



ISL-Anforderungen

ONTAP MetroCluster

NetApp
April 25, 2024

This PDF was generated from <https://docs.netapp.com/de-de/ontap-metrocluster/install-ip/overview-isl-requirements.html> on April 25, 2024. Always check docs.netapp.com for the latest.

Inhalt

- ISL-Anforderungen 1
 - ISL-Anforderungen im Überblick 1
 - Von NetApp validierte und MetroCluster-konforme Switches 1
 - Überlegungen für ISLs 2
 - Überlegungen bei der Bereitstellung von MetroCluster in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken 5
 - Überlegungen zur Verwendung von MetroCluster-konformen Switches 13
 - Beispiele für MetroCluster Netzwerktopologien 20

ISL-Anforderungen

ISL-Anforderungen im Überblick

Überprüfen Sie, ob Ihre MetroCluster IP-Konfiguration und Ihr Netzwerk alle ISL-Anforderungen (Inter-Switch Link) erfüllen. Obwohl bestimmte Anforderungen nicht auf Ihre Konfiguration zutreffen, sollten Sie dennoch alle ISL-Anforderungen kennen, um ein besseres Verständnis der Gesamtkonfiguration zu erhalten.

Die folgende Tabelle bietet einen Überblick über die in diesem Abschnitt behandelten Themen.

Titel	Beschreibung
"Von NetApp validierte und MetroCluster-konforme Switches"	<p>Beschreibt die Switch-Anforderungen.</p> <p>Gilt für alle in MetroCluster-Konfigurationen verwendeten Switches, einschließlich Backend-Switches.</p>
"Überlegungen für ISLs"	<p>Beschreibt die ISL-Anforderungen.</p> <p>Gilt für alle MetroCluster Konfigurationen, unabhängig von der Netzwerktopologie und ob Sie NetApp validierte Switches oder MetroCluster konforme Switches verwenden.</p>
"Überlegungen bei der Bereitstellung von MetroCluster in einem gemeinsam genutzten Layer-2- oder Layer-3-Netzwerk"	<p>Beschreibt die Anforderungen für gemeinsam genutzte Layer-2- oder Layer-3-Netzwerke.</p> <p>Gilt für alle Konfigurationen mit Ausnahme von MetroCluster Konfigurationen mit von NetApp validierten Switches und mit direkt verbundenen ISLs.</p>
"Überlegungen beim Einsatz von MetroCluster-kompatiblen Switches"	<p>Beschreibt die Anforderungen für MetroCluster-konforme Switches.</p> <p>Gilt für alle MetroCluster Konfigurationen ohne NetApp validierte Switches.</p>
"Beispiele für MetroCluster Netzwerktopologien"	<p>Enthält Beispiele verschiedener MetroCluster-Netzwerktopologien.</p> <p>Gilt für alle MetroCluster Konfigurationen.</p>

Von NetApp validierte und MetroCluster-konforme Switches

Alle in der Konfiguration verwendeten Switches, einschließlich Backend-Switches, müssen entweder NetApp-validiert oder MetroCluster konform sein.

Von NetApp validierte Switches

Ein Switch wird von NetApp validiert, wenn er die folgenden Anforderungen erfüllt:

- Der Switch wird von NetApp im Rahmen der MetroCluster IP Konfiguration bereitgestellt
- Der Switch ist im aufgeführt "[NetApp Hardware Universe](#)" Als unterstützter Switch unter *MetroCluster-over-IP-connections*

- Der Switch wird nur verwendet, um MetroCluster IP-Controller und in einigen Konfigurationen NS224-Laufwerk-Shelfs zu verbinden
- Der Switch wird mit der von NetApp bereitgestellten Referenzkonfigurationsdatei (RCF) konfiguriert

Jeder Switch, der diese Anforderungen nicht erfüllt, ist **nicht** ein von NetApp validierter Switch.

MetroCluster-konforme Switches

Ein MetroCluster-konformer Switch ist nicht von NetApp validiert, kann aber in einer MetroCluster IP-Konfiguration verwendet werden, wenn er bestimmte Anforderungen und Konfigurationsrichtlinien erfüllt.



NetApp bietet keine Services zur Fehlerbehebung oder Konfiguration von Support für nicht validierte MetroCluster-kompatible Switches.

Überlegungen für ISLs

Inter-Switch Links (ISLs), die MetroCluster-Datenverkehr auf allen MetroCluster IP-Konfigurationen und Netzwerktopologien übertragen, haben bestimmte Anforderungen. Diese Anforderungen gelten für alle ISLs, die MetroCluster-Datenverkehr tragen, unabhängig davon, ob die ISLs direkt sind oder von den Kunden-Switches gemeinsam genutzt werden.

Allgemeine MetroCluster-ISL-Anforderungen

Folgendes gilt für ISLs in allen MetroCluster IP-Konfigurationen:

- Beide Fabrics müssen die gleiche Anzahl von ISLs aufweisen.
- ISLs in einer Fabric müssen alle dieselbe Geschwindigkeit und Länge haben.
- ISLs müssen in beiden Fabrics dieselbe Geschwindigkeit und Länge haben.
- Die maximale unterstützte Differenz im Abstand zwischen Fabric 1 und Fabric 2 beträgt 20 km oder 0,2 ms.
- Die ISLs müssen über dieselbe Topologie verfügen. Sie sollten beispielsweise alle direkte Links sein, oder wenn die Konfiguration WDM verwendet, müssen alle WDM verwenden.
- Die ISL-Geschwindigkeit muss mindestens 10 Gbit/s betragen.
- Es muss mindestens ein 10 Gbit/s-ISL-Port pro Fabric geben.

Grenzwerte für Latenz und Paketverlust in den ISLs

Folgendes gilt für den Rundreiseverkehr zwischen den MetroCluster-IP-Switches an Standort_A und Standort_B, wobei die MetroCluster-Konfiguration im stabilen Betrieb ist:

- Mit zunehmender Entfernung zwischen zwei MetroCluster Standorten steigt die Latenz, in der Regel im Bereich von 1 ms Paketumlaufzeit pro 100 km (62 Meilen). Die Latenz hängt auch von der SLA (Network Service Level Agreement) ab, was die Bandbreite der ISL-Verbindungen, die Paketdrop-Rate und den Jitter im Netzwerk betrifft. Geringe Bandbreite, hoher Jitter und zufällige Paketabbrüche führen zu verschiedenen Wiederherstellungsmechanismen durch die Switches oder die TCP-Engine auf den Controller-Modulen für eine erfolgreiche Paketzustellung. Diese Recovery-Mechanismen können die Latenz insgesamt erhöhen. Spezifische Informationen zur Latenz bei und für die maximale Entfernung

Ihrer Konfiguration finden Sie im "[Hardware Universe](#):"

- Geräte, die zur Latenz beitragen, müssen berücksichtigt werden.
- Der "[Hardware Universe](#):" Bietet die Entfernung in km. Sie müssen für alle 100 km 1 ms zuweisen. Der maximale Abstand wird durch das zuerst erreichte definiert, entweder durch die maximale Rundreisezeit (RTT) in ms oder durch den Abstand in km Beispiel: Wenn *das Hardware Universe* eine Entfernung von 300 km auflistet, die auf 3 ms übersetzt wird, kann Ihr ISL nicht weiter als 300 km sein und der maximale RTT nicht mehr als 3 ms überschreiten – je nachdem, welcher Wert zuerst erreicht wird.
- Paketverlust muss kleiner oder gleich 0.01 % sein. Der maximale Paketverlust ist die Summe aller Verluste auf allen Verbindungen auf dem Pfad zwischen den MetroCluster-Knoten und der Verlust auf den lokalen MetroCluster-IP-Schnittstellen.
- Der unterstützte Jitter-Wert beträgt 3 ms für die Rundreise (oder 1,5 ms für die einfache Strecke).
- Das Netzwerk sollte die für den MetroCluster-Datenverkehr erforderliche SLA-Bandbreite zuweisen und aufrechterhalten, unabhängig von Mikroplatausbrüchen und Spitzen im Datenverkehr.
- Bei Verwendung von ONTAP 9.7 oder höher muss das Zwischennetzwerk zwischen den beiden Standorten eine Mindestbandbreite von 4,5 Gbit/s für die MetroCluster IP-Konfiguration bereitstellen.

Hinweise zu Transceiver und Kabeln

SFPs oder QSFPs, die vom Geräteanbieter unterstützt werden, werden von den MetroCluster ISLs unterstützt. SFP-Module und QSFPs von NetApp oder vom Geräteanbieter müssen von der Switch- und Switch-Firmware unterstützt werden.

Beim Anschließen der Controller an die Switches und die lokalen Cluster-ISLs müssen Sie die Transceiver und Kabel verwenden, die von NetApp mit dem MetroCluster bereitgestellt werden.

Wenn Sie einen QSFP-SFP-Adapter verwenden, hängt es vom Switch-Modell und der Firmware ab, ob Sie den Port im Breakout- oder im nativen Geschwindigkeitsmodus konfigurieren. Beispielsweise muss der Port bei der Verwendung eines QSFP-SFP-Adapters mit Cisco 9336C Switches mit der NX-OS-Firmware 9.x oder 10.x im nativen Geschwindigkeitsmodus konfiguriert werden.



Wenn Sie eine RCF konfigurieren, überprüfen Sie, ob Sie den richtigen Geschwindigkeitsmodus auswählen oder einen Port mit einem geeigneten Geschwindigkeitsmodus verwenden.

Verwenden von xWDM, TDM und externen Verschlüsselungsgeräten

Wenn Sie xWDM-/TDM-Geräte oder -Geräte verwenden, die in einer MetroCluster IP-Konfiguration verschlüsselt werden, muss Ihre Umgebung die folgenden Anforderungen erfüllen:

- Beim Anschluss der MetroCluster IP-Switches an den xWDM/TDM müssen die externen Verschlüsselungsgeräte oder xWDM/TDM-Geräte vom Hersteller für den Switch und die Firmware zertifiziert sein. Die Zertifizierung muss den Betriebsmodus abdecken (z. B. Trunking und Verschlüsselung).
- Die gesamte End-to-End-Latenz und der Jitter, einschließlich der Verschlüsselung, darf nicht höher sein als die in der IMT und in dieser Dokumentation angegebene Höchstmenge.

Unterstützte Anzahl von ISLs und Breakout-Kabeln

Die folgende Tabelle zeigt die unterstützte maximale Anzahl von ISLs, die auf einem MetroCluster IP-Switch mithilfe der RCF-Konfiguration (Reference Configuration File) konfiguriert werden können.

MetroCluster IP-Switch-Modell	Porttyp	Maximale Anzahl von ISLs
Von Broadcom unterstützte BES-53248-Switches	Native Ports	4 ISLs mit 10 Gbit/s oder 25 Gbit/s.
Von Broadcom unterstützte BES-53248-Switches	Native Ports (Hinweis 1)	2 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 3132Q-V	Native Ports	6 ISLs mit 40 Gbit/s.
Cisco 3132Q-V	Breakout-Kabel	16 ISLs mit 10 Gbit/s
Cisco 3232C	Native Ports	6 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 3232C	Breakout-Kabel	16 ISLs mit 10 Gbit/s
Cisco 9336C-FX2 (kein Anschluss von NS224-Shelfs)	Native Ports	6 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 9336C-FX2 (kein Anschluss von NS224-Shelfs)	Breakout-Kabel	16 ISLs mit 10
Cisco 9336C-FX2 (Anschluss von NS224-Shelfs)	Native Ports (Hinweis 2)	4 ISLs mit 40 Gbit/s oder 100 Gbit/s.
Cisco 9336C-FX2 (Anschluss von NS224-Shelfs)	Breakout-Kabel (Hinweis 2)	16 ISLs mit 10 Gbit/s
NVIDIA SN2100	Native Ports (Hinweis 2)	2 ISLs mit 40 Gbit/s oder 100 Gbit/s.
NVIDIA SN2100	Breakout-Kabel (Hinweis 2)	8 ISLs mit 10 Gbit/s oder 25 Gbit/s.

Hinweis 1: Die Verwendung von 40 Gbit/s oder 100 Gbit/s ISLs auf einem BES-53248 Switch erfordert eine zusätzliche Lizenz.

Hinweis 2: Die gleichen Ports werden für den nativen Geschwindigkeits- und Breakout-Modus verwendet. Sie müssen beim Erstellen der RCF-Datei Ports im einheitlichen Geschwindigkeitsmodus oder im Breakout-Modus verwenden.

- Alle ISLs an einem MetroCluster IP-Switch müssen die gleiche Geschwindigkeit aufweisen. Es wird nicht unterstützt, verschiedene ISL-Ports mit unterschiedlichen Geschwindigkeiten gleichzeitig zu verwenden.
- Um eine optimale Leistung zu erzielen, sollten Sie mindestens eine 40-Gbit/s-ISL pro Netzwerk verwenden. Sie sollten für FAS9000, AFF A700 oder andere Plattformen mit hoher Kapazität keine ISL mit 10 Gbit/s pro Netzwerk verwenden.



NetApp empfiehlt, eine kleine Anzahl von ISLs mit hoher Bandbreite zu konfigurieren, anstatt eine hohe Anzahl von ISLs mit niedriger Bandbreite. Es wird beispielsweise bevorzugt, eine 40-Gbit/s-ISL anstelle von vier 10-Gbit/s-ISLs zu konfigurieren. Bei Verwendung mehrerer ISLs kann sich der statistische Lastausgleich auf den maximalen Durchsatz auswirken. Bei einer ungleichmäßigen Verteilung kann der Durchsatz auf einen einzelnen ISL reduziert werden.

Überlegungen bei der Bereitstellung von MetroCluster in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken

Je nach Ihren Anforderungen können Sie gemeinsam genutzte Layer-2- oder Layer-3-Netzwerke zur Implementierung von MetroCluster verwenden.

Ab ONTAP 9.6 können MetroCluster IP-Konfigurationen mit unterstützten Cisco Switches vorhandene Netzwerke für ISLs (Inter-Switch Links) gemeinsam nutzen, anstatt dedizierte MetroCluster-ISLs zu verwenden. Diese Topologie wird als *Shared Layer 2 Networks* bezeichnet.

Ab ONTAP 9.9 können MetroCluster IP-Konfigurationen mit IP-Routing (Layer 3)-Backend-Verbindungen implementiert werden. Diese Topologie wird als *Shared Layer 3 Networks* bezeichnet.



- Sie müssen überprüfen, ob Sie über ausreichende Netzwerkkapazität verfügen und ob die ISL-Größe für Ihre Konfiguration geeignet ist. Eine niedrige Latenz ist für die Replizierung von Daten zwischen den MetroCluster Standorten von großer Bedeutung. Latenzprobleme auf diesen Verbindungen können sich nachteilig auf das Client-I/O auswirken
- Alle Verweise auf MetroCluster Backend-Switches beziehen sich auf NetApp validierte Switches oder MetroCluster konforme Switches. Siehe "[Von NetApp validierte und MetroCluster-konforme Switches](#)" Entnehmen.

ISL-Anforderungen für Layer-2- und Layer-3-Netzwerke

Folgendes gilt für Layer-2- und Layer-3-Netzwerke:

- Die Geschwindigkeit und Anzahl der ISLs zwischen den MetroCluster Switches und den mittleren Netzwerk-Switches müssen nicht übereinstimmen. Ebenso muss die Geschwindigkeit zwischen den mittleren Netzwerk-Switches nicht übereinstimmen.

MetroCluster Switches können beispielsweise über eine 40-Gbit/s-ISL mit den Intermediate Switches verbunden werden, wobei die Intermediate Switches über zwei 100-Gbit/s-ISLs miteinander verbunden werden können.

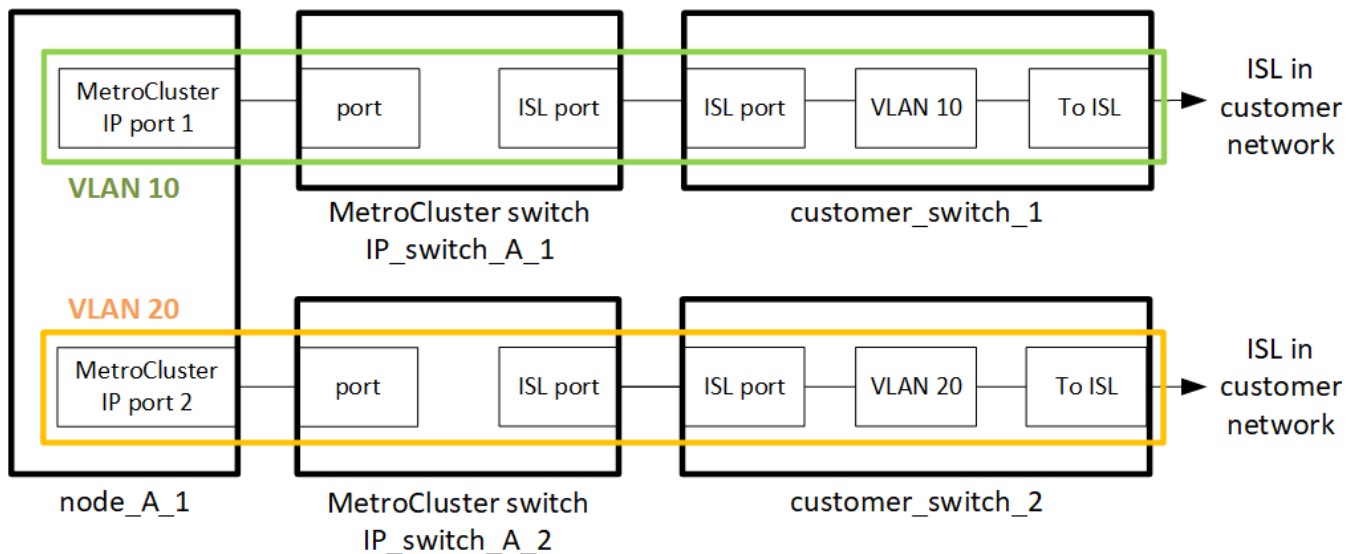
- Die Netzwerküberwachung sollte im Zwischennetzwerk konfiguriert werden, um die ISLs auf Auslastung, Fehler (Abgänge, Verbindungsklappen, Beschädigungen usw.) zu überwachen. und Ausfällen.
- Die MTU-Größe muss für alle Ports mit MetroCluster-End-to-End-Datenverkehr auf 9216 eingestellt sein.
- Kein anderer Datenverkehr kann mit einer höheren Priorität konfiguriert werden als Class of Service (COS) 5.
- Die explizite Staubenachrichtigung (ECN) muss auf allen Pfaden konfiguriert werden, die End-to-End-MetroCluster-Datenverkehr übertragen.
- ISLs, die MetroCluster Traffic tragen, müssen native Links zwischen den Switches sein.

Link-Sharing-Dienste wie Multiprotocol Label Switching (MPLS)-Links werden nicht unterstützt.

- Die Layer-2-VLANs müssen nativ über die Standorte hinweg eingesetzt werden. VLAN-Overlay wie Virtual Extensible LAN (VXLAN) wird nicht unterstützt.
- Die Anzahl der Zwischenschalter ist nicht begrenzt. NetApp empfiehlt jedoch, die Anzahl der Switches auf die erforderliche Mindestzahl zu beschränken.
- ISLs in MetroCluster Switches sind mit folgenden Konfigurationen konfiguriert:
 - Switch Port-Modus 'Trunk' als Teil eines LACP Port-Channels
 - Die MTU-Größe beträgt 9216
 - Es ist kein natives VLAN konfiguriert
 - Nur VLANs, die standortübergreifenden MetroCluster-Datenverkehr übertragen, sind zulässig
 - Das Standard-VLAN des Switches ist nicht zulässig

Überlegungen für Layer-2-Netzwerke

Die MetroCluster Backend-Switches sind mit dem Kundennetzwerk verbunden.



Die vom Kunden bereitgestellten Zwischenschalter müssen die folgenden Anforderungen erfüllen:

- Das Zwischennetzwerk muss die gleichen VLANs zwischen den Standorten bereitstellen. Dies muss mit den in der RCF-Datei festgelegten MetroCluster-VLANs übereinstimmen.
- Der RcfFileGenerator erlaubt das Erstellen einer RCF-Datei nicht mit VLANs, die von der Plattform nicht unterstützt werden.
- Der RcfFileGenerator kann beispielsweise die Verwendung bestimmter VLAN-IDs einschränken, wenn diese für die zukünftige Verwendung vorgesehen sind. Im Allgemeinen sind reservierte VLANs bis einschließlich 100.
- Layer-2-VLANs mit IDs, die zu den MetroCluster-VLAN-IDs passen, müssen das gemeinsam genutzte Netzwerk umfassen.

VLAN-Konfiguration in ONTAP

Sie können das VLAN nur während der Schnittstellenerstellung angeben. Nachdem die MetroCluster-Schnittstellen erstellt wurden, kann die VLAN-ID nicht mehr geändert werden. Sie können andere VLANs während der Schnittstellenerstellung konfigurieren, müssen jedoch im Bereich von 10 bis 20 oder im Bereich von 101 bis 4096 liegen (oder die vom Switch-Anbieter unterstützte Zahl, je nachdem, welcher Wert die

niedrigere Zahl ist).



Einige Switch-Anbieter reservieren möglicherweise die Nutzung bestimmter VLANs.

Für die folgenden Systeme ist keine VLAN-Konfiguration innerhalb von ONTAP erforderlich. Das VLAN wird durch die Switch-Port-Konfiguration festgelegt:

- FAS8200 UND AFF A300
- AFF A320
- FAS9000 und AFF A700
- AFF A800, ASA A800, AFF C800 und ASA C800



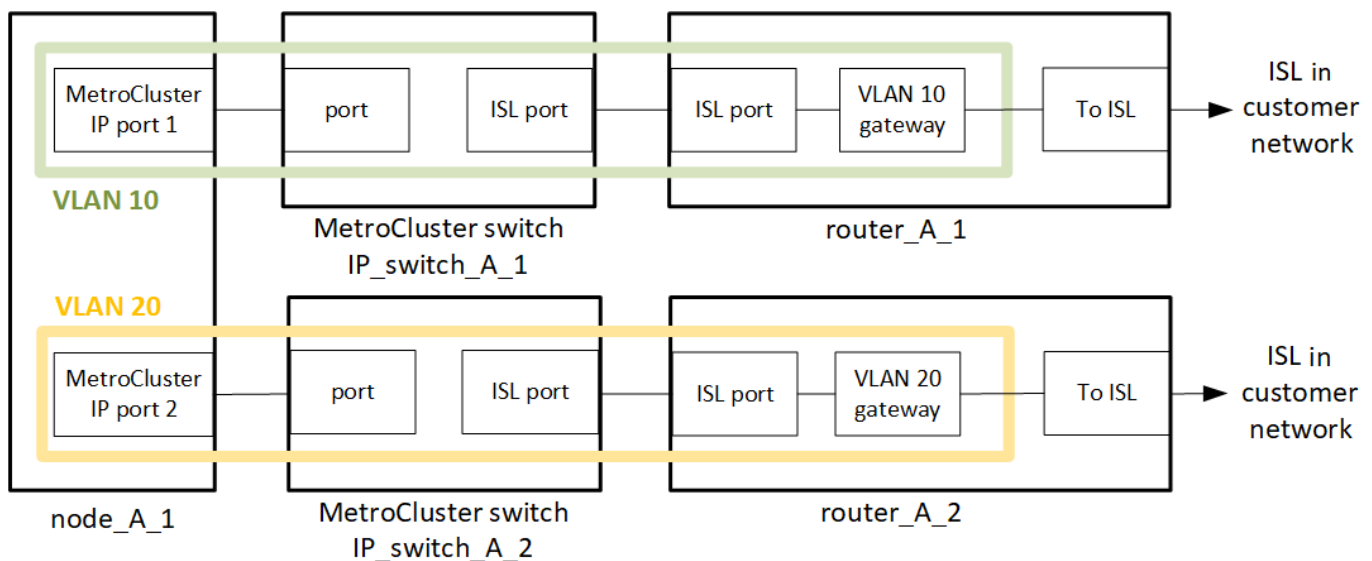
Die oben aufgeführten Systeme können mit VLANs 100 und niedriger konfiguriert werden. Einige VLANs in diesem Bereich sind jedoch möglicherweise für andere oder zukünftige Zwecke reserviert.

Bei allen anderen Systemen müssen Sie das VLAN konfigurieren, wenn Sie die MetroCluster-Schnittstellen in ONTAP erstellen. Es gelten die folgenden Einschränkungen:

- Das Standard-VLAN ist 10 und 20
- Wenn Sie ONTAP 9.7 oder früher verwenden, können Sie nur die Standard-VLAN 10 und 20 verwenden.
- Wenn Sie ONTAP 9.8 oder höher verwenden, können Sie das Standard-VLAN 10 und 20 verwenden, und ein VLAN über 100 (101 und höher) kann auch verwendet werden.

Überlegungen für Layer-3-Netzwerke

Die Back-End-Switches von MetroCluster sind mit dem gerouteten IP-Netzwerk verbunden, entweder direkt mit Routern (wie im folgenden vereinfachten Beispiel dargestellt) oder über andere intervenierenden Switches.



Die MetroCluster Umgebung ist wie in beschrieben als MetroCluster IP-Standardkonfiguration konfiguriert und verkabelt "[Konfigurieren Sie die Hardwarekomponenten von MetroCluster](#)". Wenn Sie das Installations- und Verkabelungsverfahren durchführen, müssen Sie die für eine Layer-3-Konfiguration spezifischen Schritte ausführen. Folgendes gilt für Layer-3-Konfigurationen:

- Sie können MetroCluster-Switches direkt an den Router oder an einen oder mehrere dazwischenliegenden Switches anschließen.
- Sie können MetroCluster IP-Schnittstellen direkt an den Router oder an einen der dazwischen liegenden Switches anschließen.
- Das VLAN muss auf das Gateway-Gerät erweitert werden.
- Sie verwenden das `-gateway parameter` So konfigurieren Sie die IP-Schnittstellenadresse des MetroCluster mit einer IP-Gateway-Adresse.
- Die VLAN-IDs für die MetroCluster-VLANs müssen an jedem Standort identisch sein. Die Subnetze können jedoch anders sein.
- Dynamisches Routing wird für den MetroCluster-Datenverkehr nicht unterstützt.
- Die folgenden Funktionen werden nicht unterstützt:
 - MetroCluster Konfigurationen mit acht Nodes
 - Aktualisieren einer MetroCluster-Konfiguration mit vier Nodes
 - Umstellung von MetroCluster FC auf MetroCluster IP
- An jedem MetroCluster Standort sind zwei Subnetze erforderlich – eins in jedem Netzwerk.
- Die Auto-IP-Zuweisung wird nicht unterstützt.

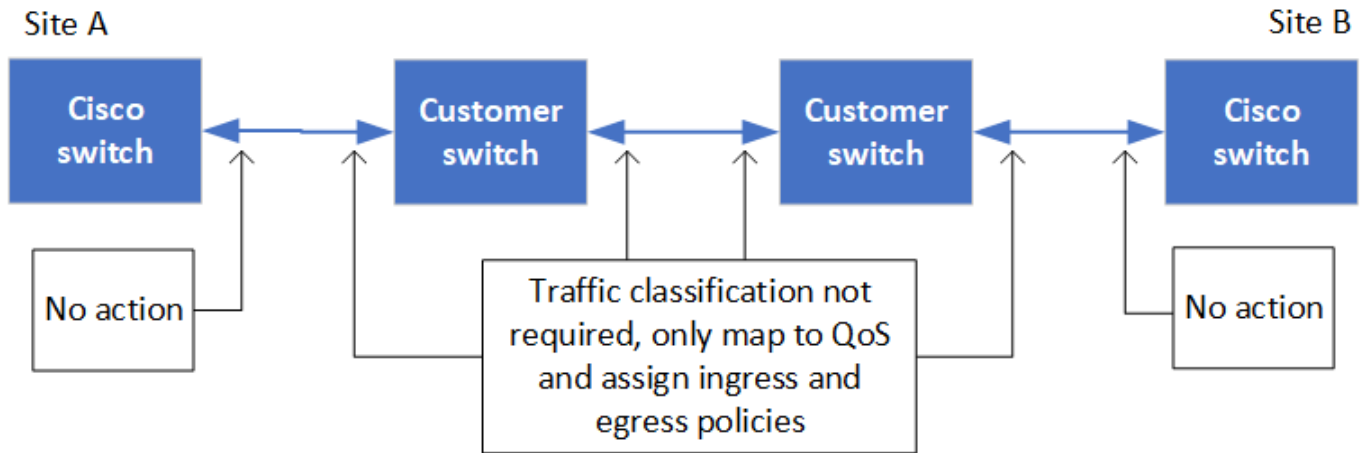
Wenn Sie Router und Gateway-IP-Adressen konfigurieren, müssen Sie die folgenden Anforderungen erfüllen:

- Zwei Schnittstellen auf einem Node können nicht die gleiche Gateway-IP-Adresse aufweisen.
- Die entsprechenden Schnittstellen auf den HA-Paaren an jedem Standort müssen über dieselbe Gateway-IP-Adresse verfügen.
- Die entsprechenden Schnittstellen auf einem Node und seinen DR- und AUX-Partnern können nicht dieselbe Gateway-IP-Adresse haben.
- Die entsprechenden Schnittstellen auf einem Node und seinen DR- und AUX-Partnern müssen dieselbe VLAN-ID aufweisen.

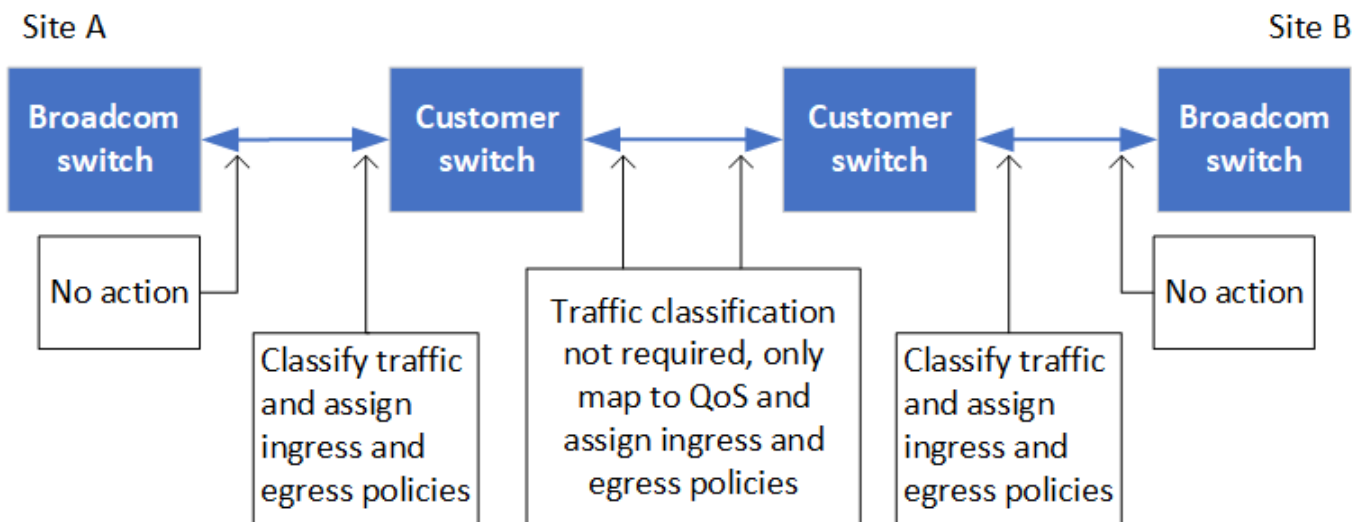
Erforderliche Einstellungen für Zwischenschalter

Wenn MetroCluster-Verkehr in einem mittleren Netzwerk eine ISL durchquert, sollten Sie überprüfen, ob die Konfiguration der mittleren Switches sicherstellt, dass der MetroCluster-Verkehr (RDMA und Storage) über den gesamten Pfad zwischen den MetroCluster Standorten die erforderlichen Service-Level erfüllt.

Das folgende Diagramm gibt eine Übersicht über die erforderlichen Einstellungen bei Verwendung von NetApp Validated Cisco Switches:



Das folgende Diagramm gibt einen Überblick über die erforderlichen Einstellungen für ein freigegebenes Netzwerk, wenn es sich bei den externen Switches um Broadcom-IP-Switches handelt.



In diesem Beispiel werden für den MetroCluster-Datenverkehr die folgenden Richtlinien und Zuordnungen erstellt:

- Der `MetroClusterIP_ISL_Ingress` Die Richtlinie wird auf Ports auf dem Zwischenswitch angewendet, der eine Verbindung zu den MetroCluster IP-Switches herstellt.

Der `MetroClusterIP_ISL_Ingress` Die Richtlinie ordnet den eingehenden gekennzeichneten Datenverkehr der entsprechenden Warteschlange auf dem Zwischenswitch zu.

- A `MetroClusterIP_ISL_Egress` Die Richtlinie wird auf Ports auf dem Zwischenswitch angewendet, die mit ISLs zwischen Zwischenswitches verbunden sind.
- Sie müssen die Zwischen-Switches mit übereinstimmenden QoS-Zugriffskarten, Klassenkarten und Richtlinienzuordnungen zwischen den MetroCluster IP-Switches konfigurieren. Die Zwischen-Switches weisen den RDMA-Datenverkehr auf COS5 und den Storage-Datenverkehr auf COS4 zu.

Die folgenden Beispiele gelten für Cisco Nexus 3232C- und 9336C-FX2-Switches. Je nach Switch-Hersteller und -Modell müssen Sie überprüfen, ob Ihre Zwischenswitches über eine geeignete Konfiguration verfügen.

Konfigurieren Sie die Klassenzuordnung für den ISL-Port des Zwischenswitches

Das folgende Beispiel zeigt die Klassenzuordnungsdefinitionen, je nachdem, ob der Datenverkehr beim

Eindringen klassifiziert oder abgeglichen werden muss.

Klassifizieren des Datenverkehrs beim Eindringen:

```
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200

class-map type qos match-all rdma
  match access-group name rdma
class-map type qos match-all storage
  match access-group name storage
```

Datenverkehr beim Eindringen abgleichen:

```
class-map type qos match-any c5
  match cos 5
  match dscp 40
class-map type qos match-any c4
  match cos 4
  match dscp 32
```

Erstellen Sie eine Eingangs-Policy Map auf dem ISL-Port des Intermediate Switch:

Die folgenden Beispiele zeigen, wie Sie eine Eingangs-Policy-Map erstellen, je nachdem, ob Sie den Datenverkehr beim Eindringen klassifizieren oder abgleichen müssen.

Klassifizieren Sie den Verkehr beim Eindringen:

```
policy-map type qos MetroClusterIP_ISL_Ingress_Classify
  class rdma
    set dscp 40
    set cos 5
    set qos-group 5
  class storage
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Gleichen Sie den Datenverkehr beim Eindringen ab:

```
policy-map type qos MetroClusterIP_ISL_Ingress_Match
  class c5
    set dscp 40
    set cos 5
    set qos-group 5
  class c4
    set dscp 32
    set cos 4
    set qos-group 4
  class class-default
    set qos-group 0
```

Konfigurieren Sie die Ausgangs-Queuing-Richtlinie für die ISL-Ports

Das folgende Beispiel zeigt, wie die Richtlinie für die Ausgangs-Warteschlange konfiguriert wird:

```

policy-map type queuing MetroClusterIP_ISL_Egress
  class type queuing c-out-8q-q7
    priority level 1
  class type queuing c-out-8q-q6
    priority level 2
  class type queuing c-out-8q-q5
    priority level 3
    random-detect threshold burst-optimized ecn
  class type queuing c-out-8q-q4
    priority level 4
    random-detect threshold burst-optimized ecn
  class type queuing c-out-8q-q3
    priority level 5
  class type queuing c-out-8q-q2
    priority level 6
  class type queuing c-out-8q-q1
    priority level 7
  class type queuing c-out-8q-q-default
    bandwidth remaining percent 100
    random-detect threshold burst-optimized ecn

```

Diese Einstellungen müssen auf alle Switches und ISLs angewendet werden, die MetroCluster-Datenverkehr tragen.

In diesem Beispiel werden Q4 und Q5 mit konfiguriert `random-detect threshold burst-optimized ecn`. Abhängig von Ihrer Konfiguration müssen Sie möglicherweise die minimalen und maximalen Schwellenwerte festlegen, wie im folgenden Beispiel gezeigt:

```

class type queuing c-out-8q-q5
  priority level 3
  random-detect minimum-threshold 3000 kbytes maximum-threshold 4000
  kbytes drop-probability 0 weight 0 ecn
class type queuing c-out-8q-q4
  priority level 4
  random-detect minimum-threshold 2000 kbytes maximum-threshold 3000
  kbytes drop-probability 0 weight 0 ecn

```



Die Mindest- und Höchstwerte variieren je nach Switch und Ihren Anforderungen.

Beispiel 1: Cisco

Wenn Ihre Konfiguration über Cisco Switches verfügt, müssen Sie den ersten Ingress-Port des Intermediate Switch nicht klassifizieren. Anschließend konfigurieren Sie die folgenden Zuordnungen und Richtlinien:

- `class-map type qos match-any c5`

- `class-map type qos match-any c4`
- `MetroClusterIP_ISL_Ingress_Match`

Sie weisen die zu `MetroClusterIP_ISL_Ingress_Match` Richtlinienzuordnung zu den ISL-Ports, die MetroCluster-Datenverkehr übertragen.

Beispiel 2: Broadcom

Wenn Ihre Konfiguration über Broadcom-Switches verfügt, müssen Sie den ersten Ingress-Port des Intermediate-Switches klassifizieren. Anschließend konfigurieren Sie die folgenden Zuordnungen und Richtlinien:

- `ip access-list rdma`
- `ip access-list storage`
- `class-map type qos match-all rdma`
- `class-map type qos match-all storage`
- `MetroClusterIP_ISL_Ingress_Classify`
- `MetroClusterIP_ISL_Ingress_Match`

Sie zuweisen the `MetroClusterIP_ISL_Ingress_Classify` Die Richtlinien werden den ISL-Ports auf dem Zwischenswitch zugeordnet, der den Broadcom-Switch verbindet.

Sie weisen die zu `MetroClusterIP_ISL_Ingress_Match` Die Richtlinien werden den ISL-Ports auf dem Zwischenswitch zugeordnet, der MetroCluster-Datenverkehr ausführt, aber keinen Broadcom-Switch verbindet.

Überlegungen zur Verwendung von MetroCluster-konformen Switches

Anforderungen und Einschränkungen beim Einsatz von MetroCluster-konformen Switches

Ab ONTAP 9.7 können in MetroCluster IP Konfigurationen MetroCluster-konforme Switches verwendet werden. Dabei handelt es sich um Switches, die nicht von NetApp validiert wurden, die jedoch die Spezifikationen von NetApp erfüllen. NetApp bietet jedoch keine Fehlerbehebungs- oder Konfigurationsunterstützung für nicht validierte Switches an. Die allgemeinen Anforderungen und Einschränkungen bei der Verwendung von MetroCluster-konformen Switches sollten Sie sich bewusst sein.

Allgemeine Anforderungen für MetroCluster-konforme Switches

Der Switch, der die MetroCluster IP-Schnittstellen verbindet, muss die folgenden allgemeinen Anforderungen erfüllen:

- Die Switches müssen für Quality of Service (QoS) und Traffic-Klassifizierung sorgen.
- Die Schalter müssen eine explizite Benachrichtigung über eine Staumeldung (ECN) unterstützen.
- Die Switches müssen eine Load-Balancing-Richtlinie unterstützen, um die Reihenfolge entlang des Pfads beizubehalten.

- Die Switches müssen L2 Flow Control (L2FC) unterstützen.
- Der Switch-Port muss eine dedizierte Rate bereitstellen und darf nicht überlastet sein.
- Die Kabel und Transceiver, die die Nodes mit den Switches verbinden, müssen von NetApp bereitgestellt werden. Diese Kabel müssen vom Switch-Anbieter unterstützt werden. Wenn Sie optische Kabel verwenden, wird der Transceiver im Switch möglicherweise nicht von NetApp bereitgestellt. Sie müssen überprüfen, ob es mit dem Transceiver im Controller kompatibel ist.
- Die Switches, die die MetroCluster Nodes verbinden, können keinen MetroCluster Datenverkehr übertragen.
- Nur Plattformen, die dedizierte Ports für Cluster Interconnects ohne Switches bereitstellen, können mit einem MetroCluster-konformen Switch verwendet werden. Plattformen wie FAS2750 und AFF A220 können nicht verwendet werden, da sich MetroCluster Traffic und der MetroCluster Interconnect Traffic auf dieselben Netzwerk-Ports befinden.
- Der MetroCluster-kompatible Switch darf nicht für lokale Cluster-Verbindungen verwendet werden.
- Die MetroCluster IP-Schnittstelle kann an jeden Switch-Port angeschlossen werden, der entsprechend den Anforderungen konfiguriert werden kann.
- Es sind vier IP-Switches erforderlich, zwei für jede Switch-Fabric. Wenn Sie Directors verwenden, können Sie einen einzelnen Director auf jeder Seite verwenden, aber die MetroCluster IP-Schnittstellen müssen sich mit zwei verschiedenen Blades in zwei verschiedenen Ausfall-Domains auf diesem Director verbinden.
- Die MetroCluster-Schnittstellen von einem Node müssen mit zwei Netzwerk-Switches oder Blades verbunden werden. Die MetroCluster-Schnittstellen eines Node können nicht mit demselben Netzwerk, Switch oder Blade verbunden werden.
- Das Netzwerk muss die in den folgenden Abschnitten beschriebenen Anforderungen erfüllen:
 - ["Überlegungen für ISLs"](#)
 - ["Überlegungen bei der Bereitstellung von MetroCluster in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken"](#)
- Die maximale Übertragungseinheit (MTU) von 9216 muss auf allen Switches mit MetroCluster-IP-Datenverkehr konfiguriert werden.
- Das Zurücksetzen auf ONTAP 9.6 oder eine frühere Version wird nicht unterstützt.

Alle Zwischenschalter, die Sie zwischen den Switches verwenden, die die MetroCluster IP-Schnittstellen an beiden Standorten verbinden, müssen die Anforderungen erfüllen und wie in beschrieben konfiguriert werden ["Überlegungen bei der Bereitstellung von MetroCluster in gemeinsam genutzten Layer-2- oder Layer-3-Netzwerken"](#).

Einschränkungen bei Verwendung von MetroCluster-konformen Switches

Sie können keine Konfiguration oder Funktion verwenden, die erfordert, dass lokale Cluster-Verbindungen mit einem Switch verbunden sind. Mit einem MetroCluster-kompatiblen Switch können Sie beispielsweise die folgenden Konfigurationen und Verfahren nicht verwenden:

- MetroCluster Konfigurationen mit acht Nodes
- Der Wechsel von MetroCluster FC- zu MetroCluster IP-Konfigurationen
- Aktualisieren einer MetroCluster IP-Konfiguration mit vier Knoten
- Plattformen mit einer physischen Schnittstelle für lokalen Cluster und MetroCluster-Datenverkehr. Siehe ["Plattformspezifische Netzwerkgeschwindigkeiten und Switch Port-Modi für MetroCluster-konforme Switches"](#) Für unterstützte Geschwindigkeiten.

Plattformspezifische Netzwerkgeschwindigkeiten und Switch Port-Modi für MetroCluster-konforme Switches

Wenn Sie MetroCluster-kompatible Switches verwenden, sollten Sie die plattformspezifischen Netzwerkgeschwindigkeiten und die Anforderungen für den Switch-Port-Modus kennen.

Die folgende Tabelle bietet plattformspezifische Netzwerkgeschwindigkeiten und Switch Port-Modi für MetroCluster-konforme Switches. Sie sollten den Switch-Port-Modus gemäß der Tabelle konfigurieren.



Fehlende Werte geben an, dass die Plattform nicht mit einem MetroCluster-konformen Switch verwendet werden kann.

Platform	Network Speed (Gbps)	Switch port mode
FAS9500 AFF A900 ASA A900	100Gbps 40Gbps when upgrade PCM from FAS9000 / AFF A700	trunk mode
AFF C800 ASA C800 AFF A800 ASA A800	40Gbps or 100Gbps	access mode
FAS9000 AFF A700	40Gbps	access mode
FAS8300 AFF C400 ASA C400 AFF A400 ASA A400	40Gbps or 100Gbps	trunk mode
AFF A320	40Gbps or 100Gbps	access mode
FAS8200 AFF A300	25Gbps	access mode
FAS500f AFF C250 ASA C250 AFF A250 ASA A250	-	-
FAS2750 AFF A220	-	-
AFF A150 ASA A150	-	-

Beispiele für die Switch-Port-Konfiguration

Erfahren Sie mehr über die verschiedenen Switch-Port-Konfigurationen.



In den folgenden Beispielen werden Dezimalwerte verwendet. Die Tabelle ist für Cisco Switches gültig. Je nach Switch-Anbieter benötigen Sie möglicherweise unterschiedliche Werte für DSCP. Informationen zur Bestätigung des korrekten Werts finden Sie in der entsprechenden Tabelle Ihres Switch-Anbieters.

DSCP-Wert	Dezimal	Sechskant	Bedeutung
101 000	16	0x10	CS2
011 000	24	0x18	CS3
100 000	32	0x20	CS4
101 000	40	0x28	CS5

Switch-Port zum Anschließen einer MetroCluster-Schnittstelle

- Klassifizierung für RDMA-Datenverkehr (Remote Direct Memory Access):
 - Übereinstimmung : TCP-Port 10006, Quelle, Ziel oder beides
 - Optionale Übereinstimmung: COS 5
 - Optionales Match: DSCP 40
 - Legen Sie DSCP 40 fest
 - COS 5 einstellen
 - Optional : Ratenformung bis 20Gbps
- Klassifizierung für iSCSI-Datenverkehr:
 - Übereinstimmung : TCP-Port 62500, Quelle, Ziel oder beides
 - Optionale Übereinstimmung: COS 4
 - Optionales Match: DSCP 32
 - Legen Sie DSCP 32 fest
 - COS 4 einstellen
- L2FlowControl (Pause), RX und TX

ISL-Ports

- Klassifizierung:
 - Übereinstimmung mit COS 5 oder DSCP 40
 - Legen Sie DSCP 40 fest
 - COS 5 einstellen
 - Übereinstimmung mit COS 4 oder DSCP 32
 - Legen Sie DSCP 32 fest

- COS 4 einstellen
- Warteschlange für ausgehenden Datenverkehr
 - Die COS-Gruppe 4 hat einen minimalen Konfigurationsschwellenwert von 2000 und einen maximalen Schwellenwert von 3000
 - Die COS-Gruppe 5 hat einen minimalen Konfigurationsschwellenwert von 3500 und einen maximalen Schwellenwert von 6500.



Die Konfigurationsschwellenwerte können je nach Umgebung variieren. Sie müssen die Konfigurationsschwellenwerte entsprechend Ihrer individuellen Umgebung bewerten.

- ECN aktiviert für Q4 und Q5
- ROT aktiviert für Q4 und Q5

Bandbreitenzuordnung (Switch Ports, die MetroCluster-Schnittstellen und ISL-Ports verbinden)

- RDMA, COS 5 / DSCP 40: 60 %
- ISCSI, COS 4/DSCP 32: 40 %
- Mindestanforderungen für die Kapazität pro MetroCluster-Konfiguration und Netzwerk: 10 GB/s



Wenn Sie die Tarifgrenzen verwenden, sollte der Verkehr **geformt** werden, ohne dass es zu einem Verlust kommt.

Beispiele für die Konfiguration von Switch-Ports, die den MetroCluster-Controller verbinden

Die angegebenen Beispielbefehle gelten für Cisco NX332- oder Cisco NX9336-Switches. Befehle variieren je nach Switch-Typ.

Wenn eine in den Beispielen abgebildete Funktion oder ihr Äquivalent auf dem Switch nicht verfügbar ist, erfüllt der Switch nicht die Mindestanforderungen und kann nicht für die Bereitstellung einer MetroCluster-Konfiguration verwendet werden. Dies gilt für alle Switches, die eine Verbindung zu einer MetroCluster-Konfiguration herstellen, und für alle Zwischenswitches.



In den folgenden Beispielen wird möglicherweise nur die Konfiguration für ein Netzwerk angezeigt.

Basiskonfiguration

In jedem Netzwerk muss ein virtuelles LAN (VLAN) konfiguriert werden. Das folgende Beispiel zeigt, wie ein VLAN in Netzwerk 10 konfiguriert wird.

Beispiel:

```
# vlan 10
The load balancing policy should be set so that order is preserved.
```

Beispiel:

```
# port-channel load-balance src-dst ip-l4port-vlan
```

Beispiele für die Konfiguration der Klassifizierung

Sie müssen Zugriffs- und Klassenzuordnungen konfigurieren, um RDMA- und iSCSI-Datenverkehr den entsprechenden Klassen zuzuordnen.

Im folgenden Beispiel wird der gesamte TCP-Datenverkehr von und zu Port 65200 der Storage-Klasse (iSCSI) zugeordnet. Der gesamte TCP-Datenverkehr zum und vom Port 10006 ist der RDMA-Klasse zugeordnet. Diese Richtlinienzuordnungen werden an Switch-Ports verwendet, die die MetroCluster-Schnittstellen verbinden.

Beispiel:

```
ip access-list storage
  10 permit tcp any eq 65200 any
  20 permit tcp any any eq 65200
ip access-list rdma
  10 permit tcp any eq 10006 any
  20 permit tcp any any eq 10006

class-map type qos match-all storage
  match access-group name storage
class-map type qos match-all rdma
  match access-group name rdma
```

Sie müssen eine Eingangs-Richtlinie konfigurieren. Eine Ingress-Richtlinie ordnet den Datenverkehr verschiedenen COS-Gruppen zu. In diesem Beispiel wird der RDMA-Verkehr der COS-Gruppe 5 zugeordnet und iSCSI-Verkehr der COS-Gruppe 4 zugeordnet. Die Ingress-Richtlinie wird auf Switch-Ports verwendet, die die MetroCluster-Schnittstellen verbinden, und auf den ISL-Ports, die MetroCluster-Datenverkehr übertragen.

Beispiel:

```
policy-map type qos MetroClusterIP_Node_Ingress
class rdma
  set dscp 40
  set cos 5
  set qos-group 5
class storage
  set dscp 32
  set cos 4
  set qos-group 4
```

NetApp empfiehlt, den Datenverkehr an Switch-Ports, die eine MetroCluster-Schnittstelle verbinden, wie im folgenden Beispiel gezeigt zu gestalten:

Beispiel:

```

policy-map type queuing MetroClusterIP_Node_Egress
class type queuing c-out-8q-q7
  priority level 1
class type queuing c-out-8q-q6
  priority level 2
class type queuing c-out-8q-q5
  priority level 3
  shape min 0 gbps max 20 gbps
class type queuing c-out-8q-q4
  priority level 4
class type queuing c-out-8q-q3
  priority level 5
class type queuing c-out-8q-q2
  priority level 6
class type queuing c-out-8q-q1
  priority level 7
class type queuing c-out-8q-q-default
  bandwidth remaining percent 100
  random-detect threshold burst-optimized ecn

```

Beispiele für die Konfiguration der Node-Ports

Möglicherweise müssen Sie einen Node-Port im Breakout-Modus konfigurieren. Im folgenden Beispiel sind die Ports 25 und 26 im Breakout-Modus 4 x 25 Gbit/s konfiguriert.

Beispiel:

```
interface breakout module 1 port 25-26 map 25g-4x
```

Sie müssen möglicherweise die Port-Geschwindigkeit der MetroCluster-Schnittstelle konfigurieren. Das folgende Beispiel zeigt, wie die Geschwindigkeit auf **Auto** oder in den 40-Gbit/s-Modus konfiguriert wird:

Beispiel:

```

speed auto

speed 40000

```

Das folgende Beispiel zeigt einen Switch-Port, der für den Anschluss einer MetroCluster-Schnittstelle konfiguriert ist. Es handelt sich um einen Access-Mode-Port in VLAN 10 mit einer MTU von 9216 und arbeitet in nativer Geschwindigkeit. Die symmetrische Flusssteuerung (Senden und Empfangen) ist aktiviert (Pause) und den MetroCluster-Richtlinien für ein- und ausgehenden Datenverkehr sind zugewiesen.

Beispiel:

```

interface eth1/9
description MetroCluster-IP Node Port
speed auto
switchport access vlan 10
spanning-tree port type edge
spanning-tree bpduguard enable
mtu 9216
flowcontrol receive on
flowcontrol send on
service-policy type qos input MetroClusterIP_Node_Ingress
service-policy type queuing output MetroClusterIP_Node_Egress
no shutdown

```

Bei 25-Gbit/s-Ports müssen Sie möglicherweise die Einstellung Vorwärts-Fehlerkorrektur (FEC) auf „aus“ setzen, wie im folgenden Beispiel gezeigt.

Beispiel:

```
fec off
```

Beispiele für die Konfiguration von ISL-Ports im gesamten Netzwerk

Ein MetroCluster-konformer Switch gilt als Zwischenschalter, selbst er verbindet die MetroCluster-Schnittstellen direkt. Die ISL-Ports, die MetroCluster-Datenverkehr auf dem MetroCluster-konformen Switch übertragen, müssen auf die gleiche Weise wie die ISL-Ports an einem Zwischen-Switch konfiguriert werden. Siehe ["Erforderliche Einstellungen an Zwischenschaltern"](#) Für Anleitungen und Beispiele.



Einige Richtlinienzuordnungen sind für Switch-Ports, die MetroCluster-Schnittstellen verbinden, und ISLs mit MetroCluster-Datenverkehr identisch. Sie können für beide Portnutzungsarten dieselbe Richtlinienzuordnung verwenden.

Beispiele für MetroCluster Netzwerktopologien

Ab ONTAP 9.6 werden einige zusätzliche Netzwerkkonfigurationen für MetroCluster IP-Konfigurationen unterstützt. Dieser Abschnitt enthält einige Beispiele für unterstützte Netzwerkkonfigurationen. Es werden nicht alle unterstützten Topologien aufgeführt.

In diesen Topologien wird davon ausgegangen, dass das ISL- und das Zwischennetzwerk entsprechend den in beschriebenen Anforderungen konfiguriert ist ["Überlegungen für ISLs"](#).

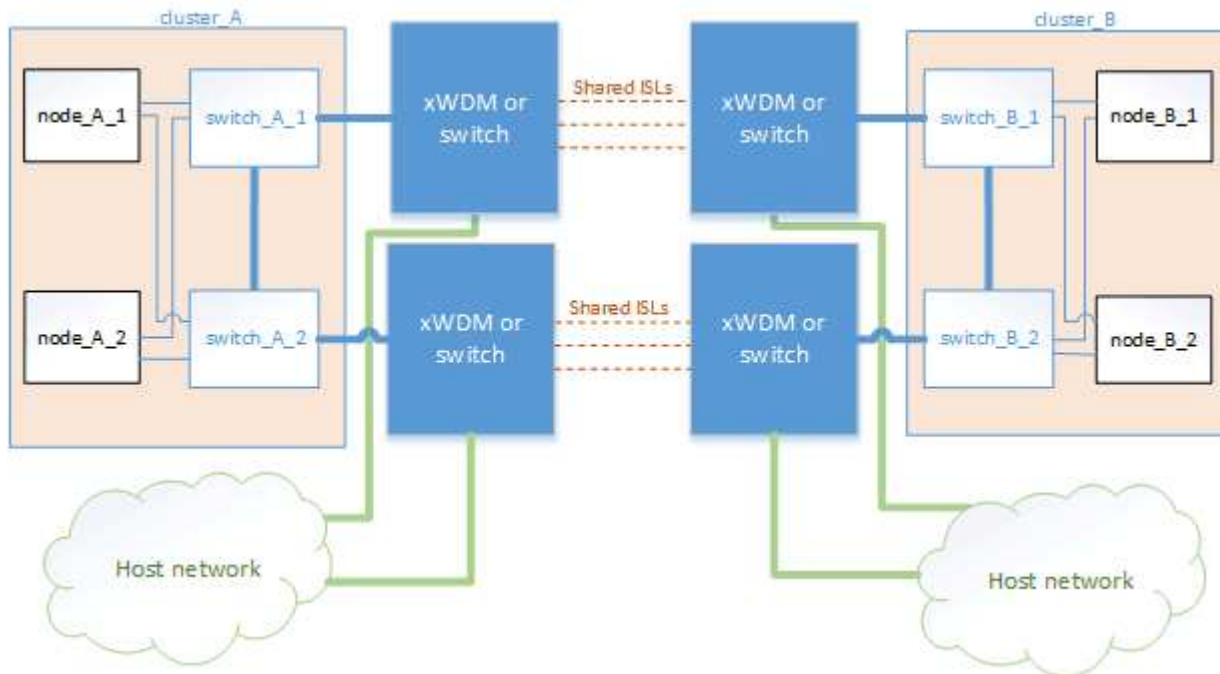


Wenn Sie eine ISL für nicht-MetroCluster Verkehr freigeben, müssen Sie sicherstellen, dass die MetroCluster jederzeit mindestens über die erforderliche Mindestbandbreite verfügt.

Konfiguration für gemeinsam genutztes Netzwerk mit direkten Links

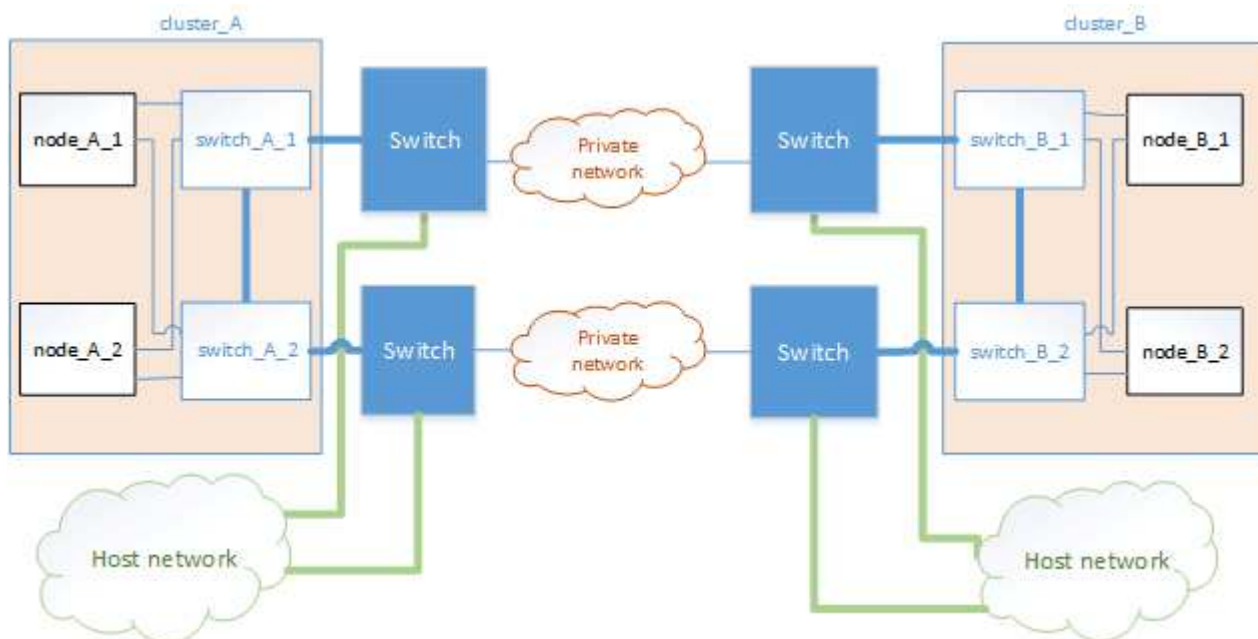
In dieser Topologie sind zwei unterschiedliche Standorte durch direkte Links verbunden. Diese Verbindungen

können zwischen xWDM- und TDM-Geräten oder -Switches bestehen. Die Kapazität der ISLs ist nicht für den MetroCluster-Verkehr reserviert, wird aber für anderen nicht-MetroCluster Verkehr freigegeben.



Gemeinsam genutzte Infrastruktur mit Zwischennetzen

In dieser Topologie sind die MetroCluster-Standorte nicht direkt verbunden, sondern MetroCluster und der Host-Datenverkehr werden über ein Netzwerk geleitet. Das Netzwerk kann aus einer Reihe von xWDM und TDM und Switches bestehen, aber im Gegensatz zur gemeinsamen Konfiguration mit direkten ISLs sind die Verbindungen nicht direkt zwischen den Standorten. Je nach Infrastruktur zwischen den Standorten ist eine beliebige Kombination von Netzwerkkonfigurationen möglich.

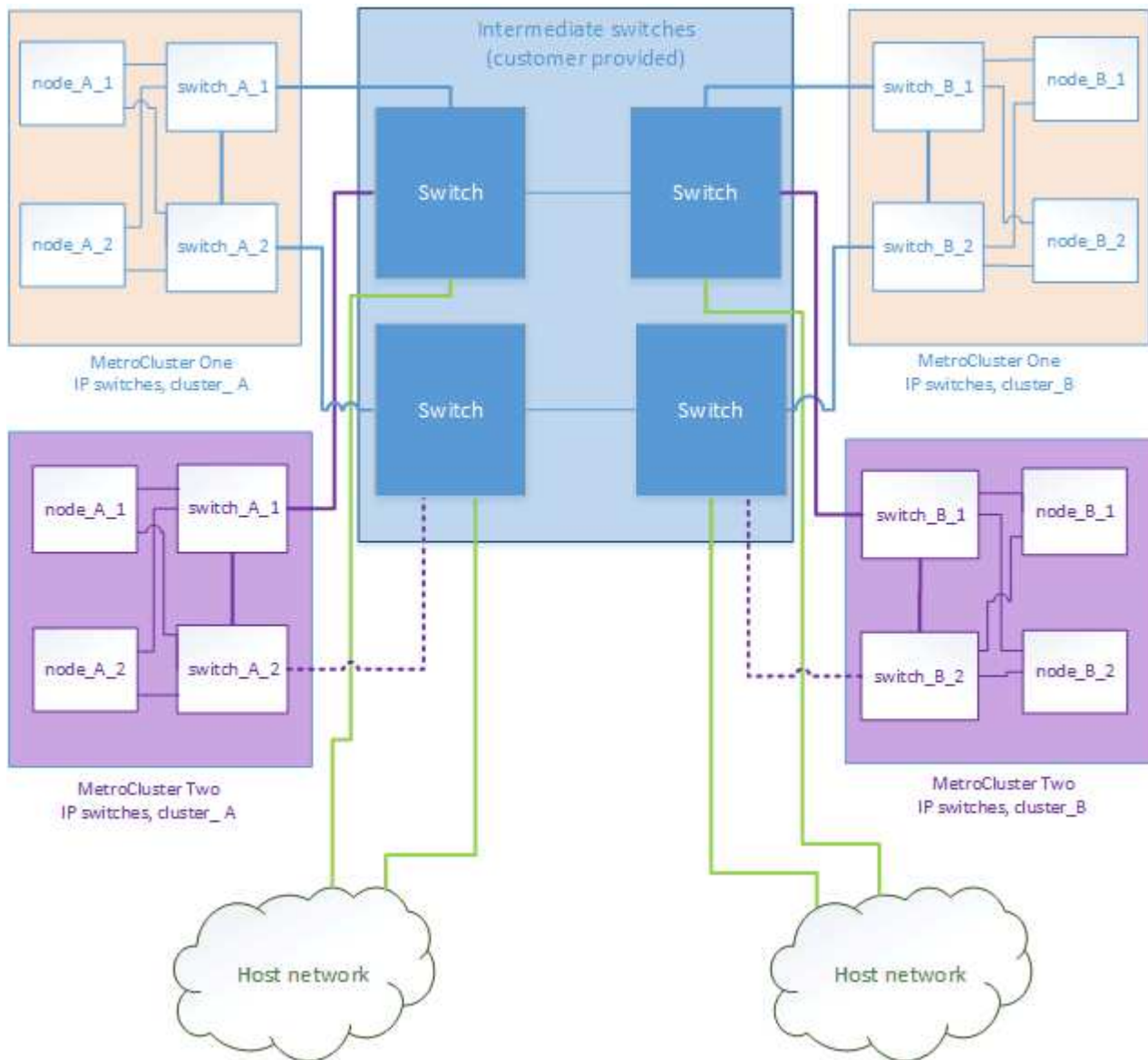


Mehrere MetroCluster-Konfigurationen nutzen ein Zwischennetzwerk

In dieser Topologie teilen sich zwei separate MetroCluster-Konfigurationen dasselbe Zwischennetzwerk. Im Beispiel MetroCluster One Switch_A_1 und MetroCluster Two Switch_A_1 verbinden sich beide mit demselben Zwischenswitch.

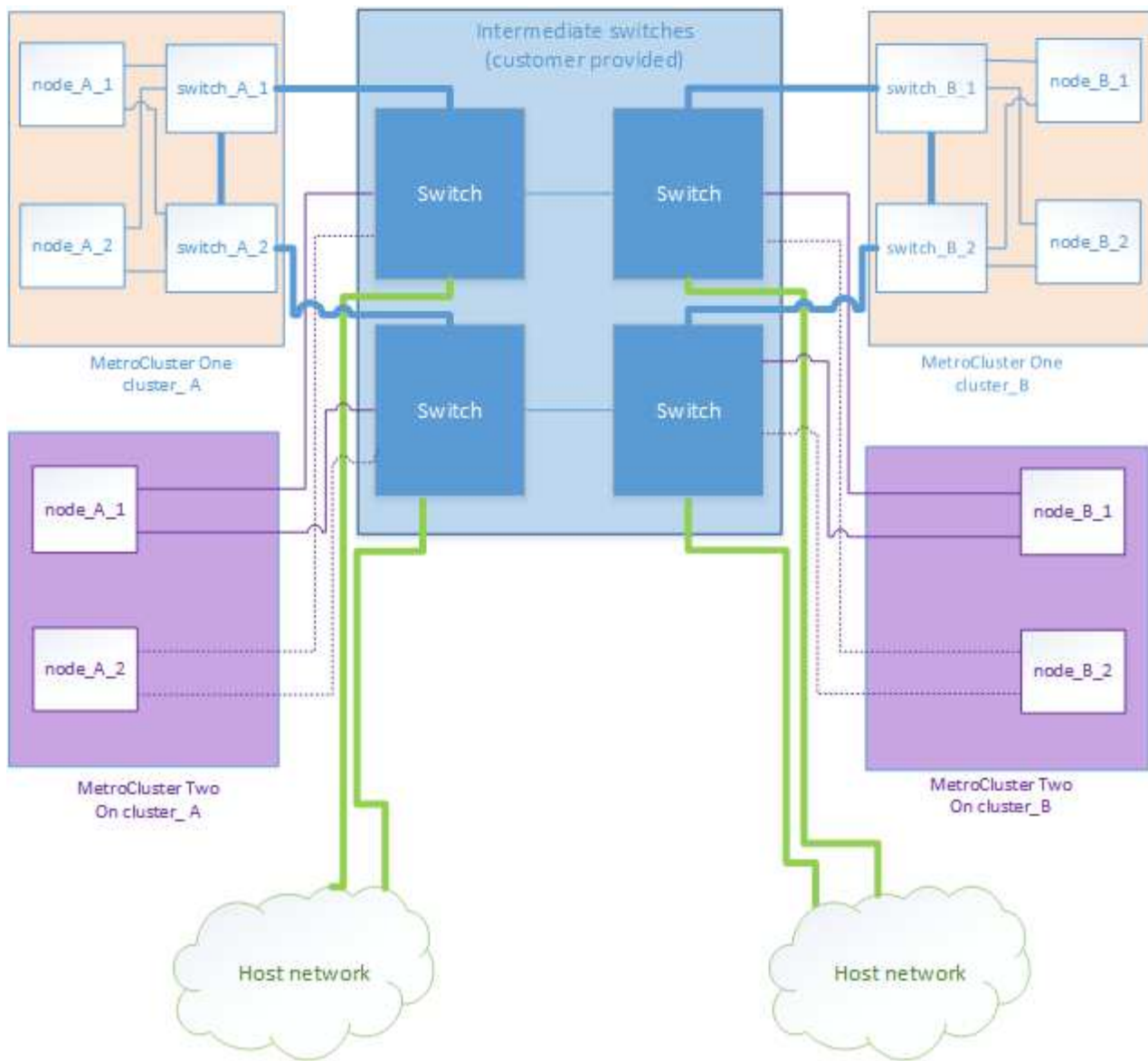


Sowohl „MetroCluster One“ als auch „MetroCluster Two“ kann eine MetroCluster Konfiguration mit acht Nodes oder zwei MetroCluster Konfigurationen mit vier Nodes sein.



Kombination einer MetroCluster Konfiguration mit validierten NetApp Switches und einer Konfiguration mit MetroCluster konformen Switches

Zwei separate MetroCluster Konfigurationen nutzen denselben Intermediate Switch, bei dem ein MetroCluster mit validierten NetApp Switches in einer Shared Layer 2-Konfiguration (MetroCluster One) konfiguriert ist und der andere MetroCluster mithilfe von MetroCluster-konformen Switches konfiguriert wird, die direkt mit den Intermediate Switches verbinden (MetroCluster Two).



Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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