



Verfügbarkeitsende-Schalter

Install and maintain

NetApp

February 13, 2026

Inhalt

Verfügbarkeitsende-Schalter	1
Ende der Verfügbarkeit	1
Ankündigungen zum Verkaufsende und Produktlebenszyklusende	1
Cisco Nexus 3232C	1
Erste Schritte	1
Installieren der Hardware	5
Software konfigurieren	14
Schalter migrieren	77
Schalter austauschen	99
Cisco 3232C Storage Switches	141
Cisco Nexus 3132Q-V	148
Erste Schritte	148
Installieren der Hardware	152
Software konfigurieren	160
Schalter migrieren	225
Schalter austauschen	249
Cisco Nexus 92300YC	295
Erste Schritte	295
Installieren der Hardware	300
Konfigurieren der Software	313
Schalter migrieren	353
Schalter austauschen	371
NetApp CN1610	402
Übersicht über Installation und Konfiguration von NetApp CN1610-Switches	402
Workflow für NetApp CN1610-Switches installieren und konfigurieren	403
Dokumentationsanforderungen für NetApp CN1610-Switches	403
Installieren und konfigurieren	404
Schalter migrieren	441
Schalter austauschen	468

Verfügbarkeitsende-Schalter

Ende der Verfügbarkeit

Die folgenden Schalter sind nicht mehr käuflich erhältlich, werden aber weiterhin unterstützt.

- ["Cisco Nexus 3232C"](#)
- ["Cisco Nexus 3132Q-V"](#)
- ["Cisco Nexus 92300YC"](#)
- ["NetApp CN1610"](#)

Ankündigungen zum Verkaufsende und Produktlebenszyklusende

- ["Ankündigung zum Verkaufs- und Produktlebenszyklusende für den Cisco Nexus 3232C"](#)
- ["Ankündigung zum Verkaufs- und Produktlebenszyklusende für die Cisco Nexus 31108PC-V, 31108TC-V und Nexus 3132Q-V"](#)
- ["Ankündigung zum Verkaufs- und Produktlebenszyklusende für die Cisco N9K-C93120TX und N9K-C92300YC"](#)
- ["Ankündigung zum Verkaufs- und Produktlebenszyklusende der Cisco Nexus 5500 Series Switches"](#)
- ["Verfügbarkeitsende: NetApp CN1610 Cluster Interconnect SKUs"](#)

Cisco Nexus 3232C

Erste Schritte

Installations- und Einrichtungsworkflow für Cisco Nexus 3232C-Switches

Cisco Nexus 3232C 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 3232C-Switch zu installieren und einzurichten.

1

["Konfigurationsanforderungen"](#)

Überprüfen Sie die Konfigurationsanforderungen für den 3232C-Cluster-Switch.

2

["Erforderliche Dokumentation"](#)

Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 3232C-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 3232C-Switches

Bei der Installation und Wartung des Cisco Nexus 3232C Switches sollten Sie unbedingt die Konfigurations- und Netzwerkanforderungen überprüfen.

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 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 Ihre Konfigurationsanforderungen bestätigt haben, können Sie die "[erforderliche Dokumentation](#)". Die

Dokumentationsanforderungen für Cisco Nexus 3232C-Switches

Für die Installation und Wartung des Cisco Nexus 3232C Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation lesen.

Switch-Dokumentation

Für die Einrichtung der Cisco Nexus 3232C Switches benötigen Sie die folgende Dokumentation von "[Cisco Nexus 3000 Series Switches Unterstützung](#)" Seite.

Dokumenttitel	Beschreibung
<i>Hardware-Installationsanleitung für die Nexus 3000-Serie</i>	Bietet detaillierte Informationen zu Standortanforderungen, Hardware-Details der Schalter und Installationsoptionen.
<i>Softwarekonfigurationshandbücher für Cisco Nexus 3000 Series Switches</i> (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.
<i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide</i> (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.
Cisco Nexus 3000 MIBs-Referenz	Beschreibt die Management Information Base (MIB)-Dateien für die Nexus 3000 Switches.
<i>Referenz der NX-OS-Systemmeldungen der Nexus 3000-Serie</i>	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.
<i>Cisco Nexus 3000 Series NX-OS Versionshinweise</i> (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
<i>Controllerspezifische Installations- und Einrichtungsanweisungen</i>	Beschreibt die Installation von NetApp -Hardware.

Name	Beschreibung
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 3232C 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 3232C Switch in einem NetApp -Schrank"	Beschreibt die Installation eines Cisco Nexus 3232C 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 3232C-Switches

So installieren und konfigurieren Sie die Hardware für einen 3232C-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 3232C-Switch.

3

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

Installieren Sie den 3232C-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 3232C

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 100GbE-Port, 40GbE-Port oder 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	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	1	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
2	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	2	4x10GbE/4x25GbE- oder 40/100GbE-Knoten

Clusterschalter A		Clusterschalter B	
3	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	3	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
4	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	4	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
5	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	5	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
6	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	6	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
7	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	7	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
8	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	8	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
9	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	9	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
10	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	10	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
11	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	11	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
12	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	12	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
13	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	13	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
14	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	14	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
15	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	15	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
16	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	16	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
17	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	17	4x10GbE/4x25GbE- oder 40/100GbE-Knoten

Clusterschalter A		Clusterschalter B	
18	4x10GbE/4x25GbE- oder 40/100GbE-Knoten	18	4x10GbE/4x25GbE- oder 40/100GbE-Knoten
19	40G/100GbE-Knoten 19	19	40G/100GbE-Knoten 19
20	40G/100GbE-Knoten 20	20	40G/100GbE-Knoten 20
21	40G/100GbE-Knoten 21	21	40G/100GbE-Knoten 21
22	40G/100GbE-Knoten 22	22	40G/100GbE-Knoten 22
23	40G/100GbE-Knoten 23	23	40G/100GbE-Knoten 23
24	40G/100GbE-Knoten 24	24	40G/100GbE-Knoten 24
25 bis 30	Reserviert	25 bis 30	Reserviert
31	100GbE ISL zu Switch B Port 31	31	100GbE ISL zu Switch A Port 31
32	100GbE ISL zu Switch B Port 32	32	100GbE 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	
4		4	
5		5	
6		6	

Clusterschalter A		Clusterschalter B	
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
31	100GbE ISL zu Switch B Port 31	31	100GbE ISL zu Switch A Port 31
32	100GbE ISL zu Switch B Port 32	32	100GbE ISL zu Switch A Port 32

Was kommt als nächstes

Nachdem Sie Ihre Verkabelungsarbeitsblätter ausgefüllt haben, können Sie ["Installieren Sie den Schalter"](#)Die

Installieren Sie den 3232C-Cluster-Switch

Gehen Sie wie folgt vor, um den Cisco Nexus 3232C 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 3232C in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> .
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 3223C-Switch in einem NetApp -Schrank"](#)Die Ansonsten gehen Sie zu ["Verkabelung und Konfiguration überprüfen"](#)Die

Installieren Sie einen Cisco Nexus 3232C Cluster-Switch in einem NetApp Schrank

Je nach Konfiguration müssen Sie möglicherweise den Cisco Nexus 3232C Cluster-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
- Für jeden Schalter werden die acht 10-32 oder 12-24 Schrauben und Clipmutter benötigt, um die Halterungen und Gleitschienen an den vorderen und hinteren Gehäusepfosten zu befestigen.
- Cisco Standard-Schienenkit zur Installation des Switches in einem NetApp -Schrack.



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

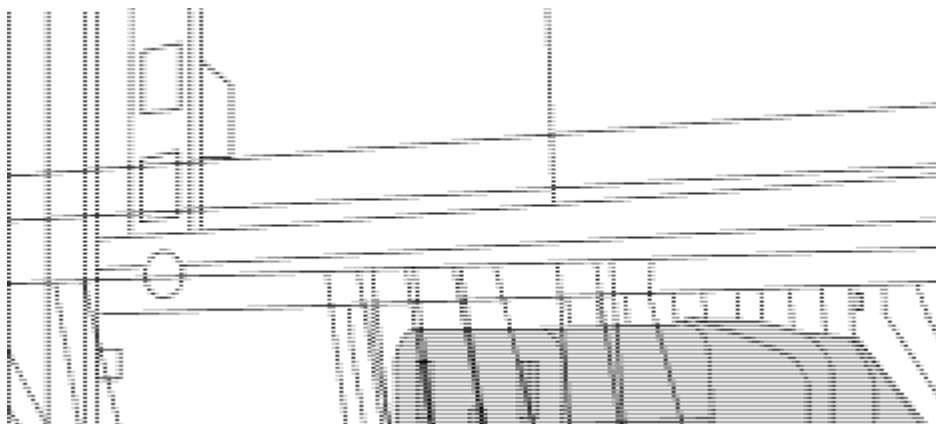
1. Installieren Sie die Durchgangsabdeckung im NetApp -Schrack.

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
 - i. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

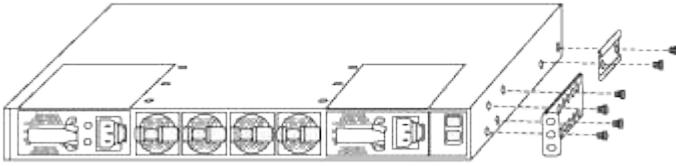
Bei diesem Verfahren wird die Abdeckplatte in U40 installiert.
 - ii. Montieren Sie auf jeder Seite zwei Clipmuttern in den entsprechenden quadratischen Löchern für die vorderen Schrankschienen.
 - iii. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.
 - iv. Führen Sie die weiblichen Stecker beider 48-Zoll-Überbrückungskabel von der Rückseite des Bedienfelds durch die Bürstenbaugruppe.



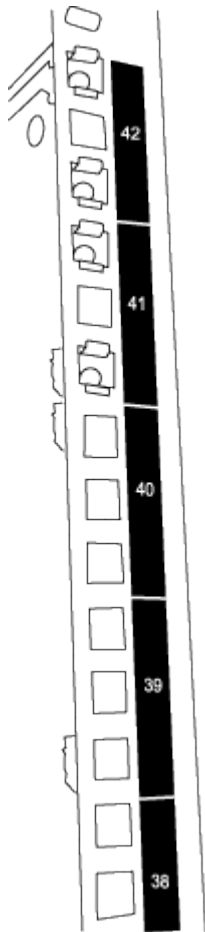
(1) Weiblicher Stecker des Überbrückungskabels.

1. Montieren Sie die Rack-Montagehalterungen am Nexus 3232C 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.

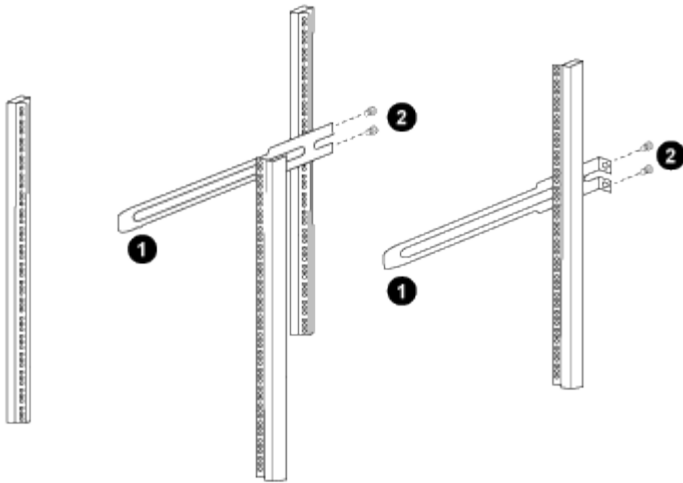


- b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.
 - c. Installieren Sie die hintere Rackmontagehalterung am Switch-Gehäuse.
 - d. Wiederholen Sie Schritt 2c mit der anderen hinteren Rackmontagehalterung auf der anderen Seite des Switches.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



Die beiden 3232C-Switches werden immer in den oberen 2 HE des Schrankes RU41 und 42 montiert.

3. 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) Schieben 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.

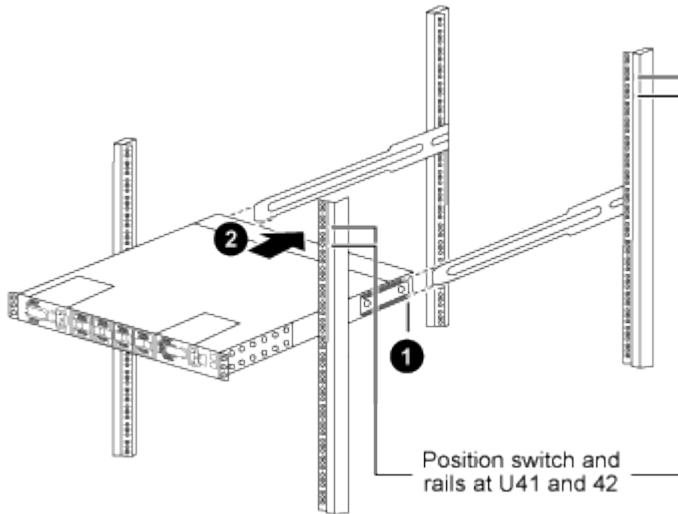
- a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.
- b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Positionen am Schrank.

4. 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.

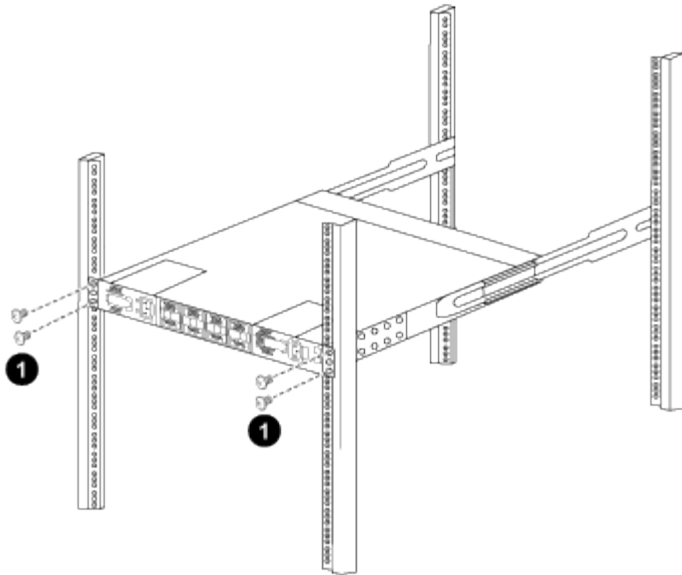
- a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



- (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 waagrecht 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.



Durch die Verwendung des fertig montierten Schalters als Stütze ist es nicht notwendig, den zweiten Schalter während des Montagevorgangs vorne festzuhalten.

5. Wenn die Schalter installiert sind, schließen Sie die Überbrückungskabel an die Stromeingänge der Schalter an.
6. 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.

7. Verbinden Sie den Management-Port jedes 3232C-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 3232C 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
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(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 3232C-Cluster-Switches

Um die Software für einen Cisco Nexus 3232C-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 3232C-Cluster-Switch.

2

["Bereiten Sie die Installation der NX-OS-Software und des RCF vor."](#)

Die Cisco NX-OS-Software und Referenzkonfigurationsdateien (RCFs) müssen auf Cisco 3232C-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 3232C-Cluster-Switch.

4

["Installieren Sie den RCF"](#)

Installieren Sie das RCF, nachdem Sie den Cisco 3232C-Switch zum ersten Mal eingerichtet haben.

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 3232C-Cluster-Switch-Einstellungen.

Konfigurieren des Cluster-Switches 3232C

Gehen Sie wie folgt vor, um den Cisco Nexus 3232C Switch einzurichten und 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 zum Cluster-Netzwerk und zum Management-Netzwerk-Switch.

Sehen "[Erforderliche Dokumentation](#)" für weitere Informationen.

- Erforderliche Controller-Dokumentation und ONTAP Dokumentation.

"[NetApp Dokumentation](#)"

- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.
- Ausgefüllte Verkabelungs-Arbeitsblätter.
- 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 3232C in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> .
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.
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 .
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.

Prompt	Antwort
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 Anzahl der Schlüsselbits im Bereich von 1024 bis 2048 ein.
Den NTP-Server konfigurieren? (ja/nein)	Antworten Sie mit nein . Die Standardeinstellung ist Nein.
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.

- 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.

- 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, können Sie "[Bereiten Sie die Installation von NX-OS und RCF vor](#)." Die

Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei (RCF) 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.

Nomenklatur von Schaltern und Knoten

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

- 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=x h`

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.

- 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp	e0a	cs1	Eth1/2	N3K-
C3232C	e0b	cs2	Eth1/2	N3K-
C3232C				
cluster1-01/cdp	e0a	cs1	Eth1/1	N3K-
C3232C	e0b	cs2	Eth1/1	N3K-
C3232C				

4 entries were displayed.

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
```

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

```
Node: cluster1-01
```

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

```
4 entries were displayed.
```

- a. Informationen zu den LIFs anzeigen: `network interface show -vserver Cluster`

Beispiel anzeigen

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

Current Vserver Port	Logical Current Is Interface Home	Status Admin/Oper	Network Address/Mask	Node

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			

4 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
```

Packet	Source	Destination
Node	Date	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

```

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

4 entries were displayed.

Wie geht es weiter?

Nachdem Sie die Installation der NX-OS-Software und von RCF vorbereitet haben, können Sie ["Installieren Sie die NX-OS-Software"](#)Die

Installieren Sie die NX-OS-Software

Mit diesem Verfahren können Sie die NX-OS-Software auf dem Nexus 3232C Cluster-Switch installieren.

Überprüfungsanforderungen

Bevor Sie beginnen

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- ["Cisco Ethernet-Switch-Seite"](#). 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

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 von NX-OS und RCF 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

Dieses Beispiel bestätigt, dass der Switch den Server unter der IP-Adresse 172.19.2.1 erreichen kann:

```
cs2# ping 172.19.2.1
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-
C3232C
          e0d    cs2                Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N3K-
C3232C
          e0d    cs2                Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N3K-
C3232C
          e0b    cs2                Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N3K-
C3232C
          e0b    cs2                Ethernet1/1/2    N3K-
C3232C
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

Health	Health				Speed (Mbps)	
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
```

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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-
C3232C
    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-
C3232C
    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 und die EPLD-Images auf den Nexus 3232C-Switch.

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:
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.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
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:
sftp> progress
Progress meter enabled
sftp> get    /code/n9000-epld.9.3.4.img    /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img  100%  161MB    9.5MB/s    00:16
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) 2002-2019, 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 08.37
  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 Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGD

  Device name: cs2
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

Last reset at 74117 usecs after Tue Nov 24 06:24:23 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          v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(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 08.37
  NXOS: version 9.3(4)
  BIOS compile time: 01/28/2020
  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 Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGS

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
Reason: Reset due to upgrade
```

```
System version: 9.3(3)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

10. Aktualisieren Sie das EPLD-Image und starten Sie den Switch neu.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x12
IO	FPGA	0x11

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	Disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Up-Required
1	SUP	MI FPGA	0x12	0x12	No
1	SUP	IO FPGA	0x11	0x12	Yes

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

Module 1 EPLD upgrade is successful.

```
cs2#
```

11. Wenn Sie auf NX-OS Version 9.3(11) aktualisieren, müssen Sie auch das EPLD aktualisieren. golden Image erstellen und den Switch erneut starten. Andernfalls fahren Sie mit Schritt 12 fort.

Sehen "EPLD-Upgrade-Versionshinweise, Version 9.3(11)" für weitere Einzelheiten.

Beispiel anzeigen

```
cs2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable      Impact          Reason
-----
-----
          1          SUP          Yes          Disruptive      Module
Upgradable

Retrieving EPLD versions.... Please wait.
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
cs2#
```

12. Nach dem Neustart des Switches melden Sie sich an, um zu überprüfen, ob die neue Version von EPLD erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x12
IO	FPGA	0x12

13. 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

Health	Health				Speed (Mbps)	
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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-01/cdp	e0a	cs1	Ethernet1/7	N3K-
C3232C	e0d	cs2	Ethernet1/7	N3K-
C3232C				
cluster01-2/cdp	e0a	cs1	Ethernet1/8	N3K-
C3232C	e0d	cs2	Ethernet1/8	N3K-
C3232C				
cluster01-3/cdp	e0a	cs1	Ethernet1/1/1	N3K-
C3232C	e0b	cs2	Ethernet1/1/1	N3K-
C3232C				
cluster1-04/cdp	e0a	cs1	Ethernet1/1/2	N3K-
C3232C	e0b	cs2	Ethernet1/1/2	N3K-
C3232C				

```
cluster1::*> system cluster-switch show -is-monitoring-enabled  
-operational true
```

Switch Model	Type	Address	
cs1	cluster-network	10.233.205.90	N3K-
C3232C			
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-

```

C3232C
  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.

```

14. 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::*>

```

15. Wiederholen Sie die Schritte 6 bis 14 auf Switch cs1.

16. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

17. 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 3232C-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 3232C-Switches 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
Storage 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 Übersicht über die Installations- oder Aktualisierungsprozedur von RCF durchgelesen haben, können Sie "[Installieren Sie den RCF](#)" oder "[Aktualisieren Sie Ihren RCF](#)" wie erforderlich.

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus 3232C-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.

Stellen Sie sicher, dass Sie den Vorgang abschließen in "[Bereiten Sie die Installation von NX-OS und RCF vor.](#)" Befolgen Sie anschließend die folgenden Schritte.

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich per SSH oder über eine serielle Konsole bei Switch CS2 an.
2. 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 Handbuch im "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenz](#)".

Beispiel anzeigen

Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches CS2 zu kopieren:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_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)...
```

3. 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](#)"

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei. Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt wird auf Switch CS2 installiert:

```
cs2# copy Nexus_3232C_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.

4. Untersuchen Sie die Bannerausgabe von `show banner motd` Befehl. Um die korrekte Konfiguration und den ordnungsgemäßen Betrieb des Schalters sicherzustellen, müssen Sie die Anweisungen unter **Wichtige Hinweise** lesen und befolgen.
5. 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.

6. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe "[Überprüfung der Verkabelung und Konfigurationsüberlegungen](#)" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
7. Speichern Sie die grundlegenden Konfigurationsdetails in der `write_erase.cfg` Datei auf dem Bootflash.



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

```
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
```

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

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>  
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.

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

```
show file bootflash:write_erase.cfg
```

10. 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
```

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

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

12. Neustartschalter cs2:

```
cs2# reload
```

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

13. Wiederholen Sie die Schritte 1 bis 12 auf Switch cs1.

14. 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 -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::*>				

Wenn Cluster-LIFS nicht zu ihren Home-Ports zurückgekehrt sind, setzen Sie sie manuell zurück:

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

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
4 entries were displayed.
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-
C3232C
          e0d    cs2                Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N3K-
C3232C
          e0d    cs2                Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N3K-
C3232C
          e0b    cs2                Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N3K-
C3232C
          e0b    cs2                Ethernet1/1/2    N3K-
C3232C
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 -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     10.233.205.92
NX3232C
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(4)
    Version Source: CDP
cs2                                     cluster-network     10.233.205.93
NX3232C
    Serial Number: FOXXXXXXXXGD
    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.
```

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

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
```



Um Netzwerkverbindungsprobleme zu vermeiden, sollten **alle** verbundenen Cluster-Ports abgeschaltet werden. Siehe den Artikel in der Wissensdatenbank. "[Knoten außerhalb des Quorums bei Migration des Cluster-LIF während des Switch-OS-Upgrades](#)" für weitere Einzelheiten.

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 -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	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			
8 entries were displayed.				
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
4 entries were displayed.
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. Alle benutzerdefinierten Ergänzungen zwischen dem aktuellen running-config und die verwendete RCF-Datei (z. B. eine SNMP-Konfiguration für Ihre Organisation).
6. Speichern Sie die grundlegenden Konfigurationsdetails in der write_erase.cfg Datei auf dem Bootflash.



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

```
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 racl-lite 512" >>
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 CS2 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 Handbuch im "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenz](#)" Führer.

Beispiel anzeigen

Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches CS2 zu kopieren:

```
cs2# copy tftp: bootflash: vrf management  
Enter source filename: Nexus_3232C_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

Dieses Beispiel zeigt die RCF-Datei. `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` wird auf Switch CS2 installiert:

```
cs2# copy Nexus_3232C_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 Porteeinstellungen
- 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.

16. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe "[Überprüfung der Verkabelung und Konfigurationsüberlegungen](#)" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
17. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Schaltereinstellungen korrekt sind, kopieren Sie die Running-Config-Datei in die Startup-Config-Datei.

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

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

18. Neustart des Switches CS2. Sie können die auf den Knoten gemeldeten Ereignisse vom Typ „Cluster-Ports ausgefallen“ ignorieren, während der Switch neu startet.

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

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

a. Überprüfen Sie, ob die e0d-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 des Switches vom Cluster aus (dabei wird möglicherweise der Switch cs2 nicht angezeigt, da LIFs nicht auf e0d liegen).

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-C3232C
          e0d      cs2                      Ethernet1/7
N3K-C3232C
cluster01-2/cdp
          e0a      cs1                      Ethernet1/8
N3K-C3232C
          e0d      cs2                      Ethernet1/8
N3K-C3232C
cluster01-3/cdp
          e0a      cs1                      Ethernet1/1/1
N3K-C3232C
          e0b      cs2                      Ethernet1/1/1
N3K-C3232C
cluster1-04/cdp
          e0a      cs1                      Ethernet1/1/2
N3K-C3232C
          e0b      cs2                      Ethernet1/1/2
N3K-C3232C
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
-----
cs1                                     cluster-network      10.233.205.90
N3K-C3232C
    Serial Number: FOXXXXXXXXGD
    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-C3232C
    Serial Number: FOXXXXXXXXGS
```

```
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.
```



Abhängig von der zuvor auf dem Switch geladenen RCF-Version können Sie auf der Konsole des cs1-Switches möglicherweise die folgende Ausgabe beobachten: 2020 Nov 17 16:07:18 cs1 %\$ VDC-1 %\$ %STP-2-UNBLOCK_CONSIST_PORT: Entsperrten von Port Port-Channel1 auf VLAN0092. Portkonsistenz wiederhergestellt. 17. November 2020, 16:07:23 Uhr cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_PEER: Blockierung von Port-Channel1 auf VLAN0001. Inkonsistentes Peer-VLAN. 17. November 2020, 16:07:23 Uhr cs1 %\$ VDC-1 %\$ %STP-2-BLOCK_PVID_LOCAL: Blockierung von Port-Channel1 auf VLAN0092. Inkonsistentes lokales 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

Das folgende Beispiel verwendet die Ausgabe des Schnittstellenbeispiels aus Schritt 1:

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

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 -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	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		
8 entries were displayed.				
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 4 bis 19 auf Switch cs1.
24. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

Schritt 3: Überprüfen Sie die Clusternetzwerkconfiguration und den Clusterzustand.

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 -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::*>				

Wenn Cluster-LIFS nicht zu ihren Home-Ports zurückgekehrt sind, setzen Sie sie manuell zurück:

```
network interface revert -vserver vservice_name -lif lif_name
```

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

4 entries were displayed.

```
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, um eine Zugänglichkeitsprüfung für die Clusterkonnektivität zu starten und dann die Details anzuzeigen: `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
```

Packet			Source	Destination
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				
.				
.				
cluster1-03				
.				
.				
.				
.				
cluster1-04				
.				
.				
.				
.				

Alle ONTAP Versionen

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

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Wie geht es weiter?

Nach dem Upgrade Ihres RCF können Sie ["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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVliewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(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 3232C-Cluster-Switch auf die Werkseinstellungen zurück

Um den 3232C-Cluster-Switch auf die Werkseinstellungen zurückzusetzen, müssen Sie die 3232C-Switch-Einstellungen 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 Zwei-Knoten-Switchless-Clustern

Migration von einem Zwei-Knoten-Switchless-Cluster-Workflow

Befolgen Sie diese Workflow-Schritte, um von einem Zwei-Knoten-Cluster ohne Switches zu einem Cluster mit Cisco Nexus 3232C Cluster-Switches zu migrieren.

1

["Migrationsanforderungen"](#)

Prüfen Sie die Beispielinformationen zum Migrationsprozess.

2

"Bereiten Sie sich auf die Migration vor"

Bereiten Sie Ihren Zwei-Knoten-Cluster ohne Switches für die Migration zu einem Zwei-Knoten-Cluster mit Switches vor.

3

"Konfigurieren Sie Ihre Ports"

Konfigurieren Sie Ihren Zwei-Knoten-Cluster ohne Schalter für die Migration zu einem Zwei-Knoten-Cluster mit Schaltern.

4

"Schließen Sie Ihre Migration ab."

Schließen Sie Ihre Migration zu einem Zwei-Knoten-Switched-Cluster ab.

Migrationsanforderungen

Wenn Sie einen Zwei-Knoten-Cluster ohne Switches haben, können Sie zu einem Zwei-Knoten-Cluster mit Switches migrieren, der Cisco Nexus 3232C Cluster-Netzwerk-Switches enthält. Dies ist ein unterbrechungsfreies Verfahren.

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Für Knotenverbindungen stehen Ports zur Verfügung. Die Cluster-Switches verwenden die Inter-Switch Link (ISL)-Ports e1/31-32.
- Sie verfügen über die passenden Kabel für die Clusterverbindungen:
 - Die Knoten mit 10-GbE-Clusterverbindungen benötigen QSFP-Lichtwellenleitermodule mit Breakout-Glasfaserkabeln oder QSFP-zu-SFP+-Kupfer-Breakout-Kabel.
 - Die Knoten mit 40/100 GbE Cluster-Verbindungen benötigen unterstützte QSFP/QSFP28 optische Module mit Glasfaserkabeln oder QSFP/QSFP28 Kupfer-Direktanschlusskabel.
 - Die Cluster-Switches benötigen die entsprechende ISL-Verkabelung:
 - 2x QSFP28 Glasfaser- oder Kupfer-Direktanschlusskabel.
- Die Konfigurationen sind ordnungsgemäß eingerichtet und funktionieren.

Die beiden Knoten müssen in einer Zwei-Knoten-Clusterumgebung ohne Schalter verbunden und funktionsfähig sein.

- Alle Cluster-Ports befinden sich im Status **up**.
- Der Cisco Nexus 3232C Cluster-Switch wird unterstützt.
- Die bestehende Cluster-Netzwerkkonfiguration weist folgende Merkmale auf:
 - Eine redundante und voll funktionsfähige Nexus 3232C Cluster-Infrastruktur auf beiden Switches
 - Die neuesten RCF- und NX-OS-Versionen auf Ihren Switches
 - Management-Konnektivität auf beiden Switches

- Konsolenzugriff auf beide Schalter
- Alle logischen Schnittstellen (LIFs) des Clusters im Status **up**, die noch nicht migriert wurden
- Erste Anpassung des Schalters
- Alle ISL-Ports sind aktiviert und verkabelt.

Zu den verwendeten Beispielen

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

- Nexus 3232C 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-Universum](#)" enthält Details zu den Cluster-Ports auf Ihren Plattformen.

- **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 40/100-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die auf dem Server verfügbar sind. "[Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen](#)" Seite.



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 Migrationsanforderungen geprüft haben, können Sie "[Bereiten Sie sich auf die Migration Ihrer Schalter vor.](#)" Die

Vorbereitung der Migration von Zwei-Knoten-Clustern ohne Switches zu Zwei-Knoten-Clustern mit Switches

Befolgen Sie diese Schritte, um Ihren Zwei-Knoten-Switchless-Cluster für die Migration zu einem Zwei-Knoten-Switched-Cluster mit Cisco Nexus 3232C Cluster-Netzwerk-Switches 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 -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.
```

b. Informationen über die logischen Schnittstellen und ihre jeweiligen Heimatknoten anzeigen:

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

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.
```

- c. Überprüfen Sie mithilfe des Befehls mit erweiterten Berechtigungen, ob die Erkennung von Switchless-Clustern aktiviert ist:

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

Beispiel anzeigen

Die Ausgabe im folgenden Beispiel zeigt, dass die Erkennung von Clustern ohne Schalter aktiviert ist:

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

3. Überprüfen Sie, ob die entsprechenden RCFs und das Image auf den neuen 3232C-Switches installiert sind, und nehmen Sie alle notwendigen Standortanpassungen vor, z. B. das Hinzufügen von Benutzern, Passwörtern und Netzwerkadressen.

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

- a. Gehen Sie auf die Seite *Cisco Ethernet Switches* auf der NetApp Support-Website.

["Cisco Ethernet-Switches"](#)

- 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.

["Cisco Cluster- und Management-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen"](#)

- 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.
- 5. Deaktivieren Sie auf den Nexus 3232C Switches C1 und C2 alle zum Knoten hin ausgerichteten Ports C1 und C2, deaktivieren Sie jedoch nicht die ISL-Ports e1/31-32.

Weitere Informationen zu Cisco -Befehlen finden Sie in der folgenden Liste: ["Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen"](#) Die

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Ports 1 bis 30 auf den Nexus 3232C Cluster-Switches C1 und C2 mithilfe einer in RCF unterstützten Konfiguration deaktiviert werden.

NX3232_RCF_v1.0_24p10g_24p100g.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
```

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

```
show port-channel summary
```

Weitere Informationen zu Cisco -Befehlen finden Sie in der folgenden Liste: ["Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen"](#) Die

Beispiel anzeigen

Das folgende Beispiel zeigt das Cisco `show port-channel summary` Befehl, der verwendet wird, um zu überprüfen, ob die ISL-Ports auf C1 und C2 funktionsfähig sind:

```
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
```

```
-----
-----
Port-
Group Channel          Type   Protocol  Member Ports
-----
-----
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)
```

8. Zeigen Sie die Liste der benachbarten Geräte am Switch an.

Weitere Informationen zu Cisco -Befehlen finden Sie in der folgenden Liste: ["Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen"](#) Die

Beispiel anzeigen

Das folgende Beispiel zeigt den Cisco -Befehl `show cdp neighbors` wird verwendet, um die benachbarten Geräte am Switch anzuzeigen:

```
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-C3232C
Eth1/31
C2                  Eth1/32       174      R S I s          N3K-C3232C
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-C3232C
Eth1/31
C1                  Eth1/32       178      R S I s          N3K-C3232C
Eth1/32
Total entries displayed: 2
```

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

```
network device-discovery show
```

Beispiel anzeigen

Das folgende Beispiel zeigt die Cluster-Port-Konnektivität für eine Zwei-Knoten-Switchless-Cluster-Konfiguration:

```
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

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 einem Zwei-Knoten-Cluster ohne Switches zu einem Zwei-Knoten-Cluster mit Switches.

Befolgen Sie diese Schritte, um Ihre Ports für die Migration von einem Zwei-Knoten-Cluster ohne Switches zu einem Zwei-Knoten-Cluster mit Switches auf Nexus 3232C-Switches zu konfigurieren.

Schritte

1. Migrieren Sie die LIFs n1_clus1 und n2_clus1 zu den physischen Ports ihrer Zielknoten:

```
network interface migrate -vserver vservice-name -lif lif-name source-node  
source-node-name -destination-port destination-port-name
```

Beispiel anzeigen

Sie müssen den Befehl für jeden lokalen Knoten ausführen, wie im folgenden Beispiel gezeigt:

```
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
```

2. Überprüfen Sie, ob die Cluster-Schnittstellen erfolgreich migriert wurden:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass der Status „Is Home“ für die LIFs n1_clus1 und n2_clus1 nach Abschluss der Migration auf „false“ geändert wurde:

```
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.
```

3. Die Cluster-Ports für die LIFs n1_clus1 und n2_clus1, die in Schritt 9 migriert wurden, werden heruntergefahren:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Sie müssen den Befehl für jeden Port ausführen, wie im folgenden Beispiel gezeigt:

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

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					
-----	-----	-----	-----	-----	-----
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>
```

```

cluster1::*> cluster ping-cluster -node local
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 9000 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 an n1 verbinden, indem Sie die für Nexus 3232C-Switches unterstützten Kabel verwenden.

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.

Weitere Informationen zu Cisco -Befehlen finden Sie in den in der folgenden Liste aufgeführten Anleitungen: "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen](#)" Die

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Ports 1 bis 30 auf den Nexus 3232C Cluster-Switches C1 und C2 mithilfe der in RCF unterstützten Konfiguration aktiviert werden.

NX3232_RCF_v1.0_24p10g_26p100g.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 -node node-name -port port-name -up-admin true
```

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 -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.
```

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

```
network interface revert -vserver cluster -lif lif-name
```

Beispiel anzeigen

Sie müssen jeden LIF einzeln auf seinen Heimatport zurückführen, wie im folgenden Beispiel gezeigt:

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

7. Überprüfen Sie, ob alle LIFs nun wieder an ihren ursprünglichen Ports angeschlossen sind:

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

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-C3232C
      e4e      n2      e4e      FAS9000
n2      /cdp
      e4a      C1      Ethernet1/8      N3K-C3232C
      e4e      n1      e4e      FAS9000
```

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

```
network interface migrate cluster -lif lif-name -source-node source-node-name
-destination-node destination-node-name -destination-port destination-port-
name
```

Beispiel anzeigen

Sie müssen jede LIF einzeln an ihren jeweiligen Heimatport migrieren, wie im folgenden Beispiel gezeigt:

```
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
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die angegebenen Ports eingestellt werden. `false`, wodurch die 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 am Knoten n1 verbinden, indem Sie die für das Switch-Modell Nexus 3232C geeignete Verkabelung verwenden.

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

Sie können die laufende Konfiguration heranziehen und e4e mit dem nächsten verfügbaren 40-GbE-Port auf C2, Port 1/8, verbinden, indem Sie die für das Switch-Modell Nexus 3232C geeignete Verkabelung verwenden.

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.

NX3232C_RCF_v1.0_24p10g_26p100g.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
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der zweite Cluster-Port e4e auf jedem Knoten aktiviert wird:

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

16. 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_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

Wie geht es weiter?

Nachdem Sie Ihre Ports konfiguriert haben, können Sie ["Schließen Sie Ihre Migration ab."](#) Die

Schließen Sie Ihre Migration von einem Zwei-Knoten-Cluster ohne Switches zu einem Zwei-Knoten-Cluster mit Switches ab.

Führen Sie die folgenden Schritte durch, um die Migration des Zwei-Knoten-Clusters

ohne Switches zu einem Zwei-Knoten-Cluster mit Switches auf Nexus 3232C-Switches abzuschließen.

Schritte

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

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

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.
```

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

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

3. Zeigen Sie die Portnummern der Cluster-Switches an, über die jeder Cluster-Port mit 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-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

4. 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
NX3232CV		
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version 7.0(3)I6(1)		
Version Source: CDP		
C2	cluster-network	10.10.1.102
NX3232CV		
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software,		
Version 7.0(3)I6(1)		
Version Source: CDP		

2 entries were displayed.

5. Überprüfen Sie, ob die Erkennung des schalterlosen Clusters die Option „Schalterloser Cluster“ auf deaktiviert gesetzt hat:

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

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				
-----	-----	-----	-----	-----

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>
```

```

cluster1::*> cluster ping-cluster -node local
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 9000 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 Fehlerstellung 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

Ersetzen Sie einen Cisco Nexus 3232C Cluster-Switch

Befolgen Sie diese Schritte, um einen defekten Cisco Nexus 3232C Switch in einem Cluster auszutauschen. Dies ist ein unterbrechungsfreies Verfahren.

Überprüfungsanforderungen

Was du brauchst

Stellen Sie sicher, dass die bestehende Cluster- und Netzwerkkonfiguration die folgenden Eigenschaften aufweist:

- Die Nexus 3232C Cluster-Infrastruktur ist redundant und auf beiden Switches voll funktionsfähig.

Auf der Cisco Ethernet Switches-Seite finden Sie die neuesten RCF- und NX-OS-Versionen für Ihre

Switches.

- Alle Cluster-Ports müssen sich im Status **up** befinden.
- Die Management-Konnektivität muss auf beiden Switches vorhanden sein.
- Alle logischen Schnittstellen (LIFs) des Clusters befinden sich im Status **up** und wurden nicht migriert.

Der Ersatz-Switch Cisco Nexus 3232C weist folgende Merkmale auf:

- Die Managementnetzwerkanbindung ist funktionsfähig.
- Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
- Das entsprechende RCF- und NX-OS-Betriebssystemabbild wird auf den Switch geladen.
- Die erste Konfiguration des Schalters ist abgeschlossen.

Weitere Informationen

Siehe Folgendes:

- ["Cisco Ethernet-Switches"](#)
- ["Hardware Universe"](#)
- ["Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?"](#)

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.

Informationen zu diesem Vorgang

Dieses Austauschverfahren beschreibt folgendes Szenario:

- Der Cluster besteht anfänglich aus vier Knoten, die mit zwei Nexus 3232C Cluster-Switches, CL1 und CL2, verbunden sind.
- Sie planen, den Cluster-Schalter CL2 durch C2 zu ersetzen (Schritte 1 bis 21):
 - Auf jedem Knoten migrieren Sie die mit dem Cluster-Switch CL2 verbundenen Cluster-LIFs zu den mit dem Cluster-Switch CL1 verbundenen Cluster-Ports.
 - Sie trennen die Verkabelung von allen Ports des Cluster-Switches CL2 und schließen die Verkabelung an die gleichen Ports des Ersatz-Cluster-Switches C2 an.
 - Sie stellen die migrierten Cluster-LIFs auf jedem Knoten wieder her.

Zu den Beispielen

Bei diesem Austauschverfahren wird der zweite Nexus 3232C Cluster-Switch CL2 durch den neuen 3232C Switch C2 ersetzt.

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

- Die vier Knoten sind n1, n2, n3 und n4.
- 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 40/100-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die unter [URL] verfügbar sind. ["Cisco Cluster-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen"](#) Die

Die Beispiele in diesem Ersetzungsverfahren verwenden vier Knoten. Zwei der Knoten nutzen vier 10-GB-Cluster-Interconnect-Ports: e0a, e0b, e0c und e0d. Die anderen beiden Knoten verwenden zwei 40-GB-Cluster-Interconnect-Ports: e4a und e4e. Siehe die ["Hardware Universe"](#) um die korrekten Cluster-Ports für Ihre Plattform zu überprüfen.

Schritt 1: Cluster-Ports anzeigen und auf den Switch migrieren

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
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3232C
	e0b	CL2	Ethernet1/1/1	N3K-C3232C
	e0c	CL2	Ethernet1/1/2	N3K-C3232C
n2	e0d	CL1	Ethernet1/1/2	N3K-C3232C
	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
n3	e0c	CL2	Ethernet1/1/4	N3K-C3232C
	e0d	CL1	Ethernet1/1/4	N3K-C3232C
	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3232C
n4	e4e	CL2	Ethernet1/7	N3K-C3232C
	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3232C
	e4e	CL2	Ethernet1/8	N3K-C3232C

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

a. Netzwerkportattribute anzeigen:

```
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
```

```
-----  
-----  
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

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

```

b. Informationen zu den logischen Schnittstellen (LIFs) anzeigen:

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

Beispiel anzeigen

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

	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			

c. Die gefundenen Cluster-Switches anzeigen:

```
system cluster-switch show
```

Beispiel anzeigen

Das folgende Ausgabebeispiel zeigt die Cluster-Switches an:

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

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
CL2 NX3232C	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

4. Überprüfen Sie, ob die entsprechende RCF-Datei und das Image auf dem neuen Nexus 3232C-Switch installiert sind und nehmen Sie alle erforderlichen Standortanpassungen vor.

- a. Besuchen Sie die NetApp Supportseite.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- b. Rufen Sie die Seite * Cisco Ethernet Switches * auf und notieren Sie sich die erforderlichen Softwareversionen in der Tabelle.

["Cisco Ethernet-Switches"](#)

- c. Laden Sie die passende Version der RCF herunter.

- d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und navigieren Sie dann zur Seite **Download**.

- e. Laden Sie die richtige Version der Image-Software von der Seite * Cisco® Cluster and Management Network Switch Reference Configuration File Download* herunter.

["Cisco Cluster- und Management-Netzwerk-Switch-Referenzkonfigurationsdatei herunterladen"](#)

5. Migrieren Sie die Cluster-LIFs auf die physischen Knotenports, die mit dem Ersatzswitch C2 verbunden

sind:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node  
node-name -destination-node node-name -destination-port port-name
```

Beispiel anzeigen

Sie müssen alle Cluster-LIFs einzeln migrieren, wie im folgenden Beispiel gezeigt:

```
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 Status der Cluster-Ports und deren Home-Zuordnungen:

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

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
e0a          n1_clus1    up/up      10.10.0.1/24      n1
true
e0a          n1_clus2    up/up      10.10.0.2/24      n1
false
e0d          n1_clus3    up/up      10.10.0.3/24      n1
false
e0d          n1_clus4    up/up      10.10.0.4/24      n1
true
e0a          n2_clus1    up/up      10.10.0.5/24      n2
true
e0a          n2_clus2    up/up      10.10.0.6/24      n2
false
e0d          n2_clus3    up/up      10.10.0.7/24      n2
false
e0d          n2_clus4    up/up      10.10.0.8/24      n2
true
e4a          n3_clus1    up/up      10.10.0.9/24      n3
true
e4a          n3_clus2    up/up      10.10.0.10/24     n3
false
e4a          n4_clus1    up/up      10.10.0.11/24     n4
true
e4a          n4_clus2    up/up      10.10.0.12/24     n4
false
```

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

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Verbindungsports auf allen Knoten deaktiviert sind:

```
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 Vorgang ausführen. `show` Befehl zum Anzeigen der Details.

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

Packet		Source	Destination
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>
```

```
cluster1::*> cluster ping-cluster -node local
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 9000 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 2: ISLs migrieren, um CL1 und C2 zu verschalten

1. Schalten Sie die Ports 1/31 und 1/32 am Cluster-Switch CL1 ab.

Weitere Informationen zu Cisco -Befehlen finden Sie in den in der folgenden Liste aufgeführten Anleitungen: "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen](#)" Die

Beispiel anzeigen

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

2. Entfernen Sie alle Kabel, die am Cluster-Switch CL2 angeschlossen sind, und verbinden Sie sie für alle Knoten mit dem Ersatz-Switch C2.
3. Entfernen Sie die Inter-Switch-Link-Kabel (ISL) von den Ports e1/31 und e1/32 des Cluster-Switches CL2 und schließen Sie sie an die gleichen Ports des Ersatz-Switches C2 an.
4. Aktivieren Sie die ISL-Ports 1/31 und 1/32 am Cluster-Switch CL1.

Weitere Informationen zu Cisco -Befehlen finden Sie in den in der folgenden Liste aufgeführten Anleitungen: "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen](#)" Die

Beispiel anzeigen

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

5. Überprüfen Sie, ob die ISLs auf CL1 aktiv sind.

Weitere Informationen zu Cisco -Befehlen finden Sie in den in der folgenden Liste aufgeführten Anleitungen: "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen](#)" Die

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)
```

6. Überprüfen Sie, ob die ISLs auf dem Cluster-Switch C2 aktiv sind.

Weitere Informationen zu Cisco -Befehlen finden Sie in den in der folgenden Liste aufgeführten Anleitungen: "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen](#)" Die

Beispiel anzeigen

Die Ports Eth1/31 und Eth1/32 sollten (P) anzeigen, was bedeutet, dass beide ISL-Ports im Port-Channel aktiv sind.

```
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)
```

7. Aktivieren Sie auf allen Knoten alle Cluster-Verbindungsports, die mit dem Ersatz-Switch C2 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin true
```

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
```

Schritt 3: Alle LIFs auf die ursprünglich zugewiesenen Ports zurücksetzen

1. Alle migrierten Cluster-Interconnect-LIFs auf allen Knoten zurücksetzen:

```
network interface revert -vserver cluster -lif lif-name
```

Beispiel anzeigen

Sie müssen alle Cluster-Interconnect-LIFs einzeln zurücksetzen, wie im folgenden Beispiel gezeigt:

```
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
```

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

```
network interface show
```

Beispiel anzeigen

Das folgende 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 ein Port den Wert hat `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			

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

```
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
```

```
-----
```

```
-----
```

```
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
------	---------	-----------	--------	------	-----	------------	--------

e4a	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

e4e	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

-

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
```

Packet		Source	Destination
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>
```

```
cluster1::*> cluster ping-cluster -node local
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 9000 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 4: Überprüfen Sie, ob alle Ports und LIF korrekt migriert wurden.

1. Die Informationen zu den Geräten in Ihrer Konfiguration können Sie mit den folgenden Befehlen anzeigen:

Sie können die folgenden Befehle in beliebiger Reihenfolge ausführen:

- ° 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-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

```
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

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

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	

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	

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

cluster::*> **network interface show -role cluster**

		Logical	Status	Network	Current
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	
Port	Home				

Cluster					
	nm1_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			

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

Switch	Type	Address
Model		
-----	-----	-----
CL1	cluster-network	10.10.1.101
NX3232C		
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
CL2	cluster-network	10.10.1.102
NX3232C		
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2	cluster-network	10.10.1.103
NX3232C		
Serial Number: FOX000003		

```
Is Monitored: true
```

```
Reason: None
```

```
Software Version: Cisco Nexus Operating System (NX-OS)
```

```
Software, Version 7.0(3)I6(1)
```

```
Version Source: CDP 3 entries were displayed.
```

2. Löschen Sie den ausgetauschten Cluster-Schalter CL2, falls er nicht automatisch entfernt wurde:

```
system cluster-switch delete -device cluster-switch-name
```

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

```
system cluster-switch show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Switches überwacht werden, weil die Is Monitored Der Zustand ist true Die

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

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

4. Wenn Sie die automatische Fehlerstellung 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 3232C Cluster-Switches durch switchlose Verbindungen.

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

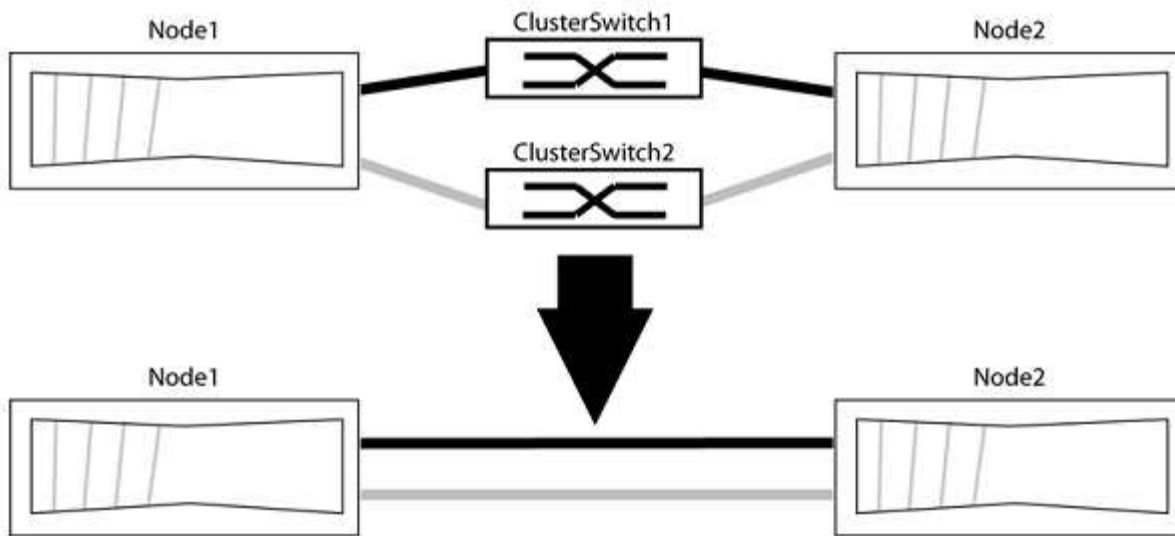
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- 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

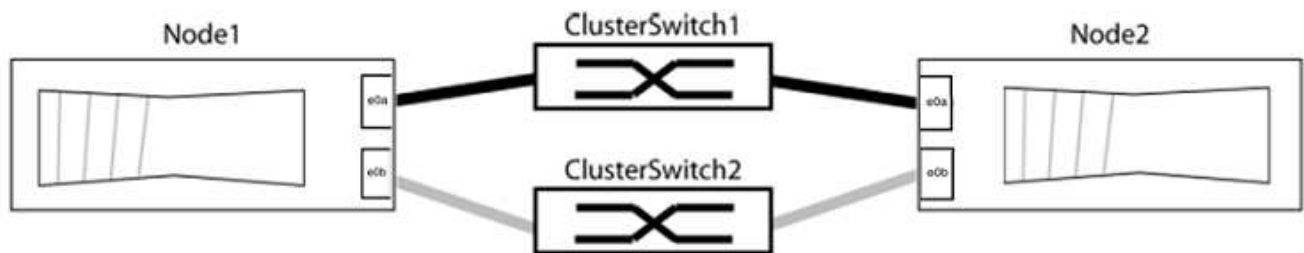
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

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.

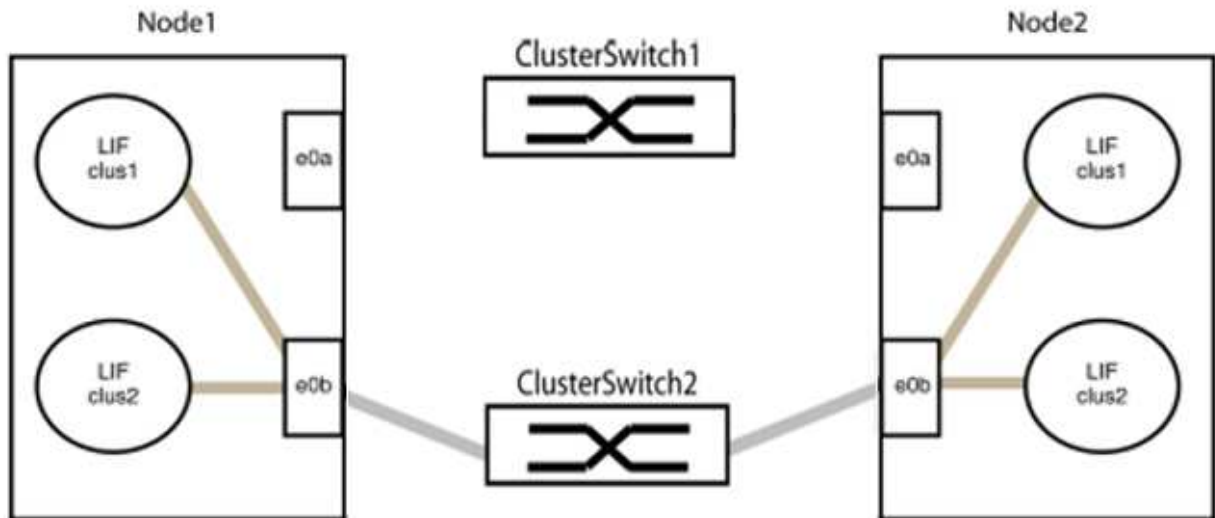
2. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 1 ein.



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**.

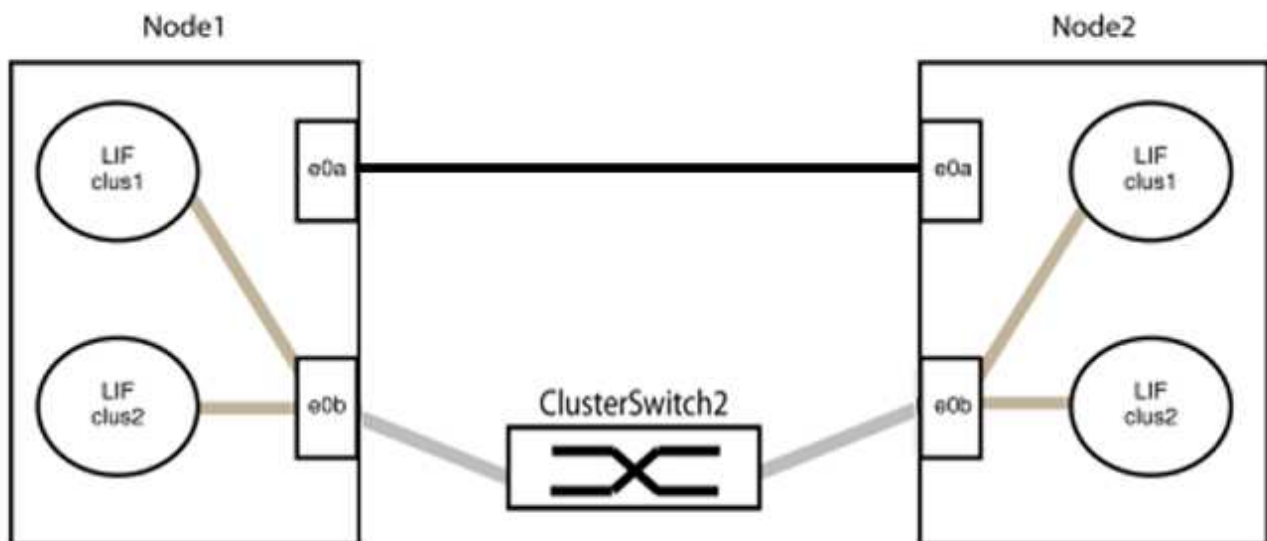
- a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

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.

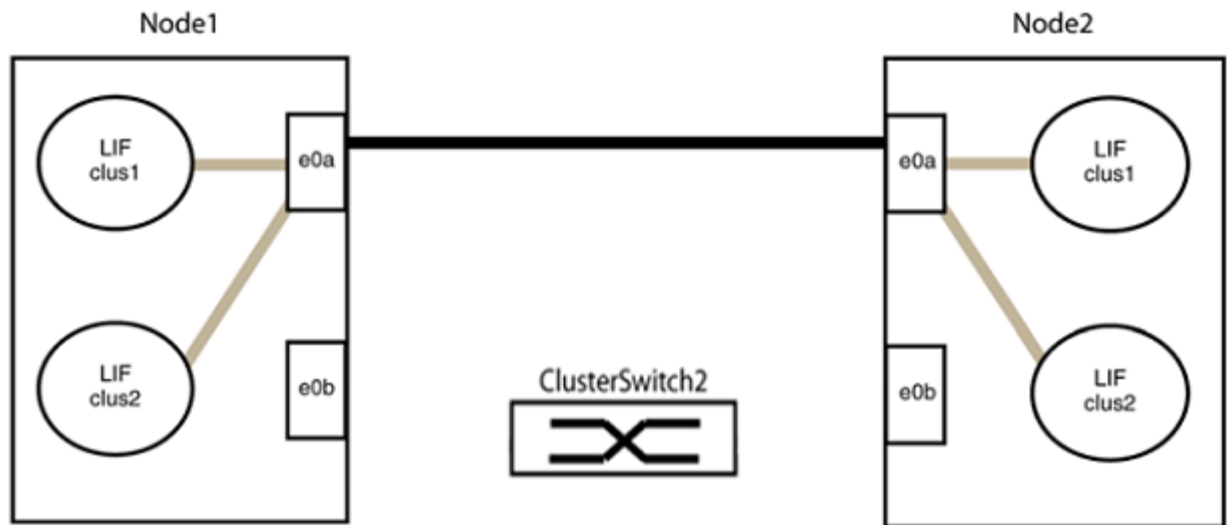
1. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 2 ein.



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
```

Cisco 3232C Storage Switches

Ersetzen Sie einen Cisco Nexus 3232C Speicherswitch

Befolgen Sie diese Schritte, um einen defekten Cisco Nexus 3232C Storage-Switch auszutauschen. Dies ist ein unterbrechungsfreies Verfahren.

Überprüfungsanforderungen

Die bestehende Netzwerkkonfiguration muss folgende Eigenschaften aufweisen:

- Auf der Cisco Ethernet Switches-Seite finden Sie die neuesten RCF- und NX-OS-Versionen für Ihre Switches.
- Die Management-Konnektivität muss auf beiden Switches vorhanden sein.



Stellen Sie sicher, dass alle Schritte zur Fehlerbehebung abgeschlossen sind, um zu bestätigen, dass Ihr Schalter ausgetauscht werden muss.

Der Ersatz-Switch Cisco Nexus 3232C muss folgende Eigenschaften aufweisen:

- Die Managementnetzwerkanbindung muss funktionsfähig sein.
- Der Zugang zum Ersatzschalter über die Konsole muss gewährleistet sein.
- Das entsprechende RCF- und NX-OS-Betriebssystemabbild muss auf den Switch geladen werden.
- Die Erstkonfiguration des Schalters muss abgeschlossen sein.

Tauschen Sie den Schalter aus.

Bei diesem Verfahren wird der zweite Nexus 3232C Speicherschalter S2 durch den neuen 3232C Schalter NS2 ersetzt. Die beiden Knoten sind Knoten1 und Knoten2.

Schritt 1: Prüfen Sie, ob es sich bei dem auszutauschenden Schalter um S2 handelt.

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. Überprüfen Sie den Gesundheitszustand der Speicherknotenports, um sicherzustellen, dass eine Verbindung zum Speicherswitch S1 besteht:

```
storage port show -port-type ENET
```

Beispiel anzeigen

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed		Status	VLAN
				(Gb/s)	State		ID

node1	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

3. Prüfen Sie, ob der Speicherschalter S1 verfügbar ist:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1/cdp	e3a	S1	Ethernet1/1	
NX3232C	e4a	node2	e4a	AFF-
A700	e4e	node2	e4e	AFF-
A700				
node1/lldp	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
node2/cdp	e3a	S1	Ethernet1/2	
NX3232C	e4a	node1	e4a	AFF-
A700	e4e	node1	e4e	AFF-
A700				
node2/lldp	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-

4. Führe die `show lldp neighbors` Führen Sie einen Befehl auf dem funktionierenden Switch aus, um zu bestätigen, dass Sie beide Knoten und alle Regale sehen können:

```
show lldp neighbors
```

Beispiel anzeigen

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID                Local Intf          Hold-time  Capability  Port
ID
node1                    Eth1/1             121        S           e3a
node2                    Eth1/2             121        S           e3a
SHFGD2008000011          Eth1/5             121        S           e0a
SHFGD2008000011          Eth1/6             120        S           e0a
SHFGD2008000022          Eth1/7             120        S           e0a
SHFGD2008000022          Eth1/8             120        S           e0a
```

Schritt 2: Verkabelung konfigurieren

1. Überprüfen Sie die Regalanschlüsse im Speichersystem:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-
port

shelf  id  remote-port  remote-device
----- --  -
3.20   0  Ethernet1/5  S1
3.20   1  -            -
3.20   2  Ethernet1/6  S1
3.20   3  -            -
3.30   0  Ethernet1/7  S1
3.20   1  -            -
3.30   2  Ethernet1/8  S1
3.20   3  -            -
```

2. Entfernen Sie alle Kabel, die am Speicherschalter S2 angeschlossen sind.
3. Schließen Sie alle Kabel wieder an den Ersatzschalter NS2 an.

Schritt 3: Überprüfen Sie alle Gerätekonfigurationen auf dem Switch NS2.

1. Überprüfen Sie den Gesundheitszustand der Speicherknotenports:

```
storage port show -port-type ENET
```

Beispiel anzeigen

```
storage::*> storage port show -port-type ENET
```

		Speed				
VLAN	Node	Port	Type	Mode	(Gb/s)	State
ID						Status

node1						
		e3a	ENET	storage	100	enabled online
30		e3b	ENET	storage	0	enabled offline
30		e7a	ENET	storage	0	enabled offline
30		e7b	ENET	storage	100	enabled online
30						
node2						
		e3a	ENET	storage	100	enabled online
30		e3b	ENET	storage	0	enabled offline
30		e7a	ENET	storage	0	enabled offline
30		e7b	ENET	storage	100	enabled online
30						

2. Vergewissern Sie sich, dass beide Schalter verfügbar sind:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	

node1/cdp				
	e3a	S1	Ethernet1/1	
NX3232C	e4a	node2	e4a	AFF-
A700	e4e	node2	e4e	AFF-
A700	e7b	NS2	Ethernet1/1	
NX3232C				
node1/lldp				
	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
	e7b	NS2	Ethernet1/1	-
node2/cdp				
	e3a	S1	Ethernet1/2	
NX3232C	e4a	node1	e4a	AFF-
A700	e4e	node1	e4e	AFF-
A700	e7b	NS2	Ethernet1/2	
NX3232C				
node2/lldp				
	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-
	e7b	NS2	Ethernet1/2	-

3. Überprüfen Sie die Regalanschlüsse im Lagersystem:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf id remote-port remote-device  
-----  
3.20 0 Ethernet1/5 S1  
3.20 1 Ethernet1/5 NS2  
3.20 2 Ethernet1/6 S1  
3.20 3 Ethernet1/6 NS2  
3.30 0 Ethernet1/7 S1  
3.20 1 Ethernet1/7 NS2  
3.30 2 Ethernet1/8 S1  
3.20 3 Ethernet1/8 NS2
```

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?

["Switch-Zustandsüberwachung konfigurieren"](#)

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
<i>Hardware-Installationsanleitung für die Nexus 3000-Serie</i>	Bietet detaillierte Informationen zu Standortanforderungen, Hardware-Details der Schalter und Installationsoptionen.
<i>Softwarekonfigurationshandbücher für Cisco Nexus 3000 Series Switches</i> (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.
<i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide</i> (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.
Cisco Nexus 3000 MIBs-Referenz	Beschreibt die Management Information Base (MIB)-Dateien für die Nexus 3000 Switches.
<i>Referenz der NX-OS-Systemmeldungen der Nexus 3000-Serie</i>	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.
<i>Cisco Nexus 3000 Series NX-OS Versionshinweise</i> (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 <i>Installations- und Einrichtungsanweisungen</i>	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 Kontaktnamen (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 -Schrunk."

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

Clusterschalter A		Clusterschalter B	
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
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

Clusterschalter A		Clusterschalter B	
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	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	

Clusterschalter A		Clusterschalter B	
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
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"](https://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 <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> .
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).

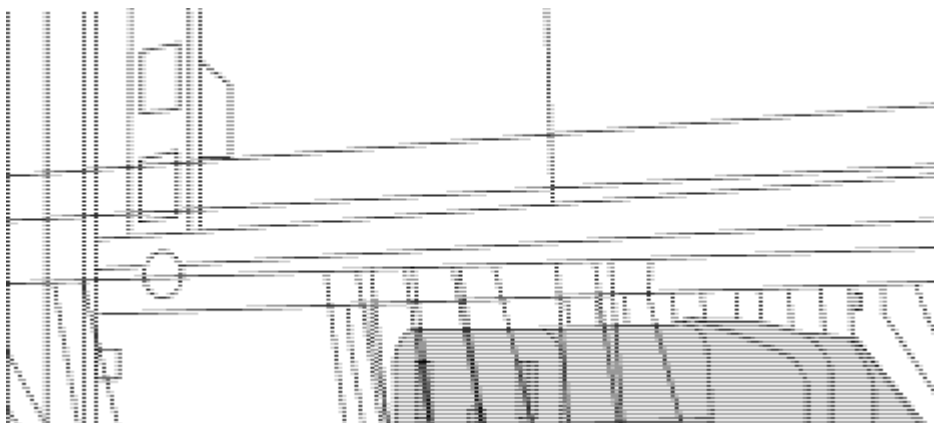
Schritte

1. Installieren Sie die Durchgangsabdeckung im NetApp -Schränk.

- a. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

Bei diesem Verfahren wird die Abdeckplatte in U40 installiert.

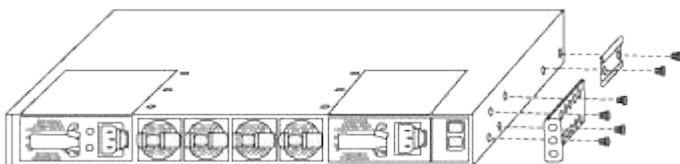
- b. Montieren Sie auf jeder Seite zwei Clipmuttern in den entsprechenden quadratischen Löchern für die vorderen Schrankschienen.
- c. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.
- d. Führen Sie die weiblichen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



(1) Weiblicher Stecker des Überbrückungskabels.

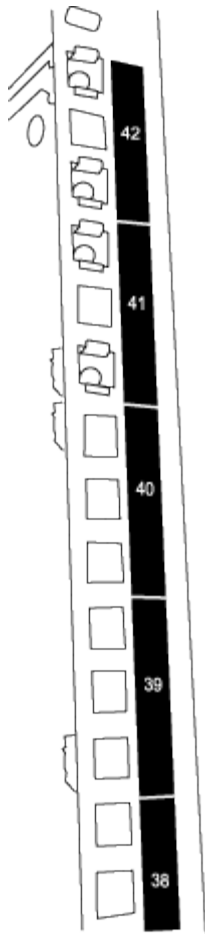
2. Montieren Sie die Rack-Montagehalterungen am Nexus 3132Q-V Switch-Gehäuse.

- 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.

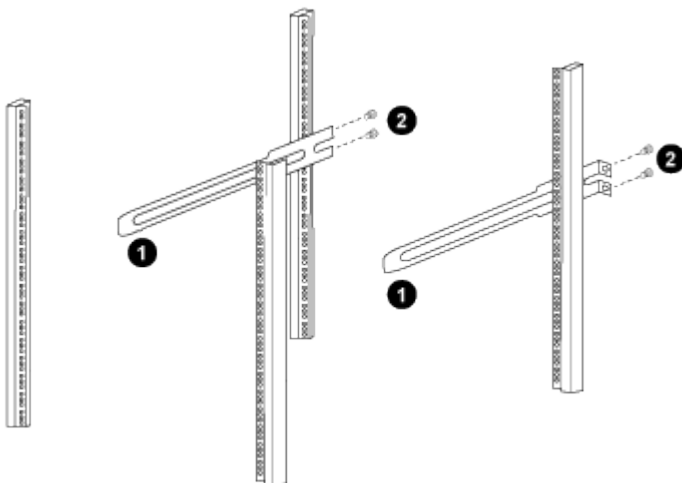
3. Installieren Sie die Clipmuttern in den quadratischen Lochpositionen für alle vier IEA-Pfosten.



Die beiden 3132Q-V-Switches werden immer in den oberen 2 HE des Schrankes 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.

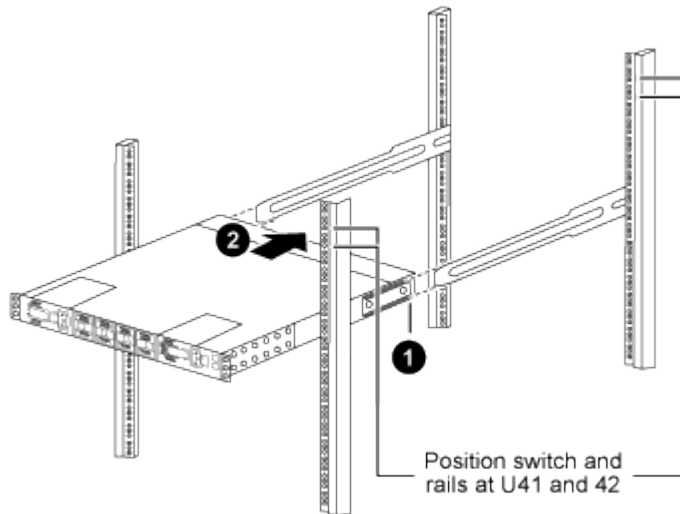
(2) Ziehen Sie die Schrauben der Gleitschienen an den Schrankpfosten fest.

- 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.

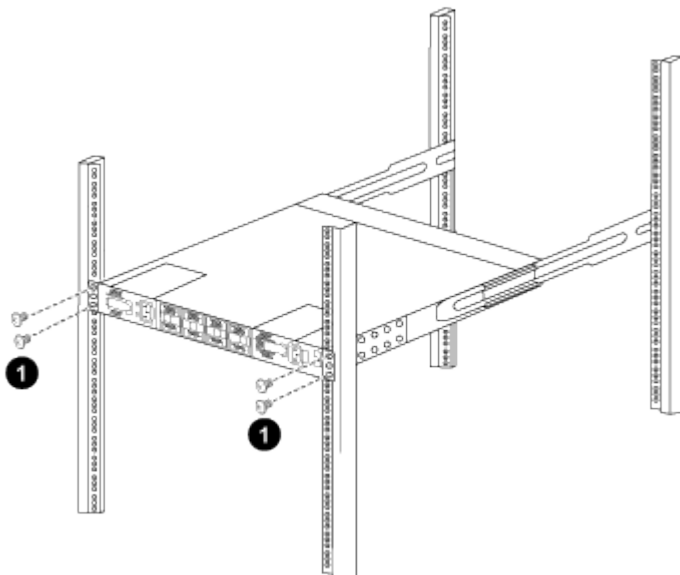
- a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(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 waagrecht 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 <i>Installing a Cisco Nexus 3132Q-V cluster switch and pass-through panel in a NetApp cabinet</i> .
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 .
Ein weiteres Benutzerkonto erstellen? (ja/nein)	Die Antwort hängt von den Richtlinien Ihrer Website bezüglich alternativer Administratoren ab. Die Standardeinstellung ist nein .

Prompt	Antwort
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.
Standard-Schnittstellenschicht (L3/L2) konfigurieren:	Antworte mit L2 . Standardmäßig ist L2 eingestellt.

Prompt	Antwort
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.

- 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.
- 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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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
```

Current Is	Logical	Status	Network	Current
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
```

Packet		Source	Destination
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
```

Vserver	Logical 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

Health	Health				Speed (Mbps)	
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
```

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
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

Health	Health				Speed (Mbps)	
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 -ipospace 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: FOXXXXXXXXGS
    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: FOXXXXXXXXGD
    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.

- 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

```

Current Is	Logical	Status	Network	Current
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::*>				

- 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: FOXXXXXXXXGS
    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: FOXXXXXXXXGD
    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 Porteeinstellungen
- 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	Broadcast	Domain	Link	MTU	Admin/Oper			
Port	IPspace								
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	Broadcast	Domain	Link	MTU	Admin/Oper			
Port	IPspace								
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	Broadcast	Domain	Link	MTU	Admin/Oper			
Port	IPspace								
Status	Status								
-----	-----	-----				-----			
-----	-----								
e0a	Cluster	Cluster		up	9000	auto/100000			
healthy	false								
e0d	Cluster	Cluster		up	9000	auto/100000			
healthy	false								

Node: cluster1-04

Ignore

Health	Health					Speed (Mbps)
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: FOXXXXXXXXGD		
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: FOXXXXXXXXGS
    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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

(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.



["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 Fehlerstellung 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

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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
```

Node	Local Port	Discovered 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				LIF	LIF				
Node	Date								
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 Wiederanschießen 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)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a true n1_clus1 up/up 10.10.0.1/24 n1
e4e true n1_clus2 up/up 10.10.0.2/24 n1
e4a true n2_clus1 up/up 10.10.0.3/24 n2
e4e true n2_clus2 up/up 10.10.0.4/24 n2
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
```

Node	Local Port	Discovered 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 Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.102
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				LIF	LIF				
Node	Date								
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 Fehlerstellung 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			Link	MTU	Admin/Oper	
Port	IPspace	Broadcast	Domain				
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			Link	MTU	Admin/Oper	
Port	IPspace	Broadcast	Domain				
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 Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.102
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](#)"
 - 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)
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	n1_clus1	up/up	10.10.0.1/24	n1
e0a	n1_clus2	up/up	10.10.0.2/24	n1
e0d	n1_clus3	up/up	10.10.0.3/24	n1
e0d	n1_clus4	up/up	10.10.0.4/24	n1
e0a	n2_clus1	up/up	10.10.0.5/24	n2
e0a	n2_clus2	up/up	10.10.0.6/24	n2
e0d	n2_clus3	up/up	10.10.0.7/24	n2
e0d	n2_clus4	up/up	10.10.0.8/24	n2
e4a	n3_clus1	up/up	10.10.0.9/24	n3
e4a	n3_clus2	up/up	10.10.0.10/24	n3
e4a	n4_clus1	up/up	10.10.0.11/24	n4
e4a	n4_clus2	up/up	10.10.0.12/24	n4

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
```

Node	Date	Source LIF	Destination LIF	Packet 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)
```

Current Is	Logical	Status	Network	Current
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
```

Node	Date	Source LIF	Destination LIF	Packet 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
```

Node	Local Port	Discovered 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
```

Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Speed(Mbps)	Health 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 Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.102
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 NX3132V	cluster-network	10.10.1.103
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 Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
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 NX3132V	cluster-network	10.10.1.103
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 Fehlerstellung 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

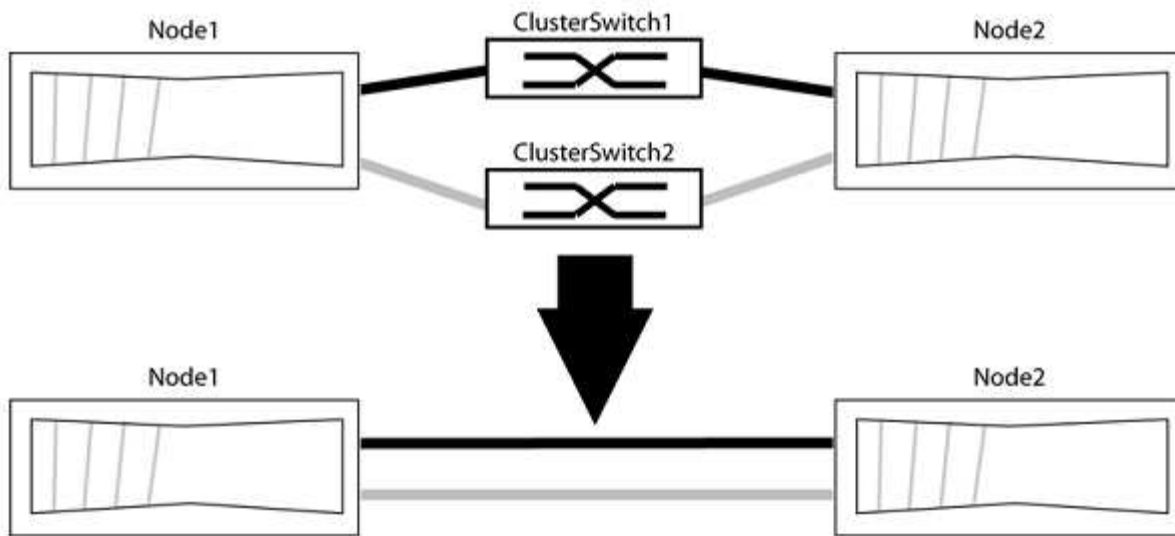
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- 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

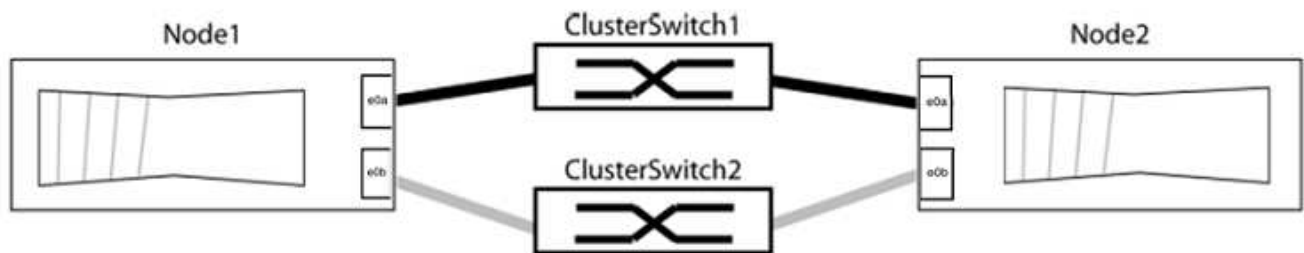
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

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.

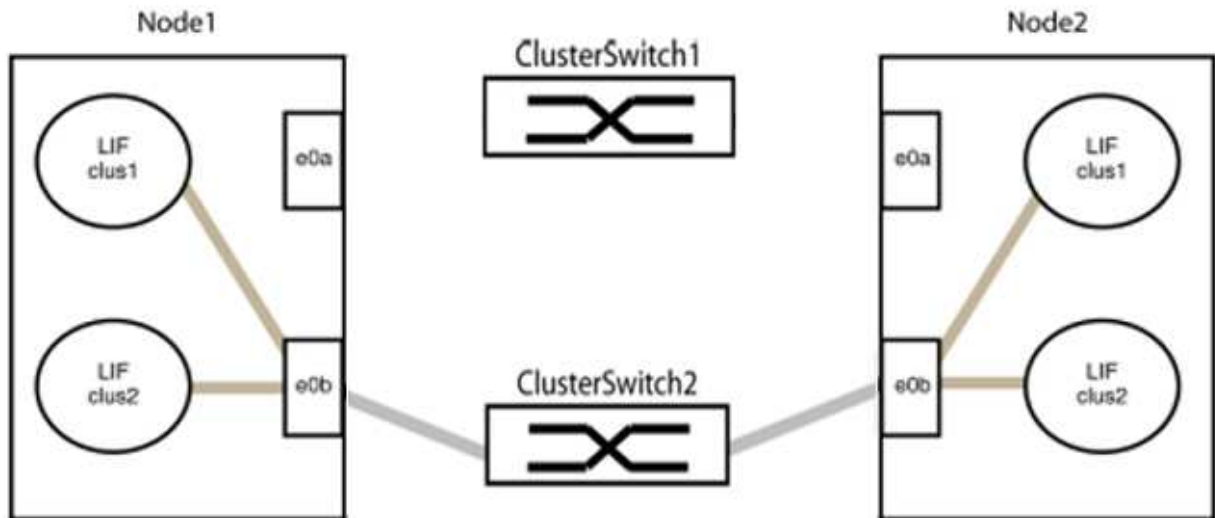
2. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 1 ein.



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**.

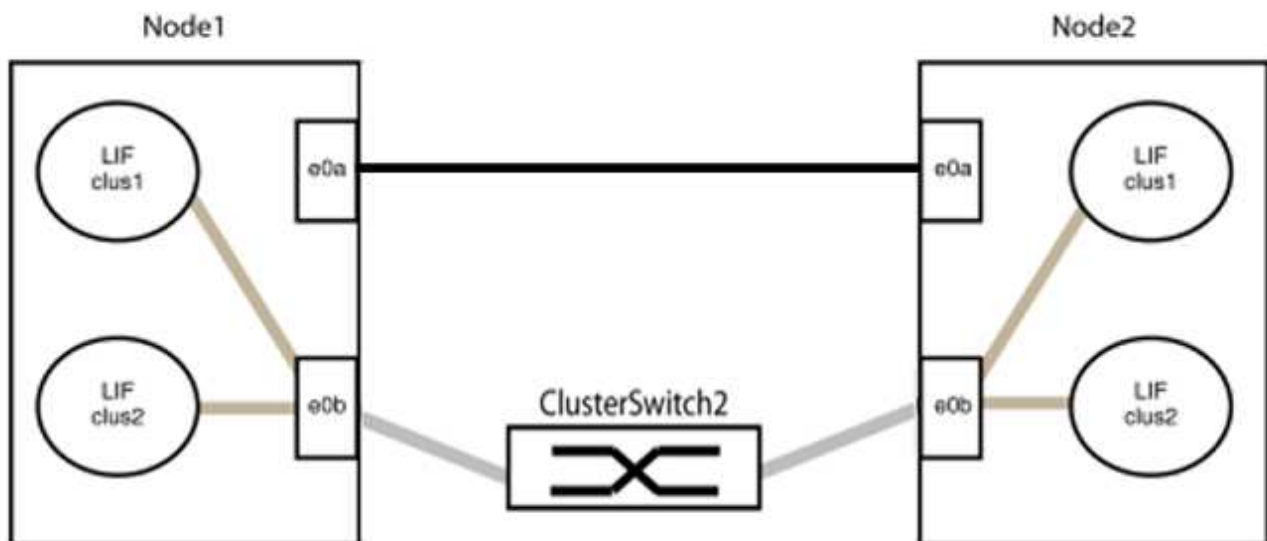
- a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

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.

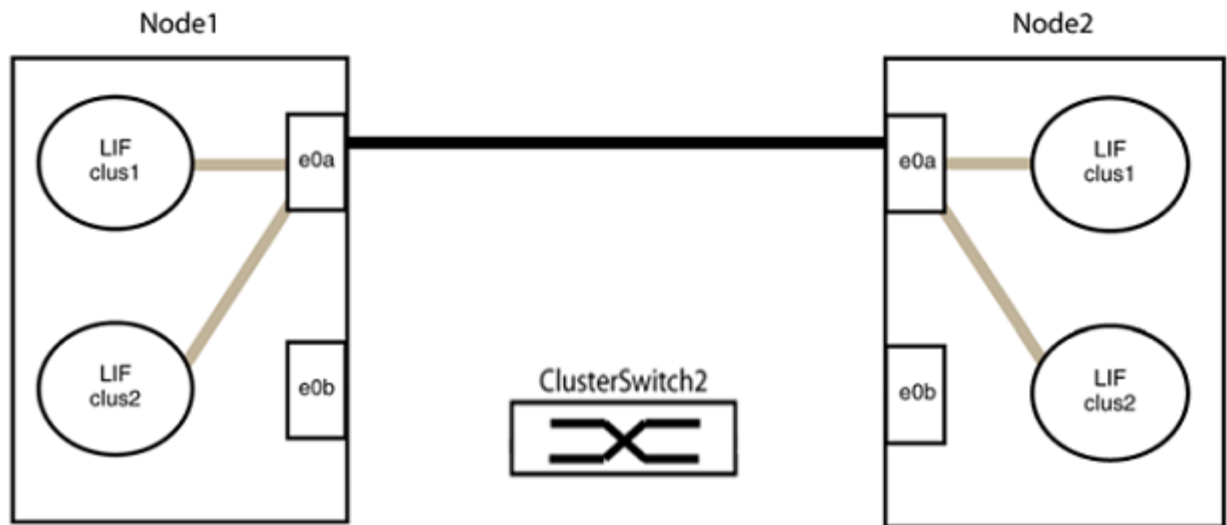
1. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 2 ein.



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
```

Cisco Nexus 92300YC

Erste Schritte

Installations- und Einrichtungsworkflow für Cisco Nexus 92300YC-Switches

Cisco Nexus 92300YC-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 92300YC-Switch zu installieren und einzurichten.

1

"Konfigurationsanforderungen"

Prüfen Sie die Konfigurationsanforderungen für den Cluster-Switch 92300YC.

2

"Erforderliche Dokumentation"

Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 92300YC-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 92300YC-Switches

Bei der Installation und Wartung des Cisco Nexus 92300YC Switches sollten Sie unbedingt alle Konfigurations- und Netzwerkanforderungen überprüfen.

Wenn Sie ONTAP -Cluster mit mehr als zwei Knoten aufbauen möchten, benötigen Sie zwei unterstützte Cluster-Netzwerk-Switches. Sie können zusätzliche Management-Schalter verwenden, die optional sind.

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 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 Ihre ["Komponenten und Teilenummern"](#)Die

Komponenten und Teilenummern für Cisco Nexus 92300YC-Switches

Bei der Installation und Wartung des Cisco Nexus 92300YC Switches sollten Sie unbedingt alle Switch-Komponenten und Teilenummern überprüfen. Siehe die ["Hardware Universe"](#) für Details. 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 folgende Tabelle listet die Teilenummer und Beschreibung für den Schalter 92300YC, die Lüfter und die Netzteile auf:

Teilenummer	Beschreibung
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX (PTSX = Port Side Exhaust)
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN (PSIN = Port Side Intake)
X-NXA-FAN-35CFM-B	Lüfter, Cisco N9K, seitlicher Lufteinlass
X-NXA-FAN-35CFM-F	Lüfter, Cisco N9K, seitlicher Luftauslass
X-NXA-PAC-650W-B	Netzteil, Cisco 650W - Einlass an der Portseite
X-NXA-PAC-650W-F	Netzteil, Cisco 650W - Auslassöffnung an der Portseite

Details zum Luftstrom des Cisco Nexus 92300YC Switches:

- Abluftstrom auf der Backbordseite (Standardluft) — Kühle Luft strömt durch die Lüfter- und Netzteilmodule im Kaltgang in das Gehäuse und wird durch das Backbordende des Gehäuses im Warmgang wieder ausgestoßen. Abluftstrom auf der Backbordseite mit blauer Färbung.
- Luftansaugung an der Backbordseite (umgekehrte Luftführung) — Kühle Luft strömt durch die Backbordseite im Kaltgang in das Gehäuse und wird durch die Lüfter- und Stromversorgungsmodule im Warmgang wieder ausgestoßen. Lufteinlass auf der Backbordseite mit bordeauxroter Färbung.

Was kommt als nächstes

Nachdem Sie Ihre Komponenten und Teilenummern bestätigt haben, können Sie die folgenden überprüfen: ["erforderliche Dokumentation"](#)Die

Dokumentationsanforderungen für Cisco Nexus 92300YC-Switches

Für die Installation und Wartung des Cisco Nexus 92300YC Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation durchlesen.

Switch-Dokumentation

Für die Einrichtung der Cisco Nexus 92300YC Switches benötigen Sie die folgende Dokumentation von ["Cisco Nexus 9000 Series Switches Unterstützung"](#) Seite:

Dokumenttitel	Beschreibung
<i>Hardware-Installationsanleitung für die Nexus 9000-Serie</i>	Bietet detaillierte Informationen zu Standortanforderungen, Hardware-Details der Schalter und Installationsoptionen.
<i>Softwarekonfigurationshandbücher für Cisco Nexus 9000 Series Switches</i> (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.
<i>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</i> (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 9000 Serie NX-OS Befehlsreferenz – Masterindex	Bietet Links zu den verschiedenen Befehlsreferenzen von Cisco.
Cisco Nexus 9000 MIBs-Referenz	Beschreibt die Management Information Base (MIB)-Dateien für die Nexus 9000 Switches.
<i>Referenz der NX-OS-Systemmeldungen der Nexus 9000-Serie</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000-Serie, sowohl die informativen als auch die, die bei der Diagnose von Problemen mit Verbindungen, interner Hardware oder der Systemsoftware hilfreich sein können.
<i>Cisco Nexus 9000 Series NX-OS Versionshinweise</i> (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)	Beschreibt die Funktionen, Fehler und Einschränkungen der Cisco Nexus 9000-Serie.
Informationen zur Einhaltung gesetzlicher Bestimmungen und zur Sicherheit für die Cisco Nexus 9000-Serie	Bietet Informationen zur Einhaltung internationaler behördlicher Vorschriften, zur Sicherheit und zu gesetzlichen Bestimmungen für die Switches der Serie Nexus 9000.

ONTAP-Systemdokumentation

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

Name	Beschreibung
Controllerspezifische <i>Installations- und Einrichtungsanweisungen</i>	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 Nexus 92300YC 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 92300YC Switch in einem NetApp -Schrank "	Beschreibt die Installation eines Cisco Nexus 92300YC 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 92300YC-Switches

Gehen Sie folgendermaßen vor, um die Hardware für einen 92300YC-Cluster-Switch zu installieren und zu konfigurieren:

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 Schalter 92300YC.

3

"Installieren Sie den Switch in einem NetApp -Schränk."

Installieren Sie den 92300YC-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 92300YC

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.

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	10/25 GbE-Knoten	1	10/25 GbE-Knoten

Clusterschalter A		Clusterschalter B	
2	10/25 GbE-Knoten	2	10/25 GbE-Knoten
3	10/25 GbE-Knoten	3	10/25 GbE-Knoten
4	10/25 GbE-Knoten	4	10/25 GbE-Knoten
5	10/25 GbE-Knoten	5	10/25 GbE-Knoten
6	10/25 GbE-Knoten	6	10/25 GbE-Knoten
7	10/25 GbE-Knoten	7	10/25 GbE-Knoten
8	10/25 GbE-Knoten	8	10/25 GbE-Knoten
9	10/25 GbE-Knoten	9	10/25 GbE-Knoten
10	10/25 GbE-Knoten	10	10/25 GbE-Knoten
11	10/25 GbE-Knoten	11	10/25 GbE-Knoten
12	10/25 GbE-Knoten	12	10/25 GbE-Knoten
13	10/25 GbE-Knoten	13	10/25 GbE-Knoten
14	10/25 GbE-Knoten	14	10/25 GbE-Knoten
15	10/25 GbE-Knoten	15	10/25 GbE-Knoten
16	10/25 GbE-Knoten	16	10/25 GbE-Knoten
17	10/25 GbE-Knoten	17	10/25 GbE-Knoten
18	10/25 GbE-Knoten	18	10/25 GbE-Knoten
19	10/25 GbE-Knoten	19	10/25 GbE-Knoten
20	10/25 GbE-Knoten	20	10/25 GbE-Knoten
21	10/25 GbE-Knoten	21	10/25 GbE-Knoten
22	10/25 GbE-Knoten	22	10/25 GbE-Knoten
23	10/25 GbE-Knoten	23	10/25 GbE-Knoten

Clusterschalter A		Clusterschalter B	
24	10/25 GbE-Knoten	24	10/25 GbE-Knoten
25	10/25 GbE-Knoten	25	10/25 GbE-Knoten
26	10/25 GbE-Knoten	26	10/25 GbE-Knoten
27	10/25 GbE-Knoten	27	10/25 GbE-Knoten
28	10/25 GbE-Knoten	28	10/25 GbE-Knoten
29	10/25 GbE-Knoten	29	10/25 GbE-Knoten
30	10/25 GbE-Knoten	30	10/25 GbE-Knoten
31	10/25 GbE-Knoten	31	10/25 GbE-Knoten
32	10/25 GbE-Knoten	32	10/25 GbE-Knoten
33	10/25 GbE-Knoten	33	10/25 GbE-Knoten
34	10/25 GbE-Knoten	34	10/25 GbE-Knoten
35	10/25 GbE-Knoten	35	10/25 GbE-Knoten
36	10/25 GbE-Knoten	36	10/25 GbE-Knoten
37	10/25 GbE-Knoten	37	10/25 GbE-Knoten
38	10/25 GbE-Knoten	38	10/25 GbE-Knoten
39	10/25 GbE-Knoten	39	10/25 GbE-Knoten
40	10/25 GbE-Knoten	40	10/25 GbE-Knoten
41	10/25 GbE-Knoten	41	10/25 GbE-Knoten
42	10/25 GbE-Knoten	42	10/25 GbE-Knoten
43	10/25 GbE-Knoten	43	10/25 GbE-Knoten
44	10/25 GbE-Knoten	44	10/25 GbE-Knoten
45	10/25 GbE-Knoten	45	10/25 GbE-Knoten

Clusterschalter A		Clusterschalter B	
46	10/25 GbE-Knoten	46	10/25 GbE-Knoten
47	10/25 GbE-Knoten	47	10/25 GbE-Knoten
48	10/25 GbE-Knoten	48	10/25 GbE-Knoten
49	40/100-GbE-Knoten	49	40/100-GbE-Knoten
50	40/100-GbE-Knoten	50	40/100-GbE-Knoten
51	40/100-GbE-Knoten	51	40/100-GbE-Knoten
52	40/100-GbE-Knoten	52	40/100-GbE-Knoten
53	40/100-GbE-Knoten	53	40/100-GbE-Knoten
54	40/100-GbE-Knoten	54	40/100-GbE-Knoten
55	40/100-GbE-Knoten	55	40/100-GbE-Knoten
56	40/100-GbE-Knoten	56	40/100-GbE-Knoten
57	40/100-GbE-Knoten	57	40/100-GbE-Knoten
58	40/100-GbE-Knoten	58	40/100-GbE-Knoten
59	40/100-GbE-Knoten	59	40/100-GbE-Knoten
60	40/100-GbE-Knoten	60	40/100-GbE-Knoten
61	40/100-GbE-Knoten	61	40/100-GbE-Knoten
62	40/100-GbE-Knoten	62	40/100-GbE-Knoten
63	40/100-GbE-Knoten	63	40/100-GbE-Knoten
64	40/100-GbE-Knoten	64	40/100-GbE-Knoten
65	100-GbE-ISL-zu-Switch-B-Port 65	65	100-GbE-ISL-zu-Switch-A-Port 65
66	100-GbE-ISL-zu-Switch-B-Port 66	66	100-GbE-ISL-zu-Switch-A-Port 65

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	
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	

Clusterschalter A		Clusterschalter B	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	

Clusterschalter A		Clusterschalter B	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	

Clusterschalter A		Clusterschalter B	
64		64	
65	ISL zum Schalter B Port 65	65	ISL zum Umschalten von Port 65
66	ISL zum Schalter B Port 66	66	ISL zum Umschalten von Port 66

Was kommt als nächstes

Nachdem Sie Ihre Verkabelungsarbeitsblätter ausgefüllt haben, können Sie ["Installieren Sie den Schalter"](#) Die

Installieren Sie den Cluster-Switch 92300YC

Gehen Sie wie folgt vor, um den Cisco Nexus 92300YC 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 92300YC in einem NetApp -Systemschrank	Anweisungen zur Installation des Switches in einem NetApp -Schrank finden Sie im Handbuch „Installieren eines Cisco Nexus 92300YC-Cluster-Switches und Pass-Through-Panels in einem NetApp -Schrank“.
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 3223C-Switch in einem NetApp -Schrank"](#) Die Ansonsten gehen Sie zu ["Kabel und Konfiguration prüfen"](#) Die

Installieren Sie einen Cisco Nexus 92300YC-Cluster-Switch in einem NetApp Schrank

Abhängig von Ihrer Konfiguration müssen Sie den Cisco Nexus 92300YC-Cluster-Switch und das Pass-Through-Panel möglicherweise mit den im Lieferumfang des Switches enthaltenen Standardhalterungen in einem NetApp -Schrank installieren.

Bevor Sie beginnen

- Die anfänglichen Vorbereitungsanforderungen, der Inhalt des Kits und die Sicherheitsvorkehrungen im ["Hardware-Installationshandbuch für die Cisco Nexus 9000-Serie"](#) Die
- Für jeden Schalter werden die acht 10-32 oder 12-24 Schrauben und Clipmutter benötigt, um die Halterungen und Gleitschienen an den vorderen und hinteren Gehäusepfosten zu befestigen.
- 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.

Das Durchgangspanel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

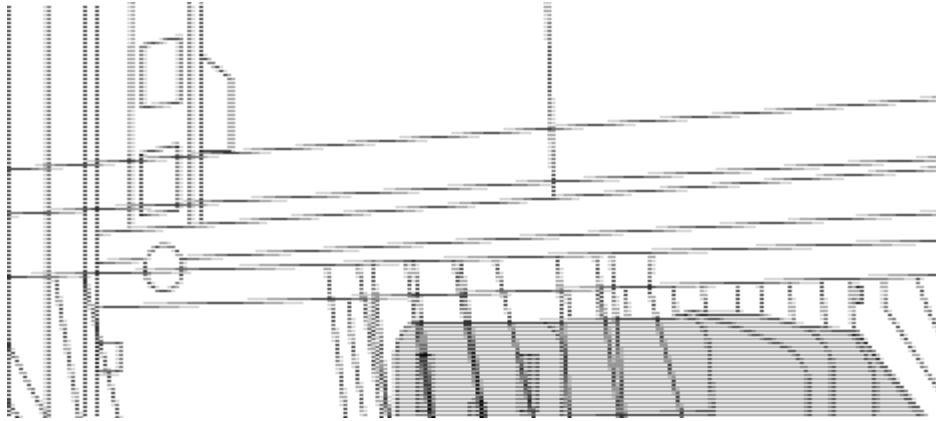
Das NetApp Pass-Through-Panel-Kit enthält die folgende Hardware:

- Eine Durchgangs-Blindplatte
- Vier 10-32 x 0,75 Schrauben
- Vier 10-32 Clipmuttern

i. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

Bei diesem Verfahren wird die Abdeckplatte in U40 installiert.

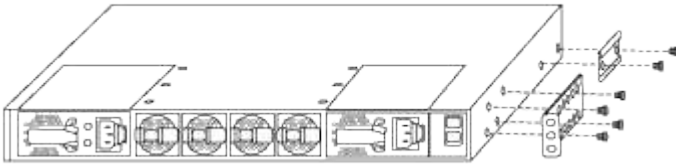
- ii. Montieren Sie auf jeder Seite zwei Clipmuttern in den entsprechenden quadratischen Löchern für die vorderen Schrankschienen.
- iii. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.
- iv. Führen Sie die weiblichen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



(1) Weiblicher Stecker des Überbrückungskabels.

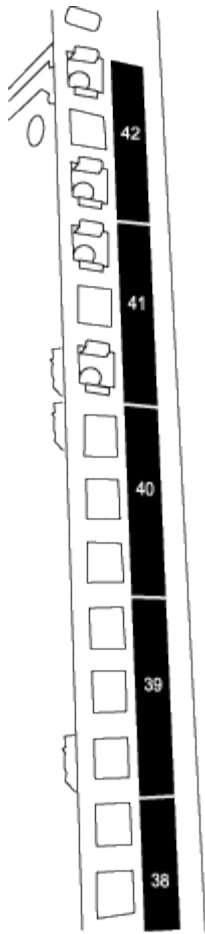
1. Installieren Sie die Rackmontagehalterungen am Nexus 92300YC-Switch-Gehäuse.

- 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.

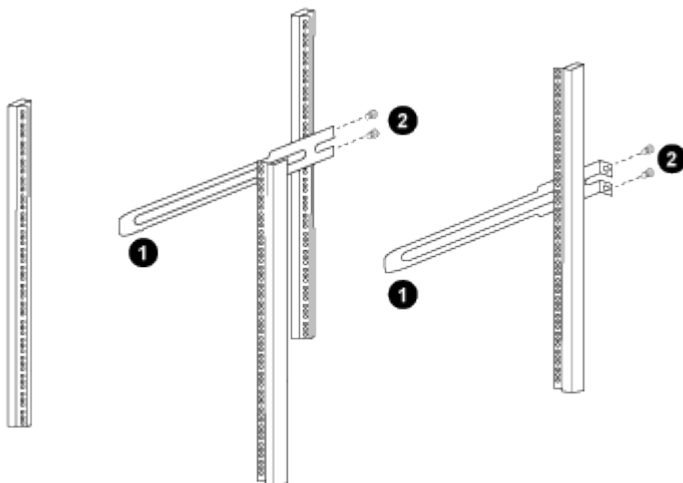
2. Installieren Sie die Clipmuttern in den quadratischen Lochpositionen für alle vier IEA-Pfosten.



Die beiden 92300YC-Switches werden immer in den oberen 2 HE der Schränke RU41 und 42 montiert.

3. 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.



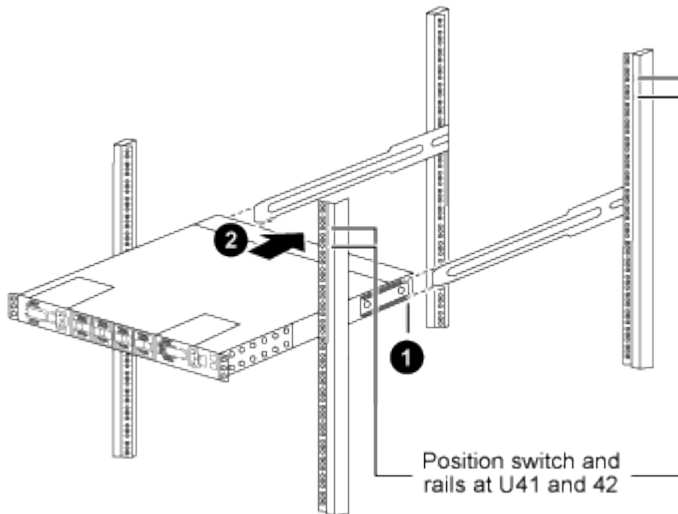
- (1) Schieben Sie die Gleitschiene vorsichtig und richten Sie sie an den Schraubenlöchern im Gestell aus.
- (2) Ziehen Sie die Schrauben der Gleitschienen an den Schrankpfosten fest.

- a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.
 - b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Positionen am Schrank.
4. 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.

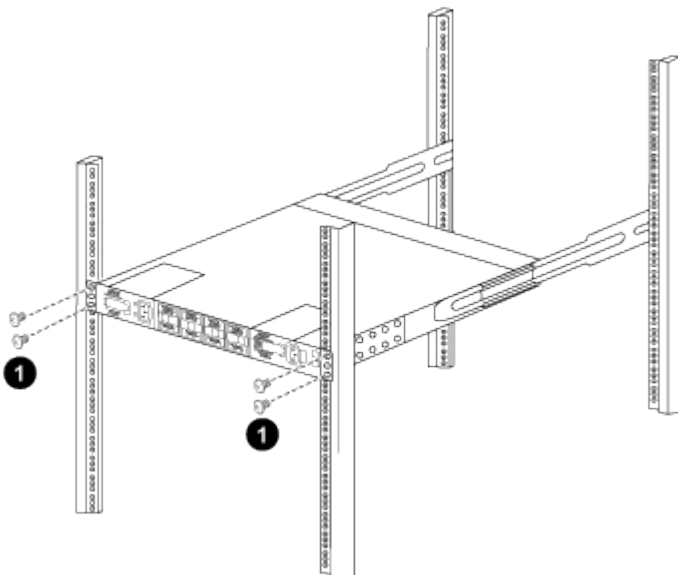
- a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(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 waagrecht 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.



Durch die Verwendung des fertig montierten Schalters als Stütze ist es nicht notwendig, den zweiten Schalter während des Montagevorgangs vorne festzuhalten.

5. Wenn die Schalter installiert sind, schließen Sie die Überbrückungskabel an die Stromeingänge der Schalter an.
6. 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.

7. Verbinden Sie den Verwaltungsport an jedem 92300YC-Switch mit einem der Verwaltungsswitches (falls bestellt) oder verbinden Sie sie direkt mit Ihrem Verwaltungsnetzwerk.

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.

Was kommt als nächstes

Nachdem Sie die Switches im NetApp -Schrack installiert haben, können Sie ["Konfigurieren Sie den Switch"](#) Die

Überprüfung der Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 92300YC 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
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(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.

Konfigurieren der Software

Workflow zur Softwareinstallation für Cisco Nexus 92300YC-Cluster-Switches

Um die Software für einen Cisco Nexus 92300YC-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 Cluster-Switch 92300YC.

2

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

Die Cisco NX-OS-Software und Referenzkonfigurationsdateien (RCFs) müssen auf Cisco 92300YC-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 392300YC-Cluster-Switch.

4

"Installieren Sie den RCF"

Installieren Sie das RCF, nachdem Sie den Cisco 92300YC-Switch zum ersten Mal eingerichtet haben.

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.

Konfigurieren Sie den Cisco Nexus 92300YC-Switch

Gehen Sie wie folgt vor, um den Cisco Nexus 92300YC Switch einzurichten und zu konfigurieren.

Schritte

1. Verbinden Sie den seriellen Port mit einem Host oder einem seriellen Port.
2. Verbinden Sie den Management-Port (auf der Nicht-Port-Seite des Switches) mit demselben Netzwerk, in dem sich Ihr SFTP-Server befindet.
3. Nehmen Sie an der Konsole die seriellen Einstellungen auf dem Host vor:
 - 9600 Baud

- 8 Datenbits
 - 1 Stoppbit
 - Parität: keine
 - Flusssteuerung: keine
4. Beim erstmaligen Hochfahren oder beim Neustart nach dem Löschen der laufenden Konfiguration gerät der Switch Nexus 92300YC in eine Boot-Schleife. Unterbrechen Sie diesen Vorgang, indem Sie **ja** eingeben, um die automatische Stromversorgung abzubrechen.

Die Einrichtung des Systemadministratorkontos wird angezeigt.

Beispiel anzeigen

```
$ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
[yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no) [no]: y
Disabling POAP.....Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
wait... (This may take 5-15 minutes)

      ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:
```

5. Geben Sie **y** ein, um den sicheren Passwortstandard zu erzwingen:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Geben Sie das Passwort für den Benutzer „admin“ ein und bestätigen Sie es:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Geben Sie **ja** ein, um den Dialog „Systemgrundkonfiguration“ aufzurufen.

Beispiel anzeigen

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

Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 devices must be registered to receive entitled support services.

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

Would you like to enter the basic configuration dialog (yes/no):

8. Erstellen Sie ein weiteres Benutzerkonto:

Create another login account (yes/no) [n]:

9. Konfigurieren von schreibgeschützten und Lese-/Schreib-SNMP-Community-Strings:

Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:

10. Konfigurieren Sie den Cluster-Switch-Namen:

Enter the switch name : **cs2**

11. Konfigurieren Sie die Out-of-Band-Managementschnittstelle:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Erweiterte IP-Optionen konfigurieren:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Telnet-Dienste konfigurieren:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Konfigurieren von SSH-Diensten und SSH-Schlüsseln:

```
Enable the ssh service? (yes/no) [y]: y

Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Konfigurieren Sie weitere Einstellungen:

```
Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L2]: L2

Configure default switchport interface state (shut/noshut) [noshut]:
noshut

Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Schalterinformationen bestätigen und Konfiguration speichern:

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

```
Use this configuration and save it? (yes/no) [y]: y
```

```
[ ] 100%
```

```
Copy complete, now saving to disk (please wait)...
```

```
Copy complete.
```

Wie geht es weiter?

Nachdem Sie Ihre Schalter konfiguriert haben, können Sie ["Bereiten Sie die Installation der NX-OS-Software und RCF vor"](#)Die

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Geeignete Software und Upgrade-Anleitungen sind erhältlich bei ["Cisco Nexus 9000 Series Switches"](#) Die

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.

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 `node1` Und `node2` Die
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.
- 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 9000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben. Die Befehlsausgaben können je nach ONTAP Version variieren.

Schritte

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

```
set -privilege advanced
```

Die erweiterte Aufforderung(*>) erscheint.

2. 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.

Der folgende Befehl unterdrückt die automatische Fallerstellung für zwei Stunden:

```
cluster1:> **system node autosupport invoke -node * -type all -message  
MAINT=2h**
```

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-
C92300YC				
	e0b	cs2	Eth1/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C92300YC				
	e0b	cs2	Eth1/1	N9K-
C92300YC				

4 entries were displayed.

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: node2

Health					Speed (Mbps)	
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: node1

Health					Speed (Mbps)	
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						

4 entries were displayed.

b. Informationen zu den LIFs anzeigen: `network interface show -vserver Cluster`

Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	node1_clus1	up/up	169.254.209.69/16	node1
e0b	true			
e0a	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
e0a	node2_clus1	up/up	169.254.47.194/16	node2
e0b	true			
e0a	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 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 169.254.19.183 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. Überprüfen Sie, ob der Befehl zur automatischen Rücksetzung auf allen Cluster-LIFs aktiviert ist:

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

Beispiel anzeigen

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

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

Wie geht es weiter?

Nachdem Sie die Installation der NX-OS-Software und von RCF vorbereitet haben, können Sie ["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 Switch Nexus 92300YC zu installieren.

NX-OS ist ein Netzwerkbetriebssystem für die Nexus-Serie von Ethernet-Switches und die MDS-Serie von Fibre Channel (FC) Storage Area Network Switches von Cisco Systems.

Überprüfungsanforderungen

Unterstützte Ports und Knotenverbindungen

- Die für die Nexus 92300YC Switches unterstützten Inter-Switch Links (ISLs) sind die Ports 1/65 und 1/66.
- Die für die Nexus 92300YC Switches unterstützten Knotenverbindungen sind die Ports 1/1 bis 1/66.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Die passende NetApp Cisco NX-OS-Software für Ihre Switches finden Sie auf der NetApp Support-Website. ["mysupport.netapp.com"](https://mysupport.netapp.com)
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- ["Cisco Ethernet-Switch-Seite"](#). In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und NX-OS-Versionen.

Installieren Sie die Software

Die Beispiele in diesem Verfahren verwenden zwei Knoten, aber ein Cluster kann bis zu 24 Knoten umfassen.

Zu den Beispielen

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

- Die Bezeichnungen der Nexus 92300YC-Switches lauten: `cs1` Und `cs2` Die
- Das in diesem Verfahren verwendete Beispiel startet das Upgrade auf dem zweiten Switch, `*cs2*`.
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.
- Der IPspace-Name lautet: `Cluster` Die
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Knoten sind benannt `e0a` Und `e0b` Die

Siehe die "[Hardware-Universum^](#)" für die tatsächlich von Ihrer Plattform unterstützten Cluster-Ports. 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](#).

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

Dieses Beispiel bestätigt, dass der Switch den Server unter der IP-Adresse 172.19.2.1 erreichen kann:

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

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

3. Kopieren Sie die NX-OS-Software und die EPLD-Images auf den Nexus 92300YC-Switch.

Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.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:
sftp> progress
Progress meter enabled
sftp> get /code/nxos.9.2.2.bin /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.bin 100% 1261MB 9.3MB/s 02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.2.2.img
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:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.2.2.img /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. 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) 2002-2018, 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 05.31
  NXOS: version 9.2(1)
  BIOS compile time: 05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time: 7/17/2018 16:00:00 [07/18/2018 00:21:19]

Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

  Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
System version: 9.2(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. 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.9.2.2.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

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

```
Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.2.2.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	9.2(1)	
9.2(2)	yes		
1	bios	v05.31(05/17/2018):v05.28(01/18/2018)	
v05.33(09/08/2018)	yes		

```
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
```

```
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:  
Successfully deactivated virtual service 'guestshell+'
```

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

6. 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) 2002-2018, 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 05.33
  NXOS: version 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)
```

```
Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

Reason: Reset due to upgrade

System version: 9.2(1)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

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

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	IO FPGA	Success

1 SUP Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. Nach dem Neustart des Switches melden Sie sich erneut an und überprüfen Sie, ob die neue Version von EPLD erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# *show version module 1 epld*
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x19
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

Wie geht es weiter?

Nach der Installation der NX-OS-Software können Sie ["Installieren Sie die Referenzkonfigurationsdatei"](#)Die

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können die RCF-Datei installieren, nachdem Sie den Switch Nexus 92300YC zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

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.

Informationen zu diesem Vorgang

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 node1 Und node2 Die
- Die Cluster-LIF-Namen sind node1_clus1 , node1_clus2 , node2_clus1 , Und node2_clus2 Die
- Der cluster1 : : * > Die Eingabeaufforderung zeigt den Namen des Clusters an.



- Das Verfahren erfordert die Verwendung sowohl von ONTAP -Befehlen als auch von "[Cisco Nexus 9000 Series Switches](#)" Sofern nicht anders angegeben, werden ONTAP -Befehle verwendet.
- Bevor Sie diese Prozedur durchführen, stellen Sie sicher, dass Sie über eine aktuelle Sicherungskopie der Switch-Konfiguration verfügen.
- 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.

Schritte

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
-----
node1/cdp
C92300YC   e0a     cs1                      Ethernet1/1/1      N9K-
C92300YC   e0b     cs2                      Ethernet1/1/1      N9K-
node2/cdp
C92300YC   e0a     cs1                      Ethernet1/1/2      N9K-
C92300YC   e0b     cs2                      Ethernet1/1/2      N9K-
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: node1

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e0c         Cluster      Cluster      up    9000  auto/100000
healthy false
e0d         Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node2

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e0c         Cluster      Cluster      up    9000  auto/100000
healthy false
e0d         Cluster      Cluster      up    9000  auto/100000
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
e0c      true      node1_clus1      up/up      169.254.3.4/23      node1
e0d      true      node1_clus2      up/up      169.254.3.5/23      node1
e0c      true      node2_clus1      up/up      169.254.3.8/23      node2
e0d      true      node2_clus2      up/up      169.254.3.9/23      node2
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                    10.233.205.92
N9K-C92300YC
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                                9.3(4)
    Version Source: CDP

cs2                                  cluster-network                    10.233.205.93
N9K-C92300YC
    Serial Number: FOXXXXXXXXGD
    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.
```

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

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

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Überprüfen Sie, ob die Cluster-Ports auf die Ports migriert wurden, die auf dem Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern. `network interface show -vserver`

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	node1_clus1	up/up	169.254.3.4/23	node1
e0c	true			
	node1_clus2	up/up	169.254.3.5/23	node1
e0c	false			
	node2_clus1	up/up	169.254.3.8/23	node2
e0c	true			
	node2_clus2	up/up	169.254.3.9/23	node2
e0c	false			

```
cluster1::*>
```

6. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert: `cluster show`

Beispiel anzeigen

```
cluster1::*> *cluster show*
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	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. Bereinigen Sie die Konfiguration auf Switch CS2 und führen Sie eine grundlegende Einrichtung durch.



Beim Aktualisieren oder Anwenden eines neuen RCF müssen Sie die Schaltereinstellungen löschen und eine grundlegende Konfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase
```

Warning: This command will erase the startup-configuration.

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

b. Führen Sie einen Neustart des Switches durch:

Beispiel anzeigen

```
(cs2)# reload
```

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

9. 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 Handbuch im "[Cisco Nexus 9000 Series Switches](#)" Führer.

Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches CS2 zu kopieren:

```
cs2# copy tftp: bootflash: vrf management  
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt  
Enter hostname for the tftp 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:  
tftp> progress  
Progress meter enabled  
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin  
/code/Nexus_92300YC_R 100% 9687 530.2KB/s 00:00  
tftp> exit  
Copy complete, now saving to disk (please wait)...  
Copy complete.
```

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

Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000](#)

Dieses Beispiel zeigt die RCF-Datei. Nexus_92300YC_RCF_v1.0.2.txt wird auf Switch CS2 installiert:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands
```

```
Disabling ssh: as its enabled right now:
```

```
  generating ecdsa key(521 bits).....
```

```
generated ecdsa key
```

```
Enabling ssh: as it has been disabled
```

```
  this command enables edge port type (portfast) by default on all  
interfaces. You
```

```
  should now disable edge port type (portfast) explicitly on switched  
ports leading to hubs,
```

```
  switches and bridges as they may create temporary bridging loops.
```

```
Edge port type (portfast) should only be enabled on ports connected to a  
single
```

```
  host. Connecting hubs, concentrators, switches, bridges, etc... to  
this
```

```
  interface when edge port type (portfast) is enabled, can cause  
temporary bridging loops.
```

```
  Use with CAUTION
```

```
Edge Port Type (Portfast) has been configured on Ethernet1/1 but will  
only
```

```
  have effect when the interface is in a non-trunking mode.
```

```
...
```

```
Copy complete, now saving to disk (please wait)...
```

```
Copy complete.
```

11. Überprüfen Sie auf dem Switch, ob die RCF-Datei erfolgreich zusammengeführt wurde:

```
show running-config
```

```

cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJlRtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1 - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*

```



Bei der erstmaligen Anwendung des RCF ist die Fehlermeldung **ERROR: Failed to write VSH commands** zu erwarten und kann ignoriert werden.

1. Überprüfen Sie, ob die RCF-Datei die richtige neuere Version ist: `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 Porteneinstellungen
- 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.

2. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe ["Überprüfung der Verkabelung und Konfigurationsüberlegungen"](#) Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
3. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Schaltereinstellungen korrekt sind, kopieren Sie die Running-Config-Datei in die Startup-Config-Datei.

Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im ["Cisco Nexus 9000 Series Switches"](#) Führer.

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

4. Neustart des Switches CS2. Sie können die auf den Knoten gemeldeten Ereignisse vom Typ „Cluster-Ports ausgefallen“ ignorieren, während der Switch neu startet.

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

5. Überprüfen Sie den Zustand der Cluster-Ports im Cluster.
 - a. Überprüfen Sie, ob die e0d-Ports auf allen Knoten im Cluster aktiv und fehlerfrei sind: `network port show -ip space Cluster`

Beispiel anzeigen

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

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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
```

- b. Überprüfen Sie den Zustand des Switches vom Cluster aus (dabei wird möglicherweise der Switch cs2 nicht angezeigt, da LIFs nicht auf e0d liegen).

Beispiel anzeigen



```

cluster1::*> *network device-discovery show -protocol cdp*
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1/cdp
          e0a    cs1                      Ethernet1/1
N9K-C92300YC
          e0b    cs2                      Ethernet1/1
N9K-C92300YC
node2/cdp
          e0a    cs1                      Ethernet1/2
N9K-C92300YC
          e0b    cs2                      Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch          Type          Address
Model
-----
cs1              cluster-network  10.233.205.90
N9K-C92300YC
    Serial Number: FOXXXXXXXXGD
    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
N9K-C92300YC
    Serial Number: FOXXXXXXXXGS
    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.

```

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.
```

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

Das folgende Beispiel verwendet die Ausgabe des Schnittstellenbeispiels aus Schritt 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

- 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
e0d      node1_clus1      up/up      169.254.3.4/23      node1
false
e0d      node1_clus2      up/up      169.254.3.5/23      node1
true
e0d      node2_clus1      up/up      169.254.3.8/23      node2
false
e0d      node2_clus2      up/up      169.254.3.9/23      node2
true
cluster1::*>
```

- Überprüfen Sie, ob der Cluster fehlerfrei funktioniert: `cluster show`

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node           Health   Eligibility   Epsilon
-----
node1          true    true          false
node2          true    true          false
cluster1::*>
```

9. Wiederholen Sie die Schritte 7 bis 14 auf Switch cs1.
10. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

11. 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
```

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

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1      eth  access up    none
10G(D) --
Ethernet1/2      1      eth  access up    none
10G(D) --
Ethernet1/3      1      eth  trunk  up    none
100G(D) --
Ethernet1/4      1      eth  trunk  up    none
100G(D) --
.
.
```

13. 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      Eth1/65 (P)  Eth1/66 (P)
cs1#
```

14. 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
          node1_clus1  up/up      169.254.3.4/23  node1
e0d       true
          node1_clus2  up/up      169.254.3.5/23  node1
e0d       true
          node2_clus1  up/up      169.254.3.8/23  node2
e0d       true
          node2_clus2  up/up      169.254.3.9/23  node2
e0d       true
cluster1::*>
```

15. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert: `cluster show`

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node           Health Eligibility  Epsilon
-----
node1          true   true       false
node2          true   true       false
```

16. 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 node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)

```

Wie geht es weiter?

Nach der Installation des RCF können Sie ["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  
AAAAB3NzaC1yc2EAAAADAQABAAQgQDiNrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew  
17nwlIoC6HBejxluIObAH8hrW8kR+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  
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e  
vke273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z  
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1  
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

Schalter migrieren

Migrieren Sie zu einem Zwei-Knoten-Switch-Cluster mit einem Cisco Nexus 92300YC-Switch

Wenn Sie bereits eine *switchlose* Clusterumgebung mit zwei Knoten besitzen, können Sie mithilfe von Cisco Nexus 92300YC Switches zu einer *switched* Clusterumgebung mit zwei Knoten migrieren, um die Anzahl der Knoten im Cluster auf mehr als zwei zu erhöhen.

Die Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerkanschlüsse oder an jedem Controller einen einzelnen Clusteranschluss haben. Der dokumentierte Prozess funktioniert für alle Knoten, die optische oder Twinax-Anschlüsse verwenden, wird jedoch von diesem Switch nicht unterstützt, wenn die Knoten Onboard-10Gb BASE-T RJ45-Anschlüsse für die Cluster-Netzwerkanschlüsse verwenden.

Die meisten Systeme benötigen zwei dedizierte Cluster-Netzwerkanschlüsse an jedem Controller.



Nach Abschluss der Migration müssen Sie möglicherweise die erforderliche Konfigurationsdatei installieren, um den Cluster Switch Health Monitor (CSHM) für 92300YC Cluster-Switches zu unterstützen. Sehen "[Switch-Zustandsüberwachung \(CSHM\)](#)".

Überprüfungsanforderungen

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

Bei einer schalterlosen Konfiguration mit zwei Knoten ist Folgendes sicherzustellen:

- Die Zwei-Knoten-Konfiguration ohne Schalter ist ordnungsgemäß eingerichtet und funktioniert.
- Auf den Knoten läuft ONTAP 9.6 oder höher.
- Alle Cluster-Ports befinden sich im Status **up**.
- Alle logischen Schnittstellen (LIFs) des Clusters befinden sich im Status **up** und sind an ihren jeweiligen Ports angeschlossen.

Für die Konfiguration des Cisco Nexus 92300YC Switches:

- Beide Switches verfügen über eine Management-Netzwerkanbindung.
- Es besteht Konsolenzugriff auf die Cluster-Switches.
- Die Knoten-zu-Knoten- und Schalter-zu-Schalter-Verbindungen des Nexus 92300YC verwenden Twinax- oder Glasfaserkabel.

"[Hardware Universe – Schalter](#)" enthält weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel sind an die Ports 1/65 und 1/66 beider 92300YC-Switches angeschlossen.
- Die erste Anpassung beider 92300YC-Switches ist abgeschlossen. Damit die:
 - Auf den 92300YC-Switches läuft die neueste Softwareversion.
 - Referenzkonfigurationsdateien (RCFs) werden auf die Switches angewendet. Jegliche standortspezifische Anpassung, wie z. B. SMTP, SNMP und SSH, wird auf den neuen Switches konfiguriert.

Den Schalter migrieren

Zu den Beispielen

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

- Die Bezeichnungen der 92300YC-Switches lauten cs1 und cs2.
- Die Namen der Cluster-SVMs lauten node1 und node2.
- Die Namen der LIFs lauten node1_clus1 und node1_clus2 auf Knoten 1 bzw. node2_clus1 und node2_clus2 auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e0a und e0b.

["Hardware Universe"](#) Enthält die aktuellsten Informationen zu den tatsächlichen Cluster-Ports für Ihre Plattformen.

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. 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.

Beispiel anzeigen

Der folgende Befehl unterdrückt die automatische Fallerstellung für zwei Stunden:

```
cluster1::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Schritt 2: Kabel und Anschlüsse konfigurieren

1. Deaktivieren Sie alle zum Knoten führenden Ports (außer ISL-Ports) an den beiden neuen Cluster-Switches cs1 und cs2.

Die ISL-Ports dürfen nicht deaktiviert werden.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die dem Knoten zugewandten Ports 1 bis 64 am Switch cs1 deaktiviert sind:

```
cs1# config  
Enter configuration commands, one per line. End with CNTL/Z.  
cs1(config)# interface e/1-64  
cs1(config-if-range)# shutdown
```

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden 92300YC-Switches cs1 und cs2 an den Ports 1/65 und 1/66 aktiv sind:

```
show port-channel summary
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs1 aktiv sind:

```
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      Eth1/65 (P)  Eth1/66 (P)
```

+ Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch cs2 aktiv sind:

+

```
(cs2)# 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      Eth1/65 (P)  Eth1/66 (P)
```

3. Liste der benachbarten Geräte anzeigen:

```
show cdp neighbors
```

Dieser Befehl liefert Informationen über die mit dem System verbundenen Geräte.

Beispiel anzeigen

Das folgende Beispiel listet die benachbarten Geräte am Switch cs1 auf:

```
cs1# 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
cs2 (FDO220329V5) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs2 (FDO220329V5) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 2

+ Das folgende Beispiel listet die benachbarten Geräte am Switch cs2 auf:

+

```
cs2# 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
cs1 (FDO220329KU) Eth1/65	Eth1/65	177	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	177	R S I s	N9K-C92300YC

Total entries displayed: 2

4. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Jeder Port sollte angezeigt werden für Link und gesund für Health Status Die

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4 entries were displayed.

5. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind:

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

Jeder Cluster-LIF sollte „true“ anzeigen für Is Home und haben Status Admin/Oper von oben/aufwärts

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

4 entries were displayed.

6. Automatische Wiederherstellung auf allen Cluster-LIFs deaktivieren:

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

Beispiel anzeigen

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

	Logical	
Vserver	Interface	auto-revert

Cluster		
	node1_clus1	false
	node1_clus2	false
	node2_clus1	false
	node2_clus2	false

4 entries were displayed.

7. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 1 und verbinden Sie dann e0a mit Port 1 auf dem Cluster-Switch cs1. Verwenden Sie dazu die von den 92300YC-Switches unterstützten geeigneten Kabel.

Der "[Hardware Universe - Schalter](#)" enthält weitere Informationen zur Verkabelung.

8. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 2 und verbinden Sie dann e0a mit Port 2 auf Cluster-Switch cs1. Verwenden Sie dazu die von den 92300YC-Switches unterstützten Kabel.
9. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/64 am Switch cs1 aktiviert sind:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

10. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind und als „true“ angezeigt werden. Is Home :

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf Knoten 1 und Knoten 2 aktiv sind und dass Is Home Die Ergebnisse sind korrekt:

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	----				
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

4 entries were displayed.

11. Informationen über den Status der Knoten im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster an:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1	true	true	false
node2	true	true	false

```
2 entries were displayed.
```

12. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 1 und verbinden Sie dann e0b mit Port 1 auf Cluster-Switch cs2. Verwenden Sie dazu die von den 92300YC-Switches unterstützten geeigneten Kabel.
13. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 2 und verbinden Sie dann e0b mit Port 2 des Cluster-Switches cs2 unter Verwendung der von den 92300YC-Switches unterstützten geeigneten Verkabelung.
14. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs2.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/64 am Switch cs2 aktiviert sind:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-64
cs2(config-if-range)# no shutdown
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

2. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

```
network port show -ipSpace Cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports auf Knoten 1 und Knoten 2 aktiv sind:

```
cluster1::*> 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. Überprüfen Sie, ob alle Schnittstellen den Wert „true“ anzeigen. Is Home :

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



Dieser Vorgang kann mehrere Minuten dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf Knoten 1 und Knoten 2 aktiv sind und dass Is Home Die Ergebnisse sind korrekt:

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

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	----				
Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
true					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

4 entries were displayed.

4. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
show cdp neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
(cs1)# 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs2 (FDO220329V5) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs2 (FDO220329V5) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 4

```
(cs2)# 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	133	H	FAS2980
node2 e0b	Eth1/2	133	H	FAS2980
cs1 (FDO220329KU) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 4

5. Informationen zu den in Ihrem Cluster gefundenen Netzwerkgeräten anzeigen:

```
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
-----
node2          /cdp
               e0a     cs1                      0/2      N9K-
C92300YC
               e0b     cs2                      0/2      N9K-
C92300YC
node1          /cdp
               e0a     cs1                      0/1      N9K-
C92300YC
               e0b     cs2                      0/1      N9K-
C92300YC

4 entries were displayed.
```

6. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

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



Die Ausführung des Befehls kann mehrere Minuten dauern. Warten Sie auf die Ansage „Noch 3 Minuten bis zum Ablauf der Gültigkeitsdauer“.

Beispiel anzeigen

Die falsche Ausgabe im folgenden Beispiel zeigt, dass die Konfigurationseinstellungen deaktiviert sind:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

7. Überprüfen Sie den Status der Knoten im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	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 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 Fehlerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

Beispiel anzeigen

```
cluster1::~*> system node autosupport invoke -node * -type all
               -message MAINT=END
```

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

```
set -privilege admin
```

Wie geht es weiter?

Nachdem Sie Ihre SSH-Konfiguration überprüft haben, können Sie ["Konfigurieren der Switch-Integritätsüberwachung"](#) Die

Schalter austauschen

Ersetzen Sie einen Cisco Nexus 92300YC-Switch

Der Austausch eines defekten Nexus 92300YC-Switches in einem Clusternetzwerk ist ein nicht-unterbrechendes Verfahren (NDU).

Überprüfungsanforderungen

Bevor Sie beginnen

Vor dem Austausch des Schalters stellen Sie bitte Folgendes sicher:

- In der bestehenden Cluster- und Netzwerkinfrastruktur:
 - Der bestehende Cluster wurde als voll funktionsfähig verifiziert, wobei mindestens ein Cluster-Switch vollständig angeschlossen ist.
 - Alle Cluster-Ports sind aktiv.
 - Alle logischen Schnittstellen (LIFs) des Clusters sind aktiv und an ihren jeweiligen Ports angeschlossen.
 - Der Befehl `ONTAP cluster ping-cluster -node node1` muss anzeigen, dass die grundlegende Konnektivität und die Kommunikation größer als PMTU auf allen Pfaden erfolgreich sind.
- Für den Ersatzschalter Nexus 92300YC:
 - Die Management-Netzwerkanbindung des Ersatz-Switches ist funktionsfähig.
 - Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
 - Die Knotenverbindungen sind die Ports 1/1 bis 1/64.
 - Alle Inter-Switch Link (ISL)-Ports sind an den Ports 1/65 und 1/66 deaktiviert.
 - Die gewünschte Referenzkonfigurationsdatei (RCF) und das NX-OS-Betriebssystem-Image werden auf den Switch geladen.
 - Die erste Anpassung des Schalters ist abgeschlossen, wie in der folgenden Beschreibung detailliert aufgeführt: ["Konfigurieren Sie den Cisco Nexus 92300YC-Switch"](#) Die

Alle zuvor vorgenommenen Anpassungen am Standort, wie z. B. STP, SNMP und SSH, werden auf den neuen Switch kopiert.

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.

Zu den Beispielen

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

- Die Namen der vorhandenen Nexus 92300YC Switches lauten cs1 und cs2.
- Der neue Switch Nexus 92300YC trägt den Namen newcs2.
- Die Knotennamen lauten Knoten1 und Knoten2.
- Die Cluster-Ports auf jedem Knoten tragen die Namen e0a und e0b.
- Die Cluster-LIF-Namen lauten node1_clus1 und node1_clus2 für Knoten 1 sowie node2_clus1 und node2_clus2 für Knoten 2.
- Die Aufforderung zum Ändern aller Clusterknoten lautet cluster1::*>

Informationen zu diesem Vorgang

Sie müssen den Befehl zur Migration eines Cluster-LIF von dem Knoten ausführen, auf dem der Cluster-LIF gehostet wird.

Das folgende Verfahren basiert auf der folgenden Cluster-Netzwerktopologie:

Topologie anzeigen

```
cluster1::*> 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.

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

Cluster					
	node1_clus1	up/up	169.254.209.69/16	node1	e0a
true					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b

```

true
node2_clus1 up/up 169.254.47.194/16 node2 e0a
true
node2_clus2 up/up 169.254.19.183/16 node2 e0b
true
4 entries were displayed.

```

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

Node/	Local	Discovered			
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform	
node2	/cdp				
	e0a	cs1	Eth1/2	N9K-	
C92300YC					
	e0b	cs2	Eth1/2	N9K-	
C92300YC					
node1	/cdp				
	e0a	cs1	Eth1/1	N9K-	
C92300YC					
	e0b	cs2	Eth1/1	N9K-	
C92300YC					

4 entries were displayed.

```
cs1# 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					
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2 (FD0220329V5)	Eth1/65	176	R S I s	N9K-C92300YC	
Eth1/65					
cs2 (FD0220329V5)	Eth1/66	176	R S I s	N9K-C92300YC	
Eth1/66					

Total entries displayed: 4

```
cs2# 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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1 (FDO220329KU)	Eth1/65	178	R S I s	N9K-C92300YC	
Eth1/65					
cs1 (FDO220329KU)	Eth1/66	178	R S I s	N9K-C92300YC	
Eth1/66					

Total entries displayed: 4

Schritt 1: Vorbereitung auf den Austausch

1. Installieren Sie die entsprechende RCF-Datei und das Image auf dem Switch newcs2 und treffen Sie alle notwendigen Vorbereitungen vor Ort.

Prüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und NX-OS-Software für den neuen Switch. Wenn Sie überprüft haben, dass der neue Switch korrekt eingerichtet ist und keine Aktualisierungen der RCF- und NX-OS-Software erforderlich sind, fahren Sie mit Schritt 2 fort.

- a. Gehen Sie auf der NetApp Support-Website zur Seite „NetApp Cluster and Management Network Switches Reference Configuration File Description Page“.
 - b. Klicken Sie auf den Link zur *Kompatibilitätsmatrix für Cluster- und Managementnetzwerke* und notieren Sie sich anschließend die erforderliche Switch-Softwareversion.
 - c. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur **Beschreibungsseite** zurückzukehren, klicken Sie auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und gehen Sie dann zur **Download**-Seite.
 - d. Folgen Sie den Anweisungen auf der Downloadseite, um die korrekten RCF- und NX-OS-Dateien für die Version der ONTAP -Software herunterzuladen, die Sie installieren.
2. Melden Sie sich auf dem neuen Switch als Administrator an und fahren Sie alle Ports herunter, die mit den Knotenclusterschnittstellen verbunden werden (Ports 1/1 bis 1/64).

Wenn der zu ersetzende Schalter nicht funktionsfähig und ausgeschaltet ist, fahren Sie mit Schritt 4 fort. Die LIFs auf den Clusterknoten sollten bereits für jeden Knoten auf den anderen Clusterport umgeschaltet haben.

Beispiel anzeigen

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

3. Überprüfen Sie, ob für alle Cluster-LIFs die automatische Rücksetzung aktiviert ist:

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

Beispiel anzeigen

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

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
Cluster	node1_clus2	true
Cluster	node2_clus1	true
Cluster	node2_clus2	true

```
4 entries were displayed.
```

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)

```

Schritt 2: Kabel und Anschlüsse konfigurieren

1. Schalten Sie die ISL-Ports 1/65 und 1/66 am Switch Nexus 92300YC cs1 ab:

Beispiel anzeigen

```

cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/65-66
cs1(config-if-range)# shutdown
cs1(config-if-range)#

```

2. Entfernen Sie alle Kabel vom Nexus 92300YC cs2-Switch und schließen Sie sie dann an dieselben Ports am Nexus 92300YC newcs2-Switch an.
3. Aktivieren Sie die ISL-Ports 1/65 und 1/66 zwischen den Switches cs1 und newcs2 und überprüfen Sie dann den Betriebsstatus des Portkanals.

Port-Channel sollte Po1(SU) und Member Ports sollten Eth1/65(P) und Eth1/66(P) anzeigen.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/65 und 1/66 und zeigt die Port-Kanal-Zusammenfassung auf Switch cs1 an:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
cs1(config-if-range)# no shutdown

cs1(config-if-range)# 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      Eth1/65 (P)  Eth1/66 (P)

cs1(config-if-range)#
```

4. Überprüfen Sie, ob Port e0b auf allen Knoten aktiv ist:

```
network port show ipspace Cluster
```

Beispiel anzeigen

Die Ausgabe sollte in etwa wie folgt aussehen:

```
cluster1::*> 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/auto -
false						

4 entries were displayed.

5. Auf demselben Knoten, den Sie im vorherigen Schritt verwendet haben, stellen Sie die Cluster-LIF, die dem Port im vorherigen Schritt zugeordnet ist, mit dem Befehl `network interface revert` wieder her.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert Home true ist und der Port e0b lautet.

Die folgenden Befehle geben LIF zurück. node1_clus2 An node1 zum Heimathafen e0a und zeigt Informationen über die LIFs auf beiden Knoten an. Das Hochfahren des ersten Knotens ist erfolgreich, wenn die Spalte „Is Home“ für beide Cluster-Schnittstellen den Wert „true“ aufweist und die korrekten Portzuweisungen angezeigt werden. e0a Und e0b auf Knoten1.

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
	node2_clus1	up/up	169.254.47.194/16	node2
e0a	true			
	node2_clus2	up/up	169.254.19.183/16	node2
e0a	false			

4 entries were displayed.

6. Informationen über die Knoten in einem Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Knotenstatus für Knoten 1 und Knoten 2 in diesem Cluster „true“ ist:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	false	true
node2	true	true

7. Überprüfen Sie, ob alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

Beispiel anzeigen

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

Node: node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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.

Schritt 3: Schließen Sie den Vorgang ab.

1. 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. Bestätigen Sie die folgende Cluster-Netzwerkconfiguration:

```
network port show
```

Beispiel anzeigen

```
cluster1::*> 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.
```

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	-----			
Cluster				
	node1_clus1	up/up	169.254.209.69/16	node1
e0a	true			
	node1_clus2	up/up	169.254.49.125/16	node1

```
e0b      true
          node2_clus1  up/up    169.254.47.194/16  node2
e0a      true
          node2_clus2  up/up    169.254.19.183/16  node2
e0b      true
```

4 entries were displayed.

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	0/2	N9K-
C92300YC				
	e0b	newcs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C92300YC				
	e0b	newcs2	0/1	N9K-
C92300YC				

4 entries were displayed.

```
cs1# 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1	Eth1/1	144	H	FAS2980
e0a				
node2	Eth1/2	145	H	FAS2980
e0a				
newcs2 (FDO296348FU)	Eth1/65	176	R S I s	N9K-C92300YC
Eth1/65				
newcs2 (FDO296348FU)	Eth1/66	176	R S I s	N9K-C92300YC

Eth1/66

Total entries displayed: 4

cs2# **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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 (FDO220329KU) Eth1/65	Eth1/65	178	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	178	R S I s	N9K-C92300YC

Total entries displayed: 4

Wie geht es weiter?

Nachdem Sie Ihre SSH-Konfiguration überprüft haben, können Sie ["Konfigurieren der Switch-Integritätsüberwachung"](#)Die

Ersetzen Sie Cisco Nexus 92300YC Cluster-Switches durch switchlose Verbindungen.

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

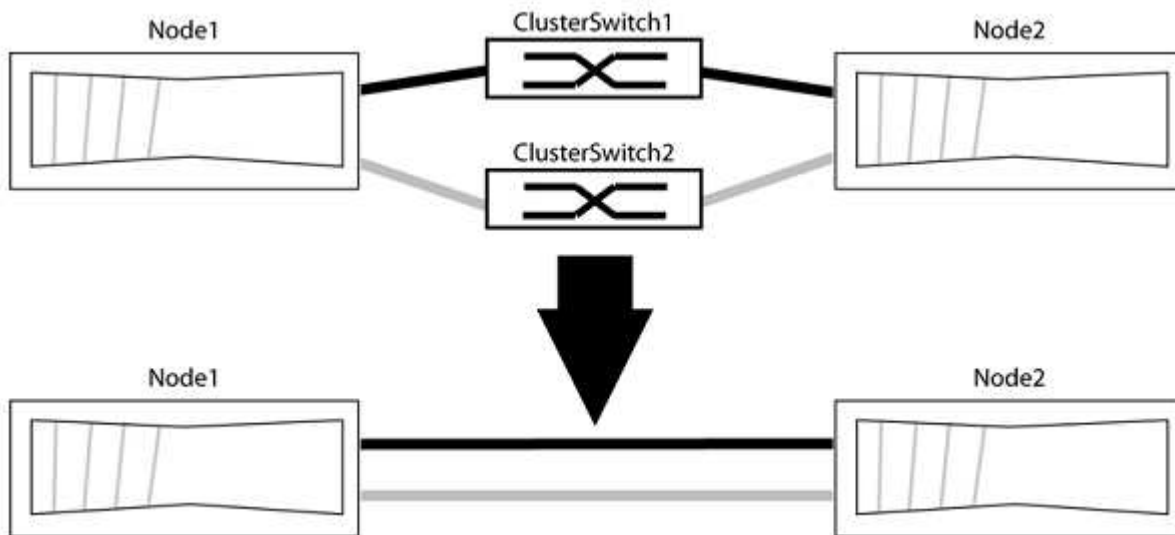
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- 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

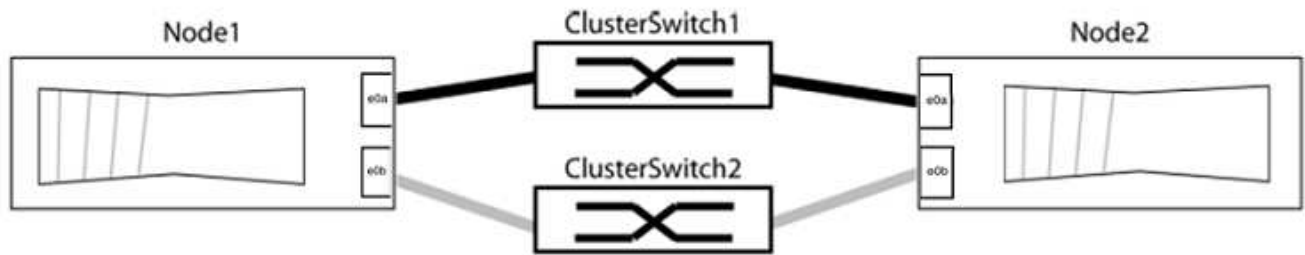
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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.

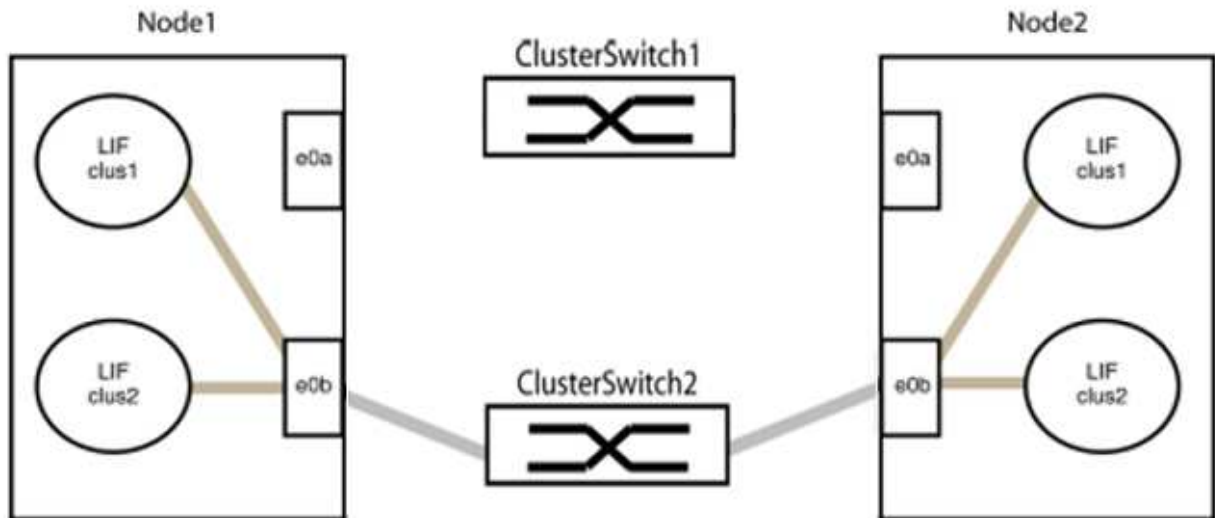
2. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 1 ein.



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**.

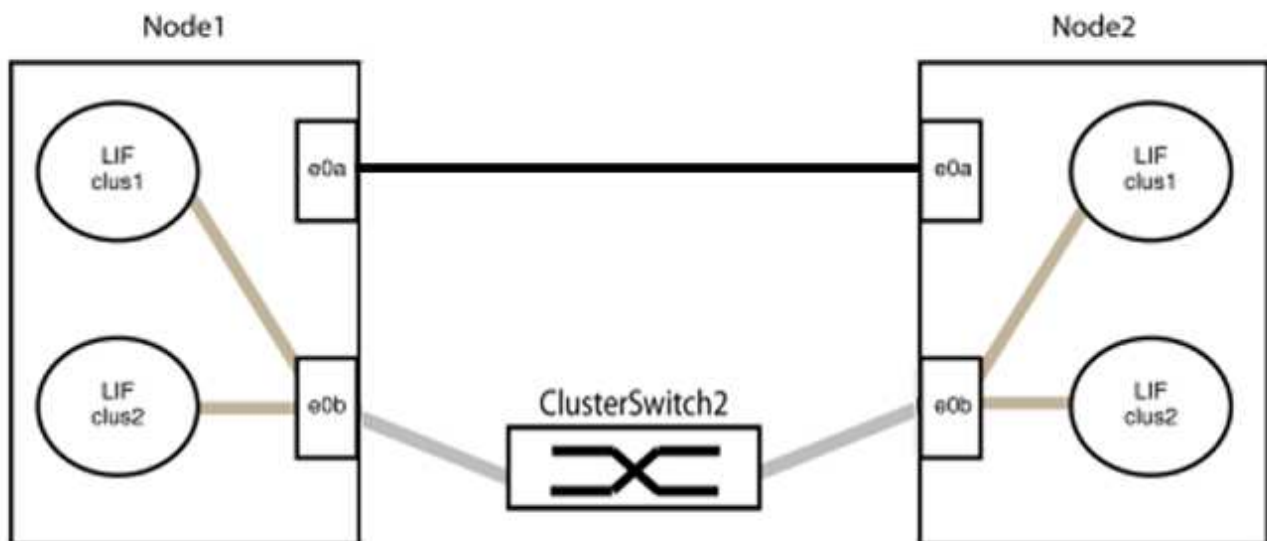
- a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

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.

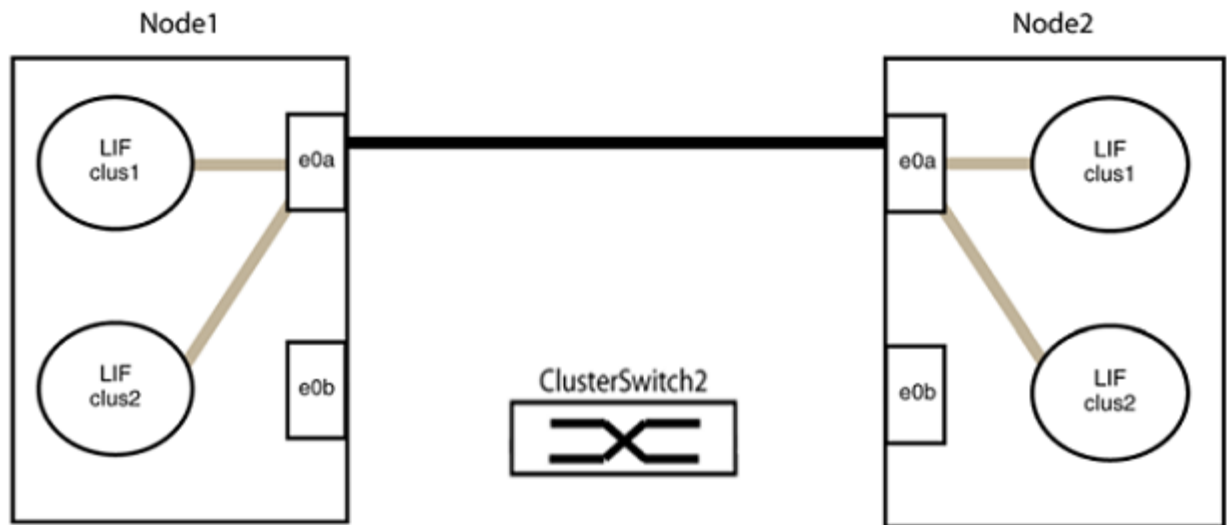
1. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 2 ein.



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
```

NetApp CN1610

Übersicht über Installation und Konfiguration von NetApp CN1610-Switches

Der CN1610 ist ein Managed Layer 2 Switch mit hoher Bandbreite, der 16 10-Gigabit Small Form-Factor Pluggable Plus (SFP+) Ports bietet.

Der Switch verfügt über redundante Netzteile und Lüftereinschübe, die Hot-Swapping für hohe Verfügbarkeit unterstützen. Dieser 1U-Switch kann in einem Standard-19-Zoll NetApp 42U-Systemschrank oder in einem

Schrank eines Drittanbieters installiert werden.

Der Switch unterstützt die lokale Verwaltung über den Konsolenanschluss oder die Fernverwaltung mittels Telnet oder SSH über eine Netzwerkverbindung. Der CN1610 verfügt über einen dedizierten 1-Gigabit-Ethernet-RJ45-Management-Port für die Out-of-Band-Switch-Verwaltung. Sie können den Switch verwalten, indem Sie Befehle in die Befehlszeilenschnittstelle (CLI) eingeben oder ein SNMP-basiertes Netzwerkmanagementsystem (NMS) verwenden.

Workflow für NetApp CN1610-Switches installieren und konfigurieren

Um einen NetApp CN1610 Switch auf Systemen mit ONTAP zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

1. ["Installieren der Hardware"](#)
2. ["Installieren Sie die FASTPATH-Software"](#)
3. ["Installationsreferenzkonfigurationsdatei"](#)

Wenn auf den Switches ONTAP 8.3.1 oder höher ausgeführt wird, befolgen Sie die Anweisungen in ["Installieren Sie FASTPATH und RCFs auf Switches, auf denen ONTAP 8.3.1 und höher ausgeführt wird."](#)

4. ["Schalter konfigurieren"](#)

Dokumentationsanforderungen für NetApp CN1610-Switches

Für die Installation und Wartung des NetApp CN1610 Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation durchlesen.

Dokumenttitel	Beschreibung
"1G-Installationsanleitung"	Ein Überblick über die Hardware- und Softwarefunktionen des CN1601-Switches sowie den Installationsprozess.
"10G Installationsanleitung"	Ein Überblick über die Hardware- und Softwarefunktionen des CN1610-Switches sowie eine Beschreibung der Funktionen zur Installation des Switches und zum Zugriff auf die CLI.
"Einrichtungs- und Konfigurationsleitfaden für die Switches CN1601 und CN1610"	Detaillierte Informationen zur Konfiguration der Switch-Hardware und -Software für Ihre Clusterumgebung.
CN1601 Switch-Administratorhandbuch	Liefert Beispiele für die Verwendung des CN1601-Switches in einem typischen Netzwerk. • "Administratorhandbuch" • "Administratorhandbuch, Version 1.1.xx" • "Administratorhandbuch, Version 1.2.xx"

Dokumenttitel	Beschreibung
CN1610 Netzwerk-Switch CLI-Befehlsreferenz	Bietet detaillierte Informationen zu den Befehlszeilenschnittstellenbefehlen (CLI), die Sie zur Konfiguration der CN1601-Software verwenden. • "Befehlsreferenz" • "Befehlsreferenz, Version 1.1.xx" • "Befehlsreferenz, Version 1.2.xx"

Installieren und konfigurieren

Installieren Sie die Hardware für den NetApp CN1610-Switch

Um die NetApp CN1610 Switch-Hardware zu installieren, folgen Sie den Anweisungen in einem der folgenden Handbücher.

- ["1G-Installationsanleitung"](#).

Ein Überblick über die Hardware- und Softwarefunktionen des CN1601-Switches sowie den Installationsprozess.

- ["10G Installationsanleitung"](#)

Ein Überblick über die Hardware- und Softwarefunktionen des CN1610-Switches sowie eine Beschreibung der Funktionen zur Installation des Switches und zum Zugriff auf die CLI.

Installieren Sie die FASTPATH-Software

Wenn Sie die FASTPATH-Software auf Ihren NetApp -Switches installieren, müssen Sie das Upgrade mit dem zweiten Switch, cs2, beginnen.

Überprüfungsanforderungen

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 und keine defekten Cluster-Netzwerkschnittstellenkarten (NICs) oder ähnliche Probleme).
- Voll funktionsfähige Portverbindungen am Cluster-Switch.
- Alle Cluster-Ports eingerichtet.
- Alle logischen Schnittstellen (LIFs) des Clusters müssen eingerichtet sein (dürfen nicht migriert worden sein).
- Ein erfolgreicher Kommunikationsweg: ONTAP (Privileg: fortgeschritten) `cluster ping-cluster -node node1` Der Befehl muss angeben, dass `larger than PMTU communication` ist auf allen Wegen erfolgreich.
- Eine unterstützte Version von FASTPATH und ONTAP.

Bitte konsultieren Sie die Tabelle zur Schalterkompatibilität auf der Website. "[NetApp CN1601 und CN1610 Switches](#)" Seite für die unterstützten FASTPATH- und ONTAP Versionen.

Installieren Sie FASTPATH

Das folgende Verfahren verwendet die Clustered Data ONTAP 8.2 Syntax. Daher unterscheiden sich der Cluster-Vserver, die LIF-Namen und die CLI-Ausgabe von denen in Data ONTAP 8.3.

Zwischen der Befehlssyntax in den RCF- und FASTPATH-Versionen können Befehlsabhängigkeiten bestehen.

Zu den Beispielen

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

- Die beiden NetApp Switches sind cs1 und cs2.
- Die beiden Cluster-LIFs sind clus1 und clus2.
- Die Vserver sind vs1 und vs2.
- Der `cluster::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Knoten tragen die Namen e1a und e2a.

"[Hardware Universe](#)" enthält weitere Informationen zu den tatsächlichen Cluster-Ports, die auf Ihrer Plattform unterstützt werden.

- Die unterstützten Inter-Switch-Links (ISLs) sind die Ports 0/13 bis 0/16.
- Die unterstützten Knotenverbindungen sind die Ports 0/1 bis 0/12.

Schritt 1: Cluster migrieren

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. Melden Sie sich als Administrator am Switch an. Es gibt standardmäßig kein Passwort. Am (cs2) # Eingabeaufforderung, geben Sie die `enable` Befehl. Auch hier gilt: Standardmäßig ist kein Passwort erforderlich. Dies ermöglicht Ihnen den Zugriff auf den privilegierten EXEC-Modus, mit dem Sie die Netzwerkschnittstelle konfigurieren können.

Beispiel anzeigen

```
(cs2) # enable
Password (Enter)
(cs2) #
```

3. Auf der Konsole jedes Knotens migrieren Sie clus2 auf Port e1a:

```
network interface migrate
```

Beispiel anzeigen

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-destnode node1 -dest-port e1a
cluster::*> network interface migrate -vserver vs2 -lif clus2
-destnode node2 -dest-port e1a
```

4. Überprüfen Sie auf der Konsole jedes Knotens, ob die Migration durchgeführt wurde:

```
network interface show
```

Das folgende Beispiel zeigt, dass clus2 auf beiden Knoten auf Port e1a migriert wurde:

Beispiel anzeigen

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

Vserver	Logical Interface	Status Admin/Open	Network Address/Mask	Current Node	Current Port	Is Home
vs1						
	clus1	up/up	10.10.10.1/16	node1	e1a	true
	clus2	up/up	10.10.10.2/16	node1	e1a	
false						
vs2						
	clus1	up/up	10.10.10.1/16	node2	e1a	true
	clus2	up/up	10.10.10.2/16	node2	e1a	
false						

Schritt 2: Installieren Sie die FASTPATH-Software

1. Schalten Sie den Cluster-Port e2a auf beiden Knoten ab:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie Port e2a auf beiden Knoten abgeschaltet wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin  
false  
cluster::*> network port modify -node node2 -port e2a -up-admin  
false
```

2. Überprüfen Sie, ob Port e2a auf beiden Knoten deaktiviert ist:

```
network port show
```

Beispiel anzeigen

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

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
-----	----	-----	----	-----	-----	-----	
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

3. Schalten Sie die Inter-Switch Link (ISL)-Ports am aktiven NetApp Switch cs1 ab:

Beispiel anzeigen

```
(cs1) # configure  
(cs1)(config) # interface 0/13-0/16  
(cs1)(Interface 0/13-0/16) # shutdown  
(cs1)(Interface 0/13-0/16) # exit  
(cs1)(config) # exit
```

4. Sichern Sie das aktuell aktive Image auf cs2.

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions      .

  active:
  backup:

Images currently available on Flash

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

      1          1.1.0.3      1.1.0.1          1.1.0.3          1.1.0.3

(cs2) # copy active backup
Copying active to backup
Copy operation successful

(cs2) #
```

5. Laden Sie die Image-Datei auf den Switch herunter.

Durch das Kopieren der Image-Datei in das aktive Image wird beim Neustart die laufende FASTPATH-Version aus diesem Image erstellt. Das vorherige Image bleibt als Backup verfügbar.

Beispiel anzeigen

```
(cs2) # copy tftp://10.0.0.1/NetApp_CN1610_1.1.0.5.stk active

Mode..... TFTP
Set Server IP..... 10.0.0.1
Path..... ./
Filename..... NetApp_CN1610_1.1.0.5.stk
Data Type..... Code
Destination Filename..... active

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

File transfer operation completed successfully.
```

6. Überprüfen Sie die laufende Version der FASTPATH-Software.

```
show version
```

Beispiel anzeigen

```
(cs2) # show version

Switch: 1

System Description..... Broadcom Scorpion 56820
                           Development System - 16 TENGIG,
                           1.1.0.3, Linux 2.6.21.7
Machine Type.....        Broadcom Scorpion 56820
                           Development System - 16TENGIG
Machine Model.....        BCM-56820
Serial Number.....        10611100004
FRU Number.....
Part Number.....          BCM56820
Maintenance Level.....    A
Manufacturer.....          0xbc00
Burned In MAC Address..... 00:A0:98:4B:A9:AA
Software Version.....      1.1.0.3
Operating System.....      Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Additional Packages.....    FASTPATH QOS
                           FASTPATH IPv6 Management
```

7. Sehen Sie sich die Startabbilder für die aktive und die Sicherungskonfiguration an.

```
show bootvar
```

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions

  active :
  backup :

  Images currently available on Flash

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

      1          1.1.0.3      1.1.0.3          1.1.0.3          1.1.0.5
```

8. Starten Sie den Switch neu.

reload

Beispiel anzeigen

```
(cs2) # reload

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

System will now restart!
```

Schritt 3: Installation überprüfen

1. Melden Sie sich erneut an und überprüfen Sie die neue Version der FASTPATH-Software.

show version

Beispiel anzeigen

```
(cs2) # show version

Switch: 1

System Description..... Broadcom Scorpion 56820
                          Development System - 16
TENGIG,
                          1.1.0.5, Linux 2.6.21.7
Machine Type.....      Broadcom Scorpion 56820
                          Development System - 16TENGIG
Machine Model.....      BCM-56820
Serial Number.....      10611100004
FRU Number.....
Part Number.....        BCM56820
Maintenance Level.....   A
Manufacturer.....        0xbc00
Burned In MAC Address..... 00:A0:98:4B:A9:AA
Software Version.....    1.1.0.5
Operating System.....    Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Additional Packages.....  FASTPATH QOS
                          FASTPATH IPv6 Management
```

2. Schalten Sie die ISL-Ports auf cs1, dem aktiven Switch, ein.

```
configure
```

Beispiel anzeigen

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # no shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

3. Überprüfen Sie, ob die ISLs betriebsbereit sind:

```
show port-channel 3/1
```

Das Feld „Verbindungsstatus“ sollte Folgendes anzeigen: Up Die

Beispiel anzeigen

```
(cs2) # show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports   Timeout      Speed     Active
-----
0/13    actor/long      10G Full  True
        partner/long
0/14    actor/long      10G Full  True
        partner/long
0/15    actor/long      10G Full  True
        partner/long
0/16    actor/long      10G Full  True
        partner/long
```

4. Kopiere die running-config Datei an die startup-config Die Datei wird erst geladen, wenn Sie mit den Softwareversionen und Schaltereinstellungen zufrieden sind.

Beispiel anzeigen

```
(cs2) # write memory

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

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

Config file 'startup-config' created successfully .

Configuration Saved!
```

5. Aktivieren Sie den zweiten Cluster-Port, e2a, auf jedem Knoten:

```
network port modify
```

Beispiel anzeigen

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> **network port modify -node node2 -port e2a -up-admin
true**
```

6. Rückgängig machen von clus2, das mit Port e2a verknüpft ist:

```
network interface revert
```

Die LIF-Einstellungen können sich je nach Version Ihrer ONTAP -Software automatisch zurücksetzen.

Beispiel anzeigen

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

7. Überprüfen Sie, ob sich das LIF jetzt im Startbereich befindet.(true) auf beiden Knoten:

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

Beispiel anzeigen

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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	----
vs1						
	clus1	up/up	10.10.10.1/24	node1	e1a	true
	clus2	up/up	10.10.10.2/24	node1	e2a	true
vs2						
	clus1	up/up	10.10.10.1/24	node2	e1a	true
	clus2	up/up	10.10.10.2/24	node2	e2a	true

8. Den Status der Knoten anzeigen:

```
cluster show
```

Beispiel anzeigen

```
cluster::> cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

9. Wiederholen Sie die vorherigen Schritte, um die FASTPATH-Software auf dem anderen Switch, cs1, zu installieren.
10. Wenn Sie die automatische Fehlerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Installieren einer Referenzkonfigurationsdatei auf einem CN1610-Switch

Gehen Sie wie folgt vor, um eine Referenzkonfigurationsdatei (RCF) zu installieren.

Vor der Installation eines RCF müssen Sie zuerst die Cluster-LIFs vom Switch cs2 migrieren. Nach der Installation und Validierung des RCF können die LIFs zurückmigriert werden.

Überprüfungsanforderungen

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 und keine defekten Cluster-Netzwerkschnittstellenkarten (NICs) oder ähnliche Probleme).
- Voll funktionsfähige Portverbindungen am Cluster-Switch.
- Alle Cluster-Ports eingerichtet.
- Alle logischen Schnittstellen (LIFs) des Clusters wurden eingerichtet.
- Ein erfolgreicher Kommunikationsweg: ONTAP (Privileg: fortgeschritten) `cluster ping-cluster -node node1` Der Befehl muss angeben, dass larger than PMTU communication ist auf allen Wegen erfolgreich.
- Eine unterstützte Version von RCF und ONTAP.

Bitte konsultieren Sie die Tabelle zur Schalterkompatibilität auf der Website. ["NetApp CN1601 und CN1610 Switches"](#) Seite für die unterstützten RCF- und ONTAP Versionen.

Installieren Sie den RCF

Das folgende Verfahren verwendet die Clustered Data ONTAP 8.2 Syntax. Daher unterscheiden sich der Cluster-Vserver, die LIF-Namen und die CLI-Ausgabe von denen in Data ONTAP 8.3.

Zwischen der Befehlssyntax in den RCF- und FASTPATH-Versionen können Befehlsabhängigkeiten bestehen.



In RCF Version 1.2 wurde die Unterstützung für Telnet aus Sicherheitsgründen explizit deaktiviert. Um Verbindungsprobleme während der Installation von RCF 1.2 zu vermeiden, vergewissern Sie sich, dass Secure Shell (SSH) aktiviert ist. Der ["NetApp CN1610 Switch – Administratorhandbuch"](#) enthält weitere Informationen zu SSH.

Zu den Beispielen

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

- Die beiden NetApp Switches sind cs1 und cs2.
- Die beiden Cluster-LIFs sind clus1 und clus2.
- Die Vserver sind vs1 und vs2.
- Der `cluster::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Knoten tragen die Namen e1a und e2a.

["Hardware Universe"](#) enthält weitere Informationen zu den tatsächlichen Cluster-Ports, die auf Ihrer Plattform unterstützt werden.

- Die unterstützten Inter-Switch-Links (ISLs) sind die Ports 0/13 bis 0/16.
- Die unterstützten Knotenverbindungen sind die Ports 0/1 bis 0/12.
- Eine unterstützte Version von FASTPATH, RCF und ONTAP.

Bitte konsultieren Sie die Tabelle zur Schalterkompatibilität auf der Website. ["NetApp CN1601 und CN1610 Switches"](#) Seite für die unterstützten FASTPATH-, RCF- und ONTAP Versionen.

Schritt 1: Cluster migrieren

1. Speichern Sie Ihre aktuellen Switch-Konfigurationsinformationen:

```
write memory
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die aktuelle Switch-Konfiguration in der Startkonfiguration gespeichert wird.(`startup-config`) Datei auf Switch CS2:

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!
```

2. Auf der Konsole jedes Knotens migrieren Sie clus2 auf Port e1a:

```
network interface migrate
```

Beispiel anzeigen

```
cluster:*> network interface migrate -vserver vs1 -lif clus2
-source-node node1 -destnode node1 -dest-port e1a

cluster:*> network interface migrate -vserver vs2 -lif clus2
-source-node node2 -destnode node2 -dest-port e1a
```

3. Überprüfen Sie auf der Konsole jedes Knotens, ob die Migration stattgefunden hat:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass clus2 auf beiden Knoten auf Port e1a migriert wurde:

```
cluster:*> network port show -role cluster
      clus1      up/up      10.10.10.1/16      node2      e1a      true
      clus2      up/up      10.10.10.2/16      node2      e1a
false
```

4. Schalten Sie Port e2a auf beiden Knoten ab:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie Port e2a auf beiden Knoten abgeschaltet wird:

```
cluster:*> network port modify -node node1 -port e2a -up-admin
false
cluster:*> network port modify -node node2 -port e2a -up-admin
false
```

5. Überprüfen Sie, ob Port e2a auf beiden Knoten deaktiviert ist:

```
network port show
```

Beispiel anzeigen

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

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
-----	-----	-----	----	-----	-----	-----	-----
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

6. Schalten Sie die ISL-Ports am aktiven NetApp Switch cs1 ab.

Beispiel anzeigen

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (interface 0/13-0/16) # shutdown
(cs1) (interface 0/13-0/16) # exit
(cs1) (config) # exit
```

Schritt 2: RCF installieren

1. Kopieren Sie die RCF-Datei auf den Switch.



Sie müssen die `.scr` Dateinamenserweiterung muss vor dem Aufruf des Skripts Teil des Dateinamens sein. Diese Erweiterung ist für das FASTPATH-Betriebssystem.

Der Switch validiert das Skript automatisch beim Herunterladen auf den Switch, und die Ausgabe wird in der Konsole angezeigt.

Beispiel anzeigen

```
(cs2) # copy tftp://10.10.0.1/CN1610_CS_RCF_v1.1.txt nvram:script
CN1610_CS_RCF_v1.1.scr

[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```

2. Überprüfen Sie, ob das Skript heruntergeladen und unter dem von Ihnen angegebenen Dateinamen gespeichert wurde.

Beispiel anzeigen

```
(cs2) # script list
Configuration Script Name          Size(Bytes)
-----
running-config.scr                6960
CN1610_CS_RCF_v1.1.scr            2199

2 configuration script(s) found.
6038 Kbytes free.
```

3. Überprüfen Sie das Skript.



Das Skript wird während des Downloads validiert, um sicherzustellen, dass jede Zeile eine gültige Switch-Befehlszeile ist.

Beispiel anzeigen

```
(cs2) # script validate CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script 'CN1610_CS_RCF_v1.1.scr' validated.
```

4. Wende das Skript auf den Schalter an.

Beispiel anzeigen

```
(cs2) #script apply CN1610_CS_RCF_v1.1.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.1.scr' applied.
```

5. Überprüfen Sie, ob Ihre Änderungen auf dem Switch implementiert wurden.

```
(cs2) # show running-config
```

Das Beispiel zeigt die `running-config` Datei auf dem Switch. Sie müssen die Datei mit der RCF-Datei vergleichen, um zu überprüfen, ob die von Ihnen festgelegten Parameter Ihren Erwartungen entsprechen.

6. Speichern Sie die Änderungen.
7. Stellen Sie die `running-config` Die Datei soll die Standarddatei sein.

Beispiel anzeigen

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.
```

8. Starten Sie den Switch neu und überprüfen Sie, ob der `running-config` Die Datei ist korrekt.

Nach Abschluss des Neustarts müssen Sie sich anmelden und die `running-config` Datei und suchen Sie dann nach der Beschreibung auf Schnittstelle 3/64, das ist die Versionsbezeichnung für die RCF.

Beispiel anzeigen

```
(cs2) # reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

9. Schalten Sie die ISL-Ports auf cs1, dem aktiven Switch, ein.

Beispiel anzeigen

```
(cs1) # configure
(cs1) (config)# interface 0/13-0/16
(cs1) (Interface 0/13-0/16)# no shutdown
(cs1) (Interface 0/13-0/16)# exit
(cs1) (config)# exit
```

10. Überprüfen Sie, ob die ISLs betriebsbereit sind:

```
show port-channel 3/1
```

Das Feld „Verbindungsstatus“ sollte Folgendes anzeigen: Up Die

Beispiel anzeigen

```
(cs2) # show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/13     actor/long      10G Full   True
         partner/long
0/14     actor/long      10G Full   True
         partner/long
0/15     actor/long      10G Full   True
         partner/long
0/16     actor/long      10G Full   True
         partner/long
```

11. Aktivieren Sie den Cluster-Port e2a auf beiden Knoten:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie Port e2a auf Knoten 1 und Knoten 2 aktiviert wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

Schritt 3: Installation überprüfen

1. Überprüfen Sie, ob Port e2a auf beiden Knoten aktiv ist:

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

Beispiel anzeigen

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

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
-----	----	-----	----	----	-----	-----	-----
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	up	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	up	9000	true/true	full/full	auto/10000

2. Auf beiden Knoten muss der mit Port e2a verknüpfte clus2-Befehl zurückgesetzt werden:

```
network interface revert
```

Die LIF-Einstellungen werden möglicherweise automatisch zurückgesetzt, abhängig von Ihrer ONTAP-Version.

Beispiel anzeigen

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

3. Überprüfen Sie, ob sich das LIF jetzt im Startbereich befindet.(true) auf beiden Knoten:

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

Beispiel anzeigen

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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home

vs1	clus1	up/up	10.10.10.1/24	node1	e1a	true
	clus2	up/up	10.10.10.2/24	node1	e2a	true
vs2	clus1	up/up	10.10.10.1/24	node2	e1a	true
	clus2	up/up	10.10.10.2/24	node2	e2a	true

4. Den Status der Knotenmitglieder anzeigen:

```
cluster show
```

Beispiel anzeigen

```
cluster::> cluster show
```

Node	Health	Eligibility

node1	true	true
node2	true	true

5. Kopiere die running-config Datei an die startup-config Die Datei wird erst geladen, wenn Sie mit den Softwareversionen und Schaltereinstellungen zufrieden sind.

Beispiel anzeigen

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!
```

6. Wiederholen Sie die vorherigen Schritte, um den RCF auf dem anderen Switch, cs1, zu installieren.

Wie geht es weiter?

["Switch-Zustandsüberwachung konfigurieren"](#)

Installieren Sie die FASTPATH-Software und die RCFs für ONTAP 8.3.1 und höher.

Folgen Sie diesem Verfahren, um die FASTPATH-Software und RCFs für ONTAP 8.3.1 und höher zu installieren.

Die Installationsschritte sind für NetApp CN1601 Management-Switches und CN1610 Cluster-Switches mit ONTAP 8.3.1 oder höher identisch. Allerdings benötigen die beiden Modelle unterschiedliche Software und RCFs.

Überprüfungsanforderungen

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 und keine defekten Cluster-Netzwerkschnittstellenkarten (NICs) oder ähnliche Probleme).
- Voll funktionsfähige Portverbindungen am Cluster-Switch.
- Alle Cluster-Ports eingerichtet.
- Alle logischen Schnittstellen (LIFs) des Clusters müssen eingerichtet sein (dürfen nicht migriert worden sein).
- Ein erfolgreicher Kommunikationsweg: ONTAP (Privileg: fortgeschritten) `cluster ping-cluster -node node1` Der Befehl muss angeben, dass `larger than PMTU communication` ist auf allen Wegen erfolgreich.
- Eine unterstützte Version von FASTPATH, RCF und ONTAP.

Bitte konsultieren Sie die Tabelle zur Schalterkompatibilität auf der Website. ["NetApp CN1601 und CN1610 Switches"](#) Seite für die unterstützten FASTPATH-, RCF- und ONTAP Versionen.

Installieren Sie die FASTPATH-Software

Das folgende Verfahren verwendet die Clustered Data ONTAP 8.2 Syntax. Daher unterscheiden sich der Cluster-Vserver, die LIF-Namen und die CLI-Ausgabe von denen in Data ONTAP 8.3.

Zwischen der Befehlssyntax in den RCF- und FASTPATH-Versionen können Befehlsabhängigkeiten bestehen.



In RCF Version 1.2 wurde die Unterstützung für Telnet aus Sicherheitsgründen explizit deaktiviert. Um Verbindungsprobleme während der Installation von RCF 1.2 zu vermeiden, vergewissern Sie sich, dass Secure Shell (SSH) aktiviert ist. Der ["NetApp CN1610 Switch – Administratorhandbuch"](#) enthält weitere Informationen zu SSH.

Zu den Beispielen

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

- Die beiden NetApp Switches tragen die Namen cs1 und cs2.
- Die Namen der logischen Clusterschnittstellen (LIF) lauten node1_clus1 und node1_clus2 für Knoten 1 sowie node2_clus1 und node2_clus2 für Knoten 2. (Ein Cluster kann bis zu 24 Knoten enthalten.)
- Der Name der Storage Virtual Machine (SVM) lautet Cluster.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Knoten tragen die Namen e0a und e0b.

["Hardware Universe"](#) enthält weitere Informationen zu den tatsächlichen Cluster-Ports, die auf Ihrer Plattform unterstützt werden.

- Die unterstützten Inter-Switch-Links (ISLs) sind die Ports 0/13 bis 0/16.
- Die unterstützten Knotenverbindungen sind die Ports 0/1 bis 0/12.

Schritt 1: Cluster migrieren

1. Informationen zu den Netzwerkports des Clusters anzeigen:

```
network port show -ipspace cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt die Art der Ausgabe des Befehls:

```
cluster1::> network port show -ipspace cluster
```

					Speed
(Mbps)					
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					

node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
4 entries were displayed.					

2. Informationen zu den LIFs im Cluster anzeigen:

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

Beispiel anzeigen

Das folgende Beispiel zeigt die logischen Schnittstellen des Clusters. In diesem Beispiel `-role` Der Parameter zeigt Informationen über die LIFs an, die den Cluster-Ports zugeordnet sind:

```
cluster1::> network interface show -role cluster
(network interface show)

      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e0a      node1_clus1  up/up      10.254.66.82/16    node1
      true
e0b      node1_clus2  up/up      10.254.206.128/16  node1
      true
e0a      node2_clus1  up/up      10.254.48.152/16   node2
      true
e0b      node2_clus2  up/up      10.254.42.74/16    node2
      true
4 entries were displayed.
```

3. Auf jedem der jeweiligen Knoten migrieren Sie mithilfe eines Knotenverwaltungs-LIF `node1_clus2` auf `node1` nach `e0a` und `node2_clus2` auf `node2` nach `e0a`:

```
network interface migrate
```

Sie müssen die Befehle auf den Controller-Konsolen eingeben, denen die jeweiligen Cluster-LIFs gehören.

Beispiel anzeigen

```
cluster1::> network interface migrate -vserver Cluster -lif
node1_clus2 -destination-node node1 -destination-port e0a
cluster1::> network interface migrate -vserver Cluster -lif
node2_clus2 -destination-node node2 -destination-port e0a
```



Bei diesem Befehl ist die Groß-/Kleinschreibung des Clusternamens zu beachten, und der Befehl muss auf jedem Knoten ausgeführt werden. Dieser Befehl kann im allgemeinen Cluster-LIF nicht ausgeführt werden.

4. Überprüfen Sie mithilfe des `network interface show` Befehl auf einem Knoten.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass clus2 auf den Knoten node1 und node2 auf Port e0a migriert wurde:

```
cluster1::> **network interface show -role cluster**
          Logical      Status      Network      Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
          node1_clus1  up/up      10.254.66.82/16   node1
e0a       true
          node1_clus2  up/up      10.254.206.128/16 node1
e0a       false
          node2_clus1  up/up      10.254.48.152/16  node2
e0a       true
          node2_clus2  up/up      10.254.42.74/16  node2
e0a       false
4 entries were displayed.
```

5. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie bei Aufforderung „y“ eingeben:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

6. Schalten Sie den Cluster-Port e0b auf beiden Knoten ab:

```
network port modify -node node_name -port port_name -up-admin false
```

Sie müssen die Befehle auf den Controller-Konsolen eingeben, denen die jeweiligen Cluster-LIFs gehören.

Beispiel anzeigen

Das folgende Beispiel zeigt die Befehle zum Herunterfahren des Ports e0b auf allen Knoten:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
false
cluster1::*> network port modify -node node2 -port e0b -up-admin
false
```

7. Überprüfen Sie, ob Port e0b auf beiden Knoten deaktiviert ist:

network port show

Beispiel anzeigen

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

					Speed
(Mbps)					
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----	-----	-----	-----	-----	-----
node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	down	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	down	9000
auto/10000					
4 entries were displayed.					

8. Schalten Sie die Inter-Switch Link (ISL)-Ports auf cs1 ab.

Beispiel anzeigen

```
(cs1) #configure
(cs1) (Config)#interface 0/13-0/16
(cs1) (Interface 0/13-0/16)#shutdown
(cs1) (Interface 0/13-0/16)#exit
(cs1) (Config)#exit
```

9. Sichern Sie das aktuell aktive Image auf cs2.

Beispiel anzeigen

```
(cs2) # show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active

1	1.1.0.5	1.1.0.3	1.1.0.5	1.1.0.5

```
(cs2) # copy active backup
```

Copying active to backup

Copy operation successful

Schritt 2: Installieren Sie die FASTPATH-Software und RCF.

1. Überprüfen Sie die laufende Version der FASTPATH-Software.

Beispiel anzeigen

```
(cs2) # show version

Switch: 1

System Description..... NetApp CN1610,
1.1.0.5, Linux
                               2.6.21.7
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 20211200106
Burned In MAC Address..... 00:A0:98:21:83:69
Software Version..... 1.1.0.5
Operating System..... Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Part Number..... 111-00893

--More-- or (q)uit

Additional Packages..... FASTPATH QOS
                               FASTPATH IPv6
Management
```

2. Laden Sie die Image-Datei auf den Switch herunter.

Durch das Kopieren der Image-Datei in das aktive Image wird beim Neustart die laufende FASTPATH-Version aus diesem Image erstellt. Das vorherige Image bleibt als Backup verfügbar.

Beispiel anzeigen

```
(cs2) #copy
sftp://root@10.22.201.50//tftpboot/NetApp_CN1610_1.2.0.7.stk active
Remote Password:*****

Mode..... SFTP
Set Server IP..... 10.22.201.50
Path..... /tftpboot/
Filename.....
NetApp_CN1610_1.2.0.7.stk
Data Type..... Code
Destination Filename..... active

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

File transfer operation completed successfully.
```

3. Bestätigen Sie die aktuelle und die nächste aktive Boot-Image-Version:

```
show bootvar
```

Beispiel anzeigen

```
(cs2) #show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash

-----
unit      active      backup      current-active      next-active
-----
1         1.1.0.8      1.1.0.8      1.1.0.8             1.2.0.7
```

4. Installieren Sie die kompatible RCF-Datei für die neue Image-Version auf dem Switch.

Wenn die RCF-Version bereits korrekt ist, aktivieren Sie die ISL-Ports.

Beispiel anzeigen

```
(cs2) #copy tftp://10.22.201.50//CN1610_CS_RCF_v1.2.txt nvram:script
CN1610_CS_RCF_v1.2.scr

Mode..... TFTP
Set Server IP..... 10.22.201.50
Path..... /
Filename.....
CN1610_CS_RCF_v1.2.txt
Data Type..... Config Script
Destination Filename.....
CN1610_CS_RCF_v1.2.scr

File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

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

Validating configuration script...
[the script is now displayed line by line]

Configuration script validated.
File transfer operation completed successfully.
```



Der .scr Die Dateinamenserweiterung muss vor dem Aufruf des Skripts festgelegt werden. Diese Erweiterung ist für das FASTPATH-Betriebssystem.

Der Switch validiert das Skript automatisch, sobald es auf den Switch heruntergeladen wird. Die Ausgabe erfolgt in der Konsole.

5. Überprüfen Sie, ob das Skript heruntergeladen und unter dem von Ihnen angegebenen Dateinamen gespeichert wurde.

Beispiel anzeigen

```
(cs2) #script list

Configuration Script Name          Size(Bytes)
-----
CN1610_CS_RCF_v1.2.scr            2191

1 configuration script(s) found.
2541 Kbytes free.
```

6. Wende das Skript auf den Schalter an.

Beispiel anzeigen

```
(cs2) #script apply CN1610_CS_RCF_v1.2.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.2.scr' applied.
```

7. Überprüfen Sie, ob die Änderungen am Switch übernommen wurden, und speichern Sie sie anschließend:

```
show running-config
```

Beispiel anzeigen

```
(cs2) #show running-config
```

8. Speichern Sie die laufende Konfiguration, damit sie beim Neustart des Switches als Startkonfiguration verwendet wird.

Beispiel anzeigen

```
(cs2) #write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!
```

9. Starten Sie den Switch neu.

Beispiel anzeigen

```
(cs2) #reload

The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.
Configuration Saved!
System will now restart!
```

Schritt 3: Installation überprüfen

1. Melden Sie sich erneut an und überprüfen Sie dann, ob auf dem Switch die neue Version der FASTPATH-Software ausgeführt wird.

Beispiel anzeigen

```
(cs2) #show version

Switch: 1

System Description..... NetApp CN1610,
1.2.0.7,Linux
                               3.8.13-4ce360e8
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 20211200106
Burned In MAC Address..... 00:A0:98:21:83:69
Software Version..... 1.2.0.7
Operating System..... Linux 3.8.13-
4ce360e8
Network Processing Device..... BCM56820_B0
Part Number..... 111-00893
CPLD version..... 0x5

Additional Packages..... FASTPATH QOS
                          FASTPATH IPv6
Management
```

Nach Abschluss des Neustarts müssen Sie sich anmelden, um die Image-Version zu überprüfen, die laufende Konfiguration anzuzeigen und nach der Beschreibung auf der Schnittstelle 3/64 zu suchen. Dies ist die Versionsbezeichnung für die RCF.

2. Schalten Sie die ISL-Ports auf cs1, dem aktiven Switch, ein.

Beispiel anzeigen

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #no shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

3. Überprüfen Sie, ob die ISLs betriebsbereit sind:

```
show port-channel 3/1
```

Das Feld „Verbindungsstatus“ sollte Folgendes anzeigen: Up Die

Beispiel anzeigen

```
(cs1) #show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/13     actor/long      10G Full   True
         partner/long
0/14     actor/long      10G Full   True
         partner/long
0/15     actor/long      10G Full   False
         partner/long
0/16     actor/long      10G Full   True
         partner/long
```

4. Aktivieren Sie den Cluster-Port e0b auf allen Knoten:

```
network port modify
```

Sie müssen die Befehle auf den Controller-Konsolen eingeben, denen die jeweiligen Cluster-LIFs gehören.

Beispiel anzeigen

Das folgende Beispiel zeigt, wie Port e0b auf Knoten 1 und Knoten 2 aktiviert wird:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
true
cluster1::*> network port modify -node node2 -port e0b -up-admin
true
```

5. Überprüfen Sie, ob Port e0b auf allen Knoten aktiv ist:

```
network port show -ip space cluster
```

Beispiel anzeigen

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

(Mbps)					Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					

node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					

4 entries were displayed.

6. Überprüfen Sie, ob sich das LIF jetzt im Startbereich befindet.(true) auf beiden Knoten:

```
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				
	node1_clus1	up/up	169.254.66.82/16	node1
e0a	true			
	node1_clus2	up/up	169.254.206.128/16	node1
e0b	true			
	node2_clus1	up/up	169.254.48.152/16	node2
e0a	true			
	node2_clus2	up/up	169.254.42.74/16	node2
e0b	true			
4 entries were displayed.				

7. Den Status der Knotenmitglieder anzeigen:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false
2 entries were displayed.			

8. Zurück zur Administratorrechtebene:

```
set -privilege admin
```

9. Wiederholen Sie die vorherigen Schritte, um die FASTPATH-Software und RCF auf dem anderen Switch, cs1, zu installieren.

Konfigurieren Sie die Hardware für den NetApp CN1610-Switch

Informationen zur Konfiguration der Switch-Hardware und -Software für Ihre Clusterumgebung finden Sie in der entsprechenden Dokumentation. ["Einrichtungs- und Konfigurationsleitfaden für die Switches CN1601 und CN1610"](#) Die

Schalter migrieren

Migration von einer switchlosen Clusterumgebung zu einer switchierten NetApp CN1610 Clusterumgebung

Wenn Sie bereits eine switchlose Clusterumgebung mit zwei Knoten besitzen, können Sie mithilfe von CN1610 Cluster-Netzwerk-Switches zu einer switchierten Clusterumgebung mit zwei Knoten migrieren, die Ihnen eine Skalierung über zwei Knoten hinaus ermöglicht.

Überprüfungsanforderungen

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

Bei einer schalterlosen Konfiguration mit zwei Knoten ist Folgendes sicherzustellen:

- Die Zwei-Knoten-Konfiguration ohne Schalter ist ordnungsgemäß eingerichtet und funktioniert.
- Auf den Knoten läuft ONTAP 8.2 oder höher.
- Alle Cluster-Ports befinden sich im `up` Zustand.
- Alle logischen Schnittstellen (LIFs) des Clusters befinden sich in der `up` in den jeweiligen Bundesstaaten und in ihren Heimathäfen.

Für die Konfiguration des CN1610-Cluster-Switches:

- Die CN1610 Cluster-Switch-Infrastruktur ist auf beiden Switches voll funktionsfähig.
- Beide Switches verfügen über eine Management-Netzwerkanbindung.
- Es besteht Konsolenzugriff auf die Cluster-Switches.
- CN1610-Knoten-zu-Knoten- und Schalter-zu-Schalter-Verbindungen verwenden Twinax- oder Glasfaserkabel.

Der ["Hardware Universe"](#) enthält weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel sind an die Ports 13 bis 16 beider CN1610-Switches angeschlossen.
- Die erste Anpassung beider CN1610-Schalter ist abgeschlossen.

Alle zuvor vorgenommenen Anpassungen am Standort, wie z. B. SMTP, SNMP und SSH, sollten auf die neuen Switches kopiert werden.

Ähnliche Informationen

- ["Hardware Universe"](#)
- ["NetApp CN1601 und CN1610"](#)

- ["Einrichtung und Konfiguration der Switches CN1601 und CN1610"](#)
- ["NetApp KB-Artikel 1010449: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster"](#)

Migrieren Sie die Schalter

Zu den Beispielen

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

- Die Namen der CN1610-Schalter lauten cs1 und cs2.
- Die Namen der LIFs lauten clus1 und clus2.
- Die Namen der Knoten lauten Knoten1 und Knoten2.
- Der `cluster::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e1a und e2a.

Der ["Hardware Universe"](#) Enthält die aktuellsten Informationen zu den tatsächlichen Cluster-Ports für Ihre Plattformen.

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 Eingabeaufforderung (`*>`) wird angezeigt.

2. 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.

Beispiel anzeigen

Der folgende Befehl unterdrückt die automatische Fallerstellung für zwei Stunden:

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

Schritt 2: Ports konfigurieren

1. Deaktivieren Sie alle zum Knoten hin ausgerichteten Ports (nicht die ISL-Ports) an den beiden neuen Cluster-Switches cs1 und cs2.

Die ISL-Ports dürfen nicht deaktiviert werden.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die dem Knoten zugewandten Ports 1 bis 12 am Switch cs1 deaktiviert sind:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

Das folgende Beispiel zeigt, dass die dem Knoten zugewandten Ports 1 bis 12 am Switch cs2 deaktiviert sind:

```
(c2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden CN1610 Cluster-Switches cs1 und cs2 verbunden sind. up :

```
show port-channel
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports up auf Switch CS1:

```
(cs1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr Ports	Device/ Timeout	Port Speed	Port Active
-----	-----	-----	-----
0/13	actor/long partner/long	10G Full	True
0/14	actor/long partner/long	10G Full	True
0/15	actor/long partner/long	10G Full	True
0/16	actor/long partner/long	10G Full	True

Das folgende Beispiel zeigt, dass die ISL-Ports up auf der Switch CS2:

```
(cs2)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr	Device/ Ports	Port Timeout	Port Speed	Port Active
-----	-----	-----	-----	-----
0/13	actor/long partner/long	10G Full	True	
0/14	actor/long partner/long	10G Full	True	
0/15	actor/long partner/long	10G Full	True	
0/16	actor/long partner/long	10G Full	True	

3. Liste der benachbarten Geräte anzeigen:

```
show isdp neighbors
```

Dieser Befehl liefert Informationen über die mit dem System verbundenen Geräte.

Beispiel anzeigen

Das folgende Beispiel listet die benachbarten Geräte am Switch cs1 auf:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
cs2                0/13          11        S           CN1610
0/13
cs2                0/14          11        S           CN1610
0/14
cs2                0/15          11        S           CN1610
0/15
cs2                0/16          11        S           CN1610
0/16
```

Das folgende Beispiel listet die benachbarten Geräte am Switch cs2 auf:

```
(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
cs1                0/13          11        S           CN1610
0/13
cs1                0/14          11        S           CN1610
0/14
cs1                0/15          11        S           CN1610
0/15
cs1                0/16          11        S           CN1610
0/16
```

4. Liste der Cluster-Ports anzeigen:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt die verfügbaren Cluster-Ports:

```
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						
e0c	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4b	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						
e0c	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

```
12 entries were displayed.
```

5. Überprüfen Sie, ob jeder Cluster-Port mit dem entsprechenden Port des zugehörigen Partner-Cluster-Knotens verbunden ist:

```
run * cdpd show-neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports e1a und e2a mit demselben Port auf ihrem Cluster-Partnerknoten verbunden sind:

```
cluster::*> run * cdpd show-neighbors
2 entries were acted on.
```

Node: node1

Local Remote	Remote	Remote	Remote	Hold
Port Device	Interface	Platform	Time	
Capability				

e1a	node2	e1a	FAS3270	137
H				
e2a	node2	e2a	FAS3270	137
H				

Node: node2

Local Remote	Remote	Remote	Remote	Hold
Port Device	Interface	Platform	Time	
Capability				

e1a	node1	e1a	FAS3270	161
H				
e2a	node1	e2a	FAS3270	161
H				

6. Überprüfen Sie, ob alle Cluster-LIFs vorhanden sind. up und betriebsbereit:

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

Jeder Cluster-LIF sollte Folgendes anzeigen true in der Spalte "Ist zu Hause".

Beispiel anzeigen

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
true	clus1	up/up	10.10.10.1/16	node1	e1a
true	clus2	up/up	10.10.10.2/16	node1	e2a
node2					
true	clus1	up/up	10.10.11.1/16	node2	e1a
true	clus2	up/up	10.10.11.2/16	node2	e2a

4 entries were displayed.



Die folgenden Änderungs- und Migrationsbefehle in den Schritten 10 bis 13 müssen vom lokalen Knoten aus ausgeführt werden.

7. Überprüfen Sie, ob alle Cluster-Ports up :

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

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

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							
-----	-----	-----	-----	-----	-----	-----	
node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

8. Stellen Sie die `-auto-revert` Parameter zu `false` auf den Cluster-LIFs `clus1` und `clus2` auf beiden Knoten:

```
network interface modify
```

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert false
```



Für Version 8.3 und höher verwenden Sie folgenden Befehl: `network interface modify -vserver Cluster -lif * -auto-revert 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 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. Migrieren Sie clus1 auf Port e2a auf der Konsole jedes Knotens:

```
network interface migrate
```

Beispiel anzeigen

Das folgende Beispiel zeigt den Prozess zur Migration von clus1 auf Port e2a auf Knoten 1 und Knoten 2:

```

cluster::*> network interface migrate -vserver node1 -lif clus1
-source-node node1 -dest-node node1 -dest-port e2a
cluster::*> network interface migrate -vserver node2 -lif clus1
-source-node node2 -dest-node node2 -dest-port e2a

```



Für Version 8.3 und höher verwenden Sie folgenden Befehl: `network interface migrate -vserver Cluster -lif clus1 -destination-node node1 -destination-port e2a`

2. Überprüfen Sie, ob die Migration stattgefunden hat:

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

Beispiel anzeigen

Das folgende Beispiel verifiziert, dass clus1 auf Knoten 1 und Knoten 2 auf Port e2a migriert wurde:

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
	clus1	up/up	10.10.10.1/16	node1	e2a
false					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2					
	clus1	up/up	10.10.11.1/16	node2	e2a
false					
	clus2	up/up	10.10.11.2/16	node2	e2a
true					

4 entries were displayed.

3. Schalten Sie den Cluster-Port e1a auf beiden Knoten ab:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e1a auf Knoten 1 und Knoten 2 deaktiviert wird:

```
cluster::*> network port modify -node node1 -port e1a -up-admin  
false  
cluster::*> network port modify -node node2 -port e1a -up-admin  
false
```

4. Überprüfen Sie den Portstatus:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e1a ist down auf Knoten 1 und Knoten 2:

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

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	down	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	down	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

5. Trennen Sie das Kabel vom Cluster-Port e1a auf Knoten 1 und verbinden Sie dann e1a mit Port 1 des Cluster-Switches cs1. Verwenden Sie dazu die von den CN1610-Switches unterstützten Kabel.

Der "[Hardware Universe](#)" enthält weitere Informationen zur Verkabelung.

6. Trennen Sie das Kabel vom Cluster-Port e1a auf Knoten 2 und verbinden Sie dann e1a mit Port 2 auf dem Cluster-Switch cs1. Verwenden Sie dazu die von den CN1610-Switches unterstützten geeigneten Kabel.
7. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1 bis 12 am Switch cs1 aktiviert sind:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# no shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

8. Aktivieren Sie den ersten Cluster-Port e1a auf jedem Knoten:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e1a auf Knoten 1 und Knoten 2 aktiviert wird:

```
cluster::*> network port modify -node node1 -port e1a -up-admin true
cluster::*> network port modify -node node2 -port e1a -up-admin true
```

9. Überprüfen Sie, ob alle Cluster-Ports aktiv sind. up :

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports up auf Knoten 1 und Knoten 2:

```
cluster::*> network port show -ipSPACE Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

10. clus1 (das zuvor migriert wurde) auf beiden Knoten wieder auf e1a zurücksetzen:

```
network interface revert
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie man clus1 auf Knoten 1 und Knoten 2 wieder auf Port e1a umstellt:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```



Für Version 8.3 und höher verwenden Sie folgenden Befehl: `network interface revert -vserver Cluster -lif <nodename_clus<N>>`

11. Überprüfen Sie, ob alle Cluster-LIFs vorhanden sind. up , betriebsbereit und Anzeige als true in der Spalte „Ist zu Hause“:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs up auf Knoten 1 und Knoten 2 und dass die Ergebnisse der Spalte "Ist zu Hause" true :

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2					
	clus1	up/up	10.10.11.1/16	node2	e1a
true					
	clus2	up/up	10.10.11.2/16	node2	e2a
true					

4 entries were displayed.

12. Informationen über den Status der Knoten im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster an:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         false
node2                true    true         false
```

13. Migrieren Sie clus2 auf Port e1a der Konsole jedes Knotens:

```
network interface migrate
```

Beispiel anzeigen

Das folgende Beispiel zeigt den Prozess zur Migration von clus2 auf Port e1a auf Knoten 1 und Knoten 2:

```
cluster::*> network interface migrate -vserver node1 -lif clus2
-source-node node1 -dest-node node1 -dest-port e1a
cluster::*> network interface migrate -vserver node2 -lif clus2
-source-node node2 -dest-node node2 -dest-port e1a
```



Für Version 8.3 und höher verwenden Sie folgenden Befehl: `network interface migrate -vserver Cluster -lif node1_clus2 -dest-node node1 -dest-port e1a`

14. Überprüfen Sie, ob die Migration stattgefunden hat:

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

Beispiel anzeigen

Das folgende Beispiel verifiziert, dass clus2 auf Knoten 1 und Knoten 2 auf Port e1a migriert wurde:

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
true	clus1	up/up	10.10.10.1/16	node1	e1a
false	clus2	up/up	10.10.10.2/16	node1	e1a
node2					
true	clus1	up/up	10.10.11.1/16	node2	e1a
false	clus2	up/up	10.10.11.2/16	node2	e1a

4 entries were displayed.

15. Schalten Sie den Cluster-Port e2a auf beiden Knoten ab:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e2a auf Knoten 1 und Knoten 2 deaktiviert wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin  
false  
cluster::*> network port modify -node node2 -port e2a -up-admin  
false
```

16. Überprüfen Sie den Portstatus:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e2a ist down auf Knoten 1 und Knoten 2:

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

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	down	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	down	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

17. Trennen Sie das Kabel vom Cluster-Port e2a auf Knoten 1 und verbinden Sie dann e2a mit Port 1 auf dem Cluster-Switch cs2. Verwenden Sie dazu die von den CN1610-Switches unterstützten Kabel.
18. Trennen Sie das Kabel vom Cluster-Port e2a auf Knoten 2 und verbinden Sie dann e2a mit Port 2 des Cluster-Switches cs2 unter Verwendung der von den CN1610-Switches unterstützten geeigneten Verkabelung.
19. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs2.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1 bis 12 am Switch cs2 aktiviert sind:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# no shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

20. Aktivieren Sie den zweiten Cluster-Port e2a auf jedem Knoten.

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e2a auf Knoten 1 und Knoten 2 aktiviert wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

21. Überprüfen Sie, ob alle Cluster-Ports aktiv sind. up :

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports up auf Knoten 1 und Knoten 2:

```
cluster::*> network port show -ipSPACE Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)	Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper
Admin/Oper							
-----	-----	-----	-----	-----	-----	-----	-----
node1							
		e1a	clus1	up	9000	true/true	full/full
auto/10000							
		e2a	clus2	up	9000	true/true	full/full
auto/10000							
node2							
		e1a	clus1	up	9000	true/true	full/full
auto/10000							
		e2a	clus2	up	9000	true/true	full/full
auto/10000							

4 entries were displayed.

22. clus2 (das zuvor migriert wurde) auf beiden Knoten wieder auf e2a zurücksetzen:

```
network interface revert
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie man clus2 auf Knoten 1 und Knoten 2 wieder auf den Port e2a umstellt:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```



Für Version 8.3 und höher lauten die Befehle: `cluster::*> network interface revert -vserver Cluster -lif node1_clus2` Und `cluster::*> network interface revert -vserver Cluster -lif node2_clus2`

Schritt 3: Konfiguration abschließen

1. Überprüfen Sie, ob alle Schnittstellen angezeigt werden. `true` in der Spalte „Ist zu Hause“:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs up auf Knoten 1 und Knoten 2 und dass die Ergebnisse der Spalte "Ist zu Hause" `true` :

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
node1				
	clus1	up/up	10.10.10.1/16	node1
e1a	true			
	clus2	up/up	10.10.10.2/16	node1
e2a	true			
node2				
	clus1	up/up	10.10.11.1/16	node2
e1a	true			
	clus2	up/up	10.10.11.2/16	node2
e2a	true			

2. 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 3]] Überprüfen Sie, ob beide Knoten über zwei Verbindungen zu jedem Switch verfügen:

```
show isdp neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
node1              0/1            132       H           FAS3270
e1a
node2              0/2            163       H           FAS3270
e1a
cs2                0/13           11        S           CN1610
0/13
cs2                0/14           11        S           CN1610
0/14
cs2                0/15           11        S           CN1610
0/15
cs2                0/16           11        S           CN1610
0/16

(cs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID          Intf          Holdtime  Capability  Platform
Port ID
-----
node1              0/1            132       H           FAS3270
e2a
node2              0/2            163       H           FAS3270
e2a
cs1                0/13           11        S           CN1610
0/13
cs1                0/14           11        S           CN1610
0/14
cs1                0/15           11        S           CN1610
0/15
cs1                0/16           11        S           CN1610
0/16
```

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device discovery show
```

3. Deaktivieren Sie die Einstellungen für die Zwei-Knoten-Switchless-Konfiguration auf beiden Knoten mithilfe des erweiterten Berechtigungsbefehls:

```
network options detect-switchless modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Einstellungen für die schalterlose Konfiguration deaktiviert werden:

```
cluster::*> network options detect-switchless modify -enabled false
```



Bei Version 9.2 und höher kann dieser Schritt übersprungen werden, da die Konfiguration automatisch konvertiert wird.

4. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

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

Beispiel anzeigen

Die Ausgabe im folgenden Beispiel zeigt, dass die Konfigurationseinstellungen deaktiviert sind:

```
cluster::*> network options detect-switchless-cluster show
Enable Switchless Cluster Detection: false
```



Für Version 9.2 und höher warten Sie bitte bis `Enable Switchless Cluster` ist auf „false“ gesetzt. Dies kann bis zu drei Minuten dauern.

5. Konfigurieren Sie die Cluster `clus1` und `clus2` so, dass sie auf jedem Knoten automatisch zurückgesetzt werden, und bestätigen Sie dies.

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert true
```



Für Version 8.3 und höher verwenden Sie folgenden Befehl: `network interface modify -vserver Cluster -lif * -auto-revert true` um die automatische Wiederherstellung auf allen Knoten im Cluster zu aktivieren.

6. Überprüfen Sie den Status der Knoten im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true   true         false
node2                true   true         false
```

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

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

Beispiel anzeigen

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

8. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

```
set -privilege admin
```

Schalter austauschen

Ersetzen Sie einen NetApp CN1610 Cluster-Switch

Befolgen Sie diese Schritte, um einen defekten NetApp CN1610 Switch in einem Clusternetzwerk auszutauschen. Dies ist ein nicht-unterbrechendes Verfahren (NDU).

Überprüfungsanforderungen

Bevor Sie beginnen

Bevor Sie den Switch austauschen, müssen die folgenden Bedingungen in der aktuellen Umgebung und am Ersatz-Switch für die bestehende Cluster- und Netzwerkinfrastruktur erfüllt sein:

- Der bestehende Cluster muss auf seine volle Funktionsfähigkeit überprüft werden, wobei mindestens ein Cluster-Switch vollständig angeschlossen sein muss.
- Alle Cluster-Ports müssen **aktiv** sein.
- Alle logischen Schnittstellen (LIFs) des Clusters müssen aktiv sein und dürfen nicht migriert worden sein.
- Der ONTAP Cluster `ping-cluster -node node1` Der Befehl muss anzeigen, dass die grundlegende Konnektivität und die Kommunikation über PMTU hinaus auf allen Pfaden erfolgreich sind.

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.

Informationen zu diesem Vorgang

Sie müssen den Befehl zur Migration eines Cluster-LIF von dem Knoten ausführen, auf dem der Cluster-LIF gehostet wird.

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

- Die Namen der beiden CN1610 Cluster-Switches lauten: `cs1` Und `cs2` Die
- Die Bezeichnung des zu ersetzenden CN1610-Schalters (des defekten Schalters) lautet: `old_cs1` Die
- Die Bezeichnung des neuen CN1610-Schalters (des Ersatzschalters) lautet: `new_cs1` Die
- Der Name des Partnerschalters, der nicht ausgetauscht wird, lautet: `cs2` Die

Schritte

1. Vergewissern Sie sich, dass die Startkonfigurationsdatei mit der laufenden Konfigurationsdatei

übereinstimmt. Sie müssen diese Dateien lokal speichern, um sie während des Austauschs verwenden zu können.

Die Konfigurationsbefehle im folgenden Beispiel gelten für FASTPATH 1.2.0.7:

Beispiel anzeigen

```
(old_cs1)> enable
(old_cs1)# show running-config
(old_cs1)# show startup-config
```

2. Erstellen Sie eine Kopie der laufenden Konfigurationsdatei.

Der Befehl im folgenden Beispiel gilt für FASTPATH 1.2.0.7:

Beispiel anzeigen

```
(old_cs1)# show running-config filename.scr
Config script created successfully.
```



Sie können jeden beliebigen Dateinamen verwenden, außer `CN1610_CS_RCF_v1.2.scr`. Der Dateiname muss die Dateiendung `.scr` haben.

1. Speichern Sie die laufende Konfigurationsdatei des Switches auf einem externen Host, um den Austausch vorzubereiten.

Beispiel anzeigen

```
(old_cs1)# copy nvram:script filename.scr
scp://<Username>@<remote_IP_address>/path_to_file/filename.scr
```

2. Prüfen Sie, ob die Versionen von Switch und ONTAP in der Kompatibilitätsmatrix übereinstimmen. Siehe die ["NetApp CN1601 und CN1610 Switches"](#). Weitere Details finden Sie auf der entsprechenden Seite.
3. vom ["Seite für Software-Downloads"](#) Auf der NetApp Support-Website können Sie unter „NetApp Cluster Switches“ die entsprechenden RCF- und FASTPATH-Versionen herunterladen.
4. Richten Sie einen Trivial File Transfer Protocol (TFTP)-Server mit FASTPATH, RCF und gespeicherter Konfiguration ein. `.scr` Datei zur Verwendung mit dem neuen Schalter.
5. Verbinden Sie den seriellen Port (den RJ-45-Anschluss mit der Bezeichnung „IOIOI“ auf der rechten Seite des Switches) mit einem verfügbaren Host mit Terminalemulation.
6. Auf dem Host die Einstellungen für die serielle Terminalverbindung vornehmen:
 - a. 9600 Baud

- b. 8 Datenbits
 - c. 1 Stoppbit
 - d. Parität: keine
 - e. Flusssteuerung: keine
7. Verbinden Sie den Management-Port (den RJ-45-Schraubenschlüssel-Anschluss auf der linken Seite des Switches) mit demselben Netzwerk, in dem sich Ihr TFTP-Server befindet.
8. Bereiten Sie die Verbindung zum Netzwerk mit dem TFTP-Server vor.

Wenn Sie das Dynamic Host Configuration Protocol (DHCP) verwenden, müssen Sie dem Switch zu diesem Zeitpunkt keine IP-Adresse konfigurieren. Der Service-Port ist standardmäßig auf DHCP eingestellt. Der Netzwerkmanagement-Port ist für die IPv4- und IPv6-Protokolleinstellungen auf „Keine“ gesetzt. Wenn Ihr Schraubenschlüsselanschluss mit einem Netzwerk verbunden ist, das über einen DHCP-Server verfügt, werden die Servereinstellungen automatisch konfiguriert.

Um eine statische IP-Adresse festzulegen, sollten Sie die Befehle `serviceport protocol`, `network protocol` und `serviceport ip` verwenden.

Beispiel anzeigen

```
(new_cs1) # serviceport ip <ipaddr> <netmask> <gateway>
```

9. Optionalerweise kann, falls sich der TFTP-Server auf einem Laptop befindet, der CN1610-Switch mit einem Standard-Ethernet-Kabel an den Laptop angeschlossen und anschließend sein Netzwerkport im selben Netzwerk mit einer alternativen IP-Adresse konfiguriert werden.

Sie können die `ping` Befehl zur Überprüfung der Adresse. Falls Sie keine Verbindung herstellen können, sollten Sie ein nicht geroutetes Netzwerk verwenden und den Service-Port mit der IP-Adresse 192.168.x oder 172.16.x konfigurieren. Sie können den Service-Port zu einem späteren Zeitpunkt auf die Produktionsmanagement-IP-Adresse umkonfigurieren.

10. Optional können Sie die entsprechenden Versionen der RCF- und FASTPATH-Software für den neuen Switch überprüfen und installieren. Wenn Sie überprüft haben, dass der neue Switch korrekt eingerichtet ist und keine Aktualisierungen der RCF- und FASTPATH-Software erforderlich sind, sollten Sie mit Schritt 13 fortfahren.
- a. Überprüfen Sie die neuen Schaltereinstellungen.

Beispiel anzeigen

```
(new_cs1) > enable  
(new_cs1) # show version
```

- b. Laden Sie die RCF-Datei auf den neuen Switch herunter.

Beispiel anzeigen

```
(new_cs1)# copy tftp://<server_ip_address>/CN1610_CS_RCF_v1.2.txt
nvram:script CN1610_CS_RCF_v1.2.scr
Mode.      TFTP
Set Server IP. 172.22.201.50
Path.      /
Filename.....
CN1610_CS_RCF_v1.2.txt
Data Type..... Config Script
Destination Filename.....
CN1610_CS_RCF_v1.2.scr
File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

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

File transfer in progress. Management access will be blocked for
the duration of the transfer. please wait...
Validating configuration script...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script validated.
File transfer operation completed successfully.
```

- c. Überprüfen Sie, ob die RCF-Datei auf den Switch heruntergeladen wurde.

Beispiel anzeigen

```
(new_cs1)# script list
Configuration Script Nam    Size(Bytes)
-----
CN1610_CS_RCF_v1.1.scr      2191
CN1610_CS_RCF_v1.2.scr      2240
latest_config.scr           2356

4 configuration script(s) found.
2039 Kbytes free.
```

11. Bringen Sie den RCF am Schalter CN1610 an.

Beispiel anzeigen

```
(new_cs1)# script apply CN1610_CS_RCF_v1.2.scr
Are you sure you want to apply the configuration script? (y/n) y
...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script 'CN1610_CS_RCF_v1.2.scr' applied. Note that the
script output will go to the console.
After the script is applied, those settings will be active in the
running-config file. To save them to the startup-config file, you
must use the write memory command, or if you used the reload answer
yes when asked if you want to save the changes.
```

- a. Speichern Sie die laufende Konfigurationsdatei, damit sie beim Neustart des Switches zur Startkonfigurationsdatei wird.

Beispiel anzeigen

```
(new_cs1)# write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!
```

- b. Laden Sie das Image auf den CN1610-Switch herunter.

Beispiel anzeigen

```
(new_cs1)# copy
tftp://<server_ip_address>/NetApp_CN1610_1.2.0.7.stk active
Mode.      TFTP
Set Server IP.  tftp_server_ip_address
Path.        /
Filename.....
NetApp_CN1610_1.2.0.7.stk
Data Type.   Code
Destination Filename.  active

Management access will be blocked for the duration of the
transfer

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

TFTP Code transfer starting...

File transfer operation completed successfully.
```

- c. Starten Sie den Switch neu, um das neue aktive Boot-Image zu laden.

Der Switch muss neu gestartet werden, damit der Befehl in Schritt 6 das neue Image widerspiegelt. Es gibt zwei mögliche Ansichten für eine Antwort, die Ihnen nach Eingabe des Befehls „reload“ angezeigt werden könnte.

Beispiel anzeigen

```
(new_cs1)# reload
The system has unsaved changes.
Would you like to save them now? (y/n) y

Config file 'startup-config' created successfully.

Configuration Saved! System will now restart!
.
.
.
Cluster Interconnect Infrastructure

User:admin Password: (new_cs1) >*enable*
```

- a. Kopieren Sie die gespeicherte Konfigurationsdatei vom alten Switch auf den neuen Switch.

Beispiel anzeigen

```
(new_cs1) # copy tftp://<server_ip_address>/<filename>.scr  
nvram:script <filename>.scr
```

- b. Wenden Sie die zuvor gespeicherte Konfiguration auf den neuen Switch an.

Beispiel anzeigen

```
(new_cs1) # script apply <filename>.scr  
Are you sure you want to apply the configuration script? (y/n) y  
  
The system has unsaved changes.  
Would you like to save them now? (y/n) y  
  
Config file 'startup-config' created successfully.  
  
Configuration Saved!
```

- c. Speichern Sie die laufende Konfigurationsdatei in der Startkonfigurationsdatei.

Beispiel anzeigen

```
(new_cs1) # write memory
```

12. 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.

13. Melden Sie sich auf dem neuen Switch new_cs1 als Administrator an und schalten Sie alle Ports ab, die mit den Schnittstellen des Knotenclusters verbunden sind (Ports 1 bis 12).

Beispiel anzeigen

```
User:*admin*
Password:
(new_cs1)> enable
(new_cs1)#
(new_cs1)# config
(new_cs1) (config)# interface 0/1-0/12
(new_cs1) (interface 0/1-0/12)# shutdown
(new_cs1) (interface 0/1-0/12)# exit
(new_cs1)# write memory
```

14. Migrieren Sie die Cluster-LIFs von den Ports, die mit dem Switch old_cs1 verbunden sind.

Sie müssen jeden Cluster-LIF von der Verwaltungsschnittstelle seines aktuellen Knotens migrieren.

Beispiel anzeigen

```
cluster::> set -privilege advanced
cluster::> network interface migrate -vserver <vserver_name> -lif
<Cluster_LIF_to_be_moved> - sourcenode <current_node> -dest-node
<current_node> -dest-port <cluster_port_that_is_UP>
```

15. Überprüfen Sie, ob alle Cluster-LIFs auf den entsprechenden Cluster-Port auf jedem Knoten verschoben wurden.

Beispiel anzeigen

```
cluster::> network interface show -role cluster
```

16. Schalten Sie die Cluster-Ports ab, die an den ausgetauschten Switch angeschlossen sind.

Beispiel anzeigen

```
cluster::*> network port modify -node <node_name> -port
<port_to_admin_down> -up-admin false
```

17. Überprüfen Sie den Zustand des Clusters.

Beispiel anzeigen

```
cluster::*> cluster show
```

18. Überprüfen Sie, ob die Ports deaktiviert sind.

Beispiel anzeigen

```
cluster::*> cluster ping-cluster -node <node_name>
```

19. Schalten Sie am Switch cs2 die ISL-Ports 13 bis 16 ab.

Beispiel anzeigen

```
(cs2)# config
(cs2)(config)# interface 0/13-0/16
(cs2)(interface 0/13-0/16)# shutdown
(cs2)# show port-channel 3/1
```

20. Prüfen Sie, ob der Speicheradministrator für den Austausch des Switches bereit ist.
21. Entfernen Sie alle Kabel vom alten Switch cs1 und schließen Sie die Kabel dann an die gleichen Ports am neuen Switch cs1 an.
22. Aktivieren Sie am Switch cs2 die ISL-Ports 13 bis 16.

Beispiel anzeigen

```
(cs2)# config
(cs2)(config)# interface 0/13-0/16
(cs2)(interface 0/13-0/16)# no shutdown
```

23. Schalten Sie die Ports des neuen Switches ein, die mit den Clusterknoten verbunden sind.

Beispiel anzeigen

```
(new_cs1)# config
(new_cs1)(config)# interface 0/1-0/12
(new_cs1)(interface 0/13-0/16)# no shutdown
```

24. Auf einem einzelnen Knoten wird der Clusterknotenport aktiviert, der mit dem ausgetauschten Switch verbunden ist. Anschließend wird überprüft, ob die Verbindung hergestellt wurde.

Beispiel anzeigen

```
cluster::*> network port modify -node node1 -port  
<port_to_be_onlined> -up-admin true  
cluster::*> network port show -role cluster
```

25. Setzen Sie die Cluster-LIFs, die dem Port in Schritt 25 auf demselben Knoten zugeordnet sind, zurück.

In diesem Beispiel werden die LIFs auf Knoten 1 erfolgreich zurückgesetzt, wenn die Spalte „Is Home“ den Wert „true“ hat.

Beispiel anzeigen

```
cluster::*> network interface revert -vserver node1 -lif  
<cluster_lif_to_be_reverted>  
cluster::*> network interface show -role cluster
```

26. Wenn der Cluster-LIF des ersten Knotens aktiv ist und auf seinen Heimatport zurückgesetzt wird, wiederholen Sie die Schritte 25 und 26, um die Cluster-Ports zu aktivieren und die Cluster-LIFs auf den anderen Knoten im Cluster zurückzusetzen.
27. Zeigt Informationen über die Knoten im Cluster an.

Beispiel anzeigen

```
cluster::*> cluster show
```

28. Prüfen Sie, ob die Startkonfigurationsdatei und die laufende Konfigurationsdatei auf dem ausgetauschten Switch korrekt sind. Diese Konfigurationsdatei sollte mit der Ausgabe in Schritt 1 übereinstimmen.

Beispiel anzeigen

```
(new_cs1)> enable  
(new_cs1)# show running-config  
(new_cs1)# show startup-config
```

29. 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
```

Ersetzen Sie NetApp CN1610 Cluster-Switches durch switchlose Verbindungen.

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

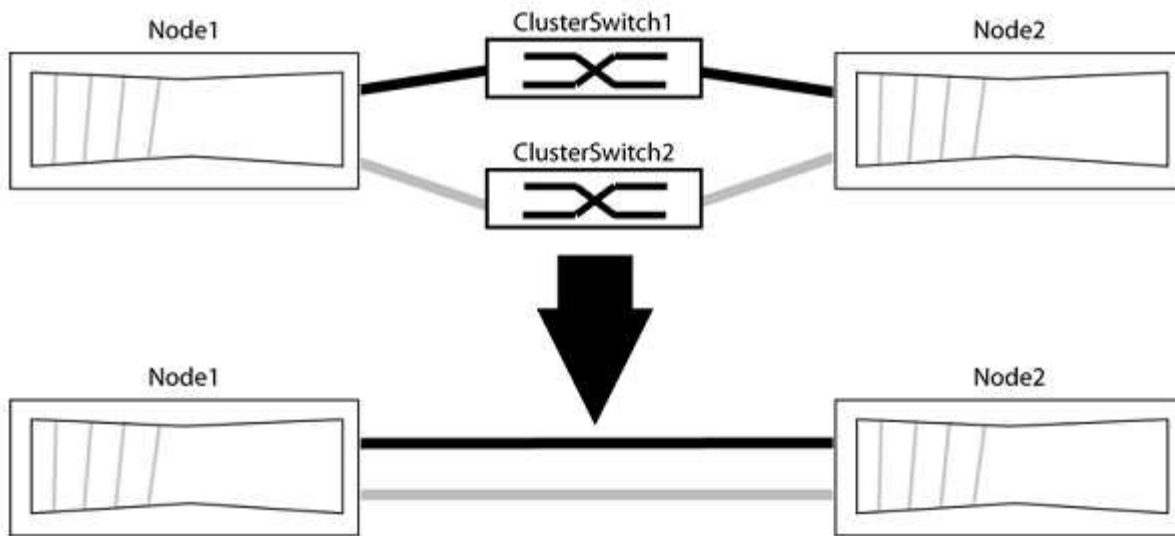
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- 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

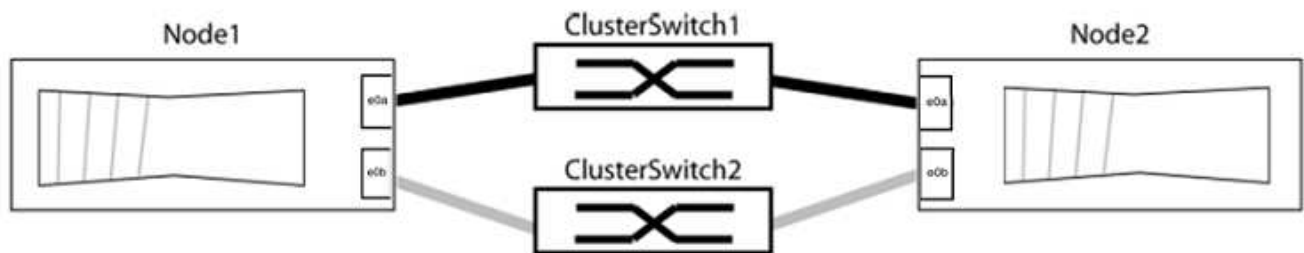
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

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
node2				
	3/5/2022 19:21:20 -06:00		node1_clus2	node2_clus2
node1				
	3/5/2022 19:21:18 -06:00		node2_clus2	node1_clus1
node2				
	3/5/2022 19:21:20 -06:00		node2_clus2	node1_clus2

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.

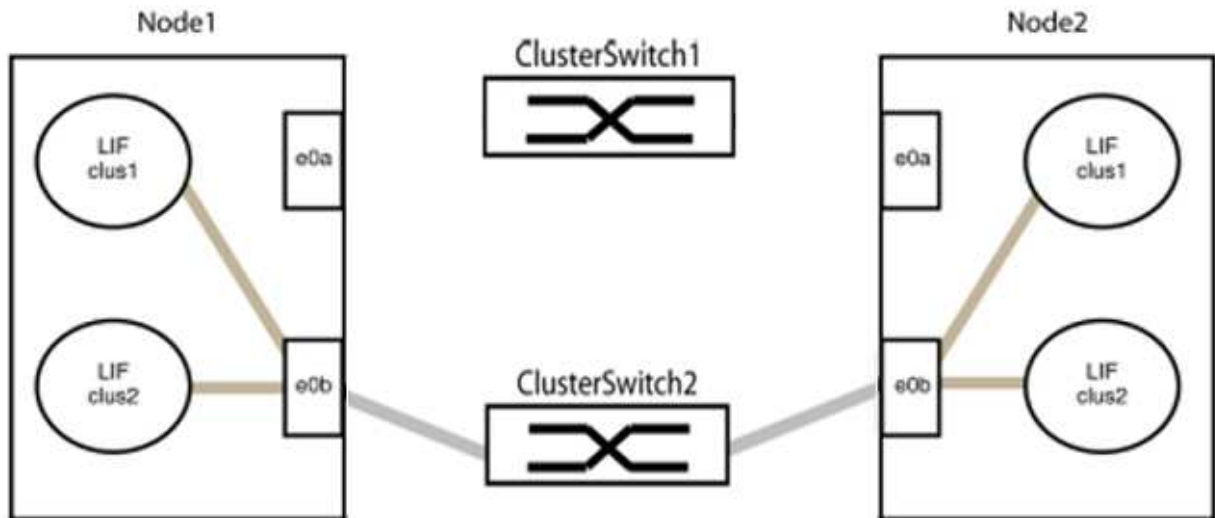
2. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 1 ein.



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**.

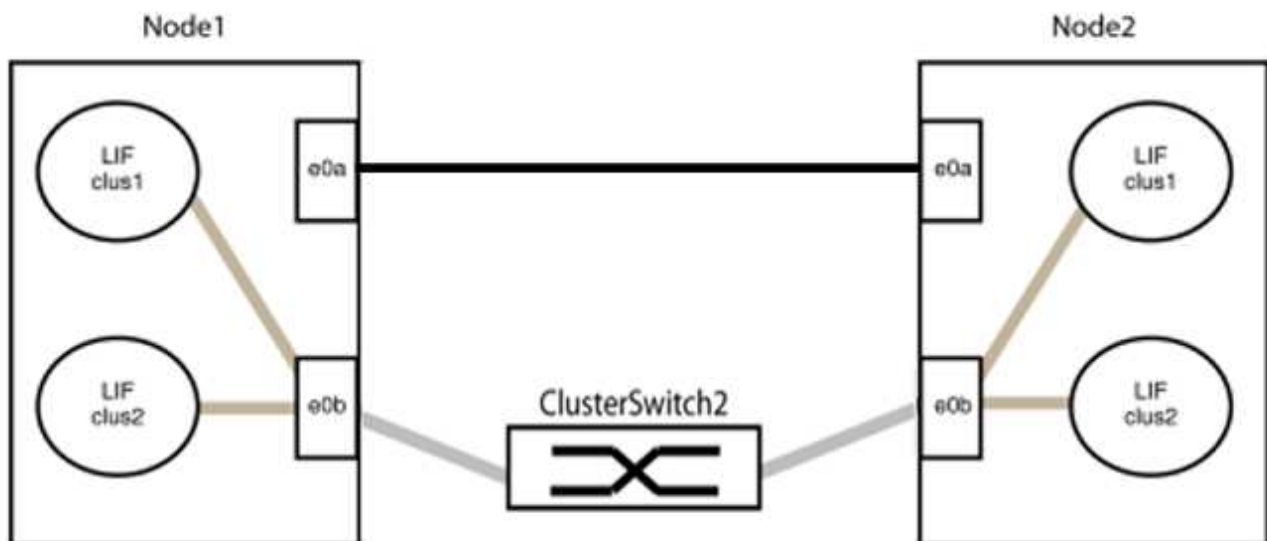
- a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

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.

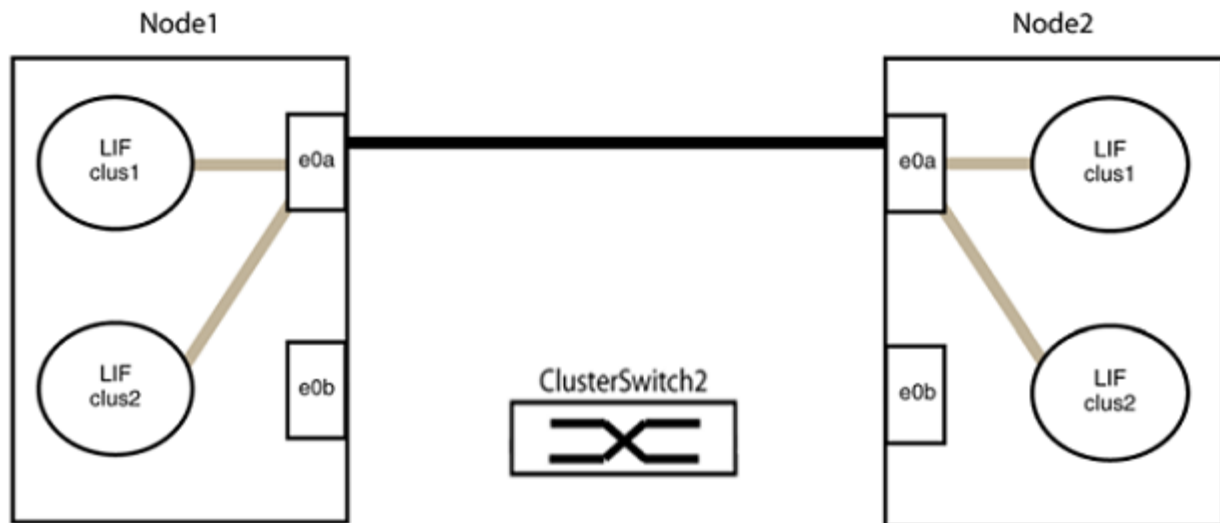
1. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 2 ein.



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**.

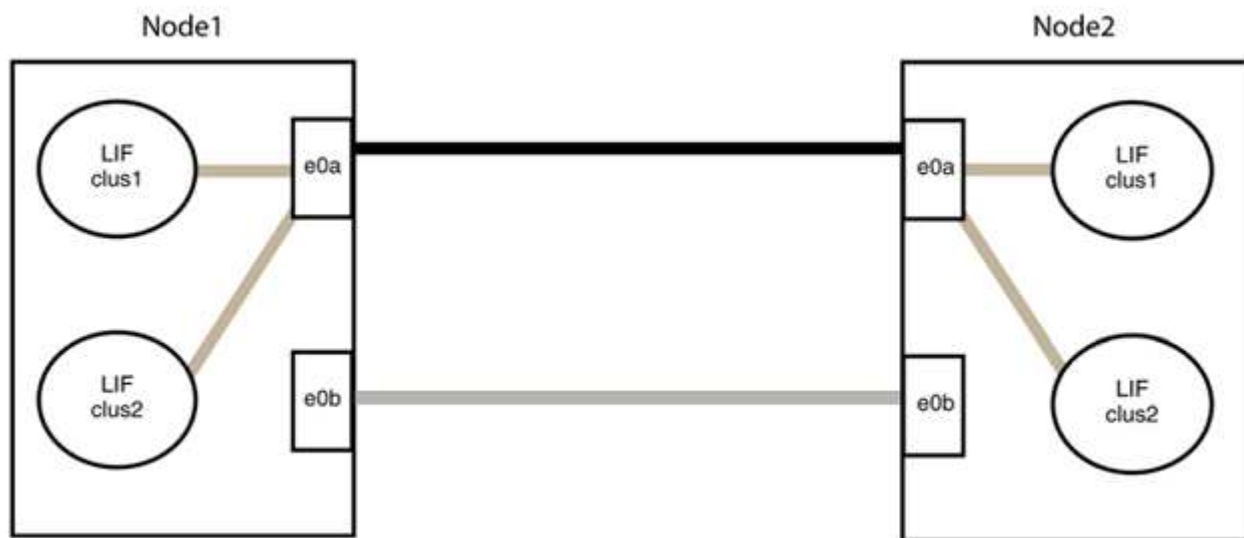
- a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 2.

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
```

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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