Configuração de storage em sistemas ASA R2

Enterprise applications

NetApp
February 11, 2026

Índice

Configuração de storage em sistemas ASA R2

Visão geral

O NetApp ASA R2 é uma solução simplificada e avançada para clientes somente SAN que executam workloads essenciais. A combinação da plataforma ASA R2 que executa soluções de storage ONTAP e do Microsoft SQL Server permite designs de storage de banco de dados de nível empresarial que podem atender aos requisitos de aplicativos mais exigentes da atualidade.

As plataformas ASA a seguir são classificadas como sistemas ASA R2 compatíveis com todos os protocolos SAN (iSCSI, FC, NVMe/FC, NVMe/TCP). Os protocolos iSCSI, FC, NVMe/FC e NVMe/TCP são compatíveis com arquitetura ativo-ativo simétrica para multipathing, de modo que todos os caminhos entre os hosts e o storage fiquem ativos/otimizados:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20

Para obter mais informações, consulte "NetApp ASA"

A otimização de uma solução SQL Server no ONTAP requer a compreensão do padrão e/S do SQL Server. Um layout de armazenamento bem projetado para um banco de dados do SQL Server deve suportar os requisitos de desempenho do SQL Server, além de fornecer o máximo de gerenciamento da infraestrutura como um todo. Um bom layout de storage também permite que a implantação inicial seja bem-sucedida e o ambiente cresça suavemente ao longo do tempo à medida que a empresa cresce.

Design de storage de dados

A Microsoft recomenda colocar os dados e arquivos de log em unidades separadas. Para aplicativos que simultaneamente atualizam e solicitam dados, o arquivo de log é intenso de gravação e o arquivo de dados (dependendo do aplicativo) é intenso de leitura/gravação. Para a recuperação de dados, o ficheiro de registo não é necessário. Portanto, as solicitações de dados podem ser satisfeitas a partir do arquivo de dados colocado em sua própria unidade.

Ao criar um novo banco de dados, a Microsoft recomenda especificar unidades separadas para os dados e logs. Para mover arquivos após a criação do banco de dados, o banco de dados deve ser offline. Para obter mais recomendações da Microsoft, "Coloque dados e arquivos de log em unidades separadas"consulte .

Considerações sobre a unidade de armazenamento

A unidade de storage no ASA refere-se a LUN para hosts SCSI/FC ou um namespace NVMe para hosts NVMe. Com base no protocolo compatível, você será solicitado a criar LUN, namespace NVMe ou ambos. Antes de criar uma unidade de armazenamento para implantação de banco de dados, é importante entender como o padrão e as caraterísticas de e/S do SQL Server variam dependendo da carga de trabalho e dos requisitos de backup e recuperação. Consulte as seguintes recomendações do NetApp para a unidade de armazenamento:

- Evite compartilhar a mesma unidade de armazenamento entre vários SQL Server em execução no mesmo host para evitar gerenciamento complicado. No caso de executar várias instâncias do SQL Server no mesmo host, a menos que você esteja perto do limite da unidade de armazenamento em um nó, evite compartilhar e, em vez disso, tenha uma unidade de armazenamento separada por instância por host para facilitar o gerenciamento de dados.
- Use pontos de montagem NTFS em vez de letras de unidade para superar a limitação de 26 unidades no Windows.
- Desative as programações de snapshot e as políticas de retenção. Em vez disso, use o SnapCenter para coordenar cópias Snapshot da unidade de storage de dados do SQL Server.
- Coloque os bancos de dados do sistema do SQL Server em uma unidade de armazenamento dedicada.
- Tempdb é um banco de dados de sistema usado pelo SQL Server como um espaço de trabalho temporário, especialmente para operações de e/S intensivas DBCC CHECKDB. Portanto, coloque esse banco de dados em uma unidade de armazenamento dedicada. Em ambientes grandes em que a contagem de unidades de armazenamento é um desafio, você pode consolidar tempdb com bancos de dados de sistema na mesma unidade de armazenamento após um Planejamento cuidadoso. A proteção de dados para tempdb não é uma prioridade alta porque este banco de dados é recriado sempre que o SQL Server é reiniciado.
- Coloque os arquivos de dados do usuário (`.mdf`) em uma unidade de armazenamento separada, porque eles são cargas de trabalho de leitura/gravação aleatórias. É comum criar backups de log de transações com mais frequência do que backups de banco de dados. Por esse motivo, coloque arquivos de log de transações (`.ldf`) em uma unidade de armazenamento separada ou VMDK dos arquivos de dados para que programações de backup independentes possam ser criadas para cada um. Essa separação também isola a e/S de gravação sequencial dos arquivos de log da e/S de leitura/gravação aleatória de arquivos de dados e melhora significativamente o desempenho do SQL Server.
- Certifique-se de que os arquivos do banco de dados do usuário e o diretório de log para armazenar o backup de log estão em uma unidade de armazenamento separada para impedir que a política de retenção substitua snapshots quando eles são usados com o recurso SnapMirror com diretiva Vault.
- Não misture arquivos de banco de dados e não de banco de dados, como arquivos relacionados à pesquisa de texto completo, na mesma unidade de armazenamento.
- Colocar arquivos secundários de banco de dados (como parte de um grupo de arquivos) em uma unidade de armazenamento separada melhora o desempenho do banco de dados SQL Server. Esta separação só é válida se o ficheiro da base de dados `.mdf` não partilhar a sua unidade de armazenamento com quaisquer outros `.mdf` ficheiros.
- Ao formatar o disco usando o gerenciador de discos no servidor Windows, certifique-se de que o tamanho da unidade de alocação está definido como 64K para partição.
- Não coloque bancos de dados do usuário ou bancos de dados do sistema em uma unidade de armazenamento que hospeda pontos de montagem.
- Consulte "Microsoft Windows e MPIO nativo sob as práticas recomendadas do ONTAP para SAN moderna"para aplicar suporte multipathing no Windows a dispositivos iSCSI nas propriedades MPIO.
- Se você estiver usando uma instância de cluster sempre em failover, os bancos de dados de usuários devem ser colocados na unidade de armazenamento compartilhada entre os nós de cluster de failover do servidor Windows e os recursos de cluster de disco físico serão atribuídos ao grupo de cluster associado à instância do SQL Server.

Arquivos de banco de dados e grupos de arquivos

O posicionamento adequado do arquivo de banco de dados do SQL Server no ONTAP é

fundamental durante a fase inicial de implantação. Isso garante um desempenho ideal, gerenciamento de espaço, backup e tempos de restauração que podem ser configurados para atender aos requisitos da sua empresa.

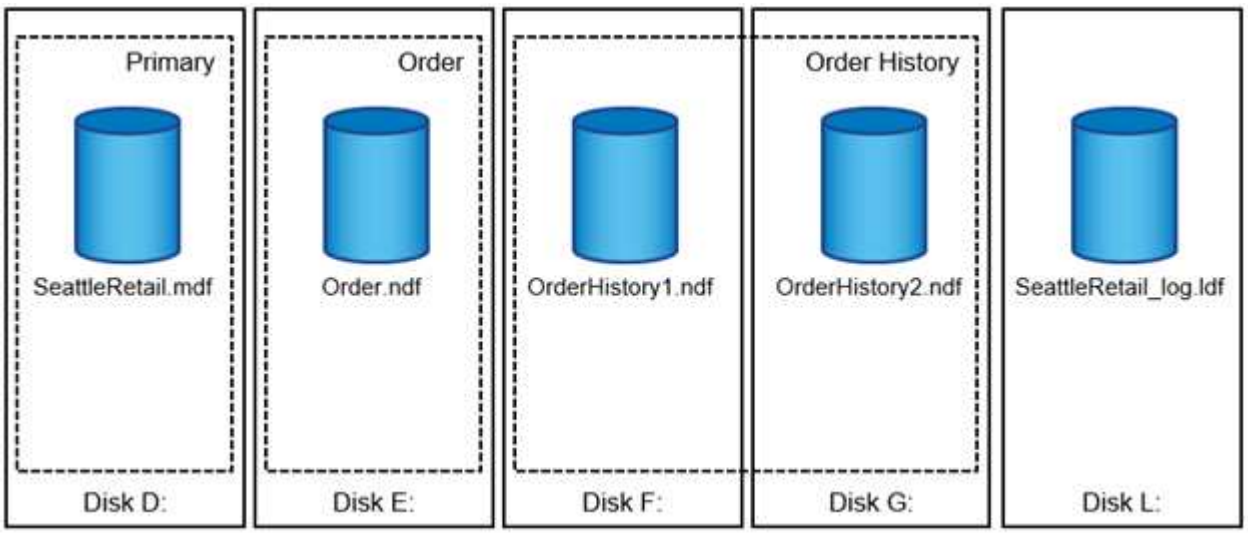
Em teoria, o SQL Server (64 bits) suporta 32.767 bancos de dados por instância e 524.272TB GB de tamanho de banco de dados, embora a instalação típica geralmente tenha vários bancos de dados. No entanto, o número de bancos de dados que o SQL Server pode manipular depende da carga e do hardware. Não é incomum ver instâncias do SQL Server hospedando dezenas, centenas ou até milhares de bancos de dados pequenos.

Ficheiros da base de dados e grupo de ficheiros

Cada banco de dados consiste em um ou mais arquivos de dados e um ou mais arquivos de log de transações. O log de transações armazena as informações sobre transações de banco de dados e todas as modificações de dados feitas por cada sessão. Sempre que os dados são modificados, o SQL Server armazena informações suficientes no log de transações para desfazer (reverter) ou refazer (reproduzir) a ação. Um log de transações do SQL Server é parte integrante da reputação do SQL Server em relação à integridade e robustez dos dados. O log de transações é vital para os recursos de atomicidade, consistência, isolamento e durabilidade (ACID) do SQL Server. O SQL Server grava no log de transações assim que qualquer alteração na página de dados ocorrer. Cada declaração DML (Data Manipulation Language) (por exemplo, selecionar, inserir, atualizar ou excluir) é uma transação completa, e o log de transações garante que toda a operação baseada em conjunto ocorra, certificando-se da atomicidade da transação.

Cada banco de dados tem um arquivo de dados primário, que, por padrão, tem a extensão .mdf. Além disso, cada banco de dados pode ter arquivos de banco de dados secundários. Esses arquivos, por padrão, têm extensões .ndf.

Todos os arquivos de banco de dados são agrupados em grupos de arquivos. Um grupo de arquivos é a unidade lógica, o que simplifica a administração do banco de dados. Eles permitem a separação entre o posicionamento lógico de objetos e arquivos de banco de dados físicos. Quando você cria as tabelas de objetos de banco de dados, você especifica em que grupo de arquivos eles devem ser colocados sem se preocupar com a configuração do arquivo de dados subjacente.



A capacidade de colocar vários arquivos de dados dentro do grupo de arquivos permite que você espalhe a carga entre diferentes dispositivos de armazenamento, o que ajuda a melhorar o desempenho de e/S do sistema. O log de transação em contraste não se beneficia dos vários arquivos porque o SQL Server grava no log de transação de forma sequencial.

A separação entre o posicionamento lógico de objetos nos grupos de arquivos e arquivos físicos de banco de dados permite ajustar o layout do arquivo do banco de dados, obtendo o máximo do subsistema de armazenamento. O número de arquivos de dados que suportam uma determinada carga de trabalho pode ser variado conforme necessário para dar suporte aos requisitos de e/S e à capacidade esperada, sem afetar a aplicação. Essas variações no layout do banco de dados são transparentes para os desenvolvedores de aplicativos, que estão colocando os objetos do banco de dados nos grupos de arquivos em vez de arquivos do banco de dados.

NetApp recomenda evitar o uso do grupo de arquivos primário para qualquer coisa além de objetos do sistema. Criar um grupo de arquivos separado ou um conjunto de grupos de arquivos para os objetos do usuário simplifica a administração do banco de dados e a recuperação de desastres, especialmente no caso de bancos de dados grandes.

Inicialização do arquivo de instância do banco de dados

Você pode especificar o tamanho inicial do arquivo e os parâmetros de crescimento automático no momento em que você cria o banco de dados ou adiciona novos arquivos a um banco de dados existente. O SQL Server usa um algoritmo de preenchimento proporcional ao escolher em qual arquivo de dados ele deve gravar dados. Ele grava uma quantidade de dados proporcionalmente ao espaço livre disponível nos arquivos. Quanto mais espaço livre no arquivo, mais escreve ele lida.

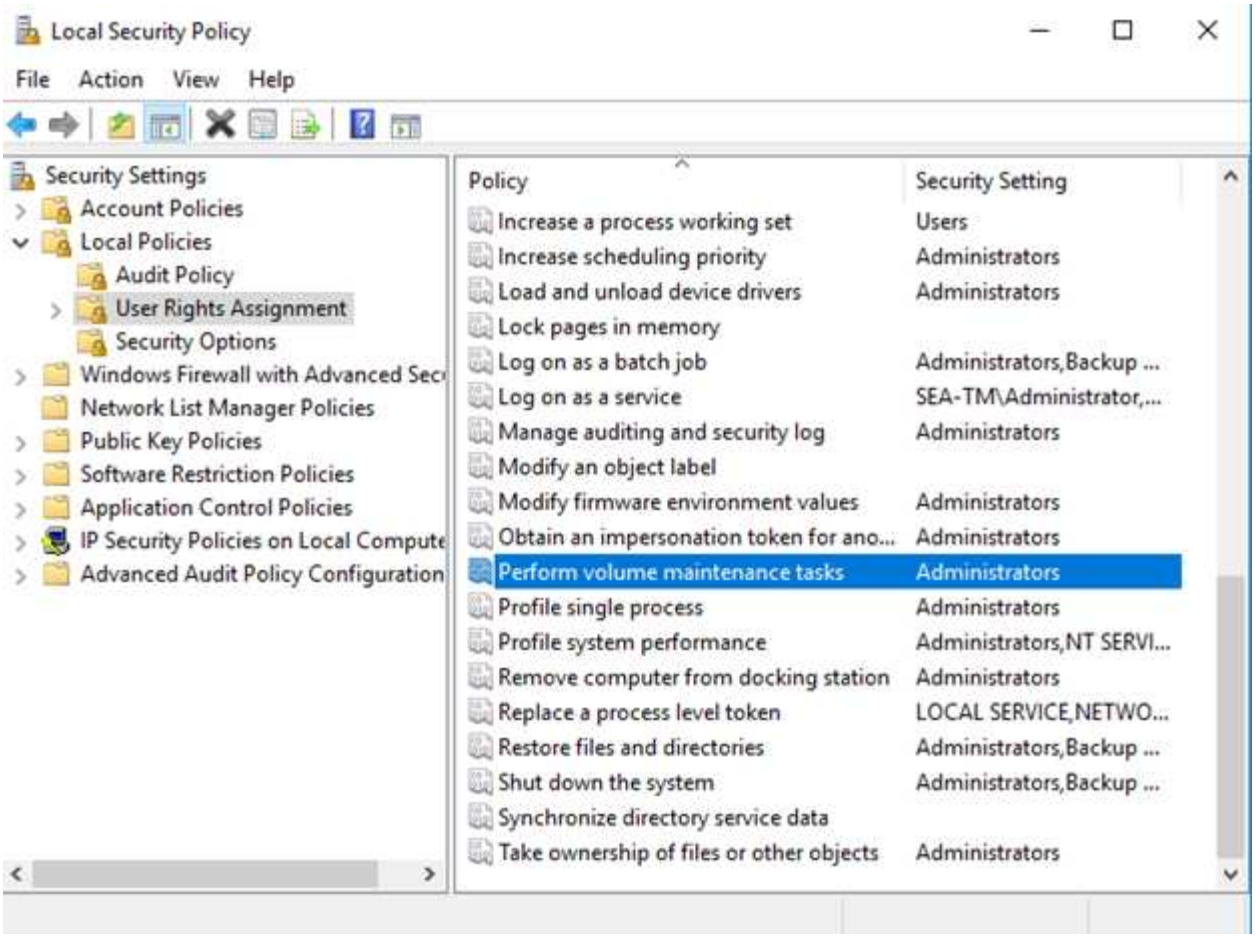
A NetApp recomenda que todos os arquivos no único grupo de arquivos tenham o mesmo tamanho inicial e parâmetros de crescimento automático, com o tamanho de crescimento definido em megabytes em vez de porcentagens. Isso ajuda o algoritmo de preenchimento proporcional equilibrar uniformemente as atividades de gravação em todos os arquivos de dados.

Toda vez que o SQL Server cresce arquivos, ele preenche o espaço recém-alocado com zeros. Esse processo bloqueia todas as sessões que precisam gravar no arquivo correspondente ou, em caso de crescimento de log de transações, gerar Registros de log de transações.

O SQL Server sempre apaga o log de transações e esse comportamento não pode ser alterado. No entanto, você pode controlar se os arquivos de dados estão zerando para fora habilitando ou desativando a inicialização instantânea de arquivos. Ativar a inicialização instantânea de arquivos ajuda a acelerar o crescimento de arquivos de dados e reduz o tempo necessário para criar ou restaurar o banco de dados.

Um pequeno risco de segurança está associado à inicialização instantânea de arquivos. Quando esta opção está ativada, partes não alocadas do arquivo de dados podem conter informações de arquivos do sistema operacional excluídos anteriormente. Os administradores de banco de dados podem examinar esses dados.

Você pode habilitar a inicialização instantânea de arquivos adicionando a permissão SA_MANAGE_VOLUME_NAME, também conhecida como "executar tarefa de manutenção de volume", à conta de inicialização do SQL Server. Você pode fazer isso sob o aplicativo de gerenciamento de políticas de segurança local (secpol.msc), como mostrado na figura a seguir. Abra as propriedades da permissão "Executar tarefa de manutenção de volume" e adicione a conta de inicialização do SQL Server à lista de usuários lá.



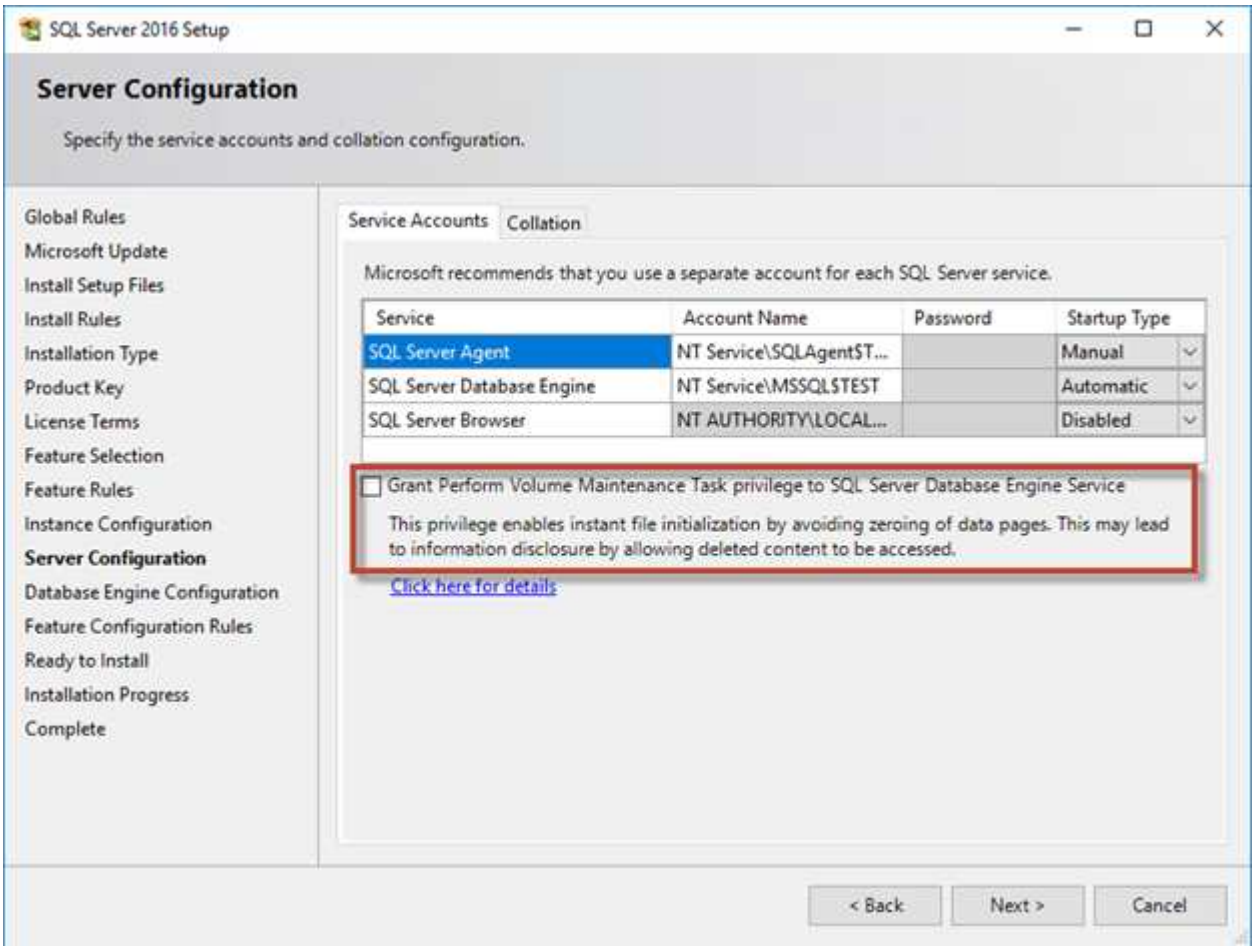
Para verificar se a permissão está ativada, você pode usar o código do exemplo a seguir. Esse código define dois sinalizadores de rastreamento que forçam o SQL Server a gravar informações adicionais no log de erros, criar um pequeno banco de dados e ler o conteúdo do log.

```
DBCC TRACEON(3004,3605,-1)
GO
CREATE DATABASE DelMe
GO
EXECUTE sp_readerrorlog
GO
DROP DATABASE DelMe
GO
DBCC TRACEOFF(3004,3605,-1)
GO
```

Quando a inicialização instantânea do arquivo não está ativada, o log de erro do SQL Server mostra que o SQL Server está zerando o arquivo de dados do mdf, além de zerar o arquivo de log ldf, como mostrado no exemplo a seguir. Quando a inicialização instantânea do arquivo está ativada, ele exibe apenas a restauração do arquivo de log.

	LogDate	ProcessInfo	Text
365	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 flush delta counts.
366	2017-02-09 08:10:07.660	spid53	Ckpt dbid 3 logging active xact info.
367	2017-02-09 08:10:07.750	spid53	Ckpt dbid 3 phase 1 ended (8)
368	2017-02-09 08:10:07.750	spid53	About to log Checkpoint end.
369	2017-02-09 08:10:07.880	spid53	Ckpt dbid 3 complete
370	2017-02-09 08:10:08.130	spid53	Starting up database 'DelMe'.
371	2017-02-09 08:10:08.150	spid53	FixupLogTail(progress) zeroing C:\Program Files\Micros
372	2017-02-09 08:10:08.160	spid53	Zeroing C:\Program Files\Microsoft SQL Server\MSSQ
373	2017-02-09 08:10:08.170	spid53	Zeroing completed on C:\Program Files\Microsoft SQL
374	2017-02-09 08:10:08.710	spid53	Ckpt dbid 6 started
375	2017-02-09 08:10:08.710	spid53	About to log Checkpoint begin.

A tarefa realizar manutenção de volume é simplificada no SQL Server 2016 e é fornecida posteriormente como uma opção durante o processo de instalação. Esta figura exibe a opção de conceder ao serviço do mecanismo de banco de dados SQL Server o privilégio de executar a tarefa de manutenção de volume.



Outra opção importante de banco de dados que controla os tamanhos de arquivo de banco de dados é o auto-retrátil. Quando essa opção está ativada, o SQL Server diminui regularmente os arquivos do banco de dados, reduz seu tamanho e libera espaço para o sistema operacional. Esta operação é intensiva em recursos e raramente é útil porque os arquivos de banco de dados crescem novamente após algum tempo quando novos dados entram no sistema. O Autoshink não deve ser ativado no banco de dados.

Diretório de log

O diretório de log é especificado no SQL Server para armazenar dados de backup de log de transação no nível do host. Se você estiver usando o SnapCenter para fazer backup de arquivos de log, cada host do SQL Server usado pelo SnapCenter deve ter um diretório de log do host configurado para executar backups de log.

Coloque o diretório de registo numa unidade de armazenamento dedicada. A quantidade de dados no diretório de log do host depende do tamanho dos backups e do número de dias em que os backups são mantidos. O SnapCenter permite apenas um diretório de log de host por host do SQL Server. Você pode configurar os diretórios de log do host em SnapCenter -→ Host -→ Configurar Plug-in.

A NetApp recomenda o seguinte para um diretório de log do host:

- Certifique-se de que o diretório de log do host não é compartilhado por nenhum outro tipo de dados que possa potencialmente corromper os dados instantâneos do backup.
- Crie o diretório de log do host em uma unidade de armazenamento dedicada à qual o SnapCenter copia logs de transações.
- Se você estiver usando uma instância de cluster sempre em failover, a unidade de armazenamento usada para o diretório de log do host deve ser um recurso de disco de cluster no mesmo grupo de cluster que a instância do SQL Server que está sendo feita backup no SnapCenter.

Proteção de dados

As estratégias de backup de banco de dados devem ser baseadas em requisitos de negócios identificados, não em recursos teóricos. Ao combinar a tecnologia Snapshot da ONTAP e aproveitar as API do Microsoft SQL Server, você pode rapidamente fazer backup consistente de aplicativos, independentemente do tamanho dos bancos de dados do usuário. Para requisitos de gerenciamento de dados mais avançados ou com escalabilidade horizontal, a NetApp oferece SnapCenter.

SnapCenter

O SnapCenter é o software de proteção de dados da NetApp para aplicações empresariais. Os bancos de dados do SQL Server podem ser protegidos rápida e facilmente com o plug-in do SnapCenter para SQL Server e com operações do SO gerenciadas pelo plug-in do SnapCenter para Microsoft Windows.

A instância do SQL Server pode ser uma configuração autônoma, uma instância de cluster de failover ou pode estar sempre no grupo de disponibilidade. O resultado é que, a partir de um painel único, os bancos de dados podem ser protegidos, clonados e restaurados da cópia primária ou secundária. O SnapCenter pode gerenciar bancos de dados do SQL Server tanto no local, na nuvem e configurações híbridas. Cópias de banco de dados também podem ser criadas em poucos minutos no host original ou alternativo para desenvolvimento ou para fins de geração de relatórios.

O SQL Server também requer coordenação entre o sistema operacional e o armazenamento para garantir que os dados corretos estejam presentes em snapshots no momento da criação. Na maioria dos casos, o único método seguro para fazer isso é com SnapCenter ou T-SQL. Os instantâneos criados sem essa coordenação adicional podem não ser recuperáveis de forma confiável.

Para obter mais detalhes sobre o plug-in do SQL Server para SnapCenter, "TR-4714: Guia de práticas recomendadas para SQL Server usando NetApp SnapCenter"consulte .

Proteção de banco de dados usando snapshots T-SQL

No SQL Server 2022, a Microsoft introduziu snapshots T-SQL que oferece um caminho para a execução de scripts e automação de operações de backups. Em vez de executar cópias de tamanho completo, você pode preparar o banco de dados para snapshots. Depois que o banco de dados estiver pronto para backup, você poderá aproveitar as APIs REST do ONTAP para criar snapshots.

O seguinte é um exemplo de fluxo de trabalho de backup:

1. Congelar um banco de dados com comando ALTER. Ele prepara o banco de dados para um snapshot consistente no storage subjacente. Após o congelamento, você pode descongelar o banco de dados e gravar o instantâneo com o comando BACKUP.
2. Execute snapshots de vários bancos de dados nas unidades de armazenamento simultaneamente com os novos comandos DO GRUPO DE backup e DO SERVIDOR DE BACKUP.
3. Se a carga de trabalho do banco de dados for expandida em várias unidades de armazenamento, crie grupos de consistência para simplificar a tarefa de gerenciamento. O grupo de consistência é um conjunto de unidades de armazenamento que são gerenciadas como uma única unidade.
4. Execute backups COMPLETOS ou backups COMPLETOS Copy_ONLY. Esses backups também são gravados em msdb.
5. Execute recuperação pontual usando backups de log feitos com a abordagem de streaming normal após o backup COMPLETO do snapshot. Backups diferenciais de streaming também são suportados, se desejado.

Para saber mais, "Documentação da Microsoft para saber sobre os snapshots T-SQL"consulte .

A NetApp recomenda usar o SnapCenter para criar cópias Snapshot. O método T-SQL descrito acima também funciona, mas o SnapCenter oferece automação completa no processo de backup, restauração e clonagem. Ele também executa a descoberta para garantir que os snapshots corretos estejam sendo criados.

Recuperação de desastres

Recuperação de desastres

Bancos de dados empresariais e infraestruturas de aplicações geralmente exigem replicação para proteger contra desastres naturais ou interrupções inesperadas dos negócios com o mínimo de tempo de inatividade.

O recurso de replicação de grupo de disponibilidade contínua do SQL Server pode ser uma excelente opção, e o NetApp oferece opções para integrar a proteção de dados sempre ativa. Em alguns casos, no entanto, você pode querer considerar a tecnologia de replicação do ONTAP usando as seguintes opções.

SnapMirror

A tecnologia SnapMirror oferece uma solução empresarial rápida e flexível para replicação de dados em LANs e WANs. A tecnologia SnapMirror transfere apenas blocos de dados alterados para o destino após a criação do espelhamento inicial, reduzindo significativamente os requisitos de largura de banda da rede. Ele pode ser configurado em modo síncrono ou assíncrono. A replicação síncrona do SnapMirror no NetApp ASA é configurada usando a sincronização ativa do SnapMirror.

Sincronização ativa do SnapMirror

Para muitos clientes, a continuidade dos negócios exige mais do que apenas possuir uma cópia remota de dados. Para isso, ela exige a capacidade de usar rapidamente esses dados, o que é possível no NetApp ONTAP usando a sincronização ativa do SnapMirror

Com o SnapMirror active Sync, você tem essencialmente dois sistemas ONTAP diferentes que mantêm cópias independentes dos seus dados LUN, mas cooperam para apresentar uma única instância desse LUN. Do ponto de vista do host, é uma única entidade LUN. A sincronização ativa do SnapMirror é suportada para LUN baseado em iSCSI/FC.

O SnapMirror active Sync pode fornecer replicação RPO igual a 0 e é fácil de implementar entre dois clusters independentes. Assim que as duas cópias de dados estiverem sincronizadas, os dois clusters só precisam espelhar gravações. Quando ocorre uma gravação em um cluster, ela é replicada para o outro cluster. A gravação só é reconhecida para o host quando a gravação for concluída em ambos os sites. Além desse comportamento de divisão de protocolo, os dois clusters são, de outra forma, clusters ONTAP normais.

Um dos principais casos de uso para SM-as é a replicação granular. Às vezes, você não quer replicar todos os dados como uma única unidade ou precisa ser capaz de falhar seletivamente em determinados workloads.

Outro importante caso de uso para SM-as é para operações ativas-ativas, em que você deseja que cópias totalmente utilizáveis de dados estejam disponíveis em dois clusters diferentes localizados em dois locais diferentes com características de desempenho idênticas e, se desejado, não é necessário estender a SAN entre locais. Você pode ter suas aplicações já em execução em ambos os locais, contanto que a aplicação seja compatível, o que reduz o rto geral durante operações de failover.

SnapMirror

Veja a seguir as recomendações do SnapMirror para SQL Server:

- Use a replicação síncrona com o SnapMirror active Sync, onde a demanda por recuperação rápida de dados é maior e soluções assíncronas para flexibilidade no RPO.
- Se você estiver usando o SnapCenter para fazer backup de bancos de dados e replicar snapshots para um cluster remoto, não programe atualizações do SnapMirror dos controladores para fins de consistência. Em vez disso, ative as atualizações do SnapMirror do SnapCenter para atualizar o SnapMirror após a conclusão da cópia de segurança completa ou de registo.
- Equilibre as unidades de storage que contêm dados do SQL Server entre diferentes nós no cluster para permitir que todos os nós de cluster compartilhem a atividade de replicação do SnapMirror. Essa distribuição otimiza o uso de recursos de nós.

Para obter mais informações sobre o SnapMirror, "TR-4015: Guia de práticas recomendadas e configuração do SnapMirror para ONTAP 9"consulte .

Sincronização ativa do SnapMirror

Visão geral

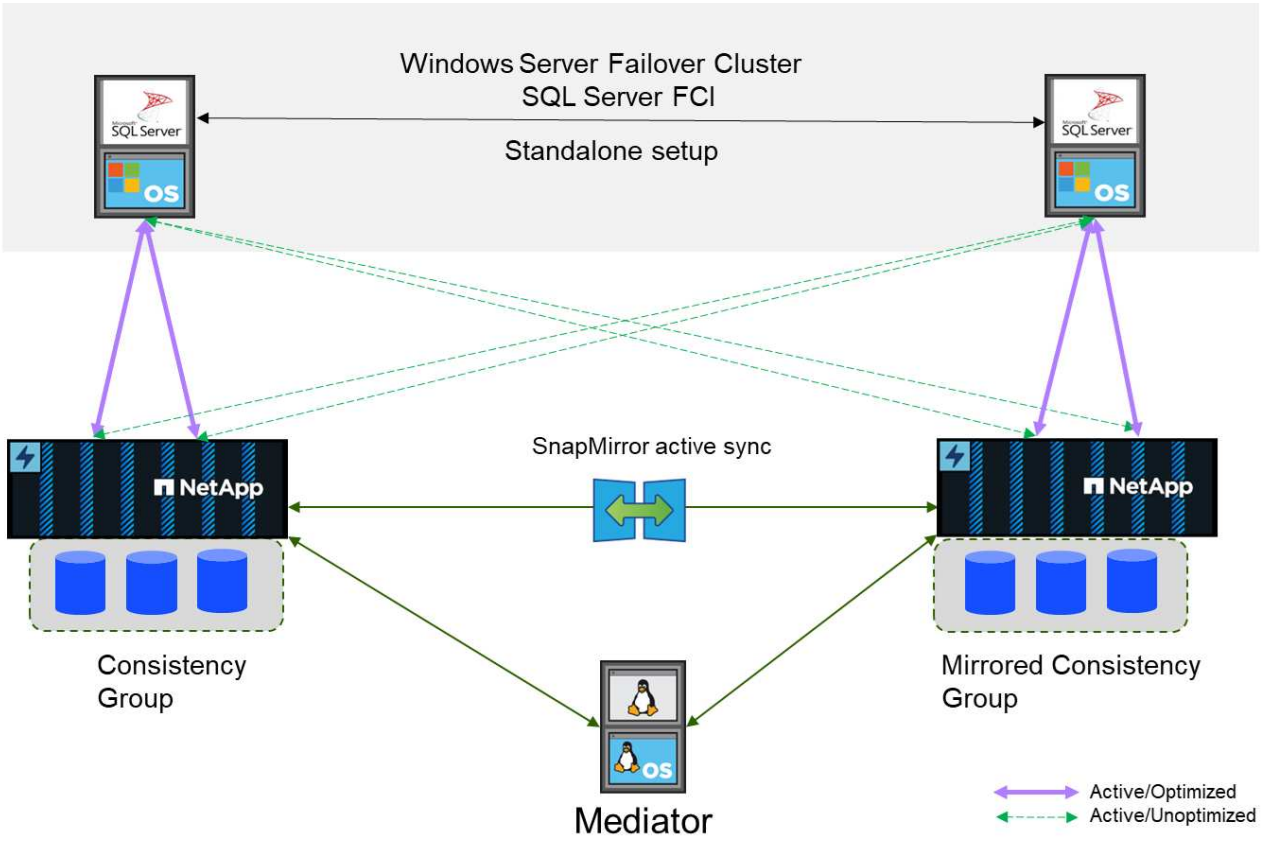
O SnapMirror active Sync permite que bancos de dados e aplicações individuais do SQL Server continuem as operações durante interrupções de storage e rede, com failover transparente de storage sem qualquer intervenção manual.

O SnapMirror active Sync é compatível com arquitetura ativo-ativo simétrica que fornece replicação bidirecional síncrona para continuidade dos negócios e recuperação de desastres. Ele ajuda você a proteger o

acesso a dados para workloads SAN críticos com acesso de leitura e gravação simultâneos a dados em vários domínios de falha, garantindo operações ininterruptas e minimizando o tempo de inatividade durante desastres ou falhas do sistema.

Os hosts do SQL Server acessam o storage usando Fibre Channel (FC) ou iSCSI LUNs. Replicação entre cada cluster que hospeda uma cópia dos dados replicados. Como esse recurso é replicação no nível de armazenamento, as instâncias do SQL Server executadas em instâncias de cluster de host ou failover independentes podem executar operações de leitura/gravação em cluster. Para obter informações sobre as etapas de Planejamento e configuração, "Documentação do ONTAP na sincronização ativa do SnapMirror"consulte .

Arquitetura do SnapMirror ativo com ativo-ativo simétrico



Replicação síncrona

Em operação normal, cada cópia é uma réplica síncrona RPO/0 em todos os momentos, com uma exceção. Se os dados não puderem ser replicados, o ONTAP cumprirá o requisito de replicar dados e retomar a distribuição de I/o em um local, enquanto os LUNs no outro local ficam offline.

Hardware de armazenamento

Ao contrário de outras soluções de recuperação de desastres de storage, o SnapMirror active Sync oferece flexibilidade assimétrica de plataforma. O hardware em cada local não precisa ser idêntico. Esse recurso permite dimensionar corretamente o hardware usado para suportar a sincronização ativa do SnapMirror. O sistema de storage remoto pode ser idêntico ao local principal se precisar dar suporte a uma carga de trabalho de produção completa, mas se um desastre resultar em e/S reduzida, do que um sistema menor no local remoto pode ser mais econômico.

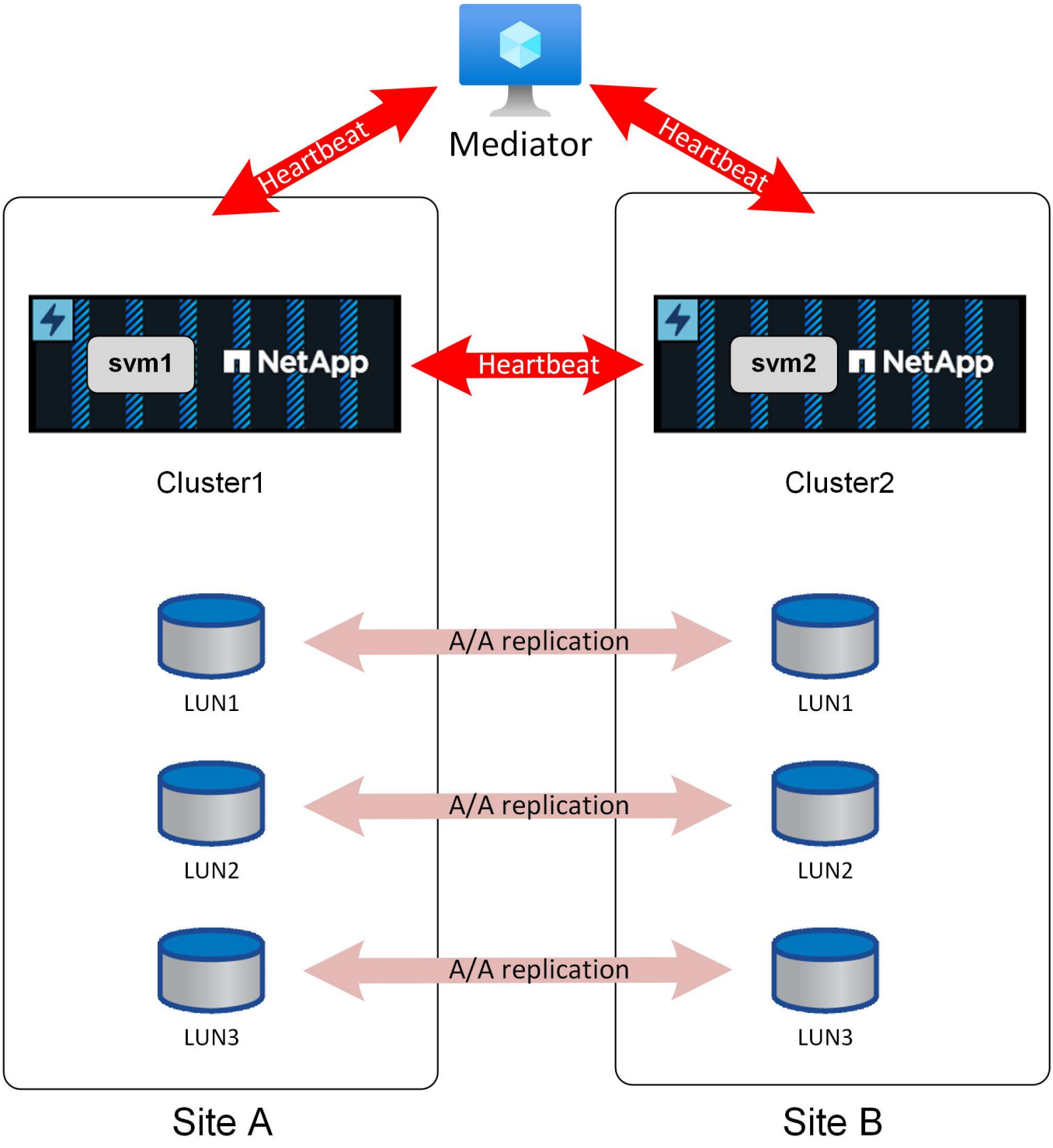
Mediador ONTAP

O Mediador ONTAP é um aplicativo de software que é baixado do suporte do NetApp e normalmente é implantado em uma pequena máquina virtual. O Mediador ONTAP não é um tiebreaker. É um canal de comunicação alternativo para os dois clusters que participam da replicação de sincronização ativa do SnapMirror. As operações automatizadas são orientadas pelo ONTAP com base nas respostas recebidas do parceiro por meio de conexões diretas e por meio do mediador.

Mediador do ONTAP

O mediador é necessário para automatizar o failover com segurança. Idealmente, ele seria colocado em um local 3rd independente, mas ainda pode funcionar para a maioria das necessidades se colocasse em um dos clusters que participam da replicação.

O mediador não é realmente um tiebreaker, embora essa seja efetivamente a função que ele fornece. Ele não realiza nenhuma ação; em vez disso, fornece um canal de comunicação alternativo para comunicação de cluster para cluster.



O desafio nº 1 com failover automatizado é o problema de split-brain, e esse problema surge se os dois locais perderem a conetividade entre si. O que deve acontecer? Você não quer que dois sites diferentes se designem como as cópias sobreviventes dos dados, mas como um único site pode dizer a diferença entre a perda real do site oposto e a incapacidade de se comunicar com o site oposto?

É aqui que o mediador entra na imagem. Se for colocado em um site 3rd e cada site tiver uma conexão de rede separada com esse site, então você terá um caminho adicional para cada site validar a integridade do outro. Olhe para a imagem acima novamente e considere os seguintes cenários.

- O que acontece se o mediador falhar ou não estiver acessível a partir de um ou de ambos os sites?
  - Os dois clusters ainda podem se comunicar entre si pelo mesmo link usado para serviços de replicação.
  - Os dados ainda são servidos com proteção RPO igual a 0
- O que acontece se o Site A falhar?
  - O local B verá ambos os canais de comunicação diminuírem.
  - O local B assumirá os serviços de dados, mas sem o espelhamento RPO igual a 0
- O que acontece se o local B falhar?
  - O local A verá ambos os canais de comunicação diminuírem.
  - O local A assumirá os serviços de dados, mas sem o espelhamento do RPO igual a 0

Há um outro cenário a considerar: Perda do link de replicação de dados. Se o link de replicação entre locais for perdido, o espelhamento RPO 0 obviamente será impossível. O que deve acontecer então?

Isso é controlado pelo status do site preferido. Em uma relação SM-as, um dos locais é secundário ao outro. Isso não tem efeito nas operações normais, e todo o acesso aos dados é simétrico, mas se a replicação for interrompida, o empate terá que ser quebrado para retomar as operações. O resultado é que o local preferido continuará as operações sem espelhamento, e o local secundário interromperá o processamento de e/S até que a comunicação de replicação seja restaurada.

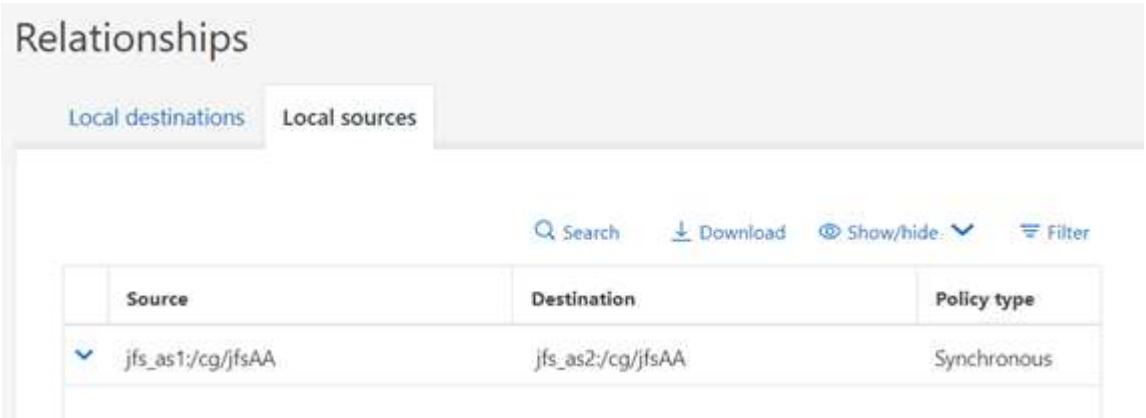
Site preferido

O comportamento de sincronização ativa do SnapMirror é simétrico, com uma exceção importante - configuração de site preferida.

A sincronização ativa do SnapMirror considerará um site a "fonte" e o outro o "destino". Isso implica uma relação de replicação unidirecional, mas isso não se aplica ao comportamento de IO. A replicação é bidirecional e simétrica, e os tempos de resposta de e/S são os mesmos em ambos os lados do espelho.

A `source` designação é controla o local preferido. Se o link de replicação for perdido, os caminhos de LUN na cópia de origem continuarão a servir dados enquanto os caminhos de LUN na cópia de destino ficarão indisponíveis até que a replicação seja restabelecida e o SnapMirror reinsira um estado síncrono. Os caminhos irão então retomar a veiculação de dados.

A configuração de origem/destino pode ser visualizada através do SystemManager:



Ou na CLI:

```
Cluster2::> snapmirror show -destination-path jfs_as2:/cg/jfsAA

                           Source Path: jfs_as1:/cg/jfsAA
                     Destination Path: jfs_as2:/cg/jfsAA
                    Relationship Type: XDP
                Relationship Group Type: consistencygroup
                    SnapMirror Schedule: -
                 SnapMirror Policy Type: automated-failover-duplex
                      SnapMirror Policy: AutomatedFailOverDuplex
                            Tries Limit: -
                      Throttle (KB/sec): -
                           Mirror State: Snapmirrored
                    Relationship Status: InSync
```

O segredo é que a fonte é o SVM no cluster1. Como mencionado acima, os termos "fonte" e "destino" não descrevem o fluxo de dados replicados. Ambos os sites podem processar uma gravação e replicá-la para o site oposto. Com efeito, ambos os clusters são fontes e destinos. O efeito de designar um cluster como uma fonte simplesmente controla qual cluster sobrevive como um sistema de armazenamento de leitura e gravação se o link de replicação for perdido.

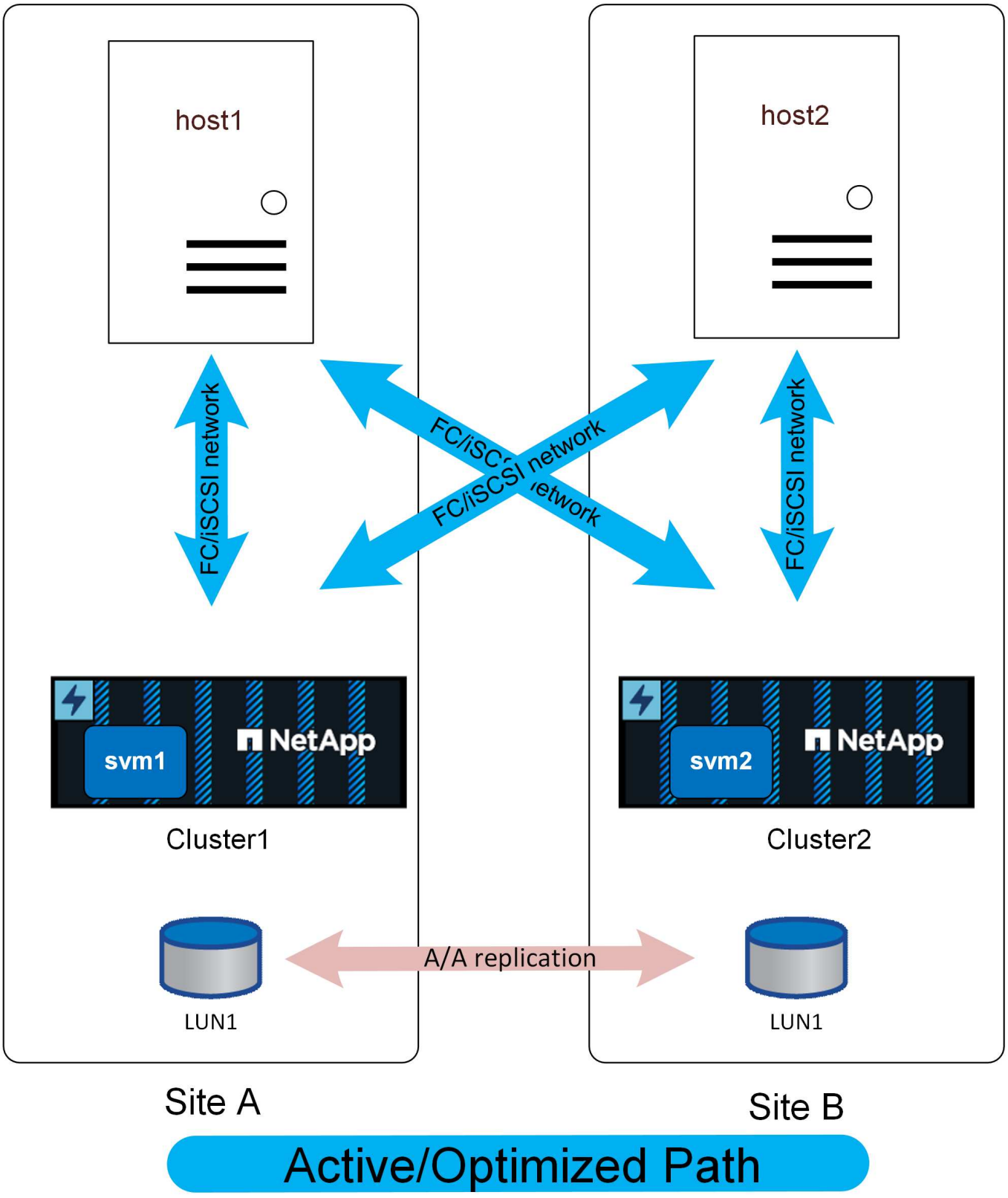
Topologia de rede

Acesso uniforme

Rede de acesso uniforme significa que os hosts são capazes de acessar caminhos em ambos os sites (ou domínios de falha dentro do mesmo site).

Um recurso importante do SM-as é a capacidade de configurar os sistemas de storage para saber onde os hosts estão localizados. Quando você mapeia os LUNs para um determinado host, você pode indicar se eles são ou não proximais a um determinado sistema de armazenamento.

Os sistemas NetApp ASA oferecem multipathing ativo-ativo em todos os caminhos em um cluster. Isso também se aplica às configurações SM-as.



Com acesso uniforme, o IO estaria atravessando a WAN. É um cluster de rede de malha completa e isso pode ou não ser desejável para todos os casos de uso.

Se os dois locais estivessem a 100 metros de distância com conetividade de fibra, não deveria haver latência adicional detetável cruzando a WAN, mas se os locais estivessem a uma distância longa, então o

desempenho de leitura sofreria em ambos os locais. O ASA com rede de acesso não uniforme seria uma opção para obter os benefícios de custo e recursos do ASA sem incorrer em uma penalidade de acesso à latência entre sites ou usar o recurso de proximidade do host para permitir acesso local de leitura/gravação para ambos os sites.

O ASA com SM-as em uma configuração de baixa latência oferece dois benefícios interessantes. Primeiro, ele basicamente **dobra** a performance de qualquer host porque a e/S pode ser atendida por duas vezes mais controladoras usando o dobro de caminhos. Em segundo lugar, em um ambiente de local único, ele oferece disponibilidade extrema porque todo um sistema de storage pode ser perdido sem interromper o acesso de host.

Definições de proximidade

Proximidade refere-se a uma configuração por cluster que indica que um determinado host WWN ou ID de iniciador iSCSI pertence a um host local. É uma segunda etapa opcional para configurar o acesso LUN.

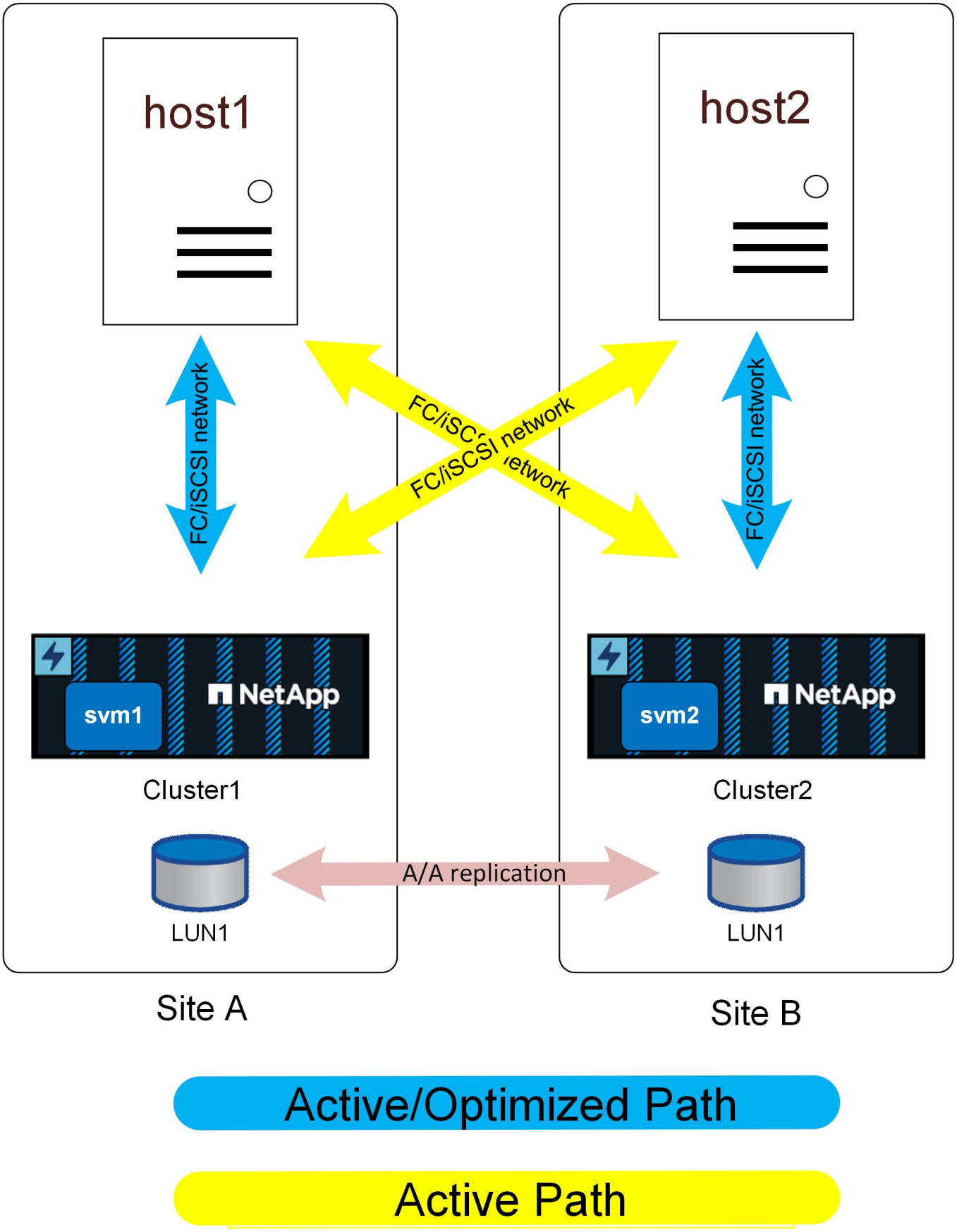
O primeiro passo é a configuração usual do igroup. Cada LUN deve ser mapeado para um grupo que contenha as IDs WWN/iSCSI dos hosts que precisam de acesso a esse LUN. Isso controla qual host tem *access* para um LUN.

A segunda etapa opcional é configurar a proximidade do host. Isso não controla o acesso, ele controla *Priority*.

Por exemplo, um host no local A pode ser configurado para acessar um LUN que é protegido pela sincronização ativa do SnapMirror e, como a SAN é estendida entre sites, há caminhos disponíveis para esse LUN usando armazenamento no local A ou armazenamento no local B.

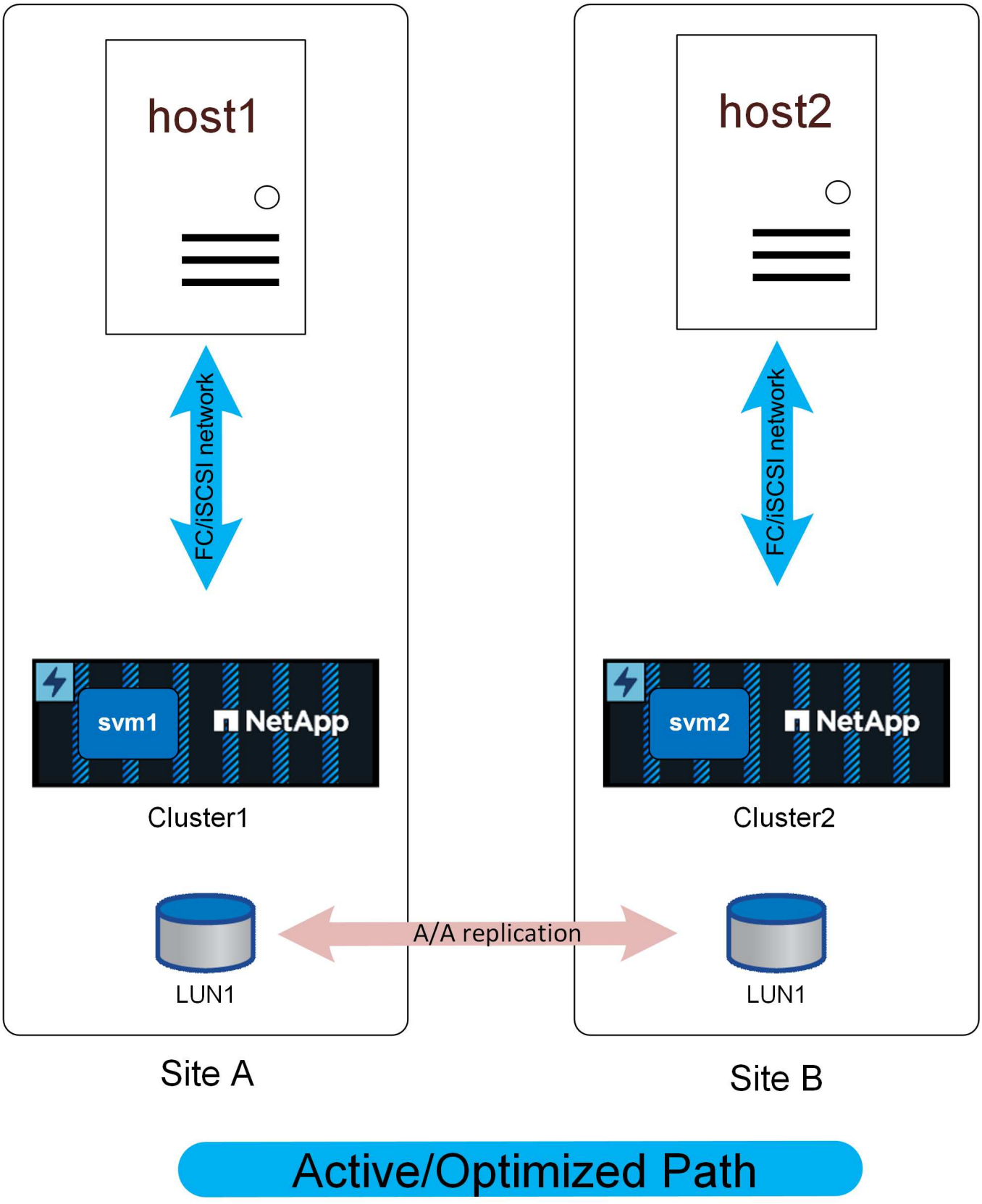
Sem configurações de proximidade, esse host usará ambos os sistemas de storage igualmente porque ambos os sistemas de storage anunciarão caminhos ativos/otimizados. Se a latência da SAN e/ou a largura de banda entre locais for limitada, isso pode não ser desejado e você pode querer garantir que, durante a operação normal, cada host utilize preferencialmente caminhos para o sistema de armazenamento local. Isso é configurado adicionando o ID WWN/iSCSI do host ao cluster local como um host proximal. Isso pode ser feito na CLI ou no SystemManager.

Os caminhos aparecerão como mostrado abaixo quando a proximidade do host for configurada.


host1
host2
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
FC/iSCSI network
svm1
NetApp
svm2
NetApp
Cluster1
Cluster2
A/A replication
LUN1
LUN1
Site A
Site B
Active/Optimized Path
Active Path

Acesso não uniforme

A rede de acesso não uniforme significa que cada host só tem acesso às portas no sistema de storage local. A SAN não é estendida entre sites (ou domínios de falha dentro do mesmo site).



O principal benefício dessa abordagem é a simplicidade da SAN - você elimina a necessidade de estender uma SAN pela rede. Alguns clientes não têm conetividade de baixa latência suficiente entre locais ou não têm infraestrutura para túnel do tráfego SAN FC em uma rede entre locais.

A desvantagem para o acesso não uniforme é que certos cenários de falha, incluindo a perda do link de replicação, resultarão em alguns hosts perdendo acesso ao armazenamento. Os aplicativos que são executados como instâncias únicas, como um banco de dados não agrupado, que inerentemente está sendo executado apenas em um único host em qualquer montagem, falharão se a conetividade de armazenamento local for perdida. Os dados ainda seriam protegidos, mas o servidor de banco de dados não teria mais acesso. Ele precisaria ser reiniciado em um local remoto, de preferência através de um processo automatizado. Por exemplo, o VMware HA pode detetar uma situação de todos os caminhos em um servidor e reiniciar uma VM em outro servidor onde os caminhos estão disponíveis.

Em contraste, um aplicativo em cluster, como o Oracle RAC, pode fornecer um serviço que está disponível simultaneamente em dois locais diferentes. Perder um site não significa perda do serviço do aplicativo como um todo. As instâncias ainda estão disponíveis e em execução no local sobrevivente.

Em muitos casos, a sobrecarga de latência adicional de um aplicativo que acessa o storage em um link local a local seria inaceitável. Isso significa que a disponibilidade aprimorada de redes uniformes é mínima, uma vez que a perda de armazenamento em um local levaria à necessidade de encerrar serviços nesse local com falha de qualquer maneira.

Há caminhos redundantes pelo cluster local que não são mostrados nesses diagramas por uma questão de simplicidade. Os sistemas de storage da ONTAP estão HA, portanto, uma falha da controladora não deve resultar em falha do local. Deve apenas resultar em uma mudança na qual os caminhos locais são usados no site afetado.

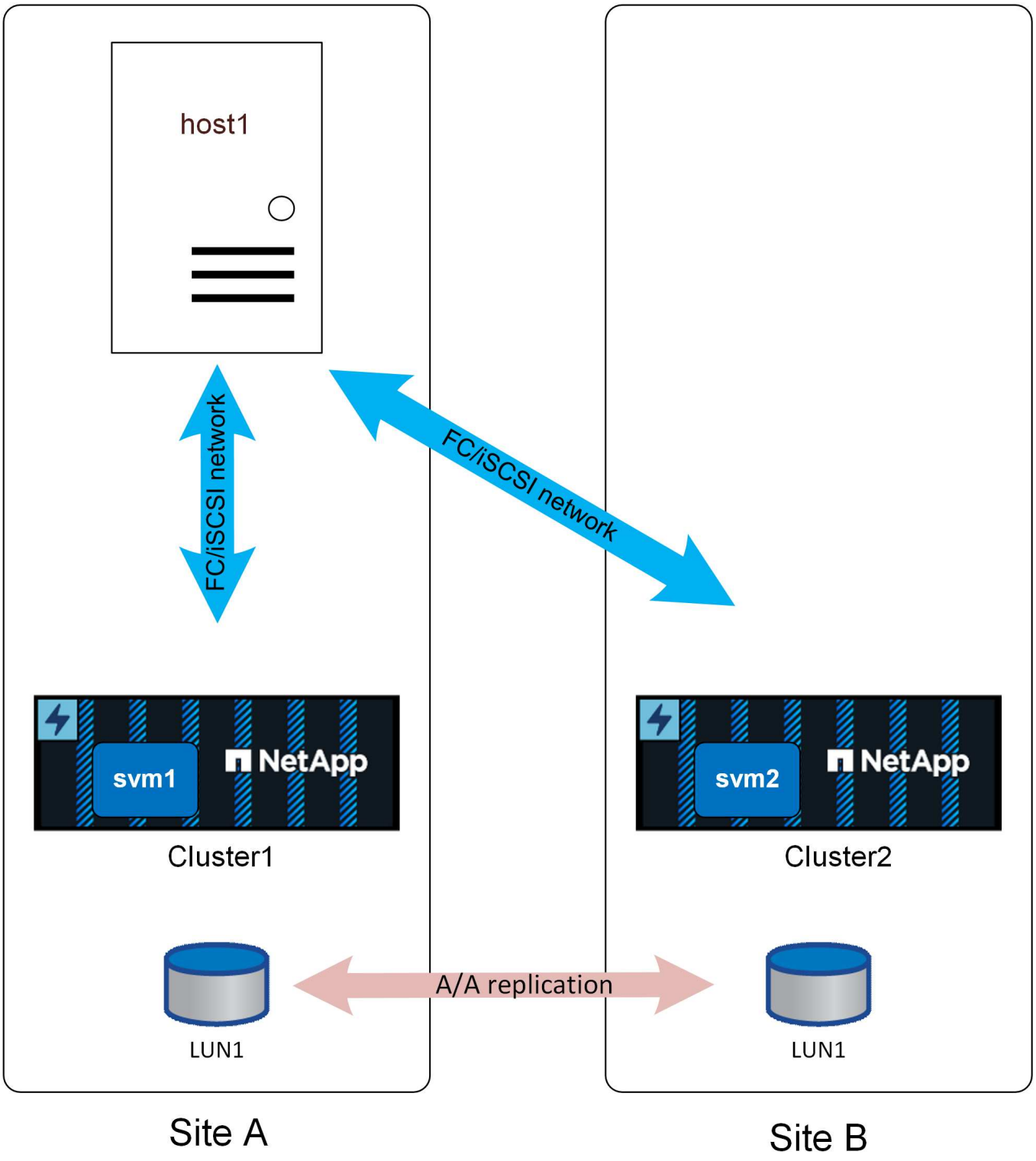
Visão geral

O SQL Server pode ser configurado para trabalhar com a sincronização ativa do SnapMirror de várias maneiras. A resposta certa depende da conectividade de rede disponível, dos requisitos de RPO e dos requisitos de disponibilidade.

Instância autônoma do SQL Server

As práticas recomendadas para layout de arquivo e configuração de servidor são as mesmas recomendadas "SQL Server no ONTAP"na documentação.

Com uma configuração autônoma, o SQL Server poderia estar sendo executado apenas em um site. Presumivelmente "uniforme" o acesso seria usado.



Com acesso uniforme, uma falha de armazenamento em qualquer um dos locais não interromperia as operações do banco de dados. Uma falha completa do local no site que incluía o servidor do banco de dados resultaria, naturalmente, em uma falha.

Alguns clientes podem configurar um sistema operacional em execução no site remoto com uma configuração pré-configurada do SQL Server, atualizada com uma versão de compilação equivalente como a da instância de produção. O failover exigiria a ativação dessa instância autônoma do SQL Server no local alternativo, a descoberta dos LUNS e a inicialização do banco de dados. O processo completo pode ser automatizado com

o cmdlet do Windows PowerShell, pois não são necessárias operações do lado do storage.

"Não uniforme" o acesso também poderia ser usado, mas o resultado seria uma interrupção do banco de dados se o sistema de storage em que o servidor de banco de dados estava localizado tivesse falhado porque o banco de dados não teria caminhos disponíveis para o storage. Isso ainda pode ser aceitável em alguns casos. O SnapMirror ative Sync ainda estaria fornecendo proteção de dados RPO igual a 0 e, em caso de falha do local, a cópia sobrevivente estaria ativa e pronta para retomar as operações usando o mesmo procedimento usado com acesso uniforme, conforme descrito acima.

Um processo de failover simples e automatizado pode ser mais facilmente configurado com o uso de um host Virtualize. Por exemplo, se os arquivos de dados do SQL Server forem replicados sincronamente para o armazenamento secundário, juntamente com um VMDK de inicialização, em caso de desastre, o ambiente completo poderá ser ativado no local alternativo. Um administrador pode ativar manualmente o host no local sobrevivente ou automatizar o processo por meio de um serviço como o VMware HA.

Instância de cluster de failover do SQL Server

As instâncias de failover do SQL Server também podem ser hospedadas em um cluster de failover do Windows executado em um servidor físico ou servidor virtual como sistema operacional convidado. Essa arquitetura de vários hosts oferece resiliência de armazenamento e instância do SQL Server. Essa implantação é útil em ambientes de alta demanda que buscam processos de failover robustos, mantendo o desempenho aprimorado. Em uma configuração de cluster de failover, quando um host ou storage primário é afetado, o SQL Services será failover para o host secundário e, ao mesmo tempo, o storage secundário estará disponível para servir e/S. Nenhum script de automação ou intervenção do administrador é necessário.

Cenários de falha

Planejar uma arquitetura completa de aplicativos de sincronização ativa do SnapMirror requer entender como o SM-as responderá em vários cenários de failover planejados e não planejados.

Para os exemplos a seguir, suponha que o site A esteja configurado como o site preferido.

Perda de conetividade de replicação

Se a replicação SM-as for interrompida, não é possível concluir a e/S de gravação porque seria impossível que um cluster replique alterações no local oposto.

Local A (local preferido)

O resultado da falha do link de replicação no site preferido será uma pausa de aproximadamente 15 segundos no processamento de e/S de gravação, à medida que o ONTAP tenta novamente as operações de gravação replicadas antes de determinar que o link de replicação é genuinamente inacessível. Após os 15 segundos decorridos, o Site Um sistema retoma o processamento de e/S de leitura e escrita. Os caminhos de SAN não serão alterados e os LUNs permanecerão online.

Local B

Como o local B não é o site preferido de sincronização ativa do SnapMirror, seus caminhos de LUN ficarão indisponíveis após cerca de 15 segundos.

Falha do sistema de storage

O resultado de uma falha do sistema de armazenamento é quase idêntico ao resultado da perda do link de replicação. O local sobrevivente deve experimentar uma pausa de IO de aproximadamente 15 segundos. Uma

vez decorrido esse período de 15 segundos, o IO será retomado nesse site como de costume.

Perda do mediador

O serviço mediador não controla diretamente as operações de storage. Ele funciona como um caminho de controle alternativo entre clusters. Ele existe principalmente para automatizar o failover sem o risco de um cenário de divisão cerebral. Em operação normal, cada cluster replica alterações em seu parceiro, e cada cluster pode verificar se o cluster do parceiro está on-line e fornecendo dados. Se o link de replicação falhar, a replicação cessaria.

O motivo pelo qual um mediador é necessário para o failover automatizado seguro é porque, de outra forma, seria impossível que um cluster de storage pudesse determinar se a perda de comunicação bidirecional foi o resultado de uma interrupção da rede ou falha real do storage.

O mediador fornece um caminho alternativo para cada cluster para verificar a integridade de seu parceiro. Os cenários são os seguintes:

- Se um cluster puder entrar em Contato diretamente com seu parceiro, os serviços de replicação estarão operacionais. Nenhuma ação necessária.
- Se um site preferido não puder entrar em Contato diretamente com seu parceiro ou por meio do mediador, ele assumirá que ele está realmente indisponível ou foi isolado e que levou seus caminhos LUN off-line. O site preferido continuará lançando o estado RPO/0 e continuará processando e/S de leitura e gravação.
- Se um site não preferencial não puder entrar em Contato diretamente com seu parceiro, mas puder contatá-lo por meio do mediador, ele tomará seus caminhos off-line e aguardará o retorno da conexão de replicação.
- Se um site não preferencial não puder entrar em Contato com seu parceiro diretamente ou por meio de um mediador operacional, ele assumirá que o parceiro está realmente indisponível ou foi isolado e que tomou seus caminhos LUN off-line. O site não preferencial lançará o estado RPO 0 e continuará processando e/S de leitura e gravação. Ele assumirá o papel da fonte de replicação e se tornará o novo site preferido.

Se o mediador não estiver totalmente disponível:

- A falha dos serviços de replicação por qualquer motivo, incluindo a falha do sistema de storage ou local não preferido, resultará no lançamento do estado RPO/0 e no reinício do processamento de e/S de leitura e gravação. O site não preferencial tomará seus caminhos off-line.
- A falha do site preferido resultará em uma falha porque o site não-preferido não será capaz de verificar se o site oposto está realmente off-line e, portanto, não seria seguro para o site não-preferido retomar os serviços.

Restauração de serviços

Depois que uma falha é resolvida, como restaurar a conetividade site-a-site ou ligar um sistema com falha, os pontos de extremidade de sincronização ativa do SnapMirror detetarão automaticamente a presença de uma relação de replicação com defeito e o devolverão ao estado RPO-0. Uma vez que a replicação síncrona for restabelecida, os caminhos com falha ficarão online novamente.

Em muitos casos, os aplicativos em cluster detetarão automaticamente o retorno de caminhos com falha, e esses aplicativos também voltarão online. Em outros casos, pode ser necessária uma análise SAN no nível do host ou os aplicativos podem precisar ser colocados online manualmente. Depende do aplicativo e como ele é configurado e, em geral, essas tarefas podem ser facilmente automatizadas. O próprio ONTAP é com autorrecuperação e não deve exigir a intervenção do usuário para retomar as operações de storage RPO de 0.

Failover manual

Alterar o local preferido requer uma operação simples. A e/S pausa por um segundo ou dois como autoridade sobre os switches de comportamento de replicação entre clusters, mas a e/S não é afetada.

Informações sobre direitos autorais

Informações sobre marcas comerciais