



# **VMware Site Recovery Manager com ONTAP**

Enterprise applications

NetApp  
February 11, 2026

# Índice

VMware Site Recovery Manager com ONTAP . . . . .	1
Recuperação do site ao vivo da VMware com o ONTAP . . . . .	1
Por que usar o ONTAP com VLSR ou SRM? . . . . .	1
Como o VLSR utiliza o ONTAP 9 . . . . .	2
VLSR com ONTAP e outros casos de uso: Nuvem híbrida e migração . . . . .	2
Práticas recomendadas de implantação . . . . .	3
Use a versão mais recente das ferramentas do ONTAP 10 . . . . .	3
Layout e segmentação do SVM para SMT . . . . .	3
Práticas recomendadas para gerenciamento de sistemas ONTAP 9 . . . . .	3
Práticas recomendadas operacionais . . . . .	4
Armazenamentos de dados e protocolos . . . . .	4
Sobre os pares de array . . . . .	5
Sobre os grupos de replicação . . . . .	6
Sobre grupos de proteção . . . . .	6
Sobre planos de recuperação . . . . .	7
Failover de teste . . . . .	7
Considerações sobre failover . . . . .	7
Reproteger . . . . .	8
Fallback . . . . .	8
Reproteger o site original . . . . .	8
Topologias de replicação . . . . .	8
Layouts SnapMirror suportados . . . . .	9
Suporte VMFS com sincronização ativa SnapMirror . . . . .	11
Layouts do Array Manager compatíveis . . . . .	12
Esquemas não suportados . . . . .	13
Cascata de SnapMirror . . . . .	14
SnapMirror e SnapVault . . . . .	15
Uso de Qtrees em ambientes do Site Recovery Manager . . . . .	17
Ambientes FC e iSCSI mistos . . . . .	17
Solução de problemas do VLSRM/SRM ao usar a replicação do vVols . . . . .	18
Informações adicionais . . . . .	19

# VMware Site Recovery Manager com ONTAP

## Recuperação do site ao vivo da VMware com o ONTAP

O ONTAP tem sido uma solução de armazenamento líder para o VMware vSphere e, mais recentemente, para o Cloud Foundation, desde que o ESX foi introduzido em datacenters modernos há mais de duas décadas. A NetApp continua a introduzir sistemas inovadores, como a última geração da série ASA A, juntamente com recursos como a sincronização ativa SnapMirror. Esses avanços simplificam o gerenciamento, aumentam a resiliência e reduzem o custo total de propriedade (TCO) da sua infraestrutura de TI.

Este documento apresenta a solução ONTAP para VMware Live Site Recovery (VLSR), anteriormente conhecido como Site Recovery Manager (SRM), o software de recuperação de desastres (DR) líder do setor da VMware, incluindo as informações mais recentes sobre o produto e as melhores práticas para otimizar a implantação, reduzir riscos e simplificar o gerenciamento contínuo.



Esta documentação substitui o relatório técnico publicado anteriormente *TR-4900: VMware Site Recovery Manager com ONTAP*

As práticas recomendadas complementam outros documentos, como guias e ferramentas de compatibilidade. Eles são desenvolvidos com base em testes de laboratório e extensa experiência de campo por engenheiros e clientes da NetApp. Em alguns casos, as melhores práticas recomendadas podem não ser a opção certa para o seu ambiente; no entanto, geralmente são as soluções mais simples que atendem às necessidades da maioria dos clientes.

Este documento se concentra nos recursos das versões recentes do ONTAP 9 quando usado em conjunto com as ferramentas do ONTAP para VMware vSphere 10,4 (que inclui o adaptador de replicação de armazenamento NetApp [SRA] e o provedor VASA [VP]), bem como o VMware Live Site Recovery 9.

### Por que usar o ONTAP com VLSR ou SRM?

As plataformas de gerenciamento de dados da NetApp com tecnologia ONTAP são algumas das soluções de armazenamento mais amplamente adotadas para VLSR. Os motivos são muitos: uma plataforma de gerenciamento de dados segura, de alto desempenho e com protocolo unificado (NAS e SAN juntos) que fornece eficiência de armazenamento que define o setor, multilocação, controles de qualidade de serviço, proteção de dados com instantâneos com eficiência de espaço e replicação com SnapMirror. Tudo isso aproveitando a integração nativa de multi-nuvem híbrida para a proteção de cargas de trabalho do VMware e uma infinidade de ferramentas de automação e orquestração ao seu alcance.

Ao usar o SnapMirror para replicação baseada em array, você aproveita uma das tecnologias mais comprovadas e maduras do ONTAP. O SnapMirror oferece a vantagem de transferências de dados seguras e altamente eficientes, copiando apenas blocos alterados do sistema de arquivos, não VMs ou armazenamentos de dados inteiros. Mesmo esses blocos aproveitam a economia de espaço, como desduplicação, compactação e compactação. Os sistemas ONTAP modernos agora usam o SnapMirror independente de versão, permitindo flexibilidade na seleção de seus clusters de origem e destino. O SnapMirror realmente se tornou uma das ferramentas mais poderosas disponíveis para recuperação de desastres.

Não importa se você usa armazenamentos de dados tradicionais NFS, iSCSI ou Fibre Channel (agora com suporte para armazenamentos de dados vVols), o VLSR fornece uma oferta primária robusta que aproveita o melhor dos recursos do ONTAP para recuperação de desastres ou planejamento e orquestração de migração

de datacenter.

## Como o VLSR utiliza o ONTAP 9

O VLSR aproveita as tecnologias avançadas de gerenciamento de dados dos sistemas ONTAP integrando-se às ferramentas do ONTAP para VMware vSphere, um dispositivo virtual que inclui três componentes principais:

- O plug-in do ONTAP Tools vCenter, anteriormente conhecido como VSC (Virtual Storage Console), simplifica o gerenciamento de storage e os recursos de eficiência, aprimora a disponibilidade e reduz os custos de storage e a sobrecarga operacional, não importa se você está usando SAN ou nas. Ele usa as práticas recomendadas para provisionar armazenamentos de dados e otimiza as configurações de host ESXi para ambientes de storage de bloco e NFS. Para todos esses benefícios, a NetApp recomenda esse plug-in ao usar o vSphere com sistemas que executam o ONTAP.
- O provedor VASA (ONTAP Tools) oferece suporte à estrutura VMware vStorage APIs for Storage Awareness (VASA). O provedor VASA conecta o vCenter Server com o ONTAP para auxiliar no provisionamento e monitoramento do armazenamento de VM. Isso permitiu o suporte ao VMware Virtual volumes (vVols), o gerenciamento de políticas de storage de VM e o desempenho individual do VM vVols. Ele também fornece alarmes para monitorar a capacidade e conformidade com os perfis.
- O SRA é usado em conjunto com o VLSR para gerenciar a replicação de dados de VM entre locais de produção e recuperação de desastres para armazenamentos de dados VMFS e NFS tradicionais e também para testes sem interrupções de réplicas de DR. Ele ajuda a automatizar as tarefas de descoberta, recuperação e re proteção. Ele inclui um dispositivo de servidor SRA e adaptadores SRA para o servidor Windows SRM e o dispositivo VLSR.

Depois de instalar e configurar os adaptadores SRA no servidor VLSR para proteger armazenamentos de dados não vVols, você pode começar a tarefa de configurar seu ambiente vSphere para recuperação de desastres.

O SRA oferece uma interface de comando e controle para o servidor VLSR gerenciar os volumes ONTAP FlexVol que contêm suas máquinas virtuais (VMs) da VMware, bem como a replicação do SnapMirror que os protege.

A VLSR pode testar seu plano de DR sem interrupções usando a tecnologia FlexClone proprietária da NetApp para fazer clones quase instantâneos de seus armazenamentos de dados protegidos em seu site de DR. O VLSR cria um sandbox para testes seguros, para que sua organização e seus clientes estejam protegidos em caso de um desastre real, dando a você confiança na capacidade de sua organização de executar um failover durante um desastre.

No caso de um verdadeiro desastre ou mesmo de uma migração planejada, o VLSR permite que você envie quaisquer alterações de última hora para o conjunto de dados por meio de uma atualização final do SnapMirror (se você optar por fazê-lo). Em seguida, ele quebra o espelho e monta o datastore em seus hosts de DR. Nesse ponto, suas VMs podem ser automaticamente ativadas em qualquer ordem de acordo com sua estratégia pré-planejada.

 Embora os sistemas ONTAP permitam emparelhar SVMs no mesmo cluster para replicação do SnapMirror, esse cenário não é testado e certificado com o VLSR. Portanto, é recomendável usar apenas SVMs de diferentes clusters ao usar o VLSR.

## VLSR com ONTAP e outros casos de uso: Nuvem híbrida e migração

A integração da sua implantação de VLSR com os recursos avançados de gerenciamento de dados do ONTAP permite escala e desempenho significativamente melhores quando comparado com opções de

armazenamento local. Mas mais do que isso, ele traz a flexibilidade da nuvem híbrida. A nuvem híbrida permite que você economize dinheiro ao hierarquizar blocos de dados não utilizados do seu array de alto desempenho para o seu hiperescalador preferido usando o FabricPool, que pode ser um armazenamento S3 local, como o NetApp StorageGRID. Você também pode usar o SnapMirror para sistemas baseados em borda com ONTAP Select definido por software ou DR baseado em nuvem usando "["Armazenamento NetApp no Equinix Metal"](#)", ou outros serviços ONTAP hospedados.

Depois, você pode executar failover de teste no data center de um fornecedor de serviços de nuvem com espaço físico de storage quase zero graças ao FlexClone. Proteger sua organização agora pode custar menos do que nunca.

O VLSR também pode ser usado para executar migrações planejadas utilizando o SnapMirror para transferir eficientemente suas VMs de um data center para outro ou até mesmo dentro do mesmo data center, seja seu, ou por meio de qualquer número de provedores de serviços parceiros da NetApp.

## Práticas recomendadas de implantação

As seções a seguir descrevem as práticas recomendadas de implantação com o ONTAP e o VMware SRM.

### Use a versão mais recente das ferramentas do ONTAP 10

O ONTAP Tools 10 fornece melhorias significativas em relação às versões anteriores, incluindo o seguinte:

- failover de teste 8xx mais rápido\*
- limpeza e repreção 2xx mais rápidas\*
- failover 32% mais rápido\*
- Maior escala
- Suporte nativo para layouts de site compartilhados

\*Essas melhorias são baseadas em testes internos e podem variar de acordo com o seu ambiente.

### Layout e segmentação do SVM para SMT

Com o ONTAP, o conceito de máquina virtual de storage (SVM) fornece segmentação rigorosa em ambientes multitenant seguros. Os usuários do SVM em um SVM não podem acessar ou gerenciar recursos de outro. Dessa forma, você pode utilizar a tecnologia ONTAP criando SVMs separadas para diferentes unidades de negócios que gerenciam seus próprios fluxos de trabalho SRM no mesmo cluster para maior eficiência geral de storage.

Considere o gerenciamento do ONTAP usando contas com escopo SVM e LIFs de gerenciamento de SVM para aprimorar não apenas os controles de segurança, mas também a performance. O desempenho é inherentemente maior ao usar conexões com escopo SVM, pois o SRA não é necessário para processar todos os recursos em um cluster inteiro, incluindo recursos físicos. Em vez disso, ele só precisa entender os ativos lógicos que são abstraídos para o SVM específico.

### Práticas recomendadas para gerenciamento de sistemas ONTAP 9

Como mencionado anteriormente, você pode gerenciar clusters do ONTAP usando credenciais de escopo do cluster ou SVM e LIFs de gerenciamento. Para um desempenho ideal, você pode considerar o uso de credenciais com escopo SVM sempre que não estiver usando vVols. No entanto, ao fazer isso, você deve

estar ciente de alguns requisitos, e que você perde alguma funcionalidade.

- A conta padrão do vsadmin SVM não tem o nível de acesso necessário para executar tarefas de ferramentas do ONTAP. Portanto, você precisa criar uma nova conta SVM. ["Configurar as funções de usuário do ONTAP e o Privileges"](#) Usando o arquivo JSON incluído. Isso pode ser usado para contas com escopo de SVM ou cluster.
- Como o plug-in da IU do vCenter, o provedor VASA e o servidor SRA são todos microsserviços totalmente integrados, você deve adicionar armazenamento ao adaptador SRA no SRM da mesma forma que você adiciona armazenamento na IU do vCenter para ferramentas do ONTAP. Caso contrário, o servidor SRA pode não reconhecer as solicitações enviadas do SRM através do adaptador SRA.
- A verificação de caminho NFS não é realizada ao usar credenciais com escopo SVM, a menos que você primeiro ["clusters integrados"](#) no Gerenciador de ferramentas do ONTAP e associe-as a vCenters. Isso ocorre porque a localização física é logicamente abstraída do SVM. No entanto, isso não é motivo de preocupação, já que os sistemas ONTAP modernos não sofrem mais nenhum declínio de desempenho perceptível ao usar caminhos indiretos.
- Economias de espaço agregado devido à eficiência de storage podem não ser relatadas.
- Quando suportado, os espelhos de partilha de carga não podem ser atualizados.
- O log do EMS pode não ser realizado em sistemas ONTAP gerenciados com credenciais de escopo da SVM.

## Práticas recomendadas operacionais

As seções a seguir descrevem as práticas recomendadas operacionais para o storage VMware SRM e ONTAP.

### Armazenamentos de dados e protocolos

- Se possível, sempre use ferramentas do ONTAP para provisionar armazenamentos de dados e volumes. Isso garante que volumes, caminhos de junção, LUNs, grupos, políticas de exportação e outras configurações sejam configurados de maneira compatível.
- O SRM dá suporte a iSCSI, Fibre Channel e NFS versão 3 com ONTAP 9 ao usar replicação baseada em array por meio do SRA. O SRM não dá suporte à replicação baseada em array para NFS versão 4,1 com datastores tradicionais ou vVols.
- Para confirmar a conectividade, verifique sempre se é possível montar e desmontar um novo datastorer de teste no local de DR do cluster do ONTAP de destino. Teste cada protocolo que você pretende usar para a conectividade do datastorer. Uma prática recomendada é usar as ferramentas do ONTAP para criar seu datastorer de teste, já que ele está fazendo toda a automação do datastorer, conforme indicado pelo SRM.
- Os protocolos SAN devem ser homogêneos para cada local. Você pode misturar NFS e SAN, mas os protocolos SAN não devem ser misturados em um local. Por exemplo, você pode usar FCP no local A e iSCSI no local B. você não deve usar FCP e iSCSI no local A.
- Guias anteriores aconselharam a criação de LIF para localidade de dados. Ou seja, monte sempre um datastorer usando um LIF localizado no nó que possui fisicamente o volume. Embora essa ainda seja a melhor prática, não é mais um requisito nas versões modernas do ONTAP 9. Sempre que possível, e se forem dadas credenciais com escopo de cluster, as ferramentas do ONTAP ainda escolherão o balanceamento de carga entre LIFs locais para os dados, mas não será um requisito de alta disponibilidade ou desempenho.
- O ONTAP 9 pode ser configurado para remover automaticamente snapshots para preservar o tempo de atividade em caso de uma condição fora do espaço quando o dimensionamento automático não é capaz de fornecer capacidade de emergência suficiente. A configuração padrão para esse recurso não exclui

automaticamente os snapshots criados pelo SnapMirror. Se os snapshots do SnapMirror forem excluídos, o NetApp SRA não poderá reverter e resincronizar a replicação para o volume afetado. Para evitar que o ONTAP elimine instantâneos do SnapMirror, configure a capacidade de instantâneos para "tentar".

```
snap autodelete modify -volume -commitment try
```

- O dimensionamento automático de volume deve ser definido como `grow` para volumes que contêm armazenamentos de dados SAN e `grow_shrink` para armazenamentos de dados NFS. Saiba mais sobre este tópico em "[Configure volumes para aumentar e diminuir automaticamente o tamanho](#)".
- O SRM tem melhor desempenho quando o número de datastors e, portanto, os grupos de proteção são minimizados em seus planos de recuperação. Portanto, você deve considerar a otimização para a densidade da VM em ambientes protegidos pelo SRM, onde o rto é de importância fundamental.
- Use o DRS (Distributed Resource Scheduler) para ajudar a equilibrar a carga nos clusters ESXi protegidos e de recuperação. Lembre-se de que, se você planeja fazer o fallback, ao executar uma re proteção, os clusters anteriormente protegidos se tornarão os novos clusters de recuperação. O DRS ajudará a equilibrar a colocação em ambas as direções.
- Sempre que possível, evite usar a personalização de IP com o SRM, pois isso pode aumentar seu rto.

## Sobre os pares de array

Um gerenciador de array é criado para cada par de array. Com as ferramentas SRM e ONTAP, cada emparelhamento de array é feito com o escopo de uma SVM, mesmo que você esteja usando credenciais de cluster. Isso permite segmentar fluxos de trabalho de DR entre locatários com base em quais SVMs eles foram atribuídos a gerenciar. Você pode criar vários gerenciadores de array para um determinado cluster, e eles podem ser assimétricos. Você pode fazer fan-out ou fan-out entre diferentes clusters do ONTAP 9. Por exemplo, você pode fazer a replicação do SVM-A e do SVM-B no Cluster-1 para SVM-C no Cluster-2, SVM-D no Cluster-3 ou vice-versa.

Ao configurar pares de matrizes no SRM, deve sempre adicioná-los no SRM da mesma forma que os adicionou às Ferramentas do ONTAP, ou seja, devem utilizar o mesmo nome de utilizador, palavra-passe e LIF de gestão. Esse requisito garante que o SRA se comunique adequadamente com o array. A captura de tela a seguir ilustra como um cluster pode aparecer nas Ferramentas do ONTAP e como ele pode ser adicionado a um gerenciador de array.

Storage Systems

Name	Type	IP Address
cluster2	Cluster	cluster2.demo.netapp.com

## Edit Local Array Manager

Enter a name for the array manager on "vc2.demo.netapp.com":

vc2\_array\_manager

Storage Array Parameters

Storage Management IP Address or Hostname

cluster2 demo.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

## Sobre os grupos de replicação

Os grupos de replicação contêm coleções lógicas de máquinas virtuais que são recuperadas juntas. Como a replicação do ONTAP SnapMirror ocorre no nível do volume, todas as VMs em um volume estão no mesmo grupo de replicação.

Há vários fatores a serem considerados nos grupos de replicação e como você distribui VMs pelos volumes do FlexVol. Agrupar VMs semelhantes no mesmo volume pode aumentar a eficiência de storage com sistemas ONTAP mais antigos que não possuem deduplicação em nível de agregado, mas o agrupamento aumenta o tamanho do volume e reduz a simultaneidade de e/S do volume. O melhor equilíbrio entre performance e eficiência de storage pode ser obtido em sistemas ONTAP modernos, distribuindo máquinas virtuais por volumes FlexVol no mesmo agregado, aproveitando a deduplicação em nível de agregado e obtendo maior paralelização de e/S em vários volumes. Você pode recuperar VMs nos volumes juntos porque um grupo de proteção (discutido abaixo) pode conter vários grupos de replicação. A desvantagem desse layout é que os blocos podem ser transmitidos por cabo várias vezes, porque o SnapMirror não leva em conta a deduplicação agregada.

Uma consideração final para grupos de replicação é que cada um é, por sua natureza, um grupo de consistência lógica (não deve ser confundido com grupos de consistência SRM). Isso ocorre porque todas as VMs no volume são transferidas juntas usando o mesmo snapshot. Portanto, se você tiver VMs que precisam ser consistentes umas com as outras, considere armazená-las no mesmo FlexVol.

## Sobre grupos de proteção

Os grupos de proteção definem VMs e datastores em grupos que são recuperados juntos do site protegido. O local protegido é onde as VMs configuradas em um grupo de proteção existem durante operações normais de estado estacionário. É importante notar que, embora o SRM possa exibir vários gerenciadores de matriz para um grupo de proteção, um grupo de proteção não pode abranger vários gerenciadores de matriz. Por esse motivo, você não deve estender arquivos de VM entre armazenamentos de dados em diferentes SVMs.

## Sobre planos de recuperação

Os planos de recuperação definem quais grupos de proteção são recuperados no mesmo processo. Vários grupos de proteção podem ser configurados no mesmo plano de recuperação. Além disso, para permitir mais opções para a execução de planos de recuperação, um único grupo de proteção pode ser incluído em vários planos de recuperação.

Os planos de recuperação permitem que os administradores do SRM definam fluxos de trabalho de recuperação atribuindo VMs a um grupo de prioridades de 1 (mais alto) a 5 (mais baixo), sendo 3 (médio) o padrão. Dentro de um grupo de prioridade, as VMs podem ser configuradas para dependências.

Por exemplo, sua empresa pode ter um aplicativo essencial para negócios de nível 1 que depende de um servidor Microsoft SQL para seu banco de dados. Então, você decide colocar suas VMs no grupo de prioridades 1. No grupo de prioridade 1, você começa a Planejar o pedido para abrir serviços. Você provavelmente quer que o controlador de domínio do Microsoft Windows seja inicializado antes do servidor Microsoft SQL, que precisaria estar online antes do servidor de aplicativos, e assim por diante. Você adicionaria todas essas VMs ao grupo de prioridade e, em seguida, definiria as dependências porque as dependências se aplicam somente a um determinado grupo de prioridade.

A NetApp recomenda fortemente que você trabalhe com suas equipes de aplicações para entender a ordem das operações necessárias em um cenário de failover e para construir seus planos de recuperação adequadamente.

## Failover de teste

Como prática recomendada, sempre execute um failover de teste sempre que for feita uma alteração na configuração do storage de VM protegido. Isso garante que, no caso de um desastre, você possa confiar que o Site Recovery Manager pode restaurar serviços dentro do rto esperado.

O NetApp também recomenda confirmar ocasionalmente a funcionalidade do aplicativo in-Guest, especialmente depois de reconfigurar o armazenamento de VM.

Quando uma operação de recuperação de teste é executada, uma rede privada de bolhas de teste é criada no host ESXi para as VMs. No entanto, essa rede não é conectada automaticamente a nenhum adaptador de rede físico e, portanto, não fornece conectividade entre os hosts ESXi. Para permitir a comunicação entre VMs que estão sendo executadas em diferentes hosts ESXi durante o teste de DR, uma rede privada física é criada entre os hosts ESXi no local de DR. Para verificar se a rede de teste é privada, a rede de bolhas de teste pode ser separada fisicamente ou usando VLANs ou marcação de VLAN. Essa rede deve ser segregada da rede de produção porque, à medida que as VMs são recuperadas, elas não podem ser colocadas na rede de produção com endereços IP que podem entrar em conflito com os sistemas de produção reais. Quando um plano de recuperação é criado no SRM, a rede de teste criada pode ser selecionada como a rede privada para conectar as VMs durante o teste.

Depois que o teste tiver sido validado e não for mais necessário, execute uma operação de limpeza. A limpeza em execução retorna as VMs protegidas ao seu estado inicial e redefine o plano de recuperação para o estado Pronto.

## Considerações sobre failover

Há várias outras considerações quando se trata de falhar em um local, além da ordem de operações mencionada neste guia.

Um problema que você pode ter que lidar com as diferenças de rede entre sites. Alguns ambientes podem ser capazes de usar os mesmos endereços IP de rede no local principal e no local de DR. Essa capacidade é

referida como uma LAN virtual (VLAN) estendida ou configuração de rede estendida. Outros ambientes podem ter um requisito para usar endereços IP de rede diferentes (por exemplo, em VLANs diferentes) no local principal em relação ao local de DR.

A VMware oferece várias maneiras de resolver esse problema. Por um lado, tecnologias de virtualização de rede como o VMware NSX-T Data Center abstraem toda a pilha de rede das camadas 2 a 7 do ambiente operacional, permitindo soluções mais portáteis. Saiba mais "["Opções NSX-T com SRM"](#)" sobre o .

O SRM também lhe dá a capacidade de alterar a configuração de rede de uma VM à medida que ela é recuperada. Essa reconfiguração inclui configurações como endereços IP, endereços de gateway e configurações de servidor DNS. Diferentes configurações de rede, que são aplicadas a VMs individuais à medida que são recuperadas, podem ser especificadas nas configurações da propriedade de uma VM no plano de recuperação.

Para configurar o SRM para aplicar diferentes configurações de rede a várias VMs sem ter que editar as propriedades de cada uma no plano de recuperação, a VMware fornece uma ferramenta chamada DR-ip-Customizer. Saiba como usar este utilitário, "["Documentação da VMware"](#)" consulte .

## Reproteger

Após uma recuperação, o local de recuperação se torna o novo local de produção. Como a operação de recuperação quebrou a replicação do SnapMirror, o novo local de produção não fica protegido de nenhum desastre futuro. Uma prática recomendada é proteger o novo local de produção para outro local imediatamente após uma recuperação. Se o local de produção original estiver operacional, o administrador da VMware poderá usar o local de produção original como um novo local de recuperação para proteger o novo local de produção, invertendo efetivamente o sentido de proteção. A re proteção está disponível apenas em falhas não catastróficas. Portanto, os vCenter Servers originais, os servidores ESXi, os servidores SRM e os bancos de dados correspondentes devem ser eventualmente recuperáveis. Se eles não estiverem disponíveis, um novo grupo de proteção e um novo plano de recuperação devem ser criados.

## Failback

Uma operação de failback é fundamentalmente um failover em uma direção diferente do anterior. Como prática recomendada, você verifica se o site original está de volta aos níveis aceitáveis de funcionalidade antes de tentar failback ou, em outras palavras, failover para o site original. Se o local original ainda estiver comprometido, você deve atrasar o failback até que a falha seja suficientemente remediada.

Outra prática recomendada de failback é sempre executar um failover de teste após concluir a re proteção e antes de fazer seu failback final. Isso verifica se os sistemas no local original podem concluir a operação.

## Reproteger o site original

Após o failback, você deve confirmar com todas as partes interessadas que seus serviços foram devolvidos ao normal antes de executar o reprotect novamente,

A execução do reprotect After failback coloca essencialmente o ambiente de volta ao estado em que estava no início, com a replicação do SnapMirror sendo executada novamente do local de produção para o local de recuperação.

## Topologias de replicação

No ONTAP 9, os componentes físicos de um cluster são visíveis para os administradores de cluster, mas não são visíveis diretamente para os aplicativos e hosts que usam o

cluster. Os componentes físicos fornecem um pool de recursos compartilhados a partir do qual os recursos lógicos do cluster são construídos. As aplicações e os hosts acessam dados somente por meio de SVMs que contêm volumes e LIFs.

Cada NetApp SVM é tratado como uma matriz exclusiva no Site Recovery Manager. O VLSR oferece suporte a determinados layouts de replicação de matriz para matriz (ou SVM para SVM).

Uma única VM não pode possuir dados – Virtual Machine Disk (VMDK) ou RDM – em mais de um array VLSR pelos seguintes motivos:

- O VLSR vê apenas o SVM, e não um controlador físico individual.
- Um SVM pode controlar LUNs e volumes que abrangem vários nós em um cluster.

#### **Prática recomendada**

Para determinar a capacidade de suporte, tenha em mente esta regra: Para proteger uma VM usando o VLSR e o NetApp SRA, todas as partes da VM devem existir em apenas uma SVM. Esta regra aplica-se tanto no local protegido como no local de recuperação.

### **Layouts SnapMirror suportados**

As figuras a seguir mostram os cenários de layout de relacionamento do SnapMirror que o VLSR e o SRA suportam. Cada VM nos volumes replicados possui dados em apenas um array VLSR (SVM) em cada local.

### SnapMirror Replication



#### Protected Site

SVM-A1

VM1

#### Recovery Site

SVM-B1

VM1

SVM-A2

VM2

SVM-B2

VM2

### SnapMirror Replication



#### Protected Site

SVM-A1

VM2

VM1

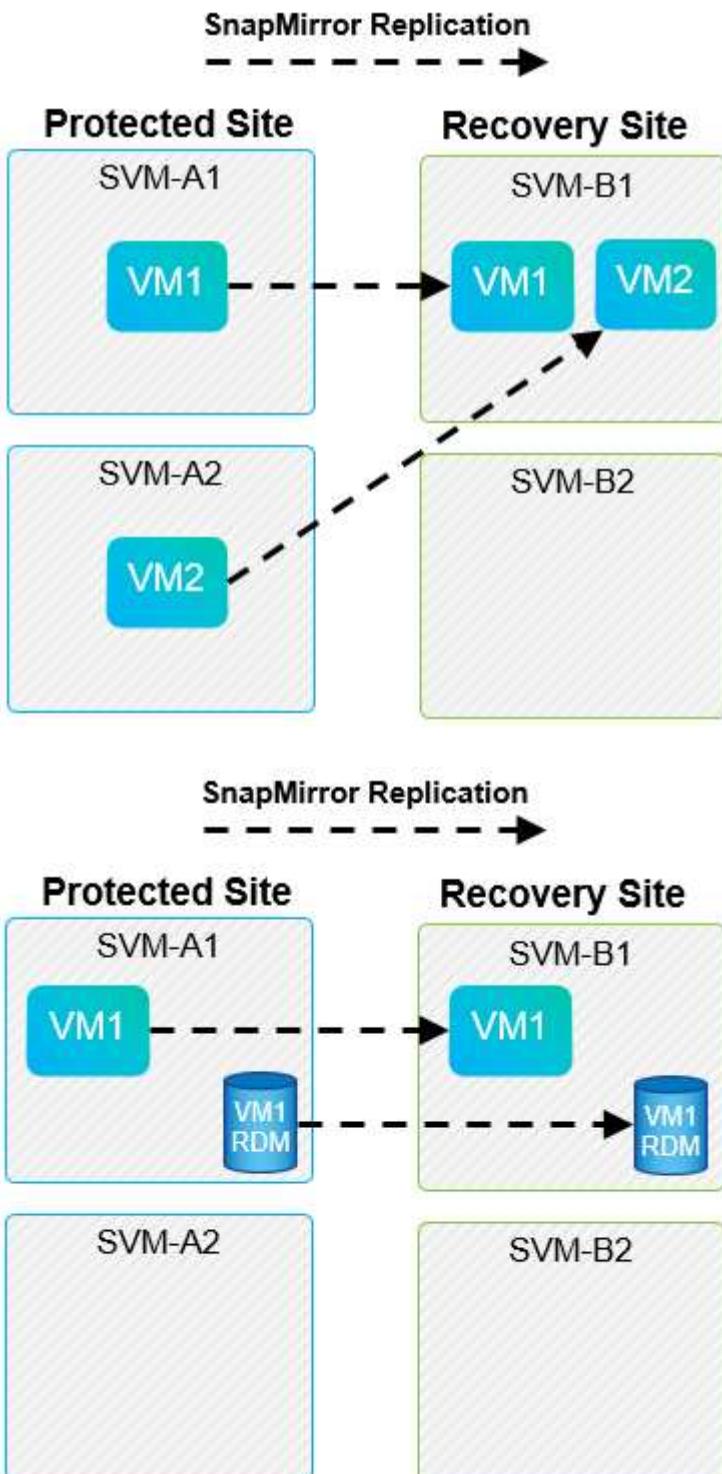
#### Recovery Site

SVM-B1

VM1

SVM-B2

VM2



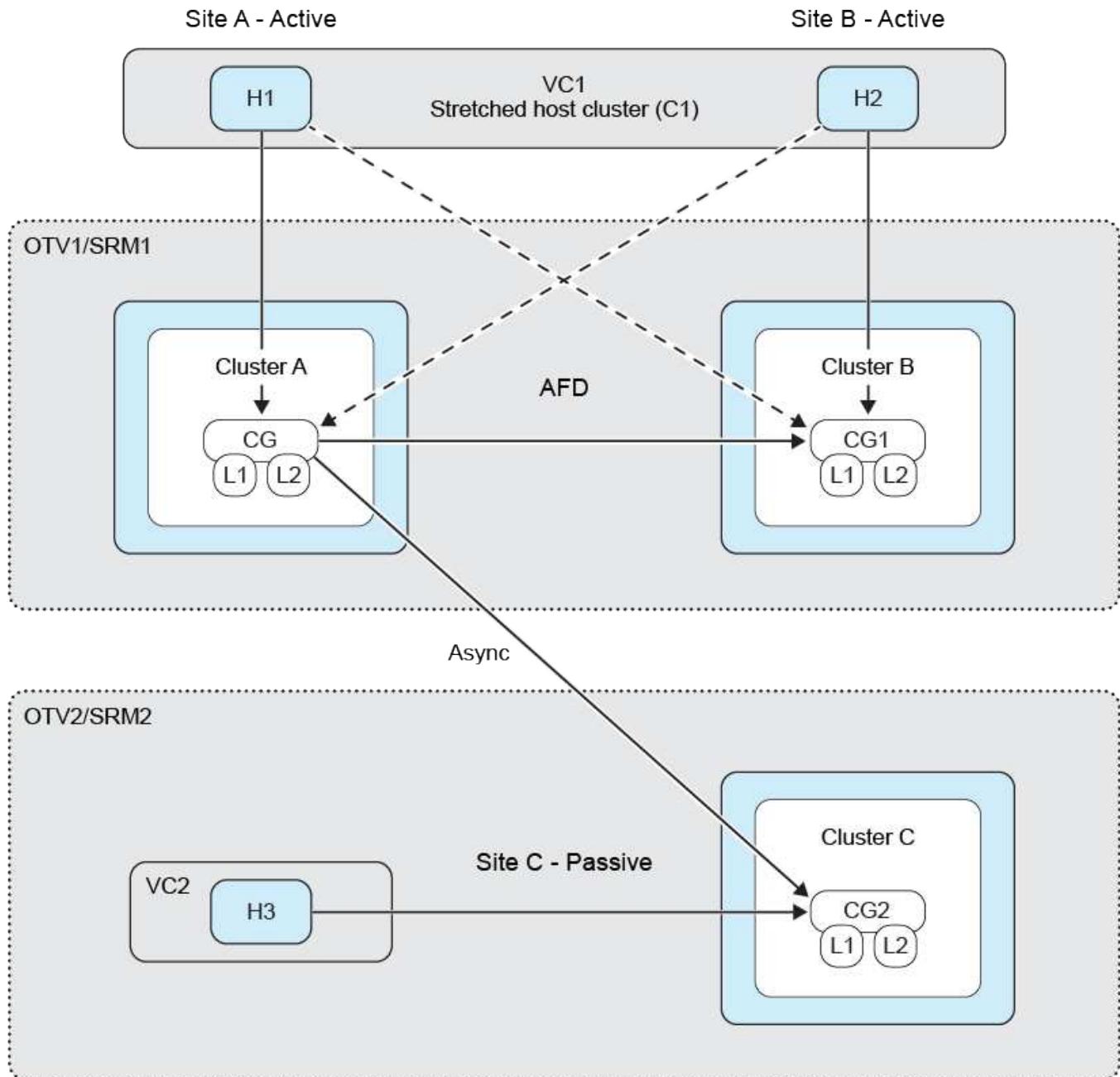
## Suporte VMFS com sincronização ativa SnapMirror

As ferramentas ONTAP 10.3 e posteriores também oferecem suporte à proteção de seus armazenamentos de dados VMFS com sincronização ativa do SnapMirror (SMas). Isso permite failover transparente para continuidade de negócios entre dois datacenters (chamados de domínios de falha) que estão relativamente próximos. A recuperação de desastres de longa distância pode então ser orquestrada usando o SnapMirror de forma assíncrona por meio das ferramentas ONTAP SRA com VLSR.

["Saiba mais sobre a sincronização ativa do ONTAP SnapMirror"](#)

Os armazenamentos de dados são reunidos em um grupo de consistência (CG), e as VMs em todos os armazenamentos de dados permanecerão consistentes na ordem de gravação como membros do mesmo CG.

Alguns exemplos podem ser ter sites em Berlim e Hamburgo protegidos por SMAs e uma terceira réplica de site usando SnapMirror assíncrono e protegido por VLSR. Outro exemplo pode ser proteger locais em Nova York e Nova Jersey usando SMAs, com um terceiro local em Chicago.



## Layouts do Array Manager compatíveis

Quando você usa a replicação baseada em array (ABR) no VLSR, os grupos de proteção são isolados a um único par de array, como mostrado na captura de tela a seguir. Neste cenário, SVM1 e SVM2 são percorridos com SVM3 e SVM4 no local de recuperação. No entanto, você pode selecionar apenas um dos dois pares de

matrizes ao criar um grupo de proteção.

New Protection Group

Type

1 Name and direction

2 Type

3 Datastore groups

4 Recovery plan

5 Ready to complete

Select the type of protection group you want to create:

Datastore groups (array-based replication)  
Protect all virtual machines which are on specific datastores.

Individual VMs (vSphere Replication)  
Protect specific virtual machines, regardless of the datastores.

Virtual Volumes (vVol replication)  
Protect virtual machines which are on replicated vVol storage.

Storage policies (array-based replication)  
Protect virtual machines with specific storage policies.

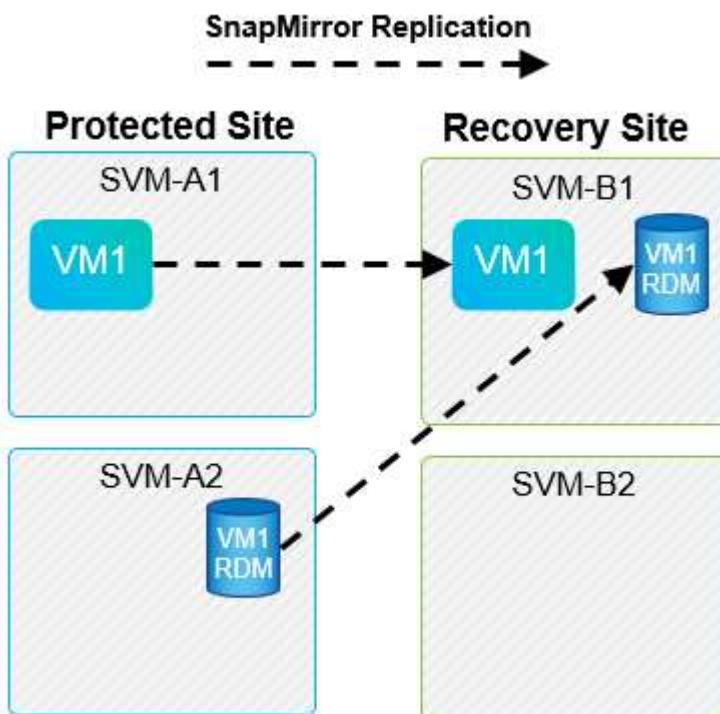
Select array pair

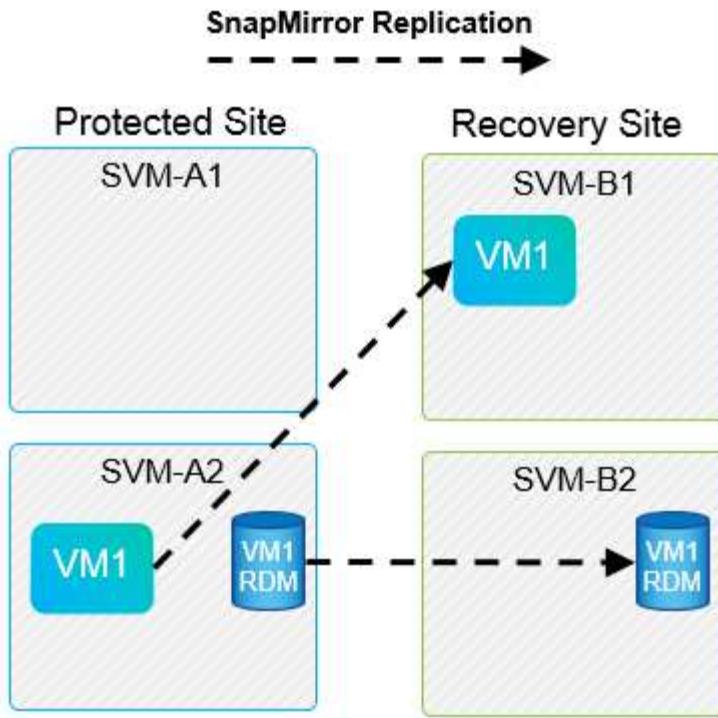
Array Pair	Array Manager Pair
<input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

CANCEL BACK NEXT

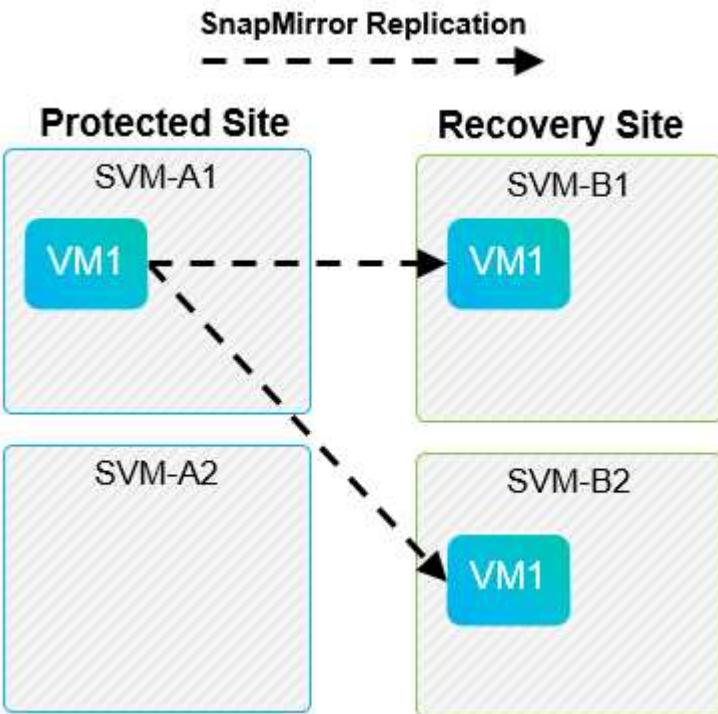
## Esquemas não suportados

Configurações não suportadas têm dados (VMDK ou RDM) em vários SVMs que são de propriedade de uma VM individual. Nos exemplos mostrados nas figuras a seguir, VM1 não pode ser configurado para proteção com VLSR VM1 porque tem dados em dois SVMs.





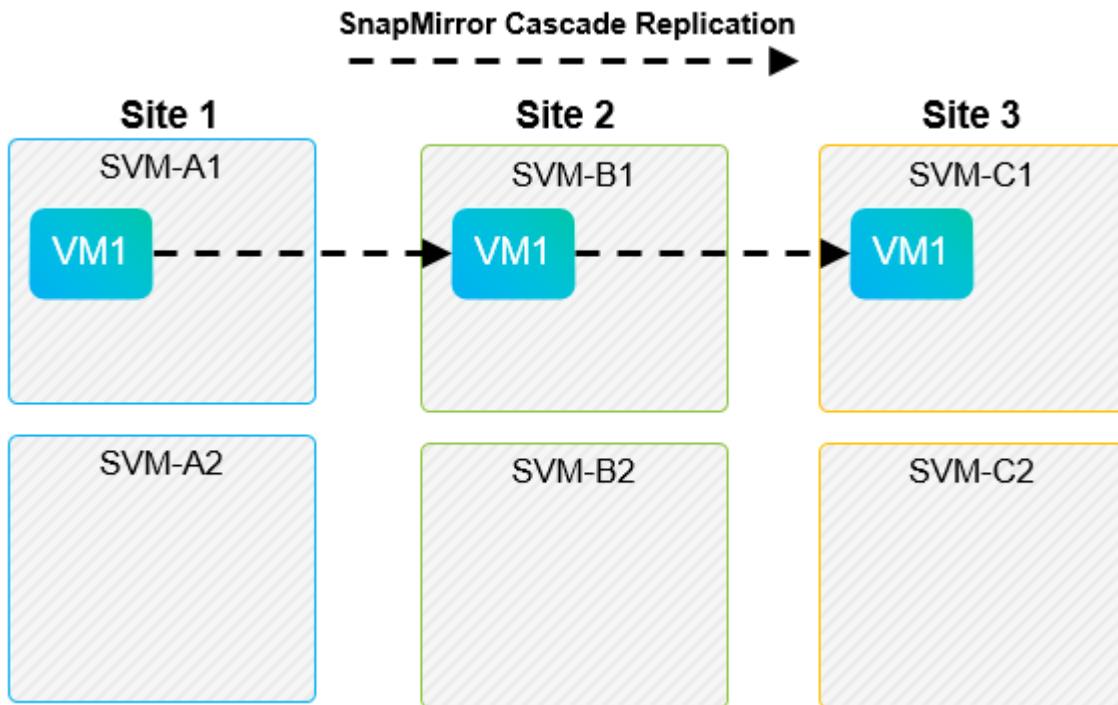
Qualquer relação de replicação na qual um volume de NetApp individual é replicado de uma SVM de origem para vários destinos no mesmo SVM ou em SVMs diferentes é chamada de fan-out do SnapMirror. Fan-out não é suportado com VLSR. No exemplo mostrado na figura a seguir, VM1 não pode ser configurado para proteção no VLSR porque ele é replicado com o SnapMirror para dois locais diferentes.



## Cascata de SnapMirror

O VLSR não oferece suporte a cascata de relacionamentos SnapMirror, nas quais um volume de origem é replicado para um volume de destino e esse volume de destino também é replicado com o SnapMirror para

outro volume de destino. No cenário mostrado na figura a seguir, o VLSR não pode ser usado para failover entre sites.



## SnapMirror e SnapVault

O software NetApp SnapVault permite o backup baseado em disco de dados empresariais entre sistemas de storage NetApp. O SnapVault e o SnapMirror podem coexistir no mesmo ambiente; no entanto, o VLSR suporta o failover apenas das relações SnapMirror.



O NetApp SRA suporta o `mirror-vault` tipo de política.

SnapVault foi reconstruído a partir do zero para ONTAP 8,2. Embora antigos usuários do Data ONTAP 7-Mode devam encontrar semelhanças, grandes melhorias foram feitas nesta versão do SnapVault. Um grande avanço é a capacidade de preservar eficiências de storage de dados primários durante transferências SnapVault.

Uma mudança arquitetônica importante é que o in ONTAP 9 replica no nível de volume em vez de no nível de qtree, como é o caso do SnapVault 7-Mode SnapVault. Essa configuração significa que a origem de um relacionamento do SnapVault deve ser um volume e esse volume deve ser replicado para seu próprio volume no sistema secundário do SnapVault.

Em um ambiente em que o SnapVault é usado, os snapshots nomeados especificamente são criados no sistema de storage primário. Dependendo da configuração implementada, os instantâneos nomeados podem ser criados no sistema principal por um agendamento do SnapVault ou por um aplicativo como o NetApp Active IQ Unified Manager. Os instantâneos nomeados que são criados no sistema primário são replicados para o destino SnapMirror e, a partir daí, são abobadados para o destino SnapVault.

Um volume de origem pode ser criado em uma configuração em cascata na qual um volume é replicado para um destino SnapMirror no local de DR e, a partir daí, é abobadado para um destino SnapVault. Um volume de origem também pode ser criado em uma relação de fan-out em que um destino é um destino SnapMirror e o outro destino é um destino SnapVault. No entanto, o SRA não reconfigura automaticamente a relação do SnapVault para usar o volume de destino do SnapMirror como a origem do Vault quando ocorre failover ou

reversão de replicação do VLSR.

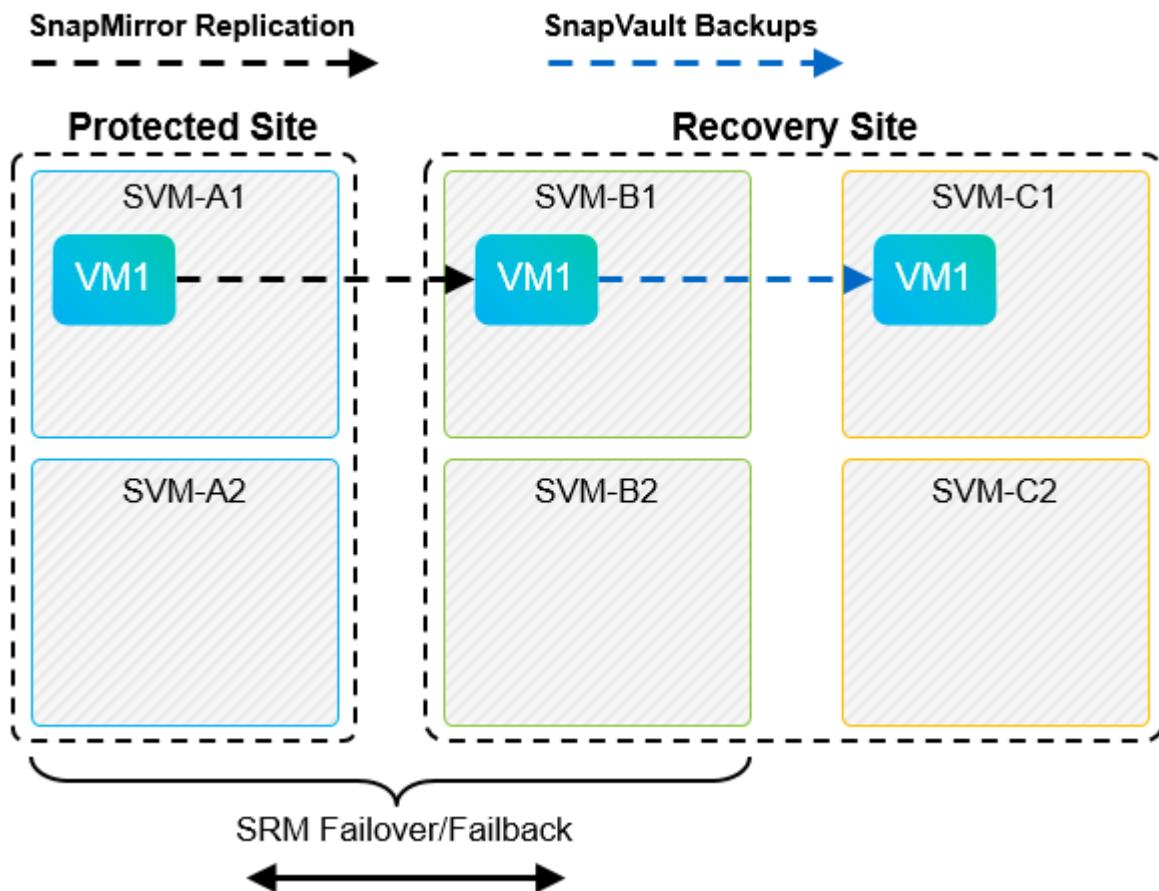
Para obter as informações mais recentes sobre o SnapMirror e o SnapVault para ONTAP 9, consulte ["TR-4015 Guia de práticas recomendadas de configuração do SnapMirror para ONTAP 9."](#)

#### Prática recomendada

Se o SnapVault e o VLSR forem usados no mesmo ambiente, a NetApp recomenda o uso de uma configuração em cascata SnapMirror to SnapVault na qual os backups do SnapVault normalmente são executados a partir do destino do SnapMirror no local de DR. Em caso de desastre, essa configuração torna o site primário inacessível. Manter o destino do SnapVault no local de recuperação permite que os backups do SnapVault sejam reconfigurados após o failover para que os backups do SnapVault possam continuar operando no local de recuperação.

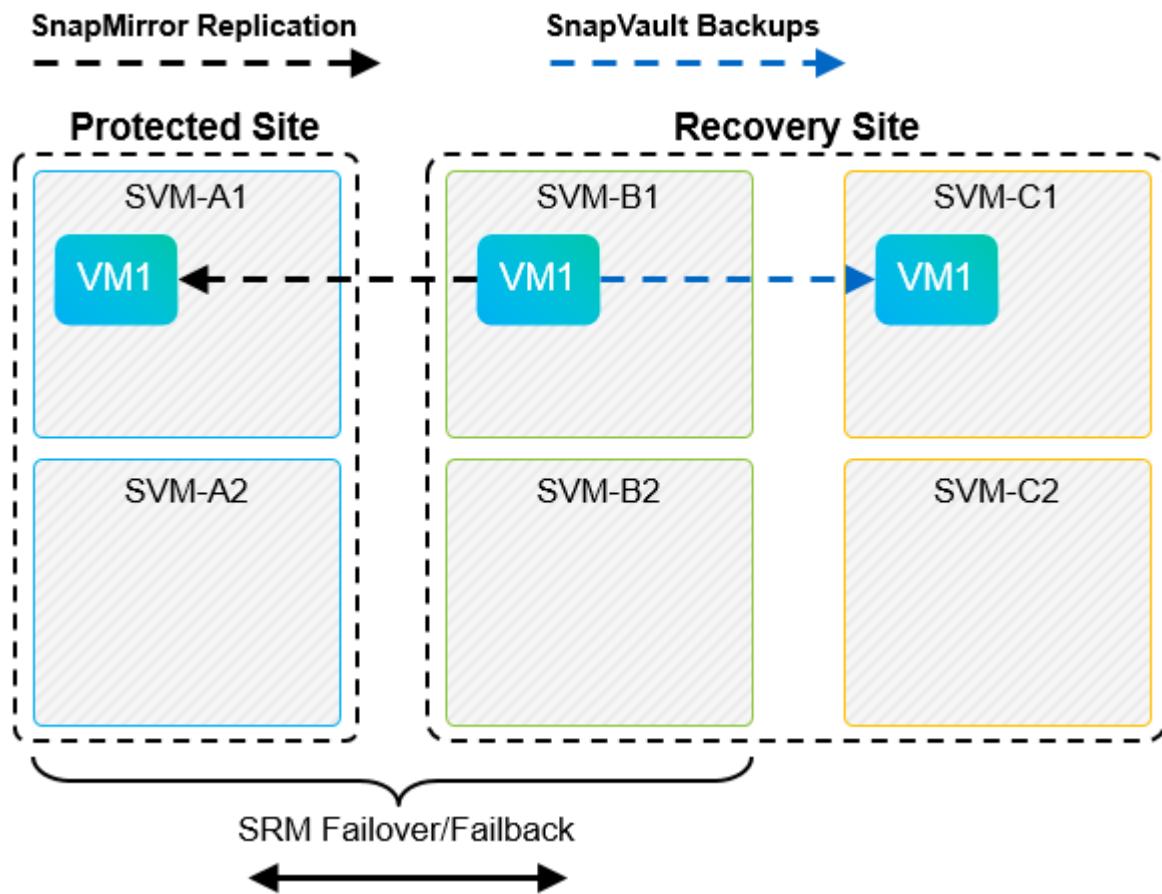
Em um ambiente VMware, cada datastore tem um identificador exclusivo universal (UUID) e cada VM tem um ID de objeto gerenciado exclusivo (MOID). Essas IDs não são mantidas pelo VLSR durante o failover ou fallback. Como os UUIDs do datastore e os MOIDs de VM não são mantidos durante o failover pelo VLSR, todos os aplicativos que dependem desses IDs devem ser reconfigurados após o failover do VLSR. Um aplicativo de exemplo é o NetApp Active IQ Unified Manager, que coordena a replicação do SnapVault com o ambiente vSphere.

A figura a seguir mostra uma configuração em cascata SnapMirror to SnapVault. Se o destino do SnapVault estiver no local de DR ou em um local terciário que não seja afetado por uma interrupção no local primário, o ambiente poderá ser reconfigurado para permitir que os backups continuem após o failover.



A figura a seguir mostra a configuração depois que o VLSR foi usado para reverter a replicação do SnapMirror de volta para o local principal. O ambiente também foi reconfigurado de modo que os backups do SnapVault estão ocorrendo a partir do que é agora a fonte SnapMirror. Esta configuração é uma configuração de fan-out

do SnapMirror SnapVault.



Depois que o vsrm executa o failback e uma segunda reversão das relações do SnapMirror, os dados de produção estão de volta ao local principal. Agora, esses dados estão protegidos da mesma maneira que antes do failover para o local de recuperação de desastres, por meio de backups SnapMirror e SnapVault.

## Uso de Qtrees em ambientes do Site Recovery Manager

Qtrees são diretórios especiais que permitem a aplicação de cotas de sistema de arquivos para nas. O ONTAP 9 permite a criação de qtrees, e qtrees podem existir em volumes replicados com o SnapMirror. No entanto, o SnapMirror não permite replicação de qtrees individuais ou replicação em nível de qtree. Toda a replicação do SnapMirror está apenas no nível do volume. Por esta razão, o NetApp não recomenda o uso de qtrees com VLSR.

## Ambientes FC e iSCSI mistos

Com os protocolos SAN compatíveis (FC, FCoE e iSCSI), o ONTAP 9 fornece serviços LUN, ou seja, a capacidade de criar e mapear LUNs para hosts conectados. Como o cluster consiste em vários controladores, há vários caminhos lógicos gerenciados pela e/S multipath em qualquer LUN individual. O acesso de unidade lógica assimétrica (ALUA) é usado nos hosts para que o caminho otimizado para um LUN seja selecionado e seja ativado para transferência de dados. Se o caminho otimizado para qualquer LUN mudar (por exemplo, porque o volume que contém é movido), o ONTAP 9 reconhece e ajusta-se automaticamente para essa alteração sem interrupções. Se o caminho otimizado ficar indisponível, o ONTAP poderá alternar para qualquer outro caminho disponível sem interrupções.

O VMware VLSR e o NetApp SRA suportam o uso do protocolo FC em um local e do protocolo iSCSI no outro local. No entanto, ele não dá suporte a uma combinação de armazenamentos de dados anexados a FC e

armazenamentos de dados anexados a iSCSI no mesmo host ESXi ou em hosts diferentes no mesmo cluster. Esta configuração não é suportada com o VLSR porque, durante o failover VLSR ou failover de teste, o VLSR inclui todos os iniciadores FC e iSCSI nos hosts ESXi na solicitação.

#### Prática recomendada

O VLSR e o SRA oferecem suporte a protocolos FC e iSCSI mistos entre os locais protegidos e de recuperação. No entanto, cada local deve ser configurado com apenas um protocolo, FC ou iSCSI, e não com ambos os protocolos no mesmo local. Se houver um requisito para que os protocolos FC e iSCSI sejam configurados no mesmo local, o NetApp recomenda que alguns hosts usem iSCSI e outros hosts usem FC. O NetApp também recomenda, neste caso, que os mapeamentos de recursos do VLSR sejam configurados para que as VMs sejam configuradas para failover em um grupo de hosts ou outro.

## Solução de problemas do VLSRM/SRM ao usar a replicação do vVols

Ao usar as ferramentas do ONTAP 9.13P2, o fluxo de trabalho dentro do VLSR e SRM é significativamente diferente ao usar a replicação vVols do que é usado com o SRA e armazenamentos de dados tradicionais. Por exemplo, não há conceito de gerenciador de array. Como tal, `discoverarrays` e `discoverdevices` comandos nunca são vistos.

Ao solucionar problemas, é benéfico entender os novos fluxos de trabalho, listados abaixo:

1. `QueryReplicationPeer`: Descobre os acordos de replicação entre dois domínios de falha.
2. `QueryFaultDomain`: Descobre a hierarquia do domínio de falha.
3. `QueryReplicationGroup`: Descobre os grupos de replicação presentes nos domínios de origem ou destino.
4. `SyncReplicationGroup`: Sincroniza os dados entre origem e destino.
5. `QueryPointInTimeReplica`: Descobre as réplicas de ponto no tempo em um destino.
6. `TestFailoverReplicationGroupStart`: Inicia o failover de teste.
7. `TestFailoverReplicationGroupStop`: Termina o failover de teste.
8. `PromoteReplicationGroup`: Promove um grupo atualmente em teste para produção.
9. `PrepareFailoverReplicationGroup`: Prepara-se para uma recuperação de desastres.
10. `FailoverReplicationGroup`: Executa recuperação de desastres.
11. `ReverseReplicateGroup`: Inicia a replicação reversa.
12. `QueryMatchingContainer`: Localiza contentores (junto com hosts ou grupos de replicação) que podem satisfazer uma solicitação de provisionamento com uma determinada política.
13. `QueryResourceMetadata`: Descobre os metadados de todos os recursos do provedor VASA, a utilização de recursos pode ser retornada como uma resposta para a função `queryMatchingContainer`.

O erro mais comum visto ao configurar a replicação do vVols é uma falha ao descobrir as relações do SnapMirror. Isso ocorre porque os volumes e as relações SnapMirror são criadas fora do escopo das Ferramentas do ONTAP. Portanto, é uma prática recomendada sempre garantir que sua relação com o SnapMirror esteja totalmente inicializada e que você tenha executado uma redescoberta nas Ferramentas do ONTAP em ambos os sites antes de tentar criar um armazenamento de dados vVols replicado.

## Informações adicionais

Para saber mais sobre as informações descritas neste documento, consulte os seguintes documentos e/ou sites:

- Ferramentas do ONTAP para recursos do VMware vSphere 10.x.  
["https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"](https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab)
- Ferramentas do ONTAP para recursos do VMware vSphere 9.x.  
["https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"](https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab)
- TR-4597: VMware vSphere for ONTAP "<https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vsphere-overview.html>"
- TR-4400: VMware vSphere Virtual volumes com ONTAP "<https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html>"
- TR-4015 Guia de Melhores Práticas de Configuração do SnapMirror para ONTAP 9  
<https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf>
- Documentação do VMware Live Site Recovery "<https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html>"

Consulte o "[Ferramenta de Matriz de interoperabilidade \(IMT\)](#)" no site de suporte da NetApp para validar se as versões exatas de produtos e recursos descritas neste documento são compatíveis com o seu ambiente específico. O NetApp IMT define os componentes e versões do produto que podem ser usados para construir configurações compatíveis com o NetApp. Os resultados específicos dependem da instalação de cada cliente de acordo com as especificações publicadas.

## 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 SOBRESSAENTES; 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.