SAN Konfigurationsreferenz

ONTAP 9

NetApp
November 10, 2026

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

Inhalt

SAN Konfigurationsreferenz . . . 1
Erfahren Sie mehr über die ONTAP SAN-Konfiguration . . . 1
iSCSI Konfigurationen . . . 1
iSCSI Netzwerkkonfigurationen für ONTAP Systeme . . . 1
Vorteile der Verwendung von VLANs mit ONTAP Systemen in iSCSI-Konfigurationen . . . 3
FC Konfigurationen . . . 4
FC- und FC-NVMe Fabric- sowie Direct-Attach-Konfigurationen für ONTAP . . . 4
Best Practices für die FC-Fabric-Konfiguration von ONTAP Systemen . . . 7
Unterstützte FC-Zielportgeschwindigkeiten für Ihr ONTAP System ermitteln . . . 8
Vermeidung von Verbindungsverlusten mit einem X1133A-R6 Adapter auf ONTAP Systemen . . . 9
FCoE Konfigurationen . . . 9
FCoE-Fabric-Konfigurationen für ONTAP Systeme . . . 9
ONTAP unterstützte FCoE Initiator- und Zielportkombinationen . . . 12
FC- und FCoE-Zonierung . . . 13
Informationen zu FC- und FCoE-Zoning mit ONTAP Systemen . . . 13
Empfohlene FC- und FCoE-Zoning-Konfigurationen für ONTAP Systeme . . . 14
Anforderungen an SAN-Hosts, die mit ONTAP und Nicht-NetApp-Systemen verbunden sind . . . 17
SAN-Konfigurationen in einer MetroCluster Umgebung . . . 17
Unterstützte SAN-Konfigurationen in einer ONTAP MetroCluster Umgebung . . . 17
Portüberschneidungen während ONTAP MetroCluster Switchover und Switchback vermeiden . . . 18
ONTAP Unterstützung für SAN Host Multipathing . . . 19
Empfohlene Anzahl von Pfaden vom Host zu den Knoten im Cluster . . . 20
Konfigurationsgrenzen . . . 21
Maximal unterstützte Knoten und SAN-Hosts pro ONTAP Cluster bestimmen . . . 21
ONTAP ASA Konfigurationsgrenzen und Unterstützung . . . 22
Konfigurationsgrenzen für FC-Switches, die mit ONTAP Systemen verwendet werden . . . 24
Maximale Anzahl an unterstützten FC- und FCoE-Hops in ONTAP . . . 24
Warteschlangentiefe für ONTAP FC Hosts berechnen . . . 25
Warteschlangentiefen für ONTAP SAN Hosts anpassen . . . 27

SAN Konfigurationsreferenz

Erfahren Sie mehr über die ONTAP SAN-Konfiguration

Ein storage area network (SAN) besteht aus einer Speicherlösung, die über ein SAN-Transportprotokoll wie iSCSI oder FC mit Hosts verbunden ist. Sie können Ihr SAN so konfigurieren, dass Ihre Speicherlösung über einen oder mehrere Switches mit Ihren Hosts verbunden wird. Wenn Sie iSCSI verwenden, können Sie Ihr SAN auch so konfigurieren, dass Ihre Speicherlösung direkt mit Ihrem Host verbunden wird, ohne einen Switch zu verwenden.

In einem SAN können mehrere Hosts mit unterschiedlichen Betriebssystemen wie Windows, Linux oder UNIX gleichzeitig auf die Speicherlösung zugreifen. Es können "Selektive LUN Zuordnung" und "Portsets" verwendet werden, um den Datenzugriff zwischen den Hosts und dem Speicher zu begrenzen.

Bei iSCSI wird die Netzwerktopologie zwischen der Speicherlösung und den Hosts als Netzwerk bezeichnet. Bei FC, FC/NVMe und FCoE wird die Netzwerktopologie zwischen der Speicherlösung und den Hosts als Fabric bezeichnet. Zur Schaffung von Redundanz, die vor dem Verlust des Datenzugriffs schützt, empfiehlt sich die Einrichtung des SAN mit HA-Paaren in einer Multi-Netzwerk- oder Multi-Fabric-Konfiguration. Konfigurationen mit einzelnen Knoten oder einzelnen Netzwerken/Fabrics sind nicht vollständig redundant und daher nicht empfehlenswert.

Nachdem Ihr SAN konfiguriert ist, können Sie "Speicher für iSCSI oder FC bereitstellen" oder "Storage für FC/NVMe bereitstellen". Anschließend ist eine Verbindung zu Ihren Hosts möglich, um mit der Datenverarbeitung zu beginnen.

Die Unterstützung des SAN-Protokolls variiert je nach Ihrer ONTAP Version, Ihrer Plattform und Ihrer Konfiguration. Details zu Ihrer spezifischen Konfiguration sind in der "NetApp Interoperabilitätsmatrix-Tool" zu finden.

Verwandte Informationen

- "SAN-Administration Übersicht"
- "NVMe Konfiguration, Unterstützung und Einschränkungen"

iSCSI Konfigurationen

iSCSI Netzwerkkonfigurationen für ONTAP Systeme

Die iSCSI-Konfiguration sollte mit Hochverfügbarkeitspaaren (HA) eingerichtet werden, die entweder direkt an die iSCSI-SAN-Hosts angeschlossen sind oder über einen oder mehrere IP-Switches mit den Hosts verbunden werden.

"HA-Paare"sind als Meldeknoten für die Active/Optimized- und die Active/Unoptimized-Pfade definiert, die von den Hosts für den Zugriff auf die LUNs verwendet werden. Mehrere Hosts mit unterschiedlichen Betriebssystemen wie Windows, Linux oder UNIX können gleichzeitig auf den Storage zugreifen. Für Hosts ist eine unterstützte Multipathing-Lösung erforderlich, die ALUA unterstützt und konfiguriert ist. Unterstützte Betriebssysteme und Multipathing-Lösungen können auf der "NetApp Interoperabilitätsmatrix-Tool" überprüft werden.

In einer Multi-Network-Konfiguration verbinden zwei oder mehr Switches die Hosts mit dem Speichersystem.

Multi-Network-Konfigurationen werden empfohlen, da sie vollständig redundant sind. In einer Single-Network-Konfiguration verbindet ein Switch die Hosts mit dem Speichersystem. Single-Network-Konfigurationen sind nicht vollständig redundant.

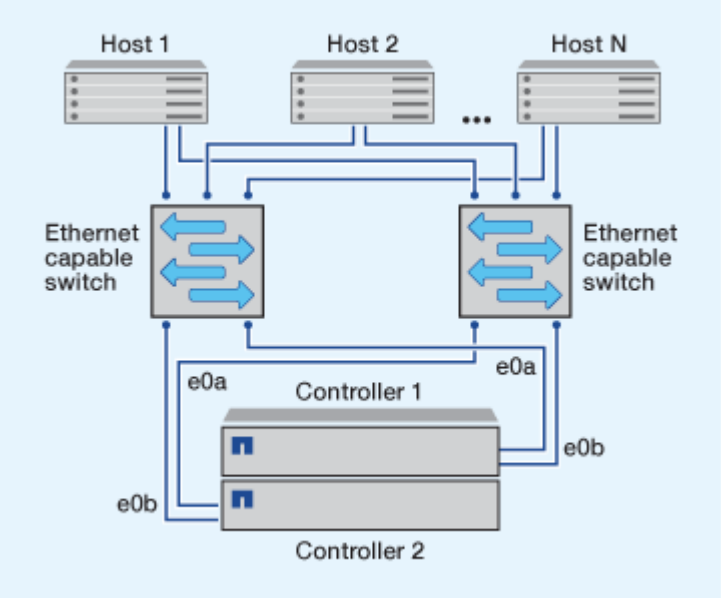
"Single-Node Konfigurationen" werden nicht empfohlen, da sie nicht die Redundanz bieten, die für Fehlertoleranz und unterbrechungsfreien Betrieb erforderlich ist.

Verwandte Informationen

- Erfahren Sie, wie "Selektives LUN Mapping (SLM)" die Pfade eingeschränkt werden, die für den Zugriff auf die LUNs eines HA-Paares verwendet werden.
- Informationen dazu "SAN-LIFs".
- Informationen zu "Vorteile von VLANs in iSCSI".

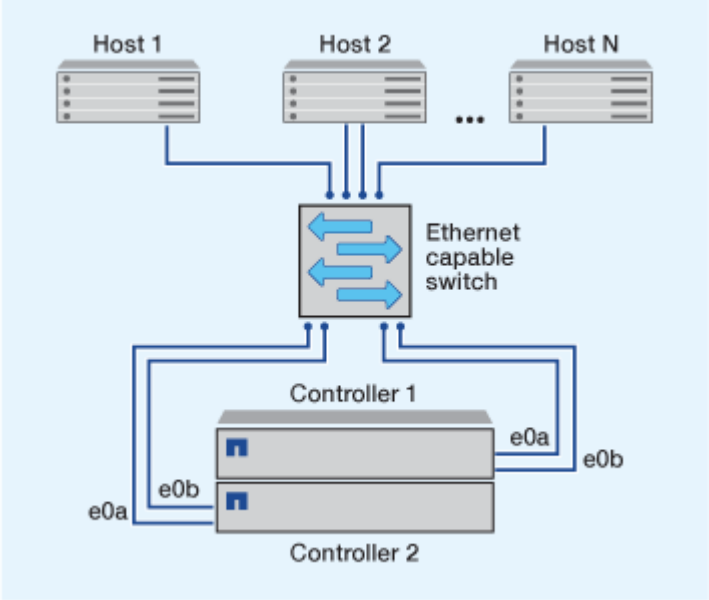
Multi-Network iSCSI Konfigurationen

In Multi-Netzwerk-HA-Paar-Konfigurationen verbinden zwei oder mehr Switches das HA-Paar mit einem oder mehreren Hosts. Da mehrere Switches vorhanden sind, ist diese Konfiguration vollständig redundant.



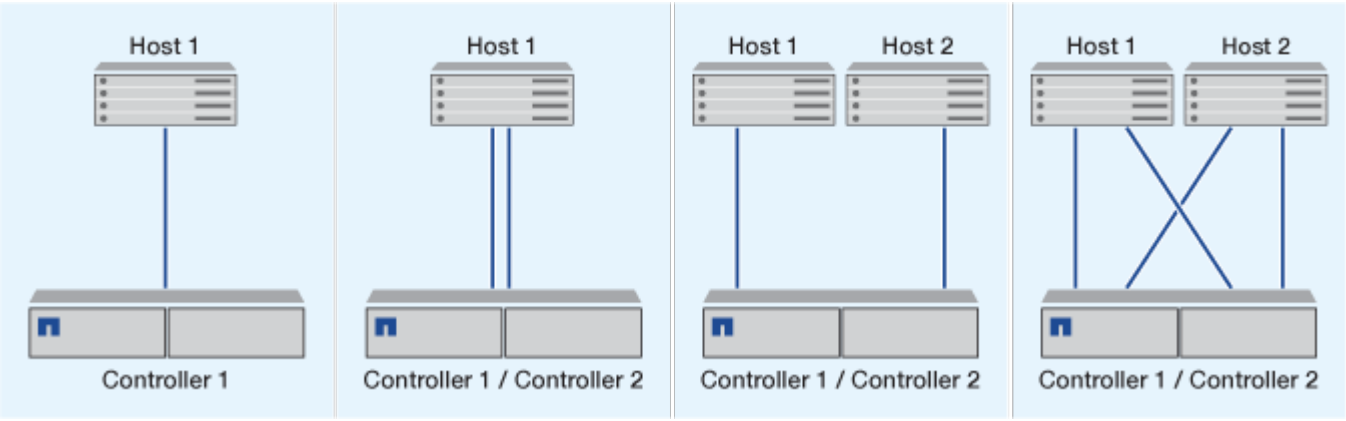
iSCSI-Konfigurationen für ein einzelnes Netzwerk

Bei HA-Paarkonfigurationen mit einem einzigen Netzwerk verbindet ein Switch das HA-Paar mit einem oder mehreren Hosts. Da nur ein einziger Switch verwendet wird, ist diese Konfiguration nicht vollständig redundant.



Direct-Attachment iSCSI Konfiguration

In einer direkt angeschlossenen Konfiguration sind ein oder mehrere Hosts direkt mit den Controllern verbunden.



Vorteile der Verwendung von VLANs mit ONTAP Systemen in iSCSI-Konfigurationen

Ein VLAN besteht aus einer Gruppe von Switch-Ports, die in einer Broadcast-Domäne zusammengefasst sind. Ein VLAN kann sich auf einem einzelnen Switch befinden oder mehrere Switch-Gehäuse umfassen. Statische und dynamische VLANs erhöhen die Sicherheit, isolieren Probleme und begrenzen die verfügbaren Pfade innerhalb Ihrer IP-Netzwerkinfrastruktur.

Bei der Implementierung von VLANs in großen IP-Netzwerkinfrastrukturen ergeben sich folgende Vorteile:

- Erhöhte Sicherheit.

  VLANs ermöglichen die Nutzung der bestehenden Infrastruktur und bieten gleichzeitig erhöhte Sicherheit, da sie den Zugriff zwischen verschiedenen Knoten eines Ethernet-Netzwerks oder eines IP-SANs einschränken.

- Verbesserte Zuverlässigkeit des Ethernet-Netzwerks und des IP-SAN durch Isolierung von Problemen.
- Verkürzung der Problemlösungszeit durch Begrenzung des Problemraums.
- Reduzierung der Anzahl verfügbarer Pfade zu einem bestimmten iSCSI-Zielport.
- Reduzierung der maximalen Anzahl von Pfaden, die von einem Host verwendet werden.

  Zu viele Pfade verlängern die Wiederverbindungszeiten. Wenn ein Host keine Multipathing-Lösung hat, kann VLANs verwendet werden, um nur einen Pfad zuzulassen.

Dynamische VLANs

Dynamische VLANs basieren auf MAC-Adressen. Ein VLAN kann definiert werden, indem die MAC-Adresse der Mitglieder angegeben wird, die eingeschlossen werden sollen.

Dynamische VLANs bieten Flexibilität und erfordern keine Zuordnung zu den physischen Ports, an denen das Gerät physisch mit dem Switch verbunden ist. Ein Kabel kann von einem Port auf einen anderen umgesteckt werden, ohne dass das VLAN neu konfiguriert werden muss.

Statische VLANs

Statische VLANs sind Port-basiert. Der Switch und der Switch-Port definieren das VLAN und seine Mitglieder.

Statische VLANs bieten eine höhere Sicherheit, da es nicht möglich ist, VLANs durch Media Access Control (MAC)-Spoofing zu kompromittieren. Wenn jedoch jemand physischen Zugriff auf den Switch hat, kann durch Austausch eines Kabels und Neukonfiguration der Netzwerkadresse Zugriff erlangt werden.

In manchen Umgebungen ist es einfacher, statische VLANs zu erstellen und zu verwalten als dynamische VLANs. Dies liegt daran, dass bei statischen VLANs lediglich der Switch und die Portkennung angegeben werden müssen, anstatt der 48-Bit-MAC-Adresse. Zusätzlich können Switch-Portbereiche mit der VLAN-Kennung gekennzeichnet werden.

FC Konfigurationen

FC- und FC-NVMe Fabric- sowie Direct-Attach-Konfigurationen für ONTAP

Bei FC und FC/NVMe wird die Netzwerktopologie zwischen der Speicherlösung und den Hosts als Fabric bezeichnet. Um Redundanz zu schaffen, die Sie vor dem Verlust des Datenzugriffs schützt, wird empfohlen, Ihr SAN mit HA-Paaren unter Verwendung von zwei oder mehr Switches in einer Multi-Fabric-Konfiguration einzurichten. Single-Fabric-Konfigurationen, die nur einen Switch zwischen den Hosts und der Speicherlösung verwenden, sind nicht vollständig redundant.

Ab ONTAP 9.19.1 können Sie FC- oder FC-NVMe-SAN-Hosts auch direkt ohne Switch an HA-Paare anschließen. Direktanschlusskonfigurationen können besonders an Remote-Standorten und in hybriden Umgebungen wertvoll sein, wo Einfachheit entscheidend ist.

Kaskadierte, partielle, vollständige, Core-Edge- und Director-Fabrics sind branchenübliche Methoden zur Verbindung von FC-Switches mit einem Fabric und werden alle unterstützt. Die Verwendung heterogener FC-Switch-Fabrics wird nicht unterstützt, außer bei eingebetteten Blade-Switches. Spezifische Ausnahmen sind auf der "Interoperabilitätsmatrix-Tool" aufgeführt. Ein Fabric kann aus einem oder mehreren Switches bestehen, und die Storage-Controller können mit mehreren Switches verbunden sein.

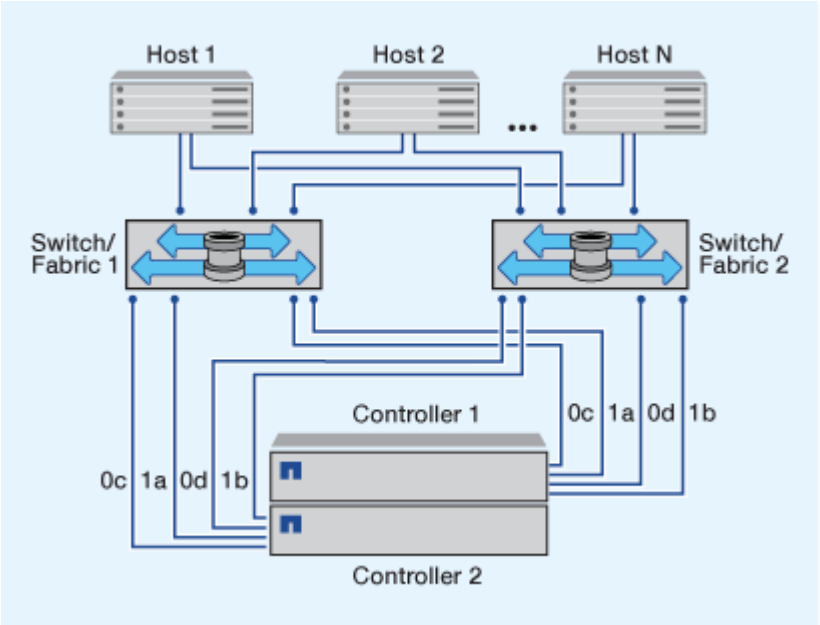
Mehrere Hosts mit unterschiedlichen Betriebssystemen wie Windows, Linux oder UNIX können gleichzeitig auf die Storage-Controller zugreifen. Hosts benötigen, dass eine unterstützte Multipathing-Lösung installiert und konfiguriert ist. Unterstützte Betriebssysteme und Multipathing-Lösungen können im Interoperability Matrix Tool überprüft werden.

Multifabric FC und FC-NVMe Konfigurationen

Es wird empfohlen, Ihre FC- und FC-NVMe-SAN-Hosts mit HA-Paaren und mindestens zwei Switches zu konfigurieren. [EH5.1][FD5.2][EH5.3] Dies gewährleistet Redundanz auf Fabric- und Speichersystemebene und unterstützt Fehlertoleranz und unterbrechungsfreie Vorgänge.

In einer Multifabric-HA-Paarkonfiguration verbinden zwei oder mehr Switches das HA-Paar mit einem oder mehreren Hosts. Jeder Switch erzeugt ein separates Fabric, das aus den Pfaden zwischen den Hosts und dem HA-Paar besteht, die über den Switch verlaufen. Durch Hinzufügen eines weiteren Switches wird ein zusätzliches Fabric erzeugt. Eine Multifabric-Konfiguration kann zwei oder mehr Switches und ihre zugehörigen Fabrics umfassen. Zur Vereinfachung zeigt die folgende Abbildung nur zwei Switches, die zwei separate Fabrics repräsentieren.

Die FC-Zielportnummern (0c, 0d, 1a, 1b) in den Abbildungen sind Beispiele. Die tatsächlichen Portnummern variieren je nach Modell Ihres Speicherknotens und ob Erweiterungsadapter verwendet werden.

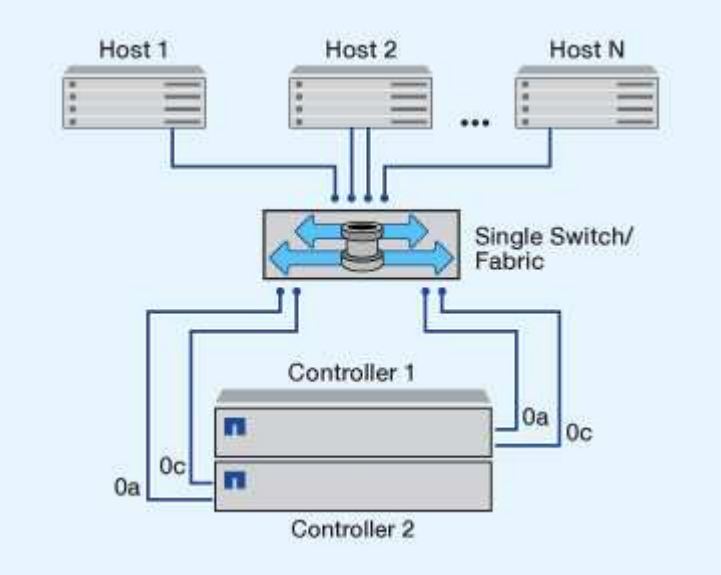


Single-fabric FC- und FC-NVMe-Konfigurationen

In Single-Fabric-HA-Paarkonfigurationen verbindet ein einzelner Switch das HA-Paar mit einem oder mehreren Hosts. Dieser einzelne Switch bildet ein einziges Fabric, das alle Pfade zwischen den Hosts und dem HA-Paar umfasst. Da keine Redundanz vorhanden ist, kann ein Switch-Ausfall zu Dienstunterbrechungen führen.

Die FC-Zielportnummern (0a, 0c) in den Abbildungen sind Beispiele. Die tatsächlichen Portnummern variieren je nach Modell Ihres Speicherknotens und ob Erweiterungsadapter verwendet werden.

Alle Plattformen, die FC-Konfigurationen unterstützen, unterstützen HA-Paar-Konfigurationen mit einem einzelnen Fabric.

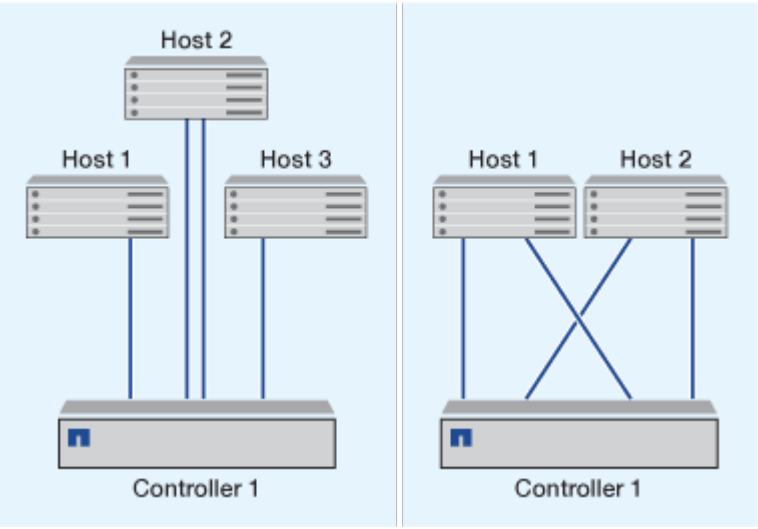


Direktanschluss-FC- und FC-NVMe-Konfigurationen

Ab ONTAP 9.19.1 werden Direct-Attachment-FC- und FC-NVMe-Konfigurationen für bestimmte AFF, ASA r2 und FAS Systeme mit der erforderlichen QLogic oder Emulex FC-Adapterkarte unterstützt. Bei einer Direct-Attachment-Konfiguration werden ein oder mehrere Hosts direkt an Ihre HA-Paare angeschlossen, ohne dass ein Switch vorhanden ist. Diese Konfiguration kann besonders wertvoll an Remote-Standorten und in hybriden Umgebungen sein, in denen Einfachheit entscheidend ist.

- MetroCluster Konfigurationen unterstützen keine direkte Anbindung.
- Direktanschlusskonfigurationen unterstützen "SVM-Migration" nicht.

Eine vollständige Liste der unterstützten Plattformen und Adapterkarten finden Sie unter "NetApp Hardware Universe".



Verwandte Informationen

- "Konfigurieren Sie ONTAP FC-Ports für die direkte Verbindung mit FC- und FC-NVMe-Hosts".
- Erfahren Sie, wie "Selektives LUN Mapping (SLM)" die Pfade eingeschränkt werden, die für den Zugriff auf die LUNs eines HA-Paares verwendet werden.

- Informationen dazu "SAN-LIFs".

Best Practices für die FC-Fabric-Konfiguration von ONTAP Systemen

Die Einhaltung bewährter Verfahren bei der FC Fabric Konfiguration verbessert Performance, Zuverlässigkeit und Stabilität von Host und Zielsystem bei Änderungen der Fabric.

Empfohlene Best Practices für die FC Fabric-Konfiguration

- **Single-Initiator / Single-Target (SI/ST)-Zonierung**

  SI/ST Zonierung reduziert Latenzspitzen bei Fabric-Änderungen, beseitigt Übersprechen, begrenzt Registered State Change Notifications (RSCNs), vereinfacht die Fehlersuche und hält die Pfadanzahl innerhalb der Host-Grenzen.

  - Auswirkungen auf den Host: Die SI/ST-Zonierung gewährleistet ein vorhersehbares MPIO-Verhalten, eine schnellere Erkennung und weniger All Path Down (APD)/Permanent Device Loss (PDL)-Ereignisse.
  - Zielwirkung: Die SI/ST-Zonierung gewährleistet weniger An- und Abmeldevorgänge und stabile FC-Sitzungen.

- **WWPN-basierte Zonierung unter Verwendung von Ziel-LIF-WWPNs (nicht physischen Ports)**

  Die WWPN-basierte Zonierung ermöglicht die Mobilität von LIF, Takeover/Giveback, unterbrechungsfreie Abläufe ohne erneute Zonierung und verhindert Pfadresets während der Wartung.

  - Auswirkungen auf den Host: Die WWPN-basierte Zonierung gewährleistet, dass es bei LIF-Verschiebungen oder Controller-Failover zu keinem Pfadverlust kommt.
  - Zielwirkung: Die WWPN-basierte Zonierung gewährleistet, dass ONTAP die Ziel-LIFs transparent verschieben kann.

- **NPIV auf allen FC-Switches aktiviert**

  Alle mit dem Fabric verbundenen Switches müssen NPIV unterstützen, und NPIV muss aktiviert sein. ONTAP verwendet N_Port ID-Virtualisierung (NPIV), um FC-Ziele bereitzustellen. Ohne NPIV können sich Ziel-LIFs nicht korrekt anmelden.

  - Auswirkungen auf den Host: NPIV verhindert zeitweilige Pfadabbrüche und fehlende Geräte.
  - Zielwirkung: NPIV gewährleistet die Transparenz der Ziel-LIFs und stabile FC-Logins.

- **Zwei unabhängige, vollständig isolierte Fabrics**

  Ein duales, unabhängiges Fabric besteht aus zwei separaten physischen Switches, Netzteilen und Verkabelungen. Fabric A und Fabric B sind niemals miteinander verbunden. Jedes Fabric verwaltet seinen eigenen FC-Nameserver, seine eigenen Zonensätze und Domänen-IDs. Da die Fabrics vollständig isoliert sind, gibt es keinen Single Point of Failure. Unterbrechungsfreie Wartungsarbeiten können an einem Fabric durchgeführt werden, während das andere weiter in Betrieb bleibt.

  - Auswirkungen auf den Host: Zwei unabhängige Fabrics unterstützen kontinuierliche E/A bei Firmware-Upgrades oder Ausfällen der Fabric.
  - Zielauswirkung: Zwei unabhängige Fabrics gewährleisten redundanten Zielzugriff bei Switch-Problemen.

- **Feste FC-Portgeschwindigkeiten (automatische Aushandlung vermeiden)**

Die automatische Aushandlung kann den Wiederaufbau der Fabric verzögern, zu Geschwindigkeitsabweichungen führen und Verzögerungen bei der Rekonvergenz sowie Link-Flaps verursachen.

  - Auswirkungen auf den Host: Feste FC Portgeschwindigkeiten führen bei Link-Resets zu kürzeren Ausfallzeiten.
  - Zielwirkung: Feste FC-Portgeschwindigkeiten sorgen dafür, dass die Ports nach Knoten- oder Switch-Ereignissen schneller wieder online kommen.

- **Strenge Einhaltung der von NetApp Interoperability Matrix Tool (IMT) validierten Konfigurationen (HBA, Treiber, Firmware, Switch)**

  Die strikte Einhaltung der im "NetApp IMT" validierten Konfigurationen gewährleistet die erwartete Latenz und den erwarteten Durchsatz.

  - Auswirkungen auf den Host: Durch die Verwendung von durch IMT validierten Konfigurationen lassen sich unerklärliche E/A-Fehler und Timeouts vermeiden.
  - Zielwirkung: Die Verwendung von IMT validierten Konfigurationen verhindert Inkompatibilitäten auf Protokollebene.

- **Proaktive Überwachung der FC-Fehlerzähler (CRC, Synchronisationsverlust, RECV_ERROR)**

  Fabric-Fehler äußern sich häufig als hostseitige Latenz- oder E/A-Fehler, bevor ONTAP Storage-Zähler sie erkennen. Die proaktive Überwachung der FC-Fehleranzahl verhindert einen kontinuierlichen Anstieg der Latenz.

  - Auswirkungen auf den Host: Proaktives Monitoring ermöglicht die frühzeitige Erkennung und verhindert erneute Host-E/A-Versuche sowie Stillstände von Applikationen.
  - Zielwirkung: Proaktives Monitoring verhindert, dass Fabric-Probleme fälschlicherweise Storage Problemen zugeschrieben werden.

- **Vermeidung einer Überbelegung der Inter-Switch-Verbindung (ISL) für SAN-Datenverkehr**

  Überlastete ISLs führen zu Kreditknappheit und Slow-Drain-Verhalten.

  - Auswirkungen auf den Host: Die Vermeidung einer ISL-Überbelegung reduziert Host-E/A-Wartezeiten und die Warteschlangenbildung.
  - Zielwirkung: Die Vermeidung einer ISL-Überbelegung verhindert Rückstau an ONTAP FC-Ports.

Verwandte Informationen

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

Unterstützte FC-Zielportgeschwindigkeiten für Ihr ONTAP System ermitteln

FC-Zielports können für das FC-NVMe-Protokoll genauso konfiguriert und verwendet werden wie für das FC-Protokoll.

Für optimale Leistung und höchste Verfügbarkeit wird die empfohlene Zielportkonfiguration, die in "NetApp Hardware Universe" für Ihr spezifisches ONTAP System aufgeführt ist, verwendet.

Jeder Onboard FC Port und jeder Erweiterungsadapter Port kann individuell für unterschiedliche, unterstützte Geschwindigkeiten konfiguriert werden. Die unterstützten Geschwindigkeiten variieren je nach ONTAP System und HBAs. Alle von einem Host verwendeten Zielports sollten auf dieselbe Geschwindigkeit eingestellt sein.

Es empfiehlt sich, für alle Ihre Initiator-, Switch- und Zielports eine einheitliche Geschwindigkeit zu konfigurieren. Wenn die Geschwindigkeiten von Port und Initiator unterschiedlich sind und keine gemeinsame Geschwindigkeit ausgehandelt werden kann, kann keine Sitzung hergestellt werden. Die Verwendung der automatischen Aushandlung zur Festlegung der Portgeschwindigkeit wird nicht empfohlen. Die automatische Aushandlung kann den Sitzungsaufbau und die Wiederherstellung nach einer Unterbrechung verlangsamen.

Die unterstützten Geschwindigkeiten sind im NetApp Hardware Universe unter **Unterstützte Adapterkarten** für jedes ONTAP System aufgeführt.

Schritte

1. Zu "NetApp Hardware Universe" wechseln.
2. **Produkte** auswählen.
3. Unter **Plattformen** den Systemtyp auswählen.
4. Wählen Sie Ihr spezifisches System und anschließend Ihre ONTAP Version.
5. **Ergebnisse anzeigen** auswählen und dann **Unterstützte Adapterkarten** auswählen.

   FC-Adapterkarten sind unter **Category** als „Block Access (Target)“ aufgeführt, und die unterstützten Geschwindigkeiten sind unter **Supported Protocol(s)** aufgeführt.

Vermeidung von Verbindungsverlusten mit einem X1133A-R6 Adapter auf ONTAP Systemen

Ein Verbindungsverlust während eines Portausfalls lässt sich verhindern, wenn das System mit redundanten Pfaden zu separaten X1133A-R6 HBAs konfiguriert ist.

Der X1133A-R6 HBA ist ein 4-Port 16-Gb-FC-Adapter, bestehend aus zwei 2-Port-Paaren. Der X1133A-R6 Adapter kann im Target-Modus oder Initiator-Modus konfiguriert werden. Jedes 2-Port-Paar wird von einem einzelnen ASIC unterstützt (zum Beispiel Port 1 und Port 2 auf ASIC 1 sowie Port 3 und Port 4 auf ASIC 2). Beide Ports eines einzelnen ASIC müssen im selben Modus betrieben werden, entweder im Target-Modus oder im Initiator-Modus. Tritt ein Fehler bei dem ASIC auf, der ein Paar unterstützt, gehen beide Ports des Paares offline.

Um diesen Verbindungsverlust zu verhindern, wird das System mit redundanten Pfaden zu separaten X1133A-R6 HBAs oder mit redundanten Pfaden zu Ports, die von verschiedenen ASICs auf dem HBA unterstützt werden, konfiguriert.

FCoE Konfigurationen

FCoE-Fabric-Konfigurationen für ONTAP Systeme

FCoE kann mithilfe von FCoE Switches auf verschiedene Weise konfiguriert werden. Direkt angeschlossene Konfigurationen werden in FCoE nicht unterstützt.

Alle FCoE Konfigurationen sind dual-fabric, vollständig redundant und erfordern Multipathing-Software auf Host-Seite. In allen FCoE Konfigurationen können mehrere FCoE und FC Switches im Pfad zwischen Initiator und Ziel vorhanden sein, bis zur maximalen Hop-Anzahl. Um Switches miteinander zu verbinden, muss auf den Switches eine Firmware-Version ausgeführt werden, die Ethernet ISLs unterstützt. Jeder Host in einer FCoE Konfiguration kann mit einem anderen Betriebssystem konfiguriert werden.

FCoE-Konfigurationen erfordern Ethernet-Switches, die FCoE-Funktionen explizit unterstützen. FCoE-Konfigurationen werden durch dasselbe Interoperabilitäts- und Qualitätssicherungsverfahren wie FC-Switches

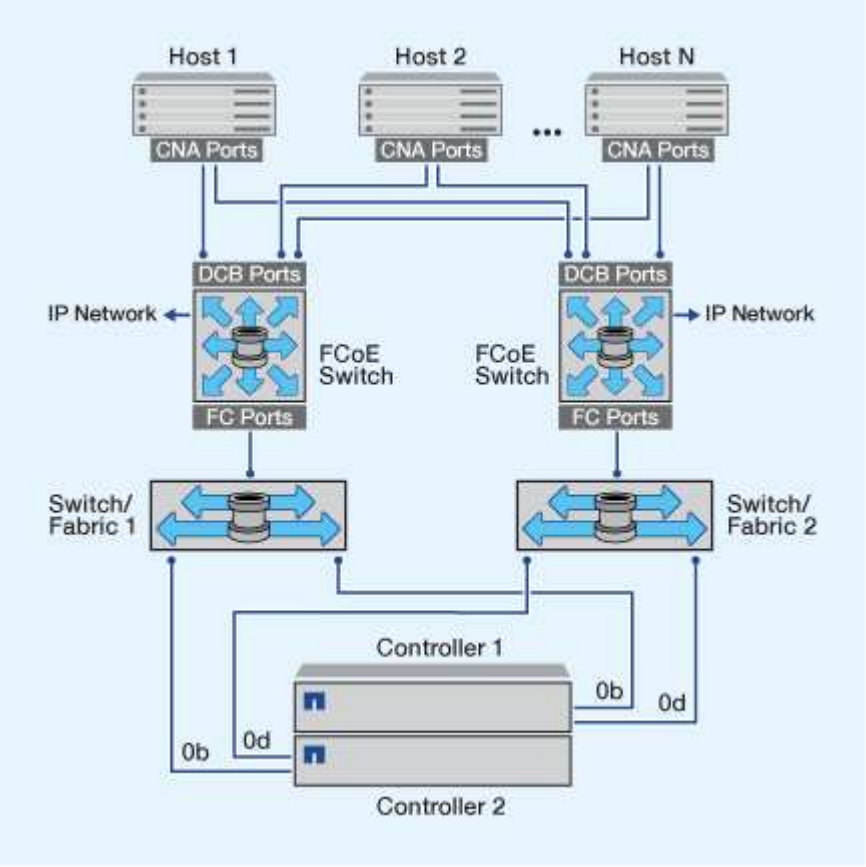
validiert. Unterstützte Konfigurationen sind in der Interoperabilitätsmatrix aufgeführt. Zu den Parametern dieser unterstützten Konfigurationen gehören das Switch-Modell, die Anzahl der Switches, die in einem einzelnen Fabric eingesetzt werden können, und die unterstützte Switch-Firmware-Version.

Die in den Abbildungen angegebenen Portnummern der FC-Zielerweiterungsadapter sind Beispiele. Die tatsächlichen Portnummern können je nach den Erweiterungssteckplätzen, in denen die FCoE-Zielerweiterungsadapter installiert sind, variieren.

FCoE-Initiator zu FC-Ziel

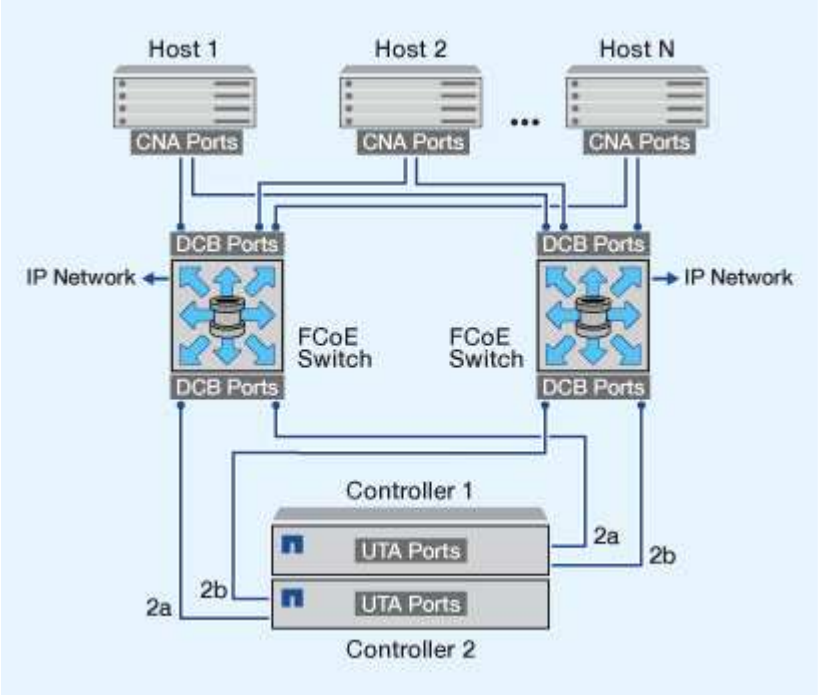
Mithilfe von FCoE-Initiatoren (CNAs) können Hosts über FCoE-Switches mit beiden Controllern in einem HA-Paar zu FC-Zielports verbunden werden. Der FCoE-Switch muss ebenfalls über FC-Ports verfügen. Der Host-FCoE-Initiator ist immer mit dem FCoE-Switch verbunden. Der FCoE-Switch kann entweder direkt mit dem FC-Ziel verbunden sein oder über FC-Switches mit dem FC-Ziel verbunden werden.

Die folgende Abbildung zeigt Host-CNAs, die sich mit einem FCoE Switch und dann mit einem FC Switch verbinden, bevor sie mit dem HA-Paar verbunden werden:



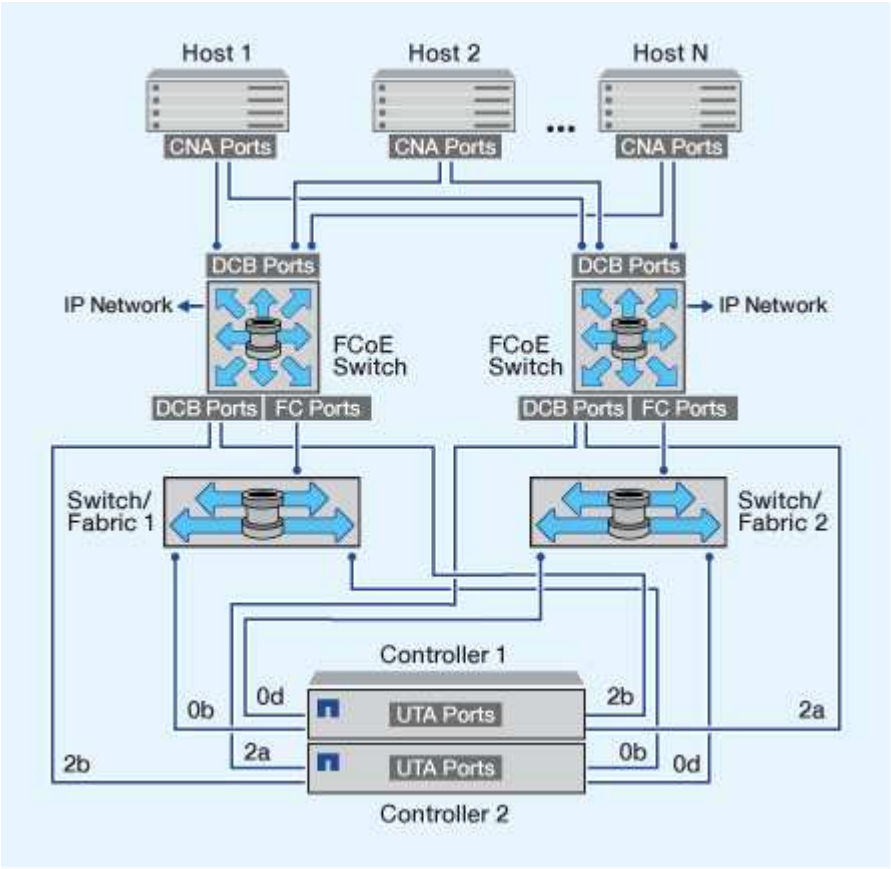
FCoE-Initiator zu FCoE-Target

Mithilfe von Host-FCoE-Initiatoren (CNAs) können Hosts mit beiden Controllern eines HA-Paares über FCoE-Switches mit FCoE-Zielports (auch UTAs oder UTA2s genannt) verbunden werden.



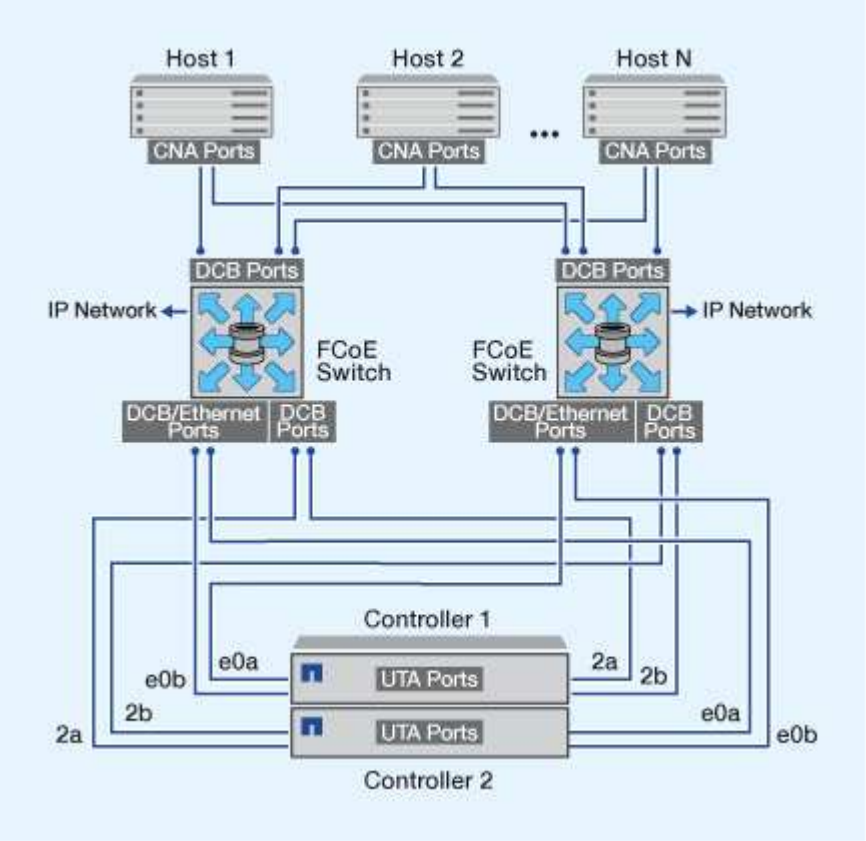
FCoE-Initiator zu FCoE- und FC-Zielen

Mit Host-FCoE-Initiatoren (CNAs) ist eine Verbindung von Hosts zu beiden Controllern in einem HA-Paar mit FCoE- und FC-Zielports (auch UTAs oder UTA2s genannt) über FCoE-Switches möglich.



FCoE gemischt mit IP-Speicherprotokollen

Mithilfe von Host-FCoE-Initiatoren (CNAs) können Hosts mit beiden Controllern eines HA-Paares über FCoE-Switches mit FCoE-Zielports (auch UTAs oder UTA2s genannt) verbunden werden. FCoE-Ports können keine herkömmliche Link-Aggregation zu einem einzelnen Switch verwenden. Cisco Switches unterstützen eine spezielle Art der Link-Aggregation (Virtual Port Channel), die FCoE unterstützt. Ein Virtual Port Channel aggregiert einzelne Verbindungen zu zwei Switches. Virtual Port Channels können auch für anderen Ethernet-Datenverkehr verwendet werden. Ports, die für anderen Datenverkehr als FCoE verwendet werden, einschließlich NFS, SMB, iSCSI und anderem Ethernet-Datenverkehr, können reguläre Ethernet-Ports an den FCoE-Switches verwenden.



ONTAP unterstützte FCoE Initiator- und Zielportkombinationen

Bestimmte Kombinationen von FCoE- und traditionellen FC-Initiatoren und -Targets werden unterstützt.

FCoE Initiatoren

FCoE-Initiatoren können in Host-Computern mit sowohl FCoE- als auch herkömmlichen FC-Targets in Speicherkontrollern verwendet werden. Der Host-FCoE-Initiator muss mit einem FCoE-DCB-Switch (Data Center Bridging) verbunden sein, eine direkte Verbindung zu einem Target wird nicht unterstützt.

Die folgende Tabelle listet die unterstützten Kombinationen auf:

Initiator	Ziel	Unterstützt?
FC	FC	Ja
FC	FCoE	Ja

Initiator	Ziel	Unterstützt?
FCoE	FC	Ja
FCoE	FCoE	Ja

FCoE Ziele

Sie können FCoE-Zielports mit 4-Gb, 8-Gb oder 16-Gb FC-Ports auf dem Storage Controller kombinieren, unabhängig davon, ob die FC-Ports Add-in-Zieladapter oder Onboard-Ports sind. Sowohl FCoE- als auch FC-Zieladapter können im selben Storage Controller vorhanden sein.

Die Regeln für die Kombination von Onboard FC-Ports und Erweiterungs FC-Ports gelten weiterhin.

FC- und FCoE-Zonierung

Informationen zu FC- und FCoE-Zoning mit ONTAP Systemen

Eine FC-, FC-NVMe- oder FCoE-Zone ist eine logische Gruppierung eines oder mehrerer Ports innerhalb eines Fabric. Damit Geräte einander sehen, sich verbinden, Sitzungen miteinander aufbauen und kommunizieren können, müssen beide Ports Mitglieder derselben Zone sein.

Die Zoneneinteilung erhöht die Sicherheit, indem der Zugriff und die Konnektivität auf Endpunkte innerhalb einer gemeinsamen Zone beschränkt werden. Ports, die sich nicht in derselben Zone befinden, können nicht miteinander kommunizieren. Dadurch wird das Übersprechen zwischen Initiator-HBAs reduziert oder eliminiert. Treten Verbindungsprobleme auf, trägt die Zoneneinteilung dazu bei, die Probleme auf eine bestimmte Gruppe von Ports einzugrenzen, wodurch die Lösungszeit verkürzt wird.

Zoning reduziert die Anzahl der verfügbaren Pfade zu einem bestimmten Port und die Anzahl der Pfade zwischen einem Host und dem Speichersystem. Beispielsweise haben einige Multipathing-Lösungen von Host-Betriebssystemen eine Begrenzung hinsichtlich der Anzahl der Pfade, die sie verwalten können. Zoning kann die Anzahl der für den Host sichtbaren Pfade so verringern, dass die Pfade zum Host die vom Host-Betriebssystem maximal erlaubte Anzahl nicht überschreiten.

World Wide Name-basierte Zoneneinteilung

Die Zoneneinteilung basierend auf dem World Wide Name (WWN) legt die WWNs der in die Zone einzuschließenden Mitglieder fest. Obwohl die Zoneneinteilung basierend auf dem World Wide Node Name (WWNN) bei einigen Switch-Herstellern möglich ist, muss bei der Zoneneinteilung in ONTAP die Zoneneinteilung basierend auf dem World Wide Port Name (WWPN) verwendet werden.

Die WWPN-Zonierung ist erforderlich, um einen bestimmten Port korrekt zu definieren und NPIV effektiv zu nutzen. FC-Switches sollten anhand der WWPNs der logischen Schnittstellen (LIFs) des Ziels zoniert werden, nicht anhand der WWPNs der physischen Ports des Knotens. Die WWPNs der physischen Ports beginnen mit „50“ und die WWPNs der LIFs beginnen mit „20“.

Die WWPN-Zonierung bietet Flexibilität, da der Zugriff nicht davon abhängt, wo das Gerät physisch mit dem Fabric verbunden ist. Ein Kabel kann von einem Port auf einen anderen umgesteckt werden, ohne die Zonen neu konfigurieren zu müssen.

Empfohlene FC- und FCoE-Zoning-Konfigurationen für ONTAP Systeme

Eine Zoning-Konfiguration ist erforderlich, wenn auf Ihrem Host keine Multipathing-Lösung installiert ist, wenn vier oder mehr Hosts mit Ihrem SAN verbunden sind oder wenn Selective LUN Mapping auf den Knoten in Ihrem Cluster nicht implementiert ist.

In der empfohlenen FC- und FCoE Zoning-Konfiguration umfasst jede Zone einen Initiator-Port und einen oder mehrere Ziel-LIFs. Diese Konfiguration ermöglicht jedem Host-Initiator den Zugriff auf jeden Knoten, verhindert jedoch, dass Hosts, die auf denselben Knoten zugreifen, die Ports der jeweils anderen sehen.

Alle LIFs der Storage Virtual Machine (SVM) zur Zone mit dem Host-Initiator hinzufügen. So ist es möglich, Volumes oder LUNs zu verschieben, ohne die bestehenden Zonen zu bearbeiten oder neue Zonen zu erstellen.

Dual-fabric Zoning-Konfigurationen

Dual-fabric Zoning-Konfigurationen werden empfohlen, da sie Schutz vor Datenverlust durch den Ausfall einer einzelnen Komponente bieten. In einer Dual-fabric Konfiguration ist jeder Host-Initiator über unterschiedliche Switches mit jedem Knoten im Cluster verbunden. Fällt ein Switch aus, bleibt der Datenzugriff über den verbleibenden Switch erhalten. Auf dem Host ist Multipathing-Software erforderlich, um mehrere Pfade zu verwalten.

In der folgenden Abbildung verfügt der Host über zwei Initiatoren und verwendet Multipathing Software. Es gibt zwei Zonen. "Selektives LUN Mapping (SLM)" ist so konfiguriert, dass alle Knoten als meldende Knoten gelten.

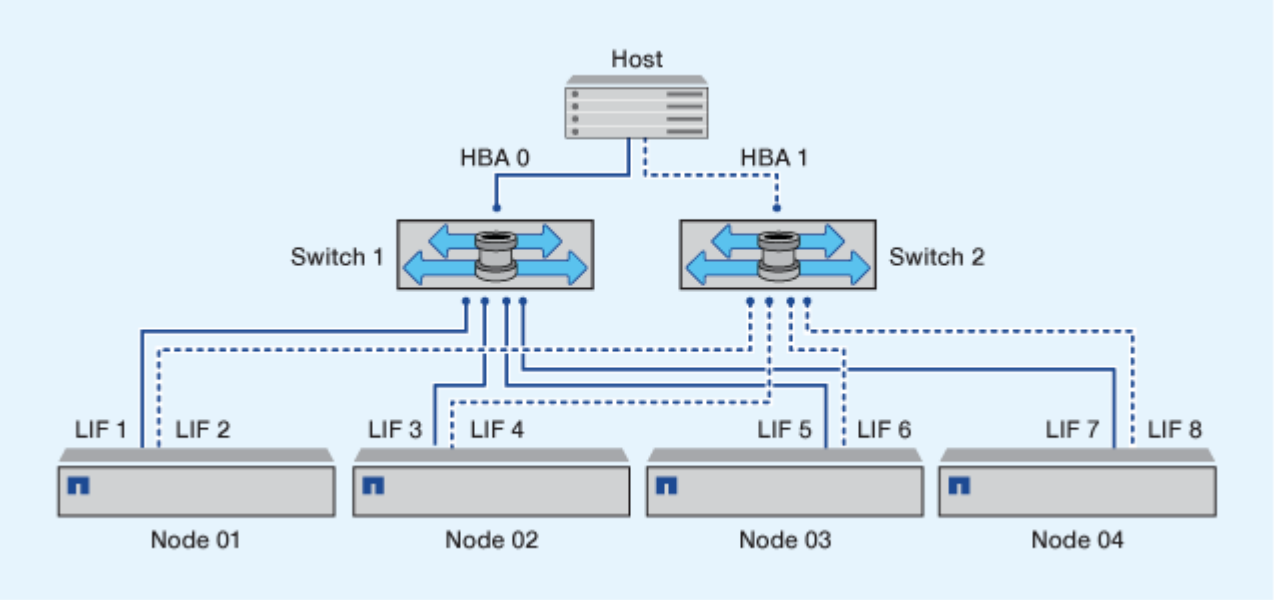
> Die in dieser Abbildung verwendete Namenskonvention ist lediglich eine Empfehlung für eine mögliche Namenskonvention, die für Ihre ONTAP Lösung gewählt werden kann.

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

Jeder Host-Initiator ist über einen separaten Switch angebunden. Zone 1 ist über Switch 1 zugänglich. Zone 2 ist über Switch 2 zugänglich.

Jeder Host kann auf eine LIF auf jedem Knoten zugreifen. Dadurch ist weiterhin der Zugriff des Hosts auf seine LUNs möglich, falls ein Knoten ausfällt. SVMs haben Zugriff auf alle iSCSI- und FC-LIFs auf jedem Knoten im Cluster, basierend auf Ihrer SLM-Meldeknoten-Konfiguration. SLM, Portsets oder FC-Switch-Zoning können verwendet werden, um die Anzahl der Pfade von einer SVM zum Host und von einer SVM zu einer LUN zu reduzieren.

Wenn die Konfiguration mehr Knoten umfasst, sind die LIFs für die zusätzlichen Knoten in diesen Zonen enthalten.



Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der Pfade unterstützen, die für den Zugriff auf die LUNs auf den Knoten verwendet wird.

Single-fabric-Zoning

In einer Single Fabric-Konfiguration wird jeder Host-Initiator über einen einzelnen Switch mit jedem Speicherknoten verbunden. Single Fabric Zoning-Konfigurationen werden nicht empfohlen, da sie keinen Schutz vor Datenverlust durch den Ausfall einer einzelnen Komponente bieten. Falls eine Single Fabric Zoning-Konfiguration gewählt wird, sollte jeder Host über zwei Initiatoren für Multipathing verfügen, um die Ausfallsicherheit der Lösung zu gewährleisten. Auf dem Host ist Multipathing-Software erforderlich, um mehrere Pfade zu verwalten.

Jeder Host-Initiator sollte mindestens eine LIF von jedem Knoten haben, auf den er zugreifen kann. Die Zonierung sollte mindestens einen Pfad vom Host-Initiator zum HA-Paar von Knoten im Cluster ermöglichen, um einen Pfad für die LUN-Konnektivität bereitzustellen. Das bedeutet, dass jeder Initiator auf dem Host in seiner Zoning-Konfiguration möglicherweise nur eine Ziel-LIF pro Knoten hat. Besteht die Anforderung für Multipathing zum selben Knoten oder zu mehreren Knoten im Cluster, hat dann jeder Knoten mehrere LIFs pro Knoten in seiner Zoning-Konfiguration. So kann der Host weiterhin auf seine LUNs zugreifen, falls ein Knoten ausfällt oder ein Volume mit der LUN auf einen anderen Knoten verschoben wird. Dazu müssen die Reporting-Knoten entsprechend eingestellt sein.

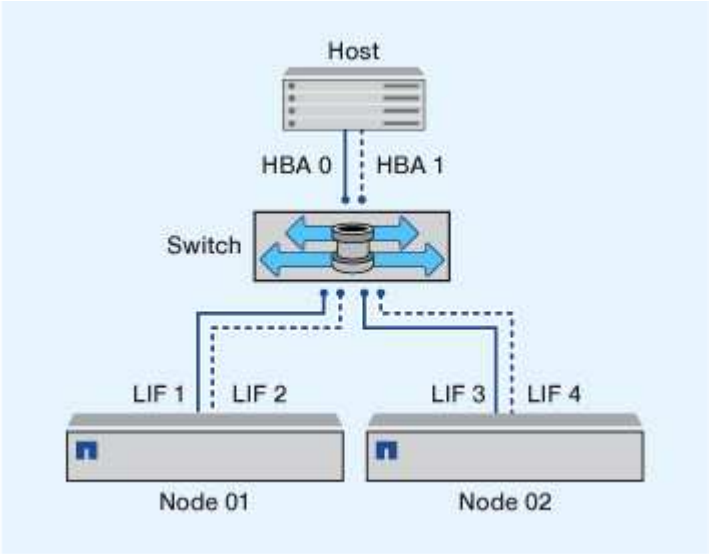
Bei Verwendung von Cisco FC- und FCoE-Switches darf eine einzelne Fabric-Zone nicht mehr als eine Ziel-LIF für denselben physischen Port enthalten. Befinden sich mehrere LIFs auf demselben Port in derselben Zone, können die LIF-Ports möglicherweise nach einem Verbindungsverlust nicht wiederhergestellt werden.

In der folgenden Abbildung verfügt der Host über zwei Initiatoren und verwendet Multipathing Software. Es gibt zwei Zonen:

Die in dieser Abbildung verwendete Namenskonvention ist lediglich eine Empfehlung für eine mögliche Namenskonvention, die für Ihre ONTAP Lösung gewählt werden kann.

- Zone 1: HBA 0, LIF_1 und LIF_3
- Zone 2: HBA 1, LIF_2 und LIF_4

Wenn die Konfiguration mehr Knoten umfasst, werden die LIFs für die zusätzlichen Knoten in diese Zonen aufgenommen.



In diesem Beispiel könnten Sie auch alle vier LIFs in jeder Zone haben. In diesem Fall wären die Zonen wie folgt:

- Zone 1: HBA 0, LIF_1, LIF_2, LIF_3 und LIF_4
- Zone 2: HBA 1, LIF_1, LIF_2, LIF_3 und LIF_4

Das Host-Betriebssystem und die Multipathing-Software müssen die Anzahl der unterstützten Pfade, die für den Zugriff auf die LUNs auf den Knoten verwendet werden, unterstützen. Zur Ermittlung der Anzahl der Pfade, die für den Zugriff auf die LUNs auf den Knoten verwendet werden, siehe den Abschnitt zu den SAN-Konfigurationsgrenzen.

Zonenbeschränkungen für Cisco FC und FCoE Switches

Bei der Verwendung von Cisco FC und FCoE Switches gelten bestimmte Einschränkungen für die Nutzung von physischen Ports und logischen Schnittstellen (LIFs) in Zonen.

Physische Ports

- FC-NVMe und FC können denselben 32 Gb-physikalischen Port gemeinsam nutzen.
- FC-NVMe und FCoE können nicht denselben physischen Port verwenden.
- FC und FCoE können denselben physischen Port nutzen, aber ihre Protokoll-LIFs müssen in separaten Zonen sein.

Logische Schnittstellen (LIFs)

- Eine Zone kann eine LIF von jedem Zielport im Cluster enthalten.

  Die SLM-Konfiguration sollte so überprüft werden, dass die maximal zulässige Anzahl von Pfaden zum Host nicht überschritten wird.

- Jeder LIF an einem bestimmten Port muss sich in einer separaten Zone von anderen LIFs an diesem Port befinden
- LIFs auf verschiedenen physischen Ports können in derselben Zone sein.

Anforderungen an SAN-Hosts, die mit ONTAP und Nicht-NetApp-Systemen verbunden sind

Gemeinsam genutzte SAN-Konfigurationen sind Hosts, die sowohl an ONTAP Speichersysteme als auch an Speichersysteme anderer Hersteller angeschlossen sind. Der Zugriff auf ONTAP Speichersysteme und Speichersysteme anderer Hersteller von einem einzelnen Host aus wird unterstützt, sofern bestimmte Voraussetzungen erfüllt sind.

Für alle Host-Betriebssysteme ist es eine Best Practice, separate Adapter für die Verbindung zu den Speichersystemen der jeweiligen Hersteller zu verwenden. Die Verwendung separater Adapter verringert die Wahrscheinlichkeit von Treiber- und Einstellungskonflikten. Für Verbindungen zu einem ONTAP-Speichersystem müssen Adaptermodell, BIOS, Firmware und Treiber im NetApp Interoperability Matrix Tool als unterstützt aufgeführt sein.

Sie sollten die erforderlichen oder empfohlenen Zeitüberschreitungswerte und andere Speicherparameter für den Host festlegen. Die NetApp Software muss immer zuletzt installiert bzw. die NetApp Einstellungen zuletzt angewendet werden.

- Für AIX sind die Werte aus der AIX Host Utilities Version zu verwenden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.
- Für ESX sollten Sie die Host-Einstellungen mithilfe von ONTAP tools for VMware vSphere anwenden.
- Für HP-UX sind die HP-UX Standardspeichereinstellungen zu verwenden.
- Für Linux sind die Werte aus der Linux Host Utilities Version zu verwenden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.
- Für Solaris sind die Werte aus der Solaris Host Utilities Version zu verwenden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.
- Für Windows sollte die Version von Windows Host Utilities installiert werden, die im Interoperability Matrix Tool für Ihre Konfiguration aufgeführt ist.

Verwandte Informationen

"NetApp Interoperabilitätsmatrix-Tool"

SAN-Konfigurationen in einer MetroCluster Umgebung

Unterstützte SAN-Konfigurationen in einer ONTAP MetroCluster Umgebung

Bei der Verwendung von SAN Konfigurationen in einer MetroCluster Umgebung sind bestimmte Aspekte zu berücksichtigen.

- MetroCluster Konfigurationen unterstützen keine Frontend-FC-Fabric-“routed”-vSAN-Konfigurationen.
- Ab ONTAP 9.15.1 werden Vier-Knoten MetroCluster IP-Konfigurationen auf NVMe/TCP unterstützt.
- Ab ONTAP 9.12.1 werden vier Knoten MetroCluster IP-Konfigurationen auf NVMe/FC unterstützt. MetroCluster Konfigurationen werden für Frontend-NVMe-Netzwerke vor ONTAP 9.12.1 nicht unterstützt.
- Andere SAN-Protokolle wie iSCSI, FC und FCoE werden in MetroCluster Konfigurationen unterstützt.
- Bei der Verwendung von SAN-Clientkonfigurationen ist zu prüfen, ob besondere Hinweise für MetroCluster-Konfigurationen in den Anmerkungen im "NetApp Interoperabilitätsmatrix-Tool" (IMT)

enthalten sind.

- Betriebssysteme und Anwendungen müssen eine I/O-Resilienz von 120 Sekunden bereitstellen, um MetroCluster automatische ungeplante Umschaltungen sowie durch Tiebreaker oder Mediator initiierte Umschaltungen zu unterstützen.
- MetroCluster Konfigurationen verwenden auf beiden Seiten des Frontend-FC-Fabrics die gleichen WWNNs und WWPNs.

Verwandte Informationen

- "Verständnis von MetroCluster Datenschutz und Notfallwiederherstellung"
- "NetApp Knowledge Base: Welche Aspekte der AIX-Hostunterstützung sind in einer MetroCluster Konfiguration zu beachten?"
- "NetApp Knowledge Base: Überlegungen zur Solaris-Hostunterstützung in einer MetroCluster Konfiguration"

Portüberschneidungen während ONTAP MetroCluster Switchover und Switchback vermeiden

In einer SAN-Umgebung können die Frontend-Switches so konfiguriert werden, dass Überlappungen vermieden werden, wenn der alte Port offline geht und der neue Port online geht.

Während der Umschaltung kann es vorkommen, dass sich der FC-Port am verbleibenden Standort beim Fabric anmeldet, bevor das Fabric erkennt, dass der FC-Port am betroffenen Standort offline ist und diesen Port aus den Namens- und Verzeichnisdiensten entfernt hat.

Wenn der FC-Port am betroffenen Standort noch nicht entfernt wurde, kann der Anmeldeversuch des FC-Ports am verbleibenden Standort aufgrund einer doppelten WWPN abgelehnt werden. Dieses Verhalten der FC-Switches kann so geändert werden, dass die Anmeldung des vorherigen Geräts und nicht die des aktuellen Geräts berücksichtigt wird. Die Auswirkungen dieses Verhaltens auf andere Fabric-Geräte sollten überprüft werden. Für weitere Informationen ist der Switch-Hersteller zu kontaktieren.

Wählen Sie das richtige Verfahren entsprechend Ihrem Switch-Typ.

Beispiel 1. Schritte

Cisco Switch

1. Stellen Sie eine Verbindung zum Switch her und melden Sie sich an.
2. In den Konfigurationsmodus wechseln:

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

3. Der erste Geräteeintrag in der Name-Server-Datenbank wird mit dem neuen Gerät überschrieben:

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

4. Bei Switches, auf denen NX-OS 8.x läuft, ist zu bestätigen, dass das flogi quiesce Zeitüberschreitung

auf Null gesetzt ist:

a. Den Ruhetimer anzeigen:

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

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

b. Falls die Ausgabe im vorherigen Schritt nicht anzeigt, dass timerval null ist, sollte er auf null gesetzt werden:

```
switch(config)# flogi scale enable
switch(config)$ flogi quiesce timeout 0
```

Brocade Switch

1. Stellen Sie eine Verbindung zum Switch her und melden Sie sich an.
2. Den `switchDisable`Befehl eingeben.
3. Geben Sie den `configure` Befehl ein und drücken Sie `y` an der Eingabeaufforderung.

```
  F-Port login parameters (yes, y, no, n): [no] y
```

4. Einstellung 1 auswählen:

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. Beantworten Sie die restlichen Eingabeaufforderungen oder drücken Sie **Strg + D**.
6. Den `switchEnable`Befehl eingeben.

Verwandte Informationen

"Umschaltung für Tests oder Wartungsarbeiten"

ONTAP Unterstützung für SAN Host Multipathing

ONTAP verwendet Asymmetric Logical Unit Access (ALUA) Software für Multipathing mit sowohl FC- als auch iSCSI-Hosts.

Ab ONTAP 9.5 wird Multipath-Hochverfügbarkeit (HA) mit Failover/Giveback für NVMe-Hosts über Asynchronous Namespace Access (ANA) unterstützt. In ONTAP 9.4 unterstützt NVMe nur einen Pfad vom Host zum Ziel, daher muss der Anwendungshost das Pfad-Failover zu seinem HA-Partner verwalten.

Informationen darüber, welche spezifischen Hostkonfigurationen ALUA oder ANA unterstützen, finden sich in

der "NetApp Interoperabilitätsmatrix-Tool" und "ONTAP SAN Hostkonfiguration" für Ihr Host-Betriebssystem.

Multipathing-Software, auch bekannt als MPIO (Multipath I/O), wird für HA-Konfigurationen empfohlen. Die Multipathing-Software ist auf Ihrem SAN-Host erforderlich, damit dieser über mehrere Pfade auf eine LUN oder einen NVMe-Namespace zugreifen kann. Sie stellt dem Betriebssystem für alle Pfade zu einer LUN oder einem NVMe-Namespace eine einzige Festplatte bereit. Ohne sie könnte das Betriebssystem jeden Pfad als separate Festplatte behandeln, was zu Datenbeschädigung führen kann.

Ihre Lösung gilt als mehrpfadig, wenn eine der folgenden Bedingungen erfüllt ist:

- Ein einzelner Initiator-Port im Host, der mit mehreren SAN-LIFs in der SVM verbunden ist
- Mehrere Initiator-Ports sind an eine einzelne SAN LIF in der SVM angeschlossen.
- Mehrere Initiator-Ports, die mit mehreren SAN-LIFs in der SVM verbunden sind

Sie sollten Selective LUN Map, FC-Switch-Zoning oder Portsets verwenden, um die Pfade für den Zugriff auf LUNs und Namespaces einzuschränken.

Verwandte Informationen

Informationen dazu "Von ONTAP unterstützte SAN-Multipath-Konfigurationen".

Empfohlene Anzahl von Pfaden vom Host zu den Knoten im Cluster

Sie sollten nicht mehr als acht Pfade von Ihrem Host zu jedem Knoten in Ihrem Cluster verwenden. Sie sollten außerdem die Gesamtzahl der Pfade, die vom Host-Betriebssystem und dem auf dem Host verwendeten Multipathing unterstützt werden, nicht überschreiten.

Wenn Ihr Cluster vier oder mehr Knoten umfasst oder die SVMs auf einem Ihrer Knoten mehr als vier Zielports verwenden, können die folgenden Methoden eingesetzt werden, um die Anzahl der Pfade, über die auf LUNs auf Ihren Knoten zugegriffen werden kann, so zu begrenzen, dass das empfohlene Maximum von acht Pfaden nicht überschritten wird.

- "Selective LUN Map (SLM)"

  SLM reduziert die Anzahl der Pfade vom Host zur LUN auf nur Pfade auf dem Knoten, dem die LUN gehört, und dem HA-Partner des Eigentümerknotens. SLM ist standardmäßig aktiviert. Sie sollten mindestens zwei Pfade pro LUN haben, die zu jedem meldenden Knoten führen und durch SLM von der Storage Virtual Machine (SVM) in Ihrem Cluster verwendet werden. Dadurch werden Single Points of Failure eliminiert und das System kann Komponentenausfälle überstehen.

- "Port-Sets"

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

- Initiatorgruppen-Zuordnungen (igroup) von Ihrem Host

  Es besteht die Möglichkeit, igroups zu definieren und sie LUNs zuzuordnen, um zu steuern, welche Initiatoren Zugriff auf LUNs erhalten.

- "FC Switch-Zonierung"

  Sie sollten eine Zoning-Konfiguration erstellen, wenn auf Ihrem Host keine Multipathing-Lösung installiert ist, wenn vier oder mehr Hosts mit Ihrem SAN verbunden sind oder wenn SLM auf den Knoten in Ihrem

Cluster nicht implementiert ist.

Konfigurationsgrenzen

Maximal unterstützte Knoten und SAN-Hosts pro ONTAP Cluster bestimmen

Die Anzahl der unterstützten Knoten pro Cluster variiert je nach Ihrer ONTAP-Version, Ihren Controller-Modellen und dem Protokoll Ihrer Clusterknoten. Die maximale Anzahl von SAN-Hosts, die an einen Cluster angeschlossen werden können, variiert ebenfalls abhängig von Ihrer spezifischen Konfiguration.

Maximal unterstützte Anzahl an Knoten pro Cluster bestimmen

Wenn ein Knoten im Cluster für FC, FC-NVMe, FCoE oder iSCSI konfiguriert ist, unterliegt der Cluster den SAN-Knotenlimits. Knotenlimits basierend auf den Controllern in Ihrem Cluster sind im *Hardware Universe* aufgeführt.

Schritte

1. Gehe zu "NetApp Hardware Universe".
2. Oben links, neben **Home**, **Plattformen** auswählen und anschließend den Plattformtyp auswählen.
3. Wählen Sie Ihre Version von ONTAP.

   Es wird eine neue Spalte angezeigt, in der Sie Ihre Plattformen auswählen können.

4. Die in Ihrer Lösung verwendeten Plattformen auswählen.
5. Unter **Wählen Sie Ihre Spezifikationen** die Auswahl von **Alle auswählen** aufheben.
6. **Maximale Anzahl Knoten pro Cluster (NAS/SAN)** auswählen.
7. Auf **Ergebnisse anzeigen** klicken.

Ergebnisse

Die maximale Anzahl an Knoten pro Cluster für Ihre ausgewählten Plattformen wird angezeigt.

Es kann festgestellt werden, ob Ihr Cluster mehr FC Hosts unterstützen kann.

Bei FC- und FC-NVMe-Konfigurationen sollte die Anzahl der Initiator-Target-Nexus (ITNs) in Ihrem System verwendet werden, um zu bestimmen, ob weitere Hosts zu Ihrem Cluster hinzugefügt werden können.

Ein ITN repräsentiert einen Pfad vom Initiator des Hosts zum Ziel des Speichersystems. Die maximale Anzahl von ITNs pro Knoten in FC und FC-NVMe Konfigurationen beträgt 2.048. Wenn die maximale Anzahl von ITNs noch nicht erreicht ist, können dem Cluster weiterhin Hosts hinzugefügt werden.

Um die Anzahl der in Ihrem Cluster verwendeten ITNs zu ermitteln, sind für jeden Knoten im Cluster die folgenden Schritte auszuführen.

Schritte

1. Alle LIFs auf einem bestimmten Knoten identifizieren.
2. Führen Sie für jede LIF auf dem Node den folgenden Befehl aus:

```
fcp initiator show -fields wwpn, lif
```

Die Anzahl der am unteren Rand der Befehlsausgabe angezeigten Einträge entspricht Ihrer Anzahl an ITNs für diesen LIF.

3. Die Anzahl der für jedes LIF angezeigten ITNs wird festgehalten.
4. Die Anzahl der ITNs für jedes LIF auf jedem Knoten im Cluster addieren.

   Diese Gesamtzahl stellt die Anzahl der ITNs in Ihrem Cluster dar.

Es wird festgestellt, ob Ihr Cluster mehr iSCSI Hosts unterstützen kann.

Die Anzahl der Hosts, die direkt an einen Knoten oder über einen oder mehrere Switches angeschlossen werden können, hängt von der Anzahl der verfügbaren Ethernet-Ports ab. Die Anzahl der verfügbaren Ethernet-Ports wird durch das Modell des Controllers sowie die Anzahl und den Typ der im Controller installierten Adapter bestimmt. Die Anzahl der unterstützten Ethernet-Ports für Controller und Adapter ist im *Hardware Universe* verfügbar.

Bei allen Clusterkonfigurationen mit mehreren Knoten muss die Anzahl der iSCSI-Sitzungen pro Knoten ermittelt werden, um festzustellen, ob weitere Hosts zu Ihrem Cluster hinzugefügt werden können. Solange Ihr Cluster unter der maximalen Anzahl an iSCSI-Sitzungen pro Knoten bleibt, können weiterhin Hosts zu Ihrem Cluster hinzugefügt werden. Die maximale Anzahl an iSCSI-Sitzungen pro Knoten variiert je nach den Controllertypen in Ihrem Cluster.

Schritte

1. Alle Zielportalgruppen auf dem Node identifizieren.
2. Die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten prüfen:

```
iscsi session show -tpgroup _tpgroup_
```

   Die Anzahl der Einträge am Ende der Befehlsausgabe entspricht der Anzahl Ihrer iSCSI-Sitzungen für diese Zielportalgruppe.

3. Die Anzahl der für jede Zielportalgruppe angezeigten iSCSI-Sitzungen wird erfasst.
4. Die Anzahl der iSCSI-Sitzungen für jede Zielportalgruppe auf dem Knoten addieren.

   Die Gesamtzahl stellt die Anzahl der iSCSI-Sitzungen auf Ihrem Knoten dar.

ONTAP ASA Konfigurationsgrenzen und Unterstützung

Die Konfigurationsgrenzen und die Unterstützung für All-Flash SAN Array (ASA) variieren je nach ONTAP Version.

Die aktuellsten Informationen zu den unterstützten Konfigurationsgrenzen sind in "NetApp Hardware Universe" verfügbar.

Diese Einschränkungen gelten für ASA-Systeme. Wenn Sie ein ASA r2-System (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 oder ASA C30) besitzen, siehe "ASA r2 System-

Speichergrenzen".

SAN-Protokolle und unterstützte Anzahl von Nodes pro Cluster

Die unterstützten SAN-Protokolle und die maximale Anzahl von Knoten pro Cluster hängen davon ab, ob eine nicht MetroCluster oder MetroCluster Konfiguration vorliegt:

Nicht-MetroCluster Konfigurationen

Die folgende Tabelle zeigt die ASA Unterstützung für SAN-Protokolle und die unterstützte Anzahl von Knoten pro Cluster in Nicht-MetroCluster Konfigurationen:

Beginnend mit ONTAP…	Protokollunterstützung	Maximale Anzahl Knoten pro Cluster
9.11.1	• NVMe/TCP • NVMe/FC	12
9.10.1	• NVMe/TCP	2
9.9.1	• NVMe/FC	2
	• FC • iSCSI	12
9,7	• FC • iSCSI	2

MetroCluster IP-Konfigurationen

Die folgende Tabelle zeigt die ASA Unterstützung für SAN-Protokolle und die unterstützte Anzahl von Knoten pro Cluster in MetroCluster IP-Konfigurationen:

Beginnend mit ONTAP…	Protokollunterstützung	Maximale Anzahl Knoten pro Cluster
9.15.1	• NVMe/TCP	2 Knoten pro Cluster in Vier-Knoten MetroCluster IP-Konfigurationen
9.12.1	• NVMe/FC	2 Knoten pro Cluster in Vier-Knoten MetroCluster IP-Konfigurationen
9.9.1	• FC • iSCSI	4 Knoten pro Cluster in Acht-Knoten MetroCluster IP-Konfigurationen
9,7	• FC • iSCSI	2 Knoten pro Cluster in Vier-Knoten MetroCluster IP-Konfigurationen

Unterstützung für persistente Ports

Ab ONTAP 9.8 sind persistente Ports auf All-Flash SAN Arrays (ASAs), die für die Verwendung des FC-Protokolls konfiguriert sind, standardmäßig aktiviert. Persistente Ports sind nur für FC verfügbar und erfordern

die Zugehörigkeit zu einer Zone, die durch den World Wide Port Name (WWPN) identifiziert wird.

Persistente Ports reduzieren die Auswirkungen von Übernahmen, indem sie eine Schatten-LIF auf dem entsprechenden physischen Port des Hochverfügbarkeitspartners (HA-Partner) erstellen. Wird ein Knoten übernommen, nimmt die Schatten-LIF auf dem Partnerknoten die Identität der ursprünglichen LIF an, einschließlich der WWPNe. Bevor der Status des Pfads zum übernommenen Knoten auf fehlerhaft geändert wird, erscheint die Schatten-LIF dem Host-MPIO-Stack als aktiver/optimierter Pfad, und die I/O wird verschoben. Dies reduziert I/O-Unterbrechungen, da der Host auch während Storage-Failover-Operationen immer die gleiche Anzahl an Pfaden zum Ziel sieht.

Bei persistenten Ports sollten die folgenden FCP-Port-Eigenschaften innerhalb des HA-Paares identisch sein:

- FCP-Portanzahl
- FCP-Portnamen
- FCP-Portgeschwindigkeiten
- FCP LIF WWPN-basierte Zonierung

Wenn eine dieser Eigenschaften innerhalb des HA-Paares nicht identisch ist, wird die folgende EMS-Meldung generiert:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Weitere Informationen zu persistenten Ports sind unter "NetApp Technischer Bericht 4080: Bewährte Verfahren für moderne SAN" zu finden.

Konfigurationsgrenzen für FC-Switches, die mit ONTAP Systemen verwendet werden

Fibre Channel Switches haben maximale Konfigurationsgrenzen, einschließlich der Anzahl der unterstützten Anmeldungen pro Port, Portgruppe, Blade und Switch. Die Switch-Hersteller dokumentieren ihre unterstützten Grenzwerte.

Jede FC logische Schnittstelle (LIF) meldet sich an einem FC-Switch-Port an. Die Gesamtzahl der Anmeldungen von einem einzelnen Target auf dem Node entspricht der Anzahl der LIFs plus einer Anmeldung für den zugrunde liegenden physischen Port. Die Konfigurationsgrenzen des Switch-Herstellers für Anmeldungen oder andere Konfigurationswerte dürfen nicht überschritten werden. Dies gilt auch für die auf der Host-Seite verwendeten Initiatoren in virtualisierten Umgebungen mit aktiviertem NPIV. Die Konfigurationsgrenzen des Switch-Herstellers für Anmeldungen dürfen weder für das Target noch für die in der Lösung verwendeten Initiatoren überschritten werden.

Brocade Switch-Grenzen

Die Konfigurationsgrenzen für Brocade Switches sind in den *Brocade Scalability Guidelines* zu finden.

Cisco Systems Switch-Grenzwerte

Die Konfigurationsgrenzen für Cisco Switches sind im "Cisco Konfigurationsgrenzen"Guide für Ihre Version der Cisco Switch Software zu finden.

Maximale Anzahl an unterstützten FC- und FCoE-Hops in ONTAP

Die Hop-Anzahl bezeichnet die Anzahl der Switches auf dem Pfad zwischen Initiator

(Host) und Ziel (Speichersystem). Die maximal unterstützte FC-Hop-Anzahl zwischen Host und Speichersystem variiert je nach Switch-Lieferant.

In der Dokumentation von Cisco Systems wird dieser Wert auch als *Durchmesser des SAN-Fabrics* bezeichnet.

Bei FCoE können FCoE Switches mit FC Switches verbunden werden. Für durchgängige FCoE-Verbindungen muss auf den FCoE Switches eine Firmware-Version ausgeführt werden, die Ethernet Inter-Switch-Links (ISLs) unterstützt.

Switch-Lieferant	Unterstützte Hop-Anzahl
Brocade	• 7 für FC • 5 für FCoE
Cisco	• 7 für FC • Bis zu 3 der Switches können FCoE Switches sein.

Warteschlangentiefe für ONTAP FC Hosts berechnen

Möglicherweise ist eine Anpassung der FC-Warteschlangentiefe auf dem Host erforderlich, um die maximalen Werte für ITNs pro Node und FC-Port-Fan-In zu erreichen. Die maximale Anzahl von LUNs und die Anzahl der HBAs, die eine Verbindung zu einem FC-Port herstellen können, sind durch die verfügbare Warteschlangentiefe an den FC-Zielports begrenzt.

Über diese Aufgabe

Die Warteschlangentiefe ist die Anzahl der E/A-Anforderungen (SCSI-Befehle), die gleichzeitig auf einem Speicherkontroller in die Warteschlange gestellt werden können. Jede E/A-Anforderung vom initiierenden HBA des Hosts an den Zieladapter des Speicherkontrollers belegt einen Eintrag in der Warteschlange. In der Regel entspricht eine höhere Warteschlangentiefe einer besseren Performance. Wird jedoch die maximale Warteschlangentiefe des Speicherkontrollers erreicht, weist dieser eingehende Befehle mit einer QFULL-Antwort zurück. Wenn eine große Anzahl von Hosts auf einen Speicherkontroller zugreift, ist eine sorgfältige Planung erforderlich, um QFULL-Zustände zu vermeiden, da diese die Systemleistung erheblich beeinträchtigen und auf manchen Systemen zu Fehlern führen können.

In einer Konfiguration mit mehreren Initiatoren (Hosts) sollten alle Hosts eine ähnliche Warteschlangentiefe aufweisen. Aufgrund der ungleichen Warteschlangentiefe zwischen Hosts, die über denselben Zielport mit dem Storage-Controller verbunden sind, wird Hosts mit geringerer Warteschlangentiefe der Zugriff auf Ressourcen durch Hosts mit größerer Warteschlangentiefe verwehrt.

Folgende allgemeine Empfehlungen können hinsichtlich des „Tuning“ der Warteschlangentiefe gegeben werden:

- Für kleine bis mittelgroße Systeme ist eine HBA-Warteschlangentiefe von 32 zu verwenden.
- Für große Systeme wird eine HBA-Warteschlangentiefe von 128 empfohlen.
- Für Ausnahmefälle oder Leistungstests empfiehlt sich eine Warteschlangenlänge von 256, um mögliche Warteschlangenprobleme zu vermeiden.
- Alle Hosts sollten ähnliche Warteschlangentiefen eingestellt haben, um allen Hosts gleichen Zugriff zu ermöglichen.

- Um Leistungseinbußen oder Fehler zu vermeiden, darf die Warteschlangentiefe des Ziel-FC-Ports am Speichercontroller nicht überschritten werden.

Schritte

1. Die Gesamtzahl der FC-Initiatoren in allen Hosts, die mit einem FC-Zielport verbunden sind, ermitteln.
2. Mit 128 multiplizieren.
   - Ist das Ergebnis kleiner als 2.048, sollte die Warteschlangentiefe für alle Initiatoren auf 128 gesetzt werden. Sie haben 15 Hosts, wobei jeweils ein Initiator an jeden der beiden Zielports des Storage Controllers angeschlossen ist. 15 × 128 = 1.920. Da 1.920 unter dem Gesamtlimit der Warteschlangentiefe von 2.048 liegt, kann die Warteschlangentiefe für alle Initiatoren auf 128 gesetzt werden.
   - Ist das Ergebnis größer als 2.048, gehen Sie zu Schritt 3. Sie haben 30 Hosts, wobei jeweils ein Initiator an jeden der beiden Zielports des Storage Controllers angeschlossen ist. 30 × 128 = 3.840. Da 3.840 größer als das Gesamtlimit der Warteschlangentiefe von 2.048 ist, sollte eine der Optionen unter Schritt 3 zur Behebung gewählt werden.
3. Wählen Sie eine der folgenden Optionen, um dem Storage Controller weitere Hosts hinzuzufügen.
   - Option 1:
     i. Weitere FC-Zielports hinzufügen.
     ii. Verteilen Sie Ihre FC-Initiatoren neu.
     iii. Wiederholen Sie die Schritte 1 und 2. + Die gewünschte Warteschlangentiefe von 3.840 überschreitet die verfügbare Warteschlangentiefe pro Port. Um dies zu beheben, kann jedem Controller ein FC-Zieladapter mit zwei Ports hinzugefügt werden, anschließend werden die FC-Switches so umkonfiguriert, dass 15 der 30 Hosts mit einem Satz von Ports und die verbleibenden 15 Hosts mit einem zweiten Satz von Ports verbunden sind. Die Warteschlangentiefe pro Port wird dadurch auf 15 × 128 = 1.920 reduziert.
   - Option 2:
     i. Jeder Host wird entsprechend seines erwarteten E/A-Bedarfs als “large” oder “small” bezeichnet.
     ii. Die Anzahl der großen Initiatoren ist mit 128 zu multiplizieren.
     iii. Die Anzahl der kleinen Initiatoren ist mit 32 zu multiplizieren.
     iv. Die beiden Ergebnisse werden addiert.
     v. Ist das Ergebnis kleiner als 2.048, sollte die Warteschlangentiefe für große Hosts auf 128 und die Warteschlangentiefe für kleine Hosts auf 32 eingestellt werden.
     vi. Ist das Ergebnis pro Port immer noch größer als 2.048, sollte die Warteschlangenlänge pro Initiator verringert werden, bis die Gesamtwarteschlangenlänge kleiner oder gleich 2.048 ist.



Zur Abschätzung der erforderlichen Warteschlangenlänge für einen bestimmten Durchsatz von E/A pro Sekunde gilt folgende Formel:

Erforderliche Warteschlangentiefe = (Anzahl der E/A pro Sekunde) × (Antwortzeit)

Wenn beispielsweise 40.000 E/A-Vorgänge pro Sekunde bei einer Reaktionszeit von 3 Millisekunden benötigt werden, ergibt sich die erforderliche Warteschlangentiefe zu 40.000 × (0,003) = 120.

Die maximale Anzahl an Hosts, die Sie mit einem Zielport verbinden können, beträgt 64, wenn Sie die Warteschlangenlänge auf die empfohlene Basislänge von 32 beschränken. Wenn jedoch eine Warteschlangenlänge von 128 gewählt wird, können maximal 16 Hosts mit einem Zielport verbunden werden.

Je größer die Warteschlangenlänge, desto weniger Hosts kann ein einzelner Zielport unterstützen. Falls die Anforderungen so sind, dass bei der Warteschlangenlänge keine Kompromisse möglich sind, ist es erforderlich, mehr Zielports zu verwenden.

Die gewünschte Warteschlangentiefe von 3.840 überschreitet die verfügbare Warteschlangentiefe pro Port. Es sind 10 „large“ Hosts mit hohem Storage-I/O-Bedarf und 20 „small“ Hosts mit geringem I/O-Bedarf vorhanden. Die Initiator-Warteschlangentiefe sollte auf den large Hosts auf 128 und auf den small Hosts auf 32 gesetzt werden.

Die resultierende Gesamttiefe der Warteschlange beträgt (10 × 128) + (20 × 32) = 1.920.

Sie können die verfügbare Warteschlangenlänge gleichmäßig auf alle Initiatoren verteilen.

Die daraus resultierende Warteschlangenlänge pro Initiator beträgt 2,048 ÷ 30 = 68.

Warteschlangentiefen für ONTAP SAN Hosts anpassen

Möglicherweise müssen Sie die Warteschlangenlängen auf Ihrem Host anpassen, um die maximalen Werte für ITNs pro Node und FC Port Fan-In zu erreichen. "die optimale Warteschlangenlänge berechnen" für Ihre Umgebung.

AIX-Hosts

Die Warteschlangentiefe auf AIX-Hosts kann mit dem `chdev` Befehl geändert werden. Änderungen, die mit dem `chdev` Befehl vorgenommen werden, bleiben nach einem Neustart erhalten.

Beispiele:

- Um die Warteschlangenlänge für das Gerät hdisk7 zu ändern, wird folgender Befehl verwendet:

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- Zum Ändern der Warteschlangenlänge für den fcs0 HBA wird folgender Befehl verwendet:

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  Der Standardwert für `num_cmd_elems` ist 200. Der Maximalwert ist 2.048.

> ⓘ Es kann erforderlich sein, den HBA offline zu nehmen, um `num_cmd_elems` zu ändern und ihn dann mit den Befehlen `rmdev -l fcs0 -R` und `makdev -l fcs0 -P` wieder online zu bringen.

HP-UX Hosts

Die LUN- oder Gerätewarteschlangentiefe auf HP-UX-Hosts kann mit dem Kernel-Parameter `scsi_max_qdepth` geändert werden. Die HBA-Warteschlangentiefe kann mit dem Kernel-Parameter `max_fcp_reqs` geändert werden.

- Der Standardwert für `scsi_max_qdepth` ist 8. Der Maximalwert ist 255.

  `scsi_max_qdepth`Die Einstellung kann im laufenden System dynamisch mit der `-u` Option des `kmtune` Befehls geändert werden. Die Änderung gilt für alle Geräte im System. Zum Beispiel

kann mit dem folgenden Befehl die LUN-Warteschlangentiefe auf 64 erhöht werden:

```
kmtune -u -s scsi_max_qdepth=64
```

Die Warteschlangenlänge für einzelne Gerätedateien kann mithilfe des `scsictl` Befehls geändert werden. Änderungen mit dem `scsictl` Befehl bleiben nach einem Systemneustart nicht erhalten. Die Warteschlangenlänge für eine bestimmte Gerätedatei kann mit folgendem Befehl angezeigt und geändert werden:

```
scsictl -a /dev/rdsk/c2t2d0

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

- Der Standardwert für `max_fcp_reqs` ist 512. Der Maximalwert ist 1024.

  Der Kernel muss neu kompiliert und das System neu gestartet werden, damit die Änderungen `max_fcp_reqs` wirksam werden. Um beispielsweise die HBA-Warteschlangentiefe auf 256 zu ändern, kann folgender Befehl verwendet werden:

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Solaris Hosts

Sie können die LUN- und HBA-Warteschlangentiefe für Ihre Solaris Hosts festlegen.

- Für die LUN-Warteschlangentiefe gilt: Die Anzahl der auf einem Host verwendeten LUNs multipliziert mit der Drosselung pro LUN (lun-queue-depth) muss kleiner oder gleich dem Wert tgt-queue-depth auf dem Host sein.
- Für die Warteschlangentiefe in einem Sun-Stack: Die nativen Treiber erlauben keine Einstellungen pro LUN oder pro Ziel `max_throttle` auf HBA-Ebene. Die empfohlene Methode zur Festlegung des `max_throttle` Werts für native Treiber ist auf Geräte-Typ-Ebene (VID_PID) in den `/kernel/drv/sd.conf` und `/kernel/drv/ssd.conf` Dateien. Das Host Utility setzt diesen Wert auf 64 für MPxIO Konfigurationen und auf 8 für Veritas DMP Konfigurationen.

Schritte

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. Suchen nach `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   Der Standardwert ist bei der Installation auf 32 festgelegt.

4. Der gewünschte Wert wird entsprechend der Konfiguration Ihrer Umgebung festgelegt.
5. Die Datei speichern.
6. Den Host mit dem `sync; sync; sync; reboot -- -r` Befehl neu starten.

VMware Hosts für einen QLogic HBA

Mit dem `esxcfg-module` Befehl lassen sich die HBA Zeitüberschreitungseinstellungen ändern. Eine

manuelle Aktualisierung der `esx.conf` Datei wird nicht empfohlen.

Schritte

1. Melden Sie sich an der Service-Konsole als Root-Benutzer an.
2. Mit dem `#vmkload_mod -l` Befehl lässt sich überprüfen, welches Qlogic HBA Modul aktuell geladen ist.
3. Für eine einzelne Instanz einer Qlogic HBA wird folgender Befehl ausgeführt:

   ```
   #esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
   ```

   Dieses Beispiel verwendet das Modul qla2300_707. Das passende Modul ist entsprechend der Ausgabe von `vmkload_mod -l` zu wählen.

4. Die Änderungen werden mit folgendem Befehl gespeichert:

   ```
   #/usr/sbin/esxcfg-boot -b
   ```

5. Starten Sie den Server mit folgendem Befehl neu:

   ```
   #reboot
   ```

6. Die Änderungen werden mit den folgenden Befehlen bestätigt:
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

VMware Hosts für einen Emulex HBA

Mit dem `esxcfg-module` Befehl lassen sich die HBA Zeitüberschreitungseinstellungen ändern. Eine manuelle Aktualisierung der `esx.conf` Datei wird nicht empfohlen.

Schritte

1. Melden Sie sich an der Service-Konsole als Root-Benutzer an.
2. Mit dem `#vmkload_mod -l grep lpfc`Befehl lässt sich überprüfen, welcher Emulex HBA aktuell geladen ist.
3. Für eine einzelne Instanz einer Emulex HBA ist folgender Befehl einzugeben:

   ```
   #esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
   ```

   Je nach HBA-Modell kann das Modul entweder lpfcdd_7xx oder lpfcdd_732 sein. Der obige Befehl verwendet das Modul lpfcdd_7xx. Das passende Modul sollte entsprechend dem Ergebnis von `vmkload_mod -l` verwendet werden.

   Durch Ausführen dieses Befehls wird die LUN-Warteschlangentiefe für den durch lpfc0 repräsentierten HBA auf 16 gesetzt.

4. Für mehrere Instanzen einer Emulex HBA ist folgender Befehl auszuführen:

   ```
   a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
   lpfcdd_7xx
   ```

   Die LUN-Warteschlangenlänge für lpfc0 und die LUN-Warteschlangenlänge für lpfc1 ist auf 16 eingestellt.

5. Führen Sie den folgenden Befehl aus:

```
#esxcfg-boot -b
```

6. Neustart mit `#reboot`.

Windows Hosts für einen Emulex HBA

Auf Windows-Hosts kann das `LPUTILNT` Dienstprogramm verwendet werden, um die Warteschlangenlänge für Emulex HBAs zu aktualisieren.

Schritte

1. Das Dienstprogramm `LPUTILNT` im Verzeichnis `C:\WINNT\system32` ausführen.
2. Im Menü auf der rechten Seite **Laufwerksparameter** auswählen.
3. Scrollen Sie nach unten und doppelklicken Sie auf **QueueDepth**.

> Wenn Sie **QueueDepth** größer als 150 einstellen, muss auch der folgende Wert in der Windows-Registrierung entsprechend erhöht werden:
>
> `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

Windows Hosts für einen Qlogic HBA

Auf Windows-Hosts können Sie das `SANsurfer` HBA-Manager-Dienstprogramm verwenden, um die Warteschlangenlängen für Qlogic HBAs zu aktualisieren.

Schritte

1. Das `SANsurfer`HBA Manager Dienstprogramm ausführen.
2. Klicken Sie auf **HBA port** > **Einstellungen**.
3. Im Listenfeld auf **Erweiterte HBA-Porteinstellungen** klicken.
4. Der `Execution Throttle`Parameter wird aktualisiert.

Linux Hosts für Emulex HBA

Sie können die Warteschlangenlängen eines Emulex HBA auf einem Linux-Host aktualisieren. Damit die Aktualisierungen nach einem Neustart erhalten bleiben, ist das Erstellen eines neuen RAM-Disk-Images und ein anschließender Neustart des Hosts erforderlich.

Schritte

1. Die zu ändernden Parameter für die Warteschlangentiefe identifizieren:

```
modinfo lpfc|grep queue_depth
```

   Es wird eine Liste der Warteschlangenlängenparameter mit ihrer Beschreibung angezeigt. Abhängig von Ihrer Betriebssystemversion können Sie einen oder mehrere der folgenden Warteschlangenlängenparameter ändern:

   - `lpfc_lun_queue_depth`: Maximale Anzahl von FC-Befehlen, die einer bestimmten LUN (uint) zugeordnet werden können

- `lpfc_hba_queue_depth`: Maximale Anzahl von FC-Befehlen, die an einen lpfc HBA (uint) in die Warteschlange gestellt werden können
- `lpfc_tgt_queue_depth`: Maximale Anzahl von FC-Befehlen, die an einen bestimmten Zielport in die Warteschlange gestellt werden können (uint)

  Der `lpfc_tgt_queue_depth`Parameter ist nur für Red Hat Enterprise Linux 7.x Systeme, SUSE Linux Enterprise Server 11 SP4 Systeme und 12.x Systeme anwendbar.

2. Die Warteschlangenlängen werden aktualisiert, indem die Warteschlangenlängenparameter zur `/etc/modprobe.conf` Datei für ein Red Hat Enterprise Linux 5.x System und zur `/etc/modprobe.d/scsi.conf` Datei für ein Red Hat Enterprise Linux 6.x oder 7.x System oder ein SUSE Linux Enterprise Server 11.x oder 12.x System hinzugefügt werden.

   Je nach Version Ihres Betriebssystems lassen sich einer oder mehrere der folgenden Befehle hinzufügen:

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. Ein neues RAM-Disk-Image wird erstellt, anschließend wird der Host neu gestartet, damit die Aktualisierungen auch nach Neustarts erhalten bleiben.

   Weitere Informationen enthält die "Systemadministration" für Ihre Version des Linux-Betriebssystems.

4. Es sollte sichergestellt sein, dass die Werte für die Warteschlangenlänge für jeden der geänderten Warteschlangenlängen-Parameter aktualisiert wurden:

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   Der aktuelle Wert der Warteschlangenlänge wird angezeigt.

Linux Hosts für QLogic HBA

Sie können die Warteschlangentiefe eines QLogic-Treibers auf einem Linux-Host aktualisieren. Damit die Aktualisierungen nach einem Neustart erhalten bleiben, ist das Erstellen eines neuen RAM-Disk-Images und ein anschließender Neustart des Hosts erforderlich. Die Warteschlangentiefe des QLogic HBA kann über die QLogic HBA-Management-GUI oder die Befehlszeilenschnittstelle (CLI) angepasst werden.

Diese Aufgabe zeigt, wie die QLogic HBA CLI verwendet wird, um die QLogic HBA Warteschlangentiefe zu ändern

Schritte

1. Den zu ändernden Parameter für die Gerätewarteschlangenlänge identifizieren:

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   Sie können nur den `ql2xmaxqdepth` Parameter „Warteschlangentiefe“ ändern, der die maximale Warteschlangentiefe angibt, die für jede LUN festgelegt werden kann. Der Standardwert beträgt 64 für RHEL 7.5 und später. Der Standardwert beträgt 32 für RHEL 7.4 und früher.

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. Der Wert für die Gerätewarteschlangenlänge wird aktualisiert:
   - Wenn die Änderungen dauerhaft gespeichert werden sollen, sind die folgenden Schritte erforderlich:
     i. Die Warteschlangentiefen werden aktualisiert, indem der Parameter „queue depth“ zur `/etc/modprobe.conf` Datei für ein Red Hat Enterprise Linux 5.x System und zur `/etc/modprobe.d/scsi.conf` Datei für ein Red Hat Enterprise Linux 6.x oder 7.x System oder ein SUSE Linux Enterprise Server 11.x oder 12.x System hinzugefügt wird: `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. Ein neues RAM-Disk-Image wird erstellt, anschließend wird der Host neu gestartet, damit die Aktualisierungen auch nach Neustarts erhalten bleiben.

     Weitere Informationen enthält die "Systemadministration" für Ihre Version des Linux-Betriebssystems.
   - Wenn der Parameter nur für die aktuelle Sitzung geändert werden soll, ist folgender Befehl auszuführen:

     `echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

     Im folgenden Beispiel ist die Warteschlangentiefe auf 128 eingestellt.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. Es wird überprüft, ob die Werte für die Warteschlangentiefe aktualisiert wurden:

   `cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

   Der aktuelle Wert der Warteschlangenlänge wird angezeigt.

4. Die Warteschlangentiefe des QLogic HBA kann durch Aktualisierung des Firmware-Parameters `Execution Throttle` aus dem QLogic HBA BIOS geändert werden.
   a. Anmeldung an der QLogic HBA-Management-CLI:

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. Im Hauptmenü die Option `Adapter Configuration` auswählen.

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

```
QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

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


        Please Enter Selection: 2
```

c. Aus der Liste der Adapterkonfigurationsparameter die `HBA Parameters` Option auswählen.

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. Aus der Liste der HBA-Ports den erforderlichen HBA-Port auswählen.

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
```

```
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


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

Die Details des HBA-Ports werden angezeigt.

e. Im Menü „HBA-Parameter“ die `Display HBA Parameters` Option auswählen, um den aktuellen Wert der `Execution Throttle` Option anzuzeigen.

Der Standardwert der `Execution Throttle` Option ist 65535.

```
HBA Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
-------------------------------------------------------------------------
--------
Connection Options            : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                     : Auto
Frame Size                    : 2048
Hard Loop ID                  : 0
Loop Reset Delay (seconds)    : 5
```

```
Enable Host HBA BIOS           : Enabled
Enable Hard Loop ID            : Disabled
Enable FC Tape Support         : Enabled
Operation Mode                 : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)  : 0
**Execution Throttle             : 65535**
Login Retry Count              : 8
Port Down Retry Count          : 30
Enable LIP Full Login          : Enabled
Link Down Timeout (seconds)    : 30
Enable Target Reset            : Enabled
LUNs Per Target                : 128
Out Of Order Frame Assembly    : Disabled
Enable LR Ext. Credits         : Disabled
Enable Fabric Assigned WWN     : N/A

Press <Enter> to continue:
```

a. **Eingabetaste** drücken, um fortzufahren.

b. Im Menü „HBA-Parameter“ die Option `Configure HBA Parameters` zum Ändern der HBA-Parameter auswählen.

c. Im Menü „Parameter konfigurieren“ die Option `Execute Throttle` auswählen und den Wert dieses Parameters aktualisieren.

```
Configure Parameters Menu

=====================================================
HBA            : 2 Port: 1
SN             : BFD1524C78510
HBA Model      : QLE2562
HBA Desc.      : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version     : 8.01.02
WWPN           : 21-00-00-24-FF-8D-98-E0
WWNN           : 20-00-00-24-FF-8D-98-E0
Link           : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
```

```
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. **Eingabetaste** drücken, um fortzufahren.

e. Im Menü „Parameter konfigurieren“ die Option `Commit Changes` zum Speichern der Änderungen auswählen.

f. Das Menü wird beendet.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.