



Aktualisieren Sie den Switch

Install and maintain

NetApp

February 13, 2026

Inhalt

Aktualisieren Sie den Switch	1
Upgrade-Workflow für BES-53248-Cluster-Switches.....	1
Aktualisieren Sie die EFOS-Software	1
Bereiten Sie sich auf das Upgrade vor	1
Aktualisieren Sie die Software	3
Aktualisieren Sie die Referenzkonfigurationsdatei (RCF)	12
Schritt 1: Vorbereitung auf das Upgrade	14
Schritt 2: Ports konfigurieren	20
Schritt 3: Konfiguration überprüfen	37
Überprüfen Sie das ONTAP Clusternetzwerk nach einem EFOS-Software- oder RCF-Upgrade der BES-53248-Cluster-Switches.....	43

Aktualisieren Sie den Switch

Upgrade-Workflow für BES-53248-Cluster-Switches

Führen Sie die folgenden Schritte aus, um die EFOS-Software und die Referenzkonfigurationsdateien (RCFs) auf Broadcom BES-54328 Cluster-Switches zu aktualisieren, sofern zutreffend.

1

"Aktualisieren Sie Ihre EFOS-Version"

Laden Sie die Ethernet Fabric OS (EFOS)-Software herunter und installieren Sie sie auf dem Cluster-Switch BES-53248.

2

"Aktualisieren Sie Ihre RCF-Version"

Aktualisieren Sie die RCF auf dem BES-53248 Cluster-Switch und überprüfen Sie anschließend die Ports auf eine zusätzliche Lizenz, nachdem die RCF angewendet wurde.

3

"Überprüfen Sie das ONTAP Clusternetzwerk nach dem Upgrade."

Überprüfen Sie den Zustand des ONTAP -Clusternetzwerks nach einem Upgrade der EFOS-Software oder des RCF für BES-53248-Cluster-Switches.

Aktualisieren Sie die EFOS-Software

Führen Sie diese Schritte aus, um die EFOS-Software auf dem Cluster-Switch BES-53248 zu aktualisieren.

Die EFOS-Software umfasst eine Reihe fortschrittlicher Netzwerkfunktionen und -protokolle zur Entwicklung von Ethernet- und IP-Infrastruktursystemen. Diese Softwarearchitektur eignet sich für jedes Netzwerkgerät, das Anwendungen nutzt, die eine gründliche Paketprüfung oder -trennung erfordern.

Bereiten Sie sich auf das Upgrade vor

Bevor Sie beginnen

- Laden Sie die passende Broadcom EFOS-Software für Ihre Cluster-Switches von der Website herunter. "[Broadcom Ethernet-Switch-Unterstützung](#)" Website.
- Beachten Sie bitte die folgenden Hinweise zu den EFOS-Versionen.

Bitte beachten Sie Folgendes:

- Beim Upgrade von EFOS 3.4.xx auf EFOS 3.7.xx oder höher muss auf dem Switch EFOS 3.4.4.6 (oder eine spätere Version der 3.4.xx-Reihe) installiert sein. Wenn Sie eine ältere Version verwenden, aktualisieren Sie den Switch zuerst auf EFOS 3.4.4.6 (oder eine spätere Version der 3.4.xx-Reihe) und anschließend auf EFOS 3.7.xx oder höher.
- Die Konfigurationen für EFOS 3.4.xx und 3.7.xx oder höher sind unterschiedlich. Um die EFOS-Version von 3.4.xx auf 3.7.xx oder höher zu ändern oder umgekehrt, muss die Switch auf die Werkseinstellungen zurückgesetzt und die RCF-Dateien für die entsprechende EFOS-Version (erneut) angewendet werden. Für dieses Verfahren ist der Zugriff über die serielle Konsole erforderlich.
- Ab EFOS Version 3.7.xx oder höher ist eine nicht FIPS-konforme und eine FIPS-konforme Version verfügbar. Beim Wechsel von einer nicht FIPS-konformen zu einer FIPS-konformen Version oder umgekehrt sind unterschiedliche Schritte erforderlich. Durch den Wechsel von einer nicht FIPS-konformen EFOS-Version zu einer FIPS-konformen Version oder umgekehrt wird der Switch auf die Werkseinstellungen zurückgesetzt. Für dieses Verfahren ist der Zugriff über die serielle Konsole erforderlich.

Verfahren	Aktuelle EFOS -Version	Neue EFOS-Version	Hochrangige Schritte
Schritte zum Upgrade von EFOS zwischen zwei (nicht) FIPS-konformen Versionen	3.4.x.x	3.4.x.x	Aktualisieren Sie das neue EFOS-Image mit Methode 1: EFOS-Upgrade . Die Konfigurations- und Lizenzinformationen bleiben erhalten.
3.4.4.6 (oder später 3.4.xx)	3.7.xx oder später nicht FIPS-konform	EFOS aktualisieren mit Methode 1: EFOS-Upgrade . Die Setzen Sie den Switch auf die Werkseinstellungen zurück und wenden Sie die RCF-Datei für EFOS 3.7.xx oder höher an.	3.7.xx oder später nicht FIPS-konform
3.4.4.6 (oder später 3.4.xx)	EFOS downgraden mit Methode 1: EFOS-Upgrade . Die Setzen Sie den Switch auf die Werkseinstellungen zurück und wenden Sie die RCF-Datei für EFOS 3.4.xx an.	3.7.xx oder später nicht FIPS-konform	

Aktualisieren Sie das neue EFOS-Image mit Methode 1: EFOS-Upgrade . Die Konfigurations- und Lizenzinformationen bleiben erhalten.	3.7.xx oder höher FIPS-konform	3.7.xx oder höher FIPS-konform	Aktualisieren Sie das neue EFOS-Image mit Methode 1: EFOS-Upgrade . Die Konfigurations- und Lizenzinformationen bleiben erhalten.
Schritte zum Upgrade auf/von einer FIPS-konformen EFOS-Version	Nicht FIPS-konform	FIPS-konform	Aktualisierung des EFOS-Images mit Methode 2: EFOS mithilfe der ONIE OS-Installation aktualisieren . Die Switch-Konfiguration und die Lizenzinformationen gehen verloren.

Um zu überprüfen, ob Ihre EFOS-Version FIPS-konform oder nicht FIPS-konform ist, verwenden Sie die `show fips status` Befehl. In den folgenden Beispielen verwendet **IP_switch_a1** FIPS-konformes EFOS und **IP_switch_a2** verwendet nicht FIPS-konformes EFOS.

- Auf Switch IP_switch_a1 (FIPS-konformes EFOS):

```
IP_switch_a1 # show fips status
```

System running in FIPS mode

- Auf Switch IP_switch_a2 (nicht FIPS-konformes EFOS):

```
IP_switch_a2 # show fips status
```

^

% Invalid input detected at ^ marker.

Aktualisieren Sie die Software

Verwenden Sie eine der folgenden Methoden:

- [Methode 1: EFOS-Upgrade](#). Für die meisten Anwendungsfälle geeignet (siehe Tabelle oben).
- [Methode 2: EFOS mithilfe der ONIE OS-Installation aktualisieren](#). Verwenden Sie diese Option, wenn eine EFOS-Version FIPS-konform ist und die andere EFOS-Version nicht FIPS-konform ist.



Um den kontinuierlichen Betrieb des Clusternetzwerks zu gewährleisten, aktualisieren Sie EFOS auf jeweils einem Switch.

Methode 1: EFOS-Upgrade

Führen Sie die folgenden Schritte aus, um die EFOS-Software zu aktualisieren.



Bitte beachten Sie, dass nach dem Upgrade von BES-53248 Cluster-Switches von EFOS 3.3.xx oder 3.4.xx auf EFOS 3.7.0.4 oder 3.8.0.2 die Inter-Switch Links (ISLs) und Port-Channels im Status **Down** markiert sind. Dies ist das erwartete Verhalten, und Sie können das Upgrade bedenkenlos fortsetzen, es sei denn, Sie haben Probleme mit der automatischen Rücksetzung von LIFs. Siehe den Artikel in der Wissensdatenbank: "[BES-53248 Cluster Switch NDU konnte nicht auf EFOS 3.7.0.4 und höher aktualisiert werden.](#)" für weitere Einzelheiten.

Schritte

1. Verbinden Sie den Cluster-Switch BES-53248 mit dem Management-Netzwerk.
2. Verwenden Sie die `ping` Befehl zur Überprüfung der Verbindung zum Server, auf dem EFOS, Lizenzen und die RCF-Datei gehostet werden.

Dieses Beispiel überprüft, ob der Switch mit dem Server unter der IP-Adresse 172.19.2.1 verbunden ist:

```
(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. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

4. Anzeige der Startabbilder für die aktive und die Sicherungskonfiguration:

```
show bootvar
```

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1        3.7.0.4    3.4.4.6      3.7.0.4        3.7.0.4
```

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

Durch das Kopieren der Image-Datei in das Backup-Image wird beim Neustart die laufende EFOS-Version dieses Images erstellt und das Update abgeschlossen.

```
(cs2) # copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk backup
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.10.0.3.stk
Data Type..... Code
Destination Filename..... backup

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

File transfer operation completed successfully.
```

6. Anzeige der Startabbilder für die aktive und die Sicherungskonfiguration:

```
show bootvar
```

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1        3.7.0.4    3.10.0.3    3.7.0.4    3.10.0.3
```

7. Starten Sie das System von der Sicherungskonfiguration:

```
boot system backup
```

```
(cs2) # boot system backup
Activating image backup ..
```

8. Anzeige der Startabbilder für die aktive und die Sicherungskonfiguration:

```
show bootvar
```

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1        3.10.0.3    3.10.0.3    3.10.0.3    3.10.0.3
```

9. Die laufende Konfiguration in der Startkonfiguration speichern:

```
write memory
```

Beispiel anzeigen

```
(cs2) # write memory
```

```
This operation may take a few minutes.
```

```
Management interfaces will not be available during this time.
```

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

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

10. Starten Sie den Switch neu:

```
reload
```

Beispiel anzeigen

```
(cs2) # reload
```

```
The system has unsaved changes.
```

```
Would you like to save them now? (y/n) y
```

```
Config file 'startup-config' created successfully.
```

```
Configuration Saved!
```

```
System will now restart!
```

11. Melden Sie sich erneut an und überprüfen Sie die neue Version der EFOS-Software:

```
show version
```

Beispiel anzeigen

```
(cs2) # show version

Switch: 1

System Description..... BES-53248A1,
3.10.0.3, Linux 4.4.211-28a6fe76, 2016.05.00.04
Machine Type..... BES-53248A1,
Machine Model..... BES-53248
Serial Number..... QTFCU38260023
Maintenance Level..... A
Manufacturer..... 0xbc00
Burned In MAC Address..... D8:C4:97:71:0F:40
Software Version..... 3.10.0.3
Operating System..... Linux 4.4.211-
28a6fe76
Network Processing Device..... BCM56873_A0
CPLD Version..... 0xff040c03

Additional Packages..... BGP-4
..... QOS
..... Multicast
..... IPv6
..... Routing
..... Data Center
..... OpEN API
..... Prototype Open API
```

12. Wiederholen Sie die Schritte 5 bis 11 am Schalter cs1.
13. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

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

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

Weitere Einzelheiten finden Sie unter "[LIF zum Heimathafen zurückversetzen](#)" Die

Methode 2: EFOS mithilfe der ONIE OS-Installation aktualisieren

Die folgenden Schritte können Sie durchführen, wenn eine EFOS-Version FIPS-konform und die andere EFOS-Version nicht FIPS-konform ist. Diese Schritte können verwendet werden, um das Nicht-FIPS- oder FIPS-konforme EFOS 3.7.xx-Image von ONIE zu aktualisieren, falls der Switch nicht bootet.



Diese Funktionalität ist nur für EFOS 3.7.xx oder spätere, nicht FIPS-konforme Versionen verfügbar.



Wenn Sie EFOS mithilfe der ONIE OS-Installation aktualisieren, werden die Konfigurationen auf die Werkseinstellungen zurückgesetzt und die Lizenzen gelöscht. Sie müssen den Switch einrichten und Lizenzen sowie eine unterstützte RCF installieren, um den Switch wieder in den Normalbetrieb zu versetzen.

Schritte

1. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

2. Starten Sie den Switch im ONIE-Installationsmodus.

Wählen Sie während des Systemstarts ONIE aus, wenn die entsprechende Aufforderung angezeigt wird:

```
+-----+  
| EFOS |  
| *ONIE|  
|      |  
|      |  
|      |  
|      |  
|      |  
|      |  
|      |  
|      |  
|      |  
|      |  
+-----+
```

Nachdem Sie **ONIE** ausgewählt haben, lädt die Schaltfläche und zeigt Ihnen mehrere Optionen an. Wählen Sie **Betriebssystem installieren**.

```
+-----+  
| *ONIE: Install OS  
| ONIE: Rescue  
| ONIE: Uninstall OS  
| ONIE: Update ONIE  
| ONIE: Embed ONIE  
| DIAG: Diagnostic Mode  
| DIAG: Burn-In Mode  
|  
|  
|  
|  
|  
|  
+-----+
```

Der Switch startet im ONIE-Installationsmodus.

3. Beenden Sie die ONIE-Erkennung und konfigurieren Sie die Ethernet-Schnittstelle.

Wenn die folgende Meldung erscheint, drücken Sie **Enter**, um die ONIE-Konsole aufzurufen:

```
Please press Enter to activate this console. Info: eth0: Checking  
link... up.  
ONIE:/ #
```



Die ONIE-Erkennung wird fortgesetzt und Meldungen werden auf der Konsole ausgegeben.

```
Stop the ONIE discovery  
ONIE:/ # onie-discovery-stop  
discover: installer mode detected.  
Stopping: discover... done.  
ONIE:/ #
```

4. Konfigurieren Sie die Ethernet-Schnittstelle und fügen Sie die Route hinzu mit `ifconfig eth0 <ipAddress> netmask <netmask> up` Und `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up  
ONIE:/ # route add default gw 10.10.10.1
```

5. Überprüfen Sie, ob der Server, auf dem die ONIE-Installationsdatei gehostet wird, erreichbar ist:

`ping`

Beispiel anzeigen

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

6. Installieren Sie die neue Switch-Software:

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-installer-x86\_64
```

Beispiel anzeigen

```
ONIE:/ # onie-nos-install http://50.50.50.50/Software/onie-
installer-x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http://50.50.50.50/Software/onie-installer-3.7.0.4
...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer          100% |*****| 48841k
0:00:00 ETA
ONIE: Executing installer: http://50.50.50.50/Software/onie-
installer-3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Die Software installiert sich und startet den Switch anschließend neu. Lassen Sie den Switch normal in die neue EFOS-Version neu starten.

7. Überprüfen Sie, ob die neue Switch-Software installiert ist:

```
show bootvar
```

Beispiel anzeigen

```
(cs2) # show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
-----
unit    active      backup   current-active next-active
-----
1      3.7.0.4     3.7.0.4   3.7.0.4      3.10.0.3
(cs2) #
```

8. Schließen Sie die Installation ab. Der Switch startet ohne angewendete Konfiguration neu und wird auf die Werkseinstellungen zurückgesetzt. Führen Sie die folgenden Schritte aus, um den Switch neu zu konfigurieren:
 - a. "Lizenzen installieren"
 - b. "Installieren Sie den RCF"
 - c. "Aktivieren von SSH"
 - d. "Protokollerfassung aktivieren"
 - e. "SNMPv3 für die Überwachung konfigurieren"
9. Wiederholen Sie die Schritte 2 bis 8 am Schalter cs1.
10. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

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

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

Weitere Einzelheiten finden Sie unter "[LIF zum Heimathafen zurückversetzen](#)". Die

Aktualisieren Sie die Referenzkonfigurationsdatei (RCF)

Sie können die Referenzkonfigurationsdatei (RCF) aktualisieren, nachdem Sie das EFOS des BES-53248 Cluster-Switches aktualisiert und alle neuen Lizenzen angewendet haben.

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).
- Die aktuelle RCF-Datei ist verfügbar unter "[Broadcom Cluster-Switches](#)" Seite.
- Eine Bootkonfiguration in der RCF-Datei, die die gewünschten Boot-Images widerspiegelt, ist erforderlich, wenn Sie nur EFOS installieren und Ihre aktuelle RCF-Version beibehalten. 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.
- Eine Konsolenverbindung zum Switch ist erforderlich, wenn der RCF aus dem Werkszustand installiert wird. Diese Anforderung ist optional, wenn Sie den Wissensdatenbank-Artikel verwendet haben. "[Wie man die Konfiguration eines Broadcom-Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält](#)" Um die Konfiguration vorher zu löschen.

Empfohlene Dokumentation

- In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und RCF-Versionen. Siehe die "[EFOS-Software-Download](#)" Seite. Beachten Sie, dass zwischen der Befehlssyntax in der RCF und der in EFOS-Versionen vorhandenen Befehlssyntax Abhängigkeiten bestehen können.
- Beachten Sie die entsprechenden Software- und Upgrade-Anleitungen, die auf der Website verfügbar sind. "[Broadcom](#)" Auf dieser Website finden Sie die vollständige Dokumentation zu den Upgrade- und Downgrade-Verfahren des BES-53248-Switches.

Zu den Beispielen

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

- Die beiden BES-53248-Switches tragen die Bezeichnungen cs1 und cs2.
- Die Knotennamen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1 und cluster1-04_clus2.
- Der `cluster1::*` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Beispiele in diesem Verfahren verwenden vier Knoten. Diese Knoten nutzen zwei 10GbE-Cluster-Verbindungsports. e0a Und e0b Die Siehe die "[Hardware Universe](#)" um die korrekten Cluster-Ports auf Ihren Plattformen zu überprüfen.



Die Befehlsausgaben können je nach ONTAP Version variieren.

Informationen zu diesem Vorgang

Für dieses Verfahren müssen sowohl ONTAP -Befehle als auch Broadcom-Switch-Befehle verwendet werden; 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 gewährleisten, migriert das folgende Verfahren alle Cluster-LIFs zum operativen Partner-Switch, während die Schritte auf dem Ziel-Switch ausgeführt werden.



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, lesen Sie bitte den Knowledge-Base-Artikel. "[Wie man die Konfiguration eines Broadcom-Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält](#)" Die Wenn Sie die Schaltereinstellungen vollständig löschen müssen, müssen Sie die Grundkonfiguration erneut durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein, da eine vollständige Konfigurationslöschung die Konfiguration des Management-Netzwerks zurücksetzt.

Schritt 1: Vorbereitung auf das Upgrade

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

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

wobei x die Dauer des Wartungsfensters in Stunden ist.



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

Der folgende Befehl unterdrückt die automatische Fallerstellung für zwei Stunden:

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

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

```
set -privilege advanced
```

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

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          0/2        BES-
53248
      e0b    cs2          0/2        BES-
53248
cluster1-02/cdp
      e0a    cs1          0/1        BES-
53248
      e0b    cs2          0/1        BES-
53248
cluster1-03/cdp
      e0a    cs1          0/4        BES-
53248
      e0b    cs2          0/4        BES-
53248
cluster1-04/cdp
      e0a    cs1          0/3        BES-
53248
      e0b    cs2          0/3        BES-
53248
cluster1::*
```

4. 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
e0b      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
e0b      Cluster      Cluster          up    9000  auto/100000
healthy false
8 entries were displayed.

Node: cluster1-03

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

```
Node: cluster1-04
```

```
Ignore
```

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

```
cluster1::*>
```

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

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

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
      Logical          Status      Network
Current   Current  Is
Vserver    Interface           Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
      cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a      true
      cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0b      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  e0b      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
```

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

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie folgenden Befehl:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
	Serial Number: QTWCU22510008		
	Is Monitored: true		
	Reason: None		
	Software Version: 3.10.0.3		
	Version Source: CDP/ISDP		
cs2	cluster-network	10.228.143.202	BES-
53248			
	Serial Number: QTWCU22510009		
	Is Monitored: true		
	Reason: None		
	Software Version: 3.10.0.3		
	Version Source: CDP/ISDP		

```
cluster1::*>
```

ONTAP 9.7 und früher

Für ONTAP 9.7 und ältere Versionen verwenden Sie folgenden Befehl:

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

```

cluster1::*> system cluster-switch show -is-monitoring-enabled
- operational true
Switch Type Address Model
-----
-----
cs1 cluster-network 10.228.143.200 BES-
53248
    Serial Number: QTWCU22510008
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP

cs2 cluster-network 10.228.143.202 BES-
53248
    Serial Number: QTWCU22510009
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP
cluster1::*>

```

1. Automatische Rücksetzung der Cluster-LIFs deaktivieren.

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

Schritt 2: Ports konfigurieren

1. Überprüfen Sie auf Switch cs2 die Liste der Ports, die mit den Knoten im Cluster verbunden sind.

```
show isdp neighbor
```

2. Schalten Sie auf Switch cs2 die Ports ab, die mit den Cluster-Ports der Knoten verbunden sind. Wenn beispielsweise die Ports 0/1 bis 0/16 mit ONTAP Knoten verbunden sind:

```

(cs2)> enable
(cs2)# configure
(cs2)(Config)# interface 0/1-0/16
(cs2)(Interface 0/1-0/16)# shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#

```

3. Überprüfen Sie, ob die Cluster-LIFs auf die Ports migriert wurden, die auf dem Cluster-Switch cs1 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   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::*
```

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
```

5. Falls noch nicht geschehen, speichern Sie die aktuelle Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Protokolldatei kopieren:

```
show running-config
```

6. Bereinigen Sie die Konfiguration auf Switch CS2 und führen Sie eine grundlegende Einrichtung durch.



Beim Aktualisieren oder Anwenden eines neuen RCF müssen Sie die Schaltereinstellungen löschen und eine grundlegende Konfiguration durchführen. Um die Switch-Einstellungen zu löschen, müssen Sie über die serielle Konsole mit dem Switch verbunden sein. Diese Anforderung ist optional, wenn Sie den Wissensdatenbank-Artikel verwendet haben. ["Wie man die Konfiguration eines Broadcom-Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält"](#) Um die Konfiguration vorher zu löschen.



Das Löschen der Konfiguration führt nicht zum Löschen der Lizenzien.

- a. Stellen Sie eine SSH-Verbindung zum Switch her.

Fahren Sie erst fort, wenn alle Cluster-LIFs von den Ports des Switches entfernt wurden und der Switch bereit ist, die Konfiguration zu löschen.

- b. Privilegierten Modus aktivieren:

```
(cs2)> enable
(cs2) #
```

- c. Kopieren Sie die folgenden Befehle und fügen Sie sie ein, um die vorherige RCF-Konfiguration zu entfernen (abhängig von der zuvor verwendeten RCF-Version können einige Befehle einen Fehler erzeugen, wenn eine bestimmte Einstellung nicht vorhanden ist):

```
clear config interface 0/1-0/56
Y
clear config interface lag 1
Y
```

```

configure
deleteport 1/1 all
no policy-map CLUSTER
no policy-map WRED_25G
no policy-map WRED_100G
no policy-map InShared
no policy-map InMetroCluster
no policy-map InCluster
no policy-map InClusterRdma
no class-map CLUSTER
no class-map HA
no class-map RDMA
no class-map c5
no class-map c4
no class-map CLUSTER
no class-map CLUSTER_RDMA
no class-map StorageSrc
no class-map StorageDst
no class-map RdmaSrc
no class-map RdmaDstA
no classofservice dot1p-mapping
no random-detect queue-parms 0
no random-detect queue-parms 1
no random-detect queue-parms 2
no random-detect queue-parms 3
no random-detect queue-parms 4
no random-detect queue-parms 5
no random-detect queue-parms 6
no random-detect queue-parms 7
no cos-queue min-bandwidth
no cos-queue random-detect 0
no cos-queue random-detect 1
no cos-queue random-detect 2
no cos-queue random-detect 3
no cos-queue random-detect 4
no cos-queue random-detect 5
no cos-queue random-detect 6
no cos-queue random-detect 7
exit
vlan database
no vlan 17
no vlan 18
exit
show running-config

```

d. Die laufende Konfiguration in der Startkonfiguration speichern:

```
write memory
```

```
(cs2)# write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.

Configuration Saved!

- e. Führen Sie einen Neustart des Switches durch:

```
reload
```

```
(cs2)# reload
```

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

- a. Melden Sie sich erneut per SSH am Switch an, um die RCF-Installation abzuschließen.

7. Beachten Sie Folgendes:

- a. Falls zusätzliche Portlizenzen auf dem Switch installiert wurden, müssen Sie die RCF-Datei ändern, um die zusätzlichen lizenzierten Ports zu konfigurieren. Sehen "["Aktivieren Sie neu lizenzierte Ports"](#)" für weitere Details. Wenn Sie jedoch auf RCF 1.12 oder höher aktualisieren, sind die Änderungen nicht mehr erforderlich, da alle Schnittstellen jetzt vorkonfiguriert sind.
- b. Alle im vorherigen RCF vorgenommenen Anpassungen sollten protokolliert und auf das neue RCF angewendet werden. Zum Beispiel durch Festlegen von Portgeschwindigkeiten oder durch Festcodieren des FEC-Modus.

EFOS Version 3.12.x und höher

1. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs2: HTTP, HTTPS, FTP, TFTP, SFTP oder SCP.

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

```
(cs2) # copy sftp://172.19.2.1/BES-53248-RCF-v1.9-Cluster-HA.txt  
nvram:reference-config  
Remote Password:**  
Mode..... TFTP  
Set Server IP..... 172.19.2.1  
Path..... /  
Filename..... BES-53248_RCF_v1.9-  
Cluster-HA.txt  
Data Type..... Config Script  
Destination Filename..... reference-config.scr  
Management access will be blocked for the duration of the transfer  
Are you sure you want to start? (y/n) y  
TFTP Code transfer starting...  
File transfer operation completed successfully.
```

1. Überprüfen Sie, ob das Skript heruntergeladen und unter dem von Ihnen angegebenen Dateinamen gespeichert wurde:

```
script list
```

```
(cs2) # script list  
  
Configuration Script Name          Size (Bytes)  Date of  
Modification  
-----  
-----  
reference-config.scr           2680        2024 05 31  
21:54:22  
2 configuration script(s) found.  
2042 Kbytes free.
```

2. Wenden Sie das Skript auf den Schalter an:

```
script apply
```

```
(cs2) # script apply reference-config.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'reference-config.scr' applied.
```

Alle anderen EFOS-Versionen

1. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs2: HTTP, HTTPS, FTP, TFTP, SFTP oder SCP.

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

```
(cs2) # copy sftp://172.19.2.1/tmp/BES-53248_RCF_v1.9-Cluster-HA.txt
nvrarn:script BES-53248_RCF_v1.9-Cluster-HA.scr
Remote Password:**
Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... BES-53248_RCF_v1.9-
Cluster-HA.txt
Data Type..... Config Script
Destination Filename..... BES-53248_RCF_v1.9-
Cluster-HA.scr
Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
SFTP Code transfer starting...
File transfer operation completed successfully.
```

1. Überprüfen Sie, ob das Skript heruntergeladen und unter dem von Ihnen angegebenen Dateinamen gespeichert wurde:

```
script list
```

```
(cs2) # script list

Configuration Script Name          Size (Bytes) Date of
Modification

-----
-----  

BES-53248_RCF_v1.9-Cluster-HA.scr      2241        2020 09 30
05:41:00

1 configuration script(s) found.
```

2. Wenden Sie das Skript auf den Schalter an:

```
script apply
```

```
(cs2) # script apply BES-53248_RCF_v1.9-Cluster-HA.scr

Are you sure you want to apply the configuration script? (y/n) y

The system has unsaved changes.
Would you like to save them now? (y/n) y
Config file 'startup-config' created successfully.
Configuration Saved!

Configuration script 'BES-53248_RCF_v1.9-Cluster-HA.scr' applied.
```

1. Untersuchen Sie die Bannerausgabe von der `show clibanner` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um die ordnungsgemäße Konfiguration und den ordnungsgemäßen Betrieb des Switches sicherzustellen.

```
show clibanner
```

Beispiel anzeigen

```
(cs2) # show clibanner

Banner Message configured :
=====
BES-53248 Reference Configuration File v1.9 for Cluster/HA/RDMA

Switch      : BES-53248
Filename   : BES-53248-RCF-v1.9-Cluster.txt
Date       : 10-26-2022
Version    : v1.9
Port Usage:
Ports 01 - 16: 10/25GbE Cluster Node Ports, base config
Ports 17 - 48: 10/25GbE Cluster Node Ports, with licenses
Ports 49 - 54: 40/100GbE Cluster Node Ports, with licenses, added
right to left
Ports 55 - 56: 100GbE Cluster ISL Ports, base config
NOTE:
- The 48 SFP28/SFP+ ports are organized into 4-port groups in terms
of port
speed:
Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-
40, 41-44,
45-48
The port speed should be the same (10GbE or 25GbE) across all ports
in a 4-port
group
- If additional licenses are purchased, follow the 'Additional Node
Ports
activated with Licenses' section for instructions
- If SSH is active, it will have to be re-enabled manually after
'erase
startup-config'
command has been executed and the switch rebooted
```

2. Überprüfen Sie am Switch, ob die zusätzlichen lizenzierten Ports nach der Anwendung des RCF angezeigt werden:

```
show port all | exclude Detach
```

Beispiel anzeigen

```
(cs2)# show port all | exclude Detach
```

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					
0/1	Enable long	Enable	Auto		Down	Enable
0/2	Enable long	Enable	Auto		Down	Enable
0/3	Enable long	Enable	Auto		Down	Enable
0/4	Enable long	Enable	Auto		Down	Enable
0/5	Enable long	Enable	Auto		Down	Enable
0/6	Enable long	Enable	Auto		Down	Enable
0/7	Enable long	Enable	Auto		Down	Enable
0/8	Enable long	Enable	Auto		Down	Enable
0/9	Enable long	Enable	Auto		Down	Enable
0/10	Enable long	Enable	Auto		Down	Enable
0/11	Enable long	Enable	Auto		Down	Enable
0/12	Enable long	Enable	Auto		Down	Enable
0/13	Enable long	Enable	Auto		Down	Enable
0/14	Enable long	Enable	Auto		Down	Enable
0/15	Enable long	Enable	Auto		Down	Enable
0/16	Enable long	Enable	Auto		Down	Enable
0/49	Enable long	Enable	40G Full		Down	Enable
0/50	Enable long	Enable	40G Full		Down	Enable

0/51	Enable	100G Full	Down	Enable
Enable long				
0/52	Enable	100G Full	Down	Enable
Enable long				
0/53	Enable	100G Full	Down	Enable
Enable long				
0/54	Enable	100G Full	Down	Enable
Enable long				
0/55	Enable	100G Full	Down	Enable
Enable long				
0/56	Enable	100G Full	Down	Enable
Enable long				

3. Überprüfen Sie am Switch, ob Ihre Änderungen vorgenommen wurden.

```
show running-config
```

4. Speichern Sie die laufende Konfiguration, damit sie beim Neustart des Switches als Startkonfiguration verwendet wird:

```
write memory
```

Beispiel anzeigen

```
(cs2) # write memory
This operation may take a few minutes.
Management interfaces will not be available during this time.

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

Config file 'startup-config' created successfully.
Configuration Saved!
```

5. Starten Sie den Switch neu und überprüfen Sie, ob die laufende Konfiguration korrekt ist.

```
reload
```

```
(cs2) # reload
Are you sure you would like to reset the system? (y/n) y
System will now restart!
```

6. Auf dem Cluster-Switch cs2 werden die mit den Cluster-Ports der Knoten verbundenen Ports aktiviert.

```
(cs2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/16
(cs2) (Interface 0/1-0/16)# no shutdown
(cs2) (Config)# exit
```

7. Die laufende Konfiguration in der Startkonfiguration speichern:

```
write memory
```

Beispiel anzeigen

```
(cs2)# write memory

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

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

Config file 'startup-config' created successfully.
Configuration Saved!
```

8. Überprüfen Sie die Ports am Switch CS2:

```
show interfaces status all | exclude Detach
```

Beispiel anzeigen

```
(cs1)# show interfaces status all | exclude Detach

Link      Physical      Physical
Media     Flow
Port      Name          State   Mode    Status   Type
Control   VLAN
-----  -----
-----  -----  -----  -----  -----  -----
.
.
.
0/16      10/25GbE Node Port   Down   Auto
Inactive   Trunk
0/17      10/25GbE Node Port   Down   Auto
Inactive   Trunk
0/18      10/25GbE Node Port   Up     25G Full  25G Full
25GBase-SR Inactive   Trunk
0/19      10/25GbE Node Port   Up     25G Full  25G Full
25GBase-SR Inactive   Trunk
.
.
.
0/50      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/51      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/52      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/53      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/54      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/55      Cluster   ISL Port   Up     Auto    100G Full
Copper    Inactive   Trunk
0/56      Cluster   ISL Port   Up     Auto    100G Full
Copper    Inactive   Trunk
```

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

a. Überprüfen Sie, ob die e0b-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
e0b      Cluster        Cluster          up    9000  auto/100000
healthy false
```

```
Node: cluster1-04
```

```
Ignore
```

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

b. Überprüfen Sie den Zustand der Switches im Cluster:

```
network device-discovery show
```

Beispiel anzeigen

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

-----
-----
cluster1-01/cdp
      e0a     cs1          0/2
BES-53248
      e0b     cs2          0/2
BES-53248
cluster01-2/cdp
      e0a     cs1          0/1
BES-53248
      e0b     cs2          0/1
BES-53248
cluster01-3/cdp
      e0a     cs1          0/4
BES-53248
      e0b     cs2          0/4
BES-53248
cluster1-04/cdp
      e0a     cs1          0/3
BES-53248
      e0b     cs2          0/2
BES-53248
```

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

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie folgenden Befehl:

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

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

Switch	Type	Address	Model
cs1	cluster-network	10.228.143.200	BES-
53248			
	Serial Number: QTWCU22510008		
	Is Monitored: true		
	Reason: None		
	Software Version: 3.10.0.3		
	Version Source: CDP/ISDP		
cs2	cluster-network	10.228.143.202	BES-
53248			
	Serial Number: QTWCU22510009		
	Is Monitored: true		
	Reason: None		
	Software Version: 3.10.0.3		
	Version Source: CDP/ISDP		

```
cluster1::*>
```

ONTAP 9.7 und früher

Für ONTAP 9.7 und ältere Versionen verwenden Sie folgenden Befehl:

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

```

cluster1::*> system cluster-switch show -is-monitoring-enabled
- operational true
Switch Type Address Model
-----
-----
cs1 cluster-network 10.228.143.200 BES-
53248
    Serial Number: QTWCU22510008
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP

cs2 cluster-network 10.228.143.202 BES-
53248
    Serial Number: QTWCU22510009
    Is Monitored: true
    Reason: None
    Software Version: 3.10.0.3
    Version Source: CDP/ISDP
cluster1::*>

```

1. Wiederholen Sie die Schritte 1 bis 20 auf dem Schalter cs1.
2. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

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

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

Weitere Einzelheiten finden Sie unter "[LIF zum Heimathafen zurückversetzen](#)". Die

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie am Switch cs1, ob die mit den Cluster-Ports verbundenen Switch-Ports **aktiv** sind:

```
show interfaces status all
```

Beispiel anzeigen

```
(cs1)# show interfaces status all | exclude Detach

Link      Physical      Physical
Media     Flow
Port      Name          State   Mode    Status   Type
Control   VLAN
-----  -----
-----  -----  -----
.
.
.
0/16      10/25GbE Node Port   Down   Auto
Inactive   Trunk
0/17      10/25GbE Node Port   Down   Auto
Inactive   Trunk
0/18      10/25GbE Node Port   Up     25G Full  25G Full
25GBase-SR Inactive   Trunk
0/19      10/25GbE Node Port   Up     25G Full  25G Full
25GBase-SR Inactive   Trunk
.
.
.
0/50      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/51      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/52      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/53      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/54      40/100GbE Node Port  Down   Auto
Inactive   Trunk
0/55      Cluster   ISL Port   Up     Auto    100G Full
Copper    Inactive   Trunk
0/56      Cluster   ISL Port   Up     Auto    100G Full
Copper    Inactive   Trunk
```

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

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

Beispiel anzeigen

```
(cs1)# show port-channel 1/1
Local Interface..... 1/1
Channel Name..... Cluster-ISL
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Port-channel Min-links..... 1
Load Balance Option..... 7
(Enhanced hashing mode)
Mbr Device/ Port Port
Ports Timeout Speed Active
-----
0/55 actor/long Auto True
      partner/long
0/56 actor/long Auto True
      partner/long
```

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         e0a        true
  cluster1-01_clus2  up/up      169.254.3.5/23
  cluster1-01         e0b        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         e0b        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
```

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
```

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 cluster01-  
02_clus1 none  
3/5/2022 19:21:20 -06:00 cluster1-01_clus2 cluster01-  
02_clus2 none  
  
cluster1-02  
3/5/2022 19:21:18 -06:00 cluster1-02_clus2 cluster1-02_clus1  
none  
3/5/2022 19:21:20 -06:00 cluster1-02_clus2 cluster1-02_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 cluster1-03
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 e0b
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
  Local 169.254.1.3 to Remote 169.254.1.6
  Local 169.254.1.3 to Remote 169.254.1.7
  Local 169.254.1.3 to Remote 169.254.3.4
  Local 169.254.1.3 to Remote 169.254.3.5
  Local 169.254.1.3 to Remote 169.254.3.8
  Local 169.254.1.3 to Remote 169.254.3.9
  Local 169.254.1.1 to Remote 169.254.1.6
  Local 169.254.1.1 to Remote 169.254.1.7
  Local 169.254.1.1 to Remote 169.254.3.4
  Local 169.254.1.1 to Remote 169.254.3.5
  Local 169.254.1.1 to Remote 169.254.3.8
  Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
  6 paths up, 0 paths down (tcp check)
  6 paths up, 0 paths down (udp check)

```

1. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

```
set -privilege admin
```

2. Wenn Sie die automatische Fehlerstellung unterdrückt haben, können Sie sie durch Aufruf einer

AutoSupport Nachricht wieder aktivieren:

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

Überprüfen Sie das ONTAP Clusternetzwerk nach einem EFOS-Software- oder RCF-Upgrade der BES-53248-Cluster-Switches.

Mit den folgenden Befehlen können Sie den Zustand des ONTAP -Clusternetzwerks nach einem Upgrade der EFOS-Software oder des RCF für BES-53248-Cluster-Switches überprüfen.

Schritte

1. Informationen zu den Netzwerkports des Clusters können mit folgendem Befehl angezeigt werden:

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

Link muss den Wert haben `up Und Health Status muss sein healthy Die

Beispiel anzeigen

Das folgende Beispiel zeigt die Ausgabe des Befehls:

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

Node: node1

Ignore                                         Speed (Mbps)  Health
Health
Port    IPspace      Broadcast  Domain  Link  MTU  Admin/Oper  Status
Status

-----
-----  

e0a    Cluster      Cluster        up     9000  auto/10000 healthy
false
e0b    Cluster      Cluster        up     9000  auto/10000 healthy
false

Node: node2

Ignore                                         Speed (Mbps)  Health
Health
Port    IPspace      Broadcast  Domain  Link  MTU  Admin/Oper  Status
Status

-----
-----  

e0a    Cluster      Cluster        up     9000  auto/10000 healthy
false
e0b    Cluster      Cluster        up     9000  auto/10000 healthy
false
```

2. Überprüfen Sie für jeden LIF, ob Is Home Ist true Und status Admin/Oper Ist up auf beiden Knoten mit folgendem Befehl:

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

Beispiel anzeigen

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

          Logical      Status      Network      Current
Current Is
Vserver      Interface Admin/Oper Address/Mask      Node
Port       Home
-----  -----  -----  -----
-----  ----
Cluster
          node1_clus1  up/up    169.254.217.125/16 node1
e0a        true
          node1_clus2  up/up    169.254.205.88/16 node1
e0b        true
          node2_clus1  up/up    169.254.252.125/16 node2
e0a        true
          node2_clus2  up/up    169.254.110.131/16 node2
e0b        true
```

3. Überprüfen Sie, ob die Health Status jedes Knotens ist true mit dem Befehl:

```
cluster show
```

Beispiel anzeigen

```
cluster1::> cluster show

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

Wie geht es weiter?

Nachdem Sie das Upgrade Ihrer EFOS-Software oder Ihres RCF bestätigt haben, können Sie "[Konfigurieren der Switch-Integritätsüberwachung](#)" 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, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDERWEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

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

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

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

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

Markeninformationen

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