# SAN-Storage-Management

ONTAP 9

NetApp
January 08, 2026

# Inhalt

# SAN-Storage-Management

# SAN-Konzepte

## SAN-Bereitstellung mit iSCSI

In SAN-Umgebungen sind Storage-Systeme Ziele mit Storage-Zielgeräten. Bei iSCSI und FC werden die Storage-Zielgeräte als LUNs (logische Einheiten) bezeichnet. Bei Non-Volatile Memory Express (NVMe) über Fibre Channel werden die Storage-Zielgeräte als Namespaces bezeichnet.

Sie konfigurieren Storage, indem Sie LUNs für iSCSI und FC erstellen oder Namespaces für NVMe erstellen. Auf die LUNs oder Namespaces wird von Hosts über iSCSI (Internet Small Computer Systems Interface)- oder FC-Protokollnetzwerke (Fibre Channel) zugegriffen.

Zur Verbindung mit iSCSI-Netzwerken können Hosts standardmäßige Ethernet-Netzwerkadapter (NICs), TCP Offload Engine (TOE) mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte iSCSI Host Bus Adapter (HBAs) verwenden.

Für die Verbindung mit FC-Netzwerken benötigen Hosts FC-HBAs oder CNAs.

Unterstützte FC-Protokolle:

- FC
- FCoE
- NVMe

#### Netzwerkverbindungen und Namen der iSCSI-Zielknoten

ISCSI-Zielknoten können sich auf verschiedene Weise mit dem Netzwerk verbinden:

- Über Ethernet-Schnittstellen mit in ONTAP integrierter Software
- Über mehrere Systemschnittstellen hinweg kann eine für iSCSI verwendete Schnittstelle auch den Datenverkehr für andere Protokolle, wie SMB und NFS, übertragen.
- Mit einem Unified Target Adapter (UTA) oder einem konvergierten Netzwerkadapter (CNA).

Jeder iSCSI-Knoten muss einen Knotennamen haben.

Die beiden Formate bzw. Typenbezeichnungen für iSCSI-Knotennamen sind *iqn* und *eui*. Das iSCSI-Ziel der SVM verwendet immer den iqn-Typ-Designator. Der Initiator kann entweder den iqn-Typ oder den eui-Typ-Designator verwenden.

#### Name des Storage-System-Nodes

Jede SVM, auf der iSCSI ausgeführt wird, verfügt über einen Standard-Node-Namen, der auf einem umgekehrten Domänennamen und einer eindeutigen Kodierungsnummer basiert.

Der Node-Name wird im folgenden Format angezeigt:

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

Im folgenden Beispiel wird der Standardknotenname für ein Speichersystem mit einer eindeutigen Kodierungsnummer angezeigt:

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

#### TCP-Port für iSCSI

Das iSCSI-Protokoll ist in ONTAP für die Verwendung von TCP-Portnummer 3260 konfiguriert.

ONTAP unterstützt nicht das Ändern der Portnummer für iSCSI. Die Portnummer 3260 ist als Teil der iSCSI-Spezifikation registriert und kann von keiner anderen Anwendung oder einem anderen Dienst verwendet werden.

#### Verwandte Informationen

"NetApp Dokumentation: ONTAP SAN Host-Konfiguration"

## ISCSI-Service-Management

#### ISCSI-Service-Management

Sie können die Verfügbarkeit des iSCSI-Dienstes auf den logischen iSCSI-Schnittstellen der SVM (Storage Virtual Machine) mit den `vserver iscsi interface enable` `vserver iscsi interface disable` Befehlen oder managen.

Standardmäßig ist der iSCSI-Service auf allen logischen iSCSI-Schnittstellen aktiviert.

##### Wie iSCSI auf dem Host implementiert wird

ISCSI kann auf dem Host mithilfe von Hardware oder Software implementiert werden.

Sie können iSCSI auf eine der folgenden Arten implementieren:

- Mit Initiator-Software, die die Standard-Ethernet-Schnittstellen des Hosts verwendet.
- Über einen iSCSI-Host Bus Adapter (HBA): Ein iSCSI-HBA erscheint dem Host-Betriebssystem als SCSI-Festplattenadapter mit lokalen Festplatten.
- Verwendung eines Adapters für die TCP Offload Engine (TOE), der die TCP/IP-Verarbeitung entlastet.

  Die iSCSI-Protokollverarbeitung wird weiterhin von der Host-Software durchgeführt.

#### Funktionsweise der iSCSI-Authentifizierung

Während der ersten Phase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanforderung an das Speichersystem, um eine iSCSI-Sitzung zu starten. Das Storage-System erlaubt dann entweder die Login-Anfrage oder lehnt sie ab oder stellt fest, dass keine Anmeldung erforderlich ist.

ISCSI-Authentifizierungsmethoden:

- Challenge Handshake Authentication Protocol (CHAP): Der Initiator meldet sich mit einem CHAP-Benutzernamen und -Passwort an.

Sie können ein CHAP-Kennwort festlegen oder ein hexadezimales Geheimkennwort generieren. Es gibt zwei Typen von CHAP-Benutzernamen und -Passwörtern:

  - Inbound – das Storage-System authentifiziert den Initiator.

    Eingehende Einstellungen sind erforderlich, wenn Sie die CHAP-Authentifizierung verwenden.

  - Outbound – Dies ist eine optionale Einstellung, die es dem Initiator ermöglicht, das Speichersystem zu authentifizieren.

    Sie können Outbound-Einstellungen nur verwenden, wenn Sie einen eingehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren.

- Deny- der Initiator wird dem Zugriff auf das Speichersystem verweigert.
- Keine – das Storage-System erfordert keine Authentifizierung für den Initiator.

Sie können die Liste der Initiatoren und deren Authentifizierungsmethoden definieren. Sie können auch eine Standardauthentifizierungsmethode definieren, die für Initiatoren gilt, die nicht in dieser Liste enthalten sind.

**Verwandte Informationen**

"Multipathing-Optionen für Windows mit Data ONTAP: Fibre Channel und iSCSI"

### Verwalten der iSCSI-Initiator-Sicherheit

ONTAP bietet eine Reihe von Funktionen zum Verwalten der Sicherheit für iSCSI-Initiatoren. Sie können eine Liste der iSCSI-Initiatoren und die Authentifizierungsmethode für jeden definieren, die Initiatoren und ihre zugehörigen Authentifizierungsmethoden in der Authentifizierungsliste anzeigen, Initiatoren aus der Authentifizierungsliste hinzufügen oder entfernen sowie die Standard-Authentifizierungsmethode für iSCSI-Initiatoren definieren, die nicht in der Liste enthalten sind.

### Isolierung von iSCSI-Endpunkten

Vorhandene iSCSI-Sicherheitsbefehle können einen IP-Adressbereich oder mehrere IP-Adressen akzeptieren.

Alle iSCSI-Initiatoren müssen die Ursprung-IP-Adressen bereitstellen, wenn eine Sitzung oder Verbindung zu einem Ziel eingerichtet wird. Durch diese neue Funktion wird verhindert, dass sich ein Initiator beim Cluster anmelden kann, wenn die Ursprung-IP-Adresse nicht unterstützt oder unbekannt ist und somit ein eindeutiges Identifikationsschema bereitgestellt wird. Jeder Initiator, der von einer nicht unterstützten oder unbekannten IP-Adresse stammt, wird seine Anmeldung auf der iSCSI-Sitzungsebene abgelehnt. Dies verhindert, dass der Initiator auf beliebige LUNs oder Volumes innerhalb des Clusters zugreift.

Implementieren Sie diese neue Funktion mit zwei neuen Befehlen, um bereits vorhandene Einträge zu verwalten.

#### Fügen Sie den Adressbereich des Initiators hinzu

Verbessern Sie die Sicherheitsverwaltung von iSCSI-Initiatoren, indem Sie einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security add-initiator-address-range` Befehl hinzufügen.

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

#### Entfernen Sie den Adressbereich des Initiators

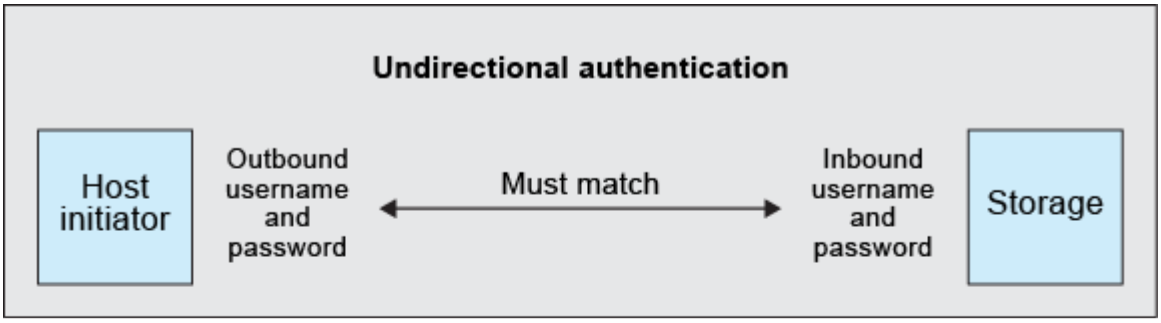
Entfernen Sie einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security remove-initiator-address-range` Befehl.

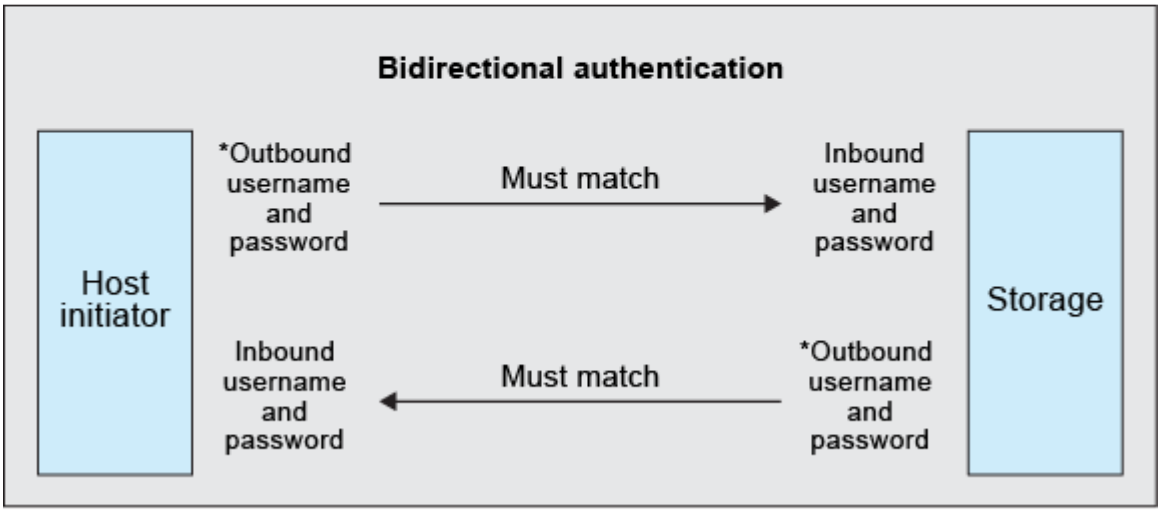
```
cluster1::> vserver iscsi security remove-initiator-address-range
```

### Erfahren Sie mehr über die CHAP-Authentifizierung für iSCSI-Initiatoren in ONTAP

Das Challenge Handshake Authentication Protocol (CHAP) ermöglicht die authentifizierte Kommunikation zwischen iSCSI-Initiatoren und Zielen. Wenn Sie CHAP-Authentifizierung verwenden, definieren Sie sowohl auf dem Initiator als auch auf dem Speichersystem CHAP-Benutzernamen und -Kennwörter.

Während der ersten Phase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanforderung an das Speichersystem, um die Sitzung zu starten. Die Anmeldeanforderung umfasst den CHAP-Benutzernamen und den CHAP-Algorithmus des Initiators. Das Speichersystem reagiert mit einer CHAP-Herausforderung. Der Initiator liefert eine CHAP-Antwort. Das Storage-System überprüft die Antwort und authentifiziert den Initiator. Das CHAP-Passwort wird zur Berechnung der Antwort verwendet.




*The outbound username and password for the host initiator must be different from the outbound username and password for the storage.

| Authentifizierung | Abgehender Anruf | Eingehend | Übereinstimmen? |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Unidirektional | Benutzername und Kennwort des Hostinitiators | Speicherbenutzername und Kennwort | Muss übereinstimmen |
| Bidirektional | Benutzername und Kennwort des Hostinitiators | Speicherbenutzername und Kennwort | Muss übereinstimmen |
| Bidirektional | Speicherbenutzername und Kennwort | Benutzername und Kennwort des Hostinitiators | Muss übereinstimmen |

Der ausgehende Benutzername und das Kennwort für den Hostinitiator müssen sich vom ausgehenden Benutzernamen und Kennwort für das Speichersystem unterscheiden.

#### Richtlinien für die Verwendung der CHAP-Authentifizierung

Befolgen Sie diese Richtlinien, wenn Sie die CHAP-Authentifizierung verwenden.

- Wenn Sie einen eingehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren, müssen Sie denselben Benutzernamen und dasselbe Kennwort für ausgehende CHAP-Einstellungen auf dem Initiator verwenden. Wenn Sie außerdem einen ausgehenden Benutzernamen und ein Kennwort auf dem Speichersystem definieren, um die bidirektionale Authentifizierung zu aktivieren, müssen Sie denselben Benutzernamen und dasselbe Kennwort für eingehende CHAP-Einstellungen auf dem Initiator verwenden.
- Sie können nicht denselben Benutzernamen und dasselbe Kennwort für ein- und ausgehende Einstellungen auf dem Speichersystem verwenden.
- CHAP-Benutzernamen können 1 bis 128 Bytes betragen.

  Das System lässt keine Null-Benutzernamen zu.

- CHAP-Passwörter (Schlüssel) können 1 bis 512 Bytes betragen.

  Passwörter können Hexadezimalwerte oder Zeichenfolgen sein. Bei Hexadezimalwerten sollten Sie den Wert mit dem Präfix „`0x`“ oder „`0X`“ eingeben.

  Das System lässt kein Nullkennwort zu.

> ONTAP ermöglicht die Verwendung von Sonderzeichen, nicht englischen Buchstaben, Zahlen und Leerzeichen für CHAP-Passwörter (Secrets). Dies unterliegt jedoch Host-Einschränkungen. Wenn einer dieser Server von Ihrem spezifischen Host nicht erlaubt ist, können diese nicht verwendet werden.
>
> Der Microsoft iSCSI-Software-Initiator beispielsweise erfordert, dass die CHAP-Passwörter für Initiator und Ziel mindestens 12 Bytes betragen, wenn keine IPsec-Verschlüsselung verwendet wird. Die maximale Kennwortlänge beträgt 16 Byte, unabhängig davon, ob IPsec verwendet wird.
>
> Weitere Einschränkungen finden Sie in der Dokumentation des Initiators.

### Die Verwendung von Zugriffslisten für iSCSI-Schnittstellen zur Begrenzung von Initiator-Schnittstellen kann Performance und Sicherheit erhöhen

MITHILFE VON ISCSI-Schnittstellenzutrittslisten kann die Anzahl der LIFs in einer SVM

begrenzt werden, auf die ein Initiator zugreifen kann. Dies erhöht die Performance und Sicherheit.

Wenn ein Initiator eine Erkennungssitzung mit einem iSCSI- `SendTargets`Befehl startet, erhält er die IP-Adressen, die dem LIF (Netzwerkschnittstelle) in der Zugriffsliste zugeordnet sind. Standardmäßig haben alle Initiatoren Zugriff auf alle iSCSI LIFs in der SVM. Mithilfe der Zugriffsliste können Sie die Anzahl der LIFs in einer SVM, auf die ein Initiator Zugriff hat, einschränken.

#### Internet Storage Name Service (iSNS) in ONTAP

Der Internet Storage Name Service (iSNS) ist ein Protokoll, das die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem TCP/IP-Speichernetzwerk ermöglicht. Ein iSNS-Server speichert Informationen über aktive iSCSI-Geräte im Netzwerk, einschließlich ihrer IP-Adressen, iSCSI-Knotennamen IQN's und Portalgruppen.

Sie können einen iSNS-Server von einem Drittanbieter beziehen. Wenn Sie in Ihrem Netzwerk einen iSNS-Server konfiguriert und für die Verwendung durch den Initiator und das Ziel aktiviert haben, können Sie die Management-LIF für eine Storage Virtual Machine (SVM) verwenden, um alle iSCSI-LIFs für diese SVM auf dem iSNS-Server zu registrieren. Nach Abschluss der Registrierung kann der iSCSI-Initiator den iSNS-Server abfragen, um alle LIFs für diese bestimmte SVM zu ermitteln.

Wenn Sie sich für die Verwendung eines iSNS-Dienstes entscheiden, müssen Sie sicherstellen, dass Ihre Storage Virtual Machines (SVMs) ordnungsgemäß bei einem Internet Storage Name Service (iSNS)-Server registriert sind.

Wenn Sie keinen iSNS-Server im Netzwerk haben, müssen Sie jedes Ziel manuell so konfigurieren, dass es für den Host sichtbar ist.

##### Was macht ein iSNS-Server

Ein iSNS-Server verwendet das iSNS-Protokoll (Internet Storage Name Service), um Informationen über aktive iSCSI-Geräte im Netzwerk zu erhalten, einschließlich ihrer IP-Adressen, iSCSI-Node-Namen (IQNs) und Portalgruppen.

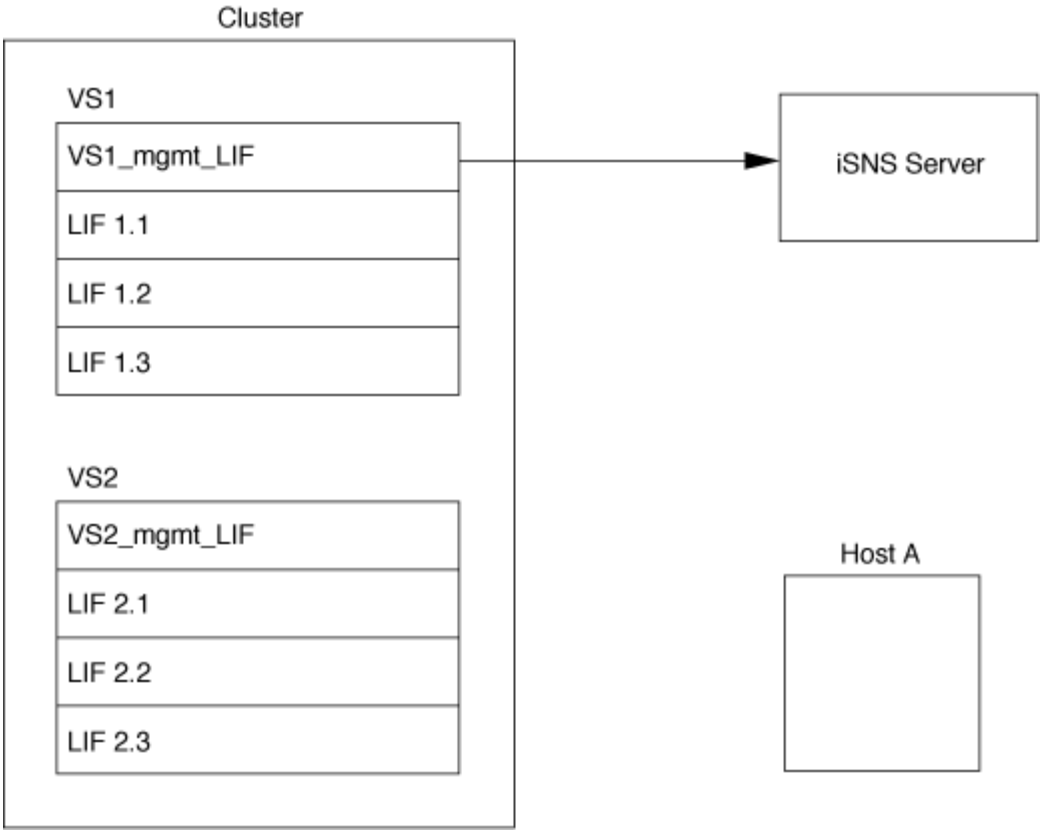
Das iSNS-Protokoll ermöglicht die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem IP-Speichernetzwerk. Ein iSCSI-Initiator kann den iSNS-Server abfragen, um iSCSI-Zielgeräte zu ermitteln.

NetApp bietet keine iSNS Server an oder verkauft diese weiter. Sie können diese Server von einem von NetApp unterstützten Anbieter beziehen.

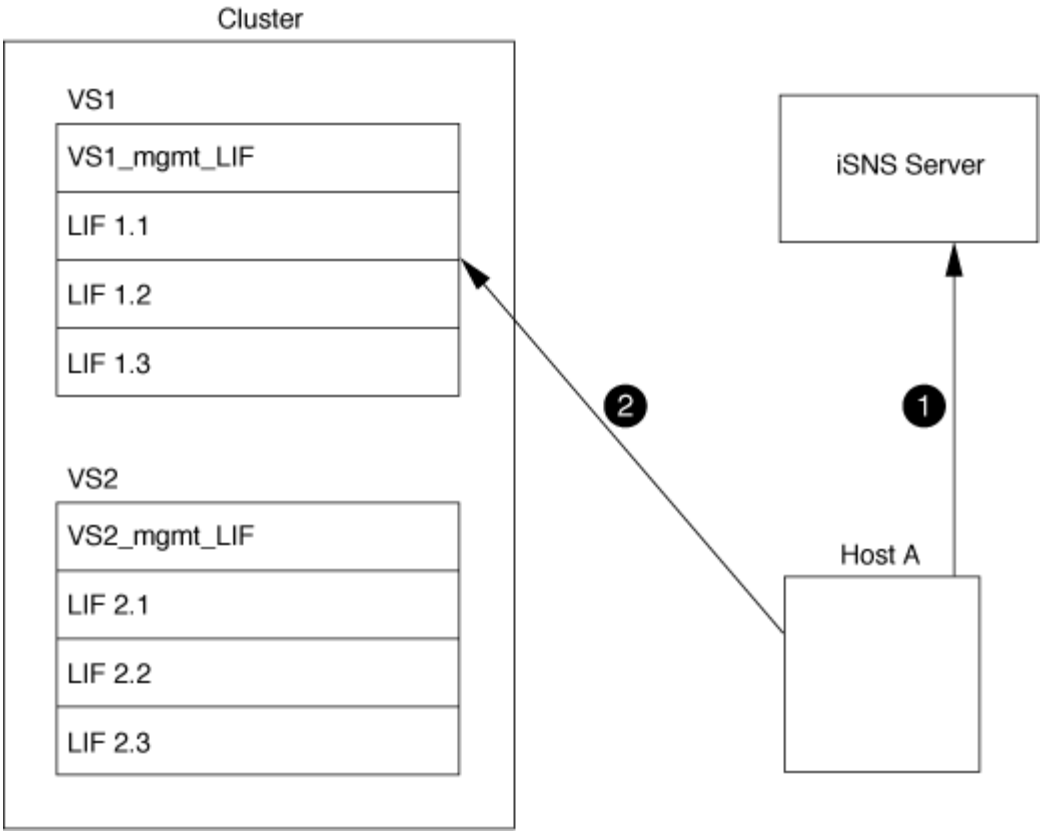
##### Interaktion von SVMs mit einem iSNS-Server

Der iSNS-Server kommuniziert über die SVM-Management-LIF mit jeder Storage Virtual Machine (SVM). Die Management-LIF registriert alle iSCSI-Zielknotennamen, -Alias und -Portalinformationen beim iSNS-Service für eine bestimmte SVM.

Im folgenden Beispiel verwendet die SVM „`VS1`“ die SVM-Management-LIF „`VS1_mgmt_LIF`“, um sich beim iSNS-Server zu registrieren. Während der iSNS-Registrierung sendet eine SVM alle iSCSI-LIFs über die SVM-Management-LIF an den iSNS-Server. Nach Abschluss der iSNS-Registrierung enthält der iSNS-Server eine Liste aller LIFs, die iSCSI in „`VS1`“ bereitstellen. Wenn ein Cluster mehrere SVMs enthält, muss sich jede SVM einzeln beim iSNS-Server registrieren, um den iSNS-Service nutzen zu können.




Im nächsten Beispiel kann Host A, nachdem der iSNS-Server die Registrierung beim Ziel abgeschlossen hat, alle LIFs für „`VS1`“ über den iSNS-Server ermitteln, wie in Schritt 1 angegeben. Nachdem Host A die Erkennung der LIFs für „`VS1`“ abgeschlossen hat, kann Host A wie in Schritt 2 gezeigt eine Verbindung zu jedem der LIFs in „`VS1`“ herstellen. Host A erkennt keine der LIFs in „`VS2`“, bis sich die Management-LIF „`VS2_mgmt_LIF`“ für „`VS2`“ beim iSNS-Server registriert hat.




Wenn Sie jedoch die Schnittstellenzugriffslisten definieren, kann der Host nur die definierten LIFs in der Schnittstellenzugangsliste verwenden, um das Ziel zu erreichen.

Nach der anfänglichen Konfiguration von iSNS aktualisiert ONTAP den iSNS-Server automatisch, wenn sich die SVM-Konfigurationseinstellungen ändern.

Zwischen dem Zeitpunkt, zu dem Sie die Konfigurationsänderungen vornehmen, und dem Zeitpunkt, an dem ONTAP das Update an den iSNS-Server sendet, kann es zu einer Verzögerung von einigen Minuten kommen. Sofortige Aktualisierung der iSNS-Informationen auf dem iSNS-Server erzwingen: `vserver iscsi isns update`. Erfahren Sie mehr über `vserver iscsi isns update` in der "ONTAP-Befehlsreferenz".

#### Befehle zum Verwalten von iSNS

ONTAP bietet Befehle zur Verwaltung Ihres iSNS-Service.

| Ihr Ziel ist | Befehl |
|---|---|
| Konfigurieren Sie einen iSNS-Dienst | `vserver iscsi isns create` |
| Starten Sie einen iSNS-Dienst | `vserver iscsi isns start` |
| Ändern eines iSNS-Dienstes | `vserver iscsi isns modify` |
| ISNS-Servicekonfiguration anzeigen | `vserver iscsi isns show` |

| | |
|---|---|
| Aktualisierung der registrierten iSNS-Informationen erzwingen | `vserver iscsi isns update` |
| Stoppen Sie einen iSNS-Dienst | `vserver iscsi isns stop` |
| Entfernen Sie einen iSNS-Dienst | `vserver iscsi isns delete` |
| Zeigen Sie die man-Page für einen Befehl an | `man command name` |

Erfahren Sie mehr über `vserver iscsi isns` in der "ONTAP-Befehlsreferenz".

## SAN Provisionierung mit FC

Wichtige Konzepte sollten Sie kennen, um zu verstehen, wie ONTAP FC SAN implementiert.

### Wie FC-Ziel-Nodes mit dem Netzwerk verbunden werden

Storage-Systeme und Hosts verfügen über Adapter, sodass sie mit Kabeln FC-Switches verbunden werden können.

Wenn ein Node mit dem FC SAN verbunden ist, registriert jede SVM zusammen mit dem Fabric Name Service den World Wide Port Name (WWPN) ihrer logischen Schnittstelle. Der WWNN der SVM und der WWPN jeder logischen Schnittstelle werden automatisch durch ONTAP zugewiesen.

Die direkte Verbindung zu Nodes von Hosts mit FC wird nicht unterstützt, NPIV ist erforderlich und dies erfordert einen Switch, der verwendet werden muss. Bei iSCSI-Sessions funktioniert die Kommunikation mit Verbindungen, die entweder über Netzwerk oder direkt verbunden sind. Beide Methoden werden jedoch von ONTAP unterstützt.

### So werden FC-Knoten identifiziert

Jede mit FC konfigurierte SVM wird durch einen Worldwide Node Name (WWNN) identifiziert.

### Verwendung von WWPNs

WWPNs identifizieren jede LIF in einer SVM, die zur Unterstützung von FC konfiguriert ist. Diese LIFs verwenden die physischen FC-Ports in jedem Node im Cluster, bei denen es sich um FC-Zielkarten, UTA oder UTA2 handeln kann, die als FC oder FCoE in den Nodes konfiguriert sind.

- Erstellen einer Initiatorgruppe

  Die WWPNs der HBAs des Hosts werden zum Erstellen einer Initiatorgruppe verwendet. Eine Initiatorgruppe wird verwendet, um den Host-Zugriff auf bestimmte LUNs zu steuern. Sie können eine Initiatorgruppe erstellen, indem Sie eine Sammlung von WWPNs von Initiatoren in einem FC-Netzwerk angeben. Wenn Sie eine LUN auf einem Storage-System einer Initiatorgruppe zuordnen, können Sie allen Initiatoren in dieser Gruppe Zugriff auf diese LUN gewähren. Wenn der WWPN eines Hosts nicht zu einer Initiatorgruppe gehört, die einer LUN zugeordnet ist, hat der Host keinen Zugriff auf die LUN. Das bedeutet, dass die LUNs nicht als Datenträger auf diesem Host angezeigt werden.

Sie können auch Portsätze erstellen, um eine LUN nur auf bestimmten Zielports sichtbar zu machen. Ein Port-Satz besteht aus einer Gruppe von FC-Ziel-Ports. Sie können eine Initiatorgruppe an einen Portsatz binden. Jeder Host in der Initiatorgruppe kann nur durch Verbindung mit den Ziel-Ports im festgelegten Port auf die LUNs zugreifen.

- Identifizierung von FC-LIFs auf einzigartige Weise

  WWPNs identifizieren jede logische FC-Schnittstelle individuell. Das Host-Betriebssystem verwendet die Kombination des WWNN und WWPN, um SVMs und FC LIFs zu identifizieren. Einige Betriebssysteme erfordern eine dauerhafte Bindung, um sicherzustellen, dass die LUN mit derselben Ziel-ID auf dem Host angezeigt wird.

### Funktionsweise von weltweiten Namenszuweisungen

Weltweite Namen werden sequenziell in ONTAP erstellt. Aufgrund der Art und Weise, wie ONTAP sie zuweist, werden sie möglicherweise in nicht-sequenzieller Reihenfolge zugewiesen.

Jeder Adapter verfügt über einen vorkonfigurierten WWPN und den WWNN, ONTAP verwendet jedoch diese vorkonfigurierten Werte nicht. Stattdessen weist ONTAP basierend auf den MAC-Adressen der integrierten Ethernet-Ports seine eigenen WWPNs oder WWNNs zu.

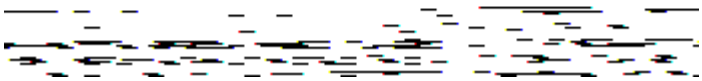
Die weltweiten Namen scheinen aus folgenden Gründen nicht sequenziell zu sein:

- Alle Nodes und Storage Virtual Machines (SVMs) im Cluster werden weltweit Namen zugewiesen.
- Freigegebene weltweite Namen werden wiederverwertet und wieder dem Pool verfügbarer Namen hinzugefügt.

### So werden FC Switches identifiziert

Fibre Channel-Switches verfügen über einen Worldwide Node Name (WWNN) für das Gerät selbst und einen weltweiten Port-Namen (WWPN) für jeden seiner Ports.

Das folgende Diagramm zeigt beispielsweise, wie den jeweiligen Ports auf einem Brocade Switch mit 16 Ports die WWPNs zugewiesen werden. Weitere Informationen zur Nummer der Ports für einen bestimmten Switch finden Sie in der Dokumentation des Anbieters für diesen Switch.



Port **0**, WWPN 20:**00**:00:60:69:51:06:b4

Port **1**, WWPN 20:**01**:00:60:69:51:06:b4

Port **14**, WWPN 20:**0e**:00:60:69:51:06:b4

Port **15**, WWPN 20:**0f**:00:60:69:51:06:b4

## SAN-Provisionierung mit NVMe

Ab ONTAP 9.4 wird NVMe/FC in der SAN-Umgebung unterstützt. Mit NVMe/FC können Storage-Administratoren Namespaces und Subsysteme bereitstellen und anschließend den Namespaces Subsystemen zuordnen, ähnlich der Art und Weise, wie LUNs bereitgestellt und Initiatorgruppen für FC und iSCSI zugeordnet werden.

Ein NVMe Namespace ist eine Menge nicht-flüchtiger Speicher, der in logische Blöcke formatiert werden kann. Namespaces sind das Äquivalent von LUNs für FC- und iSCSI-Protokolle, und ein NVMe-Subsystem entspricht einer igroup. Ein NVMe-Subsystem kann Initiatoren zugeordnet werden, sodass die zugehörigen Initiatoren auf Namespaces innerhalb des Subsystems zugreifen können.

Obwohl die Funktion analog ist, unterstützen NVMe-Namespaces nicht alle von LUNs unterstützten Funktionen.

Ab ONTAP 9.5 ist eine Lizenz erforderlich, um den Host-bezogenen Datenzugriff mit NVMe zu unterstützen. Wenn NVMe in ONTAP 9.4 aktiviert ist, erhält der Erwerb der Lizenz nach dem Upgrade auf ONTAP 9.5 eine 90-tägige Gnadenfrist. Falls ja"ONTAP One", sind die NVMe Lizenzen enthalten. Sie können die Lizenz mit dem folgenden Befehl aktivieren:

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

**Verwandte Informationen**

"Technischer Bericht von NetApp 4684: Implementieren und Konfigurieren moderner SANs mit NVMe/FC"

## SAN Volumes

### Über SAN Volumes – Übersicht

ONTAP bietet drei grundlegende Volume-Bereitstellungsoptionen: Thick Provisioning, Thin Provisioning und semi-Thick Provisioning. Jede Option nutzt unterschiedliche Methoden zum Managen des Volume-Speicherplatzes und des Platzbedarfs für die ONTAP Technologien zur gemeinsamen Nutzung von Blöcken. Wenn Sie verstehen, wie diese Optionen funktionieren, können Sie die beste Option für Ihre Umgebung wählen.

Es wird nicht empfohlen, SAN-LUNs und NAS-Freigaben in ein und demselben FlexVol-Volume einzurichten. Sie sollten separate FlexVol Volumes speziell für Ihre SAN LUNs bereitstellen, und Sie sollten separate FlexVol Volumes speziell für Ihre NAS-Freigaben bereitstellen. Dies vereinfacht die Implementierung von Management und Replizierung und Parallelen zur Unterstützung von FlexVol Volumes durch Active IQ Unified Manager (ehemals OnCommand Unified Manager).

#### Thin Provisioning für Volumes

Wenn ein Thin Provisioning Volume erstellt wird, reserviert ONTAP bei der Erstellung des Volume keinen zusätzlichen Speicherplatz. Wenn Daten auf das Volume geschrieben werden, fordert das Volume zur Erfüllung der Schreibvorgänge den erforderlichen Storage vom Aggregat an. Bei der Verwendung von Volumes, die Thin Provisioning einsetzen, können Sie Ihr Aggregat bei einer Überprovisionierung einsetzen. Dadurch wird es möglich, dass das Volume den erforderlichen Speicherplatz nicht sichern kann, wenn dem Aggregat der freie Speicherplatz ausgeht.

Sie erstellen eine FlexVol volume mit Thin Provisioning, indem Sie die `-space-guarantee` Option auf setzen `none`.

#### Thick Provisioning für Volumes

Wenn ein Thick Provisioning Volume erstellt wird, legt ONTAP ausreichend Storage vom Aggregat ab, um sicherzustellen, dass jeder Block im Volume jederzeit geschrieben werden kann. Wenn Sie ein Volume für die Nutzung von Thick Provisioning konfigurieren, können Sie jede der ONTAP Storage-Effizienz-Funktionen einsetzen, beispielsweise für Komprimierung und Deduplizierung, um die höheren Storage-Anforderungen im Vorfeld zu erfüllen.

Sie erstellen eine Thick-Provisioning-FlexVol volume, indem Sie deren `-space-slo` Option (Service-Level-Ziel) auf setzen `thick`.

#### Semi-Thick Provisioning für Volumes

Wenn ein Volume mit semi-Thick Provisioning erstellt wird, legt ONTAP Storage vom Aggregat zu, um die Volume-Größe zu berücksichtigen. Ist der Speicherplatz des Volume knapp, weil Blöcke durch Block-Sharing-Technologien genutzt werden, ist ONTAP bemüht, Sicherungsdatenobjekte (Snapshots und FlexClone-Dateien sowie LUNs) zu löschen, um den Speicherplatz freizugeben. Solange ONTAP die geschützten Datenobjekte schnell genug löschen kann, um mit dem für Überschreibungen erforderlichen Speicherplatz Schritt zu halten, sind die Schreibvorgänge weiterhin erfolgreich. Dies wird als „`Best Effort`“-Garantie bezeichnet.

**Hinweis:** die folgende Funktionalität wird auf Volumes, die semi-Thick Provisioning verwenden, nicht unterstützt:

- Storage-Effizienztechnologien wie Deduplizierung, Komprimierung und Data-Compaction
- Microsoft Offloaded Data Transfer (ODX)

Sie erstellen eine FlexVol volume mit halbem Thick Provisioning, indem Sie die `-space-slo` Option (Service Level Objective) auf setzen `semi-thick`.

#### Nutzung mit platzsparenden Dateien und LUNs

Eine speicherreservierte Datei oder eine LUN ist eine Datei, für die beim Erstellen Speicherplatz zugewiesen wird. Ursprünglich hat NetApp den Begriff „`Thin-Provision-LUN`“ verwendet, um eine LUN zu bedeuten, für die Platzreservierung deaktiviert ist (eine nicht-space-reservierte LUN).

**Hinweis:** nicht-speicherreservierte Dateien werden allgemein nicht als “Thin Provisioning-Dateien” bezeichnet.

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen der Verwendung der drei Optionen zur Volume-Bereitstellung für platzreservierte Dateien und LUNs zusammengefasst:

| Volume-Provisionierung | LUN-/Dateispeicherreservierung | Überschreibung | Sicherungsdaten[2] | Storage-Effizienz[3] |
|---|---|---|---|---|
| Dick | Unterstützt | Garantiert[1] | Garantiert | Unterstützt |
| Dünn | Keine Auswirkung | Keine | Garantiert | Unterstützt |
| Semi-dick | Unterstützt | Bester Aufwand[1] | So gut wie möglich | Nicht unterstützt |

### Hinweise

1. Um Überschreibungen zu garantieren oder ihnen eine optimale Überschreibsicherung zu ermöglichen, ist die Speicherplatzreservierung auf dem LUN oder der Datei aktiviert.
2. Zu den Sicherungsdaten gehören Snapshots sowie FlexClone-Dateien und LUNs, die zum automatischen Löschen markiert sind (Backup-Klone).
3. Storage-Effizienz umfasst Deduplizierung, Komprimierung sowie alle FlexClone-Dateien und LUNs, die nicht zum automatischen Löschen markiert sind (aktive Klone) und Unterdateien von FlexClone (für Copy Offload verwendet).

#### Unterstützung von SCSI Thin Provisioning LUNs

ONTAP unterstützt T10 SCSI Thin Provisioning LUNs sowie NetApp Thin Provisioning LUNs. Mit T10 SCSI Thin Provisioning können Host-Applikationen SCSI-Funktionen unterstützen, einschließlich LUN-Speicherplatzrückgewinnung und LUN-Speicherplatzüberwachung für Umgebungen mit Blöcken. T10 SCSI Thin Provisioning muss von Ihrer SCSI-Host-Software unterstützt werden.

Sie verwenden die ONTAP- `space-allocation`Einstellung, um die Unterstützung für den T10 Thin Provisioning auf einer LUN zu aktivieren/deaktivieren. Sie verwenden die ONTAP- `space-allocation enable`Einstellung, um T10-SCSI-Thin-Provisioning auf einer LUN zu aktivieren.

Der `[-space-allocation {enabled|disabled}]` Befehl im "ONTAP-Befehlsreferenz" bietet weitere Informationen zum Aktivieren/Deaktivieren der Unterstützung für T10 Thin Provisioning und zum Aktivieren von T10 SCSI Thin Provisioning auf einer LUN.

### Konfiguration der Bereitstellungsoptionen für Volumes

## Sie können ein Volume für Thin Provisioning, Thick Provisioning oder Semi-Thick Provisioning konfigurieren.

#### Über diese Aufgabe

```
`-space-slo` `thick`Durch Festlegen der Option wird Folgendes
sichergestellt:
```

- Das gesamte Volume wird im Aggregat vorab zugewiesen. Sie können die `volume create` `volume modify` `-space-guarantee` Option des Volumes nicht mit dem Befehl oder konfigurieren.
- 100 % des für Überschreibungen benötigten Speicherplatzes ist reserviert. Sie können die `volume modify` `-fractional-reserve` Option des Volumes nicht mit dem Befehl konfigurieren

```
`-space-slo` `semi-thick`Durch Festlegen der Option wird Folgendes
sichergestellt:
```

- Das gesamte Volume wird im Aggregat vorab zugewiesen. Sie können die `volume create` `volume modify` `-space-guarantee` Option des Volumes nicht mit dem Befehl oder konfigurieren.
- Kein Speicherplatz für Überschreibungen reserviert. Sie können die `volume modify` `-fractional -reserve` Option des Volumes mit dem Befehl konfigurieren.
- Das automatische Löschen von Snapshots ist aktiviert.

**Schritt**

1. Konfiguration der Bereitstellungsoptionen für Volumes:

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

   Die `-space-guarantee` Option ist standardmäßig `none` für AFF Systeme und für Volumes ohne AFF-DP eingestellt. Andernfalls wird standardmäßig auf `volume`. Verwenden Sie für vorhandene FlexVol-Volumes den `volume modify` Befehl, um Bereitstellungsoptionen zu konfigurieren.

   Der folgende Befehl konfiguriert vol1 auf SVM vs1 für Thin Provisioning:

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

   Mit dem folgenden Befehl wird vol1 auf SVM vs1 für Thick Provisioning konfiguriert:

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

   Mit dem folgenden Befehl wird vol1 auf SVM vs1 für semi-Thick Provisioning konfiguriert:

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

**SAN Volume-Konfigurationsoptionen**

Sie müssen verschiedene Optionen auf dem Volume festlegen, das Ihre LUN enthält. Die Art und Weise, wie Sie die Volume-Optionen festlegen, bestimmt die Menge an Speicherplatz, die LUNs im Volume zur Verfügung steht.

**Autogrow**

Sie können Autogrow aktivieren oder deaktivieren. Wenn Sie es aktivieren, ermöglicht es Autogrow ONTAP, die Größe des Volumes automatisch auf eine maximale Größe zu erhöhen, die Sie vorab bestimmen. Um das automatische Wachstum des Volumes zu unterstützen, muss im enthaltenden Aggregat Platz vorhanden sein. Wenn Sie Autogrow aktivieren, müssen Sie daher den freien Speicherplatz im Aggregat, der enthält, überwachen und bei Bedarf mehr hinzufügen.

Autogrow kann nicht zur Unterstützung der Snapshot-Erstellung ausgelöst werden. Wenn Sie versuchen, einen Snapshot zu erstellen und nicht genügend Speicherplatz auf dem Volume vorhanden ist, schlägt die Erstellung des Snapshots fehl, selbst bei aktivierter Autogrow.

Wenn Autogrow deaktiviert ist, bleibt die Größe Ihres Volumes dieselbe.

**Autochrink**

Sie können Autochrink aktivieren oder deaktivieren. Wenn Sie ihn aktivieren, ermöglicht Autochrink es ONTAP,

die Gesamtgröße eines Volumes automatisch zu verringern, wenn die Menge an Speicherplatz, die im Volume verbraucht wird, einen vorab festgelegten Schwellenwert verringert. Dies erhöht die Storage-Effizienz, indem Volumes automatisch ungenutzten freien Speicherplatz freigeben.

#### Snapshot wird automatisches Löschen erstellt

Snapshot Autodelete löscht Snapshots automatisch, wenn eine der folgenden Aktionen durchgeführt wird:

- Das Volume ist fast voll.
- Der Speicherplatz der Snapshot-Reserve ist fast voll.
- Der Speicherplatz der Überschreibungsreserve ist voll.

Sie können das automatische Löschen von Snapshots so konfigurieren, dass Snapshots vom ältesten zum neuesten oder vom neuesten zum ältesten gelöscht werden. Snapshots, die mit Snapshots in geklonten Volumes oder LUNs verknüpft sind, werden durch automatisches Löschen von Snapshots nicht gelöscht.

Wenn Ihr Volume zusätzlichen Platz benötigt und Sie sowohl Autogrow als auch Snapshot Autodelete aktiviert haben, versucht ONTAP standardmäßig, den benötigten Platz zu beschaffen, indem zuerst Autogrow ausgelöst wird. Wenn nicht genügend Speicherplatz über Autogrow erworben wird, dann wird Snapshot Autodelete ausgelöst.

#### Snapshot Reserve

Snapshot-Reserve definiert den Speicherplatz im Volume, der für Snapshots reserviert ist. Der Snapshot-Reserve zugewiesener Speicherplatz kann nicht für einen anderen Zweck verwendet werden. Wenn der gesamte für die Snapshot-Reserve zugewiesene Speicherplatz verwendet wird, beginnen Snapshots, zusätzlichen Speicherplatz auf dem Volume zu beanspruchen.

### Anforderung für das Verschieben von Volumes in SAN-Umgebungen

Bevor Sie ein Volume mit LUNs oder Namespaces verschieben, müssen Sie bestimmte Anforderungen erfüllen.

- Für Volumes mit einer oder mehreren LUNs sollten mindestens zwei Pfade pro LUN (LIFs) vorhanden sein, die mit jedem Node im Cluster verbunden sind.

  So werden Single Points of Failure eliminiert und das System kann den Ausfall von Komponenten überleben.

- Für Volumes, die Namespaces enthalten, muss auf dem Cluster ONTAP 9.6 oder höher ausgeführt werden.

  Die Volume-Verschiebung wird für NVMe Konfigurationen mit ONTAP 9.5 nicht unterstützt.

### Überlegungen bei der Festlegung der fraktionalen Reserve

Die fraktionale Reserve, auch *LUN Overwrite Reserve* genannt, ermöglicht Ihnen die Abschaltung der Überschreibungsreserve für platzsparende LUNs und Dateien in einem FlexVol Volume. So können Sie Ihre Storage-Auslastung maximieren, aber wenn Ihre Umgebung durch mangelnde Schreibzugriffe beeinträchtigt ist, müssen Sie die Anforderungen dieser Konfiguration kennen und verstehen, die diese Konfiguration mit sich bringt.

Die Einstellung für die fraktionale Reserve wird als Prozentsatz angegeben; die einzigen gültigen Werte sind `0` und `100` Prozent. Die Einstellung der fraktionalen Reserve ist ein Attribut des Volume.

Wenn Sie die fraktionale Reserve einstellen, um `0` Ihre Storage-Auslastung zu erhöhen. Bei einer Applikation, die auf Daten im Volume zugreift, kann es jedoch zu einem Datenausfall kommen, wenn der Speicherplatz auf `volume`dem Volume nicht mehr voll ist, selbst wenn die Volume-Garantie auf festgelegt ist. Durch ordnungsgemäße Volume-Konfiguration und Nutzung können Sie jedoch die Wahrscheinlichkeit eines Schreibversagens minimieren. ONTAP bietet eine „`Best Effort`"-Schreibgarantie für Volumes mit einer fraktionalen Reserve `0`, die auf „ all" der folgenden Anforderungen gesetzt wurde:

- Die Deduplizierung wird nicht verwendet
- Die Komprimierung wird nicht verwendet
- Die Unterdateien von FlexClone werden nicht verwendet
- Alle FlexClone Dateien und FlexClone LUNs sind zum automatischen Löschen aktiviert

  Dies ist nicht die Standardeinstellung. Sie müssen das automatische Löschen entweder während der Erstellung oder durch Ändern der FlexClone Datei oder der FlexClone LUN nach der Erstellung aktivieren.

- ODX und FlexClone Copy Offload werden derzeit nicht genutzt
- Volume-Garantie wird auf festgelegt `volume`
- Die Speicherplatzreservierung für Datei oder LUN ist `enabled`
- Die Volume Snapshot Reserve wurde auf festgelegt `0`
- Volume Snapshot automatische Löschung ist `enabled` mit einem Commitment-Level von `destroy`, eine Destroy-Liste von `lun_clone,vol_clone,cifs_share,file_clone,sfsr`, und ein Trigger von `volume`

  Diese Einstellung stellt zudem sicher, dass FlexClone Dateien und FlexClone LUNs im Bedarfsfall gelöscht werden.

Beachten Sie, dass bei einer hohen Änderungsrate in seltenen Fällen das automatische Löschen von Snapshots zurückfallen kann, was dazu führt, dass der Speicherplatz auf dem Volume nicht mehr zur Verfügung steht, selbst wenn alle oben genannten erforderlichen Konfigurationseinstellungen verwendet werden.

Optional können Sie auch die Volume Autogrow Funktion verwenden, um die Wahrscheinlichkeit zu verringern, dass Volume Snapshots automatisch gelöscht werden müssen. Wenn Sie die Autogrow-Funktion aktivieren, müssen Sie den freien Speicherplatz im zugehörigen Aggregat überwachen. Wenn das Aggregat voll genug wird, dass das Volumen daran gehindert wird zu wachsen, werden wahrscheinlich mehr Snapshots gelöscht werden, da der freie Platz im Volumen erschöpft ist.

Wenn Sie nicht alle oben genannten Konfigurationsanforderungen erfüllen können und Sie sicherstellen müssen, dass dem Volume nicht der Platz knapp wird, müssen Sie die fraktionale Reserve des Volume auf einstellen `100`. Dies erfordert vorab mehr freien Speicherplatz, garantiert jedoch, dass Datenänderungen auch dann erfolgreich ausgeführt werden, wenn die oben aufgeführten Technologien eingesetzt werden.

Der Standardwert und die zulässigen Werte für die Einstellung der fraktionalen Reserve hängen von der Garantie des Volume ab:

| Volume-Garantie | Standardmäßige fraktionale Reserve | Zulässige Werte |
|---|---|---|
| Datenmenge | 100 | 0, 100 |
| Keine | 0 | 0, 100 |

## SAN-Host-seitiges Speicherplatzmanagement

In einer Thin Provisioning-Umgebung schließt das Host-seitige Speicherplatzmanagement den Prozess der Verwaltung von Speicherplatz vom Storage-System ab, das im Host File-System freigegeben wurde.

Ein Host-Filesystem enthält Metadaten, um zu verfolgen, welche Blöcke zum Speichern neuer Daten verfügbar sind und welche Blöcke gültige Daten enthalten, die nicht überschrieben werden dürfen. Diese Metadaten werden innerhalb der LUN oder im Namespace gespeichert. Wenn eine Datei im Host-Filesystem gelöscht wird, werden die Metadaten des Filesystems aktualisiert, um die Blöcke dieser Datei als freien Speicherplatz zu markieren. Der gesamte freie Speicherplatz des Filesystems wird dann neu berechnet, um die neu freigegebenen Blöcke einzubeziehen. Für das Speichersystem werden diese Metadatenaktualisierungen nicht von anderen Schreibvorgängen angezeigt, die vom Host ausgeführt werden. Daher ist im Storage-System keine Löschung aufgetreten.

Dadurch entsteht eine Diskrepanz zwischen der Menge an freiem Speicherplatz, die vom Host gemeldet wird, und der Menge an freiem Speicherplatz, die vom zugrunde liegenden Storage-System gemeldet wird. Nehmen wir beispielsweise an, dass Ihrem Host durch Ihr Storage-System eine neu bereitgestellte 200-GB-LUN zugewiesen ist. Sowohl der Host als auch das Speichersystem berichten von 200 GB freiem Speicherplatz. Ihr Host schreibt dann 100 GB Daten. An diesem Punkt berichten sowohl der Host als auch das Speichersystem von 100 GB belegten Speicherplatz und 100 GB nicht genutztem Speicherplatz.

Dann löschen Sie 50 GB Daten von Ihrem Host. An dieser Stelle meldet Ihr Host 50 GB verbrauchten Speicherplatz und 150 GB nicht genutzten Speicherplatz. Ihr Speichersystem wird jedoch 100 GB verwendeten Speicherplatzes und 100 GB nicht genutzten Speicherplatz melden.

Das Host-seitige Speicherplatzmanagement verwendet verschiedene Methoden, um den Speicherplatzunterschied zwischen dem Host und dem Storage-System abzugleichen.

#### Vereinfachtes Host-Management mit SnapCenter

Mit SnapCenter können Sie einige Management- und Datensicherungsaufgaben von iSCSI- und FC-Storage vereinfachen. SnapCenter ist ein optionales Management-Paket für Windows- und UNIX-Hosts.

Mit der SnapCenter Software lassen sich aus Storage-Pools problemlos virtuelle Festplatten erstellen, die an mehrere Storage-Systeme verteilt werden können. Außerdem lassen sich Storage-Bereitstellungsaufgaben automatisieren und die Erstellung von Snapshots und Klonen aus Snapshots gemäß den Host-Daten vereinfachen.

Weitere Informationen finden Sie in der NetApp Produktdokumentation zu "SnapCenter".

#### Weiterführende Links

"ONTAP-Speicherplatzzuweisung für SAN-Protokolle aktivieren"

## Allgemeines zu Initiatorgruppen

Initiatorgruppen sind Tabellen mit FC-Protokoll-Host-WWPNs oder iSCSI-Host-Node-Namen. Sie können Initiatorgruppen definieren und sie LUNs zuordnen, um zu steuern, welche Initiatoren Zugriff auf LUNs haben.

Normalerweise möchten Sie, dass alle Initiator-Ports oder Software-Initiatoren des Hosts Zugriff auf eine LUN haben. Wenn Sie Multipathing-Software oder Cluster-Hosts verwenden, benötigt jeder Initiator- oder Software-Initiator jedes Cluster-Hosts redundante Pfade zu derselben LUN.

Sie können Initiatorgruppen erstellen, die angeben, welche Initiatoren entweder vor oder nach dem Erstellen der LUNs Zugriff auf die LUNs haben. Sie müssen jedoch Initiatorgruppen erstellen, bevor Sie eine LUN einer Initiatorgruppe zuordnen können.

Initiatorgruppen können mehrere Initiatoren haben, und mehrere Initiatorgruppen können denselben Initiator haben. Sie können eine LUN jedoch nicht mehreren Initiatorgruppen zuordnen, die denselben Initiator haben. Ein Initiator kann nicht Mitglied von iGroups verschiedener ostypes sein.

#### Beispiel dafür, wie Initiatorgruppen LUN-Zugriff geben

Sie können mehrere Initiatorgruppen erstellen, um zu definieren, welche LUNs Ihren Hosts zur Verfügung stehen. Wenn Sie beispielsweise ein Host-Cluster haben, können Sie Initiatorgruppen verwenden, um sicherzustellen, dass bestimmte LUNs nur für einen Host im Cluster oder für alle Hosts im Cluster sichtbar sind.

In der folgenden Tabelle wird erläutert, wie vier Initiatorgruppen für vier verschiedene Hosts, die auf das Storage-System zugreifen, auf die LUNs zugreifen. Die Cluster-Hosts (host3 und Host4) sind beide Mitglieder derselben Initiatorgruppe (Gruppe 3) und können auf die LUNs zugreifen, die dieser Initiatorgruppe zugeordnet sind. Die igroup namens group4 enthält die WWPNs von Host4 zum Speichern von lokalen Informationen, die vom Partner nicht erkannt werden sollen.

| Hosts mit HBA-WWPNs, IQNs oder EUIs | igroups | WWPNs, IQNs, EUIs, die Initiatorgruppen hinzugefügt wurden | LUNs zugeordnet zu Initiatorgruppen |
|---|---|---|---|
| Host1, Single Path (iSCSI Software Initiator)<br><br>iqn.1991-05.com.microsoft:host1 | gruppe1 | iqn.1991-05.com.microsoft:host1 | `/vol/vol2/lun1` |
| Host 2, Multipath (zwei HBAs)<br><br>10:00:00:00:c9:2b:6b:3c<br><br>10:00:00:00:c9:2b:02:3c | gruppe2 | 10:00:00:00:c9:2b:6b:3c<br><br>10:00:00:00:c9:2b:02:3c | `/vol/vol2/lun2` |

| Hosts mit HBA-WWPNs, IQNs oder EUIs | igroups | WWPNs, IQNs, EUIs, die Initiatorgruppen hinzugefügt wurden | LUNs zugeordnet zu Initiatorgruppen |
|---|---|---|---|
| Host3, Multipath, Cluster mit Host 4<br><br>10:00:00:00:c9:2b:32:1b<br><br>10:00:00:00:c9:2b:41:02 | gruppe3 | 10:00:00:00:c9:2b:32:1b<br><br>10:00:00:00:c9:2b:41:02<br><br>10:00:00:00:c9:2b:51:2c<br><br>10:00:00:00:c9:2b:47:a2 | `/vol/vol2/qtree1/lun3` |
| HOST4, Multipath, Clustered (nicht als Host sichtbar)<br><br>10:00:00:00:c9:2b:51:2c<br><br>10:00:00:00:c9:2b:47:a2 | Gruppe 4 | 10:00:00:00:c9:2b:51:2c<br><br>10:00:00:00:c9:2b:47:a2 | `/vol/vol2/qtree2/lun4`<br>`/vol/vol2/qtree1/lun5` |

## Geben Sie Initiator-WWPNs und iSCSI-Node-Namen für eine Initiatorgruppe an

Sie können die iSCSI-Node-Namen und WWPNs der Initiatoren angeben, wenn Sie eine Initiatorgruppe erstellen oder sie später hinzufügen können. Wenn Sie beim Erstellen der LUN die iSCSI-Node-Namen und WWPNs des Initiators angeben, können diese später, falls erforderlich, entfernt werden.

Befolgen Sie die Anweisungen in der Dokumentation zu Host Utilities, um WWPNs abzurufen und die iSCSI-Node-Namen zu finden, die einem bestimmten Host zugeordnet sind. Verwenden Sie für Hosts, auf denen ESX-Software ausgeführt wird, Virtual Storage Console.

## Vorteile der Nutzung einer virtualisierten SAN-Umgebung

Wenn Sie eine virtualisierte Umgebung mithilfe von Storage Virtual Machines (SVMs) und LIFs erstellen, können Sie Ihre SAN-Umgebung auf alle Nodes im Cluster erweitern.

- Dezentrales Management

  Sie können sich bei jedem Node in der SVM anmelden, um alle Nodes in einem Cluster zu verwalten.

- Verbesserter Datenzugriff

  Mit MPIO und ALUA haben Sie Zugriff auf Ihre Daten über alle aktiven iSCSI oder FC LIFs für die SVM.

- Kontrollierter LUN-Zugriff

  Wenn Sie SLM und Portsätze verwenden, können Sie die Anzahl der LIFs begrenzen, die ein Initiator zum Zugriff auf LUNs verwenden kann.

## Verbesserung der VMware VAAI-Leistung für ESX-Hosts

ONTAP unterstützt bestimmte VMware vStorage APIs for Array Integration (VAAI)-Funktionen, wenn der ESX Host ESX 4.1 oder höher ausführt. Diese Funktionen helfen, die Vorgänge vom ESX Host auf das Storage-System zu verlagern und den Netzwerkdurchsatz zu erhöhen. Der ESX-Host aktiviert die Funktionen automatisch in der richtigen Umgebung.

Die VAAI-Funktion unterstützt die folgenden SCSI-Befehle:

- `EXTENDED_COPY`

  Diese Funktion ermöglicht es dem Host, den Datentransfer zwischen den LUNs oder innerhalb einer LUN zu initiieren, ohne den Host beim Datentransfer zu involvieren. Dies führt zu Einsparungen von ESX CPU-Zyklen und einer Erhöhung des Netzwerkdurchsatzes. Die Funktion für erweiterte Kopien, auch bekannt als „Copy Offload“, wird in Szenarien wie dem Klonen einer Virtual Machine verwendet. Wenn der ESX Host aufgerufen wird, kopiert die Funktion zum Offload die Daten im Storage-System, anstatt über das Host-Netzwerk zu gehen. Beim Copy-Offload werden Daten auf folgende Weise übertragen:

  - Innerhalb einer LUN
  - Zwischen LUNs in einem Volume erstellt
  - Zwischen LUNs auf verschiedenen Volumes innerhalb einer Storage Virtual Machine (SVM)
  - Zwischen LUNs auf verschiedenen SVMs innerhalb eines Clusters Wenn diese Funktion nicht aufgerufen werden kann, verwendet der ESX Host für den Kopiervorgang automatisch die standardmäßigen LESE- und SCHREIBBEFEHLE.

- `WRITE_SAME`

  Mit dieser Funktion wird ein Storage-Array entlastet, bei dem ein wiederholtes Muster – beispielsweise alle Nullen – geschrieben wird. Der ESX Host verwendet diese Funktion bei Vorgängen wie dem Füllen einer Datei ohne Füllen.

- `COMPARE_AND_WRITE`

  Diese Funktion umgeht bestimmte Grenzwerte für die Parallelität des Dateizugriffs, wodurch Vorgänge wie das Booten von Virtual Machines beschleunigt werden.

### Anforderungen für die Nutzung der VAAI Umgebung

Die VAAI-Funktionen sind Teil des ESX-Betriebssystems und werden automatisch vom ESX-Host aufgerufen, wenn Sie die richtige Umgebung eingerichtet haben.

Die Umgebungsanforderungen lauten wie folgt:

- Der ESX Host muss ESX 4.1 oder höher ausführen.
- Das NetApp Storage-System, das den VMware-Datenspeicher hostet, muss ONTAP ausführen.
- (Nur beim Copy Offload) die Quelle und das Ziel des Kopiervorgangs von VMware müssen auf demselben Storage-System innerhalb desselben Clusters gehostet werden.

> Die Copy-Offload-Funktion unterstützt derzeit das Kopieren von Daten zwischen VMware Datenspeichern, die auf verschiedenen Storage-Systemen gehostet werden.

#### Ermitteln, ob VAAI Funktionen von ESX unterstützt werden

Um zu überprüfen, ob das ESX-Betriebssystem die VAAI-Funktionen unterstützt, können Sie den vSphere-Client prüfen oder andere Mittel zum Zugriff auf den Host verwenden. ONTAP unterstützt standardmäßig die SCSI-Befehle.

Sie können die erweiterten Einstellungen Ihres ESX Hosts überprüfen, um festzustellen, ob die VAAI-Funktionen aktiviert sind. Die Tabelle gibt an, welche SCSI-Befehle den ESX-Steuernamen entsprechen.

| SCSI-Befehl | ESX Steuername (VAAI-Funktion) |
|---|---|
| EXTENDED_COPY | `HardwareAcceleratedMove` |
| SCHREIBSCHUTZ | `HardwareAcceleratedInit` |
| COMPARE_AND_WRITE | `HardwareAcceleratedLocking` |

## SAN-Kopierauslagerung

#### Microsoft Offloaded Data Transfer (ODX)

Microsoft Offloaded Data Transfer (ODX), auch bekannt als *Copy Offload*, ermöglicht direkte Datentransfers innerhalb eines Storage-Geräts oder zwischen kompatiblen Storage-Geräten, ohne die Daten über den Host-Computer zu übertragen.

Kopierauslagerungsoperationen von VMware und Microsoft zur Steigerung der Performance und des Netzwerkdurchsatzes Sie müssen Ihr System so konfigurieren, dass es die Anforderungen der Betriebssystemumgebungen von VMware und Windows erfüllt, damit die jeweiligen Funktionen zur Offload von Kopien genutzt werden können.

Bei der Verwendung von VMware- und Microsoft-Copy-Offload in virtualisierten Umgebungen müssen Ihre LUNs aufeinander abgestimmt sein. Nicht ausgerichtete LUNs können die Leistung beeinträchtigen. "Erfahren Sie mehr über nicht ausgerichtete LUNs".

ONTAP unterstützt ODX sowohl für die SMB- als auch für SAN-Protokolle.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk an den Host übertragen. Der Host überträgt die Daten zurück über das Netzwerk an das Ziel. Bei ODX-Dateiübertragung werden die Daten ohne Durchschreiten des Hosts direkt vom Quell- zum Ziel-Volume kopiert.

Da ausgelagerte ODX Kopien direkt zwischen Quelle und Ziel erstellt werden, ergeben sich deutliche Performance-Vorteile, wenn Kopien innerhalb desselben Volumes erstellt werden. Dies umfasst auch schnellere Kopierzeiten für gleiche Volume-Kopien, eine geringere CPU- und Arbeitsspeicherauslastung auf dem Client und eine geringere Netzwerk-I/O-Bandbreitenauslastung. Wenn die Kopien über Volumes verteilt sind, ergeben sich möglicherweise keine nennenswerten Performance-Steigerungen im Vergleich zu hostbasierten Kopien.

Bei SAN-Umgebungen ist ODX nur verfügbar, wenn er sowohl vom Host als auch vom Storage-System unterstützt wird. Client-Computer, die ODX unterstützen und ODX-fähig sind, nutzen die verlagerte Dateiübertragung automatisch und transparent, wenn Dateien verschoben oder kopiert werden. ODX wird unabhängig davon verwendet, ob Sie Dateien per Drag-and-Drop über den Windows Explorer ziehen oder

Befehle zur Befehlszeilendatei kopieren verwenden oder ob eine Client-Applikation Dateikopieanforderungen initiiert.

#### Anforderungen für die Nutzung von ODX

Wenn Sie Vorhaben, ODX für Copy-Offloaded zu verwenden, müssen Sie sich mit den Anforderungen an Volume-Support, Systemanforderungen und Softwarefunktionen vertraut machen.

Zur Nutzung von ODX ist bei Ihrem System Folgendes erforderlich:

- ONTAP

  ODX ist bei unterstützten Versionen von ONTAP automatisch aktiviert.

- Mindestquellenvolumen: 2 GB

  Für eine optimale Leistung sollte das Quellvolumen größer als 260 GB sein.

- ODX-Unterstützung auf dem Windows-Client

  ODX wird unter Windows Server 2012 oder höher und in Windows 8 oder höher unterstützt. Die Interoperabilitäts-Matrix enthält die neuesten Informationen zu unterstützten Windows-Clients.

  "NetApp Interoperabilitäts-Matrix-Tool"

- Applikationssupport für ODX

  Die Applikation, die den Datentransfer durchführt, muss ODX unterstützen. Zu den Applikationsprozessen, die ODX unterstützen, gehören unter anderem:

  - Hyper-V-Verwaltungsvorgänge, wie das Erstellen und Konvertieren virtueller Festplatten (VHDs), das Verwalten von Snapshots und das Kopieren von Dateien zwischen virtuellen Maschinen
  - Betrieb in Windows Explorer
  - Windows PowerShell Kopierbefehle
  - Befehle zum Kopieren von Windows-Befehlen die Microsoft TechNet-Bibliothek enthält weitere Informationen zu unterstützten ODX-Anwendungen auf Windows-Servern und -Clients.
- Bei Verwendung komprimierter Volumes muss die Größe der Komprimierungsgruppen 8 KB sein.

  Die Größe der Komprimierungsgruppen 32.000 wird nicht unterstützt.

ODX funktioniert nicht bei den folgenden Volume-Typen:

- Quellvolumen mit einer Kapazität von weniger als 2 GB
- Schreibgeschützte Volumes
- "FlexCache Volumes"

  ODX wird auf FlexCache-Ursprungs-Volumes unterstützt.

- "Semi-Thick Provisioning Volumes"

#### Besondere Anforderungen an Systemdateien

Sie können ODX-Dateien, die in qtrees gefunden wurden, löschen. Entfernen oder ändern Sie keine anderen ODX-Systemdateien, es sei denn, Sie werden vom technischen Support dazu aufgefordert.

Bei Nutzung der ODX Funktion liegen in jedem Volume des Systems ODX Systemdateien vor. Diese Dateien ermöglichen die zeitpunktgenaue Darstellung der bei der ODX-Übertragung verwendeten Daten. Die folgenden Systemdateien befinden sich auf der Root-Ebene jedes Volumes, das LUNs oder Dateien enthält, auf die Daten ausgelagert wurden:

- `.copy-offload` (Ein verstecktes Verzeichnis)
- `.tokens` (Datei unter dem verborgenen `.copy-offload` Verzeichnis)

Mit dem `copy-offload delete-tokens -path dir_path -node` *`node_name`* Befehl können Sie einen qtree löschen, der eine ODX Datei enthält.

#### Anwendungsfälle für ODX

Bei der Verwendung von ODX auf SVMs sollten Sie sich die Anwendungsfälle bewusst sein, damit Sie unter den Umständen, unter denen ODX Ihnen Performance-Vorteile bietet, die Ergebnisse erkennen können.

Windows-Server und -Clients, die ODX unterstützen, nutzen den Copy-Offload als Standardfunktion zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows-Server oder -Client keine ODX oder eine ODX-Copy-Offload unterstützt, können der Kopier- oder Verladevorgang wieder auf herkömmliche Lese- und Schreibvorgänge für den Kopier- oder Verschiebevorgang zurückgreift.

In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen unterstützt:

- Intra-Volume

  Die Quell- und Zieldateien oder LUNs befinden sich innerhalb desselben Volumes.

- Zwischen Volumes, demselben Node, gleiche SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

  Die Quell- und Zieldateien oder LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Die Daten sind Eigentum derselben SVM.

- Zwischen SVM, demselben Node

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf demselben Node befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Zwischen SVMs, unterschiedliche Nodes

  Die Quell- und Zieldatei bzw. die LUNs befinden sich auf verschiedenen Volumes, die sich auf unterschiedlichen Nodes befinden. Im Besitz der Daten befinden sich unterschiedliche SVMs.

- Cluster zwischen Clustern

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Nodes

über die Cluster befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für SMB.

Es gibt einige weitere spezielle Anwendungsfälle:

- Bei der ONTAP ODX Implementierung können mit ODX Dateien zwischen SMB-Freigaben und virtuellen FC- oder iSCSI-Attached-Laufwerken kopiert werden.

  Mit Windows Explorer, Windows CLI, PowerShell, Hyper-V oder anderen Applikationen, die ODX unterstützen, können Dateien durch eine nahtlose Verschiebung von ODX Kopien zwischen SMB-Freigaben und verbundenen LUNs kopiert oder verschoben werden, sofern sich SMB-Freigaben und LUNs im selben Cluster befinden.

- Hyper-V stellt weitere Anwendungsfälle für den ODX Copy-Offload zur Verfügung:

  - Mithilfe des ODX Copy-Offload-Pass-Through mit Hyper-V können Daten innerhalb oder zwischen VHD-Dateien (Virtual Hard Disk) kopiert oder Daten zwischen zugewiesenen SMB-Shares und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

    Damit können Kopien von Gastbetriebssystemen an den zugrunde liegenden Storage weitergegeben werden.

  - Bei der Erstellung von VHDs mit fester Größe wird ODX zur Initialisierung der Festplatte mit Nullen verwendet, wobei ein bekannter Token mit dem Namen „Zeroed“ verwendet wird.
  - Wenn sich der Quell- und Ziel-Storage auf demselben Cluster befindet, wird eine ODX Copy Offload für die Storage-Migration bei Virtual Machines eingesetzt.

> Um von den Anwendungsfällen für einen ODX Copy-Offload-Pass-Through mit Hyper-V zu profitieren, muss das Gastbetriebssystem ODX unterstützen. Und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die durch Storage (SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten auf dem Gastbetriebssystem unterstützen keine ODX-Pass-Through-Unterstützung.

**Erfahren Sie mehr über NVMe Copy Offload**

NVMe Copy Offload ermöglicht es einem NVMe-Host, Kopiervorgänge von seiner CPU auf die CPU des ONTAP -Speichercontrollers auszulagern. Der Host kann Daten von einem NVMe-Namespace in einen anderen kopieren und dabei seine CPU-Ressourcen für Anwendungsworkloads reservieren.

Nehmen wir beispielsweise an, Sie müssen Ihre Speicherauslastung neu ausbalancieren, um die Leistungsverteilung zu verbessern. Hierfür müssen Sie zehn virtuelle Maschinen (VMs) migrieren, die 45 NVMe-Namespaces mit einer durchschnittlichen Größe von jeweils 500 GB enthalten. Das bedeutet, dass Sie rund 22,5 TB an Daten kopieren müssen. Anstatt für die Datenmigration die eigene CPU zu verwenden, kann der Host NVMe Copy Offload nutzen, um zu vermeiden, dass seine CPU-Ressourcen für Anwendungsworkloads reduziert werden, während die Daten kopiert werden.

#### NVMe-Copy-Offload-Unterstützung und -Einschränkungen

NVMe Copy Offload wird ab ONTAP 9.18.1 unterstützt. ONTAP kann den NVMe-Kopier-Offload nicht initiieren; er muss vom Host unterstützt und initiiert werden.

Für NVMe-Kopier-Offload-Operationen mit ONTAP gelten folgende Einschränkungen:

- Die maximal unterstützte Größe für Kopiervorgänge beträgt 16 MB.
- Daten können nur zwischen NVMe-Namensräumen innerhalb desselben Subsystems migriert werden.
- Daten können nur zwischen Knoten innerhalb desselben HA-Paares migriert werden.

# SAN Administration

## SAN Provisioning

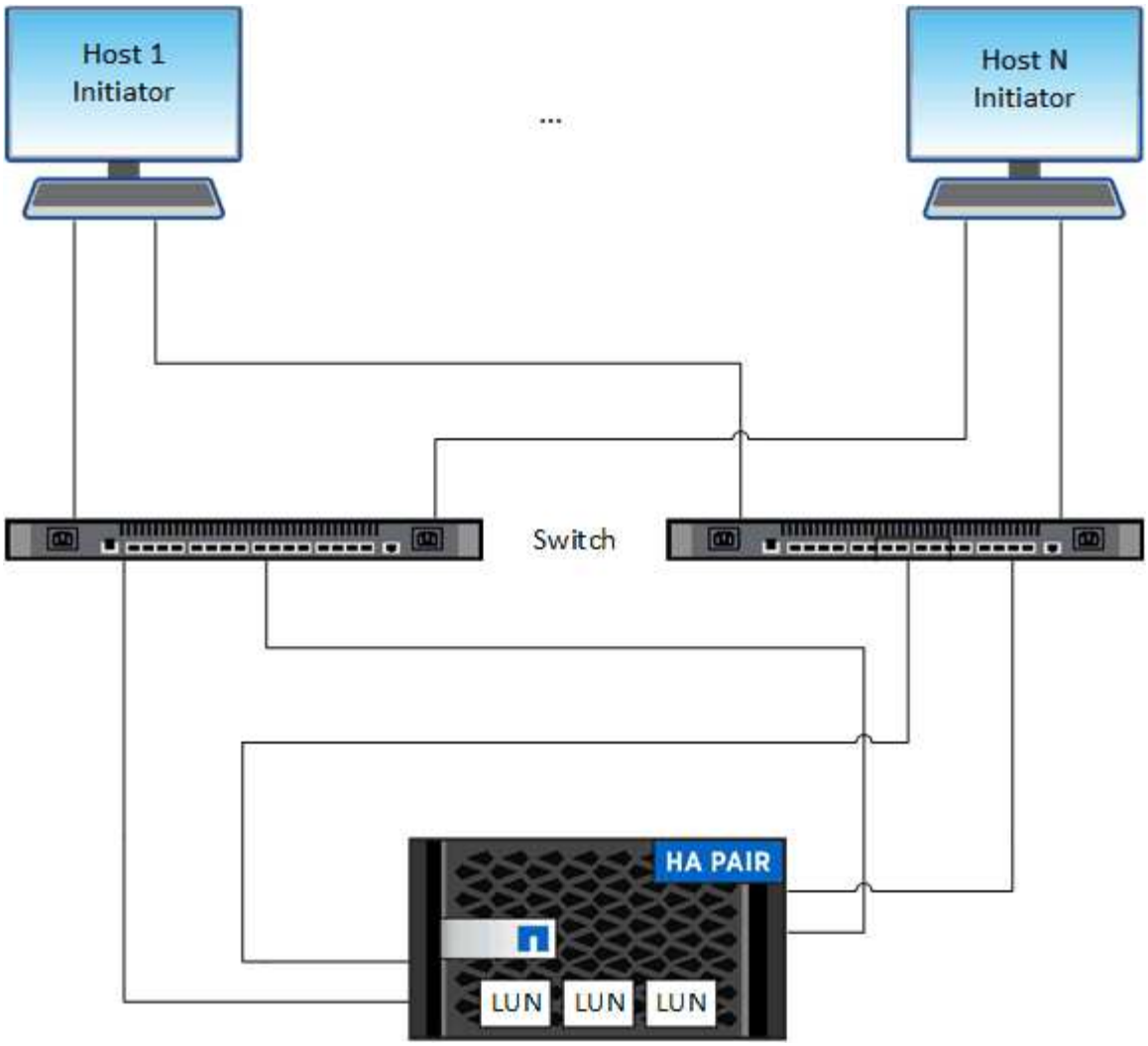
### SAN-Management-Überblick

Der Inhalt in diesem Abschnitt zeigt Ihnen, wie Sie SAN-Umgebungen mit der ONTAP Befehlszeilenschnittstelle (CLI) und System Manager in ONTAP 9.7 und neueren Versionen konfigurieren und managen.

Wenn Sie den klassischen System Manager verwenden (nur in ONTAP 9.7 und älter verfügbar), finden Sie folgende Themen:

- "ISCSI-Protokoll"
- "FC-/FCoE-Protokoll"

Sie können die iSCSI- und FC-Protokolle verwenden, um Storage in einer SAN-Umgebung bereitzustellen.




Bei iSCSI und FC werden Storage-Ziele LUNs (logische Einheiten) genannt und Hosts als Standard-Block-Geräte präsentiert. Sie erstellen LUNs und ordnen sie dann Initiatorgruppen zu. Initiatorgruppen sind Tabellen mit FC-Host-Beispiel- und iSCSI-Host-Node-Namen. Sie steuern, welche Initiatoren auf welche LUNs zugreifen können.

FC-Ziele werden über FC-Switches und Host-seitige Adapter mit dem Netzwerk verbunden und durch World Wide Port Names (WWPNs) identifiziert. ISCSI-Ziele werden über Standard-Ethernet-Netzwerkadapter (NICs), TOE-Karten (TCP Offload Engine) mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bust Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI Qualified Names (IQNs) identifiziert.

#### Finden Sie weitere Informationen

Wenn Sie über ein ASA r2-Speichersystem verfügen (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20), lesen Sie die "Dokumentation zum ASA r2 Storage-System".

### Erfahren Sie mehr über All-Flash-SAN-Array-Konfigurationen

Die NetApp All-Flash SAN-Arrays (ASAs) sind ab ONTAP 9.7 verfügbar. ASAS sind reine All-Flash-SAN-Lösungen, die auf bewährten NetApp AFF Plattformen basieren.

Zu den ASA-Plattformen gehören:

- ASA A150
- ASA A250
- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800

> Ab ONTAP 9.16.0 steht für ASA r2 Systeme (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden zur Verfügung. Wenn Sie über ein ASA r2-System verfügen, lesen Sie die "ASA r2-Systemdokumentation".

ASA Plattformen verwenden symmetrische aktiv/aktiv-Lösung für Multipathing. Alle Pfade sind aktiv/optimiert. Im Falle eines Storage Failovers muss der Host also nicht auf die ALUA-Transition der Failover-Pfade warten, um den I/O wiederaufzunehmen So verkürzt sich die Zeit für den Failover.

#### Richten Sie eine ASA ein

Für All-Flash-SAN-Arrays (ASAs) gilt dasselbe Setup-Verfahren wie für Systeme ohne ASA.

System Manager führt Sie durch die Verfahren, die zum Initialisieren des Clusters, Erstellen einer lokalen Tier, Konfigurieren von Protokollen und Bereitstellen von Speicher für Ihre ASA erforderlich sind.

Erste Schritte mit dem ONTAP-Cluster-Setup.

#### ASA Host-Einstellungen und Dienstprogramme

Die Host-Einstellungen für die Einrichtung von All-Flash-SAN-Arrays (ASAs) sind mit denen für alle anderen SAN-Hosts identisch.

Sie können die "NetApp Host Utilities Software" für Ihre spezifischen Hosts von der Support-Website herunterladen.

#### Möglichkeiten zur Identifizierung eines ASA Systems

Sie können ein ASA System mit System Manager oder mit der ONTAP Befehlszeilenschnittstelle (CLI) identifizieren.

- **Vom System Manager Dashboard**: Klicken Sie auf **Cluster > Übersicht** und wählen Sie dann den Systemknoten aus.

  Die **PERSONALITY** wird als **All-Flash SAN Array** angezeigt.

- **Vom CLI**: Geben Sie den `san config show` Befehl ein.

  Der Mehrwert der All-Flash SAN-Arrays liegt ebenso zurück wie der Wert der ASA Systeme.

  Erfahren Sie mehr über `san config show` in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

- "Technischer Bericht 4968: NetApp All-SAN-Array Data Availability and Integrity"
- "Technischer Bericht 4080 zu NetApp: Best Practices für modernes SAN"

### Konfigurieren Sie Switches für FCoE

Sie müssen Ihre Switches für FCoE konfigurieren, bevor Ihr FC-Service über die vorhandene Ethernet-Infrastruktur ausgeführt werden kann.

**Bevor Sie beginnen**

- Ihre SAN-Konfiguration muss unterstützt werden.

  Weitere Informationen zu unterstützten Konfigurationen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

- Auf Ihrem Storage-System muss ein Unified Target Adapter (UTA) installiert sein.

  Wenn Sie einen UTA2 verwenden, muss dieser auf den `cna` Modus eingestellt sein.

- Ein konvergierter Netzwerkadapter (CNA) muss auf Ihrem Host installiert sein.

**Schritte**

1. Nutzen Sie die Switch-Dokumentation, um die Switches für FCoE zu konfigurieren.
2. Überprüfen Sie, ob die DCB-Einstellungen für jeden Knoten im Cluster korrekt konfiguriert wurden.

   ```
   run -node node1 -command dcb show
   ```

   DCB-Einstellungen werden auf dem Switch konfiguriert. Wenn die Einstellungen nicht korrekt sind, konsultieren Sie die Switch-Dokumentation.

3. Überprüfen Sie, ob die FCoE-Anmeldung funktioniert, wenn der FC-Zielport-Online-Status lautet `true`.

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   Wenn der FC-Zielport-Online-Status lautet `false`, lesen Sie in der Switch-Dokumentation nach.

**Verwandte Informationen**

- "NetApp Interoperabilitäts-Matrix-Tool"
- "Technischer Bericht von NetApp 3800: End-to-End-Implementierungsleitfaden für Fibre Channel over Ethernet (FCoE"
- "Konfigurationsleitfäden für Cisco MDS 9000 NX-OS und SAN-OS Software"
- "Brocade Produkte"

### Systemanforderungen

Beim Einrichten von LUNs wird eine LUN erstellt, eine Initiatorgruppe erstellt und die LUN der Initiatorgruppe zugeordnet. Das System muss bestimmte Voraussetzungen erfüllen, bevor Sie Ihre LUNs einrichten können.

- Die Interoperabilitäts-Matrix muss Ihre SAN-Konfiguration wie unterstützt auflisten.
- Ihre SAN-Umgebung muss die in "NetApp Hardware Universe" für Ihre Version der ONTAP-Software angegebenen Konfigurationsgrenzwerte für SAN-Host und -Controller erfüllen.
- Eine unterstützte Version von Host Utilities muss installiert sein.

  Die Dokumentation zu Host Utilities enthält weitere Informationen.

- Sie müssen auf dem LUN-Eigentümer-Node und dem HA-Partner des entsprechenden Node SAN LIFs haben.

### Verwandte Informationen

- "NetApp Interoperabilitäts-Matrix-Tool"
- "ONTAP SAN-Host-Konfiguration"
- "Technischer Bericht 4017 zu Fibre Channel SAN Best Practices"

### Was muss ich wissen, bevor Sie eine LUN erstellen

Bevor Sie mit der Einrichtung der LUNs auf dem Cluster beginnen, müssen Sie diese LUN-Richtlinien überprüfen.

#### Warum die tatsächlichen LUN-Größen geringfügig variieren

Sie sollten Folgendes bezüglich der Größe Ihrer LUNs kennen.

- Wenn Sie eine LUN erstellen, kann die tatsächliche Größe der LUN abhängig vom OS-Typ der LUN geringfügig variieren. Der LUN-OS-Typ kann nach dem Erstellen der LUN nicht geändert werden.
- Wenn Sie eine LUN mit der maximalen LUN-Größe erstellen, beachten Sie, dass die tatsächliche Größe der LUN ein wenig geringer sein kann. ONTAP rundet das Limit auf etwas weniger ab.
- Die Metadaten für jede LUN benötigen ca. 64 KB Speicherplatz im Aggregat, das enthalten ist. Wenn Sie eine LUN erstellen, müssen Sie sicherstellen, dass das zugehörige Aggregat über ausreichend Platz für die Metadaten der LUN verfügt. Wenn das Aggregat nicht genügend Speicherplatz für die Metadaten der LUN enthält, können einige Hosts möglicherweise nicht auf die LUN zugreifen.

#### Richtlinien für das Zuweisen von LUN-IDs

In der Regel beginnt die Standard-LUN-ID mit 0 und wird jeder zusätzlichen zugeordneten LUN in Schritten von 1 zugewiesen. Der Host ordnet die LUN-ID dem Standort- und Pfadnamen der LUN zu. Der Bereich gültiger LUN-ID-Nummern hängt vom Host ab. Ausführliche Informationen finden Sie in der Dokumentation Ihrer Host Utilities.

#### Richtlinien zum Zuordnen von LUNs zu Initiatorgruppen

- Sie können eine LUN nur einmal einer Initiatorgruppe zuordnen.
- Als Best Practice sollten Sie eine LUN über die Initiatorgruppe nur einem bestimmten Initiator zuordnen.

- Sie können einen einzelnen Initiator mehreren Initiatorgruppen hinzufügen, der Initiator kann jedoch nur einer LUN zugeordnet werden.
- Sie können nicht dieselbe LUN-ID für zwei LUNs verwenden, die derselben Initiatorgruppe zugeordnet sind.
- Sie sollten denselben Protokolltyp für Initiatorgruppen und Port-Sets verwenden.

#### Überprüfen Sie Ihre FC- oder iSCSI-Protokolllizenz und fügen Sie sie hinzu

Bevor Sie den Blockzugriff für eine Storage Virtual Machine (SVM) mit FC oder iSCSI aktivieren können, ist eine Lizenz erforderlich. Die FC- und iSCSI-Lizenzen sind in enthalten"ONTAP One".

**Beispiel 1. Schritte**

**System Manager**

Wenn Sie keinen ONTAP besitzen, überprüfen Sie Ihre FC- oder iSCSI-Lizenz mit dem ONTAP System Manager (9.7 und höher) und fügen Sie sie hinzu.

1. Wählen Sie im System Manager **Cluster > Einstellungen > Lizenzen** aus
2. Wenn die Lizenz nicht aufgeführt ist, wählen Sie den Lizenzschlüssel aus + Add , und geben Sie ihn ein.
3. Wählen Sie **Hinzufügen**.

**CLI**

Wenn Sie keinen ONTAP One haben, überprüfen Sie Ihre FC- oder iSCSI-Lizenz und fügen Sie sie mit der ONTAP-CLI hinzu.

1. Vergewissern Sie sich, dass Sie eine aktive Lizenz für FC oder iSCSI besitzen.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- --------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Wenn Sie keine aktive Lizenz für FC oder iSCSI besitzen, fügen Sie Ihren Lizenzcode hinzu.

```
license add -license-code <your_license_code>
```

**SAN-Storage bereitstellen**

# Durch dieses Verfahren werden neue LUNs auf einer vorhandenen Storage-VM erstellt, die bereits das FC- oder iSCSI-Protokoll konfiguriert ist.

**Über diese Aufgabe**

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um Ihren Speicher bereitzustellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Wenn Sie eine neue Storage-VM erstellen und das FC- oder iSCSI-Protokoll konfigurieren müssen, finden Sie unter "Konfigurieren Sie eine SVM für FC" oder "Konfigurieren Sie eine SVM für iSCSI".

Wenn die FC-Lizenz nicht aktiviert ist, werden die LIFs und SVMs online angezeigt, der Betriebsstatus ist jedoch nicht aktiv.

LUNs werden Ihrem Host als Festplattengeräte angezeigt.

Während der LUN-Erstellung ist der asymmetrische Zugriff auf logische Einheiten (ALUA) immer aktiviert. Sie können die ALUA-Einstellung nicht ändern.

Zum Hosten der Initiatoren müssen Sie das einzelne Initiator-Zoning für alle FC-LIFs in der SVM verwenden.

Ab ONTAP 9.8 ist bei der Bereitstellung von Storage QoS standardmäßig aktiviert. Sie können die QoS während der Bereitstellung oder zu einem späteren Zeitpunkt deaktivieren oder eine benutzerdefinierte QoS-Richtlinie auswählen.

**Beispiel 2. Schritte**

**System Manager**

Erstellung von LUNs zur Bereitstellung von Storage für einen SAN-Host mithilfe des FC- oder iSCSI-Protokolls mit ONTAP System Manager (9.7 und höher)

Informationen zum Abschließen dieser Aufgabe mit System Manager Classic (verfügbar mit Version 9.7 und früher) finden Sie unter "ISCSI-Konfiguration für Red hat Enterprise Linux"

**Schritte**

1. Installieren Sie das entsprechende "SAN Host Utilities" auf Ihrem Host.
2. Klicken Sie im System Manager auf **Storage > LUNs** und dann auf **Hinzufügen**.
3. Geben Sie die zum Erstellen der LUN erforderlichen Informationen ein.
4. Je nach Ihrer Version von ONTAP können Sie auf **Weitere Optionen** klicken, um eine der folgenden Optionen zu tun.

| Option | Verfügbar ab |
|---|---|
| • Weisen Sie LUNs anstelle des übergeordneten Volume eine QoS-Richtlinie zu<br>◦ **Mehr Optionen > Speicherung und Optimierung**<br>◦ Wählen Sie **Performance Service Level**.<br>◦ Um die QoS-Richtlinie auf einzelne LUNs anstelle des gesamten Volumes anzuwenden, wählen Sie **Diese Performance-Limits für jede LUN** anwenden.<br>Standardmäßig werden Performance-Limits auf Volume-Ebene angewendet. | ONTAP 9.10.1 |
| • Erstellen Sie eine neue Initiatorgruppe unter Verwendung vorhandener Initiatorgruppen<br>◦ **Mehr Optionen > HOST-INFORMATIONEN**<br>◦ Wählen Sie **Neue Initiatorgruppe unter Verwendung vorhandener Initiatorgruppen** aus.<br>ⓘ Der OS-Typ für eine Initiatorgruppe mit anderen Initiatorgruppen kann nach ihrer Erstellung nicht mehr geändert werden. | ONTAP 9.9.1 |
| • Fügen Sie einer Initiatorgruppe oder Host-Initiator eine Beschreibung hinzu<br>Die Beschreibung dient als Alias für die Initiatorgruppe oder den Host-Initiator.<br>◦ **Mehr Optionen > HOST-INFORMATIONEN** | ONTAP 9.9.1 |

| | |
|---|---|
| • Erstellen Sie Ihre LUN auf einem vorhandenen Volume<br>Standardmäßig wird eine neue LUN in einem neuen Volume erstellt.<br>◦ **Mehr Optionen > LUNs hinzufügen**<br>◦ Wählen Sie **Gruppen bezogene LUNs** aus. | ONTAP 9.9.1 |
| • Deaktivieren Sie QoS oder wählen Sie eine individuelle QoS-Richtlinie aus<br>◦ **Mehr Optionen > Speicherung und Optimierung**<br>◦ Wählen Sie **Performance Service Level**.<br>ⓘ Wenn Sie in ONTAP 9.9.1 und höher eine benutzerdefinierte QoS-Richtlinie auswählen, können Sie auch eine manuelle Platzierung auf einer bestimmten lokalen Tier auswählen. | ONTAP 9,8 |

5. Zone der FC-Switches im Hinblick auf FC um WWPN. Verwenden Sie eine Zone pro Initiator und schließen Sie alle Ziel-Ports in jeder Zone an.
6. Erkennen Sie LUNs auf Ihrem Host.

   Für VMware vSphere verwenden Sie die Virtual Storage Console (VSC), um Ihre LUNs zu erkennen und zu initialisieren.

7. Initialisieren Sie die LUNs und erstellen Sie optional Dateisysteme.
8. Vergewissern Sie sich, dass der Host Daten auf der LUN schreiben und lesen kann.

**CLI**

Erstellen Sie LUNs, um Storage für einen SAN-Host mithilfe des FC- oder iSCSI-Protokolls mit der ONTAP-CLI bereitzustellen.

1. Überprüfen Sie, ob Sie über eine Lizenz für FC oder iSCSI verfügen.

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. Wenn Sie keine Lizenz für FC oder iSCSI haben, verwenden Sie den `license add` Befehl.

```
license add -license-code <your_license_code>
```

3. Aktivieren Sie Ihren Protokollservice auf der SVM:

   **Für iSCSI:**

```
vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
```

   ◦ Für FC:*

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. Erstellen Sie zwei LIFs für die SVMs an jedem Node:

```
network interface create -vserver <svm_name> -lif <lif_name> -role
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
<port_name> -address <ip_address> -netmask <netmask>
```

   NetApp unterstützt für jede SVM, die Daten bereitstellt, mindestens eine iSCSI- oder FC-LIF pro Node. Jedoch sind für Redundanz zwei LIFS pro Node erforderlich. Für iSCSI wird empfohlen, mindestens zwei LIFs pro Node in separaten Ethernet-Netzwerken zu konfigurieren.

5. Überprüfen Sie, ob Ihre LIFs erstellt wurden und ob ihr Betriebsstatus lautet `online`:

```
network interface show -vserver <svm_name> <lif_name>
```

6. Erstellen Sie Ihre LUNs:

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

   Der LUN-Name darf nicht mehr als 255 Zeichen enthalten und darf keine Leerzeichen enthalten.

   Die NVFAIL-Option ist automatisch aktiviert, wenn eine LUN in einem Volume erstellt wird.

7. Erstellen Sie Ihre Initiatorgruppen:

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. Ordnen Sie Ihre LUNs Initiatorgruppen zu:

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Vergewissern Sie sich, dass Ihre LUNs ordnungsgemäß konfiguriert sind:

```
lun show -vserver <svm_name>
```

10. Optional, "Erstellen Sie einen Portsatz und binden Sie es an eine Initiatorgruppe".
11. Befolgen Sie die Schritte in der Host-Dokumentation, um den Blockzugriff auf Ihren spezifischen Hosts zu ermöglichen.
12. Schließen Sie die FC- oder iSCSI-Zuordnung mithilfe der Host Utilities ab und ermitteln Sie die LUNs auf dem Host.

**Verwandte Informationen**

- "SAN-Administration – Übersicht"
- "ONTAP SAN-Host-Konfiguration"
- "Zeigen Sie SAN-Initiatorgruppen in System Manager an und verwalten Sie sie"
- "Technischer Bericht 4017 zu Fibre Channel SAN Best Practices"

## NVMe Provisionierung

### NVMe Übersicht

Sie können das Non-Volatile Memory Express-Protokoll (NVMe) verwenden, um Storage in einer SAN-Umgebung bereitzustellen. Das NVMe-Protokoll ist für die Performance von Solid-State-Storage optimiert.

Für NVMe werden Storage-Ziele als Namespaces bezeichnet. Ein NVMe Namespace ist eine Menge nicht-flüchtiger Storage, der in logische Blöcke formatiert und einem Host als Standardblock-Gerät präsentiert werden kann. Sie erstellen Namespaces und Subsysteme und ordnen die Namespaces den Subsystemen zu, ähnlich der Art und Weise, wie LUNs bereitgestellt und Initiatorgruppen für FC und iSCSI zugeordnet werden.

NVMe-Ziele sind über eine standardmäßige FC-Infrastruktur mit FC-Switches oder einer standardmäßigen TCP-Infrastruktur mit Ethernet-Switches und Host-seitigen Adaptern mit dem Netzwerk verbunden.

Support für NVMe ist abhängig von Ihrer Version von ONTAP. Weitere Informationen finden Sie unter "Unterstützung und Einschränkungen von NVMe" .

#### NVMe ist das

Das NVMe-Protokoll (Nonvolatile Memory Express) ist ein Transportprotokoll, das für den Zugriff auf nicht-flüchtige Storage-Medien verwendet wird.

NVMe over Fabrics (NVMeoF) ist eine spezifikationsdefinierte Erweiterung auf NVMe, die eine NVMe-basierte Kommunikation über andere Verbindungen als PCIe ermöglicht. Über diese Schnittstelle können externe

Speichergehäuse mit einem Server verbunden werden.

NVMe wurde entwickelt, um einen effizienten Zugriff auf Storage-Geräte zu bieten, die mit nichtflüchtigem Speicher ausgelegt sind – von Flash-Technologie bis hin zu persistenten Speichertechnologien mit höherer Performance. Es bestehen somit nicht dieselben Einschränkungen wie Storage-Protokolle für Festplatten. Flash und Solid State Devices (SSDs) sind ein Typ von nichtflüchtigem Speicher (NVM). NVM ist eine Speicherart, bei der der Inhalt bei einem Stromausfall erhalten bleibt. NVMe ist eine Möglichkeit für den Zugriff auf den Speicher.

Zu den Vorteilen von NVMe zählen höhere Geschwindigkeiten, Produktivität, Durchsatz und die Kapazität für den Datentransfer. Zu den spezifischen Merkmalen zählen:

- NVMe ist für bis zu 64 Warteschlangen konzipiert.

  Jede Warteschlange kann wiederum bis zu 64 gleichzeitige Befehle haben.

- NVMe wird von diversen Hardware- und Softwareanbietern unterstützt
- NMVe arbeitet produktiver mit Flash-Technologien, wodurch kürzere Reaktionszeiten ermöglicht werden
- NVMe ermöglicht mehrere Datenanfragen jeder „`reQuest`“, die an die SSD gesendet werden.

  NVMe benötigt weniger Zeit, um ein „`reQuest`“ zu decodieren und erfordert keine Gewindesperrung in einem Multithread-Programm.

- NVMe unterstützt die Funktionalität, die einen Engpass auf der CPU-Ebene verhindert und eine massive Skalierbarkeit bei Erweiterung der Systeme ermöglicht.

#### Allgemeines zu NVMe Namespaces

Ein NVMe Namespace ist eine Menge nichtflüchtiger Speicher (NVM), der in logische Blöcke formatiert werden kann. Namespaces werden verwendet, wenn eine Storage Virtual Machine mit dem NVMe-Protokoll konfiguriert ist und eine äquivalente von LUNs für FC- und iSCSI-Protokolle sind.

Es werden mindestens ein Namespaces bereitgestellt und mit einem NVMe-Host verbunden. Jeder Namespace kann unterschiedliche Blockgrößen unterstützen.

Das NVMe-Protokoll ermöglicht den Zugriff auf Namespaces über mehrere Controller. Durch die Verwendung von NVMe-Treibern, die auf den meisten Betriebssystemen unterstützt werden, werden Namespaces für Solid State Drives als Standard-Block-Geräte angezeigt, auf denen Filesysteme und Applikationen ohne Änderungen bereitgestellt werden können.

Eine Namespace-ID (NSID) ist eine Kennung, die von einem Controller für den Zugriff auf einen Namespace verwendet wird. Wenn Sie die NSID für einen Host oder eine Hostgruppe festlegen, konfigurieren Sie auch den Zugriff auf ein Volume durch einen Host. Ein logischer Block kann immer nur einer einzelnen Host-Gruppe zugeordnet werden, und eine bestimmte Host-Gruppe verfügt nicht über doppelte NSIDs.

#### Über NVMe-Subsysteme

Ein NVMe-Subsystem umfasst einen oder mehrere NVMe-Controller, Namespaces, NVM-Subsystem-Ports, ein NVM-Storage-Medium und eine Schnittstelle zwischen dem Controller und dem NVM-Storage-Medium. Wenn Sie einen NVMe Namespace erstellen, ist er standardmäßig nicht einem Subsystem zugeordnet. Sie können es auch als neues oder vorhandenes Subsystem zuordnen.

**Verwandte Informationen**

- Lernen Sie"NVMe-Storage wird bereitgestellt", auf ASA-, AFF- und FAS-Systemen

- Lernen Sie "Zuordnen eines NVMe-Namespace zu einem Subsystem"auf ASA AFF und FAS Systemen.
- "Konfigurieren Sie SAN-Hosts und Cloud-Clients"
- Erfahren Sie, wie Sie "Bereitstellung von SAN-Storage" auf ASA r2-Storage-Systemen (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) vertraut sind.

#### Lizenzanforderungen für NVMe

Ab ONTAP 9.5 ist für die Unterstützung von NVMe eine Lizenz erforderlich. Wenn NVMe in ONTAP 9.4 aktiviert ist, erhält der Erwerb der Lizenz nach dem Upgrade auf ONTAP 9.5 eine 90-tägige Gnadenfrist.

Sie können die Lizenz mit dem folgenden Befehl aktivieren:

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

#### Konfiguration, Support und Einschränkungen von NVMe

Ab ONTAP 9.4 "Non-Volatile Memory Express (NVMe)"ist das Protokoll für SAN-Umgebungen verfügbar. FC-NVMe verwendet dasselbe physische Setup- und Zoning-Verfahren wie herkömmliche FC-Netzwerke, ermöglicht aber höhere Bandbreite, höhere IOPS-Werte und eine geringere Latenz als FC-SCSI.

Der NVMe-Support und die Einschränkungen hängen von Ihrer Version von ONTAP, Ihrer Plattform und Ihrer Konfiguration ab. Weitere Informationen zu Ihrer spezifischen Konfiguration finden Sie im "NetApp Interoperabilitäts-Matrix-Tool". Unterstützte Grenzwerte finden Sie unter "Hardware Universe".

> Die maximale Anzahl an Knoten pro Cluster ist in Hardware Universe unter **Unterstützte Plattformmischung** verfügbar.

##### Konfiguration

- NVMe Konfiguration kann über eine einzelne Fabric oder mehrere Fabric eingerichtet werden.
- Sie sollten eine Management-LIF für jede SVM konfigurieren, die SAN unterstützt.
- Die Verwendung heterogener FC Switch Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches.

  Spezifische Ausnahmen sind auf der aufgeführt"NetApp Interoperabilitäts-Matrix-Tool".

- Kaskadierung, partielles Mesh, volles Mesh, Core-Edge und Director Fabrics sind branchenübliche Methoden, FC Switches mit einem Fabric zu verbinden. Alle werden unterstützt.

  Eine Fabric kann aus einem oder mehreren Switches bestehen und die Storage-Controller mit mehreren Switches verbunden werden.

##### Funktionen

Die folgenden NVMe Funktionen werden basierend auf Ihrer Version von ONTAP unterstützt.

| Beginnt mit ONTAP… | NVMe unterstützt |
|---|---|

| | |
|---|---|
| 9.17.1 | • SnapMirror Active Sync NVMe/FC- und NVMe/TCP-Hostzugriff für VMware-Workloads. |
| 9.15.1 | • MetroCluster IP-Konfigurationen mit vier Nodes auf NVMe/TCP |
| 9.14.1 | • Festlegen der Host-Priorität am Subsystem (Service auf Host-Ebene) |
| 9.12.1 | • MetroCluster IP-Konfigurationen mit vier Nodes auf NVMe/FC<br>• MetroCluster-Konfigurationen werden für Front-End-NVMe-Netzwerke vor ONTAP 9.12.1 nicht unterstützt.<br>• MetroCluster-Konfigurationen werden auf NVMe/TCP nicht unterstützt. |
| 9.10.1 | Ändern der Größe eines Namespace |
| 9.9.1 | • Namespaces und LUNs werden auf demselben Volume gleichzeitig ausgeführt |
| 9,8 | • Koexistenz von Protokollen<br>SCSI-, NAS- und NVMe-Protokolle können auf derselben Storage Virtual Machine (SVM) vorhanden sein.<br>Vor ONTAP 9.8 kann NVMe als einziges Protokoll auf der SVM verwendet werden. |
| 9,6 | • 512-Byte-Blöcke und 4096-Byte-Blöcke für Namespaces<br>Der Standardwert ist 4096. 512 sollte nur verwendet werden, wenn das Host-Betriebssystem keine 4096-Byte-Blöcke unterstützt.<br>• Volume-Verschiebung mit zugeordneten Namespaces |
| 9,5 | • Failover/Giveback für Multipath HA-Paare |

**Protokolle**

Die folgenden NVMe-Protokolle werden unterstützt.

| Protokoll | Beginnt mit ONTAP… | Zulässig von… |
|---|---|---|

| | | |
|---|---|---|
| TCP | 9.10.1 | Standard |
| FC | 9,4 | Standard |

Ab ONTAP 9.8 können SCSI-, NAS- und NVMe-Protokolle auf derselben Storage Virtual Machine (SVM) konfiguriert werden. In ONTAP 9.7 und älteren Versionen kann NVMe das einzige Protokoll auf der SVM sein.

#### Namespaces

Bei der Arbeit mit NVMe-Namespaces sollten Sie Folgendes beachten:

- Bei ONTAP 9.15.1 und älteren Versionen unterstützt ONTAP zur Speicherplatzrückgewinnung den Befehl für das NVMe Dataset Management (allocate) mit NVMe.
- Sie können SnapRestore nicht verwenden, um einen Namespace aus einer LUN wiederherzustellen, oder umgekehrt.
- Die Platzgarantie für Namespaces ist identisch mit der Speicherplatzgarantie für das enthaltende Volume.
- Bei einem Volume-Übergang von Data ONTAP in 7-Mode können Sie keinen Namespace erstellen.
- Namespaces bieten keine Unterstützung für Folgendes:
  - Umbenennungen
  - Verschiebung zwischen Volumes
  - Kopie zwischen Volumes
  - Copy-on-Demand

#### Weitere Einschränkungen

**Die folgenden ONTAP Funktionen werden von NVMe Konfigurationen nicht unterstützt:**

- Virtual Storage Console
- Ständige Reservierungen

**Folgendes gilt nur für Nodes mit ONTAP 9.4:**

- NVMe LIFs und Namespaces müssen auf demselben Node gehostet werden.
- Der NVMe-Service muss vor Erstellung der NVMe-LIF erstellt werden.

#### Verwandte Informationen

"Best Practices für modernes SAN"

### Konfigurieren Sie eine Storage-VM für NVMe

Wenn Sie das NVMe-Protokoll auf einem Node verwenden möchten, müssen Sie Ihre SVM speziell für NVMe konfigurieren.

#### Bevor Sie beginnen

Ihre FC- oder Ethernet-Adapter müssen NVMe unterstützen. Unterstützte Adapter sind in der aufgeführt "NetApp Hardware Universe".

**Beispiel 3. Schritte**

**System Manager**

Konfigurieren Sie eine Storage-VM für NVMe mit ONTAP System Manager (9.7 und höher).

| Und NVMe auf einer neuen Storage-VM konfigurieren | Um NVMe für eine vorhandene Storage-VM zu konfigurieren |
|---|---|
| 1. Klicken Sie im System Manager auf **Storage > Storage VMs** und dann auf **Hinzufügen**.<br>2. Geben Sie einen Namen für die Storage-VM ein.<br>3. Wählen Sie * NVMe* für das **Access Protocol** aus.<br>4. Wählen Sie **NVMe/FC aktivieren** oder **NVMe/TCP aktivieren** und **Speichern**. | 1. Klicken Sie im System Manager auf **Storage > Storage VMs**.<br>2. Klicken Sie auf die zu konfigurierende Speicher-VM.<br>3. Klicken Sie auf die Registerkarte **Settings** und dann auf ⚙ neben dem NVMe-Protokoll.<br>4. Wählen Sie **NVMe/FC aktivieren** oder **NVMe/TCP aktivieren** und **Speichern**. |

**CLI**

Konfigurieren Sie eine Storage VM für NVMe mit der ONTAP CLI.

1. Wenn Sie keine vorhandene SVM verwenden möchten, erstellen Sie eine SVM:

   ```
   vserver create -vserver <SVM_name>
   ```

   a. Vergewissern Sie sich, dass die SVM erstellt wurde:

      ```
      vserver show
      ```

2. Vergewissern Sie sich, dass im Cluster NVMe- oder TCP-fähige Adapter installiert sind:

   Für NVMe:

   ```
   network fcp adapter show -data-protocols-supported fc-nvme
   ```

   Für TCP:

   ```
   network port show
   ```

   Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

3. Wenn Sie ONTAP 9.7 oder älter nutzen, entfernen Sie alle Protokolle aus der SVM:

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

Ab ONTAP 9.8 müssen beim Hinzufügen von NVMe keine anderen Protokolle entfernt werden.

4. Fügen Sie das NVMe-Protokoll der SVM hinzu:

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. Falls ONTAP 9.7 oder eine frühere Version ausgeführt wird, überprüfen Sie, ob NVMe das einzige Protokoll auf der SVM ist:

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe sollte das einzige Protokoll sein, das in der `allowed protocols` Spalte angezeigt wird.

6. Entwicklung des NVMe-Service:

```
vserver nvme create -vserver <SVM_name>
```

7. Vergewissern Sie sich, dass der NVMe-Service erstellt wurde:

```
vserver nvme show -vserver <SVM_name>
```

Die `Administrative Status` der SVM sollte als aufgelistet werden `up`. Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".

8. NVMe/FC-LIF erstellen:
   - Für ONTAP 9.9.1 oder früher, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - Für ONTAP 9.10.1 oder höher, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- Für ONTAP 9.10.1 oder höher, TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. Erstellung einer NVMe/FC-LIF auf dem HA-Partner-Node:
   - Für ONTAP 9.9.1 oder früher, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - Für ONTAP 9.10.1 oder höher, FC:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

   - Für ONTAP 9.10.1 oder höher, TCP:

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. Überprüfen Sie, ob die NVMe/FC-LIFs erstellt wurden:

```
network interface show -vserver <SVM_name>
```

11. Erstellen Sie ein Volume auf demselben Node wie das LIF:

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

Wenn eine Warnmeldung zur Richtlinie für die automatische Effizienz angezeigt wird, kann sie sicher ignoriert werden.

**NVMe-Storage wird bereitgestellt**

## Verwenden Sie diese Schritte, um Namespaces zu erstellen und Storage für alle von NVMe unterstützten Hosts in einer vorhandenen Storage-VM bereitzustellen.

**Über diese Aufgabe**

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um Ihren Speicher bereitzustellen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

Ab ONTAP 9.8 ist bei der Bereitstellung von Storage QoS standardmäßig aktiviert. Sie können die QoS deaktivieren oder während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt eine individuelle QoS-Richtlinie auswählen.

**Bevor Sie beginnen**

Ihre Storage VM muss für NVME konfiguriert sein, und Ihr FC- oder TCP-Transport sollte bereits eingerichtet sein.

**System Manager**

Unter Verwendung von ONTAP System Manager (9.7 und höher) lassen sich Namespaces erstellen, um Storage über das NVMe-Protokoll bereitzustellen.

**Schritte**

1. Klicken Sie im System Manager auf **Storage > NVMe Namesaces** und dann auf **Add**.

   Wenn Sie ein neues Subsystem erstellen möchten, klicken Sie auf **Weitere Optionen**.

2. Wenn Sie ONTAP 9.8 oder höher verwenden und QoS deaktivieren oder eine benutzerdefinierte QoS-Richtlinie auswählen möchten, klicken Sie auf **Mehr Optionen** und wählen Sie dann unter **Speicher und Optimierung** die Option **Performance Service Level**.
3. Zonen der FC-Switches anhand des WWPN. Verwenden Sie eine Zone pro Initiator und schließen Sie alle Ziel-Ports in jeder Zone an.
4. Entdecken Sie auf Ihrem Host die neuen Namespaces.
5. Initialisieren Sie den Namespace und formatieren Sie ihn mit einem Dateisystem.
6. Vergewissern Sie sich, dass Ihr Host Daten im Namespace schreiben und lesen kann.

**CLI**

Erstellen Sie über die ONTAP CLI Namespaces, um Storage über das NVMe-Protokoll bereitzustellen.

Dabei wird ein NVMe Namespace und -Subsystem für eine vorhandene Storage-VM erstellt, die bereits für das NVMe-Protokoll konfiguriert wurde. Anschließend wird der Namespace dem Subsystem zugeordnet, um den Datenzugriff über das Host-System zu ermöglichen.

Informationen zum Konfigurieren der Storage-VM für NVMe finden Sie unter "Konfigurieren Sie eine SVM für NVMe".

**Schritte**

1. Vergewissern Sie sich, dass die SVM für NVMe konfiguriert ist:

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` Sollte unter der `allowed-protocols` Spalte angezeigt werden.

2. NVMe-Namespace erstellen:

   Das Volume, auf das Sie mit dem Parameter verweisen, muss bereits vorhanden sein. Andernfalls müssen Sie vor dem Ausführen dieses Befehls ein Volume `-path` erstellen.

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. NVMe-Subsystem erstellen:

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

Bei dem NVMe-Subsystem-Namen wird die Groß-/Kleinschreibung berücksichtigt. Er muss 1 bis 96 Zeichen enthalten. Sonderzeichen sind zulässig.

4. Überprüfen Sie, ob das Subsystem erstellt wurde:

```
vserver nvme subsystem show -vserver <svm_name>
```

Das `nvme` Subsystem sollte unter der `Subsystem` Spalte angezeigt werden.

5. Beziehen Sie das NQN vom Host.
6. Fügen Sie den Host-NQN zum Subsystem hinzu:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. Den Namespace dem Subsystem zuordnen:

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

Ein Namespace kann nur einem einzelnen Subsystem zugeordnet werden.

8. Vergewissern Sie sich, dass der Namespace dem Subsystem zugeordnet ist:

```
vserver nvme namespace show -vserver <svm_name> -instance
```

Das Subsystem sollte als aufgeführt werden `Attached subsystem`.

**Zuordnen eines NVMe Namespace zu einem Subsystem**

## Die Zuordnung eines NVMe-Namespace zu einem Subsystem ermöglicht den Datenzugriff von Ihrem Host. Sie können einen NVMe-Namespace zu einem Subsystem zuordnen, wenn Sie Storage bereitstellen, oder Sie können ihn nach der Bereitstellung des Storage durchführen.

Ab ONTAP 9.17.1 können Sie bei Verwendung einer SnapMirror Active Sync-Konfiguration eine SVM als proximalen virtuellen Server zu einem Host hinzufügen, während Sie den Host einem NVMe-Subsystem hinzufügen. Aktiv optimierte Pfade für einen Namespace in einem NVMe-Subsystem werden nur von der als proximalen virtuellen Server konfigurierten SVM auf einem Host veröffentlicht.

Ab ONTAP 9.14.1 können Sie die Ressourcenzuweisung für bestimmte Hosts priorisieren. Wenn ein Host dem NVMe-Subsystem hinzugefügt wird, erhält er standardmäßig eine regelmäßige Priorität. Mithilfe der ONTAP Befehlszeilenschnittstelle (CLI) kann die Standardpriorität manuell von „Normal“ auf „hoch“ geändert werden. Hosts, denen eine hohe Priorität zugewiesen ist, werden eine größere Anzahl von I/O-Warteschlangen und eine größere Warteschlangentiefe zugewiesen.

Wenn Sie einem Host, der einem Subsystem in ONTAP 9.13.1 oder früher hinzugefügt wurde, eine hohe Priorität zuweisen möchten, können Sie Ändern Sie die Host-Priorität.

**Bevor Sie beginnen**

Der Namespace und das Subsystem sollten bereits erstellt werden. Wenn Sie einen Namespace und ein Subsystem erstellen müssen, siehe "NVMe-Storage wird bereitgestellt".

#### Zuordnen eines NVMe-Namespace

**Schritte**

1. Beziehen Sie das NQN vom Host.
2. Fügen Sie den Host-NQN zum Subsystem hinzu:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

   Wenn Sie die Standardpriorität des Hosts von Normal auf hoch ändern möchten, verwenden Sie die `-priority high` Option. Diese Option ist ab ONTAP 9.14.1 verfügbar. Erfahren Sie mehr über `vserver nvme subsystem host add` in der "ONTAP-Befehlsreferenz".

   Wenn Sie eine SVM als `proximal-vserver` a zu einem Host hinzufügen möchten, während Sie den Host zu einem NVMe-Subsystem in einer SnapMirror mit aktiver Synchronisierung hinzufügen, können Sie die Option `-proximal-vservers` verwenden. Diese Option ist ab ONTAP 9.17.1 verfügbar. können die Quell- oder Ziel-SVM oder beide hinzufügen. Die SVM, in der Sie diesen Befehl ausführen, ist die Standard-SVM.

3. Den Namespace dem Subsystem zuordnen:

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

   Ein Namespace kann nur einem einzelnen Subsystem zugeordnet werden. Erfahren Sie mehr über `vserver nvme subsystem map add` in der "ONTAP-Befehlsreferenz".

4. Vergewissern Sie sich, dass der Namespace dem Subsystem zugeordnet ist:

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

   Das Subsystem sollte als aufgeführt werden `Attached subsystem`. Erfahren Sie mehr über `vserver nvme namespace show` in der "ONTAP-Befehlsreferenz".

# LUNs managen

### LUN-QoS-Richtliniengruppe bearbeiten

Ab ONTAP 9.10.1 können Sie mit System Manager Quality of Service (QoS)-Richtlinien auf mehreren LUNs gleichzeitig zuweisen oder entfernen.

> Wird die QoS-Richtlinie auf Volume-Ebene zugewiesen, muss sie auf Volume-Ebene geändert werden. Sie können die QoS-Richtlinie nur auf der LUN-Ebene bearbeiten, wenn sie ursprünglich auf LUN-Ebene zugewiesen wurde.

**Schritte**

1. Klicken Sie im System Manager auf **Storage > LUNs**.
2. Wählen Sie die LUN oder LUNs aus, die Sie bearbeiten möchten.

   Wenn Sie mehrere LUNs gleichzeitig bearbeiten, müssen die LUNs derselben Storage Virtual Machine (SVM) angehören. Wenn Sie LUNs auswählen, die nicht zur gleichen SVM gehören, wird die Option zum Bearbeiten der QoS-Richtliniengruppe nicht angezeigt.

3. Klicken Sie auf **Mehr** und wählen Sie **QoS Policy Group bearbeiten**.

### Konvertieren einer LUN in einen Namespace

Ab ONTAP 9.11.1 können Sie mithilfe der ONTAP CLI eine vorhandene LUN in einen NVMe Namespace konvertieren.

**Bevor Sie beginnen**

- Die angegebene LUN sollte einer Initiatorgruppe keine Zuordnungen enthalten.
- LUN sollte sich nicht in einem für MetroCluster konfigurierten SVM oder in einer SnapMirror-Active-Sync-Beziehung befinden.
- Die LUN sollte kein Protokollendpunkt oder an einen Protokollendpunkt gebunden sein.
- Die LUN sollte kein Präfix und/oder Suffix aufweisen.
- LUN sollte nicht Teil eines Snapshots oder auf der Zielseite der SnapMirror Beziehung als schreibgeschützte LUN sein.

**Schritt**

1. Konvertieren einer LUN in einen NVMe-Namespace:

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

### Versetzen einer LUN in den Offline-Modus

Ab ONTAP 9.10.1 können Sie mit System Manager LUNs in den Offline-Modus versetzen. Vor ONTAP 9.10.1 müssen Sie die ONTAP-CLI verwenden, um LUNs in den Offline-Modus zu versetzen.

**System Manager**

**Schritte**

1. Klicken Sie im System Manager auf **Storage>LUNs**.
2. Versetzen einer einzelnen oder mehrerer LUNs in den Offline-Modus

| Wenn Sie… wollen | Do this… |
|---|---|
| Versetzen einer einzelnen LUN in den Offline-Modus | Klicken Sie neben dem LUN-Namen auf ⋮ und wählen Sie **Offline nehmen** aus. |
| Versetzen Sie mehrere LUNs in den Offline-Modus | 1. Wählen Sie die LUNs aus, die Sie in den Offline-Modus versetzen möchten.<br>2. Klicken Sie auf **Mehr** und wählen Sie **Offline nehmen**. |

**CLI**

Sie können eine LUN gleichzeitig nur offline schalten, wenn Sie die CLI verwenden.

**Schritt**

1. Versetzen Sie die LUN in den Offline-Modus:

```
lun offline <lun_name> -vserver <SVM_name>
```

### Die Größe einer LUN in ONTAP ändern

Sie können eine LUN vergrößern oder verkleinern.

**Über diese Aufgabe**

Dieses Verfahren gilt für FAS-, AFF- und ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, folgen Sie "Diesen Schritten ausführen" um die Größe einer Speichereinheit zu erhöhen. ASA r2 Systeme bieten eine vereinfachte ONTAP-Erfahrung speziell für reine SAN-Kunden.

ⓘ Die Größe von Solaris LUNs kann nicht geändert werden.

#### Vergrößern einer LUN

Die Größe, in der Sie Ihre LUN vergrößern können, hängt von Ihrer Version von ONTAP ab.

| ONTAP-Version | Maximale LUN-Größe |
|---|---|
| ONTAP 9.12.1P2 und höher | 128 TB für AFF-, FAS- und ASA-Plattformen |

| | |
|---|---|
| ONTAP 9.8 und höher | • 128 TB für All-Flash SAN-Array (ASA)-Plattformen<br>• 16 TB für nicht-ASA-Plattformen |
| 9.5. ONTAP 9.6, 9.7 | 16TB |
| ONTAP 9.4 oder früher | 10 mal die ursprüngliche LUN-Größe, aber nicht größer als 16 TB, was die maximale LUN-Größe ist. Wenn Sie beispielsweise eine 100-GB-LUN erstellen, können Sie sie nur auf 1,000 GB erweitern. Die tatsächliche maximale Größe der LUN beträgt möglicherweise nicht genau 16 TB. ONTAP rundet das Limit auf etwas weniger ab. |

Sie müssen die LUN nicht in den Offline-Modus versetzen, um die Größe zu erhöhen. Nachdem Sie die Größe jedoch erhöht haben, müssen Sie die LUN auf dem Host erneut scannen, damit der Host die Größenänderung erkennen kann.

**Beispiel 4. Schritte**

**System Manager**

Vergrößern Sie die Größe einer LUN mit ONTAP System Manager (9.7 und höher).

1. Klicken Sie im System Manager auf **Storage > LUNs**.
2. Klicken Sie auf ⋮ und wählen Sie **Bearbeiten**.
3. Erhöhen Sie unter **Speicherung und Optimierung** die Größe der LUN und **Speichern**.

**CLI**

Vergrößern Sie die Größe einer LUN mit der ONTAP-CLI.

1. Vergrößern Sie die LUN:

   ```
   lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
   -size <lun_size>
   ```

   Erfahren Sie mehr über `lun resize` in der "ONTAP-Befehlsreferenz".

2. Überprüfen Sie die erweiterte LUN-Größe:

   ```
   lun show -vserver <SVM_name>
   ```

Die ONTAP-Vorgänge runden die tatsächliche maximale Größe der LUN ab, sodass sie etwas kleiner als der erwartete Wert ist. Außerdem kann die tatsächliche LUN-Größe je nach OS-Typ der LUN leicht variieren. Führen Sie im erweiterten Modus die folgenden Befehle aus, um den Wert der genauen Größe zu ermitteln:

```
set -unit B
```

`lun show -fields max-resize-size -volume volume_name -lun lun_name`

+
Erfahren Sie mehr über `lun show` in der "ONTAP-Befehlsreferenz".

1. Scannen Sie die LUN auf dem Host erneut.
2. Befolgen Sie die Host-Dokumentation, um die neu erstellte LUN-Größe für das Host-Dateisystem sichtbar zu machen.

#### Verkleinern Sie die Größe einer LUN

Bevor Sie die Größe einer LUN verkleinern, muss der Host die Blöcke mit den LUN-Daten an die Grenze der kleineren LUN-Größe migrieren. Sie sollten ein Tool wie SnapCenter verwenden, um sicherzustellen, dass die LUN ordnungsgemäß verkleinert wird, ohne Blöcke mit LUN-Daten zu kürzen. Es wird nicht empfohlen, die Größe Ihrer LUN manuell zu verringern.

Nach der Verkleinerung der LUN wird der Initiator automatisch von ONTAP benachrichtigt, dass die LUN-Größe gesunken ist. Auf Ihrem Host sind jedoch möglicherweise zusätzliche Schritte erforderlich, damit der Host die neue LUN-Größe erkennt. Informationen zur Reduzierung der Größe der Host-Dateistruktur finden Sie in der Hostdokumentation.

### Verschieben einer LUN

Sie können eine LUN zwar innerhalb einer Storage Virtual Machine (SVM) über Volumes hinweg verschieben, eine LUN jedoch nicht über SVMs hinweg. LUNs, die über Volumes innerhalb einer SVM verschoben werden, werden sofort und ohne Konnektivitätsverlust verschoben.

#### Bevor Sie beginnen

Wenn die LUN die selektive LUN-Zuordnung (SLM) verwendet, sollten Sie "Ändern Sie die Liste der SLM Reporting-Nodes"den Ziel-Node und dessen HA-Partner einbeziehen, bevor Sie die LUN verschieben.

#### Über diese Aufgabe

Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung und Data-Compaction bleiben während der LUN-Verschiebung erhalten. Sie müssen nach Abschluss der LUN-Verschiebung erneut angewendet werden.

Die Datensicherung durch Snapshots erfolgt auf Volume-Ebene. Wenn Sie eine LUN verschieben, fällt sie daher unter das Datensicherungsschema des Ziel-Volume. Wenn Sie keine Snapshots für das Zielvolume eingerichtet haben, werden keine Snapshots der LUN erstellt. Außerdem bleiben alle Snapshots der LUN im ursprünglichen Volume, bis diese Snapshots gelöscht werden.

Sie können eine LUN nicht auf folgende Volumes verschieben:

- Einem SnapMirror Ziel-Volume
- Das SVM-Root-Volume

Sie können die folgenden LUNs-Typen nicht verschieben:

- Eine LUN, die aus einer Datei erstellt wurde
- Eine LUN mit NV-Fehler-Status

- Eine LUN, die sich in einer Load-Sharing-Beziehung befindet
- Eine Protokoll-Endpunktklasse LUN

Wenn die Knoten in einem Cluster unterschiedliche ONTAP Versionen verwenden, können Sie eine LUN nur dann zwischen Volumes auf verschiedenen Knoten verschieben, wenn die Quelle eine höhere Version als das Ziel verwendet. Wenn beispielsweise der Knoten des Quellvolumes ONTAP 9.15.1 und der Knoten des Zielvolumes ONTAP 9.16.1 verwendet, können Sie die LUN nicht verschieben. Sie können LUNs zwischen Volumes auf Knoten verschieben, die dieselbe ONTAP Version verwenden.

Bei Solaris os_TYPE LUNs, die 1 TB oder größer sind, kann es während der LUN-Verschiebung auf dem Host zu einer Zeitüberschreitung kommen. Bei diesem LUN-Typ sollten Sie die Mounten der LUN aufheben, bevor Sie die Verschiebung initiieren.

**Beispiel 5. Schritte**

**System Manager**

Verschieben Sie eine LUN mit ONTAP System Manager (9.7 und höher).

Ab ONTAP 9.10.1 können Sie mit System Manager ein neues Volume erstellen, wenn Sie eine einzelne LUN verschieben. In ONTAP 9.8 und 9.9 muss das Volume, auf das Sie Ihre LUN verschieben, vorhanden sein, bevor Sie mit der LUN-Verschiebung beginnen.

Schritte

1. Klicken Sie im System Manager auf **Storage>LUNs**.
2. Klicken Sie mit der rechten Maustaste auf die LUN, die Sie verschieben möchten, klicken Sie dann auf ⋮ und wählen Sie **LUN verschieben**.

   Wählen Sie im ONTAP 9.10.1 aus, um die LUN in **ein vorhandenes Volume** oder in ein **neues Volume** zu verschieben.

   Wenn Sie sich für die Erstellung eines neuen Volumes entscheiden, geben Sie die Volume-Spezifikationen an.
3. Klicken Sie Auf **Verschieben**.

**CLI**

Verschieben Sie eine LUN mit der ONTAP CLI.

1. Verschieben der LUN:

   ```
   lun move start
   ```

   Die LUN ist während einer sehr kurzen Zeit sowohl auf dem Ursprungs- als auch auf dem Ziel-Volume sichtbar. Dies ist zu erwarten und wird nach Abschluss des Umschlusses gelöst.
2. Verfolgen Sie den Status der Verschiebung, und überprüfen Sie den erfolgreichen Abschluss:

   ```
   lun move show
   ```

**Verwandte Informationen**

- "Selektive LUN-Zuordnung"

## LUNs löschen

Sie können eine LUN aus einer Storage Virtual Machine (SVM) löschen, wenn Sie die LUN nicht mehr benötigen.

**Bevor Sie beginnen**

Die Zuordnung der LUN zur Initiatorgruppe muss aufgehoben werden, bevor Sie sie löschen können.

**Schritte**

1. Vergewissern Sie sich, dass die LUN von der Applikation oder dem Host nicht verwendet wird.
2. LUN-Zuordnung zu der Initiatorgruppe aufheben:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. LUN löschen:

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. Vergewissern Sie sich, dass Sie die LUN gelöscht haben:

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

**Was muss vor dem Kopieren von LUNs wissen**

## Vor dem Kopieren einer LUN sollten Sie bestimmte Dinge beachten.

Clusteradministratoren können eine LUN mit dem `lun copy` Befehl über Storage Virtual Machines (SVMs) innerhalb des Clusters hinweg kopieren. `vserver peer create`Bevor ein LUN-Kopiervorgang zwischen den SVMs durchgeführt wird, müssen die Clusteradministratoren die SVM-Peering-Beziehung (Storage Virtual Machine) mithilfe des Befehls einrichten. Für einen SIS-Klon muss im Quell-Volume genügend Platz vorhanden sein.

LUNs in Snapshots können als Quell-LUNs für den Befehl verwendet werden `lun copy`. Wenn Sie eine LUN mit dem `lun copy` Befehl kopieren, ist die LUN-Kopie sofort für Lese- und Schreibzugriff verfügbar. Die Quell-LUN wird durch die Erstellung einer LUN-Kopie nicht geändert. Sowohl die Quell-LUN als auch die LUN-Kopie sind als eindeutige LUNs mit unterschiedlichen LUN-Seriennummern vorhanden. Änderungen an der Quell-LUN werden nicht in der LUN-Kopie widergespiegelt und Änderungen, die an der LUN-Kopie vorgenommen werden, werden nicht in der Quell-LUN wiedergegeben. Die LUN-Zuordnung der Quell-LUN wird nicht auf die neue LUN kopiert. Die LUN Kopie muss zugeordnet werden.

Die Datensicherung durch Snapshots erfolgt auf Volume-Ebene. Wenn Sie eine LUN auf ein anderes Volume als das Volume der Quell-LUN kopieren, fällt die Ziel-LUN unter das Datensicherungsschema des Ziel-Volume. Wenn Sie keine Snapshots für das Zielvolume eingerichtet haben, werden keine Snapshots der LUN-Kopie erstellt.

Das Kopieren von LUNs ist ein unterbrechungsfreier Vorgang.

Sie können die folgenden LUNs-Typen nicht kopieren:

- Eine LUN, die aus einer Datei erstellt wurde
- Eine LUN im Status „NV-Fehler“
- Eine LUN, die sich in einer Load-Sharing-Beziehung befindet
- Eine Protokoll-Endpunktklasse LUN

Erfahren Sie mehr über `lun copy` in der "ONTAP-Befehlsreferenz".

#### Untersuchen Sie den konfigurierten und genutzten Speicherplatz einer LUN

Durch das Wissen über den konfigurierten Speicherplatz und den tatsächlich für Ihre LUNs genutzten Speicherplatz können Sie feststellen, wie viel Speicherplatz bei der Rückgewinnung von Speicherplatz, die Menge des reservierten Speicherplatzes, der Daten enthält, sowie die konfigurierte Gesamtgröße im Vergleich zur tatsächlichen Größe einer LUN ermittelt werden kann.

**Schritt**

1. Zeigen Sie den konfigurierten Speicherplatz gegenüber dem tatsächlich für eine LUN verwendeten Speicherplatz an:

   ```
   lun show
   ```

   Im folgenden Beispiel wird der konfigurierte Speicherplatz im Vergleich zum tatsächlich von den LUNs in der vs3 Storage Virtual Machine (SVM) genutzten Speicherplatz gezeigt:

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- ------------------      ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

   Erfahren Sie mehr über `lun show` in der "ONTAP-Befehlsreferenz".

#### Steuerung und Monitoring der I/O-Performance für LUNs mithilfe von Storage-QoS

Sie können die Input/Output-Performance (I/O) an LUNs steuern, indem Sie Storage QoS-Richtliniengruppen LUNs zuweisen. Sie können die I/O-Performance steuern, um sicherzustellen, dass Workloads bestimmte Performance-Ziele erreichen oder einen Workload drosseln, der sich negativ auf andere Workloads auswirkt.

**Über diese Aufgabe**

Richtliniengruppen setzen eine maximale Durchsatzbegrenzung ein (z. B. 100 MB/s). Sie können eine Richtliniengruppe erstellen, ohne den maximalen Durchsatz anzugeben. Dadurch können Sie die Performance überwachen, bevor Sie den Workload steuern.

Sie können auch Storage Virtual Machines (SVMs) mit FlexVol Volumes und LUNs Richtliniengruppen zuweisen.

Beachten Sie die folgenden Anforderungen beim Zuweisen einer LUN zu einer Richtliniengruppe:

- Die LUN muss von der SVM enthalten sein, der die Richtliniengruppe angehört.

  Sie geben beim Erstellen der Richtliniengruppe die SVM an.

- Wenn Sie eine LUN einer Richtliniengruppe zuweisen, können Sie die LUN, die Volume oder SVM enthält, nicht einer Richtliniengruppe zuweisen.

Weitere Informationen zur Verwendung von Storage QoS finden Sie im "Referenz für Systemadministration".

**Schritte**

1. `qos policy-group create`Erstellen Sie mit dem Befehl eine Richtliniengruppe.

   Erfahren Sie mehr über `qos policy-group create` in der "ONTAP-Befehlsreferenz".

2. `lun create` `lun modify` `-qos-policy-group`Weisen Sie eine LUN mit dem Befehl oder dem Befehl mit dem Parameter einer Richtliniengruppe zu.

   Erfahren Sie mehr über `lun` in der "ONTAP-Befehlsreferenz".

3. `qos statistics`Zeigen Sie mit den Befehlen Performance-Daten an.
4. Verwenden Sie bei Bedarf den `qos policy-group modify` Befehl, um das maximale Durchsatzlimit der Richtliniengruppe anzupassen.

   Erfahren Sie mehr über `qos policy-group modify` in der "ONTAP-Befehlsreferenz".

#### Verfügbare Tools für eine effektive Überwachung Ihrer LUNs

Es stehen Tools zur Verfügung, mit denen Sie Ihre LUNs effektiv überwachen und Speicherplatzbelegung vermeiden können.

- Active IQ Unified Manager ist ein kostenloses Tool, mit dem Sie den gesamten Storage über alle Cluster Ihrer Umgebung hinweg managen können.
- System Manager ist eine in ONTAP integrierte grafische Benutzeroberfläche, mit der Sie Storage-Anforderungen manuell auf Cluster-Ebene managen können.
- OnCommand Insight bietet eine zentrale Ansicht Ihrer Storage-Infrastruktur und ermöglicht so das Einrichten von automatischem Monitoring, Warnungen und Berichten, wenn der Speicherplatz für die LUNs, Volumes und Aggregate knapp wird.

#### Funktionen und Einschränkungen der migrierte LUNs

In einer SAN-Umgebung ist während der Transition eines 7-Mode Volumes zu ONTAP eine Serviceunterbrechung erforderlich. Sie müssen Ihre Hosts herunterfahren, um den Übergang abzuschließen. Nach dem Umstieg müssen Sie Ihre Host-Konfigurationen aktualisieren, bevor Sie mit der Bereitstellung von Daten in ONTAP beginnen können

Sie müssen ein Wartungsfenster planen, währenddessen Sie Ihre Hosts herunterfahren und die Transition

abschließen können.

LUNs, die von Data ONTAP im 7-Mode zu ONTAP migriert wurden, weisen bestimmte Funktionen und Einschränkungen auf, die die Art und Weise des Managements der LUNs beeinträchtigen.

Bei ummigrierte LUNs können Sie Folgendes tun:

- Zeigen Sie die LUN mit dem `lun show` Befehl an
- Mit dem `transition 7-mode show` Befehl können Sie das Inventar der vom 7-Mode-Volume übergangsierten LUNs anzeigen
- Stellen Sie ein Volume aus einem 7-Mode Snapshot wieder her

  Durch Wiederherstellen des Volumes werden alle im Snapshot erfassten LUNs wiederhergestellt
- Stellen Sie eine einzelne LUN aus einem 7-Mode-Snapshot mithilfe des Befehls wieder her `snapshot restore-file`
- Erstellen Sie einen Klon einer LUN in einem 7-Mode Snapshot
- Stellen Sie einen Block-Bereich von einer in einem 7-Mode Snapshot erfassten LUN wieder her
- Erstellen Sie eine FlexClone des Volumes mit einem 7-Mode Snapshot

Bei migrierte LUNs können Sie Folgendes nicht ausführen:

- Zugriff auf Snapshot-gestützte LUN-Klone, die im Volume erfasst wurden

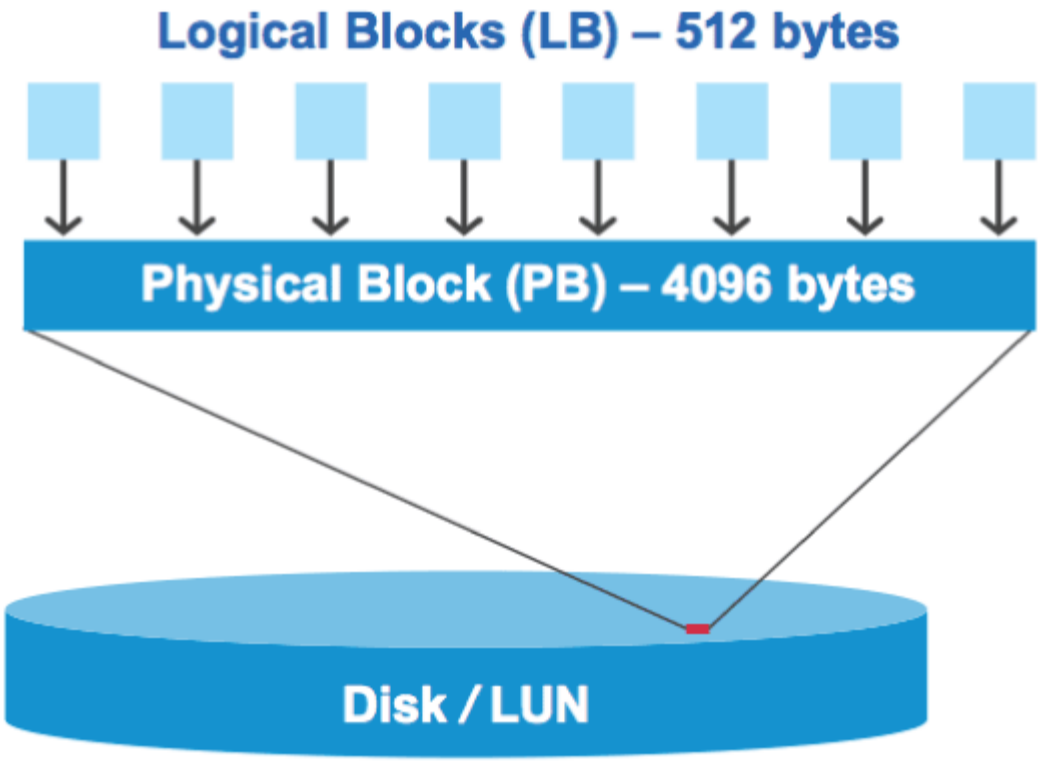
**Verwandte Informationen**

- "Kopienbasierte Transition"
- "lun anzeigen"

### I/O-Fehlausrichtungen auf korrekt ausgerichtete LUNs Übersicht

ONTAP meldet möglicherweise I/O-Fehlausrichtungen auf ordnungsgemäß ausgerichtete LUNs. Im Allgemeinen lassen sich diese Falschausrichtung von Warnungen außer Acht, wenn Sie sicher sind, dass Ihre LUN ordnungsgemäß bereitgestellt ist und Ihre Partitionierungstabelle korrekt ist.

Sowohl LUNs als auch Festplatten bieten Storage als Blöcke. Da die Blockgröße für Festplatten auf dem Host 512 Byte ist, stellen LUNs Blöcke dieser Größe dem Host zur Verfügung, während tatsächlich größere 4-KB-Blöcke zum Speichern von Daten genutzt werden. Der vom Host verwendete 512-Byte-Datenblock wird als logischer Block bezeichnet. Der von der LUN zum Speichern von Daten verwendete 4-KB-Datenblock wird als physischer Block bezeichnet. Das heißt, es gibt acht logische 512-Byte-Blöcke in jedem physischen 4-KB-Block.




Das Host-Betriebssystem kann einen I/O-Vorgang zum Lesen oder Schreiben an einem beliebigen logischen Block starten. I/O-Vorgänge gelten nur als ausgerichtet, wenn sie am ersten logischen Block im physischen Block beginnen. Wenn ein I/O-Vorgang auf einem logischen Block beginnt, der nicht unbedingt der Anfang eines physischen Blocks ist, gilt der I/O-Vorgang als falsch ausgerichtet. ONTAP erkennt Falschausrichtungen automatisch und meldet sie innerhalb der LUN. Dies bedeutet jedoch nicht zwangsläufig, dass die LUN auch falsch ausgerichtet ist. Es kann möglich sein, dass falsch ausgerichtete I/O-Vorgänge auf ordnungsgemäß ausgerichteten LUNs gemeldet werden.

Wenn Sie weitere Untersuchungen benötigen, lesen Sie die"NetApp Knowledge Base: Wie identifiziere ich nicht ausgerichtete E/A auf LUNs?"

Weitere Informationen zu Tools zur Korrektur von Ausrichtungsproblemen finden Sie in der folgenden Dokumentation: +

- "Windows Unified Host Utilities 7.1"
- "Bereitstellung der SAN-Storage-Dokumentation"

#### I/O-Ausrichtung mit LUN-OS-Typen

Bei ONTAP 9 7 oder früher sollten Sie den empfohlenen ONTAP LUN- `ostype`Wert verwenden, der Ihrem Betriebssystem am ehesten entspricht, um eine I/O-Ausrichtung mit Ihrem OS-Partitionierungsschema zu erreichen.

Das vom Host-Betriebssystem verwendete Partitionsschema ist ein wesentlicher Faktor für die I/O-Fehlausrichtungen. Einige ONTAP-LUN- `ostype`Werte verwenden einen speziellen Offset, der als „`PREFIX“ bekannt ist, um die Ausrichtung des vom Host-Betriebssystem verwendeten Standardpartitionierungsschemas zu ermöglichen.

In manchen Fällen ist möglicherweise eine individuelle Partitionstabelle erforderlich, um die I/O-Ausrichtung zu erreichen. Bei `ostype` Werten mit einem Wert von „`PREFIX`“ größer als `0` kann eine benutzerdefinierte Partition jedoch falsch ausgerichtete I/O-Vorgänge erzeugen

Weitere Informationen zu LUNs, die in ONTAP 9.7 oder früher bereitgestellt werden, finden Sie im"NetApp Knowledge Base: So identifizieren Sie nicht ausgerichtete IO auf LUNs" .

Standardmäßig verfügen neue LUNs, die in ONTAP 9.8 oder höher bereitgestellt werden, für alle LUN-OS-Typen über ein Präfix und eine Suffix-Größe von null. Die I/O-Vorgänge sollten standardmäßig an dem unterstützten Host-Betriebssystem ausgerichtet sein.

#### Besondere Überlegungen zur I/O-Ausrichtung für Linux

Linux-Distributionen bieten eine Vielzahl von Möglichkeiten zur Verwendung einer LUN, einschließlich als Rohgeräte für Datenbanken, verschiedene Volume-Manager und Dateisysteme. Bei Verwendung als Raw Device bzw. als physisches Volume in einem logischen Volume sind keine Partitionen auf einer LUN erforderlich.

Wenn bei RHEL 5 und älteren sowie SLES 10 und älteren Versionen die LUN ohne Volume Manager verwendet wird, sollten Sie die LUN partitionieren, um eine Partition zu haben, die bei einem ausgerichteten Offset beginnt, einem Sektor, der ein oder mehrere acht logische Blöcke ist.

#### Spezielle Überlegungen zur I/O-Ausrichtung für Solaris LUNs

Sie müssen verschiedene Faktoren berücksichtigen, wenn Sie bestimmen, ob Sie den `solaris` ostype oder den `solaris_efi` ostype verwenden sollten.

Weitere "Installations- und Administrationsanleitung für Solaris Host Utilities" Informationen finden Sie im.

#### Der Bericht für ESX Boot LUNs wurde falsch ausgerichtet

LUNs, die als ESX Boot LUNs genutzt werden, werden von ONTAP in der Regel als falsch ausgerichtet gemeldet. ESX erstellt mehrere Partitionen auf der Boot LUN, was eine Ausrichtung sehr schwierig macht. Falsch ausgerichtete ESX Boot LUNs stellen in der Regel kein Performance-Problem dar, da die Gesamtzahl an falsch ausgerichteten I/O klein ist. Vorausgesetzt, dass die LUN korrekt mit der VMware bereitgestellt wurde `ostype`, ist keine Aktion erforderlich.

#### Verwandte Informationen

"Koordinierung von Gast-VM-Filesystem-Partition/Festplatten für VMware vSphere, andere virtuelle Umgebungen und NetApp Storage-Systeme"

### Möglichkeiten zur Behebung von Problemen, wenn LUNs offline geschaltet werden

Wenn kein Speicherplatz für Schreibvorgänge verfügbar ist, gehen LUNs in den Offline-Modus, um die Datenintegrität zu wahren. LUNs können nicht mehr über genügend Speicherplatz verfügen und aus verschiedenen Gründen offline gehen, und es gibt mehrere Möglichkeiten, das Problem zu beheben.

| Wenn der… | Sie können… |
| --- | --- |
| Aggregat ist voll | • Fügen Sie weitere Festplatten hinzu.<br>• Mit dem `volume modify` Befehl können Sie ein Volume mit verfügbarem Speicherplatz verkleinern.<br>• Wenn bei Ihnen Speicherplatzzusagen Volumes `none` mit verfügbarem Speicherplatz vorhanden sind, ändern Sie die Volume Platzgarantie mit dem `volume modify` Befehl in. |
| Das Volume ist voll, aber im Aggregat, das enthalten ist, ist Platz verfügbar | • Für Speicherplatzzusagen-Volumes verwenden Sie den `volume modify` Befehl, um die Größe des Volumes zu erhöhen.<br>• Bei Thin Provisioning Volumes können Sie mit dem `volume modify` Befehl die maximale Größe eines Volumes erhöhen.<br>Wenn Volume Autogrow nicht aktiviert ist, verwenden Sie, `volume modify -autogrow -mode` um es zu aktivieren.<br>• Löschen Sie Snapshots manuell mit dem `volume snapshot delete` Befehl oder mit dem Befehl. `volume snapshot autodelete modify` |

**Verwandte Informationen**

"Festplatten- und lokales Tier-Management (Aggregate)"

"Logisches Storage-Management"

**Fehlerbehebung bei iSCSI-LUNs, die auf dem Host nicht sichtbar sind**

Die iSCSI-LUNs werden als lokale Festplatten für den Host angezeigt. Wenn die LUNs des Speichersystems nicht als Laufwerke auf dem Host verfügbar sind, sollten Sie die Konfigurationseinstellungen überprüfen.

| Konfigurationseinstellung | Was zu tun ist |
| --- | --- |
| Verkabelung | Vergewissern Sie sich, dass die Kabel zwischen Host und Speichersystem ordnungsgemäß angeschlossen sind. |

| Konfigurationseinstellung | Was zu tun ist |
|---|---|
| Netzwerk-Konnektivität | Vergewissern Sie sich, dass TCP/IP-Konnektivität zwischen dem Host und dem Speichersystem vorhanden ist.<br>• Über die Befehlszeile des Speichersystems, Ping der Host-Schnittstellen, die für iSCSI verwendet werden:<br>`ping –node node_name -destination host_ip_address_for_iSCSI`<br>• Über die Host-Befehlszeile, Ping der Speichersystemschnittstellen, die für iSCSI verwendet werden:<br>`ping –node node_name -destination host_ip_address_for_iSCSI` |
| Systemanforderungen | Vergewissern Sie sich, dass die Komponenten Ihrer Konfiguration qualifiziert sind. Überprüfen Sie außerdem, ob Sie über die richtige Service Pack-Stufe für das Host-Betriebssystem, die Initiatorversion, die ONTAP-Version und andere Systemanforderungen verfügen. Die Interoperabilitäts-Matrix enthält die aktuellsten Systemanforderungen. |
| Jumbo-Frames | Wenn Sie Jumbo Frames in Ihrer Konfiguration verwenden, überprüfen Sie, ob Jumbo Frames auf allen Geräten im Netzwerkpfad aktiviert sind: Host Ethernet NIC, das Speichersystem und alle Switches. |
| ISCSI-Servicestatus | Vergewissern Sie sich, dass der iSCSI-Service lizenziert und auf dem Speichersystem gestartet ist. |
| Anmeldung des Initiators | Vergewissern Sie sich, dass der Initiator beim Speichersystem angemeldet ist. Wenn in der `iscsi initiator show` Ausgabe des Befehls angezeigt wird, dass keine Initiatoren angemeldet sind, überprüfen Sie die Initiatorkonfiguration auf dem Host. Vergewissern Sie sich außerdem, dass das Storage-System als Ziel des Initiators konfiguriert ist. |
| ISCSI-Node-Namen (IQNs) | Vergewissern Sie sich, dass Sie die richtigen Initiator-Node-Namen in der iGroup-Konfiguration verwenden. Auf dem Host können Sie den Namen des Initiator-Node mit den Initiator-Tools und -Befehlen anzeigen. Die in der Initiatorgruppe und auf dem Host konfigurierten Initiator-Node-Namen müssen mit übereinstimmen. |

| Konfigurationseinstellung | Was zu tun ist |
|---|---|
| LUN-Zuordnungen | Vergewissern Sie sich, dass die LUNs einer Initiatorgruppe zugeordnet sind. An der Storage-System-Konsole können Sie einen der folgenden Befehle verwenden:<br>• `lun mapping show` Zeigt alle LUNs und die Initiatorgruppen an, denen sie zugeordnet sind.<br>• `lun mapping show -igroup` Zeigt die LUNs an, die einer bestimmten Initiatorgruppe zugeordnet sind. |
| ISCSI LIFs aktivieren | Vergewissern Sie sich, dass die logischen iSCSI-Schnittstellen aktiviert sind. |

**Verwandte Informationen**

- "NetApp Interoperabilitäts-Matrix-Tool"
- "lun-Zuordnung wird angezeigt"

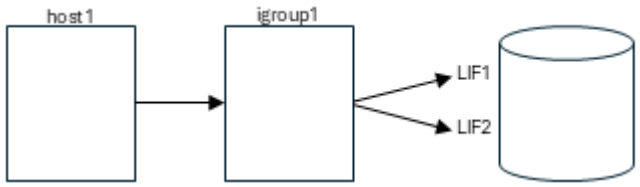
## Verwalten von Initiatorgruppen und Portsätzen

### Möglichkeiten, den LUN-Zugriff mit Portsätzen und Initiatorgruppen zu begrenzen

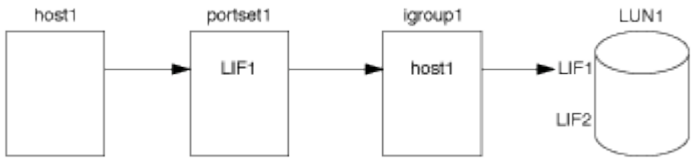
Zusätzlich zur Verwendung von Selective LUN Map (SLM) können Sie den Zugriff auf Ihre LUNs über Initiatorgruppen und Portsätze begrenzen.

Portsätze können mit SLM verwendet werden, um den Zugriff bestimmter Ziele noch weiter auf bestimmte Initiatoren zu beschränken. Wenn Sie SLM mit Portsätzen verwenden, sind die LUNs für den Satz der LIFs im Portsatz auf dem Node, der die LUN besitzt, und auf dem HA-Partner dieses Node zugänglich.

Im folgenden Beispiel hat Host1 keinen Portsatz. Ohne ein Portset kann Host1 über LIF1 und LIF2 auf LUN1 zugreifen.




Sie können den Zugriff auf LUN1 mithilfe eines Portsets einschränken. Im folgenden Beispiel kann Host1 nur über LIF1 auf LUN1 zugreifen. Allerdings kann Host1 nicht über LIF2 auf LUN1 zugreifen, da sich LIF2 nicht in Portset1 befindet.




**Verwandte Informationen**

- Selektive LUN-Zuordnung

- Erstellen Sie einen Portsatz und binden Sie diese an eine Initiatorgruppe

### Zeigen Sie SAN-Initiatoren und -Initiatorgruppen an und verwalten Sie sie

Mit System Manager können Sie Initiatorgruppen und Initiatoren anzeigen und verwalten.

#### Über diese Aufgabe

- Die Initiatorgruppen bestimmen, welche Hosts auf bestimmte LUNs im Storage-System zugreifen können.
- Nachdem ein Initiator und Initiatorgruppen erstellt wurden, können Sie auch bearbeiten oder löschen.
- Zum Verwalten von SAN-Initiatorgruppen und Initiatoren können Sie die folgenden Aufgaben durchführen:
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

#### Zeigen Sie SAN-Initiatorgruppen an und verwalten Sie sie

Mit System Manager können Sie eine Liste der Initiatorgruppen anzeigen. In der Liste können Sie weitere Vorgänge durchführen.

#### Schritte

1. Klicken Sie in System Manager auf **Hosts > SAN-Initiatorgruppen**.

   Die Seite zeigt eine Liste der Initiatorgruppen an. Wenn die Liste groß ist, können Sie weitere Seiten der Liste anzeigen, indem Sie auf die Seitenzahlen unten rechts auf der Seite klicken.

   In den Spalten werden verschiedene Informationen zu den Initiatorgruppen angezeigt. Ab 9.11.1 wird auch der Verbindungsstatus der Initiatorgruppe angezeigt. Bewegen Sie den Mauszeiger über Statuswarnungen, um Details anzuzeigen.

2. (Optional): Sie können die folgenden Aufgaben ausführen, indem Sie auf die Symbole oben rechts in der Liste klicken:
   - **Suche**
   - **Download** die Liste.
   - **Zeige** oder **Ausblenden** Spalten in der Liste.
   - **Filter** die Daten in der Liste.
3. Sie können Operationen aus der Liste ausführen:
   - Klicken Sie hier, + Add um eine Initiatorgruppe hinzuzufügen.
   - Klicken Sie auf den Namen der Initiatorgruppe, um die Seite **Übersicht** anzuzeigen, auf der Details zur Initiatorgruppe angezeigt werden.

     Auf der Seite **Übersicht** können Sie die LUNs anzeigen, die der Initiatorgruppe zugeordnet sind. Sie können die Vorgänge zum Erstellen von LUNs und zum Zuordnen der LUNs initiieren. Klicken Sie auf **Alle SAN-Initiatoren**, um zur Hauptliste zurückzukehren.

   - Bewegen Sie den Mauszeiger über die Initiatorgruppe und klicken Sie dann ⋮ neben einem Initiatorgruppennamen, um die Initiatorgruppe zu bearbeiten oder zu löschen.
   - Bewegen Sie den Mauszeiger über den Bereich links neben dem Initiatorgruppennamen, und aktivieren Sie dann das Kontrollkästchen. Wenn Sie auf *+zur Initiatorgruppe hinzufügen klicken, können Sie diese Initiatorgruppe einer anderen Initiatorgruppe hinzufügen.

- Klicken Sie in der Spalte **Storage VM** auf den Namen einer Storage VM, um Details dazu anzuzeigen.

#### Zeigen Sie SAN-Initiatoren an und verwalten Sie sie

Sie können mit System Manager eine Liste der Initiatoren anzeigen. In der Liste können Sie weitere Vorgänge durchführen.

**Schritte**

1. Klicken Sie in System Manager auf **Hosts > SAN-Initiatorgruppen**.

   Die Seite zeigt eine Liste der Initiatorgruppen an.

2. Führen Sie zum Anzeigen von Initiatoren folgende Schritte aus:

   - Klicken Sie auf die Registerkarte **FC-Initiatoren**, um eine Liste der FC-Initiatoren anzuzeigen.
   - Klicken Sie auf die Registerkarte **iSCSI-Initiatoren**, um eine Liste der iSCSI-Initiatoren anzuzeigen.

     In den Spalten werden verschiedene Informationen zu den Initiatoren angezeigt.

   Ab 9.11.1 wird auch der Verbindungsstatus des Initiators angezeigt. Bewegen Sie den Mauszeiger über Statuswarnungen, um Details anzuzeigen.

3. (Optional): Sie können die folgenden Aufgaben ausführen, indem Sie auf die Symbole oben rechts in der Liste klicken:
   - **Suche** die Liste für bestimmte Initiatoren.
   - **Download** die Liste.
   - **Zeige** oder **Ausblenden** Spalten in der Liste.
   - **Filter** die Daten in der Liste.

#### Verschachtelte Initiatorgruppe erstellen

Ab ONTAP 9.9 können Sie eine Initiatorgruppe erstellen, die aus anderen bestehenden Initiatorgruppen besteht.

1. Klicken Sie im System Manager auf **Host > SAN-Initiatorgruppen** und dann auf **Hinzufügen**.
2. Geben Sie die igroup **Name** und **Beschreibung** ein.

   Die Beschreibung dient als igroup-Alias.

3. Wählen Sie **Storage VM** und **Host Operating System** aus.

   > Der OS-Typ einer geschachtelten Initiatorgruppe kann nach dem Erstellen der Initiatorgruppe nicht geändert werden.

4. Wählen Sie unter **Initiatorgruppenmitglieder vorhandene Initiatorgruppe** aus.

   Sie können **Search** verwenden, um die Initiatorgruppen zu suchen und auszuwählen, die Sie hinzufügen möchten.

### Zuordnen von Initiatorgruppen zu mehreren LUNs

Ab ONTAP 9.9 können Sie Initiatorgruppen zwei oder mehr LUNs gleichzeitig zuordnen.

1. Klicken Sie im System Manager auf **Storage > LUNs**.
2. Wählen Sie die LUNs aus, die Sie zuordnen möchten.
3. Klicken Sie auf **Mehr** und dann auf **zu Initiatorgruppen zuordnen**.

Die ausgewählten Initiatorgruppen werden den ausgewählten LUNs hinzugefügt. Die bereits vorhandenen Zuordnungen werden nicht überschrieben.

### Erstellen Sie einen Portsatz und binden Sie diese an eine Initiatorgruppe

Zusätzlich zu verwenden "Selektive LUN-Zuordnung (SLM)"können Sie einen Portsatz erstellen und den Portsatz an eine Initiatorgruppe binden, um die LIFs, mit denen ein Initiator auf eine LUN zugreifen kann, weiter zu begrenzen.

Wenn Sie einen Portsatz nicht an eine Initiatorgruppe binden, können alle Initiatoren in der Initiatorgruppe über alle LIFs auf dem Node, der die LUN besitzt, und über den HA-Partner des entsprechenden Node auf die zugeordneten LUNs zugreifen.

#### Bevor Sie beginnen

Sie müssen mindestens eine LIF und eine Initiatorgruppe haben.

Wenn Sie keine Schnittstellengruppen verwenden, werden zwei LIFs für Redundanz sowohl für iSCSI als auch für FC empfohlen. Für Schnittstellengruppen wird nur ein LIF empfohlen.

#### Über diese Aufgabe

Es ist vorteilhaft, Portsätze mit SLM zu verwenden, wenn mehr als zwei LIFs auf einem Node vorhanden sind und Sie einen bestimmten Initiator auf eine Untermenge von LIFs beschränken möchten. Ohne Port-Sets sind alle Ziele auf dem Node für alle Initiatoren mit Zugriff auf die LUN über den Node verfügbar, der die LUN besitzt, und auf den HA-Partner des entsprechenden Node.

**Beispiel 6. Schritte**

**System Manager**

Ab ONTAP 9.10.1 können Sie mit System Manager Portsätze erstellen und an Initiatorgruppen binden.

Wenn Sie einen Portsatz erstellen und an eine Initiatorgruppe in einer ONTAP Version vor 9.10.1 binden müssen, müssen Sie das ONTAP CLI-Verfahren verwenden.

Ab ONTAP 9.12.1 müssen Sie, wenn Sie noch kein vorhandenes Portset haben, das erste mithilfe des ONTAP CLI-Verfahrens erstellen.

1. Klicken Sie in System Manager auf **Netzwerk > Übersicht > Portsätze** und dann auf **Hinzufügen**.
2. Geben Sie die Informationen für den neuen Portsatz ein und klicken Sie auf **Hinzufügen**.
3. Klicken Sie auf **Hosts > SAN-Initiatorgruppen**.
4. Um den Portsatz an eine neue Initiatorgruppe zu binden, klicken Sie auf **Hinzufügen**.

   Um den Portset an eine vorhandene Initiatorgruppe zu binden, wählen Sie die Initiatorgruppe aus, klicken Sie auf ⋮, und klicken Sie dann auf **Initiatorgruppe bearbeiten**.

**Verwandte Informationen**

"Anzeigen und Verwalten von Initiatoren und Initiatorgruppen"

**CLI**

1. Erstellen Sie einen Port-Satz, der die entsprechenden LIFs enthält:

   `portset create -vserver` *`vserver_name`* `-portset` *`portset_name`* `-protocol` *`protocol`* `-port-name` *`port_name`*

   Wenn Sie FC verwenden, geben Sie den `protocol` Parameter als `fcp`an. Wenn Sie iSCSI verwenden, geben Sie den `protocol` Parameter als an `iscsi`.

2. Bindet die Initiatorgruppe an den Portsatz:

   `lun igroup bind -vserver` *`vserver_name`* `-igroup` *`igroup_name`* `-portset` *`portset_name`*

   Erfahren Sie mehr über `lun igroup bind` in der "ONTAP-Befehlsreferenz".

3. Vergewissern Sie sich, dass Ihre Port-Sätze und LIFs richtig sind:

   `portset show -vserver` *`vserver_name`*

```
Vserver   Portset   Protocol Port Names    Igroups
--------- --------- -------- ------------- --------
vs3       portset0  iscsi    lif0,lif1     igroup1
```

### Portsätze verwalten

Zusätzlich zu "Selektive LUN-Zuordnung (SLM)"können Sie Portsätze verwenden, um zu begrenzen, welche LIFs ein Initiator für den Zugriff auf eine LUN verwenden kann.

Ab ONTAP 9.10.1 können Sie mit System Manager die mit Portsätzen verbundenen Netzwerkschnittstellen ändern und Portsätze löschen.

#### Ändern Sie die mit einem Portsatz verbundenen Netzwerkschnittstellen

1. Wählen Sie im System Manager **Netzwerk > Übersicht > Portsätze**.
2. Wählen Sie dann das Portset aus, das Sie bearbeiten möchten ⋮, und wählen Sie dann **Portset bearbeiten**.

#### Löschen Sie einen Portsatz

1. Klicken Sie in System Manager auf **Netzwerk > Übersicht > Portsätze**.
2. Um einen einzelnen Portsatz zu löschen, wählen Sie den Portsatz aus, ⋮ und wählen Sie dann **Portsätze löschen** aus.

   Um mehrere Portsätze zu löschen, wählen Sie die Portsätze aus, und klicken Sie auf **Löschen**.

### Übersicht über selektive LUN-Zuordnung

Die selektive LUN-Zuordnung (Selective LUN Map, SLM) reduziert die Anzahl der Pfade vom Host zur LUN. Wenn bei SLM eine neue LUN-Zuordnung erstellt wird, ist der Zugriff auf die LUN nur über Pfade auf dem Node möglich, der die LUN und deren HA-Partner besitzt.

SLM ermöglicht das Management einer einzelnen Initiatorgruppe pro Host und unterstützt auch unterbrechungsfreie LUN-Verschiebungsvorgänge, die keine Port-Änderung oder LUN-Neuzuordnung erfordern.

"Portsets" Kann mit SLM verwendet werden, um den Zugriff bestimmter Ziele auf bestimmte Initiatoren weiter einzuschränken. Wenn Sie SLM mit Portsätzen verwenden, sind die LUNs für den Satz der LIFs im Portsatz auf dem Node, der die LUN besitzt, und auf dem HA-Partner dieses Node zugänglich.

SLM ist standardmäßig auf allen neuen LUN-Zuordnungen aktiviert.

#### Ermitteln Sie, ob SLM auf einer LUN-Zuordnung aktiviert ist

Wenn in Ihrer Umgebung eine Kombination von LUNs erstellt wurde, die in einem ONTAP 9-Release erstellt wurden, und LUNs, die von früheren Versionen übertragen wurden, müssen Sie möglicherweise ermitteln, ob die selektive LUN-Zuordnung (SLM) für eine bestimmte LUN aktiviert ist.

Sie können die in der Ausgabe des `lun mapping show -fields reporting-nodes, node` Befehls angezeigten Informationen verwenden, um zu bestimmen, ob SLM für Ihre LUN-Zuordnung aktiviert ist. Wenn SLM nicht aktiviert ist, wird „-“ in den Zellen in der Spalte „`reporting-nodes`“ der Befehlsausgabe angezeigt. Wenn SLM aktiviert ist, wird die unter der Spalte „`Nodes`“ angezeigte Liste der Knoten in der Spalte „`reporting-nodes`“ dupliziert.

Erfahren Sie mehr über `lun mapping show` in der "ONTAP-Befehlsreferenz".

#### Ändern Sie die Liste der SLM-Reporting-Nodes

Wenn Sie eine LUN oder ein Volume mit LUNs auf ein anderes HA-Paar (High Availability) innerhalb desselben Clusters verschieben, sollten Sie die Liste mit Berichterstellungknoten für Selective LUN Map (SLM) ändern, bevor Sie die Verschiebung initiieren, um sicherzustellen, dass aktive, optimierte LUN-Pfade beibehalten werden.

**Schritte**

1. Fügen Sie den Ziel-Node und seinen Partner-Node zur Liste der Reporting-Nodes des Aggregats oder Volumes hinzu:

   ```
   lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
   -igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
   destination-volume <volume_name>]
   ```

   Wenn Sie über eine konsistente Namenskonvention verfügen, können Sie mehrere LUN-Zuordnungen gleichzeitig mithilfe von ändern `igroup_prefix* igroup_name`.

2. Prüfen Sie den Host erneut, um die neu hinzugefügten Pfade zu finden.
3. Wenn Ihr Betriebssystem benötigt wird, fügen Sie die neuen Pfade zu Ihrer Multipath-Netzwerk-I/O (MPIO)-Konfiguration hinzu.
4. Führen Sie den Befehl für den Vorgang der erforderlichen Verschiebung aus, und warten Sie, bis der Vorgang abgeschlossen ist.
5. Vergewissern Sie sich, dass die I/O-Verarbeitung über den aktiv/optimierten Pfad erfolgt:

   ```
   lun mapping show -fields reporting-nodes
   ```

6. Entfernen Sie den vorherigen LUN-Eigentümer und seinen Partner-Node aus der Liste der Reporting-Nodes:

   ```
   lun mapping remove-reporting-nodes -vserver <vserver_name> -path
   <lun_path> -igroup <igroup_name> -remote-nodes
   ```

7. Vergewissern Sie sich, dass die LUN aus der vorhandenen LUN-Zuordnung entfernt wurde:

   ```
   lun mapping show -fields reporting-nodes
   ```

8. Entfernen Sie alle veralteten Geräteeinträge für das Host-Betriebssystem.
9. Ändern Sie gegebenenfalls alle Multipathing-Konfigurationsdateien.
10. Der Host wird erneut gescannt, um das Entfernen alter Pfade zu überprüfen. + Informationen zu bestimmten Schritten finden Sie in Ihrer Host-Dokumentation, um Ihre Hosts erneut zu scannen.

# Managen des iSCSI-Protokolls

## Konfigurieren Sie Ihr Netzwerk für optimale Leistung

Ethernet-Netzwerke unterscheiden sich in ihrer Leistung stark. Sie können die Leistung des für iSCSI verwendeten Netzwerks maximieren, indem Sie bestimmte Konfigurationswerte auswählen.

### Schritte

1. Verbinden Sie den Host und die Speicher-Ports mit dem gleichen Netzwerk.

   Am besten mit den gleichen Switches verbinden. Routing sollte niemals verwendet werden.

2. Wählen Sie die verfügbaren Ports mit der höchsten Geschwindigkeit aus und weisen Sie sie iSCSI zu.

   10 GbE-Ports sind am besten. 1-GbE-Ports sind das Minimum.

3. Deaktivieren Sie die Ethernet-Flusssteuerung für alle Ports.

   Siehe "Netzwerkmanagement" für die Verwendung der CLI zum Konfigurieren der Ethernet-Port-Flusssteuerung.

4. Aktivieren von Jumbo Frames (in der Regel MTU von 9000).

   Alle Geräte im Datenpfad, einschließlich Initiatoren, Ziele und Switches, müssen Jumbo Frames unterstützen. Andernfalls verringert die Aktivierung von Jumbo Frames die Netzwerk-Performance erheblich.

## Konfigurieren Sie eine SVM für iSCSI

Um eine Storage Virtual Machine (SVM) für iSCSI zu konfigurieren, müssen Sie LIFs für die SVM erstellen und diesen LIFs das iSCSI-Protokoll zuweisen.

### Über diese Aufgabe

Sie benötigen für jede SVM, die Daten über das iSCSI-Protokoll bereitstellt, mindestens eine iSCSI-LIF pro Node. Um Redundanz zu gewährleisten, sollten Sie mindestens zwei LIFs pro Node erstellen.

**Beispiel 7. Schritte**

**System Manager**

Konfigurieren Sie eine Storage VM für iSCSI mit ONTAP System Manager (9.7 und höher).

| So konfigurieren Sie iSCSI auf einer neuen Speicher-VM | So konfigurieren Sie iSCSI auf einer vorhandenen Storage-VM |
|---|---|
| 1. Klicken Sie im System Manager auf **Storage > Storage VMs** und dann auf **Hinzufügen**.<br>2. Geben Sie einen Namen für die Storage-VM ein.<br>3. Wählen Sie **iSCSI** für das **Access Protocol**.<br>4. Klicken Sie auf **iSCSI aktivieren** und geben Sie die IP-Adresse und die Subnetzmaske für die Netzwerkschnittstelle ein. + jeder Node sollte mindestens zwei Netzwerkschnittstellen aufweisen.<br>5. Klicken Sie Auf **Speichern**. | 1. Klicken Sie im System Manager auf **Storage > Storage VMs**.<br>2. Klicken Sie auf die zu konfigurierende Speicher-VM.<br>3. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf ⚙ neben dem iSCSI-Protokoll.<br>4. Klicken Sie auf **iSCSI aktivieren** und geben Sie die IP-Adresse und die Subnetzmaske für die Netzwerkschnittstelle ein. + jeder Node sollte mindestens zwei Netzwerkschnittstellen aufweisen.<br>5. Klicken Sie Auf **Speichern**. |

**CLI**

Konfigurieren Sie eine Storage VM für iSCSI mit der ONTAP CLI.

1. Aktivieren Sie die SVMs, um iSCSI-Datenverkehr abzuhören:

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. Erstellen Sie eine LIF für die SVMs auf jedem Node, die Sie für iSCSI verwenden können:
   - Für ONTAP 9.6 und höher:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - Für ONTAP 9.5 und früher:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. Überprüfen Sie, ob Sie Ihre LIFs ordnungsgemäß einrichten:

   ```
   network interface show -vserver vserver_name
   ```

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

4. Vergewissern Sie sich, dass iSCSI betriebsbereit ist und die Ziel-IQN für diese SVM:

```
vserver iscsi show -vserver vserver_name
```

5. Erstellen Sie von Ihrem Host aus iSCSI-Sitzungen zu Ihren LIFs.

**Verwandte Informationen**

- "Technischer Bericht 4080 zu NetApp: Best Practices für modernes SAN"

### Definieren einer Sicherheitsrichtlinie für einen Initiator

Sie können eine Liste von Initiatoren und deren Authentifizierungsmethoden definieren. Sie können auch die Standardauthentifizierungsmethode ändern, die für Initiatoren gilt, die über keine benutzerdefinierte Authentifizierungsmethode verfügen.

**Über diese Aufgabe**

Sie können mithilfe von Sicherheitsrichtlinien-Algorithmen im Produkt eindeutige Passwörter generieren oder die Passwörter, die Sie verwenden möchten, manuell festlegen.

Nicht alle Initiatoren unterstützen hexadezimale CHAP-Kennwörter.

**Schritte**

1. `vserver iscsi security create`Erstellen Sie mit dem Befehl eine Sicherheitsrichtlinienmethode für einen Initiator.

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. Befolgen Sie die Bildschirmbefehle, um die Passwörter hinzuzufügen.

   Erstellt eine Sicherheitsrichtlinie für Initiator iqn.1991-05.com.microsoft:host1 mit ein- und ausgehenden CHAP-Benutzernamen und -Passwörtern.

**Verwandte Informationen**

- Funktionsweise der iSCSI-Authentifizierung
- CHAP-Authentifizierung

### Löschen eines iSCSI-Dienstes für eine SVM

Sie können einen iSCSI-Service für eine Storage Virtual Machine (SVM) löschen, wenn dieser nicht mehr benötigt wird.

**Bevor Sie beginnen**

Der Administrationsstatus des iSCSI-Dienstes muss sich im Status „`down`“ befinden, bevor Sie einen iSCSI-Dienst löschen können. Sie können den Administrationsstatus mit dem `vserver iscsi modify` Befehl nach unten verschieben.

**Schritte**

1. `vserver iscsi modify`Beenden Sie die I/O-Vorgänge für die LUN mit dem Befehl.

```
vserver iscsi modify -vserver vs1 -status-admin down
```

2. `vserver iscsi delete`Entfernen Sie den iscsi-Service mit dem Befehl von der SVM.

```
vserver iscsi delete -vserver vs_1
```

3. `vserver iscsi show command`Überprüfen Sie mit dem, ob Sie den iSCSI-Dienst von der SVM gelöscht haben.

```
vserver iscsi show -vserver vs1
```

#### Weitere Details bei der Wiederherstellung von iSCSI-Sitzungsfehlern

Wenn Sie die Recovery-Ebene für iSCSI-Sitzungsfehler erhöhen, erhalten Sie detailliertere Informationen über die Wiederherstellung von iSCSI-Fehlern. Die Verwendung eines höheren Fehlerwiederherstellungsniveaus kann zu einer geringfügigen Reduzierung der iSCSI-Sitzungsleistung führen.

##### Über diese Aufgabe

Standardmäßig ist ONTAP so konfiguriert, dass für iSCSI-Sitzungen die Fehlerwiederherstellungsstufe 0 verwendet wird. Wenn Sie einen Initiator verwenden, der für die Fehlerwiederherstellungsstufe 1 oder 2 qualifiziert wurde, können Sie wählen, die Fehlerwiederherstellungsstufe zu erhöhen. Der geänderte Wiederherstellungslevel für Sitzungsfehler betrifft nur die neu erstellten Sitzungen und wirkt sich nicht auf vorhandene Sitzungen aus.

Ab ONTAP 9.4 `max-error-recovery-level` wird die Option in den `iscsi show` `iscsi modify` Befehlen und nicht unterstützt.

##### Schritte

1. Erweiterten Modus aufrufen:

```
set -privilege advanced
```

2. Überprüfen Sie die aktuelle Einstellung mit dem `iscsi show` Befehl.

```
iscsi show -vserver vs3 -fields max-error-recovery-level
```

```
vserver max-error-recovery-level
------- ------------------------
vs3     0
```

3. Ändern Sie die Fehlerwiederherstellungs-Ebene mit dem `iscsi modify` Befehl.

```
iscsi modify -vserver vs3 -max-error-recovery-level 2
```

#### Registrieren Sie die SVM mit einem iSNS-Server

Sie können den `vserver iscsi isns` Befehl verwenden, um die Storage Virtual Machine (SVM) für die Registrierung bei einem iSNS-Server zu konfigurieren.

**Über diese Aufgabe**

Mit dem `vserver iscsi isns create` Befehl wird die SVM so konfiguriert, dass sie sich beim iSNS-Server registriert. Die SVM bietet keine Befehle, mit denen Sie den iSNS-Server konfigurieren oder verwalten können. Zur Verwaltung des iSNS-Servers können Sie die Server-Verwaltungstools oder die vom Hersteller bereitgestellte Schnittstelle für den iSNS-Server verwenden.

**Schritte**

1. Stellen Sie auf Ihrem iSNS-Server sicher, dass der iSNS-Dienst verfügbar ist.
2. Erstellung der SVM-Management-LIF auf einem Daten-Port:

   `network interface create -vserver SVM_name -lif lif_name -role data -data -protocol none -home-node home_node_name -home-port home_port -address IP_address -netmask network_mask`

   Erfahren Sie mehr über `network interface create` in der "ONTAP-Befehlsreferenz".

3. Erstellen Sie einen iSCSI-Service auf Ihrer SVM, wenn einer noch nicht vorhanden ist:

   `vserver iscsi create -vserver SVM_name`

4. Überprüfen Sie, ob der iSCSI-Service erfolgreich erstellt wurde:

   `iscsi show -vserver SVM_name`

5. Vergewissern Sie sich, dass für die SVM eine Standardroute vorhanden ist:

   `network route show -vserver SVM_name`

6. Wenn es keine Standardroute für die SVM gibt, erstellen Sie eine Standardroute:

   `network route create -vserver SVM_name -destination destination -gateway gateway`

   Erfahren Sie mehr über `network route create` in der "ONTAP-Befehlsreferenz".

7. Konfigurieren Sie die SVM für die Registrierung beim iSNS-Dienst:

   `vserver iscsi isns create -vserver SVM_name -address IP_address`

   Es werden sowohl IPv4- als auch IPv6-Adressfamilien unterstützt. Die Adressfamilie des iSNS-Servers muss mit der SVM-Management-LIF identisch sein.

   Beispielsweise können Sie keine Management-LIF für eine SVM mit einer IPv4-Adresse mit einem iSNS-Server mit einer IPv6-Adresse verbinden.

8. Überprüfen Sie, ob der iSNS-Dienst ausgeführt wird:

   `vserver iscsi isns show -vserver SVM_name`

9. Wenn der iSNS-Dienst nicht ausgeführt wird, starten Sie ihn:

   `vserver iscsi isns start -vserver SVM_name`

#### Beheben Sie iSCSI-Fehlermeldungen auf dem Speichersystem

Es gibt eine Reihe allgemeiner iSCSI-Fehlermeldungen, die Sie mit dem `event log show` Befehl anzeigen können. Sie müssen wissen, was diese Nachrichten bedeuten und was Sie tun können, um die Probleme zu lösen, die sie identifizieren.

Die folgende Tabelle enthält die häufigsten Fehlermeldungen und Anweisungen für deren Behebung:

| Nachricht | Erklärung | Was zu tun ist |
|---|---|---|
| `ISCSI: network interface identifier disabled for use; incoming connection discarded` | Der iSCSI-Dienst ist auf der Schnittstelle nicht aktiviert. | Sie können den `iscsi interface enable` iSCSI-Dienst auf der Schnittstelle mit dem Befehl aktivieren. Beispiel:<br><br>`iscsi interface enable -vserver vs1 -lif lif1` |
| `ISCSI: Authentication failed for initiator nodename` | CHAP ist für den angegebenen Initiator nicht ordnungsgemäß konfiguriert. | Sie sollten die CHAP-Einstellungen überprüfen. Sie können denselben Benutzernamen und dasselbe Kennwort für ein- und ausgehende Einstellungen auf dem Speichersystem nicht verwenden:<br><br>• Eingehende Anmeldeinformationen auf dem Speichersystem müssen mit den Outbound-Anmeldedaten auf dem Initiator übereinstimmen.<br>• Die Anmeldeinformationen für ausgehende Anrufe auf dem Speichersystem müssen mit den eingehenden Anmeldeinformationen auf dem Initiator übereinstimmen. |

Erfahren Sie mehr über `event log show` in der "ONTAP-Befehlsreferenz".

#### Aktivieren oder deaktivieren Sie den automatischen iSCSI LIF-Failover

Nach einem Upgrade auf ONTAP 9.11.1 oder höher sollten Sie für alle iSCSI LIFs, die in ONTAP 9.10.1 oder einer älteren Version erstellt wurden, manuell den automatischen LIF Failover aktivieren.

Ab ONTAP 9.11.1 können Sie automatisches LIF-Failover für iSCSI LIFs auf All-Flash-SAN-Array-Plattformen aktivieren. Im Falle eines Storage-Failovers wird die iSCSI-LIF automatisch von seinem Home Node oder Port zu seinem HA-Partnerknoten bzw. -Port migriert und nach Abschluss des Failovers dann wieder zurück. Falls der Port für iSCSI LIF nicht mehr fehlerfrei ist, wird die LIF automatisch zu einem ordnungsgemäßen Port im aktuellen Home Node und anschließend zurück zu seinem ursprünglichen Port migriert, sobald der Port wieder

funktionsfähig ist. Der ermöglicht es SAN-Workloads, die auf iSCSI ausgeführt werden, den I/O-Service nach einem Failover schneller wieder aufzunehmen.

In ONTAP 9.11.1 und höher sind neu erstellte iSCSI LIFs standardmäßig für automatischen LIF-Failover aktiviert, wenn eine der folgenden Bedingungen zutrifft:

- Auf der SVM befinden sich keine iSCSI LIFs
- Alle iSCSI-LIFs auf der SVM sind für automatisches LIF Failover aktiviert

#### Aktivieren Sie automatisches iSCSI LIF Failover

Standardmäßig sind in ONTAP 9.10.1 erstellte iSCSI LIFs für den automatischen LIF-Failover nicht aktiviert. Wenn auf der SVM iSCSI-LIFs vorhanden sind, die nicht für automatischen LIF-Failover aktiviert sind, werden die neu erstellten LIFs auch nicht für automatischen LIF-Failover aktiviert. Wenn der automatische LIF-Failover nicht aktiviert ist und ein Failover-Ereignis tritt, werden die iSCSI LIFs nicht migriert.

Erfahren Sie mehr über "LIF Failover und Giveback".

**Schritt**

1. Aktivieren Sie automatischen Failover für eine iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

   Um alle iSCSI-LIFs auf der SVM zu aktualisieren, verwenden Sie `-lif*` statt `lif` .

#### Deaktivieren Sie den automatischen iSCSI-LIF-Failover

Wenn Sie zuvor den automatischen iSCSI LIF Failover auf in ONTAP 9.10.1 oder früher erstellten iSCSI LIFs aktiviert haben, haben Sie die Möglichkeit, diesen zu deaktivieren.

**Schritt**

1. Deaktivieren Sie den automatischen Failover für eine iSCSI LIF:

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

   Um alle iSCSI-LIFs auf der SVM zu aktualisieren, verwenden Sie `-lif*` statt `lif` .

**Verwandte Informationen**

- "Erstellen Sie eine LIF"
- Manuell "Migrieren Sie LIF"
- Manuell "Zurücksetzen einer LIF auf seinen Home Port"
- "Konfigurieren Sie die Failover-Einstellungen auf einem LIF"

# Management des FC-Protokolls

## Konfigurieren Sie eine SVM für FC

Um eine Storage Virtual Machine (SVM) für FC zu konfigurieren, müssen Sie LIFs für die SVM erstellen und diesen LIFs das FC-Protokoll zuweisen.

### Bevor Sie beginnen

Sie müssen über eine FC-Lizenz ("Im Lieferumfang von ONTAP One enthalten") verfügen und diese muss aktiviert sein. Wenn die FC-Lizenz nicht aktiviert ist, scheinen die LIFs und SVMs online zu sein, der Betriebsstatus lautet jedoch `down`. Der FC-Service muss aktiviert sein, damit Ihre LIFs und SVMs funktionsfähig sind. Zum Hosten der Initiatoren müssen Sie das einzelne Initiator-Zoning für alle FC-LIFs in der SVM verwenden.

### Über diese Aufgabe

NetApp unterstützt mindestens eine FC-LIF pro Node für jede SVM, die Daten über das FC-Protokoll bereitstellt. Sie müssen zwei LIFs pro Node und zwei Fabrics verwenden, wobei eine LIF pro Node angeschlossen ist. Dies sorgt für Redundanz auf Node-Ebene und in der Fabric.

**Beispiel 8. Schritte**

**System Manager**

Konfigurieren Sie eine Storage VM für iSCSI mit ONTAP System Manager (9.7 und höher).

| So konfigurieren Sie FC auf einer neuen Storage-VM | So konfigurieren Sie FC für eine vorhandene Storage-VM |
|---|---|
| 1. Klicken Sie im System Manager auf **Storage > Storage VMs** und dann auf **Hinzufügen**.<br>2. Geben Sie einen Namen für die Storage-VM ein.<br>3. Wählen Sie * FC* für das **Zugriffsprotokoll**.<br>4. Klicken Sie auf **FC aktivieren**. + die FC-Ports werden automatisch zugewiesen.<br>5. Klicken Sie Auf **Speichern**. | 1. Klicken Sie im System Manager auf **Storage > Storage VMs**.<br>2. Klicken Sie auf die zu konfigurierende Speicher-VM.<br>3. Klicken Sie auf die Registerkarte **Einstellungen** und dann auf ⚙ neben dem FC-Protokoll.<br>4. Klicken Sie auf **FC aktivieren** und geben Sie die IP-Adresse und die Subnetzmaske für die Netzwerkschnittstelle ein. + die FC-Ports werden automatisch zugewiesen.<br>5. Klicken Sie Auf **Speichern**. |

**CLI**

1. FC-Service für die SVM aktivieren:

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. Erstellen Sie zwei LIFs für die SVMs auf jedem Node, der FC-Services bereitstellt:
   - Für ONTAP 9.6 und höher:

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - Für ONTAP 9.5 und früher:

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. Überprüfen Sie, ob Ihre LIFs erstellt wurden und ob ihr Betriebsstatus lautet `online`:

   ```
   network interface show -vserver vserver_name lif_name
   ```

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

- "NetApp Support"
- "NetApp Interoperabilitäts-Matrix-Tool"

- Überlegungen zu LIFs in Cluster-SAN-Umgebungen

#### Löschen Sie einen FC-Service für eine SVM

Sie können einen FC-Service für eine Storage Virtual Machine (SVM) löschen, wenn dieser nicht mehr benötigt wird.

##### Bevor Sie beginnen

Der Administrationsstatus muss „`down`“ sein, bevor Sie einen FC-Service für eine SVM löschen können. Sie können den Administrationsstatus mit dem `vserver fcp modify` `vserver fcp stop` Befehl oder dem Befehl auf „down“ setzen.

##### Schritte

1. `vserver fcp stop`Beenden Sie die I/O-Vorgänge für die LUN mit dem Befehl.

   ```
   vserver fcp stop -vserver vs_1
   ```

2. `vserver fcp delete`Entfernen Sie den Service mit dem Befehl aus der SVM.

   ```
   vserver fcp delete -vserver vs_1
   ```

3. `vserver fcp show`Überprüfen Sie mithilfe der, ob Sie den FC-Service von Ihrer SVM gelöscht haben:

   ```
   vserver fcp show -vserver vs_1
   ```

#### Empfohlene MTU-Konfigurationen für FCoE Jumbo Frames

Bei Fibre Channel over Ethernet (FCoE) sollten Jumbo Frames für den Ethernet-Adapteranteil des CNA bei 9000 MTU konfiguriert sein. Jumbo-Frames für den FCoE-Adapter-Teil des CNA sollten mit einer Größe von mehr als 1500 MTU konfiguriert sein. Konfigurieren Sie Jumbo Frames nur, wenn Initiator, Ziel und alle dazwischenliegenden Switches unterstützt und für Jumbo Frames konfiguriert sind.

## Managen des NVMe-Protokolls

#### Starten Sie den NVMe-Service für eine SVM

Bevor Sie das NVMe-Protokoll für Ihre Storage Virtual Machine (SVM) verwenden können, müssen Sie den NVMe-Service auf der SVM starten.

##### Bevor Sie beginnen

NVMe muss als Protokoll auf Ihrem System zugelassen sein.

Folgende NVMe-Protokolle werden unterstützt:

| Protokoll | Beginnend mit … | Zulässig von… |
|---|---|---|
| TCP | ONTAP 9.10.1 | Standard |
| FCP | ONTAP 9,4 | Standard |

**Schritte**

1. Ändern Sie die Berechtigungseinstellung in erweitert:

   ```
   set -privilege advanced
   ```

2. Vergewissern Sie sich, dass NVMe als Protokoll zulässig ist:

   ```
   vserver nvme show
   ```

3. Erstellung des NVMe-Protokollservice:

   ```
   vserver nvme create
   ```

4. Starten des NVMe-Protokollservice auf der SVM:

   ```
   vserver nvme modify -status -admin up
   ```

#### Löschen des NVMe-Service aus einer SVM

Bei Bedarf können Sie den NVMe-Service von Ihrer Storage Virtual Machine (SVM) löschen.

**Schritte**

1. Ändern Sie die Berechtigungseinstellung in erweitert:

   ```
   set -privilege advanced
   ```

2. Beenden Sie den NVMe-Service auf der SVM:

   ```
   vserver nvme modify -status -admin down
   ```

3. Löschen Sie den NVMe-Service:

   ```
   vserver nvme delete
   ```

#### Größe eines Namespace ändern

Ab ONTAP 9.10.1 können Sie mithilfe der ONTAP CLI den NVMe Namespace erhöhen oder verringern. Mit System Manager kann der NVMe Namespace vergrößert werden.

##### Vergrößern Sie den Namespace

**System Manager**

1. Klicken Sie auf **Storage > NVMe Namesaces**.
2. Hoover über den Namespace, den Sie vergrößern möchten, klicken Sie auf ⋮, und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie unter **CAPACITY** die Größe des Namespace.

**CLI**

1. Geben Sie den folgenden Befehl ein: `vserver nvme namespace modify -vserver SVM_name -path path –size new_size_of_namespace`

#### Verkleinern Sie die Größe eines Namespace

Sie müssen die ONTAP-CLI verwenden, um die Größe eines NVMe Namespace zu reduzieren.

1. Ändern Sie die Berechtigungseinstellung in erweitert:

   ```
   set –privilege advanced
   ```

2. Verkleinern Sie die Größe des Namespace:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size new_size_of_namespace
   ```

### Konvertieren eines Namespace in eine LUN

Ab ONTAP 9.11.1 können Sie die ONTAP CLI verwenden, um einen vorhandenen NVMe Namespace in eine LUN zu konvertieren.

#### Bevor Sie beginnen

- Der angegebene NVMe-Namespace sollte keine vorhandenen Zuordnungen zu einem Subsystem haben.
- Namespace sollte nicht Teil eines Snapshots oder auf der Zielseite der SnapMirror-Beziehung als schreibgeschützter Namespace sein.
- Da NVMe Namespaces nur für bestimmte Plattformen und Netzwerkkarten unterstützt werden, funktioniert diese Funktion nur mit bestimmten Hardware.

#### Schritte

1. Geben Sie den folgenden Befehl ein, um einen NVMe Namespace in eine LUN zu konvertieren:

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

   Erfahren Sie mehr über `lun convert-from-namespace` in der "ONTAP-Befehlsreferenz".

### In-Band-Authentifizierung über NVMe einrichten

Ab ONTAP 9.12.1 können Sie die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um die bandinterne (sichere), bidirektionale und unidirektionale Authentifizierung zwischen einem NVMe Host und Controller über die NVME/TCP- und NVMe/FC-Protokolle unter

## Verwendung der DH-HMAC-CHAP-Authentifizierung zu konfigurieren. Ab ONTAP 9.14.1 kann die in-Band-Authentifizierung in System Manager konfiguriert werden.

Zur Einrichtung der bandinternen Authentifizierung muss jeder Host oder Controller einem DH-HMAC-CHAP-Schlüssel zugeordnet sein. Dieser Schlüssel ist eine Kombination aus NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsschlüssel. Damit ein NVMe-Host oder -Controller seinen Peer authentifizieren kann, muss er den dem Peer zugeordneten Schlüssel kennen.

Bei der unidirektionalen Authentifizierung wird ein geheimer Schlüssel für den Host konfiguriert, nicht jedoch für den Controller. Bei der bidirektionalen Authentifizierung wird ein geheimer Schlüssel sowohl für den Host als auch für den Controller konfiguriert.

SHA-256 ist die Standard-Hash-Funktion und 2048-Bit ist die Standard-DH-Gruppe.

**System Manager**

Ab ONTAP 9.14.1 können Sie die in-Band-Authentifizierung über System Manager bei der Erstellung oder Aktualisierung eines NVMe-Subsystems, der Erstellung oder dem Klonen von NVMe-Namespaces oder dem Hinzufügen von Konsistenzgruppen mit neuen NVMe-Namespaces konfigurieren.

**Schritte**

1. Klicken Sie im System Manager auf **Hosts > NVMe-Subsystem** und dann auf **Hinzufügen**.
2. Fügen Sie den Namen des NVMe-Subsystems hinzu und wählen Sie die Storage-VM und das Host-Betriebssystem aus.
3. Geben Sie die Host-NQN ein.
4. Wählen Sie **bandinterne Authentifizierung verwenden** neben dem Host-NQN.
5. Geben Sie den Host-Schlüssel und den Controller-Schlüssel ein.

   Der DH-HMAC-CHAP-Schlüssel ist eine Kombination aus dem NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsschlüssel.

6. Wählen Sie die bevorzugte Hash-Funktion und die DH-Gruppe für jeden Host aus.

   Wenn Sie keine Hash-Funktion und keine DH-Gruppe auswählen, wird SHA-256 als Standard-Hash-Funktion zugewiesen und 2048-Bit als Standard-DH-Gruppe zugewiesen.

7. Klicken Sie optional auf **Hinzufügen** und wiederholen Sie die Schritte, um weitere Hosts hinzuzufügen.
8. Klicken Sie Auf **Speichern**.
9. Um zu überprüfen, ob die bandinterne Authentifizierung aktiviert ist, klicken Sie auf **System Manager > Hosts > NVMe-Subsystem > Grid > Peek View**.

   Ein transparentes Schlüsselsymbol neben dem Hostnamen zeigt an, dass der unidirektionale Modus aktiviert ist. Ein undurchsichtiger Schlüssel neben dem Hostnamen zeigt an, dass der bidirektionale Modus aktiviert ist.

**CLI**

**Schritte**

1. Fügen Sie Ihrem NVMe-Subsystem DH-HMAC-CHAP-Authentifizierung hinzu:

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   Erfahren Sie mehr über `vserver nvme subsystem host add` in der "ONTAP-Befehlsreferenz".

2. Vergewissern Sie sich, dass das DH-HMAC CHAP-Authentifizierungsprotokoll Ihrem Host hinzugefügt wird:

```
vserver nvme subsystem host show
```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Erfahren Sie mehr über `vserver nvme subsystem host show` in der "ONTAP-Befehlsreferenz".

3. Überprüfen Sie, ob die DH-HMAC CHAP-Authentifizierung während der Erstellung des NVMe-Controllers durchgeführt wurde:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                               Authentication
Diffie-Hellman
                                               Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                               Authentication Mode
```

**Verwandte Informationen**

- "vServer NVMe-Subsystem-Controller anzeigen"

### In-Band-Authentifizierung über NVMe deaktiviert

Wenn Sie die bandinterne Authentifizierung über NVMe mit DH-HMAC-CHAP konfiguriert haben, können Sie diese jederzeit deaktivieren.

Wenn Sie von ONTAP 9.12.1 oder höher auf ONTAP 9.12.0 oder früher zurücksetzen, müssen Sie die bandinterne Authentifizierung vor dem Zurücksetzen deaktivieren. Wenn die bandinterne Authentifizierung mit DH-HMAC-CHAP nicht deaktiviert ist, schlägt die Wiederherstellung fehl.

**Schritte**

1. Entfernen Sie den Host aus dem Subsystem, um die DH-HMAC-CHAP-Authentifizierung zu deaktivieren:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Vergewissern Sie sich, dass das DH-HMAC-CHAP-Authentifizierungsprotokoll vom Host entfernt wird:

```
vserver nvme subsystem host show
```

3. Fügen Sie den Host ohne Authentifizierung wieder zum Subsystem hinzu:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

#### TLS Secure Channel für NVMe/TCP einrichten

Ab ONTAP 9.16.1 können Sie einen sicheren TLS-Kanal für NVMe/TCP-Verbindungen konfigurieren. Sie können den System Manager oder die ONTAP CLI verwenden, um entweder ein neues NVMe-Subsystem mit aktiviertem TLS hinzuzufügen oder TLS für ein bestehendes NVMe-Subsystem zu aktivieren. ONTAP unterstützt kein TLS-Hardware-Offloading.

**System Manager**

Ab ONTAP 9.16.1 können Sie System Manager verwenden, um TLS für NVMe/TCP-Verbindungen bei der Erstellung oder Aktualisierung eines NVMe-Subsystems zu konfigurieren, NVMe-Namespaces zu erstellen oder zu klonen oder Konsistenzgruppen mit neuen NVMe-Namespaces hinzuzufügen.

**Schritte**

1. Klicken Sie im System Manager auf **Hosts > NVMe-Subsystem** und dann auf **Hinzufügen**.
2. Fügen Sie den Namen des NVMe-Subsystems hinzu und wählen Sie die Storage-VM und das Host-Betriebssystem aus.
3. Geben Sie die Host-NQN ein.
4. Wählen Sie **TLS (Transport Layer Security)** neben dem Host-NQN.
5. Geben Sie den Pre-Shared Key (PSK) an.
6. Klicken Sie Auf **Speichern**.
7. Um zu überprüfen, ob TLS Secure Channel aktiviert ist, wählen Sie **System Manager > Hosts > NVMe Subsystem > Grid > Peek View** aus.

**CLI**

**Schritte**

1. Fügen Sie einen NVMe-Subsystem-Host hinzu, der TLS Secure Channel unterstützt. Sie können einen Pre-Shared Key (PSK) bereitstellen, indem Sie `tls-configured-psk` Argument:

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Vergewissern Sie sich, dass der Host des NVMe-Subsystems für den sicheren TLS-Kanal konfiguriert ist. Optional können Sie das Argument verwenden `tls-key-type`, um nur Hosts anzuzeigen, die diesen Schlüsseltyp verwenden:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. Vergewissern Sie sich, dass der Host-Controller des NVMe-Subsystems für TLS Secure Channel konfiguriert ist. Sie können optional eines der Argumente , , `tls-identity` oder `tls-cipher` verwenden `tls-key-type`, um nur die Controller anzuzeigen, die diese TLS-Attribute haben:

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

**Verwandte Informationen**

- "nvme-Subsystem von vserver"

#### Deaktivieren Sie TLS Secure Channel für NVMe/TCP

Ab ONTAP 9.16.1 können Sie TLS Secure Channel für NVMe/TCP-Verbindungen konfigurieren. Wenn Sie TLS Secure Channel für NVMe/TCP-Verbindungen konfiguriert haben, können Sie diesen jederzeit deaktivieren.

**Schritte**

1. Entfernen Sie den Host aus dem Subsystem, um TLS Secure Channel zu deaktivieren:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Vergewissern Sie sich, dass der TLS-sichere Kanal vom Host entfernt wird:

```
vserver nvme subsystem host show
```

3. Fügen Sie den Host wieder dem Subsystem ohne TLS Secure Channel hinzu:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

**Verwandte Informationen**

- "Host des vserver nvme-Subsystems"

#### Ändern der NVMe-Host-Priorität

Ab ONTAP 9.14.1 können Sie das NVMe-Subsystem so konfigurieren, dass es die Ressourcenzuweisung für bestimmte Hosts priorisiert. Wenn ein Host dem Subsystem hinzugefügt wird, wird ihm standardmäßig eine reguläre Priorität zugewiesen. Hosts, denen eine hohe Priorität zugewiesen ist, werden eine größere Anzahl von I/O-Warteschlangen und eine größere Warteschlangentiefe zugewiesen.

Mithilfe der ONTAP Befehlszeilenschnittstelle (CLI) kann die Standardpriorität manuell von „Normal“ auf „hoch“ geändert werden. Um die einem Host zugewiesene Priorität zu ändern, müssen Sie den Host aus dem Subsystem entfernen und ihn dann wieder hinzufügen.

**Schritte**

1. Vergewissern Sie sich, dass die Host-Priorität auf „Normal“ eingestellt ist:

```
vserver nvme show-host-priority
```

   Erfahren Sie mehr über `vserver nvme show-host-priority` in der "ONTAP-Befehlsreferenz".

2. Entfernen Sie den Host aus dem Subsystem:

```
vserver nvme subsystem host remove –vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Erfahren Sie mehr über `vserver nvme subsystem host remove` in der "ONTAP-Befehlsreferenz".

3. Überprüfen Sie, ob der Host aus dem Subsystem entfernt wurde:

```
vserver nvme subsystem host show
```

Erfahren Sie mehr über `vserver nvme subsystem host show` in der "ONTAP-Befehlsreferenz".

4. Fügen Sie den Host wieder dem Subsystem mit hoher Priorität hinzu:

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

Erfahren Sie mehr über `vserver nvme subsystem host add` in der "ONTAP-Befehlsreferenz".

#### Management der automatischen Hosterkennung von NVMe/TCP Controllern in ONTAP

Ab ONTAP 9.14.1 ist die Host-Erkennung von Controllern über das NVMe/TCP-Protokoll in IP-basierten Fabrics standardmäßig automatisiert.

##### Automatische Host-Erkennung von NVMe/TCP Controllern

Wenn Sie die automatische Hosterkennung zuvor deaktiviert haben, Ihre Anforderungen jedoch geändert haben, können Sie sie erneut aktivieren.

**Schritte**

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

2. Automatische Erkennung aktivieren:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Überprüfen Sie, ob die automatische Erkennung von NVMe/TCP-Controllern aktiviert ist.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

#### Deaktivieren Sie die automatische Host-Erkennung von NVMe/TCP-Controllern

Wenn NVMe/TCP-Controller nicht automatisch von Ihrem Host erkannt werden müssen und Sie unerwünschten Multicast-Datenverkehr in Ihrem Netzwerk erkennen, sollten Sie diese Funktion deaktivieren.

**Schritte**

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

2. Automatische Erkennung deaktivieren:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Vergewissern Sie sich, dass die automatische Erkennung von NVMe/TCP-Controllern deaktiviert ist.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

#### Deaktivieren Sie die Kennung der virtuellen NVMe-Host-Maschine in ONTAP

Ab ONTAP 9.14.1 unterstützt ONTAP standardmäßig die Möglichkeit von NVMe/FC-Hosts, Virtual Machines über eine eindeutige Kennung zu identifizieren und für NVMe/FC-Hosts die Auslastung der Virtual-Machine-Ressourcen zu überwachen. Dies verbessert die hostseitige Berichterstellung und Fehlerbehebung.

Sie können das Bootarg verwenden, um diese Funktion zu deaktivieren. Siehe die"NetApp Knowledge Base: So deaktivieren Sie die NVMe-Host-VM-Kennung in ONTAP" .

## Verwalten Sie Systeme mit FC-Adaptern

#### Verwalten Sie Systeme mit FC-Adaptern

Zur Verwaltung von integrierten FC-Adaptern und FC-Adapterkarten sind Befehle verfügbar. Mit diesen Befehlen können der Adaptermodus konfiguriert, Adapterinformationen angezeigt und die Geschwindigkeit geändert werden.

Die meisten Speichersysteme verfügen über integrierte FC-Adapter, die als Initiatoren oder Ziele konfiguriert werden können. Sie können auch FC-Adapterkarten verwenden, die als Initiatoren oder Ziele konfiguriert sind. Initiatoren stellen eine Verbindung zu Back-End-Festplattenregalen und möglicherweise zu externen Speicher-Arrays her. Ziele stellen nur eine Verbindung zu FC-Switches her. Sowohl die FC-Ziel-HBA-Ports als auch die Switch-Port-Geschwindigkeit sollten auf denselben Wert eingestellt sein und nicht auf „Auto“.

**Verwandte Informationen**

"SAN-Konfiguration"

### Befehle zum Verwalten von FC-Adaptern

Sie können FC-Befehle verwenden, um FC Target-Adapter, FC Initiator-Adapter und integrierte FC-Adapter für Ihren Storage Controller zu verwalten. Mit den gleichen Befehlen werden FC-Adapter für das FC-Protokoll und das FC-NVMe-Protokoll verwaltet.

Befehle für FC Initiator-Adapter funktionieren nur auf Node-Ebene. Sie müssen den `run -node node_name` Befehl verwenden, bevor Sie die FC-Initiator-Adapterbefehle verwenden können.

#### Befehle zum Verwalten von FC-Zieladaptern

| Ihr Ziel ist | Befehl |
|---|---|
| Zeigt FC-Adapterinformationen auf einem Node an | `network fcp adapter show` |
| Ändern Sie die FC-Zieladapterparameter | `network fcp adapter modify` |
| Zeigt Informationen zum FC-Protokoll-Datenverkehr an | `run -node node_name sysstat -f` |
| Anzeigen der Dauer des FC-Protokolls | `run -node node_name uptime` |
| Adapterkonfiguration und -Status anzeigen | `run -node node_name sysconfig -v adapter` |
| Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen | `run -node node_name sysconfig -ac` |
| Zeigen Sie eine man-Page für einen Befehl an | `man <command_name>` |

#### Befehle zum Verwalten von FC-Initiator-Adaptern

| Ihr Ziel ist | Befehl |
|---|---|
| Zeigt Informationen zu allen Initiatoren und ihren Adaptern in einem Node an | `run -node node_name storage show adapter` |
| Adapterkonfiguration und -Status anzeigen | `run -node node_name sysconfig -v adapter` |
| Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen | `run -node node_name sysconfig -ac` |

#### Befehle zum Verwalten der integrierten FC-Adapter

| Ihr Ziel ist | Befehl |
|---|---|
| Zeigt den Status der integrierten FC-Ports an | `run -node node_name system hardware unified-connect show` |

#### Verwandte Informationen

- "Netzwerk-fcp-Adapter"

### Konfigurieren Sie FC-Adapter

Jeder integrierte FC-Port kann individuell als Initiator oder Ziel konfiguriert werden. Die Ports auf bestimmten FC-Adaptern können auch einzeln als Ziel-Port oder als Initiator-Port konfiguriert werden, genau wie die integrierten FC-Ports. Eine Liste der Adapter, die für den Zielmodus konfiguriert werden können, finden Sie im "NetApp Hardware Universe".

Der Zielmodus wird verwendet, um die Ports mit FC-Initiatoren zu verbinden. Der Initiatormodus dient zum Verbinden der Ports mit Bandlaufwerken, Bandbibliotheken oder Drittanbieterspeichern mit Foreign LUN Import (FLI).

Bei der Konfiguration von FC-Adaptern für das FC-Protokoll und das FC-NVMe-Protokoll kommen die gleichen Schritte zum Einsatz. Jedoch unterstützen nur bestimmte FC-Adapter FC-NVMe. Im "NetApp Hardware Universe" finden Sie eine Liste mit Adaptern, die das FC-NVMe-Protokoll unterstützen.

#### Konfigurieren Sie FC-Adapter für den Zielmodus

**Schritte**

1. Versetzen Sie den Adapter in den Offline-Modus:

   `node run -node node_name storage disable adapter adapter_name`

   Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

2. Ändern Sie den Adapter von Initiator zu Ziel:

   `system hardware unified-connect modify -t target -node node_name adapter adapter_name`

3. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
4. Vergewissern Sie sich, dass der Zielport die richtige Konfiguration hat:

   `network fcp adapter show -node node_name`

   Erfahren Sie mehr über `network fcp adapter show` in der "ONTAP-Befehlsreferenz".

5. Schalten Sie Ihren Adapter online:

   `network fcp adapter modify -node node_name -adapter adapter_port -state up`

#### Konfigurieren Sie FC-Adapter für den Initiator-Modus

**Bevor Sie beginnen**

- LIFs auf dem Adapter müssen von allen Port-Sets, deren Mitglieder sie sind, entfernt werden.
- Alle LIFs von jeder Storage Virtual Machine (SVM), die den zu ändernden physischen Port verwendet, müssen migriert oder zerstört werden, bevor sie die Persönlichkeit des physischen Ports von Ziel zu Initiator ändern.

NVMe/FC unterstützt Initiatormodus.

**Schritte**

1. Entfernen Sie alle LIFs vom Adapter:

   `network interface delete -vserver SVM_name -lif LIF_name,LIF_name`

   Erfahren Sie mehr über `network interface delete` in der "ONTAP-Befehlsreferenz".

2. Versetzen Sie Ihren Adapter in den Offline-Modus:

   `network fcp adapter modify -node node_name -adapter adapter_port -status-admin down`

   Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

3. Ändern Sie den Adapter von Ziel zu Initiator:

   `system hardware unified-connect modify -t initiator adapter_port`

4. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
5. Vergewissern Sie sich, dass die FC-Ports für Ihre Konfiguration im richtigen Status konfiguriert sind:

   `system hardware unified-connect show`

6. Versetzen Sie den Adapter wieder in den Online-Modus:

   `node run -node node_name storage enable adapter adapter_port`

### Zeigen Sie Adaptereinstellungen an

Mit bestimmten Befehlen können Sie Informationen zu Ihren FC-/UTA-Adaptern anzeigen.

#### FC Target-Adapter

**Schritt**

1. Verwenden Sie den `network fcp adapter show` Befehl, um Adapterinformationen anzuzeigen:
   `network fcp adapter show -instance -node node1 -adapter 0a`

   Die Ausgabe zeigt für jeden verwendeten Steckplatz Informationen zur Systemkonfiguration und Adapterinformationen an.

Erfahren Sie mehr über `network fcp adapter show` in der "ONTAP-Befehlsreferenz".

#### Unified Target Adapter (UTA) X1143A-R6

**Schritte**

1. Starten Sie den Controller, ohne die angeschlossenen Kabel zu verwenden.
2. Führen Sie den `system hardware unified-connect show` Befehl aus, um die Portkonfiguration und Module anzuzeigen.
3. Zeigen Sie die Portinformationen an, bevor Sie den CNA und die Ports konfigurieren.

### Ändern Sie den UTA2-Port vom CNA-Modus in den FC-Modus

Sie sollten den UTA2-Port vom Converged Network Adapter (CNA)-Modus in den Fibre Channel (FC)-Modus ändern, um den FC-Initiator und den FC-Zielmodus zu unterstützen. Sie sollten die Persönlichkeit vom CNA-Modus in den FC-Modus ändern, wenn Sie das physische Medium ändern müssen, das den Port mit seinem Netzwerk verbindet.

**Schritte**

1. Versetzen Sie den Adapter in den Offline-Modus:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-status-admin down`

2. Ändern des Portmodus:

   `ucadmin modify -node` *`node_name`* `-adapter` *`adapter_name`* `-mode fcp`

3. Booten Sie den Node neu, und versetzen Sie den Adapter dann in den Online-Modus:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-status-admin up`

4. Benachrichtigen Sie den Administrator oder VIF-Manager, dass er den Port löschen oder entfernen soll, falls zutreffend:

   - Wenn der Port als Home Port einer logischen Schnittstelle verwendet wird, ist ein Mitglied einer Interface Group (ifgrp), oder Hosts VLANs, dann sollte ein Administrator Folgendes tun:

     i. Verschieben Sie die LIFs, entfernen Sie den Port aus dem ifgrp oder löschen Sie die VLANs.

     ii. Löschen Sie den Port manuell, indem Sie den `network port delete` Befehl ausführen.

     Wenn der `network port delete` Befehl fehlschlägt, sollte der Admin die Fehler beheben und dann den Befehl erneut ausführen.

   Erfahren Sie mehr über `network port delete` in der "ONTAP-Befehlsreferenz".

   - Wenn der Port nicht als Home-Port einer LIF verwendet wird, kein Mitglied eines ifgrp ist und keine VLANs hostet, dann sollte der VIF-Manager den Port zum Zeitpunkt des Neustarts aus seinen Datensätzen entfernen.

Wenn der VIF-Manager den Port nicht entfernt, muss der Administrator ihn nach dem Neubooten mit dem `network port delete` Befehl manuell entfernen.

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                          Speed(Mbps)
Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-
port

    vserver lif                  home-port curr-port
    ------- -------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
```

```
            cluster_mgmt           e0M       e0M
    net-f8040-34
            m                      e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

Erfahren Sie mehr über `network port show` in der "ONTAP-Befehlsreferenz".

5. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

   `network fcp adapter show -instance -node -adapter`

   Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Vor dem Ändern der Konfiguration auf dem Node sollten Sie für FC entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

   Erfahren Sie mehr über `network fcp adapter show` in der "ONTAP-Befehlsreferenz".

**Verwandte Informationen**

- "Netzwerkschnittstelle"

### Ändern Sie die optischen Module des CNA/UTA2-Zieladapters

Sie sollten die optischen Module auf dem Unified Target Adapter (CNA/UTA2) ändern, um den Personality-Modus zu unterstützen, den Sie für den Adapter ausgewählt haben.

**Schritte**

1. Überprüfen Sie das aktuelle SFP+, das in der Karte verwendet wird. Ersetzen Sie dann das aktuelle SFP+ durch das entsprechende SFP+ für die bevorzugte Persönlichkeit (FC oder CNA).
2. Entfernen Sie die aktuellen optischen Module vom X1143A-R6 Adapter.
3. Setzen Sie die richtigen Module für Ihre bevorzugte Personality-Mode-Optik (FC oder CNA) ein.
4. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Unterstützte SFP+-Module und Twinax-Kabel vom Cisco Logo (Copper Kabel) sind in *Hardware Universe* aufgeführt.

**Verwandte Informationen**

- "NetApp Hardware Universe"
- "Netzwerk-fcp-Adapter wird angezeigt"

### Unterstützte Portkonfigurationen für X1143A-R6 Adapter

Der FC-Zielmodus ist die Standardkonfiguration für X1143A-R6-Adapterports. Die Ports auf diesem Adapter können jedoch entweder als 10-Gbit-Ethernet- und FCoE-Ports oder als 16-Gbit-FC-Ports konfiguriert werden.

Bei Konfiguration für Ethernet und FCoE unterstützen X1143A-R6 Adapter gleichzeitigen NIC- und FCoE-Zielverkehr auf demselben 10-GBE-Port. Bei Konfiguration für FC kann jedes Paar mit zwei Ports, das denselben ASIC verwendet, individuell für das FC-Ziel oder den FC-Initiator-Modus konfiguriert werden. Das bedeutet, dass ein einzelner X1143A-R6 Adapter einen FC-Zielmodus auf einem Paar mit zwei Ports und einen FC-Initiator-Modus auf einem anderen Paar mit zwei Ports unterstützen kann.

**Verwandte Informationen**

"NetApp Hardware Universe"

"SAN-Konfiguration"

### Konfigurieren Sie die Ports

Um den Unified Target Adapter (X1143A-R6) zu konfigurieren, müssen die beiden benachbarten Ports auf demselben Chip im selben Personality-Modus konfiguriert werden.

**Schritte**

1. Konfigurieren Sie die Ports mit dem `system node hardware unified-connect modify` Befehl nach Bedarf für Fibre Channel (FC) oder Converged Network Adapter (CNA).
2. Schließen Sie die entsprechenden Kabel für FC- oder 10-Gbit-Ethernet an.
3. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Für FC sollten Sie basierend auf der FC-Fabric, mit der verbunden ist, entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

   Erfahren Sie mehr über `network fcp adapter show` in der "ONTAP-Befehlsreferenz".

### Vermeiden Sie den Verlust der Konnektivität bei Verwendung des X1133A-R6-Adapters

Sie können den Verlust der Konnektivität bei einem Port-Ausfall verhindern, indem Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfigurieren.

Der X1133A-R6 HBA ist ein 16 GB FC-Adapter mit 4 Ports, der aus zwei 2-Port-Paaren besteht. Der X1133A-R6 Adapter kann als Zielmodus oder Initiatormodus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (z. B. Port 1 und Port 2 auf ASIC 1 und Port 3 und Port 4 auf ASIC 2). Beide Ports auf einem einzelnen ASIC müssen für die Ausführung im gleichen Modus – entweder im Ziel- oder im Initiatormodus – konfiguriert werden. Wenn ein Fehler auftritt, bei dem der ASIC ein Paar unterstützt, werden beide Ports im Paar offline geschaltet.

Um diesen Verlust der Konnektivität zu vermeiden, konfigurieren Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden.

## Management von LIFs für alle SAN-Protokolle

### Management von LIFs für alle SAN-Protokolle

Initiatoren müssen für die Failover-Funktion von Clustern in einer SAN-Umgebung Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA) verwenden. Wenn ein Node ausfällt, migrieren LIFs nicht oder übernehmen keine IP-Adressen des ausgefallenen Partner-Node. Stattdessen ist die MPIO-Software mit ALUA auf dem Host für die Auswahl der entsprechenden Pfade für den LUN-Zugriff über LIFs verantwortlich.

Sie müssen von jedem Node in einem HA-Paar einen oder mehrere iSCSI-Pfade erstellen. Dazu verwenden Sie logische Schnittstellen (LIFs), um den Zugriff auf LUNs zu ermöglichen, die vom HA-Paar verarbeitet werden. Sie sollten eine Management-LIF für jede Storage Virtual Machine (SVM) konfigurieren, die SAN unterstützt.

Für die Konnektivität wird Direct Connect oder der Einsatz von Ethernet-Switches unterstützt. Sie müssen für beide Konnektivitätstypen LIFs erstellen.

- Sie sollten eine Management-LIF für jede Storage Virtual Machine (SVM) konfigurieren, die SAN unterstützt. Sie können zwei LIFs pro Node konfigurieren, eine für jede Fabric, die bei FC verwendet wird, und Ethernet-Netzwerke für iSCSI trennen.

Nach der Erstellung von LIFs können sie aus den Port-Sets entfernt, auf andere Nodes innerhalb einer Storage Virtual Machine (SVM) verschoben und gelöscht werden.

#### Verwandte Informationen

- "Konfiguration der LIFs – Übersicht"
- "Erstellen Sie eine LIF"

### LIF auf NVMe in ONTAP konfigurieren

Bei der Konfiguration von NVMe LIFs müssen bestimmte Anforderungen erfüllt werden.

#### Bevor Sie beginnen

NVMe muss von dem FC-Adapter unterstützt werden, auf dem Sie das LIF erstellen. Unterstützte Adapter sind in aufgeführt "Hardware Universe".

#### Über diese Aufgabe

Ab ONTAP 9.12.1 und höher können zwei NVMe LIFs pro Node auf maximal 12 Nodes konfiguriert werden. In ONTAP 9.11.1 und älteren Versionen können Sie zwei NVMe LIFs pro Node auf maximal zwei Nodes konfigurieren.

Beim Erstellen einer NVMe LIF gelten die folgenden Regeln:

- NVMe kann das einzige Datenprotokoll auf Daten-LIFs sein.
- Sie sollten eine Management-LIF für jede SVM konfigurieren, die SAN unterstützt.
- Bei ONTAP 9.5 und höher müssen Sie eine NVMe LIF auf dem Node, der den Namespace enthält, und auf dem HA-Partner des Node konfigurieren.
- Nur bei ONTAP 9.4:
  - NVMe LIFs und Namespaces müssen auf demselben Node gehostet werden.
  - Es kann nur eine NVMe-Daten-LIF pro SVM konfiguriert werden.

**Schritte**

1. Erstellen des LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

NVME/TCP ist ab ONTAP 9.10.1 und höher verfügbar.

2. Vergewissern Sie sich, dass das LIF erstellt wurde:

```
network interface show -vserver <SVM_name>
```

Nach der Erstellung achten NVMe/TCP LIFs auf die Erkennung an Port 8009.

**Verwandte Informationen**

- "Netzwerkschnittstelle"

### Was muss vor dem Verschieben einer SAN-LIF wissen

Sie müssen nur eine LIF-Verschiebung durchführen, wenn Sie den Inhalt des Clusters ändern, beispielsweise das Hinzufügen von Nodes zum Cluster oder das Löschen von Nodes aus dem Cluster. Wenn Sie eine LIF-Verschiebung durchführen, müssen Sie Ihre FC-Fabric nicht erneut Zone zuweisen oder neue iSCSI-Sitzungen zwischen den verbundenen Hosts Ihres Clusters und der neuen Zielschnittstelle erstellen.

Sie können keine SAN-LIF mit dem `network interface move` Befehl verschieben. SAN LIF-Verschiebung muss durchgeführt werden, indem die LIF offline geschaltet, die LIF zu einem anderen Home Node oder Port verschoben und anschließend an ihrem neuen Speicherort wieder online geschaltet wird. ALUA (Asymmetric Logical Unit Access) bietet redundante Pfade und automatische Pfadauswahl als Teil einer ONTAP SAN-Lösung. Daher gibt es keine I/O-Unterbrechung, wenn das LIF für die Verschiebung offline geschaltet wird. Der Host versucht einfach erneut, und verschiebt I/O dann zu einer anderen LIF.

Mithilfe der LIF-Verschiebung können Sie folgende Aufgaben unterbrechungsfrei ausführen:

- Ersetzen Sie ein HA-Paar eines Clusters durch ein aktualisiertes HA-Paar. Dies ist für Hosts, die auf LUN-

Daten zugreifen, transparent

- Aktualisieren einer Zielschnittstellenkarte
- Verschieben Sie die Ressourcen einer Storage Virtual Machine (SVM) von einem Node-Satz in einem Cluster zu einer anderen Gruppe von Nodes im Cluster

### Entfernen Sie ein SAN-LIF aus einem Portsatz

Wenn das LIF, das Sie löschen oder verschieben möchten, sich in einem Port-Satz befindet, müssen Sie die LIF aus dem Portsatz entfernen, bevor Sie die LIF löschen oder verschieben können.

#### Über diese Aufgabe

Sie müssen Schritt 1 im folgenden Verfahren nur ausführen, wenn sich eine LIF im Portsatz befindet. Sie können die letzte LIF nicht in einem Portsatz entfernen, wenn der Port-Satz an eine Initiatorgruppe gebunden ist. Andernfalls können Sie mit Schritt 2 beginnen, wenn sich mehrere LIFs im Port-Satz befinden.

#### Schritte

1. Wenn sich nur eine LIF im Portsatz befindet, `lun igroup unbind` lösen Sie die Bindung des Portsatz zur Initiatorgruppe mit dem Befehl.

   Wenn Sie die Bindung einer Initiatorgruppe von einem Portsatz aufheben, haben alle Initiatoren in der Initiatorgruppe Zugriff auf alle Ziel-LUNs, die der Initiatorgruppe auf allen Netzwerkschnittstellen zugeordnet sind.

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

   Erfahren Sie mehr über `lun igroup unbind` in der "ONTAP-Befehlsreferenz".

2. `lun portset remove`Entfernen Sie die LIF mit dem Befehl aus dem Portsatz.

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

   Erfahren Sie mehr über `lun portset remove` in der "ONTAP-Befehlsreferenz".

### Verschieben Sie ein SAN-LIF

Wenn ein Node offline geschaltet werden muss, können Sie eine SAN-LIF verschieben, um seine Konfigurationsinformationen wie seinen WWPN beizubehalten und zu vermeiden, das UmZoning der Switch-Fabric zu vermeiden. Da eine SAN LIF offline geschaltet werden muss, bevor sie verschoben wird, muss der Host-Traffic auf die Multipathing-Software des Hosts zurückgreifen, um einen unterbrechungsfreien Zugriff auf die LUN zu ermöglichen. Sie können SAN-LIFs auf beliebige Nodes in einem Cluster verschieben, jedoch können Sie die SAN-LIFs nicht zwischen Storage Virtual Machines (SVMs) verschieben.

#### Bevor Sie beginnen

Wenn die LIF Mitglied eines Port-Satzes ist, muss die LIF aus dem Portsatz entfernt worden sein, bevor die LIF zu einem anderen Node verschoben werden kann.

**Über diese Aufgabe**

Der Ziel-Node und der physische Port für eine LIF, die Sie verschieben möchten, müssen sich in derselben FC-Fabric oder einem Ethernet-Netzwerk befinden. Wenn Sie ein LIF auf ein anderes Fabric verschieben, das nicht richtig begrenzt wurde, oder wenn Sie ein LIF in ein Ethernet-Netzwerk verschieben, das keine Verbindung zwischen iSCSI-Initiator und Ziel hat, ist die LUN nicht zugänglich, wenn Sie sie wieder in den Online-Modus versetzen.

**Schritte**

1. Anzeigen des Administrations- und Betriebsstatus der LIF:

   `network interface show -vserver` *`vserver_name`*

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

2. Ändern Sie den Status der LIF in `down` (offline):

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-status-admin down`

   Erfahren Sie mehr über `network interface modify` in der "ONTAP-Befehlsreferenz".

3. Weisen Sie der LIF einen neuen Node und neuen Port zu:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-home-node` *`node_name`* `-home-port` *`port_name`*

4. Ändern Sie den Status des LIF in `up` (online):

   `network interface modify -vserver` *`vserver_name`* `-lif` *`LIF_name`* `-status-admin up`

   Erfahren Sie mehr über `up` in der "ONTAP-Befehlsreferenz".

5. Überprüfen Sie Ihre Änderungen:

   `network interface show -vserver` *`vserver_name`*

**Löschen eines LIF in einer SAN-Umgebung**

Bevor Sie eine LIF löschen, sollten Sie sicherstellen, dass der mit der LIF verbundene Host über einen anderen Pfad auf die LUNs zugreifen kann.

**Bevor Sie beginnen**

Wenn die LIF, die Sie löschen möchten, Mitglied eines Port-Satzes ist, müssen Sie zuerst die LIF aus dem Portsatz entfernen, bevor Sie die LIF löschen können.

**System Manager**

Löschen Sie ein LIF mit ONTAP System Manager (9.7 und höher).

**Schritte**

1. Klicken Sie in System Manager auf **Netzwerk > Übersicht** und wählen Sie dann **Netzwerkschnittstellen** aus.
2. Wählen Sie die Storage-VM aus, von der Sie die LIF löschen möchten.
3. Klicken Sie auf ⋮ und wählen Sie **Löschen**.

**CLI**

Löschen Sie ein LIF mit der ONTAP CLI.

**Schritte**

1. Überprüfen Sie den Namen der LIF und den aktuellen Port, der gelöscht werden soll:

   ```
   network interface show –vserver vserver_name
   ```

2. LIF löschen:

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

   Erfahren Sie mehr über `network interface delete` in der "ONTAP-Befehlsreferenz".

3. Vergewissern Sie sich, dass Sie die LIF gelöscht haben:

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical  Status     Network                       Current   Current Is
   Vserver  Interface  Admin/Oper Address/Mask       Node      Port
   Home
   -------  ---------- ---------- ----------------- --------- -------
   ----
   vs1
            lif2       up/up      192.168.2.72/24   node-01   e0b
   true
            lif3       up/up      192.168.2.73/24   node-01   e0b
   true
   ```

   Erfahren Sie mehr über `network interface show` in der "ONTAP-Befehlsreferenz".

### SAN LIF-Anforderungen zum Hinzufügen von Nodes zu einem Cluster

Beim Hinzufügen von Nodes zu einem Cluster müssen bestimmte Überlegungen beachtet werden.

- Sie müssen auf den neuen Nodes je nach Bedarf LIFs erstellen, bevor Sie LUNs auf den neuen Nodes erstellen.
- Sie müssen die LIFs von den Hosts gemäß den vom Host-Stack und Protokoll vorgegeben erkennen.
- Sie müssen auf den neuen Nodes LIFs erstellen, sodass die Verschiebung von LUNs und Volumes ohne Verwendung des Cluster Interconnect Netzwerks möglich ist.

### Konfigurieren Sie iSCSI-LIFs, um FQDN an den Host-iSCSI SendTargets Discovery-Vorgang zurückzugeben

Ab ONTAP 9 können iSCSI-LIFs so konfiguriert werden, dass ein vollständig qualifizierter Domain-Name (FQDN) zurückgegeben wird, wenn ein Host-Betriebssystem einen iSCSI-SendTargets-Ermittlungsvorgang sendet. Die Rückgabe eines FQDN ist nützlich, wenn zwischen dem Host-Betriebssystem und dem Speicherdienst ein NAT-Gerät (Network Address Translation) vorhanden ist.

#### Über diese Aufgabe

IP-Adressen auf einer Seite des NAT-Geräts sind auf der anderen Seite bedeutungslos, aber FQDNs können auf beiden Seiten Bedeutung haben.

> Die Interoperabilitätsgrenze für den FQDN-Wert beträgt 128 Zeichen auf allen Hostbetriebssystemen.

#### Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

   ```
   set -privilege advanced
   ```

2. Konfigurieren Sie iSCSI-LIFs für die Rückgabe von FQDN:

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   Im folgenden Beispiel sind die iSCSI-LIFs so konfiguriert, dass sie den FQDN storagehost-005.example.com zurückgeben.

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. Vergewissern Sie sich, dass sendtargets der FQDN ist:

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   In diesem Beispiel wird storagehost-005.example.com im Ausgabfeld sendtargets-fqdn angezeigt.

```
cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
sendtargets-fqdn
vserver lif        sendtargets-fqdn
------- ---------- --------------------------
vs1     vs1_iscsi1 storagehost-005.example.com
vs1     vs1_iscsi2 storagehost-006.example.com
```

**Verwandte Informationen**

"ONTAP-Befehlsreferenz"

## ONTAP-Speicherplatzzuweisung für SAN-Protokolle aktivieren

Die ONTAP Speicherplatzzuweisung ermöglicht Unternehmen, zu verhindern, dass die LUNs oder NVMe-Namespaces offline geschaltet werden, wenn ihnen der Speicherplatz knapp wird. So können die SAN-Hosts Speicherplatz zurückgewinnen.

Die ONTAP Unterstützung für die Speicherplatzzuweisung basiert auf Ihrem SAN-Protokoll und Ihrer Version von ONTAP. Ab ONTAP 9.16.1 ist die Speicherplatzzuweisung bei neu erstellten LUNs und allen Namespaces standardmäßig für iSCSI-, FC- und NVMe-Protokolle aktiviert.

| ONTAP-Version | Protokolle | Platzzuweisung ist… |
|---|---|---|
| 9.16.1 oder höher | • ISCSI<br>• FC<br>• NVMe | Standardmäßig aktiviert für neu erstellte LUNs und alle Namespaces |
| 9.15.1 | • ISCSI<br>• FC | Standardmäßig aktiviert für neu erstellte LUNs |
| | NVMe | Nicht unterstützt |
| 9.14.1 und früher | • ISCSI<br>• FC | Standardmäßig deaktiviert für neu erstellte LUNs |
| | NVMe | Nicht unterstützt |

Wenn die Speicherplatzzuweisung aktiviert ist:

- Wenn der Speicherplatz einer LUN oder eines Namespace knapp wird, kommuniziert ONTAP mit dem Host, dass kein freier Speicherplatz für Schreibvorgänge verfügbar ist. Infolgedessen bleibt die LUN oder der Namespace online und Lesevorgänge werden weiter ausgeführt. Je nach Host-Konfiguration versucht der Host, Schreibvorgänge erneut durchzuführen, bis sie erfolgreich sind, oder das Host-Dateisystem wird offline geschaltet. Die Schreibvorgänge werden wieder aufgenommen, wenn der LUN oder Namespace zusätzlicher freier Speicherplatz zur Verfügung steht.

  Wenn die Speicherplatzzuweisung nicht aktiviert ist und bei einer LUN oder einem Namespace der Speicherplatz knapp wird, schlagen alle I/O-Vorgänge fehl und die LUN oder der Namespace wird offline geschaltet. Das Speicherplatzproblem muss gelöst werden, um den normalen Betrieb fortzusetzen. Das

erneute Scannen von LUN-Geräten kann auch auf dem Host erforderlich sein, um Pfade und Geräte wieder in den Betriebszustand zu versetzen.

- Ein Host kann SCSI- oder NVME-Operationen (manchmal auch als bezeichnet `TRIM`) ausführen `UNMAP`. Durch UNMAP-Vorgänge kann ein Host Datenblöcke identifizieren, die nicht mehr benötigt werden, da sie keine gültigen Daten mehr enthalten. Die Identifizierung erfolgt normalerweise nach dem Löschen der Datei. Das Storage-System kann diese Datenblöcke dann Zuordnung aufheben, sodass der Speicherplatz an anderer Stelle verbraucht werden kann. Dieser Deallocation verbessert die gesamte Speichereffizienz erheblich, insbesondere bei Dateisystemen mit hohem Datenumsatz.

**Bevor Sie beginnen**

Für die Aktivierung der Speicherplatzzuweisung ist eine Host-Konfiguration erforderlich, die Fehler bei der Speicherplatzzuweisung korrekt verarbeiten kann, wenn ein Schreibvorgang nicht abgeschlossen werden kann. Die Nutzung von SCSI oder NVME `UNMAP` erfordert eine Konfiguration, die eine logische Blockbereitstellung gemäß dem SCSI SBC-3-Standard verwenden kann.

Die folgenden Hosts unterstützen derzeit Thin Provisioning, wenn Sie die Speicherplatzzuweisung aktivieren:

- Citrix XenServer 6.5 und höher
- VMware ESXi 5.0 und höher
- Oracle Linux 6.2 UEK-Kernel und höher
- Red hat Enterprise Linux 6.2 und höher
- SUSE Linux Enterprise Server 11 und höher
- Solaris 11.1 und höher
- Windows

**Über diese Aufgabe**

Wenn Sie das Cluster auf ONTAP 9.15.1 oder höher aktualisieren, bleibt die Einstellung für die Speicherplatzzuweisung für alle LUNs, die vor dem Software-Upgrade erstellt wurden, unabhängig vom Host-Typ nach dem Upgrade unverändert. Wenn beispielsweise eine LUN in ONTAP 9.13.1 für einen VMware Host erstellt wurde und die Speicherplatzzuweisung deaktiviert ist, bleibt die Speicherplatzzuweisung auf dieser LUN nach dem Upgrade auf ONTAP 9.15.1 deaktiviert.

**Schritte**

1. Speicherplatzzuweisung aktivieren:

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. Vergewissern Sie sich, dass die Speicherplatzzuweisung aktiviert ist:

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Vergewissern Sie sich, dass die Speicherplatzzuweisung auf dem Host-Betriebssystem aktiviert ist.

Einige Hostkonfigurationen, einschließlich einiger Versionen von VMware ESXi, können die Einstellungsänderung automatisch erkennen und erfordern keinen Benutzereingriff. Für andere Konfigurationen ist möglicherweise ein erneuter Gerätescan erforderlich. Einige Dateisysteme und Volume-Manager benötigen möglicherweise zusätzliche spezifische Einstellungen, um die Rückgewinnung von Speicherplatz mit `SCSI UNMAP`zu ermöglichen. Es kann erforderlich sein, Dateisysteme neu zu mounten oder ein vollständiges Betriebssystem neu zu starten. Weitere Informationen finden Sie in der Dokumentation zu Ihrem Host.

#### Hostkonfiguration für VMware ESXi 8.x und höhere NVMe-Hosts

Wenn auf einem VMware-Host ESXi 8.x oder höher mit dem NVMe-Protokoll ausgeführt wird, sollten Sie nach Aktivierung der Speicherplatzzuweisung in ONTAP die folgenden Schritte auf den Hosts durchführen.

**Schritte**

1. Stellen Sie auf Ihrem ESXi-Host sicher, dass DSM deaktiviert ist:

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   Der erwartete Wert ist 0.

2. Aktivieren Sie NVMe DSM:

   ```
   esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
   ```

3. Stellen Sie sicher, dass DSM aktiviert ist:

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   Der erwartete Wert ist 1.

**Weiterführende Links**

Erfahren Sie mehr über "NVMe-of Hostkonfiguration für ESXi 8.x mit ONTAP".

## Empfohlene Kombinationen aus Volume- und Datei- oder LUN-Konfiguration

#### Überblick über Empfohlene Kombinationen aus Volume- und Datei- oder LUN-Konfiguration

Je nach Applikations- und Administrationsanforderungen können bestimmte Kombinationen aus FlexVol Volume- und Datei- oder LUN-Konfigurationen verwendet werden. Wenn Sie die Vorteile und Kosten dieser Kombinationen verstehen, können Sie bestimmt werden, welche Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung geeignet ist.

Die folgenden Kombinationen aus Volume- und LUN-Konfigurationen werden empfohlen:

- Speicherreservierte Dateien oder LUNs mit Thick Volume Provisioning
- Dateien oder LUNs ohne Speicherplatz mit Thin Volume Provisioning
- Speicherreservierte Dateien oder LUNs mit semi-Thick Volume Provisioning

Sie können SCSI Thin Provisioning auf Ihren LUNs in Verbindung mit einer dieser Konfigurationskombinationen verwenden.

#### Speicherreservierte Dateien oder LUNs mit Thick Volume Provisioning

**Vorteile:**

- Alle Schreibvorgänge innerhalb von platzsparenden Dateien sind garantiert. Aufgrund eines unzureichenden Speicherplatzes werden sie nicht ausfallen.
- Es gibt keine Beschränkungen für die Storage-Effizienz und Datensicherungstechnologien auf dem Volume.

**Kosten und Einschränkungen:**

- Es muss genügend Speicherplatz vom Aggregat im Voraus reserviert werden, um das Thick Provisioning-Volume zu unterstützen.
- Der Speicherplatz, der der doppelten Größe der LUN entspricht, wird zum Zeitpunkt der Erstellung des LUN vom Volume zugewiesen.

#### Dateien oder LUNs ohne Speicherplatz mit Thin Volume Provisioning

**Vorteile:**

- Es gibt keine Beschränkungen für die Storage-Effizienz und Datensicherungstechnologien auf dem Volume.
- Der Speicherplatz wird nur dann zugewiesen, wenn er genutzt wird.

**Kosten und Einschränkungen:**

- Schreibvorgänge sind nicht garantiert; sie können ausfallen, wenn dem Volume der freie Speicherplatz ausgeht.
- Sie müssen den freien Speicherplatz im Aggregat effektiv verwalten, um zu verhindern, dass dem Aggregat der freie Speicherplatz knapp wird.

#### Speicherreservierte Dateien oder LUNs mit semi-Thick Volume Provisioning

**Vorteile:**

Im Vorfeld wird weniger Speicherplatz als bei der Bereitstellung von Thick Volumes reserviert, und eine Schreibgarantie für besten Aufwand ist weiterhin verfügbar.

**Kosten und Einschränkungen:**

- Bei dieser Option können Schreibvorgänge fehlschlagen.

  Dieses Risiko können Sie mindern, indem Sie den freien Speicherplatz im Volume angemessen mit Volatilität abgleichen.

- Sie können sich nicht auf die Aufbewahrung von Datensicherheitsobjekten wie Snapshots, FlexClone-Dateien und LUNs verlassen.
- ONTAP Storage-Effizienzfunktionen zur gemeinsamen Blocknutzung sind nicht zulässig, die automatisch gelöscht werden können, einschließlich Deduplizierung, Komprimierung und ODX/Copy Offload.

### Ermitteln Sie die richtige Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung

Durch das Beantworten einiger grundlegender Fragen zu Ihrer Umgebung können Sie die beste Konfiguration von FlexVol Volumes und LUNs für Ihre Umgebung ermitteln.

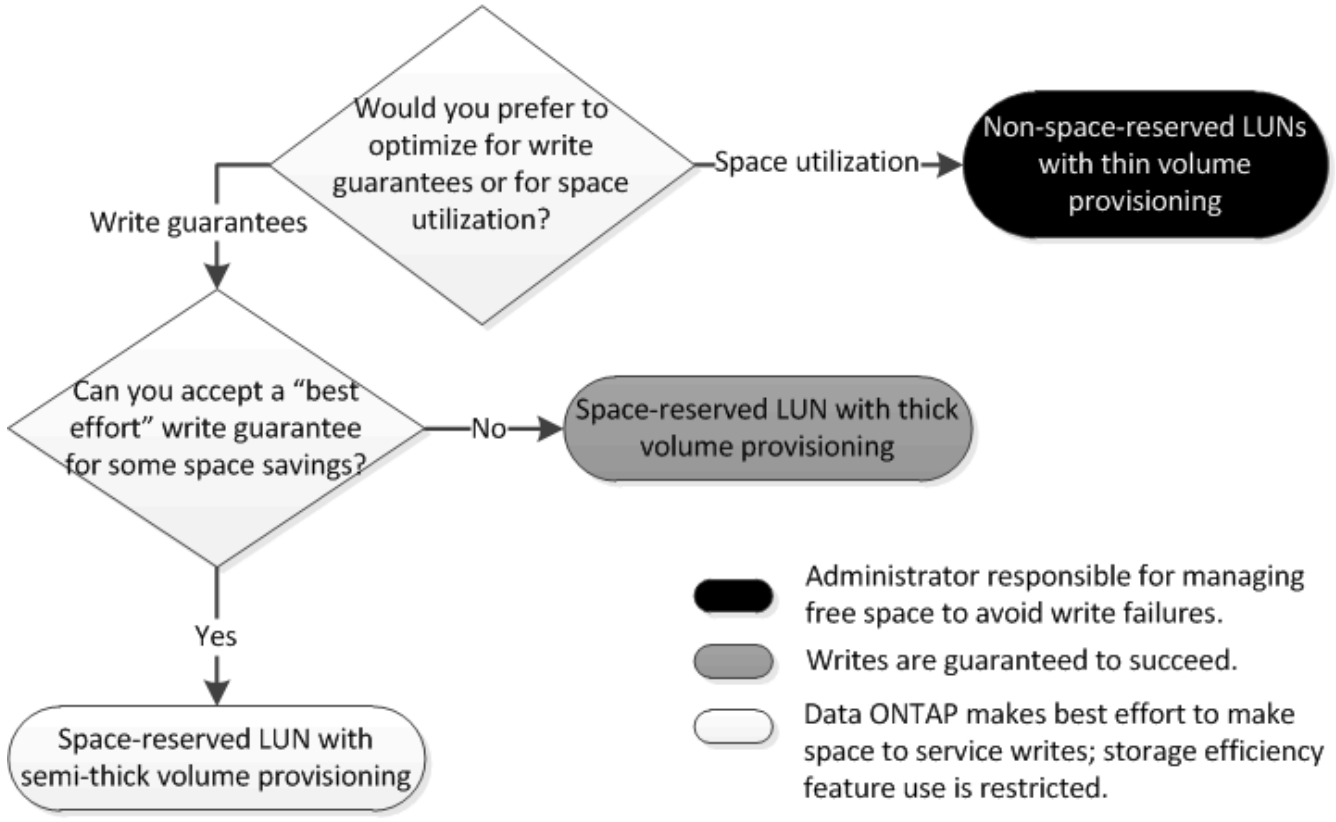
#### Über diese Aufgabe

Sie können LUN- und Volume-Konfigurationen für maximale Storage-Auslastung und für die Sicherheit von Schreibgarantien optimieren. Basierend auf Ihren Anforderungen an die Storage-Auslastung und der Möglichkeit, freien Speicherplatz schnell zu überwachen und aufzufüllen, müssen Sie das FlexVol Volume und die LUN-Volumes bestimmen, die für Ihre Installation geeignet sind.

Sie brauchen kein separates Volume für jede LUN.

#### Schritt

1. Verwenden Sie den folgenden Entscheidungsbaum, um die beste Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung zu ermitteln:




### Berechnen der Datenwachstumsrate für LUNs

Sie müssen die Geschwindigkeit kennen, mit der die LUN-Daten im Laufe der Zeit wachsen, um zu ermitteln, ob Sie platzsparende LUNs oder nicht-platzsparende LUNs verwenden sollten.

#### Über diese Aufgabe

Wenn Sie eine konstant hohe Datenwachstumsrate haben, dann sind platzreservierte LUNs möglicherweise die bessere Option für Sie. Wenn Ihre Datenwachstumsrate niedrig ist, sollten Sie nicht-Speicherplatz-reservierte LUNs in Erwägung ziehen.

Mit Tools wie OnCommand Insight können Sie die Datenwachstumsrate berechnen oder sie manuell berechnen. Die folgenden Schritte sind für die manuelle Berechnung.

**Schritte**

1. Richten Sie eine LUN ein, die Speicherplatz reserviert hat.
2. Überwachen Sie die Daten auf der LUN für einen bestimmten Zeitraum, z. B. für eine Woche.

   Stellen Sie sicher, dass Ihr Überwachungszeitraum lang genug ist, um eine repräsentative Auswahl der regelmäßig auftretenden zunehmenden Datenmengen zu bilden. So wachsen die Datenmengen z. B. am Ende eines jeden Monats durchgängig sehr stark an.

3. Notieren Sie jeden Tag in GB, wie viele Daten wachsen.
4. Fügen Sie am Ende des Überwachungszeitraums die Gesamtbeträge für jeden Tag zusammen ein, und teilen Sie sie dann nach der Anzahl der Tage in Ihrem Überwachungszeitraum.

   Diese Berechnung bringt Ihre durchschnittliche Wachstumsrate mit sich.

**Beispiel**

In diesem Beispiel benötigen Sie eine LUN mit 200 GB. Sie entscheiden sich, die LUN für eine Woche zu überwachen und die folgenden täglichen Datenänderungen aufzuzeichnen:

- Sonntag: 20 GB
- Montag: 18 GB
- Dienstag: 17 GB
- Mittwoch: 20 GB
- Donnerstag: 20 GB
- Freitag: 23 GB
- Samstag: 22 GB

In diesem Beispiel beträgt Ihre Wachstumsrate (20+18+17+20+20+23+22) / 7 = 20 GB pro Tag.

**Konfigurationseinstellungen für platzreservierte Dateien oder LUNs mit Thick Provisioning Volumes**

Diese Kombination aus FlexVol-Konfigurationen für Volumes und Dateien oder LUNs bietet die Möglichkeit, Storage-Effizienztechnologien zu nutzen. Sie müssen Ihren freien Speicherplatz nicht aktiv überwachen, da vorab ausreichend Speicherplatz zugewiesen wird.

Die folgenden Einstellungen sind erforderlich, um eine speziell für den Speicherplatz reservierte Datei oder ein LUN in einem Volume mit Thick Provisioning zu konfigurieren:

| Lautstärkereinstellung | Wert |
|---|---|
| Garantie | Datenmenge |
| Fraktionale Reserve | 100 |
| Snapshot Reserve | Alle |

| Lautstärkereinstellung | Wert |
| --- | --- |
| Snapshot wird automatisches Löschen erstellt | Optional |
| Autogrow | Optional; bei Aktivierung muss der freie Speicherplatz des Aggregats aktiv überwacht werden. |

| Datei- oder LUN-Einstellung | Wert |
| --- | --- |
| Speicherplatzreservierung | Aktiviert |

#### Konfigurationseinstellungen für Dateien oder LUNs, die nicht über Speicherplatz reserviert sind, mit Thin Provisioning Volumes

Diese Kombination aus FlexVol-Volume- und Datei- oder LUN-Konfiguration erfordert die kleinste Storage-Menge im Voraus. Es erfordert jedoch aktives, freies Speicherplatzmanagement, um Fehler aufgrund von mangelndem Speicherplatz zu vermeiden.

Folgende Einstellungen sind erforderlich, um eine Datei oder ein LUN ohne Speicherplatz in einem Volume mit Thin Provisioning zu konfigurieren:

| Lautstärkereinstellung | Wert |
| --- | --- |
| Garantie | Keine |
| Fraktionale Reserve | 0 |
| Snapshot Reserve | Alle |
| Snapshot wird automatisches Löschen erstellt | Optional |
| Autogrow | Optional |

| Datei- oder LUN-Einstellung | Wert |
| --- | --- |
| Speicherplatzreservierung | Deaktiviert |

##### Weitere Überlegungen

Wenn der Speicherplatz des Volume oder Aggregats knapp wird, können Schreibvorgänge für die Datei oder LUN ausfallen.

Wenn Sie den freien Speicherplatz nicht sowohl für das Volume als auch für das Aggregat aktiv überwachen möchten, sollten Sie Autogrow für das Volume aktivieren und die maximale Größe für das Volume auf die Größe des Aggregats festlegen. In dieser Konfiguration müssen Sie den freien Speicherplatz des Aggregats aktiv überwachen, den freien Speicherplatz im Volume jedoch nicht überwachen.

#### Konfigurationseinstellungen für platzreservierte Dateien oder LUNs mit semi-Thick Volume Provisioning

Für diese Kombination aus Volume- und Datei- oder LUN-Konfiguration von FlexVol muss vorab weniger Storage zugewiesen werden als für die vollständig bereitgestellte Kombination. Es beschränkt jedoch die Effizienztechnologien, die Sie für das Volume verwenden können. Überschreibungen werden auf optimaler Basis dieser Konfigurationskombination erfüllt.

Die folgenden Einstellungen sind erforderlich, um eine reservierte LUN in einem Volume mit semi-Thick Provisioning zu konfigurieren:

| Lautstärkereinstellung | Wert |
|---|---|
| Garantie | Datenmenge |
| Fraktionale Reserve | 0 |
| Snapshot Reserve | 0 |
| Snapshot wird automatisches Löschen erstellt | Bei einem Commit-Level der Zerstörung eine Liste mit allen Objekten, dem auf Volume eingestellten Auslöser und allen FlexClone LUNs und FlexClone Dateien für das automatische Löschen aktiviert. |
| Autogrow | Optional; bei Aktivierung muss der freie Speicherplatz des Aggregats aktiv überwacht werden. |

| Datei- oder LUN-Einstellung | Wert |
|---|---|
| Speicherplatzreservierung | Aktiviert |

##### Technologische Beschränkungen

Sie können für diese Kombination nicht die folgenden Volume-Storage-Effizienztechnologien verwenden:

- Komprimierung
- Deduplizierung
- ODX und FlexClone Copy Offload
- FlexClone LUNs und FlexClone Dateien nicht zum automatischen Löschen markiert (aktive Klone)
- Unterdateien von FlexClone
- ODX/Copy-Offload

##### Weitere Überlegungen

Beim Einsatz dieser Konfigurationskombination müssen die folgenden Fakten beachtet werden:

- Wenn das Volume, das diese LUN unterstützt, über wenig Speicherplatz verfügt, werden Sicherungsdaten

(FlexClone-LUNs und -Dateien, Snapshots) zerstört.

- Schreibvorgänge können rechtzeitig ausfallen, wenn der freie Speicherplatz auf dem Volume erschöpft ist.

Die Komprimierung ist für AFF Plattformen standardmäßig aktiviert. Sie müssen die Komprimierung explizit für jedes Volume deaktivieren, für das Sie semi-Thick Provisioning auf einer AFF Plattform verwenden möchten.

# SAN Datensicherung

## Informieren Sie sich über Datensicherungsmethoden von ONTAP für SAN-Umgebungen

Sie können Ihre Daten schützen, indem Sie Kopien davon erstellen, sodass sie bei versehentlichem Löschen, Applikationsabstürzen, Datenbeschädigung oder Ausfällen für eine Wiederherstellung verfügbar sind. Je nach Datensicherungs- und Backup-Anforderungen bietet ONTAP verschiedene Methoden zum Schutz Ihrer Daten.

### SnapMirror Active Sync

Ab ONTAP 9.9 ist diese allgemeine Verfügbarkeit mit Zero Recovery Time Objective (RTO von Null) oder transparentem Applikations-Failover (TAF) möglich und ermöglicht ein automatisches Failover geschäftskritischer Applikationen in SAN-Umgebungen. Für SnapMirror Active Sync ist die Installation von ONTAP Mediator 1.2 in einer Konfiguration mit zwei AFF-Clustern oder zwei All Flash ASA-Clustern erforderlich.

"SnapMirror Active Sync"

### Snapshot

Ermöglicht Ihnen die manuelle oder automatische Erstellung, Planung und Verwaltung mehrerer Backups Ihrer LUNs. Snapshots benötigen nur einen minimalen zusätzlichen Volume-Speicherplatz und verursachen keine Performance-Kosten. Werden Ihre LUN-Daten versehentlich geändert oder gelöscht, können diese Daten einfach und schnell aus einem der neuesten Snapshots wiederhergestellt werden.

### FlexClone LUNs (FlexClone Lizenz erforderlich)

Bietet zeitpunktgenaue, beschreibbare Kopien einer anderen LUN in einem aktiven Volume oder einem Snapshot. Ein Klon und sein übergeordnetes Objekt können unabhängig voneinander geändert werden, ohne dass sich gegenseitig beeinträchtigen.

### SnapRestore (Lizenz erforderlich)

Ermöglicht eine schnelle, platzsparende Wiederherstellung von Daten nach Bedarf aus Snapshots eines gesamten Volumes. Mit SnapRestore können Sie eine LUN auf einen früheren Zustand wiederherstellen, ohne das Storage-System neu zu booten.

### Datensicherung Spiegelungskopien (SnapMirror Lizenz erforderlich)

Sorgt für asynchrone Disaster Recovery, indem es Ihnen ermöglicht, regelmäßig Snapshots von Daten auf Ihrem Volume zu erstellen, diese Snapshots über ein lokales oder Wide Area Network auf ein Partner-Volume zu kopieren, in der Regel auf einem anderen Cluster, und diese Snapshots beizubehalten. Die gespiegelte Kopie auf dem Partner-Volume sorgt für schnelle Verfügbarkeit und Wiederherstellung von Daten aus dem Zeitpunkt des letzten Snapshots, wenn die Daten auf dem Quell-Volume beschädigt oder verloren sind.

#### SnapVault Backups (SnapMirror Lizenz erforderlich)

Ermöglicht eine effiziente und langfristige Aufbewahrung von Backups. SnapVault Beziehungen ermöglichen Ihnen, ausgewählte Snapshots von Volumes auf einem Ziel-Volume zu sichern und die Backups beizubehalten.

Falls Sie Tape-Backups und Archivierungsvorgänge durchführen, können Sie sie auch für die Daten ausführen, die bereits auf dem sekundären SnapVault Volume gesichert sind.

#### SnapDrive für Windows oder UNIX (SnapDrive-Lizenz erforderlich)

Konfiguration des LUN-Zugriffs, Management von LUNs und Management von Snapshots des Storage-Systems direkt von einem Windows- oder UNIX-Host aus

#### Natives Tape-Backup und -Recovery

Die meisten vorhandenen Bandlaufwerke werden in ONTAP unterstützt und ebenfalls eine Methode für Tape-Anbieter, um neue Geräte dynamisch zu unterstützen. ONTAP unterstützt außerdem das Remote Magnetic Tape (RMT)-Protokoll und ermöglicht so Backup und Recovery für jedes fähige System.

#### Verwandte Informationen

"NetApp Dokumentation: SnapDrive für UNIX" "NetApp Dokumentation: SnapDrive für Windows (aktuelle Versionen)" "Datensicherung mithilfe von Tape Backup"

## Stellen Sie eine einzelne LUN aus einem ONTAP-Snapshot wieder her

Sie können eine einzelne LUN aus einem Snapshot wiederherstellen, ohne das gesamte Volume wiederherzustellen, das die einzelne LUN enthält. Sie können die LUN selbst oder einen neuen Pfad im Volume wiederherstellen. Der Vorgang stellt nur die einzelne LUN wieder her, ohne dass andere Dateien oder LUNs im Volume beeinträchtigt werden. Sie können Dateien auch mit Streams wiederherstellen.

#### Bevor Sie beginnen

- Sie müssen genügend Speicherplatz auf Ihrem Volume haben, um den Wiederherstellungsvorgang abzuschließen:
  - Wenn Sie eine platzreservierte LUN wiederherstellen, wo die fraktionale Reserve 0% beträgt, benötigen Sie ein Mal die Größe der wiederhergestellten LUN.
  - Wenn Sie eine platzreservierte LUN wiederherstellen, wo die fraktionale Reserve 100% beträgt, benötigen Sie die doppelte Größe der wiederhergestellten LUN.
  - Wenn Sie eine nicht-speicherreservierte LUN wiederherstellen, benötigen Sie nur den tatsächlich für die wiederhergestellte LUN verwendeten Speicherplatz.
- Es muss ein Snapshot der Ziel-LUN erstellt worden sein.

  Wenn der Wiederherstellungsvorgang fehlschlägt, kann die Ziel-LUN gekürzt werden. In solchen Fällen können Sie den Snapshot verwenden, um Datenverlust zu vermeiden.

- Es muss ein Snapshot der Quell-LUN erstellt worden sein.

  In seltenen Fällen kann die LUN-Wiederherstellung fehlschlagen, sodass die Quell-LUN nicht mehr verwendet werden kann. In diesem Fall können Sie den Snapshot verwenden, um die LUN kurz vor der Wiederherstellung in den Status zurückzusetzen.

- Die Ziel-LUN und die Quell-LUN müssen den gleichen OS-Typ aufweisen.

  Wenn die Ziel-LUN einen anderen OS-Typ als die Quell-LUN aufweist, kann der Host nach der Wiederherstellung den Datenzugriff auf die Ziel-LUN verlieren.

**Schritte**

1. Beenden Sie vom Host den gesamten Host-Zugriff auf die LUN.
2. Heben Sie die Bereitstellung der LUN auf dem Host auf, damit der Host nicht auf die LUN zugreifen kann.
3. LUN-Zuordnung aufheben:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. Legen Sie den Snapshot fest, den Sie für die Wiederherstellung der LUN verwenden möchten:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Erstellen Sie vor dem Wiederherstellen der LUN einen Snapshot der LUN:

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. Stellen Sie die angegebene LUN in einem Volume wieder her:

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. Befolgen Sie die Schritte auf dem Bildschirm.
8. Versetzen Sie die LUN bei Bedarf in den Online-Modus:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. Falls erforderlich, LUN erneut zuordnen:

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. Mounten Sie die LUN vom Host neu.
11. Starten Sie den Zugriff auf die LUN vom Host aus neu.

## Stellen Sie alle LUNs in einem Volume aus einem ONTAP-Snapshot wieder her

Mit dem Befehl können Sie `volume snapshot restore` alle LUNs in einem angegebenen Volume aus einem Snapshot wiederherstellen.

**Schritte**

1. Beenden Sie vom Host den gesamten Host-Zugriff auf die LUNs.

   Die Verwendung von SnapRestore ohne die Unterbrechung des gesamten Host-Zugriffs auf LUNs im Volume kann zu Datenbeschädigungen und Systemfehlern führen.

2. Heben Sie die Bereitstellung der LUNs auf diesem Host auf, damit der Host nicht auf die LUNs zugreifen kann.
3. LUNs-Zuordnung aufheben:

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. Bestimmen Sie den Snapshot, auf dem Sie Ihr Volume wiederherstellen möchten:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Ändern Sie Ihre Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

6. Wiederherstellen von Daten:

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

7. Befolgen Sie die Anweisungen auf dem Bildschirm.
8. LUNs neu zuordnen:

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. Vergewissern Sie sich, dass Ihre LUNs online sind:

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. Wenn Ihre LUNs nicht online sind, bringen Sie sie in den Online-Modus:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. Ändern Sie Ihre Berechtigungseinstellung in admin:

```
set -privilege admin
```

12. Mounten Sie die LUNs vom Host neu.
13. Starten Sie den Zugriff auf Ihre LUNs vom Host aus neu.

## Sichern Sie Ihre Daten mit ONTAP FlexClone LUNs

Eine FlexClone-LUN ist eine zeitpunktgenaue, beschreibbare Kopie einer anderen LUN in einem aktiven Volume oder in einem Snapshot. Der Klon und sein übergeordnetes Objekt können unabhängig voneinander geändert werden, ohne dass sich gegenseitig beeinflussen.

Sie können FlexClone LUNs verwenden, um mehrere Kopien einer LUN mit Lese-/Schreibvorgängen zu erstellen.

**Gründe für das Erstellen von FlexClone LUNs**

- Sie müssen eine temporäre Kopie einer LUN zu Testzwecken erstellen.
- Sie müssen zusätzlichen Benutzern eine Kopie der Daten zugänglich machen, ohne ihnen den Zugang zu den Produktionsdaten zu ermöglichen.
- Sie möchten einen Klon einer Datenbank für Manipulationen und Hochrechnungen erstellen, während die ursprünglichen Daten in unveränderter Form beibehalten werden.
- Sie möchten auf eine bestimmte Untergruppe der Daten einer LUN zugreifen (ein bestimmtes logisches Volume oder Dateisystem in einer Volume-Gruppe, Oder eine bestimmte Datei oder einen bestimmten Dateisatz in einem Dateisystem) und ihre ursprüngliche LUN kopieren, ohne den Rest der Daten in der ursprünglichen LUN wiederherzustellen. Dies funktioniert auf Betriebssystemen, die das gleichzeitige Mounten einer LUN und eines Klons der LUN unterstützen. SnapDrive für UNIX unterstützt dies mit dem `snap connect` Befehl.
- Sie benötigen mehrere SAN-Boot-Hosts mit demselben Betriebssystem.

Eine FlexClone LUN verwendet zunächst den Speicherplatz der übergeordneten LUN. Standardmäßig übernimmt die FlexClone LUN das space-reservierte Attribut der übergeordneten LUN. Wenn beispielsweise die übergeordnete LUN keinen Speicherplatz reserviert ist, ist die FlexClone LUN standardmäßig auch nicht-Speicherplatz-reserviert. Sie können jedoch eine FlexClone LUN erstellen, die nicht im Speicherplatz reserviert ist, von einem übergeordneten Objekt, das eine reservierte LUN ist.

Beim Klonen einer LUN erfolgt die Blockfreigabe im Hintergrund. Sie können erst dann einen Volume-Snapshot erstellen, wenn die Blockfreigabe abgeschlossen ist.

Sie müssen das Volume so konfigurieren, dass die automatische Löschfunktion der FlexClone-LUN mit dem `volume snapshot autodelete modify` Befehl aktiviert wird. Wenn FlexClone LUNs automatisch gelöscht werden sollen, das Volume jedoch nicht für das automatische Löschen von FlexClone konfiguriert ist, wird keine der FlexClone LUNs gelöscht.

Wenn Sie eine FlexClone LUN erstellen, ist die automatische Löschung der FlexClone LUN standardmäßig deaktiviert. Sie müssen sie auf jeder FlexClone LUN manuell aktivieren, bevor die FlexClone LUN automatisch gelöscht werden kann. Wenn Sie die semi-Thick Volume-Bereitstellung nutzen und Sie die „`Best Effort`"-Garantie von dieser Option erhalten möchten, müssen Sie *all* FlexClone LUNs für das automatische Löschen zur Verfügung stellen.

> Wenn Sie eine FlexClone-LUN aus einem Snapshot erstellen, wird die LUN automatisch aus dem Snapshot mithilfe eines platzsparenden Hintergrundprozesses aufgeteilt, sodass die LUN nicht weiter vom Snapshot abhängt oder zusätzlicher Speicherplatz verbraucht wird. Wenn diese Hintergrundspaltung nicht abgeschlossen wurde und dieser Snapshot automatisch gelöscht wird, wird die FlexClone-LUN gelöscht, selbst wenn Sie die automatische FlexClone-Löschfunktion für diese FlexClone-LUN deaktiviert haben. Nach Abschluss der Hintergrundspaltung wird die FlexClone LUN nicht gelöscht, auch wenn dieser Snapshot gelöscht wird.

**Verwandte Informationen**

- "Erstellen Sie eine FlexClone-LUN"
- "Konfigurieren Sie eine FlexVol volume zum automatischen Löschen von FlexClone-LUNs"
- "Verhindern Sie, dass eine FlexClone LUN automatisch gelöscht wird"

## Konfigurieren und verwenden Sie SnapVault Backups in einer SAN-Umgebung

### Erfahren Sie mehr über ONTAP SnapVault Backups in einer SAN-Umgebung

Die Konfiguration und der Einsatz von SnapVault in einer SAN-Umgebung sind ähnlich der Konfiguration und dem Einsatz in einer NAS-Umgebung. Die Wiederherstellung von LUNs in einer SAN-Umgebung erfordert jedoch einige spezielle Verfahren.

SnapVault Backups enthalten einen Satz schreibgeschützter Kopien eines Quell-Volumes. In einer SAN-Umgebung sichern Sie immer ganze Volumes auf dem sekundären SnapVault Volume, nicht auf individuellen LUNs.

Das Verfahren zum Erstellen und Initialisieren der SnapVault-Beziehung zwischen einem primären Volume mit LUNs und einem sekundären Volume, das als SnapVault Backup fungiert, ist identisch mit dem Verfahren, das mit FlexVol Volumes für Dateiprotokolle verwendet wird. Dieses Verfahren wird ausführlich in beschrieben"Datensicherung".

Es ist wichtig, dass die gesicherten LUNs einen konsistenten Zustand aufweisen, bevor die Snapshots erstellt und auf das sekundäre SnapVault Volume kopiert werden. Die Automatisierung der Snapshot-Erstellung mit SnapCenter stellt sicher, dass gesicherte LUNs vollständig und von der ursprünglichen Applikation nutzbar sind.

Es gibt drei grundlegende Möglichkeiten für die Wiederherstellung von LUNs aus einem sekundären SnapVault-Volume:

- Eine LUN kann direkt vom sekundären SnapVault Volume zugeordnet werden und einen Host mit der LUN verbinden, um auf die Inhalte der LUN zuzugreifen.

  Die LUN ist schreibgeschützt, und Sie können nur dem letzten Snapshot im SnapVault-Backup zuordnen. Persistente Reservierungen und andere LUN-Metadaten gehen verloren. Bei Bedarf können Sie den LUN-Inhalt mit einem Kopierprogramm auf dem Host zurück auf die ursprüngliche LUN kopieren, sofern der Zugriff weiterhin möglich ist.

Die LUN verfügt über eine andere Seriennummer als die Quell-LUN.

- Sie können jeden Snapshot im sekundären SnapVault-Volume auf ein neues Lese-/Schreibvolume klonen.

  Anschließend können Sie jede der LUNs im Volume zuordnen und einen Host mit der LUN verbinden, um auf die Inhalte der LUN zuzugreifen. Bei Bedarf können Sie den LUN-Inhalt mit einem Kopierprogramm auf dem Host zurück auf die ursprüngliche LUN kopieren, sofern der Zugriff weiterhin möglich ist.

- Sie können das gesamte Volume, das die LUN enthält, von jedem beliebigen Snapshot im sekundären SnapVault-Volume wiederherstellen.

  Beim Wiederherstellen des gesamten Volume werden alle LUNs und alle Dateien im Volume ersetzt. Alle neuen LUNs, die seit der Snapshot-Erstellung erstellt wurden, gehen verloren.

  Die LUNs behalten ihre Zuordnung, Seriennummern, UUIDs und ihre persistenten Reservierungen bei.

#### Zugriff auf eine schreibgeschützte LUN-Kopie aus einem ONTAP SnapVault Backup

Sie können aus dem letzten Snapshot in einem SnapVault-Backup auf eine schreibgeschützte Kopie einer LUN zugreifen. Die LUN-ID, der Pfad und die Seriennummer unterscheiden sich von der Quell-LUN und müssen zuerst zugeordnet werden. Persistente Reservierungen, LUN-Zuordnungen und Initiatorgruppen werden nicht auf das sekundäre SnapVault Volume repliziert.

##### Bevor Sie beginnen

- Die SnapVault-Beziehung muss initialisiert werden, und der neueste Snapshot im sekundären SnapVault-Volume muss die gewünschte LUN enthalten.
- Die Storage Virtual Machine (SVM), die das SnapVault Backup enthält, muss über einen oder mehrere LIFs verfügen, wobei das gewünschte SAN-Protokoll über den Host zugänglich ist, der für den Zugriff auf die LUN-Kopie verwendet wird.
- Wenn Sie einen direkten Zugriff auf LUN-Kopien vom sekundären SnapVault Volume planen, müssen Sie vorab Ihre Initiatorgruppen auf der SnapVault SVM erstellen.

  Sie können direkt vom sekundären SnapVault Volume auf eine LUN zugreifen, ohne dass zuerst das Volume mit der LUN wiederhergestellt oder geklont werden muss.

##### Über diese Aufgabe

Wenn dem sekundären SnapVault-Volume ein neuer Snapshot hinzugefügt wird, während eine LUN aus einem vorherigen Snapshot zugeordnet ist, ändert sich der Inhalt der zugeordneten LUN. Die LUN ist weiterhin mit denselben Kennungen zugeordnet, die Daten werden jedoch aus dem neuen Snapshot entnommen. Wenn sich die LUN-Größe ändert, erkennen einige Hosts automatisch die Größenänderung. Windows Hosts müssen nach einem Festplatten-Rescan suchen, um eventuelle Größenänderungen einzuholen.

##### Schritte

1. Listen Sie die verfügbaren LUNs im sekundären SnapVault-Volume auf.

   ```
   lun show
   ```

   In diesem Beispiel sehen Sie sowohl die ursprünglichen LUNs im primären Volume srcvolA als auch die

Kopien im sekundären SnapVault Volume dstvolB:

```
cluster::> lun show

Vserver   Path                 State   Mapped   Type          Size
--------  -----------------    ------  -------  --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

Erfahren Sie mehr über `lun show` in der "ONTAP-Befehlsreferenz".

2. Wenn die Initiatorgruppe für den gewünschten Host auf der SVM, die das sekundäre SnapVault Volume enthält, nicht bereits vorhanden ist, erstellen Sie eine Initiatorgruppe.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

Mit diesem Befehl wird eine Initiatorgruppe für einen Windows Host erstellt, der das iSCSI-Protokoll verwendet:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. Ordnen Sie die gewünschte LUN-Kopie der Initiatorgruppe zu.

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

Erfahren Sie mehr über `lun mapping create` in der "ONTAP-Befehlsreferenz".

4. Verbinden Sie den Host mit der LUN, und greifen Sie nach Bedarf auf die Inhalte der LUN zu.

### Wiederherstellung einer einzelnen LUN aus einem ONTAP SnapVault-Backup

Sie können eine einzelne LUN an einem neuen Speicherort oder am ursprünglichen Speicherort wiederherstellen. Sie können von einem beliebigen Snapshot im sekundären SnapVault-Volume wiederherstellen. Um die LUN am ursprünglichen Speicherort wiederherzustellen, stellen Sie sie zuerst an einem neuen Speicherort wieder her und kopieren sie dann.

#### Bevor Sie beginnen

- Die SnapVault-Beziehung muss initialisiert werden und das sekundäre SnapVault-Volume muss einen geeigneten Snapshot für die Wiederherstellung enthalten.
- Die Storage Virtual Machine (SVM), die das sekundäre SnapVault Volume enthält, muss über eine oder mehrere LIFs mit dem gewünschten SAN-Protokoll verfügen, auf die der Host zum Zugriff auf die LUN-Kopie zugreifen kann.
- Die Initiatorgruppen müssen auf der SnapVault SVM bereits vorhanden sein.

#### Über diese Aufgabe

Der Prozess umfasst die Erstellung eines Volume-Klons mit Lese- und Schreibzugriffen aus einem Snapshot auf dem sekundären SnapVault Volume. Sie können die LUN direkt aus dem Klon verwenden oder den LUN-Inhalt optional wieder an den ursprünglichen Speicherort der LUN kopieren.

Die LUN im Klon verfügt über einen anderen Pfad und eine andere Seriennummer als die ursprüngliche LUN. Persistente Reservierungen werden nicht beibehalten.

#### Schritte

1. Überprüfen Sie das sekundäre Volume, das das SnapVault-Backup enthält.

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                         Snapmirrored
                                 Idle       -         true    -
```

2. Geben Sie den Snapshot an, aus dem Sie die LUN wiederherstellen möchten.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. Erstellen Sie aus dem gewünschten Snapshot einen Lese-/Schreibklon

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

Der Volume-Klon wird im selben Aggregat erstellt wie der SnapVault Backup. Im Aggregat muss genügend Speicherplatz vorhanden sein, um den Klon zu speichern.

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Listen Sie die LUNs im Volume-Klon auf.

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

Erfahren Sie mehr über `lun show` in der "ONTAP-Befehlsreferenz".

5. Wenn die Initiatorgruppe für den gewünschten Host auf der SVM, die das SnapVault-Backup enthält, nicht vorhanden ist, erstellen Sie eine Initiatorgruppe.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

Dieses Beispiel erstellt eine Initiatorgruppe für einen Windows Host, der das iSCSI-Protokoll verwendet:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. Ordnen Sie die gewünschte LUN-Kopie der Initiatorgruppe zu.

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

Erfahren Sie mehr über `lun mapping create` in der "ONTAP-Befehlsreferenz".

7. Verbinden Sie den Host mit der LUN und greifen Sie nach Bedarf auf den Inhalt der LUN zu.

   Die LUN ist Lese- und Schreib-LUN, die anstelle der ursprünglichen LUN verwendet werden kann. Da die LUN-Seriennummer sich unterscheidet, interpretiert der Host sie als eine andere LUN als das Original.

8. Verwenden Sie ein Kopierprogramm auf dem Host, um den LUN-Inhalt zurück auf die ursprüngliche LUN zu kopieren.

**Verwandte Informationen**

- "Snapmirror-Show"

#### Stellen Sie alle LUNs in einem Volume aus einem ONTAP SnapVault-Backup wieder her

Wenn eine oder mehrere LUNs in einem Volume aus einem SnapVault Backup wiederhergestellt werden müssen, können Sie das gesamte Volume wiederherstellen. Die Wiederherstellung des Volumes wirkt sich auf alle LUNs im Volume aus.

**Bevor Sie beginnen**

Die SnapVault-Beziehung muss initialisiert werden und das sekundäre SnapVault-Volume muss einen geeigneten Snapshot für die Wiederherstellung enthalten.

**Über diese Aufgabe**

Wenn Sie ein ganzes Volume wiederherstellen, wird das Volume in den Zustand zurückversetzt, in dem es sich zum Zeitpunkt der Erstellung des Snapshots befand. Wenn nach dem Snapshot eine LUN zum Volume hinzugefügt wurde, wird diese LUN während der Wiederherstellung entfernt.

Nach dem Wiederherstellen des Volumes bleiben die LUNs den Initiatorgruppen zugeordnet, denen sie kurz vor der Wiederherstellung zugeordnet wurden. Die LUN-Zuordnung kann sich zum Zeitpunkt des Snapshots von der Zuordnung unterscheiden. Persistente Reservierungen auf den LUNs von Host-Clustern bleiben erhalten.

**Schritte**

1. Stoppen Sie den I/O für alle LUNs im Volume.
2. Überprüfen Sie das sekundäre Volume, das das sekundäre SnapVault-Volume enthält.

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                         Snapmirrored
                                 Idle       -         true    -
```

3. Geben Sie den Snapshot an, von dem Sie wiederherstellen möchten.

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. Geben Sie den zu verwendenden Snapshot an.

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

Das Ziel, das Sie für die Wiederherstellung angeben, ist das ursprüngliche Volume, auf dem Sie wiederherstellen.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Wenn Sie LUNs über ein Host-Cluster hinweg gemeinsam nutzen, stellen Sie die persistenten Reservierungen auf den LUNs von den betroffenen Hosts wieder her.

#### Wiederherstellen eines Volumes aus einem SnapVault-Backup

Im folgenden Beispiel wurde die LUN mit dem Namen „lun_D“ dem Volume hinzugefügt, nachdem der Snapshot erstellt wurde. Nach der Wiederherstellung des gesamten Volumes aus dem Snapshot wird lun_D nicht mehr angezeigt.

In der `lun show` Befehlsausgabe des Befehls können Sie die LUNs im primären Volume srcvolA und die schreibgeschützten Kopien dieser LUNs im sekundären SnapVault Volume dstvolB sehen. Es gibt keine Kopie von lun_D im SnapVault Backup.

```
cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than snapshot hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                  State   Mapped   Type          Size
--------- ------------------    ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

Nachdem das Volume aus dem sekundären SnapVault Volume wiederhergestellt wurde, enthält das Quell-Volume nicht mehr lun_D. Sie müssen die LUNs im Quell-Volume nach der Wiederherstellung nicht neu zuordnen, da sie noch zugeordnet sind.

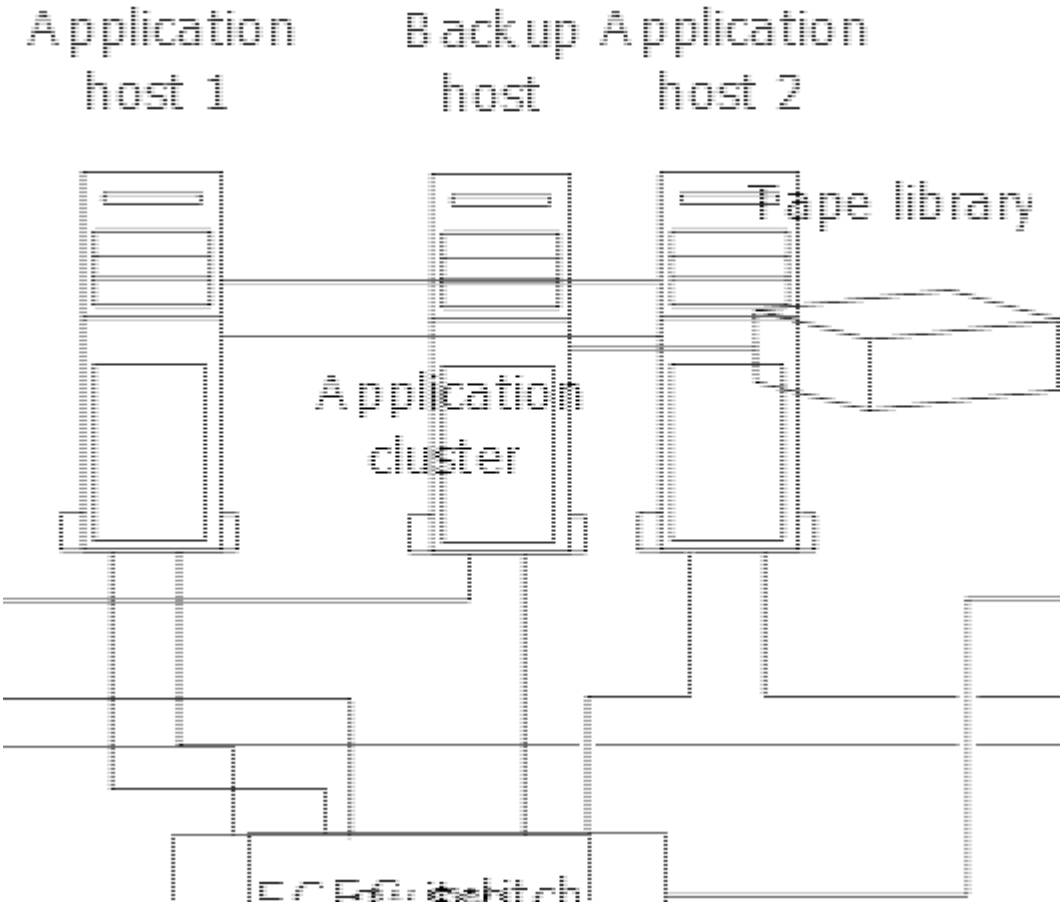
**Verwandte Informationen**

- "snapmirror Wiederherstellung"
- "Snapmirror-Show"

## Empfohlene Konfiguration für den Anschluss eines Host-Backup-Systems an ONTAP

Sie können SAN-Systeme über einen separaten Backup-Host auf Tape sichern, um Performance-Einbußen beim Applikations-Host zu vermeiden.

Es muss zwingend notwendig sein, dass SAN- und NAS-Daten für Backup-Zwecke getrennt gehalten werden. Die Abbildung unten zeigt die empfohlene physische Konfiguration für ein Host-Backup-System auf dem primären Speichersystem. Sie müssen Volumes nur als SAN konfigurieren. LUNs sind auf ein einzelnes Volume beschränkt oder die LUNs können über mehrere Volumes oder Storage-Systeme verteilt werden.




Volumes auf einem Host können aus einer einzelnen LUN bestehen, die vom Storage-System zugeordnet ist, oder aus mehreren LUNs mit einem Volume Manager, wie VxVM auf HP-UX Systemen.

## Verwenden Sie ein Host-Backup-System, um eine LUN auf Ihrem ONTAP-Speichersystem zu schützen

Sie können eine geklonte LUN aus einem Snapshot als Quelldaten für das Host-Backup-System verwenden.

#### Bevor Sie beginnen

Eine Produktions-LUN muss vorhanden sein und einer Initiatorgruppe zugeordnet sein, die den WWPN oder den Initiator-Node-Namen des Applikationsservers enthält. Außerdem muss die LUN formatiert sein und auf den Host zugreifen können

#### Schritte

1. Speichern Sie den Inhalt der Puffer des Host-Filesystems auf der Festplatte.

   Sie können den von Ihrem Host-Betriebssystem bereitgestellten Befehl verwenden oder SnapDrive für Windows oder SnapDrive für UNIX verwenden. Sie können auch entscheiden, diesen Schritt in Ihr SAN-Backup-Vorverarbeitungsskript einzutragen.

2. Erstellen Sie einen Snapshot der Produktions-LUN.

   ```
   volume snapshot create -vserver <SVM_name> -volume <volume_name>
   -snapshot <snapshot> -comment <comment> -foreground false
   ```

3. Erstellen Sie einen Klon der Produktions-LUN.

   ```
   volume file clone create -vserver <SMV_name> -volume <volume> -source
   -path <path> -snapshot-name <snapshot> -destination-path
   <destination_path>
   ```

4. Erstellen Sie eine Initiatorgruppe, die den WWPN des Backup-Servers enthält.

   ```
   lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
   <protocol> -ostype <os_type> -initiator <initiator>
   ```

5. Ordnen Sie den in Schritt 3 erstellten LUN-Klon dem Backup-Host zu.

   ```
   lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
   <lun_name> -igroup <igroup>
   ```

   Sie können diesen Schritt in das Post-Processing-Skript Ihrer SAN-Backup-Applikation einarbeiten.

6. Erkennen Sie vom Host die neue LUN und stellen Sie das Dateisystem dem Host zur Verfügung.

   Sie können diesen Schritt in das Post-Processing-Skript Ihrer SAN-Backup-Applikation einarbeiten.

7. Sichern Sie die Daten im LUN-Klon vom Backup-Host zum Tape mithilfe Ihrer SAN-Backup-Applikation.
8. Versetzen Sie den LUN-Klon in den Offline-Modus.

   ```
   lun modify -vserver <SVM_name> -path <path> -state offline
   ```

9. Entfernen Sie den LUN-Klon.

   ```
   lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
   ```

10. Entfernen Sie den Snapshot.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

# Referenz zur SAN-Konfiguration

## Erfahren Sie mehr über die ONTAP-SAN-Konfiguration

Ein Storage Area Network (SAN) besteht aus einer Storage-Lösung, die über ein SAN-Transportprotokoll wie iSCSI oder FC mit Hosts verbunden ist. Sie können Ihr SAN so konfigurieren, dass Ihre Speicherlösung über einen oder mehrere Switches mit Ihren Hosts verbunden wird. Wenn Sie iSCSI verwenden, können Sie Ihr SAN auch so konfigurieren, dass Ihre Speicherlösung ohne einen Switch direkt an Ihren Host angeschlossen wird.

In einem SAN können mehrere Hosts mit verschiedenen Betriebssystemen, wie Windows, Linux oder UNIX, gleichzeitig auf die Storage-Lösung zugreifen. Mit "Selektive LUN-Zuordnung" und können "Portsätze"Sie den Datenzugriff zwischen den Hosts und dem Speicher einschränken.

Bei iSCSI wird die Netzwerktopologie zwischen der Speicherlösung und den Hosts als Netzwerk bezeichnet. Bei FC, FC/NVMe und FCoE wird die Netzwerktopologie zwischen der Storage-Lösung und den Hosts als Fabric bezeichnet. Um Redundanz zu schaffen, die Sie vor dem Verlust des Datenzugriffs schützt, sollten Sie Ihr SAN mit HA-Paaren in einer Multi-Netzwerk- oder Multi-Fabric-Konfiguration einrichten. Konfigurationen mit einzelnen Knoten oder einzelnen Netzwerken/Fabrics sind nicht vollständig redundant und daher nicht empfohlen.

Nachdem Ihr SAN konfiguriert ist, können Sie "Bereitstellen von Storage für iSCSI oder FC", oder Sie können "Storage für FC/NVMe bereitstellen". Anschließend können Sie eine Verbindung zu Ihren Hosts herstellen, um mit der Datenpflege zu beginnen.

Die Unterstützung der SAN-Protokolle variiert abhängig von Ihrer Version von ONTAP, Ihrer Plattform und Ihrer Konfiguration. Weitere Informationen zu Ihrer spezifischen Konfiguration finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

**Verwandte Informationen**

- "ÜBERSICHT ÜBER DIE SAN-Administration"
- "Konfiguration, Support und Einschränkungen von NVMe"

## ISCSI-Konfigurationen

### Konfigurieren Sie iSCSI-Netzwerke mit ONTAP-Systemen

Sie sollten Ihre iSCSI-Konfiguration mit Hochverfügbarkeitspaaren (HA) einrichten, die direkt mit Ihren iSCSI-SAN-Hosts verbunden sind oder die über einen oder mehrere IP-Switches eine Verbindung zu Ihren Hosts herstellen.

"HA-Paare" Sind definiert als die Reporting-Nodes für die aktiv/optimiert und die aktiv/nicht optimierten Pfade, die von den Hosts für den Zugriff auf die LUNs verwendet werden. Mehrere Hosts, die verschiedene Betriebssysteme verwenden, wie z. B. Windows, Linux oder UNIX, können gleichzeitig auf den Storage

zugreifen. Hosts erfordern die Installation und Konfiguration einer unterstützten Multipathing-Lösung, die ALUA unterstützt. Unterstützte Betriebssysteme und Multipathing-Lösungen können auf der überprüft werden"NetApp Interoperabilitäts-Matrix-Tool".

In einer Konfiguration mit mehreren Netzwerken gibt es zwei oder mehr Switches, die die Hosts mit dem Speichersystem verbinden. Mehrere Netzwerkkonfigurationen werden empfohlen, da sie vollständig redundant sind. In einer Konfiguration mit einem einzigen Netzwerk gibt es einen Switch, der die Hosts mit dem Speichersystem verbindet. Einzelnetzwerkkonfigurationen sind nicht vollständig redundant.

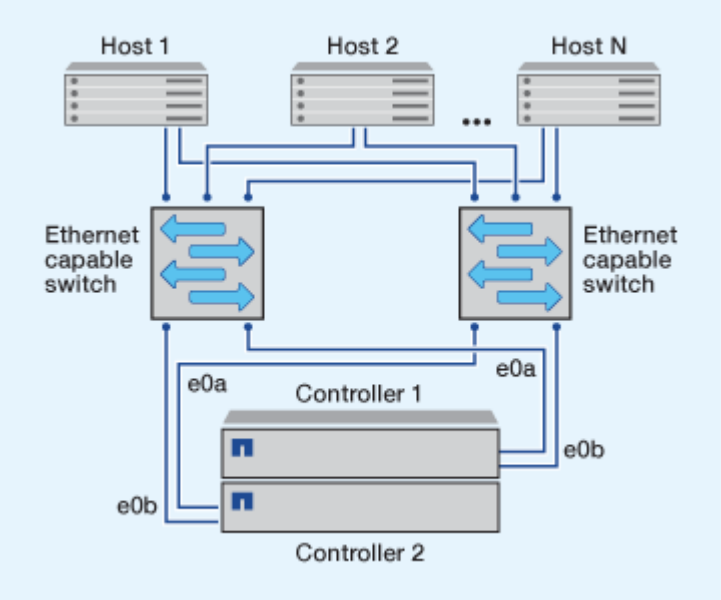
"Single-Node-Konfigurationen" Die Empfehlungen sind nicht empfehlenswert, da sie nicht die Redundanz bieten, die zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb erforderlich ist.

**Verwandte Informationen**

- Erfahren Sie, wie "Selektive LUN-Zuordnung (SLM)" beschränkt die Pfade, die für den Zugriff auf die LUNs eines HA-Paars verwendet werden.
- Erfahren Sie mehr über "SAN LIFs".
- Erfahren Sie mehr über "Vorteile von VLANs in iSCSI".

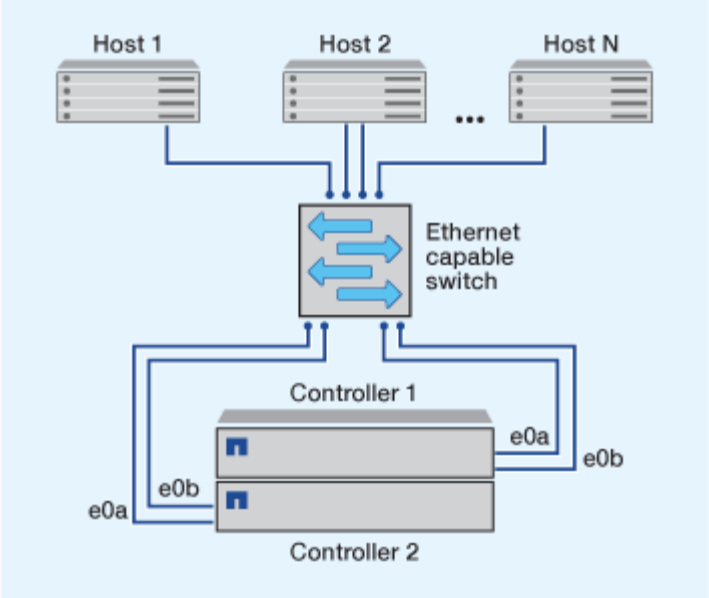
#### ISCSI-Konfigurationen mit mehreren Netzwerken

Bei HA-Paar-Konfigurationen mit mehreren Netzwerken verbinden zwei oder mehr Switches das HA-Paar mit einem oder mehreren Hosts. Da es mehrere Switches gibt, ist diese Konfiguration vollständig redundant.



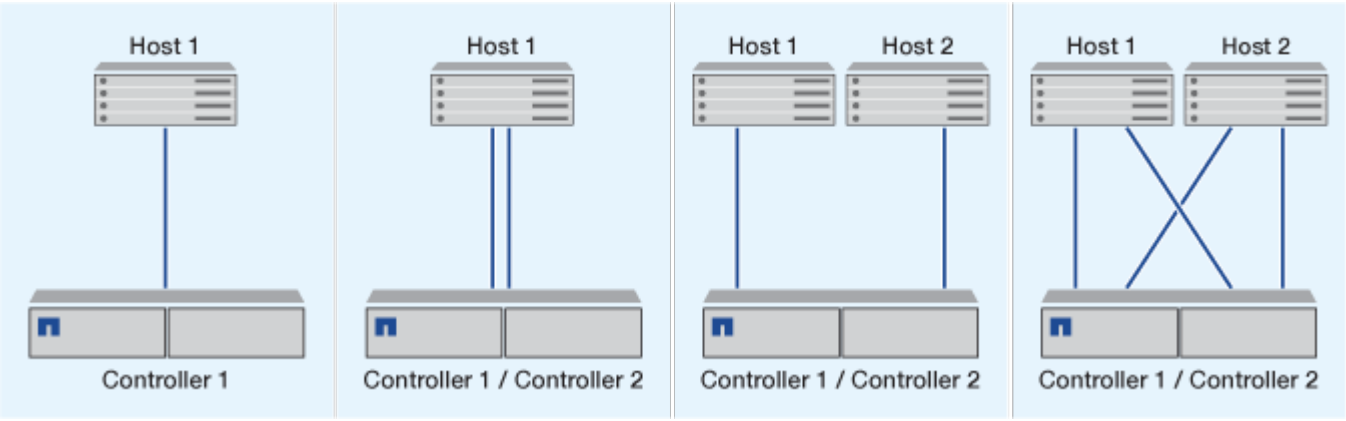

#### ISCSI-Konfigurationen mit einem Netzwerk

Bei Einzel-Netzwerk-HA-Paar-Konfigurationen verbindet ein Switch das HA-Paar mit einem oder mehreren Hosts. Da es einen einzelnen Switch gibt, ist diese Konfiguration nicht vollständig redundant.




**Konfiguration von Direct-Attachment-iSCSI**

In einer Direct-Attached-Konfiguration sind ein oder mehrere Hosts direkt mit den Controllern verbunden.




**Vorteile der Verwendung von VLANs mit ONTAP-Systemen in iSCSI-Konfigurationen**

Ein VLAN besteht aus einer Gruppe von Switch-Ports, die zu einer Broadcast-Domäne gruppiert sind. Ein VLAN kann sich auf einem einzelnen Switch befinden oder sich über mehrere Switch-Chassis erstrecken. Statische und dynamische VLANs ermöglichen die Erhöhung der Sicherheit, die Isolierung von Problemen und die Begrenzung verfügbarer Pfade innerhalb der IP-Netzwerkinfrastruktur.

Bei der Implementierung von VLANs in großen IP-Netzwerkinfrastrukturen ergeben sich folgende Vorteile:

- Erhöhte Sicherheit:

  Mit VLANs können Sie die vorhandene Infrastruktur nutzen und zugleich größere Sicherheit bieten, da sie den Zugriff auf verschiedene Nodes eines Ethernet-Netzwerks oder IP SAN beschränken.

- Verbesserte Zuverlässigkeit des Ethernet-Netzwerks und des IP SAN durch Isolierung von Problemen
- Verringerung der Problemlösungszeit durch Beschränkung des problematischen Speicherplatzes

- Reduzierung der Anzahl der verfügbaren Pfade zu einem bestimmten iSCSI-Zielport.
- Reduzierung der maximalen Anzahl von Pfaden, die von einem Host verwendet werden

  Dass zu viele Pfade die Verbindungszeiten verlangsamen. Wenn ein Host nicht über eine Multipathing-Lösung verfügt, können Sie VLANs verwenden, um nur einen Pfad zuzulassen.

#### Dynamische VLANs

Dynamische VLANs basieren auf MAC-Adressen. Sie können ein VLAN definieren, indem Sie die MAC-Adresse der Mitglieder angeben, die Sie aufnehmen möchten.

Dynamische VLANs bieten Flexibilität und sind nicht auf die physischen Ports angewiesen, an denen das Gerät physisch mit dem Switch verbunden ist. Sie können ein Kabel von einem Port in den anderen umstecken, ohne das VLAN neu zu konfigurieren.

#### Statische VLANs

Statische VLANs sind portbasiert. Der Switch und der Switch Port werden verwendet, um das VLAN und seine Mitglieder zu definieren.

Statische VLANs bieten verbesserte Sicherheit, da es nicht möglich ist, VLANs durch MAC-Spoofing (Media Access Control) zu durchbrechen. Wenn jedoch jemand physischen Zugang zum Switch hat, kann der Zugriff durch den Austausch eines Kabels und die Neukonfiguration der Netzwerkadresse möglich sein.

In manchen Umgebungen ist es einfacher, statische VLANs zu erstellen und zu managen als dynamische VLANs. Dies liegt daran, dass bei statischen VLANs nur die Switch- und Port-ID angegeben werden muss, anstatt die 48-Bit-MAC-Adresse. Darüber hinaus können Sie Switch-Portbereiche mit der VLAN-Kennung kennzeichnen.

## FC-Konfigurationen

#### Konfigurieren Sie FC- oder FC-NVME-Fabrics mit ONTAP-Systemen

Es wird empfohlen, Ihre FC- und FC-NVMe-SAN-Hosts über HA-Paare und mindestens zwei Switches zu konfigurieren. Sie bietet Redundanz auf Fabric- und Storage-Systemebene zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb. Sie können FC- oder FC-NVMe-SAN-Hosts nicht ohne Switch direkt an HA-Paare anschließen.

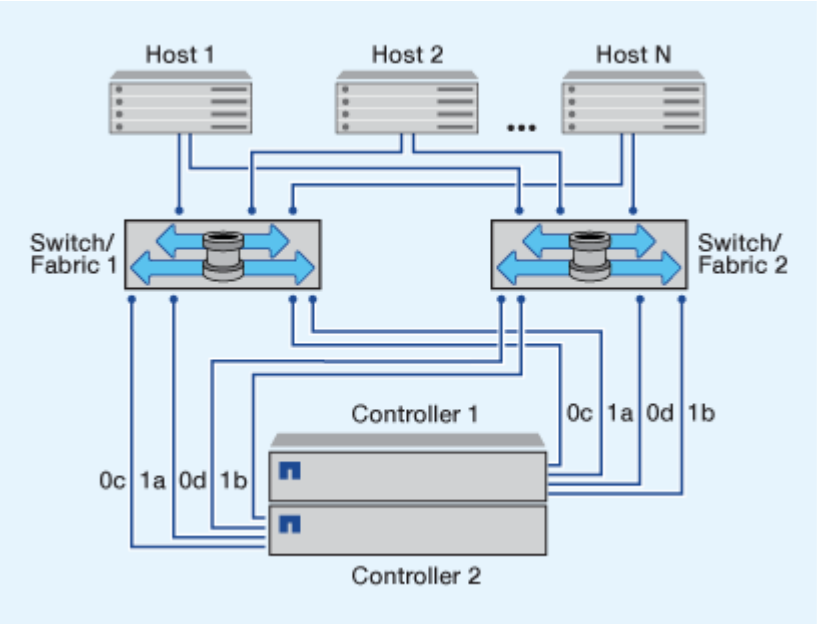
Kaskadierung, partielles Mesh, volles Mesh, Core-Edge und Director Fabrics sind branchenübliche Methoden, FC Switches mit einem Fabric zu verbinden. Alle werden unterstützt. Die Verwendung heterogener FC Switch Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches. Spezifische Ausnahmen sind auf der aufgeführt"Interoperabilitäts-Matrix-Tool". Eine Fabric kann aus einem oder mehreren Switches bestehen und die Storage-Controller mit mehreren Switches verbunden werden.

Mehrere Hosts, die verschiedene Betriebssysteme verwenden, z. B. Windows, Linux oder UNIX, können gleichzeitig auf die Storage Controller zugreifen. Hosts erfordern, dass eine unterstützte Multipathing-Lösung installiert und konfiguriert ist. Unterstützte Betriebssysteme und Multipathing-Lösungen können im Interoperabilitäts-Matrix-Tool verifiziert werden.

#### Multi-Fabric-FC- und FC-NVMe-Konfigurationen

In Multi-Fabric HA-Paar-Konfigurationen gibt es mindestens zwei Switches, die HA-Paare mit einem oder mehreren Hosts verbinden. Der Einfachheit halber werden im folgenden HA-Paar mit mehreren Fabrics nur zwei gezeigt, doch in jeder Multi-Fabric-Konfiguration können mindestens zwei Fabrics vorhanden sein.

Die FC-Ziel-Port-Nummern (0c, 0d, 1a, 1b) in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern variieren je nach Modell des Storage-Node und ob Sie Erweiterungsadapter verwenden.

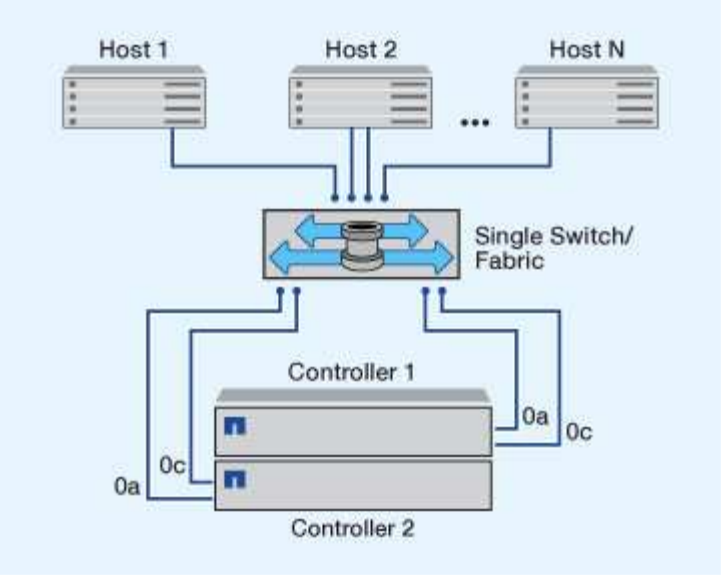



#### FC- und FC-NVMe-Konfigurationen in einem Fabric

Bei Einzel-Fabric-HA-Paar-Konfigurationen besteht ein Fabric, das beide Controller im HA-Paar mit einem oder mehreren Hosts verbindet. Da die Hosts und Controller über einen einzelnen Switch verbunden sind, sind HA-Paar-Konfigurationen in einem Fabric nicht vollständig redundant.

Die FC-Ziel-Port-Nummern (0a, 0c) in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern variieren je nach Modell des Storage-Node und ob Sie Erweiterungsadapter verwenden.

Alle Plattformen, die FC-Konfigurationen unterstützen, unterstützen HA-Paar-Konfigurationen in einem Single-Fabric-Ansatz.




"Single-Node-Konfigurationen" Die Empfehlungen sind nicht empfehlenswert, da sie nicht die Redundanz bieten, die zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb erforderlich ist.

**Verwandte Informationen**

- Erfahren Sie, wie "Selektive LUN-Zuordnung (SLM)" beschränkt die Pfade, die für den Zugriff auf die LUNs eines HA-Paars verwendet werden.
- Erfahren Sie mehr über "SAN LIFs".

### Best Practices zur Konfiguration von FC Switches mit ONTAP Systemen

Um eine optimale Performance zu erzielen, sollten Sie beim Konfigurieren Ihres FC Switch bestimmte Best Practices berücksichtigen.

Ein Festlegen der Link-Geschwindigkeit ist die Best Practice für FC Switch-Konfigurationen. Dies gilt insbesondere für große Fabrics, da es die beste Performance bei Fabric-Rebuilds bietet und dadurch Zeit sparen kann. Obwohl die Autonegotiation die größte Flexibilität bietet, funktioniert die FC-Switch-Konfiguration nicht immer wie erwartet, und sie erhöht die Zeit für die gesamte Fabric-Build-Sequenz.

Alle Switches, die mit dem Fabric verbunden sind, müssen N_Port ID Virtualization (NPIV) unterstützen und NPIV aktivieren. ONTAP verwendet NPIV, um FC-Ziele einer Fabric anzubieten.

Informationen darüber, welche Umgebungen unterstützt werden, finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Best Practices für FC und iSCSI finden Sie unter "Technischer Bericht 4080 zu NetApp: Best Practices für modernes SAN".

### Empfohlene Konfiguration für FC-Zielports und Geschwindigkeiten für ONTAP Systeme

FC-Ziel-Ports können für das FC-NVMe-Protokoll auf exakt dieselbe Weise konfiguriert und für das FC-Protokoll verwendet werden. Die Unterstützung für das FC-NVMe-Protokoll ist abhängig von Ihrer Plattform und Ihrer ONTAP Version. Verwenden Sie NetApp Hardware Universe, um den Support zu überprüfen.

Für optimale Leistung und höchste Verfügbarkeit sollten Sie die empfohlene Zielportkonfiguration verwenden, die in für Ihre spezifische Plattform aufgeführt "NetApp Hardware Universe" ist.

#### Konfiguration für FC-Ziel-Ports mit gemeinsam genutzten ASICs

Die folgenden Plattformen verfügen über Port-Paare mit gemeinsam genutzten anwendungsspezifischen integrierten Schaltungen (ASICs). Wenn Sie für diese Plattformen einen Erweiterungsadapter verwenden, sollten Sie Ihre FC-Ports so konfigurieren, dass sie nicht denselben ASIC für die Konnektivität verwenden.

| Controller | Port-Paare mit gemeinsam genutztem ASIC | Anzahl der Zielports: Empfohlene Ports |
|---|---|---|
| • FAS8200<br>• AFF A300 | 0g+0h | 1: 0g 2: 0g, 0h |
| • FAS2720<br>• FAS2750<br>• AFF A220 | 0c+0d 0e+0f | 1: 0c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f |

#### Unterstützte Geschwindigkeiten für FC-Zielport

FC-Ziel-Ports können für die Ausführung mit unterschiedlichen Geschwindigkeiten konfiguriert werden. Alle von einem bestimmten Host verwendeten Ziel-Ports sollten auf dieselbe Geschwindigkeit eingestellt sein. Sie sollten die Geschwindigkeit des Zielports so einstellen, dass sie mit der Geschwindigkeit des Geräts übereinstimmt, mit dem das Gerät verbunden wird. Verwenden Sie keine Autonegotiation für die Port-Geschwindigkeit. Ein Port, der auf die Autonegotiation festgelegt ist, kann nach einer Übernahme/Rückgabe oder einer anderen Unterbrechung länger dauern, bis die Verbindung wiederhergestellt ist.

Die integrierten Ports und Erweiterungsadapter können mit folgenden Geschwindigkeiten konfiguriert werden: Jeder Controller und jeder Erweiterungs-Adapter-Port kann je nach Bedarf individuell für unterschiedliche Geschwindigkeiten konfiguriert werden.

| 4-GB-Ports | 8-GB-Ports | 16-GB-Ports | 32-GB-Ports |
|---|---|---|---|
| • 4 Gb<br>• 2 Gb<br>• 1 Gb | • 8 Gb<br>• 4 Gb<br>• 2 Gb | • 16 Gb<br>• 8 Gb<br>• 4 Gb | • 32 Gb<br>• 16 Gb<br>• 8 Gb |

Eine vollständige Liste der unterstützten Adapter und ihrer unterstützten Geschwindigkeiten finden Sie im "NetApp Hardware Universe".

### Konfigurieren Sie die ONTAP FC-Adapterports

Onboard FC-Adapter und einige FC-Erweiterungskarten können individuell als Initiatoren oder Ziel-Ports konfiguriert werden. Andere FC-Erweiterungsadapter sind werkseitig als Initiatoren oder Ziele konfiguriert und können nicht geändert werden. Zusätzliche FC-Ports sind auch über unterstützte UTA2-Karten verfügbar, die mit FC SFP+-Adaptern konfiguriert sind.

Initiator-Ports können zur direkten Verbindung mit Back-End-Platten-Shelfs und möglicherweise mit fremden Storage-Arrays verwendet werden. Mit Zielports können nur Verbindungen zu FC-Switches hergestellt werden.

Die Anzahl der für FC konfigurierten integrierten Ports und CNA/UTA2-Ports variiert je nach Modell des Controllers. Die unterstützten Target-Erweiterungsadapter variieren ebenfalls je nach Controller-Modell. Eine vollständige Liste der integrierten FC-Ports und der unterstützten Zielerweiterungsadapter für Ihr Controller-Modell finden Sie unter"NetApp Hardware Universe".

#### Konfigurieren Sie FC-Adapter für den Initiator-Modus

Der Initiatormodus dient zum Verbinden der Ports mit Bandlaufwerken, Bandbibliotheken oder Drittanbieterspeichern mit Foreign LUN Import (FLI).

**Bevor Sie beginnen**

- LIFs auf dem Adapter müssen von allen Port-Sets, deren Mitglieder sie sind, entfernt werden.
- Alle LIFs von jeder Storage Virtual Machine (SVM), die den zu ändernden physischen Port verwendet, müssen migriert oder zerstört werden, bevor sie die Persönlichkeit des physischen Ports von Ziel zu Initiator ändern.

NVMe/FC unterstützt Initiatormodus.

**Schritte**

1. Entfernen Sie alle LIFs vom Adapter:

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. Versetzen Sie Ihren Adapter in den Offline-Modus:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

3. Ändern Sie den Adapter von Ziel zu Initiator:

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
5. Vergewissern Sie sich, dass die FC-Ports für Ihre Konfiguration im richtigen Status konfiguriert sind:

```
system hardware unified-connect show
```

6. Versetzen Sie den Adapter wieder in den Online-Modus:

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

#### Konfigurieren Sie FC-Adapter für den Zielmodus

Der Zielmodus wird verwendet, um die Ports mit FC-Initiatoren zu verbinden.

Mit diesen Schritten werden FC-Adapter für das FC-Protokoll und das FC-NVMe-Protokoll konfiguriert. Jedoch unterstützen nur bestimmte FC-Adapter FC-NVMe. Im "NetApp Hardware Universe" finden Sie eine Liste mit Adaptern, die das FC-NVMe-Protokoll unterstützen.

**Schritte**

1. Versetzen Sie den Adapter in den Offline-Modus:

   ```
   node run -node _node_name_ storage disable adapter _adapter_name_
   ```

   Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

2. Ändern Sie den Adapter von Initiator zu Ziel:

   ```
   system node hardware unified-connect modify -t target -node _node_name_
   adapter _adapter_name_
   ```

3. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
4. Vergewissern Sie sich, dass der Zielport die richtige Konfiguration hat:

   ```
   network fcp adapter show -node _node_name_
   ```

5. Schalten Sie Ihren Adapter online:

   ```
   network fcp adapter modify -node _node_name_ -adapter _adapter_port_
   -state up
   ```

#### Konfigurieren Sie die FC-Adaptergeschwindigkeit

Sie sollten die Zielportgeschwindigkeit des Adapters so konfigurieren, dass sie mit der Geschwindigkeit des Geräts übereinstimmt, zu dem die Verbindung hergestellt wird, anstatt die Autonegotiation zu verwenden. Ein Port, der auf die Autonegotiation festgelegt ist, kann nach einer Übernahme/Rückgabe oder einer anderen Unterbrechung länger dauern, bis die Verbindung wiederhergestellt ist.

**Über diese Aufgabe**

Da diese Aufgabe alle Storage Virtual Machines (SVMs) und alle LIFs in einem Cluster umfasst, müssen Sie den `-home-port` `-home-lif` Umfang dieses Vorgangs mit den Parametern und begrenzen. Wenn Sie diese Parameter nicht verwenden, gilt der Vorgang für alle LIFs im Cluster, die möglicherweise nicht wünschenswert

wären.

**Bevor Sie beginnen**

Alle LIFs, die diesen Adapter als Home-Port verwenden, müssen offline sein.

**Schritte**

1. Versetzen Sie alle LIFs auf diesem Adapter in den Offline-Modus:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. Versetzen Sie den Adapter in den Offline-Modus:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

   Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

3. Bestimmen Sie die maximale Geschwindigkeit für den Port-Adapter:

```
fcp adapter show -instance
```

   Sie können die Adaptergeschwindigkeit nicht über die Höchstgeschwindigkeit hinaus ändern.

4. Ändern Sie die Adaptergeschwindigkeit:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Versetzen Sie den Adapter in den Online-Modus:

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. Versetzen Sie alle LIFs am Adapter in den Online-Modus:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

**ONTAP-Befehle zum Verwalten von FC-Adaptern**

Sie können FC-Befehle verwenden, um FC Target-Adapter, FC Initiator-Adapter und integrierte FC-Adapter für Ihren Storage Controller zu verwalten. Mit den gleichen Befehlen werden FC-Adapter für das FC-Protokoll und das FC-NVMe-Protokoll verwaltet.

Befehle für FC Initiator-Adapter funktionieren nur auf Node-Ebene. Sie müssen den `run -node node_name` Befehl verwenden, bevor Sie die FC-Initiator-Adapterbefehle verwenden können.

#### Befehle zum Verwalten von FC-Zieladaptern

| Ihr Ziel ist | Befehl |
|---|---|
| Zeigt FC-Adapterinformationen auf einem Node an | `network fcp adapter show` |
| Ändern Sie die FC-Zieladapterparameter | `network fcp adapter modify` |
| Zeigt Informationen zum FC-Protokoll-Datenverkehr an | `run -node node_name sysstat -f` |
| Anzeigen der Dauer des FC-Protokolls | `run -node node_name uptime` |
| Adapterkonfiguration und -Status anzeigen | `run -node node_name sysconfig -v adapter` |
| Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen | `run -node node_name sysconfig -ac` |
| Zeigen Sie eine man-Page für einen Befehl an | `man command_name` |

#### Befehle zum Verwalten von FC-Initiator-Adaptern

| Ihr Ziel ist | Befehl |
|---|---|
| Zeigt Informationen zu allen Initiatoren und ihren Adaptern in einem Node an | `run -node node_name storage show adapter` |
| Adapterkonfiguration und -Status anzeigen | `run -node node_name sysconfig -v adapter` |
| Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen | `run -node node_name sysconfig -ac` |

#### Befehle zum Verwalten der integrierten FC-Adapter

| Ihr Ziel ist | Befehl |
|---|---|
| Zeigt den Status der integrierten FC-Ports an | `system node hardware unified-connect show` |

### Verwandte Informationen

- "Netzwerk-fcp-Adapter"

#### Vermeiden Sie Verbindungsverlust zu einem ONTAP-System mit einem X1133A-R6-Adapter

Sie können den Verlust der Konnektivität bei einem Port-Ausfall verhindern, indem Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfigurieren.

Der X1133A-R6 HBA ist ein 16 GB FC-Adapter mit 4 Ports, der aus zwei 2-Port-Paaren besteht. Der X1133A-R6 Adapter kann als Zielmodus oder Initiatormodus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (z. B. Port 1 und Port 2 auf ASIC 1 und Port 3 und Port 4 auf ASIC 2). Beide Ports auf einem einzelnen ASIC müssen für die Ausführung im gleichen Modus – entweder im Ziel- oder im Initiatormodus – konfiguriert werden. Wenn ein Fehler auftritt, bei dem der ASIC ein Paar unterstützt, werden beide Ports im Paar offline geschaltet.

Um diesen Verlust der Konnektivität zu vermeiden, konfigurieren Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden.

## FCoE-Konfigurationen

#### Konfigurieren Sie FCoE Fabrics mit ONTAP Systemen

FCoE lässt sich mit FCoE Switches auf verschiedene Weise konfigurieren. Direct-Attached-Konfigurationen werden in FCoE nicht unterstützt.

Alle FCoE-Konfigurationen sind Dual Fabric-Systeme, vollständig redundant und erfordern Host-seitige Multipathing-Software. In allen FCoE-Konfigurationen können Sie im Pfad zwischen dem Initiator und dem Ziel mehrere FCoE- und FC-Switches bis zur maximalen Hop Count-Grenze verwenden. Um Switches miteinander zu verbinden, müssen auf den Switches eine Firmware-Version ausgeführt werden, die Ethernet-ISLs unterstützt. Jeder Host in einer FCoE-Konfiguration kann mit einem anderen Betriebssystem konfiguriert werden.

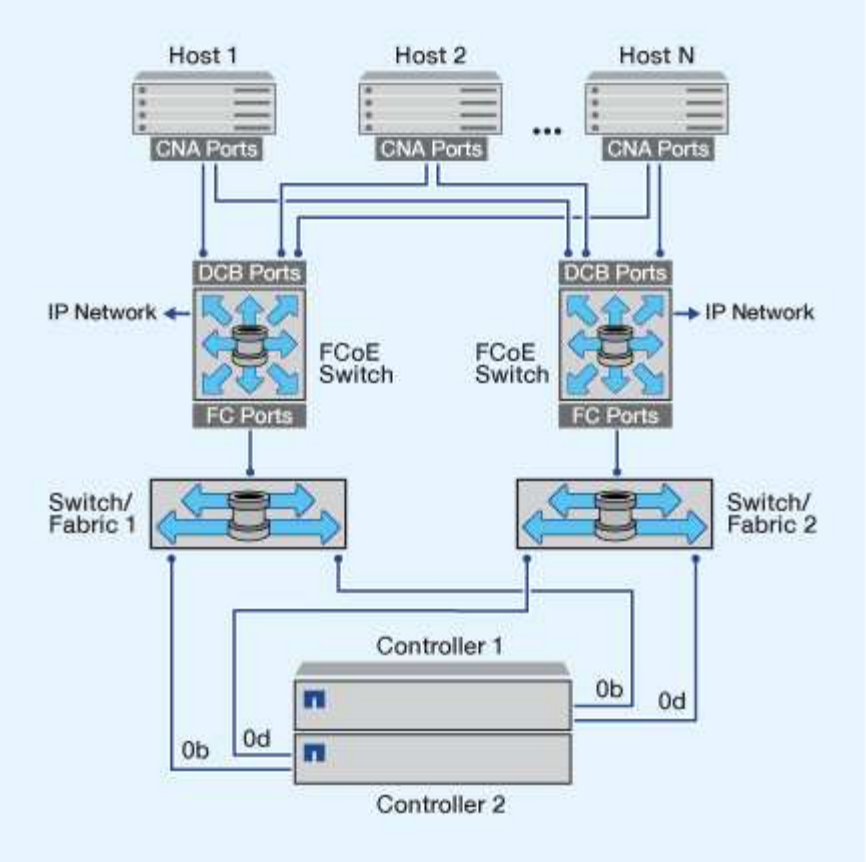
Für FCoE-Konfigurationen sind Ethernet Switches erforderlich, die explizit FCoE-Funktionen unterstützen. FCoE-Konfigurationen werden durch denselben Interoperabilitäts- und Qualitätssicherungsprozess wie FC Switches validiert. Unterstützte Konfigurationen sind in der Interoperabilitäts-Matrix aufgeführt. Einige der in diesen unterstützten Konfigurationen enthaltenen Parameter sind das Switch-Modell, die Anzahl der Switches, die in einer einzigen Fabric implementiert werden können, und die unterstützte Switch-Firmware-Version.

Die Port-Nummern der FC-Target-Erweiterungsadapter in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern können variieren, je nach den Erweiterungssteckplätzen, in denen die FCoE Ziel-Erweiterungsadapter installiert sind.

##### FCoE-Initiator zu FC-Ziel

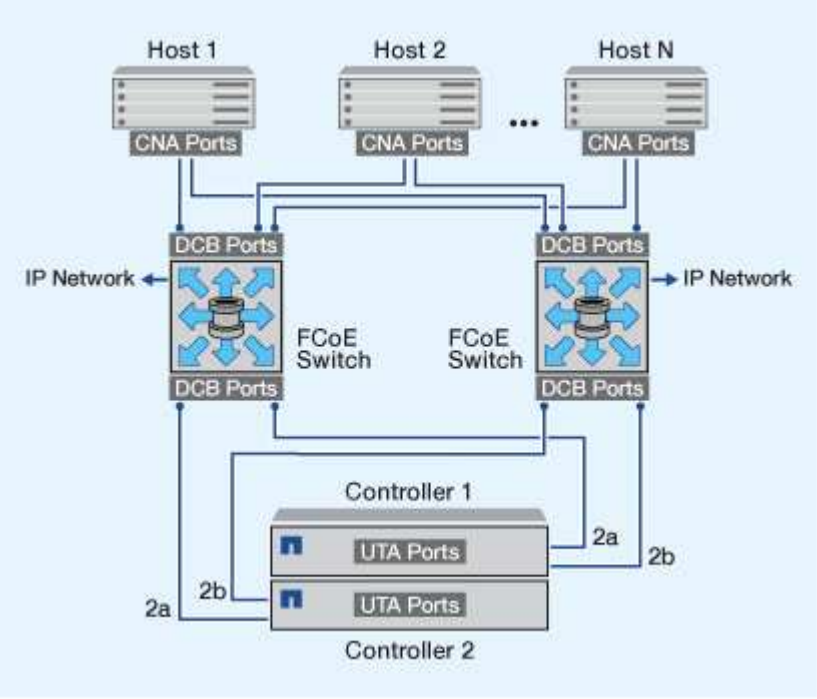
Mit FCoE-Initiatoren (CNAs) können Sie Hosts mit beiden Controllern in einem HA-Paar über FCoE Switches an FC-Ziel-Ports verbinden. Der FCoE-Switch muss auch über FC-Ports verfügen. Der Host FCoE Initiator stellt immer eine Verbindung zum FCoE-Switch her. Der FCoE Switch kann eine direkte Verbindung zum FC-Ziel herstellen oder über FC-Switches eine Verbindung zum FC-Ziel herstellen.

In der folgenden Abbildung werden die Host-CNAs, die eine Verbindung zu einem FCoE-Switch herstellen, und dann vor der Verbindung zum HA-Paar mit einem FC-Switch angezeigt:



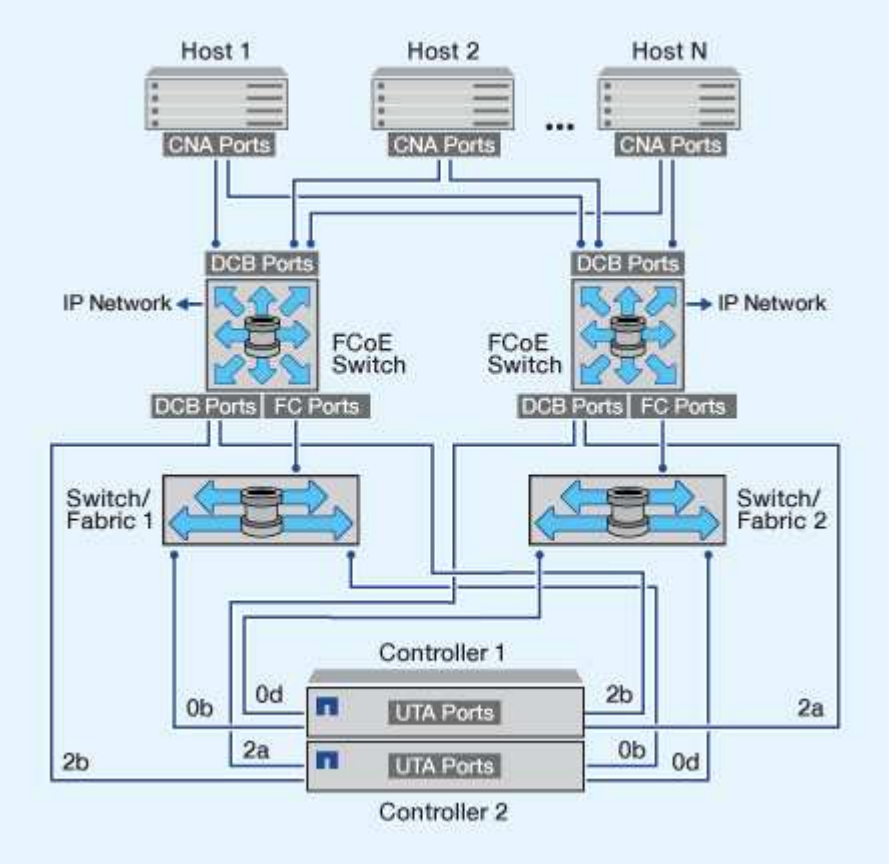

**FCoE-Initiator zu FCoE Target**

Mithilfe von Host FCoE-Initiatoren (CNAs) können Hosts über FCoE-Switches auf beiden Controllern über ein HA-Paar mit den FCoE Ziel-Ports (auch als UTAs oder UTA2 bezeichnet) verbunden werden.



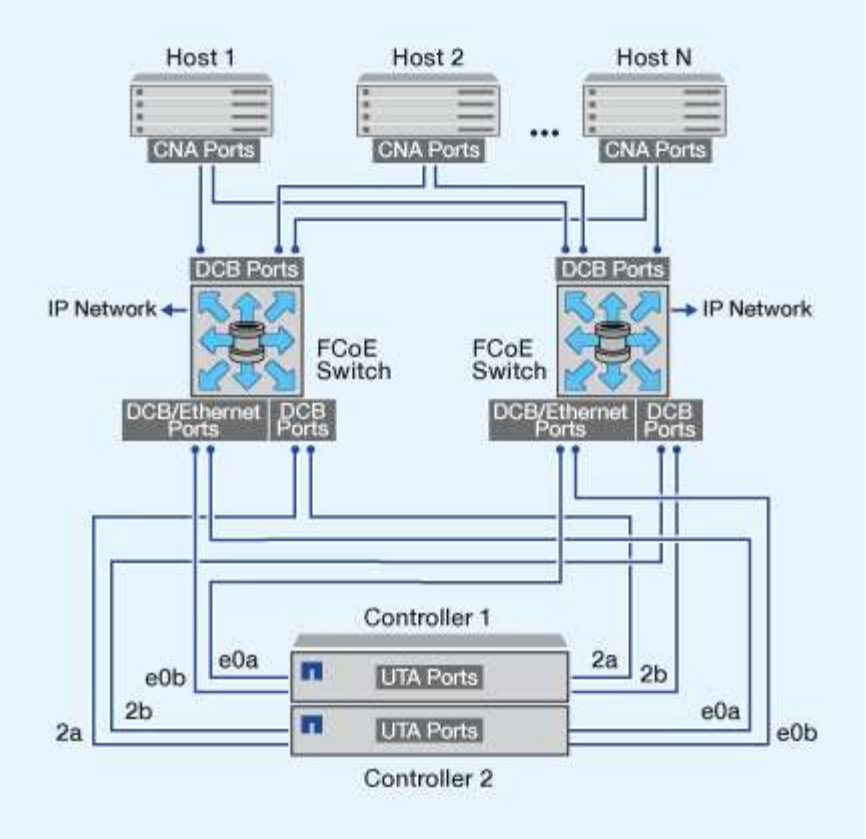
#### FCoE-Initiator auf FCoE- und FC-Ziele

Mithilfe von Host FCoE-Initiatoren (CNAs) können Hosts über FCoE Switches auf beiden Controllern in einem HA-Paar an FCoE- und FC-Ziel-Ports (auch als UTAs oder UTA2 bezeichnet) angeschlossen werden.




#### FCoE wird mit IP-Storage-Protokollen kombiniert

Mithilfe von Host FCoE-Initiatoren (CNAs) können Hosts über FCoE-Switches auf beiden Controllern über ein HA-Paar mit den FCoE Ziel-Ports (auch als UTAs oder UTA2 bezeichnet) verbunden werden. FCoE-Ports können keine herkömmliche Link-Aggregation zu einem einzelnen Switch verwenden. Cisco Switches unterstützen eine besondere Art von Link-Aggregation (Virtual Port Channel), die FCoE unterstützt. Ein Virtual Port Channel sammelt individuelle Links zu zwei Switches. Sie können virtuelle Port-Kanäle auch für andere Ethernet-Datenverkehr verwenden. Ports, die für andere Datenverkehr als FCoE verwendet werden, einschließlich NFS, SMB, iSCSI und anderer Ethernet-Datenverkehr, können regelmäßige Ethernet-Ports an den FCoE Switches nutzen.




**Von ONTAP unterstützte FCoE-Initiator- und Ziel-Port-Kombinationen**

Es werden bestimmte Kombinationen von FCoE und herkömmlichen FC-Initiatoren und -Zielen unterstützt.

#### FCoE-Initiatoren

Sie können FCoE-Initiatoren auf Host-Computern mit FCoE- und herkömmlichen FC-Zielen in Storage-Controllern verwenden. Der Host FCoE Initiator muss eine Verbindung zu einem FCoE DCB-Switch (Data Center Bridging) herstellen, eine direkte Verbindung zu einem Ziel wird nicht unterstützt.

In der folgenden Tabelle sind die unterstützten Kombinationen aufgeführt:

| Initiator | Ziel | Unterstützt? |
|---|---|---|
| FC | FC | Ja. |
| FC | FCoE | Ja. |
| FCoE | FC | Ja. |
| FCoE | FCoE | Ja. |

#### FCoE-Ziele

Sie können FCoE Ziel-Ports mit 4-, 8- oder 16-GB-FC-Ports auf dem Storage Controller kombinieren, unabhängig davon, ob es sich bei den FC-Ports um zusätzliche Zieladapter oder integrierte Ports handelt. Sie

können im selben Storage Controller sowohl FCoE- als auch FC-Zieladapter einsetzen.

Für die Kombination von Onboard- und Erweiterungs-FC-Ports gelten weiterhin die Regeln.

## FC- und FCoE-Zoning

### Erfahren Sie mehr über FC- und FCoE-Zoning mit ONTAP Systemen

Eine FC-, FC-NVMe- oder FCoE-Zone ist eine logische Gruppierung von einem oder mehreren Ports in einer Fabric. Damit Geräte einander sehen, verbinden, Sitzungen miteinander erstellen und kommunizieren können, müssen beide Ports Mitglieder derselben Zone sein.

Zoning erhöht die Sicherheit, indem es den Zugriff und die Konnektivität auf Endpunkte begrenzt, die gemeinsam eine Zone nutzen. Ports, die sich nicht in derselben Zone befinden, können nicht miteinander kommunizieren. Dadurch wird *Crosstalk* zwischen Initiator-HBAs reduziert oder eliminiert. Sollten Konnektivitätsprobleme auftreten, hilft Zoning dabei, Probleme auf einen bestimmten Port-Satz zu isolieren und dadurch die Lösungszeit zu verkürzen.

Zoning reduziert die Anzahl der verfügbaren Pfade zu einem bestimmten Port und verringert die Anzahl der Pfade zwischen einem Host und dem Speichersystem. Beispielsweise haben einige Multipathing-Lösungen des Host-Betriebssystems eine Begrenzung für die Anzahl der Pfade, die sie verwalten können. Zoning kann die Anzahl der für den Host sichtbaren Pfade verringern, sodass die Pfade zum Host nicht die vom Host-Betriebssystem zulässige Höchstzahl überschreiten.

#### World Wide Name-basiertes Zoning

Beim Zoning auf Basis des World Wide Name (WWN) werden die WWNs der Mitglieder der Zone angegeben. Obwohl das WWNN-Zoning (World Wide Node Name) bei einigen Switch-Anbietern möglich ist, müssen Sie beim Zoning in ONTAP das WWPN-Zoning (World Wide Port Name) verwenden.

Das WWPN-Zoning ist erforderlich, um einen spezifischen Port richtig zu definieren und um NPIV effektiv zu nutzen. FC-Switches sollten mit den WWPNs der logischen Schnittstellen (LIFs) des Ziels abgegrenzt werden, nicht mit den WWPNs der physischen Ports des Node. Die WWPNs der physischen Ports beginnen mit „`50`“, und die WWPNs der LIFs beginnen mit „`20`“.

Das WWPN Zoning bietet Flexibilität, da der Zugriff nicht davon bestimmt wird, wo das Gerät physisch mit der Fabric verbunden ist. Sie können ein Kabel von einem Port in den anderen umstecken, ohne dass die Zonen neu konfiguriert werden müssen.

### Empfohlene FC- und FCoE-Zoning-Konfigurationen für ONTAP Systeme

Sie sollten eine Zoning-Konfiguration erstellen, wenn auf Ihrem Host keine Multipathing-Lösung installiert ist, wenn vier oder mehr Hosts mit dem SAN verbunden sind oder wenn die selektive LUN-Zuordnung auf den Nodes im Cluster nicht implementiert ist.

In der empfohlenen FC- und FCoE-Zoning-Konfiguration enthält jede Zone einen Initiator-Port und ein oder mehrere Ziel-LIFs. Mit dieser Konfiguration kann jeder Host-Initiator auf jeden Node zugreifen, während Hosts, die auf denselben Node zugreifen, nicht sehen können, welche Ports des anderen Hosts verwendet werden

Fügen Sie mit dem Host-Initiator alle LIFs der Storage Virtual Machine (SVM) zur Zone hinzu. So können Sie Volumes oder LUNs verschieben, ohne Ihre vorhandenen Zonen zu bearbeiten oder neue Zonen zu erstellen.

#### Dual Fabric Zoning-Konfigurationen

Dual-Fabric-Zoning-Konfigurationen werden empfohlen, da sie Schutz vor Datenverlust bei dem Ausfall einer einzelnen Komponente bieten. In einer Dual-Fabric-Konfiguration ist jeder Host-Initiator über unterschiedliche Switches mit jedem Node im Cluster verbunden. Wenn ein Switch nicht mehr verfügbar ist, wird der Datenzugriff über den verbleibenden Switch aufrechterhalten. Auf dem Host wird Multipathing-Software benötigt, um mehrere Pfade verwalten zu können.

In der folgenden Abbildung hat der Host zwei Initiatoren und führt die Multipathing-Software aus. Es gibt zwei Zonen. "Selektive LUN-Zuordnung (SLM)" Ist so konfiguriert, dass alle Nodes als Reporting-Nodes angesehen werden.

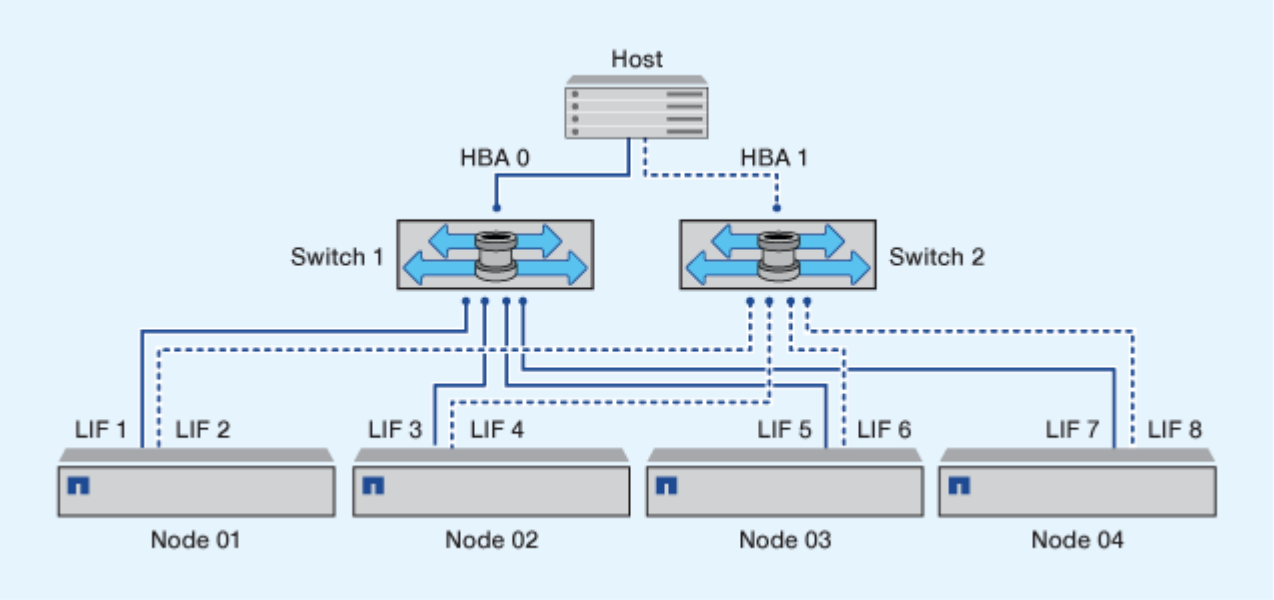
Die in dieser Abbildung verwendete Namenskonvention ist nur eine Empfehlung zu einer möglichen Namenskonvention, die Sie für Ihre ONTAP Lösung verwenden können.

- Zone 1: HBA 0, LIF_1, LIF_3, LIF_5 und LIF_7
- Zone 2: HBA 1, LIF_2, LIF_4, LIF_6 und LIF_8

Jeder Host-Initiator wird über einen anderen Switch begrenzt. Auf Zone 1 ist über Schalter 1 zugegriffen. Auf Zone 2 ist über Schalter 2 zugegriffen.

Jeder Host kann auf jedem Node auf eine LIF zugreifen. Dies ermöglicht es dem Host, weiterhin auf seine LUNs zuzugreifen, wenn ein Node ausfällt. Basierend auf der SLM-Konfiguration der Berichterstellungsknoten können SVMs auf allen iSCSI- und FC-LIFs auf jedem Node im Cluster zugreifen. Mit SLM, Portsätzen oder FC-Switch-Zoning reduzieren Sie die Anzahl der Pfade von einer SVM zum Host und die Anzahl der Pfade von einer SVM zu einer LUN.

Wenn die Konfiguration mehr Nodes umfasst, sind die LIFs für die zusätzlichen Nodes in diesen Zonen enthalten.




Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der Pfade unterstützen, die zum Zugriff auf die LUNs auf den Nodes verwendet werden.

#### Einzel-Fabric-Zoning

In einer Einzel-Fabric-Konfiguration verbinden Sie jeden Host-Initiator über einen einzelnen Switch mit jedem Storage Node. Einzel-Fabric-Zoning-Konfigurationen werden nicht empfohlen, da sie keinen Schutz vor Datenverlust bei dem Ausfall einer einzelnen Komponente bieten. Wenn Sie Single-Fabric-Zoning konfigurieren, sollte jeder Host über zwei Initiatoren für Multipathing verfügen, um Ausfallsicherheit in der Lösung bereitzustellen. Auf dem Host wird Multipathing-Software benötigt, um mehrere Pfade verwalten zu können.

Jeder Host-Initiator sollte mindestens über eine LIF von jedem Node verfügen, auf den der Initiator zugreifen kann. Das Zoning sollte mindestens einen Pfad vom Host-Initiator zum HA-Paar der Nodes im Cluster zulassen, um einen Pfad für die LUN-Konnektivität bereitzustellen. Dies bedeutet, dass jeder Initiator auf dem Host in seiner Zonenkonfiguration möglicherweise nur über ein Ziel-LIF pro Node verfügt. Wenn Multipathing zum selben Node oder zu mehreren Nodes im Cluster erforderlich ist, dann verfügt jeder Node über mehrere LIFs in seiner Zonenkonfiguration. Dies ermöglicht es dem Host, weiterhin auf seine LUNs zuzugreifen, wenn ein Node ausfällt oder ein Volume mit der LUN auf einen anderen Node verschoben wird. Dafür müssen auch die Reporting-Nodes entsprechend eingestellt werden.

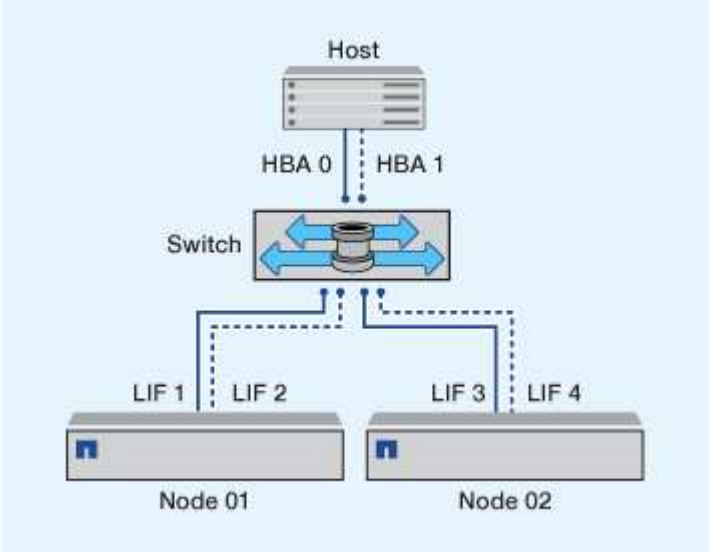
Bei Verwendung von Cisco FC und FCoE Switches darf eine einzelne Fabric-Zone nicht mehr als eine Ziel-LIF für denselben physischen Port enthalten. Wenn sich mehrere LIFs am selben Port in derselben Zone befinden, können die LIF-Ports nach einem Verlust der Verbindung möglicherweise nicht wiederherstellen.

In der folgenden Abbildung hat der Host zwei Initiatoren und führt die Multipathing-Software aus. Es gibt zwei Zonen:

> Die in dieser Abbildung verwendete Namenskonvention ist nur eine Empfehlung zu einer möglichen Namenskonvention, die Sie für Ihre ONTAP Lösung verwenden können.

- Zone 1: HBA 0, LIF_1 und LIF_3
- Zone 2: HBA 1, LIF_2 und LIF_4

Wenn die Konfiguration mehr Nodes umfasst, sind die LIFs für die zusätzlichen Nodes in diesen Zonen enthalten.s.




In diesem Beispiel könnten Sie auch alle vier LIFs in jeder Zone enthalten. In diesem Fall wären die Zonen wie folgt:

- Zone 1: HBA 0, LIF_1, LIF_2, LIF_3 und LIF_4
- Zone 2: HBA 1, LIF_1, LIF_2, LIF_3 und LIF_4

> Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der unterstützten Pfade unterstützen, die zum Zugriff auf die LUNs auf den Nodes verwendet werden. Informationen zur Bestimmung der Anzahl der Pfade für den Zugriff auf die LUNs auf Nodes finden Sie im Abschnitt über die SAN-Konfigurationsbeschränkungen.

#### Zoning-Einschränkungen für Cisco FC und FCoE Switches

Bei Verwendung von Cisco FC- und FCoE-Switches gelten bestimmte Einschränkungen für die Nutzung von physischen Ports und logischen Schnittstellen (LIFs) in Zonen.

**Physische Ports**

- FC-NVMe und FC können denselben physischen 32-GB-Port verwenden
- FC-NVMe und FCoE können nicht denselben physischen Port verwenden
- FC und FCoE können denselben physischen Port verwenden, die Protokoll-LIFs müssen sich jedoch in separaten Zonen befinden.

**Logische Schnittstellen (LIFs)**

- Eine Zone kann von jedem Ziel-Port im Cluster eine LIF enthalten.

  Überprüfen Sie die SLM-Konfiguration, damit Sie die maximal zulässige Anzahl von Pfaden für den Host nicht überschreiten.

- Jede LIF auf einem angegebenen Port muss sich in einer separaten Zone von anderen LIFs an diesem Port befinden
- LIFs an verschiedenen physischen Ports können sich in derselben Zone befinden.

## Anforderungen für SAN-Hosts, die an NetApp Systeme von ONTAP und anderen Herstellern angeschlossen sind

Konfigurationen mit Shared SAN werden als Hosts definiert, die sowohl mit ONTAP-Storage-Systemen als auch Storage-Systemen anderer Anbieter verbunden sind. Der Zugriff auf die ONTAP Storage-Systeme und die Storage-Systeme anderer Hersteller über einen einzigen Host wird unterstützt, sofern verschiedene Anforderungen erfüllt sind.

Bei allen Host-Betriebssystemen gilt es, eine Verbindung mit separaten Adaptern mit den Storage-Systemen jedes Anbieters zu herstellen. Die Verwendung separater Adapter verringert die Wahrscheinlichkeit widersprüchlicher Treiber und Einstellungen. Wenn Verbindungen zu einem ONTAP Storage-System hergestellt werden sollen, müssen das Adaptermodell, das BIOS, die Firmware und der Treiber als unterstützt im NetApp Interoperabilitäts-Matrix-Tool aufgeführt sein.

Sie sollten die erforderlichen oder empfohlenen Zeitüberschreitungswerte und andere Speicherparameter für den Host festlegen. Sie müssen immer die NetApp Software installieren oder zuletzt die NetApp-Einstellungen anwenden.

- Für AIX sollten Sie die Werte aus der AIX Host Utilities-Version anwenden, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.

- Für ESX sollten Sie die Host-Einstellungen über die Virtual Storage Console für VMware vSphere anwenden.
- Für HP-UX sollten Sie die HP-UX Standard-Speichereinstellungen verwenden.
- Bei Linux sollten Sie die Werte aus der Version Linux Host Utilities anwenden, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.
- Bei Solaris sollten Sie die Werte aus der Solaris Host Utilities-Version anwenden, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.
- Für Windows sollten Sie die Windows Host Utilities-Version installieren, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.

**Verwandte Informationen**

"NetApp Interoperabilitäts-Matrix-Tool"

## SAN-Konfigurationen in einer MetroCluster Umgebung

### Unterstützte SAN-Konfigurationen in einer ONTAP MetroCluster-Umgebung

Beim Einsatz von SAN-Konfigurationen in einer MetroCluster Umgebung müssen Sie jedoch bestimmte Überlegungen beachten.

- MetroCluster-Konfigurationen unterstützen vSAN Konfigurationen nicht auf Frontend-FC-Fabric „`Routed`“.
- Ab ONTAP 9.15.1 werden MetroCluster IP-Konfigurationen mit vier Nodes auf NVMe/TCP unterstützt.
- Ab ONTAP 9.12.1 MetroCluster werden NVMe/FC Konfigurationen mit vier Nodes unterstützt. MetroCluster-Konfigurationen werden für Front-End-NVMe-Netzwerke vor ONTAP 9.12.1 nicht unterstützt.
- Andere SAN-Protokolle wie iSCSI, FC und FCoE werden auf MetroCluster Konfigurationen unterstützt.
- Bei der Verwendung von SAN-Client-Konfigurationen müssen Sie prüfen, ob besondere Überlegungen zu MetroCluster-Konfigurationen in den Hinweisen im "NetApp Interoperabilitäts-Matrix-Tool" (IMT) enthalten sind.
- Betriebssysteme und Applikationen müssen eine I/O-Ausfallsicherheit von 120 Sekunden bieten, um die automatische, ungeplante MetroCluster Umschaltung sowie eine Tiebreaker oder Mediator-initiierte Umschaltung zu unterstützen.
- MetroCluster-Konfigurationen verwenden auf beiden Seiten des Front-End FC-Fabric die gleichen WWNNs und WWPNs.

**Verwandte Informationen**

- "MetroCluster Datensicherung und Disaster Recovery verstehen"
- "NetApp Knowledge Base: Welche Überlegungen gibt es hinsichtlich der AIX-Host-Unterstützung in einer MetroCluster -Konfiguration?"
- "NetApp Knowledge Base: Überlegungen zur Solaris-Hostunterstützung in einer MetroCluster -Konfiguration"

### Vermeiden Sie Port-Überschneidungen während ONTAP MetroCluster Switchover und Switchback

In einer SAN-Umgebung können Sie die Front-End-Switches konfigurieren, um Überlappungen zu vermeiden, wenn der alte Port offline geschaltet wird und der neue Port online geschaltet wird.

Während der Umschaltung meldet sich der FC-Port am verbleibenden Standort möglicherweise beim Fabric an, bevor die Fabric erkannt hat, dass der FC-Port am Disaster-Standort offline ist und diesen Port aus dem Namen- und Verzeichnisdienst entfernt hat.

Wenn der FC-Port bei der Katastrophe noch nicht entfernt wird, wird der Fabric-Anmeldeversuch des FC-Ports am noch intakten Standort aufgrund eines doppelten WWPN möglicherweise abgelehnt. Dieses Verhalten der FC-Switches kann geändert werden, um die Anmeldung des vorherigen Geräts und nicht des vorhandenen zu ermöglichen. Sie sollten die Auswirkungen dieses Verhaltens auf andere Fabric-Geräte überprüfen. Weitere Informationen erhalten Sie vom Switch-Anbieter.

Wählen Sie das richtige Verfahren je nach Schaltertyp aus.

**Beispiel 9. Schritte**

**Cisco Switch**

1. Stellen Sie eine Verbindung zum Switch her, und melden Sie sich an.
2. Konfigurationsmodus aufrufen:

```
switch# config t
switch(config)#
```

3. Überschreiben Sie den ersten Geräteeintrag in der Namensserver-Datenbank mit dem neuen Gerät:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Vergewissern Sie sich bei Switches, die NX-OS 8.x ausführen, dass das flogi-Timeout auf Null gesetzt ist:

   a. Anzeige des Zeitschaltuftzeitschaltufschaltudes:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Wenn die Ausgabe im vorherigen Schritt nicht angibt, dass der Zeitwert Null ist, setzen Sie ihn auf null:

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

**Brocade Switch**

1. Stellen Sie eine Verbindung zum Switch her, und melden Sie sich an.
2. Geben Sie den `switchDisable` Befehl ein.
3. Geben Sie den `configure` Befehl ein, und drücken Sie `y` an der Eingabeaufforderung.

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. Einstellung 1 auswählen:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Beantworten Sie die verbleibenden Eingabeaufforderungen, oder drücken Sie **Strg + D**.
6. Geben Sie den `switchEnable` Befehl ein.

**Verwandte Informationen**

"Umschaltung für Tests oder Wartung"

## ONTAP-Unterstützung für SAN-Host-Multipathing

### ONTAP verwendet Asymmetric Logical Unit Access (ALUA)-Software für das Multipathing mit FC- und iSCSI-Hosts.

Ab ONTAP 9.5 wird Failover/Giveback für Multipath-Hochverfügbarkeitspaare (HA) für NVMe-Hosts unterstützt, die asynchronen Namespace-Zugriff (ANA) verwenden. In ONTAP 9.4 unterstützt NVMe nur einen Pfad vom Host zum Ziel, sodass der Applikations-Host den Pfad-Failover zu seinem HA-Partner managen muss.

Die Multipathing-Software wird auf Ihrem SAN-Host benötigt, wenn sie über mehrere Pfade auf einen LUN- oder NVMe-Namespace zugreifen kann. Sie stellt dem Betriebssystem eine einzelne Festplatte für alle Pfade zu einer LUN oder einem NVMe Namespace dar. Ohne diese Technologie könnte das Betriebssystem jeden Pfad als separate Festplatte behandeln, was zu Datenbeschädigungen führt.

Ihre Lösung wird als mehrere Pfade angesehen, wenn Sie einen der folgenden haben:

- Ein einzelner Initiator-Port im Host, der an mehrere SAN LIFs in der SVM angeschlossen ist
- Mehrere Initiator-Ports, die an eine einzelne SAN-LIF in der SVM angeschlossen sind
- Mehrere Initiator-Ports, die an mehrere SAN-LIFs in der SVM angeschlossen sind

Die Multipathing-Software, die auch als MPIO-Software (Multipath I/O) bezeichnet wird, wird in HA-Konfigurationen empfohlen. Zusätzlich zur Selektiven LUN-Zuordnung wird die Verwendung von FC-Switch-Zoning oder Portsätzen zur Beschränkung der Pfade empfohlen, die für den Zugriff auf LUNs verwendet werden.

Informationen darüber, welche spezifischen Host-Konfigurationen ALUA oder ANA unterstützen, finden Sie im "NetApp Interoperabilitäts-Matrix-Tool" und "ONTAP SAN-Host-Konfiguration" Ihres Host-Betriebssystems.

#### Empfohlene Anzahl an Pfaden vom Host zu Nodes im Cluster

Sie sollten zu jedem Node im Cluster nicht mehr als acht Pfade vom Host überschreiten. Sie sollten darüber hinaus die Gesamtzahl der Pfade nicht überschreiten, die für das Host-Betriebssystem und das auf dem Host verwendete Multipathing unterstützt werden können.

Sie sollten mindestens zwei Pfade pro LUN haben, die mit jedem Reporting-Node durch die Storage Virtual Machine (SVM) im Cluster verbunden "Selektive LUN-Zuordnung (SLM)"sind. So werden Single Points of Failure eliminiert und das System kann den Ausfall von Komponenten überleben.

Wenn Sie vier oder mehr Nodes in Ihrem Cluster haben oder mehr als vier von den SVMs in einem Ihrer Nodes verwendete Ziel-Ports: Mithilfe der folgenden Methoden können Sie die Anzahl der Pfade begrenzen, die zum Zugriff auf LUNs auf Ihren Nodes verwendet werden können, damit Sie die empfohlene maximale Anzahl von acht Pfaden nicht überschreiten.

- SLM

SLM reduziert die Anzahl der Pfade vom Host zur LUN auf nur Pfade auf dem Node, der die LUN besitzt, und dem HA-Partner des entsprechenden Node. SLM ist standardmäßig aktiviert.

- "Portsets für iSCSI"
- FC igroup-Zuordnungen von Ihrem Host
- FC-Switch-Zoning

## Konfigurationseinschränkungen

### Bestimmen Sie die maximale Anzahl unterstützter Nodes und SAN-Hosts pro ONTAP-Cluster

Die Anzahl der unterstützten Nodes pro Cluster hängt von Ihrer Version von ONTAP, den Controller-Modellen und dem Protokoll der Cluster-Nodes ab. Die maximale Anzahl der SAN-Hosts, die mit einem Cluster verbunden werden können, hängt ebenfalls von der jeweiligen Konfiguration ab.

#### Ermitteln Sie die maximale Anzahl unterstützter Nodes pro Cluster

Wenn ein Node im Cluster für FC, FC-NVMe, FCoE oder iSCSI konfiguriert ist, ist dieser Cluster auf die Einschränkungen für den SAN-Node beschränkt. Node-Limits basierend auf den Controllern im Cluster werden im „*Hardware Universe*“ aufgeführt.

**Schritte**

1. Gehen Sie zu "NetApp Hardware Universe".
2. Wählen Sie oben links neben **Home Plattformen** aus, und wählen Sie dann den Plattformtyp aus.
3. Wählen Sie Ihre Version von ONTAP aus.

   Es wird eine neue Spalte angezeigt, in der Sie Ihre Plattformen auswählen können.

4. Wählen Sie die in Ihrer Lösung verwendeten Plattformen aus.
5. Wählen Sie unter **Wählen Sie Ihre Spezifikationen** die Option **Alle auswählen** aus.
6. Wählen Sie **Max Nodes per Cluster (NAS/SAN)**.
7. Klicken Sie Auf **Ergebnisse Anzeigen**.

**Ergebnisse**

Die maximale Anzahl der Nodes pro Cluster für die ausgewählten Plattformen wird angezeigt.

#### Ermitteln Sie, ob Ihr Cluster mehr FC-Hosts unterstützen kann

Für FC- und FC-NVMe-Konfigurationen sollten Sie anhand der Anzahl der Initiator-Target-Nexuses (ITNs) in Ihrem System ermitteln, ob Sie Ihrem Cluster weitere Hosts hinzufügen können.

Ein ITN steht für einen Pfad vom Host-Initiator zum Ziel des Storage-Systems. In FC- und FC-NVMe-Konfigurationen beträgt die maximale Anzahl an IT-Ns pro Node 2,048. Wenn Sie unter der maximalen Anzahl von ITNs liegen, können Sie dem Cluster weiterhin Hosts hinzufügen.

Führen Sie die folgenden Schritte für jeden Knoten im Cluster durch, um die Anzahl der in Ihrem Cluster verwendeten ITNs zu ermitteln.

**Schritte**

1. Identifizieren Sie alle LIFs an einem bestimmten Node.
2. Führen Sie den folgenden Befehl für jede LIF auf dem Node aus:

   ```
   fcp initiator show -fields wwpn, lif
   ```

   Die Anzahl der Einträge, die unten in der Befehlsausgabe angezeigt werden, stellt Ihre Anzahl an ITNs für diese LIF dar.

3. Notieren Sie die Anzahl der angezeigten ITNs für jedes LIF.
4. Fügen Sie auf jedem Knoten des Clusters die Anzahl der ITNs für jede LIF hinzu.

   Diese Summe gibt die Anzahl der ITNs in Ihrem Cluster an.

#### Stellen Sie fest, ob Ihr Cluster mehr iSCSI-Hosts unterstützen kann

Die Anzahl der Hosts, die direkt mit einem Node verbunden werden können oder die über einen oder mehrere Switches verbunden werden können, hängt von der Anzahl der verfügbaren Ethernet-Ports ab. Die Anzahl der verfügbaren Ethernet-Ports wird durch das Modell des Controllers und die Anzahl und den Typ der im Controller installierten Adapter bestimmt. Die Anzahl der unterstützten Ethernet-Ports für Controller und Adapter ist im *Hardware Universe* verfügbar.

Bei allen Cluster-Konfigurationen mit mehreren Nodes müssen Sie die Anzahl der iSCSI-Sitzungen pro Node bestimmen, damit Sie dem Cluster weitere Hosts hinzufügen können. Solange Ihr Cluster die maximale Anzahl von iSCSI-Sitzungen pro Node unterschritten hat, können Sie Ihrem Cluster weiterhin Hosts hinzufügen. Die maximale Anzahl von iSCSI-Sitzungen pro Node variiert abhängig von den Typen der Controller in Ihrem Cluster.

**Schritte**

1. Identifizieren Sie alle Zielportalgruppen auf dem Knoten.
2. Überprüfen Sie die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten:

   ```
   iscsi session show -tpgroup _tpgroup_
   ```

   Die Anzahl der Einträge, die unten in der Befehlsausgabe angezeigt werden, entspricht der Anzahl der iSCSI-Sitzungen für diese Zielportalgruppe.

3. Notieren Sie die Anzahl der für jede Zielportalgruppe angezeigten iSCSI-Sitzungen.
4. Fügen Sie die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten hinzu.

   Die Gesamtsumme stellt die Anzahl der iSCSI-Sitzungen auf Ihrem Knoten dar.

### Einschränkungen und Unterstützung für die Konfiguration und Unterstützung von All-Flash-SAN-Arrays

## Einschränkungen für die Konfiguration und den Support von All-Flash-SAN-Arrays (ASA) sind je nach ONTAP Version unterschiedlich.

Die aktuellen Details zu den unterstützten Konfigurationsgrenzwerten finden Sie unter "NetApp Hardware

Universe".

> Diese Einschränkungen gelten für ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) haben, siehe "ASA r2-Systemspeichergrenzen" .

#### SAN-Protokolle und unterstützte Anzahl von Nodes pro Cluster

Die unterstützten SAN-Protokolle und die maximale Anzahl an Nodes pro Cluster hängen davon ab, ob Sie über eine nicht-MetroCluster- oder MetroCluster-Konfiguration verfügen:

#### Konfigurationen anderer Anbieter

Die folgende Tabelle zeigt die Unterstützung von ASA für SAN-Protokolle und die unterstützte Anzahl an Nodes pro Cluster in nicht-MetroCluster Konfigurationen:

| Beginnt mit ONTAP… | Protokollunterstützung | Maximale Nodes pro Cluster |
|---|---|---|
| 9.11.1 | • NVMe/TCP<br>• NVMe/FC | 12 |
| 9.10.1 | • NVMe/TCP | 2 |
| 9.9.1 | • NVMe/FC | 2 |
| | • FC<br>• ISCSI | 12 |
| 9,7 | • FC<br>• ISCSI | 2 |

#### MetroCluster IP-Konfigurationen

Die folgende Tabelle zeigt die ASA-Unterstützung für SAN-Protokolle und die unterstützte Anzahl an Nodes pro Cluster in MetroCluster IP-Konfigurationen:

| Beginnt mit ONTAP… | Protokollunterstützung | Maximale Nodes pro Cluster |
|---|---|---|
| 9.15.1 | • NVMe/TCP | 2 Nodes pro Cluster in MetroCluster IP-Konfigurationen mit vier Nodes |
| 9.12.1 | • NVMe/FC | 2 Nodes pro Cluster in MetroCluster IP-Konfigurationen mit vier Nodes |
| 9.9.1 | • FC<br>• ISCSI | 4 Nodes pro Cluster in MetroCluster IP-Konfigurationen mit acht Nodes |
| 9,7 | • FC<br>• ISCSI | 2 Nodes pro Cluster in MetroCluster IP-Konfigurationen mit vier Nodes |

#### Unterstützung für persistente Ports

Ab ONTAP 9.8 sind persistente Ports standardmäßig auf All-Flash-SAN-Arrays (ASAs) aktiviert, die für die Verwendung des FC-Protokolls konfiguriert sind. Persistente Ports sind nur für FC verfügbar und erfordern eine vom WWPN (World Wide Port Name) angegebene Zonenmitgliedschaft.

Persistente Ports reduzieren die Auswirkungen von Übernahmen, indem sie eine Schatten-LIF auf dem entsprechenden physischen Port des Hochverfügbarkeitspartners erstellen. Wenn ein Node übernommen wird, übernimmt die Shadow-LIF auf dem Partner-Node die Identität der ursprünglichen LIF, einschließlich z. B. z. B. Beispiel B.Ne. Bevor der Status des Pfads zum übernusenen Knoten auf fehlerhaft geändert wird, wird die Shadow-LIF als aktiv/optimierter Pfad zum Host MPIO-Stack angezeigt und I/O wird verschoben. So reduziert sich die I/O-Störung, da der Host selbst während eines Storage Failover-Betriebs immer dieselbe Anzahl von Pfaden zum Ziel sieht.

Bei persistenten Ports sollten die folgenden FCP-Port-Merkmale innerhalb des HA-Paars identisch sein:

- Anzahl FCP-Ports
- FCP-Port-Namen
- FCP-Port-Geschwindigkeit
- FCP LIF WWPN-basiertes Zoning

Wenn einige dieser Merkmale innerhalb des HA-Paars nicht identisch sind, wird die folgende EMS-Meldung erzeugt:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Weitere Informationen zu persistenten Ports finden Sie unter "Technischer Bericht 4080 zu NetApp: Best Practices für modernes SAN".

### Konfigurationsbeschränkungen für FC-Switches, die in ONTAP-Systemen verwendet werden

Bei der Konfiguration der Fibre-Channel-Switches gilt es, Höchstwerte zu beachten, einschließlich der Anzahl der unterstützten Anmeldungen pro Port, Port-Gruppe, Blade und Switch. Die Switch-Anbieter dokumentieren die von ihnen unterstützten Grenzwerte.

Jede logische FC-Schnittstelle (Logical Interface, LIF) meldet sich bei einem FC-Switch-Port an. Die Gesamtzahl der Anmeldungen von einem einzelnen Ziel auf dem Node entspricht der Anzahl der LIFs plus eine Anmeldung für den zugrunde liegenden physischen Port. Überschreiten Sie nicht die Konfigurationsgrenzwerte des Switch-Anbieters für Anmeldungen oder andere Konfigurationswerte. Dies gilt auch für die Initiatoren, die auf der Host-Seite in virtualisierten Umgebungen mit aktiviertem NPIV verwendet werden. Überschreiten Sie nicht die Konfigurationsgrenzwerte des Switch-Anbieters für Anmeldungen entweder für das Ziel oder für die in der Lösung verwendeten Initiatoren.

#### Einschränkungen für den Brocade Switch

Die Konfigurationsgrenzwerte für Brocade Switches finden Sie in den „ *Brocade Scalability Guidelines*“.

#### Einschränkungen für die Switches von Cisco Systems

Die Konfigurationsbeschränkungen für Cisco-Switches finden Sie im "Einschränkungen Bei Der Konfiguration Von Cisco" Handbuch zu Ihrer Version der Cisco Switch-Software.

### Maximale Anzahl von FC- und FCoE-Hop, die in ONTAP unterstützt wird

Hop Count ist definiert als die Anzahl der Switches im Pfad zwischen dem Initiator (Host) und dem Ziel (Storage-System). Die maximal unterstützte Anzahl von FC-Hop zwischen einem Host und Speichersystem variiert je nach Switch-Anbieter.

Die Dokumentation von Cisco Systems bezieht sich auch auf diesen Wert als *Durchmesser des SAN Fabric*.

Bei FCoE lassen sich FCoE-Switches mit FC-Switches verbinden. Für lückenlose FCoE-Verbindungen müssen die FCoE Switches eine Firmware-Version ausführen, die Ethernet Inter-Switch Links (ISLs) unterstützt.

| Lieferant wechseln | Unterstützte Hop Count |
|---|---|
| Brocade | • 7 für FC<br>• 5 für FCoE |
| Cisco | • 7 für FC<br>• Es können bis zu 3 der Switches FCoE-Switches sein. |

### Berechnung der Warteschlangentiefe für ONTAP FC-Hosts

Möglicherweise müssen Sie die FC-Warteschlangentiefe auf dem Host anpassen, um die Höchstwerte für ITNs pro Knoten und FC-Port-Fan-in zu erreichen. Die maximale Anzahl an LUNs und die Anzahl der HBAs, die eine Verbindung zu einem FC-Port herstellen können, werden durch die verfügbare Warteschlangentiefe auf den FC-Ziel-Ports begrenzt.

#### Über diese Aufgabe

„Queue depth“ ist die Anzahl von I/O-Anfragen (SCSI-Befehle), die sich gleichzeitig in ein Storage Controller Warteschlange einreihen lassen. Jede I/O-Anforderung vom Initiator-HBA des Hosts zum Zieladapter des Storage-Controllers verbraucht einen Warteschlangeneintrag. Eine höhere Warteschlangentiefe entspricht in der Regel einer besseren Performance. Wenn jedoch die maximale Warteschlangentiefe des Storage Controllers erreicht wird, weist dieser Storage-Controller eingehende Befehle zurück, indem er eine QFULL-Antwort zurückgibt. Wenn eine große Anzahl von Hosts auf einen Speicher-Controller zugreifen, sollten Sie sorgfältig planen, QFULL-Bedingungen zu vermeiden, die die Systemleistung erheblich beeinträchtigen und zu Fehlern bei einigen Systemen führen können.

In einer Konfiguration mit mehreren Initiatoren (Hosts) sollten alle Hosts über ähnliche Warteschlangentiefen verfügen. Aufgrund der Ungleichheit in der Warteschlangentiefe zwischen Hosts, die über denselben Zielport mit dem Storage Controller verbunden sind, wird Hosts mit kleineren Warteschlangentiefen dem Zugriff auf Ressourcen durch Hosts mit größeren Warteschlangentiefen entzogen.

Die folgenden allgemeinen Empfehlungen bezüglich „`Tuning`“-Warteschlangentiefe:

- Verwenden Sie für kleine und mittelgroße Systeme eine HBA-Warteschlangenlänge von 32.
- Verwenden Sie für große Systeme eine HBA-Warteschlangenlänge von 128.
- Verwenden Sie für Ausnahmefälle oder Performance-Tests eine Warteschlangentiefe von 256, um mögliche Warteschlangenprobleme zu vermeiden.
- Für alle Hosts sollten die Warteschlangentiefen auf ähnliche Werte festgelegt sein, um allen Hosts gleichberechtigten Zugriff zu gewähren.
- Um Performance-Einbußen oder Fehler zu vermeiden, darf die Ziel-FC-Port-Warteschlangentiefe des Storage Controllers nicht überschritten werden.

#### Schritte

1. Zählen Sie die Gesamtzahl der FC-Initiatoren auf allen Hosts, die mit einem FC-Zielport verbunden sind.
2. Mit 128 multiplizieren.
   - Wenn das Ergebnis unter 2,048 liegt, setzen Sie die Warteschlangentiefe für alle Initiatoren auf 128. Sie haben 15 Hosts, wobei ein Initiator mit jedem der zwei Ziel-Ports auf dem Storage Controller verbunden ist. 15 × 128 = 1,920. Da 1,920 kleiner als das gesamte Warteschlangentiefe von 2,048 ist, können Sie die Warteschlangentiefe für alle Initiatoren auf 128 einstellen.
   - Wenn das Ergebnis größer als 2,048 ist, mit Schritt 3 fortfahren. Sie haben 30 Hosts, wobei ein Initiator mit jedem der zwei Ziel-Ports auf dem Storage Controller verbunden ist. 30 × 128 = 3,840. Da 3,840 die Gesamttiefe der Warteschlange von 2,048 überschreitet, sollten Sie eine der Optionen unter Schritt 3 zur Behebung wählen.
3. Wählen Sie eine der folgenden Optionen, um dem Storage Controller mehr Hosts hinzuzufügen.
   - Option 1:
     i. Weitere FC-Ziel-Ports hinzufügen.
     ii. Neuverteilung Ihrer FC-Initiatoren
     iii. Wiederholen Sie die Schritte 1 und 2. + die gewünschte Warteschlangentiefe von 3,840 überschreitet die verfügbare Warteschlangentiefe pro Port. Um dies zu beheben, können Sie jedem Controller einen FC-Zieladapter mit zwei Ports hinzufügen und Ihre FC-Switches neu Zone festlegen, so dass 15 Ihrer 30 Hosts mit einem Satz Ports verbunden werden. Die restlichen 15 Hosts verbinden sich mit einem zweiten Port-Satz. Die Warteschlangentiefe pro Port wird dann auf 15 × 128 = 1,920 reduziert.
   - Option 2:
     i. Weisen Sie jeden Host basierend auf seinem erwarteten I/O-Bedarf als „`large`“ oder „`small`“ zu.
     ii. Multiplizieren Sie die Anzahl der großen Initiatoren mit 128.
     iii. Multiplizieren Sie die Anzahl der kleinen Initiatoren mit 32.
     iv. Fügen Sie die beiden Ergebnisse zusammen.
     v. Wenn das Ergebnis weniger als 2,048 ist, stellen Sie die Warteschlangentiefe für große Hosts auf 128 und die Warteschlangentiefe für kleine Hosts auf 32 ein.
     vi. Wenn das Ergebnis immer noch größer als 2,048 pro Port ist, reduzieren Sie die Warteschlangentiefe pro Initiator, bis die gesamte Warteschlangentiefe kleiner als oder gleich 2,048 ist.

> Um die Warteschlangentiefe zu schätzen, die für einen bestimmten I/O-Durchsatz pro Sekunde erforderlich ist, verwenden Sie folgende Formel:
>
> Benötigte Queue-Tiefe = (Anzahl I/O pro Sekunde) × (Reaktionszeit)
>
> Wenn Sie beispielsweise 40,000 I/O pro Sekunde mit einer Reaktionszeit von 3 Millisekunden benötigen, dann ist die benötigte Warteschlangentiefe = 40,000 × (.003) = 120.

Die maximale Anzahl von Hosts, die Sie mit einem Zielport verbinden können, ist 64, wenn Sie sich entscheiden, die Warteschlangentiefe auf die grundlegende Empfehlung von 32 zu begrenzen. Wenn Sie sich jedoch für eine Warteschlangentiefe von 128 entscheiden, können maximal 16 Hosts mit einem Zielport verbunden sein. Je größer die Warteschlangentiefe, desto weniger Hosts, die ein einziger Zielport unterstützen kann. Wenn Sie eine solche Anforderung haben, dass Sie keine Kompromisse in der Warteschlangentiefe machen können, sollten Sie mehr Zielports erhalten.

Die gewünschte Warteschlangentiefe von 3,840 überschreitet die verfügbare Warteschlangentiefe pro Port. Es gibt 10 „`große`“ Hosts mit hohen Storage-I/O-Anforderungen und 20 „`skleine`“ Hosts mit niedrigen I/O-Anforderungen. Setzen Sie die Tiefe der Initiator-Warteschlange auf den großen Hosts auf 128 und die Tiefe der Initiator-Warteschlange auf den kleinen Hosts auf 32.

Ihre resultierende Gesamtwarteschlangentiefe beträgt (10 × 128) + (20 × 32) = 1,920.

Sie können die verfügbare Warteschlangentiefe gleichmäßig auf jeden Initiator verteilen.

Ihre resultierende Warteschlangentiefe pro Initiator beträgt 2,048 ÷ 30 = 68.

### Ändern Sie die Warteschlangentiefe für ONTAP-SAN-Hosts

Möglicherweise müssen Sie die Warteschlangentiefe auf Ihrem Host ändern, um die Höchstwerte für ITNs pro Knoten und FC-Port-Fan-in zu erreichen. Dies können Sie für Ihre Umgebung tun."Berechnen Sie die optimale Warteschlangentiefe"

#### AIX-Hosts

Sie können die Warteschlangentiefe auf AIX-Hosts mit dem `chdev` Befehl ändern. Mit dem `chdev` Befehl genommene Änderungen werden auch nach einem Neustart fortgeführt.

Beispiele:

- Um die Warteschlangentiefe für das hdisk7-Gerät zu ändern, verwenden Sie den folgenden Befehl:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Verwenden Sie den folgenden Befehl, um die Warteschlangentiefe für den FCS0-HBA zu ändern:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  Der Standardwert für `num_cmd_elems` ist 200. Der maximale Wert ist 2.048.

  > Unter Umständen muss der HBA in den Offline-Modus versetzt werden, um `num_cmd_elems` ihn zu ändern und ihn dann mithilfe der `rmdev -l fcs0 -R` `makdev -l fcs0 -P` Befehle und wieder in den Online-Modus zu versetzen.

#### HP-UX-Hosts erhältlich

Sie können die LUN- oder Gerätewarteschlangentiefe auf HP-UX-Hosts mit dem Kernel-Parameter ändern `scsi_max_qdepth`. Sie können die HBA-Warteschlangentiefe mit dem Kernel-Parameter ändern `max_fcp_reqs`.

- Der Standardwert für `scsi_max_qdepth` ist 8. Der maximale Wert ist 255.

  `scsi_max_qdepth` Kann auf einem laufenden System mit der `-u` Option des `kmtune` Befehls dynamisch geändert werden. Die Änderung wird für alle Geräte im System wirksam. Verwenden Sie beispielsweise den folgenden Befehl, um die LUN-Warteschlangentiefe auf 64 zu erhöhen:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

Mit dem `scsictl` Befehl kann die Warteschlangentiefe für einzelne Gerätedateien geändert werden. Änderungen mit dem `scsictl` Befehl gehen beim Neubooten des Systems nicht verloren. Um die Warteschlangentiefe für eine bestimmte Gerätedatei anzuzeigen und zu ändern, führen Sie den folgenden Befehl aus:

```
scsictl -a /dev/rdsk/c2t2d0

scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
```

- Der Standardwert für `max_fcp_reqs` ist 512. Der maximale Wert ist 1024.

  Der Kernel muss neu aufgebaut werden und das System muss neu gestartet werden, damit `max_fcp_reqs` die Änderungen wirksam werden. Verwenden Sie zum Ändern der HBA-Warteschlangentiefe in 256 beispielsweise den folgenden Befehl:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

#### Solaris-Hosts

Sie können die LUN- und HBA-Warteschlangentiefe für Ihre Solaris-Hosts einstellen.

- Für LUN-Warteschlangentiefe: Die Anzahl der auf einem Host verwendeten LUNs muss mit dem pro-LUN-Gashebel (lun-Queue-Tiefe) kleiner oder gleich dem Wert für die tgt-queue-Tiefe auf dem Host sein.
- Für Warteschlangentiefe in einem Sun Stack: Die nativen Treiber erlauben keine `max_throttle` Einstellungen pro LUN oder pro Ziel auf HBA-Ebene. Die empfohlene Methode zum Festlegen des `max_throttle` Werts für native Treiber ist auf der Ebene pro Device (VID_PID) in den `/kernel/drv/sd.conf` `/kernel/drv/ssd.conf` Dateien und. Das Host-Dienstprogramm setzt diesen Wert auf 64 für MPxIO-Konfigurationen und 8 für Veritas DMP-Konfigurationen.

**Schritte**

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. Suchen nach `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   Der Standardwert ist bei der Installation auf 32 gesetzt.

4. Legen Sie den gewünschten Wert basierend auf der Konfiguration Ihrer Umgebung fest.
5. Speichern Sie die Datei.
6. Starten Sie den Host mit dem `sync; sync; sync; reboot -- -r` Befehl neu.

#### VMware Hosts für einen QLogic HBA

Verwenden Sie den `esxcfg-module` Befehl, um die Einstellungen für die HBA-Zeitüberschreitung zu ändern. `esx.conf`Eine manuelle Aktualisierung der Datei wird nicht empfohlen.

**Schritte**

1. Melden Sie sich als Root-Benutzer an der Service-Konsole an.

2. `#vmkload_mod -l`Überprüfen Sie mit dem Befehl, welches Qlogic HBA-Modul aktuell geladen ist.
3. Führen Sie für eine einzelne Instanz eines Qlogic HBA den folgenden Befehl aus:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

> Dieses Beispiel verwendet das Modul qla2300_707. Verwenden Sie das entsprechende Modul basierend auf der Ausgabe von `vmkload_mod -l`.

4. Speichern Sie Ihre Änderungen mit dem folgenden Befehl:

```
#/usr/sbin/esxcfg-boot -b
```

5. Starten Sie den Server mit folgendem Befehl neu:

```
#reboot
```

6. Bestätigen Sie die Änderungen mit folgenden Befehlen:
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

#### VMware-Hosts für einen Emulex HBA

Verwenden Sie den `esxcfg-module` Befehl, um die Einstellungen für die HBA-Zeitüberschreitung zu ändern. `esx.conf`Eine manuelle Aktualisierung der Datei wird nicht empfohlen.

**Schritte**

1. Melden Sie sich als Root-Benutzer an der Service-Konsole an.
2. `#vmkload_mod -l grep lpfc`Überprüfen Sie mit dem Befehl, welcher Emulex HBA aktuell geladen ist.
3. Geben Sie für eine einzelne Instanz eines Emulex HBA den folgenden Befehl ein:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

> Je nach HBA-Modell kann das Modul entweder lpfcdd_7xx oder lpfcdd_732 sein. Der obige Befehl verwendet das lpfcdd_7xx-Modul. Sie sollten das entsprechende Modul basierend auf dem Ergebnis von verwenden `vmkload_mod -l`.

   Durch Ausführen dieses Befehls wird die LUN-Warteschlangentiefe auf 16 für den HBA festgelegt, der von lpfc0 dargestellt wird.

4. Führen Sie für mehrere Instanzen eines Emulex HBA den folgenden Befehl aus:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

   Die LUN-Warteschlangentiefe für lpfc0 und die LUN-Warteschlangentiefe für lpfc1 ist auf 16 festgelegt.

5. Geben Sie den folgenden Befehl ein:

```
#esxcfg-boot -b
```

6. Starten Sie mit `#reboot`.

#### Windows Hosts für einen Emulex HBA

Auf Windows-Hosts können Sie das `LPUTILNT` Dienstprogramm verwenden, um die Warteschlangentiefe für Emulex-HBAs zu aktualisieren.

**Schritte**

1. Führen Sie das `LPUTILNT` Dienstprogramm aus `C:\WINNT\system32`, das sich im Verzeichnis befindet.
2. Wählen Sie im Menü auf der rechten Seite die Option **Drive Parameters** aus.
3. Scrollen Sie nach unten und doppelklicken Sie auf **QueueDepth**.

> Wenn Sie **QueueDepth** größer als 150 einstellen, muss auch der folgende Wert für die Windows-Registrierung entsprechend erhöht werden:
>
> `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

#### Windows Hosts für einen Qlogic HBA

Auf Windows-Hosts können Sie die und das `SANsurfer` HBA-Manager-Dienstprogramm verwenden, um die Warteschlangentiefen für Qlogic HBAs zu aktualisieren.

**Schritte**

1. Führen Sie das `SANsurfer` HBA-Manager-Dienstprogramm aus.
2. Klicken Sie auf **HBA-Port** > **Einstellungen**.
3. Klicken Sie im Listenfeld auf **Erweiterte HBA-Porteinstellungen**.
4. Aktualisieren Sie den `Execution Throttle` Parameter.

#### Linux Hosts für Emulex HBA

Sie können die Warteschlangentiefe eines Emulex HBA auf einem Linux-Host aktualisieren. Damit die Updates bei einem Neustart erhalten bleiben, müssen Sie dann ein neues RAM-Laufwerk-Image erstellen und den Host neu starten.

**Schritte**

1. Geben Sie die zu ändernden Warteschlangentiefe an:

   ```
   modinfo lpfc|grep queue_depth
   ```

   Die Liste der Parameter für die Warteschlangentiefe mit ihrer Beschreibung wird angezeigt. Je nach Betriebssystemversion können Sie einen oder mehrere der folgenden Parameter für die Warteschlangentiefe ändern:

   - `lpfc_lun_queue_depth`: Maximale Anzahl von FC-Befehlen, die in eine bestimmte LUN (uint) eingereiht werden können
   - `lpfc_hba_queue_depth`: Maximale Anzahl von FC-Befehlen, die in eine Warteschlange für einen lpfc HBA (uint) gestellt werden können
   - `lpfc_tgt_queue_depth`: Maximale Anzahl von FC-Befehlen, die in einen bestimmten Zielport (uint)

eingereiht werden können

Der `lpfc_tgt_queue_depth` Parameter gilt nur für Red hat Enterprise Linux 7.x-Systeme, SUSE Linux Enterprise Server 11 SP4-Systeme und 12.x-Systeme.

2. Aktualisieren Sie die Warteschlangentiefe, indem Sie der `/etc/modprobe.conf` Datei für ein Red hat Enterprise Linux 5.x-System und der `/etc/modprobe.d/scsi.conf` Datei für ein Red hat Enterprise Linux 6.x- oder 7.x-System oder einem SUSE Linux Enterprise Server 11.x- oder 12.x-System die Warteschlangentiefe hinzufügen.

   Abhängig von Ihrer Betriebssystemversion können Sie einen oder mehrere der folgenden Befehle hinzufügen:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Erstellen Sie ein neues RAM-Laufwerk-Image, und starten Sie dann den Host neu, damit die Updates bei einem Neustart erhalten bleiben.

   Weitere Informationen finden Sie im "Systemadministration" für Ihre Version des Linux-Betriebssystems.

4. Vergewissern Sie sich, dass die Werte für die Warteschlangentiefe für jeden Parameter aktualisiert werden, den Sie geändert haben:

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   Der aktuelle Wert der Warteschlangentiefe wird angezeigt.

#### Linux Hosts für QLogic HBA

Sie können die Tiefe der Gerätewarteschlange eines QLogic-Treibers auf einem Linux-Host aktualisieren. Damit die Updates bei einem Neustart erhalten bleiben, müssen Sie dann ein neues RAM-Laufwerk-Image erstellen und den Host neu starten. Mithilfe der QLogic HBA Management-GUI oder der Befehlszeilenschnittstelle (CLI) lässt sich die QLogic HBA-Warteschlangentiefe ändern.

Diese Aufgabe zeigt, wie die QLogic HBA CLI zum Ändern der QLogic HBA-Warteschlangentiefe verwendet wird

**Schritte**

1. Geben Sie den Parameter für die Warteschlangentiefe des Geräts an, der geändert werden soll:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   Sie können nur den `ql2xmaxqdepth` Parameter „Warteschlangentiefe“ ändern, der die maximale Warteschlangentiefe angibt, die für jede LUN festgelegt werden kann. Der Standardwert ist 64 für RHEL 7.5 und höher. Der Standardwert ist 32 für RHEL 7.4 und früher.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Wert für die Tiefe der Gerätewarteschlange aktualisieren:
   - Wenn Sie die Änderungen persistent machen möchten, führen Sie die folgenden Schritte aus:
     i. Aktualisieren Sie die Warteschlangentiefe, indem Sie der `/etc/modprobe.conf` Datei für ein Red hat Enterprise Linux 5.x-System und der `/etc/modprobe.d/scsi.conf` Datei für ein Red hat Enterprise Linux 6.x- oder 7.x-System oder einem SUSE Linux Enterprise Server 11.x- oder 12.x-System den Parameter Warteschlangentiefe hinzufügen: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. Erstellen Sie ein neues RAM-Laufwerk-Image, und starten Sie dann den Host neu, damit die Updates bei einem Neustart erhalten bleiben.

     Weitere Informationen finden Sie im "Systemadministration" für Ihre Version des Linux-Betriebssystems.
   - Wenn Sie den Parameter nur für die aktuelle Sitzung ändern möchten, führen Sie den folgenden Befehl aus:

     `echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

     Im folgenden Beispiel wird die Warteschlangentiefe auf 128 gesetzt.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Überprüfen Sie, ob die Werte für die Warteschlangentiefe aktualisiert wurden:

   `cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

   Der aktuelle Wert der Warteschlangentiefe wird angezeigt.

4. Ändern Sie die Warteschlangentiefe von QLogic HBA, indem Sie den Firmware-Parameter `Execution Throttle` aus dem QLogic HBA BIOS aktualisieren.
   a. Melden Sie sich bei der QLogic HBA Management CLI an:

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. Wählen Sie im Hauptmenü die `Adapter Configuration` Option aus.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

c. Wählen Sie in der Liste der Adapterkonfigurationsparameter die `HBA Parameters` Option aus.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Wählen Sie aus der Liste der HBA-Ports den erforderlichen HBA-Port aus.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

Die Details des HBA-Ports werden angezeigt.

e. Wählen Sie im Menü HBA-Parameter die `Display HBA Parameters` Option aus `Execution Throttle`, um den aktuellen Wert der Option anzuzeigen.

Der Standardwert der `Execution Throttle` Option ist 65535.

```
HBA Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
--------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```
--------------------------------------------------------------------------
--------
Connection Options              : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                       : Auto
Frame Size                      : 2048
Hard Loop ID                    : 0
Loop Reset Delay (seconds)      : 5
Enable Host HBA BIOS            : Enabled
Enable Hard Loop ID             : Disabled
Enable FC Tape Support          : Enabled
Operation Mode                  : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)   : 0
**Execution Throttle              : 65535**
Login Retry Count               : 8
Port Down Retry Count           : 30
Enable LIP Full Login           : Enabled
Link Down Timeout (seconds)     : 30
Enable Target Reset             : Enabled
LUNs Per Target                 : 128
Out Of Order Frame Assembly     : Disabled
Enable LR Ext. Credits          : Disabled
Enable Fabric Assigned WWN      : N/A

Press <Enter> to continue:
```

a. Drücken Sie **Enter**, um fortzufahren.

b. Wählen Sie im Menü HBA-Parameter die `Configure HBA Parameters` Option zum Ändern der HBA-Parameter aus.

c. Wählen Sie im Menü Parameter konfigurieren die `Execute Throttle` Option aus, und aktualisieren Sie den Wert dieses Parameters.

```
Configure Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. Drücken Sie **Enter**, um fortzufahren.

e. Wählen Sie im Menü Parameter konfigurieren die `Commit Changes` Option aus, um die Änderungen zu speichern.

f. Verlassen Sie das Menü.