



Software konfigurieren

Install and maintain

NetApp

February 06, 2026

This PDF was generated from <https://docs.netapp.com/de-de/ontap-systems-switches/switch-cisco-3232c/configure-software-overview-3232c-cluster.html> on February 06, 2026. Always check docs.netapp.com for the latest.

Inhalt

Software konfigurieren	1
Workflow zur Softwareinstallation für Cisco Nexus 3232C-Cluster-Switches	1
Konfigurieren des Cluster-Switches 3232C	1
Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei (RCF) vor.	4
Installieren Sie die NX-OS-Software	11
Überprüfungsanforderungen	11
Installieren Sie die Software	11
Installieren oder aktualisieren Sie die RCF	31
Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).	32
Installieren Sie die Referenzkonfigurationsdatei (RCF).	34
Aktualisieren Sie Ihre Referenzkonfigurationsdatei (RCF)	39
Überprüfen Sie Ihre SSH-Konfiguration	62
Setzen Sie den 3232C-Cluster-Switch auf die Werkseinstellungen zurück	64

Software konfigurieren

Workflow zur Softwareinstallation für Cisco Nexus 3232C-Cluster-Switches

Um die Software für einen Cisco Nexus 3232C-Switch zu installieren und zu konfigurieren und die Referenzkonfigurationsdatei (RCF) zu installieren oder zu aktualisieren, gehen Sie wie folgt vor:

1

"Konfigurieren Sie den Schalter"

Konfigurieren Sie den 3232C-Cluster-Switch.

2

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

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

3

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

Laden Sie die NX-OS-Software herunter und installieren oder aktualisieren Sie sie auf dem Cisco 3232C-Cluster-Switch.

4

"Installieren Sie den RCF"

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

5

"SSH-Konfiguration überprüfen"

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

6

"Setzen Sie den Schalter auf die Werkseinstellungen zurück."

Löschen Sie die 3232C-Cluster-Switch-Einstellungen.

Konfigurieren des Cluster-Switches 3232C

Gehen Sie wie folgt vor, um den Cisco Nexus 3232C Switch einzurichten und zu konfigurieren.

Bevor Sie beginnen

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server am Installationsort, um die entsprechenden NX-OS- und Referenzkonfigurationsdatei-(RCF)-Versionen herunterzuladen.

- Anwendbare NX-OS-Version, heruntergeladen von "[Cisco -Software-Download](#)" Seite.
- Erforderliche Dokumentation zum Cluster-Netzwerk und zum Management-Netzwerk-Switch.
Sehen "[Erforderliche Dokumentation](#)" für weitere Informationen.
- Erforderliche Controller-Dokumentation und ONTAP Dokumentation.

["NetApp Dokumentation"](#)

- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.
- Ausgefüllte Verkabelungs-Arbeitsblätter.
- Anwendbare NetApp Clusternetzwerk- und Managementnetzwerk-RCFs, heruntergeladen von der NetApp Support-Website unter "[mysupport.netapp.com](#)" für die Schalter, die Sie erhalten. Alle Cisco Cluster-Netzwerk- und Management-Netzwerk-Switches werden mit der standardmäßigen Cisco -Werkskonfiguration ausgeliefert. Auf diesen Switches ist auch die aktuelle Version der NX-OS-Software installiert, allerdings sind die RCFs nicht geladen.

Schritte

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

Wenn Sie Ihr... installieren	Dann...
Cisco Nexus 3232C in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden <i>Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet</i> .
Ausrüstung in einem Telekommunikationsrack	Beachten Sie die in den Hardware-Installationshandbüchern für Switches und den Installations- und Einrichtungsanweisungen von NetApp beschriebenen Vorgehensweisen.

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

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

Prompt	Antwort
Automatische Bereitstellung abbrechen und mit normaler Einrichtung fortfahren? (ja/nein)	Antworten Sie mit ja . Die Standardeinstellung ist Nein.
Wollen Sie einen sicheren Passwortstandard erzwingen? (ja/nein)	Antworten Sie mit ja . Die Standardeinstellung ist Ja.

Prompt	Antwort
Geben Sie das Passwort für den Administrator ein.	Das Standardpasswort lautet "admin"; Sie müssen ein neues, sicheres Passwort erstellen. Ein schwaches Passwort kann abgelehnt werden.
Möchten Sie den Dialog zur Basiskonfiguration aufrufen? (ja/nein)	Antworten Sie bei der Erstkonfiguration des Switches mit ja .
Ein weiteres Benutzerkonto erstellen? (ja/nein)	Die Antwort hängt von den Richtlinien Ihrer Website bezüglich alternativer Administratoren ab. Die Standardeinstellung ist nein .
SNMP-Community-String schreibgeschützt konfigurieren? (ja/nein)	Antworten Sie mit nein . Die Standardeinstellung ist Nein.
SNMP-Community-Zeichenfolge für Lese- und Schreibzugriffe konfigurieren? (ja/nein)	Antworten Sie mit nein . Die Standardeinstellung ist Nein.
Geben Sie den Namen des Schalters ein.	Der Name des Schalters ist auf 63 alphanumerische Zeichen beschränkt.
Mit der Out-of-Band-Managementkonfiguration (mgmt0) fortfahren? (ja/nein)	Antworten Sie bei dieser Eingabeaufforderung mit ja (Standardeinstellung). Geben Sie an der Eingabeaufforderung mgmt0 IPv4 address: Ihre IP-Adresse ein: ip_address.
Standardgateway konfigurieren? (ja/nein)	Antworten Sie mit ja . Geben Sie an der IPv4-Adresse des Standardgateways Ihre Standardgateway-Adresse ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit nein . Die Standardeinstellung ist Nein.
Den Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit nein . Die Standardeinstellung ist Nein.
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit ja. Die Standardeinstellung ist Ja.</p> <p> Bei der Verwendung von Ethernet Switch Health Monitor (CSHM) wird SSH aufgrund seiner Protokollierungsfunktionen empfohlen. Für erhöhte Sicherheit wird auch SSHv2 empfohlen.</p>
Geben Sie den Typ des SSH-Schlüssels ein, den Sie generieren möchten (dsa/rsa/rsa1).	Standardmäßig wird rsa verwendet.

Prompt	Antwort
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits im Bereich von 1024 bis 2048 ein.
Den NTP-Server konfigurieren? (ja/nein)	Antworten Sie mit nein . Die Standardeinstellung ist Nein.
Standard-Schnittstellenschicht (L3/L2) konfigurieren:	Antworte mit L2 . Standardmäßig ist L2 eingestellt.
Standardmäßigen Schnittstellenstatus des Switch-Ports konfigurieren (ausgeschaltet/nicht ausgeschaltet):	Antworte mit noshut . Die Standardeinstellung ist noshut.
CoPP-Systemprofil konfigurieren (streng/moderat/tolerant/dicht):	Mit streng antworten. Die Standardeinstellung ist strikt.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	An dieser Stelle sollten Sie die neue Konfiguration sehen. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie gegebenenfalls die erforderlichen Änderungen vor. Antworten Sie mit nein , wenn Sie mit der Konfiguration zufrieden sind. Antworten Sie mit ja , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Diese Konfiguration verwenden und speichern? (ja/nein)	Antworten Sie mit ja , um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systemabbilder automatisch aktualisiert.
	<p> Wenn Sie die Konfiguration in diesem Schritt nicht speichern, werden beim nächsten Neustart des Switches keine der Änderungen wirksam.</p>

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

Wie geht es weiter?

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

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

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

Zu den Beispielen

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

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



Die Befehlsausgaben können je nach ONTAP Version variieren.

Nomenklatur von Schaltern und Knoten

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

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

Informationen zu diesem Vorgang

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

Schritte

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fällerstellung durch Aufruf einer AutoSupport -Nachricht: `system node autosupport invoke -node * -type all -message MAINT=x h`

wobei x die Dauer des Wartungsfensters in Stunden ist.



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

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

```
set -privilege advanced
```

Die erweiterte Aufforderung(*>) erscheint.

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

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

Beispiel anzeigen

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

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

-----
-----  

cluster1-02/cdp
      e0a    cs1          Eth1/2      N3K-
C3232C
      e0b    cs2          Eth1/2      N3K-
C3232C
cluster1-01/cdp
      e0a    cs1          Eth1/1      N3K-
C3232C
      e0b    cs2          Eth1/1      N3K-
C3232C

4 entries were displayed.
```

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

a. Netzwerkportattribute anzeigen:

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

Beispiel anzeigen

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

Node: cluster1-02
      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.
```

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

Beispiel anzeigen

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

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

4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

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

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

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

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

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

Alle ONTAP Versionen

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

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

```

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

```

1. [[Schritt 6]] Überprüfen Sie, ob die auto-revert Der Befehl ist auf allen Cluster-LIFs aktiviert: network interface show -vserver Cluster -fields auto-revert

Beispiel anzeigen

```

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

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

```

Wie geht es weiter?

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

Installieren Sie die NX-OS-Software

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

Überprüfungsanforderungen

Bevor Sie beginnen

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- "[Cisco Ethernet-Switch-Seite](#)". In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und NX-OS-Versionen.
- "[Cisco Nexus 3000 Series Switches](#)". Die vollständige Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco -Switches finden Sie in den entsprechenden Software- und Upgrade-Anleitungen auf der Cisco -Website.

Installieren Sie die Software

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

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

Schritte

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

Beispiel anzeigen

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

```
cs2# ping 172.19.2.1
Pinging 172.19.2.1 with 0 bytes of data:
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

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

```
network device-discovery show
```

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
    e0a    cs1                      Ethernet1/7      N3K-
C3232C
    e0d    cs2                      Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
    e0a    cs1                      Ethernet1/8      N3K-
C3232C
    e0d    cs2                      Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
    e0a    cs1                      Ethernet1/1/1    N3K-
C3232C
    e0b    cs2                      Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
    e0a    cs1                      Ethernet1/1/2    N3K-
C3232C
    e0b    cs2                      Ethernet1/1/2    N3K-
C3232C
cluster1::*
```

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

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

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

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```

Node: cluster1-04

Ignore

          Speed (Mbps)

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

```

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

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

Beispiel anzeigen

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

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

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch          Type          Address
Model
-----
-----
cs1           cluster-network  10.233.205.90  N3K-
C3232C
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        9.3(5)
    Version Source: CDP

cs2           cluster-network  10.233.205.91  N3K-
C3232C
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        9.3(5)
    Version Source: CDP
cluster1::*
```

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

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

6. Kopieren Sie die NX-OS-Software und die EPLD-Images auf den Nexus 3232C-Switch.

Beispiel anzeigen

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

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

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get /code/n9000-epld.9.3.4.img /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

```
show version
```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

otherwise stated, there is no warranty, express or implied,
including but not

limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/library.txt.
```

Software

```
BIOS: version 08.37
NXOS: version 9.3(3)
BIOS compile time: 01/28/2020
NXOS image file is: bootflash:///nxos.9.3.3.bin
NXOS compile time: 12/22/2019 2:00:00 [12/22/2019 14:00:37]
```

Hardware

```
cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
```

```
Processor Board ID FOCXXXXXXGD
```

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

```
Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
Reason: Reset Requested by CLI command reload
```

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

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

8. Installieren Sie das NX-OS-Image.

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

Beispiel anzeigen

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

Notifying services about system upgrade.
[] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact          Install-type  Reason
-----  -----
-----  -----
1      Yes            Disruptive      Reset          Default
upgrade is not hitless

Images will be upgraded according to following table:
Module      Image      Running-Version(pri:alt)
New-Version  Upg-Required
-----  -----
-----  -----
1          nxos      9.3(3)
9.3(4)          yes
1          bios      v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)  no

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

```
Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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

Finishing the upgrade, switch will reboot in 10 seconds.
cs2#
```

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

```
show version
```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

otherwise stated, there is no warranty, express or implied,
including but not

limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/library.txt.
```

Software

```
BIOS: version 08.37
NXOS: version 9.3(4)
BIOS compile time: 01/28/2020
NXOS image file is: bootflash:///nxos.9.3.4.bin
NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]
```

Hardware

```
cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
```

```
Processor Board ID FOCXXXXXXGS
```

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

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

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

plugin
Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

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

Beispiel anzeigen

```
cs2# show version module 1 epld

EPLD Device          Version
-----
MI    FPGA           0x12
IO    FPGA           0x11

cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
Compatibility check:
Module      Type      Upgradable      Impact      Reason
-----  -----
-----  -----
1          SUP       Yes            Disruptive   Module
Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type  EPLD          Running-Version  New-Version  Upg-
Required
-----  -----  -----          -----          -----  -----
-----  -----
1      SUP   MI  FPGA        0x12          0x12        No
1      SUP   IO  FPGA        0x11          0x12        Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

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

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

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

Beispiel anzeigen

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

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

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

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

Beispiel anzeigen

```
cs2# show version module 1 epld

EPLD Device          Version
-----
MI    FPGA           0x12
IO    FPGA           0x12
```

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

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

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

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

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

```
8 entries were displayed.
```

b. Überprüfen Sie den Zustand der Switches im Cluster.

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

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
      e0a    cs1          Ethernet1/7      N3K-
C3232C
      e0d    cs2          Ethernet1/7      N3K-
C3232C
cluster01-2/cdp
      e0a    cs1          Ethernet1/8      N3K-
C3232C
      e0d    cs2          Ethernet1/8      N3K-
C3232C
cluster01-3/cdp
      e0a    cs1          Ethernet1/1/1    N3K-
C3232C
      e0b    cs2          Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
      e0a    cs1          Ethernet1/1/2    N3K-
C3232C
      e0b    cs2          Ethernet1/1/2    N3K-
C3232C

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

-----
-----
cs1            cluster-network  10.233.205.90  N3K-
C3232C
  Serial Number: FOCXXXXXXGD
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
  9.3(5)
  Version Source: CDP

cs2            cluster-network  10.233.205.91  N3K-
```

```
C3232C
```

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

```
2 entries were displayed.
```

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

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

14. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

16. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

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

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

Beispiel anzeigen

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

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

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

Wie geht es weiter?

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

Installieren oder aktualisieren Sie die RCF

Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus 3232C-Switches zum ersten Mal eingerichtet haben. Sie aktualisieren Ihre RCF-Version, wenn auf Ihrem Switch eine vorhandene Version der RCF-Datei installiert ist.

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

Verfügbare RCF-Konfigurationen

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

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

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

Verfügbare RCFs

Die folgende Tabelle listet die verfügbaren RCFs für 3232C-Switches auf. Wählen Sie die für Ihre Konfiguration passende RCF-Version aus. Sehen "[Cisco Ethernet-Switches](#)" für weitere Informationen.

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

Empfohlene Dokumentation

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

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

- "[Cisco Nexus 3000 Series Switches](#)"

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

Zu den Beispielen

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

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

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



Die Befehlsausgaben können je nach ONTAP Version variieren.

Einzelheiten zu den verfügbaren RCF-Konfigurationen finden Sie unter "[Softwareinstallations-Workflow](#)" .

verwendete Befehle

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

Wie geht es weiter?

Nachdem Sie die Übersicht über die Installations- oder Aktualisierungsprozedur von RCF durchgelesen haben,

können Sie "[Installieren Sie den RCF](#)" oder "[Aktualisieren Sie Ihren RCF](#)" wie erforderlich.

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus 3232C-Switches zum ersten Mal eingerichtet haben.

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

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

Informationen zu diesem Vorgang

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

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

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

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich per SSH oder über eine serielle Konsole bei Switch CS2 an.
2. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs2: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 3000 Serie NX-OS Befehlsreferenz](#)" .

Beispiel anzeigen

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

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

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

Beispiel anzeigen

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

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-
      config echo-commands
```



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

4. Untersuchen Sie die Bannerausgabe von `show banner motd` Befehl. Um die korrekte Konfiguration und den ordnungsgemäßen Betrieb des Schalters sicherzustellen, müssen Sie die Anweisungen unter **Wichtige Hinweise** lesen und befolgen.
5. Überprüfen Sie, ob es sich bei der RCF-Datei um die korrekte, neuere Version handelt:

```
show running-config
```

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

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

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

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



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

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

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

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

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>  
bootflash:write_erase.cfg  
  
cs2# echo "hardware access-list tcam region qos 256" >>  
bootflash:write_erase.cfg
```

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

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

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

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

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

12. Neustartschalter cs2:

```
cs2# reload
```

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

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

14. Verbinden Sie die Cluster-Ports aller Knoten im ONTAP Cluster mit den Switches cs1 und cs2.

Schritt 2: Überprüfen Sie die Switch-Verbindungen

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

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

Beispiel anzeigen

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

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

```
show port-channel summary
```

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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

Wenn Cluster-LIFS nicht zu ihren Home-Ports zurückgekehrt sind, setzen Sie sie manuell zurück:
network interface revert -vserver <vserver_name> -lif <lif_name>

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

Schritt 3: Einrichten Ihres ONTAP Clusters

NetApp empfiehlt, neue Cluster mit dem System Manager einzurichten.

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

Siehe "[Konfigurieren Sie ONTAP auf einem neuen Cluster mit System Manager](#)" für Einrichtungsanweisungen.

Wie geht es weiter?

Nach der Installation des RCF können Sie "[Überprüfen Sie die SSH-Konfiguration](#)" Die

Aktualisieren Sie Ihre Referenzkonfigurationsdatei (RCF)

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

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

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

-  Während dieses Vorgangs ist kein betriebsbereiter Inter-Switch-Link (ISL) erforderlich. Dies ist beabsichtigt, da RCF-Versionsänderungen die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, migriert das folgende Verfahren alle Cluster-LIFs zum operativen Partner-Switch, während die Schritte auf dem Ziel-Switch ausgeführt werden.
-  Vor der Installation einer neuen Switch-Softwareversion und neuer RCFs müssen Sie die Switch-Einstellungen löschen und eine Basiskonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein oder grundlegende Konfigurationsinformationen gesichert haben, bevor Sie die Switch-Einstellungen löschen.

Schritt 1: Vorbereitung auf das Upgrade

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

```
network device-discovery show
```

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
    e0a    cs1
C3232C
    e0d    cs2
C3232C
cluster1-02/cdp
    e0a    cs1
C3232C
    e0d    cs2
C3232C
cluster1-03/cdp
    e0a    cs1
C3232C
    e0b    cs2
C3232C
cluster1-04/cdp
    e0a    cs1
C3232C
    e0b    cs2
C3232C
cluster1::*
```

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

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

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

Beispiel anzeigen

```
cluster1::*> network port show -role cluster
Node: cluster1-01

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

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

Ignore
                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
----- -----
----- 
e0a      Cluster      Cluster          up    9000  auto/10000
healthy  false
e0b      Cluster      Cluster          up    9000  auto/10000
healthy  false
Node: cluster1-04

Ignore
                                         Speed (Mbps)
```

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

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

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

Beispiel anzeigen

cluster1::*> network interface show -role cluster		Logical	Status	Network
Current	Current	Is		
Vserver	Interface		Admin/Oper	Address/Mask
Port	Home			Node

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

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

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch          Type          Address
Model
-----
-----
cs1            cluster-network 10.233.205.92
NX3232C
    Serial Number: 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
NX3232C
    Serial Number: FOXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        9.3 (4)
    Version Source: CDP
2 entries were displayed.
```

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

Schritt 2: Ports konfigurieren

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

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



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

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

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

Beispiel anzeigen

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

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

```
show running-config
```

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



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

```
cs2# show run | section "switchname" > bootflash:write_erase.cfg
cs2# show run | section "hostname" >> bootflash:write_erase.cfg
cs2# show run | i "username admin password" >> bootflash:write_erase.cfg
cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg
cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
```

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

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>
bootflash:write_erase.cfg
cs2# echo "hardware access-list tcam region qos 256" >>
bootflash:write_erase.cfg
```

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

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

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

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

11. Starten Sie den Switch CS2 neu:

```
cs2# reload
```

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

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

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

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

Beispiel anzeigen

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

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

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

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

Beispiel anzeigen

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

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```



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

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

```
show running-config
```

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

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

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

16. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an.

Siehe "[Überprüfung der Verkabelung und Konfigurationsüberlegungen](#)" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.

17. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Schaltiereinstellungen korrekt sind, kopieren Sie die Running-Config-Datei in die Startup-Config-Datei.

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

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

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

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

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

a. Überprüfen Sie, ob die e0d-Ports auf allen Knoten im Cluster aktiv und fehlerfrei sind:

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

Beispiel anzeigen

```
cluster1::*> network port show -role cluster
Node: cluster1-01

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

Ignore
                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
----- -----
----- 
e0a      Cluster      Cluster          up    9000  auto/10000
healthy  false
e0b      Cluster      Cluster          up    9000  auto/10000
healthy  false
Node: cluster1-03

Ignore
                                         Speed (Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU Admin/Oper
Status   Status
----- -----
----- 
e0a      Cluster      Cluster          up    9000  auto/100000
healthy false
e0d      Cluster      Cluster          up    9000  auto/100000
healthy false
Node: cluster1-04

Ignore
                                         Speed (Mbps)
```

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

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

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
    e0a    cs1                      Ethernet1/7
N3K-C3232C
    e0d    cs2                      Ethernet1/7
N3K-C3232C
cluster01-2/cdp
    e0a    cs1                      Ethernet1/8
N3K-C3232C
    e0d    cs2                      Ethernet1/8
N3K-C3232C
cluster01-3/cdp
    e0a    cs1                      Ethernet1/1/1
N3K-C3232C
    e0b    cs2                      Ethernet1/1/1
N3K-C3232C
cluster1-04/cdp
    e0a    cs1                      Ethernet1/1/2
N3K-C3232C
    e0b    cs2                      Ethernet1/1/2
N3K-C3232C
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                  Type          Address
Model

-----
-----
cs1                  cluster-network  10.233.205.90
N3K-C3232C
    Serial Number: FOXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(4)
    Version Source: CDP
cs2                  cluster-network  10.233.205.91
N3K-C3232C
    Serial Number: FOXXXXXXXGS
```

```
Is Monitored: true
  Reason: None
Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
  9.3 (4)
  Version Source: CDP
2 entries were displayed.
```



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



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

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

Beispiel anzeigen

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

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

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

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

Beispiel anzeigen

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

22. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

23. Wiederholen Sie die Schritte 4 bis 19 auf Switch cs1.
24. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

Schritt 3: Überprüfen Sie die Clusternetzwerkkonfiguration und den Clusterzustand.

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

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

Beispiel anzeigen

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

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

```
show port-channel summary
```

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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

Wenn Cluster-LIFS nicht zu ihren Home-Ports zurückgekehrt sind, setzen Sie sie manuell zurück:
network interface revert -vserver *vserver_name* -lif *lif_name*

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

ONTAP 9.9.1 und höher

Sie können die `network interface check cluster-connectivity` Befehl, um eine Zugänglichkeitsprüfung für die Clusterkonnektivität zu starten und dann die Details anzuzeigen: `network interface check cluster-connectivity start` Und `network interface check cluster-connectivity show`

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node      Date          LIF          LIF
Loss
-----
-----
cluster1-01
      3/5/2022 19:21:18 -06:00  cluster1-01_clus2  cluster1-02_clus1
none
      3/5/2022 19:21:20 -06:00  cluster1-01_clus2  cluster1-02_clus2
none
.
.
cluster1-02
      3/5/2022 19:21:18 -06:00  cluster1-02_clus2  cluster1-01_clus1
none
      3/5/2022 19:21:20 -06:00  cluster1-02_clus2  cluster1-01_clus2
none
.
.
cluster1-03
.
.
.
.
cluster1-04
.
.
.
.
```

Alle ONTAP Versionen

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

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

Wie geht es weiter?

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

Überprüfen Sie Ihre SSH-Konfiguration

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

Schritte

1. Überprüfen Sie, ob SSH aktiviert ist:

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

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

```
show ssh key
```

Beispiel anzeigen

```
(switch) # show ssh key

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

ssh-rsa
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:TFGe2hXn6QIpcsvyHzfthJ7Dceg0vQaULYRALZeHwQ

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

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

Wie geht es weiter?

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

Setzen Sie den 3232C-Cluster-Switch auf die Werkseinstellungen zurück

Um den 3232C-Cluster-Switch auf die Werkseinstellungen zurückzusetzen, müssen Sie die 3232C-Switch-Einstellungen löschen.

Informationen zu diesem Vorgang

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

Schritte

1. Löschen Sie die vorhandene Konfiguration:

```
write erase
```

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

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

2. Laden Sie die Switch-Software neu:

```
reload
```

```
(cs2) # reload
```

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

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

Was kommt als nächstes

Nach dem Zurücksetzen des Schalters können Sie ["neu konfigurieren"](#) Es wird Ihren Anforderungen entsprechend angefertigt.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT 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 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.