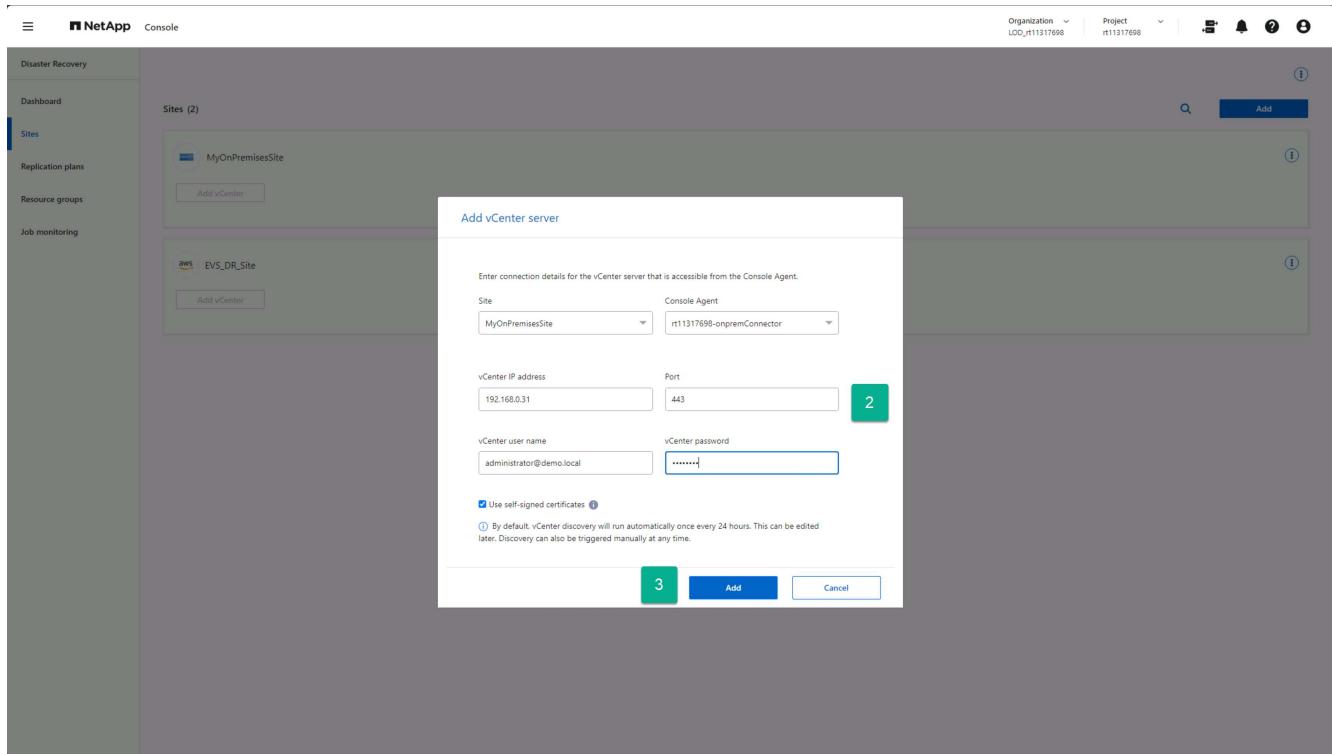
Com os sites criados, agora você adiciona seus clusters do vCenter a cada site no NetApp Disaster Recovery. Quando criamos cada site, indicamos cada tipo de site. Isso informa ao NetApp Disaster Recovery qual tipo de acesso é necessário para os vCenters hospedados em cada tipo de site. Uma das vantagens do Amazon EVS é que não há diferenciação real entre um Amazon EVS vCenter e um vCenter local. Ambos exigem as mesmas informações de conexão e autenticação.

Etapas para adicionar um vCenter a cada site

1. Na opção **Sites**, selecione **Adicionar vCenter** para o site desejado.

The screenshot shows the NetApp Console interface. On the left, there's a sidebar with options: Disaster Recovery, Dashboard, Sites (selected), Replication plans, Resource groups, and Job monitoring. The main area is titled 'Sites (2)' and lists two entries: 'MyOnPremisesSite' and 'EVS_DR_Site'. Each entry has a small icon (blue square for MyOnPremisesSite, AWS logo for EVS_DR_Site), the name, and a green '1' indicating one entry. Below each name is a blue 'Add vCenter' button. At the top right, there are buttons for Organization (LOD_111317698), Project (rt11317698), and various notifications.

2. Na caixa de diálogo Adicionar servidor vCenter, selecione ou forneça as seguintes informações:
 - a. O agente do NetApp Console hospedado na sua VPC da AWS.
 - b. O endereço IP ou FQDN do vCenter a ser adicionado.
 - c. Se for diferente, altere o valor da porta para a porta TCP usada pelo gerenciador de cluster do vCenter.
 - d. O nome de usuário do vCenter para a conta criada anteriormente que será usada pelo NetApp Disaster Recovery para gerenciar o vCenter.
 - e. A senha do vCenter para o nome de usuário fornecido.
 - f. Se sua empresa usa uma Autoridade de Certificação (CA) externa ou o vCenter Endpoint Certificate Store para obter acesso aos seus vCenters, desmarque a caixa de seleção **Usar certificados autoassinados**. Caso contrário, deixe a caixa marcada.
3. Selecione **Adicionar**.



Crie planos de replicação para o Amazon EVS

Criar planos de replicação na visão geral do NetApp Disaster Recovery

Depois de ter vCenters para proteger no site local e ter um site Amazon EVS configurado para usar o Amazon FSx for NetApp ONTAP que você pode usar como um destino de DR, você pode criar um plano de replicação (RP) para proteger qualquer conjunto de VMs hospedadas no cluster vCenter dentro do seu site local.

Para iniciar o processo de criação do plano de replicação:

1. Em qualquer tela do NetApp Disaster Recovery , selecione a opção **Planos de replicação**.

The screenshot shows the NetApp Console interface. On the left, there is a navigation sidebar with options: Disaster Recovery, Dashboard, Sites (selected), Replication plans (with a green box labeled '1'), Resource groups, and Job monitoring. The main content area is titled 'Sites (2)' and lists two sites:

Site	IP Address	Status	VMs	Datastores	Resource groups	Connector
MyOnPremisesSite	192.168.0.31	Healthy	3	3	0	rt11317698-onpremConnector
EVS_DR_Site	192.168.0.32	Healthy	1	3	0	rt11317698-onpremConnector

2. Na página Planos de replicação, selecione **Adicionar**.

The screenshot shows the NetApp Console interface. On the left, there is a navigation sidebar with options: Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main content area is titled 'Replication plans' and shows a table with one row:

Name	Compliance status	Plan status	Protected site	Resource groups	Fallover site
No data					

Isso abre o assistente Criar plano de replicação.

Continuar com "[Assistente para criação de plano de replicação Etapa 1](#)".

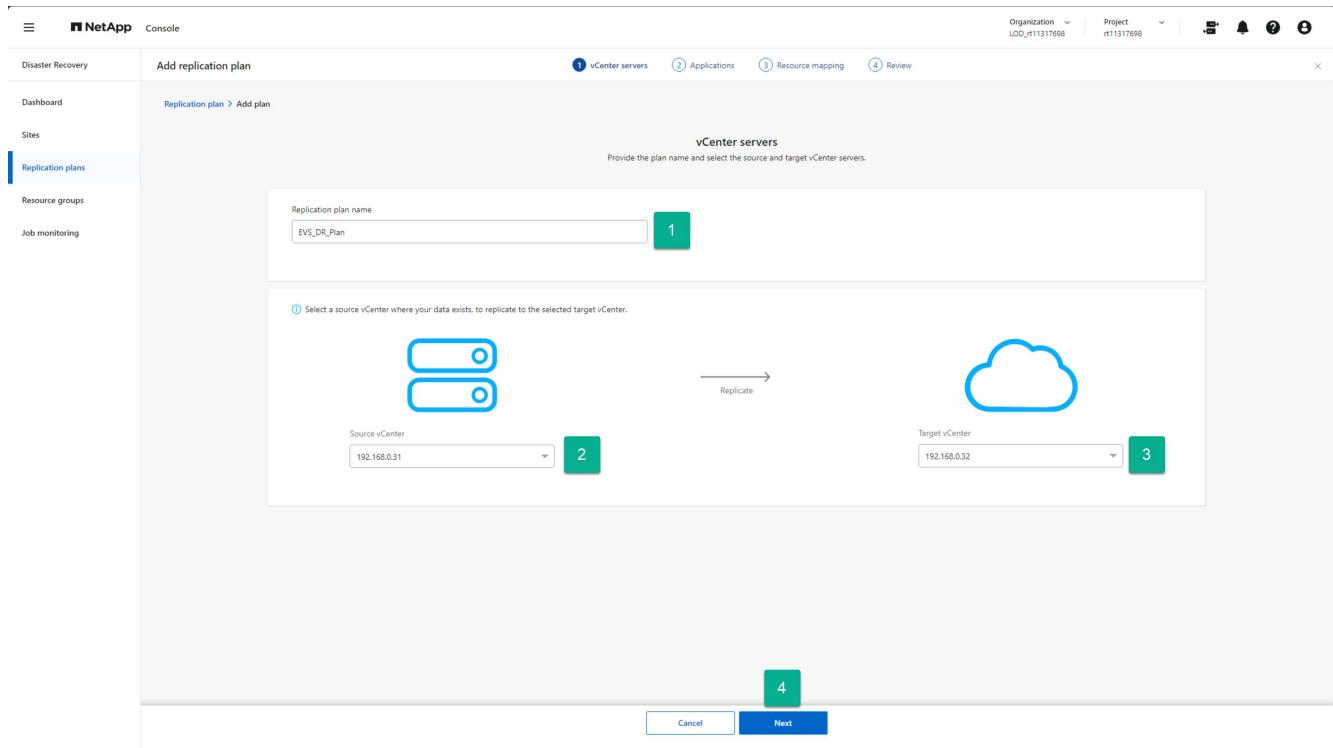
Crie um plano de replicação: Etapa 1 - Selecione vCenters no NetApp Disaster Recovery

Primeiro, usando o NetApp Disaster Recovery, forneça um nome de plano de replicação e selecione os vCenters de origem e destino para a replicação.

1. Insira um nome exclusivo para o plano de replicação.

Somente caracteres alfanuméricos e sublinhados (_) são permitidos para nomes de planos de replicação.

2. Selecione um cluster vCenter de origem.
3. Selecione um cluster vCenter de destino.
4. Selecione **Avançar**.



Continuar com "[Assistente para criar plano de replicação Etapa 2](#)" .

Criar um plano de replicação: Etapa 2 - Selecionar recursos de VM no NetApp Disaster Recovery

Selecione as máquinas virtuais a serem protegidas usando o NetApp Disaster Recovery.

Existem várias maneiras de selecionar VMs para proteção:

- **Selecionar VMs individuais:** clicar no botão **Máquinas virtuais** permite que você selecione VMs individuais para proteger. Conforme você seleciona cada VM, o serviço a adiciona a um grupo de recursos padrão localizado no lado direito da tela.
- **Selecionar grupos de recursos criados anteriormente:** Você pode criar grupos de recursos personalizados com antecedência usando a opção Grupo de recursos no menu NetApp Disaster Recovery . Isso não é um requisito, pois você pode usar os outros dois métodos para criar um grupo de recursos como parte do processo de plano de replicação. Para obter detalhes, consulte "[Crie um plano de replicação](#)".

- Selecionar datastores inteiros do vCenter:** se você tiver muitas VMs para proteger com este plano de replicação, pode não ser tão eficiente selecionar VMs individuais. Como o NetApp Disaster Recovery usa replicação SnapMirror baseada em volume para proteger as VMs, todas as VMs que residem em um armazenamento de dados serão replicadas como parte do volume. Na maioria dos casos, você deve fazer com que o NetApp Disaster Recovery proteja e reinicie quaisquer VMs localizadas no armazenamento de dados. Use esta opção para informar ao serviço para adicionar quaisquer VMs hospedadas em um armazenamento de dados selecionado à lista de VMs protegidas.

Para esta instrução guiada, selecionamos todo o armazenamento de dados do vCenter.

Passos para acessar esta página

- Na página **Plano de replicação**, continue para a seção **Aplicativos**.
- Revise as informações na página **Inscrições** que é aberta.

Etapas para selecionar o armazenamento de dados ou armazenamentos de dados:

- Selecione **Datastores**.
- Marque as caixas de seleção ao lado de cada armazenamento de dados que você deseja proteger.
- (Opcionalmente) Renomeie o grupo de recursos para um nome adequado selecionando o ícone de lápis ao lado do nome do grupo de recursos.
- Selecione **Avançar**.

Continuar com "[Assistente para criar plano de replicação Etapa 3](#)" .

Criar um plano de replicação: Etapa 3 - Mapear recursos no NetApp Disaster Recovery

Depois de ter uma lista de VMs que você deseja proteger usando o NetApp Disaster Recovery, forneça o mapeamento de failover e as informações de configuração da VM para usar durante um failover.

Você precisa mapear quatro tipos principais de informações:

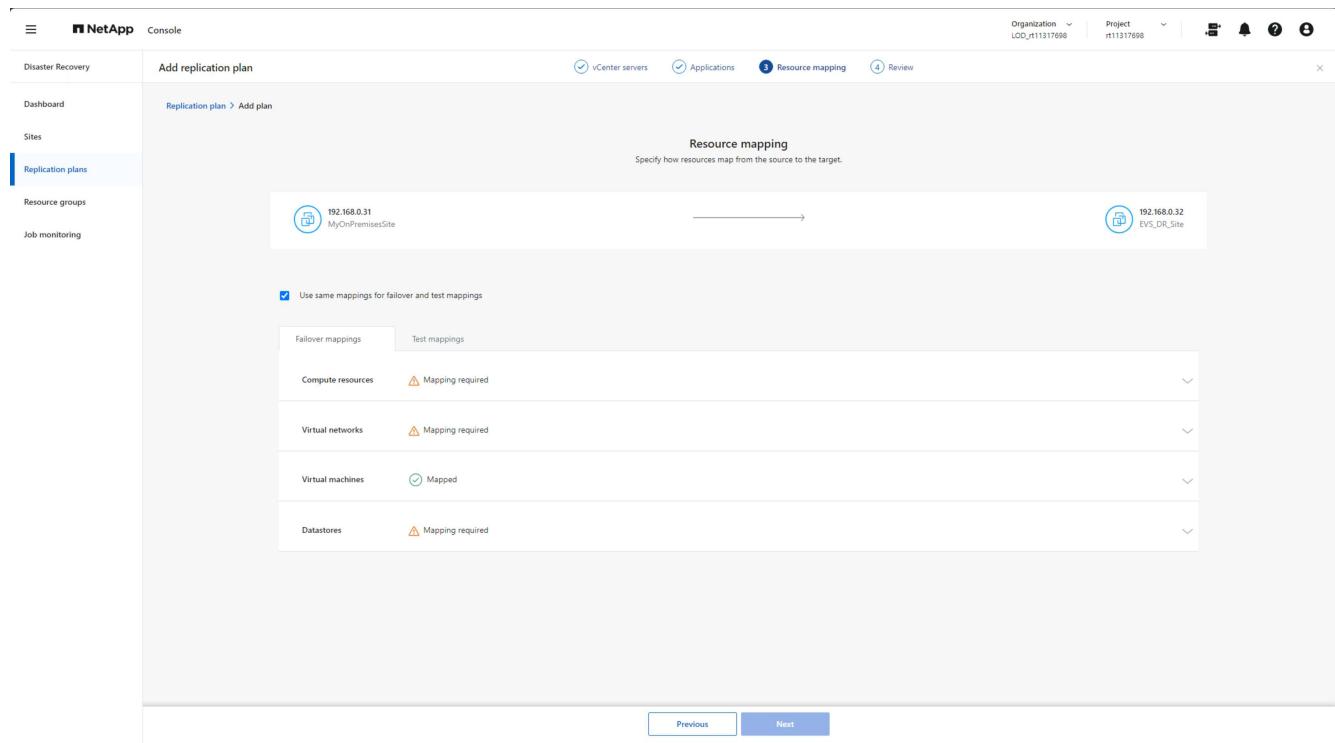
- Recursos de computação
- Redes virtuais
- Reconfiguração de VM
- Mapeamento de armazenamento de dados

Cada VM requer os três primeiros tipos de informações. O mapeamento do armazenamento de dados é necessário para cada armazenamento de dados que hospeda as VMs a serem protegidas.

- As seções com o ícone de cuidado (!) exigem que você forneça informações de mapeamento.
- A seção marcada com o ícone de verificação (✓) foram mapeados ou têm mapeamentos padrão. Revise-os para ter certeza de que a configuração atual atende aos seus requisitos.

Passos para acessar esta página

1. Na página **Plano de replicação**, continue para a seção **Mapeamento de recursos**.
2. Revise as informações na página **Mapeamento de recursos** que é aberta.



3. Para abrir cada categoria de mapeamentos necessários, selecione a seta para baixo (▼) ao lado da seção.

Mapeamento de recursos de computação

Como um site pode hospedar vários datacenters virtuais e vários clusters vCenter, você precisa identificar em qual cluster vCenter recuperar as VMs no caso de um failover.

Etapas para mapear recursos de computação

1. Selecione o datacenter virtual na lista de datacenters localizados no site de DR.
2. Selecione o cluster para hospedar os datastores e VMs na lista de clusters dentro do datacenter virtual selecionado.
3. (Opcional) Selecione um host de destino no cluster de destino.

Esta etapa não é necessária porque o NetApp Disaster Recovery seleciona o primeiro host adicionado ao cluster no vCenter. Nesse ponto, as VMs continuam a ser executadas naquele host ESXi ou o VMware DRS move a VM para um host ESXi diferente, conforme necessário, com base nas regras do DRS configuradas.

4. (Opcional) Forneça o nome de uma pasta de nível superior do vCenter para colocar os registros de VM.

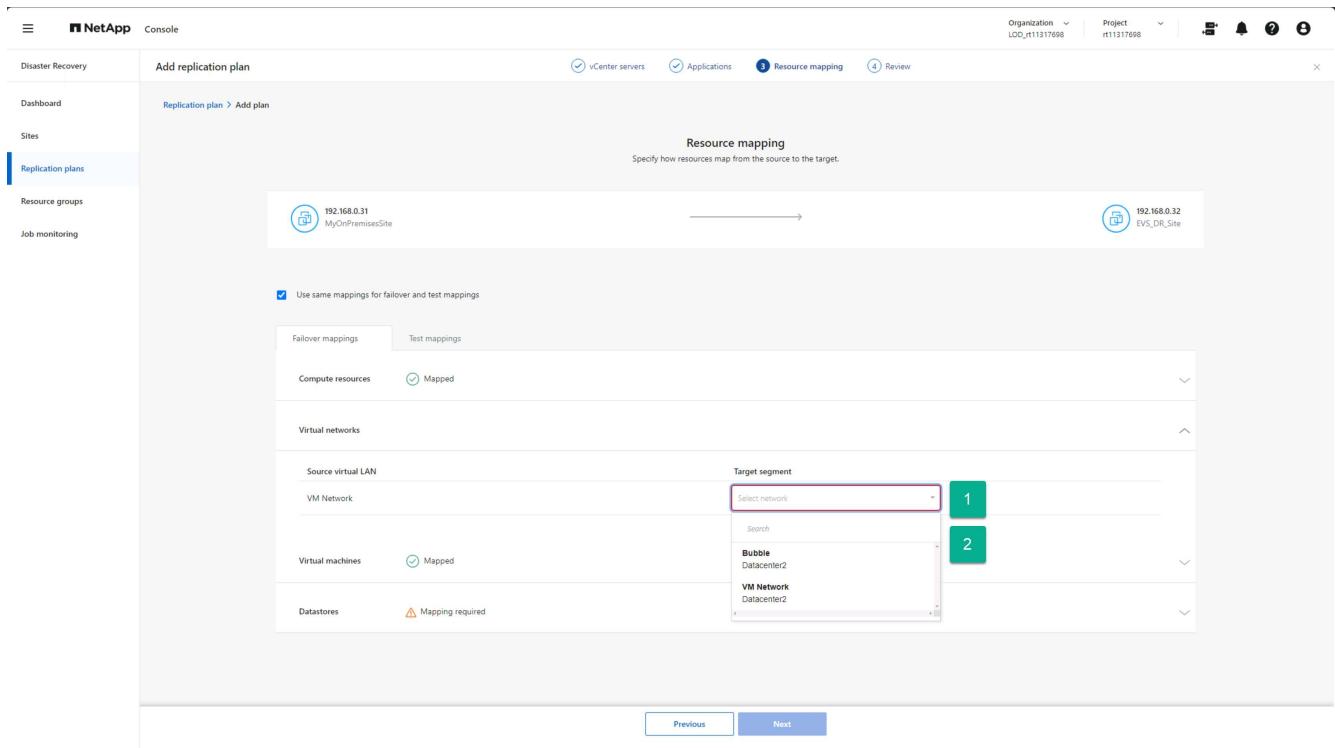
Isso é para suas necessidades organizacionais e não é obrigatório.

Mapear recursos de rede virtual

Cada VM pode ter uma ou mais NICs virtuais conectadas a redes virtuais dentro da infraestrutura de rede do vCenter. Para garantir que cada VM esteja conectada corretamente às redes desejadas ao reiniciar no site de DR, identifique em quais redes virtuais do site de DR essas VMs serão conectadas. Faça isso mapeando cada rede virtual no site local para uma rede associada no site de DR.

Selecione qual rede virtual de destino mapear cada rede virtual de origem

1. Selecione o segmento de destino na lista suspensa.
2. Repita a etapa anterior para cada rede virtual de origem listada.



Definir opções para reconfiguração de VM durante failover

Cada VM pode exigir modificações para funcionar corretamente no site do DR vCenter. A seção Máquinas virtuais permite que você forneça as alterações necessárias.

Por padrão, o NetApp Disaster Recovery usa as mesmas configurações para cada VM usadas no site local de origem. Isso pressupõe que as VMs usarão o mesmo endereço IP, CPU virtual e configuração de DRAM virtual.

Reconfiguração de rede

Os tipos de endereços IP suportados são estáticos e DHCP. Para endereços IP estáticos, você tem as seguintes configurações de IP de destino:

- Igual à origem:** como o nome sugere, o serviço usa o mesmo endereço IP na VM de destino que foi usado na VM no site de origem. Isso requer que você configure as redes virtuais que foram mapeadas na etapa anterior para as mesmas configurações de sub-rede.
- Diferente da origem:** O serviço fornece um conjunto de campos de endereço IP para cada VM que deve ser configurado para a sub-rede apropriada usada na rede virtual de destino, que você mapeou na seção anterior. Para cada VM, você deve fornecer um endereço IP, máscara de sub-rede, DNS e valores de gateway padrão. Opcionalmente, use a mesma máscara de sub-rede, DNS e configurações de gateway para todas as VMs para simplificar o processo quando todas as VMs estiverem conectadas à mesma sub-rede.
- Mapeamento de sub-rede:** esta opção reconfigura o endereço IP de cada VM com base na configuração CIDR da rede virtual de destino. Para usar esse recurso, certifique-se de que cada rede virtual do vCenter tenha uma configuração CIDR definida dentro do serviço, conforme alterado nas informações do vCenter na página Sites.

Depois de configurar sub-redes, o mapeamento de sub-redes usa o mesmo componente de unidade do endereço IP para a configuração da VM de origem e de destino, mas substitui o componente de sub-rede do

endereço IP com base nas informações CIDR fornecidas. Este recurso também requer que as redes virtuais de origem e de destino tenham a mesma classe de endereço IP (o /xx componente do CIDR). Isso garante que haja endereços IP suficientes disponíveis no site de destino para hospedar todas as VMs protegidas.

Para esta configuração do EVS, assumimos que as configurações de IP de origem e destino são as mesmas e não exigem nenhuma reconfiguração adicional.

Faça alterações na reconfiguração das configurações de rede

1. Selecione o tipo de endereçamento IP a ser usado para VMs com failover.
2. (Opcional) Forneça um esquema de renomeação de VM para VMs reiniciadas, fornecendo um valor de prefixo e sufixo opcional.

Source VM	Operating system	CPUs	RAM	Boot order	Boot delay(mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
Linux1	Linux	1	2 GiB	1	0	<input type="checkbox"/>	None	Not required
Linux4	Linux	1	2 GiB	3	5	<input type="checkbox"/>	None	Not required
Linux3	Linux	1	2 GiB	2	5	<input type="checkbox"/>	None	Not required

Reconfiguração de recursos de computação de VM

Há várias opções para reconfigurar recursos de computação de VM. O NetApp Disaster Recovery oferece suporte à alteração do número de CPUs virtuais, da quantidade de DRAM virtual e do nome da VM.

Especifique quaisquer alterações de configuração da VM

1. (Opcional) Modifique o número de CPUs virtuais que cada VM deve usar. Isso pode ser necessário se os hosts do cluster DR vCenter não tiverem tantos núcleos de CPU quanto o cluster vCenter de origem.
2. (Opcional) Modifique a quantidade de DRAM virtual que cada VM deve usar. Isso pode ser necessário se os hosts do cluster DR vCenter não tiverem tanta DRAM física quanto os hosts do cluster vCenter de origem.

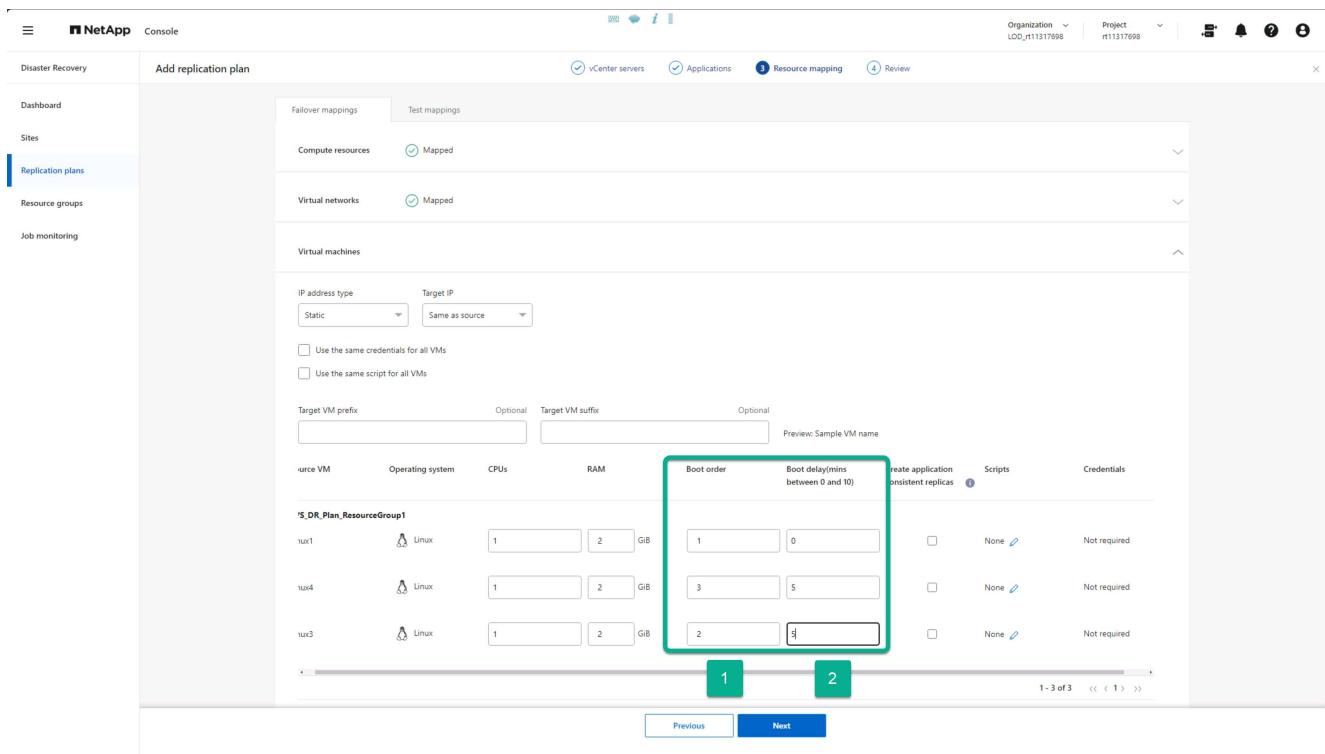
The screenshot shows the 'Add replication plan' wizard in the NetApp Console. The current step is 'Resource mapping'. The interface includes sections for 'Failover mappings' and 'Test mappings'. Under 'Compute resources', 'Virtual networks', and 'Virtual machines', specific configurations like 'IP address type' (Static), 'Target IP' (Same as source), and 'Boot order' are set. A preview of the VM names is shown. The main focus is on the 'Resource mapping' table, which maps source VMs to target VMs across various resource categories like CPUs and RAM.

Ordem de inicialização

O NetApp Disaster Recovery oferece suporte a uma reinicialização ordenada de VMs com base em um campo de ordem de inicialização. O campo Ordem de inicialização indica como as VMs em cada grupo de recursos são iniciadas. As VMs com o mesmo valor no campo Ordem de inicialização inicializam em paralelo.

Modificar as configurações da ordem de inicialização

- (Opcionalmente) Modifique a ordem em que você gostaria que suas VMs fossem reiniciadas. Este campo aceita qualquer valor numérico. O NetApp Disaster Recovery tenta reiniciar VMs que têm o mesmo valor numérico em paralelo.
- (Opcionalmente) Forneça um atraso a ser usado entre cada reinicialização da VM. O tempo é injetado após a reinicialização desta VM ser concluída e antes das VMs com o próximo número de ordem de inicialização mais alto. Este número está em minutos.



Operações personalizadas do sistema operacional convidado

O NetApp Disaster Recovery oferece suporte à execução de algumas operações de sistema operacional convidado para cada VM:

- O NetApp Disaster Recovery pode fazer backups consistentes de aplicativos de VMs que executam bancos de dados Oracle e Microsoft SQL Server.
- O NetApp Disaster Recovery pode executar scripts personalizados definidos adequados para o sistema operacional convidado de cada VM. A execução desses scripts requer credenciais de usuário aceitáveis para o sistema operacional convidado, com amplos privilégios para executar as operações listadas no script.

Modificar as operações personalizadas do sistema operacional convidado de cada VM

1. (Opcional) Marque a caixa de seleção **Criar réplicas consistentes de aplicativos** se a VM estiver hospedando um banco de dados Oracle ou SQL Server.
2. (Opcional) Para executar ações personalizadas no sistema operacional convidado como parte do processo de inicialização, carregue um script para qualquer VM. Para executar um único script em todas as VMs, use a caixa de seleção destacada e preencha os campos.
3. Certas alterações de configuração exigem credenciais de usuário com permissões adequadas para executar as operações. Forneça credenciais nos seguintes casos:
 - Um script será executado dentro da VM pelo sistema operacional convidado.
 - É necessário executar um snapshot consistente com o aplicativo.

Armazenamentos de dados de mapas

A etapa final na criação de um plano de replicação é identificar como o ONTAP deve proteger os armazenamentos de dados. Essas configurações definem o objetivo do ponto de recuperação (RPO) dos planos de replicação, quantos backups devem ser mantidos e onde replicar os volumes ONTAP de hospedagem de cada armazenamento de dados do vCenter.

Por padrão, o NetApp Disaster Recovery gerencia seu próprio agendamento de replicação de snapshots; no entanto, opcionalmente, você pode especificar que gostaria de usar o agendamento de política de replicação existente do SnapMirror para proteção do repositório de dados.

Além disso, você pode personalizar opcionalmente quais LIFs de dados (interfaces lógicas) e política de exportação usar. Se você não fornecer essas configurações, o NetApp Disaster Recovery usará todos os LIFs de dados associados ao protocolo apropriado (NFS, iSCSI ou FC) e usará a política de exportação padrão para volumes NFS.

Para configurar o mapeamento do armazenamento de dados (volume)

- (Opcional) Decida se você deseja usar um agendamento de replicação ONTAP SnapMirror existente ou se deseja que o NetApp Disaster Recovery gerencie a proteção de suas VMs (padrão).
- Forneça um ponto de partida para quando o serviço deve começar a fazer backups.
- Especifique com que frequência o serviço deve fazer um backup e replicá-lo no cluster Amazon FSx for NetApp ONTAP de destino de DR.
- Especifique quantos backups históricos devem ser mantidos. O serviço mantém o mesmo número de backups no cluster de armazenamento de origem e de destino.
- (Opcional) Selecione uma interface lógica padrão (LIFs de dados) para cada volume. Se nenhuma opção for selecionada, todos os LIFs de dados no SVM de destino que suportam o protocolo de acesso ao volume serão configurados.
- (Opcional) Selecione uma política de exportação para qualquer volume NFS. Se não for selecionado, a

política de exportação padrão será usada

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, a sidebar lists 'Disaster Recovery', 'Sites', 'Replication plans' (which is selected), 'Resource groups', and 'Job monitoring'. The main area is titled 'Add replication plan' and is currently on 'Step 4: Review'. The review step shows the following configuration:

- Compute resources:** Mapped
- Virtual networks:** Mapped
- Virtual machines:** Mapped
- Datastores:**
 - Source datastore:** nfs1 (svm0 nfs1)
 - Target datastore:** System: cluster2, SVM: svm1, Destination volume name: nfs1_DR
 - Preferred NFS LIF:** Select preferred NFS LIF
 - Export policy:** Select export policy

At the bottom, there are 'Previous' and 'Next' buttons.

Continuar com "[Assistente para criar plano de replicação Etapa 4](#)".

Criar um plano de replicação: Etapa 4 - Verificar as configurações no NetApp Disaster Recovery

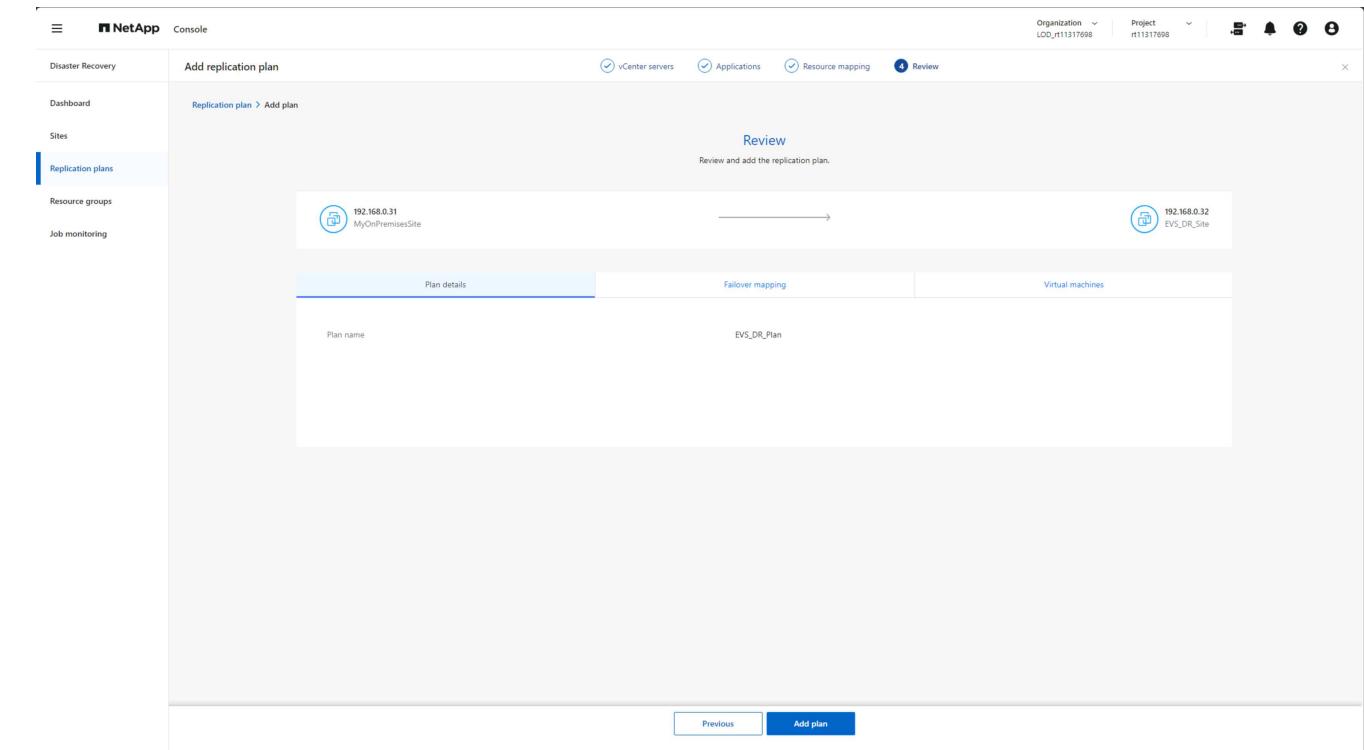
Depois de adicionar as informações do plano de replicação no NetApp Disaster Recovery, verifique se as informações inseridas estão corretas.

Passos

1. Selecione **Salvar** para revisar suas configurações antes de ativar o plano de replicação.

Você pode selecionar cada guia para revisar as configurações e fazer alterações em qualquer guia selecionando o ícone de lápis.

Revisão das configurações do plano de replicação



2. Quando estiver satisfeito com todas as configurações, selecione **Adicionar plano** na parte inferior da tela.

Continuar com "[Verifique o plano de replicação](#)" .

Verifique se tudo está funcionando no NetApp Disaster Recovery

Depois de adicionar o plano de replicação no NetApp Disaster Recovery, você retorna à página Planos de replicação, onde pode visualizar seus planos de replicação e seus status. Você deve verificar se o plano de replicação está no estado **Saudável**. Caso contrário, você deve verificar o status do plano de replicação e corrigir quaisquer problemas antes de prosseguir.

Figura: Página de planos de replicação

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
EVS_DR_Plan	Healthy	Ready	DemoOnPremSite_1	RG2	EVS_DR_Site

O NetApp Disaster Recovery executa uma série de testes para verificar se todos os componentes (cluster ONTAP , clusters vCenter e VMs) estão acessíveis e no estado adequado para que o serviço proteja as VMs. Isso é chamado de verificação de conformidade e é executado regularmente.

Na página Planos de replicação, você pode ver as seguintes informações:

- Status da última verificação de conformidade
- O estado de replicação do plano de replicação
- O nome do site protegido (fonte)
- A lista de grupos de recursos protegidos pelo plano de replicação
- O nome do site de failover (destino)

Execute operações de plano de replicação com o NetApp Disaster Recovery

Use o NetApp Disaster Recovery com Amazon EVS e Amazon FSx for NetApp ONTAP para executar as seguintes operações: failover, failover de teste, atualizar recursos, migrar, tirar um snapshot agora, desabilitar/habilitar plano de replicação, limpar snapshots antigos, reconciliar snapshots, excluir plano de replicação e editar agendamentos.

Falha

A principal operação que você pode precisar executar é aquela que você espera que nunca aconteça: fazer failover para o datacenter de DR (destino) no caso de uma falha catastrófica no site de produção local.

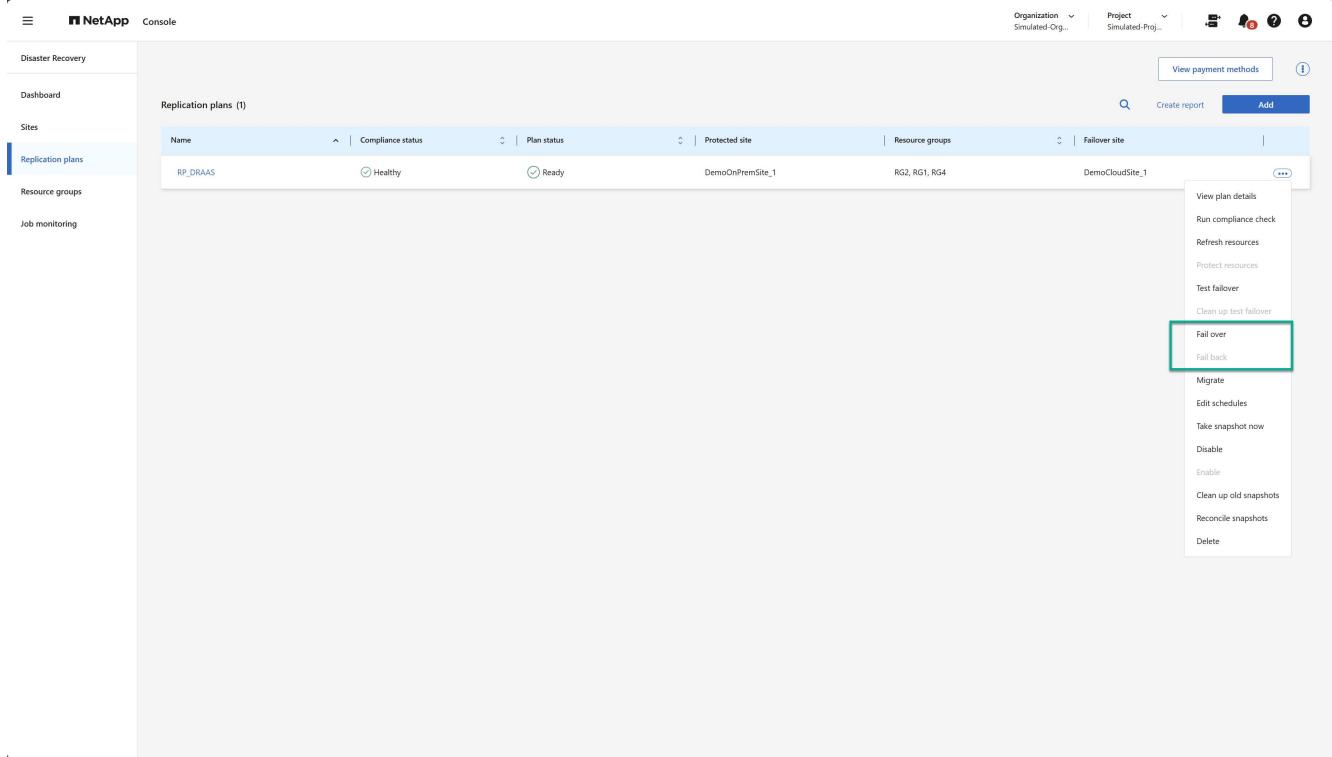
O failover é um processo iniciado manualmente.

Etapas para acessar a operação de failover

1. Na barra de navegação esquerda do NetApp Console , selecione **Proteção > Recuperação de desastres**.
2. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.

Etapas para executar um failover

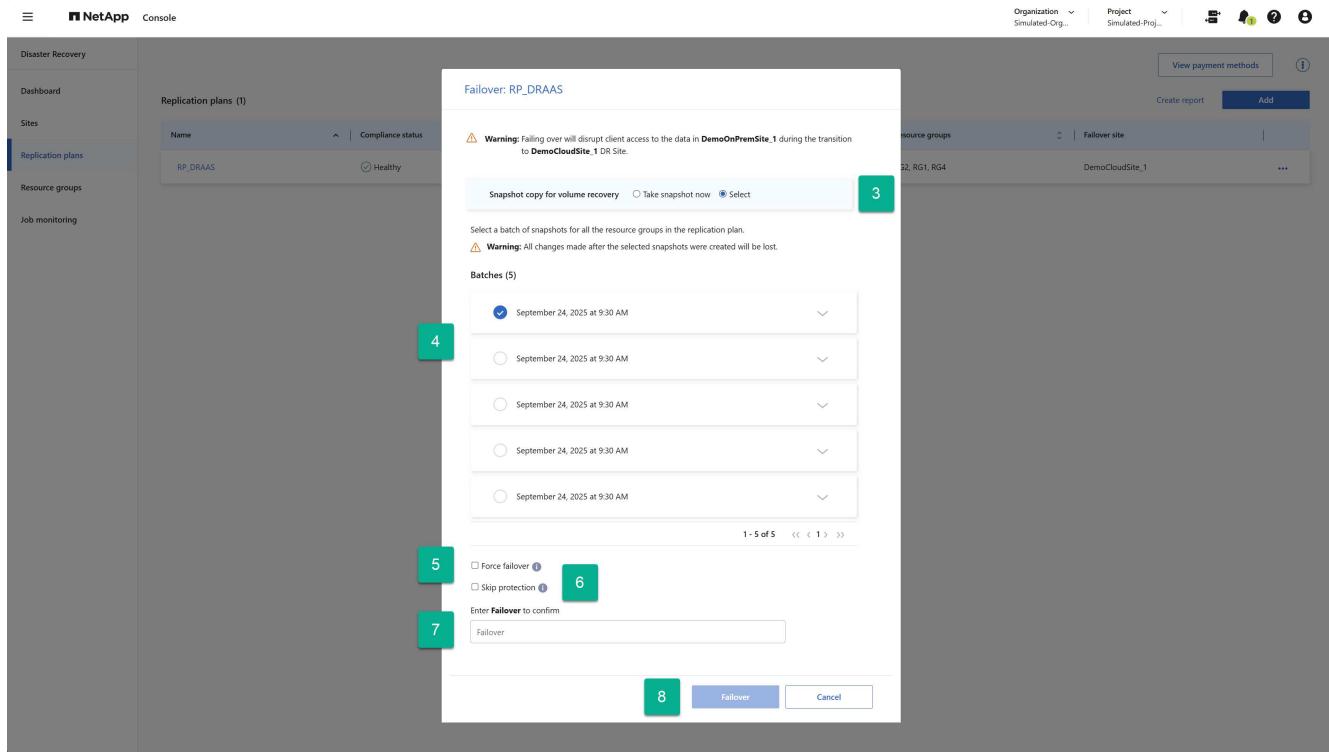
1. Na página Planos de replicação, selecione a opção Ações do plano de replicação .
2. Selecione **Fail over**.



The screenshot shows the NetApp Console interface for Disaster Recovery. On the left, there's a sidebar with 'Disaster Recovery' selected. Under 'Sites', 'Replication plans' is also selected. The main area displays a table titled 'Replication plans (1)'. The table has columns: Name, Compliance status, Plan status, Protected site, Resource groups, and Failover site. One row is shown with 'RP_DRAAS' in the Name column. To the right of the table is a context menu with various options like 'View plan details', 'Run compliance check', etc. A green box highlights the 'Fail over' option in the bottom-left corner of the menu.

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
RP_DRAAS			DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1

3. Se o site de produção (protegido) não estiver acessível, selecione um instantâneo criado anteriormente como sua imagem de recuperação. Para fazer isso, selecione **Selecionar**.
4. Selecione o backup a ser usado para a recuperação.
5. (Opcional) Selecione se deseja que o NetApp Disaster Recovery force o processo de failover, independentemente do estado do plano de replicação. Isso só deve ser feito como último recurso.
6. (Opcional) Selecione se deseja que o NetApp Disaster Recovery crie automaticamente um relacionamento de proteção reversa após a recuperação do site de produção.
7. Digite a palavra “Failover” para confirmar que você deseja prosseguir.
8. Selecione **Failover**.



Teste de failover

Um failover de teste é semelhante a um failover, exceto por duas diferenças.

- O site de produção ainda está ativo e todas as VMs continuam operando conforme o esperado.
- A proteção do NetApp Disaster Recovery das VMs de produção continua.

Isso é feito usando volumes nativos do ONTAP FlexClone no site de destino. Para saber mais sobre failover de teste, consulte "[Fazer failover de aplicativos para um site remoto | Documentação da NetApp](#)".

As etapas para executar um failover de teste são idênticas às usadas para executar um failover real, exceto que você usa a operação Test failover no menu de contexto do plano de replicação.

Passos

1. Selecione a opção Ações do plano de replicação
2. Selecione **Testar failover** no menu.

The screenshot shows the NetApp Console interface for Disaster Recovery. On the left, there's a navigation sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans, Resource groups, and Job monitoring. The main area displays a table titled 'Replication plans (1)'. The single row in the table is for 'RP_DRAAS', which is marked as 'Healthy' with a green status icon, 'Ready' for plan status, and 'DemoOnPremSite_1' as the protected site. To the right of the table is a detailed view of the replication plan. A context menu is open over the 'RP_DRAAS' row, with the 'Test failover' option highlighted and enclosed in a green box.

3. Decida se você deseja obter o estado mais recente do ambiente de produção (Tirar um instantâneo agora) ou usar um backup de plano de replicação criado anteriormente (Selecionar)
4. Se você escolheu um backup criado anteriormente, selecione o backup a ser usado para a recuperação.
5. Digite a palavra “Test failover” para verificar se você deseja prosseguir.
6. Selecione **Testar failover**.

The screenshot shows a modal dialog box titled 'Test failover: RP_DRAAS'. The dialog contains the following elements:

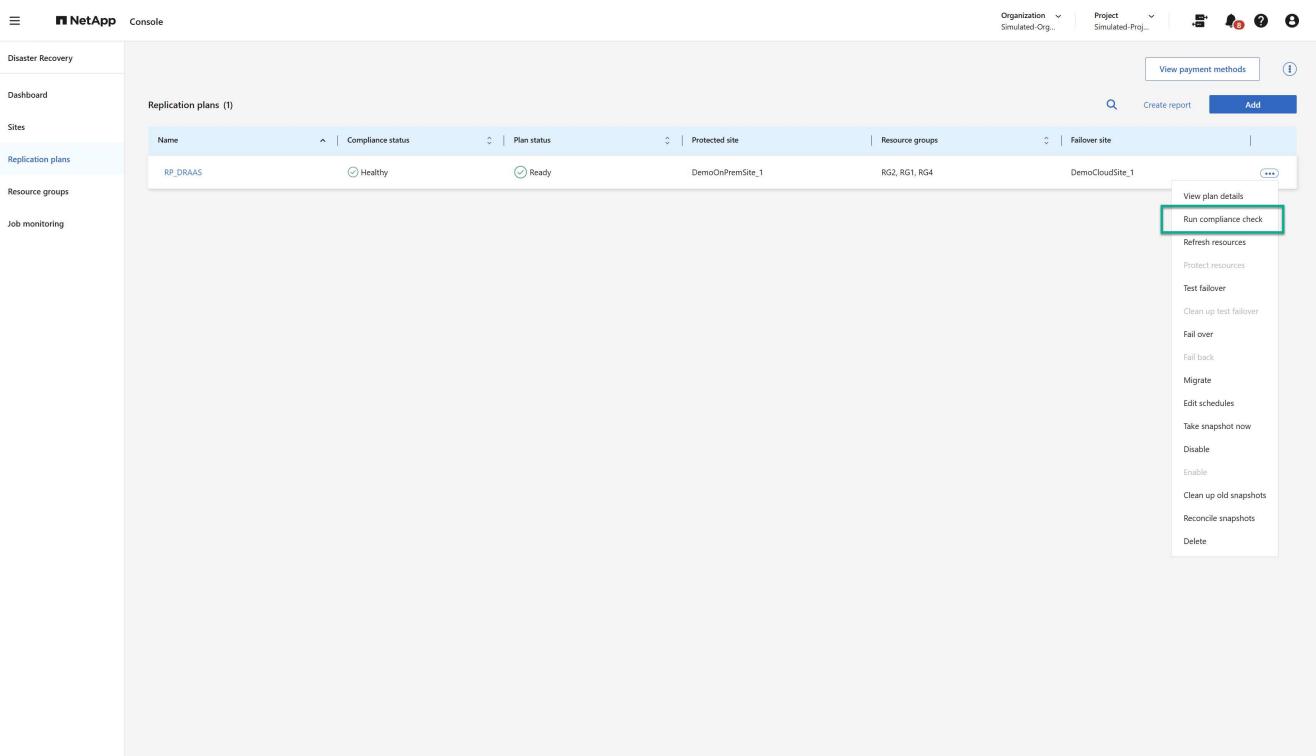
- Warning:** This test will create 6 VMs in the site DemoCloudSite_1. The test won't affect the site DemoOnPremSite_1.
- Snapshot copy for volume recovery:** Radio buttons for 'Take snapshot now' (selected) and 'Select'.
- Batches (5):** A list of five items, each with a checkbox and a dropdown arrow:
 - September 24, 2025 at 9:30 AM
 - September 24, 2025 at 9:30 AM
- Enter Test failover to confirm:** An input field containing 'Test failover'.
- Buttons:** A green button labeled '3' (step 3), a blue button labeled '4' (step 4), a blue button labeled '5' (step 5), a blue button labeled '6' (step 6), and a 'Cancel' button.

Execute uma verificação de conformidade

As verificações de conformidade são executadas a cada três horas, por padrão. A qualquer momento, você pode querer executar manualmente uma verificação de conformidade.

Passos

1. Selecione a opção *Ações*  ao lado do plano de replicação.
2. Selecione a opção **Executar verificação de conformidade** no menu Ações do plano de replicação:



3. Para alterar a frequência com que o NetApp Disaster Recovery executa verificações de conformidade automaticamente, selecione a opção **Editar agendamentos** no menu Ações do plano de replicação.

Atualizar recursos

Sempre que você fizer alterações na sua infraestrutura virtual — como adicionar ou excluir VMs, adicionar ou excluir datastores ou mover VMs entre datastores — será necessário executar uma atualização dos clusters do vCenter afetados no serviço NetApp Disaster Recovery . O serviço faz isso automaticamente uma vez a cada 24 horas por padrão, mas uma atualização manual garante que as informações mais recentes da infraestrutura virtual estejam disponíveis e sejam levadas em consideração para proteção de DR.

Há dois casos em que uma atualização é necessária:

- Atualização do vCenter: execute uma atualização do vCenter sempre que VMs forem adicionadas, excluídas ou movidas para fora de um cluster do vCenter;
- Atualização do plano de replicação: execute uma atualização do plano de replicação sempre que uma VM for movida entre armazenamentos de dados no mesmo cluster vCenter de origem.

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, there's a navigation sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area is titled 'Replication plans (1)' and lists a single plan named 'RP_DRAAS'. The plan details are as follows:

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1

A context menu is open over the 'RP_DRAAS' row, with the 'Refresh resources' option highlighted by a red box. Other options in the menu include:

- View plan details
- Run compliance check
- Refresh resources** (highlighted)
- Protect resources
- Test failover
- Clean up test failover
- Fail over
- Fail back
- Migrate
- Edit schedules
- Take snapshot now
- Disable
- Enable
- Clean up old snapshots
- Reconcile snapshots
- Delete

Migrar

Embora o NetApp Disaster Recovery seja usado principalmente para casos de recuperação de desastres, ele também pode permitir movimentações únicas de um conjunto de VMs do site de origem para o site de destino. Isso poderia ser para uma migração planejada para um projeto de nuvem ou poderia ser usado para evitar desastres — como mau tempo, conflitos políticos ou outros possíveis eventos catastróficos temporários.

1. Selecione a opção *Ações* ao lado do plano de replicação.
2. Para mover as VMs em um plano de replicação para o cluster Amazon EVS de destino, selecione **Migrar** no menu Ações do plano de replicação:

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, there's a sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area is titled 'Replication plans (1)' and shows a table with one row. The row details are: Name (RP_DRAAS), Compliance status (Healthy), Plan status (Ready), Protected site (DemoOnPremSite_1), Resource groups (RG2, RG1, RG4), and Failover site (DemoCloudSite_1). To the right of the table is a context menu with various options: View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clean up test failover, Fail over, Fall back, Migrate (which is highlighted with a red box), Edit schedules, Take snapshot now, Disable, Enable, Clean up old snapshots, Reconcile snapshots, and Delete.

3. Insira informações na caixa de diálogo Migrar.

Tire uma foto agora

A qualquer momento, você pode tirar um instantâneo imediato do plano de replicação. Este instantâneo está incluído nas considerações de NetApp Disaster Recovery definidas pela contagem de retenção de instantâneos do plano de replicação.

1. Selecione a opção *Ações* ao lado do plano de replicação.
2. Para tirar um instantâneo imediato dos recursos do plano de replicação, selecione **Tirar instantâneo agora** no menu Ações do plano de replicação:

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, there's a sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area is titled 'Replication plans (1)' and lists a single plan: RP_DRAAS. The plan details are as follows:

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1

A context menu is open over the RP_DRAAS plan, listing various actions: View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clean up test failover, Fail over, Fail back, Migrate, Edit schedules, Take snapshot now (which is highlighted with a green box), Disable, Enable, Clean up old snapshots, Reconcile snapshots, and Delete.

Desabilitar ou habilitar o plano de replicação

Pode ser necessário interromper temporariamente o plano de replicação para executar alguma operação ou manutenção que possa impactar o processo de replicação. O serviço fornece um método para parar e iniciar a replicação.

1. Para interromper temporariamente a replicação, selecione **Desativar** no menu Ações do plano de replicação.
2. Para reiniciar a replicação, selecione **Ativar** no menu Ações do plano de replicação.

Quando o plano de replicação está ativo, o comando **Ativar** fica esmaecido. Quando o plano de replicação é desabilitado, o comando **Desabilitar** fica esmaecido.

The screenshot shows the NetApp Console interface. On the left, there's a navigation sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area displays a table titled 'Replication plans (1)'. The table has columns for Name, Compliance status, Plan status, Protected site, Resource groups, and Failover site. One row is present, showing 'RP_DRAAS' with 'Healthy' compliance and 'Ready' plan status. To the right of the table is a context menu with various options: View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clean up test failover, Fail over, Fail back, Migrate, Edit schedules, Take snapshot now, Disable (which is highlighted with a red box), Enable, Clean up old snapshots (also highlighted with a red box), Reconcile snapshots, and Delete.

Limpar instantâneos antigos

Talvez você queira limpar instantâneos mais antigos que foram retidos nos sites de origem e destino. Isso pode acontecer se a contagem de retenção de snapshots do plano de replicação for alterada.

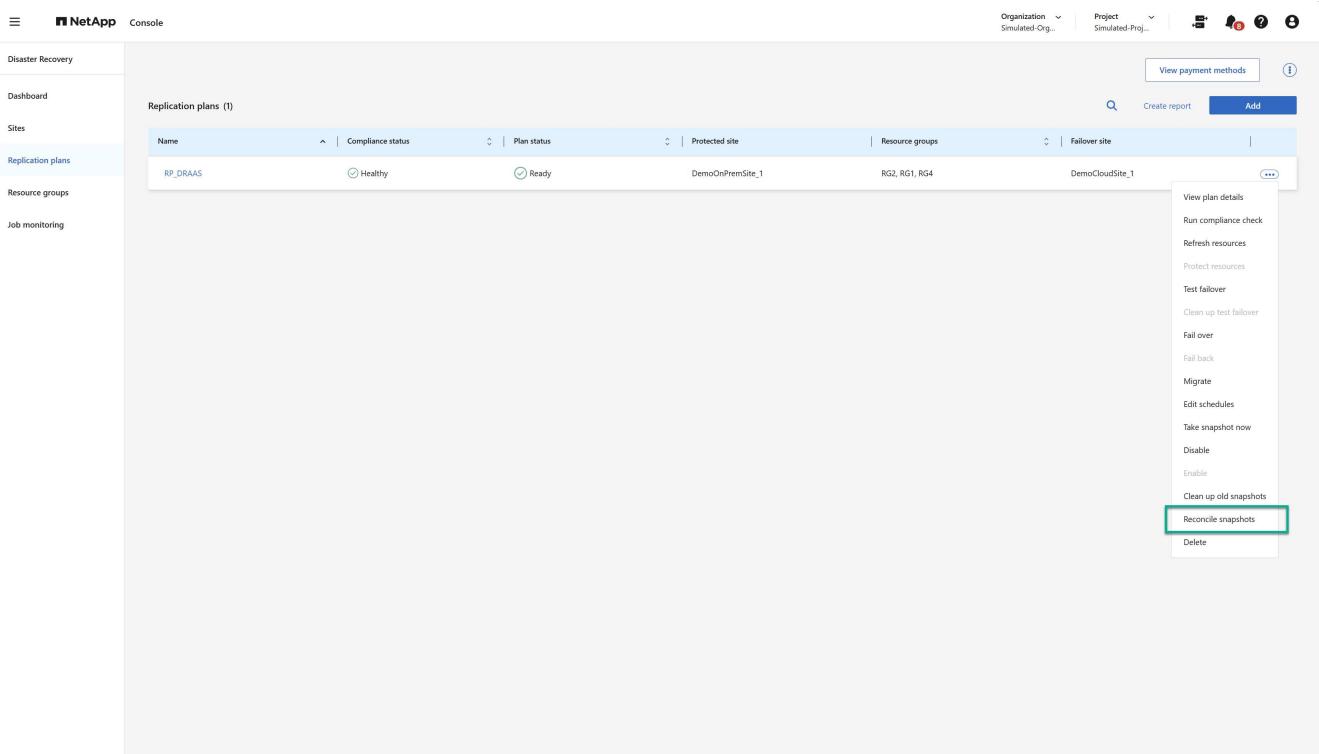
1. Selecione a opção *Ações* ao lado do plano de replicação.
2. Para remover esses instantâneos mais antigos manualmente, selecione **Limpar instantâneos antigos** no menu Ações do plano de replicação.

This screenshot is nearly identical to the one above, showing the NetApp Console interface and the same replication plan 'RP_DRAAS'. The context menu is open over the plan, and the 'Clean up old snapshots' option is highlighted with a red box, indicating it is the selected action.

Reconciliar instantâneos

Como o serviço orquestra instantâneos de volume ONTAP, é possível que um administrador de armazenamento ONTAP exclua instantâneos diretamente usando o ONTAP System Manager, a CLI do ONTAP ou as APIs REST do ONTAP sem o conhecimento do serviço. O serviço exclui automaticamente todos os snapshots na origem que não estão no cluster de destino a cada 24 horas. No entanto, você pode fazer isso sob demanda. Esse recurso permite que você garanta que os instantâneos sejam consistentes em todos os sites.

1. Selecione a opção *Ações*  ao lado do plano de replicação.
2. Para excluir instantâneos do cluster de origem que não existem no cluster de destino, selecione **Reconciliar instantâneos** no menu Ações do plano de replicação.



Name	Compliance status	Plan status	Protected site	Resource groups	Fallover site
RP_DRAAS	Healthy	Ready	DemoOnPremSite_1	RG2, RG1, RG4	DemoCloudSite_1

Excluir plano de replicação

Se o plano de replicação não for mais necessário, você poderá excluí-lo.

1. Selecione a opção *Ações*  ao lado do plano de replicação.
2. Para excluir o plano de replicação, selecione **Excluir** no menu de contexto do plano de replicação.

The screenshot shows the NetApp Console interface. On the left, there's a sidebar with options like Disaster Recovery, Dashboard, Sites, Replication plans (selected), Resource groups, and Job monitoring. The main area displays a table titled 'Replication plans (1)'. The table has columns for Name (RP_DRAAS), Compliance status (Healthy), Plan status (Ready), Protected site (DemoOnPremSite_1), Resource groups (RG2, RG1, RG4), and Failover site (DemoCloudSite_1). To the right of the table is a context menu with various options: View plan details, Run compliance check, Refresh resources, Protect resources, Test failover, Clean up test failover, Fail over, Fail back, Migrate, Edit schedules (which is highlighted with a red box), Take snapshot now, Disable, Enable, Clean up old snapshots, Reconcile snapshots, and Delete.

Editar agendamentos

Duas operações são executadas automaticamente em um cronograma regular: failovers de teste e verificações de conformidade.

1. Selecione a opção *Ações* ao lado do plano de replicação.
2. Para alterar esses agendamentos para qualquer uma dessas duas operações, selecione **Editar agendamentos** para o plano de replicação.

This screenshot is identical to the one above it, showing the NetApp Console interface and the context menu for the RP_DRAAS replication plan. The 'Edit schedules' option in the menu is specifically highlighted with a red box.

Alterar intervalo de verificação de conformidade

Por padrão, as verificações de conformidade são realizadas a cada três horas. Você pode alterar isso para qualquer intervalo entre 30 minutos e 24 horas.

Para alterar esse intervalo, altere o campo Frequência na caixa de diálogo Editar agendamentos:

The screenshot shows the NetApp Disaster Recovery Console interface. On the left, there's a sidebar with options like Dashboard, Sites, Replication plans, Resource groups, and Job monitoring. The main area shows a table of replication plans, with one named 'EVS_DR_Plan' selected. A modal window titled 'Edit schedules: EVS_DR_Plan' is open over the table. This modal contains sections for 'Compliance check' (with a frequency of '180d') and 'Test failover' (with an unchecked checkbox for 'Run test failovers on a schedule'). At the bottom of the modal are 'Save' and 'Cancel' buttons.

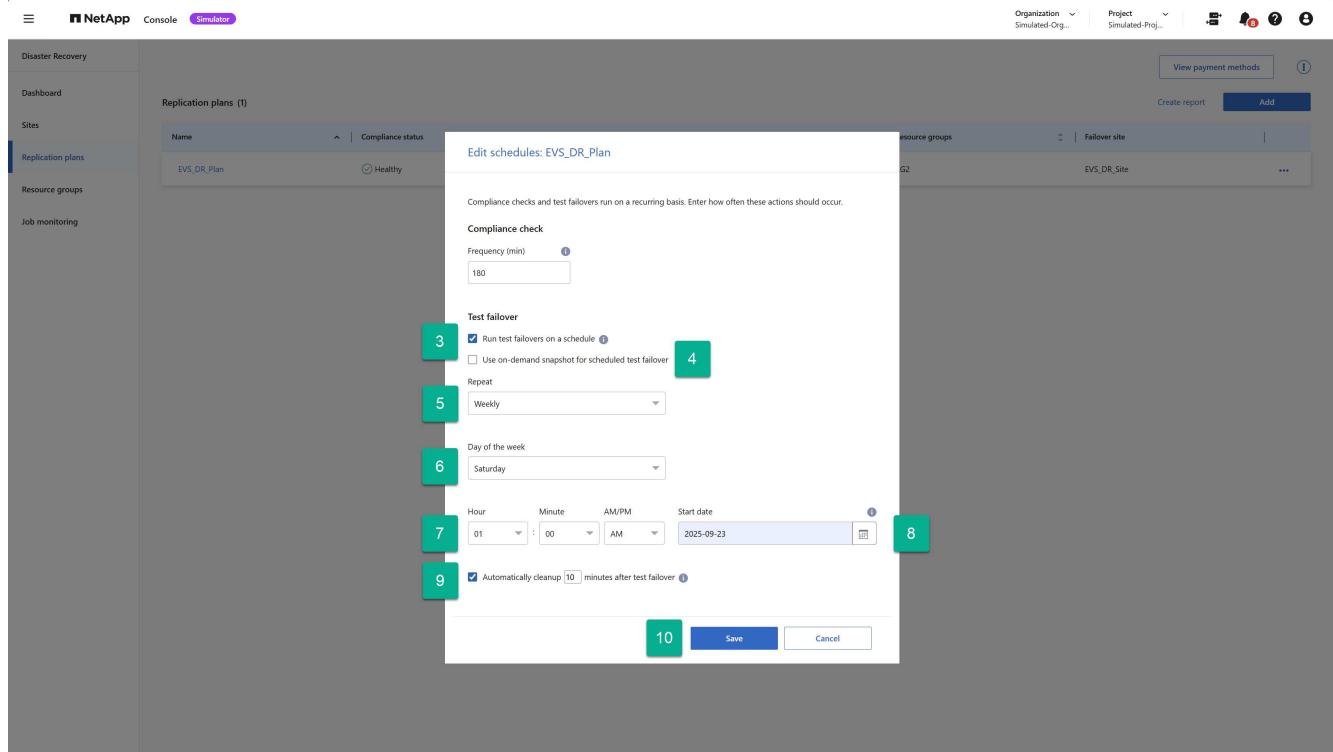
Aendar failovers de testes automatizados

Os failovers de teste são executados manualmente por padrão. Você pode agendar failovers de teste automáticos, o que ajuda a garantir que seus planos de replicação funcionem conforme o esperado. Para saber mais sobre o processo de failover de teste, consulte "["Teste o processo de failover"](#)" .

Etapas para agendar failovers de teste

1. Selecione a opção *Ações* ao lado do plano de replicação.
2. Selecione **Executar failover**.
3. Marque a caixa de seleção **Executar failovers de teste conforme uma programação**.
4. (Opcional) Marque a opção **Usar instantâneo sob demanda para failover de teste agendado**.
5. Selecione um tipo de intervalo no menu suspenso Repetir.
6. Selecione quando executar o failover de teste
 - a. Semanal: selecione o dia da semana
 - b. Mensal: selecione o dia do mês
7. Escolha a hora do dia para executar o teste de failover
8. Escolha a data de início.
9. Decida se você deseja que o serviço limpe automaticamente o ambiente de teste e por quanto tempo você gostaria que o ambiente de teste fosse executado antes que o processo de limpeza começasse.

10. Seleccione **Salvar**.



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.