



# **Cisco Nexus 9336C-FX2 oder 9336C-FX2-T**

## Cluster and storage switches

NetApp  
September 12, 2025

# Inhalt

Cisco Nexus 9336C-FX2 oder 9336C-FX2-T .....	1
Los geht's .....	1
Installations- und Einrichtungsworkflow für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Cluster-Switches .....	1
Konfigurationsanforderungen für Cisco Nexus 9336C-FX2 und 9336C-FX2-T Cluster-Switches .....	2
Komponenten und Teilenummern für Cisco Nexus 9336C-FX2 und 9336C-FX2-T Cluster-Switches .....	3
Dokumentationsanforderungen für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches .....	4
Anforderungen für Smart Call Home .....	5
Installieren Sie die Hardware .....	6
Workflow zur Hardwareinstallation für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches .....	6
Füllen Sie das Arbeitsblatt zur Verkabelung des Cisco Nexus 9336C-FX2 oder 9336C-FX2-T aus .....	6
Installieren Sie die Cluster-Switches 9336C-FX2 und 9336C-FX2-T .....	11
Installieren Sie Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem NetApp Schrank .....	12
Prüfen Sie die Verkabelung und Konfigurationsüberlegungen .....	16
Konfigurieren der Software .....	17
Workflow zur Softwareinstallation für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Cluster-Switches .....	18
Konfigurieren der Cluster-Switches 9336C-FX2 und 9336C-FX2-T .....	18
Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor .....	21
Installieren oder aktualisieren Sie die NX-OS-Software .....	28
Installieren oder aktualisieren Sie den RCF .....	49
Überprüfen Sie Ihre SSH-Konfiguration .....	87
Setzen Sie die Cluster-Switches 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurück .....	90
Migrieren Sie die Switches .....	90
Migrieren Sie von NetApp CN1610-Cluster-Switches zu Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-Switches .....	90
Migrieren Sie von älteren Cisco -Switches zu Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches .....	107
Migration auf Cluster mit zwei Nodes .....	127
Ersetzen Sie die Schalter .....	143
Ersetzen Sie die Cluster-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T .....	143
Ersetzen Sie Cisco Nexus 9336C-FX2 und 9336C-FX2-T Cluster-Switches durch Switchless-Verbindungen .....	161

# Cisco Nexus 9336C-FX2 oder 9336C-FX2-T

## Los geht's

### Installations- und Einrichtungsworkflow für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Cluster-Switches

Die Cluster-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T sind Teil der Cisco Nexus 9000-Plattform und können in einem NetApp -Systemschrank installiert werden. Mit Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Knoten erstellen.

Cisco Nexus 9336C-FX2 (36 Ports) ist ein Cluster-/Speicher-/Daten-Switch mit hoher Portdichte. Cisco Nexus 9336C-FX2-T (12 Ports) ist ein Hochleistungs-Switch mit geringer Portdichte, der 10/25/40/100GbE-Clusterkonfigurationen unterstützt.

Befolgen Sie diese Arbeitsschritte, um Ihre Cisco 9336C-FX2- und 9336C-FX2-T-Switches zu installieren und einzurichten.

1

#### "Überprüfen der Konfigurationsanforderungen"

Überprüfen Sie die Konfigurationsanforderungen für die Cluster-Switches 9336C-FX2 und 9336C-FX2-T.

2

#### "Überprüfen Sie die Komponenten und Teilenummern"

Überprüfen Sie die Komponenten und Teilenummern für die Cluster-Switches 9336C-FX2 und 9336C-FX2-T.

3

#### "Überprüfen Sie die erforderlichen Unterlagen"

Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 9336C-FX2- und 9336C-FX2-T-Switches und den ONTAP Cluster einzurichten.

4

#### "Überprüfen Sie die Smart Call Home-Anforderungen"

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

5

#### "Installieren Sie die Hardware"

Installieren Sie die Switch-Hardware.

6

#### "Konfigurieren der Software"

Konfigurieren Sie die Switch-Software.

## Konfigurationsanforderungen für Cisco Nexus 9336C-FX2 und 9336C-FX2-T Cluster-Switches

Überprüfen Sie bei der Installation und Wartung der Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T unbedingt die Konfigurations- und Netzwerkanforderungen.

### ONTAP Support

#### ONTAP 9.9.1 und höher

Ab ONTAP 9.9 können Sie mithilfe von Cisco Nexus 9336C-FX2 Switches Storage- und Cluster-Funktionen in einer gemeinsamen Switch-Konfiguration kombinieren.

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Netzwerk-Switches erforderlich.



Die Ethernet-Switch-Statusüberwachung unterstützt ONTAP 9.13.1P8 und früher und 9.14.1P3 und früher oder NX-OS Version 10.3(4a)(M) nicht.

#### ONTAP 9.10.1 und höher

Darüber hinaus können Sie ab ONTAP 9.10.1 Cisco Nexus 9336C-FX2-T-Switches verwenden, um Speicher- und Clusterfunktionen in einer gemeinsam genutzten Switch-Konfiguration zu kombinieren.

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Netzwerk-Switches erforderlich.

## Konfigurationsanforderungen

Stellen Sie sicher, dass:

- Sie verfügen über die entsprechende Anzahl und den entsprechenden Kabeltyp und Kabelstecker für Ihre Switches. Siehe "[Hardware Universe](#)".
- Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen.

## Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie die folgenden Netzwerkinformationen.

- IP-Subnetz für den Management-Netzwerkdatenverkehr
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700s Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.
- Siehe "[Hardware Universe](#)" Aktuelle Informationen.

Weitere Informationen zur Erstkonfiguration des Switches finden Sie im folgenden Handbuch: "[Cisco Nexus 9336C-FX2 – Installations- und Upgrade-Leitfaden](#)".

## Was kommt als nächstes

Nachdem Sie die Konfigurationsanforderungen überprüft haben, können Sie Ihre ["Komponenten und Teilenummern"](#).

## **Komponenten und Teilenummern für Cisco Nexus 9336C-FX2 und 9336C-FX2-T Cluster-Switches**

Für die Installation und Wartung von Cisco Switches Nexus 9336C-FX2 und 9336C-FX2-T muss die Liste der Komponenten und Teilenummern überprüft werden.

### **Details zur Teilenummer**

In der folgenden Tabelle sind die Teilenummer und die Beschreibung der Switches 9336C-FX2 und 9336C-FX2-T, Lüfter und Netzteile aufgeführt:

Teilenummer	Beschreibung
X190200-CS-PE	Cluster-Switch, N9336C 36PT PTSX 10/25/40/100G
X190200-CS-PI	Cluster-Switch, N9336C 36 PT PSIN 10/25/40/100G
X190212-CS-PE	Cluster-Switch, N9336C, 12 PT (9336C-FX2-T), PTSX 10/25/40 G
X190212-CS-PI	Cluster-Switch, N9336C, 12 PT (9336C-FX2-T), PSIN 10/25/40 G
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2 POD-Lizenz mit 24 Anschlüssen
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Zubehörkit X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W Netzteil – Luftstrom am Port Side
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W Netzteil – Luftstrom für den seitlichen Ansauganschluss
X-NXA-LÜFTER-65CFM-PE	N9K-9336C 65 CFM, Luftstrom nach Anschlussseite
X-NXA-LÜFTER-65CFM-PI	N9K-9336C 65 CFM, Luftstrom zur Ansaugöffnung an der Seite des Ports

### **Cisco Smart-Lizenzen nur für 9336C-FX2-T-Ports**

Um mehr als 12 Ports auf Ihrem Cisco Nexus 9336C-FX2-T Cluster Switch zu aktivieren, müssen Sie eine Cisco Smart Lizenz erwerben. Cisco Smart Lizenzen werden über Cisco Smart Accounts verwaltet.

1. Erstellen Sie bei Bedarf ein neues Smart-Konto. Weitere Informationen finden Sie unter ["Erstellen Sie ein neues Smart-Konto"](#).

2. Zugriff auf ein vorhandenes Smart-Konto anfordern. Weitere Informationen finden Sie unter "["Zugriff auf ein vorhandenes Smart-Konto anfordern"](#)".



Nachdem Sie Ihre Smart-Lizenz erworben haben, installieren Sie die entsprechende RCF, um alle 36 verfügbaren Ports zur Verwendung zu aktivieren und zu konfigurieren.

#### Was kommt als nächstes

Nachdem Sie Ihre Komponenten und Teilenummern bestätigt haben, überprüfen Sie die "[erforderliche Dokumentation](#)".

### Dokumentationsanforderungen für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches

Lesen Sie zur Installation und Wartung der Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches unbedingt die spezifische Switch- und Controller-Dokumentation, um Ihre Cisco 9336-FX2-Switches und den ONTAP Cluster einzurichten.

#### Switch-Dokumentation

Zur Einrichtung der Cisco Nexus 9336C-FX2 und 9336C-FX2-T Switches benötigen Sie folgende Dokumentation aus dem "["Switches Der Cisco Nexus 9000-Serie Unterstützen"](#) Seite:

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie Nexus 9000	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 9000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, 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 das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 9000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 9000-Switches.
<i>Nexus 9000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.

Dokumenttitel	Beschreibung
<i>Versionshinweise zur Cisco Nexus 9000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

## Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Version des Betriebssystems von "[ONTAP 9](#)" .

Name	Beschreibung
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP-Dokumentation	Dieser Service bietet detaillierte Informationen zu allen Aspekten der ONTAP Versionen.
"Hardware Universe"	Liefert Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

## Schienensatz und Rack-Dokumentation

Informationen zur Installation eines Cisco 9336-FX2 Switch in einem NetApp Rack finden Sie in der folgenden Hardware-Dokumentation.

Name	Beschreibung
<a href="#">"42-HE-System-Cabinet, Deep Guide"</a>	Beschreibt die FRUs, die dem 42U-Systemschrank zugeordnet sind, und bietet Anweisungen für Wartung und FRU-Austausch.
<a href="#">"Installation eines Cisco 9336-FX2 Switch in einem NetApp Rack"</a>	Beschreibt, wie Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem NetApp Schrank mit vier Pfosten installiert werden.

## 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.

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

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.
- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.
- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

Der "[Cisco Support-Website](#)" Enthält Informationen zu den Befehlen zum Konfigurieren von Smart Call Home.

## Installieren Sie die Hardware

### Workflow zur Hardwareinstallation für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches

Gehen Sie folgendermaßen vor, um die Hardware für die Cluster-Switches 9336C-FX2 und 9336C-FX2-T zu installieren und zu konfigurieren:

1

#### "Vervollständigen Sie das Verkabelungsarbeitsblatt"

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

2

#### "Den Schalter einbauen"

Installieren Sie die Schalter 9336C-FX2 und 9336C-FX2-T.

3

#### "Den Switch in einen NetApp-Schrank einbauen"

Installieren Sie die Switches 9336C-FX2 und 9336C-FX2-T und das Durchgangspanel nach Bedarf in einem NetApp Schrank.

4

#### "Überprüfung der Verkabelung und Konfiguration"

Überprüfen Sie die Unterstützung für NVIDIA Ethernet-Ports, 25GbE-FEC-Anforderungen und Informationen zu TCAM-Ressourcen.

### Füllen Sie das Arbeitsblatt zur Verkabelung des Cisco Nexus 9336C-FX2 oder 9336C-FX2-T aus

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

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

- [9336C-FX2 – Beispieldokument für Verkabelung](#)
- [9336C-FX2 Arbeitsblatt für leere Verkabelung](#)
- [Arbeitsblatt zur 9336C-FX2-T-Beispielverkabelung \(12 Anschlüsse\)](#)
- [Arbeitsblatt für die Verkabelung 9336C-FX2-T-Leereinschub \(12 Anschlüsse\)](#)

### 9336C-FX2 – Beispieldokument für Verkabelung

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	4 x 10-GbE-Node 1	1	4 x 10-GbE-Node 1
2	4 x 10-GbE-Node 2	2	4 x 10-GbE-Node 2
3	4x10 GbE Node 3	3	4x10 GbE Node 3
4	4 x 25-GbE-Node 4	4	4 x 25-GbE-Node 4
5	4 x 25-GbE-Node 5	5	4 x 25-GbE-Node 5
6	4 x 25-GbE-Node 6	6	4 x 25-GbE-Node 6
7	40/100-GbE-Node 7	7	40/100-GbE-Node 7
8	40/100-GbE-Node 8	8	40/100-GbE-Node 8
9	40/100-GbE-Node 9	9	40/100-GbE-Node 9
10	40/100-GbE-Node 10	10	40/100-GbE-Node 10
11	40/100-GbE-Node 11	11	40/100-GbE-Node 11
12	40/100-GbE-Node 12	12	40/100-GbE-Node 12
13	40/100-GbE-Node 13	13	40/100-GbE-Node 13
14	40/100-GbE-Node 14	14	40/100-GbE-Node 14
15	40/100-GbE-Node 15	15	40/100-GbE-Node 15

Cluster-Switch A		Cluster-Switch B	
16	40/100-GbE-Node 16	16	40/100-GbE-Node 16
17	40/100-GbE-Node 17	17	40/100-GbE-Node 17
18	40/100-GbE-Node 18	18	40/100-GbE-Node 18
19	40/100-GbE-Node 19	19	40/100-GbE-Node 19
20	40/100-GbE-Node 20	20	40/100-GbE-Node 20
21	40/100-GbE-Node 21	21	40/100-GbE-Node 21
22	40/100-GbE-Node 22	22	40/100-GbE-Node 22
23	40/100-GbE-Node 23	23	40/100-GbE-Node 23
24	40/100-GbE-Node 24	24	40/100-GbE-Node 24
25 bis 34	Reserviert	25 bis 34	Reserviert
35	100-GbE-ISL zu Switch B- Port 35	35	100-GbE-ISL für Switch A-Port 35
36	100-GbE-ISL zu Switch B- Port 36	36	100-GbE-ISL für Switch A-Port 36

### 9336C-FX2 Arbeitsblatt für leere Verkabelung

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des „[Hardware Universe](#)“ Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
1		1	
2		2	
3		3	
4		4	
5		5	

Cluster-Switch A		Cluster-Switch B	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 bis 34	Reserviert	25 bis 34	Reserviert
35	100-GbE-ISL zu Switch B- Port 35	35	100-GbE-ISL für Switch A-Port 35

Cluster-Switch A		Cluster-Switch B	
36	100-GbE-ISL zu Switch B- Port 36	36	100-GbE-ISL für Switch A-Port 36

### Arbeitsblatt zur 9336C-FX2-T-Beispielverkabelung (12 Anschlüsse)

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	4 x 10-GbE-Node 1	1	4 x 10-GbE-Node 1
2	4 x 10-GbE-Node 2	2	4 x 10-GbE-Node 2
3	4x10 GbE Node 3	3	4x10 GbE Node 3
4	4 x 25-GbE-Node 4	4	4 x 25-GbE-Node 4
5	4 x 25-GbE-Node 5	5	4 x 25-GbE-Node 5
6	4 x 25-GbE-Node 6	6	4 x 25-GbE-Node 6
7	40/100-GbE-Node 7	7	40/100-GbE-Node 7
8	40/100-GbE-Node 8	8	40/100-GbE-Node 8
9	40/100-GbE-Node 9	9	40/100-GbE-Node 9
10	40/100-GbE-Node 10	10	40/100-GbE-Node 10
11 bis 34	Erfordert Lizenz	11 bis 34	Erfordert Lizenz
35	100-GbE-ISL zu Switch B- Port 35	35	100-GbE-ISL für Switch A-Port 35
36	100-GbE-ISL zu Switch B- Port 36	36	100-GbE-ISL für Switch A-Port 36

### Arbeitsblatt für die Verkabelung 9336C-FX2-T-Leereinschub (12 Anschlüsse)

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des „[Hardware Universe](#)“ Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11 bis 34	Erfordert Lizenz	11 bis 34	Erfordert Lizenz
35	100-GbE-ISL zu Switch B- Port 35	35	100-GbE-ISL für Switch A-Port 35
36	100-GbE-ISL zu Switch B- Port 36	36	100-GbE-ISL für Switch A-Port 36

Siehe "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

#### **Was kommt als nächstes**

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

### **Installieren Sie die Cluster-Switches 9336C-FX2 und 9336C-FX2-T**

Befolgen Sie dieses Verfahren, um die Cisco Nexus-Switches 9336C-FX2 und 9336C-FX2-T einzurichten und zu konfigurieren.

#### **Bevor Sie beginnen**

Stellen Sie sicher, dass Sie Folgendes haben:

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von "[Cisco Software-Download](#)" Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel

- Abgeschlossen "Verkabelungsarbeitsblätter".
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden "[mysupport.netapp.com](http://mysupport.netapp.com)". Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- "[Erforderliche Switch- und ONTAP-Dokumentation](#)".

## Schritte

1. Rack-Aufbau des Cluster-Netzwerks und der Management-Netzwerk-Switches und -Controller

Wenn Sie den installieren...	Dann...
Cisco Nexus 9336C-FX2 in einem NetApp Systemschrank	Anweisungen zur Installation des Switches in einem NetApp Rack sind im Dokument <a href="#">_Installation eines Cisco Nexus 9336C-FX2 Cluster-Switch und Pass-Through-Panel in einem NetApp Rack</a> enthalten.
Geräte in einem Telco-Rack	Siehe die Verfahren in den Installationsleitfäden für die Switch-Hardware sowie in den Installations- und Setup-Anleitungen für NetApp.

2. Verkabeln Sie die Switches für das Cluster-Netzwerk und das Management-Netzwerk mithilfe der ausgefüllten Verkabelungsarbeitsblätter mit den Controllern.
3. Schalten Sie das Cluster-Netzwerk sowie die Switches und Controller des Managementnetzwerks ein.

## Was kommt als Nächstes?

Optional können Sie "[Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack](#)". Andernfalls gehen Sie zu "[Verkabelung und Konfiguration überprüfen](#)".

## Installieren Sie Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem NetApp Schrank

Abhängig von Ihrer Konfiguration müssen Sie möglicherweise den Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switch und das Pass-Through-Panel in einem NetApp Schrank installieren. Standardhalterungen sind im Lieferumfang des Schalters enthalten.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Das Pass-Through-Panel-Kit, das von NetApp erhältlich ist (Teilenummer X8784-R6).

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

- Ein Durchlauf-Blindblech
- Vier 10-32 x 0,75 Schrauben
- Vier 10-32-Clip-Muttern

- Für jeden Schalter sind acht 10-32 oder 12-24 Schrauben und Muttern zu befestigen, um die Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten zu befestigen.

- Den Cisco Standard-Schienensatz zur Installation des Switch in einem NetApp Rack



Die Jumper-Kabel sind nicht im Lieferumfang des Pass-Through-Kits enthalten und sollten in Ihrem Switch enthalten sein. Wenn die Switches nicht im Lieferumfang enthalten sind, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

- Informationen zu den anfänglichen Vorbereitungsanforderungen, zum Inhalt des Kits und zu Sicherheitsvorkehrungen finden Sie unter "[Hardware-Installationsleitfaden Der Cisco Nexus 9000-Serie](#)".

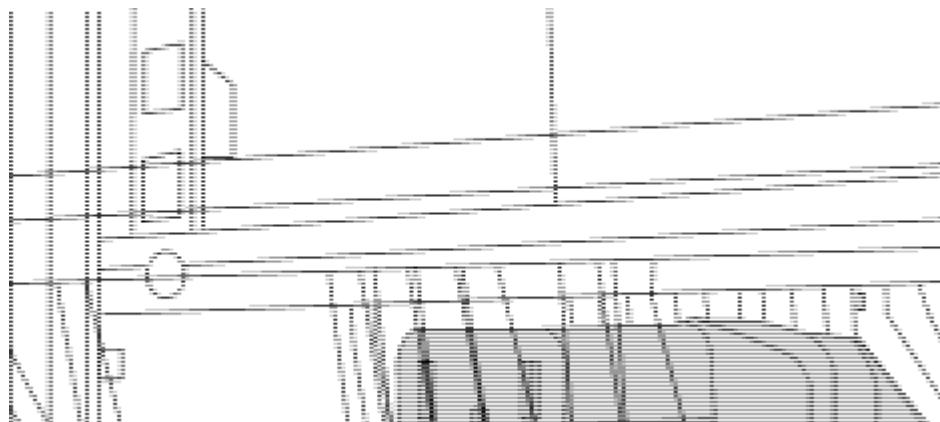
## Schritte

1. Die Pass-Through-Blindplatte in den NetApp-Schrank einbauen.

- a. Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

Bei diesem Verfahren ist die Blindplatte in U40 installiert.

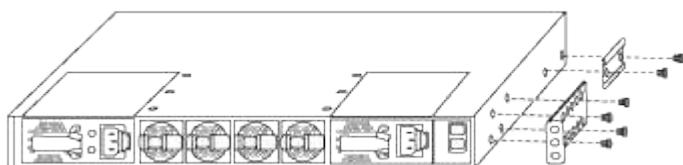
- b. Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
- c. Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
- d. Stecken Sie die Buchsen der beiden 48-Zoll-Jumper-Kabel von der Rückseite der Abdeckung und durch die Bürstenbaugruppe.



(1) Buchsenleiste des Überbrückungskabels.

2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Gehäuse des Nexus 9336C-FX2.

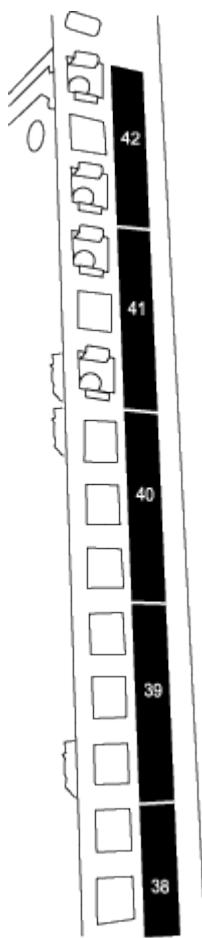
- a. Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.



- b. Wiederholen Sie den Schritt 2 a Mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
- c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.

d. Wiederholen Sie den Schritt 2c Mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite des Schalters.

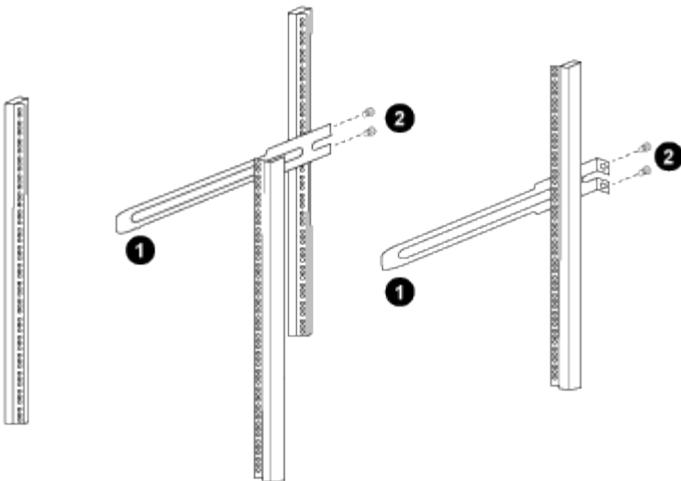
3. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



Die beiden Switches 9336C-FX2 und 9336C-FX2-T werden immer in den oberen 2HE der Schränke RU41 und 42 montiert.

4. Installieren Sie die Gleitschienen im Schrank.

a. Positionieren Sie die erste Gleitschiene an der RU42-Markierung auf der Rückseite des hinteren linken Pfosten, legen Sie die Schrauben mit dem entsprechenden Gewindetyp ein und ziehen Sie die Schrauben mit den Fingern fest.



(1) beim sanften Schieben der Gleitschiene richten Sie sie an den Schraubenbohrungen im Rack aus.

(2) Schrauben der Gleitschienen an den Schrankleisten festziehen.

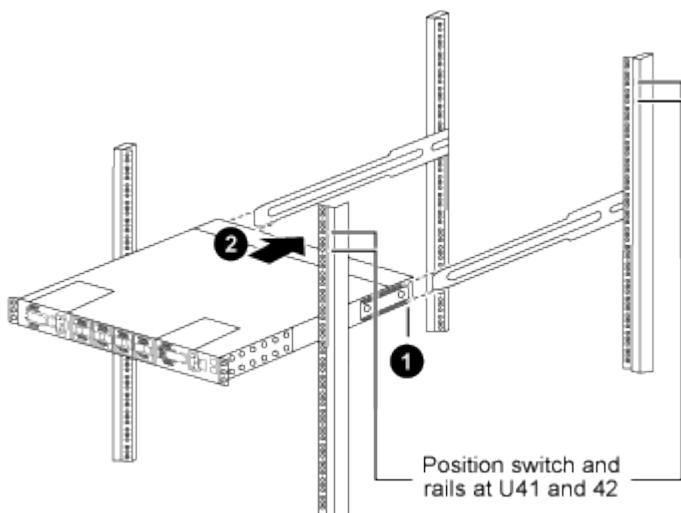
- Wiederholen Sie den Schritt 4 a Für die hintere Säule auf der rechten Seite.
- Wiederholen Sie die Schritte 4 a Und 4b An den RU41 Standorten auf dem Schrank.

5. Den Schalter in den Schrank einbauen.



Für diesen Schritt sind zwei Personen erforderlich: Eine Person muss den Schalter von vorne und von der anderen in die hinteren Gleitschienen führen.

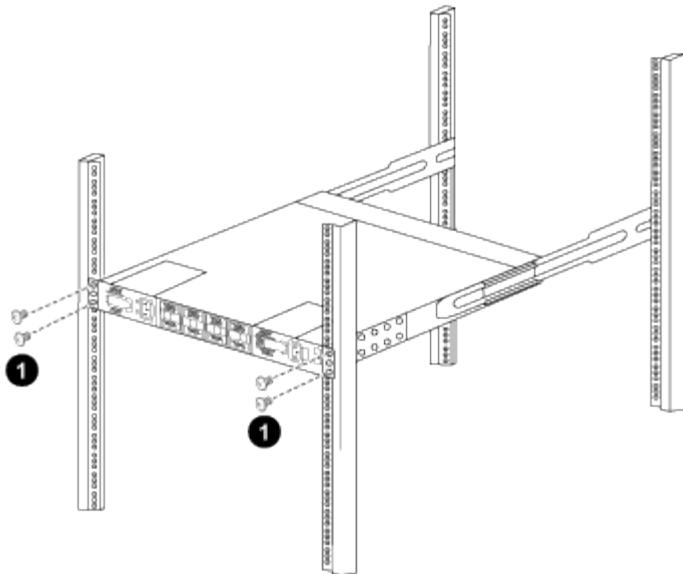
- Positionieren Sie die Rückseite des Schalters an RU41.



(1) Da das Gehäuse in Richtung der hinteren Pfosten geschoben wird, richten Sie die beiden hinteren Rackmontageführungen an den Gleitschienen aus.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Halterungen der Rackmontage bündig mit den vorderen Pfosten sind.

- Befestigen Sie den Schalter am Gehäuse.



(1) mit einer Person, die die Vorderseite des Chassis hält, sollte die andere Person die vier hinteren Schrauben vollständig an den Schrankpfosten festziehen.

- Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- Wiederholen Sie die Schritte [5a](#) Bis [5c](#) Für den zweiten Schalter an der RU42-Position.



Durch die Verwendung des vollständig installierten Schalters als Unterstützung ist es nicht erforderlich, während des Installationsvorgangs die Vorderseite des zweiten Schalters zu halten.

- Wenn die Switches installiert sind, verbinden Sie die Jumper-Kabel mit den Switch-Netzeinkabeln.
- Verbinden Sie die Stecker beider Überbrückungskabel mit den am nächsten verfügbaren PDU-Steckdosen.



Um Redundanz zu erhalten, müssen die beiden Kabel mit verschiedenen PDUs verbunden werden.

- Verbinden Sie den Verwaltungsport an jedem 9336C-FX2- und 9336C-FX2-T-Switch mit einem der Verwaltungsswitches (falls bestellt) oder verbinden Sie sie direkt mit Ihrem Verwaltungsnetzwerk.

Der Management-Port ist der oben rechts gelegene Port auf der PSU-Seite des Switch. Das CAT6-Kabel für jeden Switch muss über die Passthrough-Leiste geführt werden, nachdem die Switches zur Verbindung mit den Management-Switches oder dem Management-Netzwerk installiert wurden.

#### Was kommt als Nächstes?

Nachdem Sie die Switches im NetApp Schrank installiert haben, ["Konfigurieren Sie die Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches"](#).

#### Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihre 9336C-FX2- und 9336C-FX2-T-Switches konfigurieren, beachten Sie die folgenden Hinweise.

## Unterstützung für NVIDIA CX6-, CX6-DX- und CX7-Ethernet-Ports

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 Switch-Port-Geschwindigkeit fest kodieren.

```
(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 "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

## Anforderungen für 25 GbE FEC

### FAS2820 e0a/e0b-Ports

Für die FAS2820 e0a- und e0b-Ports sind Änderungen an der FEC-Konfiguration erforderlich, um eine Verbindung mit den Switch-Ports 9336C-FX2 und 9336C-FX2-T herzustellen. Für die Switch-Ports e0a und e0b ist die FEC-Einstellung auf `rs-cons16`.

```
(cs1) (config)# interface Ethernet1/8-9
(cs1) (config-if-range)# fec rs-cons16
(cs1) (config-if-range)# exit
(cs1) (config)# exit
Save the changes:
(cs1) # copy running-config startup-config
```

## Ports werden aufgrund von TCAM-Ressourcen nicht verbunden

Auf den Switches 9336C-FX2 und 9336C-FX2-T sind die in der vom Switch verwendeten Konfiguration konfigurierten TCAM-Ressourcen (Ternary Content Addressable Memory) erschöpft.

Weitere Informationen finden Sie im Knowledge Base-Artikel "[Aufgrund von TCAM-Ressourcen sind die Ports auf dem Cisco Nexus 9336C-FX2 nicht verbunden](#)" Für Details zur Lösung dieses Problems.

## Konfigurieren der Software

## Workflow zur Softwareinstallation für Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Cluster-Switches

Um die Software für die Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches zu installieren und zu konfigurieren und um die Referenzkonfigurationsdatei (RCF) zu installieren oder zu aktualisieren, gehen Sie wie folgt vor:

**1**

### "Konfigurieren Sie den Switch"

Konfigurieren Sie die Cluster-Switches 9336C-FX2 und 9336C-FX2-T.

**2**

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

Die Cisco NX-OS-Software und Referenzkonfigurationsdateien (RCFs) müssen auf den Cisco 9336C-FX2- und 9336C-FX2-T-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 den Cluster-Switches Cisco 9336C-FX2 und 9336C-FX2-T.

**4**

### "Installieren oder aktualisieren Sie den RCF"

Installieren oder aktualisieren Sie das RCF, nachdem Sie die Cisco -Switches 9336C-FX2 und 9336C-FX2-T zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

**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 Switch auf die Werkseinstellungen zurück"

Löschen Sie die Einstellungen der Cluster-Switches 9336C-FX2 und 9336C-FX2-T.

## Konfigurieren der Cluster-Switches 9336C-FX2 und 9336C-FX2-T

Befolgen Sie dieses Verfahren, um die Cisco Nexus-Switches 9336C-FX2 und 9336C-FX2-T zu konfigurieren.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von "[Cisco Software-Download](#)" Seite.

- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossen "["Verkabelungsarbeitsblätter"](#)".
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden "[mysupport.netapp.com](#)". Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- "["Erforderliche Switch- und ONTAP-Dokumentation"](#)".

## Schritte

1. Initiale Konfiguration der Cluster-Netzwerk-Switches durchführen.

Geben Sie beim ersten Booten des Switches die folgenden Einrichtungsfragen entsprechend an. Die Sicherheitsrichtlinie Ihres Standorts definiert die zu erstellenenden Antworten und Services.

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit <b>ja</b> . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (ja/nein)	Antworten Sie mit <b>ja</b> . Die Standardeinstellung ist ja.
Geben Sie das Passwort für den Administrator ein.	Das Standardpasswort lautet „admin“. Sie müssen ein neues, starkes Passwort erstellen. Ein schwaches Kennwort kann abgelehnt werden.
Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)	Reagieren Sie mit <b>ja</b> bei der Erstkonfiguration des Schalters.
Noch ein Login-Konto erstellen? (ja/nein)	Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen. Der Standardwert ist <b>no</b> .
Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Geben Sie den Switch-Namen ein.	Geben Sie den Switch-Namen ein, der auf 63 alphanumerische Zeichen begrenzt ist.
Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)	Beantworten Sie mit <b>ja</b> (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein.

Eingabeaufforderung	Antwort
Standard-Gateway konfigurieren? (ja/nein)	Antworten Sie mit <b>ja</b> . Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit <b>ja</b>. Die Standardeinstellung ist ja.</p> <p> SSH wird empfohlen, wenn der Ethernet Switch Health Monitor (CSHM) für die Protokollerfassungsfunktionen verwendet wird. SSHv2 wird auch für erhöhte Sicherheit empfohlen.</p>
Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1).	Der Standardwert ist <b>rsa</b> .
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits von 1024 bis 2048 ein.
Konfigurieren Sie den NTP-Server? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Konfigurieren der Standard-Schnittstellenebene (L3/L2)	Antworten Sie mit <b>L2</b> . Der Standardwert ist L2.
Konfiguration des Status der Standard-Switch-Port-Schnittstelle (Shutter/noshut)	Antworten Sie mit <b>noshut</b> . Die Standardeinstellung ist noshut.
Konfiguration des CoPP-Systemprofils (streng/mittelmäßig/lenient/dense)	Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, antworten Sie mit <b>No</b> an der Eingabeaufforderung. Beantworten Sie mit <b>ja</b> , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.

Eingabeaufforderung	Antwort
Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)	<p>Antworten Sie mit <b>ja</b>, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert.</p> <p> Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam.</p>

2. Überprüfen Sie die Konfigurationseinstellungen, die Sie am Ende der Einrichtung in der Anzeige vorgenommen haben, und stellen Sie sicher, dass Sie die Konfiguration speichern.
3. Überprüfen Sie die Version der Cluster-Netzwerk-Switches und laden Sie bei Bedarf die von NetApp unterstützte Version der Software von auf die Switches von herunter "[Cisco Software-Download](#)" Seite.

#### Was kommt als Nächstes?

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

### Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor

Bevor Sie die NX-OS-Software und die RCF-Datei (Reference Configuration File) installieren, gehen Sie wie folgt vor:

#### Vorgeschlagene Dokumentation

- "[Cisco Ethernet Switch Seite](#)"

In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.

- "[Software-Upgrade- und Downgrade-Anleitungen](#)"

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.

- "[Cisco Nexus 9000 und 3000 Upgrade und ISSU Matrix](#)"

Bietet Informationen zu disruptiven Upgrades/Downgrades für die Cisco NX-OS-Software auf Nexus 9000 Series Switches basierend auf Ihren aktuellen und Zielversionen.

Wählen Sie auf der Seite **Disruptive Upgrade** aus, und wählen Sie aus der Dropdown-Liste Ihr aktuelles Release und Ihr Ziel-Release aus.

#### Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01 und cluster1-02.
- 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::*` Eine Eingabeaufforderung gibt den Namen des Clusters an.

## Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

## Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=x h`

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie y ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung ('\*>' erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

## Beispiel anzeigen

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

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

-----
-----  

cluster1-02/cdp
      e0a    cs1          Eth1/2      N9K-
C9336C
      e0b    cs2          Eth1/2      N9K-
C9336C
cluster1-01/cdp
      e0a    cs1          Eth1/1      N9K-
C9336C
      e0b    cs2          Eth1/1      N9K-
C9336C

4 entries were displayed.
```

4. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

```
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

4 entries were displayed.
```

b. Zeigt Informationen zu den LIFs an:

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

## Beispiel anzeigen

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

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

4 entries were displayed.
```

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
                                         LIF           LIF
Packet
Node   Date
Loss
-----
```

Node	Date	Source	Destination
node1	3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-clus1
	3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
node2	3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
	3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2

## Alle ONTAP Versionen

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

```
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. Stellen Sie sicher, dass der Befehl zum automatischen Zurücksetzen 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

          Logical
Vserver   Interface          Auto-revert
-----
Cluster
          cluster1-01_clus1  true
          cluster1-01_clus2  true
          cluster1-02_clus1  true
          cluster1-02_clus2  true
4 entries were displayed.
```

## Was kommt als Nächstes?

Nachdem Sie die Installation der NX-OS-Software und RCF vorbereitet haben, "[Installieren oder aktualisieren Sie die NX-OS-Software](#)".

## Installieren oder aktualisieren Sie die NX-OS-Software

Befolgen Sie dieses Verfahren, um die NX-OS-Software auf den Cluster-Switches Nexus 9336C-FX2 und 9336C-FX2-T zu installieren oder zu aktualisieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch "[Bereiten Sie sich auf die Installation von NX-OS und RCF vor](#)".

## Prüfen Sie die Anforderungen

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).

### Vorgeschlagene Dokumentation

- "[Cisco Ethernet Switch Seite](#)"

In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.

- "[Software-Upgrade- und Downgrade-Anleitungen](#)"

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.

- "[Cisco Nexus 9000 und 3000 Upgrade und ISSU Matrix](#)"

Enthält Informationen zu störenden Upgrades/Downgrades für Cisco NX-OS-Software auf Switches der

Nexus 9000-Serie

Basierend auf Ihren aktuellen und Zielversionen.

Wählen Sie auf der Seite **Disruptive Upgrade** aus, und wählen Sie aus der Dropdown-Liste Ihr aktuelles Release und Ihr Ziel-Release aus.

## Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind 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::*` Eine Eingabeaufforderung gibt den Namen des Clusters an.

## Installieren Sie die Software

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

### Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Überprüfen Sie mit dem Ping-Befehl die Verbindung zum Server, der die NX-OS-Software und die RCF hostet.

### Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

```
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. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
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
C9336C-FX2
    e0d    cs2
C9336C-FX2
cluster1-02/cdp
    e0a    cs1
C9336C-FX2
    e0d    cs2
C9336C-FX2
cluster1-03/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1-04/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1::*>
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports **up** mit einem gesunden Status 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. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

## Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
      Logical          Status      Network
  Current      Current  Is
  Vserver      Interface
  Port        Home
  Admin/Oper  Address/Mask      Node
  -----
  -----
  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. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

```
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      N9K-
C9336C-FX2
    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      N9K-
C9336C-FX2
    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. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs. Die Cluster-LIFs führen ein Failover zum Partner-Cluster-Switch durch und bleiben dort, während Sie das Upgrade-Verfahren für den Ziel-Switch durchführen:

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

6. Kopieren Sie die NX-OS-Software und EPLD-Bilder auf den Nexus 9336C-FX2-Switch.

## Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.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.9.3.5.bin /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.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.9.3.5.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.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.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) 2002-2020, 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/library.txt.
```

### Software

```
BIOS: version 08.38
NXOS: version 9.3(4)
BIOS compile time: 05/29/2020
NXOS image file is: bootflash:///nxos.9.3.4.bin
NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 02:28:31]
```

### Hardware

```
cisco Nexus9000 C9336C-FX2 Chassis
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.

Processor Board ID FOC20291J6K
```

```
Device name: cs2
bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
  Reason: Reset Requested by CLI command reload
  System version: 9.3(4)
  Service:

  plugin
    Core Plugin, Ethernet Plugin

  Active Package(s) :

  cs2#
```

## 8. Installieren Sie das NX-OS Image.

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

## Beispiel anzeigen

```
cs2# install all nxos bootflash:nxos.9.3.5.bin

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

Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.5.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(4)                         9.3(5)
yes
1       bios      v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)      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

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

#### 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 05.33
NXOS: version 9.3(5)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.3.5.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]

Hardware
cisco Nexus9000 C9336C-FX2 Chassis
Intel (R) Xeon (R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
Processor Board ID FOC20291J6K

Device name: cs2
bootflash: 53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)
```

```
Last reset at 277524 usecs after Mon Nov 2 22:45:12 2020
```

```
Reason: Reset due to upgrade
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

10. Aktualisieren Sie das EPLD-Bild, 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

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

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

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. Melden Sie sich nach dem Neustart des Switches erneut an, und überprüfen Sie, ob die neue EPLD-Version 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
```

12. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

a. Vergewissern Sie sich, dass Cluster-Ports über alle Nodes im Cluster hinweg ordnungsgemäß hochaktiv 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 Switch-Zustand vom 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      N9K-
C9336C-FX2
    e0d    cs2                      Ethernet1/7      N9K-
C9336C-FX2
cluster01-2/cdp
    e0a    cs1                      Ethernet1/8      N9K-
C9336C-FX2
    e0d    cs2                      Ethernet1/8      N9K-
C9336C-FX2
cluster01-3/cdp
    e0a    cs1                      Ethernet1/1/1    N9K-
C9336C-FX2
    e0b    cs2                      Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
    e0a    cs1                      Ethernet1/1/2    N9K-
C9336C-FX2
    e0b    cs2                      Ethernet1/1/2    N9K-
C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                  Type          Address
Model

-----
-----
cs1                   cluster-network  10.233.205.90  N9K-
C9336C-FX2
    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  N9K-
```

```
C9336C-FX2
```

```
    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 können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:

```
2020 Nov 17 16:07:18 cs1 %% VDC-1 %% %STP-2-UNBLOCK_CONSIST_PORT:
Unlocking 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.
```

13. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
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::*
```

14. Wiederholen Sie die Schritte 6 bis 13, um die NX-OS-Software auf Switch cs1 zu installieren.

15. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

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

16. Vergewissern Sie sich, dass die Cluster-LIFs auf ihren Home-Port zurückgesetzt wurden:

```
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 an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

#### Was kommt als Nächstes?

Nachdem Sie die NX-OS-Software installiert oder aktualisiert haben, ["Installieren oder aktualisieren Sie die Referenzkonfigurationsdatei \(RCF\)." .](#)

## Installieren oder aktualisieren Sie den RCF

## Installieren oder aktualisieren Sie die Übersicht über die Referenzkonfigurationsdatei (RCF)

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus-Switches 9336C-FX2 und 9336C-FX2-T zum ersten Mal eingerichtet haben. Sie aktualisieren Ihre RCF-Version, wenn auf Ihrem Switch eine vorhandene Version der RCF-Datei installiert ist.

Weitere Informationen zur Installation oder Aktualisierung Ihres RCF finden Sie im Knowledge Base-Artikel "[Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung](#)".

### Verfügbare RCF-Konfigurationen

In der folgenden Tabelle werden die für verschiedene Konfigurationen verfügbaren RCFs beschrieben. Wählen Sie den RCF aus, der für Ihre Konfiguration geeignet ist.

Einzelheiten zur Port- und VLAN-Nutzung finden Sie im Abschnitt Banner und wichtige Hinweise in Ihrem RCF.

RCF-Name	Beschreibung
2-Cluster-HA-Breakout an	Unterstützt zweiONTAP-Cluster mit mindestens acht Nodes, einschließlich Nodes, die gemeinsam genutzte Cluster + HA-Ports verwenden.
4-Cluster-HA-Breakout an	Unterstützt vierONTAP-Cluster mit mindestens vier Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
1-Cluster-HA	Alle Ports sind für 40/100-GbE konfiguriert. Unterstützt Shared Cluster/HA-Datenverkehr auf Ports. Erforderlich für Systeme AFF A320, AFF A250 und FAS500f Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
1-Cluster-HA-Breakout an	Die Ports sind für 4x10-GbE-Breakout, 4x25-GbE-Breakout (RCF 1.6+ auf 100-GbE-Switches) und 40/100-GbE-Breakout konfiguriert. Unterstützt Shared-Cluster-/HA-Traffic auf Ports für Nodes, die Shared-Cluster/HA-Ports verwenden: AFF A320, AFF A250 und FAS500f Systeme. Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
Cluster-HA-Storage	Die Ports sind für 40/100-GbE-Cluster+HA, 4 x 10-GbE-Breakout für Cluster und 4 x 25-GbE-Breakout für Cluster+HA und 100-GbE-Ports für jedes Storage HA-Paar konfiguriert.
Cluster	Zwei RCF-Varianten mit unterschiedlichen Zuweisungen von 4x10GbE-Ports (Breakout) und 40/100-GbE-Ports. Alle FAS/AFF Nodes werden unterstützt, außer AFF A320, AFF A250 und FAS500f Systeme.
Storage	Alle Ports sind für 100-GbE-NVMe-Storage-Verbindungen konfiguriert.

### Vorgeschlagene Dokumentation

- ["Cisco Ethernet-Switches \(NSS\)"](#)

In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen auf der NetApp Support-Website. Beachten Sie, dass es zwischen der Befehlssyntax in der RCF und der Syntax in bestimmten Versionen von NX-OS Befehlssyntax bestehen kann.

- ["Switches Der Cisco Nexus 3000-Serie"](#)

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 Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco-Switches lauten **cs1** und **cs2**.
- Die Knotennamen sind **cluster1-01**, **cluster1-02**, **cluster1-03** und **cluster1-04**.
- Die Namen der Cluster-LIF sind **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::\*** Eine Eingabeaufforderung gibt den Namen des Clusters an.

Die Beispiele in diesem Verfahren verwenden vier Knoten. Diese Knoten verwenden zwei 10GbE Cluster Interconnect Ports **e0a** und **e0b**. ["Hardware Universe"](#) Überprüfen Sie im die richtigen Cluster-Ports auf Ihren Plattformen.



Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.

Weitere Informationen zu den verfügbaren RCF-Konfigurationen finden Sie unter ["Workflow für die Softwareinstallation"](#).

## Verwendete Befehle

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

## Was kommt als Nächstes?

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-Switches 9336C-FX2 und 9336C-FX2-T zum ersten Mal eingerichtet haben.

## Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Eine Konsolenverbindung zum Switch. Die Konsolenverbindung ist optional, wenn Sie Remote-Zugriff auf den Switch haben.
- Switch **cs1** und Switch **cs2** werden eingeschaltet und die Ersteinrichtung des Switches ist abgeschlossen (die Management-IP-Adresse und SSH sind eingerichtet).
- Die gewünschte NX-OS-Version wurde installiert.

- ISL-Verbindungen zwischen Switches sind angeschlossen.
- Die ONTAP Node-Cluster-Ports sind nicht verbunden.

#### Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich an, um cs1 über SSH oder über eine serielle Konsole zu wechseln.
2. Kopieren Sie den RCF mit einem der folgenden Übertragungsprotokolle auf den Bootflash von Switch cs1: FTP, TFTP, SFTP oder SCP.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfäden.

#### Beispiel anzeigen

Dieses Beispiel zeigt TFTP, mit dem eine RCF in den Bootflash auf Switch cs1 kopiert wird:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_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 RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfäden.

#### Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` Installation auf Switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

4. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

## Beispiel anzeigen

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date        : 10-23-2020
* Version     : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in config
mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

5. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

6. Wenden Sie alle vorherigen Anpassungen erneut auf die Switch-Konfiguration an. ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#) Weitere Informationen zu erforderlichen Änderungen finden Sie unter.
7. Speichern Sie die grundlegenden Konfigurationsdetails in der Datei `write_erase.cfg` auf dem Bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg  
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg  
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg  
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

8. Führen Sie für RCF Version 1.12 und höher die folgenden Befehle aus:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>  
bootflash:write_erase.cfg  
  
cs1# echo "hardware access-list tcam region egr-racl 1024" >>  
bootflash:write_erase.cfg  
  
cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>  
bootflash:write_erase.cfg
```

Siehe den Knowledge Base-Artikel ["Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung"](#) für weitere Details.

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

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

10. Geben Sie die `write erase` Befehl zum Löschen der aktuell gespeicherten Konfiguration:

```
cs1# 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 Grundkonfiguration in die Startkonfiguration.

```
cs1# copy bootflash:write_erase.cfg startup-config.
```

12. Starten Sie den Switch cs1 neu.

```
cs1# reload
```

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

13. Wiederholen Sie die Schritte 1 bis 12 auf Switch cs2.

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. Stellen Sie sicher, dass die mit den Cluster-Ports verbundenen Switch-Ports **up** sind.

```
show interface brief
```

#### 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 mit den folgenden Befehlen, ob sich die Cluster-Nodes in den richtigen Cluster-VLANS befinden:

```
show vlan brief
```

```
show interface trunk
```

## Beispiel anzeigen

```
cs1# show vlan brief

VLAN Name                               Status      Ports
---- -----
1      default                           active      Po1, Eth1/1, Eth1/2,
                                              Eth1/3
                                              Eth1/4, Eth1/5,
                                              Eth1/6, Eth1/7
                                              Eth1/8, Eth1/35,
                                              Eth1/9/1, Eth1/9/2,
                                              Eth1/9/3
                                              Eth1/9/4, Eth1/10/1,
                                              Eth1/10/2
                                              Eth1/10/3, Eth1/10/4
17     VLAN0017                          active      Eth1/1, Eth1/2,
                                              Eth1/3, Eth1/4
                                              Eth1/5, Eth1/6,
                                              Eth1/7, Eth1/8
                                              Eth1/9/1, Eth1/9/2,
                                              Eth1/9/3
                                              Eth1/9/4, Eth1/10/1,
                                              Eth1/10/2
                                              Eth1/10/3, Eth1/10/4
18     VLAN0018                          active      Eth1/1, Eth1/2,
                                              Eth1/3, Eth1/4
                                              Eth1/5, Eth1/6,
                                              Eth1/7, Eth1/8
                                              Eth1/9/1, Eth1/9/2,
                                              Eth1/9/3
                                              Eth1/9/4, Eth1/10/1,
                                              Eth1/10/2
                                              Eth1/10/3, Eth1/10/4
31     VLAN0031                          active      Eth1/11, Eth1/12,
                                              Eth1/13
                                              Eth1/14, Eth1/15,
                                              Eth1/16
                                              Eth1/17, Eth1/18,
                                              Eth1/19
                                              Eth1/20, Eth1/21,
                                              Eth1/22
                                              Eth1/23, Eth1/24,
32     VLAN0032                          active      Eth1/25
```

Eth1/28			Eth1/26, Eth1/27,
Eth1/31			Eth1/29, Eth1/30,
Eth1/34			Eth1/32, Eth1/33,
33 VLAN0033	active		Eth1/11, Eth1/12,
Eth1/13			Eth1/14, Eth1/15,
Eth1/16			Eth1/17, Eth1/18,
Eth1/19			Eth1/20, Eth1/21,
Eth1/22			Eth1/23, Eth1/24,
34 VLAN0034	active		Eth1/26, Eth1/27,
Eth1/25			Eth1/29, Eth1/30,
Eth1/28			Eth1/32, Eth1/33,
Eth1/31			Eth1/34

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--
Eth1/9/1	1	trunking	--
Eth1/9/2	1	trunking	--
Eth1/9/3	1	trunking	--
Eth1/9/4	1	trunking	--
Eth1/10/1	1	trunking	--
Eth1/10/2	1	trunking	--
Eth1/10/3	1	trunking	--
Eth1/10/4	1	trunking	--
Eth1/11	33	trunking	--

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

---

Port                    Vlans Allowed on Trunk

---

Eth1/1	1,17-18
Eth1/2	1,17-18
Eth1/3	1,17-18
Eth1/4	1,17-18
Eth1/5	1,17-18
Eth1/6	1,17-18
Eth1/7	1,17-18
Eth1/8	1,17-18
Eth1/9/1	1,17-18
Eth1/9/2	1,17-18
Eth1/9/3	1,17-18
Eth1/9/4	1,17-18
Eth1/10/1	1,17-18
Eth1/10/2	1,17-18
Eth1/10/3	1,17-18
Eth1/10/4	1,17-18

Eth1/11	31, 33
Eth1/12	31, 33
Eth1/13	31, 33
Eth1/14	31, 33
Eth1/15	31, 33
Eth1/16	31, 33
Eth1/17	31, 33
Eth1/18	31, 33
Eth1/19	31, 33
Eth1/20	31, 33
Eth1/21	31, 33
Eth1/22	31, 33
Eth1/23	32, 34
Eth1/24	32, 34
Eth1/25	32, 34
Eth1/26	32, 34
Eth1/27	32, 34
Eth1/28	32, 34
Eth1/29	32, 34
Eth1/30	32, 34
Eth1/31	32, 34
Eth1/32	32, 34
Eth1/33	32, 34
Eth1/34	32, 34
Eth1/35	1
Eth1/36	1
Po1	1
..	
..	
..	
..	
..	



Einzelheiten zur Port- und VLAN-Nutzung finden Sie im Abschnitt Banner und wichtige Hinweise in Ihrem RCF.

3. Stellen Sie sicher, dass die ISL 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      Eth1/35 (P)    Eth1/36 (P)
cs1#
```

## Schritt 3: Richten Sie Ihren ONTAP-Cluster ein

NetApp empfiehlt, zum Einrichten neuer Cluster System Manager zu verwenden.

System Manager bietet einen einfachen und einfachen Workflow für die Cluster-Einrichtung und -Konfiguration einschließlich der Zuweisung einer Node-Management-IP-Adresse, Initialisierung des Clusters, Erstellung eines lokalen Tiers, Konfiguration von Protokollen und Bereitstellung des anfänglichen Storage.

Gehen Sie zu ["Konfigurieren Sie ONTAP mit System Manager in einem neuen Cluster"](#) Für Setup-Anweisungen.

### Was kommt als Nächstes?

Nachdem Sie die RCF installiert haben, ["Überprüfen Sie die SSH-Konfiguration"](#).

### Aktualisieren der Referenzkonfigurationsdatei (RCF)

Sie aktualisieren Ihre RCF-Version, wenn auf Ihren Betriebsschaltern eine vorhandene Version der RCF-Datei installiert ist.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Der aktuelle RZB.
- Wenn Sie Ihre RCF-Version aktualisieren, benötigen Sie eine Startkonfiguration im RCF, die die gewünschten Startabbilder widerspiegelt.

Wenn Sie die Startkonfiguration ändern müssen, um die aktuellen Startabbilder zu berücksichtigen, müssen Sie dies vor dem erneuten Anwenden des RCF tun, damit die korrekte Version bei zukünftigen Neustarts instanziert wird.

 Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

 Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein oder grundlegende Konfigurationsinformationen beibehalten haben, bevor Sie die Switch-Einstellungen löschen.

#### **Schritt 1: Bereiten Sie sich auf das Upgrade vor**

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
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
C9336C
    e0d    cs2
C9336C
cluster1-02/cdp
    e0a    cs1
C9336C
    e0d    cs2
C9336C
cluster1-03/cdp
    e0a    cs1
C9336C
    e0b    cs2
C9336C
cluster1-04/cdp
    e0a    cs1
C9336C
    e0b    cs2
C9336C
cluster1::*
```

2. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports **up** mit einem gesunden Status 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. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

## Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
      Logical          Status      Network
  Current      Current  Is
  Vserver      Interface
  Port        Home
  Admin/Oper  Address/Mask      Node
  -----
  -----
  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. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

```
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      N9K-
C9336C
    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      N9K-
C9336C
    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::*
```

3. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

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

## Schritt 2: Ports konfigurieren

1. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

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

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



Stellen Sie sicher, dass Sie **alle** verbundenen Cluster-Ports herunterfahren, um Probleme mit der Netzwerkverbindung zu vermeiden. ["Kein Quorum mehr aus dem Node bei der Migration von LIF auf Cluster während des Upgrades des Switch-Betriebssystems"](#) Weitere Informationen finden Sie im Knowledge Base-Artikel.

2. Vergewissern Sie sich, dass für die Cluster-LIFs ein Failover zu den auf Cluster-Switch cs1 gehosteten Ports 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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
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. Wenn 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
```

- a. Notieren Sie alle benutzerdefinierten Ergänzungen zwischen der aktuellen Running-config und der verwendeten RCF-Datei (z. B. eine SNMP-Konfiguration für Ihr Unternehmen).
- b. Verwenden Sie für NX-OS 10.2 und neuer die `show diff running-config` Befehl zum Vergleich mit der gespeicherten RCF-Datei im Bootflash. Verwenden Sie andernfalls ein Werkzeug zum Vergleichen/Vergleichen des dritten Teils.

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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

6. Führen Sie für RCF Version 1.12 und höher die folgenden Befehle aus:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg
cs1# echo "hardware access-list tcam region ing-12-qos 1280" >>
bootflash:write_erase.cfg
```

Siehe den Knowledge Base-Artikel "["Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung"](#)" für weitere Details.

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

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

8. Führen Sie den Befehl zum Löschen des Schreibvorgangs aus, um die aktuell gespeicherte Konfiguration zu löschen:

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

9. Kopieren Sie die zuvor gespeicherte Grundkonfiguration in die Startkonfiguration.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Führen Sie einen Neustart des Switches aus:

```
switch# reload
```

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

11. Nachdem die Management-IP-Adresse wieder erreichbar ist, melden Sie sich über SSH beim Switch an.

Möglicherweise müssen Sie die Einträge der Host-Datei im Zusammenhang mit den SSH-Schlüsseln aktualisieren.

12. Kopieren Sie den RCF mit einem der folgenden Übertragungsprotokolle auf den Bootflash von Switch cs1: FTP, TFTP, SFTP oder SCP.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfäden.

#### Beispiel anzeigen

Dieses Beispiel zeigt TFTP, mit dem eine RCF in den Bootflash auf Switch cs1 kopiert wird:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_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)...
```

13. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfäden.

## Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` Installation auf Switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

14. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

## Beispiel anzeigen

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date        : 10-23-2020
* Version     : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in config
mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

15. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

16. Wenden Sie alle vorherigen Anpassungen erneut auf die Switch-Konfiguration an. ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#) Weitere Informationen zu erforderlichen Änderungen finden Sie unter.

17. Nachdem Sie überprüft haben, ob die RCF-Versionen, die benutzerdefinierten Ergänzungen und die Switch-Einstellungen 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-Serie NX-OS Command Reference"](#) Leitfäden.

```
cs1# copy running-config startup-config  
[] 100% Copy complete
```

18. Starten Sie den Switch cs1 neu. Sie können die Warnmeldungen „Cluster-Switch-Systemzustandsüberwachung“ und die Ereignisse „Cluster-Ports ausgefallen“, die von den Nodes gemeldet werden, ignorieren, während der Switch neu gebootet wird.

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

19. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

a. Vergewissern Sie sich, dass Cluster-Ports über alle Nodes im Cluster hinweg ordnungsgemäß hochaktiv 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 Switch-Zustand vom 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      N9K-
C9336C
    e0d    cs2                      Ethernet1/7      N9K-
C9336C
cluster01-2/cdp
    e0a    cs1                      Ethernet1/8      N9K-
C9336C
    e0d    cs2                      Ethernet1/8      N9K-
C9336C
cluster01-3/cdp
    e0a    cs1                      Ethernet1/1/1    N9K-
C9336C
    e0b    cs2                      Ethernet1/1/1    N9K-
C9336C
cluster1-04/cdp
    e0a    cs1                      Ethernet1/1/2    N9K-
C9336C
    e0b    cs2                      Ethernet1/1/2    N9K-
C9336C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                  Type          Address
Model

-----
-----
cs1                   cluster-network  10.233.205.90  NX9-
C9336C
    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  NX9-
```

C9336C

```
    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 können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:

```
2020 Nov 17 16:07:18 cs1 %% VDC-1 %% %STP-2-UNBLOCK_CONSIST_PORT:
Unlocking 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.
```

20. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
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::*
```

21. Wiederholen Sie die Schritte 1 bis 20 am Schalter cs2.

22. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

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

### Schritt 3: Überprüfen Sie die Cluster-Netzwerkkonfiguration und den Zustand des Clusters

1. Stellen Sie sicher, dass die mit den Cluster-Ports verbundenen Switch-Ports **up** sind.

```
show interface brief
```

#### 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 erwarteten Nodes weiterhin verbunden sind:

```
show cdp neighbors
```

## Beispiel anzeigen

```
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      133      H            FAS2980
e0a
node2          Eth1/2      133      H            FAS2980
e0a
cs1            Eth1/35     175      R S I s      N9K-C9336C
Eth1/35
cs1            Eth1/36     175      R S I s      N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Überprüfen Sie mit den folgenden Befehlen, ob sich die Cluster-Nodes in den richtigen Cluster-VLANs befinden:

```
show vlan brief
```

```
show interface trunk
```

## Beispiel anzeigen

```
cs1# show vlan brief

VLAN Name                               Status    Ports
---- -----
1      default                           active    Po1, Eth1/1, Eth1/2,
                                              Eth1/3
                                              Eth1/4, Eth1/5,
                                              Eth1/6, Eth1/7
                                              Eth1/8, Eth1/35,
                                              Eth1/9/1, Eth1/9/2,
                                              Eth1/9/3
                                              Eth1/9/4, Eth1/10/1,
                                              Eth1/10/2
                                              Eth1/10/3, Eth1/10/4
17     VLAN0017                          active    Eth1/1, Eth1/2,
                                              Eth1/3, Eth1/4
                                              Eth1/5, Eth1/6,
                                              Eth1/7, Eth1/8
                                              Eth1/9/1, Eth1/9/2,
                                              Eth1/9/3
                                              Eth1/9/4, Eth1/10/1,
                                              Eth1/10/2
                                              Eth1/10/3, Eth1/10/4
18     VLAN0018                          active    Eth1/1, Eth1/2,
                                              Eth1/3, Eth1/4
                                              Eth1/5, Eth1/6,
                                              Eth1/7, Eth1/8
                                              Eth1/9/1, Eth1/9/2,
                                              Eth1/9/3
                                              Eth1/9/4, Eth1/10/1,
                                              Eth1/10/2
                                              Eth1/10/3, Eth1/10/4
31     VLAN0031                          active    Eth1/11, Eth1/12,
                                              Eth1/13
                                              Eth1/14, Eth1/15,
                                              Eth1/16
                                              Eth1/17, Eth1/18,
                                              Eth1/19
                                              Eth1/20, Eth1/21,
                                              Eth1/22
32     VLAN0032                          active    Eth1/23, Eth1/24,
                                              Eth1/25
```

Eth1/28			Eth1/26, Eth1/27,
Eth1/31			Eth1/29, Eth1/30,
Eth1/34			Eth1/32, Eth1/33,
33 VLAN0033	active		Eth1/11, Eth1/12,
Eth1/13			Eth1/14, Eth1/15,
Eth1/16			Eth1/17, Eth1/18,
Eth1/19			Eth1/20, Eth1/21,
Eth1/22			Eth1/23, Eth1/24,
34 VLAN0034	active		Eth1/26, Eth1/27,
Eth1/25			Eth1/29, Eth1/30,
Eth1/28			Eth1/32, Eth1/33,
Eth1/31			Eth1/34

cs1# **show interface trunk**

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--
Eth1/9/1	1	trunking	--
Eth1/9/2	1	trunking	--
Eth1/9/3	1	trunking	--
Eth1/9/4	1	trunking	--
Eth1/10/1	1	trunking	--
Eth1/10/2	1	trunking	--
Eth1/10/3	1	trunking	--
Eth1/10/4	1	trunking	--
Eth1/11	33	trunking	--

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

---

Port                    Vlans Allowed on Trunk

---

Eth1/1	1,17-18
Eth1/2	1,17-18
Eth1/3	1,17-18
Eth1/4	1,17-18
Eth1/5	1,17-18
Eth1/6	1,17-18
Eth1/7	1,17-18
Eth1/8	1,17-18
Eth1/9/1	1,17-18
Eth1/9/2	1,17-18
Eth1/9/3	1,17-18
Eth1/9/4	1,17-18
Eth1/10/1	1,17-18
Eth1/10/2	1,17-18
Eth1/10/3	1,17-18
Eth1/10/4	1,17-18

Eth1/11	31, 33
Eth1/12	31, 33
Eth1/13	31, 33
Eth1/14	31, 33
Eth1/15	31, 33
Eth1/16	31, 33
Eth1/17	31, 33
Eth1/18	31, 33
Eth1/19	31, 33
Eth1/20	31, 33
Eth1/21	31, 33
Eth1/22	31, 33
Eth1/23	32, 34
Eth1/24	32, 34
Eth1/25	32, 34
Eth1/26	32, 34
Eth1/27	32, 34
Eth1/28	32, 34
Eth1/29	32, 34
Eth1/30	32, 34
Eth1/31	32, 34
Eth1/32	32, 34
Eth1/33	32, 34
Eth1/34	32, 34
Eth1/35	1
Eth1/36	1
Po1	1
..	
..	
..	
..	
..	



Einzelheiten zur Port- und VLAN-Nutzung finden Sie im Abschnitt Banner und wichtige Hinweise in Ihrem RCF.

4. Stellen Sie sicher, dass die ISL 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      Eth1/35 (P)    Eth1/36 (P)
cs1#
```

5. Vergewissern Sie sich, dass die Cluster-LIFs auf ihren Home-Port zurückgesetzt wurden:

```
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 an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

6. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
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::*>
```

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
                                         LIF           LIF
Packet
Node   Date
Loss
-----
```

Node	Date	Source	Destination
node1	3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-clus1
	3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
node2	3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
	3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2

## Alle ONTAP Versionen

Sie können für alle ONTAP Versionen auch den verwenden `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)

```

### Was kommt als Nächstes?

Nachdem Sie Ihr RCF aktualisiert haben, ["Überprüfen Sie die SSH-Konfiguration"](#).

## Überprüfen Sie Ihre SSH-Konfiguration

Wenn Sie die Funktionen des Ethernet Switch Health Monitor (CSHM) und der

Protokollsammlung verwenden, überprüfen Sie, ob SSH- und SSH-Schlüssel auf den Cluster-Switches aktiviert sind.

#### Schritte

1. Vergewissern Sie sich, dass 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
AAAAB3NzaC1yc2EAAAQABAAAAgQDiNrD52Q586wTGJjFAbjB1FaA23EpDrZ2sDCew
17nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCD Srp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAIBmlzdHA1MjEAAACFBABJ+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 den Bitcount mit dem Befehl auf dem Switch auf 256 ändern `ssh key ecdsa 256 force`. ["Konfiguration der Netzwerksicherheit mit FIPS"](#) Weitere Informationen finden Sie unter.

### Was kommt als Nächstes?

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

## Setzen Sie die Cluster-Switches 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurück

Um die Cluster-Switches 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurückzusetzen, müssen Sie die Switch-Einstellungen 9336C-FX2 und 9336C-FX2-T löschen.

### Über diese Aufgabe

- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

### 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 fortfahren.

## Migrieren Sie die Switches

### Migrieren Sie von NetApp CN1610-Cluster-Switches zu Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-Switches

Sie können NetApp CN1610-Cluster-Switches für einen ONTAP Cluster auf Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-Switches migrieren. Dies ist ein unterbrechungsfreies Verfahren.

### Prüfen Sie die Anforderungen

Sie müssen bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen beachten, wenn Sie NetApp CN1610-Cluster-Switches durch Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-

Switches ersetzen. Sie müssen auch die Seriennummer des Switches überprüfen, um sicherzustellen, dass der richtige Switch migriert wird.

## Unterstützte Switches

Folgende Cluster-Switches werden unterstützt:

- NetApp CN1610
- Cisco 9336C-FX2
- Cisco 9336C-FX2-T

Weitere Informationen zu unterstützten Ports und deren Konfigurationen finden Sie im ["Hardware Universe"](#).

## Was Sie benötigen

Stellen Sie sicher, dass Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Der vorhandene Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die Cluster-Switches Cisco 9336C-FX2 und 9336C-FX2-T sind konfiguriert und werden unter der richtigen Version von NX-OS mit angewandter Referenzkonfigurationsdatei (RCF) betrieben.
- Die vorhandene Cluster-Netzwerkkonfiguration verfügt über folgende Merkmale:
  - Ein redundantes und voll funktionsfähiges NetApp Cluster mit NetApp CN1610 Switches.
  - Managementkonnektivität und Konsolenzugriff sowohl auf die NetApp CN1610-Switches als auch auf die neuen Switches.
  - Alle Cluster-LIFs im Status „up“ mit den Cluster-LIFs befinden sich auf den Home-Ports.
- Einige der Ports sind auf den Cisco 9336C-FX2- und 9336C-FX2-T-Switches für den Betrieb mit 40 GbE oder 100 GbE konfiguriert.
- Sie haben 40GbE- und 100GbE-Konnektivität von Knoten zu Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-Switches geplant, migriert und dokumentiert.

## Migrieren Sie die Switches

### Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen CN1610 Cluster Switches sind C1 und C2.
- Die neuen Cluster-Switches 9336C-FX2 sind cs1 und cs2.
- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node 1\_clus1\_ und *node1\_clus2* und *node2\_clus1* bzw. *node2\_clus2* auf Knoten 2.
- Der `cluster1::*` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e3a und e3b.

### Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Schalter C2 wird zuerst durch Schalter cs2 ersetzt.

- Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
  - Alle Cluster-LIFs führen ein Failover auf den neuen Switch cs2 durch.
- Die Verkabelung zwischen den Knoten und C2 wird dann von C2 getrennt und wieder mit cs2 verbunden.
- Switch C1 wird durch Switch cs1 ersetzt.
  - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
    - Alle Cluster-LIFs führen ein Failover auf den neuen Switch cs1 durch.
  - Die Verkabelung zwischen den Knoten und C1 wird dann von C1 getrennt und wieder mit cs1 verbunden.

 Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Cluster-Betrieb zu gewährleisten, führt das folgende Verfahren ein Failover aller Cluster-LIFs auf den Partner-Switch des Betriebs durch, während die Schritte auf dem Ziel-Switch ausgeführt werden.

#### Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie y ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (\*>) wird angezeigt.

3. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

Wenn Sie die automatische Zurücksetzung für dieses Verfahren deaktivieren, werden die Cluster-LIFs nicht automatisch zurück zu ihrem Home Port verschoben. Sie verbleiben im aktuellen Port, während er weiterhin betriebsbereit ist.

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

#### Schritt: Ports und Verkabelung konfigurieren

1. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

Jeder Port sollte für angezeigt werden Link Und healthy Für Health Status.

- a. Zeigen Sie die Attribute des Netzwerkports an:

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

## 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
-----  -----
-----  -----
e3a      Cluster   Cluster           up   9000  auto/100000
healthy  false
e3b      Cluster   Cluster           up   9000  auto/100000
healthy  false

Node: node2

Ignore                                         Speed (Mbps)
Health   Health
Port     IPspace   Broadcast Domain Link MTU   Admin/Oper
Status   Status
-----  -----
-----  -----
e3a      Cluster   Cluster           up   9000  auto/100000
healthy  false
e3b      Cluster   Cluster           up   9000  auto/100000
healthy  false
```

b. Zeigt Informationen zu den LIFs und ihren zugewiesenen Home-Nodes an:

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

Jede LIF sollte angezeigt werden up/up Für Status Admin/Oper Und true Für Is Home.

### 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
e3a        true
          node1_clus2  up/up      169.254.49.125/16  node1
e3b        true
          node2_clus1  up/up      169.254.47.194/16  node2
e3a        true
          node2_clus2  up/up      169.254.19.183/16  node2
e3b        true
```

2. Die Cluster-Ports auf jedem Node sind mit vorhandenen Cluster-Switches auf die folgende Weise (aus Sicht der Nodes) verbunden. Verwenden Sie dazu den Befehl:

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

### Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----  -----
-----  -----
node1      /cdp
          e3a    C1  (6a:ad:4f:98:3b:3f)  0/1
          e3b    C2  (6a:ad:4f:98:4c:a4)  0/1
node2      /cdp
          e3a    C1  (6a:ad:4f:98:3b:3f)  0/2
          e3b    C2  (6a:ad:4f:98:4c:a4)  0/2
```

3. Die Cluster-Ports und -Switches sind (aus Sicht der Switches) folgendermaßen verbunden:

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
C2 0/13	0/13	179	S I s	CN1610
C2 0/14	0/14	175	S I s	CN1610
C2 0/15	0/15	179	S I s	CN1610
C2 0/16	0/16	175	S I s	CN1610

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
C1 0/13	0/13	175	S I s	CN1610
C1 0/14	0/14	175	S I s	CN1610
C1 0/15	0/15	175	S I s	CN1610
C1 0/16	0/16	175	S I s	CN1610

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
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. bei Switch C2 fahren Sie die mit den Cluster-Ports der Knoten verbundenen Ports herunter, um ein Failover der Cluster-LIFs durchzuführen.



Versuchen Sie nicht, die Cluster-LIFs manuell zu migrieren.

```

(C2) # configure
(C2) (Config) # interface 0/1-0/12
(C2) (Interface 0/1-0/12) # shutdown
(C2) (Interface 0/1-0/12) # exit
(C2) (Config) # exit

```

2. Verschieben Sie die Knotencluster-Ports vom alten Switch C2 zum neuen Switch cs2. Verwenden Sie dazu die entsprechende Verkabelung, die von Cisco 9336C-FX2 und 9336C-FX2-T unterstützt wird.
3. Zeigen Sie die Attribute des Netzwerkports an:

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

## Beispiel anzeigen

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

Node: node1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----
e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false

Node: node2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----
e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false
```

4. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

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

## Beispiel anzeigen

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

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

-----
-----
node1      /cdp
          e3a    C1  (6a:ad:4f:98:3b:3f)  0/1
CN1610
          e3b    cs2  (b8:ce:f6:19:1a:7e)  Ethernet1/1/1      N9K-
C9336C-FX2
node2      /cdp
          e3a    C1  (6a:ad:4f:98:3b:3f)  0/2
CN1610
          e3b    cs2  (b8:ce:f6:19:1b:96)  Ethernet1/1/2      N9K-
C9336C-FX2
```

5. Überprüfen Sie bei Switch cs2, ob alle Node-Cluster-Ports aktiviert sind:

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

## Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
          Logical      Status      Network      Current
Current Is
Vserver      Interfac      Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
          node1_clus1  up/up      169.254.3.4/16      node1
e0b      false
          node1_clus2  up/up      169.254.3.5/16      node1
e0b      true
          node2_clus1  up/up      169.254.3.8/16      node2
e0b      false
          node2_clus2  up/up      169.254.3.9/16      node2
e0b      true
```

6. Fahren Sie auf Switch C1 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster LIFs zu ermöglichen.

```
(C1) # configure
(C1) (Config) # interface 0/1-0/12
(C1) (Interface 0/1-0/12) # shutdown
(C1) (Interface 0/1-0/12) # exit
(C1) (Config) # exit
```

7. Verschieben Sie die Knotencluster-Ports vom alten Switch C1 zum neuen Switch cs1. Verwenden Sie dazu die entsprechende Verkabelung, die von Cisco 9336C-FX2 und 9336C-FX2-T unterstützt wird.
8. Überprüfen der endgültigen Konfiguration des Clusters:

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

Jeder Port sollte angezeigt werden **up** Für **Link** Und **healthy** Für **Health** Status.

## Beispiel anzeigen

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

Node: node1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----
e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false

Node: node2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----
e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false
```

9. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

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

## Beispiel anzeigen

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

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

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

Node/	Protocol	Port	Device (LLDP: ChassisID)	Interface
node1	/cdp	e3a	cs1 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1
		e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2
C9336C-FX2	C9336C-FX2			
node2	/cdp	e3a	cs1 (b8:ce:f6:19:1a:7e)	Ethernet1/1/1
		e3b	cs2 (b8:ce:f6:19:1b:96)	Ethernet1/1/2
C9336C-FX2	C9336C-FX2			

10. Überprüfen Sie auf den Switches cs1 und cs2, ob alle Node-Cluster-Ports aktiviert sind:

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

## Beispiel anzeigen

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

Node: node1

Ignore

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

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
```

11. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

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

## Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface
Platform

-----
-----
node1      /cdp
          e0a    cs1  (b8:ce:f6:19:1b:42)    Ethernet1/1/1  N9K-
C9336C-FX2
          e0b    cs2  (b8:ce:f6:19:1b:96)    Ethernet1/1/2  N9K-
C9336C-FX2

node2      /cdp
          e0a    cs1  (b8:ce:f6:19:1b:42)    Ethernet1/1/1  N9K-
C9336C-FX2
          e0b    cs2  (b8:ce:f6:19:1b:96)    Ethernet1/1/2  N9K-
C9336C-FX2
```

## Schritt 3: Überprüfen Sie die Konfiguration

1. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

2. Vergewissern Sie sich, dass alle Cluster-Netzwerk-LIFs wieder an ihren Home-Ports sind:

```
network interface show
```

## 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
e3a      true
      node1_clus2  up/up      169.254.49.125/16  node1
e3b      true
      node2_clus1  up/up      169.254.47.194/16  node2
e3a      true
      node2_clus2  up/up      169.254.19.183/16  node2
e3b      true
```

3. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

4. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

### Was kommt als Nächstes?

Nachdem Sie Ihre Switches migriert haben, ["Konfigurieren der Switch-Integritätsüberwachung"](#) .

## Migrieren Sie von älteren Cisco -Switches zu Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches

Sie können eine unterbrechungsfreie Migration von älteren Cisco -Cluster-Switches zu Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Cluster-Netzwerk-Switches durchführen.

### Prüfen Sie die Anforderungen

Stellen Sie sicher, dass:

- Sie haben die Seriennummer des Switches überprüft, um sicherzustellen, dass der richtige Switch migriert wird.
- Einige der Ports auf Nexus 9336C-FX2-Switches sind für 10-GbE- oder 40-GbE-Betrieb konfiguriert.
- Die 10GbE- und 40-GbE-Konnektivität von den Nodes zu Nexus 9336C-FX2 Cluster-Switches wurde

geplant, migriert und dokumentiert.

- Das Cluster funktioniert voll (es sollten keine Fehler in den Protokollen oder ähnlichen Problemen geben).
- Die anfängliche Anpassung der Cisco Nexus 9336C-FX2 Switches lautet folgendermaßen:
  - 9336C-FX2-Switches führen die neueste empfohlene Version der Software aus.
  - Vergewissern Sie sich, dass die Referenzkonfigurationsdateien (RCFs, Reference Configuration Files) vollständig auf neue Switches angewendet wurden, bevor Sie die LIFs auf die neuen Switches migrieren.
  - Überprüfen Sie die laufenden und Startkonfigurationen auf beiden Switches, bevor Sie den Netzwerkverkehr verschieben.
  - Anpassung von Websites, z. B. DNS, NTP, SMTP, SNMP, Und SSH werden auf den neuen Switches konfiguriert.
- Sie haben Zugriff auf die Switch-Kompatibilitätstabelle auf der "[Cisco Ethernet-Switches](#)" Seite für die unterstützten ONTAP-, NX-OS- und RCF-Versionen.
- Sie haben die entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website für die Upgrade- und Downgrade-Verfahren von Cisco Switches unter geprüft "[Switches Der Cisco Nexus 9000-Serie Unterstützen](#)" Seite.

 Wenn Sie die Portgeschwindigkeit der e0a- und e1a-Cluster-Ports auf AFF A800- oder AFF C800-Systemen ändern, können Sie beobachten, wie fehlerhafte Pakete nach der Geschwindigkeitskonvertierung empfangen werden. Siehe "[Bug 1570339](#)" Und den Knowledge Base Artikel "[CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE](#)" Für eine Anleitung.

## Migrieren Sie die Switches

### Zu den Beispielen

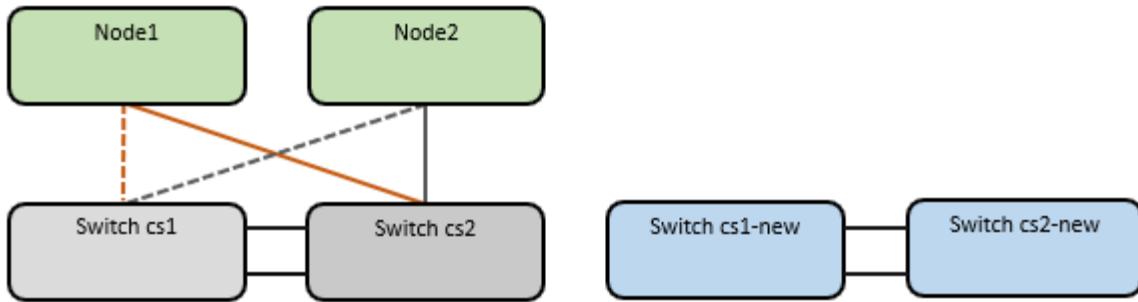
Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster Interconnect-Ports e0a und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.

 Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden vorhandenen Cisco Switches sind **cs1** und **cs2**
- Die neuen Nexus 9336C-FX2 Cluster Switches sind **cs1-neu** und **cs2-neu**.
- Die Knotennamen sind **node1** und **node2**.
- Die Cluster-LIF-Namen sind **node1\_clus1** und **node1\_clus2** für Knoten 1, und **node2\_clus1** und **node2\_clus2** für Knoten 2.
- Die Eingabeaufforderung **cluster1::>\*** gibt den Namen des Clusters an.

Beachten Sie während dieses Verfahrens das folgende Beispiel:



## Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP-Befehlen und "[Switches Der Nexus 9000 Serie](#)" Befehle; ONTAP-Befehle werden verwendet, sofern nicht anders angegeben.

Dieses Verfahren umfasst das folgende Szenario:

- Schalter cs2 wird zuerst durch Schalter cs2-New ersetzt.
  - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
    - Alle Cluster-LIFs führen ein Failover auf den neuen Switch cs2-New durch.
  - Die Verkabelung zwischen den Knoten und cs2 wird dann von cs2 getrennt und wieder mit cs2-New verbunden.
- Switch cs1 wird durch Switch cs1-New ersetzt.
  - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
    - Alle Cluster-LIFs führen ein Failover auf den neuen Switch cs1-New durch.
  - Die Verkabelung zwischen den Knoten und cs1 wird dann von cs1 getrennt und wieder mit cs1-New verbunden.

**i** Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Cluster-Betrieb zu gewährleisten, führt das folgende Verfahren ein Failover aller Cluster-LIFs auf den Partner-Switch des Betriebs durch, während die Schritte auf dem Ziel-Switch ausgeführt werden.

## Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=xh`

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (**\*>**) wird angezeigt.

#### **Schritt: Ports und Verkabelung konfigurieren**

1. Vergewissern Sie sich bei den neuen Switches, dass die ISL zwischen den Switches cs1-New und cs2-New verkabelt und ordnungsgemäß funktioniert:

```
show port-channel summary
```

## Beispiel anzeigen

```
cs1-new# 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      Eth1/35 (P)  Eth1/36 (P)

cs2-new# 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      Eth1/35 (P)  Eth1/36 (P)
```

2. Anzeigen der Cluster-Ports an jedem Node, der mit den vorhandenen Cluster-Switches verbunden ist:

```
network device-discovery show
```

## 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      N5K-
C5596UP
           e0b    cs2
                           Ethernet1/2      N5K-
C5596UP
node2      /cdp
           e0a    cs1
                           Ethernet1/1      N5K-
C5596UP
           e0b    cs2
                           Ethernet1/2      N5K-
C5596UP
```

3. Legen Sie den Administrations- oder Betriebsstatus für jeden Cluster-Port fest.

a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

## 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
```

b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) auf ihren Home-Ports befinden:

```
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      169.254.209.69/16  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
```

c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

```
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    N5K-
C5596UP
    Serial Number: FOXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
    9.3 (4)
    Version Source: CDP

cs2            cluster-network 10.233.205.93    N5K-
C5596UP
    Serial Number: FOXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
    9.3 (4)
    Version Source: CDP
```

#### 4. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs.

Wenn Sie die automatische Zurücksetzung für dieses Verfahren deaktivieren, werden die Cluster-LIFs nicht automatisch zurück zu ihrem Home Port verschoben. Sie verbleiben im aktuellen Port, während er weiterhin betriebsbereit ist.

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



Durch die Deaktivierung der automatischen Zurücksetzung wird sichergestellt, dass ONTAP nur ein Failover der Cluster-LIFs übernimmt, wenn die Switch-Ports später heruntergefahren werden.

#### 5. Fahren Sie auf Cluster-Switch cs2 die Ports herunter, die mit den Cluster-Ports von **all** Nodes verbunden sind, um ein Failover der Cluster-LIFs zu ermöglichen:

```
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

6. Vergewissern Sie sich, dass für die Cluster-LIFs ein Failover zu den auf Cluster-Switch cs1 gehosteten Ports 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
      node1_clus1      up/up      169.254.3.4/16      node1
e0a        true
      node1_clus2      up/up      169.254.3.5/16      node1
e0a        false
      node2_clus1      up/up      169.254.3.8/16      node2
e0a        true
      node2_clus2      up/up      169.254.3.9/16      node2
e0a        false
```

7. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

**Beispiel anzeigen**

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

8. Wenn die Cluster-LIFs ein Failover für den Switch cs1 durchgeführt haben und der Cluster sich in [Schritt 10](#) einem ordnungsgemäßen Zustand befindet, fahren Sie mit fort. Wenn einige Cluster-LIFs nicht ordnungsgemäß arbeiten oder das Cluster nicht funktionsfähig ist, können Sie wie folgt ein Rollback der Konnektivität zum Switch cs2 durchführen:

a. Die mit den Cluster-Ports von **all** verbundenen Ports aufrufen die Knoten:

```
cs2# configure
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# no shutdown
cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

b. Vergewissern Sie sich, dass für die Cluster-LIFs ein Failover zu den auf Cluster-Switch cs1 gehosteten Ports 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
      node1_clus1    up/up      169.254.3.4/16    node1
      e0a      true
      node1_clus2    up/up      169.254.3.5/16    node1
      e0a      false
      node2_clus1    up/up      169.254.3.8/16    node2
      e0a      true
      node2_clus2    up/up      169.254.3.9/16    node2
      e0a      false
```

c. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

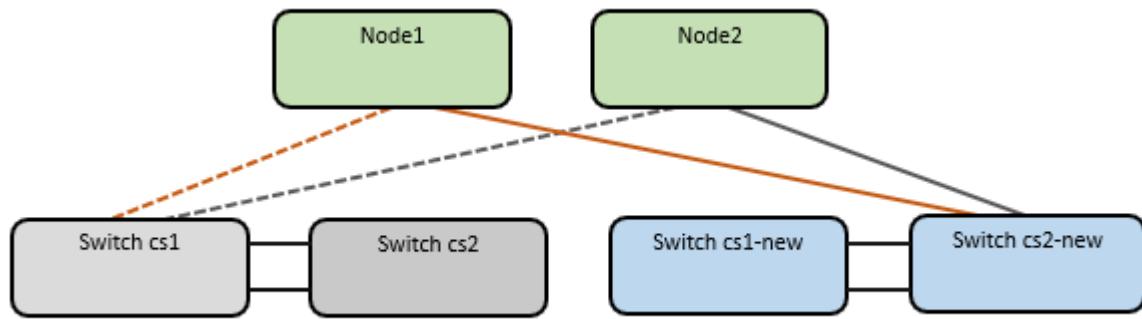
```
cluster show
```

## Beispiel anzeigen

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

9. Sobald Sie die LIF und den Clusterzustand wiederhergestellt haben, starten Sie den Prozess von [neuSchritt 4](#).
10. Verschieben Sie alle Clusterknoten-Verbindungskabel vom alten cs2-Switch auf den neuen cs2-New-Switch.

**Clusterknoten-Verbindungskabel wurden auf den cs2-New Switch verlegt**



11. Überprüfen Sie den Zustand der zu cs2-New übergewechselt Netzwerkverbindungen:

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

## Beispiel anzeigen

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

Node: node1

Ignore

Health                                         Speed (Mbps)  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

Health                                         Speed (Mbps)  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
```

Alle verschieben Cluster-Ports sollten nach oben erfolgen.

12. Überprüfen Sie die „Neighbor“-Informationen auf den Cluster-Ports:

```
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
-----  -----  -----
-----  -----
node1      /cdp
          e0a    cs1
          e0b    cs2-new
C5596UP
          e0a    cs1
          e0b    cs2-new
C9336C-FX2
          /cdp
          e0a    cs1
          e0b    cs2-new
C5596UP
          e0a    cs1
          e0b    cs2-new
C9336C-FX2
```

Vergewissern Sie sich, dass der cs2-neue Switch von den verschobenen Cluster-Ports als „Nachbarn“ angezeigt wird.

13. Bestätigen Sie die Switch-Port-Verbindungen aus der Perspektive von Switch cs2-New:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

14. Fahren Sie auf Cluster-Switch cs1 die Ports herunter, die mit den Cluster-Ports von **all** Nodes verbunden sind, um ein Failover der Cluster-LIFs durchzuführen.

```
cs1# configure
cs1(config)# interface eth1/1-1/2
cs1(config-if-range)# shutdown
cs1(config-if-range)# exit
cs1(config)# exit
cs1#
```

Alle Cluster-LIFs führen einen Failover zum cs2-neuen Switch durch.

15. Überprüfen Sie, ob für die Cluster-LIFs ein Failover zu den auf Switch cs2-New gehosteten Ports 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      Interfac Admin/Oper Address/Mask      Node
Port      Home
-----
----- Cluster
      node1_clus1  up/up      169.254.3.4/16      node1
e0b      false
      node1_clus2  up/up      169.254.3.5/16      node1
e0b      true
      node2_clus1  up/up      169.254.3.8/16      node2
e0b      false
      node2_clus2  up/up      169.254.3.9/16      node2
e0b      true
```

16. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

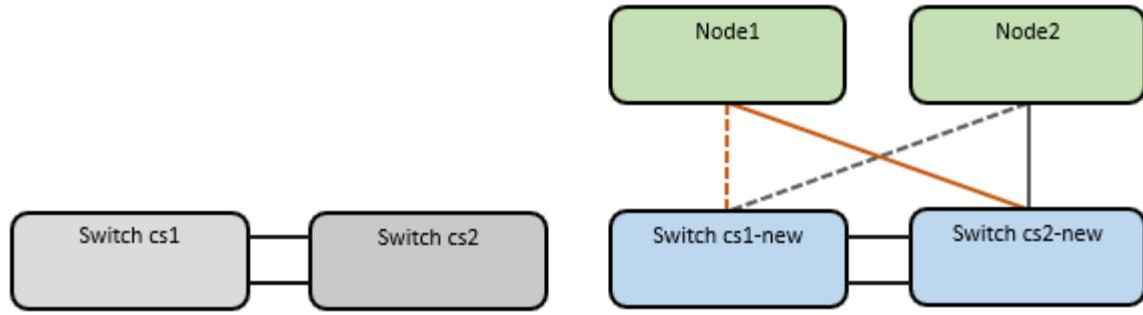
```
cluster show
```

### Beispiel anzeigen

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

17. Verschieben Sie die Verbindungskabel des Clusterknoten von cs1 zum neuen cs1-New-Switch.

**Clusterknoten-Verbindungskabel wurden auf den cs1-New Switch verlegt**



18. Überprüfen Sie den Zustand der zu cs1-New übergewechselt Netzwerkverbindungen:

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

**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

```

Alle verschiebten Cluster-Ports sollten nach oben erfolgen.

19. Überprüfen Sie die „Neighbor“-Informationen auf den Cluster-Ports:

```
network device-discovery show
```

#### Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface
Platform

-----
-----
node1      /cdp
           e0a    cs1-new
C9336C-FX2
           e0b    cs2-new
C9336C-FX2

node2      /cdp
           e0a    cs1-new
C9336C-FX2
           e0b    cs2-new
C9336C-FX2
```

Vergewissern Sie sich, dass die verschiebten Cluster-Ports den cs1-neuen Switch als Nachbarn sehen.

20. Bestätigen Sie die Switch-Port-Verbindungen aus der Perspektive von Switch cs1-New:

```
cs1-new# show interface brief
cs1-new# show cdp neighbors
```

21. Vergewissern Sie sich, dass die ISL zwischen cs1-New und cs2-New weiterhin betriebsbereit ist:

```
show port-channel summary
```

## Beispiel anzeigen

```
cs1-new# 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      Eth1/35 (P)  Eth1/36 (P)

cs2-new# 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      Eth1/35 (P)  Eth1/36 (P)
```

## Schritt 3: Überprüfen Sie die Konfiguration

1. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

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

2. Überprüfen Sie, ob die Cluster-LIFs auf ihre Home-Ports zurückgesetzt wurden (dies kann eine Minute dauern):

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

Wenn die Cluster-LIFs nicht auf ihren Home-Port zurückgesetzt wurden, setzen Sie sie manuell zurück:

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

3. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

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

```

cluster1::*> cluster ping-cluster -node node2
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. Wenn Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie erneut, indem Sie eine AutoSupport-Meldung aufrufen: system node autosupport invoke -node \* -type all -message MAINT=END

#### Was kommt als Nächstes?

Nachdem Sie die Switches migriert haben, ["Konfigurieren der Switch-Integritätsüberwachung"](#) .

## Migration auf Cluster mit zwei Nodes

Wenn Sie über eine vorhandene Clusterumgebung mit zwei Knoten und ohne Switch verfügen, können Sie mithilfe der Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T zu einer Clusterumgebung mit zwei Knoten und Switch migrieren.

Der Migrationsprozess funktioniert bei allen Knoten mit optischen oder Twinax-Ports, wird von diesem Switch jedoch nicht unterstützt, wenn die Nodes integrierte 10 GB BASE-T RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

#### Prüfen Sie die Anforderungen

##### Was Sie benötigen

- Bei der Konfiguration mit zwei Nodes ohne Switches:

- Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
- Alle Cluster-Ports haben den Status **up**.
- Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren Home-Ports.
- Siehe "[Hardware Universe](#)" Für alle unterstützten ONTAP-Versionen.
- Für die Switch-Konfiguration des Cisco Nexus 9336C-FX2:
  - Beide Switches verfügen über Management-Netzwerk-Konnektivität.
  - Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
  - Bei den Nexus 9336C-FX2 Nodes-zu-Node-Switches und Switch-zu-Switch-Verbindungen werden Twinax- oder Glasfaserkabel verwendet.
- Siehe "[Hardware Universe](#)" Weitere Informationen zur Verkabelung.
- Inter-Switch Link (ISL)-Kabel werden an den Anschlüssen 1/35 und 1/36 an beiden 9336C-FX2-Switches angeschlossen.
- Die anfängliche Anpassung der beiden 9336C-FX2-Switches erfolgt so, dass:
  - 9336C-FX2-Switches führen die neueste Version der Software aus.
  - Auf die Switches werden Referenzkonfigurationsdateien (RCFs) angewendet. Bei den neuen Switches werden alle Site-Anpassungen wie SMTP, SNMP und SSH konfiguriert.

## Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der Schalter 9336C-FX2 lauten cs1 und cs2.
- Die Namen der Cluster SVMs sind node1 und node2.
- Die Namen der LIFs sind node1\_clug1 und node1\_clus2 auf Knoten 1, und node2\_clus1 bzw. node2\_clus2 auf Knoten 2.
- Der `cluster1::*` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e0a und e0b.

Siehe "[Hardware Universe](#)" Weitere Informationen zu den Cluster-Ports für Ihre Plattformen.

## Migrieren Sie die Switches

### Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y` Wenn Sie dazu aufgefordert

werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung ('\*>' erscheint.

#### Schritt: Ports und Verkabelung konfigurieren

1. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches cs1 und cs2.

Deaktivieren Sie die ISL-Ports nicht.

#### Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 34 auf Switch cs1 deaktiviert sind:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# shutdown
```

2. Stellen Sie sicher, dass ISL und die physischen Ports auf der ISL zwischen den beiden 9336C-FX2-Switches cs1 und cs2 über die Ports 1/35 und 1/36 verfügen:

```
show port-channel summary
```

## Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports auf 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      Eth1/35 (P)  Eth1/36 (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      Eth1/35 (P)  Eth1/36 (P)
```

3. Liste der benachbarten Geräte anzeigen:

```
show cdp neighbors
```

Dieser Befehl enthält Informationen zu den Geräten, die mit dem System verbunden sind.

### Beispiel anzeigen

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs1 aufgeführt:

```
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
cs2           Eth1/35      175      R S I s      N9K-C9336C
Eth1/35
cs2           Eth1/36      175      R S I s      N9K-C9336C
Eth1/36

Total entries displayed: 2
```

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs2 aufgeführt:

```
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      Local Intrfce  Hldtme Capability  Platform
Port ID
cs1           Eth1/35      177      R S I s      N9K-C9336C
Eth1/35
cs1           Eth1/36      177      R S I s      N9K-C9336C
Eth1/36

Total entries displayed: 2
```

4. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

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

Jeder Port sollte für angezeigt werden Link Und gesund für Health Status.

**Beispiel anzeigen**

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

Node: node1

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

4 entries were displayed.

5. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

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

Jede Cluster-LIF sollte angezeigt werden true Für Is Home Und ich habe ein Status Admin/Oper Von up/Up.

### 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. Vergewissern Sie sich, dass die automatische Umrüstung 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

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

4 entries were displayed.
```

7. Trennen Sie das Kabel vom Cluster-Port e0a auf node1, und verbinden Sie dann e0a mit Port 1 am Cluster Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von den 9336C-FX2-Switches

unterstützt wird.

Der "[Hardware Universe – Switches](#)" Enthält weitere Informationen zur Verkabelung.

#### ["Hardware Universe – Switches"](#)

8. Trennen Sie das Kabel vom Cluster Port e0a auf node2, und verbinden Sie dann e0a mit Port 2 am Cluster Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von den 9336C-FX2 Switches unterstützt wird.
9. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs1.

#### **Beispiel anzeigen**

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/34 auf Switch cs1 aktiviert sind:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs1(config-if-range)# no shutdown
```

10. Vergewissern Sie sich, dass alle Cluster-LIFs aktiv und betriebsbereit sind und als angezeigt werden `true` Für Is Home:

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

### Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs sich auf node1 und node2 befinden und dass Is Home Die Ergebnisse sind wahr:

```
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 zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

### Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

```
cluster1::*> cluster show

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

2 entries were displayed.
```

### 12. Trennen Sie das Kabel von Cluster-Port e0b auf node1, und verbinden Sie dann e0b mit Port 1 am Cluster

Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den 9336C-FX2 Switches unterstützt wird.

13. Trennen Sie das Kabel von Cluster-Port e0b auf node2, und verbinden Sie dann e0b mit Port 2 am Cluster Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den 9336C-FX2 Switches unterstützt wird.
14. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs2.

#### **Beispiel anzeigen**

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/34 auf Switch cs2 aktiviert sind:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1/1-4, e1/2/1-4, e1/3/1-4, e1/4/1-4,
e1/5/1-4, e1/6/1-4, e1/7-34
cs2(config-if-range) # no shutdown
```

15. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

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

## Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

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

Node: node1

Ignore

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

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.
```

## Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass alle Schnittstellen für „true“ anzeigen Is Home:

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



Dies kann einige Minuten dauern.

## Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf node1 und node2 liegen und dass Is Home Die Ergebnisse sind wahr:

```
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.
```

2. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
show cdp neighbors
```

## Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
(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       133      H             FAS2980
e0a
node2              Eth1/2       133      H             FAS2980
e0a
cs2                Eth1/35      175      R S I s      N9K-C9336C
Eth1/35
cs2                Eth1/36      175      R S I s      N9K-C9336C
Eth1/36

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          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1       133      H             FAS2980
e0b
node2              Eth1/2       133      H             FAS2980
e0b
cs1                Eth1/35      175      R S I s      N9K-C9336C
Eth1/35
cs1                Eth1/36      175      R S I s      N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Zeigen Sie Informationen zu den erkannten Netzwerkgeräten im Cluster an:

```
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-
C9336C
          e0b    cs2          0/2          N9K-
C9336C
node1      /cdp
          e0a    cs1          0/1          N9K-
C9336C
          e0b    cs2          0/1          N9K-
C9336C

4 entries were displayed.
```

4. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

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



Es kann einige Minuten dauern, bis der Befehl abgeschlossen ist. Warten Sie, bis die Ankündigung „3 Minuten Lebensdauer abläuft“ abläuft.

**Beispiel anzeigen**

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

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

5. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

## Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

```
cluster1::*> cluster show

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

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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. Ändern Sie die Berechtigungsebene zurück zu admin:

```
set -privilege admin
```

2. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

#### Was kommt als Nächstes?

Nachdem Sie Ihre Switches migriert haben, ["Konfigurieren der Switch-Integritätsüberwachung"](#).

## Ersetzen Sie die Schalter

### Ersetzen Sie die Cluster-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T

Befolgen Sie diese Schritte, um defekte Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem Clusternetzwerk zu ersetzen. Dies ist ein unterbrechungsfreies Verfahren (NDU).

## Prüfen Sie die Anforderungen

Stellen Sie vor dem Austausch des Switches Folgendes sicher:

- Sie haben die Seriennummer des Switches überprüft, um sicherzustellen, dass der richtige Schalter ausgetauscht wird.
- In dem vorhandenen Cluster und der Netzwerkinfrastruktur:
  - Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
  - Alle Cluster-Ports sind **up**.
  - Alle logischen Cluster-Schnittstellen (LIFs) sind **up** und auf ihren Home-Ports.
  - Das `ONTAP cluster ping-cluster -node node1` Der Befehl muss angeben, dass grundlegende und größere Verbindungen als die PMTU-Kommunikation auf allen Pfaden erfolgreich sind.
- Auf dem Nexus 9336C-FX2-Ersatzschalter:
  - Das Management-Netzwerk-Konnektivität auf dem Ersatz-Switch ist funktionsfähig.
  - Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
  - Die Node-Verbindungen sind Ports 1/1 bis 1/34.
  - Alle Inter-Switch Link (ISL)-Ports sind an den Ports 1/35 und 1/36 deaktiviert.
  - Die gewünschte Referenzkonfigurationsdatei (RCF) und den NX-OS-Bildschalter werden auf den Switch geladen.
  - Die Erstanpassung des Schalters ist abgeschlossen, wie in beschrieben "[Konfigurieren Sie den Cluster-Switch 9336C-FX2](#)".

Alle zuvor erstellten Site-Anpassungen wie STP, SNMP und SSH werden auf den neuen Switch kopiert.

- Sie haben den Befehl zum Migrieren einer Cluster-LIF von dem Node ausgeführt, auf dem die Cluster-LIF gehostet wird.

## Aktivieren Sie die Konsolenprotokollierung

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

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs-AutoSupport aus, um die Case-Erstellung für die Dauer der Wartung zu deaktivieren. Lesen Sie diesen Knowledge Base-Artikel "["SU92: Unterdrücken der automatischen Case-Erstellung während geplanter Wartungsfenster"](#)" Entnehmen.
- Aktivieren Sie die Sitzungsprotokollierung für beliebige CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Knowledge Base Artikel "["So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen"](#)".

## Tauschen Sie den Schalter aus

### Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der vorhandenen Nexus 9336C-FX2 Switches lauten cs1 und cs2.
- Der Name des neuen Nexus 9336C-FX2 Switch lautet newc2.
- Die Node-Namen sind node1 und node2.
- Die Cluster-Ports auf jedem Node lauten e0a und e0b.
- Die Cluster-LIF-Namen sind node1\_clug1 und node1\_clus2 für node1, und node2\_clus1 und node2\_clus2 für node2.
- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet cluster1:>

### Über diese Aufgabe

Die folgende Vorgehensweise basiert auf der folgenden Cluster-Netzwerktopologie:

## 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/      Local   Discovered
Protocol   Port    Device (LLDP: ChassisID)  Interface      Platform
-----  -----  -----
-----  -----
node2      /cdp
          e0a    cs1
          e0b    cs2
node1      /cdp
          e0a    cs1
          e0b    cs2
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 Infrfce	Hldtme	Capability	Platform	Port
ID					
node1	Eth1/1	144	H	FAS2980	e0a
node2	Eth1/2	145	H	FAS2980	e0a
cs2	Eth1/35	176	R S I s	N9K-C9336C	
Eth1/35					
cs2 (FDO220329V5)	Eth1/36	176	R S I s	N9K-C9336C	
Eth1/36					

```
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	Local Intrfce	Hldtme	Capability	Platform	Port
ID					
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1	Eth1/35	178	R S I s	N9K-C9336C	
Eth1/35					
cs1	Eth1/36	178	R S I s	N9K-C9336C	
Eth1/36					

Total entries displayed: 4

#### Schritt 1: Vorbereitung auf den Austausch

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Installieren Sie das entsprechende RCF und Image auf dem Switch, newcs2, und nehmen Sie die erforderlichen Standortvorbereitungen vor.

Überprüfen, 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 für die RCF- und NX-OS-Software benötigen, fahren Sie mit Schritt 2 fort.

- a. Wechseln Sie auf der NetApp Support Site zur Referenzkonfigurationsdatei [Seite](#) der Referenzkonfiguration für NetApp Cluster und Management-Netzwerk-Switches.
- b. Klicken Sie auf den Link für die Kompatibilitätsmatrix *Cluster Network and Management Network*, und notieren Sie anschließend die erforderliche Switch-Softwareversion.
- c. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Seite Beschreibung zurückzukehren, klicken Sie auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung, und gehen Sie dann zur Download-Seite.
- d. Befolgen Sie die Schritte auf der Download-Seite, um die korrekten RCF- und NX-OS-Dateien für die Version der installierten ONTAP-Software herunterzuladen.

3. Bei dem neuen Switch melden Sie sich als Administrator an und fahren Sie alle Ports ab, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports 1/1 zu 1/34).

Wenn der Schalter, den Sie ersetzen, nicht funktionsfähig ist und ausgeschaltet ist, fahren Sie mit Schritt 4 fort. Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt haben.

#### Beispiel anzeigen

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-34
newcs2(config-if-range)# shutdown
```

4. Vergewissern Sie sich, dass für alle Cluster-LIFs die automatische Zurücksetzung aktiviert ist:

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

#### Beispiel anzeigen

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

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

4 entries were displayed.
```

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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: Kabel und Ports konfigurieren

1. Fahren Sie die ISL-Ports 1/35 und 1/36 auf dem Nexus 9336C-FX2 Switch cs1 herunter.

#### Beispiel anzeigen

```

cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/35-36
cs1(config-if-range)# shutdown
cs1(config-if-range)#

```

2. Entfernen Sie alle Kabel vom Nexus 9336C-FX2 cs2 Switch, und verbinden Sie sie dann mit den gleichen Ports am Nexus C9336C-FX2 newc2 Switch.
3. Bringen Sie die ISLs-Ports 1/35 und 1/36 zwischen den switches cs1 und newcs2 auf, und überprüfen Sie dann den Betriebsstatus des Port-Kanals.

Port-Channel sollte PO1(SU) angeben und Mitgliedsports sollten eth1/35(P) und eth1/36(P) angeben.

## Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/35 und 1/36 und zeigt die Zusammenfassung des Port-Kanals am Switch cs1 an:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/35-36
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      Eth1/35 (P)  Eth1/36 (P)

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

4. Vergewissern Sie sich, dass Port e0b auf allen Nodes aktiviert ist:

```
network port show ipspace Cluster
```

## Beispiel anzeigen

Die Ausgabe sollte wie folgt aussehen:

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

Node: node1

Ignore

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

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. Setzen Sie auf demselben Node, den Sie im vorherigen Schritt verwendet haben, die Cluster-LIF, die dem Port im vorherigen Schritt zugeordnet ist, mithilfe des Befehls „Netzwerkschnittstelle revert“ zurück.

## Beispiel anzeigen

In diesem Beispiel wird LIF node1\_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert für „Home“ wahr ist und der Port e0b ist.

Die folgenden Befehle geben LIF zurück node1\_clus2 Ein node1 Zu Home Port e0a Und zeigt Informationen zu den LIFs auf beiden Nodes an. Das Einrichten des ersten Node ist erfolgreich, wenn die Spalte IS Home für beide Clusterschnittstellen wahr ist und in diesem Beispiel die korrekten Port-Zuweisungen angezeigt werden e0a Und e0b Auf Knoten 1.

```
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. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

## Beispiel anzeigen

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

```
cluster1::*> cluster show

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

7. Vergewissern Sie sich, dass alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

## 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.
```

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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 3: Überprüfen Sie die Konfiguration

1. Bestätigen Sie die folgende Clusternetzwerkkonfiguration:

```
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	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp e0a	cs1	0/2	N9K-
C9336C	e0b	newcs2	0/2	N9K-
C9336C				
node1	/cdp e0a	cs1	0/1	N9K-
C9336C	e0b	newcs2	0/1	N9K-
C9336C				

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 e0a	Eth1/1	144	H	FAS2980
node2 e0a	Eth1/2	145	H	FAS2980
newcs2 Eth1/35	Eth1/35	176	R S I s	N9K-C9336C
newcs2	Eth1/36	176	R S I s	N9K-C9336C

```
Eth1/36
```

```
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 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C

```
Total entries displayed: 4
```

2. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

#### Was kommt als Nächstes?

Nachdem Sie Ihre Schalter ausgetauscht haben, ["Konfigurieren der Switch-Integritätsüberwachung"](#).

### Ersetzen Sie Cisco Nexus 9336C-FX2 und 9336C-FX2-T Cluster-Switches durch Switchless-Verbindungen

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

#### Prüfen Sie die Anforderungen

##### Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports,

jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.

- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

## **Bevor Sie beginnen**

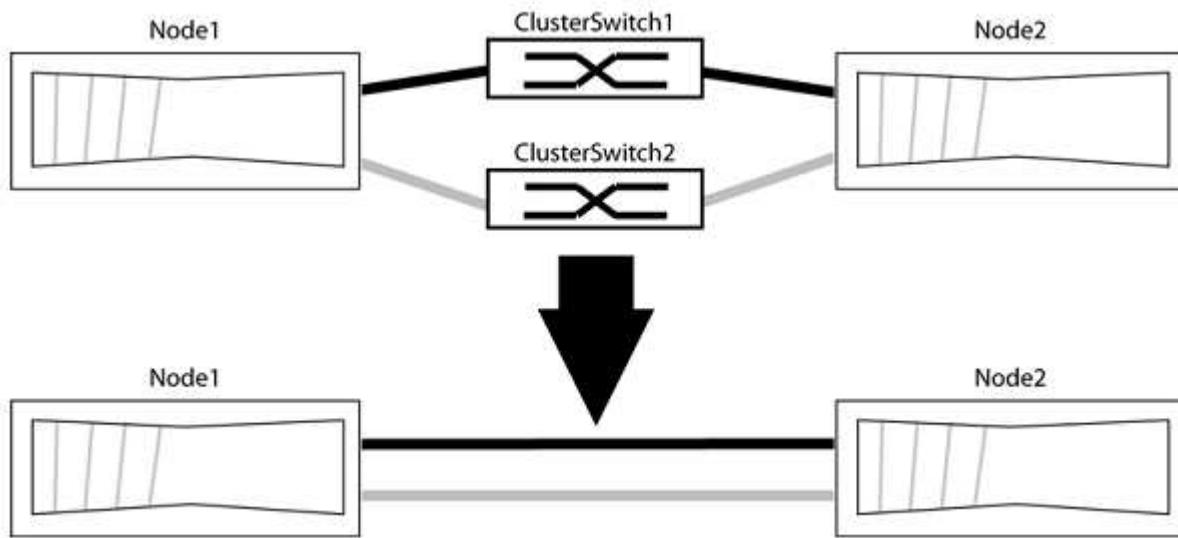
Stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

## **Migrieren Sie die Switches**

### **Über diese Aufgabe**

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



### **Zu den Beispielen**

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

#### **Schritt: Bereiten Sie sich auf die Migration vor**

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben y Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung \* > Angezeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

#### Beispiel anzeigen

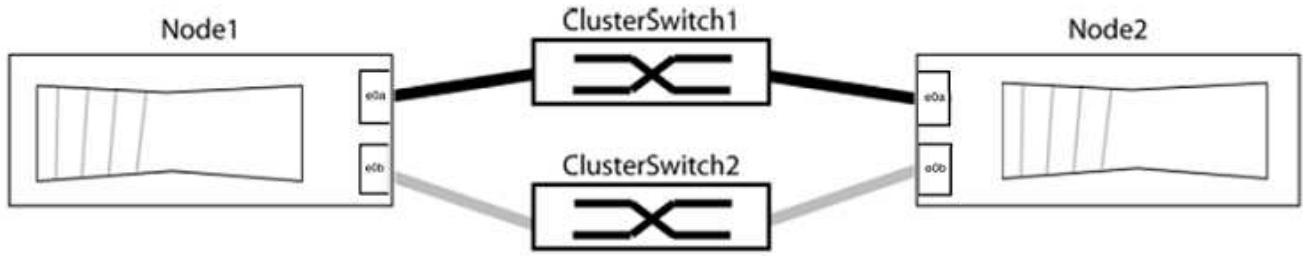
```
cluster::>*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

### Schritt: Ports und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in `grop1` zu Cluster-Switch 1 wechseln und die Cluster-Ports in `grop2` zu Cluster-Switch 2 wechseln. Diese Gruppen sind später im Verfahren erforderlich.
2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



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

### 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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird true Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

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

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

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

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

## Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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
          e0b    cs2
node2/cdp
          e0a    cs1
          e0b    cs2
4 entries were displayed.
```

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

## ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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. Überprüfen Sie, ob das Cluster ordnungsgemäß ist:

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

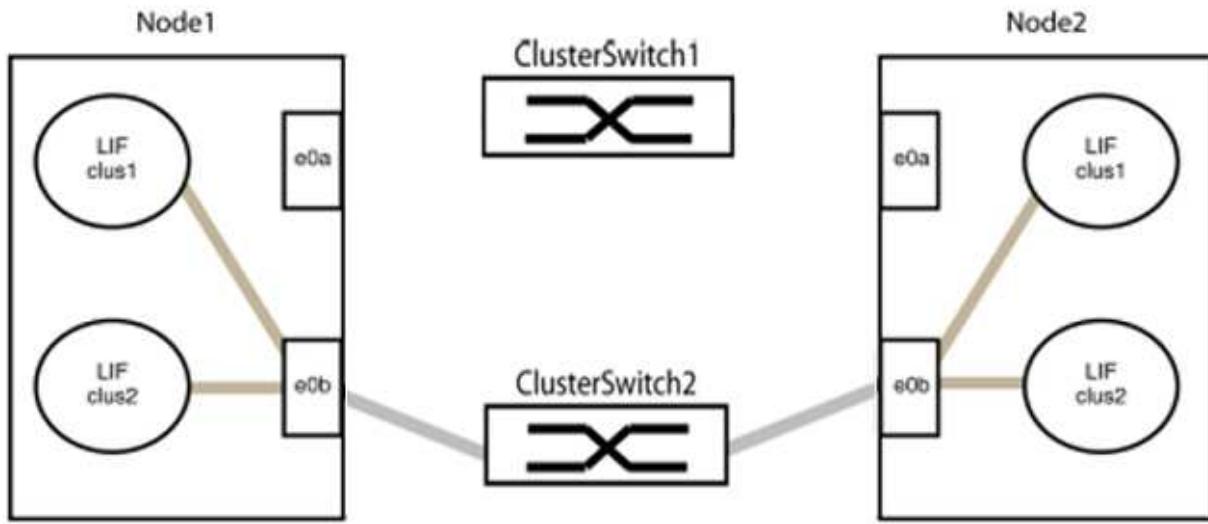
2. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

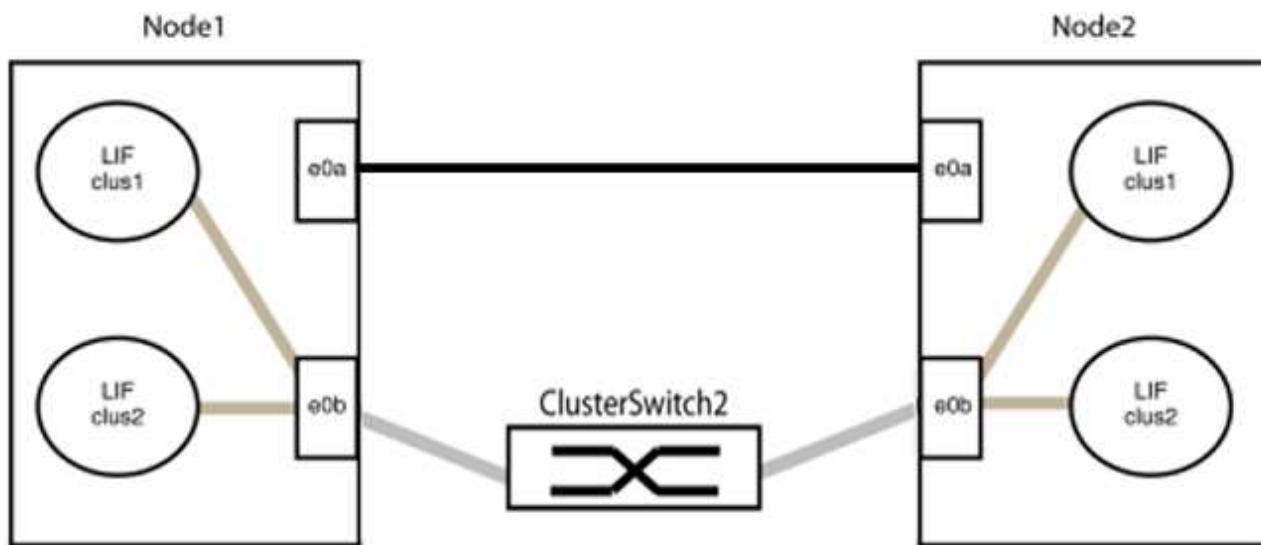
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Grupp1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



3. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

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

Das folgende Beispiel zeigt, dass das Cluster ohne Switches 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 das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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 für Gruppe 1 zu bestätigen.

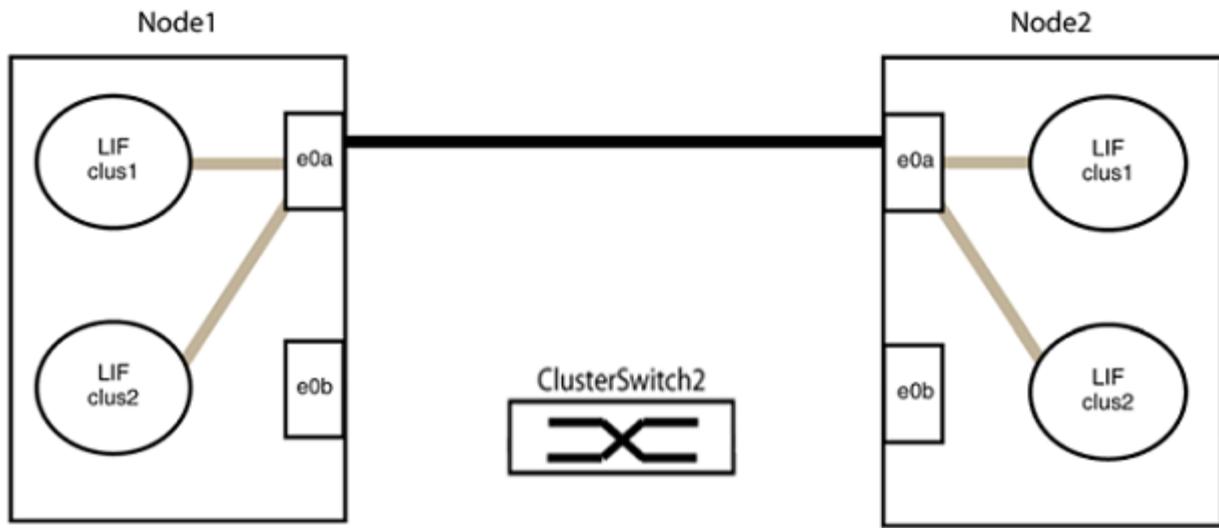
1. richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

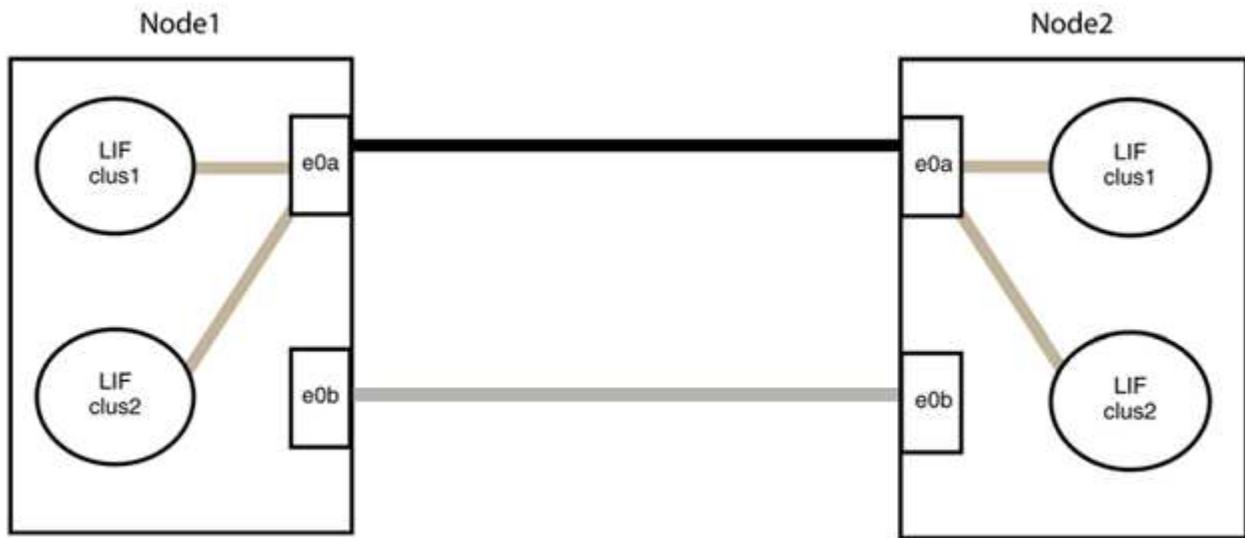
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



### Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

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

## Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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
      e0b    node2
node1/lldp
      e0a    node2 (00:a0:98:da:16:44)  e0a
      e0b    node2 (00:a0:98:da:16:44)  e0b
node2/cdp
      e0a    node1
      e0b    node1
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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

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

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

```
network interface show -vserver Cluster -lif lif_name
```

## Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

## Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `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 das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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

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

```
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. Wenn Sie die automatische Fällerstellung unterdrückt haben, aktivieren Sie sie erneut, indem Sie eine AutoSupport-Meldung aufrufen:

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

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

2. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

## Copyright-Informationen

Copyright © 2025 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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

## Markeninformationen

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