Referenz zur SAN-Konfiguration

ONTAP 9

NetApp
April 24, 2024

Inhalt

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.

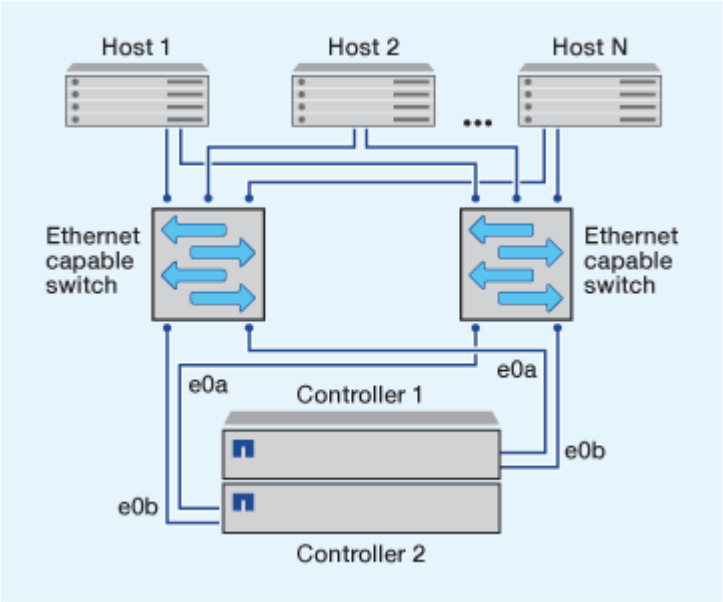
> "Single-Node-Konfigurationen" Die Empfehlungen sind nicht empfehlenswert, da sie nicht die Redundanz bieten, die zur Unterstützung von Fehlertoleranz und unterbrechungsfreiem Betrieb erforderlich ist.

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".

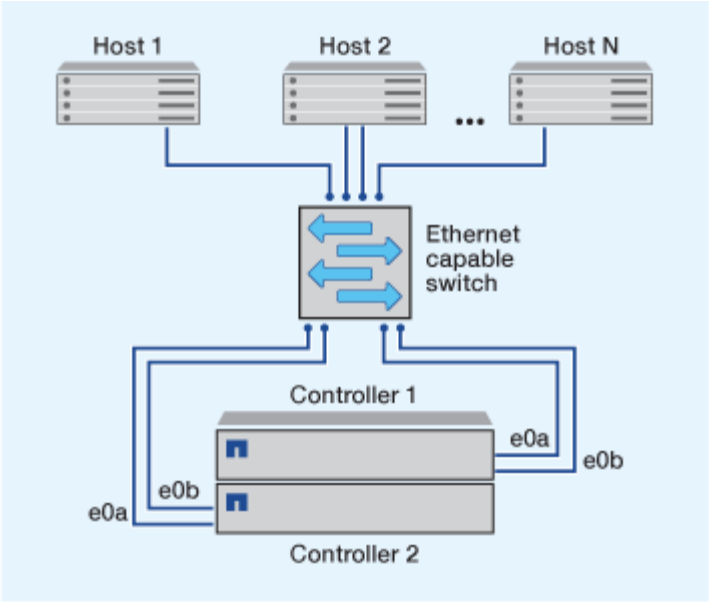
ISCSI-Konfigurationen mit mehreren Netzwerken

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.



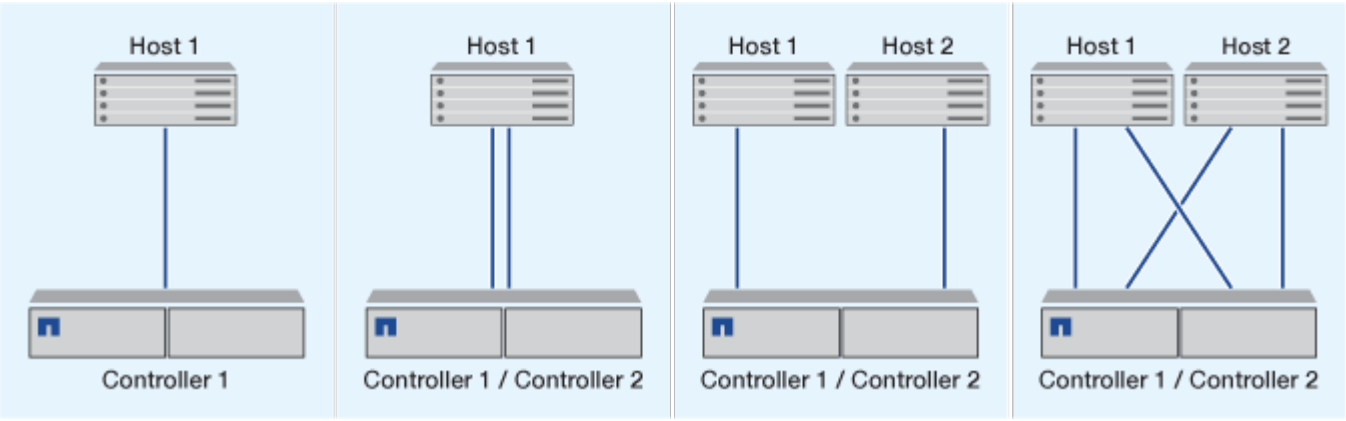
ISCSI-Konfigurationen mit einem Netzwerk

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.

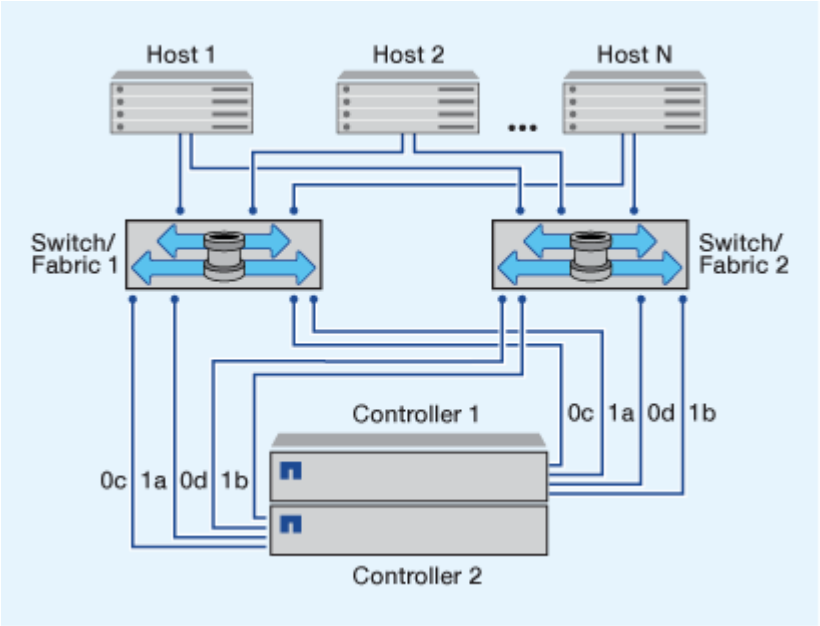
Kaskadierung, partielles Mesh, volles Mesh, Core-Edge und Director Fabrics sind branchenübliche Methoden, FC Switches mit einem Fabric zu verbinden. Alle werden unterstützt. Die Verwendung heterogener FC Switch Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches. Spezielle Ausnahmen 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.

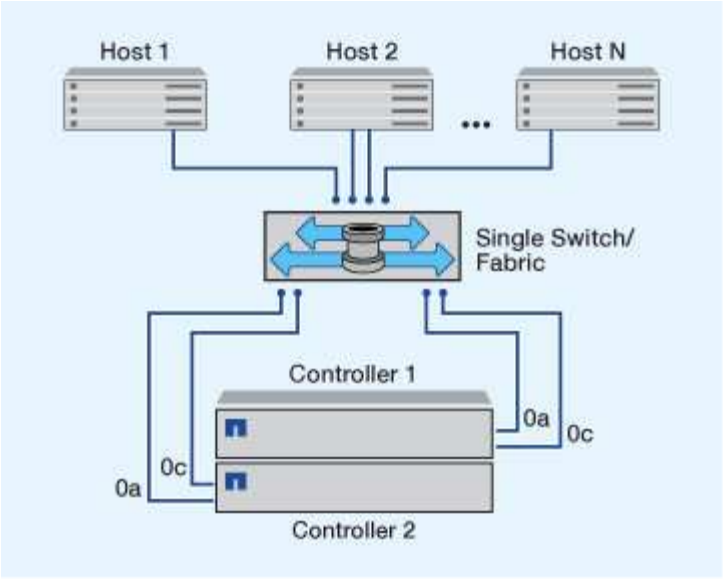


FC- und FC-NVMe-Konfigurationen in einem Fabric

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
• 4 Gb • 2 Gb • 1 Gb	• 8 Gb • 4 Gb • 2 Gb	• 16 Gb • 8 Gb • 4 Gb	• 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

Controller	Port-Paare mit gemeinsam genutztem ASIC	Anzahl der Zielports: Bevorzugte Ports
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-Adaptern

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

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

Befehle zum Verwalten von FC-Zieladaptern

Ihr Ziel ist	Befehl
Zeigt FC-Adapterinformationen auf einem Node an	`network fcp adapter show`
Ändern Sie die FC-Zieladapterparameter	`network fcp adapter modify`
Zeigt Informationen zum FC-Protokoll-Datenverkehr an	`run -node` *`node_name`* `sysstat -f`

Ihr Ziel ist	Befehl
Anzeigen der Dauer des FC-Protokolls	`run -node node_name uptime`
Adapterkonfiguration und -Status anzeigen	`run -node node_name sysconfig -v adapter`
Überprüfen Sie, welche Erweiterungskarten installiert sind und ob Konfigurationsfehler vorliegen	`run -node node_name sysconfig -ac`
Zeigen Sie eine man-Page für einen Befehl an	`man command_name`

Befehle zum Verwalten von FC-Initiator-Adaptern

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

Befehle zum Verwalten der integrierten FC-Adapter

Ihr Ziel ist	Befehl
Zeigt den Status der integrierten FC-Ports an	`system node hardware unified-connect show`

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-Adaptern können auch einzeln als Ziel-Port oder als Initiator-Port konfiguriert werden, genau wie die integrierten FC-Ports. Eine Liste der Adapter, die für den Zielmodus konfiguriert werden können, 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-Adaptern können auch einzeln als Ziel-Port oder als Initiator-Port konfiguriert werden, genau wie die integrierten FC-Ports. Eine Liste der Adapter, die für den Zielmodus konfiguriert werden können, ist im verfügbar "NetApp Hardware Universe".

Bei der Konfiguration von FC-Adaptern für das FC-Protokoll und das FC-NVMe-Protokoll kommen die gleichen Schritte zum Einsatz. Jedoch unterstützen nur bestimmte FC-Adapter FC-NVMe. 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 Zielportgeschwindigkeit 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 node1 -adapter 0c -state up
   ```

6. Versetzen Sie alle LIFs am Adapter in den Online-Modus:

   ```
   network interface modify -vserver * -lif * { -home-node node1 -home-port 0c }
   -status-admin up
   ```

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
                                                          Speed(Mbps) Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...

    net-f8040-34::> ucadmin show
                           Current  Current    Pending  Pending    Admin
    Node          Adapter  Mode     Type       Mode     Type
Status
    ------------  -------  -------  ---------  -------  ---------
-----------
    net-f8040-34-01
                  0e       cna      target     -        -
offline
    net-f8040-34-01
                  0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-port

    vserver lif                   home-port curr-port
    ------- --------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt          e0M       e0M
    net-f8040-34
            m                     e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
```

```
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed to
fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)

    Warning: Are you sure you want to reboot node "net-f8040-34-01"?
    {y|n}: y
```

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 Adaptereinstellungen 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.

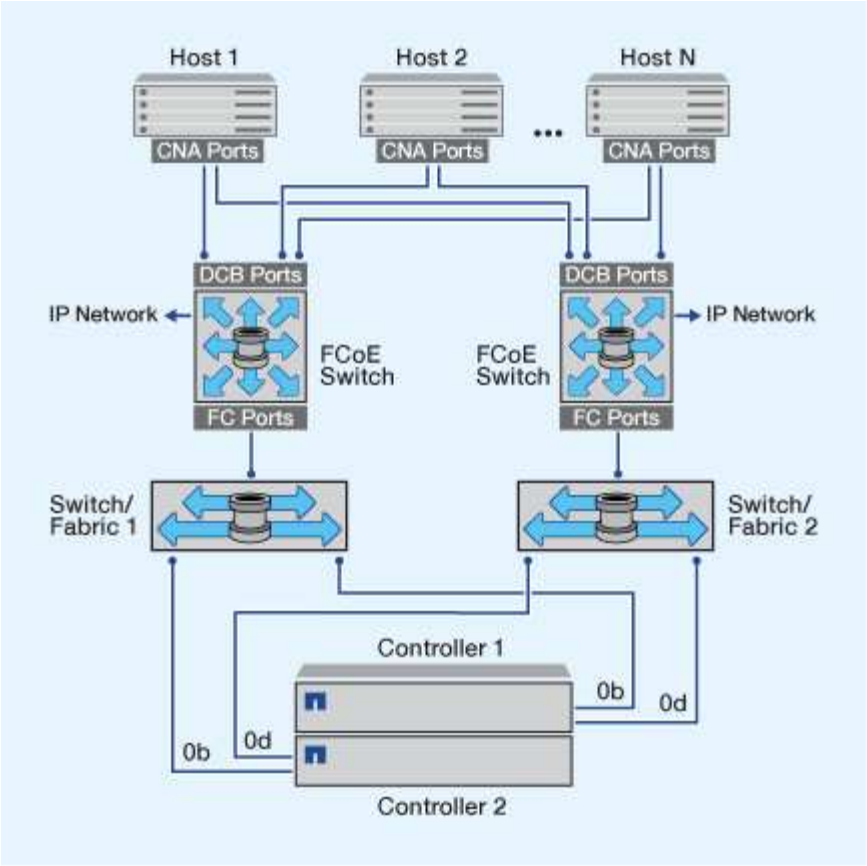
Für FCoE-Konfigurationen sind Ethernet Switches erforderlich, die explizit FCoE-Funktionen unterstützen. FCoE-Konfigurationen werden durch denselben Interoperabilitäts- und Qualitätssicherungsprozess wie FC Switches validiert. Unterstützte Konfigurationen sind in der Interoperabilitäts-Matrix aufgeführt. 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

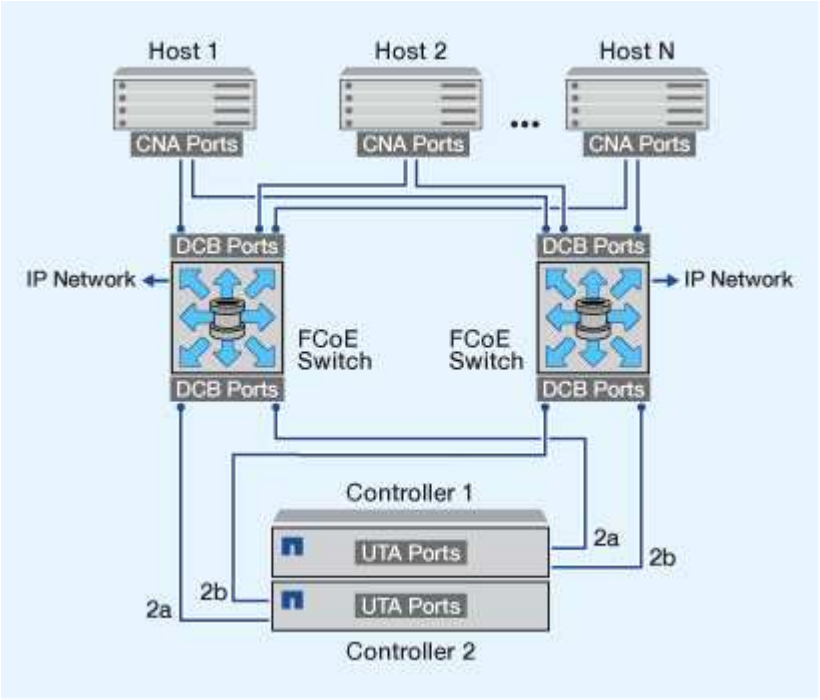
Mit FCoE-Initiatoren (CNAs) können Sie Hosts mit beiden Controllern in einem HA-Paar über FCoE Switches an FC-Ziel-Ports verbinden. Der FCoE-Switch muss auch über FC-Ports verfügen. Der Host FCoE Initiator stellt immer eine Verbindung zum FCoE-Switch her. Der FCoE Switch kann eine direkte Verbindung 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:



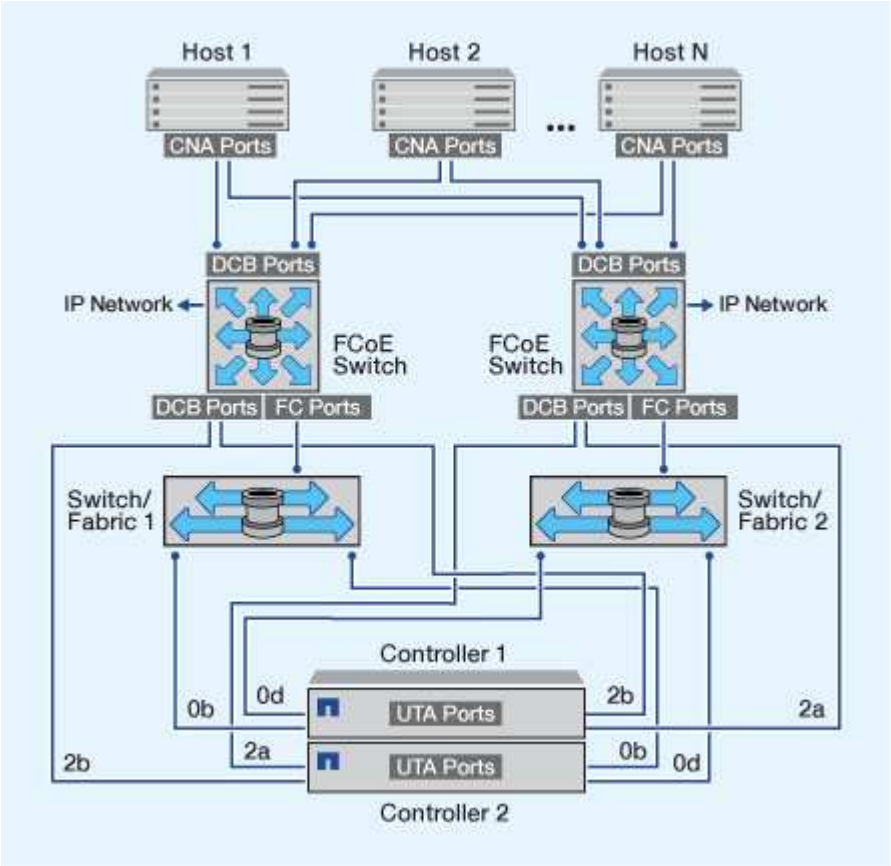
FCoE-Initiator zu FCoE Target

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.



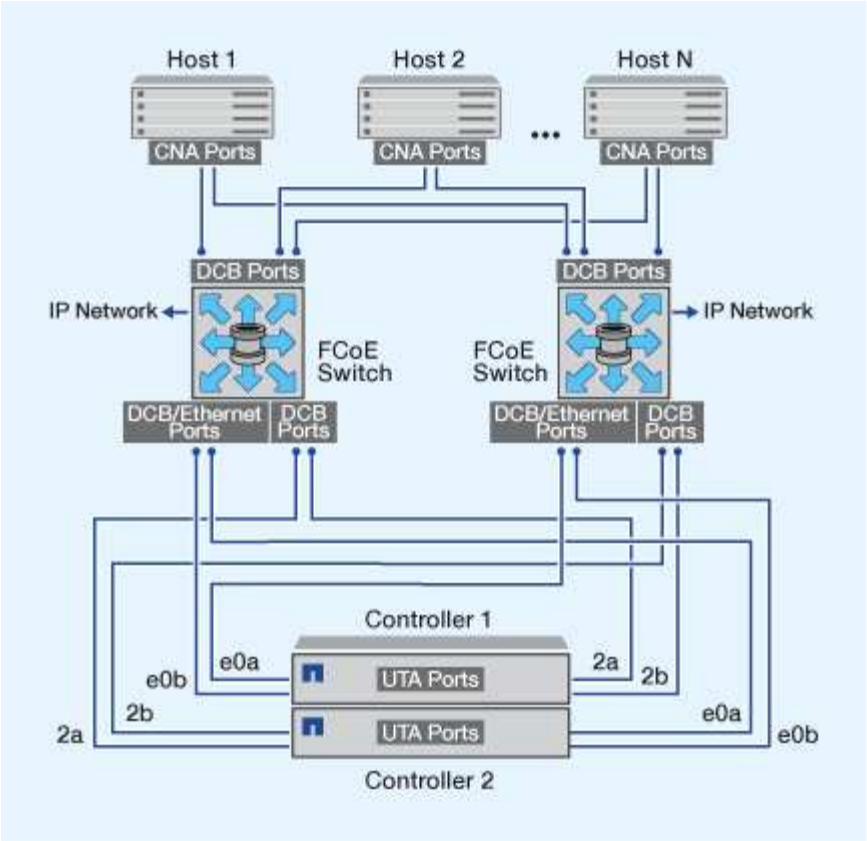
FCoE-Initiator auf FCoE- und FC-Ziele

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.
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.

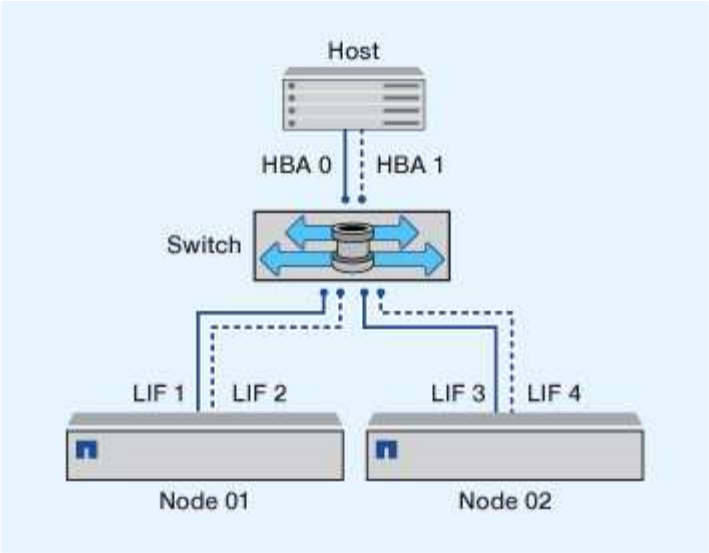
Single-Fabric-Konfigurationen werden unterstützt, jedoch nicht als hochverfügbar angesehen. Der Ausfall einer einzelnen Komponente kann zum Verlust des Zugriffs auf Daten führen.

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.

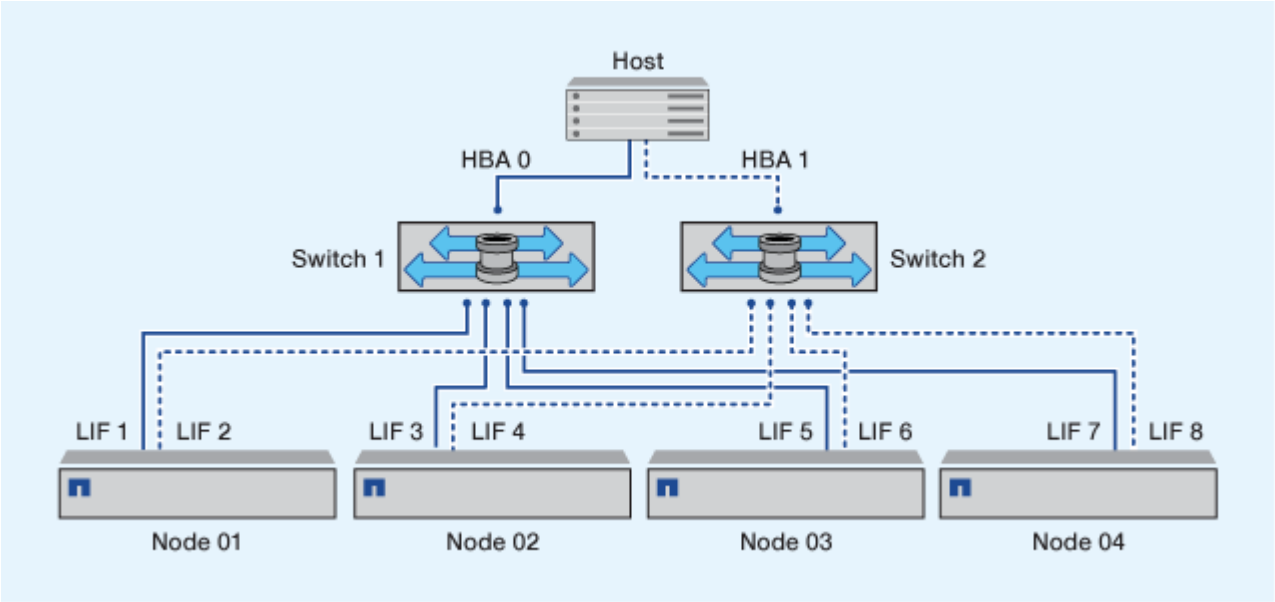
- Zone 1: HBA 0, LIF_1, LIF_3, LIF_5 und LIF_7
- Zone 2: HBA 1, LIF_2, LIF_4, LIF_6 und LIF_8

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 1. Schritte

Cisco Switch

1. Stellen Sie eine Verbindung zum Switch her, und melden Sie sich an.
2. Konfigurationsmodus aufrufen:

```
switch# config t
switch(config)#
```

3. Überschreiben Sie den ersten Geräteeintrag in der Namensserver-Datenbank mit dem neuen Gerät:

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. Vergewissern Sie sich bei Switches, die NX-OS 8.x ausführen, dass das flogi-Timeout auf Null gesetzt ist:

   a. Anzeige des Zeitschaltuftzeitschaltufschaltudes:

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. Wenn die Ausgabe im vorherigen Schritt nicht angibt, dass der Zeitwert Null ist, setzen Sie ihn auf null:

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Brocade Switch

1. Stellen Sie eine Verbindung zum Switch her, und melden Sie sich an.
2. Geben Sie 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

"NetApp Hardware Universe"

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 IT-Ns 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-Zielports begrenzt.

Über diese Aufgabe

„Queue depth“ ist die Anzahl von I/O-Anfragen (SCSI-Befehle), die sich gleichzeitig in ein Storage Controller Warteschlange einreihen lassen. Jede I/O-Anforderung vom Initiator-HBA des Hosts zum Zieladapter des Storage-Controllers verbraucht einen Warteschlangeneintrag. Eine höhere Warteschlangentiefe entspricht in der Regel einer besseren Performance. Wenn jedoch die maximale Warteschlangentiefe des Storage Controllers erreicht wird, weist dieser Storage-Controller eingehende Befehle zurück, indem er eine QFULL-Antwort zurückgibt. Wenn eine große Anzahl von Hosts auf einen Speicher-Controller zugreifen, sollten Sie sorgfältig planen, QFULL-Bedingungen zu vermeiden, die die Systemleistung erheblich beeinträchtigen und zu Fehlern bei einigen Systemen führen können.

In einer Konfiguration mit mehreren Initiatoren (Hosts) sollten alle Hosts über ähnliche Warteschlangentiefen verfügen. Aufgrund der Ungleichheit in der Warteschlangentiefe zwischen Hosts, die über denselben Zielport mit dem Storage Controller verbunden sind, wird Hosts mit kleineren Warteschlangentiefen dem Zugriff auf Ressourcen durch Hosts mit größeren Warteschlangentiefen entzogen.

Die folgenden allgemeinen Empfehlungen bezüglich „`Tuning`“-Warteschlangentiefe:

- Verwenden Sie für kleine und mittelgroße Systeme eine HBA-Warteschlangenlänge von 32.
- Verwenden Sie für große Systeme eine HBA-Warteschlangenlänge von 128.
- Verwenden Sie für Ausnahmefälle oder Performance-Tests eine Warteschlangentiefe von 256, um mögliche Warteschlangenprobleme zu vermeiden.
- Für alle Hosts sollten die Warteschlangentiefen auf ähnliche Werte festgelegt sein, um allen Hosts gleichberechtigten Zugriff zu gewähren.
- Um Performance-Einbußen oder Fehler zu vermeiden, darf die Ziel-FC-Port-Warteschlangentiefe des Storage Controllers nicht überschritten werden.

Schritte

1. Zählen Sie die Gesamtzahl der FC-Initiatoren auf allen Hosts, die mit einem FC-Zielport verbunden sind.
2. Mit 128 multiplizieren.
   - Wenn das Ergebnis unter 2,048 liegt, setzen Sie die Warteschlangentiefe für alle Initiatoren auf 128. Sie haben 15 Hosts, wobei ein Initiator mit jedem der zwei Ziel-Ports auf dem Storage Controller verbunden ist. 15 × 128 = 1,920. Da 1,920 kleiner als das gesamte Warteschlangentiefe von 2,048 ist, können Sie die Warteschlangentiefe für alle Initiatoren auf 128 einstellen.
   - Wenn das Ergebnis größer als 2,048 ist, mit Schritt 3 fortfahren. Sie haben 30 Hosts, wobei ein Initiator mit jedem der zwei Ziel-Ports auf dem Storage Controller verbunden ist. 30 × 128 = 3,840. Da 3,840 die Gesamttiefe der Warteschlange von 2,048 überschreitet, sollten Sie eine der Optionen unter Schritt 3 zur Behebung wählen.
3. Wählen Sie eine der folgenden Optionen, um dem Storage Controller mehr Hosts hinzuzufügen.
   - Option 1:
     i. Weitere FC-Ziel-Ports hinzufügen.
     ii. Neuverteilung Ihrer FC-Initiatoren
     iii. Wiederholen Sie die Schritte 1 und 2. + die gewünschte Warteschlangentiefe von 3,840 überschreitet die verfügbare Warteschlangentiefe pro Port. Um dies zu beheben, können Sie jedem Controller einen FC-Zieladapter mit zwei Ports hinzufügen und Ihre FC-Switches neu Zone festlegen, so dass 15 Ihrer 30 Hosts mit einem Satz Ports verbunden werden. Die restlichen 15 Hosts verbinden sich mit einem zweiten Port-Satz. Die Warteschlangentiefe pro Port wird dann auf 15 × 128 = 1,920 reduziert.
   - Option 2:

i. Weisen Sie jeden Host basierend auf seinem erwarteten I/O-Bedarf als „`large`“ oder „`small`“ zu.

ii. Multiplizieren Sie die Anzahl der großen Initiatoren mit 128.

iii. Multiplizieren Sie die Anzahl der kleinen Initiatoren mit 32.

iv. Fügen Sie die beiden Ergebnisse zusammen.

v. Wenn das Ergebnis weniger als 2,048 ist, stellen Sie die Warteschlangentiefe für große Hosts auf 128 und die Warteschlangentiefe für kleine Hosts auf 32 ein.

vi. Wenn das Ergebnis immer noch größer als 2,048 pro Port ist, reduzieren Sie die Warteschlangentiefe pro Initiator, bis die gesamte Warteschlangentiefe kleiner als oder gleich 2,048 ist.

> Um die Warteschlangentiefe zu schätzen, die für einen bestimmten I/O-Durchsatz pro Sekunde erforderlich ist, verwenden Sie folgende Formel:
>
> Benötigte Queue-Tiefe = (Anzahl I/O pro Sekunde) × (Reaktionszeit)
>
> Wenn Sie beispielsweise 40,000 I/O pro Sekunde mit einer Reaktionszeit von 3 Millisekunden benötigen, dann ist die benötigte Warteschlangentiefe = 40,000 × (.003) = 120.

Die maximale Anzahl von Hosts, die Sie mit einem Zielport verbinden können, ist 64, wenn Sie sich entscheiden, die Warteschlangentiefe auf die grundlegende Empfehlung von 32 zu begrenzen. Wenn Sie sich jedoch für eine Warteschlangentiefe von 128 entscheiden, können maximal 16 Hosts mit einem Zielport verbunden sein. Je größer die Warteschlangentiefe, desto weniger Hosts, die ein einziger Zielport unterstützen kann. Wenn Sie eine solche Anforderung haben, dass Sie keine Kompromisse in der Warteschlangentiefe machen können, sollten Sie mehr Zielports erhalten.

Die gewünschte Warteschlangentiefe von 3,840 überschreitet die verfügbare Warteschlangentiefe pro Port. Es gibt 10 „`große`“ Hosts mit hohen Storage-I/O-Anforderungen und 20 „`skleine`“ Hosts mit niedrigen I/O-Anforderungen. Setzen Sie die Tiefe der Initiator-Warteschlange auf den großen Hosts auf 128 und die Tiefe der Initiator-Warteschlange auf den kleinen Hosts auf 32.

Ihre resultierende Gesamtwarteschlangentiefe beträgt (10 × 128) + (20 × 32) = 1,920.

Sie können die verfügbare Warteschlangentiefe gleichmäßig auf jeden Initiator verteilen.

Ihre resultierende Warteschlangentiefe pro Initiator beträgt 2,048 ÷ 30 = 68.

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/rdsk/c2t2d0
  ```

  ```
  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- Der Standardwert für `max_fcp_reqs` Ist 512. Der maximale Wert ist 1024.

  Der Kernel muss neu aufgebaut werden und das System muss neu gestartet werden, 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 verwenden `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\lpxnds\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` Der 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_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/qaucli
      ```

   b. Wählen Sie im Hauptmenü die aus `Adapter Configuration` Option.

      ```
      [root@localhost ~]#
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
      Using config file:
      /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
      Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
      Working dir: /root

      QConvergeConsole

              CLI - Version 2.2.0 (Build 15)

          Main Menu

          1:  Adapter Information
          **2:  Adapter Configuration**
          3:  Adapter Updates
          4:  Adapter Diagnostics
          5:  Monitoring
          6:  FabricCache CLI
          7:  Refresh
          8:  Help
          9:  Exit


              Please Enter Selection: 2
      ```

c. Wählen Sie 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 (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Wählen Sie aus der Liste der HBA-Ports den erforderlichen HBA-Port aus.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

Die Details des HBA-Ports werden angezeigt.

e. Wählen Sie im Menü HBA-Parameter 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.