Use a NetApp Disaster Recovery

NetApp Disaster Recovery

NetApp
January 12, 2026

This PDF was generated from https://docs.netapp.com/pt-br/data-services-disaster-recovery/use/use-overview.html on January 12, 2026. Always check docs.netapp.com for the latest.

Índice

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

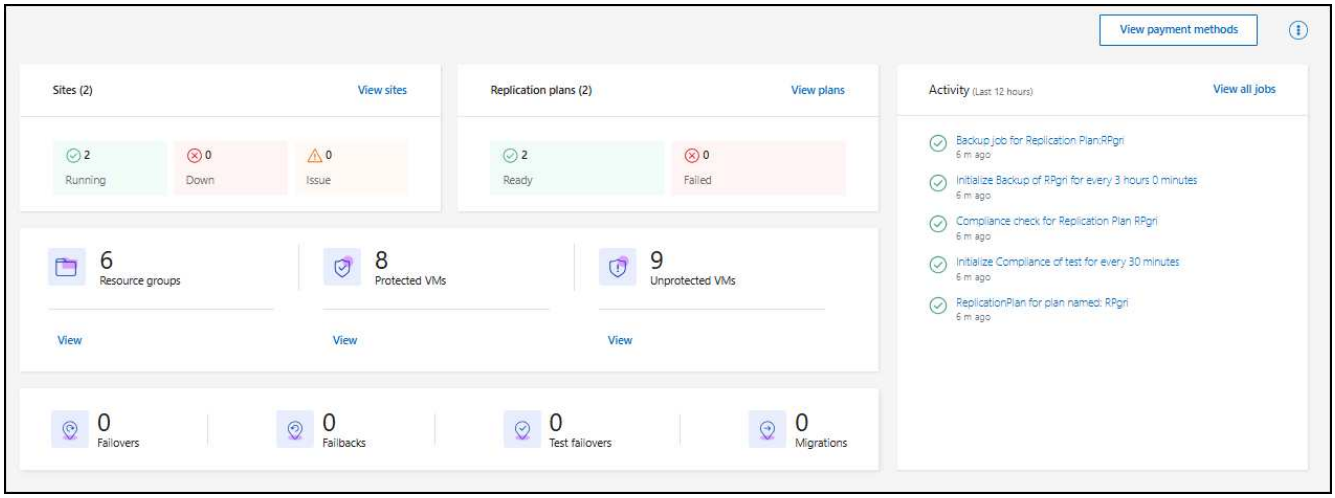
Usando o NetApp Disaster Recovery Dashboard, você pode determinar a integridade dos seus sites de recuperação de desastres e planos de replicação. Você pode verificar rapidamente quais sites e planos estão íntegros, desconectados ou degradados.

*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

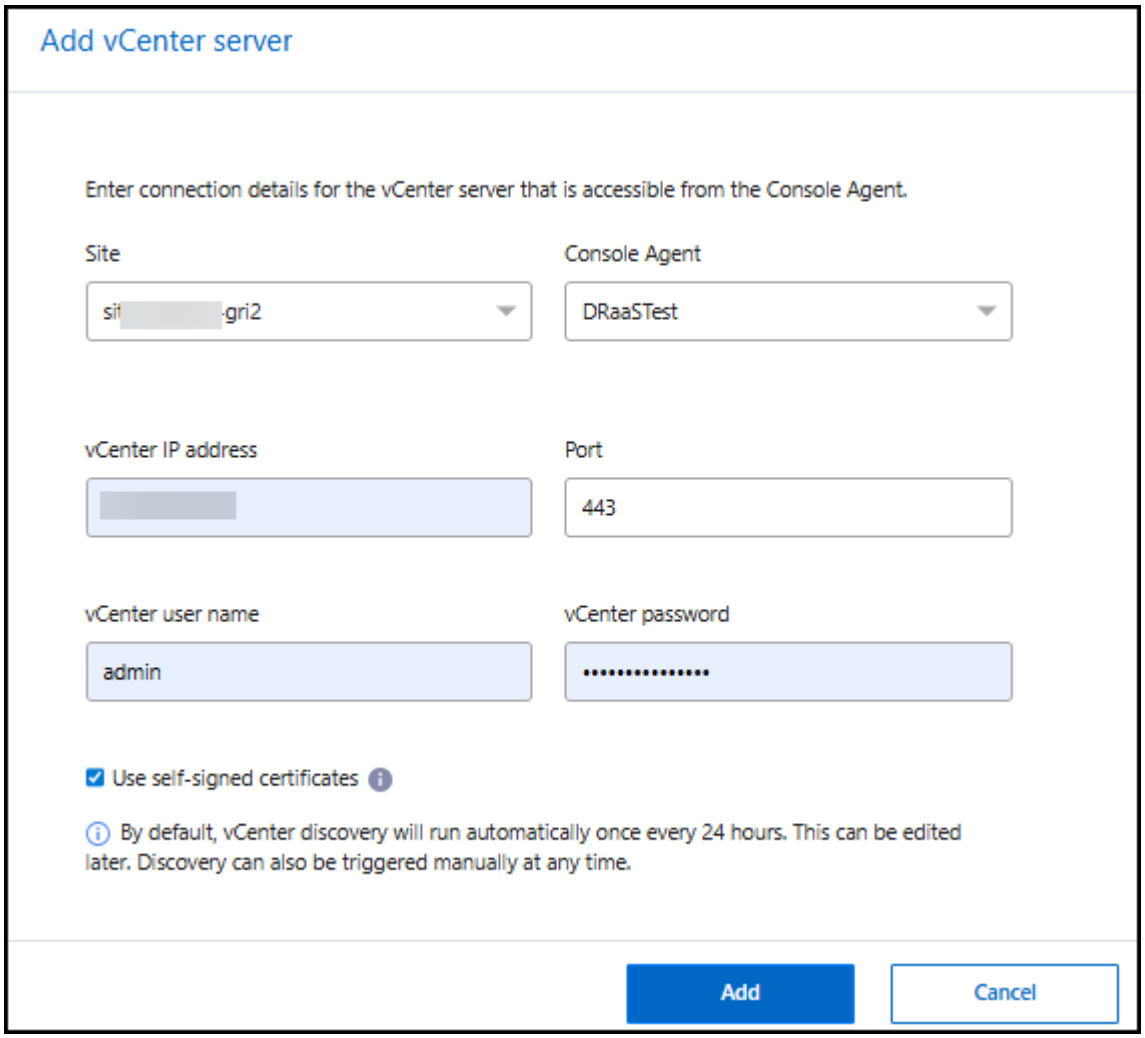
1. Faça login no "NetApp Console" .
2. Na navegação à esquerda do NetApp Console , selecione **Proteção** > **Recuperação de desastres**.

   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**.

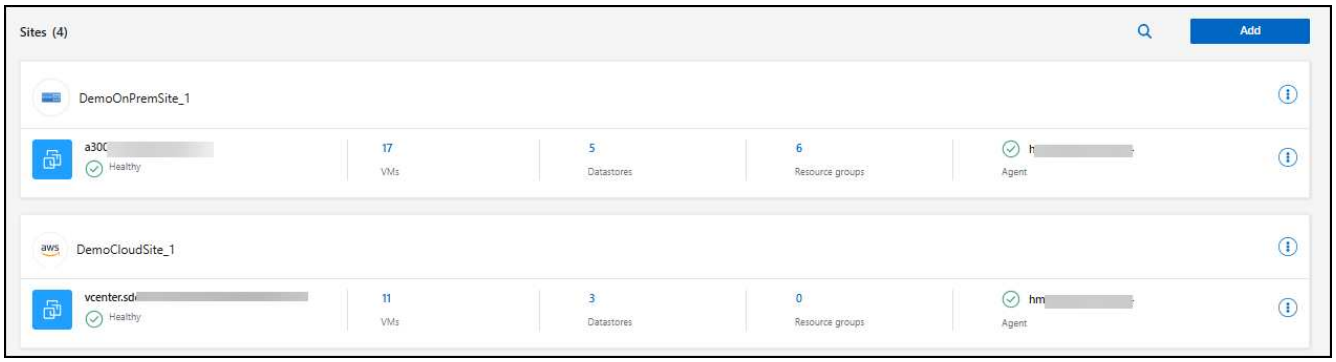
   Em seguida, adicione um vCenter de destino.

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.

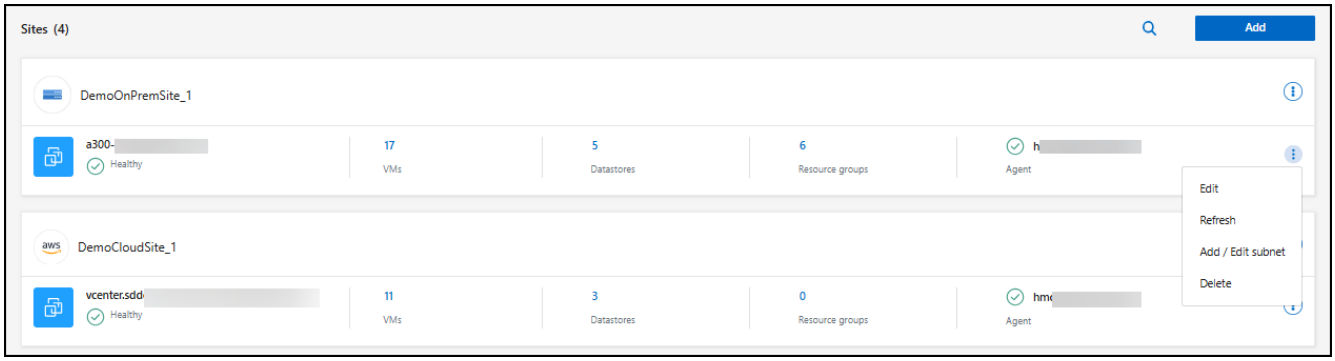
Em resumo, o endereço do host permanece o mesmo, enquanto o endereço de rede é substituído pelo que estiver configurado no mapeamento de sub-rede do site. Isso permite que você gerencie a reatribuição de endereços IP em caso de failover com mais facilidade, especialmente se você tiver centenas de redes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

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

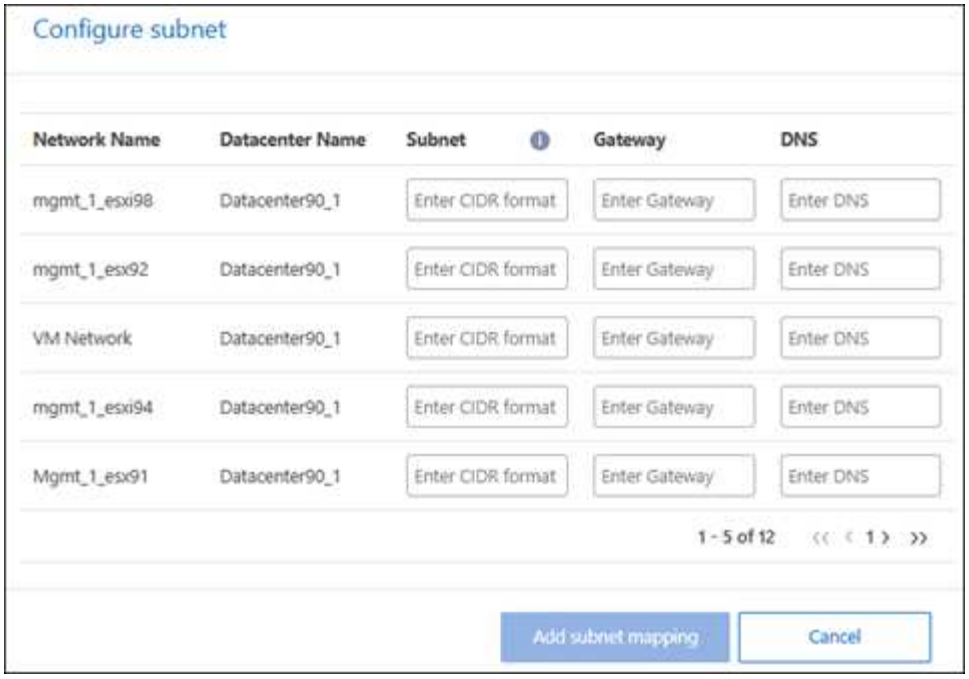
- Primeiro, adicione o mapeamento de sub-rede para cada site do vCenter.
- Em segundo lugar, no plano de replicação, indique que você deseja usar o mapeamento de sub-rede na guia Máquinas Virtuais e no campo IP de Destino.

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

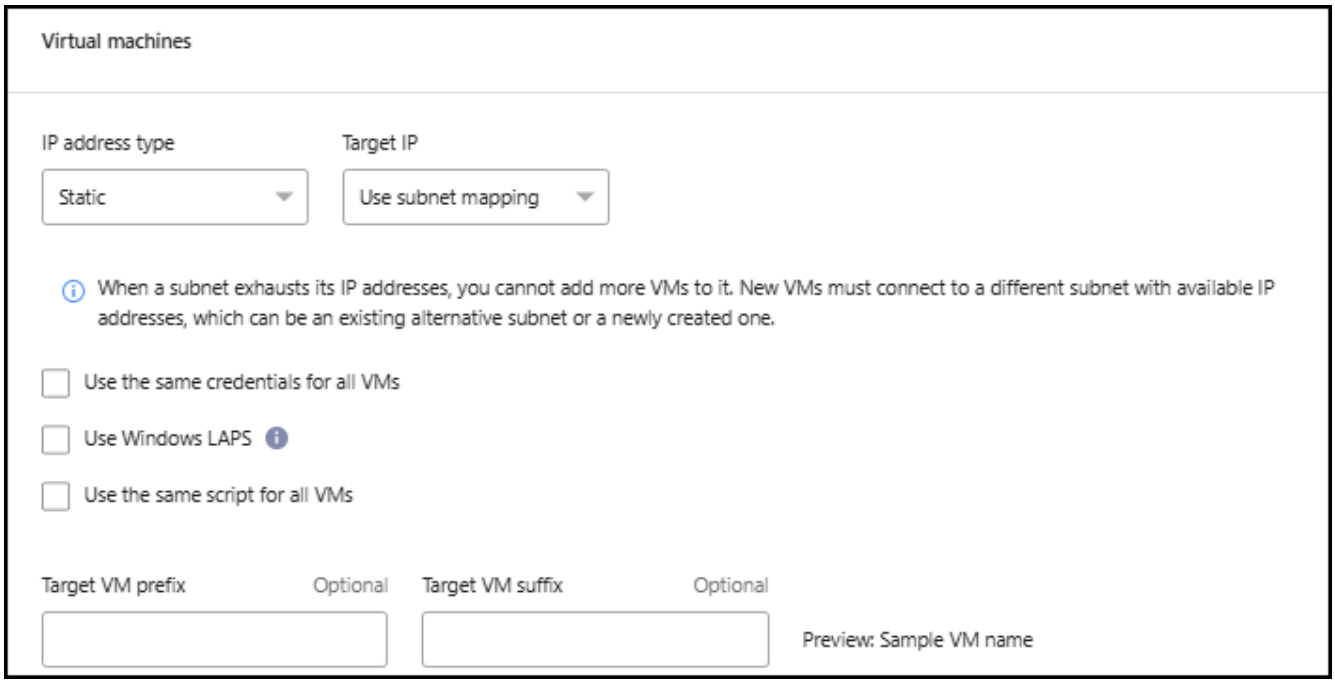
Ao criar um plano de replicação, você pode selecionar o mapeamento de sub-rede para o plano de replicação.

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

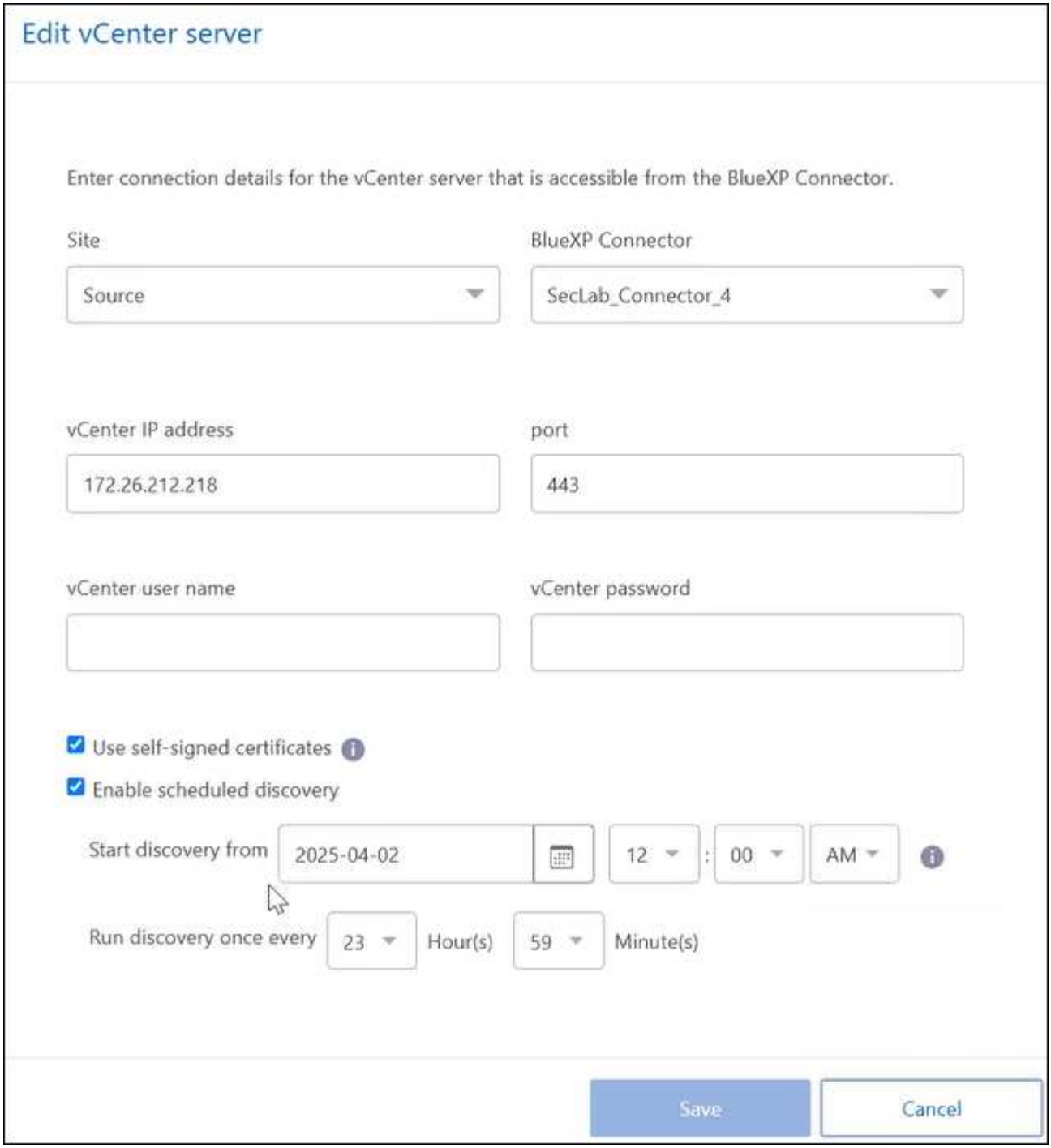
Você pode editar o site do servidor vCenter para personalizar o agendamento de descoberta. Por exemplo, se você tiver um grande número de VMs, poderá definir o agendamento de descoberta para ser executado a cada 23 horas e 59 minutos. Se você tiver um pequeno número de VMs, poderá definir o agendamento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

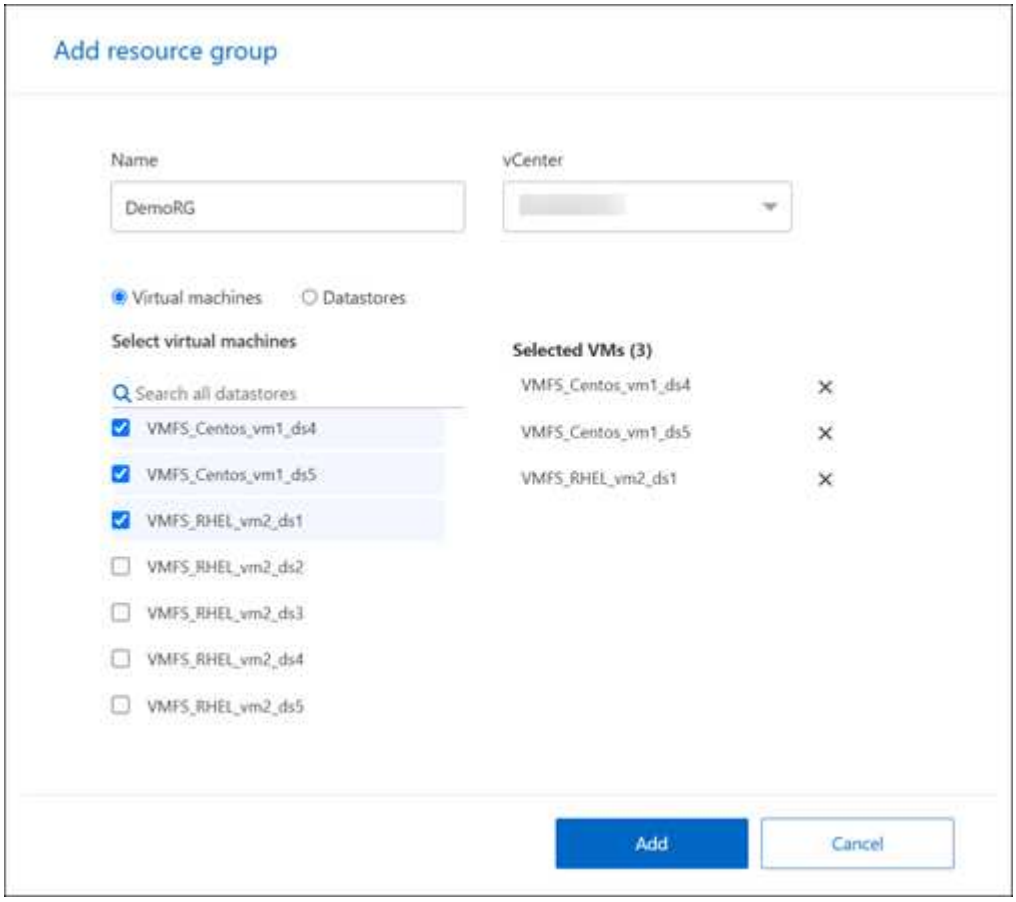
Ao criar grupos de recursos, considere as seguintes questões:

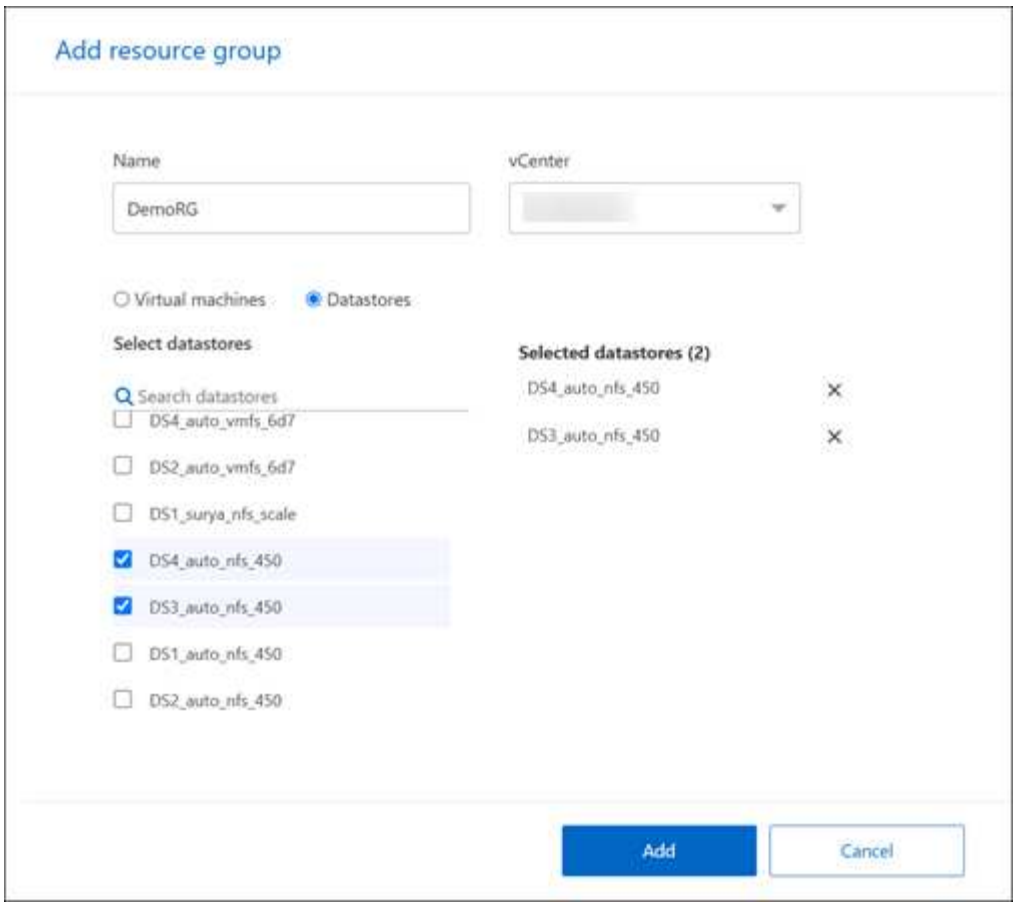
- Antes de adicionar armazenamentos de dados a grupos de recursos, inicie primeiro uma descoberta manual ou uma descoberta agendada das VMs. Isso garante que as VMs sejam descobertas e listadas no grupo de recursos. Se você não iniciar uma descoberta manual, as VMs poderão não ser listadas no grupo de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

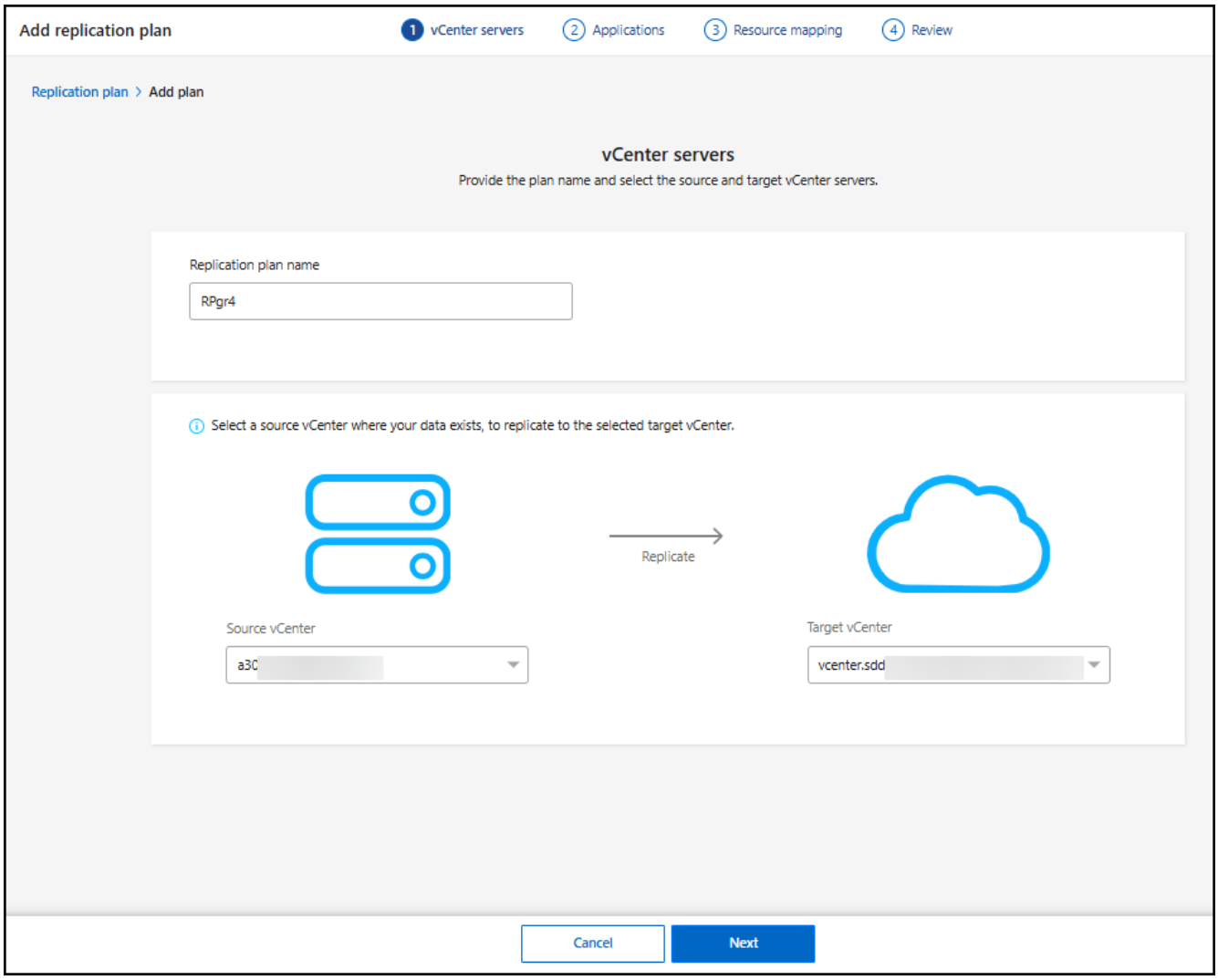
- Use as mesmas credenciais para todas as VMs no plano.
- Use o mesmo script para todas as VMs no plano.
- Use a mesma sub-rede, DNS e gateway para todas as VMs no plano.

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.

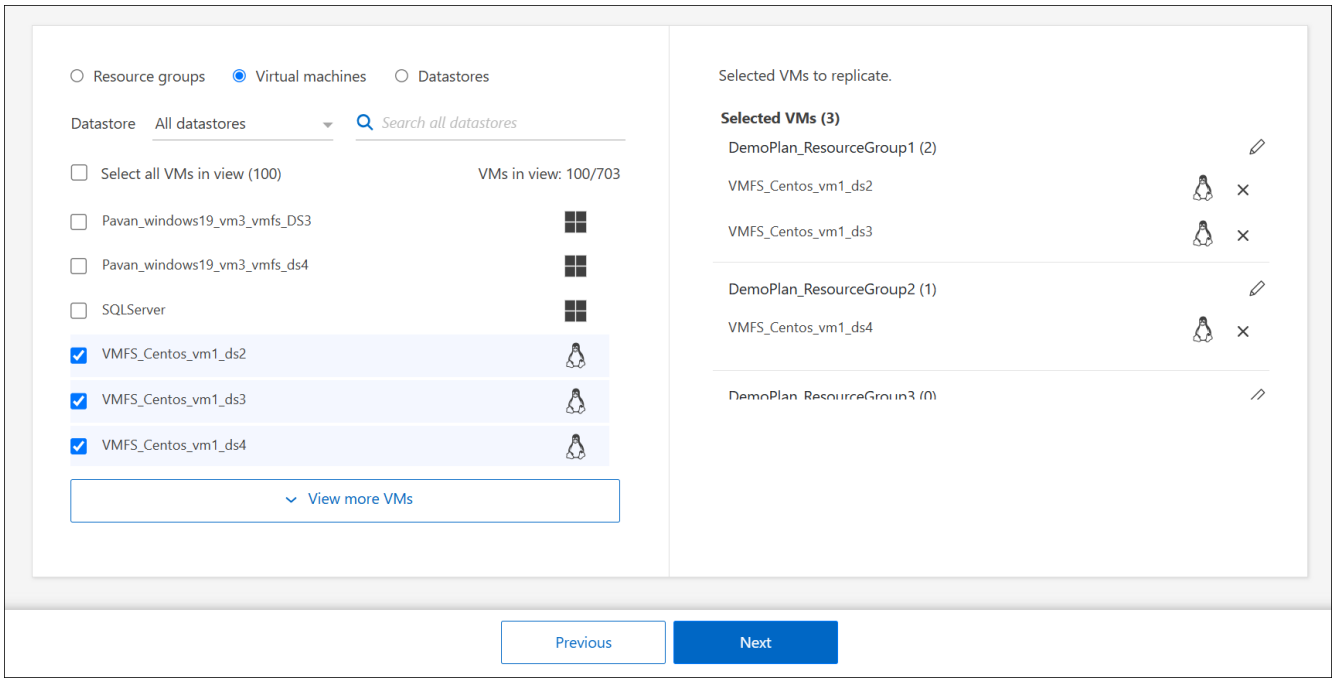
Crie um conjunto separado e dedicado de mapeamentos para seus testes de failover, a fim de evitar que as VMs sejam conectadas a redes de produção usando os mesmos endereços IP.

Passos

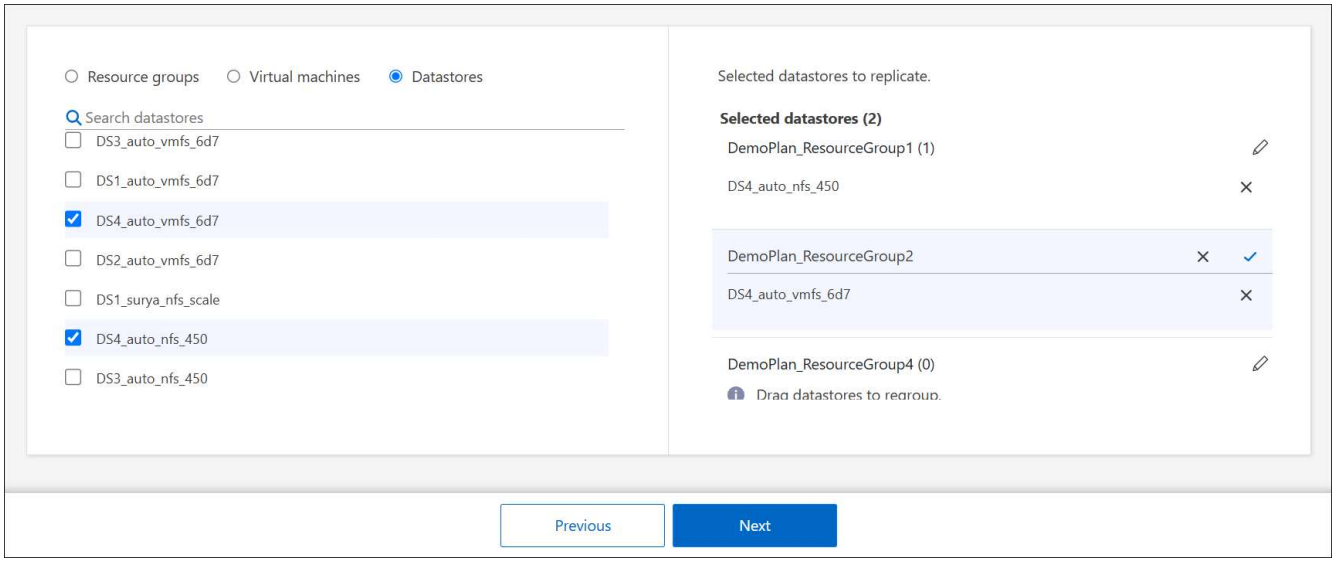
1. Selecione **Máquinas virtuais** ou **Datastores**.
2. Opcionalmente, pesquise por VM ou armazenamento de dados específico pelo nome.
3. No lado esquerdo da página Aplicativos, selecione as VMs ou os armazenamentos de dados que você deseja proteger e atribua ao grupo selecionado.

   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.

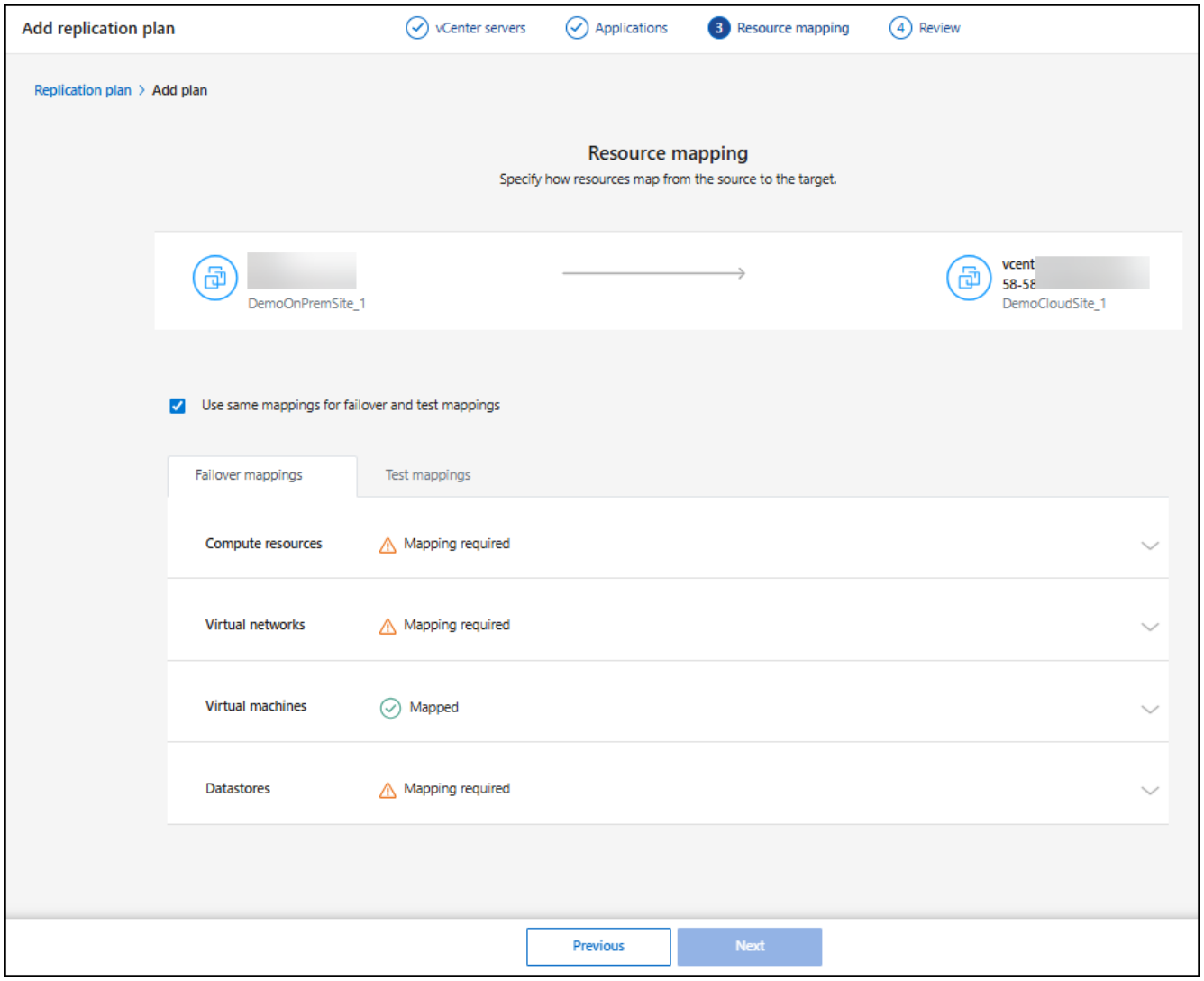
Se você planeja executar failovers de teste como parte do seu plano de DR, forneça um conjunto de mapeamentos de failover de teste para garantir que as VMs iniciadas durante o teste de failover não interfiram nas VMs de produção. Você pode fazer isso fornecendo VMs de teste com endereços IP diferentes 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.

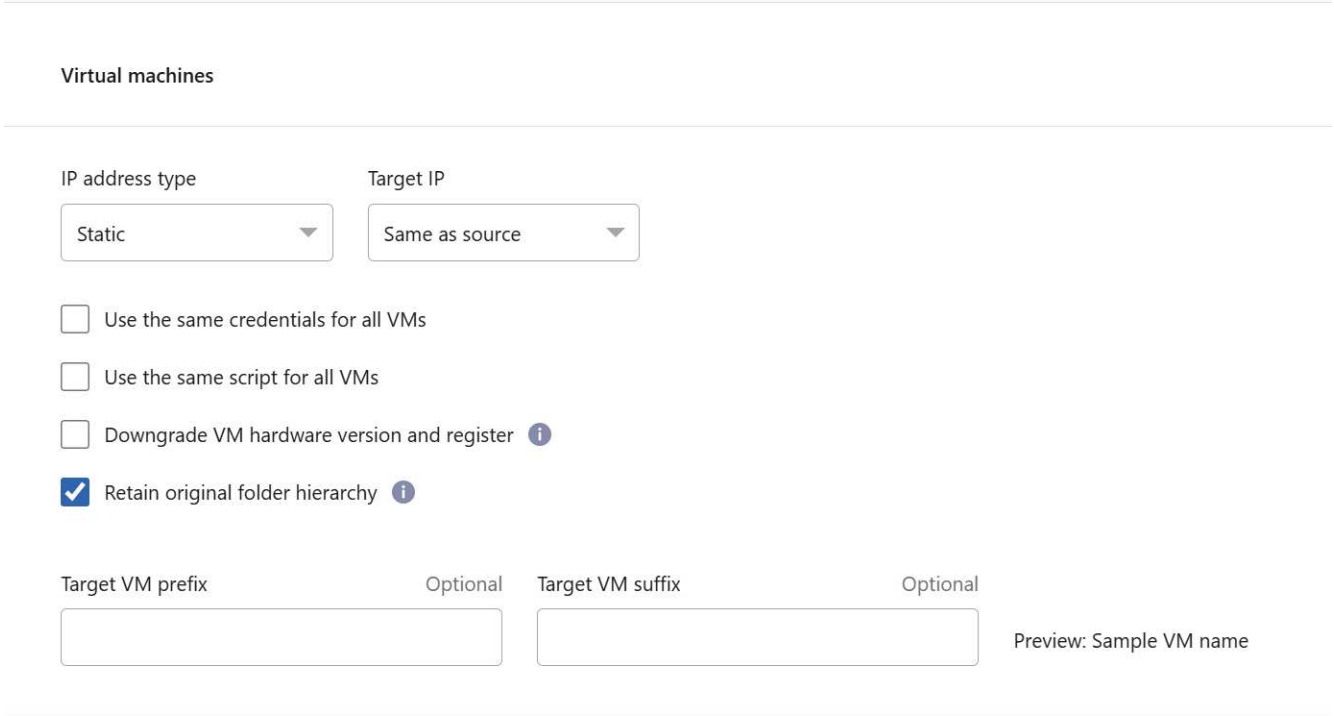
No nível mais básico (e padrão), as configurações simplesmente usam as mesmas configurações de rede TCP/IP para cada VM no site de destino usadas no site de origem. Isso requer que você configure as mesmas configurações de TCP/IP nas redes virtuais de origem e destino.

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.

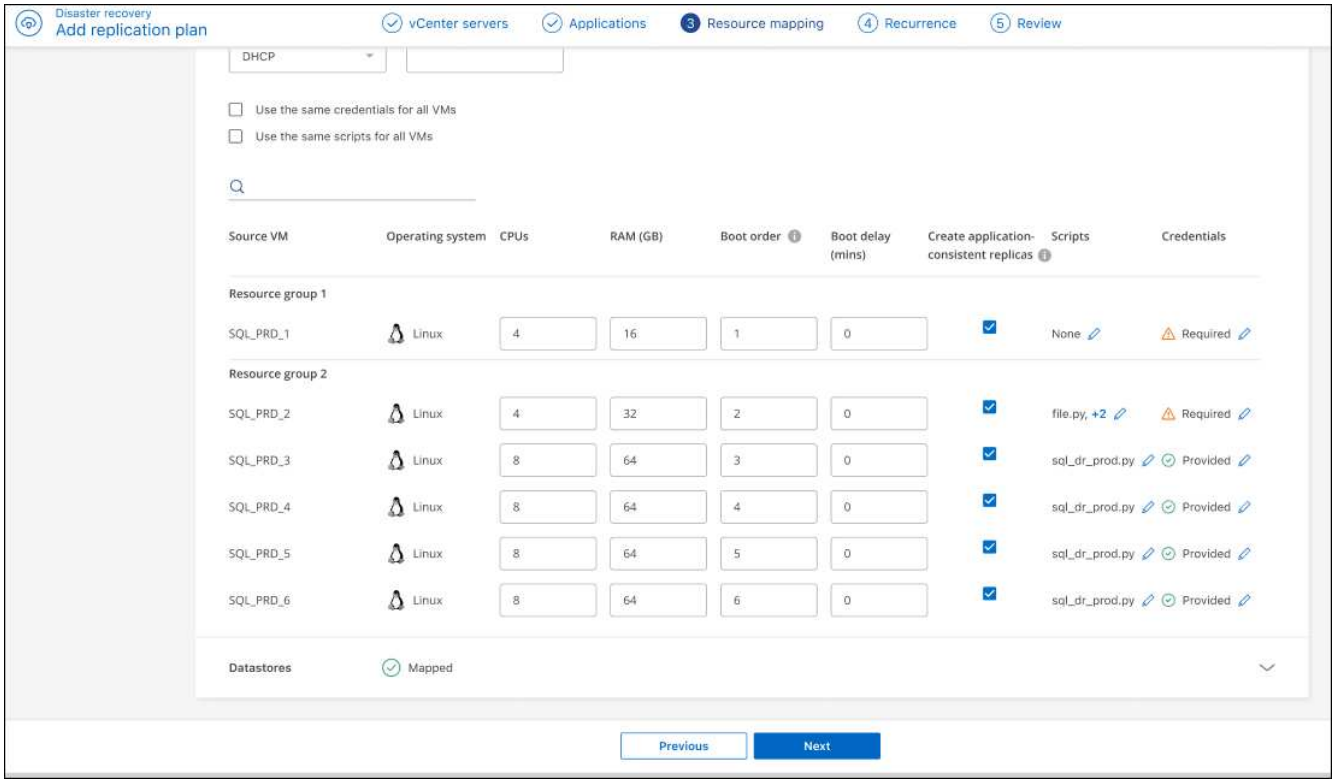
- **Prefixo e sufixo da VM de destino**: nos detalhes das máquinas virtuais, você pode, opcionalmente, adicionar um prefixo e um sufixo a cada nome de VM com failover. Isso pode ser útil para diferenciar as VMs com failover das VMs de produção em execução no mesmo cluster do vCenter. Por exemplo, você 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.

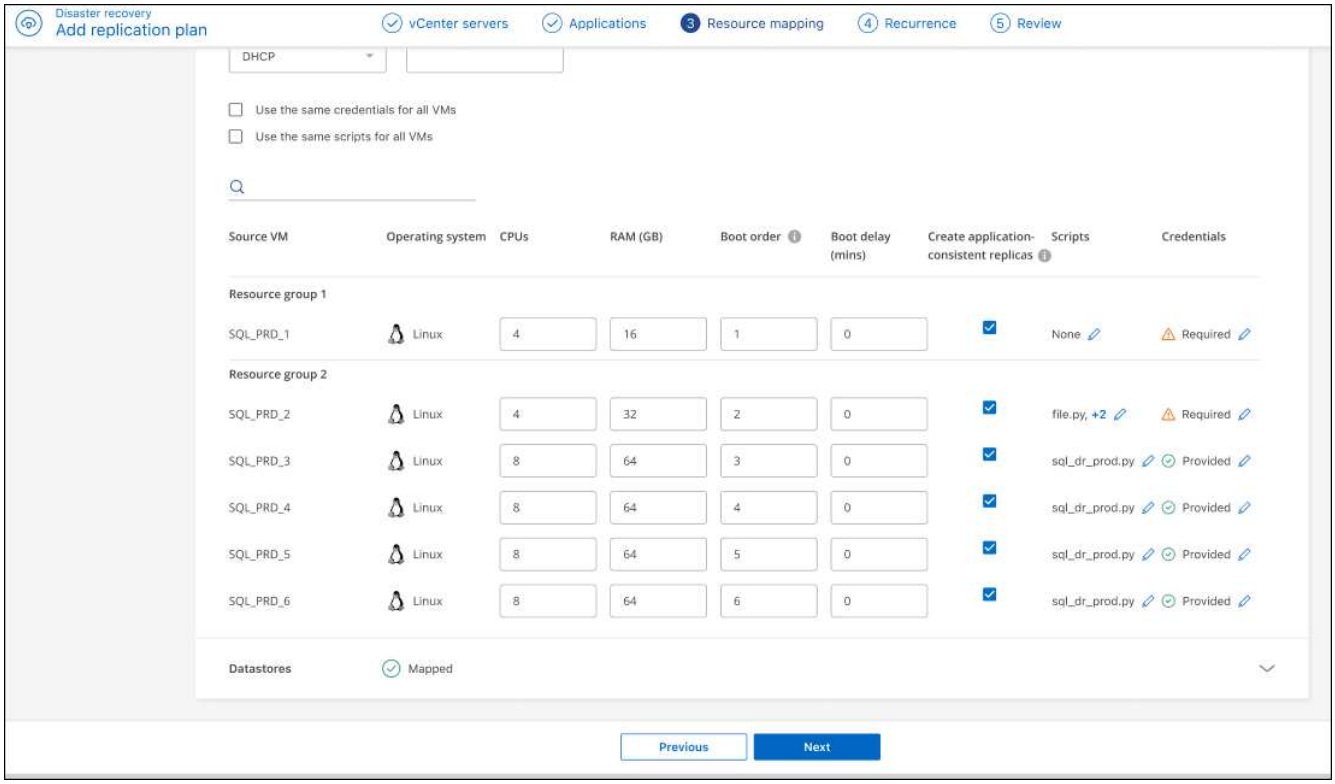
  A Recuperação de Desastres inicializa em paralelo quaisquer máquinas virtuais com o mesmo número de ordem de inicialização.

  - 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.

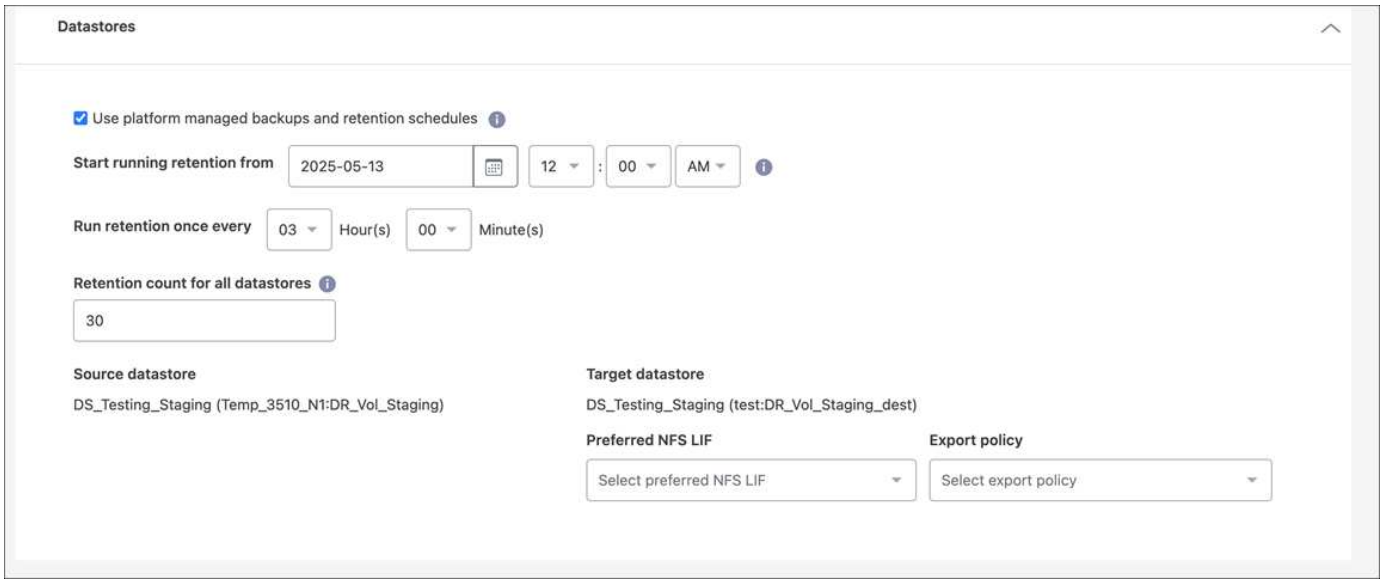
Para habilitar réplicas consistentes com o aplicativo das VMs e seus armazenamentos de dados de hospedagem, marque a caixa ao lado de **Criar réplicas consistentes com o aplicativo** para cada VM e forneça credenciais de login de convidado com os privilégios apropriados.

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.

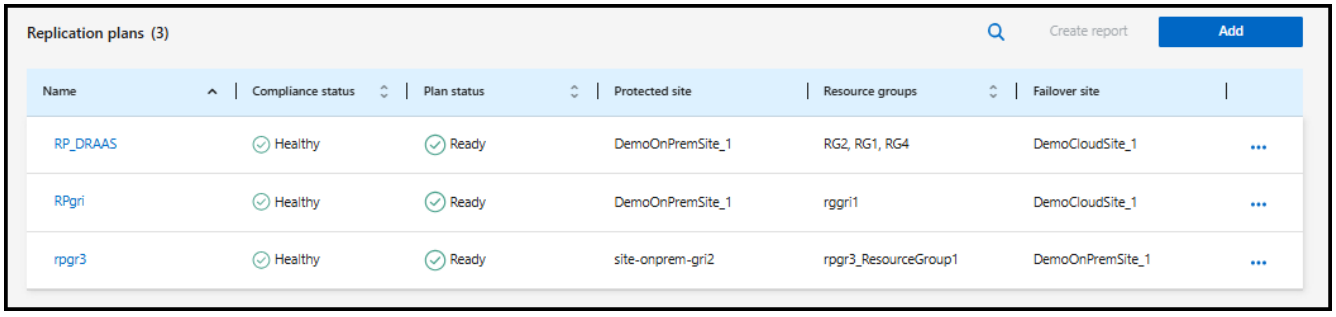
- **Impacto no tempo de conformidade**: quando um plano de replicação é criado, o serviço cria um cronograma de conformidade por padrão. O tempo de conformidade padrão é de 30 minutos. Para alterar esse horário, você pode editar o agendamento no plano de replicação.
- **Impacto do failover de teste**: 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.

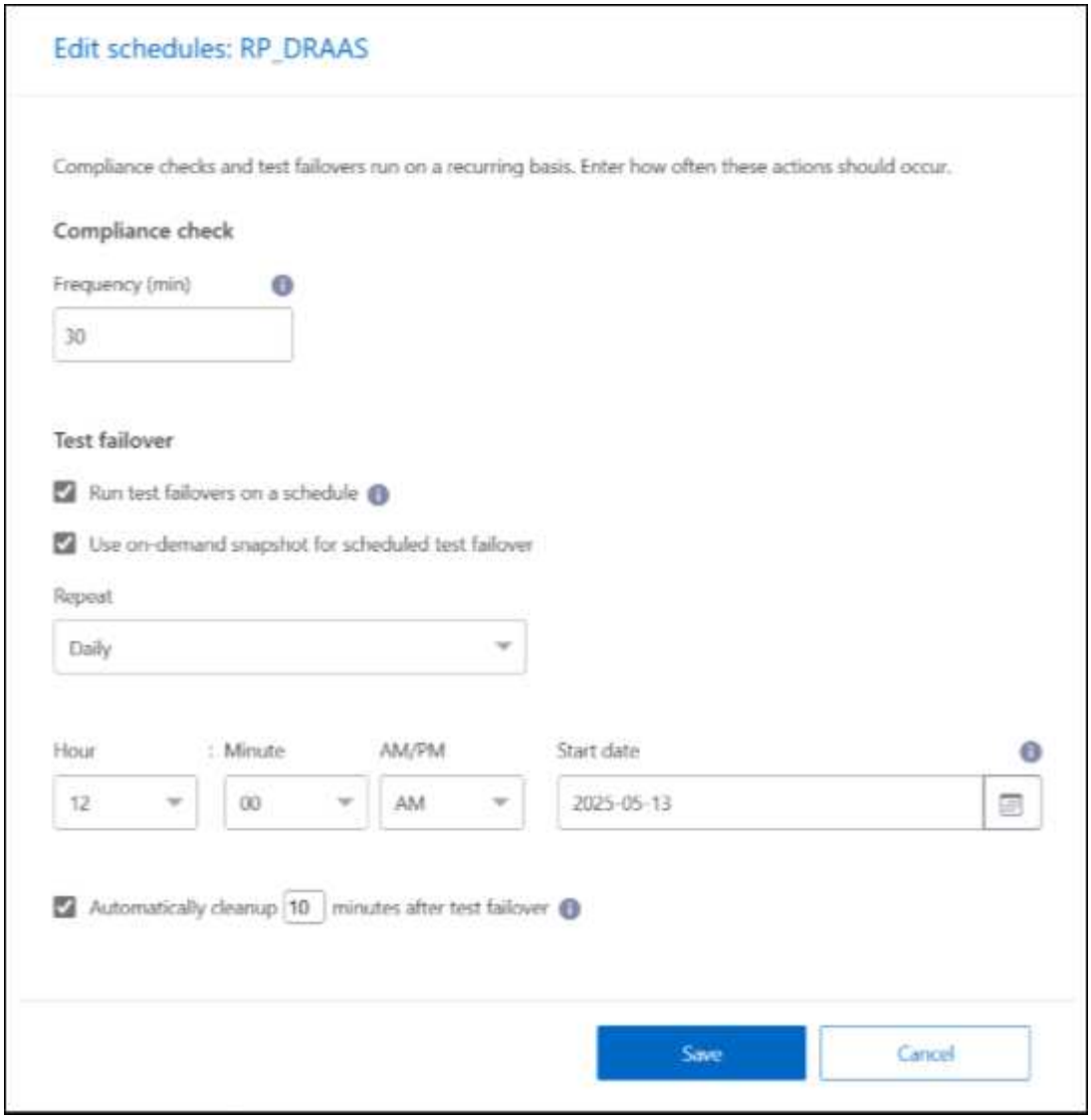
Com base no cronograma, o teste de failover é executado e garante que as cargas de trabalho sejam movidas para o destino especificado pelo plano de replicação.

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).

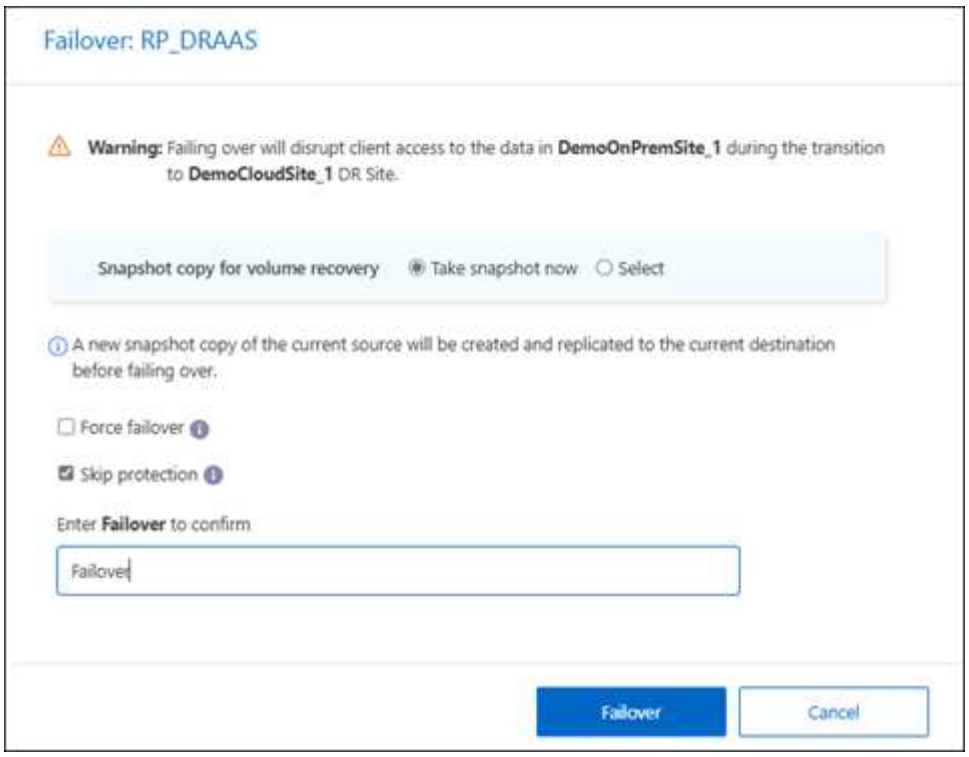
- Os armazenamentos de dados são criados e montados no cluster ou host VMware ou VMC com base nas informações capturadas no plano de replicação. Se algum armazenamento de dados for VMFS, crie e mapeie um iGroup para cada LUN.
- As máquinas virtuais de destino são registradas no vCenter como novos armazenamentos 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

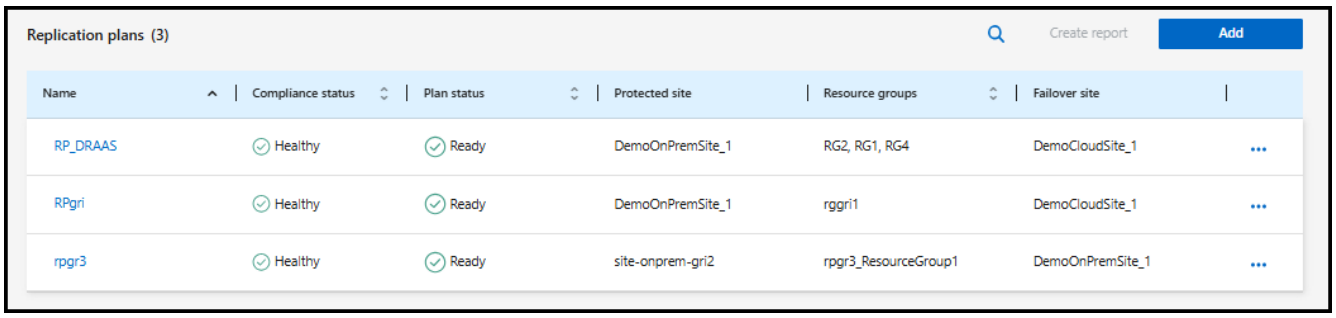
Você pode desabilitar, habilitar e excluir planos de replicação. Você pode alterar horários.

*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**.

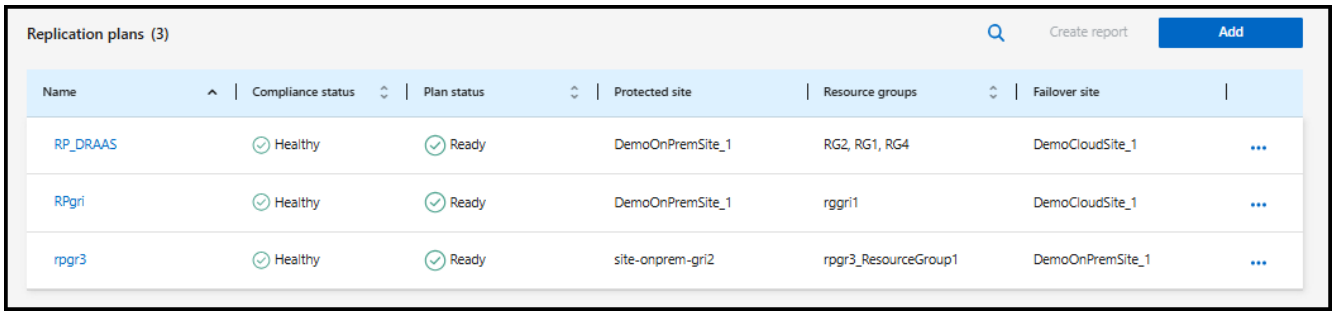
Reconciliar instantâneos sob demanda

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

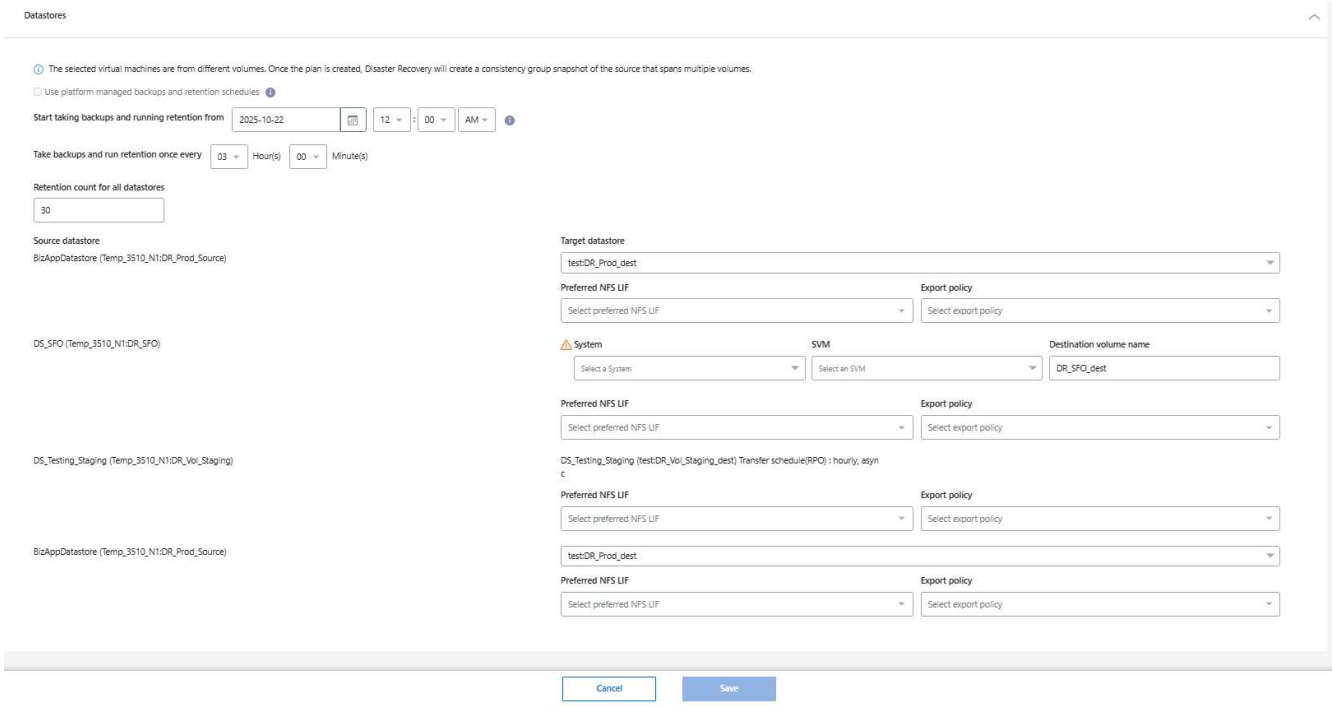
Alterar o número de retenções permite aumentar ou diminuir a quantidade de dados armazenados.

*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.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

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

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

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

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

Informações sobre marcas comerciais

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