



## Konfigurieren der Software

Install and maintain

NetApp  
November 07, 2025

# Inhalt

Konfigurieren der Software .....	1
Workflow zur Softwareinstallation für die Speicherswitches Cisco Nexus 9336C-FX2 und 9336C-FX2-T .....	1
Konfigurieren der Speicher-Switches 9336C-FX2 und 9336C-FX2-T .....	1
Bereiten Sie die Installation oder das Upgrade von NX-OS-Software und RCF vor .....	4
Installieren oder aktualisieren Sie die NX-OS-Software .....	10
Prüfen Sie die Anforderungen .....	10
Installieren Sie die Software .....	11
Überprüfen Sie Ihre SSH-Konfiguration .....	31
Installieren oder aktualisieren Sie die Übersicht über die Referenzkonfigurationsdatei (RCF) .....	34
Installieren Sie die Referenzkonfigurationsdatei .....	35
Aktualisieren der Referenzkonfigurationsdatei (RCF) .....	46
Setzen Sie die Speicher-Switches 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurück .....	55

# Konfigurieren der Software

## Workflow zur Softwareinstallation für die Speicherswitches Cisco Nexus 9336C-FX2 und 9336C-FX2-T

Gehen Sie folgendermaßen vor, um Software für die Speicher-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T zu installieren und zu konfigurieren:

1

### "Konfigurieren Sie den Switch"

Konfigurieren Sie die Speicher-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-Speicher-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 Cisco 9336C-FX2- und 9336C-FX2-T-Speicher-Switches.

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 Speicherschalter 9336C-FX2 und 9336C-FX2-T.

## Konfigurieren der Speicher-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-Dokumentation Siehe "[Erforderliche Dokumentation](#)" Finden Sie weitere Informationen.

## 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.	Der Switch-Name ist auf 63 alphanumerische Zeichen begrenzt.

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

## Bereiten Sie die Installation oder das Upgrade von NX-OS-Software und RCF vor

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

#### 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\_clusions1 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 lldp
```

#### Beispiel anzeigen

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

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

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

Ignore                                         Speed (Mbps)
Health   Health
Port      IPspace        Broadcast Domain Link MTU Admin/Oper
Status   Status
-----  -----
-----  -----
e0a      Cluster        Cluster          up    9000  auto/100000
healthy false
e0b      Cluster        Cluster          up    9000  auto/100000
healthy false

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
e0b      Cluster        Cluster          up    9000  auto/100000
healthy false

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 `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzuzeigen:

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

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

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

```
cluster1::*: network interface check cluster-connectivity show
Source          Destination
Packet
Node    Date           LIF           LIF
Loss
-----
-----
node1
      3/5/2024 19:21:18 -06:00   cluster1-01_clus2   cluster1-02-
clus1  none
      3/5/2024 19:21:20 -06:00   cluster1-01_clus2   cluster1-
02_clus2  none
node2
      3/5/2024 19:21:18 -06:00   cluster1-02_clus2   cluster1-
01_clus1  none
      3/5/2024 19:21:20 -06:00   cluster1-02_clus2   cluster1-
01_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 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 von RCF vorbereitet haben, können Sie "[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 Nexus-Switches 9336C-FX2 und 9336C-FX2-T zu installieren.

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\_clusions1, cluster1-02\_clus2 , cluster1-03\_clug1, Cluster1-03\_clus2, cluster1-04\_clut1, 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                      Ethernet1/7      N9K-
C9336C-FX2
    e0d    cs2                      Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
    e0a    cs1                      Ethernet1/8      N9K-
C9336C-FX2
    e0d    cs2                      Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/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::*>
```

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           Admin/Oper Address/Mask      Node
Port      Home

-----
-----
Cluster
      cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01  e0a      true
      cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01  e0d      true
      cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02  e0a      true
      cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02  e0d      true
      cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03  e0a      true
      cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03  e0b      true
      cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04  e0a      true
      cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04  e0b      true
8 entries were displayed.
cluster1::*>
```

- c. 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 all
```

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				
<hr/>					
<hr/>					
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: FOCXXXXXXXGD
    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-port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %% VDC-1 %% %STP-2-BLOCK_PVID_LOCAL:
Blocking port-port-channel1 on VLAN0092. Inconsistent local vlan.

```

- 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::*>

```

- Wiederholen Sie die Schritte 6 bis 13, um die NX-OS-Software auf Switch cs1 zu installieren.
- 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	Logical	Status	Network	Current
cluster1-01	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	true		
cluster1-01	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
cluster1-02	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	true		
cluster1-02	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
cluster1-03	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	true		
cluster1-03	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
cluster1-04	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	true		
cluster1-04	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?

Nach der Installation oder Aktualisierung der NX-OS-Software können Sie "[Installieren oder aktualisieren Sie RCF](#)". Die

## 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:aHwhpz07+YCD Srp3isJv2uVGz+mjMMokqdMeXVVXfd0

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/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcsvyHzftHJ7Dceg0vQaULYRALZeHwQ

(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"](#).

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

Die Referenzkonfigurationsdatei (RCF) wird nach der erstmaligen Einrichtung des Speicherswitches Nexus 9336C-FX2 installiert. 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 40/100GbE für Cluster+HA, 4x10GbE Breakout für Cluster und 4x25GbE Breakout für Cluster+HA sowie 100GbE für jedes Storage-HA-Paar konfiguriert.
Cluster	Zwei Varianten von RCF mit unterschiedlicher Belegung von 4x10GbE-Ports (Breakout) und 40/100GbE-Ports. Alle FAS und AFF Knoten werden unterstützt, mit Ausnahme der Systeme AFF A320, AFF A250 und FAS500f .
Storage	Alle Ports sind für 100-GbE-NVMe-Storage-Verbindungen konfiguriert.

## Vorgeschlagene Dokumentation

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

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 9000-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 sind cs1 und cs2.
- Die Knotennamen sind node1-01, node1-02, node1-03 und node1-04.
- Die Cluster-LIF-Namen sind node1-01\_clus1, node1-01\_clus2, node1-02\_clus1, node1-02\_clus2, node1-03\_clus1, node1-03\_clus2, node1-04\_clus1 und node1-04\_clus2.
- Der `cluster1::*` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Siehe die ["Hardware Universe"](#) um die richtigen Ports auf Ihrer Plattform zu überprüfen.



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

## 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 Installations- oder Aktualisierungsprozedur für RCF durchgelesen haben, können Sie ["Installieren Sie den RCF"](#) oder ["Aktualisieren Sie Ihren RCF"](#) nach Bedarf.

## Installieren Sie die Referenzkonfigurationsdatei

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Speicher-Switches Nexus 9336C-FX2 und 9336C-FX2-T zum ersten Mal eingerichtet haben.

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

## 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.

- 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](#)".

### 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-Storage.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](#)".

### Beispiel anzeigen

Dieses Beispiel zeigt die RCF **Nexus\_9336C\_RCF\_v1.6-Storage.txt**, die auf Switch cs1 installiert wird:

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-
commands
```

4. Überprüfen Sie die Bannerausgabe des show banner motd Befehls. Sie müssen diese Anweisungen lesen und befolgen, um die richtige Konfiguration und den korrekten Betrieb des Switches sicherzustellen.

## Beispiel anzeigen

```
cs1# show banner motd

*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Storage.txt
* Date        : 10-23-2020
* Version     : v1.6
*
* Port Usage : Storage configuration
* Ports 1-36: 100GbE Controller and Shelf Storage Ports
*****
*****
```

5. Stellen Sie sicher, dass der RCF 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. Notieren Sie alle benutzerdefinierten Ergänzungen zwischen dem aktuellen running-config Datei und die verwendete RCF-Datei.
7. Nachdem Sie überprüft haben, dass die RCF-Versionen und Schaltereinstellungen korrekt sind, kopieren Sie die running-config Datei in die startup-config Datei.

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

8. Speichern Sie grundlegende Konfigurationsdetails im `write_erase.cfg` Datei 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
```

9. Bei der Installation von RCF Version 1.12 und höher führen Sie 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.

10. Überprüfen Sie, ob die `write_erase.cfg` Die Datei wird wie erwartet ausgefüllt:

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

11. 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**

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

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

13. Starten Sie den Switch cs1 neu.

```
cs1# reload
```

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

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

15. 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
mgmt0 --          up      <mgmt ip address>
1000   1500
Eth1/11      1      eth  trunk  up      none
100G(D) --
Eth1/12      1      eth  trunk  up      none
100G(D) --
Eth1/13      1      eth  trunk  up      none
100G(D) --
Eth1/14      1      eth  trunk  up      none
100G(D) --
Eth1/15      1      eth  trunk  up      none
100G(D) --
Eth1/16      1      eth  trunk  up      none
100G(D) --
Eth1/17      1      eth  trunk  up      none
100G(D) --
Eth1/18      1      eth  trunk  up      none
100G(D) --
Eth1/23      1      eth  trunk  up      none
100G(D) --
Eth1/24      1      eth  trunk  up      none
100G(D) --
Eth1/25      1      eth  trunk  up      none
100G(D) --
Eth1/26      1      eth  trunk  up      none
100G(D) --
Eth1/27      1      eth  trunk  up      none
100G(D) --
Eth1/28      1      eth  trunk  up      none
100G(D) --
Eth1/29      1      eth  trunk  up      none
100G(D) --
Eth1/30      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	Po999
30	VLAN0030	active	Eth1/1, Eth1/2,
	Eth1/3, Eth1/4		Eth1/5, Eth1/6,
	Eth1/7, Eth1/8		Eth1/9, Eth1/10,
	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, Eth1/25,
	Eth1/26		Eth1/27, Eth1/28,
	Eth1/29		Eth1/30, Eth1/31,
	Eth1/32		Eth1/33, Eth1/34,
	Eth1/35		Eth1/36

```
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	trunking	--
Eth1/10	1	trunking	--
Eth1/11	1	trunking	--
Eth1/12	1	trunking	--
Eth1/13	1	trunking	--
Eth1/14	1	trunking	--
Eth1/15	1	trunking	--
Eth1/16	1	trunking	--
Eth1/17	1	trunking	--
Eth1/18	1	trunking	--
Eth1/19	1	trunking	--
Eth1/20	1	trunking	--
Eth1/21	1	trunking	--
Eth1/22	1	trunking	--
Eth1/23	1	trunking	--
Eth1/24	1	trunking	--
Eth1/25	1	trunking	--
Eth1/26	1	trunking	--
Eth1/27	1	trunking	--
Eth1/28	1	trunking	--
Eth1/29	1	trunking	--
Eth1/30	1	trunking	--
Eth1/31	1	trunking	--
Eth1/32	1	trunking	--
Eth1/33	1	trunking	--
Eth1/34	1	trunking	--
Eth1/35	1	trunking	--
Eth1/36	1	trunking	--

-----  
-----  
Port              Vlans Allowed on Trunk

Eth1/1	30
Eth1/2	30
Eth1/3	30
Eth1/4	30
Eth1/5	30
Eth1/6	30
Eth1/7	30
Eth1/8	30
Eth1/9	30
Eth1/10	30
Eth1/11	30
Eth1/12	30

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

---

---

---

Port                Vlans Err-disabled on Trunk

---

---

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	none
Eth1/12	none
Eth1/13	none
Eth1/14	none
Eth1/15	none
Eth1/16	none

Eth1/17	none
Eth1/18	none
Eth1/19	none
Eth1/20	none
Eth1/21	none
Eth1/22	none
Eth1/23	none
Eth1/24	none
Eth1/25	none
Eth1/26	none
Eth1/27	none
Eth1/28	none
Eth1/29	none
Eth1/30	none
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

---



---



---

Port            STP Forwarding

---



---

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	30
Eth1/12	30
Eth1/13	30
Eth1/14	30
Eth1/15	30
Eth1/16	30
Eth1/17	30
Eth1/18	30
Eth1/19	none
Eth1/20	none

Eth1/21	none
Eth1/22	none
Eth1/23	30
Eth1/24	30
Eth1/25	30
Eth1/26	30
Eth1/27	30
Eth1/28	30
Eth1/29	30
Eth1/30	30
Eth1/31	none
Eth1/32	none
Eth1/33	none
Eth1/34	none
Eth1/35	none
Eth1/36	none

---

---

Port                Vlans in spanning tree forwarding state and not pruned

---

---

Eth1/1	Feature VTP is not enabled
none	
Eth1/2	Feature VTP is not enabled
none	
Eth1/3	Feature VTP is not enabled
none	
Eth1/4	Feature VTP is not enabled
none	
Eth1/5	Feature VTP is not enabled
none	
Eth1/6	Feature VTP is not enabled
none	
Eth1/7	Feature VTP is not enabled
none	
Eth1/8	Feature VTP is not enabled
none	
Eth1/9	Feature VTP is not enabled
none	
Eth1/10	Feature VTP is not enabled
none	
Eth1/11	Feature VTP is not enabled
30	
Eth1/12	Feature VTP is not enabled
30	

Eth1/13	Feature VTP is not enabled
30	
Eth1/14	Feature VTP is not enabled
30	
Eth1/15	Feature VTP is not enabled
30	
Eth1/16	Feature VTP is not enabled
30	
Eth1/17	Feature VTP is not enabled
30	
Eth1/18	Feature VTP is not enabled
30	
Eth1/19	Feature VTP is not enabled
none	
Eth1/20	Feature VTP is not enabled
none	
Eth1/21	Feature VTP is not enabled
none	
Eth1/22	Feature VTP is not enabled
none	
Eth1/23	Feature VTP is not enabled
30	
Eth1/24	Feature VTP is not enabled
30	
Eth1/25	Feature VTP is not enabled
30	
Eth1/26	Feature VTP is not enabled
30	
Eth1/27	Feature VTP is not enabled
30	
Eth1/28	Feature VTP is not enabled
30	
Eth1/29	Feature VTP is not enabled
30	
Eth1/30	Feature VTP is not enabled
30	
Eth1/31	Feature VTP is not enabled
none	
Eth1/32	Feature VTP is not enabled
none	
Eth1/33	Feature VTP is not enabled
none	
Eth1/34	Feature VTP is not enabled
none	
Eth1/35	Feature VTP is not enabled
none	

Eth1/36	Feature VTP is not enabled
none	



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

### 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?

Nach der Installation Ihres RCF können Sie "[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. 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 angibt.

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

```
network device-discovery show
```

### Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/      Local   Discovered
Protocol    Port    Device (LLDP: ChassisID)  Interface      Platform
-----  -----  -----
-----  -----
node1-01/cdp
          e3a     cs1                      Ethernet1/7      N9K-
C9336C
          e3b     cs2                      Ethernet1/7      N9K-
C9336C
node1-02/cdp
          e3a     cs1                      Ethernet1/8      N9K-
C9336C
          e3b     cs2                      Ethernet1/8      N9K-
C9336C
.
.
.
```

4. Überprüfen Sie, ob alle Speicherports aktiv sind und einen fehlerfreien Status aufweisen:

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

#### Beispiel anzeigen

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status
<hr/>						
node1-01	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

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

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

#### Schritt 2: Ports konfigurieren

1. Fahren Sie auf Switch CS1 die Ports herunter, die mit allen Ports der Knoten verbunden sind.

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



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

- Überprüfen Sie, ob für die Cluster-LIFs ein Failover auf die auf 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
          node1-01_clus1  up/up      169.254.36.44/16  node1-01
e7a        true
          node1-01_clus2  up/up      169.254.7.5/16   node1-01
e7b        true
          node1-02_clus1  up/up      169.254.197.206/16 node1-02
e7a        true
          node1-02_clus2  up/up      169.254.195.186/16 node1-02
e7b        true
          node1-03_clus1  up/up      169.254.192.49/16  node1-03
e7a        true
          node1-03_clus2  up/up      169.254.182.76/16  node1-03
e7b        true
          node1-04_clus1  up/up      169.254.59.49/16   node1-04
e7a        true
          node1-04_clus2  up/up      169.254.62.244/16  node1-04
e7b        true

8 entries were displayed.
```

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

```
cluster show
```

## Beispiel anzeigen

```
cluster1::*> cluster show
Node          Health  Eligibility  Epsilon
-----
node1-01      true    true         false
node1-02      true    true         false
node1-03      true    true         true
node1-04      true    true         false

4 entries were displayed.
```

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 dem aktuellen `running-config` und die verwendete RCF-Datei (z. B. eine SNMP-Konfiguration für Ihre Organisation).
- b. Für NX-OS 10.2 und höher verwenden Sie die `show diff running-config` Befehl zum Vergleich mit der gespeicherten RCF-Datei im Bootflash. Alternativ können Sie ein Vergleichstool eines Drittanbieters verwenden.

5. Speichern Sie grundlegende Konfigurationsdetails im `write_erase.cfg` Datei auf dem Bootflash.

Stellen Sie sicher, dass Sie Folgendes konfigurieren:



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

```
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. Beim Upgrade auf RCF Version 1.12 und höher führen Sie 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 `write_erase.cfg` Die Datei wird wie erwartet ausgefüllt:

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

8. 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**

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

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

10. Starten Sie den Switch neu:

```
cs1# 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-Storage.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.

Dieses Beispiel zeigt die RCF-Datei. NX9336C-FX2-RCF-v1.13-1-Storage.txt wird auf Switch CS1 installiert:

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-commands
```



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

14. 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.

15. Wenden Sie alle vorherigen Anpassungen erneut auf die Switch-Konfiguration an.

16. Nachdem Sie die RCF-Versionen, benutzerdefinierten Ergänzungen und Schaltereinstellungen überprüft haben, 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
```

17. 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
```

18. Überprüfen Sie, ob alle Speicherports aktiv sind und einen fehlerfreien Status aufweisen:

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

#### Beispiel anzeigen

```
cluster1::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed		
				(Gb/s)	State	Status
<hr/>						
node1-01	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
node1-02	e3a	ENET	-	100	enabled	online
	e3b	ENET	-	100	enabled	online
	e7a	ENET	-	100	enabled	online
	e7b	ENET	-	100	enabled	online
.						
.						
.						

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

```
cluster show
```

#### Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

20. Wiederholen Sie die Schritte 4 bis 19 auf Switch cs2.

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

```
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
```

2. Überprüfen Sie, ob die erwarteten Nodes weiterhin verbunden sind:

```
show cdp neighbors
```

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

```
show vlan brief
```

```
show interface trunk
```

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

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

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>
```

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

```
cluster show
```

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

a. Sie können die `network interface check cluster-connectivity show` Befehl zum Anzeigen der Details einer Zugänglichkeitsprüfung für die Clusterkonnektivität:

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

b. Alternativ können Sie die `cluster ping-cluster -node <node-name>` Befehl zum Überprüfen

der Konnektivität:

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

#### Was kommt als Nächstes?

Nach dem Upgrade Ihres RCF können Sie "[Überprüfen Sie die SSH-Konfiguration](#)" Die

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

Um die Speicherschalter 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurückzusetzen, müssen Sie die Schaltereinstellungen 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.

#### Was kommt als nächstes

Nachdem Sie Ihre Schalter zurückgesetzt haben, können Sie "[neu konfigurieren](#)" sie nach Bedarf.

## **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, BEISPIELHAFFE 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 VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERWEINER 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.