Installieren Sie eine MetroCluster IP-Konfiguration

ONTAP MetroCluster

NetApp
August 22, 2025

Inhalt

Installieren Sie eine MetroCluster IP-Konfiguration

MetroCluster IP-Installationsworkflow

Um Ihre MetroCluster IP-Konfiguration zu installieren, müssen Sie eine Reihe von Verfahren in der richtigen Reihenfolge durchführen.

- "Bereiten Sie sich auf die Installation vor und verstehen Sie alle Anforderungen".
- "Verkabeln Sie die Komponenten"
- "Konfigurieren der Software"
- "Konfigurieren Sie den ONTAP Mediator" (Optional)
- "Testen Sie die Konfiguration"

Bereiten Sie sich auf die MetroCluster Installation vor

Supportmatrix für ONTAP MetroCluster -Konfigurationen

Die verschiedenen MetroCluster Konfigurationen weisen wesentliche Unterschiede in den erforderlichen Komponenten auf.

In allen Konfigurationen ist jeder der beiden MetroCluster-Standorte als ONTAP-Cluster konfiguriert. In einer MetroCluster Konfiguration mit zwei Nodes ist jeder Node als Single-Node-Cluster konfiguriert.

Merkmal	IP-Konfigurationen	Fabric-Attached-Konfigurationen		Stretch-Konfigurationen	
		Vier- oder acht-Knoten	* Zwei Knoten*	* Zwei-Knoten-Brücke-verbunden*	* Zwei-Knoten direkt verbunden*
Anzahl an Controllern	Vier oder acht[1]	Vier oder acht	Zwei	Zwei	Zwei
Storage Fabric mit FC-Switch	Nein	Ja.	Ja.	Nein	Nein
Verwendet eine IP Switch Storage Fabric	Ja.	Nein	Nein	Nein	Nein
Verwendung von FC-to-SAS-Bridges	Nein	Ja.	Ja.	Ja.	Nein

Nutzung von Direct-Attached SAS Storage	Ja (nur lokal in Verbindung)	Nein	Nein	Nein	Ja.
Unterstützt ADP	Ja (ab ONTAP 9.4)	Nein	Nein	Nein	Nein
Unterstützt lokale HA	Ja.	Ja.	Nein	Nein	Nein
Unterstützt ONTAP Automatic ungeplante Switchover (AUSO)	Nein	Ja.	Ja.	Ja.	Ja.
Unterstützt nicht gespiegelte Aggregate	Ja (ab ONTAP 9.8)	Ja.	Ja.	Ja.	Ja.
Unterstützt den ONTAP Mediator	Ja (ab ONTAP 9.7)	Nein	Nein	Nein	Nein
Unterstützung von MetroCluster Tiebreaker	Ja (nicht in Kombination mit ONTAP Mediator)	Ja.	Ja.	Ja.	Ja.
Unterstützt Rein SAN-basierte Arrays	Ja.	Ja.	Ja.	Ja.	Ja.

Hinweise

1. Lesen Sie die folgenden Überlegungen für MetroCluster IP-Konfigurationen mit acht Nodes:
   - Konfigurationen mit acht Nodes werden ab ONTAP 9.9 unterstützt.
   - Es werden nur NetApp validierte MetroCluster Switches (bei NetApp bestellt) unterstützt.
   - Konfigurationen, die IP-geroutet (Layer 3)-Back-End-Verbindungen verwenden, werden nicht unterstützt.

Unterstützung für alle SAN-Array-Systeme in MetroCluster Konfigurationen

Einige der All-SAN-Arrays (ASAs) werden in MetroCluster-Konfigurationen unterstützt. In der MetroCluster-Dokumentation gelten die Informationen zu AFF-Modellen auf das entsprechende ASA-System. Beispielsweise gelten alle Kabel und weitere Informationen zum AFF A400 System auch für das ASA AFF A400 System.

Unterstützte Plattformkonfigurationen sind im aufgeführt "NetApp Hardware Universe".

Unterschiede zwischen ONTAP Mediator und MetroCluster Tiebreaker

Ab ONTAP 9.7 können Sie entweder die ONTAP Mediator-gestützte automatische ungeplante Umschaltung (MAUSO) in der MetroCluster IP-Konfiguration verwenden oder die MetroCluster Tiebreaker Software verwenden. Es ist nicht erforderlich, die MAUSO- oder Tiebreaker-Software zu verwenden; wenn Sie jedoch einen dieser Dienste nicht nutzen möchten, müssen Sie dies tun "Führen Sie eine manuelle Wiederherstellung durch" Bei einem Ausfall.

Die verschiedenen MetroCluster Konfigurationen führen unter unterschiedlichen Umständen automatische Umschaltung durch:

- **MetroCluster FC-Konfigurationen mit der AUSO-Fähigkeit (nicht in MetroCluster IP-Konfigurationen vorhanden)**

  In diesen Konfigurationen wird AUSO initiiert, wenn Controller ausfallen, der Speicher (und ggf. Brücken) jedoch betriebsbereit bleiben.

- **MetroCluster-IP-Konfigurationen mit ONTAP Mediator (ONTAP 9.7 und höher)**

  In diesen Konfigurationen wird MAUSO unter denselben Umständen wie AUSO wie oben beschrieben initiiert, aber auch nach einem kompletten Standortausfall (Controller, Storage und Switches).

  "Erfahren Sie, wie der ONTAP Mediator die automatische ungeplante Umschaltung unterstützt".

- **MetroCluster IP- oder FC-Konfigurationen mit der Tiebreaker Software im aktiven Modus**

  Bei diesen Konfigurationen initiiert der Tiebreaker eine ungeplante Umschaltung nach einem vollständigen Standortausfall.

  Bevor Sie die Tiebreaker Software verwenden, überprüfen Sie das "Installation und Konfiguration der MetroCluster Tiebreaker Software"

Interoperabilität von ONTAP Mediator mit anderen Anwendungen und Geräten

Es ist nicht möglich, Applikationen oder Appliances von Drittanbietern zu verwenden, die in Kombination mit ONTAP Mediator eine Umschaltung auslösen können. Darüber hinaus wird das Monitoring einer MetroCluster-Konfiguration mit MetroCluster Tiebreaker Software bei Verwendung des ONTAP Mediator nicht unterstützt.

Erfahren Sie mehr über Remote-Speicher und MetroCluster IP-Konfigurationen

Sie sollten verstehen, wie die Controller auf den Remote-Storage zugreifen und wie die MetroCluster-IP-Adressen funktionieren.

Zugriff auf Remote-Speicher in MetroCluster IP-Konfigurationen

In MetroCluster IP Konfigurationen erfolgt die einzige Möglichkeit, wie die lokalen Controller die Remote Speicherpools über die Remote-Controller erreichen können. Die IP-Switches sind mit den Ethernet-Ports der Controller verbunden. Sie verfügen nicht über direkte Verbindungen zu Festplatten-Shelfs. Wenn der Remote-Controller ausfällt, können die lokalen Controller die Remote-Speicherpools nicht erreichen.

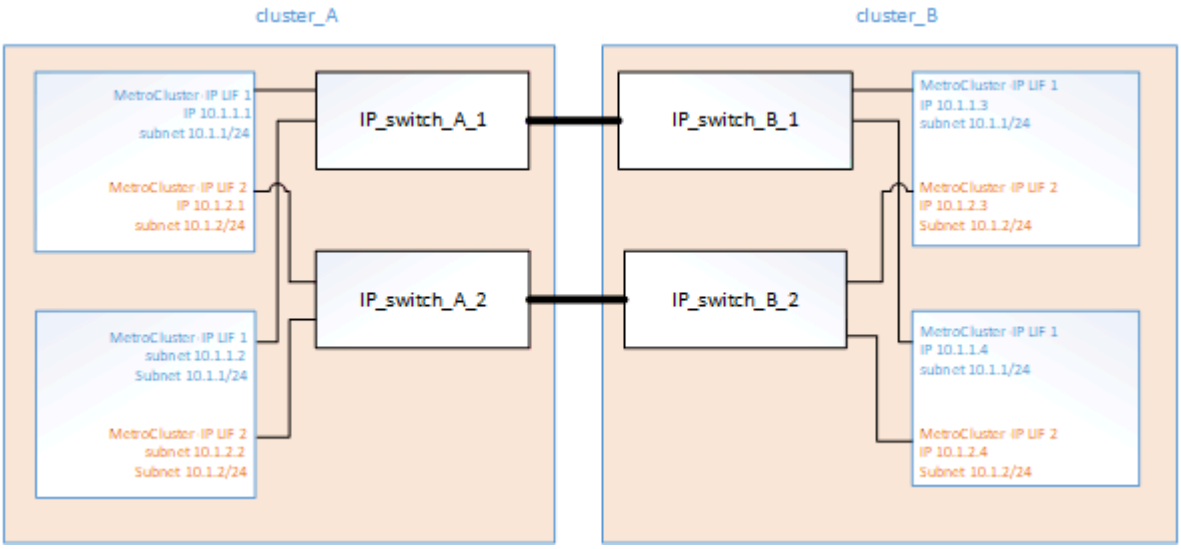
Dies unterscheidet sich von MetroCluster FC-Konfigurationen, in denen die Remote-Storage-Pools über die

FC-Fabric- oder SAS-Verbindungen mit den lokalen Controllern verbunden werden. Die lokalen Controller haben noch Zugriff auf den Remote-Storage, selbst wenn die Remote-Controller ausgefallen sind.

MetroCluster-IP-Adressen

Sie sollten wissen, wie die MetroCluster IP-Adressen und Schnittstellen in einer MetroCluster IP-Konfiguration implementiert werden, sowie welche Anforderungen damit verbunden sind.

In einer MetroCluster IP-Konfiguration werden die Replizierung von Storage und nichtflüchtigem Cache zwischen den HA-Paaren und den DR-Partnern über dedizierte Links mit hoher Bandbreite im MetroCluster IP-Fabric durchgeführt. Für die Storage-Replikation werden iSCSI-Verbindungen verwendet. Die IP-Switches werden auch für den gesamten clusterinternen Datenverkehr innerhalb der lokalen Cluster verwendet. Der MetroCluster-Datenverkehr wird mithilfe separater IP-Subnetze und VLANs vom clusterinternen Datenverkehr getrennt. Die MetroCluster IP Fabric unterscheidet sich von dem Cluster-Peering-Netzwerk.



Die MetroCluster IP-Konfiguration erfordert auf jedem Node zwei IP-Adressen, die dem Back-End MetroCluster IP Fabric vorbehalten sind. Die reservierten IP-Adressen werden während der Erstkonfiguration MetroCluster IP Logical Interfaces (LIFs) zugewiesen. Sie haben folgende Anforderungen:

> Sie müssen die MetroCluster-IP-Adressen sorgfältig auswählen, da Sie sie nach der ersten Konfiguration nicht ändern können.

- Sie müssen in einen eindeutigen IP-Bereich fallen.

  Sie dürfen sich nicht mit IP-Speicherplatz in der Umgebung überschneiden.

- Sie müssen sich in einem von zwei IP-Subnetzen befinden, die sie von allen anderen Traffic trennen.

Beispielsweise können die Nodes mit den folgenden IP-Adressen konfiguriert werden:

Knoten	Schnittstelle	IP-Adresse	Subnetz
Node_A_1	MetroCluster IP-Schnittstelle 1	10.1.1.1	10.1.1/24

Node_A_1	MetroCluster IP-Schnittstelle 2	10.1.2.1	10.1.2/24
Node_A_2	MetroCluster IP-Schnittstelle 1	10.1.1.2	10.1.1/24
Node_A_2	MetroCluster IP-Schnittstelle 2	10.1.2.2	10.1.2/24
Knoten_B_1	MetroCluster IP-Schnittstelle 1	10.1.1.3	10.1.1/24
Knoten_B_1	MetroCluster IP-Schnittstelle 2	10.1.2.3	10.1.2/24
Knoten_B_2	MetroCluster IP-Schnittstelle 1	10.1.1.4	10.1.1/24
Knoten_B_2	MetroCluster IP-Schnittstelle 2	10.1.2.4	10.1.2/24

Merkmale der MetroCluster IP-Schnittstellen

Die MetroCluster IP-Schnittstellen gelten speziell für MetroCluster IP-Konfigurationen. Sie weisen verschiedene Merkmale von anderen ONTAP Schnittstellentypen auf:

- Sie werden von der geschaffen `metrocluster configuration-settings interface create` Befehl als Teil der Erstkonfiguration von MetroCluster.

  Ab ONTAP 9.9 müssen Sie auch die angeben, wenn Sie eine Layer 3-Konfiguration verwenden `-gateway` Parameter beim Erstellen von MetroCluster-IP-Schnittstellen. Siehe "Überlegungen für Layer 3-Weitbereichs-Netzwerke".

  Sie werden nicht durch die Befehle der Netzwerkschnittstelle erstellt oder geändert.

- Sie erscheinen nicht in der Ausgabe des `network interface show` Befehl.
- Sie führen kein Failover durch, bleiben aber mit dem Port verbunden, auf dem sie erstellt wurden.
- Bei den MetroCluster IP-Konfigurationen werden bestimmte Ethernet-Ports (je nach Plattform) für die MetroCluster IP-Schnittstellen verwendet.

  Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.

MetroCluster IP-Überlegungen für automatische Laufwerkszuweisung und ADP-Systeme

Ab ONTAP 9.4 unterstützen MetroCluster IP-Konfigurationen neue Installationen mithilfe

von automatischer Festplattenzuweisung und ADP (Advanced Drive Partitioning).

Bei der Verwendung von ADP mit MetroCluster IP-Konfigurationen sollten Sie die folgenden Überlegungen beachten:

- ONTAP 9.4 und höher ist für die Verwendung von ADP mit MetroCluster IP Konfigurationen auf AFF und ASA Systemen erforderlich.
- ADPv2 wird in MetroCluster IP-Konfigurationen unterstützt.
- Das Root-Aggregat muss sich in Partition 3 für alle Knoten auf beiden Standorten befinden.
- Die Partitionierung und Festplattenzuordnung erfolgt automatisch bei der Erstkonfiguration der MetroCluster Standorte.
- Pool 0-Festplattenzuordnungen werden werkseitig ausgeführt.
- Die unverspiegelte Root wird werkseitig erstellt.
- Die Zuweisung der Daten erfolgt während des Setups am Standort des Kunden.
- In den meisten Fällen erfolgt die Laufwerkszuweisung und -Partitionierung automatisch während des Setup-Verfahrens.
- Eine Festplatte und alle Partitionen müssen im Besitz von Nodes in demselben HA-Paar (Hochverfügbarkeit) sein. Die Partitionen oder Laufwerkseigentümer innerhalb eines einzelnen Laufwerks können nicht zwischen dem lokalen HA-Paar und dem Disaster Recovery-Partner (DR) oder dem DR-Zusatzpartner gemischt werden.

  Beispiel einer unterstützten Konfiguration:

Laufwerk/Partition	Eigentümer
Laufwerk:	`ClusterA-Node01`
Partition 1:	`ClusterA-Node01`
Partition 2:	`ClusterA-Node02`
Partition 3:	`ClusterA-Node01`

Beim Upgrade von ONTAP 9.4 auf 9.5 erkennt das System die vorhandenen Festplattenzuordnungen.

Automatische Partitionierung

ADP wird automatisch während der Erstkonfiguration des Systems durchgeführt.

Ab ONTAP 9.5 muss die automatische Festplattenzuordnung mit dem aktiviert werden `storage disk option modify -autoassign on` Befehl.

Sie müssen den ha-config-Status auf festlegen `mccip` Vor der automatischen Bereitstellung, um sicherzustellen, dass die richtigen Partitionsgrößen ausgewählt sind, um eine entsprechende Root-Volume-Größe zu ermöglichen. Weitere Informationen finden Sie unter "Überprüfen des HA-Konfigurationsstatus von Komponenten".

Bis zu 96 Laufwerke können während der Installation automatisch partitioniert werden. Nach der Erstinstallation können Sie zusätzliche Laufwerke hinzufügen.

Wenn Sie interne und externe Laufwerke verwenden, initialisieren Sie zuerst die MetroCluster mit nur den internen Laufwerken unter Verwendung von ADP. Anschließend schließen Sie das externe Shelf manuell an, nachdem Sie die Installation oder Einrichtung abgeschlossen haben.

Sie müssen sicherstellen, dass für die internen Shelfs die empfohlene Mindestanzahl an Laufwerken wie in beschrieben angegeben angegeben angegeben ist Unterschiede bei der ADP- und Festplattenzuordnung nach System.

Sowohl für die internen als auch für die externen Laufwerke müssen Sie die teilweise vollständigen Shelfs ausfüllen, wie in beschrieben Wie partielle Shelves befüllt werden.

Die automatische Zuweisung von Shelfs für Shelfs

Wenn pro Standort vier externe Shelfs vorhanden sind, wird jedem Shelf ein anderer Node und ein anderer Pool zugewiesen, wie im folgenden Beispiel dargestellt:

- Alle Festplatten an Site_A-Shelf_1 werden automatisch Pool 0 von Node_A_1 zugewiesen
- Alle Festplatten auf Site_A-Shelf_3 werden automatisch dem Pool 0 der Node_A_2 zugewiesen
- Alle Festplatten an Site_B-Shelf_1 werden automatisch dem Pool 0 der Node_B_1 zugewiesen
- Alle Festplatten an Site_B-Shelf_3 werden automatisch dem Pool 0 der Node_B_2 zugewiesen
- Alle Festplatten an Site_B-Shelf_2 werden Pool 1 der Node_A_1 automatisch zugewiesen
- Alle Festplatten an Site_B-Shelf_4 werden Pool 1 der Node_A_2 automatisch zugewiesen
- Alle Festplatten an Site_A-Shelf_2 werden Pool 1 der Node_B_1 automatisch zugewiesen
- Alle Festplatten auf Site_A-Shelf_4 werden automatisch Pool 1 der Node_B_2 zugewiesen

Wie partielle Shelves befüllt werden

Wenn Ihre Konfiguration Shelfs verwendet, die nicht vollständig befüllt sind (über leere Laufwerksschächte), müssen Sie die Laufwerke je nach Richtlinien für die Festplattenzuordnung gleichmäßig im Shelf verteilen. Die Richtlinie für die Festplattenzuweisung hängt davon ab, wie viele Shelfs an jedem MetroCluster Standort vorhanden sind.

Wenn Sie an jedem Standort ein einzelnes Shelf verwenden (oder nur das interne Shelf auf einem AFF A800 System), werden Festplatten anhand einer ViertelShelf-Richtlinie zugewiesen. Wenn das Shelf nicht vollständig gefüllt ist, installieren Sie die Laufwerke gleichmäßig auf allen Quartalen.

Die folgende Tabelle zeigt ein Beispiel dafür, wie 24 Festplatten in einem internen Shelf mit 48 Laufwerken platziert werden. Das Eigentum an den Laufwerken wird ebenfalls angezeigt.

Die 48 Laufwerkschächte sind in vier Quartale unterteilt:	Installieren Sie sechs Laufwerke in den ersten sechs Schächten in jedem Quartal…
Quartal: Buchten 0-11	Schächte 0-5
Quartal: Buchten 12-23	Schächte 12-17
Quartal 3: Buchten 24-35	Schächte 24-29
Quartal 4: Buchten 36-47	Schächte 36-41

Die folgende Tabelle zeigt ein Beispiel zum Platzieren von 16 Festplatten in ein internes Shelf mit 24 Laufwerken.

Die 24 Laufwerkschächte sind in vier Quartale unterteilt:	Installieren Sie vier Laufwerke in den ersten vier Schächten pro Quartal…
Quartal: Buchten 0-5	Schächte 0-3
Quartal 2: Buchten 6-11	Schächte 6-9
Quartal 3: Buchten 12-17	Schächte 12-15
Quartal 4: Buchten 18-23	Schächte 18-21

Wenn Sie zwei externe Shelfs an jedem Standort verwenden, werden Festplatten anhand einer halben Shelf-Richtlinie zugewiesen. Wenn die Shelfs nicht vollständig gefüllt sind, installieren Sie die Laufwerke an beiden Enden des Shelfs gleich.

Wenn Sie beispielsweise 12 Laufwerke in einem Shelf mit 24 Laufwerken installieren, installieren Sie Laufwerke in den Einschüben 0-5 und 18-23.

Manuelle Laufwerkszuweisung (ONTAP 9.5)

In ONTAP 9.5 ist bei Systemen mit den folgenden Shelf-Konfigurationen eine manuelle Laufwerkszuweisung erforderlich:

- Drei externe Shelves pro Standort.

  Zwei Shelfs werden automatisch anhand einer Richtlinie für die Zuweisung halber Shelfs zugewiesen, das dritte Shelf muss jedoch manuell zugewiesen werden.

- Mehr als vier Shelves pro Standort und die Gesamtzahl der externen Shelves ist kein Vielfaches von vier.

  Zusätzliche Shelves über dem nächstgelegenen Mehrfach von vier werden nicht zugewiesen und die Laufwerke müssen manuell zugewiesen werden. Wenn z. B. an dem Standort fünf externe Shelfs vorhanden sind, müssen dann fünf Shelfs manuell zugewiesen werden.

Sie müssen nur ein einziges Laufwerk für jedes nicht zugewiesene Shelf manuell zuweisen. Die restlichen Laufwerke auf dem Shelf werden dann automatisch zugewiesen.

Manuelle Laufwerkszuweisung (ONTAP 9.4)

In ONTAP 9.4 ist bei Systemen mit den folgenden Shelf-Konfigurationen eine manuelle Laufwerkszuweisung erforderlich:

- Weniger als vier externe Shelfs pro Standort.

  Die Laufwerke müssen manuell zugewiesen werden, um eine symmetrische Zuweisung der Laufwerke zu gewährleisten, wobei jeder Pool eine gleiche Anzahl von Laufwerken hat.

- Pro Standort mehr als vier externe Shelves und die Gesamtzahl der externen Shelves ist kein Vielfaches von vier.

Zusätzliche Shelves über dem nächstgelegenen Mehrfach von vier werden nicht zugewiesen und die Laufwerke müssen manuell zugewiesen werden.

Wenn Laufwerke manuell zugewiesen werden, sollten Sie Festplatten symmetrisch zuweisen, wobei jeder Pool eine gleiche Anzahl von Laufwerken zugewiesen ist. Wenn die Konfiguration beispielsweise zwei Storage-Shelfs an jedem Standort umfasst, würden Sie ein Shelf zum lokalen HA-Paar und ein Shelf zum Remote HA-Paar verwenden:

- Weisen Sie die Hälfte der Festplatten auf Site_A-Shelf_1 dem Pool 0 von Node_A_1 zu.
- Weisen Sie die Hälfte der Festplatten auf site_A-Shelf_1 dem Pool 0 von Node_A_2 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_A-Shelf_2 Pool 1 von Node_B_1 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_A-Shelf_2 Pool 1 von Node_B_2 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_1 dem Pool 0 von Node_B_1 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_1 dem Pool 0 von Node_B_2 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_2 Pool 1 von Node_A_1 zu.
- Weisen Sie die Hälfte der Festplatten auf Site_B-Shelf_2 Pool 1 von Node_A_2 zu.

Hinzufügen von Shelfs zu einer vorhandenen Konfiguration

Die automatische Laufwerkszuweisung unterstützt das symmetrische Hinzufügen von Shelfs zu einer vorhandenen Konfiguration.

Beim Hinzufügen neuer Shelves wendet das System dieselbe Zuweisungsrichtlinie auf neu hinzugefügte Shelfs an. Wenn beispielsweise bei einem einzelnen Shelf pro Standort ein zusätzliches Shelf hinzugefügt wird, wenden die Systeme die vierteljährlichen Regeln für die Zuweisung von Shelfs auf das neue Shelf an.

Verwandte Informationen

"Erforderliche MetroCluster IP-Komponenten und Namenskonventionen"

"Festplatten- und Aggregatmanagement"

ADP- und Festplattenzuordnungsunterschiede nach System in MetroCluster IP-Konfigurationen

Der Betrieb von ADP (Advanced Drive Partitioning) und die automatische Festplattenzuordnung in MetroCluster IP Konfigurationen variiert je nach Systemmodell.

In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird. Das Root-Aggregat wird mithilfe von P3-Partitionen erstellt.

Sie müssen die MetroCluster-Grenzwerte für die maximale Anzahl unterstützter Laufwerke und anderer Richtlinien einhalten.

"NetApp Hardware Universe"

ADP und Festplattenzuordnung auf AFF A320-Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition

Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Ein Shelf wird von dem lokalen HA-Paar verwendet. Das zweite Shelf wird vom Remote HA-Paar verwendet. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP- und Festplattenzuordnung für AFF Systeme A150, ASA A150 und AFF A220

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition

Minimal empfohlene Laufwerke (pro Standort)	Nur interne Laufwerke	Die internen Laufwerke sind in vier gleiche Gruppen unterteilt. Jede Gruppe wird automatisch einem separaten Pool zugewiesen, und jeder Pool wird einem separaten Controller in der Konfiguration zugewiesen. **Hinweis:** die Hälfte der internen Laufwerke bleibt nicht zugewiesen, bevor MetroCluster konfiguriert wird.	Das lokale HA-Paar verwendet zwei Quartale. Die anderen zwei Quartale werden von dem Remote HA-Paar verwendet. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

Mindestens unterstützte Laufwerke (pro Standort)	16 interne Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen. Zwei Viertel auf einem Regal können den gleichen Pool haben. Der Pool wird basierend auf dem Knoten ausgewählt, der das Quartal besitzt: • Wenn der Eigentümer des lokalen Knotens ist, wird Pool0 verwendet. • Wenn der Remote-Knoten im Besitz ist, wird Pool1 verwendet. Ein Shelf mit den Quartalen Q1 bis Q4 kann beispielsweise folgende Aufgaben haben: • Q1: Node_A_1 pool0 • Q2: Node_A_2 pool0 • Q3: Node_B_1 pool1 • Q4:Node_B_2 Pool1 **Hinweis:** die Hälfte der internen Laufwerke bleibt nicht zugewiesen, bevor MetroCluster konfiguriert wird.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Zwei Partitionen für Daten • Zwei Paritätspartitionen • Keine Ersatzteile

ADP- und Festplattenzuweisung für AFF A250, AFF C250, ASA A250, ASA C250, FAS500f, AFF A20, AFF A30 und AFF C30 Systeme

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition

Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke (nur externe Laufwerke, keine internen Laufwerke)	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Ein Shelf wird von dem lokalen HA-Paar verwendet. Das zweite Shelf wird vom Remote HA-Paar verwendet. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
	48 Laufwerke (externe und interne Laufwerke)	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Regalen sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	16 interne Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Zwei Partitionen für Daten • Zwei Paritätspartitionen • Keine Ersatzpartitionen

ADP und Festplattenzuweisung auf AFF A50 und AFF C60 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke (nur externe Laufwerke, keine internen Laufwerke)	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Das lokale HA-Paar verwendet ein Shelf. Das Remote-HA-Paar verwendet das zweite Shelf. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
	48 Laufwerke (externe und interne Laufwerke)	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Regalen sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 interne Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Zwei Partitionen für Daten • Zwei Paritätspartitionen • Keine Ersatzpartitionen

ADP und Festplattenzuordnung auf AFF A300 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Ein Shelf wird von dem lokalen HA-Paar verwendet. Das zweite Shelf wird vom Remote HA-Paar verwendet. Partitionen auf jedem Shelf werden verwendet, um das Root-Aggregat zu erstellen. Das Root-Aggregat enthält die folgenden Partitionen in jedem Plex: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält die folgenden Partitionen: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP- und Festplattenzuweisung auf AFF C400-, AFF A400-, ASA C400- und ASA A400-Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • 20 Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen

Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP und Festplattenzuordnung auf AFF A700 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • 20 Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

ADP und Festplattenzuweisung auf AFF C800, ASA C800, ASA A800 und AFF A800 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Aggregat

Minimal empfohlene Laufwerke (pro Standort)	Interne Laufwerke und 96 externe Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Shelfs werden automatisch Shelf-einzeln zugewiesen, wobei allen Laufwerken in jedem Shelf einer der vier Nodes in der MetroCluster-Konfiguration zugewiesen ist.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen **Hinweis:** das Root-Aggregat wird mit 12 Root-Partitionen auf dem internen Regal erstellt.
Mindestens unterstützte Laufwerke (pro Standort)	24 interne Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartitionen **Hinweis:** das Root-Aggregat wird mit 12 Root-Partitionen auf dem internen Regal erstellt.

ADP- und Festplattenzuweisung auf AFF A70-, AFF A90- und AFF C80-Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Aggregat

Minimal empfohlene Laufwerke (pro Standort)	Interne Laufwerke und 96 externe Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Shelfs werden automatisch Shelf-einzeln zugewiesen, wobei allen Laufwerken in jedem Shelf einer der vier Nodes in der MetroCluster-Konfiguration zugewiesen ist.	Jedes der beiden Plexe im Root-Aggregat enthält: • Acht Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 interne Laufwerke	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartitionen

ADP- und Festplattenzuordnung für AFF Systeme A900, ASA A900 und AFF A1K

Richtlinie	Shelves pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • 20 Partitionen für Daten • Zwei Paritätspartitionen • Zwei Ersatzpartitionen
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Jedes der beiden Plexe im Root-Aggregat enthält: • Drei Partitionen für Daten • Zwei Paritätspartitionen • Eine Ersatzpartition

Festplattenzuordnung bei FAS2750 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	24 interne Laufwerke und 24 externe Laufwerke	Die internen und externen Regale sind in zwei gleiche Hälften unterteilt. Jede Hälfte wird automatisch einem anderen Pool zugewiesen	Keine Angabe
Minimal unterstützte Laufwerke (pro Standort) (aktiv/Passiv HA-Konfiguration)	Nur interne Laufwerke	Manuelle Zuweisung erforderlich	Keine Angabe

Festplattenzuordnung bei FAS8200 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke	Die Laufwerke auf den externen Shelfs sind in zwei gleiche Gruppen (Hälften) unterteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe
Minimal unterstützte Laufwerke (pro Standort) (aktiv/Passiv HA-Konfiguration)	24 Laufwerke	Manuelle Zuweisung erforderlich.	Keine Angabe

Festplattenzuordnung auf FAS500f Systemen

Für FAS500f Systeme gelten die gleichen Richtlinien und Regeln für die Festplattenzuordnung bei AFF C250 und AFF A250 Systemen. Informationen zur Festplattenzuordnung bei FAS500f Systemen finden Sie im [ADP_FAS500f] Tabelle:

Festplattenzuordnung auf FAS9000, FAS9500, FAS70 und FAS90 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	96 Laufwerke	Laufwerke werden automatisch Shelf-für-Shelf zugewiesen.	Keine Angabe

Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe

Festplattenzuordnung auf FAS50 Systemen

Richtlinie	Laufwerke pro Standort	Zuweisungsregeln für Laufwerke	ADP-Layout für Root-Partition
Minimal empfohlene Laufwerke (pro Standort)	48 Laufwerke (nur externe Laufwerke, keine internen Laufwerke)	Die Laufwerke auf jedem externen Shelf werden in zwei gleiche Gruppen (Hälften) aufgeteilt. Jedes halbe Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe
	48 Laufwerke (externe und interne Laufwerke)	Die internen Partitionen sind in vier gleiche Gruppen (Quartiere) unterteilt. Jedes Quartal wird automatisch einem separaten Pool zugewiesen. Die Laufwerke auf den externen Regalen sind in vier gleiche Gruppen (Quartale) unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe
Mindestens unterstützte Laufwerke (pro Standort)	24 Laufwerke	Die Laufwerke sind in vier gleiche Gruppen unterteilt. Jedes Quartals-Shelf wird automatisch einem separaten Pool zugewiesen.	Keine Angabe

Anforderungen für Cluster-Peering in MetroCluster IP-Konfigurationen

Jede MetroCluster Website ist als Peer-to-dessen Partner-Website konfiguriert. Sie müssen die Voraussetzungen und Richtlinien für die Konfiguration der Peering-Beziehungen kennen. Dies ist wichtig, wenn Sie entscheiden, ob Sie freigegebene oder

dedizierte Ports für diese Beziehungen verwenden möchten.

Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

Voraussetzungen für Cluster-Peering

Bevor Sie Cluster-Peering einrichten, sollten Sie bestätigen, dass die Verbindungsanforderungen zwischen Port, IP-Adresse, Subnetz, Firewall und Cluster-Benennungsanforderungen erfüllt sind.

Konnektivitätsanforderungen erfüllen

Jede Intercluster LIF auf dem lokalen Cluster muss in der Lage sein, mit jeder Intercluster LIF auf dem Remote-Cluster zu kommunizieren.

Es ist zwar nicht erforderlich, aber in der Regel ist es einfacher, die IP-Adressen zu konfigurieren, die für Intercluster LIFs im selben Subnetz verwendet werden. Die IP-Adressen können sich im gleichen Subnetz wie Daten-LIFs oder in einem anderen Subnetz befinden. Das in jedem Cluster verwendete Subnetz muss die folgenden Anforderungen erfüllen:

- Das Subnetz muss über genügend IP-Adressen verfügen, um einer Intercluster LIF pro Node zuzuweisen.

  Beispielsweise muss in einem Cluster mit vier Nodes das für die Kommunikation zwischen Clustern verwendete Subnetz vier verfügbare IP-Adressen haben.

Jeder Node muss über eine Intercluster-LIF mit einer IP-Adresse im Intercluster-Netzwerk verfügen.

Intercluster-LIFs können eine IPv4-Adresse oder eine IPv6-Adresse besitzen.

> ONTAP 9 ermöglicht Ihnen die Migration Ihrer Peering-Netzwerke von IPv4 zu IPv6, indem Sie optional zulassen, dass beide Protokolle gleichzeitig auf den Intercluster LIFs vorhanden sind. In früheren Versionen waren alle Cluster-Beziehungen für einen gesamten Cluster entweder IPv4 oder IPv6. Somit war eine Änderung der Protokolle ein potenziell störendes Ereignis.

Port-Anforderungen

Sie können dedizierte Ports für die Cluster-übergreifende Kommunikation verwenden oder vom Datennetzwerk verwendete Ports freigeben. Ports müssen folgende Anforderungen erfüllen:

- Alle Ports, die für die Kommunikation mit einem bestimmten Remote-Cluster verwendet werden, müssen sich im gleichen IPspace befinden.

  Sie können mehrere IPspaces verwenden, um mit mehreren Clustern zu Punkten. Paarweise ist Vollmaschenverbindung nur innerhalb eines IPspaces erforderlich.

- Die für die Cluster-übergreifende Kommunikation verwendete Broadcast-Domäne muss mindestens zwei Ports pro Node enthalten, sodass eine Cluster-übergreifende Kommunikation von einem Port zu einem anderen Port ausfallen kann.

  Ports, die einer Broadcast-Domäne hinzugefügt werden, können physische Netzwerk-Ports, VLANs oder Interface Groups (iffrps) sein.

- Alle Ports müssen verkabelt sein.

- Alle Ports müssen sich in einem ordnungsgemäßen Zustand befinden.
- Die MTU-Einstellungen der Ports müssen konsistent sein.

Anforderungen an die Firewall

Firewalls und die Cluster-übergreifende Firewall-Richtlinie müssen folgende Protokolle zulassen:

- ICMP-Dienst
- TCP auf die IP-Adressen aller Cluster-LIFs über die Ports 10000, 11104 und 11105
- Bidirektionales HTTPS zwischen den Intercluster-LIFs

Die standardmäßige Cluster-Firewallrichtlinie ermöglicht den Zugriff über das HTTPS-Protokoll und über alle IP-Adressen (0.0.0.0/0). Sie können die Richtlinie bei Bedarf ändern oder ersetzen.

Überlegungen bei der Verwendung von dedizierten Ports

Wenn Sie feststellen, ob die Verwendung eines dedizierten Ports für die Intercluster-Replikation die richtige Intercluster-Netzwerklösung ist, sollten Sie Konfigurationen und Anforderungen wie LAN-Typ, verfügbare WAN-Bandbreite, Replikationsintervall, Änderungsrate und Anzahl der Ports berücksichtigen.

Berücksichtigen Sie die folgenden Aspekte Ihres Netzwerks, um zu ermitteln, ob die Verwendung eines dedizierten Ports die beste Intercluster-Netzwerklösung ist:

- Wenn die verfügbare WAN-Bandbreite der der LAN-Ports ähnelt und das Replizierungsintervall so ist, dass eine Replizierung auftritt, während die normale Client-Aktivität besteht, sollten Sie Ethernet-Ports für die Cluster-übergreifende Replizierung zuweisen, um Konflikte zwischen der Replizierung und den Datenprotokollen zu vermeiden.
- Wenn die durch die Datenprotokolle (CIFS, NFS und iSCSI) generierte Netzwerkauslastung eine über 50%ige Netzwerkauslastung bedeutet, dann dedizierte Ports für die Replizierung, die bei einem Node-Failover die Performance nicht beeinträchtigen.
- Wenn physische 10-GbE- oder schnellere Ports für Daten und Replikation verwendet werden, können Sie VLAN-Ports für die Replikation erstellen und die logischen Ports für die Cluster-übergreifende Replikation zuweisen.

  Die Bandbreite des Ports wird von allen VLANs und dem Basis-Port gemeinsam genutzt.

- Berücksichtigen Sie die Datenänderungsrate und das Replizierungsintervall und ob die Datenmenge, die in jedem Intervall repliziert werden muss, genug Bandbreite erfordert. Dies kann zu Konflikten mit Datenprotokollen führen, wenn Daten-Ports gemeinsam genutzt werden.

Überlegungen bei der Freigabe von Datenports

Wenn Sie feststellen, ob die gemeinsame Nutzung eines Datenports für die Intercluster-Replikation die richtige Intercluster-Netzwerklösung ist, sollten Sie Konfigurationen und Anforderungen wie LAN-Typ, verfügbare WAN-Bandbreite, Replikationsintervall, Änderungsrate und Anzahl der Ports berücksichtigen.

Berücksichtigen Sie die folgenden Aspekte Ihres Netzwerks, um zu ermitteln, ob die gemeinsame Nutzung von Datenports die beste Intercluster-Konnektivitätslösung ist:

- In einem High-Speed-Netzwerk, wie etwa einem 40-Gigabit-Ethernet-Netzwerk (40-GbE), steht möglicherweise ausreichend lokale LAN-Bandbreite zur Verfügung, um eine Replizierung auf denselben 40-GbE-Ports durchzuführen, die für den Datenzugriff verwendet werden.

In vielen Fällen ist die verfügbare WAN-Bandbreite weit kleiner als die 10 GbE-LAN-Bandbreite.

- Unter Umständen müssen alle Nodes im Cluster Daten replizieren und die verfügbare WAN-Bandbreite gemeinsam nutzen, sodass die gemeinsame Nutzung von Daten-Ports akzeptabel ist.
- Durch die gemeinsame Nutzung von Ports für Daten und Replizierung werden keine zusätzlichen Ports mehr benötigt, die für die Bereitstellung dedizierter Ports für die Replikation benötigt werden.
- Die MTU-Größe (Maximum Transmission Unit) des Replikationsnetzwerks entspricht der Größe des Netzwerks.
- Berücksichtigen Sie die Datenänderungsrate und das Replizierungsintervall und ob die Datenmenge, die in jedem Intervall repliziert werden muss, genug Bandbreite erfordert. Dies kann zu Konflikten mit Datenprotokollen führen, wenn Daten-Ports gemeinsam genutzt werden.
- Wenn Daten-Ports für die Cluster-übergreifende Replizierung gemeinsam genutzt werden, können die Intercluster LIFs zu jedem anderen Cluster-fähigen Port desselben Nodes migriert werden, um den spezifischen Datenport zu steuern, der zur Replizierung verwendet wird.

ISL-Anforderungen

Inter-Switch-Link-Anforderungen für MetroCluster IP-Konfigurationen

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

NetApp-validierte und MetroCluster-kompatible Switches in einer MetroCluster IP-Konfiguration

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.

Anforderungen für Inter-Switch Links (ISLs) in MetroCluster -IP-Konfigurationen

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 Mikroplatzausbrüchen 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 oder 25 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 Gbit/s oder 25 Gbit/s.
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 oder 25 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.

Voraussetzungen für die Bereitstellung von MetroCluster IP-Konfigurationen 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 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.

- Nicht alle Funktionen werden in allen Netzwerktopologien unterstützt.
- 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.

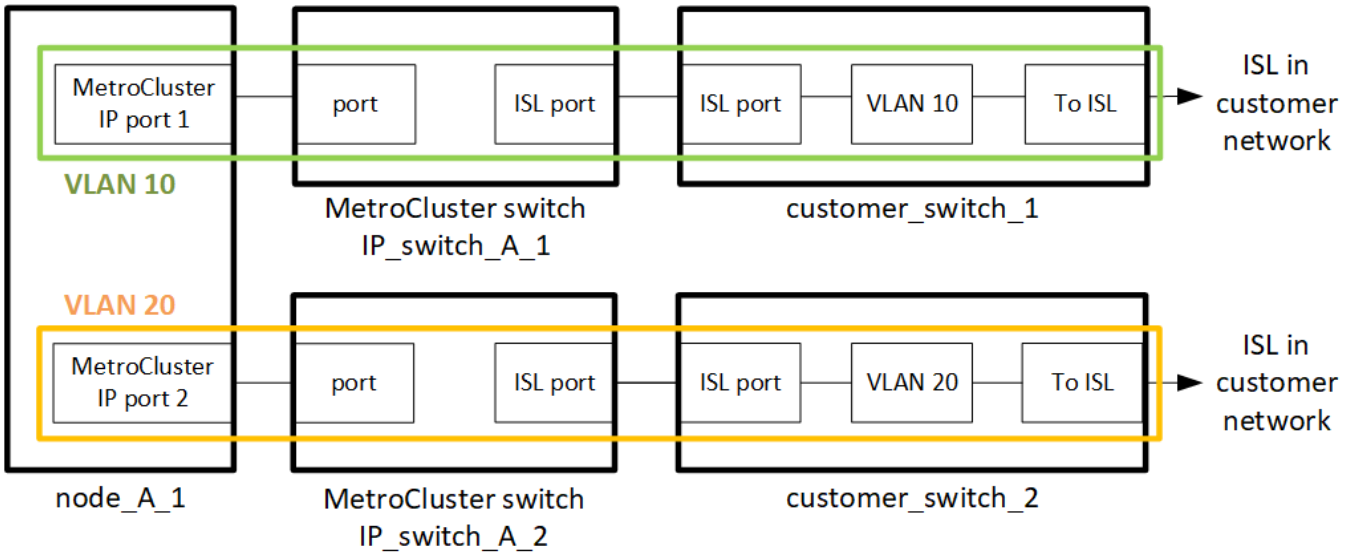
- Die MTU-Größe muss für alle Ports mit MetroCluster-End-to-End-Datenverkehr auf 9216 eingestellt sein.
- Kein anderer Datenverkehr kann mit einer höheren Priorität konfiguriert werden als Class of Service (COS) 5.
- Die explizite Staubenachrichtigung (ECN) muss auf allen Pfaden konfiguriert werden, 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. Sie können die Standard-VLANs 10 und 20 oder VLANs im Bereich von 101 bis 4096 (oder die vom Switch-Anbieter unterstützte Anzahl, je nachdem, welcher Wert niedriger ist) konfigurieren. Nachdem die MetroCluster-Schnittstellen erstellt wurden, können Sie die VLAN-ID nicht mehr ändern.

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

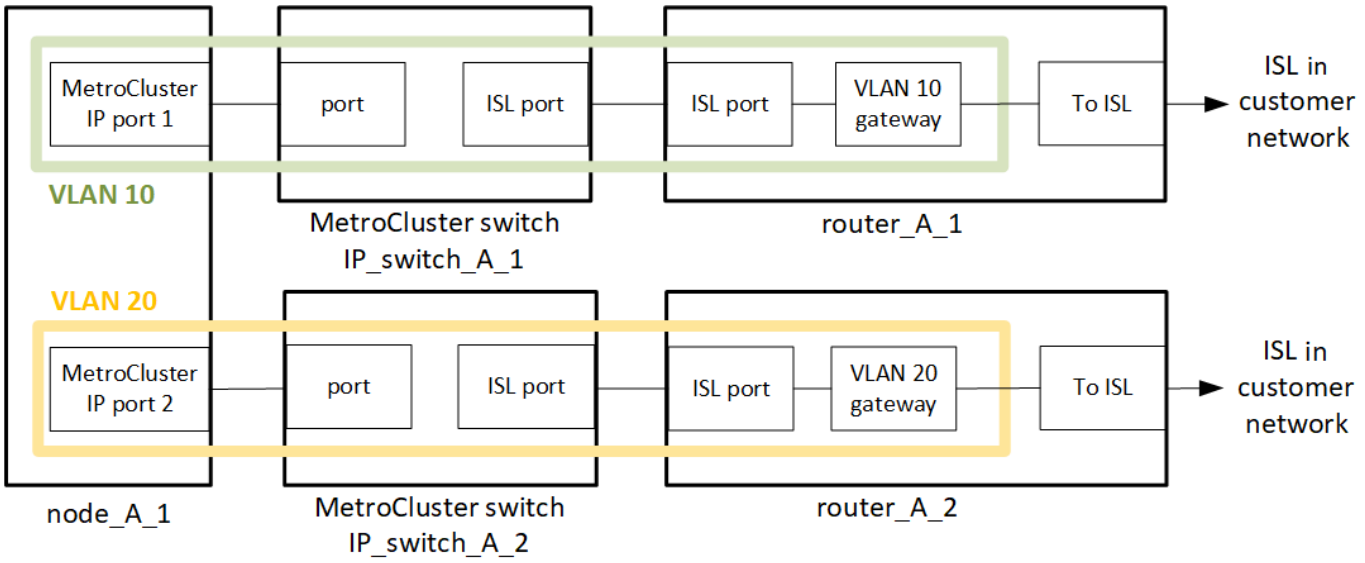
Die oben aufgeführten Systeme können mit VLANs 100 und niedriger konfiguriert werden. Einige VLANs in diesem Bereich sind jedoch möglicherweise für andere oder zukünftige Zwecke reserviert.

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.

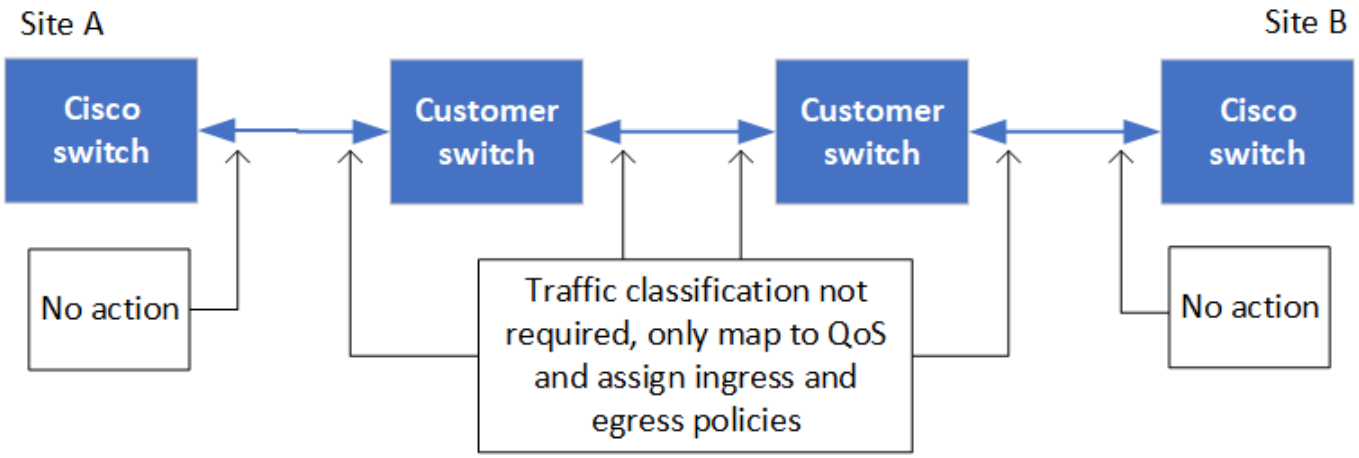
Wenn Sie Router und Gateway-IP-Adressen konfigurieren, müssen Sie die folgenden Anforderungen erfüllen:

- 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.

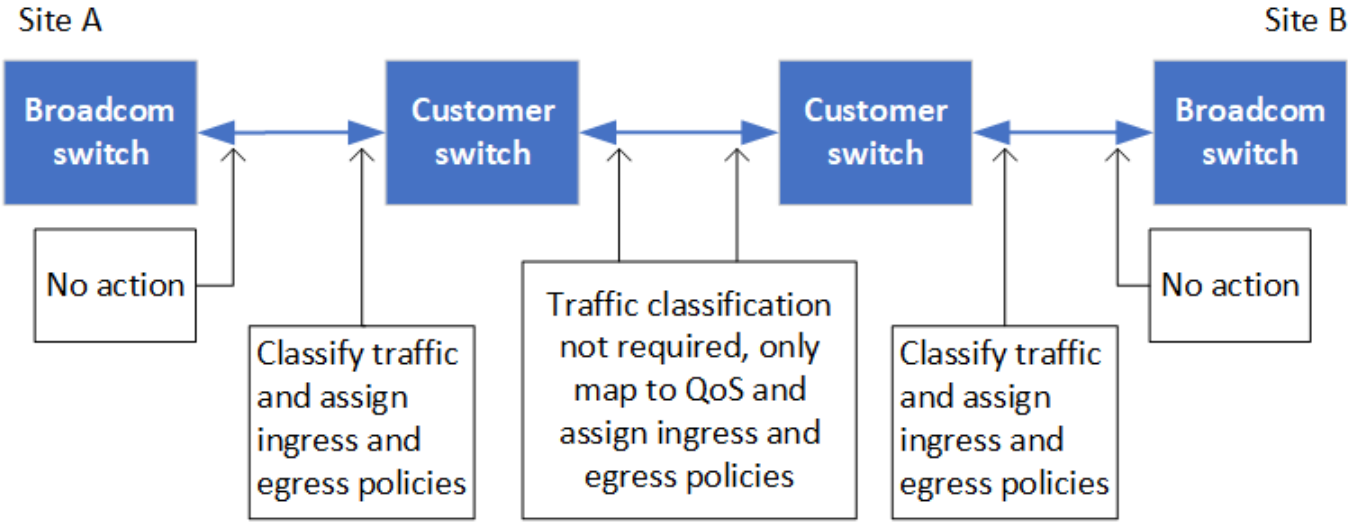
Erforderliche Einstellungen für Zwischenschalter

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 Zwischenswitters

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.

Beispiele für die Netzwerktopologie der MetroCluster IP-Konfiguration

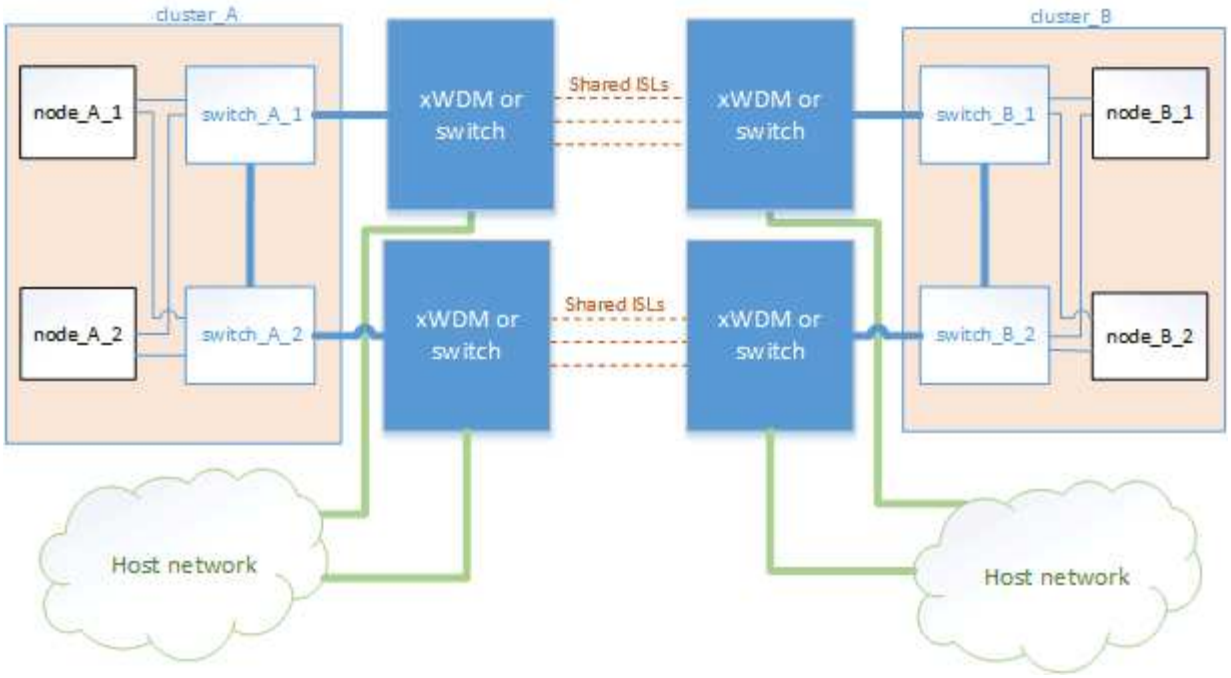
Ab ONTAP 9.6 werden einige zusätzliche Netzwerkkonfigurationen für MetroCluster IP-Konfigurationen unterstützt. Dieser Abschnitt enthält einige Beispiele für unterstützte Netzwerkkonfigurationen. Es werden nicht alle unterstützten Topologien aufgeführt.

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.

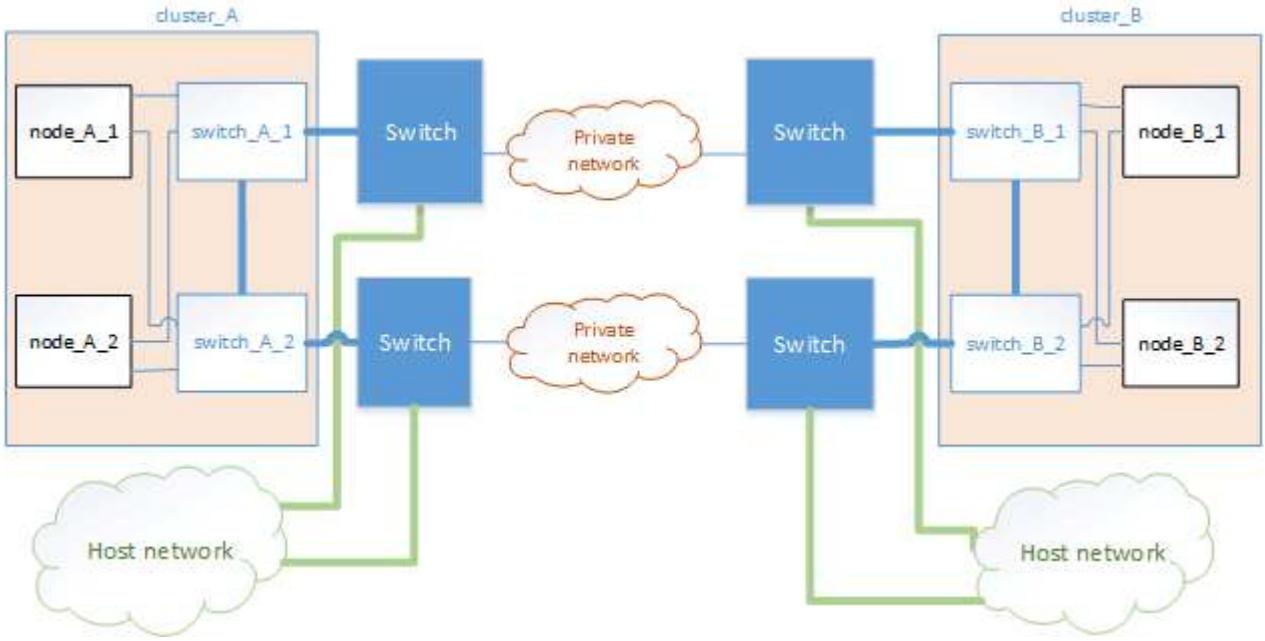
Konfiguration für gemeinsam genutztes Netzwerk mit direkten Links

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

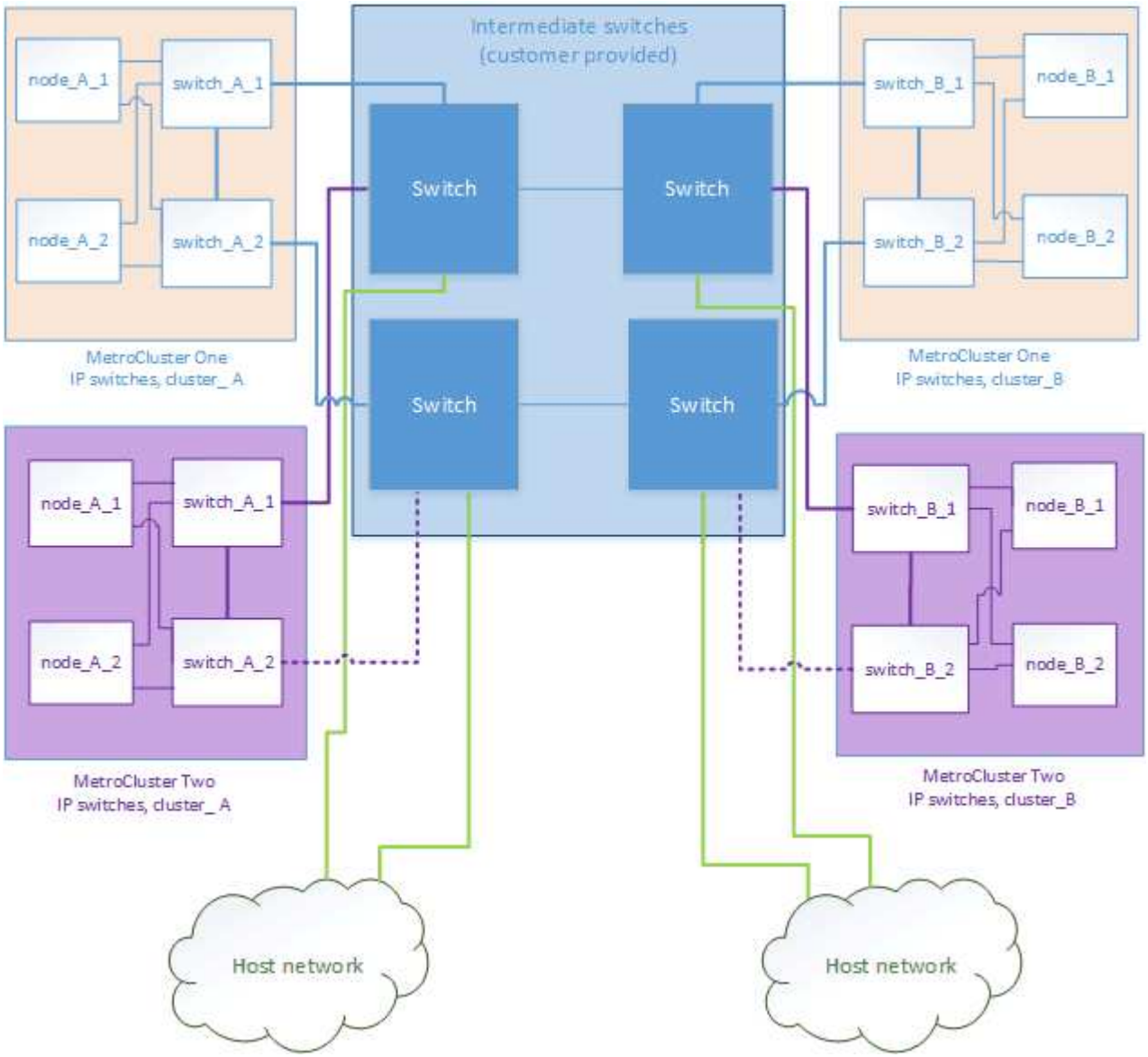
In dieser Topologie sind die MetroCluster-Standorte nicht direkt verbunden, sondern MetroCluster und der Host-Datenverkehr werden über ein Netzwerk geleitet. Das Netzwerk kann aus einer Reihe von xWDM und TDM und Switches bestehen, aber im Gegensatz zur gemeinsamen Konfiguration mit direkten ISLs sind 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

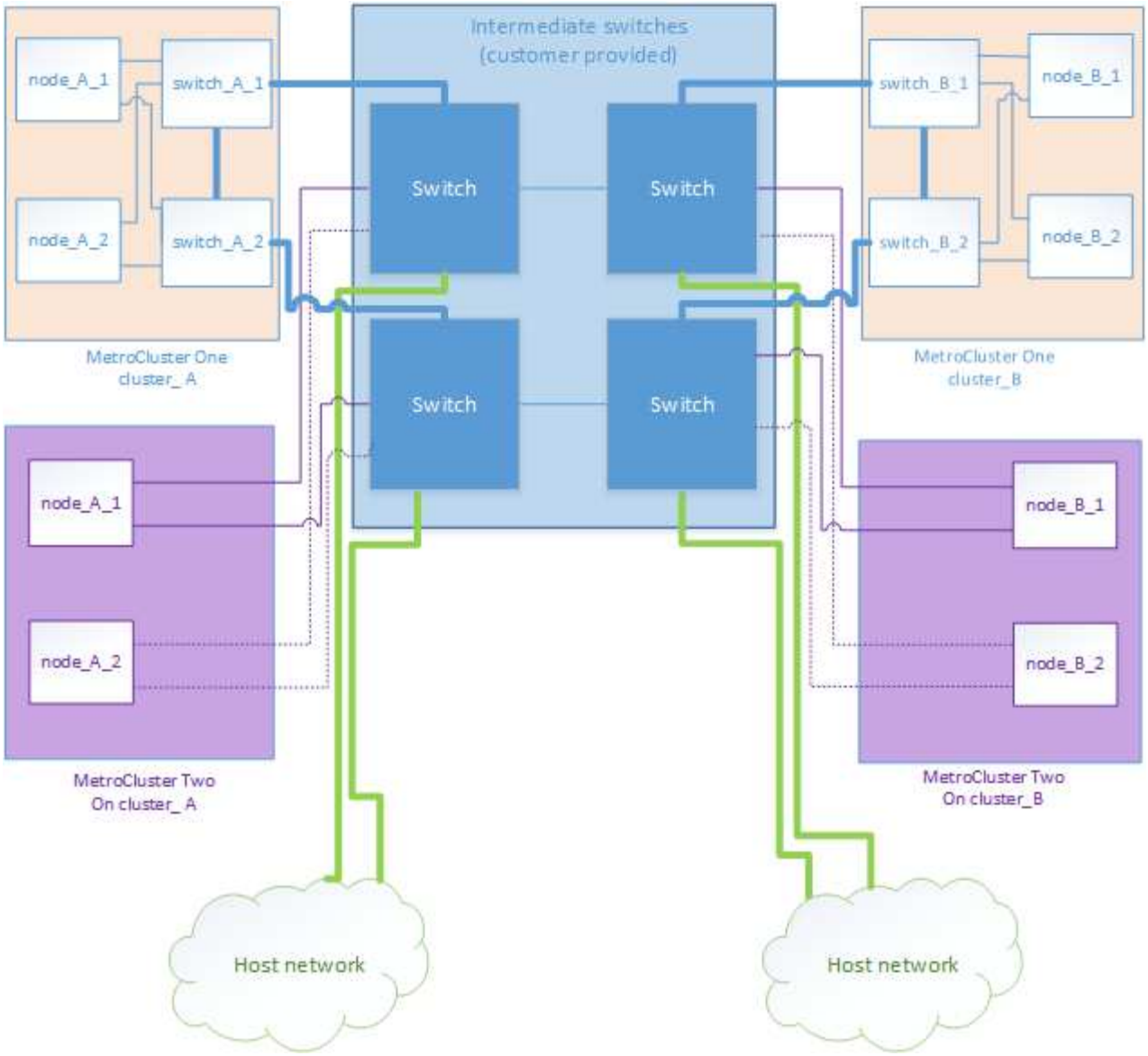
In dieser Topologie teilen sich zwei separate MetroCluster-Konfigurationen dasselbe Zwischennetzwerk. Im Beispiel MetroCluster One Switch_A_1 und MetroCluster Two Switch_A_1 verbinden sich beide mit demselben Zwischenswitch.

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).



Überlegungen zur Verwendung von MetroCluster-konformen Switches

Anforderungen und Einschränkungen für MetroCluster-kompatible 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.

MetroCluster-konform und 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.

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.

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.

ONTAP -plattformspezifische Netzwerkgeschwindigkeiten und Switch-Port-Modi für MetroCluster-kompatible 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.
- Für die Systeme AFF A30, AFF C30, AFF C60 und FAS50 ist ein QSFP-zu-SFP+ Adapter in der Karte des Controllers erforderlich, um eine Netzwerkgeschwindigkeit von 25 Gbit/s zu unterstützen.

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	-	-
AFF A20	25Gbps	trunk mode
AFF A30	25Gbps or 100Gbps	trunk mode
AFF C30	25Gbps or 100Gbps	trunk mode
AFF C60	25Gbps or 100Gbps	trunk mode
FAS50	25Gbps or 100Gbps	trunk mode
AFF A50	100Gbps	trunk mode
AFF A70	100Gbps	trunk mode
AFF A90	100Gbps	trunk mode
AFF A1K	100Gbps	trunk mode
AFF C80	100Gbps	trunk mode
FAS70	100Gbps	trunk mode
FAS90	100Gbps	trunk mode

Beispiele für die Konfiguration von MetroCluster IP-Switches

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.

Erfahren Sie mehr über nicht gespiegelte Aggregate in MetroCluster -IP -Konfigurationen

Wenn Ihre Konfiguration nicht gespiegelte Aggregate umfasst, müssen potenzielle Zugriffsprobleme nach dem Switchover berücksichtigt werden.

Ungespiegelte Aggregate und hierarchische Namespaces

Wenn Sie hierarchische Namespaces verwenden, sollten Sie den Verbindungspfad so konfigurieren, dass alle Volumes in diesem Pfad sich entweder nur auf gespiegelten Aggregaten oder nur auf nicht gespiegelten Aggregaten befinden. Wenn Sie eine Kombination aus nicht gespiegelten und gespiegelten Aggregaten im Verbindungspfad konfigurieren, ist möglicherweise nach der Umschaltung der Zugriff auf nicht gespiegelte Aggregate verhindert.

Ungespiegelte Aggregate und Wartung, die eine Stromabschaltung erfordert

Wenn Sie zu Wartungszwecken eine vereinbarte Umschaltung durchführen, die eine standortweite Stromabschaltung erfordert, sollten Sie zunächst alle nicht gespiegelten Aggregate im Besitz des Notfallstandorts manuell offline schalten.

Wenn Sie die nicht gespiegelten Aggregate des Notfallstandorts nicht offline schalten, können Knoten am verbleibenden Standort aufgrund von Multi-Disk-Panics ausfallen. Dies kann passieren, wenn umgeschaltete nicht gespiegelte Aggregate offline gehen oder fehlen, weil die Verbindung zum Speicher am Notfallstandort nach einem Stromausfall oder dem Verlust von ISLs verloren geht.

Ungespiegelte Aggregate, CRS-Metadatenvolumes und Daten-SVM-Root-Volumes

Der Configuration Replication Service (CRS) Metadaten-Volume und Daten-SVM-Root-Volumes müssen sich in einem gespiegelten Aggregat befinden. Sie können diese Volumes nicht in ein nicht gespiegeltes Aggregat verschieben. Wenn sie sich auf einem nicht gespiegelten Aggregat befinden, werden ausgehandelte Switchover- und Switchback-Operationen blockiert und die `metrocluster check` Befehl gibt eine Warnung zurück.

Ungespiegelte Aggregate und SVMs

Sie sollten SVMs nur auf gespiegelten oder nicht gespiegelten Aggregaten konfigurieren. Die Konfiguration von SVMs auf einer Mischung aus nicht gespiegelten und gespiegelten Aggregaten kann zu einem Umschaltvorgang führen, der länger als 120 Sekunden dauert. Dies kann zu einem Datenausfall führen, wenn die nicht gespiegelten Aggregate nicht online gehen.

Ungespiegelte Aggregate und SAN

Vor ONTAP 9.9.1 sollte sich eine LUN nicht auf einem nicht gespiegelten Aggregat befinden. Das Konfigurieren einer LUN auf einem nicht gespiegelten Aggregat kann zu einem Switchover von mehr als 120 Sekunden bei einem Ausfall der Daten führen.

Lagerregale für ungespiegelte Aggregate hinzufügen

Wenn Sie Regale hinzufügen und diese für nicht gespiegelte Aggregate in einer MetroCluster -IP-Konfiguration verwenden möchten, müssen Sie Folgendes tun:

1. Bevor Sie das Verfahren zum Hinzufügen der Shelves starten, geben Sie den folgenden Befehl ein:

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment true
   ```

2. Vergewissern Sie sich, dass die automatische Festplattenzuordnung deaktiviert ist:

   ```
   disk option show
   ```

3. Befolgen Sie die Schritte des Verfahrens, um das Regal hinzuzufügen.
4. Weisen Sie den Node, der im Besitz des nicht gespiegelten Aggregats oder der Aggregate ist, manuell alle Festplatten aus dem neuen Shelf zu.
5. Erstellen Sie die Aggregate:

   ```
   storage aggregate create
   ```

6. Geben Sie nach Abschluss des Verfahrens den folgenden Befehl ein:

```
metrocluster modify -enable-unmirrored-aggr-deployment false
```

7. Vergewissern Sie sich, dass die automatische Festplattenzuordnung aktiviert ist:

```
disk option show
```

Firewall-Portanforderungen für MetroCluster IP-Konfigurationen

Wenn Sie eine Firewall an einem MetroCluster-Standort verwenden, müssen Sie den Zugriff auf bestimmte erforderliche Ports sicherstellen.

Überlegungen zur Firewall-Nutzung an MetroCluster Standorten

Wenn Sie eine Firewall an einem MetroCluster-Standort verwenden, müssen Sie den Zugriff auf die erforderlichen Ports sicherstellen.

Die folgende Tabelle zeigt die Verwendung von TCP/UDP-Ports in einer externen Firewall, die zwischen zwei MetroCluster-Standorten positioniert ist.

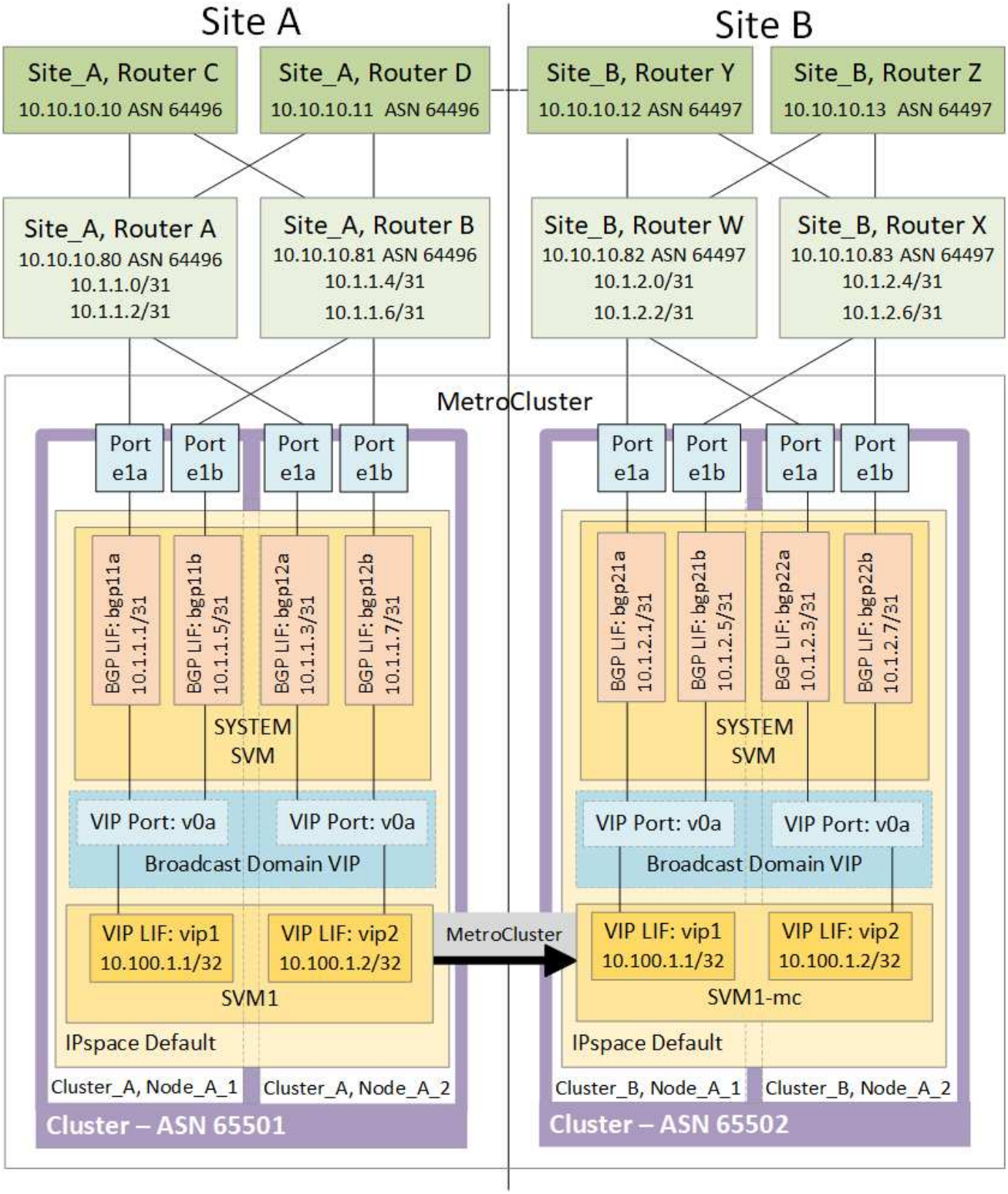
Verkehrstyp	Port/Services
Cluster-Peering	11104 / TCP 11105 / TCP
ONTAP System Manager	443 / TCP
MetroCluster IP Intercluster LIFs	65200 / TCP 10006 / TCP und UDP
Hardwareunterstützung	4444 / TCP

Erfahren Sie mehr über die Verwendung von virtueller IP und Border Gateway Protocol mit einer MetroCluster -IP-Konfiguration

Ab ONTAP 9.5 unterstützt ONTAP Layer-3-Konnektivität mithilfe von Virtual IP (VIP) und Border Gateway Protocol (BGP). Die Kombination aus VIP und BGP für Redundanz im Front-End-Netzwerk und der Back-End MetroCluster-Redundanz bietet eine Layer 3 Disaster Recovery-Lösung.

Lesen Sie die folgenden Richtlinien und Illustrationen bei der Planung Ihrer Layer 3-Lösung. Einzelheiten zur Implementierung von VIP und BGP in ONTAP finden Sie im folgenden Abschnitt:

"Konfigurieren der virtuellen IP (VIP)-LIFs"



ONTAP Einschränkungen

ONTAP überprüft nicht automatisch, ob alle Nodes auf beiden Standorten der MetroCluster Konfiguration mit BGP-Peering konfiguriert sind.

ONTAP führt keine Route-Aggregation durch, kündigt aber alle einzelnen virtuellen LIF-IPs jederzeit als

eindeutige Host-Routen an.

ONTAP unterstützt keine True Anycast - nur ein einzelner Node im Cluster weist eine bestimmte virtuelle LIF-IP auf (wird aber von allen physischen Schnittstellen akzeptiert, unabhängig davon, ob es sich um BGP LIFs handelt, vorausgesetzt, der physische Port ist Teil des korrekten IPspace). Verschiedene LIFs können unabhängig voneinander zu unterschiedlichen Hosting-Nodes migriert werden.

Richtlinien für die Verwendung dieser Layer 3-Lösung mit einer MetroCluster-Konfiguration

Sie müssen Ihr BGP und VIP korrekt konfigurieren, um die erforderliche Redundanz zu gewährleisten.

Einfachere Bereitstellungsszenarien werden gegenüber komplexeren Architekturen bevorzugt (beispielsweise ist ein BGP Peering Router über einen zwischengeschalteten, nicht BGP Router erreichbar). ONTAP ist jedoch nicht durch Einschränkungen in Netzwerkdesign oder Topologie eingeschränkt.

VIP LIFs decken nur das Frontend-/Datennetzwerk ab.

Je nach Ihrer Version von ONTAP müssen Sie BGP Peering LIFs in der Node-SVM konfigurieren, nicht jedoch das System oder die Daten-SVM. Im Jahr 9.8 sind die BGP LIFs in der Cluster (System) SVM sichtbar und die Node-SVMs sind nicht mehr vorhanden.

Jede Daten-SVM erfordert die Konfiguration aller potenziellen First-Hop-Gateway-Adressen (normalerweise der BGP-Router, der IP-Adresse Peering), sodass der Return-Datenpfad bei einer LIF-Migration oder einem MetroCluster-Failover verfügbar ist.

BGP LIFs sind Node-spezifisch, ähnlich wie Intercluster LIFs – jeder Node verfügt über eine eindeutige Konfiguration, die nicht auf DR-Standort-Nodes repliziert werden muss.

Die Existenz des v0a (v0b usw.) überprüft kontinuierlich die Konnektivität und garantiert, dass eine LIF-Migration oder ein Failover erfolgreich ist (im Gegensatz zu L2, wo eine defekte Konfiguration nur nach dem Ausfall sichtbar ist).

Ein großer Unterschied in der Architektur besteht darin, dass Clients nicht mehr dasselbe IP Subnetz wie die VIP der Daten-SVMs teilen sollten. Ein L3-Router mit den entsprechenden Resiliency- und Redundanzfunktionen der Enterprise-Klasse (z. B. VRRP/HSRP) sollte sich auf dem Weg zwischen Speicher und Clients befinden, damit der VIP ordnungsgemäß funktioniert.

Der zuverlässige Aktualisierungsprozess von BGP ermöglicht reibungslosere LIF-Migrationen, da sie geringfügig schneller sind und die Wahrscheinlichkeit einer Unterbrechung für einige Clients niedriger ist

Sie können BGP so konfigurieren, dass einige Klassen von Netzwerk- oder Switch-Fehlverhalten schneller als LACP erkannt werden, wenn diese entsprechend konfiguriert werden.

Externe BGP (EBGP) verwendet unterschiedliche Zahlen als Nummern zwischen ONTAP-Knoten und Peering-Routern und ist die bevorzugte Bereitstellung, um die Routenaggregation und -Umverteilung auf den Routern zu vereinfachen. Interne BGP (IBGP) und die Verwendung von Routenreflektoren ist nicht unmöglich, aber außerhalb des Umfangs einer einfachen VIP-Einrichtung.

Nach der Implementierung müssen Sie prüfen, ob auf die Daten-SVM zugegriffen werden kann, wenn die zugehörige virtuelle LIF zwischen allen Nodes an jedem Standort (einschließlich MetroCluster-Umschaltung) migriert wird. So müssen Sie sicherstellen, dass die korrekte Konfiguration der statischen Routen zu derselben Daten-SVM korrekt ist.

VIP funktioniert für die meisten IP-basierten Protokolle (NFS, SMB, iSCSI).

Konfigurieren Sie die Hardwarekomponenten von MetroCluster

Erfahren Sie mehr über die Verbindungen von Hardwarekomponenten in einer MetroCluster -IP-Konfiguration

Bei der Planung Ihrer MetroCluster IP-Konfiguration sollten Sie sich mit den Hardwarekomponenten und den zugehörigen Verbindungen vertraut machen.

Wichtige Hardwarekomponenten

Eine MetroCluster IP-Konfiguration umfasst die folgenden wichtigen Hardwarekomponenten:

- Storage Controller

  Die Storage Controller sind als zwei-Node-Cluster konfiguriert.

- IP-Netzwerk

  Dieses Back-End-IP-Netzwerk bietet Konnektivität für zwei unterschiedliche Anwendungen:

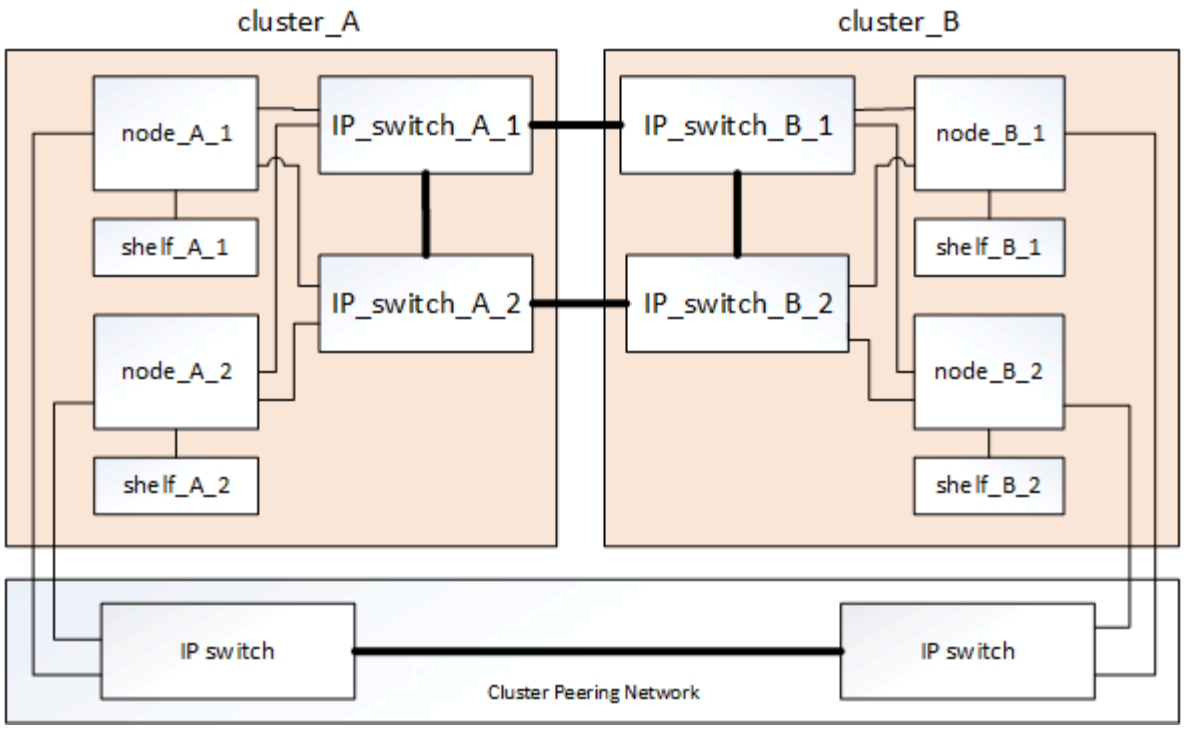
  - Standardmäßige Cluster-Konnektivität für die Cluster-interne Kommunikation

    Dies ist dieselbe Cluster-Switch-Funktion, die auch in nicht-MetroCluster-ONTAP-Clustern mit Switch verwendet wird.

  - MetroCluster Back-End-Konnektivität für die Replizierung von Storage-Daten und nichtflüchtigem Cache

- Cluster-Peering-Netzwerk

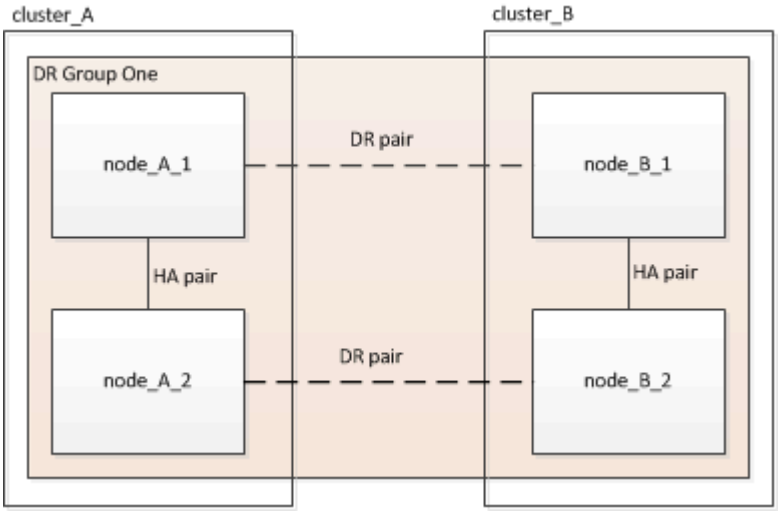
  Das Cluster-Peering-Netzwerk bietet Konnektivität zur Spiegelung der Cluster-Konfiguration, einschließlich der Storage Virtual Machine (SVM)-Konfiguration. Die Konfiguration aller SVMs auf einem Cluster wird dem Partner-Cluster gespiegelt.



Disaster-Recovery-Gruppen (DR)

Eine MetroCluster IP-Konfiguration besteht aus einer DR-Gruppe mit vier Nodes.

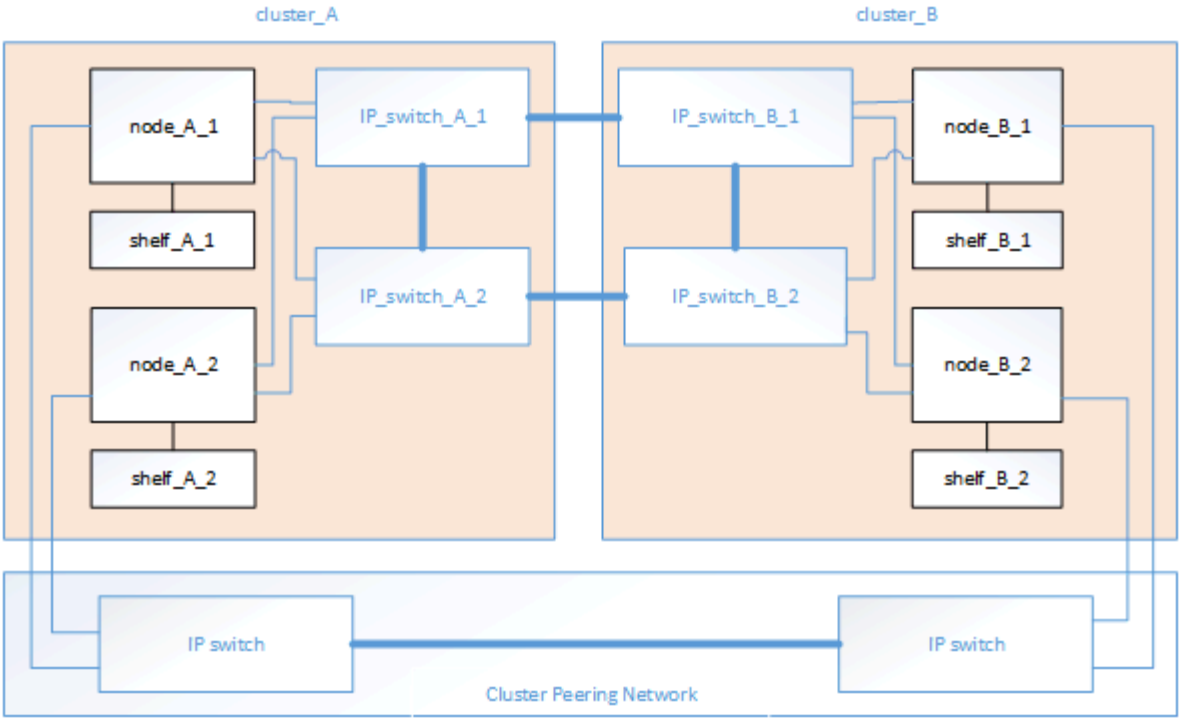
Die folgende Abbildung zeigt die Organisation der Nodes in einer MetroCluster Konfiguration mit vier Nodes:



Darstellung der lokalen HA-Paare in einer MetroCluster Konfiguration

Jeder MetroCluster Standort besteht aus Storage Controllern, die als HA-Paar konfiguriert sind. Dadurch wird lokale Redundanz ermöglicht, sodass der lokale HA-Partner übernimmt, wenn ein Storage Controller ausfällt. Solche Ausfälle können ohne MetroCluster-Switchover-Operation behoben werden.

Lokale HA-Failover- und Giveback-Vorgänge werden mit Storage Failover-Befehlen auf gleiche Weise durchgeführt wie eine andere Konfiguration von MetroCluster.

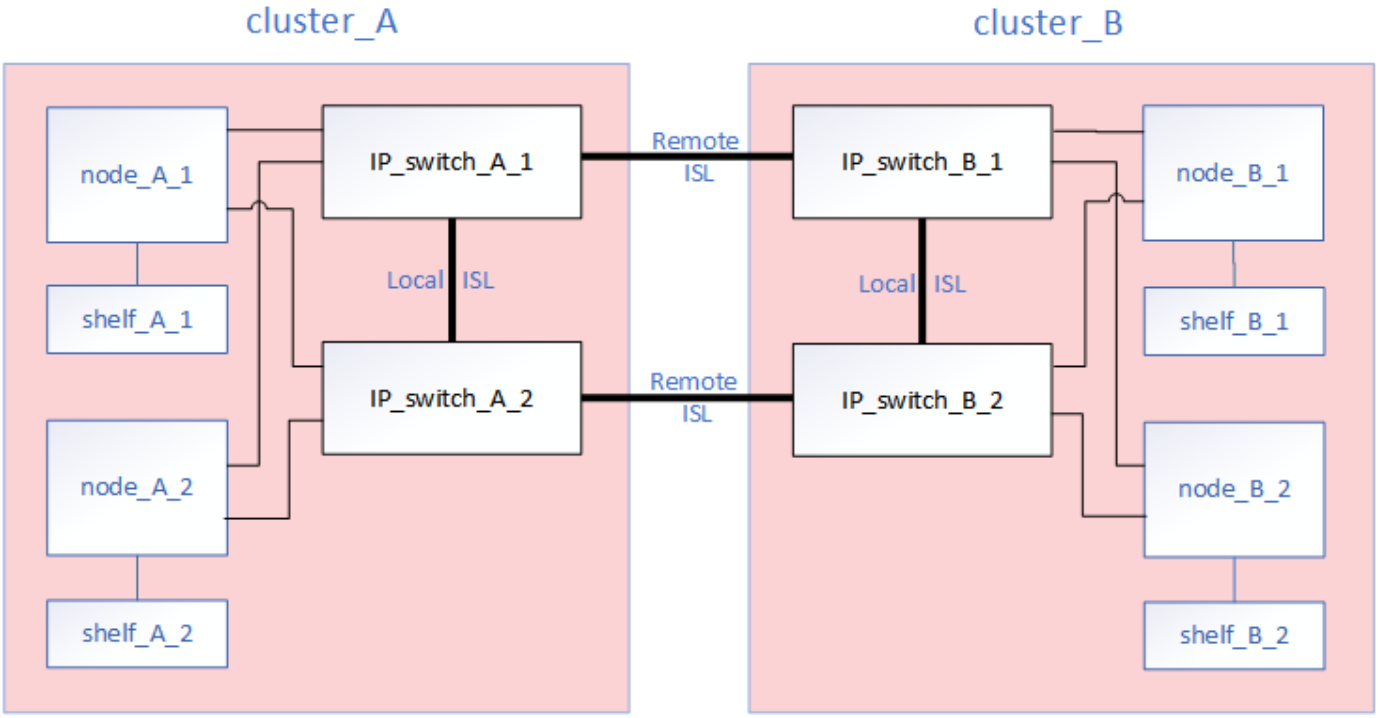


Verwandte Informationen

"ONTAP-Konzepte"

Darstellung des MetroCluster IP- und Cluster Interconnect-Netzwerks

ONTAP Cluster verfügen normalerweise über ein Cluster-Interconnect-Netzwerk für den Datenverkehr zwischen den Nodes im Cluster. In MetroCluster IP-Konfigurationen wird dieses Netzwerk auch für das übertragen von Daten-Replizierungsdatenverkehr zwischen den MetroCluster Standorten verwendet.

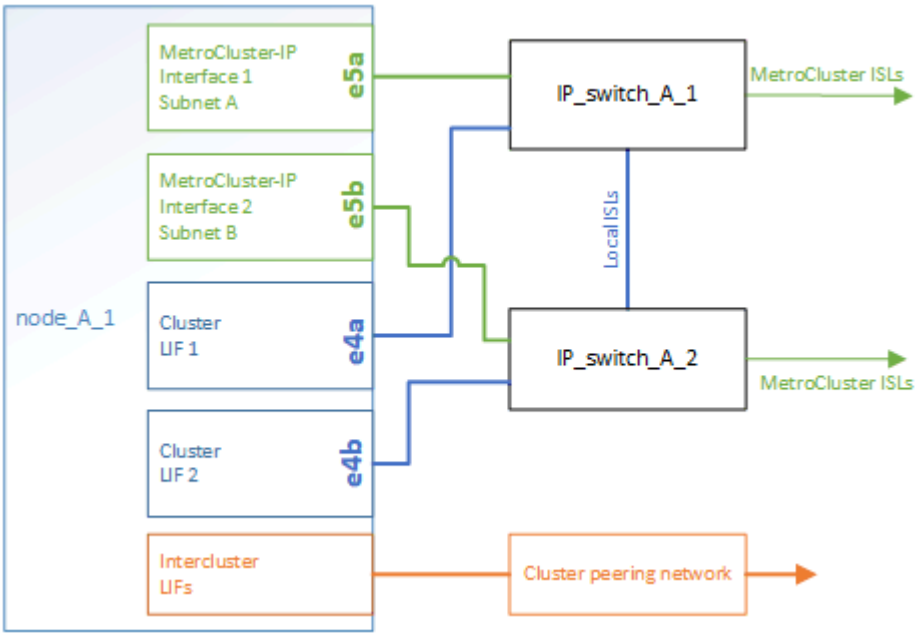


Jeder Node in der MetroCluster IP-Konfiguration verfügt über dedizierte Schnittstellen zur Verbindung mit dem

Back-End IP-Netzwerk:

- Zwei MetroCluster IP-Schnittstellen
- Zwei lokale Cluster-Schnittstellen

Die folgende Abbildung zeigt diese Schnittstellen. Die angegebene Port-Nutzung gilt für ein AFF A700 oder FAS9000 System.



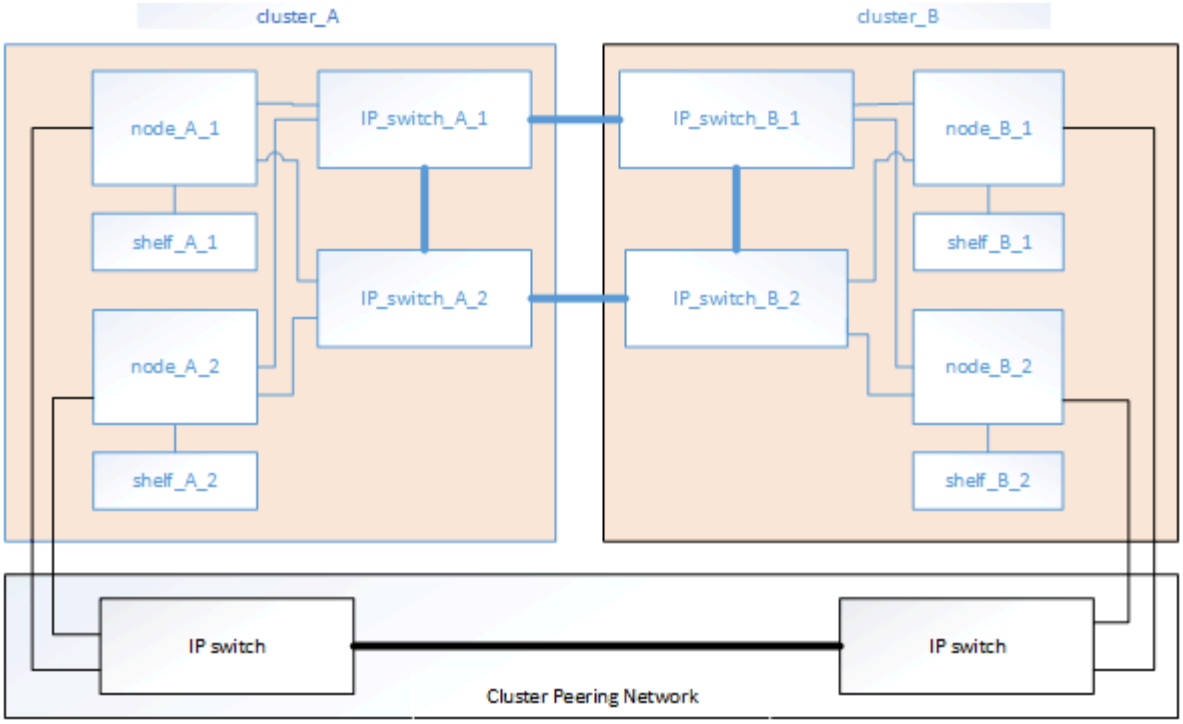
Verwandte Informationen

"Überlegungen für MetroCluster IP-Konfigurationen"

Illustration des Cluster-Peering-Netzwerks

Die beiden Cluster in der MetroCluster Konfiguration werden über ein vom Kunden bereitgestellter Cluster-Peering-Netzwerk Peering Peering durchgeführt. Cluster Peering unterstützt die synchrone Spiegelung von Storage Virtual Machines (SVMs, früher Vserver genannt) zwischen den Standorten.

Intercluster-LIFs müssen auf jedem Node in der MetroCluster-Konfiguration konfiguriert werden, und die Cluster müssen für Peering konfiguriert sein. Die Ports mit den Intercluster-LIFs sind mit dem vom Kunden bereitgestellten Cluster-Peering-Netzwerk verbunden. Die Replizierung der SVM-Konfiguration erfolgt über dieses Netzwerk über den Configuration Replication Service.



Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

"Überlegungen für die Konfiguration von Cluster-Peering"

"Verkabeln der Cluster-Peering-Verbindungen"

"Peering der Cluster"

Erforderliche MetroCluster IP-Konfigurationskomponenten und Namenskonventionen

Wenn Sie Ihre MetroCluster IP-Konfiguration planen, müssen Sie die erforderlichen und unterstützten Hardware- und Softwarekomponenten kennen. Für Einfachheit und Klarheit sollten Sie auch die Namenskonventionen verstehen, die für Komponenten in Beispielen in der gesamten Dokumentation verwendet werden.

Unterstützte Software und Hardware

Hardware und Software müssen für die MetroCluster IP-Konfiguration unterstützt werden.

"NetApp Hardware Universe"

Beim Einsatz von AFF Systemen müssen alle Controller-Module in der MetroCluster Konfiguration als AFF Systeme konfiguriert sein.

Anforderungen an Hardwareredundanz in einer MetroCluster IP-Konfiguration

Aufgrund der Hardware-Redundanz in der MetroCluster IP-Konfiguration gibt es an jedem Standort zwei Komponenten. Den Standorten werden die Buchstaben A und B willkürlich zugeordnet, und den einzelnen Komponenten werden die Zahlen 1 und 2 willkürlich zugeordnet.

ONTAP-Cluster-Anforderungen in einer MetroCluster IP-Konfiguration

Für MetroCluster IP-Konfigurationen sind zwei ONTAP Cluster erforderlich, eines an jedem MetroCluster Standort.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
- Standort B: Cluster_B

IP-Switch-Anforderungen in einer MetroCluster IP-Konfiguration

Für MetroCluster IP-Konfigurationen sind vier IP-Switches erforderlich. Die vier Switches bilden zwei Switch-Storage-Fabrics, die in der MetroCluster IP-Konfiguration zwischen jedem der Cluster die ISL bieten.

Zudem sorgen die IP-Switches für eine Intracluster-Kommunikation zwischen den Controller-Modulen in jedem Cluster.

Die Benennung muss innerhalb der MetroCluster Konfiguration eindeutig sein.

Beispielnamen:

- Standort A: Cluster_A
  - IP_Switch_A_1
  - IP_Switch_A_2
- Standort B: Cluster_B
  - IP_Switch_B_1
  - IP_Switch_B_2

Anforderungen an das Controller-Modul in einer MetroCluster IP-Konfiguration

MetroCluster IP-Konfigurationen erfordern vier oder acht Controller-Module.

Die Controller-Module an jedem Standort bilden ein HA-Paar. Jedes Controller-Modul besitzt einen DR-Partner am anderen Standort.

Jedes Controller-Modul muss die gleiche ONTAP-Version aufweisen. Unterstützte Plattformmodelle sind von der ONTAP Version abhängig:

- Neue MetroCluster IP-Installationen auf FAS Systemen werden in ONTAP 9.4 nicht unterstützt.

  Vorhandene MetroCluster IP Konfigurationen auf FAS Systemen können auf ONTAP 9.4 aktualisiert werden.

- Ab ONTAP 9.5 werden neue MetroCluster IP-Installationen auf FAS Systemen unterstützt.
- Ab ONTAP 9.4 werden für ADP konfigurierte Controller-Module unterstützt.

Beispielnamen

Die folgenden Beispielnamen werden in der Dokumentation verwendet:

- Standort A: Cluster_A
  - Controller_A_1
  - Controller_A_2
- Standort B: Cluster_B
  - Controller_B_1
  - Controller_B_2

Anforderungen für Gigabit-Ethernet-Adapter in einer MetroCluster IP-Konfiguration

Bei den MetroCluster IP-Konfigurationen wird für die IP-Schnittstellen zu den für das MetroCluster IP Fabric verwendeten IP-Switches ein Ethernet-Adapter mit 40/100 Gbit/s oder 10/25 Gbit/s verwendet.

Integrierte Ports sind in die Controller-Hardware (Steckplatz 0) integriert und können nicht ersetzt werden, der erforderliche Steckplatz für den Adapter ist daher nicht verfügbar.

Modell der Plattform	Erforderlicher Gigabit-Ethernet-Adapter	Erforderlicher Steckplatz für Adapter	Ports
AFF A900, ASA A900 und FAS9500	X91146A	Steckplatz 5, Steckplatz 7	E5b, e7b **Hinweis:** Die Ports e5a und e7a können nur für Intercluster-LIFs verwendet werden. Sie können diese Ports nicht für ein Daten-LIF verwenden.
AFF A700 UND FAS9000	X91146A-C	Einschubfach 5	e5a, e5b
AFF A800, AFF C800, ASA A800 und ASA C800	X1146A/Onboard-Ports	Steckplatz 1/gilt nicht für Onboard-Ports	e0b: e1b
FAS8300, AFF A400, ASA A400, ASA C400 und AFF C400	X1146A	Steckplatz 1	e1a, e1b
AFF A300 UND FAS8200	X1116 A	Steckplatz 1	e1a, e1b
FAS2750, AFF A150, ASA A150 und AFF A220	Onboard-Ports	Keine Angabe	e0a, e0b
FAS500f, AFF A250, ASA A250, ASA C250 und AFF C250	Onboard-Ports	Keine Angabe	e0c, e0d
AFF A320	Onboard-Ports	Keine Angabe	e0g, e0h

AFF A70, FAS70	X50132A	Steckplatz 2	e2a, e2b
AFF A90, AFF A1K, FAS90, AFF C80	X50132A	Steckplatz 2, Steckplatz 3	e2b, e3b **Hinweis:** die Ports e2a und e3a müssen unbenutzt bleiben. Die Verwendung dieser Ports für Front-End-Netzwerke oder Peering wird nicht unterstützt.
AFF A50	X60134A	Steckplatz 2	e2a, e2b
AFF A30, AFF C30, AFF C60, FAS50	X60134A	Steckplatz 2	e2a, e2b
AFF A20	X60132A	Steckplatz 4, Steckplatz 2	e2b, e4b

"Erfahren Sie mehr über die automatische Laufwerkszuordnung und ADP-Systeme in MetroCluster IP-Konfigurationen".

Pool- und Festplattenanforderungen (mindestens unterstützt)

Es werden acht SAS-Platten-Shelves empfohlen (vier Shelfs an jedem Standort), damit sich die Anschaffung von Festplatten pro Shelf zulässt.

MetroCluster IP-Konfigurationen mit vier Nodes erfordern an jedem Standort die Minimalkonfiguration:

- Jeder Node hat mindestens einen lokalen Pool und einen Remote-Pool am Standort.
- Mindestens sieben Laufwerke pro Pool.

  In einer MetroCluster-Konfiguration mit vier Nodes und einem einzelnen gespiegelten Datenaggregat pro Node sind für die Minimalkonfiguration 24 Festplatten am Standort erforderlich.

In einer minimal unterstützten Konfiguration verfügt jeder Pool über das folgende Laufwerkslayout:

- Drei Root-Laufwerke
- Drei Datenlaufwerke
- Ein Ersatzlaufwerk

Bei einer unterstützten Minimalkonfiguration ist pro Standort mindestens ein Shelf erforderlich.

MetroCluster-Konfigurationen unterstützen RAID-DP, RAID4 und RAID-TEC.

Ab ONTAP 9.4 unterstützen MetroCluster IP-Konfigurationen neue Installationen mithilfe von automatischer Festplattenzuweisung und ADP (Advanced Drive Partitioning). Weitere Informationen finden Sie unter "Überlegungen zur automatischen Laufwerkszuweisung und ADP-Systemen" .

Überlegungen zum Speicherort von Laufwerken für teilweise bestückte Shelfs

Die Laufwerke sollten sich in den Steckplätzen 0-5 und 18-23 befinden, um Laufwerke bei Verwendung von Shelfs, die halb bestückt sind (12 Laufwerke in einem Shelf mit 24 Laufwerken), automatisch zuweisen.

Bei einer Konfiguration mit einem teilweise bestückten Shelf müssen die Laufwerke gleichmäßig in die vier Quadranten des Shelfs verteilt werden.

Überlegungen zum Laufwerkstandort für interne AFF A800 Laufwerke

Für eine korrekte Implementierung der ADP-Funktion müssen die AFF A800 Systemfestplattenschächte in Quartale aufgeteilt und die Laufwerke symmetrisch in den Quartalen angeordnet sein.

Ein AFF A800 System verfügt über 48 Laufwerkschächte. Die Buchten können in Quartiere unterteilt werden:

- Quartal:
  - Einschübe 0 Bis 5
  - Buchten 24 - 29
- Quartal:
  - Buchten 6 - 11
  - Buchten 30 - 35
- Quartal:
  - Buchten 12 - 17
  - Buchten 36 - 41
- Quartal:
  - Buchten 18 - 23
  - Buchten 42 - 47

Wenn dieses System mit 16 Laufwerken bestückt ist, müssen sie symmetrisch auf die vier Quartale verteilt werden:

- Vier Laufwerke im ersten Quartal: 0, 1, 2, 3
- Im zweiten Quartal vier Laufwerke: 6, 7, 8, 9
- Im dritten Quartal vier Laufwerke: 12, 13, 14, 15
- Vier Laufwerke im vierten Quartal: 18, 19, 20, 21

Mischen von IOM12 und IOM 6 Modulen in einem Stack

Ihre Version von ONTAP muss Shelf-Mix unterstützen. Siehe "NetApp Interoperabilitäts-Matrix-Tool (IMT)" Um zu prüfen, ob Ihre Version von ONTAP Shelf-Mischungen unterstützt.

Weitere Informationen zum Anmischen von Regalen finden Sie unter "Hot-Adding-Shelfs mit IOM12-Modulen werden in einem Shelf-Stack mit IOM6-Modulen ausgeführt"

Rack der MetroCluster IP-Konfigurationshardwarekomponenten

Wenn Sie noch nicht die bereits in den Schränken installierten Geräte erhalten haben, müssen Sie die Komponenten in einem Rack unterbringen.

Über diese Aufgabe

Dieser Task muss auf beiden MetroCluster-Sites ausgeführt werden.

Schritte

1. Planen der Positionierung der MetroCluster Komponenten

   Die Rack-Fläche hängt vom Plattformmodell der Controller-Module, den Switch-Typen und der Anzahl der Festplatten-Shelf-Stacks in Ihrer Konfiguration ab.

2. Richtig gemahlen.
3. Installieren Sie die Controller-Module im Rack oder Schrank.

   Folgen Sie den Schritten zur *Installation der Hardware* unter den *Installations- und Setup-Anweisungen* für Ihr Plattformmodell im"Dokumentation zu ONTAP -Hardwaresystemen" .

4. Installieren Sie die IP-Switches im Rack oder Schrank.
5. Installieren Sie die Festplatten-Shelfs, schalten Sie sie ein und legen Sie die Shelf-IDs fest.

   - Sie müssen jedes Festplatten-Shelf aus- und wieder einschalten.
   - Um die Fehlerbehebung zu unterstützen, werden für jedes SAS-Platten-Shelf in jeder MetroCluster DR-Gruppe eindeutige Shelf-IDs empfohlen.

   > Verkabeln Sie zum jetzigen Zeitpunkt keine Festplatten-Shelfs, die nicht gespiegelte Aggregate enthalten sollen. Sie müssen warten, bis die für nicht gespiegelte Aggregate vorgesehenen Shelfs implementiert sind, bevor die MetroCluster-Konfiguration abgeschlossen ist und diese erst nach Verwendung der implementiert werden `metrocluster modify -enable-unmirrored-aggr-deployment true` Befehl.

MetroCluster IP-Switches verkabeln

So verwenden Sie die Porttabellen mit mehreren MetroCluster IP-Konfigurationen

Sie müssen verstehen, wie die Informationen in den Porttabellen verwendet werden, um Ihre RCF-Dateien korrekt zu generieren.

Bevor Sie beginnen

Lesen Sie vor der Verwendung der Tabellen diese Überlegungen durch:

- In den folgenden Tabellen wird die Portnutzung für Standort A angezeigt Für Standort B wird dieselbe Verkabelung verwendet
- Sie können die Switches nicht mit Ports unterschiedlicher Geschwindigkeit konfigurieren (z. B. eine Mischung aus 100-Gbit/s-Ports und 40-Gbit/s-Ports).
- Verfolgen Sie die MetroCluster-Portgruppe (MetroCluster 1, MetroCluster 2 usw.). Sie benötigen diese Informationen, wenn Sie das Tool RcfFileGenerator verwenden, wie später in diesem Konfigurationsverfahren beschrieben.
- Sie sollten alle Nodes auf die gleiche Weise verkabeln. Wenn für die Verkabelung der Nodes unterschiedliche Portkombinationsoptionen verfügbar sind, sollten alle Nodes die gleichen Port-Kombinationen verwenden. Beispiel: e1a auf Knoten 1 und e1a auf Knoten 2 sollten an einen Schalter angeschlossen werden. Gleichermaßen sollte der zweite Port beider Nodes an den zweiten Switch angeschlossen werden.

- Der "RCfFileGenerator für MetroCluster-IP" bietet außerdem eine Übersicht über die Verkabelung pro Port für jeden Switch. Verwenden Sie diese Verkabelungsübersicht, um Ihre Verkabelung zu überprüfen.

Verkabelung von zwei MetroCluster-Konfigurationen mit den Switches

Wenn Sie mehrere MetroCluster-Konfigurationen an einen Switch anschließen, verkabeln Sie jeden MetroCluster gemäß der entsprechenden Tabelle. Wenn Sie beispielsweise eine FAS2750 und eine AFF A700 an denselben Switch anschließen, verkabeln Sie die FAS2750 gemäß „MetroCluster 1“ in Tabelle 1 und die AFF A700 gemäß „MetroCluster 2“ oder „MetroCluster 3“ in Tabelle 2. Die FAS2750 und die AFF A700 können nicht physisch als „MetroCluster 1“ verkabelt werden.

Verkabelung von MetroCluster Konfigurationen mit acht Nodes

Bei MetroCluster Konfiguration mit ONTAP 9.8 und früher müssen bei einigen Verfahren für die Transition eines Upgrades eine zweite DR-Gruppe mit vier Nodes zur Konfiguration hinzugefügt werden, um eine temporäre Konfiguration mit acht Nodes zu erstellen. Ab ONTAP 9.9 werden dauerhafte MetroCluster-Konfigurationen mit acht Nodes unterstützt.

Über diese Aufgabe

Für Konfigurationen mit acht Knoten verwenden Sie dieselbe Methode wie oben beschrieben. Anstelle einer zweiten MetroCluster ist eine weitere DR-Gruppe mit vier Nodes verkabelt.

Ihre Konfiguration umfasst beispielsweise Folgendes:

- Cisco Switches 3132Q-V
- MetroCluster 1: FAS2750 Plattformen
- MetroCluster 2: AFF A700 Plattformen (Hinzufügen dieser Plattformen als zweite DR-Gruppe mit vier Nodes)

Schritte

1. Verkabeln Sie bei MetroCluster 1 die Cisco 3132Q-V Switches mithilfe der Tabelle für die FAS2750-Plattform und der Zeilen für MetroCluster 1-Schnittstellen.
2. Verkabeln Sie bei MetroCluster 2 (der zweiten DR-Gruppe) die Cisco 3132Q-V-Switches mithilfe der Tabelle für die AFF A700 Plattform und der Zeilen für MetroCluster 2-Schnittstellen.

Plattform-Portzuweisungen für Cisco 3132Q-V-Switches in einer MetroCluster IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Richtlinien, bevor Sie die Tabellen verwenden:

- Wenn Sie den Switch für MetroCluster FC zu IP-Übergang konfigurieren, können Port 5, Port 6, Port 13 oder Port 14 zum Verbinden der lokalen Clusterschnittstellen des MetroCluster FC-Node verwendet werden. Siehe "RCfFileGenerator" Und die generierten Verkabelungsdateien für weitere Details zur Verkabelung dieser Konfiguration. Für alle anderen Verbindungen können Sie die in den Tabellen aufgeführten Port-Nutzungszuweisungen verwenden.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
FAS2750, AFF A220	Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 1)
FAS9000, AFF A700	Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 2)
AFF A800, ASA A800	Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 3)

Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 1)

Plattform-Port-Zuordnungen zum Verkabelung eines FAS2750 oder AFF A220 Systems mit einem Cisco 3132Q-V Switch prüfen:

Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 2)

Plattform-Port-Zuweisungen prüfen, um ein FAS9000 oder AFF A700 System mit einem Cisco 3132Q-V Switch zu verkabeln:

Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Cisco 3132Q-V Plattform-Port-Zuweisungen (Gruppe 3)

Plattform-Port-Zuweisungen prüfen, um ein AFF A800 oder ASA A800 System mit einem Cisco 3132Q-V Switch zu verkabeln:

Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Plattform-Portzuweisungen für Cisco 3232C- oder 36-Port- Cisco 9336C-Switches in einer MetroCluster -IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Die Tabellen in diesem Abschnitt gelten für Cisco 3232C-Switches oder 36-Port-Cisco 9336C-FX2-Switches, die keinen NS224-Speicher verbinden.

  Wenn Sie einen 12-Port Cisco 9336C-FX2 Switch haben, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für 12-Port Cisco 9336C-FX2-Switches" .

  Wenn Sie einen Cisco 9336C-FX2-Switch mit 36 Ports haben und mindestens eine MetroCluster-Konfiguration oder DR-Gruppe NS224-Shelves mit dem MetroCluster-Switch verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für einen 36-Port Cisco 9336C-FX2-Switch, der NS224-Speicher verbindet" .

- In den folgenden Tabellen wird die Portnutzung für Standort A angezeigt Für Standort B wird dieselbe Verkabelung verwendet
- Sie können die Switches nicht mit Ports unterschiedlicher Geschwindigkeit konfigurieren (z. B. eine Mischung aus 100-Gbit/s-Ports und 40-Gbit/s-Ports).
- Wenn Sie eine einzelne MetroCluster mit den Switches konfigurieren, verwenden Sie die Portgruppe **MetroCluster 1**.

  Verfolgen Sie die MetroCluster-Portgruppe (MetroCluster 1, MetroCluster 2, MetroCluster 3 oder MetroCluster 4). Sie benötigen sie, wenn Sie das RcfFileGenerator-Tool verwenden, wie später in diesem Konfigurationsvorgang beschrieben.

- Der RcfFileGenerator für MetroCluster IP bietet auch eine Übersicht über die Verkabelung pro Port für jeden Switch.

  Verwenden Sie diese Verkabelungsübersicht, um Ihre Verkabelung zu überprüfen.

- RCF-Dateiversion Version 2.10 oder höher ist für den 25G-Breakout-Modus für MetroCluster-ISLs erforderlich.
- Für die Verwendung einer anderen Plattform als FAS8200 oder AFF A300 in der Gruppe „MetroCluster 4“ sind ONTAP 9.13.1 oder höher und RCF-Dateiversion 2.00 erforderlich.

> Die Version der RCF-Datei unterscheidet sich von der Version des RCFfilegenerator-Tools, mit dem die Datei generiert wird. Beispielsweise können Sie eine RCF-Datei Version 2.00 mit RCFfilegenerator v1.6c generieren.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS2750, AFF A220 FAS500f, AFF C250, ASA C250 AFF A250, ASA A250	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 1)
AFF A20	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 2)
AFF A30, AFF C30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 3a) oder 100G (Gruppe 3b) Ethernet-Karte verwenden. • Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 3a - 25G) • Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuweisungen (Gruppe 3b - 100G)
FAS8200, AFF A300	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 4)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 5)

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A50	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 6)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 7)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 8)

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 1)

Prüfen der Plattform-Port-Zuordnungen zur Verkabelung von AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 oder ASA A250 mit einem Cisco 3232C oder 9336C-FX2 Switch:

Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 2)

Überprüfen Sie die Zuweisung der Plattformschnittstelle, um ein AFF A20-System mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e2a	e4a
5/2-4		disabled	
6/1		e2a	e4a
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e2b	e4b
13/2-4		disabled	
14/1		e2b	e4b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e2b	e4b
25/2-4		disabled	
26/1		e2b	e4b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e2a	e4a
29/2-4		disabled	
30/1		e2a	e4a
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Cisco 3232C oder Cisco 9336C-FX2 – Plattform-Port-Zuordnungen (Gruppe 3a)

Überprüfen Sie die Zuordnungen der Plattformports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System über eine 25-Gbit-Ethernet-Karte mit vier Ports mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln.

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5/1	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5/2-4		disabled		disabled		disabled	
6/1		e4a	e4b	e4a	e4b	e4a	e4b
6/2-4		disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29/1	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
29/2-4		disabled		disabled		disabled	
30/1		e4a	e4b	e4a	e4b	e4a	e4b
30/2-4		disabled		disabled		disabled	
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Cisco 3232C oder Cisco 9336C-FX2 – Plattform-Port-Zuordnungen (Gruppe 3b)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem Cisco 3232C- oder 9336C-FX2-Switch über eine 100-GB-Ethernet-Karte mit zwei Ports zu verkabeln.

Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
14		e2a	e2b	e2a	e2b	e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
26		e2a	e2b	e2a	e2b	e2a	e2b
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
30		e4a	e4b	e4a	e4b	e4a	e4b
25 - 32	Unused	disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 4)

Überprüfen Sie die Zuordnungen der Plattformports, um ein FAS8200- oder AFF A300-System mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln:

Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, Local Cluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Wenn Sie ein Upgrade von älteren RCF-Dateien durchführen, verwendet die Verkabelungskonfiguration möglicherweise Ports in der Gruppe „MetroCluster 4“ (Ports 25/26 und 29/30).

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 5)

Prüfen der Port-Zuordnungen der Plattformen zur Verkabelung der AFF A320, FAS8300, AFF C400, ASA C400, FAS8700 AFF A400 oder ASA A400 System auf einen Cisco 3232C oder 9336C-FX2 Switch:

Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
2							
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
4							
5	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
10							
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
12							
13	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Für die Verwendung von Ports in der Gruppe „MetroCluster 4“ ist ONTAP 9.13.1 oder höher erforderlich.

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 6)

Überprüfen Sie die Zuweisung der Plattformschnittstelle, um ein AFF A50-System mit einem Cisco 3232C- oder 9336C-FX2-Switch zu verkabeln:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b
6		e4a	e4b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	MetroCluster 3, MetroCluster interface	e2a	e2b
14		e2a	e2b
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25	MetroCluster 4, MetroCluster interface	e2a	e2b
26		e2a	e2b
27 - 28	Unused	disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4b
30		e4a	e4b
25 - 32	Unused	disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled	

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 7)

Plattform-Port-Zuordnungen zur Verkabelung von FAS9000, AFF A700, AFF C800, ASA C800, AFF A800 prüfen, ASA A800, FAS9500, AFF A900 oder ASA A900 System mit einem Cisco 3232C oder 9336C-FX2 Switch:

Switch Port	Port use	FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6							
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	MetroCluster 3, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
14							
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16							
17							
18							
19							
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23/1-4							
24/1-4							
25	MetroCluster 4, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
26							
27 - 28	Unused	disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
30							
31 - 32	Unused	disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled	

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Für die Verwendung von Ports in der Gruppe „MetroCluster 4“ ist ONTAP 9.13.1 oder höher erforderlich.

Cisco 3232C- oder Cisco 9336C-FX2-Plattform-Port-Zuordnungen (Gruppe 8)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A70-, FAS70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System mit einem Cisco 3232C- oder 9336C-FX2 Switch zu verkabeln:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8									
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
12									
13	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
14									
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
16									
17									
18									
19									
20									
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4									
23/1-4									
24/1-4									
25	MetroCluster 4, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
26									
27 - 28	Unused	disabled		disabled		disabled		disabled	
29	MetroCluster 4, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
30									
31 - 32	Unused	disabled		disabled		disabled		disabled	
33 - 36	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled	

Plattform-Portzuweisungen für 12-Port- Cisco 9336C-FX2-Switches in einer MetroCluster -IP -Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Die Tabellen in diesem Abschnitt gelten für 12-Port-Switches Cisco 9336C-FX2.

  Wenn Sie einen 36-Port Cisco 9336C-FX2 Switch haben, der keine NS224-Shelves verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für Cisco 3232C- oder 36-Port-Switches Cisco 9336C-FX2" .

  Wenn Sie einen Cisco 9336C-FX2-Switch mit 36 Ports haben und mindestens eine MetroCluster-Konfiguration oder DR-Gruppe NS224-Shelves mit dem MetroCluster-Switch verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für einen 36-Port Cisco 9336C-FX2-Switch, der NS224-Speicher verbindet" .

  Der 12-Port-Switch Cisco 9336C-FX2 unterstützt nicht den Anschluss von NS224-Shelves an den MetroCluster-Switch.

- In den folgenden Tabellen wird die Portnutzung für Standort A angezeigt Für Standort B wird dieselbe Verkabelung verwendet
- Sie können die Switches nicht mit Ports unterschiedlicher Geschwindigkeit konfigurieren (z. B. eine Mischung aus 100-Gbit/s-Ports und 40-Gbit/s-Ports).
- Wenn Sie eine einzelne MetroCluster mit den Switches konfigurieren, verwenden Sie die Portgruppe **MetroCluster 1**.

Behalten Sie die MetroCluster-Portgruppe (MetroCluster 1, MetroCluster 2) im Auge. Sie benötigen sie, wenn Sie das Tool RcfFileGenerator verwenden, wie später in diesem Konfigurationsverfahren beschrieben.

- Der RcfFileGenerator für MetroCluster IP bietet auch eine Übersicht über die Verkabelung pro Port für jeden Switch.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 1)
AFF A20	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 2)
AFF A30, AFF C30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 3a) oder 100G (Gruppe 3b) Ethernet-Karte verwenden. • Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3a – 25G) • Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3b – 100G)
FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 4)
AFF A50	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 5)
AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 7)

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 1)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A150-, ASA A150-, FAS500f-, AFF C250-, ASA C250-, AFF A250- oder ASA A250-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF A150 ASA A150		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1-4	Unused	disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13-18	Ports disallowed to use	blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 2)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A20-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3a)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mithilfe einer 25G-Ethernet-Karte mit vier Ports an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen.

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23-36	Ports disallowed to use	blocked		blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 3b)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mithilfe einer 100G-Ethernet-Karte mit zwei Ports an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen.

Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Ports disallowed to use	blocked		blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13-18	Ports disallowed to use	blocked		blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
20							
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
22/1-4							
23-36	Ports disallowed to use	blocked		blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 4)

Überprüfen Sie die Portzuweisungen der Plattform, um ein FAS8300-, AFF C400-, ASA C400-, FAS8700-, AFF A400- oder ASA A400-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b
2					
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b
4					
5-6	Ports disallowed to use	blocked		blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b
10					
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b
12					
13-18	Ports disallowed to use	blocked		blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23-36	Ports disallowed to use	blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 5)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A50-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5-6	Ports disallowed to use	blocked	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13-18	Ports disallowed to use	blocked	
19	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster	
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster	
22/1-4			
23-36	Ports disallowed to use	blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 6)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF C800-, ASA C800-, AFF A800-, ASA A800-, FAS9500-, AFF A900- oder ASA A900-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
3 4	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a (note 2)
5-6	Ports disallowed to use	blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
13-18	Ports disallowed to use	blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Hinweis 2: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A-Adapter (40 Gbit/s) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Cisco 9336C-FX2 12-Port-Plattform-Portzuweisungen (Gruppe 7)

Überprüfen Sie die Portzuweisungen der Plattform, um ein AFF A70-, FAS70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System an einen Cisco 9336C-FX2-Switch mit 12 Ports anzuschließen:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
3 4	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
5-6	Ports disallowed to use	blocked		blocked		blocked		blocked	
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
11 12	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2b	e3b	e2b	e3b
13-18	Ports disallowed to use	blocked		blocked		blocked		blocked	
19 20	ISL, MetroCluster native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4	ISL, MetroCluster breakout mode 10G / 25G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
23-36	Ports disallowed to use	blocked		blocked		blocked		blocked	

Hinweis 1: Sie können nur die Ports 19 und 20 **oder** 21 und 22 konfigurieren. Wenn Sie zuerst die Ports 19 und 20 verwenden, werden die Ports 21 und 22 blockiert. Wenn Sie zuerst die Ports 21 und 22 verwenden, werden die Ports 19 und 20 blockiert.

Plattform-Portzuweisungen für einen 36-Port- Cisco 9336C-FX2-Switch, der NS224-Speicher in einer MetroCluster -IP-Konfiguration verbindet

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Die Tabellen in diesem Abschnitt gelten für Cisco 9336C-FX2-Switches mit 36 Ports, wenn mindestens eine MetroCluster-Konfiguration oder DR-Gruppe NS224-Shelves mit dem MetroCluster-Switch verbindet.

  Wenn Sie einen 36-Port Cisco 9336C-FX2 Switch haben, der keinen NS224-Speicher verbindet, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für Cisco 3232C- oder 36-Port-Switches Cisco 9336C-FX2" .

  Wenn Sie einen 12-Port Cisco 9336C-FX2 Switch haben, verwenden Sie die Tabellen in "Plattform-Portzuweisungen für 12-Port Cisco 9336C-FX2-Switches" .

  > ⓘ Der 12-Port-Switch Cisco 9336C-FX2 unterstützt nicht den Anschluss von NS224-Shelves an den MetroCluster-Switch.

- Wenn Sie einen Cisco 9336C-FX2-Switch verkabeln und NS224-Speicher anschließen, können Sie maximal zwei MetroCluster-Konfigurationen oder DR-Gruppen verwenden. Mindestens eine MetroCluster-Konfiguration oder DR-Gruppe muss NS224-Shelves mit dem MetroCluster-Switch verbinden. Sie können nur Plattformen verbinden, die keine Switch-angeschlossenen NS224-Shelves als zweite MetroCluster-Konfiguration oder zweite DR-Gruppe verbinden.

  Wenn Ihr zweiter MetroCluster oder Ihre DR-Gruppe keine NS224-Shelves mit dem MetroCluster-Switch verbindet, folgen Sie den Verkabelungstabellen für Controller, die keine über einen Switch angeschlossenen NS224-Regale verbinden .

- Der RcfFileGenerator zeigt nur geeignete Plattformen an, wenn die erste Plattform ausgewählt ist.
- Für das Verbinden von MetroCluster Konfigurationen mit einem oder zwei vier Nodes ist ONTAP 9.14.1 oder höher erforderlich.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Überprüfen Sie die Tabelle mit den korrekten Portzuweisungen für Ihre Konfiguration. In diesem Abschnitt gibt es zwei Sätze von Verkabelungstabellen:

- Verkabelungstabellen für Controller, die NS224-Shelfs mit Switch verbinden
- Verkabelungstabellen für Controller, die keine Switch-verbundenen NS224-Shelfs anschließen

Controller, die Switch-Attached NS224 Shelfs verbinden

Legen Sie fest, welche Portzuweisungstabelle Sie für Controller befolgen sollten, die Switch-verbundene NS224-Shelfs verbinden.

Plattform	Verwenden Sie diese Verkabelungstabelle…
AFF C30, AFF A30 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 1a) oder 100G (Gruppe 1b) Ethernet-Karte verwenden. • Cisco 9336C-FX2-Switch zur Verbindung von Port-Zuordnungen der NS224-Speicherplattform (Gruppe 1a - 25G) • Cisco 9336C-FX2-Switch zur Verbindung von NS224-Storage-Plattform-Port-Zuordnungen (Gruppe 1b - 100G)
AFF A320 AFF C400, ASA C400 AFF A400, ASA A400	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 2)
AFF A50	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 3)
AFF A700 AFF C800, ASA C800, AFF A800 AFF A900, ASA A900	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 4)
AFF A70 AFF C80 AFF A90 AFF A1K	Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 5)

Cisco 9336C-FX2-Switch, der NS224-Speicherplattform-Port-Zuweisungen verbindet (Gruppe 1a)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A30-, AFF C30- oder AFF C60-System zu verkabeln, bei dem Switch-verbundene NSS24-Shelfs über eine 25-Gbit-Ethernet-Karte mit vier Ports an einen Cisco 9336C-FX2-Switch angeschlossen werden.

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled	
2/1		e4a	e4b	e4a	e4b
2/2-4		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled	
4/1		e4a	e4b	e4a	e4b
4/2-4		disabled		disabled	
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Speicherplattform-Portzuweisungen (Gruppe 1b)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30- oder AFF C60-System zu verkabeln, das Switch-angeschlossene NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch über eine 100G-Ethernet-Karte mit zwei Ports verbindet.

Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Controllers connecting switch-attached shelves					
Switch Port	Port Use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b	e3a	e3b
18					
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b	e3a	e3b
20					
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)				
24					
25	Storage shelf 4 (6)				
26					
27	Storage shelf 5 (5)				
28					
29	Storage shelf 6 (4)				
30					
31	Storage shelf 7 (3)				
32					
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 2)

Plattform-Port-Zuweisungen prüfen, um ein AFF A320-, AFF C400-, ASA C400-, AFF A400- oder ASA A400-System zu verkabeln, bei dem die Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden werden:

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 3)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A50-System zu verkabeln, das Switch-verbundene NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbindet:

Controllers connecting switch-attached shelves			
Switch Port	Port Use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b
2		e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b
4		e4a	e4b
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e2a	e2b
10		e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b
12		e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b
18			
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b
20			
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)		
28			
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 4)

Plattform-Port-Zuweisungen prüfen, um ein AFF A700-, AFF C800-, ASA C800-, AFF A800-, AFF A900- oder ASA A900-System zu verkabeln, bei dem die Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden werden:

Controllers connecting switch-attached shelves							
Switch Port	Port Use	AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4							
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e5a	e5b	e0b	e1b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 1, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
18							
19	MetroCluster 2, Ethernet Storage Interface	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2)	e3b (option 1) e10b (option 2)
20							
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Cisco 9336C-FX2-Switch zur Verbindung von NS224-Port-Zuordnungen der Speicherplattform (Gruppe 5)

Prüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A70-, AFF C80-, AFF A90- oder AFF A1K-System zu verkabeln, bei dem die Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden werden:

Controller verbinden keine Switch-Attached NS224 Shelfs

Legen Sie fest, welche Portzuweisungstabelle Sie für Controller befolgen sollten, die keine Switch-verbundenen NS224-Shelfs verbinden.

Plattform	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS2750, AFF A220	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 6)
AFF A20	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 7)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 8)
AFF C30, AFF A30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 9a) oder 100G (Gruppe 9b) Ethernet-Karte verwenden. • Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9a) • Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9b)
FAS8200, AFF A300	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 10)
AFF A320 FAS8300, AFF C400, ASA C400, FAS8700 AFF A400, ASA A400	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 11)
AFF A50	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 12)
FAS9000, AFF A700 AFF C800, ASA C800, AFF A800, ASA A800 FAS9500, AFF A900, ASA A900	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 13)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 14)

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 6)

Plattform-Port-Zuweisungen prüfen, um ein AFF A150-, ASA A150-, FAS2750- oder AFF A220-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 7)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A20-System zu verkabeln, bei dem keine Switch-angeschlossenen NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Controllers not connecting switch-attached shelves			
Switch Port	Port Use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e2a	e4a
1/2-4		disabled	
2/1		e2a	e4a
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e2a	e4a
3/2-4		disabled	
4/1		e2a	e4a
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e2b	e4b
9/2-4		disabled	
10/1		e2b	e4b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e2b	e4b
11/2-4		disabled	
12/1		e2b	e4b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 8)

Plattform-Port-Zuweisungen prüfen, um ein FAS500f-, AFF C250-, ASA C250-, AFF A250- oder ASA A250-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9a)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs über eine 25-Gbit-Ethernet-Karte mit vier Ports an einen Cisco 9336C-FX2-Switch angeschlossen sind.

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
1/2-4		disabled		disabled		disabled	
2/1		e4a	e4b	e4a	e4b	e4a	e4b
2/2-4		disabled		disabled		disabled	
3/1	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3/2-4		disabled		disabled		disabled	
4/1		e4a	e4b	e4a	e4b	e4a	e4b
4/2-4		disabled		disabled		disabled	
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 9b)

Prüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs über eine 100-GB-Ethernet-Karte mit zwei Ports an einen Cisco 9336C-FX2-Switch angeschlossen sind.

Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Controllers not connecting switch-attached shelves							
Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10		e2a	e2b	e2a	e2b	e2a	e2b
11	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12		e2a	e2b	e2a	e2b	e2a	e2b
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 10)

Plattform-Port-Zuordnungen prüfen, um ein FAS8200- oder AFF A300-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 11)

Plattform-Port-Zuweisungen prüfen, um ein AFF A320-, FAS8300-, AFF C400-, ASA C400-, FAS8700-, AFF A400- oder ASA A400-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind:

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 12)

Prüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A50-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2-Switch verbunden sind.

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 13)

Plattform-Port-Zuordnungen prüfen, um ein FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 oder ASA A900 System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2 Switch verbunden sind:

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

Cisco 9336C-FX2-Switch verbindet NS224-Speicherplattform-Port-Zuweisungen nicht (Gruppe 14)

Prüfen Sie die Plattform-Port-Zuweisungen, um ein AFF A70-, FAS70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System zu verkabeln, bei dem keine Switch-Attached NSS24-Shelfs mit einem Cisco 9336C-FX2 Switch verbunden sind:

Plattform-Portzuweisungen für von Broadcom unterstützte BES-53248-IP-Switches in einer MetroCluster -IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Sie können die Switches nicht mit Remote-ISL-Ports unterschiedlicher Geschwindigkeit verwenden (z. B. ein 25-Gbit/s-Port, der an einen 10-Gbit/s-ISL-Port angeschlossen ist).
- Wenn Sie den Switch für den Übergang von MetroCluster FC zu IP konfigurieren, werden die folgenden Ports je nach gewählter Zielplattform verwendet:

Zielplattform	Port
FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 oder FAS8700 Plattformen eingesetzt	Ports 1 bis 6, 10 Gbit/s
FAS8200 oder AFF A300 Plattformen	Ports 3 - 4 und 9 - 12, 10 Gbit/s

- Bei AFF A320 Systemen, die mit Broadcom BES-53248-Switches konfiguriert sind, werden möglicherweise nicht alle Funktionen unterstützt.

  Jede Konfiguration oder Funktion, die erfordert, dass die lokalen Cluster-Verbindungen mit einem Switch verbunden sind, wird nicht unterstützt. Beispielsweise werden die folgenden Konfigurationen und Verfahren nicht unterstützt:

  - MetroCluster Konfigurationen mit acht Nodes
  - Der Wechsel von MetroCluster FC- zu MetroCluster IP-Konfigurationen
  - Aktualisieren einer MetroCluster IP-Konfiguration mit vier Nodes (ONTAP 9.8 und höher)

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS2750 AFF A220	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 1)
FAS500f AFF C250, ASA C250 AFF A250, ASA A250	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 2)
AFF A20	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 3)
AFF C30, AFF A30 FAS50 AFF C60	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 4)
FAS8200, AFF A300	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 5)
AFF A320	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 6)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700	Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 7)

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 1)

Plattform-Port-Zuordnungen zum Verkabelung eines AFF A150, ASA A150, FAS2750 oder AFF A220 Systems mit einem Broadcom BES-53248 Switch prüfen:

Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
2			
3	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
4			
5-8	Unused	disabled	
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0a	e0b
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- Wenn beide MetroCluster-Konfigurationen dieselbe Plattform verwenden, empfiehlt NetApp die Auswahl der Gruppe „MetroCluster 3“ für eine Konfiguration und die Gruppe „MetroCluster 4“ für die andere Konfiguration. Wenn die Plattformen unterschiedlich sind, müssen Sie für die erste Konfiguration „MetroCluster 3“ oder „MetroCluster 4“ und für die zweite Konfiguration „MetroCluster 1“ oder „MetroCluster 2“ auswählen.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 2)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein FAS500f-, AFF C250-, ASA C250-, AFF A250- oder ASA A250-System mit einem Broadcom BES-53248-Switch zu verkabeln:

Physical Port	Port use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
6			
7	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
8			
9	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d
10			
11	MetroCluster 4, Shared Cluster and MetroCluster interface	e0c	e0d
12			
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- Wenn beide MetroCluster-Konfigurationen dieselbe Plattform verwenden, empfiehlt NetApp die Auswahl der Gruppe „MetroCluster 3“ für eine Konfiguration und die Gruppe „MetroCluster 4“ für die andere Konfiguration. Wenn die Plattformen unterschiedlich sind, müssen Sie für die erste Konfiguration „MetroCluster 3“ oder „MetroCluster 4“ und für die zweite Konfiguration „MetroCluster 1“ oder „MetroCluster 2“ auswählen.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 3)

Überprüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A20-System mit einem Broadcom BES-53248-Switch zu verkabeln:

Physical Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e2a	e4a
2			
3	MetroCluster 2, Local Cluster interface	e2a	e4a
4			
5	MetroCluster 1, MetroCluster interface	e2b	e4b
6			
7	MetroCluster 2, MetroCluster interface	e2b	e4b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17	MetroCluster 3, Local Cluster interface (note 1)	e2a	e4a
18			
19	MetroCluster 3, MetroCluster interface (note 1)	e2b	e4b
20			
21	MetroCluster 4, Local Cluster interface (note 1)	e2a	e4a
22			
23	MetroCluster 4, MetroCluster interface (note 1)	e2b	e4b
24			
..	Ports not licensed (25 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 4)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem Broadcom BES-53248-Switch unter Verwendung einer 25-Gbit-Ethernet-Karte mit vier Ports zu verkabeln.

- Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.
- Diese Konfiguration erfordert einen QSFP-zu-SFP+-Adapter in der Karte des Controllers, um eine Netzwerkgeschwindigkeit von 25 Gbit/s zu unterstützen.

Physical Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2							
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4							
5	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
6							
7	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9 - 12	Unused	disabled		disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17	MetroCluster 3, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
18							
19	MetroCluster 3, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
20							
21	MetroCluster 4, Local Cluster interface (note 1)	e4a	e4b	e4a	e4b	e4a	e4b
22							
23	MetroCluster 4, MetroCluster interface (note 1)	e2a	e2b	e2a	e2b	e2a	e2b
24							
..	Ports not licensed (25 - 54)						
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
54							
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
56							

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 5)

Prüfen Sie die Zuordnungen der Plattform-Ports zur Verkabelung eines FAS8200 oder AFF A300 Systems mit einem Broadcom BES-53248-Switch:

Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 6)

Überprüfen Sie die Zuweisungen der Plattform-Ports, um ein AFF A320-System mit einem Broadcom BES-53248-Switch zu verkabeln:

Physical Port	Port use	AFF A320	
		IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (Note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see Note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (Note 2)	e0g	e0h
56			

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- **Hinweis 2**: Nur ein MetroCluster mit vier Knoten kann mit AFF A320 Systemen an den Switch angeschlossen werden.

  Funktionen, die einen Switch-Cluster erfordern, werden in dieser Konfiguration nicht unterstützt. Dazu gehören auch die Verfahren zur Umstellung von MetroCluster FC auf IP und zur Technologieaktualisierung.

Broadcom BES-53248-Plattform-Port-Zuweisungen (Gruppe 7)

Prüfen der Plattform-Port-Zuordnungen für die Verkabelung einer FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 oder FAS8700 System auf einen Broadcom BES-53248 Switch:

Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see Note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (Note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (Note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (Note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

- **Hinweis 1**: Die Verwendung dieser Ports erfordert eine zusätzliche Lizenz.
- **Hinweis 2**: Nur ein MetroCluster mit vier Knoten kann mit AFF A320 Systemen an den Switch angeschlossen werden.

  Funktionen, die einen Switch-Cluster erfordern, werden in dieser Konfiguration nicht unterstützt. Dazu gehören auch die Verfahren zur Umstellung von MetroCluster FC auf IP und zur Technologieaktualisierung.

Plattform-Portzuweisungen für von NVIDIA unterstützte SN2100-IP-Switches in einer MetroCluster IP-Konfiguration

Die Portnutzung in einer MetroCluster IP-Konfiguration hängt vom Switch-Modell und dem Plattformtyp ab.

Lesen Sie die folgenden Überlegungen, bevor Sie die Konfigurationstabellen verwenden:

- Zum Verbinden einer MetroCluster-Konfiguration mit acht oder zwei vier Nodes sind ONTAP 9.14.1 oder höher und RCF-Dateiversion 2.00 oder höher erforderlich.

  Die Version der RCF-Datei unterscheidet sich von der Version des RCFfilegenerator-Tools, mit dem die Datei generiert wird. Beispielsweise können Sie eine RCF-Datei Version 2.00 mit RCFfilegenerator v1.6c generieren.

- Wenn Sie mehrere MetroCluster-Konfigurationen verkabeln, folgen Sie dann der entsprechenden Tabelle. Beispiel:
  - Wenn Sie zwei MetroCluster-Konfigurationen des Typs AFF A700 mit vier Nodes verkabeln, verbinden Sie die erste MetroCluster, die als „MetroCluster 1“ angezeigt wird, und die zweite MetroCluster, die in der AFF A700 Tabelle als „MetroCluster 2“ dargestellt ist.

  Die Ports 13 und 14 können im nativen Geschwindigkeitsmodus mit Unterstützung von 40 Gbit/s und 100 Gbit/s oder im Breakout-Modus zur Unterstützung von 4 × 25 Gbit/s oder 4 × 10 Gbit/s verwendet werden. Wenn sie den einheitlichen Geschwindigkeitsmodus verwenden, werden sie als Ports 13 und 14 dargestellt. Wenn sie den Breakout-Modus verwenden, entweder 4 × 25 Gbit/s oder 4 × 10 Gbit/s, dann werden sie als Ports 13s0-3 und 14s0-3 dargestellt.

In den folgenden Abschnitten wird die Beschreibung der physischen Verkabelung beschrieben. Sie können auch auf die verweisen "RCfFileGenerator" Für detaillierte Informationen zur Verkabelung.

Wählen Sie die richtige Verkabelungstabelle für Ihre Konfiguration aus

Ermitteln Sie anhand der folgenden Tabelle, welche Verkabelungstabelle Sie befolgen sollten.

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF A150, ASA A150 FAS500f AFF C250, ASA C250 AFF A250, ASA A250	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 1)
AFF A20	NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 2)

Wenn Ihr System…	Verwenden Sie diese Verkabelungstabelle…
AFF C30, AFF A30 FAS50 AFF C60	Die folgende Tabelle hängt davon ab, ob Sie eine 25G (Gruppe 3a) oder 100G (Gruppe 3b) Ethernet-Karte verwenden. • NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 3a -25G) • NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 3b -100G)
FAS8300 AFF C400, ASA C400 AFF A400, ASA A400 FAS8700 FAS9000, AFF A700	NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 4)
AFF A50	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 5)
AFF C800, ASA C800 AFF A800, ASA A800 FAS9500 AFF A900, ASA A900	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 6)
FAS70, AFF A70 AFF C80 FAS90, AFF A90 AFF A1K	NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 7)

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 1)

Überprüfen Sie die Zuordnungen der Plattformports zur Verkabelung von AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 oder ASA A250-System auf einem NVIDIA SN2100-Switch:

Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 2)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A20-System mit einem NVIDIA SN2100-Switch zu verkabeln:

Switch Port	Port use	AFF A20	
		IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e2a	e4a
s1s1-3		disabled	
2s0		e2a	e4a
2s1-3		disabled	
3s0	MetroCluster 2, Local Cluster interface	e2a	e4a
3s1-3		disabled	
4s0		e2a	e4a
4s1-3		disabled	
5s0	MetroCluster 3, Local Cluster interface	e2a	e4a
5s1-3		disabled	
6s0		e2a	e4a
6s1-3		disabled	
7	MetroCluster 1, MetroCluster interface	e2b	e4b
8			
9	MetroCluster 2, MetroCluster interface	e2b	e4b
10			
11	MetroCluster 3, MetroCluster interface	e2b	e4b
12			
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster	
14 / 14s0-3			
15	ISL, Local Cluster 100G	ISL, Local Cluster	
16			

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 3a)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem NVIDIA SN2100-Switch über eine 25-Gbit-Ethernet-Karte mit vier Ports zu verkabeln:

Diese Konfiguration erfordert eine 25-Gbit-Ethernet-Karte mit vier Ports in Steckplatz 4, um das lokale Cluster und die HA-Schnittstellen anzuschließen.

Switch Port	Port use	AFF C30 (25G Cluster/HA) AFF A30 (25G Cluster/HA)		FAS50 (25G Cluster/HA)		AFF C60 (25G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1s0	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
s1s1-3		disabled		disabled		disabled	
2s0		e4a	e4b	e4a	e4b	e4a	e4b
2s1-3		disabled		disabled		disabled	
3s0	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
3s1-3		disabled		disabled		disabled	
4s0		e4a	e4b	e4a	e4b	e4a	e4b
4s1-3		disabled		disabled		disabled	
5s0	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
5s1-3		disabled		disabled		disabled	
6s0		e4a	e4b	e4a	e4b	e4a	e4b
6s1-3		disabled		disabled		disabled	
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 3b)

Überprüfen Sie die Zuweisung der Plattform-Ports, um ein AFF A30-, AFF C30-, AFF C60- oder FAS50-System mit einem NVIDIA SN2100-Switch über eine 100-GbE-Karte mit zwei Ports zu verkabeln:

Für diese Konfiguration ist eine 100-GB-Ethernet-Karte mit zwei Ports in Steckplatz 4 erforderlich, um das lokale Cluster und die HA-Schnittstellen zu verbinden.

Switch Port	Port use	AFF C30 (100G Cluster/HA) AFF A30 (100G Cluster/HA)		FAS50 (100G Cluster/HA)		AFF C60 (100G Cluster/HA)	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
2		e4a	e4b	e4a	e4b	e4a	e4b
3	MetroCluster 2, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
4		e4a	e4b	e4a	e4b	e4a	e4b
5	MetroCluster 3, Local Cluster interface	e4a	e4b	e4a	e4b	e4a	e4b
6		e4a	e4b	e4a	e4b	e4a	e4b
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
8							
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
10							
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e2b	e2a	e2b
12							
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3							
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16							

NVIDIA SN2100-Plattform-Port-Zuweisungen (Gruppe 4)

Prüfen der Plattform-Port-Zuordnungen für die Verkabelung einer FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 FAS8700, FAS9000 oder AFF A700 System auf einem NVIDIA SN2100 Switch:

Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1,	e0c	e0d	e3a	e3b	e4a	e4e / e8a
2	Local Cluster interface						Note 1
3	MetroCluster 2,	e0c	e0d	e3a	e3b	e4a	e4e / e8a
4	Local Cluster interface						Note 1
5	MetroCluster 3,	e0c	e0d	e3a	e3b	e4a	e4e / e8a
6	Local Cluster interface						Note 1
7	MetroCluster 1,	e1a	e1b	e1a	e1b	e5a	e5b
8	MetroCluster interface						
9	MetroCluster 2,	e1a	e1b	e1a	e1b	e5a	e5b
10	MetroCluster interface						
11	MetroCluster 3,	e1a	e1b	e1a	e1b	e5a	e5b
12	MetroCluster interface						
13 / 13s0-3	MetroCluster ISL	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3	40/100G or 4x25G or 4x10G						
15	ISL, Local Cluster	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16	100G						

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 5)

Überprüfen Sie die Zuordnungen der Plattform-Ports, um ein AFF A50-System mit einem NVIDIA SN2100-Switch zu verkabeln:

Switch Port	Port use	AFF A50	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1,	e4a	e4b
2	Local Cluster interface		
3	MetroCluster 2,	e4a	e4b
4	Local Cluster interface		
5	MetroCluster 3,	e4a	e4b
6	Local Cluster interface		
7	MetroCluster 1,	e2a	e2b
8	MetroCluster interface		
9	MetroCluster 2,	e2a	e2b
10	MetroCluster interface		
11	MetroCluster 3,	e2a	e2b
12	MetroCluster interface		
13 / 13s0-3	MetroCluster ISL	ISL, MetroCluster	
14 / 14s0-3	40/100G or 4x25G or 4x10G		
15	ISL, Local Cluster	ISL, Local Cluster	
16	100G		

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 6)

Plattform-Port-Zuordnungen zur Verkabelung von AFF C800, ASA C800, AFF A800, ASA A800, FAS9500 prüfen AFF A900 oder ASA A900 System zu einem NVIDIA SN2100-Switch:

Switch Port	Port use	AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
2					
3	MetroCluster 2, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
4					
5	MetroCluster 3, Local Cluster interface	e0a	e1a	e4a	e4b(e) / e8a Note 1
6					
7	MetroCluster 1, MetroCluster interface	e0b	e1b	e5b	e7b
8					
9	MetroCluster 2, MetroCluster interface	e0b	e1b	e5b	e7b
10					
11	MetroCluster 3, MetroCluster interface	e0b	e1b	e5b	e7b
12					
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Hinweis 1: Verwenden Sie entweder die Ports e4a und e4e oder e4a und e8a, wenn Sie einen X91440A Adapter (40Gbps) verwenden. Verwenden Sie entweder die Ports e4a und e4b oder e4a und e8a, wenn Sie einen X91153A-Adapter (100 Gbit/s) verwenden.

NVIDIA SN2100 Plattform-Port-Zuweisungen (Gruppe 7)

Prüfen Sie die Zuordnungen der Plattform-Ports, um ein FAS70-, AFF A70-, AFF C80-, FAS90-, AFF A90- oder AFF A1K-System mit einem NVIDIA SN2100-Switch zu verkabeln:

Switch Port	Port use	FAS70 AFF A70		AFF C80		FAS90 AFF A90		AFF A1K	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
2									
3	MetroCluster 2, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
4									
5	MetroCluster 3, Local Cluster interface	e1a	e7a	e1a	e7a	e1a	e7a	e1a	e7a
6									
7	MetroCluster 1, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
8									
9	MetroCluster 2, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
10									
11	MetroCluster 3, MetroCluster interface	e2a	e2b	e2a	e3b	e2b	e3b	e2b	e3b
12									
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3									
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16									

Verkabeln Sie die ONTAP Controllermodul-Ports in einer MetroCluster IP-Konfiguration

Sie müssen die für Cluster-Peering, Management und Datenkonnektivität verwendeten Controller-Modul-Ports verkabeln.

Diese Aufgabe muss für jedes Controller-Modul der MetroCluster-Konfiguration ausgeführt werden.

Mindestens zwei Ports auf jedem Controller-Modul sollten für Cluster-Peering verwendet werden.

Die empfohlene minimale Bandbreite für die Ports und Netzwerkkonnektivität ist 1 GbE.

1. Identifizieren und verkabeln Sie mindestens zwei Ports für Cluster-Peering und vergewissern Sie sich,

dass sie über eine Netzwerkverbindung mit dem Partner-Cluster verfügen.

Cluster-Peering kann auf dedizierten Ports oder auf Daten-Ports durchgeführt werden. Durch den Einsatz von dedizierten Ports wird ein höherer Durchsatz für den Cluster-Peering-Datenverkehr erzielt.

"Express-Konfiguration für Cluster und SVM-Peering"

2. Verkabeln Sie die Management- und Daten-Ports des Controllers mit den Management- und Datennetzwerken am lokalen Standort.

   Befolgen Sie die Installationsanweisungen für Ihre Plattform auf der "Dokumentation zu ONTAP Hardwaresystemen".

   MetroCluster IP-Systeme verfügen über keine dedizierten HA-Ports (High Availability). Je nach Plattform wird der HA-Datenverkehr über die MetroCluster, den lokalen Cluster oder die Shared Cluster/MetroCluster-Schnittstelle bedient. Wenn Sie zur Installation Ihrer Plattform *ONTAP Hardware Systems Documentation* verwenden, sollten Sie die Anweisungen zum Verkabelung des Clusters und der HA-Ports nicht befolgen.

Konfigurieren Sie die MetroCluster IP-Switches

Wählen Sie das richtige Konfigurationsverfahren für den MetroCluster IP-Switch

Sie müssen die IP-Switches konfigurieren, um eine Back-End-MetroCluster-IP-Konnektivität bereitzustellen. Das von Ihnen zu befolgende Verfahren hängt von Ihrem Switch-Anbieter ab.

- "Konfigurieren Sie Broadcom IP-Switches"
- "Konfigurieren Sie Cisco IP-Switches"
- "Konfigurieren Sie NVIDIA IP-Switches"

Konfigurieren Sie Broadcom IP-Switches für Cluster-Interconnect und Backend- MetroCluster IP-Konnektivität

Sie müssen die Broadcom IP-Switches für die Verwendung als Cluster-Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

Ihre Konfiguration erfordert zusätzliche Lizenzen (6 x 100-GB-Port-Lizenz) in den folgenden Szenarien:

- Die Ports 53 und 54 werden als MetroCluster-ISL mit 40 Gbit/s oder 100 Gbit/s verwendet.
- Sie verwenden eine Plattform, die das lokale Cluster und MetroCluster-Schnittstellen mit den Ports 49 - 52 verbindet.

Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen

Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Broadcom-Switch-Einstellungen löschen und eine grundlegende Konfiguration durchführen.

Über diese Aufgabe

- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Wechseln Sie zur erhöhten Eingabeaufforderung (`#`): `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Löschen Sie die Startkonfiguration, und entfernen Sie das Banner

   a. Löschen der Startkonfiguration:

   `erase startup-config`

```
(IP_switch_A_1) #erase startup-config

Are you sure you want to clear the configuration? (y/n) y

(IP_switch_A_1) #
```

   Dieser Befehl löscht das Banner nicht.

   b. Entfernen Sie das Banner:

   `no set clibanner`

```
(IP_switch_A_1) #configure
(IP_switch_A_1)(Config) # no set clibanner
(IP_switch_A_1)(Config) #
```

3. Starten Sie den Switch neu:*`(IP_switch_A_1) #reload*`

```
Are you sure you would like to reset the system? (y/n) y
```

   Wenn das System fragt, ob die nicht gespeicherte oder geänderte Konfiguration vor dem erneuten Laden des Switches gespeichert werden soll, wählen Sie **Nein** aus.

4. Warten Sie, bis der Schalter neu geladen wurde, und melden Sie sich dann am Switch an.

   Der Standardbenutzer lautet „`admin`“, und es ist kein Passwort festgelegt. Es wird eine Eingabeaufforderung wie die folgende angezeigt:

```
(Routing)>
```

5. Zur erhöhten Eingabeaufforderung wechseln:

   `enable`

```
Routing)> enable
(Routing) #
```

6. Legen Sie das Service-Port-Protokoll auf fest `none`:

   `serviceport protocol none`

```
(Routing) #serviceport protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

(Routing) #
```

7. Weisen Sie die IP-Adresse dem Service-Port zu:

   `serviceport ip` *`ip-address netmask gateway`*

   Das folgende Beispiel zeigt eine dem Service-Port zugewiesene IP-Adresse „10.10.10.10“ mit dem Subnetz „255.255.255.0“ und dem Gateway „10.10.10.1“:

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Überprüfen Sie, ob der Service-Port ordnungsgemäß konfiguriert ist:

   `show serviceport`

   Das folgende Beispiel zeigt, dass der Port als aktiv ist und die richtigen Adressen zugewiesen wurden:

```
(Routing) #show serviceport

Interface Status.............................. Up
IP Address..................................... 10.10.10.10
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.10.10.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:56:87:D7

(Routing) #
```

9. Konfigurieren Sie den SSH-Server.

- Die RCF-Datei deaktiviert das Telnet-Protokoll. Wenn Sie den SSH-Server nicht konfigurieren, können Sie nur über die serielle Port-Verbindung auf die Bridge zugreifen.
- Sie müssen den SSH-Server konfigurieren, um die Protokollsammlung und andere externe Tools verwenden zu können.

a. Generieren von RSA-Schlüsseln.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. DSA-Schlüssel generieren (optional)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Wenn Sie die FIPS-konforme Version von EFOS verwenden, generieren Sie die ECDSA-Schlüssel. Im folgenden Beispiel werden die Schlüssel mit einer Länge von 521 erstellt. Gültige Werte sind 256, 384 oder 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Aktivieren Sie den SSH-Server.

Schließen Sie bei Bedarf den Konfigurationskontext.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+

> Wenn Schlüssel bereits vorhanden sind, werden Sie möglicherweise aufgefordert, sie zu überschreiben.

10. Konfigurieren Sie bei Bedarf die Domäne und den Namensserver:

    `configure`

    Das folgende Beispiel zeigt die `ip domain` Und `ip name server` Befehl:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. Konfigurieren Sie auf Wunsch die Zeitzone und die Zeitsynchronisierung (SNTP).

    Das folgende Beispiel zeigt die `sntp` Befehle, die IP-Adresse des SNTP-Servers und der relativen Zeitzone angeben.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

    Verwenden Sie für EFOS Version 3.10.0.3 und höher den `ntp` Befehl, wie im folgenden Beispiel dargestellt:

```
> (Config)# ntp ?

authenticate              Enables NTP authentication.
authentication-key        Configure NTP authentication key.
broadcast                 Enables NTP broadcast mode.
broadcastdelay            Configure NTP broadcast delay in microseconds.
server                    Configure NTP server.
source-interface          Configure the NTP source-interface.
trusted-key               Configure NTP authentication key number for
trusted time source.
vrf                       Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. Konfigurieren Sie den Switch-Namen:

    `hostname IP_switch_A_1`

    In der Switch-Eingabeaufforderung wird der neue Name angezeigt:

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. Konfiguration speichern:

    `write memory`

    Sie erhalten Eingabeaufforderungen und Ausgabe ähnlich dem folgenden Beispiel:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

14. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Broadcom-Switch EFOS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe muss bei jedem Switch in der MetroCluster IP-Konfiguration wiederholt werden.

Beachten Sie Folgendes:

- Beim Upgrade von EFOS 3.4.x.x auf EFOS 3.7.x.x oder höher muss auf dem Switch EFOS 3.4.4.6 (oder höher 3.4.x.x-Version) ausgeführt werden. Wenn Sie vor dieser Version eine Version ausführen, aktualisieren Sie zuerst den Switch auf EFOS 3.4.4.6 (oder höher 3.4.x.x Version), und aktualisieren Sie dann den Switch auf EFOS 3.7.x.x oder höher.
- Die Konfiguration für EFOS 3.4.x.x und 3.7.x.x oder höher ist unterschiedlich. Wenn Sie die EFOS-Version von 3.4.x.x auf 3.7.x.x oder höher ändern oder umgekehrt, müssen Sie den Switch auf die Werkseinstellungen zurücksetzen und die RCF-Dateien für die entsprechende EFOS-Version werden (neu) angewendet. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.
- Ab EFOS Version 3.7.x.x oder höher ist eine FIPS-konforme Version und eine FIPS-konforme Version verfügbar. Verschiedene Schritte gelten für den Wechsel von einem nicht FIPS-konformen auf eine FIPS-konforme Version oder umgekehrt. Wenn EFOS von einer nicht FIPS-konformen Version oder umgekehrt geändert wird, wird der Switch auf die Werkseinstellungen zurückgesetzt. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.

Schritte

1. Laden Sie die Switch-Firmware aus dem herunter"Broadcom Support-Site".
2. Überprüfen Sie, ob Ihre EFOS-Version FIPS-konform oder nicht-FIPS-konform ist, indem Sie die verwenden `show fips status` Befehl. In den folgenden Beispielen: `IP_switch_A_1` Verwendet FIPS-konformes EFOS und `IP_switch_A_2` Verwendet ein nicht FIPS-konformes EFOS.

Beispiel 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Beispiel 2

```
IP_switch_A_2 #show fips status
                     ^
% Invalid input detected at `^` marker.

IP_switch_A_2 #
```

3. Bestimmen Sie anhand der folgenden Tabelle, welche Methode Sie befolgen müssen:

Verfahren	**Aktuelle EFOS-Version**	* Neue EFOS-Version*	**Hohe Stufen**
Schritte zur Aktualisierung von EFOS zwischen zwei (nicht) FIPS-konformen Versionen	3.4.x.x	3.4.x.x	Installieren Sie das neue EFOS-Image mit Methode 1) die Konfigurations- und Lizenzinformationen bleiben erhalten
3.4.4.6 (oder höher 3.4.x.x)	3.7.x.x oder höher ohne FIPS-konform	EFOS mit Methode 1 aktualisieren. Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.7.x.x oder höher an	3.7.x.x oder höher ohne FIPS-konform
3.4.4.6 (oder höher 3.4.x.x)	EFOS mit Methode 1 abstufen. Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.4.x.x an	3.7.x.x oder höher ohne FIPS-konform	

Installieren Sie das neue EFOS-Image mit Methode 1. Die Konfigurations- und Lizenzdaten bleiben erhalten	3.7.x.x oder höher FIPS-konform	3.7.x.x oder höher FIPS-konform	Installieren Sie das neue EFOS-Image mit Methode 1. Die Konfigurations- und Lizenzdaten bleiben erhalten
Schritte zum Upgrade auf/von einer FIPS-konformen EFOS-Version	Nicht FIPS-konform	FIPS-konform	Installation des EFOS-Images unter Verwendung von Methode 2. Informationen zur Switch-Konfiguration und -Lizenz gehen verloren.

- Methode 1: Schritte zum Aktualisieren von EFOS beim Herunterladen des Software-Images auf die Backup-Boot-Partition
- Methode 2: Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation

Schritte zum Aktualisieren von EFOS beim Herunterladen des Software-Images auf die Backup-Boot-Partition

Die folgenden Schritte können nur ausgeführt werden, wenn beide EFOS-Versionen nicht FIPS-konform sind oder beide EFOS-Versionen FIPS-konform sind.

> Führen Sie diese Schritte nicht aus, wenn eine Version FIPS-konform ist und die andere Version nicht FIPS-konform ist.

Schritte

1. Kopieren Sie die Switch-Software auf den Switch: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   In diesem Beispiel wird die betriebssystemdatei efos-3.4.4.6.stk vom SFTP-Server unter 50.50.50.50 auf die Sicherungspartition kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /switchsoftware/
Filename..................................... efos-3.4.4.6.stk
Data Type.................................... Code
Destination Filename.......................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Legen Sie beim nächsten Neustart des Switches den Switch fest, der von der Backup-Partition aus gestartet werden soll:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Vergewissern Sie sich, dass das neue Startabbild beim nächsten Start aktiv ist:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Konfiguration speichern:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Starten Sie den Switch neu:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Warten Sie, bis der Schalter neu gestartet wurde.

In seltenen Fällen kann der Switch nicht booten. Folgen Sie den Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation Um das neue Image zu installieren.

7. Wenn Sie den Switch von EFOS 3.4.x.x auf EFOS 3.7.x.x oder umgekehrt umstellen, befolgen Sie die folgenden beiden Verfahren, um die korrekte Konfiguration (RCF) anzuwenden:
   a. Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen
   b. Herunterladen und Installieren der Broadcom RCF-Dateien
8. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation

Sie können die folgenden Schritte durchführen, wenn eine EFOS-Version FIPS-konform ist und die andere EFOS-Version nicht FIPS-konform ist. Mit diesen Schritten kann das nicht-FIPS- oder FIPS-konforme EFOS 3.7.x.x-Image von ONIE installiert werden, wenn der Switch nicht startet.

Schritte

1. Starten Sie den Schalter in den ONIE-Installationsmodus.

   Wählen Sie während des Startvorgangs ONIE aus, wenn der folgende Bildschirm angezeigt wird:

```
+--------------------------------------------------------------------+
|EFOS                                                                |
|*ONIE                                                               |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
|                                                                    |
+--------------------------------------------------------------------+
```

   Nach der Auswahl von „ONIE“ wird der Schalter geladen und Ihnen folgende Auswahlmöglichkeiten zur Verfügung stehen:

```
 +--------------------------------------------------------------------+
 |*ONIE: Install OS                                                   |
 | ONIE: Rescue                                                       |
 | ONIE: Uninstall OS                                                 |
 | ONIE: Update ONIE                                                  |
 | ONIE: Embed ONIE                                                   |
 | DIAG: Diagnostic Mode                                              |
 | DIAG: Burn-In Mode                                                 |
 |                                                                    |
 |                                                                    |
 |                                                                    |
 |                                                                    |
 |                                                                    |
 +--------------------------------------------------------------------+
```

Der Schalter startet nun in den ONIE-Installationsmodus.

2. Beenden Sie die ONIE-Erkennung, und konfigurieren Sie die ethernet-Schnittstelle

   Sobald die folgende Meldung angezeigt wird, drücken Sie <ENTER>, um die ONIE-Konsole zu öffnen:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   Die ONIE-Erkennung wird fortgesetzt, und Meldungen werden auf die Konsole gedruckt.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Konfigurieren Sie die ethernet-Schnittstelle und fügen Sie die Route mit hinzu `ifconfig eth0 <ipAddress> netmask <netmask> up` Und `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Stellen Sie sicher, dass der Server, der die ONIE-Installationsdatei hostet, erreichbar ist:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Installieren Sie die neue Switch-Software

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Die Software wird installiert und startet den Switch dann neu. Lassen Sie den Switch normal in die neue EFOS-Version neu starten.

6. Vergewissern Sie sich, dass die neue Switch-Software installiert ist

`show bootvar`

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Schließen Sie die Installation ab

   Der Switch wird neu gestartet, ohne dass die Konfiguration angewendet wurde, und setzt die Werkseinstellungen zurück. Befolgen Sie die beiden Verfahren, um die Grundeinstellungen des Switches zu konfigurieren und die RCF-Datei anzuwenden, wie in den folgenden beiden Dokumenten beschrieben:

   a. Konfigurieren Sie die Grundeinstellungen des Switches. Befolgen Sie Schritt 4 und höher: Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen
   b. Erstellen und wenden Sie die RCF-Datei wie in beschrieben an Herunterladen und Installieren der Broadcom RCF-Dateien

Herunterladen und Installieren der Broadcom RCF-Dateien

Sie müssen die Switch-RCF-Datei für jeden Switch in der MetroCluster IP-Konfiguration generieren und installieren.

Bevor Sie beginnen

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Über diese Aufgabe

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Es gibt vier RCF-Dateien, eine für jeden der vier Schalter in der MetroCluster IP-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
IP_Switch_A_1	v1.32_Switch-A1.txt
IP_Switch_A_2	v1.32_Switch-A2.txt
IP_Switch_B_1	v1.32_Switch-B1.txt
IP_Switch_B_2	v1.32_Switch-B2.txt

Die RCF-Dateien für EFOS Version 3.4.4.6 oder höher 3.4.x.x Version und EFOS Version 3.7.0.4 sind unterschiedlich. Sie müssen sicherstellen, dass Sie die richtigen RCF-Dateien für die EFOS-Version erstellt haben, auf der der Switch ausgeführt wird.

EFOS-Version	RCF-Dateiversion
3.4.x.x	V1.3x, v1.4x
3.7.x.x	v2.x

Schritte

1. Generieren Sie die Broadcom RCF-Dateien für die MetroCluster-IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP"
   b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

Änderungen an den RCF-Dateien nach dem Download werden nicht unterstützt.

2. Kopieren Sie die RCF-Dateien auf die Switches:

   a. Kopieren Sie die RCF-Dateien auf den ersten Switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

      In diesem Beispiel wird die RCF-Datei „BES-53248_v1.32_Switch-A1.txt“ vom SFTP-Server unter „50.50.50.50“ in den lokalen Bootflash kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /RcfFiles/
Filename..................................... BES-
53248_v1.32_Switch-A1.txt
Data Type.................................... Config Script
Destination Filename......................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"************************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248


...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Überprüfen Sie, ob die RCF-Datei als Skript gespeichert ist:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr            852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Anwenden des RCF-Skripts:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"************************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Konfiguration speichern:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Starten Sie den Switch neu:

```
reload
```

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

a. Wiederholen Sie die vorherigen Schritte für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Schalter neu laden:

```
reload
```

```
IP_switch_A_1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe des RCF-Datei-Banners:

> Wenn sich der Port im Breakout-Modus befindet, kann der im Befehl angegebene Portname von dem im RCF-Banner angegebenen Namen abweichen. Sie können auch die RCF-Verkabelungsdateien verwenden, um den Portnamen zu finden.

Für Details zum ISL-Port

Führen Sie den Befehl aus `show port all`.

Für Port-Channel-Details

Führen Sie den Befehl aus `show port-channel all`.

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle.

   Sie müssen die folgenden Befehle für jeden identifizierten nicht verwendeten Port oder Port-Kanal ausführen.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

Konfigurieren Sie Cisco IP-Switches

Konfigurieren Sie Cisco IP-Switches für Cluster-Interconnect und Backend- MetroCluster IP-Konnektivität

Sie müssen die Cisco IP Switches für die Verwendung als Cluster Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

Über diese Aufgabe

Einige der Verfahren in diesem Abschnitt sind unabhängige Verfahren, und Sie müssen nur diejenigen ausführen, die Sie an Ihre Aufgabe gerichtet sind oder für Ihre Aufgabe relevant sind.

Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen

Bevor Sie eine RCF-Datei installieren, müssen Sie die Cisco Switch-Konfiguration löschen und die grundlegende Konfiguration durchführen. Dieses Verfahren ist erforderlich, wenn Sie dieselbe RCF-Datei nach einer vorherigen Installation neu installieren möchten oder wenn Sie eine neue Version einer RCF-Datei installieren möchten.

Über diese Aufgabe

- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Setzen Sie den Schalter auf die werkseitigen Standardeinstellungen zurück:

   a. Löschen Sie die vorhandene Konfiguration:

      `write erase`

b. Laden Sie die Switch-Software neu:

```
reload
```

Das System startet neu und wechselt in den Konfigurationsassistenten. Wenn Sie während des Startvorgangs die Eingabeaufforderung „`Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/Nein)[n]`", you should respond `yes` Fortfahren.

c. Geben Sie im Konfigurationsassistenten die grundlegenden Switch-Einstellungen ein:

- Admin-Passwort
- Switch-Name
- Out-of-Band-Managementkonfiguration
- Standard-Gateway
- SSH-Service (RSA)

Nach Abschluss des Konfigurationsassistenten wird der Switch neu gestartet.

d. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das Kennwort ein, um sich beim Switch anzumelden.

Das folgende Beispiel zeigt die Eingabeaufforderungen und Systemantworten bei der Konfiguration des Switches. Die Winkelklammern (`<<<`Geben Sie an, wo Sie die Informationen eingeben.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

Sie geben grundlegende Informationen in die nächsten Eingabeaufforderungen ein, einschließlich Switch-Name, Managementadresse und Gateway, und wählen SSH mit RSA aus.

Dieses Beispiel zeigt die minimalen Informationen, die für die Konfiguration des RCF erforderlich sind. Nach der Anwendung des RCF können weitere Optionen konfiguriert werden. Sie können beispielsweise SNMPv3, NTP oder SCP/SFTP konfigurieren, nachdem Sie den RCF installiert haben.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Die letzte Reihe von Eingabeaufforderungen vervollständigt die Konfiguration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Konfiguration speichern:

```
IP_switch-A-1# copy running-config startup-config
```

3. Starten Sie den Switch neu, und warten Sie, bis der Schalter neu geladen wurde:

```
IP_switch-A-1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco Switch NX-OS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Schritte

1. Laden Sie die unterstützte NX-OS-Softwaredatei herunter.

   "Cisco Software-Download"

2. Kopieren Sie die Switch-Software auf den Switch:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   In diesem Beispiel werden die Datei nxos.7.0.3.I4.6.bin und das EPLD-Image vom SFTP-Server 10.10.99.99 in den lokalen Bootflash kopiert:

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img                161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

3. Überprüfen Sie auf jedem Switch, ob die NX-OS-Dateien des Switches im Bootflash-Verzeichnis jedes Switches vorhanden sind:

   `dir bootflash:`

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installieren der Switch-Software:

   `install all nxos bootflash:nxos.version-number.bin`

   Der Switch wird automatisch neu geladen (neu gestartet), nachdem die Switch-Software installiert wurde.

   Das folgende Beispiel zeigt die Softwareinstallation auf IP_Switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

Performing module support checks.            [####################] 100%
-- SUCCESS

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  default upgrade is not
hitless



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos               7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Warten Sie, bis der Schalter neu geladen ist, und melden Sie sich dann am Schalter an.

   Nach dem Neustart des Switches wird die Eingabeaufforderung für die Anmeldung angezeigt:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Überprüfen Sie, ob die Switch-Software installiert wurde:
`show version`

   Das folgende Beispiel zeigt die Ausgabe:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

```
IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  ------------------ ------------ ----------- -----------------
     1         SUP         Yes           disruptive  Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------- ------ ----------------- ----------------- ------------
------------
     1  SUP    MI FPGA           0x07              0x07         No
     1  SUP    IO FPGA           0x17              0x19         Yes
     1  SUP    MI FPGA2          0x02              0x02         No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module   Type  Upgrade-Result
-------- ----- --------------
     1   SUP   Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. [[STEP 8]]nach dem Neustart des Switches melden Sie sich erneut an und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

   ```
   show version module 1 epld
   ```

9. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco IP RCF-Dateien

Sie müssen die RCF-Datei für jeden Switch in der MetroCluster IP-Konfiguration generieren und installieren.

Über diese Aufgabe

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Wenn Sie einen QSFP-zu-SFP+-Adapter verwenden, müssen Sie den ISL-Port möglicherweise im nativen Geschwindigkeitsmodus statt im Breakout-Speed-Modus konfigurieren. Informationen zur Bestimmung des ISL-Port-Geschwindigkeitsmodus finden Sie in der Dokumentation des Switch-Herstellers.

Es gibt vier RCF-Dateien, eine für jeden der vier Schalter in der MetroCluster IP-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
IP_Switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_Switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_Switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_Switch_B_2	NX3232_v1.80_Switch-B2.txt

Schritte

1. Erstellen Sie die Cisco RCF-Dateien für MetroCluster IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP"
   b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

   Änderungen an den RCF-Dateien nach dem Download werden nicht unterstützt.

2. Kopieren Sie die RCF-Dateien auf die Switches:
   a. Kopieren Sie die RCF-Dateien auf den ersten Switch:

      ```
      copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
      bootflash: vrf management
      ```

      In diesem Beispiel wird die RCF-Datei NX3232_v1.80_Switch-A1.txt vom SFTP-Server unter 10.10.99.99 auf den lokalen Bootflash kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Wiederholen Sie den vorherigen Unterschritt für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Überprüfen Sie bei jedem Switch, ob die RCF-Datei im Bootflash-Verzeichnis jedes Switches vorhanden ist:

   `dir bootflash:`

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

Usage for bootflash://sup-local
1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Konfigurieren Sie die TCAM-Regionen auf Cisco Switches 3132Q-V und Cisco 3232C-Switches.

   Überspringen Sie diesen Schritt, wenn Cisco 3132Q-V oder Cisco 32Q-V Switches nicht vorhanden sind.

a. Stellen Sie auf dem Cisco Switch 3132Q-V die folgenden TCAM-Bereiche ein:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. Legen Sie auf dem Cisco 3232C Switch die folgenden TCAM-Regionen fest:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Speichern Sie nach dem Einstellen der TCAM-Bereiche die Konfiguration, und laden Sie den Schalter neu:

```
copy running-config startup-config
reload
```

5. Kopieren Sie die passende RCF-Datei vom lokalen Bootflash auf jeden Switch in die laufende Konfiguration:

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Kopieren Sie die RCF-Dateien von der ausgeführten Konfiguration auf die Startkonfiguration auf jedem Switch:

   `copy running-config startup-config`

   Sie sollten eine Ausgabe wie die folgende sehen:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Schalter neu laden:

   `reload`

```
IP_switch_A_1# reload
```

8. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Einstellen der Vorwärtskorrektur für Systeme mit 25-Gbit/s-Konnektivität

Wenn Ihr System mit 25-Gbit/s-Konnektivität konfiguriert ist, müssen Sie den fec-Parameter (Forward Error Correction) nach Anwendung der RCF-Datei manuell auf OFF setzen. Die RCF-Datei wendet diese Einstellung nicht an.

Über diese Aufgabe

Die 25-Gbps-Ports müssen vor Durchführung dieses Verfahrens verkabelt werden.

"Plattform-Port-Zuweisungen für Cisco 3232C- oder Cisco 9336C-Switches"

Diese Aufgabe gilt nur für Plattformen mit 25-Gbit/s-Konnektivität:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Diese Aufgabe muss an allen vier Switches der MetroCluster IP-Konfiguration ausgeführt werden.

Schritte

1. Stellen Sie den fec-Parameter auf aus für jeden 25-Gbit/s-Port, der mit einem Controller-Modul verbunden ist, und kopieren Sie dann die laufende Konfiguration in die Startkonfiguration:

   a. Konfigurationsmodus aufrufen: `config t`

   b. Geben Sie die zu konfigurierende 25-Gbit/s-Schnittstelle an: `interface interface-ID`

   c. fec auf aus stellen: `fec off`

   d. Wiederholen Sie die vorherigen Schritte für jeden 25-Gbit/s-Port am Switch.

   e. Konfigurationsmodus beenden: `exit`

   Im folgenden Beispiel werden die Befehle für Interface ethernet1/25/1 auf Switch IP_Switch_A_1 angezeigt:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Wiederholen Sie den vorherigen Schritt auf den anderen drei Switches der MetroCluster IP-Konfiguration.

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle:

   ```
   show interface brief
   ```

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle.

   Sie müssen die folgenden Befehle für jeden identifizierten nicht verwendeten Port oder Port-Kanal ausführen.

   ```
   SwitchA_1# config t
   Enter configuration commands, one per line. End with CNTL/Z.
   SwitchA_1(config)# int Eth1/14
   SwitchA_1(config-if)# shutdown
   SwitchA_12(config-if)# exit
   SwitchA_1(config-if)# copy running-config startup-config
   [########################################] 100%
   Copy complete, now saving to disk (please wait)...
   Copy complete.
   ```

Konfigurieren Sie die MACsec-Verschlüsselung auf Cisco 9336C-Switches in einem MetroCluster IP-Standort

Die MACsec-Verschlüsselung kann nur auf die WAN-ISL-Ports angewendet werden.

Konfigurieren Sie die MACsec-Verschlüsselung auf Cisco 9336C-Switches

Sie müssen die MACsec-Verschlüsselung nur für die WAN-ISL-Ports konfigurieren, die zwischen den Standorten ausgeführt werden. Sie müssen MACsec konfigurieren, nachdem Sie die korrekte RCF-Datei angewendet haben.

Lizenzierungsanforderungen für MACsec

MACsec erfordert eine Sicherheitslizenz. Eine vollständige Erläuterung des Cisco NX-OS-Lizenzschemas und der Beschaffung und Anwendung von Lizenzen finden Sie im "Cisco NX-OS Licensing Guide"

Aktivierung von Cisco MACs Encryption WAN-ISLs in MetroCluster IP-Konfigurationen

Sie können die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration aktivieren.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   ```
   configure terminal
   ```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Aktivieren Sie MACsec und MKA auf dem Gerät:

   `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Konfigurieren Sie eine MACsec-Schlüsselkette und -Tasten

Sie können eine MACsec-Schlüsselkette oder Schlüssel für Ihre Konfiguration erstellen.

- Key Lifetime und Hitless Key Rollover*

Eine MACsec-Schlüsselkette kann über mehrere vorinstallierte PSKs (Preshared Keys) verfügen, die jeweils mit einer Schlüssel-ID und einer optionalen Lebensdauer konfiguriert sind. Eine Schlüssellebensdauer legt fest, zu welcher Zeit die Taste aktiviert und abläuft. Wenn keine lebenslange Konfiguration vorhanden ist, ist die Standardlebensdauer unbegrenzt. Wenn eine Lebensdauer konfiguriert ist, rollt MKA nach Ablauf der Lebensdauer zum nächsten konfigurierten vorfreigegebenen Schlüssel in der Schlüsselkette um. Die Zeitzone des Schlüssels kann lokal oder UTC sein. Die Standardzeitzone ist UTC. Ein Schlüssel kann auf einen zweiten Schlüssel innerhalb derselben Schlüsselkette übertragen werden, wenn Sie den zweiten Schlüssel (in der Schlüsselkette) konfigurieren und eine Lebensdauer für den ersten Schlüssel konfigurieren. Wenn die Lebensdauer der ersten Taste abläuft, wird automatisch die nächste Taste in der Liste angezeigt. Wenn dieselbe Taste auf beiden Seiten des Links gleichzeitig konfiguriert ist, ist der Schlüsselüberschlag ohne Unterbrechung des Datenverkehrs aktiviert (d. h. der Schlüssel wird ohne Unterbrechung des Datenverkehrs überrollt).

Schritte

1. Den globalen Konfigurationsmodus aufrufen:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Um den verschlüsselten Schlüsselzeichenkette auszublenden, ersetzen Sie den String in der Ausgabe des durch ein Platzhalterzeichen `show running-config` Und `show startup-config` Befehl:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

Die Oktett-Zeichenfolge wird ebenfalls ausgeblendet, wenn Sie die Konfiguration in einer Datei speichern.

Standardmäßig werden PSK-Schlüssel im verschlüsselten Format angezeigt und können einfach entschlüsselt werden. Dieser Befehl gilt nur für MACsec-Schlüsselketten.

3. Erstellen Sie eine MACsec-Schlüsselkette, um eine Reihe von MACsec-Schlüsseln zu halten und den MACsec-Konfigurationsmodus für die Schlüsselkette aufzurufen:

   `key chain name macsec`

   ```
   IP_switch_A_1(config)# key chain 1 macsec
   IP_switch_A_1(config-macseckeychain)#
   ```

4. Erstellen Sie eine MACsec-Taste, und rufen Sie den MACsec-Key-Konfigurationsmodus auf:

   `key key-id`

   Der Bereich liegt zwischen 1 und 32 hex-stelligen Schlüsselzeichenfolge und die maximale Größe beträgt 64 Zeichen.

   ```
   IP_switch_A_1 switch(config-macseckeychain)# key 1000
   IP_switch_A_1 (config-macseckeychain-macseckey)#
   ```

5. Konfigurieren Sie die Oktett-Zeichenfolge für den Schlüssel:

   `key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
   abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
   cryptographic-algorithm AES_256_CMAC
   ```

   Das Argument Octet-string kann bis zu 64 hexadezimale Zeichen enthalten. Der Oktett-Schlüssel wird intern kodiert, so dass der Schlüssel im Klartext nicht in der Ausgabe des angezeigt wird `show running-config macsec` Befehl.

6. Konfigurieren einer Sendezeit für die Taste (in Sekunden):

   `send-lifetime start-time duration duration`

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

Standardmäßig behandelt das Gerät die Startzeit als UTC. Das Argument Start-Time ist die Uhrzeit und das Datum, zu der der Schlüssel aktiv wird. Das Argument „Dauer“ ist die Länge der Lebensdauer in Sekunden. Die maximale Länge beträgt 2147483646 Sekunden (ca. 68 Jahre).

7. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Zeigt die Schlüsselkettenkonfiguration an:

   `show key chain name`

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Konfigurieren einer MACsec-Richtlinie

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Erstellen einer MACsec-Richtlinie:

   `macsec policy name`

```
IP_switch_A_1(config)# macsec policy abc
IP_switch_A_1(config-macsec-policy)#
```

3. Konfigurieren Sie eine der folgenden Chiffren GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 oder GCM-AES-XPN-256:

   `cipher-suite name`

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Konfigurieren Sie die zentrale Serverpriorität, um die Verbindung zwischen Peers während eines Schlüsselaustauschs zu unterbrechen:

   `key-server-priority number`

   ```
   switch(config-macsec-policy)# key-server-priority 0
   ```

5. Konfigurieren Sie die Sicherheitsrichtlinie, um den Umgang mit Daten und Kontrollpaketen zu definieren:

   `security-policy security policy`

   Wählen Sie aus den folgenden Optionen eine Sicherheitsrichtlinie aus:

   - Must-Secure — Pakete, die keine MACsec-Header tragen, werden verworfen
   - Sollte-sicher — Pakete, die keine MACsec-Header tragen, sind zulässig (dies ist der Standardwert)

   ```
   IP_switch_A_1(config-macsec-policy)# security-policy should-secure
   ```

6. Konfigurieren Sie das Replay Protection-Fenster, damit die gesicherte Schnittstelle kein Paket akzeptiert, das kleiner als die konfigurierte Fenstergröße ist: `window-size number`

   > Die Größe des Replay Protection Window stellt die maximale Anzahl von Frames dar, die von MACsec akzeptiert und nicht verworfen werden. Der Bereich liegt zwischen 0 und 596000000.

   ```
   IP_switch_A_1(config-macsec-policy)# window-size 512
   ```

7. Konfigurieren Sie die Zeit in Sekunden, um einen SAK-Rekey zu erzwingen:

   `sak-expiry-time time`

   Sie können mit diesem Befehl den Sitzungsschlüssel in ein vorhersehbares Zeitintervall ändern. Der Standardwert ist 0.

   ```
   IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
   ```

8. Konfigurieren Sie einen der folgenden Vertraulichkeitsvereinbarungen im Layer 2-Frame, in dem die Verschlüsselung beginnt:

   `conf-offsetconfidentiality offset`

   Wählen Sie eine der folgenden Optionen:

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

Dieser Befehl kann erforderlich sein, damit zwischen den Zwischenschaltern Paketheader (dmac, smac, etype) wie MPLS-Tags verwendet werden können.

9. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   ```
   copy running-config startup-config
   ```

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

10. Die MACsec-Richtlinienkonfiguration anzeigen:

    ```
    show macsec policy
    ```

    ```
    IP_switch_A_1(config-macsec-policy)# show macsec policy
    ```

Aktivieren Sie die Verschlüsselung von Cisco MACsec an den Schnittstellen

1. Globalen Konfigurationsmodus aufrufen:

   ```
   configure terminal
   ```

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Wählen Sie die Schnittstelle aus, die Sie mit MACsec-Verschlüsselung konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

3. Fügen Sie die Schlüsselanhänger und die Richtlinie, die auf der Schnittstelle konfiguriert werden sollen, hinzu, um die MACsec-Konfiguration hinzuzufügen:

   ```
   macsec keychain keychain-name policy policy-name
   ```

   ```
   IP_switch_A_1(config-if)# macsec keychain 1 policy abc
   ```

4. Wiederholen Sie die Schritte 1 und 2 auf allen Schnittstellen, für die die MACsec-Verschlüsselung

konfiguriert werden soll.

5. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Deaktivieren Sie Cisco MACs Verschlüsselungs-WAN-ISLs in MetroCluster IP-Konfigurationen

Möglicherweise müssen Sie die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration deaktivieren.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Deaktivieren Sie die MACsec-Konfiguration auf dem Gerät:

   `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```

   Durch Auswahl der Option „no“ wird die MACsec-Funktion wiederhergestellt.

3. Wählen Sie die Schnittstelle aus, die Sie bereits mit MACsec konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Entfernen Sie die auf der Schnittstelle konfigurierte Schlüsselanhänger und Richtlinie, um die MACsec-Konfiguration zu entfernen:

   `no macsec keychain keychain-name policy policy-name`

```
IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
```

5. Wiederholen Sie die Schritte 3 und 4 auf allen Schnittstellen, für die MACsec konfiguriert ist.
6. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Überprüfen der MACsec-Konfiguration

Schritte

1. Wiederholen Sie * alle* der vorherigen Vorgänge auf dem zweiten Schalter innerhalb der Konfiguration, um eine MACsec-Sitzung einzurichten.
2. Führen Sie die folgenden Befehle aus, um zu überprüfen, ob beide Switches erfolgreich verschlüsselt sind:

   a. Ausführen: `show macsec mka summary`

   b. Ausführen: `show macsec mka session`

   c. Ausführen: `show macsec mka statistics`

   Sie können die MACsec-Konfiguration mit den folgenden Befehlen überprüfen:

Befehl	Zeigt Informationen über… an.
`show macsec mka session interface typeslot/port number`	Die MKA-Sitzung von MACsec für eine bestimmte Schnittstelle oder für alle Schnittstellen
`show key chain name`	Konfiguration der Schlüsselkette
`show macsec mka summary`	Die MKA-Konfiguration von MACsec
`show macsec policy policy-name`	Die Konfiguration für eine bestimmte MACsec-Richtlinie oder für alle MACsec-Richtlinien

Konfigurieren Sie NVIDIA IP-Switches

Konfigurieren Sie den NVIDIA IP SN2100-Switch für die Clusterverbindung und die Backend- MetroCluster IP-Konnektivität

Sie müssen die NVIDIA SN2100 IP-Switches für die Verwendung als Cluster-Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

[[Reset-the-Switch] setzt den NVIDIA IP SN2100-Schalter auf die Werkseinstellungen zurück

Sie können eine der folgenden Methoden auswählen, um einen Schalter auf die werkseitigen Standardeinstellungen zurückzusetzen.

- Setzen Sie den Switch mithilfe der RCF-Dateioption zurück

- Laden Sie die Cumulus-Software herunter und installieren Sie sie

Zurücksetzen des Switches mit der RCF-Dateioption

Bevor Sie eine neue RCF-Konfiguration installieren, müssen Sie die NVIDIA-Switch-Einstellungen zurücksetzen.

Über diese Aufgabe

Um den Switch auf die Standardeinstellungen zurückzusetzen, führen Sie die RCF-Datei mit dem aus `restoreDefaults` Option. Mit dieser Option werden die ursprünglichen gesicherten Dateien an den ursprünglichen Speicherort kopiert und anschließend der Switch neu gestartet. Nach dem Neustart wird der Switch mit der ursprünglichen Konfiguration online geschaltet, die bei der ersten Ausführung der RCF-Datei zum Konfigurieren des Switches existierte.

Die folgenden Konfigurationsdetails werden nicht zurückgesetzt:

- Konfiguration von Benutzern und Anmeldeinformationen
- Konfiguration des Management-Netzwerk-Ports, eth0

> Alle anderen Konfigurationsänderungen, die während der Anwendung der RCF-Datei auftreten, werden auf die ursprüngliche Konfiguration zurückgesetzt.

Bevor Sie beginnen

- Sie müssen den Switch gemäß konfigurieren Laden Sie die NVIDIA RCF-Datei herunter, und installieren Sie sie. Wenn Sie auf diese Weise nicht konfiguriert haben oder vor der Ausführung der RCF-Datei zusätzliche Funktionen konfiguriert haben, können Sie dieses Verfahren nicht verwenden.
- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über eine serielle Konsolenverbindung mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Überprüfen Sie, ob die RCF-Konfiguration erfolgreich mit derselben oder einer kompatiblen RCF-Dateiversion angewendet wurde und ob die Sicherungsdateien vorhanden sind.

> Die Ausgabe kann Backup-Dateien, erhaltene Dateien oder beides anzeigen. Wenn Sicherungsdateien oder nicht vorhandene Dateien nicht in der Ausgabe angezeigt werden, können Sie dieses Verfahren nicht verwenden.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
  Backup files exist.
    Preserved files exist.
    Listing completion of the steps:
        Success: Step: 1: Performing Backup and Restore
        Success: Step: 2: updating MOTD file
        Success: Step: 3: Disabling apt-get
        Success: Step: 4: Disabling cdp
        Success: Step: 5: Adding lldp config
        Success: Step: 6: Creating interfaces
        Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
        Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
        Success: Step: 9: Configuring switch basic settings: ecn
        Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
        Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
        Success: Step: 12: Configuring switch basic settings: traffic
classification
        Success: Step: 13: Configuring LAG load balancing policies
        Success: Step: 14: Configuring the VLAN bridge
        Success: Step: 15: Configuring local cluster ISL ports
        Success: Step: 16: Configuring MetroCluster ISL ports
        Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
        Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
        Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
        Success: Step: 20: Configuring L2FC for MetroCluster interfaces
        Success: Step: 21: Configuring the interface to UP
        Success: Step: 22: Final commit
        Success: Step: 23: Final reboot of the switch
    Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Führen Sie die RCF-Datei mit der Option zum Wiederherstellen der Standardeinstellungen aus: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_2.py restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Beantworten Sie die Eingabeaufforderung mit „Ja“. Der Switch wird auf die ursprüngliche Konfiguration zurückgesetzt und startet neu.
4. Warten Sie, bis der Schalter neu gestartet wurde.

   Der Switch wird zurückgesetzt und behält die ursprüngliche Konfiguration wie z. B. die Konfiguration des Managementnetzwerks und die aktuellen Zugangsdaten vor dem Anwenden der RCF-Datei bei. Nach dem Neustart können Sie eine neue Konfiguration anwenden, indem Sie dieselbe oder eine andere Version der RCF-Datei verwenden.

Laden Sie die Cumulus-Software herunter und installieren Sie sie

Über diese Aufgabe

Verwenden Sie diese Schritte, wenn Sie den Schalter vollständig zurücksetzen möchten, indem Sie das Cumulus-Bild anwenden.

Bevor Sie beginnen

- Sie müssen über eine serielle Konsolenverbindung mit dem Switch verbunden sein.
- Das Cumulus Switch-Softwarebild ist über HTTP zugänglich.

  Weitere Informationen zur Installation von Cumulus Linux finden Sie unter "Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches"

- Sie müssen das Root-Passwort für haben `sudo` Zugriff auf die Befehle.

Schritte

1. Von der Cumulus-Konsole herunterladen und die Switch-Software-Installation mit dem Befehl in Warteschlange stellen `onie-install -a -i` Anschließend folgt der Dateipfad zur Switch-Software:

   In diesem Beispiel die Firmware-Datei `cumulus-linux-4.4.3-mlx-amd64.bin` Wird vom HTTP-Server '50.50.50.50' auf den lokalen Switch kopiert.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
mlx-amd64.bin
##################################################################
# 100.0%
```

```
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
```

```
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Antworten `y` Um die Eingabeaufforderung zur Bestätigung der Installation zu bestätigen, wenn das Image heruntergeladen und verifiziert wurde.
3. Starten Sie den Switch neu, um die neue Software zu installieren: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```

> Der Switch startet neu und wechselt in die Switch-Software-Installation, was einige Zeit in Anspruch nimmt. Nach Abschluss der Installation wird der Switch neu gestartet und bleibt an der Eingabeaufforderung „Login“.

4. Konfigurieren Sie die grundlegenden Switch-Einstellungen
   a. Wenn der Switch gestartet wird und in der Anmeldeaufforderung angezeigt wird, melden Sie sich an, und ändern Sie das Passwort.

> Der Benutzername ist 'Cumulus' und das Standardpasswort lautet 'Cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Konfigurieren Sie die Managementoberfläche.

   Die von Ihnen verwendeten Befehle hängen von der verwendeten Switch-Firmware-Version ab.

   Die folgenden Beispielbefehle konfigurieren den Hostnamen als IP_Switch_A_1, die IP-Adresse als 10.10.10.10, die Netzmaske als 255.255.255.0 (24) und die Gateway-Adresse als 10.10.10.1.

Cumulus 4.4.x

Mit den folgenden Beispielbefehlen können Sie den Hostnamen, die IP-Adresse, die Netzmaske und das Gateway auf einem Switch konfigurieren, auf dem Cumulus 4.4.x. ausgeführt wird

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


net add/del commands since the last "net commit"


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

Cumulus 5.4.x und höher

Mit den folgenden Beispielbefehlen können Sie den Hostnamen, die IP-Adresse, die Netzmaske und das Gateway auf einem Switch konfigurieren, auf dem Cumulus 5.4.x. ausgeführt wird Oder höher.

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. Starten Sie den Switch mithilfe des neu `sudo reboot` Befehl.

```
cumulus@cumulus:~$ sudo reboot
```

Wenn der Switch neu startet, können Sie eine neue Konfiguration mit den Schritten unter anwenden Laden Sie die NVIDIA RCF-Datei herunter, und installieren Sie sie.

Laden Sie die NVIDIA RCF-Dateien herunter und installieren Sie sie

Sie müssen die Switch-RCF-Datei für jeden Switch in der MetroCluster IP-Konfiguration generieren und installieren.

Bevor Sie beginnen

- Sie müssen das Root-Passwort für haben `sudo` Zugriff auf die Befehle.
- Die Switch-Software wird installiert und das Managementnetzwerk konfiguriert.
- Sie haben die ersten Schritte zur Installation des Switches mit der Methode 1 oder Methode 2 ausgeführt.
- Nach der Erstinstallation haben Sie keine zusätzliche Konfiguration angewendet.

> Wenn Sie nach dem Zurücksetzen des Switches und vor dem Anwenden der RCF-Datei eine weitere Konfiguration durchführen, können Sie dieses Verfahren nicht verwenden.

Über diese Aufgabe

Sie müssen diese Schritte bei jedem der IP-Schalter in der MetroCluster IP-Konfiguration (neue Installation) oder am Ersatzschalter (Switch-Austausch) wiederholen.

Wenn Sie einen QSFP-zu-SFP+-Adapter verwenden, müssen Sie den ISL-Port möglicherweise im nativen Geschwindigkeitsmodus statt im Breakout-Speed-Modus konfigurieren. Informationen zur Bestimmung des ISL-Port-Geschwindigkeitsmodus finden Sie in der Dokumentation des Switch-Herstellers.

Schritte

1. Generieren Sie die NVIDIA RCF-Dateien für MetroCluster IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP".

b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

c. Navigieren Sie zu Ihrem Home Directory. Wenn Sie als 'cumulus' angemeldet sind, lautet der Dateipfad `/home/cumulus`.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

d. Laden Sie die RCF-Datei in dieses Verzeichnis herunter. Das folgende Beispiel zeigt, dass Sie die Datei mit SCP herunterladen `SN2100_v2.0.0_IP_switch_A_1.txt` Von Server '50.50.50.50' in Ihr Home-Verzeichnis und speichern Sie es als `SN2100_v2.0.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
**********************************************************************
**
Banner of the SCP server
**********************************************************************
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Ausführen der RCF-Datei. Die RCF-Datei erfordert eine Option zum Anwenden eines oder mehrerer Schritte. Führen Sie die RCF-Datei ohne die Befehlszeilenoption aus, sofern Sie nicht vom technischen Support dazu aufgefordert werden. Um den Abschlussstatus der verschiedenen Schritte der RCF-Datei zu überprüfen, verwenden Sie die Option '-1' oder 'all', um alle (ausstehenden) Schritte anzuwenden.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

3. Wenn Ihre Konfiguration DAC-Kabel verwendet, aktivieren Sie die DAC-Option an den Switch-Ports:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

Im folgenden Beispiel wird die DAC-Option für den Port aktiviert `swp7`:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.00
    Running command: Enabling the DacOption for port swp7
    runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. Starten Sie den Switch nach Aktivierung der DAC-Option an den Switch-Ports neu:

```
sudo reboot
```

> Wenn Sie die DAC-Option für mehrere Switch-Ports festlegen, müssen Sie den Switch nur einmal neu starten.

Legen Sie die Fehlerkorrektur für Systeme mit 25-Gbit/s-Konnektivität vor

Wenn Ihr System über eine 25-Gbit/s-Konnektivität konfiguriert ist, stellen Sie den Parameter Vorwärtskorrektur (fec) nach Anwendung des RCF manuell auf aus. Die RCF wendet diese Einstellung nicht an.

Über diese Aufgabe

- Diese Aufgabe gilt nur für Plattformen mit 25-Gbit/s-Konnektivität. Siehe "Plattform-Port-Zuweisungen für von NVIDIA unterstützte SN2100 IP-Switches".
- Diese Aufgabe muss an allen vier Switches der MetroCluster IP-Konfiguration ausgeführt werden.
- Sie müssen jeden Switch-Port einzeln aktualisieren. Sie können im Befehl nicht mehrere Ports oder Portbereiche angeben.

Schritte

1. Stellen Sie den `fec` Parameter für den ersten Switch-Port, der eine 25-Gbit/s-Konnektivität verwendet, auf aus:

   ```
   sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
   ```

2. Wiederholen Sie den Schritt für jeden 25-Gbit/s-Switch-Port, der mit einem Controller-Modul verbunden ist.

Stellen Sie die Switch-Port-Geschwindigkeit für die MetroCluster IP-Schnittstellen ein

Über diese Aufgabe

- Gehen Sie folgendermaßen vor, um die Switch-Port-Geschwindigkeit für die folgenden Systeme auf 100 G einzustellen:
  - AFF A70, AFF A90, AFF A1K, AFF C80
  - AFF A30, AFF C30, AFF A50, AFF C60
  - FAS50, FAS70 UND FAS90
- Sie müssen jeden Switch-Port einzeln aktualisieren. Sie können im Befehl nicht mehrere Ports oder Portbereiche angeben.

Schritt

1. Verwenden Sie die RCF-Datei mit der `runCmd` Option, um die Geschwindigkeit einzustellen. Dies wendet die Einstellung an und speichert die Konfiguration.

   Die folgenden Befehle legen die Geschwindigkeit für die MetroCluster-Schnittstellen `swp7` und `swp8`fest:

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
   ```

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
   ```

   Beispiel

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
swp7 speed 100
[sudo] password for cumulus: <password>
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.20
    Running command: Setting switchport swp7 to 100G speed
    runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
    runCmd: 'nv set interface swp7 link speed 100G', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@Switch-A-1:mgmt:~$
```

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden. Sie müssen jeden Port oder Port-Kanal einzeln deaktivieren. Im Befehl können Sie nicht mehrere Ports oder Port-Bereiche angeben.

Schritte

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe des RCF-Datei-Banners:

   Wenn sich der Port im Breakout-Modus befindet, kann der im Befehl angegebene Portname von dem im RCF-Banner angegebenen Namen abweichen. Sie können auch die RCF-Verkabelungsdateien verwenden, um den Portnamen zu finden.

   ```
   net show interface
   ```

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe der RCF-Datei.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

Mit dem folgenden Beispielbefehl wird der Port „swp14“ deaktiviert:

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Wiederholen Sie diesen Schritt für jeden identifizierten nicht verwendeten Port oder Port-Kanal.

Installieren Sie die Konfigurationsdatei des Ethernet Switch Health Monitors für einen NVIDIA SN2100 MetroCluster IP-Switch

Um die Integritätsüberwachung von Ethernet-Switches auf NVIDIA-Ethernet-Switches zu konfigurieren, befolgen Sie dieses Verfahren.

Diese Anweisungen gelten, wenn NVIDIA X190006-PE und X190006-PI Switches nicht richtig erkannt werden.

Dies kann durch Ausführen von `system switch ethernet show` und prüfen Sie, ob **OTHER** für Ihr Modell angezeigt wird. Um Ihr NVIDIA-Switch-Modell zu identifizieren, suchen Sie die Teilenummer mit dem Befehl `nv show platform hardware` für NVIDIA CL 5.8 und früher oder `nv show platform` für spätere Versionen.

Diese Schritte werden auch empfohlen, wenn Sie möchten, dass die Integritätsüberwachung und Protokollerfassung bei Verwendung von NVIDIA CL 5.11.x mit den folgenden ONTAP-Versionen wie vorgesehen funktioniert. Auch ohne diese Schritte funktionieren Integritätsüberwachung und Protokollerfassung möglicherweise weiterhin, aber durch deren Befolgung wird sichergestellt, dass alles ordnungsgemäß funktioniert.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 und spätere Patch-Versionen

Bevor Sie beginnen

- Stellen Sie sicher, dass das ONTAP Cluster betriebsbereit ist und ausgeführt wird.
- Aktivieren Sie SSH auf dem Switch, um alle in CSHM verfügbaren Funktionen zu nutzen.
- Löschen Sie das `/mroot/etc/cshm_nod/nod_sign/` Verzeichnis auf allen Knoten:

  a. Betreten Sie die Nodeshell:

  ```
  system node run -node <name>
  ```

  b. Zu erweiterten Berechtigungen wechseln:

  ```
  priv set advanced
  ```

  c. Listen Sie die Konfigurationsdateien im `/etc/cshm_nod/nod_sign` Verzeichnis auf. Wenn das Verzeichnis existiert und Konfigurationsdateien enthält, werden die Dateinamen aufgelistet.

  ```
  ls /etc/cshm_nod/nod_sign
  ```

  d. Löschen Sie alle Konfigurationsdateien, die Ihren angeschlossenen Switch-Modellen entsprechen.

  Wenn Sie sich nicht sicher sind, entfernen Sie alle Konfigurationsdateien für die oben aufgeführten unterstützten Modelle, laden Sie die neuesten Konfigurationsdateien für dieselben Modelle herunter, und installieren Sie sie.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

  a. Vergewissern Sie sich, dass die gelöschten Konfigurationsdateien nicht mehr im Verzeichnis sind:

  ```
  ls /etc/cshm_nod/nod_sign
  ```

Schritte

1. Laden Sie die ZIP-Datei für die Konfiguration der Ethernet-Switch-Systemzustandsüberwachung basierend auf der entsprechenden ONTAP-Version herunter. Diese Datei ist auf der Seite verfügbar "NVIDIA Ethernet-Switches" .
   a. Wählen Sie auf der Download-Seite der NVIDIA SN2100-Software **Nvidia CSHM-Datei** aus.
   b. Aktivieren Sie auf der Seite Achtung/muss gelesen werden das Kontrollkästchen, um zuzustimmen.
   c. Aktivieren Sie auf der Seite Endbenutzer-Lizenzvereinbarung das Kontrollkästchen, um zuzustimmen, und klicken Sie auf **Akzeptieren und Fortfahren**.

d. Wählen Sie auf der Seite Nvidia CSHM File - Download die entsprechende Konfigurationsdatei aus. Folgende Dateien sind verfügbar:

ONTAP 9.15.1 und höher

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 bis 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Laden Sie die entsprechende ZIP-Datei auf Ihren internen Webserver hoch.
2. Greifen Sie von einem der ONTAP-Systeme im Cluster aus auf den erweiterten Modus zu.

   `set -privilege advanced`

3. Führen Sie den Befehl Switch Health Monitor configure aus.

   ```
   cluster1::> system switch ethernet
   ```

4. Überprüfen Sie, ob die Befehlsausgabe mit dem folgenden Text für Ihre ONTAP-Version endet:

ONTAP 9.15.1 und höher

Die Konfigurationsdatei wurde von der Statusüberwachung des Ethernet-Switches installiert.

ONTAP 9.11.1 bis 9.14.1

SHM hat die Konfigurationsdatei installiert.

ONTAP 9.10.1

Das heruntergeladene CSHM-Paket wurde erfolgreich verarbeitet.

Sollte ein Fehler auftreten, wenden Sie sich an den NetApp Support.

1. Warten Sie bis zu zweimal das Abfrageintervall der Ethernet-Switch-Integritätsüberwachung, das durch Ausführen gefunden `system switch ethernet polling-interval show`wird, bevor Sie den nächsten Schritt abschließen.
2. Führen Sie den Befehl auf dem ONTAP-System aus `system switch ethernet show` , und stellen Sie sicher, dass die Cluster-Switches erkannt werden, wobei das überwachte Feld auf **true** und das Seriennummernfeld nicht **Unknown** anzeigt.

```
cluster1::> system switch ethernet show
```

Wenn Ihr Modell nach der Anwendung der Konfigurationsdatei immer noch **ANDERE** anzeigt, wenden Sie sich an den NetApp-Support.

Siehe die "System-Switch-Ethernet-Konfigurations-Health-Monitor" Befehl für weitere Details.

Was kommt als Nächstes?

"Konfigurieren Sie die Überwachung des Switch-Systemzustands".

Überwachen der Integrität des MetroCluster-IP-Switches

Erfahren Sie mehr über die Switch-Integritätsüberwachung in einer MetroCluster-IP-Konfiguration

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich.

Wichtige Hinweise zur Konfiguration von CSHM in einer MetroCluster-IP-Konfiguration

Dieser Abschnitt enthält die allgemeinen Schritte zur Konfiguration von SNMPv3 und zur Protokollerfassung auf Cisco-, Broadcom- und NVIDIA SN2100-Switches. Sie müssen die Schritte für eine Switch-Firmware-Version befolgen, die in einer MetroCluster-IP-Konfiguration unterstützt wird. Weitere Informationen finden Sie im "Hardware Universe" um die unterstützten Firmware-Versionen zu überprüfen.

In einer MetroCluster-Konfiguration konfigurieren Sie die Integritätsüberwachung nur auf den lokalen Cluster-Switches.

Für die Protokollerfassung mit Broadcom- und Cisco-Switches muss für jeden Cluster mit aktivierter Protokollerfassung ein neuer Benutzer auf dem Switch erstellt werden. In einer MetroCluster-Konfiguration bedeutet dies, dass für MetroCluster 1, MetroCluster 2, MetroCluster 3 und MetroCluster 4 jeweils ein separater Benutzer auf den Switches konfiguriert werden muss. Diese Switches unterstützen nicht mehrere SSH-Schlüssel für denselben Benutzer. Bei jeder weiteren Einrichtung der Protokollerfassung werden alle bereits vorhandenen SSH-Schlüssel für den Benutzer überschrieben.

Bevor Sie CSHM konfigurieren, sollten Sie nicht verwendete ISLs deaktivieren, um unnötige ISL-Warnmeldungen zu vermeiden.

Konfigurieren Sie SNMPv3, um den Zustand von MetroCluster IP-Switches zu überwachen

In MetroCluster IP-Konfigurationen können Sie SNMPv3 zur Überwachung des Funktionszustands von IP-Switches konfigurieren.

Dieses Verfahren zeigt die allgemeinen Schritte zum Konfigurieren von SNMPv3 auf einem Switch. Einige der aufgeführten Switch-Firmware-Versionen werden in einer MetroCluster-IP-Konfiguration möglicherweise nicht unterstützt.

Sie müssen die Schritte für eine Switch-Firmware-Version befolgen, die in einer MetroCluster-IP-Konfiguration unterstützt wird. Weitere Informationen finden Sie im "Hardware Universe" um die unterstützten Firmware-Versionen zu überprüfen.

- SNMPv3 wird nur auf ONTAP 9.12.1 und höher unterstützt.
- ONTAP 9.13.1P12, 9.14.1P9, 9.15.1P5, 9.16.1 und spätere Versionen beheben diese beiden Probleme:
  - "Bei der ONTAP-Integritätsüberwachung von Cisco-Switches kann der SNMPv2-Verkehr nach der Umstellung auf SNMPv3 zur Überwachung weiterhin sichtbar sein."
  - "Falsch-positive Switch-Lüfter- und Stromwarnungen bei SNMP-Fehlern"

Über diese Aufgabe

Die folgenden Befehle werden verwendet, um einen SNMPv3-Benutzernamen auf den Switches **Broadcom**, **Cisco** und **NVIDIA** zu konfigurieren:

Broadcom-Switches

Konfigurieren Sie einen NETZWERKBETREIBER für SNMPv3-Benutzernamen auf Broadcom BES-53248-Switches.

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```

- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-
md5|auth-sha] [priv-aes128|priv-des]
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version
SNMPv3 -community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp status
```

```
(sw1)(Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>

(cs1)(Config)# show snmp user snmp

     Name            Group Name      Auth Priv
                                     Meth Meth    Remote Engine ID
---------------- ------------------ ---- ------
-------------------------
<username>        network-admin      MD5  AES128
8000113d03d8c497710bee
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: BES-53248
                                Switch Network: cluster-network
                              Software Version: 3.9.0.2
                    Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                     Source Of Switch Version: CDP/ISDP
                               Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

4. Überprüfen Sie nach dem Abwarten der CSHM-Abfrageperiode, ob die Seriennummer für den Ethernet-Switch eingetragen ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
                                  Device Name: sw1
                                   IP Address: 10.228.136.24
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: <username>
                                 Model Number: BES-53248
                               Switch Network: cluster-network
                             Software Version: 3.9.0.2
                       Reason For Not Monitoring: None  <---- should
display this if SNMP settings are valid
                        Source Of Switch Version: CDP/ISDP
                                  Is Monitored ?: true
                    Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA
```

Cisco Switches

Konfigurieren Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf Cisco 9336C-FX2-Switches:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```

- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt  auth [md5|sha] AUTH-
PASSWORD priv aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

```
(sw1)(Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1)(Config)# show snmp user

-----------------------------------------------------------------------
---------
                              SNMP USERS
-----------------------------------------------------------------------
---------

User              Auth            Priv(enforce)   Groups
acl_filter
----------------- --------------- --------------- ---------------
-----------
admin             md5             des(no)         network-admin
SNMPv3User        md5             aes-128(no)     network-operator

-----------------------------------------------------------------------
---------
     NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
-----------------------------------------------------------------------
---------

User              Auth                Priv
----------------- ------------------ ------------

(sw1)(Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                  Device Name: sw1
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv2c
                                Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: cshm1!
                                   Model Number: N9K-C9336C-FX2
                                 Switch Network: cluster-network
                               Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                     Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                      Source Of Switch Version: CDP/ISDP
                                Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                   RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                  Device Name: sw1
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
   SNMPv2c Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: N9K-C9336C-FX2
                               Switch Network: cluster-network
                             Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                      Reason For Not Monitoring: None  <---- displays
when SNMP settings are valid
                       Source Of Switch Version: CDP/ISDP
                                 Is Monitored ?: true
                   Serial Number of the Device: QTFCU3826001C
                                  RCF Version: v1.8X2 for
Cluster/HA/RDMA

cluster1::*>
```

NVIDIA – CL 5.4.0

Konfigurieren Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf NVIDIA SN2100-Switches mit CLI 5.4.0:

- Für **keine Authentifizierung**:

```
nv set service snmp-server username SNMPv3_USER auth-none
```

- Für * MD5/SHA-Authentifizierung*:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
nv set service snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
net show snmp status
```

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     4318
Version 1 and 2c Community String  Configured
Version 3 Usernames                Not Configured
---------------------------------  ----------------
cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf        2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf   2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
 # Auto-generated config file: do not edit. #
 agentaddress udp:@mgmt:161
 agentxperms 777 777 snmp snmp
 agentxsocket /var/agentx/master
 createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
 ifmib_max_num_ifaces 500
 iquerysecname _snmptrapusernameX
 master agentx
 monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
```

```
 pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
 pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
 pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
 pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
 pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
 pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
 pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
 pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
 pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
 pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
 pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
 pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
 pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshm1! default
 rouser _snmptrapusernameX
+rouser SNMPv3User priv
 sysobjectid 1.3.6.1.4.1.40310
 sysservices 72
-rocommunity cshm1! default


net add/del commands since the last "net commit"

User        Timestamp                   Command
----------  --------------------------
-------------------------------------------------------------------
-----
SNMPv3User  2020-08-11 00:13:51.826987  net add snmp-server username
SNMPv3User auth-md5 <password> encrypt-aes <password>

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
---------------------------------  ----------------
Current Status                     active (running)
Reload Status                      enabled
Listening IP Addresses             all vrf mgmt
Main snmpd PID                     24253
Version 1 and 2c Community String  Configured
Version 3 Usernames                Configured     <---- Configured
here
---------------------------------  ----------------
cumulus@sw1:~$
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name SNMPv3User -application
snmp -authentication-method usm -remote-switch-ipaddress
10.231.80.212
```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                SNMP Version: SNMPv2c
                               Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                 SNMP Version: SNMPv3
                                Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.4.0 running on Mellanox Technologies Ltd. MSN2100
                      Reason For Not Monitoring: None
                       Source Of Switch Version: LLDP
                                 Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

NVIDIA – CL 5.11.0

Konfigurieren Sie einen SNMPv3-Benutzernamen SNMPv3_USER auf NVIDIA SN2100-Switches mit CLI 5.11.0:

- Für **keine Authentifizierung**:

```
nv set system snmp-server username SNMPv3_USER auth-none
```

- Für * MD5/SHA-Authentifizierung*:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD
```

- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
nv set system snmp-server username SNMPv3_USER [auth-md5|auth-sha]
AUTH-PASSWORD [encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
security login create -user-or-group-name SNMPv3_USER -application snmp
-authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

   ```
   nv show system snmp-server
   ```

   ```
   cumulus@sw1:~$ nv show system snmp-server
                         applied
   --------------------  ----------------------------------------
   [username]            SNMPv3_USER
   [username]            limiteduser1
   [username]            testuserauth
   [username]            testuserauthaes
   [username]            testusernoauth
   trap-link-up
     check-frequency     60
   trap-link-down
     check-frequency     60
   [listening-address]   all
   [readonly-community]  $nvsec$94d69b56e921aec1790844eb53e772bf
   state                 enabled
   cumulus@sw1:~$
   ```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

   ```
   security login create -user-or-group-name SNMPv3User -application
   snmp -authentication-method usm -remote-switch-ipaddress
   10.231.80.212
   ```

```
cluster1::*> security login create -user-or-group-name SNMPv3User
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)"
-instance
```

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                SNMP Version: SNMPv2c
                               Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: cshm1!
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

```
cluster1::*> system switch ethernet polling-interval show
         Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance
                                  Device Name: sw1
(b8:59:9f:09:7c:22)
                                   IP Address: 10.231.80.212
                                SNMP Version: SNMPv3
                               Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
           Community String or SNMPv3 Username: SNMPv3User
                                 Model Number: MSN2100-CB2FC
                               Switch Network: cluster-network
                             Software Version: Cumulus Linux
version 5.11.0 running on Mellanox Technologies Ltd. MSN2100
                     Reason For Not Monitoring: None
                      Source Of Switch Version: LLDP
                                Is Monitored ?: true
                   Serial Number of the Device: MT2110X06399  <----
serial number to check
                                   RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Konfigurieren der Protokollsammlung auf einem MetroCluster-IP-Switch

In einer MetroCluster-IP-Konfiguration können Sie die Protokollsammlung so konfigurieren, dass Switch-Protokolle zu Debugzwecken gesammelt werden.

> Auf Broadcom- und Cisco-Switches ist für jeden Cluster mit Protokollsammlung ein neuer Benutzer erforderlich. Beispielsweise erfordern MetroCluster 1, MetroCluster 2, MetroCluster 3 und MetroCluster 4 die Konfiguration eines separaten Benutzers auf den Switches. Mehrere SSH-Schlüssel für denselben Benutzer werden nicht unterstützt.

Über diese Aufgabe

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung der Erfassung, der Anforderung detaillierter **Support** Protokolle und der Aktivierung einer stündlichen Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

HINWEIS: Wenn Sie den FIPS-Modus aktivieren, müssen Sie Folgendes ausführen:

1. Generieren Sie SSH-Schlüssel auf dem Switch mithilfe der Herstelleranweisungen neu.
2. Regenerieren Sie SSH-Schlüssel in ONTAP mit `debug system regenerate-systemshell-key-pair`
3. Führen Sie die Setup-Routine für die Protokollsammlung mit dem `system switch ethernet log setup-password` Befehl erneut aus

Bevor Sie beginnen

- Der Benutzer muss Zugriff auf die Switch-Befehle haben `show` . Wenn diese nicht verfügbar sind, erstellen Sie einen neuen Benutzer und erteilen Sie dem Benutzer die erforderlichen Berechtigungen.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass `Is Monitored:` Feld ist in der Ausgabe des `system switch ethernet show` Befehl.
- Für die Protokollerfassung mit Broadcom- und Cisco-Switches:
  - Der lokale Benutzer muss über Netzwerkadministratorrechte verfügen.
  - Für jedes Cluster-Setup sollte auf dem Switch ein neuer Benutzer erstellt werden, bei dem die Protokollerfassung aktiviert ist. Diese Switches unterstützen nicht mehrere SSH-Schlüssel für denselben Benutzer. Bei jeder weiteren Einrichtung der Protokollerfassung werden alle bereits vorhandenen SSH-Schlüssel für den Benutzer überschrieben.
- Für die Unterstützung der Log-Erfassung mit NVIDIA-Switches muss der *user* für die Log-Sammlung berechtigt sein `cl-support`, den Befehl auszuführen, ohne ein Passwort angeben zu müssen. Führen Sie den folgenden Befehl aus, um diese Verwendung zuzulassen:

```
echo '<user> ALL = NOPASSWD: /usr/cumulus/bin/cl-support' | sudo EDITOR='tee -a' visudo -f /etc/sudoers.d/cumulus
```

Schritte

ONTAP 9.15.1 und höher

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

   HINWEIS: Wenn Sie bei der Benutzerspezifikationsabfrage mit **y** antworten, stellen Sie sicher, dass der Benutzer über die erforderlichen Berechtigungen verfügt, wie in Bevor Sie beginnen .

   ```
   system switch ethernet log setup-password
   ```

   ```
   cluster1::*> system switch ethernet log setup-password
   Enter the switch name: <return>
   The switch name entered is not recognized.
   Choose from the following list:
   cs1
   cs2

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs1
   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>

   cluster1::*> system switch ethernet log setup-password

   Enter the switch name: cs2

   Would you like to specify a user other than admin for log
   collection? {y|n}: n

   Enter the password: <enter switch password>
   Enter the password again: <enter switch password>
   ```

   Erstellen Sie für CL 5.11.1 den Benutzer **cumulus** und antworten Sie mit **y** auf die folgende Eingabeaufforderung: Möchten Sie für die Protokollerfassung einen anderen Benutzer als den Administrator angeben? {y|n}: **y**

1. [[Schritt 2]]Aktivieren Sie die regelmäßige Protokollerfassung:

```
system switch ethernet log modify -device <switch-name> -periodic
-enabled true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs1: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log modify -device cs2 -periodic
-enabled true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

cs2: Periodic log collection has been scheduled to run every hour.

cluster1::*> system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       true        scheduled
never-run
cs2                                       true        scheduled
never-run
2 entries were displayed.
```

2. Support-Protokoll anfordern:

```
system switch ethernet log collect-support-log -device <switch-name>
```

```
cluster1::*> system switch ethernet log collect-support-log -device
cs1

cs1: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> system switch ethernet log collect-support-log -device
cs2

cs2: Waiting for the next Ethernet switch polling cycle to begin
support collection.

cluster1::*> *system switch ethernet log show
                                          Periodic    Periodic
Support
Switch                                    Log Enabled Log State
Log State

cs1                                       false       halted
initiated
cs2                                       true        scheduled
initiated
2 entries were displayed.
```

3. Um alle Details der Protokollsammlung anzuzeigen, einschließlich der Aktivierung, Statusmeldung, des vorherigen Zeitstempels und des Dateinamens der periodischen Erfassung, des Anforderungsstatus, der Statusmeldung und des vorherigen Zeitstempels und des Dateinamens der Support-Sammlung, verwenden Sie Folgendes:

```
system switch ethernet log show -instance
```

```
cluster1::*> system switch ethernet log show -instance

                    Switch Name: cs1
           Periodic Log Enabled: true
            Periodic Log Status: Periodic log collection has been
scheduled to run every hour.
    Last Periodic Log Timestamp: 3/11/2024 11:02:59
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:14:20
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz

                    Switch Name: cs2
           Periodic Log Enabled: false
            Periodic Log Status: Periodic collection has been
halted.
    Last Periodic Log Timestamp: 3/11/2024 11:05:18
          Periodic Log Filename: cluster1:/mroot/etc/log/shm-
cluster-info.tgz
          Support Log Requested: false
             Support Log Status: Successfully gathered support logs
- see filename for their location.
     Last Support Log Timestamp: 3/11/2024 11:18:54
           Support Log Filename: cluster1:/mroot/etc/log/shm-
cluster-log.tgz
2 entries were displayed.
```

ONTAP 9.14.1 und frühere Versionen

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

   HINWEIS: Wenn Sie auf die Eingabeaufforderung der Benutzerspezifikation antworten `y`, stellen Sie sicher, dass der Benutzer die erforderlichen Berechtigungen hatBevor Sie beginnen, wie in beschrieben.

   ```
   system switch ethernet log setup-password
   ```

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2

Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Erstellen Sie für CL 5.11.1 den Benutzer **cumulus** und antworten Sie mit **y** auf die folgende Eingabeaufforderung: Möchten Sie für die Protokollerfassung einen anderen Benutzer als den Administrator angeben? {y|n}: **y**

1. [[Schritt 2]] Um die Erfassung des Support-Protokolls anzufordern und die regelmäßige Erfassung zu aktivieren, führen Sie den folgenden Befehl aus. Damit werden beide Arten der Protokollerfassung gestartet: Die detaillierten `Support` Protokolle und eine stündliche Datenerfassung `Periodic`.

```
system switch ethernet log modify -device <switch-name> -log-request
true
```

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Wenn Fehlerzustände durch die Log-Collection-Funktion (sichtbar in der Ausgabe von) gemeldet werden `system switch ethernet log show`, siehe "Fehlerbehebung bei der Protokollerfassung" für weitere Details.

Verwalten Sie die Überwachung von Ethernet-Switches in einer MetroCluster-IP-Konfiguration

In den meisten Fällen werden Ethernet-Switches automatisch von ONTAP erkannt und von CSHM überwacht. Die auf den Switch angewendete Referenzkonfigurationsdatei (RCF) aktiviert unter anderem das Cisco Discovery Protocol (CDP) und/oder das Link Layer Discovery Protocol (LLDP). Möglicherweise müssen Sie jedoch manuell einen Switch hinzufügen, der nicht erkannt wird, oder einen Switch entfernen, der nicht mehr verwendet wird. Sie können die aktive Überwachung auch beenden, während Sie den Switch in der Konfiguration beibehalten, z. B. während der Wartung.

Erstellen Sie einen Switch-Eintrag, damit ONTAP ihn überwachen kann

Über diese Aufgabe

Verwenden Sie den `system switch ethernet create` Befehl, um die Überwachung für einen bestimmten Ethernet-Switch manuell zu konfigurieren und zu aktivieren. Dies ist hilfreich, wenn ONTAP den Switch nicht automatisch hinzufügt, oder wenn Sie den Switch zuvor entfernt haben und ihn erneut hinzufügen möchten.

```
system switch ethernet create -device DeviceName -address 1.2.3.4 -snmp
-version SNMPv2c -community-or-username cshm1! -model NX3132V -type
cluster-network
```

Ein typisches Beispiel ist das Hinzufügen eines Switches namens [DeviceName] mit der IP-Adresse 1.2.3.4 und SNMPv2c-Anmeldeinformationen auf **cshm1!**. Verwenden Sie `-type storage-network` statt `-type cluster-network`, wenn Sie einen Speicherschalter konfigurieren.

Deaktivieren Sie die Überwachung, ohne den Switch zu löschen

Wenn Sie die Überwachung für einen bestimmten Switch anhalten oder beenden möchten, ihn aber für eine zukünftige Überwachung beibehalten möchten, ändern Sie dessen Parameter, `is-monitoring-enabled-admim` anstatt ihn zu löschen.

Beispiel:

```
system switch ethernet modify -device DeviceName -is-monitoring-enabled
-admin false
```

Auf diese Weise können Sie die Switch-Details und -Konfiguration beibehalten, ohne neue Warnmeldungen oder erneute Ermittlungen zu erzeugen.

Entfernen Sie einen Schalter, den Sie nicht mehr benötigen

Verwenden Sie diese Option `system switch ethernet delete`, um einen Switch zu löschen, der getrennt wurde oder nicht mehr benötigt wird:

```
system switch ethernet delete -device DeviceName
```

Standardmäßig ist dieser Befehl nur erfolgreich, wenn ONTAP den Switch derzeit nicht über CDP oder LLDP erkennt. Um einen erkannten Switch zu entfernen, verwenden Sie den `-force` Parameter:

```
system switch ethernet delete -device DeviceName -force
```

Wenn `-force` verwendet wird, wird der Switch möglicherweise automatisch wieder hinzugefügt, wenn ONTAP ihn erneut erkennt.

Überprüfen der Ethernet-Switch-Überwachung in einer MetroCluster-IP-Konfiguration

Die Ethernet-Switch-Systemzustandsüberwachung (CSHM) versucht automatisch, die erkannten Switches zu überwachen. Wenn die Switches jedoch nicht richtig konfiguriert sind, erfolgt die Überwachung möglicherweise nicht automatisch. Sie sollten überprüfen, ob die Systemzustandsüberwachung ordnungsgemäß für das Monitoring Ihrer Switches konfiguriert ist.

Überwachung der angeschlossenen Ethernet-Switches bestätigen

Über diese Aufgabe

Um zu überprüfen, ob die angeschlossenen Ethernet-Switches überwacht werden, führen Sie Folgendes aus:

```
system switch ethernet show
```

Wenn in der `Model` Spalte **OTHER** angezeigt wird oder im `IS Monitored` Feld **false** angezeigt wird, kann ONTAP den Switch nicht überwachen. Ein Wert von **ANDERE** zeigt in der Regel an, dass ONTAP diesen Switch für die Integritätsüberwachung nicht unterstützt.

Das `IS Monitored` Feld wird aus dem im Feld angegebenen Grund auf **false** gesetzt `Reason`.

> Wenn ein Switch in der Befehlsausgabe nicht aufgeführt ist, hat ONTAP ihn wahrscheinlich nicht erkannt. Vergewissern Sie sich, dass der Switch ordnungsgemäß verkabelt ist. Bei Bedarf können Sie den Schalter manuell hinzufügen. Weitere Informationen finden Sie unter "Verwalten Sie die Überwachung von Ethernet-Switches" .

Vergewissern Sie sich, dass die Firmware- und RCF-Versionen auf dem neuesten Stand sind

Stellen Sie sicher, dass auf dem Switch die neueste unterstützte Firmware ausgeführt wird und dass eine kompatible Referenzkonfigurationsdatei (RCF) angewendet wurde. Weitere Informationen finden Sie auf der "NetApp Support Downloads Seite".

Standardmäßig verwendet der Gesundheitsmonitor SNMPv2c mit der Community-Zeichenfolge **cshm1!** für die Überwachung, aber SNMPv3 kann auch konfiguriert werden.

Wenn Sie die Standard-SNMPv2c-Community-Zeichenfolge ändern müssen, stellen Sie sicher, dass die gewünschte SNMPv2c-Community-Zeichenfolge auf dem Switch konfiguriert wurde.

```
system switch ethernet modify -device SwitchA -snmp-version SNMPv2c
-community-or-username newCommunity!
```

> Weitere Informationen zur Konfiguration von SNMPv3 für die Verwendung finden Sie unter"Optional: SNMPv3 konfigurieren".

Bestätigen Sie die Verbindung zum Managementnetzwerk

Vergewissern Sie sich, dass der Managementport des Switch mit dem Managementnetzwerk verbunden ist.

Für die Ausführung von SNMP-Abfragen und Protokollerfassung ist eine korrekte Management-Port-Verbindung für ONTAP erforderlich.

Verwandte Informationen

- "Fehlerbehebung bei Warnmeldungen"

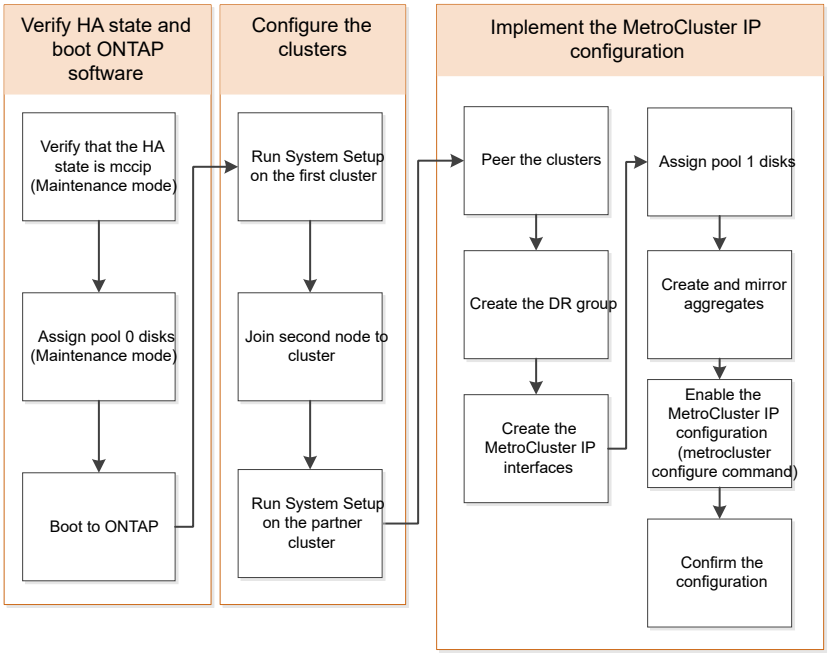
Konfigurieren Sie die MetroCluster Software in ONTAP

Konfigurieren Sie die MetroCluster-Software mithilfe der CLI

Einrichten der ONTAP Knoten und -Cluster in der MetroCluster -IP-Konfiguration

Sie müssen jeden Node in der MetroCluster Konfiguration in ONTAP einrichten, einschließlich der Node-Konfiguration und der Konfiguration der Nodes an zwei Standorten. Sie müssen auch die MetroCluster Beziehung zwischen beiden Standorten implementieren.

Wenn ein Controller-Modul während der Konfiguration ausfällt, lesen Sie "Ausfallszenarien für Controller-Module während der MetroCluster-Installation".



Konfigurieren Sie MetroCluster IP-Konfigurationen mit acht Knoten

Eine MetroCluster Konfiguration mit acht Nodes besteht aus zwei DR-Gruppen. Um die erste DR-Gruppe zu konfigurieren, führen Sie die Aufgaben in diesem Abschnitt aus. Nachdem Sie die erste DR-Gruppe konfiguriert haben, können Sie die folgenden Schritte ausführen: "Erweitern Sie eine MetroCluster IP-Konfiguration mit vier Knoten auf eine Konfiguration mit acht Knoten" .

Sammeln Sie die erforderlichen Informationen für Ihre MetroCluster -IP-Konfiguration

Sie müssen die erforderlichen IP-Adressen für die Controller-Module erfassen, bevor Sie mit dem Konfigurationsprozess beginnen.

Über diese Links können Sie CSV-Dateien herunterladen und die Tabellen mit Ihren standortspezifischen Informationen ausfüllen.

"MetroCluster IP-Setup-Arbeitsblatt, Site_A"

"MetroCluster IP-Setup-Arbeitsblatt, Site_B"

Vergleichen Sie ONTAP Standardcluster- und MetroCluster -Konfigurationen

Die Konfiguration der Nodes in jedem Cluster in einer MetroCluster-Konfiguration ist ähnlich wie bei den Nodes in einem Standard-Cluster.

Die MetroCluster-Konfiguration basiert auf zwei Standard-Clustern. Physisch muss die Konfiguration symmetrisch sein, wobei jeder Node über dieselbe Hardware-Konfiguration verfügt. Außerdem müssen alle MetroCluster Komponenten verkabelt und konfiguriert werden. Die grundlegende Softwarekonfiguration für Nodes in einer MetroCluster-Konfiguration ist jedoch dieselbe wie für Nodes in einem Standard-Cluster.

Konfigurationsschritt	Standardmäßige Cluster-Konfiguration	MetroCluster-Konfiguration
Konfiguration von Management-, Cluster- und Daten-LIFs auf jedem Node	Gleiches gilt für beide Cluster-Typen	
Konfigurieren Sie das Root-Aggregat.	Gleiches gilt für beide Cluster-Typen	
Richten Sie das Cluster auf einem Node im Cluster ein.	Gleiches gilt für beide Cluster-Typen	
Fügen Sie den anderen Node zum Cluster hinzu.	Gleiches gilt für beide Cluster-Typen	
Erstellen Sie ein gespiegeltes Root-Aggregat.	Optional	Erforderlich
Peer-to-Peer-Cluster	Optional	Erforderlich
Aktivieren der MetroCluster-Konfiguration	Nicht zutreffend	Erforderlich

Überprüfen Sie den HA-Konfigurationsstatus Ihrer Controller- und Chassis-Komponenten in einer MetroCluster -IP-Konfiguration

In einer MetroCluster IP-Konfiguration müssen Sie überprüfen, ob der ha-Konfigurationsstatus der Controller- und Chassis-Komponenten auf „`mccip`“ eingestellt ist, damit sie ordnungsgemäß booten. Obwohl dieser Wert auf werkseitig empfangene Systeme vorkonfiguriert sein sollte, sollten Sie die Einstellung dennoch überprüfen, bevor Sie fortfahren.

Wenn der HA-Status des Controller-Moduls und des Chassis falsch ist, können Sie die MetroCluster nicht konfigurieren, ohne den Node neu zu initialisieren. Sie müssen die Einstellung mit diesem Verfahren korrigieren und dann das System mit einem der folgenden Verfahren initialisieren:

- Führen Sie in einer MetroCluster IP-Konfiguration die Schritte in "Systemstandardwerte auf einem Controller-Modul wiederherstellen"aus.
- Führen Sie in einer MetroCluster FC-Konfiguration die Schritte in "Stellen Sie die Systemstandardeinstellungen wieder her und konfigurieren Sie den HBA-Typ auf einem Controller-Modul"aus.

Bevor Sie beginnen

Vergewissern Sie sich, dass sich das System im Wartungsmodus befindet.

Schritte

1. Zeigen Sie im Wartungsmodus den HA-Status des Controller-Moduls und des Chassis an:

   `ha-config show`

   Der richtige HA-Status hängt von Ihrer MetroCluster-Konfiguration ab.

MetroCluster-Konfigurationstyp	HA-Status für alle Komponenten…
MetroCluster FC-Konfiguration mit acht oder vier Nodes	mcc
MetroCluster FC-Konfiguration mit zwei Nodes	mcc-2n
MetroCluster IP-Konfiguration mit acht oder vier Nodes	Mccip

2. Wenn der angezeigte Systemstatus des Controllers nicht korrekt ist, legen Sie den korrekten HA-Status für Ihre Konfiguration auf dem Controller-Modul fest:

MetroCluster-Konfigurationstyp	Befehl
MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify controller mcc-2n`
MetroCluster IP-Konfiguration mit acht oder vier Nodes	`ha-config modify controller mccip`

3. Wenn der angezeigte Systemstatus des Chassis nicht korrekt ist, legen Sie den korrekten HA-Status für Ihre Konfiguration auf dem Chassis fest:

MetroCluster-Konfigurationstyp	Befehl

MetroCluster FC-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mcc`
MetroCluster FC-Konfiguration mit zwei Nodes	`ha-config modify chassis mcc-2n`
MetroCluster IP-Konfiguration mit acht oder vier Nodes	`ha-config modify chassis mccip`

4. Booten des Node zu ONTAP:

   `boot_ontap`

5. Wiederholen Sie dieses gesamte Verfahren, um den HA-Status auf jedem Node in der MetroCluster-Konfiguration zu überprüfen.

Stellen Sie die Systemstandards auf einem Controllermodul wieder her, bevor Sie eine MetroCluster IP-Konfiguration einrichten

Setzen Sie die Standardeinstellungen der Controller-Module zurück und stellen Sie sie wieder her.

1. Geben Sie an der LOADER-Eingabeaufforderung Umgebungsvariablen auf ihre Standardeinstellung zurück: `set-defaults`
2. Starten Sie den Knoten im Startmenü: `boot_ontap menu`

   Warten Sie, bis das Startmenü angezeigt wird, nachdem Sie diesen Befehl ausgeführt haben.

3. Löschen Sie die Node-Konfiguration:

   - Wenn Sie Systeme verwenden, die für ADP konfiguriert sind, wählen Sie Option `9a` Über das Startmenü und antworten `no` Wenn Sie dazu aufgefordert werden.

     Dieser Prozess ist störend.

     Auf dem folgenden Bildschirm wird die Eingabeaufforderung des Startmenüs angezeigt:

```
Please choose one of the following:

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 9a
...

########## WARNING: AGGREGATES WILL BE DESTROYED ##########
This is a disruptive operation that applies to all the disks
that are attached and visible to this node.

Before proceeding further, make sure that:

The aggregates visible from this node do not contain
data that needs to be preserved.
This option (9a) has been executed or will be executed
on the HA partner node (and DR/DR-AUX partner nodes if
applicable), prior to reinitializing any system in the
HA-pair or MetroCluster configuration.
The HA partner node (and DR/DR-AUX partner nodes if
applicable) is currently waiting at the boot menu.
Do you want to abort this operation (yes/no)? no
```

- Wenn Ihr System nicht für ADP konfiguriert ist, geben Sie ein `wipeconfig` Drücken Sie an der Eingabeaufforderung des Startmenüs die Eingabetaste.

  Auf dem folgenden Bildschirm wird die Eingabeaufforderung des Startmenüs angezeigt:

```
Please choose one of the following:

    (1) Normal Boot.
    (2) Boot without /etc/rc.
    (3) Change password.
    (4) Clean configuration and initialize all disks.
    (5) Maintenance mode boot.
    (6) Update flash from backup config.
    (7) Install new software first.
    (8) Reboot node.
    (9) Configure Advanced Drive Partitioning.
    Selection (1-9)?  wipeconfig
This option deletes critical system configuration, including cluster
membership.
Warning: do not run this option on a HA node that has been taken over.
Are you sure you want to continue?: yes
Rebooting to finish wipeconfig request.
```

Manuelles Zuweisen von Laufwerken zu Pool 0 in einer MetroCluster -IP-Konfiguration

Wenn Sie die werkseitig konfigurierten Systeme nicht empfangen haben, müssen Sie die Pool-0-Laufwerke möglicherweise manuell zuweisen. Je nach Plattformmodell und ob das System ADP nutzt, müssen Sie für jeden Knoten der MetroCluster-IP-Konfiguration Laufwerke manuell dem Pool 0 zuweisen. Das von Ihnen verwendete Verfahren hängt von der Version von ONTAP ab.

Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.4 und höher)

Wenn das System werkseitig nicht konfiguriert wurde und die Anforderungen für die automatische Laufwerkszuweisung nicht erfüllt, müssen Sie die Pool-0-Laufwerke manuell zuweisen.

Über diese Aufgabe

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.4 oder höher.

Um festzustellen, ob Ihr System eine manuelle Festplattenzuweisung benötigt, sollten Sie prüfen "Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher".

Sie führen diese Schritte im Wartungsmodus aus. Der Vorgang muss an jedem Knoten der Konfiguration durchgeführt werden.

Die Beispiele in diesem Abschnitt basieren auf folgenden Annahmen:

- Node_A_1 und Node_A_2 eigene Laufwerke auf:
  - Standort_A-Shelf_1 (lokal)
  - Standort_B-Shelf_2 (Remote)
- Eigene Laufwerke Node_B_1 und Node_B_2 auf:

- Standort_B-Shelf_1 (lokal)
- Standort_A-Shelf_2 (Remote)

Schritte

1. Anzeigen des Startmenüs:

   ```
   boot_ontap menu
   ```

2. Wählen Sie Option 9a, und antworten `no` Wenn Sie dazu aufgefordert werden.

   Auf dem folgenden Bildschirm wird die Eingabeaufforderung des Startmenüs angezeigt:

   ```
   Please choose one of the following:

   (1) Normal Boot.
   (2) Boot without /etc/rc.
   (3) Change password.
   (4) Clean configuration and initialize all disks.
   (5) Maintenance mode boot.
   (6) Update flash from backup config.
   (7) Install new software first.
   (8) Reboot node.
   (9) Configure Advanced Drive Partitioning.
   (10) Set Onboard Key Manager recovery secrets.
   (11) Configure node for external key management.
   Selection (1-11)? 9a

   ...

   ########## WARNING: AGGREGATES WILL BE DESTROYED ##########
   This is a disruptive operation that applies to all the disks
   that are attached and visible to this node.

   Before proceeding further, make sure that:

   The aggregates visible from this node do not contain
   data that needs to be preserved.
   This option (9a) has been executed or will be executed
   on the HA partner node (and DR/DR-AUX partner nodes if
   applicable), prior to reinitializing any system in the
   HA-pair or MetroCluster configuration.
   The HA partner node (and DR/DR-AUX partner nodes if
   applicable) is currently waiting at the boot menu.
   Do you want to abort this operation (yes/no)? no
   ```

3. Wenn der Knoten neu gestartet wird, drücken Sie bei Aufforderung Strg-C, um das Startmenü anzuzeigen, und wählen Sie dann die Option für **Wartungsmodus Boot** aus.

4. Weisen Sie im Wartungsmodus den lokalen Aggregaten auf dem Node manuell Laufwerke zu:

   `disk assign *disk-id* -p 0 -s *local-node-sysid*`

   Die Laufwerke sollten symmetrisch zugeordnet werden, sodass jeder Knoten eine gleiche Anzahl von Laufwerken hat. Nachfolgend finden Sie eine Konfiguration mit zwei Storage-Shelfs an jedem Standort.

   a. Bei der Konfiguration von Node_A_1 weisen Sie Laufwerke von Steckplatz 0 bis 11 manuell dem Pool0 des Node A1 von Site_A-Shelf_1 zu.
   b. Bei der Konfiguration von Node_A_2 weisen Sie die Laufwerke von Steckplatz 12 bis 23 manuell dem Pool0 des Node A2 von Site_A-Shelf_1 zu.
   c. Beim Konfigurieren von Node_B_1 weisen Sie Laufwerke von Steckplatz 0 bis 11 manuell dem Pool0 des Node B1 von Site_B-Shelf_1 zu.
   d. Beim Konfigurieren von Node_B_2 weisen Sie Laufwerke manuell zwischen Steckplatz 12 und 23 dem Pool0 des Node B2 von Site_B-Shelf_1 zu.
5. Beenden des Wartungsmodus:

   `halt`

6. Anzeigen des Startmenüs:

   `boot_ontap menu`

7. Wiederholen Sie diese Schritte auf den anderen Knoten der MetroCluster IP-Konfiguration.
8. Wählen Sie Option **4** aus dem Startmenü auf beiden Knoten und lassen Sie das System booten.
9. Fahren Sie mit fort "Einrichtung von ONTAP".

Manuelles Zuweisen von Laufwerken für Pool 0 (ONTAP 9.3)

Wenn für jeden Node mindestens zwei Festplatten-Shelfs vorhanden sind, können Sie die automatische Zuweisung von ONTAP nutzen, um die lokalen (Pool 0) Festplatten automatisch zuzuweisen.

Über diese Aufgabe

Im Wartungsmodus des Node müssen Sie zunächst eine einzelne Festplatte in den entsprechenden Shelfs Pool 0 zuweisen. ONTAP weist dann automatisch den Rest der Festplatten im Shelf demselben Pool zu. Diese Aufgabe ist nicht erforderlich für Systeme, die vom Werk empfangen werden, die über Pool 0 verfügen, um das vorkonfigurierte Root-Aggregat zu enthalten.

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.3.

Dieser Vorgang ist nicht erforderlich, wenn Sie Ihre MetroCluster-Konfiguration vom Werk erhalten haben. Die Nodes aus dem Werk werden mit Pool 0-Festplatten und Root-Aggregaten konfiguriert.

Dieses Verfahren kann nur angewandt werden, wenn mindestens zwei Festplatten-Shelfs für jeden Node vorhanden sind, sodass die automatische Zuweisung von Festplatten auf Shelf-Ebene möglich ist. Wenn Sie die automatische Zuweisung auf Shelf-Ebene nicht verwenden können, müssen Sie die lokalen Festplatten manuell zuweisen, damit jeder Node über einen lokalen Festplatten-Pool (Pool 0) verfügt.

Diese Schritte müssen im Wartungsmodus ausgeführt werden.

Beispiele in diesem Abschnitt setzen die folgenden Platten-Shelves voraus:

- Node_A_1 besitzt Festplatten auf:
  - Standort_A-Shelf_1 (lokal)
  - Standort_B-Shelf_2 (Remote)
- Node_A_2 ist verbunden mit:
  - Standort_A-Shelf_3 (lokal)
  - Standort_B-Shelf_4 (Remote)
- Node_B_1 ist verbunden mit:
  - Standort_B-Shelf_1 (lokal)
  - Standort_A-Shelf_2 (Remote)
- Node_B_2 ist verbunden mit:
  - Standort_B-Shelf_3 (lokal)
  - Standort_A-Shelf_4 (Remote)

Schritte

1. Weisen Sie auf jedem Knoten manuell eine einzelne Festplatte für das Root-Aggregat zu:

   `disk assign *disk-id* -p 0 -s *local-node-sysid*`

   Durch die manuelle Zuweisung dieser Festplatten kann die Funktion für die automatische Zuweisung von ONTAP den Rest der Festplatten auf jedem Shelf zuweisen.

   a. Weisen Sie auf Node_A_1 manuell einer Festplatte aus dem lokalen Standort_A-Shelf_1 dem Pool 0 zu.
   b. Weisen Sie auf Node_A_2 manuell einer Festplatte aus dem lokalen Site_A-Shelf_3 dem Pool 0 zu.
   c. Weisen Sie auf Node_B_1 manuell eine Festplatte vom lokalen Standort_B-Shelf_1 dem Pool 0 zu.
   d. Weisen Sie auf Node_B_2 dem Pool 0 manuell eine Festplatte von Local Site_B-Shelf_3 zu.
2. Starten Sie jeden Knoten an Standort A mit Option 4 im Startmenü:

   Sie sollten diesen Schritt auf einem Node abschließen, bevor Sie mit dem nächsten Node fortfahren.

   a. Beenden des Wartungsmodus:

      `halt`

   b. Anzeigen des Startmenüs:

      `boot_ontap menu`

   c. Wählen Sie im Startmenü Option 4, und fahren Sie fort.
3. Starten Sie jeden Knoten an Standort B mit Option 4 im Startmenü:

   Sie sollten diesen Schritt auf einem Node abschließen, bevor Sie mit dem nächsten Node fortfahren.

   a. Beenden des Wartungsmodus:

      `halt`

b. Anzeigen des Startmenüs:

```
boot_ontap menu
```

c. Wählen Sie im Startmenü Option 4, und fahren Sie fort.

Einrichten von ONTAP -Knoten in einer MetroCluster -IP-Konfiguration

Nachdem Sie jeden Node gebootet haben, werden Sie aufgefordert, eine grundlegende Node- und Cluster-Konfiguration durchzuführen. Nach dem Konfigurieren des Clusters kehren Sie zur ONTAP-CLI zurück, um Aggregate zu erstellen und die MetroCluster-Konfiguration zu erstellen.

Bevor Sie beginnen

- Sie müssen die MetroCluster-Konfiguration verkabelt haben.

Wenn Sie die neuen Controller mit einem Netboot booten müssen, siehe "Booten Sie die neuen Controller-Module ein".

Über diese Aufgabe

Diese Aufgabe muss auf beiden Clustern in der MetroCluster Konfiguration ausgeführt werden.

Schritte

1. Schalten Sie jeden Node am lokalen Standort ein, wenn dies noch nicht geschehen ist, und lassen Sie ihn alle vollständig booten.

   Wenn sich das System im Wartungsmodus befindet, müssen Sie den Stopp-Befehl eingeben, um den Wartungsmodus zu beenden, und geben Sie dann den aus `boot_ontap` Befehl zum Booten des Systems und Abrufen des Cluster-Setups.

2. Fahren Sie auf dem ersten Node in jedem Cluster mit den Aufforderungen zum Konfigurieren des Clusters fort.

   a. Aktivieren Sie das AutoSupport-Tool, indem Sie den vom System bereitgestellten Anweisungen folgen.

      Die Ausgabe sollte wie folgt aussehen:

```
Welcome to the cluster setup wizard.

    You can enter the following commands at any time:
    "help" or "?" - if you want to have a question clarified,
    "back" - if you want to change previously answered questions, and
    "exit" or "quit" - if you want to quit the cluster setup wizard.
    Any changes you made before quitting will be saved.

    You can return to cluster setup at any time by typing "cluster
setup".
    To accept a default or omit a question, do not enter a value.

    This system will send event messages and periodic reports to
NetApp Technical
    Support. To disable this feature, enter
    autosupport modify -support disable
    within 24 hours.

    Enabling AutoSupport can significantly speed problem
determination and
    resolution should a problem occur on your system.
    For further information on AutoSupport, see:
    http://support.netapp.com/autosupport/

    Type yes to confirm and continue {yes}: yes
.
.
.
```

b. Konfigurieren Sie die Node-Managementoberfläche, indem Sie auf die Eingabeaufforderungen antworten.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Enter the node management interface port [e0M]:
Enter the node management interface IP address: 172.17.8.229
Enter the node management interface netmask: 255.255.254.0
Enter the node management interface default gateway: 172.17.8.1
A node management interface on port e0M with IP address 172.17.8.229
has been created.
```

c. Erstellen Sie das Cluster, indem Sie auf die Eingabeaufforderungen antworten.

   Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
create


Do you intend for this node to be used as a single node cluster?
{yes, no} [no]:
no

Existing cluster interface configuration found:

Port MTU IP Netmask
e0a 1500 169.254.18.124 255.255.0.0
e1a 1500 169.254.184.44 255.255.0.0

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
Private cluster network ports [e0a,e1a].
Cluster port MTU values will be set to 9000.
Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: no

Enter the cluster administrator's (username "admin") password:

Retype the password:


Step 1 of 5: Create a Cluster
You can type "back", "exit", or "help" at any question.

List the private cluster network ports [e0a,e1a]:
Enter the cluster ports' MTU size [9000]:
Enter the cluster network netmask [255.255.0.0]: 255.255.254.0
Enter the cluster interface IP address for port e0a: 172.17.10.228
Enter the cluster interface IP address for port e1a: 172.17.10.229
Enter the cluster name: cluster_A

Creating cluster cluster_A

Starting cluster support services ...

Cluster cluster_A has been created.
```

d. Fügen Sie Lizenzen hinzu, richten Sie eine SVM für die Cluster-Administration ein, und geben Sie DNS-Informationen ein, indem Sie auf die Eingabeaufforderungen antworten.

Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Step 2 of 5: Add Feature License Keys
You can type "back", "exit", or "help" at any question.

Enter an additional license key []:


Step 3 of 5: Set Up a Vserver for Cluster Administration
You can type "back", "exit", or "help" at any question.


Enter the cluster management interface port [e3a]:
Enter the cluster management interface IP address: 172.17.12.153
Enter the cluster management interface netmask: 255.255.252.0
Enter the cluster management interface default gateway: 172.17.12.1

A cluster management interface on port e3a with IP address
172.17.12.153 has been created. You can use this address to connect
to and manage the cluster.

Enter the DNS domain names: lab.netapp.com
Enter the name server IP addresses: 172.19.2.30
DNS lookup for the admin Vserver will use the lab.netapp.com domain.

Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: svl
```

e. Aktivieren Sie das Speicherausfallschutz, und richten Sie den Knoten ein, indem Sie auf die Eingabeaufforderungen antworten.

Die Eingabeaufforderungen sind ähnlich wie folgende:

```
Step 4 of 5: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.


SFO will be enabled when the partner joins the cluster.


Step 5 of 5: Set Up the Node
You can type "back", "exit", or "help" at any question.

Where is the controller located []: site_A
```

f. Die Konfiguration des Node abschließen, jedoch keine Datenaggregate erstellen.

Sie können ONTAP System Manager verwenden und im Webbrowser die Cluster-Management-IP-Adresse (https://172.17.12.153).) aufrufen

"Cluster-Management mithilfe von System Manager (ONTAP 9.7 und früher)"

"ONTAP System Manager (Version 9.7 und höher)"

g. Konfigurieren Sie den Service-Prozessor (SP):

"Konfigurieren Sie das SP/BMC-Netzwerk"

"Verwenden Sie einen Service Processor mit System Manager - ONTAP 9.7 und früher"

3. Booten Sie den nächsten Controller, und verbinden Sie ihn mit den Aufforderungen zum Cluster.
4. Sicherstellen, dass die Nodes im Hochverfügbarkeits-Modus konfiguriert sind:

```
storage failover show -fields mode
```

Wenn dies nicht der Fall ist, müssen Sie auf jedem Node den HA-Modus konfigurieren und dann die Nodes neu booten:

```
storage failover modify -mode ha -node localhost
```

Der erwartete Konfigurationsstatus von HA und Storage-Failover lautet wie folgt:

- DER HA-Modus ist konfiguriert, ein Storage-Failover ist jedoch nicht aktiviert.
- DIE HA-Übernahmemfunktion ist deaktiviert.
- HA-Schnittstellen sind offline.
- SPÄTER werden HA-Modus, Storage Failover und Schnittstellen konfiguriert.

5. Sicherstellen, dass vier Ports als Cluster Interconnects konfiguriert sind:

```
network port show
```

Die MetroCluster-IP-Schnittstellen sind derzeit nicht konfiguriert und werden nicht in der Befehlsausgabe angezeigt.

Im folgenden Beispiel werden zwei Cluster-Ports auf Node_A_1 angezeigt:

```
cluster_A::*> network port show -role cluster


Node: node_A_1


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false

e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


Node: node_A_2


Ignore

                                                  Speed(Mbps) Health
Health

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status

--------- ------------ ---------------- ---- ---- ----------- --------
------

e4a       Cluster      Cluster          up   9000  auto/40000 healthy
false
```

```
e4e       Cluster      Cluster          up   9000  auto/40000 healthy
false


4 entries were displayed.
```

6. Wiederholen Sie diese Schritte auf dem Partner-Cluster.

Nächste Schritte

Kehren Sie zur ONTAP-Befehlszeilenschnittstelle zurück und führen Sie die MetroCluster-Konfiguration durch. Führen Sie dazu die folgenden Aufgaben aus.

Konfigurieren Sie ONTAP -Cluster in einer MetroCluster -IP-Konfiguration

Sie müssen die Cluster Peer, die Root-Aggregate spiegeln, ein gespiegeltes Datenaggregat erstellen und dann den Befehl zum Implementieren der MetroCluster Operationen ausgeben.

Über diese Aufgabe

Bevor Sie ausführen `metrocluster configure`, HA-Modus und DR-Spiegelung sind nicht aktiviert und Sie können eine Fehlermeldung in Bezug auf dieses erwartete Verhalten sehen. Sie aktivieren später den HA-Modus und die DR-Spiegelung, wenn Sie den Befehl ausführen `metrocluster configure` Um die Konfiguration zu implementieren.

Deaktivieren der automatischen Laufwerkszuweisung (bei manueller Zuweisung in ONTAP 9.4)

Wenn in ONTAP 9.4 Ihre MetroCluster IP-Konfiguration weniger als vier externe Storage-Shelfs pro Standort umfasst, müssen Sie die automatische Laufwerkszuweisung auf allen Nodes deaktivieren und Laufwerke manuell zuweisen.

Über diese Aufgabe

In ONTAP 9.5 und höher ist diese Aufgabe nicht erforderlich.

Diese Aufgabe gilt nicht für ein AFF A800 System mit einem internen Shelf und ohne externen Shelfs.

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Automatische Laufwerkszuweisung deaktivieren:

   ```
   storage disk option modify -node <node_name> -autoassign off
   ```

2. Sie müssen diesen Befehl für alle Knoten in der MetroCluster IP Konfiguration ausgeben.

Überprüfen der Laufwerkszuweisung von Pool 0-Laufwerken

Sie müssen überprüfen, ob die Remote-Laufwerke für die Knoten sichtbar sind und ordnungsgemäß zugewiesen wurden.

Über diese Aufgabe

Die automatische Zuweisung ist abhängig vom Plattformmodell für Storage-Systeme und der Anordnung der

Festplatten-Shelfs.

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Vergewissern Sie sich, dass Pool-0-Laufwerke automatisch zugewiesen werden:

   ```
   disk show
   ```

   Das folgende Beispiel zeigt die Ausgabe „Cluster_A“ für ein AFF A800 System ohne externe Shelfs.

   Ein Viertel (8 Laufwerke) wurde automatisch „Node_A_1“ zugewiesen und ein Quartal wurde automatisch „Node_A_2“ zugewiesen. Die übrigen Laufwerke sind Remote-Laufwerke (Pool 1) für „Node_B_1“ und „Node_B_2“.

   ```
   cluster_A::*> disk show
                    Usable      Disk      Container           Container
   Disk             Size        Shelf Bay Type    Type        Name
   Owner
   ---------------- ---------- ----- --- ------- ----------- ---------
   --------
   node_A_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
   node_A_1
   node_A_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
   node_A_1
   node_A_2:0n.0    1.75TB     0     0   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.1    1.75TB     0     1   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.2    1.75TB     0     2   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.3    1.75TB     0     3   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.4    1.75TB     0     4   SSD-NVM shared
   aggr0_node_A_2_0 node_A_2
   node_A_2:0n.5    1.75TB     0     5   SSD-NVM shared
   ```

```
aggr0_node_A_2_0 node_A_2
node_A_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_A_2_0 node_A_2
node_A_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_A_2
node_A_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_A_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_A_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_A_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_A_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_A_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_A_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_A_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_A_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_A_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_A_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_A_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_A_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_A_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_A_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_A_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.
```

Im folgenden Beispiel wird die Ausgabe „Cluster_B“ angezeigt:

```
cluster_B::> disk show
                 Usable     Disk              Container   Container
Disk             Size       Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------

Info: This cluster has partitioned disks. To get a complete list of
spare disk
capacity use "storage aggregate show-spare-disks".
node_B_1:0n.12   1.75TB     0     12  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.13   1.75TB     0     13  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.14   1.75TB     0     14  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.15   1.75TB     0     15  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.16   1.75TB     0     16  SSD-NVM shared      aggr0
node_B_1
```

```
node_B_1:0n.17   1.75TB     0     17  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.18   1.75TB     0     18  SSD-NVM shared      aggr0
node_B_1
node_B_1:0n.19   1.75TB     0     19  SSD-NVM shared      -
node_B_1
node_B_2:0n.0    1.75TB     0     0   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.1    1.75TB     0     1   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.2    1.75TB     0     2   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.3    1.75TB     0     3   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.4    1.75TB     0     4   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.5    1.75TB     0     5   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.6    1.75TB     0     6   SSD-NVM shared
aggr0_node_B_1_0 node_B_2
node_B_2:0n.7    1.75TB     0     7   SSD-NVM shared      -
node_B_2
node_B_2:0n.24   -          0     24  SSD-NVM unassigned  -         -
node_B_2:0n.25   -          0     25  SSD-NVM unassigned  -         -
node_B_2:0n.26   -          0     26  SSD-NVM unassigned  -         -
node_B_2:0n.27   -          0     27  SSD-NVM unassigned  -         -
node_B_2:0n.28   -          0     28  SSD-NVM unassigned  -         -
node_B_2:0n.29   -          0     29  SSD-NVM unassigned  -         -
node_B_2:0n.30   -          0     30  SSD-NVM unassigned  -         -
node_B_2:0n.31   -          0     31  SSD-NVM unassigned  -         -
node_B_2:0n.36   -          0     36  SSD-NVM unassigned  -         -
node_B_2:0n.37   -          0     37  SSD-NVM unassigned  -         -
node_B_2:0n.38   -          0     38  SSD-NVM unassigned  -         -
node_B_2:0n.39   -          0     39  SSD-NVM unassigned  -         -
node_B_2:0n.40   -          0     40  SSD-NVM unassigned  -         -
node_B_2:0n.41   -          0     41  SSD-NVM unassigned  -         -
node_B_2:0n.42   -          0     42  SSD-NVM unassigned  -         -
node_B_2:0n.43   -          0     43  SSD-NVM unassigned  -         -
32 entries were displayed.

cluster_B::>
```

Peering der Cluster

Die Cluster in der MetroCluster Konfiguration müssen sich in einer Peer-Beziehung zueinander finden, damit sie kommunizieren und die für MetroCluster Disaster Recovery essentielle Datenspiegelung durchführen

können.

Verwandte Informationen

"Express-Konfiguration für Cluster und SVM-Peering"

"Überlegungen bei der Verwendung von dedizierten Ports"

"Überlegungen bei der Freigabe von Datenports"

Konfigurieren von Intercluster LIFs für Cluster-Peering

Sie müssen Intercluster-LIFs an Ports erstellen, die für die Kommunikation zwischen den MetroCluster-Partner-Clustern verwendet werden. Sie können dedizierte Ports oder Ports verwenden, die auch Datenverkehr haben.

Konfigurieren von Intercluster-LIFs auf dedizierten Ports

Sie können Intercluster-LIFs auf dedizierten Ports konfigurieren. Dadurch wird typischerweise die verfügbare Bandbreite für den Replizierungsverkehr erhöht.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerk-Ports in „cluster01“ angezeigt:

   ```
   cluster01::> network port show
                                                                  Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
          e0e       Default      Default          up     1500   auto/1000
          e0f       Default      Default          up     1500   auto/1000
   ```

2. Bestimmen Sie, welche Ports für die Intercluster-Kommunikation verfügbar sind:

   ```
   network interface show -fields home-port,curr-port
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Das folgende Beispiel zeigt, dass den Ports „e0e“ und „e0f“ keine LIFs zugewiesen wurden:

   ```
   cluster01::> network interface show -fields home-port,curr-port
   vserver lif                  home-port curr-port
   ------- -------------------- --------- ---------
   Cluster cluster01-01_clus1   e0a       e0a
   Cluster cluster01-01_clus2   e0b       e0b
   Cluster cluster01-02_clus1   e0a       e0a
   Cluster cluster01-02_clus2   e0b       e0b
   cluster01
           cluster_mgmt         e0c       e0c
   cluster01
           cluster01-01_mgmt1   e0c       e0c
   cluster01
           cluster01-02_mgmt1   e0c       e0c
   ```

3. Erstellen Sie eine Failover-Gruppe für die dedizierten Ports:

   ```
   network interface failover-groups create -vserver <system_svm> -failover-group
   <failover_group> -targets <physical_or_logical_ports>
   ```

   Im folgenden Beispiel werden die Ports „e0e“ und „e0f“ der Failover-Gruppe „intercluster01“ auf dem System „SVMcluster01“ zugewiesen:

   ```
   cluster01::> network interface failover-groups create -vserver cluster01
   -failover-group
   intercluster01 -targets
   cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
   ```

4. Vergewissern Sie sich, dass die Failover-Gruppe erstellt wurde:

   ```
   network interface failover-groups show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
-----------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Erstellen Sie Intercluster-LIFs auf der System-SVM und weisen Sie sie der Failover-Gruppe zu.

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask_address> -failover-group
<failover_group>
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic.01“ und „cluster01_ic02“ in Failover-Gruppe „intercluster01“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show -service-policy default-intercluster
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface show -role intercluster
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

7. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show -service-policy default-intercluster -failover
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface show -role intercluster -failover
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass der Intercluster LIFs „cluster01_ic.01“, und „cluster01_ic.02“ auf dem „SVMe0e“ Port an den „e0f“-Port scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Verwandte Informationen

"Überlegungen bei der Verwendung von dedizierten Ports"

Konfigurieren von Intercluster-LIFs auf gemeinsam genutzten Datenports

Sie können Intercluster-LIFs an Ports konfigurieren, die gemeinsam mit dem Datennetzwerk verwendet werden. Auf diese Weise wird die Anzahl der Ports reduziert, die Sie für Intercluster-Netzwerke benötigen.

Schritte

1. Liste der Ports im Cluster:

   ```
   network port show
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel werden die Netzwerk-Ports in „cluster01“ angezeigt:

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Intercluster-LIFs auf der System-SVM erstellen:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-intercluster -home-node <node_name> -home-port <port_name>
-address <port_ip_address> -netmask <netmask>
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface create -vserver <system_svm> -lif <lif_name> -role
intercluster -home-node <node_name> -home-port <port_name> -address
<port_ip_address> -netmask <netmask>
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden Intercluster-LIFs „cluster01_ic.01“ und „cluster01_ic.02“ erstellt:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Überprüfen Sie, ob die Intercluster-LIFs erstellt wurden:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show -service-policy default-intercluster
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface show -role intercluster
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vergewissern Sie sich, dass die Intercluster-LIFs redundant sind:

Führen Sie in ONTAP 9.6 und höher Folgendes aus:

```
network interface show –service-policy default-intercluster -failover
```

Führen Sie in ONTAP 9.5 und früher Folgendes aus:

```
network interface show -role intercluster -failover
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

Das folgende Beispiel zeigt, dass Intercluster LIFs „cluster01_ic.01“ und „cluster01_ic.02“ auf dem „e0c“-Port an den „e0d“-Port scheitern.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Verwandte Informationen

"Überlegungen bei der Freigabe von Datenports"

Erstellen einer Cluster-Peer-Beziehung

Mit dem Befehl Cluster Peer create können Sie eine Peer-Beziehung zwischen einem lokalen und einem Remote-Cluster erstellen. Nachdem die Peer-Beziehung erstellt wurde, können Sie Cluster Peer Creation im Remote-Cluster ausführen, um sie für den lokalen Cluster zu authentifizieren.

Über diese Aufgabe

- Sie müssen auf jedem Node in den Clustern, die Peering durchführen, Intercluster LIFs erstellt haben.
- Die Cluster müssen ONTAP 9.3 oder höher ausführen.

Schritte

1. Erstellen Sie auf dem Ziel-Cluster eine Peer-Beziehung mit dem Quell-Cluster:

   ```
   cluster peer create -generate-passphrase -offer-expiration <MM/DD/YYYY
   HH:MM:SS|1…7days|1…168hours> -peer-addrs <peer_lif_ip_addresses> -ipspace
   <ipspace>
   ```

   Wenn Sie beides angeben `-generate-passphrase` Und `-peer-addrs`, Nur der Cluster, dessen Intercluster LIFs in angegeben sind `-peer-addrs` Kann das generierte Passwort verwenden.

   Sie können die ignorieren `-ipspace` Option, wenn kein benutzerdefinierter IPspace verwendet wird. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird eine Cluster-Peer-Beziehung auf einem nicht angegebenen Remote-Cluster erstellt:

```
cluster02::> cluster peer create -generate-passphrase -offer-expiration
2days

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: -
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Authentifizierung des Quellclusters im Quellcluster beim Ziel-Cluster:

   ```
   cluster peer create -peer-addrs <peer_lif_ip_addresses> -ipspace <ipspace>
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Im folgenden Beispiel wird der lokale Cluster an den Remote-Cluster unter LIF-IP-Adressen „192.140.112.101“ und „192.140.112.102“ authentifiziert:

   ```
   cluster01::> cluster peer create -peer-addrs
   192.140.112.101,192.140.112.102

   Notice: Use a generated passphrase or choose a passphrase of 8 or more
   characters.
           To ensure the authenticity of the peering relationship, use a
   phrase or sequence of characters that would be hard to guess.

   Enter the passphrase:
   Confirm the passphrase:

   Clusters cluster02 and cluster01 are peered.
   ```

   Geben Sie die Passphrase für die Peer-Beziehung ein, wenn Sie dazu aufgefordert werden.

3. Vergewissern Sie sich, dass die Cluster-Peer-Beziehung erstellt wurde:

   ```
   cluster peer show -instance
   ```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                             Remote Cluster Name: cluster2
                             Active IP Addresses: 192.140.112.101,
192.140.112.102
                           Cluster Serial Number: 1-80-123456
                  Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                 Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. Prüfen Sie die Konnektivität und den Status der Knoten in der Peer-Beziehung:

   `cluster peer health show`

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health  Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true            true
```

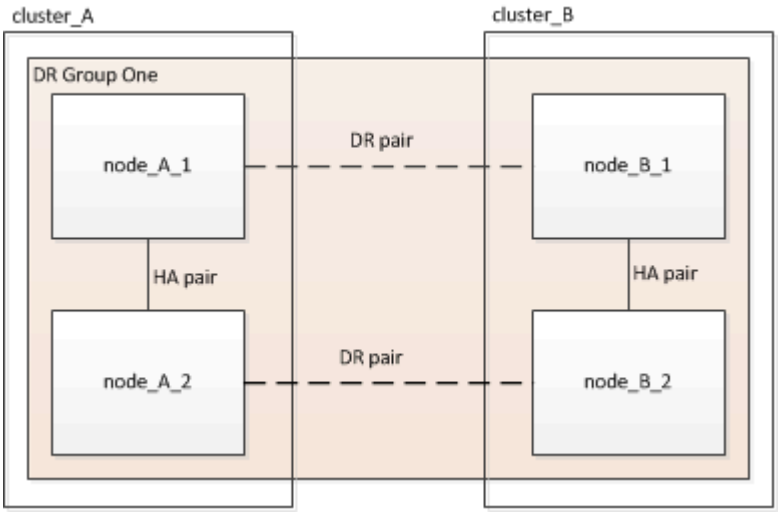
Erstellen der DR-Gruppe

Sie müssen die Disaster-Recovery-Gruppenbeziehungen (DR) zwischen den Clustern erstellen.

Über diese Aufgabe

Sie führen dieses Verfahren auf einem der Cluster in der MetroCluster-Konfiguration durch, um die DR-Beziehungen zwischen den Nodes in beiden Clustern zu erstellen.

Die DR-Beziehungen können nach Erstellung der DR-Gruppen nicht mehr geändert werden.



Schritte

1. Überprüfen Sie, ob die Nodes bereit für die Erstellung der DR-Gruppe sind, indem Sie auf jedem Node den folgenden Befehl eingeben:

   ```
   metrocluster configuration-settings show-status
   ```

   Die Befehlsausgabe sollte zeigen, dass die Nodes bereit sind:

   ```
   cluster_A::> metrocluster configuration-settings show-status
   Cluster                   Node          Configuration Settings Status
   ------------------------- -------------
   --------------------------------
   cluster_A                 node_A_1      ready for DR group create
                             node_A_2      ready for DR group create
   2 entries were displayed.
   ```

   ```
   cluster_B::> metrocluster configuration-settings show-status
   Cluster                   Node          Configuration Settings Status
   ------------------------- -------------
   --------------------------------
   cluster_B                 node_B_1      ready for DR group create
                             node_B_2      ready for DR group create
   2 entries were displayed.
   ```

2. Erstellen der DR-Gruppe:

   ```
   metrocluster configuration-settings dr-group create -partner-cluster
   ```

`<partner_cluster_name> -local-node <local_node_name> -remote-node <remote_node_name>`

Dieser Befehl wird nur einmal ausgegeben. Es muss nicht auf dem Partner-Cluster wiederholt werden. Sie geben im Befehl den Namen des Remote-Clusters und den Namen eines lokalen Node und eines Node im Partner-Cluster an.

Die beiden Nodes, die Sie angeben, sind als DR-Partner konfiguriert, und die anderen beiden Nodes (die im Befehl nicht angegeben sind) werden als das zweite DR-Paar in der DR-Gruppe konfiguriert. Diese Beziehungen können nicht geändert werden, wenn Sie diesen Befehl eingeben.

Mit dem folgenden Befehl werden diese DR-Paare erstellt:

- Node_A_1 und Node_B_1
- Node_A_2 und Node_B_2

```
Cluster_A::> metrocluster configuration-settings dr-group create
-partner-cluster cluster_B -local-node node_A_1 -remote-node node_B_1
[Job 27] Job succeeded: DR Group Create is successful.
```

Konfigurieren und Anschließen der MetroCluster IP-Schnittstellen

Sie müssen die MetroCluster IP-Schnittstellen konfigurieren, die zur Replizierung von Storage und nicht-flüchtigem Cache jedes Nodes verwendet werden. Anschließend stellen Sie die Verbindungen mithilfe der MetroCluster-IP-Schnittstellen bereit. Dadurch werden iSCSI-Verbindungen für die Speicherreplikation erstellt.

> Die MetroCluster-IP-Adresse und die verbundenen Switch-Ports werden erst online geschaltet, nachdem Sie die MetroCluster-IP-Schnittstellen erstellt haben.

Über diese Aufgabe

- Sie müssen für jeden Node zwei Schnittstellen erstellen. Die Schnittstellen müssen mit den in der MetroCluster RCF-Datei definierten VLANs verknüpft sein.
- Sie müssen alle MetroCluster IP Schnittstelle „A“-Ports in demselben VLAN und alle MetroCluster IP Schnittstelle „B“-Ports in dem anderen VLAN erstellen. Siehe "Überlegungen zur MetroCluster IP-Konfiguration".
- Ab ONTAP 9.9 müssen Sie auch die angeben, wenn Sie eine Layer 3-Konfiguration verwenden `-gateway` Parameter beim Erstellen von MetroCluster-IP-Schnittstellen. Siehe "Überlegungen für Layer 3-Weitbereichs-Netzwerke".

  Bestimmte Plattformen verwenden ein VLAN für die MetroCluster IP Schnittstelle. Standardmäßig verwenden alle beiden Ports ein anderes VLAN: 10 und 20.

  Falls unterstützt, können Sie auch ein anderes (nicht standardmäßiges) VLAN über 100 (zwischen 101 und 4095) angeben. Verwenden Sie dazu den `-vlan-id` Parameter im `metrocluster configuration-settings interface create` Befehl.

  Die folgenden Plattformen unterstützen **Not** den `-vlan-id` Parameter:

  - FAS8200 UND AFF A300
  - AFF A320

- FAS9000 und AFF A700
- AFF C800, ASA C800, AFF A800 und ASA A800

Alle anderen Plattformen unterstützen den `-vlan-id` Parameter.

Die Standard- und gültigen VLAN-Zuweisungen hängen davon ab, ob die Plattform den folgenden Parameter unterstützt `-vlan-id`:

Plattformen, die <code>-vlan-</code> unterstützen

Standard-VLAN:

- Wenn der `-vlan-id` Parameter nicht angegeben wird, werden die Schnittstellen mit VLAN 10 für die „A“-Ports und VLAN 20 für die „B“-Ports erstellt.
- Das angegebene VLAN muss mit dem im RCF ausgewählten VLAN übereinstimmen.

Gültige VLAN-Bereiche:

- Standard-VLAN 10 und 20
- VLANs 101 und höher (zwischen 101 und 4095)

Plattformen, die <code>-vlan-</code> nicht unterstützen

Standard-VLAN:

- Keine Angabe. Für die Schnittstelle muss kein VLAN auf der MetroCluster-Schnittstelle angegeben werden. Der Switch-Port definiert das verwendete VLAN.

Gültige VLAN-Bereiche:

- Alle VLANs werden beim Generieren der RCF nicht explizit ausgeschlossen. Die RCF warnt Sie, wenn das VLAN ungültig ist.

- Die von den MetroCluster IP-Schnittstellen verwendeten physischen Ports hängen vom Plattformmodell ab. Informationen zur Verwendung des Ports für Ihr System finden Sie unter "MetroCluster IP-Switches verkabeln" .
- Die folgenden IP-Adressen und Subnetze werden in den Beispielen verwendet:

Knoten	Schnittstelle	IP-Adresse	Subnetz
Node_A_1	MetroCluster IP-Schnittstelle 1	10.1.1.1	10.1.1/24
MetroCluster IP-Schnittstelle 2	10.1.2.1	10.1.2/24	Node_A_2
MetroCluster IP-Schnittstelle 1	10.1.1.2	10.1.1/24	MetroCluster IP-Schnittstelle 2

10.1.2.2	10.1.2/24	Knoten_B_1	MetroCluster IP-Schnittstelle 1
10.1.1.3	10.1.1/24	MetroCluster IP-Schnittstelle 2	10.1.2.3
10.1.2/24	Knoten_B_2	MetroCluster IP-Schnittstelle 1	10.1.1.4
10.1.1/24	MetroCluster IP-Schnittstelle 2	10.1.2.4	10.1.2/24

- Bei diesem Verfahren werden folgende Beispiele verwendet:

  Die Ports für ein AFF A700 oder ein FAS9000 System (e5a und e5b).

  Die Ports für ein AFF A220-System, um zu zeigen, wie der Parameter auf einer unterstützten Plattform verwendet `-vlan-id` wird.

  Konfigurieren Sie die Schnittstellen an den richtigen Ports für Ihr Plattformmodell.

Schritte

1. Vergewissern Sie sich, dass die automatische Festplattenzuordnung für jeden Node aktiviert ist:

   `storage disk option show`

   Bei der automatischen Festplattenzuweisung werden Pool 0- und Pool 1-Festplatten auf Shelf-Basis zugewiesen.

   In der Spalte Automatische Zuweisung wird angegeben, ob die automatische Zuweisung der Festplatte aktiviert ist.

```
Node        BKg. FW. Upd.  Auto Copy   Auto Assign  Auto Assign Policy
----------  -------------  ----------  -----------  ------------------
node_A_1             on           on           on           default
node_A_2             on           on           on           default
2 entries were displayed.
```

2. Vergewissern Sie sich, dass Sie auf den Nodes MetroCluster IP-Schnittstellen erstellen können:

   `metrocluster configuration-settings show-status`

   Alle Nodes sollten bereit sein:

```
Cluster       Node          Configuration Settings Status
----------    -----------   --------------------------------
cluster_A
              node_A_1      ready for interface create
              node_A_2      ready for interface create
cluster_B
              node_B_1      ready for interface create
              node_B_2      ready for interface create
4 entries were displayed.
```

3. Erstellen Sie die Schnittstellen auf Node_A_1.

   a. Konfigurieren Sie die Schnittstelle am Port „e5a“ auf „Node_A_1“:

      Verwenden Sie beim Erstellen von MetroCluster-IP-Schnittstellen keine IP-Adressen 169.254.17.x oder 169.254.18.x, um Konflikte mit automatisch generierten Schnittstellen-IP-Adressen im gleichen Bereich zu vermeiden.

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

      Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_A_1" mit IP-Adresse "10.1.1.1":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_1 -home-port e5a -address
      10.1.1.1 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

      Bei Plattformmodellen, die VLANs für die MetroCluster IP Schnittstelle unterstützen, können Sie die einschließen `-vlan-id` Parameter, wenn Sie die Standard-VLAN-IDs nicht verwenden möchten. Das folgende Beispiel zeigt den Befehl für ein AFF A220 System mit einer VLAN-ID von 120:

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_A -home-node node_A_2 -home-port e0a -address
      10.1.1.2 -netmask 255.255.255.0 -vlan-id 120
      [Job 28] Job succeeded: Interface Create is successful.
      cluster_A::>
      ```

   b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_A_1“:

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
      ```

```
-netmask <netmask>
```

Das folgende Beispiel zeigt die Erstellung der Schnittstelle am Port „e5b“ auf „Node_A_1“ mit der IP-Adresse „10.1.2.1“:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_1 -home-port e5b -address
10.1.2.1 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

Sie können überprüfen, ob diese Schnittstellen mit vorhanden sind `metrocluster configuration-settings interface show` Befehl.

4. Erstellen Sie die Schnittstellen auf Node_A_2.

   a. Konfigurieren Sie die Schnittstelle am Port „e5a“ auf „Node_A_2“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_A_2" mit IP-Adresse "10.1.1.2":

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_A -home-node node_A_2 -home-port e5a -address
   10.1.1.2 -netmask 255.255.255.0
   [Job 28] Job succeeded: Interface Create is successful.
   cluster_A::>
   ```

   b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_A_2“:

   ```
   metrocluster configuration-settings interface create -cluster-name
   <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
   -netmask <netmask>
   ```

   Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf dem Port „e5b“ auf „Node_A_2“ mit der IP-Adresse „10.1.2.2“:

   ```
   cluster_A::> metrocluster configuration-settings interface create
   -cluster-name cluster_A -home-node node_A_2 -home-port e5b -address
   10.1.2.2 -netmask 255.255.255.0
   [Job 28] Job succeeded: Interface Create is successful.
   cluster_A::>
   ```

Bei Plattformmodellen, die VLANs für die MetroCluster IP Schnittstelle unterstützen, können Sie die einschließen `-vlan-id` Parameter, wenn Sie die Standard-VLAN-IDs nicht verwenden möchten. Das folgende Beispiel zeigt den Befehl für ein AFF A220 System mit einer VLAN-ID von 220:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_A -home-node node_A_2 -home-port e0b -address
10.1.2.2 -netmask 255.255.255.0 -vlan-id 220
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

5. Erstellen Sie die Schnittstellen auf „Node_B_1“.

   a. Konfigurieren Sie die Schnittstelle am Port „e5a“ auf „Node_B_1“:

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

      Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_B_1" mit IP-Adresse "10.1.1.3":

      ```
      cluster_A::> metrocluster configuration-settings interface create
      -cluster-name cluster_B -home-node node_B_1 -home-port e5a -address
      10.1.1.3 -netmask 255.255.255.0
      [Job 28] Job succeeded: Interface Create is successful.cluster_B::>
      ```

   b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_B_1“:

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
      -netmask <netmask>
      ```

      Das folgende Beispiel zeigt die Erstellung der Schnittstelle am Port „e5b“ auf „Node_B_1“ mit der IP-Adresse „10.1.2.3“:

```
cluster_A::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_1 -home-port e5b -address
10.1.2.3 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_B::>
```

6. Erstellen Sie die Schnittstellen auf „Node_B_2“.

   a. Konfigurieren Sie die Schnittstelle am Port e5a auf Node_B_2:

      ```
      metrocluster configuration-settings interface create -cluster-name
      <cluster_name> -home-node <node_name> -home-port e5a -address <ip_address>
      -netmask <netmask>
      ```

Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf Port "e5a" auf "Node_B_2" mit IP-Adresse "10.1.1.4":

```
cluster_B::>metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5a -address
10.1.1.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.cluster_A::>
```

b. Konfigurieren Sie die Schnittstelle am Port „e5b“ auf „Node_B_2“:

```
metrocluster configuration-settings interface create -cluster-name
<cluster_name> -home-node <node_name> -home-port e5b -address <ip_address>
-netmask <netmask>
```

Das folgende Beispiel zeigt die Erstellung der Schnittstelle auf dem Port „e5b“ auf „Node_B_2“ mit der IP-Adresse „10.1.2.4“:

```
cluster_B::> metrocluster configuration-settings interface create
-cluster-name cluster_B -home-node node_B_2 -home-port e5b -address
10.1.2.4 -netmask 255.255.255.0
[Job 28] Job succeeded: Interface Create is successful.
cluster_A::>
```

7. Vergewissern Sie sich, dass die Schnittstellen konfiguriert sind:

```
metrocluster configuration-settings interface show
```

Das folgende Beispiel zeigt, dass der Konfigurationsstatus für jede Schnittstelle abgeschlossen ist.

```
cluster_A::> metrocluster configuration-settings interface show
DR                                                                 Config
Group Cluster Node    Network Address Netmask         Gateway   State
----- ------- ------- --------------- --------------- --------- ----------
1     cluster_A  node_A_1
                  Home Port: e5a
                       10.1.1.1     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.1     255.255.255.0   -         completed
                  node_A_2
                  Home Port: e5a
                       10.1.1.2     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.2     255.255.255.0   -         completed
      cluster_B  node_B_1
                  Home Port: e5a
                       10.1.1.3     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.3     255.255.255.0   -         completed
                  node_B_2
                  Home Port: e5a
                       10.1.1.4     255.255.255.0   -         completed
                  Home Port: e5b
                       10.1.2.4     255.255.255.0   -         completed
8 entries were displayed.
cluster_A::>
```

8. Vergewissern Sie sich, dass die Nodes bereit sind, die MetroCluster-Schnittstellen zu verbinden:

   `metrocluster configuration-settings show-status`

   Im folgenden Beispiel werden alle Knoten im Status „bereit für die Verbindung“ angezeigt:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     ready for connection connect
              node_A_2     ready for connection connect
cluster_B
              node_B_1     ready for connection connect
              node_B_2     ready for connection connect
4 entries were displayed.
```

9. Stellen Sie die Verbindungen her: `metrocluster configuration-settings connection connect`

   Wenn Sie eine Version vor ONTAP 9.10.1 ausführen, können die IP-Adressen nach dem Ausführen dieses Befehls nicht geändert werden.

   Im folgenden Beispiel wird gezeigt, dass Cluster_A erfolgreich verbunden ist:

```
cluster_A::> metrocluster configuration-settings connection connect
[Job 53] Job succeeded: Connect is successful.
cluster_A::>
```

10. Stellen Sie sicher, dass die Verbindungen hergestellt wurden:

    `metrocluster configuration-settings show-status`

    Der Status der Konfigurationseinstellungen für alle Knoten sollte abgeschlossen sein:

```
Cluster       Node         Configuration Settings Status
----------    -----------  ---------------------------------
cluster_A
              node_A_1     completed
              node_A_2     completed
cluster_B
              node_B_1     completed
              node_B_2     completed
4 entries were displayed.
```

11. Vergewissern Sie sich, dass die iSCSI-Verbindungen hergestellt sind:

    a. Ändern Sie die erweiterte Berechtigungsebene:

       `set -privilege advanced`

       Sie müssen mit reagieren `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen, wird die Eingabeaufforderung für den erweiterten Modus angezeigt (`*>`).

    b. Anzeigen der Verbindungen:

       `storage iscsi-initiator show`

       Auf Systemen mit ONTAP 9.5 gibt es für jedes Cluster acht MetroCluster-IP-Initiatoren, die in der Ausgabe angezeigt werden sollten.

       Auf Systemen mit ONTAP 9.4 und früheren Versionen gibt es für jedes Cluster vier MetroCluster IP-Initiatoren, die in der Ausgabe angezeigt werden sollten.

       Im folgenden Beispiel werden die acht MetroCluster-IP-Initiatoren auf einem Cluster mit ONTAP 9.5 angezeigt:

```
cluster_A::*> storage iscsi-initiator show
Node Type Label    Target Portal           Target Name
Admin/Op
---- ---- -------- ------------------
-------------------------------- --------

cluster_A-01
     dr_auxiliary
               mccip-aux-a-initiator
                    10.227.16.113:65200     prod506.com.company:abab44
up/up
               mccip-aux-a-initiator2
                    10.227.16.113:65200     prod507.com.company:abab44
up/up
               mccip-aux-b-initiator
                    10.227.95.166:65200     prod506.com.company:abab44
up/up
               mccip-aux-b-initiator2
                    10.227.95.166:65200     prod507.com.company:abab44
up/up
     dr_partner
               mccip-pri-a-initiator
                    10.227.16.112:65200     prod506.com.company:cdcd88
up/up
               mccip-pri-a-initiator2
                    10.227.16.112:65200     prod507.com.company:cdcd88
up/up
               mccip-pri-b-initiator
                    10.227.95.165:65200     prod506.com.company:cdcd88
up/up
               mccip-pri-b-initiator2
                    10.227.95.165:65200     prod507.com.company:cdcd88
up/up
cluster_A-02
     dr_auxiliary
               mccip-aux-a-initiator
                    10.227.16.112:65200     prod506.com.company:cdcd88
up/up
               mccip-aux-a-initiator2
                    10.227.16.112:65200     prod507.com.company:cdcd88
up/up
               mccip-aux-b-initiator
                    10.227.95.165:65200     prod506.com.company:cdcd88
up/up
               mccip-aux-b-initiator2
```

```
                    10.227.95.165:65200     prod507.com.company:cdcd88
up/up
     dr_partner
               mccip-pri-a-initiator
                    10.227.16.113:65200     prod506.com.company:abab44
up/up
               mccip-pri-a-initiator2
                    10.227.16.113:65200     prod507.com.company:abab44
up/up
               mccip-pri-b-initiator
                    10.227.95.166:65200     prod506.com.company:abab44
up/up
               mccip-pri-b-initiator2
                    10.227.95.166:65200     prod507.com.company:abab44
up/up
16 entries were displayed.
```

a. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

12. Vergewissern Sie sich, dass die Knoten bereit sind für die abschließende Implementierung der MetroCluster Konfiguration:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- --------- ----
-     cluster_A
              node_A_1          ready to configure -     -
              node_A_2          ready to configure -     -
2 entries were displayed.
cluster_A::>
```

```
cluster_B::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- --------- ----
-     cluster_B
              node_B_1          ready to configure -     -
              node_B_2          ready to configure -     -
2 entries were displayed.
cluster_B::>
```

Überprüfen oder manuelles Durchführen der Zuweisung von Pool-1-Laufwerken

Je nach Storage-Konfiguration müssen Sie für jeden Node der MetroCluster IP-Konfiguration entweder die Laufwerkszuweisung Pool 1 überprüfen oder Laufwerken manuell Pool 1 zuweisen. Das von Ihnen verwendete Verfahren hängt von der Version von ONTAP ab.

Konfigurationstyp	Verfahren
Die Systeme erfüllen die Anforderungen für die automatische Laufwerkszuweisung oder wurden bei Verwendung von ONTAP 9.3 vom Werk empfangen.	Überprüfen der Festplattenzuordnung für Pool 1-Festplatten
Die Konfiguration umfasst drei oder, wenn sie mehr als vier Shelfs enthält, besteht aus einem ungleichen Vielfaches von vier Shelfs (z. B. sieben Shelfs) und läuft mit ONTAP 9.5.	Manuelles Zuweisen von Laufwerken für Pool 1 (ONTAP 9.4 oder höher)
Die Konfiguration umfasst nicht vier Storage Shelfs pro Standort und läuft mit ONTAP 9.4	Manuelles Zuweisen von Laufwerken für Pool 1 (ONTAP 9.4 oder höher)
Die Systeme wurden nicht ab Werk empfangen und führen ONTAP 9.3Systeme aus, die von der Fabrik empfangen wurden, sind mit zugewiesenen Laufwerken vorkonfiguriert.	Manuelles Zuweisen von Disketten für Pool 1 (ONTAP 9.3)

Überprüfen der Festplattenzuordnung für Pool 1-Festplatten

Sie müssen überprüfen, ob die Remote-Festplatten für die Knoten sichtbar sind und ordnungsgemäß zugewiesen wurden.

Bevor Sie beginnen

Sie müssen mindestens zehn Minuten warten, bis die automatische Zuweisung von Laufwerken abgeschlossen ist, nachdem die MetroCluster-IP-Schnittstellen und -Verbindungen mit dem erstellt wurden `metrocluster configuration-settings connection connect` Befehl.

Befehlsausgabe zeigt Festplattennamen in Form an: Node-Name:0m.i1.0L1

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Vergewissern Sie sich, dass Pool 1-Festplatten automatisch zugewiesen sind:

   ```
   disk show
   ```

   Die folgende Ausgabe zeigt die Ausgabe eines AFF A800 Systems ohne externe Shelfs.

   Die automatische Laufwerkszuweisung hat einem Viertel (8 Laufwerke) zu „Node_A_1“ und einem Viertel zu „Node_A_2“ zugewiesen. Die übrigen Laufwerke sind Remote-Festplatten (Pool 1) für „Node_B_1“ und „Node_B_2“.

   ```
   cluster_B::> disk show -host-adapter 0m -owner node_B_2
                        Usable     Disk              Container   Container
   Disk                 Size       Shelf Bay Type    Type        Name
   Owner
   ----------------     ---------- ----- --- ------- ----------- ---------
   --------
   node_B_2:0m.i0.2L4   894.0GB    0     29  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.2L10 894.0GB    0     25  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L3   894.0GB    0     28  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L9   894.0GB    0     24  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L11 894.0GB    0     26  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L12 894.0GB    0     27  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L15 894.0GB    0     30  SSD-NVM shared      -
   node_B_2
   node_B_2:0m.i0.3L16 894.0GB    0     31  SSD-NVM shared      -
   node_B_2
   8 entries were displayed.

   cluster_B::> disk show -host-adapter 0m -owner node_B_1
                        Usable     Disk              Container   Container
   Disk                 Size       Shelf Bay Type    Type        Name
   Owner
   ----------------     ---------- ----- --- ------- ----------- ---------
   --------
   node_B_1:0m.i2.3L19 1.75TB     0     42  SSD-NVM shared      -
   node_B_1
   node_B_1:0m.i2.3L20 1.75TB     0     43  SSD-NVM spare       Pool1
   node_B_1
   node_B_1:0m.i2.3L23 1.75TB     0     40  SSD-NVM shared       -
   node_B_1
   ```

```
node_B_1:0m.i2.3L24 1.75TB     0     41  SSD-NVM spare       Pool1
node_B_1
node_B_1:0m.i2.3L29 1.75TB     0     36  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L30 1.75TB     0     37  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L31 1.75TB     0     38  SSD-NVM shared       -
node_B_1
node_B_1:0m.i2.3L32 1.75TB     0     39  SSD-NVM shared       -
node_B_1
8 entries were displayed.

cluster_B::> disk show
                    Usable     Disk              Container   Container
Disk                Size       Shelf Bay Type    Type        Name
Owner
----------------    ---------- ----- --- ------- ----------- ---------
--------
node_B_1:0m.i1.0L6  1.75TB     0     1   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L8  1.75TB     0     3   SSD-NVM shared      -
node_A_2
node_B_1:0m.i1.0L17 1.75TB     0     18  SSD-NVM shared      -
node_A_1
node_B_1:0m.i1.0L22 1.75TB     0     17 SSD-NVM shared - node_A_1
node_B_1:0m.i1.0L25 1.75TB     0     12 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L2  1.75TB     0     5 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L7  1.75TB     0     2 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L14 1.75TB     0     7 SSD-NVM shared - node_A_2
node_B_1:0m.i1.2L21 1.75TB     0     16 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L27 1.75TB     0     14 SSD-NVM shared - node_A_1
node_B_1:0m.i1.2L28 1.75TB     0     15 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L1  1.75TB     0     4 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L5  1.75TB     0     0 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L13 1.75TB     0     6 SSD-NVM shared - node_A_2
node_B_1:0m.i2.1L18 1.75TB     0     19 SSD-NVM shared - node_A_1
node_B_1:0m.i2.1L26 1.75TB     0     13 SSD-NVM shared - node_A_1
node_B_1:0m.i2.3L19 1.75TB     0 42 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L20 1.75TB     0 43 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L23 1.75TB     0 40 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L24 1.75TB     0 41 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L29 1.75TB     0 36 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L30 1.75TB     0 37 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L31 1.75TB     0 38 SSD-NVM shared - node_B_1
node_B_1:0m.i2.3L32 1.75TB     0 39 SSD-NVM shared - node_B_1
node_B_1:0n.12      1.75TB     0 12 SSD-NVM shared aggr0 node_B_1
```

```
node_B_1:0n.13      1.75TB     0 13 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.14      1.75TB     0 14 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.15      1.75TB 0 15 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.16      1.75TB 0 16 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.17      1.75TB 0 17 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.18      1.75TB 0 18 SSD-NVM shared aggr0 node_B_1
node_B_1:0n.19      1.75TB 0 19 SSD-NVM shared - node_B_1
node_B_1:0n.24      894.0GB 0 24 SSD-NVM shared - node_A_2
node_B_1:0n.25      894.0GB 0 25 SSD-NVM shared - node_A_2
node_B_1:0n.26      894.0GB 0 26 SSD-NVM shared - node_A_2
node_B_1:0n.27      894.0GB 0 27 SSD-NVM shared - node_A_2
node_B_1:0n.28      894.0GB 0 28 SSD-NVM shared - node_A_2
node_B_1:0n.29      894.0GB 0 29 SSD-NVM shared - node_A_2
node_B_1:0n.30      894.0GB 0 30 SSD-NVM shared - node_A_2
node_B_1:0n.31      894.0GB 0 31 SSD-NVM shared - node_A_2
node_B_1:0n.36      1.75TB 0 36 SSD-NVM shared - node_A_1
node_B_1:0n.37      1.75TB 0 37 SSD-NVM shared - node_A_1
node_B_1:0n.38      1.75TB 0 38 SSD-NVM shared - node_A_1
node_B_1:0n.39      1.75TB 0 39 SSD-NVM shared - node_A_1
node_B_1:0n.40      1.75TB 0 40 SSD-NVM shared - node_A_1
node_B_1:0n.41      1.75TB 0 41 SSD-NVM shared - node_A_1
node_B_1:0n.42      1.75TB 0 42 SSD-NVM shared - node_A_1
node_B_1:0n.43      1.75TB 0 43 SSD-NVM shared - node_A_1
node_B_2:0m.i0.2L4  894.0GB 0 29 SSD-NVM shared - node_B_2
node_B_2:0m.i0.2L10 894.0GB 0 25 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L3  894.0GB 0 28 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L9  894.0GB 0 24 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L11 894.0GB 0 26 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L12 894.0GB 0 27 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L15 894.0GB 0 30 SSD-NVM shared - node_B_2
node_B_2:0m.i0.3L16 894.0GB 0 31 SSD-NVM shared - node_B_2
node_B_2:0n.0       1.75TB 0 0 SSD-NVM shared aggr0_rha12_b1_cm_02_0
node_B_2
node_B_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_rha12_b1_cm_02_0 node_B_2
node_B_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_B_2
64 entries were displayed.

cluster_B::>


cluster_A::> disk show
```

```
Usable Disk Container Container
Disk Size Shelf Bay Type Type Name Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_1:0m.i1.0L2 1.75TB 0 5 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L8 1.75TB 0 3 SSD-NVM shared - node_B_2
node_A_1:0m.i1.0L18 1.75TB 0 19 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L25 1.75TB 0 12 SSD-NVM shared - node_B_1
node_A_1:0m.i1.0L27 1.75TB 0 14 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L1 1.75TB 0 4 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L6 1.75TB 0 1 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L7 1.75TB 0 2 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L14 1.75TB 0 7 SSD-NVM shared - node_B_2
node_A_1:0m.i1.2L17 1.75TB 0 18 SSD-NVM shared - node_B_1
node_A_1:0m.i1.2L22 1.75TB 0 17 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L5 1.75TB 0 0 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L13 1.75TB 0 6 SSD-NVM shared - node_B_2
node_A_1:0m.i2.1L21 1.75TB 0 16 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L26 1.75TB 0 13 SSD-NVM shared - node_B_1
node_A_1:0m.i2.1L28 1.75TB 0 15 SSD-NVM shared - node_B_1
node_A_1:0m.i2.3L19 1.75TB 0 42 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L20 1.75TB 0 43 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L23 1.75TB 0 40 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L24 1.75TB 0 41 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L29 1.75TB 0 36 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L30 1.75TB 0 37 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L31 1.75TB 0 38 SSD-NVM shared - node_A_1
node_A_1:0m.i2.3L32 1.75TB 0 39 SSD-NVM shared - node_A_1
node_A_1:0n.12 1.75TB 0 12 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.13 1.75TB 0 13 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.14 1.75TB 0 14 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.15 1.75TB 0 15 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.16 1.75TB 0 16 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.17 1.75TB 0 17 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.18 1.75TB 0 18 SSD-NVM shared aggr0 node_A_1
node_A_1:0n.19 1.75TB 0 19 SSD-NVM shared - node_A_1
node_A_1:0n.24 894.0GB 0 24 SSD-NVM shared - node_B_2
node_A_1:0n.25 894.0GB 0 25 SSD-NVM shared - node_B_2
node_A_1:0n.26 894.0GB 0 26 SSD-NVM shared - node_B_2
node_A_1:0n.27 894.0GB 0 27 SSD-NVM shared - node_B_2
node_A_1:0n.28 894.0GB 0 28 SSD-NVM shared - node_B_2
node_A_1:0n.29 894.0GB 0 29 SSD-NVM shared - node_B_2
node_A_1:0n.30 894.0GB 0 30 SSD-NVM shared - node_B_2
node_A_1:0n.31 894.0GB 0 31 SSD-NVM shared - node_B_2
node_A_1:0n.36 1.75TB 0 36 SSD-NVM shared - node_B_1
node_A_1:0n.37 1.75TB 0 37 SSD-NVM shared - node_B_1
```

```
node_A_1:0n.38 1.75TB 0 38 SSD-NVM shared - node_B_1
node_A_1:0n.39 1.75TB 0 39 SSD-NVM shared - node_B_1
node_A_1:0n.40 1.75TB 0 40 SSD-NVM shared - node_B_1
node_A_1:0n.41 1.75TB 0 41 SSD-NVM shared - node_B_1
node_A_1:0n.42 1.75TB 0 42 SSD-NVM shared - node_B_1
node_A_1:0n.43 1.75TB 0 43 SSD-NVM shared - node_B_1
node_A_2:0m.i2.3L3 894.0GB 0 28 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L4 894.0GB 0 29 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L9 894.0GB 0 24 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L10 894.0GB 0 25 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L11 894.0GB 0 26 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L12 894.0GB 0 27 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L15 894.0GB 0 30 SSD-NVM shared - node_A_2
node_A_2:0m.i2.3L16 894.0GB 0 31 SSD-NVM shared - node_A_2
node_A_2:0n.0 1.75TB 0 0 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.1 1.75TB 0 1 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.2 1.75TB 0 2 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.3 1.75TB 0 3 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.4 1.75TB 0 4 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.5 1.75TB 0 5 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.6 1.75TB 0 6 SSD-NVM shared aggr0_node_A_2_0 node_A_2
node_A_2:0n.7 1.75TB 0 7 SSD-NVM shared - node_A_2
64 entries were displayed.

cluster_A::>
```

Manuelles Zuweisen von Laufwerken für Pool 1 (ONTAP 9.4 oder höher)

Wenn das System werkseitig nicht vorkonfiguriert war und die Anforderungen für die automatische Laufwerkszuweisung nicht erfüllt, müssen Sie die Remote Pool 1-Laufwerke manuell zuweisen.

Über diese Aufgabe

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.4 oder höher.

Weitere Informationen zur Bestimmung, ob Ihr System eine manuelle Festplattenzuordnung erfordert, finden Sie in "Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher".

Wenn die Konfiguration nur zwei externe Shelfs pro Standort umfasst, sollten 1 Laufwerke für jeden Standort aus demselben Shelf gemeinsam genutzt werden, wie in den folgenden Beispielen dargestellt:

- Node_A_1 wird Laufwerken in Einschüben 0-11 an Standort_B-Shelf_2 (Remote) zugewiesen
- Node_A_2 wird Laufwerken in Einschüben 12-23 an Standort_B-Shelf_2 (Remote) zugewiesen

Schritte

1. Weisen Sie auf jedem Knoten in der MetroCluster IP-Konfiguration Remote-Laufwerke Pool 1 zu.

   a. Zeigt die Liste der nicht zugewiesenen Laufwerke an:

```
disk show -host-adapter 0m -container-type unassigned
```

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

b. Weisen Sie dem Pool 1 des ersten Knotens (z. B. Node_A_1) die Eigentümerschaft von Remote-Laufwerken (0m) zu:

```
disk assign -disk <disk-id> -pool 1 -owner <owner_node_name>
```

`disk-id` Muss ein Laufwerk auf einem Remote-Shelf von identifizieren `owner_node_name`.

c. Vergewissern Sie sich, dass die Laufwerke Pool 1 zugewiesen wurden:

```
disk show -host-adapter 0m -container-type unassigned
```

> Die iSCSI-Verbindung, die zum Zugriff auf die Remote-Laufwerke verwendet wird, wird als Gerät 0 m angezeigt.

Die folgende Ausgabe zeigt, dass die Laufwerke in Shelf 23 zugewiesen wurden, da sie in der Liste der nicht zugewiesenen Laufwerke nicht mehr angezeigt werden:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Wiederholen Sie diese Schritte, um dem zweiten Node an Standort A Pool 1-Laufwerke zuzuweisen (z. B. „Node_A_2“).

b. Wiederholen Sie diese Schritte vor Ort B.

Manuelles Zuweisen von Disketten für Pool 1 (ONTAP 9.3)

Wenn Sie für jeden Node mindestens zwei Festplatten-Shelfs haben, können Sie die Remote-Festplatten (Pool1) über die automatische Zuweisungsfunktion von ONTAP automatisch zuweisen.

Bevor Sie beginnen

Sie müssen zuerst eine Festplatte im Shelf Pool 1 zuweisen. ONTAP weist dann automatisch den Rest der Festplatten im Shelf demselben Pool zu.

Über diese Aufgabe

Dieses Verfahren gilt für Konfigurationen mit ONTAP 9.3.

Diese Vorgehensweise kann nur verwendet werden, wenn mindestens zwei Festplatten-Shelfs für jeden Node vorhanden sind, wodurch die automatische Zuweisung von Festplatten auf Shelf-Ebene ermöglicht wird.

Wenn Sie die automatische Zuweisung auf Shelf-Ebene nicht verwenden können, müssen Sie die Remote-Festplatten manuell zuweisen, damit jeder Node über einen Remote-Pool von Festplatten (Pool 1) verfügt.

Die Funktion für die automatische Festplattenzuweisung von ONTAP weist die Festplatten für das Shelf zu. Beispiel:

- Alle Festplatten auf Site_B-Shelf_2 werden dem Pool1 von Node_A_1 automatisch zugewiesen
- Alle Festplatten auf Site_B-Shelf_4 werden dem Pool1 der Node_A_2 automatisch zugewiesen
- Alle Festplatten auf Site_A-Shelf_2 werden dem Pool1 der Node_B_1 automatisch zugewiesen
- Alle Festplatten auf Site_A-Shelf_4 werden dem Pool1 der Node_B_2 automatisch zugewiesen

Sie müssen die automatische Zuweisung durch Angabe einer einzelnen Festplatte für jedes Shelf „Seeding“:

Schritte

1. Weisen Sie von jedem Knoten in der MetroCluster IP-Konfiguration einem Pool 1 eine Remote-Festplatte zu.

   a. Zeigen Sie die Liste der nicht zugewiesenen Festplatten an:

      `disk show -host-adapter 0m -container-type unassigned`

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
6.23.0                    -    23   0 SSD     unassigned  -         -
6.23.1                    -    23   1 SSD     unassigned  -         -
.
.
.
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
.
.
.
48 entries were displayed.

cluster_A::>
```

   b. Wählen Sie ein Remote-Laufwerk (0m) aus, und weisen Sie dem Pool 1 des ersten Knotens (z. B. „Node_A_1“) den Besitz der Festplatte zu:

      `disk assign -disk <disk_id> -pool 1 -owner <owner_node_name>`

      Das `disk-id` muss eine Festplatte in einem Remote-Shelf von identifizieren `owner_node_name`.

      Die automatische Zuweisung von ONTAP-Festplatten weist alle Festplatten im Remote-Shelf zu, das die angegebene Festplatte enthält.

   c. Nachdem Sie mindestens 60 Sekunden gewartet haben, bis die automatische Zuweisung der Festplatte erfolgt ist, vergewissern Sie sich, dass die Remote-Festplatten auf dem Shelf Pool 1 automatisch zugewiesen wurden:

      `disk show -host-adapter 0m -container-type unassigned`

      > Die iSCSI-Verbindung, die zum Zugriff auf die Remote-Festplatten verwendet wird, wird als Gerät 0 m angezeigt.

      Die folgende Ausgabe zeigt, dass die Festplatten in Shelf 23 nun zugewiesen sind und nicht mehr angezeigt werden:

```
cluster_A::> disk show -host-adapter 0m -container-type unassigned
                     Usable           Disk    Container   Container
Disk                   Size Shelf Bay Type    Type        Name
Owner
---------------- ---------- ----- --- ------- ----------- ---------
--------
node_A_2:0m.i1.2L51       -    21  14 SSD     unassigned  -         -
node_A_2:0m.i1.2L64       -    21  10 SSD     unassigned  -         -
node_A_2:0m.i1.2L72       -    21  23 SSD     unassigned  -         -
node_A_2:0m.i1.2L74       -    21   1 SSD     unassigned  -         -
node_A_2:0m.i1.2L83       -    21  22 SSD     unassigned  -         -
node_A_2:0m.i1.2L90       -    21   7 SSD     unassigned  -         -
node_A_2:0m.i1.3L52       -    21   6 SSD     unassigned  -         -
node_A_2:0m.i1.3L59       -    21  13 SSD     unassigned  -         -
node_A_2:0m.i1.3L66       -    21  17 SSD     unassigned  -         -
node_A_2:0m.i1.3L73       -    21  12 SSD     unassigned  -         -
node_A_2:0m.i1.3L80       -    21   5 SSD     unassigned  -         -
node_A_2:0m.i1.3L81       -    21   2 SSD     unassigned  -         -
node_A_2:0m.i1.3L82       -    21  16 SSD     unassigned  -         -
node_A_2:0m.i1.3L91       -    21   3 SSD     unassigned  -         -
node_A_2:0m.i2.0L49       -    21  15 SSD     unassigned  -         -
node_A_2:0m.i2.0L50       -    21   4 SSD     unassigned  -         -
node_A_2:0m.i2.1L57       -    21  18 SSD     unassigned  -         -
node_A_2:0m.i2.1L58       -    21  11 SSD     unassigned  -         -
node_A_2:0m.i2.1L59       -    21  21 SSD     unassigned  -         -
node_A_2:0m.i2.1L65       -    21  20 SSD     unassigned  -         -
node_A_2:0m.i2.1L72       -    21   9 SSD     unassigned  -         -
node_A_2:0m.i2.1L80       -    21   0 SSD     unassigned  -         -
node_A_2:0m.i2.1L88       -    21   8 SSD     unassigned  -         -
node_A_2:0m.i2.1L90       -    21  19 SSD     unassigned  -         -
24 entries were displayed.

cluster_A::>
```

a. Wiederholen Sie diese Schritte, um Pool 1-Festplatten dem zweiten Knoten an Standort A zuzuweisen (z. B. „Node_A_2“).

b. Wiederholen Sie diese Schritte vor Ort B.

Aktivieren der automatischen Laufwerkszuweisung in ONTAP 9.4

Über diese Aufgabe

Wenn Sie in ONTAP 9.4 die automatische Laufwerkszuweisung wie zuvor in diesem Verfahren beschrieben deaktiviert haben, müssen Sie sie auf allen Knoten erneut aktivieren.

"Überlegungen zur automatischen Laufwerkszuweisung und zu ADP-Systemen in ONTAP 9.4 und höher"

Schritte

1. Automatische Laufwerkszuweisung aktivieren:

   ```
   storage disk option modify -node <node_name> -autoassign on
   ```

   Sie müssen diesen Befehl für alle Nodes in der MetroCluster IP-Konfiguration ausgeben.

Spiegelung der Root-Aggregate

Um Datensicherung zu ermöglichen, müssen Sie die Root-Aggregate spiegeln.

Über diese Aufgabe

Standardmäßig wird das Root-Aggregat als RAID-DP Typ Aggregat erstellt. Sie können das Root-Aggregat von RAID-DP zu einem Aggregat des RAID4-Typs ändern. Mit dem folgenden Befehl wird das Root-Aggregat für das RAID4-Typ-Aggregat modifiziert:

```
storage aggregate modify –aggregate <aggr_name> -raidtype raid4
```

Auf Systemen anderer Hersteller kann der RAID-Typ des Aggregats von dem Standard RAID-DP zu RAID4 vor oder nach der Spiegelung des Aggregats geändert werden.

Schritte

1. Root-Aggregat spiegeln:

   ```
   storage aggregate mirror <aggr_name>
   ```

   Der folgende Befehl spiegelt das Root-Aggregat für „Controller_A_1“:

   ```
   controller_A_1::> storage aggregate mirror aggr0_controller_A_1
   ```

   Dies spiegelt das Aggregat, also besteht es aus einem lokalen Plex und einem Remote Plex am Remote MetroCluster Standort.

2. Wiederholen Sie den vorherigen Schritt für jeden Node in der MetroCluster-Konfiguration.

Verwandte Informationen

"Logisches Storage-Management"

Erstellung eines gespiegelten Datenaggregats auf jedem Node

Sie müssen auf jedem Knoten in der DR-Gruppe ein gespiegeltes Datenaggregat erstellen.

Über diese Aufgabe

- Sie sollten wissen, welche Laufwerke in dem neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie sicherstellen können, dass der richtige Laufwerkstyp ausgewählt ist.
- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.

In Systemen mit ADP werden Aggregate mithilfe von Partitionen erstellt, in denen jedes Laufwerk in die Partitionen P1, P2 und P3 partitioniert wird.

- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.

  "Festplatten- und Aggregatmanagement"

Schritte

1. Liste der verfügbaren Ersatzteile anzeigen:

   ```
   storage disk show -spare -owner <node_name>
   ```

2. Erstellen Sie das Aggregat:

   ```
   storage aggregate create -mirror true
   ```

   Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um sicherzustellen, dass das Aggregat auf einem bestimmten Node erstellt wird, verwenden Sie die `-node` Parameter oder geben Sie Laufwerke an, die diesem Node gehören.

   Sie können die folgenden Optionen angeben:

   - Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
   - Liste spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke

     In der unterstützten Minimalkonfiguration, bei der eine begrenzte Anzahl an Laufwerken verfügbar ist, müssen Sie die Force-Small-Aggregate Option verwenden, um das Erstellen eines drei Festplatten-RAID-DP Aggregats zu ermöglichen.

   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Unabhängig davon, ob Laufwerke mit unterschiedlichen RPM zugelassen sind, finden Sie auf der man Page zum Erstellen von Storage-Aggregaten.

     Mit dem folgenden Befehl wird ein gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
cluster_A::> storage aggregate create aggr1_node_A_1 -diskcount 10 -node
node_A_1 -mirror true
[Job 15] Job is queued: Create aggr1_node_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

3. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   `storage aggregate show-status -aggregate <aggregate-name>`

Implementieren der MetroCluster-Konfiguration

Sie müssen den ausführen `metrocluster configure` Befehl zum Starten der Datensicherung in einer MetroCluster-Konfiguration.

Über diese Aufgabe

- Es sollten mindestens zwei gespiegelte Datenaggregate ohne Root-Wurzeln auf jedem Cluster vorhanden sein.

  Sie können dies mit dem überprüfen `storage aggregate show` Befehl.

  Wenn Sie ein einzelnes gespiegeltes Datenaggregat verwenden möchten, finden Sie weitere Informationen unter Schritt 1 Weitere Anweisungen.

- Der HA-Konfigurationsstatus der Controller und des Chassis muss „mccip“ sein.

Sie stellen das aus `metrocluster configure` Aktivieren Sie einmal den Befehl auf einem der Nodes, um die MetroCluster-Konfiguration zu aktivieren. Sie müssen den Befehl nicht für jede der Standorte oder Nodes ausführen. Es ist nicht von Bedeutung, auf welchem Node oder Standort Sie den Befehl ausgeben möchten.

Der `metrocluster configure` Befehl koppelt die beiden Nodes automatisch mit den niedrigsten System-IDs in jedem der beiden Cluster als Disaster Recovery (DR) Partner. In einer MetroCluster Konfiguration mit vier Nodes gibt es zwei DR-Partnerpaare. Das zweite DR-Paar wird aus den beiden Knoten mit höheren System-IDs erstellt.

Sie müssen vor Ausführung des Befehls * Onboard Key Manager (OKM) oder externe Schlüsselverwaltung nicht konfigurieren `metrocluster configure`.

Schritte

1. Konfigurieren Sie die MetroCluster im folgenden Format:

Wenn Ihre MetroCluster Konfiguration…	Dann tun Sie das…
Mehrere Datenaggregate	Konfigurieren Sie an der Eingabeaufforderung eines beliebigen Nodes MetroCluster: `metrocluster configure <node_name>`

Ein einzelnes gespiegeltes Datenaggregat	a. Ändern Sie von der Eingabeaufforderung eines beliebigen Node auf die erweiterte Berechtigungsebene:
	
	`set -privilege advanced`
	
	Sie müssen mit reagieren `y` Wenn Sie aufgefordert werden, den erweiterten Modus fortzusetzen, wird die Eingabeaufforderung für den erweiterten Modus (*>) angezeigt.
	
	b. Konfigurieren Sie die MetroCluster mit dem `-allow-with-one-aggregate true` Parameter:
	
	`metrocluster configure -allow-with -one-aggregate true <node_name>`
	
	c. Zurück zur Administratorberechtigungsebene:
	
	`set -privilege admin`

Die Best Practice besteht in der Nutzung mehrerer Datenaggregate. Wenn die erste DR-Gruppe nur ein Aggregat hat und Sie eine DR-Gruppe mit einem Aggregat hinzufügen möchten, müssen Sie das Metadaten-Volume aus dem einzelnen Datenaggregat verschieben. Weitere Informationen zu diesem Verfahren finden Sie unter "Verschieben eines Metadaten-Volumes in MetroCluster Konfigurationen".

Mit dem folgenden Befehl wird die MetroCluster-Konfiguration auf allen Knoten in der DR-Gruppe aktiviert, die „Controller_A_1“ enthält:

```
cluster_A::*> metrocluster configure -node-name controller_A_1

[Job 121] Job succeeded: Configure is successful.
```

2. Überprüfen Sie den Netzwerkstatus auf Standort A:

   `network port show`

   Im folgenden Beispiel wird die Verwendung von Netzwerkports in einer MetroCluster Konfiguration mit vier Nodes angezeigt:

```
cluster_A::> network port show
                                                                 Speed (Mbps)
Node   Port      IPspace   Broadcast Domain Link   MTU    Admin/Oper
------ --------- --------- ---------------- ----- ------- ------------
controller_A_1
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
controller_A_2
       e0a       Cluster   Cluster          up     9000  auto/1000
       e0b       Cluster   Cluster          up     9000  auto/1000
       e0c       Default   Default          up     1500  auto/1000
       e0d       Default   Default          up     1500  auto/1000
       e0e       Default   Default          up     1500  auto/1000
       e0f       Default   Default          up     1500  auto/1000
       e0g       Default   Default          up     1500  auto/1000
14 entries were displayed.
```

3. Überprüfen Sie die MetroCluster Konfiguration von beiden Standorten in der MetroCluster Konfiguration.

   a. Überprüfen Sie die Konfiguration von Standort A:

      `metrocluster show`

      ```
      cluster_A::> metrocluster show

      Configuration: IP fabric

      Cluster                   Entry Name          State
      ------------------------- ------------------- -----------
       Local: cluster_A         Configuration state configured
                                Mode                normal
      Remote: cluster_B         Configuration state configured
                                Mode                normal
      ```

   b. Überprüfen Sie die Konfiguration von Standort B:

      `metrocluster show`

```
cluster_B::> metrocluster show

Configuration: IP fabric

Cluster                   Entry Name          State
------------------------- ------------------- -----------
 Local: cluster_B         Configuration state configured
                          Mode                normal
Remote: cluster_A         Configuration state configured
                          Mode                normal
```

4. Um mögliche Probleme bei der nicht-flüchtigen Speicherspiegelung zu vermeiden, müssen Sie jeden der vier Nodes neu booten:

   `node reboot -node <node_name> -inhibit-takeover true`

5. Stellen Sie das aus `metrocluster show` Befehl auf beiden Clustern, um die Konfiguration erneut zu überprüfen.

Konfigurieren der zweiten DR-Gruppe in einer Konfiguration mit acht Nodes

Wiederholen Sie die vorherigen Aufgaben, um die Nodes in der zweiten DR-Gruppe zu konfigurieren.

Erstellen von nicht gespiegelten Datenaggregaten

Optional können Sie nicht gespiegelte Datenaggregate für Daten erstellen, für die keine redundante Spiegelung von MetroCluster-Konfigurationen erforderlich ist.

Über diese Aufgabe

- Stellen Sie sicher, dass Sie wissen, welche Laufwerke im neuen Aggregat verwendet werden.
- Wenn Sie mehrere Laufwerktypen in Ihrem System haben (heterogener Speicher), sollten Sie verstehen, wie Sie überprüfen können, ob der richtige Laufwerkstyp ausgewählt ist.

> In MetroCluster IP-Konfigurationen können Remote-Aggregate nach einem Switchover nicht zugänglich gemacht werden

> Die nicht gespiegelten Aggregate müssen sich lokal an dem Node halten, auf dem sie sich enthalten.

- Laufwerke sind Eigentum eines bestimmten Nodes. Wenn Sie ein Aggregat erstellen, müssen alle Laufwerke in diesem Aggregat im Besitz desselben Nodes sein, der zum Home-Node für das Aggregat wird.
- Aggregatnamen sollten dem Benennungsschema entsprechen, das Sie beim Planen Ihrer MetroCluster-Konfiguration ermittelt haben.
- *Festplatten- und Aggregatmanagement* enthält weitere Informationen zur Spiegelung von Aggregaten.

Schritte

1. Implementierung von nicht gespiegelten Aggregaten:

```
metrocluster modify -enable-unmirrored-aggr-deployment true
```

2. Vergewissern Sie sich, dass die automatische Festplattenzuordnung deaktiviert ist:

   ```
   disk option show
   ```

3. Installieren und verkabeln Sie die Festplatten-Shelfs, die die nicht gespiegelten Aggregate enthalten.

   Sie können die Verfahren in der Dokumentation Installation und Setup für Ihre Plattform und Platten-Shelfs verwenden.

   "Dokumentation zu ONTAP Hardwaresystemen"

4. Weisen Sie alle Festplatten auf dem neuen Shelf dem entsprechenden Node manuell zu:

   ```
   disk assign -disk <disk_id> -owner <owner_node_name>
   ```

5. Erstellen Sie das Aggregat:

   ```
   storage aggregate create
   ```

   Wenn Sie auf der Cluster-Managementoberfläche beim Cluster angemeldet sind, können Sie auf jedem Node im Cluster ein Aggregat erstellen. Um zu überprüfen, ob das Aggregat auf einem bestimmten Node erstellt wird, sollten Sie den Parameter -Node verwenden oder Laufwerke angeben, die Eigentum dieses Node sind.

   Darüber hinaus müssen Sie sicherstellen, dass Sie nur Laufwerke in das nicht gespiegelte Shelf zum Aggregat aufnehmen.

   Sie können die folgenden Optionen angeben:

   - Der Home Node des Aggregats (d. h. der Knoten, der das Aggregat im normalen Betrieb besitzt)
   - Liste spezifischer Laufwerke, die dem Aggregat hinzugefügt werden sollen
   - Anzahl der zu einführenden Laufwerke
   - Prüfsummenstil, den Sie für das Aggregat verwenden möchten
   - Typ der zu verwendenden Laufwerke
   - Die Größe der zu verwendenden Laufwerke
   - Fahrgeschwindigkeit zu verwenden
   - RAID-Typ für RAID-Gruppen auf dem Aggregat
   - Maximale Anzahl an Laufwerken, die in eine RAID-Gruppe aufgenommen werden können
   - Gibt an, ob Laufwerke mit unterschiedlichen U/min zulässig sind

     Weitere Informationen zu diesen Optionen finden Sie auf der „Storage Aggregate create man page“.

     Mit dem folgenden Befehl wird ein nicht gespiegeltes Aggregat mit 10 Festplatten erstellt:

```
controller_A_1::> storage aggregate create aggr1_controller_A_1
-diskcount 10 -node controller_A_1
[Job 15] Job is queued: Create aggr1_controller_A_1.
[Job 15] The job is starting.
[Job 15] Job succeeded: DONE
```

6. Überprüfen Sie die RAID-Gruppe und die Laufwerke Ihres neuen Aggregats:

   ```
   storage aggregate show-status -aggregate <aggregate_name>
   ```

7. Deaktivieren der Implementierung nicht gespiegelter Aggregate

   ```
   metrocluster modify -enable-unmirrored-aggr-deployment false
   ```

8. Vergewissern Sie sich, dass die automatische Festplattenzuordnung aktiviert ist:

   ```
   disk option show
   ```

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

Überprüfen der MetroCluster-Konfiguration

Sie können überprüfen, ob die Komponenten und Beziehungen in der MetroCluster Konfiguration ordnungsgemäß funktionieren.

Über diese Aufgabe

Nach der Erstkonfiguration und nach sämtlichen Änderungen an der MetroCluster-Konfiguration sollten Sie einen Check durchführen.

Sie sollten auch vor einer ausgehandelten (geplanten) Umschaltung oder einem Switchback prüfen.

Wenn der `metrocluster check run` Befehl wird zweimal innerhalb kürzester Zeit auf einem oder beiden Clustern ausgegeben. Ein Konflikt kann auftreten, und der Befehl erfasst möglicherweise nicht alle Daten. Danach `metrocluster check show` Befehle zeigen nicht die erwartete Ausgabe an.

Schritte

1. Überprüfen Sie die Konfiguration:

   ```
   metrocluster check run
   ```

   Der Befehl wird als Hintergrundjob ausgeführt und wird möglicherweise nicht sofort ausgeführt.

```
cluster_A::> metrocluster check run
The operation has been started and is running in the background. Wait
for
it to complete and run "metrocluster check show" to view the results. To
check the status of the running metrocluster check operation, use the
command,
"metrocluster operation history show -job-id 2245"
```

```
cluster_A::> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         ok
volumes             ok
7 entries were displayed.
```

2. Zeigen Sie detailliertere Ergebnisse des letzten MetroCluster-Prüfbefehls an:

```
metrocluster check aggregate show

metrocluster check cluster show

metrocluster check config-replication show

metrocluster check lif show

metrocluster check node show
```

> Der `metrocluster check show` Befehle zeigen die Ergebnisse der letzten `metrocluster check run` Befehl. Sie sollten immer den ausführen `metrocluster check run` Befehl vor Verwendung des `metrocluster check show` Befehle, sodass die angezeigten Informationen aktuell sind.

Das folgende Beispiel zeigt die `metrocluster check aggregate show` Befehlsausgabe für eine gesunde MetroCluster Konfiguration mit vier Nodes:

```
cluster_A::> metrocluster check aggregate show
```

```
Node                Aggregate                Check
Result
---------------     --------------------     ---------------------
---------
controller_A_1      controller_A_1_aggr0
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_1_aggr1
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_1_aggr2
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok

controller_A_2      controller_A_2_aggr0
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_2_aggr1
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
                                             ownership-state
ok
                    controller_A_2_aggr2
                                             mirroring-status
ok
                                             disk-pool-allocation
ok
```

```
                                                    ownership-state
ok

18 entries were displayed.
```

Im folgenden Beispiel wird die Ausgabe des Befehls „MetroCluster Check Cluster show“ für eine gesunde MetroCluster Konfiguration mit vier Nodes angezeigt. Sie zeigt an, dass die Cluster bei Bedarf bereit sind, eine ausgehandelte Umschaltung durchzuführen.

```
Cluster               Check                          Result
--------------------- ------------------------------ ---------
mccint-fas9000-0102
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
mccint-fas9000-0304
                      negotiated-switchover-ready    not-applicable
                      switchback-ready               not-applicable
                      job-schedules                  ok
                      licenses                       ok
                      periodic-check-enabled         ok
10 entries were displayed.
```

Verwandte Informationen

"Festplatten- und Aggregatmanagement"

"Netzwerk- und LIF-Management"

ONTAP-Konfiguration abschließen

Nach dem Konfigurieren, Aktivieren und Prüfen der MetroCluster Konfiguration können Sie die Cluster-Konfiguration fortsetzen, indem Sie nach Bedarf weitere SVMs, Netzwerkschnittstellen und andere ONTAP Funktionen hinzufügen.

Konfigurieren Sie die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration

Ab ONTAP 9.15.1 können Sie auf unterstützten Systemen eine End-to-End-Verschlüsselung konfigurieren, um Back-End-Verkehr, wie z. B. NVlog- und Speicherreplikationsdaten, zwischen den Standorten in einer MetroCluster -IP -Konfiguration zu verschlüsseln.

Über diese Aufgabe

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Bevor Sie die End-to-End-Verschlüsselung konfigurieren können, müssen Sie dies tun "Externes Verschlüsselungsmanagement konfigurieren".

- Prüfen Sie die unterstützten Systeme und die Mindestversion von ONTAP, die erforderlich sind, um die End-to-End-Verschlüsselung in einer MetroCluster IP-Konfiguration zu konfigurieren:

Minimale ONTAP-Version	Unterstützte Systeme
ONTAP 9.17.1	• AFF A800, AFF C800 • AFF A20, AFF A30, AFF C30, AFF A50, AFF C60 • AFF A70, AFF A90, AFF A1K, AFF C80 • FAS50, FAS70 UND FAS90
ONTAP 9.15.1	• AFF A400 • FAS8300 • FAS8700

End-to-End-Verschlüsselung

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu aktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

   b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

   ```
   metrocluster check show
   ```

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

```
security key-manager external show-status
```

3. End-to-End-Verschlüsselung für jede DR-Gruppe aktivieren:

```
metrocluster modify -is-encryption-enabled true -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
         replication data sent between MetroCluster nodes and have an
impact on
         performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung aktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          true
1           cluster_A  node_A_2  configured          true
1           cluster_B  node_B_1  configured          true
1           cluster_B  node_B_2  configured          true
4 entries were displayed.
```

End-to-End-Verschlüsselung deaktivieren

Führen Sie die folgenden Schritte aus, um die End-to-End-Verschlüsselung zu deaktivieren.

Schritte

1. Überprüfen Sie den Systemzustand der MetroCluster-Konfiguration.

   a. Vergewissern Sie sich, dass die MetroCluster-Komponenten ordnungsgemäß sind:

   ```
   metrocluster check run
   ```

   ```
   cluster_A::*> metrocluster check run
   ```

   Der Vorgang wird im Hintergrund ausgeführt.

   b. Nach dem `metrocluster check run` Vorgang abgeschlossen, Ausführen:

   ```
   metrocluster check show
   ```

   Nach etwa fünf Minuten werden die folgenden Ergebnisse angezeigt:

```
cluster_A:::*> metrocluster check show

Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
clusters            ok
connections         not-applicable
volumes             ok
7 entries were displayed.
```

a. Überprüfen Sie den Status des laufenden MetroCluster-Prüfvorgangs:

```
metrocluster operation history show -job-id <id>
```

b. Vergewissern Sie sich, dass es keine Systemzustandsmeldungen gibt:

```
system health alert show
```

2. Vergewissern Sie sich, dass das externe Schlüsselmanagement auf beiden Clustern konfiguriert ist:

```
security key-manager external show-status
```

3. Deaktivieren Sie die End-to-End-Verschlüsselung für jede DR-Gruppe:

```
metrocluster modify -is-encryption-enabled false -dr-group-id
<dr_group_id>
```

Beispiel

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Wiederholen Sie diesen Schritt für jede DR-Gruppe in der Konfiguration.

4. Vergewissern Sie sich, dass die End-to-End-Verschlüsselung deaktiviert ist:

```
metrocluster node show -fields is-encryption-enabled
```

Beispiel

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster    node      configuration-state is-encryption-
enabled
----------- ---------- --------  ------------------- -----------------
1           cluster_A  node_A_1  configured          false
1           cluster_A  node_A_2  configured          false
1           cluster_B  node_B_1  configured          false
1           cluster_B  node_B_2  configured          false
4 entries were displayed.
```

Einrichten von MetroCluster Tiebreaker oder ONTAP Mediator für eine MetroCluster -IP-Konfiguration

Sie können entweder die MetroCluster Tiebreaker Software auf einem dritten Standort herunterladen und installieren oder, beginnend mit ONTAP 9.7, dem ONTAP Mediator.

Bevor Sie beginnen

Der verfügbare Linux-Host mit Netzwerkkonnektivität zu beiden Clustern in der MetroCluster-Konfiguration muss über einen Linux-Host verfügen. Die spezifischen Anforderungen sind in der Dokumentation MetroCluster Tiebreaker oder ONTAP Mediator enthalten.

Wenn Sie eine Verbindung zu einer vorhandenen Tiebreaker- oder ONTAP Mediator-Instanz herstellen, benötigen Sie den Benutzernamen, das Kennwort und die IP-Adresse des Tiebreakers oder Mediators.

Wenn Sie eine neue Instanz des ONTAP Mediators installieren müssen, befolgen Sie die Anweisungen, um die Software zu installieren und zu konfigurieren.

"Konfigurieren Sie ONTAP Mediator für ungeplante automatische Umschaltung"

Wenn Sie eine neue Instanz der Tiebreaker Software installieren müssen, befolgen Sie die "Anweisungen zur Installation und Konfiguration der Software".

Über diese Aufgabe

Sie können die MetroCluster Tiebreaker Software und den ONTAP Mediator nicht mit derselben MetroCluster Konfiguration verwenden.

"Überlegungen zur Verwendung von ONTAP Mediator oder MetroCluster Tiebreaker"

Schritt

1. Konfigurieren Sie ONTAP Mediator oder die Tiebreaker-Software:
   - Wenn Sie eine vorhandene Instanz des ONTAP Mediators verwenden, fügen Sie ONTAP Mediator zu ONTAP hinzu:

```
metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
```

- Wenn Sie die Tiebreaker Software verwenden, lesen Sie die "Tiebreaker Dokumentation".

Sichern Sie Cluster-Konfigurationsdateien in einer MetroCluster -IP-Konfiguration

Sie können einen zusätzlichen Schutz für die Backup-Dateien der Clusterkonfiguration bieten, indem Sie eine Remote-URL (entweder HTTP oder FTP) angeben, bei der die Backup-Dateien der Konfiguration zusätzlich zu den Standardstandorten im lokalen Cluster hochgeladen werden.

Schritt

1. Legen Sie die URL des Remote-Ziels für die Backup-Dateien der Konfiguration fest:

```
system configuration backup settings modify URL-of-destination
```

Der "Cluster-Management mit der CLI" Enthält zusätzliche Informationen unter dem Abschnitt *Verwalten von Konfigurations-Backups*.

Konfigurieren Sie die MetroCluster Software mit System Manager

Richten Sie eine MetroCluster IP-Site mit ONTAP System Manager ein

Ab ONTAP 9.8 können Sie mit System Manager einen MetroCluster IP-Standort einrichten.

Ein MetroCluster-Standort besteht aus zwei Clustern. In der Regel befinden sich die Cluster an verschiedenen geografischen Standorten.

Bevor Sie beginnen

- Das System sollte bereits gemäß dem installiert und verkabelt sein "Installations- und Setup-Anleitung", der mit dem System geliefert wurde.
- Clusternetzwerkschnittstellen sollten auf jedem Knoten eines jeden Clusters für die Kommunikation innerhalb des Clusters konfiguriert werden.

Weisen Sie eine Node-Management-IP-Adresse zu

Windows System

Sie sollten Ihren Windows-Computer mit dem Subnetz verbinden, mit dem die Controller verbunden sind. Dadurch wird Ihrem System automatisch eine Node-Management-IP-Adresse zugewiesen.

Schritte

1. Öffnen Sie vom Windows-System aus das Laufwerk **Network**, um die Knoten zu erkennen.
2. Doppelklicken Sie auf den Node, um den Cluster-Setup-Assistenten zu starten.

Andere Systeme

Sie sollten die Node-Management-IP-Adresse für einen der Nodes im Cluster konfigurieren. Sie können diese Node-Management-IP-Adresse verwenden, um den Setup-Assistenten für das Cluster zu starten.

"Erstellen des Clusters auf dem ersten Node"Informationen zum Zuweisen einer Node-Management-IP-Adresse finden Sie unter.

Initialisieren und konfigurieren Sie den Cluster

Sie initialisieren den Cluster, indem Sie ein Administratorpasswort für das Cluster festlegen und die Cluster-Management- und Node-Managementnetzwerke einrichten. Sie können auch Dienste wie einen DNS (Domain Name Server) konfigurieren, um Hostnamen aufzulösen, und einen NTP-Server zur Synchronisierung der Zeit.

Schritte

1. Geben Sie in einem Webbrowser die konfigurierte Node-Management-IP-Adresse ein: "https://node-management-IP"

   System Manager erkennt die im Cluster verbliebenen Nodes automatisch.

2. Führen Sie im Fenster **Storage System initialisieren** folgende Schritte durch:
   a. Geben Sie die Netzwerkkonfigurationsdaten des Cluster-Managements ein.
   b. Geben Sie die Node-Management-IP-Adressen für alle Nodes ein.
   c. Geben Sie DNS-Details an.
   d. Aktivieren Sie im Abschnitt **andere** das Kontrollkästchen **Zeitdienst verwenden (NTP)**, um die Zeitserver hinzuzufügen.

Wenn Sie auf **Absenden** klicken, warten Sie, bis der Cluster erstellt und konfiguriert wurde. Anschließend erfolgt ein Validierungsprozess.

Nächste Schritte

Führen Sie nach dem Einrichten, Initialisieren und Konfigurieren beider Cluster das Verfahren durch"MetroCluster IP-Peering einrichten".

Konfigurieren Sie ONTAP auf einem neuen Cluster-Video

Richten Sie MetroCluster IP-Peering mit ONTAP System Manager ein

Ab ONTAP 9.8 können Sie MetroCluster IP-Konfigurationsvorgänge mit System Manager managen. Nachdem Sie zwei Cluster eingerichtet haben, richten Sie Peering zwischen ihnen ein.

Bevor Sie beginnen

Richten Sie zwei Cluster ein. Siehe "Richten Sie einen MetroCluster IP-Standort ein"Verfahren.

Bestimmte Schritte dieses Prozesses werden von verschiedenen Systemadministratoren an den geografischen Standorten des jeweiligen Clusters ausgeführt. Zur Erläuterung dieses Verfahrens werden die Cluster „Standort A Cluster“ und „Standort B Cluster“ genannt.

Führen Sie den Peering-Prozess von Standort A aus

Dieser Prozess wird von einem Systemadministrator an Standort A durchgeführt

Schritte

1. Melden Sie sich bei Site A Cluster an.
2. Wählen Sie in System Manager in der linken Navigationsleiste **Dashboard** aus, um die Clusterübersicht anzuzeigen.

   Im Dashboard werden die Details zu diesem Cluster angezeigt (Standort A). Im Abschnitt **MetroCluster** wird Standort A Cluster auf der linken Seite angezeigt.
3. Klicken Sie Auf **Partner-Cluster Anhängen**.
4. Geben Sie die Details der Netzwerkschnittstellen ein, die es den Knoten in Standort-A-Cluster ermöglichen, mit den Knoten im Standort-B-Cluster zu kommunizieren.

5. Klicken Sie auf **Speichern und fortfahren**.
6. Wählen Sie im Fenster **Partner Cluster anhängen Ich habe keine Passphrase**. Auf diese Weise können Sie eine Passphrase generieren.
7. Kopieren Sie die generierte Passphrase, und teilen Sie sie mit dem Systemadministrator an Standort B
8. Wählen Sie **Schließen**.

Peering-Prozess von Standort B durchführen

Dieser Prozess wird von einem Systemadministrator an Standort B durchgeführt

Schritte

1. Melden Sie sich bei Standort B-Cluster an.
2. Wählen Sie in System Manager **Dashboard** aus, um die Clusterübersicht anzuzeigen.

   Das Dashboard zeigt die Details zu diesem Cluster an (Standort B). Im Abschnitt MetroCluster wird links Standort-B-Cluster angezeigt.

3. Klicken Sie auf **Attach Partner Cluster**, um den Peering-Prozess zu starten.
4. Geben Sie die Details der Netzwerkschnittstellen ein, die es den Knoten im Cluster Standort B ermöglichen, mit den Knoten in Standort A zu kommunizieren.
5. Klicken Sie auf **Speichern und fortfahren**.
6. Wählen Sie im Fenster **Partner Cluster anhängen Ich habe eine Passphrase**. Auf diese Weise können Sie die Passphrase eingeben, die Sie vom Systemadministrator an Standort A erhalten haben
7. Wählen Sie **Peer**, um den Peering-Prozess abzuschließen.

Was kommt als Nächstes?

Nachdem der Peering-Prozess erfolgreich abgeschlossen wurde, konfigurieren Sie die Cluster. Siehe "Konfigurieren Sie einen MetroCluster IP-Standort".

Konfigurieren Sie eine MetroCluster IP-Site mit ONTAP System Manager

Ab ONTAP 9.8 können Sie MetroCluster IP-Konfigurationsvorgänge mit System Manager managen. Dazu müssen zwei Cluster eingerichtet, Cluster-Peering durchgeführt und die Cluster konfiguriert werden.

Bevor Sie beginnen

Gehen Sie wie folgt vor:

- "Richten Sie einen MetroCluster IP-Standort ein"
- "MetroCluster IP-Peering einrichten"

Konfigurieren Sie die Verbindung zwischen Clustern

Schritte

1. Melden Sie sich an einem der Standorte bei System Manager an, und wählen Sie **Dashboard**.

   Im Abschnitt **MetroCluster** zeigt die Grafik die beiden Cluster, die Sie für die MetroCluster-Sites eingerichtet und angepasst haben. Das Cluster, von dem Sie arbeiten (lokales Cluster), wird auf der linken Seite angezeigt.

2. Klicken Sie auf **MetroCluster konfigurieren**. Führen Sie in diesem Fenster die folgenden Schritte aus:
   a. Es werden die Nodes für jedes Cluster in der MetroCluster-Konfiguration dargestellt. Wählen Sie in den Dropdown-Listen die Knoten im lokalen Cluster aus, die Disaster-Recovery-Partner für die Knoten im Remote-Cluster sind.
   b. Aktivieren Sie das Kontrollkästchen, wenn Sie ONTAP Mediator konfigurieren möchten. Siehe "ONTAP Mediator konfigurieren".
   c. Wenn beide Cluster über eine Lizenz zur Aktivierung der Verschlüsselung verfügen, wird der Abschnitt **Verschlüsselung** angezeigt.

      Geben Sie zum Aktivieren der Verschlüsselung eine Passphrase ein.

   d. Aktivieren Sie das Kontrollkästchen, wenn Sie MetroCluster mit einem freigegebenen Layer-3-Netzwerk konfigurieren möchten.

      Die HA-Partner-Nodes und die mit den Nodes verbundenen Netzwerk-Switches müssen über eine passende Konfiguration verfügen.

3. Klicken Sie auf **Speichern**, um die MetroCluster-Sites zu konfigurieren.

   Auf dem **Dashboard** im Abschnitt **MetroCluster** zeigt die Grafik ein Häkchen auf der Verbindung zwischen den beiden Clustern an, was auf eine gesunde Verbindung hinweist.

Konfigurieren Sie ONTAP Mediator für ungeplante automatische Umschaltung

Vorbereitung der Installation von ONTAP Mediator in einer MetroCluster -IP -Konfiguration

Ihre Umgebung muss bestimmte Anforderungen erfüllen.

Die folgenden Anforderungen gelten für eine Disaster Recovery-Gruppe (DR-Gruppe). Weitere Informationen zu "DR-Gruppen".

- Wenn Sie Ihre Linux-Version aktualisieren möchten, tun Sie dies, bevor Sie die aktuellste Version von ONTAP Mediator installieren.
- Die ONTAP Mediator- und MetroCluster Tiebreaker-Software sollten nicht beide mit derselben MetroCluster-Konfiguration verwendet werden.
- ONTAP Mediator muss auf einem Linux-Host an einem anderen Standort als den MetroCluster-Sites installiert werden.

  Die Konnektivität zwischen dem ONTAP Mediator und jedem Standort muss aus zwei separaten Ausfall-Domains bestehen.

- ONTAP Mediator kann bis zu fünf MetroCluster-Konfigurationen gleichzeitig unterstützen.
- Die automatische ungeplante Umschaltung wird in ONTAP 9.7 und höher unterstützt.
- IPv6 wird mit ONTAP Mediator nicht unterstützt.

Netzwerkanforderungen für die Verwendung von ONTAP Mediator in einer MetroCluster-Konfiguration

Um ONTAP Mediator in einer MetroCluster-Konfiguration zu installieren, müssen Sie sicherstellen, dass die Konfiguration mehrere Netzwerkanforderungen erfüllt.

- Latenz

  Maximale Latenz von weniger als 75 ms (RTT).

  Jitter darf nicht mehr als 5 ms betragen.

- MTU

  Die MTU-Größe muss mindestens 1400 betragen.

- Paketverlust

  Sowohl für das Internet Control Message Protocol (ICMP) als auch für TCP-Datenverkehr muss der Paketverlust unter 0.01 % liegen.

- Bandbreite

  Die Verbindung zwischen ONTAP Mediator und einer DR-Gruppe muss über eine Bandbreite von mindestens 20 Mbit/s verfügen.

- Unabhängige Konnektivität

  Es ist eine unabhängige Verbindung zwischen jedem Standort und dem ONTAP Mediator erforderlich. Ein Ausfall an einem Standort darf die IP-Verbindung zwischen den anderen beiden nicht betroffenen Standorten nicht unterbrechen.

Hostanforderungen für ONTAP Mediator in einer MetroCluster-Konfiguration

Sie müssen sicherstellen, dass die Konfiguration mehrere Host-Anforderungen erfüllt.

- ONTAP Mediator muss an einem externen Standort installiert sein, der physisch von den beiden ONTAP Clustern getrennt ist.
- ONTAP Mediator unterstützt maximal fünf MetroCluster-Konfigurationen.
- ONTAP Mediator benötigt nicht mehr als die Mindestanforderungen des Host-Betriebssystems an CPU und Arbeitsspeicher (RAM).
- Zusätzlich zu den Mindestanforderungen des Host-Betriebssystems muss mindestens 30 GB zusätzlicher nutzbarer Festplattenspeicher zur Verfügung stehen.
  - Jede DR-Gruppe benötigt bis zu 200 MB Festplattenspeicher.

Firewall-Anforderungen für ONTAP Mediator

ONTAP Mediator verwendet eine Reihe von Ports für die Kommunikation mit bestimmten Diensten.

Wenn Sie eine Firewall eines Drittanbieters verwenden:

- HTTPS-Zugriff muss aktiviert sein.
- Er muss so konfiguriert sein, dass der Zugriff auf die Ports 31784 und 3260 möglich ist.

Bei Verwendung der standardmäßigen Red hat oder CentOS Firewall wird die Firewall während der Mediator-Installation automatisch konfiguriert.

In der folgenden Tabelle sind die Ports aufgeführt, die Sie in Ihrer Firewall zulassen müssen:

- Der iSCSI-Port ist nur in einer MetroCluster-IP-Konfiguration erforderlich.
- Der 22/tcp-Port ist für den normalen Betrieb nicht erforderlich, Sie können ihn jedoch vorübergehend für Wartungsarbeiten aktivieren und deaktivieren, wenn die Wartungssitzung beendet ist.

Port/Services	Quelle	Richtung	Ziel	Zweck
22/tcp	Management-Host	Eingehend	ONTAP Mediator	SSH / ONTAP Mediatormanagement
31784/tcp	Cluster-MGM- und Node-MGM-LIFs	Eingehend	Web-Server ONTAP Mediator	REST-API (HTTPS)
3260/tcp	Knotenverwaltungs-LIFs	Bidirektional	ONTAP Mediator iSCSI-Ziele	ISCSI-Datenverbindung für Mailboxen

Richtlinien zum Upgrade von ONTAP Mediator in einer MetroCluster-Konfiguration

Wenn Sie ONTAP Mediator aktualisieren, müssen Sie die Linux-Versionsanforderungen erfüllen und die Richtlinien für die Aktualisierung befolgen.

- ONTAP Mediator kann von einer unmittelbar vorhergehenden Version auf die aktuelle Version aktualisiert werden.
- Alle Mediator-Versionen werden von MetroCluster IP-Konfigurationen mit ONTAP 9.7 oder höher unterstützt.

"Installieren oder aktualisieren Sie ONTAP Mediator"

Nach dem Upgrade

Nachdem die Aktualisierung von Mediator und Betriebssystem abgeschlossen ist, sollten Sie den ausgeben `storage iscsi-initiator show` Befehl, um zu bestätigen, dass die Mediator-Verbindungen aktiv sind.

Einrichten des ONTAP Mediators für eine MetroCluster -IP-Konfiguration

ONTAP Mediator muss auf dem ONTAP-Knoten für die Verwendung in einer MetroCluster-IP-Konfiguration konfiguriert werden.

Bevor Sie beginnen

- ONTAP Mediator muss erfolgreich an einem Netzwerkstandort installiert worden sein, der von beiden MetroCluster-Standorten aus erreichbar ist.

  "Installieren oder aktualisieren Sie ONTAP Mediator"

- Sie müssen über die IP-Adresse des Hosts verfügen, auf dem ONTAP Mediator ausgeführt wird.
- Sie müssen über den Benutzernamen und das Passwort für ONTAP Mediator verfügen.
- Alle Nodes der MetroCluster IP-Konfiguration müssen online sein.

> Ab ONTAP 9.12.1 kann die Funktion zur automatischen erzwungenen Umschaltung von MetroCluster in einer MetroCluster IP Konfiguration aktiviert werden. Diese Funktion ist eine Erweiterung der mediatorgestützten ungeplanten Umschaltung. Bevor Sie diese Funktion aktivieren, überprüfen Sie die "Risiken und Einschränkungen bei der automatischen erzwungenen MetroCluster Umschaltung".

Über diese Aufgabe

- Diese Aufgabe ermöglicht standardmäßig automatische ungeplante Umschaltung.
- Diese Aufgabe kann auf der ONTAP-Schnittstelle eines beliebigen Knotens der MetroCluster IP-Konfiguration ausgeführt werden.
- Eine einzelne Installation von ONTAP Mediator kann mit bis zu fünf MetroCluster-IP-Konfigurationen konfiguriert werden.

Schritte

1. Fügen Sie ONTAP Mediator zu ONTAP hinzu:

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

   > Sie werden aufgefordert, den Benutzernamen und das Kennwort für das Mediator Admin-Benutzerkonto einzugeben.

2. Stellen Sie sicher, dass die automatische Umschaltfunktion aktiviert ist:

   ```
   metrocluster show
   ```

3. Überprüfen Sie, ob der Mediator jetzt ausgeführt wird.

   a. Zeigen Sie die virtuellen Mediator-Laufwerke an:

      ```
      storage disk show -container-type mediator
      ```

```
 cluster_A::> storage disk show -container-type mediator
                       Usable           Disk    Container
Container
 Disk                  Size Shelf Bay Type    Type        Name
Owner
 ---------------- ---------- ----- --- ------- ----------- ---------
--------
 NET-1.5                  -     -   - VMDISK  mediator    -
node_A_2
 NET-1.6                  -     -   - VMDISK  mediator    -
node_B_1
 NET-1.7                  -     -   - VMDISK  mediator    -
node_B_2
 NET-1.8                  -     -   - VMDISK  mediator    -
node_A_1
```

b. Legen Sie den Berechtigungsmodus auf erweitert fest:

```
set advanced
```

```
 cluster_A::> set advanced
```

c. Anzeigen der Initiatoren, die als Mediator bezeichnet werden:

```
storage iscsi-initiator show -label mediator
```

```
 cluster_A::*> storage iscsi-initiator show -label mediator
   (storage iscsi-initiator show)
  +
Status
 Node Type Label    Target Portal      Target Name
Admin/Op
 ---- ---- -------- ------------------
--------------------------------- --------
 node_A_1
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68- 00a098cbca9e:1 up/up
 node_A_2
      mailbox
           mediator 1.1.1.1       iqn.2012-
05.local:mailbox.target.6616cd3f-9ef1-11e9-aada-
00a098ccf5d8:a05e1ffb-9ef1-11e9-8f68-00a098cbca9e:1 up/up
```

d. Überprüfen Sie den Status der AUSO-Fehlerdomäne (Automatic Unplanmäßigen Switchover):

`metrocluster show`

> Die folgende Beispielausgabe gilt für ONTAP 9.13.1 und höher. Bei ONTAP 9.12.1 und älteren Versionen sollte der Status der AUSO-Fehlerdomäne sein `auso-on-cluster-disaster`.

```
cluster_A::> metrocluster show
Cluster                   Entry Name          State
------------------------- ------------------- -----------
Local: cluster_A         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-dr-group-disaster
Remote: cluster_B         Configuration state configured
                          Mode                normal
                          AUSO Failure Domain auso-on-dr-group-disaster
```

4. Optional können Sie die automatische erzwungene Umschaltung von MetroCluster konfigurieren.

   Sie können den folgenden Befehl nur auf der erweiterten Berechtigungsebene verwenden.

   > Bevor Sie diesen Befehl verwenden, überprüfen Sie die "Risiken und Einschränkungen bei der automatischen erzwungenen MetroCluster Umschaltung".

   `metrocluster modify -allow-auto-forced-switchover true`

```
cluster_A::*> metrocluster modify -allow-auto-forced-switchover true
```

Entfernen Sie den ONTAP Mediator aus einer MetroCluster -IP-Konfiguration

Sie können ONTAP Mediator aus der MetroCluster-IP-Konfiguration dekonfigurieren.

Bevor Sie beginnen

Sie müssen ONTAP Mediator erfolgreich an einem Netzwerkstandort installiert und konfiguriert haben, der von beiden MetroCluster-Sites aus erreichbar ist.

Schritte

1. Dekonfigurieren Sie ONTAP Mediator mit dem folgenden Befehl:

   `metrocluster configuration-settings mediator remove`

   Sie werden aufgefordert, den Benutzernamen und das Passwort für das Administratorkonto des ONTAP Mediators einzugeben.

   > Wenn der ONTAP Mediator ausfällt, `metrocluster configuration-settings mediator remove` Der Befehl fordert Sie weiterhin auf, den Benutzernamen und das Kennwort für das ONTAP Mediator-Administratorbenutzerkonto einzugeben, und entfernt ONTAP Mediator aus der MetroCluster-Konfiguration.

   a. Überprüfen Sie mit dem folgenden Befehl, ob beschädigte Festplatten vorhanden sind:

      `disk show -broken`

      Beispiel

```
There are no entries matching your query.
```

2. Bestätigen Sie, dass ONTAP Mediator aus der MetroCluster-Konfiguration entfernt wurde, indem Sie die folgenden Befehle auf beiden Clustern ausführen:

   a. `metrocluster configuration-settings mediator show`

      Beispiel

```
This table is currently empty.
```

   b. `storage iscsi-initiator show -label mediator`

      Beispiel

```
There are no entries matching your query.
```

Verbinden Sie eine MetroCluster IP-Konfiguration mit einer anderen ONTAP Mediator-Instanz

Wenn Sie die MetroCluster-Knoten mit einer anderen ONTAP-Mediator-Instanz verbinden möchten, müssen Sie die Konfiguration aufheben und dann die Mediatorverbindung in der ONTAP-Software neu konfigurieren.

Bevor Sie beginnen

Sie benötigen den Benutzernamen, das Passwort und die IP-Adresse der neuen ONTAP Mediator-Instanz.

Über diese Aufgabe

Diese Befehle können von jedem Node in der MetroCluster Konfiguration ausgegeben werden.

Schritte

1. Entfernen Sie den aktuellen ONTAP Mediator aus der MetroCluster-Konfiguration:

   ```
   metrocluster configuration-settings mediator remove
   ```

2. Stellen Sie die neue ONTAP Mediator-Verbindung zur MetroCluster-Konfiguration her:

   ```
   metrocluster configuration-settings mediator add -mediator-address ip-address-of-mediator-host
   ```

Wie der ONTAP Mediator automatische ungeplante Switchover in MetroCluster -IP -Konfigurationen unterstützt

ONTAP Mediator stellt Postfach-LUNs zur Speicherung von Statusinformationen zu den MetroCluster-IP-Knoten bereit. Diese LUNs befinden sich am selben Standort wie ONTAP Mediator, der auf einem Linux-Host ausgeführt wird, der physisch von den MetroCluster-Standorten getrennt ist. Die MetroCluster IP-Knoten können die Mailbox-Informationen nutzen, um den Status ihrer Disaster Recovery (DR)-Partner zu überwachen und im Notfall eine Mediator-gestützte ungeplante Umschaltung (MAUSO) zu implementieren.

MAUSO wird in MetroCluster FC-Konfigurationen nicht unterstützt.

Wenn ein Node einen Standortausfall erkennt, der ein Switchover erfordert, so wird nur schrittweise bestätigt, dass die Umschaltung angemessen ist und falls ja, auch die Umschaltung durchgeführt wird. Standardmäßig wird ein MAUSO für die folgenden Szenarien initiiert:

- Zum Zeitpunkt des Ausfalls werden sowohl SyncMirror-Spiegelung als auch DR-Spiegelung des nichtflüchtigen Cache jedes Node ausgeführt. Die Caches und Spiegelungen werden synchronisiert.
- Keiner der Knoten am noch verbleibenden Standort befindet sich im Übernahmemodus.
- Bei einem Standortausfall. Ein Standortausfall ist ein Ausfall von *all* Nodes am selben Standort.

Ein MAUSO wird in den folgenden Shutdown-Szenarien *Not* initiiert:

- Sie initiieren ein Herunterfahren. Beispiel, wenn Sie:
  - Halten Sie die Nodes an

◦ Booten Sie die Nodes neu

Erfahren Sie mehr über die MAUSO-Funktionen, die mit jeder Version von ONTAP 9 verfügbar sind.

Beginnt mit…	Beschreibung
ONTAP 9.13.1	• Ein MAUSO wird initiiert, wenn ein Standardszenario Tritt auf, und ein Lüfter- oder Hardwareausfall initiiert ein Herunterfahren der Umgebung. Beispiele für Hardwareausfälle sind eine hohe oder niedrige Temperatur, ein Netzteil, eine NVRAM-Batterie oder ein Heartbeat-Fehler des Service-Prozessors. • Der Standardwert für die Fehlerdomäne ist in einer MetroCluster IP-Konfiguration auf „aus-on-dr-Group“ gesetzt. Bei ONTAP 9.12.1 und älteren Versionen ist der Standardwert auf „auso-on-Cluster-Disaster“ eingestellt. In einer MetroCluster IP Konfiguration mit acht Nodes löst „auso-on-dr-Gruppe“ einen MAUSO aus, entweder beim Ausfall des Clusters oder bei einem HA-Paar in einer DR-Gruppe. Bei einem HA-Paar müssen beide Nodes gleichzeitig ausfallen. Optional können Sie die Einstellung der Fehlerdomäne in die Domäne „auso-on-Cluster-Disaster“ mit ändern `metrocluster modify -auto-switchover -failure-domain auso-on-cluster-disaster` Befehl zum Auslösen eines MAUSO nur, wenn in beiden DR-Gruppen ein HA-Node-Paar-Fehler vorhanden ist. • Sie können das Verhalten so ändern, dass ein MAUSO erzwungen wird, auch wenn der NVRAM zum Zeitpunkt des Fehlers nicht synchron ist.
ONTAP 9.12.1	Sie können die automatische erzwungene Umschaltung von MetroCluster in einer MetroCluster IP-Konfiguration mithilfe von aktivieren `metrocluster modify -allow -auto-forced-switchover true` Befehl. Umschaltung bei Erkennung eines Standortausfalls erfolgt automatisch, wenn die MetroCluster Funktion zur automatischen erzwungenen Umschaltung aktiviert wird. Diese Funktion ergänzt die MetroCluster IP Funktion zur automatischen Umschaltung. **Risiken und Einschränkungen bei der automatischen erzwungenen MetroCluster Umschaltung** Wenn Sie zulassen, dass eine MetroCluster-IP-Konfiguration im automatischen Umschaltmodus betrieben wird, kann das folgende bekannte Problem zu Datenverlust führen: • Der nicht-flüchtige Speicher in den Storage Controllern wird nicht zum Remote-DR-Partner am Partnerstandort gespiegelt. **Achtung**: Es können Szenarien auftreten, die nicht erwähnt werden. NetApp ist nicht verantwortlich für Datenkorruption, Datenverlust oder andere Schäden, die durch die Aktivierung der automatischen erzwungenen MetroCluster Switchover-Funktion entstehen können. Verwenden Sie die Funktion zur automatischen erzwungenen Umschaltung nicht von MetroCluster, wenn das Risiko und die Einschränkungen für Sie nicht akzeptabel sind.

Verwalten Sie den ONTAP Mediator mit System Manager in MetroCluster -IP -Konfigurationen

Mit System Manager können Sie Aufgaben zum Verwalten von ONTAP Mediator ausführen.

Über diese Aufgaben

Ab ONTAP 9.8 können Sie System Manager als vereinfachte Schnittstelle zur Verwaltung einer MetroCluster IP-Konfiguration mit vier Knoten verwenden. Zu dieser Konfiguration kann auch ein ONTAP Mediator an einem dritten Standort gehören.

Ab ONTAP 9.14.1 können Sie die folgenden Vorgänge auch für einen MetroCluster IP-Standort mit acht Nodes ausführen. Sie können ein System mit acht Nodes nicht mit System Manager einrichten oder erweitern, aber wenn Sie bereits ein MetroCluster IP-System mit acht Nodes eingerichtet haben, können Sie diese Vorgänge trotzdem ausführen.

Führen Sie die folgenden Aufgaben aus, um ONTAP Mediator zu verwalten.

Aufgabe durchführen…	Ergreifen Sie diese Maßnahmen…
ONTAP Mediator konfigurieren	Beide Cluster an den MetroCluster Standorten sollten up und Peering durchgeführt werden. **Schritte** 1. Wählen Sie unter System Manager in ONTAP 9.8 die Option **Cluster > Einstellungen** aus. 2. Klicken Sie im Abschnitt **Mediator** auf ⚙. 3. Klicken Sie im Fenster **Mediator konfigurieren** auf **Hinzufügen+**. 4. Geben Sie die Konfigurationsdetails für ONTAP Mediator ein. Sie können die folgenden Details eingeben, während Sie ONTAP Mediator mit System Manager konfigurieren. ◦ Die IP-Adresse des ONTAP Mediators. ◦ Der Benutzername. ◦ Das Passwort.

Aktivieren oder Deaktivieren der Mediator-gestützten automatischen Umschaltung (MAUSO)	**Schritte** 1. Klicken Sie in System Manager auf **Dashboard**. 2. Blättern Sie zum Abschnitt „MetroCluster“. 3. Klicken Sie neben dem Namen der MetroCluster-Site auf ⋮ . 4. Wählen Sie **Enable** oder **Disable**. 5. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie dann auf **enable** oder **Disable**. ⓘ Sie können ONTAP Mediator aktivieren oder deaktivieren, wenn er erreichbar ist und sich beide Standorte im „Normal“-Modus befinden. ONTAP Mediator ist weiterhin erreichbar, wenn MAUSO aktiviert oder deaktiviert ist und das MetroCluster-System fehlerfrei ist.
Entfernen Sie ONTAP Mediator aus der MetroCluster-Konfiguration	**Schritte** 1. Klicken Sie in System Manager auf **Dashboard**. 2. Blättern Sie zum Abschnitt „MetroCluster“. 3. Klicken Sie neben dem Namen der MetroCluster-Site auf ⋮ . 4. Wählen Sie **Mediator Entfernen**. 5. Geben Sie den Benutzernamen und das Kennwort des Administrators ein, und klicken Sie dann auf **Entfernen**.
Überprüfen Sie den Zustand von ONTAP Mediator	Führen Sie die spezifischen Schritte des System Managers in "Überprüfen Sie den Funktionszustand einer MetroCluster-Konfiguration"aus.
Durchführen einer Umschaltung und eines Switchback	Führen Sie die Schritte in "Verwenden Sie System Manager für Umschaltung und Switchback (nur MetroCluster IP-Konfigurationen)."aus.

Testen Sie die ONTAP -Knotenumschaltung für Ihre MetroCluster IP-Konfiguration

Sie können Fehlerszenarien testen, um den korrekten Betrieb der MetroCluster-Konfiguration zu bestätigen.

Überprüfung der ausgehandelten Umschaltung

Sie können die ausgehandelte (geplante) Umschaltung testen, um die unterbrechungsfreie Datenverfügbarkeit zu bestätigen.

Über diese Aufgabe

Dieser Test überprüft, ob sich die Datenverfügbarkeit nicht auf die Protokolle Microsoft Server Message Block (SMB) und Solaris Fibre Channel auswirkt (ausgenommen Microsoft Server Message Block), indem der Cluster in das zweite Rechenzentrum umgeschaltet wird.

Dieser Test dauert etwa 30 Minuten.

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Der `metrocluster switchover` Der Befehl gibt eine Warnmeldung an.

  Wenn Sie antworten `yes` In der Eingabeaufforderung wechselt der Standort, von dem der Befehl ausgegeben wird, über die Partnerseite.

Für MetroCluster IP-Konfigurationen:

- Für ONTAP 9.4 und früher:
  - Gespiegelte Aggregate werden nach der ausgehandelten Umschaltung herabgestuft.
- Für ONTAP 9.5 und höher:
  - Gespiegelte Aggregate bleiben im normalen Status, wenn auf den Remote-Storage zugegriffen werden kann.
  - Gespiegelte Aggregate werden nach der ausgehandelten Umschaltung herabgesetzt, wenn der Zugriff auf den Remote-Storage verloren geht.
- Für ONTAP 9.8 und höher:
  - Nicht gespiegelte Aggregate, die sich am Disaster-Standort befinden, sind bei einem Ausfall des Remote-Storage nicht verfügbar. Dies kann zu einem Controller-Ausfall führen.

Schritte

1. Vergewissern Sie sich, dass sich alle Nodes im konfigurierten Status und im normalen Modus befinden:

   `metrocluster node show`

   ```
   cluster_A::>  metrocluster node show

   Cluster                     Configuration State    Mode
   --------------------------- ---------------------
   ------------------------
    Local: cluster_A              configured             normal
   Remote: cluster_B              configured             normal
   ```

2. Starten Sie den Switchover-Vorgang:

   `metrocluster switchover`

   ```
   cluster_A::> metrocluster switchover
   Warning: negotiated switchover is about to start. It will stop all the
   data Vservers on cluster "cluster_B" and
   automatically re-start them on cluster "cluster_A". It will finally
   gracefully shutdown cluster "cluster_B".
   ```

3. Vergewissern Sie sich, dass sich das lokale Cluster im konfigurierten Zustand befindet und der Switchover-Modus aktiviert ist:

```
metrocluster node show
```

```
cluster_A::>  metrocluster node show

Cluster                           Configuration State    Mode
--------------------------------- ---------------------
------------------------
Local: cluster_A                   configured             switchover
Remote: cluster_B                  not-reachable          -
              configured             normal
```

4. Bestätigen Sie, dass der Switchover-Vorgang erfolgreich war:

```
metrocluster operation show
```

```
cluster_A::>  metrocluster operation show

cluster_A::> metrocluster operation show
  Operation: switchover
      State: successful
 Start Time: 2/6/2016 13:28:50
   End Time: 2/6/2016 13:29:41
     Errors: -
```

5. Verwenden Sie die `vserver show` Und `network interface show` Befehle, um zu überprüfen, ob DR-SVMs und LIFs online sind.

Überprüfung der Heilung und manueller Umkehrschalter

Sie können die Healing- und manuellen Switchback-Vorgänge testen, um zu überprüfen, ob die Datenverfügbarkeit nicht beeinträchtigt ist (außer bei SMB- und Solaris-FC-Konfigurationen), indem Sie nach einer ausgehandelten Umschaltung das Cluster wieder zum ursprünglichen Datacenter wechseln.

Über diese Aufgabe

Dieser Test dauert etwa 30 Minuten.

Das erwartete Ergebnis dieses Verfahrens ist, dass Services zurück auf ihre Home-Knoten geschaltet werden sollten.

Die Heilungsschritte sind auf Systemen mit ONTAP 9.5 oder höher nicht erforderlich, auf denen nach einer ausgehandelten Umschaltung automatisch eine Heilung durchgeführt wird. Auf Systemen mit ONTAP 9.6 und höher wird die Reparatur auch nach nicht ungeplanter Umschaltung automatisch durchgeführt.

Schritte

1. Wenn ONTAP 9.4 oder eine frühere Version des Systems ausgeführt wird, kann das Datenaggregat repariert werden:

```
metrocluster heal aggregates
```

Im folgenden Beispiel wird die erfolgreiche Ausführung des Befehls angezeigt:

```
cluster_A::> metrocluster heal aggregates
[Job 936] Job succeeded: Heal Aggregates is successful.
```

2. Wenn das System ONTAP 9.4 oder älter ausführt, können Sie das Root-Aggregat heilen:

   `metrocluster heal root-aggregates`

   Dieser Schritt ist für folgende Konfigurationen erforderlich:

   - MetroCluster FC-Konfigurationen
   - MetroCluster IP-Konfigurationen mit ONTAP 9.4 oder einer früheren Version Im folgenden Beispiel wird die erfolgreiche Ausführung des Befehls angezeigt:

```
cluster_A::> metrocluster heal root-aggregates
[Job 937] Job succeeded: Heal Root Aggregates is successful.
```

3. Vergewissern Sie sich, dass die Heilung abgeschlossen ist:

   `metrocluster node show`

   Im folgenden Beispiel wird die erfolgreiche Ausführung des Befehls angezeigt:

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   heal roots
completed
      cluster_B
              node_B_2         unreachable    -         switched over
42 entries were displayed.metrocluster operation show
```

   Wenn der automatische Heilvorgang aus irgendeinem Grund fehlschlägt, müssen Sie den ausgeben `metrocluster heal` Befehle, die manuell wie in ONTAP-Versionen vor ONTAP 9.5 ausgeführt werden. Sie können das verwenden `metrocluster operation show` Und `metrocluster operation history show -instance` Befehle, um den Status der Reparatur zu überwachen und die Ursache eines Fehlers zu bestimmen.

4. Überprüfen der Spiegelung aller Aggregate:

   `storage aggregate show`

   Das folgende Beispiel zeigt, dass alle Aggregate einen RAID-Status der Spiegelung aufweisen:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster
            4.19TB    4.13TB    2% online       8 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster
           715.5GB   212.7GB   70% online       1 node_A_1    raid4,
                                                               mirrored,
                                                               normal
cluster_B Switched Over Aggregates:
Aggregate Size     Available Used% State   #Vols  Nodes       RAID
Status
--------- -------- --------- ----- ------- ------ ----------
------------
data_cluster_B
            4.19TB    4.11TB    2% online       5 node_A_1    raid_dp,
                                                               mirrored,
                                                               normal
root_cluster_B    -         -     - unknown      - node_A_1   -
```

5. Überprüfen Sie den Status der zurückkehrenden Wiederherstellung:

   `metrocluster node show`

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ----------------- -------------- ---------
--------------------
1     cluster_A
             node_A_1           configured     enabled   heal roots
completed
      cluster_B
             node_B_2           configured     enabled   waiting for
switchback
                                                         recovery
2 entries were displayed.
```

6. Führen Sie den Wechsel zurück:

```
metrocluster switchback
```

```
cluster_A::> metrocluster switchback
[Job 938] Job succeeded: Switchback is successful.Verify switchback
```

7. Status der Knoten bestätigen:

```
metrocluster node show
```

```
cluster_A::> metrocluster node show
DR                              Configuration  DR
Group Cluster Node              State          Mirroring Mode
----- ------- ------------------ -------------- ---------
--------------------
1     cluster_A
              node_A_1         configured     enabled   normal
      cluster_B
              node_B_2         configured     enabled   normal

2 entries were displayed.
```

8. Status des MetroCluster-Vorgangs bestätigen:

```
metrocluster operation show
```

Die Ausgabe sollte einen erfolgreichen Status aufweisen.

```
cluster_A::> metrocluster operation show
  Operation: switchback
      State: successful
 Start Time: 2/6/2016 13:54:25
   End Time: 2/6/2016 13:56:15
     Errors: -
```

Überprüfung des Betriebs nach Stromunterbrechung

Sie können die Antwort der MetroCluster-Konfiguration auf den Ausfall einer PDU testen.

Über diese Aufgabe

Als Best Practice empfiehlt es sich, jede Netzteileinheit (PSU) einer Komponente mit separaten Netzteilen zu verbinden. Wenn beide Netzteile mit derselben Stromverteilereinheit (Power Distribution Unit, PDU) verbunden sind und eine elektrische Störung auftritt, kann der Standort ausfallen oder ein komplettes Shelf nicht mehr verfügbar sein. Der Ausfall einer Stromleitung wird getestet, um zu bestätigen, dass keine Verkabelungsabweichung besteht, die zu einer Serviceunterbrechung führen kann.

Dieser Test dauert etwa 15 Minuten.

Für diesen Test müssen alle linken PDUs und dann alle rechten PDUs an allen Racks mit den MetroCluster-Komponenten ausgeschaltet werden.

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Fehler sollten beim Trennen der PDUs generiert werden.
- Es sollte kein Failover oder Serviceverlust auftreten.

Schritte

1. Schalten Sie die Stromversorgung der PDUs auf der linken Seite des Racks aus, in dem die MetroCluster-Komponenten enthalten sind.
2. Überwachen Sie das Ergebnis auf der Konsole:

   ```
   system environment sensors show -state fault

   storage shelf show -errors
   ```

   ```
   cluster_A::> system environment sensors show -state fault

   Node Sensor             State Value/Units Crit-Low Warn-Low Warn-Hi
   Crit-Hi
   ---- -------------------- ------ ----------- -------- -------- -------
   -------
   node_A_1
           PSU1            fault
                               PSU_OFF
           PSU1 Pwr In OK  fault
                               FAULT
   node_A_2
           PSU1            fault
                               PSU_OFF
           PSU1 Pwr In OK  fault
                               FAULT
   4 entries were displayed.

   cluster_A::> storage shelf show -errors
       Shelf Name: 1.1
        Shelf UID: 50:0a:09:80:03:6c:44:d5
    Serial Number: SHFHU1443000059

   Error Type          Description
   ------------------  ---------------------------
   Power               Critical condition is detected in storage shelf
   power supply unit "1". The unit might fail.Reconnect PSU1
   ```

3. Schalten Sie das Netzteil wieder ein, und schalten Sie es wieder ein.
4. Stellen Sie sicher, dass ONTAP die Fehlerbedingung beseitigt.
5. Wiederholen Sie die vorherigen Schritte mit den rechten PDUs.

Überprüfung des Betriebs nach Ausfall eines einzelnen Storage Shelfs

Sie können den Ausfall eines einzelnen Storage Shelf testen, um sicherzustellen, dass es keinen Single Point of Failure gibt.

Über diese Aufgabe

Dieses Verfahren hat folgende erwartete Ergebnisse:

- Eine Fehlermeldung sollte von der Überwachungssoftware gemeldet werden.
- Es sollte kein Failover oder Serviceverlust auftreten.
- Die Neusynchronisierung der Spiegelung wird automatisch nach Wiederherstellung des Hardwareausfalls gestartet.

Schritte

1. Überprüfen Sie den Status des Storage-Failovers:

   ```
   storage failover show
   ```

   ```
   cluster_A::> storage failover show

   Node           Partner        Possible State Description
   -------------- -------------- --------
   ------------------------------------
   node_A_1       node_A_2       true     Connected to node_A_2
   node_A_2       node_A_1       true     Connected to node_A_1
   2 entries were displayed.
   ```

2. Prüfen Sie den Aggregatstatus:

   ```
   storage aggregate show
   ```

```
cluster_A::> storage aggregate show

cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirrored,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirrored,

normal
```

3. Vergewissern Sie sich, dass alle Data SVMs und Daten-Volumes online sind und Daten bereitstellen:

```
vserver show -type data
```

```
network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_2_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_2_data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

4. Identifizieren Sie ein Shelf in Pool 1 für Node „Node_A_2“, um ein plötzliches Hardware-Versagen zu simulieren:

`storage aggregate show -r -node node-name !*root`

Das ausgewählte Shelf muss Laufwerke enthalten, die Teil eines gespiegelten Datenaggregats sind.

Im folgenden Beispiel ist die Shelf-ID „31“ ausgewählt, um den Fehler zu verhindern.

```
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirrored) (block
checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.4                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                      0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                      0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (online, normal, active, pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  1.31.7                      1   BSAS    7200  827.7GB
828.0GB (normal)
     parity   1.31.6                      1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.3                      1   BSAS    7200  827.7GB
828.0GB (normal)
     data     1.31.4                      1   BSAS    7200  827.7GB
```

```
828.0GB (normal)
     data     1.31.5                          1   BSAS    7200  827.7GB
828.0GB (normal)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                     0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.21                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                     0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

5. Schalten Sie das ausgewählte Shelf physisch aus.
6. Überprüfen Sie erneut den Aggregatstatus:

   ```
   storage aggregate show

   storage aggregate show -r -node node_A_2 !*root
   ```

   Das Aggregat mit Laufwerken auf dem ausgeschalteten Shelf sollte einen „degradierten“ RAID-Status haben, und Laufwerke auf dem betroffenen Plex sollten den Status „Fehlgeschlagen“ aufweisen, wie im folgenden Beispiel dargestellt:

   ```
   cluster_A::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1data01_mirrored
              4.15TB    3.40TB   18% online       3 node_A_1
   ```

```
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

mirror

degraded
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

mirror

degraded
cluster_A::> storage aggregate show -r -node node_A_2 !*root
Owner Node: node_A_2
 Aggregate: node_A_2_data01_mirrored (online, raid_dp, mirror degraded)
(block checksums)
  Plex: /node_A_2_data01_mirrored/plex0 (online, normal, active, pool0)
   RAID Group /node_A_2_data01_mirrored/plex0/rg0 (normal, block
checksums)
                                                                   Usable
Physical
     Position Disk                       Pool Type     RPM     Size
Size Status
     -------- -------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.3                      0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     parity   2.30.4                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.6                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.8                     0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.5                     0   BSAS    7200  827.7GB
828.0GB (normal)

  Plex: /node_A_2_data01_mirrored/plex4 (offline, failed, inactive,
pool1)
   RAID Group /node_A_2_data01_mirrored/plex4/rg0 (partial, none
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  FAILED                     -   -          -  827.7GB
-  (failed)
     parity   FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)
     data     FAILED                     -   -          -  827.7GB
-  (failed)

 Aggregate: node_A_2_data02_unmirrored (online, raid_dp) (block
checksums)
  Plex: /node_A_2_data02_unmirrored/plex0 (online, normal, active,
pool0)
   RAID Group /node_A_2_data02_unmirrored/plex0/rg0 (normal, block
checksums)
                                                                  Usable
Physical
     Position Disk                      Pool Type     RPM     Size
Size Status
     -------- ------------------------- ---- ----- ------ --------
-------- ----------
     dparity  2.30.12                    0   BSAS    7200  827.7GB
828.0GB (normal)
     parity   2.30.22                    0   BSAS    7200  827.7GB
828.0GB (normal)
```

```
     data     2.30.21                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.20                    0   BSAS    7200  827.7GB
828.0GB (normal)
     data     2.30.14                    0   BSAS    7200  827.7GB
828.0GB (normal)
15 entries were displayed.
```

7. Vergewissern Sie sich, dass die Daten bereitgestellt werden und alle Volumes noch online sind:

```
vserver show -type data

network interface show -fields is-home false

volume show !vol0,!MDV*
```

```
cluster_A::> vserver show -type data

cluster_A::> vserver show -type data
                                Admin      Operational Root
Vserver     Type    Subtype    State      State       Volume
Aggregate
----------- ------- ---------- ---------- ----------- ----------
----------
SVM1        data    sync-source           running     SVM1_root
node_A_1_data01_mirrored
SVM2        data    sync-source           running     SVM2_root
node_A_1_data01_mirrored

cluster_A::> network interface show -fields is-home false
There are no entries matching your query.

cluster_A::> volume show !vol0,!MDV*
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
SVM1
          SVM1_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.50GB    5%
SVM1
          SVM1_data_vol
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_root
                       node_A_1data01_mirrored
                                    online     RW         10GB
9.49GB    5%
SVM2
          SVM2_data_vol
                       node_A_2_data02_unmirrored
                                    online     RW          1GB
972.6MB    5%
```

8. Schalten Sie das Shelf physisch ein.

   Die Neusynchronisierung wird automatisch gestartet.

9. Überprüfen Sie, ob die Neusynchronisierung gestartet wurde:

   ```
   storage aggregate show
   ```

   Das betroffene Aggregat sollte den RAID-Status „Resynchronisierung“ aufweisen, wie im folgenden Beispiel dargestellt:

   ```
   cluster_A::> storage aggregate show
   cluster Aggregates:
   Aggregate     Size Available Used% State   #Vols  Nodes            RAID
   Status
   --------- -------- --------- ----- ------- ------ ----------------
   ------------
   node_A_1_data01_mirrored
              4.15TB    3.40TB   18% online       3 node_A_1
   raid_dp,

   mirrored,

   normal
   node_A_1_root
             707.7GB   34.29GB   95% online       1 node_A_1
   raid_dp,

   mirrored,

   normal
   node_A_2_data01_mirrored
              4.15TB    4.12TB    1% online       2 node_A_2
   raid_dp,

   resyncing
   node_A_2_data02_unmirrored
              2.18TB    2.18TB    0% online       1 node_A_2
   raid_dp,

   normal
   node_A_2_root
             707.7GB   34.27GB   95% online       1 node_A_2
   raid_dp,

   resyncing
   ```

10. Überwachen Sie das Aggregat, um sicherzustellen, dass die Neusynchronisierung abgeschlossen ist:

    ```
    storage aggregate show
    ```

Das betroffene Aggregat sollte einen RAID-Status von „Normal“ haben, wie im folgenden Beispiel dargestellt:

```
cluster_A::> storage aggregate show
cluster Aggregates:
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
node_A_1data01_mirrored
            4.15TB    3.40TB   18% online       3 node_A_1
raid_dp,

mirrored,

normal
node_A_1root
           707.7GB   34.29GB   95% online       1 node_A_1
raid_dp,

mirrored,

normal
node_A_2_data01_mirrored
            4.15TB    4.12TB    1% online       2 node_A_2
raid_dp,

normal
node_A_2_data02_unmirrored
            2.18TB    2.18TB    0% online       1 node_A_2
raid_dp,

normal
node_A_2_root
           707.7GB   34.27GB   95% online       1 node_A_2
raid_dp,

resyncing
```

MetroCluster-Konfigurationen entfernen

Wenden Sie sich an den technischen Support, wenn Sie die MetroCluster Konfiguration entfernen müssen.

Kontaktieren Sie den technischen Support von NetApp und lesen Sie das entsprechende Handbuch für Ihre

Konfiguration von "Entfernen von Knoten aus einer MetroCluster Konfiguration - Auflösungsleitfaden."

> Die Konfiguration von MetroCluster kann nicht rückgängig gemacht werden. Dieses Verfahren sollte nur mit Unterstützung durch den technischen Support erfolgen. Nach dem Entfernen der MetroCluster-Konfiguration sollten alle Festplatten-Konnektivität und Interconnects auf einen unterstützten Zustand eingestellt werden.

Anforderungen und Überlegungen für ONTAP -Operationen mit MetroCluster -IP-Konfigurationen

Wenn Sie ONTAP in einer MetroCluster-Konfiguration verwenden, sollten Sie bestimmte Überlegungen bei der Lizenzierung, beim Peering an Cluster außerhalb der MetroCluster-Konfiguration, bei der Durchführung von Volume-Vorgängen, NVFAIL-Vorgängen und anderen ONTAP-Vorgängen beachten.

Die ONTAP Konfiguration der beiden Cluster einschließlich Netzwerk sollte identisch sein, da die MetroCluster Funktion darauf setzt, dass ein Cluster bei einem Switchover Daten nahtlos für seinen Partner bereitstellen kann.

Überlegungen zur Lizenzierung

- Beide Standorte sollten für die gleiche Site-lizenzierte Funktionen lizenziert sein.
- Alle Nodes sollten für die gleichen Node-gesperrten Funktionen lizenziert sein.

Überlegungen zu SnapMirror

- Die Disaster Recovery für SnapMirror SVMs wird nur auf MetroCluster Konfigurationen mit Versionen von ONTAP 9.5 oder höher unterstützt.

MetroCluster-Vorgänge in ONTAP System Manager

Je nach ONTAP Version können einige MetroCluster spezifische Vorgänge mit ONTAP System Manager ausgeführt werden.

Weitere Informationen finden Sie im "Managen Sie MetroCluster Standorte mit System Manager" Dokumentation.

FlexCache-Unterstützung in einer MetroCluster-Konfiguration

Ab ONTAP 9.7 werden FlexCache Volumes von MetroCluster Konfigurationen unterstützt. Sie sollten die Anforderungen für die manuelle Aufhebung nach dem Switchover oder Switchback-Betrieb kennen.

SVM wird nach der Umschaltung wieder aufgehoben, wenn sich die FlexCache Herkunft und der Cache innerhalb desselben Standorts befinden. MetroCluster

Nach einer vereinbarten oder ungeplanten Umschaltung muss jede SVM-FlexCache-Peering-Beziehung innerhalb des Clusters manuell konfiguriert werden.

Beispielsweise befinden sich SVMs vs1 (Cache) und vs2 (Ursprung) auf Site_A Diese SVMs sind Peering-Punkte.

Nach der Umschaltung werden SVMs vs1-mc und vs2-mc am Partner-Standort (Site_B) aktiviert. Sie müssen manuell aufgehoben werden, damit FlexCache mit dem vserver Peer Repeer Befehl arbeiten kann.

SVM wird nach dem Switchover aufgehoben oder zurückgeschaltet, wenn sich ein FlexCache Ziel auf einem dritten Cluster befindet und sich im getrennten Modus befindet

Für FlexCache-Beziehungen zu einem Cluster außerhalb der MetroCluster-Konfiguration muss nach einem Switchover das Peering immer manuell neu konfiguriert werden, wenn die betroffenen Cluster während der Umschaltung in einem getrennten Modus sind.

Beispiel:

- Ein Ende der FlexCache (Cache_1 auf vs1) befindet sich auf MetroCluster site_A hat ein Ende der FlexCache
- Das andere Ende der FlexCache (Origin_1 auf vs2) befindet sich auf site_C (nicht in der MetroCluster-Konfiguration)

Wenn die Umschaltung ausgelöst wird und wenn Site_A und site_C nicht verbunden sind, müssen Sie die SVMs On site_B (das Switchover-Cluster) und site_C nach der Umschaltung manuell mit dem vserver Peer-Repeer-Befehl aufheben.

Wenn ein Wechsel zurück durchgeführt wird, müssen Sie die SVMs on site_A (das ursprüngliche Cluster) und site_C. erneut aufheben

Verwandte Informationen

"Management von FlexCache Volumes mit der CLI"

FabricPool-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.7 unterstützen MetroCluster Konfigurationen FabricPool Storage Tiers.

Allgemeine Informationen zur Verwendung von FabricPool finden Sie unter "Festplatten- und Tier-Management (Aggregat)".

Überlegungen bei der Verwendung von FabricPool

- Die Cluster müssen über FabricPool-Lizenzen mit entsprechenden Kapazitätslimits verfügen.
- Die Cluster müssen IPspaces mit übereinstimmenden Namen haben.

  Dies kann der standardmäßige IP-Speicherplatz sein oder ein IP-Speicherplatz, den eine Verwaltung erstellt hat. Dieser IPspace wird für die Konfiguration des FabricPool-Objektspeichers verwendet.

- Für den ausgewählten IPspace muss für jedes Cluster eine Intercluster LIF definiert sein, die zum externen Objektspeicher gelangen kann.
- FabricPool unterstützt die SVM-Migration nicht, wenn die Quelle oder das Ziel ein MetroCluster-Cluster ist.

  "Erfahren Sie mehr über SVM-Datenmobilität".

Konfigurieren eines Aggregats zur Verwendung in einer gespiegelten FabricPool

Bevor Sie das Aggregat konfigurieren, müssen Sie Objektspeichern gemäß der Beschreibung unter „Einrichten von Objektspeichern für FabricPool in einer MetroCluster-Konfiguration“ in einrichten "Festplatten- und Aggregatmanagement".

Schritte

So konfigurieren Sie ein Aggregat für die Verwendung in einem FabricPool:

1. Erstellen Sie das Aggregat oder wählen Sie ein vorhandenes Aggregat aus.
2. Spiegeln Sie das Aggregat als ein typisches gespiegeltes Aggregat innerhalb der MetroCluster Konfiguration.
3. Erstellen Sie die FabricPool Spiegelung mit dem Aggregat, wie in beschrieben "Festplatten- und Aggregatmanagement"
   a. Hängen Sie einen primären Objektspeicher an.

      Dieser Objektspeicher befindet sich physisch näher am Cluster.

   b. Fügen Sie einen Mirror-Objektspeicher hinzu.

      Dieser Objektspeicher ist physisch weiter entfernt zum Cluster als der primäre Objektspeicher.

FlexGroup-Unterstützung in MetroCluster-Konfigurationen

Ab ONTAP 9.6 unterstützen MetroCluster Konfigurationen FlexGroup Volumes.

Job-Zeitpläne in einer MetroCluster-Konfiguration

In ONTAP 9.3 und höher werden benutzererstellte Job-Zeitpläne automatisch zwischen Clustern in einer MetroCluster Konfiguration repliziert. Wenn Sie einen Job-Zeitplan auf einem Cluster erstellen, ändern oder löschen, wird derselbe Zeitplan automatisch auf dem Partner-Cluster unter Verwendung des Configuration Replication Service (CRS) erstellt.

Systemerstellte Zeitpläne werden nicht repliziert, und Sie müssen manuell denselben Vorgang auf dem Partner-Cluster durchführen, damit Job-Zeitpläne auf beiden Clustern identisch sind.

Cluster-Peering vom MetroCluster Standort zu einem dritten Cluster

Da die Peering-Konfiguration nicht repliziert wird, müssen Sie auch das Peering auf dem Partner MetroCluster Cluster konfigurieren, wenn Sie eines der Cluster in der MetroCluster Konfiguration zu einem dritten Cluster außerhalb dieser Konfiguration Peer. So bleibt Peering bei einem Switchover erhalten.

Der nicht-MetroCluster Cluster muss ONTAP 8.3 oder höher ausführen. Andernfalls geht Peering verloren, wenn ein Switchover auftritt, selbst wenn Peering für beide MetroCluster-Partner konfiguriert wurde.

Replikation der LDAP-Client-Konfiguration in einer MetroCluster-Konfiguration

Eine auf einer Storage Virtual Machine (SVM) auf einem lokalen Cluster erstellte LDAP-Client-Konfiguration wird auf die Partnerdaten-SVM auf dem Remote-Cluster repliziert. Wenn beispielsweise die LDAP-Client-Konfiguration auf der Admin-SVM auf dem lokalen Cluster erstellt wird, wird sie auf allen Admin-Daten-SVMs im Remote-Cluster repliziert. Diese MetroCluster Funktion ist vorsätzlich, sodass die LDAP-Client-Konfiguration in allen Partner-SVMs des Remote-Clusters aktiv ist.

Richtlinien zur Erstellung von Networking und LIF für MetroCluster Konfigurationen

Sie sollten beachten, wie in einer MetroCluster Konfiguration LIFs erstellt und repliziert werden. Außerdem müssen Sie über die Notwendigkeit der Konsistenz Bescheid wissen, damit Sie bei der Konfiguration Ihres Netzwerks richtige Entscheidungen treffen können.

Verwandte Informationen

"Netzwerk- und LIF-Management"

"Anforderungen für die Replikation von IPspace-Objekten und die Subnetz-Konfiguration"

"Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration"

"Anforderungen und Probleme bei der LIF-Replizierung sowie bei der Platzierung"

Anforderungen für die Replikation von IPspace-Objekten und die Subnetz-Konfiguration

Sie sollten die Anforderungen für das Replizieren von IPspace-Objekten in das Partner-Cluster sowie für die Konfiguration von Subnetzen und IPv6 in einer MetroCluster-Konfiguration kennen.

IPspace-Replizierung

Beim Replizieren von IPspace-Objekten in das Partner-Cluster müssen Sie die folgenden Richtlinien berücksichtigen:

- Die IPspace-Namen der beiden Standorte müssen übereinstimmen.
- IPspace-Objekte müssen manuell auf das Partner-Cluster repliziert werden.

  Storage Virtual Machines (SVMs), die vor der Replizierung des IPspaces erstellt und einem IPspace zugewiesen werden, werden nicht zum Partner-Cluster repliziert.

Subnetz-Konfiguration

Beim Konfigurieren von Subnetzen in einer MetroCluster-Konfiguration müssen Sie die folgenden Richtlinien berücksichtigen:

- Beide Cluster der MetroCluster-Konfiguration müssen ein Subnetz im selben IPspace mit demselben Subnetz, Subnetz, Broadcast-Domäne und Gateway aufweisen.
- Der IP-Bereich der beiden Cluster muss unterschiedlich sein.

  Im folgenden Beispiel unterscheiden sich die IP-Bereiche:

```
cluster_A::> network subnet show

IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------       -------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.11-192.168.2.20

cluster_B::> network subnet show
 IPspace: Default
Subnet                      Broadcast                    Avail/
Name      Subnet            Domain    Gateway            Total    Ranges
--------- ----------------- --------- ------------      --------
---------------
subnet1   192.168.2.0/24    Default   192.168.2.1        10/10
192.168.2.21-192.168.2.30
```

IPv6-Konfiguration

Wenn IPv6 auf einem Standort konfiguriert ist, muss IPv6 auch auf dem anderen Standort konfiguriert werden.

Verwandte Informationen

"Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration"

"Anforderungen und Probleme bei der LIF-Replizierung sowie bei der Platzierung"

Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration

Bei der Konfiguration Ihres Netzwerks in einer MetroCluster-Konfiguration sollten Sie die Anforderungen zum Erstellen von LIFs kennen.

Beim Erstellen von LIFs müssen Sie die folgenden Richtlinien beachten:

- Fibre Channel: Sie müssen gestreckte VSAN-Fabrics oder Stretched Fabrics verwenden
- IP/iSCSI: Sie müssen Layer 2-Strecked-Netzwerk verwenden
- ARP-Sendungen: Sie müssen ARP-Übertragungen zwischen den beiden Clustern aktivieren
- Doppelte LIFs: Sie müssen nicht mehrere LIFs mit derselben IP-Adresse (doppelte LIFs) in einem IPspace erstellen
- NFS- und SAN-Konfigurationen: Es müssen unterschiedliche Storage Virtual Machines (SVMs) sowohl für nicht gespiegelte als auch gespiegelte Aggregate verwendet werden
- Sie sollten ein Subnetz-Objekt erstellen, bevor Sie eine LIF erstellen. Mithilfe eines Subnetzobjekts kann ONTAP Failover-Ziele auf dem Zielcluster ermitteln, da ihm eine Broadcast-Domäne zugeordnet ist.

Überprüfen Sie die LIF-Erstellung

Sie können die erfolgreiche Erstellung einer logischen Schnittstelle in einer MetroCluster-Konfiguration bestätigen, indem Sie den MetroCluster Check lif show-Befehl ausführen. Falls beim Erstellen des LIF Probleme auftreten, können Sie den Befehl MetroCluster Check lif Repair-Placement zum Beheben von Problemen verwenden.

Verwandte Informationen

"Anforderungen für die Replikation von IPspace-Objekten und die Subnetz-Konfiguration"

"Anforderungen und Probleme bei der LIF-Replizierung sowie bei der Platzierung"

Anforderungen und Probleme bei der LIF-Replizierung sowie bei der Platzierung

Sie sollten die LIF-Replizierungsanforderungen in einer MetroCluster-Konfiguration kennen. Sie sollten auch wissen, wie eine replizierte LIF auf einem Partner-Cluster platziert ist. Beachten Sie die Probleme, die bei Ausfall der LIF-Replizierung oder der LIF-Platzierung auftreten.

Replizierung von LIFs am Partner-Cluster

Wenn Sie eine LIF auf einem Cluster in einer MetroCluster-Konfiguration erstellen, wird diese LIF im Partner-Cluster repliziert. LIFs werden nicht nach Eins-zu-Eins-Namen platziert. Für die Verfügbarkeit von LIFs nach einem Switchover überprüft der Prozess über die LIF-Platzierung, ob die Ports die LIF auf Basis von Erreichbarkeit und Port-Attributprüfungen hosten können.

Das System muss die folgenden Bedingungen erfüllen, um die replizierten LIFs auf das Partner-Cluster zu platzieren:

Zustand	LIF-Typ: FC	LIF-Typ: IP/iSCSI
Knotenidentifikation	ONTAP versucht, die replizierte LIF auf den Disaster Recovery (DR) Partner des Nodes zu platzieren, auf dem sie erstellt wurde. Falls der DR-Partner nicht verfügbar ist, wird der DR-Hilfspartner zur Platzierung verwendet.	ONTAP versucht, die replizierte LIF auf den DR-Partner des Nodes, auf dem sie erstellt wurde, zu platzieren. Falls der DR-Partner nicht verfügbar ist, wird der DR-Hilfspartner zur Platzierung verwendet.
Port-ID	ONTAP identifiziert die verbundenen FC-Ziel-Ports auf dem DR-Cluster.	Die Ports auf dem DR-Cluster, die sich im gleichen IPspace wie die Quell-LIF befinden, werden für eine Überprüfung der Erreichbarkeit ausgewählt.Wenn sich im DR-Cluster keine Ports im gleichen IPspace befinden, kann die LIF nicht platziert werden. Alle Ports im DR-Cluster, die bereits ein LIF im selben IPspace und Subnetz hosten, werden automatisch als erreichbar markiert und können zur Platzierung verwendet werden. Diese Ports sind nicht in der Überprüfung der Erreichbarkeit enthalten.

Erreichbarkeit prüfen	Die Erreichbarkeit wird dadurch bestimmt, dass die Konnektivität der Quell-Fabric-WWN auf den Ports im DR-Cluster geprüft wird.Wenn dieselbe Fabric nicht am DR-Standort vorhanden ist, wird die LIF auf einen zufälligen Port am DR-Partner platziert.	Die Erreichbarkeit wird durch die Reaktion auf ein ARP-Protokoll (Address Resolution Protocol) bestimmt, das von jedem zuvor identifizierten Port des DR-Clusters auf die Quell-IP-Adresse der zu platzierten LIF gesendet wird.um die Erreichbarkeit erfolgreich zu prüfen, müssen ARP-Übertragungen zwischen den beiden Clustern zulässig sein. Jeder Port, der eine Antwort vom Quell-LIF erhält, wird zur Platzierung so markiert.
Portauswahl	ONTAP kategorisiert die Ports anhand von Attributen wie Adaptertyp und -Geschwindigkeit und wählt dann die Ports mit übereinstimmenden Attributen aus.Wenn keine Ports mit übereinstimmenden Attributen gefunden werden, wird die LIF auf einem zufällig verbundenen Port des DR-Partners platziert.	Von den Ports, die während der Prüfung der Erreichbarkeit als erreichbar markiert sind, ONTAP bevorzugt Ports, die in der Broadcast-Domäne vorhanden sind, die mit dem Subnetz der logischen Schnittstelle verknüpft sind.Wenn im DR-Cluster keine Netzwerk-Ports verfügbar sind, die sich in der Broadcast-Domäne befinden, die mit dem Subnetz der logischen Schnittstelle verknüpft ist, Dann wählt ONTAP Ports aus, die eine Erreichbarkeit der Quell-LIF haben. Wenn keine Ports mit Reachability zur Quell-LIF vorhanden sind, wird aus der Broadcast-Domäne ein Port ausgewählt, der mit dem Subnetz der Quell-LIF verknüpft ist. Wenn keine solche Broadcast-Domäne vorhanden ist, wird ein zufälliger Port ausgewählt. ONTAP kategorisiert die Ports anhand von Attributen wie Adaptertyp, Schnittstellentyp und Geschwindigkeit und wählt dann die Ports mit übereinstimmenden Attributen aus.
LIF-Platzierung	Über die erreichbaren Ports wählt ONTAP den am wenigsten geladenen Port zur Platzierung aus.	Von den ausgewählten Ports aus wählt ONTAP den am wenigsten geladenen Port zur Platzierung aus.

Platzierung replizierter LIFs, wenn der DR-Partner-Node ausfällt

Wenn auf einem Node, dessen DR-Partner übernommen wurde, eine iSCSI- oder FC-LIF erstellt wird, wird die replizierte LIF auf den zusätzlichen DR-Partner-Knoten platziert. Nach einem nachfolgenden Giveback-Vorgang werden die LIFs nicht automatisch an den DR-Partner übertragen. Dies kann dazu führen, dass sich LIFs auf einen einzelnen Node im Partner-Cluster konzentrieren. Bei einer MetroCluster-Umschaltung versuchen Sie anschließend, die LUNs, die zur SVM (Storage Virtual Machine) gehören, zuzuordnen.

Sie sollten den ausführen `metrocluster check lif show` Befehl nach einem Takeover- oder Giveback-Vorgang, um zu überprüfen, dass die LIF-Platzierung korrekt ist. Wenn Fehler vorhanden sind, können Sie den ausführen `metrocluster check lif repair-placement` Befehl zum Beheben der Probleme.

Fehler beim LIF-Platzierung

Fehler beim LIF-Platzierung, die von angezeigt werden `metrocluster check lif show` Der Befehl bleibt

nach einem Switchover-Vorgang erhalten. Wenn der `network interface modify`, `network interface rename`, Oder `network interface delete` Befehl wird für ein LIF mit einem Platzierungsfehler ausgegeben, der Fehler wird entfernt und in der Ausgabe des wird nicht angezeigt `metrocluster check lif show` Befehl.

Fehler bei der LIF-Replizierung

Sie können außerdem prüfen, ob die LIF-Replizierung mithilfe von erfolgreich war `metrocluster check lif show` Befehl. Wenn die LIF-Replikation fehlschlägt, wird eine EMS-Meldung angezeigt.

Sie können einen Replikationsfehler beheben, indem Sie den ausführen `metrocluster check lif repair-placement` Befehl für jedes LIF, das einen korrekten Port nicht findet. Sie sollten alle LIF-Replizierungsfehler so schnell wie möglich beheben, um die Verfügbarkeit von LIF während eines MetroCluster-Switchover-Vorgangs zu überprüfen.

> Selbst wenn die Quell-SVM ausfällt, wird die LIF-Platzierung möglicherweise normal fortgesetzt, wenn in einem Port mit demselben IPspace und Netzwerk in der Ziel-SVM eine LIF zu einer anderen SVM gehört.

Verwandte Informationen

"Anforderungen für die Replikation von IPspace-Objekten und die Subnetz-Konfiguration"

"Anforderungen für die LIF-Erstellung in einer MetroCluster-Konfiguration"

Volume-Erstellung auf einem Root-Aggregat

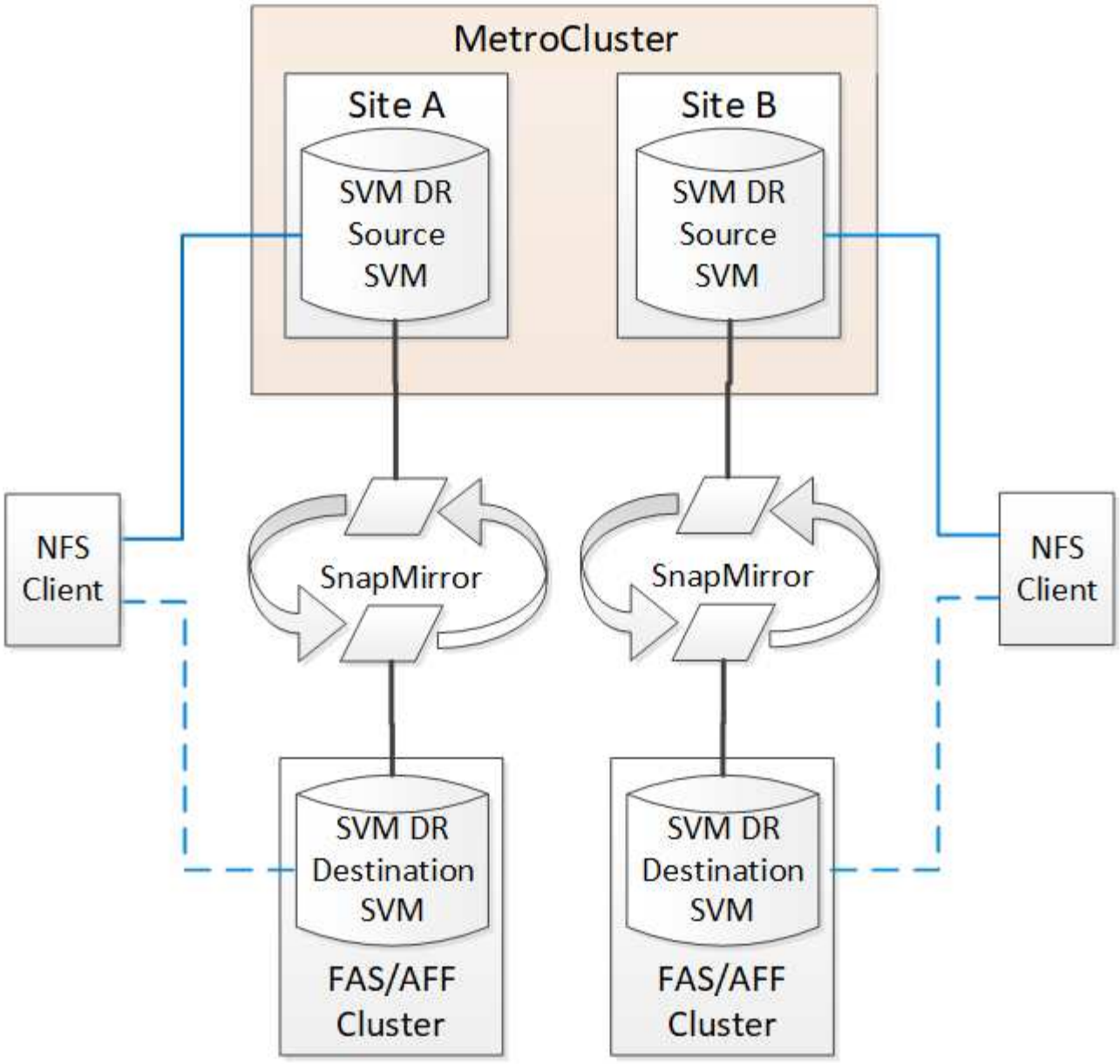
Das System lässt nicht die Erstellung neuer Volumes im Root-Aggregat (ein Aggregat mit einer HA-Richtlinie von CFO) eines Knotens in einer MetroCluster-Konfiguration zu.

Aufgrund dieser Einschränkung können Root-Aggregate mit dem nicht zu einer SVM hinzugefügt werden `vserver add-aggregates` Befehl.

SVM Disaster Recovery in einer MetroCluster-Konfiguration

Ab ONTAP 9.5 können aktive Storage Virtual Machines (SVMs) in einer MetroCluster Konfiguration als Quellen mit der Disaster-Recovery-Funktion der SnapMirror SVM verwendet werden. Ziel-SVM muss sich auf dem dritten Cluster außerhalb der MetroCluster Konfiguration befinden.

Ab ONTAP 9.11.1 können beide Standorte innerhalb einer MetroCluster-Konfiguration die Quelle für eine SVM-DR-Beziehung mit einem FAS oder einem AFF-Ziel-Cluster sein, wie im folgenden Image dargestellt.



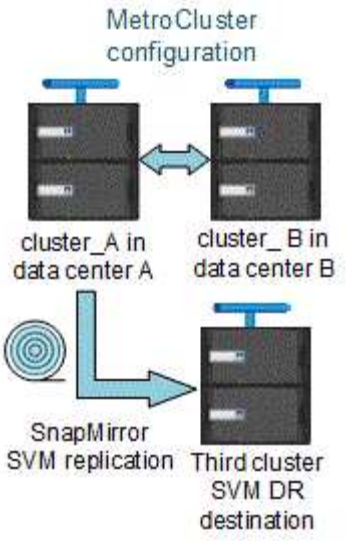
Bei der Verwendung von SVMs mit SnapMirror Disaster Recovery sollten Sie die folgenden Anforderungen und Einschränkungen beachten:

- Nur eine aktive SVM innerhalb einer MetroCluster-Konfiguration kann als Quelle einer SVM Disaster-Recovery-Beziehung verwendet werden.

  Eine Quelle kann eine synchrone Quell-SVM vor der Umschaltung oder eine synchrone Ziel-SVM nach der Umschaltung sein.

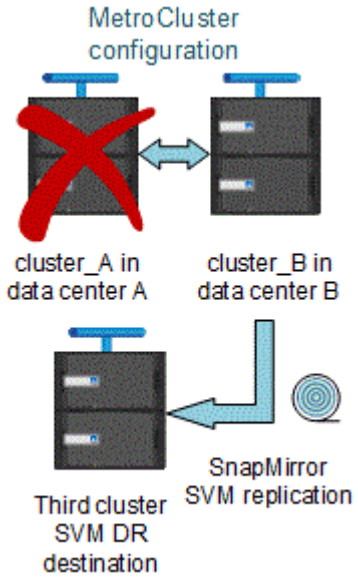
- Wenn eine MetroCluster-Konfiguration sich in einem stabilen Zustand befindet, kann die MetroCluster SVM, die synchrone Ziel-SVM, nicht als Quelle für eine SVM Disaster-Recovery-Beziehung dienen, da die Volumes nicht online sind.

  Das folgende Bild zeigt das Verhalten der SVM Disaster Recovery in einem stabilen Zustand:



- Wenn die synchrone SVM-Quelle die Quelle einer SVM-DR-Beziehung ist, werden die Quell-SVM-DR-Beziehungsinformationen zum MetroCluster Partner repliziert.

  Dadurch können die SVM-DR-Updates nach einer Umschaltung fortgesetzt werden, wie im folgenden Image dargestellt:



- Während der Switchover- und Switchover-Prozesse kann die Replizierung zur SVM-DR-Ziel fehlschlagen.

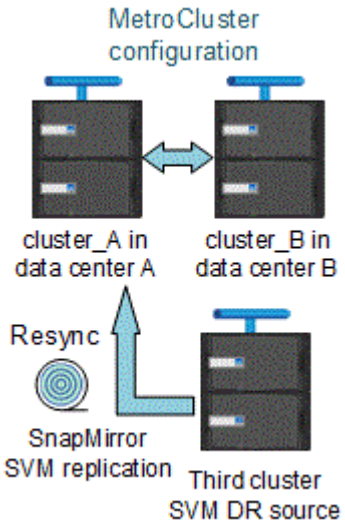
  Nach Abschluss des Switchover- oder Switch-Prozesses werden jedoch die nächsten geplanten SVM-DR-Updates erfolgreich durchgeführt.

Weitere Informationen finden Sie unter „`Replizieren der SVM-Konfiguration`“ in "Datensicherung" Weitere Informationen zur Konfiguration einer SVM-DR-Beziehung.

Neusynchronisierung der SVM an einem Disaster-Recovery-Standort

Während der Resynchronisierung wird die Disaster-Recovery-Quelle (DR) der Storage Virtual Machines (SVMs) auf der MetroCluster Konfiguration auf der Ziel-SVM auf dem Standort, der nicht von MetroCluster stammt, wiederhergestellt.

Während der Resynchronisierung fungiert die Quell-SVM (Cluster_A) als Ziel-SVM, wie in dem folgenden Image dargestellt:



Wenn während der Neusynchronisierung eine ungeplante Umschaltung erfolgt

Ungeplante Umschalt, die während der Neusynchronisierung auftreten, stoppt die Neusynchronisierung. Wenn eine ungeplante Umschaltung stattfindet, gelten die folgenden Bedingungen:

- Die Ziel-SVM auf dem MetroCluster Standort (als Quell-SVM vor der Resynchronisierung) bleibt als Ziel-SVM erhalten. Der Untertyp der SVM im Partner-Cluster bleibt weiterhin inaktiv.
- Die SnapMirror Beziehung muss manuell und als Ziel mit der SVM für das synchrone Ziel neu erstellt werden.
- Die SnapMirror Beziehung erscheint nicht in der SnapMirror-Ausgabe nach einer Umschaltung am Survivor-Standort, es sei denn, ein SnapMirror Erstellungsvorgang wird ausgeführt.

Während der Neusynchronisierung erfolgt der Wechsel zurück nach einer ungeplanten Umschaltung

Um den Switchback-Prozess erfolgreich durchzuführen, muss die Resynchronisierung-Beziehung gebrochen und gelöscht werden. Der Wechsel zurück ist nicht zulässig, wenn in der MetroCluster Konfiguration SnapMirror DR-Ziel-SVMs vorhanden sind oder wenn der Cluster über eine SVM mit dem Untertyp „`dp-Destination`“ verfügt.

Die Ausgabe des Befehls „Plex show“ für das Storage-Aggregat ist nach einer MetroCluster-Umschaltung nicht bestimmt

Wenn Sie den Befehl Storage Aggregate Plex show nach einer MetroCluster-Umschaltung ausführen, ist der Status von Plex0 des über das Root-Aggregat umgeschaltet unbestimmt und wird als fehlgeschlagen angezeigt. Während dieser Zeit wird die umschaltete Root nicht aktualisiert. Der tatsächliche Status dieses Plex kann nur nach der MetroCluster-Heilungsphase ermittelt werden.

Ändern von Volumes zum Festlegen des NV-Fehler-Flags bei Umschalten

Sie können ein Volume so ändern, dass bei einer MetroCluster-Umschaltung das NV-Fehler-Flag auf das Volume gesetzt wird. Das NVFAIL-Flag bewirkt, dass das Volumen von allen Änderungen abgetrennt wird. Dies ist für Volumes erforderlich, die so behandelt werden müssen, als würden bestimmte Schreibvorgänge auf dem Volume nach der Umschaltung verloren gehen.

In ONTAP-Versionen vor 9.0 wird für jede Umschaltung das NV-Fehler-Flag verwendet. In ONTAP 9.0 und neueren Versionen kommt die ungeplante Umschaltung (USO) zum Einsatz.

Schritt

1. Aktivieren Sie die MetroCluster-Konfiguration, um NVFAIL bei der Umschaltung auszulösen, indem Sie den einstellen `vol -dr-force-nvfail` Parameter an:

   ```
   vol modify -vserver vserver-name -volume volume-name -dr-force-nvfail on
   ```

So verwenden Sie den Active IQ Unified Manager und ONTAP System Manager für weitere Konfiguration und Monitoring

Verwenden Sie den Active IQ Unified Manager und den ONTAP System Manager für die weitere Konfiguration und Überwachung in einer MetroCluster -IP -Konfiguration

Active IQ Unified Manager und ONTAP System Manager können für das GUI-Management der Cluster und für das Monitoring der Konfiguration verwendet werden.

Auf jedem Node ist ONTAP System Manager vorinstalliert. Geben Sie zum Laden von System Manager die LIF-Adresse für das Cluster-Management als URL in einem Webbrowser, der mit dem Node verbunden ist.

Sie können die MetroCluster-Konfiguration auch mit Active IQ Unified Manager überwachen.

Verwandte Informationen

"Active IQ Unified Manager-Dokumentation"

Synchronisieren Sie die Systemzeit mit NTP in einer MetroCluster -IP-Konfiguration

Jedes Cluster benötigt einen eigenen NTP-Server (Network Time Protocol), um die Zeit zwischen den Nodes und ihren Clients zu synchronisieren.

Über diese Aufgabe

- Nach dem Takeover können Sie die Zeitzoneneinstellungen für einen ausgefallenen Node oder den Partner-Node nicht ändern.
- Jedes Cluster in der MetroCluster IP-Konfiguration sollte über einen eigenen NTP-Server oder eigene Server verfügen, die von den Nodes und IP-Switches am MetroCluster-Standort verwendet werden.
- Wenn Sie den MetroCluster Tiebreak oder ONTAP Mediator verwenden, sollte es auch einen eigenen separaten NTP-Server haben.
- Dieses Verfahren zeigt, wie Sie NTP konfigurieren, nachdem Sie die MetroCluster IP-Cluster bereits eingerichtet haben. Wenn Sie die Cluster mit System Manager konfiguriert haben, sollten Sie die NTP-Server bereits im Rahmen des Cluster-Setups konfiguriert haben. Weitere Informationen finden Sie unter "Richten Sie einen MetroCluster IP-Standort ein" .

Abhängig von Ihrer ONTAP-Version können Sie den NTP über die Registerkarte **Cluster** oder **Insights** in der Benutzeroberfläche des Systemmanagers konfigurieren.

Cluster

In System Manager können Sie den NTP auf der Registerkarte **Cluster** mit zwei verschiedenen Optionen konfigurieren, je nach ONTAP-Version:

ONTAP 9.8 oder höher:

Führen Sie die folgenden Schritte aus, um das NTP von der Registerkarte **Cluster** in ONTAP 9.8 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Wählen Sie dann die Option und dann 

Bearbeiten.
3. Wählen Sie im Fenster **Cluster-Details bearbeiten** die Option **+Hinzufügen** unter NTP-Servern aus.
4. Fügen Sie den Namen und den Speicherort hinzu, und geben Sie die IP-Adresse des Zeitservers an.
5. Wählen Sie dann **Speichern**.
6. Wiederholen Sie die Schritte für weitere Zeitserver.

ONTAP 9.11.1 oder höher:

Führen Sie die folgenden Schritte aus, um den NTP vom Fenster **Insights** auf der Registerkarte **Cluster** in ONTAP 9.11.1 oder höher zu synchronisieren.

Schritte

1. Gehen Sie zu **Cluster > Übersicht**
2. Scrollen Sie auf der Seite nach unten zum Fenster **Insights**, suchen Sie **zu wenige NTP-Server sind konfiguriert**, und wählen Sie dann **Fix IT**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

Einblick

In ONTAP 9.11.1 oder höher können Sie NTP auch über die Registerkarte **Insights** in System Manager konfigurieren:

Schritte

1. Wechseln Sie in der System Manager-Benutzeroberfläche zur Registerkarte **Insights**.
2. Scrollen Sie nach unten zu **zu wenige NTP-Server sind konfiguriert** und wählen Sie **Fix it**.
3. Geben Sie die IP-Adresse des Zeitservers ein, und wählen Sie dann **Speichern**.
4. Wiederholen Sie den vorherigen Schritt für weitere Zeitserver.

Wo Sie weitere Informationen zu MetroCluster IP finden

Weitere Informationen zur MetroCluster Konfiguration.

MetroCluster und sonstige Informationen

Informationsdaten	Betreff

"Architektur und Design der MetroCluster IP-Lösung, TR-4689"	• Eine technische Übersicht über die Konfiguration und den Betrieb der MetroCluster IP-Adresse. • Best Practices für eine MetroCluster-IP-Konfiguration.
"Installation und Konfiguration von Fabric-Attached MetroCluster"	• Fabric-Attached MetroCluster-Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der FC-Switches • Konfigurieren der MetroCluster in ONTAP
"Installation und Konfiguration von Stretch MetroCluster"	• Stretch-MetroCluster Architektur • Verkabelung der Konfiguration • Konfiguration der FC-to-SAS-Bridges • Konfigurieren der MetroCluster in ONTAP
"MetroCluster Management"	• Allgemeines zur MetroCluster-Konfiguration • Umschaltung, Heilen und zurückwechseln
"Disaster Recovery"	• Disaster Recovery • Erzwungene Umschaltung • Recovery nach einem Multi-Controller- oder Storage-Ausfall

"MetroCluster-Wartung"	• Richtlinien für die Wartung in einer MetroCluster FC-Konfiguration • Verfahren zum Austausch oder Upgrade von Hardware und Firmware-Upgrades für FC-to-SAS-Bridges und FC-Switches • Hot-hinzufügen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Hot-entfernen eines Festplatten-Shelfs in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Austausch von Hardware an einem Disaster-Standort in einer Fabric-Attached- oder Stretch-MetroCluster FC-Konfiguration • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit zwei Nodes auf eine MetroCluster Konfiguration mit vier Nodes. • Erweitern einer Fabric-Attached oder Stretch-MetroCluster FC-Konfiguration mit vier Nodes auf eine MetroCluster FC-Konfiguration mit acht Nodes
"MetroCluster Upgrade und Erweiterung"	• Aktualisierung oder Aktualisierung einer MetroCluster Konfiguration • Erweitern einer MetroCluster Konfiguration durch Hinzufügen weiterer Nodes
"MetroCluster Transition"	• Umstellung von einer MetroCluster FC-Konfiguration auf eine MetroCluster IP-Konfiguration
"MetroCluster: Upgrade, Transition und Erweiterung"	• Monitoring der MetroCluster Konfiguration mit der MetroCluster Tiebreaker Software
"Dokumentation zu ONTAP Hardwaresystemen" **Hinweis:** die standardmäßigen Speicherregal-Wartungsverfahren können mit MetroCluster IP-Konfigurationen verwendet werden.	• Hot-Adding eines Festplatten-Shelfs • Hot-entfernen eines Festplatten-Shelfs
"Kopienbasierte Transition"	• Migration von Daten von 7-Mode Storage-Systemen zu geclusterten Storage-Systemen
"ONTAP-Konzepte"	• Funktionsweise der gespiegelten Aggregate