Configurar replicação síncrona com NetApp SnapMirror Active Sync e clusters de expansão da Microsoft

NetApp virtualization solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/pt-br/netapp-solutions-virtualization/hyperv/hyperv-smas.html on August 18, 2025. Always check docs.netapp.com for the latest.

Índice

Configurar replicação síncrona com NetApp SnapMirror Active Sync e clusters de expansão da Microsoft . . . 1
Introdução . . . 1
Casos de uso . . . 1
Arquitetura da Solução . . . 2
Instalar um cluster de failover do Microsoft Stretch . . . 3
Criar peering entre clusters . . . 5
Configurar o Mediador com ONTAP . . . 6
Configurar proteção simétrica ativa/ativa . . . 8
Executar teste de validação de failover de cluster . . . 9
Resumo . . . 11

Configurar replicação síncrona com NetApp SnapMirror Active Sync e clusters de expansão da Microsoft

Use o SnapMirror Active Sync para configurar a replicação síncrona e bidirecional entre clusters de failover estendidos da Microsoft. Este procedimento inclui a instalação de um cluster de failover estendido, a criação de peering entre clusters, a configuração de um mediador com ONTAP, a ativação da proteção simétrica ativa/ativa e a execução de testes de validação de failover de cluster.

Introdução

A partir do ONTAP 9.15.1, a sincronização ativa do SnapMirror oferece suporte a implantações ativas/ativas simétricas, permitindo operações de E/S de leitura e gravação de ambas as cópias de um LUN protegido com replicação síncrona bidirecional. Um Windows Stretch Cluster é uma extensão do recurso Windows Failover Cluster que abrange vários locais geográficos para fornecer alta disponibilidade e recuperação de desastres. Com o SnapMirror Active Sync Simétrico Ativo/Ativo e aplicativos em cluster, como o cluster de failover do Windows, podemos obter disponibilidade contínua para aplicativos críticos de negócios do Microsoft Hyper-V para atingir RTO e RPO zero durante incidentes inesperados. Esta solução oferece os seguintes benefícios:

- Perda zero de dados: garante que os dados sejam replicados de forma síncrona, atingindo o objetivo de ponto de recuperação (RPO) zero.
- Alta disponibilidade e balanceamento de carga: ambos os sites podem lidar ativamente com solicitações, fornecendo balanceamento de carga e alta disponibilidade.
- Continuidade dos negócios: implemente uma configuração simétrica ativa/ativa para garantir que ambos os data centers estejam atendendo ativamente aos aplicativos e possam assumir o controle sem problemas em caso de falha.
- Melhore o desempenho: use a configuração simétrica ativa/ativa para distribuir a carga entre vários sistemas de armazenamento, melhorando os tempos de resposta e o desempenho geral do sistema.

Este artigo documenta a replicação bidirecional síncrona da tecnologia de sincronização ativa SnapMirror entre clusters de failover extensíveis da Microsoft, permitindo que dados de aplicativos multisite, como MSSQL e Oracle, sejam ativamente acessíveis e sincronizados em ambos os sites. Caso ocorra uma falha, os aplicativos são imediatamente redirecionados para o site ativo restante, sem perda de dados e sem perda de acesso, proporcionando alta disponibilidade, recuperação de desastres e redundância geográfica.

Casos de uso

No caso de uma interrupção, como um ataque cibernético, queda de energia ou desastre natural, um ambiente de negócios conectado globalmente exige recuperação rápida de dados de aplicativos essenciais aos negócios, com perda zero de dados. Essas demandas são maiores em áreas como finanças e naquelas que aderem a mandatos regulatórios como o Regulamento Geral de Proteção de Dados (GDPR). Implante uma configuração simétrica ativa/ativa para replicar dados entre locais geograficamente dispersos, fornecendo acesso local aos dados e garantindo a continuidade em caso de interrupções regionais.

A sincronização ativa do SnapMirror fornece os seguintes casos de uso:

Implantação de aplicativo para objeto de tempo de recuperação zero (RTO)

Em uma implantação de sincronização ativa do SnapMirror , você tem um cluster primário e um cluster de espelho. Um LUN no cluster primário (L1P) tem um espelho (L1S) no secundário; leituras e gravações são atendidas pelo site local para os hosts com base nas configurações de proximidade ativa.

Implantação de aplicativos para RTO ou TAF zero

O Transparent Application Failover (TAF) é baseado no failover de caminho baseado em software MPIO do host para obter acesso sem interrupções ao armazenamento. Ambas as cópias de LUN — por exemplo, primária (L1P) e cópia espelho (L1S) — têm a mesma identidade (número de série) e são relatadas como legíveis e graváveis para o host.

Aplicações agrupadas

Aplicativos em cluster, incluindo VMware vSphere Metro Storage Cluster (vMSC), Oracle RAC e Windows Failover Clustering com SQL, exigem acesso simultâneo para que as VMs possam fazer failover para o outro site sem nenhuma sobrecarga de desempenho. O SnapMirror ativo/ativo simétrico de sincronização ativa atende E/S localmente com replicação bidirecional para atender aos requisitos de aplicativos em cluster.

Cenário de desastre

Replique sincronicamente vários volumes para um aplicativo entre sites em localizações geograficamente dispersas. Você pode fazer failover automaticamente para a cópia secundária em caso de interrupção na primária, permitindo assim a continuidade dos negócios para aplicativos de nível um.

Failover do Windows

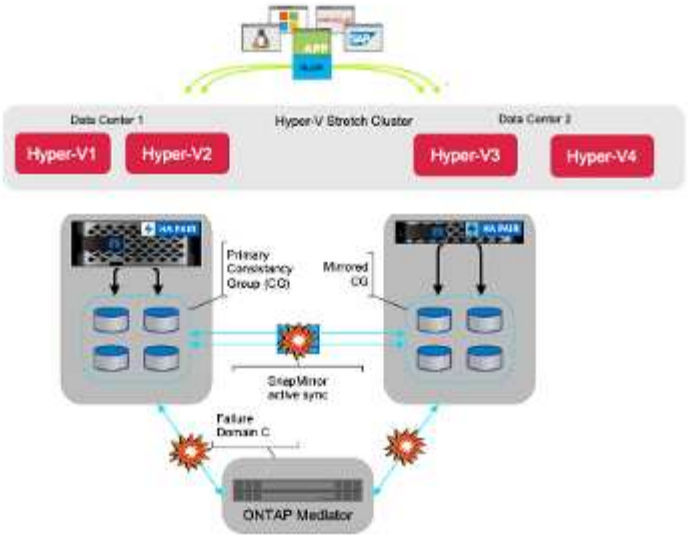
O SnapMirror Active Sync oferece flexibilidade com granularidade fácil de usar no nível do aplicativo e failover automático para atingir alta disponibilidade de dados e replicação rápida de dados para seus aplicativos essenciais aos negócios, como Oracle, Microsoft SQL Server e assim por diante, em ambientes virtuais e físicos.

Arquitetura da Solução

O cluster extensível da Microsoft tem dois nós do Hyper-V em cada site. Esses dois nós compartilham o armazenamento NetApp e usam o SnapMirror Active Sync Simétrico Ativo-Ativo para replicar os volumes entre os dois sites. Um grupo de consistência garante que todos os volumes de um conjunto de dados sejam desativados e, em seguida, capturados precisamente no mesmo momento. Isso fornece um ponto de restauração consistente de dados em todos os volumes que suportam o conjunto de dados. O Mediador ONTAP recebe informações de integridade sobre clusters e nós ONTAP pareados, orquestrando entre os dois e determinando se cada nó/cluster está íntegro e em execução.

Componentes da solução:

- Dois sistemas de armazenamento NetApp ONTAP 9.15.1: primeiro e segundo domínio de falha
- Uma VM Redhat 8.7 para mediador ONTAP
- Três clusters de failover do Hyper-V no Windows 2022:
  - site1, site 2 para as aplicações
  - local 3 para mediador
- VM no Hyper-V: Controlador de Domínio Microsoft, instância de cluster MSSQL Always On Failover, Mediador ONTAP



Instalar um cluster de failover do Microsoft Stretch

Você pode usar o Windows Admin Center, o PowerShell ou o console do Gerenciador do Servidor para instalar o recurso Failover Clustering e seus cmdlets do PowerShell associados. Para obter detalhes sobre pré-requisitos e etapas, confira criar um cluster de failover.

Aqui está um guia passo a passo para configurar um Windows Stretch Cluster:

1. Instale o Windows 2022 em todos os quatro servidores hyperv1, hyperv2, hyperv3 e hyperv4
2. Junte todos os quatro servidores ao mesmo domínio do Active Directory: hyperv.local.
3. Instale os recursos do Windows failover-clustering, Hyper-V, Hyper-V_Powershell e MPIO em cada servidor.

```
Install-WindowsFeature -Name "Failover-Clustering", "Hyper-V", "Hyper-V-Powershell", "MPIO" -IncludeManagementTools
```

4. Configure o MPIO e adicione suporte para dispositivos iSCSI.

5. No armazenamento ONTAP do site 1 e do site 2, crie dois LUNs iSCSI (SQLdata e SQLlog) e mapeie para o grupo iqn dos servidores Windows. Use o iniciador de software iSCSI da Microsoft para conectar os

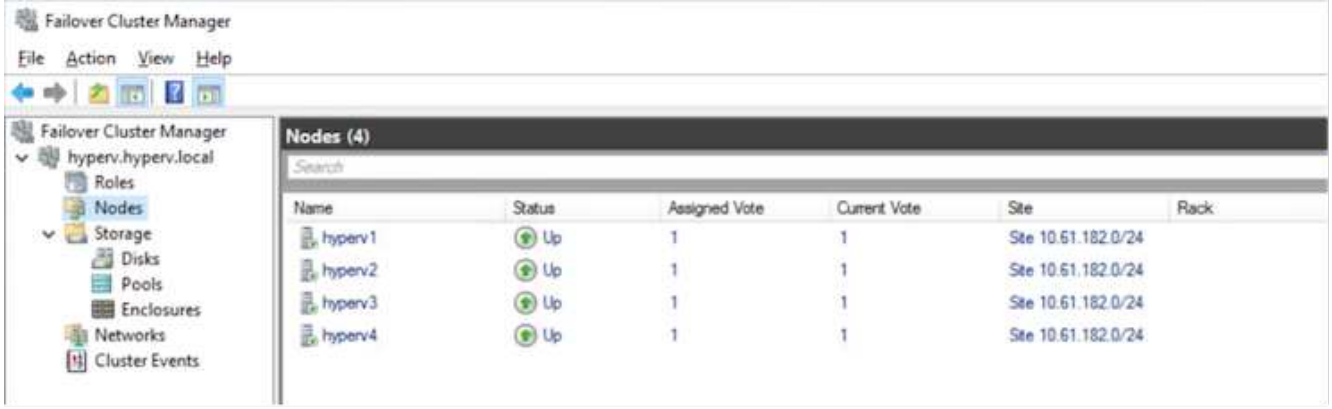
LUNs. Para mais detalhes, consulte"Configuração iSCSI para Windows" .

6. Execute o relatório de validação do cluster para detectar erros ou avisos.

```
Test-Cluster -Node hyperv1, hyperv2, hyperv3, hyperv4
```

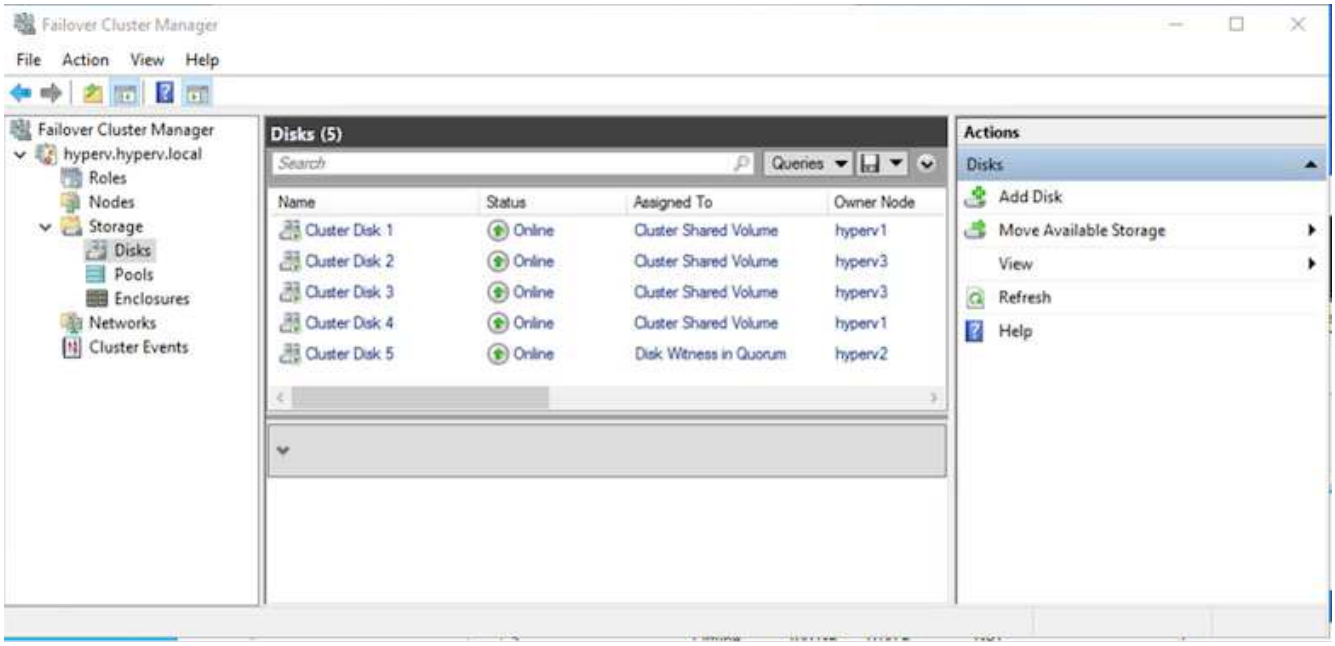
7. Crie um cluster de failover, atribua um endereço IP estático,

```
New-Cluster -Name <clustername> -Node hyperv1, hyperv2, hyperv3,
hyperv4, StaticAddress <IPaddress>
```



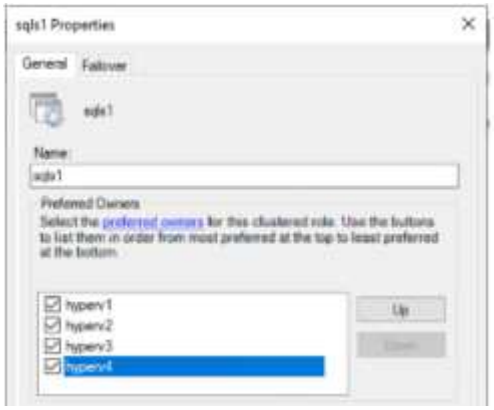
8. Adicione os armazenamentos iSCSI mapeados ao cluster de failover.
9. Configure uma testemunha para o quorum, clique com o botão direito do mouse no cluster → Mais ações → Configurar definições de quorum do cluster, escolha testemunha de disco.

   O diagrama abaixo mostra quatro LUNs compartilhados em cluster – dois sites sqldata e sqllog e uma testemunha de disco no quorum.



Instância de cluster de failover sempre ativa

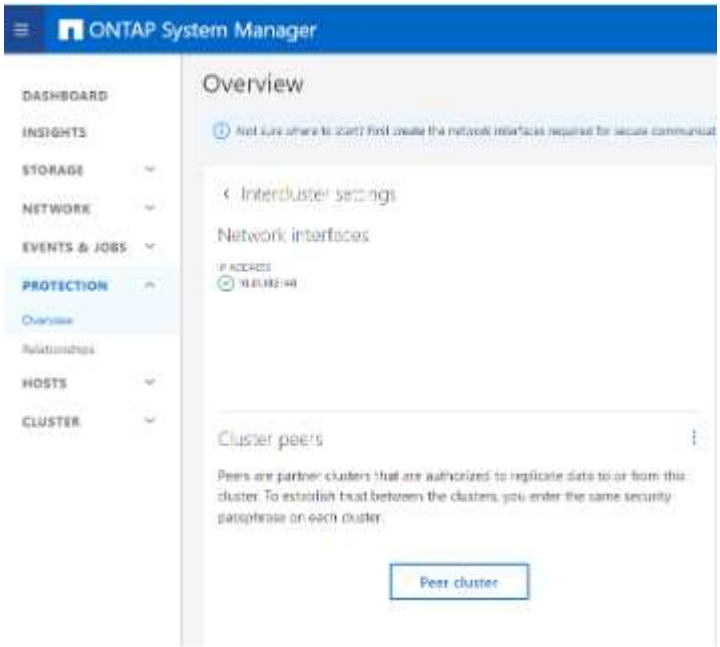
Uma instância de cluster de failover Always On (FCI) é uma instância do SQL Server instalada em nós com armazenamento em disco compartilhado SAN em um WSFC. Durante um failover, o serviço WSFC transfere a propriedade dos recursos da instância para um nó de failover designado. A instância do SQL Server é então reiniciada no nó de failover e os bancos de dados são recuperados normalmente. Para mais detalhes sobre a configuração, confira Clustering de Failover do Windows com SQL. Crie duas VMs Hyper-V SQL FCI em cada site e defina a prioridade. Use hyperv1 e hyperv2 como proprietários preferenciais para as VMs do site 1 e hyperv3 e hyperv4 como proprietários preferenciais para as VMs do site 2.



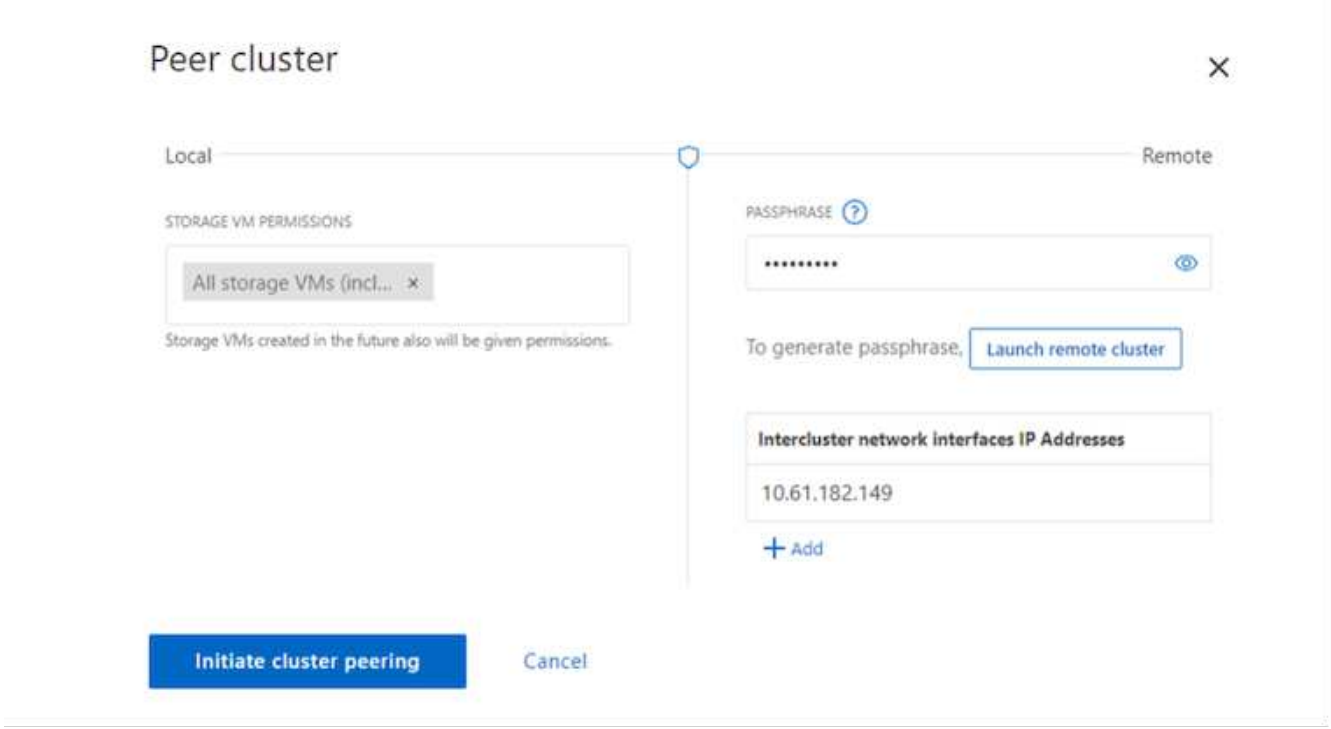
Criar peering entre clusters

Você deve criar relacionamentos de pares entre os clusters de origem e destino antes de poder replicar cópias do Snapshot usando o SnapMirror.

1. Adicionar interfaces de rede intercluster em ambos os clusters



2. Você pode usar o comando cluster peer create para criar um relacionamento de peer entre um cluster local e remoto. Depois que o relacionamento entre pares for criado, você pode executar cluster peer create no cluster remoto para autenticá-lo no cluster local.



Configurar o Mediador com ONTAP

O Mediador ONTAP recebe informações de integridade sobre clusters e nós ONTAP pareados, orquestrando entre os dois e determinando se cada nó/cluster está íntegro e em execução. O SM-as permite que os dados sejam replicados para o destino assim que forem gravados no volume de origem. O mediador deve ser implantado no terceiro domínio de falha. Pré-requisitos

- Especificações de hardware: 8 GB de RAM, CPU 2x2 GHz, rede de 1 Gb (<125 ms RTT)
- Instalado o sistema operacional Red Hat 8.7, verifique"Versão do ONTAP Mediator e versão Linux suportada" .
- Configurar o host Linux do Mediator: configuração de rede e portas de firewall 31784 e 3260
- Instale o pacote yum-utils
- "Registre uma chave de segurança quando o UEFI Secure Boot estiver habilitado"

Passos

1. Baixe o pacote de instalação do Mediator em"Página de download do ONTAP Mediator" .
2. Verifique a assinatura do código do Mediador ONTAP .
3. Execute o instalador e responda às solicitações conforme necessário:

```
./ontap-mediator-1.8.0/ontap-mediator-1.8.0 -y
```

4. Quando o Secure Boot estiver ativado, você deverá tomar medidas adicionais para registrar a chave de segurança após a instalação:
   a. Siga as instruções no arquivo README para assinar o módulo do kernel SCST:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.mo
dule-signing
```

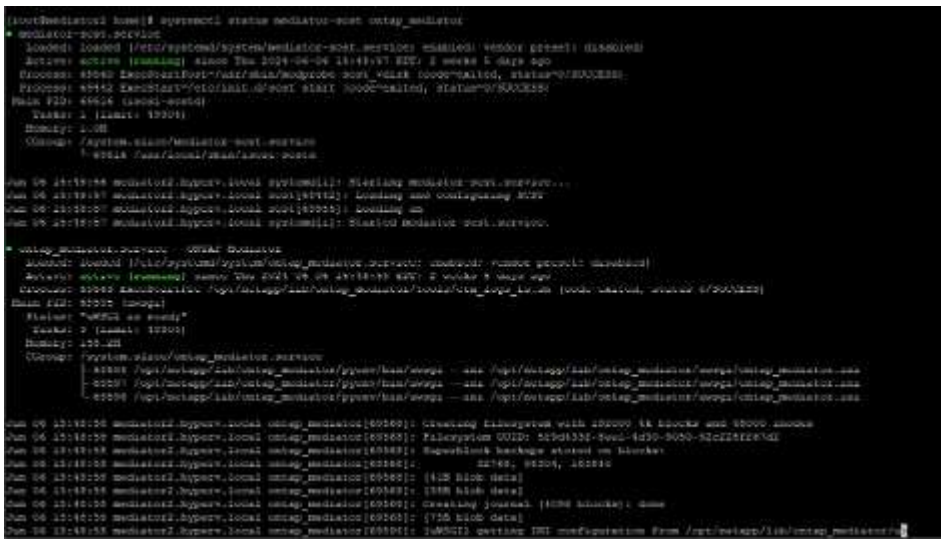
b. Localize as chaves necessárias:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

5. Verifique a instalação

a. Confirme os processos:

```
systemctl status ontap_mediator mediator-scst
```



b. Confirme as portas usadas pelo serviço ONTAP Mediator:

```
[root@mediator2 server_config]# netstat -anlt | grep -E '3260|31784'
tcp        0      0 0.0.0.0:3260            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:31784           0.0.0.0:*               LISTEN
tcp        0      0 10.61.182.163:31784     10.61.182.148:26429     ESTABLISHED
tcp        0      0 10.61.182.163:31784     10.61.182.148:24546     FIN_WAIT2
tcp6       0      0 :::3260                 :::*                    LISTEN
```

6. Inicialize o ONTAP Mediator para sincronização ativa do SnapMirror usando certificados autoassinados

a. Encontre o certificado da CA do ONTAP Mediator no local de instalação do software host/VM Linux do ONTAP Mediator cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config.

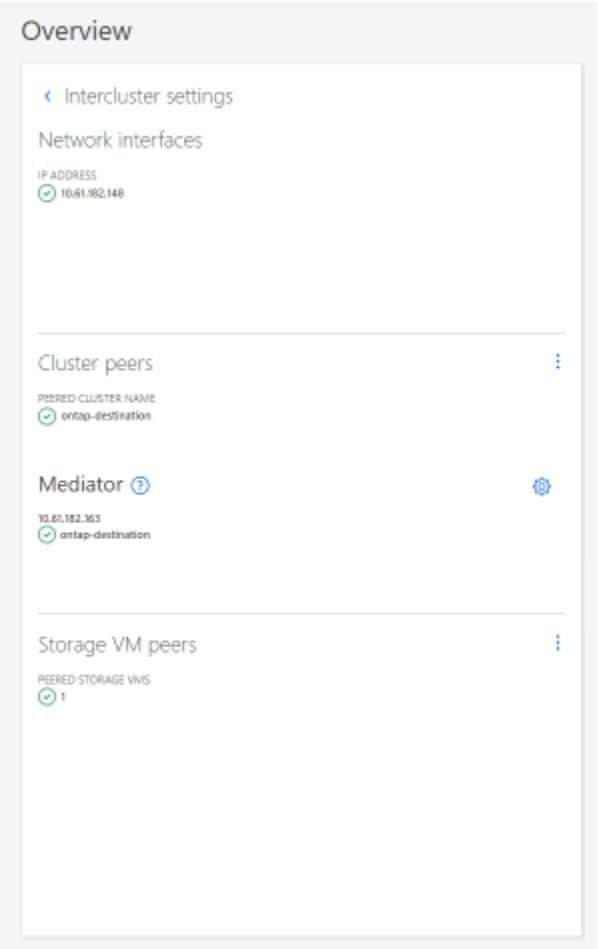
b. Adicione o certificado ONTAP Mediator CA a um cluster ONTAP .

```
security certificate install -type server-ca -vserver <vserver_name>
```

7. Adicione o mediador, vá para Gerenciador de Sistema, proteger>Visão geral>mediador, insira o endereço

IP do mediador, nome de usuário (o padrão do usuário da API é mediatoradmin), senha e a porta 31784.

O diagrama a seguir mostra a interface de rede intercluster, os pares de cluster, o mediador e o par SVM, todos configurados.

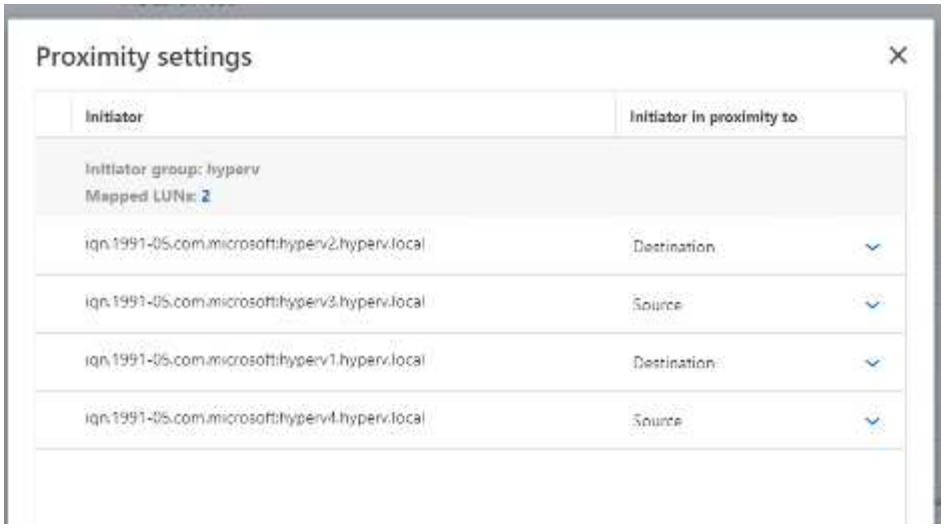


Configurar proteção simétrica ativa/ativa

Grupos de consistência facilitam o gerenciamento da carga de trabalho do aplicativo, fornecendo políticas de proteção locais e remotas facilmente configuradas e cópias instantâneas simultâneas, consistentes com falhas ou consistentes com aplicativos, de uma coleção de volumes em um determinado momento. Para mais detalhes consulte"visão geral do grupo de consistência" . Usamos uma configuração uniforme para esta instalação.

Etapas para uma configuração uniforme

1. Ao criar o grupo de consistência, especifique iniciadores de host para criar igroups.
2. Marque a caixa de seleção para Habilitar SnapMirror e escolha a política AutomatedFailoverDuplex.
3. Na caixa de diálogo exibida, marque a caixa de seleção Replicar grupos de iniciadores para replicar igroups. Em Editar configurações proximais, defina SVMs proximais para seus hosts.



4. Selecione Salvar

   A relação de proteção é estabelecida entre a origem e o destino.

Executar teste de validação de failover de cluster

Recomendamos que você execute testes de failover planejados para fazer uma verificação de validação do cluster. Os bancos de dados SQL ou qualquer software em cluster em ambos os sites – o site principal ou espelhado deve continuar acessível durante os testes.

Os requisitos do cluster de failover do Hyper-V incluem:

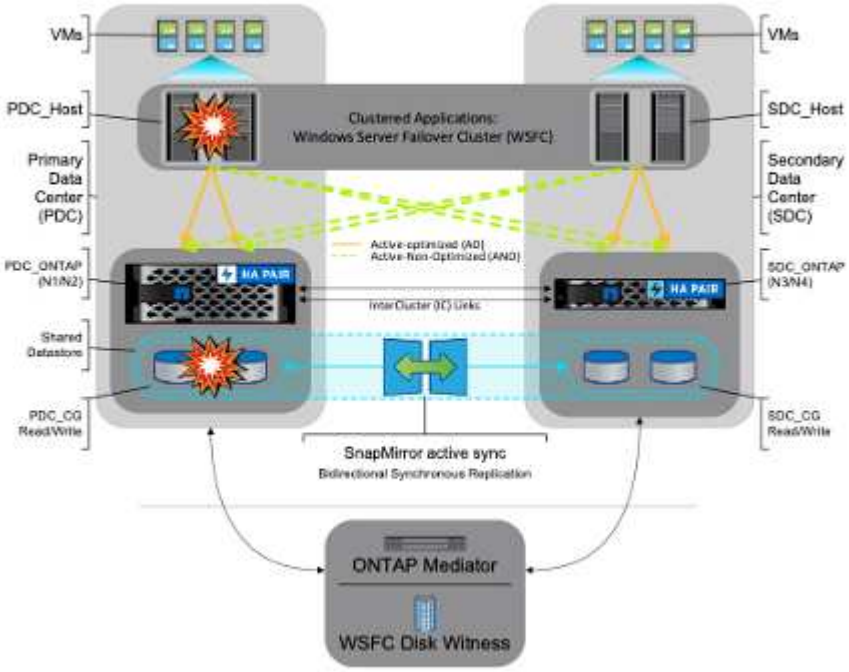
- O relacionamento de sincronização ativa do SnapMirror deve estar sincronizado.
- Não é possível iniciar um failover planejado quando uma operação não disruptiva estiver em andamento. Operações não disruptivas incluem movimentações de volumes, realocações de agregados e failovers de armazenamento.
- O Mediador ONTAP deve estar configurado, conectado e em quorum.
- Pelo menos dois nós de cluster do Hyper-V em cada site com processadores de CPU pertencem à mesma

família de CPU para otimizar o processo de migração de VM. As CPUs devem ser CPUs com suporte para virtualização assistida por hardware e Prevenção de Execução de Dados (DEP) baseada em hardware.

- Os nós do cluster do Hyper-V devem ser os mesmos membros do Domínio do Active Directory para garantir resiliência.
- Os nós do cluster Hyper-V e os nós de armazenamento NetApp devem ser conectados por redes redundantes para evitar um único ponto de falha.
- Armazenamento compartilhado, que pode ser acessado por todos os nós do cluster via protocolo iSCSI, Fibre Channel ou SMB 3.0.

Cenários de teste

Há muitas maneiras de acionar um failover em um host, armazenamento ou rede.



O Hyper-V falhou no nó ou em um site

- Falha de nó Um nó de cluster de failover pode assumir a carga de trabalho de um nó com falha, um processo conhecido como failover. Ação: Desligue um nó do Hyper-V. Resultado esperado: O outro nó no cluster assumirá a carga de trabalho. As VMs serão migradas para o outro nó.
- Falha em um site Também podemos causar falha em todo o site e acionar o failover do site principal para o site espelho: Ação: Desative os dois nós do Hyper-V em um site. Resultado esperado: as VMs no site principal migrarão para o cluster Hyper-V do site espelho porque o SnapMirror Active Sync Simétrico Ativo/Ativo atende E/S localmente com replicação bidirecional, sem impacto na carga de trabalho com RPO zero e RTO zero.

Falha de armazenamento em um site

- Interromper uma SVM no site primário Ação: Interromper a SVM iSCSI Resultados esperados: O cluster primário do Hyper-V já está conectado ao site espelhado e, com o SnapMirror ativo, a sincronização simétrica ativa/ativa não causa impacto na carga de trabalho, com RPO zero e RTO zero.

Critérios de sucesso

Durante os testes, observe o seguinte:

- Observe o comportamento do cluster e garanta que os serviços sejam transferidos para os nós restantes.
- Verifique se há erros ou interrupções no serviço.
- Certifique-se de que o cluster possa lidar com falhas de armazenamento e continuar operando.
- Verifique se os dados do banco de dados permanecem acessíveis e se os serviços continuam operando.
- Verifique se a integridade dos dados do banco de dados é mantida.
- Valide se aplicativos específicos podem fazer failover para outro nó sem impacto no usuário.
- Verifique se o cluster pode balancear a carga e manter o desempenho durante e após um failover.

Resumo

A sincronização ativa do SnapMirror pode ajudar dados de aplicativos de vários sites, por exemplo, MSSQL e Oracle, a serem ativamente acessíveis e sincronizados em ambos os sites. Se ocorrer uma falha, os aplicativos serão imediatamente redirecionados para o site ativo restante, sem perda de dados e sem perda de acesso.

Informações sobre direitos autorais

Copyright © 2025 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.