Documentação do NetApp Disaster Recovery

NetApp Disaster Recovery

NetApp
February 04, 2026

Índice

Documentação do NetApp Disaster Recovery . . . 1
Notas de lançamento . . . 2
Novidades no NetApp Disaster Recovery . . . 2
12 de janeiro de 2026 . . . 2
09 de dezembro de 2025 . . . 3
01 de dezembro de 2025 . . . 3
10 de novembro de 2025 . . . 3
06 de outubro de 2025 . . . 4
04 de agosto de 2025 . . . 5
14 de julho de 2025 . . . 5
30 de junho de 2025 . . . 6
23 de junho de 2025 . . . 6
09 de junho de 2025 . . . 7
13 de maio de 2025 . . . 7
16 de abril de 2025 . . . 8
10 de março de 2025 . . . 9
19 de fevereiro de 2025 . . . 10
30 de outubro de 2024 . . . 10
20 de setembro de 2024 . . . 12
02 de agosto de 2024 . . . 12
17 de julho de 2024 . . . 13
05 de julho de 2024 . . . 13
15 de maio de 2024 . . . 14
05 de março de 2024 . . . 15
01 de fevereiro de 2024 . . . 15
11 de janeiro de 2024 . . . 16
20 de outubro de 2023 . . . 16
27 de setembro de 2023 . . . 17
01 de agosto de 2023 . . . 18
18 de maio de 2023 . . . 18
Limitações na NetApp Disaster Recovery . . . 19
Aguarde até que o failback seja concluído antes de executar a descoberta . . . 19
O NetApp Console pode não detectar o Amazon FSx for NetApp ONTAP . . . 19
Limitações do Google Cloud NetApp Volumes . . . 19
Começar . . . 20
Saiba mais sobre o NetApp Disaster Recovery para VMware . . . 20
NetApp Console . . . 21
Benefícios de usar o NetApp Disaster Recovery para VMware . . . 21
O que você pode fazer com o NetApp Disaster Recovery para VMware . . . 22
Custo . . . 23
Licenciamento . . . 23
Teste gratuito de 30 dias . . . 24
Como funciona a NetApp Disaster Recovery . . . 24

Destinos de proteção e tipos de armazenamento de dados suportados . . . 26
Termos que podem ajudar você com a NetApp Disaster Recovery . . . 27
Pré-requisitos do NetApp Disaster Recovery . . . 27
Versões de software . . . 27
Pré-requisitos e considerações do Google Cloud . . . 28
Pré-requisitos de armazenamento ONTAP . . . 29
Pré-requisitos dos clusters VMware vCenter . . . 29
Pré-requisitos do NetApp Console . . . 29
Pré-requisitos de carga de trabalho . . . 31
Mais informações . . . 31
Início rápido para NetApp Disaster Recovery . . . 31
Configure sua infraestrutura para NetApp Disaster Recovery . . . 32
Nuvem híbrida com VMware Cloud e Amazon FSx for NetApp ONTAP . . . 32
Nuvem privada . . . 34
Acesse a NetApp Disaster Recovery . . . 35
Configurar licenciamento para NetApp Disaster Recovery . . . 37
Experimente usando um teste gratuito de 30 dias . . . 37
Após o término do teste, assine através de um dos Marketplaces . . . 38
Após o término do teste, adquira uma licença BYOL através da NetApp . . . 39
Atualize sua licença quando ela expirar . . . 40
Encerrar o teste gratuito . . . 40
Use a NetApp Disaster Recovery . . . 42
Visão geral do uso do NetApp Disaster Recovery . . . 42
Veja a integridade dos seus planos de NetApp Disaster Recovery no painel . . . 42
Adicionar vCenters a um site no NetApp Disaster Recovery . . . 43
Adicionar mapeamento de sub-rede para um site vCenter . . . 46
Edite o site do servidor vCenter e personalize o cronograma de descoberta . . . 49
Atualizar descoberta manualmente . . . 50
Crie um grupo de recursos para organizar VMs no NetApp Disaster Recovery . . . 51
Crie um plano de replicação no NetApp Disaster Recovery . . . 54
Crie o plano . . . 56
Editar cronogramas para testar a conformidade e garantir que os testes de failover funcionem . . . 70
Replique aplicativos para outro site com o NetApp Disaster Recovery . . . 71
Migrar aplicativos para outro site com o NetApp Disaster Recovery . . . 72
Faça failover de aplicativos para um site remoto com o NetApp Disaster Recovery . . . 73
Teste o processo de failover . . . 73
Limpe o ambiente de teste após um teste de failover . . . 74
Fazer failover do site de origem para um site de recuperação de desastres . . . 74
Faça failback de aplicativos para a fonte original com o NetApp Disaster Recovery . . . 76
Sobre o failback . . . 77
Antes de começar . . . 77
Passos . . . 77
Gerencie sites, grupos de recursos, planos de replicação, repositórios de dados e informações de máquinas virtuais com o NetApp Disaster Recovery . . . 77
Gerenciar sites do vCenter . . . 78

Gerenciar grupos de recursos . . . 78
Gerenciar planos de replicação . . . 79
Exibir informações dos armazenamentos de dados . . . 81
Exibir informações das máquinas virtuais . . . 82
Monitorar trabalhos de NetApp Disaster Recovery . . . 82
Ver empregos . . . 82
Cancelar um trabalho . . . 82
Crie relatórios de NetApp Disaster Recovery . . . 83
Referência . . . 84
Privilégios necessários do vCenter para NetApp Disaster Recovery . . . 84
Alternar agentes do Console ao usar o NetApp Disaster Recovery . . . 87
Antes de começar . . . 87
Passos . . . 87
Mais informações . . . 88
Use a NetApp Disaster Recovery com o Amazon EVS . . . 88
Introdução ao NetApp Disaster Recovery usando o Amazon Elastic VMware Service e o Amazon FSx for NetApp ONTAP . . . 88
Visão geral da solução de NetApp Disaster Recovery usando Amazon EVS e Amazon FSs para NetApp ONTAP . . . 89
Instalar o agente do NetApp Console para NetApp Disaster Recovery . . . 91
Configurar o NetApp Disaster Recovery para Amazon EVS . . . 91
Crie planos de replicação para o Amazon EVS . . . 104
Execute operações de plano de replicação com o NetApp Disaster Recovery . . . 117
Perguntas frequentes sobre NetApp Disaster Recovery . . . 130
Conhecimento e suporte . . . 131
Registre-se para obter suporte . . . 131
Visão geral do registro de suporte . . . 131
Registre o NetApp Console para suporte ao NetApp . . . 131
Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP . . . 133
Obter ajuda . . . 135
Obtenha suporte para um serviço de arquivo de provedor de nuvem . . . 135
Use opções de autoapoio . . . 135
Crie um caso com o suporte da NetApp . . . 135
Gerencie seus casos de suporte . . . 138
Avisos legais . . . 139
Direitos autorais . . . 139
Marcas Registradas . . . 139
Patentes . . . 139
Política de Privacidade . . . 139
Código aberto . . . 139

Documentação do NetApp Disaster Recovery

Notas de lançamento

Novidades no NetApp Disaster Recovery

Descubra as novidades em NetApp Disaster Recovery.

12 de janeiro de 2026

Versão 4.2.9

Suporte para vários agentes do Console em ambientes locais.

Se você utiliza a Recuperação de Desastres localmente, agora pode implantar um agente de console para cada instância do vCenter, melhorando a resiliência.

Por exemplo, se você tiver dois sites (Sites A e B), o Site A pode ter o agente de console A anexado ao vCenter 1, à implantação ONTAP 1 e à implantação ONTAP 2. O Site B pode ter o agente de console B anexado às implantações do vCenter 2 e do ONTAP 3 e 4.

Para obter informações sobre o agente do Console na Recuperação de Desastres, consulte "Crie o agente do Console".

Adicionar VMs após failover para planos de replicação usando proteção baseada em armazenamento de dados

Quando o failover é acionado, qualquer plano de replicação que utilize proteção baseada em armazenamento de dados inclui as VMs que foram adicionadas ao armazenamento de dados, desde que tenham sido detectadas. Você deve fornecer os detalhes de mapeamento para as VMs adicionadas antes que o failover seja concluído.

Para mais informações, consulte "Aplicativos de failover".

Novas notificações por e-mail

A Recuperação de Desastres agora fornece notificações por e-mail para os seguintes eventos:

- Aproximando-se do limite de utilização da capacidade
- Geração de relatório concluída
- Fracassos no trabalho
- Vencimento da licença ou violações

Melhorias no Swagger

Agora você pode acessar a documentação do Swagger diretamente do Disaster Recovery. Na seção Recuperação de Desastres, selecione **Configurações** e, em seguida, **Documentação da API** para acessar o Swagger, ou visite este URL no modo anônimo/privado do seu navegador: "https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas".

Interfaces de usuário aprimoradas

A Recuperação de Desastres agora oferece avisos aprimorados e soluções de erros. Esta versão corrige um

erro que impedia a exibição de trabalhos cancelados na interface do usuário. Os trabalhos cancelados agora estão visíveis. Também há um novo aviso quando a mesma rede de destino é mapeada para várias redes de origem diferentes.

Manter a estrutura de pastas da VM adicionada como padrão nos planos de replicação

Ao criar uma réplica, a nova configuração padrão é manter a estrutura de pastas da máquina virtual. Se o destino da recuperação não tiver a hierarquia de pastas original, a Recuperação de Desastres a criará. Você pode desmarcar esta opção para ignorar a hierarquia de pastas original.

Para mais informações, consulte "Crie um plano de replicação".

09 de dezembro de 2025

Versão 4.2.8P1

Retenção da hierarquia de pastas

Por padrão, a Recuperação de Desastres mantém a hierarquia de inventário da VM (estrutura de pastas) em caso de failover. Se o destino da recuperação não tiver a pasta necessária, a Recuperação de Desastres a criará.

Agora você pode substituir essa configuração designando uma nova pasta principal para a máquina virtual ou desmarcando a opção **Manter a hierarquia de pastas original**.

Para mais informações, consulte "Crie um plano de replicação".

Atualização simplificada do agente do console

A Recuperação de Desastres agora oferece suporte a um processo simplificado para o uso de vários agentes do Console em um ambiente de trabalho. Para alternar entre agentes do Console, você deve editar a configuração do vCenter, redescobrir as credenciais e atualizar os planos de replicação para usar o novo agente do Console.

Para mais informações, consulte "Agentes do console de troca".

01 de dezembro de 2025

Versão 4.2.8

Suporte para o Google Cloud VMware Engine usando o Google Cloud NetApp Volumes

O NetApp Disaster Recovery agora oferece suporte ao Google Cloud VMware Engine, utilizando o Google Cloud NetApp Volumes para operações de migração, failover, failback e teste. Essa integração possibilita fluxos de trabalho de recuperação de desastres contínuos entre ambientes locais e o Google Cloud.

Certifique-se de revisar o"pré-requisitos" e"limitações" para o Google Cloud.

10 de novembro de 2025

Versão 4.2.7

Suporte a failover em cascata

Agora você pode configurar um relacionamento em cascata no ONTAP e usar qualquer um dos ramos desse relacionamento de replicação para recuperação de desastres.

Reduzir o suporte de hardware da VMware durante o registro

O Disaster Recovery agora oferece suporte ao downgrade do hardware VMware para uma versão anterior do vSphere durante o registro. Isso é útil quando o host ESX de origem está executando uma versão mais recente do que o site de recuperação de desastres.

Para mais informações, consulte "Crie um plano de replicação no NetApp Disaster Recovery".

Encerramento elegante

A Recuperação de Desastres agora desliga as VMs de forma controlada, em vez de desligá-las completamente. Se uma determinada máquina virtual demorar mais de dez minutos para ser desligada, o sistema de Recuperação de Desastres a desliga automaticamente.

Suporte para scripts de pré-backup

Agora você pode inserir scripts personalizados no fluxo de trabalho de failover para serem executados antes da criação de um backup. A criação de scripts de pré-backup permite controlar o estado da máquina virtual antes da replicação de um snapshot e preparar a máquina virtual para uma transição. Por exemplo, você pode injetar um script que desmonta uma montagem NFS, a qual será remontada usando um script diferente após a recuperação de falha.

Para mais informações, consulte "Crie um plano de replicação no NetApp Disaster Recovery".

06 de outubro de 2025

Versão 4.2.6

A BlueXP disaster recovery agora é NetApp Disaster Recovery

A BlueXP disaster recovery foi renomeada para NetApp Disaster Recovery.

BlueXP agora é NetApp Console

O NetApp Console, criado com base na base aprimorada e reestruturada do BlueXP , fornece gerenciamento centralizado do armazenamento NetApp e do NetApp Data Services em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada, que é altamente segura e compatível.

Para obter detalhes sobre o que mudou, consulte o "Notas de versão do NetApp Console".

Outras atualizações

- O suporte para o Amazon Elastic VMware Service (EVS) com o Amazon FSx for NetApp ONTAP estava em uma prévia pública. Com este lançamento, ele agora está disponível para o público em geral. Para mais detalhes, consulte"Introdução ao NetApp Disaster Recovery usando o Amazon Elastic VMware Service e o Amazon FSx for NetApp ONTAP" .
- Melhorias na descoberta de armazenamento, incluindo tempos de descoberta reduzidos para implantações locais

- Suporte ao Gerenciamento de Identidade e Acesso (IAM), incluindo controle de acesso baseado em função (RBAC) e permissões de usuário aprimoradas
- Suporte de visualização privada para solução Azure VMware e Cloud Volumes ONTAP. Com esse suporte, agora você pode configurar a proteção de recuperação de desastres do local para a solução Azure VMware usando o armazenamento Cloud Volumes ONTAP .

04 de agosto de 2025

Versão 4.2.5P2

Atualizações do NetApp Disaster Recovery

Esta versão inclui as seguintes atualizações:

- Melhorou o suporte do VMFS para lidar com o mesmo LUN apresentado por várias máquinas virtuais de armazenamento.
- Melhorou a limpeza de desmontagem do teste para lidar com o armazenamento de dados que já está sendo desmontado e/ou excluído.
- Mapeamento de sub-rede aprimorado para que agora valide se o gateway inserido está contido na rede fornecida.
- Foi corrigido um problema que poderia causar falha no plano de replicação se o nome da VM contivesse ".com".
- Foi removida uma restrição que impedia que o volume de destino fosse o mesmo que o volume de origem ao criar o volume como parte da criação do plano de replicação.
- Adicionou suporte para uma assinatura de pagamento conforme o uso (PAYGO) para o NetApp Intelligent Services no Azure Marketplace e adicionou um link para o Azure Marketplace na caixa de diálogo de teste gratuito.

  Para mais detalhes, consulte "Licenciamento de NetApp Disaster Recovery" e "Configurar licenciamento para NetApp Disaster Recovery" .

14 de julho de 2025

Versão 4.2.5

Funções de usuário no NetApp Disaster Recovery

O NetApp Disaster Recovery agora emprega funções para controlar o acesso que cada usuário tem a recursos e ações específicos.

O serviço usa as seguintes funções específicas do NetApp Disaster Recovery.

- **Administrador de recuperação de desastres**: execute quaisquer ações no NetApp Disaster Recovery.
- **Administrador de failover de recuperação de desastres**: execute ações de failover e migração no NetApp Disaster Recovery.
- **Administrador do aplicativo de recuperação de desastres**: Crie e modifique planos de replicação e inicie failovers de teste.
- **Visualizador de recuperação de desastres**: visualize informações no NetApp Disaster Recovery, mas não pode executar nenhuma ação.

Se estiver clicando no serviço NetApp Disaster Recovery e configurando-o pela primeira vez, você deverá ter a permissão **SnapCenterAdmin** ou ter a função **Organization Admin**.

Para mais detalhes, veja"Funções e permissões do usuário no NetApp Disaster Recovery" .

"Saiba mais sobre funções de acesso para todos os serviços".

Outras atualizações no NetApp Disaster Recovery

- Descoberta de rede aprimorada
- Melhorias de escalabilidade:
  - Filtragem dos metadados necessários em vez de todos os detalhes
  - Melhorias na descoberta para recuperar e atualizar recursos de VM mais rapidamente
  - Otimização de memória e otimização de desempenho para recuperação e atualização de dados
  - Melhorias na criação de clientes do vCenter SDK e no gerenciamento de pools
- Gerenciamento de dados obsoletos na próxima descoberta agendada ou manual:
  - Quando uma VM é excluída no vCenter, o NetApp Disaster Recovery agora a remove automaticamente do plano de replicação.
  - Quando um armazenamento de dados ou rede é excluído no vCenter, o NetApp Disaster Recovery agora o exclui do plano de replicação e do grupo de recursos.
  - Quando um cluster, host ou datacenter é excluído do vCenter, o NetApp Disaster Recovery agora o exclui do plano de replicação e do grupo de recursos.
- Agora você pode acessar a documentação do Swagger no modo anônimo do seu navegador. Você pode acessá-lo no NetApp Disaster Recovery na opção Configurações > Documentação da API ou diretamente no seguinte URL no modo anônimo do seu navegador: "Documentação do Swagger" .
- Em algumas situações, após uma operação de failback, o iGroup foi deixado para trás após a conclusão da operação. Esta atualização remove o iGroup se ele estiver obsoleto.
- Se o FQDN do NFS foi usado no plano de replicação, o NetApp Disaster Recovery agora o resolve para um endereço IP. Esta atualização é útil se o FQDN não puder ser resolvido no site de recuperação de desastres.
- Melhorias no alinhamento da interface do usuário
- Melhorias no log para capturar os detalhes de dimensionamento do vCenter após a descoberta bem-sucedida

30 de junho de 2025

Versão 4.2.4P2

Melhorias na descoberta

Esta atualização melhora o processo de descoberta, o que reduz o tempo necessário para a descoberta.

23 de junho de 2025

Versão 4.2.4P1

Melhorias no mapeamento de sub-redes

Esta atualização aprimora a caixa de diálogo Adicionar e editar mapeamento de sub-rede com uma nova funcionalidade de pesquisa. Agora você pode encontrar rapidamente sub-redes específicas inserindo termos de pesquisa, facilitando o gerenciamento de mapeamentos de sub-redes.

09 de junho de 2025

Versão 4.2.4

Suporte à solução de senha de administrador local do Windows (LAPS)

O Windows Local Administrator Password Solution (Windows LAPS) é um recurso do Windows que gerencia e faz backup automaticamente da senha de uma conta de administrador local no Active Directory.

Agora você pode selecionar opções de mapeamento de sub-rede e verificar a opção LAPS fornecendo os detalhes do controlador de domínio. Usando esta opção, você não precisa fornecer uma senha para cada uma de suas máquinas virtuais.

Para mais detalhes, consulte "Crie um plano de replicação" .

13 de maio de 2025

Versão 4.2.3

Mapeamento de sub-rede

Com esta versão, você pode gerenciar endereços IP em failover de uma nova maneira usando o mapeamento de sub-redes, que permite adicionar sub-redes para cada vCenter. Ao fazer isso, você define o CIDR IPv4, o gateway padrão e o DNS para cada rede virtual.

Após o failover, o NetApp Disaster Recovery determina o endereço IP apropriado de cada vNIC observando o CIDR fornecido para a rede virtual mapeada e o usa para derivar o novo endereço IP.

Por exemplo:

- RedeA = 10.1.1.0/24
- RedeB = 192.168.1.0/24

A VM1 tem uma vNIC (10.1.1.50) que está conectada à RedeA. A RedeA é mapeada para a RedeB nas configurações do plano de replicação.

No failover, o NetApp Disaster Recovery substitui a parte de rede do endereço IP original (10.1.1) e mantém o endereço de host (.50) do endereço IP original (10.1.1.50). Para VM1, o NetApp Disaster Recovery analisa as configurações CIDR da NetworkB e usa a parte da rede NetworkB 192.168.1, mantendo a parte do host (.50) para criar o novo endereço IP para VM1. O novo IP se torna 192.168.1.50.

Em resumo, o endereço do host permanece o mesmo, enquanto o endereço de rede é substituído pelo que estiver configurado no mapeamento de sub-rede do site. Isso permite que você gerencie a reatribuição de endereços IP em caso de failover com mais facilidade, especialmente se você tiver centenas de redes e milhares de VMs para gerenciar.

Para obter detalhes sobre como incluir o mapeamento de sub-redes em seus sites, consulte "Adicionar sites do servidor vCenter" .

Proteção contra pulos

Agora você pode pular a proteção para que o serviço não crie automaticamente um relacionamento de proteção reversa após um failover do plano de replicação. Isso é útil se você quiser executar operações adicionais no site restaurado antes de colocá-lo novamente online no NetApp Disaster Recovery.

Quando você inicia um failover, por padrão, o serviço cria automaticamente um relacionamento de proteção reversa para cada volume no plano de replicação, se o site de origem original estiver online. Isso significa que o serviço cria um relacionamento SnapMirror do site de destino de volta ao site de origem. O serviço também reverte automaticamente o relacionamento do SnapMirror quando você inicia um failback.

Ao iniciar um failover, agora você pode escolher a opção **Ignorar proteção**. Com isso, o serviço não reverte automaticamente o relacionamento do SnapMirror . Em vez disso, ele deixa o volume gravável em ambos os lados do plano de replicação.

Depois que o site de origem estiver online novamente, você poderá estabelecer a proteção reversa selecionando **Proteger recursos** no menu Ações do plano de replicação. Isso tenta criar um relacionamento de replicação reversa para cada volume no plano. Você pode executar esta tarefa repetidamente até que a proteção seja restaurada. Quando a proteção for restaurada, você poderá iniciar um failback da maneira usual.

Para obter detalhes sobre a proteção contra saltos, consulte "Falha na execução de aplicativos para um site remoto" .

Atualizações de agendamento do SnapMirror no plano de replicação

O NetApp Disaster Recovery agora oferece suporte ao uso de soluções externas de gerenciamento de snapshots, como o agendador de políticas nativo ONTAP SnapMirror ou integrações de terceiros com o ONTAP. Se cada armazenamento de dados (volume) no plano de replicação já tiver um relacionamento SnapMirror que esteja sendo gerenciado em outro lugar, você poderá usar esses instantâneos como pontos de recuperação no NetApp Disaster Recovery.

Para configurar, na seção Plano de replicação > Mapeamento de recursos, marque a caixa de seleção **Usar backups e agendamentos de retenção gerenciados pela plataforma** ao configurar o mapeamento de Datastores.

Quando a opção é selecionada, o NetApp Disaster Recovery não configura um agendamento de backup. No entanto, você ainda precisa configurar um cronograma de retenção porque snapshots ainda podem ser tirados para operações de teste, failover e failback.

Depois que isso for configurado, o serviço não fará nenhum snapshot agendado regularmente, mas dependerá da entidade externa para tirar e atualizar esses snapshots.

Para obter detalhes sobre como usar soluções de snapshots externos no plano de replicação, consulte "Crie um plano de replicação" .

16 de abril de 2025

Versão 4.2.2

Descoberta agendada para VMs

O NetApp Disaster Recovery realiza a descoberta uma vez a cada 24 horas. Com esta versão, agora você pode personalizar o cronograma de descoberta para atender às suas necessidades e reduzir o impacto no desempenho quando precisar. Por exemplo, se você tiver um grande número de VMs, poderá definir o

agendamento de descoberta para ser executado a cada 48 horas. Se você tiver um pequeno número de VMs, poderá definir o agendamento de descoberta para ser executado a cada 12 horas.

Se não quiser agendar a descoberta, você pode desabilitar a opção de descoberta agendada e atualizar a descoberta manualmente a qualquer momento.

Para mais detalhes, consulte "Adicionar sites do servidor vCenter" .

Suporte ao armazenamento de dados do grupo de recursos

Anteriormente, você só podia criar grupos de recursos por VMs. Com esta versão, você pode criar um grupo de recursos por armazenamentos de dados. Ao criar um plano de replicação e um grupo de recursos para esse plano, todas as VMs em um armazenamento de dados serão listadas. Isso é útil se você tiver um grande número de VMs e quiser agrupá-las por armazenamento de dados.

Você pode criar um grupo de recursos com um armazenamento de dados das seguintes maneiras:

- Ao adicionar um grupo de recursos usando armazenamentos de dados, você pode ver uma lista de armazenamentos de dados. Você pode selecionar um ou mais armazenamentos de dados para criar um grupo de recursos.
- Ao criar um plano de replicação e um grupo de recursos dentro do plano, você pode ver as VMs nos armazenamentos de dados.

Para mais detalhes, consulte "Crie um plano de replicação" .

Notificações de teste gratuito ou expiração de licença

Esta versão fornece notificações de que o teste gratuito irá expirar em 60 dias para garantir que você tenha tempo de obter uma licença. Esta versão também fornece notificações sobre o dia em que a licença expira.

Notificação de atualizações de serviço

Com esta versão, um banner aparece na parte superior para indicar que os serviços estão sendo atualizados e que o serviço foi colocado em modo de manutenção. O banner aparece quando o serviço está sendo atualizado e desaparece quando a atualização é concluída. Embora você possa continuar trabalhando na interface do usuário enquanto a atualização estiver em andamento, não será possível enviar novos trabalhos. Os trabalhos agendados serão executados após a conclusão da atualização e o serviço retornar ao modo de produção.

10 de março de 2025

Versão 4.2.1

Suporte a proxy inteligente

O agente do NetApp Console oferece suporte ao proxy inteligente. O proxy inteligente é uma maneira leve, segura e eficiente de conectar seu sistema local ao NetApp Disaster Recovery. Ele fornece uma conexão segura entre seu sistema e o NetApp Disaster Recovery sem exigir uma VPN ou acesso direto à Internet. Essa implementação de proxy otimizada descarrega o tráfego de API dentro da rede local.

Quando um proxy é configurado, o NetApp Disaster Recovery tenta se comunicar diretamente com o VMware ou o ONTAP e usa o proxy configurado se a comunicação direta falhar.

A implementação do proxy de NetApp Disaster Recovery requer comunicação na porta 443 entre o agente do

Console e quaisquer servidores vCenter e matrizes ONTAP usando um protocolo HTTPS. O agente NetApp Disaster Recovery dentro do agente do Console se comunica diretamente com o VMware vSphere, o VC ou o ONTAP ao executar qualquer ação.

Para obter mais informações sobre o proxy inteligente para NetApp Disaster Recovery, consulte "Configure sua infraestrutura para NetApp Disaster Recovery" .

Para obter mais informações sobre a configuração geral de proxy no NetApp Console, consulte "Configurar o agente do Console para usar um servidor proxy" .

Encerre o teste gratuito a qualquer momento

Você pode interromper o teste gratuito a qualquer momento ou esperar até que ele expire.

Ver "Encerrar o teste gratuito" .

19 de fevereiro de 2025

Versão 4.2

Suporte ASA r2 para VMs e datastores em armazenamento VMFS

Esta versão do NetApp Disaster Recovery oferece suporte ao ASA r2 para VMs e datastores no armazenamento VMFS. Em um sistema ASA r2, o software ONTAP oferece suporte à funcionalidade SAN essencial e remove recursos não suportados em ambientes SAN.

Esta versão oferece suporte aos seguintes recursos para ASA r2:

- Provisionamento de grupo de consistência para armazenamento primário (somente grupo de consistência plano, ou seja, apenas um nível sem estrutura hierárquica)
- Operações de backup (grupo de consistência), incluindo automação SnapMirror

O suporte para ASA r2 no NetApp Disaster Recovery usa o ONTAP 9.16.1.

Embora os armazenamentos de dados possam ser montados em um volume ONTAP ou em uma unidade de armazenamento ASA r2, um grupo de recursos no NetApp Disaster Recovery não pode incluir um armazenamento de dados do ONTAP e um do ASA r2. Você pode selecionar um armazenamento de dados do ONTAP ou um armazenamento de dados do ASA r2 em um grupo de recursos.

30 de outubro de 2024

Relatórios

Agora você pode gerar e baixar relatórios para ajudar a analisar seu cenário. Relatórios pré-projetados resumem failovers e failbacks, mostram detalhes de replicação em todos os sites e mostram detalhes do trabalho dos últimos sete dias.

Consulte "Criar relatórios de recuperação de desastres" .

Teste gratuito de 30 dias

Agora você pode se inscrever para um teste gratuito de 30 dias do NetApp Disaster Recovery. Anteriormente, os testes gratuitos eram de 90 dias.

Consulte "Configurar licenciamento" .

Desabilitar e habilitar planos de replicação

Uma versão anterior incluía atualizações na estrutura de programação de testes de failover, o que era necessário para dar suporte a programações diárias e semanais. Esta atualização exigiu que você desabilitasse e reabilitasse todos os planos de replicação existentes para que você pudesse usar os novos agendamentos de testes de failover diários e semanais. Este é um requisito único.

Veja como:

1. No menu, selecione **Planos de replicação**.
2. Selecione um plano e selecione o ícone Ações para mostrar o menu suspenso.
3. Selecione **Desativar**.
4. Após alguns minutos, selecione **Ativar**.

Mapeamento de pastas

Ao criar um plano de replicação e mapear recursos de computação, agora você pode mapear pastas para que as VMs sejam recuperadas em uma pasta especificada para datacenter, cluster e host.

Para mais detalhes, consulte "Crie um plano de replicação" .

Detalhes da VM disponíveis para failover, failback e failover de teste

Quando ocorre uma falha e você está iniciando um failover, executando um failback ou testando o failover, agora você pode ver detalhes das VMs e identificar quais VMs não foram reiniciadas.

Consulte "Falha na execução de aplicativos para um site remoto" .

Atraso na inicialização da VM com sequência de inicialização ordenada

Ao criar um plano de replicação, agora você pode definir um atraso de inicialização para cada VM no plano. Isso permite que você defina uma sequência para as VMs iniciarem, a fim de garantir que todas as suas VMs de prioridade um estejam em execução antes que as VMs de prioridade subsequentes sejam iniciadas.

Para mais detalhes, consulte "Crie um plano de replicação" .

Informações do sistema operacional da VM

Ao criar um plano de replicação, agora você pode ver o sistema operacional de cada VM no plano. Isso é útil para decidir como agrupar VMs em um grupo de recursos.

Para mais detalhes, consulte "Crie um plano de replicação" .

Alias de nome de VM

Ao criar um plano de replicação, agora você pode adicionar um prefixo e um sufixo aos nomes de VM no local de recuperação de desastres. Isso permite que você use um nome mais descritivo para as VMs no plano.

Para mais detalhes, consulte "Crie um plano de replicação" .

Limpar instantâneos antigos

Você pode excluir quaisquer snapshots que não sejam mais necessários além da contagem de retenção especificada. Os instantâneos podem se acumular ao longo do tempo quando você diminui sua contagem de retenção de instantâneos, e agora você pode removê-los para liberar espaço. Você pode fazer isso a qualquer momento, sob demanda, ou ao excluir um plano de replicação.

Para mais detalhes, consulte "Gerenciar sites, grupos de recursos, planos de replicação, armazenamentos de dados e informações de máquinas virtuais" .

Reconciliar instantâneos

Agora você pode reconciliar snapshots que estão fora de sincronia entre a origem e o destino. Isso pode ocorrer se os snapshots forem excluídos em um destino fora do NetApp Disaster Recovery. O serviço exclui o snapshot na origem automaticamente 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.

Para mais detalhes, consulte "Gerenciar planos de replicação" .

20 de setembro de 2024

Suporte para datastores VMware VMFS locais para locais

Esta versão inclui suporte para VMs montadas em datastores do sistema de arquivos de máquina virtual VMware vSphere (VMFS) para iSCSI e FC protegidos para armazenamento local. Anteriormente, o serviço fornecia uma *prévia de tecnologia* com suporte a armazenamentos de dados VMFS para iSCSI e FC.

Aqui estão algumas considerações adicionais sobre os protocolos iSCSI e FC:

- O suporte ao FC é para protocolos de front-end do cliente, não para replicação.
- O NetApp Disaster Recovery suporta apenas um único LUN por volume ONTAP . O volume não deve ter vários LUNs.
- Para qualquer plano de replicação, o volume ONTAP de destino deve usar os mesmos protocolos que o volume ONTAP de origem que hospeda as VMs protegidas. Por exemplo, se a origem usa um protocolo FC, o destino também deve usar FC.

02 de agosto de 2024

Suporte para datastores VMware VMFS locais para locais para FC

Esta versão inclui uma *prévia tecnológica* de suporte para VMs montadas em armazenamentos de dados do sistema de arquivos de máquina virtual (VMFS) VMware vSphere para FC protegido para armazenamento local. Anteriormente, o serviço fornecia uma prévia de tecnologia com suporte a armazenamentos de dados VMFS para iSCSI.

A NetApp não cobra por nenhuma capacidade de carga de trabalho visualizada.

Cancelamento de trabalho

Com esta versão, agora você pode cancelar um trabalho na interface do Job Monitor.

Consulte "Monitorar trabalhos" .

17 de julho de 2024

Cronogramas de testes de failover

Esta versão inclui atualizações na estrutura de agendamento de testes de failover, que eram necessárias para dar suporte a agendamentos diários e semanais. Esta atualização exige que você desabilite e reabilite todos os planos de replicação existentes para que você possa usar os novos agendamentos de testes de failover diários e semanais. Este é um requisito único.

Veja como:

1. No menu, selecione **Planos de replicação**.
2. Selecione um plano e selecione o ícone Ações para mostrar o menu suspenso.
3. Selecione **Desativar**.
4. Após alguns minutos, selecione **Ativar**.

Atualizações do plano de replicação

Esta versão inclui atualizações nos dados do plano de replicação, o que resolve o problema de "instantâneo não encontrado". Isso requer que você altere a contagem de retenção em todos os planos de replicação para 1 e inicie um instantâneo sob demanda. Este processo cria um novo backup e remove todos os backups mais antigos.

Veja como:

1. No menu, selecione **Planos de replicação**.
2. Selecione o plano de replicação, selecione a guia **Mapeamento de failover** e selecione o ícone de lápis **Editar**.
3. Selecione a seta **Datastores** para expandi-la.
4. Observe o valor da contagem de retenção no plano de replicação. Você precisa restaurar esse valor original quando terminar essas etapas.
5. Reduza a contagem para 1.
6. Inicie um snapshot sob demanda. Para isso, na página do plano de replicação, selecione o plano, selecione o ícone Ações e selecione **Tirar instantâneo agora**.
7. Após a conclusão bem-sucedida do trabalho de instantâneo, aumente a contagem no plano de replicação de volta ao valor original anotado na primeira etapa.
8. Repita essas etapas para todos os planos de replicação existentes.

05 de julho de 2024

Esta versão do NetApp Disaster Recovery inclui as seguintes atualizações:

Suporte para AFF série A

Esta versão oferece suporte às plataformas de hardware NetApp AFF série A.

Suporte para datastores VMware VMFS locais para locais

Esta versão inclui uma *prévia tecnológica* de suporte para VMs montadas em armazenamentos de dados do sistema de arquivos de máquina virtual (VMFS) VMware vSphere protegidos no armazenamento local. Com

esta versão, a recuperação de desastres é suportada em uma prévia de tecnologia para cargas de trabalho VMware locais para ambientes VMware locais com armazenamentos de dados VMFS.

A NetApp não cobra por nenhuma capacidade de carga de trabalho visualizada.

Atualizações do plano de replicação

Você pode adicionar um plano de replicação mais facilmente filtrando VMs por armazenamento de dados na página Aplicativos e selecionando mais detalhes de destino na página Mapeamento de recursos. Consulte "Crie um plano de replicação" .

Editar planos de replicação

Com esta versão, a página de mapeamentos de failover foi aprimorada para maior clareza.

Consulte "Gerenciar planos" .

Editar VMs

Com esta versão, o processo de edição de VMs no plano incluiu algumas pequenas melhorias na interface do usuário.

Consulte "Gerenciar VMs" .

Atualizações de failover

Antes de iniciar um failover, agora você pode determinar o status das VMs e se elas estão ligadas ou desligadas. O processo de failover agora permite que você tire um snapshot ou escolha os snapshots.

Consulte "Falha na execução de aplicativos para um site remoto" .

Cronogramas de testes de failover

Agora você pode editar os testes de failover e definir agendamentos diários, semanais e mensais para o teste de failover.

Consulte "Gerenciar planos" .

Atualizações nas informações de pré-requisitos

As informações sobre pré-requisitos do NetApp Disaster Recovery foram atualizadas.

Consulte "Pré-requisitos do NetApp Disaster Recovery" .

15 de maio de 2024

Esta versão do NetApp Disaster Recovery inclui as seguintes atualizações:

Replicando cargas de trabalho do VMware de local para local

Agora isso foi lançado como um recurso de disponibilidade geral. Anteriormente, era uma prévia de tecnologia com funcionalidade limitada.

Atualizações de licenciamento

Com o NetApp Disaster Recovery, você pode se inscrever para um teste gratuito de 90 dias, comprar uma assinatura pré-paga (PAYGO) no Amazon Marketplace ou Bring Your Own License (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém do seu representante de vendas NetApp ou do site de suporte NetApp (NSS).

Para obter detalhes sobre a configuração do licenciamento para o NetApp Disaster Recovery, consulte"Configurar licenciamento" .

"Saiba mais sobre a NetApp Disaster Recovery".

05 de março de 2024

Esta é a versão de disponibilidade geral do NetApp Disaster Recovery, que inclui as seguintes atualizações.

Atualizações de licenciamento

Com o NetApp Disaster Recovery, você pode se inscrever para um teste gratuito de 90 dias ou Traga sua própria licença (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém do seu representante de vendas NetApp . Você pode usar o número de série da licença para ativar o BYOL nas assinaturas do NetApp Console . As cobranças do NetApp Disaster Recovery são baseadas na capacidade provisionada dos datastores.

Para obter detalhes sobre como configurar o licenciamento do NetApp Disaster Recovery, consulte [link para a documentação]. "Configurar licenciamento" .

Para obter detalhes sobre o gerenciamento de licenças para **todos** os serviços de dados do NetApp Console , consulte "Gerenciar licenças para todos os serviços de dados do NetApp Console" .

Editar agendamentos

Com esta versão, agora você pode configurar agendamentos para testar testes de conformidade e failover para garantir que eles funcionarão corretamente caso você precise deles.

Para mais detalhes, consulte "Crie o plano de replicação" .

01 de fevereiro de 2024

Esta versão de pré-lançamento do NetApp Disaster Recovery inclui as seguintes atualizações:

Aprimoramento de rede

Com esta versão, agora você pode redimensionar os valores de CPU e RAM da VM. Agora você também pode selecionar um DHCP de rede ou um endereço IP estático para a VM.

- DHCP: se você escolher esta opção, fornecerá credenciais para a VM.
- IP estático: você pode selecionar as mesmas informações ou informações diferentes da VM de origem. Se você escolher o mesmo que a fonte, não precisará inserir credenciais. Por outro lado, se você optar por usar informações diferentes da fonte, poderá fornecer as credenciais, endereço IP, máscara de sub-rede, DNS e informações de gateway.

Para mais detalhes, consulte "Crie um plano de replicação" .

Scripts personalizados

Agora podem ser incluídos como processos pós-failover. Com scripts personalizados, você pode fazer com que o NetApp Disaster Recovery execute seu script após um processo de failover. Por exemplo, você pode usar um script personalizado para retomar todas as transações do banco de dados após a conclusão do failover.

Para mais detalhes, consulte "Failover para um site remoto" .

Relacionamento SnapMirror

Agora você pode criar um relacionamento SnapMirror enquanto desenvolve o plano de replicação. Anteriormente, você tinha que criar o relacionamento fora do NetApp Disaster Recovery.

Para mais detalhes, consulte "Crie um plano de replicação" .

Grupos de consistência

Ao criar um plano de replicação, você pode incluir VMs de volumes diferentes e SVMs diferentes. O NetApp Disaster Recovery cria um instantâneo de grupo de consistência incluindo todos os volumes e atualiza todos os locais secundários.

Para mais detalhes, consulte "Crie um plano de replicação" .

Opção de atraso na inicialização da VM

Ao criar um plano de replicação, você pode adicionar VMs a um Grupo de Recursos. Com Grupos de Recursos, você pode definir um atraso em cada VM para que elas sejam inicializadas em uma sequência atrasada.

Para mais detalhes, consulte "Crie um plano de replicação" .

Cópias de instantâneo consistentes com o aplicativo

Você pode especificar a criação de cópias de Snapshot consistentes com o aplicativo. O serviço desativará o aplicativo e, em seguida, fará um Snapshot para obter um estado consistente do aplicativo.

Para mais detalhes, consulte "Crie um plano de replicação" .

11 de janeiro de 2024

Esta versão de pré-visualização do NetApp Disaster Recovery inclui as seguintes atualizações:

Painel mais rápido

Com esta versão, você pode acessar informações em outras páginas do Painel mais rapidamente.

"Saiba mais sobre a NetApp Disaster Recovery".

20 de outubro de 2023

Esta versão de pré-visualização do NetApp Disaster Recovery inclui as seguintes atualizações.

Proteja cargas de trabalho VMware locais baseadas em NFS

Agora, com o NetApp Disaster Recovery, você pode proteger suas cargas de trabalho VMware locais baseadas em NFS contra desastres em outro ambiente VMware local baseado em NFS, além da nuvem pública. O NetApp Disaster Recovery orquestra a conclusão dos planos de recuperação de desastres.

> Com esta oferta de pré-visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

"Saiba mais sobre a NetApp Disaster Recovery".

27 de setembro de 2023

Esta versão de pré-visualização do NetApp Disaster Recovery inclui as seguintes atualizações:

Atualizações do painel

Agora você pode selecionar as opções no Painel de Controle, facilitando a revisão rápida das informações. Além disso, o Painel agora mostra o status de failovers e migrações.

Consulte "Veja a integridade dos seus planos de recuperação de desastres no Painel" .

Atualizações do plano de replicação

- **RPO**: Agora você pode inserir o Objetivo de Ponto de Recuperação (RPO) e a contagem de Retenção na seção Datastores do plano de Replicação. Isso indica a quantidade de dados que deve existir e que não seja mais antiga que o tempo definido. Se, por exemplo, você definir 5 minutos, o sistema poderá perder até 5 minutos de dados se ocorrer um desastre, sem afetar as necessidades críticas dos negócios.

  Consulte "Crie um plano de replicação" .

- **Melhorias de rede**: Ao mapear a rede entre os locais de origem e destino na seção de máquinas virtuais do plano de replicação, o NetApp Disaster Recovery agora oferece duas opções: DHCP ou IP estático. Anteriormente, apenas DHCP era suportado. Para IPs estáticos, você configura a sub-rede, o gateway e os servidores DNS. Além disso, agora você pode inserir credenciais para máquinas virtuais.

  Consulte "Crie um plano de replicação" .

- **Editar agendamentos**: Agora você pode atualizar agendamentos de planos de replicação.

  Consulte "Gerenciar recursos" .

- * Automação do SnapMirror *: Ao criar o plano de replicação nesta versão, você pode definir o relacionamento do SnapMirror entre os volumes de origem e de destino em uma das seguintes configurações:
  - 1 a 1
  - 1 para muitos em uma arquitetura fanout
  - Muitos para 1 como um grupo de consistência
  - Muitos para muitos

    Consulte "Crie um plano de replicação" .

01 de agosto de 2023

Prévia do NetApp Disaster Recovery

O NetApp Disaster Recovery Preview é um serviço de recuperação de desastres baseado em nuvem que automatiza fluxos de trabalho de recuperação de desastres. Inicialmente, com a visualização do NetApp Disaster Recovery , você pode proteger suas cargas de trabalho VMware locais baseadas em NFS executando armazenamento NetApp no VMware Cloud (VMC) na AWS com o Amazon FSx para ONTAP.

> Com esta oferta de pré-visualização, a NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da disponibilidade geral.

"Saiba mais sobre a NetApp Disaster Recovery".

Esta versão inclui as seguintes atualizações:

Atualização de grupos de recursos para ordem de inicialização

Ao criar um plano de recuperação de desastres ou replicação, você pode adicionar máquinas virtuais a grupos de recursos funcionais. Grupos de recursos permitem que você coloque um conjunto de máquinas virtuais dependentes em grupos lógicos que atendem aos seus requisitos. Por exemplo, grupos podem conter ordens de inicialização que podem ser executadas na recuperação. Com esta versão, cada grupo de recursos pode incluir uma ou mais máquinas virtuais. As máquinas virtuais serão ligadas com base na sequência em que você as incluir no plano. Consulte "Selecione aplicativos para replicar e atribuir grupos de recursos" .

Verificação de replicação

Depois de criar o plano de recuperação de desastres ou replicação, identificar a recorrência no assistente e iniciar uma replicação para um site de recuperação de desastres, a cada 30 minutos o NetApp Disaster Recovery verifica se a replicação está realmente ocorrendo de acordo com o plano. Você pode monitorar o progresso na página Job Monitor. Consulte "Replicar aplicativos para outro site" .

O plano de replicação mostra os cronogramas de transferência do objetivo do ponto de recuperação (RPO)

Ao criar um plano de recuperação de desastres ou replicação, você seleciona as VMs. Nesta versão, agora você pode visualizar o SnapMirror associado a cada um dos volumes associados ao armazenamento de dados ou à VM. Você também pode ver os cronogramas de transferência de RPO associados ao cronograma do SnapMirror . O RPO ajuda você a determinar se seu cronograma de backup é suficiente para recuperação após um desastre. Consulte "Crie um plano de replicação" .

Atualização do Job Monitor

A página Job Monitor agora inclui uma opção Atualizar para que você possa obter um status atualizado das operações. Consulte "Monitorar trabalhos de recuperação de desastres" .

18 de maio de 2023

Esta é a versão inicial do NetApp Disaster Recovery.

Serviço de recuperação de desastres baseado em nuvem

O NetApp Disaster Recovery é um serviço de recuperação de desastres baseado em nuvem que automatiza fluxos de trabalho de recuperação de desastres. Inicialmente, com a visualização do NetApp Disaster

Recovery , você pode proteger suas cargas de trabalho VMware locais baseadas em NFS executando armazenamento NetApp no VMware Cloud (VMC) na AWS com o Amazon FSx para ONTAP.

"Saiba mais sobre a NetApp Disaster Recovery".

Limitações na NetApp Disaster Recovery

Limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportados por esta versão do serviço ou que não interoperam corretamente com ele.

Aguarde até que o failback seja concluído antes de executar a descoberta

Após a conclusão de um failover, não inicie a descoberta no vCenter de origem manualmente. Aguarde até que o failback seja concluído e inicie a descoberta no vCenter de origem.

O NetApp Console pode não detectar o Amazon FSx for NetApp ONTAP

Às vezes, o NetApp Console não descobre o Amazon FSx for NetApp ONTAP . Isso pode ocorrer porque as credenciais do FSx não estavam corretas.

Solução alternativa: adicione o cluster Amazon FSx for NetApp ONTAP no NetApp Console e atualize periodicamente o cluster para exibir quaisquer alterações.

Se você precisar remover o cluster ONTAP FSx do NetApp Disaster Recovery, conclua as seguintes etapas:

1. No agente do NetApp Console , use as opções de conectividade do seu provedor de nuvem, conecte-se à VM Linux na qual o agente do Console é executado, reinicie o serviço "occm" usando o `docker restart occm` comando.

Consulte "Gerenciar agentes de console existentes" .

1. Na página NetApp Console Systems, adicione o sistema Amazon FSx for ONTAP novamente e forneça as credenciais do FSx.

   Consulte "Crie um sistema de arquivos Amazon FSx for NetApp ONTAP" .

2. No NetApp Disaster Recovery, selecione **Sites**, na linha vCenter selecione a opção **Ações***  **e, no menu Ações, selecione *Atualizar** para atualizar a descoberta do FSx no NetApp Disaster Recovery.

   Isso redescobre o armazenamento de dados, suas máquinas virtuais e seu relacionamento de destino.

Limitações do Google Cloud NetApp Volumes

- Após executar um teste de failover, você precisa esperar pelo menos 52 horas para excluir o volume clonado. Você precisa excluir o volume manualmente. Após 52 horas, você poderá testar o failover novamente.
- Se alguma parte da operação de montagem falhar, o failover não será bem-sucedido e as tarefas expirarão. O Google pode levar até três dias para analisar o problema, período durante o qual todas as operações relacionadas ao armazenamento de dados no vCenter ficam bloqueadas.

Começar

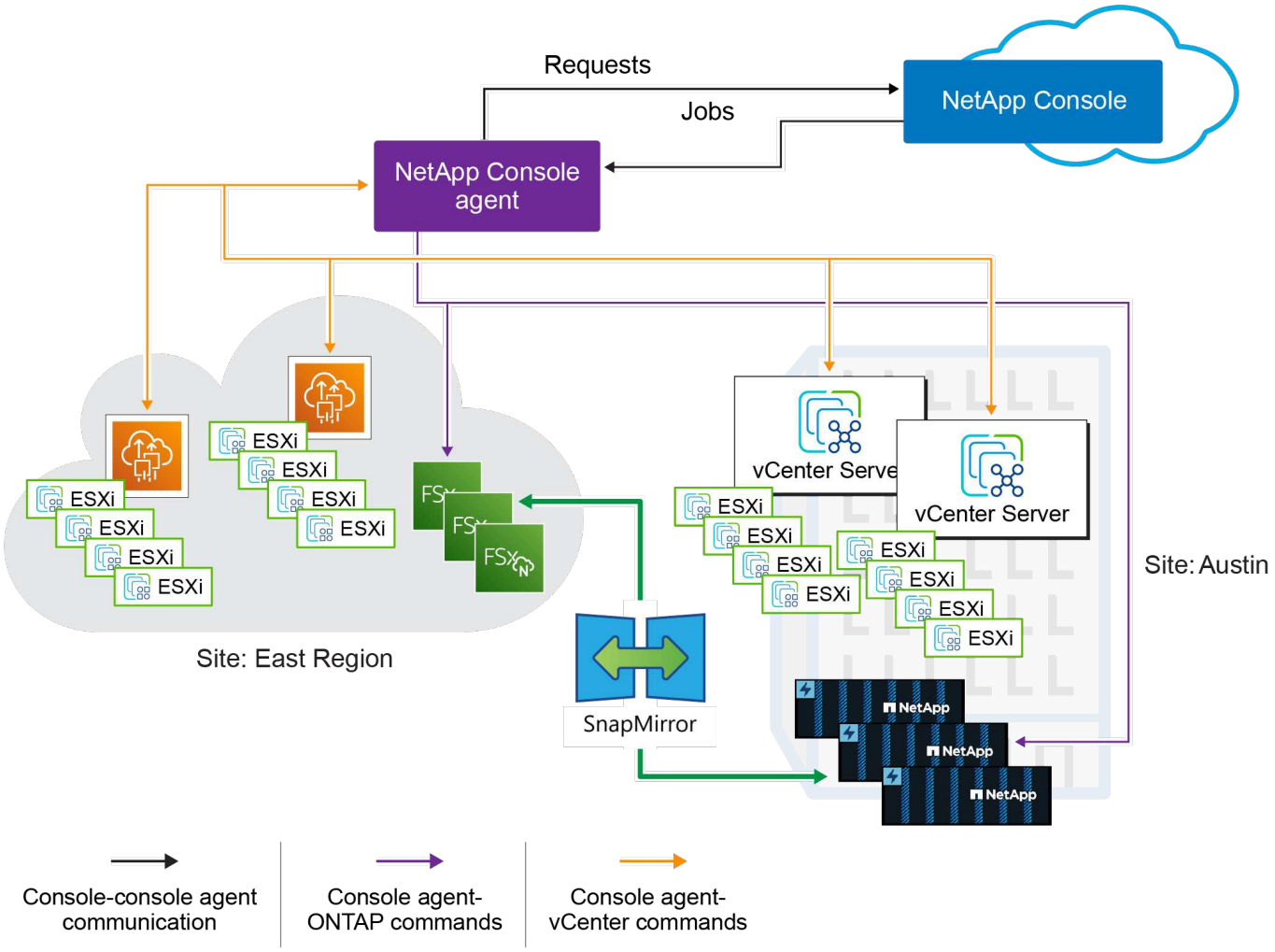
Saiba mais sobre o NetApp Disaster Recovery para VMware

A recuperação de desastres na nuvem é uma maneira resiliente e econômica de proteger cargas de trabalho contra interrupções do site e eventos de corrupção de dados. Com o NetApp Disaster Recovery for VMware, você pode replicar suas cargas de trabalho de VM ou datastore VMware locais executando armazenamento ONTAP para um data center definido por software VMware em uma nuvem pública usando o armazenamento em nuvem NetApp ou para outro ambiente VMware local com armazenamento ONTAP como um site de recuperação de desastres. Você também pode usar o Disaster Recovery para migrar cargas de trabalho de VM de um site para outro.

O NetApp Disaster Recovery é um serviço de recuperação de desastres baseado em nuvem que automatiza fluxos de trabalho de recuperação de desastres. Com o NetApp Disaster Recovery, você pode proteger suas cargas de trabalho locais baseadas em NFS e os armazenamentos de dados do sistema de arquivos de máquina virtual (VMFS) VMware vSphere para iSCSI e FC executando o armazenamento NetApp em um dos seguintes locais:

- Amazon Elastic VMware Service (EVS) com Amazon FSx for NetApp ONTAP Para obter detalhes, consulte"Introdução ao NetApp Disaster Recovery usando o Amazon Elastic VMware Service e o Amazon FSx for NetApp ONTAP" .
- VMware Cloud (VMC) na AWS com Amazon FSx for NetApp ONTAP
- Azure VMware Solution (AVS) com NetApp Cloud Volumes ONTAP (iSCSI) (visualização privada)
- Google Cloud VMware Engine (GCVE) com Google Cloud NetApp Volumes
- Outro ambiente VMware local baseado em NFS e/ou VMFS (iSCSI/FC) com armazenamento ONTAP

O NetApp Disaster Recovery usa a tecnologia ONTAP SnapMirror com orquestração VMware nativa integrada para proteger VMs VMware e suas imagens de sistema operacional em disco associadas, mantendo todos os benefícios de eficiência de armazenamento do ONTAP. A recuperação de desastres usa essas tecnologias como transporte de replicação para o local de recuperação de desastres. Isso permite a melhor eficiência de armazenamento do setor (compactação e desduplicação) em sites primários e secundários.



NetApp Console

O NetApp Disaster Recovery pode ser acessado por meio do NetApp Console.

O NetApp Console fornece gerenciamento centralizado de serviços de armazenamento e dados da NetApp em ambientes locais e na nuvem em nível empresarial. O Console é necessário para acessar e usar os serviços de dados do NetApp . Como uma interface de gerenciamento, ele permite que você gerencie muitos recursos de armazenamento a partir de uma única interface. Os administradores do console podem controlar o acesso ao armazenamento e aos serviços de todos os sistemas da empresa.

Você não precisa de uma licença ou assinatura para começar a usar o NetApp Console e só incorrerá em cobranças quando precisar implantar agentes do Console na sua nuvem para garantir a conectividade com seus sistemas de armazenamento ou serviços de dados do NetApp . No entanto, alguns serviços de dados da NetApp acessíveis pelo Console são licenciados ou baseados em assinatura.

Saiba mais sobre o "NetApp Console" .

Benefícios de usar o NetApp Disaster Recovery para VMware

O NetApp Disaster Recovery oferece os seguintes benefícios:

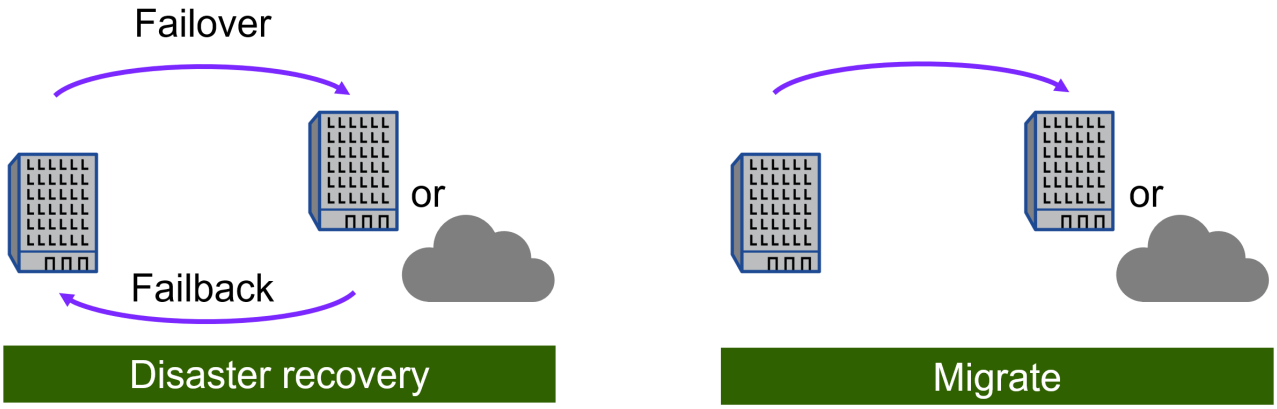
- Experiência de usuário simplificada para descoberta e recuperação de aplicativos do vCenter com múltiplas operações de recuperação em um determinado momento.

- Menor custo total de propriedade com menor custo de operações e capacidade de criar e ajustar planos de recuperação de desastres com recursos mínimos.
- Preparação contínua para recuperação de desastres com testes de failover virtual que não interrompem as operações. Você pode testar regularmente seus planos de failover de DR sem afetar as cargas de trabalho de produção.
- Menor tempo de retorno com mudanças dinâmicas no seu ambiente de TI e capacidade de abordar isso em seus planos de recuperação de desastres.
- Capacidade de gerenciar as camadas de armazenamento e virtuais por meio da orquestração de backend do ONTAP e do VMware ao mesmo tempo, sem a necessidade de dispositivos de servidor virtual (VSAs) que precisam ser implantados e mantidos.
- Soluções de DR para VMware podem exigir muitos recursos. Muitas soluções de DR replicam VMs na camada virtual do VMware usando VSAs, o que pode consumir mais recursos de computação e perder as valiosas eficiências de armazenamento do ONTAP. Como o Disaster Recovery usa a tecnologia ONTAP SnapMirror , ele pode replicar dados de armazenamentos de dados de produção para o site de DR usando nosso modelo de replicação incremental contínua com todas as eficiências nativas de compactação e desduplicação de dados do ONTAP.

O que você pode fazer com o NetApp Disaster Recovery para VMware

O NetApp Disaster Recovery oferece a você o uso completo de diversas tecnologias da NetApp para atingir os seguintes objetivos:

- Replique aplicativos VMware em seu site de produção local para um site remoto de recuperação de desastres na nuvem ou no local usando a replicação do SnapMirror .
- Migre cargas de trabalho do VMware do seu site original para outro site.
- Realize um teste de failover. Quando você faz isso, o serviço cria máquinas virtuais temporárias. A Recuperação de Desastres cria um novo volume FlexClone a partir do snapshot selecionado, e um armazenamento de dados temporário, que é apoiado pelo volume FlexClone , é mapeado para os hosts ESXi. Este processo não consome capacidade física adicional no armazenamento ONTAP local ou no FSx para armazenamento ONTAP da NetApp na AWS. O volume de origem original não é modificado e os trabalhos de réplica podem continuar mesmo durante a recuperação de desastres.
- Em caso de desastre, faça failover do seu site principal sob demanda para o site de recuperação de desastres, que pode ser o VMware Cloud on AWS com Amazon FSx for NetApp ONTAP ou um ambiente VMware local com ONTAP.
- Após a resolução do desastre, faça o failback sob demanda do site de recuperação de desastres para o site principal.
- Agrupe VMs ou armazenamentos de dados em grupos de recursos lógicos para um gerenciamento eficiente.



A configuração do servidor vSphere é feita fora do NetApp Disaster Recovery no vSphere Server.

Custo

A NetApp não cobra pelo uso da versão de avaliação do NetApp Disaster Recovery.

O NetApp Disaster Recovery pode ser usado com uma licença da NetApp ou com um plano de assinatura anual por meio da Amazon Web Services.

Alguns lançamentos incluem uma prévia da tecnologia. A NetApp não cobra por nenhuma capacidade de carga de trabalho visualizada. Ver"Novidades no NetApp Disaster Recovery" para obter informações sobre as últimas novidades tecnológicas.

Licenciamento

Você pode usar os seguintes tipos de licença:

- Inscreva-se para um teste gratuito de 30 dias.
- Compre uma assinatura pré-paga (PAYGO) com o Amazon Web Services (AWS) Marketplace ou o Microsoft Azure Marketplace. Esta licença permite que você compre uma licença de capacidade protegida fixa sem nenhum compromisso de longo prazo.
- Traga sua própria licença (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém do seu representante de vendas NetApp . Você pode usar o número de série da licença para ativar o BYOL no NetApp Console.

As licenças para todos os serviços de dados do NetApp são gerenciadas por meio de assinaturas no NetApp Console. Depois de configurar seu BYOL, você poderá ver uma licença ativa para o serviço no Console.

O serviço é licenciado com base na quantidade de dados hospedados em volumes ONTAP protegidos. O serviço determina quais volumes devem ser considerados para fins de licenciamento mapeando VMs protegidas para seus armazenamentos de dados do vCenter. Cada armazenamento de dados é hospedado em um volume ONTAP ou LUN. A capacidade usada relatada pelo ONTAP para esse volume ou LUN é usada para determinações de licenciamento.

Volumes protegidos podem hospedar muitas VMs. Alguns podem não fazer parte de um grupo de recursos de NetApp Disaster Recovery . Independentemente disso, o armazenamento consumido por todas as VMs naquele volume ou LUN é usado em relação à capacidade máxima da licença.

> As cobranças do NetApp Disaster Recovery são baseadas na capacidade usada dos armazenamentos de dados no site de origem quando há pelo menos uma VM com um plano de replicação. A capacidade para um armazenamento de dados com failover não está incluída na capacidade permitida. Para um BYOL, se os dados excederem a capacidade permitida, as operações no serviço serão limitadas até que você obtenha uma licença de capacidade adicional ou atualize a licença no NetApp Console.

Para obter detalhes sobre a configuração do licenciamento para o NetApp Disaster Recovery, consulte"Configurar o licenciamento do NetApp Disaster Recovery" .

Teste gratuito de 30 dias

Você pode experimentar o NetApp Disaster Recovery usando uma avaliação gratuita de 30 dias.

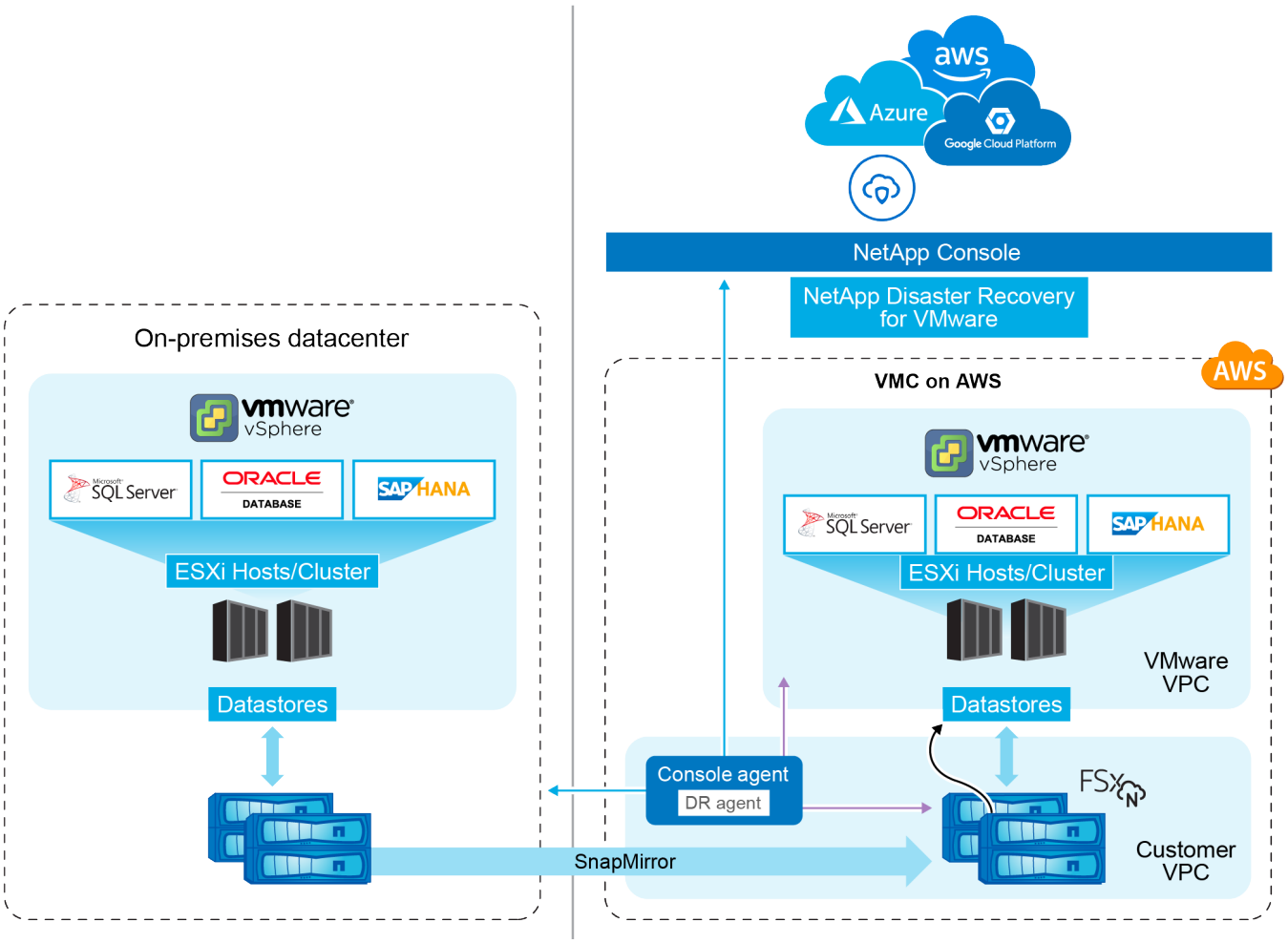
Para continuar após o teste de 30 dias, você precisará obter uma assinatura pré-paga (PAYGO) do seu provedor de nuvem ou comprar uma licença BYOL da NetApp.

Você pode comprar uma licença a qualquer momento e não será cobrado até o término do teste de 30 dias.

Como funciona a NetApp Disaster Recovery

O NetApp Disaster Recovery é um serviço hospedado no ambiente de software como serviço (SaaS) do NetApp Console . A recuperação de desastres pode recuperar cargas de trabalho replicadas de um site local para o Amazon FSx for ONTAP ou para outro site local. Este serviço automatiza a recuperação do nível SnapMirror , por meio do registro de máquinas virtuais no VMware Cloud na AWS, e para mapeamentos de rede diretamente na plataforma de virtualização e segurança de rede da VMware, NSX-T. Este recurso está incluído em todos os ambientes do Virtual Machine Cloud.

O NetApp Disaster Recovery usa a tecnologia ONTAP SnapMirror , que fornece replicação altamente eficiente e preserva as eficiências de snapshot incremental e permanente do ONTAP . A replicação do SnapMirror garante que cópias de snapshot consistentes com o aplicativo estejam sempre sincronizadas e que os dados possam ser usados imediatamente após um failover.



Quando ocorre um desastre, este serviço ajuda você a recuperar máquinas virtuais no outro ambiente VMware local ou VMC, interrompendo os relacionamentos do SnapMirror e tornando o site de destino ativo.

- O serviço também permite que você faça failback de máquinas virtuais para o local de origem original.
- Você pode testar o processo de failover de recuperação de desastres sem interromper as máquinas virtuais originais. O teste recupera máquinas virtuais para uma rede isolada criando um FlexClone do volume.
- Para o processo de failover ou failover de teste, você pode escolher o snapshot mais recente (padrão) ou selecionado para recuperar sua máquina virtual.

Componentes da Recuperação de Desastres

A recuperação de desastres usa os seguintes componentes para fornecer recuperação de desastres para cargas de trabalho do VMware:

- * NetApp Console*: A interface do usuário para gerenciar seus planos de recuperação de desastres. Você pode usar o NetApp Console para criar e gerenciar planos de replicação, grupos de recursos e operações de failover em seus ambientes locais e na nuvem.
- **Agente de console**: Um componente de software leve que é executado na sua rede hospedada na nuvem ou no seu ambiente VMware local. Ele se comunica com o NetApp Console e gerencia a replicação de dados entre seu ambiente local e o site de recuperação de desastres. O agente do Console é instalado em uma máquina virtual no seu ambiente VMware.

- * Clusters de armazenamento ONTAP *: Os clusters de armazenamento ONTAP são os principais sistemas de armazenamento que hospedam suas cargas de trabalho do VMware. Os clusters de armazenamento ONTAP fornecem a infraestrutura de armazenamento subjacente para seus planos de recuperação de desastres. A recuperação de desastres usa APIs de armazenamento ONTAP para gerenciar clusters de armazenamento ONTAP , como matrizes locais e soluções baseadas em nuvem, como o Amazon FSx for NetApp ONTAP.
- **Servidores vCenter**: O VMware vCenter é o servidor de gerenciamento do seu ambiente VMware. Ele gerencia os hosts ESXi e seus armazenamentos de dados associados. O agente do Console se comunica com o VMware vCenter para gerenciar a replicação de dados entre seu ambiente local e o site de recuperação de desastres. Isso inclui registrar LUNs e volumes ONTAP como armazenamentos de dados, reconfigurar VMs e iniciar e parar VMs.

O fluxo de trabalho de proteção de recuperação de desastres

Quando um plano de replicação é atribuído a um grupo de recursos, o Disaster Recovery executa uma verificação de descoberta de todos os componentes no grupo de recursos e no plano para garantir que o plano possa ser ativado.

Se essa verificação for bem-sucedida, o Disaster Recovery executará as seguintes etapas de inicialização:

1. Para cada VM no grupo de recursos de destino, identifique o armazenamento de dados VMware de hospedagem.
2. Para cada armazenamento de dados VMware encontrado, identifique o FlexVol volume ou LUN do ONTAP FlexVol de hospedagem.
3. Para cada volume ONTAP e LUN encontrado, determine se há um relacionamento SnapMirror existente entre os volumes de origem e um volume de destino no site de destino.
    a. Se não houver um relacionamento SnapMirror preexistente, crie novos volumes de destino e crie um novo relacionamento SnapMirror entre cada volume de origem desprotegido.
    b. Se houver um relacionamento SnapMirror preexistente, use esse relacionamento para executar todas as operações de replicação.

Depois que o Disaster Recovery cria e inicializa todos os relacionamentos, em cada backup agendado, o serviço executa as seguintes etapas de proteção de dados:

1. Para cada VM sinalizada como “consistente com o aplicativo”, use o VMtools para colocar o aplicativo suportado em um estado de backup.
2. Crie um novo snapshot de todos os volumes ONTAP que hospedam datastores VMware protegidos.
3. Execute uma operação de atualização do SnapMirror para replicar esses instantâneos no cluster ONTAP de destino.
4. Determine se o número de instantâneos retidos excedeu a retenção máxima de instantâneos definida no plano de replicação e exclua quaisquer instantâneos estranhos dos volumes de origem e destino.

Destinos de proteção e tipos de armazenamento de dados suportados

Tipos de armazenamento de dados suportados O NetApp Disaster Recovery oferece suporte aos seguintes tipos de armazenamento de dados:

- Armazenamentos de dados NFS hospedados em volumes ONTAP FlexVol que residem em clusters ONTAP .
- Armazenamentos de dados do sistema de arquivos de máquina virtual VMware vSphere (VMFS) usando o

protocolo iSCSI ou FC

Metas de proteção suportadas

- VMware Cloud (VMC) na AWS com Amazon FSx for NetApp ONTAP
- Outro ambiente VMware local baseado em NFS com armazenamento ONTAP ou um FC/iSCSI VMSF local
- Serviço Amazon Elastic VMware
- Azure VMware Solution (AVS) com NetApp Cloud Volumes ONTAP (iSCSI) (visualização privada)
- Google Cloud VMware Engine (GCVE) com Google Cloud NetApp Volumes

Termos que podem ajudar você com a NetApp Disaster Recovery

Você pode se beneficiar ao entender alguma terminologia relacionada à recuperação de desastres.

- **Datastore**: Um contêiner de dados do VMware vCenter, que usa um sistema de arquivos para armazenar arquivos VMDK. Os tipos típicos de armazenamento de dados são NFS, VMFS, vSAN ou vVol. A recuperação de desastres oferece suporte a armazenamentos de dados NFS e VMFS. Cada armazenamento de dados VMware é hospedado em um único volume ONTAP ou LUN. O Disaster Recovery oferece suporte a datastores NFS e VMFS hospedados em volumes FlexVol que residem em clusters ONTAP .
- **Plano de replicação**: Um conjunto de regras sobre a frequência com que os backups ocorrem e como lidar com eventos de failover. Os planos são atribuídos a um ou mais grupos de recursos.
- **Objetivo do ponto de recuperação (RPO)**: A quantidade máxima de perda de dados aceitável em caso de desastre. O RPO é definido na frequência de replicação de dados ou no cronograma de replicação do plano de replicação.
- **Objetivo de tempo de recuperação (RTO)**: O tempo máximo aceitável para se recuperar de um desastre. O RTO é definido no plano de replicação e é o tempo necessário para fazer failover para o site de DR e reiniciar todas as VMs.
- **Grupo de recursos**: um contêiner lógico que permite gerenciar várias VMs como uma única unidade. Uma VM pode estar em apenas um grupo de recursos por vez. Você pode criar um grupo de recursos para cada aplicativo ou carga de trabalho que deseja proteger.
- **Site**: Um contêiner lógico normalmente associado a um datacenter físico ou local na nuvem que hospeda um ou mais clusters do vCenter e armazenamento ONTAP .

Pré-requisitos do NetApp Disaster Recovery

Antes de usar o NetApp Disaster Recovery, certifique-se de que seu ambiente atenda aos requisitos de armazenamento ONTAP , cluster VMware vCenter e NetApp Console .

Versões de software

Componente	Versão mínima
Amazon FSx for NetApp ONTAP	Última versão disponível
Google Cloud VMware Engine usando Google Cloud NetApp Volumes	Última versão disponível

Componente	Versão mínima
Software ONTAP	ONTAP 9.10.0 ou posterior
VMware Cloud para AWS	Última versão disponível
VMware vCenter local	7.0u3 ou posterior

Pré-requisitos e considerações do Google Cloud

Ao utilizar o Disaster Recovery no Google Cloud VMware Engine com o Google Cloud NetApp Volumes, certifique-se de configurar as permissões corretas e seguir as considerações indicadas.

- Entre em contato com a equipe de SRE do Google para adicionar os seguintes itens à lista de permissões:
  - API de sincronização para transferir snapshots do armazenamento local para o Google Cloud NetApp Volumes.
  - O projeto do Google com o mecanismo da VMware para criar, montar e desmontar armazenamentos de dados.
- Você deve"Envie uma solicitação para adicionar seus volumes à lista de permissões para replicação híbrida." .
- Esteja ciente do"Cota e limites do Google Cloud NetApp Volumes" .
- Você só pode adicionar um volume ou armazenamento de dados a um plano de replicação.
- Analise o"limitações" .

Considerações sobre failover

- O failover só é compatível com o snapshot mais recente. Se necessário, você pode criar um novo snapshot durante o failover (ou seja, a opção de snapshot seletivo deve estar desativada).
- Não é possível criar um novo snapshot após um failover.
- Não é possível manter e reconciliar snapshots após um failover.

Considerações sobre planos de contingência

- O failback só é possível com a opção de snapshot seletivo. Não é possível realizar um failback tirando um novo snapshot.
- Se você remover o emparelhamento de cluster entre o armazenamento local e os clusters de armazenamento do Google Cloud NetApp Volumes , será necessário limpar manualmente a entrada de emparelhamento do cluster e da VM de armazenamento no cluster local. Para mais informações, consulte "Excluir um relacionamento de pares do servidor virtual".

Permissões do Google Cloud

A entidade de serviço no Google Cloud deve ter atribuídas as seguintes funções ou permissões equivalentes:

- "Função de Administrador de Computação"
- "Permissões do Google Cloud para o NetApp Console"
- "Administrador de Google Cloud NetApp Volumes"

- "Administrador de serviço do VMware Engine"

Permissões do NetApp Console

O usuário do NetApp Console deve ter as seguintes funções:

- "Administrador do Google Cloud NetApp Volumes"
- "Administrador do SnapCenter"
- "Administrador de failover de recuperação de desastres"

Pré-requisitos de armazenamento ONTAP

Esses pré-requisitos se aplicam ao ONTAP ou ao Amazon FSX para instâncias do NetApp ONTAP .

- Os clusters de origem e destino devem ter um relacionamento de pares.
- O SVM que hospeda os volumes de recuperação de desastres deve existir no cluster de destino.
- O SVM de origem e o SVM de destino devem ter um relacionamento de mesmo nível.
- Se estiver implantando com o Amazon FSx for NetApp ONTAP, o seguinte pré-requisito se aplica:
  - Uma instância do Amazon FSx for NetApp ONTAP para hospedar datastores do VMware DR deve existir na sua VPC. Para começar, veja"a documentação do Amazon FSx para ONTAP" .

Pré-requisitos dos clusters VMware vCenter

Esses pré-requisitos se aplicam aos clusters vCenter locais e ao data center definido por software (SDDC) do VMware Cloud for AWS.

- Análise"Privilégios do vCenter" necessário para NetApp Disaster Recovery.
- Todos os clusters VMware que você deseja que o NetApp Disaster Recovery gerencie usam volumes ONTAP para hospedar quaisquer VMs que você deseja proteger.
- Todos os datastores VMware a serem gerenciados pelo NetApp Disaster Recovery devem usar um dos seguintes protocolos:
  - NFS
  - VMFS usando o protocolo iSCSI ou FC
- VMware vSphere versão 7.0 Atualização 3 (7.0v3) ou posterior
- Se você estiver usando o VMware Cloud SDDC, estes pré-requisitos se aplicam.
  - No VMware Cloud Console, use as funções de serviço de Administrador e Administrador do NSX Cloud. Use também o proprietário da organização para a função Organização. Consulte "Usando o VMware Cloud Foundations com AWS FSx para documentação do NetApp ONTAP" .
  - Vincule o VMware Cloud SDDC ao Amazon FSx for NetApp ONTAP . Consulte "Integração do VMware Cloud on AWS com o Amazon FSx for NetApp ONTAP" .

Pré-requisitos do NetApp Console

Comece a usar o NetApp Console

Se você ainda não o fez, "inscreva-se no NetApp Console e crie uma organização" .

Reúna credenciais para ONTAP e VMware

- As credenciais do Amazon FSx para ONTAP e da AWS devem ser adicionadas ao sistema dentro do projeto do NetApp Console que gerencia o NetApp Disaster Recovery.
- O NetApp Disaster Recovery requer credenciais do vCenter. Você insere as credenciais do vCenter ao adicionar um site no NetApp Disaster Recovery.

  Para obter uma lista de privilégios do vCenter necessários, consulte"Privilégios do vCenter necessários para NetApp Disaster Recovery" . Para obter instruções sobre como adicionar um site, consulte"Adicionar um site" .

Crie o agente do NetApp Console

O agente do Console é um componente de software que permite que o Console se comunique com seus clusters de armazenamento ONTAP e VMware vCenter. É necessário para que a Recuperação de Desastres funcione corretamente. O agente reside em sua rede privada (seja um data center local ou uma VPC na nuvem) e se comunica com suas instâncias de armazenamento ONTAP e quaisquer componentes adicionais de servidor e aplicativo. Para recuperação de desastres, este é o acesso aos seus clusters vCenter gerenciados.

Um agente do Console deve ser configurado no NetApp Console. Quando você usa o agente, ele inclui os recursos apropriados para o serviço de Recuperação de Desastres.

- O NetApp Disaster Recovery funciona apenas com a implantação do agente no modo padrão. Ver "Introdução ao NetApp Console no modo padrão" .
- Certifique-se de que tanto os clusters de origem quanto de destino vCenter usem o mesmo agente do Console.
- Tipo de agente de console necessário:
  - **Recuperação de desastres local para local**: Instale o agente do Console local no site de recuperação de desastres. Usando este método, uma falha no site primário não impede que o serviço reinicie seus recursos virtuais no site de DR. Consulte "Instalar e configurar o agente do Console no local".

    A Recuperação de Desastres também oferece suporte ao uso de vários agentes de console com configurações locais. Nesse cenário, os agentes do Console direcionam as ações para os clusters vCenter e ONTAP , e a origem e o destino teriam cada um seu próprio agente do Console. Recomenda-se o uso de vários agentes do Console para reduzir a latência e melhorar o tempo de recuperação caso um agente do Console ou um site apresente falhas.

  - **No local para AWS**: Instale o agente do Console para AWS na sua VPC da AWS. Consulte "Opções de instalação do agente de console na AWS" .

    Para locais para locais, use o agente do Console local. Para o local na AWS, use o agente do Console da AWS, que tem acesso ao vCenter local de origem e ao vCenter local de destino.

  - O agente de console instalado deve ser capaz de acessar quaisquer instâncias de cluster do VMware vCenter e hosts ESXi gerenciados por esses clusters do vCenter que serão gerenciados pela Recuperação de Desastres.
- Todos os arrays ONTAP a serem gerenciados pelo NetApp Disaster Recovery devem ser adicionados a qualquer sistema dentro do projeto do NetApp Console que será usado para gerenciar o NetApp Disaster Recovery.

Ver "Descubra clusters ONTAP locais" .

- Para obter informações sobre como configurar um proxy inteligente para o NetApp Disaster Recovery, consulte"Configure sua infraestrutura para NetApp Disaster Recovery" .

Pré-requisitos de carga de trabalho

Para garantir que os processos de consistência de aplicativos sejam bem-sucedidos, aplique estes pré-requisitos:

- Certifique-se de que as ferramentas VMware (ou ferramentas Open VM) estejam em execução nas VMs que serão protegidas.
- Para máquinas virtuais Windows que executam o Microsoft SQL Server, o Oracle Database ou ambos, os gravadores VSS dos bancos de dados devem estar habilitados.
- Os bancos de dados Oracle que estão sendo executados em um sistema operacional Linux devem ter a autenticação de usuário do sistema operacional habilitada para a função SYSDBA do banco de dados Oracle.

Mais informações

- Privilégios necessários vCenter
- Pré-requisitos para Amazon EVS com NetApp Disaster Recovery

Início rápido para NetApp Disaster Recovery

Veja aqui uma visão geral das etapas necessárias para começar a usar o NetApp Disaster Recovery. Os links em cada etapa levam você a uma página que fornece mais detalhes.

Revise os pré-requisitos

"Certifique-se de que seu sistema atenda a esses requisitos" .

Configurar o NetApp Disaster Recovery

- "Configurar a infraestrutura para o serviço" .
- "Configurar licenciamento" .

O que vem a seguir?

Depois de configurar o serviço, veja o que você pode fazer em seguida.

- "Adicione seus sites do vCenter ao NetApp Disaster Recovery" .
- "Crie seu primeiro grupo de recursos" .
- "Crie seu primeiro plano de replicação" .
- "Replicar aplicativos para outro site" .

- "Falha na execução de aplicativos para um site remoto" .
- "Fazer failback de aplicativos para o site de origem original" .
- "Gerenciar sites, grupos de recursos e planos de replicação" .
- "Monitorar operações de recuperação de desastres" .

Configure sua infraestrutura para NetApp Disaster Recovery

Para usar o NetApp Disaster Recovery, siga algumas etapas para configurá-lo no Amazon Web Services (AWS) e no NetApp Console.

Análise"pré-requisitos" para garantir que seu sistema esteja pronto.

Você pode usar o NetApp Disaster Recovery nas seguintes infraestruturas:

- DR de nuvem híbrida que replica um datacenter VMware mais ONTAP local para uma infraestrutura de DR da AWS baseada no VMware Cloud on AWS e no Amazon FSx for NetApp ONTAP.
- DR de nuvem privada que replica um VMware mais ONTAP vCenter local para outro VMware mais ONTAP vCenter local.

Nuvem híbrida com VMware Cloud e Amazon FSx for NetApp ONTAP

Este método consiste em uma infraestrutura vCenter de produção local usando datastores hospedados em volumes ONTAP FlexVol usando um protocolo NFS. O site de DR consiste em uma ou mais instâncias do VMware Cloud SDDC usando armazenamentos de dados hospedados em volumes FlexVol fornecidos por uma ou mais instâncias do FSx for ONTAP usando um protocolo NFS.

Os sites de produção e DR são conectados por uma conexão segura compatível com AWS. Os tipos comuns de conexão são VPN segura (privada ou fornecida pela AWS), AWS Direct Connect ou outros métodos de interconexão aprovados.

Para recuperação de desastres envolvendo infraestrutura de nuvem da AWS, você deve usar o agente do Console para AWS. O agente deve ser instalado na mesma VPC que a instância do FSx para ONTAP . Se instâncias adicionais do FSx for ONTAP foram implantadas em outras VPCs, a VPC que hospeda o agente deve ter acesso às outras VPCs.

Zonas de disponibilidade da AWS

A AWS oferece suporte à implantação de soluções em uma ou mais zonas de disponibilidade (AZ) dentro de uma determinada região. O Disaster Recovery usa dois serviços hospedados na AWS: VMware Cloud para AWS e AWS FSx para NetApp ONTAP.

- **VMware Cloud para AWS**: oferece suporte à implantação em um ambiente SDDC de cluster extensível de AZ única ou de AZ dupla. O Disaster Recovery oferece suporte a uma implantação de SDDC de AZ único somente para o Amazon VMware Cloud para AWS.
- **AWS FSx para NetApp ONTAP**: Quando implantado em uma configuração dual-AZ, cada volume pertence a um único sistema FSx. Cada volume pertence a um único sistema FSx. Os dados do volume são espelhados para o segundo sistema FSx. O FSx para sistemas ONTAP pode ser implantado em implantações de AZ simples ou duplas. O Disaster Recovery oferece suporte a FSx de AZ única e múltipla para implantações de FSx para ONTAP .

PRÁTICA RECOMENDADA: Para configuração de site de DR da AWS, a NetApp recomenda usar implantações de AZ única para instâncias VMware Cloud e AWS FSx para ONTAP . Como a AWS está sendo usada para DR, não há vantagem em introduzir várias AZs. Multi-AZs podem aumentar custos e complexidade.

No local para AWS

A AWS fornece os seguintes métodos para conectar datacenters privados à nuvem AWS. Cada solução tem seus benefícios e considerações de custo.

- **AWS Direct Connect**: Esta é uma interconexão de nuvem da AWS localizada na mesma área geográfica do seu datacenter privado e fornecida por um parceiro da AWS. Esta solução fornece uma conexão segura e privada entre seu datacenter local e a nuvem AWS sem a necessidade de uma conexão pública com a internet. Este é o método de conexão mais direto e eficiente oferecido pela AWS.
- **AWS Internet Gateway**: fornece conectividade pública entre recursos de nuvem da AWS e recursos de computação externos. Esse tipo de conexão normalmente é usado para fornecer serviços a clientes externos, como serviços HTTP/HTTPS, onde a segurança não é um requisito. Não há controle de qualidade de serviço, segurança ou garantia de conectividade. Por esse motivo, esse método de conexão não é recomendado para conectar um datacenter de produção à nuvem.
- **AWS Site-Site VPN**: Esta conexão de rede privada virtual pode ser usada para fornecer conexões de acesso seguras junto com um provedor de serviços de Internet público. A VPN criptografa e descriptografa todos os dados que viajam de e para a nuvem AWS. VPNs podem ser baseadas em software ou hardware. Para aplicações empresariais, o provedor de serviços de Internet público (ISP) deve oferecer garantias de qualidade de serviço para assegurar que largura de banda e latência adequadas sejam fornecidas para replicação de DR.

PRÁTICA RECOMENDADA: Para configuração de site de DR da AWS, a NetApp recomenda usar o AWS Direct Connect. Esta solução oferece o mais alto desempenho e segurança para aplicativos corporativos. Caso não esteja disponível, uma conexão ISP pública de alto desempenho juntamente com uma VPN deve ser usada. Certifique-se de que o ISP ofereça níveis de serviço de QoS comerciais para garantir um desempenho de rede adequado.

Interconexões VPC para VPC

A AWS oferece os seguintes tipos de interconexões de VPC para VPC. Cada solução tem seus benefícios e considerações de custo.

- **VPC Peering**: Esta é uma conexão privada entre duas VPCs. É o método de conexão mais direto e eficiente oferecido pela AWS. O peering de VPC pode ser usado para conectar VPCs na mesma região da AWS ou em regiões diferentes.
- **AWS Internet Gateway**: normalmente é usado para fornecer conexões entre recursos do AWS VPC e recursos e endpoints que não são da AWS. Todo o tráfego segue um caminho "em grampo" em que o tráfego da VPC destinado a outra VPC sai da infraestrutura da AWS pelo gateway da Internet e retorna à infraestrutura da AWS pelo mesmo gateway ou por um diferente. Este não é um tipo de conexão VPC adequado para soluções VMware corporativas.
- **AWS Transit Gateway**: Este é um tipo de conexão centralizada baseada em roteador que permite que cada VPC se conecte a um único gateway central, que atua como um hub central para todo o tráfego de VPC para VPC. Isso também pode ser conectado à sua solução VPN para permitir que recursos do datacenter local acessem recursos hospedados no AWS VPC. Esse tipo de conexão normalmente exige um custo adicional para ser implementado.

PRÁTICA RECOMENDADA: Para soluções de DR envolvendo VMware Cloud e um único FSx para ONTAP VPC, a NetApp recomenda que você use a conexão de peer VPC. Se vários FSx para VPCs ONTAP forem

implantados, recomendamos usar um AWS Transit Gateway para reduzir a sobrecarga de gerenciamento de várias conexões de peers de VPC.

Prepare-se para a proteção local para a nuvem usando a AWS

Para configurar o NetApp Disaster Recovery para proteção local para a nuvem usando a AWS, você precisa configurar o seguinte:

- Configurar o AWS FSx para NetApp ONTAP
- Configurar o VMware Cloud no AWS SDDC

Configurar o AWS FSx para NetApp ONTAP

- Crie um sistema de arquivos Amazon FSx for NetApp ONTAP .
  - Provisione e configure o FSx para ONTAP. O Amazon FSx for NetApp ONTAP é um serviço totalmente gerenciado que fornece armazenamento de arquivos altamente confiável, escalável, de alto desempenho e rico em recursos, criado no sistema de arquivos NetApp ONTAP .
  - Siga os passos em "Relatório técnico 4938: Monte o Amazon FSx ONTAP como um armazenamento de dados NFS com o VMware Cloud na AWS" e "Início rápido para Amazon FSx for NetApp ONTAP" Para provisionar e configurar o FSx para ONTAP.
- Adicione o Amazon FSx para ONTAP ao sistema e adicione credenciais da AWS para o FSx para ONTAP.
- Crie ou verifique seu SVM ONTAP de destino no AWS FSx para a instância ONTAP .
- Configure a replicação entre seu cluster ONTAP local de origem e sua instância do FSx for ONTAP no NetApp Console.

Consulte "como configurar um FSx para sistema ONTAP" para etapas detalhadas.

Configurar o VMware Cloud no AWS SDDC

"VMware Cloud na AWS"fornece uma experiência nativa em nuvem para cargas de trabalho baseadas em VMware no ecossistema da AWS. Cada data center definido por software (SDDC) da VMware 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 VMware Cloud na AWS, siga as etapas em "Implantar e configurar o ambiente de virtualização na AWS" . Um conjunto de luzes piloto também pode ser usado para fins de recuperação de desastres.

Nuvem privada

Você pode usar o NetApp Disaster Recovery para proteger VMs VMware hospedadas em um ou mais clusters vCenter replicando datastores de VM para outro cluster vCenter no mesmo datacenter privado ou em um datacenter privado ou colocalizado remoto.

Para situações de local para local, instale o agente do Console em um dos sites físicos.

O Disaster Recovery oferece suporte à replicação de site para site usando Ethernet e TCP/IP. Certifique-se de que haja largura de banda adequada disponível para suportar taxas de alteração de dados nas VMs do site de produção, para que todas as alterações possam ser replicadas no site de DR dentro do período do Objetivo de Ponto de Recuperação (RPO).

Prepare-se para proteção local para local

Certifique-se de que os seguintes requisitos sejam atendidos antes de configurar o NetApp Disaster Recovery para proteção local para local:

- Armazenamento ONTAP
  - Certifique-se de ter credenciais ONTAP .
  - Crie ou verifique seu site de recuperação de desastres.
  - Crie ou verifique seu ONTAP SVM de destino.
  - Certifique-se de que seus SVMs ONTAP de origem e destino estejam pareados.
- Clusters do vCenter
  - Certifique-se de que as VMs que você deseja proteger estejam hospedadas em datastores NFS (usando volumes ONTAP NFS) ou datastores VMFS (usando LUNs iSCSI da NetApp).
  - Análise"Privilégios do vCenter" necessário para NetApp Disaster Recovery.
  - Crie uma conta de usuário de recuperação de desastres (não a conta de administrador padrão do vCenter) e atribua os privilégios do vCenter à conta.

Suporte a proxy inteligente

O agente do NetApp Console oferece suporte ao proxy inteligente. O proxy inteligente é uma maneira leve, segura e eficiente de conectar seu ambiente local ao NetApp Console. Ele fornece uma conexão segura entre seu sistema e o serviço do Console sem exigir uma VPN ou acesso direto à Internet. Essa implementação de proxy otimizada descarrega o tráfego de API dentro da rede local.

Quando um proxy é configurado, o NetApp Disaster Recovery tenta se comunicar diretamente com o VMware ou o ONTAP e usa o proxy configurado se a comunicação direta falhar.

A implementação do proxy de NetApp Disaster Recovery requer comunicação na porta 443 entre o agente do Console e quaisquer servidores vCenter e matrizes ONTAP usando um protocolo HTTPS. O agente NetApp Disaster Recovery dentro do agente do Console se comunica diretamente com o VMware vSphere, o VC ou o ONTAP ao executar qualquer ação.

Para obter mais informações sobre a configuração geral de proxy no NetApp Console, consulte "Configurar o agente do Console para usar um servidor proxy" .

Acesse a NetApp Disaster Recovery

Use o NetApp Console para efetuar login no serviço NetApp Disaster Recovery .

Para fazer login, você pode usar suas credenciais do site de suporte da NetApp ou pode se inscrever para um login na nuvem da NetApp usando seu e-mail e uma senha. "Saiba mais sobre como fazer login" .

Tarefas específicas exigem funções de usuário específicas. "Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

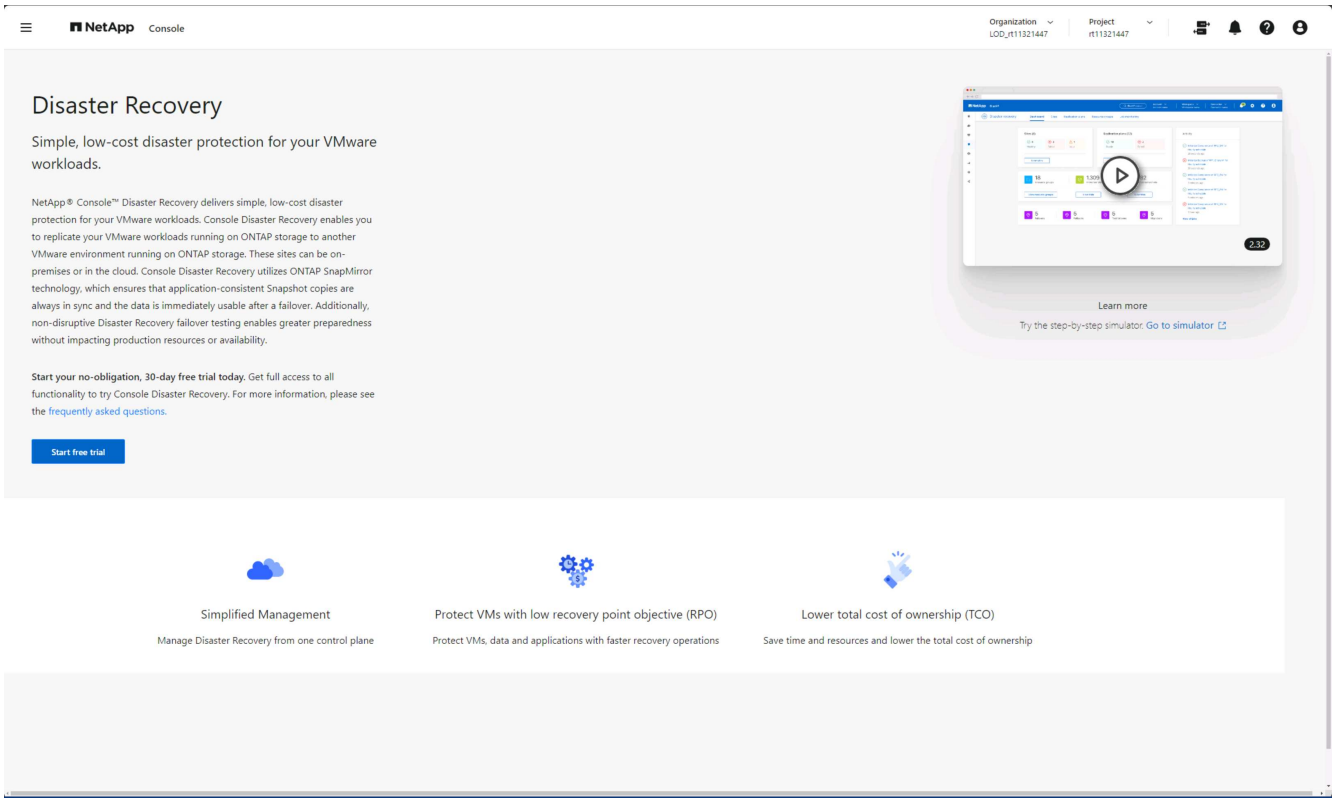
Passos

1. Abra um navegador da web e vá para o "NetApp Console" .

   A página de login do NetApp Console é exibida.

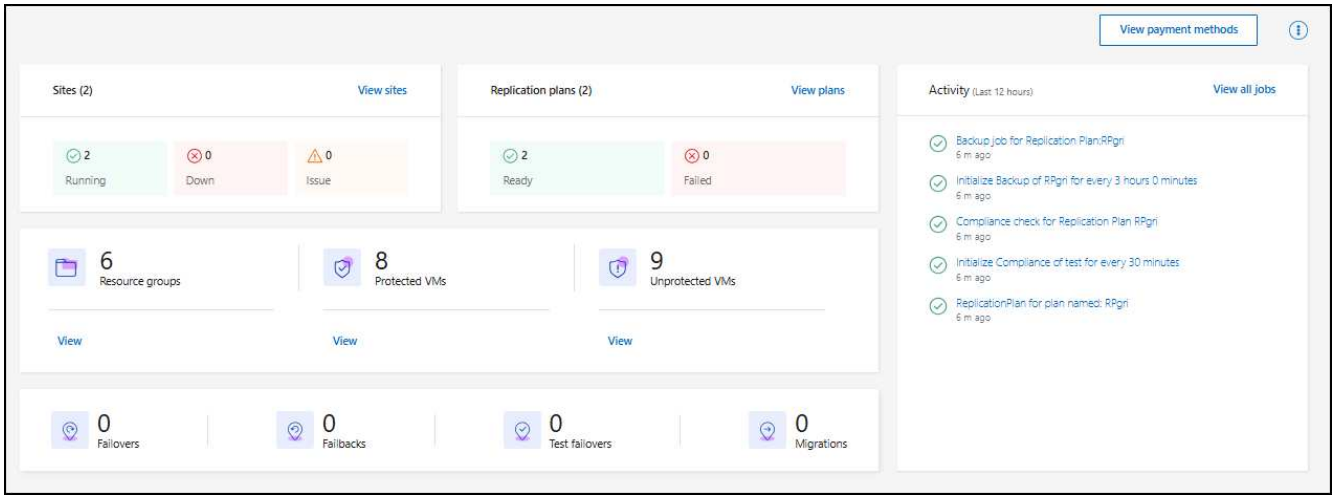
2. Efetue login no NetApp Console.
3. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.

   Se esta for a primeira vez que você faz login neste serviço, a página de destino aparecerá e você poderá se inscrever para um teste gratuito.



Caso contrário, o Painel de NetApp Disaster Recovery será exibido.

- Se você ainda não adicionou um agente do NetApp Console , será necessário adicionar um. Para adicionar o agente, consulte "Saiba mais sobre os agentes do Console" .
- Se você for um usuário do NetApp Console com um agente existente, ao selecionar "Recuperação de desastres", uma mensagem sobre a inscrição será exibida.
- Se você já estiver usando o serviço, ao selecionar "Recuperação de desastres", o Painel será exibido.



Configurar licenciamento para NetApp Disaster Recovery

Com o NetApp Disaster Recovery, você pode usar diferentes planos de licenciamento, incluindo um teste gratuito, uma assinatura paga conforme o uso ou trazer sua própria licença.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre funções de acesso para todos os serviços".

Opções de licenciamento Você pode usar as seguintes opções de licenciamento:

- Inscreva-se para um teste gratuito de 30 dias.
- Compre uma assinatura pré-paga (PAYGO) do Amazon Web Services (AWS) Marketplace ou do Microsoft Azure Marketplace.
- Traga sua própria licença (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém do seu representante de vendas NetApp . Você pode usar o número de série da licença para ativar o BYOL no NetApp Console.

> As cobranças do NetApp Disaster Recovery são baseadas na capacidade usada dos armazenamentos de dados no site de origem quando há pelo menos uma VM com um plano de replicação. A capacidade para um armazenamento de dados com failover não está incluída na capacidade permitida. Para um BYOL, se os dados excederem a capacidade permitida, as operações no serviço serão limitadas até que você obtenha uma licença de capacidade adicional ou atualize a licença no NetApp Console.

"Saiba mais sobre assinaturas".

Após o término do teste gratuito ou a licença expirar, você ainda poderá fazer o seguinte no serviço:

- Visualize qualquer recurso, como uma carga de trabalho ou plano de replicação.
- Exclua qualquer recurso, como uma carga de trabalho ou plano de replicação.
- Execute todas as operações agendadas que foram criadas durante o período de teste ou sob a licença.

Experimente usando um teste gratuito de 30 dias

Você pode experimentar o NetApp Disaster Recovery usando um teste gratuito de 30 dias.

> Não há limites de capacidade impostos durante o julgamento.

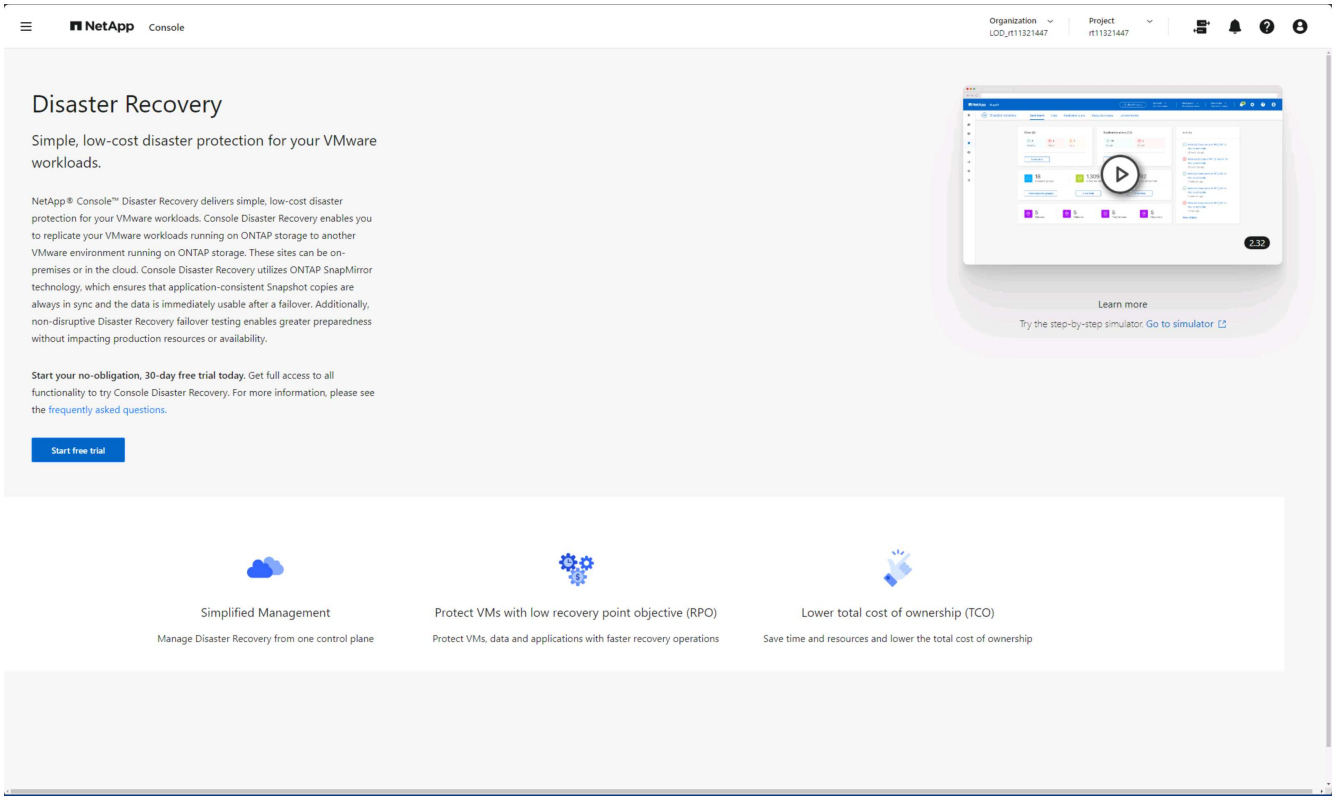
Para continuar após o teste, você precisará comprar uma licença BYOL ou uma assinatura PAYGO AWS. Você pode obter uma licença a qualquer momento e não será cobrado até o término do período de teste.

Durante o teste, você terá funcionalidade total.

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.

Se esta for a primeira vez que você faz login neste serviço, a página de destino será exibida.



3. Se você ainda não adicionou um agente do Console para outros serviços, adicione um.

   Para adicionar um agente de console, consulte "Saiba mais sobre os agentes do Console" .

4. Depois de configurar o agente, na página inicial do NetApp Disaster Recovery , o botão para adicionar o agente muda para um botão para iniciar um teste gratuito. Selecione **Iniciar teste gratuito**.
5. Comece adicionando vCenters.

   Para obter detalhes, consulte "Adicionar sites do vCenter" .

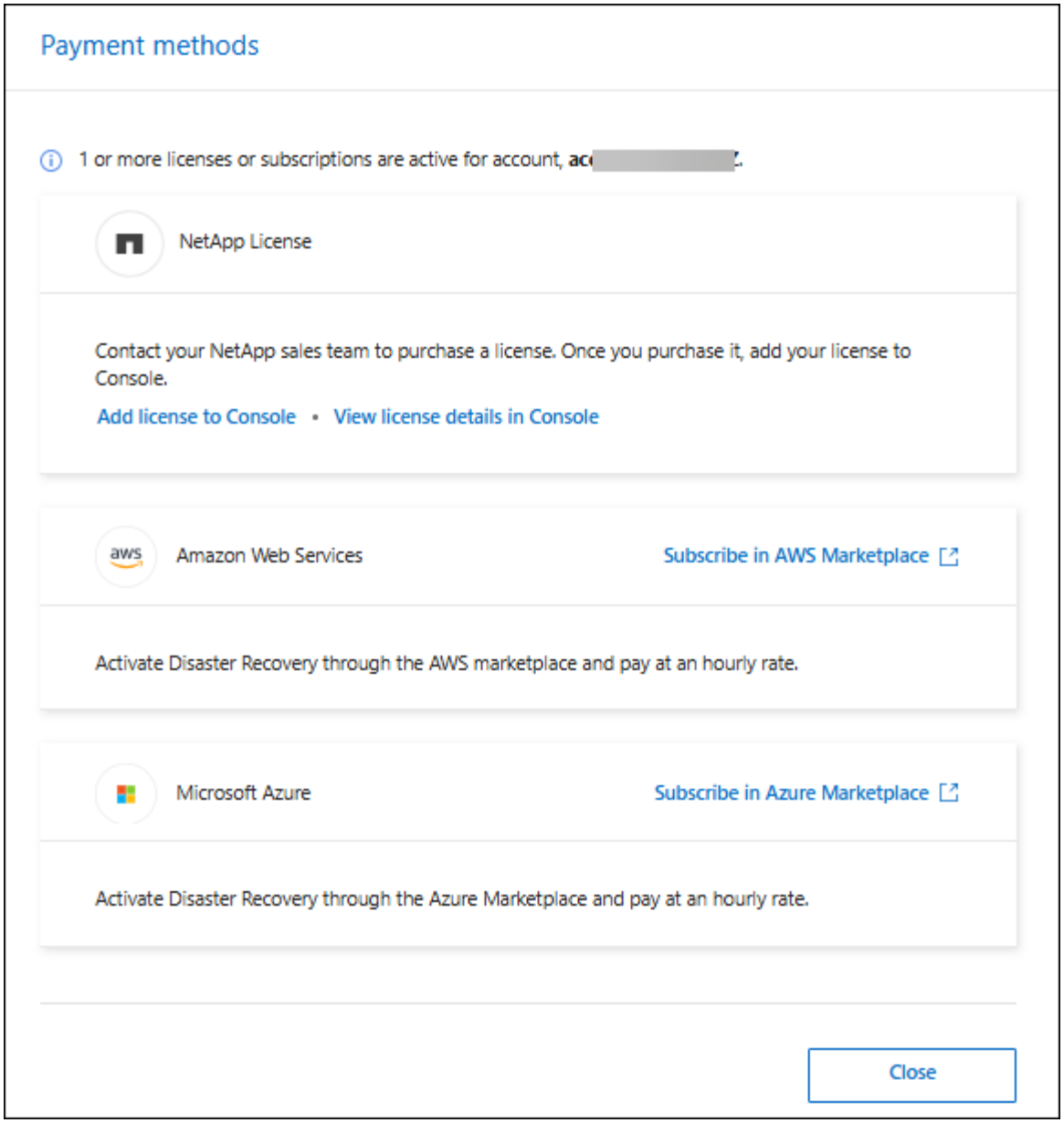
Após o término do teste, assine através de um dos Marketplaces

Após o término do teste gratuito, você pode comprar uma licença da NetApp ou assinar pelo AWS Marketplace ou Microsoft Azure Marketplace. Este procedimento fornece uma visão geral de alto nível de como assinar diretamente em um dos Marketplaces.

Passos

1. No NetApp Disaster Recovery, você vê uma mensagem informando que o teste gratuito está expirando. Na mensagem, selecione **Assinar ou comprar uma licença**.

   Ou, em , selecione **Ver métodos de pagamento**.



2. Selecione **Assinar no AWS Marketplace** ou **Assinar no Azure Marketplace**.
3. Use o AWS Marketplace ou o Microsoft Azure Marketplace para assinar o * NetApp Disaster Recovery*.
4. Quando você retorna ao NetApp Disaster Recovery, uma mensagem informa que você está inscrito.

   Você pode visualizar os detalhes da assinatura na página de assinatura do NetApp Console . "Saiba mais sobre o gerenciamento de assinaturas com o NetApp Console".

Após o término do teste, adquira uma licença BYOL através da NetApp

Após o término do teste, você poderá comprar uma licença por meio do seu representante de vendas da NetApp .

Se você trouxer sua própria licença (BYOL), a configuração inclui a compra da licença, a obtenção do arquivo de licença NetApp (NLF) e a adição da licença ao NetApp Console.

Adicione a licença ao NetApp Console* Depois de comprar sua licença do NetApp Disaster Recovery de um

representante de vendas da NetApp , você pode gerenciá-la no Console.

"Saiba mais sobre como adicionar licenças com o NetApp Console".

Atualize sua licença quando ela expirar

Se o prazo da sua licença estiver próximo da data de expiração ou se a capacidade da sua licença estiver atingindo o limite, você será notificado na interface do usuário do NetApp Disaster Recovery . Você pode atualizar sua licença do NetApp Disaster Recovery antes que ela expire para que não haja interrupção na sua capacidade de acessar seus dados digitalizados.

Esta mensagem também aparece no NetApp Console e em "Notificações" .

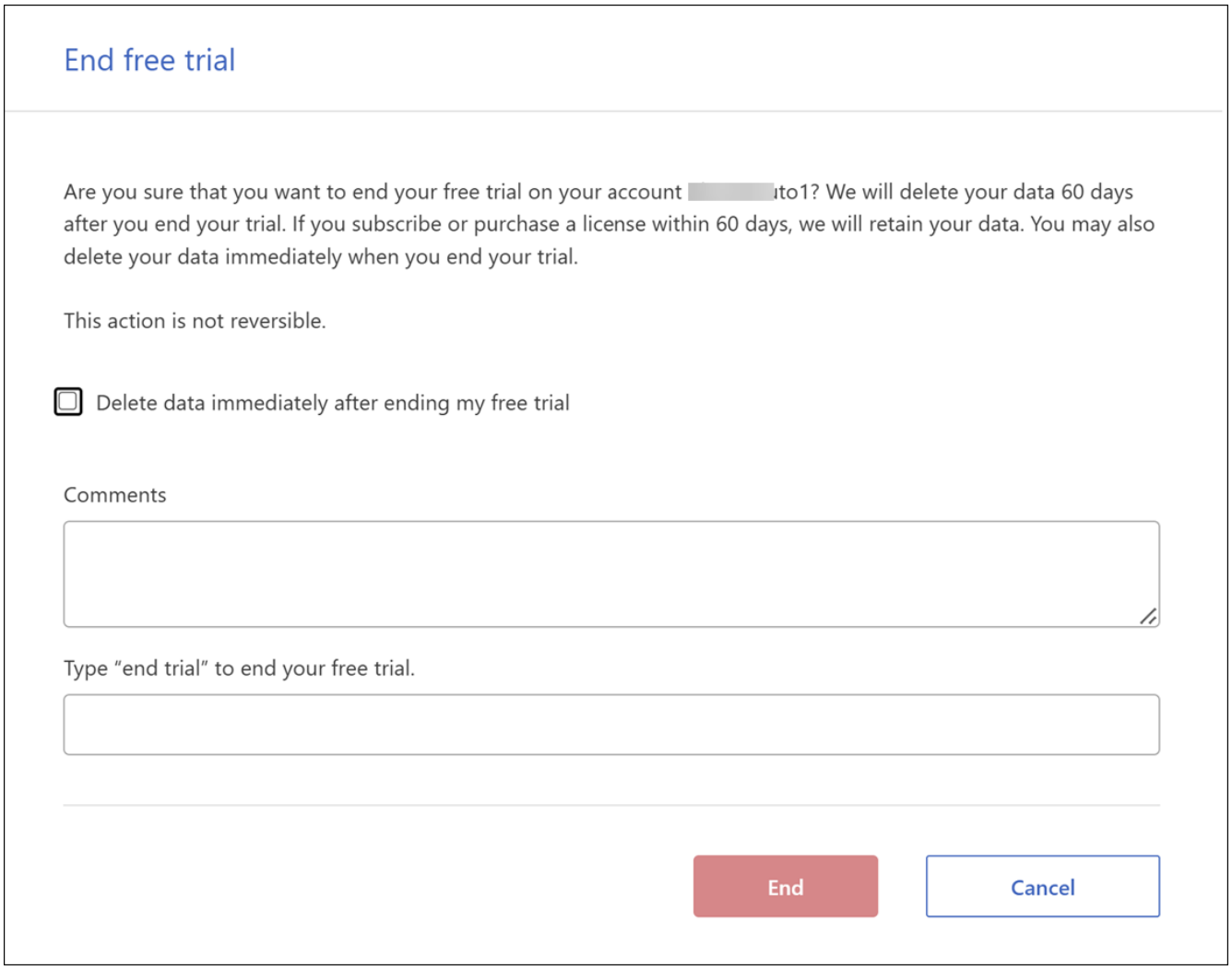
"Saiba mais sobre como atualizar licenças com o NetApp Console".

Encerrar o teste gratuito

Você pode interromper o teste gratuito a qualquer momento ou esperar até que ele expire.

Passos

1. No NetApp Disaster Recovery, selecione **Teste gratuito - Ver detalhes**.
2. Nos detalhes do menu suspenso, selecione **Encerrar teste gratuito**.



3. Se você quiser excluir todos os dados, marque **Excluir dados imediatamente após encerrar meu teste gratuito**.

   Isso exclui todos os agendamentos, planos de replicação, grupos de recursos, vCenters e sites. Dados de auditoria, registros de operação e histórico de trabalhos são mantidos até o fim da vida útil do produto.

   > Se você encerrar o teste gratuito, não solicitar a exclusão de dados e não comprar uma licença ou assinatura, o NetApp Disaster Recovery excluirá todos os seus dados 60 dias após o término do teste gratuito.

4. Digite "encerrar teste" na caixa de texto.
5. Selecione **Fim**.

Use a NetApp Disaster Recovery

Visão geral do uso do NetApp Disaster Recovery

Usando o NetApp Disaster Recovery, você pode atingir os seguintes objetivos:

- "Veja a saúde dos seus planos de recuperação de desastres" .
- "Adicionar sites do vCenter" .
- "Crie grupos de recursos para organizar VMs em conjunto"
- "Crie um plano de recuperação de desastres" .
- "Replicar aplicativos VMware"no seu site principal para um site remoto de recuperação de desastres na nuvem usando a replicação do SnapMirror .
- "Migrar aplicativos VMware"do seu site principal para outro site.
- "Teste o fail over"sem interromper as máquinas virtuais originais.
- Em caso de desastre,"falha no seu site principal" para VMware Cloud na AWS com FSx para NetApp ONTAP.
- Depois que o desastre for resolvido,"falha de retorno" do local de recuperação de desastres para o local principal.
- "Monitorar operações de recuperação de desastres"na página Monitoramento de Tarefas.

Veja a integridade dos seus planos de NetApp Disaster Recovery no painel

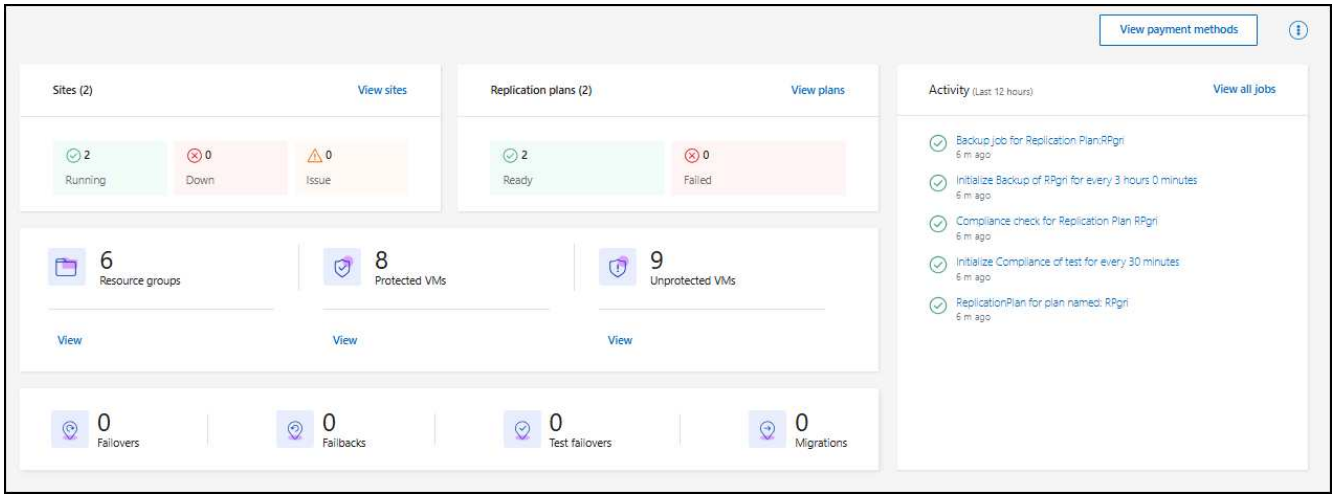
Usando o NetApp Disaster Recovery Dashboard, você pode determinar a integridade dos seus sites de recuperação de desastres e planos de replicação. Você pode verificar rapidamente quais sites e planos estão íntegros, desconectados ou degradados.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de aplicativo de recuperação de desastres ou função de visualizador de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu NetApp Disaster Recovery , selecione **Painel**.



4. Revise as seguintes informações no Painel:
   - **Sites**: veja a saúde dos seus sites. Um site pode ter um dos seguintes status:
     - **Em execução**: O vCenter está conectado, íntegro e em execução.
     - **Inativo**: O vCenter não está acessível ou está com problemas de conectividade.
     - **Problema**: O vCenter não está acessível ou está com problemas de conectividade.

       Para ver detalhes do site, selecione **Ver tudo** para ver um status ou **Ver sites** para ver todos.
   - **Planos de replicação**: visualize a integridade dos seus planos. Um plano pode ter um dos seguintes status:
     - **Preparar**
     - **Fracassado**

       Para revisar os detalhes do plano de replicação, selecione **Exibir tudo** para ver um status ou **Exibir planos de replicação** para ver todos.
   - **Grupos de recursos**: visualize a integridade dos seus grupos de recursos. Um grupo de recursos pode ter um dos seguintes status:
   - **VMs protegidas**: As VMs fazem parte de um grupo de recursos.
   - **VMs desprotegidas**: As VMs não fazem parte de um grupo de recursos.

     Para revisar detalhes, selecione o link **Exibir** abaixo de cada um.
   - O número de failovers, failovers de teste e migrações. Por exemplo, se você criou dois planos e migrou para os destinos, a contagem de migrações aparecerá como "2".
5. Revise todas as operações no painel Atividade. Para visualizar todas as operações no Job Monitor, selecione **Exibir todos os trabalhos**.

Adicionar vCenters a um site no NetApp Disaster Recovery

Antes de criar um plano de recuperação de desastres, você precisa adicionar um servidor vCenter primário a um site e um site de recuperação de desastres do vCenter de destino no NetApp Console.

Certifique-se de que os vCenters de origem e de destino usem o mesmo agente do NetApp Console .

Após a adição dos vCenters, o NetApp Disaster Recovery realiza uma descoberta profunda dos ambientes do vCenter, incluindo clusters do vCenter, hosts ESXi, datastores, área de armazenamento, detalhes da máquina virtual, réplicas do SnapMirror e redes de máquinas virtuais.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto ou administrador de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Sobre esta tarefa

Se você adicionou vCenters em versões anteriores e deseja personalizar o agendamento de descoberta, edite o site do servidor vCenter e defina o agendamento.

O NetApp Disaster Recovery realiza a descoberta uma vez a cada 24 horas. Depois de configurar um site, você pode editar o vCenter para personalizar o cronograma de descoberta que atenda às suas necessidades. Por exemplo, se você tiver um grande número de VMs, poderá definir o agendamento de descoberta para ser executado a cada 23 horas e 59 minutos. Se você tiver um pequeno número de VMs, poderá definir o agendamento de descoberta para ser executado a cada 12 horas. O intervalo mínimo é de 30 minutos e o máximo é de 24 horas.

Primeiro, você deve executar algumas descobertas manuais para obter as informações mais atualizadas sobre seu ambiente. Depois disso, você pode definir a programação para ser executada automaticamente.

Se você tiver vCenters de versões anteriores e quiser alterar quando a descoberta será executada, edite o site do servidor vCenter e defina a programação.

VMs recém-adicionadas ou excluídas são reconhecidas na próxima descoberta agendada ou durante uma descoberta manual imediata.

As VMs podem ser protegidas somente se o plano de replicação estiver em um dos seguintes estados:

- Preparar
- Failback confirmado
- Falha de teste confirmada

Clusters vCenter em um site Cada site contém um ou mais vCenters. Esses vCenters usam um ou mais clusters de armazenamento ONTAP para hospedar armazenamentos de dados NFS ou VMFS.

Um cluster do vCenter pode residir em apenas um site. Você precisa das seguintes informações para adicionar um cluster vCenter a um site:

- O endereço IP de gerenciamento do vCenter ou FQDN
- Credenciais para uma conta do vCenter com os privilégios necessários para executar operações. Ver"privilégios necessários do vCenter" para mais informações.
- Para sites VMware hospedados na nuvem, as chaves de acesso à nuvem necessárias
- Um certificado de segurança para acessar seu vCenter.

O serviço oferece suporte a certificados de segurança autoassinados ou certificados de uma autoridade de certificação central (CA).

Passos

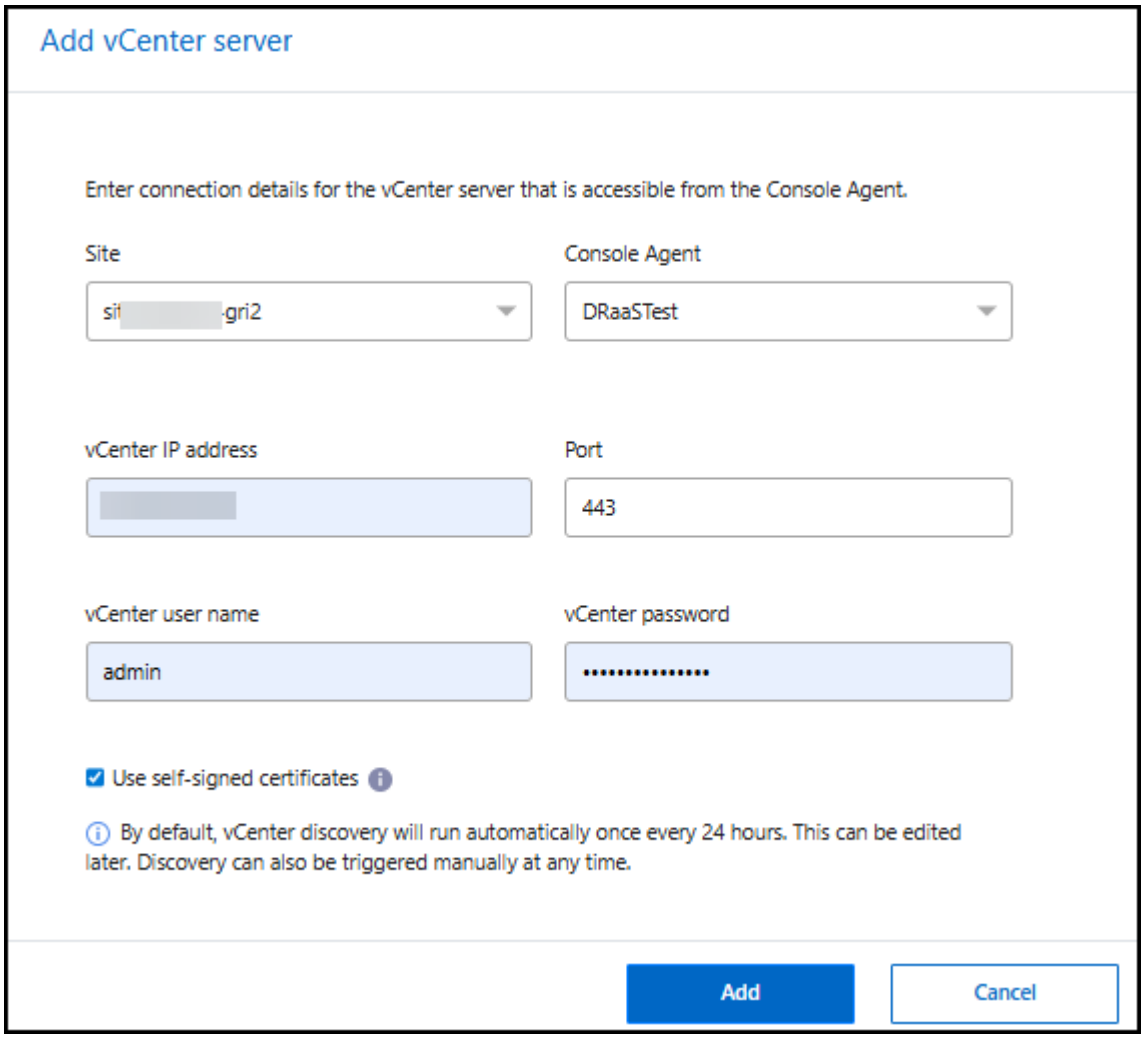
1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.

   Se esta for a sua primeira vez utilizando o NetApp Disaster Recovery, você precisa adicionar as informações do vCenter. Se você já adicionou informações do vCenter, verá o painel de controle.

   Campos diferentes aparecem dependendo do tipo de site que você está adicionando.

3. Se alguns sites do vCenter já existirem e você quiser adicionar mais, no menu, selecione **Sites** e depois selecione **Adicionar**.
4. Na página Sites, selecione o site e selecione **Adicionar vCenter**.
5. **Origem**: Selecione **Descobrir servidores vCenter** para inserir informações sobre o site de origem do vCenter.

   Para adicionar mais sites do vCenter, selecione **Sites** e depois **Adicionar**.



- Selecione um site, depois o agente do NetApp Console e forneça as credenciais do vCenter.
- **Apenas para sites locais:** Para aceitar certificados autoassinados para o vCenter de origem, marque a caixa.

> Certificados autoassinados não são tão seguros quanto outros certificados. Se o seu vCenter **NÃO** estiver configurado com certificados de autoridade de certificação (CA), você deve marcar esta caixa; caso contrário, a conexão com o vCenter não funcionará.

6. Selecione **Adicionar**.

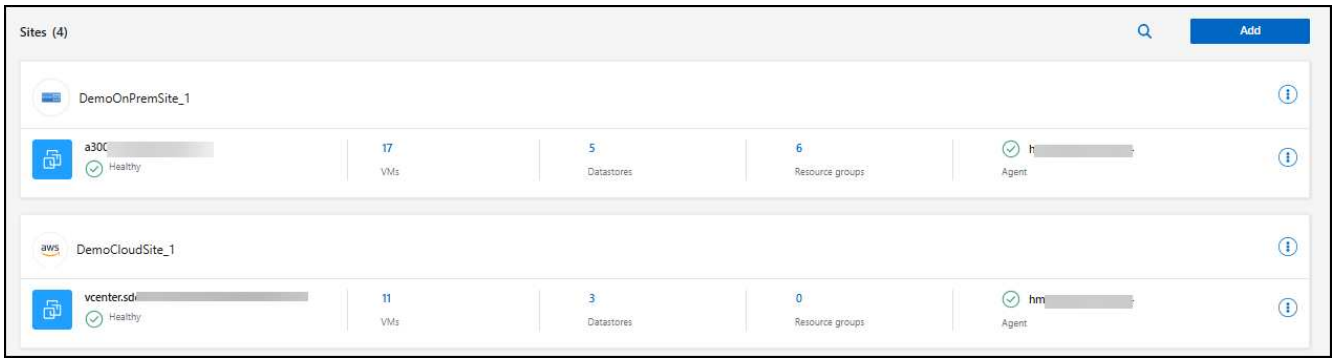
   Em seguida, adicione um vCenter de destino.

7. Adicione um site novamente para o vCenter de destino.
8. Novamente, selecione **Adicionar vCenter** e adicione informações do vCenter de destino.
9. **Alvo**:

   a. Escolha o site de destino e a localização. Se o destino for a nuvem, selecione **AWS**.
      - (Aplica-se somente a sites na nuvem) **Token de API**: insira o token de API para autorizar o acesso ao serviço para sua organização. Crie o token de API fornecendo funções específicas de organização e serviço.
      - (Aplica-se somente a sites na nuvem) **ID da organização longa**: insira o ID exclusivo da organização. Você pode identificar esse ID clicando no nome de usuário na seção Conta do NetApp Console.

   b. Selecione **Adicionar**.

      Os vCenters de origem e de destino aparecem na lista de sites.



10. Para ver o progresso da operação, no menu, selecione **Monitoramento de tarefas**.

Adicionar mapeamento de sub-rede para um site vCenter

Você pode gerenciar endereços IP em operações de failover usando o mapeamento de sub-redes, que permite adicionar sub-redes para cada vCenter. Ao fazer isso, você define o CIDR IPv4, o gateway padrão e o DNS para cada rede virtual.

Após o failover, o NetApp Disaster Recovery usa o CIDR da rede mapeada para atribuir a cada vNIC um novo endereço IP.

Por exemplo:

- RedeA = 10.1.1.0/24
- RedeB = 192.168.1.0/24

A VM1 tem uma vNIC (10.1.1.50) que está conectada à RedeA. A RedeA é mapeada para a RedeB nas configurações do plano de replicação.

No failover, o NetApp Disaster Recovery substitui a parte de rede do endereço IP original (10.1.1) e mantém o endereço de host (.50) do endereço IP original (10.1.1.50). Para VM1, o NetApp Disaster Recovery analisa as configurações CIDR da NetworkB e usa a parte da rede NetworkB 192.168.1, mantendo a parte do host (.50) para criar o novo endereço IP para VM1. O novo IP se torna 192.168.1.50.

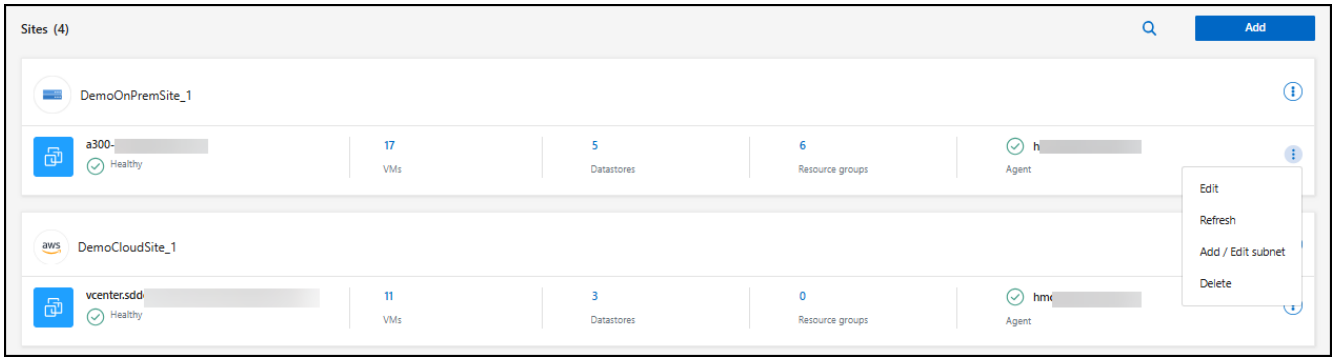
Em resumo, o endereço do host permanece o mesmo, enquanto o endereço de rede é substituído pelo que estiver configurado no mapeamento de sub-rede do site. Isso permite que você gerencie a reatribuição de endereços IP em caso de failover com mais facilidade, especialmente se você tiver centenas de redes e milhares de VMs para gerenciar.

O uso do mapeamento de sub-rede é um processo opcional de duas etapas:

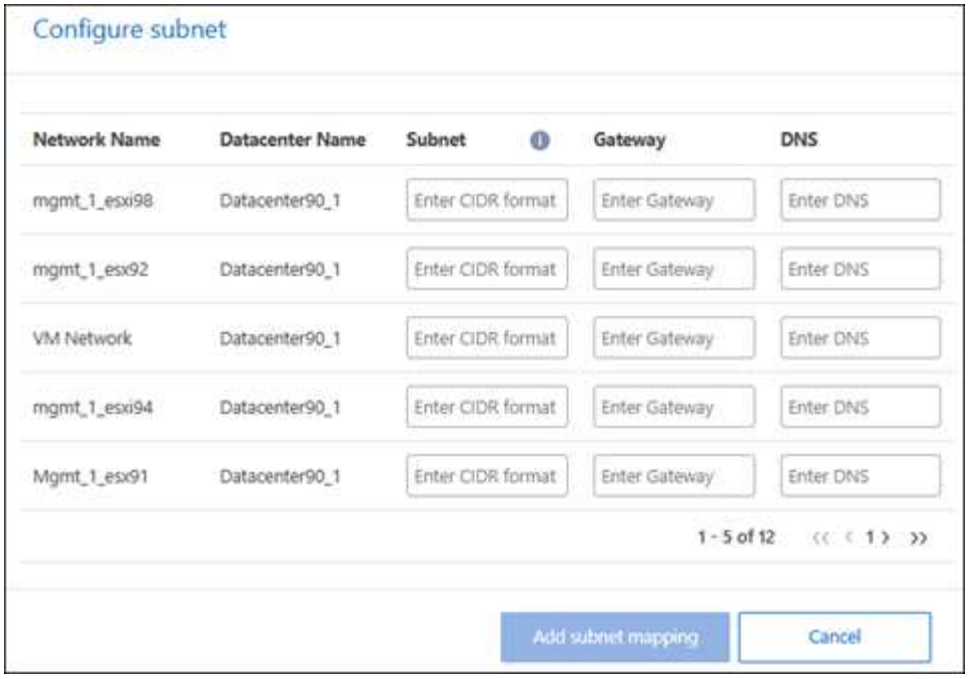
- Primeiro, adicione o mapeamento de sub-rede para cada site do vCenter.
- Em segundo lugar, no plano de replicação, indique que você deseja usar o mapeamento de sub-rede na guia Máquinas Virtuais e no campo IP de Destino.

Passos

1. No menu NetApp Disaster Recovery , selecione **Sites**.
2. Das Ações ícone à direita, selecione **Adicionar sub-rede**.



A página Configurar sub-rede é exibida:



3. Na página Configurar sub-rede, insira as seguintes informações:
   a. Sub-rede: insira o CIDR IPv4 para a sub-rede até /32.

> A notação CIDR é um método de especificação de endereços IP e suas máscaras de rede. /24 denota a máscara de rede. O número consiste em um endereço IP com o número depois da "/" indicando quantos bits do endereço IP denotam a rede. Por exemplo, 192.168.0.50/24, o endereço IP é 192.168.0.50 e o número total de bits no endereço de rede é 24. 192.168.0.50 255.255.255.0 se torna 192.168.0.0/24.

   b. Gateway: insira o gateway padrão para a sub-rede.
   c. DNS: Digite o DNS da sub-rede.
4. Selecione **Adicionar mapeamento de sub-rede**.

Selecione o mapeamento de sub-rede para um plano de replicação

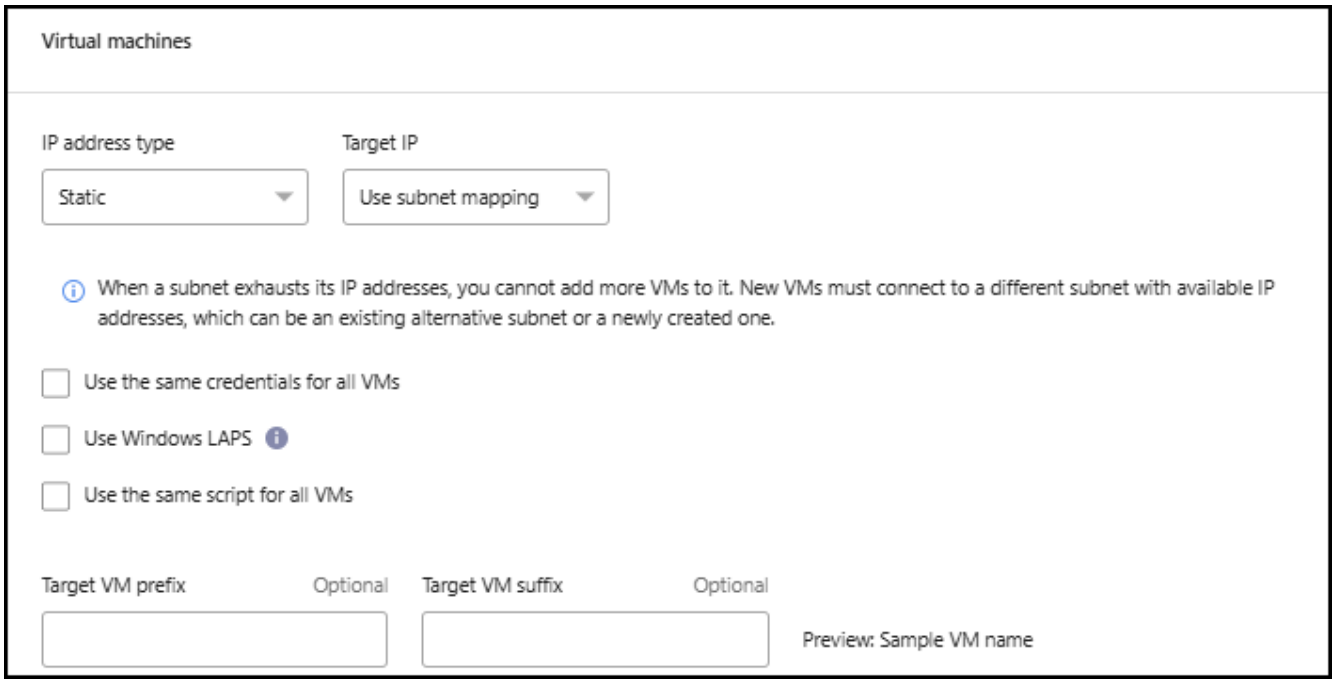
Ao criar um plano de replicação, você pode selecionar o mapeamento de sub-rede para o plano de replicação.

O uso do mapeamento de sub-rede é um processo opcional de duas etapas:

- Primeiro, adicione o mapeamento de sub-rede para cada site do vCenter.
- Em segundo lugar, no plano de replicação, indique que você deseja usar o mapeamento de sub-rede.

Passos

1. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.
2. Selecione **Adicionar** para adicionar um plano de replicação.
3. Preencha os campos da maneira usual, adicionando os servidores vCenter, selecionando os grupos de recursos ou aplicativos e concluindo os mapeamentos.
4. Na página Plano de replicação > Mapeamento de recursos, selecione a seção **Máquinas virtuais**.



5. No campo **IP de destino**, selecione **Usar mapeamento de sub-rede** na lista suspensa.

> Se houver duas VMs (por exemplo, uma é Linux e a outra é Windows), as credenciais serão necessárias apenas para o Windows.

6. Continue criando o plano de replicação.

Edite o site do servidor vCenter e personalize o cronograma de descoberta

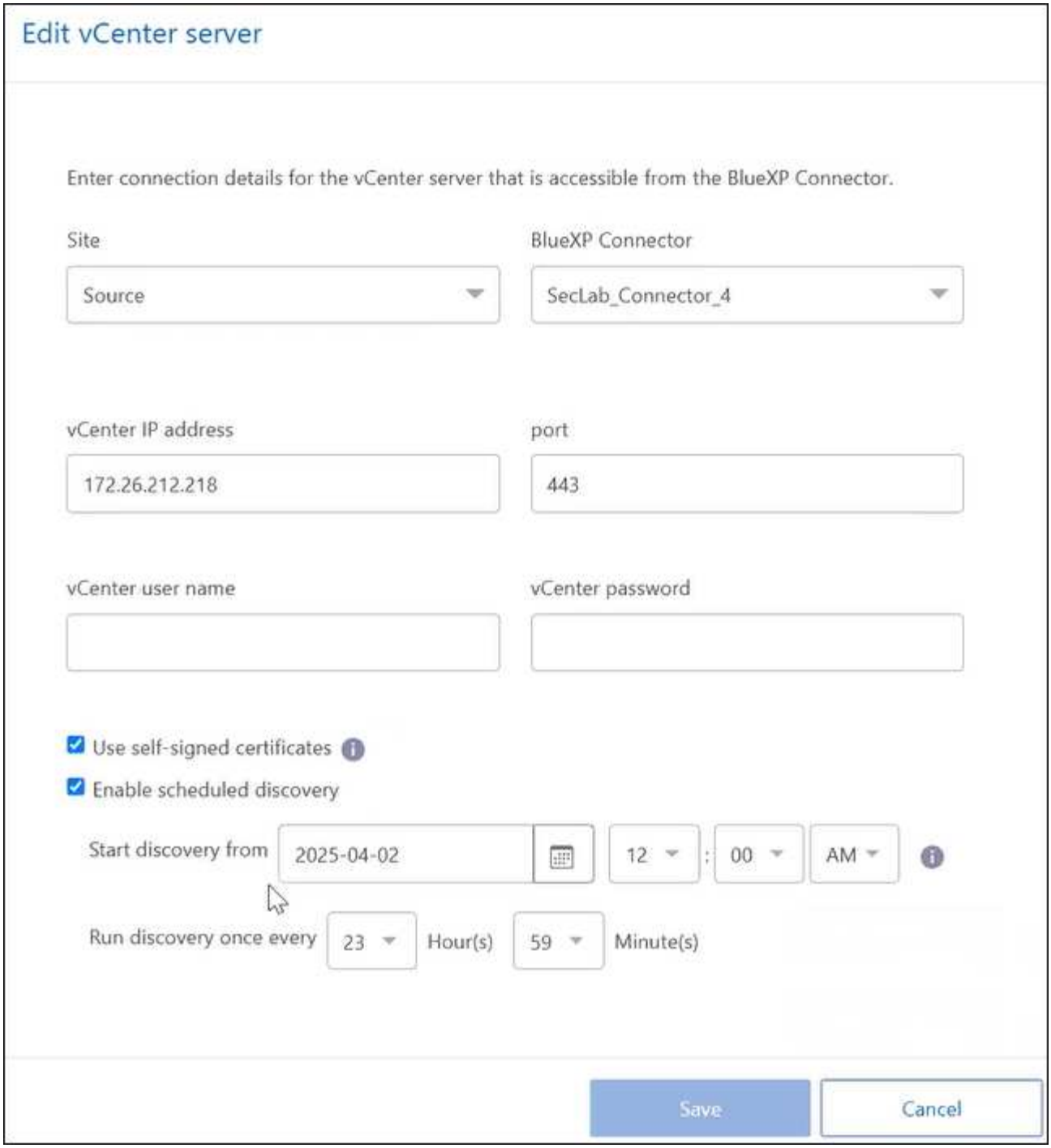
Você pode editar o site do servidor vCenter para personalizar o agendamento de descoberta. Por exemplo, se você tiver um grande número de VMs, poderá definir o agendamento de descoberta para ser executado a cada 23 horas e 59 minutos. Se você tiver um pequeno número de VMs, poderá definir o agendamento de descoberta para ser executado a cada 12 horas.

Se você tiver vCenters de versões anteriores e quiser alterar quando a descoberta será executada, edite o site do servidor vCenter e defina a programação.

Se não quiser agendar a descoberta, você pode desabilitar a opção de descoberta agendada e atualizar a descoberta manualmente a qualquer momento.

Passos

1. No menu NetApp Disaster Recovery , selecione **Sites**.
2. Selecione o site que você deseja editar.
3. Selecione as Ações ícone à direita e selecione **Editar**.
4. Na página Editar servidor vCenter, edite os campos conforme necessário.
5. Para personalizar o agendamento de descoberta, marque a caixa **Ativar descoberta agendada** e selecione o intervalo de data e hora desejado.



6. Selecione **Salvar**.

Atualizar descoberta manualmente

Você pode atualizar a descoberta manualmente a qualquer momento. Isso é útil se você adicionou ou removeu VMs e deseja atualizar as informações no NetApp Disaster Recovery.

Passos

1. No menu NetApp Disaster Recovery , selecione **Sites**.
2. Selecione o site que você deseja atualizar.
3.

Selecione as Ações  ícone à direita e selecione **Atualizar**.

Crie um grupo de recursos para organizar VMs no NetApp Disaster Recovery

Depois de adicionar sites do vCenter, você pode criar grupos de recursos para proteger VMs por VM ou armazenamento de dados como uma única unidade. Grupos de recursos permitem que você organize um conjunto de VMs dependentes em grupos lógicos que atendem aos seus requisitos. Por exemplo, você pode agrupar VMs associadas a um aplicativo ou agrupar aplicativos que tenham níveis semelhantes. Como outro exemplo, grupos podem conter ordens de inicialização atrasadas que podem ser executadas na recuperação.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Sobre esta tarefa

Você pode agrupar VMs em si ou VMs em armazenamentos de dados.

Você pode criar grupos de recursos usando os seguintes métodos:

- Na opção Grupos de recursos
- Enquanto você cria um plano de recuperação de desastres ou *replicação*. Se você tiver muitas VMs hospedadas por um cluster vCenter de origem, pode ser mais fácil criar os grupos de recursos enquanto cria o plano de replicação. Para obter instruções sobre como criar grupos de recursos enquanto você cria um plano de replicação, consulte"Crie um plano de replicação" .

Cada grupo de recursos pode incluir uma ou mais VMs ou armazenamentos de dados. As VMs serão ligadas com base na sequência em que você as incluir no plano de replicação. Você pode alterar a ordem arrastando as VMs ou os armazenamentos de dados para cima ou para baixo na lista de grupos de recursos.

Sobre grupos de recursos

Grupos de recursos permitem que você combine VMs ou armazenamentos de dados como uma única unidade.

Por exemplo, um aplicativo de ponto de venda pode usar várias VMs para bancos de dados, lógica de negócios e vitrines. Você pode gerenciar todas essas VMs com um grupo de recursos. Configure grupos de recursos para aplicar regras de plano de replicação para ordem de inicialização de VM, conexão de rede e recuperação de todas as VMs necessárias para o aplicativo.

Como funciona?

O NetApp Disaster Recovery protege as VMs replicando os volumes ONTAP subjacentes e os LUNs que hospedam as VMs no grupo de recursos. Para fazer isso, o sistema consulta o vCenter para obter o nome de cada armazenamento de dados que hospeda VMs em um grupo de recursos. O NetApp Disaster Recovery identifica então o volume ONTAP de origem ou LUN que hospeda esse armazenamento de dados. Toda a

proteção é executada no nível de volume ONTAP usando a replicação SnapMirror .

Se as VMs no grupo de recursos estiverem hospedadas em diferentes armazenamentos de dados, o NetApp Disaster Recovery usará um dos seguintes métodos para criar um instantâneo consistente de dados dos volumes ONTAP ou LUNs.

Localização relativa dos volumes FlexVol	**Processo de réplica de instantâneo**
Vários armazenamentos de dados - volumes FlexVol no **mesmo SVM**	• Grupo de consistência ONTAP criado • Instantâneos do grupo de consistência tirados • Replicação SnapMirror com escopo de volume realizada
Vários armazenamentos de dados - volumes FlexVol em **vários SVMs**	• API ONTAP : `cg_start` . Silencia todos os volumes para que instantâneos possam ser tirados e inicia instantâneos com escopo de volume de todos os volumes do grupo de recursos. • API ONTAP : `cg_end` . Retoma a E/S em todos os volumes e habilita a replicação do SnapMirror no escopo do volume após os snapshots serem tirados.

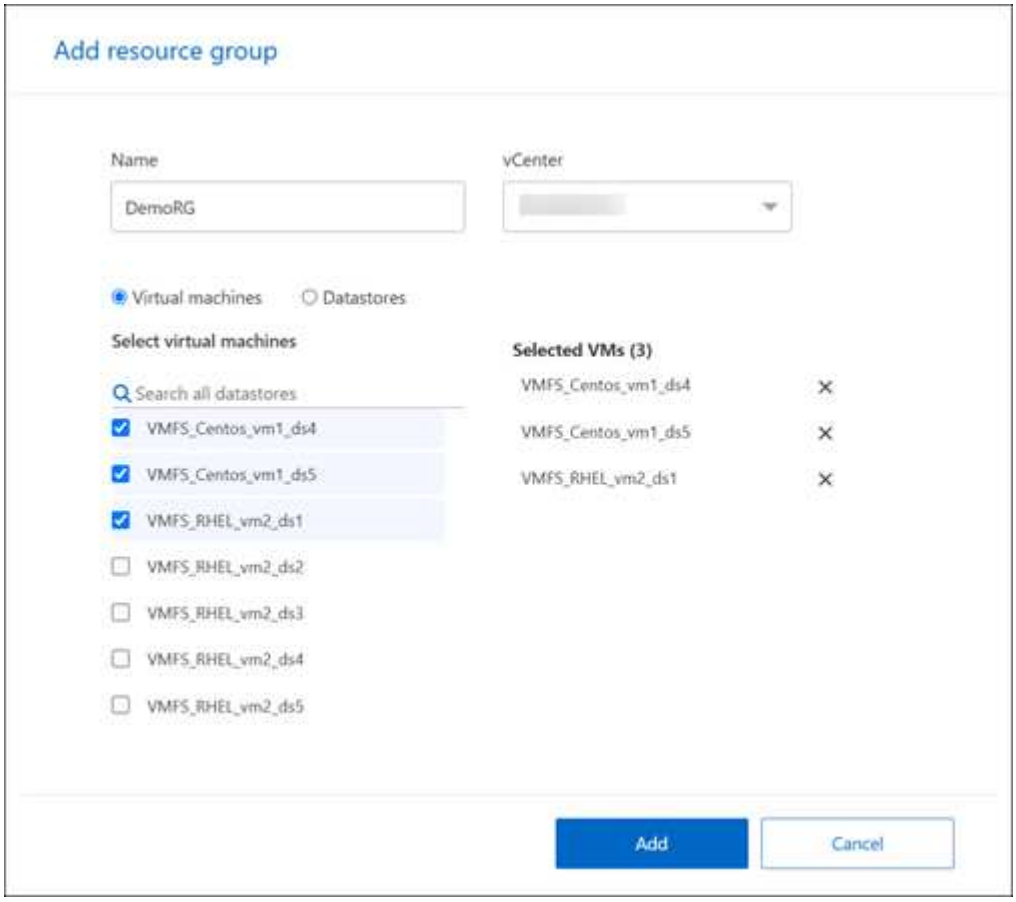
Ao criar grupos de recursos, considere as seguintes questões:

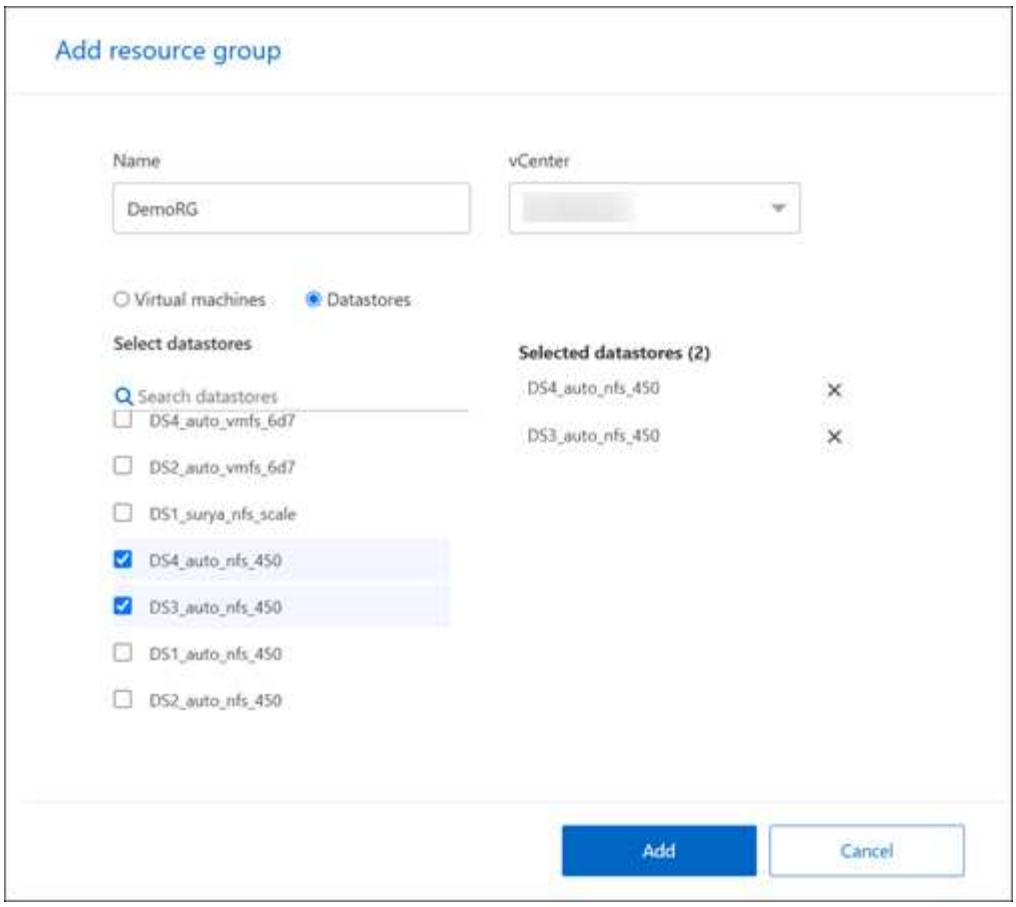
- Antes de adicionar armazenamentos de dados a grupos de recursos, inicie primeiro uma descoberta manual ou uma descoberta agendada das VMs. Isso garante que as VMs sejam descobertas e listadas no grupo de recursos. Se você não iniciar uma descoberta manual, as VMs poderão não ser listadas no grupo de recursos.
- Certifique-se de que haja pelo menos uma VM no armazenamento de dados. Se não houver VMs no armazenamento de dados, a Recuperação de Desastres não descobrirá o armazenamento de dados.
- Um único armazenamento de dados não deve hospedar VMs protegidas por mais de um plano de replicação.
- Não hospede VMs protegidas e desprotegidas no mesmo armazenamento de dados. Se VMs protegidas e desprotegidas estiverem hospedadas no mesmo armazenamento de dados, os seguintes problemas poderão surgir:
  - Como o NetApp Disaster Recovery usa o SnapMirror e o sistema replica volumes ONTAP inteiros, a capacidade usada desse volume é usada para considerações de licenciamento. Nesse caso, o espaço de volume consumido por VMs protegidas e desprotegidas seria incluído neste cálculo.
  - Se o grupo de recursos e seus armazenamentos de dados associados precisarem ser transferidos para o site de recuperação de desastres, quaisquer VMs desprotegidas (VMs que não fazem parte do grupo de recursos, mas hospedadas no volume ONTAP) não existirão mais no site de origem a partir do processo de failover, resultando em falha de VMs desprotegidas no site de origem. Além disso, o NetApp Disaster Recovery não iniciará essas VMs desprotegidas no site do vCenter de failover.
- Para ter uma VM protegida, ela deve ser incluída em um grupo de recursos.

PRÁTICA RECOMENDADA: Organize suas VMs antes de implantar o NetApp Disaster Recovery para minimizar a "dispersão do armazenamento de dados". Coloque as VMs que precisam de proteção em um subconjunto de armazenamentos de dados e coloque as VMs que não serão protegidas em um subconjunto diferente de armazenamentos de dados. Certifique-se de que as VMs em qualquer armazenamento de dados não estejam protegidas por diferentes planos de replicação.

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu NetApp Disaster Recovery , selecione **Grupos de recursos**.
4. Selecione **Adicionar**.
5. Insira um nome para o grupo de recursos.
6. Selecione o cluster vCenter de origem onde as VMs estão localizadas.
7. Selecione **Máquinas virtuais** ou **Armazenamentos de dados** dependendo de como você deseja pesquisar.
8. Selecione a aba **Adicionar grupos de recursos**. O sistema lista todos os armazenamentos de dados ou VMs no cluster vCenter selecionado. Se você selecionou **Datastores**, o sistema listará todos os datastores no cluster vCenter selecionado. Se você selecionou **Máquinas virtuais**, o sistema listará todas as VMs no cluster vCenter selecionado.
9. No lado esquerdo da página Adicionar grupos de recursos, selecione as VMs que você deseja proteger.





10. Opcionalmente, altere a ordem das VMs à direita arrastando cada VM para cima ou para baixo na lista. As VMs serão ligadas com base na sequência em que você as incluir.
11. Selecione **Adicionar**.

Crie um plano de replicação no NetApp Disaster Recovery

Depois de adicionar os sites do vCenter, você estará pronto para criar um plano de recuperação de desastres ou de replicação. Os planos de replicação gerenciam a proteção de dados da infraestrutura VMware. Selecione os vCenters de origem e destino, escolha os grupos de recursos e agrupe como os aplicativos devem ser restaurados e ligados. Por exemplo, você pode agrupar máquinas virtuais (VMs) associadas a um aplicativo ou pode agrupar aplicativos que tenham camadas semelhantes. Esses planos são às vezes chamados de *projetos*.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Sobre esta tarefa

Você pode criar um plano de replicação e também editar cronogramas para conformidade e testes. Execute failovers de teste de VMs sem afetar as cargas de trabalho de produção.

Você pode proteger várias VMs em vários armazenamentos de dados. O NetApp Disaster Recovery cria grupos de consistência ONTAP para todos os volumes ONTAP que hospedam armazenamentos de dados de VM protegidos.

As VMs podem ser protegidas somente se o plano de replicação estiver em um dos seguintes estados:

- Preparar
- Failback confirmado
- Falha de teste confirmada

Instantâneos do plano de replicação

A recuperação de desastres mantém o mesmo número de instantâneos nos clusters de origem e destino. Por padrão, o serviço executa um processo de reconciliação de instantâneos a cada 24 horas para garantir que o número de instantâneos nos clusters de origem e destino seja o mesmo.

As seguintes situações podem fazer com que o número de instantâneos seja diferente entre os clusters de origem e de destino:

- Algumas situações podem fazer com que operações ONTAP fora da Recuperação de Desastres adicionem ou removam instantâneos do volume:
  - Se houver snapshots ausentes no site de origem, os snapshots correspondentes no site de destino poderão ser excluídos, dependendo da política padrão do SnapMirror para o relacionamento.
  - Se houver instantâneos ausentes no site de destino, o serviço poderá excluir os instantâneos correspondentes no site de origem durante o próximo processo de reconciliação de instantâneos agendado, dependendo da política padrão do SnapMirror para o relacionamento.
- Uma redução na contagem de retenção de snapshots do plano de replicação pode fazer com que o serviço exclua os snapshots mais antigos nos sites de origem e de destino para atender ao número de retenção recém-reduzido.

Nesses casos, o Disaster Recovery remove snapshots mais antigos dos clusters de origem e destino na próxima verificação de consistência. Ou o administrador pode executar uma limpeza instantânea imediata selecionando **Ações*** ••• **ícone no plano de replicação e selecionando *Limpar instantâneos**.

O serviço executa verificações de simetria de instantâneos a cada 24 horas.

Antes de começar

- Antes de criar um relacionamento SnapMirror , configure o cluster e o peering SVM fora do Disaster Recovery.
- Com o Google Cloud, você só pode adicionar um volume ou armazenamento de dados a um plano de replicação.

Organize suas máquinas virtuais antes de implantar o NetApp Disaster Recovery para minimizar a "proliferação descontrolada de datastores". Coloque as VMs que precisam de proteção em um subconjunto de armazenamentos de dados e coloque as VMs que não serão protegidas em um subconjunto diferente de armazenamentos de dados. Use proteção baseada em armazenamento de dados para garantir que as VMs em qualquer armazenamento de dados estejam protegidas.

Crie o plano

Um assistente guia você por estas etapas:

- Selecione servidores vCenter.
- Selecione as VMs ou armazenamentos de dados que você deseja replicar e atribua grupos de recursos.
- Mapeie como os recursos do ambiente de origem são mapeados para o destino.
- Defina a frequência com que o plano é executado, execute um script hospedado pelo convidado, defina a ordem de inicialização e selecione o objetivo do ponto de recuperação.
- Revise o plano.

Ao criar o plano, você deve seguir estas diretrizes:

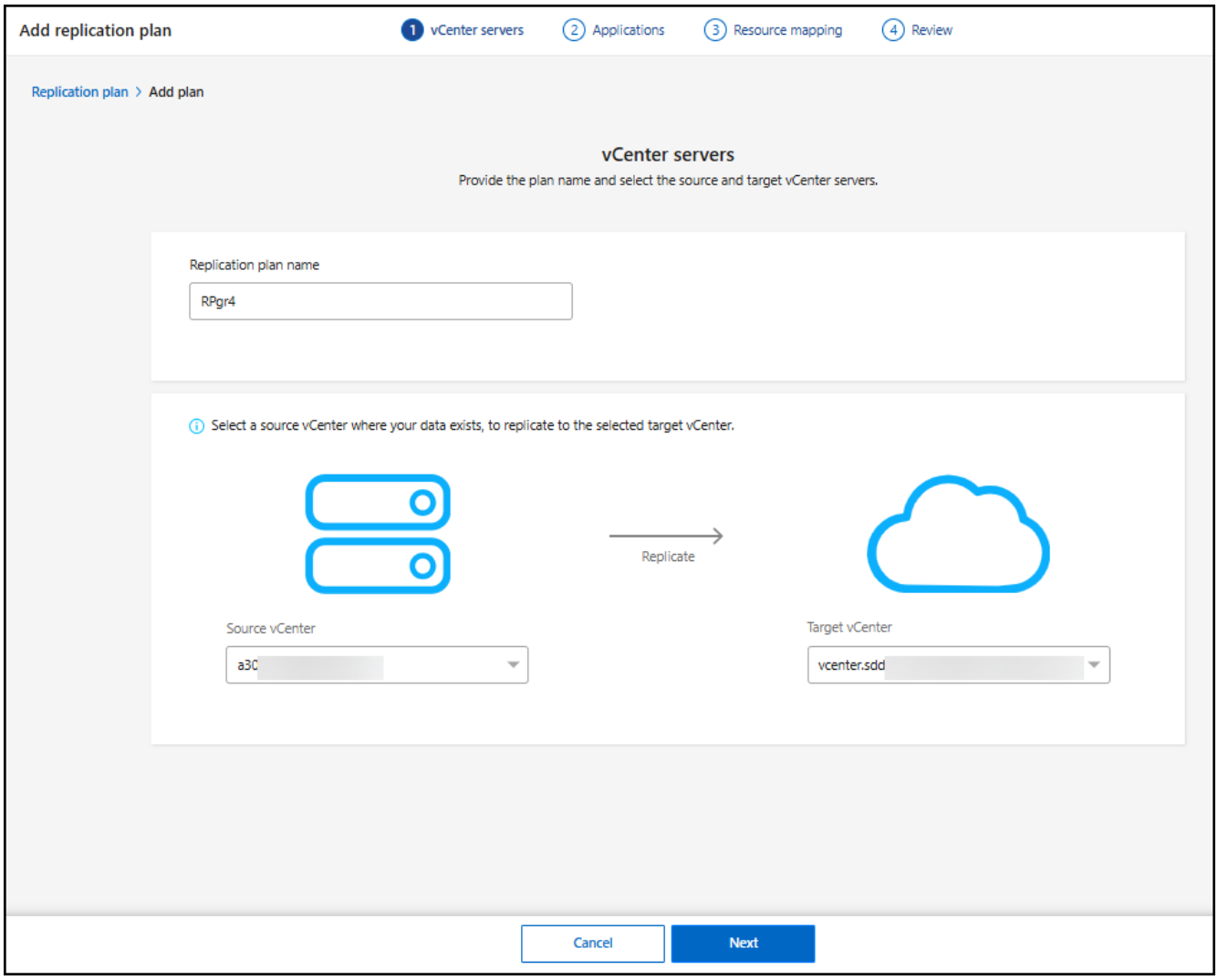
- Use as mesmas credenciais para todas as VMs no plano.
- Use o mesmo script para todas as VMs no plano.
- Use a mesma sub-rede, DNS e gateway para todas as VMs no plano.

Selecione servidores vCenter

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

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu NetApp Disaster Recovery , selecione **Planos de replicação** e selecione **Adicionar**. Ou, se você estiver apenas começando a usar o serviço, no Painel, selecione **Adicionar plano de replicação**.



4. Crie um nome para o plano de replicação.
5. Selecione os vCenters de origem e destino nas listas de vCenters de origem e destino.
6. Selecione **Avançar**.

Selecione aplicativos para replicar e atribuir grupos de recursos

A próxima etapa é agrupar as VMs ou armazenamentos de dados necessários em grupos de recursos funcionais. Grupos de recursos permitem que você proteja um conjunto de VMs ou armazenamentos de dados com um snapshot comum.

Ao selecionar aplicativos no plano de replicação, você pode ver o sistema operacional de cada VM ou armazenamento de dados no plano. Isso é útil para decidir como agrupar VMs ou armazenamentos de dados em um grupo de recursos.

Cada grupo de recursos pode incluir uma ou mais VMs ou armazenamentos de dados.

Ao criar grupos de recursos, considere as seguintes questões:

- Antes de adicionar armazenamentos de dados a grupos de recursos, inicie primeiro uma descoberta manual ou uma descoberta agendada das VMs. Isso garante que as VMs sejam descobertas e listadas no grupo de recursos. Se você não acionar uma descoberta manual, as VMs poderão não ser listadas no

grupo de recursos.

- Certifique-se de que haja pelo menos uma VM no armazenamento de dados. Se não houver VMs no armazenamento de dados, o armazenamento de dados não será descoberto.
- Um único armazenamento de dados não deve hospedar VMs protegidas por mais de um plano de replicação.
- Não hospede VMs protegidas e desprotegidas no mesmo armazenamento de dados. Se VMs protegidas e desprotegidas estiverem hospedadas no mesmo armazenamento de dados, os seguintes problemas poderão surgir:
  - Como o NetApp Disaster Recovery usa o SnapMirror e o sistema replica volumes ONTAP inteiros, a capacidade usada desse volume é usada para considerações de licenciamento. Nesse caso, o espaço de volume consumido por VMs protegidas e desprotegidas seria incluído neste cálculo.
  - Se o grupo de recursos e seus armazenamentos de dados associados precisarem ser transferidos para o site de recuperação de desastres, quaisquer VMs desprotegidas (VMs que não fazem parte do grupo de recursos, mas hospedadas no volume ONTAP) não existirão mais no site de origem a partir do processo de failover, resultando em falha de VMs desprotegidas no site de origem. Além disso, o NetApp Disaster Recovery não iniciará essas VMs desprotegidas no site do vCenter de failover.
- Para ter uma VM protegida, ela deve ser incluída em um grupo de recursos.

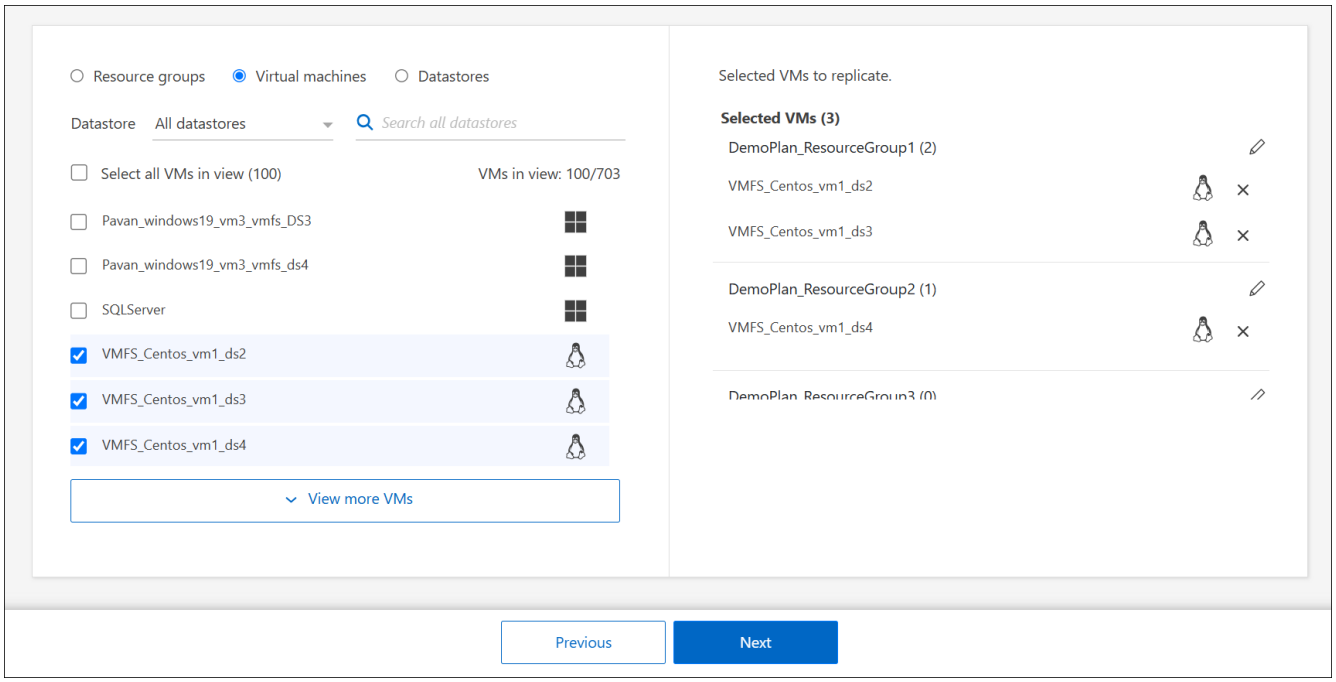
Crie um conjunto separado e dedicado de mapeamentos para seus testes de failover, a fim de evitar que as VMs sejam conectadas a redes de produção usando os mesmos endereços IP.

Passos

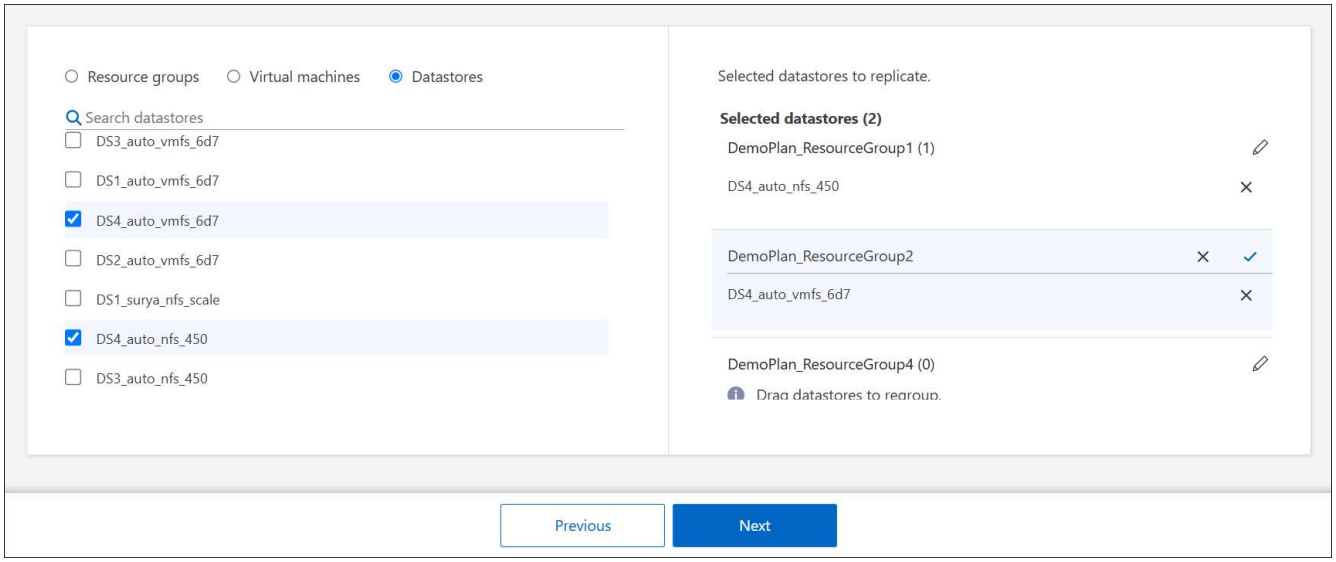
1. Selecione **Máquinas virtuais** ou **Datastores**.
2. Opcionalmente, pesquise por VM ou armazenamento de dados específico pelo nome.
3. No lado esquerdo da página Aplicativos, selecione as VMs ou os armazenamentos de dados que você deseja proteger e atribua ao grupo selecionado.

   O vCenter de origem deve residir no vCenter local. O vCenter de destino pode ser um segundo vCenter local no mesmo site ou em um site remoto, ou ainda um data center definido por software (SDDC) baseado em nuvem, como o VMware Cloud on AWS. Ambos os vCenters já devem ter sido adicionados ao seu ambiente de trabalho de Recuperação de Desastres.

   O recurso selecionado é adicionado automaticamente ao grupo 1 e um novo grupo 2 é iniciado. Cada vez que você adiciona um recurso ao último grupo, outro grupo é adicionado.



Ou, para armazenamentos de dados:



4. Opcionalmente, faça qualquer um dos seguintes:
   - Para alterar o nome do grupo, clique no grupo *Editar* ícone.
   - Para remover um recurso de um grupo, selecione **X** ao lado do recurso.
   - Para mover um recurso para um grupo diferente, arraste e solte-o no novo grupo.

> Para mover um armazenamento de dados para um grupo de recursos diferente, desmarque o armazenamento de dados indesejado e envie o plano de replicação. Em seguida, crie ou edite o outro plano de replicação e selecione novamente o armazenamento de dados.

5. Selecione **Avançar**.

Mapear recursos de origem para o destino

Na etapa Mapeamento de recursos, especifique como os recursos do ambiente de origem devem ser mapeados para o destino. Ao criar um plano de replicação, você pode definir um atraso e uma ordem de inicialização para cada VM no plano. Isso permite que você defina uma sequência para as VMs iniciarem.

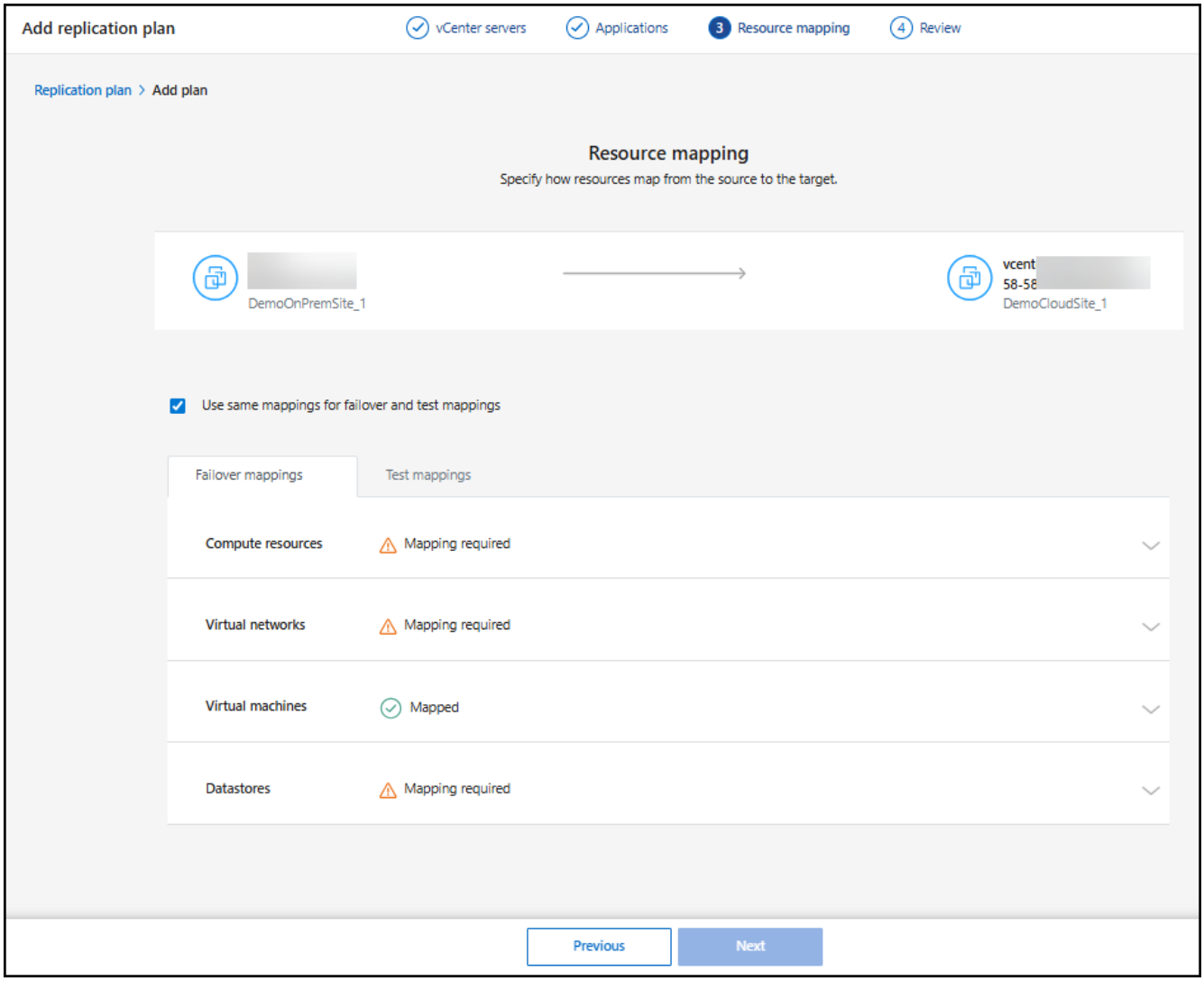
Se você planeja executar failovers de teste como parte do seu plano de DR, forneça um conjunto de mapeamentos de failover de teste para garantir que as VMs iniciadas durante o teste de failover não interfiram nas VMs de produção. Você pode fazer isso fornecendo VMs de teste com endereços IP diferentes ou mapeando as NICs virtuais das VMs de teste para uma rede diferente que esteja isolada da produção, mas que tenha a mesma configuração de IP (chamada de *bolha* ou *rede de teste*).

Antes de começar

Se você quiser criar um relacionamento SnapMirror neste serviço, o cluster e seu peering SVM já deverão ter sido configurados fora do NetApp Disaster Recovery.

Passos

1. Na página de mapeamento de recursos, marque a caixa para usar os mesmos mapeamentos tanto para operações de failover quanto para operações de teste.



2. Na guia Mapeamentos de failover, selecione a seta para baixo à direita de cada recurso e mapeie os recursos em cada seção:

- Recursos de computação
- Redes virtuais
- Máquinas virtuais
- Armazenamentos de dados

Recursos do mapa > Seção Recursos de computação

A seção Recursos de computação define onde as VMs serão restauradas após um failover. Mapeie o data center e o cluster do vCenter de origem para um data center e cluster de destino.

Opcionalmente, as VMs podem ser reiniciadas em um host vCenter ESXi específico. Se o VMWare DRS estiver habilitado, você poderá mover a VM para um host alternativo automaticamente, se necessário, para atender à política de DR configurada.

Opcionalmente, você pode colocar todas as VMs neste plano de replicação em uma pasta exclusiva com o vCenter. Isso fornece uma maneira fácil de organizar rapidamente VMs com failover no vCenter.

Selecione a seta para baixo ao lado de **Recursos de computação**.

- **Datacenters de origem e destino**
- **Grupo alvo**
- **Host de destino** (opcional): Depois de selecionar o cluster, você pode definir essas informações.

Se um vCenter tiver um Distributed Resource Scheduler (DRS) configurado para gerenciar vários hosts em um cluster, você não precisará selecionar um host. Se você selecionar um host, o NetApp Disaster Recovery colocará todas as VMs no host selecionado. * **Pasta da VM de destino** (opcional): Crie uma nova pasta raiz para armazenar as VMs selecionadas.

Recursos do mapa > Seção Redes virtuais

As VMs usam NICs virtuais conectadas a redes virtuais. No processo de failover, o serviço conecta essas NICs virtuais às redes virtuais definidas no ambiente VMware de destino. Para cada rede virtual de origem usada pelas VMs no grupo de recursos, o serviço requer uma atribuição de rede virtual de destino.

Você pode atribuir várias redes virtuais de origem à mesma rede virtual de destino. No entanto, isso pode criar conflitos de configuração de rede IP. Você pode mapear várias redes de origem para uma única rede de destino para garantir que todas as redes de origem tenham a mesma configuração.

Na guia Mapeamentos de failover, selecione a seta para baixo ao lado de **Redes virtuais**. Selecione a LAN virtual de origem e a LAN virtual de destino.

Selecione o mapeamento de rede para a LAN virtual apropriada. As LANs virtuais já devem estar provisionadas, então selecione a LAN virtual apropriada para mapear a VM.

Recursos do mapa > seção de máquinas virtuais

Você pode configurar cada VM no grupo de recursos protegido pelo plano de replicação para se adequar ao ambiente virtual vCenter de destino, definindo qualquer uma das seguintes opções:

- O número de CPUs virtuais

- A quantidade de DRAM virtual
- A configuração do endereço IP
- A capacidade de executar scripts de shell do sistema operacional convidado como parte do processo de failover
- A capacidade de alterar nomes de VMs com failover usando um prefixo e sufixo exclusivos
- A capacidade de definir a ordem de reinicialização durante o failover da VM

Na guia Mapeamentos de failover, selecione a seta para baixo ao lado de **Máquinas virtuais**.

O padrão para as VMs é mapeado. O mapeamento padrão usa as mesmas configurações que as VMs usam no ambiente de produção (mesmo endereço IP, máscara de sub-rede e gateway).

Se você fizer alguma alteração nas configurações padrão, deverá alterar o campo IP de destino para "Diferente da origem".

Se você alterar as configurações para "Diferente da origem", precisará fornecer as credenciais do sistema operacional convidado da VM.

Esta seção pode exibir campos diferentes dependendo da sua seleção.

Você pode aumentar ou diminuir o número de CPUs virtuais atribuídas a cada VM com failover. No entanto, cada VM requer pelo menos uma CPU virtual. Você pode alterar o número de CPUs virtuais e DRAM virtuais atribuídas a cada VM. O motivo mais comum pelo qual você pode querer alterar as configurações padrão da CPU virtual e da DRAM virtual é se os nós do cluster vCenter de destino não tiverem tantos recursos disponíveis quanto o cluster vCenter de origem.

Configurações de rede O Disaster Recovery oferece suporte a um amplo conjunto de opções de configuração para redes de VMs. Pode ser necessário alterá-las se o site de destino tiver redes virtuais que usam configurações TCP/IP diferentes das redes virtuais de produção no site de origem.

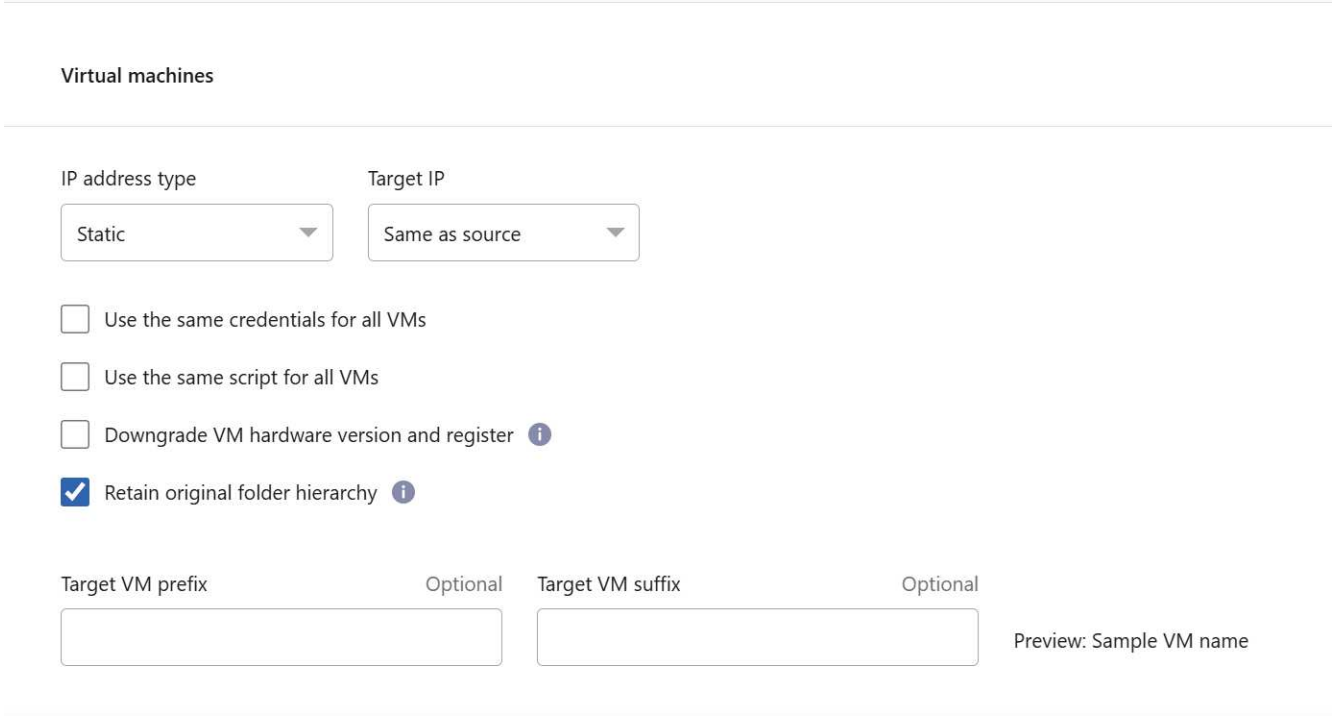
No nível mais básico (e padrão), as configurações simplesmente usam as mesmas configurações de rede TCP/IP para cada VM no site de destino usadas no site de origem. Isso requer que você configure as mesmas configurações de TCP/IP nas redes virtuais de origem e destino.

O serviço oferece suporte a configurações de rede de IP estático ou DHCP (Dynamic Host Configuration Protocol) para VMs. O DHCP fornece um método baseado em padrões para configurar dinamicamente as configurações TCP/IP de uma porta de rede host. O DHCP deve fornecer, no mínimo, um endereço TCP/IP e também pode fornecer um endereço de gateway padrão (para roteamento para uma conexão de internet externa), uma máscara de sub-rede e um endereço de servidor DNS. O DHCP é comumente usado para dispositivos de computação de usuários finais, como desktops, laptops e conexões de celulares de funcionários, mas também pode ser usado para qualquer dispositivo de computação em rede, como servidores.

- Opção **Usar a mesma máscara de sub-rede, DNS e configurações de gateway**: como essas configurações geralmente são as mesmas para todas as VMs conectadas às mesmas redes virtuais, pode ser mais fácil configurá-las uma vez e deixar que o Disaster Recovery use as configurações para todas as VMs no grupo de recursos protegido pelo plano de replicação. Se algumas VMs usarem configurações diferentes, você precisará desmarcar esta caixa e fornecer essas configurações para cada VM.
- **Tipo de endereço IP**: Reconfigure as VMs para corresponder aos requisitos da rede virtual de destino. O NetApp Disaster Recovery oferece duas opções: DHCP ou IP estático. Para IPs estáticos, configure a máscara de sub-rede, o gateway e os servidores DNS. Além disso, insira credenciais para VMs.

- **DHCP**: Selecione esta configuração se quiser que suas VMs obtenham informações de configuração de rede de um servidor DHCP. Se você escolher esta opção, fornecerá apenas as credenciais para a VM.
- **IP estático**: selecione esta configuração se quiser especificar informações de configuração de IP manualmente. Você pode selecionar uma das seguintes opções: igual à origem, diferente da origem ou mapeamento de sub-rede. Se você escolher o mesmo que a fonte, não precisará inserir credenciais. Por outro lado, se você optar por usar informações diferentes da fonte, poderá fornecer as credenciais, o endereço IP da VM, a máscara de sub-rede, o DNS e as informações do gateway. As credenciais do sistema operacional convidado da VM devem ser fornecidas no nível global ou em cada nível de VM.

  Isso pode ser muito útil ao recuperar grandes ambientes para clusters de destino menores ou para conduzir testes de recuperação de desastres sem precisar provisionar uma infraestrutura física VMware individual.



- **Scripts**: Você pode incluir scripts personalizados hospedados no sistema operacional convidado nos formatos .sh, .bat ou .ps1 como pós-processos. Com scripts personalizados, a Recuperação de Desastres pode executar seu script após processos de failover, failback e migração. Por exemplo, você pode usar um script personalizado para retomar todas as transações do banco de dados após a conclusão do failover. O serviço pode executar scripts em máquinas virtuais com Microsoft Windows ou qualquer variante Linux compatível com parâmetros de linha de comando. Você pode atribuir um script a VMs individuais ou a todas as VMs no plano de replicação.

  Para habilitar a execução do script com o sistema operacional convidado da VM, as seguintes condições devem ser atendidas:

  - O VMware Tools deve ser instalado na VM.
  - Credenciais de usuário apropriadas devem ser fornecidas com privilégios adequados do sistema operacional convidado para executar o script.
  - Opcionalmente, inclua um valor de tempo limite em segundos para o script.

VMs executando Microsoft Windows: podem executar scripts em lote do Windows (.bat) ou do PowerShell (ps1). Os scripts do Windows podem usar argumentos de linha de comando. Formate cada argumento no `arg_name$value` formato, onde `arg_name` é o nome do argumento e `$value` é o valor do argumento e um ponto e vírgula separa cada `argument$value` par.

VMs executando Linux: podem executar qualquer script de shell (.sh) suportado pela versão do Linux usada pela VM. Os scripts do Linux podem usar argumentos de linha de comando. Forneça argumentos em uma lista de valores separados por ponto e vírgula. Argumentos nomeados não são suportados. Adicione cada argumento ao `Arg[x]` lista de argumentos e faz referência a cada valor usando um ponteiro para `Arg[x]` matriz, por exemplo, `value1;value2;value3` .

- **Reduzir a versão do hardware da VM e registrá-la**: Selecione esta opção se a versão do host ESX de destino for anterior à de origem, para que correspondam durante o registro.
- **Manter a hierarquia de pastas original**: Por padrão, a Recuperação de Desastres mantém a hierarquia de inventário da VM (estrutura de pastas) em caso de failover. Se o destino da recuperação *não* tiver a hierarquia de pastas original, a Recuperação de Desastres a criará.

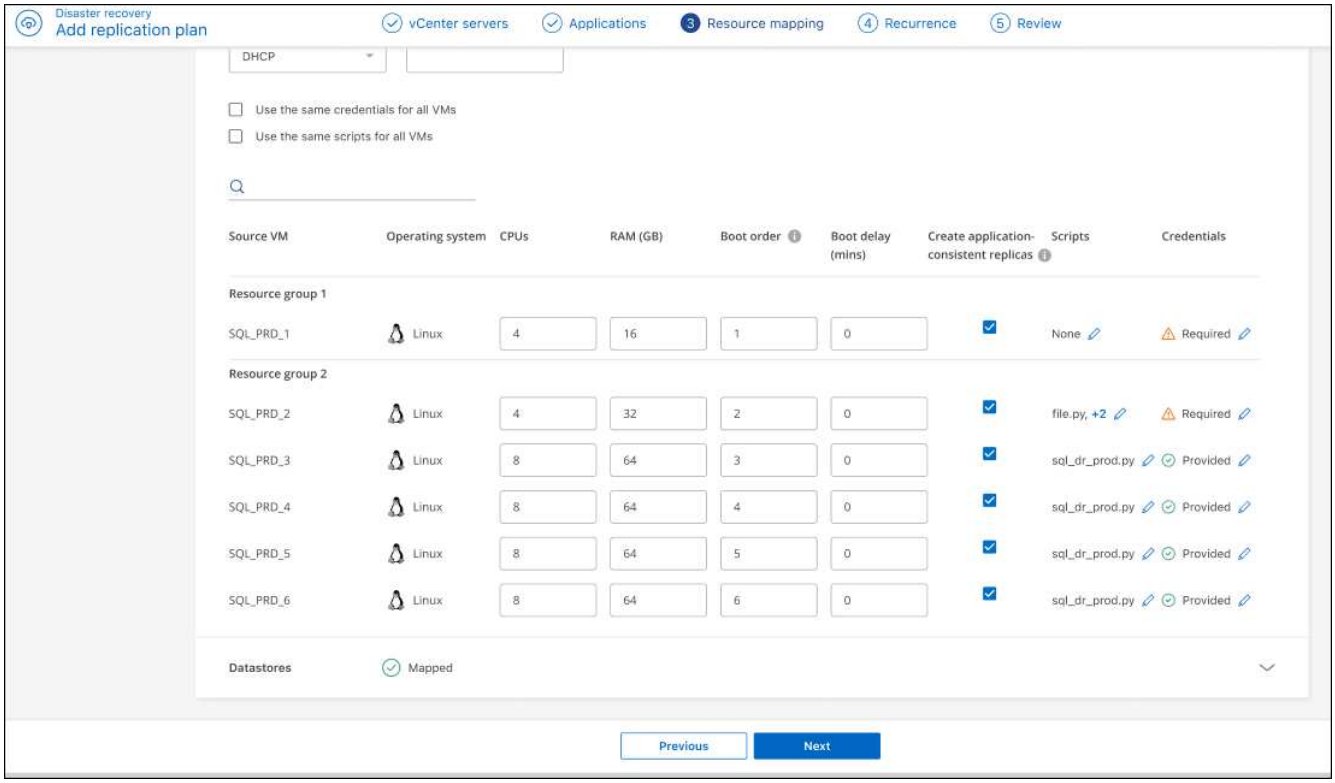
  Desmarque esta caixa para ignorar a hierarquia de pastas original.

- **Prefixo e sufixo da VM de destino**: nos detalhes das máquinas virtuais, você pode, opcionalmente, adicionar um prefixo e um sufixo a cada nome de VM com failover. Isso pode ser útil para diferenciar as VMs com failover das VMs de produção em execução no mesmo cluster do vCenter. Por exemplo, você pode adicionar um prefixo "DR-" e um sufixo "-failover" ao nome da VM. Algumas pessoas adicionam um segundo vCenter de produção para hospedar VMs temporariamente em um site diferente no caso de um desastre. Adicionar um prefixo ou sufixo pode ajudar você a identificar rapidamente VMs com failover. Você também pode usar o prefixo ou sufixo em scripts personalizados.

  Você pode usar o método alternativo de definir a pasta da VM de destino na seção Recursos de computação.

- **CPU e RAM da VM de origem**: Nos detalhes das máquinas virtuais, você pode redimensionar opcionalmente os parâmetros de CPU e RAM da VM.

  Você pode configurar a DRAM em gigabytes (GiB) ou megabytes (MiB). Embora cada VM exija pelo menos um MiB de RAM, a quantidade real deve garantir que o sistema operacional convidado da VM e quaisquer aplicativos em execução possam operar com eficiência.



- **Ordem de inicialização**: Você pode modificar a ordem de inicialização após um failover para todas as máquinas virtuais selecionadas nos grupos de recursos. Por padrão, todas as VMs inicializam juntas em paralelo; no entanto, você pode fazer alterações nesta fase. Isso é útil para garantir que todas as suas VMs de prioridade um estejam em execução antes que as VMs de prioridade subsequentes sejam iniciadas.

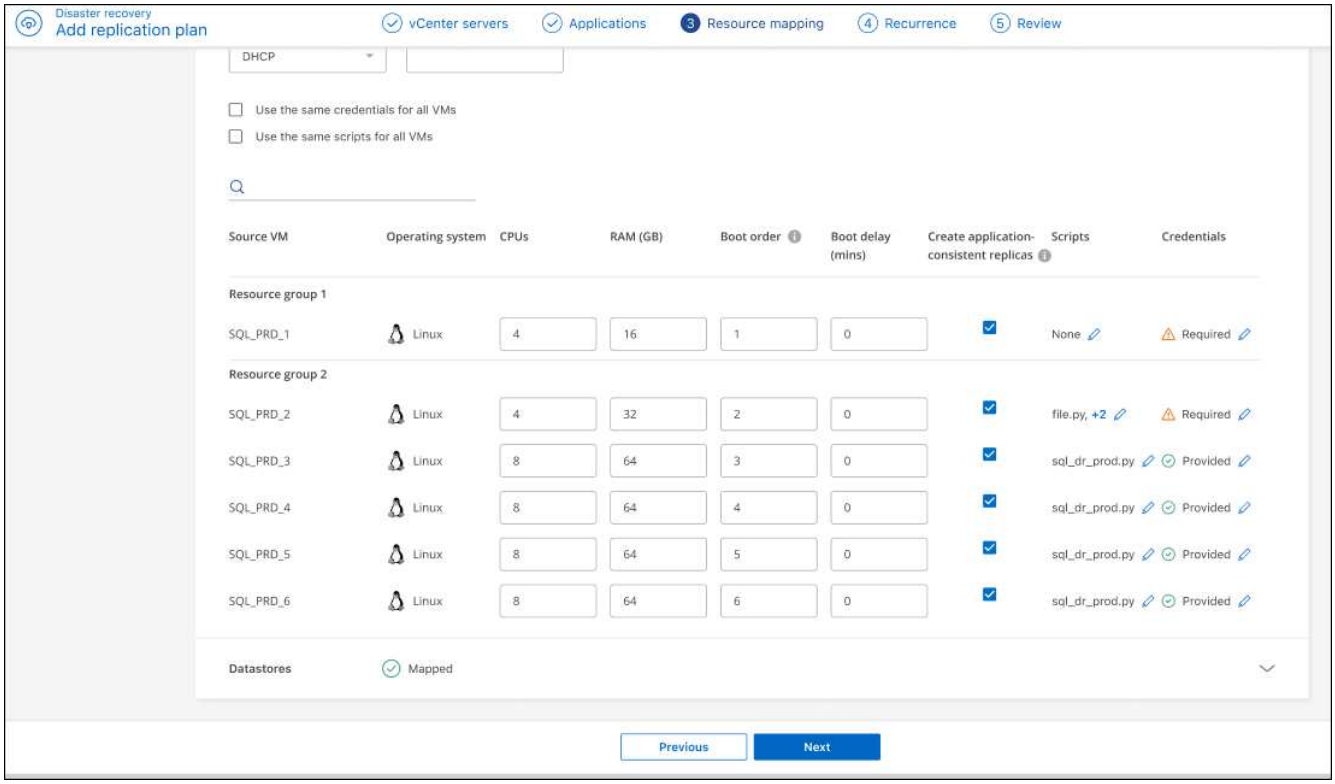
  A Recuperação de Desastres inicializa em paralelo quaisquer máquinas virtuais com o mesmo número de ordem de inicialização.

  - Inicialização sequencial: atribua a cada VM um número exclusivo para inicializar na ordem atribuída, por exemplo, 1,2,3,4,5.
  - Inicialização simultânea: atribua o mesmo número a todas as VMs para inicializá-las ao mesmo tempo, por exemplo, 1,1,1,1,2,2,3,4,4.
- **Atraso na inicialização**: ajuste o atraso em minutos da ação de inicialização, indicando a quantidade de tempo que a VM aguardará antes de iniciar o processo de inicialização. Insira um valor de 0 a 10 minutos.

> Para redefinir a ordem de inicialização para o padrão, selecione **Redefinir configurações da VM para o padrão** e escolha quais configurações você deseja alterar de volta para o padrão.

- **Criar réplicas consistentes com o aplicativo**: indique se deseja criar cópias de snapshot consistentes com o aplicativo. O serviço desativará o aplicativo e, em seguida, tirará um instantâneo para obter um estado consistente do aplicativo. Este recurso é compatível com Oracle em execução no Windows e Linux e SQL Server em execução no Windows. Veja mais detalhes a seguir.
- **Usar Windows LAPS**: Se você estiver usando a Solução de Senha de Administrador Local do Windows (Windows LAPS), marque esta caixa. Esta opção só estará disponível se você tiver selecionado a opção **IP estático**. Ao marcar esta caixa, você não precisa fornecer uma senha para cada uma de suas máquinas virtuais. Em vez disso, você fornece os detalhes do controlador de domínio.

Se você não usar o Windows LAPS, a VM será uma VM do Windows e a opção de credenciais na linha VM estará habilitada. Você pode fornecer as credenciais para a VM.



Crie réplicas consistentes com o aplicativo

Muitas VMs hospedam servidores de banco de dados como Oracle ou Microsoft SQL Server. Esses servidores de banco de dados exigem instantâneos consistentes com o aplicativo para garantir que o banco de dados esteja em um estado consistente quando o instantâneo for tirado.

Snapshots consistentes com o aplicativo garantem que o banco de dados esteja em um estado consistente quando o snapshot é tirado. Isso é importante porque garante que o banco de dados possa ser restaurado para um estado consistente após uma operação de failover ou failback.

Os dados gerenciados pelo servidor de banco de dados podem ser hospedados no mesmo armazenamento de dados que a VM que hospeda o servidor de banco de dados ou podem ser hospedados em um armazenamento de dados diferente. A tabela a seguir mostra as configurações suportadas para snapshots consistentes com o aplicativo na Recuperação de Desastres:

Localização dos dados	Suportado	Notas
No mesmo armazenamento de dados do vCenter que a VM	Sim	Como o servidor de banco de dados e o banco de dados residem no mesmo armazenamento de dados, tanto o servidor quanto os dados estarão sincronizados no failover.

Localização dos dados	Suportado	Notas
Dentro de um armazenamento de dados vCenter diferente da VM	Não	O Disaster Recovery não consegue identificar quando os dados de um servidor de banco de dados estão em um armazenamento de dados diferente do vCenter. O serviço não pode replicar os dados, mas pode replicar a VM do servidor de banco de dados. Embora os dados do banco de dados não possam ser replicados, o serviço garante que o servidor de banco de dados execute todas as etapas necessárias para garantir que o banco de dados esteja inativo no momento do backup da VM.
Dentro de uma fonte de dados externa	Não	Se os dados residirem em um LUN montado no convidado ou em um compartilhamento NFS, o Disaster Recovery não poderá replicar os dados, mas poderá replicar a VM do servidor de banco de dados. Embora os dados do banco de dados não possam ser replicados, o serviço garante que o servidor de banco de dados execute todas as etapas necessárias para garantir que o banco de dados esteja inativo no momento do backup da VM.

Durante um backup agendado, o Disaster Recovery desativa o servidor de banco de dados e, em seguida, tira um instantâneo da VM que hospeda o servidor de banco de dados. Isso garante que o banco de dados esteja em um estado consistente quando o instantâneo for tirado.

- Para VMs do Windows, o serviço usa o Microsoft Volume Shadow Copy Service (VSS) para coordenar com qualquer servidor de banco de dados.
- Para VMs Linux, o serviço usa um conjunto de scripts para colocar o servidor Oracle no modo de backup.

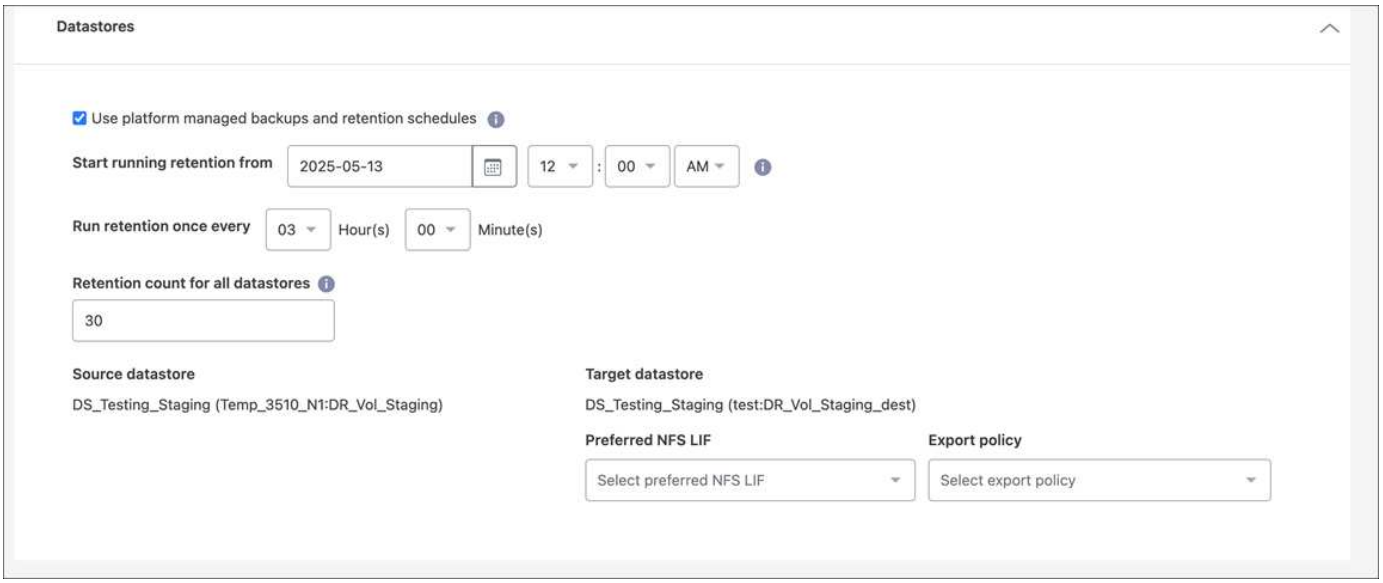
Para habilitar réplicas consistentes com o aplicativo das VMs e seus armazenamentos de dados de hospedagem, marque a caixa ao lado de **Criar réplicas consistentes com o aplicativo** para cada VM e forneça credenciais de login de convidado com os privilégios apropriados.

Recursos do mapa > Seção Datastores

Os datastores VMware são hospedados em volumes ONTAP FlexVol ou em LUNs ONTAP iSCSI ou FC usando VMware VMFS. Use a seção Datastores para definir o cluster ONTAP de destino, a máquina virtual de armazenamento (SVM) e o volume ou LUN para replicar os dados no disco para o destino.

Selecione a seta para baixo ao lado de **Datastores**. Com base na seleção de VMs, os mapeamentos de armazenamento de dados são selecionados automaticamente.

Esta seção pode ser ativada ou desativada dependendo da sua seleção.



- **Usar backups gerenciados pela plataforma e agendamentos de retenção**: se estiver usando uma solução externa de gerenciamento de snapshots, marque esta caixa. O NetApp Disaster Recovery oferece suporte ao uso de soluções externas de gerenciamento de snapshots, como o agendador de políticas nativo ONTAP SnapMirror ou integrações de terceiros. Se cada armazenamento de dados (volume) no plano de replicação já tiver um relacionamento SnapMirror que esteja sendo gerenciado em outro lugar, você poderá usar esses instantâneos como pontos de recuperação no NetApp Disaster Recovery.

  Quando esta opção é selecionada, o NetApp Disaster Recovery não configura um agendamento de backup. No entanto, você ainda precisa configurar um cronograma de retenção porque snapshots ainda podem ser tirados para operações de teste, failover e failback.

  Depois que isso for configurado, o serviço não fará nenhum snapshot agendado regularmente, mas dependerá da entidade externa para tirar e atualizar esses snapshots.

- **Hora de início**: insira a data e a hora em que você deseja que os backups e a retenção comecem a ser executados.
- **Intervalo de execução**: insira o intervalo de tempo em horas e minutos. Por exemplo, se você inserir 1 hora, o serviço fará um snapshot a cada hora.
- **Contagem de retenção**: insira o número de instantâneos que você deseja reter.

  O número de instantâneos retidos, juntamente com a taxa de alteração de dados entre cada instantâneo, determina a quantidade de espaço de armazenamento consumido na origem e no destino. Quanto mais instantâneos você retém, mais espaço de armazenamento é consumido.

- **Datastores de origem e destino**: Se houver vários relacionamentos SnapMirror (fan-out), você poderá selecionar o destino a ser usado. Se um volume já tiver um relacionamento SnapMirror estabelecido, os armazenamentos de dados de origem e destino correspondentes serão exibidos. Se um volume não tiver um relacionamento SnapMirror , você poderá criar um agora selecionando um cluster de destino, selecionando um SVM de destino e fornecendo um nome de volume. O serviço criará o volume e o relacionamento do SnapMirror .

  Se você quiser criar um relacionamento SnapMirror neste serviço, o cluster e seu peering SVM já deverão ter sido configurados fora do NetApp Disaster Recovery.

- Se as VMs forem do mesmo volume e do mesmo SVM, o serviço executará um snapshot ONTAP padrão e atualizará os destinos secundários.
- Se as VMs forem de volumes diferentes e do mesmo SVM, o serviço criará um instantâneo do grupo de consistência incluindo todos os volumes e atualizará os destinos secundários.
- Se as VMs forem de volumes diferentes e SVMs diferentes, o serviço executará um instantâneo da fase de início do grupo de consistência e da fase de confirmação, incluindo todos os volumes no mesmo cluster ou em um cluster diferente e atualizando os destinos secundários.
- Durante o failover, você pode selecionar qualquer snapshot. Se você selecionar o snapshot mais recente, o serviço criará um backup sob demanda, atualizará o destino e usará esse snapshot para o failover.

- **NFS LIF preferencial** e **Política de exportação**: Normalmente, deixe o serviço selecionar o NFS LIF preferencial e a política de exportação. Se você quiser usar um NFS LIF ou uma política de exportação específica, selecione a seta para baixo ao lado de cada campo e selecione a opção apropriada.

  Opcionalmente, você pode usar interfaces de dados específicas (LIFs) para um volume após um evento de failover. Isso é útil para balanceamento de tráfego de dados se o SVM de destino tiver vários LIFs.

  Para controle adicional sobre a segurança de acesso aos dados do NAS, o serviço pode atribuir diferentes volumes de armazenamento de dados a políticas de exportação NAS específicas. As políticas de exportação definem as regras de controle de acesso para clientes NFS que acessam os volumes do armazenamento de dados. Se você não especificar uma política de exportação, o serviço usará a política de exportação padrão para o SVM.

Recomenda-se criar uma política de exportação dedicada que limite o acesso ao volume *apenas* aos hosts vCenter ESXi de origem e destino que hospedarão as VMs protegidas. Isso garante que entidades externas não consigam acessar a exportação NFS.

Adicionar mapeamentos de failover de teste

Passos

1. Para definir mapeamentos diferentes para o ambiente de teste, desmarque a caixa e selecione a aba **Mapeamentos de teste**.
2. Percorra cada aba como antes, mas desta vez para o ambiente de teste.

   Na guia Mapeamentos de teste, os mapeamentos de máquinas virtuais e armazenamentos de dados estão desabilitados.

Você pode testar o plano completo mais tarde. Agora, você está configurando os mapeamentos para o ambiente de teste.

Revise o plano de replicação

Por fim, reserve alguns minutos para revisar o plano de replicação.

Mais tarde, você pode desabilitar ou excluir o plano de replicação.

Passos

1. Revise as informações em cada guia: Detalhes do plano, Mapeamento de failover e VMs.

2. Selecione **Adicionar plano**.

   O plano é adicionado à lista de planos.

Editar cronogramas para testar a conformidade e garantir que os testes de failover funcionem

Talvez você queira configurar cronogramas para testar a conformidade e os testes de failover para garantir que eles funcionarão corretamente caso você precise deles.

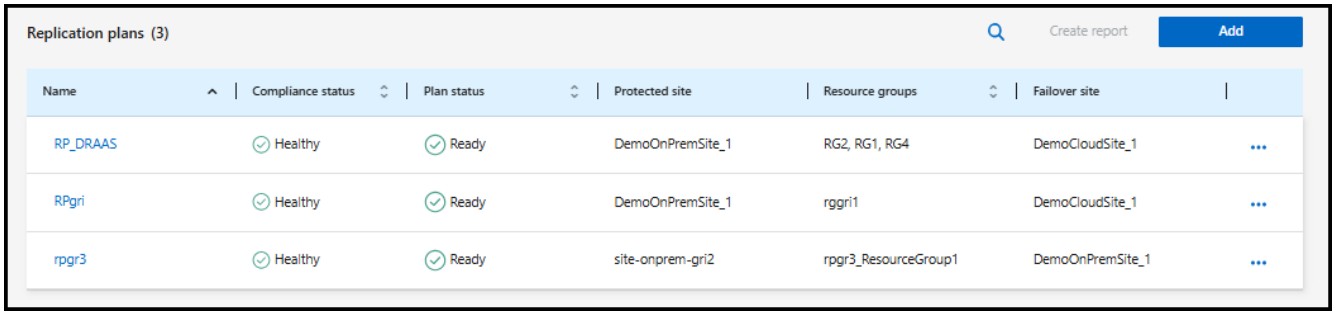
- **Impacto no tempo de conformidade**: quando um plano de replicação é criado, o serviço cria um cronograma de conformidade por padrão. O tempo de conformidade padrão é de 30 minutos. Para alterar esse horário, você pode editar o agendamento no plano de replicação.
- **Impacto do failover de teste**: Você pode testar um processo de failover sob demanda ou por meio de um agendamento. Isso permite que você teste o failover de máquinas virtuais para um destino especificado em um plano de replicação.

  Um failover de teste cria um volume FlexClone , monta o armazenamento de dados e move a carga de trabalho para esse armazenamento de dados. Uma operação de failover de teste *não* afeta as cargas de trabalho de produção, o relacionamento SnapMirror usado no site de teste e as cargas de trabalho protegidas que devem continuar operando normalmente.

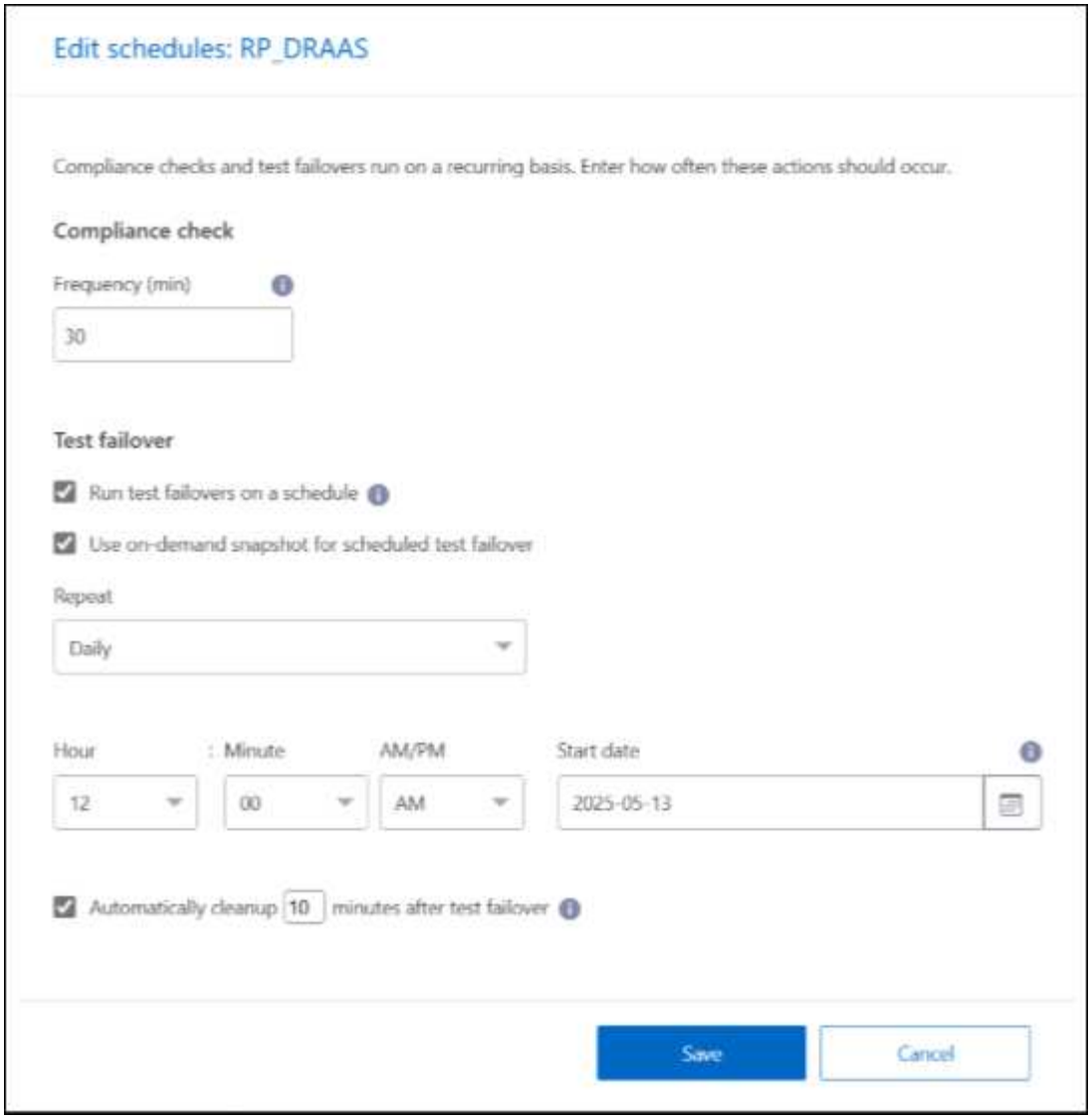
Com base no cronograma, o teste de failover é executado e garante que as cargas de trabalho sejam movidas para o destino especificado pelo plano de replicação.

Passos

1. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.



2. Selecione as **Ações*** ••• **ícone e selecione *Editar agendamentos**.
3. Insira com que frequência, em minutos, você deseja que o NetApp Disaster Recovery verifique a conformidade do teste.
4. Para verificar se seus testes de failover estão íntegros, marque **Executar failovers em uma programação mensal**.
   a. Selecione o dia do mês e a hora em que deseja que esses testes sejam executados.
   b. Insira a data no formato aaaa-mm-dd em que você deseja que o teste comece.



5. **Usar snapshot sob demanda para failover de teste agendado**: Para tirar um novo snapshot antes de iniciar o failover de teste automatizado, marque esta caixa.
6. Para limpar o ambiente de teste após a conclusão do teste de failover, marque **Limpar automaticamente após o failover do teste** e insira o número de minutos que você deseja aguardar antes que a limpeza comece.

> Este processo cancela o registro das VMs temporárias do local de teste, exclui o volume FlexClone que foi criado e desmonta os armazenamentos de dados temporários.

7. Selecione **Salvar**.

Replique aplicativos para outro site com o NetApp Disaster Recovery

Usando o NetApp Disaster Recovery, você pode replicar aplicativos VMware no seu site de origem para um site remoto de recuperação de desastres na nuvem usando a replicação SnapMirror .

Depois de criar o plano de recuperação de desastres, identificar a recorrência no assistente e iniciar uma replicação para um site de recuperação de desastres, a cada 30 minutos o NetApp Disaster Recovery verifica se a replicação está realmente ocorrendo de acordo com o plano. Você pode monitorar o progresso na página Job Monitor.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres ou administrador de failover de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Antes de começar

Antes de iniciar a replicação, você deve ter criado um plano de replicação e selecionado replicar os aplicativos. Em seguida, a opção **Replicar** aparece no menu Ações.

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu, selecione **Planos de replicação**.
4. Selecione o plano de replicação.
5. À direita, selecione a opção **Ações*** ••• **e selecione *Replicar**.

Migrar aplicativos para outro site com o NetApp Disaster Recovery

Usando o NetApp Disaster Recovery, você pode migrar aplicativos VMware do seu site de origem para outro site.

Depois de criar o plano de replicação, identificar a recorrência no assistente e iniciar a migração, a cada 30 minutos o NetApp Disaster Recovery verifica se a migração está realmente ocorrendo de acordo com o plano. Você pode monitorar o progresso na página Job Monitor.

Antes de começar

Antes de iniciar a migração, você deve ter criado um plano de replicação e selecionado migrar os aplicativos. Em seguida, a opção **Migrar** aparece no menu Ações.

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu, selecione **Planos de replicação**.
4. Selecione o plano de replicação.
5. À direita, selecione a opção **Ações*** ••• **e selecione *Migrar**.

Faça failover de aplicativos para um site remoto com o NetApp Disaster Recovery

Em caso de desastre, faça failover do seu site VMware local principal para outro site VMware local ou VMware Cloud na AWS. Você pode testar o processo de failover para garantir o sucesso quando precisar.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres ou administrador de failover de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Sobre esta tarefa

Durante uma falha de sistema, a Recuperação de Desastres usa, por padrão, a cópia de snapshot mais recente do SnapMirror , embora você possa selecionar um snapshot específico a partir de um snapshot pontual (de acordo com a política de retenção do SnapMirror). Utilize a opção de verificação pontual caso as réplicas mais recentes estejam comprometidas, como durante um ataque de ransomware.

Esse processo difere dependendo se o site de produção está íntegro e se você está executando um failover para o site de recuperação de desastres por outros motivos que não uma falha crítica de infraestrutura:

- Falha crítica no local de produção em que o cluster vCenter ou ONTAP de origem não está acessível: o NetApp Disaster Recovery permite que você selecione qualquer snapshot disponível para restaurar.
- O ambiente de produção está íntegro: você pode "Tirar um snapshot agora" ou selecionar um snapshot criado anteriormente.

Este procedimento interrompe o relacionamento de replicação, coloca as VMs de origem do vCenter offline, registra os volumes como armazenamentos de dados no vCenter de recuperação de desastres, reinicia as VMs protegidas usando as regras de failover no plano e habilita a leitura/gravação no site de destino.

Teste o processo de failover

Antes de iniciar o failover, você pode testar o processo. O teste não coloca as máquinas virtuais offline.

Durante um teste de failover, o Disaster Recovery cria máquinas virtuais temporariamente. O Risaster Recovery mapeia um armazenamento de dados temporário que faz backup do volume FlexClone nos hosts ESXi.

Esse processo não consome capacidade física adicional no armazenamento ONTAP local ou no FSx para armazenamento NetApp ONTAP na AWS. O volume de origem original não é modificado e as tarefas de replicação podem continuar mesmo durante a recuperação de desastres.

Quando terminar o teste, você deve redefinir as máquinas virtuais com a opção **Limpar teste**. Embora isso seja recomendado, não é obrigatório.

Uma operação de failover de teste *não* afeta as cargas de trabalho de produção, o relacionamento SnapMirror usado no site de teste e as cargas de trabalho protegidas que devem continuar operando normalmente.

Para um failover de teste, o Disaster Recovery executa as seguintes operações:

- Execute pré-verificações no cluster de destino e no relacionamento do SnapMirror .

- Crie um novo volume FlexClone a partir do snapshot selecionado para cada volume ONTAP protegido no cluster ONTAP do site de destino.
- Se algum armazenamento de dados for VMFS, crie e mapeie um iGroup para cada LUN.
- Registre as máquinas virtuais de destino no vCenter como novos armazenamentos de dados.
- Ligue as máquinas virtuais de destino com base na ordem de inicialização capturada na página Grupos de recursos.
- Desative todos os aplicativos de banco de dados suportados em VMs indicadas como "consistentes com o aplicativo".
- Se os clusters vCenter e ONTAP de origem ainda estiverem ativos, crie um relacionamento SnapMirror de direção reversa para replicar quaisquer alterações durante o estado de failover de volta ao site de origem original.

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.
4. Selecione o plano de replicação.
5. À direita, selecione a opção **Ações*** ••• **e selecione *Testar failover**.
6. Na página Test failover, insira “Test failover” e selecione **Test fail over**.
7. Após a conclusão do teste, limpe o ambiente de teste.

Limpe o ambiente de teste após um teste de failover

Após a conclusão do teste de failover, você deve limpar o ambiente de teste. Este processo remove as VMs temporárias do local de teste, os FlexClones e os armazenamentos de dados temporários.

Passos

1. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.
2. Selecione o plano de replicação.
3. À direita, selecione a opção **Ações**. ••• Em seguida, **limpe o teste de failover**.
4. Na página de teste de failover, digite "Limpar failover" e selecione **Limpeza do teste de failover**.

Fazer failover do site de origem para um site de recuperação de desastres

Em caso de desastre, faça failover do seu site VMware local principal sob demanda para outro site VMware local ou VMware Cloud on AWS com FSx para NetApp ONTAP.

O processo de failover envolve as seguintes operações:

- O Disaster Recovery executa pré-verificações no cluster de destino e no relacionamento do SnapMirror .
- Se você selecionou o snapshot mais recente, a atualização do SnapMirror será executada para replicar as últimas alterações.
- As máquinas virtuais de origem são desligadas.
- O relacionamento SnapMirror é quebrado e o volume de destino é tornado leitura/gravação.
- Com base na seleção do instantâneo, o sistema de arquivos ativo é restaurado para o instantâneo

especificado (mais recente ou selecionado).

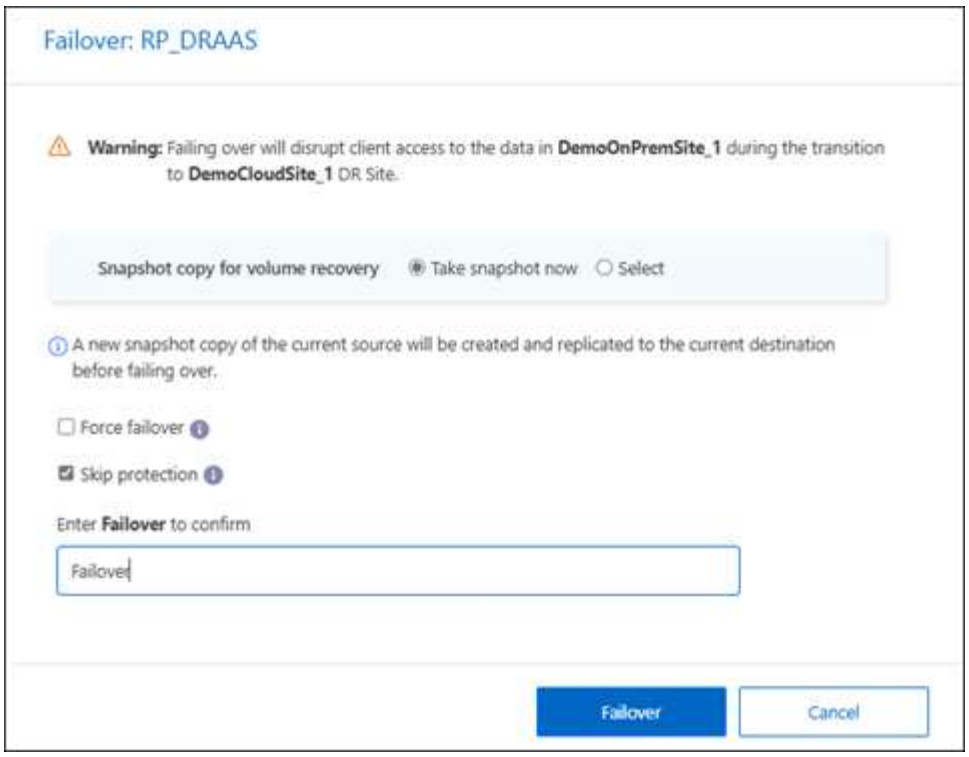
- Os armazenamentos de dados são criados e montados no cluster ou host VMware ou VMC com base nas informações capturadas no plano de replicação. Se algum armazenamento de dados for VMFS, crie e mapeie um iGroup para cada LUN.
- As máquinas virtuais de destino são registradas no vCenter como novos armazenamentos de dados.
- As máquinas virtuais de destino são ligadas com base na ordem de inicialização capturada na página Grupos de recursos.
- Se o vCenter de origem ainda estiver ativo, desligue todas as VMs do lado de origem que estão sofrendo failover.
- Desative todos os aplicativos de banco de dados suportados em VMs indicadas como "consistentes com o aplicativo".
- Se os clusters vCenter e ONTAP de origem ainda estiverem ativos, crie um relacionamento SnapMirror de direção reversa para replicar quaisquer alterações durante o estado de failover de volta para o site de origem original. O relacionamento do SnapMirror é revertido da máquina virtual de destino para a de origem.

Para planos de replicação baseados em armazenamento de dados, se você adicionou e descobriu alguma máquina virtual, mas não forneceu detalhes de mapeamento, essas máquinas virtuais serão incluídas no failover. A operação de failover falhará e uma notificação será exibida nos trabalhos. Você precisa fornecer os detalhes do mapeamento para concluir o failover com sucesso.

Após o início do failover, você poderá ver as VMs recuperadas no vCenter do site de recuperação de desastres (máquinas virtuais, redes e armazenamentos de dados). Por padrão, as máquinas virtuais são recuperadas para a pasta Carga de trabalho.

Passos

1. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.
2. Selecione o plano de replicação.
3. À direita, selecione a opção **Ações*** **e selecione *Fail over**.



4. Na página de Failover, crie um novo snapshot agora ou escolha um snapshot existente para o armazenamento de dados usar como base para a recuperação. A versão padrão é a mais recente.

   Um instantâneo da origem atual será tirado e replicado para o destino atual antes que o failover ocorra.

5. Opcionalmente, selecione **Forçar failover** se quiser que o failover ocorra mesmo se for detectado um erro que normalmente impediria a ocorrência do failover.
6. Opcionalmente, selecione **Ignorar proteção** se desejar que o serviço não crie automaticamente um relacionamento de proteção reversa do SnapMirror após um failover do plano de replicação. Isso é útil se você quiser executar operações adicionais no site restaurado antes de colocá-lo novamente online no NetApp Disaster Recovery.

   Você pode estabelecer proteção reversa selecionando **Proteger recursos** no menu Ações do plano de replicação. Isso tenta criar um relacionamento de replicação reversa para cada volume no plano. Você pode executar esta tarefa repetidamente até que a proteção seja restaurada. Quando a proteção for restaurada, você poderá iniciar um failback da maneira usual.

7. Digite "failover" na caixa.
8. Selecione **Fail over**.
9. Para verificar o progresso, no menu, selecione **Monitoramento de tarefas**.

Faça failback de aplicativos para a fonte original com o NetApp Disaster Recovery

Após a resolução de um desastre, faça failback do site de recuperação de desastres para o site de origem para retornar às operações normais. Você pode selecionar o snapshot do qual deseja recuperar.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres ou administrador de failover de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Sobre o failback

Em caso de failback, o NetApp Disaster Recovery replica (ressincroniza) quaisquer alterações de volta para a máquina virtual de origem original antes de inverter a direção da replicação. Esse processo começa com um relacionamento que concluiu a transição para um destino e envolve as seguintes etapas:

- Execute uma verificação de conformidade no site recuperado.
- Atualize as informações do vCenter para cada cluster do vCenter identificado como localizado no site recuperado.
- No site de destino, desligue e cancele o registro das máquinas virtuais e desmonte os volumes.
- Interrompa o relacionamento SnapMirror na fonte original para torná-la de leitura/gravação.
- Ressincronize o relacionamento do SnapMirror para reverter a replicação.
- Ligue e registre as máquinas virtuais de origem e monte os volumes na origem.

Antes de começar

Se você estiver usando proteção baseada em armazenamento de dados, as VMs que foram adicionadas ao armazenamento de dados podem ser adicionadas novamente durante o processo de failover. Caso isso tenha ocorrido, certifique-se de fornecer as informações de mapeamento adicionais para essas VMs antes de iniciar o failback. Para editar o mapeamento de recursos, consulte "Gerenciar planos de replicação".

Passos

1. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
2. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.
3. Selecione o plano de replicação.
4. À direita, selecione a opção **Ações*** ••• **e selecione *Fail back**.
5. Insira o nome do plano de replicação para iniciar o failback.
6. Escolha o snapshot do armazenamento de dados do qual deseja recuperar. O padrão é o mais recente.
7. Para monitorar o progresso da tarefa, selecione **Monitoramento de tarefas** no menu Recuperação de desastres.

Gerencie sites, grupos de recursos, planos de replicação, repositórios de dados e informações de máquinas virtuais com o NetApp Disaster Recovery

O NetApp Disaster Recovery oferece visões gerais e perspectivas mais detalhadas de todos os seus recursos:

- Locais

- Grupos de recursos
- Planos de replicação
- Armazenamentos de dados
- Máquinas virtuais

As tarefas exigem funções diferentes do NetApp Console . Para obter detalhes, consulte a seção *Função necessária do NetApp Console * em cada tarefa.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Gerenciar sites do vCenter

Você pode editar o nome do site do vCenter e o tipo de site (local ou AWS).

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto ou administrador de recuperação de desastres.

Passos

1. No menu, selecione **Sites**.
2. Selecione a opção **Ações***  **à direita do nome do vCenter e selecione *Editar**.
3. Edite o nome e o local do site do vCenter.

Gerenciar grupos de recursos

Você pode criar grupos de recursos por máquinas virtuais ou por datastores. Eles podem ser adicionados ao criar o plano de replicação ou posteriormente.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

Você pode criar um grupo de recursos por armazenamentos de dados das seguintes maneiras:

- Ao adicionar um grupo de recursos usando armazenamentos de dados, você pode ver uma lista de armazenamentos de dados. Você pode selecionar um ou mais armazenamentos de dados para criar um grupo de recursos.
- Ao criar um plano de replicação e um grupo de recursos dentro do plano, você pode ver as VMs nos armazenamentos de dados.

Você pode realizar as seguintes tarefas com grupos de recursos:

- Alterar o nome do grupo de recursos.
- Adicione VMs ao grupo de recursos.
- Remova VMs do grupo de recursos.
- Excluir grupos de recursos.

Para obter detalhes sobre como criar um grupo de recursos, consulte"Crie um grupo de recursos para organizar VMs em conjunto" .

Passos

1. No menu, selecione **Grupos de recursos**.
2. Para adicionar um grupo de recursos, selecione **Adicionar grupo**.
3. Você pode modificar ou excluir o grupo de recursos selecionando a opção **Ações**. ••• .

Gerenciar planos de replicação

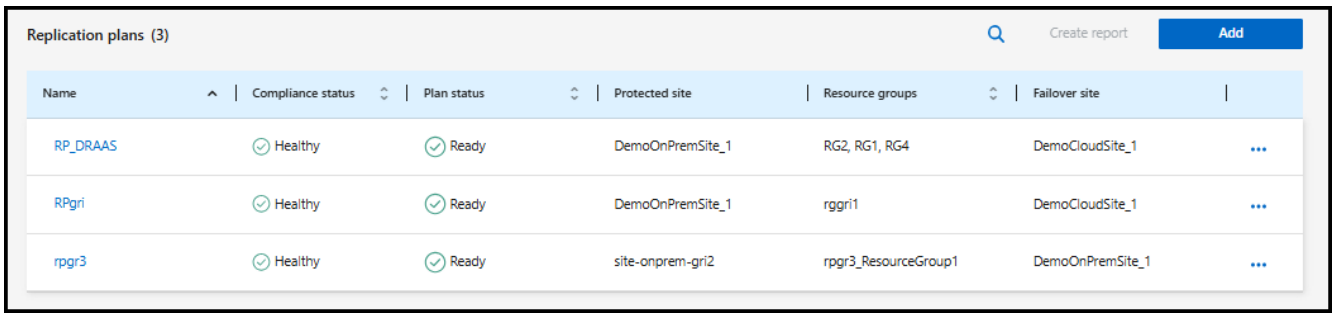
Você pode desabilitar, habilitar e excluir planos de replicação. Você pode alterar horários.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

- Se quiser pausar um plano de replicação temporariamente, você pode desativá-lo e habilitá-lo depois.
- Se você não precisar mais do plano, poderá excluí-lo.

Passos

1. No menu, selecione **Planos de replicação**.



2. Para visualizar os detalhes do plano, selecione a opção **Ações*** ••• **e selecione *Ver detalhes do plano**.
3. Faça qualquer um dos seguintes:
   - Para editar os detalhes do plano (alterar a recorrência), selecione a aba **Detalhes do plano** e selecione o ícone **Editar** à direita.
   - Para editar os mapeamentos de recursos, selecione a guia **Mapeamento de failover** e selecione o ícone **Editar**.
   - Para adicionar ou editar as máquinas virtuais, selecione a aba **Máquinas virtuais** e selecione a opção **Adicionar VMs** ou o ícone **Editar**.
4. Retorne à lista de planos selecionando "Planos de replicação" nas trilhas de navegação à esquerda.
5. Para executar ações com o plano, na lista de planos de replicação, selecione a opção **Ações*** ••• **à direita do plano e selecione qualquer uma das opções, como *Editar agendamentos**, **Testar failover**, **Failover**, **Failback**, **Migrar**, **Tirar snapshot agora**, **Limpar snapshots antigos**, **Desativar**, **Ativar** ou **Excluir**.
6. Para definir ou alterar um cronograma de failover de teste ou definir a verificação de frequência de conformidade, selecione a opção **Ações*** ••• **à direita do plano e selecione *Editar agendamentos**.
   a. Na página Editar agendamentos, insira a frequência em minutos com que você deseja que a verificação de conformidade de failover ocorra.
   b. Marque **Executar failovers de teste conforme agendamento**.
   c. Na opção Repetir, selecione a programação diária, semanal ou mensal.

d. Selecione **Salvar**.

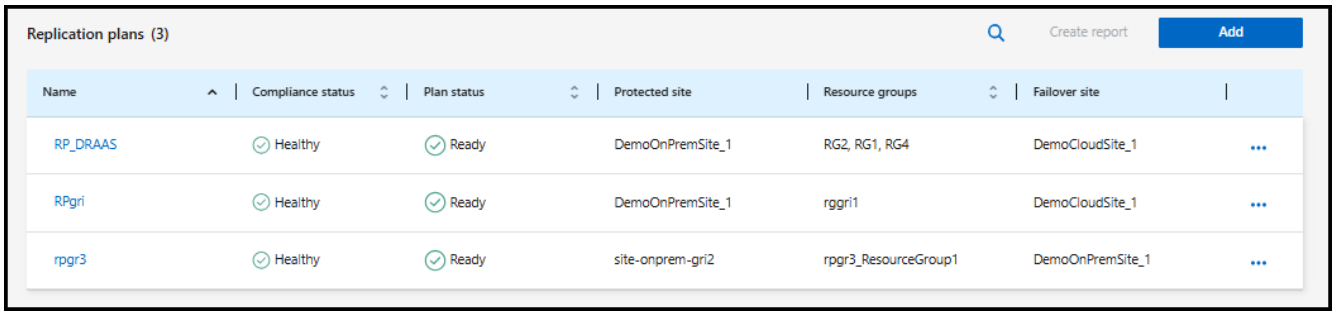
Reconciliar instantâneos sob demanda

A Recuperação de Desastres exclui automaticamente os snapshots na origem a cada 24 horas. Se você descobrir que os snapshots estão dessincronizados entre a origem e o destino, precisará resolver a discrepância entre os snapshots para garantir a consistência entre os sites.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

Passos

1. No menu, selecione **Planos de replicação**.



2. Na lista de planos de replicação, selecione a opção **Ações**. ••• Em seguida, **Reconciliar instantâneos**.
3. Revise as informações de reconciliação.
4. Selecione **Reconciliar**.

Excluir um plano de replicação

Se você excluir um plano de replicação, também poderá excluir os snapshots primários e secundários criados pelo plano.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

Passos

1. No menu, selecione **Planos de replicação**.
2. Selecione a opção **Ações*** ••• **à direita do plano e selecione *Excluir**.
3. Selecione se deseja excluir os snapshots primários, os snapshots secundários ou apenas os metadados criados pelo plano.
4. Digite "excluir" para confirmar a exclusão.
5. Selecione **Excluir**.

Alterar contagem de retenção para agendamentos de failover

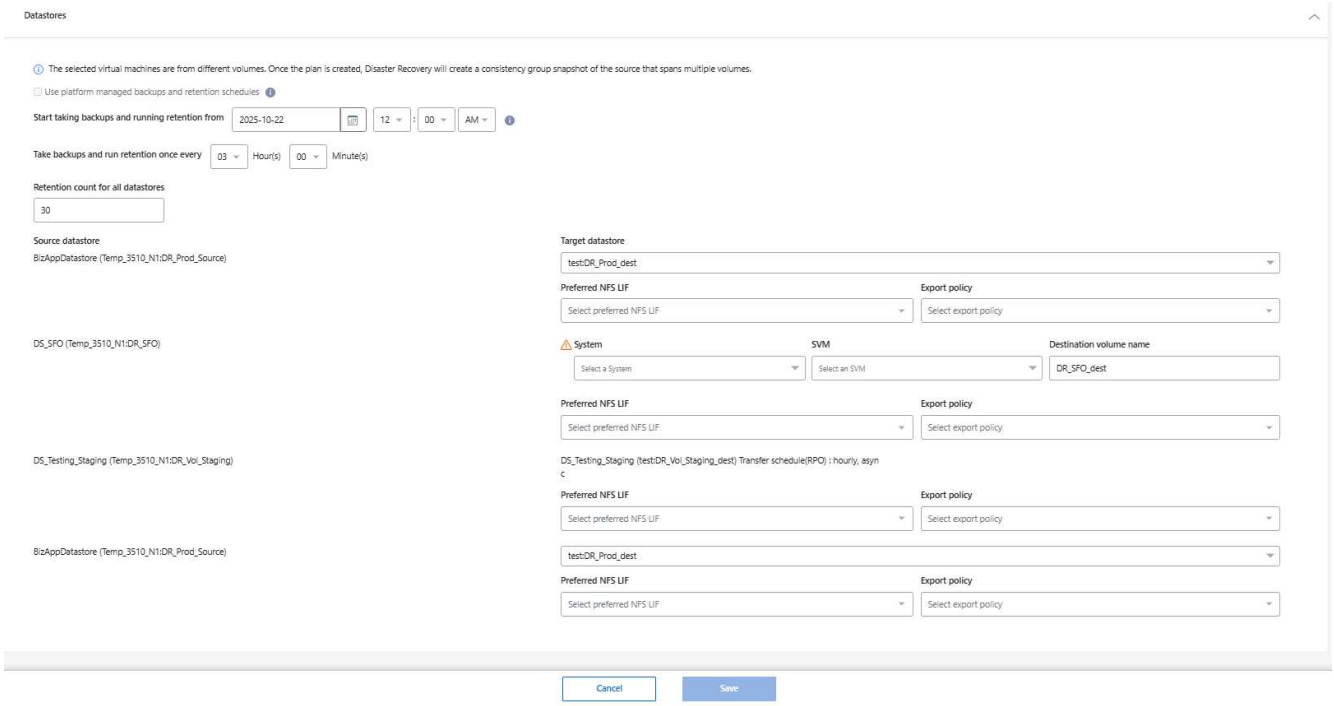
Alterar o número de retenções permite aumentar ou diminuir a quantidade de dados armazenados.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto,

administrador de recuperação de desastres, administrador de failover de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

Passos

1. No menu, selecione **Planos de replicação**.
2. Selecione o plano de replicação e, em seguida, a guia **Mapeamento de failover**. Selecione o ícone de lápis **Editar**.
3. Selecione a seta para baixo na linha **Datastores** para expandi-la.



4. Altere o valor da **Contagem de retenção para todos os armazenamentos de dados**.
5. Com o plano de replicação selecionado, selecione o menu Ações e, em seguida, selecione **Limpar instantâneos antigos** para remover instantâneos antigos no destino para corresponder à nova contagem de retenção.

Exibir informações dos armazenamentos de dados

Você pode visualizar informações sobre quantos armazenamentos de dados existem na origem e no destino.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres, administrador de aplicativo de recuperação de desastres ou função de visualizador de recuperação de desastres.

Passos

1. No menu, selecione **Painel**.
2. Selecione o vCenter na linha do site.
3. Selecione **Datastores**.
4. Visualize as informações dos armazenamentos de dados.

Exibir informações das máquinas virtuais

Você pode visualizar informações sobre quantas máquinas virtuais existem na origem e no destino, juntamente com CPU, memória e capacidade disponível.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres, administrador de aplicativo de recuperação de desastres ou função de visualizador de recuperação de desastres.

Passos

1. No menu, selecione **Painel**.
2. Selecione o vCenter na linha do site.
3. Selecione **Máquinas virtuais**.
4. Veja as informações das máquinas virtuais.

Monitorar trabalhos de NetApp Disaster Recovery

Você pode monitorar todos os trabalhos de NetApp Disaster Recovery e determinar seu progresso.

Ver empregos

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de aplicativo de recuperação de desastres ou função de visualizador de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as funções de acesso do NetApp Console para todos os serviços".

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. No menu, selecione **Monitoramento de tarefas**.
4. Explore todos os trabalhos relacionados às operações e revise seus registros de data e hora e status.
5. Para visualizar detalhes de um trabalho específico, selecione essa linha.
6. Para atualizar as informações, selecione **Atualizar**.

Cancelar um trabalho

Se um trabalho estiver em andamento ou em estado de fila e você não quiser que ele continue, você pode cancelá-lo. Talvez você queira cancelar um trabalho se ele estiver travado no mesmo estado e você quiser liberar a próxima operação na fila. Talvez você queira cancelar um trabalho antes que ele expire.

*Função necessária do NetApp Console * Administrador da organização, administrador de pasta ou projeto, administrador de recuperação de desastres, administrador de failover de recuperação de desastres ou administrador de aplicativo de recuperação de desastres.

"Saiba mais sobre funções e permissões de usuário no NetApp Disaster Recovery". "Saiba mais sobre as

funções de acesso do NetApp Console para todos os serviços".

Passos

1. Na barra de navegação esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
2. No menu, selecione **Monitoramento de tarefas**.
3. Na página Monitor de tarefas, anote o ID da tarefa que você deseja cancelar.

   O trabalho deve estar no estado "Em andamento" ou "Na fila".

4. Na coluna Ações, selecione **Cancelar trabalho**.

Crie relatórios de NetApp Disaster Recovery

Analisar os relatórios de NetApp Disaster Recovery pode ajudar você a analisar sua preparação para recuperação de desastres. Os relatórios pré-projetados incluem um resumo de failovers de teste, detalhes do plano de replicação e detalhes do trabalho em todos os sites de uma conta nos últimos sete dias.

Você pode baixar relatórios em formato PDF, HTML ou JSON.

O link para download é válido por seis horas.

Passos

1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
3. Na barra de navegação esquerda do NetApp Console , selecione **Planos de replicação**.
4. Selecione **Criar relatório**.
5. Selecione o tipo de formato de arquivo e o período nos últimos 7 dias.
6. Selecione **Criar**.

   O relatório pode levar alguns minutos para ser exibido.

7. Para baixar um relatório, selecione **Baixar relatório** e selecione-o na pasta Download do administrador.

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

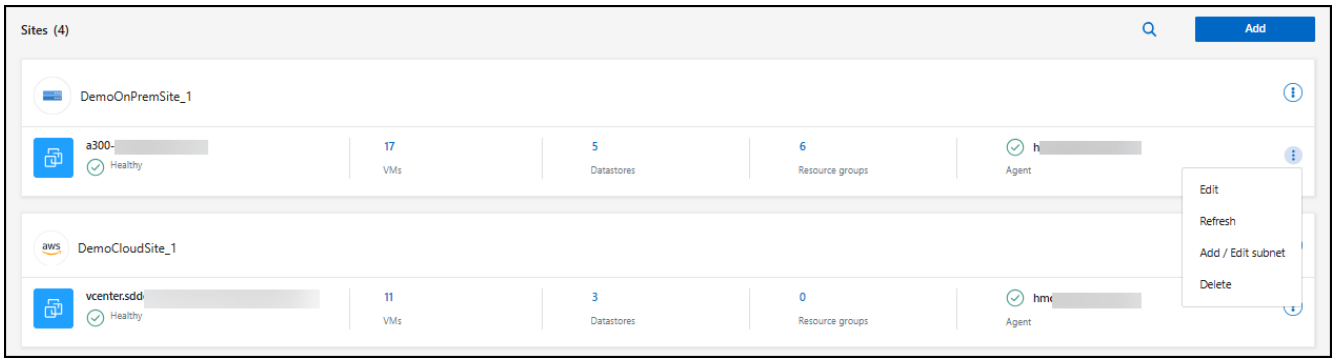
O NetApp Console suporta o uso de vários agentes de console em um único ambiente de trabalho. Utilizar vários agentes de console pode ser útil para manter o acesso aos recursos enquanto se realiza manutenção em outro agente de console ou caso um agente de console apresente falha. Como cada agente do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

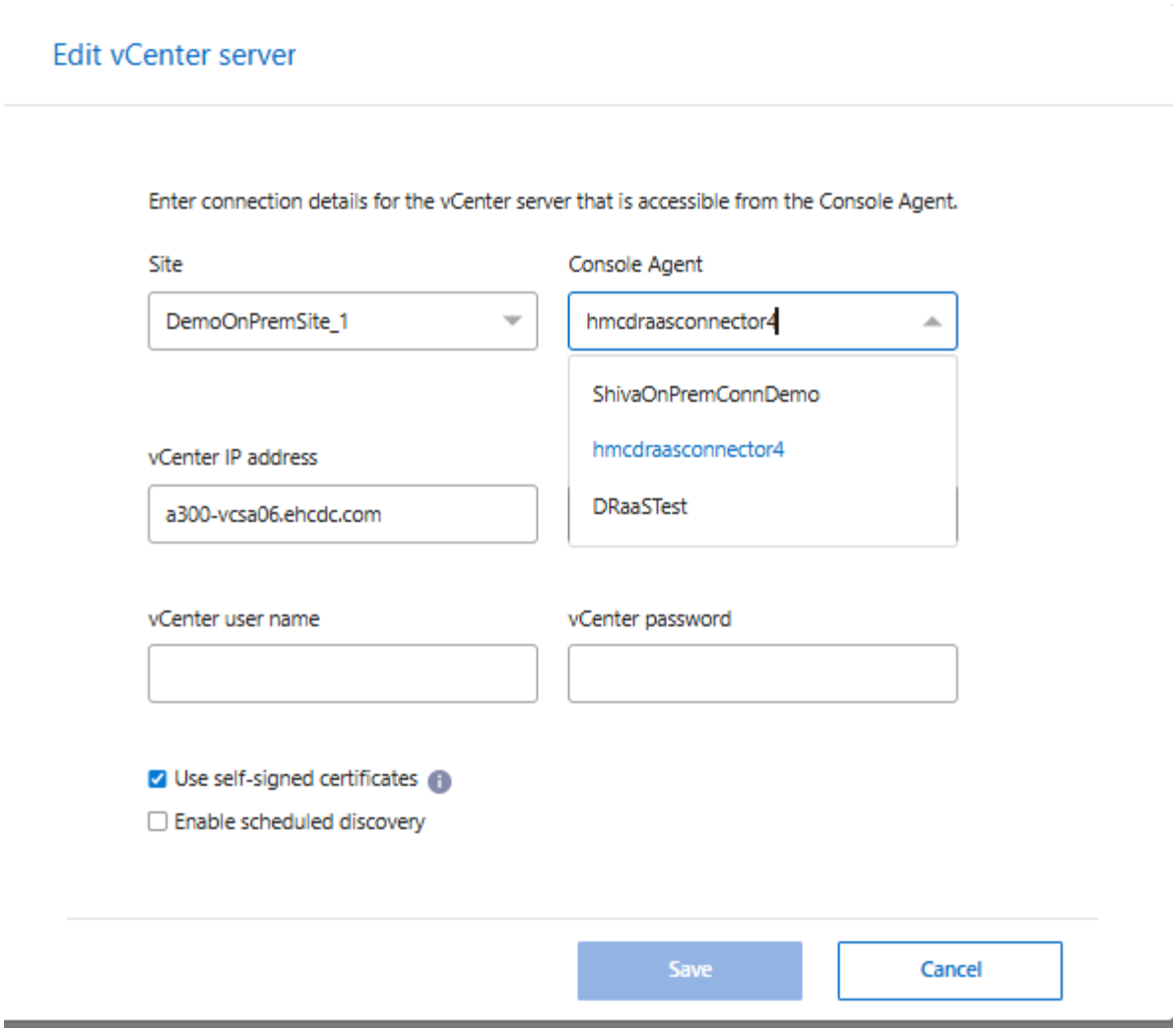
- Você deve terAdicionou pelo menos dois agentes de console ao seu ambiente de trabalho. .
- Ambos os agentes do Console devem conter os mesmos clusters ONTAP .

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**.



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

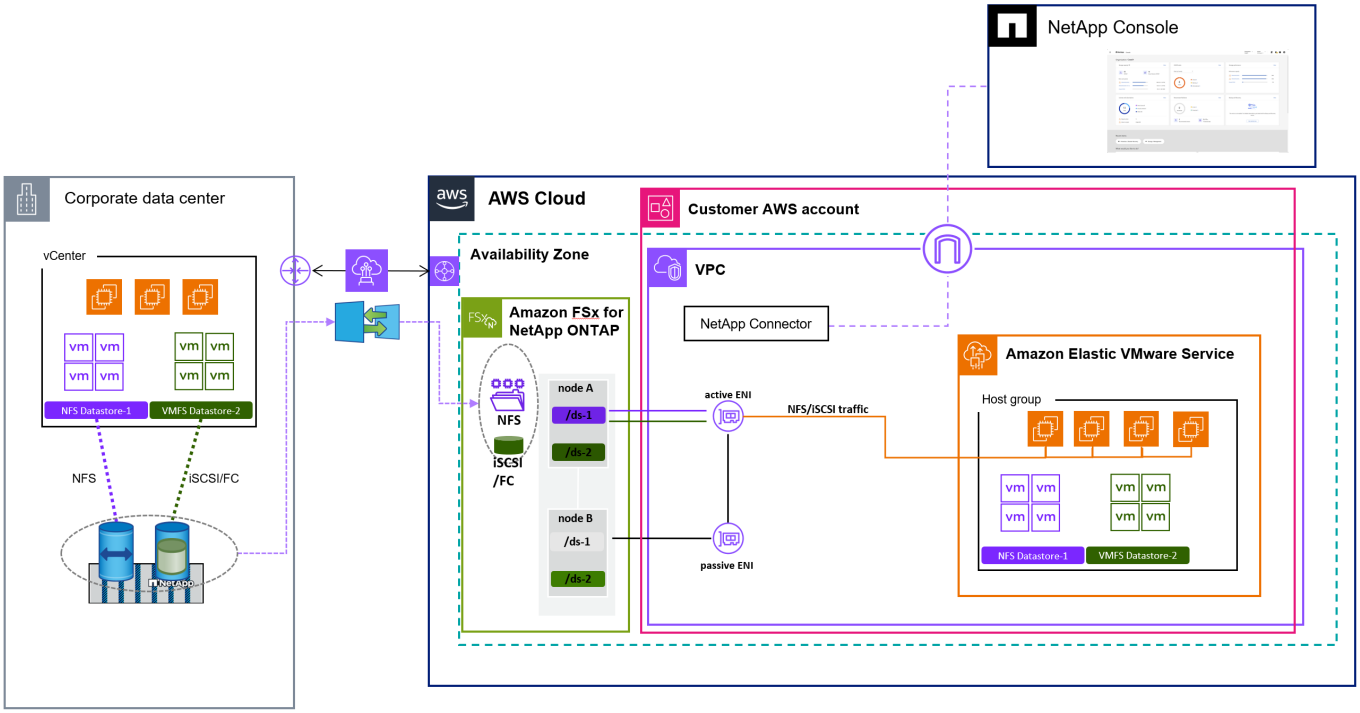
O NetApp Disaster Recovery é um serviço de valor agregado hospedado no ambiente de software como serviço do NetApp Console , que depende da arquitetura principal do NetApp Console . Vários componentes principais compõem o serviço DR para proteção do VMware no Console.

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 distribui 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 .

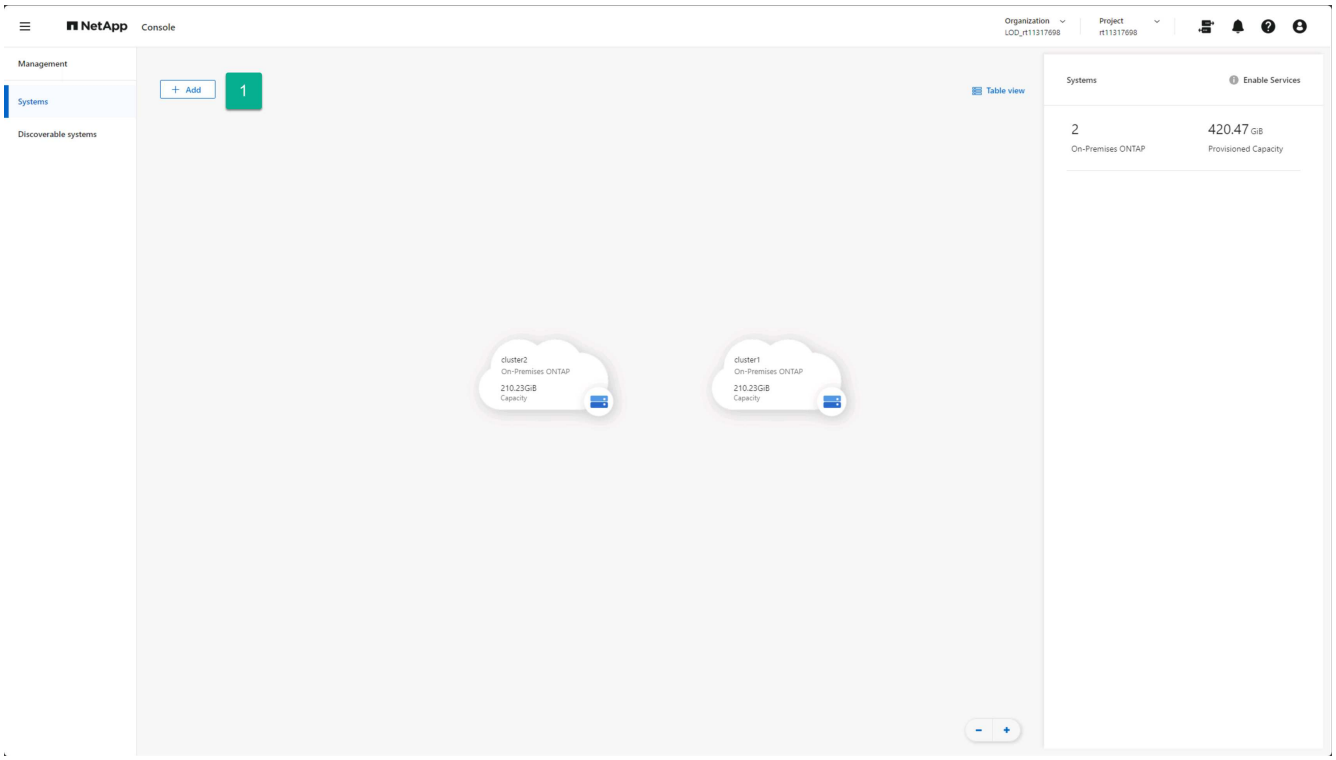
Você precisa fazer o seguinte:

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

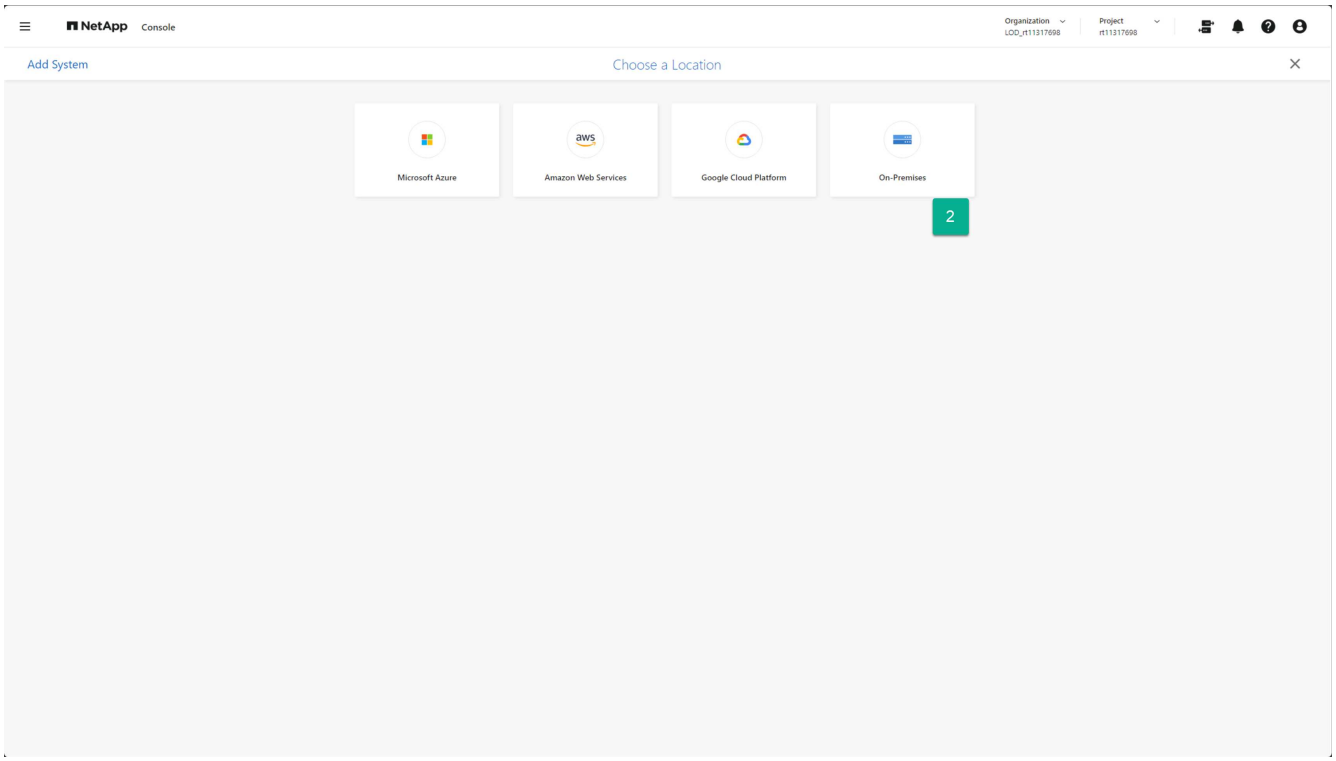
Adicionar matrizes de armazenamento locais ao sistema NetApp Console

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

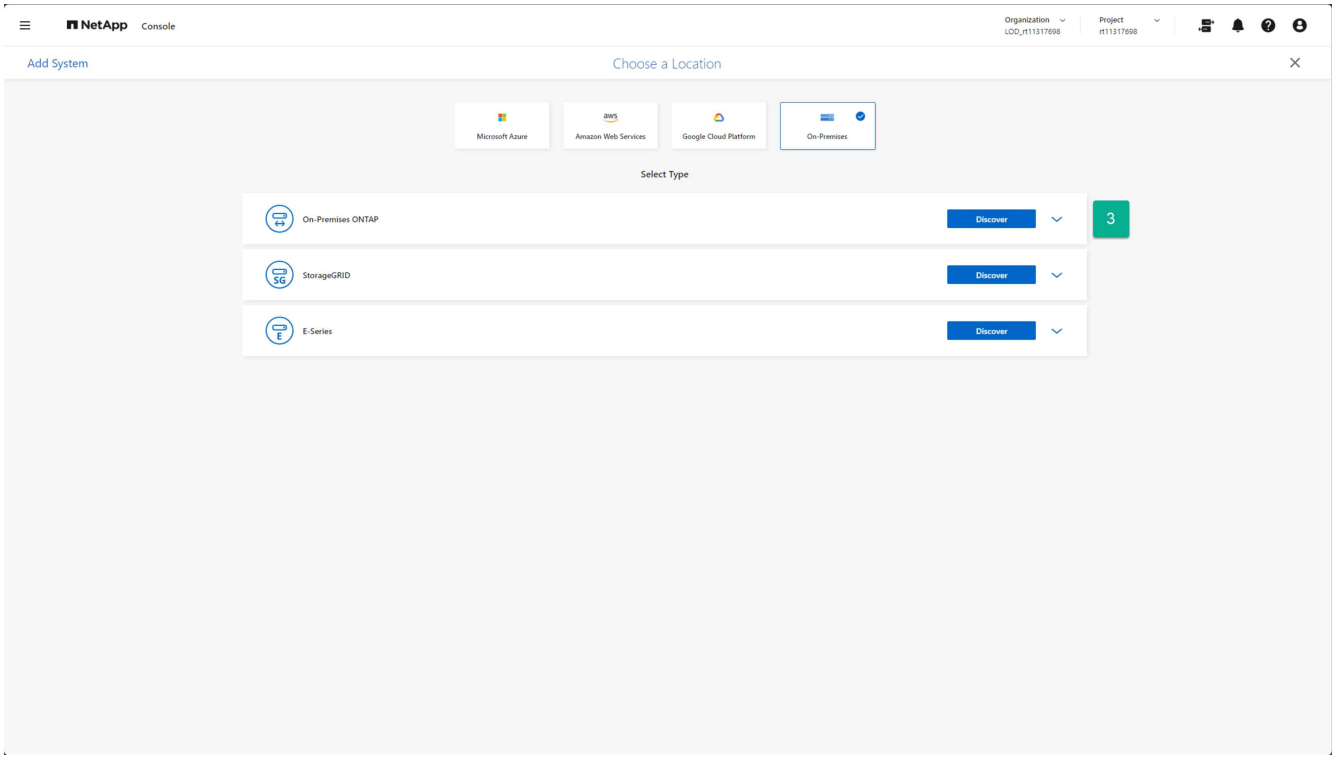
1. Na página Sistemas do NetApp Console , selecione **Adicionar sistema**.



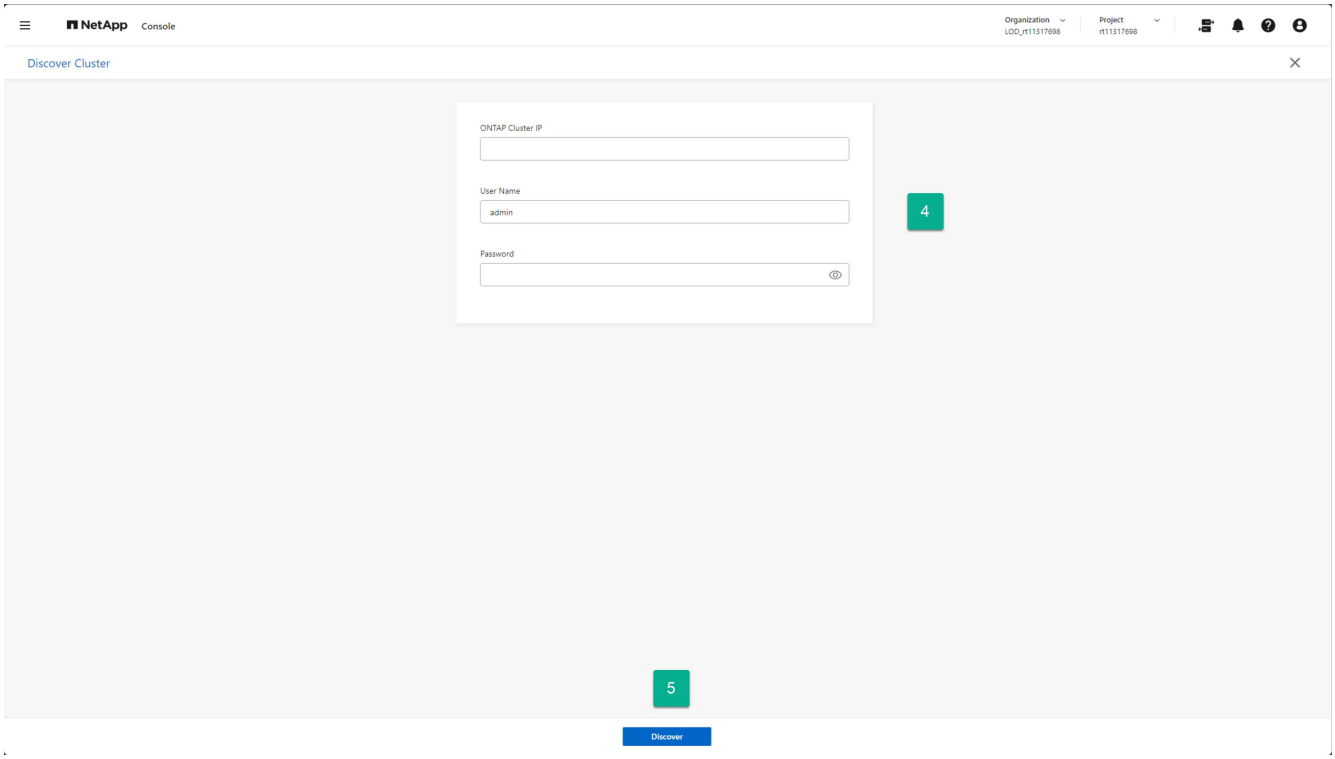
2. Na página Adicionar sistema, selecione o cartão **On-Premises**.



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



4. Na página Descobrir Cluster, insira as seguintes informações:
   a. O endereço IP da porta de gerenciamento do cluster do array ONTAP
   b. O nome de usuário do administrador
   c. A senha do administrador
5. Selecione **Descobrir** na parte inferior da página.

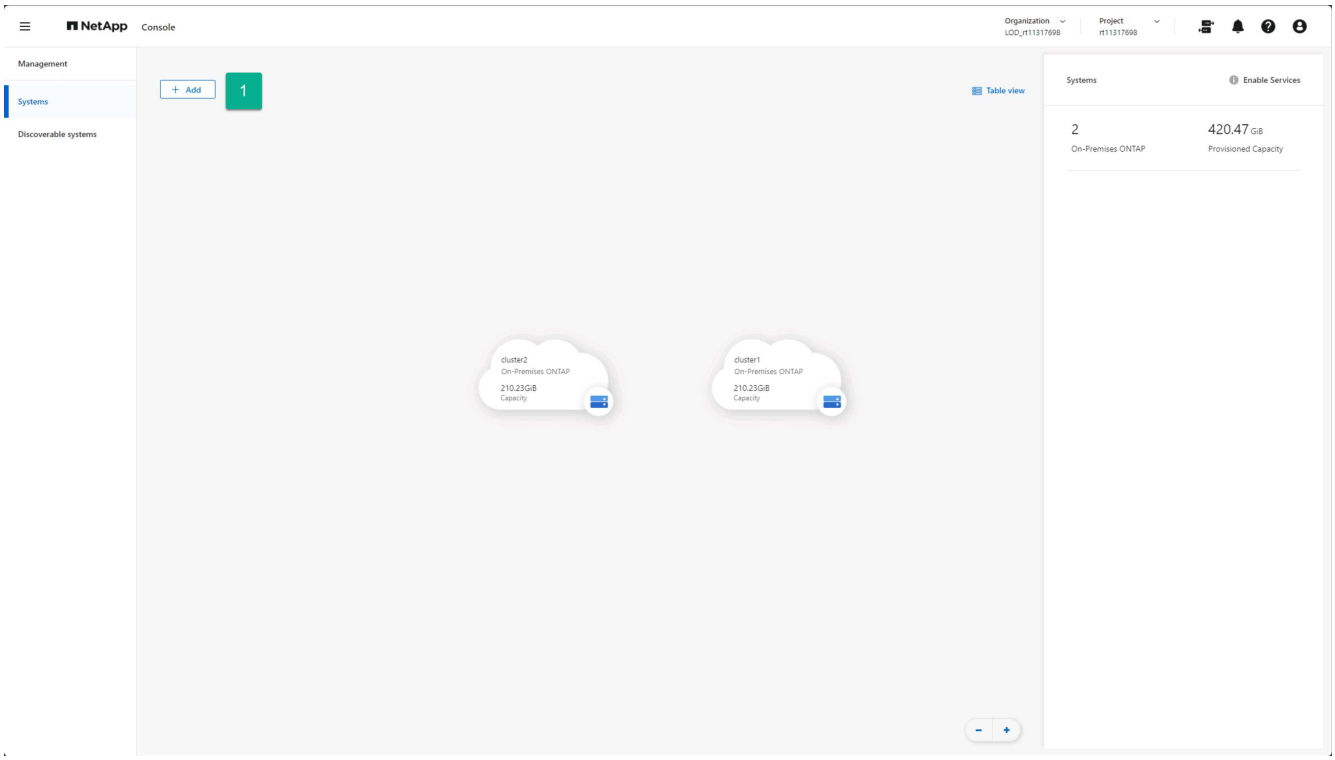


6. Repita as etapas 1 a 5 para cada matriz ONTAP que hospedará os armazenamentos de dados do vCenter.

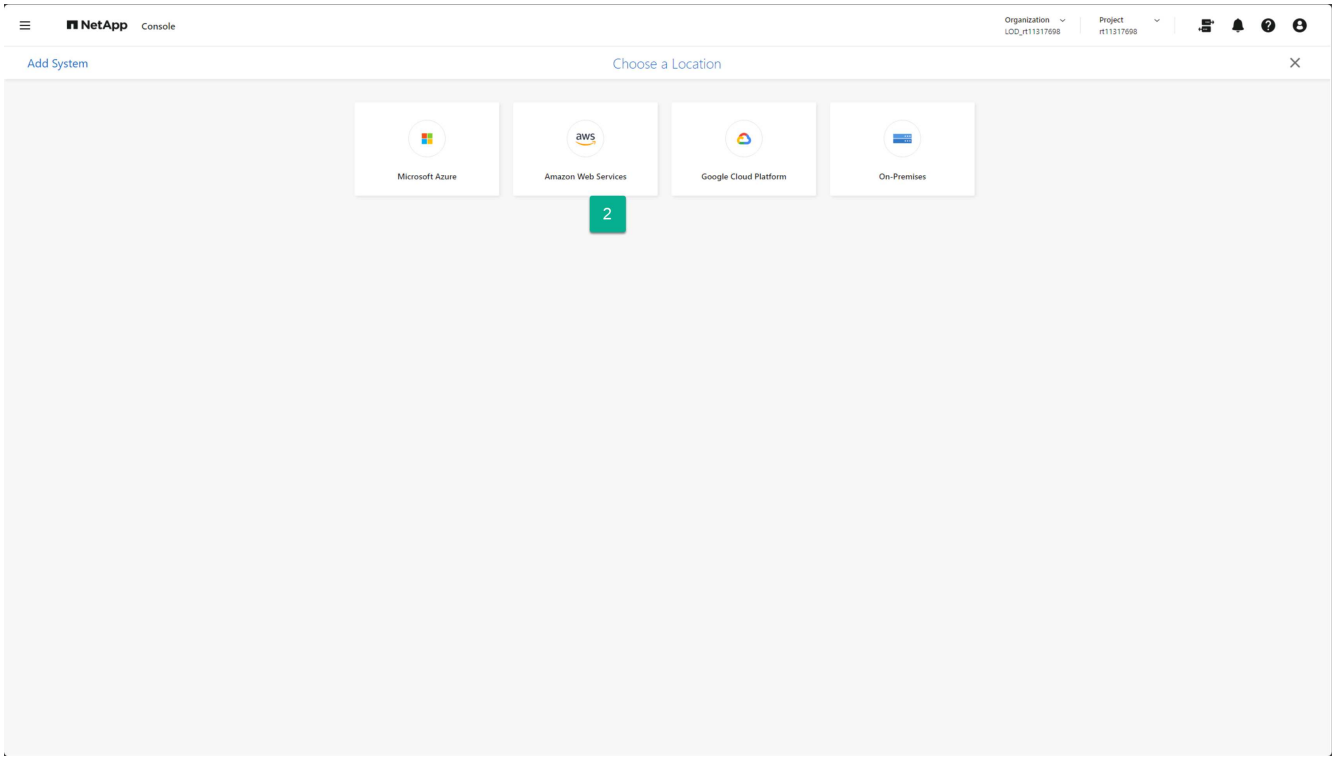
Adicionar instâncias de armazenamento do Amazon FSx for NetApp ONTAP ao sistema NetApp Console

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

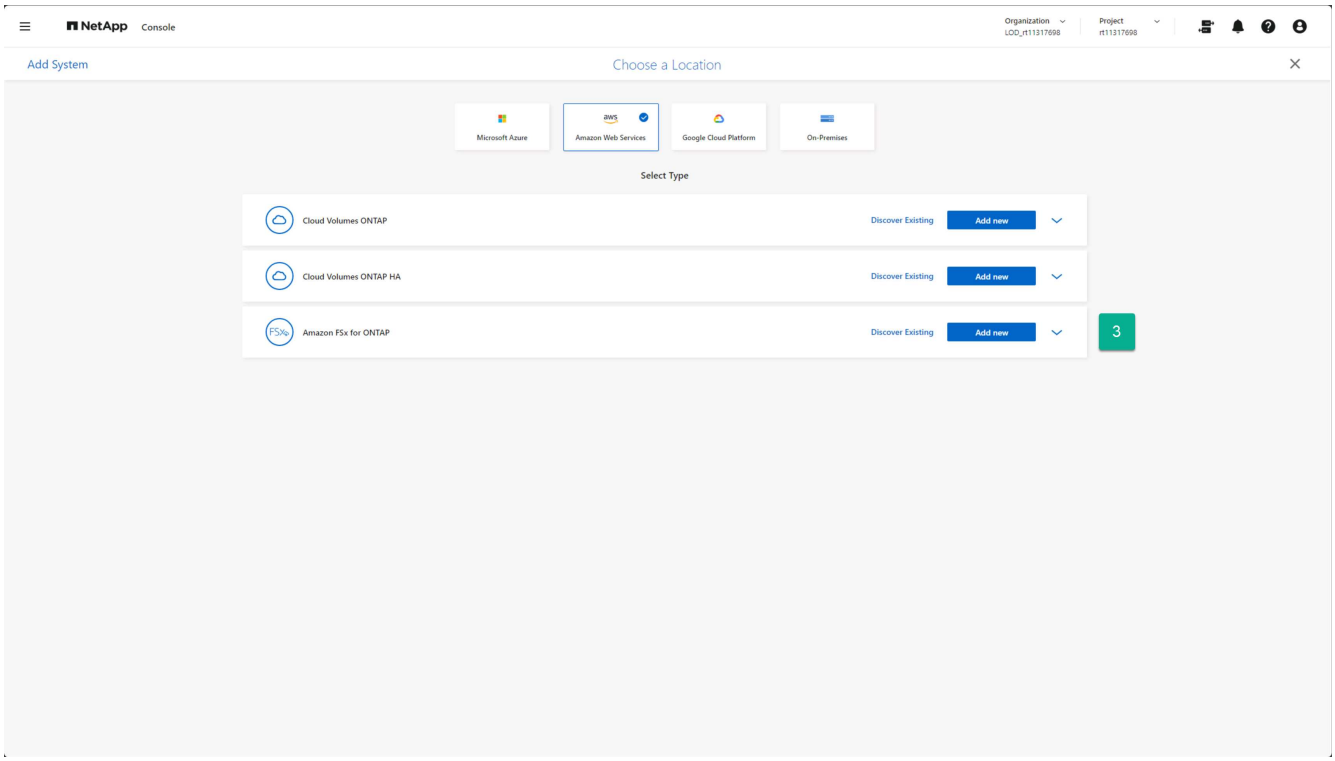
1. Na página Sistemas do NetApp Console , selecione **Adicionar sistema**.



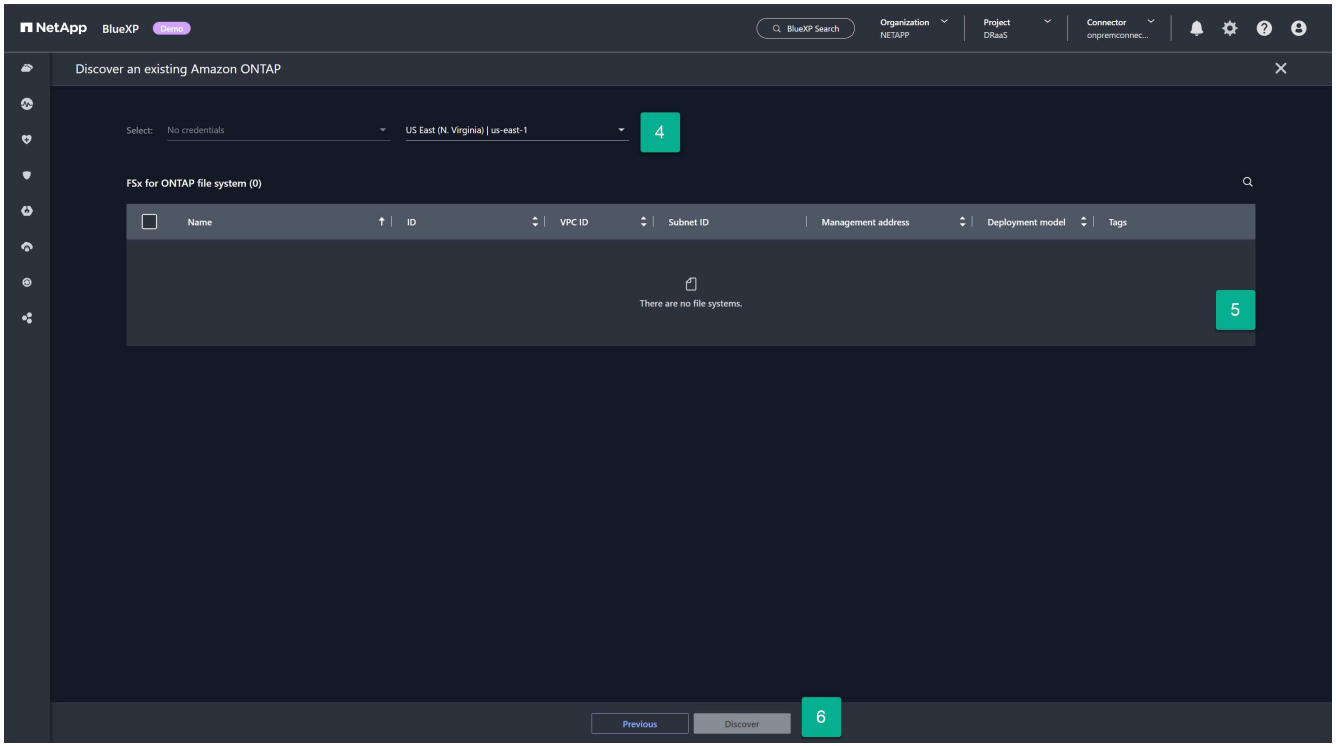
2. Na página Adicionar sistema, selecione o cartão **Amazon Web Services**.



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:

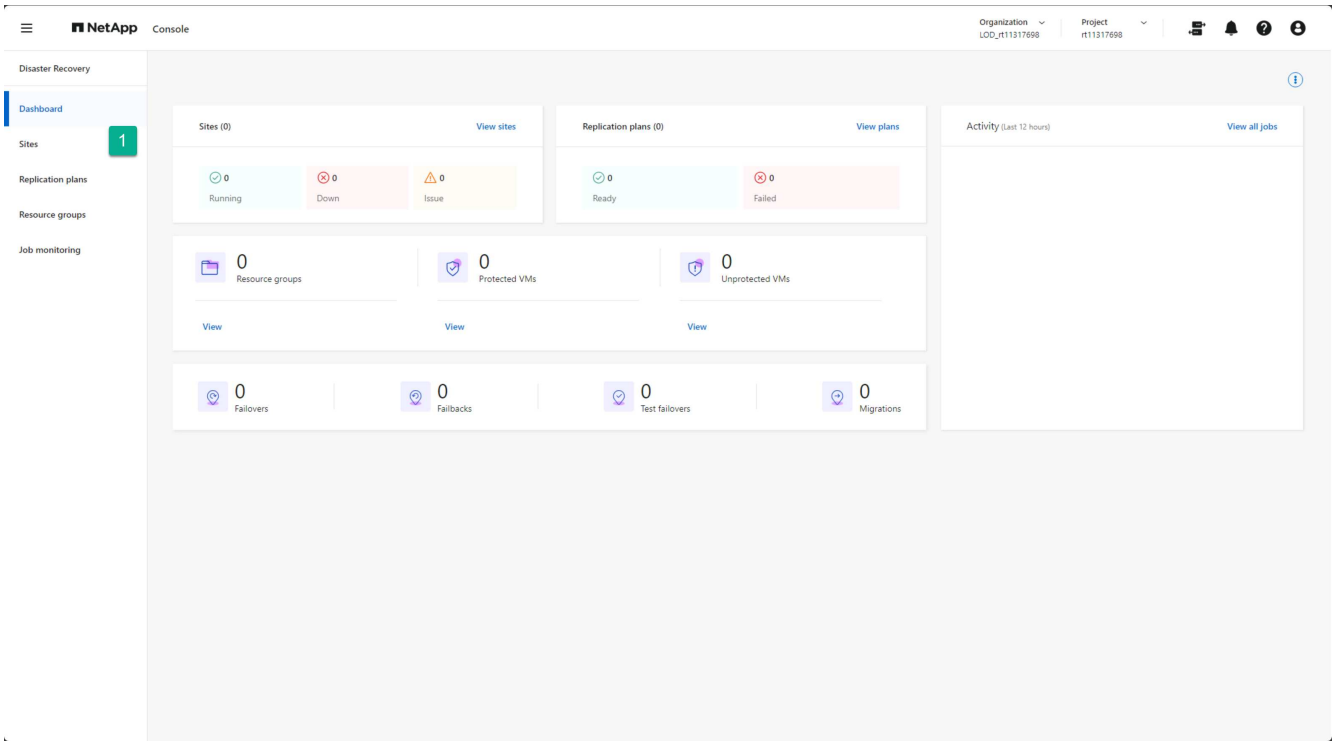
- Um site para representar cada datacenter de produção onde seus clusters vCenter de produção residem
- Um site para seu datacenter em nuvem Amazon EVS/ Amazon FSx for NetApp ONTAP

Crie sites locais

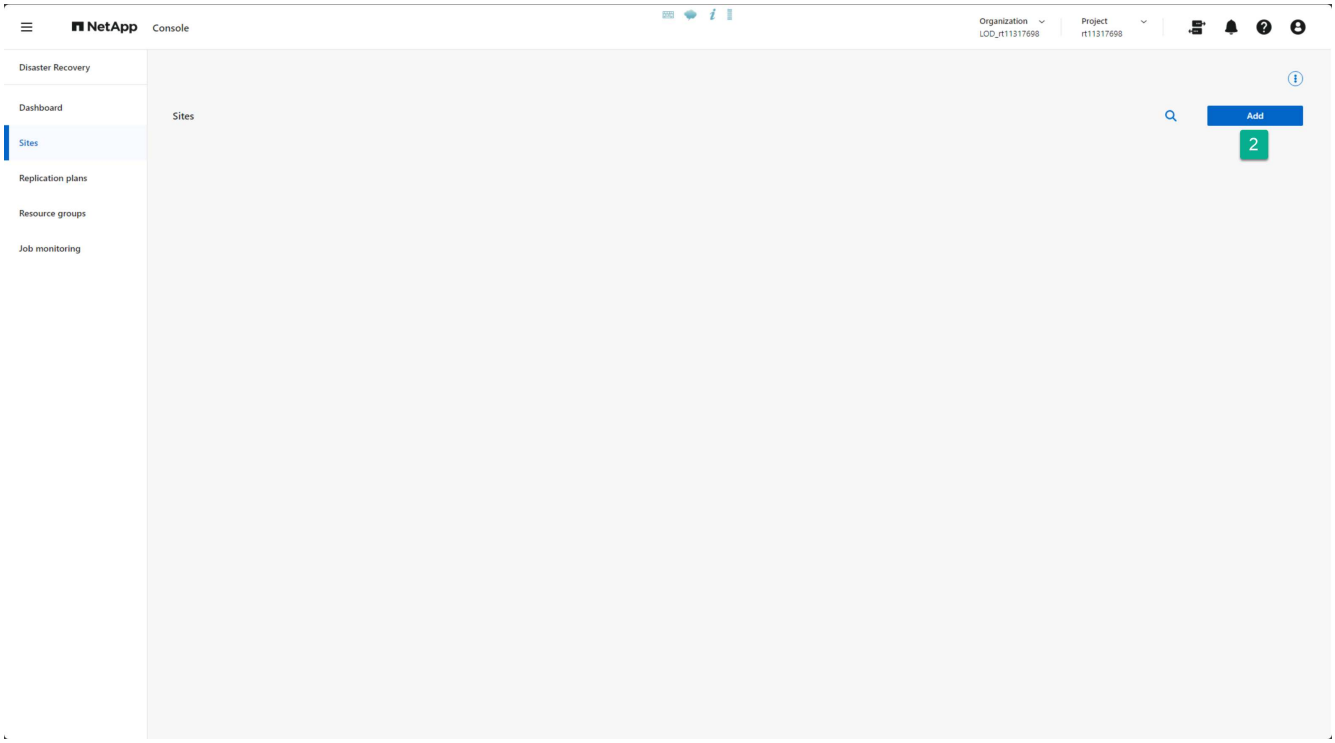
Crie um site de produção do vCenter.

Passos

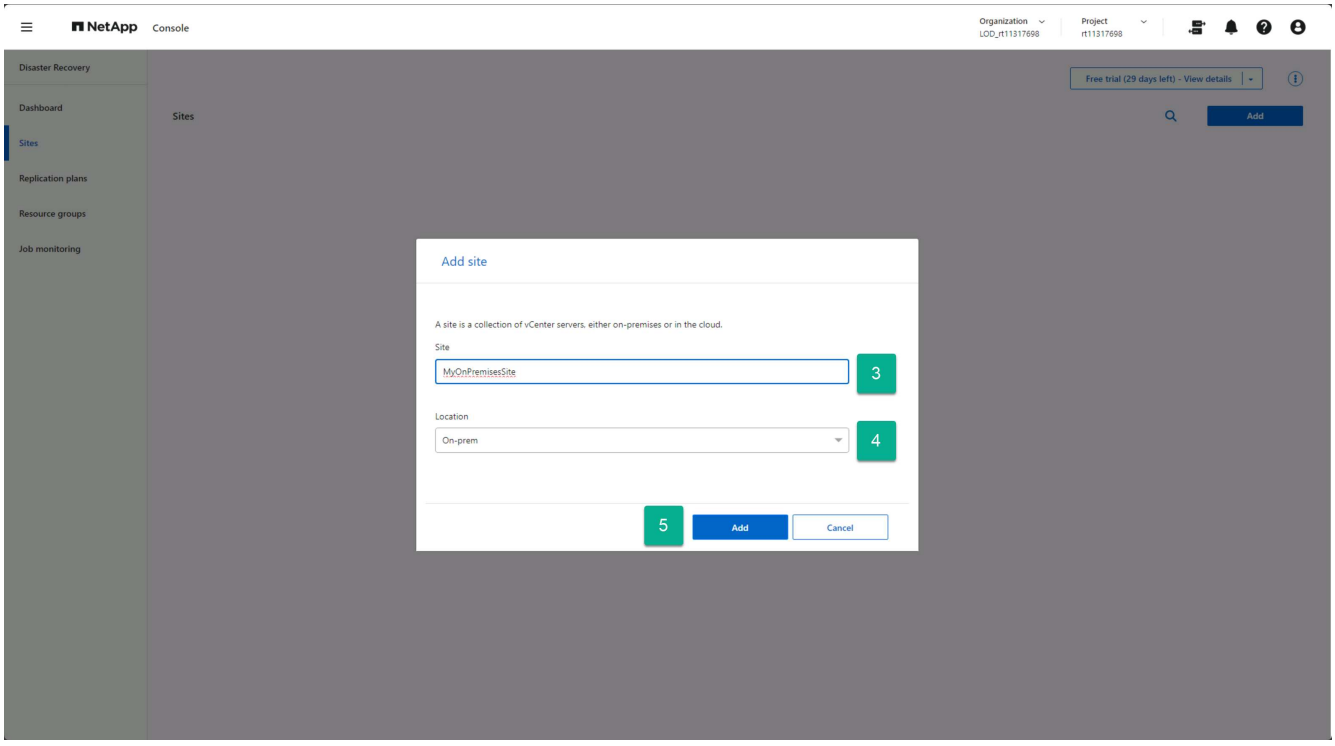
1. Na barra de navegação esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
2. Em qualquer página do NetApp Disaster Recovery, selecione a opção **Sites**.



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**.

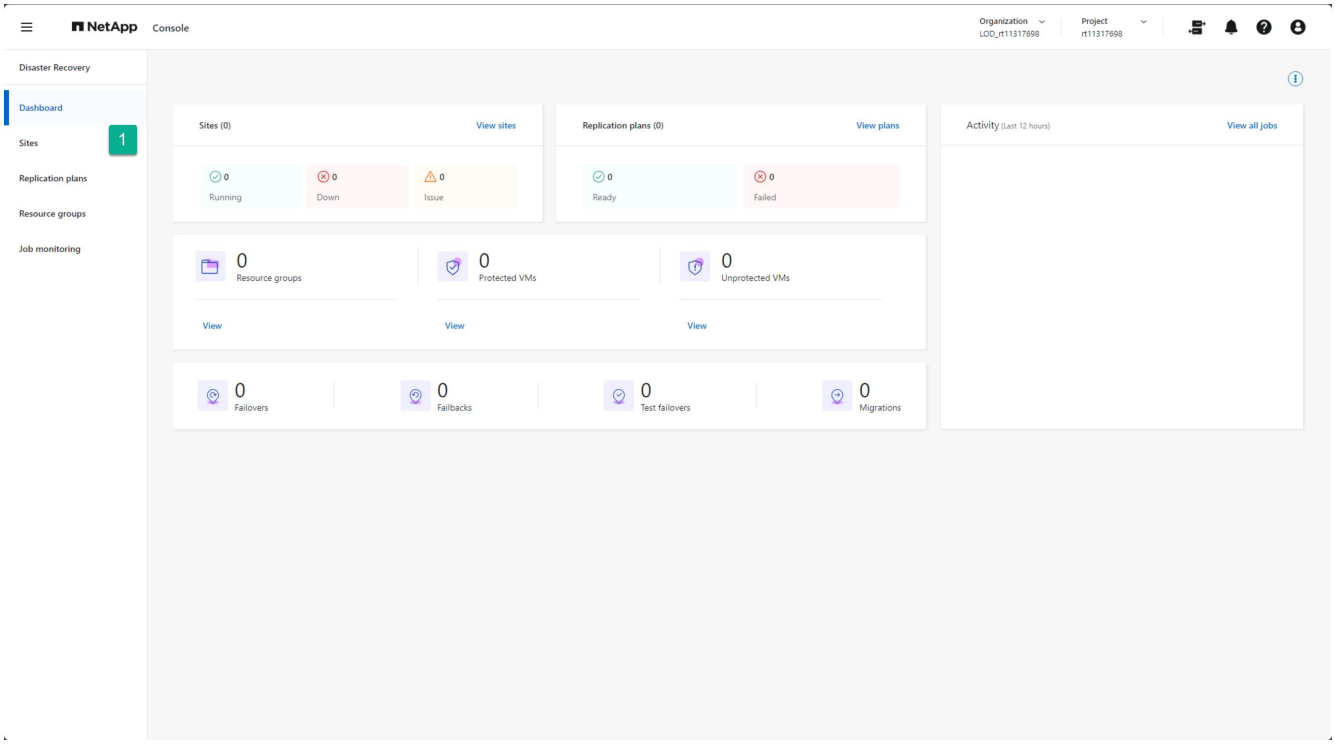


Se você tiver outros sites de produção do vCenter, poderá adicioná-los usando as mesmas etapas.

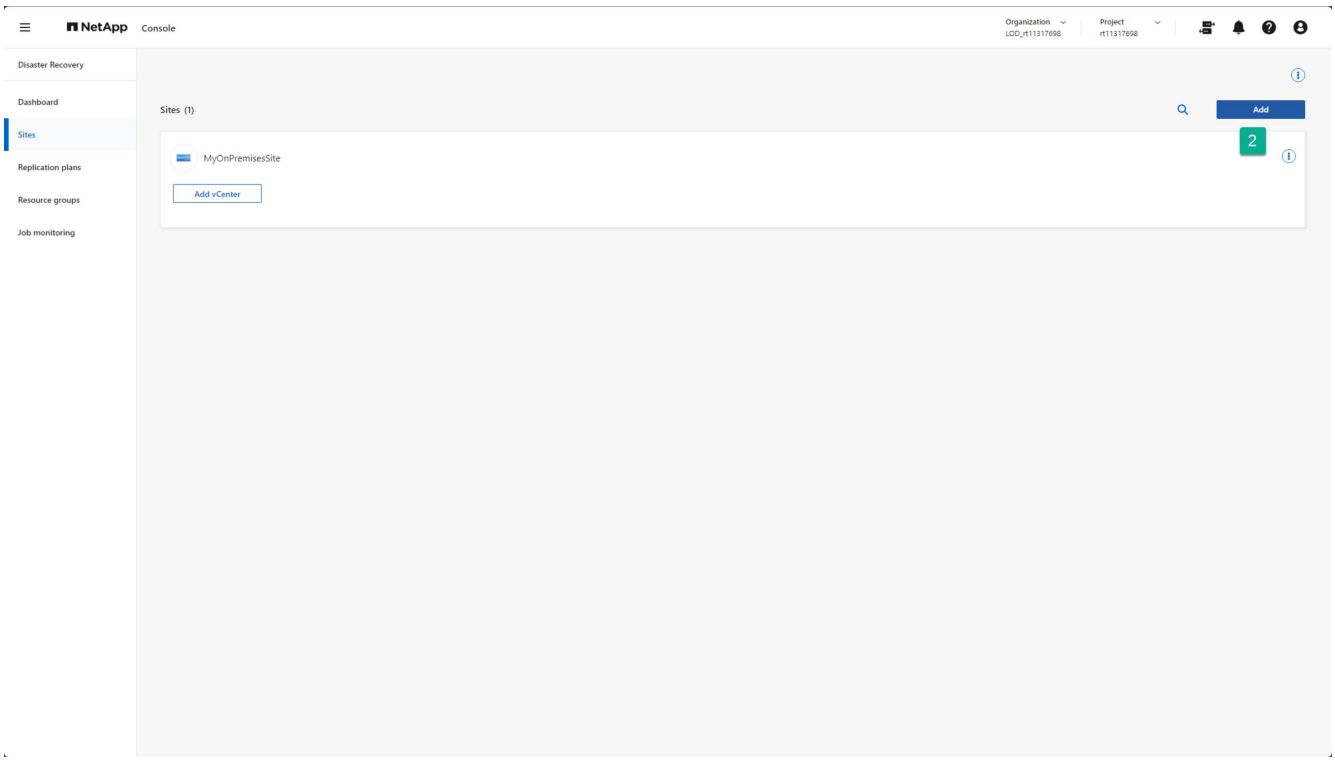
Crie sites na nuvem da Amazon

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**.

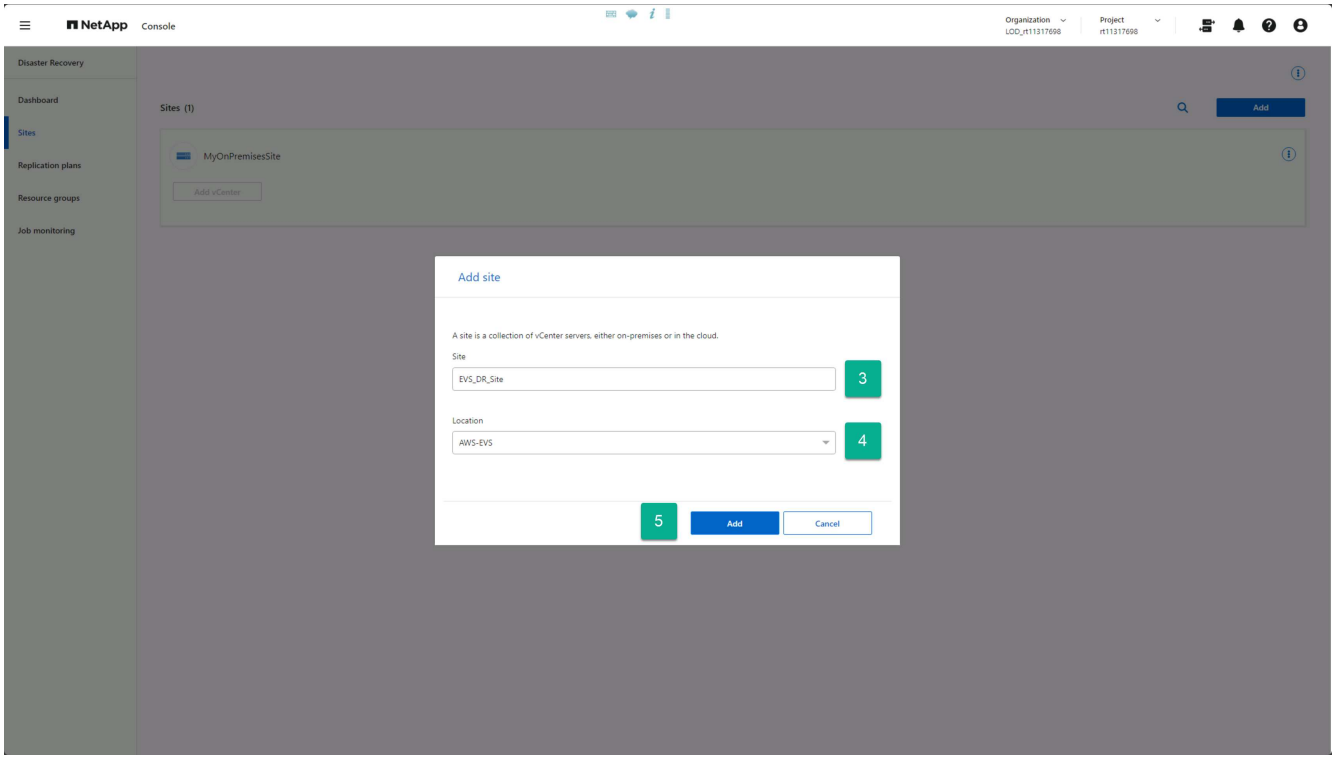


2. Na opção Sites, selecione **Adicionar**.



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

4. Selecione "AWS-EVS" como Local.
5. Selecione **Adicionar**.



Resultado

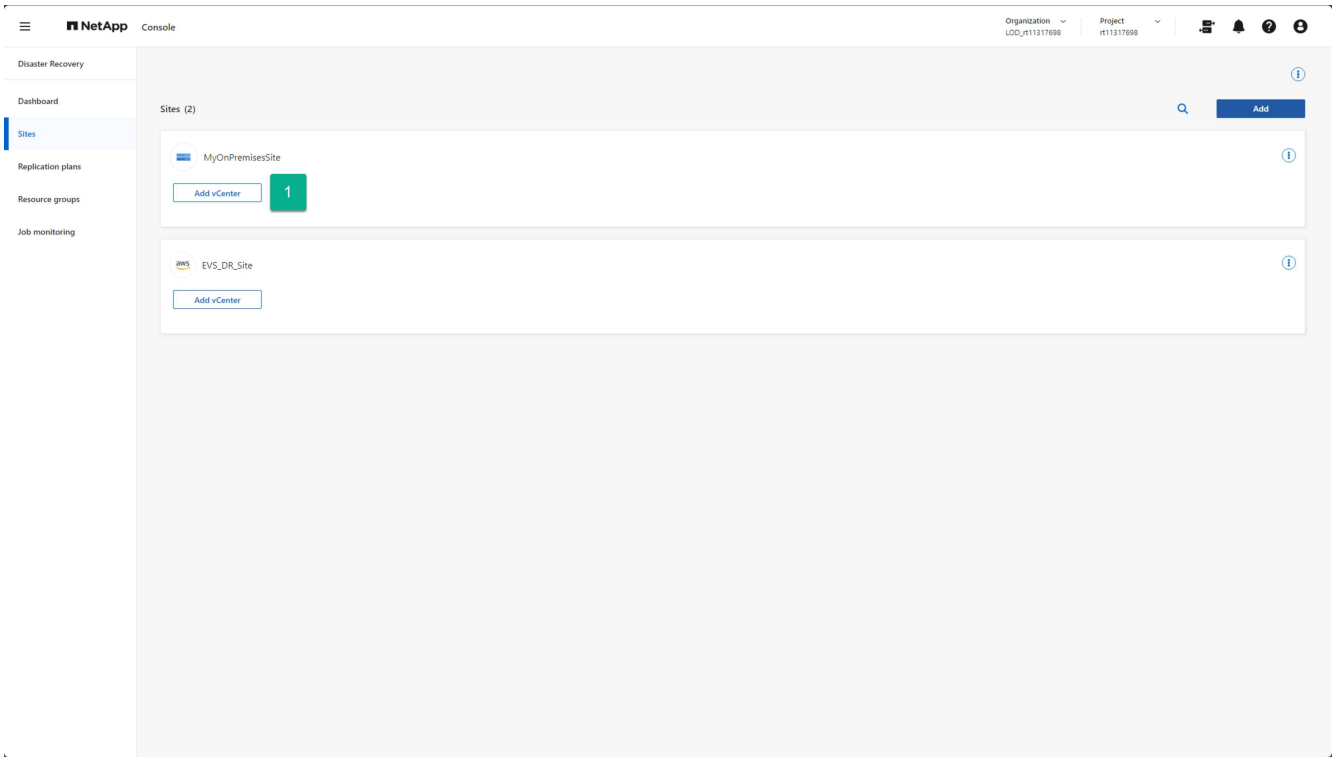
Agora você tem um site de produção (origem) e um site de DR (destino) criados.

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

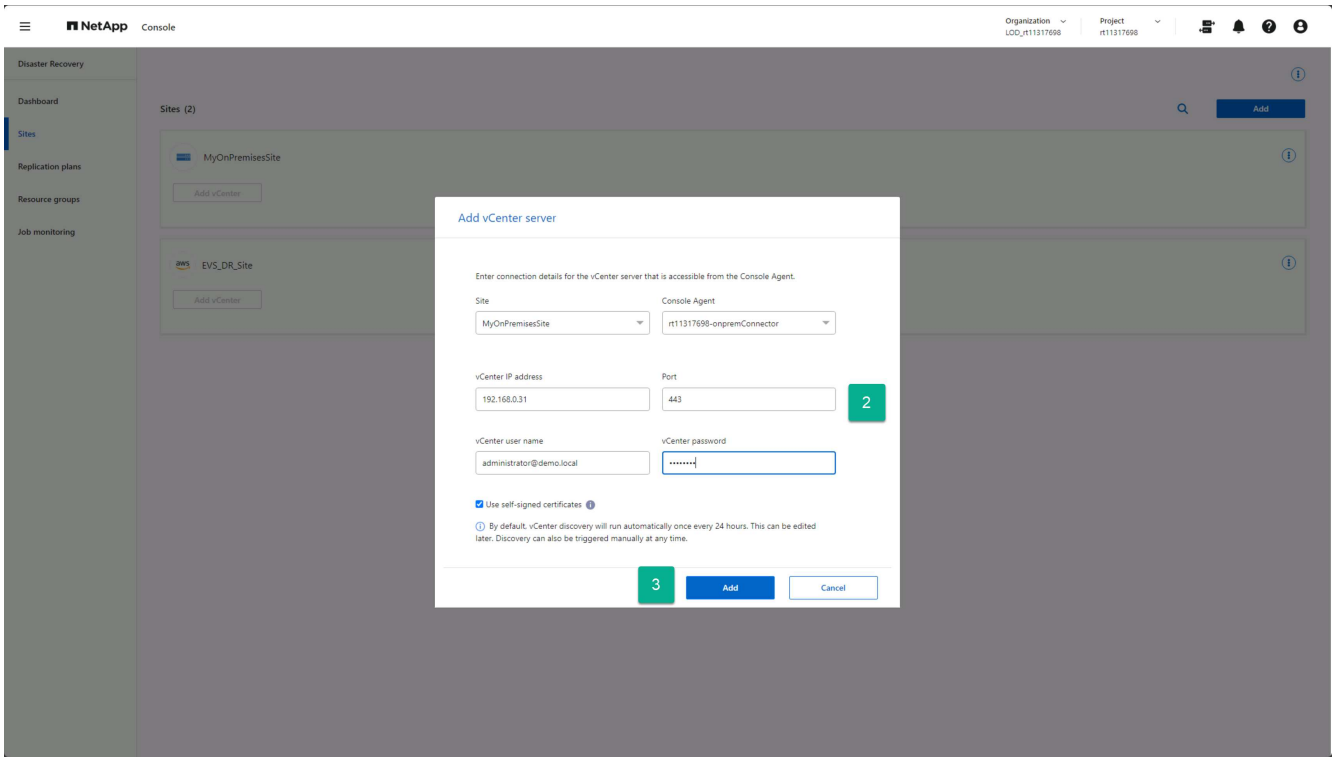
Com os sites criados, agora você adiciona seus clusters do vCenter a cada site no NetApp Disaster Recovery. Quando criamos cada site, indicamos cada tipo de site. Isso informa ao NetApp Disaster Recovery qual tipo de acesso é necessário para os vCenters hospedados em cada tipo de site. Uma das vantagens 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.



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**.



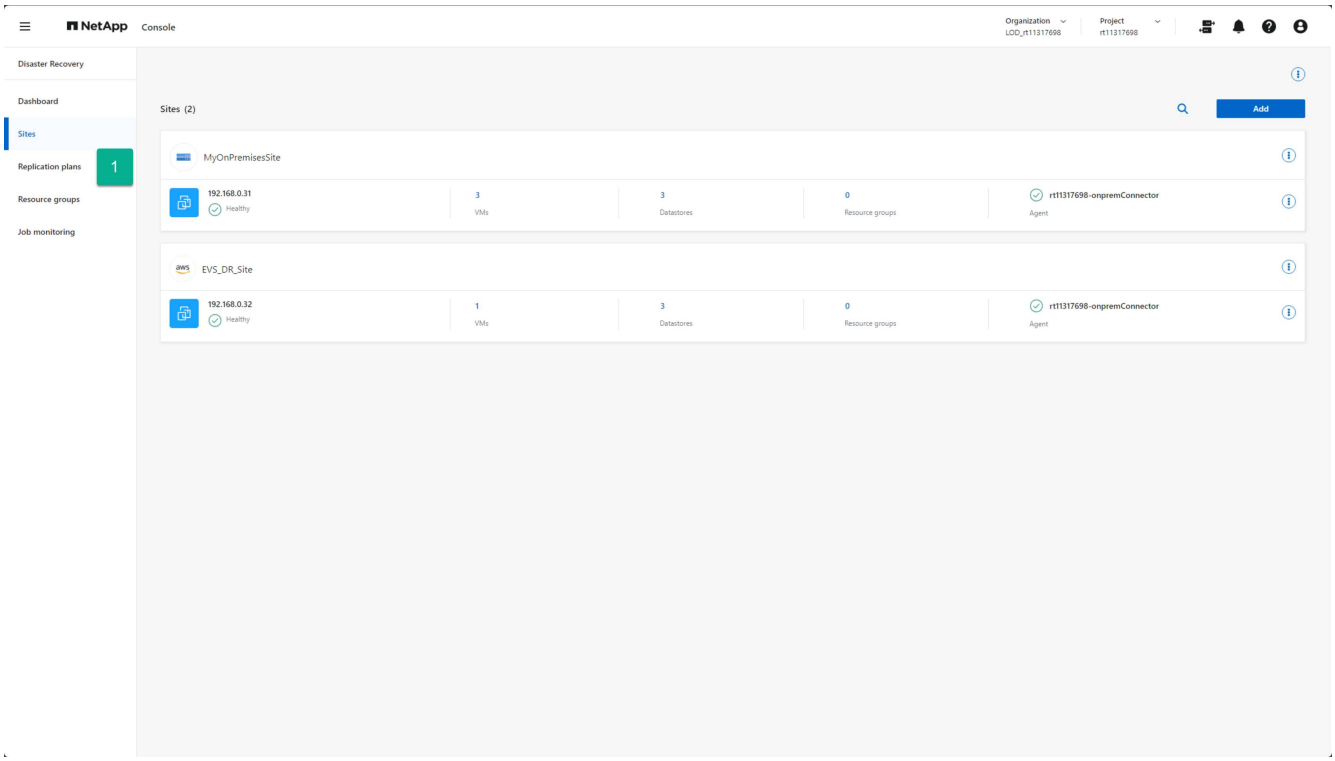
Crie planos de replicação para o Amazon EVS

Criar planos de replicação na visão geral do NetApp Disaster Recovery

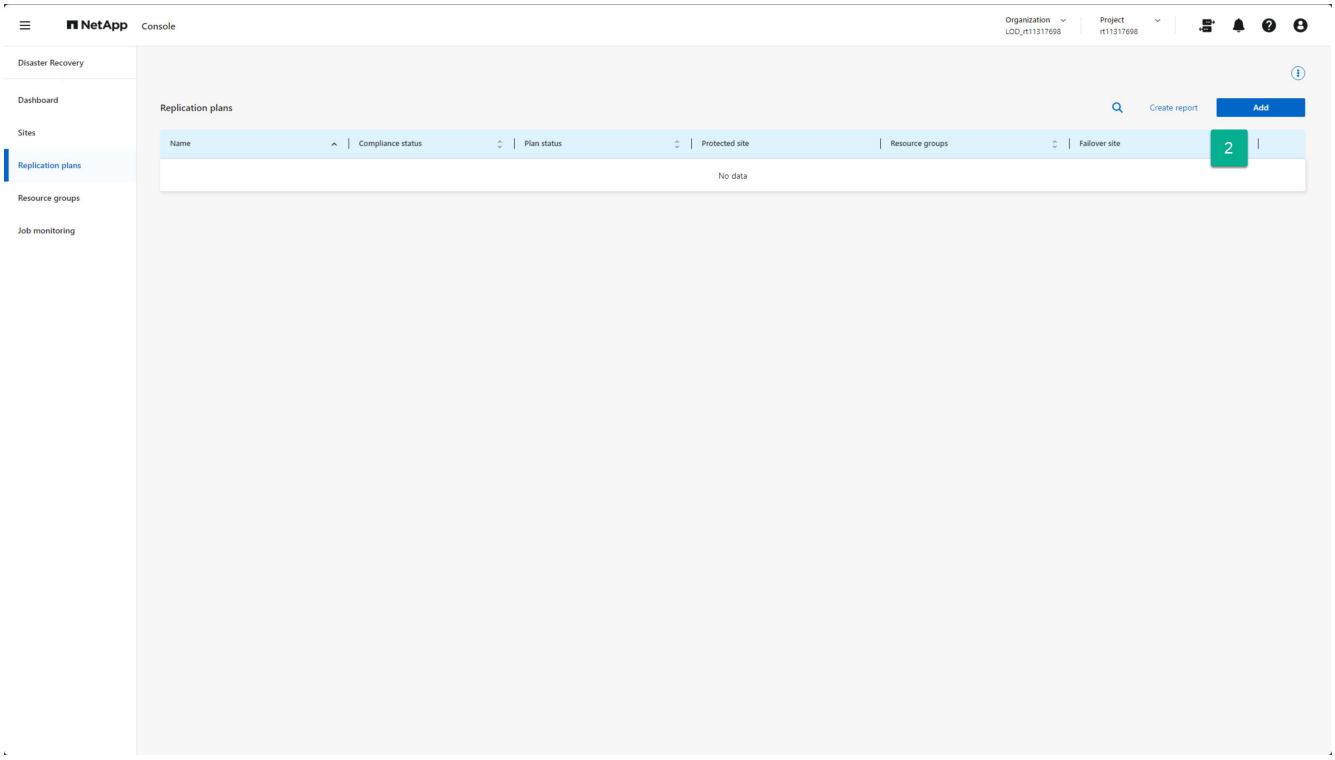
Depois de ter vCenters para proteger no site local e ter um site Amazon EVS configurado para usar o Amazon FSx for NetApp ONTAP que você pode usar como um destino de DR, você pode criar um plano de replicação (RP) para proteger qualquer conjunto de VMs hospedadas no cluster vCenter dentro do seu site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



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



Isso abre o assistente Criar plano de replicação.

Continuar com"Assistente para criação de plano de replicação Etapa 1" .

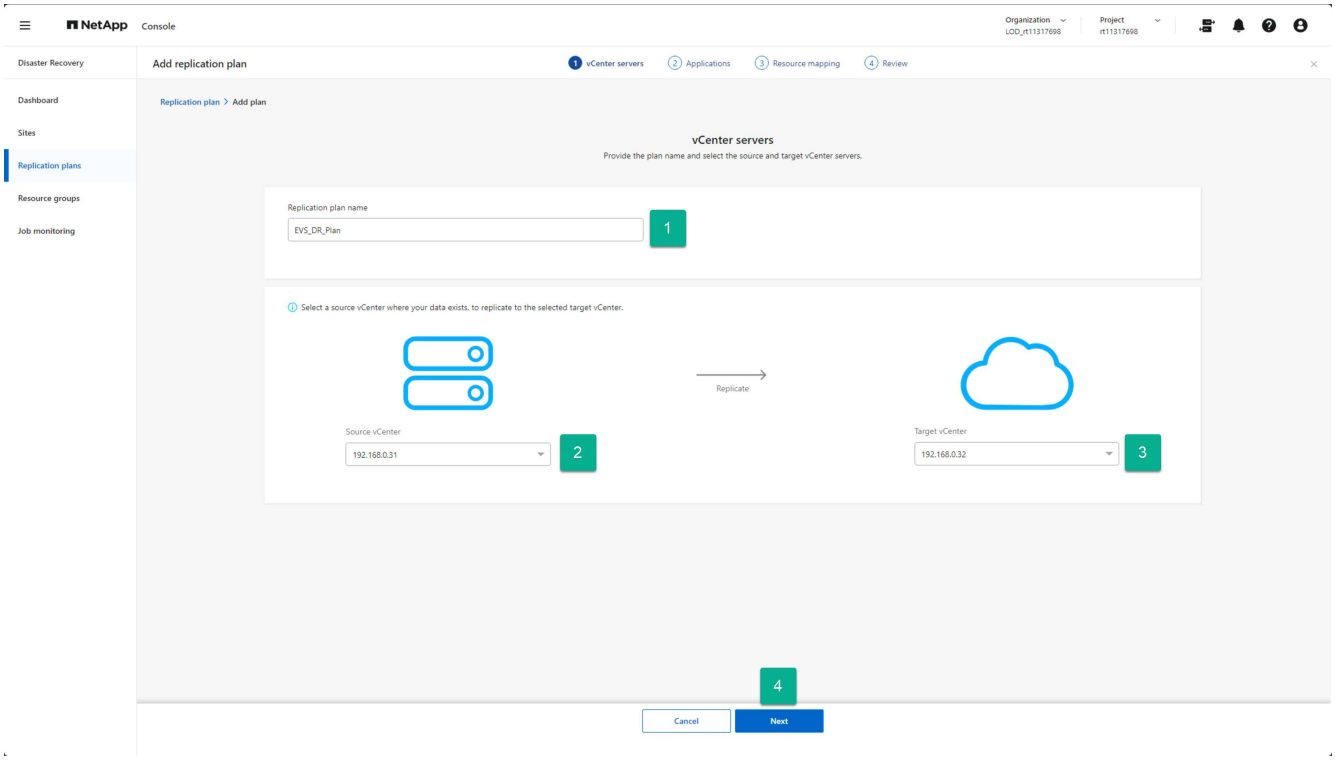
Crie um plano de replicação: Etapa 1 - Selecione vCenters no NetApp Disaster Recovery

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:

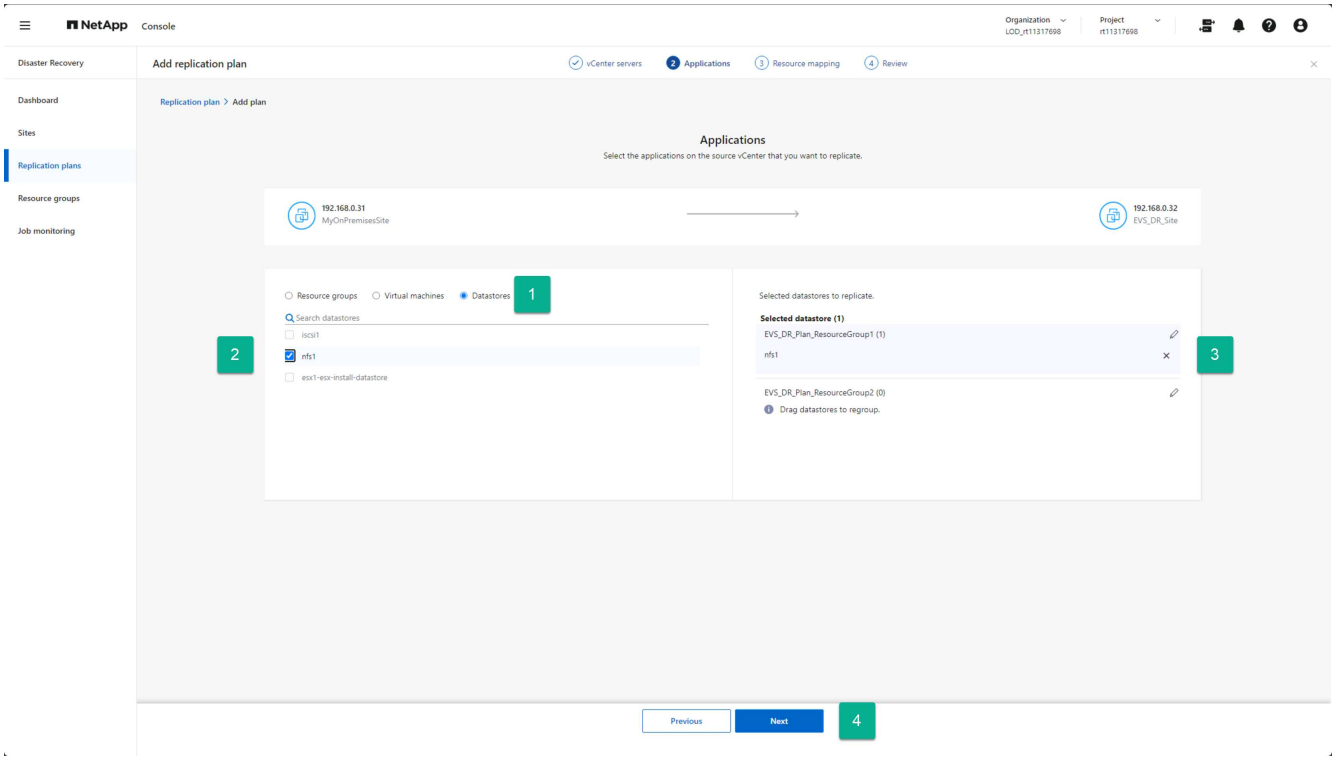
- **Selecionar VMs individuais**: clicar no botão **Máquinas virtuais** permite que você selecione VMs individuais para proteger. Conforme você seleciona cada VM, o serviço a adiciona a um grupo de recursos padrão localizado no lado direito da tela.
- **Selecionar grupos de recursos criados anteriormente**: 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

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



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

1. Selecione **Datastores**.
2. Marque as caixas de seleção ao lado de cada armazenamento de dados que você deseja proteger.
3. (Opcionalmente) Renomeie o grupo de recursos para um nome adequado selecionando o ícone de lápis ao lado do nome do grupo de recursos.
4. 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:

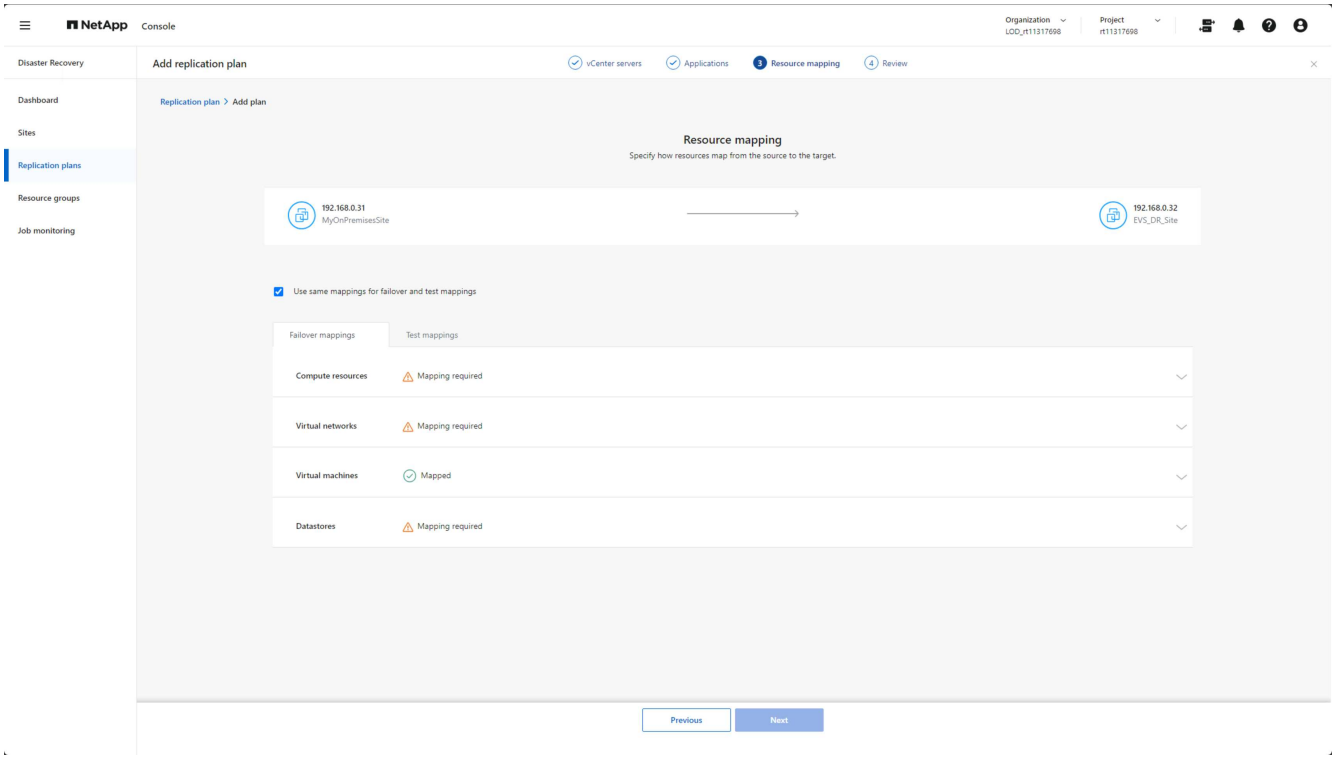
- Recursos de computação
- Redes virtuais
- Reconfiguração de VM
- Mapeamento de armazenamento de dados

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 (**v**) 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.

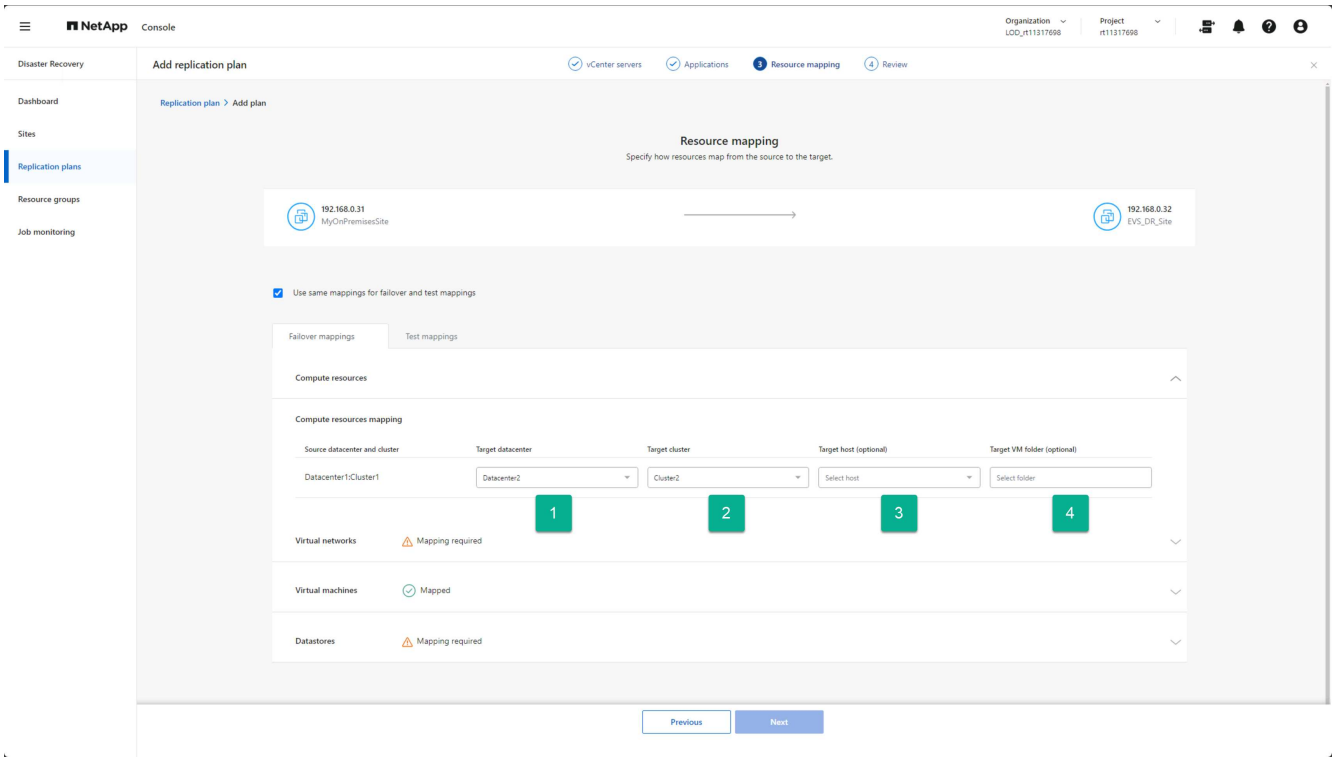
Etapas para mapear recursos de computação

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.

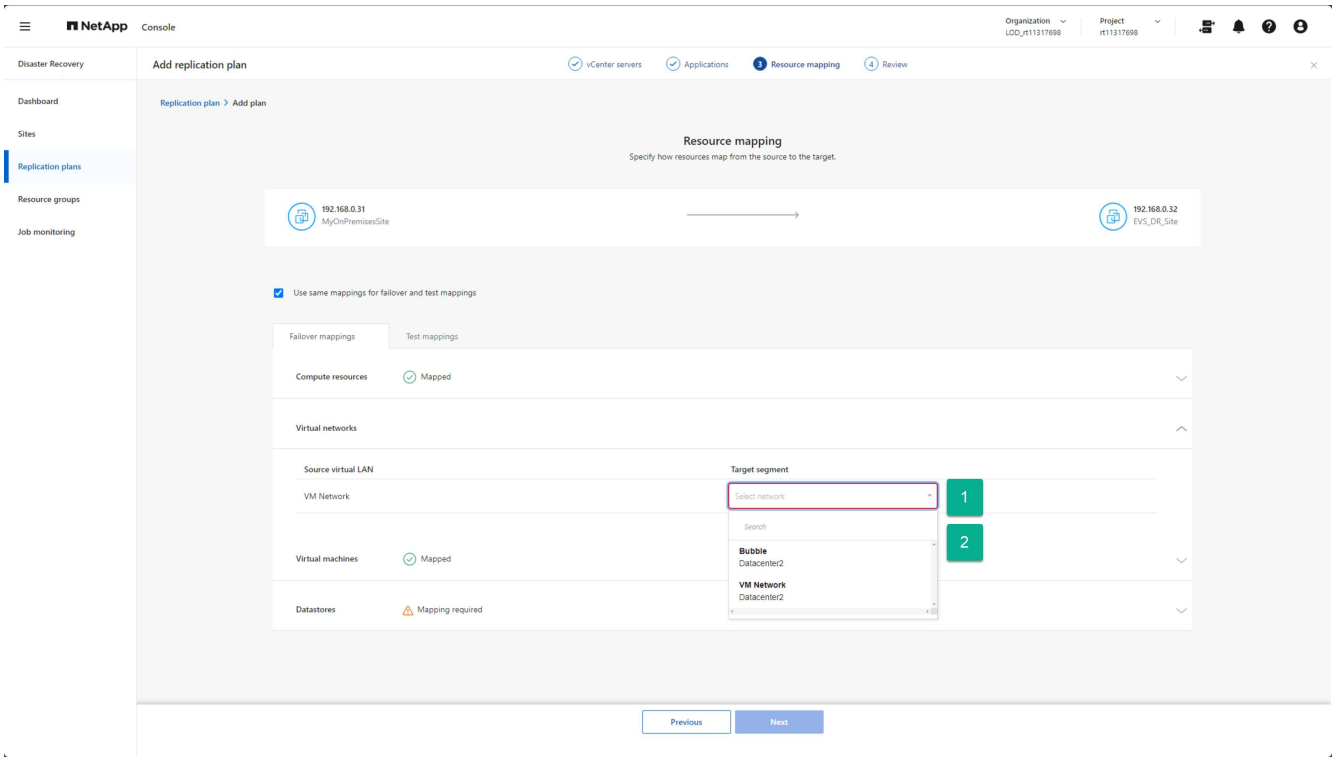


Mapear recursos de rede virtual

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.

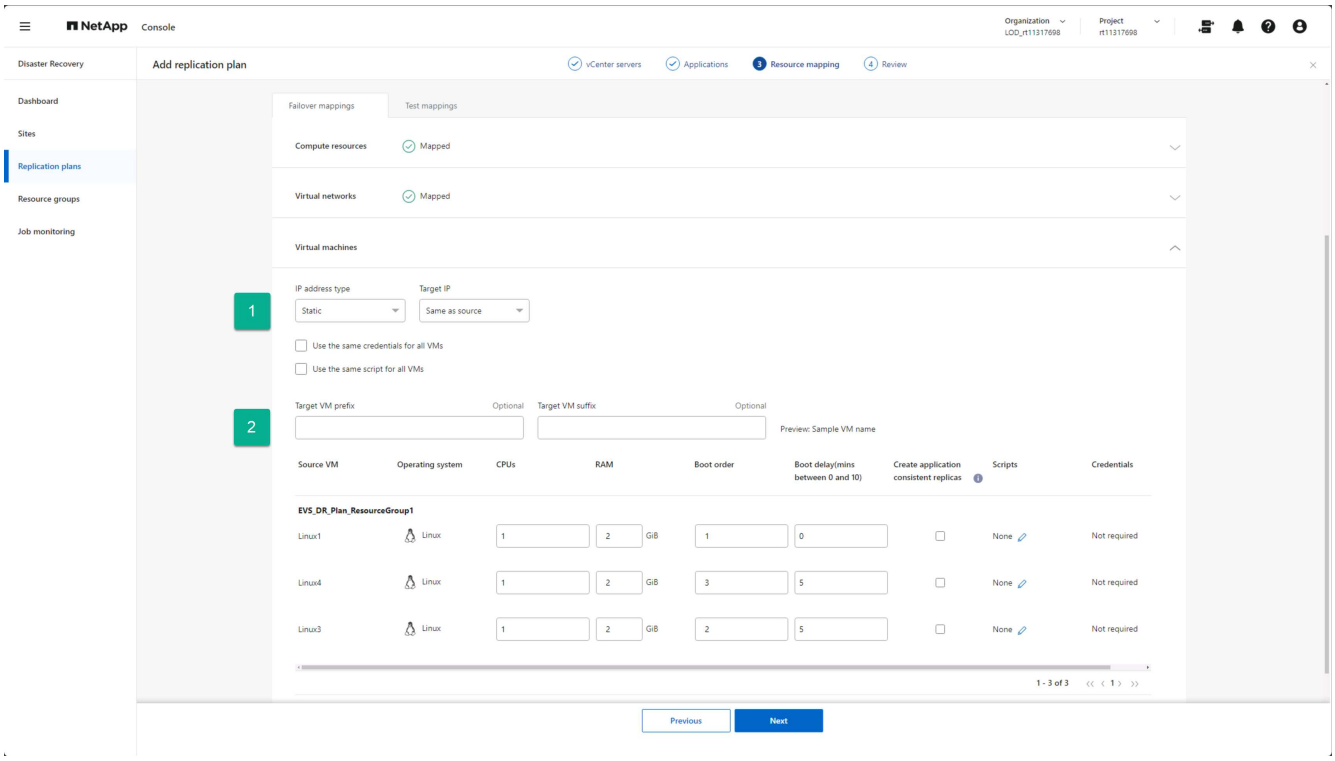
Depois de configurar sub-redes, o mapeamento de sub-redes usa o mesmo componente de unidade do endereço IP para a configuração da VM de origem e de destino, mas substitui o componente de sub-rede do

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.

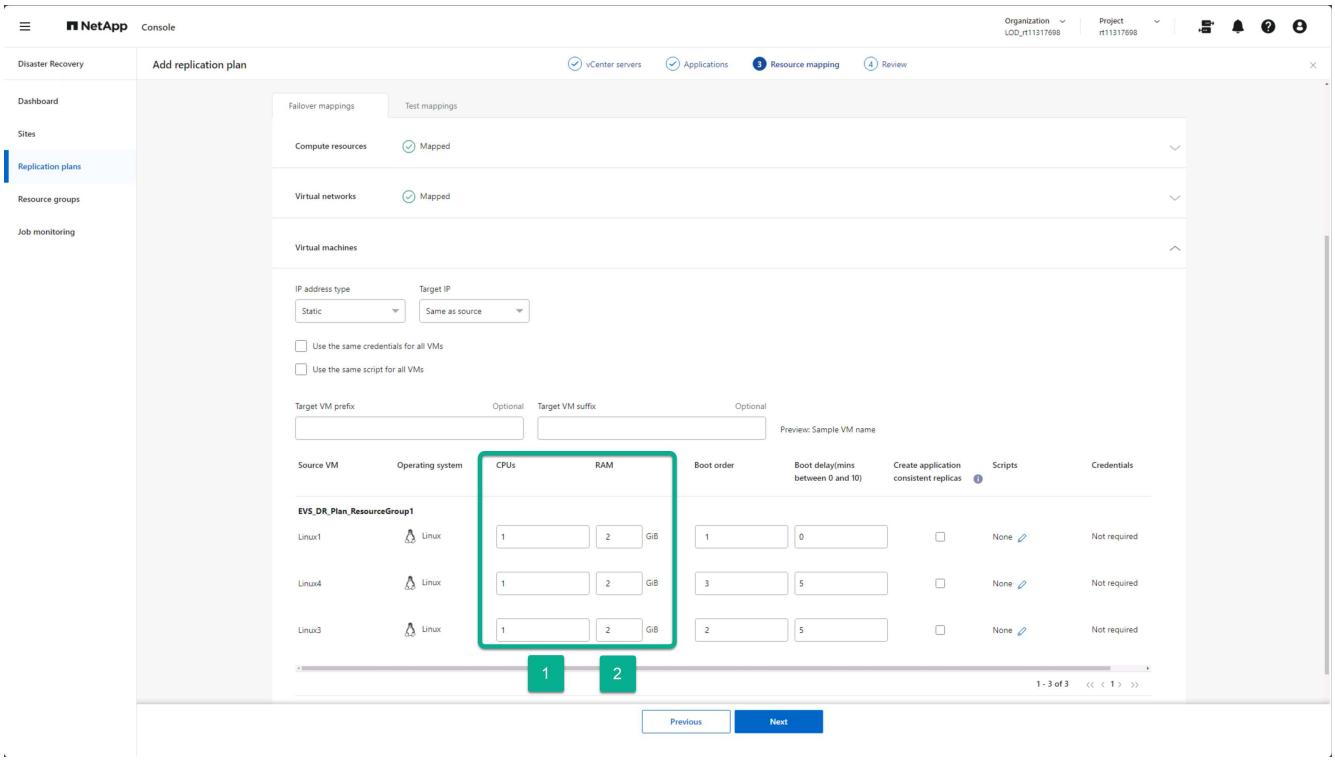


Reconfiguração de recursos de computação de VM

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.

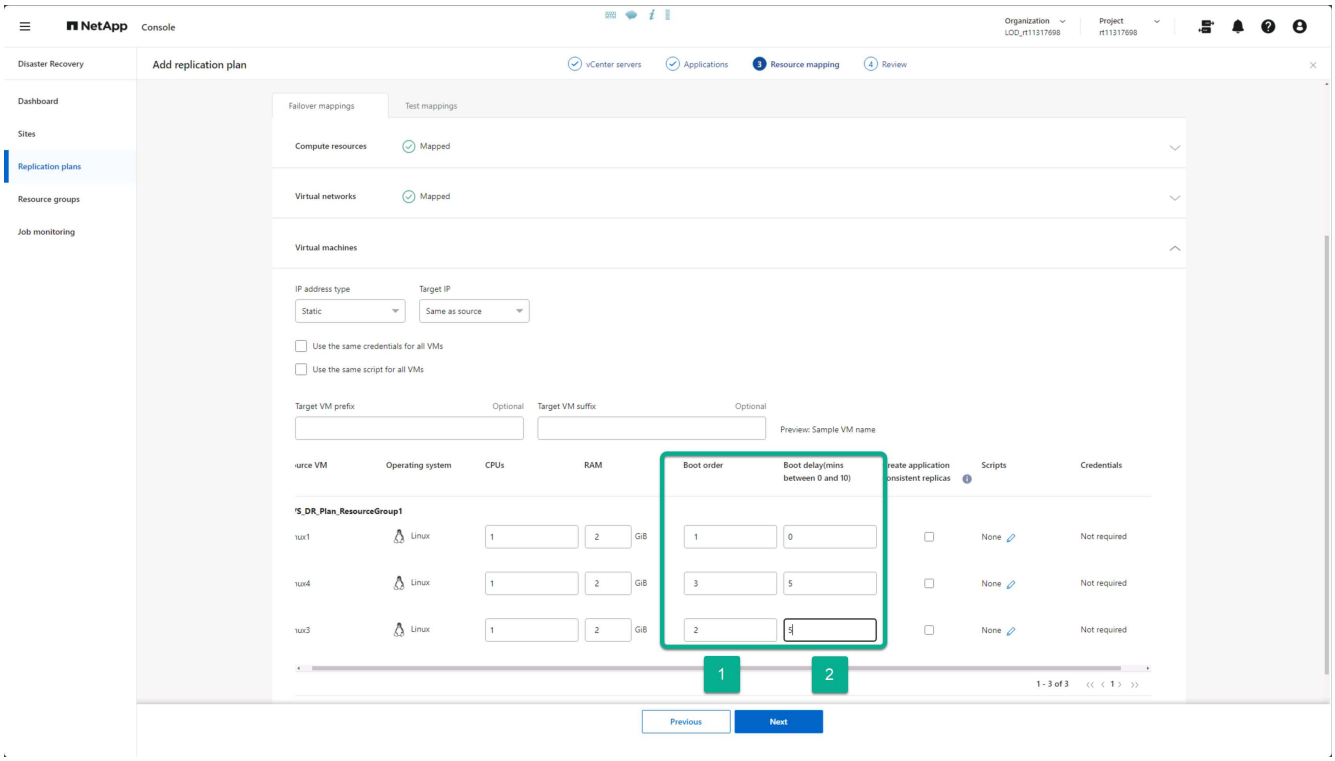


Ordem de inicialização

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

1. (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.
2. (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.



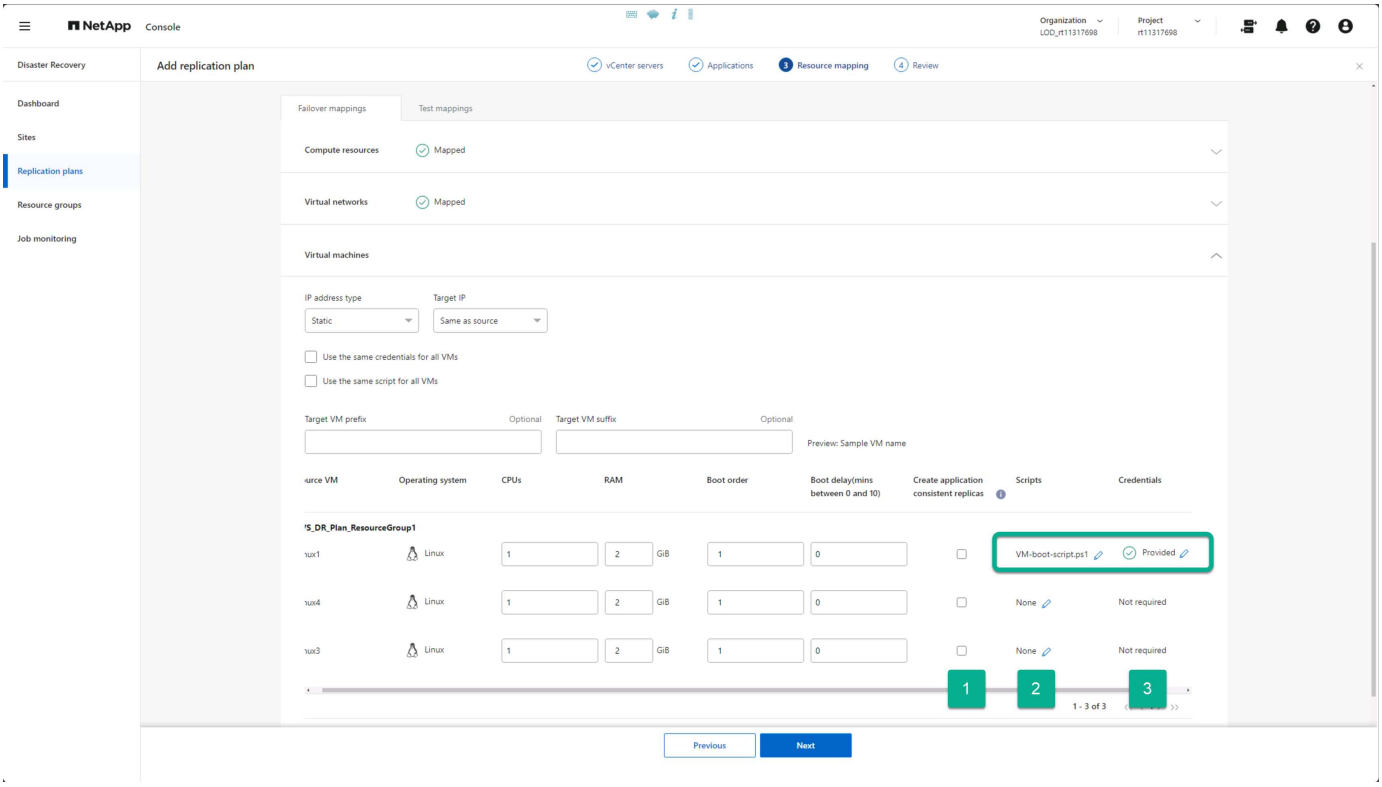
Operações personalizadas do sistema operacional convidado

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.

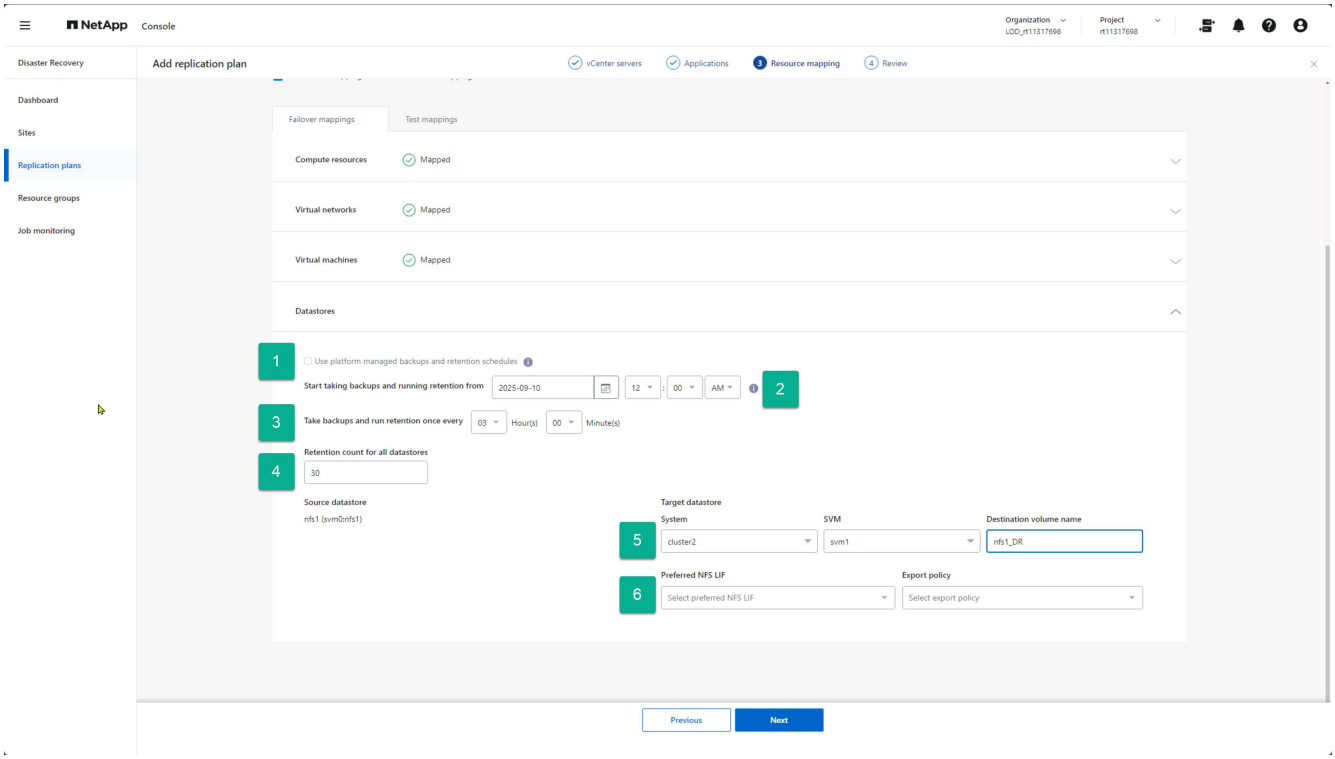
Por padrão, o NetApp Disaster Recovery gerencia seu próprio agendamento de replicação de snapshots; no entanto, opcionalmente, você pode especificar que gostaria de usar o agendamento de política de replicação existente do SnapMirror para proteção do repositório de dados.

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)

1. (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).
2. Forneça um ponto de partida para quando o serviço deve começar a fazer backups.
3. Especifique com que frequência o serviço deve fazer um backup e replicá-lo no cluster Amazon FSx for NetApp ONTAP de destino de DR.
4. Especifique quantos backups históricos devem ser mantidos. O serviço mantém o mesmo número de backups no cluster de armazenamento de origem e de destino.
5. (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.
6. (Opcional) Selecione uma política de exportação para qualquer volume NFS. Se não for selecionado, a

política de exportação padrão será usada



Continuar com"Assistente para criar plano de replicação Etapa 4" .

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

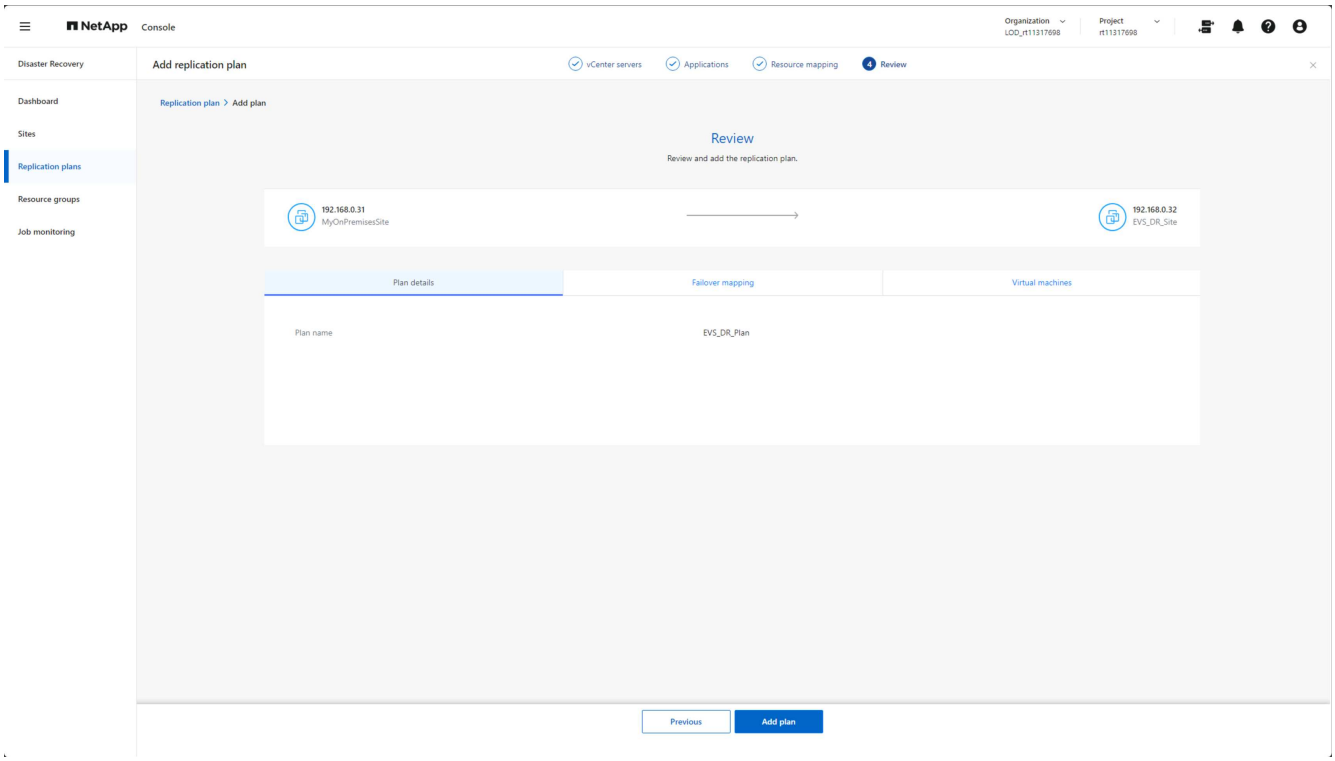
Depois de adicionar as informações do plano de replicação no NetApp Disaster Recovery, verifique se as informações inseridas estão corretas.

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



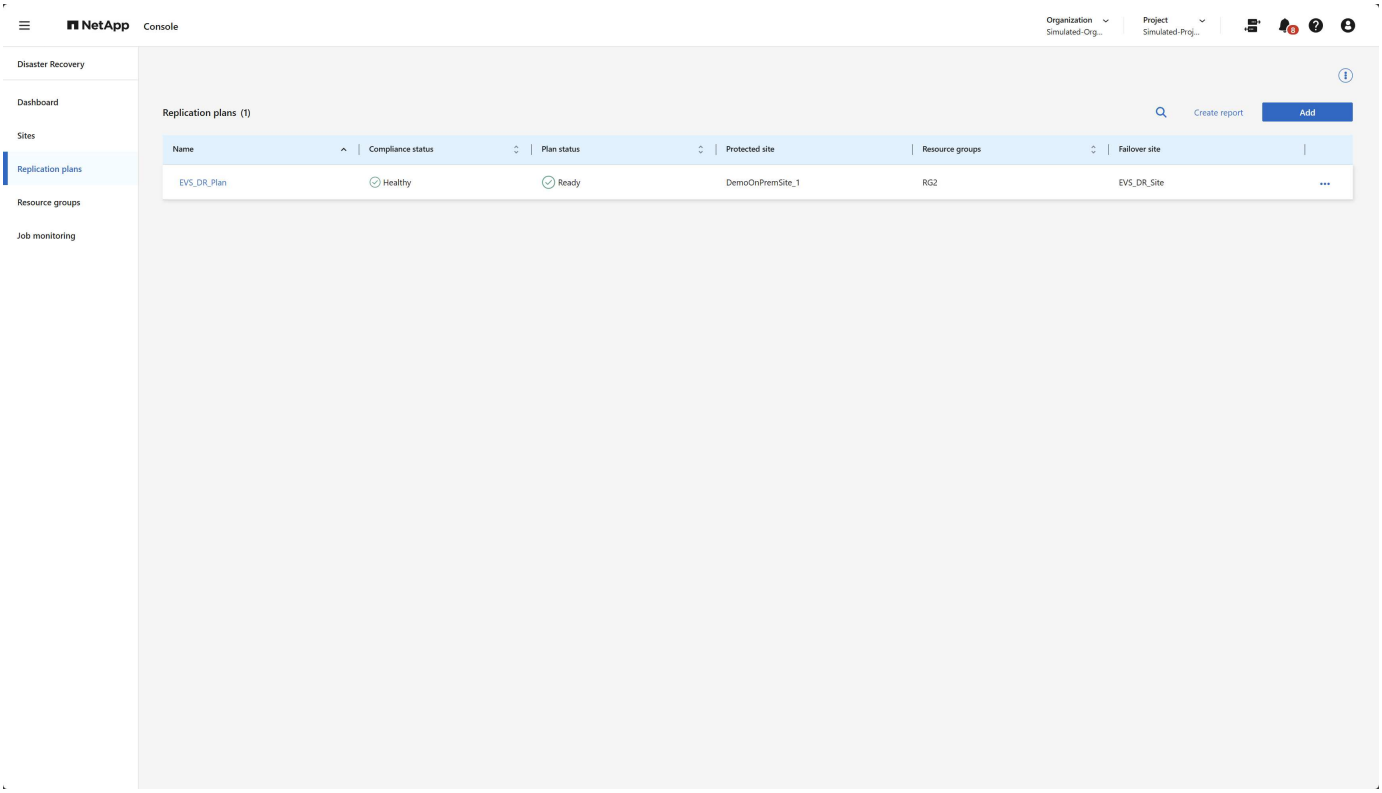
2. Quando estiver satisfeito com todas as configurações, selecione **Adicionar plano** na parte inferior da tela.

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



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.

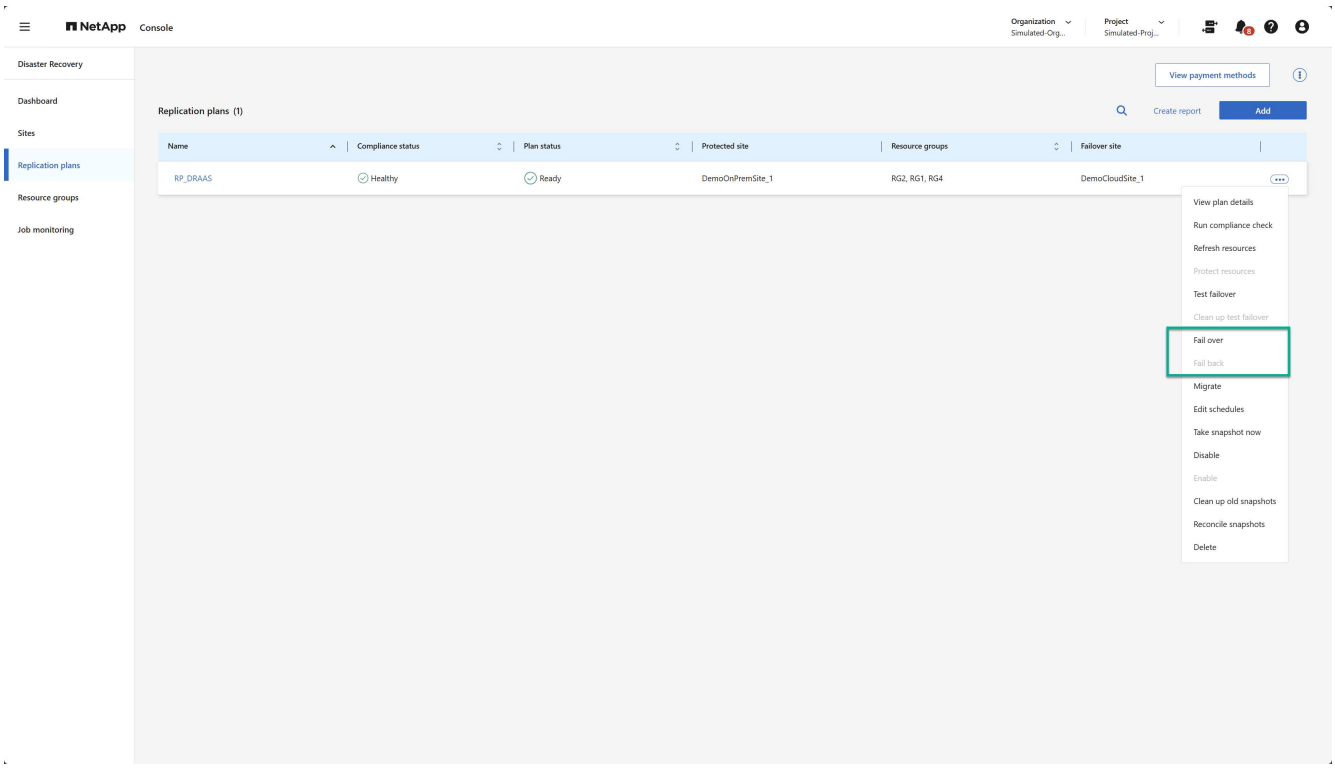
O failover é um processo iniciado manualmente.

Etapas para acessar a operação de failover

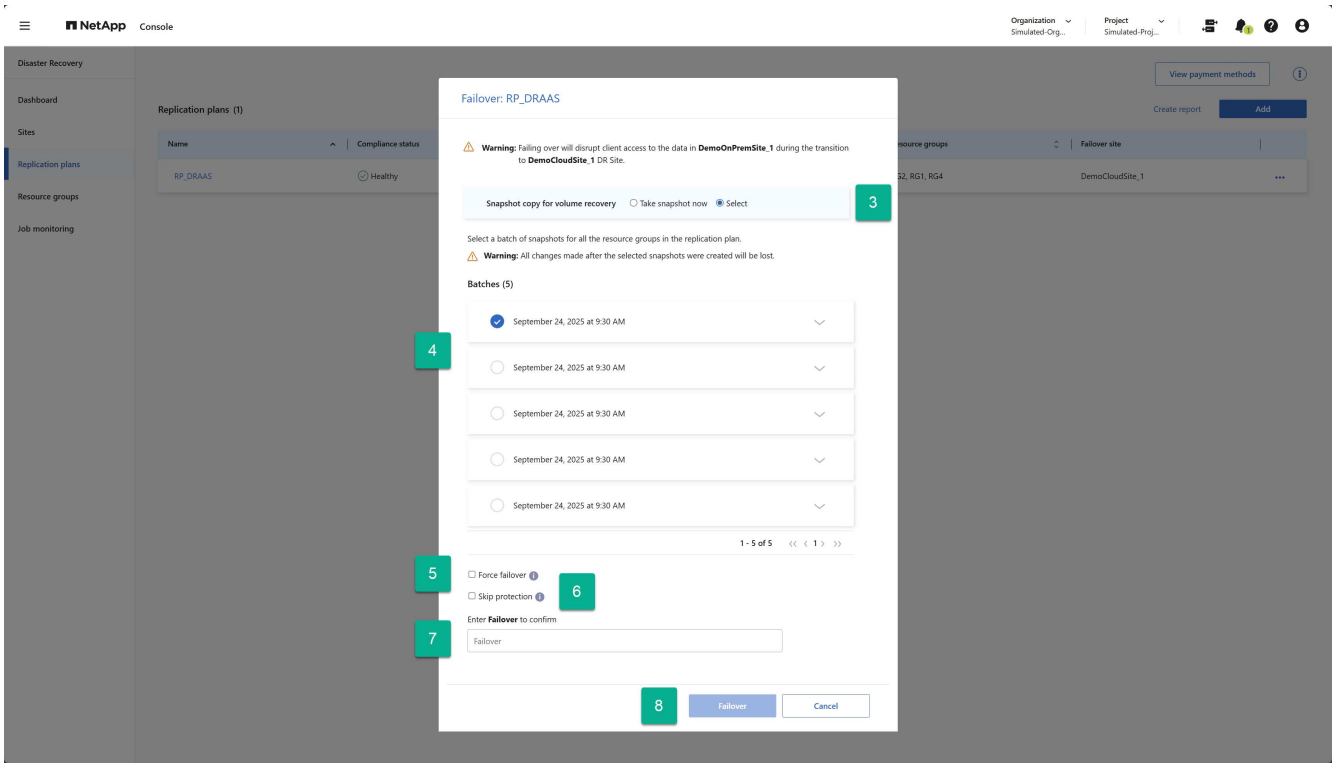
1. Na barra de navegação esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.
2. No menu NetApp Disaster Recovery , selecione **Planos de replicação**.

Etapas para executar um failover

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



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.

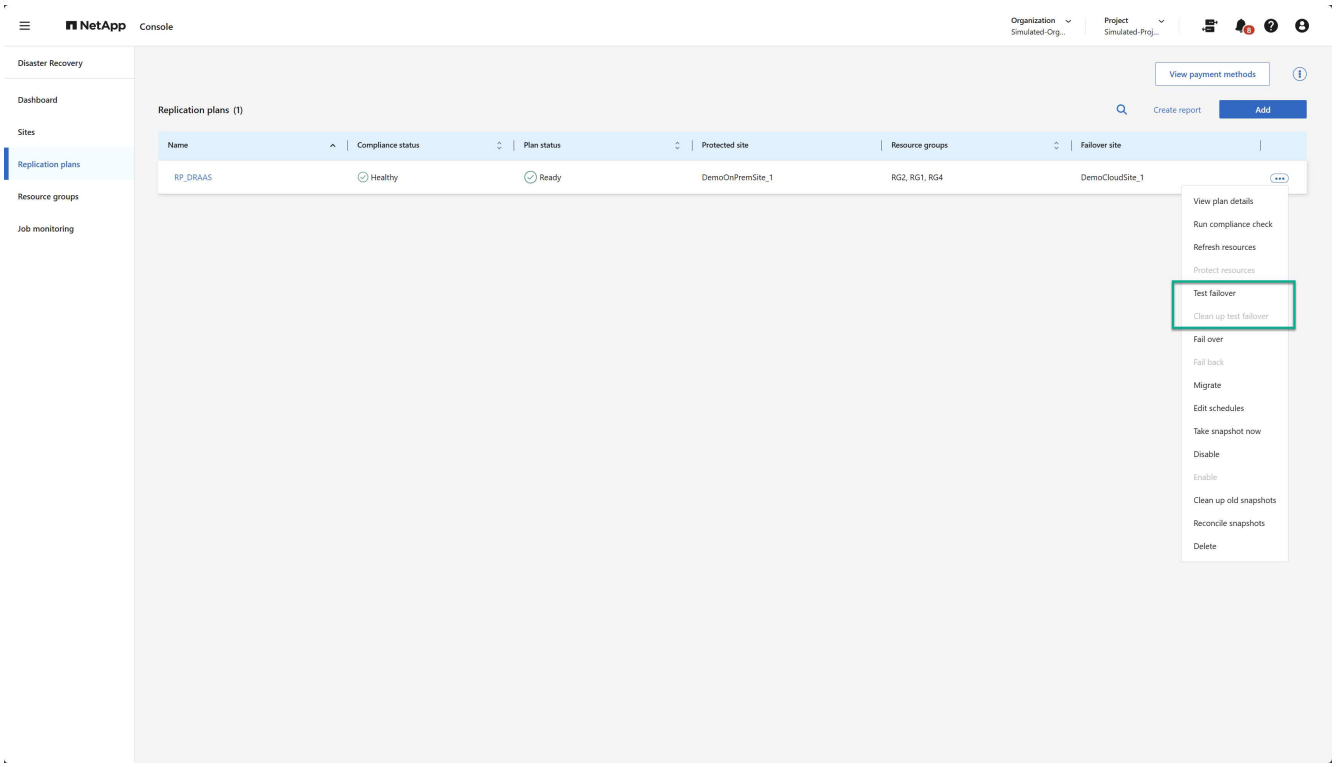
- O site de produção ainda está ativo e todas as VMs continuam operando conforme o esperado.
- A proteção do NetApp Disaster Recovery das VMs de produção continua.

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" .

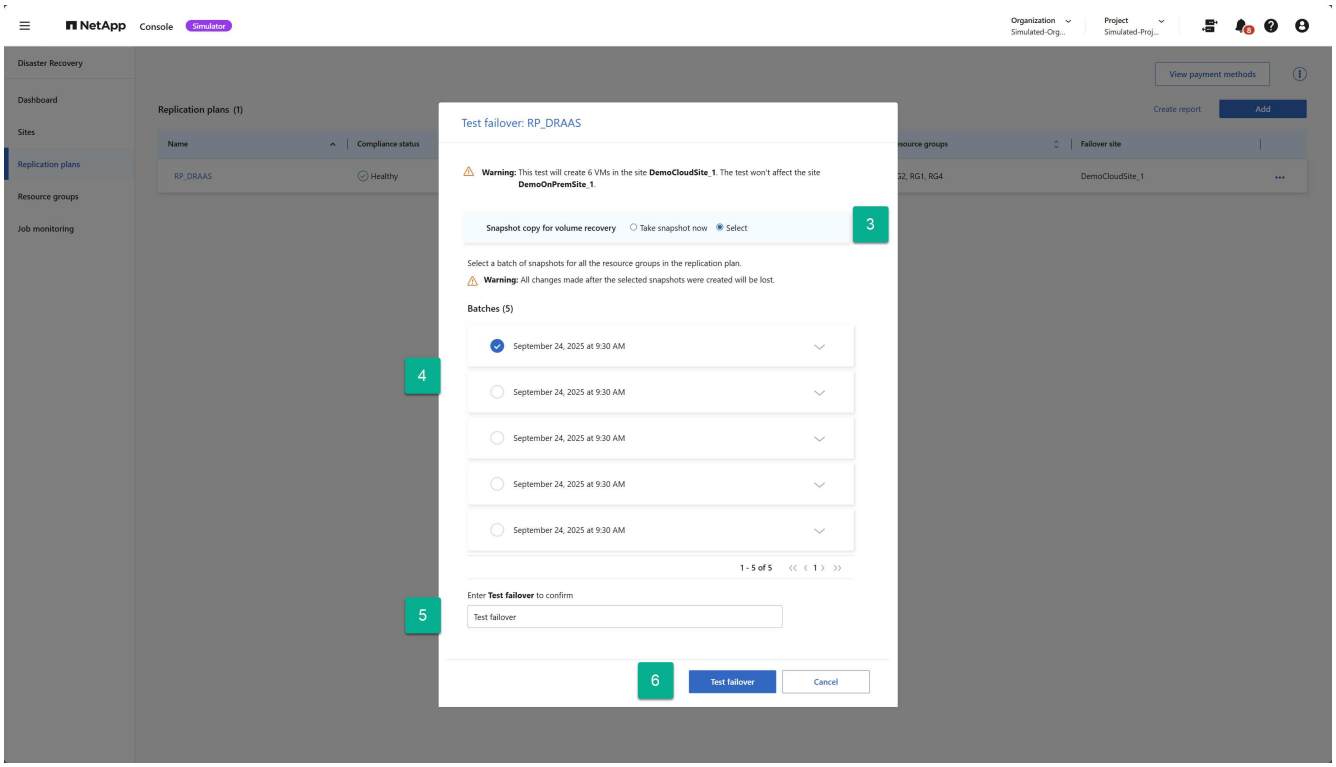
As etapas para executar um failover de teste são idênticas às usadas para executar um failover real, exceto que você usa a operação Test failover no menu de contexto do plano de replicação.

Passos

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



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**.

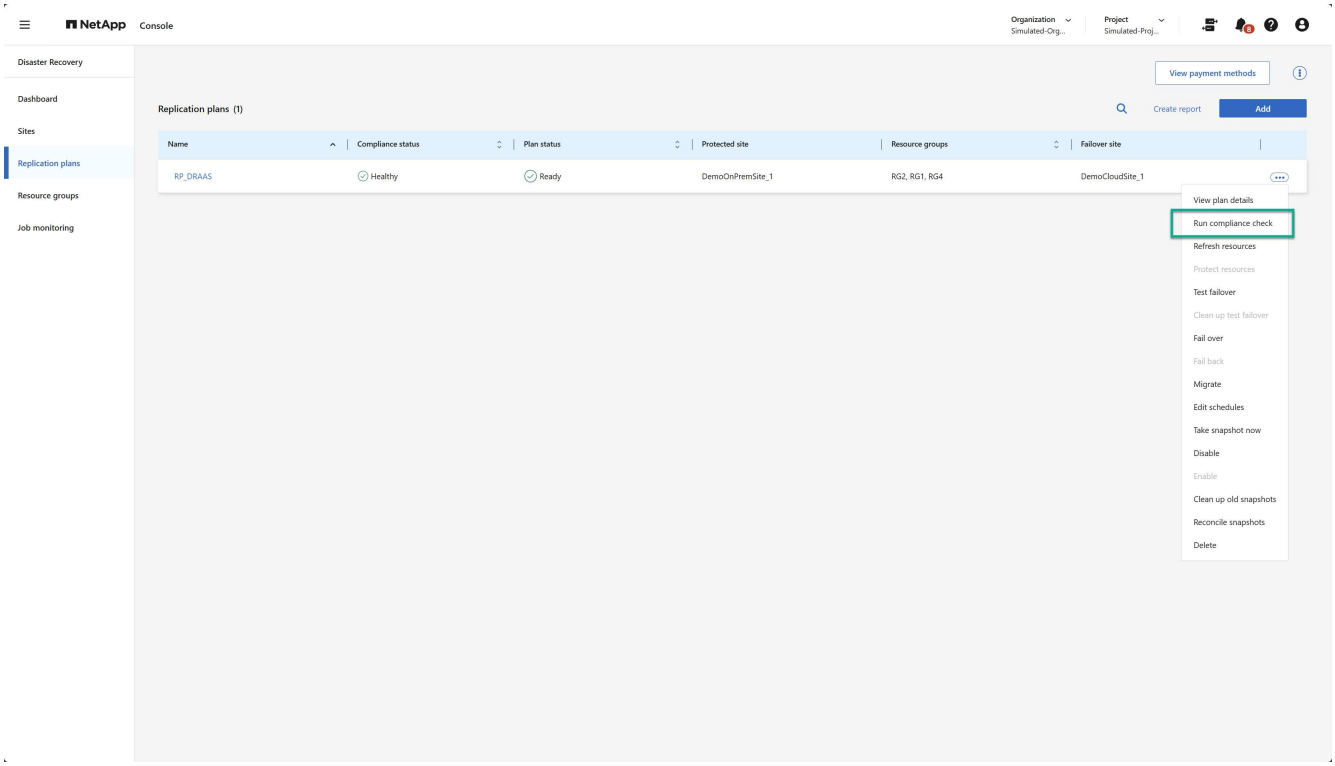


Execute uma verificação de conformidade

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:



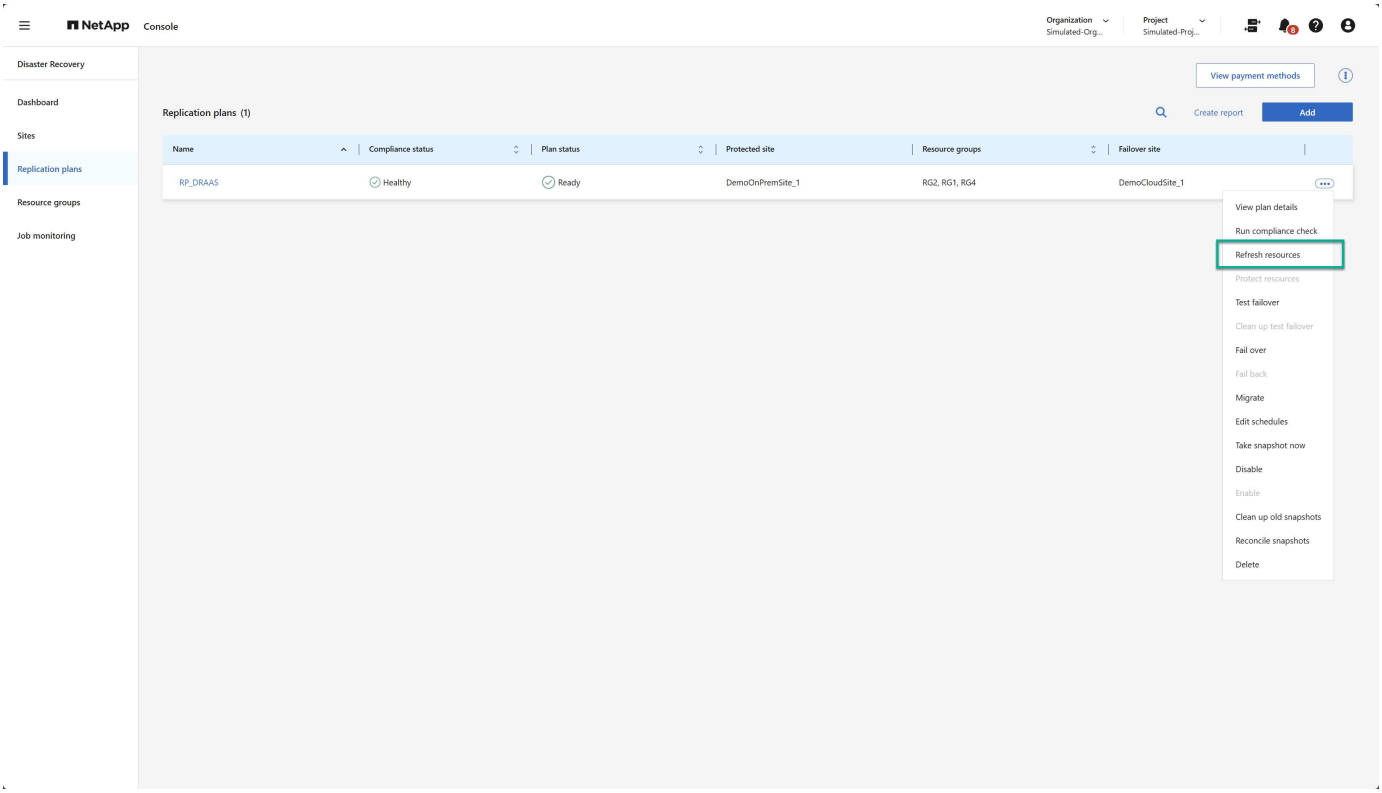
3. Para alterar a frequência com que o NetApp Disaster Recovery executa verificações de conformidade automaticamente, selecione a opção **Editar agendamentos** no menu Ações do plano de replicação.

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:

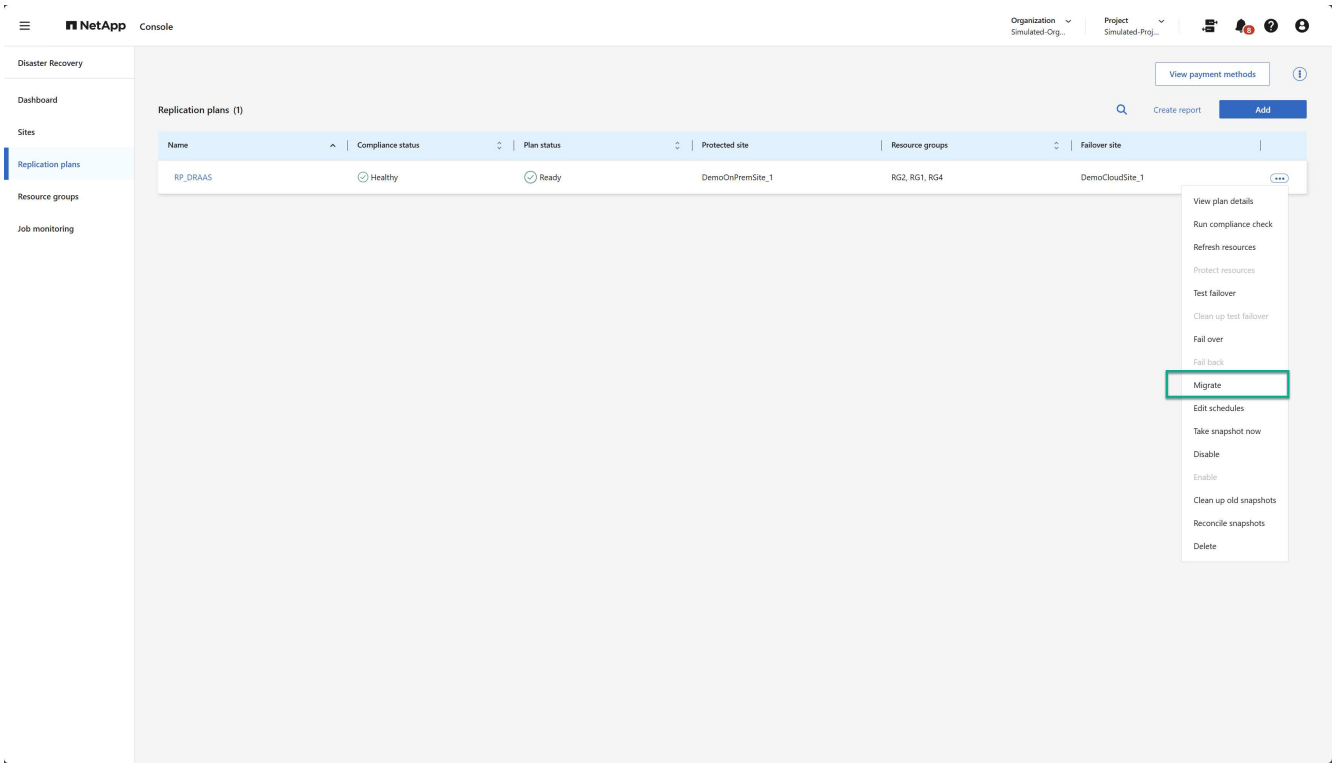
- Atualização do vCenter: execute uma atualização do vCenter sempre que VMs forem adicionadas, excluídas ou movidas para fora de um cluster do vCenter:
- Atualização do plano de replicação: execute uma atualização do plano de replicação sempre que uma VM for movida entre armazenamentos de dados no mesmo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



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:

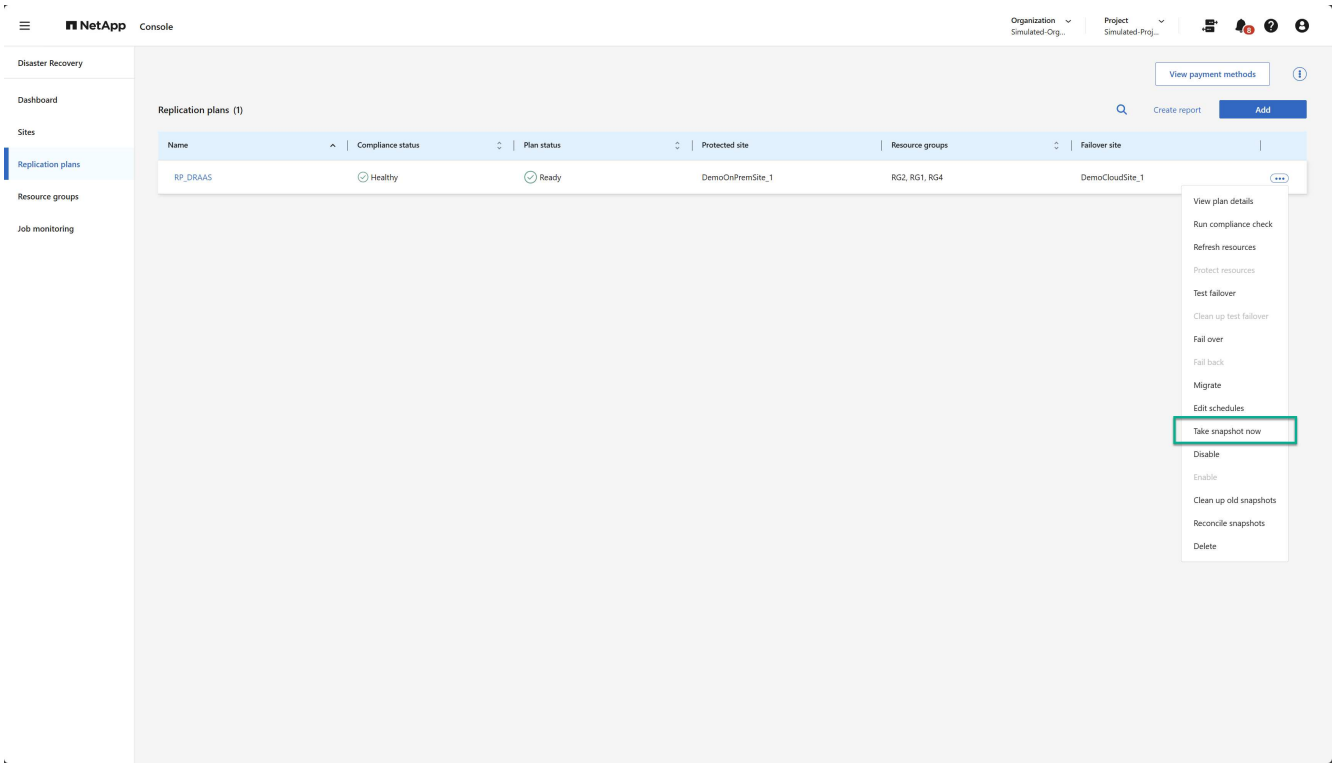


3. Insira informações na caixa de diálogo Migrar.

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:

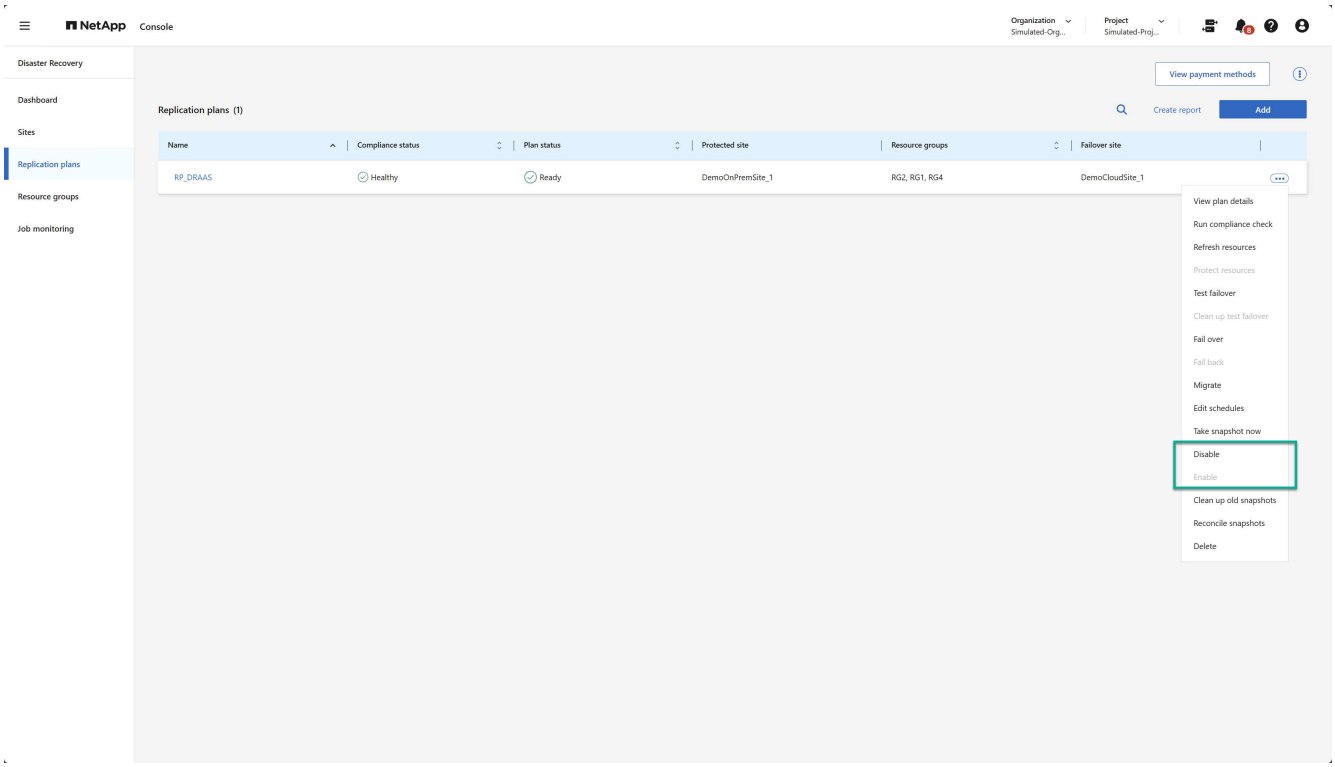


Desabilitar ou habilitar o plano de replicação

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.

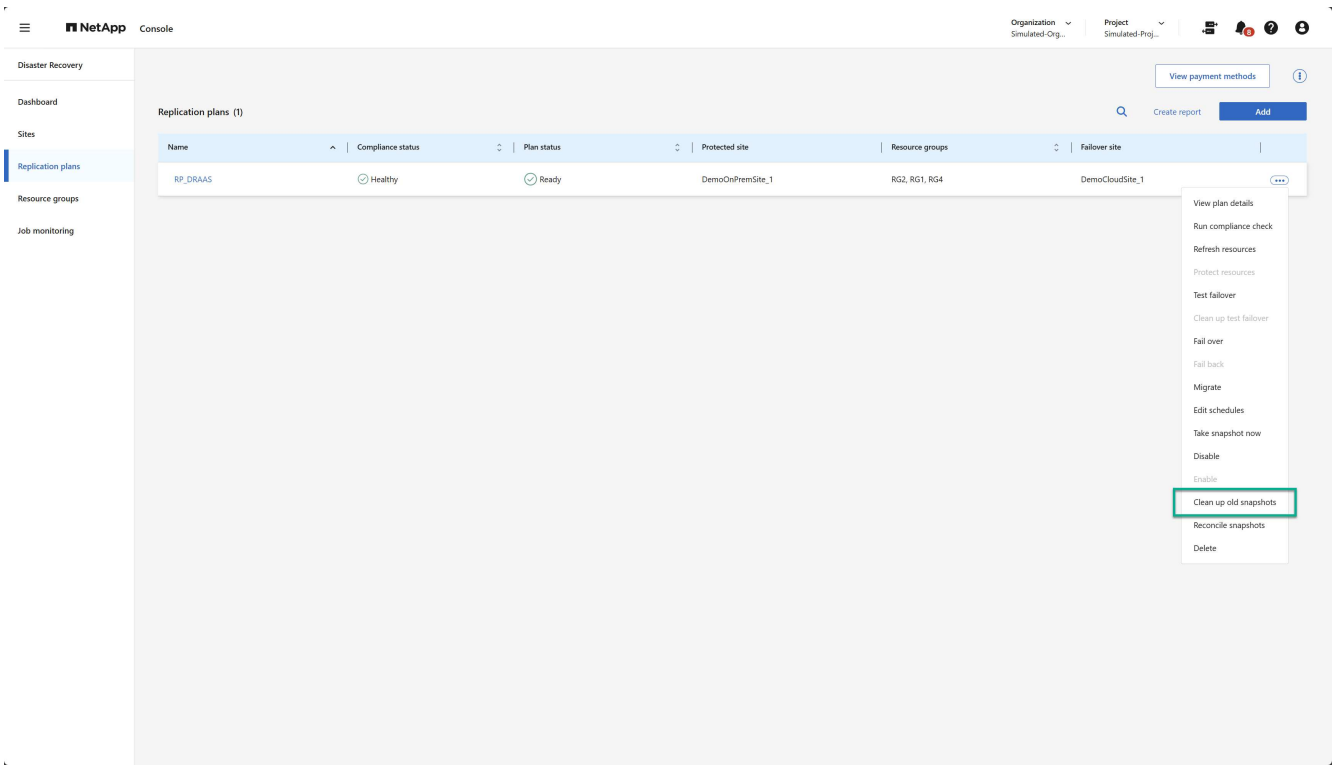
   Quando o plano de replicação está ativo, o comando **Ativar** fica esmaecido. Quando o plano de replicação é desabilitado, o comando **Desabilitar** fica esmaecido.



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.

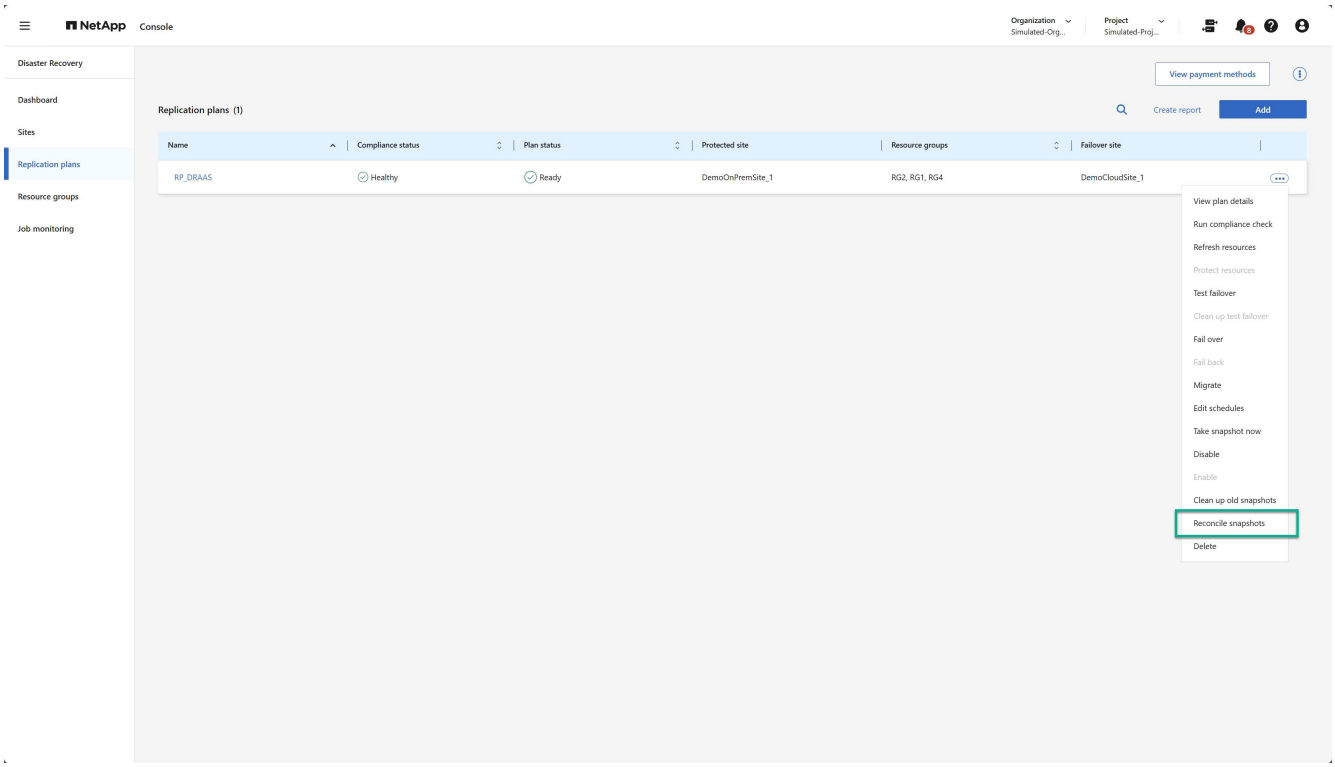
1. Selecione a opção *Ações* ••• ao lado do plano de replicação.
2. Para remover esses instantâneos mais antigos manualmente, selecione **Limpar instantâneos antigos** no menu Ações do plano de replicação.



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.

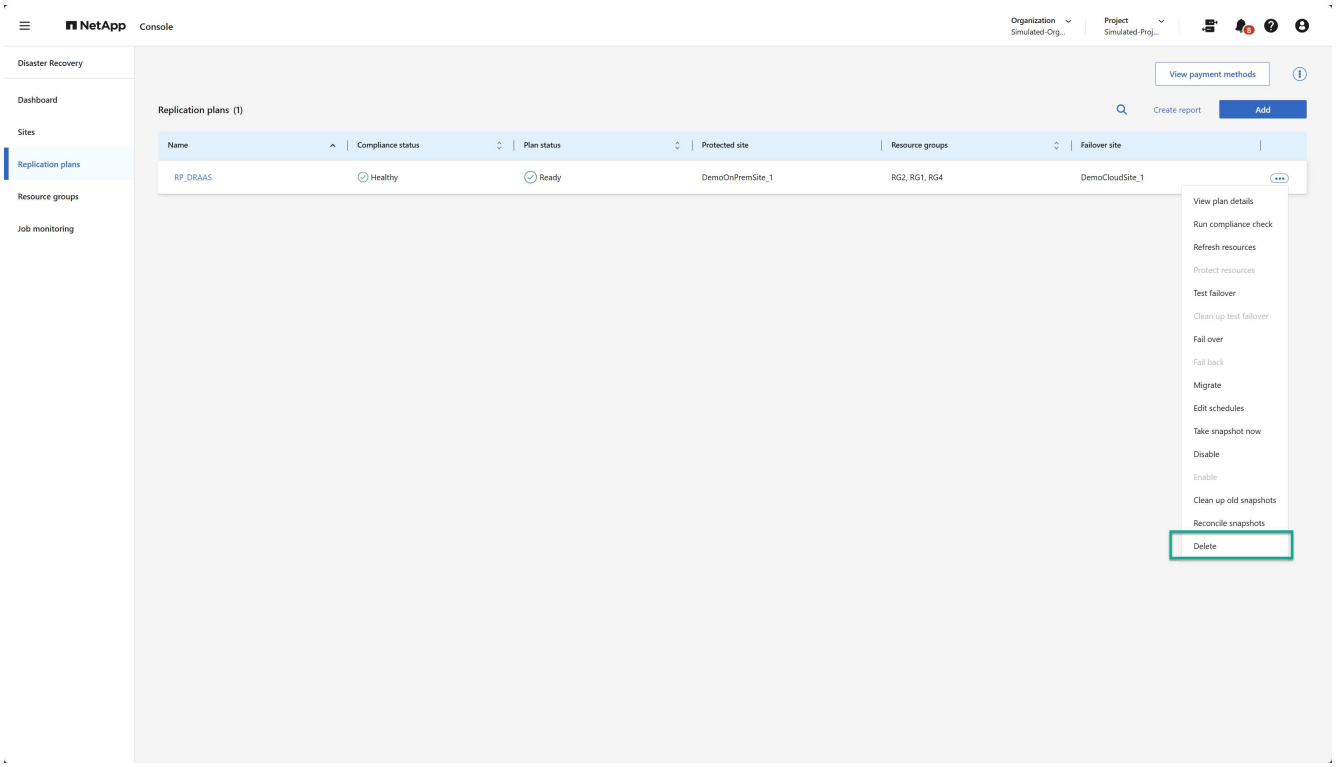
1. Selecione a opção *Ações* ••• ao lado do plano de replicação.
2. Para excluir instantâneos do cluster de origem que não existem no cluster de destino, selecione **Reconciliar instantâneos** no menu Ações do plano de replicação.



Excluir plano de replicação

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

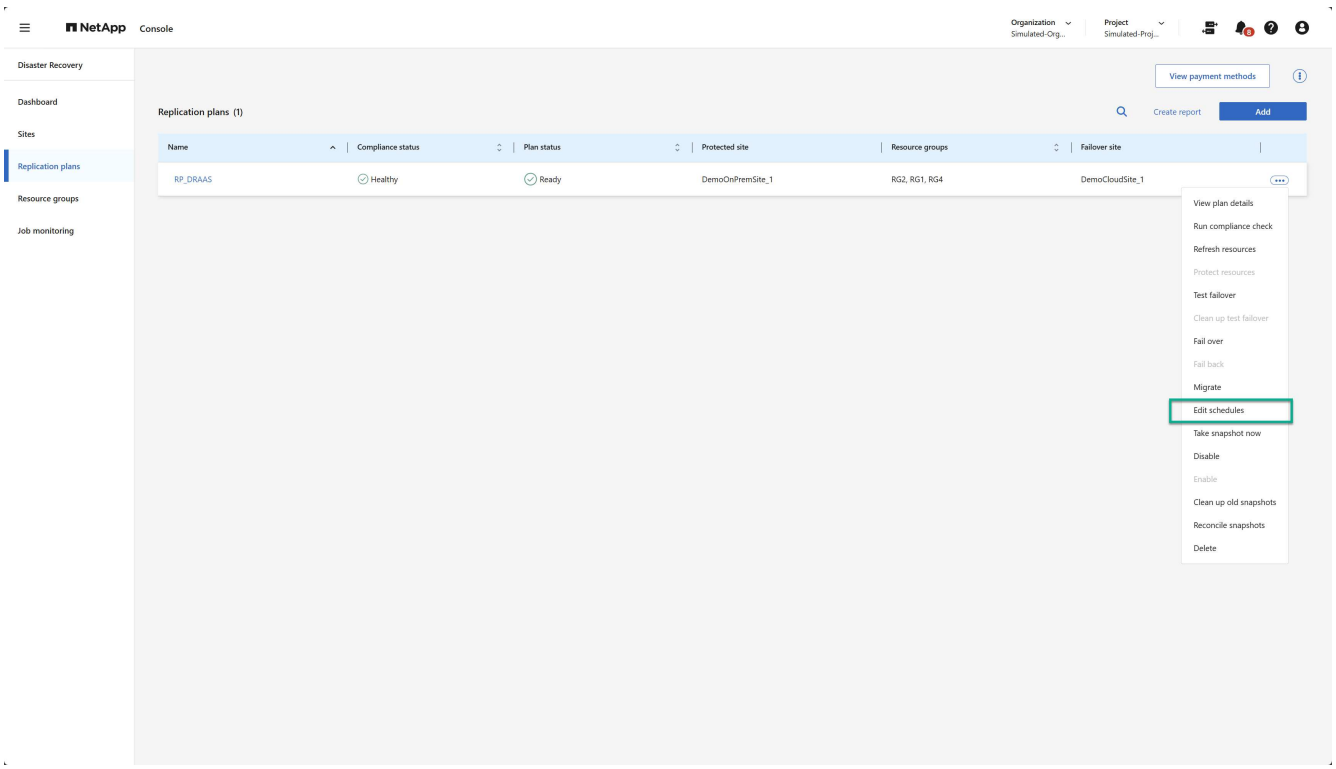
1. Selecione a opção *Ações* ••• ao lado do plano de replicação.
2. Para excluir o plano de replicação, selecione **Excluir** no menu de contexto do plano de replicação.



Editar agendamentos

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

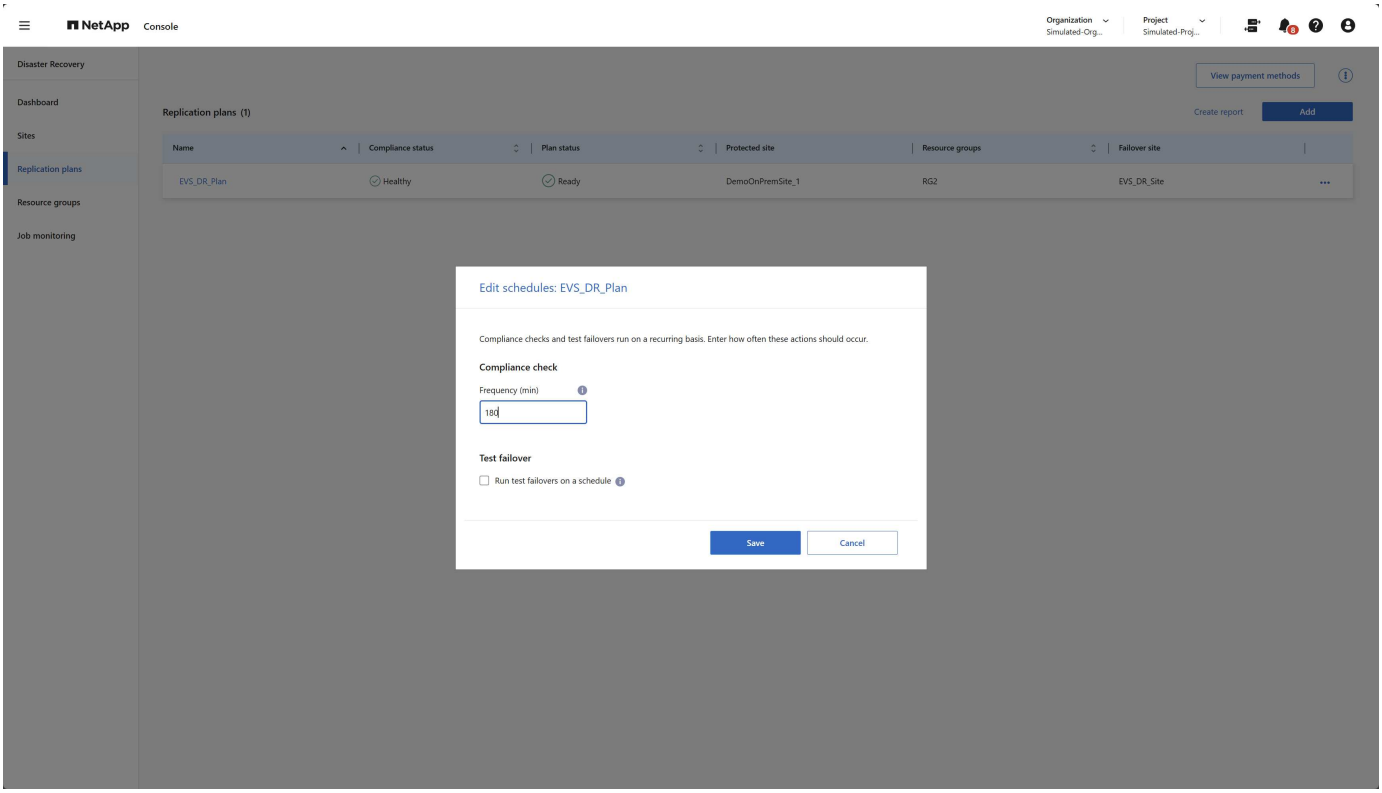
1. Selecione a opção *Ações* ••• ao lado do plano de replicação.
2. Para alterar esses agendamentos para qualquer uma dessas duas operações, selecione **Editar agendamentos** para o plano de replicação.



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:



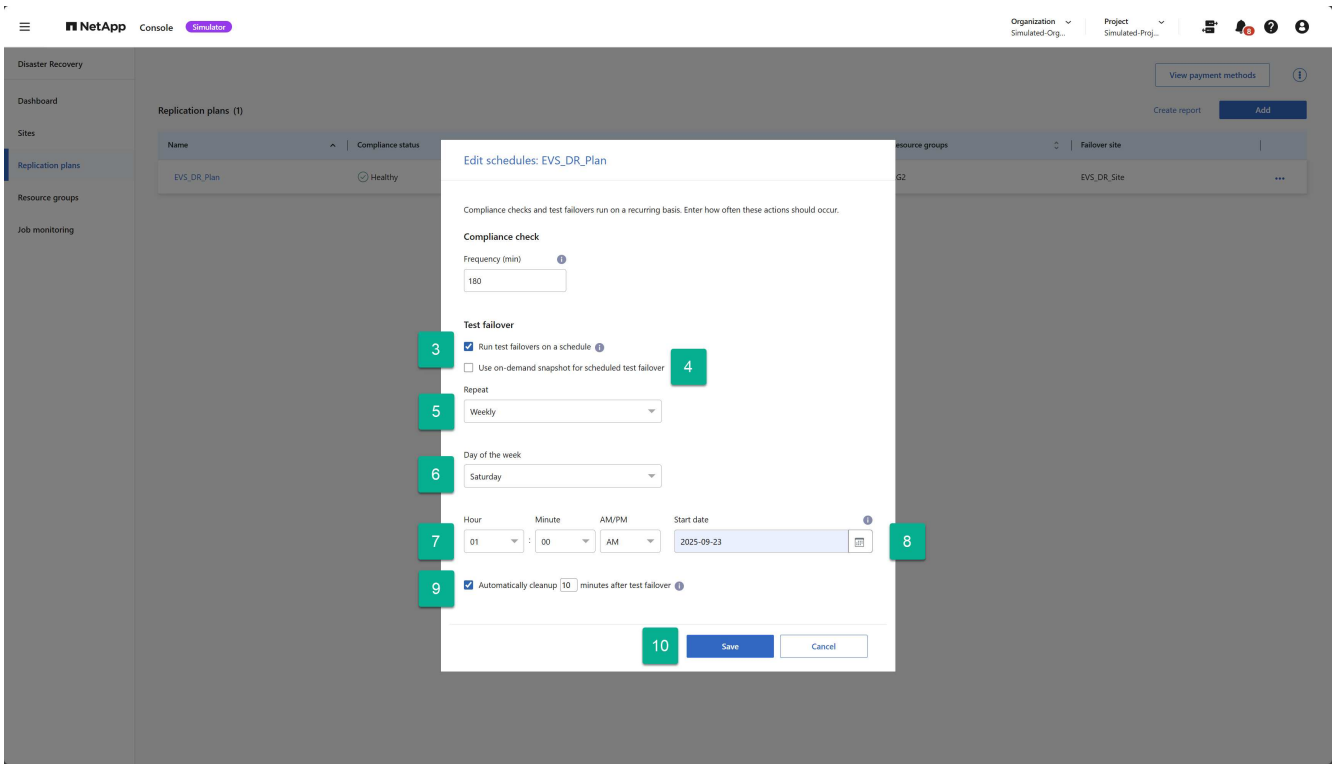
Agendar failovers de testes automatizados

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. Selecione **Salvar**.



Perguntas frequentes sobre NetApp Disaster Recovery

Estas perguntas frequentes podem ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

Qual é o URL do NetApp Disaster Recovery ? Para o URL, em um navegador, digite: "https://console.netapp.com/" para acessar o console do NetApp .

Você precisa de uma licença para usar o NetApp Disaster Recovery? Uma licença do NetApp Disaster Recovery é necessária para acesso completo. No entanto, você pode experimentá-lo com o teste gratuito.

Para obter detalhes sobre a configuração do licenciamento para o NetApp Disaster Recovery, consulte"Configurar o licenciamento do NetApp Disaster Recovery" .

Como você acessa o NetApp Disaster Recovery? O NetApp Disaster Recovery não requer nenhuma ativação. A opção de recuperação de desastres aparece automaticamente na navegação à esquerda do NetApp Console .

Conhecimento e suporte

Registre-se para obter suporte

O registro de suporte é necessário para receber suporte técnico específico para o NetApp Console e suas soluções de armazenamento e serviços de dados. O registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP .

O registro para suporte não habilita o suporte da NetApp para um serviço de arquivo do provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte "Obter ajuda" na documentação do produto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Visão geral do registro de suporte

Existem duas formas de registro para ativar o direito ao suporte:

- Registrando o número de série da sua conta do NetApp Console (seu número de série 960xxxxxxxx de 20 dígitos localizado na página Recursos de suporte no Console).

  Isso serve como seu único ID de assinatura de suporte para qualquer serviço no Console. Cada conta do Console deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no marketplace do seu provedor de nuvem (são números de série 909201xxxxxxxxx de 20 dígitos).

  Esses números de série são comumente chamados de *números de série PAYGO* e são gerados pelo NetApp Console no momento da implantação do Cloud Volumes ONTAP .

Registrar ambos os tipos de números de série habilita recursos como abertura de tickets de suporte e geração automática de casos. O registro é concluído adicionando contas do NetApp Support Site (NSS) ao Console, conforme descrito abaixo.

Registre o NetApp Console para suporte ao NetApp

Para se registrar para obter suporte e ativar o direito ao suporte, um usuário na sua conta do NetApp Console deve associar uma conta do NetApp Support Site ao seu login no Console. A maneira como você se registra para o suporte da NetApp depende se você já tem uma conta no NetApp Support Site (NSS).

Cliente existente com uma conta NSS

Se você for um cliente NetApp com uma conta NSS, basta se registrar para receber suporte pelo Console.

Passos

1. Selecione **Administração** > **Credenciais**.
2. Selecione **Credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do NetApp Support Site (NSS).
4. Para confirmar que o processo de registro foi bem-sucedido, selecione o ícone Ajuda e selecione **Suporte**.

   A página **Recursos** deve mostrar que sua conta do Console está registrada para suporte.

   Observe que outros usuários do Console não verão o mesmo status de registro de suporte se não tiverem associado uma conta do Site de Suporte da NetApp ao seu login. No entanto, isso não significa que sua conta não esteja registrada para suporte. Desde que um usuário na organização tenha seguido essas etapas, sua conta foi registrada.

Cliente existente, mas sem conta NSS

Se você já for um cliente da NetApp com licenças e números de série existentes, mas *nenhuma* conta NSS, será necessário criar uma conta NSS e associá-la ao seu login do Console.

Passos

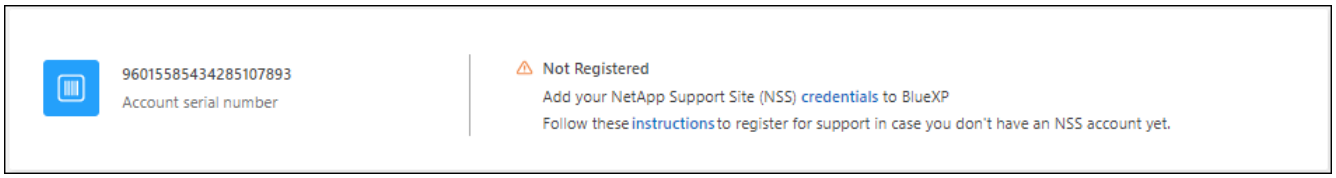
1. Crie uma conta no site de suporte da NetApp preenchendo o "Formulário de registro de usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
   b. Certifique-se de copiar o número de série da conta do Console (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento da conta.
2. Associe sua nova conta NSS ao seu login do Console concluindo as etapas emCliente existente com uma conta NSS .

Novidade na NetApp

Se você é novo na NetApp e não tem uma conta NSS, siga cada etapa abaixo.

Passos

1. No canto superior direito do Console, selecione o ícone Ajuda e selecione **Suporte**.
2. Localize o número de série do seu ID de conta na página de Registro de Suporte.



3. Navegar para "Site de registro de suporte da NetApp" e selecione *Não sou um cliente registrado da NetApp *.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **Linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta da etapa 2 acima, conclua a verificação de segurança e confirme que você leu a Política Global de Privacidade de Dados da NetApp.

   Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Não deixe de verificar sua caixa de spam caso o e-mail de validação não chegue em alguns minutos.

7. Confirme a ação no e-mail.

   A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta no site de suporte da NetApp .

8. Crie uma conta no site de suporte da NetApp preenchendo o "Formulário de registro de usuário do site de suporte da NetApp"
   a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento.

Depois que você terminar

A NetApp entrará em contato com você durante esse processo. Este é um exercício de integração único para novos usuários.

Depois de ter sua conta do Site de Suporte NetApp , associe a conta ao seu login do Console concluindo as etapas emCliente existente com uma conta NSS .

Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP

É necessário associar as credenciais do NetApp Support Site à sua conta do Console para habilitar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

  É necessário fornecer sua conta NSS para ativar o suporte para seu sistema e obter acesso aos recursos de suporte técnico da NetApp .

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer sua conta NSS para que o Console possa carregar sua chave de licença e habilitar a assinatura para o período que você comprou. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

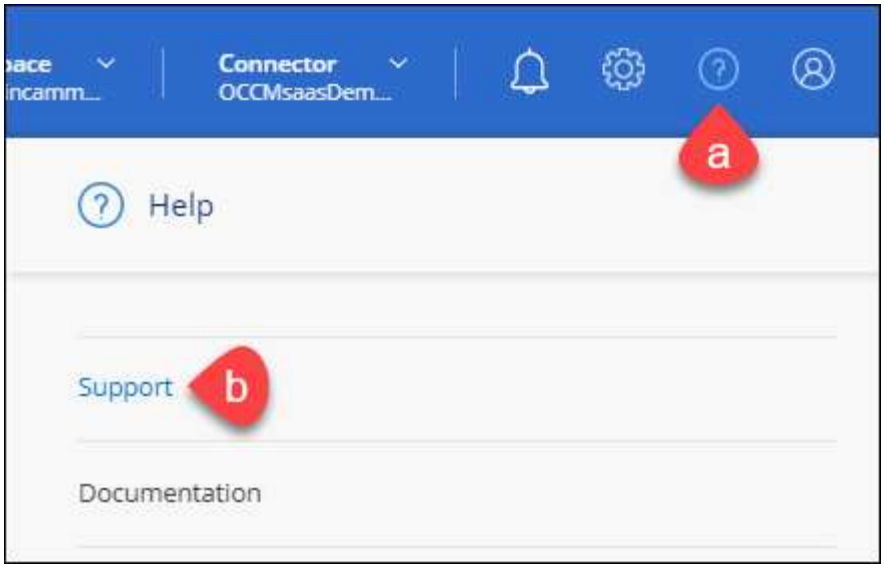
A associação de credenciais do NSS à sua conta do NetApp Console é diferente da associação da conta do NSS a um login de usuário do Console.

Essas credenciais NSS estão associadas ao ID específico da sua conta do Console. Usuários que pertencem à organização Console podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

- Se você tiver uma conta de nível de cliente, poderá adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, poderá adicionar uma ou mais contas NSS, mas elas não poderão ser adicionadas junto com contas de nível de cliente.

Passos

1. No canto superior direito do Console, selecione o ícone Ajuda e selecione **Suporte**.



2. Selecione **Gerenciamento NSS > Adicionar conta NSS**.
3. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

   A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp para realizar o processo de autenticação.

   Essas ações permitem que o Console use sua conta NSS para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

   Observe o seguinte:

   - A conta NSS deve ser uma conta de nível de cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS em nível de cliente.
   - Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS em nível de cliente e existir uma conta em nível de parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, pois já existem usuários NSS de tipos diferentes."

   O mesmo é verdadeiro se você tiver contas NSS pré-existentes em nível de cliente e tentar adicionar uma conta em nível de parceiro.

   - Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que mapeia para seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail do ••• menu.

   - Se você precisar atualizar seus tokens de credenciais de login, também há uma opção **Atualizar credenciais** no ••• menu.

     Usar esta opção solicitará que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será publicada para alertá-lo sobre isso.

Obter ajuda

A NetApp fornece suporte para o NetApp Console e seus serviços de nuvem de diversas maneiras. Há diversas opções gratuitas de autoatendimento disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. Seu cadastro no suporte inclui suporte técnico remoto por meio de tickets online.

Obtenha suporte para um serviço de arquivo de provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte a documentação desse produto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Para receber suporte técnico específico para a NetApp e suas soluções de armazenamento e serviços de dados, use as opções de suporte descritas abaixo.

Use opções de autoapoio

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do NetApp Console que você está visualizando no momento.

- "Base de conhecimento"

  Pesquise na base de conhecimento da NetApp para encontrar artigos úteis para solucionar problemas.

- "Comunidades"

  Participe da comunidade do NetApp Console para acompanhar discussões em andamento ou criar novas.

Crie um caso com o suporte da NetApp

Além das opções de autossuporte acima, você pode trabalhar com um especialista em suporte da NetApp para resolver quaisquer problemas após ativar o suporte.

Antes de começar

- Para usar o recurso **Criar um caso**, você deve primeiro associar suas credenciais do site de suporte da NetApp ao seu login do console. "Aprenda a gerenciar credenciais associadas ao seu login do Console" .
- Se você estiver abrindo um caso para um sistema ONTAP que tenha um número de série, sua conta NSS deverá estar associada ao número de série desse sistema.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Na página **Recursos**, escolha uma das opções disponíveis em Suporte Técnico:

a. Selecione **Ligue para nós** se quiser falar com alguém por telefone. Você será direcionado para uma página no netapp.com que lista os números de telefone para os quais você pode ligar.

b. Selecione **Criar um caso** para abrir um tíquete com um especialista de suporte da NetApp :

   - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, * NetApp Console* quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do Console.
   - **Sistema**: Se aplicável ao armazenamento, selecione * Cloud Volumes ONTAP* ou **On-Prem** e, em seguida, o ambiente de trabalho associado.

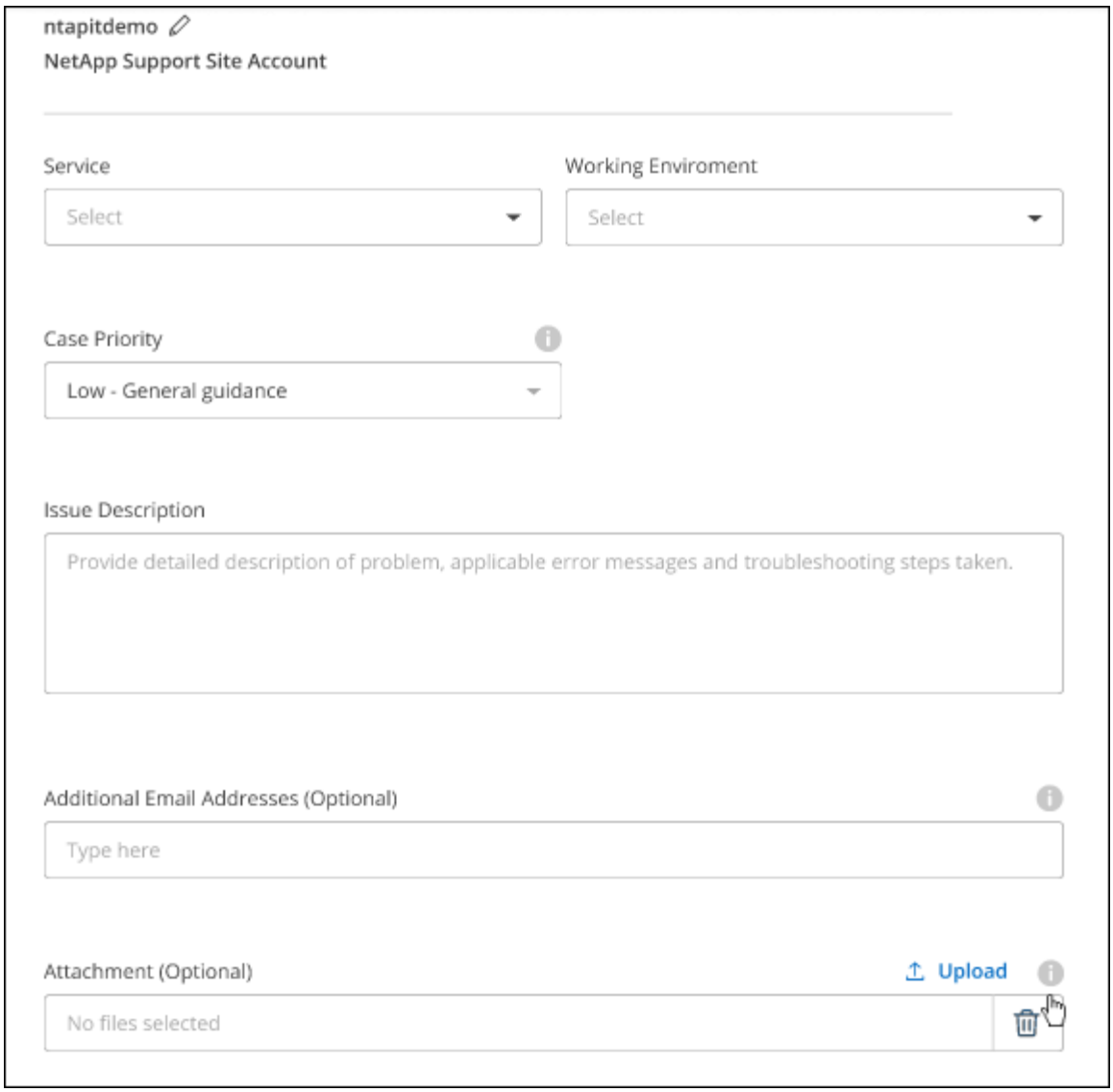
     A lista de sistemas está dentro do escopo da organização do Console e do agente do Console que você selecionou no banner superior.

   - **Prioridade do caso**: escolha a prioridade do caso, que pode ser Baixa, Média, Alta ou Crítica.

     Para saber mais detalhes sobre essas prioridades, passe o mouse sobre o ícone de informações ao lado do nome do campo.

   - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
   - **Endereços de e-mail adicionais**: insira endereços de e-mail adicionais se quiser informar outra pessoa sobre esse problema.
   - **Anexo (Opcional)**: Carregue até cinco anexos, um de cada vez.

     Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Depois que você terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp analisará seu caso e entrará em contato com você em breve.

Para obter um histórico dos seus casos de suporte, você pode selecionar **Configurações > Linha do tempo** e procurar por ações chamadas "criar caso de suporte". Um botão na extrema direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa registrada à qual ela está associada não são a mesma empresa registrada para o número de série da conta do NetApp Console (por exemplo, 960xxxx) ou o número de série do ambiente de trabalho. Você pode buscar assistência usando uma das seguintes opções:

- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerencie seus casos de suporte

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do Console. Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
  - A visualização à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta NSS do usuário que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses no nível da sua empresa com base na sua conta de usuário NSS.

  Os resultados na tabela refletem os casos relacionados à exibição que você selecionou.
- Você pode adicionar ou remover colunas de interesse e filtrar o conteúdo de colunas como Prioridade e Status. Outras colunas fornecem apenas recursos de classificação.

  Veja as etapas abaixo para mais detalhes.
- Em cada caso, oferecemos a possibilidade de atualizar notas do caso ou fechar um caso que ainda não esteja no status Fechado ou Pendente Fechado.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Selecione **Gerenciamento de casos** e, se solicitado, adicione sua conta NSS ao Console.

   A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à sua conta de usuário do Console. Esta é a mesma conta NSS que aparece no topo da página **Gerenciamento NSS**.
3. Modifique opcionalmente as informações exibidas na tabela:
   - Em **Casos da organização**, selecione **Exibir** para visualizar todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um período de tempo diferente.
   - Filtrar o conteúdo das colunas.
   - Altere as colunas que aparecem na tabela selecionando e então escolher as colunas que você gostaria de exibir.
4. Gerencie um caso existente selecionando e selecionando uma das opções disponíveis:
   - **Ver caso**: Veja detalhes completos sobre um caso específico.
   - **Atualizar notas do caso**: Forneça detalhes adicionais sobre seu problema ou selecione **Carregar arquivos** para anexar até no máximo cinco arquivos.

     Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Fechar caso**: Forneça detalhes sobre o motivo pelo qual você está fechando o caso e selecione **Fechar caso**.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de Privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

"Aviso para NetApp Disaster Recovery"

Informações sobre direitos autorais

Informações sobre marcas comerciais