Cisco Nexus 3132Q-V

Install and maintain

NetApp
February 13, 2026

Inhalt

Cisco Nexus 3132Q-V

Erste Schritte

Installations- und Einrichtungsworkflow für Cisco Nexus 3132Q-V-Switches

Cisco Nexus 3132Q-V Switches können als Cluster-Switches in Ihrem AFF oder FAS Cluster verwendet werden. Mit Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Knoten erstellen.

Befolgen Sie diese Arbeitsschritte, um Ihren Cisco Nexus 3132Q-V-Switch zu installieren und einzurichten.

1. **"Konfigurationsanforderungen"**
   Prüfen Sie die Konfigurationsanforderungen für den Cluster-Switch 3132Q-V.

2. **"Erforderliche Dokumentation"**
   Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 3132Q-V-Switches und den ONTAP Cluster einzurichten.

3. **"Anforderungen für Smart Call Home"**
   Überprüfen Sie die Anforderungen für die Cisco Smart Call Home-Funktion, die zur Überwachung der Hardware- und Softwarekomponenten in Ihrem Netzwerk verwendet wird.

4. **"Installieren Sie die Hardware"**
   Installieren Sie die Switch-Hardware.

5. **"Konfigurieren der Software"**
   Konfigurieren Sie die Switch-Software.

Konfigurationsanforderungen für Cisco Nexus 3132Q-V-Switches

Bei der Installation und Wartung des Cisco Nexus 3132Q-V Switches sollten Sie unbedingt die Netzwerk- und Konfigurationsanforderungen beachten.

Konfigurationsanforderungen

Zur Konfiguration Ihres Clusters benötigen Sie die entsprechende Anzahl und Art von Kabeln und Kabelverbindern für Ihre Switches. Je nach Art des Switches, den Sie initial konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Konsolenport des Switches herstellen; außerdem müssen Sie spezifische Netzwerkinformationen angeben.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie folgende Netzwerkinformationen:

- IP-Subnetz für den Verwaltungsnetzwerkverkehr.
- Hostnamen und IP-Adressen für jeden der Speichersystem-Controller und alle entsprechenden Switches.
- Die meisten Speichersystem-Controller werden über die e0M-Schnittstelle verwaltet, indem eine Verbindung zum Ethernet-Service-Port (Schraubenschlüsselsymbol) hergestellt wird. Bei den Systemen AFF A800 und AFF A700 verwendet die e0M-Schnittstelle einen dedizierten Ethernet-Anschluss.

Siehe die "Hardware Universe" für die aktuellsten Informationen. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Weitere Informationen zu den Installationsanforderungen des Schalters finden Sie hier.

Was kommt als nächstes

Nachdem Sie die Konfigurationsanforderungen geprüft haben, können Sie die "erforderliche Dokumentation"Die

Dokumentationsanforderungen für Cisco Nexus 3132Q-V-Switches

Für die Installation und Wartung des Cisco Nexus 3132Q-V Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation durchlesen.

Switch-Dokumentation

Für die Einrichtung der Cisco Nexus 3132Q-V Switches benötigen Sie die folgende Dokumentation von "Cisco Nexus 3000 Series Switches Unterstützung" Seite.

Dokumenttitel	Beschreibung
Hardware-Installationsanleitung für die Nexus 3000-Serie	Bietet detaillierte Informationen zu Standortanforderungen, Hardware-Details der Schalter und Installationsoptionen.
Softwarekonfigurationshandbücher für Cisco Nexus 3000 Series Switches (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version aus)	Liefert die grundlegenden Switch-Konfigurationsinformationen, die Sie benötigen, bevor Sie den Switch für den ONTAP -Betrieb konfigurieren können.
Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide (Wählen Sie den Leitfaden für die auf Ihren Switches installierte NX-OS-Version aus)	Bietet Informationen darüber, wie der Switch gegebenenfalls auf eine von ONTAP unterstützte Switch-Software heruntergestuft werden kann.
Cisco Nexus 3000 Serie NX-OS Befehlsreferenz – Masterindex	Bietet Links zu den verschiedenen Befehlsreferenzen von Cisco.

Dokumenttitel	Beschreibung
Cisco Nexus 3000 MIBs-Referenz	Beschreibt die Management Information Base (MIB)-Dateien für die Nexus 3000 Switches.
Referenz der NX-OS-Systemmeldungen der Nexus 3000-Serie	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 3000-Serie, sowohl die informativen als auch die, die bei der Diagnose von Problemen mit Verbindungen, interner Hardware oder der Systemsoftware hilfreich sein können.
Cisco Nexus 3000 Series NX-OS Versionshinweise (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)	Beschreibt die Funktionen, Fehler und Einschränkungen der Cisco Nexus 3000-Serie.
Informationen zu Vorschriften, Konformität und Sicherheit für die Cisco Nexus 6000-, Cisco Nexus 5000-, Cisco Nexus 3000- und Cisco Nexus 2000-Serie	Bietet Informationen zur Einhaltung internationaler behördlicher Vorschriften, zur Sicherheit und zu gesetzlichen Bestimmungen für die Switches der Nexus 3000-Serie.

ONTAP-Systemdokumentation

Um ein ONTAP -System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Version des Betriebssystems von "ONTAP 9" Die

Name	Beschreibung
Controllerspezifische *Installations- und Einrichtungsanweisungen*	Beschreibt die Installation von NetApp -Hardware.
ONTAP-Dokumentation	Bietet detaillierte Informationen zu allen Aspekten der ONTAP Releases.
"Hardware Universe"	Bietet Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Dokumentation für Schienenbausatz und Schrank

Informationen zur Installation eines Cisco 3132Q-V Switches in einem NetApp -Schrank finden Sie in der folgenden Hardware-Dokumentation.

Name	Beschreibung
"42U Systemschrank, Tiefenführung"	Beschreibt die mit dem 42U-Systemschrank verbundenen FRUs und gibt Anweisungen zur Wartung und zum Austausch der FRUs.
"Installieren Sie einen Cisco Nexus 3132Q-V Switch in einem NetApp Schrank."	Beschreibt die Installation eines Cisco Nexus 3132Q-V Switches in einem NetApp Vier-Pfosten-Schrank.

Anforderungen für Smart Call Home

Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch für die Kommunikation per E-Mail mit dem Smart Call Home-System konfigurieren. Darüber hinaus können Sie Ihren Cluster-Netzwerk-Switch optional so einrichten, dass er die integrierte Smart Call Home-Supportfunktion von Cisco nutzt.

Smart Call Home überwacht die Hardware- und Softwarekomponenten in Ihrem Netzwerk. Wenn eine kritische Systemkonfiguration auftritt, wird eine E-Mail-Benachrichtigung generiert und ein Alarm an alle Empfänger gesendet, die in Ihrem Zielprofil konfiguriert sind.

Smart Call Home überwacht die Hardware- und Softwarekomponenten in Ihrem Netzwerk. Wenn eine kritische Systemkonfiguration auftritt, wird eine E-Mail-Benachrichtigung generiert und ein Alarm an alle Empfänger gesendet, die in Ihrem Zielprofil konfiguriert sind.

Bevor Sie Smart Call Home verwenden können, beachten Sie die folgenden Anforderungen:

- Ein E-Mail-Server muss vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Kontaktname (SNMP-Server-Kontakt), die Telefonnummer und die Straßenadresse müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu ermitteln.
- Eine CCO-ID muss mit einem passenden Cisco SMARTnet Servicevertrag für Ihr Unternehmen verknüpft sein.
- Für die Registrierung des Geräts muss der Cisco SMARTnet-Dienst eingerichtet sein.

Der "Cisco Supportseite" enthält Informationen zu den Befehlen zur Konfiguration von Smart Call Home.

Installieren der Hardware

Workflow zur Hardwareinstallation für Cisco Nexus 3132Q-V-Switches

So installieren und konfigurieren Sie die Hardware für einen 3132Q-V-Cluster-Switch:

1. **"Vervollständigen Sie das Verkabelungsarbeitsblatt"**

Das Beispiel-Verkabelungs-Arbeitsblatt enthält Beispiele für empfohlene Portzuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt dient als Vorlage, die Sie beim Einrichten Ihres Clusters verwenden können.

2. **"Installieren Sie den Schalter"**

Installieren Sie den 3132Q-V-Schalter.

3. **"Installieren Sie den Switch in einem NetApp -Schrank."**

Installieren Sie den 3132Q-V-Switch und das Durchgangspanel nach Bedarf in einem NetApp Schrank.

4 **"Kabel und Konfiguration prüfen"**

Überprüfen Sie die Unterstützung für NVIDIA -Ethernet-Ports.

Vollständiges Verkabelungs-Arbeitsblatt für Cisco Nexus 3132Q-V

Wenn Sie die unterstützten Plattformen dokumentieren möchten, laden Sie eine PDF-Datei dieser Seite herunter und füllen Sie das Verkabelungsarbeitsblatt aus.

Das Beispiel-Verkabelungs-Arbeitsblatt enthält Beispiele für empfohlene Portzuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt dient als Vorlage, die Sie beim Einrichten Ihres Clusters verwenden können.

Jeder Switch kann als einzelner 40GbE-Port oder als 4 x 10GbE-Ports konfiguriert werden.

Beispiel-Verkabelungsarbeitsblatt

Die Beispiel-Portdefinition für jedes Switch-Paar lautet wie folgt:

Clusterschalter A		**Clusterschalter B**	
Switch-Port	Knoten- und Portnutzung	Switch-Port	Knoten- und Portnutzung
1	4x10G/40G-Knoten	1	4x10G/40G-Knoten
2	4x10G/40G-Knoten	2	4x10G/40G-Knoten
3	4x10G/40G-Knoten	3	4x10G/40G-Knoten
4	4x10G/40G-Knoten	4	4x10G/40G-Knoten
5	4x10G/40G-Knoten	5	4x10G/40G-Knoten
6	4x10G/40G-Knoten	6	4x10G/40G-Knoten
7	4x10G/40G-Knoten	7	4x10G/40G-Knoten
8	4x10G/40G-Knoten	8	4x10G/40G-Knoten
9	4x10G/40G-Knoten	9	4x10G/40G-Knoten
10	4x10G/40G-Knoten	10	4x10G/40G-Knoten
11	4x10G/40G-Knoten	11	4x10G/40G-Knoten
12	4x10G/40G-Knoten	12	4x10G/40G-Knoten
13	4x10G/40G-Knoten	13	4x10G/40G-Knoten

Clusterschalter A		Clusterschalter B	
14	4x10G/40G-Knoten	14	4x10G/40G-Knoten
15	4x10G/40G-Knoten	15	4x10G/40G-Knoten
16	4x10G/40G-Knoten	16	4x10G/40G-Knoten
17	4x10G/40G-Knoten	17	4x10G/40G-Knoten
18	4x10G/40G-Knoten	18	4x10G/40G-Knoten
19	40G-Knoten 19	19	40G-Knoten 19
20	40G-Knoten 20	20	40G-Knoten 20
21	40G-Knoten 21	21	40G-Knoten 21
22	40G-Knoten 22	22	40G-Knoten 22
23	40G-Knoten 23	23	40G-Knoten 23
24	40G-Knoten 24	24	40G-Knoten 24
25 bis 30	Reserviert	25 bis 30	Reserviert
31	40G ISL an Switch B Port 31	31	40G ISL an Switch A Port 31
32	40G ISL zu Switch B Port 32	32	40G ISL zu Switch A Port 32

Leeres Verkabelungsarbeitsblatt

Mithilfe des leeren Verkabelungsarbeitsblatts können Sie die Plattformen dokumentieren, die als Knoten in einem Cluster unterstützt werden. Der Abschnitt *Unterstützte Clusterverbindungen* der "Hardware Universe" Definiert die von der Plattform verwendeten Cluster-Ports.

Clusterschalter A		Clusterschalter B	
Switch-Port	Knoten-/Portnutzung	Switch-Port	Knoten-/Portnutzung
1		1	
2		2	
3		3	

Clusterschalter A		Clusterschalter B	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 bis 30	Reserviert	25 bis 30	Reserviert

Clusterschalter A		Clusterschalter B	
31	40G ISL an Switch B Port 31	31	40G ISL an Switch A Port 31
32	40G ISL zu Switch B Port 32	32	40G ISL zu Switch A Port 32

Was kommt als nächstes

Nachdem Sie Ihre Verkabelungsarbeitsblätter ausgefüllt haben, "Installieren Sie den Schalter"Die

Installieren Sie den 3132Q-V-Cluster-Switch

Befolgen Sie dieses Verfahren, um den Cisco Nexus 3132Q-V-Switch einzurichten und zu konfigurieren.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server am Installationsort, um die entsprechenden NX-OS- und Referenzkonfigurationsdatei-(RCF)-Versionen herunterzuladen.
- Anwendbare NX-OS-Version, heruntergeladen von "Cisco -Software-Download" Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.
- Vollendet"Verkabelungs-Arbeitsblätter" Die
- Anwendbare NetApp -Clusternetzwerk- und Managementnetzwerk-RCFs, die von der NetApp -Support -Website heruntergeladen wurden unter "mysupport.netapp.com" Die Alle Cisco Cluster-Netzwerk- und Management-Netzwerk-Switches werden mit der standardmäßigen Cisco -Werkskonfiguration ausgeliefert. Diese Switches verfügen ebenfalls über die aktuelle Version der NX-OS-Software, haben jedoch die RCFs nicht geladen.
- "Erforderliche Switch- und ONTAP Dokumentation".

Schritte

1. Installieren Sie die Cluster-Netzwerk- und Management-Netzwerk-Switches und -Controller.

Wenn Sie die… installieren	Dann…
Cisco Nexus 9336C-FX2 in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet*.
Ausrüstung in einem Telekommunikationsrack	Beachten Sie die in den Hardware-Installationshandbüchern für Switches und den Installations- und Einrichtungsanweisungen von NetApp beschriebenen Vorgehensweisen.

2. Verbinden Sie die Cluster-Netzwerk- und Management-Netzwerk-Switches mithilfe der ausgefüllten Verkabelungsarbeitsblätter mit den Controllern.
3. Schalten Sie die Cluster-Netzwerk- und Management-Netzwerk-Switches und -Controller ein.

Wie geht es weiter?

Optional können Sie "Installieren Sie einen Cisco Nexus 3132Q-V-Switch in einem NetApp Schrank"Die Andernfalls können Sie "Überprüfen Sie die Verkabelung und Konfiguration." Anforderungen.

Installieren Sie einen Cisco Nexus 3132Q-V Cluster-Switch in einem NetApp Schrank

Je nach Konfiguration müssen Sie möglicherweise den Cisco Nexus 3132Q-V Switch und das Pass-Through-Panel in einem NetApp -Schrank mit den standardmäßigen Halterungen installieren, die im Lieferumfang des Switches enthalten sind.

Bevor Sie beginnen

- Die anfänglichen Vorbereitungsanforderungen, der Inhalt des Kits und die Sicherheitsvorkehrungen im "Hardware-Installationshandbuch für die Cisco Nexus 3000-Serie" Die Lesen Sie diese Dokumente sorgfältig durch, bevor Sie mit dem Verfahren beginnen.
- Das Durchgangspanel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6). Das NetApp Pass-Through-Panel-Kit enthält die folgende Hardware:
  - Eine Durchgangs-Blindplatte
  - Vier 10-32 x 0,75 Schrauben
  - Vier 10-32 Clipmuttern
- Acht 10-32 oder 12-24 Schrauben und Clipmuttern zur Befestigung der Halterungen und Gleitschienen an den vorderen und hinteren Schrankpfosten.
- Cisco Standard-Schienenkit zur Installation des Switches in einem NetApp -Schrank.

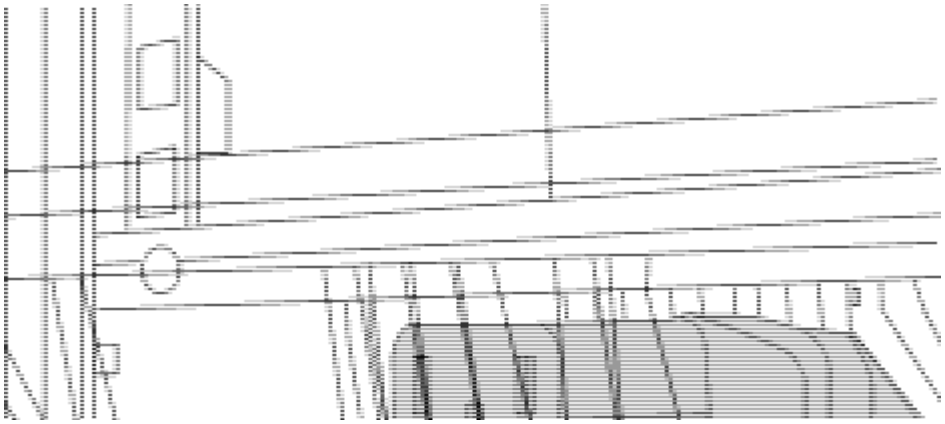
> Die Überbrückungskabel sind nicht im Durchgangskit enthalten und sollten Ihren Schaltern beiliegen. Falls sie nicht mit den Switches geliefert wurden, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

Schritte

1. Installieren Sie die Durchgangsabdeckung im NetApp -Schrank.
   a. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

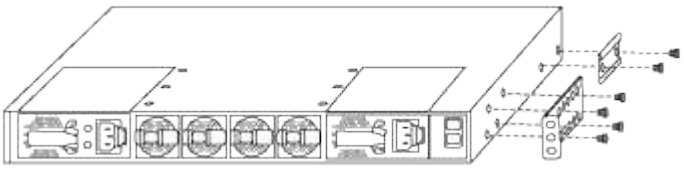
      Bei diesem Verfahren wird die Abdeckplatte in U40 installiert.

   b. Montieren Sie auf jeder Seite zwei Clipmuttern in den entsprechenden quadratischen Löchern für die vorderen Schrankschienen.
   c. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.
   d. Führen Sie die weiblichen Stecker beider 48-Zoll-Überbrückungskabel von der Rückseite des Bedienfelds durch die Bürstenbaugruppe.

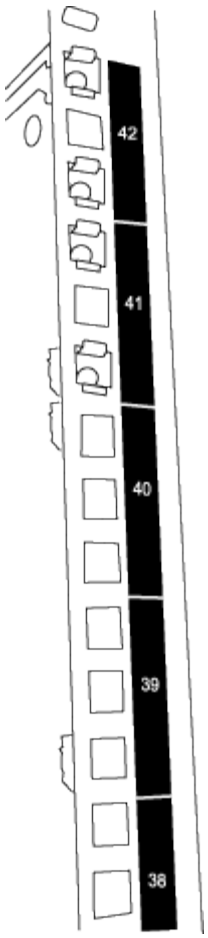


(1) Weiblicher Stecker des Überbrückungskabels.

2. Montieren Sie die Rack-Montagehalterungen am Nexus 3132Q-V Switch-Gehäuse.
   a. Positionieren Sie eine vordere Rackmontagehalterung auf einer Seite des Switch-Gehäuses, sodass die Montageöse mit der Gehäusefrontplatte (auf der Netzteil- oder Lüfterseite) ausgerichtet ist, und befestigen Sie die Halterung dann mit vier M4-Schrauben am Gehäuse.



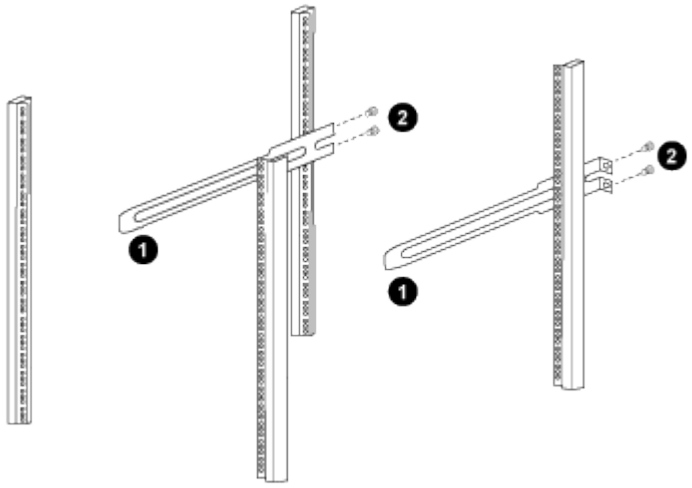
   b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.
   c. Installieren Sie die hintere Rackmontagehalterung am Switch-Gehäuse.
   d. Wiederholen Sie Schritt 2c mit der anderen hinteren Rackmontagehalterung auf der anderen Seite des Switches.
3. Installieren Sie die Clipmuttern in den quadratischen Lochpositionen für alle vier IEA-Pfosten.



Die beiden 3132Q-V-Switches werden immer in den oberen 2 HE des Schranks RU41 und 42 montiert.

4. Montieren Sie die Gleitschienen im Schrank.

   a. Positionieren Sie die erste Gleitschiene an der Markierung RU42 auf der Rückseite des linken hinteren Pfostens, setzen Sie Schrauben mit dem passenden Gewinde ein und ziehen Sie die Schrauben dann mit den Fingern fest.



   (1) Verschieben Sie die Gleitschiene vorsichtig und richten Sie sie an den Schraubenlöchern im Gestell aus.

(2) Ziehen Sie die Schrauben der Gleitschienen an den Schrankpfosten fest.

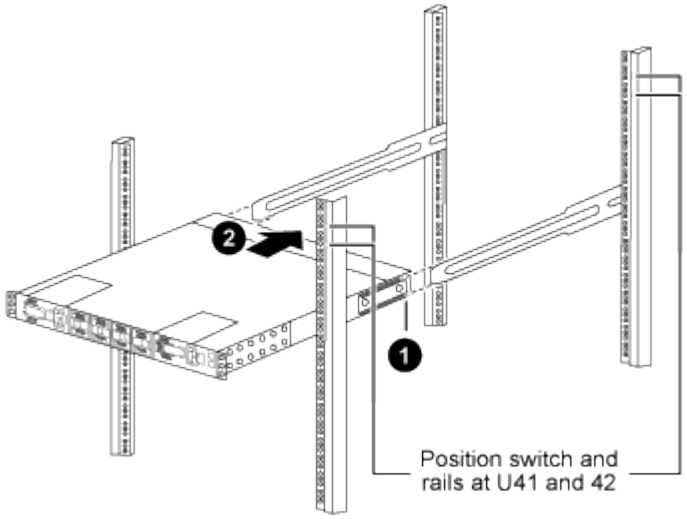
a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.

b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Positionen am Schrank.

5. Bauen Sie den Schalter in den Schrank ein.

Für diesen Schritt sind zwei Personen erforderlich: eine Person, die den Schalter von vorne stützt, und eine andere, die den Schalter in die hinteren Gleitschienen führt.

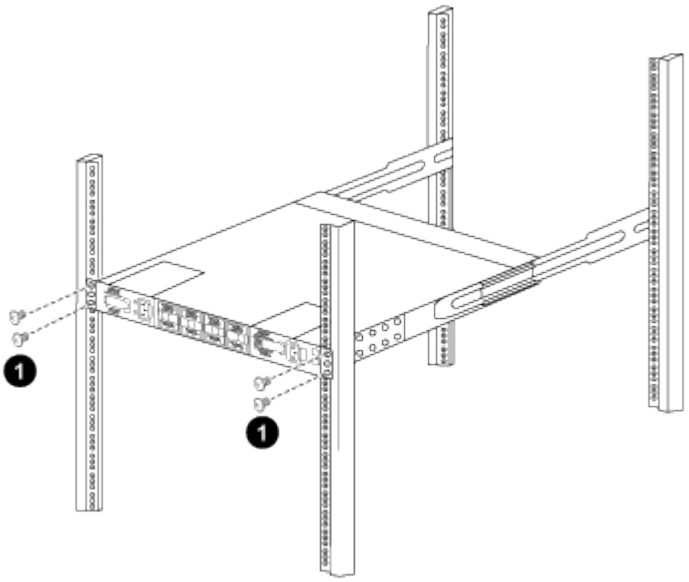
a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(1) Beim Hineinschieben des Chassis in Richtung der hinteren Pfosten müssen die beiden hinteren Rack-Montageführungen mit den Gleitschienen ausgerichtet werden.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Rack-Montagehalterungen bündig mit den vorderen Pfosten abschließen.

b. Befestigen Sie den Schalter am Gehäuse.



(1) Während eine Person die Vorderseite des Chassis waagerecht hält, sollte die andere Person die vier hinteren Schrauben an den Gehäusepfosten vollständig festziehen.

a. Wenn das Chassis nun ohne Hilfe gestützt wird, ziehen Sie die vorderen Schrauben an den Pfosten vollständig fest.

b. Wiederholen Sie die Schritte 5a bis 5c für den zweiten Schalter am Standort RU42.

> Da der bereits installierte Schalter als Stütze dient, müssen Sie die Vorderseite des zweiten Schalters während des Installationsvorgangs nicht festhalten.

6. Wenn die Schalter installiert sind, schließen Sie die Überbrückungskabel an die Stromeingänge der Schalter an.
7. Schließen Sie die Stecker beider Überbrückungskabel an die nächstgelegenen verfügbaren PDU-Steckdosen an.

> Um die Redundanz aufrechtzuerhalten, müssen die beiden Kabel an verschiedene PDUs angeschlossen werden.

8. Verbinden Sie den Management-Port jedes 3132Q-V-Switches mit einem der Management-Switches (falls bestellt) oder verbinden Sie diese direkt mit Ihrem Management-Netzwerk.

   Der Verwaltungsport ist der obere rechte Port auf der Netzteilseite des Switches. Das CAT6-Kabel für jeden Switch muss nach der Installation der Switches durch das Durchgangspanel geführt werden, um eine Verbindung zu den Verwaltungs-Switches oder dem Verwaltungsnetzwerk herzustellen.

Überprüfung der Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 3132Q-V Switch konfigurieren, beachten Sie bitte die folgenden Hinweise.

Unterstützung für NVIDIA CX6-, CX6-DX- und CX7-Ethernet-Anschlüsse

Wenn Sie einen Switch-Port mit einem ONTAP Controller über NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) oder ConnectX-7 (CX7) NIC-Ports verbinden, müssen Sie die Geschwindigkeit des Switch-Ports fest codieren.

```
(cs1)(config)# interface Ethernet1/19
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Siehe die "Hardware Universe" Weitere Informationen zu Switch-Ports finden Sie hier. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

Software konfigurieren

Workflow zur Softwareinstallation für Cisco Nexus 3132Q-V-Cluster-Switches

Um die Software für einen Cisco Nexus 3132Q-V-Switch zu installieren und zu konfigurieren und die Referenzkonfigurationsdatei (RCF) zu installieren oder zu aktualisieren, gehen Sie wie folgt vor:

1. **"Konfigurieren Sie den Schalter"**

Konfigurieren Sie den 3132Q-V-Cluster-Switch.

2. **"Bereiten Sie die Installation der NX-OS-Software und des RCF vor."**

Die Cisco NX-OS-Software und RCF müssen auf Cisco 3132Q-V-Cluster-Switches installiert werden.

3. **"Installieren oder aktualisieren Sie die NX-OS-Software."**

Laden Sie die NX-OS-Software herunter und installieren oder aktualisieren Sie sie auf dem Cisco 3132Q-V-Cluster-Switch.

4. **"Installieren oder aktualisieren Sie die RCF"**

Installieren oder aktualisieren Sie das RCF nach der Einrichtung des Cisco 3132Q-V Switches.

5. **"SSH-Konfiguration überprüfen"**

Stellen Sie sicher, dass SSH auf den Switches aktiviert ist, um den Ethernet Switch Health Monitor (CSHM) und die Protokollerfassungsfunktionen zu verwenden.

6. **"Setzen Sie den Schalter auf die Werkseinstellungen zurück."**

Löschen Sie die 3132Q-V-Cluster-Switch-Einstellungen.

Konfigurieren Sie den Cisco Nexus 3132Q-V-Switch

Gehen Sie wie folgt vor, um den Cisco Nexus 3132Q-V Switch zu konfigurieren.

Bevor Sie beginnen

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server am Installationsort, um die entsprechenden NX-OS- und Referenzkonfigurationsdatei-(RCF)-Versionen herunterzuladen.
- Anwendbare NX-OS-Version, heruntergeladen von "Cisco -Software-Download" Seite.
- Erforderliche Dokumentation für Netzwerk-Switches, Controller und ONTAP . Weitere Informationen finden Sie unter "Erforderliche Dokumentation".
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.

- Ausgefüllte Verkabelungs-Arbeitsblätter. Sehen"Vollständiges Verkabelungs-Arbeitsblatt für Cisco Nexus 3132Q-V" .
- Anwendbare NetApp Clusternetzwerk- und Managementnetzwerk-RCFs, heruntergeladen von der NetApp Support-Website unter "mysupport.netapp.com" für die Schalter, die Sie erhalten. Alle Cisco Cluster-Netzwerk- und Management-Netzwerk-Switches werden mit der standardmäßigen Cisco -Werkskonfiguration ausgeliefert. Auf diesen Switches ist auch die aktuelle Version der NX-OS-Software installiert, allerdings sind die RCFs nicht geladen.

Schritte

1. Installieren Sie die Cluster-Netzwerk- und Management-Netzwerk-Switches und -Controller.

Wenn Sie Ihr… installieren	Dann…
Cisco Nexus 3132Q-V in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden *Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet*.
Ausrüstung in einem Telekommunikationsrack	Beachten Sie die in den Hardware-Installationshandbüchern für Switches und den Installations- und Einrichtungsanweisungen von NetApp beschriebenen Vorgehensweisen.

2. Verkabeln Sie die Cluster-Netzwerk- und Management-Netzwerk-Switches mithilfe des ausgefüllten Verkabelungsarbeitsblatts wie beschrieben in"Vollständiges Verkabelungs-Arbeitsblatt für Cisco Nexus 3132Q-V" Die
3. Schalten Sie die Cluster-Netzwerk- und Management-Netzwerk-Switches und -Controller ein.
4. Führen Sie eine Erstkonfiguration der Cluster-Netzwerk-Switches durch.

   Beantworten Sie die folgenden Fragen zur Ersteinrichtung, wenn Sie den Switch zum ersten Mal einschalten. Die Sicherheitsrichtlinie Ihrer Website definiert die zu aktivierenden Antworten und Dienste.

Prompt	Antwort
Automatische Bereitstellung abbrechen und mit normaler Einrichtung fortfahren? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Nein.
Wollen Sie einen sicheren Passwortstandard erzwingen? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Ja.
Geben Sie das Passwort für den Administrator ein:	Das Standardpasswort lautet “admin”; Sie müssen ein neues, sicheres Passwort erstellen. Ein schwaches Passwort kann abgelehnt werden.
Möchten Sie den Dialog zur Basiskonfiguration aufrufen? (ja/nein)	Antworten Sie bei der Erstkonfiguration des Switches mit **ja**.

Prompt	Antwort
Ein weiteres Benutzerkonto erstellen? (ja/nein)	Die Antwort hängt von den Richtlinien Ihrer Website bezüglich alternativer Administratoren ab. Die Standardeinstellung ist **nein**.
SNMP-Community-String schreibgeschützt konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
SNMP-Community-Zeichenfolge für Lese- und Schreibzugriffe konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
Geben Sie den Namen des Schalters ein.	Der Name des Schalters ist auf 63 alphanumerische Zeichen beschränkt.
Mit der Out-of-Band-Managementkonfiguration (mgmt0) fortfahren? (ja/nein)	Antworten Sie bei dieser Eingabeaufforderung mit **ja** (Standardeinstellung). Geben Sie an der Eingabeaufforderung mgmt0 IPv4 address: Ihre IP-Adresse ein: ip_address.
Standardgateway konfigurieren? (ja/nein)	Antworten Sie mit **ja**. Geben Sie an der IPv4-Adresse des Standardgateways Ihre Standardgateway-Adresse ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
Den Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
SSH-Dienst aktiviert? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Ja. Bei der Verwendung von Ethernet Switch Health Monitor (CSHM) wird SSH aufgrund seiner Protokollierungsfunktionen empfohlen. Für erhöhte Sicherheit wird auch SSHv2 empfohlen.
Geben Sie den Typ des SSH-Schlüssels ein, den Sie generieren möchten (dsa/rsa/rsa1).	Standardmäßig wird **rsa** verwendet.
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Schlüsselbits von 1024-2048 ein.
Den NTP-Server konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.

Prompt	Antwort
Standard-Schnittstellenschicht (L3/L2) konfigurieren:	Antworte mit **L2**. Standardmäßig ist L2 eingestellt.
Standardmäßigen Schnittstellenstatus des Switch-Ports konfigurieren (ausgeschaltet/nicht ausgeschaltet):	Antworte mit **noshut**. Die Standardeinstellung ist noshut.
CoPP-Systemprofil konfigurieren (streng/moderat/tolerant/dicht):	Mit **streng** antworten. Die Standardeinstellung ist strikt.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	An dieser Stelle sollten Sie die neue Konfiguration sehen. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie gegebenenfalls die erforderlichen Änderungen vor. Antworten Sie mit **nein**, wenn Sie mit der Konfiguration zufrieden sind. Antworten Sie mit **ja**, wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Diese Konfiguration verwenden und speichern? (ja/nein)	Antworten Sie mit **ja**, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systemabbilder automatisch aktualisiert. Wenn Sie die Konfiguration in diesem Schritt nicht speichern, werden beim nächsten Neustart des Switches keine der Änderungen wirksam.

5. Überprüfen Sie die von Ihnen getroffenen Konfigurationseinstellungen in der Anzeige, die am Ende des Setups erscheint, und stellen Sie sicher, dass Sie die Konfiguration speichern.
6. Überprüfen Sie die Version auf den Cluster-Netzwerk-Switches und laden Sie gegebenenfalls die von NetApp unterstützte Softwareversion auf die Switches herunter. "Cisco -Software-Download" Seite.

Wie geht es weiter?

Nachdem Sie Ihre Schalter konfiguriert haben, "Bereiten Sie die Installation von NX-OS und RCF vor."Die

Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei vor.

Bevor Sie die NX-OS-Software und die Referenzkonfigurationsdatei (RCF) installieren, befolgen Sie bitte diese Schritte.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Knoten nutzen zwei 10GbE-Cluster-Verbindungsports. `e0a` Und `e0b` Die

Siehe die"Hardware Universe" um die korrekten Cluster-Ports auf Ihren Plattformen zu überprüfen. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

Die Befehlsausgaben können je nach ONTAP Version variieren.

Die Beispiele in diesem Verfahren verwenden die folgende Schalter- und Knotennomenklatur:

- Die Namen der beiden Cisco Switches lauten: `cs1` Und `cs2` Die
- Die Knotennamen lauten `cluster1-01` Und `cluster1-02` Die
- Die Cluster-LIF-Namen sind `cluster1-01_clus1` Und `cluster1-01_clus2` für Cluster1-01 und `cluster1-02_clus1` Und `cluster1-02_clus2` für Cluster1-02.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

Informationen zu diesem Vorgang

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

   ```
   system node autosupport invoke -node * -type all -message MAINT=xh
   ```

   wobei *x* die Dauer des Wartungsfensters in Stunden ist.

   Die AutoSupport Meldung benachrichtigt den technischen Support über diese Wartungsaufgabe, sodass die automatische Fallerstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie **y** eingeben, wenn Sie zur Fortsetzung aufgefordert werden:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung(`*>`) erscheint.

3. Zeigen Sie an, wie viele Cluster-Verbindungsschnittstellen in jedem Knoten für jeden Cluster-Verbindungs-Switch konfiguriert sind:

   ```
   network device-discovery show -protocol cdp
   ```

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N3K-
C3132Q-V
            e0b    cs2                       Eth1/2            N3K-
C3132Q-V
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N3K-
C3132Q-V
            e0b    cs2                       Eth1/1            N3K-
C3132Q-V
```

4. Prüfen Sie den administrativen oder operativen Status jeder Cluster-Schnittstelle.

   a. Netzwerkportattribute anzeigen:

      ```
      network port show –ipspace Cluster
      ```

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-02
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy
```

b. Informationen zu den LIFs anzeigen:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster

            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01   e0a     true
            cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01   e0b     true
            cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02   e0a     true
            cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02   e0b     true
```

5. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Befehl „show“ ausführen, um die Details anzuzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------
------------------- -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster1-02_clus2
none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-01_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-01_clus2
none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

`cluster ping-cluster -node <name>`

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 6]]Überprüfen Sie, ob die `auto-revert` Der Befehl ist auf allen Cluster-LIFs aktiviert:

   `network interface show -vserver Cluster -fields auto-revert`

   Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster -fields auto-
revert

          Logical
Vserver   Interface           Auto-revert
--------- ------------------- ------------
Cluster
          cluster1-01_clus1   true
          cluster1-01_clus2   true
          cluster1-02_clus1   true
          cluster1-02_clus2   true
```

Wie geht es weiter?

Nachdem Sie die Installation der NX-OS-Software und von RCF vorbereitet haben, "Installieren Sie die NX-OS-Software"Die

Installieren Sie die NX-OS-Software

Gehen Sie wie folgt vor, um die NX-OS-Software auf dem Cluster-Switch Nexus 3132Q-V zu installieren.

Überprüfungsanforderungen

Bevor Sie beginnen

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).

Empfohlene Dokumentation

- "Cisco Ethernet-Switch". In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und NX-OS-Versionen.
- "Cisco Nexus 3000 Series Switches". Die vollständige Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco -Switches finden Sie in den entsprechenden Software- und Upgrade-Anleitungen auf der Cisco -Website.

Installieren Sie die Software

Informationen zu diesem Vorgang

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Stellen Sie sicher, dass Sie den Vorgang abschließen in"Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei vor." Befolgen Sie anschließend die folgenden Schritte.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung zum Server, auf dem die NX-OS-Software und die RCF gehostet werden.

   Beispiel anzeigen

   ```
   cs2# ping 172.19.2.1 vrf management
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

4. Überprüfen Sie den administrativen und operativen Status jedes Cluster-Ports.

   a. Überprüfen Sie, ob alle Cluster-Ports **aktiv** sind und einen fehlerfreien Status aufweisen:

      `network port show -role cluster`

Beispiel anzeigen

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Überprüfen Sie, ob alle Cluster-Schnittstellen (LIFs) am Home-Port angeschlossen sind:

```
network interface show -role Cluster
```

Beispiel anzeigen

```
cluster1::*> network interface show -role Cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. Überprüfen Sie, ob der Cluster Informationen für beide Cluster-Switches anzeigt:

`system cluster-switch show -is-monitoring-enabled-operational true`

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90    N3K-
C3132Q-V
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N3K-
C3132Q-V
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

5. Automatische Wiederherstellung der Cluster-LIFs deaktivieren. Die Cluster-LIFs wechseln zum Partner-Cluster-Switch und bleiben dort, während Sie das Upgrade-Verfahren auf dem Ziel-Switch durchführen:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

6. Kopieren Sie die NX-OS-Software mithilfe eines der folgenden Übertragungsprotokolle auf den Nexus 3132Q-V Switch: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Leitfaden in "Cisco Nexus 3000 Serie NX-OS Befehlsreferenzhandbücher" Die

Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password: xxxxxxxx
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

7. Überprüfen Sie die laufende Version der NX-OS-Software:

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 04.25
NXOS: version 9.3(3)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
                NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:37]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash:   15137792 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
cs2#
```

8. Installieren Sie das NX-OS-Image.

   Durch die Installation der Image-Datei wird diese bei jedem Neustart des Switches geladen.

Beispiel anzeigen

```
cs2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 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        9.3(3)
9.3(4)               yes
     1       bios        v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)   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.
cs2#
```

9. Überprüfen Sie nach dem Neustart des Switches die neue Version der NX-OS-Software:

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 04.25
NXOS: version 9.3(4)
  BIOS compile time:  05/22/2019
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 06:28:31]


Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash:   15137792 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

10. Überprüfen Sie den Zustand der Cluster-Ports im Cluster.

    a. Überprüfen Sie, ob die Cluster-Ports auf allen Knoten im Cluster aktiv und fehlerfrei sind:

       ```
       network port show -role cluster
       ```

Beispiel anzeigen

```
cluster1::*> network port show -role cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Überprüfen Sie den Zustand der Switches im Cluster.

```
network device-discovery show -protocol cdp
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                       Type               Address
Model
---------------------------- ------------------ ----------------
------------
cs1                          cluster-network    10.233.205.90    N3K-
C3132Q-V
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                          cluster-network    10.233.205.91    N3K-
```

```
C3132Q-V
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version kann die folgende Ausgabe auf der cs1-Switch-Konsole angezeigt werden:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

11. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

    `cluster show`

    Beispiel anzeigen

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

12. Wiederholen Sie die Schritte 6 bis 11 auf Switch cs1.
13. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

    `network interface modify -vserver Cluster -lif * -auto-revert true`

14. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihren Heimatport zurückgekehrt sind:

```
network interface show -role cluster
```

Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Falls Cluster-LIFs nicht zu ihren Heimatports zurückgekehrt sind, setzen Sie sie manuell vom lokalen Knoten aus zurück:

```
network interface revert -vserver Cluster -lif <lif_name>
```

Wie geht es weiter?

Nach der Installation der NX-OS-Software können Sie "Installieren oder aktualisieren Sie die Referenzkonfigurationsdatei (RCF)."Die

Installieren oder aktualisieren Sie die RCF

Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus 3132Q-V-Switches zum ersten Mal eingerichtet haben. Sie aktualisieren Ihre RCF-Version, wenn auf Ihrem Switch eine vorhandene Version der RCF-Datei installiert ist.

Siehe den Artikel in der Wissensdatenbank."Wie man die Konfiguration eines Cisco Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält" Weitere Informationen zur Installation oder Aufrüstung Ihres RCF erhalten Sie bei Bedarf.

Verfügbare RCF-Konfigurationen

Die folgende Tabelle beschreibt die für verschiedene Konfigurationen verfügbaren RCFs. Wählen Sie den für Ihre Konfiguration passenden RCF aus.

Für spezifische Details zur Port- und VLAN-Nutzung verweisen wir auf den Abschnitt „Banner und wichtige Hinweise“ in Ihrem RCF.

RCF-Name	Beschreibung
2-Cluster-HA-Ausbruch	Unterstützt zwei ONTAP -Cluster mit mindestens acht Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
4-Cluster-HA-Ausbruch	Unterstützt vier ONTAP -Cluster mit mindestens vier Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
1-Cluster-HA	Alle Ports sind für 40/100GbE konfiguriert. Unterstützt gemeinsam genutzten Cluster-/HA-Datenverkehr auf Ports. Erforderlich für die Systeme AFF A320, AFF A250 und FAS500f . Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
1-Cluster-HA-Ausbruch	Die Ports sind für 4x10GbE Breakout, 4x25GbE Breakout (RCF 1.6+ auf 100GbE Switches) und 40/100GbE konfiguriert. Unterstützt gemeinsam genutzten Cluster-/HA-Datenverkehr auf Ports für Knoten, die gemeinsam genutzte Cluster-/HA-Ports verwenden: AFF A320, AFF A250 und FAS500f Systeme. Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
Cluster-HA-Speicher	Die Ports sind für 40/100GbE für Cluster+HA, 4x10GbE Breakout für Cluster und 4x25GbE Breakout für Cluster+HA sowie 100GbE für jedes Storage HA-Paar konfiguriert.
Cluster	Zwei Varianten von RCF mit unterschiedlicher Belegung von 4x10GbE-Ports (Breakout) und 40/100GbE-Ports. Alle FAS/ AFF -Knoten werden unterstützt, mit Ausnahme der Systeme AFF A320, AFF A250 und FAS500f .
Storage	Alle Ports sind für 100GbE NVMe-Speicherverbindungen konfiguriert.

Verfügbare RCFs

Die folgende Tabelle listet die verfügbaren RCFs für 3132Q-V-Schalter auf. Wählen Sie die für Ihre Konfiguration passende RCF-Version aus. Sehen"Cisco Ethernet-Switches" für weitere Informationen.

RCF-Name
Cluster-HA-Breakout RCF v1.*xx*
Cluster-HA RCF v1.*xx*
Cluster RCF 1.*xx*

Empfohlene Dokumentation

- "Cisco Ethernet-Switches (NSS)"

  Auf der NetApp Support-Website finden Sie die Tabelle zur Switch-Kompatibilität, in der die unterstützten ONTAP und RCF-Versionen aufgeführt sind. Beachten Sie, dass zwischen der Befehlssyntax in der RCF und der Syntax in bestimmten Versionen von NX-OS Befehlsabhängigkeiten bestehen können.

- "Cisco Nexus 3000 Series Switches"

  Die vollständige Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco -Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco -Website.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Schalter- und Knotennomenklatur:

- Die Namen der beiden Cisco Switches lauten **cs1** und **cs2**.
- Die Knotennamen lauten **cluster1-01**, **cluster1-02**, **cluster1-03** und **cluster1-04**.
- Die Cluster-LIF-Namen lauten **cluster1-01_clus1**, **cluster1-01_clus2**, **cluster1-02_clus1**, **cluster1-02_clus2**, **cluster1-03_clus1**, **cluster1-03_clus2**, **cluster1-04_clus1** und **cluster1-04_clus2**.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

Die Beispiele in diesem Verfahren verwenden vier Knoten. Diese Knoten verwenden zwei 10GbE-Cluster-Verbindungsports **e0a** und **e0b**. Siehe die "Hardware Universe" um die korrekten Cluster-Ports auf Ihren Plattformen zu überprüfen.

Die Befehlsausgaben können je nach ONTAP Version variieren.

Einzelheiten zu den verfügbaren RCF-Konfigurationen finden Sie unter"Softwareinstallations-Workflow" .

verwendete Befehle

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Wie geht es weiter?

Nachdem Sie die Schritte zur Installation oder Aktualisierung von RCF gelesen haben,"Installieren Sie den RCF" oder"Aktualisieren Sie Ihren RCF" nach Bedarf.

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus 3132Q-V-Switches zum ersten Mal eingerichtet haben.

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Der aktuelle RCF.
- Für die Installation des RCF ist eine Konsolenverbindung zum Switch erforderlich.

Informationen zu diesem Vorgang

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Während dieses Vorgangs ist kein betriebsbereiter Inter-Switch-Link (ISL) erforderlich. Dies ist beabsichtigt, da RCF-Versionsänderungen die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu ermöglichen, migriert das folgende Verfahren alle Cluster-LIFs auf den operativen Partner-Switch, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

2. Überprüfen Sie den administrativen und operativen Status jedes Cluster-Ports.

   a. Überprüfen Sie, ob alle Cluster-Ports aktiv und fehlerfrei sind:

      `network port show -ipspace Cluster`

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
Node: cluster1-03
   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
Node: cluster1-04

Ignore
                                                  Speed(Mbps)
```

```
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Überprüfen Sie, ob alle Cluster-Schnittstellen (LIFs) am Home-Port angeschlossen sind:

`network interface show -vserver Cluster`

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
cluster1::*>
```

c. Überprüfen Sie, ob der Cluster Informationen für beide Cluster-Switches anzeigt:

`system cluster-switch show -is-monitoring-enabled-operational true`

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                        Type               Address
Model
---------------------------- ------------------ ----------------
---------------
cs1                           cluster-network    10.0.0.1
NX3132QV
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP
cs2                           cluster-network    10.0.0.2
NX3132QV
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP
2 entries were displayed.
```

Für ONTAP 9.8 und höher verwenden Sie den Befehl `system switch ethernet show -is-monitoring-enabled-operational true` Die

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

Stellen Sie sicher, dass die automatische Wiederherstellung nach Ausführung dieses Befehls deaktiviert ist.

4. Schalten Sie auf dem Cluster-Switch cs2 die Ports ab, die mit den Cluster-Ports der Knoten verbunden sind.

```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit
```

Die Anzahl der angezeigten Ports variiert je nach Anzahl der Knoten im Cluster.

5. Überprüfen Sie, ob für die Cluster-Ports ein Failover auf die Ports auf dem Cluster-Switch cs1 durchgeführt wurde. Dies kann einige Sekunden dauern.

   `network interface show -vserver Cluster`

   Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

6. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
cluster1::*>
```

7. Falls Sie dies noch nicht getan haben, speichern Sie eine Kopie der aktuellen Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Textdatei kopieren:

   ```
   show running-config
   ```

8. Notieren Sie alle benutzerdefinierten Ergänzungen zwischen der aktuellen laufenden Konfiguration und der verwendeten RCF-Datei.

   Stellen Sie sicher, dass Sie Folgendes konfigurieren: * Benutzername und Passwort * Verwaltungs-IP-Adresse * Standard-Gateway * Switch-Name

9. Speichern Sie die grundlegenden Konfigurationsdetails in der `write_erase.cfg` Datei auf dem Bootflash.

   Beim Upgrade oder Anwenden eines neuen RCF müssen Sie die Switch-Einstellungen löschen und eine Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

   ```
   cs2# show run | section "switchname" > bootflash:write_erase.cfg

   cs2# show run | section "hostname" >> bootflash:write_erase.cfg

   cs2# show run | i "username admin password" >> bootflash:write_erase.cfg

   cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg

   cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
   ```

10. Bei der Installation von RCF Version 1.12 und höher führen Sie die folgenden Befehle aus:

    ```
    cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
    bootflash:write_erase.cfg

    cs2# echo "hardware access-list tcam region racl 256" >>
    bootflash:write_erase.cfg
    ```

```
cs2# echo "hardware access-list tcam region e-racl 256" >>
bootflash:write_erase.cfg

cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

Siehe den Artikel in der Wissensdatenbank. "Wie man die Konfiguration eines Cisco Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält" für weitere Einzelheiten.

11. Überprüfen Sie, ob die `write_erase.cfg` Die Datei ist wie erwartet gefüllt:

    `show file bootflash:write_erase.cfg`

12. Stellen Sie die `write erase` Befehl zum Löschen der aktuell gespeicherten Konfiguration:

    ```
    cs2# write erase

    Warning: This command will erase the startup-configuration.

    Do you wish to proceed anyway? (y/n) [n] y
    ```

13. Kopieren Sie die zuvor gespeicherte Basiskonfiguration in die Startkonfiguration.

    ```
    cs2# copy bootflash:write_erase.cfg startup-config
    ```

14. Starten Sie den Switch neu:

    ```
    cs2# reload

    This command will reboot the system. (y/n)? [n] y
    ```

15. Wiederholen Sie die Schritte 7 bis 14 auf Switch cs1.
16. Verbinden Sie die Cluster-Ports aller Knoten im ONTAP Cluster mit den Switches cs1 und cs2.

Schritt 2: Überprüfen Sie die Switch-Verbindungen

1. Überprüfen Sie, ob die mit den Cluster-Ports verbundenen Switch-Ports **aktiv** sind.

    ```
    show interface brief | grep up
    ```

Beispiel anzeigen

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none
10G(D) --
Eth1/1/2      1       eth  access up      none
10G(D) --
Eth1/7        1       eth  trunk  up      none
100G(D) --
Eth1/8        1       eth  trunk  up      none
100G(D) --
.
.
```

2. Überprüfen Sie, ob die ISL-Verbindung zwischen cs1 und cs2 funktionsfähig ist:

   `show port-channel summary`

Beispiel anzeigen

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
cs1#
```

3. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihren Heimatport zurückgekehrt sind:

   `network interface show -vserver Cluster`

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

Beispiel anzeigen

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
cluster1::*>
```

Schritt 3: Einrichten Ihres ONTAP Clusters

NetApp empfiehlt, neue Cluster mit dem System Manager einzurichten.

System Manager bietet einen einfachen und unkomplizierten Arbeitsablauf für die Einrichtung und Konfiguration des Clusters, einschließlich der Zuweisung einer IP-Adresse für die Knotenverwaltung, der Initialisierung des Clusters, der Erstellung einer lokalen Ebene, der Konfiguration von Protokollen und der Bereitstellung des anfänglichen Speichers.

Siehe"Konfigurieren Sie ONTAP auf einem neuen Cluster mit System Manager" für Einrichtungsanweisungen.

Wie geht es weiter?

Nach der Installation des RCF können Sie "Überprüfen Sie die SSH-Konfiguration"Die

Aktualisieren Sie Ihre Referenzkonfigurationsdatei (RCF)

Sie aktualisieren Ihre RCF-Version, wenn auf Ihren betriebsbereiten Switches bereits eine Version der RCF-Datei installiert ist.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Der aktuelle RCF.
- Wenn Sie Ihre RCF-Version aktualisieren, benötigen Sie eine Boot-Konfiguration in der RCF, die die gewünschten Boot-Images widerspiegelt.

  Wenn Sie die Bootkonfiguration ändern müssen, um die aktuellen Boot-Images widerzuspiegeln, müssen Sie dies tun, bevor Sie die RCF erneut anwenden, damit bei zukünftigen Neustarts die richtige Version instanziiert wird.

Während dieses Vorgangs ist kein betriebsbereiter Inter-Switch-Link (ISL) erforderlich. Dies ist beabsichtigt, da RCF-Versionsänderungen die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, migriert das folgende Verfahren alle Cluster-LIFs zum operativen Partner-Switch, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Vor der Installation einer neuen Switch-Softwareversion und neuer RCFs müssen Sie die Switch-Einstellungen löschen und eine Basiskonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein oder grundlegende Konfigurationsinformationen gesichert haben, bevor Sie die Switch-Einstellungen löschen.

Schritt 1: Vorbereitung auf das Upgrade

1. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/7       N3K-
C3132Q-V
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3132Q-V
            e0d    cs2                       Ethernet1/8       N3K-
C3132Q-V
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/1     N3K-
C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3132Q-V
            e0b    cs2                       Ethernet1/1/2     N3K-
C3132Q-V
cluster1::*>
```

2. Überprüfen Sie den administrativen und operativen Status jedes Cluster-Ports.

   a. Überprüfen Sie, ob alle Cluster-Ports aktiv und fehlerfrei sind:

      `network port show -ipspace Cluster`

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

   Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false
cluster1::*>
```

b. Überprüfen Sie, ob alle Cluster-Schnittstellen (LIFs) am Home-Port angeschlossen sind:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
cluster1::*>
```

c. Überprüfen Sie, ob der Cluster Informationen für beide Cluster-Switches anzeigt:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.0.0.1
NX3132QV
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.0.0.2
NX3132QV
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

Für ONTAP 9.8 und höher verwenden Sie den Befehl `system switch ethernet show -is-monitoring-enabled-operational true` Die

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

Stellen Sie sicher, dass die automatische Wiederherstellung nach Ausführung dieses Befehls deaktiviert ist.

Schritt 2: Ports konfigurieren

1. Schalten Sie auf dem Cluster-Switch cs2 die Ports ab, die mit den Cluster-Ports der Knoten verbunden sind.

```
cs2> enable
cs2# configure
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2# exit
```

   Die Anzahl der angezeigten Ports variiert je nach Anzahl der Knoten im Cluster.

2. Überprüfen Sie, ob für die Cluster-Ports ein Failover auf die Ports auf dem Cluster-Switch cs1 durchgeführt wurde. Dies kann einige Sekunden dauern.

   ```
   network interface show -vserver Cluster
   ```

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical           Status     Network            Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask       Node
Port    Home
----------- ----------------- ---------- ------------------
------------ ------- ----
Cluster
            cluster1-01_clus1 up/up      169.254.3.4/23
cluster1-01   e0a     true
            cluster1-01_clus2 up/up      169.254.3.5/23
cluster1-01   e0a     false
            cluster1-02_clus1 up/up      169.254.3.8/23
cluster1-02   e0a     true
            cluster1-02_clus2 up/up      169.254.3.9/23
cluster1-02   e0a     false
            cluster1-03_clus1 up/up      169.254.1.3/23
cluster1-03   e0a     true
            cluster1-03_clus2 up/up      169.254.1.1/23
cluster1-03   e0a     false
            cluster1-04_clus1 up/up      169.254.1.6/23
cluster1-04   e0a     true
            cluster1-04_clus2 up/up      169.254.1.7/23
cluster1-04   e0a     false
cluster1::*>
```

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

Beispiel anzeigen

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  -------
cluster1-01           true    true          false
cluster1-02           true    true          false
cluster1-03           true    true          true
cluster1-04           true    true          false
cluster1::*>
```

4. Falls Sie dies noch nicht getan haben, speichern Sie eine Kopie der aktuellen Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Textdatei kopieren:

   ```
   show running-config
   ```

5. Notieren Sie alle benutzerdefinierten Ergänzungen zwischen der aktuellen laufenden Konfiguration und der verwendeten RCF-Datei.

   Stellen Sie sicher, dass Sie Folgendes konfigurieren:

   - Benutzername und Passwort
   - Verwaltungs-IP-Adresse
   - Standardgateway
   - Schaltername

6. Speichern Sie die grundlegenden Konfigurationsdetails in der `write_erase.cfg` Datei auf dem Bootflash.

   Beim Upgrade oder der Anwendung eines neuen RCF müssen Sie die Schaltereinstellungen löschen und eine Grundkonfiguration durchführen.

   ```
   cs2# show run | section "switchname" > bootflash:write_erase.cfg

   cs2# show run | section "hostname" >> bootflash:write_erase.cfg

   cs2# show run | i "username admin password" >> bootflash:write_erase.cfg

   cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg

   cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
   ```

7. Beim Upgrade auf RCF Version 1.12 und höher führen Sie die folgenden Befehle aus:

   ```
   cs2# echo "hardware access-list tcam region vpc-convergence 256" >>
   bootflash:write_erase.cfg

   cs2# echo "hardware access-list tcam region racl 256" >>
   bootflash:write_erase.cfg

   cs2# echo "hardware access-list tcam region e-racl 256" >>
   bootflash:write_erase.cfg

   cs2# echo "hardware access-list tcam region qos 256" >>
   bootflash:write_erase.cfg
   ```

8. Überprüfen Sie, ob die `write_erase.cfg` Die Datei ist wie erwartet gefüllt:

   `show file bootflash:write_erase.cfg`

9. Stellen Sie die `write erase` Befehl zum Löschen der aktuell gespeicherten Konfiguration:

```
cs2# write erase

Warning: This command will erase the startup-configuration.

Do you wish to proceed anyway? (y/n) [n] y
```

10. Kopieren Sie die zuvor gespeicherte Basiskonfiguration in die Startkonfiguration.

```
cs2# copy bootflash:write_erase.cfg startup-config
```

11. Starten Sie den Switch neu:

```
cs2# reload

This command will reboot the system. (y/n)? [n] y
```

12. Sobald die Management-IP-Adresse wieder erreichbar ist, melden Sie sich über SSH am Switch an.

    Möglicherweise müssen Sie die Einträge in der Host-Datei aktualisieren, die mit den SSH-Schlüsseln zusammenhängen.

13. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs2: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Leitfaden in der"Cisco Nexus 3000 Serie NX-OS Befehlsreferenz" Leitfäden.

    Beispiel anzeigen

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server......Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

14. Wenden Sie die zuvor heruntergeladene RCF-Datei auf den Bootflash an.

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 3000 Serie NX-OS Befehlsreferenz" Führer.

    Beispiel anzeigen

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

Lesen Sie die Abschnitte **Installationshinweise**, **Wichtige Hinweise** und **Banner** Ihres RCF gründlich durch. Sie müssen diese Anweisungen lesen und befolgen, um die ordnungsgemäße Konfiguration und den ordnungsgemäßen Betrieb des Switches sicherzustellen.

15. Überprüfen Sie, ob es sich bei der RCF-Datei um die korrekte, neuere Version handelt:

    `show running-config`

    Wenn Sie die Ausgabe überprüfen, um sicherzustellen, dass Sie die richtige RCF-Datei haben, achten Sie darauf, dass die folgenden Informationen korrekt sind:

    - Das RCF-Banner
    - Die Knoten- und Porteinstellungen
    - Anpassungen

      Das Ergebnis variiert je nach Ihrer Website-Konfiguration. Prüfen Sie die Port-Einstellungen und beachten Sie die Versionshinweise, um sich über etwaige Änderungen zu informieren, die speziell für die von Ihnen installierte RCF-Version gelten.

    Schritte zum Online-Schalten Ihrer 10GbE-Ports nach einem Upgrade des RCF finden Sie im Knowledge Base-Artikel"Die 10GbE-Ports eines Cisco 3132Q Cluster-Switches werden nicht online geschaltet." .

16. Nachdem Sie überprüft haben, dass die RCF-Versionen und Switch-Einstellungen korrekt sind, kopieren Sie die `running-config` Datei in die `startup-config` Datei.

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Leitfaden in der"Cisco Nexus 3000 Serie NX-OS Befehlsreferenz" Leitfäden.

    Beispiel anzeigen

    ```
    cs2# copy running-config startup-config
    [########################################] 100% Copy complete
    ```

17. Neustart des Switches CS2. Sie können sowohl die auf den Knoten gemeldeten Ereignisse „Cluster-Ports ausgefallen“ während des Neustarts des Switches als auch den Fehler ignorieren. `% Invalid command at '^' marker` Ausgabe.

    ```
    cs2# reload
    This command will reboot the system. (y/n)?  [n] y
    ```

18. Wenden Sie alle zuvor vorgenommenen Anpassungen erneut auf die Switch-Konfiguration an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
19. Überprüfen Sie den Zustand der Cluster-Ports im Cluster.

a. Überprüfen Sie, ob die Cluster-Ports auf allen Knoten im Cluster aktiv und fehlerfrei sind:

```
network port show -ipspace Cluster
```

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster

Node: cluster1-01

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-02

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e0b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: cluster1-03

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
```

b. Überprüfen Sie den Zustand der Switches im Cluster.

```
network device-discovery show -protocol cdp
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7
N3K-C3132Q-V
            e0d    cs2                       Ethernet1/7
N3K-C3132Q-V
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8
N3K-C3132Q-V
            e0d    cs2                       Ethernet1/8
N3K-C3132Q-V
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1
N3K-C3132Q-V
            e0b    cs2                       Ethernet1/1/1
N3K-C3132Q-V
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2
N3K-C3132Q-V
            e0b    cs2                       Ethernet1/1/2
N3K-C3132Q-V

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90
N3K-C3132Q-V
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
```

```
N3K-C3132Q-V
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
```

Für ONTAP 9.8 und höher verwenden Sie den Befehl `system switch ethernet show -is-monitoring-enabled-operational true` Die

Je nach der zuvor auf dem Switch geladenen RCF-Version kann die folgende Ausgabe auf der cs1-Switch-Konsole angezeigt werden:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: Unblocking port port-channel1 on
VLAN0092. Port consistency restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

+

Es kann bis zu 5 Minuten dauern, bis die Clusterknoten als fehlerfrei gemeldet werden.

20. Schalten Sie auf dem Cluster-Switch cs1 die Ports ab, die mit den Cluster-Ports der Knoten verbunden sind.

Beispiel anzeigen

```
cs1> enable
cs1# configure
cs1(config)# interface eth1/1/1-2,eth1/7-8
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1# exit
```

Die Anzahl der angezeigten Ports variiert je nach Anzahl der Knoten im Cluster.

21. Überprüfen Sie, ob die Cluster-LIFs auf die Ports migriert wurden, die auf Switch cs2 gehostet werden. Dies kann einige Sekunden dauern.

    `network interface show -vserver Cluster`

    Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     false
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     false
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     false
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

22. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

    `cluster show`

Beispiel anzeigen

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
cluster1-01          true     true          false
cluster1-02          true     true          false
cluster1-03          true     true          true
cluster1-04          true     true          false
4 entries were displayed.
cluster1::*>
```

23. Wiederholen Sie die Schritte 1 bis 19 auf Switch cs1.
24. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

25. Neustart des Switches cs1. Dadurch werden die Cluster-LIFs veranlasst, zu ihren ursprünglichen Ports zurückzukehren. Sie können die auf den Knoten gemeldeten Ereignisse vom Typ „Cluster-Ports ausgefallen“ ignorieren, während der Switch neu startet.

```
cs1# reload
This command will reboot the system. (y/n)?  [n] y
```

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie, ob die mit den Cluster-Ports verbundenen Switch-Ports aktiv sind.

```
show interface brief | grep up
```

Beispiel anzeigen

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1       eth  access up      none
10G(D) --
Eth1/1/2      1       eth  access up      none
10G(D) --
Eth1/7        1       eth  trunk  up      none
100G(D) --
Eth1/8        1       eth  trunk  up      none
100G(D) --
.
.
```

2. Überprüfen Sie, ob die ISL-Verbindung zwischen cs1 und cs2 funktionsfähig ist:

   `show port-channel summary`

Beispiel anzeigen

```
cs1# show port-channel summary
Flags:  D - Down         P - Up in port-channel (members)
        I - Individual   H - Hot-standby (LACP only)
        s - Suspended    r - Module-removed
        b - BFD Session Wait
        S - Switched     R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
cs1#
```

3. Überprüfen Sie, ob die Cluster-LIFs zu ihren Home-Ports zurückgekehrt sind:

   `network interface show -vserver Cluster`

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
cluster1::*>
```

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

Beispiel anzeigen

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------- -------
cluster1-01          true    true          false
cluster1-02          true    true          false
cluster1-03          true    true          true
cluster1-04          true    true          false
cluster1::*>
```

5. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Befehl „show“ ausführen, um die Details anzuzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source              Destination
Packet
Node   Date                       LIF                 LIF
Loss
------ -------------------------- ------------------
------------------- -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2   cluster1-02_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2   cluster1-02_clus2
none

cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2   cluster1-01_clus1
none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2   cluster1-01_clus2
none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

`cluster ping-cluster -node <name>`

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status: ......
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Wie geht es weiter?

Nachdem Sie Ihr RCF aufgerüstet haben,"Überprüfen Sie die SSH-Konfiguration" Die

Überprüfen Sie Ihre SSH-Konfiguration

Wenn Sie die Funktionen Ethernet Switch Health Monitor (CSHM) und Protokollerfassung verwenden, überprüfen Sie, ob SSH und SSH-Schlüssel auf den Cluster-Switches aktiviert sind.

Schritte

1. Überprüfen Sie, ob SSH aktiviert ist:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Überprüfen Sie, ob die SSH-Schlüssel aktiviert sind:

```
show ssh key
```

Beispiel anzeigen

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Wenn Sie FIPS aktivieren, müssen Sie die Bitanzahl am Switch mithilfe des Befehls auf 256 ändern. `ssh key ecdsa 256 force` Die Sehen "Konfigurieren Sie die Netzwerksicherheit mithilfe von FIPS." Weitere Einzelheiten.

Wie geht es weiter?

Nachdem Sie Ihre SSH-Konfiguration überprüft haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Setzen Sie den 3132Q-V-Cluster-Switch auf die Werkseinstellungen zurück

Um den Cluster-Switch 3132Q-V auf die Werkseinstellungen zurückzusetzen, müssen Sie die Switch-Einstellungen 3132Q-V löschen.

Informationen zu diesem Vorgang

- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Diese Aufgabe setzt die Konfiguration des Managementnetzwerks zurück.

Schritte

1. Löschen Sie die vorhandene Konfiguration:

   `write erase`

   ```
   (cs2)# write erase

   Warning: This command will erase the startup-configuration.
   Do you wish to proceed anyway? (y/n) [n] y
   ```

2. Laden Sie die Switch-Software neu:

   `reload`

   ```
   (cs2)# reload

   This command will reboot the system. (y/n)? [n] y
   ```

   Das System wird neu gestartet und der Konfigurationsassistent wird aufgerufen. Wenn Sie während des Startvorgangs die Aufforderung „Auto Provisioning abbrechen und mit der normalen Einrichtung fortfahren?“ erhalten, (ja/nein)[n]“, sollten Sie mit **ja** antworten, um fortzufahren.

Was kommt als nächstes

Nach dem Zurücksetzen des Schalters können Sie"neu konfigurieren" Es wird Ihren Anforderungen entsprechend angefertigt.

Schalter migrieren

Migration von schalterlosen Clustern zu Zwei-Knoten-Clustern mit Schaltern

Workflow zur Migration von schalterlosen Clustern zu Zwei-Knoten-Clustern mit Schaltern

Befolgen Sie diese Workflow-Schritte, um von einem Zwei-Knoten-Cluster ohne Switches zu einem Zwei-Knoten-Cluster mit Switches zu migrieren, der Cisco Nexus 3132Q-V Cluster-Netzwerk-Switches enthält.

1 **"Migrationsanforderungen"**

Prüfen Sie die Anforderungen und Beispielinformationen zum Migrationsprozess.

2 **"Bereiten Sie sich auf die Migration vor"**

Bereiten Sie Ihre switchlosen Cluster auf die Migration zu Zwei-Knoten-Switch-Clustern vor.

3 **"Konfigurieren Sie Ihre Ports"**

Konfigurieren Sie Ihre Ports für die Migration von Zwei-Knoten-Clustern ohne Switches zu Zwei-Knoten-Clustern mit Switches.

4 **"Schließen Sie Ihre Migration ab."**

Schließen Sie Ihre Migration von Clustern ohne Switches zu Clustern mit zwei Knoten und Switches ab.

Migrationsanforderungen

Wenn Sie einen Zwei-Knoten-Cluster ohne Switches haben, lesen Sie bitte dieses Verfahren, um die geltenden Anforderungen für die Migration zu einem Zwei-Knoten-Cluster mit Switches zu ermitteln.

> Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Weitere Informationen finden Sie unter:

- "NetApp CN1601 und CN1610"
- "Cisco Ethernet-Switch"
- "Hardware Universe"

Port- und Knotenverbindungen

Achten Sie darauf, die Anforderungen an Port- und Knotenverbindungen sowie die Verkabelung zu verstehen, wenn Sie auf einen Zwei-Knoten-Switch-Cluster mit Cisco Nexus 3132Q-V Cluster-Switches migrieren.

- Die Cluster-Switches verwenden die Inter-Switch Link (ISL)-Ports e1/31-32.
- Der"Hardware Universe" enthält Informationen zur unterstützten Verkabelung von Nexus 3132Q-V Switches:
  - Die Knoten mit 10-GbE-Clusterverbindungen benötigen QSFP-Lichtwellenleitermodule mit Breakout-Glasfaserkabeln oder QSFP-zu-SFP+-Kupfer-Breakout-Kabel.
  - Die Knoten mit 40-GbE-Clusterverbindungen benötigen unterstützte QSFP/QSFP28-Optikmodule mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direktanschlusskabel.
  - Die Cluster-Switches verwenden die entsprechende ISL-Verkabelung: 2x QSFP28 Glasfaser- oder Kupfer-Direktanschlusskabel.

- Beim Nexus 3132Q-V können Sie die QSFP-Ports entweder im 40-Gb-Ethernet- oder im 4x10-Gb-Ethernet-Modus betreiben.

  Standardmäßig stehen im 40-GbE-Ethernet-Modus 32 Ports zur Verfügung. Diese 40-Gb-Ethernet-Ports sind nach dem 2-Tupel-Namensschema nummeriert. Beispielsweise ist der zweite 40-Gb-Ethernet-Anschluss mit 1/2 nummeriert. Der Vorgang, bei dem die Konfiguration von 40-Gb-Ethernet auf 10-Gb-Ethernet geändert wird, wird als *breakout* bezeichnet, und der Vorgang, bei dem die Konfiguration von 10-Gb-Ethernet auf 40-Gb-Ethernet geändert wird, wird als *breakin* bezeichnet. Wenn man einen 40-Gb-Ethernet-Anschluss in 10-Gb-Ethernet-Anschlüsse aufteilt, werden die resultierenden Anschlüsse nach dem 3-Tupel-Namensschema nummeriert. Beispielsweise sind die Breakout-Ports des zweiten 40-Gb-Ethernet-Ports mit 1/2/1, 1/2/2, 1/2/3 und 1/2/4 nummeriert.

- Auf der linken Seite des Nexus 3132Q-V befindet sich ein Satz von vier SFP+-Ports, die mit dem ersten QSFP-Port gemultiplext sind.

  Standardmäßig ist das RCF so konfiguriert, dass es den ersten QSFP-Port verwendet.

  Sie können vier SFP+-Ports anstelle eines QSFP-Ports für den Nexus 3132Q-V aktivieren, indem Sie die `hardware profile front portmode sfp-plus` Befehl. Ebenso können Sie den Nexus 3132Q-V so zurücksetzen, dass er anstelle von vier SFP+-Ports einen QSFP-Port verwendet, indem Sie die folgende Anleitung verwenden: `hardware profile front portmode qsfp` Befehl.

- Stellen Sie sicher, dass Sie einige der Ports am Nexus 3132Q-V für den Betrieb mit 10 GbE oder 40 GbE konfiguriert haben.

  Sie können die ersten sechs Ports im 4x10-GbE-Modus konfigurieren, indem Sie die `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Ebenso können Sie die ersten sechs QSFP+-Ports aus der Breakout-Konfiguration mithilfe der folgenden Funktion neu gruppieren: `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Die Anzahl der 10-GbE- und 40-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die unter [URL] verfügbar sind."Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen" Die

Bevor Sie beginnen

- Konfigurationen ordnungsgemäß eingerichtet und funktionsfähig.
- Knoten, auf denen ONTAP 9.4 oder höher läuft.
- Alle Cluster-Ports im `up` Zustand.
- Der Cluster-Switch Cisco Nexus 3132Q-V wird unterstützt.
- Die bestehende Cluster-Netzwerkkonfiguration weist folgende Merkmale auf:
  - Die Nexus 3132 Cluster-Infrastruktur ist redundant und auf beiden Switches voll funktionsfähig.
  - Die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.

    "Cisco Ethernet-Switches"enthält Informationen über die in diesem Verfahren unterstützten ONTAP und NX-OS-Versionen.

  - Management-Konnektivität auf beiden Switches.
  - Konsolenzugriff auf beide Switches.
  - Alle logischen Schnittstellen (LIFs) des Clusters `up` Zustand ohne Migration.
  - Erste Anpassung des Schalters.

- Alle ISL-Ports sind aktiviert und verkabelt.

Darüber hinaus müssen Sie die 10-GbE- und 40-GbE-Konnektivität von den Knoten zu den Nexus 3132Q-V Cluster-Switches planen, migrieren und die erforderliche Dokumentation dazu lesen.

Zu den verwendeten Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Schalter- und Knotennomenklatur:

- Nexus 3132Q-V Cluster-Switches, C1 und C2.
- Die Knoten sind n1 und n2.

> Die Beispiele in diesem Verfahren verwenden zwei Knoten, die jeweils zwei 40-GbE-Cluster-Verbindungsports **e4a** und **e4e** verwenden. Der"Hardware Universe" enthält Details zu den Cluster-Ports auf Ihren Plattformen.

Dieses Verfahren umfasst die folgenden Szenarien:

- **n1_clus1** ist die erste logische Clusterschnittstelle (LIF), die für den Knoten **n1** mit dem Cluster-Switch C1 verbunden wird.
- **n1_clus2** ist der erste Cluster-LIF, der mit dem Cluster-Switch C2 für den Knoten **n1** verbunden ist.
- **n2_clus1** ist der erste Cluster-LIF, der mit dem Cluster-Switch C1 für den Knoten **n2** verbunden ist.
- **n2_clus2** ist der zweite Cluster-LIF, der mit dem Cluster-Switch C2 für den Knoten **n2** verbunden werden soll.
- Die Anzahl der 10-GbE- und 40-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die unter [URL] verfügbar sind."Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen" Die

> Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

- Der Cluster startet mit zwei Knoten, die in einer Zwei-Knoten-Switchless-Cluster-Konfiguration verbunden sind und funktionieren.
- Der erste Cluster-Port wird auf C1 verschoben.
- Der zweite Cluster-Port wurde auf C2 verschoben.
- Die Option „Zwei-Knoten-Switchless-Cluster“ ist deaktiviert.

Wie geht es weiter?

Nachdem Sie die Migrationsanforderungen geprüft haben, können Sie"Bereiten Sie sich auf die Migration Ihrer Schalter vor." Die

Vorbereitung auf die Migration von schalterlosen Clustern zu geschalteten Clustern

Befolgen Sie diese Schritte, um Ihren Switchless-Cluster für die Migration zu einem Switched-Cluster mit zwei Knoten vorzubereiten.

Schritte

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

x ist die Dauer des Wartungsfensters in Stunden.

> Die AutoSupport Meldung benachrichtigt den technischen Support über diese Wartungsaufgabe, sodass die automatische Fallerstellung während des Wartungsfensters unterdrückt wird.

2. Ermitteln Sie den administrativen oder operativen Status jeder Clusterschnittstelle:

   a. Netzwerkportattribute anzeigen:

   ```
   network port show
   ```

   Beispiel anzeigen

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
4 entries were displayed.
```

b. Informationen zu den logischen Schnittstellen anzeigen:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

3. Prüfen Sie, ob die entsprechenden RCFs und das Image gemäß Ihren Anforderungen auf den neuen 3132Q-V Switches installiert sind, und nehmen Sie alle notwendigen Standortanpassungen vor, z. B. Benutzer und Passwörter, Netzwerkadressen usw.

   Sie müssen jetzt beide Schalter vorbereiten. Falls Sie die RCF- und Bildverarbeitungssoftware aktualisieren müssen, befolgen Sie bitte diese Schritte:

   a. Gehe zu"Cisco Ethernet-Switches" auf der NetApp Supportseite.
   b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
   c. Laden Sie die passende Version von RCF herunter.
   d. Wählen Sie auf der Seite **Beschreibung WEITER**, akzeptieren Sie die Lizenzvereinbarung und folgen Sie dann den Anweisungen auf der Seite **Download**, um die RCF-Datei herunterzuladen.
   e. Laden Sie die passende Version der Bildbearbeitungssoftware herunter.

4. Wählen Sie auf der Seite **Beschreibung WEITER**, akzeptieren Sie die Lizenzvereinbarung und folgen Sie dann den Anweisungen auf der Seite **Download**, um die RCF-Datei herunterzuladen.

Wie geht es weiter?

Nachdem Sie die Migration Ihrer Switches vorbereitet haben, können Sie"Konfigurieren Sie Ihre Ports" Die

Konfigurieren Sie Ihre Ports für die Migration von Clustern ohne Switches zu Clustern mit Switches.

Befolgen Sie diese Schritte, um Ihre Ports für die Migration von Zwei-Knoten-Clustern ohne Switches zu Zwei-Knoten-Clustern mit Switches zu konfigurieren.

Schritte

1. Bei den Nexus 3132Q-V Switches C1 und C2 müssen alle zum Knoten hin ausgerichteten Ports C1 und C2 deaktiviert werden, die ISL-Ports dürfen jedoch nicht deaktiviert werden.

   Beispiel anzeigen

   Das folgende Beispiel zeigt, wie die Ports 1 bis 30 auf den Nexus 3132Q-V Cluster-Switches C1 und C2 mithilfe einer in RCF unterstützten Konfiguration deaktiviert werden. `NX3132_RCF_v1.1_24p10g_26p40g.txt`:

   ```
   C1# copy running-config startup-config
   [########################################] 100%
   Copy complete.
   C1# configure
   C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
   4,e1/7-30
   C1(config-if-range)# shutdown
   C1(config-if-range)# exit
   C1(config)# exit

   C2# copy running-config startup-config
   [########################################] 100%
   Copy complete.
   C2# configure
   C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
   4,e1/7-30
   C2(config-if-range)# shutdown
   C2(config-if-range)# exit
   C2(config)# exit
   ```

2. Verbinden Sie die Ports 1/31 und 1/32 auf C1 mit den entsprechenden Ports auf C2 mithilfe von unterstützten Kabeln.
3. Überprüfen Sie, ob die ISL-Ports auf C1 und C2 betriebsbereit sind:

   ```
   show port-channel summary
   ```

Beispiel anzeigen

```
C1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)

C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

4. Zeigt die Liste der benachbarten Geräte am Switch an:

   `show cdp neighbors`

Beispiel anzeigen

```
C1# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C2                 Eth1/31        174    R S I s     N3K-C3132Q-V
Eth1/31
C2                 Eth1/32        174    R S I s     N3K-C3132Q-V
Eth1/32

Total entries displayed: 2

C2# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
C1                 Eth1/31        178    R S I s     N3K-C3132Q-V
Eth1/31
C1                 Eth1/32        178    R S I s     N3K-C3132Q-V
Eth1/32

Total entries displayed: 2
```

5. Zeigen Sie die Cluster-Port-Konnektivität auf jedem Knoten an:

   `network device-discovery show`

Beispiel anzeigen

Das folgende Beispiel zeigt eine Konfiguration eines schalterlosen Clusters mit zwei Knoten.

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e4a    n2                   e4a              FAS9000
            e4e    n2                   e4e              FAS9000
n2         /cdp
            e4a    n1                   e4a              FAS9000
            e4e    n1                   e4e              FAS9000
```

6. Migrieren Sie die clus1-Schnittstelle auf den physischen Port, der clus2 hostet:

   `network interface migrate`

   Führen Sie diesen Befehl von jedem lokalen Knoten aus.

   Beispiel anzeigen

   ```
   cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
   -source-node n1
   -destination-node n1 -destination-port e4e
   cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
   -source-node n2
   -destination-node n2 -destination-port e4e
   ```

7. Überprüfen Sie die Migration der Cluster-Schnittstellen:

   `network interface show`

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4e     false
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4e     false
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

8. Schalten Sie die Cluster-Ports clus1 LIF auf beiden Knoten ab:

   `network port modify`

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

9. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Befehl „show“ ausführen, um die Details anzuzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2        n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2        n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2        n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2        n1_clus2      none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e4a 10.10.0.1
Cluster n1_clus2 n1     e4e 10.10.0.2
Cluster n2_clus1 n2     e4a 10.10.0.3
Cluster n2_clus2 n2     e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

1. Trennen Sie das Kabel von e4a am Knoten n1.

   Sie können sich auf die laufende Konfiguration beziehen und den ersten 40-GbE-Port am Switch C1 (Port 1/7 in diesem Beispiel) mit e4a auf n1 unter Verwendung unterstützter Kabel auf Nexus 3132Q-V verbinden.

   Beim Wiederanschließen von Kabeln an einen neuen Cisco Cluster-Switch müssen die verwendeten Kabel entweder Glasfaserkabel oder von Cisco unterstützte Kabel sein.

2. Trennen Sie das Kabel von e4a am Knoten n2.

   Sie können die laufende Konfiguration konsultieren und e4a mit dem nächsten verfügbaren 40-GbE-Port auf C1, Port 1/8, unter Verwendung unterstützter Kabel verbinden.

3. Aktivieren Sie alle zum Knoten führenden Ports an C1.

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Ports 1 bis 30 auf den Nexus 3132Q-V Cluster-Switches C1 und C2 mithilfe der in RCF unterstützten Konfiguration aktiviert werden.
`NX3132_RCF_v1.1_24p10g_26p40g.txt`:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

4. Aktivieren Sie den ersten Cluster-Port, e4a, auf jedem Knoten:

   `network port modify`

   Beispiel anzeigen

   ```
   cluster::*> network port modify -node n1 -port e4a -up-admin true
   cluster::*> network port modify -node n2 -port e4a -up-admin true
   ```

5. Überprüfen Sie, ob die Cluster auf beiden Knoten aktiv sind:

   `network port show`

Beispiel anzeigen

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
4 entries were displayed.
```

6. Für jeden Knoten müssen alle migrierten Cluster-Interconnect-LIFs wiederhergestellt werden:

   `network interface revert`

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die migrierten LIFs auf ihre ursprünglichen Ports zurückgesetzt werden.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

7. Überprüfen Sie, ob alle Cluster-Verbindungsports nun wieder auf ihre ursprünglichen Ports zurückgesetzt sind:

   `network interface show`

   Der `Is Home` Die Spalte sollte einen Wert anzeigen `true` für alle in der Liste aufgeführten Häfen `Current Port` Spalte. Wenn der angezeigte Wert `false` Der Port wurde nicht wiederhergestellt.

   Beispiel anzeigen

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

8. Zeigen Sie die Cluster-Port-Konnektivität auf jedem Knoten an:

   `network device-discovery show`

Beispiel anzeigen

```
cluster::*> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3132Q-V
            e4e    n2                 e4e              FAS9000
n2         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3132Q-V
            e4e    n1                 e4e              FAS9000
```

9. Auf der Konsole jedes Knotens migrieren Sie clus2 auf Port e4a:

   `network interface migrate`

   Beispiel anzeigen

   ```
   cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
   -source-node n1
   -destination-node n1 -destination-port e4a
   cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
   -source-node n2
   -destination-node n2 -destination-port e4a
   ```

10. Schalten Sie die Cluster-Ports clus2 LIF auf beiden Knoten ab:

    `network port modify`

    Das folgende Beispiel zeigt, wie die angegebenen Ports auf beiden Knoten abgeschaltet werden:

    ```
    cluster::*> network port modify -node n1 -port e4e -up-admin false
    cluster::*> network port modify -node n2 -port e4e -up-admin false
    ```

11. Überprüfen Sie den Cluster-LIF-Status:

    `network interface show`

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4a     false
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4a     false
4 entries were displayed.
```

12. Trennen Sie das Kabel von e4e am Knoten n1.

    Sie können sich auf die laufende Konfiguration beziehen und den ersten 40-GbE-Port am Switch C2 (Port 1/7 in diesem Beispiel) mit e4e auf n1 unter Verwendung unterstützter Kabel auf Nexus 3132Q-V verbinden.

13. Trennen Sie das Kabel von e4e am Knoten n2.

    Sie können die laufende Konfiguration konsultieren und e4e mit dem nächsten verfügbaren 40-GbE-Port auf C2, Port 1/8, unter Verwendung unterstützter Kabel verbinden.

14. Aktivieren Sie alle zum Knoten führenden Ports auf C2.

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Ports 1 bis 30 auf den Nexus 3132Q-V Cluster-Switches C1 und C2 mithilfe einer in RCF unterstützten Konfiguration aktiviert werden. `NX3132_RCF_v1.1_24p10g_26p40g.txt`:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

15. Aktivieren Sie den zweiten Cluster-Port, e4e, auf jedem Knoten:

    `network port modify`

    Das folgende Beispiel zeigt, wie die angegebenen Ports aktiviert werden:

    ```
    cluster::*> network port modify -node n1 -port e4e -up-admin true
    cluster::*> network port modify -node n2 -port e4e -up-admin true
    ```

16. Für jeden Knoten müssen alle migrierten Cluster-Interconnect-LIFs wiederhergestellt werden:

    `network interface revert`

    Das folgende Beispiel zeigt, wie die migrierten LIFs auf ihre ursprünglichen Ports zurückgesetzt werden.

    ```
    cluster::*> network interface revert -vserver Cluster -lif n1_clus2
    cluster::*> network interface revert -vserver Cluster -lif n2_clus2
    ```

17. Überprüfen Sie, ob alle Cluster-Verbindungsports nun wieder auf ihre ursprünglichen Ports zurückgesetzt sind:

    `network interface show`

    Der `Is Home` Die Spalte sollte einen Wert anzeigen `true` für alle in der Liste aufgeführten Häfen `Current Port` Spalte. Wenn der angezeigte Wert `false` Der Port wurde nicht wiederhergestellt.

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e4a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e4e     true
            n2_clus1   up/up      10.10.0.3/24       n2
e4a     true
            n2_clus2   up/up      10.10.0.4/24       n2
e4e     true
4 entries were displayed.
```

18. Überprüfen Sie, ob alle Cluster-Verbindungsports im Zustand „intakt“ sind. `up` Zustand.

    `network port show -role cluster`

Beispiel anzeigen

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
4 entries were displayed.
```

Wie geht es weiter?

Nachdem Sie Ihre Switch-Ports konfiguriert haben, können Sie"Schließen Sie Ihre Migration ab." Die

Schließen Sie die Migration von Zwei-Knoten-Clustern ohne Switches zu Zwei-Knoten-Clustern mit Switches ab.

Befolgen Sie diese Schritte, um die Migration von Clustern ohne Switches zu Clustern mit zwei Knoten und Switches abzuschließen.

Schritte

1. Zeigen Sie die Cluster-Switch-Portnummern an, mit denen jeder Cluster-Port auf jedem Knoten verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
    cluster::*> network device-discovery show
             Local  Discovered
Node         Port   Device               Interface        Platform
-----------  ------ -------------------- ----------------
----------------
n1          /cdp
             e4a    C1                   Ethernet1/7      N3K-C3132Q-V
             e4e    C2                   Ethernet1/7      N3K-C3132Q-V
n2          /cdp
             e4a    C1                   Ethernet1/8      N3K-C3132Q-V
             e4e    C2                   Ethernet1/8      N3K-C3132Q-V
```

2. Anzeige der erkannten und überwachten Cluster-Switches:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
C1                          cluster-network    10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

C2                          cluster-network      10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

3. Deaktivieren Sie die Einstellungen für die schalterlose Zwei-Knoten-Konfiguration auf einem beliebigen Knoten:

   `network options switchless-cluster`

   ```
   network options switchless-cluster modify -enabled false
   ```

4. Überprüfen Sie, ob die `switchless-cluster` Diese Option wurde deaktiviert.

   ```
   network options switchless-cluster show
   ```

5. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Befehl „show“ ausführen, um die Details anzuzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2        n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2        n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2        n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2        n1_clus2      none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

```
cluster ping-cluster -node <name>
```

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e4a 10.10.0.1
Cluster n1_clus2 n1     e4e 10.10.0.2
Cluster n2_clus1 n2     e4a 10.10.0.3
Cluster n2_clus2 n2     e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

1. Wenn Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Wie geht es weiter?

Nachdem Sie Ihre Switch-Migration abgeschlossen haben, können Sie"Konfigurieren der Switch-Integritätsüberwachung" Die

Schalter austauschen

Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster-Switches

Achten Sie beim Austausch von Cluster-Switches darauf, die Konfigurationsanforderungen, Portverbindungen und Verkabelungsanforderungen zu verstehen.

Cisco Nexus 3132Q-V Anforderungen

- Der Cluster-Switch Cisco Nexus 3132Q-V wird unterstützt.

- Die Anzahl der 10-GbE- und 40-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die unter [URL] verfügbar sind."Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen" Die
- Die Cluster-Switches verwenden die Inter-Switch Link (ISL)-Ports e1/31-32.
- Der"Hardware Universe" enthält Informationen zur unterstützten Verkabelung für Nexus 3132Q-V Switches:
  - Die Knoten mit 10-GbE-Clusterverbindungen benötigen QSFP-Lichtwellenleitermodule mit Breakout-Glasfaserkabeln oder QSFP-zu-SFP+-Kupfer-Breakout-Kabel.
  - Die Knoten mit 40-GbE-Clusterverbindungen benötigen unterstützte QSFP/QSFP28-Optikmodule mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direktanschlusskabel.
  - Die Cluster-Switches verwenden die entsprechende ISL-Verkabelung: 2x QSFP28 Glasfaser- oder Kupfer-Direktanschlusskabel.
- Beim Nexus 3132Q-V können Sie die QSFP-Ports entweder im 40-Gb-Ethernet- oder im 4x10-Gb-Ethernet-Modus betreiben.

  Standardmäßig stehen im 40-GbE-Ethernet-Modus 32 Ports zur Verfügung. Diese 40-Gb-Ethernet-Ports sind nach dem 2-Tupel-Namensschema nummeriert. Beispielsweise ist der zweite 40-Gb-Ethernet-Anschluss mit 1/2 nummeriert. Der Vorgang, bei dem die Konfiguration von 40-Gb-Ethernet auf 10-Gb-Ethernet geändert wird, wird als *breakout* bezeichnet, und der Vorgang, bei dem die Konfiguration von 10-Gb-Ethernet auf 40-Gb-Ethernet geändert wird, wird als *breakin* bezeichnet. Wenn man einen 40-Gb-Ethernet-Anschluss in 10-Gb-Ethernet-Anschlüsse aufteilt, werden die resultierenden Anschlüsse nach dem 3-Tupel-Namensschema nummeriert. Beispielsweise sind die Breakout-Ports des zweiten 40-Gb-Ethernet-Ports mit 1/2/1, 1/2/2, 1/2/3 und 1/2/4 nummeriert.

- Auf der linken Seite des Nexus 3132Q-V befindet sich ein Satz von vier SFP+-Ports, die mit dem ersten QSFP-Port gemultiplext sind.

  Standardmäßig ist das RCF so konfiguriert, dass es den ersten QSFP-Port verwendet.

  Sie können vier SFP+-Ports anstelle eines QSFP-Ports für den Nexus 3132Q-V aktivieren, indem Sie die `hardware profile front portmode sfp-plus` Befehl. Ebenso können Sie den Nexus 3132Q-V so zurücksetzen, dass er anstelle von vier SFP+-Ports einen QSFP-Port verwendet, indem Sie die folgende Anleitung verwenden: `hardware profile front portmode qsfp` Befehl.

- Sie müssen einige der Ports am Nexus 3132Q-V so konfiguriert haben, dass sie mit 10 GbE oder 40 GbE laufen.

  Sie können die ersten sechs Ports im 4x10-GbE-Modus konfigurieren, indem Sie die `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Ebenso können Sie die ersten sechs QSFP+-Ports aus der Breakout-Konfiguration mithilfe der folgenden Funktion neu gruppieren: `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie müssen die Planung und Migration durchgeführt und die erforderliche Dokumentation zur 10-GbE- und 40-GbE-Konnektivität von den Knoten zu den Nexus 3132Q-V Cluster-Switches gelesen haben.

  "Cisco Ethernet-Switches"enthält Informationen über die in diesem Verfahren unterstützten ONTAP und NX-OS-Versionen.

Cisco Nexus 5596 Anforderungen

- Folgende Cluster-Switches werden unterstützt:

- Nexus 5596
- Nexus 3132Q-V

- Die Anzahl der 10-GbE- und 40-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die unter [URL] verfügbar sind."Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen" Die
- Die Cluster-Switches verwenden die folgenden Ports für die Verbindungen zu den Knoten:
  - Ports e1/1-40 (10 GbE): Nexus 5596
  - Anschlüsse e1/1-30 (40 GbE): Nexus 3132Q-V
- Die Cluster-Switches verwenden die folgenden Inter-Switch Link (ISL)-Ports:
  - Ports e1/41–48 (10 GbE): Nexus 5596
  - Anschlüsse e1/31-32 (40 GbE): Nexus 3132Q-V
- Der"Hardware Universe" enthält Informationen zur unterstützten Verkabelung von Nexus 3132Q-V Switches:
  - Knoten mit 10-GbE-Clusterverbindungen benötigen QSFP-zu-SFP+-Glasfaser-Breakout-Kabel oder QSFP-zu-SFP+-Kupfer-Breakout-Kabel.
  - Knoten mit 40-GbE-Clusterverbindungen benötigen unterstützte QSFP/QSFP28-Optikmodule mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direktanschlusskabel.
- Die Cluster-Switches verwenden die entsprechende ISL-Verkabelung:
  - Beginn: Nexus 5596 zu Nexus 5596 (SFP+ zu SFP+)
    - 8x SFP+ Glasfaser- oder Kupfer-Direktanschlusskabel
  - Interim: Nexus 5596 zu Nexus 3132Q-V (QSFP zu 4xSFP+ Breakout)
    - 1x QSFP-zu-SFP+-Glasfaser- oder Kupfer-Breakout-Kabel
  - Endgültig: Nexus 3132Q-V zu Nexus 3132Q-V (QSFP28 zu QSFP28)
    - 2x QSFP28 Glasfaser- oder Kupfer-Direktanschlusskabel
- Bei Nexus 3132Q-V Switches können Sie QSFP/QSFP28 Ports entweder im 40 Gigabit Ethernet-Modus oder im 4 x 10 Gigabit Ethernet-Modus betreiben.

  Standardmäßig stehen im 40-Gigabit-Ethernet-Modus 32 Ports zur Verfügung. Diese 40 Gigabit-Ethernet-Ports sind nach dem 2-Tupel-Namensschema nummeriert. Beispielsweise ist der zweite 40-Gigabit-Ethernet-Anschluss mit 1/2 nummeriert. Der Vorgang der Umstellung der Konfiguration von 40-Gigabit-Ethernet auf 10-Gigabit-Ethernet wird als *breakout* bezeichnet, und der Vorgang der Umstellung der Konfiguration von 10-Gigabit-Ethernet auf 40-Gigabit-Ethernet wird als *breakin* bezeichnet. Wenn man einen 40-Gigabit-Ethernet-Port in 10 Gigabit-Ethernet-Ports aufteilt, werden die resultierenden Ports nach dem 3-Tupel-Namensschema nummeriert. Beispielsweise sind die Breakout-Ports des zweiten 40-Gigabit-Ethernet-Ports mit 1/2/1, 1/2/2, 1/2/3 und 1/2/4 nummeriert.

- Auf der linken Seite der Nexus 3132Q-V Switches befindet sich ein Satz von 4 SFP+ Ports, die mit dem QSFP28 Port gemultiplext sind.

  Standardmäßig ist das RCF so konfiguriert, dass es den QSFP28-Port verwendet.

Sie können 4x SFP+-Ports anstelle eines QSFP-Ports für Nexus 3132Q-V-Switches aktivieren, indem Sie die `hardware profile front portmode sfp-plus` Befehl. Ebenso können Sie Nexus 3132Q-V-Switches so zurücksetzen, dass sie einen QSFP-Port anstelle von 4x SFP+-Ports verwenden, indem Sie Folgendes verwenden: `hardware profile front portmode qsfp` Befehl.

- Sie haben einige Ports an Nexus 3132Q-V Switches so konfiguriert, dass sie mit 10 GbE oder 40 GbE laufen.

Sie können die ersten sechs Ports in den 4x10-GbE-Modus aufteilen, indem Sie die `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Ebenso können Sie die ersten sechs QSFP+-Ports aus der Breakout-Konfiguration mithilfe der folgenden Funktion neu gruppieren: `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie haben die Planung und Migration durchgeführt und die erforderliche Dokumentation zur 10-GbE- und 40-GbE-Konnektivität von den Knoten zu den Nexus 3132Q-V Cluster-Switches gelesen.
- Die in diesem Verfahren unterstützten ONTAP und NX-OS-Versionen sind:"Cisco Ethernet-Switches" Die

NetApp CN1610 Anforderungen

- Folgende Cluster-Switches werden unterstützt:
  - NetApp CN1610
  - Cisco Nexus 3132Q-V
- Die Cluster-Switches unterstützen folgende Knotenverbindungen:
  - NetApp CN1610: Ports 0/1 bis 0/12 (10 GbE)
  - Cisco Nexus 3132Q-V: Ports e1/1-30 (40 GbE)
- Die Cluster-Switches verwenden die folgenden Inter-Switch-Link-Ports (ISL):
  - NetApp CN1610: Ports 0/13 bis 0/16 (10 GbE)
  - Cisco Nexus 3132Q-V: Ports e1/31-32 (40 GbE)
- Der"Hardware Universe" enthält Informationen zur unterstützten Verkabelung von Nexus 3132Q-V Switches:
  - Knoten mit 10-GbE-Clusterverbindungen benötigen QSFP-zu-SFP+-Glasfaser-Breakout-Kabel oder QSFP-zu-SFP+-Kupfer-Breakout-Kabel.
  - Knoten mit 40-GbE-Clusterverbindungen benötigen unterstützte QSFP/QSFP28-Optikmodule mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direktanschlusskabel.
- Die entsprechende ISL-Verkabelung sieht wie folgt aus:
  - Beginn: Für CN1610 zu CN1610 (SFP+ zu SFP+), vier SFP+ Glasfaser- oder Kupfer-Direktanschlusskabel
  - Interim: Für CN1610 zu Nexus 3132Q-V (QSFP auf vier SFP+ Breakout), ein QSFP auf SFP+ Glasfaser- oder Kupfer-Breakout-Kabel
  - Abschließend: Für Nexus 3132Q-V zu Nexus 3132Q-V (QSFP28 zu QSFP28) zwei QSFP28 Glasfaser- oder Kupfer-Direktanschlusskabel
- NetApp Twinax-Kabel sind nicht mit Cisco Nexus 3132Q-V Switches kompatibel.

Wenn Ihre aktuelle CN1610-Konfiguration NetApp Twinax-Kabel für Cluster-Node-zu-Switch-Verbindungen oder ISL-Verbindungen verwendet und Sie Twinax weiterhin in Ihrer Umgebung nutzen möchten, müssen Sie Cisco Twinax-Kabel beschaffen. Alternativ können Sie Glasfaserkabel sowohl für die ISL-Verbindungen als auch für die Verbindungen zwischen Clusterknoten und Switch verwenden.

- Bei Nexus 3132Q-V Switches können Sie QSFP/QSFP28 Ports entweder im 40-Gb-Ethernet-Modus oder im 4x 10-Gb-Ethernet-Modus betreiben.

  Standardmäßig stehen im 40-GbE-Ethernet-Modus 32 Ports zur Verfügung. Diese 40-Gb-Ethernet-Ports sind nach dem 2-Tupel-Namensschema nummeriert. Beispielsweise ist der zweite 40-Gb-Ethernet-Anschluss mit 1/2 nummeriert. Der Vorgang, bei dem die Konfiguration von 40-Gb-Ethernet auf 10-Gb-Ethernet geändert wird, wird als *breakout* bezeichnet, und der Vorgang, bei dem die Konfiguration von 10-Gb-Ethernet auf 40-Gb-Ethernet geändert wird, wird als *breakin* bezeichnet. Wenn man einen 40-Gb-Ethernet-Anschluss in 10-Gb-Ethernet-Anschlüsse aufteilt, werden die resultierenden Anschlüsse nach dem 3-Tupel-Namensschema nummeriert. Beispielsweise sind die Breakout-Ports des zweiten 40-Gb-Ethernet-Ports mit 1/2/1, 1/2/2, 1/2/3 und 1/2/4 nummeriert.

- Auf der linken Seite der Nexus 3132Q-V Switches befindet sich ein Satz von vier SFP+ Ports, die mit dem ersten QSFP Port gemultiplext sind.

  Standardmäßig ist die Referenzkonfigurationsdatei (RCF) so strukturiert, dass der erste QSFP-Port verwendet wird.

  Sie können vier SFP+-Ports anstelle eines QSFP-Ports für Nexus 3132Q-V-Switches aktivieren, indem Sie die `hardware profile front portmode sfp-plus` Befehl. Ebenso können Sie Nexus 3132Q-V-Switches so zurücksetzen, dass sie einen QSFP-Port anstelle von vier SFP+-Ports verwenden, indem Sie die folgende Methode verwenden: `hardware profile front portmode qsfp` Befehl.

  > ⓘ Wenn Sie die ersten vier SFP+-Ports verwenden, wird der erste 40GbE QSFP-Port deaktiviert.

- Sie müssen einige Ports an den Nexus 3132Q-V Switches so konfiguriert haben, dass sie mit 10 GbE oder 40 GbE laufen.

  Sie können die ersten sechs Ports in den 4x10-GbE-Modus aufteilen, indem Sie die `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Ebenso können Sie die ersten sechs QSFP+-Ports aus der *breakout*-Konfiguration mithilfe der folgenden Funktion neu gruppieren: `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie müssen die Planung und Migration durchgeführt und die erforderliche Dokumentation zur 10-GbE- und 40-GbE-Konnektivität von den Knoten zu den Nexus 3132Q-V Cluster-Switches gelesen haben.
- Die in diesem Verfahren unterstützten ONTAP und NX-OS-Versionen sind aufgelistet auf"Cisco Ethernet-Switches" Die
- Die in diesem Verfahren unterstützten ONTAP und FASTPATH-Versionen sind aufgelistet auf"NetApp CN1601 und CN1610 Switches" Die

Ersetzen Sie die Cisco Nexus 3132Q-V Cluster-Switches

Gehen Sie wie folgt vor, um einen defekten Cisco Nexus 3132Q-V Switch in einem Clusternetzwerk auszutauschen. Der Austauschvorgang ist ein nicht-invasiver Vorgang (NDO).

Überprüfungsanforderungen

Anforderungen an die Schalter

Überprüfen Sie die"Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster-Switches" Die

Bevor Sie beginnen

- Die bestehende Cluster- und Netzwerkkonfiguration umfasst Folgendes:
  - Die Nexus 3132Q-V Cluster-Infrastruktur ist redundant und auf beiden Switches voll funktionsfähig.

    "Cisco Ethernet-Switch"verfügt über die neuesten RCF- und NX-OS-Versionen für Ihre Switches.

  - Alle Cluster-Ports befinden sich im `up` Zustand.
  - Die Management-Konnektivität ist auf beiden Switches vorhanden.
  - Alle logischen Schnittstellen (LIFs) des Clusters befinden sich in der `up` Bundesstaat und sind migriert worden.
- Für den Austausch des Schalters Nexus 3132Q-V ist Folgendes zu beachten:
  - Die Management-Netzwerkanbindung des Ersatz-Switches ist funktionsfähig.
  - Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
  - Das gewünschte RCF- und NX-OS-Betriebssystem-Image wird auf den Switch geladen.
  - Die erste Konfiguration des Schalters ist abgeschlossen.
- "Hardware Universe"

Konsolenprotokollierung aktivieren

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den verwendeten Geräten zu aktivieren und beim Austausch Ihres Switches die folgenden Maßnahmen zu ergreifen:

- Lassen Sie AutoSupport während der Wartungsarbeiten aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs AutoSupport aus, um die Fallerstellung für die Dauer der Wartung zu deaktivieren. Siehe diesen Wissensdatenbankartikel"SU92: Wie man die automatische Fallerstellung während geplanter Wartungsfenster unterdrückt" für weitere Einzelheiten.
- Aktivieren Sie die Sitzungsprotokollierung für alle CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Wissensdatenbankartikel."Wie konfiguriert man PuTTY für eine optimale Verbindung zu ONTAP -Systemen?" Die

Tauschen Sie den Schalter aus.

Bei diesem Verfahren wird der zweite Nexus 3132Q-V Cluster-Schalter CL2 durch einen neuen 3132Q-V Schalter C2 ersetzt.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Schalter- und Knotennomenklatur:

- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die mit dem Cluster-Switch C1 für Knoten n1 verbunden ist.
- n1_clus2 ist der erste Cluster-LIF, der mit dem Cluster-Switch CL2 oder C2 für Knoten n1 verbunden ist.
- n1_clus3 ist die zweite LIF, die mit dem Cluster-Switch C2 für Knoten n1 verbunden ist.

- n1_clus4 ist die zweite LIF, die mit dem Cluster-Switch CL1 für Knoten n1 verbunden ist.
- Die Anzahl der 10-GbE- und 40-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die unter [URL] verfügbar sind."Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen" Die
- Die Knoten sind n1, n2, n3 und n4. - Die Beispiele in diesem Verfahren verwenden vier Knoten: Zwei Knoten verwenden vier 10 GB Cluster-Verbindungsports: e0a, e0b, e0c und e0d. Die anderen beiden Knoten verwenden zwei 40-GB-Cluster-Interconnect-Ports: e4a und e4e. Siehe die"Hardware Universe" für die tatsächlichen Cluster-Ports auf Ihren Plattformen.

Informationen zu diesem Vorgang

Dieses Verfahren umfasst folgendes Szenario:

- Der Cluster beginnt mit vier Knoten, die mit zwei Nexus 3132Q-V Cluster-Switches, CL1 und CL2, verbunden sind.
- Der Cluster-Schalter CL2 soll durch C2 ersetzt werden.
  - Auf jedem Knoten werden die mit CL2 verbundenen Cluster-LIFs auf die mit CL1 verbundenen Cluster-Ports migriert.
  - Trennen Sie die Verkabelung von allen Ports an CL2 und schließen Sie die Verkabelung an die gleichen Ports am Ersatz-Switch C2 an.
  - Auf jedem Knoten werden die migrierten Cluster-LIFs zurückgesetzt.

Schritt 1: Vorbereitung auf den Austausch

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

   ```
   system node autosupport invoke -node * -type all - message MAINT=xh
   ```

   x ist die Dauer des Wartungsfensters in Stunden.

   > Die AutoSupport Meldung benachrichtigt den technischen Support über diese Wartungsaufgabe, sodass die automatische Fallerstellung während des Wartungsfensters unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

   ```
   network device-discovery show
   ```

Beispiel anzeigen

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface         Platform
----------- ------ ------------------- ----------------
----------------
n1         /cdp
            e0a    CL1                 Ethernet1/1/1    N3K-C3132Q-V
            e0b    CL2                 Ethernet1/1/1    N3K-C3132Q-V
            e0c    CL2                 Ethernet1/1/2    N3K-C3132Q-V
            e0d    CL1                 Ethernet1/1/2    N3K-C3132Q-V
n2         /cdp
            e0a    CL1                 Ethernet1/1/3    N3K-C3132Q-V
            e0b    CL2                 Ethernet1/1/3    N3K-C3132Q-V
            e0c    CL2                 Ethernet1/1/4    N3K-C3132Q-V
            e0d    CL1                 Ethernet1/1/4    N3K-C3132Q-V
n3         /cdp
            e4a    CL1                 Ethernet1/7      N3K-C3132Q-V
            e4e    CL2                 Ethernet1/7      N3K-C3132Q-V
n4         /cdp
            e4a    CL1                 Ethernet1/8      N3K-C3132Q-V
            e4e    CL2                 Ethernet1/8      N3K-C3132Q-V

12 entries were displayed
```

3. Ermitteln Sie den administrativen oder operativen Status jeder Clusterschnittstelle:

   a. Netzwerkportattribute anzeigen:

      ```
      network port show
      ```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
       (network port show)

Node: n1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                  Speed(Mbps)
Health   Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                   Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

b. Informationen zu den logischen Schnittstellen anzeigen:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
       (network interface show)

             Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------
------------- ------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e0a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e0e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e0a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e0e     true

12 entries were displayed.
```

c. Zeigen Sie die Informationen zu den gefundenen Cluster-Switches an:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network   10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL2                          cluster-network   10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

2 entries were displayed.
```

4. Vergewissern Sie sich, dass die entsprechende RCF-Datei und das entsprechende Image gemäß Ihren Anforderungen auf dem neuen Nexus 3132Q-V Switch installiert sind, und nehmen Sie alle notwendigen Standortanpassungen vor.

   Sie müssen jetzt den Ersatzschalter vorbereiten. Falls Sie die RCF-Datei und das Image aktualisieren müssen, befolgen Sie bitte diese Schritte:

   a. Auf der NetApp Supportseite finden Sie weitere Informationen."Cisco Ethernet-Switches" Die
   b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
   c. Laden Sie die passende Version der RCF herunter.
   d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und folgen Sie dann den Anweisungen auf der Seite **Download**, um die RCF-Datei herunterzuladen.
   e. Laden Sie die passende Version der Bildbearbeitungssoftware herunter.
5. Migrieren Sie die LIFs, die den mit Switch C2 verbundenen Cluster-Ports zugeordnet sind:

```
network interface migrate
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass die LIF-Migration auf allen Knoten durchgeführt wird:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 –destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 –destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 –destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 –destination-node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 –destination-node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 –destination-node n4 -destination-port e4a
```

6. Überprüfen Sie den Zustand des Clusters:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
       (network interface show)

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0a     false
            n1_clus3   up/up      10.10.0.3/24       n1
e0d     false
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0a     false
            n2_clus3   up/up      10.10.0.7/24       n2
e0d     false
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4a     false
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4a     false
12 entries were displayed.
```

7. Schalten Sie die Cluster-Verbindungsports ab, die physisch mit Switch CL2 verbunden sind:

   `network port modify`

Beispiel anzeigen

Dieses Beispiel zeigt, wie die angegebenen Ports auf allen Knoten abgeschaltet werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Befehl „show“ ausführen, um die Details anzuzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source     Destination   Packet
Node   Date                       LIF        LIF           Loss
------ -------------------------- ---------- ------------ -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2   n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2   n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2   n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2   n1_clus2      none
n3
...
...
n4
...
...
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

`cluster ping-cluster -node <name>`

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n1_clus3 n1     e0c 10.10.0.3
Cluster n1_clus4 n1     e0d 10.10.0.4
Cluster n2_clus1 n2     e0a 10.10.0.5
```

```
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
Cluster n2_clus4 n2     e0d 10.10.0.8
Cluster n3_clus1 n4     e0a 10.10.0.9
Cluster n3_clus2 n3     e0e 10.10.0.10
Cluster n4_clus1 n4     e0a 10.10.0.11
Cluster n4_clus2 n4     e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
```

```
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12

Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

1. Schalten Sie die Ports 1/31 und 1/32 an CL1 sowie den aktiven Nexus 3132Q-V Switch ab:

   `shutdown`

   Beispiel anzeigen

   Dieses Beispiel zeigt, wie die ISL-Ports 1/31 und 1/32 am Switch CL1 abgeschaltet werden:

   ```
   (CL1)# configure
   (CL1)(Config)# interface e1/31-32
   (CL1)(config-if-range)# shutdown
   (CL1)(config-if-range)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

Schritt 2: Ports konfigurieren

1. Entfernen Sie alle Kabel, die am Switch CL2 des Nexus 3132Q-V angeschlossen sind, und verbinden Sie sie an allen Knoten mit dem Ersatz-Switch C2.
2. Entfernen Sie die ISL-Kabel von den Ports e1/31 und e1/32 an CL2 und schließen Sie sie an die gleichen Ports am Ersatz-Switch C2 an.
3. Aktivieren Sie die ISL-Ports 1/31 und 1/32 am Nexus 3132Q-V Switch CL1:

   ```
   (CL1)# configure
   (CL1)(Config)# interface e1/31-32
   (CL1)(config-if-range)# no shutdown
   (CL1)(config-if-range)# exit
   (CL1)(Config)# exit
   (CL1)#
   ```

4. Überprüfen Sie, ob die ISLs auf CL1 aktiv sind:

   `show port-channel`

Die Ports Eth1/31 und Eth1/32 sollten anzeigen `(P)` Das bedeutet, dass die ISL-Ports im Portkanal aktiv sind.

Beispiel anzeigen

```
CL1# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member
Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

5. Überprüfen Sie, ob die ISLs auf C2 aktiv sind:

   `show port-channel summary`

   Die Ports Eth1/31 und Eth1/32 sollten anzeigen `(P)` Das bedeutet, dass beide ISL-Ports im Portkanal aktiv sind.

   Beispiel anzeigen

```
C2# show port-channel summary
Flags: D - Down         P - Up in port-channel (members)
       I - Individual   H - Hot-standby (LACP only)
       s - Suspended    r - Module-removed
       S - Switched     R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-        Type   Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)      Eth    LACP      Eth1/31(P)   Eth1/32(P)
```

6. Aktivieren Sie auf allen Knoten alle Cluster-Interconnect-Ports, die mit dem Nexus 3132Q-V Switch C2 verbunden sind:

   `network port modify`

   Beispiel anzeigen

   ```
   cluster::*> network port modify -node n1 -port e0b -up-admin true
   cluster::*> network port modify -node n1 -port e0c -up-admin true
   cluster::*> network port modify -node n2 -port e0b -up-admin true
   cluster::*> network port modify -node n2 -port e0c -up-admin true
   cluster::*> network port modify -node n3 -port e4e -up-admin true
   cluster::*> network port modify -node n4 -port e4e -up-admin true
   ```

7. Für alle Knoten müssen alle migrierten Cluster-Interconnect-LIFs zurückgesetzt werden:

   `network interface revert`

   Beispiel anzeigen

   ```
   cluster::*> network interface revert -vserver Cluster -lif n1_clus2
   cluster::*> network interface revert -vserver Cluster -lif n1_clus3
   cluster::*> network interface revert -vserver Cluster -lif n2_clus2
   cluster::*> network interface revert -vserver Cluster -lif n2_clus3
   cluster::*> network interface revert -vserver Cluster -lif n3_clus2
   cluster::*> network interface revert -vserver Cluster -lif n4_clus2
   ```

8. Überprüfen Sie, ob die Cluster-Verbindungsports nun wieder auf ihre Ausgangsposition zurückgesetzt sind:

   `network interface show`

Beispiel anzeigen

Dieses Beispiel zeigt, dass alle LIFs erfolgreich zurückgesetzt wurden, da die unter dem Eintrag aufgeführten Ports `Current Port` Spalte haben den Status `true` im `Is Home` Spalte. Wenn die `Is Home` Spaltenwert ist `false` Der LIF wurde nicht rückgängig gemacht.

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

9. Überprüfen Sie, ob die Cluster-Ports verbunden sind:

   `network port show`

Beispiel anzeigen

```
cluster::*> network port show -role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-

Node: n2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
```

```
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
12 entries were displayed.
```

10. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Befehl „show“ ausführen, um die Details anzuzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source     Destination   Packet
Node   Date                       LIF        LIF           Loss
------ -------------------------- ---------- ------------ -----------
n1
       3/5/2022 19:21:18 -06:00   n1_clus2   n2_clus1      none
       3/5/2022 19:21:20 -06:00   n1_clus2   n2_clus2      none

n2
       3/5/2022 19:21:18 -06:00   n2_clus2   n1_clus1      none
       3/5/2022 19:21:20 -06:00   n2_clus2   n1_clus2      none
n3
...
...
n4
...
...
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

`cluster ping-cluster -node <name>`

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1     e0a 10.10.0.1
Cluster n1_clus2 n1     e0b 10.10.0.2
Cluster n2_clus1 n2     e0a 10.10.0.5
Cluster n2_clus2 n2     e0b 10.10.0.6
Cluster n2_clus3 n2     e0c 10.10.0.7
```

```
Cluster n2_clus4 n2     e0d 10.10.0.8
Cluster n3_clus1 n3     e0a 10.10.0.9
Cluster n3_clus2 n3     e0e 10.10.0.10
Cluster n4_clus1 n4     e0a 10.10.0.11
Cluster n4_clus2 n4     e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9 10.10.0.10
10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.9
    Local 10.10.0.3 to Remote 10.10.0.10
    Local 10.10.0.3 to Remote 10.10.0.11
    Local 10.10.0.3 to Remote 10.10.0.12
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.9
    Local 10.10.0.4 to Remote 10.10.0.10
```

```
    Local 10.10.0.4 to Remote 10.10.0.11
    Local 10.10.0.4 to Remote 10.10.0.12

Larger than PMTU communication succeeds on 32 path(s)
RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

Schritt 3: Konfiguration überprüfen

1. Zeigen Sie die Informationen zu den Geräten in Ihrer Konfiguration an:
    - `network device-discovery show`
    - `network port show -role cluster`
    - `network interface show -role cluster`
    - `system cluster-switch show`

Beispiel anzeigen

```
cluster::> network device-discovery show
            Local  Discovered
Node        Port   Device               Interface        Platform
----------- ------ ------------------ ----------------
----------------
n1         /cdp
            e0a    C1                 Ethernet1/1/1    N3K-C3132Q-V
            e0b    C2                 Ethernet1/1/1    N3K-C3132Q-V
            e0c    C2                 Ethernet1/1/2    N3K-C3132Q-V
            e0d    C1                 Ethernet1/1/2    N3K-C3132Q-V
n2         /cdp
            e0a    C1                 Ethernet1/1/3    N3K-C3132Q-V
            e0b    C2                 Ethernet1/1/3    N3K-C3132Q-V
            e0c    C2                 Ethernet1/1/4    N3K-C3132Q-V
            e0d    C1                 Ethernet1/1/4    N3K-C3132Q-V
n3         /cdp
            e4a    C1                 Ethernet1/7      N3K-C3132Q-V
            e4e    C2                 Ethernet1/7      N3K-C3132Q-V
n4         /cdp
            e4a    C1                 Ethernet1/8      N3K-C3132Q-V
            e4e    C2                 Ethernet1/8      N3K-C3132Q-V
12 entries were displayed.
```

```
cluster::*> network port show –role cluster
  (network port show)
Node: n1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000 auto/10000  -
-
e0b       Cluster      Cluster          up   9000 auto/10000  -
-
e0c       Cluster      Cluster          up   9000 auto/10000  -
-
e0d       Cluster      Cluster          up   9000 auto/10000  -
-
```

```
Node: n2

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/10000 -
-
e0b       Cluster      Cluster          up   9000  auto/10000 -
-
e0c       Cluster      Cluster          up   9000  auto/10000 -
-
e0d       Cluster      Cluster          up   9000  auto/10000 -
-

Node: n3

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-

Node: n4

Ignore
                                                       Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e4a       Cluster      Cluster          up   9000 auto/40000  -
-
e4e       Cluster      Cluster          up   9000 auto/40000  -
-
```

```
12 entries were displayed.
```

```
cluster::*> network interface show -role cluster
 (network interface show)
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            n1_clus1   up/up      10.10.0.1/24       n1
e0a     true
            n1_clus2   up/up      10.10.0.2/24       n1
e0b     true
            n1_clus3   up/up      10.10.0.3/24       n1
e0c     true
            n1_clus4   up/up      10.10.0.4/24       n1
e0d     true
            n2_clus1   up/up      10.10.0.5/24       n2
e0a     true
            n2_clus2   up/up      10.10.0.6/24       n2
e0b     true
            n2_clus3   up/up      10.10.0.7/24       n2
e0c     true
            n2_clus4   up/up      10.10.0.8/24       n2
e0d     true
            n3_clus1   up/up      10.10.0.9/24       n3
e4a     true
            n3_clus2   up/up      10.10.0.10/24      n3
e4e     true
            n4_clus1   up/up      10.10.0.11/24      n4
e4a     true
            n4_clus2   up/up      10.10.0.12/24      n4
e4e     true
12 entries were displayed.
```

```
cluster::*> system cluster-switch show

Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
CL1                          cluster-network   10.10.1.101
NX3132V
     Serial Number: FOX000001
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

CL2                          cluster-network   10.10.1.102
NX3132V
     Serial Number: FOX000002
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP
C2                          cluster-network    10.10.1.103
NX3132V
     Serial Number: FOX000003
      Is Monitored: true
            Reason:
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    7.0(3)I4(1)
    Version Source: CDP

3 entries were displayed.
```

2. Entfernen Sie den ausgetauschten Nexus 3132Q-V-Schalter, falls er nicht bereits automatisch entfernt wurde:

   `system cluster-switch delete`

```
cluster::*> system cluster-switch delete –device CL2
```

3. Stellen Sie sicher, dass die richtigen Cluster-Switches überwacht werden:

   ```
   system cluster-switch show
   ```

   Beispiel anzeigen

   ```
   cluster::> system cluster-switch show

   Switch                      Type               Address
   Model
   --------------------------- ------------------ ----------------
   ---------------
   CL1                          cluster-network    10.10.1.101
   NX3132V
        Serial Number: FOX000001
         Is Monitored: true
               Reason:
     Software Version: Cisco Nexus Operating System (NX-OS) Software,
   Version
                       7.0(3)I4(1)
       Version Source: CDP

   C2                          cluster-network     10.10.1.103
   NX3132V
        Serial Number: FOX000002
         Is Monitored: true
               Reason:
     Software Version: Cisco Nexus Operating System (NX-OS) Software,
   Version
                       7.0(3)I4(1)
       Version Source: CDP

   2 entries were displayed.
   ```

4. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

Wie geht es weiter?

Nachdem Sie Ihren Schalter ausgetauscht haben, können Sie"Konfigurieren der Switch-Integritätsüberwachung" Die

Ersetzen Sie Cisco Nexus 3132Q-V Cluster-Switches durch switchlose Verbindungen.

In ONTAP 9.3 und späteren Versionen können Sie von einem Cluster mit einem Switched-Cluster-Netzwerk zu einem Cluster migrieren, in dem zwei Knoten direkt miteinander verbunden sind.

NetApp empfiehlt, vor der Durchführung der Umstellung von einem Switched- auf einen Switchless-Cluster-Vorgang für Cisco Nexus 3132Q-V Switches die ONTAP Version zu aktualisieren.

Weitere Einzelheiten finden Sie im Folgenden:

- "SU540: Chelsio T6 NIC-Fehler verursachen Systemabschaltung beim Upgrade von 40G- auf 100G-Netzwerk-Switches"
- "Knotenabsturz nach Migration von einem Cluster mit Switches zu einem Cluster ohne Switches"

Für ONTAP 9.3 und höher können Sie von einem Cluster mit einem Switched-Cluster-Netzwerk zu einem Cluster migrieren, in dem zwei Knoten direkt miteinander verbunden sind.

Überprüfungsanforderungen

Richtlinien

Bitte beachten Sie die folgenden Richtlinien:

- Die Migration zu einer Zwei-Knoten-Clusterkonfiguration ohne Switches ist ein unterbrechungsfreier Vorgang. Die meisten Systeme verfügen über zwei dedizierte Cluster-Interconnect-Ports pro Knoten. Dieses Verfahren kann aber auch für Systeme mit einer größeren Anzahl dedizierter Cluster-Interconnect-Ports pro Knoten angewendet werden, beispielsweise vier, sechs oder acht.
- Die Funktion „Switchless Cluster Interconnect“ kann nicht mit mehr als zwei Knoten verwendet werden.
- Wenn Sie über einen bestehenden Zwei-Knoten-Cluster verfügen, der Cluster-Interconnect-Switches verwendet und auf dem ONTAP 9.3 oder höher läuft, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Knoten ersetzen.

Bevor Sie beginnen

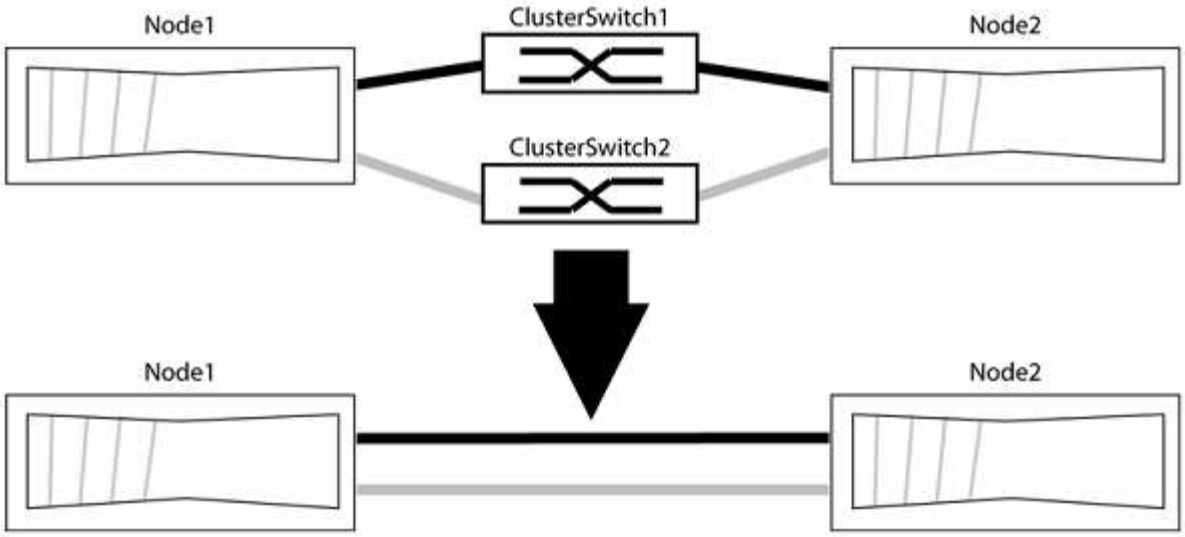
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesunder Cluster, der aus zwei Knoten besteht, die über Cluster-Switches verbunden sind. Auf den Knoten muss die gleiche ONTAP Version laufen.
- Jeder Knoten verfügt über die erforderliche Anzahl dedizierter Cluster-Ports, die redundante Cluster-Verbindungen bereitstellen, um Ihre Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster-Verbindungsports auf jedem Knoten.

Migrieren Sie die Schalter

Informationen zu diesem Vorgang

Das folgende Verfahren entfernt die Cluster-Switches in einem Zwei-Knoten-Cluster und ersetzt jede Verbindung zum Switch durch eine direkte Verbindung zum Partnerknoten.



Zu den Beispielen

Die Beispiele im folgenden Verfahren zeigen Knoten, die "e0a" und "e0b" als Cluster-Ports verwenden. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.

Schritt 1: Vorbereitung auf die Migration

1. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung `*>` erscheint.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von switchlosen Clustern, die standardmäßig aktiviert ist.

   Sie können überprüfen, ob die Erkennung von Clustern ohne Switch aktiviert ist, indem Sie den Befehl mit erweiterten Berechtigungen ausführen:

   ```
   network options detect-switchless-cluster show
   ```

   Beispiel anzeigen

   Die folgende Beispielausgabe zeigt, ob die Option aktiviert ist.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Wenn "Schalterlose Clustererkennung aktivieren" `false` Wenden Sie sich an den NetApp Support.

3. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` ist die Dauer des Wartungsfensters in Stunden. Die Meldung informiert den technischen Support über diese Wartungsaufgabe, damit dieser die automatische Fallerstellung während des Wartungsfensters unterdrücken kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Fallerstellung für zwei Stunden:

Beispiel anzeigen

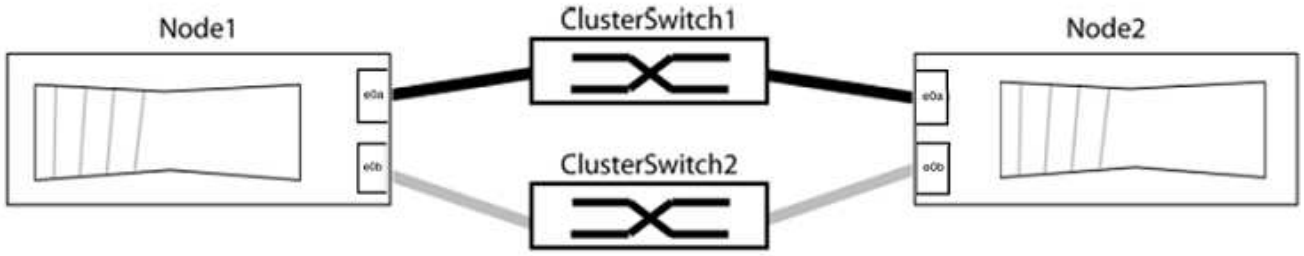
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen ein, sodass die Cluster-Ports in Gruppe 1 an Cluster-Switch 1 und die Cluster-Ports in Gruppe 2 an Cluster-Switch 2 angeschlossen werden. Diese Gruppen werden im weiteren Verlauf des Verfahrens benötigt.
2. Identifizieren Sie die Cluster-Ports und überprüfen Sie den Verbindungsstatus und die Integrität:

   ```
   network port show -ipspace Cluster
   ```

   Im folgenden Beispiel für Knoten mit Cluster-Ports „e0a“ und „e0b“ wird eine Gruppe als „node1:e0a“ und „node2:e0a“ und die andere Gruppe als „node1:e0b“ und „node2:e0b“ identifiziert. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



   Überprüfen Sie, ob die Ports den Wert haben. `up` für die Spalte „Link“ und einen Wert von `healthy` für die Spalte „Gesundheitszustand“.

Beispiel anzeigen

```
cluster::> network port show -ipspace Cluster
Node: node1

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false

Node: node2

Ignore
                                             Speed(Mbps) Health
Health
Port  IPspace   Broadcast Domain Link  MTU   Admin/Oper  Status
Status
----- --------- ---------------- ----- ----- ----------- -------
-------
e0a   Cluster   Cluster          up    9000  auto/10000  healthy
false
e0b   Cluster   Cluster          up    9000  auto/10000  healthy
false
4 entries were displayed.
```

3. Vergewissern Sie sich, dass alle Cluster-LIFs an ihren jeweiligen Heimatports angeschlossen sind.

   Überprüfen Sie, ob die Spalte „is-home“ `true` für jeden der Cluster-LIFs:

   `network interface show -vserver Cluster -fields is-home`

Beispiel anzeigen

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Falls Cluster-LIFs vorhanden sind, die sich nicht auf ihren Heimatports befinden, werden diese LIFs wieder auf ihre Heimatports zurückgesetzt:

```
network interface revert -vserver Cluster -lif *
```

4. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

   ```
   network interface modify -vserver Cluster -lif * -auto-revert false
   ```

5. Überprüfen Sie, ob alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

   ```
   network device-discovery show -port cluster_port
   ```

   In der Spalte „Erkanntes Gerät“ sollte der Name des Cluster-Switches stehen, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports "e0a" und "e0b" korrekt mit den Cluster-Switches "cs1" und "cs2" verbunden sind.

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Vorgang ausführen. `show` Befehl zum Anzeigen der Details.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 7]] Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster ring show
   ```

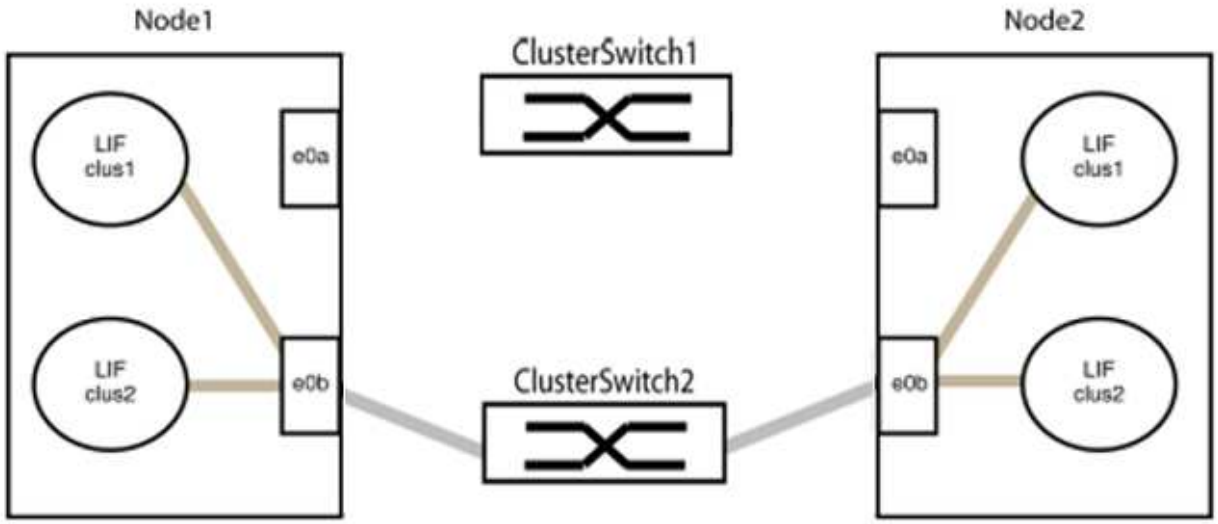
   Alle Einheiten müssen entweder Master- oder Sekundäreinheiten sein.

2. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 1 ein.

   > Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe1 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

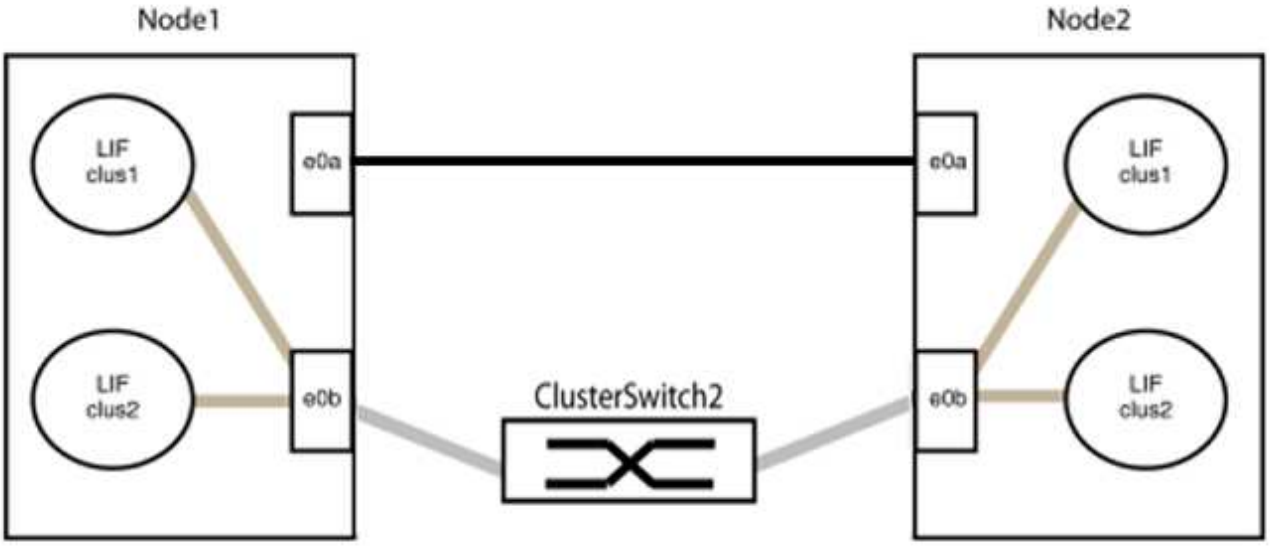
   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

      Im folgenden Beispiel werden die Kabel an Port „e0a“ auf jedem Knoten getrennt, und der Cluster-Datenverkehr wird weiterhin über den Switch und Port „e0b“ auf jedem Knoten abgewickelt:



b. Verbinden Sie die Ports in Gruppe 1 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden:



3. Die Option für ein schalterloses Clusternetzwerk wechselt von `false` Zu `true` Die Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „Schalterlos“ aktiviert ist. `true` :

`network options switchless-cluster show`

Das folgende Beispiel zeigt, dass der switchlose Cluster aktiviert ist:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Vorgang ausführen. `show` Befehl zum Anzeigen der Details.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

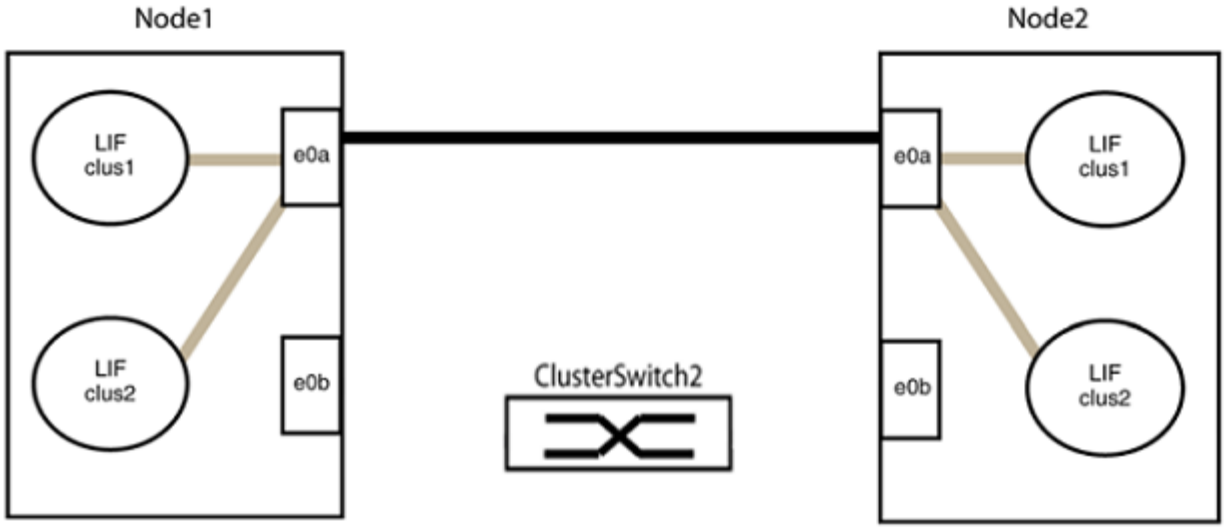
Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung in Gruppe 1 zu bestätigen.

1. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 2 ein.

   Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe 2 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 2.

      Im folgenden Beispiel werden die Kabel von Port "e0b" an jedem Knoten getrennt, und der Cluster-Datenverkehr wird über die direkte Verbindung zwischen den Ports "e0a" fortgesetzt:



b. Verbinden Sie die Ports in Gruppe 2 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden und "e0b" auf Knoten 1 ist mit "e0b" auf Knoten 2 verbunden:

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie, ob die Ports an beiden Knoten korrekt verbunden sind:

```
network device-discovery show -port cluster_port
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port des Cluster-Partners verbunden sind:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Automatische Rücksetzung für die Cluster-LIFs wieder aktivieren:

   `network interface modify -vserver Cluster -lif * -auto-revert true`

3. Überprüfen Sie, ob alle LIFs zu Hause sind. Dies kann einige Sekunden dauern.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „Ist zu Hause“ den Wert „Ist zu Hause“ aufweist. `true` , wie gezeigt für `node1_clus2` Und `node2_clus2` im folgenden Beispiel:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif          curr-port is-home
-------- ------------ --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

Falls Cluster-LIFS nicht zu ihren Heimatports zurückgekehrt sind, setzen Sie sie manuell vom lokalen Knoten aus zurück:

`network interface revert -vserver Cluster -lif` *`lif_name`*

4. Überprüfen Sie den Clusterstatus der Knoten über die Systemkonsole eines der beiden Knoten:

   `cluster show`

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass epsilon an beiden Knoten gleich ist. `false` :

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

5. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen:

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl zum Starten einer Zugriffsprüfung für die Clusterkonnektivität und anschließenden Anzeigen der Details:

`network interface check cluster-connectivity start`Und `network interface check cluster-connectivity show`

```
cluster1::*> network interface check cluster-connectivity start
```

HINWEIS: Warten Sie einige Sekunden, bevor Sie den Vorgang ausführen. `show` Befehl zum Anzeigen der Details.

```
cluster1::*> network interface check cluster-connectivity show
                                  Source           Destination
Packet
Node   Date                       LIF              LIF
Loss
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

Für alle ONTAP Versionen können Sie auch die `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Verbindung:

```
cluster ping-cluster -node <name>
```

```
cluster1::*> cluster ping-cluster -node local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Falls Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

   ```
   system node autosupport invoke -node * -type all -message MAINT=END
   ```

   Weitere Informationen finden Sie unter "NetApp KB-Artikel 1010449: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster".

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```