



SAN-Storage-Management

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from <https://docs.netapp.com/de-de/ontap/san-admin/san-host-provisioning-concept.html> on April 24, 2024. Always check docs.netapp.com for the latest.

Inhalt

- SAN-Storage-Management 1
 - SAN-Konzepte 1
 - SAN-Administration 24
 - SAN Datensicherung 101
 - Referenz zur SAN-Konfiguration 122

SAN-Storage-Management

SAN-Konzepte

SAN-Bereitstellung mit iSCSI

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

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

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

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

Unterstützte FC-Protokolle:

- FC
- FCoE
- NVMe

Netzwerkverbindungen und Namen der iSCSI-Zielknoten

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

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

Jeder iSCSI-Knoten muss einen Knotennamen haben.

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

Name des Storage-System-Nodes

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

Der Node-Name wird im folgenden Format angezeigt:

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

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

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

TCP-Port für iSCSI

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

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

Verwandte Informationen

["NetApp Dokumentation: ONTAP SAN Host-Konfiguration"](#)

ISCSI-Service-Management

ISCSI-Service-Management

Über das können Sie die Verfügbarkeit des iSCSI-Service auf den logischen iSCSI-Schnittstellen der Storage Virtual Machine (SVM) managen `vserver iscsi interface enable` Oder `vserver iscsi interface disable` Befehle.

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

Wie iSCSI auf dem Host implementiert wird

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

Sie können iSCSI auf eine der folgenden Arten implementieren:

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

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

Funktionsweise der iSCSI-Authentifizierung

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

iSCSI-Authentifizierungsmethoden:

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

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

- Inbound – das Storage-System authentifiziert den Initiator.

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

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

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

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

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

Verwandte Informationen

["Multipathing-Optionen für Windows mit Data ONTAP: Fibre Channel und iSCSI"](#)

Verwalten der iSCSI-Initiator-Sicherheit

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

Isolierung von iSCSI-Endpunkten

Ab ONTAP 9.1 wurden bestehende iSCSI-Sicherheitsbefehle auf den IP-Adressbereich oder mehrere IP-Adressen erweitert.

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

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

Fügen Sie den Adressbereich des Initiators hinzu

Verbessern Sie das Sicherheitsmanagement für iSCSI-Initiatoren, indem Sie dem einen IP-Adressbereich oder mehrere IP-Adressen hinzufügen `vserver iscsi security add-initiator-address-range` Befehl.

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

Entfernen Sie den Adressbereich des Initiators

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

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

Welche CHAP-Authentifizierung ist

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

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

Richtlinien für die Verwendung der CHAP-Authentifizierung

Bei der Verwendung der CHAP-Authentifizierung sollten Sie bestimmte Richtlinien befolgen.

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

Ein Null-Benutzername ist nicht zulässig.

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

Passwörter können hexadezimale Werte oder Strings sein. Für hexadezimale Werte sollten Sie den Wert mit einem Präfix von „0x“ oder „0X“ eingeben. Ein Null-Kennwort ist nicht zulässig.

ONTAP ermöglicht die Verwendung von Sonderzeichen, nicht englischen Buchstaben, Zahlen und Leerzeichen für CHAP-Passwörter (Secrets). Dies unterliegt jedoch Host-Einschränkungen. Wenn einer dieser Server von Ihrem spezifischen Host nicht erlaubt ist, können diese nicht verwendet werden.



Der Microsoft iSCSI-Software-Initiator beispielsweise erfordert, dass die CHAP-Passwörter für Initiator und Ziel mindestens 12 Bytes betragen, wenn keine IPsec-Verschlüsselung verwendet wird. Die maximale Kennwortlänge beträgt 16 Byte, unabhängig davon, ob IPsec verwendet wird.

Weitere Einschränkungen finden Sie in der Dokumentation des Initiators.

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

MITHILFE VON iSCSI-Schnittstellenzugriffslisten kann die Anzahl der LIFs in einer SVM begrenzt werden, auf die ein Initiator zugreifen kann. Dies erhöht die Performance und Sicherheit.

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

Internet Storage Name Service (iSNS)

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

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

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

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

Was macht ein iSNS-Server

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

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

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

Interaktion von SVMs mit einem iSNS-Server

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

Im folgenden Beispiel verwendet die SVM „vs1“ die SVM-Management-LIF „vs1_mgmt_LIF“, um sich beim iSNS-Server zu registrieren. Während der iSNS-Registrierung sendet eine SVM alle iSCSI-LIFs über die SVM-

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

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

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

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

Zwischen dem Zeitpunkt, zu dem Sie die Konfigurationsänderungen vornehmen, und dem Zeitpunkt, an dem ONTAP das Update an den iSNS-Server sendet, kann es zu einer Verzögerung von einigen Minuten kommen.

Sofortige Aktualisierung der iSNS-Informationen auf dem iSNS-Server erzwingen: `vserver iscsi isns update`

Befehle zum Verwalten von iSNS

ONTAP bietet Befehle zur Verwaltung Ihres iSNS-Service.

Ihr Ziel ist	Befehl
Konfigurieren Sie einen iSNS-Dienst	<code>vserver iscsi isns create</code>
Starten Sie einen iSNS-Dienst	<code>vserver iscsi isns start</code>
Ändern eines iSNS-Dienstes	<code>vserver iscsi isns modify</code>
iSNS-Servicekonfiguration anzeigen	<code>vserver iscsi isns show</code>
Aktualisierung der registrierten iSNS-Informationen erzwingen	<code>vserver iscsi isns update</code>
Stoppen Sie einen iSNS-Dienst	<code>vserver iscsi isns stop</code>
Entfernen Sie einen iSNS-Dienst	<code>vserver iscsi isns delete</code>
Zeigen Sie die man-Page für einen Befehl an	<code>man <i>command name</i></code>

Weitere Informationen finden Sie auf der man-Page für jeden Befehl.

SAN Provisionierung mit FC

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

Wie FC-Ziel-Nodes mit dem Netzwerk verbunden werden

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

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



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

So werden FC-Knoten identifiziert

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

Verwendung von WWPNs

WWPNs identifizieren jede LIF in einer SVM, die zur Unterstützung von FC konfiguriert ist. Diese LIFs nutzen die physischen FC-Ports in jedem Node im Cluster. Dabei können es sich um FC-Target-Karten, UTA oder UTA2 handeln, die in den Nodes als FC oder FCoE konfiguriert wurden.

- Erstellen einer Initiatorgruppe

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

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

- Identifizierung von FC-LIFs auf einzigartige Weise

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

Funktionsweise von weltweiten Namenszuweisungen

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

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

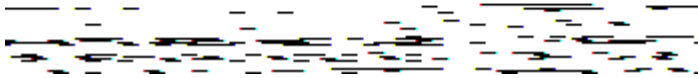
Die weltweiten Namen scheinen aus folgenden Gründen nicht sequenziell zu sein:

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

So werden FC Switches identifiziert

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

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



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

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

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

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

SAN-Provisionierung mit NVMe

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

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



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

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

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

Verwandte Informationen

["Technischer Bericht von NetApp 4684: Implementieren und Konfigurieren moderner SANs mit NVMe/FC"](#)

SAN Volumes

Über SAN Volumes – Übersicht

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



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

Thin Provisioning für Volumes

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

Sie erstellen ein FlexVol-Volume mit Thin Provisioning, indem Sie dessen festlegen `-space-guarantee` Option auf `none`.

Thick Provisioning für Volumes

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

Sie erstellen ein per Thick Provisioning bereitgestelltes FlexVol-Volume durch Festlegen dessen `-space-slo` (Service Level Objective)-Option nach `thick`.

Semi-Thick Provisioning für Volumes

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

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

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

Sie erstellen ein FlexVol-Volume mit semi-Thick-Provision-Funktion, indem Sie dessen festlegen `-space-slo` (Service Level Objective)-Option nach `semi-thick`.

Nutzung mit platzsparenden Dateien und LUNs

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

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

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

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

Hinweise

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

Unterstützung von SCSI Thin Provisioning LUNs

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

Sie verwenden die ONTAP `space-allocation` Einstellung zum Aktivieren/Deaktivieren der Unterstützung für das T10 Thin Provisioning auf einer LUN. Sie verwenden die ONTAP `space-allocation enable` Einstellung zum Aktivieren von T10 SCSI Thin Provisioning auf einem LUN.

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

"ONTAP 9-Befehle"

Konfiguration der Bereitstellungsoptionen für Volumes

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

Über diese Aufgabe

Einstellen des `-space-slo` Option auf `thick` Stellt Folgendes sicher:

- Das gesamte Volume wird im Aggregat vorab zugewiesen. Sie können das nicht verwenden `volume create` Oder `volume modify` Befehl zum Konfigurieren des Volume `-space-guarantee` Option.
- 100 % des für Überschreibungen benötigten Speicherplatzes ist reserviert. Sie können das nicht verwenden `volume modify` Befehl zum Konfigurieren des Volume `-fractional-reserve` Option

Einstellen des `-space-slo` Option auf `semi-thick` Stellt Folgendes sicher:

- Das gesamte Volume wird im Aggregat vorab zugewiesen. Sie können das nicht verwenden `volume create` Oder `volume modify` Befehl zum Konfigurieren des Volume `-space-guarantee` Option.
- Kein Speicherplatz für Überschreibungen reserviert. Sie können das verwenden `volume modify` Befehl zum Konfigurieren des Volume `-fractional-reserve` Option.
- Das automatische Löschen von Snapshot-Kopien ist aktiviert.

Schritt

1. Konfiguration der Bereitstellungsoptionen für Volumes:

```
volume create -vserver vs1 -volume vol1 -aggregate aggr1 -space-slo none|thick|semi-thick -space-guarantee none|volume
```

Der `-space-guarantee` Die Option ist standardmäßig aktiviert `none` Für AFF Systeme und für DP-Volumes ohne All Flash FAS. Andernfalls wird standardmäßig auf verwendet `volume`. Verwenden Sie für vorhandene FlexVol-Volumes das `volume modify` Befehl zum Konfigurieren von Bereitstellungsoptionen.

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

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

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

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

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

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

SAN Volume-Konfigurationsoptionen

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

Autogrow

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

Autogrow kann nicht ausgelöst werden, um Snapshot Erstellung zu unterstützen. Wenn Sie versuchen, eine Snapshot Kopie zu erstellen und es zu wenig Speicherplatz auf dem Volume gibt, schlägt die Snapshot-Erstellung fehl, selbst wenn Autogrow aktiviert ist.

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

Autochrink

Sie können Autochrink aktivieren oder deaktivieren. Wenn Sie ihn aktivieren, ermöglicht Autochrink es ONTAP, die Gesamtgröße eines Volumes automatisch zu verringern, wenn die Menge an Speicherplatz, die im Volume verbraucht wird, einen vorab festgelegten Schwellenwert verringert. Dies erhöht die Storage-Effizienz, indem Volumes automatisch ungenutzten freien Speicherplatz freigeben.

Snapshot wird automatisches Löschen erstellt

Durch das automatische Löschen von Snapshots werden Snapshot Kopien automatisch gelöscht, wenn eine der folgenden tritt:

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

Sie können die Snapshot automatisches Löschen konfigurieren, um Snapshot Kopien von ältesten bis neuesten oder von neuesten bis ältesten zu löschen. Durch das Löschen von Snapshots werden keine Snapshot Kopien gelöscht, die mit Snapshot-Kopien in geklonten Volumes oder LUNs verknüpft sind.

Wenn Ihr Volume zusätzlichen Speicherplatz benötigt und Sie sowohl Autogrow als auch Snapshot Autodelete aktiviert haben, versucht ONTAP standardmäßig, den erforderlichen Speicherplatz durch Auslösung von Autogrow zu erwerben. Wenn nicht genügend Speicherplatz durch Autogrow erfasst wird, dann wird Snapshot Autodelete ausgelöst.

Snapshot Reserve

Die Snapshot Reserve definiert die Menge an Speicherplatz im Volume, das für Snapshot Kopien reserviert ist. Der zur Snapshot Reserve zugewiesenen Speicherplatz kann nicht für andere Zwecke verwendet werden. Wenn der gesamte für die Snapshot-Reserve zugewiesene Speicherplatz verwendet wird, dann beginnen Snapshot Kopien, zusätzlichen Speicherplatz auf dem Volume zu belegen.

Anforderung für das Verschieben von Volumes in SAN-Umgebungen

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

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

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

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

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

Überlegungen bei der Festlegung der fraktionalen Reserve

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

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

Einstellung der fraktionalen Reserve auf 0 Verbessern Sie Ihre Storage-Auslastung. Wenn jedoch für eine Applikation, die auf Daten im Volume zugreift, ein Datenausfall auftritt, könnte es sein, wenn das Volume über keinen freien Speicherplatz verfügt, selbst wenn die Volume-Garantie festgelegt wurde `volume`. Durch ordnungsgemäße Volume-Konfiguration und Nutzung können Sie jedoch die Wahrscheinlichkeit eines Schreibversagens minimieren. ONTAP bietet eine „Best Effort“-Garantie für Volumes mit als fraktionaler Reserve 0 Wenn *all* der folgenden Anforderungen erfüllt sind:

- Die Deduplizierung wird nicht verwendet

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

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

- ODX und FlexClone Copy Offload werden derzeit nicht genutzt
- Die Volume-Garantie ist auf festgelegt `volume`
- Datei- oder LUN-Speicherplatzreservierung ist `enabled`
- Die Snapshot-Reserve des Volumes ist auf festgelegt `0`
- Das automatische Löschen von Volume Snapshot Kopien ist `enabled` Mit einem Maß an Engagement `destroy`, Eine zerstörte Liste von `lun_clone`, `vol_clone`, `cifs_share`, `file_clone`, `sfsr`, Und ein Auslöser von `volume`

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

Beachten Sie, dass wenn Ihre Änderungsrate hoch ist, in seltenen Fällen kann das automatische Löschen der Snapshot-Kopie den Wert hinterherhinken, sodass das Volume nicht mehr über genügend Speicherplatz verfügt. Dies gilt auch für alle oben genannten Konfigurationseinstellungen.

Darüber hinaus können Sie optional die Funktion Volume Autogrow verwenden, um die Wahrscheinlichkeit zu verringern, dass Volume-Snapshot-Kopien automatisch gelöscht werden müssen. Wenn Sie die Autogrow-Funktion aktivieren, müssen Sie den freien Speicherplatz im zugehörigen Aggregat überwachen. Wenn das Aggregat voll genug ist, um das Volume nicht mehr zu wachsen, werden wahrscheinlich mehr Snapshot-Kopien gelöscht, da der freie Speicherplatz im Volume erschöpft ist.

Wenn Sie nicht alle oben genannten Konfigurationsanforderungen erfüllen können und Sie sicherstellen müssen, dass das Volume nicht über genügend Speicherplatz verfügt, müssen Sie die Einstellung für die fraktionale Reserve des Volume auf festlegen `100`. Dies erfordert vorab mehr freien Speicherplatz, garantiert jedoch, dass Datenänderungen auch dann erfolgreich ausgeführt werden, wenn die oben aufgeführten Technologien eingesetzt werden.

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

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

SAN-Host-seitiges Speicherplatzmanagement

In einer durch Thin Provisioning bereitgestellten Umgebung rundet das Platzmanagement auf der Host-Seite den Prozess des Speicherplatzmanagements auf dem Storage-System ab, das im Host-Filesystem freigegeben wurde.

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

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

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

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

Vereinfachtes Host-Management mit SnapCenter

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

Mit SnapCenter lassen sich mühelos virtuelle Festplatten aus Storage-Pools erstellen, die auf verschiedene Storage-Systeme verteilt werden können. Die Storage-Provisionierung wird automatisiert und die Erstellung von Snapshot Kopien und Klonen von Snapshot Kopien, die mit Host-Daten konsistent sind, wird vereinfacht.

Weitere Informationen finden Sie in der NetApp Produktdokumentation "[SnapCenter](#)".

Weiterführende Links

["Aktivieren Sie die Speicherplatzzuweisung für Thin Provisioning LUNs von SCSI"](#)

Allgemeines zu Initiatorgruppen

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

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

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

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

Beispiel dafür, wie Initiatorgruppen LUN-Zugriff geben

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

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

Hosts mit HBA-WWPNs, IQNs oder EUIs	igroups	WWPNs, IQNs, EUIs, die Initiatorgruppen hinzugefügt wurden	LUNs zugeordnet zu Initiatorgruppen
Host1, Single Path (iSCSI Software Initiator) iqn.1991-05.com.microsoft:host1	gruppe1	iqn.1991-05.com.microsoft:host1	/vol/vol2/lun1
Host 2, Multipath (zwei HBAs) 10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	gruppe2	10:00:00:00:c9:2b:6b:3c 10:00:00:00:c9:2b:02:3c	/vol/vol2/lun2
Host3, Multipath, Cluster mit Host 4 10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02	gruppe3	10:00:00:00:c9:2b:32:1b 10:00:00:00:c9:2b:41:02 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees1/lun3
HOST4, Multipath, Clustered (nicht als Host sichtbar) 10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	Gruppe 4	10:00:00:00:c9:2b:51:2c 10:00:00:00:c9:2b:47:a2	/vol/vol2/qtrees2/lun4 /vol/vol2/qtrees1/lun5

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

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

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

Storage-Virtualisierung mit Copy-Offload von VMware und Microsoft

Überblick: Storage-Virtualisierung mit VMware und Microsoft Copy-Offload

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

Bei der Nutzung von VMware und Microsoft Copy-Offload in virtualisierten Umgebungen müssen Ihre LUNs aufeinander abgestimmt werden. Nicht ausgerichtete LUNs können die Performance beeinträchtigen.

Vorteile der Nutzung einer virtualisierten SAN-Umgebung

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

- Dezentrales Management

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

- Verbesselter Datenzugriff

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

- Kontrollierter LUN-Zugriff

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

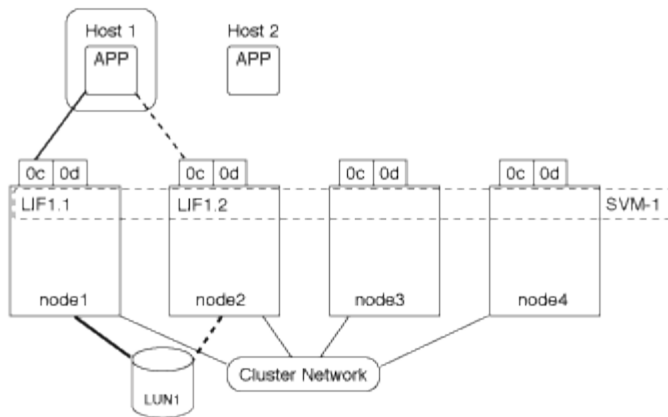
Der Zugriff auf LUNs erfolgt in einer virtualisierten Umgebung

In einer virtualisierten Umgebung können Hosts (Clients) mithilfe von optimierten und nicht optimierten Pfaden auf LUNs zugreifen.

Eine LIF ist eine logische Schnittstelle, die die SVM mit einem physischen Port verbindet. Obwohl mehrere SVMs mehrere LIFs am selben Port aufweisen können, gehört eine LIF zu einer SVM. Die LUNs können über die LIFs der SVMs aufgerufen werden.

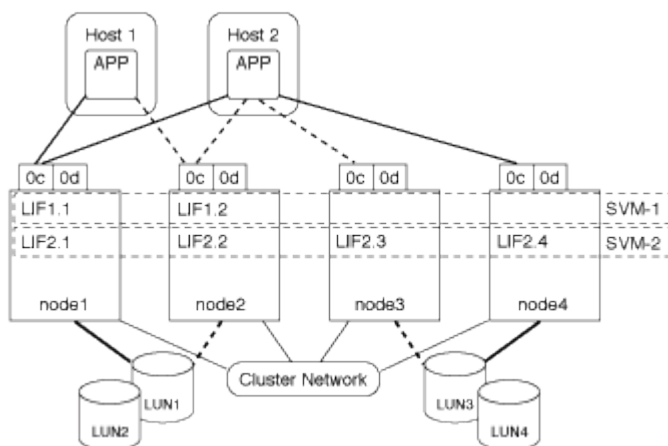
Beispiel für einen LUN-Zugriff über eine einzelne SVM in einem Cluster

Im folgenden Beispiel stellt Host 1 eine Verbindung zu LIF1.1 und LIF1.2 in SVM-1 her, um auf LUN1 zuzugreifen. LIF1.1 verwendet den physischen Port Nr. 1:0c und LIF1.2 mit dem Node2:0c. LIF1.1 und LIF1.2 gehören nur zu SVM-1. Wenn eine neue LUN auf Node 1 oder Node 2 für SVM-1 erstellt wird, können sie dieselben LIFs verwenden. Wenn eine neue SVM erstellt wird, können neue LIFs mit physischen Ports 0c oder 0d der beiden Nodes erstellt werden.



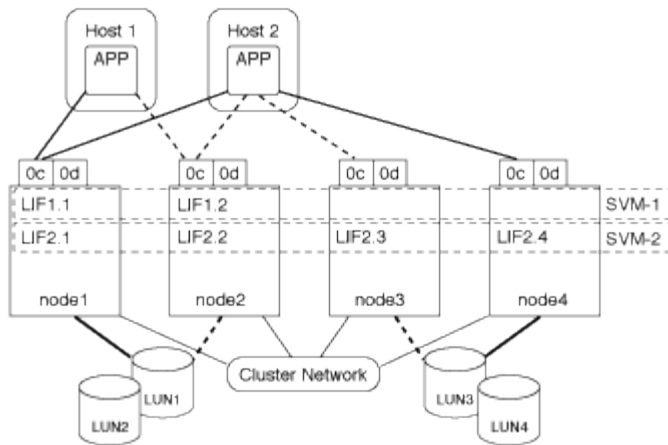
Beispiel eines LUN-Zugriffs mit mehreren SVMs in einem Cluster

Ein physischer Port kann mehrere LIFs unterstützen, die unterschiedliche SVMs unterstützen. Da LIFs einer bestimmten SVM zugeordnet sind, können die Cluster-Nodes den eingehenden Datenverkehr an die richtige SVM senden. Im folgenden Beispiel verfügt jeder Node von 1 bis 4 über eine LIF für SVM-2 mit dem physischen Port 0c auf jedem Node. Host 1 stellt eine Verbindung zu LIF1.1 und LIF1.2 in SVM-1 her, um auf LUN1 zuzugreifen. Host 2 stellt eine Verbindung zu LIF2.1 und LIF2.2 in SVM-2 her, um auf LUN2 zuzugreifen. Beide SVMs teilen sich den physischen Port 0c auf den Nodes 1 und 2. SVM-2 verfügt über zusätzliche LIFs, über die Host 2 auf LUNs 3 und 4 zugreift. Diese LIFs verwenden den physischen Port 0c an den Nodes 3 und 4. Mehrere SVMs können die physischen Ports auf den Nodes gemeinsam nutzen.



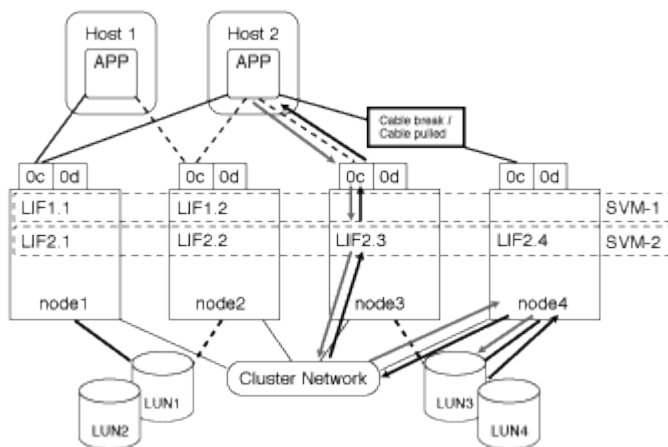
Beispiel eines aktiven oder optimierten Pfads zu einer LUN von einem Host-System aus

In einem aktiven oder optimierten Pfad bewegt sich der Datenverkehr nicht über das Cluster-Netzwerk. Er reist die direkteste Route zur LUN. Der aktive oder optimierte Pfad zu LUN1 erfolgt über LIF1.1 in node1, wobei der physische Port 0c verwendet wird. Host 2 verfügt über zwei aktive oder optimierte Pfade, einen Pfad zu node1, LIF2.1, der den physischen Port 0c und den anderen Pfad zu node4, LIF2.4 nutzt, der physischen Port 0c verwendet.



Beispiel eines aktiven oder nicht optimierten Pfads (indirekter) zu einer LUN von einem Host-System aus

In einem aktiven oder nicht optimierten Pfad (indirekter) wird der Datenverkehr über das Cluster-Netzwerk übertragen. Dieses Problem tritt nur auf, wenn alle aktiven oder optimierten Pfade eines Hosts nicht zur Verarbeitung des Datenverkehrs zur Verfügung stehen. Wenn der Pfad von Host 2 zu SVM-2 LIF2.4 verloren geht, durchläuft der Zugriff auf LUN3 und LUN4 das Cluster-Netzwerk. Zugriff von Host 2 verwendet LIF2.3 auf node3. Dann gelangt der Traffic zum Cluster-Netzwerk-Switch und sichert bis zu node4 für den Zugriff auf LUN3 und LUN4. Diese erfolgt dann wieder über den Cluster-Netzwerk-Switch und dann über LIF2.3 auf Host 2. Dieser aktive oder nicht optimierte Pfad wird verwendet, bis der Pfad zu LIF2.4 wiederhergestellt ist oder eine neue LIF auf einem anderen physischen Port auf Node 4 für SVM-2 eingerichtet wurde.



=

:allow-uri-read:

Verbesserung der VMware VAAI-Leistung für ESX-Hosts

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

Die VAAI-Funktion unterstützt die folgenden SCSI-Befehle:

- EXTENDED_COPY

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

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

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

- `COMPARE_AND_WRITE`

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

Anforderungen für die Nutzung der VAAI Umgebung

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

Die Umgebungsanforderungen lauten wie folgt:

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



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

Ermitteln, ob VAAI Funktionen von ESX unterstützt werden

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

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

SCSI-Befehl	ESX Steuernamen (VAAI-Funktion)
EXTENDED_COPY	HardwareAcceleratedMove
SCHREIBSCHUTZ	HardwareAcceleratedInit
COMPARE_AND_WRITE	HardwareAcceleratedLocking

Microsoft Offloaded Data Transfer (ODX)

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

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

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

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

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

Anforderungen für die Nutzung von ODX

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

Zur Nutzung von ODX ist bei Ihrem System Folgendes erforderlich:

- ONTAP

ODX ist bei unterstützten Versionen von ONTAP automatisch aktiviert.

- Mindestquellenvolumen: 2 GB

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

- ODX-Unterstützung auf dem Windows-Client

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

"NetApp Interoperabilitäts-Matrix-Tool"

- Applikationssupport für ODX

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

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

Die Größe der Komprimierungsgruppen 32.000 wird nicht unterstützt.

ODX funktioniert nicht bei den folgenden Volume-Typen:

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



ODX wird auf FlexCache-Ursprungs-Volumes unterstützt.

- "Semi-Thick Provisioning Volumes"

Besondere Anforderungen an Systemdateien

Sie können ODX-Dateien, die in qtrees gefunden wurden, löschen. Andere ODX-Systemdateien dürfen nur entfernt oder geändert werden, wenn Ihnen der technische Support dazu aufgefordert wird.

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

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

Sie können das verwenden `copy-offload delete-tokens -path dir_path -node node_name` Befehl zum Löschen eines qtree mit einer ODX-Datei

Anwendungsfälle für ODX

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

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

In den folgenden Anwendungsfällen werden ODX Kopien und Verschiebungen unterstützt:

- Intra-Volume

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

- Zwischen Volumes, demselben Node, gleiche SVM

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

- Zwischen Volumes, verschiedenen Nodes, dieselbe SVM

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

- Zwischen SVM, demselben Node

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

- Zwischen SVMs, unterschiedliche Nodes

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

- Cluster zwischen Clustern

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

Es gibt einige weitere spezielle Anwendungsfälle:

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

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

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

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

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

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



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

SAN-Administration

SAN Provisionierung

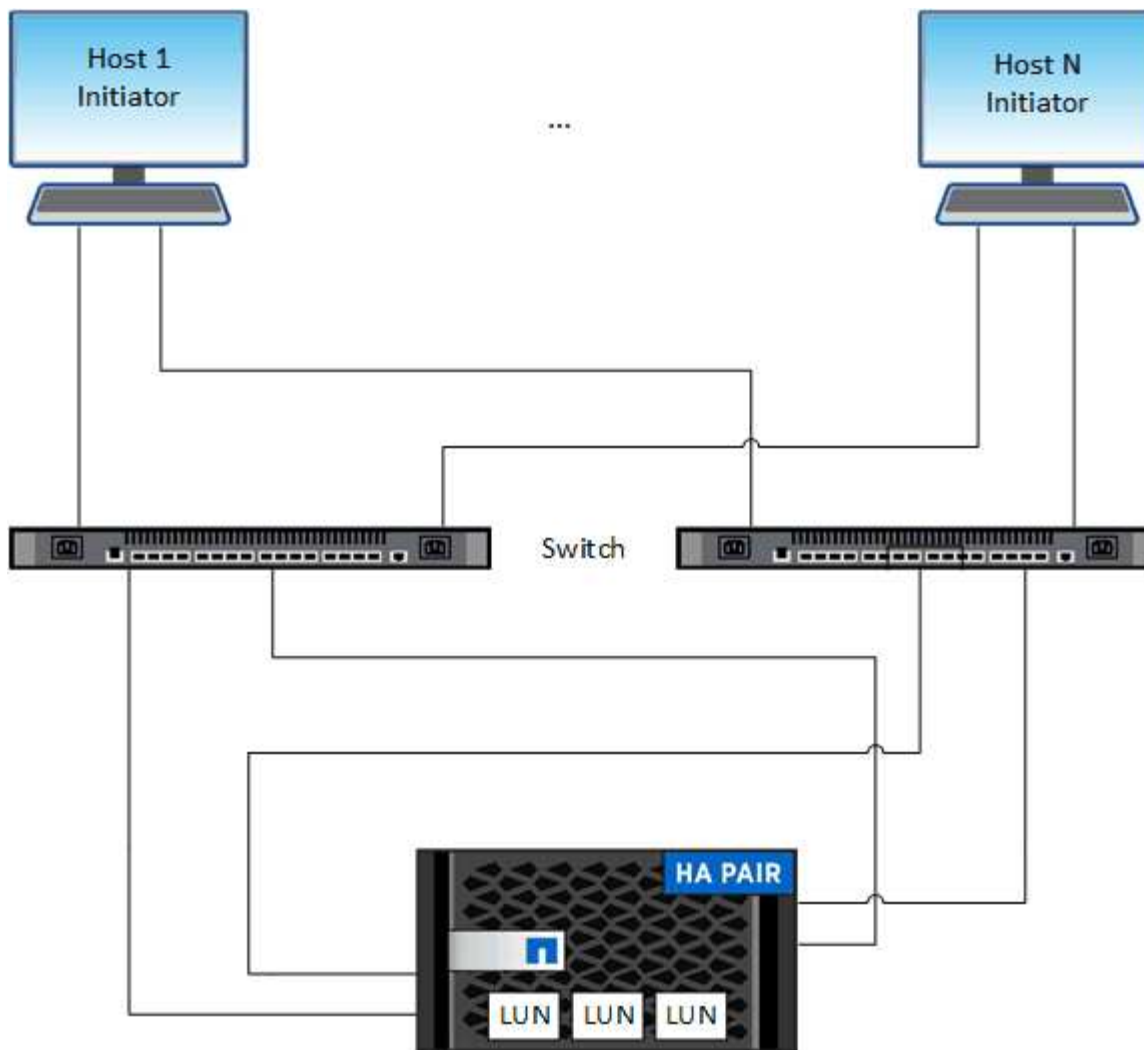
SAN-Management-Überblick

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

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

- ["iSCSI-Protokoll"](#)
- ["FC-/FCoE-Protokoll"](#)

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



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

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

Konfigurieren Sie Switches für FCoE

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

Was Sie benötigen

- Ihre SAN-Konfiguration muss unterstützt werden.

Weitere Informationen zu unterstützten Konfigurationen finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

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

Wenn Sie eine UTA2 verwenden, muss er auf festgelegt sein `cna` Modus.

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

Schritte

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

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

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

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

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

Wenn der Online-Status des FC-Zielports lautet `false`, Konsultieren Sie Ihre Switch-Dokumentation.

Verwandte Informationen

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

Systemanforderungen

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

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

Die Dokumentation zu Host Utilities enthält weitere Informationen.

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

Verwandte Informationen

- ["NetApp Interoperabilitäts-Matrix-Tool"](#)
- ["ONTAP SAN-Host-Konfiguration"](#)
- ["Technischer Bericht 4017 zu Fibre Channel SAN Best Practices"](#)

Was muss ich wissen, bevor Sie eine LUN erstellen

Warum die tatsächlichen LUN-Größen geringfügig variieren

Sie sollten Folgendes bezüglich der Größe Ihrer LUNs kennen.

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

Richtlinien für das Zuweisen von LUN-IDs

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

Richtlinien zum Zuordnen von LUNs zu Initiatorgruppen

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

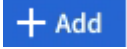
Überprüfen Sie Ihre FC- oder iSCSI-Protokolllizenz und fügen Sie sie hinzu

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

Beispiel 1. Schritte

System Manager

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

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

CLI

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

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

```
system license show
```

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

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

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

Provisionierung von SAN-Storage

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

Informationen zum Erstellen einer neuen Storage-VM und zum Konfigurieren des FC- oder iSCSI-Protokolls finden Sie unter ["Konfigurieren Sie eine SVM für FC"](#) Oder ["Konfigurieren Sie eine SVM für iSCSI"](#).

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

LUNs werden Ihrem Host als Festplattengeräte angezeigt.



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

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

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

Beispiel 2. Schritte

System Manager

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

Informationen zum Abschließen dieser Aufgabe mit System Manager Classic (verfügbar mit 9.7 und älter) finden Sie unter ["iSCSI-Konfiguration für Red hat Enterprise Linux"](#)

Schritte

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

Option	Verfügbar ab
<ul style="list-style-type: none">• Weisen Sie LUNs anstelle des übergeordneten Volume eine QoS-Richtlinie zu<ul style="list-style-type: none">◦ Mehr Optionen > Speicherung und Optimierung◦ Wählen Sie Performance Service Level.◦ Um die QoS-Richtlinie auf einzelne LUNs anstelle des gesamten Volumes anzuwenden, wählen Sie Diese Performance-Limits für jede LUN anwenden. <p>Standardmäßig werden Performance-Limits auf Volume-Ebene angewendet.</p>	ONTAP 9.10.1
<ul style="list-style-type: none">• Erstellen Sie eine neue Initiatorgruppe unter Verwendung vorhandener Initiatorgruppen<ul style="list-style-type: none">◦ Mehr Optionen > HOST-INFORMATIONEN◦ Wählen Sie Neue Initiatorgruppe unter Verwendung vorhandener Initiatorgruppen aus. <p>HINWEIS: Der OS-Typ für eine Initiatorgruppe, die andere Initiatorgruppen enthält, kann nach dem Erstellen nicht mehr geändert werden.</p>	ONTAP 9.9.1
<ul style="list-style-type: none">• Fügen Sie einer Initiatorgruppe oder Host-Initiator eine Beschreibung hinzu <p>Die Beschreibung dient als Alias für die Initiatorgruppe oder den Host-Initiator.</p> <ul style="list-style-type: none">◦ Mehr Optionen > HOST-INFORMATIONEN	ONTAP 9.9.1

<ul style="list-style-type: none"> • Erstellen Sie Ihre LUN auf einem vorhandenen Volume <p>Standardmäßig wird eine neue LUN in einem neuen Volume erstellt.</p> <ul style="list-style-type: none"> ◦ Mehr Optionen > LUNs hinzufügen ◦ Wählen Sie Gruppen bezogene LUNs aus. 	ONTAP 9.9.1
<ul style="list-style-type: none"> • Deaktivieren Sie QoS oder wählen Sie eine individuelle QoS-Richtlinie aus ◦ Mehr Optionen > Speicherung und Optimierung ◦ Wählen Sie Performance Service Level. <p>HINWEIS: Wenn Sie in ONTAP 9.9.1 und höher eine benutzerdefinierte QoS-Richtlinie auswählen, können Sie auch die manuelle Platzierung auf einer bestimmten lokalen Ebene auswählen.</p>	ONTAP 9.8

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

6. Erkennen Sie LUNs auf Ihrem Host.

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

7. Initialisieren Sie die LUNs und erstellen Sie optional Dateisysteme.

8. Vergewissern Sie sich, dass der Host Daten auf der LUN schreiben und lesen kann.

CLI

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

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

```
system license show
```

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

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

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

3. Aktivieren Sie Ihren Protokollservice auf der SVM:

Für iSCSI:

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

◦ Für FC:*

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

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

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

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

5. Vergewissern Sie sich, dass Ihre LIFs erstellt wurden und dass ihr Betriebsstatus lautet `online`:

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

6. Erstellen Sie Ihre LUNs:

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

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



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

7. Erstellen Sie Ihre Initiatorgruppen:

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

8. Ordnen Sie Ihre LUNs Initiatorgruppen zu:

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

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

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

10. Optional ["Erstellen Sie einen Portsatz und binden Sie es an eine Initiatorgruppe"](#).

11. Befolgen Sie die Schritte in der Host-Dokumentation, um den Blockzugriff auf Ihren spezifischen Hosts zu ermöglichen.

12. Schließen Sie die FC- oder iSCSI-Zuordnung mithilfe der Host Utilities ab und ermitteln Sie die LUNs auf dem Host.

Verwandte Informationen

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

NVMe Provisionierung

NVMe Übersicht

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

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

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

Support für NVMe ist abhängig von Ihrer Version von ONTAP. Siehe ["Unterstützung und Einschränkungen von NVMe"](#) Entsprechende Details.

NVMe ist das

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

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

Speichergehäuse mit einem Server verbunden werden.

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

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

- NVMe ist für bis zu 64 Warteschlangen konzipiert.

Jede Warteschlange kann wiederum bis zu 64 gleichzeitige Befehle haben.

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

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

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

Allgemeines zu NVMe Namespaces

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

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

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

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

Über NVMe-Subsysteme

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

Verwandte Informationen

- ["NVMe-Storage wird bereitgestellt"](#)

- ["Zuordnen eines NVMe Namespace zu einem Subsystem"](#)
- ["Konfigurieren Sie SAN-Hosts und Cloud-Clients"](#)

Lizenzanforderungen für NVMe

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

Sie können die Lizenz mit dem folgenden Befehl aktivieren:

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

Konfiguration, Support und Einschränkungen von NVMe

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

Der NVMe-Support und die Einschränkungen hängen von Ihrer Version von ONTAP, Ihrer Plattform und Ihrer Konfiguration ab. Weitere Informationen zu Ihrer spezifischen Konfiguration finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#). Informationen zu unterstützten Grenzwerten finden Sie unter ["Hardware Universe"](#).



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

Konfiguration

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

Spezielle Ausnahmen sind in aufgeführt ["NetApp Interoperabilitäts-Matrix-Tool"](#).

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

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

Funktionen

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

Beginnt mit ONTAP...	NVMe unterstützt
----------------------	------------------

9.12.1	<p>MetroCluster IP Konfigurationen mit 4 Nodes auf NVMe/FC</p> <ul style="list-style-type: none"> • MetroCluster Konfigurationen werden für NVMe vor 9.12.1 nicht unterstützt. • MetroCluster-Konfigurationen werden auf NVMe/TCP nicht unterstützt.
9.10.1	Ändern der Größe eines Namespace
9.9.1	<ul style="list-style-type: none"> • Namespaces und LUNs werden auf demselben Volume gleichzeitig ausgeführt.
9.8	<ul style="list-style-type: none"> • Koexistenz von Protokollen <p>SCSI-, NAS- und NVMe-Protokolle können auf derselben Storage Virtual Machine (SVM) vorhanden sein.</p> <p>Vor ONTAP 9.8 kann NVMe als einziges Protokoll auf der SVM verwendet werden. *</p>
9.6	<ul style="list-style-type: none"> • 512-Byte-Blöcke und 4096-Byte-Blöcke für Namespaces <p>Der Standardwert ist 4096. 512 sollte nur verwendet werden, wenn das Host-Betriebssystem keine 4096-Byte-Blöcke unterstützt.</p> <ul style="list-style-type: none"> • Volume-Verschiebung mit zugeordneten Namespaces
9.5	Failover/Giveback mit Multipath HA-Paar

Protokolle

Die folgenden NVMe-Protokolle werden unterstützt.

Protokoll	Beginnt mit ONTAP...	Zulässig von...
TCP	9.10.1	Standard
FC	9.4	Standard

Ab ONTAP 9.8 können SCSI-, NAS- und NVMe-Protokolle auf derselben Storage Virtual Machine (SVM) konfiguriert werden.

In ONTAP 9.7 und älteren Versionen kann NVMe das einzige Protokoll auf der SVM sein.

Namespaces

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

- Wenn Daten in einer LUN verloren gehen, kann sie nicht aus einem Namespace wiederhergestellt werden, und umgekehrt.
- Die Platzgarantie für Namespaces ist identisch mit der Speicherplatzgarantie für das enthaltende Volume.
- Sie können auf einem Volume-Übergang von Data ONTAP im 7-Mode keinen Namespace erstellen.
- Namespaces bieten keine Unterstützung für Folgendes:
 - Umbenennungen
 - Verschiebung zwischen Volumes
 - Kopie zwischen Volumes
 - Copy-on-Demand

Weitere Einschränkungen

Die folgenden ONTAP Funktionen werden von NVMe Konfigurationen nicht unterstützt:

- Synchron
- Virtual Storage Console

Folgendes gilt nur für Nodes mit ONTAP 9.4:

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

Verwandte Informationen

["Best Practices für modernes SAN"](#)

Konfigurieren Sie eine Storage-VM für NVMe

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

Bevor Sie beginnen

Ihre FC- oder Ethernet-Adapter müssen NVMe unterstützen. Unterstützte Adapter werden im [aufgeführt "NetApp Hardware Universe"](#).

Beispiel 3. Schritte

System Manager

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

Und NVMe auf einer neuen Storage-VM konfigurieren	Um NVMe für eine vorhandene Storage-VM zu konfigurieren
<ol style="list-style-type: none">1. Klicken Sie im System Manager auf Storage > Storage VMs und dann auf Hinzufügen.2. Geben Sie einen Namen für die Storage-VM ein.3. Wählen Sie * NVMe* für das Access Protocol aus.4. Wählen Sie NVMe/FC aktivieren oder NVMe/TCP aktivieren und Speichern.	<ol style="list-style-type: none">1. Klicken Sie im System Manager auf Storage > Storage VMs.2. Klicken Sie auf die zu konfigurierende Speicher-VM.3. Klicken Sie auf die Registerkarte Einstellungen und dann auf  Neben dem NVMe-Protokoll.4. Wählen Sie NVMe/FC aktivieren oder NVMe/TCP aktivieren und Speichern.

CLI

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

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

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

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

```
vserver show
```

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

Für NVMe:

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

Für TCP:

```
network port show
```

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

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


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

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

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

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

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

NVMe sollte das einzige Protokoll sein, das unter dem angezeigt wird `allowed protocols` Spalte.

6. Entwicklung des NVMe-Service:

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

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

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

Der Administrative Status Der SVM sollte als aufgeführt werden `up`.

8. NVMe/FC-LIF erstellen:

- Für ONTAP 9.9.1 oder früher, FC:

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

- Für ONTAP 9.10.1 oder höher, FC oder TCP:

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

9. Erstellung einer NVMe/FC-LIF auf dem HA-Partner-Node:

- Für ONTAP 9.9.1 oder früher, FC:

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

- Für ONTAP 9.10.1 oder höher, FC oder TCP:

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

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

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

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

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

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

NVMe-Storage wird bereitgestellt

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

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

Bevor Sie beginnen

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

System Manager

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

Schritte

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

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

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

CLI

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

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

Informationen zum Konfigurieren der Storage-VM für NVMe finden Sie unter ["Konfigurieren Sie eine SVM für NVMe"](#).

Schritte

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

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

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

2. NVMe-Namespace erstellen:

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

3. NVMe-Subsystem erstellen:

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

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

4. Überprüfen Sie, ob das Subsystem erstellt wurde:

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

Der `nvme` Das Subsystem sollte unter dem angezeigt werden Subsystem Spalte.

5. Beziehen Sie das NQN vom Host.

6. Fügen Sie den Host-NQN zum Subsystem hinzu:

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

7. Den Namespace dem Subsystem zuordnen:

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

Ein Namespace kann nur einem einzelnen Subsystem zugeordnet werden.

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

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

Das Subsystem sollte als aufgeführt werden `Attached subsystem`.

Zuordnen eines NVMe Namespace zu einem Subsystem

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

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



Wenn Sie einem Host, der zu einem Subsystem in ONTAP 9.13.1 oder früher hinzugefügt wurde, eine hohe Priorität zuweisen möchten, können Sie dies tun [Ändern Sie die Host-Priorität](#).

Bevor Sie beginnen

Der Namespace und das Subsystem sollten bereits erstellt werden. Wenn Sie einen Namespace und ein Subsystem erstellen müssen, lesen Sie ["NVMe-Storage wird bereitgestellt"](#).

Schritte

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

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

Wenn Sie die Standardpriorität des Hosts von Normal auf hoch ändern möchten, verwenden Sie die `-priority high` Option. Diese Option ist ab ONTAP 9.14.1 verfügbar.

3. Den Namespace dem Subsystem zuordnen:

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

Ein Namespace kann nur einem einzelnen Subsystem zugeordnet werden.

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

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

Das Subsystem sollte als aufgeführt werden `Attached subsystem`.

LUNs managen

LUN-QoS-Richtliniengruppe bearbeiten

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



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

Schritte

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

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

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

Konvertieren einer LUN in einen Namespace

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

Was Sie benötigen

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

Schritt

1. Konvertieren einer LUN in einen NVMe-Namespace:

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


Versetzen einer LUN in den Offline-Modus

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

System Manager

Schritte

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

Wenn Sie... wollen	Do this...
Versetzen einer einzelnen LUN in den Offline-Modus	Klicken Sie neben dem LUN-Namen auf  Und wählen Sie Offline nehmen .
Versetzen Sie mehrere LUNs in den Offline-Modus	<ol style="list-style-type: none">1. Wählen Sie die LUNs aus, die Sie in den Offline-Modus versetzen möchten.2. Klicken Sie auf Mehr und wählen Sie Offline nehmen.

CLI

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

Schritt

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

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

Ändern der Größe einer LUN

Sie können eine LUN vergrößern oder verkleinern.



Die Größe von Solaris LUNs kann nicht geändert werden.

Vergrößern einer LUN

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

ONTAP-Version	Maximale LUN-Größe
ONTAP 9.12.1P2 und höher	128 TB für AFF-, FAS- und ASA-Plattformen
ONTAP 9.8 und höher	<ul style="list-style-type: none">• 128 TB für All-Flash SAN-Array (ASA)-Plattformen• 16 TB für nicht-ASA-Plattformen
9.5. ONTAP 9.6, 9.7	16 TB

ONTAP 9.4 oder früher	10 mal die ursprüngliche LUN-Größe, aber nicht größer als 16 TB, was die maximale LUN-Größe ist. Wenn Sie beispielsweise eine 100-GB-LUN erstellen, können Sie sie nur auf 1,000 GB erweitern. Die tatsächliche maximale Größe der LUN beträgt möglicherweise nicht genau 16 TB. ONTAP rundet das Limit auf etwas weniger ab.
-----------------------	---


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

Auf der Seite Command Reference finden Sie Informationen zum `lun resize` Befehl. Weitere Informationen zum Ändern der Größe einer LUN.

Beispiel 4. Schritte

System Manager

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

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

CLI

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

1. Vergrößern Sie die LUN:

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

2. Überprüfen Sie die erweiterte LUN-Größe:

```
lun show -vserver <SVM_name_>
```

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

```
set -unit B
```

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


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

Verkleinern Sie die Größe einer LUN

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

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

Verschieben einer LUN

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

Was Sie benötigen

Wenn Ihre LUN die selektive LUN-Zuordnung (SLM) verwendet, sollten Sie dies tun ["Ändern Sie die Liste der SLM Reporting-Nodes"](#) Um den Ziel-Node und dessen HA-Partner einzuschließen, bevor Sie die LUN verschieben.

Über diese Aufgabe

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

Die Datensicherung durch Snapshot-Kopien findet auf Volume-Ebene statt. Wenn Sie eine LUN verschieben, fällt sie daher unter das Datensicherungsschema des Ziel-Volume. Wenn für das Ziel-Volume keine Snapshot Kopien eingerichtet wurden, werden keine Snapshot Kopien der LUN erstellt. Außerdem verbleiben alle Snapshot Kopien der LUN im Original-Volume, bis diese Snapshot-Kopien gelöscht werden.

Sie können eine LUN nicht auf folgende Volumes verschieben:

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

Sie können die folgenden LUNs-Typen nicht verschieben:

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



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


Beispiel 5. Schritte

System Manager

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

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

Schritte

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

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

Wenn Sie sich für die Erstellung eines neuen Volumes entscheiden, geben Sie die Volume-Spezifikationen an.

3. Klicken Sie Auf **Verschieben**.

CLI

Verschieben Sie eine LUN mit der ONTAP CLI.

1. Verschieben der LUN:

```
lun move start
```

Die LUN ist während einer sehr kurzen Zeit sowohl auf dem Ursprungs- als auch auf dem Ziel-Volume sichtbar. Dies ist zu erwarten und wird nach Abschluss des Umschlusses gelöst.

2. Verfolgen Sie den Status der Verschiebung, und überprüfen Sie den erfolgreichen Abschluss:

```
lun move show
```

Verwandte Informationen

- ["Selektive LUN-Zuordnung"](#)

LUNs löschen

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

Was Sie benötigen

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

Schritte

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

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

3. LUN löschen:

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

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

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

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

Was muss vor dem Kopieren von LUNs wissen

Vor dem Kopieren einer LUN sollten Sie bestimmte Dinge beachten.

Cluster-Administratoren können eine LUN mithilfe der in Storage Virtual Machines (SVMs) innerhalb des Clusters kopieren `lun copy` Befehl. Cluster-Administratoren müssen die Storage Virtual Machine (SVM)-Peering-Beziehung mithilfe des `peer create` Befehl, bevor ein LUN-Kopiervorgang zwischen den SVMs ausgeführt wird. Für einen SIS-Klon muss im Quell-Volumen genügend Platz vorhanden sein.

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

Die Datensicherung durch Snapshot-Kopien findet auf Volume-Ebene statt. Wenn Sie eine LUN auf ein anderes Volume als das Volume der Quell-LUN kopieren, fällt die Ziel-LUN unter das Datensicherungsschema des Ziel-Volumens. Wenn für das Ziel-Volumen keine Snapshot Kopien eingerichtet wurden, werden keine Snapshot Kopien von der LUN-Kopie erstellt.

Das Kopieren von LUNs ist ein unterbrechungsfreier Vorgang.

Sie können die folgenden LUNs-Typen nicht kopieren:

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

Untersuchen Sie den konfigurierten und genutzten Speicherplatz einer LUN

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

Schritt

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

```
lun show
```

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

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

vserver	path	size	space-reserve	size-used
vs3	/vol/vol0/lun1	50.01GB	disabled	25.00GB
vs3	/vol/vol0/lun1_backup	50.01GB	disabled	32.15GB
vs3	/vol/vol0/lun2	75.00GB	disabled	0B
vs3	/vol/volospace/lun0	5.00GB	enabled	4.50GB

4 entries were displayed.

Aktivieren Sie die Speicherplatzzuweisung für Thin Provisioning LUNs von SCSI

Wenn Ihr Host SCSI Thin Provisioning unterstützt, können Sie die Speicherplatzzuweisung für über SCSI Thin Provisioning bereitgestellte LUNs in ONTAP aktivieren. Wenn die Speicherplatzzuweisung aktiviert ist, benachrichtigt ONTAP den Host, wenn der Speicherplatz des Volume knapp ist und die LUN im Volume keine Schreibvorgänge akzeptieren kann. ONTAP fordert auch automatisch den Speicherplatz wieder an, wenn Ihr Host Daten löscht.

Auf Hosts, die SCSI Thin Provisioning nicht unterstützen, wird die LUN offline geschaltet, wenn dem Volume mit LUN-Kapazität knapp wird und nicht automatisch erweitert werden kann. Auf Hosts, die SCSI Thin

Provisioning unterstützen, nimmt ONTAP die LUN nicht offline, wenn der Speicherplatz knapp wird. Die LUN bleibt im schreibgeschützten Modus online, und der Host wird benachrichtigt, dass die LUN Schreibvorgänge nicht mehr akzeptieren kann.

Wenn Daten auf einem Host gelöscht werden, der SCSI Thin Provisioning unterstützt, identifiziert die hostseitige Speicherplatzverwaltung die Blöcke gelöschter Daten auf dem Host-Dateisystem und stellt automatisch einen oder mehrere aus SCSI UNMAP Befehle zur Freigabe entsprechender Blöcke im Storage-System.

Bevor Sie beginnen

Um die Speicherplatzzuweisung zu aktivieren, muss SCSI Thin Provisioning von Ihrem Host unterstützt werden. SCSI Thin Provisioning verwendet logische Blockbereitstellung gemäß dem SCSI SBC-3-Standard. Nur Hosts, die diesen Standard unterstützen, können SCSI Thin Provisioning in ONTAP verwenden.

Die folgenden Hosts unterstützen derzeit SCSI Thin Provisioning beim Aktivieren der Speicherplatzzuweisung:

- Citrix XenServer 6.5 und höher
- ESXi 5.0 und höher
- Oracle Linux 6.2 UEK-Kernel oder höher
- RHEL 6.2 und höher
- SLES11 und höher
- Solaris 11.1 und höher
- Windows

Über diese Aufgabe

Standardmäßig ist die Speicherplatzzuweisung für alle LUNs deaktiviert. Sie müssen die LUN offline schalten, um die Speicherplatzzuweisung zu aktivieren. Anschließend müssen Sie die Erkennung auf dem Host durchführen, bevor der Host erkennt, dass die Speicherplatzzuweisung aktiviert wurde.

Schritte

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

```
lun modify -vserver vservice_name -volume volume_name -lun lun_name  
-state offline
```

2. Speicherplatzzuweisung aktivieren:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-space-allocation enabled
```

3. Vergewissern Sie sich, dass die Speicherplatzzuweisung aktiviert ist:

```
lun show -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-fields space-allocation
```

4. Versetzen Sie die LUN in den Online-Modus:

```
lun modify -vserver _vserver_name_ -volume _volume_name_ -lun _lun_name_  
-state online
```

5. Auf dem Host, scannen Sie alle Festplatten neu, um sicherzustellen, dass die Änderung an `-space` `-allocation` Die Option wurde ordnungsgemäß erkannt.

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

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

Über diese Aufgabe

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

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

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

- Die LUN muss von der SVM enthalten sein, der die Richtliniengruppe angehört.
Sie geben beim Erstellen der Richtliniengruppe die SVM an.
- Wenn Sie eine LUN einer Richtliniengruppe zuweisen, können Sie die LUN, die Volume oder SVM enthält, nicht einer Richtliniengruppe zuweisen.

Weitere Informationen zur Verwendung von Storage-QoS finden Sie unter ["Referenz für Systemadministration"](#).

Schritte

1. Verwenden Sie die `qos policy-group create` Befehl zum Erstellen einer Richtliniengruppe.
2. Verwenden Sie die `lun create` Befehl oder das `lun modify` Befehl mit dem `-qos-policy-group` Parameter zum Zuweisen einer LUN zu einer Richtliniengruppe.
3. Verwenden Sie die `qos statistics` Befehle zum Anzeigen von Performance-Daten.
4. Verwenden Sie bei Bedarf das `qos policy-group modify` Befehl zum Anpassen der maximalen Durchsatzbegrenzung der Richtliniengruppe.

Verfügbare Tools für eine effektive Überwachung Ihrer LUNs

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

- Active IQ Unified Manager ist ein kostenloses Tool, mit dem Sie den gesamten Storage über alle Cluster

Ihrer Umgebung hinweg managen können.

- System Manager ist eine in ONTAP integrierte grafische Benutzeroberfläche, mit der Sie Storage-Anforderungen manuell auf Cluster-Ebene managen können.
- OnCommand Insight bietet eine zentrale Ansicht Ihrer Storage-Infrastruktur und ermöglicht so das Einrichten von automatischem Monitoring, Warnungen und Berichten, wenn der Speicherplatz für die LUNs, Volumes und Aggregate knapp wird.

Funktionen und Einschränkungen der migrierte LUNs

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

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

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

Bei ummigrierte LUNs können Sie Folgendes tun:

- Zeigen Sie die LUN mit `an lun show` Befehl
- Sehen Sie sich das Inventar der LUNs an, die aus dem 7-Mode Volume mithilfe des verschoben wurden `transition 7-mode show` Befehl
- Wiederherstellung eines Volumes aus einer 7-Mode Snapshot Kopie

Durch Wiederherstellung des Volume werden alle LUNs, die in der Snapshot Kopie erfasst wurden, umgestellt

- Stellen Sie eine einzelne LUN aus einer 7-Mode Snapshot Kopie mit dem `wieder her snapshot restore-file` Befehl
- Erstellen Sie einen Klon einer LUN in einer Snapshot Kopie mit 7-Mode
- Wiederherstellung verschiedener Blöcke aus einer LUN, die in einer Snapshot Kopie mit 7-Mode erfasst wurde
- Erstellen Sie mithilfe einer Snapshot Kopie mit 7-Mode einen FlexClone des Volumes

Bei migrierte LUNs können Sie Folgendes nicht ausführen:

- Greifen Sie auf LUN-Klone zu, die durch Snapshot Kopien gesichert werden, die im Volume erfasst wurden

Verwandte Informationen

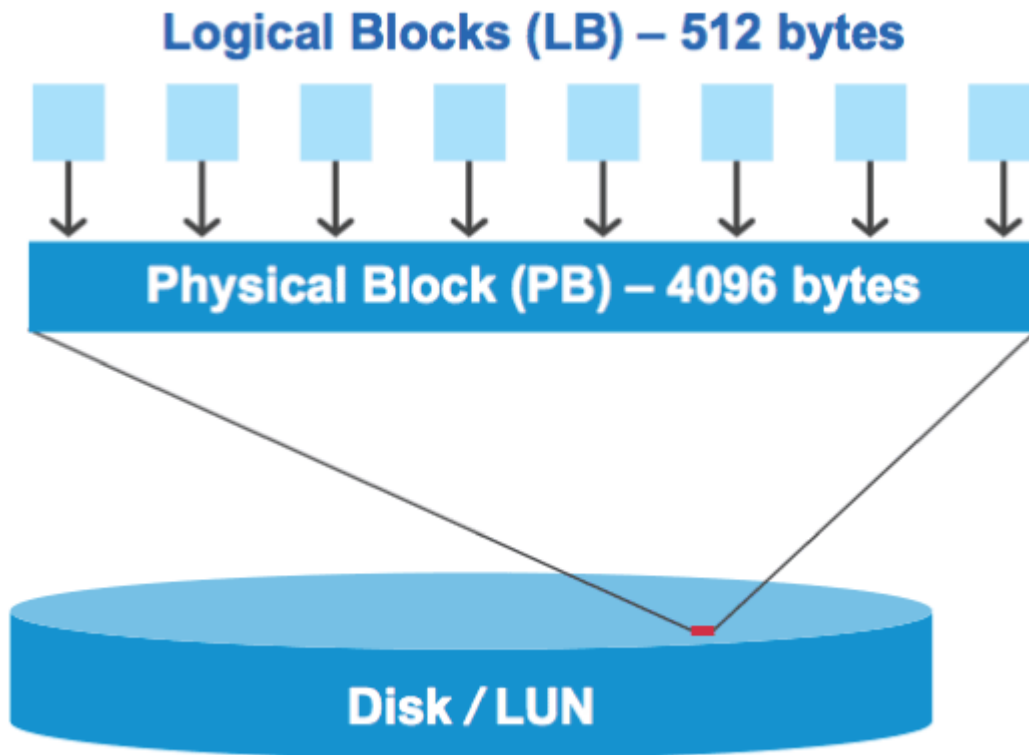
["Kopienbasierte Transition"](#)

I/O-Fehlausrichtungen auf korrekt ausgerichtete LUNs Übersicht

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

Partitionierungstabelle korrekt ist.

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



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

Wenn Sie weitere Untersuchungen benötigen, lesen Sie den Artikel in der Knowledge Base ["Wie identifizieren Sie nicht ausgerichtete I/O-Vorgänge auf LUNs?"](#)

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

- ["Windows Unified Host Utilities 7.1"](#)
- ["Virtual Storage Console for VMware vSphere Installations- und Administratorleitfaden"](#)

I/O-Ausrichtung mit LUN-OS-Typen

Für ONTAP 9.7 oder frühere Versionen sollten Sie die empfohlene ONTAP-LUN verwenden `ostype` Wert, der Ihrem Betriebssystem am nächsten kommt, um eine I/O-Abstimmung mit Ihrem OS-Partitionierungsschema zu

erreichen.

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



In manchen Fällen ist möglicherweise eine individuelle Partitionstabelle erforderlich, um die I/O-Ausrichtung zu erreichen. Jedoch für `ostype` Werte mit einem „PREFIX“-Wert größer als 0, Eine benutzerdefinierte Partition kann falsch ausgerichtete I/O erstellen

Weitere Informationen zu LUNs, die in ONTAP 9.7 oder einer älteren Version bereitgestellt wurden, finden Sie im KB-Artikel ["Identifizieren von nicht ausgerichteten I/O-Vorgängen auf LUNs"](#).



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

Besondere Überlegungen zur I/O-Ausrichtung für Linux

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

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

Spezielle Überlegungen zur I/O-Ausrichtung für Solaris LUNs

Bei der Entscheidung, ob Sie den verwenden sollten, müssen Sie verschiedene Faktoren berücksichtigen `solaris` Ostype oder der `solaris_efi` Ostype:

Siehe ["Installations- und Administrationsanleitung für Solaris Host Utilities"](#) Ausführliche Informationen finden Sie unter.

Der Bericht für ESX Boot LUNs wurde falsch ausgerichtet

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

Verwandte Informationen

["Koordinierung von Gast-VM-Dateisystem-Partition/Festplatten für VMware vSphere, andere virtuelle Umgebungen und NetApp Storage-Systeme"](#)

Möglichkeiten zur Behebung von Problemen, wenn LUNs offline geschaltet werden

Wenn kein Speicherplatz für Schreibvorgänge verfügbar ist, gehen LUNs in den Offline-Modus, um die Datenintegrität zu wahren. LUNs können nicht mehr über genügend

Speicherplatz verfügen und aus verschiedenen Gründen offline gehen, und es gibt mehrere Möglichkeiten, das Problem zu beheben.

Wenn der...	Sie können...
Aggregat ist voll	<ul style="list-style-type: none">• Fügen Sie weitere Festplatten hinzu.• Verwenden Sie die <code>volume modify</code> Befehl zum Verkleinern eines Volumes mit verfügbarem Platz.• Wenn Sie über Volumes mit Platzgarantie verfügen, die über verfügbaren Speicherplatz verfügen, ändern Sie die Volume-Speicherplatzzusage in <code>none</code> Mit dem <code>volume modify</code> Befehl.
Das Volume ist voll, aber im Aggregat, das enthalten ist, ist Platz verfügbar	<ul style="list-style-type: none">• Für Volumes mit Speicherplatzzusagen verwenden Sie den <code>volume modify</code> Erhöhen Sie die Größe Ihres Volumens mit einem Befehl.• Verwenden Sie bei Volumes, die über Thin Provisioning bereitgestellt wurden, den <code>volume modify</code> Befehl zum Erhöhen der Maximalgröße des Volumes. <p>Wenn Autogrow nicht aktiviert ist, verwenden Sie <code>volume modify -autogrow-mode</code> Um sie zu aktivieren.</p> <ul style="list-style-type: none">• Löschen Sie Snapshot-Kopien manuell mit dem <code>volume snapshot delete</code> Befehl oder verwenden Sie den <code>volume snapshot autodelete modify</code> Befehl zum automatischen Löschen von Snapshot Kopien.

Verwandte Informationen

["Festplatten- und lokales Tier-Management \(Aggregate\)"](#)

["Logisches Storage-Management"](#)

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

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

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

Konfigurationseinstellung	Was zu tun ist
Netzwerk-Konnektivität	<p>Vergewissern Sie sich, dass TCP/IP-Konnektivität zwischen dem Host und dem Speichersystem vorhanden ist.</p> <ul style="list-style-type: none"> Über die Befehlszeile des Speichersystems, Ping der Host-Schnittstellen, die für iSCSI verwendet werden: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre> <ul style="list-style-type: none"> Über die Host-Befehlszeile, Ping der Speichersystemschnittstellen, die für iSCSI verwendet werden: <pre>ping -node node_name -destination host_ip_address_for_iSCSI</pre>
Systemanforderungen	Vergewissern Sie sich, dass die Komponenten Ihrer Konfiguration qualifiziert sind. Überprüfen Sie außerdem, ob Sie über die richtige Service Pack-Stufe für das Host-Betriebssystem, die Initiatorversion, die ONTAP-Version und andere Systemanforderungen verfügen. Die Interoperabilitäts-Matrix enthält die aktuellsten Systemanforderungen.
Jumbo-Frames	Wenn Sie Jumbo Frames in Ihrer Konfiguration verwenden, überprüfen Sie, ob Jumbo Frames auf allen Geräten im Netzwerkpfad aktiviert sind: Host Ethernet NIC, das Speichersystem und alle Switches.
iSCSI-Servicestatus	Vergewissern Sie sich, dass der iSCSI-Service lizenziert und auf dem Speichersystem gestartet ist.
Anmeldung des Initiators	Vergewissern Sie sich, dass der Initiator beim Speichersystem angemeldet ist. Wenn der <code>iscsi initiator show</code> In der Befehlsausgabe werden keine Initiatoren angezeigt. Überprüfen Sie die Initiator-Konfiguration auf dem Host. Vergewissern Sie sich außerdem, dass das Storage-System als Ziel des Initiators konfiguriert ist.
iSCSI-Node-Namen (IQNs)	Vergewissern Sie sich, dass Sie die richtigen Initiator-Node-Namen in der iGroup-Konfiguration verwenden. Auf dem Host können Sie den Namen des Initiator-Node mit den Initiator-Tools und -Befehlen anzeigen. Die in der Initiatorgruppe und auf dem Host konfigurierten Initiator-Node-Namen müssen mit übereinstimmen.

Konfigurationseinstellung	Was zu tun ist
LUN-Zuordnungen	<p>Vergewissern Sie sich, dass die LUNs einer Initiatorgruppe zugeordnet sind. An der Storage-System-Konsole können Sie einen der folgenden Befehle verwenden:</p> <ul style="list-style-type: none"> • <code>lun mapping show</code> Zeigt alle LUNs und Initiatorgruppen an, denen sie zugeordnet sind. • <code>lun mapping show -igroup</code> Zeigt die LUNs an, die einer bestimmten Initiatorgruppe zugeordnet sind.
ISCSI LIFs aktivieren	Vergewissern Sie sich, dass die logischen iSCSI-Schnittstellen aktiviert sind.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

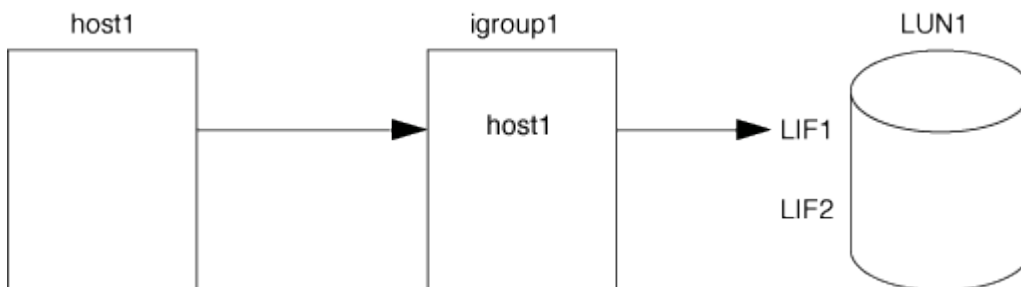
Verwalten von Initiatorgruppen und Portsätzen

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

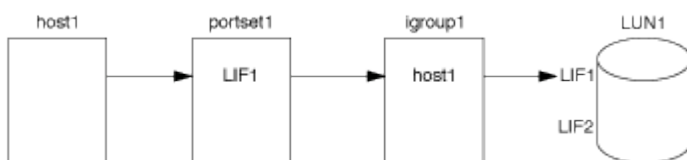
Zusätzlich zur Verwendung von Selective LUN Map (SLM) können Sie den Zugriff auf Ihre LUNs über Initiatorgruppen und Portsätze begrenzen.

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

Im folgenden Beispiel hat initiator1 keinen Portsatz. Ohne Portset kann initiator1 sowohl über LIF1 als auch über LIF2 auf LUN1 zugreifen.



Sie können den Zugriff auf LUN1 mithilfe eines Portsatzes einschränken. Im folgenden Beispiel kann initiator1 nur über LIF1 auf LUN1 zugreifen. Initiator1 kann jedoch nicht über LIF2 auf LUN1 zugreifen, weil sich LIF2 nicht im Portset1 befindet.



Verwandte Informationen

- [Selektive LUN-Zuordnung](#)
- [Erstellen Sie einen Portsatz und binden Sie diese an eine Initiatorgruppe](#)

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

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

Über diese Aufgabe

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

Zeigen Sie SAN-Initiatorgruppen an und verwalten Sie sie

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

Schritte

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

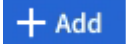
Die Seite zeigt eine Liste der Initiatorgruppen an. Wenn die Liste groß ist, können Sie weitere Seiten der Liste anzeigen, indem Sie auf die Seitenzahlen unten rechts auf der Seite klicken.

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


2. (Optional): Sie können die folgenden Aufgaben ausführen, indem Sie auf die Symbole oben rechts in der Liste klicken:

- **Suche**
- **Download** die Liste.
- **Zeige** oder **Ausblenden** Spalten in der Liste.
- **Filter** die Daten in der Liste.

3. Sie können Operationen aus der Liste ausführen:

- Klicken Sie Auf  **Add** Um eine Initiatorgruppe hinzuzufügen.
- Klicken Sie auf den Namen der Initiatorgruppe, um die Seite **Übersicht** anzuzeigen, auf der Details zur Initiatorgruppe angezeigt werden.

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

- Halten Sie den Mauszeiger über die Initiatorgruppe und klicken Sie dann auf  Neben einem Initiatorgruppennamen, der bearbeitet oder gelöscht werden soll.
- Bewegen Sie den Mauszeiger über den Bereich links neben dem Initiatorgruppennamen, und aktivieren Sie dann das Kontrollkästchen. Wenn Sie auf **+** zur Initiatorgruppe hinzufügen klicken,

können Sie diese Initiatorgruppe einer anderen Initiatorgruppe hinzufügen.

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

Zeigen Sie SAN-Initiatoren an und verwalten Sie sie

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

Schritte

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

Die Seite zeigt eine Liste der Initiatorgruppen an.

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

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

In den Spalten werden verschiedene Informationen zu den Initiatoren angezeigt.

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

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

Verschachtelte Initiatorgruppe erstellen

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

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

Die Beschreibung dient als igroup-Alias.

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



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

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

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

Zuordnen von Initiatorgruppen zu mehreren LUNs

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

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



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

Erstellen Sie einen Portsatz und binden Sie diese an eine Initiatorgruppe

Zusätzlich zu verwenden "**Selektive LUN-Zuordnung (SLM)**", Sie können einen Portsatz erstellen und den Portsatz an eine Initiatorgruppe binden, um einen weiteren Grenzwert für den Zugriff auf eine LUN zu verwenden.

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

Was Sie benötigen

Sie müssen mindestens eine LIF und eine Initiatorgruppe haben.

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

Über diese Aufgabe

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

Beispiel 6. Schritte

System Manager

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

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

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

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

Verwandte Informationen

["Anzeigen und Verwalten von Initiatoren und Initiatorgruppen"](#)

CLI

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

```
portset create -vserver vsample_name -portset portset_name -protocol  
protocol -port-name port_name
```

Wenn Sie FC verwenden, geben Sie das an `protocol` Parameter als `fc`. Wenn Sie iSCSI verwenden, geben Sie die an `protocol` Parameter als `iscsi`.

2. Bindet die Initiatorgruppe an den Portsatz:

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

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

```
portset show -vserver vsample_name
```


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

Portsätze verwalten


Zusätzlich zu ["Selektive LUN-Zuordnung \(SLM\)"](#), Sie können Portsätze verwenden, um die Möglichkeiten eines Initiators für den Zugriff auf eine LUN zu begrenzen.

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

Ändern Sie die mit einem Portsatz verbundenen Netzwerkschnittstellen

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

Löschen Sie einen Portsatz

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

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

Übersicht über selektive LUN-Zuordnung

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

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

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

SLM ist standardmäßig auf allen neuen LUN-Zuordnungen aktiviert.

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

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

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

Ändern Sie die Liste der SLM-Reporting-Nodes

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

Schritte

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

```
lun mapping add-reporting-nodes -vserver _vserver_name_ -path _lun_path_  
-igroup _igroup_name_ [-destination-aggregate _aggregate_name_|-  
destination-volume _volume_name_]
```

Wenn Sie eine konsistente Namenskonvention haben, können Sie mehrere LUN-Zuordnungen gleichzeitig ändern, indem Sie verwenden *igroup_prefix** Statt *igroup_name*.

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

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

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

```
lun mapping remove-reporting-nodes -vserver _vserver_name_ -path  
_lun_path_ -igroup _igroup_name_ -remote-nodes
```

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

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

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

Managen des iSCSI-Protokolls

Konfigurieren Sie Ihr Netzwerk für optimale Leistung

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

Schritte

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

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

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

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

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

Sie sollten es sehen "[Netzwerkmanagement](#)" Zum Konfigurieren der Ethernet-Port-Flusssteuerung über die CLI.

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

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

Konfigurieren Sie eine SVM für iSCSI

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


Über diese Aufgabe

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

Beispiel 7. Schritte

System Manager

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

So konfigurieren Sie iSCSI auf einer neuen Speicher-VM	So konfigurieren Sie iSCSI auf einer vorhandenen Storage-VM
<ol style="list-style-type: none">1. Klicken Sie im System Manager auf Storage > Storage VMs und dann auf Hinzufügen.2. Geben Sie einen Namen für die Storage-VM ein.3. Wählen Sie iSCSI für das Access Protocol.4. Klicken Sie auf iSCSI aktivieren und geben Sie die IP-Adresse und die Subnetzmaske für die Netzwerkschnittstelle ein. + jeder Node sollte mindestens zwei Netzwerkschnittstellen aufweisen.5. Klicken Sie Auf Speichern.	<ol style="list-style-type: none">1. Klicken Sie im System Manager auf Storage > Storage VMs.2. Klicken Sie auf die zu konfigurierende Speicher-VM.3. Klicken Sie auf die Registerkarte Einstellungen und dann auf  Neben dem iSCSI-Protokoll.4. Klicken Sie auf iSCSI aktivieren und geben Sie die IP-Adresse und die Subnetzmaske für die Netzwerkschnittstelle ein. + jeder Node sollte mindestens zwei Netzwerkschnittstellen aufweisen.5. Klicken Sie Auf Speichern.

CLI

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

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

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

2. Erstellen Sie eine LIF für die SVMs auf jedem Node, die Sie für iSCSI verwenden können:

- Für ONTAP 9.6 und höher:

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

- Für ONTAP 9.5 und früher:

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

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

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

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

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

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

Verwandte Informationen

["Technischer Bericht 4080 zu NetApp: Best Practices für modernes SAN"](#)

Definieren einer Sicherheitsrichtlinie für einen Initiator

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

Über diese Aufgabe

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



Nicht alle Initiatoren unterstützen hexadezimale CHAP-Kennwörter.

Schritte

1. Verwenden Sie die `vserver iscsi security create` Befehl zum Erstellen einer Sicherheitsrichtlinie für einen Initiator.

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

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

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

Verwandte Informationen

- [Funktionsweise der iSCSI-Authentifizierung](#)
- [CHAP-Authentifizierung](#)

Löschen eines iSCSI-Dienstes für eine SVM

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

Was Sie benötigen

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

Schritte

1. Verwenden Sie die `vserver iscsi modify` Befehl zum Beenden der I/O-Vorgänge auf der LUN.

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

2. Verwenden Sie die `vserver iscsi delete` Befehl zum Entfernen des iSCSI-Service von der SVM.

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

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

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

Weitere Details bei der Wiederherstellung von iSCSI-Sitzungsfehlern

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

Über diese Aufgabe

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

Ab ONTAP 9.4 beginnt der `max-error-recovery-level` Die Option wird in nicht unterstützt `iscsi show` Und `iscsi modify` Befehle.

Schritte

1. Erweiterten Modus aufrufen:

```
set -privilege advanced
```

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

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

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

3. Ändern Sie die Fehlerwiederherstellungsebene mit `iscsi modify` Befehl.

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

Registrieren Sie die SVM mit einem iSNS-Server

Sie können das verwenden `vserver iscsi isns` Befehl zum Konfigurieren der Storage Virtual Machine (SVM) für die Registrierung bei einem iSNS-Server.

Über diese Aufgabe

Der `vserver iscsi isns create` Der Befehl konfiguriert die SVM für die Registrierung beim iSNS-Server. Die SVM bietet keine Befehle, mit denen Sie den iSNS-Server konfigurieren oder verwalten können. Zur Verwaltung des iSNS-Servers können Sie die Server-Verwaltungstools oder die vom Hersteller bereitgestellte Schnittstelle für den iSNS-Server verwenden.

Schritte

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

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

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

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

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

```
iscsi show -vserver SVM_name
```

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

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

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

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

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

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

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

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

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

```
vserver iscsi isns show -vserver SVM_name
```

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

```
vserver iscsi isns start -vserver SVM_name
```

Beheben Sie iSCSI-Fehlermeldungen auf dem Speichersystem

Es gibt eine Reihe von gängigen iSCSI-bezogenen Fehlermeldungen, die Sie mit dem `event log show` Befehl anzeigen können. Sie müssen wissen, was diese Nachrichten

bedeuten und was Sie tun können, um die Probleme zu lösen, die sie identifizieren.

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

Nachricht	Erklärung	Was zu tun ist
ISCSI: network interface identifier disabled for use; incoming connection discarded	Der iSCSI-Dienst ist auf der Schnittstelle nicht aktiviert.	Sie können das verwenden <code>iscsi interface enable</code> Befehl zum Aktivieren des iSCSI-Dienstes auf der Schnittstelle. Beispiel: <code>iscsi interface enable -vserver vs1 -lif lif1</code>
ISCSI: Authentication failed for initiator nodename	CHAP ist für den angegebenen Initiator nicht ordnungsgemäß konfiguriert.	Sie sollten die CHAP-Einstellungen überprüfen. Sie können denselben Benutzernamen und dasselbe Kennwort für ein- und ausgehende Einstellungen auf dem Speichersystem nicht verwenden: <ul style="list-style-type: none">• Eingehende Anmeldeinformationen auf dem Speichersystem müssen mit den Outbound-Anmeldedaten auf dem Initiator übereinstimmen.• Die Anmeldeinformationen für ausgehende Anrufe auf dem Speichersystem müssen mit den eingehenden Anmeldeinformationen auf dem Initiator übereinstimmen.

Aktivieren oder deaktivieren Sie den automatischen iSCSI LIF-Failover

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

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

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

- Auf der SVM befinden sich keine iSCSI LIFs

- Alle iSCSI-LIFs auf der SVM sind für automatisches LIF Failover aktiviert

Aktivieren Sie automatisches iSCSI LIF Failover

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

Weitere Informationen zu ["LIF Failover und Giveback"](#).

Schritt

1. Aktivieren Sie automatischen Failover für eine iSCSI LIF:

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

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

Deaktivieren Sie den automatischen iSCSI-LIF-Failover

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

Schritt

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

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

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

Verwandte Informationen

- ["Erstellen eines LIF"](#)
- Manuell ["Migrieren Sie LIF"](#)
- Manuell ["Zurücksetzen einer LIF auf seinen Home Port"](#)
- ["Konfigurieren Sie die Failover-Einstellungen auf einem LIF"](#)

Management des FC-Protokolls

Konfigurieren Sie eine SVM für FC

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

Bevor Sie beginnen

Sie müssen eine FC-Lizenz (["Im Lieferumfang von ONTAP One enthalten"](#)) Und es muss aktiviert sein. Wenn

die FC-Lizenz nicht aktiviert ist, werden die LIFs und SVMs online angezeigt, während der Betriebsstatus jedoch lautet `down`. Der FC-Service muss aktiviert sein, damit Ihre LIFs und SVMs funktionsfähig sind. Zum Hosten der Initiator-Zoning müssen Sie das einzelne Initiator-Zoning für alle FC-LIFs in der SVM verwenden.

Über diese Aufgabe

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

Beispiel 8. Schritte

System Manager

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

So konfigurieren Sie FC auf einer neuen Storage-VM	So konfigurieren Sie FC für eine vorhandene Storage-VM
<ol style="list-style-type: none">1. Klicken Sie im System Manager auf Storage > Storage VMs und dann auf Hinzufügen.2. Geben Sie einen Namen für die Storage-VM ein.3. Wählen Sie * FC* für das Zugriffsprotokoll.4. Klicken Sie auf FC aktivieren. + die FC-Ports werden automatisch zugewiesen.5. Klicken Sie Auf Speichern.	<ol style="list-style-type: none">1. Klicken Sie im System Manager auf Storage > Storage VMs.2. Klicken Sie auf die zu konfigurierende Speicher-VM.3. Klicken Sie auf die Registerkarte Einstellungen und dann auf  Neben dem FC-Protokoll.4. Klicken Sie auf FC aktivieren und geben Sie die IP-Adresse und die Subnetzmaske für die Netzwerkschnittstelle ein. + die FC-Ports werden automatisch zugewiesen.5. Klicken Sie Auf Speichern.

CLI

1. FC-Service für die SVM aktivieren:

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

2. Erstellen Sie zwei LIFs für die SVMs auf jedem Node, der FC-Services bereitstellt:

- Für ONTAP 9.6 und höher:

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

- Für ONTAP 9.5 und früher:

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

3. Vergewissern Sie sich, dass Ihre LIFs erstellt wurden und dass ihr Betriebsstatus lautet online:

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

Verwandte Informationen

["NetApp Support"](#)

["NetApp Interoperabilitäts-Matrix-Tool"](#)

[Überlegungen zu LIFs in Cluster-SAN-Umgebungen](#)

Löschen Sie einen FC-Service für eine SVM

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

Was Sie benötigen

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

Schritte

1. Verwenden Sie die `vserver fcp stop` Befehl zum Beenden der I/O-Vorgänge auf der LUN.

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

2. Verwenden Sie die `vserver fcp delete` Befehl zum Entfernen des Service aus der SVM.

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

3. Verwenden Sie die `vserver fcp show` Um zu überprüfen, ob Sie den FC-Service von Ihrer SVM gelöscht haben:

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

Empfohlene MTU-Konfigurationen für FCoE Jumbo Frames

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

Managen des NVMe-Protokolls

Starten Sie den NVMe-Service für eine SVM

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

Bevor Sie beginnen

NVMe muss als Protokoll auf Ihrem System zugelassen sein.

Folgende NVMe-Protokolle werden unterstützt:

Protokoll	Beginnend mit ...	Zulässig von...
TCP	ONTAP 9.10.1	Standard
FCP	ONTAP 9.4	Standard

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

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

```
vserver nvme show
```

3. Erstellung des NVMe-Protokollservice:

```
vserver nvme create
```

4. Starten des NVMe-Protokollservice auf der SVM:

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

Löschen des NVMe-Service aus einer SVM

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

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

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

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

3. Löschen Sie den NVMe-Service:


```
vserver nvme delete
```

Größe eines Namespace ändern

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

Vergrößern Sie den Namespace

System Manager

1. Klicken Sie auf **Storage > NVMe Namespaces**.
2. Klicken Sie auf den Namespace, den Sie vergrößern möchten , Und klicken Sie dann auf **Bearbeiten**.
3. Ändern Sie unter **CAPACITY** die Größe des Namespace.

CLI

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

Verkleinern Sie die Größe eines Namespace

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

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Verkleinern Sie die Größe des Namespace:

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

Konvertieren eines Namespace in eine LUN

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

Bevor Sie beginnen

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

Schritte

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

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

In-Band-Authentifizierung über NVMe einrichten

Ab ONTAP 9.12.1 können Sie die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um die bandinterne (sichere), bidirektionale und unidirektionale Authentifizierung zwischen einem NVMe Host und Controller über die NVMe/TCP- und NVMe/FC-Protokolle unter Verwendung der DH-HMAC-CHAP-Authentifizierung zu konfigurieren. Ab ONTAP 9.14.1

kann die in-Band-Authentifizierung in System Manager konfiguriert werden.

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

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

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

System Manager

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

Schritte

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

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

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

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

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

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

CLI

Schritte

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

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

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


```
vserver nvme subsystem host show
```

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

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

```
vserver nvme subsystem controller show
```

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

In-Band-Authentifizierung über NVMe deaktiviert

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

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

Schritte

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

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

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

```
vserver nvme subsystem host show
```

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

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

Ändern der NVMe-Host-Priorität

Ab ONTAP 9.14.1 können Sie das NVMe-Subsystem so konfigurieren, dass es die Ressourcenzuweisung für bestimmte Hosts priorisiert. Wenn ein Host dem Subsystem hinzugefügt wird, wird ihm standardmäßig eine reguläre Priorität zugewiesen. Hosts, denen eine hohe Priorität zugewiesen ist, werden eine größere Anzahl von I/O-Warteschlangen und eine größere Warteschlangentiefe zugewiesen.

Mithilfe der ONTAP Befehlszeilenschnittstelle (CLI) kann die Standardpriorität manuell von „Normal“ auf „hoch“ geändert werden. Um die einem Host zugewiesene Priorität zu ändern, müssen Sie den Host aus dem Subsystem entfernen und ihn dann wieder hinzufügen.

Schritte

1. Vergewissern Sie sich, dass die Host-Priorität auf „Normal“ eingestellt ist:

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

2. Entfernen Sie den Host aus dem Subsystem:

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

3. Überprüfen Sie, ob der Host aus dem Subsystem entfernt wurde:

```
vserver nvme subsystem host show
```

4. Fügen Sie den Host wieder dem Subsystem mit hoher Priorität hinzu:

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

Management automatischer Hosterkennung von NVMe/TCP Controllern

Ab ONTAP 9.14.1 ist die Host-Erkennung von Controllern über das NVMe/TCP-Protokoll in IP-basierten Fabrics standardmäßig automatisiert.

Automatische Host-Erkennung von NVMe/TCP Controllern

Wenn Sie die automatische Hosterkennung zuvor deaktiviert haben, Ihre Anforderungen jedoch geändert haben, können Sie sie erneut aktivieren.

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

2. Automatische Erkennung aktivieren:

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

3. Überprüfen Sie, ob die automatische Erkennung von NVMe/TCP-Controllern aktiviert ist.

```
vserver nvme show
```

Deaktivieren Sie die automatische Host-Erkennung von NVMe/TCP-Controllern

Wenn NVMe/TCP-Controller nicht automatisch von Ihrem Host erkannt werden müssen und Sie unerwünschten Multicast-Datenverkehr in Ihrem Netzwerk erkennen, sollten Sie diese Funktion deaktivieren.

Schritte

1. Wechseln Sie in den erweiterten Berechtigungsmodus:

```
set -privilege advanced
```

2. Automatische Erkennung deaktivieren:

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

3. Vergewissern Sie sich, dass die automatische Erkennung von NVMe/TCP-Controllern deaktiviert ist.

```
vserver nvme show
```

Deaktivieren Sie die Kennung der virtuellen NVMe-Host-Maschine

Ab ONTAP 9.14.1 unterstützt ONTAP standardmäßig die Möglichkeit von NVMe/FC-Hosts, Virtual Machines über eine eindeutige Kennung zu identifizieren und für NVMe/FC-Hosts die Auslastung der Virtual-Machine-Ressourcen zu überwachen. Dies verbessert die hostseitige Berichterstellung und Fehlerbehebung.

Sie können diese Funktion mit dem Bootarg deaktivieren.

Schritt

1. Deaktivieren Sie die Kennung der virtuellen Maschine:

```
bootargs set fct_sli_appid_off <port>, <port>
```

Im folgenden Beispiel wird die VMID auf Port 0g und Port 0i deaktiviert.

```
bootargs set fct_sli_appid_off 0g,0i

fct_sli_appid_off == 0g,0i
```

Verwalten Sie Systeme mit FC-Adapttern

Verwalten Sie Systeme mit FC-Adapttern

Zur Verwaltung von integrierten FC-Adapttern und FC-Adapterkarten sind Befehle verfügbar. Mit diesen Befehlen können der Adaptermodus konfiguriert, Adapterinformationen angezeigt und die Geschwindigkeit geändert werden.

Die meisten Storage-Systeme verfügen über integrierte FC-Adapter, die als Initiator oder Ziele konfiguriert werden können. Sie können auch FC-Adapterkarten verwenden, die als Initiator oder Ziele konfiguriert sind. Initiator verbinden sich mit Back-End-Festplatten-Shelves und möglicherweise mit anderen Storage-Arrays (FlexArray). Ziele werden nur mit FC Switches verbunden. Sowohl die FC-Ziel-HBA-Ports als auch die Switch-Port-Geschwindigkeit sollten auf den gleichen Wert gesetzt werden und sollten nicht auf die automatische Einstellung eingestellt werden.

Verwandte Informationen

Befehle zum Verwalten von FC-Adapttern

Sie können FC-Befehle verwenden, um FC Target-Adapter, FC Initiator-Adapter und integrierte FC-Adapter für Ihren Storage Controller zu verwalten. Mit den gleichen Befehlen werden FC-Adapter für das FC-Protokoll und das FC-NVMe-Protokoll verwaltet.

Befehle für FC Initiator-Adapter funktionieren nur auf Node-Ebene. Sie müssen den verwenden `run -node node_name` Befehl bevor Sie die Befehle des FC-Initiator-Adapters verwenden können.

Befehle zum Verwalten von FC-Zieladapttern

Ihr Ziel ist	Befehl
Zeigt FC-Adapterinformationen auf einem Node an	<code>network fcp adapter show</code>
Ändern Sie die FC-Zieladapterparameter	<code>network fcp adapter modify</code>
Zeigt Informationen zum FC-Protokoll-Datenverkehr an	<code>run -node node_name sysstat -f</code>
Anzeigen der Dauer des FC-Protokolls	<code>run -node node_name uptime</code>
Adapterkonfiguration und -Status anzeigen	<code>run -node node_name sysconfig -v adapter</code>
Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen	<code>run -node node_name sysconfig -ac</code>
Zeigen Sie eine man-Page für einen Befehl an	<code>man command_name</code>

Befehle zum Verwalten von FC-Initiator-Adapttern

Ihr Ziel ist	Befehl
Zeigt Informationen zu allen Initiatoren und ihren Adaptern in einem Node an	<code>run -node node_name storage show adapter</code>
Adapterkonfiguration und -Status anzeigen	<code>run -node node_name sysconfig -v adapter</code>
Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen	<code>run -node node_name sysconfig -ac</code>

Befehle zum Verwalten der integrierten FC-Adapter

Ihr Ziel ist	Befehl
Zeigt den Status der integrierten FC-Ports an	<pre>run -node <i>node_name</i> system hardware unified-connect show</pre>

Konfigurieren Sie FC-Adapter

Jeder integrierte FC-Port kann individuell als Initiator oder Ziel konfiguriert werden. Die Ports auf bestimmten FC-Adaptoren können auch einzeln als Ziel-Port oder als Initiator-Port konfiguriert werden, genau wie die integrierten FC-Ports. Eine Liste der Adapter, die für den Zielmodus konfiguriert werden können, ist im verfügbar ["NetApp Hardware Universe"](#).

Der Zielmodus wird verwendet, um die Ports mit FC-Initiatoren zu verbinden. Der Initiator-Modus wird verwendet, um die Ports mit Bandlaufwerken, Tape Libraries oder Storage von Drittanbietern mit FlexArray Virtualisierung oder dem Import fremder LUNs (Foreign LUN Import, FLI) zu verbinden.

Bei der Konfiguration von FC-Adaptoren für das FC-Protokoll und das FC-NVMe-Protokoll kommen die gleichen Schritte zum Einsatz. Jedoch unterstützen nur bestimmte FC-Adapter FC-NVMe. Siehe ["NetApp Hardware Universe"](#) Für eine Liste von Adaptern, die das FC-NVMe-Protokoll unterstützen

Konfigurieren Sie FC-Adapter für den Zielmodus

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

```
node run -node node_name storage disable adapter adapter_name
```

Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

2. Ändern Sie den Adapter von Initiator zu Ziel:

```
system hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
4. Vergewissern Sie sich, dass der Zielport die richtige Konfiguration hat:

```
network fcp adapter show -node node_name
```

5. Schalten Sie Ihren Adapter online:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

Konfigurieren Sie FC-Adapter für den Initiator-Modus

Was Sie benötigen

- LIFs auf dem Adapter müssen von allen Port-Sets, deren Mitglieder sie sind, entfernt werden.

- Alle LIFs von jeder Storage Virtual Machine (SVM), die den zu ändernden physischen Port verwendet, müssen migriert oder zerstört werden, bevor sie die Persönlichkeit des physischen Ports von Ziel zu Initiator ändern.



NVMe/FC unterstützt Initiatormodus.

Schritte

1. Entfernen Sie alle LIFs vom Adapter:

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

2. Versetzen Sie Ihren Adapter in den Offline-Modus:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

3. Ändern Sie den Adapter von Ziel zu Initiator:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
5. Vergewissern Sie sich, dass die FC-Ports für Ihre Konfiguration im richtigen Status konfiguriert sind:

```
system hardware unified-connect show
```

6. Versetzen Sie den Adapter wieder in den Online-Modus:

```
node run -node node_name storage enable adapter adapter_port
```

Zeigen Sie Adaptereinstellungen an

Mit bestimmten Befehlen können Sie Informationen zu Ihren FC-/UTA-Adaptoren anzeigen.

FC Target-Adapter

Schritt

1. Verwenden Sie die `network fcp adapter show` Befehl zum Anzeigen von Adapterinformationen:

```
network fcp adapter show -instance -node node1 -adapter 0a
```

Die Ausgabe zeigt für jeden verwendeten Steckplatz Informationen zur Systemkonfiguration und Adapterinformationen an.

Unified Target Adapter (UTA) X1143A-R6

Schritte

1. Starten Sie den Controller, ohne die angeschlossenen Kabel zu verwenden.

2. Führen Sie die aus `system hardware unified-connect show` Befehl zum Anzeigen der Portkonfiguration und der Module.
3. Zeigen Sie die Portinformationen an, bevor Sie den CNA und die Ports konfigurieren.

Ändern Sie den UTA2-Port vom CNA-Modus in den FC-Modus

Sie sollten den UTA2-Port vom Converged Network Adapter (CNA)-Modus in den Fibre Channel (FC)-Modus ändern, um den FC-Initiator und den FC-Zielmodus zu unterstützen. Sie sollten die Persönlichkeit vom CNA-Modus in den FC-Modus ändern, wenn Sie das physische Medium ändern müssen, das den Port mit seinem Netzwerk verbindet.

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin down
```

2. Ändern des Portmodus:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Booten Sie den Node neu, und versetzen Sie den Adapter dann in den Online-Modus:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin up
```

4. Benachrichtigen Sie den Administrator oder VIF-Manager, dass er den Port löschen oder entfernen soll, falls zutreffend:

- Wenn der Port als Home Port einer logischen Schnittstelle verwendet wird, ist ein Mitglied einer Interface Group (ifgrp), oder Hosts VLANs, dann sollte ein Administrator Folgendes tun:
 - i. Verschieben Sie die LIFs, entfernen Sie den Port aus dem ifgrp oder löschen Sie die VLANs.
 - ii. Löschen Sie den Port manuell, indem Sie den ausführen `network port delete` Befehl.

Wenn der `network port delete` Der Befehl schlägt fehl, der Administrator sollte die Fehler beheben, und führen Sie dann den Befehl erneut aus.

- Wenn der Port nicht als Home-Port einer LIF verwendet wird, kein Mitglied eines ifgrp ist und keine VLANs hostet, dann sollte der VIF-Manager den Port zum Zeitpunkt des Neustarts aus seinen Datensätzen entfernen.

Wenn der VIF-Manager den Port nicht entfernt, muss der Administrator ihn nach dem Neustart manuell entfernen, indem er die verwendet `network port delete` Befehl.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast Domain	Link MTU	Speed (Mbps)	Health
				Admin/Oper	Status


```

-----
...
e0i      Default      Default      down 1500  auto/10  -
e0f      Default      Default      down 1500  auto/10  -
...

net-f8040-34::> ucadmin show

Admin
Node      Adapter  Mode      Type      Pending  Pending
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
```

5. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Vor dem Ändern der Konfiguration auf dem Node sollten Sie für FC entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

Ändern Sie die optischen Module des CNA/UTA2-Zieladapters

Sie sollten die optischen Module auf dem Unified Target Adapter (CNA/UTA2) ändern, um den Personality-Modus zu unterstützen, den Sie für den Adapter ausgewählt haben.

Schritte

1. Überprüfen Sie das aktuelle SFP+, das in der Karte verwendet wird. Ersetzen Sie dann das aktuelle SFP+ durch das entsprechende SFP+ für die bevorzugte Persönlichkeit (FC oder CNA).
2. Entfernen Sie die aktuellen optischen Module vom X1143A-R6 Adapter.
3. Setzen Sie die richtigen Module für Ihre bevorzugte Personality-Mode-Optik (FC oder CNA) ein.
4. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Unterstützte SFP+-Module und Twinax-Kabel vom Cisco Logo (Copper Kabel) sind in *Hardware Universe* aufgeführt.

Verwandte Informationen

["NetApp Hardware Universe"](#)

Unterstützte Portkonfigurationen für X1143A-R6 Adapter

Der FC-Zielmodus ist die Standardkonfiguration für X1143A-R6-Adapterports. Die Ports auf diesem Adapter können jedoch entweder als 10-Gbit-Ethernet- und FCoE-Ports oder als 16-Gbit-FC-Ports konfiguriert werden.

Bei Konfiguration für Ethernet und FCoE unterstützen X1143A-R6 Adapter gleichzeitigen NIC- und FCoE-Zielverkehr auf demselben 10-GBE-Port. Bei Konfiguration für FC kann jedes Paar mit zwei Ports, das denselben ASIC verwendet, individuell für das FC-Ziel oder den FC-Initiator-Modus konfiguriert werden. Das bedeutet, dass ein einzelner X1143A-R6 Adapter einen FC-Zielmodus auf einem Paar mit zwei Ports und einen FC-Initiator-Modus auf einem anderen Paar mit zwei Ports unterstützen kann.

Verwandte Informationen

["NetApp Hardware Universe"](#)

["SAN-Konfiguration"](#)

Konfigurieren Sie die Ports

Um den Unified Target Adapter (X1143A-R6) zu konfigurieren, müssen die beiden benachbarten Ports auf demselben Chip im selben Personality-Modus konfiguriert werden.

Schritte

1. Konfigurieren Sie die Ports mithilfe des nach Bedarf für Fibre Channel (FC) oder Converged Network Adapter (CNA) `system node hardware unified-connect modify` Befehl.
2. Schließen Sie die entsprechenden Kabel für FC- oder 10-Gbit-Ethernet an.
3. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Für FC sollten Sie basierend auf der FC-Fabric, mit der verbunden ist, entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

Vermeiden Sie den Verlust der Konnektivität bei Verwendung des X1133A-R6-Adapters

Sie können den Verlust der Konnektivität bei einem Port-Ausfall verhindern, indem Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfigurieren.

Der X1133A-R6 HBA ist ein 16 GB FC-Adapter mit 4 Ports, der aus zwei 2-Port-Paaren besteht. Der X1133A-R6 Adapter kann als Zielmodus oder Initiatormodus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (z. B. Port 1 und Port 2 auf ASIC 1 und Port 3 und Port 4 auf ASIC 2). Beide Ports auf einem einzelnen ASIC müssen für die Ausführung im gleichen Modus – entweder im Ziel- oder im Initiatormodus – konfiguriert werden. Wenn ein Fehler auftritt, bei dem der ASIC ein Paar unterstützt, werden beide Ports im Paar offline geschaltet.

Um diesen Verlust der Konnektivität zu vermeiden, konfigurieren Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden.

Management von LIFs für alle SAN-Protokolle

Management von LIFs für alle SAN-Protokolle

Initiatoren müssen für die Failover-Funktion von Clustern in einer SAN-Umgebung Multipath I/O (MPIO) und Asymmetric Logical Unit Access (ALUA) verwenden. Wenn ein Node ausfällt, migrieren LIFs nicht oder übernehmen keine IP-Adressen des ausgefallenen Partner-Node. Stattdessen ist die MPIO-Software mit ALUA auf dem Host für die Auswahl der entsprechenden Pfade für den LUN-Zugriff über LIFs verantwortlich.

Sie müssen von jedem Node in einem HA-Paar einen oder mehrere iSCSI-Pfade erstellen. Dazu verwenden Sie logische Schnittstellen (LIFs), um den Zugriff auf LUNs zu ermöglichen, die vom HA-Paar verarbeitet

werden. Sie sollten eine Management-LIF für jede Storage Virtual Machine (SVM) konfigurieren, die SAN unterstützt.

Für die Konnektivität wird Direct Connect oder der Einsatz von Ethernet-Switches unterstützt. Sie müssen für beide Konnektivitätstypen LIFs erstellen.

- Sie sollten eine Management-LIF für jede Storage Virtual Machine (SVM) konfigurieren, die SAN unterstützt.
Sie können zwei LIFs pro Node konfigurieren, eine für jede Fabric, die bei FC verwendet wird, und Ethernet-Netzwerke für iSCSI trennen.

Nach der Erstellung von LIFs können sie aus den Port-Sets entfernt, auf andere Nodes innerhalb einer Storage Virtual Machine (SVM) verschoben und gelöscht werden.

Verwandte Informationen

- ["Konfiguration der LIFs über zeiw"](#)
- ["Erstellen eines LIF"](#)

Konfigurieren Sie eine NVMe-LIF

Bei der Konfiguration von NVMe LIFs müssen bestimmte Anforderungen erfüllt werden.

Bevor Sie beginnen

NVMe muss von dem FC-Adapter unterstützt werden, auf dem Sie das LIF erstellen. Unterstützte Adapter sind in aufgeführt ["Hardware Universe"](#).

Über diese Aufgabe

Ab ONTAP 9.12.1 und höher können zwei NVMe LIFs pro Node auf maximal 12 Nodes konfiguriert werden. In ONTAP 9.11.1 und älteren Versionen können Sie zwei NVMe LIFs pro Node auf maximal zwei Nodes konfigurieren.

Beim Erstellen einer NVMe LIF gelten die folgenden Regeln:

- NVMe kann das einzige Datenprotokoll auf Daten-LIFs sein.
- Sie sollten eine Management-LIF für jede SVM konfigurieren, die SAN unterstützt.
- Bei ONTAP 9.5 und höher müssen Sie eine NVMe LIF auf dem Node, der den Namespace enthält, und auf dem HA-Partner des Node konfigurieren.
- Nur bei ONTAP 9.4:
 - NVMe LIFs und Namespaces müssen auf demselben Node gehostet werden.
 - Es kann nur eine NVMe-Daten-LIF pro SVM konfiguriert werden.

Schritte

1. Erstellen des LIF:

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role  
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>  
-home-port <home_port>
```



NVME/TCP ist ab ONTAP 9.10.1 und höher verfügbar.

2. Vergewissern Sie sich, dass das LIF erstellt wurde:

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

Nach der Erstellung achten NVMe/TCP LIFs auf die Erkennung an Port 8009.

Was muss vor dem Verschieben einer SAN-LIF wissen

Sie müssen nur eine LIF-Verschiebung durchführen, wenn Sie den Inhalt des Clusters ändern, beispielsweise das Hinzufügen von Nodes zum Cluster oder das Löschen von Nodes aus dem Cluster. Wenn Sie eine LIF-Verschiebung durchführen, müssen Sie Ihre FC-Fabric nicht erneut Zone zuweisen oder neue iSCSI-Sitzungen zwischen den verbundenen Hosts Ihres Clusters und der neuen Zielschnittstelle erstellen.

Sie können ein SAN-LIF nicht mit verschieben `network interface move` Befehl. SAN LIF-Verschiebung muss durchgeführt werden, indem die LIF offline geschaltet, die LIF zu einem anderen Home Node oder Port verschoben und anschließend an ihrem neuen Speicherort wieder online geschaltet wird. ALUA (Asymmetric Logical Unit Access) bietet redundante Pfade und automatische Pfadauswahl als Teil einer ONTAP SAN-Lösung. Daher gibt es keine I/O-Unterbrechung, wenn das LIF für die Verschiebung offline geschaltet wird. Der Host versucht einfach erneut, und verschiebt I/O dann zu einer anderen LIF.

Mithilfe der LIF-Verschiebung können Sie folgende Aufgaben unterbrechungsfrei ausführen:

- Ersetzen Sie ein HA-Paar eines Clusters durch ein aktualisiertes HA-Paar. Dies ist für Hosts, die auf LUN-Daten zugreifen, transparent
- Aktualisieren einer Zielschnittstellenkarte
- Verschieben Sie die Ressourcen einer Storage Virtual Machine (SVM) von einem Node-Satz in einem Cluster zu einer anderen Gruppe von Nodes im Cluster

Entfernen Sie ein SAN-LIF aus einem Portsatz

Wenn das LIF, das Sie löschen oder verschieben möchten, sich in einem Port-Satz befindet, müssen Sie die LIF aus dem Portsatz entfernen, bevor Sie die LIF löschen oder verschieben können.

Über diese Aufgabe

Sie müssen Schritt 1 im folgenden Verfahren nur ausführen, wenn sich eine LIF im Portsatz befindet. Sie können die letzte LIF nicht in einem Portsatz entfernen, wenn der Port-Satz an eine Initiatorgruppe gebunden ist. Andernfalls können Sie mit Schritt 2 beginnen, wenn sich mehrere LIFs im Port-Satz befinden.

Schritte

1. Wenn sich nur ein LIF im Portsatz befindet, verwenden Sie den `lun igroup unbind` Befehl zum Aufheben der Bindung des PortSatzes an die Initiatorgruppe.



Wenn Sie die Bindung einer Initiatorgruppe von einem Portsatz aufheben, haben alle Initiatoren in der Initiatorgruppe Zugriff auf alle Ziel-LUNs, die der Initiatorgruppe auf allen Netzwerkschnittstellen zugeordnet sind.

```
cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
```

2. Verwenden Sie die `lun portset remove` Befehl zum Entfernen des LIF vom Portsatz.

```
cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
```

Verschieben Sie ein SAN-LIF

Wenn ein Node offline geschaltet werden muss, können Sie eine SAN-LIF verschieben, um seine Konfigurationsinformationen wie seinen WWPN beizubehalten und zu vermeiden, das UmZoning der Switch-Fabric zu vermeiden. Da eine SAN LIF offline geschaltet werden muss, bevor sie verschoben wird, muss der Host-Traffic auf die Multipathing-Software des Hosts zurückgreifen, um einen unterbrechungsfreien Zugriff auf die LUN zu ermöglichen. Sie können SAN-LIFs auf beliebige Nodes in einem Cluster verschieben, jedoch können Sie die SAN-LIFs nicht zwischen Storage Virtual Machines (SVMs) verschieben.

Was Sie benötigen

Wenn die LIF Mitglied eines Port-Satzes ist, muss die LIF aus dem Portsatz entfernt worden sein, bevor die LIF zu einem anderen Node verschoben werden kann.

Über diese Aufgabe

Der Ziel-Node und der physische Port für eine LIF, die Sie verschieben möchten, müssen sich in derselben FC-Fabric oder einem Ethernet-Netzwerk befinden. Wenn Sie ein LIF auf ein anderes Fabric verschieben, das nicht richtig begrenzt wurde, oder wenn Sie ein LIF in ein Ethernet-Netzwerk verschieben, das keine Verbindung zwischen iSCSI-Initiator und Ziel hat, ist die LUN nicht zugänglich, wenn Sie sie wieder in den Online-Modus versetzen.

Schritte

1. Anzeigen des Administrations- und Betriebsstatus der LIF:

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

2. Ändern Sie den Status des LIF in down (Offline):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin  
down
```

3. Weisen Sie der LIF einen neuen Node und neuen Port zu:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node  
node_name -home-port port_name
```

4. Ändern Sie den Status des LIF in up (Online):

```
network interface modify -vserver vserver_name -lif LIF_name -status-admin up
```

5. Überprüfen Sie Ihre Änderungen:

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

Löschen eines LIF in einer SAN-Umgebung

Bevor Sie eine LIF löschen, sollten Sie sicherstellen, dass der mit der LIF verbundene Host über einen anderen Pfad auf die LUNs zugreifen kann.


Was Sie benötigen

Wenn die LIF, die Sie löschen möchten, Mitglied eines Port-Satzes ist, müssen Sie zuerst die LIF aus dem Portsatz entfernen, bevor Sie die LIF löschen können.

System Manager

Löschen Sie ein LIF mit ONTAP System Manager (9.7 und höher).

Schritte

1. Klicken Sie in System Manager auf **Netzwerk > Übersicht** und wählen Sie dann **Netzwerkschnittstellen** aus.
2. Wählen Sie die Storage-VM aus, von der Sie die LIF löschen möchten.
3. Klicken Sie Auf  Und wählen Sie **Löschen**.

CLI

Löschen Sie ein LIF mit der ONTAP CLI.

Schritte

1. Überprüfen Sie den Namen der LIF und den aktuellen Port, der gelöscht werden soll:

```
network interface show -vserver vs1 -lif lif1
```

2. Löschen Sie das LIF:

```
network interface delete
```

```
network interface delete -vserver vs1 -lif lif1
```

3. Überprüfen Sie, ob Sie das LIF gelöscht haben:

```
network interface show
```

```
network interface show -vserver vs1
```

Logical Status	Network	Current	Current Is
Vserver Interface	Admin/Oper	Address/Mask	Node Port
Home			
-----	-----	-----	-----

vs1			
lif2	up/up	192.168.2.72/24	node-01 e0b
true			
lif3	up/up	192.168.2.73/24	node-01 e0b
true			

SAN LIF-Anforderungen zum Hinzufügen von Nodes zu einem Cluster

Beim Hinzufügen von Nodes zu einem Cluster müssen bestimmte Überlegungen beachtet werden.

- Sie müssen auf den neuen Nodes je nach Bedarf LIFs erstellen, bevor Sie LUNs auf den neuen Nodes

erstellen.

- Sie müssen die LIFs von den Hosts gemäß den vom Host-Stack und Protokoll vorgegeben erkennen.
- Sie müssen auf den neuen Nodes LIFs erstellen, sodass die Verschiebung von LUNs und Volumes ohne Verwendung des Cluster Interconnect Netzwerks möglich ist.

Konfigurieren Sie iSCSI-LIFs, um FQDN an den Host-iSCSI SendTargets Discovery-Vorgang zurückzugeben

Ab ONTAP 9 können iSCSI-LIFs so konfiguriert werden, dass ein vollständig qualifizierter Domain-Name (FQDN) zurückgegeben wird, wenn ein Host-Betriebssystem einen iSCSI-SendTargets-Ermittlungsvorgang sendet. Die Rückgabe eines FQDN ist nützlich, wenn zwischen dem Host-Betriebssystem und dem Speicherdienst ein NAT-Gerät (Network Address Translation) vorhanden ist.

Über diese Aufgabe

IP-Adressen auf einer Seite des NAT-Geräts sind auf der anderen Seite bedeutungslos, aber FQDNs können auf beiden Seiten Bedeutung haben.



Die Interoperabilitätsgrenze für den FQDN-Wert beträgt 128 Zeichen auf allen Hostbetriebssystemen.

Schritte

1. Ändern Sie die Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

2. Konfigurieren Sie iSCSI-LIFs für die Rückgabe von FQDN:

```
vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name  
-sendtargets_fqdn FQDN
```

Im folgenden Beispiel sind die iSCSI-LIFs so konfiguriert, dass sie den FQDN storagehost-005.example.com zurückgeben.

```
vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn  
storagehost-005.example.com
```

3. Vergewissern Sie sich, dass sendtargets der FQDN ist:

```
vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
```

In diesem Beispiel wird storagehost-005.example.com im 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
```

Empfohlene Kombinationen aus Volume- und Datei- oder LUN-Konfiguration

Überblick über Empfohlene Kombinationen aus Volume- und Datei- oder LUN-Konfiguration

Je nach Applikations- und Administrationsanforderungen können bestimmte Kombinationen aus FlexVol Volume- und Datei- oder LUN-Konfigurationen verwendet werden. Wenn Sie die Vorteile und Kosten dieser Kombinationen verstehen, können Sie bestimmt werden, welche Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung geeignet ist.

Die folgenden Kombinationen aus Volume- und LUN-Konfigurationen werden empfohlen:

- Speicherreservierte Dateien oder LUNs mit Thick Volume Provisioning
- Dateien oder LUNs ohne Speicherplatz mit Thin Volume Provisioning
- Speicherreservierte Dateien oder LUNs mit semi-Thick Volume Provisioning

Sie können SCSI Thin Provisioning auf Ihren LUNs in Verbindung mit einer dieser Konfigurationskombinationen verwenden.

Speicherreservierte Dateien oder LUNs mit Thick Volume Provisioning

Vorteile:

- Alle Schreibvorgänge innerhalb von platzsparenden Dateien sind garantiert. Aufgrund eines unzureichenden Speicherplatzes werden sie nicht ausfallen.
- Es gibt keine Beschränkungen für die Storage-Effizienz und Datensicherungstechnologien auf dem Volume.

Kosten und Einschränkungen:

- Es muss genügend Speicherplatz vom Aggregat im Voraus reserviert werden, um das Thick Provisioning-Volume zu unterstützen.
- Der Speicherplatz, der der doppelten Größe der LUN entspricht, wird zum Zeitpunkt der Erstellung des LUN vom Volume zugewiesen.

Dateien oder LUNs ohne Speicherplatz mit Thin Volume Provisioning

Vorteile:

- Es gibt keine Beschränkungen für die Storage-Effizienz und Datensicherungstechnologien auf dem Volume.
- Der Speicherplatz wird nur dann zugewiesen, wenn er genutzt wird.

Kosten und Einschränkungen:

- Schreibvorgänge sind nicht garantiert; sie können ausfallen, wenn dem Volume der freie Speicherplatz ausgeht.

- Sie müssen den freien Speicherplatz im Aggregat effektiv verwalten, um zu verhindern, dass dem Aggregat der freie Speicherplatz knapp wird.

Speicherreservierte Dateien oder LUNs mit semi-Thick Volume Provisioning

Vorteile:

Im Vorfeld wird weniger Speicherplatz als bei der Bereitstellung von Thick Volumes reserviert, und eine Schreibgarantie für besten Aufwand ist weiterhin verfügbar.

Kosten und Einschränkungen:

- Bei dieser Option können Schreibvorgänge fehlschlagen.

Dieses Risiko können Sie mindern, indem Sie den freien Speicherplatz im Volume angemessen mit Volatilität abgleichen.

- Sie können sich nicht auf die Aufbewahrung von Datensicherungsobjekten wie Snapshot Kopien, FlexClone Dateien und LUNs verlassen.
- ONTAP Storage-Effizienzfunktionen zur gemeinsamen Blocknutzung sind nicht zulässig, die automatisch gelöscht werden können, einschließlich Deduplizierung, Komprimierung und ODX/Copy Offload.

Ermitteln Sie die richtige Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung

Durch das Beantworten einiger grundlegender Fragen zu Ihrer Umgebung können Sie die beste Konfiguration von FlexVol Volumes und LUNs für Ihre Umgebung ermitteln.

Über diese Aufgabe

Sie können LUN- und Volume-Konfigurationen für maximale Storage-Auslastung und für die Sicherheit von Schreibgarantien optimieren. Basierend auf Ihren Anforderungen an die Storage-Auslastung und der Möglichkeit, freien Speicherplatz schnell zu überwachen und aufzufüllen, müssen Sie das FlexVol Volume und die LUN-Volumes bestimmen, die für Ihre Installation geeignet sind.



Sie brauchen kein separates Volume für jede LUN.

Schritt

1. Verwenden Sie den folgenden Entscheidungsbaum, um die beste Kombination aus Volume- und LUN-Konfiguration für Ihre Umgebung zu ermitteln:



Berechnen der Datenwachstumsrate für LUNs

Sie müssen die Geschwindigkeit kennen, mit der die LUN-Daten im Laufe der Zeit wachsen, um zu ermitteln, ob Sie platzsparende LUNs oder nicht-platzsparende LUNs verwenden sollten.

Über diese Aufgabe

Wenn Sie eine konstant hohe Datenwachstumsrate haben, dann sind platzreservierte LUNs möglicherweise die bessere Option für Sie. Wenn Ihre Datenwachstumsrate niedrig ist, sollten Sie nicht-Speicherplatz-reservierte LUNs in Erwägung ziehen.

Mit Tools wie OnCommand Insight können Sie die Datenwachstumsrate berechnen oder sie manuell berechnen. Die folgenden Schritte sind für die manuelle Berechnung.

Schritte

1. Richten Sie eine LUN ein, die Speicherplatz reserviert hat.
2. Überwachen Sie die Daten auf der LUN für einen bestimmten Zeitraum, z. B. für eine Woche.

Stellen Sie sicher, dass Ihr Überwachungszeitraum lang genug ist, um eine repräsentative Auswahl der regelmäßig auftretenden zunehmenden Datenmengen zu bilden. So wachsen die Datenmengen z. B. am Ende eines jeden Monats durchgängig sehr stark an.

3. Notieren Sie jeden Tag in GB, wie viele Daten wachsen.
4. Fügen Sie am Ende des Überwachungszeitraums die Gesamtbeträge für jeden Tag zusammen ein, und teilen Sie sie dann nach der Anzahl der Tage in Ihrem Überwachungszeitraum.

Diese Berechnung bringt Ihre durchschnittliche Wachstumsrate mit sich.

Beispiel

In diesem Beispiel benötigen Sie eine LUN mit 200 GB. Sie entscheiden sich, die LUN für eine Woche zu überwachen und die folgenden täglichen Datenänderungen aufzuzeichnen:

- Sonntag: 20 GB
- Montag: 18 GB
- Dienstag: 17 GB
- Mittwoch: 20 GB
- Donnerstag: 20 GB
- Freitag: 23 GB
- Samstag: 22 GB

In diesem Beispiel beträgt Ihre Wachstumsrate $(20+18+17+20+20+23+22) / 7 = 20$ GB pro Tag.

Konfigurationseinstellungen für platzreservierte Dateien oder LUNs mit Thick Provisioning Volumes

Diese Kombination aus FlexVol-Konfigurationen für Volumes und Dateien oder LUNs bietet die Möglichkeit, Storage-Effizienztechnologien zu nutzen. Sie müssen Ihren freien Speicherplatz nicht aktiv überwachen, da vorab ausreichend Speicherplatz zugewiesen wird.

Die folgenden Einstellungen sind erforderlich, um eine speziell für den Speicherplatz reservierte Datei oder ein LUN in einem Volume mit Thick Provisioning zu konfigurieren:

Lautstärkereinstellung	Wert
Garantie	Datenmenge
Fraktionale Reserve	100
Snapshot Reserve	Alle
Snapshot wird automatisches Löschen erstellt	Optional
Autogrow	Optional; bei Aktivierung muss der freie Speicherplatz des Aggregats aktiv überwacht werden.

Datei- oder LUN-Einstellung	Wert
Speicherplatzreservierung	Aktiviert

Konfigurationseinstellungen für Dateien oder LUNs, die nicht über Speicherplatz reserviert sind, mit Thin Provisioning Volumes

Diese Kombination aus FlexVol-Volume- und Datei- oder LUN-Konfiguration erfordert die kleinste Storage-Menge im Voraus. Es erfordert jedoch aktives, freies Speicherplatzmanagement, um Fehler aufgrund von mangelndem Speicherplatz zu

vermeiden.

Folgende Einstellungen sind erforderlich, um eine Datei oder ein LUN ohne Speicherplatz in einem Volume mit Thin Provisioning zu konfigurieren:

Lautstärkereinstellung	Wert
Garantie	Keine
Fraktionale Reserve	0
Snapshot Reserve	Alle
Snapshot wird automatisches Löschen erstellt	Optional
Autogrow	Optional

Datei- oder LUN-Einstellung	Wert
Speicherplatzreservierung	Deaktiviert

Weitere Überlegungen

Wenn der Speicherplatz des Volume oder Aggregats knapp wird, können Schreibvorgänge für die Datei oder LUN ausfallen.

Wenn Sie den freien Speicherplatz nicht sowohl für das Volume als auch für das Aggregat aktiv überwachen möchten, sollten Sie Autogrow für das Volume aktivieren und die maximale Größe für das Volume auf die Größe des Aggregats festlegen. In dieser Konfiguration müssen Sie den freien Speicherplatz des Aggregats aktiv überwachen, den freien Speicherplatz im Volume jedoch nicht überwachen.

Konfigurationseinstellungen für platzreservierte Dateien oder LUNs mit semi-Thick Volume Provisioning

Für diese Kombination aus Volume- und Datei- oder LUN-Konfiguration von FlexVol muss vorab weniger Storage zugewiesen werden als für die vollständig bereitgestellte Kombination. Es beschränkt jedoch die Effizienztechnologien, die Sie für das Volume verwenden können. Überschreibungen werden auf optimaler Basis dieser Konfigurationskombination erfüllt.

Die folgenden Einstellungen sind erforderlich, um eine reservierte LUN in einem Volume mit semi-Thick Provisioning zu konfigurieren:

Lautstärkereinstellung	Wert
Garantie	Datenmenge
Fraktionale Reserve	0

Lautstärkereinstellung	Wert
Snapshot Reserve	0
Snapshot wird automatisches Löschen erstellt	Bei einem Commit-Level der Zerstörung eine Liste mit allen Objekten, dem auf Volume eingestellten Auslöser und allen FlexClone LUNs und FlexClone Dateien für das automatische Löschen aktiviert.
Autogrow	Optional; bei Aktivierung muss der freie Speicherplatz des Aggregats aktiv überwacht werden.

Datei- oder LUN-Einstellung	Wert
Speicherplatzreservierung	Aktiviert

Technologische Beschränkungen

Sie können für diese Kombination nicht die folgenden Volume-Storage-Effizienztechnologien verwenden:

- Komprimierung
- Deduplizierung
- ODX und FlexClone Copy Offload
- FlexClone LUNs und FlexClone Dateien nicht zum automatischen Löschen markiert (aktive Klone)
- Unterdateien von FlexClone
- ODX/Copy-Offload

Weitere Überlegungen

Beim Einsatz dieser Konfigurationskombination müssen die folgenden Fakten beachtet werden:

- Wenn der Speicherplatz des Volumes, das die LUN unterstützt, knapp wird, werden Sicherungsdaten (FlexClone LUNs und Dateien, Snapshot Kopien) zerstört.
- Schreibvorgänge können rechtzeitig ausfallen, wenn der freie Speicherplatz auf dem Volume erschöpft ist.

Die Komprimierung ist für AFF Plattformen standardmäßig aktiviert. Sie müssen die Komprimierung explizit für jedes Volume deaktivieren, für das Sie semi-Thick Provisioning auf einer AFF Plattform verwenden möchten.

SAN Datensicherung

Datensicherungs-Methoden in SAN-Umgebungen im Überblick

Sie können Ihre Daten schützen, indem Sie Kopien davon erstellen, sodass sie bei versehentlichem Löschen, Applikationsabstürzen, Datenbeschädigung oder Ausfällen für eine Wiederherstellung verfügbar sind. Je nach Datensicherungs- und Backup-Anforderungen bietet ONTAP verschiedene Methoden zum Schutz Ihrer Daten.

SnapMirror Business Continuity (SM-BC)

Ab ONTAP 9.9 ist diese allgemeine Verfügbarkeit mit Zero Recovery Time Objective (RTO von Null) oder transparentem Applikations-Failover (TAF) möglich und ermöglicht ein automatisches Failover geschäftskritischer Applikationen in SAN-Umgebungen. SM-BC erfordert die Installation von ONTAP Mediator 1.2 in einer Konfiguration mit zwei AFF-Clustern oder zwei All-Flash SAN-Array (ASA)-Clustern.

["NetApp Dokumentation: SnapMirror Business Continuity"](#)

Snapshot Kopie

Ermöglicht Ihnen das manuelle oder automatische Erstellen, Planen und Pflegen mehrerer Backups Ihrer LUNs. Snapshot Kopien belegen nur eine minimale Menge an zusätzlichem Volume-Speicherplatz und liegen keine Performance-Kosten vor. Wenn Ihre LUN-Daten versehentlich geändert oder gelöscht werden, können diese Daten aus einer der neuesten Snapshot Kopien einfach und schnell wiederhergestellt werden.

FlexClone LUNs (FlexClone Lizenz erforderlich)

Erstellung zeitpunktgenauer, beschreibbarer Kopien einer anderen LUN in einem aktiven Volume oder in einer Snapshot Kopie Ein Klon und sein übergeordnetes Objekt können unabhängig voneinander geändert werden, ohne dass sich gegenseitig beeinträchtigen.

SnapRestore (Lizenz erforderlich)

Snapshot Kopien auf einem gesamten Volume ermöglichen eine schnelle, platzsparende Datenwiederherstellung nach Bedarf. Mit SnapRestore können Sie eine LUN auf einen früheren Zustand wiederherstellen, ohne das Storage-System neu zu booten.

Datensicherung Spiegelungskopien (SnapMirror Lizenz erforderlich)

Bietet asynchrone Disaster Recovery, da Sie die Möglichkeit haben, regelmäßig Snapshot-Kopien von Daten auf Ihrem Volume zu erstellen, diese Snapshot-Kopien über ein lokales oder Wide Area Network zu einem Partner-Volume zu kopieren, normalerweise in einem anderen Cluster. Diese Snapshot Kopien bleiben erhalten. Die gespiegelte Kopie auf dem Partner-Volume sorgt für eine rasche Verfügbarkeit und Wiederherstellung der Daten aus dem Zeitpunkt der letzten Snapshot Kopie, sofern die Daten auf dem Quell-Volume beschädigt oder verloren sind.

SnapVault Backups (SnapMirror Lizenz erforderlich)

Ermöglicht eine effiziente und langfristige Aufbewahrung von Backups. Mithilfe von SnapVault Beziehungen können Sie ausgewählte Snapshot Kopien von Volumes auf einem Ziel-Volume sichern und die Backups beibehalten.

Falls Sie Tape-Backups und Archivierungsvorgänge durchführen, können Sie sie auch für die Daten ausführen, die bereits auf dem sekundären SnapVault Volume gesichert sind.

SnapDrive für Windows oder UNIX (SnapDrive-Lizenz erforderlich)

Konfiguration des Zugriffs auf LUNs, Management von LUNs und Management von Snapshot Kopien des Storage-Systems direkt von einem Windows oder UNIX Host aus

Natives Tape-Backup und -Recovery

Die meisten vorhandenen Bandlaufwerke werden in ONTAP unterstützt und ebenfalls eine Methode für Tape-Anbieter, um neue Geräte dynamisch zu unterstützen. ONTAP unterstützt außerdem das Remote Magnetic

Tape (RMT)-Protokoll und ermöglicht so Backup und Recovery für jedes fähige System.

Verwandte Informationen

["NetApp Dokumentation: SnapDrive für UNIX"](#)

["NetApp Dokumentation: SnapDrive für Windows \(aktuelle Versionen\)"](#)

["Datensicherung mithilfe von Tape Backup"](#)

Auswirkung des Verschiebens oder Kopieren einer LUN auf Snapshot Kopien

Auswirkung des Verschiebens oder Kopieren einer LUN auf die Übersicht über Snapshot Kopien

Snapshot Kopien werden auf Volume-Ebene erstellt. Wenn Sie eine LUN kopieren oder verschieben auf ein anderes Volume, wird die Richtlinie für die Snapshot Kopie des Ziel-Volume auf das kopierte oder verschobene Volume angewendet. Wenn keine Snapshot Kopien für das Ziel-Volume erstellt werden, werden keine Snapshot Kopien von der verschobenen oder kopierten LUN erstellt.

Wiederherstellen einer einzelnen LUN aus einer Snapshot Kopie

Sie können eine einzelne LUN aus einer Snapshot-Kopie wiederherstellen, ohne das gesamte Volume, das die einzelne LUN enthält, wiederherzustellen. Sie können die LUN selbst oder einen neuen Pfad im Volume wiederherstellen. Der Vorgang stellt nur die einzelne LUN wieder her, ohne dass andere Dateien oder LUNs im Volume beeinträchtigt werden. Sie können Dateien auch mit Streams wiederherstellen.

Was Sie benötigen

- Sie müssen genügend Speicherplatz auf Ihrem Volume haben, um den Wiederherstellungsvorgang abzuschließen:
 - Wenn Sie eine platzreservierte LUN wiederherstellen, wo die fraktionale Reserve 0% beträgt, benötigen Sie ein Mal die Größe der wiederhergestellten LUN.
 - Wenn Sie eine platzreservierte LUN wiederherstellen, wo die fraktionale Reserve 100% beträgt, benötigen Sie die doppelte Größe der wiederhergestellten LUN.
 - Wenn Sie eine nicht-speicherreservierte LUN wiederherstellen, benötigen Sie nur den tatsächlich für die wiederhergestellte LUN verwendeten Speicherplatz.
- Eine Snapshot Kopie der Ziel-LUN muss erstellt worden sein.

Wenn der Wiederherstellungsvorgang fehlschlägt, kann die Ziel-LUN gekürzt werden. In diesen Fällen können Sie die Snapshot Kopie verwenden, um Datenverlust zu vermeiden.

- Eine Snapshot Kopie der Quell-LUN muss erstellt worden sein.

In seltenen Fällen kann die LUN-Wiederherstellung fehlschlagen, sodass die Quell-LUN nicht mehr verwendet werden kann. Wenn dies der Fall ist, können Sie die Snapshot Kopie verwenden, um die LUN kurz vor dem Wiederherstellungsversuch in den Zustand zurückzusetzen.

- Die Ziel-LUN und die Quell-LUN müssen den gleichen OS-Typ aufweisen.

Wenn die Ziel-LUN einen anderen OS-Typ als die Quell-LUN aufweist, kann der Host nach der

Wiederherstellung den Datenzugriff auf die Ziel-LUN verlieren.

Schritte

1. Beenden Sie vom Host den gesamten Host-Zugriff auf die LUN.
2. Heben Sie die Bereitstellung der LUN auf dem Host auf, damit der Host nicht auf die LUN zugreifen kann.
3. LUN-Zuordnung aufheben:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Legen Sie die Snapshot Kopie fest, die Sie Ihre LUN wiederherstellen möchten:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Erstellen Sie vor dem Wiederherstellen der LUN eine Snapshot Kopie der LUN:

```
volume snapshot create -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

6. Stellen Sie die angegebene LUN in einem Volume wieder her:

```
volume snapshot restore-file -vserver vserver_name -volume volume_name  
-snapshot snapshot_name -path lun_path
```

7. Befolgen Sie die Schritte auf dem Bildschirm.
8. Versetzen Sie die LUN bei Bedarf in den Online-Modus:

```
lun modify -vserver vserver_name -path lun_path -state online
```

9. Falls erforderlich, LUN erneut zuordnen:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

10. Mounten Sie die LUN vom Host neu.
11. Starten Sie den Zugriff auf die LUN vom Host aus neu.

Wiederherstellen aller LUNs in einem Volume aus einer Snapshot Kopie

Verwenden Sie können `volume snapshot restore` Befehl zum Wiederherstellen aller LUNs in einem bestimmten Volume aus einer Snapshot Kopie.

Schritte

1. Beenden Sie vom Host den gesamten Host-Zugriff auf die LUNs.

Die Verwendung von SnapRestore ohne die Unterbrechung des gesamten Host-Zugriffs auf LUNs im Volume kann zu Datenbeschädigungen und Systemfehlern führen.

2. Heben Sie die Bereitstellung der LUNs auf diesem Host auf, damit der Host nicht auf die LUNs zugreifen kann.

3. LUNs-Zuordnung aufheben:

```
lun mapping delete -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

4. Legen Sie die Snapshot Kopie fest, auf die Sie Ihr Volume wiederherstellen möchten:

```
volume snapshot show -vserver vserver_name -volume volume_name
```

5. Ändern Sie Ihre Berechtigungseinstellung in erweitert:

```
set -privilege advanced
```

6. Wiederherstellen von Daten:

```
volume snapshot restore -vserver vserver_name -volume volume_name -snapshot  
snapshot_name
```

7. Befolgen Sie die Anweisungen auf dem Bildschirm.

8. LUNs neu zuordnen:

```
lun mapping create -vserver vserver_name -volume volume_name -lun lun_name  
-igroup igroup_name
```

9. Vergewissern Sie sich, dass Ihre LUNs online sind:

```
lun show -vserver vserver_name -path lun_path -fields state
```

10. Wenn Ihre LUNs nicht online sind, bringen Sie sie in den Online-Modus:

```
lun modify -vserver vserver_name -path lun_path -state online
```

11. Ändern Sie Ihre Berechtigungseinstellung in admin:

```
set -privilege admin
```

12. Mounten Sie die LUNs vom Host neu.

13. Starten Sie den Zugriff auf Ihre LUNs vom Host aus neu.

Löschen Sie eine oder mehrere vorhandene Snapshot Kopien von einem Volume

Sie können eine oder mehrere vorhandene Snapshot Kopien manuell aus dem Volume löschen. Möglicherweise möchten Sie dies tun, wenn Sie mehr Platz auf Ihrem Volume benötigen.

Schritte

1. Verwenden Sie die `volume snapshot show` Befehl zum Überprüfen, welche Snapshot Kopien Sie löschen möchten.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3
```

Vserver	Volume	Snapshot	Size	---Blocks---	
				Total%	Used%
vs3	vol3				
		snap1.2013-05-01_0015	100KB	0%	38%
		snap1.2013-05-08_0015	76KB	0%	32%
		snap2.2013-05-09_0010	76KB	0%	32%
		snap2.2013-05-10_0010	76KB	0%	32%
		snap3.2013-05-10_1005	72KB	0%	31%
		snap3.2013-05-10_1105	72KB	0%	31%
		snap3.2013-05-10_1205	72KB	0%	31%
		snap3.2013-05-10_1305	72KB	0%	31%
		snap3.2013-05-10_1405	72KB	0%	31%
		snap3.2013-05-10_1505	72KB	0%	31%

10 entries were displayed.

2. Verwenden Sie die `volume snapshot delete` Befehl zum Löschen von Snapshot Kopien.

Ihr Ziel ist	Diesen Befehl eingeben...
Löschen einer einzelnen Snapshot Kopie	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name</code>
Mehrere Snapshot Kopien löschen	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot snapshot_name1[, snapshot_name2,...]</code>
Löschen Sie alle Snapshot Kopien	<code>volume snapshot delete -vserver svm_name -volume vol_name -snapshot *</code>

Im folgenden Beispiel werden alle Snapshot Kopien auf dem Volume vol3 gelöscht.

```
cluster::> volume snapshot delete -vserver vs3 -volume vol3 *
```

10 entries were acted on.

Setzen Sie FlexClone LUNs ein, um Ihre Daten zu schützen

Sichern Sie Ihre Übersicht mit FlexClone LUNs

Eine FlexClone LUN ist eine zeitpunktgenaue, beschreibbare Kopie einer anderen LUN in

einem aktiven Volume oder in einer Snapshot Kopie. Der Klon und sein übergeordnetes Objekt können unabhängig voneinander geändert werden, ohne dass sich gegenseitig beeinflussen.

Eine FlexClone LUN verwendet zunächst den Speicherplatz der übergeordneten LUN. Standardmäßig übernimmt die FlexClone LUN das space-reservierte Attribut der übergeordneten LUN. Wenn beispielsweise die übergeordnete LUN keinen Speicherplatz reserviert ist, ist die FlexClone LUN standardmäßig auch nicht-Speicherplatz-reserviert. Sie können jedoch eine FlexClone LUN erstellen, die nicht im Speicherplatz reserviert ist, von einem übergeordneten Objekt, das eine reservierte LUN ist.

Wenn Sie eine LUN klonen, erfolgt die gemeinsame Nutzung von Blöcken im Hintergrund und Sie können erst dann eine Volume-Snapshot-Kopie erstellen, wenn die Freigabe des Blocks abgeschlossen ist.

Sie müssen das Volume so konfigurieren, dass die automatische Löschung von FlexClone LUNs mit dem aktiviert wird `volume snapshot autodelete modify` Befehl. Wenn FlexClone LUNs automatisch gelöscht werden sollen, das Volume jedoch nicht für das automatische Löschen von FlexClone konfiguriert ist, wird keine der FlexClone LUNs gelöscht.

Wenn Sie eine FlexClone LUN erstellen, ist die automatische Löschung der FlexClone LUN standardmäßig deaktiviert. Sie müssen sie auf jeder FlexClone LUN manuell aktivieren, bevor die FlexClone LUN automatisch gelöscht werden kann. Wenn Sie die semi-Thick Volume-Bereitstellung nutzen und Sie die „Best Effort“-Garantie von dieser Option erhalten möchten, müssen Sie *all* FlexClone LUNs für das automatische Löschen zur Verfügung stellen.



Wenn Sie eine FlexClone LUN aus einer Snapshot Kopie erstellen, wird die LUN automatisch mithilfe eines platzsparenden Hintergrundprozesses von der Snapshot Kopie abgetrennt, damit die LUN nicht von der Snapshot Kopie abhängt oder zusätzlichen Speicherplatz belegt. Wenn dieser Hintergrundsplit noch nicht abgeschlossen wurde und diese Snapshot Kopie automatisch gelöscht wird, wird diese FlexClone LUN gelöscht, auch wenn Sie die automatische Löschungsfunktion von FlexClone für diese FlexClone LUN deaktiviert haben. Nachdem die Hintergrundspaltung abgeschlossen ist, wird die FlexClone LUN auch dann nicht gelöscht, wenn die Snapshot Kopie gelöscht wird.

Verwandte Informationen

["Logisches Storage-Management"](#)

Gründe für die Verwendung von FlexClone LUNs

Sie können FlexClone LUNs verwenden, um mehrere Kopien einer LUN mit Lese-/Schreibvorgängen zu erstellen.

Dies könnten Sie aus den folgenden Gründen tun:

- Sie müssen eine temporäre Kopie einer LUN zu Testzwecken erstellen.
- Sie müssen zusätzlichen Benutzern eine Kopie der Daten zugänglich machen, ohne ihnen den Zugang zu den Produktionsdaten zu ermöglichen.
- Sie möchten einen Klon einer Datenbank für Manipulationen und Hochrechnungen erstellen, während die ursprünglichen Daten in unveränderter Form beibehalten werden.
- Sie möchten auf eine bestimmte Untergruppe der Daten einer LUN zugreifen (ein bestimmtes logisches Volume oder Dateisystem in einer Volume-Gruppe, Oder eine bestimmte Datei oder einen bestimmten Dateisatz in einem Dateisystem) und ihre ursprüngliche LUN kopieren, ohne den Rest der Daten in der ursprünglichen LUN wiederherzustellen. Dies funktioniert auf Betriebssystemen, die das gleichzeitige

Mounten einer LUN und eines Klon der LUN unterstützen. SnapDrive für UNIX unterstützt dies mit dem `snap connect` Befehl.

- Sie benötigen mehrere SAN-Boot-Hosts mit demselben Betriebssystem.

Wie ein FlexVol Volume mithilfe von Autodelete-Einstellungen freien Speicherplatz zurückgewinnen kann

Sie können die Autodelete-Einstellung eines FlexVol Volume aktivieren, um FlexClone Dateien und FlexClone LUNs automatisch zu löschen. Durch Aktivieren von Autodelete können Sie bei fast vollem Volume freien Speicherplatz auf dem Volume zurückgewinnen.

Sie können ein Volume so konfigurieren, dass automatisch mit dem Löschen von FlexClone Dateien und FlexClone LUNs begonnen wird, wenn der freie Speicherplatz im Volume unter einen bestimmten Schwellenwert sinkt und das Löschen von Klonen automatisch beendet wird, wenn eine Zielmenge an freiem Speicherplatz im Volume zurückgewonnen wird. Obwohl Sie den Schwellenwert nicht angeben können, der das automatische Löschen von Klonen startet, können Sie angeben, ob ein Klon für das Löschen geeignet ist. Außerdem können Sie die Zielmenge an freiem Speicherplatz für ein Volume angeben.

Ein Volume löscht automatisch FlexClone Dateien und FlexClone LUNs, wenn der freie Speicherplatz im Volume unter einem bestimmten Schwellenwert abnimmt und *beide* der folgenden Anforderungen erfüllt werden:

- Die Funktion zum Löschen ist für das Volume aktiviert, das die Dateien von FlexClone sowie FlexClone LUNs enthält.

Sie können die Autodelete-Funktion für ein FlexVol Volume mithilfe von aktivieren `volume snapshot autodelete modify` Befehl. Sie müssen die einstellen `-trigger` Parameter an `volume` Oder `snap_reserve` Wenn ein Volume FlexClone Dateien und FlexClone LUNs automatisch löscht,

- Die Funktion zum Löschen ist für FlexClone Dateien und FlexClone LUNs aktiviert.

Sie können Autodelete für eine FlexClone Datei oder für FlexClone LUN aktivieren, indem Sie die verwenden `file clone create` Befehl mit dem `-autodelete` Parameter. Folglich können bestimmte FlexClone Dateien und FlexClone LUNs beibehalten werden, indem Autodelete für die Klone deaktiviert wird und sichergestellt wird, dass die Kloneinstellung bei anderen Volume-Einstellungen nicht außer Kraft gesetzt wird.

Konfigurieren Sie ein FlexVol Volume, um FlexClone Dateien und FlexClone LUNs automatisch zu löschen

Sie können ein FlexVol Volume zum automatischen Löschen von FlexClone Dateien und FlexClone LUNs mit aktivierter Autodelete aktivieren, wenn der freie Speicherplatz im Volume unter einen bestimmten Schwellenwert fällt.

Was Sie benötigen

- Das FlexVol Volume muss FlexClone Dateien und FlexClone LUNs enthalten und online sein.
- Das FlexVol Volume darf kein schreibgeschütztes Volume sein.

Schritte

1. Aktivieren Sie das automatische Löschen von FlexClone Dateien und FlexClone LUNs im FlexVol Volume

mithilfe von `volume snapshot autodelete modify` Befehl.

- Für das `-trigger` Parameter, den Sie angeben können `volume` Oder `snap_reserve`.
- Für das `-destroy-list` Parameter, müssen Sie immer angeben `lun_clone, file_clone` Unabhängig davon, ob Sie nur eine Klontyp löschen möchten. + das folgende Beispiel zeigt, wie Sie Volume `vol1` aktivieren können, um das automatische Löschen von FlexClone-Dateien und FlexClone LUNs für die Rückgewinnung von ungenutztem Speicherplatz zu aktivieren, bis 25% des Volumes aus freiem Speicherplatz besteht:

```
cluster1::> volume snapshot autodelete modify -vserver vs1 -volume  
vol1 -enabled true -commitment disrupt -trigger volume -target-free  
-space 25 -destroy-list lun_clone,file_clone
```

```
Volume modify successful on volume:vol1
```



Während Sie FlexVol-Volumes für automatisches Löschen aktivieren, wenn Sie den Wert von festlegen `-commitment` Parameter an `destroy`, Alle FlexClone Dateien und FlexClone LUNs mit dem `-autodelete` Parameter auf gesetzt `true` Wird möglicherweise gelöscht, wenn der freie Speicherplatz im Volume unter den angegebenen Schwellenwert sinkt. FlexClone Dateien und FlexClone LUNs mit dem jedoch `-autodelete` Parameter auf gesetzt `false` Wird nicht gelöscht.

2. Überprüfen Sie, ob das automatische Löschen von FlexClone Dateien und FlexClone LUNs im FlexVol Volume mithilfe von aktiviert ist `volume snapshot autodelete show` Befehl.

Das folgende Beispiel zeigt, dass Volume `vol1` für das automatische Löschen von FlexClone Dateien und FlexClone LUNs aktiviert ist:

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1  
  
Vserver Name: vs1  
Volume Name: vol1  
Enabled: true  
Commitment: disrupt  
Defer Delete: user_created  
Delete Order: oldest_first  
Defer Delete Prefix: (not specified)*  
Target Free Space: 25%  
Trigger: volume  
Destroy List: lun_clone,file_clone  
Is Constituent Volume: false
```

3. Stellen Sie sicher, dass Autodelete für die Dateien von FlexClone und die FlexClone LUNs im Volume aktiviert ist, die Sie löschen möchten, und führen Sie dazu folgende Schritte aus:
 - a. Aktivieren Sie das automatische Löschen einer bestimmten FlexClone Datei oder eines FlexClone LUN mithilfe von `volume file clone autodelete` Befehl.

Sie können das automatische Löschen einer bestimmten FlexClone Datei oder eines FlexClone LUN mithilfe von erzwingen `volume file clone autodelete` Befehl mit dem `-force` Parameter.

Das folgende Beispiel zeigt, dass das automatische Löschen der FlexClone LUN „lun1_Clone“ in Volume vol1 aktiviert ist:

```
cluster1::> volume file clone autodelete -vserver vs1 -clone-path  
/vol/vol1/lun1_clone -enabled true
```

Sie können Autodelete aktivieren, wenn Sie FlexClone Dateien und FlexClone LUNs erstellen.

- b. Überprüfen Sie, ob die FlexClone Datei oder das FlexClone LUN zum automatischen Löschen mit der aktiviert ist `volume file clone show-autodelete` Befehl.

Das folgende Beispiel zeigt, dass die FlexClone LUN „lun1_Clone“ für das automatische Löschen aktiviert ist:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone  
-path vol/vol1/lun1_clone  
  
Name: vs1 Vserver  
  
Path: vol/vol1/lun1_clone Clone  
  
**Autodelete Enabled: true**
```

Weitere Informationen über die Verwendung der Befehle finden Sie auf den jeweiligen man-Pages.

Klonen von LUNs aus einem aktiven Volume

Sie können Kopien Ihrer LUNs erstellen, indem Sie die LUNs im aktiven Volume klonen. Diese FlexClone LUNs sind lesbare und beschreibbare Kopien der Original-LUNs im aktiven Volume.

Was Sie benötigen

Eine FlexClone Lizenz muss installiert sein. Diese Lizenz ist im enthalten ["ONTAP One"](#).

Über diese Aufgabe

Eine platzreservierte FlexClone LUN benötigt genauso viel Speicherplatz wie die reservierte übergeordnete LUN. Falls die FlexClone LUN nicht reserviert ist, müssen Sie sicherstellen, dass das Volume über genügend Speicherplatz verfügt, um Änderungen an der FlexClone LUN gerecht zu werden.

Schritte

1. Sie müssen überprüft haben, ob die LUNs keiner Initiatorgruppe zugeordnet sind oder in geschrieben werden, bevor Sie den Klon erstellen.
2. Verwenden Sie die `lun show` Befehl zum Überprüfen, ob die LUN vorhanden ist.


```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1	online	unmapped	windows	47.07MB

3. Verwenden Sie die `volume file clone create` Befehl zum Erstellen der FlexClone LUN.

```
volume file clone create -vserver vs1 -volume vol1 -source-path lun1  
-destination-path/lun1_clone
```

Wenn die FlexClone LUN für das automatische Löschen verfügbar sein soll, schließen Sie Folgendes ein `-autodelete true`. Wenn Sie diese FlexClone LUN in einem Volume mit Semi-Thick Provisioning erstellen, müssen Sie das automatische Löschen für alle FlexClone LUNs aktivieren.

4. Verwenden Sie die `lun show` Befehl zum Überprüfen, ob Sie eine LUN erstellt haben.

```
lun show -vserver vs1
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/volX/lun1	online	unmapped	windows	47.07MB
vs1	/vol/volX/lun1_clone	online	unmapped	windows	47.07MB

Erstellung von FlexClone LUNs aus einer Snapshot Kopie in einem Volume

Sie können eine Snapshot Kopie in Ihrem Volume verwenden, um FlexClone Kopien Ihrer LUNs zu erstellen. Die FlexClone Kopien von LUNs sind sowohl lesbar als auch schreibbar.

Was Sie benötigen

Eine FlexClone Lizenz muss installiert sein. Diese Lizenz ist in enthalten ["ONTAP One"](#).

Über diese Aufgabe

Die FlexClone LUN übernimmt das Attribut für Platzreservierungen der übergeordneten LUN. Eine platzreservierte FlexClone LUN benötigt genauso viel Speicherplatz wie die reservierte übergeordnete LUN. Falls die FlexClone LUN nicht reserviert ist, muss das Volume über genügend Speicherplatz verfügen, um Änderungen am Klon gerecht zu werden.

Schritte

1. Vergewissern Sie sich, dass die LUN nicht zugeordnet ist oder nicht in geschrieben wird.
2. Erstellen einer Snapshot Kopie des Volume, das die LUNs enthält:

```
volume snapshot create -vserver vs1 -volume vol1 -snapshot  
snapshot_name
```

Sie müssen eine Snapshot Kopie (die zugrunde liegende Snapshot Kopie) der LUN erstellen, die Sie

klonen möchten.

3. Erstellen Sie die FlexClone LUN aus der Snapshot Kopie:

```
file clone create -vserver vserver_name -volume volume_name -source-path  
source_path -snapshot-name snapshot_name -destination-path destination_path
```

Wenn die FlexClone LUN für das automatische Löschen verfügbar sein soll, schließen Sie Folgendes ein `-autodelete true`. Wenn Sie diese FlexClone LUN in einem Volume mit Semi-Thick Provisioning erstellen, müssen Sie das automatische Löschen für alle FlexClone LUNs aktivieren.

4. Vergewissern Sie sich, dass die FlexClone LUN richtig ist:

```
lun show -vserver vserver_name
```

Vserver	Path	State	Mapped	Type	Size
vs1	/vol/vol1/lun1_clone	online	unmapped	windows	47.07MB
vs1	/vol/vol1/lun1_snap_clone	online	unmapped	windows	47.07MB

Das automatische Löschen einer bestimmten FlexClone Datei oder eines FlexClone LUN wird verhindert

Wenn Sie ein FlexVol Volume zum automatischen Löschen von FlexClone Dateien und FlexClone LUNs konfigurieren, wird jeder Klon, der den angegebenen Kriterien entspricht, gelöscht. Wenn Sie bestimmte FlexClone Dateien oder FlexClone LUNs haben, die Sie erhalten möchten, können Sie diese beim automatischen Löschvorgang von FlexClone ausschließen.

Was Sie benötigen

Eine FlexClone Lizenz muss installiert sein. Diese Lizenz ist in enthalten ["ONTAP One"](#).

Über diese Aufgabe

Wenn Sie eine FlexClone Datei oder eine FlexClone LUN erstellen, ist die Autodelete-Einstellung für den Klon standardmäßig deaktiviert. FlexClone Dateien und FlexClone LUNs mit deaktiviertem Löschen bleiben erhalten, wenn Sie ein FlexVol Volume so konfigurieren, dass Klone automatisch gelöscht werden, um Speicherplatz auf dem Volume freizugeben.



Wenn Sie die einstellen `commitment` Ebene auf das Volume zu `try` Oder `disrupt`, Sie können spezifische FlexClone Dateien oder FlexClone LUNs individuell erhalten, indem Sie Autodelete für diese Klone deaktivieren. Wenn Sie jedoch die einstellen `commitment` Ebene auf das Volume zu `destroy` Und die Listen zum Löschen enthalten `lun_clone`, `file_clone`, Die Volume-Einstellung überschreibt die Kloneinstellung und alle FlexClone Dateien und FlexClone LUNs können unabhängig von der Autodelete-Einstellung für die Klone gelöscht werden.

Schritte

1. Eine bestimmte FlexClone Datei oder ein FlexClone LUN kann nicht mithilfe der automatisch gelöscht werden `volume file clone autodelete` Befehl.

Das folgende Beispiel zeigt, wie Sie Autodelete für FlexClone LUN „lun1_Clone“ in vol1 deaktivieren können:

```
cluster1::> volume file clone autodelete -vserver vs1 -volume voll  
-clone-path lun1_clone -enable false
```

Eine FlexClone Datei oder ein FlexClone LUN mit deaktiviertem Löschen kann nicht automatisch gelöscht werden, um Speicherplatz auf dem Volume freizugeben.

2. Vergewissern Sie sich, dass Autodelete für die FlexClone Datei oder für FlexClone LUN mit der deaktiviert ist `volume file clone show-autodelete` Befehl.

Das folgende Beispiel zeigt, dass Autodelete für die FlexClone LUN „lun1_Clone“ false ist:

```
cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path  
vol/voll/lun1_clone
```

	Vserver
Name:	vs1
	Clone Path:
	vol/voll/lun1_clone
	Autodelete
Enabled:	false

Konfigurieren und verwenden Sie SnapVault Backups in einer SAN-Umgebung

Konfiguration und Verwendung von SnapVault Backups in einer Übersicht über die SAN-Umgebung

Die Konfiguration und der Einsatz von SnapVault in einer SAN-Umgebung sind ähnlich der Konfiguration und dem Einsatz in einer NAS-Umgebung. Die Wiederherstellung von LUNs in einer SAN-Umgebung erfordert jedoch einige spezielle Verfahren.

SnapVault Backups enthalten einen Satz schreibgeschützter Kopien eines Quell-Volumes. In einer SAN-Umgebung sichern Sie immer ganze Volumes auf dem sekundären SnapVault Volume, nicht auf individuellen LUNs.

Das Verfahren zum Erstellen und Initialisieren der SnapVault-Beziehung zwischen einem primären Volume mit LUNs und einem sekundären Volume, das als SnapVault Backup fungiert, ist identisch mit dem Verfahren, das mit FlexVol Volumes für Dateiprotokolle verwendet wird. Dieses Verfahren wird ausführlich beschrieben ["Datensicherung"](#).

Es muss sichergestellt werden, dass die zu sichernden LUNs sich in einem konsistenten Zustand befinden, bevor die Snapshot-Kopien erstellt und auf das sekundäre SnapVault Volume kopiert werden. Durch die Automatisierung der Erstellung von Snapshot Kopien mit SnapCenter wird sichergestellt, dass die gesicherten LUNs vollständig erstellt und von der ursprünglichen Applikation verwendet werden können.

Es gibt drei grundlegende Möglichkeiten für die Wiederherstellung von LUNs aus einem sekundären SnapVault-Volume:

- Eine LUN kann direkt vom sekundären SnapVault Volume zugeordnet werden und einen Host mit der LUN verbinden, um auf die Inhalte der LUN zuzugreifen.

Die LUN ist schreibgeschützt, und Sie können nur von der letzten Snapshot-Kopie im SnapVault Backup zuordnen. Persistente Reservierungen und andere LUN-Metadaten gehen verloren. Bei Bedarf können Sie den LUN-Inhalt mit einem Kopierprogramm auf dem Host zurück auf die ursprüngliche LUN kopieren, sofern der Zugriff weiterhin möglich ist.

Die LUN verfügt über eine andere Seriennummer als die Quell-LUN.

- Sie können jede beliebige Snapshot Kopie im sekundären SnapVault Volume auf ein neues Schreib-Volume klonen.

Anschließend können Sie jede der LUNs im Volume zuordnen und einen Host mit der LUN verbinden, um auf die Inhalte der LUN zuzugreifen. Bei Bedarf können Sie den LUN-Inhalt mit einem Kopierprogramm auf dem Host zurück auf die ursprüngliche LUN kopieren, sofern der Zugriff weiterhin möglich ist.

- Sie können das gesamte Volume, das die LUN enthält, aus einer beliebigen Snapshot Kopie im sekundären SnapVault Volume wiederherstellen.

Beim Wiederherstellen des gesamten Volume werden alle LUNs und alle Dateien im Volume ersetzt. Alle neuen LUNs, die seit dem Erstellen der Snapshot Kopie erstellt wurden, gehen verloren.

Die LUNs behalten ihre Zuordnung, Seriennummern, UUIDs und ihre persistenten Reservierungen bei.

Zugriff auf eine schreibgeschützte LUN-Kopie aus einem SnapVault Backup

Sie können von der neuesten Snapshot-Kopie in einem SnapVault-Backup auf eine schreibgeschützte Kopie einer LUN zugreifen. Die LUN-ID, der Pfad und die Seriennummer unterscheiden sich von der Quell-LUN und müssen zuerst zugeordnet werden. Persistente Reservierungen, LUN-Zuordnungen und Initiatorgruppen werden nicht auf das sekundäre SnapVault Volume repliziert.

Was Sie benötigen

- Die SnapVault-Beziehung muss initialisiert werden und die neueste Snapshot Kopie im sekundären SnapVault Volume muss die gewünschte LUN enthalten.
- Die Storage Virtual Machine (SVM), die das SnapVault Backup enthält, muss über einen oder mehrere LIFs verfügen, wobei das gewünschte SAN-Protokoll über den Host zugänglich ist, der für den Zugriff auf die LUN-Kopie verwendet wird.
- Wenn Sie einen direkten Zugriff auf LUN-Kopien vom sekundären SnapVault Volume planen, müssen Sie vorab Ihre Initiatorgruppen auf der SnapVault SVM erstellen.

Sie können direkt vom sekundären SnapVault Volume auf eine LUN zugreifen, ohne dass zuerst das Volume mit der LUN wiederhergestellt oder geklont werden muss.

Über diese Aufgabe

Wenn eine neue Snapshot Kopie dem sekundären SnapVault Volume hinzugefügt wird, während eine LUN aus einer vorherigen Snapshot Kopie zugeordnet ist, ändert sich der Inhalt der zugeordneten LUN. Die LUN ist weiterhin mit denselben IDs zugeordnet, die Daten werden jedoch aus der neuen Snapshot Kopie entnommen. Wenn sich die LUN-Größe ändert, erkennen einige Hosts automatisch die Größenänderung. Windows Hosts müssen nach einem Festplatten-Rescan suchen, um eventuelle Größenänderungen einzuholen.

Schritte

1. Führen Sie die aus `lun show` Befehl, um die verfügbaren LUNs im sekundären SnapVault Volume aufzulisten.

In diesem Beispiel sehen Sie sowohl die ursprünglichen LUNs im primären Volume `srcvolA` als auch die Kopien im sekundären SnapVault Volume `dstvolB`:

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
-----	-----	-----	-----	-----	-----
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

2. Wenn auf der SVM, die das sekundäre SnapVault Volume enthält, die Initiatorgruppe für den gewünschten Host nicht bereits vorhanden ist, führen Sie die aus `igroup create` Befehl zum Erstellen einer Initiatorgruppe

Mit diesem Befehl wird eine Initiatorgruppe für einen Windows Host erstellt, der das iSCSI-Protokoll verwendet:

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
               -protocol iscsi -ostype windows
               -initiator iqn.1991-05.com.microsoft:hostA
```

3. Führen Sie die aus `lun mapping create` Befehl zum Zuordnen der gewünschten LUN-Kopie zur Initiatorgruppe.

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
               -igroup temp_igroup
```

4. Verbinden Sie den Host mit der LUN, und greifen Sie nach Bedarf auf die Inhalte der LUN zu.

Stellen Sie eine einzelne LUN aus einem SnapVault-Backup wieder her

Sie können eine einzelne LUN an einem neuen Speicherort oder am ursprünglichen Speicherort wiederherstellen. Sie können Restores von jeder beliebigen Snapshot Kopie im sekundären SnapVault Volume durchführen. Um die LUN am ursprünglichen Speicherort wiederherzustellen, stellen Sie sie zuerst an einem neuen Speicherort wieder

her und kopieren sie dann.

Was Sie benötigen

- Die SnapVault-Beziehung muss initialisiert werden und das sekundäre SnapVault Volume muss eine entsprechende Snapshot Kopie enthalten, um sie wiederherzustellen.
- Die Storage Virtual Machine (SVM), die das sekundäre SnapVault Volume enthält, muss über eine oder mehrere LIFs mit dem gewünschten SAN-Protokoll verfügen, auf die der Host zum Zugriff auf die LUN-Kopie zugreifen kann.
- Die Initiatorgruppen müssen auf der SnapVault SVM bereits vorhanden sein.

Über diese Aufgabe

Dieser Prozess umfasst die Erstellung eines Volume-Klons mit Lese- und Schreibvorgängen aus einer Snapshot Kopie im sekundären SnapVault Volume. Sie können die LUN direkt aus dem Klon verwenden oder den LUN-Inhalt optional wieder an den ursprünglichen Speicherort der LUN kopieren.

Die LUN im Klon verfügt über einen anderen Pfad und eine andere Seriennummer als die ursprüngliche LUN. Persistente Reservierungen werden nicht beibehalten.

Schritte

1. Führen Sie die aus `snapmirror show` Befehl zur Überprüfung des sekundären Volumes, das das SnapVault Backup enthält.

```
cluster::> snapmirror show
```

Source Path	Dest Type	Mirror Path	Relation State	Total Progress	Healthy	Last Updated
vserverA:srcvolA	XDP	vserverB:dstvolB	Snapmirrored Idle	-	true	-

2. Führen Sie die aus `volume snapshot show` Befehl zum Identifizieren der Snapshot Kopie, aus der Sie die LUN wiederherstellen möchten.

```
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. Führen Sie die aus `volume clone create` Befehl, um einen Klon mit Lese- und Schreibvorgängen aus

der gewünschten Snapshot Kopie zu erstellen.

Der Volume-Klon wird im selben Aggregat erstellt wie der SnapVault Backup. Im Aggregat muss genügend Speicherplatz vorhanden sein, um den Klon zu speichern.

```
cluster::> volume clone create -vserver vserverB
      -flexclone dstvolB_clone -type RW -parent-volume dstvolB
      -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. Führen Sie die aus `lun show` Befehl zum Auflisten der LUNs im Klon des Volumes

```
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.

5. Wenn die Initiatorgruppe für den gewünschten Host auf der SVM, die das SnapVault-Backup enthält, nicht bereits vorhanden ist, führen Sie die aus `igroup create` Befehl zum Erstellen einer Initiatorgruppe

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. Führen Sie die aus `lun mapping create` Befehl zum Zuordnen der gewünschten LUN-Kopie zur Initiatorgruppe.

```
cluster::> lun mapping create -vserver vserverB
      -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

7. Verbinden Sie den Host mit der LUN und greifen Sie nach Bedarf auf den Inhalt der LUN zu.

Die LUN ist Lese- und Schreib-LUN, die anstelle der ursprünglichen LUN verwendet werden kann. Da die LUN-Seriennummer sich unterscheidet, interpretiert der Host sie als eine andere LUN als das Original.

8. Verwenden Sie ein Kopierprogramm auf dem Host, um den LUN-Inhalt zurück auf die ursprüngliche LUN zu kopieren.

Wiederherstellen aller LUNs in einem Volume aus einem SnapVault-Backup

Wenn eine oder mehrere LUNs in einem Volume aus einem SnapVault Backup wiederhergestellt werden müssen, können Sie das gesamte Volume wiederherstellen. Die Wiederherstellung des Volumes wirkt sich auf alle LUNs im Volume aus.

Was Sie benötigen

Die SnapVault-Beziehung muss initialisiert werden und das sekundäre SnapVault Volume muss eine entsprechende Snapshot Kopie enthalten, um sie wiederherzustellen.

Über diese Aufgabe

Wenn ein gesamtes Volume wiederhergestellt wird, kehrt es in den Zustand zurück, in dem es sich zum Zeitpunkt der Erstellung der Snapshot Kopie befand. Falls nach der Snapshot Kopie dem Volume eine LUN hinzugefügt wurde, wird diese LUN während des Wiederherstellungsprozesses entfernt.

Nach dem Wiederherstellen des Volumes bleiben die LUNs den Initiatorgruppen zugeordnet, denen sie kurz vor der Wiederherstellung zugeordnet wurden. Die LUN-Zuordnung kann sich zum Zeitpunkt der Snapshot Kopie von der Zuordnung unterscheiden. Persistente Reservierungen auf den LUNs von Host-Clustern bleiben erhalten.

Schritte

1. Stoppen Sie den I/O für alle LUNs im Volume.
2. Führen Sie die aus `snapmirror show` Befehl zur Überprüfung des sekundären Volumes, das das sekundäre SnapVault Volume enthält

```
cluster::> snapmirror show
```

Source Path	Type	Dest Path	Mirror State	Relation Status	Total Progress	Healthy	Last Updated
vserverA:srcvolA							
	XDP	vserverB:dstvolB					
			Snapmirrored				
				Idle	-	true	-

3. Führen Sie die aus `volume snapshot show` Befehl zum Identifizieren der Snapshot Kopie, aus der Sie wiederherstellen möchten.


```
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. Führen Sie die aus `snapmirror restore` Befehl und geben Sie den an `-source-snapshot` Option zum Angeben der zu verwendenden Snapshot Kopie.

Das Ziel, das Sie für die Wiederherstellung angeben, ist das ursprüngliche Volume, auf dem Sie wiederherstellen.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA  
-source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010
```

```
Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on  
volume vserverA:src_volA will be deleted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 98] Job is queued: snapmirror restore from source  
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. Wenn Sie LUNs über ein Host-Cluster hinweg gemeinsam nutzen, stellen Sie die persistenten Reservierungen auf den LUNs von den betroffenen Hosts wieder her.

Wiederherstellen eines Volumes aus einem SnapVault-Backup

Im folgenden Beispiel wurde die LUN mit dem Namen „lun_D“ dem Volume hinzugefügt, nachdem die Snapshot Kopie erstellt wurde. Nach dem Wiederherstellen des gesamten Volumes aus der Snapshot Kopie wird lun_D nicht mehr angezeigt.

Im `lun show` Die Ausgabe des Befehls, Sie sehen die LUNs im primären Volume srcvolA und die schreibgeschützten Kopien dieser LUNs im sekundären SnapVault Volume dstvolB. Es gibt keine Kopie von lun_D im SnapVault Backup.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_D	online	mapped	windows	250.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

7 entries were displayed.

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
-source-path vserverB:dstvolB
-source-snapshot daily.2013-02-10_0010
```

Warning: All data newer than Snapshot 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.

```
cluster::> lun show
```

Vserver	Path	State	Mapped	Type	Size
vserverA	/vol/srcvolA/lun_A	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_B	online	mapped	windows	300.0GB
vserverA	/vol/srcvolA/lun_C	online	mapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_A	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_B	online	unmapped	windows	300.0GB
vserverB	/vol/dstvolB/lun_C	online	unmapped	windows	300.0GB

6 entries were displayed.

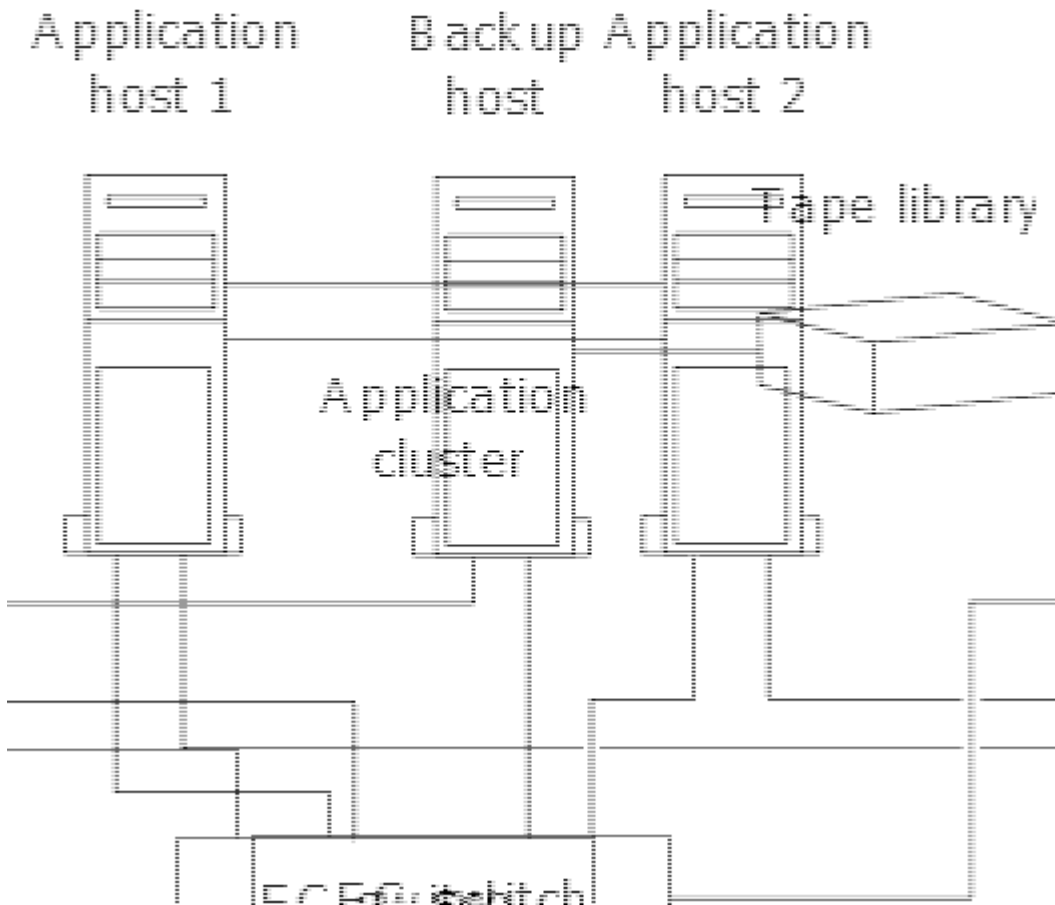
Nachdem das Volume aus dem sekundären SnapVault Volume wiederhergestellt wurde, enthält das Quell-Volume nicht mehr lun_D. Sie müssen die LUNs im Quell-Volume nach der Wiederherstellung nicht neu zuordnen, da sie noch zugeordnet sind.

Wie Sie ein Host Backup-System mit dem primären Storage-System verbinden können

Sie können SAN-Systeme über einen separaten Backup-Host auf Tape sichern, um Performance-Einbußen beim Applikations-Host zu vermeiden.

Es muss zwingend notwendig sein, dass SAN- und NAS-Daten für Backup-Zwecke getrennt gehalten werden.

Die Abbildung unten zeigt die empfohlene physische Konfiguration für ein Host-Backup-System auf dem primären Speichersystem. Sie müssen Volumes nur als SAN konfigurieren. LUNs sind auf ein einzelnes Volume beschränkt oder die LUNs können über mehrere Volumes oder Storage-Systeme verteilt werden.



Volumes auf einem Host können aus einer einzelnen LUN bestehen, die vom Storage-System zugeordnet ist, oder aus mehreren LUNs mit einem Volume Manager, wie VxVM auf HP-UX Systemen.

Sichern Sie eine LUN über ein Host-Backup-System

Sie können eine geklonte LUN aus einer Snapshot Kopie als Quelldaten für das Host Backup System verwenden.

Was Sie benötigen

Eine Produktions-LUN muss vorhanden sein und einer Initiatorgruppe zugeordnet sein, die den WWPN oder den Initiator-Node-Namen des Applikationsservers enthält. Außerdem muss die LUN formatiert sein und auf den Host zugreifen können

Schritte

1. Speichern Sie den Inhalt der Puffer des Host-Filesystems auf der Festplatte.

Sie können den von Ihrem Host-Betriebssystem bereitgestellten Befehl verwenden oder SnapDrive für Windows oder SnapDrive für UNIX verwenden. Sie können auch entscheiden, diesen Schritt in Ihr SAN-Backup-Vorverarbeitungsskript einzutragen.

2. Verwenden Sie die `volume snapshot create` Befehl zum Erstellen einer Snapshot Kopie der Produktions-LUN.

```
volume snapshot create -vserver vs0 -volume vol3 -snapshot vol3_snapshot  
-comment "Single snapshot" -foreground false
```

3. Verwenden Sie die `volume file clone create` Befehl zum Erstellen eines Klons der Produktions-LUN.

```
volume file clone create -vserver vs3 -volume vol3 -source-path lun1 -snapshot  
-name snap_vol3 -destination-path lun1_backup
```

4. Verwenden Sie die `lun igroup create` Befehl zum Erstellen einer Initiatorgruppe, die den WWPN des Backup-Servers enthält.

```
lun igroup create -vserver vs3 -igroup igroup3 -protocol fc -ostype windows  
-initiator 10:00:00:00:c9:73:5b:91
```

5. Verwenden Sie die `lun mapping create` Befehl zum Zuordnen des in Schritt 3 erstellten LUN-Klons zum Backup-Host.

```
lun mapping create -vserver vs3 -volume vol3 -lun lun1_backup -igroup igroup3
```

Sie können diesen Schritt in das Post-Processing-Skript Ihrer SAN-Backup-Applikation einarbeiten.

6. Erkennen Sie vom Host die neue LUN und stellen Sie das Dateisystem dem Host zur Verfügung.

Sie können diesen Schritt in das Post-Processing-Skript Ihrer SAN-Backup-Applikation einarbeiten.

7. Sichern Sie die Daten im LUN-Klon vom Backup-Host zum Tape mithilfe Ihrer SAN-Backup-Applikation.

8. Verwenden Sie die `lun modify` Befehl, um den LUN-Klon in den Offline-Modus zu versetzen.

```
lun modify -vserver vs3 -path /vol/vol3/lun1_backup -state offline
```

9. Verwenden Sie die `lun delete` Um den LUN-Klon zu entfernen.

```
lun delete -vserver vs3 -volume vol3 -lun lun1_backup
```

10. Verwenden Sie die `volume snapshot delete` Befehl zum Entfernen der Snapshot Kopie.

```
volume snapshot delete -vserver vs3 -volume vol3 -snapshot vol3_snapshot
```

Referenz zur SAN-Konfiguration

Übersicht über die SAN-Konfiguration

Ein Storage Area Network (SAN) besteht aus einer Storage-Lösung, die über ein SAN-Transportprotokoll wie iSCSI oder FC mit Hosts verbunden ist. Sie können Ihr SAN so konfigurieren, dass Ihre Speicherlösung über einen oder mehrere Switches mit Ihren Hosts verbunden wird. Wenn Sie iSCSI verwenden, können Sie Ihr SAN auch so konfigurieren, dass Ihre Speicherlösung ohne einen Switch direkt an Ihren Host angeschlossen wird.

In einem SAN können mehrere Hosts mit verschiedenen Betriebssystemen, wie Windows, Linux oder UNIX, gleichzeitig auf die Storage-Lösung zugreifen. Verwenden Sie können ["Selektive LUN-Zuordnung"](#) Und ["Portsätze"](#) Um den Datenzugriff zwischen den Hosts und dem Speicher zu beschränken.

Bei iSCSI wird die Netzwerktopologie zwischen der Speicherlösung und den Hosts als Netzwerk bezeichnet. Bei FC, FC/NVMe und FCoE wird die Netzwerktopologie zwischen der Storage-Lösung und den Hosts als Fabric bezeichnet. Um Redundanz zu schaffen, die Sie vor dem Verlust des Datenzugriffs schützt, sollten Sie Ihr SAN mit HA-Paaren in einer Multi-Netzwerk- oder Multi-Fabric-Konfiguration einrichten. Konfigurationen mit einzelnen Knoten oder einzelnen Netzwerken/Fabrics sind nicht vollständig redundant und daher nicht empfohlen.

Nach der Konfiguration des SAN können Sie dies tun ["Bereitstellen von Storage für iSCSI oder FC"](#), Oder Sie können ["Storage für FC/NVMe bereitstellen"](#). Anschließend können Sie eine Verbindung zu Ihren Hosts herstellen, um mit der Datenpflege zu beginnen.

Die Unterstützung der SAN-Protokolle variiert abhängig von Ihrer Version von ONTAP, Ihrer Plattform und Ihrer Konfiguration. Weitere Informationen zu Ihrer spezifischen Konfiguration finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

Verwandte Informationen

- ["ÜBERSICHT ÜBER DIE SAN-Administration"](#)
- ["Konfiguration, Support und Einschränkungen von NVMe"](#)

ISCSI-Konfigurationen

Möglichkeiten zur Konfiguration von iSCSI-SAN-Hosts

Sie sollten Ihre iSCSI-Konfiguration mit Hochverfügbarkeitspaaren (HA) einrichten, die direkt mit Ihren iSCSI-SAN-Hosts verbunden sind oder die über einen oder mehrere IP-Switches eine Verbindung zu Ihren Hosts herstellen.

["HA-Paare"](#) Sind definiert als die Reporting-Nodes für die aktiv/optimiert und die aktiv/nicht optimierten Pfade, die von den Hosts für den Zugriff auf die LUNs verwendet werden. Mehrere Hosts, die verschiedene Betriebssysteme verwenden, wie z. B. Windows, Linux oder UNIX, können gleichzeitig auf den Storage zugreifen. Hosts erfordern die Installation und Konfiguration einer unterstützten Multipathing-Lösung, die ALUA unterstützt. Unterstützte Betriebssysteme und Multipathing-Lösungen können auf dem verifiziert werden ["NetApp Interoperabilitäts-Matrix-Tool"](#).

In einer Konfiguration mit mehreren Netzwerken gibt es zwei oder mehr Switches, die die Hosts mit dem Speichersystem verbinden. Mehrere Netzwerkkonfigurationen werden empfohlen, da sie vollständig redundant sind. In einer Konfiguration mit einem einzigen Netzwerk gibt es einen Switch, der die Hosts mit dem Speichersystem verbindet. Einzelnetzwerkkonfigurationen sind nicht vollständig redundant.



["Single-Node-Konfigurationen"](#) Die Empfehlungen sind nicht empfehlenswert, da sie nicht die Redundanz bieten, die zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb erforderlich ist.

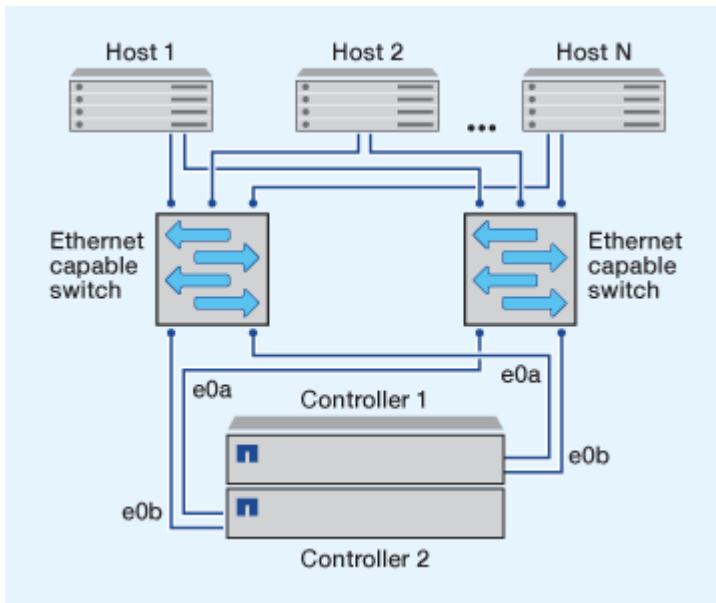
Verwandte Informationen

- Erfahren Sie, wie ["Selektive LUN-Zuordnung \(SLM\)"](#) Beschränkt die Pfade, die für den Zugriff auf die LUNs verwendet werden, die sich im Besitz eines HA-Paars befinden.
- Erfahren Sie mehr über ["SAN LIFs"](#).

- Erfahren Sie mehr über die ["Vorteile von VLANs in iSCSI"](#).

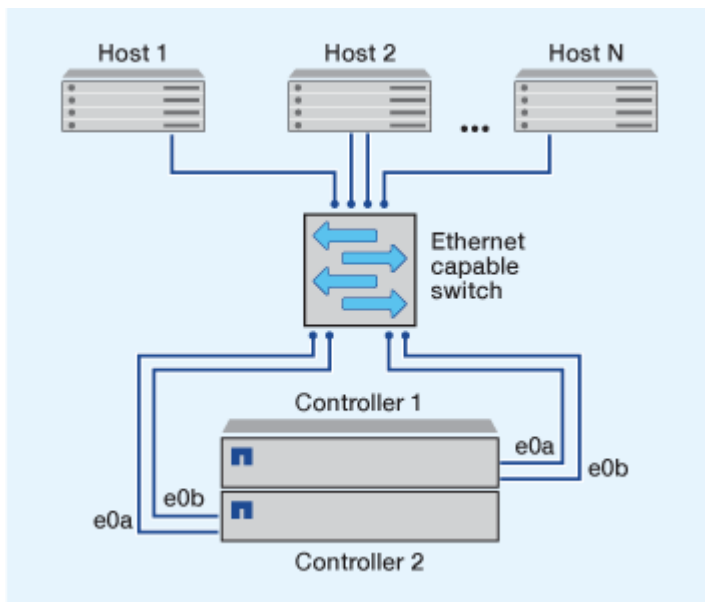
ISCSI-Konfigurationen mit mehreren Netzwerken

Bei HA-Paar-Konfigurationen mit mehreren Netzwerken verbinden zwei oder mehr Switches das HA-Paar mit einem oder mehreren Hosts. Da es mehrere Switches gibt, ist diese Konfiguration vollständig redundant.



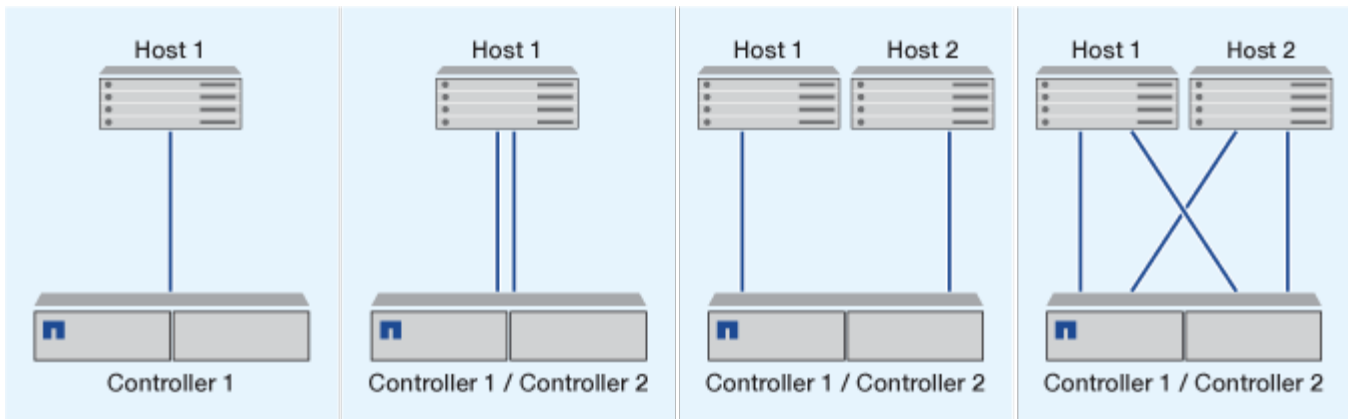
ISCSI-Konfigurationen mit einem Netzwerk

Bei Einzel-Netzwerk-HA-Paar-Konfigurationen verbindet ein Switch das HA-Paar mit einem oder mehreren Hosts. Da es einen einzelnen Switch gibt, ist diese Konfiguration nicht vollständig redundant.



Konfiguration von Direct-Attachment-iSCSI

In einer Direct-Attached-Konfiguration sind ein oder mehrere Hosts direkt mit den Controllern verbunden.



Vorteile durch die Nutzung von VLANs in iSCSI-Konfigurationen

Ein VLAN besteht aus einer Gruppe von Switch-Ports, die zu einer Broadcast-Domäne gruppiert sind. Ein VLAN kann sich auf einem einzelnen Switch befinden oder sich über mehrere Switch-Chassis erstrecken. Statische und dynamische VLANs ermöglichen die Erhöhung der Sicherheit, die Isolierung von Problemen und die Begrenzung verfügbarer Pfade innerhalb der IP-Netzwerkinfrastruktur.

Bei der Implementierung von VLANs in großen IP-Netzwerkinfrastrukturen ergeben sich folgende Vorteile:

- Erhöhte Sicherheit:

Mit VLANs können Sie die vorhandene Infrastruktur nutzen und zugleich größere Sicherheit bieten, da sie den Zugriff auf verschiedene Nodes eines Ethernet-Netzwerks oder IP SAN beschränken.

- Verbesserte Zuverlässigkeit des Ethernet-Netzwerks und des IP SAN durch Isolierung von Problemen
- Verringerung der Problemlösungszeit durch Beschränkung des problematischen Speicherplatzes
- Reduzierung der Anzahl der verfügbaren Pfade zu einem bestimmten iSCSI-Zielport.
- Reduzierung der maximalen Anzahl von Pfaden, die von einem Host verwendet werden

Dass zu viele Pfade die Verbindungszeiten verlangsamen. Wenn ein Host nicht über eine Multipathing-Lösung verfügt, können Sie VLANs verwenden, um nur einen Pfad zuzulassen.

Dynamische VLANs

Dynamische VLANs basieren auf MAC-Adressen. Sie können ein VLAN definieren, indem Sie die MAC-Adresse der Mitglieder angeben, die Sie aufnehmen möchten.

Dynamische VLANs bieten Flexibilität und sind nicht auf die physischen Ports angewiesen, an denen das Gerät physisch mit dem Switch verbunden ist. Sie können ein Kabel von einem Port in den anderen umstecken, ohne das VLAN neu zu konfigurieren.

Statische VLANs

Statische VLANs sind portbasiert. Der Switch und der Switch Port werden verwendet, um das VLAN und seine Mitglieder zu definieren.

Statische VLANs bieten verbesserte Sicherheit, da es nicht möglich ist, VLANs durch MAC-Spoofing (Media Access Control) zu durchbrechen. Wenn jedoch jemand physischen Zugang zum Switch hat, kann der Zugriff

durch den Austausch eines Kabels und die Neukonfiguration der Netzwerkadresse möglich sein.

In manchen Umgebungen ist es einfacher, statische VLANs zu erstellen und zu managen als dynamische VLANs. Dies liegt daran, dass bei statischen VLANs nur die Switch- und Port-ID angegeben werden muss, anstatt die 48-Bit-MAC-Adresse. Darüber hinaus können Sie Switch-Portbereiche mit der VLAN-Kennung kennzeichnen.

FC-Konfigurationen

Möglichkeiten zur Konfiguration von FC- und FC-NVMe-SAN-Hosts

Es wird empfohlen, Ihre FC- und FC-NVMe-SAN-Hosts über HA-Paare und mindestens zwei Switches zu konfigurieren. Sie bietet Redundanz auf Fabric- und Storage-Systemebene zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb. Sie können FC- oder FC-NVMe-SAN-Hosts nicht ohne Switch direkt an HA-Paare anschließen.

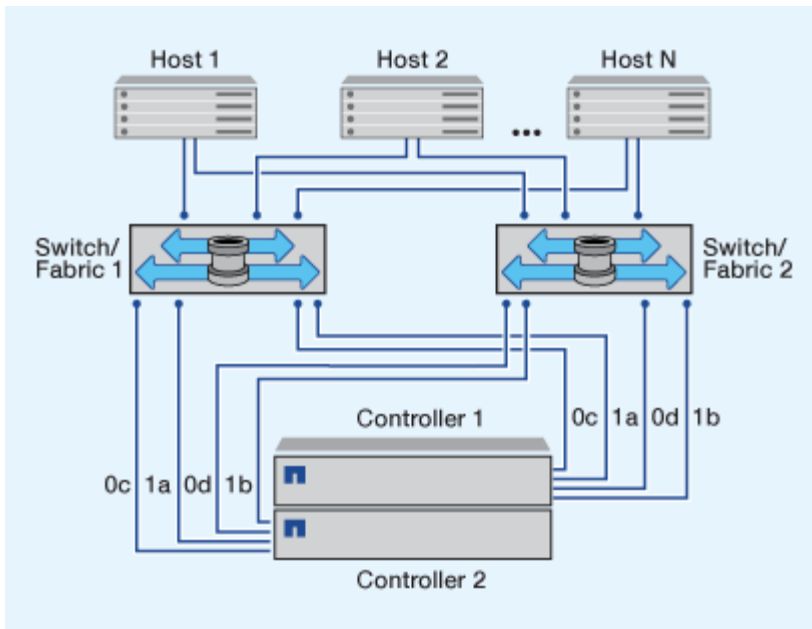
Kaskadierung, partielles Mesh, volles Mesh, Core-Edge und Director Fabrics sind branchenübliche Methoden, FC Switches mit einem Fabric zu verbinden. Alle werden unterstützt. Die Verwendung heterogener FC Switch Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches. Spezielle Ausnahmen sind in aufgeführt ["Interoperabilitäts-Matrix-Tool"](#). Eine Fabric kann aus einem oder mehreren Switches bestehen und die Storage-Controller mit mehreren Switches verbunden werden.

Mehrere Hosts, die verschiedene Betriebssysteme verwenden, z. B. Windows, Linux oder UNIX, können gleichzeitig auf die Storage Controller zugreifen. Hosts erfordern, dass eine unterstützte Multipathing-Lösung installiert und konfiguriert ist. Unterstützte Betriebssysteme und Multipathing-Lösungen können im Interoperabilitäts-Matrix-Tool verifiziert werden.

Multi-Fabric-FC- und FC-NVMe-Konfigurationen

In Multi-Fabric HA-Paar-Konfigurationen gibt es mindestens zwei Switches, die HA-Paare mit einem oder mehreren Hosts verbinden. Der Einfachheit halber werden im folgenden HA-Paar mit mehreren Fabrics nur zwei gezeigt, doch in jeder Multi-Fabric-Konfiguration können mindestens zwei Fabrics vorhanden sein.

Die FC-Ziel-Port-Nummern (0c, 0d, 1a, 1b) in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern variieren je nach Modell des Storage-Node und ob Sie Erweiterungsadapter verwenden.

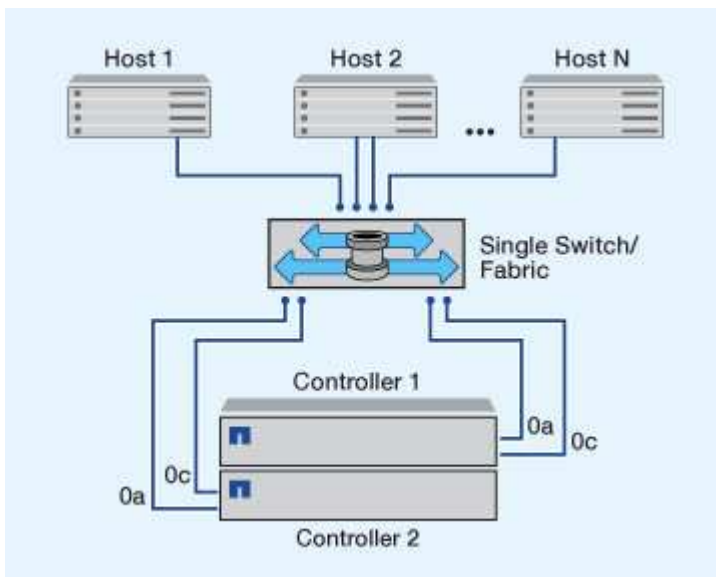


FC- und FC-NVMe-Konfigurationen in einem Fabric

Bei Einzel-Fabric-HA-Paar-Konfigurationen besteht ein Fabric, das beide Controller im HA-Paar mit einem oder mehreren Hosts verbindet. Da die Hosts und Controller über einen einzelnen Switch verbunden sind, sind HA-Paar-Konfigurationen in einem Fabric nicht vollständig redundant.

Die FC-Ziel-Port-Nummern (0a, 0c) in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern variieren je nach Modell des Storage-Node und ob Sie Erweiterungsadapter verwenden.

Alle Plattformen, die FC-Konfigurationen unterstützen, unterstützen HA-Paar-Konfigurationen in einem Single-Fabric-Ansatz.



"Single-Node-Konfigurationen" Die Empfehlungen sind nicht empfehlenswert, da sie nicht die Redundanz bieten, die zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb erforderlich ist.

Verwandte Informationen

- Erfahren Sie, wie ["Selektive LUN-Zuordnung \(SLM\)"](#) Beschränkt die Pfade, die für den Zugriff auf die LUNs verwendet werden, die sich im Besitz eines HA-Paars befinden.
- Erfahren Sie mehr über ["SAN LIFs"](#).

Best Practices der FC-Switch-Konfiguration

Um eine optimale Performance zu erzielen, sollten Sie beim Konfigurieren Ihres FC Switch bestimmte Best Practices berücksichtigen.

Ein Festlegen der Link-Geschwindigkeit ist die Best Practice für FC Switch-Konfigurationen. Dies gilt insbesondere für große Fabrics, da es die beste Performance bei Fabric-Rebuilds bietet und dadurch Zeit sparen kann. Obwohl die Autonegotiation die größte Flexibilität bietet, funktioniert die FC-Switch-Konfiguration nicht immer wie erwartet, und sie erhöht die Zeit für die gesamte Fabric-Build-Sequenz.

Alle Switches, die mit dem Fabric verbunden sind, müssen N_Port ID Virtualization (NPIV) unterstützen und NPIV aktivieren. ONTAP verwendet NPIV, um FC-Ziele einer Fabric anzubieten.

Weitere Informationen darüber, welche Umgebungen unterstützt werden, finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#).

Best Practices für FC und iSCSI finden Sie unter ["Technischer Bericht 4080 zu NetApp: Best Practices für modernes SAN"](#).

Unterstützte Anzahl an FC-Hops

Die maximal unterstützte Anzahl an FC-Hops (Hop Count) zwischen einem Host und einem Storage-System hängt vom Switch-Anbieter und der Unterstützung des Storage-Systems für FC-Konfigurationen ab.

Hop Count ist definiert als die Anzahl der Switches im Pfad zwischen dem Initiator (Host) und dem Ziel (Storage-System). Cisco bezeichnet diesen Wert auch als „*Durchmesser des SAN Fabric*“.

Lieferant wechseln	Unterstützte Hop Count
Brocade	7 für FC, 5 für FCoE
Cisco	7 für FC können bis zu 3 der Switches FCoE-Switches sein.

Verwandte Informationen

["NetApp Downloads: Brocade Scalability Matrix Documents"](#)

["NetApp Downloads: Cisco Scalability Matrix Documents"](#)

Unterstützte Geschwindigkeiten für FC-Zielport

FC-Ziel-Ports können für die Ausführung mit unterschiedlichen Geschwindigkeiten konfiguriert werden. Sie sollten die Geschwindigkeit des Zielports so einstellen, dass sie mit der Geschwindigkeit des Geräts übereinstimmt, mit dem das Gerät verbunden wird. Alle von einem bestimmten Host verwendeten Ziel-Ports sollten auf dieselbe

Geschwindigkeit eingestellt sein.

FC-Ziel-Ports können für FC-NVMe-Konfigurationen genau auf die gleiche Weise verwendet werden wie für FC-Konfigurationen.

Sie sollten die Geschwindigkeit des Zielports so einstellen, dass sie mit der Geschwindigkeit des Geräts übereinstimmt, zu dem eine Verbindung hergestellt wird, anstatt die Autonegotiation zu verwenden. Ein Port, der auf die Autonegotiation festgelegt ist, kann nach einer Übernahme/Rückgabe oder einer anderen Unterbrechung länger dauern, bis die Verbindung wiederhergestellt ist.

Die integrierten Ports und Erweiterungsadapter können mit folgenden Geschwindigkeiten konfiguriert werden: Jeder Controller und jeder Erweiterungs-Adapter-Port kann je nach Bedarf individuell für unterschiedliche Geschwindigkeiten konfiguriert werden.

4-GB-Ports	8-GB-Ports	16-GB-Ports	32-GB-Ports
<ul style="list-style-type: none">• 4 Gb• 2 Gb• 1 Gb	<ul style="list-style-type: none">• 8 Gb• 4 Gb• 2 Gb	<ul style="list-style-type: none">• 16 Gb• 8 Gb• 4 Gb	<ul style="list-style-type: none">• 32 Gb• 16 Gb• 8 Gb



UTA2-Ports können bei Bedarf einen 8-GB-SFP+-Adapter verwenden, um Geschwindigkeiten von 8, 4 und 2 GB zu unterstützen.

Empfehlungen für die Konfiguration des FC-Zielports

Um eine optimale Performance und höchste Verfügbarkeit zu erzielen, sollten Sie die empfohlene FC-Ziel-Port-Konfiguration verwenden.

In der folgenden Tabelle wird die bevorzugte Portnutzungsreihenfolge für integrierte FC- und FC-NVMe-Zielports angezeigt. Für Erweiterungsadapter sollten die FC-Ports verteilt werden, damit sie nicht denselben ASIC für die Konnektivität verwenden. Die bevorzugte Steckplatzreihenfolge wird in aufgeführt ["NetApp Hardware Universe"](#) Für die von Ihrem Controller verwendete Version der ONTAP-Software.

FC-NVMe wird auf folgenden Modellen unterstützt:

- AFF A300



Die integrierten Ports der AFF A300 unterstützen keine FC-NVMe.

- AFF A700
- AFF A700s
- AFF A800



Die FAS2520 Systeme verfügen über keine integrierten FC Ports und unterstützen keine Add-on-Adapter.

Controller	Port-Paare mit gemeinsam genutztem ASIC	Anzahl der Zielports: Bevorzugte Ports
FAS9000, AFF A700, AFF A700S UND AFF A800	Keine	Alle Daten-Ports sind auf Erweiterungsadaptern gespeichert. Siehe " NetApp Hardware Universe " Finden Sie weitere Informationen.
8080, 8060 und 8040	0e+0f 0g+0h	1: 0e 2: 0e, 0g 3: 0e, 0g, 0h 4: 0e, 0g, 0f, 0h
FAS8200 UND AFF A300	0g+0h	1: 0g 2: 0g, 0h
8020	0c+0d	1: 0 c 2: 0c, 0d
62xx	0a+0b 0c+0d	1: 0 a 2: 0a, 0c 3: 0a, 0c, 0b 4: 0a, 0c, 0b, 0d
32xx	0c+0d	1: 0 c 2: 0c, 0d
FAS2554, FAS2552, FAS2600 SERIES, FAS2720, FAS2750, AFF A200 UND AFF A220	0c+0d 0e+0f	1: 0 c 2: 0c, 0e 3: 0c, 0e, 0d 4: 0c, 0e, 0d, 0f

Verwalten Sie Systeme mit FC-Adaptern

Überblick über das Verwalten von Systemen mit FC-Adaptern

Zur Verwaltung von integrierten FC-Adaptern und FC-Adapterkarten sind Befehle verfügbar. Mit diesen Befehlen können der Adaptermodus konfiguriert, Adapterinformationen angezeigt und die Geschwindigkeit geändert werden.

Die meisten Storage-Systeme verfügen über integrierte FC-Adapter, die als Initiatoren oder Ziele konfiguriert werden können. Sie können auch FC-Adapterkarten verwenden, die als Initiatoren oder Ziele konfiguriert sind. Initiatoren verbinden sich mit Back-End-Festplatten-Shelfs und möglicherweise mit anderen Storage-Arrays (FlexArray). Ziele werden nur mit FC Switches verbunden. Sowohl die FC-Ziel-HBA-Ports als auch die Switch-Port-Geschwindigkeit sollten auf den gleichen Wert gesetzt werden und sollten nicht auf die automatische Einstellung eingestellt werden.

Befehle zum Verwalten von FC-Adapttern

Sie können FC-Befehle verwenden, um FC Target-Adapter, FC Initiator-Adapter und integrierte FC-Adapter für Ihren Storage Controller zu verwalten. Mit den gleichen Befehlen werden FC-Adapter für das FC-Protokoll und das FC-NVMe-Protokoll verwaltet.

Befehle für FC Initiator-Adapter funktionieren nur auf Node-Ebene. Sie müssen den verwenden `run -node node_name` Befehl bevor Sie die Befehle des FC-Initiator-Adapters verwenden können.

Befehle zum Verwalten von FC-Zieladapttern

Ihr Ziel ist	Befehl
Zeigt FC-Adapterinformationen auf einem Node an	<code>network fcp adapter show</code>
Ändern Sie die FC-Zieladapterparameter	<code>network fcp adapter modify</code>
Zeigt Informationen zum FC-Protokoll-Datenverkehr an	<code>run -node node_name sysstat -f</code>
Anzeigen der Dauer des FC-Protokolls	<code>run -node node_name uptime</code>
Adapterkonfiguration und -Status anzeigen	<code>run -node node_name sysconfig -v adapter</code>
Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen	<code>run -node node_name sysconfig -ac</code>
Zeigen Sie eine man-Page für einen Befehl an	<code>man command_name</code>

Befehle zum Verwalten von FC-Initiator-Adapttern

Ihr Ziel ist	Befehl
Zeigt Informationen zu allen Initiatoren und ihren Adaptern in einem Node an	<code>run -node node_name storage show adapter</code>
Adapterkonfiguration und -Status anzeigen	<code>run -node node_name sysconfig -v adapter</code>

Ihr Ziel ist	Befehl
Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen	<code>run -node <i>node_name</i> sysconfig -ac</code>

Befehle zum Verwalten der integrierten FC-Adapter

Ihr Ziel ist	Befehl
Zeigt den Status der integrierten FC-Ports an	<code>system node hardware unified-connect show</code>

Konfigurieren Sie FC-Adapter für den Initiator-Modus

Sie können individuelle FC-Ports der integrierten Adapter und bestimmte FC-Adapterkarten für den Initiator-Modus konfigurieren. Der Initiator-Modus wird verwendet, um die Ports mit Bandlaufwerken, Tape Libraries oder Storage von Drittanbietern mit FlexArray Virtualisierung oder dem Import fremder LUNs (Foreign LUN Import, FLI) zu verbinden.

Was Sie benötigen

- LIFs auf dem Adapter müssen von allen Port-Sets, deren Mitglieder sie sind, entfernt werden.
- Alle LIFs von jeder Storage Virtual Machine (SVM), die den zu ändernden physischen Port verwendet, müssen migriert oder zerstört werden, bevor sie die Persönlichkeit des physischen Ports von Ziel zu Initiator ändern.

Über diese Aufgabe

Jeder integrierte FC-Port kann individuell als Initiator oder Ziel konfiguriert werden. Die Ports auf bestimmten FC-Adaptoren können auch einzeln als Ziel-Port oder als Initiator-Port konfiguriert werden, genau wie die integrierten FC-Ports. Eine Liste der Adapter, die für den Zielmodus konfiguriert werden können, ist in verfügbar "[NetApp Hardware Universe](#)".



NVMe/FC unterstützt Initiatormodus.

Schritte

1. Entfernen Sie alle LIFs vom Adapter:

```
network interface delete -vserver SVM_name -lif lif_name,lif_name
```

2. Versetzen Sie Ihren Adapter in den Offline-Modus:

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

3. Ändern Sie den Adapter von Ziel zu Initiator:

```
system hardware unified-connect modify -t initiator adapter_port
```

4. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
5. Vergewissern Sie sich, dass die FC-Ports für Ihre Konfiguration im richtigen Status konfiguriert sind:

```
system hardware unified-connect show
```

6. Versetzen Sie den Adapter wieder in den Online-Modus:

```
node run -node node_name storage enable adapter adapter_port
```

Konfigurieren Sie FC-Adapter für den Zielmodus

Sie können individuelle FC-Ports der integrierten Adapter und bestimmte FC-Adapterkarten für den Zielmodus konfigurieren. Der Zielmodus wird verwendet, um die Ports mit FC-Initiatoren zu verbinden.

Über diese Aufgabe

Jeder integrierte FC-Port kann individuell als Initiator oder Ziel konfiguriert werden. Die Ports auf bestimmten FC-Adaptoren können auch einzeln als Ziel-Port oder als Initiator-Port konfiguriert werden, genau wie die integrierten FC-Ports. Eine Liste der Adapter, die für den Zielmodus konfiguriert werden können, ist im verfügbar ["NetApp Hardware Universe"](#).

Bei der Konfiguration von FC-Adaptoren für das FC-Protokoll und das FC-NVMe-Protokoll kommen die gleichen Schritte zum Einsatz. Jedoch unterstützen nur bestimmte FC-Adapter FC-NVMe. Siehe ["NetApp Hardware Universe"](#) Für eine Liste von Adaptern, die das FC-NVMe-Protokoll unterstützen

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

```
node run -node node_name storage disable adapter adapter_name
```

Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

2. Ändern Sie den Adapter von Initiator zu Ziel:

```
system node hardware unified-connect modify -t target -node node_name adapter adapter_name
```

3. Booten Sie den Node neu, der den Adapter hostet, den Sie geändert haben.
4. Vergewissern Sie sich, dass der Zielport die richtige Konfiguration hat:

```
network fcp adapter show -node node_name
```

5. Schalten Sie Ihren Adapter online:

```
network fcp adapter modify -node node_name -adapter adapter_port -state up
```

Zeigt Informationen zu einem FC-Zieladapter an

Sie können das verwenden `network fcp adapter show` Befehl zum Anzeigen von Systemkonfiguration und Adapterinformationen für jeden FC-Adapter im System.

Schritt

1. Zeigen Sie mithilfe des Informationen zum FC-Adapter an `network fcp adapter show` Befehl.

Die Ausgabe zeigt für jeden verwendeten Steckplatz Informationen zur Systemkonfiguration und Adapterinformationen an.

```
network fcp adapter show -instance -node node1 -adapter 0a
```

Ändern Sie die FC-Adaptergeschwindigkeit

Sie sollten die Zielporgeschwindigkeit des Adapters so einstellen, dass sie mit der Geschwindigkeit des Geräts übereinstimmt, zu dem es eine Verbindung herstellt, anstatt die Autonegotiation zu verwenden. Ein Port, der auf die Autonegotiation festgelegt ist, kann nach einer Übernahme/Rückgabe oder einer anderen Unterbrechung länger dauern, bis die Verbindung wiederhergestellt ist.

Was Sie benötigen

Alle LIFs, die diesen Adapter als Home-Port verwenden, müssen offline sein.

Über diese Aufgabe

Da diese Aufgabe alle Storage Virtual Machines (SVMs) und alle LIFs in einem Cluster umfasst, müssen Sie das verwenden `-home-port` Und `-home-lif` Parameter, um den Umfang dieses Vorgangs zu begrenzen. Wenn Sie diese Parameter nicht verwenden, gilt der Vorgang für alle LIFs im Cluster, die möglicherweise nicht wünschenswert wären.

Schritte

1. Versetzen Sie alle LIFs auf diesem Adapter in den Offline-Modus:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }  
-status-admin down
```

2. Versetzen Sie den Adapter in den Offline-Modus:

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

Wenn der Adapter nicht in den Offline-Modus versetzt wird, können Sie das Kabel auch vom entsprechenden Adapterport im System entfernen.

3. Bestimmen Sie die maximale Geschwindigkeit für den Port-Adapter:

```
fcp adapter show -instance
```

Sie können die Adaptergeschwindigkeit nicht über die Höchstgeschwindigkeit hinaus ändern.

4. Ändern Sie die Adaptergeschwindigkeit:

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```


5. Versetzen Sie den Adapter in den Online-Modus:

```
network fcp adapter modify -node nodel -adapter 0c -state up
```

6. Versetzen Sie alle LIFs am Adapter in den Online-Modus:

```
network interface modify -vserver * -lif * { -home-node nodel -home-port 0c }  
-status-admin up
```

Unterstützte FC-Ports

Die Anzahl der für FC konfigurierten integrierten FC-Ports und CNA-/UTA2-Ports variiert basierend auf dem Modell des Controllers. FC-Ports sind auch über unterstützte FC-Zielerweiterungsadapter oder zusätzliche UTA2-Karten verfügbar, die mit FC SFP+ Adaptern konfiguriert sind.

Onboard FC-, UTA- und UTA2-Ports

- Die Onboard-Ports können individuell als Ziel- oder Initiator-FC-Ports konfiguriert werden.
- Die Anzahl der integrierten FC-Ports variiert je nach Controller-Modell.

Der "[NetApp Hardware Universe](#)" Enthält eine vollständige Liste der integrierten FC-Ports auf jedem Controller-Modell.

- FAS2520 Systeme unterstützen keine FC.

FC-Ports für den Zielerweiterungsadapter

- Die verfügbaren Zielerweiterungsadapter variieren je nach Controller-Modell.

Der "[NetApp Hardware Universe](#)" Enthält eine vollständige Liste der Adapter zur Zielerweiterung für jedes Controller-Modell.

- Die Ports auf einigen FC-Erweiterungsadaptern werden werkseitig als Initiatoren oder Ziele konfiguriert und können nicht geändert werden.

Andere können wie die integrierten FC-Ports individuell als Ziel- oder Initiator-FC-Ports konfiguriert werden. Eine vollständige Liste finden Sie in "[NetApp Hardware Universe](#)".

Vermeiden Sie den Verlust der Konnektivität bei Verwendung des X1133A-R6-Adapters

Sie können den Verlust der Konnektivität bei einem Port-Ausfall verhindern, indem Sie Ihr System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfigurieren.

Der X1133A-R6 HBA ist ein 16 GB FC-Adapter mit 4 Ports, der aus zwei 2-Port-Paaren besteht. Der X1133A-R6 Adapter kann als Zielmodus oder Initiatormodus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (z. B. Port 1 und Port 2 auf ASIC 1 und Port 3 und Port 4 auf ASIC 2). Beide Ports auf einem einzelnen ASIC müssen für die Ausführung im gleichen Modus – entweder im Ziel- oder im Initiatormodus – konfiguriert werden. Wenn ein Fehler auftritt, bei dem der ASIC ein Paar unterstützt, werden beide Ports im Paar offline geschaltet.

Um diesen Verlust der Konnektivität zu vermeiden, konfigurieren Sie Ihr System mit redundanten Pfaden zu

separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden.

Verwalten Sie X1143A-R6 Adapter

Überblick über die unterstützten Portkonfigurationen für X1143A-R6 Adapter

Standardmäßig ist der X1143A-R6 Adapter im FC-Zielmodus konfiguriert, Sie können seine Ports jedoch entweder als 10-GB-Ethernet- und FCoE-Ports (CNA) oder als 16-GB-FC-Initiator oder Ziel-Ports konfigurieren. Dazu sind andere SFP+-Adapter erforderlich.

Bei Konfiguration für Ethernet und FCoE unterstützen X1143A-R6 Adapter gleichzeitigen NIC- und FCoE-Zielverkehr auf demselben 10-GBE-Port. Bei Konfiguration für FC kann jedes Paar mit zwei Ports, das denselben ASIC verwendet, individuell für das FC-Ziel oder den FC-Initiator-Modus konfiguriert werden. Das bedeutet, dass ein einzelner X1143A-R6 Adapter einen FC-Zielmodus auf einem Paar mit zwei Ports und einen FC-Initiator-Modus auf einem anderen Paar mit zwei Ports unterstützen kann. Die mit demselben ASIC verbundenen Port-Paare müssen im gleichen Modus konfiguriert werden.

Im FC-Modus verhält sich der X1143A-R6 Adapter wie jedes vorhandene FC-Gerät mit Geschwindigkeiten von bis zu 16 Gbit/s. Im CNA-Modus können Sie den X1143A-R6-Adapter für den gleichzeitigen NIC- und FCoE-Datenverkehr verwenden, der denselben 10-GbE-Port nutzt. Der CNA-Modus unterstützt für die FCoE-Funktion nur den FC-Zielmodus.

Konfigurieren Sie die Ports

Um den Unified Target Adapter (X1143A-R6) zu konfigurieren, müssen die beiden benachbarten Ports auf demselben Chip im selben Personality-Modus konfiguriert werden.

Schritte

1. Konfigurieren Sie die Ports mithilfe des nach Bedarf für Fibre Channel (FC) oder Converged Network Adapter (CNA) `system node hardware unified-connect modify` Befehl.
2. Schließen Sie die entsprechenden Kabel für FC- oder 10-Gbit-Ethernet an.
3. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Für FC sollten Sie basierend auf der FC-Fabric, mit der verbunden ist, entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

Ändern Sie den UTA2-Port vom CNA-Modus in den FC-Modus

Sie sollten den UTA2-Port vom Converged Network Adapter (CNA)-Modus in den Fibre Channel (FC)-Modus ändern, um den FC-Initiator und den FC-Zielmodus zu unterstützen. Sie sollten die Persönlichkeit vom CNA-Modus in den FC-Modus ändern, wenn Sie das physische Medium ändern müssen, das den Port mit seinem Netzwerk verbindet.

Schritte

1. Versetzen Sie den Adapter in den Offline-Modus:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
down
```

2. Ändern des Portmodus:

```
ucadmin modify -node node_name -adapter adapter_name -mode fcp
```

3. Booten Sie den Node neu, und versetzen Sie den Adapter dann in den Online-Modus:

```
network fcp adapter modify -node node_name -adapter adapter_name -status-admin
up
```

4. Benachrichtigen Sie den Administrator oder VIF-Manager, dass er den Port löschen oder entfernen soll, falls zutreffend:

- Wenn der Port als Home Port einer logischen Schnittstelle verwendet wird, ist ein Mitglied einer Interface Group (ifgrp), oder Hosts VLANs, dann sollte ein Administrator Folgendes tun:
 - i. Verschieben Sie die LIFs, entfernen Sie den Port aus dem ifgrp oder löschen Sie die VLANs.
 - ii. Löschen Sie den Port manuell, indem Sie den ausführen `network port delete` Befehl.

Wenn der `network port delete` Der Befehl schlägt fehl, der Administrator sollte die Fehler beheben, und führen Sie dann den Befehl erneut aus.

- Wenn der Port nicht als Home-Port einer LIF verwendet wird, kein Mitglied eines ifgrp ist und keine VLANs hostet, dann sollte der VIF-Manager den Port zum Zeitpunkt des Neustarts aus seinen Datensätzen entfernen.

Wenn der VIF-Manager den Port nicht entfernt, muss der Administrator ihn nach dem Neustart manuell entfernen, indem er die verwendet `network port delete` Befehl.

```
net-f8040-34::> network port show
```

```
Node: net-f8040-34-01
```

Port	IPspace	Broadcast	Domain	Link	MTU	Speed (Mbps) Admin/Oper	Health Status
...							
e0i	Default	Default		down	1500	auto/10	-
e0f	Default	Default		down	1500	auto/10	-
...							

```
net-f8040-34::> ucadmin show
```

Node	Adapter	Current Mode	Current Type	Pending Mode	Pending Type	Admin
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

```

5. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Für CNA sollten Sie einen 10-GB-Ethernet SFP verwenden. Vor dem Ändern der Konfiguration auf dem Node sollten Sie für FC entweder einen 8-Gbit-SFP oder einen 16-Gbit-SFP verwenden.

Ändern Sie die optischen Module des CNA/UTA2-Zieladapters

Sie sollten die optischen Module auf dem Unified Target Adapter (CNA/UTA2) ändern, um den Personality-Modus zu unterstützen, den Sie für den Adapter ausgewählt haben.

Schritte

1. Überprüfen Sie das aktuelle SFP+, das in der Karte verwendet wird. Ersetzen Sie dann das aktuelle SFP+ durch das entsprechende SFP+ für die bevorzugte Persönlichkeit (FC oder CNA).
2. Entfernen Sie die aktuellen optischen Module vom X1143A-R6 Adapter.
3. Setzen Sie die richtigen Module für Ihre bevorzugte Personality-Mode-Optik (FC oder CNA) ein.
4. Vergewissern Sie sich, dass das richtige SFP+ installiert ist:

```
network fcp adapter show -instance -node -adapter
```

Unterstützte SFP+-Module und Twinax-Kabel (Cisco Branding Kupfer) sind in aufgeführt ["NetApp Hardware Universe"](#).

Zeigen Sie Adaptoreinstellungen an

Um die Einstellungen für Ihren Unified Target Adapter (X1143A-R6) anzuzeigen, müssen Sie den ausführen `system hardware unified-connect show` Befehl zum Anzeigen aller Module auf Ihrem Controller.

Schritte

1. Starten Sie den Controller, ohne die angeschlossenen Kabel zu verwenden.
2. Führen Sie die aus `system hardware unified-connect show` Befehl zum Anzeigen der Portkonfiguration und der Module.
3. Zeigen Sie die Portinformationen an, bevor Sie den CNA und die Ports konfigurieren.

FCoE-Konfigurationen

Möglichkeiten zur FCoE-Konfiguration – Übersicht

FCoE lässt sich mit FCoE Switches auf verschiedene Weise konfigurieren. Direct-Attached-Konfigurationen werden in FCoE nicht unterstützt.

Alle FCoE-Konfigurationen sind Dual Fabric-Systeme, vollständig redundant und erfordern Host-seitige Multipathing-Software. In allen FCoE-Konfigurationen können Sie im Pfad zwischen dem Initiator und dem Ziel mehrere FCoE- und FC-Switches bis zur maximalen Hop Count-Grenze verwenden. Um Switches miteinander zu verbinden, müssen auf den Switches eine Firmware-Version ausgeführt werden, die Ethernet-ISLs unterstützt. Jeder Host in einer FCoE-Konfiguration kann mit einem anderen Betriebssystem konfiguriert werden.

Für FCoE-Konfigurationen sind Ethernet Switches erforderlich, die explizit FCoE-Funktionen unterstützen. FCoE-Konfigurationen werden durch denselben Interoperabilitäts- und Qualitätssicherungsprozess wie FC Switches validiert. Unterstützte Konfigurationen sind in der Interoperabilitäts-Matrix aufgeführt. Einige der in

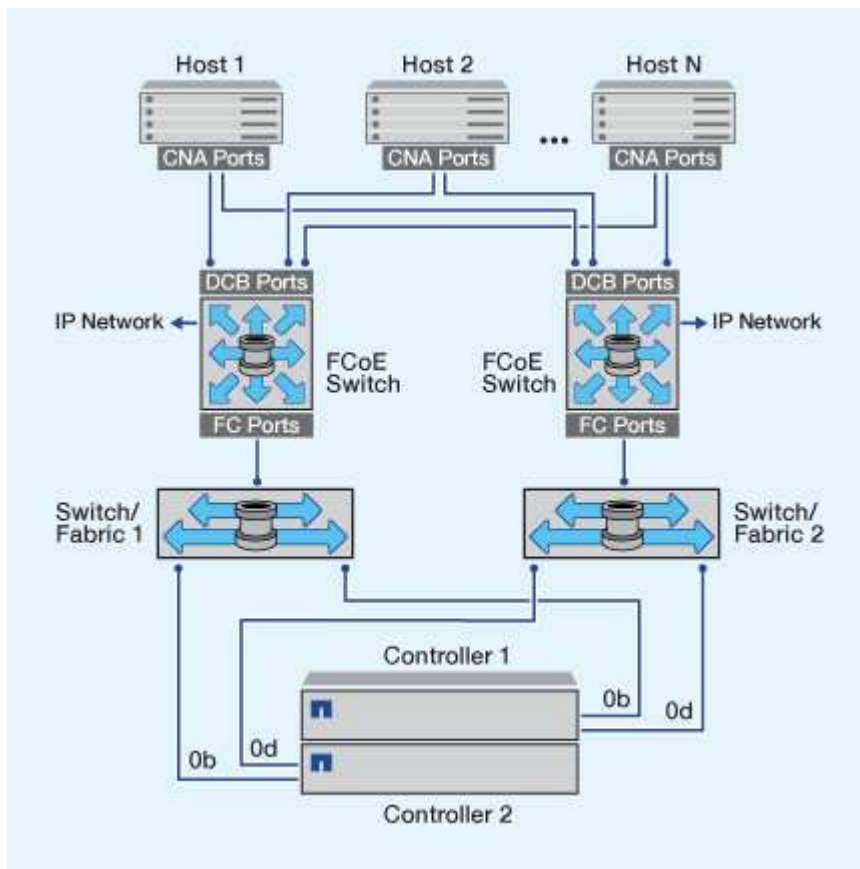
diesen unterstützten Konfigurationen enthaltenen Parameter sind das Switch-Modell, die Anzahl der Switches, die in einer einzigen Fabric implementiert werden können, und die unterstützte Switch-Firmware-Version.

Die Port-Nummern der FC-Target-Erweiterungsadapter in den Abbildungen sind Beispiele. Die tatsächlichen Port-Nummern können variieren, je nach den Erweiterungssteckplätzen, in denen die FCoE Ziel-Erweiterungsadapter installiert sind.

FCoE-Initiator zu FC-Ziel

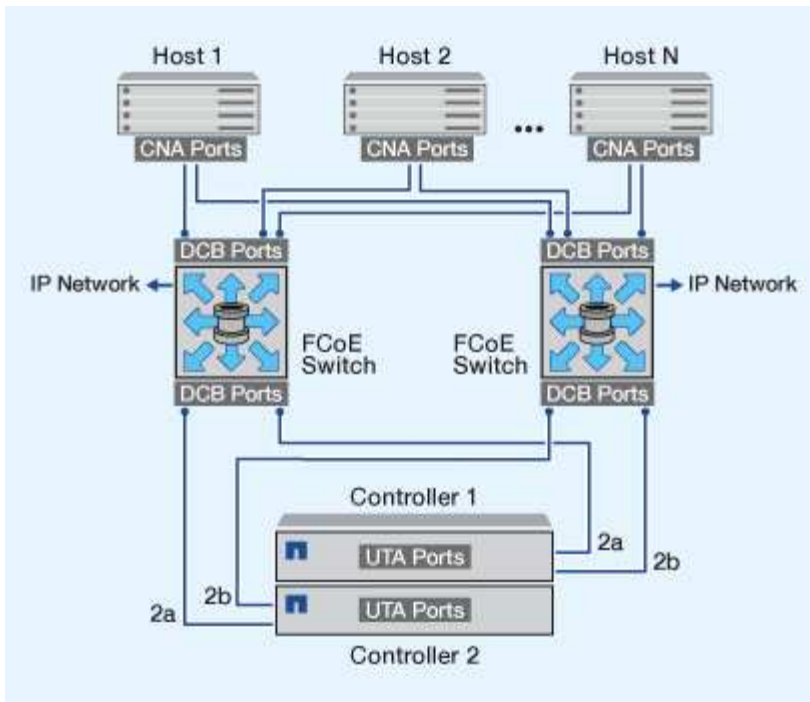
Mit FCoE-Initiatoren (CNAs) können Sie Hosts mit beiden Controllern in einem HA-Paar über FCoE Switches an FC-Ziel-Ports verbinden. Der FCoE-Switch muss auch über FC-Ports verfügen. Der Host FCoE Initiator stellt immer eine Verbindung zum FCoE-Switch her. Der FCoE Switch kann eine direkte Verbindung zum FC-Ziel herstellen oder über FC-Switches eine Verbindung zum FC-Ziel herstellen.

In der folgenden Abbildung werden die Host-CNAs, die eine Verbindung zu einem FCoE-Switch herstellen, und dann vor der Verbindung zum HA-Paar mit einem FC-Switch angezeigt:



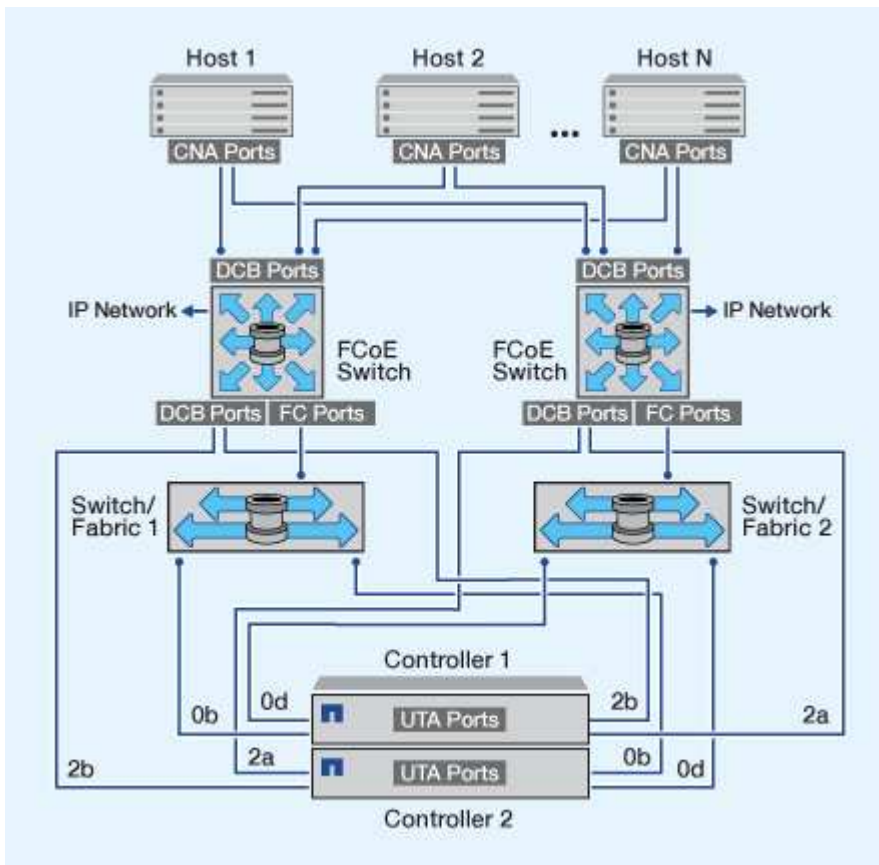
FCoE-Initiator zu FCoE Target

Mithilfe von Host FCoE-Initiatoren (CNAs) können Hosts über FCoE-Switches auf beiden Controllern über ein HA-Paar mit den FCoE Ziel-Ports (auch als UTAs oder UTA2 bezeichnet) verbunden werden.



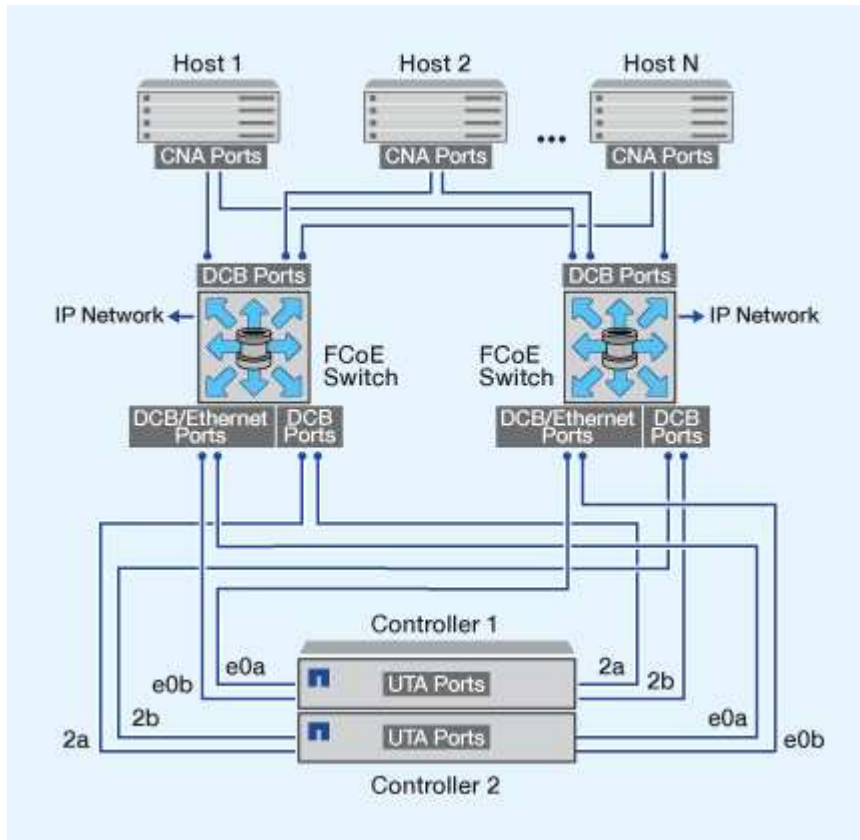
FCoE-Initiator auf FCoE- und FC-Ziele

Mithilfe von Host FCoE-Initiatoren (CNAs) können Hosts über FCoE Switches auf beiden Controllern in einem HA-Paar an FCoE- und FC-Ziel-Ports (auch als UTAs oder UTA2 bezeichnet) angeschlossen werden.



FCoE wird mit IP-Storage-Protokollen kombiniert

Mithilfe von Host FCoE-Initiatoren (CNAs) können Hosts über FCoE-Switches auf beiden Controllern über ein HA-Paar mit den FCoE Ziel-Ports (auch als UTAs oder UTA2 bezeichnet) verbunden werden. FCoE-Ports können keine herkömmliche Link-Aggregation zu einem einzelnen Switch verwenden. Cisco Switches unterstützen eine besondere Art von Link-Aggregation (Virtual Port Channel), die FCoE unterstützt. Ein Virtual Port Channel sammelt individuelle Links zu zwei Switches. Sie können virtuelle Port-Kanäle auch für andere Ethernet-Datenverkehr verwenden. Ports, die für andere Datenverkehr als FCoE verwendet werden, einschließlich NFS, SMB, iSCSI und anderer Ethernet-Datenverkehr, können regelmäßige Ethernet-Ports an den FCoE Switches nutzen.



FCoE-Initiator- und Zielkombinationen

Es werden bestimmte Kombinationen von FCoE und herkömmlichen FC-Initiatoren und -Zielen unterstützt.

FCoE-Initiatoren

Sie können FCoE-Initiatoren auf Host-Computern mit FCoE- und herkömmlichen FC-Zielen in Storage-Controllern verwenden. Der Host FCoE Initiator muss eine Verbindung zu einem FCoE DCB-Switch (Data Center Bridging) herstellen, eine direkte Verbindung zu einem Ziel wird nicht unterstützt.

In der folgenden Tabelle sind die unterstützten Kombinationen aufgeführt:

Initiator	Ziel	Unterstützt?
FC	FC	Ja.

Initiator	Ziel	Unterstützt?
FC	FCoE	Ja.
FCoE	FC	Ja.
FCoE	FCoE	Ja.

FCoE-Ziele

Sie können FCoE Ziel-Ports mit 4-, 8- oder 16-GB-FC-Ports auf dem Storage Controller kombinieren, unabhängig davon, ob es sich bei den FC-Ports um zusätzliche Zieladapter oder integrierte Ports handelt. Sie können im selben Storage Controller sowohl FCoE- als auch FC-Zieladapter einsetzen.



Für die Kombination von Onboard- und Erweiterungs-FC-Ports gelten weiterhin die Regeln.

FCoE-unterstützte Hop Count

Die maximal unterstützte Anzahl an Fibre Channel over Ethernet (FCoE)-Hops (Hop Count) zwischen einem Host und einem Storage-System hängt vom Switch-Anbieter und der Unterstützung des Storage-Systems für FCoE-Konfigurationen ab.

Hop Count ist definiert als die Anzahl der Switches im Pfad zwischen dem Initiator (Host) und dem Ziel (Storage-System). Die Dokumentation von Cisco Systems bezieht sich auch auf diesen Wert als *Durchmesser des SAN Fabric*.

Bei FCoE lassen sich FCoE-Switches mit FC-Switches verbinden.

Für lückenlose FCoE-Verbindungen müssen die FCoE Switches eine Firmware-Version ausführen, die Ethernet Inter-Switch Links (ISLs) unterstützt.

In der folgenden Tabelle sind die maximal unterstützten Hop Counts aufgeführt:

Lieferant wechseln	Unterstützte Hop Count
Brocade	7 für FC 5 für FCoE
Cisco	7 Es können bis zu 3 der Switches FCoE-Switches sein.

Fibre Channel- und FCoE-Zoning

Übersicht über Fibre Channel und FCoE Zoning

Eine FC-, FC-NVMe- oder FCoE-Zone ist eine logische Gruppierung von einem oder mehreren Ports in einer Fabric. Damit Geräte sich gegenseitig sehen können, eine

Verbindung herstellen, Sitzungen miteinander erstellen und kommunizieren können, müssen beide Ports eine gemeinsame Zonenmitgliedschaft aufweisen. Das Einzel-Initiator-Zoning wird empfohlen.

Gründe für das Zoning

- Das Zoning reduziert oder beseitigt *Crosstalk* zwischen Initiator-HBAs.

Dies geschieht sogar in kleinen Umgebungen und ist eines der besten Argumente für die Implementierung des Zoning. Die durch das Zoning erstellten logischen Fabric-Teilbereiche eliminieren etwaige Crosstalk-Probleme.

- Zoning reduziert die Anzahl der verfügbaren Pfade zu einem bestimmten FC-, FC-NVMe- oder FCoE-Port und reduziert die Anzahl der Pfade zwischen einem Host und einer bestimmten LUN, die sichtbar ist.

Beispielsweise haben einige Multipathing-Lösungen des Host-Betriebssystems eine Begrenzung für die Anzahl der Pfade, die sie verwalten können. Zoning kann die Anzahl der Pfade reduzieren, die ein Multipathing-Treiber für das Betriebssystem sieht. Wenn auf einem Host keine Multipathing-Lösung installiert ist, müssen Sie überprüfen, ob nur ein Pfad zu einer LUN sichtbar ist, indem Sie entweder die Zoneneinteilung in der Fabric oder eine Kombination aus Selective LUN Mapping (SLM) und Portsätze in der SVM verwenden.

- Zoning erhöht die Sicherheit, indem es den Zugriff und die Konnektivität auf Endpunkte begrenzt, die gemeinsam eine Zone nutzen.

Ports, die keine gemeinsamen Zonen haben, können nicht miteinander kommunizieren.

- Zoning verbessert die SAN-Zuverlässigkeit, indem es auftretende Probleme isoliert, und sorgt dafür, dass sich die Problemlösungszeit verringert, indem es den problematischen Speicherplatz einschränkt.

Empfehlungen für das Zoning

- Sie sollten das Zoning jederzeit implementieren, wenn vier oder mehr Hosts mit einem SAN verbunden sind oder SLM nicht auf den Nodes mit einem SAN implementiert wird.
- Obwohl das World Wide Node Name Zoning mit einigen Switch-Anbietern möglich ist, ist das World Wide Port Name Zoning erforderlich, um einen bestimmten Port ordnungsgemäß zu definieren und NPIV effektiv zu verwenden.
- Sie sollten die Zonengröße begrenzen und dabei die Verwaltbarkeit wahren.

Mehrere Zonen können sich überlappen, was die Größe verringert. Idealerweise wird eine Zone pro Host oder Host-Cluster definiert.

- Verwenden Sie das Einzel-Initiator-Zoning, um Crosstalk zwischen Initiator-HBAs zu eliminieren.

World Wide Name-basiertes Zoning

Beim Zoning auf Basis des World Wide Name (WWN) werden die WWNs der Mitglieder der Zone angegeben. Beim Zoning in ONTAP müssen Sie das WWPN-Zoning (World Wide Port Name) verwenden.

Das WWPN Zoning bietet Flexibilität, da der Zugriff nicht davon bestimmt wird, wo das Gerät physisch mit der Fabric verbunden ist. Sie können ein Kabel von einem Port in den anderen umstecken, ohne dass die Zonen neu konfiguriert werden müssen.

Für Fibre Channel-Pfade zu Storage Controllern, auf denen ONTAP ausgeführt wird, stellen Sie sicher, dass die FC-Switches mit den WWPNs der logischen Zielschnittstellen (LIFs) und nicht den WWPNs der physischen Ports auf dem Node begrenzt sind. Weitere Informationen zu LIFs finden Sie im *ONTAP Netzwerkmanagement-Leitfaden*.

"Netzwerkmanagement"

Individuelle Zonen

In der empfohlenen Zoning-Konfiguration gibt es einen Host-Initiator pro Zone. Die Zone besteht aus dem Host-Initiator-Port und einem oder mehreren Ziel-LIFs auf den Storage Nodes, die den Zugriff auf die LUNs bis zur gewünschten Anzahl der Pfade pro Ziel ermöglichen. Das bedeutet, dass Hosts, die auf dieselben Nodes zugreifen, die Ports der jeweils anderen Hosts nicht sehen können, aber jeder Initiator kann auf jeden Node zugreifen.

Sie sollten alle LIF von der Storage Virtual Machine (SVM) in die Zone mit dem Host-Initiator hinzufügen. So können Sie Volumes oder LUNs verschieben, ohne Ihre vorhandenen Zonen zu bearbeiten oder neue Zonen zu erstellen.

Vergewissern Sie sich bei Fibre Channel-Pfaden zu Nodes, auf denen ONTAP ausgeführt wird, dass die FC Switches mit den WWPNs der logischen Zielschnittstellen (LIFs) begrenzt sind, nicht mit den WWPNs der physischen Ports auf dem Node. Die WWPNs der physischen Ports beginnen mit „50“, und die WWPNs der LIFs beginnen mit „20“.

Einzel-Fabric-Zoning

In einer Einzel-Fabric-Konfiguration können Sie weiterhin jeden Host-Initiator mit jedem Storage Node verbinden. Auf dem Host wird Multipathing-Software benötigt, um mehrere Pfade verwalten zu können. Jeder Host sollte zwei Initiatoren für Multipathing haben, um Ausfallsicherheit in der Lösung zu gewährleisten.

Jeder Initiator sollte von jedem Node, auf den der Initiator zugreifen kann, mindestens eine LIF besitzen. Das Zoning sollte mindestens einen Pfad vom Host-Initiator zum HA-Paar der Nodes im Cluster zulassen, um einen Pfad für die LUN-Konnektivität bereitzustellen. Dies bedeutet, dass jeder Initiator auf dem Host in seiner Zonenkonfiguration möglicherweise nur über ein Ziel-LIF pro Node verfügt. Wenn Multipathing zum selben Node oder zu mehreren Nodes im Cluster erforderlich ist, dann verfügt jeder Node über mehrere LIFs in seiner Zonenkonfiguration. Dies ermöglicht es dem Host, weiterhin auf seine LUNs zuzugreifen, wenn ein Node ausfällt oder ein Volume mit der LUN auf einen anderen Node verschoben wird. Dafür müssen auch die Reporting-Nodes entsprechend eingestellt werden.

Single-Fabric-Konfigurationen werden unterstützt, jedoch nicht als hochverfügbar angesehen. Der Ausfall einer einzelnen Komponente kann zum Verlust des Zugriffs auf Daten führen.

In der folgenden Abbildung hat der Host zwei Initiatoren und führt die Multipathing-Software aus. Es gibt zwei Zonen:

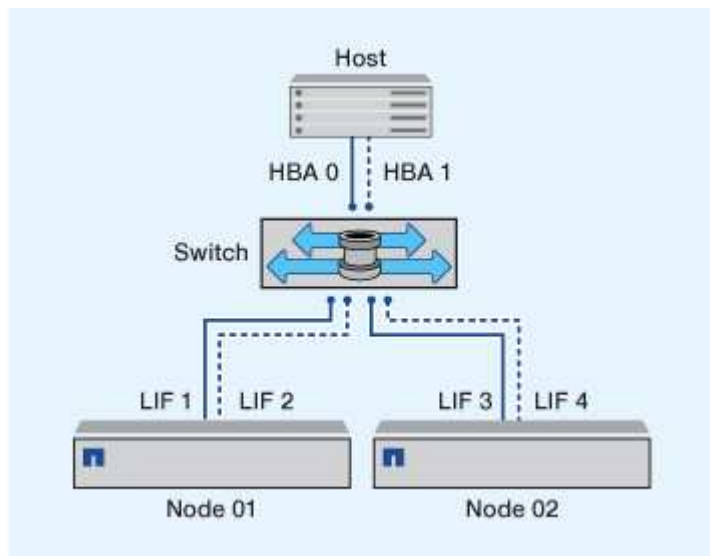


Die in dieser Abbildung verwendete Namenskonvention ist nur eine Empfehlung zu einer möglichen Namenskonvention, die Sie für Ihre ONTAP Lösung verwenden können.

- Zone 1: HBA 0, LIF_1 und LIF_3

- Zone 2: HBA 1, LIF_2 und LIF_4

Wenn die Konfiguration mehr Nodes enthielt, wären die LIFs für die zusätzlichen Nodes in diesen Zonen enthalten.



In diesem Beispiel könnten Sie auch alle vier LIFs in jeder Zone enthalten. In diesem Fall wären die Zonen wie folgt:

- Zone 1: HBA 0, LIF_1, LIF_2, LIF_3 und LIF_4
- Zone 2: HBA 1, LIF_1, LIF_2, LIF_3 und LIF_4



Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der unterstützten Pfade unterstützen, die zum Zugriff auf die LUNs auf den Nodes verwendet werden. Informationen zur Bestimmung der Anzahl der Pfade für den Zugriff auf die LUNs auf Nodes finden Sie im Abschnitt über die SAN-Konfigurationsbeschränkungen.

Verwandte Informationen

["NetApp Hardware Universe"](#)

Dual-Fabric-HA-Paar-Zoning

Bei Dual-Fabric-Konfigurationen können Sie jeden Host-Initiator mit jedem Cluster Node verbinden. Jeder Host Initiator verwendet einen anderen Switch, um auf die Cluster-Nodes zuzugreifen. Auf dem Host wird Multipathing-Software benötigt, um mehrere Pfade verwalten zu können.

Dual-Fabric-Konfigurationen gelten als Hochverfügbarkeit, da bei einem Ausfall einer einzelnen Komponente der Datenzugriff erhalten bleibt.

In der folgenden Abbildung hat der Host zwei Initiatoren und führt die Multipathing-Software aus. Es gibt zwei Zonen. SLM ist so konfiguriert, dass alle Nodes als Reporting-Nodes betrachtet werden.



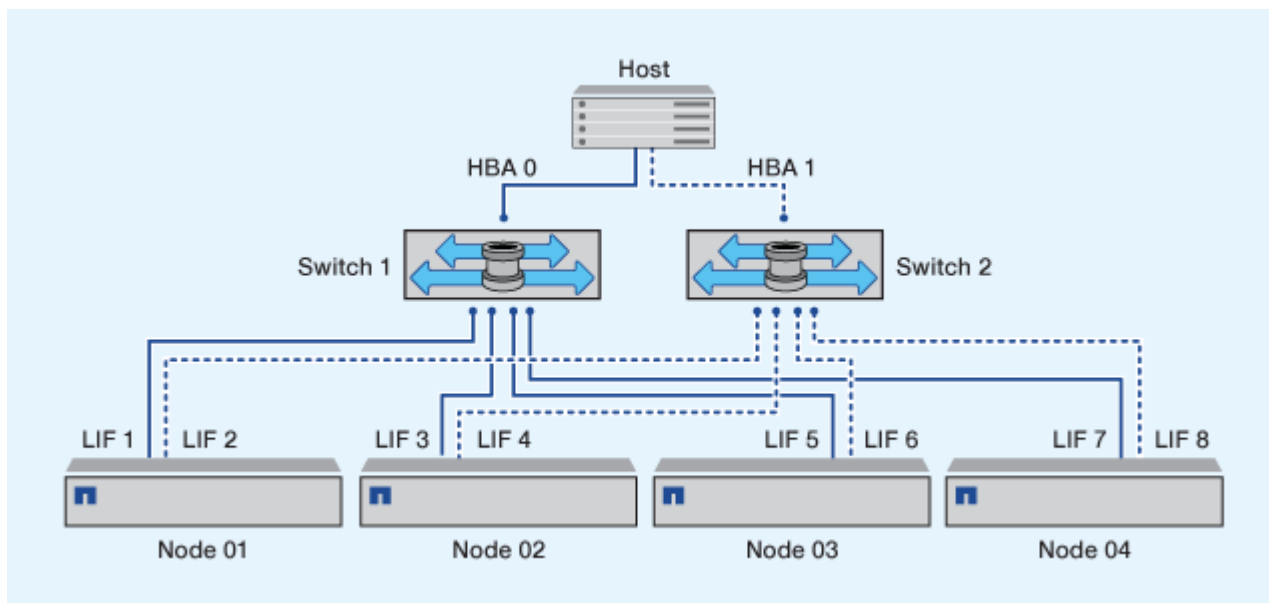
Die in dieser Abbildung verwendete Namenskonvention ist nur eine Empfehlung zu einer möglichen Namenskonvention, die Sie für Ihre ONTAP Lösung verwenden können.

- Zone 1: HBA 0, LIF_1, LIF_3, LIF_5 und LIF_7
- Zone 2: HBA 1, LIF_2, LIF_4, LIF_6 und LIF_8

Jeder Host-Initiator wird über einen anderen Switch begrenzt. Der Zugriff auf Zone 1 erfolgt über Schalter 1. Auf Zone 2 ist über Schalter 2 zugegriffen.

Jeder Initiator kann auf jedem Node auf ein LIF zugreifen. Dies ermöglicht es dem Host, weiterhin auf seine LUNs zuzugreifen, wenn ein Node ausfällt. SVMs können auf alle iSCSI- und FC-LIFs auf jedem Node in einer Cluster-Lösung zugreifen, basierend auf der Einstellung für Selective LUN Map (SLM) und der Konfiguration der Nodes für die Berichterstellung. Mit SLM, Portsätzen oder FC-Switch-Zoning reduzieren Sie die Anzahl der Pfade von einer SVM zum Host und die Anzahl der Pfade von einer SVM zu einer LUN.

Wenn die Konfiguration mehr Nodes enthielt, wären die LIFs für die zusätzlichen Nodes in diesen Zonen enthalten.



Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der Pfade unterstützen, die zum Zugriff auf die LUNs auf den Nodes verwendet werden.

Verwandte Informationen

["NetApp Hardware Universe"](#)

Zoning-Einschränkungen für Cisco FC und FCoE Switches

Bei Verwendung von Cisco FC und FCoE Switches darf eine einzelne Fabric-Zone nicht mehr als eine Ziel-LIF für denselben physischen Port enthalten. Wenn sich mehrere LIFs am selben Port in derselben Zone befinden, können die LIF-Ports nach einem Verlust der Verbindung möglicherweise nicht wiederherstellen.

Regelmäßige FC-Switches werden für das FC-NVMe-Protokoll auf dieselbe Weise verwendet wie für das FC-Protokoll.

- Mehrere LIFs für die FC- und FCoE-Protokolle können physische Ports auf einem Node gemeinsam nutzen, sofern sie sich in verschiedenen Zonen befinden.

- FC-NVMe und FCoE können sich nicht denselben physischen Port teilen.
- FC und FC-NVMe können sich denselben 32 GB physischen Port teilen.
- Bei Cisco FC- und FCoE-Switches muss sich jede LIF auf einem bestimmten Port in einer separaten Zone von den anderen LIFs an diesem Port befinden.
- Eine einzelne Zone kann sowohl FC- als auch FCoE-LIFs haben. Eine Zone kann von jedem Ziel-Port im Cluster eine LIF enthalten, gehen Sie jedoch darauf ein, die Pfadgrenzen des Hosts nicht zu überschreiten und die SLM-Konfiguration zu überprüfen.
- LIFs an verschiedenen physischen Ports können sich in derselben Zone befinden.
- Für Cisco Switches müssen LIFs getrennt sein.

Das Trennen von LIFs ist zwar nicht erforderlich, das Trennen aller Switches wird jedoch empfohlen

Anforderungen für Shared-SAN-Konfigurationen

Konfigurationen mit Shared SAN werden als Hosts definiert, die sowohl mit ONTAP-Storage-Systemen als auch Storage-Systemen anderer Anbieter verbunden sind. Der Zugriff auf die ONTAP Storage-Systeme und die Storage-Systeme anderer Hersteller über einen einzigen Host wird unterstützt, sofern verschiedene Anforderungen erfüllt sind.

Bei allen Host-Betriebssystemen gilt es, eine Verbindung mit separaten Adaptern mit den Storage-Systemen jedes Anbieters zu herstellen. Die Verwendung separater Adapter verringert die Wahrscheinlichkeit widersprüchlicher Treiber und Einstellungen. Wenn Verbindungen zu einem ONTAP Storage-System hergestellt werden sollen, müssen das Adaptermodell, das BIOS, die Firmware und der Treiber als unterstützt im NetApp Interoperabilitäts-Matrix-Tool aufgeführt sein.

Sie sollten die erforderlichen oder empfohlenen Zeitüberschreitungswerte und andere Speicherparameter für den Host festlegen. Sie müssen immer die NetApp Software installieren oder zuletzt die NetApp-Einstellungen anwenden.

- Für AIX sollten Sie die Werte aus der AIX Host Utilities-Version anwenden, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.
- Für ESX sollten Sie die Host-Einstellungen über die Virtual Storage Console für VMware vSphere anwenden.
- Für HP-UX sollten Sie die HP-UX Standard-Speichereinstellungen verwenden.
- Bei Linux sollten Sie die Werte aus der Version Linux Host Utilities anwenden, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.
- Bei Solaris sollten Sie die Werte aus der Solaris Host Utilities-Version anwenden, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.
- Für Windows sollten Sie die Windows Host Utilities-Version installieren, die im Interoperabilitäts-Matrix-Tool für Ihre Konfiguration aufgeführt ist.

Verwandte Informationen

["NetApp Interoperabilitäts-Matrix-Tool"](#)

SAN-Konfigurationen in einer MetroCluster Umgebung

SAN-Konfigurationen in einer MetroCluster Umgebung

Beim Einsatz von SAN-Konfigurationen in einer MetroCluster Umgebung müssen Sie jedoch bestimmte Überlegungen beachten.

- MetroCluster-Konfigurationen unterstützen vSAN Konfigurationen nicht auf Frontend-FC-Fabric „Routed“.
- Ab ONTAP 9.12.1 MetroCluster werden NVMe/FC Konfigurationen mit vier Nodes unterstützt. MetroCluster-Konfigurationen werden auf NVMe/TCP nicht unterstützt. MetroCluster Konfigurationen werden für NVMe vor ONTAP 9.12.1 nicht unterstützt.
- Andere SAN-Protokolle wie iSCSI, FC und FCoE werden auf MetroCluster Konfigurationen unterstützt.
- Bei der Verwendung von SAN-Client-Konfigurationen müssen Sie prüfen, ob spezielle Überlegungen für MetroCluster-Konfigurationen in den Notizen, die in aufgeführt sind, enthalten sind ["NetApp Interoperabilitäts-Matrix-Tool" \(IMT\)](#).
- Betriebssysteme und Applikationen müssen eine I/O-Ausfallsicherheit von 120 Sekunden bieten, um die automatische, ungeplante MetroCluster Umschaltung sowie eine Tiebreaker oder Mediator-initiierte Umschaltung zu unterstützen.
- Das MetroCluster verwendet dieselben WWPNs auf beiden Seiten des Front-End-SAN.

Verwandte Informationen

- ["MetroCluster Datensicherung und Disaster Recovery verstehen"](#)
- ["Knowledge Base-Artikel: Was sind Überlegungen zur Unterstützung von AIX-Hosts in einer MetroCluster-Konfiguration?"](#)
- ["Knowledge Base-Artikel: Überlegungen zur Unterstützung von Solaris-Hosts in einer MetroCluster-Konfiguration"](#)

Vermeiden Sie Überschneidungen zwischen Switchover und Switchback

In einer SAN-Umgebung können Sie die Front-End-Switches konfigurieren, um Überlappungen zu vermeiden, wenn der alte Port offline geschaltet wird und der neue Port online geschaltet wird.

Während der Umschaltung meldet sich der FC-Port am verbleibenden Standort möglicherweise beim Fabric an, bevor die Fabric erkannt hat, dass der FC-Port am Disaster-Standort offline ist und diesen Port aus dem Namen- und Verzeichnisdienst entfernt hat.

Wenn der FC-Port bei der Katastrophe noch nicht entfernt wird, wird der Fabric-Anmeldeversuch des FC-Ports am noch intakten Standort aufgrund eines doppelten WWPN möglicherweise abgelehnt. Dieses Verhalten der FC-Switches kann geändert werden, um die Anmeldung des vorherigen Geräts und nicht des vorhandenen zu ermöglichen. Sie sollten die Auswirkungen dieses Verhaltens auf andere Fabric-Geräte überprüfen. Weitere Informationen erhalten Sie vom Switch-Anbieter.

Wählen Sie das richtige Verfahren je nach Schaltertyp aus.

Beispiel 9. Schritte

Cisco Switch

1. Stellen Sie eine Verbindung zum Switch her, und melden Sie sich an.
2. Konfigurationsmodus aufrufen:

```
switch# config t
switch(config)#
```

3. Überschreiben Sie den ersten Geräteeintrag in der Namensserver-Datenbank mit dem neuen Gerät:

```
switch(config)# no fcns reject-duplicate-pwvn vsan 1
```

4. Vergewissern Sie sich bei Switches, die NX-OS 8.x ausführen, dass das flogi-Timeout auf Null gesetzt ist:

- a. Anzeige des Zeitschaltuftszeitumschaltudes:

```
switch(config)# show flogi interval info \ i quiesce
```

```
Stats: fs flogi quiesce timerval: 0
```

- b. Wenn die Ausgabe im vorherigen Schritt nicht angibt, dass der Zeitwert Null ist, setzen Sie ihn auf null:

```
switch(config)# flogi scale enable
```

```
switch(config)$ flogi quiesce timeout 0
```

Brocade Switch

1. Stellen Sie eine Verbindung zum Switch her, und melden Sie sich an.
2. Geben Sie das ein switchDisable Befehl.
3. Geben Sie das ein configure Befehl und drücken Sie y An der Eingabeaufforderung.

```
F-Port login parameters (yes, y, no, n): [no] y
```

4. Einstellung 1 auswählen:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```


5. Beantworten Sie die verbleibenden Eingabeaufforderungen, oder drücken Sie **Strg + D**.
6. Geben Sie das ein `switchEnable` Befehl.

Verwandte Informationen

["Umschaltung für Tests oder Wartung"](#)

Host-Unterstützung für Multipathing

Host-Unterstützung für Multipathing – Übersicht

ONTAP verwendet für FC- und iSCSI-Pfade immer Asymmetric Logical Unit Access (ALUA). Nutzen Sie Host-Konfigurationen, die ALUA für FC- und iSCSI-Protokolle unterstützen.

Ab ONTAP 9.5 wird Multipath HA-Paar-Failover/Giveback für NVMe-Konfigurationen unter Verwendung von Asynchronous Namespace Access (ANA) unterstützt. In ONTAP 9.4 unterstützt NVMe nur einen Pfad vom Host zum Ziel. Der Applikations-Host muss Pfad-Failover zu seinem Hochverfügbarkeits-Partner managen.

Informationen darüber, welche spezifischen Host-Konfigurationen ALUA oder ANA unterstützen, finden Sie im ["NetApp Interoperabilitäts-Matrix-Tool"](#) Und ["ONTAP SAN-Host-Konfiguration"](#) Für Ihr Host-Betriebssystem.

Wenn die Host-Multipathing-Software erforderlich ist

Wenn sich mehrere Pfade von den logischen Schnittstellen (LIFs) der Storage Virtual Machine (SVM) zu dem Fabric befinden, ist eine Multipathing-Software erforderlich. Auf dem Host ist jederzeit Multipathing-Software erforderlich, wenn der Host über mehrere Pfade auf eine LUN zugreifen kann.

Die Multipathing-Software stellt dem Betriebssystem eine einzelne Festplatte für alle Pfade zu einer LUN zur Verfügung. Ohne Multipathing-Software kann das Betriebssystem jeden Pfad als separate Festplatte behandeln, was zu Datenbeschädigungen führen kann.

Ihre Lösung wird als mehrere Pfade angesehen, wenn Sie einen der folgenden haben:

- Ein einzelner Initiator-Port im Host, der an mehrere SAN LIFs in der SVM angeschlossen ist
- Mehrere Initiator-Ports, die an eine einzelne SAN-LIF in der SVM angeschlossen sind
- Mehrere Initiator-Ports, die an mehrere SAN-LIFs in der SVM angeschlossen sind

Multipathing-Software wird in HA-Konfigurationen empfohlen. Zusätzlich zur Selective LUN Map wird empfohlen, die Verwendung von FC Switch Zoning oder Portsets zur Beschränkung der Pfade für den Zugriff auf LUNs verwendet.

Multipathing-Software wird auch als MPIO-Software (Multipath I/O) bezeichnet.

Empfohlene Anzahl an Pfaden vom Host zu Nodes im Cluster

Sie sollten mehr als acht Pfade von Ihrem Host zu jedem Node im Cluster nicht überschreiten. Achten Sie auf die Gesamtzahl der Pfade, die für das Host-Betriebssystem und das auf dem Host verwendete Multipathing unterstützt werden

können.

Pro LUN sollten Sie mindestens zwei Pfade haben, die mit jedem Reporting Node durch eine selektive LUN Map (SLM) verbunden sind, die von der Storage Virtual Machine (SVM) in Ihrem Cluster verwendet wird. So werden Single Points of Failure eliminiert und das System kann den Ausfall von Komponenten überleben.

Wenn Sie vier oder mehr Nodes in Ihrem Cluster haben oder mehr als vier von den SVMs in einem Ihrer Nodes verwendete Ziel-Ports: Mithilfe der folgenden Methoden können Sie die Anzahl der Pfade begrenzen, die zum Zugriff auf LUNs auf Ihren Nodes verwendet werden können, damit Sie die empfohlene maximale Anzahl von acht Pfaden nicht überschreiten.

- SLM

SLM reduziert die Anzahl der Pfade vom Host zur LUN auf nur Pfade auf dem Node, der die LUN besitzt, und dem HA-Partner des entsprechenden Node. SLM ist standardmäßig aktiviert.

- Portsets für iSCSI
- FC igroup-Zuordnungen von Ihrem Host
- FC-Switch-Zoning

Verwandte Informationen

["SAN-Administration"](#)

Konfigurationseinschränkungen

Anzahl der unterstützten Nodes für SAN-Konfigurationen ermitteln

Die von ONTAP unterstützte Anzahl der Nodes pro Cluster variiert je nach Version von ONTAP, den Storage-Controller-Modellen im Cluster und dem Protokoll der Cluster-Nodes.

Über diese Aufgabe

Wenn ein Node im Cluster für FC, FC-NVMe, FCoE oder iSCSI konfiguriert ist, ist dieser Cluster auf die Einschränkungen für den SAN-Node beschränkt. Node-Limits basierend auf den Controllern im Cluster werden im „*Hardware Universe*“ aufgeführt.

Schritte

1. Gehen Sie zu ["NetApp Hardware Universe"](#).
2. Klicken Sie oben links auf **Plattformen** (neben der Schaltfläche **Home**) und wählen Sie den Plattformtyp aus.
3. Aktivieren Sie das Kontrollkästchen neben Ihrer ONTAP-Version.

Es wird eine neue Spalte angezeigt, in der Sie Ihre Plattformen auswählen können.

4. Aktivieren Sie die Kontrollkästchen neben den Plattformen, die in Ihrer Lösung verwendet werden.
5. Deaktivieren Sie das Kontrollkästchen * Alle auswählen* in der Spalte **Wählen Sie Ihre Spezifikationen**.
6. Aktivieren Sie das Kontrollkästchen * Max Nodes pro Cluster (NAS/SAN)*.
7. Klicken Sie Auf **Ergebnisse Anzeigen**.

Verwandte Informationen

Legen Sie die Anzahl der unterstützten Hosts pro Cluster in FC- und FC-NVMe-Konfigurationen fest

Die maximale Anzahl an SAN-Hosts, die mit einem Cluster verbunden werden können, variiert stark. Dies hängt von Ihrer spezifischen Kombination aus mehreren Cluster-Attributen ab, z. B. die Anzahl der mit jedem Cluster Node verbundenen Hosts, Initiatoren pro Host, Sitzungen pro Host und Nodes im Cluster.

Über diese Aufgabe

Für FC- und FC-NVMe-Konfigurationen sollten Sie anhand der Anzahl der Initiator-Target-Nexuses (ITNs) in Ihrem System ermitteln, ob Sie Ihrem Cluster weitere Hosts hinzufügen können.

Ein ITN steht für einen Pfad vom Host-Initiator zum Ziel des Storage-Systems. In FC- und FC-NVMe-Konfigurationen beträgt die maximale Anzahl an ITNs pro Node 2,048. Solange Sie unter der maximalen Anzahl von ITNs liegen, können Sie Ihrem Cluster weiterhin Hosts hinzufügen.

Führen Sie die folgenden Schritte für jeden Knoten im Cluster durch, um die Anzahl der in Ihrem Cluster verwendeten ITNs zu ermitteln.

Schritte

1. Identifizieren Sie alle LIFs an einem bestimmten Node.
2. Führen Sie den folgenden Befehl für jede LIF auf dem Node aus:

```
fcp initiator show -fields wwpn, lif
```

Die Anzahl der Einträge, die unten in der Befehlsausgabe angezeigt werden, stellt Ihre Anzahl an ITNs für diese LIF dar.

3. Notieren Sie die Anzahl der angezeigten ITNs für jedes LIF.
4. Fügen Sie auf jedem Knoten des Clusters die Anzahl der ITNs für jede LIF hinzu.

Diese Summe gibt die Anzahl der ITNs in Ihrem Cluster an.

Bestimmen Sie die unterstützte Anzahl von Hosts in iSCSI-Konfigurationen

Die maximale Anzahl an SAN-Hosts, die in iSCSI-Konfigurationen verbunden werden können, variiert je nach Ihrer spezifischen Kombination aus mehreren Cluster-Attributen wie die Anzahl der mit jedem Cluster-Node verbundenen Hosts, Initiatoren pro Host, Anmeldungen pro Host und Nodes im Cluster stark.

Über diese Aufgabe

Die Anzahl der Hosts, die direkt mit einem Node verbunden werden können oder die über einen oder mehrere Switches verbunden werden können, hängt von der Anzahl der verfügbaren Ethernet-Ports ab. Die Anzahl der verfügbaren Ethernet-Ports wird durch das Modell des Controllers und die Anzahl und den Typ der im Controller installierten Adapter bestimmt. Die Anzahl der unterstützten Ethernet-Ports für Controller und Adapter ist im *Hardware Universe* verfügbar.

Bei allen Cluster-Konfigurationen mit mehreren Nodes müssen Sie die Anzahl der iSCSI-Sitzungen pro Node bestimmen, damit Sie dem Cluster weitere Hosts hinzufügen können. Solange Ihr Cluster die maximale Anzahl von iSCSI-Sitzungen pro Node unterschritten hat, können Sie Ihrem Cluster weiterhin Hosts hinzufügen. Die

maximale Anzahl von iSCSI-Sitzungen pro Node variiert abhängig von den Typen der Controller in Ihrem Cluster.

Schritte

1. Identifizieren Sie alle Zielportalgruppen auf dem Knoten.
2. Überprüfen Sie die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten:

```
iscsi session show -tpgroup tpgroup
```

Die Anzahl der Einträge, die unten in der Befehlsausgabe angezeigt werden, entspricht der Anzahl der iSCSI-Sitzungen für diese Zielportalgruppe.

3. Notieren Sie die Anzahl der für jede Zielportalgruppe angezeigten iSCSI-Sitzungen.
4. Fügen Sie die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten hinzu.

Die Gesamtsumme stellt die Anzahl der iSCSI-Sitzungen auf Ihrem Knoten dar.

Einschränkungen bei der Konfiguration des FC-Switch

Bei der Konfiguration der Fibre-Channel-Switches gilt es, Höchstwerte zu beachten, einschließlich der Anzahl der unterstützten Anmeldungen pro Port, Port-Gruppe, Blade und Switch. Die Switch-Anbieter dokumentieren die von ihnen unterstützten Grenzwerte.

Jede logische FC-Schnittstelle (Logical Interface, LIF) meldet sich bei einem FC-Switch-Port an. Die Gesamtzahl der Anmeldungen von einem einzelnen Ziel auf dem Node entspricht der Anzahl der LIFs plus eine Anmeldung für den zugrunde liegenden physischen Port. Überschreiten Sie nicht die Konfigurationsgrenzwerte des Switch-Anbieters für Anmeldungen oder andere Konfigurationswerte. Dies gilt auch für die Initiatoren, die auf der Host-Seite in virtualisierten Umgebungen mit aktiviertem NPIV verwendet werden. Überschreiten Sie nicht die Konfigurationsgrenzwerte des Switch-Anbieters für Anmeldungen entweder für das Ziel oder für die in der Lösung verwendeten Initiatoren.

Einschränkungen für den Brocade Switch

Die Konfigurationsgrenzwerte für Brocade Switches finden Sie in den „*Brocade Scalability Guidelines*“.

Einschränkungen für die Switches von Cisco Systems

Die Konfigurationsbeschränkungen für Cisco Switches finden Sie im ["Einschränkungen Bei Der Konfiguration Von Cisco"](#) Leitfaden für Ihre Version der Cisco Switch-Software.

Warteschlangentiefe berechnen – Übersicht

Möglicherweise müssen Sie Ihre FC-Warteschlangentiefe auf dem Host abstimmen, um die maximalen Werte für ITNs pro Node und FC-Port-Fan-in zu erreichen. Die maximale Anzahl der LUNs und die Anzahl der HBAs, die eine Verbindung zu einem FC-Port herstellen können, sind durch die verfügbare Warteschlangentiefe auf den FC-Zielpports begrenzt.

Über diese Aufgabe

„Queue depth“ ist die Anzahl von I/O-Anfragen (SCSI-Befehle), die sich gleichzeitig in ein Storage Controller Warteschlange einreihen lassen. Jede I/O-Anforderung vom Initiator-HBA des Hosts zum Zieladapter des

Storage-Controllers verbraucht einen Warteschlangeneintrag. Eine höhere Warteschlangentiefe entspricht in der Regel einer besseren Performance. Wenn jedoch die maximale Warteschlangentiefe des Storage Controllers erreicht wird, weist dieser Storage-Controller eingehende Befehle zurück, indem er eine QFULL-Antwort zurückgibt. Wenn eine große Anzahl von Hosts auf einen Speicher-Controller zugreifen, sollten Sie sorgfältig planen, QFULL-Bedingungen zu vermeiden, die die Systemleistung erheblich beeinträchtigen und zu Fehlern bei einigen Systemen führen können.

In einer Konfiguration mit mehreren Initiatoren (Hosts) sollten alle Hosts über ähnliche Warteschlangentiefen verfügen. Aufgrund der Ungleichheit in der Warteschlangentiefe zwischen Hosts, die über denselben Zielport mit dem Storage Controller verbunden sind, wird Hosts mit kleineren Warteschlangentiefen dem Zugriff auf Ressourcen durch Hosts mit größeren Warteschlangentiefen entzogen.

Die folgenden allgemeinen Empfehlungen bezüglich „Tuning“-Warteschlangentiefe:

- Verwenden Sie für kleine und mittelgroße Systeme eine HBA-Warteschlangenlänge von 32.
- Verwenden Sie für große Systeme eine HBA-Warteschlangenlänge von 128.
- Verwenden Sie für Ausnahmefälle oder Performance-Tests eine Warteschlangentiefe von 256, um mögliche Warteschlangenprobleme zu vermeiden.
- Für alle Hosts sollten die Warteschlangentiefen auf ähnliche Werte festgelegt sein, um allen Hosts gleichberechtigten Zugriff zu gewähren.
- Um Performance-Einbußen oder Fehler zu vermeiden, darf die Ziel-FC-Port-Warteschlangentiefe des Storage Controllers nicht überschritten werden.

Schritte

1. Zählen Sie die Gesamtzahl der FC-Initiatoren auf allen Hosts, die mit einem FC-Zielport verbunden sind.
2. Mit 128 multiplizieren.
 - Wenn das Ergebnis unter 2,048 liegt, setzen Sie die Warteschlangentiefe für alle Initiatoren auf 128. Sie haben 15 Hosts, wobei ein Initiator mit jedem der zwei Ziel-Ports auf dem Storage Controller verbunden ist. $15 \times 128 = 1,920$. Da 1,920 kleiner als die gesamte Warteschlangentiefe von 2,048 ist, können Sie die Warteschlangentiefe für alle Initiatoren auf 128 einstellen.
 - Wenn das Ergebnis größer als 2,048 ist, mit Schritt 3 fortfahren. Sie haben 30 Hosts, wobei ein Initiator mit jedem der zwei Ziel-Ports auf dem Storage Controller verbunden ist. $30 \times 128 = 3,840$. Da 3,840 die Gesamttiefe der Warteschlange von 2,048 überschreitet, sollten Sie eine der Optionen unter Schritt 3 zur Behebung wählen.
3. Wählen Sie eine der folgenden Optionen, um dem Storage Controller mehr Hosts hinzuzufügen.
 - Option 1:
 - i. Weitere FC-Ziel-Ports hinzufügen.
 - ii. Neuverteilung Ihrer FC-Initiatoren
 - iii. Wiederholen Sie die Schritte 1 und 2. + die gewünschte Warteschlangentiefe von 3,840 überschreitet die verfügbare Warteschlangentiefe pro Port. Um dies zu beheben, können Sie jedem Controller einen FC-Zieladapter mit zwei Ports hinzufügen und Ihre FC-Switches neu Zone festlegen, so dass 15 Ihrer 30 Hosts mit einem Satz Ports verbunden werden. Die restlichen 15 Hosts verbinden sich mit einem zweiten Port-Satz. Die Warteschlangentiefe pro Port wird dann auf $15 \times 128 = 1,920$ reduziert.
 - Option 2:
 - i. Weisen Sie jeden Host basierend auf seinem erwarteten I/O-Bedarf als „large“ oder „small“ zu.
 - ii. Multiplizieren Sie die Anzahl der großen Initiatoren mit 128.

- iii. Multiplizieren Sie die Anzahl der kleinen Initiatoren mit 32.
- iv. Fügen Sie die beiden Ergebnisse zusammen.
- v. Wenn das Ergebnis weniger als 2,048 ist, stellen Sie die Warteschlangentiefe für große Hosts auf 128 und die Warteschlangentiefe für kleine Hosts auf 32 ein.
- vi. Wenn das Ergebnis immer noch größer als 2,048 pro Port ist, reduzieren Sie die Warteschlangentiefe pro Initiator, bis die gesamte Warteschlangentiefe kleiner als oder gleich 2,048 ist.



Um die Warteschlangentiefe zu schätzen, die für einen bestimmten I/O-Durchsatz pro Sekunde erforderlich ist, verwenden Sie folgende Formel:

Benötigte Queue-Tiefe = (Anzahl I/O pro Sekunde) × (Reaktionszeit)

Wenn Sie beispielsweise 40,000 I/O pro Sekunde mit einer Reaktionszeit von 3 Millisekunden benötigen, dann ist die benötigte Warteschlangentiefe = $40,000 \times (.003) = 120$.

Die maximale Anzahl von Hosts, die Sie mit einem Zielport verbinden können, ist 64, wenn Sie sich entscheiden, die Warteschlangentiefe auf die grundlegende Empfehlung von 32 zu begrenzen. Wenn Sie sich jedoch für eine Warteschlangentiefe von 128 entscheiden, können maximal 16 Hosts mit einem Zielport verbunden sein. Je größer die Warteschlangentiefe, desto weniger Hosts, die ein einziger Zielport unterstützen kann. Wenn Sie eine solche Anforderung haben, dass Sie keine Kompromisse in der Warteschlangentiefe machen können, sollten Sie mehr Zielports erhalten.

Die gewünschte Warteschlangentiefe von 3,840 überschreitet die verfügbare Warteschlangentiefe pro Port. Es gibt 10 „große“ Hosts mit hohen Storage-I/O-Anforderungen und 20 „kleine“ Hosts mit niedrigen I/O-Anforderungen. Setzen Sie die Tiefe der Initiator-Warteschlange auf den großen Hosts auf 128 und die Tiefe der Initiator-Warteschlange auf den kleinen Hosts auf 32.

Ihre resultierende Gesamtwarteschlangentiefe beträgt $(10 \times 128) + (20 \times 32) = 1,920$.

Sie können die verfügbare Warteschlangentiefe gleichmäßig auf jeden Initiator verteilen.

Ihre resultierende Warteschlangentiefe pro Initiator beträgt $2,048 \div 30 = 68$.

Festlegen der Warteschlangentiefe auf SAN-Hosts

Möglicherweise müssen Sie die Warteschlangentiefe auf Ihrem Host ändern, um die maximalen Werte für ITNs pro Knoten und FC-Port-Fan-in zu erreichen.

AIX-Hosts

Sie können die Warteschlangentiefe auf AIX-Hosts mithilfe der ändern `chdev` Befehl. Änderungen, die mit dem vorgenommen wurden `chdev` Befehl bleibt während eines Neustarts bestehen.

Beispiele:

- Um die Warteschlangentiefe für das `hdisk7`-Gerät zu ändern, verwenden Sie den folgenden Befehl:

```
chdev -l hdisk7 -a queue_depth=32
```

- Verwenden Sie den folgenden Befehl, um die Warteschlangentiefe für den `FCS0-HBA` zu ändern:

```
chdev -l fcs0 -a num_cmd_elems=128
```

Der Standardwert für `num_cmd_elems` ist 200. Der maximale Wert ist 2,048.



Möglicherweise muss der HBA in den Offline-Modus versetzt werden, um ihn zu ändern `num_cmd_elems` Und bringen Sie es dann wieder online mit dem `rmdev -l fcs0 -R` Und `makdev -l fcs0 -P` Befehle.

HP-UX-Hosts erhältlich

Sie können die LUN- oder Gerätewarteschlangentiefe auf HP-UX-Hosts mithilfe des Kernel-Parameters ändern `scsi_max_qdepth`. Sie können die HBA-Warteschlangentiefe mit dem Kernel-Parameter ändern `max_fcp_reqs`.

- Der Standardwert für `scsi_max_qdepth` ist 8. Der maximale Wert ist 255.

`scsi_max_qdepth` Kann auf einem laufenden System mit dynamisch verändert werden `-u` Option auf der `kmtune` Befehl. Die Änderung wird für alle Geräte im System wirksam. Verwenden Sie beispielsweise den folgenden Befehl, um die LUN-Warteschlangentiefe auf 64 zu erhöhen:

```
kmtune -u -s scsi_max_qdepth=64
```

Es ist möglich, die Warteschlangentiefe für einzelne Gerätedateien mit dem zu ändern `scsictl` Befehl. Änderungen mithilfe von `scsictl` Der Befehl bleibt beim Neustart des Systems erhalten. Um die Warteschlangentiefe für eine bestimmte Gerätedatei anzuzeigen und zu ändern, führen Sie den folgenden Befehl aus:

```
scsictl -a /dev/rdisk/c2t2d0
```

```
scsictl -m queue_depth=16 /dev/rdisk/c2t2d0
```

- Der Standardwert für `max_fcp_reqs` ist 512. Der maximale Wert ist 1024.

Der Kernel muss neu aufgebaut werden und das System muss neu gestartet werden, um Änderungen an vornehmen zu können `max_fcp_reqs` Um wirksam zu werden. Verwenden Sie zum Ändern der HBA-Warteschlangentiefe in 256 beispielsweise den folgenden Befehl:

```
kmtune -u -s max_fcp_reqs=256
```

Solaris-Hosts

Sie können die LUN- und HBA-Warteschlangentiefe für Ihre Solaris-Hosts einstellen.

- Für LUN-Warteschlangentiefe: Die Anzahl der auf einem Host verwendeten LUNs muss mit dem pro-LUN-Gashebel (`lun-Queue-Tiefe`) kleiner oder gleich dem Wert für die `tgt-queue-Tiefe` auf dem Host sein.
- Für die Warteschlangentiefe in einem Sun-Stack: Die nativen Treiber ermöglichen nicht pro LUN oder Ziel `max_throttle` Einstellungen auf HBA-Ebene. Die empfohlene Methode zum Einstellen des `max_throttle` Der Wert für native Treiber befindet sich auf der Ebene des Typs pro Gerät (`VID_PID`) im `/kernel/drv/sd.conf` Und `/kernel/drv/ssd.conf` Dateien: Das Host-Dienstprogramm setzt diesen Wert auf 64 für MPxIO-Konfigurationen und 8 für Veritas DMP-Konfigurationen.

Schritte

1. # cd/kernel/drv
2. # vi lpfc.conf
3. Suche nach /tft-queue (/tgt-queue)

```
tgt-queue-depth=32
```



Der Standardwert ist bei der Installation auf 32 gesetzt.

4. Legen Sie den gewünschten Wert basierend auf der Konfiguration Ihrer Umgebung fest.
5. Speichern Sie die Datei.
6. Starten Sie den Host mithilfe des neu `sync; sync; sync; reboot -- -r` Befehl.

VMware Hosts für einen QLogic HBA

Verwenden Sie die `esxcfg-module` Befehl zum Ändern der HBA-Zeitüberschreitungseinstellungen. Manuelles Aktualisieren des `esx.conf` Datei wird nicht empfohlen.

Schritte

1. Melden Sie sich als Root-Benutzer an der Service-Konsole an.
2. Verwenden Sie die `#vmkload_mod -l` Befehl zur Überprüfung, welches Qlogic HBA-Modul derzeit geladen ist.
3. Führen Sie für eine einzelne Instanz eines Qlogic HBA den folgenden Befehl aus:

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```



Dieses Beispiel verwendet das Modul `qla2300_707`. Verwenden Sie das entsprechende Modul basierend auf der Ausgabe von `vmkload_mod -l`.

4. Speichern Sie Ihre Änderungen mit dem folgenden Befehl:

```
#!/usr/sbin/esxcfg-boot -b
```

5. Starten Sie den Server mit folgendem Befehl neu:

```
#reboot
```

6. Bestätigen Sie die Änderungen mit folgenden Befehlen:

a. `#esxcfg-module -g qla2300_707`

b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware-Hosts für einen Emulex HBA

Verwenden Sie die `esxcfg-module` Befehl zum Ändern der HBA-Zeitüberschreitungseinstellungen. Manuelles Aktualisieren des `esx.conf` Datei wird nicht empfohlen.

Schritte

1. Melden Sie sich als Root-Benutzer an der Service-Konsole an.

2. Verwenden Sie die `#vmkload_mod -l grep lpfc` Befehl zur Überprüfung, welcher Emulex HBA aktuell geladen ist.
3. Geben Sie für eine einzelne Instanz eines Emulex HBA den folgenden Befehl ein:

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```



Je nach HBA-Modell kann das Modul entweder `lpfcdd_7xx` oder `lpfcdd_732` sein. Der obige Befehl verwendet das `lpfcdd_7xx`-Modul. Sie sollten das entsprechende Modul basierend auf dem Ergebnis von `verwenden vmkload_mod -l`.

Durch Ausführen dieses Befehls wird die LUN-Warteschlangentiefe auf 16 für den HBA festgelegt, der von `lpfc0` dargestellt wird.

4. Führen Sie für mehrere Instanzen eines Emulex HBA den folgenden Befehl aus:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

Die LUN-Warteschlangentiefe für `lpfc0` und die LUN-Warteschlangentiefe für `lpfc1` ist auf 16 festgelegt.

5. Geben Sie den folgenden Befehl ein:

```
#esxcfg-boot -b
```

6. Booten Sie mit neu `#reboot`.

Windows Hosts für einen Emulex HBA

Auf Windows-Hosts können Sie das verwendete `LPUTILNT` Dienstprogramm zur Aktualisierung der Warteschlangentiefe für Emulex-HBAs.

Schritte

1. Führen Sie die aus `LPUTILNT` Dienstprogramm befindet sich im `C:\WINNT\system32` Verzeichnis.
2. Wählen Sie im Menü auf der rechten Seite die Option **Drive Parameters** aus.
3. Scrollen Sie nach unten und doppelklicken Sie auf **QueueDepth**.



Wenn Sie **QueueDepth** größer als 150 einstellen, muss auch der folgende Wert für die Windows-Registrierung entsprechend erhöht werden:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnids\Parameters\Device\NumberOfRequests
```

Windows Hosts für einen Qlogic HBA

Auf Windows-Hosts können Sie das und verwenden `SANsurfer HBA Manager Utility` zum Aktualisieren der Queue Depths für Qlogic HBAs.

Schritte

1. Führen Sie die aus `SANsurfer HBA Manager Utility`:
2. Klicken Sie auf **HBA-Port > Einstellungen**.

3. Klicken Sie im Listenfeld auf **Erweiterte HBA-Porteinstellungen**.

4. Aktualisieren Sie die `Execution Throttle` Parameter.

Linux Hosts für Emulex HBA

Sie können die Warteschlangentiefe eines Emulex HBA auf einem Linux-Host aktualisieren. Damit die Updates bei einem Neustart erhalten bleiben, müssen Sie dann ein neues RAM-Laufwerk-Image erstellen und den Host neu starten.

Schritte

1. Geben Sie die zu ändernden Warteschlangentiefe an:

```
modinfo lpfc|grep queue_depth
```

Die Liste der Parameter für die Warteschlangentiefe mit ihrer Beschreibung wird angezeigt. Je nach Betriebssystemversion können Sie einen oder mehrere der folgenden Parameter für die Warteschlangentiefe ändern:

- `lpfc_lun_queue_depth`: Maximale Anzahl von FC-Befehlen, die an eine bestimmte LUN in Warteschlange gestellt werden können (uint)
- `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. Aktualisieren Sie die Warteschlangentiefe, indem Sie dem die Parameter für die Warteschlangentiefe hinzufügen `/etc/modprobe.conf` Datei für ein Red hat Enterprise Linux 5.x-System und zum `/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.

Abhängig von Ihrer Betriebssystemversion können Sie einen oder mehrere der folgenden Befehle hinzufügen:

- `options lpfc lpfc_hba_queue_depth=new_queue_depth`
- `options lpfc lpfc_lun_queue_depth=new_queue_depth`
- `options lpfc lpfc_tgt_queue_depth=new_queue_depth`

3. Erstellen Sie ein neues RAM-Laufwerk-Image, und starten Sie dann den Host neu, damit die Updates bei einem Neustart erhalten bleiben.

Weitere Informationen finden Sie im ["Systemadministration"](#) Für Ihre Linux-Version.

4. Vergewissern Sie sich, dass die Werte für die Warteschlangentiefe für jeden Parameter aktualisiert werden, den Sie geändert haben:

```
root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```

Der aktuelle Wert der Warteschlangentiefe wird angezeigt.

Linux Hosts für QLogic HBA

Sie können die Tiefe der Gerätewarteschlange eines QLogic-Treibers auf einem Linux-Host aktualisieren. Damit die Updates bei einem Neustart erhalten bleiben, müssen Sie dann ein neues RAM-Laufwerk-Image erstellen und den Host neu starten. Mithilfe der QLogic HBA Management-GUI oder der Befehlszeilenschnittstelle (CLI) lässt sich die QLogic HBA-Warteschlangentiefe ändern.

Diese Aufgabe zeigt, wie die QLogic HBA CLI zum Ändern der QLogic HBA-Warteschlangentiefe verwendet wird

Schritte

1. Geben Sie den Parameter für die Warteschlangentiefe des Geräts an, der geändert werden soll:

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

Sie können nur die ändern `ql2xmaxqdepth` Parameter für die Warteschlangentiefe, der die maximale Warteschlangentiefe angibt, die für jede LUN festgelegt werden kann. Der Standardwert ist 64 für RHEL 7.5 und höher. Der Standardwert ist 32 für RHEL 7.4 und früher.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:          ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Wert für die Tiefe der Gerätewarteschlange aktualisieren:

- Wenn Sie die Änderungen persistent machen möchten, führen Sie die folgenden Schritte aus:
 - i. Aktualisieren Sie die Warteschlangentiefe, indem Sie dem den Parameter Warteschlangentiefe hinzufügen `/etc/modprobe.conf` Datei für ein Red hat Enterprise Linux 5.x-System und zum `/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: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
 - ii. Erstellen Sie ein neues RAM-Laufwerk-Image, und starten Sie dann den Host neu, damit die Updates bei einem Neustart erhalten bleiben.

Weitere Informationen finden Sie im ["Systemadministration"](#) Für Ihre Linux-Version.

- Wenn Sie den Parameter nur für die aktuelle Sitzung ändern möchten, führen Sie den folgenden Befehl aus:

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Im folgenden Beispiel wird die Warteschlangentiefe auf 128 gesetzt.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Überprüfen Sie, ob die Werte für die Warteschlangentiefe aktualisiert wurden:

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Der aktuelle Wert der Warteschlangentiefe wird angezeigt.

4. Ändern Sie die QLogic HBA-Warteschlangentiefe durch Aktualisieren des Firmware-Parameters Execution Throttle Über das QLogic HBA BIOS.

a. Melden Sie sich bei der QLogic HBA Management CLI an:

```
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
```

b. Wählen Sie im Hauptmenü die aus Adapter Configuration Option.

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qauccli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

          CLI - Version 2.2.0 (Build 15)

Main Menu

1:  Adapter Information
**2:  Adapter Configuration**
3:  Adapter Updates
4:  Adapter Diagnostics
5:  Monitoring
6:  FabricCache CLI
7:  Refresh
8:  Help
9:  Exit

Please Enter Selection: 2
```

c. Wählen Sie aus der Liste der Adapterkonfigurationsparameter die aus HBA Parameters Option.

```

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 (iidDMA)
8:  Export (Save) Configuration
9:  Generate Reports
10:  Personality
11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 3

```

d. Wählen Sie aus der Liste der HBA-Ports den erforderlichen HBA-Port aus.

```

Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510
  1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
  2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
HBA Model QLE2672 SN: RFE1241G81915
  3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
  4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
Please Enter Selection: 1

```

Die Details des HBA-Ports werden angezeigt.

e. Wählen Sie im Menü HBA-Parameter den aus Display HBA Parameters Option zum Anzeigen des aktuellen Werts des Execution Throttle Option.

Der Standardwert des Execution Throttle Option ist 65535.

```

HBA Parameters Menu

=====
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02

```

```
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
```

```
=====
```

- 1: Display HBA Parameters
- 2: Configure HBA Parameters
- 3: Restore Defaults

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
Please Enter Selection: 1

```
-----
```

```
-----
```

```
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```
-----
```

```
-----
```

```
Connection Options          : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                   : Auto
Frame Size                  : 2048
Hard Loop ID                : 0
Loop Reset Delay (seconds)  : 5
Enable Host HBA BIOS        : Enabled
Enable Hard Loop ID         : Disabled
Enable FC Tape Support      : Enabled
Operation Mode              : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us) : 0
**Execution Throttle       : 65535**
Login Retry Count           : 8
Port Down Retry Count       : 30
Enable LIP Full Login       : Enabled
Link Down Timeout (seconds) : 30
Enable Target Reset         : Enabled
LUNs Per Target             : 128
Out Of Order Frame Assembly : Disabled
Enable LR Ext. Credits      : Disabled
Enable Fabric Assigned WWN  : N/A
```

Press <Enter> to continue:

- a. Drücken Sie **Enter**, um fortzufahren.
- b. Wählen Sie im Menü HBA-Parameter den aus Configure HBA Parameters Option zum Ändern der HBA-Parameter.

- c. Wählen Sie im Menü Parameter konfigurieren die Option `Execute Throttle Option` 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. Drücken Sie **Enter**, um fortzufahren.

- e. Wählen Sie im Menü Parameter konfigurieren die Option `Commit Changes Option` zum Speichern der

Änderungen.

f. Verlassen Sie das Menü.

Copyright-Informationen

Copyright © 2024 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 IRGEND EINER 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.