



Conceitos de SAN

ONTAP 9

NetApp
January 17, 2025

Índice

- Conceitos de SAN 1
 - Provisionamento DE SAN com iSCSI 1
 - Gerenciamento de serviços iSCSI 2
 - Provisionamento DE SAN com FC 8
 - Provisionamento DE SAN com NVMe 9
- Volumes SAN 10
 - Gerenciamento de espaço no lado do host SAN 15
 - Sobre os grupos 16
 - Especifique WWPNs do iniciador e nomes de nó iSCSI para um grupo 17
 - Virtualização de storage com descarga de cópia VMware e Microsoft 18

Conceitos de SAN

Provisionamento DE SAN com iSCSI

Em ambientes SAN, os sistemas de armazenamento são alvos que têm dispositivos de armazenamento de destino. Para iSCSI e FC, os dispositivos de destino de armazenamento são referidos como LUNs (unidades lógicas). Para Non-Volatile Memory Express (NVMe) em Fibre Channel, os dispositivos de destino de storage são chamados de namespaces.

Você configura o storage criando LUNs para iSCSI e FC ou criando namespaces para NVMe. Os LUNs ou namespaces são então acessados por hosts que usam redes de protocolo iSCSI (Internet Small Computer Systems Interface) ou Fibre Channel (FC).

Para se conectar a redes iSCSI, os hosts podem usar placas de rede Ethernet (NICs) padrão, TOE (TCP offload Engine) com iniciadores de software, adaptadores de rede convergidos (CNAs) ou adaptadores de barramento de host iSCSI dedicados (HBAs).

Para se conectar a redes FC, os hosts exigem HBAs FC ou CNAs.

Os protocolos FC compatíveis incluem:

- FC
- FCoE
- NVMe

Ligações e nomes de rede de nó de destino iSCSI

Os nós de destino iSCSI podem se conectar à rede de várias maneiras:

- Interfaces over Ethernet usando software integrado ao ONTAP.
- Em várias interfaces de sistema, com uma interface usada para iSCSI que também pode transmitir tráfego para outros protocolos, como SMB e NFS.
- Usando um adaptador de destino unificado (UTA) ou um adaptador de rede convergente (CNA).

Cada nó iSCSI deve ter um nome de nó.

Os dois formatos, ou designadores de tipo, para nomes de nós iSCSI são *iqn* e *eui*. O destino SVM iSCSI sempre usa o designador do tipo *iqn*. O iniciador pode usar o designador *iqn-type* ou *eui-type*.

Nome do nó do sistema de storage

Cada SVM que executa iSCSI tem um nome de nó padrão com base em um nome de domínio reverso e um número de codificação exclusivo.

O nome do nó é exibido no seguinte formato:

`iqn.1992-08.com.NetApp:sn.unique-encoding-number`

O exemplo a seguir mostra o nome do nó padrão para um sistema de armazenamento com um número de

codificação exclusivo:

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

Porta TCP para iSCSI

O protocolo iSCSI está configurado no ONTAP para utilizar a porta TCP número 3260.

O ONTAP não suporta a alteração do número da porta para iSCSI. A porta número 3260 está registrada como parte da especificação iSCSI e não pode ser utilizada por qualquer outra aplicação ou serviço.

Informações relacionadas

["Documentação do NetApp: Configuração do host SAN ONTAP"](#)

Gerenciamento de serviços iSCSI

Gerenciamento de serviços iSCSI

Você pode gerenciar a disponibilidade do serviço iSCSI nas interfaces lógicas iSCSI da máquina virtual de storage (SVM) usando os `vserver iscsi interface enable` comandos ou `vserver iscsi interface disable`.

Por predefinição, o serviço iSCSI está ativado em todas as interfaces lógicas iSCSI.

Como o iSCSI é implementado no host

O iSCSI pode ser implementado no host usando hardware ou software.

Você pode implementar iSCSI de uma das seguintes maneiras:

- Usando o software Initiator que usa as interfaces Ethernet padrão do host.
- Através de um adaptador de barramento de host iSCSI (HBA): Um HBA iSCSI aparece para o sistema operacional do host como um adaptador de disco SCSI com discos locais.
- Usando um adaptador TOE (TCP Offload Engine) que descarrega o processamento TCP/IP.

O processamento do protocolo iSCSI ainda é realizado pelo software anfitrião.

Como a autenticação iSCSI funciona

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar uma sessão iSCSI. O sistema de armazenamento permite ou nega a solicitação de login ou determina que não é necessário fazer login.

Os métodos de autenticação iSCSI são:

- Challenge Handshake Authentication Protocol (CHAP) - o iniciador faz login usando um nome de usuário e senha CHAP.

Você pode especificar uma senha CHAP ou gerar uma senha secreta hexadecimal. Existem dois tipos de nomes de usuário CHAP e senhas:

- Entrada - o sistema de armazenamento autentica o iniciador.

As configurações de entrada são necessárias se você estiver usando a autenticação CHAP.

- Outbound — esta é uma configuração opcional para permitir que o iniciador autentique o sistema de armazenamento.

Só pode utilizar as definições de saída se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento.

- Negar - o iniciador tem acesso negado ao sistema de armazenamento.
- Nenhum - o sistema de storage não requer autenticação para o iniciador.

Pode definir a lista de iniciadores e os respetivos métodos de autenticação. Você também pode definir um método de autenticação padrão que se aplica a iniciadores que não estão nesta lista.

Informações relacionadas

["Opções de multipathing do Windows com Data ONTAP: Fibre Channel e iSCSI"](#)

Gerenciamento de segurança do iniciador iSCSI

O ONTAP fornece uma série de recursos para gerenciar a segurança para iniciadores iSCSI. Pode definir uma lista de iniciadores iSCSI e o método de autenticação para cada um, apresentar os iniciadores e os respetivos métodos de autenticação associados na lista de autenticação, adicionar e remover iniciadores da lista de autenticação e definir o método de autenticação do iniciador iSCSI predefinido para iniciadores que não estão na lista.

Isolamento do ponto de extremidade iSCSI

A partir do ONTAP 9.1, os comandos de segurança iSCSI existentes foram melhorados para aceitar um intervalo de endereços IP ou vários endereços IP.

Todos os iniciadores iSCSI devem fornecer endereços IP de origem ao estabelecer uma sessão ou conexão com um destino. Essa nova funcionalidade impede que um iniciador faça login no cluster se o endereço IP de origem não for suportado ou desconhecido, fornecendo um esquema de identificação exclusivo. Qualquer iniciador originado de um endereço IP não suportado ou desconhecido terá seu login rejeitado na camada de sessão iSCSI, impedindo que o iniciador acesse qualquer LUN ou volume dentro do cluster.

Implemente essa nova funcionalidade com dois novos comandos para ajudar a gerenciar entradas pré-existentes.

Adicionar intervalo de endereços do iniciador

Melhore o gerenciamento de segurança do iniciador iSCSI adicionando um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security add-initiator-address-range` comando.

```
cluster1::> vserver iscsi security add-initiator-address-range
```

Remova o intervalo de endereços do iniciador

Remova um intervalo de endereços IP ou vários endereços IP com o `vserver iscsi security remove-initiator-address-range` comando.

```
cluster1::> vserver iscsi security remove-initiator-address-range
```

O que é a autenticação CHAP

O CHAP (Challenge Handshake Authentication Protocol) permite a comunicação autenticada entre iniciadores e destinos iSCSI. Quando você usa autenticação CHAP, você define nomes de usuário CHAP e senhas tanto no iniciador quanto no sistema de armazenamento.

Durante a fase inicial de uma sessão iSCSI, o iniciador envia uma solicitação de login ao sistema de armazenamento para iniciar a sessão. A solicitação de login inclui o nome de usuário CHAP do iniciador e o algoritmo CHAP. O sistema de armazenamento responde com um desafio CHAP. O iniciador fornece uma resposta CHAP. O sistema de armazenamento verifica a resposta e autentica o iniciador. A senha CHAP é usada para calcular a resposta.

Diretrizes para o uso da autenticação CHAP

Você deve seguir certas diretrizes ao usar a autenticação CHAP.

- Se definir um nome de utilizador e uma palavra-passe de entrada no sistema de armazenamento, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de saída no iniciador. Se também definir um nome de utilizador e uma palavra-passe de saída no sistema de armazenamento para ativar a autenticação bidirecional, tem de utilizar o mesmo nome de utilizador e palavra-passe para as definições CHAP de entrada no iniciador.
- Você não pode usar o mesmo nome de usuário e senha para configurações de entrada e saída no sistema de armazenamento.
- Os nomes de usuário CHAP podem ser de 1 a 128 bytes.

Um nome de usuário nulo não é permitido.

- As senhas CHAP (segredos) podem ter 1 a 512 bytes.

As senhas podem ser valores hexadecimais ou strings. Para valores hexadecimais, você deve inserir o valor com um prefixo "0x" ou "0X". Não é permitida uma palavra-passe nula.

O ONTAP permite o uso de caracteres especiais, letras não inglesas, números e espaços para senhas CHAP (segredos). No entanto, isso está sujeito a restrições de host. Se algum destes não for permitido pelo seu anfitrião específico, não poderão ser utilizados.



Por exemplo, o iniciador de software iSCSI da Microsoft requer que as senhas CHAP do iniciador e do destino tenham pelo menos 12 bytes se a criptografia IPsec não estiver sendo usada. O comprimento máximo da senha é de 16 bytes, independentemente de o IPsec ser usado.

Para restrições adicionais, você deve ver a documentação do iniciador.

Como usar listas de acesso à interface iSCSI para limitar as interfaces do iniciador pode aumentar o desempenho e a segurança

As listas de acesso à interface iSCSI podem ser usadas para limitar o número de LIFs em uma SVM que um iniciador pode acessar, aumentando assim a performance e a segurança.

Quando um iniciador inicia uma sessão de descoberta usando um comando iSCSI `SendTargets`, ele recebe os endereços IP associados ao LIF (interface de rede) que está na lista de acesso. Por padrão, todos os iniciadores têm acesso a todas as LIFs iSCSI na SVM. Você pode usar a lista de acesso para restringir o número de LIFs em uma SVM a que um iniciador tem acesso.

Serviço de nomes de armazenamento de Internet (iSNS)

O iSNS (Internet Storage Name Service) é um protocolo que permite a detecção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento TCP/IP. Um servidor iSNS mantém informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI IQN e grupos de portais.

Você pode obter um servidor iSNS de um fornecedor terceirizado. Se você tiver um servidor iSNS na rede configurado e habilitado para uso pelo iniciador e destino, poderá usar o LIF de gerenciamento de uma máquina virtual de armazenamento (SVM) para Registrar todos os LIFs iSCSI para esse SVM no servidor iSNS. Depois que o Registro estiver concluído, o iniciador iSCSI pode consultar o servidor iSNS para descobrir todos os LIFs para esse SVM específico.

Se você decidir usar um serviço iSNS, deve garantir que suas máquinas virtuais de armazenamento (SVMs) estejam registradas corretamente em um servidor iSNS (Internet Storage Name Service).

Se você não tiver um servidor iSNS na rede, você deverá configurar manualmente cada destino para ser visível para o host.

O que um servidor iSNS faz

Um servidor iSNS usa o protocolo iSNS (Internet Storage Name Service) para manter informações sobre dispositivos iSCSI ativos na rede, incluindo seus endereços IP, nomes de nós iSCSI (IQNs) e grupos de portais.

O protocolo iSNS permite a detecção e o gerenciamento automatizados de dispositivos iSCSI em uma rede de armazenamento IP. Um iniciador iSCSI pode consultar o servidor iSNS para descobrir dispositivos de destino iSCSI.

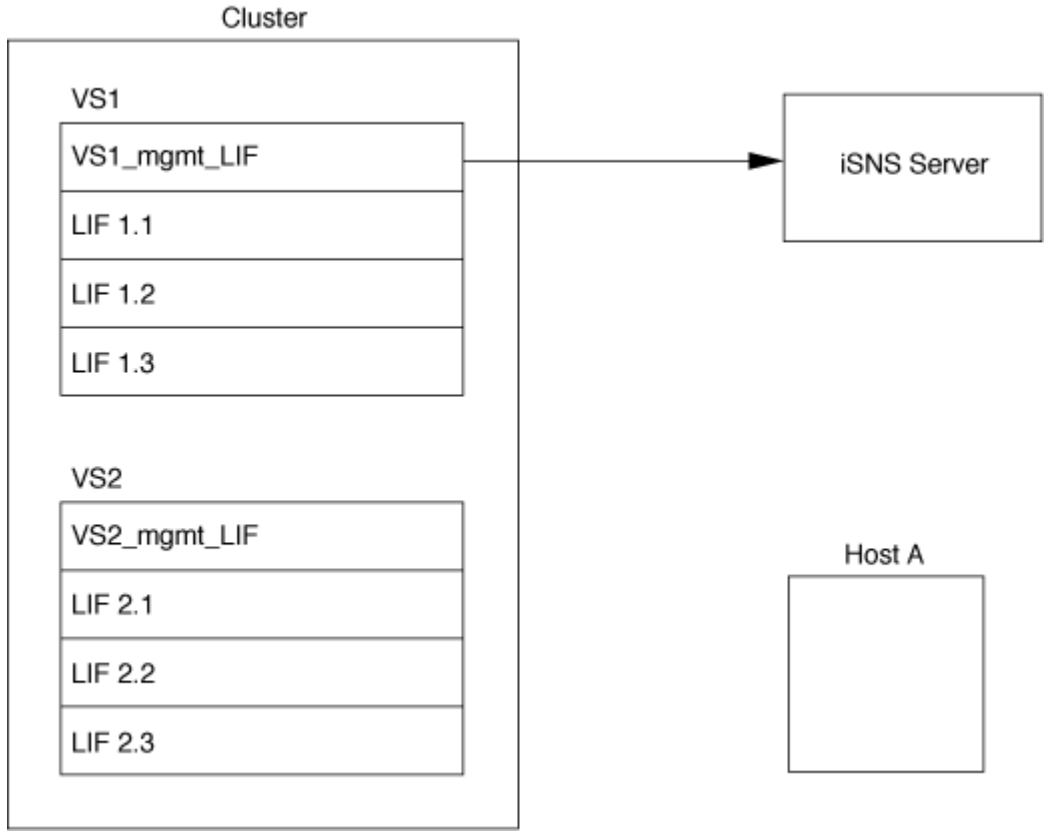
A NetApp não fornece ou revender servidores iSNS. Você pode obter esses servidores de um fornecedor suportado pelo NetApp.

Como os SVMs interagem com um servidor iSNS

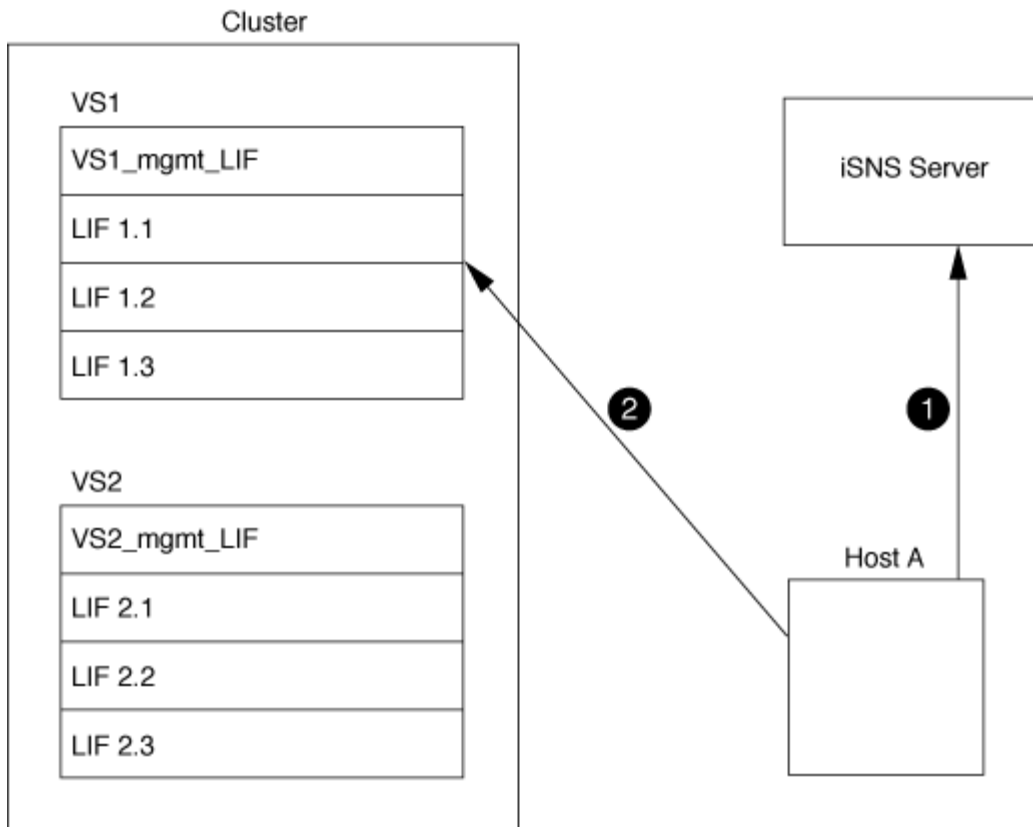
O servidor iSNS se comunica com cada máquina virtual de storage (SVM) por meio do LIF de gerenciamento do SVM. O LIF de gerenciamento Registra todos os nomes, alias e informações do portal do nó de destino iSCSI com o serviço iSNS para um SVM específico.

No exemplo a seguir, o SVM "VS1" usa o gerenciamento de SVM LIF "VS1_mgmt_lif" para se Registrar no servidor iSNS. Durante o Registro do iSNS, um SVM envia todas as LIFs iSCSI por meio do LIF de gerenciamento do SVM para o iSNS Server. Depois que o Registro do iSNS for concluído, o servidor iSNS tem

uma lista de todos os LIFs que servem iSCSI em "VS1". Se um cluster contiver vários SVMs, cada SVM precisará se Registrar individualmente no servidor iSNS para usar o serviço iSNS.



No próximo exemplo, depois que o servidor iSNS concluir o Registro com o destino, o Host A pode descobrir todos os LIFs para "VS1" através do servidor iSNS, conforme indicado na Etapa 1. Depois que o Host A concluir a descoberta dos LIFs para "VS1", o Host A pode estabelecer uma conexão com qualquer um dos LIFs em "VS1", como mostrado na Etapa 2. O host A não está ciente de nenhum dos LIFs em "VS2" até que o LIF de gerenciamento "VS2_mgmt_LIF" para Registros "VS2" com o servidor iSNS.



No entanto, se você definir as listas de acesso à interface, o host só poderá usar as LIFs definidas na lista de acesso à interface para acessar o destino.

Depois que o iSNS for configurado inicialmente, o ONTAP atualizará automaticamente o servidor iSNS quando as configurações do SVM mudarem.

Pode ocorrer um atraso de alguns minutos entre o momento em que você faz as alterações de configuração e quando o ONTAP envia a atualização para o servidor iSNS. Forçar uma atualização imediata das informações do iSNS no servidor iSNS: `vserver iscsi isns update`

Comandos para gerenciar iSNS

O ONTAP fornece comandos para gerenciar seu serviço iSNS.

Se você quiser...	Use este comando...
Configurar um serviço iSNS	<code>vserver iscsi isns create</code>
Inicie um serviço iSNS	<code>vserver iscsi isns start</code>
Modifique um serviço iSNS	<code>vserver iscsi isns modify</code>
Exibir a configuração do serviço iSNS	<code>vserver iscsi isns show</code>
Forçar uma atualização das informações do iSNS registradas	<code>vserver iscsi isns update</code>

Pare um serviço iSNS	<code>vserver iscsi isns stop</code>
Remova um serviço iSNS	<code>vserver iscsi isns delete</code>
Veja a página de manual para um comando	<code>man <i>command name</i></code>

Consulte a página de manual de cada comando para obter mais informações.

Provisionamento DE SAN com FC

Você deve estar ciente dos conceitos importantes que são necessários para entender como o ONTAP implementa uma SAN FC.

Como os nós de destino FC se conectam à rede

Os sistemas de storage e os hosts têm adaptadores para que possam ser conectados a switches FC com cabos.

Quando um nó é conectado à SAN FC, cada SVM Registra o World Wide Port Name (WWPN) de seu LIF com o switch Fabric Name Service. O WWNN do SVM e o WWPN de cada LIF é atribuído automaticamente pelo ONTAP.



A conexão direta com nós de hosts com FC não é suportada, NPIV é necessária e isso requer que um switch seja usado. Com sessões iSCSI, a comunicação funciona com conexões roteadas ou conectadas diretamente à rede. No entanto, ambos os métodos são suportados com o ONTAP.

Como os nós FC são identificados

Cada SVM configurado com FC é identificado por um nome de nó mundial (WWNN).

Como WWPNs são usados

As WWPNs identificam cada LIF em uma SVM configurada para dar suporte ao FC. Essas LIFs utilizam as portas FC físicas em cada nó do cluster, que podem ser placas de destino FC, UTA ou UTA2 configuradas como FC ou FCoE nos nós.

- Criando um grupo de iniciadores

Os WWPNs dos HBAs do host são usados para criar um grupo de iniciadores (iggroup). Um iggroup é usado para controlar o acesso do host a LUNs específicos. Você pode criar um grupo de iniciadores especificando uma coleção de WWPNs de iniciadores em uma rede FC. Quando você mapeia um LUN em um sistema de armazenamento para um grupo, você pode conceder a todos os iniciadores nesse grupo acesso a esse LUN. Se o WWPN de um host não estiver em um grupo que é mapeado para um LUN, esse host não terá acesso ao LUN. Isso significa que os LUNs não aparecem como discos nesse host.

Você também pode criar conjuntos de portas para tornar um LUN visível apenas em portas de destino específicas. Um conjunto de portas consiste em um grupo de portas de destino FC. Você pode vincular um iggroup a um conjunto de portas. Qualquer host no grupo pode acessar os LUNs somente conectando-se

às portas de destino no conjunto de portas.

- Identificação única de FC LIFs

WWPNs identificam de forma exclusiva cada interface lógica FC. O sistema operacional host usa a combinação de WWNN e WWPN para identificar SVMs e FC LIFs. Alguns sistemas operacionais exigem vinculação persistente para garantir que o LUN seja exibido no mesmo ID de destino no host.

Como as atribuições de nomes em todo o mundo funcionam

Nomes mundiais são criados sequencialmente em ONTAP. No entanto, devido à forma como o ONTAP os atribui, eles podem parecer atribuídos em uma ordem não sequencial.

Cada adaptador tem um WWPN e WWNN pré-configurados, mas o ONTAP não usa esses valores pré-configurados. Em vez disso, o ONTAP atribui seus próprios WWPNs ou WWNNs, com base nos endereços MAC das portas Ethernet integradas.

Os nomes mundiais podem parecer não sequenciais quando atribuídos pelas seguintes razões:

- Nomes mundiais são atribuídos em todos os nós e máquinas virtuais de storage (SVMs) no cluster.
- Os nomes do mundo livre são reciclados e adicionados de volta ao conjunto de nomes disponíveis.

Como os switches FC são identificados

Os switches Fibre Channel têm um nome de nó mundial (WWNN) para o próprio dispositivo e um nome de porta mundial (WWPN) para cada uma de suas portas.

Por exemplo, o diagrama a seguir mostra como os WWPNs são atribuídos a cada uma das portas em um switch Brocade de 16 portas. Para obter detalhes sobre como as portas são numeradas para um switch específico, consulte a documentação fornecida pelo fornecedor para esse switch.



Porta **0**, WWPN 20:**00**:00:60:69:51:06:B4

Porta **1**, WWPN 20:**01**:00:60:69:51:06:B4

Porta **14**, WWPN 20:**0e**:00:60:69:51:06:B4

Porta **15**, WWPN 20:**0f**:00:60:69:51:06:B4

Provisionamento DE SAN com NVMe

A partir do ONTAP 9.4, o NVMe/FC é compatível com ambiente SAN. O NVMe/FC permite que os administradores de storage provisionem namespaces e subsistemas e mapeem os namespaces para subsistemas, de forma semelhante à maneira como os LUNs são provisionados e mapeados para grupos de FC e iSCSI.

Um namespace NVMe é uma quantidade de memória não volátil que pode ser formatada em blocos lógicos. Namespaces são o equivalente a LUNs para protocolos FC e iSCSI, e um subsistema NVMe é análogo a um iggroup. Um subsistema NVMe pode ser associado a iniciadores para que os namespaces dentro do subsistema possam ser acessados pelos iniciadores associados.



Embora análogos em função, os namespaces NVMe não são compatíveis com todos os recursos compatíveis com LUNs.

A partir do ONTAP 9.5, é necessária uma licença para dar suporte ao acesso de dados voltado para o host com NVMe. Se o NVMe estiver habilitado no ONTAP 9.4, um período de carência de 90 dias será concedido para adquirir a licença após a atualização para o ONTAP 9.5. Se você tiver "ONTAP One", as licenças NVMe serão incluídas. Você pode ativar a licença usando o seguinte comando:

```
system license add -license-code NVMe_license_key
```

Informações relacionadas

["Relatório técnico da NetApp 4684: Implementando e configurando SANs modernas com NVMe/FC"](#)

Volumes SAN

Sobre a visão geral dos volumes SAN

O ONTAP oferece três opções básicas de provisionamento de volume: Provisionamento thick, thin Provisioning e provisionamento semi-thick. Cada opção usa maneiras diferentes de gerenciar o espaço de volume e os requisitos de espaço para as tecnologias de compartilhamento de blocos do ONTAP. Entender como as opções funcionam permite que você escolha a melhor opção para o seu ambiente.



Não é recomendável colocar LUNs SAN e compartilhamentos nas no mesmo FlexVol volume. Você deve provisionar volumes FlexVol separados, especificamente para suas LUNs de SAN, e provisionar volumes FlexVol separados, especificamente para seus compartilhamentos nas. Isso simplifica as implantações de gerenciamento e replicação, além de simplificar o modo como os volumes do FlexVol são suportados no Active IQ Unified Manager (anteriormente OnCommand Unified Manager).

Thin Provisioning para volumes

Quando um volume provisionado é criado, o ONTAP não reserva nenhum espaço extra quando o volume é criado. À medida que os dados são gravados no volume, o volume solicita o storage de que ele precisa do agregado para acomodar a operação de gravação. O uso de volumes provisionados por thin permite comprometer seu agregado, o que introduz a possibilidade de o volume não ser capaz de proteger o espaço necessário quando o agregado ficar sem espaço livre.

Você cria um FlexVol volume com provisionamento reduzido definindo sua `-space-guarantee` opção como `none`.

Provisionamento espesso para volumes

Quando um volume provisionado com espessura é criado, o ONTAP reserva armazenamento suficiente do agregado para garantir que qualquer bloco no volume possa ser gravado a qualquer momento. Ao configurar um volume para usar o provisionamento thick, você pode empregar qualquer um dos recursos de eficiência de

storage da ONTAP, como compactação e deduplicação, para compensar os maiores requisitos de storage iniciais.

Você cria um FlexVol volume com provisionamento excessivo definindo sua `-space-slo` opção (objetivo de nível de serviço) como `thick`.

Provisionamento semi-espesso para volumes

Quando um volume usando provisionamento semi-espesso é criado, o ONTAP separa o espaço de armazenamento do agregado para contabilizar o tamanho do volume. Se o volume estiver sem espaço livre porque os blocos estão em uso por tecnologias de compartilhamento de bloco, o ONTAP se esforça para excluir objetos de dados de proteção (cópias Snapshot e arquivos FlexClone e LUNs) para liberar o espaço que eles estão segurando. Enquanto o ONTAP puder excluir os objetos de dados de proteção com a rapidez suficiente para acompanhar o espaço necessário para sobrescritas, as operações de gravação continuarão a ser bem-sucedidas. Isso é chamado de garantia de escrita "melhor esforço".

Observação: a seguinte funcionalidade não é suportada em volumes que usam provisionamento semi-espesso:

- tecnologias de eficiência de storage, como deduplicação, compressão e compactação
- Microsoft offloaded Data Transfer (ODX)

Você cria um FlexVol volume provisionado semi-espesso definindo sua `-space-slo` opção (objetivo de nível de serviço) como `semi-thick`.

Use com arquivos e LUNs reservados ao espaço

Um arquivo ou LUN com espaço reservado é aquele para o qual o armazenamento é alocado quando é criado. Historicamente, o NetApp usou o termo "LUN com provisionamento reduzido" para significar um LUN para o qual a reserva de espaço está desativada (um LUN sem espaço reservado).

*Nota: * Arquivos não reservados ao espaço não são geralmente chamados de "arquivos thin-provisionados".

A tabela a seguir resume as principais diferenças em como as três opções de provisionamento de volume podem ser usadas com arquivos reservados ao espaço e LUNs:

Provisionamento de volume	Reserva de espaço LUN/ficheiro	Sobrescreve	Proteção de dados 2	A eficiência de armazenamento 3
Espesso	Suportado	1	Garantido	Suportado
Fino	Sem efeito	Nenhum	Garantido	Suportado
Semi-espesso	Suportado	O melhor esforço 1	Melhor esforço	Não suportado

Notas

1. A capacidade de garantir substituições ou fornecer uma garantia de substituição de melhor esforço requer que a reserva de espaço esteja ativada no LUN ou arquivo.
2. Os dados de proteção incluem cópias Snapshot e arquivos FlexClone e LUNs marcados para exclusão automática (clones de backup).

3. A eficiência de storage inclui deduplicação, compactação, arquivos FlexClone e LUNs não marcados para exclusão automática (clones ativos) e subarquivos FlexClone (usados para descarregar cópias).

Suporte para LUNs de thin Provisioning SCSI

O ONTAP oferece suporte a T10 LUNs de thin Provisioning SCSI, bem como LUNs de thin Provisioning NetApp. O thin Provisioning SCSI T10 permite que os aplicativos host suportem recursos SCSI, incluindo recuperação de espaço LUN e recursos de monitoramento de espaço LUN para ambientes de blocos. O thin Provisioning SCSI T10 deve ser suportado pelo software de host SCSI.

Você usa a configuração ONTAP `space-allocation` para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 em um LUN. Você usa a configuração ONTAP `space-allocation enable` para habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

O `[-space-allocation {enabled|disabled}]` comando no Manual de Referência de comando do ONTAP tem mais informações para habilitar/desabilitar o suporte ao provisionamento de thin Provisioning T10 e habilitar o provisionamento de thin Provisioning SCSI T10 em um LUN.

["Referência do comando ONTAP"](#)

Configurar opções de provisionamento de volume

Você pode configurar um volume para thin Provisioning, thin Provisioning ou provisionamento semi-espesso.

Sobre esta tarefa

Definir a `-space-slo` opção para `thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- 100% do espaço necessário para as substituições é reservado. Você não pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`

Definir a `-space-slo` opção para `semi-thick` garantir o seguinte:

- Todo o volume é pré-alocado no agregado. Não é possível usar o `volume create` comando ou `volume modify` para configurar a opção do volume `-space-guarantee`.
- Nenhum espaço é reservado para substituições. Você pode usar o `volume modify` comando para configurar a opção do volume `-fractional-reserve`.
- A exclusão automática de cópias Snapshot está ativada.

Passo

1. Configurar opções de provisionamento de volume:

```
volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
```

A `-space-guarantee` opção padrão é `none` para sistemas AFF e para volumes DP não AFF. Caso contrário, o padrão é `volume`. Para volumes FlexVol existentes, use o `volume modify` comando para configurar opções de provisionamento.

O comando a seguir configura o vol1 no SVM VS1 para thin Provisioning:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee none
```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento espesso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

O comando a seguir configura o vol1 no SVM VS1 para provisionamento semi-espesso:

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-thick
```

Opções de configuração de VOLUME SAN

Tem de definir várias opções no volume que contém o LUN. A forma como definir as opções de volume determina a quantidade de espaço disponível para LUNs no volume.

Crescimento automático

Você pode ativar ou desativar o crescimento automático. Se você ativá-lo, o crescimento automático permite que o ONTAP aumente automaticamente o tamanho do volume até um tamanho máximo que você predeterminar. Deve haver espaço disponível no agregado contendo para suportar o crescimento automático do volume. Portanto, se você ativar o crescimento automático, você deve monitorar o espaço livre no agregado contendo e adicionar mais quando necessário.

O crescimento automático não pode ser acionado para suportar a criação de Snapshot. Se você tentar criar uma cópia Snapshot e não houver espaço suficiente no volume, a criação de snapshot falhará, mesmo com o crescimento automático ativado.

Se o crescimento automático estiver desativado, o tamanho do seu volume permanecerá o mesmo.

Auto-retrátil

Pode ativar ou desativar o Autoshrink. Se você ativá-lo, o recurso de auto-redução permite que o ONTAP diminua automaticamente o tamanho geral de um volume quando a quantidade de espaço consumida no volume diminui um limite predeterminado. Isso aumenta a eficiência de storage acionando volumes para liberar espaço livre não utilizado automaticamente.

snapshot Autodelete

O snapshot autodelete exclui automaticamente cópias snapshot quando uma das seguintes situações ocorre:

- O volume está quase cheio.
- O espaço de reserva do Snapshot está quase cheio.
- O espaço de reserva de substituição está cheio.

Você pode configurar o snapshot autodelete para excluir cópias Snapshot do mais antigo para o mais recente ou do mais recente para o mais antigo. O snapshot autodelete não exclui cópias snapshot vinculadas a cópias snapshot em volumes clonados ou LUNs.

Se o seu volume precisar de espaço adicional e você tiver ativado o crescimento automático e o snapshot Autodelete, por padrão, o ONTAP tentará adquirir o espaço necessário acionando primeiro o crescimento automático. Se não for adquirido espaço suficiente através do crescimento automático, o snapshot autodelete é acionado.

Reserva do Snapshot

A reserva do Snapshot define a quantidade de espaço no volume reservado para cópias Snapshot. O espaço alocado à reserva Instantânea não pode ser usado para qualquer outra finalidade. Se todo o espaço alocado para o Snapshot Reserve for usado, as cópias Snapshot começarão a consumir espaço adicional no volume.

Requisito para movimentação de volumes em ambientes SAN

Antes de mover um volume que contenha LUNs ou namespaces, você precisa atender a certos requisitos.

- Para volumes que contêm um ou mais LUNs, você deve ter no mínimo dois caminhos por LUN (LIFs) conectados a cada nó no cluster.

Isso elimina pontos únicos de falha e permite que o sistema sobreviva a falhas de componentes.

- Para volumes que contêm namespaces, o cluster precisa estar executando o ONTAP 9.6 ou posterior.

A movimentação de volume não é compatível com configurações NVMe que executam o ONTAP 9.5.

Considerações para definir a reserva fracionária

A reserva fracionária, também chamada de *reserva de substituição LUN*, permite desativar a reserva de substituição para LUNs e arquivos reservados no espaço em um FlexVol volume. Isso pode ajudar a maximizar a utilização do storage, mas se o ambiente for afetado negativamente por falhas nas operações de gravação devido à falta de espaço, você precisa entender os requisitos que essa configuração impõe.

A configuração de reserva fracionária é expressa como uma porcentagem; os únicos valores válidos são 0 e 100 porcentagem. A configuração de reserva fracionária é um atributo do volume.

Definir a reserva fracionária para 0 aumentar a utilização do armazenamento. No entanto, um aplicativo que acessa dados que residem no volume pode ter uma interrupção de dados se o volume estiver sem espaço livre, mesmo com a garantia de volume definida como `volume`. No entanto, com a configuração e o uso adequados de volume, você pode minimizar a chance de falhas de gravação. O ONTAP fornece uma garantia de gravação "melhor esforço" para volumes com reserva fracionária definida para 0 quando *todos* dos seguintes requisitos são atendidos:

- A deduplicação não está em uso
- A compressão não está a ser utilizada
- Os subficheiros FlexClone não estão a ser utilizados

- Todos os arquivos FlexClone e LUNs FlexClone são ativados para exclusão automática

Esta não é a configuração padrão. Você deve ativar explicitamente a exclusão automática, seja no momento da criação ou modificando o arquivo FlexClone ou LUN FlexClone depois que ele for criado.

- A descarga de cópia ODX e FlexClone não está em uso
- A garantia de volume está definida para `volume`
- A reserva de espaço de arquivo ou LUN é `enabled`
- A reserva de instantâneo de volume está definida como `0`
- A exclusão automática da cópia Snapshot do volume é `enabled` com um nível de compromisso de `destroy`, uma lista de destruição de `lun_clone, vol_clone, cifs_share, file_clone, sfsr` e um gatilho de `volume`

Essa configuração também garante que arquivos FlexClone e LUNs FlexClone sejam excluídos quando necessário.

Observe que, se sua taxa de alteração for alta, em casos raros, a exclusão automática da cópia Snapshot pode ficar para trás, resultando em falta de espaço no volume, mesmo com todas as configurações necessárias acima em uso.

Além disso, você pode, como opção, usar a funcionalidade de volume com crescimento automático para diminuir a probabilidade de as cópias do Snapshot precisarem ser excluídas automaticamente. Se você ativar a capacidade de crescimento automático, deverá monitorar o espaço livre no agregado associado. Se o agregado ficar cheio o suficiente para que o volume seja impedido de crescer, mais cópias Snapshot provavelmente serão excluídas à medida que o espaço livre no volume estiver esgotado.

Se você não puder atender a todos os requisitos de configuração acima e precisar garantir que o volume não fique sem espaço, defina a configuração de reserva fracionária do volume como `100`. Isso requer mais espaço livre na frente, mas garante que as operações de modificação de dados serão bem-sucedidas mesmo quando as tecnologias listadas acima estiverem em uso.

O valor padrão e os valores permitidos para a configuração de reserva fracionária dependem da garantia do volume:

Garantia de volume	Reserva fracionária predefinida	Valores permitidos
Volume	100	0, 100
Nenhum	0	0, 100

Gerenciamento de espaço no lado do host SAN

Em um ambiente com provisionamento reduzido, o gerenciamento de espaço no lado do host conclui o processo de gerenciamento de espaço do sistema de storage que foi liberado no sistema de arquivos do host.

Um sistema de arquivos host contém metadados para acompanhar quais blocos estão disponíveis para armazenar novos dados e quais blocos contêm dados válidos que não devem ser sobrescritos. Esses metadados são armazenados no LUN ou namespace. Quando um arquivo é excluído no sistema de arquivos

host, os metadados do sistema de arquivos são atualizados para marcar os blocos desse arquivo como espaço livre. O espaço livre total do sistema de arquivos é então recalculado para incluir os blocos recém-liberados. Para o sistema de storage, essas atualizações de metadados não parecem diferentes de quaisquer outras gravações que estejam sendo executadas pelo host. Portanto, o sistema de armazenamento não tem conhecimento de que quaisquer exclusões ocorreram.

Isso cria uma discrepância entre a quantidade de espaço livre relatada pelo host e a quantidade de espaço livre relatada pelo sistema de armazenamento subjacente. Por exemplo, suponha que você tenha um LUN de 200 GB recém-provisionado atribuído ao seu host pelo sistema de armazenamento. Tanto o host quanto o sistema de armazenamento relatam 200 GB de espaço livre. Seu host então grava 100 GB de dados. Nesse ponto, tanto o host quanto o sistema de armazenamento relatam 100 GB de espaço usado e 100 GB de espaço não utilizado.

Em seguida, você exclui 50 GB de dados do seu host. Neste ponto, seu host irá relatar 50 GB de espaço usado e 150 GB de espaço não utilizado. No entanto, seu sistema de armazenamento irá relatar 100 GB de espaço usado e 100 GB de espaço não utilizado.

O gerenciamento de espaço no lado do host usa vários métodos para reconciliar o diferencial de espaço entre o host e o sistema de armazenamento.

Gerenciamento de host simplificado com o SnapCenter

Você pode usar o software SnapCenter para simplificar algumas tarefas de gerenciamento e proteção de dados associadas ao storage iSCSI e FC. O SnapCenter é um pacote de gerenciamento opcional para hosts Windows e UNIX.

Você pode usar o software SnapCenter para criar facilmente discos virtuais de pools de storage que podem ser distribuídos entre vários sistemas de storage e automatizar as tarefas de provisionamento de storage e simplificar o processo de criação de cópias Snapshot e clones consistentes com os dados de host.

Consulte a documentação do produto NetApp para obter mais informações ["SnapCenter"](#) sobre .

Links relacionados

["Ativar a alocação de espaço ONTAP para protocolos SAN"](#)

Sobre os grupos

Grupos de iniciadores (grupos de iniciadores) são tabelas de WWPNs de host de protocolo FC ou nomes de nós de host iSCSI. Você pode definir grupos e mapeá-los para LUNs para controlar quais iniciadores têm acesso a LUNs.

Normalmente, você deseja que todas as portas de iniciador do host ou iniciadores de software tenham acesso a um LUN. Se você estiver usando software multipathing ou tiver hosts em cluster, cada porta iniciador ou iniciador de software de cada host em cluster precisa de caminhos redundantes para o mesmo LUN.

Você pode criar grupos que especificam quais iniciadores têm acesso aos LUNs antes ou depois de criar LUNs, mas você deve criar grupos antes de poder mapear um LUN para um grupo.

Os grupos de iniciadores podem ter vários iniciadores, e vários grupos podem ter o mesmo iniciador. No entanto, não é possível mapear um LUN para vários grupos que tenham o mesmo iniciador. Um iniciador não pode ser um membro de grupos de diferentes ostypes.

Exemplo de como os grupos dão acesso LUN

Você pode criar vários grupos para definir quais LUNs estão disponíveis para seus hosts. Por exemplo, se você tiver um cluster de host, pode usar igroups para garantir que LUNs específicos sejam visíveis para apenas um host no cluster ou para todos os hosts no cluster.

A tabela a seguir ilustra como quatro grupos dão acesso aos LUNs para quatro hosts diferentes que estão acessando o sistema de armazenamento. Os hosts em cluster (Host3 e Host4) são membros do mesmo grupo (Group3) e podem acessar os LUNs mapeados para esse grupo. O grupo chamado Group4 contém as WWPNs de Host4 para armazenar informações locais que não se destinam a ser vistas por seu parceiro.

Hosts com WWPNs HBA, IQNs ou EUIs	grupos	WWPNs, IQNs, EUIs adicionados aos grupos	LUNs mapeados para grupos
Host1, caminho único (iniciador de software iSCSI) iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	/vol/vol2/lun1
Host2, multipath (dois HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	/vol/vol2/lun2
Host3, multipath, em cluster com host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees1/lun3
Host4, multipath, agrupado (não visível para Host3) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees2/lun4 /vol/vol2/qtrees1/lun5

Especifique WWPNs do iniciador e nomes de nó iSCSI para um grupo

Você pode especificar os nomes de nós iSCSI e WWPNs dos iniciadores quando você cria um iggroup ou pode adicioná-los mais tarde. Se você optar por especificar os nomes dos nós iSCSI do iniciador e WWPNs ao criar o LUN, eles poderão ser removidos mais tarde, se necessário.

Siga as instruções na documentação dos Utilitários de host para obter WWPNs e localizar os nomes de nó iSCSI associados a um host específico. Para hosts que executam o software ESX, use o Virtual Storage Console.

Virtualização de storage com descarga de cópia VMware e Microsoft

Visão geral da virtualização de storage com descarga de cópia VMware e Microsoft

VMware e Microsoft suportam operações de descarga de cópia para aumentar o desempenho e a taxa de transferência de rede. Você deve configurar o sistema para atender aos requisitos dos ambientes do sistema operacional VMware e Windows para usar suas respectivas funções de descarga de cópia.

Ao usar a descarga de cópia da VMware e da Microsoft em ambientes virtualizados, os LUNs precisam estar alinhados. LUNs desalinhados podem degradar o desempenho.

Vantagens de usar um ambiente SAN virtualizado

A criação de um ambiente virtualizado com o uso de máquinas virtuais de storage (SVMs) e LIFs permite expandir seu ambiente SAN para todos os nós do cluster.

- Gerenciamento distribuído

É possível fazer login em qualquer nó da SVM para administrar todos os nós em um cluster.

- Maior acesso aos dados

Com o MPIO e o ALUA, você tem acesso aos dados por meio de iSCSI ou FC LIFs ativos para o SVM.

- Acesso controlado LUN

Se você usar SLM e portsets, poderá limitar quais LIFs um iniciador pode usar para acessar LUNs.

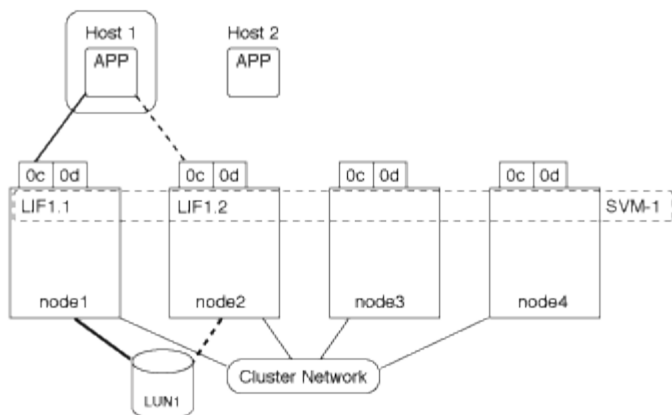
Como o acesso LUN funciona em um ambiente virtualizado

Em um ambiente virtualizado, os LIFs permitem que os hosts (clientes) acessem LUNs por meio de caminhos otimizados e não otimizados.

Um LIF é uma interface lógica que conecta o SVM a uma porta física. Embora vários SVMs possam ter várias LIFs na mesma porta, um LIF pertence a uma SVM. Você pode acessar LUNs por meio das LIFs SVMs.

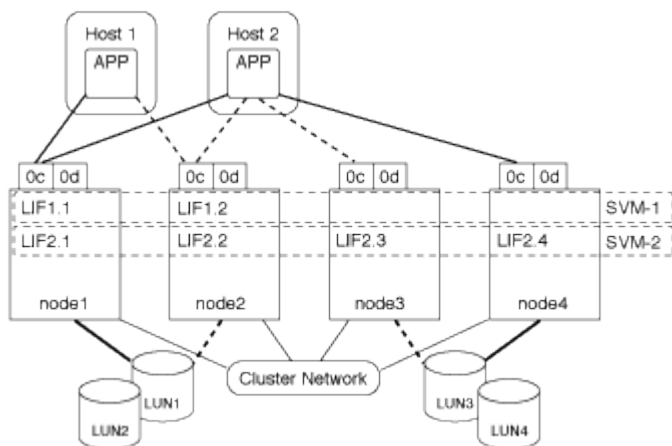
Exemplo de acesso LUN com uma única SVM em um cluster

No exemplo a seguir, o host 1 se conecta ao LIF1,1 e LIF1,2 no SVM-1 para acessar o LUN1. LIF1,1 usa a porta física node1:0C e LIF1,2 usa o node2:0C. O LIF1,1 e o LIF1,2 pertencem apenas à SVM-1. Se um novo LUN for criado no nó 1 ou no nó 2, para SVM-1, ele poderá usar essas mesmas LIFs. Se um novo SVM for criado, novas LIFs poderão ser criadas usando as portas físicas 0C ou 0d em ambos os nós.



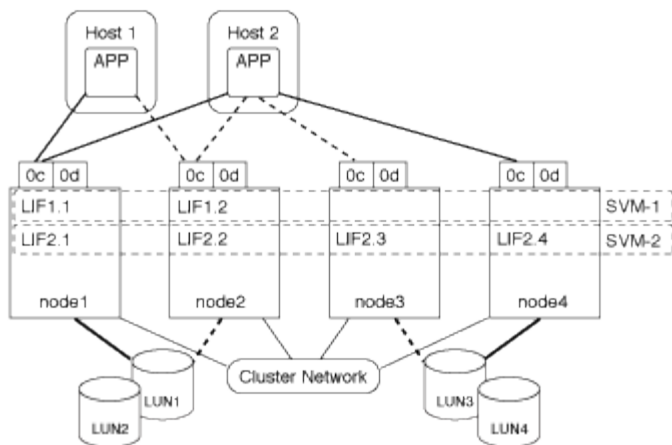
Exemplo de acesso LUN com vários SVMs em um cluster

Uma porta física pode suportar vários LIFs que servem diferentes SVMs. Como os LIFs estão associados a uma SVM específica, os nós de cluster podem enviar o tráfego de dados de entrada para o SVM correto. No exemplo a seguir, cada nó de 1 a 4 tem um LIF para SVM-2 usando a porta física 0C em cada nó. O host 1 se conecta ao LIF1,1 e ao LIF1,2 na SVM-1 para acessar o LUN1. O host 2 se conecta ao LIF2-1 e ao LIF2-2 na SVM-2 para acessar o LUN2. Ambos os SVMs estão compartilhando a porta física 0C nos nós 1 e 2. O SVM-2 tem LIFs adicionais que o host 2 está usando para acessar LUNs 3 e 4. Esses LIFs estão usando a porta física 0C nos nós 3 e 4. Vários SVMs podem compartilhar as portas físicas nos nós.



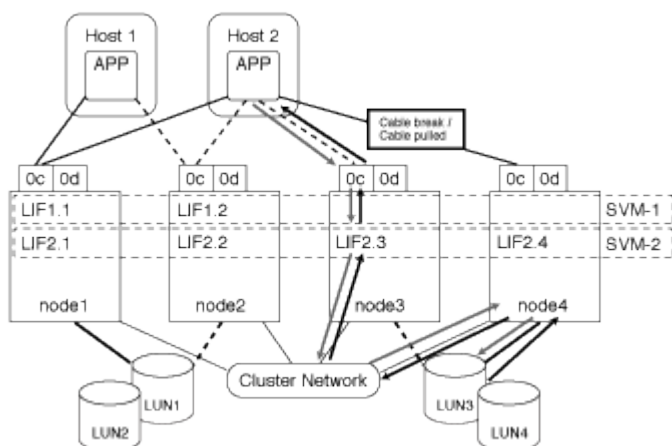
Exemplo de um caminho ativo ou otimizado para um LUN a partir de um sistema host

Em um caminho ativo ou otimizado, o tráfego de dados não percorre a rede do cluster; ele viaja a rota mais direta para o LUN. O caminho ativo ou otimizado para LUN1 é através de LIF1,1 em node1, usando a porta física 0C. O host 2 tem dois caminhos ativos ou otimizados, um caminho para node1, LIF2,1, que está compartilhando a porta física 0C e o outro caminho para node4, LIF2,4, que está usando a porta física 0C.



Exemplo de um caminho ativo ou não otimizado (indireto) para um LUN a partir de um sistema host

Em um caminho ativo ou não otimizado (indireto), o tráfego de dados viaja pela rede do cluster. Esse problema ocorre somente se todos os caminhos ativos ou otimizados de um host não estiverem disponíveis para lidar com o tráfego. Se o caminho do Host 2 para o SVM-2 LIF2,4 for perdido, o acesso ao LUN3 e ao LUN4 percorre a rede do cluster. O acesso a partir do Host 2 usa o LIF2,3 em node3. Em seguida, o tráfego entra no switch de rede do cluster e faz backup de até node4 para acesso ao LUN3 e ao LUN4. Em seguida, ele passará para trás pelo switch de rede de cluster e, em seguida, voltará para o LIF2,3 para o Host 2. Esse caminho ativo ou não otimizado é usado até que o caminho para o LIF2,4 seja restaurado ou um novo LIF seja estabelecido para SVM-2 em outra porta física no nó 4.



= :allow-uri-read:

Melhorar o desempenho do VMware VAAI para hosts ESX

O ONTAP oferece suporte a determinados recursos de VMware vStorage APIs para integração de storage (VAAI) quando o host ESX estiver executando o ESX 4,1 ou posterior. Esses recursos ajudam a descarregar as operações do host ESX para o sistema de storage e a aumentar a taxa de transferência da rede. O host ESX habilita os recursos automaticamente no ambiente correto.

O recurso VAAI suporta os seguintes comandos SCSI:

- EXTENDED_COPY

Esse recurso permite que o host inicie a transferência de dados entre os LUNs ou em um LUN sem envolver o host na transferência de dados. Isso resulta em salvar ciclos de CPU ESX e aumentar a taxa de transferência da rede. O recurso de cópia estendida, também conhecido como "descarga de cópia", é usado em cenários como clonagem de uma máquina virtual. Quando invocado pelo host ESX, o recurso de descarga de cópia copia os dados dentro do sistema de storage em vez de passar pela rede do host. A descarga de cópia transfere dados das seguintes maneiras:

- Dentro de um LUN
 - Entre LUNs em um volume
 - Entre LUNs em diferentes volumes em uma máquina virtual de storage (SVM)
 - Entre LUNs em diferentes SVMs dentro de um cluster se esse recurso não puder ser invocado, o host ESX usa automaticamente os comandos padrão DE LEITURA e GRAVAÇÃO para a operação de cópia.
- WRITE_SAME

Esse recurso descarrega o trabalho de escrever um padrão repetido, como todos os zeros, para um storage array. O host ESX usa esse recurso em operações como o preenchimento zero de um arquivo.

- COMPARE_AND_WRITE

Esse recurso ignora certos limites de simultaneidade de acesso a arquivos, o que acelera operações como inicializar máquinas virtuais.

Requisitos para usar o ambiente VAAI

Os recursos VAAI fazem parte do sistema operacional ESX e são invocados automaticamente pelo host ESX quando você configurou o ambiente correto.

Os requisitos ambientais são os seguintes:

- O host ESX deve estar executando o ESX 4,1 ou posterior.
- O sistema de storage NetApp que hospeda o armazenamento de dados VMware deve estar executando o ONTAP.
- (Somente descarga de cópia) a origem e o destino da operação de cópia VMware devem ser hospedados no mesmo sistema de storage no mesmo cluster.



O recurso de descarga de cópia atualmente não oferece suporte à cópia de dados entre datastores VMware hospedados em diferentes sistemas de storage.

Determine se os recursos VAAI são suportados pelo ESX

Para confirmar se o sistema operacional ESX suporta os recursos VAAI, você pode verificar o vSphere Client ou usar qualquer outro meio de acessar o host. O ONTAP suporta os comandos SCSI por padrão.

Você pode verificar as configurações avançadas do host ESX para determinar se os recursos do VAAI estão ativados. A tabela indica quais comandos SCSI correspondem aos nomes de controle ESX.

Comando SCSI	Nome do controle ESX (recurso VAAI)
EXTENDED_COPY (CÓPIA_ESTENDIDA)	HardwareAcceleratedMove
WRITE_SAME	HardwareAcceleratedInit
COMPARE_E_ESCREVA	HardwareAcceleratedLocking

Microsoft offloaded Data Transfer (ODX)

A Microsoft Offloaded Data Transfer (ODX), também conhecida como *copy offload*, permite transferências diretas de dados dentro de um dispositivo de armazenamento ou entre dispositivos de armazenamento compatíveis sem transferir os dados através do computador host.

O ONTAP oferece suporte ao ODX para os protocolos SMB e SAN.

Em transferências de arquivos não ODX, os dados são lidos da origem e são transferidos pela rede para o host. O host transfere os dados de volta pela rede para o destino. Na transferência de arquivos ODX, os dados são copiados diretamente da origem para o destino sem passar pelo host.

Como as cópias descarregadas do ODX são executadas diretamente entre a origem e o destino, benefícios significativos de desempenho são obtidos se as cópias forem executadas dentro do mesmo volume, incluindo tempo de cópia mais rápido para cópias do mesmo volume, utilização reduzida da CPU e memória no cliente e utilização reduzida da largura de banda de e/S de rede. Se as cópias estiverem em volumes, talvez não haja ganhos significativos de desempenho em comparação com as cópias baseadas em host.

Para ambientes SAN, o ODX só está disponível quando é suportado pelo host e pelo sistema de armazenamento. Os computadores clientes que suportam ODX e têm o ODX ativado automaticamente e de forma transparente usam transferência de arquivos descarregados ao mover ou copiar arquivos. O ODX é usado independentemente de você arrastar e soltar arquivos através do Windows Explorer ou usar comandos de cópia de arquivo de linha de comando ou se um aplicativo cliente inicia solicitações de cópia de arquivo.

Requisitos para usar ODX

Se você planeja usar o ODX para descarregamentos de cópias, você precisa estar familiarizado com considerações de suporte de volume, requisitos de sistema e requisitos de capacidade de software.

Para usar o ODX, seu sistema deve ter o seguinte:

- ONTAP

O ODX é ativado automaticamente em versões suportadas do ONTAP.

- Volume mínimo de origem de 2 GB

Para um desempenho ideal, o volume de origem deve ser superior a 260 GB.

- Suporte ODX no cliente Windows

O ODX é suportado no Windows Server 2012 ou posterior e no Windows 8 ou posterior. A Matriz de interoperabilidade contém as informações mais recentes sobre clientes Windows suportados.

"Ferramenta de Matriz de interoperabilidade do NetApp"

- Cópia de suporte de aplicativo para ODX

O aplicativo que executa a transferência de dados deve suportar ODX. As operações de aplicação que suportam ODX incluem o seguinte:

- Operações de gerenciamento do Hyper-V, como criar e converter discos rígidos virtuais (VHDs), gerenciar cópias Snapshot e copiar arquivos entre máquinas virtuais
 - Operações do Windows Explorer
 - Comandos de cópia do Windows PowerShell
 - Comandos de cópia do prompt de comando do Windows a Biblioteca Microsoft TechNet contém mais informações sobre aplicativos ODX suportados em servidores e clientes Windows.
- Se você usar volumes compactados, o tamanho do grupo de compactação deve ser 8K.

O tamanho do grupo de compressão 32K não é suportado.

O ODX não funciona com os seguintes tipos de volume:

- Volumes de origem com capacidades inferiores a 2 GB
- Volumes só de leitura
- "Volumes FlexCache"



O ODX é compatível com volumes de origem FlexCache.

- "Volumes provisionados semi-grossos"

Requisitos especiais de arquivo do sistema

Você pode excluir arquivos ODX encontrados no `qtrees`. Não remova ou modifique quaisquer outros arquivos de sistema ODX, a menos que você seja informado pelo suporte técnico para fazê-lo.

Ao usar o recurso ODX, existem arquivos de sistema ODX que existem em cada volume do sistema. Esses arquivos permitem a representação pontual dos dados usados durante a transferência do ODX. Os seguintes arquivos de sistema estão no nível raiz de cada volume que contém LUNs ou arquivos para os quais os dados foram descarregados:

- `.copy-offload` (um diretório oculto)
- `.tokens` (arquivo sob o diretório oculto `.copy-offload`)

Você pode usar o `copy-offload delete-tokens -path dir_path -node node_name` comando para excluir uma `qtree` contendo um arquivo ODX.

Casos de uso para ODX

Você deve estar ciente dos casos de uso para usar o ODX em SVMs para que você possa determinar em que circunstâncias o ODX fornece benefícios de desempenho.

Os servidores e clientes do Windows que suportam ODX usam a descarga de cópia como a forma padrão de copiar dados em servidores remotos. Se o servidor ou cliente do Windows não suportar ODX ou a descarga

de cópia ODX falhar em qualquer ponto, a operação de cópia ou movimentação volta para leituras e gravações tradicionais para a operação de cópia ou movimentação.

Os seguintes casos de uso suportam o uso de cópias e movimentos ODX:

- Intra-volume

Os arquivos de origem e destino ou LUNs estão dentro do mesmo volume.

- Entre volumes, mesmo nó e SVM

Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem ao mesmo SVM.

- Entre volumes, nós diferentes e o mesmo SVM

Os arquivos de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem ao mesmo SVM.

- Entre SVM, mesmo nó

O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados no mesmo nó. Os dados pertencem a diferentes SVMs.

- Entre SVM, nós diferentes

O arquivo de origem e destino ou LUNs estão em volumes diferentes localizados em nós diferentes. Os dados pertencem a diferentes SVMs.

- Inter-cluster

As LUNs de origem e destino estão em volumes diferentes, localizados em nós diferentes, entre clusters. Isso só é suportado para SAN e não funciona para SMB.

Existem alguns casos de uso especiais adicionais:

- Com a implementação do ONTAP ODX, você pode usar o ODX para copiar arquivos entre compartilhamentos SMB e unidades virtuais conectadas a FC ou iSCSI.

Você pode usar o Windows Explorer, a CLI do Windows ou PowerShell, Hyper-V ou outras aplicações compatíveis com ODX para copiar ou mover arquivos sem interrupções usando a descarga de cópia ODX entre compartilhamentos SMB e LUNs conectados, desde que os compartilhamentos SMB e LUNs estejam no mesmo cluster.

- O Hyper-V fornece alguns casos de uso adicionais para descarga de cópia ODX:

- Você pode usar a passagem de descarga de cópia ODX com o Hyper-V para copiar dados dentro ou através de arquivos de disco rígido virtual (VHD) ou para copiar dados entre compartilhamentos SMB mapeados e LUNs iSCSI conectados dentro do mesmo cluster.

Isso permite que cópias de sistemas operacionais convidados passem para o storage subjacente.

- Ao criar VHDs de tamanho fixo, o ODX é usado para inicializar o disco com zeros, usando um token zerado bem conhecido.
- A descarga de cópia ODX é usada para migração de armazenamento de máquina virtual se o

armazenamento de origem e destino estiver no mesmo cluster.



Para aproveitar os casos de uso para a passagem de descarga de cópia ODX com Hyper-V, o sistema operacional convidado deve suportar ODX e os discos do sistema operacional convidado devem ser discos SCSI suportados pelo armazenamento (SMB ou SAN) que suporte ODX. Os discos IDE no sistema operacional convidado não suportam passagem ODX.

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 DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, 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.