



Installieren oder aktualisieren Sie die RCF

Install and maintain

NetApp

February 13, 2026

Inhalt

Installieren oder aktualisieren Sie die RCF	1
Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).	1
Installieren Sie die Referenzkonfigurationsdatei (RCF).	3
Schritt 1: Installieren Sie die RCF auf den Schaltern	3
Schritt 2: Überprüfen Sie die Switch-Verbindungen	10
Schritt 3: Einrichten Ihres ONTAP Clusters	13
Aktualisieren Sie Ihre Referenzkonfigurationsdatei (RCF)	13
Schritt 1: Vorbereitung auf das Upgrade	13
Schritt 2: Ports konfigurieren	19
Schritt 3: Konfiguration überprüfen	30

Installieren oder aktualisieren Sie die RCF

Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).

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

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

Verfügbare RCF-Konfigurationen

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

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

RCF-Name	Beschreibung
2-Cluster-HA-Ausbruch	Unterstützt zweiONTAP -Cluster mit mindestens acht Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
4-Cluster-HA-Ausbruch	Unterstützt vierONTAP -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.

RCF-Name	Beschreibung
Cluster	Zwei Varianten von RCF mit unterschiedlicher Belegung von 4x10GbE-Ports (Breakout) und 40/100GbE-Ports. Alle FAS/ AFF -Knoten werden unterstützt, mit Ausnahme der Systeme AFF A320, AFF A250 und FAS500f .
Storage	Alle Ports sind für 100GbE NVMe-Speicherverbindungen konfiguriert.

Verfügbare RCFs

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

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

Empfohlene Dokumentation

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

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

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

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

Zu den Beispielen

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

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

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



Die Befehlausgaben können je nach ONTAP Version variieren.

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

verwendete Befehle

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

Wie geht es weiter?

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

Installieren Sie die Referenzkonfigurationsdatei (RCF).

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

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

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

Informationen zu diesem Vorgang

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

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

Schritt 1: Installieren Sie die RCF auf den Schaltern

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

```
network device-discovery show
```

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
      e0a    cs1                      Ethernet1/7      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
      e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
      e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
      e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*
```

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

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

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

Beispiel anzeigen

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

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

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

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

Ignore                                         Speed (Mbps)
```

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

```
cluster1::*>
```

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

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

Beispiel anzeigen

Logical		Status	Network	
Current	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
cluster1-01	e0a	up/up	169.254.3.4/23	
cluster1-01	e0d	up/up	169.254.3.5/23	
cluster1-02	e0a	up/up	169.254.3.8/23	
cluster1-02	e0d	up/up	169.254.3.9/23	
cluster1-03	e0a	up/up	169.254.1.3/23	
cluster1-03	e0b	up/up	169.254.1.1/23	
cluster1-04	e0a	up/up	169.254.1.6/23	
cluster1-04	e0b	up/up	169.254.1.7/23	

```
cluster1::*>
```

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

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

Beispiel anzeigen

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



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

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

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

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

```

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

```



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

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

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

Beispiel anzeigen

```

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

```

- Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

```
show running-config
```

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



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

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



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

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

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

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

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

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

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

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

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

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

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

14. Starten Sie den Switch neu:

```
cs2# reload
```

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

15. Wiederholen Sie die Schritte 7 bis 14 auf Switch cs1.

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

Schritt 2: Überprüfen Sie die Switch-Verbindungen

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

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

Beispiel anzeigen

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

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

```
show port-channel summary
```

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

Schritt 3: Einrichten Ihres ONTAP Clusters

NetApp empfiehlt, neue Cluster mit dem System Manager einzurichten.

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

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

Wie geht es weiter?

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

Aktualisieren Sie Ihre Referenzkonfigurationsdatei (RCF)

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

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

Wenn Sie die Bootkonfiguration ändern müssen, um die aktuellen Boot-Images widerzuspiegeln, müssen Sie dies tun, bevor Sie die RCF erneut anwenden, damit bei zukünftigen Neustarts die richtige Version 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                      Ethernet1/7      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
      e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
      e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
      e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
      e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
      e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*
```

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

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

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

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```

Node: cluster1-04

Ignore                                         Speed (Mbps)

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

```

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

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

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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



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

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

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

Schritt 2: Ports konfigurieren

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

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



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

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

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

Beispiel anzeigen

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

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

```
show running-config
```

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

Stellen Sie sicher, dass Sie Folgendes konfigurieren:



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

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



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

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

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

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

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

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

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

```
cs2# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

11. Starten Sie den Switch neu:

```
cs2# reload
```

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

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

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

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

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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



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

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

```
show running-config
```

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

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

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



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

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

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

Beispiel anzeigen

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

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

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

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

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

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

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

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

b. Überprüfen Sie den Zustand der Switches im Cluster.

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

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
    e0a      cs1                      Ethernet1/7
N3K-C3132Q-V
    e0d      cs2                      Ethernet1/7
N3K-C3132Q-V
cluster01-2/cdp
    e0a      cs1                      Ethernet1/8
N3K-C3132Q-V
    e0d      cs2                      Ethernet1/8
N3K-C3132Q-V
cluster01-3/cdp
    e0a      cs1                      Ethernet1/1/1
N3K-C3132Q-V
    e0b      cs2                      Ethernet1/1/1
N3K-C3132Q-V
cluster1-04/cdp
    e0a      cs1                      Ethernet1/1/2
N3K-C3132Q-V
    e0b      cs2                      Ethernet1/1/2
N3K-C3132Q-V

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

-----
-----
cs1                    cluster-network  10.233.205.90
N3K-C3132Q-V
    Serial Number: FOXXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
    9.3(4)
    Version Source: CDP

cs2                    cluster-network  10.233.205.91
```

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

2 entries were displayed.
```

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

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

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

+

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

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

Beispiel anzeigen

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

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

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

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

Beispiel anzeigen

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

22. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

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

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

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

Schritt 3: Konfiguration überprüfen

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

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

Beispiel anzeigen

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

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

```
show port-channel summary
```

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

ONTAP 9.9.1 und höher

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

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

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

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

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

Alle ONTAP Versionen

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

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

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

Wie geht es weiter?

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

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 VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERINER 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.