



Proteja armazenamentos de dados e máquinas virtuais

ONTAP tools for VMware vSphere 105

NetApp
July 24, 2026

Índice

Proteja armazenamentos de dados e máquinas virtuais	1
Proteja um cluster de hosts nas ONTAP tools	1
Proteja usando a proteção SRA	2
Configure o SRA nas ONTAP tools para proteger datastores	2
Configure o SRA em ONTAP tools for VMware vSphere para ambientes SAN e NAS	3
Configure o SRA nas ONTAP tools para ambientes altamente escaláveis	4
Configure o SRA no appliance VMware Live Site Recovery usando as ONTAP tools	5
Atualizar credenciais SRA nas ferramentas ONTAP	6
Configure sites protegidos e de recuperação nas ferramentas ONTAP	7
Configure os recursos do site protegido e do site de recuperação	9
Verifique os sistemas de armazenamento replicados nas ferramentas ONTAP	13
Proteção contra fan-out em ONTAP tools	13

Proteja armazenamentos de dados e máquinas virtuais

Proteja um cluster de hosts nas ONTAP tools

ONTAP tools for VMware vSphere gerencia a proteção de clusters de hosts. Todos os datastores pertencentes à SVM selecionada e montados em um ou mais hosts do cluster são protegidos sob um cluster de hosts.

Antes de começar

Certifique-se de atender a esses requisitos antes de proteger um cluster de hosts:

- O cluster de hosts contém datastores de uma única SVM.
- Os datastores no cluster de hosts não são montados em hosts fora do cluster.
- Os datastores montados no cluster host são datastores VMFS com protocolo iSCSI ou FC. Você não pode usar vVols, NFS ou datastores VMFS com protocolos NVMe/FC e NVMe/TCP.
- Os armazenamentos de dados baseados em volumes FlexVol/LUN montados em um host não fazem parte de nenhum grupo de consistência.
- Os armazenamentos de dados baseados em volumes FlexVol/LUN montados em um host não fazem parte de nenhum relacionamento SnapMirror.
- O cluster de hosts contém pelo menos um datastore.

Passos

1. Faça login no cliente vSphere.
2. Clique com o botão direito do mouse em um cluster de hosts e selecione **NetApp ONTAP tools > Proteger Cluster**.
3. Na janela de proteção do cluster, o sistema preenche automaticamente o tipo de datastore e os detalhes da máquina virtual de storage (VM) de origem. Selecione o link de datastores para visualizar os datastores protegidos.
4. Selecione **Adicionar relacionamento**.
5. Na janela **Adicionar SnapMirror Relationship**, selecione a **VM de armazenamento de destino** e o tipo de **política**.

O tipo de política pode ser Assíncrono ou AutomatedFailOverDuplex.

Ao adicionar a relação do SnapMirror como uma política do tipo AutomatedFailOverDuplex, você deve adicionar a VM de armazenamento de destino como um backend de armazenamento no mesmo vCenter onde ONTAP tools for VMware vSphere está implantado.

No tipo de política AutomatedFailOverDuplex, existem configurações de host uniformes e não uniformes. Ao selecionar o botão de alternância **Configuração de host uniforme**, a configuração do grupo iniciador do host é replicada implicitamente no site de destino. Para mais informações, consulte "[Conceitos e termos-chave](#)".

6. Se optar por uma configuração de host não uniforme, selecione o acesso ao host (origem/destino) para cada host dentro desse cluster.

7. Selecione **Add**.
8. Você pode editar a proteção do cluster de hosts usando a operação **Modificar proteção do cluster de hosts**. Você pode editar ou excluir os relacionamentos usando as opções do menu de reticências.
9. Selecione o botão **Proteger**.

O sistema cria uma tarefa do vCenter com detalhes do ID do trabalho e mostra seu progresso no painel de tarefas recentes. Esta é uma tarefa assíncrona; a interface de usuário mostra apenas o status de envio da solicitação e não aguarda a conclusão da tarefa.

10. Para visualizar os clusters de hosts protegidos, acesse **NetApp ONTAP tools > Proteção > Relacionamentos de clusters de hosts**. Selecione um grupo de consistência para visualizar sua capacidade, datastores associados e grupos de consistência filhos.



Se você precisar remover a proteção dentro de uma hora após a criação, execute primeiro a descoberta de armazenamento.

Informações relacionadas

["VMware vSphere Metro Storage Cluster \(vMSC\)"](#)

Proteja usando a proteção SRA

Configure o SRA nas ONTAP tools para proteger datastores

ONTAP tools for VMware vSphere oferece a opção de habilitar o recurso SRA para configurar a recuperação de desastres.

Antes de começar

- Você já deve ter configurado sua instância de servidor vCenter e os hosts ESXi.
- Você deveria ter implantado ONTAP tools for VMware vSphere.
- Você deveria ter baixado o arquivo do adaptador SRA `.tar.gz` do ["NetApp site de suporte"](#).
- Você deve ter os mesmos agendamentos personalizados de SnapMirror em ambos os clusters ONTAP de origem e destino antes de executar os fluxos de trabalho do SRA.
- ["Habilite os serviços do ONTAP tools for VMware vSphere"](#) para habilitar a funcionalidade SRA.

Passos

1. Faça login na interface de gerenciamento do VMware Live Site Recovery appliance usando o URL: `https://<srm_ip>:5480`, e então acesse Adaptadores de Replicação de Storage na interface de gerenciamento do VMware Live Site Recovery appliance.
2. Selecione **Novo Adaptador**.
3. Faça o upload do instalador `.tar.gz` do plug-in SRA para o VMware Live Site Recovery.
4. Analise novamente os adaptadores para verificar se os detalhes foram atualizados na página Storage Replication Adapters do VMware Live Site Recovery.



Após um failover, ações como expandir, montar e excluir podem não estar disponíveis para os datastores. Execute a descoberta de datastores para atualizar e exibir as ações apropriadas do menu de contexto.



Após cada operação de reproteção, você deve executar a descoberta de armazenamento em ambos os sites.

Em uma nova configuração com proteção SRA, sempre execute um teste de failover. Ignorar o teste de failover pode fazer com que a operação de reprotect falhe.

Em uma configuração de fan-out, após um failover do SnapMirror Active Sync em que a fonte do SnapMirror muda para o site B para Automated Failover Duplex e Asynchronous SnapMirror, execute um failover de teste entre os sites B e C. Ignorar esta etapa pode resultar em falha na operação de reproteção.

Informações relacionadas

["Configurar a recuperação de desastres para datastores NFS usando o VMware Site Recovery Manager"](#)

Configure o SRA em ONTAP tools for VMware vSphere para ambientes SAN e NAS

Você deve configurar os sistemas de armazenamento antes de executar o Storage Replication Adapter (SRA) para VMware Live Site Recovery.

Configurar o SRA para ambientes SAN



Os grupos de consistência em fluxos de trabalho SRA são suportados apenas com protocolos SAN (iSCSI e Fibre Channel) em sistemas de storage Unified e ASA r2.

Antes de começar

Você deve ter os seguintes programas instalados no site protegido e no site de recuperação:

- VMware Live Site Recovery: o site da VMware fornece documentação de instalação para o VMware Live Site Recovery.

["Sobre o VMware Live Site Recovery"](#)

- SRA: instale o adaptador no VMware Live Site Recovery.

Para configurações do protocolo iSCSI, observe o seguinte antes de executar os fluxos de trabalho do SRA:

- **Site protegido:** os adaptadores de armazenamento iSCSI e os detalhes da LIF de dados são configurados automaticamente ao provisionar datastores. Nenhuma configuração manual é necessária.
- **Local de recuperação:** os adaptadores de storage iSCSI devem ser configurados manualmente em cada host ESXi incluído no mapeamento de recursos para recuperação de desastres. Para evitar configurar adaptadores individualmente em cada host, crie um datastore de espaço reservado do tipo iSCSI no local de recuperação usando a SVM na qual os fluxos de trabalho do SRA estão configurados. Isso adiciona automaticamente o adaptador iSCSI e os endereços IP LIF de dados necessários a todos os hosts ESXi mapeados. Consulte ["Configure armazenamentos de dados de espaço reservado nas ONTAP tools"](#) para mais detalhes.

Passos

1. Verifique se os hosts ESXi primários estão conectados aos LUNs no sistema de storage primário no site protegido.
2. Verifique se os LUNs estão em igroups que têm a `ostype` opção definida como *VMware* no sistema de storage primário.
3. Verifique se os hosts ESXi no site de recuperação possuem conectividade iSCSI e Fibre Channel

apropriada com a storage virtual machine (SVM). Os hosts ESXi do site secundário devem ter acesso ao storage do site secundário, e os hosts ESXi do site primário devem ter acesso ao storage do site primário.

Você pode fazer isso verificando se os hosts ESXi possuem LUNs locais conectados à SVM ou executando o comando `iscsi show initiators` nas SVMs. Verifique o acesso às LUNs mapeadas no host ESXi para verificar a conectividade iSCSI.

Configurar o SRA para ambientes NAS



Grupos de consistência não são suportados para NFS em fluxos de trabalho do SRA. Se volumes de datastore NFS forem colocados em um grupo de consistência e protegidos, a operação Discover Devices falhará. Não use grupos de consistência ao proteger datastores NFS com o SRA.

Antes de começar

Você deve ter os seguintes programas instalados no site protegido e no site de recuperação:

- VMware Live Site Recovery: Você pode encontrar a documentação de instalação do VMware Live Site Recovery no site da VMware. "[Sobre o VMware Live Site Recovery](#)"
- SRA: instale o adaptador no VMware Live Site Recovery e no servidor SRA.

Passos

1. Verifique se os armazenamentos de dados no site protegido contêm máquinas virtuais registradas no vCenter Server.
2. Verifique se os hosts ESXi no site protegido montaram os volumes de exportação NFS da storage virtual machine (SVM).
3. Verifique se os endereços IP válidos nos quais as exportações NFS estão presentes estão especificados no campo **Endereços NFS** ao usar o assistente do Array Manager para adicionar arrays ao VMware Live Site Recovery. Não use o nome do host NFS ou o FQDN no campo **Endereços NFS**.
4. Use o comando `ping` em cada host ESXi no site de recuperação para verificar se o host possui uma porta VMkernel que pode acessar os endereços IP usados para fornecer exports NFS da SVM.

Configure o SRA nas ONTAP tools para ambientes altamente escaláveis

Você deve configurar os intervalos de tempo limite de armazenamento de acordo com as configurações recomendadas para o Storage Replication Adapter (SRA) para obter o melhor desempenho em ambientes de alta escalabilidade.

Configurações do provedor de armazenamento

Você deve definir os seguintes valores de tempo limite no VMware Live Site Recovery para ambientes dimensionados:

Configurações avançadas	Valores de tempo limite
<code>StorageProvider.resignatureTimeout</code>	Aumente o valor da configuração de 900 segundos para 12000 segundos.
<code>storageProvider.hostRescanDelaySec</code>	60

<code>storageProvider.hostRescanRepeatCnt</code>	20
<code>storageProvider.hostRescanTimeoutSec</code>	Defina um valor alto (por exemplo: 99999)

Você também deve habilitar a `StorageProvider.autoResignatureMode` opção.

Consulte ["Alterar configurações do provedor de armazenamento"](#) para obter mais informações sobre como modificar as configurações do Storage Provider.

Configurações de armazenamento

Quando você atingir um tempo limite, aumente os valores de `storage.commandTimeout` e `storage.maxConcurrentCommandCnt` para um valor mais alto.



O intervalo de tempo limite especificado é o valor máximo. Não é necessário esperar que o tempo limite máximo seja atingido. A maioria dos comandos termina dentro do intervalo de tempo limite máximo definido.

Consulte ["Alterar configurações de armazenamento"](#) para modificar as configurações do provedor SAN.

Configure o SRA no appliance VMware Live Site Recovery usando as ONTAP tools

Após implantar o appliance VMware Live Site Recovery, configure o Storage Replication Adapter (SRA) para habilitar o gerenciamento de recuperação de desastres.

Configurar o SRA no appliance VMware Live Site Recovery salva as credenciais das ONTAP tools for VMware vSphere dentro do appliance, permitindo a comunicação entre o VMware Live Site Recovery e o SRA.

Antes de começar

- Baixe o arquivo `.tar.gz` do ["NetApp site de suporte"](#).
- Habilite os serviços SRA no ONTAP tools Manager. Para obter mais informações, consulte a ["Habilitar serviços"](#) seção.
- Adicione servidores vCenter à appliance ONTAP tools for VMware vSphere. Para obter mais informações, consulte a ["Adicionar servidores vCenter"](#) seção.
- Adicione backends de armazenamento às ONTAP tools for VMware vSphere. Para obter mais informações, consulte a ["Adicionar backends de armazenamento"](#) seção.



Se você aplicou o patch de certificado do vCenter das ONTAP tools, atualize a configuração do vCenter no appliance VMware Live Site Recovery usando a porta (:5480). Para obter instruções, consulte ["Reconfigure o appliance do Site Recovery Manager"](#).

Passos

1. Na tela do appliance VMware Live Site Recovery, selecione **Storage Replication Adapter > New Adapter**.
2. Faça o upload do arquivo `.tar.gz` para o VMware Live Site Recovery.
3. Faça login no appliance VMware Live Site Recovery usando uma conta de administrador por meio de um cliente SSH, como o PuTTY.

4. Alterne para o usuário raiz usando o comando: `su root`
5. Execute o comando `cd /var/log/vmware/srm` para acessar o diretório de logs.
6. No local do log, insira o comando para obter o docker id usado pelo SRA: `docker ps -l`
7. Para fazer login no ID do contêiner, digite o comando: `docker exec -it -u srm <container id> sh`
8. Configure o VMware Live Site Recovery com o endereço IP e a senha das ONTAP tools for VMware vSphere usando o comando: `perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <Application username> --otv-password <Application password> --vcenter-guid <VCENTER_GUID>`
 - Forneça a senha entre aspas simples para que o script Perl trate os caracteres especiais como parte da senha, não como delimitadores.
 - Você pode definir o nome de usuário e a senha do aplicativo (VASA Provider/SRA) no ONTAP tools Manager ao habilitar esses serviços pela primeira vez. Use essas credenciais para registrar o SRA no VMware Live Site Recovery.
 - Para localizar o GUID do vCenter, vá para a página do servidor vCenter em ONTAP tools Manager após adicionar sua instância do vCenter. Consulte a seção ["Adicionar servidores vCenter"](#).
9. Verifique novamente os adaptadores para confirmar que os detalhes atualizados aparecem na página Adaptadores de Replicação de Storage do VMware Live Site Recovery.

Resultados Uma mensagem de confirmação é exibida, indicando que as credenciais de armazenamento foram salvas. Agora você pode usar o SRA para se comunicar com o servidor SRA usando o endereço IP, a porta e as credenciais especificadas.

Atualizar credenciais SRA nas ferramentas ONTAP

Para que o VMware Live Site Recovery se comunique com o SRA, você deve atualizar as credenciais do SRA no servidor VMware Live Site Recovery caso as tenha modificado.

Antes de começar

Você deveria ter executado os passos mencionados no tópico ["Configurando o SRA no appliance VMware Live Site Recovery"](#).

Passos

1. Execute os seguintes comandos para excluir as credenciais armazenadas em cache das ferramentas ONTAP da máquina VMware Live Site Recovery:
 - a. `sudo su <enter root password>`
 - b. `docker ps`
 - c. `docker exec -it <container_id> sh`
 - d. `cd conf/`
 - e. `rm -rf *`
2. Execute o comando Perl para configurar o SRA com as novas credenciais:
 - a. `cd ..`
 - b. ``perl command.pl -I --otv-ip <OTV_IP>:8443 --otv-username <OTV_ADMIN_USERNAME> --otv`

-password <OTV_ADMIN_PASSWORD> --vcenter-guid <VCENTER_GUID>`Você precisa colocar o valor da senha entre aspas simples.

Uma mensagem de sucesso confirmando que as credenciais de armazenamento foram salvas é exibida. O SRA pode se comunicar com o servidor SRA usando o endereço IP, a porta e as credenciais fornecidas.

Reconfigure vCenter no appliance VMware Live Site Recovery após uma alteração de certificado

Se o certificado do vCenter for alterado, por exemplo, após uma atualização do vCenter, você poderá encontrar um erro de incompatibilidade de impressão digital na extensão Site Recovery. Execute as seguintes etapas para resolvê-lo.

Passos

1. Reconfigure vCenter no appliance VMware Live Site Recovery

- a. Abra a interface de gerenciamento do VMware Live Site Recovery appliance em um navegador:
`https://<SRM_IP>:5480`
- b. Selecione a aba **Resumo**.
- c. Selecione **Reconfigurar** para a conexão do servidor vCenter.

Isso busca e aceita a impressão digital do certificado mais recente de vCenter.

2. Reconectar o emparelhamento do site (se o erro persistir)

Se o erro de incompatibilidade de impressão digital persistir após a reconfiguração:

- a. Faça login na interface de usuário do vCenter.
- b. Acesse a extensão **Site Recovery**.
- c. Localize a seção **Emparelhamento de Sites**.
- d. Selecione **Reconectar** para restabelecer o emparelhamento do site com o certificado atualizado.

Configure sites protegidos e de recuperação nas ferramentas ONTAP

Você deve criar grupos de proteção para proteger um grupo de máquinas virtuais no site protegido.

Ao adicionar um novo datastore, você pode incluí-lo no grupo de datastore existente ou adicionar um novo datastore e criar um novo volume ou grupo de consistência para proteção. Após adicionar um novo datastore a um grupo de consistência ou volume protegido, atualize SnapMirror e execute a descoberta de storage nos sites protegido e de recuperação. Você pode executar a descoberta manualmente ou em um agendamento para garantir que o novo datastore seja detectado e protegido.

Pareie os sites protegidos e de recuperação

Você deve emparelhar os sites protegidos e de recuperação criados usando seu vSphere Client para permitir que o Storage Replication Adapter (SRA) descubra os sistemas de storage.



O Adaptador de Replicação de Armazenamento (SRA) suporta fan-out com um relacionamento síncrono do tipo Automated Failover Duplex e um relacionamento assíncrono SnapMirror em grupo de consistência. No entanto, fan-out com dois relacionamentos assíncronos SnapMirror em grupos de consistência ou relacionamentos de fan-out SnapMirror em volumes não é suportado. Relacionamentos do tipo Vault SnapMirror não são considerados nessas restrições de fan-out. O suporte a grupo de consistência no SRA é limitado a protocolos SAN (iSCSI e fibre channel) em sistemas de armazenamento Unified e ASA r2. Grupos de consistência não são suportados para NFS. Se volumes de datastore NFS forem colocados em um grupo de consistência, a operação de descoberta de dispositivos falhará.

Antes de começar

- Você deve ter o VMware Live Site Recovery instalado nos sites protegidos e de recuperação.
- Você deve ter o SRA instalado nos sites protegidos e de recuperação.

Passos

1. Na página inicial do cliente vSphere, clicar duas vezes no ícone **Recuperação de Site** e depois selecione **Sites**.
2. Selecione **Objetos > Ações > Parear Sites**.
3. Na caixa de diálogo **Emparelhar servidores do Site Recovery Manager**, insira o endereço do Platform Services Controller do site protegido e selecione **Next**.
4. Na seção Selecionar vCenter Server, faça o seguinte:
 - a. Verifique se o servidor vCenter do site protegido aparece como um candidato compatível para emparelhamento.
 - b. Insira as credenciais administrativas do SSO e selecione **Concluir**.
5. Se solicitado, selecione **Sim** para aceitar os certificados de segurança.

Resultado

A caixa de diálogo **Objetos** exibe os sites protegidos e de recuperação.

Configurar grupos de proteção

Antes de começar

Você deve garantir que os sites de origem e destino estejam configurados para o seguinte:

- Mesma versão do VMware Live Site Recovery instalada
- Máquinas virtuais
- Locais protegidos e de recuperação emparelhados
- Os armazenamentos de dados de origem e destino devem ser montados em seus respectivos sites

Passos

1. Faça login no vCenter Server e selecione **Recuperação do Site > Grupos de Proteção**.
2. No painel **Grupos de Proteção**, selecione **Novo**.
3. Especifique um nome e uma descrição para o grupo de proteção, a direção e selecione **Next**.
4. No campo **Tipo**, selecione a opção **Tipo** como grupos de datastore (replicação baseada em array) para datastore NFS e VMFS. O domínio de falha consiste em SVMs com replicação habilitada. As SVMs que possuem apenas o peering implementado e não apresentam problemas são exibidas.

5. Na guia Grupos de replicação, selecione o par de arrays ativado ou os grupos de replicação que têm a máquina virtual que você configurou e, em seguida, selecione **Avançar**.

Todas as máquinas virtuais no grupo de replicação são adicionadas ao grupo de proteção.

6. Você pode selecionar o plano de recuperação existente ou criar um novo selecionando **Adicionar a um novo plano de recuperação**.
7. Na guia Pronto para concluir, revise os detalhes do grupo de proteção que você criou e selecione **Concluir**.

Configure os recursos do site protegido e do site de recuperação

Configure os mapeamentos de rede nas ferramentas ONTAP

Você deve configurar seus mapeamentos de recursos, como redes de máquinas virtuais, hosts ESXi e pastas em ambos os sites para permitir o mapeamento de cada recurso do site protegido para o recurso apropriado no site de recuperação.

Você deve concluir as seguintes configurações de recursos:

- Mapeamentos de rede
- Mapeamento de pastas
- Mapeamentos de recursos
- Datastores de espaço reservado

Antes de começar

Você deveria ter conectado os sites de proteção e de recuperação.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de Rede > Novo** na guia manage para criar um novo mapeamento de rede.
4. No assistente Criar Mapeamento de Rede, faça o seguinte:
 - a. Selecione **Preparar mapeamentos automaticamente para redes com nomes correspondentes** e selecione **Avançar**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Avançar** após os mapeamentos serem criados com sucesso.
 - d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e, em seguida, selecione **Finish**.

Resultado

A página Mapeamentos de Rede exibe os recursos do site protegido e os recursos do site de recuperação. Você pode seguir os mesmos passos para outras redes em seu ambiente.

Configure o mapeamento de pastas nas ferramentas ONTAP

Você deve mapear suas pastas no site protegido e no site de recuperação para permitir a comunicação entre eles.

Antes de começar

Você deveria ter conectado os sites de proteção e de recuperação.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de Pastas > ícone Pasta** na guia Gerenciar para criar um novo mapeamento de pastas.
4. No assistente Criar Mapeamento de Pastas, execute o seguinte:
 - a. Selecione **Preparar mapeamentos automaticamente para pastas com nomes correspondentes** e selecione **Avançar**.
 - b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
 - c. Selecione **Avançar** após os mapeamentos serem criados com sucesso.
 - d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e, em seguida, selecione **Finish**.

Resultado

A página Mapeamento de Pastas exibe os recursos do site protegido e os recursos do site de recuperação. Você pode seguir os mesmos passos para outras pastas em seu ambiente.

Configure os mapeamentos de recursos nas ONTAP tools

Você deve mapear seus recursos no site protegido e no site de recuperação para que as máquinas virtuais sejam configuradas para realizar failover para um grupo de hosts ou outro.

Antes de começar

Você deveria ter conectado os sites de proteção e de recuperação.



No VMware Live Site Recovery, os recursos podem ser pools de recursos, hosts ESXi ou vSphere clusters.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Mapeamentos de Recursos > Novo** na guia manage para criar um novo mapeamento de recursos.
4. No assistente Criar Mapeamento de Recursos, execute o seguinte:
 - a. Selecione **Preparar mapeamentos automaticamente para recursos com nomes correspondentes** e selecione **Avançar**.

- b. Selecione os objetos de data center necessários para os sites protegidos e de recuperação e selecione **Adicionar mapeamentos**.
- c. Selecione **Avançar** após os mapeamentos serem criados com sucesso.
- d. Selecione o objeto usado anteriormente para criar o mapeamento reverso e, em seguida, selecione **Finish**.

Resultado

A página Mapeamento de Recursos exibe os recursos do site protegido e os recursos do site de recuperação. Você pode seguir os mesmos passos para outros recursos em seu ambiente.

Configure armazenamentos de dados de espaço reservado nas ONTAP tools

Configure um datastore de espaço reservado para reservar espaço no inventário do vCenter no site de recuperação para máquinas virtuais (VMs) protegidas. Os datastores de espaço reservado exigem capacidade mínima, pois as VMs de espaço reservado são pequenas e normalmente usam apenas algumas centenas de kilobytes.

Antes de começar

- Certifique-se de que os locais protegidos e de recuperação estejam conectados.
- Verifique se os mapeamentos de recursos foram configurados.

Passos

1. Faça login no vCenter Server e selecione **Recuperação de Site > Sites**.
2. Selecione seu site protegido e selecione **Gerenciar**.
3. Selecione **Datastores de espaço reservado > Novo** na guia gerenciar para criar um novo datastore de espaço reservado.
4. Selecione o datastore apropriado e clique em **OK**.



Os armazenamentos de dados provisórios podem residir em storage local ou remoto, mas não requerem replicação.

5. Repita os passos 3 a 5 para configurar um datastore provisório para o site de recuperação.

Configure o SRA usando o gerenciador de arrays nas ferramentas ONTAP

Você pode configurar o Storage Replication Adapter (SRA) usando o assistente Array Manager do VMware Live Site Recovery para habilitar as interações entre o VMware Live Site Recovery e as storage virtual machines (SVMs).

Antes de começar

- Você deveria ter emparelhado os sites protegidos e os sites de recuperação no VMware Live Site Recovery.
- Você deve ter configurado seu storage integrado antes de configurar o gerenciador de arrays.
- Você deve ter configurado e replicado as relações do SnapMirror entre os sites protegidos e os sites de recuperação.
- Você deveria ter habilitado as LIFs de gerenciamento do SVM para permitir a multilocação.

O SRA oferece suporte ao gerenciamento em nível de cluster e em nível de SVM. Se você adicionar armazenamento em nível de cluster, poderá descobrir e executar operações em todas as SVMs do cluster. Se você adicionar armazenamento em nível de SVM, poderá gerenciar apenas essa SVM específica.

Passos

1. No VMware Live Site Recovery, selecione **Gerenciadores de Array > Adicionar Gerenciador de Array**.
2. Insira as seguintes informações para descrever o array no VMware Live Site Recovery:
 - a. Insira um nome para identificar o gerenciador de arrays no campo **Nome de Exibição**.
 - b. No campo **Tipo de SRA**, selecione **NetApp Storage Replication Adapter for ONTAP**.
 - c. Insira as informações para conectar ao cluster ou à SVM:
 - Se você estiver se conectando a um cluster, você deve inserir a LIF de gerenciamento do cluster.
 - Se você estiver se conectando diretamente a uma SVM, você deve inserir o endereço IP da LIF de gerenciamento da SVM.



Ao configurar o gerenciador de arrays, você deve usar a mesma conexão (endereço IP) para o sistema de storage que foi usada para integrar o sistema de storage em ONTAP tools for VMware vSphere. Por exemplo, se a configuração do gerenciador de arrays estiver no escopo SVM, então o storage em ONTAP tools for VMware vSphere deve ser adicionado no nível SVM.

- d. Ao conectar-se a um cluster, especifique o nome da SVM no campo **Nome da SVM** ou deixe-o em branco para gerenciar todas as SVMs no cluster.
- e. Insira os volumes a serem descobertos no campo **Volume include list**.

Você pode inserir o volume de origem no site protegido e o volume de destino replicado no site de recuperação.

Por exemplo, se você quiser descobrir o volume `src_vol1` que está em uma relação do SnapMirror com o volume `dst_vol1`, você deve especificar `src_vol1` no campo de site protegido e `dst_vol1` no campo de site de recuperação.

- f. **(Opcional)** Insira os volumes a serem excluídos da descoberta no campo **Volume exclude list**.

Você pode inserir o volume de origem no site protegido e o volume de destino replicado no site de recuperação.

Por exemplo, se você quiser excluir o volume `src_vol1` que está em uma relação do SnapMirror com o volume `dst_vol1`, você deve especificar `src_vol1` no campo do site protegido e `dst_vol1` no campo do site de recuperação.

3. Selecione **Next**.
4. Verifique se a matriz foi detectada e exibida na parte inferior da janela Add Array Manager e selecione **Finish**.

Você pode seguir os mesmos passos para o site de recuperação usando os endereços IP de gerenciamento SVM e credenciais apropriados. Na tela Habilitar Pares de Arrays do assistente Adicionar Gerenciador de Arrays, você deve verificar se o par de arrays correto está selecionado e se ele aparece como pronto para ser habilitado.

Verifique os sistemas de armazenamento replicados nas ferramentas ONTAP

Você deve verificar se o site protegido e o site de recuperação foram emparelhados com sucesso após configurar o Storage Replication Adapter (SRA). O sistema de storage replicado deve ser detectável tanto pelo site protegido quanto pelo site de recuperação.

Antes de começar

- Você deveria ter configurado seu sistema de storage.
- Você deveria ter emparelhado o site protegido e o site de recuperação usando o gerenciador de arrays do VMware Live Site Recovery.
- Você deve ter habilitado a licença FlexClone e a licença SnapMirror antes de executar a operação de failover de teste e a operação de failover para SRA.
- Você deve ter as mesmas políticas e cronogramas de SnapMirror nos sites de origem e de destino.
- Se você estiver usando políticas personalizadas do SnapMirror com um agendamento personalizado, deverá configurar o mesmo agendamento e a mesma política nos sites protegidos e de recuperação.
- Se você estiver usando políticas personalizadas do SnapMirror (com agendamento padrão ou personalizado), deverá realizar a descoberta de storage a partir das ONTAP tools para que a nova política seja reconhecida. Sem isso, os fluxos de trabalho do SRA, incluindo test failover e failover, falharão. Realize a descoberta de storage nos seguintes pontos:
 - Após criar a política personalizada no site de recuperação.
 - Após uma operação de re proteção, que recria a política no site protegido.

Passos

1. Faça login no seu vCenter Server.
2. Acesse **Recuperação de Site > Replicação Baseada em Array**.
3. Selecione o par de matrizes desejado e verifique os detalhes correspondentes.

Os sistemas de armazenamento devem ser detectados no site protegido e no site de recuperação com o status **Enabled**.

Proteção contra fan-out em ONTAP tools

Em um cenário de proteção fan-out, o grupo de consistência é duplamente protegido com um relacionamento síncrono no primeiro destino ONTAP cluster e com um relacionamento assíncrono no segundo destino ONTAP cluster. Os fluxos de trabalho de criação, edição e exclusão de proteção ativa de SnapMirror mantêm a proteção síncrona. Os fluxos de trabalho de failover e re proteção do appliance VMware Live Site Recovery mantêm a proteção assíncrona.



O recurso Fan-out não é suportado para usuários de SVM.

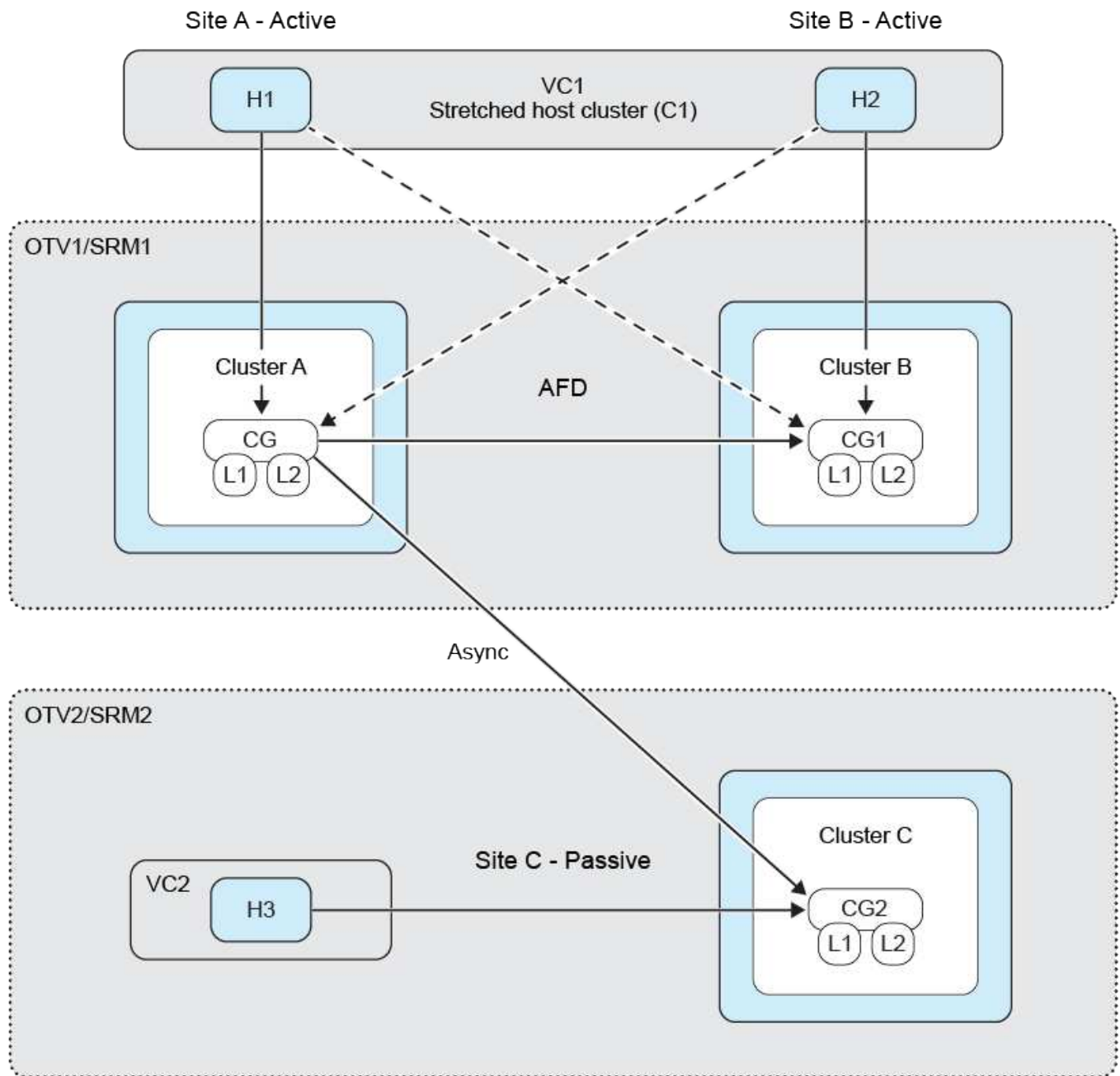
Para configurar a proteção contra dispersão (fan-out), faça o peering dos três clusters do site e das SVMs.

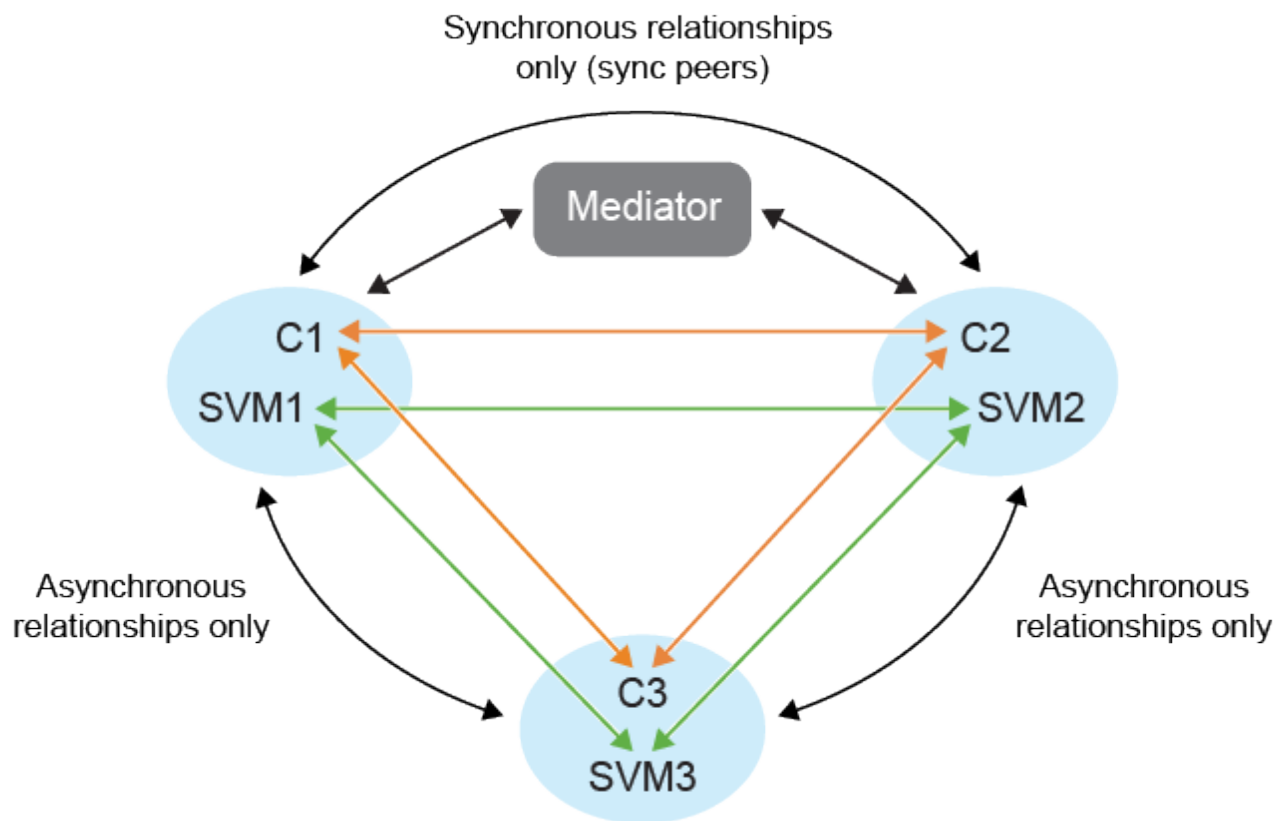
Exemplo:

Se	então
----	-------

• O grupo de consistência de origem está no cluster c1 e SVM svm1 • O primeiro grupo de consistência de destino está no cluster c2 e SVM svm2 e • O segundo grupo de consistência de destino está no cluster c3 e SVM svm3	• O peering de cluster no cluster ONTAP de origem será (C1, C2) e (C1, C3). • O peering de cluster no primeiro cluster ONTAP de destino será (C2, C1) e (C2, C3) e • O peering de cluster no segundo cluster ONTAP de destino será (C3, C1) e (C3, C2). • O peering SVM na SVM de origem será (svm1, svm2) e (svm1, svm3). • O peering SVM no primeiro SVM de destino será (svm2, svm1) e (svm2, svm3) e • O peering SVM no segundo destino svm será (svm3, svm1) e (svm3, svm2).
--	--

O diagrama a seguir mostra a configuração de proteção contra dispersão (fan-out):





Passos

1. Selecione um novo repositório de dados provisório. Os critérios de seleção do repositório de dados provisório para proteção faseada são:
 - Não coloque o datastore placeholder no cluster de hosts que você está protegendo.
 - Se precisar incluir o datastore placeholder no cluster de hosts, adicione-o ao appliance do VMware Live Site Recovery antes de configurar a proteção de sincronização ativa do SnapMirror. Com essa configuração, você pode deixar o datastore placeholder fora da proteção.

Para obter mais informações, consulte ["Selecione um datastore de espaço reservado"](#)

2. Adicione armazenamentos de dados à proteção do cluster de hosts seguindo ["Modificar cluster de hosts protegidos"](#). Adicione tipos de política assíncrona e síncrona.

Informações sobre direitos autorais

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

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

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