SAN Speicherverwaltung

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/san-admin/san-host-provisioning-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

SAN Speicherverwaltung . . . 1
SAN Konzepte . . . 1
SAN Provisionierung mit iSCSI in ONTAP . . . 1
iSCSI-Service-Management . . . 2
SAN-Provisionierung mit FC in ONTAP . . . 9
Informationen zur ONTAP Unterstützung für FC-SP-3-Sicherheit . . . 10
SAN Provisionierung mit NVMe in ONTAP . . . 11
Unterstützung von ONTAP für SAN Multipathing und automatischen LIF Failover . . . 11
SAN-Volumes . . . 16
Informationen zum SAN hostseitigen Speicherplatzmanagement in ONTAP . . . 21
Erfahren Sie mehr über ONTAP SAN igroups . . . 22
Initiator WWPNs und iSCSI-Knotennamen für ONTAP igroups . . . 23
Vorteile der Verwendung einer virtualisierten SAN-Umgebung in ONTAP . . . 23
Wie ONTAP VMware VAAI Funktionen die Performance von ESX Hosts verbessern . . . 26
SAN Copy Offload . . . 27
SAN Verwaltung . . . 31
SAN Bereitstellung . . . 31
NVMe Bereitstellung . . . 41
LUNs verwalten . . . 52
Initiatorgruppen und Portsets verwalten . . . 66
iSCSI Protokollverwaltung . . . 72
FC-Protokoll verwalten . . . 79
NVMe-Protokoll verwalten . . . 81
Systeme mit FC Adaptern verwalten . . . 90
LIFs für alle SAN-Protokolle verwalten . . . 101
ONTAP Speicherplatzzuweisung für SAN-Protokolle aktivieren . . . 107
Empfohlene Kombinationen für Volume- und Datei- oder LUN-Konfigurationen . . . 109
SAN Datenschutz . . . 114
ONTAP Datenschutzmethoden für SAN-Umgebungen . . . 114
Wiederherstellung einer einzelnen LUN aus einem ONTAP Snapshot . . . 115
Alle LUNs eines Volumes aus einem ONTAP Snapshot wiederherstellen . . . 117
Informationen zu ONTAP FlexClone LUNs . . . 118
Konfiguration und Nutzung von SnapVault Backups in einer SAN-Umgebung . . . 119
Empfohlene Konfiguration für den Anschluss eines Host-Backup-Systems an ONTAP . . . 127
Ein Host-Backup-System kann zum Schutz einer LUN auf dem ONTAP-Speichersystem eingesetzt werden. . . . 128
SAN Konfigurationsreferenz . . . 129
Erfahren Sie mehr über die ONTAP SAN-Konfiguration . . . 130
iSCSI Konfigurationen . . . 130
FC Konfigurationen . . . 133
FCoE Konfigurationen . . . 138
FC- und FCoE-Zonierung . . . 142
Anforderungen an SAN-Hosts, die mit ONTAP und Nicht-NetApp-Systemen verbunden sind . . . 146

SAN-Konfigurationen in einer MetroCluster Umgebung 146
ONTAP Unterstützung für SAN Host Multipathing 148
Konfigurationsgrenzen 150

SAN Speicherverwaltung

SAN Konzepte

SAN Provisionierung mit iSCSI in ONTAP

In SAN-Umgebungen sind Speichersysteme Ziele, die Speicherzielgeräte besitzen. Für iSCSI und FC werden die Speicherzielgeräte als LUNs (logische Einheiten) bezeichnet. Für Non-Volatile Memory Express (NVMe) über Fibre Channel werden die Speicherzielgeräte als Namespaces bezeichnet.

Der Speicher wird konfiguriert, indem LUNs für iSCSI und FC oder Namespaces für NVMe erstellt werden. Auf die LUNs oder Namespaces greifen Hosts über Internet Small Computer Systems Interface (iSCSI) oder Fibre Channel (FC) Protokollnetzwerke zu.

Zur Verbindung mit iSCSI-Netzwerken können Hosts Standard-Ethernet-Netzwerkadapter (NICs), TCP-Offload-Engine-Karten (TOE) mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte iSCSI-Hostbusadapter (HBAs) verwenden.

Für die Verbindung mit FC-Netzwerken sind FC-HBAs oder CNAs auf den Hosts erforderlich.

Unterstützte FC-Protokolle umfassen:

- FC
- FCoE
- NVMe

iSCSI-Zielknoten-Netzwerkverbindungen und Namen

iSCSI-Zielknoten können auf verschiedene Arten mit dem Netzwerk verbunden werden:

- Über Ethernet-Schnittstellen mit in ONTAP integrierter Software.
- Über mehrere Systemschnittstellen, wobei eine Schnittstelle für iSCSI verwendet wird, die auch Datenverkehr für andere Protokolle wie SMB und NFS übertragen kann.
- Verwendung eines Unified Zieladapter (UTA) oder eines konvergierten Netzwerkadapters (CNA).

Jeder iSCSI-Knoten muss einen Node-Name haben.

Die beiden Formate bzw. Typbezeichnungen für iSCSI-Node-Namen sind *iqn* und *eui*. Das SVM iSCSI-Ziel verwendet immer die iqn-Typbezeichnung. Der Initiator kann entweder die iqn-Typbezeichnung oder die eui-Typbezeichnung verwenden.

Node-Name des Storage-Systems

Jede SVM, die iSCSI ausführt, hat einen Node-Name, der auf einem umgekehrten Domänennamen und einer eindeutigen Codierungsnummer basiert.

Der Node-Name wird im folgenden Format angezeigt:

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

Das folgende Beispiel zeigt den standardmäßigen Node-Name für ein Speichersystem mit einer eindeutigen Codierungsnummer:

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

TCP-Port für iSCSI

Das iSCSI-Protokoll ist in ONTAP so konfiguriert, dass es den TCP-Port 3260 verwendet.

ONTAP unterstützt keine Änderung der Portnummer für iSCSI. Portnummer 3260 ist als Teil der iSCSI-Spezifikation registriert und kann von keiner anderen Anwendung oder keinem anderen Dienst verwendet werden.

Verwandte Informationen

"NetApp Dokumentation: ONTAP SAN Hostkonfiguration"

iSCSI-Service-Management

Informationen zur Verwaltung des iSCSI-Service in ONTAP

Die Verfügbarkeit des iSCSI-Service auf den iSCSI-Logischen Schnittstellen der Storage Virtual Machine (SVM) kann mit den `vserver iscsi interface enable`- oder `vserver iscsi interface disable`-Befehlen verwaltet werden.

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

Wie iSCSI auf dem Host implementiert ist

iSCSI kann auf dem Host mit Hardware oder Software implementiert werden.

iSCSI kann auf eine der folgenden Arten implementiert werden:

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

  Die Verarbeitung des iSCSI-Protokolls erfolgt weiterhin durch die Host-Software.

Wie die iSCSI-Authentifizierung in ONTAP funktioniert

In der Anfangsphase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanfrage an das Speichersystem, um eine iSCSI-Sitzung zu beginnen. Das Speichersystem genehmigt oder verweigert anschließend die Anmeldeanfrage oder stellt fest, dass keine Anmeldung erforderlich ist.

iSCSI-Authentifizierungsverfahren sind:

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

Sie können ein CHAP-Passwort festlegen oder ein hexadezimales geheimes Passwort generieren. Es gibt zwei Arten von CHAP-Benutzernamen und Passwörtern:

  - Eingehend, das Speichersystem authentifiziert den Initiator.

    Eingangseinstellungen sind erforderlich, wenn Sie die CHAP-Authentifizierung verwenden.

  - Ausgehend, dies ist eine optionale Einstellung, um dem Initiator die Authentifizierung des Speichersystems zu ermöglichen.

    Ausgehende Einstellungen können nur verwendet werden, wenn im Speichersystem ein eingehender Benutzername und ein Passwort definiert sind.

- deny—Dem Initiator wird der Zugriff auf das Speichersystem verweigert.
- keine, das Speichersystem erfordert keine Authentifizierung für den Initiator.

Sie können die Liste der Initiatoren und deren Authentifizierungsverfahren definieren. Es kann auch ein Standard-Authentifizierungsverfahren definiert werden, das für Initiatoren gilt, die nicht in dieser Liste enthalten sind.

Verwandte Informationen

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

Informationen zum Sicherheitsmanagement von iSCSI-Initiatoren in ONTAP

ONTAP bietet zahlreiche Funktionen zur Verwaltung der Sicherheit für iSCSI-Initiatoren. Es ist möglich, eine Liste von iSCSI-Initiatoren und das jeweilige Authentifizierungsverfahren für jeden Initiator zu definieren, die Initiatoren und ihre zugehörigen Authentifizierungsverfahren in der Authentifizierungsliste anzuzeigen, Initiatoren zur Authentifizierungsliste hinzuzufügen oder daraus zu entfernen sowie das Standard-Authentifizierungsverfahren für iSCSI-Initiatoren festzulegen, die nicht in der Liste enthalten sind.

Informationen zur iSCSI-Endpunktisolierung in ONTAP

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

Alle iSCSI-Initiatoren müssen beim Aufbau einer Sitzung oder Verbindung mit einem Ziel ihre Ursprungs-IP-Adresse angeben. Diese neue Funktion verhindert, dass sich ein Initiator im Cluster anmeldet, wenn die Ursprungs-IP-Adresse nicht unterstützt wird oder unbekannt ist, und stellt ein eindeutiges Identifizierungsschema bereit. Jeder Initiator, der von einer nicht unterstützten oder unbekannten IP-Adresse stammt, wird auf der iSCSI-Sitzungsschicht bei der Anmeldung abgewiesen, sodass der Initiator keinen Zugriff auf LUNs oder Volumes innerhalb des Clusters erhält.

Diese neue Funktionalität wird mit zwei neuen Befehlen implementiert, die bei der Verwaltung bereits vorhandener Einträge unterstützen.

Initiator-Adressbereich hinzufügen

Die Sicherheitsverwaltung des iSCSI-Initiators lässt sich verbessern, indem ein IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security add-initiator-address-range` Befehl

hinzugefügt werden.

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

Initiator-Adressbereich entfernen

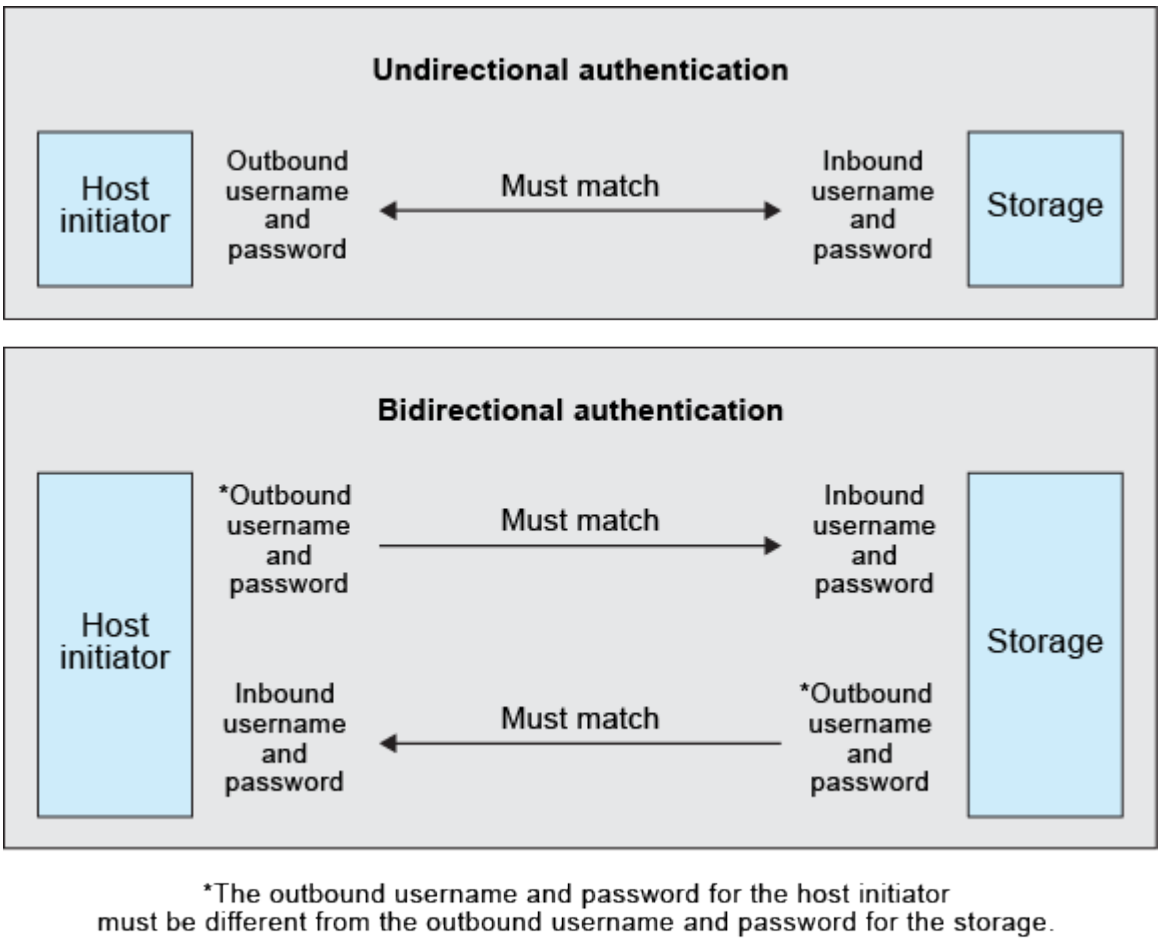
Einen IP-Adressbereich oder mehrere IP-Adressen mit dem `vserver iscsi security remove-initiator-address-range` Befehl entfernen.

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

Informationen zur CHAP-Authentifizierung für iSCSI-Initiatoren in ONTAP

Das Challenge Handshake Authentication Protocol (CHAP) ermöglicht die authentifizierte Kommunikation zwischen iSCSI-Initiatoren und Zielen. Bei Verwendung der CHAP-Authentifizierung werden CHAP-Benutzernamen und -Passwörter sowohl auf dem Initiator als auch auf dem Speichersystem definiert.

In der Initialisierungsphase einer iSCSI-Sitzung sendet der Initiator eine Anmeldeanfrage an das Speichersystem, um die Sitzung zu beginnen. Die Anmeldeanfrage enthält den CHAP-Benutzernamen des Initiators und den CHAP-Algorithmus. Das Speichersystem antwortet mit einer CHAP-Herausforderung. Der Initiator gibt eine CHAP-Antwort an. Das Speichersystem überprüft die Antwort und authentifiziert den Initiator. Das CHAP-Passwort wird zur Berechnung der Antwort verwendet.



Authentifizierung	Ausgehend	Eingehend	Übereinstimmung?
Unidirektional	Benutzername und Passwort des Host-Initiators	Benutzername und Passwort für Storage	Muss übereinstimmen
Bidirektional	Benutzername und Passwort des Host-Initiators	Benutzername und Passwort für Storage	Muss übereinstimmen
Bidirektional	Benutzername und Passwort für Storage	Benutzername und Passwort des Host-Initiators	Muss übereinstimmen

Der Benutzername und das Passwort für den ausgehenden Host-Initiator müssen sich von dem Benutzernamen und dem Passwort für das Speichersystem unterscheiden.

Richtlinien für die Verwendung der CHAP-Authentifizierung

Diese Richtlinien sind bei der Verwendung der CHAP-Authentifizierung zu beachten.

- Wenn auf dem Speichersystem ein Benutzername und ein Passwort für eingehende Verbindungen definiert werden, müssen derselbe Benutzername und dasselbe Passwort für die ausgehenden CHAP-Einstellungen auf dem Initiator verwendet werden. Wenn auf dem Speichersystem zusätzlich ein Benutzername und ein Passwort für ausgehende Verbindungen definiert werden, um die bidirektionale Authentifizierung zu ermöglichen, müssen derselbe Benutzername und dasselbe Passwort für die eingehenden CHAP-Einstellungen auf dem Initiator verwendet werden.
- Sie können nicht denselben Benutzernamen und dasselbe Passwort für die Einstellungen für eingehende und ausgehende Verbindungen im Speichersystem verwenden.
- CHAP-Benutzernamen können zwischen 1 und 128 Byte lang sein.

  Das System lässt keine leeren Benutzernamen zu.

- CHAP-Passwörter (Geheimnisse) können 1 bis 512 Byte lang sein.

  Passwörter können Hexadezimalwerte oder Zeichenketten sein. Bei Hexadezimalwerten sollte der Wert mit dem Präfix “0x” oder “0X” eingegeben werden.

  Das System lässt kein leeres Passwort zu.

> ONTAP erlaubt die Verwendung von Sonderzeichen, nicht-englischen Buchstaben, Zahlen und Leerzeichen für CHAP-Passwörter (Geheimnisse). Dies unterliegt jedoch den Einschränkungen des Hosts. Wenn einer dieser Werte von Ihrem spezifischen Host nicht erlaubt ist, können sie nicht verwendet werden.
>
> Beispielsweise erfordert der Microsoft iSCSI Softwareinitiator, dass sowohl das Initiator- als auch das Ziel-CHAP-Passwort mindestens 12 Byte lang sind, wenn keine IPsec-Verschlüsselung verwendet wird. Die maximale Passwortlänge beträgt unabhängig davon, ob IPsec verwendet wird, 16 Byte.
>
> Zusätzliche Einschränkungen sind in der Dokumentation des Initiators aufgeführt.

Wie ONTAP iSCSI Schnittstellenzugriffslisten die Performance und Sicherheit verbessern

ISCSI-Schnittstellenzugriffslisten können verwendet werden, um die Anzahl der LIFs in

einer SVM zu begrenzen, auf die ein Initiator zugreifen kann, wodurch Leistung und Sicherheit erhöht werden.

Wenn ein Initiator eine Erkennungssitzung mit einem iSCSI `SendTargets` Befehl startet, erhält er die IP-Adressen, die der LIF (Netzwerkschnittstelle) zugeordnet sind und sich in der Zugriffsliste befindet. Standardmäßig haben alle Initiatoren Zugriff auf alle iSCSI LIFs in der SVM. Mit der Zugriffsliste kann die Anzahl der LIFs in der SVM, auf die ein Initiator Zugriff hat, eingeschränkt werden.

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 verwaltet Informationen über aktive iSCSI-Geräte im Netzwerk, einschließlich ihrer IP-Adressen, iSCSI-Node-Namen (IQNs) 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 Initiator und Ziel aktiviert haben, kann die Management-LIF einer Storage Virtual Machine (SVM) verwendet werden, um alle iSCSI-LIFs dieser SVM auf dem iSNS-Server zu registrieren. Nach Abschluss der Registrierung kann der iSCSI-Initiator den iSNS-Server abfragen, um alle LIFs für diese SVM zu ermitteln.

Wenn Sie sich für die Nutzung eines iSNS-Service entscheiden, muss sichergestellt sein, dass Ihre Storage Virtual Machines (SVMs) ordnungsgemäß bei einem Internet Storage Name Service (iSNS) Server registriert sind.

Falls kein iSNS-Server im Netzwerk vorhanden ist, muss jedes Ziel manuell so konfiguriert werden, dass es für den Host sichtbar ist.

Was ein iSNS-Server tut

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

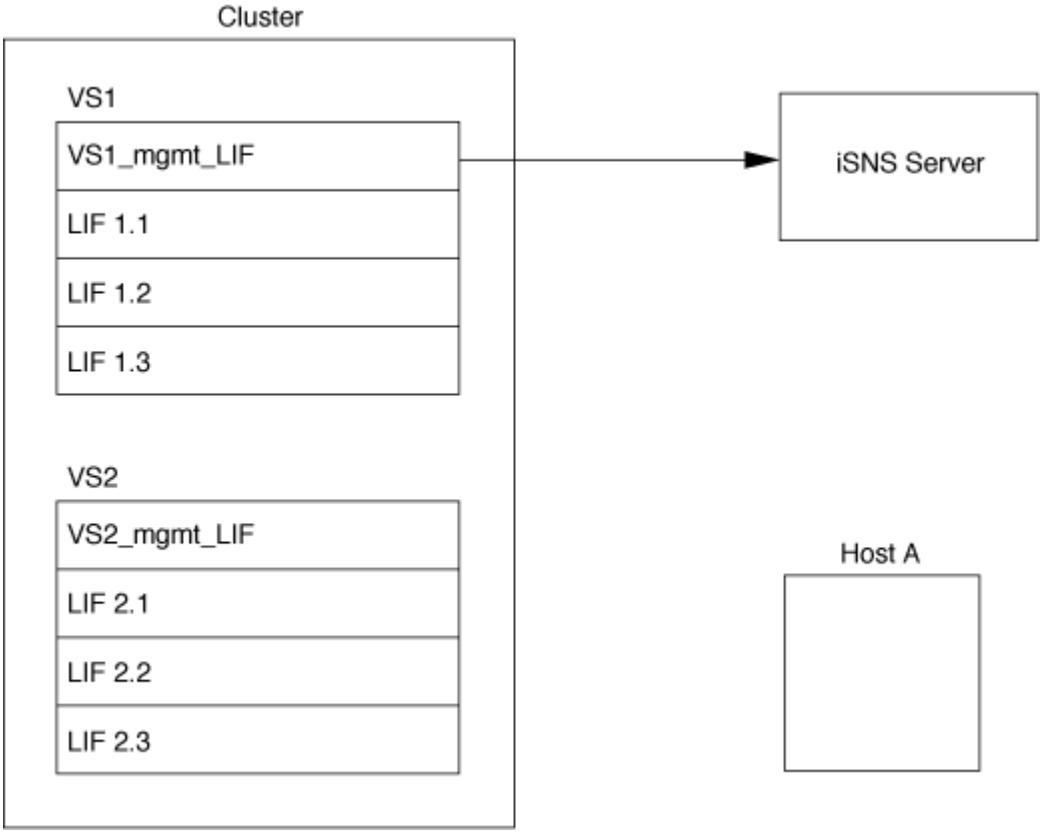
Das iSNS-Protokoll ermöglicht die automatische Erkennung und Verwaltung von iSCSI-Geräten in einem IP-Speichernetzwerk. Ein iSCSI-Initiator kann den iSNS-Server abfragen, um iSCSI-Zielgeräte zu entdecken.

NetApp liefert oder vertreibt keine iSNS-Server. Sie können diese Server von einem von NetApp unterstützten Anbieter beziehen.

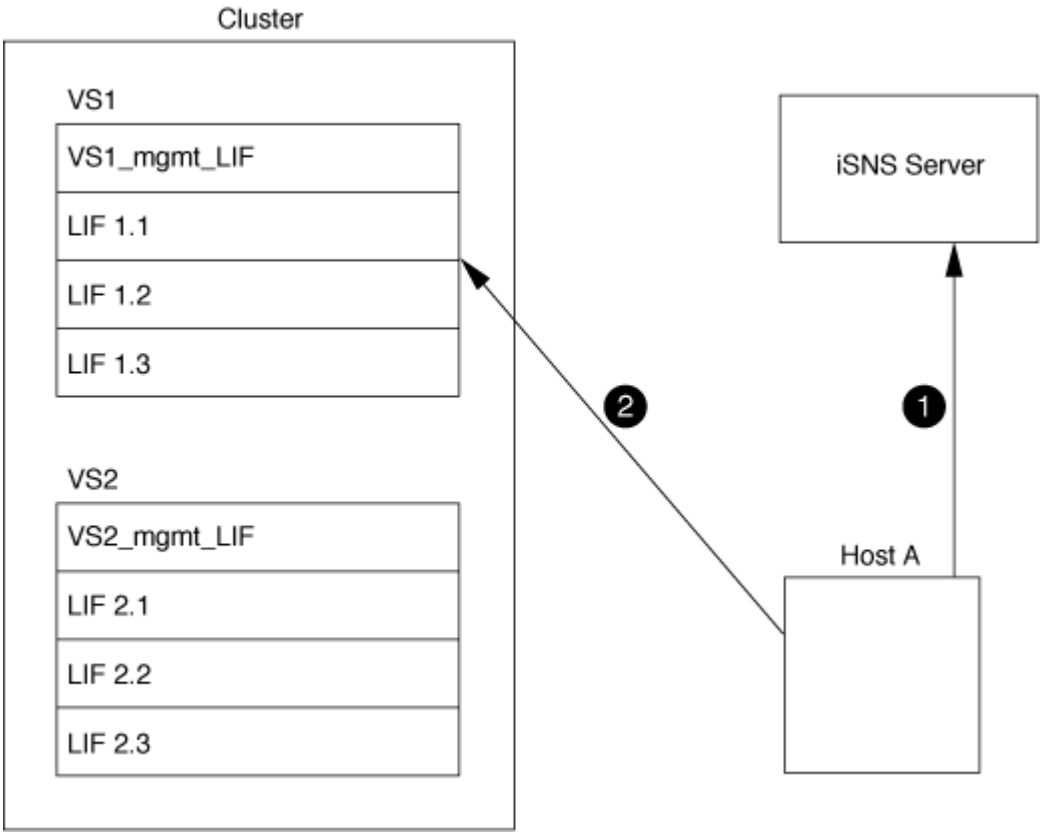
Wie SVMs mit einem iSNS-Server interagieren

Der iSNS-Server kommuniziert mit jeder Storage Virtual Machine (SVM) über die SVM-Management-LIF. Die Management-LIF registriert alle iSCSI-Ziel Node-Name, 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 verfügt der iSNS Server über 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 zu nutzen.



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 LIFs für „VS1“ ermittelt hat, kann Host A eine Verbindung zu jeder beliebigen LIF in „VS1“ herstellen, wie in Schritt 2 gezeigt. Host A kennt keine der LIFs in „VS2“, bis die Management-LIF „VS2_mgmt_LIF“ für „VS2“ sich beim iSNS-Server registriert hat.



Wenn Sie jedoch die Schnittstellenzugriffslisten definieren, kann der Host nur die in der Schnittstellenzugriffsliste definierten LIFs verwenden, um auf das Ziel zuzugreifen.

Nach der Erstkonfiguration 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 Versand der Aktualisierung durch ONTAP an den iSNS-Server kann eine Verzögerung von einigen Minuten auftreten. Eine sofortige Aktualisierung der iSNS-Informationen auf dem iSNS-Server kann erzwungen werden: `vserver iscsi isns update`. Weitere Informationen zu `vserver iscsi isns update` finden sich in der "ONTAP-Befehlsreferenz".

Befehle zur Verwaltung von iSNS

ONTAP stellt Befehle zur Verwaltung Ihres iSNS-Dienstes bereit.

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Konfiguration eines iSNS-Dienstes	`vserver iscsi isns create`
Einen iSNS-Dienst starten	`vserver iscsi isns start`
Einen iSNS Dienst modifizieren	`vserver iscsi isns modify`
iSNS-Dienstkonfiguration anzeigen	`vserver iscsi isns show`
Eine Aktualisierung der registrierten iSNS-Informationen erzwingen	`vserver iscsi isns update`
Einen iSNS-Dienst beenden	`vserver iscsi isns stop`

Einen iSNS Dienst entfernen	`vserver iscsi isns delete`
Die Manpage für einen Befehl anzeigen	`man command name`

Weitere Informationen zu `vserver iscsi isns` finden sich in der "ONTAP-Befehlsreferenz".

SAN-Provisionierung mit FC in ONTAP

Es ist wichtig, die grundlegenden Konzepte zu kennen, die zum Verständnis der Implementierung eines FC SAN durch ONTAP erforderlich sind.

Wie FC-Zielknoten mit dem Netzwerk verbunden sind

Speichersysteme und Hosts verfügen über Adapter, sodass sie mit Kabeln an FC-Switches angeschlossen werden können.

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

> Direkte Verbindungen von Hosts mit FC zu Nodes werden nicht unterstützt, NPIV ist erforderlich und dies erfordert die Verwendung eines Switches. Bei iSCSI-Sitzungen funktioniert die Kommunikation sowohl mit netzwerkgerouteten Verbindungen als auch mit Direktverbindungen. Beide Methoden werden jedoch von ONTAP unterstützt.

Wie FC-Nodes identifiziert werden

Jede mit FC konfigurierte SVM ist durch einen weltweiten Node-Name (WWNN) identifiziert.

Wie WWPNs verwendet werden

WWPNs identifizieren jede LIF in einer SVM, die für FC konfiguriert ist. Diese LIFs nutzen die physischen FC-Ports in jedem Node im Cluster, wobei es sich um FC-Zieladapter, UTA oder UTA2 handeln kann, die in den Nodes als FC oder FCoE konfiguriert sind.

- Erstellung einer Initiatorgruppe

  Die WWPNs der HBAs des Hosts werden verwendet, um eine Initiatorgruppe (igroup) zu erstellen. Eine Initiatorgruppe wird verwendet, um den Hostzugriff auf bestimmte LUNs zu steuern. Eine Initiatorgruppe kann erstellt werden, indem eine Sammlung von WWPNs von Initiatoren in einem FC-Netzwerk angegeben wird. Wenn eine LUN auf einem Speichersystem einer Initiatorgruppe zugeordnet wird, erhalten alle Initiatoren dieser Gruppe Zugriff auf diese LUN. Befindet sich die WWPN eines Hosts nicht in einer Initiatorgruppe, die einer LUN zugeordnet ist, hat dieser Host keinen Zugriff auf die LUN. Das bedeutet, dass die LUNs auf diesem Host nicht als Datenträger angezeigt werden.

  Sie können auch Portsets erstellen, um eine LUN nur auf bestimmten Zielports sichtbar zu machen. Ein Portset besteht aus einer Gruppe von FC-Zielports. Eine Initiatorgruppe kann an ein Portset gebunden werden. Jeder Host in der Initiatorgruppe kann auf die LUNs nur zugreifen, indem er eine Verbindung zu den Zielports im Portset herstellt.

- Eindeutige Identifizierung von FC LIFs

  WWPNs identifizieren eindeutig jede FC logische Schnittstelle. Das Host-Betriebssystem verwendet die

Kombination aus WWNN und WWPN, um SVMs und FC LIFs zu identifizieren. Einige Betriebssysteme erfordern persistentes Binden, damit die LUN auf dem Host unter derselben Ziel-ID erscheint.

Wie die weltweite Namensvergabe funktioniert

Weltweite Namen werden in ONTAP sequenziell erstellt. Aufgrund der Art und Weise, wie ONTAP sie zuweist, kann es jedoch so erscheinen, als ob sie in einer nicht-sequenziellen Reihenfolge vergeben werden.

Jeder Adapter verfügt über eine vorkonfigurierte WWPN und WWNN, aber ONTAP verwendet diese vorkonfigurierten Werte nicht. Stattdessen weist ONTAP eigene WWPNs oder WWNNs zu, basierend auf den MAC-Adressen der integrierten Ethernet-Ports.

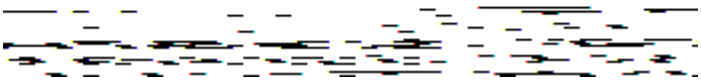
Die weltweiten Namen erscheinen bei ihrer Vergabe möglicherweise nicht fortlaufend, aus folgenden Gründen:

- Weltweit werden Namen für alle Nodes und Storage Virtual Machines (SVMs) im Cluster vergeben.
- Weltweit freigegebene Namen werden wiederverwendet und dem Pool verfügbarer Namen hinzugefügt.

Wie FC-Switches identifiziert werden

Fibre Channel Switches haben einen weltweiten Node-Name (WWNN) für das Gerät selbst und einen weltweiten Portnamen (WWPN) für jeden seiner Ports.

Das folgende Diagramm zeigt beispielsweise, wie die WWPNs den einzelnen Ports eines 16-Port Brocade Switches zugewiesen werden. Einzelheiten dazu, wie die Ports bei einem bestimmten Switch nummeriert sind, enthält die vom Hersteller bereitgestellte Dokumentation 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

Informationen zur ONTAP Unterstützung für FC-SP-3-Sicherheit

Ab ONTAP 9.20.1 unterstützt ONTAP Authentifizierung und Verschlüsselung nach Fibre Channel Security Protocol 3 (FC-SP-3) für sichere Broadcom Hostbusadapter (HBAs) auf bestimmten ONTAP Systemen. FC-SP-3 bietet Verschlüsselung auf Hardware-Ebene und Geräteauthentifizierung, um Daten auf der Übertragungsstrecke zwischen FC- und NVMe/FC-Hosts sowie ONTAP Storage-Systemen vor Abfangen, Manipulation und unberechtigtem Zugriff zu schützen, bei gleichbleibender Performance und in Übereinstimmung mit den T11 FC-Sicherheitsstandards.

Die folgenden sicheren HBAs von Broadcom unterstützen FC-SP-3:

- Zielkarten: LPe38104
- Initiatorkarten: LPe38102 (64G), LPe37102 (32G)

Mit "NetApp Hardware Universe" können Sie überprüfen, ob Ihr spezifisches ONTAP System die erforderlichen HBAs unterstützt.

Sie können auch den `fcp adapter show -fields transport-security-supported`Befehl verwenden, um zu überprüfen, ob Ihr HBA FC-SP-3 unterstützt. Das Feld **transport-security-supported** ist **true**, wenn FC-SP-3 unterstützt wird.

Aktivierung der FC-SP-3-Unterstützung

Wenn Ihre Konfiguration FC-SP-3 unterstützt, kann es aktiviert werden, wenn Sie eine Netzwerkschnittstelle (LIF) "erstellen" oder "ändern", indem Sie den `-fc-transport-security option` auf **mandatory** oder **preferred** setzen. Die Einstellung **mandatory** verhindert, dass Hosts, die FC-SP-3 nicht unterstützen, auf das Storage-System zugreifen. Mit der Einstellung **preferred** versucht ONTAP, eine FC-SP-3-Verbindung herzustellen, während der Hostzugriff weiterhin möglich ist, wenn FC-SP-3 nicht eingerichtet werden kann.

SAN Provisionierung mit NVMe in ONTAP

Ab ONTAP 9.4 wird NVMe/FC in SAN-Umgebungen unterstützt. NVMe/FC ermöglicht Speicheradministratoren die Bereitstellung von Namespaces und Subsystemen sowie die Zuordnung der Namespaces zu Subsystemen, ähnlich wie LUNs für FC und iSCSI bereitgestellt und Initiatorgruppen zugeordnet werden.

Ein NVMe-Namensraum ist eine Menge nichtflüchtigen Speichers, die in logische Blöcke formatiert werden kann. Namensräume entsprechen den LUNs der FC- und iSCSI-Protokolle, und ein NVMe-Subsystem ist analog zu einer Initiatorgruppe. Ein NVMe-Subsystem kann mit Initiatoren verknüpft werden, sodass die Namensräume innerhalb des Subsystems von den zugehörigen Initiatoren genutzt werden können.

> Obwohl NVMe-Namespaces in ihrer Funktion analog sind, werden nicht alle von LUNs unterstützten Funktionen unterstützt.

Ab ONTAP 9.5 ist eine Lizenz erforderlich, um den hostseitigen Datenzugriff mit NVMe zu unterstützen. Wenn NVMe in ONTAP 9.4 aktiviert ist, wird nach dem Upgrade auf ONTAP 9.5 eine 90-tägige Kulanzfrist gewährt, um die Lizenz zu erwerben. Wenn Sie "ONTAP One"haben, ist die NVMe-Lizenz enthalten. Die Lizenz kann mit dem folgenden Befehl aktiviert werden:

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

Verwandte Informationen

"NetApp Technical Report 4684: Implementierung und Konfiguration moderner SANs mit NVMe/FC"

Unterstützung von ONTAP für SAN Multipathing und automatischen LIF Failover

In Multipath-Konfigurationen werden mehrere Netzwerkpfade zwischen Ihrem Host und dem Speichersystem konfiguriert, sodass bei Ausfall eines Pfads der E/A-Verkehr auf einen alternativen Pfad umgeleitet werden kann, um Serviceunterbrechungen zu verhindern. Automatisches LIF-Failover ermöglicht es einer logischen Schnittstelle (LIF), automatisch auf einen anderen Port zu migrieren, wenn ihr Heimatport fehlerhaft wird

oder ein Storage-Failover auftritt. Multipathing mit automatischem LIF-Failover leitet den E/A-Verkehr nahtlos auf den am besten optimierten verfügbaren Pfad um, ohne dass ein Failover-Pfadwechsel erforderlich ist.

SAN unterstützte Multipath-Konfigurationen

Für SAN-Umgebungen werden die folgenden Multipath-Konfigurationen unterstützt.

lokal-aktiv

Pfade auf dem Knoten, dem die LUN oder der Namespace gehört, sind aktiv und optimiert. Die Pfade auf dem HA-Partner sind aktiv, aber nicht optimiert.

Aktiv/Aktiv

Alle Pfade im HA-Paar, die die LUN oder den Namespace besitzen, sind aktiv und optimiert.

nur Aktiv/Aktiv-SCSI

Pfade auf dem Knoten, dem die LUN oder der Namespace gehört, sind aktiv und optimiert. Pfade auf dem HA-Partner können je nach SAN-Protokoll aktiv-optimiert oder aktiv-nicht-optimiert sein. Die Aktiv/Aktiv-SCSI-only-Konfiguration wird nur auf ASA-Systemen unterstützt.

Die Unterstützung für SAN-Multipath-Konfigurationen variiert je nach Speichersystem und ONTAP Version.

System	ONTAP Version	Unterstützte Multipath-Konfigurationen	Standardmäßige Multipath-Konfiguration
FAS	9.0 und höher	lokal-aktiv	lokal-aktiv
AFF	9.19.1 und später	• Aktiv/Aktiv • lokal-aktiv	lokal-aktiv
	9.18.1 und früher	lokal-aktiv	lokal-aktiv
ASA	9.19.1 und später	• Aktiv/Aktiv • nur Aktiv/Aktiv-SCSI	Aktiv/Aktiv
	9.18.1 und früher	• Aktiv/Aktiv • nur Aktiv/Aktiv-SCSI	nur Aktiv/Aktiv-SCSI
ASA r2	9.16.1 und später	Aktiv/Aktiv	Aktiv/Aktiv

Standardmäßiges LIF-Failover-Verhalten gemäß Konfiguration

Abhängig von der Multipath-Konfiguration sind die Pfade zwischen Host und Speichersystem entweder aktiv-optimiert oder aktiv-nicht-optimiert. Bei einem Speicher-Failover mit aktiv-optimierten Pfaden muss der Host nicht auf den ALUA- oder ANA-Übergang der Failover-Pfade warten, um die E/A wieder aufzunehmen. Bei aktiv-nicht-optimierten Pfaden muss ALUA oder ANA die E/A von den ausgefallenen Pfaden auf den HA-Partner übertragen, bevor die E/A wieder aufgenommen werden kann. Weitere Informationen zu "ALUA und ANA".

Multipath-Konfiguration	Protokoll	Standardmäßige LIF-Failover-Richtlinie	Eigentümer-Knotenpfade	HA-Partnerpfade
lokal-aktiv	• iSCSI • NVMe/TCP • NVMe/FC	nur lokal	aktiv-optimiert	aktiv-nicht-optimiert
Aktiv/Aktiv	• iSCSI • NVMe/TCP	sfo-partner-only	aktiv-optimiert	aktiv-optimiert
	• FCP • NVMe/FC	Nicht zutreffend Persistente Ports werden für Failover verwendet	aktiv-optimiert	aktiv-optimiert
active-active-scsi-only (Nur auf ASA-Plattformen verfügbar)	iSCSI	sfo-partner-only	aktiv-optimiert	aktiv-optimiert
	NVMe/TCP	nur lokal	aktiv-optimiert	aktiv-nicht-optimiert
	FC	Nicht zutreffend Persistente Ports werden für Failover verwendet	aktiv-optimiert	aktiv-optimiert
	NVMe/FC	Nicht zutreffend Persistente Ports werden für Failover verwendet	aktiv-optimiert	aktiv-nicht-optimiert

Unterstützung für automatisches ONTAP LIF Failover

Automatisches LIF-Failover wird bei Aktiv/Aktiv Multipath-Konfigurationen mit den Protokollen iSCSI und NVMe/TCP sowie bei Aktiv/Aktiv-SCSI-only Multipath-Konfigurationen mit dem iSCSI-Protokoll unterstützt. LIFs sind standardmäßig so konfiguriert, dass sie die vom System erstellte Failover-Richtlinie sfo-partner-only verwenden. Die Standardrichtlinie sfo-partner-only kann geändert werden.

Automatisches LIF-Failover wird bei lokal-aktiven Multipath-Konfigurationen nicht unterstützt. Die standardmäßige Richtlinie für ausschließlich lokale Zugriffe kann nicht geändert werden.

Aktiv/Aktiv-Multipath-Konfigurationen, die das FC- oder NVMe-FC-Protokoll verwenden, nutzen persistente Ports für das Failover. Persistente Ports werden ab ONTAP 9.8 unterstützt und verwenden keine Failover-Richtlinien. Weitere Informationen zu "Unterstützung für persistente Ports".

Die Unterstützung für automatisches LIF-Failover hängt von Ihrem Speichersystem, der ONTAP Version und dem SAN-Protokoll ab.

Speichersystem	ONTAP Version	SAN-Protokoll	LIF-Failover-Unterstützung
FAS	9.0 und höher	Alle	Nicht unterstützt

Speichersystem	ONTAP Version	SAN-Protokoll	LIF-Failover-Unterstützung
AFF	9.19.1 und später	iSCSI	Automatisches LIF-Failover mit Aktiv/Aktiv- oder Aktiv/Aktiv-SCSI-Only-Multipathing-Konfigurationen
		NVMe/TCP	Automatisches LIF-Failover mit Aktiv/Aktiv-Multipathing-Konfiguration
		• FC • NVMe/FC	Failover mit persistenten Ports
	9.18.1 und früher	Alle	Nicht unterstützt
ASA	9.19.1 und später	iSCSI	Automatisches LIF-Failover mit Aktiv/Aktiv- oder Aktiv/Aktiv-SCSI-Only-Multipathing-Konfigurationen
		NVMe/TCP	Automatisches LIF-Failover mit Aktiv/Aktiv-Multipathing-Konfiguration
		• FC • NVMe/FC	Failover mit persistenten Ports
	9.18.1 bis 9.11.1	iSCSI	Automatisches LIF-Failover
		FC	Failover mit persistenten Ports
		• NVMe/FC • NVMe/TCP	Nicht unterstützt
	9.10.1 bis 9.8	FC	Failover mit persistenten Ports
		• iSCSI • NVMe/FC • NVMe/TCP	Nicht unterstützt
	9,7	Alle	Nicht unterstützt
ASA r2	9.19.1 und später	• iSCSI • NVMe/TCP	Automatisches LIF-Failover mit Aktiv/Aktiv-Multipathing-Konfiguration
		• FC • NVMe/FC	Failover mit persistenten Ports

Wenn auf einem System, das das NVMe/TCP-Protokoll ausführt, ein automatisches LIF-Failover stattfindet und die maximale Anzahl von NVMe-Controllern auf dem verbleibenden Node

verwendet wird, können auf den LIFs, die das Failover durchgeführt haben, keine neuen NVMe-Controller erstellt werden.

Einschränkungen der Multipathing-Konfiguration

Es gibt Einschränkungen bei der SAN-Multipathing-Konfiguration für Storage Virtual Machines (SVMs) in einer SnapMirror active sync-Beziehung und für MetroCluster-Konfigurationen.

- **SnapMirror Active Sync**

  Beide Cluster in einer SnapMirror Aktiv/Aktiv-Synchronisierungsbeziehung müssen dieselbe Version von ONTAP 9.19.1 oder höher ausführen, und die Multipath-Konfiguration auf der Quell-SVM und der Ziel-SVM muss identisch sein. Das Konfigurieren unterschiedlicher Multipath-Konfigurationen für die Quell-SVM und die Ziel-SVM wird nicht unterstützt.

- **MetroCluster-Konfigurationen**

  Der Speichersystemtyp muss an den primären und sekundären Standorten identisch sein, und beide Cluster müssen ONTAP 9.19.1 oder höher ausführen, wenn auf einem der Cluster Aktiv/Aktiv-SVMs konfiguriert sind. Wenn auf einem Cluster ONTAP 9.18.1 oder früher ausgeführt wird, kann das Erstellen von iSCSI- oder NVMe/TCP-LIFs mit der Failover-Richtlinie „sfo-partner-only“ in Aktiv/Aktiv- oder Aktiv/Aktiv-SCSI-Only-Konfigurationen dazu führen, dass die LIF-Replikation auf dem Ziel-Cluster fehlschlägt.

Aktiv/Aktiv-Multipathing auf AFF-Systemen

Ab ONTAP 9.19.1 unterstützen AFF-Systeme Aktiv/Aktiv-Multipathing mit automatischem LIF-Failover auf SVM-Ebene in SAN-Umgebungen. Dies verkürzt die Failover-Zeit und ermöglicht es SAN-Kunden, geschäftskritische Workloads auf AFF-Systemen mit derselben unterbrechungsfreien Pfadausfallsicherheit und Lastverteilung auszuführen, die zuvor nur auf ASA-Systemen verfügbar waren. Die Unterstützung von Aktiv/Aktiv-Multipathing und automatischem LIF-Failover auf Ihren AFF-Systemen ermöglicht Ihnen die Konsolidierung von Management-Domänen, die Optimierung Ihres Speicherbedarfs, die Nutzung bestehender NAS-Investitionen und die Standardisierung auf ein einziges Speichersystem für alle Ihre Protokollanforderungen, während Sie gleichzeitig strenge Verfügbarkeits- und Leistungs-SLAs einhalten.

Auf AFF-Systemen kann Aktiv/Aktiv-Multipathing nur beim Erstellen einer neuen SVM in ONTAP 9.19.1 und höher konfiguriert werden. Eine SVM kann nicht von einer Local-Active-Konfiguration in eine Aktiv/Aktiv-Konfiguration konvertiert werden.

Sie können bestehende LUNs und Namensräume von SVMs, die für lokal-aktives Multipathing konfiguriert sind, zu SVMs verschieben, die für Aktiv/Aktiv-Multipathing konfiguriert sind. Wenn Sie eine LUN oder einen Namensraum zu einer neuen SVM verschieben, müssen Sie Ihren Host der neuen SVM neu zuordnen, bevor Sie mit der Datenbereitstellung beginnen.

Wenn Ihr Cluster ONTAP 9.19.1 oder höher verwendet und sowohl FAS als auch AFF-Systeme umfasst, sollten Sie für alle Systeme die lokal-aktive Multipath-Konfiguration verwenden. Die Verwendung einer lokal-aktiven Konfiguration für FAS-Systeme und einer Aktiv/Aktiv-Konfiguration für AFF-Systeme im selben Cluster wird nicht empfohlen.

Verwandte Informationen

- Weitere Informationen zu "automatisches iSCSI LIF-Failover auf ASA-Systemen".
- Weitere Informationen zu "automatisches iSCSI LIF-Failover auf ASA r2-Systemen".

SAN-Volumes

Informationen zu ONTAP SAN Volumes

ONTAP bietet drei grundlegende Optionen für die Volume-Bereitstellung: Thick Provisioning, Thin Provisioning und Semi-Thick Provisioning. Jede Option verwendet unterschiedliche Methoden zur Verwaltung des Volume-Speicherplatzes und der Speicheranforderungen für ONTAP Block-Sharing-Technologien. Ein Verständnis der Funktionsweise der Optionen ermöglicht die Auswahl der besten Option für die jeweilige Umgebung.

> Es wird nicht empfohlen, SAN-LUNs und NAS-Freigaben im selben FlexVol Volume zu platzieren. Sie sollten separate FlexVol Volumes speziell für Ihre SAN-LUNs und separate FlexVol Volumes speziell für Ihre NAS-Freigaben bereitstellen. Dies vereinfacht die Verwaltung sowie Replikationsbereitstellungen und entspricht der Art und Weise, wie FlexVol Volumes in Active IQ Unified Manager (ehemals OnCommand Unified Manager) unterstützt werden.

Thin Provisioning für Volumes

Wenn ein Thin-Provisioned-Volume erstellt wird, reserviert ONTAP beim Erstellen des Volumes keinen zusätzlichen Speicherplatz. Wenn Daten auf das Volume geschrieben werden, fordert das Volume den benötigten Speicherplatz vom Aggregat an, um den Schreibvorgang auszuführen. Die Verwendung von Thin-Provisioned-Volumes ermöglicht es, das Aggregat zu überprovisionieren, was das Risiko birgt, dass das Volume nicht den benötigten Speicherplatz erhält, wenn im Aggregat kein freier Speicherplatz mehr vorhanden ist.

Ein dünn-provisioniertes FlexVol Volume wird erstellt, indem die `-space-guarantee` Option auf `none` gesetzt wird.

Thick Provisioning für Volumes

Wenn ein Thick-Provisioning-Volume erstellt wird, reserviert ONTAP ausreichend Speicherplatz im Aggregat, um sicherzustellen, dass jeder Block im Volume jederzeit beschrieben werden kann. Bei der Konfiguration eines Volumes für die Verwendung von Thick Provisioning können alle ONTAP-Speichereffizienzfunktionen wie Komprimierung und Deduplizierung eingesetzt werden, um den höheren anfänglichen Speicherbedarf auszugleichen.

Ein dick-provisioniertes FlexVol Volume wird erstellt, indem die Option `-space-slo` (Service Level Objective) auf `thick` gesetzt wird.

Semi-thick Provisioning für Volumes

Wird ein Volume mit Semi-Thick Provisioning erstellt, reserviert ONTAP Speicherplatz im Aggregat, um die Volume-Größe zu berücksichtigen. Reicht der freie Speicherplatz auf dem Volume aufgrund von Block-Sharing-Technologien nicht mehr aus, versucht ONTAP, Schutzdatenobjekte (Snapshots sowie FlexClone Dateien und LUNs) zu löschen, um den belegten Speicherplatz freizugeben. Solange ONTAP die Schutzdatenobjekte schnell genug löschen kann, um den für Überschreibungen benötigten Speicherplatz bereitzustellen, bleiben die Schreibvorgänge erfolgreich. Dies wird als „Best Effort“-Schreibgarantie bezeichnet.

Hinweis: Die folgende Funktionalität wird auf Volumes, die Semi-Thick Provisioning verwenden, nicht unterstützt:

- Speichereffizienztechnologien wie Deduplizierung, Komprimierung und Verdichtung
- Microsoft Offloaded Data Transfer (ODX)

Ein halb-dick-provisioniertes FlexVol Volume wird erstellt, indem die Option `-space-slo` (Service Level Objective) auf `semi-thick` gesetzt wird.

Verwendung mit speicherplatzreservierten Dateien und LUNs

Eine speicherplatzreservierte Datei oder LUN ist eine Datei oder LUN, für die bei der Erstellung Speicherplatz zugewiesen wird. Historisch hat NetApp den Begriff „thin-provisioned LUN“ verwendet, um eine LUN zu bezeichnen, bei der die Speicherplatzreservierung deaktiviert ist (eine nicht speicherplatzreservierte LUN).

Hinweis: Dateien ohne reservierten Speicherplatz werden im Allgemeinen nicht als „`thin-provisioned files`“ bezeichnet.

Die folgende Tabelle fasst die wichtigsten Unterschiede in der Verwendung der drei Optionen zur Volumenbereitstellung mit Speicherplatzreservierung für Dateien und LUNs zusammen:

Volumenbereitstellung	LUN/Speicherplatzreservierung	Überschreibvorgänge	Schutzdaten[2]	Speichereffizienz[3]
Thick	Unterstützt	Garantiert[1]	Garantiert	Unterstützt
Dünn	Keine Wirkung	Keine	Garantiert	Unterstützt
Halbdick	Unterstützt	Best Effort[1]	Best Effort	Nicht unterstützt

Anmerkungen

1. Die Möglichkeit, Überschreibungen zu garantieren oder eine bestmögliche Überschreibungsgarantie zu bieten, setzt voraus, dass Speicherplatzreservierung auf der LUN oder Datei aktiviert ist.
2. Zu den Schutzdaten gehören Snapshots sowie FlexClone Dateien und LUNs, die für die automatische Löschung gekennzeichnet sind (Backup-Klone).
3. Zur Speichereffizienz gehören Deduplizierung, Komprimierung, alle FlexClone Dateien und LUNs, die nicht zur automatischen Löschung markiert sind (aktive Klone), sowie FlexClone Unterdateien (die für Copy Offload verwendet werden).

Unterstützung für SCSI Thin-Provisioned LUNs

ONTAP unterstützt T10 SCSI Thin-Provisioned-LUNs sowie NetApp Thin-Provisioned-LUNs. T10 SCSI Thin Provisioning ermöglicht Host-Anwendungen die Unterstützung von SCSI-Funktionen, einschließlich LUN-Speicherplatzrückgewinnung und LUN-Speicherplatzüberwachung für Blockumgebungen. T10 SCSI Thin Provisioning muss von Ihrer SCSI-Host-Software unterstützt werden.

Die ONTAP `space-allocation` Einstellung wird verwendet, um die Unterstützung für T10 Thin Provisioning auf einer LUN zu aktivieren oder zu deaktivieren. Die ONTAP `space-allocation enable` Einstellung wird verwendet, um T10 SCSI Thin Provisioning auf einer LUN zu aktivieren.

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

Konfigurieren Sie ONTAP Volume-Bereitstellungsoptionen

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

Über diese Aufgabe

Das Setzen der `-space-slo` Option auf `thick` stellt Folgendes sicher:

- Das gesamte Volume ist im Aggregat vorab zugewiesen. Es ist nicht möglich, den `volume create`- oder `volume modify`-Befehl zu verwenden, um die `-space-guarantee`-Option des Volumes zu konfigurieren.
- Der für Überschreibungen benötigte Speicherplatz ist zu 100 % reserviert. Der `volume modify` Befehl kann nicht verwendet werden, um die `-fractional-reserve` Option des Volumes zu konfigurieren.

Das Setzen der `-space-slo` Option auf `semi-thick` stellt Folgendes sicher:

- Das gesamte Volume ist im Aggregat vorab zugewiesen. Es ist nicht möglich, den `volume create`- oder `volume modify`-Befehl zu verwenden, um die `-space-guarantee`-Option des Volumes zu konfigurieren.
- Es ist kein Speicherplatz für Überschreibungen reserviert. Mit dem `volume modify` Befehl lässt sich die `-fractional-reserve` Option des Volumes konfigurieren.
- Die automatische Löschung von Snapshots ist aktiviert.

Schritt

1. Optionen zur Volumenbereitstellung konfigurieren:

   `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 nicht-AFF DP-Volumes aktiviert. Andernfalls ist sie standardmäßig `volume`. Für bestehende FlexVol Volumes kann der `volume modify` Befehl zur Konfiguration der Bereitstellungsoptionen verwendet werden.

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

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

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

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

   Der folgende Befehl konfiguriert vol1 auf SVM vs1 für Semi-Thick Provisioning:

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

Konfigurationsoptionen für SAN Volumes in ONTAP

Sie müssen verschiedene Optionen für das Volume festlegen, das Ihre LUN enthält. Die Art, wie die Volume-Optionen festgelegt werden, bestimmt den für LUNs im Volume verfügbaren Speicherplatz.

Automatisches Wachstum

Sie können Autogrow aktivieren oder deaktivieren. Wenn Sie Autogrow aktivieren, ermöglicht Autogrow ONTAP, die Größe des Volumes automatisch bis zu einer von Ihnen festgelegten Maximalgröße zu erhöhen. Im übergeordneten Aggregat muss ausreichend Speicherplatz vorhanden sein, um das automatische Wachstum des Volumes zu unterstützen. Daher ist bei aktiviertem Autogrow eine Überwachung des freien Speicherplatzes im übergeordneten Aggregat erforderlich, und bei Bedarf muss zusätzlicher Speicherplatz hinzugefügt werden.

Die automatische Vergrößerung kann nicht zur Erstellung von Snapshots ausgelöst werden. Wenn versucht wird, einen Snapshot zu erstellen und nicht genügend Speicherplatz auf dem Volume vorhanden ist, schlägt die Snapshot-Erstellung fehl, selbst wenn die automatische Vergrößerung aktiviert ist.

Wenn die automatische Vergrößerung deaktiviert ist, bleibt die Größe Ihres Volumes gleich.

Autoshrink

Sie können Autoshrink aktivieren oder deaktivieren. Wenn Autoshrink aktiviert ist, ermöglicht es ONTAP, die Gesamtgröße eines Volumes automatisch zu verringern, wenn der belegte Speicherplatz im Volume einen vordefinierten Schwellenwert unterschreitet. Dies erhöht die Speichereffizienz, indem Volumes ungenutzten freien Speicherplatz automatisch freigeben.

Snapshot Autolöschung

Snapshot Autodelete löscht Snapshots automatisch, wenn einer der folgenden Fälle eintritt:

- Das Volume ist fast voll.
- Der Speicherplatz für Momentaufnahmen ist nahezu voll.
- Der Überschreibungsreservebereich ist voll.

Sie können die automatische Snapshot-Löschung so konfigurieren, dass Snapshots entweder vom ältesten zum neuesten oder vom neuesten zum ältesten gelöscht werden. Die automatische Snapshot-Löschung entfernt keine Snapshots, die mit Snapshots in geklonten Volumes oder LUNs verknüpft sind.

Wenn Ihr Volume zusätzlichen Speicherplatz benötigt und sowohl Autogrow als auch Snapshot Autodelete aktiviert sind, versucht ONTAP standardmäßig, den benötigten Speicherplatz zunächst durch Autogrow bereitzustellen. Wird durch Autogrow nicht genügend Speicherplatz bereitgestellt, wird anschließend Snapshot Autodelete ausgelöst.

Snapshot-Reserve

Die Snapshot-Reserve definiert den Speicherplatz im Volume, der für Snapshots reserviert ist. Der für die Snapshot-Reserve zugewiesene Speicherplatz kann nicht für andere Zwecke verwendet werden. Wenn der gesamte für die Snapshot-Reserve zugewiesene Speicherplatz belegt ist, belegen Snapshots zusätzlichen Speicherplatz auf dem Volume.

Anforderungen für die Verschiebung von Volumes in ONTAP SAN-Umgebungen

Bevor ein Volume verschoben wird, das LUNs oder Namespaces enthält, müssen bestimmte Voraussetzungen erfüllt sein.

- Für Volumes, die eine oder mehrere LUNs enthalten, ist es empfehlenswert, mindestens zwei Pfade pro LUN (LIFs) zu jedem Knoten im Cluster zu haben.

  Dadurch werden Single Points of Failure eliminiert und das System kann Komponentenausfälle überstehen.

- Für Volumes, die Namespaces enthalten, muss das Cluster mit ONTAP 9.6 oder höher betrieben werden.

  Das Verschieben von Volumes wird für NVMe Konfigurationen mit ONTAP 9.5 nicht unterstützt.

Informationen zur fraktionellen Reserve in ONTAP

Die fraktionale Reserve, auch *LUN-Überschreibungsreserve* genannt, ermöglicht das Deaktivieren der Überschreibungsreserve für speicherplatzreservierte LUNs und Dateien in einem FlexVol volume. Dies kann die Speichernutzung maximieren, jedoch ist es wichtig, die Anforderungen dieser Konfiguration zu kennen, falls Ihre Umgebung negativ durch fehlgeschlagene Schreibvorgänge aufgrund von Platzmangel beeinflusst wird.

Die Einstellung der Mindestreserve wird als Prozentsatz ausgedrückt; die einzigen gültigen Werte sind `0` und `100` Prozent. Die Einstellung der Mindestreserve ist eine Eigenschaft des Volumens.

Das Setzen der fraktionalen Reserve auf `0` erhöht Ihre Speicherauslastung. Allerdings kann eine Anwendung, die auf im Volume gespeicherte Daten zugreift, einen Datenverlust erfahren, wenn das Volume keinen freien Speicherplatz mehr hat, selbst wenn die Volume-Garantie auf `volume` gesetzt ist. Mit einer geeigneten Volume-Konfiguration und -Nutzung lässt sich jedoch die Wahrscheinlichkeit fehlgeschlagener Schreibvorgänge minimieren. ONTAP bietet eine „Best-Effort“-Schreibgarantie für Volumes mit fraktionaler Reserve auf `0` gesetzt, wenn *alle* der folgenden Anforderungen erfüllt sind:

- Die Deduplizierung ist nicht in Verwendung
- Kompression ist nicht in Verwendung
- FlexClone Unterdateien werden nicht verwendet
- Alle FlexClone Dateien und FlexClone LUNs sind für die automatische Löschung aktiviert.

  Dies ist nicht die Standardeinstellung. Die automatische Löschung muss explizit aktiviert werden, entweder bei der Erstellung oder durch Ändern der FlexClone Datei oder FlexClone LUN nach deren Erstellung.

- ODX und FlexClone Copy Offload werden nicht verwendet
- Die Mengengarantie ist auf `volume` eingestellt
- Datei- oder LUN-Speicherplatzreservierung ist `enabled`
- Die Reserve für Volume Snapshot ist auf `0` eingestellt
- Die automatische Löschung von Volume-Snapshots ist `enabled` mit einem Commitment-Level von `destroy`, einer Destroy-Liste von `lun_clone,vol_clone,cifs_share,file_clone,sfsr` und einem Trigger von `volume`

Diese Einstellung stellt außerdem sicher, dass FlexClone Dateien und FlexClone LUNs bei Bedarf gelöscht werden.

Es ist zu beachten, dass bei einer hohen Änderungsrate in seltenen Fällen die automatische Snapshot-Löschung nicht nachkommt, sodass der Speicherplatz auf dem Volume ausgehen kann, selbst wenn alle oben genannten erforderlichen Konfigurationseinstellungen in Verwendung sind.

Zusätzlich kann optional die Volume-Autogrow-Funktion verwendet werden, um die Wahrscheinlichkeit zu verringern, dass Volume-Snapshots automatisch gelöscht werden müssen. Wenn die Autogrow-Funktion aktiviert ist, muss der freie Speicherplatz im zugehörigen Aggregat überwacht werden. Wenn das Aggregat so voll wird, dass das Volume nicht mehr wachsen kann, werden wahrscheinlich mehr Snapshots gelöscht, da der freie Speicherplatz im Volume erschöpft ist.

Falls Sie nicht alle oben genannten Konfigurationsanforderungen erfüllen können und sicherstellen müssen, dass der Speicherplatz des Volumes nicht ausgeht, muss die Einstellung für die fraktionelle Reserve des Volumes auf `100` gesetzt werden. Dies erfordert zwar zunächst mehr freien Speicherplatz, garantiert aber, dass Datenänderungsvorgänge auch dann erfolgreich sind, wenn die oben genannten Technologien verwendet werden.

Der Standardwert und die zulässigen Werte für die Einstellung der Teilreserve hängen von der Garantie des Volumes ab:

Volumengarantie	Standardmäßige Teilreserve	Zulässige Werte
Volumen	100	0, 100
Keine	0	0, 100

Informationen zum SAN hostseitigen Speicherplatzmanagement in ONTAP

In einer Thin-Provisioning-Umgebung schließt das hostseitige Speicherplatzmanagement den Prozess der Verwaltung des im Host-Dateisystem freigegebenen Speicherplatzes vom Speichersystem ab.

Das Dateisystem eines Hosts enthält Metadaten, die festlegen, welche Blöcke für neue Daten verfügbar sind und welche Blöcke gültige Daten enthalten, die nicht überschrieben werden dürfen. Diese Metadaten werden in der LUN oder im Namensraum gespeichert. Wenn eine Datei im Dateisystem des Hosts gelöscht wird, werden die Metadaten des Dateisystems aktualisiert, um die Blöcke dieser Datei als freien Speicherplatz zu markieren. Der gesamte freie Speicherplatz des Dateisystems wird dann neu berechnet, sodass die neu freigegebenen Blöcke einbezogen werden. Für das Speichersystem unterscheiden sich diese Metadatenaktualisierungen nicht von anderen Schreibvorgängen des Hosts. Daher ist dem Speichersystem nicht bekannt, dass Löschungen erfolgt sind.

Dies führt zu einer Diskrepanz zwischen dem vom Host und dem vom zugrunde liegenden Speichersystem gemeldeten freien Speicherplatz. Beispielsweise weist das Speichersystem Ihrem Host eine neu bereitgestellte 200-GB-LUN zu. Sowohl der Host als auch das Speichersystem melden 200 GB freien Speicherplatz. Anschließend schreibt der Host 100 GB Daten. Zu diesem Zeitpunkt melden sowohl der Host als auch das Speichersystem 100 GB belegten und 100 GB ungenutzten Speicherplatz.

Dann werden 50 GB Daten von Ihrem Host gelöscht. Zu diesem Zeitpunkt meldet Ihr Host 50 GB belegten und 150 GB ungenutzten Speicherplatz. Ihr Speichersystem meldet jedoch 100 GB belegten und 100 GB ungenutzten Speicherplatz.

Das Host-seitige Speicherplatzmanagement nutzt verschiedene Methoden, um die Speicherdifferenz zwischen Host und Speichersystem auszugleichen.

Vereinfachte Hostverwaltung mit SnapCenter

Mit der SnapCenter software lassen sich einige Verwaltungs- und Datenschutzaufgaben im Zusammenhang mit iSCSI- und FC-Speicher vereinfachen. SnapCenter ist ein optionales Verwaltungspaket für Windows- und UNIX-Hosts.

Mit der SnapCenter Software lassen sich virtuelle Festplatten aus Speicherpools einfach erstellen, die auf mehrere Speichersysteme verteilt werden können. Zudem werden Aufgaben zur Speicherbereitstellung automatisiert und der Prozess zur Erstellung von Snapshots und Klonen aus Snapshots, die mit den Hostdaten konsistent sind, vereinfacht.

In der NetApp Produktdokumentation sind weitere Informationen zu "SnapCenter" zu finden.

Verwandte Links

"ONTAP Speicherplatzzuweisung für SAN-Protokolle aktivieren"

Erfahren Sie mehr über ONTAP SAN igroups

Initiatorgruppen (igroups) sind Tabellen mit WWPNs von FC-Protokoll-Hosts oder iSCSI-Hostknotennamen. Es besteht die Möglichkeit, igroups zu definieren und sie LUNs zuzuordnen, um zu steuern, welche Initiatoren Zugriff auf LUNs erhalten.

Im Normalfall sollten alle Initiator-Ports oder Softwareinitiatoren eines Hosts Zugriff auf eine LUN haben. Wenn Multipathing-Software verwendet wird oder Hosts in einem Cluster betrieben werden, benötigt jeder Initiator-Port oder Softwareinitiator jedes Cluster-Hosts redundante Pfade zur selben LUN.

Es ist möglich, igroups zu erstellen, die festlegen, welche Initiatoren Zugriff auf die LUNs haben, entweder vor oder nach der Erstellung der LUNs, jedoch müssen igroups erstellt werden, bevor eine LUN einer Initiatorgruppe zugeordnet werden kann.

Initiatorgruppen können mehrere Initiatoren haben, und mehrere Initiatorgruppen können denselben Initiator haben. Es ist jedoch nicht möglich, eine LUN mehreren Initiatorgruppen mit demselben Initiator zuzuordnen. Ein Initiator darf nicht Mitglied von Initiatorgruppen mit unterschiedlichen ostypes sein.

Beispiel dafür, wie igroups den Zugriff auf LUNs ermöglichen

Sie können mehrere igroups erstellen, um festzulegen, welche LUNs Ihren Hosts zur Verfügung stehen. Wenn beispielsweise ein Host-Cluster vorhanden ist, kann mit igroups sichergestellt werden, dass bestimmte LUNs nur für einen Host im Cluster oder für alle Hosts im Cluster sichtbar sind.

Die folgende Tabelle veranschaulicht, wie vier Initiatorgruppen den Zugriff auf die LUNs für vier verschiedene Hosts ermöglichen, die auf das Speichersystem zugreifen. Die Cluster-Hosts (Host3 und Host4) sind beide Mitglieder derselben Initiatorgruppe (group3) und können auf die LUNs zugreifen, die dieser Initiatorgruppe zugeordnet sind. Die Initiatorgruppe group4 enthält die WWPNs von Host4, um lokale Informationen zu speichern, die für den Partner nicht sichtbar sein sollen.

Hosts mit HBA WWPNs, IQNs oder EUIs	igroups	WWPNs, IQNs, EUIs wurden zu Initiatorgruppen hinzugefügt	LUNs, die Initiatorgruppen zugeordnet sind
Host1, Single-Path (iSCSI Softwareinitiator) iqn.1991-05.com.microsoft:host1	group1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`
Host2, Multipath (zwei HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	group2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	`/vol/vol2/lun2`
Host3, Multipath, in einem Cluster mit Host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	group3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree1/lun3`
Host4, Multipath, Clustered (für Host3 nicht sichtbar) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	group4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

Initiator WWPNs und iSCSI-Knotennamen für ONTAP igroups

Sie können die iSCSI-Knotennamen und WWPNs der Initiatoren beim Erstellen einer Initiatorgruppe angeben oder sie später hinzufügen. Wenn Sie die iSCSI-Knotennamen und WWPNs der Initiatoren beim Erstellen der LUN angeben, können diese bei Bedarf später entfernt werden.

Befolgen Sie die Anweisungen in Ihrer Host Utilities Dokumentation, um WWPNs zu erhalten und die iSCSI-Knotennamen zu ermitteln, die einem bestimmten Host zugeordnet sind. Für Hosts, auf denen ESX Software ausgeführt wird, sind ONTAP tools for VMware vSphere zu verwenden.

Vorteile der Verwendung einer virtualisierten SAN-Umgebung in ONTAP

Durch die Erstellung einer virtualisierten Umgebung mithilfe von Storage Virtual Machines (SVMs) und LIFs wird eine Erweiterung Ihrer SAN-Umgebung auf alle Knoten in Ihrem Cluster ermöglicht.

- Verteiltes Management

  Sie können sich an jedem Knoten in der SVM anmelden, um alle Knoten in einem Cluster zu verwalten.

- Erweiterter Datenzugriff

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

- Kontrollierter LUN-Zugriff

  Wenn SLM und Portsets verwendet werden, lässt sich einschränken, welche LIFs ein Initiator für den Zugriff auf LUNs nutzen kann.

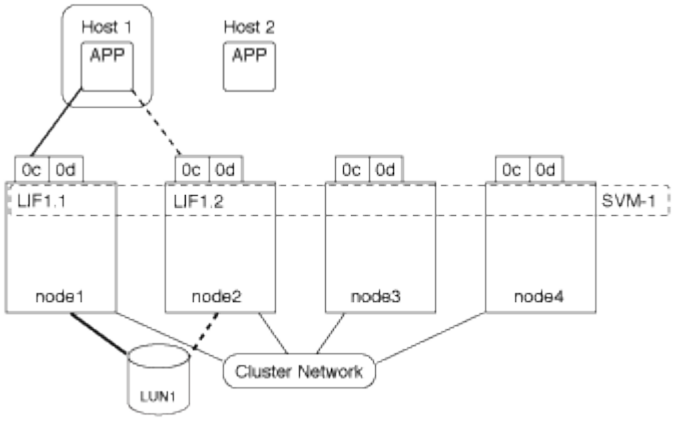
Wie der LUN-Zugriff in einer virtualisierten Umgebung funktioniert

In einer virtualisierten Umgebung ermöglichen LIFs Hosts (Clients) den Zugriff auf LUNs über optimierte und nicht optimierte Pfade.

Eine LIF ist eine logische Schnittstelle, die die Storage Virtual Machine (SVM) mit einem physischen Port verbindet. Obwohl mehrere SVMs mehrere LIFs am selben Port haben können, gehört eine LIF zu einer SVM. Auf LUNs kann über die LIFs der SVMs zugegriffen werden.

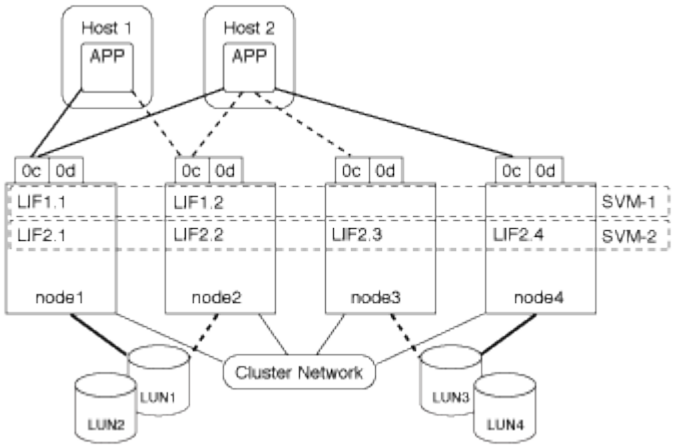
Beispiel für den LUN-Zugriff mit einer einzelnen SVM in einem Cluster

Im folgenden Beispiel verbindet sich Host 1 mit LIF1.1 und LIF1.2 in SVM-1, um auf LUN1 zuzugreifen. LIF1.1 verwendet den physischen Port node1:0c und LIF1.2 den physischen Port node2:0c. LIF1.1 und LIF1.2 gehören ausschließlich zu SVM-1. Wenn für SVM-1 auf Knoten 1 oder Knoten 2 eine neue LUN erstellt wird, kann sie dieselben LIFs verwenden. Wenn eine neue SVM erstellt wird, können neue LIFs über die physischen Ports 0c oder 0d auf beiden Knoten erstellt werden.



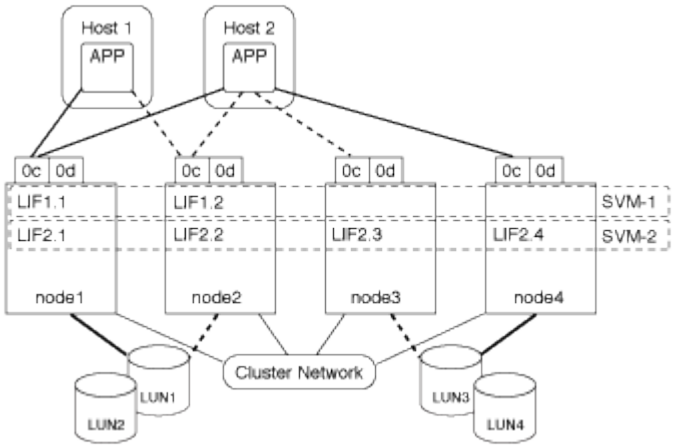
Beispiel für den LUN-Zugriff mit mehreren SVMs in einem Cluster

Ein physischer Port kann mehrere LIFs unterstützen, die verschiedene SVMs bedienen. Da LIFs einer bestimmten SVM zugeordnet sind, können die Clusterknoten den eingehenden Datenverkehr an die richtige SVM weiterleiten. Im folgenden Beispiel verfügt jeder Knoten von 1 bis 4 über eine LIF für SVM-2, die den physischen Port 0c auf jedem Knoten nutzt. Host 1 verbindet sich mit LIF1.1 und LIF1.2 in SVM-1, um auf LUN1 zuzugreifen. Host 2 verbindet sich mit LIF2-1 und LIF2-2 in SVM-2, um auf LUN2 zuzugreifen. Beide SVMs teilen sich den physischen Port 0c auf den Knoten 1 und 2. SVM-2 verfügt über zusätzliche LIFs, die Host 2 für den Zugriff auf LUN3 und LUN4 verwendet. Diese LIFs nutzen den physischen Port 0c auf den Knoten 3 und 4. Mehrere SVMs können die physischen Ports auf den Knoten gemeinsam nutzen.



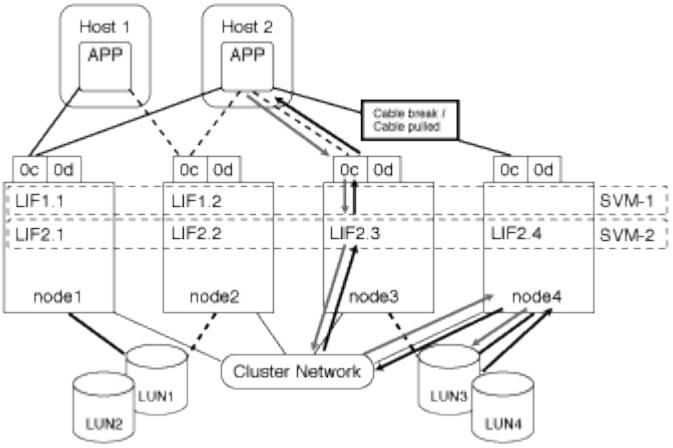
Beispiel eines aktiven oder optimierten Pfads zu einer LUN von einem Hostsystem

Auf einem aktiven oder optimierten Pfad wird der Datenverkehr nicht über das Cluster-Netzwerk geleitet, sondern nimmt den direktesten Weg zur LUN. Der aktive oder optimierte Pfad zu LUN1 verläuft über LIF1.1 in node1 und nutzt den physischen Port 0c. Host 2 verfügt über zwei aktive oder optimierte Pfade: einen Pfad zu node1, LIF2.1, der den physischen Port 0c mitbenutzt, und einen weiteren Pfad zu node4, LIF2.4, der ebenfalls den physischen Port 0c nutzt.



Beispiel für einen aktiven oder nicht optimierten (indirekten) Pfad zu einer LUN von einem Hostsystem

Bei einem aktiven oder nicht optimierten (indirekten) Pfad wird der Datenverkehr über das Clusternetzwerk geleitet. Dieses Problem tritt nur auf, wenn alle aktiven oder optimierten Pfade von einem Host aus nicht verfügbar sind, um den Datenverkehr zu übernehmen. Fällt der Pfad von Host 2 zu SVM-2 LIF2.4 aus, erfolgt der Zugriff auf LUN3 und LUN4 über das Clusternetzwerk. Der Zugriff von Host 2 nutzt LIF2.3 auf Node 3. Der Datenverkehr gelangt dann in den Cluster Netzwerk-Switch und wird zurück zu Node 4 geleitet, um auf LUN3 und LUN4 zuzugreifen. Anschließend durchläuft er erneut den Cluster Netzwerk-Switch und gelangt dann über LIF2.3 wieder zu Host 2. Dieser aktive oder nicht optimierte Pfad wird verwendet, bis der Pfad zu LIF2.4 wiederhergestellt ist oder ein neuer LIF für SVM-2 an einem anderen physischen Port auf Node 4 eingerichtet wird.



Wie ONTAP VMware VAAI Funktionen die Performance von ESX Hosts verbessern

ONTAP unterstützt bestimmte VMware vStorage APIs für Array Integration (VAAI) Features, wenn auf dem ESX Host ESX 4.1 oder höher ausgeführt wird. Diese Features helfen dabei, Operationen vom ESX Host auf das Speichersystem auszulagern und den Netzwerkdurchsatz zu erhöhen. Die Features werden vom ESX Host in der passenden Umgebung automatisch aktiviert.

Die VAAI Funktion unterstützt die folgenden SCSI-Befehle:

- `EXTENDED_COPY`

  Diese Funktion ermöglicht es dem Host, die Übertragung von Daten zwischen den LUNs oder innerhalb einer LUN zu initiieren, ohne dass der Host selbst am Datentransfer beteiligt ist. Dies führt zu einer Einsparung von ESX-CPU-Zyklen und einer Erhöhung des Netzwerkdurchsatzes. Die erweiterte Kopierfunktion, auch als „copy offload“ bekannt, wird in Szenarien wie dem Klonen einer virtuellen Maschine verwendet. Wenn die Funktion vom ESX Host aufgerufen wird, kopiert die copy offload Funktion die Daten innerhalb des Speichersystems, anstatt sie über das Host-Netzwerk zu übertragen. Copy offload überträgt Daten auf folgende Weise:

  - Innerhalb einer LUN
  - Zwischen LUNs innerhalb eines Volumens
  - 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 automatisch die Standardbefehle READ und WRITE für den Kopiervorgang.

- `WRITE_SAME`

  Diese Funktion lagert die Arbeit des Schreibens eines sich wiederholenden Musters, wie z. B. lauter Nullen, an ein Speicherarray aus. Der ESX Host verwendet diese Funktion bei Vorgängen wie dem Auffüllen einer Datei mit Nullen.

- `COMPARE_AND_WRITE`

  Diese Funktion umgeht bestimmte Beschränkungen der Dateizugriffskonkurrenz, wodurch Vorgänge wie das Hochfahren virtueller Maschinen beschleunigt werden.

Anforderungen für die Nutzung der VAAI-Umgebung

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

Die Umgebungsanforderungen lauten wie folgt:

- Der ESX Host muss ESX 4.1 oder eine neuere Version ausführen.
- Das NetApp Speichersystem, das den VMware-Datenspeicher hostet, muss unter ONTAP betrieben werden.
- (Nur Copy Offload) Quelle und Ziel des VMware-Kopiervorgangs müssen sich auf demselben Speichersystem innerhalb desselben Clusters befinden.

> ⓘ Die Copy Offload-Funktion unterstützt derzeit kein Kopieren von Daten zwischen VMware-Datenspeichern, die auf unterschiedlichen Speichersystemen gehostet werden.

Es kann festgestellt werden, ob die VAAI-Funktionen von ESX unterstützt werden.

Um zu überprüfen, ob das ESX-Betriebssystem die VAAI-Funktionen unterstützt, kann der vSphere Client geprüft oder auf anderem Wege auf den Host zugegriffen werden. ONTAP unterstützt standardmäßig die SCSI-Befehle.

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

SCSI Befehl	ESX-Steuerungsname (VAAI-Funktion)
ERWEITERTE KOPIE	`HardwareAcceleratedMove`
WRITE_SAME	`HardwareAcceleratedInit`
VERGLEICHEN UND SCHREIBEN	`HardwareAcceleratedLocking`

SAN Copy Offload

Microsoft Offloaded Data Transfer ODX in ONTAP

Microsoft Offloaded Data Transfer (ODX), auch bekannt als Copy Offload, ermöglicht direkte Datentransfers innerhalb eines Speichergeräts oder zwischen kompatiblen Speichergeräten, ohne dass die Daten über den Host-Computer übertragen werden.

VMware und Microsoft unterstützen Copy Offload-Operationen, um die Leistung und den Netzwerkdurchsatz zu steigern. Das System muss so konfiguriert sein, dass die Anforderungen der VMware- und Windows-Betriebssystemumgebungen für die Nutzung der jeweiligen Copy Offload-Funktionen erfüllt werden.

Bei der Verwendung von VMware und Microsoft Copy Offload in virtualisierten Umgebungen müssen Ihre LUNs ausgerichtet sein. Nicht ausgerichtete LUNs können die Leistung beeinträchtigen. "Weitere Informationen zu nicht ausgerichteten LUNs".

ONTAP unterstützt ODX sowohl für das SMB- als auch für das SAN-Protokoll.

Bei Dateiübertragungen ohne ODX werden die Daten von der Quelle gelesen und über das Netzwerk zum Host übertragen. Der Host überträgt die Daten über das Netzwerk zurück zum Ziel. Bei ODX-

Dateiübertragungen werden die Daten direkt von der Quelle zum Ziel kopiert, ohne den Host zu durchlaufen.

Da ODX-basierte Auslagerungskopien direkt zwischen Quelle und Ziel erfolgen, ergeben sich erhebliche Leistungsvorteile, wenn die Kopien innerhalb desselben Volumes durchgeführt werden, einschließlich kürzerer Kopierzeiten für Kopien auf demselben Volume, geringerer CPU- und Speicherauslastung auf dem Client und reduzierter Netzwerk-I/O-Bandbreitennutzung. Wenn Kopien über verschiedene Volumes hinweg erfolgen, sind im Vergleich zu hostbasierten Kopien möglicherweise keine signifikanten Leistungssteigerungen zu erwarten.

In SAN-Umgebungen ist ODX nur verfügbar, wenn es sowohl vom Host als auch vom Speichersystem unterstützt wird. Clientcomputer, die ODX unterstützen und bei denen ODX aktiviert ist, nutzen beim Verschieben oder Kopieren von Dateien automatisch und transparent die ausgelagerte Dateiübertragung. ODX wird unabhängig davon verwendet, ob Dateien per Drag-and-Drop im Windows Explorer verschoben werden, Befehle zum Kopieren über die Befehlszeile genutzt werden oder eine Clientanwendung Kopieranforderungen auslöst.

Voraussetzungen für die Nutzung von ODX

Wenn ODX für Kopier-Offloads verwendet werden soll, sind die Überlegungen zur Volumenunterstützung, die Systemanforderungen und die Anforderungen an die Softwarefunktionen zu berücksichtigen.

Um ODX zu verwenden, muss Ihr System Folgendes aufweisen:

- ONTAP

  ODX ist in unterstützten Versionen von ONTAP automatisch aktiviert.

- Mindestquellvolumen von 2 GB

  Für eine optimale Leistung sollte das Quell-Volume größer als 260 GB sein.

- ODX Unterstützung auf dem Windows Client

  Die Interoperabilitätsmatrix enthält die neuesten Informationen zu unterstützten Windows Clients.

  "NetApp Interoperabilitätsmatrix-Tool"

- Unterstützung von Kopieranwendungen für ODX

  Die Anwendung, die den Datentransfer durchführt, muss ODX unterstützen. Zu den Anwendungsoperationen, die ODX unterstützen, gehören die folgenden:

  - Hyper-V Managementvorgänge, wie das Erstellen und Konvertieren virtueller Festplatten (VHDs), das Verwalten von Snapshots und das Kopieren von Dateien zwischen virtuellen Maschinen
  - Windows Explorer Operationen
  - Windows PowerShell Kopierbefehle
  - Windows-Eingabeaufforderungs-Kopierbefehle Die Microsoft TechNet Library enthält weitere Informationen zu unterstützten ODX-Anwendungen auf Windows Servern und Clients.

- Wenn Sie komprimierte Volumes verwenden, muss die Komprimierungsgruppengröße 8K betragen.

  Eine Komprimierungsgruppengröße von 32 KB wird nicht unterstützt.

ODX funktioniert nicht mit den folgenden Volume-Typen:

- Quellvolumes mit Kapazitäten von weniger als 2 GB
- Schreibgeschützte Volumes
- "FlexCache Volumes"

  ODX wird auf FlexCache Ursprungsvolumes unterstützt.

- "Semi-thick provisionierte Volumes"

Spezielle Systemdateianforderungen

Sie können ODX-Dateien, die in Qtrees gefunden werden, löschen. Andere ODX-Systemdateien sollten nicht entfernt oder geändert werden, es sei denn, der technische Support fordert Sie dazu auf.

Bei Verwendung der ODX-Funktion existieren auf jedem Volume des Systems ODX-Systemdateien. Diese Dateien ermöglichen die zeitpunktgenaue Darstellung der während der ODX-Übertragung verwendeten Daten. Die folgenden Systemdateien befinden sich im Stammverzeichnis jedes Volumes, das LUNs oder Dateien enthält, in die Daten ausgelagert wurden:

- `.copy-offload` (ein verstecktes Verzeichnis)
- `.tokens` (Datei im versteckten `.copy-offload` Verzeichnis)

Der `copy-offload delete-tokens -path dir_path -node *node_name*`Befehl kann verwendet werden, um einen Qtree zu löschen, der eine ODX-Datei enthält.

Anwendungsfälle für ODX

Sie sollten sich der Anwendungsfälle für die Nutzung von ODX auf SVMs bewusst sein, damit Sie bestimmen können, unter welchen Umständen ODX Ihnen Leistungsvorteile bietet.

Windows Server und Clients, die ODX unterstützen, verwenden Copy Offload als Standardmethode zum Kopieren von Daten zwischen Remote-Servern. Wenn der Windows Server oder Client ODX nicht unterstützt oder der ODX Copy Offload an irgendeiner Stelle fehlschlägt, erfolgt der Kopier- oder Verschiebevorgang über herkömmliche Lese- und Schreibvorgänge.

Die folgenden Anwendungsfälle unterstützen die Verwendung von ODX Kopien und ODX Verschiebungen:

- Intra-Volume

  Die Quell- und Zieldateien bzw. LUNs befinden sich im selben Volume.

- Inter-Volume, gleicher Node, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf demselben Knoten befinden. Die Daten gehören demselben SVM.

- Inter-Volume, unterschiedliche Knoten, gleiche SVM

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören demselben SVM.

- Inter-SVM, gleicher Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf

demselben Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Inter-SVM, verschiedene Knoten

  Die Quell- und Zieldateien bzw. LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten befinden. Die Daten gehören verschiedenen SVMs.

- Intercluster

  Die Quell- und Ziel-LUNs befinden sich auf unterschiedlichen Volumes, die sich auf verschiedenen Knoten in unterschiedlichen Clustern befinden. Dies wird nur für SAN unterstützt und funktioniert nicht für SMB.

Es gibt noch einige weitere spezielle Anwendungsfälle:

- Mit der ONTAP ODX Implementierung kann ODX verwendet werden, um Dateien zwischen SMB-Freigaben und an FC oder iSCSI angeschlossenen virtuellen Laufwerken zu kopieren.

  Sie können den Windows Explorer, die Windows CLI oder PowerShell, Hyper-V oder andere Anwendungen, die ODX unterstützen, verwenden, um Dateien nahtlos mithilfe von ODX Copy Offload zwischen SMB-Freigaben und verbundenen LUNs zu kopieren oder zu verschieben, vorausgesetzt, die SMB-Freigaben und LUNs befinden sich im selben Cluster.

- Hyper-V bietet einige zusätzliche Anwendungsfälle für ODX Copy Offload:

  - Mit ODX Copy Offload Pass-Through kann in Verbindung mit Hyper-V Daten innerhalb oder zwischen virtuellen Festplattendateien (VHD) kopiert werden oder Daten zwischen zugeordneten SMB-Freigaben und verbundenen iSCSI-LUNs innerhalb desselben Clusters kopiert werden.

    Dadurch können Kopien von Gastbetriebssystemen an den zugrunde liegenden Speicher weitergegeben werden.

  - Bei der Erstellung von VHDs mit fester Größe wird ODX verwendet, um die Festplatte mit Nullen zu initialisieren, wobei ein bekanntes Null-Token zum Einsatz kommt.
  - ODX Copy Offload wird für die Migration von virtuellen Maschinen-Speichern verwendet, wenn sich Quell- und Zielspeicher im selben Cluster befinden.

> Um die Anwendungsfälle für ODX Copy Offload Pass-Through mit Hyper-V zu nutzen, muss das Gastbetriebssystem ODX unterstützen und die Festplatten des Gastbetriebssystems müssen SCSI-Festplatten sein, die von einem Speicher (entweder SMB oder SAN) unterstützt werden, der ODX unterstützt. IDE-Festplatten im Gastbetriebssystem unterstützen kein ODX Pass-Through.

Informationen zu NVMe copy offload in ONTAP

NVMe Copy Offload ermöglicht einem NVMe-Host, Kopiervorgänge von seiner CPU auf die CPU des ONTAP Storage Controllers auszulagern. Der Host kann Daten von einem NVMe-Namespace in einen anderen kopieren, während seine CPU-Ressourcen für Anwendungsworkloads reserviert bleiben.

Angenommen, Sie müssen beispielsweise Ihre Storage-Workloads neu ausbalancieren, um die Leistungsverteilung zu verbessern. Dazu ist es erforderlich, zehn virtuelle Maschinen (VMs) mit 45 NVMe-Namespaces und einer durchschnittlichen Größe von jeweils 500 GB zu migrieren. Das bedeutet, dass etwa 22,5 TB an Daten kopiert werden müssen. Anstatt die eigene CPU für die Datenmigration zu verwenden, kann der Host NVMe Copy Offload nutzen, um die CPU-Ressourcen für Anwendungs-Workloads während des

Kopiervorgangs nicht zu reduzieren.

NVMe Copy Offload Unterstützung und Einschränkungen

NVMe Copy Offload wird ab ONTAP 9.18.1 unterstützt. ONTAP kann NVMe Copy Offload nicht initiieren, es muss vom Host unterstützt und initiiert werden.

Die folgenden Einschränkungen gelten für NVMe Copy-Offload-Operationen mit ONTAP:

- Die maximal unterstützte Größe für NVMe-Kopiervorgänge beträgt 16 MB.
- Daten lassen sich nur zwischen NVMe-Namespaces im selben Subsystem kopieren.
- Die Quell- und Ziel-Namespaces müssen im selben HA-Paar sein.
- Alle Quellbereiche in einem NVMe-Kopiervorgang müssen aus Namespaces stammen, die auf demselben Knoten gehostet sind.

SAN Verwaltung

SAN Bereitstellung

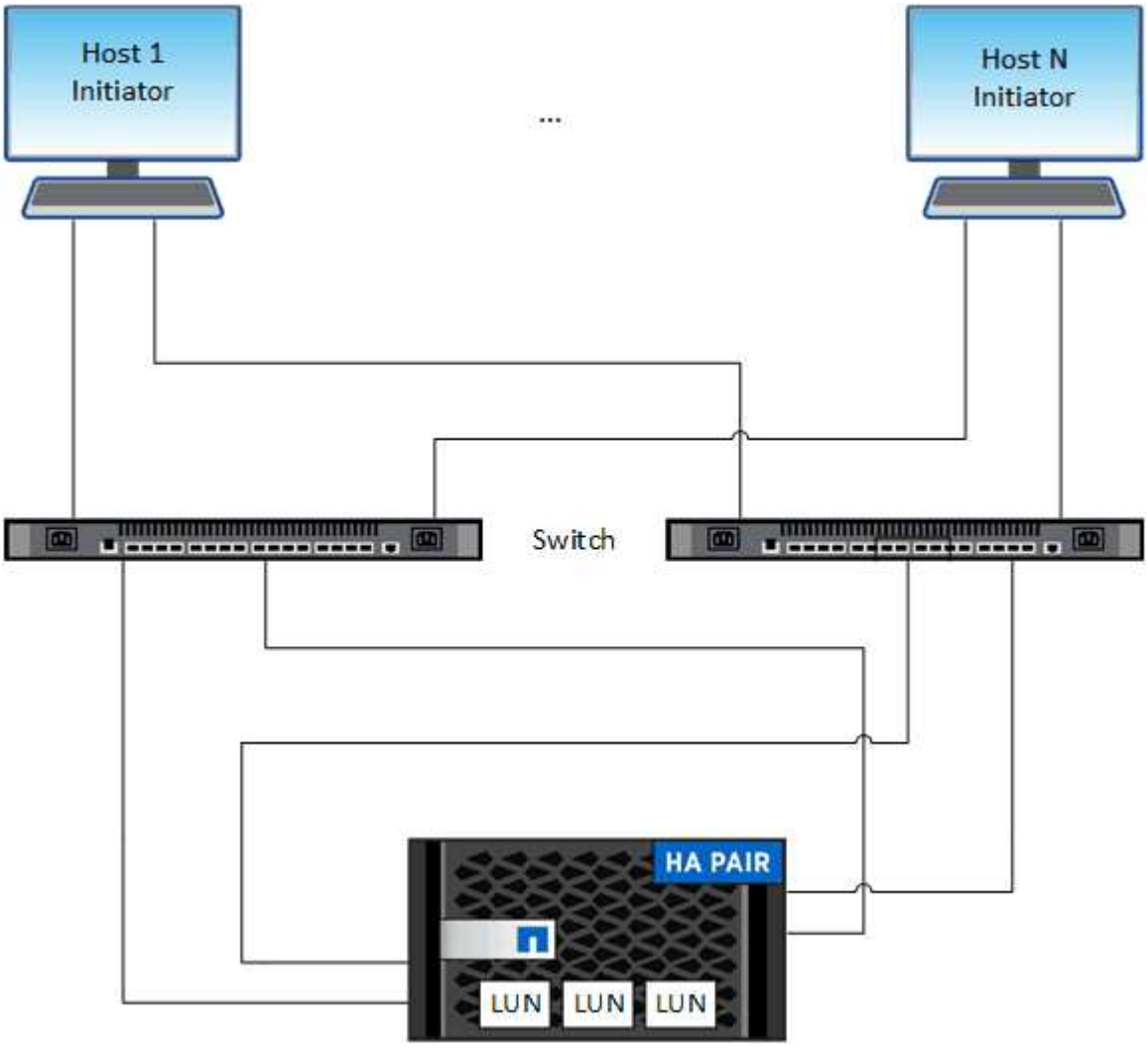
Informationen zum SAN-Management mit ONTAP

In diesem Abschnitt wird erläutert, wie SAN-Umgebungen mit der ONTAP Befehlszeilenschnittstelle (CLI) und dem System Manager in ONTAP 9.7 und späteren Versionen konfiguriert und verwaltet werden.

Wenn Sie den klassischen System Manager verwenden (nur in ONTAP 9.7 und früher verfügbar), finden Sie hierzu die folgenden Themen:

- "iSCSI Protokoll"
- "FC/FCoE Protokoll"

Die iSCSI- und FC-Protokolle können verwendet werden, um Speicher in einer SAN-Umgebung bereitzustellen.



Bei iSCSI und FC werden Speicherziele als LUNs (logische Einheiten) bezeichnet und den Hosts als Standard-Blockgeräte präsentiert. LUNs werden erstellt und anschließend Initiatorgruppen (igroups) zugeordnet. Initiatorgruppen sind Tabellen mit FC-Host-WWPs und iSCSI-Host-Node-Namen und steuern, welche Initiatoren auf welche LUNs zugreifen können.

FC-Ziele werden über FC-Switches und Host-seitige Adapter mit dem Netzwerk verbunden und durch weltweite Portnamen (WWPNs) identifiziert. iSCSI-Ziele werden über Standard Ethernet Netzwerkadapter (NICs), TCP Offload Engine Karten (TOE) mit Software-Initiatoren, konvergierte Netzwerkadapter (CNAs) oder dedizierte Host Bus Adapter (HBAs) mit dem Netzwerk verbunden und durch iSCSI-qualifizierte Namen (IQNs) identifiziert.

Für weitere Informationen

Wenn Sie ein ASA r2 Speichersystem (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) besitzen, siehe die "ASA r2 Speichersystemdokumentation".

Informationen zu 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 AFF NetApp Plattformen basieren.

Zu den ASA Plattformen gehören die folgenden:

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

> Ab ONTAP 9.16.0 ist eine vereinfachte ONTAP Erfahrung, die speziell für reine SAN-Kunden entwickelt wurde, auf ASA r2 Systemen (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) verfügbar. Bei einem ASA r2 System finden Sie Informationen im "ASA r2 Systemdokumentation".

ASA Plattformen nutzen symmetrisches Aktiv/Aktiv für Multipathing. Alle Pfade sind aktiv/optimiert, sodass der Host im Falle eines Storage-Failovers nicht auf den ALUA-Übergang der Failover-Pfade warten muss, um die I/O wieder aufzunehmen. Dies verkürzt die Zeit bis zum Failover.

Eine ASA einrichten

All-Flash SAN Arrays (ASAs) folgen dem gleichen Einrichtungsverfahren wie Nicht-ASA Systeme.

Der System Manager führt durch die notwendigen Schritte zur Initialisierung Ihres Clusters, zur Erstellung einer lokalen Ebene, zur Konfiguration von Protokollen und zur Bereitstellung von Speicher für Ihre ASA.

Einstieg in die ONTAP Cluster-Einrichtung.

ASA Host-Einstellungen und Dienstprogramme

Die Host-Einstellungen für die Einrichtung von All-Flash SAN Arrays (ASA) sind die gleichen wie für alle anderen SAN-Hosts.

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

Möglichkeiten zur Identifizierung eines ASA Systems

Ein ASA System lässt sich mithilfe des System Manager oder über die ONTAP Befehlszeile (CLI) identifizieren.

- **Im System Manager Dashboard**: **Cluster > Übersicht** auswählen und anschließend den Systemknoten auswählen.

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

- **Über die Befehlszeile**: Den `san config show` Befehl eingeben.

  Der Wert "All-Flash SAN Array" wird für ASA Systeme als true zurückgegeben.

  Weitere Informationen zu `san config show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Technischer Bericht 4968: NetApp All-SAN Array Datenverfügbarkeit und -integrität"
- "NetApp Technischer Bericht 4080: Bewährte Verfahren für moderne SAN"

Konfiguration der Switches für FCoE in ONTAP

Die Switches müssen für FCoE konfiguriert sein, bevor der FC-Dienst über die bestehende Ethernet-Infrastruktur ausgeführt werden kann.

Bevor Sie beginnen

- Ihre SAN Konfiguration muss unterstützt werden.

  Weitere Informationen zu den unterstützten Konfigurationen sind unter "NetApp Interoperabilitätsmatrix-Tool" zu finden.

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

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

- Auf Ihrem Host muss ein konvergierter Netzwerkadapter (CNA) installiert sein.

Schritte

1. Die Switch-Dokumentation bietet Anleitungen zur Konfiguration der Switches für FCoE.
2. Es sollte sichergestellt sein, dass die DCB-Einstellungen für jeden Knoten im Cluster korrekt konfiguriert sind.

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

   Die DCB-Einstellungen werden am Switch konfiguriert. Die Switch-Dokumentation bietet Unterstützung, falls die Einstellungen nicht korrekt sind.

3. Es sollte überprüft werden, ob die FCoE-Anmeldung funktioniert, wenn der FC-Zielport den Status online `true` hat.

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

   Wenn der Online-Status des FC-Zielports `false` ist, empfiehlt sich ein Blick in die Switch-Dokumentation.

Verwandte Informationen

- "NetApp Interoperabilitätsmatrix-Tool"
- "NetApp Technical Report 3800: Leitfaden zur End-to-End-Bereitstellung von Fibre Channel over Ethernet (FCoE)"
- "Cisco MDS 9000 NX-OS und SAN-OS Software-Konfigurationshandbücher"
- "Brocade Produkte"

Voraussetzungen für die Einrichtung von ONTAP LUNs

Die Einrichtung von LUNs umfasst das Erstellen einer LUN, das Erstellen einer Initiatorgruppe und das Zuordnen der LUN zur Initiatorgruppe. Ihr System muss bestimmte Voraussetzungen erfüllen, bevor die LUNs eingerichtet werden können.

- Die Interoperabilitätsmatrix muss Ihre SAN-Konfiguration als unterstützt auflisten.
- Ihre SAN-Umgebung muss die SAN-Host- und Controller-Konfigurationsgrenzen erfüllen, die in "NetApp Hardware Universe" für Ihre Version der ONTAP Software angegeben sind.
- Es muss eine unterstützte Version von Host Utilities installiert sein.

  Weitere Informationen enthält die Dokumentation zu Host Utilities.

- Sie benötigen SAN LIFs auf dem Knoten, der die LUN besitzt, und auf dem HA-Partner des Knotens, der die LUN besitzt.

Verwandte Informationen

- "NetApp Interoperabilitätsmatrix-Tool"
- "ONTAP SAN Hostkonfiguration"
- "NetApp Technical Report 4017: Best Practices für Fibre Channel SAN"

LUN-Richtlinien für SAN-Umgebungen in ONTAP

Vor der Einrichtung Ihrer LUNs auf Ihrem Cluster sollten diese LUN-Richtlinien überprüft werden.

Warum die tatsächlichen LUN Größen leicht variieren

Im Hinblick auf die Größe Ihrer LUNs ist Folgendes zu berücksichtigen.

- Beim Erstellen einer LUN kann die tatsächliche Größe der LUN je nach OS-Typ der LUN geringfügig variieren. Der LUN OS-Typ kann nach der Erstellung der LUN nicht mehr geändert werden.
- Wenn Sie eine LUN mit der maximalen LUN-Größe erstellen, ist zu beachten, dass die tatsächliche Größe der LUN etwas geringer sein kann. ONTAP rundet das Limit geringfügig nach unten ab.
- Die Metadaten jeder LUN benötigen ca. 64 KB Speicherplatz im übergeordneten Aggregat. Wenn eine LUN erstellt wird, muss sichergestellt sein, dass das übergeordnete Aggregat über ausreichend Speicherplatz 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 die Vergabe von LUN-IDs

Die Standard-LUN-ID beginnt üblicherweise mit 0 und wird für jede weitere zugeordnete LUN in Schritten von 1 vergeben. Der Host ordnet die LUN-ID dem Speicherort und Pfadnamen der LUN zu. Der Bereich gültiger LUN-ID-Nummern hängt vom Host ab. Detaillierte Informationen enthält die Dokumentation, die mit Ihren Host Utilities bereitgestellt wird.

Richtlinien für die Zuordnung von LUNs zu Initiatorgruppen

- Eine LUN kann nur einmal einer Initiatorgruppe zugeordnet werden.
- Als bewährte Vorgehensweise wird empfohlen, eine LUN nur einem bestimmten Initiator über die Initiatorgruppe zuzuordnen.

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

Überprüfung und Hinzufügen Ihrer FC- oder iSCSI-Lizenz in ONTAP

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

Beispiel 1. Schritte

System Manager

Falls ONTAP One nicht vorhanden ist, sollte die FC- oder iSCSI-Lizenz mit ONTAP System Manager (9.7 und höher) überprüft und hinzugefügt werden.

1. Im System Manager **Cluster > Einstellungen > Lizenzen** auswählen
2. Falls die Lizenz nicht aufgeführt ist, + Add auswählen und den Lizenzschlüssel eingeben.
3. Wählen Sie **Add**.

CLI

Falls ONTAP One nicht vorhanden ist, sollte die FC- oder iSCSI-Lizenz mit der ONTAP CLI überprüft und hinzugefügt werden.

1. Es sollte überprüft werden, ob eine gültige Lizenz für FC oder iSCSI vorhanden ist.

```
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. Falls Sie keine aktive Lizenz für FC oder iSCSI besitzen, kann Ihr Lizenzcode hinzugefügt werden.

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

Bereitstellung von SAN Storage in ONTAP

Dieses Verfahren erstellt neue LUNs auf einer bestehenden Storage-VM, auf der das FC- oder iSCSI-Protokoll bereits konfiguriert ist.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" für die Bereitstellung des Speichers zu verwenden. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Wenn eine neue Storage-VM erstellt und das FC- oder iSCSI-Protokoll konfiguriert werden soll, siehe "Eine SVM für FC konfigurieren" oder "Eine SVM für iSCSI konfigurieren".

Wenn die FC-Lizenz nicht aktiviert ist, erscheinen die LIFs und SVMs als online, aber der Betriebsstatus ist „down“.

LUNs erscheinen Ihrem Host als Datenträgergeräte.



Der asymmetrische Zugriff auf logische Einheiten (ALUA) ist bei der LUN-Erstellung immer aktiviert. Die ALUA-Einstellung kann nicht geändert werden.

Für alle FC LIFs in der SVM ist Single Initiator Zoning zu verwenden, um die Initiatoren zu hosten.

Ab ONTAP 9.8 ist QoS bei der Speicherbereitstellung standardmäßig aktiviert. QoS kann während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt deaktiviert oder eine benutzerdefinierte QoS-Richtlinie ausgewählt werden.

Beispiel 2. Schritte

System Manager

LUNs werden erstellt, um Speicher für einen SAN-Host mithilfe des FC- oder iSCSI-Protokolls mit ONTAP System Manager (9.7 und höher) bereitzustellen.

Um diese Aufgabe mit System Manager Classic (verfügbar mit 9.7 und früher) abzuschließen, siehe "iSCSI-Konfiguration für Red Hat Enterprise Linux"

Schritte

1. Die entsprechende "SAN Host-Dienstprogramme" auf Ihrem Host installieren.
2. Im System Manager unter **Storage > LUNs** auf **Add** klicken.
3. Die erforderlichen Informationen zum Erstellen der LUN eingeben.
4. Sie können auf **Weitere Optionen** klicken, um je nach Ihrer Version von ONTAP eine der folgenden Aktionen auszuführen.

Option	Verfügbar ab

• QoS-Richtlinie LUNs statt dem übergeordneten Volume zuweisen ◦ **Weitere Optionen > Storage and Optimization** ◦ **Performance Service Level** auswählen. ◦ Um die QoS-Richtlinie auf einzelne LUNs anstatt auf das gesamte Volume anzuwenden, **Diese Leistungsbegrenzungen auf jede LUN anwenden** auswählen. Standardmäßig werden Leistungsgrenzen auf Volumenebene angewendet.	ONTAP 9.10.1
• Eine neue Initiatorgruppe mithilfe vorhandener Initiatorgruppen erstellen ◦ **Weitere Optionen > HOST-INFORMATIONEN** ◦ **Neue Initiatorgruppe unter Verwendung vorhandener Initiatorgruppen** auswählen. ⓘ Der OS-Typ einer Initiatorgruppe, die andere Initiatorgruppen enthält, kann nach ihrer Erstellung nicht mehr geändert werden.	ONTAP 9.9.1
• Fügen Sie Ihrer Initiatorgruppe oder Ihrem Host-Initiator eine Beschreibung hinzu. Die Beschreibung dient als Alias für die Initiatorgruppe oder den Host-Initiator. ◦ **Weitere Optionen > HOST-INFORMATIONEN**	ONTAP 9.9.1
• Erstellen Sie Ihre LUN auf einem vorhandenen Volume Standardmäßig wird eine neue LUN in einem neuen Volume erstellt. ◦ **Weitere Optionen > LUNs hinzufügen** ◦ **Gruppenbezogene LUNs** auswählen.	ONTAP 9.9.1
• QoS deaktivieren oder eine benutzerdefinierte QoS-Richtlinie auswählen ◦ **Weitere Optionen > Storage and Optimization** ◦ **Performance Service Level** auswählen. ⓘ In ONTAP 9.9.1 und höher ist bei Auswahl einer benutzerdefinierten QoS-Richtlinie auch eine manuelle Platzierung auf einer bestimmten lokalen Ebene möglich.	ONTAP 9.8

5. Für FC sollten die FC-Switches nach WWPN zoniert werden. Es wird eine Zone pro Initiator verwendet, wobei alle Zielports in jede Zone aufgenommen werden.
6. LUNs auf Ihrem Host erkennen.

   Verwenden Sie für VMware vSphere ONTAP tools for VMware vSphere, um Ihre LUNs zu erkennen und zu initialisieren.
7. Die LUNs werden initialisiert und optional Dateisysteme erstellt.
8. Es sollte sichergestellt werden, dass der Host Daten auf der LUN schreiben und lesen kann.

CLI

LUNs werden erstellt, um Speicher für einen SAN-Host mithilfe des FC- oder iSCSI-Protokolls mit der ONTAP CLI bereitzustellen.

1. Es sollte überprüft werden, ob eine Lizenz für FC oder iSCSI vorhanden ist.

```
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. Falls Sie keine Lizenz für FC oder iSCSI besitzen, kann der `license add` Befehl verwendet werden.

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

3. Der Protokolldienst wird auf der SVM aktiviert:

   Für iSCSI:

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

   Für FC:

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

4. Zwei LIFs für die SVMs auf jedem Knoten erstellen:

```
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 mindestens ein iSCSI- oder FC-LIF pro Knoten für jede SVM, die Daten bereitstellt. Für Redundanz sind jedoch zwei LIFs pro Knoten erforderlich. Für iSCSI wird empfohlen, mindestens zwei LIFs pro Knoten in separaten Ethernet-Netzwerken zu konfigurieren.

5. Es wird überprüft, ob Ihre LIFs erstellt wurden und ob ihr Betriebsstatus `online` ist:

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

6. LUNs erstellen:

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

   Ihr LUN Name darf maximal 255 Zeichen lang sein und keine Leerzeichen enthalten.

   Die NVFAIL Option wird 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. Es sollte überprüft werden, ob die LUNs korrekt konfiguriert sind:

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

10. Optional, "Einen Portsatz erstellen und an eine Initiatorgruppe binden".
11. In der Dokumentation Ihres Hostsystems finden Sie die Schritte zur Aktivierung des Blockzugriffs auf Ihren jeweiligen Hosts.
12. Mit den Host-Dienstprogrammen lässt sich die FC- oder iSCSI-Zuordnung abschließen und die LUNs auf dem Host erkennen.

Verwandte Informationen

- "SAN-Administration Übersicht"
- "ONTAP SAN Hostkonfiguration"
- "SAN-Initiatorgruppen in System Manager anzeigen und verwalten"
- "NetApp Technical Report 4017: Best Practices für Fibre Channel SAN"

NVMe Bereitstellung

Informationen zum NVMe-Protokoll in ONTAP

Das Protokoll Non-Volatile Memory Express (NVMe) kann zur Bereitstellung von Speicher in einer SAN-Umgebung verwendet werden. Das NVMe-Protokoll ist für die Leistung mit Solid-State-Speicher optimiert.

Bei NVMe werden Speicherziele als Namespaces bezeichnet. Ein NVMe Namespace ist eine Menge nichtflüchtigen Speichers, die in logische Blöcke formatiert und einem Host als Standard-Blockgerät bereitgestellt werden kann. Namespaces und Subsysteme werden erstellt und anschließend werden die Namespaces den Subsystemen zugeordnet, ähnlich wie LUNs für FC und iSCSI bereitgestellt und Initiatorgruppen zugeordnet werden.

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

Die Unterstützung für NVMe variiert je nach Ihrer Version von ONTAP. Siehe "NVMe Unterstützung und Einschränkungen" für Details.

Was NVMe ist

Das Nonvolatile Memory Express (NVMe) Protokoll ist ein Transportprotokoll, das für den Zugriff auf nichtflüchtige Speichermedien verwendet wird.

NVMe over Fabrics (NVMeoF) ist eine spezifikationsdefinierte Erweiterung von NVMe, die die NVMe-basierte Kommunikation über andere Verbindungen als PCIe ermöglicht. Diese Schnittstelle ermöglicht den Anschluss externer Speichergehäuse an einen Server.

NVMe wurde entwickelt, um effizienten Zugriff auf Speichermedien mit nichtflüchtigem Speicher zu ermöglichen, von Flash-Technologie bis hin zu leistungsstärkeren, persistenten Speichertechnologien. Daher unterliegt es nicht den gleichen Einschränkungen wie Speicherprotokolle, die für Festplattenlaufwerke entwickelt wurden. Flash- und Solid State Devices (SSDs) sind eine Art von nichtflüchtigem Speicher (NVM). NVM ist ein Speichertyp, der seinen Inhalt auch bei einem Stromausfall behält. NVMe ist eine Möglichkeit, auf diesen Speicher zuzugreifen.

Zu den Vorteilen von NVMe gehören höhere Geschwindigkeiten, gesteigerte Produktivität, höherer Durchsatz und größere Kapazität für Datentransfer. Zu den spezifischen Merkmalen zählen:

- NVMe ist für bis zu 64.000 Warteschlangen ausgelegt.

  Jede Warteschlange kann wiederum bis zu 64.000 gleichzeitige Befehle verarbeiten.

- NVMe wird von mehreren Hardware- und Softwareanbietern unterstützt
- NMVe ist mit Flash-Technologien produktiver, da diese schnellere Reaktionszeiten ermöglichen.
- NVMe ermöglicht mehrere Datenanforderungen für jede “request”, die an die SSD gesendet wird.

  NVMe benötigt weniger Zeit, um eine “request” zu decodieren, und erfordert keine Thread-Sperrung in einem Multithread-Programm.

- NVMe unterstützt Funktionen, die einen Flaschenhals auf CPU-Ebene verhindern und enorme Skalierbarkeit ermöglichen, wenn Systeme erweitert werden.

Über NVMe Namensräume

Ein NVMe-Namespace ist eine Menge nichtflüchtigen Speichers (NVM), die in logische Blöcke formatiert werden kann. Namespaces werden verwendet, wenn eine Storage Virtual Machine mit dem NVMe-Protokoll konfiguriert ist, und entsprechen den LUNs bei den FC- und iSCSI-Protokollen.

Ein oder mehrere Namespaces sind bereitgestellt und mit einem NVMe-Host verbunden. Jeder Namespace kann verschiedene Blockgrößen unterstützen.

Das NVMe-Protokoll ermöglicht den Zugriff auf Namensräume über mehrere Controller. Mithilfe von NVMe-Treibern, die von den meisten Betriebssystemen unterstützt werden, erscheinen Solid State Drive (SSD)-Namensräume als Standard-Blockgeräte, auf denen Dateisysteme und Anwendungen ohne jegliche Modifikation bereitgestellt werden können.

Eine Namespace-ID (NSID) ist ein Bezeichner, der von einem Controller verwendet wird, um den Zugriff auf einen Namespace bereitzustellen. Beim Festlegen der NSID für einen Host oder eine Hostgruppe wird auch die Zugänglichkeit eines Volumes durch einen Host konfiguriert. Ein logischer Block kann jeweils nur einer einzigen Hostgruppe zugeordnet werden, und eine bestimmte Hostgruppe enthält keine doppelten NSIDs.

Über NVMe Subsysteme

Ein NVMe-Subsystem umfasst einen oder mehrere NVMe-Controller, Namespaces, NVM-Subsystem-Ports, ein NVM-Speichermedium und eine Schnittstelle zwischen dem Controller und dem NVM-Speichermedium. Wenn ein NVMe-Namespace erstellt wird, ist er standardmäßig keinem Subsystem zugeordnet. Es besteht auch die Möglichkeit, ihn einem neuen oder bestehenden Subsystem zuzuordnen.

Verwandte Informationen

- "NVMe-Speicher bereitstellen" auf ASA, AFF und FAS Systemen verwenden
- "einen NVMe Namensraum einem Subsystem zuordnen" auf ASA AFF und FAS Systemen anwenden.
- "SAN-Hosts und Cloud-Clients konfigurieren"
- Erfahren Sie, wie "SAN Storage bereitstellen" auf ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 oder ASA A20) Speichersystemen gearbeitet wird.

ONTAP NVMe Lizenzanforderungen

Ab ONTAP 9.5 ist eine Lizenz zur Unterstützung von NVMe erforderlich. Wenn NVMe in ONTAP 9.4 aktiviert ist, wird nach dem Upgrade auf ONTAP 9.5 eine 90-tägige Kulanzfrist gewährt, um die Lizenz zu erwerben.

Die Lizenz kann mit dem folgenden Befehl aktiviert werden:

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

NVMe Konfiguration, Unterstützung und Einschränkungen in ONTAP

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

NVMe-Unterstützung und Einschränkungen variieren je nach Ihrer Version von ONTAP, Ihrer Plattform und Ihrer Konfiguration. Details zu Ihrer spezifischen Konfiguration sind in der "NetApp Interoperabilitätsmatrix-

Tool" zu finden. Informationen zu den unterstützten Grenzwerten finden sich unter "Hardware Universe".

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

Konfiguration

- Die NVMe Konfiguration kann mit einem einzelnen Fabric oder mit mehreren Fabrics eingerichtet werden.
- Für jede SVM, die SAN unterstützt, sollte eine Management-LIF konfiguriert werden.
- Die Verwendung heterogener FC-Switch-Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches.

  Spezifische Ausnahmen sind auf der "NetApp Interoperabilitätsmatrix-Tool" aufgeführt.

- Kaskadierte, partielle, vollständige, Core-Edge- und Director-Fabrics sind branchenübliche Methoden zur Verbindung von FC-Switches mit einem Fabric und werden alle unterstützt.

  Ein Fabric kann aus einem oder mehreren Switches bestehen, und die Storage-Controller können mit mehreren Switches verbunden sein.

Features

Die folgenden NVMe-Funktionen werden abhängig von Ihrer ONTAP-Version unterstützt.

Beginnend mit ONTAP…	NVMe unterstützt
9.17.1	• SnapMirror active sync NVMe/FC- und NVMe/TCP-Hostzugriff für VMware Workloads.
9.15.1	• Vier-Knoten MetroCluster IP-Konfigurationen auf NVMe/TCP
9.14.1	• Festlegung der Hostpriorität auf Subsystemebene (Host-Level-QoS)
9.12.1	• Vier-Knoten MetroCluster IP-Konfigurationen auf NVMe/FC • MetroCluster Konfigurationen werden für Frontend-NVMe-Netzwerke vor ONTAP 9.12.1 nicht unterstützt. • MetroCluster Konfigurationen werden auf NVMe/TCP nicht unterstützt.
9.10.1	Ändern der Größe eines Namensraums
9.9.1	• Koexistenz von Namensräumen und LUNs auf demselben Volume

9,8	• Protokollkoexistenz Die Protokolle SCSI, NAS und NVMe können auf derselben virtuellen Speichermaschine (SVM) existieren. Wenn die gleichzeitige Nutzung mehrerer Protokolle vom Host-Betriebssystem nicht unterstützt wird, sollten Sie für jedes vom Host unterstützte Protokoll eine separate SVM konfigurieren. Vor ONTAP 9.8 konnte NVMe das einzige Protokoll auf der SVM sein.
9,6	• 512-Byte-Blöcke und 4096-Byte-Blöcke für Namensräume 4096 ist der Standardwert. 512 sollte nur verwendet werden, wenn das Host-Betriebssystem keine 4096-Byte-Blöcke unterstützt. • Volume Move mit zugeordneten Namespaces
9,5	• Multipath HA Pair Failover/Giveback

Protokolle

Die folgenden NVMe-Protokolle werden unterstützt.

Protokoll	Beginnend mit ONTAP…	Erlaubt durch…
TCP	9.10.1	Standard
FC	9,4	Standard

Ab ONTAP 9.8 ist es möglich, die Protokolle SCSI, NAS und NVMe auf derselben Storage Virtual Machine (SVM) zu konfigurieren. In ONTAP 9.7 und früher kann NVMe das einzige Protokoll auf der SVM sein.

Namensräume

Beim Arbeiten mit NVMe Namespaces ist Folgendes zu beachten:

- Für ONTAP 9.15.1 und frühere Versionen unterstützt ONTAP den NVMe DataSet Management-Befehl (deallocate) mit NVMe zur Speicherplatzzurückgewinnung nicht.
- Sie können SnapRestore nicht verwenden, um einen Namespace von einer LUN wiederherzustellen oder umgekehrt.
- Die Speicherplatzzusage für Namensräume entspricht der Speicherplatzzusage des übergeordneten Volumes.
- Bei einem Volume-Übergang von Data ONTAP, das im 7-Mode betrieben wird, kann kein Namespace erstellt werden.
- Namensräume unterstützen Folgendes nicht:
  - Umbenennung
  - Inter-Volume-Verschiebung

- Inter-Volume-Kopie
- Kopie auf Anfrage

Weitere Einschränkungen

Die folgenden ONTAP Funktionen werden von NVMe Konfigurationen nicht unterstützt:

- persistente Reservierungen

Das Folgende gilt nur für Knoten, auf denen ONTAP 9.4 ausgeführt wird:

- NVMe LIFs und Namespaces müssen auf demselben Knoten gehostet werden.
- Der NVMe Service muss erstellt werden, bevor die NVMe LIF erstellt wird.

Verwandte Informationen

"Bewährte Verfahren für moderne SAN"

Konfiguration einer ONTAP Storage VM für NVMe

Wenn Sie das NVMe-Protokoll auf einem Knoten verwenden möchten, muss Ihre SVM speziell für NVMe konfiguriert werden.

Bevor Sie beginnen

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

Beispiel 3. Schritte

System Manager

Eine Storage-VM für NVMe mit ONTAP System Manager (9.7 und höher) konfigurieren.

NVMe auf einer neuen Storage-VM konfigurieren	NVMe auf einer vorhandenen Storage-VM konfigurieren
1. Im System Manager auf **Storage > Storage VMs** klicken und dann auf **Add**. 2. Geben Sie einen Namen für die Storage-VM ein. 3. **NVMe** für das **Zugriffsprotokoll** auswählen. 4. Wählen Sie **NVMe/FC aktivieren** oder **NVMe/TCP aktivieren**. 5. Wenn Sie NVMe/TCP aktivieren und Netzwerkpfade im Falle eines Knotenausfalls automatisch auf den HA-Partner umgeschaltet werden sollen, gehen Sie wie folgt vor: Diese Option ist in ONTAP 9.19.1 und späteren Versionen nur auf AFF- und ASA-Systemen verfügbar. ◦ Wählen Sie für AFF-Systeme **Symmetrisches Aktiv/Aktiv-Multipathing** und anschließend **Symmetrisches Aktiv/Aktiv-Multipathing aktivieren**. ◦ Wählen Sie für ASA-Systeme **Symmetrisches Aktiv/Aktiv-Multipathing** und anschließend **Aktivieren für SCSI- und NVMe-Protokolle**. 6. **Speichern** auswählen.	1. Im System Manager auf **Storage > Storage-VMs** klicken. 2. Auf die Storage-VM, die konfiguriert werden soll, klicken. 3. Auf die Registerkarte **Einstellungen** wechseln und anschließend ⚙ neben dem NVMe-Protokoll auswählen. 4. **NVMe/FC aktivieren** oder **NVMe/TCP aktivieren** und **Speichern** auswählen.

CLI

Eine Storage-VM für NVMe mit der ONTAP CLI konfigurieren.

1. Wenn keine vorhandene SVM verwendet werden soll, kann eine neue erstellt werden:

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

   a. Es sollte überprüft werden, ob die SVM erstellt wurde:

```
vserver show
```

2. Es sollte überprüft werden, ob in Ihrem Cluster NVMe- oder TCP-fähige Adapter installiert sind:

   Für NVMe:

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

Für TCP:

```
network port show
```

Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

3. Wenn Sie ONTAP 9.7 oder eine frühere Version verwenden, alle Protokolle aus der SVM entfernen:

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

Ab ONTAP 9.8 ist es nicht erforderlich, andere Protokolle zu entfernen, wenn NVMe hinzugefügt wird.

4. Das NVMe-Protokoll zur SVM hinzufügen:

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

5. Wenn Sie ONTAP 9.7 oder eine ältere Version verwenden, überprüfen Sie, ob NVMe das einzige auf der SVM zulässige Protokoll ist:

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

Nur das NVMe-Protokoll sollte in der `allowed protocols`Spalte angezeigt werden.

6. NVMe-Dienst erstellen:

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

7. Es sollte überprüft werden, ob der NVMe-Dienst erstellt wurde:

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

Der `Administrative Status` der SVM sollte als `up` aufgeführt sein.

8. Eine NVMe/FC LIF erstellen:
   - Für ONTAP 9.9.1 oder älter, 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. Eine NVMe/FC-LIF auf dem HA-Partnerknoten erstellen:
   - Für ONTAP 9.9.1 oder älter, 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, ob die NVMe/FC LIFs erstellt wurden:

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

11. Volume auf demselben Knoten wie die LIF erstellen:

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

Wenn eine Warnmeldung bezüglich der automatischen Effizienzrichtlinie angezeigt wird, kann diese getrost ignoriert werden.

Bereitstellung von NVMe Storage in ONTAP

Bei der Bereitstellung von Speicher ermöglichen Sie Ihren NVMe-Hosts das Lesen und Schreiben von Daten auf ONTAP-Speichersystemen. Für Systeme, die das NVMe-Protokoll verwenden, ist die Erstellung eines oder mehrerer NVMe-Namespaces und NVMe-Subsysteme erforderlich. Jeder Namespace kann dann einem NVMe-Subsystem zugeordnet werden, um den Datenzugriff von Ihrem Host zu ermöglichen.

Verfügt die Storage Virtual Machine (SVM), die das NVMe-Subsystem enthält, über sowohl NVMe/FC- als auch NVMe/TCP-Netzwerkschnittstellen, können die dem NVMe-Subsystem zugeordneten Namespaces sowohl über NVMe/FC- als auch über NVMe/TCP-Transportprotokolle zugegriffen werden. NVMe-Unterstützung für FC ist ab ONTAP 9.4 und höher verfügbar. NVMe-Unterstützung für TCP ist ab ONTAP 9.10.1 und höher verfügbar. Wenn Sie protokollspezifischen Zugriff auf Ihre Namespaces benötigen, sollten Sie "Konfigurieren einer SVM" für jedes Protokoll vornehmen.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" für die Bereitstellung des Speichers zu verwenden. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

Ab ONTAP 9.8 ist QoS bei der Speicherbereitstellung standardmäßig aktiviert. QoS kann während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt deaktiviert oder eine benutzerdefinierte QoS-Richtlinie ausgewählt werden.

Bevor Sie beginnen

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

System Manager

Mit ONTAP System Manager (Version 9.7 und höher) lassen sich Namespaces erstellen, um Speicher mithilfe des NVMe-Protokolls bereitzustellen.

Schritte

1. Im System Manager auf **Storage > NVMe Namespaces** klicken und dann auf **Add** klicken.

   Falls ein neues Subsystem erstellt werden soll, auf **Weitere Optionen** klicken.

2. Wenn ONTAP 9.8 oder höher verwendet wird und QoS deaktiviert oder eine benutzerdefinierte QoS-Richtlinie ausgewählt werden soll, unter **Speicher und Optimierung** die Option **Leistungsdienststufe** auswählen, nachdem auf **Weitere Optionen** geklickt wurde.
3. Die FC-Switches werden nach WWPN zoniert. Es wird eine Zone pro Initiator verwendet, wobei alle Zielports in jede Zone aufgenommen werden.
4. Auf Ihrem Host die neuen Namensräume erkennen.
5. Der Namensraum wird initialisiert und mit einem Dateisystem formatiert.
6. Es sollte sichergestellt sein, dass Ihr Host Daten im Namespace schreiben und lesen kann.

CLI

Mit der ONTAP CLI Namespaces erstellen, um Speicher über das NVMe-Protokoll bereitzustellen.

Dieses Verfahren erstellt einen NVMe-Namespace und ein NVMe-Subsystem auf einer vorhandenen Storage-VM, die bereits für das NVMe-Protokoll konfiguriert wurde, und ordnet dann den Namespace dem Subsystem zu, um den Datenzugriff von Ihrem Hostsystem zu ermöglichen.

Wenn die Storage-VM für NVMe konfiguriert werden soll, siehe "Eine SVM für NVMe konfigurieren".

Schritte

1. Es sollte überprüft werden, ob die SVM für NVMe konfiguriert ist:

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

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

2. Den NVMe-Namespace erstellen:

   Das mit dem `-path` Parameter referenzierte Volume muss bereits existieren oder es muss vor der Ausführung dieses Befehls erstellt werden.

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

3. Das NVMe-Subsystem erstellen:

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

   Der Name des NVMe-Subsystems unterscheidet Groß-/Kleinschreibung. Er muss 1 bis 96 Zeichen lang sein. Sonderzeichen sind zulässig.

4. Es sollte überprüft werden, ob das Subsystem erstellt wurde.

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

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

5. Den NQN vom Host abrufen.
6. Den Host-NQN zum Subsystem hinzufügen:

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

7. Den Namensraum dem Subsystem zuordnen:

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

Ein Namensraum kann nur einem einzigen Subsystem zugeordnet werden.

8. Es sollte überprüft werden, ob der Namensraum dem Subsystem zugeordnet ist:

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

Das Subsystem sollte als `Attached subsystem` aufgeführt sein.

Zuordnung eines NVMe Namespace zu einem Subsystem in ONTAP

Durch die Zuordnung eines NVMe-Namensraums zu einem Subsystem wird der Datenzugriff von Ihrem Host aus ermöglicht. Ein NVMe-Namensraum kann einem Subsystem entweder bei der Bereitstellung des Speichers oder nach der Bereitstellung zugeordnet werden.

Ab ONTAP 9.17.1 kann bei Verwendung einer SnapMirror Active Sync Konfiguration eine SVM als proximaler vServer zu einem Host hinzugefügt werden, während der Host zu einem NVMe Subsystem hinzugefügt wird. Aktiv-optimierte Pfade für einen Namespace in einem NVMe Subsystem werden nur von der als proximaler vServer konfigurierten SVM an einen Host veröffentlicht.

Ab ONTAP 9.14.1 kann die Ressourcenzuweisung für bestimmte Hosts priorisiert werden. Standardmäßig erhält ein Host beim Hinzufügen zum NVMe Subsystem die Priorität Normal. Die Standardpriorität kann über die ONTAP command line interface (CLI) manuell von Normal auf Hoch geändert werden. Hosts mit hoher Priorität werden größere I/O-Warteschlangenzahlen und Warteschlangentiefen zugewiesen.

Wenn einem Host, der in ONTAP 9.13.1 oder früher zu einem Subsystem hinzugefügt wurde, eine hohe Priorität zugewiesen werden soll, ist dies möglich die Host-Priorität ändern.

Bevor Sie beginnen

Ihr Namespace und Ihr Subsystem sollten bereits erstellt sein. Falls ein Namespace und ein Subsystem erstellt werden müssen, siehe "NVMe Storage bereitstellen".

Einem NVMe-Namensraum eine Zuordnung zuweisen

Schritte

1. Den NQN vom Host abrufen.
2. Den Host-NQN zum Subsystem hinzufügen:

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

   Wenn die Standardpriorität des Hosts von „Normal“ auf „Hoch“ geändert werden soll, steht die `-priority high` Option zur Verfügung. Diese Option ist ab ONTAP 9.14.1 verfügbar. Weitere Informationen zu `vserver nvme subsystem host add` finden sich in der "ONTAP-Befehlsreferenz".

   Wenn eine SVM als `proximal-vserver` zu einem Host hinzugefügt werden soll, während der Host zu einem NVMe-Subsystem in einer SnapMirror active sync Konfiguration hinzugefügt wird, kann die `-proximal-vservers` Option verwendet werden. Diese Option ist ab ONTAP 9.17.1 verfügbar. Es kann die Quell- oder Ziel-SVM oder beide hinzugefügt werden. Die SVM, in der dieser Befehl ausgeführt wird, ist die Standard-SVM.

3. Den Namensraum dem Subsystem zuordnen:

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

   Ein Namensraum kann nur einem einzigen Subsystem zugeordnet werden. Weitere Informationen zu `vserver nvme subsystem map add` finden sich in der "ONTAP-Befehlsreferenz".

4. Es sollte überprüft werden, ob der Namensraum dem Subsystem zugeordnet ist:

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

   Das Subsystem sollte als `Attached subsystem` aufgeführt sein. Weitere Informationen zu `vserver nvme namespace show` finden sich in der "ONTAP-Befehlsreferenz".

LUNs verwalten

Bearbeiten einer ONTAP LUN QoS-Richtliniengruppe

Ab ONTAP 9.10.1 kann mit System Manager Quality of Service (QoS)-Richtlinien gleichzeitig mehreren LUNs zugewiesen oder von diesen entfernt werden.

Wenn die QoS-Richtlinie auf Volume-Ebene zugewiesen ist, muss sie auf Volume-Ebene

geändert werden. Die QoS-Richtlinie kann nur auf LUN-Ebene bearbeitet werden, wenn sie ursprünglich auf LUN-Ebene zugewiesen wurde.

Schritte

1. Im System Manager auf **Speicher > LUNs** klicken.
2. Wählen Sie die LUN oder LUNs aus, die bearbeitet werden sollen.

   Wenn Sie mehrere LUNs gleichzeitig bearbeiten, müssen diese zur selben Storage Virtual Machine (SVM) gehören. Wenn Sie LUNs auswählen, die nicht zur selben SVM gehören, wird die Option zum Bearbeiten der QoS Policy Group nicht angezeigt.

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

Konvertierung einer ONTAP LUN in einen NVME Namespace

Ab ONTAP 9.11.1 kann die ONTAP CLI verwendet werden, um eine bestehende LUN direkt in einen NVMe Namespace zu konvertieren.

Bevor Sie beginnen

- Die angegebene LUN sollte keine bestehenden Zuordnungen zu einer Initiatorgruppe haben.
- Die LUN sollte sich nicht in einer für MetroCluster konfigurierten SVM oder in einer SnapMirror active sync Beziehung befinden.
- LUN sollte kein Protokollendpunkt sein oder an einen Protokollendpunkt gebunden sein.
- LUN sollte keinen Präfix- und/oder Suffix-Stream ungleich Null aufweisen.
- Die LUN sollte nicht Teil eines Snapshots sein oder auf der Zielseite der SnapMirror Beziehung als schreibgeschützte LUN vorliegen.

Schritt

1. Eine LUN in einen NVMe-Namensraum konvertieren:

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

Eine ONTAP LUN offline schalten

Ab ONTAP 9.10.1 kann der System Manager verwendet werden, um LUNs offline zu nehmen. Vor ONTAP 9.10.1 muss die ONTAP CLI verwendet werden, um LUNs offline zu nehmen.

System Manager

Schritte

1. Im System Manager auf **Speicher > LUNs** klicken.
2. Eine einzelne LUN oder mehrere LUNs offline nehmen

Wenn Sie Folgendes tun möchten…	Tun Sie Folgendes…
Eine einzelne LUN offline nehmen	Neben dem LUN-Namen auf ⋮ klicken und **Offline nehmen** auswählen.
Mehrere LUNs offline schalten	1. Wählen Sie die LUNs aus, die offline genommen werden sollen. 2. Klicken Sie auf **Mehr** und wählen Sie **Offline nehmen**.

CLI

Über die CLI kann immer nur eine LUN gleichzeitig offline genommen werden.

Schritt

1. Die LUN offline schalten:

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

Ändern der Größe einer LUN in ONTAP

Sie können die Größe einer LUN vergrößern oder verkleinern.

Über diese Aufgabe

Dieses Verfahren gilt für FAS, AFF und ASA Systeme. Bei einem ASA r2 System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) ist "diese Schritte" zu befolgen, um die Größe einer Speichereinheit zu erhöhen. ASA r2 Systeme bieten eine vereinfachte ONTAP Erfahrung speziell für ausschließlich SAN-basierte Kunden.

ⓘ Solaris LUNs können nicht in ihrer Größe verändert werden.

Die Größe einer LUN vergrößern

Die Größe, auf die Sie Ihre LUN erweitern können, variiert je nach Ihrer Version von ONTAP.

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 • 16 TB für Nicht-ASA Plattformen
ONTAP 9.5, 9.6, 9.7	16 TB
ONTAP 9.4 oder früher	Das Zehnfache der ursprünglichen LUN-Größe, jedoch nicht mehr als 16 TB, was die maximale LUN-Größe ist. Beispielsweise kann eine LUN mit 100 GB nur auf 1.000 GB vergrößert werden. Die tatsächliche maximale Größe der LUN beträgt möglicherweise nicht exakt 16 TB. ONTAP rundet das Limit geringfügig nach unten ab.

Sie müssen die LUN nicht offline nehmen, um ihre Größe zu erhöhen. Nachdem Sie die Größe erhöht haben, muss die LUN jedoch auf dem Host erneut gescannt werden, damit der Host die Größenänderung erkennt.

Beispiel 4. Schritte

System Manager

Die Größe einer LUN mit ONTAP System Manager (9.7 und höher) vergrößern.

1. Im System Manager auf **Speicher > LUNs** klicken.
2. Klicken Sie ⋮ und wählen Sie **Bearbeiten**.
3. Unter **Speicher und Optimierung** die Größe der LUN erhöhen und **Speichern** auswählen.

CLI

Die Größe einer LUN lässt sich mit der ONTAP CLI erhöhen.

1. Die Größe der LUN erhöhen:

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

   Weitere Informationen zu `lun resize` finden sich in der "ONTAP-Befehlsreferenz".

2. Die erhöhte LUN-Größe kann überprüft werden:

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

ONTAP Operationen runden die tatsächliche Maximalgröße der LUN ab, sodass sie etwas kleiner als der erwartete Wert ist. Die tatsächliche LUN-Größe kann zudem je nach Betriebssystemtyp der LUN leicht variieren. Der exakte Wert der angepassten Größe lässt sich durch Ausführen der folgenden Befehle im erweiterten Modus ermitteln:

```
set -unit B

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

+
Weitere Informationen zu `lun show` finden sich in der "ONTAP-Befehlsreferenz".

1. Die LUN auf dem Host wird erneut gescannt.
2. In der Hostdokumentation finden sich Hinweise darauf, wie die Größe der neu erstellten LUN im Host-Dateisystem sichtbar wird.

Die Größe einer LUN verringern

Bevor die Größe einer LUN verringert wird, muss der Host die Blöcke mit den LUN-Daten in den Bereich der kleineren LUN-Größe migrieren. Ein Tool wie SnapCenter sollte verwendet werden, um sicherzustellen, dass die LUN korrekt verkleinert wird, ohne dass Blöcke mit LUN-Daten abgeschnitten werden. Eine manuelle Verringerung der LUN-Größe wird nicht empfohlen.

Nachdem Sie die Größe Ihrer LUN verringert haben, benachrichtigt ONTAP den Initiator automatisch darüber, dass die LUN-Größe verringert wurde. Unter Umständen sind jedoch zusätzliche Schritte auf Ihrem Host erforderlich, damit der Host die neue LUN-Größe erkennt. In der Dokumentation Ihres Hosts finden sich spezifische Informationen zur Verkleinerung der Host-Dateistruktur.

Eine ONTAP LUN verschieben

Sie können eine LUN innerhalb einer Storage Virtual Machine (SVM) zwischen Volumes verschieben, jedoch nicht zwischen SVMs. LUNs, die innerhalb einer SVM zwischen Volumes verschoben werden, werden sofort und ohne Verbindungsverlust übertragen.

Bevor Sie beginnen

Wenn Ihre LUN Selective LUN Map (SLM) verwendet, sollte "die SLM Reporting-Nodes-Liste ändern" der Zielknoten und sein HA-Partner einbezogen werden, bevor die LUN verschoben wird.

Über diese Aufgabe

Funktionen zur Speichereffizienz wie Deduplizierung, Komprimierung und Verdichtung bleiben bei einer LUN-Verschiebung nicht erhalten. Sie müssen nach Abschluss der LUN-Verschiebung erneut angewendet werden.

Der Datenschutz durch Snapshots erfolgt auf Volume-Ebene. Daher unterliegt eine LUN nach dem Verschieben dem Datenschutzschema des Zielvolumes. Wenn für das Zielvolume keine Snapshots eingerichtet sind, werden keine Snapshots der LUN erstellt. Außerdem verbleiben alle Snapshots der LUN im ursprünglichen Volume, bis diese Snapshots gelöscht werden.

Sie können eine LUN nicht auf die folgenden Volumes verschieben:

- Ein SnapMirror Zielvolumen
- Das SVM Root-Volume

Die folgenden LUN-Typen können nicht verschoben werden:

- Eine LUN, die aus einer Datei erstellt wurde
- Eine LUN im NVFail Zustand
- Eine LUN, die sich in einer Lastverteilungsbeziehung befindet
- Eine Protokoll-Endpunkt-Klasse LUN

Wenn die Knoten in einem Cluster unterschiedliche ONTAP Versionen verwenden, kann eine LUN nur zwischen Volumes auf verschiedenen Knoten verschoben werden, wenn die Quelle eine neuere Version als das Ziel verwendet. Wenn beispielsweise der Knoten des Quell-Volumes ONTAP 9.15.1 und der Knoten des Ziel-Volumes ONTAP 9.16.1 verwendet, ist eine Verschiebung der LUN nicht möglich. LUNs können zwischen Volumes auf Knoten verschoben werden, die dieselbe ONTAP Version verwenden.



Bei Solaris os_type LUNs mit einer Größe von 1 TB oder mehr kann es während des Verschiebens der LUN auf dem Host zu einer Zeitüberschreitung kommen. Bei diesem LUN-Typ sollte die LUN vor dem Starten des Verschiebevorgangs ausgehängt werden.

Beispiel 5. Schritte

System Manager

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

Ab ONTAP 9.10.1 kann mit dem System Manager ein neues Volume erstellt werden, wenn eine einzelne LUN verschoben wird. In ONTAP 9.8 und 9.9.1 muss das Volume, auf das die LUN verschoben wird, bereits existieren, bevor der LUN-Verschiebungsvorgang beginnt.

Schritte

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

   In ONTAP 9.10.1 kann ausgewählt werden, ob die LUN auf **ein vorhandenes Volume** oder auf ein **neues Volume** verschoben wird.

   Wenn Sie die Option zum Erstellen eines neuen Volumes auswählen, geben Sie die Volume-Spezifikationen an.
3. Auf **Verschieben** klicken.

CLI

Eine LUN mit der ONTAP CLI verschieben.

1. Die LUN verschieben:

   ```
   lun move start
   ```

   Für einen sehr kurzen Zeitraum ist die LUN sowohl auf dem Quell- als auch auf dem Zielvolume sichtbar. Dies ist zu erwarten und wird nach Abschluss des Umzugs behoben.
2. Den Status des Umzugs nachverfolgen und den erfolgreichen Abschluss überprüfen:

   ```
   lun move show
   ```

Verwandte Informationen

- "Selektive LUN Zuordnung"

ONTAP LUNs löschen

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

Bevor Sie beginnen

Die LUN muss von ihrer Initiatorgruppe getrennt werden, bevor sie gelöscht werden kann.

Schritte

1. Es sollte sichergestellt werden, dass die Anwendung oder der Host die LUN nicht verwendet.
2. LUN aus der Initiatorgruppe entfernen:

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

3. Die LUN löschen:

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

4. Überprüfen, ob die LUN gelöscht wurde:

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

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

Informationen zum Kopieren von ONTAP LUNs

Vor dem Kopieren einer LUN sind bestimmte Aspekte zu berücksichtigen.

Clusteradministratoren können eine LUN mithilfe des `lun copy` Befehls zwischen Storage Virtual Machines (SVMs) innerhalb des Clusters kopieren. Clusteradministratoren müssen die Peering-Beziehung zwischen den Storage Virtual Machines (SVMs) mithilfe des `vserver peer create` Befehls herstellen, bevor eine LUN-Kopie zwischen SVMs durchgeführt wird. Auf dem Quellvolume muss ausreichend Speicherplatz für einen SIS-Klon vorhanden sein.

LUNs in Snapshots können als Quell-LUNs für den `lun copy` Befehl verwendet werden. Beim Kopieren einer LUN mit dem `lun copy` Befehl ist die LUN-Kopie sofort für Lese- und Schreibzugriffe verfügbar. Die Quell-LUN bleibt durch das Erstellen einer LUN-Kopie unverändert. Sowohl die Quell-LUN als auch die LUN-Kopie existieren als eindeutige LUNs mit unterschiedlichen LUN-Seriennummern. Änderungen an der Quell-LUN werden nicht in der LUN-Kopie übernommen, und Änderungen an der LUN-Kopie werden nicht in der Quell-LUN übernommen. Die LUN-Zuordnung der Quell-LUN wird nicht auf die neue LUN kopiert, die LUN-Kopie muss zugeordnet werden.

Der Datenschutz durch Snapshots erfolgt auf Volume-Ebene. Wenn eine LUN auf ein anderes Volume als das Volume der Quell-LUN kopiert wird, unterliegt die Ziel-LUN dem Datenschutzschema des Ziel-Volumes. Wenn für das Ziel-Volume keine Snapshots eingerichtet sind, werden von der LUN-Kopie keine Snapshots erstellt.

Das Kopieren von LUNs ist ein unterbrechungsfreier Vorgang.

Die folgenden LUN-Typen können nicht kopiert werden:

- Eine LUN, die aus einer Datei erstellt wurde

- Eine LUN im NVFAIL Zustand
- Eine LUN, die sich in einer Lastverteilungsbeziehung befindet
- Eine Protokoll-Endpunkt-Klasse LUN

Weitere Informationen zu `lun copy` finden sich in der "ONTAP-Befehlsreferenz".

Prüfung des konfigurierten und belegten Speicherplatzes einer ONTAP LUN

Die Kenntnis des konfigurierten Speicherplatzes und des tatsächlich für Ihre LUNs verwendeten Speicherplatzes kann dabei helfen, die Menge an Speicherplatz zu bestimmen, die bei der Speicherplatzrückgewinnung zurückgewonnen werden kann, die Menge des reservierten Speicherplatzes, der Daten enthält, sowie die gesamte konfigurierte Größe im Vergleich zur tatsächlich für eine LUN verwendeten Größe.

Schritt

1. Anzeigen des konfigurierten Speicherplatzes im Vergleich zum tatsächlich für eine LUN verwendeten Speicherplatz:

   ```
   lun show
   ```

   Das folgende Beispiel zeigt den konfigurierten Speicherplatz im Vergleich zum tatsächlich von den LUNs in der vs3 Storage Virtual Machine (SVM) belegten Speicherplatz:

   ```
   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.
   ```

   Weitere Informationen zu `lun show` finden sich in der "ONTAP-Befehlsreferenz".

Steuerung und Überwachung der E/A-Performance von LUNs mithilfe von ONTAP Storage QoS

Sie können die Ein-/Ausgabeleistung (E/A) von LUNs steuern, indem Sie LUNs Storage QoS-Richtliniengruppen zuweisen. Die Steuerung der E/A-Leistung kann dazu dienen, sicherzustellen, dass Workloads bestimmte Leistungsziele erreichen, oder um einen Workload zu drosseln, der andere Workloads beeinträchtigt.

Über diese Aufgabe

Richtliniengruppen erzwingen eine maximale Durchsatzbegrenzung (z. B. 100 MB/s). Sie können eine Richtliniengruppe erstellen, ohne eine maximale Durchsatzbegrenzung anzugeben, wodurch Sie die Leistung überwachen können, bevor Sie die Arbeitslast steuern.

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

zuweisen.

Beachten Sie die folgenden Anforderungen für die Zuordnung einer LUN zu einer Richtliniengruppe:

- Die LUN muss sich in der SVM befinden, zu der die Richtliniengruppe gehört.

  Die SVM wird beim Erstellen der Richtliniengruppe angegeben.

- Wenn eine LUN einer Richtliniengruppe zugewiesen wird, kann das die LUN enthaltende Volume oder die SVM nicht einer Richtliniengruppe zugewiesen werden.

Weitere Informationen zur Verwendung von Storage QoS sind unter "Systemadministrationsreferenz" zu finden.

Schritte

1. Mit dem `qos policy-group create` Befehl lässt sich eine Richtliniengruppe erstellen.

   Weitere Informationen zu `qos policy-group create` finden sich in der "ONTAP-Befehlsreferenz".

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

   Weitere Informationen zu `lun` finden sich in der "ONTAP-Befehlsreferenz".

3. Die `qos statistics` Befehle ermöglichen die Anzeige von Leistungsdaten.
4. Gegebenenfalls kann der `qos policy-group modify` Befehl verwendet werden, um die maximale Durchsatzbegrenzung der Policy-Gruppe anzupassen.

   Weitere Informationen zu `qos policy-group modify` finden sich in der "ONTAP-Befehlsreferenz".

Verfügbare Tools zur effektiven Überwachung von ONTAP LUNs

Tools stehen zur Verfügung, um Ihre LUNs effektiv zu überwachen und Speicherplatzprobleme zu vermeiden.

- Active IQ Unified Manager ist ein kostenloses Tool, das die Verwaltung des gesamten Speichers über alle Cluster in Ihrer Umgebung ermöglicht.
- Der System Manager ist eine grafische Benutzeroberfläche, die in ONTAP integriert ist und die manuelle Verwaltung des Speicherbedarfs auf Clusterebene ermöglicht.
- OnCommand Insight bietet eine einheitliche Sicht auf Ihre Speicherinfrastruktur und ermöglicht die Einrichtung von automatischer Überwachung, Benachrichtigungen und Berichten, wenn der Speicherplatz Ihrer LUNs, Volumes und Aggregate knapp wird.

Funktionen und Einschränkungen von transitionierten ONTAP LUNs

In einer SAN-Umgebung ist während der Transition eines 7-Mode-Volumes zu ONTAP eine Dienstunterbrechung erforderlich. Zum Abschluss der Transition ist das Herunterfahren der Hosts notwendig. Nach der Transition müssen die Host-Konfigurationen aktualisiert werden, bevor die Datenbereitstellung in ONTAP beginnen kann.

Ein Wartungsfenster ist einzuplanen, in dem Sie Ihre Hosts herunterfahren und den Übergang abschließen können.

LUNs, die von Data ONTAP im 7-Mode-Betrieb auf ONTAP migriert wurden, verfügen über bestimmte Fähigkeiten und Einschränkungen, die die Verwaltung der LUNs beeinflussen.

Mit migrierten LUNs sind folgende Aktionen möglich:

- Die LUN kann mit dem `lun show` Befehl angezeigt werden.
- Die Liste der aus dem 7-Mode-Volume migrierten LUNs kann mit dem `transition 7-mode show` Befehl angezeigt werden.
- Wiederherstellung eines Volumes aus einem 7-Mode-Snapshot

  Durch die Wiederherstellung des Volumes werden alle im Snapshot erfassten LUNs in den vorherigen Zustand zurückversetzt.

- Eine einzelne LUN aus einem 7-Mode Snapshot mithilfe des `snapshot restore-file` Befehls wiederherstellen
- Einen Klon einer LUN in einem 7-Mode-Snapshot erstellen
- Einen Blockbereich einer LUN wiederherstellen, der in einem 7-Mode Snapshot erfasst wurde
- Einen FlexClone des Volumes mithilfe eines 7-Mode-Snapshots erstellen

Folgendes ist bei migrierten LUNs nicht möglich:

- Auf Snapshot-gesicherte LUN-Klone, die im Volume erfasst wurden, kann zugegriffen werden

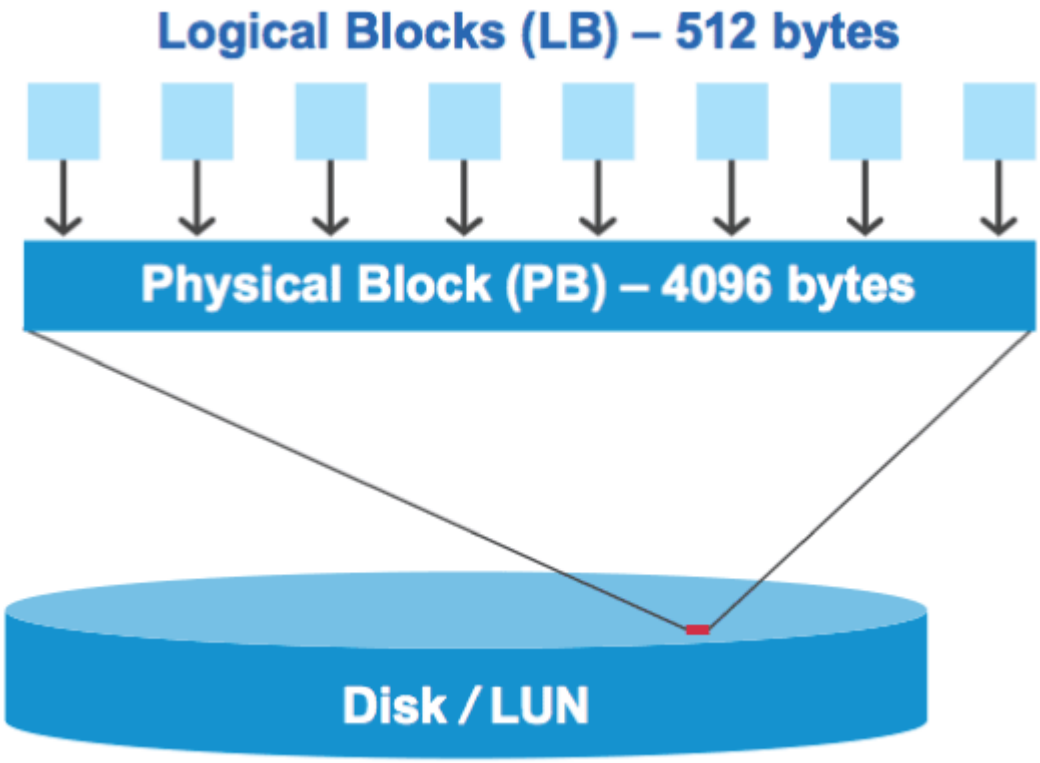
Verwandte Informationen

- "Kopierbasierter Übergang"
- "lun show"

Informationen zu E/A-Fehlausrichtungen bei korrekt ausgerichteten ONTAP LUNs

ONTAP meldet möglicherweise E/A-Fehlausrichtungen bei korrekt ausgerichteten LUNs. Im Allgemeinen können diese Fehlausrichtungswarnungen ignoriert werden, sofern Sie sicher sind, dass Ihre LUN korrekt bereitgestellt ist und Ihre Partitionstabelle korrekt ist.

LUNs und Festplatten stellen beide Speicher als Blöcke bereit. Da die Blockgröße von Festplatten auf dem Host 512 Byte beträgt, präsentieren LUNs dem Host Blöcke dieser Größe, verwenden jedoch tatsächlich größere 4-KB-Blöcke zur Datenspeicherung. Der vom Host verwendete 512-Byte-Datenblock wird als logischer Block bezeichnet. Der von der LUN zur Datenspeicherung verwendete 4-KB-Datenblock wird als physischer Block bezeichnet. Das bedeutet, dass sich in jedem 4-KB-physikalischen Block acht logische 512-Byte-Blöcke befinden.



Das Host-Betriebssystem kann einen Lese- oder Schreib-E/A-Vorgang an jedem logischen Block starten. E/A-Vorgänge gelten nur als ausgerichtet, wenn sie am ersten logischen Block im physischen Block beginnen. Beginnt ein E/A-Vorgang an einem logischen Block, der nicht auch der Anfang eines physischen Blocks ist, gilt der E/A-Vorgang als nicht ausgerichtet. ONTAP erkennt die Fehlausrichtung automatisch und meldet sie auf der LUN. Das Vorhandensein nicht ausgerichteter E/A-Vorgänge bedeutet jedoch nicht zwangsläufig, dass die LUN ebenfalls nicht ausgerichtet ist. Es ist möglich, dass nicht ausgerichtete E/A-Vorgänge auch auf korrekt ausgerichteten LUNs gemeldet werden.

Falls weitere Untersuchungen erforderlich sind, siehe die "NetApp Knowledge Base: Wie können nicht ausgerichtete IOs auf LUNs identifiziert werden?"

Weitere Informationen zu Werkzeugen zur Behebung von Ausrichtungsproblemen sind in der folgenden Dokumentation zu finden: +

- "Windows Unified Host Utilities 7.1"
- "Dokumentation zur Bereitstellung von SAN-Speicher"

E/A-Ausrichtung mithilfe von LUN-OS-Typen erzielen

Für ONTAP 9.7 oder früher sollte der empfohlene ONTAP LUN `ostype` Wert verwendet werden, der am besten zu Ihrem Betriebssystem passt, um eine I/O-Ausrichtung mit Ihrem Betriebssystem-Partitionierungsschema zu erzielen.

Das vom Host-Betriebssystem verwendete Partitionierungsschema trägt maßgeblich zu E/A-Fehlausrichtungen bei. Einige ONTAP LUN `ostype`-Werte verwenden einen speziellen Offset, das sogenannte „Präfix“, damit das standardmäßige Partitionierungsschema des Host-Betriebssystems ausgerichtet werden kann.

Unter bestimmten Umständen ist möglicherweise eine benutzerdefinierte Partitionstabelle

erforderlich, um eine I/O-Ausrichtung zu erreichen. Bei `ostype`-Werten mit einem “prefix”-Wert größer als `0` kann eine benutzerdefinierte Partition jedoch zu einer nicht ausgerichteten I/O führen.

Weitere Informationen zu LUNs, die in ONTAP 9.7 oder früher bereitgestellt wurden, finden sich unter "NetApp Knowledge Base: Wie nicht ausgerichtete E/A auf LUNs identifiziert werden können".

Standardmäßig haben neue LUNs, die in ONTAP 9.8 oder höher bereitgestellt werden, für alle LUN-OS-Typen eine Präfix- und Suffixgröße von Null. Die I/O sollte standardmäßig mit dem unterstützten Host-OS abgestimmt sein.

Besondere Überlegungen zur I/O-Ausrichtung für Linux

Linux-Distributionen bieten vielfältige Möglichkeiten zur Verwendung von LUNs, beispielsweise als Rohgeräte für Datenbanken, verschiedene Volume-Manager und Dateisysteme. Es ist nicht erforderlich, Partitionen auf einer LUN zu erstellen, wenn sie als Rohgerät oder als physisches Volume in einem logischen Volume verwendet wird.

Für RHEL 5 und frühere Versionen sowie SLES 10 und frühere Versionen gilt: Wenn die LUN ohne Volume-Manager verwendet wird, sollte die LUN so partitioniert werden, dass sie eine Partition hat, die bei einem ausgerichteten Offset beginnt, also einem Sektor, der ein gerades Vielfaches von acht logischen Blöcken ist.

Besondere Überlegungen zur I/O-Ausrichtung für Solaris LUNs

Bei der Entscheidung, ob der `solaris`ostype oder der `solaris_efi`ostype verwendet werden sollte, sind verschiedene Faktoren zu berücksichtigen.

Detaillierte Informationen sind in der "Solaris Host Utilities Installations- und Administrationsleitfaden" zu finden.

ESX Boot-LUNs werden als falsch ausgerichtet gemeldet

Als ESX-Boot-LUNs verwendete LUNs werden von ONTAP typischerweise als nicht ausgerichtet gemeldet. ESX erstellt mehrere Partitionen auf der Boot-LUN, was eine Ausrichtung sehr schwierig macht. Nicht ausgerichtete ESX-Boot-LUNs stellen in der Regel kein Leistungsproblem dar, da die Gesamtmenge der nicht ausgerichteten E/A gering ist. Sofern die LUN mit der VMware `ostype` korrekt bereitgestellt wurde, sind keine Maßnahmen erforderlich.

Verwandte Informationen

"Ausrichtung der Dateisystempartitionen/Festplatten der Gast-VMs für VMware vSphere, andere virtuelle Umgebungen und NetApp Speichersysteme"

Möglichkeiten zur Behebung von Problemen, wenn ONTAP LUNs offline gehen

Wenn kein Speicherplatz mehr für Schreibvorgänge verfügbar ist, werden LUNs offline geschaltet, um die Datenintegrität zu gewährleisten. LUNs können aus verschiedenen Gründen keinen Speicherplatz mehr haben und offline gehen, und es gibt mehrere Möglichkeiten, dieses Problem zu beheben.

Wenn die…	Sie können…
Das Aggregat ist voll	• Weitere Festplatten hinzufügen. • Mit dem `volume modify` Befehl lässt sich ein Volume mit verfügbarem Speicherplatz verkleinern. • Wenn Volumes mit Speicherplatzzusage vorhanden sind, die über verfügbaren Speicherplatz verfügen, kann die Speicherplatzzusage des Volumes auf `none`mit dem `volume modify`Befehl geändert werden.
Das Volume ist voll, aber im umschließenden Aggregat ist noch Platz.	• Für Speicherplatzzusage-Volumes kann der `volume modify` Befehl verwendet werden, um die Größe des Volumes zu erhöhen. • Für dünn bereitgestellte Volumes kann der `volume modify` Befehl verwendet werden, um die maximale Größe Ihres Volumes zu erhöhen. Falls die automatische Volumenvergrößerung nicht aktiviert ist, `volume modify -autogrow -mode`kann sie aktiviert werden. • Snapshots können manuell mit dem `volume snapshot delete` Befehl gelöscht werden, oder der `volume snapshot autodelete modify` Befehl wird verwendet, um Snapshots automatisch zu löschen.

Verwandte Informationen

"Festplatten- und lokale Tier (Aggregat)-Verwaltung"

"Logische Speicherverwaltung"

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

Die iSCSI-LUNs werden dem Host als lokale Datenträger angezeigt. Wenn die Speichersystem-LUNs auf dem Host nicht als Datenträger verfügbar sind, empfiehlt sich eine Überprüfung der Konfigurationseinstellungen.

Konfigurationseinstellung	Was zu tun ist
Verkabelung	Es sollte überprüft werden, ob die Kabel zwischen Host und Speichersystem ordnungsgemäß angeschlossen sind.

Konfigurationseinstellung	Was zu tun ist
Netzwerkverbindungen	Es sollte überprüft werden, ob eine TCP/IP-Verbindung zwischen Host und Storage-System besteht. • Von der Storage-System-Konsole aus die Host-Schnittstellen anpingen, die für iSCSI verwendet werden: `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`* • Von der Host-Befehlszeile aus die Storage-System-Schnittstellen anpingen, die für iSCSI verwendet werden: `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`*
Systemvoraussetzungen	Überprüfung, ob die Komponenten Ihrer Konfiguration qualifiziert sind. Zudem sollte sichergestellt sein, dass das korrekte Service Pack des Host-Betriebssystems (OS), die richtige Initiatorversion, die ONTAP Version sowie weitere Systemanforderungen vorliegen. Die Interoperability Matrix enthält die aktuellsten Systemanforderungen.
Jumbo Frames	Wenn in der Konfiguration Jumbo-Frames verwendet werden, sollte überprüft werden, ob Jumbo-Frames auf allen Geräten im Netzwerkpfad aktiviert sind: der Host-Ethernet-NIC, dem Storage-System und allen Switches.
iSCSI-Service-Status	Es sollte sichergestellt sein, dass der iSCSI-Service auf dem Storage-System lizenziert und gestartet ist.
Initiator-Login	Es sollte überprüft werden, ob der Initiator am Storage-System angemeldet ist. Wenn die `iscsi initiator show` Befehlsausgabe anzeigt, dass keine Initiatoren angemeldet sind, sollte die Initiatorkonfiguration auf dem Host überprüft werden. Zudem sollte überprüft werden, ob das Storage-System als Ziel des Initiators konfiguriert ist.
iSCSI-Node-Namen (IQNs)	Stellen Sie sicher, dass Sie in der Initiatorgruppe-Konfiguration die korrekten Node-Namen der Initiatoren verwenden. Auf dem Host können die Initiator-Tools und -Befehle genutzt werden, um den Node-Name des Initiators anzuzeigen. Die in der Initiatorgruppe und auf dem Host konfigurierten Node-Namen der Initiatoren müssen übereinstimmen.
LUN-Zuordnungen	Es sollte überprüft werden, ob die LUNs einer Initiatorgruppe zugeordnet sind. Auf der Storage-System-Konsole kann einer der folgenden Befehle verwendet werden: • `lun mapping show`zeigt alle LUNs und die Initiatorgruppen, denen sie zugeordnet sind, an. • `lun mapping show -igroup`zeigt die LUNs, die einer bestimmten Initiatorgruppe zugeordnet sind.
iSCSI LIFs ermöglichen	Es sollte sichergestellt sein, dass die logischen iSCSI-Schnittstellen aktiviert sind.

Verwandte Informationen

- "NetApp Interoperabilitätsmatrix-Tool"
- "lun mapping show"

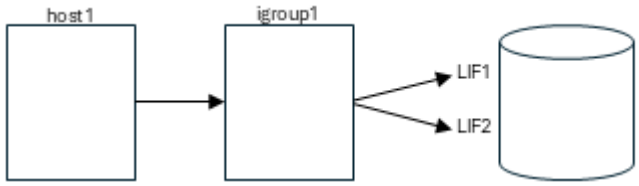
Initiatorgruppen und Portsets verwalten

Möglichkeiten zur Einschränkung des LUN-Zugriffs mit Portsets und igroups in ONTAP

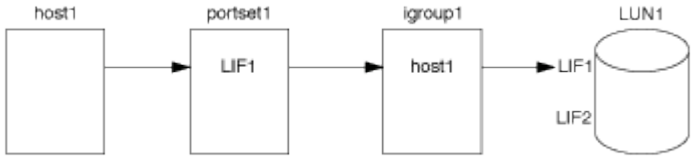
Zusätzlich zur Verwendung von Selective LUN Map (SLM) kann der Zugriff auf Ihre LUNs über Initiatorgruppen und Portsets eingeschränkt werden.

Portsets können in Verbindung mit SLM verwendet werden, um den Zugriff bestimmter Ziele auf bestimmte Initiatoren weiter einzuschränken. Bei Verwendung von SLM mit Portsets sind LUNs auf der Menge der LIFs im Portset auf dem Node, dem die LUN gehört, und auf dem HA-Partner dieses Nodes zugänglich.

Im folgenden Beispiel verfügt host1 über keinen Portsatz. Ohne Portsatz kann host1 auf LUN1 sowohl über LIF1 als auch über LIF2 zugreifen.



Sie können den Zugriff auf LUN1 mithilfe eines Portsets einschränken. Im folgenden Beispiel kann Host1 nur über LIF1 auf LUN1 zugreifen. Host1 kann jedoch nicht über LIF2 auf LUN1 zugreifen, da LIF2 nicht in portset1 ist.



Verwandte Informationen

- Selektive LUN Zuordnung
- Ein Portset erstellen und an eine Initiatorgruppe binden

Anzeigen und Managen von SAN-Initiatoren und igroups in ONTAP

Mit dem System Manager lassen sich Initiatorgruppen (igroups) und Initiatoren anzeigen und verwalten.

Über diese Aufgabe

- Die Initiatorgruppen legen fest, welche Hosts auf bestimmte LUNs im Speichersystem zugreifen können.
- Nachdem ein Initiator und Initiatorgruppen erstellt wurden, ist auch eine Bearbeitung oder das Löschen möglich.
- Zur Verwaltung von SAN-Initiatorgruppen und Initiatoren können die folgenden Aufgaben durchgeführt werden:
  - SAN Initiatorgruppen anzeigen und verwalten
  - SAN Initiatoren anzeigen und verwalten

SAN Initiatorgruppen anzeigen und verwalten

Sie können den System Manager verwenden, um eine Liste der Initiatorgruppen (Initiatorgruppen) anzuzeigen. Aus der Liste können zusätzliche Operationen durchgeführt werden.

Schritte

1. Im System Manager auf **Hosts > SAN Initiatorgruppen** klicken.

   Auf der Seite wird eine Liste der Initiatorgruppen (Initiatorgruppen) angezeigt. Wenn die Liste lang ist, können zusätzliche Seiten der Liste angezeigt werden, indem auf die Seitenzahlen in der unteren rechten Ecke der Seite geklickt wird.

   Die Spalten zeigen verschiedene Informationen zu den Initiatorgruppen an. Ab Version 9.11.1 wird auch der Verbindungsstatus der Initiatorgruppe angezeigt. Durch das Überfahren der Statusmeldungen mit dem Mauszeiger werden Details angezeigt.

2. (Optional): Die folgenden Aufgaben können durch Klicken auf die Symbole in der oberen rechten Ecke der Liste ausgeführt werden:
   - **Suchen**
   - **Laden** Sie die Liste herunter.
   - **Anzeigen** oder **Ausblenden** von Spalten in der Liste.
   - **Filtern** Sie die Daten in der Liste.
3. Folgende Operationen aus der Liste sind möglich:
   - Klicken Sie auf + Add, um eine Initiatorgruppe hinzuzufügen.
   - Klicken Sie auf den Namen der Initiatorgruppe, um die **Übersicht**-Seite anzuzeigen, die Details zur Initiatorgruppe enthält.

     Auf der Seite **Übersicht** können die mit der Initiatorgruppe verknüpften LUNs angezeigt werden, und es besteht die Möglichkeit, Vorgänge zum Erstellen und Zuordnen von LUNs zu initiieren. **Alle SAN-Initiatoren** kann ausgewählt werden, um zur Hauptliste zurückzukehren.

   - Fahren Sie mit dem Mauszeiger über die Initiatorgruppe und klicken Sie dann auf ⋮ neben einem Initiatorgruppen-Namen, um die Initiatorgruppe zu bearbeiten oder zu löschen.
   - Bewegen Sie den Mauszeiger über den Bereich links neben dem Initiatorgruppenamen und aktivieren Sie das Kästchen. Bei Auswahl von **+Zur Initiatorgruppe hinzufügen** besteht die Möglichkeit, diese Initiatorgruppe einer anderen Initiatorgruppe hinzuzufügen.
   - In der Spalte **Speicher-VM** auf den Namen einer Speicher-VM klicken, um Details dazu anzuzeigen.

SAN Initiatoren anzeigen und verwalten

Im System Manager können Sie eine Liste der Initiatoren anzeigen. Aus der Liste können zusätzliche Operationen durchgeführt werden.

Schritte

1. Im System Manager auf **Hosts > SAN Initiatorgruppen** klicken.

   Auf der Seite wird eine Liste der Initiatorgruppen (Initiatorgruppen) angezeigt.

2. So können die Initiatoren angezeigt werden:

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

  Die Spalten enthalten verschiedene Informationen über die Initiatoren.

Ab Version 9.11.1 wird auch der Verbindungsstatus des Initiators angezeigt. Durch das Überfahren der Statusmeldungen mit dem Mauszeiger werden Details angezeigt.

3. (Optional): Die folgenden Aufgaben können durch Klicken auf die Symbole in der oberen rechten Ecke der Liste ausgeführt werden:
   - Die Liste kann nach bestimmten Initiatoren durchsucht werden.
   - **Laden** Sie die Liste herunter.
   - **Anzeigen** oder **Ausblenden** von Spalten in der Liste.
   - **Filtern** Sie die Daten in der Liste.

Eine verschachtelte Initiatorgruppe in ONTAP erstellen

Ab ONTAP 9.9.1 kann eine Initiatorgruppe erstellt werden, die aus anderen bereits vorhandenen igroups besteht.

1. Im System Manager auf **Host > SAN Initiatorgruppen** klicken und dann auf **Hinzufügen**.
2. Geben Sie den **Namen** und die **Beschreibung** der Initiatorgruppe ein.

   Die Beschreibung dient als Alias der Initiatorgruppe.

3. Die **Storage-VM** und das **Host-Betriebssystem** auswählen.

   Der Betriebssystemtyp einer verschachtelten Initiatorgruppe kann nach der Erstellung der Initiatorgruppe nicht mehr geändert werden.

4. Unter **Mitglieder der Initiatorgruppe** die Option **Vorhandene Initiatorgruppe** auswählen.

   Die **Suche** kann verwendet werden, um die Initiatorgruppen zu finden und auszuwählen, die hinzugefügt werden sollen.

Initiatorgruppen mehreren LUNs in ONTAP zuordnen

Ab ONTAP 9.9.1 ist es möglich, Initiatorgruppen gleichzeitig zwei oder mehr LUNs zuzuordnen.

1. Im System Manager auf **Speicher > LUNs** klicken.
2. Wählen Sie die LUNs aus, die Sie zuordnen möchten.
3. **Mehr** auswählen und anschließend **Initiatorgruppen zuordnen** wählen.

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

Erstellung eines ONTAP Portsets und Bindung an eine Initiatorgruppe

Zusätzlich zur Verwendung von "Selective LUN Map (SLM)" kann ein Portset erstellt und das Portset an eine Initiatorgruppe gebunden werden, um weiter einzuschränken, welche LIFs von einem Initiator für den Zugriff auf eine LUN verwendet werden können.

Wenn kein Portset an eine Initiatorgruppe gebunden ist, können alle Initiatoren in der Initiatorgruppe auf zugeordnete LUNs über alle LIFs auf dem Knoten, dem die LUN gehört, sowie auf dem HA-Partner des besitzenden Knotens zugreifen.

Bevor Sie beginnen

Sie benötigen mindestens eine LIF und eine Initiatorgruppe.

Sofern Sie keine Schnittstellengruppen verwenden, werden für iSCSI und FC zwei LIFs zur Redundanz empfohlen. Für Schnittstellengruppen wird nur ein LIF empfohlen.

Über diese Aufgabe

Die Verwendung von Portsets mit SLM ist vorteilhaft, wenn auf einem Knoten mehr als zwei LIFs vorhanden sind und ein bestimmter Initiator auf eine Teilmenge der LIFs beschränkt werden soll. Ohne Portsets sind alle Ziele auf dem Knoten für alle Initiatoren mit Zugriff auf die LUN über den Knoten, dem die LUN gehört, und den HA-Partner des Eigentümerknotens zugänglich.

Beispiel 6. Schritte

System Manager

Ab ONTAP 9.10.1 ist es möglich, mit System Manager Portsets zu erstellen und sie an Initiatorgruppen zu binden.

Wenn ein Portset erstellt und an eine Initiatorgruppe in einer ONTAP Version vor 9.10.1 gebunden werden soll, ist das ONTAP CLI Verfahren zu verwenden.

Ab ONTAP 9.12.1 ist, falls noch kein Portset vorhanden ist, das erste Portset mithilfe der ONTAP CLI-Prozedur zu erstellen.

1. Im System Manager auf **Netzwerk > Übersicht > Portsets** klicken und anschließend auf **Hinzufügen**.
2. Geben Sie die Informationen für das neue Portset ein und wählen Sie **Hinzufügen** aus.
3. **Hosts > SAN Initiator Groups** auswählen.
4. Zum Binden des Portsets an eine neue Initiatorgruppe auf **Hinzufügen** klicken.

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

Verwandte Informationen

"Initiatoren und Initiatorgruppen anzeigen und verwalten"

CLI

1. Einen Portsatz erstellen, 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 `iscsi` an.

2. Die Initiatorgruppe an den Portsatz binden:

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

   Weitere Informationen zu `lun igroup bind` finden sich in der "ONTAP-Befehlsreferenz".

3. Überprüfen, ob die Port-Sets und LIFs korrekt sind:

   `portset show -vserver vserver_name`

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

Managen von ONTAP Portsets

Zusätzlich zu "Selective LUN Map (SLM)"können Portsets verwendet werden, um weiter einzuschränken, welche LIFs von einem Initiator zum Zugriff auf eine LUN genutzt werden können.

Ab ONTAP 9.10.1 kann im System Manager die den Portsets zugeordneten Netzwerkschnittstellen geändert und Portsets gelöscht werden.

Ändern der einem Portset zugeordneten Netzwerkschnittstellen

1. Im System Manager **Netzwerk > Übersicht > Portsets** auswählen.
2. Wählen Sie das Portset aus, das Sie bearbeiten möchten, ⋮ dann **Portset bearbeiten** auswählen.

Löschen eines Portsets

1. Im System Manager unter **Network > Overview > Portsets** navigieren.
2. Um ein einzelnes Portset zu löschen, wählen Sie das Portset aus, wählen Sie ⋮ und dann **Portsets löschen**.

   Mehrere Portsets können gelöscht werden, indem die Portsets ausgewählt und auf **Löschen** geklickt wird.

Informationen zur selektiven LUN-Zuordnung in ONTAP

Selective LUN Map (SLM) reduziert die Anzahl der Pfade vom Host zur LUN. Mit SLM ist die LUN bei der Erstellung einer neuen LUN-Zuordnung nur über Pfade auf dem Knoten, dem die LUN gehört, und seinem HA-Partner erreichbar.

SLM ermöglicht die Verwaltung einer einzelnen Initiatorgruppe pro Host und unterstützt außerdem unterbrechungsfreie LUN-Verschiebungsvorgänge, die keine Portset-Manipulation oder LUN-Neuzuordnung erfordern.

"Port-Sets"Kann in Verbindung mit SLM verwendet werden, um den Zugriff bestimmter Targets auf bestimmte Initiatoren weiter einzuschränken. Bei Verwendung von SLM mit Portsets sind LUNs auf der Menge der LIFs im Portset auf dem Node, dem die LUN gehört, und auf dem HA-Partner dieses Nodes zugänglich.

SLM ist standardmäßig auf allen neuen LUN Maps aktiviert.

Ermitteln, ob SLM auf einer LUN-Zuordnung aktiviert ist

Wenn Ihre Umgebung eine Kombination aus LUNs enthält, die in einer ONTAP 9-Version erstellt wurden, und LUNs, die aus früheren Versionen migriert wurden, muss möglicherweise festgestellt werden, ob Selective LUN Map (SLM) für eine bestimmte LUN aktiviert ist.

Die in der Ausgabe des `lun mapping show -fields reporting-nodes, node` Befehls angezeigten Informationen können zur Feststellung verwendet werden, ob SLM auf Ihrer LUN-Zuordnung aktiviert ist. Wenn SLM nicht aktiviert ist, wird in den Zellen unter der Spalte „`reporting-nodes`“ der Befehlsausgabe ein „-“ angezeigt. Wenn SLM aktiviert ist, wird die Liste der unter der Spalte „`nodes`“ angezeigten Knoten auch in der Spalte „`reporting-nodes`“ angezeigt.

Weitere Informationen zu `lun mapping show` finden sich in der "ONTAP-Befehlsreferenz".

Die SLM-Berichtsknotenliste ändern

Wenn Sie eine LUN oder ein Volume mit LUNs innerhalb desselben Clusters auf ein anderes Hochverfügbarkeitspaar (HA) verschieben, sollten Sie die Reporting-Nodes-Liste der Selective LUN Map (SLM) vor dem Verschieben anpassen, um sicherzustellen, dass aktive, optimierte LUN-Pfade erhalten bleiben.

Schritte

1. Der Zielknoten und sein Partnerknoten werden der Reporting-Nodes-Liste des Aggregats oder Volumes hinzugefügt:

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

   Wenn Sie eine einheitliche Namenskonvention haben, können Sie mehrere LUN-Zuordnungen gleichzeitig ändern, indem Sie `igroup_prefix*` anstelle von `igroup_name` verwenden.

2. Der Host wird erneut gescannt, damit die neu hinzugefügten Pfade erkannt werden.
3. Falls Ihr Betriebssystem dies erfordert, sind die neuen Pfade der Multipath Network I/O (MPIO) Konfiguration hinzuzufügen.
4. Den Befehl für den benötigten Verschiebevorgang ausführen und abwarten, bis der Vorgang abgeschlossen ist.
5. Es sollte überprüft werden, ob die E/A über den Active/Optimized-Pfad erfolgt:

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

6. Den vorherigen LUN-Besitzer und seinen Partnerknoten aus der Reporting-Nodes-Liste entfernen:

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

7. Es sollte überprüft werden, ob die LUN aus der bestehenden LUN-Zuordnung entfernt wurde:

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

8. Alle veralteten Geräteeinträge für das Host-Betriebssystem entfernen.
9. Gegebenenfalls sind die Multipathing-Konfigurationsdateien anzupassen.
10. Den Host erneut scannen, um die Entfernung alter Pfade zu überprüfen. + In der Host-Dokumentation sind spezifische Schritte zum erneuten Scannen der Hosts zu finden.

iSCSI Protokollverwaltung

Konfiguration Ihres Netzwerks für optimale iSCSI Performance in ONTAP

Die Leistung von Ethernet Netzwerken variiert stark. Die Leistung des für iSCSI verwendeten Netzwerks lässt sich durch die Auswahl bestimmter Konfigurationswerte maximieren.

Schritte

1. Die Host- und Speicheranschlüsse sind mit demselben Netzwerk verbunden.

   Am besten wird eine Verbindung zu denselben Switches hergestellt. Routing sollte niemals verwendet werden.

2. Die schnellsten verfügbaren Ports sollten ausgewählt und für iSCSI reserviert werden.

   10 GbE-Ports sind optimal. 1 GbE-Ports sind das Minimum.

3. Die Ethernet-Flusssteuerung ist für alle Ports zu deaktivieren.

   Es sollte "Netzwerkmanagement" für die Verwendung der CLI zur Konfiguration der Ethernet-Port-Flusssteuerung angezeigt werden.

4. Jumbo Frames aktivieren (typischerweise MTU von 9000).

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

Konfiguration einer ONTAP SVM für iSCSI

Um eine Storage Virtual Machine (SVM) für iSCSI zu konfigurieren, müssen LIFs für die SVM erstellt und diesen LIFs das iSCSI-Protokoll zugewiesen werden.

Über diese Aufgabe

- Sie benötigen mindestens eine iSCSI-LIF pro Knoten für jede SVM, die Daten mit dem iSCSI-Protokoll bereitstellt. Für Redundanz empfiehlt es sich, mindestens zwei LIFs pro Knoten zu erstellen.

- Ab ONTAP 9.19.1 unterstützen AFF-Systeme Aktiv/Aktiv-Multipathing mit automatischem LIF-Failover auf SVM-Ebene in SAN-Umgebungen. Sie müssen Aktiv/Aktiv-Multipathing auf AFF-Systemen aktivieren, wenn Sie die SVM erstmals erstellen.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Beispiel 7. Schritte

System Manager

Eine Storage-VM für iSCSI mit ONTAP System Manager (9.7 und höher) konfigurieren.

iSCSI auf einer neuen Storage-VM konfigurieren	iSCSI auf einer vorhandenen Storage-VM konfigurieren
1. Im System Manager wählen Sie **Storage > Storage VMs** und anschließend **Add**. 2. Geben Sie einen Namen für die Storage-VM ein. 3. **iSCSI** für das **Zugriffsprotokoll** auswählen. 4. Wählen Sie **iSCSI aktivieren** und geben Sie die IP-Adresse und Subnetzmaske für die logische Schnittstelle ein. Jeder Knoten sollte über mindestens zwei Netzwerkschnittstellen verfügen. 5. Wenn Sie möchten, dass Netzwerkpfade im Falle eines Knotenausfalls automatisch auf den HA-Partner umgeschaltet werden, gehen Sie wie folgt vor: Diese Option ist in ONTAP 9.19.1 und späteren Versionen nur auf AFF- und ASA-Systemen verfügbar. ◦ Wählen Sie für AFF-Systeme **Symmetrisches Aktiv/Aktiv-Multipathing** und anschließend **Symmetrisches Aktiv/Aktiv-Multipathing aktivieren**. ◦ Wählen Sie für ASA-Systeme **Symmetrisches Aktiv/Aktiv-Multipathing** und anschließend **Aktivieren für SCSI- und NVMe-Protokolle**. 6. **Speichern** auswählen.	1. Im System Manager unter **Storage > Storage-VMs** auswählen. 2. Wählen Sie die Storage-VM aus, die Sie konfigurieren möchten. 3. Wählen Sie auf der Registerkarte **Einstellungen** aus und dann ⚙ neben dem iSCSI-Protokoll. 4. Wählen Sie **iSCSI aktivieren** und geben Sie die IP-Adresse und Subnetzmaske für die logische Schnittstelle ein. + Jeder Knoten sollte mindestens zwei logische Schnittstellen besitzen. 5. **Speichern** auswählen.

CLI

Eine Storage-VM für iSCSI mit der ONTAP CLI konfigurieren.

1. Die SVMs werden so konfiguriert, dass sie iSCSI-Datenverkehr empfangen:

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

2. Eine LIF für die SVMs auf jedem Knoten erstellen, die für iSCSI verwendet wird:
   - 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 frühere Versionen:

     ```
     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. Überprüfung, ob die LIFs korrekt eingerichtet wurden:

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

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

4. Es sollte sichergestellt werden, dass iSCSI betriebsbereit ist und der Ziel-IQN für diese SVM vorhanden ist:

   ```
   vserver iscsi show –vserver vserver_name
   ```

5. Vom Host aus werden iSCSI-Sitzungen zu den LIFs erstellt.

Verwandte Informationen

- "NetApp Technischer Bericht 4080: Bewährte Verfahren für moderne SAN"

Definition einer ONTAP Sicherheitsrichtlinienmethode für einen Initiator

Sie können eine Liste von Initiatoren und deren Authentifizierungsverfahren definieren. Es ist außerdem möglich, das Standard-Authentifizierungsverfahren zu ändern, das für Initiatoren gilt, die kein benutzerdefiniertes Authentifizierungsverfahren haben.

Über diese Aufgabe

Sie können mithilfe der im Produkt integrierten Sicherheitsrichtlinienalgorithmen eindeutige Passwörter generieren oder die gewünschten Passwörter manuell angeben.

Nicht alle Initiatoren unterstützen hexadezimale CHAP-Geheimpasswörter.

Schritte

1. Mit dem `vserver iscsi security create` Befehl lässt sich eine Sicherheitsrichtlinienmethode für einen Initiator erstellen.

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

2. Folgen Sie den Anweisungen auf dem Bildschirm, um die Passwörter hinzuzufügen.

Erstellt ein Sicherheitsrichtlinienverfahren für den Initiator iqn.1991-05.com.microsoft:host1 mit eingehenden und ausgehenden CHAP-Benutzernamen und -Kennwörtern.

Verwandte Informationen

- Wie die iSCSI-Authentifizierung funktioniert
- CHAP-Authentifizierung

Löschen eines iSCSI-Service von einer ONTAP SVM

Ein iSCSI-Service für eine Storage Virtual Machine (SVM) kann gelöscht werden, wenn er nicht mehr benötigt wird.

Bevor Sie beginnen

Der Administrationsstatus des iSCSI-Service muss sich im Zustand „down“ befinden, bevor ein iSCSI-Service gelöscht werden kann. Der Administrationsstatus kann mit dem `vserver iscsi modify` Befehl auf „down“ gesetzt werden.

Schritte

1. Der `vserver iscsi modify`-Befehl kann verwendet werden, um die I/O zur LUN zu stoppen.

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

2. Mit dem `vserver iscsi delete`Befehl lässt sich der iSCSI-Service aus der SVM entfernen.

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

3. Verwenden Sie den `vserver iscsi show command`, um zu überprüfen, ob der iSCSI-Service von der SVM gelöscht wurde.

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

Weitere Details zu iSCSI-Sitzungsfehlerbehebungen

Durch Erhöhen des Fehlerwiederherstellungslevels für iSCSI-Sitzungen werden detailliertere Informationen zu iSCSI-Fehlerbehebungen bereitgestellt. Die Verwendung eines höheren Fehlerwiederherstellungslevels kann zu einer geringfügigen Reduzierung der iSCSI-Sitzungsleistung führen.

Über diese Aufgabe

ONTAP ist standardmäßig so konfiguriert, dass für iSCSI-Sitzungen die Fehlerbehebungsstufe 0 verwendet wird. Wenn ein Initiator verwendet wird, der für Fehlerbehebungsstufe 1 oder 2 qualifiziert ist, besteht die Möglichkeit, die Fehlerbehebungsstufe zu erhöhen. Die geänderte Fehlerbehebungsstufe für die Sitzung betrifft nur neu erstellte Sitzungen und hat keine Auswirkungen auf bestehende Sitzungen.

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

Schritte

1. Erweiterter Modus:

   ```
   set -privilege advanced
   ```

2. Die aktuelle Einstellung lässt sich mit dem `iscsi show` Befehl überprüfen.

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

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

3. Der Fehlerbehandlungsgrad kann mit dem `iscsi modify` Befehl geändert werden.

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

Registrierung einer ONTAP SVM bei einem iSNS-Server

Der `vserver iscsi isns` Befehl kann verwendet werden, um die Storage Virtual Machine (SVM) so zu konfigurieren, dass sie sich bei einem iSNS-Server registriert.

Über diese Aufgabe

Der `vserver iscsi isns create` Befehl konfiguriert die SVM so, dass sie sich beim iSNS-Server registriert. Die SVM stellt keine Befehle zur Verfügung, mit denen sich der iSNS-Server konfigurieren oder verwalten lässt. Für die Verwaltung des iSNS-Servers stehen die Server-Administrationstools oder die vom Anbieter für den iSNS-Server bereitgestellte Schnittstelle zur Verfügung.

Schritte

1. Auf Ihrem iSNS-Server muss sichergestellt sein, dass Ihr iSNS-Service aktiv und betriebsbereit ist.
2. Die SVM-Management-LIF auf einem Datenport erstellen:

   ```
   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
   ```

   Weitere Informationen zu `network interface create` finden sich in der "ONTAP-Befehlsreferenz".

3. Ein iSCSI-Service auf Ihrer SVM ist zu erstellen, falls noch keiner vorhanden ist:

   ```
   vserver iscsi create -vserver SVM_name
   ```

4. Es sollte überprüft werden, ob der iSCSI-Service erfolgreich erstellt wurde:

   ```
   iscsi show -vserver SVM_name
   ```

5. Es sollte überprüft werden, ob für die SVM eine Standardroute existiert:

   ```
   network route show -vserver SVM_name
   ```

6. Falls für die SVM keine Standardroute existiert, kann eine Standardroute erstellt werden:

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

Weitere Informationen zu `network route create` finden sich in der "ONTAP-Befehlsreferenz".

7. Die SVM wird für die Registrierung beim iSNS-Service konfiguriert:

   `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 des SVM-Management-LIF übereinstimmen.

   Beispielsweise ist es nicht möglich, eine SVM Management-LIF mit einer IPv4-Adresse mit einem iSNS-Server mit einer IPv6-Adresse zu verbinden.

8. Es sollte überprüft werden, ob der iSNS-Service läuft:

   `vserver iscsi isns show -vserver SVM_name`

9. Falls der iSNS-Service nicht läuft, sollte er gestartet werden:

   `vserver iscsi isns start -vserver SVM_name`

iSCSI-Fehlermeldungen und deren Behebung in ONTAP

Es gibt eine Reihe häufiger iSCSI-bezogener Fehlermeldungen, die mit dem `event log show` Befehl angezeigt werden können. Es ist erforderlich zu wissen, was diese Meldungen bedeuten und welche Möglichkeiten zur Behebung der darin identifizierten Probleme bestehen.

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

Nachricht	Erläuterung	Was zu tun ist
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	Der iSCSI-Service ist auf der Schnittstelle nicht aktiviert.	Der `iscsi interface enable` Befehl kann verwendet werden, um den iSCSI-Service auf der Schnittstelle zu aktivieren. Beispiel: `iscsi interface enable -vserver vs1 -lif lif1`

Nachricht	Erläuterung	Was zu tun ist
`ISCSI: Authentication failed for initiator nodename`	CHAP ist für den angegebenen Initiator nicht korrekt konfiguriert.	Die CHAP-Einstellungen sind zu überprüfen; es ist nicht möglich, denselben Benutzernamen und dasselbe Passwort für eingehende und ausgehende Einstellungen im Speichersystem zu verwenden: • Die eingehenden Anmeldeinformationen auf dem Speichersystem müssen mit den ausgehenden Anmeldeinformationen auf dem Initiator übereinstimmen. • Die ausgehenden Anmeldeinformationen auf dem Speichersystem müssen mit den eingehenden Anmeldeinformationen auf dem Initiator übereinstimmen.

Weitere Informationen zu `event log show` finden sich in der "ONTAP-Befehlsreferenz".

Aktivierung oder Deaktivierung des automatischen iSCSI LIF Failover in ONTAP

Nach dem Upgrade auf ONTAP 9.11.1 oder höher sollte das automatische LIF-Failover auf allen iSCSI-LIFs, die in ONTAP 9.10.1 oder früher erstellt wurden, manuell aktiviert werden.

Ab ONTAP 9.11.1 kann das automatische LIF-Failover für iSCSI LIFs auf All-flash SAN Array Plattformen aktiviert werden. Wenn ein Storage-Failover auftritt, wird die iSCSI LIF automatisch von ihrem Heimatknoten oder -port auf den HA-Partnerknoten oder -port migriert und nach Abschluss des Failovers wieder zurückmigriert. Oder wenn der Port für die iSCSI LIF fehlerhaft wird, wird die LIF automatisch auf einen funktionsfähigen Port ihres aktuellen Heimatknotens migriert und nach Wiederherstellung des Ports wieder auf ihren ursprünglichen Port zurückmigriert. Dadurch können SAN-Workloads, die auf iSCSI laufen, den I/O-Service nach einem Failover schneller wieder aufnehmen.

In ONTAP 9.11.1 und später ist die automatische LIF-Failover-Funktion für neu erstellte iSCSI-LIFs standardmäßig aktiviert, wenn eine der folgenden Bedingungen zutrifft:

- Auf der SVM sind keine iSCSI LIFs vorhanden.
- Alle iSCSI LIFs auf der SVM sind für automatisches LIF-Failover aktiviert.

Automatisches iSCSI LIF-Failover aktivieren

Standardmäßig ist für iSCSI-LIFs, die in ONTAP 9.10.1 und früher erstellt wurden, kein automatisches LIF-Failover aktiviert. Wenn auf der SVM iSCSI-LIFs vorhanden sind, für die kein automatisches LIF-Failover aktiviert ist, werden auch neu erstellte LIFs nicht für automatisches LIF-Failover aktiviert. Wenn das automatische LIF-Failover nicht aktiviert ist und ein Failover-Ereignis auftritt, migrieren Ihre iSCSI-LIFs nicht.

Weitere Informationen zu "LIF-Failover und Giveback".

Schritt

1. Automatisches Failover für eine iSCSI-LIF aktivieren:

```
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, sollte `-lif*` anstelle von `lif` verwendet werden.

Automatisches iSCSI LIF-Failover deaktivieren

Wenn zuvor das automatische iSCSI LIF-Failover für iSCSI LIFs aktiviert wurde, die in ONTAP 9.10.1 oder früher erstellt wurden, besteht die Möglichkeit, es zu deaktivieren.

Schritt

1. Automatisches Failover für eine iSCSI-LIF deaktivieren:

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

Um alle iSCSI LIFs auf der SVM zu aktualisieren, sollte `-lif*` anstelle von `lif` verwendet werden.

Verwandte Informationen

- "Eine LIF erstellen"
- Manuell "eine LIF migrieren"
- Manuell "einen LIF auf seinen Home-Port zurücksetzen"
- "Failover-Einstellungen auf einem LIF konfigurieren"

FC-Protokoll verwalten

Konfiguration einer ONTAP SVM für FC

Um eine Storage Virtual Machine (SVM) für FC zu konfigurieren, müssen LIFs für die SVM erstellt und diesen LIFs das FC-Protokoll zugewiesen werden.

Über diese Aufgabe

NetApp unterstützt mindestens ein FC-LIF pro Knoten für jede SVM, die Daten mit dem FC-Protokoll bereitstellt. Es sind zwei LIFs pro Knoten und zwei Fabrics zu verwenden, wobei jedem Knoten ein LIF zugeordnet ist. Dadurch entsteht Redundanz auf der Knotenebene und im Fabric.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Sie benötigen eine FC-Lizenz ("im Lieferumfang von ONTAP One enthalten") und diese muss aktiviert sein. Ist die FC-Lizenz nicht aktiviert, werden die LIFs und SVMs zwar als online angezeigt, aber der Betriebsstatus ist `down`. Der FC-Dienst muss aktiviert sein, damit Ihre LIFs und SVMs betriebsbereit sind. Für alle FC LIFs in der SVM ist Single Initiator Zoning zu verwenden, um die Initiatoren zu hosten.

Beispiel 8. Schritte

System Manager

Eine Storage-VM für iSCSI mit ONTAP System Manager (9.7 und höher) konfigurieren.

FC auf einer neuen Storage-VM konfigurieren	FC auf einer vorhandenen Storage-VM konfigurieren
1. Im System Manager wählen Sie **Storage > Storage VMs** und anschließend **Add**. 2. Geben Sie einen Namen für die Storage-VM ein. 3. **FC** für das **Zugriffsprotokoll** auswählen. 4. Wählen Sie **FC aktivieren**. Die FC-Ports werden automatisch zugewiesen. 5. **Speichern** auswählen.	1. Im System Manager unter **Storage > Storage-VMs** auswählen. 2. Wählen Sie die Storage-VM aus, die Sie konfigurieren möchten. 3. Wählen Sie auf der Registerkarte **Einstellungen** und anschließend ⚙ neben dem FC-Protokoll aus. 4. Wählen Sie **FC aktivieren** und geben Sie die IP-Adresse und Subnetzmaske für die Netzwerkschnittstelle ein. + Die FC-Ports werden automatisch zugewiesen. 5. **Speichern** auswählen.

CLI

1. FC-Dienst auf der SVM aktivieren:

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

2. Zwei LIFs für die SVMs auf jedem Knoten, der FC bereitstellt, erstellen.
   - 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 frühere Versionen:

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

3. Es wird überprüft, ob Ihre LIFs erstellt wurden und ob ihr Betriebsstatus `online` ist:

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

Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

"Erfahren Sie mehr über ONTAP LIFs für SAN-Umgebungen".

Löschen eines FC-Dienstes von einer ONTAP SVM

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

Bevor Sie beginnen

Der Administrationsstatus muss „down“ sein, bevor ein FC-Service für eine SVM gelöscht werden kann. Der Administrationsstatus kann mit dem `vserver fcp modify` Befehl oder dem `vserver fcp stop` Befehl auf „down“ gesetzt werden.

Schritte

1. Der `vserver fcp stop`-Befehl kann verwendet werden, um die I/O zur LUN zu stoppen.

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

2. Mit dem `vserver fcp delete`Befehl lässt sich der Dienst aus der SVM entfernen.

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

3. Verwenden Sie das `vserver fcp show`, um zu überprüfen, ob der FC-Service von Ihrer SVM entfernt wurde:

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

Empfohlene MTU-Konfigurationen für FCoE-Jumbo-Frames in ONTAP

Für Fibre Channel over Ethernet (FCoE) sollten Jumbo-Frames für den Ethernet-Adapter des CNA mit einer MTU von 9000 konfiguriert werden. Jumbo-Frames für den FCoE-Adapter des CNA sollten mit einer MTU von mehr als 1500 konfiguriert werden. Jumbo-Frames sollten nur konfiguriert werden, wenn Initiator, Ziel und alle dazwischenliegenden Switches Jumbo-Frames unterstützen und entsprechend konfiguriert sind.

NVMe-Protokoll verwalten

Start des NVMe-Service für eine ONTAP SVM

Bevor Sie das NVMe-Protokoll auf Ihrer Storage Virtual Machine (SVM) verwenden können, muss der NVMe-Dienst auf der SVM gestartet werden.

Bevor Sie beginnen

NVMe muss als Protokoll auf Ihrem System zugelassen sein.

Folgende NVMe-Protokolle werden unterstützt:

Protokoll	Ab Version …	Erlaubt durch…
TCP	ONTAP 9.10.1	Standard
FCP	ONTAP 9.4	Standard

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. Es sollte überprüft werden, ob NVMe als Protokoll zulässig ist:

   ```
   vserver nvme show
   ```

3. Den NVMe-Protokolldienst erstellen:

   ```
   vserver nvme create
   ```

4. Der NVMe-Protokolldienst auf der SVM wird gestartet:

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

NVMe-Service von einer ONTAP SVM löschen

Bei Bedarf kann der NVMe-Service von Ihrer Storage Virtual Machine (SVM) entfernt werden.

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. Den NVMe-Service auf der SVM beenden:

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

3. Der NVMe-Dienst wird gelöscht:

   ```
   vserver nvme delete
   ```

Größenänderung eines ONTAP NVMe Namespace

Ab ONTAP 9.10.1 kann die Größe eines NVMe Namespace über die ONTAP Befehlszeile (CLI) erhöht oder verringert werden. Mit dem System Manager kann die Größe eines NVMe Namespace erhöht werden.

Die Größe eines Namespace vergrößern

System Manager

1. **Speicher > NVMe Namespaces** auswählen.

2. Fahren Sie mit dem Mauszeiger über den Namespace, den Sie vergrößern möchten, klicken Sie auf ⋮ und anschließend auf **Bearbeiten**.
3. Unter **CAPACITY** die Größe des Namensraums ändern.

CLI

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

Die Größe eines Namensraums verringern

Die ONTAP CLI muss verwendet werden, um die Größe eines NVMe Namespace zu verringern.

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set –privilege advanced
   ```

2. Die Größe des Namensraums verringern:

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

Konvertierung eines NVMe-Namespace in eine ONTAP LUN

Ab ONTAP 9.11.1 kann die ONTAP CLI verwendet werden, um einen vorhandenen NVMe Namespace direkt in eine LUN zu konvertieren.

Bevor Sie beginnen

- Der angegebene NVMe Namespace sollte keine bestehenden Zuordnungen zu einem Subsystem haben.
- Der Namespace sollte weder Teil eines Snapshots sein noch auf der Zielseite der SnapMirror Beziehung als schreibgeschützter Namespace vorliegen.
- Da NVMe-Namespaces nur von bestimmten Plattformen und Netzwerkkarten unterstützt werden, funktioniert diese Funktion nur mit bestimmter 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
   ```

   Weitere Informationen zu `lun convert-from-namespace` finden sich in der "ONTAP-Befehlsreferenz".

Einrichten der In-Band-Authentifizierung über NVMe in ONTAP

Ab ONTAP 9.12.1 kann die ONTAP Befehlszeilenschnittstelle (CLI) verwendet werden, um die In-Band-Authentifizierung (sicher), bidirektionale und unidirektionale Authentifizierung zwischen einem NVMe-Host und einem Controller über die Protokolle NVMe/TCP und NVMe/FC mittels DH-HMAC-CHAP Authentifizierung zu konfigurieren. Ab ONTAP 9.14.1 kann die In-Band-Authentifizierung im System Manager konfiguriert werden.

Um die In-Band-Authentifizierung einzurichten, muss jedem Host oder Controller ein DH-HMAC-CHAP-Schlüssel zugeordnet werden, der eine Kombination aus dem NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsgeheimnis ist. 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, aber nicht für den Controller konfiguriert. Bei der bidirektionalen Authentifizierung wird ein geheimer Schlüssel sowohl für den Host als auch für den Controller konfiguriert.

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

System Manager

Ab ONTAP 9.14.1 kann mit dem System Manager die In-Band-Authentifizierung beim Erstellen oder Aktualisieren eines NVMe-Subsystems, beim Erstellen oder Klonen von NVMe-Namespaces oder beim Hinzufügen von Konsistenzgruppen mit neuen NVMe-Namespaces konfiguriert werden.

Schritte

1. Im System Manager auf **Hosts > NVMe Subsystem** und dann auf **Hinzufügen** klicken.
2. Den Namen des NVMe-Subsystems hinzufügen sowie die Storage-VM und das Host-Betriebssystem auswählen.
3. Geben Sie den Host NQN ein.
4. Neben dem Host-NQN ist **In-Band-Authentifizierung verwenden** auszuwählen.
5. Das Host-Geheimnis und das Controller-Geheimnis angeben.

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

6. Die bevorzugte Hash-Funktion und DH-Gruppe für jeden Host auswählen.

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

7. Optional auf **Hinzufügen** klicken und die Schritte nach Bedarf wiederholen, um weitere Hosts hinzuzufügen.
8. Auf **Speichern** klicken.
9. Zur Überprüfung, ob die In-Band Authentifizierung aktiviert ist, **System Manager > Hosts > NVMe Subsystem > Grid > Peek view** auswählen.

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

CLI

Schritte

1. DH-HMAC-CHAP-Authentifizierung zum NVMe-Subsystem hinzufügen:

```
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>
```

Weitere Informationen zu `vserver nvme subsystem host add` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sollte überprüft werden, ob das DH-HMAC CHAP Authentifizierungsprotokoll zu Ihrem Host hinzugefügt wurde:

```
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
```

Weitere Informationen zu `vserver nvme subsystem host show` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob die DH-HMAC CHAP Authentifizierung während der Erstellung des NVMe Controllers erfolgt ist:

```
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 show"

Deaktivieren der In-Band-Authentifizierung über NVMe in ONTAP

Wenn Sie die In-Band-Authentifizierung über NVMe mit DH-HMAC-CHAP konfiguriert haben, kann sie jederzeit deaktiviert werden.

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

Schritte

1. Den Host aus dem Subsystem entfernen, um die DH-HMAC-CHAP Authentifizierung zu deaktivieren:

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

2. Es sollte überprüft werden, ob das DH-HMAC-CHAP Authentifizierungsprotokoll vom Host entfernt ist:

```
vserver nvme subsystem host show
```

3. Den Host ohne Authentifizierung wieder dem Subsystem hinzufügen:

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

Einrichten eines TLS-sicheren Kanals für NVMe/TCP in ONTAP

Ab ONTAP 9.16.1 ist die Konfiguration eines sicheren TLS-Kanals für NVMe/TCP-Verbindungen möglich. System Manager oder die ONTAP CLI können verwendet werden, um entweder ein neues NVMe-Subsystem mit aktiviertem TLS hinzuzufügen oder TLS für ein bestehendes NVMe-Subsystem zu aktivieren. Ab ONTAP 9.19.1 wird TLS Hardware Offload unterstützt.

System Manager

Ab ONTAP 9.16.1 kann mit System Manager TLS für NVMe/TCP-Verbindungen konfiguriert werden, wenn ein NVMe-Subsystem erstellt oder aktualisiert, NVMe-Namespaces erstellt oder geklont oder Konsistenzgruppen mit neuen NVMe-Namespaces hinzugefügt werden.

Schritte

1. Im System Manager auf **Hosts > NVMe Subsystem** und dann auf **Hinzufügen** klicken.
2. Den Namen des NVMe-Subsystems hinzufügen sowie die Storage-VM und das Host-Betriebssystem auswählen.
3. Geben Sie den Host NQN ein.
4. Neben dem Host-NQN ist **Transport Layer Security (TLS) erforderlich** auszuwählen.
5. Den vorab geteilten Schlüssel (PSK) angeben.

6. Auf **Speichern** klicken.
7. Zur Überprüfung, ob der sichere TLS-Kanal aktiviert ist, **System Manager > Hosts > NVMe Subsystem > Grid > Peek view** auswählen.

CLI

Schritte

1. Einen NVMe-Subsystem-Host hinzufügen, der TLS Secure Channel unterstützt. Ein vorab geteilter Schlüssel (PSK) kann mit dem `tls-configured-psk` Argument bereitgestellt werden.

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Es sollte überprüft werden, ob der NVMe-Subsystem-Host für den sicheren TLS-Kanal konfiguriert ist. Optional kann das `tls-key-type` Argument verwendet werden, 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. Es sollte überprüft werden, ob der Hostcontroller des NVMe-Subsystems für einen sicheren TLS-Kanal konfiguriert ist. Optional können die Argumente `tls-key-type`, `tls-identity` oder `tls-cipher` verwendet werden, um nur die Controller anzuzeigen, die diese TLS-Attribute aufweisen.

```
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

- "vserver nvme Subsystem"
- "TLS-Hardware-Offload konfigurieren"

TLS sicheren Kanal für NVMe/TCP in ONTAP deaktivieren

Ab ONTAP 9.16.1 kann ein TLS-Sicherheitskanal für NVMe/TCP-Verbindungen konfiguriert werden. Wenn ein TLS-Sicherheitskanal für NVMe/TCP-Verbindungen konfiguriert wurde, besteht jederzeit die Möglichkeit, ihn zu deaktivieren.

Schritte

1. Entfernen Sie den Host aus dem Subsystem, um den sicheren TLS-Kanal zu deaktivieren:

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

2. Es sollte überprüft werden, ob der sichere TLS-Kanal vom Host entfernt wurde:

```
vserver nvme subsystem host show
```

3. Den Host ohne sicheren TLS-Kanal wieder zum Subsystem hinzufügen:

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

Verwandte Informationen

- "vserver nvme subsystem host"

Ändern der NVMe Hostpriorität in ONTAP

Ab ONTAP 9.14.1 kann das NVMe-Subsystem so konfiguriert werden, dass die Ressourcenzuweisung für bestimmte Hosts priorisiert wird. Standardmäßig wird einem Host, der dem Subsystem hinzugefügt wird, eine reguläre Priorität zugewiesen. Hosts mit hoher Priorität werden größere I/O-Warteschlangenzahlen und Warteschlangentiefen zugewiesen.

Die Standardpriorität kann über die ONTAP command line interface (CLI) manuell von Normal auf Hoch geändert werden. Um die einem Host zugewiesene Priorität zu ändern, ist es erforderlich, den Host aus dem Subsystem zu entfernen und anschließend wieder hinzuzufügen.

Schritte

1. Es sollte überprüft werden, ob die Hostpriorität auf „regulär“ gesetzt ist:

```
vserver nvme show-host-priority
```

   Weitere Informationen zu `vserver nvme show-host-priority` finden sich in der "ONTAP-Befehlsreferenz".

2. Den Host aus dem Subsystem entfernen:

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

   Weitere Informationen zu `vserver nvme subsystem host remove` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob der Host aus dem Subsystem entfernt wurde:

```
vserver nvme subsystem host show
```

Weitere Informationen zu `vserver nvme subsystem host show` finden sich in der "ONTAP-Befehlsreferenz".

4. Den Host mit hoher Priorität wieder dem Subsystem hinzufügen:

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

Weitere Informationen zu `vserver nvme subsystem host add` finden sich in der "ONTAP-Befehlsreferenz".

Automatische Host-Erkennung von NVMe/TCP-Controllern in ONTAP verwalten

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 ermöglichen

Falls die automatische Host-Erkennung zuvor deaktiviert wurde, sich die Anforderungen jedoch geändert haben, kann sie wieder aktiviert werden.

Schritte

1. Erweiterten Berechtigungsmodus aktivieren:

```
set -privilege advanced
```

2. Automatische Erkennung:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Es wird überprüft, ob die automatische Erkennung von NVMe/TCP Controllern aktiviert ist.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Automatische Erkennung von NVMe/TCP-Controllern auf Hosts deaktivieren

Wenn es nicht erforderlich ist, dass NVMe/TCP Controller von Ihrem Host automatisch erkannt werden und unerwünschter Multicast-Verkehr in Ihrem Netzwerk festgestellt wird, empfiehlt sich das Deaktivieren dieser Funktionalität.

Schritte

1. Erweiterten Berechtigungsmodus aktivieren:

```
set -privilege advanced
```

2. Automatische Erkennung deaktivieren:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Es wird überprüft, ob die automatische Erkennung von NVMe/TCP Controllern deaktiviert ist.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

NVMe-Host-VM-Kennung in ONTAP deaktivieren

Ab ONTAP 9.14.1 unterstützt ONTAP standardmäßig die Möglichkeit von NVMe/FC-Hosts, virtuelle Maschinen anhand einer eindeutigen Kennung zu identifizieren und für NVMe/FC-Hosts, die Ressourcenauslastung virtueller Maschinen zu überwachen. Dies verbessert die Berichterstellung und Fehlerbehebung auf Host-Seite.

Sie können das Bootargument verwenden, um diese Funktionalität zu deaktivieren. Siehe "NetApp Knowledge Base: Wie die NVMe-Host-VM-Kennung in ONTAP deaktiviert wird".

Systeme mit FC Adaptern verwalten

Management von FC Adaptern in ONTAP

Es stehen Befehle zur Verfügung, um die integrierten FC-Adapter und FC-Adapterkarten zu verwalten. Diese Befehle können verwendet werden, um den Adaptermodus zu konfigurieren, Adapterinformationen anzuzeigen und die Geschwindigkeit zu ändern.

Die meisten Speichersysteme verfügen über integrierte FC-Adapter, die als Initiatoren oder Targets konfiguriert werden können. Es können auch FC-Adapterkarten verwendet werden, die als Initiatoren oder Targets konfiguriert sind. Initiatoren verbinden sich mit Back-End-Disk-Shelfs und gegebenenfalls mit fremden Storage-Arrays. Targets verbinden sich ausschließlich mit FC-Switches. Sowohl die FC-Target-HBA-Ports als auch die Switch-Port-Geschwindigkeit sollten auf denselben Wert eingestellt werden und nicht auf Auto gesetzt sein.

Verwandte Informationen

"SAN-Konfiguration"

Befehle zur Verwaltung von FC-Adaptern in ONTAP

Sie können FC-Befehle verwenden, um FC-Zieladapter, FC-Initiatoradapter und Onboard FC-Adapter Ihres Speicherkontrollers zu verwalten. Dieselben Befehle werden zur Verwaltung von FC-Adaptern für das FC-Protokoll und das FC-NVMe-Protokoll verwendet.

Die Befehle des FC-Initiator-Adapters funktionieren nur auf Knotenebene. Der `run -node` *`node_name`*

Befehl muss verwendet werden, bevor die Befehle des FC-Initiator-Adapters verwendet werden können.

Befehle zur Verwaltung von FC Zieladaptern

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
FC-Adapterinformationen auf einem Node anzeigen	`network fcp adapter show`
FC Zieladapter-Parameter ändern	`network fcp adapter modify`
FC-Protokoll-Verkehrsinformationen	`run -node node_name sysstat -f`
Anzeigen, wie lange das FC-Protokoll bereits läuft	`run -node node_name uptime`
Konfiguration und Status des Grafikadapters	`run -node node_name sysconfig -v adapter`
Es wird geprüft, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen.	`run -node node_name sysconfig -ac`
Eine Manpage für einen Befehl anzeigen	`man <command_name>`

Befehle zur Verwaltung von FC Initiatoradaptern

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Informationen für alle Initiatoren und ihre Adapter in einem Knoten anzeigen	`run -node node_name storage show adapter`
Konfiguration und Status des Grafikadapters	`run -node node_name sysconfig -v adapter`
Es wird geprüft, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen.	`run -node node_name sysconfig -ac`

Befehle zur Verwaltung der Onboard-FC-Adapter

Wenn Sie möchten…	Verwenden Sie diesen Befehl…
Status der integrierten FC-Ports anzeigen	`run -node node_name system hardware unified-connect show`

Verwandte Informationen

- "Netzwerk FCP Adapter"

Konfiguration von FC-Adaptern in ONTAP

Onboard FC Adapter und einige FC-Erweiterungsadapterkarten können individuell als Initiator- oder Target-Ports konfiguriert werden. Andere FC-Erweiterungsadapter sind im Werk als Initiator- oder Target-Ports 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 verwendet werden, um direkt mit Backend-Disk-Shelves und gegebenenfalls mit fremden Speichersystemen verbunden zu werden. Target-Ports können nur zur Verbindung mit FC-Switches verwendet werden.

Die Anzahl der Onboard-Ports und der für FC konfigurierten CNA/UTA2-Ports variiert je nach Controller-Modell. Auch die unterstützten Zielerweiterungsadapter sind modellabhängig. Siehe "NetApp Hardware Universe" für eine vollständige Liste der Onboard-FC-Ports und der unterstützten Zielerweiterungsadapter für Ihr Controller-Modell.

FC-Adapter für den Initiatormodus konfigurieren

Der Initiatormodus wird verwendet, um die Ports mit Bandlaufwerken, Bandbibliotheken oder Storage von Drittanbietern "Foreign LUN Import (FLI)" zu verbinden.

Bevor Sie beginnen

- Die LIFs auf dem Adapter müssen aus allen Portsets entfernt werden, zu denen sie gehören.
- Alle LIFs aller Storage Virtual Machines (SVMs), die den zu modifizierenden physischen Port verwenden, müssen migriert oder zerstört werden, bevor die Persönlichkeit des physischen Ports von Target auf Initiator geändert wird.

NVMe/FC unterstützt den Initiator-Modus nicht.

Schritte

1. Alle LIFs vom Adapter entfernen:

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. Adapter offline schalten:

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

Wenn der Adapter nicht offline geht, kann das Kabel auch vom entsprechenden Adapterport am System entfernt werden.

3. Den Adapter von Ziel auf Initiator ändern:

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. Der Knoten, auf dem der geänderte Adapter gehostet wird, muss neu gestartet werden.
5. Es sollte sichergestellt werden, dass die FC-Ports für Ihre Konfiguration im richtigen Zustand konfiguriert sind:

```
system hardware unified-connect show
```

6. Den Adapter wieder online bringen:

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

FC-Adapter für den Zielmodus konfigurieren

Der Zielmodus wird verwendet, um die Ports mit FC-Initiatoren zu verbinden.

Die Konfiguration von FC-Adaptern für das FC-Protokoll und das FC-NVMe-Protokoll erfolgt nach denselben Schritten. Allerdings unterstützen nur bestimmte FC-Adapter FC-NVMe. Siehe "NetApp Hardware Universe" für eine Liste der Adapter, die das FC-NVMe-Protokoll unterstützen.

Schritte

1. Den Adapter offline schalten:

   ```
   node run -node _node_name_ storage disable adapter _adapter_name_
   ```

   Wenn der Adapter nicht offline geht, kann das Kabel auch vom entsprechenden Adapterport am System entfernt werden.

2. Den Adapter von Initiator auf Ziel ändern:

   ```
   system node hardware unified-connect modify -t target -node _node_name_
   adapter _adapter_name_
   ```

3. Der Knoten, auf dem der geänderte Adapter gehostet wird, muss neu gestartet werden.
4. Es sollte sichergestellt werden, dass der Zielport die korrekte Konfiguration aufweist:

   ```
   network fcp adapter show -node _node_name_
   ```

5. Adapter online schalten:

   ```
   network fcp adapter modify -node _node_name_ -adapter _adapter_port_
   -status-admin up
   ```

FC-Adapter für den direkten Anschluss an FC- und FC-NVMe-Hosts konfigurieren

Ab ONTAP 9.19.1 ist kein FC-Switch erforderlich, um Verbindungen zwischen FC- und FC-NVMe-Hosts und ONTAP Storage herzustellen. Hosts können direkt an FC-Adapterports von AFF, ASA, ASA r2 und FAS Systemen angeschlossen werden. Die Direktanschlussfähigkeit kann besonders an Remote-Standorten und in hybriden Umgebungen wertvoll sein, in denen Einfachheit entscheidend ist. Sie müssen den FC-Port offline nehmen und seine Topologie ändern, bevor er direkt an einen Host angeschlossen werden kann.

Für FC-Ports, die in Direktanschlusskonfigurationen verwendet werden, gelten folgende Einschränkungen:

- Der Port kann nur einer Storage-VM (SVM) zugewiesen werden.
- Nach der Konfiguration des Ports für den direkten Anschluss kann diesem nur eine Netzwerkschnittstelle (LIF) zugewiesen werden.
- Der Port kann entweder das FC-Protokoll oder das FC-NVMe-Protokoll unterstützen, aber nicht beide.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein.

System Manager

1. Im System Manager wählen Sie **Netzwerk > FC ports**.
2. Wählen Sie ⋮ neben dem Port, den Sie für die direkte Verbindung konfigurieren möchten, und wählen Sie dann **Topologie bearbeiten**.
3. Unter **Topologie** wählen Sie **Direkt** und dann **Ich möchte die Topologie ändern und den Port offline nehmen**.
4. Wählen Sie **Speichern** aus.
5. Verbinden Sie das Kabel für den Zielport direkt mit dem Host-Initiator.
6. Wenn Sie ein AFF, ASA oder FAS-System haben, befolgen Sie diese Schritte, um eine LIF zu erstellen: Wenn Sie ein ASA r2-System haben, folgen Sie "dieses System Manager-Verfahren", um eine LIF zu erstellen.
   a. Wählen Sie **Netzwerk > Schnittstellen** und anschließend + Add .
   b. Wählen Sie das FC- oder NVMe/FC-Protokoll.
   c. Benennen Sie die LIF oder übernehmen Sie den von ONTAP generierten Namen.
   d. Wählen Sie den Home-Port aus.
   e. **Speichern** auswählen.

      Der Port wird automatisch online geschaltet, sobald das LIF erstellt wird.

Was kommt als Nächstes?

Im System Manager wählen Sie **Netzwerk > FC ports** und überprüfen Sie anschließend, ob die **Topologie** als **Direct** angezeigt wird.

CLI

1. Vergewissern Sie sich, dass der Port, den Sie für die direkte Verbindung verwenden möchten, die direkte Topologie unterstützt:

```
network fcp adapter show -fields topologies-supported
```

2. Sehen Sie sich den administrativen und betrieblichen Status des für den Adapterport verwendeten LIF an:

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

3. Nehmen Sie die für den Adapterport verwendete LIF offline:

```
network interface modify -vserver <SVM_name> -lif * -home-port
<adapter_port> -status-admin down
```

4. Entfernen Sie alle LIFs vom Adapterport:

```
network interface delete -vserver <SVM_name> -lif * -home-port
<adapter_port>
```

5. Den Adapter offline schalten:

```
network fcp adapter modify -node <node_name> -adapter <adapter_port>
-status-admin down
```

6. Ändern Sie die Adapterport-Topologie auf Direkt:

```
network fcp adapter modify -node <node_name> -adapter <adapter_port>
-topology direct
```

7. Verbinden Sie das Kabel für den Zielport direkt mit dem Host-Initiator.
8. Erstellen einer einzelnen LIF-Schnittstelle:

```
network interface create -vserver <SVM_name> -lif <lif_name> -data
protocol fcp|fcp-nvme -home-node <node_name> -home-port <port_name>
```

   Der Port wird nach der Erstellung der LIF automatisch aktiviert.

9. Überprüfen Sie, ob der Port für die direkte Verbindung konfiguriert ist:

```
network fcp interface show
```

   Die Topologie sollte als direkt angezeigt werden.

Verwandte Informationen

- Informationen dazu "FC- und FC-NVMe-Fabrics und Direktanschlusskonfigurationen".

FC-Adaptergeschwindigkeit konfigurieren

Sie sollten die Zielportgeschwindigkeit Ihres Adapters an die Geschwindigkeit des Geräts anpassen, mit dem er verbunden ist, anstatt die automatische Aushandlung zu verwenden. Ein Port, der auf automatische Aushandlung eingestellt ist, kann nach einer Übernahme/Rückgabe oder einer anderen Unterbrechung länger für die Wiederherstellung der Verbindung benötigen.

Über diese Aufgabe

Da diese Aufgabe alle Storage Virtual Machines (SVMs) und alle LIFs in einem Cluster umfasst, müssen die `-home-port` und `-home-lif` Parameter verwendet werden, um den Umfang dieser Operation einzuschränken. Wenn diese Parameter nicht verwendet werden, gilt die Operation für alle LIFs im Cluster,

was möglicherweise nicht erwünscht ist.

Bevor Sie beginnen

Alle LIFs, die diesen Adapter als ihren Home-Port verwenden, müssen offline sein.

Schritte

1. Alle LIFs dieses Adapters offline schalten:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. Den Adapter offline schalten:

```
network fcp adapter modify -node node1 -adapter 0c -status-admin down
```

   Wenn der Adapter nicht offline geht, kann das Kabel auch vom entsprechenden Adapterport am System entfernt werden.

3. Die maximale Geschwindigkeit für den Portadapter bestimmen:

```
fcp adapter show -instance
```

   Die Adaptergeschwindigkeit kann nicht über die maximale Geschwindigkeit hinaus verändert werden.

4. Adaptergeschwindigkeit ändern:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. Den Adapter online schalten:

```
network fcp adapter modify -node node1 -adapter 0c -status-admin up
```

6. Alle LIFs auf dem Adapter online schalten:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

Verwandte Informationen

- Informationen dazu "Möglichkeiten zur Einschränkung des LUN-Zugriffs mit Portsätzen und Initiatorgruppen".
- Erfahren Sie, wie "Selektives LUN Mapping (SLM)" die Pfade eingeschränkt werden, die für den Zugriff auf die LUNs eines HA-Paares verwendet werden.

Anzeigen der ONTAP FC/UTA-Adaptereinstellungen

Sie können spezifische Befehle verwenden, um Informationen über Ihre FC/UTA-Adapter anzuzeigen.

FC Zieladapter

Schritt

1. Mit dem `network fcp adapter show`Befehl werden Adapterinformationen angezeigt: `network fcp adapter show -instance -node node1 -adapter 0a`

   Die Ausgabe zeigt Systemkonfigurationsinformationen und Adapterinformationen für jeden verwendeten Steckplatz an.

   Weitere Informationen zu `network fcp adapter show` finden sich in der "ONTAP-Befehlsreferenz".

Unified Target Adapter (UTA) X1143A-R6

Schritte

1. Starten Sie Ihren Controller ohne angeschlossene Kabel.
2. Mit dem `system hardware unified-connect show` Befehl lassen sich die Portkonfiguration und die Module anzeigen.
3. Die Portinformationen sollten vor der Konfiguration von CNA und Ports eingesehen werden.

Ändern eines UTA2-Ports des ONTAP Systems vom CNA-Modus in den FC-Modus

Sie sollten den UTA2-Port vom Modus Converged Network Adapter (CNA) in den Modus Fibre Channel (FC) umstellen, um den FC-Initiator- und FC-Zielmodus zu unterstützen. Die Personality sollte vom CNA-Modus auf den FC-Modus geändert werden, wenn das physische Medium geändert werden muss, das den Port mit seinem Netzwerk verbindet.

Schritte

1. Den Adapter offline schalten:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-status-admin down`

2. Portmodus ändern:

   `ucadmin modify -node` *`node_name`* `-adapter` *`adapter_name`* `-mode fcp`

3. Den Knoten neu starten und anschließend den Adapter online schalten:

   `network fcp adapter modify -node` *`node_name`* `-adapter` *`adapter_name`* `-status-admin up`

4. Benachrichtigen Sie Ihren Administrator oder VIF-Manager, damit der Port je nach Bedarf gelöscht oder entfernt wird:

   - Wenn der Port als Home-Port eines LIF verwendet wird, Mitglied einer Schnittstellengruppe (ifgrp) ist oder VLANs hostet, sollte ein Administrator Folgendes tun:

i. Die LIFs verschieben, den Port aus der ifgrp entfernen oder die VLANs löschen.

ii. Der Port kann manuell gelöscht werden, indem der `network port delete` Befehl ausgeführt wird.

Falls der `network port delete` Befehl fehlschlägt, sollte der Administrator die Fehler beheben und dann den Befehl erneut ausführen.

Weitere Informationen zu `network port delete` finden sich in der "ONTAP-Befehlsreferenz".

◦ Wenn der Port nicht als Home-Port eines LIF verwendet wird, kein Mitglied einer ifgrp ist und keine VLANs hostet, sollte der VIF Manager den Port beim Neustart aus seinen Datensätzen entfernen.

Falls der VIF-Manager den Port nicht entfernt, muss der Administrator ihn nach dem Neustart manuell mit dem `network port delete` Befehl 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
```

Weitere Informationen zu `network port show` finden sich in der "ONTAP-Befehlsreferenz".

5. Es sollte überprüft werden, ob das richtige SFP+ installiert ist:

   `network fcp adapter show -instance -node -adapter`

   Für CNA sollte ein 10Gb Ethernet SFP verwendet werden. Für FC sollte entweder ein 8 Gb SFP oder ein 16 Gb SFP verwendet werden, bevor die Konfiguration am Node geändert wird.

   Weitere Informationen zu `network fcp adapter show` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "Netzwerkschnittstelle"

Austausch der optischen Module des CNA/UTA2 Zieladapters auf einem ONTAP System

Die optischen Module des Unified Zieladapter (CNA/UTA2) sind so zu wechseln, dass der für den Adapter ausgewählte Persönlichkeitsmodus unterstützt wird.

Schritte

1. Den aktuell in der Karte verwendeten SFP+ überprüfen. Anschließend den aktuellen SFP+ durch den für die gewünschte Personality (FC oder CNA) geeigneten SFP+ ersetzen.
2. Die vorhandenen optischen Module werden aus dem X1143A-R6 Adapter entfernt.
3. Die passenden Module für den bevorzugten Persönlichkeitsmodus (FC oder CNA) Optiken einsetzen.
4. Es sollte überprüft werden, ob das richtige SFP+ installiert ist:

   ```
   network fcp adapter show -instance -node -adapter
   ```

   Unterstützte SFP+-Module und Cisco-branded Kupferkabel (Twinax) sind im *Hardware Universe* aufgeführt.

Verwandte Informationen

- "NetApp Hardware Universe"
- "network fcp adapter anzeigen"

Unterstützte Portkonfigurationen für X1143A-R6-Adapter in ONTAP

Der FC-Zielmodus ist die Standardkonfiguration für die Ports des X1143A-R6 Adapters. Die Ports dieses Adapters können jedoch entweder als 10-Gb-Ethernet- und FCoE-Ports oder als 16-Gb-FC-Ports konfiguriert werden.

Bei Konfiguration für Ethernet und FCoE unterstützen X1143A-R6 Adapter gleichzeitigen NIC- und FCoE-Zieldatenverkehr über denselben 10-GBE-Port. Bei FC-Konfiguration kann jedes Zwei-Port-Paar, das denselben ASIC nutzt, individuell für den FC-Ziel- oder FC-Initiator-Modus konfiguriert werden. Das bedeutet, dass ein einzelner X1143A-R6 Adapter den FC-Zielmodus auf einem Zwei-Port-Paar und den FC-Initiator-Modus auf einem anderen Zwei-Port-Paar unterstützen kann.

Verwandte Informationen

"NetApp Hardware Universe"

"SAN-Konfiguration"

Konfiguration der einheitlichen Zieladapter-Ports Ihres ONTAP Systems

Um den einheitlichen Zieladapter (X1143A-R6) zu konfigurieren, müssen die beiden benachbarten Ports auf demselben Chip im gleichen Personality-Modus konfiguriert werden.

Schritte

1. Die Ports können nach Bedarf für Fibre Channel (FC) oder Converged Network Adapter (CNA) mit dem `system node hardware unified-connect modify` Befehl konfiguriert werden.
2. Die entsprechenden Kabel für FC oder 10 Gbit/s Ethernet anschließen.
3. Es sollte überprüft werden, ob das richtige SFP+ installiert ist:

`network fcp adapter show -instance -node -adapter`

Für CNA sollte ein 10Gb Ethernet SFP verwendet werden. Für FC sollte abhängig vom angeschlossenen FC-Fabric entweder ein 8-Gb-SFP oder ein 16-Gb-SFP verwendet werden.

Weitere Informationen zu `network fcp adapter show` finden sich in der "ONTAP-Befehlsreferenz".

Vermeidung von Verbindungsverlusten mithilfe des X1133A-R6 Adapters in ONTAP

Ein Verbindungsverlust während eines Portausfalls lässt sich verhindern, wenn das System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfiguriert ist.

Der X1133A-R6 HBA ist ein 4-Port 16-Gb-FC-Adapter, bestehend aus zwei 2-Port-Paaren. Der X1133A-R6 Adapter kann im Target-Modus oder Initiator-Modus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (zum Beispiel Port 1 und Port 2 auf ASIC 1 sowie Port 3 und Port 4 auf ASIC 2). Beide Ports eines einzelnen ASIC müssen im selben Modus betrieben werden, entweder im Target-Modus oder im Initiator-Modus. Tritt ein Fehler bei dem ASIC auf, der ein Paar unterstützt, gehen beide Ports des Paares offline.

Um diesen Verbindungsverlust zu verhindern, wird das System mit redundanten Pfaden zu separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden, konfiguriert.

LIFs für alle SAN-Protokolle verwalten

Erfahren Sie mehr über ONTAP LIFs für SAN-Umgebungen

In Ihrem ONTAP-System befinden sich LUNs und Namensräume in Storage Virtual Machines (SVMs). Netzwerkschnittstellen (LIFs) ermöglichen es Ihren SAN-Clients, eine Verbindung zu einer SVM herzustellen und auf die darin enthaltenen Daten in den LUNs und Namensräumen zuzugreifen.

- Sie sollten für jede Storage Virtual Machine (SVM), die SAN unterstützt, eine Management-LIF konfigurieren.
- Sie können pro Knoten zwei LIFs konfigurieren, eines für jedes Fabric, das mit FC verwendet wird, und für separate Ethernet-Netzwerke für iSCSI.
- Für die Konnektivität wird entweder eine direkte Verbindung oder die Verwendung von Ethernet-Switches unterstützt. Sie müssen LIFs für beide Verbindungsarten konfigurieren.

Lernen Sie "Eine LIF erstellen"

Verwandte Informationen

- "Erfahren Sie mehr über die LIF-Konfiguration"
- "Erfahren Sie mehr über die Unterstützung für automatisches SAN-LIF-Failover".

Konfiguration eines NVMe LIF in ONTAP

Bei der Konfiguration von NVMe LIFs müssen bestimmte Anforderungen erfüllt sein.

Bevor Sie beginnen

NVMe muss vom FC-Adapter unterstützt werden, auf dem die LIF erstellt wird. Unterstützte Adapter sind in

"Hardware Universe" aufgeführt.

Über diese Aufgabe

Ab ONTAP 9.12.1 und höher können zwei NVMe-LIFs pro Knoten auf maximal 12 Knoten konfiguriert werden. In ONTAP 9.11.1 und früher können zwei NVMe-LIFs pro Knoten auf maximal zwei Knoten konfiguriert werden.

Beim Erstellen einer NVMe-LIF gelten die folgenden Regeln:

- NVMe kann das einzige Datenprotokoll auf Daten-LIFs sein.
- Für jede SVM, die SAN unterstützt, sollte eine Management-LIF konfiguriert werden.
- Für ONTAP 9.5 und höher ist eine NVMe LIF auf dem Knoten, der den Namespace enthält, und auf dem HA-Partner des Knotens zu konfigurieren.
- Nur für ONTAP 9.4:
  - NVMe LIFs und Namespaces müssen auf demselben Knoten gehostet werden.
  - Pro SVM kann nur ein NVMe Daten-LIF konfiguriert werden.

Schritte

1. LIF erstellen:

```
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. Es sollte überprüft werden, ob die LIF erstellt wurde:

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

Nach der Erstellung warten NVMe/TCP LIFs auf Port 8009 auf die Erkennung.

Verwandte Informationen

- "Netzwerkschnittstelle"

Entfernen eines ONTAP SAN LIF aus einem Port Set

Wenn sich die LIF, die Sie löschen oder verschieben möchten, in einem Portset befindet, muss die LIF aus dem Portset entfernt werden, bevor die LIF gelöscht oder verschoben werden kann.

Über diese Aufgabe

Schritt 1 der folgenden Vorgehensweise ist nur erforderlich, wenn sich genau eine LIF im Portset befindet. Die letzte LIF in einem Portset kann nicht entfernt werden, wenn das Portset an eine Initiatorgruppe gebunden ist. Andernfalls kann mit Schritt 2 begonnen werden, falls sich mehrere LIFs im Portset befinden.

Schritte

1. Wenn sich nur ein LIF im Port-Set befindet, kann mit dem `lun igroup unbind` Befehl das Port-Set von der Initiatorgruppe getrennt werden.

   > Wenn eine Initiatorgruppe von einem Portsatz getrennt wird, 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
   ```

   Weitere Informationen zu `lun igroup unbind` finden sich in der "ONTAP-Befehlsreferenz".

2. Mit dem `lun portset remove` Befehl lässt sich die LIF aus dem Port-Set entfernen.

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

   Weitere Informationen zu `lun portset remove` finden sich in der "ONTAP-Befehlsreferenz".

Verschieben Sie eine ONTAP SAN LIF

Wenn ein Knoten offline genommen werden muss, können Sie eine SAN LIF verschieben, um deren Konfigurationsinformationen, wie z. B. die WWPN, zu erhalten. Das Verschieben einer LIF erfordert weder eine Neuzonierung Ihres FC-Fabric noch die Erstellung neuer iSCSI-Sitzungen zwischen Cluster-Hosts und der Ziel-Schnittstelle. Sie können SAN LIFs auf jeden beliebigen Knoten im Cluster verschieben, jedoch nicht zwischen Storage Virtual Machines (SVMs).

Sie können eine LIF verschieben, um die folgenden Aktionen unterbrechungsfrei durchzuführen:

- Ersetzen Sie ein HA-Paar eines Clusters durch ein aktualisiertes HA-Paar auf eine Weise, die für Hosts, die auf LUN- oder Namespace-Daten zugreifen, transparent ist
- Upgrade einer Ziel-Interfacekarte
- Die Ressourcen einer Storage Virtual Machine (SVM) von einer Gruppe von Knoten in einem Cluster auf eine andere Gruppe von Knoten im Cluster verschieben

Sie können ein SAN LIF nicht mit dem `network interface move` Befehl verschieben. Um ein SAN LIF zu verschieben, müssen Sie es offline nehmen, auf einen neuen Home-Node oder Port verschieben und dann wieder online schalten. Da ein SAN LIF vor der Verschiebung offline genommen werden muss, muss der Host-Datenverkehr auf Host-Multipathing-Software zurückgreifen, um unterbrechungsfreien Zugriff auf die LUN zu gewährleisten, sodass keine E/A-Unterbrechung auftritt.

Bevor Sie beginnen

Wenn die LIF Mitglied eines Portsets ist, muss die LIF aus dem Portset entfernt worden sein, bevor die LIF auf einen anderen Knoten verschoben werden kann.

Über diese Aufgabe

Der Zielknoten und der physische Port einer LIF, die Sie verschieben möchten, müssen sich im selben FC-Fabric oder Ethernet-Netzwerk befinden. Wenn eine LIF in ein anderes Fabric verschoben wird, das nicht korrekt zoniert ist, oder wenn eine LIF in ein Ethernet-Netzwerk verschoben wird, das keine Verbindung zwischen iSCSI-Initiator und Ziel aufweist, ist die LUN nach der Wiederinbetriebnahme nicht erreichbar.

Schritte

1. Der administrative und operative Status des LIF wird angezeigt:

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

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

2. Den Status des LIF auf `down` (offline) ändern:

```
network interface modify -vserver <SVM_name> -lif <LIF_name> -status
-admin down
```

   Weitere Informationen zu `network interface modify` finden sich in der "ONTAP-Befehlsreferenz".

3. Dem LIF werden ein neuer Knoten und ein neuer Port zugewiesen:

```
network interface modify -vserver <SVM_name> -lif <LIF_name> -home-node
<node_name> -home-port <port_name>
```

4. Den Status des LIF auf `up` (online) ändern:

```
network interface modify -vserver <SVM_name> -lif <LIF_name> -status
-admin up
```

5. Änderungen überprüfen:

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

Löschen einer LIF in einer ONTAP SAN-Umgebung

Bevor Sie eine LIF löschen, sollte sichergestellt sein, 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 Portsets ist, muss die LIF zuerst aus dem Portset entfernt werden, bevor die LIF gelöscht werden kann.

System Manager

Eine LIF mit ONTAP System Manager (9.7 und höher) löschen.

Schritte

1. Im System Manager auf **Netzwerk > Übersicht** klicken und anschließend **Netzwerkschnittstellen** auswählen.

2. Die Storage-VM auswählen, aus der die LIF gelöscht werden soll.
3. Klicken Sie auf ⋮ und wählen Sie **Löschen** aus.

CLI

Eine LIF mit der ONTAP CLI löschen.

Schritte

1. Der Name des LIF und der aktuelle Port, der gelöscht werden soll, können überprüft werden:

   ```
   network interface show –vserver vserver_name
   ```

2. Die LIF löschen:

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

   Weitere Informationen zu `network interface delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Überprüfen, ob die LIF gelöscht wurde:

   ```
   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
   ```

   Weitere Informationen zu `network interface show` finden sich in der "ONTAP-Befehlsreferenz".

SAN LIF Anforderungen für das Hinzufügen von Knoten zu einem ONTAP Cluster

Beim Hinzufügen von Knoten zu einem Cluster sind bestimmte Aspekte zu berücksichtigen.

- Sie müssen gegebenenfalls LIFs auf den neuen Knoten erstellen, bevor Sie LUNs auf diesen neuen Knoten erstellen.
- Diese LIFs sind von den Hosts entsprechend dem Host-Stack und dem Protokoll zu ermitteln.

- Sie müssen LIFs auf den neuen Knoten erstellen, damit LUN- und Volume-Verschiebungen ohne Verwendung des Cluster-Interconnect-Netzwerks möglich sind.

Konfiguration von ONTAP iSCSI LIFs zur Rückgabe des FQDN für die SendTargets-Erkennung

Ab ONTAP 9 können iSCSI LIFs so konfiguriert werden, dass sie einen Fully Qualified Domain Name (FQDN) zurückgeben, wenn ein Host-Betriebssystem eine iSCSI SendTargets Discovery Operation sendet. Die Rückgabe eines FQDN ist hilfreich, wenn sich ein Network Address Translation (NAT) Gerät zwischen dem Host-Betriebssystem und dem Speicherdienst befindet.

Über diese Aufgabe

IP-Adressen auf der einen Seite des NAT-Geräts sind auf der anderen Seite bedeutungslos, aber FQDNs können auf beiden Seiten eine Bedeutung haben.

> Der Interoperabilitätsgrenzwert für den FQDN beträgt auf allen Host-Betriebssystemen 128 Zeichen.

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. iSCSI-LIFs so konfigurieren, dass sie den FQDN zurückgeben:

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   Im folgenden Beispiel sind die iSCSI LIFs so konfiguriert, dass storagehost-005.example.com als FQDN zurückgegeben wird.

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. Es sollte überprüft werden, ob sendtargets der FQDN ist:

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   In diesem Beispiel wird storagehost-005.example.com im Ausgabefeld 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

ONTAP Speicherplatzzuweisung hilft dabei, zu verhindern, dass Ihre LUNs oder NVMe-Namespaces offline genommen werden, wenn der Speicherplatz ausgeht, und ermöglicht es Ihren SAN-Hosts, Speicherplatz zurückzugewinnen.

Die ONTAP Unterstützung für die Speicherplatzzuweisung hängt von Ihrem SAN-Protokoll und Ihrer ONTAP Version ab. Ab ONTAP 9.16.1 ist die Speicherplatzzuweisung für iSCSI, FC und NVMe Protokolle bei neu erstellten LUNs und allen Namespaces standardmäßig aktiviert.

ONTAP Version	Protokolle	Die Speicherplatzzuweisung ist…
9.16.1 oder höher	• iSCSI • FC • NVMe	Standardmäßig für neu erstellte LUNs und alle Namensräume aktiviert
9.15.1	• iSCSI • FC	Standardmäßig für neu erstellte LUNs aktiviert
	NVMe	Nicht unterstützt
9.14.1 und früher	• iSCSI • FC	Standardmäßig für neu erstellte LUNs deaktiviert
	NVMe	Nicht unterstützt

Wenn die Speicherplatzzuweisung aktiviert ist:

- Wenn auf einer LUN oder in einem Namespace der Speicherplatz ausgeht, teilt ONTAP dem Host mit, dass kein freier Speicherplatz für Schreibvorgänge verfügbar ist. Die LUN oder der Namespace bleiben daher online und Lesevorgänge werden weiterhin ausgeführt. Abhängig von der Hostkonfiguration wiederholt der Host entweder die Schreibvorgänge, bis sie erfolgreich sind, oder das Host-Dateisystem wird offline genommen. Schreibvorgänge werden fortgesetzt, sobald wieder freier Speicherplatz für die LUN oder den Namespace verfügbar ist.

  Wenn die Speicherplatzzuweisung nicht aktiviert ist, schlagen bei Erschöpfung des Speicherplatzes einer LUN oder eines Namespace alle E/A-Operationen fehl und die LUN bzw. der Namespace wird offline genommen; das Speicherplatzproblem muss behoben werden, damit der normale Betrieb fortgesetzt werden kann. Ein erneutes Scannen der LUN-Geräte auf dem Host kann ebenfalls erforderlich sein, um Pfade und Geräte wieder in einen betriebsbereiten Zustand zu versetzen.

- Ein Host kann SCSI- oder NVME `UNMAP` (manchmal auch als `TRIM`) Operationen ausführen. UNMAP-Operationen ermöglichen es einem Host, Datenblöcke zu identifizieren, die nicht mehr benötigt werden, weil sie keine gültigen Daten mehr enthalten. Die Identifizierung erfolgt normalerweise nach dem Löschen von Dateien. Das Speichersystem kann diese Datenblöcke dann freigeben, sodass der Speicherplatz anderweitig genutzt werden kann. Diese Freigabe verbessert die Speichereffizienz erheblich, insbesondere bei Dateisystemen mit hohem Datenumsatz.

Bevor Sie beginnen

Die Aktivierung der Speicherplatzzuweisung erfordert eine Hostkonfiguration, die Speicherplatzzuweisungsfehler korrekt behandeln kann, wenn ein Schreibvorgang nicht abgeschlossen werden kann. Die Nutzung von SCSI oder NVME `UNMAP` erfordert eine Konfiguration, die die logische Blockbereitstellung gemäß dem SCSI SBC-3 Standard unterstützt.

Die folgenden Hosts unterstützen derzeit Thin Provisioning, wenn die Speicherplatzzuweisung aktiviert ist:

- 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 später
- Windows

Über diese Aufgabe

Wenn der Cluster auf ONTAP 9.15.1 oder höher aktualisiert wird, bleibt die Einstellung für die Speicherplatzzuweisung für alle LUNs, die vor dem Software-Upgrade erstellt wurden, nach dem Upgrade unabhängig vom Hosttyp unverändert. Wenn beispielsweise eine LUN in ONTAP 9.13.1 für einen VMware Host mit deaktivierter Speicherplatzzuweisung erstellt wurde, 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. Überprüfen, ob die Speicherplatzzuweisung aktiviert ist:

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. Es sollte überprüft werden, ob die Speicherplatzverwaltung auf dem Host-Betriebssystem aktiviert ist.

> Einige Hostkonfigurationen, darunter bestimmte Versionen von VMware ESXi, erkennen die Einstellungsänderung automatisch und erfordern keine Benutzerinteraktion. Andere Konfigurationen erfordern möglicherweise einen erneuten Gerätescan. Manche Dateisysteme und Volume-Manager benötigen möglicherweise zusätzliche spezifische Einstellungen, um die Speicherplatzfreigabe mithilfe von `SCSI UNMAP` zu ermöglichen. Das erneute Einhängen von Dateisystemen oder ein vollständiger Neustart des Betriebssystems kann erforderlich sein. In der Dokumentation des jeweiligen Hosts finden sich entsprechende Hinweise.

Hostkonfiguration für VMware ESXi 8.x und spätere NVMe-Hosts

Wenn Sie einen VMware-Host mit ESXi 8.x oder höher und dem NVMe-Protokoll verwenden, sollten nach der Aktivierung der Speicherplatzzuweisung in ONTAP die folgenden Schritte auf den Hosts durchgeführt werden.

Schritte

1. Auf dem ESXi-Host überprüfen, ob DSM deaktiviert ist:

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

Der Erwartungswert ist 0.

2. NVMe DSM aktivieren:

```
esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
```

3. Es sollte überprüft werden, ob DSM aktiviert ist:

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

Der Erwartungswert ist 1.

Verwandte Links

Weitere Informationen zu "NVMe-oF Hostkonfiguration für ESXi 8.x mit ONTAP".

Empfohlene Kombinationen für Volume- und Datei- oder LUN-Konfigurationen

Informationen zu Volume- und LUN-Konfigurationskombinationen in ONTAP

Es gibt spezifische Kombinationen von FlexVol volume und Datei- oder LUN-Konfigurationen, die je nach Ihren Anwendungs- und Verwaltungsanforderungen verwendet werden können. Das Verständnis der Vorteile und Kosten dieser Kombinationen kann dabei helfen, die richtige Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung zu bestimmen.

Die folgenden Kombinationen aus Volume- und LUN-Konfiguration werden empfohlen:

- Speicherplatzreservierte Dateien oder LUNs mit Thick Volume-Bereitstellung
- Nicht speicherplatzreservierte Dateien oder LUNs mit Thin Volume Provisioning
- Speicherplatzreservierte Dateien oder LUNs mit semi-thick Volume Provisioning

Sie können SCSI Thin Provisioning auf Ihren LUNs in Verbindung mit jeder dieser Konfigurationskombinationen verwenden.

Speicherplatzreservierte Dateien oder LUNs mit Thick Volume-Bereitstellung

Vorteile:

- Alle Schreibvorgänge in Dateien mit reserviertem Speicherplatz sind garantiert; sie schlagen nicht aufgrund von unzureichendem Speicherplatz fehl.
- Für das Speichervolumen gelten keine Beschränkungen hinsichtlich Speichereffizienz und Datenschutztechnologien.

Kosten und Einschränkungen:

- Im Vorfeld muss ausreichend Speicherplatz im Aggregat reserviert werden, um das thickly provisioned Volume zu unterstützen.
- Bei der Erstellung der LUN wird Speicherplatz aus dem Volume zugewiesen, der dem Doppelten der Größe der LUN entspricht.

Nicht speicherplatzreservierte Dateien oder LUNs mit Thin Volume Provisioning

Vorteile:

- Für das Speichervolumen gelten keine Beschränkungen hinsichtlich Speichereffizienz und Datenschutztechnologien.
- Platz wird nur nach Bedarf zugeteilt.

Kosten und Einschränkungen:

- Schreibvorgänge sind nicht garantiert; sie können fehlschlagen, wenn das Volume keinen freien Speicherplatz mehr hat.
- Der freie Speicherplatz im Aggregat muss effektiv verwaltet werden, damit das Aggregat nicht ohne freien Speicherplatz bleibt.

Speicherplatzreservierte Dateien oder LUNs mit semi-thick Volume Provisioning

Vorteile:

Im Vergleich zur Bereitstellung dicker Volumes wird weniger Speicherplatz im Voraus reserviert, und eine bestmögliche Schreibgarantie wird weiterhin bereitgestellt.

Kosten und Einschränkungen:

- Bei dieser Option können Schreibvorgänge fehlschlagen.

  Dieses Risiko kann durch eine angemessene Balance zwischen freiem Speicherplatz im Volume und der Datenvolatilität gemindert werden.

- Sie können sich nicht darauf verlassen, dass Datensicherungsobjekte wie Snapshots und FlexClone Dateien und LUNs aufbewahrt werden.
- Sie können ONTAP Block-Sharing-Speichereffizienzfunktionen, die nicht automatisch gelöscht werden können, einschließlich Deduplizierung, Komprimierung und ODX/Copy Offload, nicht verwenden.

Die korrekte Volume- und LUN-Konfiguration für Ihre ONTAP Umgebung bestimmen

Die Beantwortung einiger grundlegender Fragen zu Ihrer Umgebung kann dabei helfen, die optimale FlexVol volume und LUN-Konfiguration für Ihre Umgebung zu bestimmen.

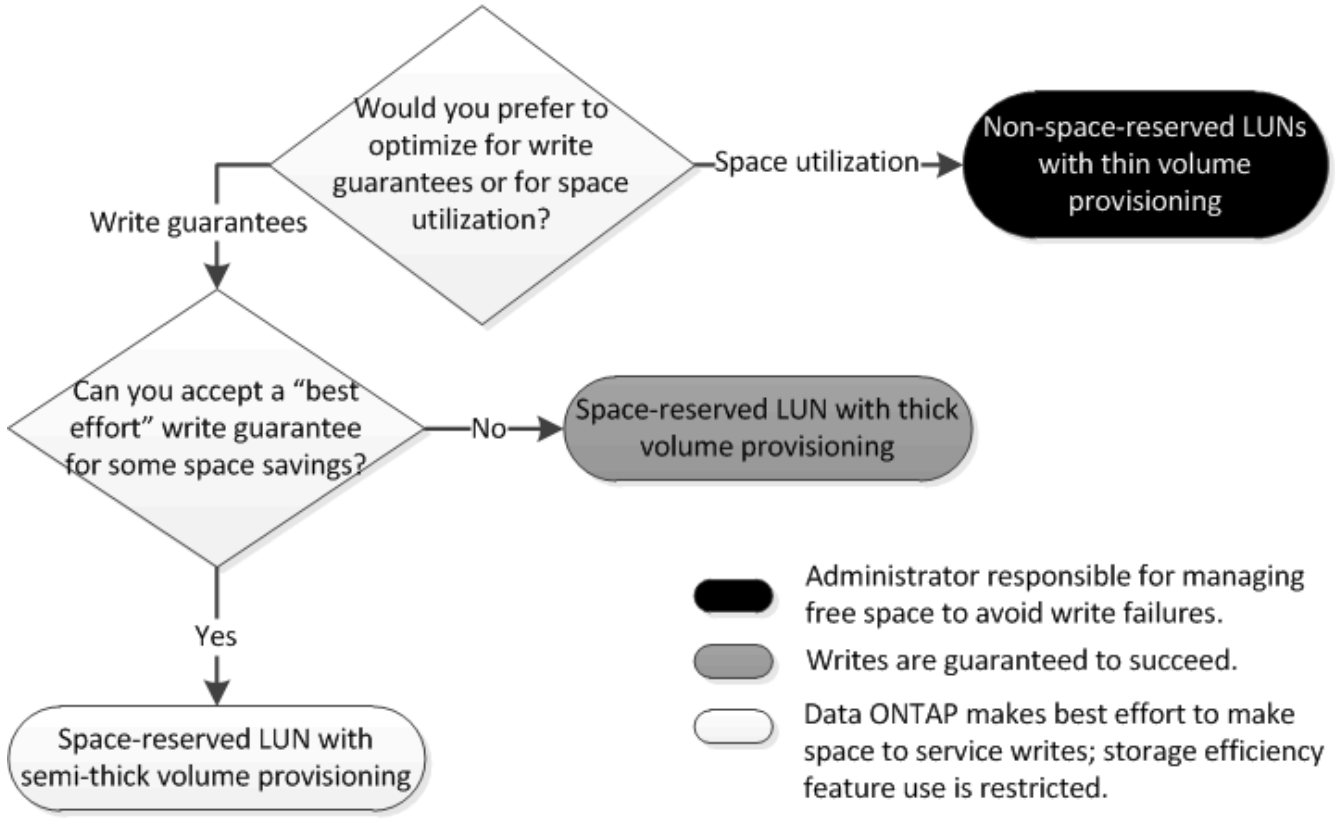
Über diese Aufgabe

Sie können Ihre LUN- und Volume-Konfigurationen für maximale Speicherauslastung oder für die Sicherheit von Schreibzusagen optimieren. Abhängig von Ihren Anforderungen an die Speicherauslastung und Ihrer Fähigkeit, freien Speicherplatz schnell zu überwachen und wieder aufzufüllen, ist zu bestimmen, welche FlexVol volume- und LUN-Volumes für Ihre Installation geeignet sind.

Sie benötigen kein separates Volume für jede LUN.

Schritt

1. Der folgende Entscheidungsbaum zeigt, welche Kombination aus Volume- und LUN-Konfiguration am besten für Ihre Umgebung geeignet ist:



Datenwachstumsrate für ONTAP LUNs berechnen

Es ist erforderlich, die Wachstumsrate Ihrer LUN-Daten im Zeitverlauf zu kennen, um festzustellen, ob speicherplatzreservierte oder nicht speicherplatzreservierte LUNs verwendet werden sollten.

Über diese Aufgabe

Bei einem konstant hohen Datenwachstum könnten LUNs mit reserviertem Speicherplatz die bessere Option sein. Bei einem geringen Datenwachstum sind LUNs ohne Speicherplatzreservierung eine Überlegung wert.

Sie können Tools wie OnCommand Insight verwenden, um Ihre Datenwachstumsrate zu berechnen, oder Sie können sie manuell berechnen. Die folgenden Schritte sind für die manuelle Berechnung.

Schritte

1. Eine LUN mit reserviertem Speicherplatz einrichten.
2. Die Daten auf der LUN werden über einen festgelegten Zeitraum, beispielsweise eine Woche, überwacht.

   Der Überwachungszeitraum sollte lang genug sein, um eine repräsentative Stichprobe regelmäßig auftretender Datenzuwächse zu bilden. Zum Beispiel kann es am Ende jedes Monats regelmäßig zu einem starken Datenzuwachs kommen.

3. Jeden Tag wird in GB festgehalten, um wie viel Ihr Datenvolumen wächst.
4. Am Ende des Überwachungszeitraums werden die Summen für jeden Tag zusammengezählt und anschließend durch die Anzahl der Tage im Überwachungszeitraum geteilt.

   Diese Berechnung ergibt Ihre durchschnittliche Wachstumsrate.

Beispiel

In diesem Beispiel benötigen Sie eine 200 GB LUN. Es wird beschlossen, die LUN eine Woche lang 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.

Informationen zu Einstellungen für die Platzreservierung bei Thick Volumes

Diese FlexVol volume- und Datei- oder LUN-Konfigurationskombination ermöglicht die Nutzung von Speichereffizienztechnologien und erfordert keine aktive Überwachung Ihres freien Speicherplatzes, da ausreichend Speicherplatz im Voraus zugewiesen wird.

Folgende Einstellungen sind erforderlich, um eine speicherplatzreservierte Datei oder LUN in einem Volume mithilfe von Thick Provisioning zu konfigurieren:

Volume-Einstellung	Wert
Garantie	Volumen
Teilreserve	100
Snapshot-Reserve	Beliebig
Snapshot Autolöschung	Optional
Automatisches Wachstum	Optional; falls aktiviert, muss der freie Speicherplatz des Aggregats aktiv überwacht werden.

Datei- oder LUN-Einstellung	Wert
Platzreservierung	Aktiviert

Einstellungen für nicht speicherplatzreservierte LUNs in ONTAP Volumes mit Thin Provisioning

Diese FlexVol Volume- und Datei- oder LUN-Konfigurationskombination erfordert die geringste Menge an Speicherplatz, die im Voraus zugewiesen werden muss, erfordert jedoch ein aktives Speicherplatzmanagement, um Fehler aufgrund von Speicherplatzmangel zu vermeiden.

Folgende Einstellungen sind erforderlich, um nicht speicherplatzreservierte Dateien oder LUNs in einem Thin-Provisioning Volume zu konfigurieren:

Volume-Einstellung	Wert
Garantie	Keine

Volume-Einstellung	Wert
Teilreserve	0
Snapshot-Reserve	Beliebig
Snapshot Autolöschung	Optional
Automatisches Wachstum	Optional

Datei- oder LUN-Einstellung	Wert
Platzreservierung	Deaktiviert

Weitere Überlegungen

Wenn der Speicherplatz auf dem Volume oder Aggregat erschöpft ist, können Schreibvorgänge auf die Datei oder LUN fehlschlagen.

Wenn Sie den freien Speicherplatz sowohl des Volumes als auch des Aggregats nicht aktiv überwachen möchten, sollte Autogrow für das Volume aktiviert werden und die maximale Größe des Volumes auf die Größe des Aggregats festgelegt werden. In dieser Konfiguration ist eine aktive Überwachung des freien Speicherplatzes im Aggregat erforderlich, während der freie Speicherplatz im Volume nicht überwacht werden muss.

Informationen zu Einstellungen für die Speicherplatzreservierung bei semi-thick Volumes

Diese FlexVol volume- und Datei- oder LUN-Konfigurationskombination erfordert weniger Speicherplatz, der im Voraus zugewiesen werden muss, als die vollständig bereitgestellte Kombination, schränkt jedoch die Effizienztechnologien ein, die für das Volume verwendet werden können. Überschreibungen werden bei dieser Konfigurationskombination nach dem Best-Effort-Prinzip erfüllt.

Folgende Einstellungen sind erforderlich, um eine speicherplatzreservierte LUN in einem Volume mithilfe von Semi-Thick Provisioning zu konfigurieren:

Volume-Einstellung	Wert
Garantie	Volumen
Teilreserve	0
Snapshot-Reserve	0
Snapshot Autolöschung	Aktiviert, mit der Verpflichtungsstufe zerstören, einer zerstören-Liste, die alle Objekte umfasst, dem auf Volume eingestellten Auslöser und allen FlexClone LUNs und FlexClone Dateien, die für die automatische Löschung aktiviert sind.
Automatisches Wachstum	Optional; falls aktiviert, muss der freie Speicherplatz des Aggregats aktiv überwacht werden.

Datei- oder LUN-Einstellung	Wert
Platzreservierung	Aktiviert

Technologische Beschränkungen

Die folgenden Technologien zur Steigerung der Speichereffizienz können für diese Konfigurationskombination nicht verwendet werden:

- Komprimierung
- Deduplizierung
- ODX und FlexClone Copy Offload
- FlexClone LUNs und FlexClone Dateien, die nicht zur automatischen Löschung markiert sind (aktive Klone)
- FlexClone Unterdateien
- ODX/Copy Offload

Weitere Überlegungen

Bei der Verwendung dieser Konfigurationskombination sind folgende Punkte zu berücksichtigen:

- Wenn auf dem Volume, das diese LUN unterstützt, der Speicherplatz knapp wird, werden die Schutzdaten (FlexClone LUNs und Dateien, Snapshots) zerstört.
- Schreibvorgänge können aufgrund eines Zeitlimits fehlschlagen, wenn der freie Speicherplatz auf dem Volume erschöpft ist.

Die Komprimierung ist für AFF Plattformen standardmäßig aktiviert. Die Komprimierung muss explizit für jedes Volume deaktiviert werden, für das Semi-Thick Provisioning auf einer AFF Plattform verwendet werden soll.

SAN Datenschutz

ONTAP Datenschutzmethoden für SAN-Umgebungen

Sie können Ihre Daten schützen, indem Sie Kopien davon erstellen, sodass sie im Falle versehentlichen Löschens, Anwendungsabstürzen, Datenbeschädigung oder Katastrophen für eine Wiederherstellung zur Verfügung stehen. Abhängig von Ihren Anforderungen an Datenschutz und Backup bietet ONTAP verschiedene Methoden, mit denen Sie Ihre Daten schützen können.

SnapMirror Active Sync

Ab der allgemeinen Verfügbarkeit in ONTAP 9.9.1 wird ein Zero Recovery Time Objective (Zero RTO) oder ein Transparent Application Failover (TAF) bereitgestellt, um ein automatisches Failover von geschäftskritischen Anwendungen in SAN-Umgebungen zu ermöglichen. SnapMirror active sync erfordert die Installation von ONTAP Mediator 1.2 in einer Konfiguration mit entweder zwei AFF Clustern oder zwei All-Flash SAN Array (ASA) Clustern.

- "ONTAP Mediator Dokumentation"
- "SnapMirror active sync Dokumentation"

Schnappschuss

Ermöglicht das manuelle oder automatische Erstellen, Planen und Verwalten mehrerer Backups Ihrer LUNs. Snapshots benötigen nur minimalen zusätzlichen Volume-Speicherplatz und verursachen keine Performance-

Einbußen. Wenn Ihre LUN-Daten versehentlich geändert oder gelöscht wurden, lässt sich diese Daten einfach und schnell aus einem der letzten Snapshots wiederherstellen.

FlexClone LUNs (FlexClone Lizenz erforderlich)

Stellt zeitpunktgenau beschreibbare Kopien einer anderen LUN in einem aktiven Volume oder in einem Snapshot bereit. Ein Klon und sein übergeordnetes Volume können unabhängig voneinander geändert werden, ohne sich gegenseitig zu beeinflussen.

SnapRestore (Lizenz erforderlich)

Ermöglicht eine schnelle, platzsparende und bedarfsgesteuerte Datenwiederherstellung aus Snapshots eines gesamten Volumes. Mit SnapRestore kann eine LUN in einen früheren, gesicherten Zustand zurückversetzt werden, ohne dass das Storage-System neu gestartet werden muss.

Datenschutz-Spiegelkopien (SnapMirror Lizenz erforderlich)

Ermöglicht asynchrone Notfallwiederherstellung, indem periodisch Snapshots der Daten auf dem Volume erstellt, diese Snapshots über ein lokales oder Weitverkehrsnetzwerk auf ein Partner-Volume, üblicherweise in einem anderen Cluster, kopiert und dort aufbewahrt werden. Die Spiegelkopie auf dem Partner-Volume bietet schnelle Verfügbarkeit und Wiederherstellung der Daten ab dem Zeitpunkt des letzten Snapshots, falls die Daten auf dem Quell-Volume beschädigt oder verloren sind.

SnapVault Backups (SnapMirror Lizenz erforderlich)

Bietet platzsparende und langfristige Aufbewahrung von Backups. SnapVault Beziehungen ermöglichen die Sicherung ausgewählter Snapshots von Volumes auf einem Zielvolume und die Aufbewahrung der Backups.

Wenn Bandsicherungen und Archivierungsvorgänge durchgeführt werden, ist dies mit den Daten möglich, die bereits auf dem SnapVault sekundären Volume gesichert wurden.

Native Tape-Backup und Recovery

Die Unterstützung für die meisten vorhandenen Bandlaufwerke ist in ONTAP enthalten, ebenso wie eine Methode, mit der Bandhersteller dynamisch die Unterstützung für neue Geräte hinzufügen können. ONTAP unterstützt außerdem das Remote Magnetic Tape (RMT) Protokoll, wodurch Backup und Recovery auf jedem geeigneten System möglich ist.

Verwandte Informationen

"Datensicherung mit Tape-Backup"

Wiederherstellung einer einzelnen LUN aus einem ONTAP Snapshot

Sie können eine einzelne LUN aus einem Snapshot wiederherstellen, ohne das gesamte Volume, das die einzelne LUN enthält, wiederherzustellen. Die LUN kann am selben Ort oder an einem neuen Pfad im Volume wiederhergestellt werden. Der Vorgang stellt nur die einzelne LUN wieder her, ohne andere Dateien oder LUNs im Volume zu beeinträchtigen. Auch Dateien mit Streams können wiederhergestellt werden.

Bevor Sie beginnen

- Sie benötigen ausreichend Speicherplatz auf Ihrem Volume, um den Wiederherstellungsvorgang abzuschließen:

- Wenn Sie eine speicherplatzreservierte LUN wiederherstellen, bei der die fraktionelle Reserve 0 % beträgt, wird der einmalige Speicherplatzbedarf in der Größe der wiederhergestellten LUN benötigt.
- Wenn Sie eine speicherplatzreservierte LUN wiederherstellen, bei der die Teilreserve 100 % beträgt, benötigen Sie die doppelte Größe der wiederherzustellenden LUN.
- Wenn Sie eine nicht speicherplatzreservierte LUN wiederherstellen, wird nur der tatsächlich für die wiederhergestellte LUN verwendete Speicherplatz benötigt.

- Ein Snapshot der Ziel-LUN muss erstellt worden sein.

  Schlägt die Wiederherstellung fehl, kann die Ziel-LUN abgeschnitten werden. In solchen Fällen lässt sich der Snapshot verwenden, um Datenverlust zu verhindern.

- Es muss ein Snapshot der Quell-LUN erstellt worden sein.

  In seltenen Fällen kann die Wiederherstellung der LUN fehlschlagen, wodurch die Quell-LUN unbrauchbar wird. Tritt dies auf, kann mithilfe des Snapshots die LUN in den Zustand unmittelbar vor dem Wiederherstellungsversuch zurückgesetzt werden.

- Die Ziel-LUN und die Quell-LUN müssen denselben Betriebssystemtyp aufweisen.

  Wenn Ihre Ziel-LUN einen anderen Betriebssystemtyp als Ihre Quell-LUN aufweist, kann Ihr Host nach dem Wiederherstellungsvorgang den Datenzugriff auf die Ziel-LUN verlieren.

Schritte

1. Vom Host aus sollte jeglicher Hostzugriff auf die LUN beendet werden.
2. Hängen Sie die LUN auf dem Host aus, sodass der Host nicht mehr 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. Bestimmen Sie den Snapshot, auf den Ihre LUN wiederhergestellt werden soll:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Vor der Wiederherstellung der LUN einen Snapshot der LUN erstellen:

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. Die angegebene LUN in einem Volume wiederherstellen:

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. Folgen Sie den Anweisungen auf dem Bildschirm.
8. Falls erforderlich kann die LUN online geschaltet werden:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. Falls erforderlich kann die LUN neu zugeordnet werden:

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

10. Vom Host aus die LUN erneut einbinden.
11. Vom Host aus wird der Zugriff auf die LUN neu gestartet.

Alle LUNs eines Volumes aus einem ONTAP Snapshot wiederherstellen

Mit dem `volume snapshot restore`-Befehl lassen sich alle LUNs in einem angegebenen Volume aus einem Snapshot wiederherstellen.

Schritte

1. Vom Host aus ist jeglicher Hostzugriff auf die LUNs zu beenden.

   Die Verwendung von SnapRestore ohne Unterbrechung des gesamten Hostzugriffs auf die LUNs im Volume kann zu Datenbeschädigung und Systemfehlern führen.

2. Die LUNs auf diesem Host werden ausgehängt, sodass der Host nicht mehr auf die LUNs zugreifen kann.
3. LUNs aufheben:

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

4. Bestimmen Sie den Snapshot, auf den das Volume wiederhergestellt werden soll:

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. Die Berechtigungseinstellung auf „Erweitert“ ändern:

```
set -privilege advanced
```

6. Daten wiederherstellen:

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
```

```
-snapshot <snapshot_name>
```

7. Folgen Sie den Anweisungen auf dem Bildschirm.
8. LUNs neu zuordnen:

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

9. Es sollte überprüft werden, ob die LUNs online sind:

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. Falls Ihre LUNs nicht online sind, können sie online geschaltet werden:

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. Die Berechtigungseinstellung auf Administrator ändern:

```
set -privilege admin
```

12. Vom Host aus die LUNs erneut einbinden.
13. Vom Host aus wird der Zugriff auf Ihre LUNs neu gestartet.

Informationen zu ONTAP FlexClone LUNs

Eine FlexClone LUN ist eine zeitpunktgenau beschreibbare Kopie einer anderen LUN in einem aktiven Volume oder in einem Snapshot. Die Kopie und die übergeordnete LUN können unabhängig voneinander geändert werden, ohne sich gegenseitig zu beeinflussen.

Mit FlexClone LUNs können mehrere lesen/schreiben-Kopien einer LUN erstellt werden.

Gründe für die Erstellung von FlexClone LUNs

- Eine temporäre Kopie einer LUN für Testzwecke wird benötigt.
- Eine Kopie Ihrer Daten muss für zusätzliche Benutzer verfügbar sein, ohne dass ihnen Zugriff auf die Produktionsdaten gewährt wird.
- Es soll ein Klon einer Datenbank für Manipulations- und Projektionsvorgänge erstellt werden, wobei die Originaldaten in unveränderter Form erhalten bleiben.
- Sie möchten auf eine bestimmte Teilmenge der Daten einer LUN zugreifen (ein bestimmtes logisches Volume oder Dateisystem in einer Volume-Gruppe oder eine bestimmte Datei oder Dateigruppe in einem Dateisystem) und diese auf die ursprüngliche LUN kopieren, ohne die übrigen Daten in der ursprünglichen LUN wiederherzustellen. Dies funktioniert auf Betriebssystemen, die das gleichzeitige Einbinden einer LUN und eines Klons der LUN unterstützen.

- Sie benötigen mehrere SAN Boot Hosts mit demselben Betriebssystem.

Eine FlexClone LUN teilt sich zunächst den Speicherplatz mit ihrer übergeordneten LUN. Standardmäßig erbt die FlexClone LUN das Attribut „reservierter Speicherplatz“ der übergeordneten LUN. Wenn die übergeordnete LUN beispielsweise keinen reservierten Speicherplatz hat, ist die FlexClone LUN standardmäßig ebenfalls ohne reservierten Speicherplatz. Es ist jedoch möglich, eine FlexClone LUN ohne reservierten Speicherplatz aus einer übergeordneten LUN mit reserviertem Speicherplatz zu erstellen.

Beim Klonen einer LUN findet die Blockfreigabe im Hintergrund statt und Sie können erst dann einen Volume-Snapshot erstellen, wenn die Blockfreigabe abgeschlossen ist.

Das Volume muss so konfiguriert werden, dass die automatische Löschfunktion für FlexClone LUNs mit dem `volume snapshot autodelete modify` Befehl aktiviert wird. Andernfalls, wenn FlexClone LUNs automatisch gelöscht werden sollen, das Volume jedoch nicht für die automatische Löschung von FlexClone LUNs konfiguriert ist, werden keine FlexClone LUNs gelöscht.

Wenn eine FlexClone LUN erstellt wird, ist die automatische Löschfunktion für die FlexClone LUN standardmäßig deaktiviert. Sie muss für jede FlexClone LUN manuell aktiviert werden, bevor diese FlexClone LUN automatisch gelöscht werden kann. Bei Verwendung von semi-thick Volume-Provisioning und dem Wunsch nach der durch diese Option bereitgestellten „best effort“-Schreibgarantie müssen *alle* FlexClone LUNs für die automatische Löschung verfügbar gemacht werden.

> Wenn eine FlexClone LUN aus einem Snapshot erstellt wird, wird die LUN automatisch mithilfe eines platzsparenden Hintergrundprozesses vom Snapshot getrennt, sodass die LUN nicht weiterhin vom Snapshot abhängig ist oder zusätzlichen Speicherplatz belegt. Wenn diese Hintergrundtrennung noch nicht abgeschlossen ist und dieser Snapshot automatisch gelöscht wird, wird diese FlexClone LUN gelöscht, selbst wenn die FlexClone Auto-Delete-Funktion für diese FlexClone LUN deaktiviert wurde. Nach Abschluss der Hintergrundtrennung wird die FlexClone LUN nicht gelöscht, selbst wenn dieser Snapshot gelöscht wird.

Verwandte Informationen

- "Eine FlexClone LUN erstellen"
- "Ein FlexVol volume kann so konfiguriert werden, dass FlexClone LUNs automatisch gelöscht werden"
- "Verhindern, dass eine FlexClone LUN automatisch gelöscht wird"

Konfiguration und Nutzung von SnapVault Backups in einer SAN-Umgebung

Informationen zu ONTAP SnapVault Backups in einer SAN-Umgebung

SnapVault Konfiguration und Verwendung in einer SAN-Umgebung ist der Konfiguration und Verwendung in einer NAS-Umgebung sehr ähnlich, aber die Wiederherstellung von LUNs in einer SAN-Umgebung erfordert einige spezielle Verfahren.

SnapVault Backups enthalten eine Reihe schreibgeschützter Kopien eines Quellvolumes. In einer SAN-Umgebung werden immer ganze Volumes auf das SnapVault sekundäre Volume gesichert, nicht einzelne LUNs.

Das Verfahren zum Erstellen und Initialisieren der SnapVault Beziehung zwischen einem primären Volume mit LUNs und einem sekundären Volume, das als SnapVault Backup dient, ist identisch mit dem Verfahren, das bei FlexVol Volumes für Dateiprotokolle verwendet wird. Dieses Verfahren wird ausführlich in "Datensicherung" beschrieben.

Es ist wichtig sicherzustellen, dass sich die zu sichernden LUNs in einem konsistenten Zustand befinden, bevor die Snapshots erstellt und auf das SnapVault sekundäre Volume kopiert werden. Die Automatisierung der Snapshot-Erstellung mit SnapCenter gewährleistet, dass die gesicherten LUNs vollständig und von der ursprünglichen Anwendung nutzbar sind.

Es gibt drei grundlegende Möglichkeiten zur Wiederherstellung von LUNs aus einem SnapVault sekundäres Volume:

- Sie können eine LUN direkt vom SnapVault sekundären Volume zuordnen und einen Host mit der LUN verbinden, um auf den Inhalt der LUN zuzugreifen.

  Die LUN ist schreibgeschützt und kann nur vom aktuellsten Snapshot im SnapVault Backup zugeordnet werden. Persistente Reservierungen und andere LUN-Metadaten gehen verloren. Falls gewünscht, lässt sich mithilfe eines Kopierprogramms auf dem Host der Inhalt der LUN zurück auf die ursprüngliche LUN kopieren, sofern diese noch zugänglich ist.

  Die LUN hat eine andere Seriennummer als die Quell-LUN.

- Jeder Snapshot im SnapVault sekundären Volume kann auf ein neues Lese-/Schreib-Volume geklont werden.

  Anschließend kann jede beliebige LUN im Volume zugeordnet und ein Host mit der LUN verbunden werden, um auf den Inhalt der LUN zuzugreifen. Falls gewünscht, lässt sich mithilfe eines Kopierprogramms auf dem Host der Inhalt der LUN zurück auf die ursprüngliche LUN kopieren, sofern diese noch zugänglich ist.

- Das gesamte Volume, das die LUN enthält, kann aus einem beliebigen Snapshot im SnapVault sekundären Volume wiederhergestellt werden.

  Durch die Wiederherstellung des gesamten Volumes werden alle LUNs und alle Dateien im Volume ersetzt. Alle seit der Erstellung des Snapshots neu erstellten LUNs gehen verloren.

  Die LUNs behalten ihre Zuordnung, Seriennummern, UUIDs und persistenten Reservierungen.

Zugriff auf eine schreibgeschützte LUN-Kopie aus einem ONTAP SnapVault Backup

Sie können auf eine schreibgeschützte Kopie einer LUN aus dem letzten Snapshot in einem SnapVault Backup zugreifen. Die LUN-ID, der Pfad und die Seriennummer unterscheiden sich von der Quell-LUN und müssen zunächst zugeordnet werden. Persistente Reservierungen, LUN-Zuordnungen und Initiatorgruppen werden nicht auf das SnapVault sekundäre Volume repliziert.

Bevor Sie beginnen

- Die SnapVault Beziehung muss initialisiert werden und der neueste Snapshot im SnapVault sekundären Volume muss die gewünschte LUN enthalten.
- Die Storage Virtual Machine (SVM), die das SnapVault Backup enthält, muss über eine oder mehrere LIFs mit dem gewünschten SAN-Protokoll verfügen, die von dem Host aus erreichbar sind, der zum Zugriff auf die LUN-Kopie verwendet wird.
- Wenn Sie planen, direkt vom SnapVault sekundären Volume auf LUN-Kopien zuzugreifen, müssen Sie Ihre Initiatorgruppen im Voraus auf der SnapVault SVM erstellen.

  Sie können direkt auf eine LUN vom SnapVault sekundäres Volume zugreifen, ohne zuerst das Volume, das die LUN enthält, wiederherstellen oder klonen zu müssen.

Über diese Aufgabe

Wenn dem SnapVault sekundären Volume ein neuer Snapshot hinzugefügt wird, während Sie eine LUN aus einem vorherigen Snapshot zugeordnet haben, ändert sich der Inhalt der zugeordneten LUN. Die LUN ist weiterhin mit denselben Kennungen zugeordnet, aber die Daten stammen aus dem neuen Snapshot. Wenn sich die LUN-Größe ändert, erkennen einige Hosts die Größenänderung automatisch; Windows-Hosts benötigen einen erneuten Datenträgerscan, um eine Größenänderung zu erkennen.

Schritte

1. Die verfügbaren LUNs im SnapVault sekundären Volume auflisten.

```
lun show
```

   In diesem Beispiel sind sowohl die ursprünglichen LUNs im primären Volume srcvolA als auch die Kopien im SnapVault sekundären Volume dstvolB zu sehen:

```
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.
```

   Weitere Informationen zu `lun show` finden sich in der "ONTAP-Befehlsreferenz".

2. Falls die Initiatorgruppe für den gewünschten Host auf der SVM, die das SnapVault sekundäre Volume enthält, noch nicht existiert, sollte eine Initiatorgruppe erstellt werden.

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

   Dieser Befehl 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
```

3. Die gewünschte LUN-Kopie wird der Initiatorgruppe zugeordnet.

```
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
```

Weitere Informationen zu `lun mapping create` finden sich in der "ONTAP-Befehlsreferenz".

4. Den Host mit der LUN verbinden und nach Bedarf auf die Inhalte der LUN zugreifen.

Wiederherstellung einer einzelnen LUN aus einem ONTAP SnapVault Backup

Sie können eine einzelne LUN an einem neuen oder am ursprünglichen Speicherort wiederherstellen. Sie können von jedem Snapshot im SnapVault sekundären Volume wiederherstellen. Um die LUN am ursprünglichen Speicherort wiederherzustellen, wird sie zunächst an einem neuen Speicherort wiederhergestellt und anschließend kopiert.

Bevor Sie beginnen

- Die SnapVault Beziehung muss initialisiert werden und das SnapVault sekundäre Volume muss einen geeigneten Snapshot zur Wiederherstellung enthalten.
- Die Storage Virtual Machine (SVM), die das SnapVault sekundäre Volume enthält, muss über eine oder mehrere LIFs mit dem gewünschten SAN-Protokoll verfügen, die von dem Host aus erreichbar sind, der zum Zugriff auf die LUN-Kopie verwendet wird.
- Die igroups müssen bereits auf der SnapVault SVM existieren.

Über diese Aufgabe

Der Prozess umfasst das Erstellen eines Lese-/Schreib-Volume-Klons aus einem Snapshot im SnapVault sekundären Volume. Die LUN kann direkt aus dem Klon verwendet werden, alternativ ist es möglich, den LUN-Inhalt zurück an den ursprünglichen LUN-Speicherort zu kopieren.

Die LUN im Klon hat einen anderen Pfad und eine andere Seriennummer als die ursprüngliche LUN. Persistente Reservierungen werden nicht beibehalten.

Schritte

1. Das sekundäre Volume, das die SnapVault Sicherung enthält, überprüfen.

```
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. Den Snapshot identifizieren, aus dem die LUN wiederhergestellt werden soll.

```
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. Einen Lese-/Schreibklon aus dem gewünschten Snapshot erstellen

```
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 wie das SnapVault Backup erstellt. Im Aggregat muss ausreichend Speicherplatz für den Klon vorhanden sein.

```
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. Die LUNs im Volume Clone auflisten.

```
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.
```

Weitere Informationen zu `lun show` finden sich in der "ONTAP-Befehlsreferenz".

5. Falls die Initiatorgruppe für den gewünschten Host auf der SVM, die das SnapVault Backup enthält, noch nicht existiert, ist eine Initiatorgruppe zu erstellen.

```
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. Die gewünschte LUN-Kopie wird der Initiatorgruppe zugeordnet.

```
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
```

Weitere Informationen zu `lun mapping create` finden sich in der "ONTAP-Befehlsreferenz".

7. Den Host mit der LUN verbinden und nach Bedarf auf die Inhalte der LUN zugreifen.

Die LUN ist les- und beschreibbar und kann anstelle der ursprünglichen LUN verwendet werden. Da die Seriennummer der LUN abweicht, interpretiert der Host sie als eine andere LUN als die ursprüngliche.

8. Ein Kopierprogramm auf dem Host kann verwendet werden, um den Inhalt der LUN zurück auf die ursprüngliche LUN zu kopieren.

Verwandte Informationen

- "snapmirror show"

Alle LUNs in einem Volume aus einem ONTAP SnapVault Backup wiederherstellen

Wenn ein oder mehrere LUNs in einem Volume aus einem SnapVault Backup

wiederhergestellt werden müssen, ist eine Wiederherstellung des gesamten Volumes möglich. Die Wiederherstellung des Volumes betrifft alle LUNs im Volume.

Bevor Sie beginnen

Die SnapVault Beziehung muss initialisiert werden und das SnapVault sekundäre Volume muss einen geeigneten Snapshot zur Wiederherstellung enthalten.

Über diese Aufgabe

Durch die Wiederherstellung eines gesamten Volumes wird dieses in den Zustand zurückversetzt, in dem es sich zum Zeitpunkt der Snapshot-Erstellung befand. Wurde dem Volume nach der Snapshot-Erstellung eine LUN hinzugefügt, wird diese LUN während des Wiederherstellungsprozesses entfernt.

Nach der Wiederherstellung des Volumes bleiben die LUNs den Initiatorgruppen zugeordnet, denen sie unmittelbar vor der Wiederherstellung zugeordnet waren. Die LUN-Zuordnung kann sich von der Zuordnung zum Zeitpunkt des Snapshots unterscheiden. Persistente Reservierungen auf den LUNs von Host-Clustern bleiben erhalten.

Schritte

1. Die E/A für alle LUNs im Volume anhalten.
2. Das sekundäre Volume überprüfen, das das SnapVault sekundäre 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. Den Snapshot identifizieren, von dem die Wiederherstellung erfolgen soll.

```
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 von Ihnen für die Wiederherstellung angegebene Ziel ist das ursprüngliche Volume, auf das 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 LUNs über einen Hostcluster hinweg gemeinsam genutzt werden, sollten die persistenten Reservierungen auf den LUNs von den betroffenen Hosts wiederhergestellt werden.

Wiederherstellen eines Volumes aus einem SnapVault Backup

Im folgenden Beispiel wurde die LUN mit dem Namen lun_D nach der Erstellung des Snapshots dem Volume hinzugefügt. Nach der Wiederherstellung des gesamten Volumes aus dem Snapshot ist lun_D nicht mehr vorhanden.

In der `lun show`Befehlsausgabe sind die LUNs im primären Volume srcvolA und die schreibgeschützten Kopien dieser LUNs im SnapVault sekundären Volume dstvolB zu sehen. Es gibt keine Kopie von lun_D in der SnapVault Sicherung.

```
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.
```

Nach der Wiederherstellung des Volumes vom SnapVault sekundären Volume enthält das Quell-Volume keine lun_D mehr. Die LUNs im Quell-Volume müssen nach der Wiederherstellung nicht neu zugeordnet werden, da sie weiterhin zugeordnet sind.

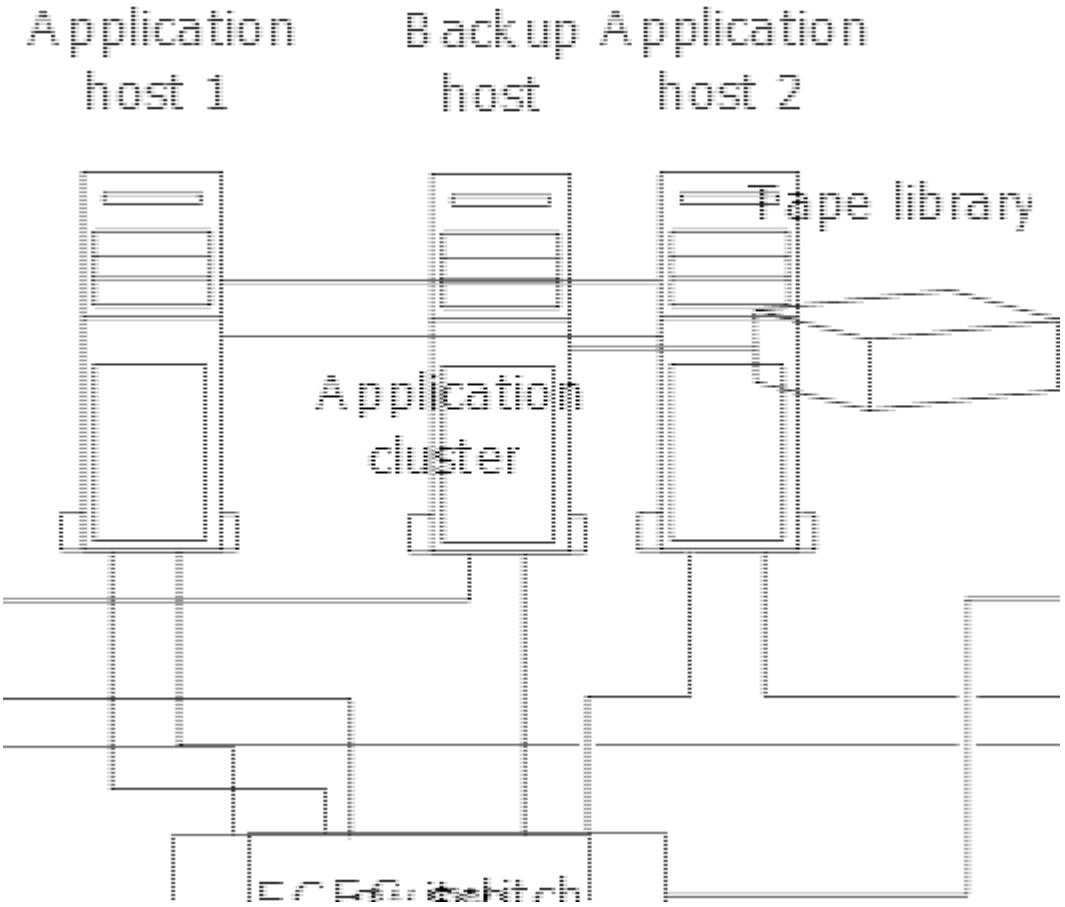
Verwandte Informationen

- "SnapMirror Restore"
- "snapmirror show"

Empfohlene Konfiguration für den Anschluss eines Host-Backup-Systems an ONTAP

SAN-Systeme lassen sich über einen separaten Backup-Host auf Band sichern, wodurch Leistungseinbußen auf dem Anwendungshost vermieden werden.

Für Backupzwecke ist es unerlässlich, SAN- und NAS-Daten getrennt zu speichern. Die folgende Abbildung zeigt die empfohlene physische Konfiguration für ein Host-Backup-System auf dem primären Storage-System. Volumes müssen ausschließlich als SAN konfiguriert werden. LUNs können auf ein einzelnes Volume beschränkt oder auf mehrere Volumes oder Storage-Systeme verteilt werden.



Volumes auf einem Host können aus einer einzelnen LUN bestehen, die vom Storage-System gemappt wird, oder aus mehreren LUNs mithilfe eines Volume-Managers wie VxVM auf HP-UX-Systemen.

Ein Host-Backup-System kann zum Schutz einer LUN auf dem ONTAP-Speichersystem eingesetzt werden.

Eine geklonte LUN aus einem Snapshot kann als Quelldaten für das Host-Backup-System genutzt werden.

Bevor Sie beginnen

Es muss eine Produktions-LUN vorhanden sein, die einer Initiatorgruppe zugeordnet ist, die den WWPN oder Node-Name des Anwendungsservers enthält. Die LUN muss außerdem formatiert und für den Host zugänglich sein.

Schritte

1. Speichern Sie den Inhalt der Puffer des Host-Dateisystems auf der Festplatte.

   Sie können den vom Host-Betriebssystem bereitgestellten Befehl verwenden. Sie können diesen Schritt auch als Teil Ihres SAN-Backup-Vorverarbeitungsskripts ausführen.

2. Ein Snapshot der Produktions-LUN wird erstellt.

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. Einen Klon der Produktions-LUN erstellen.

```
volume file clone create -vserver <svm_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. Eine Initiatorgruppe erstellen, 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 optional in das Nachbearbeitungsskript Ihrer SAN Backup-Anwendung integrieren.

6. Vom Host aus die neue LUN erkennen und das Dateisystem für den Host verfügbar machen.

   Sie können diesen Schritt optional in das Nachbearbeitungsskript Ihrer SAN Backup-Anwendung integrieren.

7. Die Daten im LUN-Klon werden vom Backup-Host mithilfe der SAN-Backup-Anwendung auf Band gesichert.
8. Den LUN-Klon offline schalten.

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. Den LUN-Klon entfernen.

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. Den Snapshot entfernen.

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN Konfigurationsreferenz

Erfahren Sie mehr über die ONTAP SAN-Konfiguration

Ein storage area network (SAN) besteht aus einer Speicherlösung, 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 direkt mit Ihrem Host verbunden wird, ohne einen Switch zu verwenden.

In einem SAN können mehrere Hosts mit unterschiedlichen Betriebssystemen wie Windows, Linux oder UNIX gleichzeitig auf die Speicherlösung zugreifen. Es können "Selektive LUN Zuordnung" und "Portsets" verwendet werden, um den Datenzugriff zwischen den Hosts und dem Speicher zu begrenzen.

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 Speicherlösung und den Hosts als Fabric bezeichnet. Zur Schaffung von Redundanz, die vor dem Verlust des Datenzugriffs schützt, empfiehlt sich die Einrichtung des SAN mit HA-Paaren in einer Multi-Netzwerk- oder Multi-Fabric-Konfiguration. Konfigurationen mit einzelnen Knoten oder einzelnen Netzwerken/Fabrics sind nicht vollständig redundant und daher nicht empfehlenswert.

Nachdem Ihr SAN konfiguriert ist, können Sie "Speicher für iSCSI oder FC bereitstellen" oder "Storage für FC/NVMe bereitstellen". Anschließend ist eine Verbindung zu Ihren Hosts möglich, um mit der Datenverarbeitung zu beginnen.

Die Unterstützung des SAN-Protokolls variiert je nach Ihrer ONTAP Version, Ihrer Plattform und Ihrer Konfiguration. Details zu Ihrer spezifischen Konfiguration sind in der "NetApp Interoperabilitätsmatrix-Tool" zu finden.

Verwandte Informationen

- "SAN-Administration Übersicht"
- "NVMe Konfiguration, Unterstützung und Einschränkungen"

iSCSI Konfigurationen

iSCSI Netzwerkkonfigurationen für ONTAP Systeme

Die iSCSI-Konfiguration sollte mit Hochverfügbarkeitspaaren (HA) eingerichtet werden, die entweder direkt an die iSCSI-SAN-Hosts angeschlossen sind oder über einen oder mehrere IP-Switches mit den Hosts verbunden werden.

"HA-Paare"sind als Meldeknoten für die Active/Optimized- und die Active/Unoptimized-Pfade definiert, die von den Hosts für den Zugriff auf die LUNs verwendet werden. Mehrere Hosts mit unterschiedlichen Betriebssystemen wie Windows, Linux oder UNIX können gleichzeitig auf den Storage zugreifen. Für Hosts ist eine unterstützte Multipathing-Lösung erforderlich, die ALUA unterstützt und konfiguriert ist. Unterstützte Betriebssysteme und Multipathing-Lösungen können auf der "NetApp Interoperabilitätsmatrix-Tool" überprüft werden.

In einer Multi-Network-Konfiguration verbinden zwei oder mehr Switches die Hosts mit dem Speichersystem. Multi-Network-Konfigurationen werden empfohlen, da sie vollständig redundant sind. In einer Single-Network-Konfiguration verbindet ein Switch die Hosts mit dem Speichersystem. Single-Network-Konfigurationen sind nicht vollständig redundant.

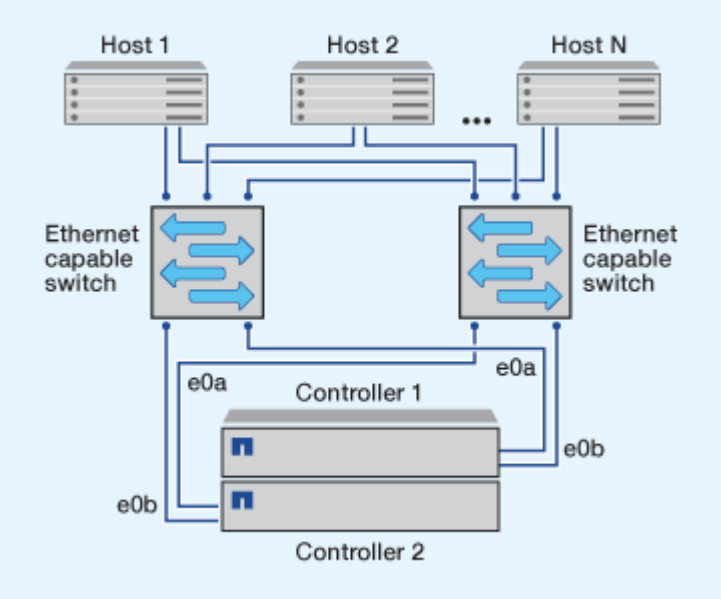
"Single-Node Konfigurationen" werden nicht empfohlen, da sie nicht die Redundanz bieten, die für Fehlertoleranz und unterbrechungsfreien Betrieb erforderlich ist.

Verwandte Informationen

- Erfahren Sie, wie "Selektives LUN Mapping (SLM)" die Pfade eingeschränkt werden, die für den Zugriff auf die LUNs eines HA-Paares verwendet werden.
- Informationen dazu "SAN-LIFs".
- Informationen zu "Vorteile von VLANs in iSCSI".

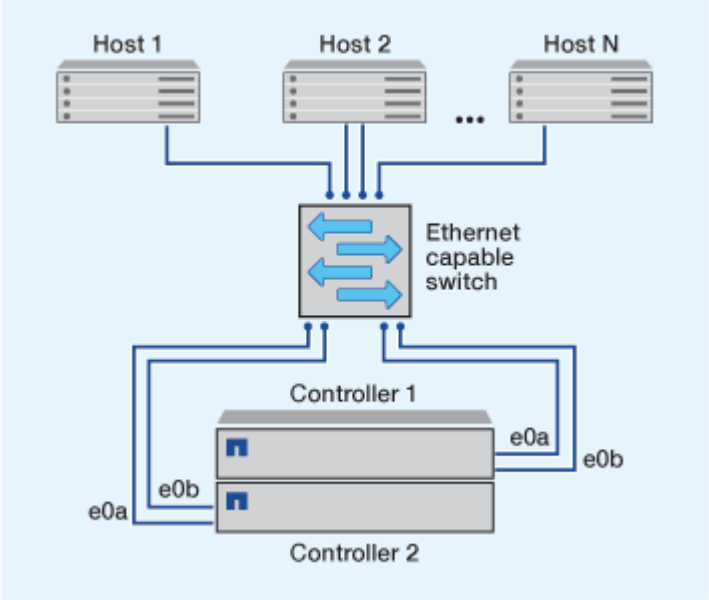
Multi-Network iSCSI Konfigurationen

In Multi-Netzwerk-HA-Paar-Konfigurationen verbinden zwei oder mehr Switches das HA-Paar mit einem oder mehreren Hosts. Da mehrere Switches vorhanden sind, ist diese Konfiguration vollständig redundant.



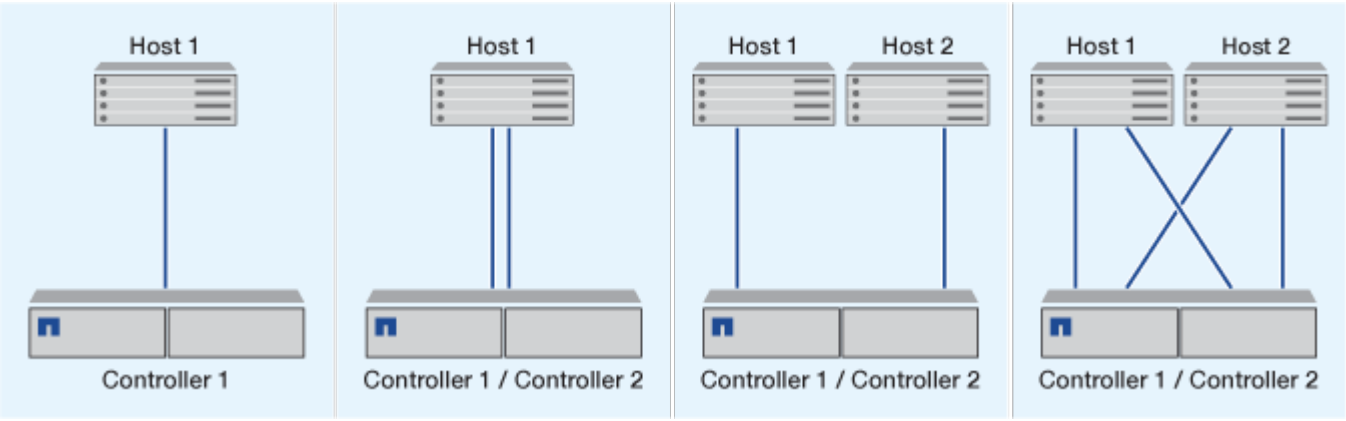
iSCSI-Konfigurationen für ein einzelnes Netzwerk

Bei HA-Paarkonfigurationen mit einem einzigen Netzwerk verbindet ein Switch das HA-Paar mit einem oder mehreren Hosts. Da nur ein einziger Switch verwendet wird, ist diese Konfiguration nicht vollständig redundant.



Direct-Attachment iSCSI Konfiguration

In einer direkt angeschlossenen 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 in einer Broadcast-Domäne zusammengefasst sind. Ein VLAN kann sich auf einem einzelnen Switch befinden oder mehrere Switch-Gehäuse umfassen. Statische und dynamische VLANs erhöhen die Sicherheit, isolieren Probleme und begrenzen die verfügbaren Pfade innerhalb Ihrer IP-Netzwerkinfrastruktur.

Bei der Implementierung von VLANs in großen IP-Netzwerkinfrastrukturen ergeben sich folgende Vorteile:

- Erhöhte Sicherheit.

  VLANs ermöglichen die Nutzung der bestehenden Infrastruktur und bieten gleichzeitig erhöhte Sicherheit, da sie den Zugriff zwischen verschiedenen Knoten eines Ethernet-Netzwerks oder eines IP-SANs einschränken.

- Verbesserte Zuverlässigkeit des Ethernet-Netzwerks und des IP-SAN durch Isolierung von Problemen.
- Verkürzung der Problemlösungszeit durch Begrenzung des Problemraums.
- Reduzierung der Anzahl verfügbarer Pfade zu einem bestimmten iSCSI-Zielport.
- Reduzierung der maximalen Anzahl von Pfaden, die von einem Host verwendet werden.

  Zu viele Pfade verlängern die Wiederverbindungszeiten. Wenn ein Host keine Multipathing-Lösung hat, kann VLANs verwendet werden, um nur einen Pfad zuzulassen.

Dynamische VLANs

Dynamische VLANs basieren auf MAC-Adressen. Ein VLAN kann definiert werden, indem die MAC-Adresse der Mitglieder angegeben wird, die eingeschlossen werden sollen.

Dynamische VLANs bieten Flexibilität und erfordern keine Zuordnung zu den physischen Ports, an denen das Gerät physisch mit dem Switch verbunden ist. Ein Kabel kann von einem Port auf einen anderen umgesteckt werden, ohne dass das VLAN neu konfiguriert werden muss.

Statische VLANs

Statische VLANs sind Port-basiert. Der Switch und der Switch-Port definieren das VLAN und seine Mitglieder.

Statische VLANs bieten eine höhere Sicherheit, da es nicht möglich ist, VLANs durch Media Access Control (MAC)-Spoofing zu kompromittieren. Wenn jedoch jemand physischen Zugriff auf den Switch hat, kann durch Austausch eines Kabels und Neukonfiguration der Netzwerkadresse Zugriff erlangt werden.

In manchen Umgebungen ist es einfacher, statische VLANs zu erstellen und zu verwalten als dynamische VLANs. Dies liegt daran, dass bei statischen VLANs lediglich der Switch und die Portkennung angegeben werden müssen, anstatt der 48-Bit-MAC-Adresse. Zusätzlich können Switch-Portbereiche mit der VLAN-Kennung gekennzeichnet werden.

FC Konfigurationen

FC- und FC-NVMe Fabric- sowie Direct-Attach-Konfigurationen für ONTAP

Bei FC und FC/NVMe wird die Netzwerktopologie zwischen der Speicherlösung und den Hosts als Fabric bezeichnet. Um Redundanz zu schaffen, die Sie vor dem Verlust des Datenzugriffs schützt, wird empfohlen, Ihr SAN mit HA-Paaren unter Verwendung von zwei oder mehr Switches in einer Multi-Fabric-Konfiguration einzurichten. Single-Fabric-Konfigurationen, die nur einen Switch zwischen den Hosts und der Speicherlösung verwenden, sind nicht vollständig redundant.

Ab ONTAP 9.19.1 können Sie FC- oder FC-NVMe-SAN-Hosts auch direkt ohne Switch an HA-Paare anschließen. Direktanschlusskonfigurationen können besonders an Remote-Standorten und in hybriden Umgebungen wertvoll sein, wo Einfachheit entscheidend ist.

Kaskadierte, partielle, vollständige, Core-Edge- und Director-Fabrics sind branchenübliche Methoden zur Verbindung von FC-Switches mit einem Fabric und werden alle unterstützt. Die Verwendung heterogener FC-Switch-Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches. Spezifische Ausnahmen sind auf der "Interoperabilitätsmatrix-Tool" aufgeführt. Ein Fabric kann aus einem oder mehreren Switches bestehen, und die Storage-Controller können mit mehreren Switches verbunden sein.

Mehrere Hosts mit unterschiedlichen Betriebssystemen wie Windows, Linux oder UNIX können gleichzeitig auf

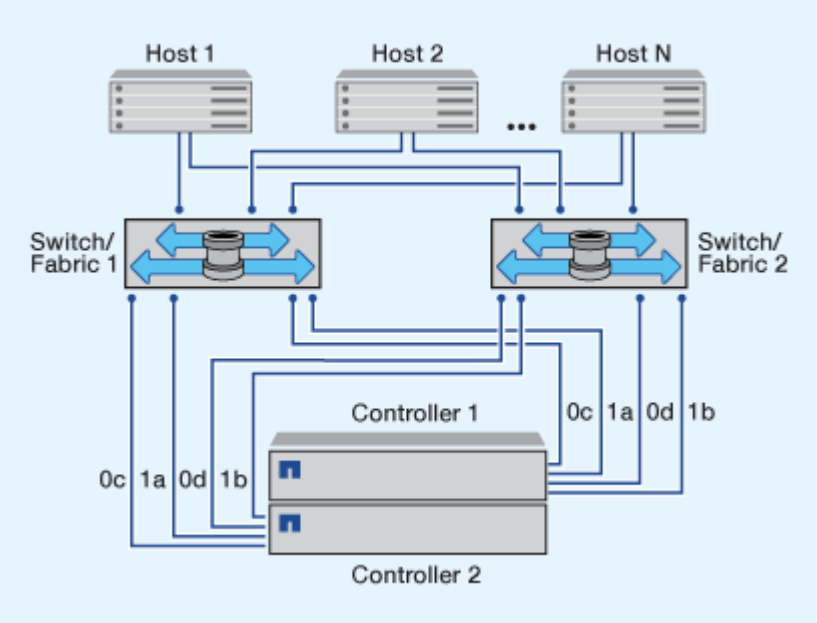
die Storage-Controller zugreifen. Hosts benötigen, dass eine unterstützte Multipathing-Lösung installiert und konfiguriert ist. Unterstützte Betriebssysteme und Multipathing-Lösungen können im Interoperability Matrix Tool überprüft werden.

Multifabric FC und FC-NVMe Konfigurationen

Es wird empfohlen, Ihre FC- und FC-NVMe-SAN-Hosts mit HA-Paaren und mindestens zwei Switches zu konfigurieren. [EH5.1][FD5.2][EH5.3] Dies gewährleistet Redundanz auf Fabric- und Speichersystemebene und unterstützt Fehlertoleranz und unterbrechungsfreie Vorgänge.

In einer Multifabric-HA-Paarkonfiguration verbinden zwei oder mehr Switches das HA-Paar mit einem oder mehreren Hosts. Jeder Switch erzeugt ein separates Fabric, das aus den Pfaden zwischen den Hosts und dem HA-Paar besteht, die über den Switch verlaufen. Durch Hinzufügen eines weiteren Switches wird ein zusätzliches Fabric erzeugt. Eine Multifabric-Konfiguration kann zwei oder mehr Switches und ihre zugehörigen Fabrics umfassen. Zur Vereinfachung zeigt die folgende Abbildung nur zwei Switches, die zwei separate Fabrics repräsentieren.

Die FC-Zielportnummern (0c, 0d, 1a, 1b) in den Abbildungen sind Beispiele. Die tatsächlichen Portnummern variieren je nach Modell Ihres Speicherknotens und ob Erweiterungsadapter verwendet werden.

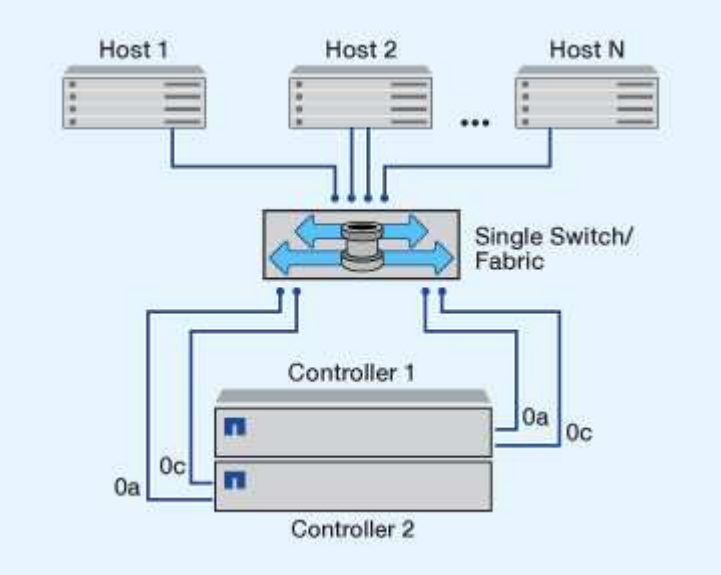


Single-fabric FC- und FC-NVMe-Konfigurationen

In Single-Fabric-HA-Paarkonfigurationen verbindet ein einzelner Switch das HA-Paar mit einem oder mehreren Hosts. Dieser einzelne Switch bildet ein einziges Fabric, das alle Pfade zwischen den Hosts und dem HA-Paar umfasst. Da keine Redundanz vorhanden ist, kann ein Switch-Ausfall zu Dienstunterbrechungen führen.

Die FC-Zielportnummern (0a, 0c) in den Abbildungen sind Beispiele. Die tatsächlichen Portnummern variieren je nach Modell Ihres Speicherknotens und ob Erweiterungsadapter verwendet werden.

Alle Plattformen, die FC-Konfigurationen unterstützen, unterstützen HA-Paar-Konfigurationen mit einem einzelnen Fabric.

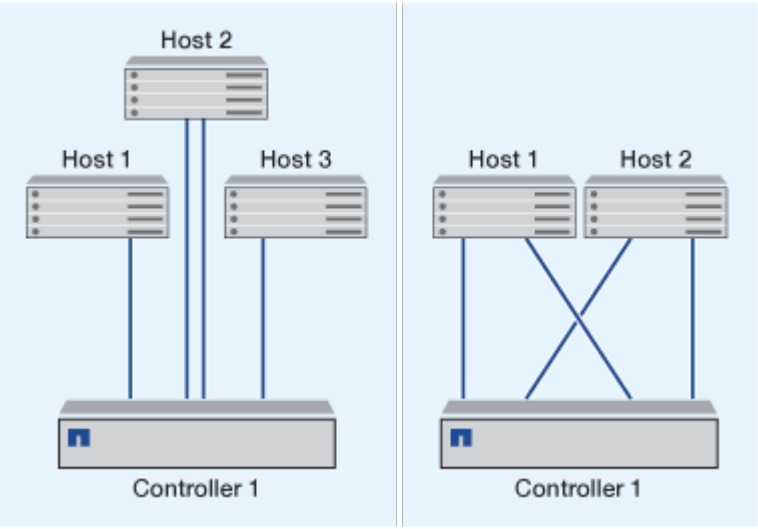


Direktanschluss-FC- und FC-NVMe-Konfigurationen

Ab ONTAP 9.19.1 werden Direct-Attachment-FC- und FC-NVMe-Konfigurationen für bestimmte AFF, ASA r2 und FAS Systeme mit der erforderlichen QLogic oder Emulex FC-Adapterkarte unterstützt. Bei einer Direct-Attachment-Konfiguration werden ein oder mehrere Hosts direkt an Ihre HA-Paare angeschlossen, ohne dass ein Switch vorhanden ist. Diese Konfiguration kann besonders wertvoll an Remote-Standorten und in hybriden Umgebungen sein, in denen Einfachheit entscheidend ist.

- MetroCluster Konfigurationen unterstützen keine direkte Anbindung.
- Direktanschlusskonfigurationen unterstützen "SVM-Migration" nicht.

Eine vollständige Liste der unterstützten Plattformen und Adapterkarten finden Sie unter "NetApp Hardware Universe".



Verwandte Informationen

- "Konfigurieren Sie ONTAP FC-Ports für die direkte Verbindung mit FC- und FC-NVMe-Hosts".
- Erfahren Sie, wie "Selektives LUN Mapping (SLM)" die Pfade eingeschränkt werden, die für den Zugriff auf die LUNs eines HA-Paares verwendet werden.

- Informationen dazu "SAN-LIFs".

Best Practices für die FC-Fabric-Konfiguration von ONTAP Systemen

Die Einhaltung bewährter Verfahren bei der FC Fabric Konfiguration verbessert Performance, Zuverlässigkeit und Stabilität von Host und Zielsystem bei Änderungen der Fabric.

Empfohlene Best Practices für die FC Fabric-Konfiguration

- **Single-Initiator / Single-Target (SI/ST)-Zonierung**

  SI/ST Zonierung reduziert Latenzspitzen bei Fabric-Änderungen, beseitigt Übersprechen, begrenzt Registered State Change Notifications (RSCNs), vereinfacht die Fehlersuche und hält die Pfadanzahl innerhalb der Host-Grenzen.

  - Auswirkungen auf den Host: Die SI/ST-Zonierung gewährleistet ein vorhersehbares MPIO-Verhalten, eine schnellere Erkennung und weniger All Path Down (APD)/Permanent Device Loss (PDL)-Ereignisse.
  - Zielwirkung: Die SI/ST-Zonierung gewährleistet weniger An- und Abmeldevorgänge und stabile FC-Sitzungen.

- **WWPN-basierte Zonierung unter Verwendung von Ziel-LIF-WWPNs (nicht physischen Ports)**

  Die WWPN-basierte Zonierung ermöglicht die Mobilität von LIF, Takeover/Giveback, unterbrechungsfreie Abläufe ohne erneute Zonierung und verhindert Pfadresets während der Wartung.

  - Auswirkungen auf den Host: Die WWPN-basierte Zonierung gewährleistet, dass es bei LIF-Verschiebungen oder Controller-Failover zu keinem Pfadverlust kommt.
  - Zielwirkung: Die WWPN-basierte Zonierung gewährleistet, dass ONTAP die Ziel-LIFs transparent verschieben kann.

- **NPIV auf allen FC-Switches aktiviert**

  Alle mit dem Fabric verbundenen Switches müssen NPIV unterstützen, und NPIV muss aktiviert sein. ONTAP verwendet N_Port ID-Virtualisierung (NPIV), um FC-Ziele bereitzustellen. Ohne NPIV können sich Ziel-LIFs nicht korrekt anmelden.

  - Auswirkungen auf den Host: NPIV verhindert zeitweilige Pfadabbrüche und fehlende Geräte.
  - Zielwirkung: NPIV gewährleistet die Transparenz der Ziel-LIFs und stabile FC-Logins.

- **Zwei unabhängige, vollständig isolierte Fabrics**

  Ein duales, unabhängiges Fabric besteht aus zwei separaten physischen Switches, Netzteilen und Verkabelungen. Fabric A und Fabric B sind niemals miteinander verbunden. Jedes Fabric verwaltet seinen eigenen FC-Nameserver, seine eigenen Zonensätze und Domänen-IDs. Da die Fabrics vollständig isoliert sind, gibt es keinen Single Point of Failure. Unterbrechungsfreie Wartungsarbeiten können an einem Fabric durchgeführt werden, während das andere weiter in Betrieb bleibt.

  - Auswirkungen auf den Host: Zwei unabhängige Fabrics unterstützen kontinuierliche E/A bei Firmware-Upgrades oder Ausfällen der Fabric.
  - Zielauswirkung: Zwei unabhängige Fabrics gewährleisten redundanten Zielzugriff bei Switch-Problemen.

- **Feste FC-Portgeschwindigkeiten (automatische Aushandlung vermeiden)**

Die automatische Aushandlung kann den Wiederaufbau der Fabric verzögern, zu Geschwindigkeitsabweichungen führen und Verzögerungen bei der Rekonvergenz sowie Link-Flaps verursachen.

  - Auswirkungen auf den Host: Feste FC Portgeschwindigkeiten führen bei Link-Resets zu kürzeren Ausfallzeiten.
  - Zielwirkung: Feste FC-Portgeschwindigkeiten sorgen dafür, dass die Ports nach Knoten- oder Switch-Ereignissen schneller wieder online kommen.

- **Strenge Einhaltung der von NetApp Interoperability Matrix Tool (IMT) validierten Konfigurationen (HBA, Treiber, Firmware, Switch)**

  Die strikte Einhaltung der im "NetApp IMT" validierten Konfigurationen gewährleistet die erwartete Latenz und den erwarteten Durchsatz.

  - Auswirkungen auf den Host: Durch die Verwendung von durch IMT validierten Konfigurationen lassen sich unerklärliche E/A-Fehler und Timeouts vermeiden.
  - Zielwirkung: Die Verwendung von IMT validierten Konfigurationen verhindert Inkompatibilitäten auf Protokollebene.

- **Proaktive Überwachung der FC-Fehlerzähler (CRC, Synchronisationsverlust, RECV_ERROR)**

  Fabric-Fehler äußern sich häufig als hostseitige Latenz- oder E/A-Fehler, bevor ONTAP Storage-Zähler sie erkennen. Die proaktive Überwachung der FC-Fehleranzahl verhindert einen kontinuierlichen Anstieg der Latenz.

  - Auswirkungen auf den Host: Proaktives Monitoring ermöglicht die frühzeitige Erkennung und verhindert erneute Host-E/A-Versuche sowie Stillstände von Applikationen.
  - Zielwirkung: Proaktives Monitoring verhindert, dass Fabric-Probleme fälschlicherweise Storage Problemen zugeschrieben werden.

- **Vermeidung einer Überbelegung der Inter-Switch-Verbindung (ISL) für SAN-Datenverkehr**

  Überlastete ISLs führen zu Kreditknappheit und Slow-Drain-Verhalten.

  - Auswirkungen auf den Host: Die Vermeidung einer ISL-Überbelegung reduziert Host-E/A-Wartezeiten und die Warteschlangenbildung.
  - Zielwirkung: Die Vermeidung einer ISL-Überbelegung verhindert Rückstau an ONTAP FC-Ports.

Verwandte Informationen

"NetApp Technischer Bericht 4080: Bewährte Verfahren für moderne SAN".

Unterstützte FC-Zielportgeschwindigkeiten für Ihr ONTAP System ermitteln

FC-Zielports können für das FC-NVMe-Protokoll genauso konfiguriert und verwendet werden wie für das FC-Protokoll.

Für optimale Leistung und höchste Verfügbarkeit wird die empfohlene Zielportkonfiguration, die in "NetApp Hardware Universe" für Ihr spezifisches ONTAP System aufgeführt ist, verwendet.

Jeder Onboard FC Port und jeder Erweiterungsadapter Port kann individuell für unterschiedliche, unterstützte Geschwindigkeiten konfiguriert werden. Die unterstützten Geschwindigkeiten variieren je nach ONTAP System und HBAs. Alle von einem Host verwendeten Zielports sollten auf dieselbe Geschwindigkeit eingestellt sein.

Es empfiehlt sich, für alle Ihre Initiator-, Switch- und Zielports eine einheitliche Geschwindigkeit zu konfigurieren. Wenn die Geschwindigkeiten von Port und Initiator unterschiedlich sind und keine gemeinsame Geschwindigkeit ausgehandelt werden kann, kann keine Sitzung hergestellt werden. Die Verwendung der automatischen Aushandlung zur Festlegung der Portgeschwindigkeit wird nicht empfohlen. Die automatische Aushandlung kann den Sitzungsaufbau und die Wiederherstellung nach einer Unterbrechung verlangsamen.

Die unterstützten Geschwindigkeiten sind im NetApp Hardware Universe unter **Unterstützte Adapterkarten** für jedes ONTAP System aufgeführt.

Schritte

1. Zu "NetApp Hardware Universe" wechseln.
2. **Produkte** auswählen.
3. Unter **Plattformen** den Systemtyp auswählen.
4. Wählen Sie Ihr spezifisches System und anschließend Ihre ONTAP Version.
5. **Ergebnisse anzeigen** auswählen und dann **Unterstützte Adapterkarten** auswählen.

   FC-Adapterkarten sind unter **Category** als „Block Access (Target)“ aufgeführt, und die unterstützten Geschwindigkeiten sind unter **Supported Protocol(s)** aufgeführt.

Vermeidung von Verbindungsverlusten mit einem X1133A-R6 Adapter auf ONTAP Systemen

Ein Verbindungsverlust während eines Portausfalls lässt sich verhindern, wenn das System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfiguriert ist.

Der X1133A-R6 HBA ist ein 4-Port 16-Gb-FC-Adapter, bestehend aus zwei 2-Port-Paaren. Der X1133A-R6 Adapter kann im Target-Modus oder Initiator-Modus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (zum Beispiel Port 1 und Port 2 auf ASIC 1 sowie Port 3 und Port 4 auf ASIC 2). Beide Ports eines einzelnen ASIC müssen im selben Modus betrieben werden, entweder im Target-Modus oder im Initiator-Modus. Tritt ein Fehler bei dem ASIC auf, der ein Paar unterstützt, gehen beide Ports des Paares offline.

Um diesen Verbindungsverlust zu verhindern, wird das System mit redundanten Pfaden zu separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden, konfiguriert.

FCoE Konfigurationen

FCoE-Fabric-Konfigurationen für ONTAP Systeme

FCoE kann mithilfe von FCoE Switches auf verschiedene Weise konfiguriert werden. Direkt angeschlossene Konfigurationen werden in FCoE nicht unterstützt.

Alle FCoE Konfigurationen sind dual-fabric, vollständig redundant und erfordern Multipathing-Software auf Host-Seite. In allen FCoE Konfigurationen können mehrere FCoE und FC Switches im Pfad zwischen Initiator und Ziel vorhanden sein, bis zur maximalen Hop-Anzahl. Um Switches miteinander zu verbinden, muss 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.

FCoE-Konfigurationen erfordern Ethernet-Switches, die FCoE-Funktionen explizit unterstützen. FCoE-Konfigurationen werden durch dasselbe Interoperabilitäts- und Qualitätssicherungsverfahren wie FC-Switches validiert. Unterstützte Konfigurationen sind in der Interoperabilitätsmatrix aufgeführt. Zu den Parametern dieser

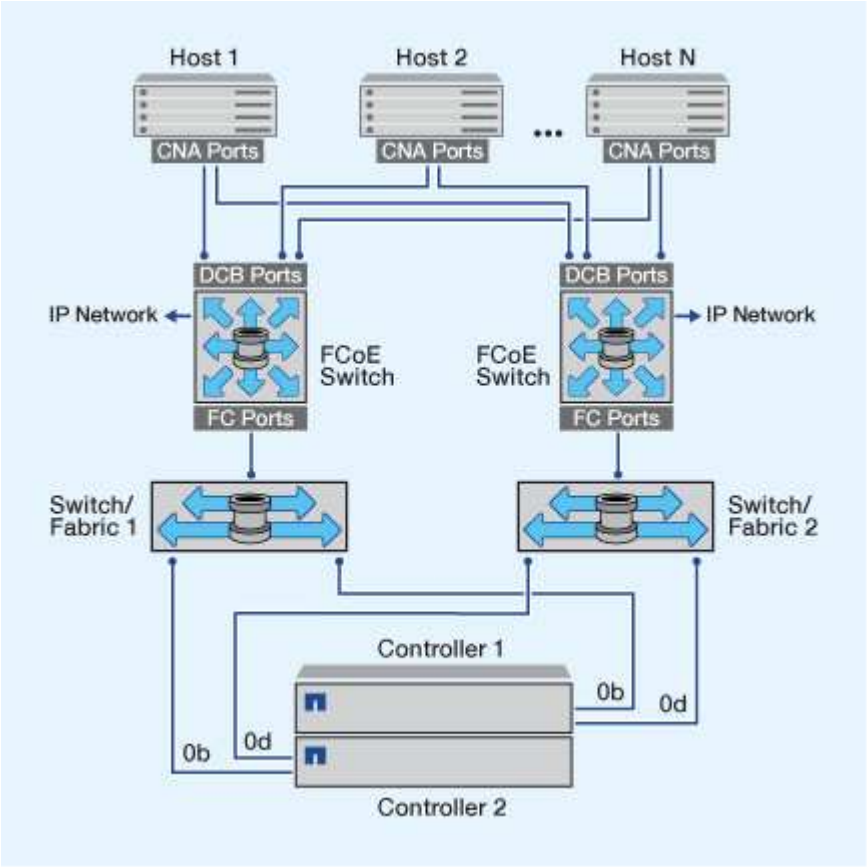
unterstützten Konfigurationen gehören das Switch-Modell, die Anzahl der Switches, die in einem einzelnen Fabric eingesetzt werden können, und die unterstützte Switch-Firmware-Version.

Die in den Abbildungen angegebenen Portnummern der FC-Zielerweiterungsadapter sind Beispiele. Die tatsächlichen Portnummern können je nach den Erweiterungssteckplätzen, in denen die FCoE-Zielerweiterungsadapter installiert sind, variieren.

FCoE-Initiator zu FC-Ziel

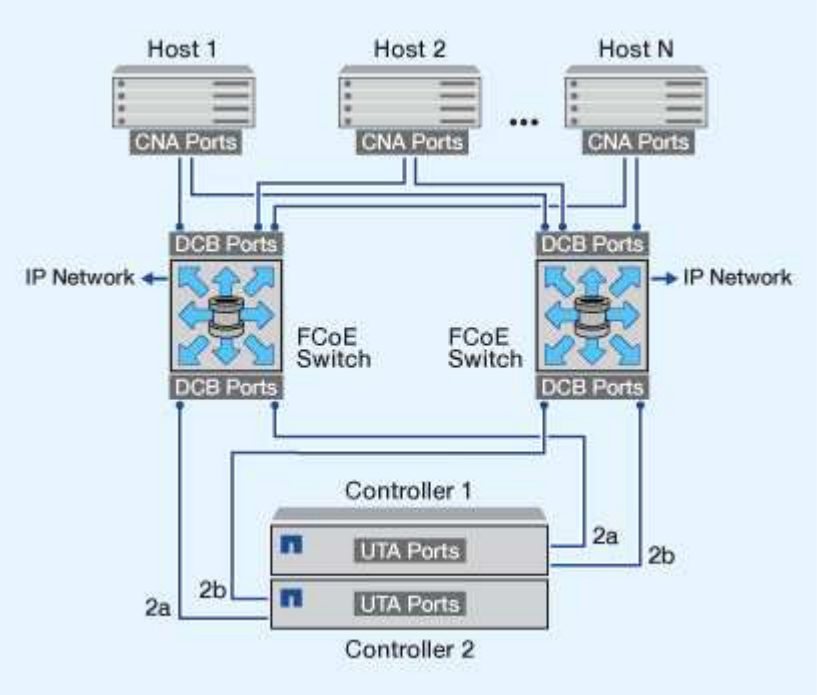
Mithilfe von FCoE-Initiatoren (CNAs) können Hosts über FCoE-Switches mit beiden Controllern in einem HA-Paar zu FC-Zielports verbunden werden. Der FCoE-Switch muss ebenfalls über FC-Ports verfügen. Der Host-FCoE-Initiator ist immer mit dem FCoE-Switch verbunden. Der FCoE-Switch kann entweder direkt mit dem FC-Ziel verbunden sein oder über FC-Switches mit dem FC-Ziel verbunden werden.

Die folgende Abbildung zeigt Host-CNAs, die sich mit einem FCoE Switch und dann mit einem FC Switch verbinden, bevor sie mit dem HA-Paar verbunden werden:



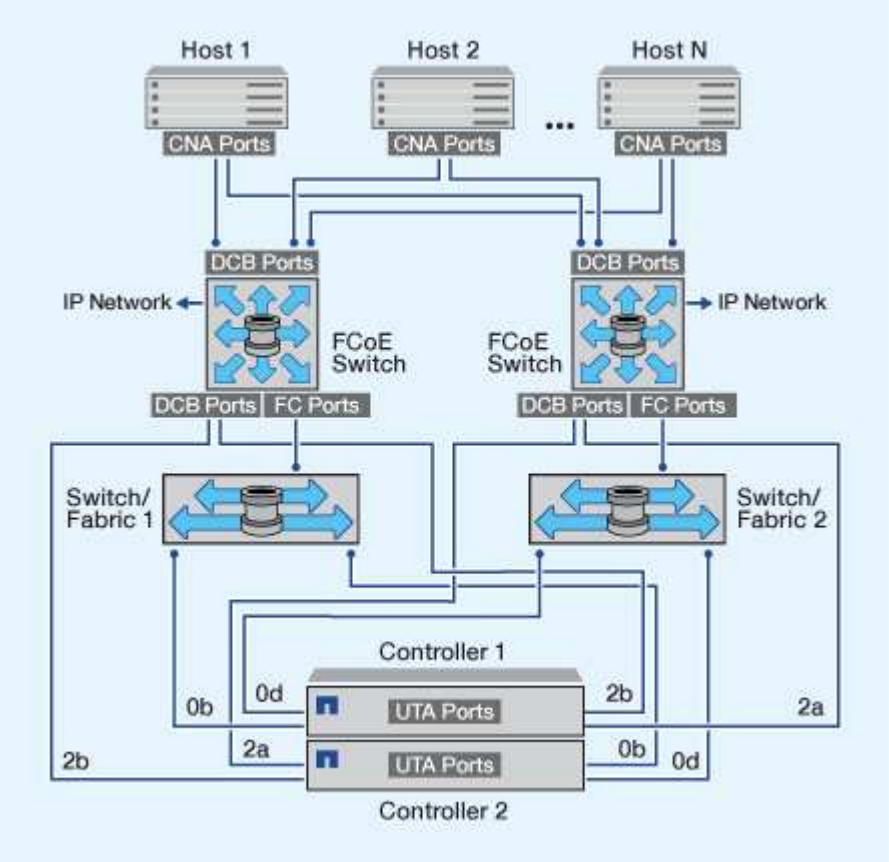
FCoE-Initiator zu FCoE-Target

Mithilfe von Host-FCoE-Initiatoren (CNAs) können Hosts mit beiden Controllern eines HA-Paares über FCoE-Switches mit FCoE-Zielports (auch UTAs oder UTA2s genannt) verbunden werden.



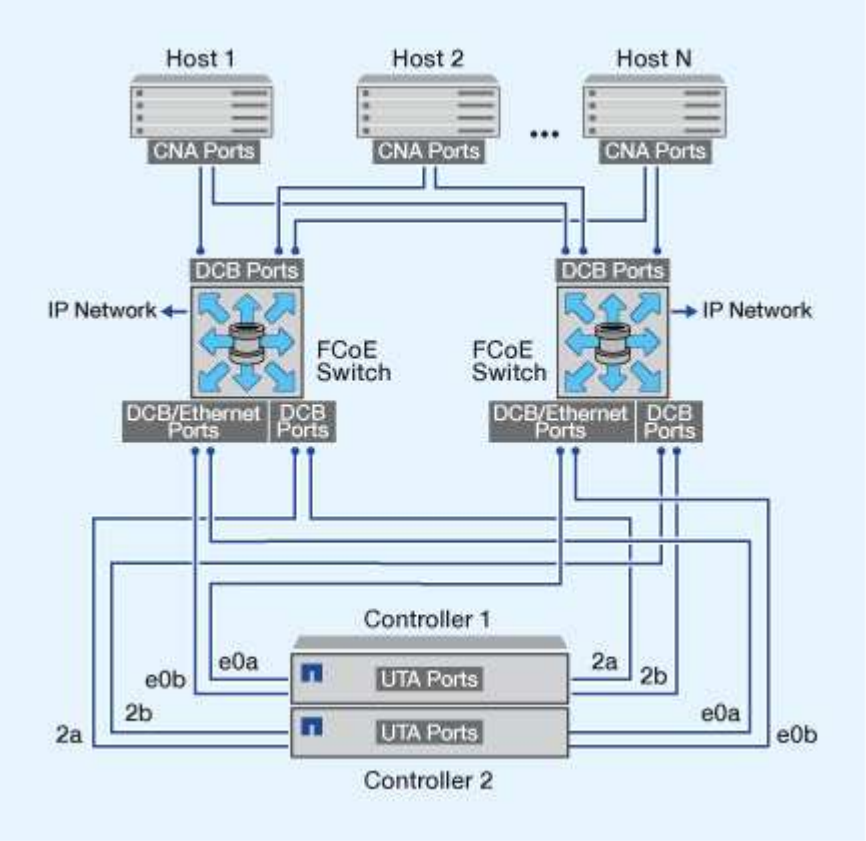
FCoE-Initiator zu FCoE- und FC-Zielen

Mit Host-FCoE-Initiatoren (CNAs) ist eine Verbindung von Hosts zu beiden Controllern in einem HA-Paar mit FCoE- und FC-Zielports (auch UTAs oder UTA2s genannt) über FCoE-Switches möglich.



FCoE gemischt mit IP-Speicherprotokollen

Mithilfe von Host-FCoE-Initiatoren (CNAs) können Hosts mit beiden Controllern eines HA-Paares über FCoE-Switches mit FCoE-Zielports (auch UTAs oder UTA2s genannt) verbunden werden. FCoE-Ports können keine herkömmliche Link-Aggregation zu einem einzelnen Switch verwenden. Cisco Switches unterstützen eine spezielle Art der Link-Aggregation (Virtual Port Channel), die FCoE unterstützt. Ein Virtual Port Channel aggregiert einzelne Verbindungen zu zwei Switches. Virtual Port Channels können auch für anderen Ethernet-Datenverkehr verwendet werden. Ports, die für anderen Datenverkehr als FCoE verwendet werden, einschließlich NFS, SMB, iSCSI und anderem Ethernet-Datenverkehr, können reguläre Ethernet-Ports an den FCoE-Switches verwenden.



ONTAP unterstützte FCoE Initiator- und Zielportkombinationen

Bestimmte Kombinationen von FCoE- und traditionellen FC-Initiatoren und -Targets werden unterstützt.

FCoE Initiatoren

FCoE-Initiatoren können in Host-Computern mit sowohl FCoE- als auch herkömmlichen FC-Targets in Speicherkontrollern verwendet werden. Der Host-FCoE-Initiator muss mit einem FCoE-DCB-Switch (Data Center Bridging) verbunden sein, eine direkte Verbindung zu einem Target wird nicht unterstützt.

Die folgende Tabelle listet die unterstützten Kombinationen auf:

Initiator	Ziel	Unterstützt?
FC	FC	Ja
FC	FCoE	Ja

Initiator	Ziel	Unterstützt?
FCoE	FC	Ja
FCoE	FCoE	Ja

FCoE Ziele

Sie können FCoE-Zielports mit 4-Gb, 8-Gb oder 16-Gb FC-Ports auf dem Storage Controller kombinieren, unabhängig davon, ob die FC-Ports Add-in-Zieladapter oder Onboard-Ports sind. Sowohl FCoE- als auch FC-Zieladapter können im selben Storage Controller vorhanden sein.

Die Regeln für die Kombination von Onboard FC-Ports und Erweiterungs FC-Ports gelten weiterhin.

FC- und FCoE-Zonierung

Informationen zu FC- und FCoE-Zoning mit ONTAP Systemen

Eine FC-, FC-NVMe- oder FCoE-Zone ist eine logische Gruppierung eines oder mehrerer Ports innerhalb eines Fabric. Damit Geräte einander sehen, sich verbinden, Sitzungen miteinander aufbauen und kommunizieren können, müssen beide Ports Mitglieder derselben Zone sein.

Die Zoneneinteilung erhöht die Sicherheit, indem der Zugriff und die Konnektivität auf Endpunkte innerhalb einer gemeinsamen Zone beschränkt werden. Ports, die sich nicht in derselben Zone befinden, können nicht miteinander kommunizieren. Dadurch wird das Übersprechen zwischen Initiator-HBAs reduziert oder eliminiert. Treten Verbindungsprobleme auf, trägt die Zoneneinteilung dazu bei, die Probleme auf eine bestimmte Gruppe von Ports einzugrenzen, wodurch die Lösungszeit verkürzt wird.

Zoning reduziert die Anzahl der verfügbaren Pfade zu einem bestimmten Port und die Anzahl der Pfade zwischen einem Host und dem Speichersystem. Beispielsweise haben einige Multipathing-Lösungen von Host-Betriebssystemen eine Begrenzung hinsichtlich der Anzahl der Pfade, die sie verwalten können. Zoning kann die Anzahl der für den Host sichtbaren Pfade so verringern, dass die Pfade zum Host die vom Host-Betriebssystem maximal erlaubte Anzahl nicht überschreiten.

World Wide Name-basierte Zoneneinteilung

Die Zoneneinteilung basierend auf dem World Wide Name (WWN) legt die WWNs der in die Zone einzuschließenden Mitglieder fest. Obwohl die Zoneneinteilung basierend auf dem World Wide Node Name (WWNN) bei einigen Switch-Herstellern möglich ist, muss bei der Zoneneinteilung in ONTAP die Zoneneinteilung basierend auf dem World Wide Port Name (WWPN) verwendet werden.

Die WWPN-Zonierung ist erforderlich, um einen bestimmten Port korrekt zu definieren und NPIV effektiv zu nutzen. FC-Switches sollten anhand der WWPNs der logischen Schnittstellen (LIFs) des Ziels zoniert werden, nicht anhand der WWPNs der physischen Ports des Knotens. Die WWPNs der physischen Ports beginnen mit „50“ und die WWPNs der LIFs beginnen mit „20“.

Die WWPN-Zonierung bietet Flexibilität, da der Zugriff nicht davon abhängt, wo das Gerät physisch mit dem Fabric verbunden ist. Ein Kabel kann von einem Port auf einen anderen umgesteckt werden, ohne die Zonen neu konfigurieren zu müssen.

Empfohlene FC- und FCoE-Zoning-Konfigurationen für ONTAP Systeme

Eine Zoning-Konfiguration ist erforderlich, wenn auf Ihrem Host keine Multipathing-Lösung installiert ist, wenn vier oder mehr Hosts mit Ihrem SAN verbunden sind oder wenn Selective LUN Mapping auf den Knoten in Ihrem Cluster nicht implementiert ist.

In der empfohlenen FC- und FCoE Zoning-Konfiguration umfasst jede Zone einen Initiator-Port und einen oder mehrere Ziel-LIFs. Diese Konfiguration ermöglicht jedem Host-Initiator den Zugriff auf jeden Knoten, verhindert jedoch, dass Hosts, die auf denselben Knoten zugreifen, die Ports der jeweils anderen sehen.

Alle LIFs der Storage Virtual Machine (SVM) zur Zone mit dem Host-Initiator hinzufügen. So ist es möglich, Volumes oder LUNs zu verschieben, ohne die bestehenden Zonen zu bearbeiten oder neue Zonen zu erstellen.

Dual-fabric Zoning-Konfigurationen

Dual-fabric Zoning-Konfigurationen werden empfohlen, da sie Schutz vor Datenverlust durch den Ausfall einer einzelnen Komponente bieten. In einer Dual-fabric Konfiguration ist jeder Host-Initiator über unterschiedliche Switches mit jedem Knoten im Cluster verbunden. Fällt ein Switch aus, bleibt der Datenzugriff über den verbleibenden Switch erhalten. Auf dem Host ist Multipathing-Software erforderlich, um mehrere Pfade zu verwalten.

In der folgenden Abbildung verfügt der Host über zwei Initiatoren und verwendet Multipathing Software. Es gibt zwei Zonen. "Selektives LUN Mapping (SLM)" ist so konfiguriert, dass alle Knoten als meldende Knoten gelten.

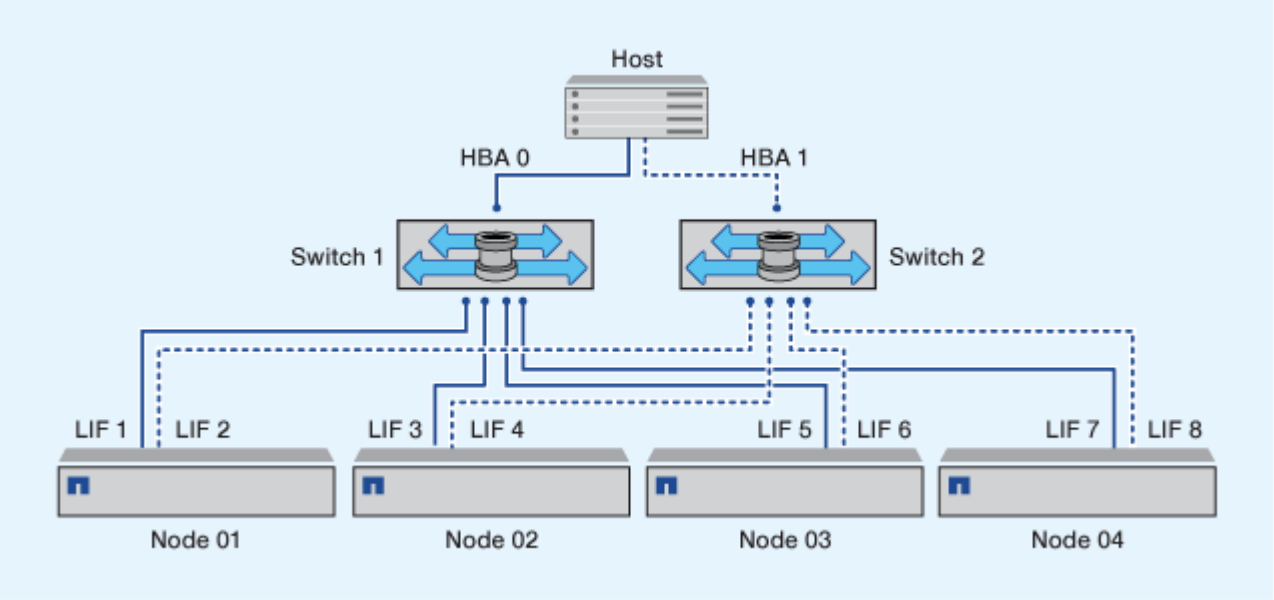
> Die in dieser Abbildung verwendete Namenskonvention ist lediglich eine Empfehlung für eine mögliche Namenskonvention, die für Ihre ONTAP Lösung gewählt werden kann.

- 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 ist über einen separaten Switch angebunden. Zone 1 ist über Switch 1 zugänglich. Zone 2 ist über Switch 2 zugänglich.

Jeder Host kann auf eine LIF auf jedem Knoten zugreifen. Dadurch ist weiterhin der Zugriff des Hosts auf seine LUNs möglich, falls ein Knoten ausfällt. SVMs haben Zugriff auf alle iSCSI- und FC-LIFs auf jedem Knoten im Cluster, basierend auf Ihrer SLM-Meldeknoten-Konfiguration. SLM, Portsets oder FC-Switch-Zoning können verwendet werden, um die Anzahl der Pfade von einer SVM zum Host und von einer SVM zu einer LUN zu reduzieren.

Wenn die Konfiguration mehr Knoten umfasst, sind die LIFs für die zusätzlichen Knoten in diesen Zonen enthalten.



Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der Pfade unterstützen, die für den Zugriff auf die LUNs auf den Knoten verwendet wird.

Single-fabric-Zoning

In einer Single Fabric-Konfiguration wird jeder Host-Initiator über einen einzelnen Switch mit jedem Speicherknoten verbunden. Single Fabric Zoning-Konfigurationen werden nicht empfohlen, da sie keinen Schutz vor Datenverlust durch den Ausfall einer einzelnen Komponente bieten. Falls eine Single Fabric Zoning-Konfiguration gewählt wird, sollte jeder Host über zwei Initiatoren für Multipathing verfügen, um die Ausfallsicherheit der Lösung zu gewährleisten. Auf dem Host ist Multipathing-Software erforderlich, um mehrere Pfade zu verwalten.

Jeder Host-Initiator sollte mindestens eine LIF von jedem Knoten haben, auf den er zugreifen kann. Die Zonierung sollte mindestens einen Pfad vom Host-Initiator zum HA-Paar von Knoten im Cluster ermöglichen, um einen Pfad für die LUN-Konnektivität bereitzustellen. Das bedeutet, dass jeder Initiator auf dem Host in seiner Zoning-Konfiguration möglicherweise nur eine Ziel-LIF pro Knoten hat. Besteht die Anforderung für Multipathing zum selben Knoten oder zu mehreren Knoten im Cluster, hat dann jeder Knoten mehrere LIFs pro Knoten in seiner Zoning-Konfiguration. So kann der Host weiterhin auf seine LUNs zugreifen, falls ein Knoten ausfällt oder ein Volume mit der LUN auf einen anderen Knoten verschoben wird. Dazu müssen die Reporting-Knoten entsprechend eingestellt sein.

Bei Verwendung von Cisco FC- und FCoE-Switches darf eine einzelne Fabric-Zone nicht mehr als eine Ziel-LIF für denselben physischen Port enthalten. Befinden sich mehrere LIFs auf demselben Port in derselben Zone, können die LIF-Ports möglicherweise nach einem Verbindungsverlust nicht wiederhergestellt werden.

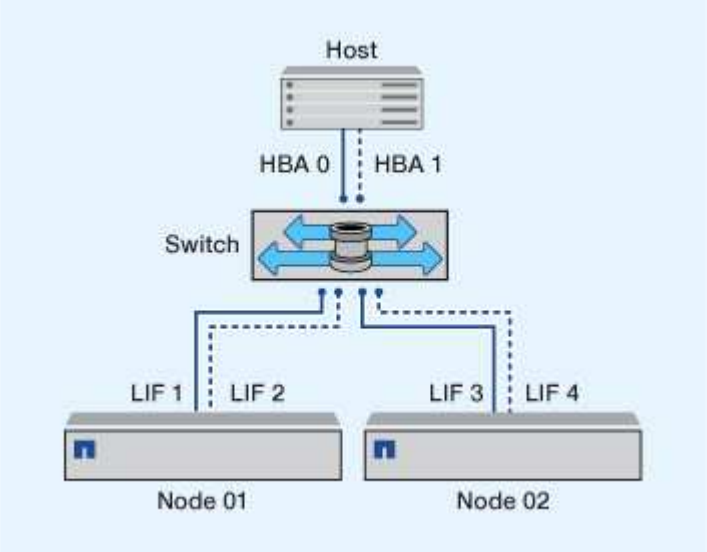
In der folgenden Abbildung verfügt der Host über zwei Initiatoren und verwendet Multipathing Software. Es gibt zwei Zonen:

Die in dieser Abbildung verwendete Namenskonvention ist lediglich eine Empfehlung für eine mögliche Namenskonvention, die für Ihre ONTAP Lösung gewählt werden kann.

- Zone 1: HBA 0, LIF_1 und LIF_3
- Zone 2: HBA 1, LIF_2 und LIF_4

Wenn die Konfiguration mehr Knoten umfasst, werden die LIFs für die zusätzlichen Knoten in diese Zonen

aufgenommen.



In diesem Beispiel könnten Sie auch alle vier LIFs in jeder Zone haben. 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, die für den Zugriff auf die LUNs auf den Knoten verwendet werden, unterstützen. Zur Ermittlung der Anzahl der Pfade, die für den Zugriff auf die LUNs auf den Knoten verwendet werden, siehe den Abschnitt zu den SAN-Konfigurationsgrenzen.

Zonenbeschränkungen für Cisco FC und FCoE Switches

Bei der 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 32 Gb-physikalischen Port gemeinsam nutzen.
- FC-NVMe und FCoE können nicht denselben physischen Port verwenden.
- FC und FCoE können denselben physischen Port nutzen, aber ihre Protokoll-LIFs müssen in separaten Zonen sein.

Logische Schnittstellen (LIFs)

- Eine Zone kann eine LIF von jedem Zielport im Cluster enthalten.

  Die SLM-Konfiguration sollte so überprüft werden, dass die maximal zulässige Anzahl von Pfaden zum Host nicht überschritten wird.

- Jeder LIF an einem bestimmten Port muss sich in einer separaten Zone von anderen LIFs an diesem Port befinden
- LIFs auf verschiedenen physischen Ports können in derselben Zone sein.

Anforderungen an SAN-Hosts, die mit ONTAP und Nicht-NetApp-Systemen verbunden sind

Gemeinsam genutzte SAN-Konfigurationen sind Hosts, die sowohl an ONTAP Speichersysteme als auch an Speichersysteme anderer Hersteller angeschlossen sind. Der Zugriff auf ONTAP Speichersysteme und Speichersysteme anderer Hersteller von einem einzelnen Host aus wird unterstützt, sofern bestimmte Voraussetzungen erfüllt sind.

Für alle Host-Betriebssysteme ist es eine Best Practice, separate Adapter für die Verbindung zu den Speichersystemen der jeweiligen Hersteller zu verwenden. Die Verwendung separater Adapter verringert die Wahrscheinlichkeit von Treiber- und Einstellungskonflikten. Für Verbindungen zu einem ONTAP-Speichersystem müssen Adaptermodell, BIOS, Firmware und Treiber im NetApp Interoperability Matrix Tool als unterstützt aufgeführt sein.

Sie sollten die erforderlichen oder empfohlenen Zeitüberschreitungswerte und andere Speicherparameter für den Host festlegen. Die NetApp Software muss immer zuletzt installiert bzw. die NetApp Einstellungen zuletzt angewendet werden.

- Für AIX sind die Werte aus der AIX Host Utilities Version zu verwenden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.
- Für ESX sollten Sie die Host-Einstellungen mithilfe von ONTAP tools for VMware vSphere anwenden.
- Für HP-UX sind die HP-UX Standardspeichereinstellungen zu verwenden.
- Für Linux sind die Werte aus der Linux Host Utilities Version zu verwenden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.
- Für Solaris sind die Werte aus der Solaris Host Utilities Version zu verwenden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.
- Für Windows sollte die Version von Windows Host Utilities installiert werden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

SAN-Konfigurationen in einer MetroCluster Umgebung

Unterstützte SAN-Konfigurationen in einer ONTAP MetroCluster Umgebung

Bei der Verwendung von SAN Konfigurationen in einer MetroCluster Umgebung sind bestimmte Aspekte zu berücksichtigen.

- MetroCluster Konfigurationen unterstützen keine Frontend-FC-Fabric-“routed”-vSAN-Konfigurationen.
- Ab ONTAP 9.15.1 werden Vier-Knoten MetroCluster IP-Konfigurationen auf NVMe/TCP unterstützt.
- Ab ONTAP 9.12.1 werden vier Knoten MetroCluster IP-Konfigurationen auf NVMe/FC unterstützt. MetroCluster Konfigurationen werden für Frontend-NVMe-Netzwerke vor ONTAP 9.12.1 nicht unterstützt.
- Andere SAN-Protokolle wie iSCSI, FC und FCoE werden in MetroCluster Konfigurationen unterstützt.
- Bei der Verwendung von SAN-Clientkonfigurationen ist zu prüfen, ob besondere Hinweise für MetroCluster-Konfigurationen in den Anmerkungen im "NetApp Interoperabilitätsmatrix-Tool" (IMT) enthalten sind.

- Betriebssysteme und Anwendungen müssen eine I/O-Resilienz von 120 Sekunden bereitstellen, um MetroCluster automatische ungeplante Umschaltungen sowie durch Tiebreaker oder Mediator initiierte Umschaltungen zu unterstützen.
- MetroCluster Konfigurationen verwenden auf beiden Seiten des Frontend-FC-Fabrics die gleichen WWNNs und WWPNs.

Verwandte Informationen

- "Verständnis von MetroCluster Datenschutz und Notfallwiederherstellung"
- "NetApp Knowledge Base: Welche Aspekte der AIX-Hostunterstützung sind in einer MetroCluster Konfiguration zu beachten?"
- "NetApp Knowledge Base: Überlegungen zur Solaris-Hostunterstützung in einer MetroCluster Konfiguration"

Portüberschneidungen während ONTAP MetroCluster Switchover und Switchback vermeiden

In einer SAN-Umgebung können die Frontend-Switches so konfiguriert werden, dass Überlappungen vermieden werden, wenn der alte Port offline geht und der neue Port online geht.

Während der Umschaltung kann es vorkommen, dass sich der FC-Port am verbleibenden Standort beim Fabric anmeldet, bevor das Fabric erkennt, dass der FC-Port am betroffenen Standort offline ist und diesen Port aus den Namens- und Verzeichnisdiensten entfernt hat.

Wenn der FC-Port am betroffenen Standort noch nicht entfernt wurde, kann der Anmeldeversuch des FC-Ports am verbleibenden Standort aufgrund einer doppelten WWPN abgelehnt werden. Dieses Verhalten der FC-Switches kann so geändert werden, dass die Anmeldung des vorherigen Geräts und nicht die des aktuellen Geräts berücksichtigt wird. Die Auswirkungen dieses Verhaltens auf andere Fabric-Geräte sollten überprüft werden. Für weitere Informationen ist der Switch-Hersteller zu kontaktieren.

Wählen Sie das richtige Verfahren entsprechend Ihrem Switch-Typ.

Beispiel 9. Schritte

Cisco Switch

1. Stellen Sie eine Verbindung zum Switch her und melden Sie sich an.
2. In den Konfigurationsmodus wechseln:

```
switch# config t
switch(config)#
```

3. Der erste Geräteeintrag in der Name-Server-Datenbank wird mit dem neuen Gerät überschrieben:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Bei Switches, auf denen NX-OS 8.x läuft, ist zu bestätigen, dass das flogi quiesce Zeitüberschreitung auf Null gesetzt ist:

   a. Den Ruhetimer anzeigen:

```
switch(config)# show flogi interval info \| i quiesce
```

```
Stats:  fs flogi quiesce timerval:  0
```

b. Falls die Ausgabe im vorherigen Schritt nicht anzeigt, dass timerval null ist, sollte er auf null gesetzt werden:

```
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. Den `switchDisable`Befehl eingeben.
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 restlichen Eingabeaufforderungen oder drücken Sie **Strg + D**.
6. Den `switchEnable`Befehl eingeben.

Verwandte Informationen

"Umschaltung für Tests oder Wartungsarbeiten"

ONTAP Unterstützung für SAN Host Multipathing

ONTAP verwendet Asymmetric Logical Unit Access (ALUA) Software für Multipathing mit sowohl FC- als auch iSCSI-Hosts.

Ab ONTAP 9.5 wird Multipath-Hochverfügbarkeit (HA) mit Failover/Giveback für NVMe-Hosts über Asynchronous Namespace Access (ANA) unterstützt. In ONTAP 9.4 unterstützt NVMe nur einen Pfad vom Host zum Ziel, daher muss der Anwendungshost das Pfad-Failover zu seinem HA-Partner verwalten.

Informationen darüber, welche spezifischen Hostkonfigurationen ALUA oder ANA unterstützen, finden sich in der "NetApp Interoperabilitätsmatrix-Tool" und "ONTAP SAN Hostkonfiguration" für Ihr Host-Betriebssystem.

Multipathing-Software, auch bekannt als MPIO (Multipath I/O), wird für HA-Konfigurationen empfohlen. Die Multipathing-Software ist auf Ihrem SAN-Host erforderlich, damit dieser über mehrere Pfade auf eine LUN oder einen NVMe-Namespace zugreifen kann. Sie stellt dem Betriebssystem für alle Pfade zu einer LUN oder

einem NVMe-Namespace eine einzige Festplatte bereit. Ohne sie könnte das Betriebssystem jeden Pfad als separate Festplatte behandeln, was zu Datenbeschädigung führen kann.

Ihre Lösung gilt als mehrpfadig, wenn eine der folgenden Bedingungen erfüllt ist:

- Ein einzelner Initiator-Port im Host, der mit mehreren SAN-LIFs in der SVM verbunden ist
- Mehrere Initiator-Ports sind an eine einzelne SAN LIF in der SVM angeschlossen.
- Mehrere Initiator-Ports, die mit mehreren SAN-LIFs in der SVM verbunden sind

Sie sollten Selective LUN Map, FC-Switch-Zoning oder Portsets verwenden, um die Pfade für den Zugriff auf LUNs und Namespaces einzuschränken.

Verwandte Informationen

Informationen dazu "Von ONTAP unterstützte SAN-Multipath-Konfigurationen".

Empfohlene Anzahl von Pfaden vom Host zu den Knoten im Cluster

Sie sollten nicht mehr als acht Pfade von Ihrem Host zu jedem Knoten in Ihrem Cluster verwenden. Sie sollten außerdem die Gesamtzahl der Pfade, die vom Host-Betriebssystem und dem auf dem Host verwendeten Multipathing unterstützt werden, nicht überschreiten.

Wenn Ihr Cluster vier oder mehr Knoten umfasst oder die SVMs auf einem Ihrer Knoten mehr als vier Zielports verwenden, können die folgenden Methoden eingesetzt werden, um die Anzahl der Pfade, über die auf LUNs auf Ihren Knoten zugegriffen werden kann, so zu begrenzen, dass das empfohlene Maximum von acht Pfaden nicht überschritten wird.

- "Selective LUN Map (SLM)"

  SLM reduziert die Anzahl der Pfade vom Host zur LUN auf nur Pfade auf dem Knoten, dem die LUN gehört, und dem HA-Partner des Eigentümerknotens. SLM ist standardmäßig aktiviert. Sie sollten mindestens zwei Pfade pro LUN haben, die zu jedem meldenden Knoten führen und durch SLM von der Storage Virtual Machine (SVM) in Ihrem Cluster verwendet werden. Dadurch werden Single Points of Failure eliminiert und das System kann Komponentenausfälle überstehen.

- "Port-Sets"

  Portsets können in Verbindung mit SLM verwendet werden, um den Zugriff bestimmter Ziele auf bestimmte Initiatoren weiter einzuschränken. Bei Verwendung von SLM mit Portsets sind LUNs auf der Menge der LIFs im Portset auf dem Node, dem die LUN gehört, und auf dem HA-Partner dieses Nodes zugänglich.

- Initiatorgruppen-Zuordnungen (igroup) von Ihrem Host

  Es besteht die Möglichkeit, igroups zu definieren und sie LUNs zuzuordnen, um zu steuern, welche Initiatoren Zugriff auf LUNs erhalten.

- "FC Switch-Zonierung"

  Sie sollten eine Zoning-Konfiguration erstellen, wenn auf Ihrem Host keine Multipathing-Lösung installiert ist, wenn vier oder mehr Hosts mit Ihrem SAN verbunden sind oder wenn SLM auf den Knoten in Ihrem Cluster nicht implementiert ist.

Konfigurationsgrenzen

Maximal unterstützte Knoten und SAN-Hosts pro ONTAP Cluster bestimmen

Die Anzahl der unterstützten Knoten pro Cluster variiert je nach Ihrer ONTAP-Version, Ihren Controller-Modellen und dem Protokoll Ihrer Clusterknoten. Die maximale Anzahl von SAN-Hosts, die an einen Cluster angeschlossen werden können, variiert ebenfalls abhängig von Ihrer spezifischen Konfiguration.

Maximal unterstützte Anzahl an Knoten pro Cluster bestimmen

Wenn ein Knoten im Cluster für FC, FC-NVMe, FCoE oder iSCSI konfiguriert ist, unterliegt der Cluster den SAN-Knotenlimits. Knotenlimits basierend auf den Controllern in Ihrem Cluster sind im *Hardware Universe* aufgeführt.

Schritte

1. Gehe zu "NetApp Hardware Universe".
2. Oben links, neben **Home**, **Plattformen** auswählen und anschließend den Plattformtyp auswählen.
3. Wählen Sie Ihre Version von ONTAP.

   Es wird eine neue Spalte angezeigt, in der Sie Ihre Plattformen auswählen können.
4. Die in Ihrer Lösung verwendeten Plattformen auswählen.
5. Unter **Wählen Sie Ihre Spezifikationen** die Auswahl von **Alle auswählen** aufheben.
6. **Maximale Anzahl Knoten pro Cluster (NAS/SAN)** auswählen.
7. Auf **Ergebnisse anzeigen** klicken.

Ergebnisse

Die maximale Anzahl an Knoten pro Cluster für Ihre ausgewählten Plattformen wird angezeigt.

Es kann festgestellt werden, ob Ihr Cluster mehr FC Hosts unterstützen kann.

Bei FC- und FC-NVMe-Konfigurationen sollte die Anzahl der Initiator-Target-Nexus (ITNs) in Ihrem System verwendet werden, um zu bestimmen, ob weitere Hosts zu Ihrem Cluster hinzugefügt werden können.

Ein ITN repräsentiert einen Pfad vom Initiator des Hosts zum Ziel des Speichersystems. Die maximale Anzahl von ITNs pro Knoten in FC und FC-NVMe Konfigurationen beträgt 2.048. Wenn die maximale Anzahl von ITNs noch nicht erreicht ist, können dem Cluster weiterhin Hosts hinzugefügt werden.

Um die Anzahl der in Ihrem Cluster verwendeten ITNs zu ermitteln, sind für jeden Knoten im Cluster die folgenden Schritte auszuführen.

Schritte

1. Alle LIFs auf einem bestimmten Knoten identifizieren.
2. Führen Sie für jede LIF auf dem Node den folgenden Befehl aus:

   ```
   fcp initiator show -fields wwpn, lif
   ```

   Die Anzahl der am unteren Rand der Befehlsausgabe angezeigten Einträge entspricht Ihrer Anzahl an

ITNs für diesen LIF.

3. Die Anzahl der für jedes LIF angezeigten ITNs wird festgehalten.
4. Die Anzahl der ITNs für jedes LIF auf jedem Knoten im Cluster addieren.

   Diese Gesamtzahl stellt die Anzahl der ITNs in Ihrem Cluster dar.

Es wird festgestellt, ob Ihr Cluster mehr iSCSI Hosts unterstützen kann.

Die Anzahl der Hosts, die direkt an einen Knoten oder über einen oder mehrere Switches angeschlossen werden können, hängt von der Anzahl der verfügbaren Ethernet-Ports ab. Die Anzahl der verfügbaren Ethernet-Ports wird durch das Modell des Controllers sowie 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 Clusterkonfigurationen mit mehreren Knoten muss die Anzahl der iSCSI-Sitzungen pro Knoten ermittelt werden, um festzustellen, ob weitere Hosts zu Ihrem Cluster hinzugefügt werden können. Solange Ihr Cluster unter der maximalen Anzahl an iSCSI-Sitzungen pro Knoten bleibt, können weiterhin Hosts zu Ihrem Cluster hinzugefügt werden. Die maximale Anzahl an iSCSI-Sitzungen pro Knoten variiert je nach den Controllertypen in Ihrem Cluster.

Schritte

1. Alle Zielportalgruppen auf dem Node identifizieren.
2. Die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten prüfen:

   ```
   iscsi session show -tpgroup _tpgroup_
   ```

   Die Anzahl der Einträge am Ende der Befehlsausgabe entspricht der Anzahl Ihrer iSCSI-Sitzungen für diese Zielportalgruppe.

3. Die Anzahl der für jede Zielportalgruppe angezeigten iSCSI-Sitzungen wird erfasst.
4. Die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten addieren.

   Die Gesamtzahl stellt die Anzahl der iSCSI-Sitzungen auf Ihrem Knoten dar.

ONTAP ASA Konfigurationsgrenzen und Unterstützung

Die Konfigurationsgrenzen und die Unterstützung für All-Flash SAN Array (ASA) variieren je nach ONTAP Version.

Die aktuellsten Informationen zu den unterstützten Konfigurationsgrenzen sind in "NetApp Hardware Universe" verfügbar.

> 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) besitzen, siehe "ASA r2 System-Speichergrenzen".

SAN-Protokolle und unterstützte Anzahl von Nodes pro Cluster

Die unterstützten SAN-Protokolle und die maximale Anzahl von Knoten pro Cluster hängen davon ab, ob eine nicht MetroCluster oder MetroCluster Konfiguration vorliegt:

Nicht-MetroCluster Konfigurationen

Die folgende Tabelle zeigt die ASA Unterstützung für SAN-Protokolle und die unterstützte Anzahl von Knoten pro Cluster in Nicht-MetroCluster Konfigurationen:

Beginnend mit ONTAP…	Protokollunterstützung	Maximale Anzahl Knoten pro Cluster
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • iSCSI	12
9,7	• FC • iSCSI	2

MetroCluster IP-Konfigurationen

Die folgende Tabelle zeigt die ASA Unterstützung für SAN-Protokolle und die unterstützte Anzahl von Knoten pro Cluster in MetroCluster IP-Konfigurationen:

Beginnend mit ONTAP…	Protokollunterstützung	Maximale Anzahl Knoten pro Cluster
9.15.1	• NVMe/TCP	2 Knoten pro Cluster in Vier-Knoten MetroCluster IP-Konfigurationen
9.12.1	• NVMe/FC	2 Knoten pro Cluster in Vier-Knoten MetroCluster IP-Konfigurationen
9.9.1	• FC • iSCSI	4 Knoten pro Cluster in Acht-Knoten MetroCluster IP-Konfigurationen
9,7	• FC • iSCSI	2 Knoten pro Cluster in Vier-Knoten MetroCluster IP-Konfigurationen

Unterstützung für persistente Ports

Ab ONTAP 9.8 sind persistente Ports auf All-Flash SAN Arrays (ASAs), die für die Verwendung des FC-Protokolls konfiguriert sind, standardmäßig aktiviert. Persistente Ports sind nur für FC verfügbar und erfordern die Zugehörigkeit zu einer Zone, die durch den World Wide Port Name (WWPN) identifiziert wird.

Persistente Ports reduzieren die Auswirkungen von Übernahmen, indem sie eine Schatten-LIF auf dem entsprechenden physischen Port des Hochverfügbarkeitspartners (HA-Partner) erstellen. Wird ein Knoten übernommen, nimmt die Schatten-LIF auf dem Partnerknoten die Identität der ursprünglichen LIF an, einschließlich der WWPNe. Bevor der Status des Pfads zum übernommenen Knoten auf fehlerhaft geändert wird, erscheint die Schatten-LIF dem Host-MPIO-Stack als aktiver/optimierter Pfad, und die I/O wird

verschoben. Dies reduziert I/O-Unterbrechungen, da der Host auch während Storage-Failover-Operationen immer die gleiche Anzahl an Pfaden zum Ziel sieht.

Bei persistenten Ports sollten die folgenden FCP-Port-Eigenschaften innerhalb des HA-Paares identisch sein:

- FCP-Portanzahl
- FCP-Portnamen
- FCP-Portgeschwindigkeiten
- FCP LIF WWPN-basierte Zonierung

Wenn eine dieser Eigenschaften innerhalb des HA-Paares nicht identisch ist, wird die folgende EMS-Meldung generiert:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Weitere Informationen zu persistenten Ports sind unter "NetApp Technischer Bericht 4080: Bewährte Verfahren für moderne SAN" zu finden.

Konfigurationsgrenzen für FC-Switches, die mit ONTAP Systemen verwendet werden

Fibre Channel Switches haben maximale Konfigurationsgrenzen, einschließlich der Anzahl der unterstützten Anmeldungen pro Port, Portgruppe, Blade und Switch. Die Switch-Hersteller dokumentieren ihre unterstützten Grenzwerte.

Jede FC logische Schnittstelle (LIF) meldet sich an einem FC-Switch-Port an. Die Gesamtzahl der Anmeldungen von einem einzelnen Target auf dem Node entspricht der Anzahl der LIFs plus einer Anmeldung für den zugrunde liegenden physischen Port. Die Konfigurationsgrenzen des Switch-Herstellers für Anmeldungen oder andere Konfigurationswerte dürfen nicht überschritten werden. Dies gilt auch für die auf der Host-Seite verwendeten Initiatoren in virtualisierten Umgebungen mit aktiviertem NPIV. Die Konfigurationsgrenzen des Switch-Herstellers für Anmeldungen dürfen weder für das Target noch für die in der Lösung verwendeten Initiatoren überschritten werden.

Brocade Switch-Grenzen

Die Konfigurationsgrenzen für Brocade Switches sind in den *Brocade Scalability Guidelines* zu finden.

Cisco Systems Switch-Grenzwerte

Die Konfigurationsgrenzen für Cisco Switches sind im "Cisco Konfigurationsgrenzen"Guide für Ihre Version der Cisco Switch Software zu finden.

Maximale Anzahl an unterstützten FC- und FCoE-Hops in ONTAP

Die Hop-Anzahl bezeichnet die Anzahl der Switches auf dem Pfad zwischen Initiator (Host) und Ziel (Speichersystem). Die maximal unterstützte FC-Hop-Anzahl zwischen Host und Speichersystem variiert je nach Switch-Lieferant.

In der Dokumentation von Cisco Systems wird dieser Wert auch als *Durchmesser des SAN-Fabrics* bezeichnet.

Bei FCoE können FCoE Switches mit FC Switches verbunden werden. Für durchgängige FCoE-Verbindungen muss auf den FCoE Switches eine Firmware-Version ausgeführt werden, die Ethernet Inter-Switch-Links (ISLs)

unterstützt.

Switch-Lieferant	Unterstützte Hop-Anzahl
Brocade	• 7 für FC • 5 für FCoE
Cisco	• 7 für FC • Bis zu 3 der Switches können FCoE Switches sein.

Warteschlangentiefe für ONTAP FC Hosts berechnen

Möglicherweise ist eine Anpassung der FC-Warteschlangentiefe auf dem Host erforderlich, um die maximalen Werte für ITNs pro Node und FC-Port-Fan-In zu erreichen. Die maximale Anzahl von LUNs und die Anzahl der HBAs, die eine Verbindung zu einem FC-Port herstellen können, sind durch die verfügbare Warteschlangentiefe an den FC-Zielports begrenzt.

Über diese Aufgabe

Die Warteschlangentiefe ist die Anzahl der E/A-Anforderungen (SCSI-Befehle), die gleichzeitig auf einem Speicherkontroller in die Warteschlange gestellt werden können. Jede E/A-Anforderung vom initiierenden HBA des Hosts an den Zieladapter des Speicherkontrollers belegt einen Eintrag in der Warteschlange. In der Regel entspricht eine höhere Warteschlangentiefe einer besseren Performance. Wird jedoch die maximale Warteschlangentiefe des Speicherkontrollers erreicht, weist dieser eingehende Befehle mit einer QFULL-Antwort zurück. Wenn eine große Anzahl von Hosts auf einen Speicherkontroller zugreift, ist eine sorgfältige Planung erforderlich, um QFULL-Zustände zu vermeiden, da diese die Systemleistung erheblich beeinträchtigen und auf manchen Systemen zu Fehlern führen können.

In einer Konfiguration mit mehreren Initiatoren (Hosts) sollten alle Hosts eine ähnliche Warteschlangentiefe aufweisen. Aufgrund der ungleichen Warteschlangentiefe zwischen Hosts, die über denselben Zielport mit dem Storage-Controller verbunden sind, wird Hosts mit geringerer Warteschlangentiefe der Zugriff auf Ressourcen durch Hosts mit größerer Warteschlangentiefe verwehrt.

Folgende allgemeine Empfehlungen können hinsichtlich des „Tuning“ der Warteschlangentiefe gegeben werden:

- Für kleine bis mittelgroße Systeme ist eine HBA-Warteschlangentiefe von 32 zu verwenden.
- Für große Systeme wird eine HBA-Warteschlangentiefe von 128 empfohlen.
- Für Ausnahmefälle oder Leistungstests empfiehlt sich eine Warteschlangenlänge von 256, um mögliche Warteschlangenprobleme zu vermeiden.
- Alle Hosts sollten ähnliche Warteschlangentiefen eingestellt haben, um allen Hosts gleichen Zugriff zu ermöglichen.
- Um Leistungseinbußen oder Fehler zu vermeiden, darf die Warteschlangentiefe des Ziel-FC-Ports am Speichercontroller nicht überschritten werden.

Schritte

1. Die Gesamtzahl der FC-Initiatoren in allen Hosts, die mit einem FC-Zielport verbunden sind, ermitteln.
2. Mit 128 multiplizieren.
    - Ist das Ergebnis kleiner als 2.048, sollte die Warteschlangentiefe für alle Initiatoren auf 128 gesetzt

werden. Sie haben 15 Hosts, wobei jeweils ein Initiator an jeden der beiden Zielports des Storage Controllers angeschlossen ist. 15 × 128 = 1.920. Da 1.920 unter dem Gesamtlimit der Warteschlangentiefe von 2.048 liegt, kann die Warteschlangentiefe für alle Initiatoren auf 128 gesetzt werden.

- Ist das Ergebnis größer als 2.048, gehen Sie zu Schritt 3. Sie haben 30 Hosts, wobei jeweils ein Initiator an jeden der beiden Zielports des Storage Controllers angeschlossen ist. 30 × 128 = 3.840. Da 3.840 größer als das Gesamtlimit der Warteschlangentiefe von 2.048 ist, sollte eine der Optionen unter Schritt 3 zur Behebung gewählt werden.

3. Wählen Sie eine der folgenden Optionen, um dem Storage Controller weitere Hosts hinzuzufügen.
   - Option 1:
     i. Weitere FC-Zielports hinzufügen.
     ii. Verteilen Sie Ihre FC-Initiatoren neu.
     iii. Wiederholen Sie die Schritte 1 und 2. + Die gewünschte Warteschlangentiefe von 3.840 überschreitet die verfügbare Warteschlangentiefe pro Port. Um dies zu beheben, kann jedem Controller ein FC-Zieladapter mit zwei Ports hinzugefügt werden, anschließend werden die FC-Switches so umkonfiguriert, dass 15 der 30 Hosts mit einem Satz von Ports und die verbleibenden 15 Hosts mit einem zweiten Satz von Ports verbunden sind. Die Warteschlangentiefe pro Port wird dadurch auf 15 × 128 = 1.920 reduziert.
   - Option 2:
     i. Jeder Host wird entsprechend seines erwarteten E/A-Bedarfs als “large” oder “small” bezeichnet.
     ii. Die Anzahl der großen Initiatoren ist mit 128 zu multiplizieren.
     iii. Die Anzahl der kleinen Initiatoren ist mit 32 zu multiplizieren.
     iv. Die beiden Ergebnisse werden addiert.
     v. Ist das Ergebnis kleiner als 2.048, sollte die Warteschlangentiefe für große Hosts auf 128 und die Warteschlangentiefe für kleine Hosts auf 32 eingestellt werden.
     vi. Ist das Ergebnis pro Port immer noch größer als 2.048, sollte die Warteschlangenlänge pro Initiator verringert werden, bis die Gesamtwarteschlangenlänge kleiner oder gleich 2.048 ist.

> Zur Abschätzung der erforderlichen Warteschlangenlänge für einen bestimmten Durchsatz von E/A pro Sekunde gilt folgende Formel:
>
> Erforderliche Warteschlangentiefe = (Anzahl der E/A pro Sekunde) × (Antwortzeit)
>
> Wenn beispielsweise 40.000 E/A-Vorgänge pro Sekunde bei einer Reaktionszeit von 3 Millisekunden benötigt werden, ergibt sich die erforderliche Warteschlangentiefe zu 40.000 × (0,003) = 120.

Die maximale Anzahl an Hosts, die Sie mit einem Zielport verbinden können, beträgt 64, wenn Sie die Warteschlangenlänge auf die empfohlene Basislänge von 32 beschränken. Wenn jedoch eine Warteschlangenlänge von 128 gewählt wird, können maximal 16 Hosts mit einem Zielport verbunden werden. Je größer die Warteschlangenlänge, desto weniger Hosts kann ein einzelner Zielport unterstützen. Falls die Anforderungen so sind, dass bei der Warteschlangenlänge keine Kompromisse möglich sind, ist es erforderlich, mehr Zielports zu verwenden.

Die gewünschte Warteschlangentiefe von 3.840 überschreitet die verfügbare Warteschlangentiefe pro Port. Es sind 10 „large“ Hosts mit hohem Storage-I/O-Bedarf und 20 „small“ Hosts mit geringem I/O-Bedarf vorhanden. Die Initiator-Warteschlangentiefe sollte auf den large Hosts auf 128 und auf den small Hosts auf 32 gesetzt werden.

Die resultierende Gesamttiefe der Warteschlange beträgt (10 × 128) + (20 × 32) = 1.920.

Sie können die verfügbare Warteschlangenlänge gleichmäßig auf alle Initiatoren verteilen.

Die daraus resultierende Warteschlangenlänge pro Initiator beträgt 2,048 ÷ 30 = 68.

Warteschlangentiefen für ONTAP SAN Hosts anpassen

Möglicherweise müssen Sie die Warteschlangenlängen auf Ihrem Host anpassen, um die maximalen Werte für ITNs pro Node und FC Port Fan-In zu erreichen. "die optimale Warteschlangenlänge berechnen" für Ihre Umgebung.

AIX-Hosts

Die Warteschlangentiefe auf AIX-Hosts kann mit dem `chdev` Befehl geändert werden. Änderungen, die mit dem `chdev` Befehl vorgenommen werden, bleiben nach einem Neustart erhalten.

Beispiele:

- Um die Warteschlangenlänge für das Gerät hdisk7 zu ändern, wird folgender Befehl verwendet:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Zum Ändern der Warteschlangenlänge für den fcs0 HBA wird folgender Befehl verwendet:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  Der Standardwert für `num_cmd_elems` ist 200. Der Maximalwert ist 2.048.

> ⓘ Es kann erforderlich sein, den HBA offline zu nehmen, um `num_cmd_elems` zu ändern und ihn dann mit den Befehlen `rmdev -l fcs0 -R` und `makdev -l fcs0 -P` wieder online zu bringen.

HP-UX Hosts

Die LUN- oder Gerätewarteschlangentiefe auf HP-UX-Hosts kann mit dem Kernel-Parameter `scsi_max_qdepth` geändert werden. Die HBA-Warteschlangentiefe kann mit dem Kernel-Parameter `max_fcp_reqs` geändert werden.

- Der Standardwert für `scsi_max_qdepth` ist 8. Der Maximalwert ist 255.

  `scsi_max_qdepth`Die Einstellung kann im laufenden System dynamisch mit der `-u` Option des `kmtune` Befehls geändert werden. Die Änderung gilt für alle Geräte im System. Zum Beispiel kann mit dem folgenden Befehl die LUN-Warteschlangentiefe auf 64 erhöht werden:

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  Die Warteschlangenlänge für einzelne Gerätedateien kann mithilfe des `scsictl` Befehls geändert werden. Änderungen mit dem `scsictl` Befehl bleiben nach einem Systemneustart nicht erhalten. Die Warteschlangenlänge für eine bestimmte Gerätedatei kann mit folgendem Befehl angezeigt und geändert werden:

  ```
  scsictl -a /dev/rdsk/c2t2d0
  ```

```
scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
```

- Der Standardwert für `max_fcp_reqs` ist 512. Der Maximalwert ist 1024.

  Der Kernel muss neu kompiliert und das System neu gestartet werden, damit die Änderungen `max_fcp_reqs` wirksam werden. Um beispielsweise die HBA-Warteschlangentiefe auf 256 zu ändern, kann folgender Befehl verwendet werden:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Solaris Hosts

Sie können die LUN- und HBA-Warteschlangentiefe für Ihre Solaris Hosts festlegen.

- Für die LUN-Warteschlangentiefe gilt: Die Anzahl der auf einem Host verwendeten LUNs multipliziert mit der Drosselung pro LUN (lun-queue-depth) muss kleiner oder gleich dem Wert tgt-queue-depth auf dem Host sein.
- Für die Warteschlangentiefe in einem Sun-Stack: Die nativen Treiber erlauben keine Einstellungen pro LUN oder pro Ziel `max_throttle` auf HBA-Ebene. Die empfohlene Methode zur Festlegung des `max_throttle` Werts für native Treiber ist auf Geräte-Typ-Ebene (VID_PID) in den `/kernel/drv/sd.conf` und `/kernel/drv/ssd.conf` Dateien. Das Host Utility setzt diesen Wert auf 64 für MPxIO Konfigurationen und auf 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 festgelegt.

4. Der gewünschte Wert wird entsprechend der Konfiguration Ihrer Umgebung festgelegt.
5. Die Datei speichern.
6. Den Host mit dem `sync; sync; sync; reboot -- -r` Befehl neu starten.

VMware Hosts für einen QLogic HBA

Mit dem `esxcfg-module` Befehl lassen sich die HBA Zeitüberschreitungseinstellungen ändern. Eine manuelle Aktualisierung der `esx.conf` Datei wird nicht empfohlen.

Schritte

1. Melden Sie sich an der Service-Konsole als Root-Benutzer an.
2. Mit dem `#vmkload_mod -l` Befehl lässt sich überprüfen, welches Qlogic HBA Modul aktuell geladen ist.
3. Für eine einzelne Instanz einer Qlogic HBA wird folgender Befehl ausgeführt:

   ```
   #esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
   ```

   Dieses Beispiel verwendet das Modul qla2300_707. Das passende Modul ist entsprechend

der Ausgabe von `vmkload_mod -l` zu wählen.

4. Die Änderungen werden mit folgendem Befehl gespeichert:

   ```
   #/usr/sbin/esxcfg-boot -b
   ```

5. Starten Sie den Server mit folgendem Befehl neu:

   ```
   #reboot
   ```

6. Die Änderungen werden mit den folgenden Befehlen bestätigt:

   a. `#esxcfg-module -g qla2300_707`

   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware Hosts für einen Emulex HBA

Mit dem `esxcfg-module` Befehl lassen sich die HBA Zeitüberschreitungseinstellungen ändern. Eine manuelle Aktualisierung der `esx.conf` Datei wird nicht empfohlen.

Schritte

1. Melden Sie sich an der Service-Konsole als Root-Benutzer an.
2. Mit dem `#vmkload_mod -l grep lpfc`Befehl lässt sich überprüfen, welcher Emulex HBA aktuell geladen ist.
3. Für eine einzelne Instanz einer Emulex HBA ist folgender Befehl einzugeben:

   ```
   #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 Modul lpfcdd_7xx. Das passende Modul sollte entsprechend dem Ergebnis von `vmkload_mod -l` verwendet werden.

   Durch Ausführen dieses Befehls wird die LUN-Warteschlangentiefe für den durch lpfc0 repräsentierten HBA auf 16 gesetzt.

4. Für mehrere Instanzen einer Emulex HBA ist folgender Befehl auszuführen:

   ```
   a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
   lpfcdd_7xx
   ```

   Die LUN-Warteschlangenlänge für lpfc0 und die LUN-Warteschlangenlänge für lpfc1 ist auf 16 eingestellt.

5. Führen Sie den folgenden Befehl aus:

   ```
   #esxcfg-boot -b
   ```

6. Neustart mit `#reboot`.

Windows Hosts für einen Emulex HBA

Auf Windows-Hosts kann das `LPUTILNT` Dienstprogramm verwendet werden, um die Warteschlangenlänge für Emulex HBAs zu aktualisieren.

Schritte

1. Das Dienstprogramm `LPUTILNT` im Verzeichnis `C:\WINNT\system32` ausführen.
2. Im Menü auf der rechten Seite **Laufwerksparameter** auswählen.
3. Scrollen Sie nach unten und doppelklicken Sie auf **QueueDepth**.

> Wenn Sie **QueueDepth** größer als 150 einstellen, muss auch der folgende Wert in der 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 das `SANsurfer` HBA-Manager-Dienstprogramm verwenden, um die Warteschlangenlängen für Qlogic HBAs zu aktualisieren.

Schritte

1. Das `SANsurfer`HBA Manager Dienstprogramm ausführen.
2. Klicken Sie auf **HBA port** > **Einstellungen**.
3. Im Listenfeld auf **Erweiterte HBA-Porteinstellungen** klicken.
4. Der `Execution Throttle`Parameter wird aktualisiert.

Linux Hosts für Emulex HBA

Sie können die Warteschlangenlängen eines Emulex HBA auf einem Linux-Host aktualisieren. Damit die Aktualisierungen nach einem Neustart erhalten bleiben, ist das Erstellen eines neuen RAM-Disk-Images und ein anschließender Neustart des Hosts erforderlich.

Schritte

1. Die zu ändernden Parameter für die Warteschlangentiefe identifizieren:

   ```
   modinfo lpfc|grep queue_depth
   ```

   Es wird eine Liste der Warteschlangenlängenparameter mit ihrer Beschreibung angezeigt. Abhängig von Ihrer Betriebssystemversion können Sie einen oder mehrere der folgenden Warteschlangenlängenparameter ändern:

   - `lpfc_lun_queue_depth`: Maximale Anzahl von FC-Befehlen, die einer bestimmten LUN (uint) zugeordnet werden können
   - `lpfc_hba_queue_depth`: Maximale Anzahl von FC-Befehlen, die an einen lpfc HBA (uint) in die Warteschlange gestellt werden können
   - `lpfc_tgt_queue_depth`: Maximale Anzahl von FC-Befehlen, die an einen bestimmten Zielport in die Warteschlange gestellt werden können (uint)

     Der `lpfc_tgt_queue_depth`Parameter ist nur für Red Hat Enterprise Linux 7.x Systeme, SUSE Linux Enterprise Server 11 SP4 Systeme und 12.x Systeme anwendbar.

2. Die Warteschlangenlängen werden aktualisiert, indem die Warteschlangenlängenparameter zur `/etc/modprobe.conf` Datei für ein Red Hat Enterprise Linux 5.x System und zur `/etc/modprobe.d/scsi.conf` Datei für ein Red Hat Enterprise Linux 6.x oder 7.x System oder ein

SUSE Linux Enterprise Server 11.x oder 12.x System hinzugefügt werden.

Je nach Version Ihres Betriebssystems lassen sich einer 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. Ein neues RAM-Disk-Image wird erstellt, anschließend wird der Host neu gestartet, damit die Aktualisierungen auch nach Neustarts erhalten bleiben.

   Weitere Informationen enthält die "Systemadministration" für Ihre Version des Linux-Betriebssystems.

4. Es sollte sichergestellt sein, dass die Werte für die Warteschlangenlänge für jeden der geänderten Warteschlangenlängen-Parameter aktualisiert wurden:

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
      30
```

   Der aktuelle Wert der Warteschlangenlänge wird angezeigt.

Linux Hosts für QLogic HBA

Sie können die Warteschlangentiefe eines QLogic-Treibers auf einem Linux-Host aktualisieren. Damit die Aktualisierungen nach einem Neustart erhalten bleiben, ist das Erstellen eines neuen RAM-Disk-Images und ein anschließender Neustart des Hosts erforderlich. Die Warteschlangentiefe des QLogic HBA kann über die QLogic HBA-Management-GUI oder die Befehlszeilenschnittstelle (CLI) angepasst werden.

Diese Aufgabe zeigt, wie die QLogic HBA CLI verwendet wird, um die QLogic HBA Warteschlangentiefe zu ändern

Schritte

1. Den zu ändernden Parameter für die Gerätewarteschlangenlänge identifizieren:

   `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 beträgt 64 für RHEL 7.5 und später. Der Standardwert beträgt 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. Der Wert für die Gerätewarteschlangenlänge wird aktualisiert:

   - Wenn die Änderungen dauerhaft gespeichert werden sollen, sind die folgenden Schritte erforderlich:
     i. Die Warteschlangentiefen werden aktualisiert, indem der Parameter „queue depth“ zur `/etc/modprobe.conf` Datei für ein Red Hat Enterprise Linux 5.x System und zur

`/etc/modprobe.d/scsi.conf` Datei für ein Red Hat Enterprise Linux 6.x oder 7.x System oder ein SUSE Linux Enterprise Server 11.x oder 12.x System hinzugefügt wird: `options qla2xxx ql2xmaxqdepth=new_queue_depth`

ii. Ein neues RAM-Disk-Image wird erstellt, anschließend wird der Host neu gestartet, damit die Aktualisierungen auch nach Neustarts erhalten bleiben.

Weitere Informationen enthält die "Systemadministration" für Ihre Version des Linux-Betriebssystems.

◦ Wenn der Parameter nur für die aktuelle Sitzung geändert werden soll, ist folgender Befehl auszuführen:

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Im folgenden Beispiel ist die Warteschlangentiefe auf 128 eingestellt.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Es wird überprüft, ob die Werte für die Warteschlangentiefe aktualisiert wurden:

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Der aktuelle Wert der Warteschlangenlänge wird angezeigt.

4. Die Warteschlangentiefe des QLogic HBA kann durch Aktualisierung des Firmware-Parameters `Execution Throttle` aus dem QLogic HBA BIOS geändert werden.

a. Anmeldung an der QLogic HBA-Management-CLI:

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
```

b. Im Hauptmenü die Option `Adapter Configuration` auswählen.

```
[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. Aus der Liste der Adapterkonfigurationsparameter die `HBA Parameters` Option auswählen.

```
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. Aus der Liste der HBA-Ports den erforderlichen HBA-Port auswählen.

```
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. Im Menü „HBA-Parameter“ die `Display HBA Parameters` Option auswählen, um den aktuellen Wert der `Execution Throttle` 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. **Eingabetaste** drücken, um fortzufahren.

b. Im Menü „HBA-Parameter“ die Option `Configure HBA Parameters` zum Ändern der HBA-Parameter auswählen.

c. Im Menü „Parameter konfigurieren“ die Option `Execute Throttle` auswählen und den Wert dieses Parameters aktualisieren.

```
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. **Eingabetaste** drücken, um fortzufahren.

e. Im Menü „Parameter konfigurieren“ die Option `Commit Changes` zum Speichern der Änderungen auswählen.

f. Das Menü wird beendet.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.