Cluster-Switches

Install and maintain

NetApp
February 06, 2026

Inhalt

Cluster-Switches

Broadcom-unterstützter BES-53248

Erste Schritte

Installations- und Einrichtungsablauf für BES-53248-Switches

Der BES-53248 ist ein Bare-Metal-Switch, der für den Einsatz in ONTAP Clustern mit zwei bis 24 Knoten konzipiert ist.

Befolgen Sie diese Arbeitsschritte, um Ihre BES-53248-Switches zu installieren und einzurichten.

1. **"Überprüfen der Konfigurationsanforderungen"**
Prüfen Sie die Konfigurationsanforderungen für den Cluster-Switch BES-53248.

2. **"Überprüfen Sie die Komponenten und Teilenummern"**
Überprüfen Sie die Komponenten und Teilenummern für den Cluster-Switch BES-53248.

3. **"Überprüfen Sie die erforderlichen Unterlagen"**
Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre BES-53248-Switches und den ONTAP Cluster einzurichten.

4. **"Installieren Sie die Hardware"**
Installieren Sie die Switch-Hardware.

5. **"Konfigurieren der Software"**
Konfigurieren Sie die Switch-Software.

Konfigurationsanforderungen für BES-53248 Cluster-Switches

Bei der Installation und Wartung des BES-53248-Switches sollten Sie unbedingt die Support- und Konfigurationsanforderungen für EFOS und ONTAP beachten.

EFOS- und ONTAP Unterstützung

Siehe die "NetApp Hardware Universe" Und "Broadcom-Switch-Kompatibilitätsmatrix" Informationen zur Kompatibilität von EFOS und ONTAP mit BES-53248-Switches finden Sie hier. Die Unterstützung von EFOS und ONTAP kann je nach Maschinentyp des BES-53248-Switches variieren. Einzelheiten zu allen Weichenmaschinentypen des Typs BES-52348 finden Sie unter"Komponenten und Teilenummern für BES-53248 Cluster-Schalter" Die Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?"^ Weitere Informationen zu den Installationsanforderungen des

Schalters finden Sie hier.

Konfigurationsanforderungen

Zur Konfiguration eines Clusters benötigen Sie die entsprechende Anzahl und Art von Kabeln und Kabelverbindern für die Cluster-Switches. Je nachdem, welchen Cluster-Switch Sie initial konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Konsolenport des Switches herstellen.

Portzuweisungen für Cluster-Switches

Die von Broadcom unterstützte Tabelle der Portzuweisungen für den BES-53248 Cluster-Switch kann als Leitfaden für die Konfiguration Ihres Clusters verwendet werden.

Switch-Ports	Portnutzung
01-16	10/25GbE-Cluster-Portknoten, Basiskonfiguration
17-48	10/25GbE-Cluster-Portknoten mit Lizenzen
49-54	40/100GbE-Cluster-Portknoten mit Lizenzen, hinzugefügt von rechts nach links
55-56	100GbE-Cluster-Inter-Switch-Link (ISL)-Ports, Basiskonfiguration

Siehe die "Hardware Universe" Weitere Informationen zu Switch-Ports finden Sie hier. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

Geschwindigkeitsbeschränkung der Portgruppe

- Bei den Cluster-Switches BES-53248 sind die 48 10/25GbE (SFP28/SFP+)-Ports in 12 x 4-Port-Gruppen wie folgt zusammengefasst: Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 und 45-48.
- Die SFP28/SFP+-Portgeschwindigkeit muss bei allen Ports der 4-Port-Gruppe gleich sein (10GbE oder 25GbE).

Zusätzliche Anforderungen

- Wenn Sie zusätzliche Lizenzen erwerben, siehe"Aktivieren Sie neu lizenzierte Ports" Einzelheiten zur Aktivierung finden Sie dort.
- Wenn SSH aktiv ist, müssen Sie es nach Ausführung des Befehls manuell wieder aktivieren. `erase startup-config` und den Switch neu starten.

Was kommt als nächstes

Nachdem Sie die Konfigurationsanforderungen geprüft haben, können Sie Ihre "Komponenten und Teilenummern"Die

Komponenten und Teilenummern für BES-53248 Cluster-Schalter

Für die Installation und Wartung des Schalters BES-53248 sollten Sie unbedingt die Liste der Komponenten und Teilenummern überprüfen.

Die folgende Tabelle listet die Teilenummer, die Beschreibung und die minimalen EFOS- und ONTAP Versionen für die Cluster-Switch-Komponenten BES-53248 auf, einschließlich Details zum Rack-Montage-Schienensatz.

Für die Teilenummern **X190005-B** und **X190005R-B** ist mindestens die EFOS-Version **3.10.0.3** erforderlich.

Teilenummer	Beschreibung	Mindestversion von EFOS	Mindestversion von ONTAP
X190005-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX = Backbordseitiger Auslass)	3.10.0.3	9,8
X190005R-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PSIN (PSIN = Port Side Intake)	3.10.0.3	9,8
X190005	BES-53248, CLSW, 16Pt10/25GB, PTSX, BRDCM SUPP	3.4.4.6	9.5P8
X190005R	BES-53248, CLSW, 16Pt10/25GB, PSIN, BRDCM SUPP	3.4.4.6	9.5P8
X-RAIL-4POST-190005	Ozeki 4-Pfosten-Rack-Montagesatz 19"	k. A.	k. A.

Beachten Sie bitte folgende Informationen zu den Maschinentypen:

Maschinentyp	Mindestversion von EFOS
BES-53248A1	3.4.4.6
BES-53248A2	3.10.0.3
BES-53248A3	3.10.0.3

Sie können Ihren spezifischen Maschinentyp mit folgendem Befehl ermitteln: `show version`

Beispiel anzeigen

```
(cs1)# show version

Switch: cs1

System Description.............................. EFOS, 3.10.0.3, Linux
5.4.2-b4581018, 2016.05.00.07
Machine Type.................................... BES-53248A3
Machine Model................................... BES-53248
Serial Number................................... QTWCU225xxxxx
Part Number..................................... 1IX8BZxxxxx
Maintenance Level............................... a3a
Manufacturer.................................... QTMC
Burned In MAC Address........................... C0:18:50:F4:3x:xx
Software Version................................ 3.10.0.3
Operating System................................ Linux 5.4.2-b4581018
Network Processing Device....................... BCM56873_A0
.
.
.
```

Was kommt als nächstes

Nachdem Sie Ihre Komponenten und Teilenummern bestätigt haben, können Sie die folgenden überprüfen: "erforderliche Dokumentation"Die

Dokumentationsanforderungen für BES-53248 Cluster-Switches

Für die Installation und Wartung des BES-53248-Switches sollten Sie unbedingt die spezifische Dokumentation des Switches und des Controllers beachten.

Broadcom-Dokumentation

Für die Einrichtung des Cluster-Switches BES-53248 benötigen Sie die folgenden Dokumente, die auf der Broadcom-Support-Website verfügbar sind: "Broadcom Ethernet-Switch-Produktlinie"

Dokumenttitel	Beschreibung
EFOS-Administratorhandbuch v3.4.3	Liefert Beispiele für die Verwendung des BES-53248-Switches in einem typischen Netzwerk.
EFOS CLI-Befehlsreferenz v3.4.3	Beschreibt die Befehle der Kommandozeilenschnittstelle (CLI), die Sie zum Anzeigen und Konfigurieren der BES-53248-Software verwenden.
EFOS-Einführungsleitfaden v3.4.3	Bietet detaillierte Informationen zum BES-53248-Switch.

Dokumenttitel	Beschreibung
EFOS SNMP-Referenzhandbuch v3.4.3	Liefert Beispiele für die Verwendung des BES-53248-Switches in einem typischen Netzwerk.
EFOS-Skalierungsparameter und -werte v3.4.3	Beschreibt die Standard-Skalierungsparameter, mit denen die EFOS-Software ausgeliefert und auf den unterstützten Plattformen validiert wird.
EFOS-Funktionsspezifikationen v3.4.3	Beschreibt die Spezifikationen der EFOS-Software auf den unterstützten Plattformen.
EFOS Versionshinweise v3.4.3	Bietet versionsspezifische Informationen zur BES-53248-Software.
Kompatibilitätsmatrix für Clusternetzwerke und Managementnetzwerke	Liefert Informationen zur Netzwerkkompatibilität. Die Matrix ist auf der Downloadseite des BES-53248-Switches verfügbar unter "Broadcom-Cluster-Switches" Die

Dokumentation und Wissensdatenbankartikel zu ONTAP Systemen

Um ein ONTAP -System einzurichten, benötigen Sie die folgenden Dokumente von der NetApp Support-Website unter "mysupport.netapp.com" oder die Wissensdatenbank (KB)-Website unter "kb.netapp.com" Die

Name	Beschreibung
"NetApp Hardware Universe"	Beschreibt die Stromversorgungs- und Standortanforderungen für die gesamte NetApp Hardware, einschließlich der Systemschränke, und liefert Informationen zu den relevanten Steckverbindern und Kabeloptionen sowie deren Teilenummern.
Controllerspezifische *Installations- und Einrichtungsanweisungen*	Beschreibt die Installation von NetApp -Hardware.
ONTAP 9	Bietet detaillierte Informationen zu allen Aspekten der ONTAP 9-Version.
So fügen Sie zusätzliche Portlizenzen für den Broadcom-unterstützten BES-53248-Switch hinzu	Bietet detaillierte Informationen zum Hinzufügen von Portlizenzen. Gehe zu "KB-Artikel" Die

Installieren Sie die Hardware

Workflow zur Hardwareinstallation für BES-53248-Switches

Um die Hardware für einen BES-53248-Cluster-Switch zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

1 **"Installieren Sie die Switch-Hardware"**

Installieren und konfigurieren Sie die BES-53248-Switch-Hardware.

2 **"Kabel und Konfiguration prüfen"**

Überprüfen Sie die Verkabelungs- und Konfigurationshinweise für den Cluster-Switch BES-53248.

Installieren Sie die Hardware für den Cluster-Switch BES-53248.

Informationen zur Installation der BES-53248-Hardware finden Sie in der Dokumentation von Broadcom.

Schritte

1. Überprüfen Sie die"Konfigurationsanforderungen" Die
2. Befolgen Sie die Anweisungen in der "Installationsanleitung für den von Broadcom unterstützten BES-53248 Cluster-Switch" Die

Wie geht es weiter?

Nachdem Sie die Hardware für den Switch installiert haben, können Sie "Verkabelung und Konfiguration überprüfen" Anforderungen.

Überprüfung der Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Broadcom BES-53248 Switch konfigurieren, beachten Sie bitte die folgenden Hinweise.

Cluster-Port-Switch-Zuweisungen

Sie können die von Broadcom unterstützte Tabelle der Portzuweisungen für den BES-53248 Cluster-Switch als Leitfaden für die Konfiguration Ihres Clusters verwenden.

Switch-Ports	Portnutzung
0-16	10/25GbE-Cluster-Portknoten, Basiskonfiguration
17-48	10/25GbE-Cluster-Portknoten mit Lizenzen
49-54	40/100GbE-Cluster-Portknoten mit Lizenzen, hinzugefügt von rechts nach links
55-56	100GbE-Cluster-Inter-Switch-Link (ISL)-Ports, Basiskonfiguration

Siehe die "Hardware Universe" Weitere Informationen zu Switch-Ports finden Sie hier. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

Geschwindigkeitsbeschränkung der Portgruppe

- Bei den Cluster-Switches BES-53248 sind die 48 10/25GbE (SFP28/SFP+)-Ports in 12 x 4-Port-Gruppen wie folgt zusammengefasst: Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 und 45-48.
- Die SFP28/SFP+-Portgeschwindigkeit muss bei allen Ports der 4-Port-Gruppe gleich sein (10GbE oder 25GbE).
- Wenn die Geschwindigkeiten in einer 4-Port-Gruppe unterschiedlich sind, funktionieren die Switch-Ports nicht ordnungsgemäß.

FEC Anforderungen

- Für 25G-Ports mit Kupferkabeln siehe die folgende Tabelle für Details.

  Wenn die Controller-Seite `auto` Die Schalterseite ist auf FEC 25G eingestellt.

FAS2820 FEC			**Switch FEC**			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	UP
fc	FC-FEC/BASE-R	FC-FEC/BASE-R	FEC 25G	FEC 25G	CL-74	UP
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	No FEC	FEC Disabled	FEC Disabled	UP
none	none	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	UP
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	UP

- Einzelheiten zu 25G-Ports mit Glasfaser-/Lichtwellenleiterkabeln finden Sie in der folgenden Tabelle:

FAS2820 FEC			Switch FEC			
write	read		write	read		link status
	requested_fec	negotiated_fec		Configured FEC Mode	Physical FEC Status	
fc	FC-FEC/BASE-R	none	No FEC	FEC Disabled	FEC Disabled	DOWN
fc	**FC-FEC/BASE-R**	**FC-FEC/BASE-R**	**FEC 25G**	**FEC 25G**	**CL-74**	**UP**
auto	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
auto	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN
none	**none**	**none**	**No FEC**	**FEC Disabled**	**FEC Disabled**	**UP**
none	none	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	FEC 25G	FEC 25G	CL74	DOWN
rs	RS-FEC	none	No FEC	FEC Disabled	FEC Disabled	DOWN

Bootarg-Implementierung

Verwenden Sie den folgenden Befehl, um die FEC des 25G-Ports auf einen der folgenden Werte einzustellen: `auto` oder `fc` , wie erforderlich:

```
systemshell -node <node> -command sudo sysctl
dev.ice.<X>.requested_fec=<auto/fc>
```

- Wenn eingestellt auf*`auto` *:
  - Der `auto` Die Einstellung wird sofort an die Hardware weitergegeben, ein Neustart ist nicht erforderlich.
  - Wenn `bootarg.cpk_fec_fc_eXx already exists` Es wird aus dem Bootargumentspeicher gelöscht.
  - Nach einem Neustart `auto` Die Einstellung bleibt bestehen, seitdem `auto` ist die Standardeinstellung für FEC.
- Wenn eingestellt auf*`fc` *:
  - Der `FC-FEC` Die Einstellung wird sofort an die Hardware weitergegeben, ein Neustart ist nicht erforderlich.
  - Ein neues `bootarg.cpk_fec_fc_eXx` wird mit dem Wert "true" erstellt.
  - Nach einem Neustart `FC-FEC` Die Einstellungen bleiben für den Treibercode weiterhin gültig.

Konfigurieren der Software

Workflow für die Softwareinstallation für BES-53248-Switches

Um die Software für einen BES-53248 Cluster-Switch zu installieren und zu konfigurieren, befolgen Sie diese Schritte:

1. **"Konfigurieren Sie den Schalter"**

Konfigurieren Sie den Cluster-Switch BES-53248.

2. **"Installieren Sie die EFOS-Software"**

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

3. **"Lizenzen für BES-53248 Cluster-Switches installieren"**

Optional können Sie neue Ports hinzufügen, indem Sie weitere Lizenzen erwerben und installieren. Das Switch-Basismodell ist für 16 10GbE- oder 25GbE-Ports und zwei 100GbE-Ports lizenziert.

4. **"Installieren Sie die Referenzkonfigurationsdatei (RCF)."**

Installieren oder 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.

5. **"Aktivieren Sie SSH auf BES-53248 Cluster-Switches."**

Wenn Sie die Funktionen Ethernet Switch Health Monitor (CSHM) und Protokollerfassung nutzen, aktivieren Sie SSH auf den Switches.

6. **"Setzen Sie den Schalter auf die Werkseinstellungen zurück."**

Löschen Sie die Einstellungen des Cluster-Schalters BES-53248.

Konfigurieren des Cluster-Switches BES-53248

Führen Sie die folgenden Schritte aus, um die Ersteinrichtung des Cluster-Switches BES-53248 durchzuführen.

Bevor Sie beginnen

- Die Hardware wird wie beschrieben installiert."Installieren Sie die Hardware" Die
- Sie haben Folgendes geprüft:
  - "Konfigurationsanforderungen"
  - "Komponenten und Teilenummern"
  - "Dokumentationsanforderungen"

Zu den Beispielen

Die Beispiele in den Konfigurationsanleitungen verwenden die folgende Switch- und Knotennomenklatur:

- Die Namen der NetApp -Switches lauten: `cs1` Und `cs2` Die Das Upgrade beginnt mit dem zweiten Switch, *cs2.*
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.
- Der IPspace-Name lautet Cluster.
- Der `cluster1::>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Knoten sind benannt `e0a` Und `e0b` Die Siehe die "NetApp Hardware Universe" für die tatsächlich von Ihrer Plattform unterstützten Cluster-Ports.
- Die für die NetApp Switches unterstützten Inter-Switch-Links (ISLs) sind die Ports 0/55 und 0/56.
- Die für die NetApp Switches unterstützten Knotenverbindungen sind die Ports 0/1 bis 0/16 mit Standardlizenzierung.
- Die Beispiele verwenden zwei Knoten, aber ein Cluster kann bis zu 24 Knoten umfassen.

Schritte

1. Verbinden Sie den seriellen Port mit einem Host oder einem seriellen Port.
2. Verbinden Sie den Management-Port (den RJ-45-Schraubenschlüssel-Anschluss auf der linken Seite des Switches) mit demselben Netzwerk, in dem sich Ihr TFTP-Server befindet.
3. Nehmen Sie an der Konsole die seriellen Einstellungen auf dem Host vor:
   - 115200 Baud
   - 8 Datenbits
   - 1 Stoppbit
   - Parität: keine
   - Flusssteuerung: keine
4. Melden Sie sich am Switch an als `admin` und drücken Sie **Enter**, wenn Sie zur Eingabe eines Passworts aufgefordert werden. Der Standard-Switch-Name lautet **routing**. Geben Sie bei Aufforderung Folgendes ein `enable` Die Dies ermöglicht Ihnen den Zugriff auf den privilegierten EXEC-Modus zur Switch-Konfiguration.

   ```
   User: admin
   Password:
   (Routing)> enable
   Password:
   (Routing)#
   ```

5. Ändern Sie den Schalternamen in **cs2**.

   ```
   (Routing)# hostname cs2
   (cs2)#
   ```

6. So legen Sie eine statische IPv4- oder IPv6-Verwaltungsadresse für den Service-Port des Switches fest:

IPv4

Der Serviceport ist standardmäßig auf die Verwendung von DHCP eingestellt. Die IP-Adresse, die Subnetzmaske und die Standardgateway-Adresse werden automatisch zugewiesen.

```
(cs2)# serviceport protocol none
(cs2)# network protocol none
(cs2)# serviceport ip <ip-address> <netmask> <gateway>
```

IPv6

Der Serviceport ist standardmäßig auf die Verwendung von DHCP eingestellt. Die IP-Adresse, die Subnetzmaske und die Standardgateway-Adresse werden automatisch zugewiesen.

```
(cs2)# serviceport protocol none
(cs2)# network protocol none
(cs2)# serviceport ipv6 <address>
(cs2)# serviceport ipv6 <gateway>
```

1. Überprüfen Sie die Ergebnisse mit dem Befehl:

   `show serviceport`

   ```
   (cs2)# show serviceport
   Interface Status.............................. Up
   IP Address.................................... 172.19.2.2
   Subnet Mask................................... 255.255.255.0
   Default Gateway............................... 172.19.2.254
   IPv6 Administrative Mode...................... Enabled
   IPv6 Prefix is ..............................
   fe80::dac4:97ff:fe71:123c/64
   IPv6 Default Router........................... fe80::20b:45ff:fea9:5dc0
   Configured IPv4 Protocol...................... DHCP
   Configured IPv6 Protocol...................... None
   IPv6 AutoConfig Mode.......................... Disabled
   Burned In MAC Address......................... D8:C4:97:71:12:3C
   ```

2. Konfigurieren Sie die Domäne und den Nameserver:

   ```
   ip domain name <domain_name>
   ip name server <server_name>
   ```

```
(cs2)# configure
(cs2)(Config)# ip domain name company.com
(cs2)(Config)# ip name server 10.10.99.1 10.10.99.2
(cs2)(Config)# exit
(cs2)#
```

3. Konfigurieren Sie den NTP-Server.

EFOS 3.10.0.3 und höher

Konfigurieren Sie die Zeitzone und die Zeitsynchronisierung (NTP):

```
sntp server <server_name>
clock
```

```
(cs2)# configure
(cs2)(Config)# ntp server 10.99.99.5
(cs2)(Config)# clock timezone -7
(cs2)(Config)# exit
(cs2)#
```

EFOS 3.9.0.2 und früher

Konfigurieren Sie die Zeitzone und die Zeitsynchronisierung (SNTP):

```
sntp client mode <client_mode>
sntp server <server_name>
clock
```

```
(cs2)# configure
(cs2)(Config)# sntp client mode unicast
(cs2)(Config)# sntp server 10.99.99.5
(cs2)(Config)# clock timezone -7
(cs2)(Config)# exit
(cs2)#
```

1. Konfigurieren Sie die Zeit manuell, wenn Sie im vorherigen Schritt keinen NTP-Server konfiguriert haben.

EFOS 3.10.0.3 und höher

Die Zeit manuell einstellen.

`clock`

```
(cs2)# configure
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

EFOS 3.9.0.2 und früher

Die Zeit manuell einstellen.

`clock`

```
(cs2)# configure
(cs2)(Config)# no sntp client mode
(cs2)(Config)# clock summer-time recurring 1 sun mar 02:00 1 sun nov
02:00 offset 60 zone EST
(cs2)(Config)# clock timezone -5 zone EST
(cs2)(Config)# clock set 07:00:00
(cs2)(Config)# clock set 10/20/2023
(cs2)(Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2023
No time source

(cs2)(Config)# exit
(cs2)#
```

1. Speichern Sie die laufende Konfiguration in der Startkonfiguration:

   `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!
```

Wie geht es weiter?

Nachdem Sie Ihre Schalter konfiguriert haben, können Sie "Installieren Sie die EFOS-Software"Die

Installieren Sie die EFOS-Software

Führen Sie diese Schritte aus, um die Ethernet Fabric OS (EFOS)-Software auf dem Cluster-Switch BES-53248 zu installieren.

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.

Vorbereiten der Installation

Bevor Sie beginnen

- Dieses Verfahren eignet sich nur für Neuinstallationen.
- Laden Sie die passende Broadcom EFOS-Software für Ihre Cluster-Switches von der Website herunter. "Broadcom Ethernet-Switch-Unterstützung" Website.
- Stellen Sie sicher, dass"Der BES-53248 Cluster-Switch ist konfiguriert." Die

Installieren Sie die Software

Verwenden Sie eine der folgenden Methoden, um die EFOS-Software zu installieren:

- Methode 1: EFOS installieren. Für die meisten Anwendungsfälle geeignet.
- Methode 2: EFOS im ONIE-Modus installieren. Verwenden Sie diese Option, wenn eine EFOS-Version FIPS-konform und die andere EFOS-Version nicht FIPS-konform ist.

Methode 1: EFOS installieren

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

Schritte

1. Melden Sie sich am seriellen Konsolenport des Switches an oder stellen Sie eine SSH-Verbindung her.
2. Verwenden Sie die `ping` Befehl zur Überprüfung der Verbindung zum Server, auf dem EFOS, Lizenzen und die RCF-Datei gehostet werden.

Beispiel anzeigen

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

   In der folgenden Tabelle finden Sie Informationen zu den unterstützten Kopierprotokollen:

Protokoll	Voraussetzung
Trivial File Transfer Protocol (TFTP)	Keine
SSH-Dateiübertragungsprotokoll (SFTP)	Ihre Software muss eine sichere Verwaltung unterstützen.
FTP	Passwort erforderlich
XMODEM	Keine
YMODEM	Keine
ZMODEM	Keine
Secure Copy Protocol (SCP)	Ihre Software muss eine sichere Verwaltung unterstützen.
HTTP	Dateiübertragungen über die Befehlszeile werden auf ausgewählten Plattformen unterstützt, sofern ein natives WGET-Dienstprogramm verfügbar ist.
HTTPS	Dateiübertragungen über die Befehlszeile werden auf ausgewählten Plattformen unterstützt, sofern ein natives WGET-Dienstprogramm verfügbar ist.

   Durch das Kopieren der Image-Datei in das aktive Image wird beim Neustart die laufende EFOS-Version anhand dieses Images festgelegt. Das vorherige Image bleibt als Backup verfügbar.

Beispiel anzeigen

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.10.0.3.stk active
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......................... active

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.
```

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     3.7.0.4     3.7.0.4           3.10.0.3
```

5. 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!
```

6. 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
```

7. Schließen Sie die Installation ab. Führen Sie diese vier Schritte aus, um den Switch neu zu konfigurieren:
    a. "Lizenzen installieren"
    b. "Installieren Sie die RCF-Datei"
    c. "Aktivieren von SSH"
    d. "Switch-Zustandsüberwachung konfigurieren"
8. Wiederholen Sie die Schritte 1 bis 7 am Partnerschalter.

Methode 2: EFOS im ONIE-Modus installieren

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 installieren, falls der Switch nicht bootet.

Schritte

1. Stellen Sie eine Verbindung zu einer Konsole her, die an den seriellen Port des Switches angeschlossen ist.
2. Starten Sie den Switch im ONIE-Installationsmodus.

    Wählen Sie während des Bootvorgangs ONIE aus, wenn Sie dazu aufgefordert werden.

Beispiel anzeigen

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

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

Beispiel anzeigen

```
+-----------------------------------------------------------------
-+
|*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 des Management-Ports des Switches 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. Melden Sie sich an und 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. Befolgen Sie diese fünf Schritte, um den Switch neu zu konfigurieren:
   a. "Schalter konfigurieren"
   b. "Lizenzen installieren"
   c. "Installieren Sie die RCF-Datei"
   d. "Aktivieren von SSH"

e. "Switch-Zustandsüberwachung konfigurieren"

9. Wiederholen Sie die Schritte 1 bis 8 am Partnerschalter.

Was kommt als nächstes

Nach der Installation der EFOS-Software können Sie "Installieren Sie Ihre Lizenzen"Die

Installieren Sie die Referenzkonfigurationsdatei (RCF) und die Lizenzdatei.

Ab EFOS 3.12.0.1 können Sie die Referenzkonfigurationsdatei (RCF) und die Lizenzdatei nach der Konfiguration des Cluster-Switches BES-53248 installieren.

Alle Ports werden bei der Installation des RCF konfiguriert, aber Sie müssen Ihre Lizenz installieren, um die konfigurierten Ports zu aktivieren.

Überprüfungsanforderungen

Bevor Sie beginnen

Bitte vergewissern Sie sich, dass Folgendes vorhanden ist:

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Das aktuelle RCF ist erhältlich bei "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 instanziiert 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.

Installieren Sie die Konfigurationsdatei

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 der Installation

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:

   ```
   cluster1::*> 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
                                                          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          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 dem Cluster-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 Lizenzen.

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 RdmaDst
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
```

d. Die laufende Konfiguration in der Startkonfiguration speichern:

```
(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:

```
(cs2)# reload

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

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

7. 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.
8. Kopieren Sie die RCF-Datei mithilfe eines der folgenden Übertragungsprotokolle in den Bootflash des Switches cs2: FTP, HTTP, TFTP, SFTP oder SCP.

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

Beispiel anzeigen

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-RCF-v1.12-
Cluster-HA.txt nvram:reference-config

Mode..................................... HTTP
Set Server IP............................ 172.19.2.1
Path..................................... <ip-to-
webserver>/path/to/
Filename................................. BES-53248-RCF-v1.12-
Cluster-HA.txt
Data Type................................ Unknown

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y
File transfer in progress.
Management access will be blocked for the duration of the transfer.
Please wait...
HTTP Unknown file type transfer starting...
Validating configuration script.....
Configuration script validated.
File transfer operation completed successfully.
```

9. 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
1 configuration script(s) found.
2045 Kbytes free.
```

10. Wenden Sie das Skript auf den Schalter an:

    `script apply`

Beispiel anzeigen

```
(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.
```

11. Installieren Sie die Lizenzdatei.

Beispiel anzeigen

```
(cs2)# copy http://<ip-to-webserver>/path/to/BES-53248-LIC.dat
nvram:license-key 1
Mode........................................... HTTP
Set Server IP.................................. 172.19.2.1
Path........................................... <ip-to-
webserver>/path/to/
Filename....................................... BES-53248-LIC.dat
Data Type...................................... license

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

File transfer in progress. Management access will be blocked for the
duration of the transfer.

Please wait...

License Key transfer operation completed successfully.

System reboot is required.
(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!

(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
...
...
```

12. Untersuchen Sie die Bannerausgabe von `show clibanner` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um die korrekte Konfiguration und Funktion des Schalters zu gewährleisten.

Beispiel anzeigen

```
(cs2)# show clibanner

Banner Message configured :
=========================
BES-53248 Reference Configuration File v1.12 for Cluster/HA/RDMA

Switch   : BES-53248
Filename : BES-53248-RCF-v1.12-Cluster.txt
Date     : 11-04-2024
Version  : v1.12
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"
```

13. 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

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

```
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
```

14. Überprüfen Sie am Schalter, ob Ihre Änderungen vorgenommen wurden:

```
show running-config
```

```
(cs2)# show running-config
```

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

```
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!
```

16. 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!
```

17. Auf dem Cluster-Switch cs2 werden die mit den Cluster-Ports der Knoten verbundenen Ports aktiviert. 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)# no shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

18. 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
```

19. 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
                                                          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
```

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                       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
```

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

   Das folgende Beispiel verwendet die Ausgabe des Schnittstellenbeispiels:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# shutdown
```

2. 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        e0a      false
            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      false
            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      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        e0a      false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04        e0b      true
cluster1::*>
```

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

   Beispiel anzeigen

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

4. Wiederholen Sie die Schritte 4 bis 19 auf Switch cs1.

5. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

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

```
(cs1)# 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!
```

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 | 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
```

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 Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer

AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Installation der RCF- und Lizenzdatei können Sie "SSH aktivieren"Die

Lizenzen für BES-53248 Cluster-Switches installieren

Das Basismodell des Cluster-Switches BES-53248 ist für 16 10GbE- oder 25GbE-Ports und zwei 100GbE-Ports lizenziert. Sie können neue Ports hinzufügen, indem Sie weitere Lizenzen erwerben.

Für EFOS 3.12 und höher befolgen Sie die Installationsschritte in"Installieren Sie die Referenzkonfigurationsdatei (RCF) und die Lizenzdatei." Die

Prüfen Sie die verfügbaren Lizenzen.

Für die Verwendung auf dem Cluster-Switch BES-53248 stehen folgende Lizenzen zur Verfügung:

Lizenztyp	Lizenzdetails	Unterstützte Firmware-Version
SW-BES-53248A2-8P-2P	Broadcom 8PT-10G25G + 2PT-40G100G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES-53248A2-8P-1025G	Broadcom 8-Port 10G25G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248A2-6P-40-100G	Broadcom 6-Port 40G100G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher

Um einen Transaktionsschlüssel für eine Portlizenzschlüsseldatei einzulösen, gehen Sie zu"Lizenzportal für Broadcom-unterstützte Ethernet-Switches" Seite. Siehe den Artikel in der Wissensdatenbank."So fügen Sie zusätzliche Portlizenzen für den Broadcom BES-53248 Switch hinzu" für weitere Einzelheiten.

Legacy-Lizenzen

Die folgende Tabelle listet die älteren Lizenzen auf, die für die Verwendung auf dem Cluster-Switch BES-53248 verfügbar waren:

Lizenztyp	Lizenzdetails	Unterstützte Firmware-Version
SW-BES-53248A1-G1-8P-LIC	Broadcom 8P 10-25,2P40-100 Lizenzschlüssel, X190005/R	EFOS 3.4.3.3 und höher
SW-BES-53248A1-G1-16P-LIC	Broadcom 16P 10-25,4P40-100 Lizenzschlüssel, X190005/R	EFOS 3.4.3.3 und höher
SW-BES-53248A1-G1-24P-LIC	Broadcom 24P 10-25,6P40-100 Lizenzschlüssel, X190005/R	EFOS 3.4.3.3 und höher
SW-BES54248-40-100G-LIC	Broadcom 6-Port 40G100G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248-8P-10G25G-LIC	Broadcom 8Port 10G25G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248-16P-1025G-LIC	Broadcom 16-Port 10G25G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248-24P-1025G-LIC	Broadcom 24-Port 10G25G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher

Für die Basiskonfiguration ist keine Lizenz erforderlich.

Lizenzdateien installieren

Befolgen Sie diese Schritte, um Lizenzen für BES-53248 Cluster-Switches zu installieren.

Schritte

1. Verbinden Sie den Cluster-Switch 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.

Beispiel anzeigen

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. Überprüfen Sie die aktuelle Lizenznutzung auf Switch CS2:

   `show license`

   Beispiel anzeigen

   ```
   (cs2)# show license
   Reboot needed.................................. No
   Number of active licenses..................... 0

   License Index  License Type     Status
   -------------- ---------------- -----------

   No license file found.
   ```

4. Installieren Sie die Lizenzdatei.

   Wiederholen Sie diesen Schritt, um weitere Lizenzen zu laden und andere Schlüsselindexnummern zu verwenden.

   Beispiel anzeigen

   Im folgenden Beispiel wird SFTP verwendet, um eine Lizenzdatei auf einen Schlüsselindex 1 zu kopieren.

   ```
   (cs2)# copy sftp://root@172.19.2.1/var/lib/tftpboot/license.dat
   nvram:license-key 1
   Remote Password:**

   Mode........................................... SFTP
   Set Server IP.................................. 172.19.2.1
   Path........................................... /var/lib/tftpboot/
   Filename....................................... license.dat
   Data Type...................................... license

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

   File transfer in progress. Management access will be blocked for the
   duration of the transfer. Please wait...


   License Key transfer operation completed successfully. System reboot
   is required.
   ```

5. Zeigen Sie alle aktuellen Lizenzinformationen an und notieren Sie den Lizenzstatus, bevor Switch CS2 neu gestartet wird:

   ```
   show license
   ```

   Beispiel anzeigen

   ```
   (cs2)# show license

   Reboot needed.................................. Yes
   Number of active licenses...................... 0


   License Index  License Type      Status
   -------------- ----------------- --------------------------------
   1              Port              License valid but not applied
   ```

6. Alle lizenzierten Ports anzeigen:

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

   Die Ports aus den zusätzlichen Lizenzdateien werden erst nach einem Neustart des Switches angezeigt.

Beispiel anzeigen

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

                Admin     Physical   Physical   Link   Link    LACP
Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode
Timeout
--------- ------ --------- ---------- ---------- ------ -------
------ --------
0/1             Disable   Auto                  Down   Enable
Enable long
0/2             Disable   Auto                  Down   Enable
Enable long
0/3             Disable   Auto                  Down   Enable
Enable long
0/4             Disable   Auto                  Down   Enable
Enable long
0/5             Disable   Auto                  Down   Enable
Enable long
0/6             Disable   Auto                  Down   Enable
Enable long
0/7             Disable   Auto                  Down   Enable
Enable long
0/8             Disable   Auto                  Down   Enable
Enable long
0/9             Disable   Auto                  Down   Enable
Enable long
0/10            Disable   Auto                  Down   Enable
Enable long
0/11            Disable   Auto                  Down   Enable
Enable long
0/12            Disable   Auto                  Down   Enable
Enable long
0/13            Disable   Auto                  Down   Enable
Enable long
0/14            Disable   Auto                  Down   Enable
Enable long
0/15            Disable   Auto                  Down   Enable
Enable long
0/16            Disable   Auto                  Down   Enable
Enable long
0/55            Disable   Auto                  Down   Enable
Enable long
0/56            Disable   Auto                  Down   Enable
Enable long
```

7. 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!
   Are you sure you would like to reset the system? (y/n) y
   ```

8. Prüfen Sie, ob die neue Lizenz aktiv ist und vermerken Sie, dass die Lizenz angewendet wurde:

   ```
   show license
   ```

   Beispiel anzeigen

   ```
   (cs2)# show license

   Reboot needed.................................. No
   Number of installed licenses................... 1
   Total Downlink Ports enabled................... 16
   Total Uplink Ports enabled..................... 8

   License Index  License Type              Status
   -------------- ------------------------
   ----------------------------------
   1              Port                      License applied
   ```

9. Prüfen Sie, ob alle neuen Ports verfügbar sind:

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

Beispiel anzeigen

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

                Admin     Physical   Physical   Link   Link    LACP
Actor
Intf      Type  Mode      Mode       Status     Status Trap    Mode
Timeout
--------- ------ --------- ---------- ---------- ------ -------
------ --------
0/1             Disable    Auto                  Down   Enable
Enable long
0/2             Disable    Auto                  Down   Enable
Enable long
0/3             Disable    Auto                  Down   Enable
Enable long
0/4             Disable    Auto                  Down   Enable
Enable long
0/5             Disable    Auto                  Down   Enable
Enable long
0/6             Disable    Auto                  Down   Enable
Enable long
0/7             Disable    Auto                  Down   Enable
Enable long
0/8             Disable    Auto                  Down   Enable
Enable long
0/9             Disable    Auto                  Down   Enable
Enable long
0/10            Disable    Auto                  Down   Enable
Enable long
0/11            Disable    Auto                  Down   Enable
Enable long
0/12            Disable    Auto                  Down   Enable
Enable long
0/13            Disable    Auto                  Down   Enable
Enable long
0/14            Disable    Auto                  Down   Enable
Enable long
0/15            Disable    Auto                  Down   Enable
Enable long
0/16            Disable    Auto                  Down   Enable
Enable long
0/49            Disable   100G Full              Down   Enable
Enable long
0/50            Disable   100G Full              Down   Enable
Enable long
```

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

Bei der Installation zusätzlicher Lizenzen müssen Sie die neuen Schnittstellen manuell konfigurieren. Ein RCF darf nicht erneut auf einen bereits funktionierenden Produktionsschalter angewendet werden.

Behebung von Installationsproblemen

Wenn bei der Installation einer Lizenz Probleme auftreten, führen Sie die folgenden Debug-Befehle aus, bevor Sie die Lizenz installieren. `copy` Den Befehl erneut geben.

Zu verwendende Debug-Befehle: `debug transfer` Und `debug license`

Beispiel anzeigen

```
(cs2)# debug transfer
Debug transfer output is enabled.
(cs2)# debug license
Enabled capability licensing debugging.
```

Wenn Sie die `copy` Befehl mit dem `debug transfer` Und `debug license` Wenn diese Optionen aktiviert sind, wird die Protokollausgabe zurückgegeben.

Beispiel anzeigen

```
transfer.c(3083):Transfer process  key or certificate file type = 43
transfer.c(3229):Transfer process  key/certificate cmd = cp
/mnt/download//license.dat.1 /mnt/fastpath/ >/dev/null 2>&1CAPABILITY
LICENSING :
Fri Sep 11 13:41:32 2020: License file with index 1 added.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Validating hash value
29de5e9a8af3e510f1f16764a13e8273922d3537d3f13c9c3d445c72a180a2e6.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Parsing JSON buffer {
  "license": {
    "header": {
      "version": "1.0",
      "license-key": "964B-2D37-4E52-BA14",
      "serial-number": "QTFCU38290012",
      "model": "BES-53248"
  },
  "description": "",
  "ports": "0+6"
  }
}.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: License data does not
contain 'features' field.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Serial number
QTFCU38290012 matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Model BES-53248
matched.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Feature not found in
license file with index = 1.
CAPABILITY LICENSING : Fri Sep 11 13:41:32 2020: Applying license file
1.
```

Prüfen Sie in der Debug-Ausgabe Folgendes:

- Prüfen Sie, ob die Seriennummer übereinstimmt: `Serial number QTFCU38290012 matched.`
- Prüfen Sie, ob das Schaltermodell übereinstimmt: `Model BES-53248 matched.`
- Prüfen Sie, ob der angegebene Lizenzindex nicht bereits verwendet wurde. Wenn bereits ein Lizenzindex verwendet wird, wird folgender Fehler zurückgegeben: `License file /mnt/download//license.dat.1 already exists.`
- Eine Portlizenz ist keine Funktionslizenz. Daher ist folgende Aussage zu erwarten: `Feature not found in license file with index = 1.`

Verwenden Sie die `copy` Befehl zum Sichern der Portlizenzen auf dem Server:

```
(cs2)# copy nvram:license-key 1
scp://<UserName>@<IP_address>/saved_license_1.dat
```

Falls Sie die Switch-Software von Version 3.4.4.6 downgraden müssen, werden die Lizenzen entfernt. Dies ist ein erwartbares Verhalten.

Bevor Sie auf eine ältere Version der Software zurückgreifen können, müssen Sie eine entsprechende ältere Lizenz installieren.

Aktivieren Sie neu lizenzierte Ports

Um neu lizenzierte Ports zu aktivieren, müssen Sie die neueste Version der RCF bearbeiten und die entsprechenden Portdetails einkommentieren.

Die Standardlizenz aktiviert die Ports 0/1 bis 0/16 und 0/55 bis 0/56, während die neu lizenzierten Ports je nach Art und Anzahl der verfügbaren Lizenzen zwischen den Ports 0/17 und 0/54 liegen. Um beispielsweise die Lizenz SW-BES54248-40-100G-LIC zu aktivieren, müssen Sie den folgenden Abschnitt in der RCF-Datei einkommentieren:

Beispiel anzeigen

```
.
.
!
! 2-port or 6-port 40/100GbE node port license block
!
interface 0/49
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/50
no shutdown
description "40/100GbE Node Port"
!speed 100G full-duplex
speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/51
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
```

```
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/52
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/53
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
interface 0/54
no shutdown
description "40/100GbE Node Port"
speed 100G full-duplex
!speed 40G full-duplex
service-policy in WRED_100G
spanning-tree edgeport
mtu 9216
switchport mode trunk
datacenter-bridging
```

```
priority-flow-control mode on
priority-flow-control priority 5 no-drop
exit
exit
!
.
.
```

Bei Hochgeschwindigkeitsports zwischen 0/49 und 0/54 (einschließlich) entfernen Sie die Kommentarzeichen vor jedem Port, jedoch nur vor einer **speed**-Zeile in der RCF für jeden dieser Ports, entweder: **speed 100G full-duplex** oder **speed 40G full-duplex**, wie im Beispiel gezeigt. Bei langsamen Ports zwischen 0/17 und 0/48 (einschließlich) muss der gesamte Abschnitt mit 8 Ports einkommentiert werden, sobald eine entsprechende Lizenz aktiviert wurde.

Wie geht es weiter?

Nach der Installation der Lizenzen können Sie "Installieren Sie die Referenzkonfigurationsdatei (RCF)." oder "RCF aufrüsten"Die

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können die Referenzkonfigurationsdatei (RCF) installieren, nachdem Sie den Cluster-Switch BES-53248 konfiguriert und die neuen Lizenzen angewendet haben.

Für EFOS 3.12 und höher befolgen Sie die Installationsschritte in"Installieren Sie die Referenzkonfigurationsdatei (RCF) und die Lizenzdatei." Die

Überprüfungsanforderungen

Bevor Sie beginnen

Bitte vergewissern Sie sich, dass Folgendes vorhanden ist:

- 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 instanziiert 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.

Installieren Sie die Konfigurationsdatei

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 der Installation

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:

```
cluster1::*> 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
                                                          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          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 dem Cluster-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 Lizenzen.

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 class-map CLUSTER
no class-map HA
no class-map RDMA
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
```

d. Die laufende Konfiguration in der Startkonfiguration speichern:

```
(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:

```
(cs2)# reload

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

f. 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 Details.

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 tftp://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
nvram: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 `show clibanner` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um die korrekte Konfiguration und Funktion des Schalters zu gewährleisten.

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

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

```
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
```

```
(cs2)# show running-config
```

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

```
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!
```

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. 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)# no shutdown
(cs2)(Interface 0/1-0/16)# exit
(cs2)(Config)#
```

7. 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
```

8. 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
                                                          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
```

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                       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
```

9. 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. Schalten Sie auf dem Cluster-Switch cs1 die mit den Cluster-Ports der Knoten verbundenen Ports ab.

   Das folgende Beispiel verwendet die Ausgabe des Schnittstellenbeispiels:

```
(cs1)> enable
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# shutdown
```

2. 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        e0a      false
            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      false
            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      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        e0a      false
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04        e0b      true
cluster1::*>
```

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

   Beispiel anzeigen

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

4. Wiederholen Sie die Schritte 4 bis 19 auf Switch cs1.

5. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

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

```
(cs1)# 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!
```

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 | 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
```

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 Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer

AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Installation des RCF können Sie "SSH aktivieren"Die

Aktivieren Sie SSH auf BES-53248 Cluster-Switches.

Wenn Sie die Funktionen Ethernet Switch Health Monitor (CSHM) und Protokollerfassung verwenden, müssen Sie die SSH-Schlüssel generieren und anschließend SSH auf den Cluster-Switches aktivieren.

Schritte

1. Überprüfen Sie, ob SSH deaktiviert ist:

   ```
   show ip ssh
   ```

   Beispiel anzeigen

   ```
   (switch)# show ip ssh

   SSH Configuration

   Administrative Mode: ......................... Disabled
   SSH Port: ..................................... 22
   Protocol Level: ............................... Version 2
   SSH Sessions Currently Active: ................ 0
   Max SSH Sessions Allowed: ..................... 5
   SSH Timeout (mins): ........................... 5
   Keys Present: ................................. DSA(1024) RSA(1024)
   ECDSA(521)
   Key Generation In Progress: ................... None
   SSH Public Key Authentication Mode: ........... Disabled
   SCP server Administrative Mode: ............... Disabled
   ```

   - Falls SSH nicht deaktiviert ist, deaktivieren Sie es wie folgt:

     ```
     no ip ssh server enable

     no ip scp server enable
     ```

- Für EFOS 3.12 und höher ist Konsolenzugriff erforderlich, da aktive SSH-Sitzungen verloren gehen, wenn SSH deaktiviert ist.
- Bei EFOS 3.11 und früher bleiben aktuelle SSH-Sitzungen nach der Deaktivierung des SSH-Servers offen.

+

Stellen Sie sicher, dass Sie SSH deaktivieren, bevor Sie die Schlüssel ändern, andernfalls wird eine Warnung auf dem Switch angezeigt.

2. Generieren Sie im Konfigurationsmodus die SSH-Schlüssel:

   `crypto key generate`

   Beispiel anzeigen

   ```
   (switch)# config

   (switch) (Config)# crypto key generate rsa

   Do you want to overwrite the existing RSA keys? (y/n): y


   (switch) (Config)# crypto key generate dsa

   Do you want to overwrite the existing DSA keys? (y/n): y


   (switch) (Config)# crypto key generate ecdsa 521

   Do you want to overwrite the existing ECDSA keys? (y/n): y
   ```

3. Legen Sie im Konfigurationsmodus die AAA-Autorisierung für die ONTAP Protokollerfassung fest:

   `aaa authorization commands "noCmdAuthList" none`

   Beispiel anzeigen

   ```
   (switch) (Config)# aaa authorization commands "noCmdAuthList" none
   (switch) (Config)# exit
   ```

4. Aktivieren Sie SSH/SCP erneut.

Beispiel anzeigen

```
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
```

5. Speichern Sie diese Änderungen in der Startkonfiguration:

   `write memory`

   Beispiel anzeigen

```
(switch)# 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!
```

6. Verschlüsseln Sie die SSH-Schlüssel (nur für den **FIPS-Modus**):

   Im FIPS-Modus müssen die Schlüssel aus Sicherheitsgründen mit einer Passphrase verschlüsselt werden. Fehlt ein verschlüsselter Schlüssel, kann die Anwendung nicht gestartet werden. Die Schlüssel werden mithilfe der folgenden Befehle erstellt und verschlüsselt:

Beispiel anzeigen

```
(switch) configure
(switch) (Config)# crypto key encrypt write rsa passphrase
<passphase>

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): y

Config file 'startup-config' created successfully.

(switch) (Config)# crypto key encrypt write dsa passphrase
<passphase>

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): y

Config file 'startup-config' created successfully.

(switch)(Config)# crypto key encrypt write ecdsa passphrase
<passphase>

The key will be encrypted and saved on NVRAM.
This will result in saving all existing configuration also.
Do you want to continue? (y/n): y

Config file 'startup-config' created successfully.

(switch) (Config)# end
(switch)# 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!
```

7. Starten Sie den Switch neu:

```
reload
```

8. Überprüfen Sie, ob SSH aktiviert ist:

   ```
   show ip ssh
   ```

   Beispiel anzeigen

   ```
   (switch)# show ip ssh

   SSH Configuration

   Administrative Mode: ..... Enabled
   SSH Port: ..... 22
   Protocol Level: ..... Version 2
   SSH Sessions Currently Active: ..... 0
   Max SSH Sessions Allowed: ..... 5
   SSH Timeout (mins): ..... 5
   Keys Present: ..... DSA(1024) RSA(1024)
   ECDSA(521)
   Key Generation In Progress: ..... None
   SSH Public Key Authentication Mode: ..... Enabled
   SCP server Administrative Mode: ..... Enabled
   ```

Wie geht es weiter?

Nachdem Sie SSH aktiviert haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Setzen Sie den Cluster-Schalter BES-53248 auf die Werkseinstellungen zurück.

Um den Cluster-Switch BES-53248 auf die Werkseinstellungen zurückzusetzen, müssen Sie die Switch-Einstellungen BES-53248 löschen.

Informationen zu diesem Vorgang

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

Schritte

1. Wechseln Sie zur Eingabeaufforderung mit Administratorrechten.

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

2. Startkonfiguration löschen.

   ```
   erase startup-config
   ```

```
(cs2)# erase startup-config

Are you sure you want to clear the configuration? (y/n) y
```

3. Starten Sie den Switch neu.

```
(cs2)# reload
Are you sure you would like to reset the system? (y/n) y
```

Wenn das System fragt, ob die nicht gespeicherte oder geänderte Konfiguration vor dem Neustart des Switches gespeichert werden soll, wählen Sie **Nein**.

1. Warten Sie, bis der Switch neu geladen ist, und melden Sie sich dann am Switch an.

Der Standardbenutzer ist „admin“, und es ist kein Passwort festgelegt. Es wird eine Eingabeaufforderung ähnlich der folgenden angezeigt:

```
(Routing)>
```

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 mitMethode 1: EFOS-Upgrade Die 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 mitMethode 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 mitMethode 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 mitMethode 1: EFOS-Upgrade Die 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 mitMethode 1: EFOS-Upgrade Die 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 mitMethode 2: EFOS mithilfe der ONIE OS-Installation aktualisieren Die 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    3.7.0.4             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 instanziiert 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
                                                  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          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 Lizenzen.

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
nvram: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

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

```
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
                                                          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
```

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 Fallerstellung 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

Migrieren Sie die Schalter

CN1610-Cluster-Switches auf BES-53248-Cluster-Switches migrieren

Um die CN1610-Cluster-Switches in einem Cluster auf Broadcom-unterstützte BES-53248-Cluster-Switches zu migrieren, überprüfen Sie die Migrationsanforderungen und

folgen Sie dann dem Migrationsverfahren.

Folgende Cluster-Switches werden unterstützt:

- CN1610
- BES-53248

Überprüfungsanforderungen

Vergewissern Sie sich, dass Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Einige der Ports der BES-53248-Switches sind für den Betrieb mit 10GbE konfiguriert.
- Die 10GbE-Konnektivität von den Knoten zu den BES-53248 Cluster-Switches wurde geplant, migriert und dokumentiert.
- Der Cluster ist voll funktionsfähig (es sollten keine Fehler in den Protokollen oder ähnliche Probleme auftreten).
- Die Erstkonfiguration der BES-53248-Switches ist abgeschlossen, sodass:
  - Die BES-53248-Switches verwenden die neueste empfohlene Version der EFOS-Software.
  - Referenzkonfigurationsdateien (RCFs) wurden auf die Switches angewendet.
  - Sämtliche Standortanpassungen, wie z. B. DNS, NTP, SMTP, SNMP und SSH, werden auf den neuen Switches konfiguriert.

Knotenverbindungen

Die Cluster-Switches unterstützen folgende Knotenverbindungen:

- NetApp CN1610: Ports 0/1 bis 0/12 (10GbE)
- BES-53248: Ports 0/1-0/16 (10GbE/25GbE)

> Zusätzliche Ports können durch den Kauf von Portlizenzen aktiviert werden.

ISL-Ports

Die Cluster-Switches verwenden die folgenden Inter-Switch-Link-Ports (ISL):

- NetApp CN1610: Ports 0/13 bis 0/16 (10GbE)
- BES-53248: Ports 0/55-0/56 (100GbE)

Der "*NetApp Hardware Universe*" Enthält Informationen zur ONTAP Kompatibilität, zur unterstützten EFOS-Firmware und zur Verkabelung von BES-53248 Cluster-Switches. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

ISL-Verkabelung

Die entsprechende ISL-Verkabelung sieht wie folgt aus:

- **Anfang:** Für CN1610 zu CN1610 (SFP+ zu SFP+) vier SFP+ Glasfaser- oder Kupfer-Direktanschlusskabel.

- **Final:** Für BES-53248 zu BES-53248 (QSFP28 zu QSFP28), zwei QSFP28 optische Transceiver/Glasfaser- oder Kupfer-Direktanschlusskabel.

Migrieren Sie die Schalter

Gehen Sie wie folgt vor, um CN1610-Cluster-Switches auf BES-53248-Cluster-Switches zu migrieren.

Zu den Beispielen

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

- Die Beispiele verwenden zwei Knoten, von denen jeder zwei 10-GbE-Cluster-Verbindungsports bereitstellt: `e0a` Und `e0b` Die
- Die Befehlsausgaben können je nach Version der ONTAP -Software variieren.
- Die auszutauschenden CN1610-Schalter sind `CL1` Und `CL2` Die
- Die BES-53248-Schalter als Ersatz für die CN1610-Schalter sind `cs1` Und `cs2` Die
- Die Knoten sind `node1` Und `node2` Die
- Zuerst wird der Schalter CL2 durch cs2 ersetzt, dann CL1 durch cs1.
- Die BES-53248 Switches sind mit den unterstützten Versionen der Reference Configuration File (RCF) und des Ethernet Fabric OS (EFOS) vorinstalliert, wobei ISL-Kabel an den Ports 55 und 56 angeschlossen sind.
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.

Informationen zu diesem Vorgang

Dieses Verfahren umfasst folgendes Szenario:

- Der Cluster beginnt mit zwei Knoten, die mit zwei CN1610 Cluster-Switches verbunden sind.
- Der CN1610-Schalter CL2 wird durch den BES-53248-Schalter cs2 ersetzt:
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
  - Trennen Sie die Kabel von allen Cluster-Ports auf allen mit CL2 verbundenen Knoten und verwenden Sie dann unterstützte Kabel, um die Ports wieder mit dem neuen Cluster-Switch cs2 zu verbinden.
- Der CN1610-Schalter CL1 wird durch den BES-53248-Schalter cs1 ersetzt:
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
  - Trennen Sie die Kabel von allen Cluster-Ports auf allen mit CL1 verbundenen Knoten und verwenden Sie dann unterstützte Kabel, um die Ports wieder mit dem neuen Cluster-Switch cs1 zu verbinden.

> 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.

Schritt 1: Vorbereitung auf die Migration

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:

   ```
   cluster1::*> 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.

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Prüfen Sie an den neuen Switches, ob die ISL-Verbindung zwischen den Switches cs1 und cs2 hergestellt und funktionsfähig ist:

   ```
   show port-channel
   ```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs1 **aktiv** sind:

```
(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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
(cs1) #
```

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs2 **aktiv** sind:

```
(cs2)# 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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

2. Zeigen Sie die Cluster-Ports auf jedem Knoten an, der mit den vorhandenen Cluster-Switches verbunden

ist:

`network device-discovery show -protocol cdp`

Beispiel anzeigen

Das folgende Beispiel zeigt, wie viele Cluster-Interconnect-Schnittstellen in jedem Knoten für jeden Cluster-Interconnect-Switch konfiguriert wurden:

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    CL1                       0/2
CN1610
            e0b    CL2                       0/2
CN1610
node1      /cdp
            e0a    CL1                       0/1
CN1610
            e0b    CL2                       0/1
CN1610
```

3. Ermitteln Sie den administrativen oder operativen Status jeder Clusterschnittstelle.

   a. Überprüfen Sie, ob alle Cluster-Ports aktiv sind. `up` mit einem `healthy` Status:

      `network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

b. Überprüfen Sie, ob alle Cluster-Schnittstellen (LIFs) an ihren jeweiligen Heimatports 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
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
```

4. 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
----------------------------- ----------------- ------------- --------
CL1                           cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP

CL2                           cluster-network  10.10.1.102   CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: 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
----------------------------- ----------------- ------------- --------
CL1                           cluster-network  10.10.1.101   CN1610
     Serial Number: 01234567
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP

CL2                           cluster-network  10.10.1.102   CN1610
     Serial Number: 01234568
      Is Monitored: true
            Reason:
  Software Version: 1.3.0.3
    Version Source: ISDP
cluster1::*>
```

1. Automatische Rücksetzung der Cluster-LIFs deaktivieren.

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

2. Schalten Sie auf dem Cluster-Switch CL2 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen:

```
(CL2)# configure
(CL2)(Config)# interface 0/1-0/16
(CL2)(Interface 0/1-0/16)# shutdown
(CL2)(Interface 0/1-0/16)# exit
(CL2)(Config)# exit
(CL2)#
```

3. Überprüfen Sie, ob die Cluster-LIFs auf die Ports des Cluster-Switches CL1 umgeschaltet haben. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0a     false
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false
```

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

Beispiel anzeigen

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

5. Verlegen Sie alle Cluster-Knotenverbindungskabel vom alten CL2-Switch zum neuen cs2-Switch.
6. Überprüfen Sie den Zustand der auf CS2 verschobenen Netzwerkverbindungen:

   `network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

Alle verschobenen Cluster-Ports sollten `up` Die

7. Überprüfen Sie die Nachbarinformationen an den Cluster-Ports:

   `network device-discovery show -protocol cdp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    CL1                       0/2
CN1610
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    CL1                       0/1
CN1610
            e0b    cs2                       0/1               BES-
53248
```

8. Prüfen Sie aus Sicht des Switches CS2, ob die Portverbindungen des Switches einwandfrei funktionieren:

```
cs2# show interface all
cs2# show isdp neighbors
```

9. Schalten Sie auf dem Cluster-Switch CL1 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs durchzuführen:

```
(CL1)# configure
(CL1)(Config)# interface 0/1-0/16
(CL1)(Interface 0/1-0/16)# shutdown
(CL1)(Interface 0/13-0/16)# exit
(CL1)(Config)# exit
(CL1)#
```

Alle Cluster-LIFs schalten auf den Switch cs2 um.

10. Überprüfen Sie, ob für die Cluster-LIFs ein Failover auf die auf Switch cs2 gehosteten Ports durchgeführt wurde. Dies kann einige Sekunden dauern:

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

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0b     false
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0b     false
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true
```

11. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

    `cluster show`

    Beispiel anzeigen

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

12. Verlegen Sie die Cluster-Knoten-Verbindungskabel von CL1 zum neuen Switch cs1.
13. Überprüfen Sie den Zustand der Netzwerkverbindungen, die zu CS1 verschoben wurden:

    `network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

Alle verschobenen Cluster-Ports sollten `up` Die

14. Überprüfen Sie die Nachbarinformationen an den Cluster-Ports:

`network device-discovery show`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
```

15. Prüfen Sie aus Sicht des Switches cs1, ob die Portverbindungen des Switches einwandfrei funktionieren:

```
cs1# show interface all
cs1# show isdp neighbors
```

16. Überprüfen Sie, ob die ISL zwischen cs1 und cs2 noch funktionsfähig ist:

```
show port-channel
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs1 **aktiv** sind:

```
(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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
(cs1) #
```

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs2 **aktiv** sind:

```
(cs2)# 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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

17. Löschen Sie die ersetzten CN1610-Switches aus der Switch-Tabelle des Clusters, falls sie nicht

automatisch entfernt werden:

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie folgenden Befehl: `system switch ethernet delete -device device-name`

```
cluster::*> system switch ethernet delete -device CL1
cluster::*> system switch ethernet delete -device CL2
```

ONTAP 9.7 und früher

Für ONTAP 9.7 und ältere Versionen verwenden Sie folgenden Befehl: `system cluster-switch delete -device device-name`

```
cluster::*> system cluster-switch delete -device CL1
cluster::*> system cluster-switch delete -device CL2
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

2. Auf Switch cs2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

```
cs2> enable
cs2# configure
cs2(config)# interface 0/1-0/16
cs2(config-if-range)# shutdown

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

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

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

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

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

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster show
   ```

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
------ -------------------------- --------------- -----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Wenn Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

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

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Migration zu einer umgeschalteten NetApp Clusterumgebung

Wenn Sie bereits eine *switchlose* Clusterumgebung mit zwei Knoten besitzen, können Sie mithilfe von Broadcom-unterstützten BES-53248 Cluster-Switches zu einer *switched* Clusterumgebung mit zwei Knoten migrieren. Dadurch können Sie die Anzahl der Knoten im Cluster auf über zwei Knoten erhöhen.

Der Migrationsprozess funktioniert für alle Clusterknotenports, die optische oder Twinax-Ports verwenden. Er wird jedoch von diesem Switch nicht unterstützt, wenn die Knoten Onboard-10GBASE-T-RJ45-Ports für die

Clusternetzwerkports verwenden.

Überprüfungsanforderungen

Bitte beachten Sie die folgenden Anforderungen an die Clusterumgebung.

- Beachten Sie, dass die meisten Systeme zwei dedizierte Cluster-Netzwerkanschlüsse an jedem Controller benötigen.
- Stellen Sie sicher, dass der Cluster-Switch BES-53248 wie beschrieben eingerichtet ist."Ersetzen Sie die Anforderungen" vor Beginn dieses Migrationsprozesses.
- Für die schalterlose Zwei-Knoten-Konfiguration ist Folgendes sicherzustellen:
  - Die Zwei-Knoten-Konfiguration ohne Schalter ist ordnungsgemäß eingerichtet und funktioniert.
  - Auf den Knoten läuft ONTAP 9.5P8 und höher. Die Unterstützung für 40/100 GbE Cluster-Ports beginnt mit der EFOS Firmware-Version 3.4.4.6 und höher.
  - Alle Cluster-Ports befinden sich im Status **up**.
  - Alle logischen Schnittstellen (LIFs) des Clusters befinden sich im Status **up** und sind an ihren jeweiligen Ports angeschlossen.
- Stellen Sie für die Konfiguration des von Broadcom unterstützten BES-53248 Cluster-Switches Folgendes sicher:
  - Der Cluster-Switch BES-53248 ist auf beiden Switches voll funktionsfähig.
  - Beide Switches verfügen über eine Management-Netzwerkanbindung.
  - Es besteht Konsolenzugriff auf die Cluster-Switches.
  - Die Knoten-zu-Knoten- und Schalter-zu-Schalter-Verbindungen des BES-53248 verwenden Twinax- oder Glasfaserkabel.

    Der "*NetApp Hardware Universe*" Enthält Informationen zur ONTAP Kompatibilität, zur unterstützten EFOS-Firmware und zur Verkabelung mit BES-53248-Switches. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.
- Inter-Switch Link (ISL)-Kabel sind an die Ports 0/55 und 0/56 beider BES-53248-Switches angeschlossen.
- Die Erstkonfiguration beider BES-53248-Switches ist abgeschlossen, sodass:
  - Die BES-53248-Switches laufen mit der neuesten Softwareversion.
  - Die Switches BES-53248 verfügen über optional installierte Portlizenzen, sofern diese erworben wurden.
  - Referenzkonfigurationsdateien (RCFs) werden auf die Switches angewendet.
- Sämtliche Standortanpassungen (SMTP, SNMP und SSH) werden auf den neuen Switches konfiguriert.

Geschwindigkeitsbeschränkungen der Portgruppe

- Die 48 10/25GbE (SFP28/SFP+)-Ports sind in 12 x 4-Port-Gruppen wie folgt zusammengefasst: Ports 1-4, 5-8, 9-12, 13-16, 17-20, 21-24, 25-28, 29-32, 33-36, 37-40, 41-44 und 45-48.
- Die SFP28/SFP+-Portgeschwindigkeit muss bei allen Ports der 4-Port-Gruppe gleich sein (10GbE oder 25GbE).
- Wenn die Geschwindigkeiten in einer 4-Port-Gruppe unterschiedlich sind, funktionieren die Switch-Ports nicht ordnungsgemäß.

Zu den Beispielen

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

- Die Namen der BES-53248-Switches lauten: `cs1` Und `cs2` Die
- Die Namen der Cluster-SVMs sind `node1` Und `node2` Die
- Die Namen der LIFs sind `node1_clus1` Und `node1_clus2` auf Knoten 1 und `node2_clus1` Und `node2_clus2` jeweils an Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind `e0a` Und `e0b` Die

  Der "*NetApp Hardware Universe*" Enthält die aktuellsten Informationen zu den tatsächlichen Cluster-Ports für Ihre Plattformen.

Schritt 1: Vorbereitung auf die Migration

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:

   ```
   cluster1::*> 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 Aufforderung(`*>`) erscheint.

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Deaktivieren Sie alle aktivierten, zum Knoten führenden Ports (nicht ISL-Ports) an beiden neuen Cluster-Switches cs1 **und** cs2.

   > Die ISL-Ports dürfen nicht deaktiviert werden.

   Das folgende Beispiel zeigt, dass die dem Knoten zugewandten Ports 1 bis 16 am Switch cs1 deaktiviert

sind:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# shutdown
(cs1)(Interface 0/1-0/16)# exit
(cs1)(Config)# exit
```

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden BES-53248-Switches cs1 und cs2 aktiv sind:

   ```
   show port-channel
   ```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs1 aktiv sind:

```
(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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
(cs1) #
```

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs2 aktiv sind:

```
(cs2)# 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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

3. Liste der benachbarten Geräte anzeigen:

```
show isdp neighbors
```

Dieser Befehl liefert Informationen über die mit dem System verbundenen Geräte.

Beispiel anzeigen

Das folgende Beispiel listet die benachbarten Geräte am Switch cs1 auf:

```
(cs1)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf     Holdtime  Capability   Platform    Port ID
-------------- -------- --------- ------------ ----------- ---------
cs2            0/55     176       R            BES-53248   0/55
cs2            0/56     176       R            BES-53248   0/56
```

Das folgende Beispiel listet die benachbarten Geräte am Switch cs2 auf:

```
(cs2)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf     Holdtime  Capability   Platform    Port ID
-------------- -------- --------- ------------ ----------- ---------
cs2            0/55     176       R            BES-53248   0/55
cs2            0/56     176       R            BES-53248   0/56
```

4. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

5. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit 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
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true
```

6. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

7. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 1 und verbinden Sie dann e0a mit Port 1 des Cluster-Switches cs1 unter Verwendung der von den BES-53248-Switches unterstützten geeigneten Verkabelung.

   Der "*NetApp Hardware Universe*" enthält weitere Informationen zur Verkabelung.

8. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 2 und verbinden Sie dann e0a mit Port 2 des Cluster-Switches cs1 unter Verwendung der von den BES-53248-Switches unterstützten geeigneten Verkabelung.
9. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs1.

   Das folgende Beispiel zeigt, dass die Ports 1 bis 16 am Switch cs1 aktiviert sind:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/16
(cs1)(Interface 0/1-0/16)# no shutdown
(cs1)(Interface 0/1-0/16)# exit
(cs1)(Config)# exit
```

10. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

11. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit 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
         node1_clus1  up/up      169.254.209.69/16  node1       e0a
true
         node1_clus2  up/up      169.254.49.125/16  node1       e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2       e0a
true
         node2_clus2  up/up      169.254.19.183/16  node2       e0b
true
```

12. Informationen über den Status der Knoten im Cluster anzeigen:

    `cluster show`

    Beispiel anzeigen

    Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster an:

    ```
    cluster1::*> cluster show

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

13. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 1 und verbinden Sie dann e0b mit Port 1 auf Cluster-Switch cs2. Verwenden Sie dazu die von den BES-53248-Switches unterstützten geeigneten Kabel.
14. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 2 und verbinden Sie dann e0b mit Port 2 des Cluster-Switches cs2 unter Verwendung der von den BES-53248-Switches unterstützten geeigneten Verkabelung.
15. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs2.

Das folgende Beispiel zeigt, dass die Ports 1 bis 16 am Switch cs2 aktiviert sind:

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

16. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

`network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

2. Auf Switch cs2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

```
cs2> enable
cs2# configure
cs2(config)# interface 0/1-0/16
cs2(config-if-range)# shutdown

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

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

   `network interface show -vserver Cluster`

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

   `network interface revert -vserver Cluster -lif *`

4. Überprüfen Sie, ob alle Schnittstellen angezeigt werden. `true` für `Is Home` :

   `network interface show -vserver Cluster`

   Dieser Vorgang kann mehrere Minuten dauern.

Beispiel anzeigen

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

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true
```

5. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

   `show isdp neighbors`

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
(cs1)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf         Holdtime  Capability   Platform -- Port
ID
-------------- ------------ --------- ------------ -----------
----------
node1          0/1          175       H            FAS2750     e0a
node2          0/2          157       H            FAS2750     e0a
cs2            0/55         178       R            BES-53248   0/55
cs2            0/56         178       R            BES-53248   0/56


(cs2)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater
Device ID      Intf         Holdtime  Capability   Platform    Port
ID
-------------- ------------ --------- ------------ -----------
------------
node1          0/1          137       H            FAS2750     e0b
node2          0/2          179       H            FAS2750     e0b
cs1            0/55         175       R            BES-53248   0/55
cs1            0/56         175       R            BES-53248   0/56
```

6. Informationen zu den in Ihrem Cluster gefundenen Netzwerkgeräten anzeigen:

   `network device-discovery show -protocol cdp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
```

7. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

   `network options switchless-cluster show`

   Die Ausführung des Befehls kann mehrere Minuten dauern. Warten Sie auf die Ansage „Noch 3 Minuten bis zum Ablauf der Gültigkeitsdauer“.

   Der `false` Die Ausgabe im folgenden Beispiel zeigt, dass die Konfigurationseinstellungen deaktiviert sind:

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

8. Überprüfen Sie den Status der Knoten im Cluster:

   `cluster show`

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster:

```
cluster1::*> cluster show

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

9. 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
------ -------------------------- --------------- -----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

2. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

   Beispiel anzeigen

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=END
   ```

   Weitere Informationen finden Sie unter: "NetApp Knowledge Base-Artikel: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster"

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Ersetzen Sie die Schalter

Ersatzbedarf

Bevor Sie den Schalter austauschen, stellen Sie sicher, dass die folgenden Bedingungen in der aktuellen Umgebung und am Ersatzschalter erfüllt sind.

Vorhandene Cluster- und Netzwerkinfrastruktur

Stellen Sie sicher, dass:

- Der bestehende Cluster wurde als voll funktionsfähig verifiziert, wobei mindestens ein Cluster-Switch vollständig angeschlossen ist.
- Alle Cluster-Ports sind **aktiv**.
- Alle logischen Schnittstellen (LIFs) des Clusters sind administrativ und betriebsbereit und an ihren jeweiligen Ports angeschlossen.
- Das ONTAP `cluster ping-cluster -node node1` Der Befehl muss angeben, dass die Einstellungen `basic connectivity` Und `larger than PMTU communication` sind auf allen Wegen erfolgreich.

BES-53248 Ersatz-Clusterschalter

Stellen Sie sicher, dass:

- Die Management-Netzwerkanbindung des Ersatz-Switches ist funktionsfähig.
- Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
- Die Knotenverbindungen erfolgen über die Ports 0/1 bis 0/16 mit Standardlizenzierung.
- Alle Inter-Switch Link (ISL)-Ports sind an den Ports 0/55 und 0/56 deaktiviert.
- Die gewünschte Referenzkonfigurationsdatei (RCF) und das EFOS-Betriebssystem-Switch-Image werden auf den Switch geladen.
- Die erste Anpassung des Schalters ist abgeschlossen, wie in folgendem Abschnitt detailliert beschrieben:"Konfigurieren des Cluster-Switches BES-53248" Die

Alle zuvor vorgenommenen Anpassungen am Standort, wie z. B. STP, SNMP und SSH, werden auf den neuen Switch kopiert.

Konsolenprotokollierung aktivieren

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

- Lassen Sie AutoSupport während der Wartungsarbeiten aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs AutoSupport aus, um die Fallerstellung für die Dauer der Wartung zu deaktivieren. Siehe diesen Wissensdatenbankartikel "SU92: Wie man die automatische Fallerstellung während geplanter Wartungsfenster unterdrückt" für weitere Einzelheiten.
- Aktivieren Sie die Sitzungsprotokollierung für alle CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Wissensdatenbankartikel. "Wie konfiguriert man PuTTY für eine optimale Verbindung zu ONTAP -Systemen?" Die

Weitere Informationen

- "NetApp Support Site"
- "NetApp Hardware Universe"

Ersetzen Sie einen von Broadcom unterstützten BES-53248-Cluster-Switch

Gehen Sie wie folgt vor, um einen defekten Broadcom-unterstützten BES-53248 Cluster-Switch in einem Cluster-Netzwerk auszutauschen. Dies ist ein unterbrechungsfreies Verfahren (NDU).

Zu den Beispielen

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

- Die Namen der bestehenden BES-53248-Switches lauten: `cs1` Und `cs2` Die
- Die Bezeichnung des neuen BES-53248-Switches lautet: `newcs2` Die
- Die Knotennamen lauten `node1` Und `node2` Die
- Die Cluster-Ports auf jedem Knoten sind benannt `e0a` Und `e0b` Die
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.
- Die Aufforderung zur Änderung aller Clusterknoten lautet: `cluster1::>`

Zur Topologie

Dieses Verfahren basiert auf folgender Cluster-Netzwerktopologie:

Beispieltopologie anzeigen

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

Node: node1

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


Node: node2

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


cluster1::> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
true
```

```
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true


cluster1::> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               BES-
53248
            e0b    cs2                       0/2               BES-
53248
node1      /cdp
            e0a    cs1                       0/1               BES-
53248
            e0b    cs2                       0/1               BES-
53248
```

```
(cs1)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID                Intf      Holdtime  Capability Platform
Port ID
------------------------ --------- --------- ----------
---------------- ---------
node1                    0/1       175       H          FAS2750
e0a
node2                    0/2       152       H          FAS2750
e0a
cs2                      0/55      179       R          BES-53248
0/55
cs2                      0/56      179       R          BES-53248
0/56


(cs2)# show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID                Intf      Holdtime  Capability Platform
Port ID
------------------------ --------- --------- ----------
---------------- ---------
node1                    0/1       129       H          FAS2750
e0b
node2                    0/2       165       H          FAS2750
e0b
cs1                      0/55      179       R          BES-53248
0/55
cs1                      0/56      179       R          BES-53248
0/56
```

Schritte

1. Überprüfen Sie die"Ersatzbedarf" Die
2. 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.

3. Installieren Sie die entsprechende Referenzkonfigurationsdatei (RCF) und das Image auf dem Switch newcs2 und treffen Sie alle notwendigen Vorbereitungen vor Ort.

   Prüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und EFOS-Software für den neuen Switch. Wenn Sie überprüft haben, dass der neue Switch korrekt eingerichtet ist und keine Aktualisierungen der RCF- und EFOS-Software erforderlich sind, fahren Sie mit Schritt 2 fort.

   a. Sie können die passende Broadcom EFOS-Software für Ihre Cluster-Switches von der folgenden Website herunterladen: "Broadcom Ethernet-Switch-Unterstützung" Website. Folgen Sie den Anweisungen auf der Downloadseite, um die EFOS-Datei für die Version der ONTAP -Software herunterzuladen, die Sie installieren.

   b. Die entsprechende RCF ist erhältlich bei der "Broadcom Cluster-Switches" Seite. Folgen Sie den Anweisungen auf der Downloadseite, um die richtige RCF-Datei für die Version der ONTAP -Software herunterzuladen, die Sie installieren.

4. Melden Sie sich auf dem neuen Switch an als `admin` und schalten Sie alle Ports ab, die mit den Schnittstellen des Knotenclusters verbunden werden (Ports 1 bis 16).

   > Falls Sie zusätzliche Lizenzen für weitere Ports erworben haben, schalten Sie auch diese Ports ab.

   Falls der zu ersetzende Switch nicht funktionsfähig und ausgeschaltet ist, sollten die LIFs auf den Clusterknoten bereits auf den anderen Clusterport für jeden Knoten umgeschaltet haben.

   > Für die Anmeldung ist kein Passwort erforderlich. `enable` Modus.

   Beispiel anzeigen

   ```
   User: admin
   Password:
   (newcs2)> enable
   (newcs2)# config
   (newcs2)(config)# interface 0/1-0/16
   (newcs2)(interface 0/1-0/16)# shutdown
   (newcs2)(interface 0/1-0/16)# exit
   (newcs2)(config)# exit
   (newcs2)#
   ```

5. Überprüfen Sie, ob alle Cluster-LIFs vorhanden sind. `auto-revert` ermöglicht:

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

Beispieltopologie anzeigen

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

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

6. Schalten Sie die ISL-Ports 0/55 und 0/56 am BES-53248-Switch cs1 ab:

Beispieltopologie anzeigen

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# shutdown
```

7. Entfernen Sie alle Kabel vom BES-53248 cs2 Switch und schließen Sie sie dann an die gleichen Ports am BES-53248 newcs2 Switch an.
8. Aktivieren Sie die ISL-Ports 0/55 und 0/56 zwischen den Switches cs1 und newcs2 und überprüfen Sie dann den Betriebsstatus des Portkanals.

   Der Verbindungsstatus für Portkanal 1/1 sollte **up** sein und alle Mitgliedsports sollten unter der Überschrift „Port aktiv“ den Wert „True“ haben.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 0/55 und 0/56 und zeigt den Verbindungsstatus für Portkanal 1/1 auf Switch cs1 an:

```
(cs1)# config
(cs1)(config)# interface 0/55-0/56
(cs1)(interface 0/55-0/56)# no shutdown
(cs1)(interface 0/55-0/56)# exit
(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    100G Full  True
       partner/long
0/56   actor/long    100G Full  True
       partner/long
```

9. Auf dem neuen Switch newcs2 müssen alle Ports, die mit den Schnittstellen des Knotenclusters verbunden sind (Ports 1 bis 16), wieder aktiviert werden.

Falls Sie zusätzliche Lizenzen für weitere Ports erworben haben, schalten Sie auch diese Ports ab.

Beispiel anzeigen

```
User:admin
Password:
(newcs2)> enable
(newcs2)# config
(newcs2)(config)# interface 0/1-0/16
(newcs2)(interface 0/1-0/16)# no shutdown
(newcs2)(interface 0/1-0/16)# exit
(newcs2)(config)# exit
```

10. Überprüfen Sie, ob Port e0b **aktiv** ist:

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

Beispiel anzeigen

Die Ausgabe sollte in etwa wie folgt aussehen:

```
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/auto   -
false
```

11. Warten Sie auf demselben Knoten, den Sie im vorherigen Schritt verwendet haben, bis der Cluster-LIF node1_clus2 auf Knoten 1 automatisch zurückgesetzt wird.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn `Is Home` Ist `true` und der Port ist e0b.

Der folgende Befehl zeigt Informationen über die LIFs auf beiden Knoten an. Das Hochfahren des ersten Knotens ist erfolgreich, wenn `Is Home` Ist `true` für beide Cluster-Schnittstellen und sie zeigen die korrekten Portzuweisungen an, in diesem Beispiel `e0a` Und `e0b` auf Knoten1.

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false
```

12. Informationen über die Knoten in einem Cluster anzeigen:

    `cluster show`

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Knotenzustand für `node1` Und `node2` in diesem Cluster ist `true` :

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

13. Bestätigen Sie die folgende Cluster-Netzwerkkonfiguration:

    `network port show`

```
network interface show
```

Beispiel anzeigen

```
cluster1::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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


cluster1::> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
```

```
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

14. Überprüfen Sie, ob das Clusternetzwerk fehlerfrei funktioniert:

    `show isdp neighbors`

    Beispiel anzeigen

```
(cs1)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater
Device ID    Intf    Holdtime    Capability    Platform    Port ID
---------    ----    --------    ----------    --------    --------
node1        0/1     175         H             FAS2750     e0a
node2        0/2     152         H             FAS2750     e0a
newcs2       0/55    179         R             BES-53248   0/55
newcs2       0/56    179         R             BES-53248   0/56

(newcs2)# show isdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route
Bridge,
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Intf    Holdtime    Capability    Platform    Port ID
---------    ----    --------    ----------    --------    --------
node1        0/1     129         H             FAS2750     e0b
node2        0/2     165         H             FAS2750     e0b
cs1          0/55    179         R             BES-53248   0/55
cs1          0/56    179         R             BES-53248   0/56
```

15. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nachdem Sie Ihre Schalter ausgetauscht haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Ersetzen Sie Broadcom BES-53248 Cluster-Switches durch switchlose Verbindungen.

Für ONTAP 9.3 und höher können Sie von einem Cluster mit einem Switched-Cluster-Netzwerk zu einem Cluster migrieren, in dem zwei Knoten direkt miteinander verbunden sind.

Überprüfungsanforderungen

Richtlinien

Bitte beachten Sie die folgenden Richtlinien:

- Die Migration zu einer Zwei-Knoten-Clusterkonfiguration ohne Switches ist ein unterbrechungsfreier Vorgang. Die meisten Systeme verfügen über zwei dedizierte Cluster-Interconnect-Ports pro Knoten. Dieses Verfahren kann aber auch für Systeme mit einer größeren Anzahl dedizierter Cluster-Interconnect-Ports pro Knoten angewendet werden, beispielsweise vier, sechs oder acht.
- Die Funktion „Switchless Cluster Interconnect“ kann nicht mit mehr als zwei Knoten verwendet werden.
- Wenn Sie über einen bestehenden Zwei-Knoten-Cluster verfügen, der Cluster-Interconnect-Switches verwendet und auf dem ONTAP 9.3 oder höher läuft, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Knoten ersetzen.

Bevor Sie beginnen

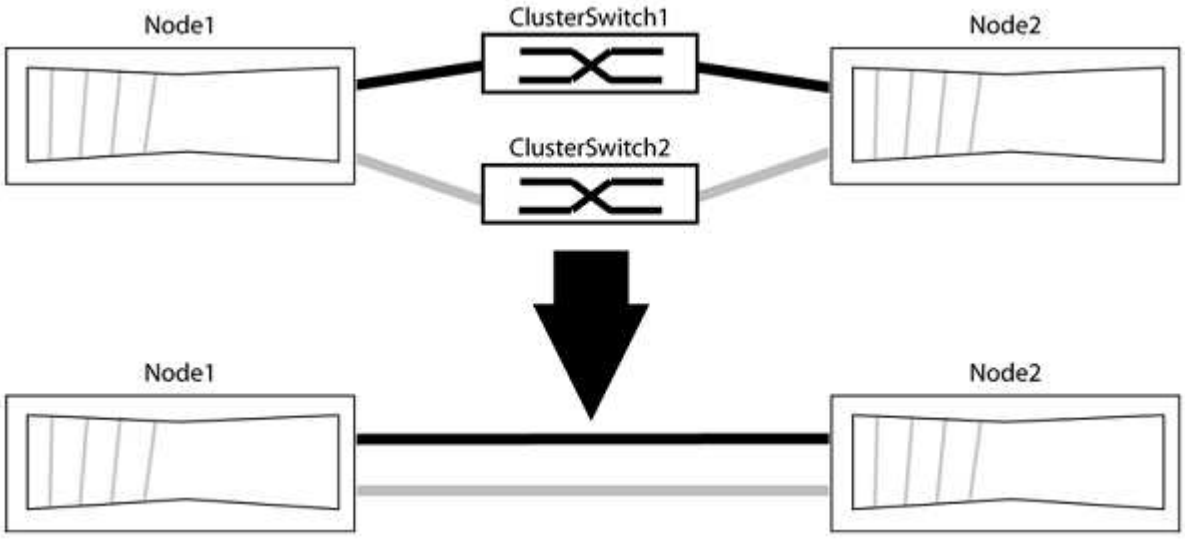
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesunder Cluster, der aus zwei Knoten besteht, die über Cluster-Switches verbunden sind. Auf den Knoten muss die gleiche ONTAP Version laufen.
- Jeder Knoten verfügt über die erforderliche Anzahl dedizierter Cluster-Ports, die redundante Cluster-Verbindungen bereitstellen, um Ihre Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster-Verbindungsports auf jedem Knoten.

Migrieren Sie die Schalter

Informationen zu diesem Vorgang

Das folgende Verfahren entfernt die Cluster-Switches in einem Zwei-Knoten-Cluster und ersetzt jede Verbindung zum Switch durch eine direkte Verbindung zum Partnerknoten.



Zu den Beispielen

Die Beispiele im folgenden Verfahren zeigen Knoten, die "e0a" und "e0b" als Cluster-Ports verwenden. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.

Schritt 1: Vorbereitung auf die Migration

1. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung `*>` erscheint.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von switchlosen Clustern, die standardmäßig aktiviert ist.

   Sie können überprüfen, ob die Erkennung von Clustern ohne Switch aktiviert ist, indem Sie den Befehl mit erweiterten Berechtigungen ausführen:

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

   Beispiel anzeigen

   Die folgende Beispielausgabe zeigt, ob die Option aktiviert ist.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Wenn "Schalterlose Clustererkennung aktivieren" `false` Wenden Sie sich an den NetApp Support.

3. 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=<number_of_hours>h
   ```

   Wo `h` ist die Dauer des Wartungsfensters in Stunden. Die Meldung informiert den technischen Support über diese Wartungsaufgabe, damit dieser die automatische Fallerstellung während des Wartungsfensters unterdrücken kann.

   Im folgenden Beispiel unterdrückt der Befehl die automatische Fallerstellung für zwei Stunden:

   Beispiel anzeigen

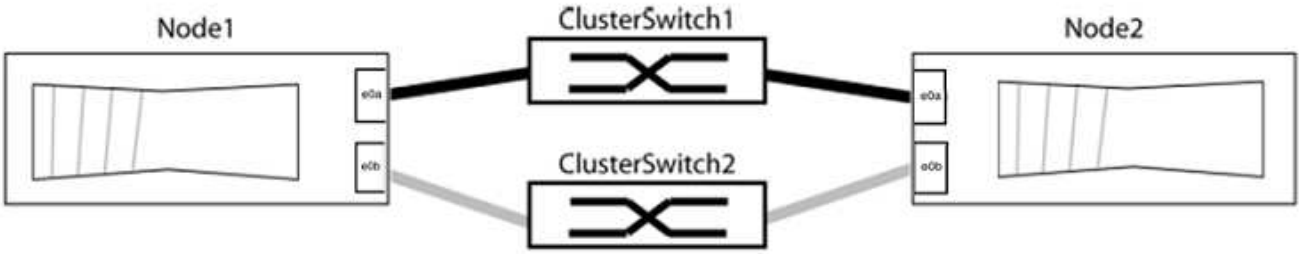
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen ein, sodass die Cluster-Ports in Gruppe 1 an Cluster-Switch 1 und die Cluster-Ports in Gruppe 2 an Cluster-Switch 2 angeschlossen werden. Diese Gruppen werden im weiteren Verlauf des Verfahrens benötigt.
2. Identifizieren Sie die Cluster-Ports und überprüfen Sie den Verbindungsstatus und die Integrität:

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

   Im folgenden Beispiel für Knoten mit Cluster-Ports „e0a“ und „e0b“ wird eine Gruppe als „node1:e0a“ und „node2:e0a“ und die andere Gruppe als „node1:e0b“ und „node2:e0b“ identifiziert. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.

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

Beispiel anzeigen

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Vergewissern Sie sich, dass alle Cluster-LIFs an ihren jeweiligen Heimatports angeschlossen sind.

   Überprüfen Sie, ob die Spalte „is-home“ `true` für jeden der Cluster-LIFs:

   `network interface show -vserver Cluster -fields is-home`

Beispiel anzeigen

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Falls Cluster-LIFs vorhanden sind, die sich nicht auf ihren Heimatports befinden, werden diese LIFs wieder auf ihre Heimatports zurückgesetzt:

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

4. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

5. Überprüfen Sie, ob alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

   In der Spalte „Erkanntes Gerät“ sollte der Name des Cluster-Switches stehen, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports "e0a" und "e0b" korrekt mit den Cluster-Switches "cs1" und "cs2" verbunden sind.

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 7]] Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster ring show
   ```

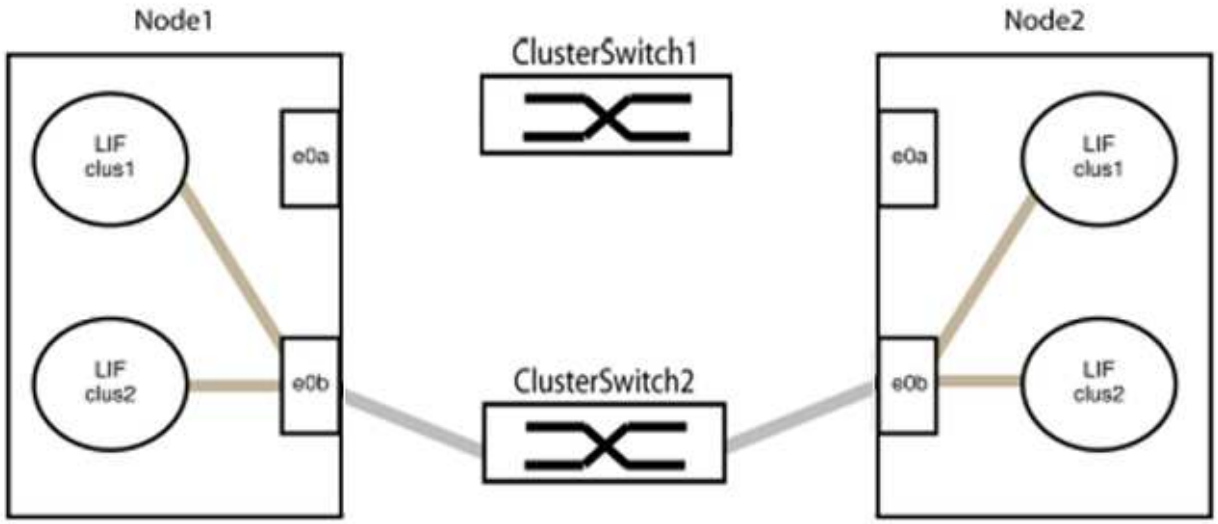
   Alle Einheiten müssen entweder Master- oder Sekundäreinheiten sein.

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

   > Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe1 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

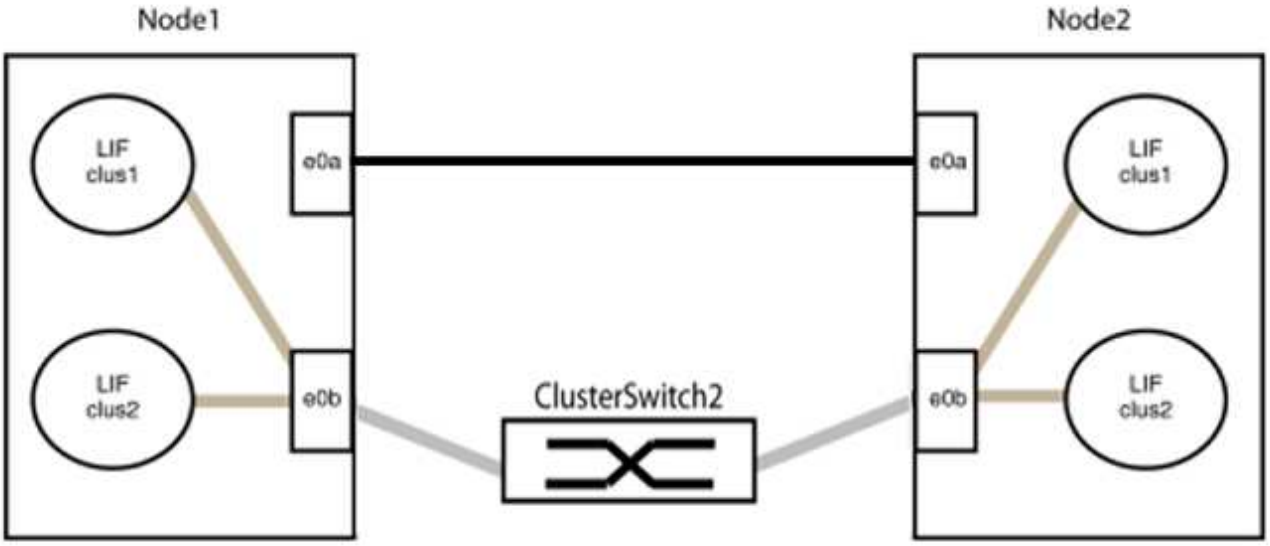
   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

      Im folgenden Beispiel werden die Kabel an Port „e0a“ auf jedem Knoten getrennt, und der Cluster-Datenverkehr wird weiterhin über den Switch und Port „e0b“ auf jedem Knoten abgewickelt:



b. Verbinden Sie die Ports in Gruppe 1 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden:



3. Die Option für ein schalterloses Clusternetzwerk wechselt von `false` Zu `true` Die Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „Schalterlos“ aktiviert ist. `true` :

`network options switchless-cluster show`

Das folgende Beispiel zeigt, dass der switchlose Cluster aktiviert ist:

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

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

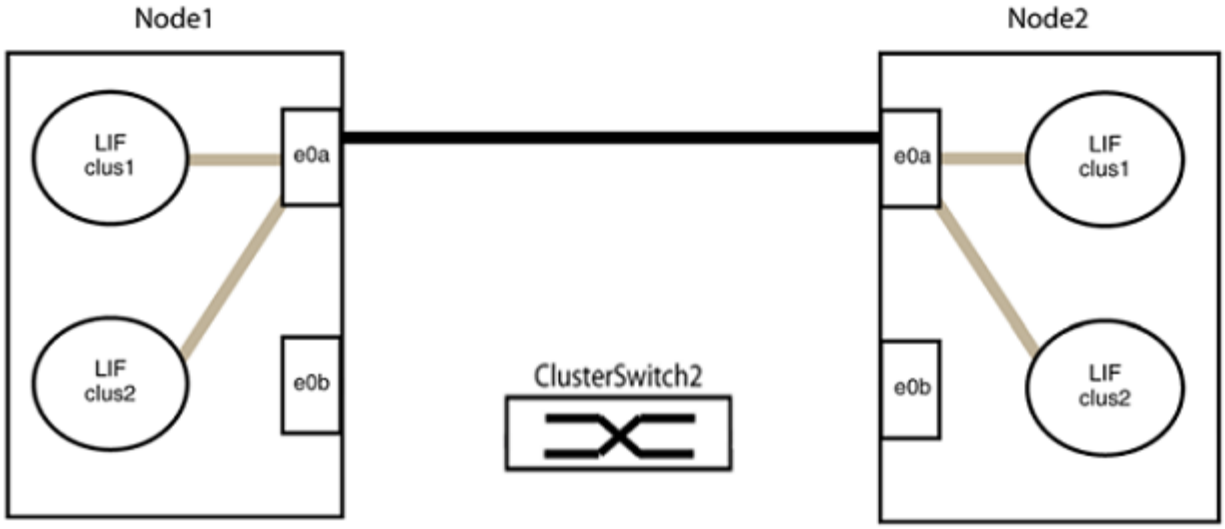
Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung in Gruppe 1 zu bestätigen.

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

   Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe 2 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 2.

      Im folgenden Beispiel werden die Kabel von Port "e0b" an jedem Knoten getrennt, und der Cluster-Datenverkehr wird über die direkte Verbindung zwischen den Ports "e0a" fortgesetzt:



b. Verbinden Sie die Ports in Gruppe 2 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden und "e0b" auf Knoten 1 ist mit "e0b" auf Knoten 2 verbunden:

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie, ob die Ports an beiden Knoten korrekt verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port des Cluster-Partners verbunden sind:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Automatische Rücksetzung für die Cluster-LIFs wieder aktivieren:

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

3. Überprüfen Sie, ob alle LIFs zu Hause sind. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „Ist zu Hause“ den Wert „Ist zu Hause“ aufweist. `true` , wie gezeigt für `node1_clus2` Und `node2_clus2` im folgenden Beispiel:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif          curr-port is-home
-------- ------------ --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

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

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

4. Überprüfen Sie den Clusterstatus der Knoten über die Systemkonsole eines der beiden Knoten:

   `cluster show`

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass epsilon an beiden Knoten gleich ist. `false` :

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Falls Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

   Weitere Informationen finden Sie unter "NetApp KB-Artikel 1010449: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster".

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

Wie geht es weiter?

Nachdem Sie Ihre Schalter ausgetauscht haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

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

Erste Schritte

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

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

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

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

1. **"Überprüfen der Konfigurationsanforderungen"**
   Überprüfen Sie die Konfigurationsanforderungen für die Cluster-Switches 9336C-FX2 und 9336C-FX2-T.
2. **"Überprüfen Sie die Komponenten und Teilenummern"**
   Überprüfen Sie die Komponenten und Teilenummern für die Cluster-Switches 9336C-FX2 und 9336C-FX2-T.
3. **"Überprüfen Sie die erforderlichen Unterlagen"**
   Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 9336C-FX2- und 9336C-FX2-T-Switches und den ONTAP Cluster einzurichten.
4. **"Überprüfen Sie die Smart Call Home-Anforderungen"**
   Überprüfen Sie die Anforderungen für die Cisco Smart Call Home-Funktion, die zur Überwachung der Hardware- und Softwarekomponenten in Ihrem Netzwerk verwendet wird.
5. **"Installieren Sie die Hardware"**
   Installieren Sie die Switch-Hardware.
6. **"Konfigurieren der Software"**
   Konfigurieren Sie die Switch-Software.

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

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

ONTAP-Unterstützung

ONTAP 9.9.1 und höher

Ab ONTAP 9.9.1 können Sie Cisco Nexus 9336C-FX2 Switches verwenden, um Speicher- und Clusterfunktionen in einer gemeinsamen Switch-Konfiguration zu kombinieren.

Wenn Sie ONTAP -Cluster mit mehr als zwei Knoten aufbauen möchten, benötigen Sie zwei unterstützte Netzwerk-Switches.

Der Ethernet-Switch-Health-Monitor unterstützt weder ONTAP 9.13.1P8 und ältere Versionen noch 9.14.1P3 und ältere Versionen oder NX-OS Version 10.3(4a)(M).

ONTAP 9.10.1 und höher

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

Wenn Sie ONTAP -Cluster mit mehr als zwei Knoten aufbauen möchten, benötigen Sie zwei unterstützte Netzwerk-Switches.

Konfigurationsanforderungen

Stellen Sie sicher, dass:

- Sie verfügen über die passende Anzahl und Art an Kabeln und Kabelsteckern für Ihre Switches. Siehe die "Hardware Universe" Die
- Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolenport herstellen.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie folgende Netzwerkinformationen.

- IP-Subnetz für den Verwaltungsnetzwerkverkehr
- Hostnamen und IP-Adressen für jeden Speichersystem-Controller und alle entsprechenden Switches
- Die meisten Speichersystem-Controller werden über die e0M-Schnittstelle verwaltet, indem eine Verbindung zum Ethernet-Service-Port (Schraubenschlüsselsymbol) hergestellt wird. Bei den Systemen AFF A800 und AFF A700s verwendet die e0M-Schnittstelle einen dedizierten Ethernet-Anschluss.
- Siehe die "Hardware Universe" für die aktuellsten Informationen.

Weitere Informationen zur Erstkonfiguration Ihres Switches finden Sie in der folgenden Anleitung: "Cisco Nexus 9336C-FX2 Installations- und Upgrade-Leitfaden" Die

Was kommt als nächstes

Nachdem Sie die Konfigurationsanforderungen geprüft haben, können Sie Ihre "Komponenten und Teilenummern"Die

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

Bei der Installation und Wartung der Cisco Nexus Switches 9336C-FX2 und 9336C-FX2-T sollten Sie unbedingt die Liste der Komponenten und Teilenummern überprüfen.

Details zur Teilenummer

Die folgende Tabelle listet die Teilenummer und Beschreibung für die Schalter, Lüfter und Netzteile 9336C-FX2 und 9336C-FX2-T auf:

Teilenummer	Beschreibung
X190200-CS-PE	Cluster-Schalter, N9336C 36Pt PTSX 10/25/40/100G
X190200-CS-PI	Cluster-Schalter, N9336C 36Pt PSIN 10/25/40/100G
X190212-CS-PE	Cluster-Schalter, N9336C 12Pt (9336C-FX2-T) PTSX 10/25/40/100G
X190212-CS-PI	Clusterschalter, N9336C 12Pt (9336C-FX2-T) PSIN 10/25/40/100G
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2 24-Port POD-Lizenz
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Zubehörset X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100W Netzteil - Abluftführung an der linken Seite
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100W Netzteil - Lufteinlass an der linken Seite
X-NXA-FAN-65CFM-PE	N9K-9336C 65 CFM, Abluftstrom an der Backbordseite
X-NXA-FAN-65CFM-PI	N9K-9336C 65 CFM, Einlassluftstrom auf der Backbordseite

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

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

1. Erstellen Sie bei Bedarf ein neues Smart-Konto. Sehen "Erstellen Sie ein neues Smart-Konto" für Details.
2. Zugriff auf ein bestehendes Smart-Konto anfordern. Sehen "Zugriff auf ein bestehendes Smart-Konto anfordern" für Details.

> ⓘ Sobald Sie Ihre Smart-Lizenz erworben haben, installieren Sie die entsprechende RCF-Datei, um alle 36 verfügbaren Ports zu aktivieren und zu konfigurieren.

Was kommt als nächstes

Nachdem Sie Ihre Komponenten und Teilenummern bestätigt haben, können Sie die folgenden überprüfen: "erforderliche Dokumentation"Die

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

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

Switch-Dokumentation

Für die Einrichtung der Cisco Nexus Switches 9336C-FX2 und 9336C-FX2-T benötigen Sie die folgende Dokumentation von "Cisco Nexus 9000 Series Switches Unterstützung" Seite:

Dokumenttitel	Beschreibung
Hardware-Installationsanleitung für die Nexus 9000-Serie	Bietet detaillierte Informationen zu Standortanforderungen, Hardware-Details der Schalter und Installationsoptionen.
Softwarekonfigurationshandbücher für Cisco Nexus 9000 Series Switches (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version aus)	Liefert die grundlegenden Switch-Konfigurationsinformationen, die Sie benötigen, bevor Sie den Switch für den ONTAP -Betrieb konfigurieren können.
Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide (Wählen Sie den Leitfaden für die auf Ihren Switches installierte NX-OS-Version aus)	Bietet Informationen darüber, wie der Switch gegebenenfalls auf eine von ONTAP unterstützte Switch-Software heruntergestuft werden kann.
Cisco Nexus 9000 Serie NX-OS Befehlsreferenz – Masterindex	Bietet Links zu den verschiedenen Befehlsreferenzen von Cisco.
Cisco Nexus 9000 MIBs-Referenz	Beschreibt die Management Information Base (MIB)-Dateien für die Nexus 9000 Switches.
Referenz der NX-OS-Systemmeldungen der Nexus 9000-Serie	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000-Serie, sowohl die informativen als auch die, die bei der Diagnose von Problemen mit Verbindungen, interner Hardware oder der Systemsoftware hilfreich sein können.
Cisco Nexus 9000 Series NX-OS Versionshinweise (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)	Beschreibt die Funktionen, Fehler und Einschränkungen der Cisco Nexus 9000-Serie.
Informationen zur Einhaltung gesetzlicher Bestimmungen und zur Sicherheit für die Cisco Nexus 9000-Serie	Bietet Informationen zur Einhaltung internationaler behördlicher Vorschriften, zur Sicherheit und zu gesetzlichen Bestimmungen für die Switches der Serie Nexus 9000.

ONTAP-Systemdokumentation

Um ein ONTAP -System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Version des Betriebssystems von "ONTAP 9" Die

Name	Beschreibung
Controllerspezifische *Installations- und Einrichtungsanweisungen*	Beschreibt die Installation von NetApp -Hardware.
ONTAP-Dokumentation	Bietet detaillierte Informationen zu allen Aspekten der ONTAP Releases.
"Hardware Universe"	Bietet Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Dokumentation für Schienenbausatz und Schrank

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

Name	Beschreibung
"42U Systemschrank, Tiefenführung"	Beschreibt die mit dem 42U-Systemschrank verbundenen FRUs und gibt Anweisungen zur Wartung und zum Austausch der FRUs.
"Installieren Sie einen Cisco 9336-FX2 Switch in einem NetApp Schrank"	Beschreibt, wie Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem NetApp Schrank mit vier Pfosten installiert werden.

Anforderungen für Smart Call Home

Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch für die Kommunikation per E-Mail mit dem Smart Call Home-System konfigurieren. Darüber hinaus können Sie Ihren Cluster-Netzwerk-Switch optional so einrichten, dass er die integrierte Smart Call Home-Supportfunktion von Cisco nutzt.

Smart Call Home überwacht die Hardware- und Softwarekomponenten in Ihrem Netzwerk. Wenn eine kritische Systemkonfiguration auftritt, wird eine E-Mail-Benachrichtigung generiert und ein Alarm an alle Empfänger gesendet, die in Ihrem Zielprofil konfiguriert sind.

Smart Call Home überwacht die Hardware- und Softwarekomponenten in Ihrem Netzwerk. Wenn eine kritische Systemkonfiguration auftritt, wird eine E-Mail-Benachrichtigung generiert und ein Alarm an alle Empfänger gesendet, die in Ihrem Zielprofil konfiguriert sind.

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

- Ein E-Mail-Server muss vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Kontaktname (SNMP-Server-Kontakt), die Telefonnummer und die Straßenadresse müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu ermitteln.

- Eine CCO-ID muss mit einem passenden Cisco SMARTnet Servicevertrag für Ihr Unternehmen verknüpft sein.
- Für die Registrierung des Geräts muss der Cisco SMARTnet-Dienst eingerichtet sein.

Der "Cisco Supportseite" enthält Informationen zu den Befehlen zur Konfiguration von Smart Call Home.

Installieren Sie die Hardware

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

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

1. **"Vervollständigen Sie das Verkabelungsarbeitsblatt"**

   Das Beispiel-Verkabelungs-Arbeitsblatt enthält Beispiele für empfohlene Portzuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt dient als Vorlage, die Sie beim Einrichten Ihres Clusters verwenden können.

2. **"Installieren Sie den Schalter"**

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

3. **"Installieren Sie den Switch in einem NetApp -Schrank."**

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

4. **"Kabel und Konfiguration prüfen"**

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

Füllen Sie das Verkabelungsarbeitsblatt für Cisco Nexus 9336C-FX2 oder 9336C-FX2-T aus.

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

Das Beispiel-Verkabelungs-Arbeitsblatt enthält Beispiele für empfohlene Portzuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt dient als Vorlage, die Sie beim Einrichten Ihres Clusters verwenden können.

- 9336C-FX2 Beispiel-Verkabelungsarbeitsblatt
- 9336C-FX2 leeres Verkabelungs-Arbeitsblatt
- 9336C-FX2-T Muster-Verkabelungsplan (12-Port)
- 9336C-FX2-T Blindkabel-Arbeitsblatt (12-Port)

9336C-FX2 Beispiel-Verkabelungsarbeitsblatt

Die Beispiel-Portdefinition für jedes Switch-Paar lautet wie folgt:

Clusterschalter A		Clusterschalter B	
Switch-Port	Knoten- und Portnutzung	Switch-Port	Knoten- und Portnutzung
1	4x10GbE-Knoten 1	1	4x10GbE-Knoten 1
2	4x10GbE-Knoten 2	2	4x10GbE-Knoten 2
3	4x10GbE-Knoten 3	3	4x10GbE-Knoten 3
4	4x25GbE-Knoten 4	4	4x25GbE-Knoten 4
5	4x25GbE-Knoten 5	5	4x25GbE-Knoten 5
6	4x25GbE-Knoten 6	6	4x25GbE-Knoten 6
7	40/100GbE-Knoten 7	7	40/100GbE-Knoten 7
8	40/100GbE-Knoten 8	8	40/100GbE-Knoten 8
9	40/100GbE-Knoten 9	9	40/100GbE-Knoten 9
10	40/100GbE-Knoten 10	10	40/100GbE-Knoten 10
11	40/100GbE-Knoten 11	11	40/100GbE-Knoten 11
12	40/100GbE-Knoten 12	12	40/100GbE-Knoten 12
13	40/100GbE-Knoten 13	13	40/100GbE-Knoten 13
14	40/100GbE-Knoten 14	14	40/100GbE-Knoten 14
15	40/100GbE-Knoten 15	15	40/100GbE-Knoten 15
16	40/100GbE-Knoten 16	16	40/100GbE-Knoten 16
17	40/100GbE-Knoten 17	17	40/100GbE-Knoten 17
18	40/100GbE-Knoten 18	18	40/100GbE-Knoten 18
19	40/100GbE-Knoten 19	19	40/100GbE-Knoten 19
20	40/100GbE-Knoten 20	20	40/100GbE-Knoten 20

Clusterschalter A		Clusterschalter B	
21	40/100GbE-Knoten 21	21	40/100GbE-Knoten 21
22	40/100GbE-Knoten 22	22	40/100GbE-Knoten 22
23	40/100GbE-Knoten 23	23	40/100GbE-Knoten 23
24	40/100GbE-Knoten 24	24	40/100GbE-Knoten 24
25 bis 34	Reserviert	25 bis 34	Reserviert
35	100GbE ISL zu Switch B Port 35	35	100GbE ISL zu Switch A Port 35
36	100GbE ISL zu Switch B Port 36	36	100GbE ISL zu Switch A Port 36

9336C-FX2 leeres Verkabelungs-Arbeitsblatt

Mithilfe des leeren Verkabelungsarbeitsblatts können Sie die Plattformen dokumentieren, die als Knoten in einem Cluster unterstützt werden. Der Abschnitt *Unterstützte Clusterverbindungen* der "Hardware Universe" Definiert die von der Plattform verwendeten Cluster-Ports.

Clusterschalter A		Clusterschalter B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	

Clusterschalter A		Clusterschalter B	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 bis 34	Reserviert	25 bis 34	Reserviert
35	100GbE ISL zu Switch B Port 35	35	100GbE ISL zu Switch A Port 35
36	100GbE ISL zu Switch B Port 36	36	100GbE ISL zu Switch A Port 36

9336C-FX2-T Muster-Verkabelungsplan (12-Port)

Die Beispiel-Portdefinition für jedes Switch-Paar lautet wie folgt:

Clusterschalter A		Clusterschalter B	
Switch-Port	Knoten- und Portnutzung	Switch-Port	Knoten- und Portnutzung
1	4x10GbE-Knoten 1	1	4x10GbE-Knoten 1

Clusterschalter A		Clusterschalter B	
2	4x10GbE-Knoten 2	2	4x10GbE-Knoten 2
3	4x10GbE-Knoten 3	3	4x10GbE-Knoten 3
4	4x25GbE-Knoten 4	4	4x25GbE-Knoten 4
5	4x25GbE-Knoten 5	5	4x25GbE-Knoten 5
6	4x25GbE-Knoten 6	6	4x25GbE-Knoten 6
7	40/100GbE-Knoten 7	7	40/100GbE-Knoten 7
8	40/100GbE-Knoten 8	8	40/100GbE-Knoten 8
9	40/100GbE-Knoten 9	9	40/100GbE-Knoten 9
10	40/100GbE-Knoten 10	10	40/100GbE-Knoten 10
11 bis 34	Lizenz erforderlich	11 bis 34	Lizenz erforderlich
35	100GbE ISL zu Switch B Port 35	35	100GbE ISL zu Switch A Port 35
36	100GbE ISL zu Switch B Port 36	36	100GbE ISL zu Switch A Port 36

9336C-FX2-T Blindkabel-Arbeitsblatt (12-Port)

Mithilfe des leeren Verkabelungsarbeitsblatts können Sie die Plattformen dokumentieren, die als Knoten in einem Cluster unterstützt werden. Der Abschnitt *Unterstützte Clusterverbindungen* der "Hardware Universe" Definiert die von der Plattform verwendeten Cluster-Ports.

Clusterschalter A		Clusterschalter B	
1		1	
2		2	
3		3	
4		4	
5		5	

Clusterschalter A		Clusterschalter B	
6		6	
7		7	
8		8	
9		9	
10		10	
11 bis 34	Lizenz erforderlich	11 bis 34	Lizenz erforderlich
35	100GbE ISL zu Switch B Port 35	35	100GbE ISL zu Switch A Port 35
36	100GbE ISL zu Switch B Port 36	36	100GbE ISL zu Switch A Port 36

Siehe die "Hardware Universe" Weitere Informationen zu Switch-Ports finden Sie hier.

Was kommt als nächstes

Nachdem Sie Ihre Verkabelungsarbeitsblätter ausgefüllt haben, können Sie "Installieren Sie den Schalter"Die

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server am Installationsort, um die entsprechenden NX-OS- und Referenzkonfigurationsdatei-(RCF)-Versionen herunterzuladen.
- Anwendbare NX-OS-Version, heruntergeladen von "Cisco -Software-Download" Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.
- Vollendet"Verkabelungs-Arbeitsblätter" Die
- Anwendbare NetApp -Clusternetzwerk- und Managementnetzwerk-RCFs, die von der NetApp -Support -Website heruntergeladen wurden unter "mysupport.netapp.com" Die Alle Cisco Cluster-Netzwerk- und Management-Netzwerk-Switches werden mit der standardmäßigen Cisco -Werkskonfiguration ausgeliefert. Diese Switches verfügen ebenfalls über die aktuelle Version der NX-OS-Software, haben jedoch die RCFs nicht geladen.
- "Erforderliche Switch- und ONTAP Dokumentation".

Schritte

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

Wenn Sie die… installieren	Dann…
Cisco Nexus 9336C-FX2 in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden *Installing a Cisco Nexus 9336C-FX2 cluster switch and pass-through panel in a NetApp cabinet*.
Ausrüstung in einem Telekommunikationsrack	Beachten Sie die in den Hardware-Installationshandbüchern für Switches und den Installations- und Einrichtungsanweisungen von NetApp beschriebenen Vorgehensweisen.

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

Wie geht es weiter?

Optional können Sie "Installieren Sie einen Cisco Nexus 9336C-FX2 Switch in einem NetApp Schrank"Die Ansonsten gehen Sie zu "Verkabelung und Konfiguration überprüfen"Die

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

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

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

  - Eine Durchgangs-Blindplatte
  - Vier 10-32 x 0,75 Schrauben
  - Vier 10-32 Clipmuttern
- Für jeden Schalter acht 10-32- oder 12-24-Schrauben und Clipmuttern zur Befestigung der Halterungen und Gleitschienen an den vorderen und hinteren Schrankpfosten.
- Das Cisco Standard-Schienenkit zur Installation des Switches in einem NetApp Schrank.

> Die Überbrückungskabel sind nicht im Durchgangskit enthalten und sollten Ihren Schaltern beiliegen. Falls sie nicht mit den Switches geliefert wurden, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

- Informationen zu den erforderlichen Vorbereitungen, dem Inhalt des Kits und den Sicherheitsvorkehrungen finden Sie unter "Hardware-Installationshandbuch für die Cisco Nexus 9000-Serie" Die

Schritte

1. Installieren Sie die Durchgangsabdeckung im NetApp -Schrank.

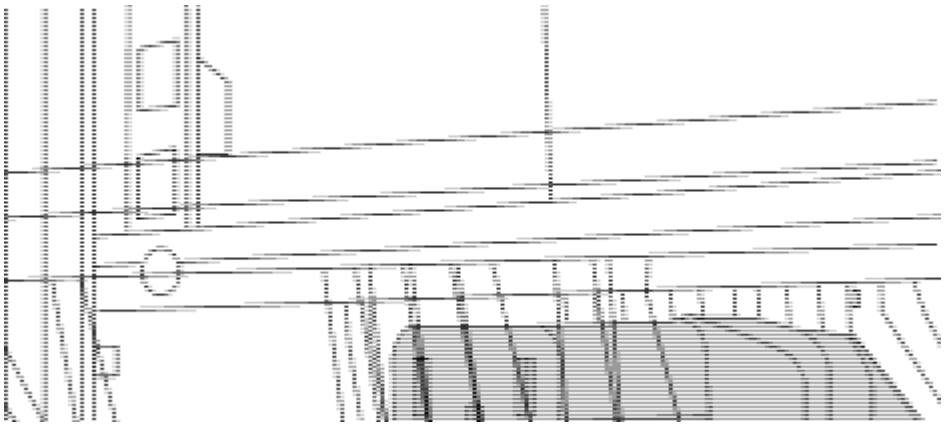
   a. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

Bei diesem Verfahren wird die Abdeckplatte in U40 installiert.

b. Montieren Sie auf jeder Seite zwei Clipmuttern in den entsprechenden quadratischen Löchern für die vorderen Schrankschienen.

c. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.

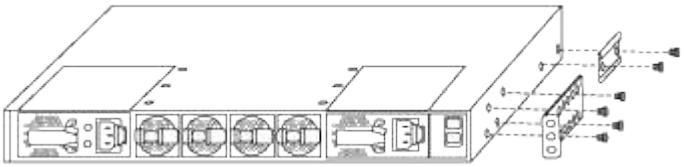
d. Führen Sie die weiblichen Stecker beider 48-Zoll-Überbrückungskabel von der Rückseite des Bedienfelds durch die Bürstenbaugruppe.



(1) Weiblicher Stecker des Überbrückungskabels.

2. Montieren Sie die Rack-Montagehalterungen am Nexus 9336C-FX2 Switch-Gehäuse.

a. Positionieren Sie eine vordere Rackmontagehalterung auf einer Seite des Switch-Gehäuses, sodass die Montageöse mit der Gehäusefrontplatte (auf der Netzteil- oder Lüfterseite) ausgerichtet ist, und befestigen Sie die Halterung dann mit vier M4-Schrauben am Gehäuse.

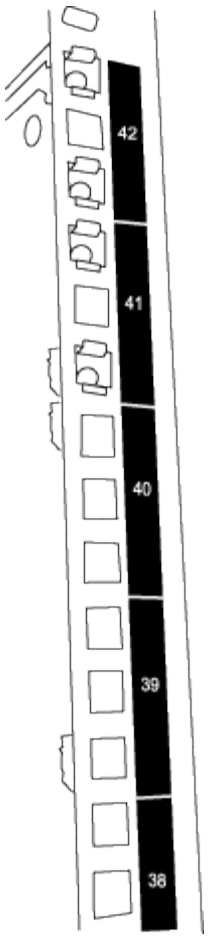


b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.

c. Installieren Sie die hintere Rackmontagehalterung am Switch-Gehäuse.

d. Wiederholen Sie Schritt 2c mit der anderen hinteren Rackmontagehalterung auf der anderen Seite des Switches.

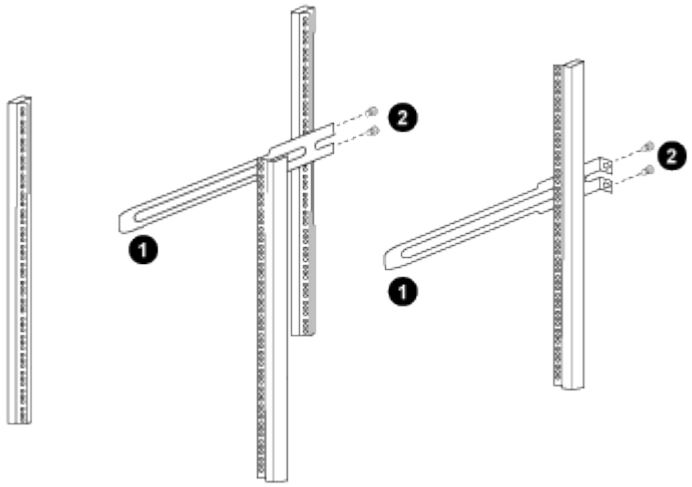
3. Installieren Sie die Clipmuttern in den quadratischen Lochpositionen für alle vier IEA-Pfosten.



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

4. Montieren Sie die Gleitschienen im Schrank.

   a. Positionieren Sie die erste Gleitschiene an der Markierung RU42 auf der Rückseite des linken hinteren Pfostens, setzen Sie Schrauben mit dem passenden Gewinde ein und ziehen Sie die Schrauben dann mit den Fingern fest.



   (1) Verschieben Sie die Gleitschiene vorsichtig und richten Sie sie an den Schraubenlöchern im Gestell aus.

(2) Ziehen Sie die Schrauben der Gleitschienen an den Schrankpfosten fest.

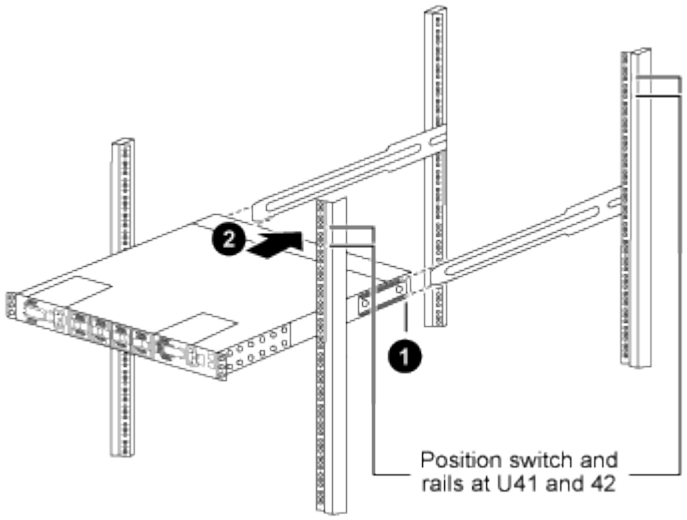
a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.

b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Positionen am Schrank.

5. Bauen Sie den Schalter in den Schrank ein.

> Für diesen Schritt sind zwei Personen erforderlich: eine Person, die den Schalter von vorne stützt, und eine andere, die den Schalter in die hinteren Gleitschienen führt.

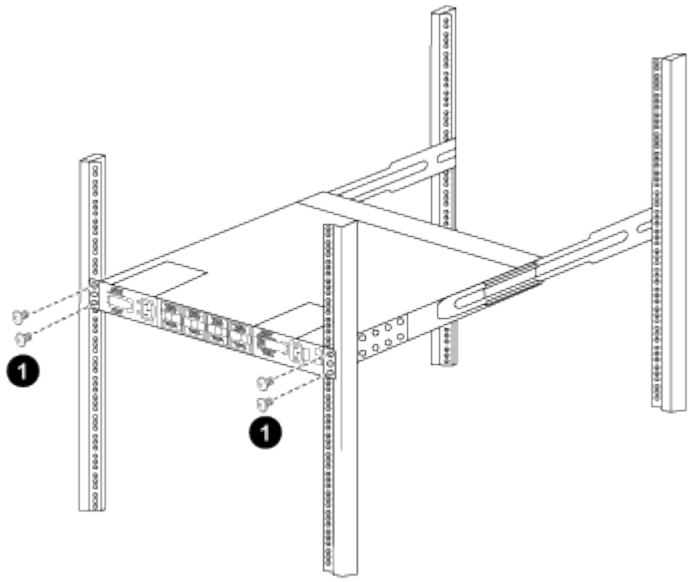
a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(1) Beim Hineinschieben des Chassis in Richtung der hinteren Pfosten müssen die beiden hinteren Rack-Montageführungen mit den Gleitschienen ausgerichtet werden.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Rack-Montagehalterungen bündig mit den vorderen Pfosten abschließen.

b. Befestigen Sie den Schalter am Gehäuse.



(1) Während eine Person die Vorderseite des Chassis waagerecht hält, sollte die andere Person die vier hinteren Schrauben an den Gehäusepfosten vollständig festziehen.

a. Wenn das Chassis nun ohne Hilfe gestützt wird, ziehen Sie die vorderen Schrauben an den Pfosten vollständig fest.

b. Wiederholen Sie die Schritte 5a bis 5c für den zweiten Schalter am Standort RU42.

> Durch die Verwendung des fertig montierten Schalters als Stütze ist es nicht notwendig, den zweiten Schalter während des Montagevorgangs vorne festzuhalten.

6. Wenn die Schalter installiert sind, schließen Sie die Überbrückungskabel an die Stromeingänge der Schalter an.
7. Schließen Sie die Stecker beider Überbrückungskabel an die nächstgelegenen verfügbaren PDU-Steckdosen an.

> Um die Redundanz aufrechtzuerhalten, müssen die beiden Kabel an verschiedene PDUs angeschlossen werden.

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

   Der Verwaltungsport ist der obere rechte Port auf der Netzteilseite des Switches. Das CAT6-Kabel für jeden Switch muss nach der Installation der Switches durch das Durchgangspanel geführt werden, um eine Verbindung zu den Verwaltungs-Switches oder dem Verwaltungsnetzwerk herzustellen.

Wie geht es weiter?

Nachdem Sie die Switches im NetApp -Schrank installiert haben, können Sie"Konfigurieren Sie die Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches" Die

Überprüfung der Verkabelung und Konfigurationsüberlegungen

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

Unterstützung für NVIDIA CX6-, CX6-DX- und CX7-Ethernet-Anschlüsse

Wenn Sie einen Switch-Port mit einem ONTAP Controller über NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) oder ConnectX-7 (CX7) NIC-Ports verbinden, müssen Sie die Geschwindigkeit des Switch-Ports fest codieren.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

Siehe die "Hardware Universe" Weitere Informationen zu Switch-Ports finden Sie hier. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

25GbE FEC-Anforderungen

FAS2820 e0a/e0b-Anschlüsse

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

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

Die Ports können aufgrund von TCAM-Ressourcen nicht verbunden werden.

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

Siehe den Artikel in der Wissensdatenbank. "Aufgrund von TCAM-Ressourcen können die Ports auf dem Cisco Nexus 9336C-FX2 keine Verbindung herstellen." Einzelheiten zur Behebung dieses Problems finden Sie hier.

Konfigurieren der Software

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

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

1 **"Konfigurieren Sie den Schalter"**

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

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

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

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

Laden Sie die NX-OS-Software herunter und installieren oder aktualisieren Sie sie auf den Cluster-Switches Cisco 9336C-FX2 und 9336C-FX2-T.

4 **"Installieren oder aktualisieren Sie die RCF"**

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

5 **"SSH-Konfiguration überprüfen"**

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

6 **"Setzen Sie den Schalter auf die Werkseinstellungen zurück."**

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

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server am Installationsort, um die entsprechenden NX-OS- und Referenzkonfigurationsdatei-(RCF)-Versionen herunterzuladen.
- Anwendbare NX-OS-Version, heruntergeladen von "Cisco -Software-Download" Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.
- Vollendet"Verkabelungs-Arbeitsblätter" Die
- Anwendbare NetApp -Clusternetzwerk- und Managementnetzwerk-RCFs, die von der NetApp -Support -Website heruntergeladen wurden unter "mysupport.netapp.com" Die Alle Cisco Cluster-Netzwerk- und Management-Netzwerk-Switches werden mit der standardmäßigen Cisco -Werkskonfiguration ausgeliefert. Diese Switches verfügen ebenfalls über die aktuelle Version der NX-OS-Software, haben jedoch die RCFs nicht geladen.

- "Erforderliche Switch- und ONTAP Dokumentation".

Schritte

1. Führen Sie eine Erstkonfiguration der Cluster-Netzwerk-Switches durch.

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

Prompt	Antwort
Automatische Bereitstellung abbrechen und mit normaler Einrichtung fortfahren? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Nein.
Wollen Sie einen sicheren Passwortstandard erzwingen? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Ja.
Geben Sie das Passwort für den Administrator ein.	Das Standardpasswort lautet “admin”; Sie müssen ein neues, sicheres Passwort erstellen. Ein schwaches Passwort kann abgelehnt werden.
Möchten Sie den Dialog zur Basiskonfiguration aufrufen? (ja/nein)	Antworten Sie bei der Erstkonfiguration des Switches mit **ja**.
Ein weiteres Benutzerkonto erstellen? (ja/nein)	Die Antwort hängt von den Richtlinien Ihrer Website bezüglich alternativer Administratoren ab. Die Standardeinstellung ist **nein**.
SNMP-Community-String schreibgeschützt konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
SNMP-Community-Zeichenfolge für Lese- und Schreibzugriffe konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
Geben Sie den Namen des Schalters ein.	Geben Sie den Namen des Schalters ein. Dieser darf maximal 63 alphanumerische Zeichen lang sein.
Mit der Out-of-Band-Managementkonfiguration (mgmt0) fortfahren? (ja/nein)	Antworten Sie bei dieser Eingabeaufforderung mit **ja** (Standardeinstellung). Geben Sie an der Eingabeaufforderung mgmt0 IPv4 address: Ihre IP-Adresse ein: ip_address.
Standardgateway konfigurieren? (ja/nein)	Antworten Sie mit **ja**. Geben Sie an der IPv4-Adresse des Standardgateways Ihre Standardgateway-Adresse ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.

Prompt	Antwort
Den Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
SSH-Dienst aktiviert? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Ja. Bei der Verwendung von Ethernet Switch Health Monitor (CSHM) wird SSH aufgrund seiner Protokollierungsfunktionen empfohlen. Für erhöhte Sicherheit wird auch SSHv2 empfohlen.
Geben Sie den Typ des SSH-Schlüssels ein, den Sie generieren möchten (dsa/rsa/rsa1).	Standardmäßig wird **rsa** verwendet.
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits zwischen 1024 und 2048 ein.
Den NTP-Server konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
Standard-Schnittstellenschicht (L3/L2) konfigurieren	Antworte mit **L2**. Standardmäßig ist L2 eingestellt.
Standardmäßigen Schnittstellenstatus des Switch-Ports konfigurieren (ausgeschaltet/nicht ausgeschaltet)	Antworte mit **noshut**. Die Standardeinstellung ist noshut.
CoPP-Systemprofil konfigurieren (streng/moderat/tolerant/dicht)	Mit **streng** antworten. Die Standardeinstellung ist strikt.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	An dieser Stelle sollten Sie die neue Konfiguration sehen. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie gegebenenfalls die erforderlichen Änderungen vor. Antworten Sie mit **nein**, wenn Sie mit der Konfiguration zufrieden sind. Antworten Sie mit **ja**, wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Diese Konfiguration verwenden und speichern? (ja/nein)	Antworten Sie mit **ja**, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systemabbilder automatisch aktualisiert. Wenn Sie die Konfiguration in diesem Schritt nicht speichern, werden beim nächsten Neustart des Switches keine der Änderungen wirksam.

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

Wie geht es weiter?

Nachdem Sie Ihre Schalter konfiguriert haben, können Sie "Bereiten Sie die Installation der NX-OS-Software und RCF vor"Die

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

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

Empfohlene Dokumentation

- "Cisco Ethernet-Switch-Seite"

  In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und NX-OS-Versionen.

- "Anleitungen für Software-Upgrades und -Downgrades"

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

- "Cisco Nexus 9000 und 3000 Upgrade- und ISSU-Matrix"

  Bietet Informationen zu unterbrechenden Upgrades/Downgrades der Cisco NX-OS-Software auf Switches der Nexus 9000-Serie basierend auf Ihren aktuellen und Zielversionen.

  Wählen Sie auf der Seite **Disruptives Upgrade** aus und wählen Sie Ihre aktuelle Version und die Zielversion aus der Dropdown-Liste.

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 und cluster1-02.
- Die Cluster-LIF-Namen lauten cluster1-01_clus1 und cluster1-01_clus2 für Cluster1-01 sowie cluster1-02_clus1 und cluster1-02_clus2 für Cluster1-02.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

Informationen zu diesem Vorgang

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 9000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Schritte

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

   wobei x die Dauer des Wartungsfensters in Stunden ist.

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

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

```
set -privilege advanced
```

Die erweiterte Aufforderung(`*>`) erscheint.

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

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

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C

4 entries were displayed.
```

4. Prüfen Sie den administrativen oder operativen Status jeder Cluster-Schnittstelle.
   a. Netzwerkportattribute anzeigen:

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

Beispiel anzeigen

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

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

Node: cluster1-01
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. Informationen zu den LIFs anzeigen:

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

Beispiel anzeigen

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

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

4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       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
node2
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Alle ONTAP Versionen

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

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

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Überprüfen Sie, ob der Befehl zur automatischen Rücksetzung auf allen Cluster-LIFs aktiviert ist:

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

Beispiel anzeigen

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

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

Wie geht es weiter?

Nachdem Sie die Installation der NX-OS-Software und von RCF vorbereitet haben, können Sie "Installieren oder aktualisieren Sie die NX-OS-Software"Die

Installieren oder aktualisieren Sie die NX-OS-Software.

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

Bevor Sie beginnen, führen Sie bitte die folgende Prozedur durch:"Bereiten Sie die Installation von NX-OS und RCF vor." Die

Überprüfungsanforderungen

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).

Empfohlene Dokumentation

- "Cisco Ethernet-Switch-Seite"

  In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und NX-OS-Versionen.

- "Anleitungen für Software-Upgrades und -Downgrades"

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

- "Cisco Nexus 9000 und 3000 Upgrade- und ISSU-Matrix"

  Bietet Informationen zu unterbrechenden Upgrades/Downgrades der Cisco NX-OS-Software auf Switches

der Nexus 9000-Serie basierend auf Ihren aktuellen und Zielversionen.

Wählen Sie auf der Seite **Disruptives Upgrade** aus und wählen Sie Ihre aktuelle Version und die Zielversion aus der Dropdown-Liste.

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 sind 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.

Installieren Sie die Software

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 9000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem die NX-OS-Software und die RCF gehostet werden.

   Beispiel anzeigen

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

   ```
   cs2# ping 172.19.2.1 VRF management
   Pinging 172.19.2.1 with 0 bytes of data:

   Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
   ```

3. 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       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2
cluster1::*>
```

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

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

      `network port show -role cluster`

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

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

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

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

Beispiel anzeigen

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

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

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

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

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

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

Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.5.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.5.bin  /bootflash/nxos.9.3.5.bin
/code/nxos.9.3.5.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
/code/n9000-epld.9.3.5.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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


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

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

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

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):


cs2#
```

8. Installieren Sie das NX-OS-Image.

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

Beispiel anzeigen

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

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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



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



Images will be upgraded according to following table:

Module   Image    Running-Version(pri:alt)                New-
Version         Upg-Required
-------  -------- ----------------------------------------
-------------------- ------------
  1      nxos     9.3(4)                                  9.3(5)
yes
  1      bios     v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)      yes
```

```
Switch will be reloaded for disruptive upgrade.

Do you want to continue with the installation (y/n)? [n] y

Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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

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

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

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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


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

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

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

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

Beispiel anzeigen

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x17
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2

cs2# install epld bootflash:n9000-epld.9.3.5.img module all
Compatibility check:
Module        Type         Upgradable        Impact    Reason
------  ------------------ ----------------- --------- -----------
     1         SUP         Yes       disruptive  Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------- ------ ----------------- ----------------- ------------
------------
     1  SUP    MI FPGA           0x07              0x07         No
     1  SUP    IO FPGA           0x17              0x19         Yes
     1  SUP    MI FPGA2          0x02              0x02         No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

11. Nach dem Neustart des Switches melden Sie sich erneut an und überprüfen Sie, ob die neue Version von EPLD erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld

EPLD Device                          Version
---------------------------------------
MI   FPGA                             0x7
IO   FPGA                             0x19
MI   FPGA2                            0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
GEM  FPGA                             0x2
```

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

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

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

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

Ignore
                                                          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.
```

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       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0d    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
--------------
cs1                         cluster-network    10.233.205.90    N9K-
C9336C-FX2
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
```

```
C9336C-FX2
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version 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.
```

13. 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::*>
```

14. Wiederholen Sie die Schritte 6 bis 13, um die NX-OS-Software auf Switch cs1 zu installieren.
15. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen, bevor Sie die automatische Rücksetzung auf den Cluster-LIFs aktivieren:

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
------ -------------------------- -------------------
------------------ -----------
node1
       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
node2
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Alle ONTAP Versionen

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

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

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-02
Getting addresses from network interface table...
Cluster cluster1-01_clus1 169.254.209.69 cluster1-01     e0a
Cluster cluster1-01_clus2 169.254.49.125 cluster1-01     e0b
Cluster cluster1-02_clus1 169.254.47.194 cluster1-02     e0a
Cluster cluster1-02_clus2 169.254.19.183 cluster1-02     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Automatische Rücksetzung der Cluster-LIFs aktivieren.

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

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

   network interface show -role cluster

Beispiel anzeigen

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

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

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

Wie geht es weiter?

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

Installieren oder aktualisieren Sie die RCF

Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).

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

ist.

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. Sehen"Cisco Ethernet-Switches" für weitere Informationen.

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

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

Verfügbare RCFs

Die folgende Tabelle listet die verfügbaren RCFs für die Switches 9336C-FX2 und 9336C-FX2-T auf. Wählen Sie die für Ihre Konfiguration passende RCF-Version aus. Sehen"Cisco Ethernet-Switches" für weitere Informationen.

RCF-Name
Cluster-HA-Breakout RCF 1.*xx*
Cluster-HA-Storage RCF 1.*xx*
Speicher RCF 1.*xx*
MultiCluster-HA 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 9000 Series Switches"

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

Zu den Beispielen

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

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

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

Die Befehlsausgaben können je nach ONTAP Version variieren.

Einzelheiten zu den verfügbaren RCF-Konfigurationen finden Sie unter"Softwareinstallations-Workflow" .

verwendete Befehle

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 9000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Wie geht es weiter?

Nachdem Sie die Installations- oder Aktualisierungsprozedur für RCF durchgelesen haben, können Sie"Installieren Sie den RCF" oder"Aktualisieren Sie Ihren RCF" wie erforderlich.

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

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Eine Konsolenverbindung zum Switch. Die Konsolenverbindung ist optional, wenn Sie Fernzugriff auf den Switch haben.
- Die Switches cs1 und cs2 sind eingeschaltet und die Ersteinrichtung der Switches ist abgeschlossen (die Management-IP-Adresse und SSH sind eingerichtet).
- Die gewünschte NX-OS-Version wurde installiert.
- Die ISL-Verbindungen zwischen den Switches sind hergestellt.
- Die Ports des ONTAP Knotenclusters sind nicht verbunden.

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich über SSH oder über eine serielle Konsole am Switch cs1 an.
2. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs1: FTP, TFTP, SFTP oder SCP.

   Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Leitfaden in der"Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" Leitfäden.

   Beispiel anzeigen

   Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches cs1 zu kopieren:

   ```
   cs1# copy tftp: bootflash: vrf management
   Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
   Enter hostname for the tftp server: 172.22.201.50
   Trying to connect to tftp server......Connection to Server
   Established.
   TFTP get operation was successful
   Copy complete, now saving to disk (please wait)...
   ```

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

   Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Leitfaden in der"Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" Leitfäden.

   Dieses Beispiel zeigt die RCF-Datei. `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` wird auf Switch CS1 installiert:

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

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

Beispiel anzeigen

```
cs1# show banner motd

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

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

   `show running-config`

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

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

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

6. Alle benutzerdefinierten Ergänzungen zwischen dem aktuellen `running-config` Datei und die verwendete RCF-Datei.
7. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Schaltereinstellungen korrekt sind, kopieren Sie die `running-config` Datei an die `startup-config` Datei.

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

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

> Stellen Sie sicher, dass Sie Folgendes konfigurieren:
>
> - Benutzername und Passwort
> - Verwaltungs-IP-Adresse
> - Standardgateway
> - Schaltername

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

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

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

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

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

Siehe den Artikel in der Wissensdatenbank."Wie man die Konfiguration eines Cisco Interconnect-Switches

löscht und gleichzeitig die Remote-Konnektivität beibehält" für weitere Einzelheiten.

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

    `show file bootflash:write_erase.cfg`

11. Wiederholen Sie die Schritte 1 bis 10 auf Switch cs2.
12. 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`

   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 mithilfe der folgenden Befehle, ob sich die Clusterknoten in den richtigen Cluster-VLANs befinden:

   `show vlan brief`

   `show interface trunk`

Beispiel anzeigen

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
-------------------------------
1    default                           active    Po1, Eth1/1, Eth1/2,
Eth1/3
                                                 Eth1/4, Eth1/5,
Eth1/6, Eth1/7
                                                 Eth1/8, Eth1/35,
Eth1/36
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
17   VLAN0017                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
18   VLAN0018                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
31   VLAN0031                          active    Eth1/11, Eth1/12,
Eth1/13
                                                 Eth1/14, Eth1/15,
Eth1/16
                                                 Eth1/17, Eth1/18,
Eth1/19
                                                 Eth1/20, Eth1/21,
Eth1/22
32   VLAN0032                          active    Eth1/23, Eth1/24,
Eth1/25
```

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

cs1# show interface trunk

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

```
Eth1/12       33      trunking      --
Eth1/13       33      trunking      --
Eth1/14       33      trunking      --
Eth1/15       33      trunking      --
Eth1/16       33      trunking      --
Eth1/17       33      trunking      --
Eth1/18       33      trunking      --
Eth1/19       33      trunking      --
Eth1/20       33      trunking      --
Eth1/21       33      trunking      --
Eth1/22       33      trunking      --
Eth1/23       34      trunking      --
Eth1/24       34      trunking      --
Eth1/25       34      trunking      --
Eth1/26       34      trunking      --
Eth1/27       34      trunking      --
Eth1/28       34      trunking      --
Eth1/29       34      trunking      --
Eth1/30       34      trunking      --
Eth1/31       34      trunking      --
Eth1/32       34      trunking      --
Eth1/33       34      trunking      --
Eth1/34       34      trunking      --
Eth1/35       1       trnk-bndl     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           1       trunking      --

----------------------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------------------
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18
```

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

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

3. 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      Eth1/35(P)        Eth1/36(P)
cs1#
```

Schritt 3: Richten Sie Ihren ONTAP Cluster ein.

NetApp empfiehlt, neue Cluster mit dem System Manager einzurichten.

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

Gehe zu "Konfigurieren Sie ONTAP auf einem neuen Cluster mit System Manager" für Installationsanweisungen.

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 instanziiert 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       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C
cluster1::*>
```

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

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

      `network port show -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          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

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

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
cs1                         cluster-network    10.233.205.90    N9K-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    N9K-
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP
cluster1::*>
```

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

Schritt 2: Ports konfigurieren

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

```
cs1> enable

cs1# configure

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

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

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

cs1# exit
```

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

2. Überprüfen Sie, ob die Cluster-LIFs auf die Ports des Cluster-Switches cs1 umgeschaltet haben. 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
8 entries were displayed.
cluster1::*>
```

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

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

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

   `show running-config`

   a. Alle benutzerdefinierten Ergänzungen zwischen dem aktuellen `running-config` und die verwendete RCF-Datei (z. B. eine SNMP-Konfiguration für Ihre Organisation).

   b. Ab NX-OS 10.2 verwenden Sie die `show diff running-config` Befehl zum Vergleich mit der gespeicherten RCF-Datei im Bootflash. Verwenden Sie andernfalls ein Vergleichstool eines Drittanbieters.

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

   Stellen Sie sicher, dass Sie Folgendes konfigurieren:

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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

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

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

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
```

```
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
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.

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

   `show file bootflash:write_erase.cfg`

8. Geben Sie den Befehl "write erase" ein, um die aktuell gespeicherte Konfiguration zu löschen:

   ```
   cs1# write erase

   Warning: This command will erase the startup-configuration.

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

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

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

10. Führen Sie einen Neustart des Switches durch:

    ```
    switch# reload

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

11. 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.

12. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs1: FTP, TFTP, SFTP oder SCP.

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Leitfaden in der"Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" Leitfäden.

    Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches cs1 zu kopieren:

    ```
    cs1# copy tftp: bootflash: vrf management
    Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
    Enter hostname for the tftp server: 172.22.201.50
    Trying to connect to tftp server......Connection to Server Established.
    TFTP get operation was successful
    Copy complete, now saving to disk (please wait)...
    ```

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

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im"Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" .

    Dieses Beispiel zeigt die RCF-Datei. `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` wird auf Switch CS1 installiert:

    ```
    cs1# copy Nexus_9336C_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.

14. 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.

15. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
16. Nachdem Sie überprüft haben, ob die RCF-Versionen, die benutzerdefinierten Erweiterungen und die Schaltereinstellungen korrekt sind, kopieren Sie die Running-Config-Datei in die Startup-Config-Datei.

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im"Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" .

    ```
    cs1# copy running-config startup-config

    [] 100% Copy complete
    ```

17. Neustart des Switches cs1. Sie können die Warnungen „`cluster switch health monitor`“ und die Ereignisse „`cluster ports down`“, die auf den Knoten während des Neustarts des Switches gemeldet werden, ignorieren.

    ```
    cs1# reload
    ```

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

18. 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
                                                          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.
```

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       N9K-
C9336C
            e0d    cs2                       Ethernet1/7       N9K-
C9336C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C
            e0d    cs2                       Ethernet1/8       N9K-
C9336C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ---------------
-----
cs1                         cluster-network    10.233.205.90    NX9-
C9336C
     Serial Number: FOCXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91    NX9-
```

```
C9336C
     Serial Number: FOCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(5)
    Version Source: CDP

2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version 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.
```

19. 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::*>
```

20. Wiederholen Sie die Schritte 1 bis 19 auf Switch cs2.
21. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

22. Führen Sie einen Neustart von Switch cs2 durch.

```
cs2# reload

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

Schritt 3: Überprüfen Sie die Clusternetzwerkkonfiguration und den Clusterzustand.

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

```
show interface brief
```

Beispiel anzeigen

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

2. Überprüfen Sie, ob die erwarteten Knoten noch verbunden sind:

```
show cdp neighbors
```

Beispiel anzeigen

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0a
node2              Eth1/2         133    H           FAS2980
e0a
cs1                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs1                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Überprüfen Sie mithilfe der folgenden Befehle, ob sich die Clusterknoten in den richtigen Cluster-VLANs befinden:

   ```
   show vlan brief

   show interface trunk
   ```

Beispiel anzeigen

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
-------------------------------
1    default                           active    Po1, Eth1/1, Eth1/2,
Eth1/3
                                                 Eth1/4, Eth1/5,
Eth1/6, Eth1/7
                                                 Eth1/8, Eth1/35,
Eth1/36
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
17   VLAN0017                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
18   VLAN0018                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9/1, Eth1/9/2,
Eth1/9/3
                                                 Eth1/9/4, Eth1/10/1,
Eth1/10/2
                                                 Eth1/10/3, Eth1/10/4
31   VLAN0031                          active    Eth1/11, Eth1/12,
Eth1/13
                                                 Eth1/14, Eth1/15,
Eth1/16
                                                 Eth1/17, Eth1/18,
Eth1/19
                                                 Eth1/20, Eth1/21,
Eth1/22
32   VLAN0032                          active    Eth1/23, Eth1/24,
Eth1/25
```

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

cs1# show interface trunk

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

```
Eth1/12       33      trunking      --
Eth1/13       33      trunking      --
Eth1/14       33      trunking      --
Eth1/15       33      trunking      --
Eth1/16       33      trunking      --
Eth1/17       33      trunking      --
Eth1/18       33      trunking      --
Eth1/19       33      trunking      --
Eth1/20       33      trunking      --
Eth1/21       33      trunking      --
Eth1/22       33      trunking      --
Eth1/23       34      trunking      --
Eth1/24       34      trunking      --
Eth1/25       34      trunking      --
Eth1/26       34      trunking      --
Eth1/27       34      trunking      --
Eth1/28       34      trunking      --
Eth1/29       34      trunking      --
Eth1/30       34      trunking      --
Eth1/31       34      trunking      --
Eth1/32       34      trunking      --
Eth1/33       34      trunking      --
Eth1/34       34      trunking      --
Eth1/35       1       trnk-bndl     Po1
Eth1/36       1       trnk-bndl     Po1
Po1           1       trunking      --

----------------------------------------------------
Port          Vlans Allowed on Trunk
----------------------------------------------------
Eth1/1        1,17-18
Eth1/2        1,17-18
Eth1/3        1,17-18
Eth1/4        1,17-18
Eth1/5        1,17-18
Eth1/6        1,17-18
Eth1/7        1,17-18
Eth1/8        1,17-18
Eth1/9/1      1,17-18
Eth1/9/2      1,17-18
Eth1/9/3      1,17-18
Eth1/9/4      1,17-18
Eth1/10/1     1,17-18
Eth1/10/2     1,17-18
Eth1/10/3     1,17-18
Eth1/10/4     1,17-18
```

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

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

4. 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      Eth1/35(P)        Eth1/36(P)
cs1#
```

5. 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
8 entries were displayed.
cluster1::*>
```

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

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

6. 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::*>
```

7. 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
------ -------------------------- -------------------
------------------ -----------
node1
       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
node2
       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 cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Wie geht es weiter?

Nach dem Upgrade Ihres RCF können Sie"Überprüfen Sie die SSH-Konfiguration" Die

Überprüfen Sie Ihre SSH-Konfiguration

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

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

Schritte

1. Überprüfen Sie, ob SSH aktiviert ist:

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

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

```
show ssh key
```

Beispiel anzeigen

```
(switch)# show ssh key

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

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

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

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

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

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

Wie geht es weiter?

Nachdem Sie Ihre SSH-Konfiguration überprüft haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

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

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

Informationen zu diesem Vorgang

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

Schritte

1. Löschen Sie die vorhandene Konfiguration:

   `write erase`

   ```
   (cs2)# write erase

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

2. Laden Sie die Switch-Software neu:

   `reload`

   ```
   (cs2)# reload

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

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

Was kommt als nächstes

Nachdem Sie Ihre Schalter zurückgesetzt haben, können Sie"neu konfigurieren" sie nach Bedarf.

Migrieren Sie die Schalter

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

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

Überprüfungsanforderungen

Sie müssen bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen

beachten, wenn Sie NetApp CN1610-Cluster-Switches durch Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-Switches ersetzen. Sie müssen auch die Seriennummer des Switches überprüfen, um sicherzustellen, dass der richtige Switch migriert wird.

Unterstützte Schalter

Folgende Cluster-Switches werden unterstützt:

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

Einzelheiten zu den unterstützten Ports und deren Konfigurationen finden Sie unter "Hardware Universe" Die Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Weitere Informationen zu den Installationsanforderungen des Schalters finden Sie hier.

Was du brauchst

Vergewissern Sie sich, dass Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Der bestehende Cluster ist korrekt eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die Cluster-Switches Cisco 9336C-FX2 und 9336C-FX2-T sind konfiguriert und werden unter der richtigen Version von NX-OS mit angewendeter Referenzkonfigurationsdatei (RCF) betrieben.
- Die bestehende Cluster-Netzwerkkonfiguration weist folgende Merkmale auf:
  - Ein redundanter und voll funktionsfähiger NetApp Cluster mit NetApp CN1610-Switches.
  - Management-Konnektivität und Konsolenzugriff sowohl auf die NetApp CN1610 Switches als auch auf die neuen Switches.
  - Alle Cluster-LIFs befinden sich im aktiven Zustand und sind an ihren Heimatports angeschlossen.
- Einige der Ports sind auf den Cisco 9336C-FX2- und 9336C-FX2-T-Switches für den Betrieb mit 40 GbE oder 100 GbE konfiguriert.
- Sie haben 40GbE- und 100GbE-Konnektivität von Knoten zu Cisco 9336C-FX2- und 9336C-FX2-T-Cluster-Switches geplant, migriert und dokumentiert.

Migrieren Sie die Schalter

Zu den Beispielen

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

- Die vorhandenen CN1610 Cluster-Switches sind *C1* und *C2*.
- Die neuen Cluster-Switches vom Typ 9336C-FX2 sind *cs1* und *cs2*.
- Die Knoten heißen *node1* und *node2*.
- Die Cluster-LIFs sind *node1_clus1* und *node1_clus2* auf Knoten 1 bzw. *node2_clus1* und *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.

Informationen zu diesem Vorgang

Dieses Verfahren umfasst folgendes Szenario:

- Der Schalter C2 wird zuerst durch den Schalter CS2 ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
    - Alle Cluster-LIFs wechseln zum neuen Switch cs2.
  - Die Verkabelung zwischen den Knoten und C2 wird dann von C2 getrennt und wieder mit cs2 verbunden.
- Der Schalter C1 wird durch den Schalter CS1 ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
    - Alle Cluster-LIFs werden auf den neuen Switch cs1 umgeschaltet.
  - Die Verkabelung zwischen den Knoten und C1 wird dann von C1 getrennt und wieder mit cs1 verbunden.

> 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, wird während der Ausführung der Schritte auf dem Ziel-Switch ein Failover aller Cluster-LIFs auf den operativen Partner-Switch durchgeführt.

Schritt 1: Vorbereitung auf die Migration

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.

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. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

   Durch Deaktivierung der automatischen Rückstellung für diesen Vorgang werden die Cluster-LIFs nicht automatisch zu ihrem Heimatport zurückbewegt. Sie bleiben im derzeitigen Hafen, solange dieser in Betrieb ist.

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

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ermitteln Sie den administrativen oder operativen Status jeder Clusterschnittstelle.

   Jeder Port sollte angezeigt werden für `Link` Und `healthy` für `Health Status` Die

   a. Netzwerkportattribute anzeigen:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

b. Informationen zu den LIFs und ihren jeweiligen Heimatknoten anzeigen:

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

Jedes LIF sollte anzeigen `up/up` für `Status Admin/Oper` Und `true` für `Is Home` Die

Beispiel anzeigen

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3b     true
```

2. Die Cluster-Ports auf jedem Knoten werden (aus Sicht der Knoten) folgendermaßen mit vorhandenen Cluster-Switches verbunden:

   `network device-discovery show -protocol`

Beispiel anzeigen

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

3. Die Cluster-Ports und Switches werden (aus Sicht der Switches) mit folgendem Befehl verbunden:

   `show cdp neighbors`

Beispiel anzeigen

```
C1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

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

C2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


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

4. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e3a
Cluster node1_clus2 169.254.49.125 node1     e3b
Cluster node2_clus1 169.254.47.194 node2     e3a
Cluster node2_clus2 169.254.19.183 node2     e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Schalten Sie auf Switch C2 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen.

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

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

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

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

   `network device-discovery show -protocol`

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e3a    C1  (6a:ad:4f:98:3b:3f)   0/1
CN1610
            e3b    cs2 (b8:ce:f6:19:1a:7e)   Ethernet1/1/1     N9K-
C9336C-FX2
node2      /cdp
            e3a    C1  (6a:ad:4f:98:3b:3f)   0/2
CN1610
            e3b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2     N9K-
C9336C-FX2
```

5. Überprüfen Sie auf Switch cs2, ob alle Ports des Knotenclusters aktiv sind:

   `network interface show -vserver Cluster`

Beispiel anzeigen

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

6. Schalten Sie auf Switch C1 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen.

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

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

   `network port show -ipspace Cluster`

   Jeder Port sollte Folgendes anzeigen `up` für `Link` Und `healthy` für `Health Status` Die

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

9. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

   `network device-discovery show -protocol`

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /cdp
            e3a    cs1 (b8:ce:f6:19:1a:7e)   Ethernet1/1/1   N9K-
C9336C-FX2
            e3b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
node2      /cdp
            e3a    cs1 (b8:ce:f6:19:1a:7e)   Ethernet1/1/1   N9K-
C9336C-FX2
            e3b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2
```

10. Überprüfen Sie an den Switches cs1 und cs2, ob alle Knotencluster-Ports aktiv sind:

    `network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

11. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

    `network device-discovery show -protocol`

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
--------------
node1      /cdp
            e0a    cs1 (b8:ce:f6:19:1b:42)   Ethernet1/1/1   N9K-
C9336C-FX2
            e0b    cs2 (b8:ce:f6:19:1b:96)   Ethernet1/1/2   N9K-
C9336C-FX2

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

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

2. Auf Switch cs2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

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

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

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

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

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

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

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster show
   ```

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
```

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

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

2. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

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

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

Überprüfungsanforderungen

Stellen Sie sicher, dass:

- Sie haben die Seriennummer des Switches überprüft, um sicherzustellen, dass der richtige Switch migriert wird.
- Einige der Ports der Nexus 9336C-FX2 Switches sind für den Betrieb mit 10GbE oder 40GbE konfiguriert.
- Die 10GbE- und 40GbE-Konnektivität von den Knoten zu den Nexus 9336C-FX2 Cluster-Switches wurde geplant, migriert und dokumentiert.
- Der Cluster ist voll funktionsfähig (es sollten keine Fehler in den Protokollen oder ähnliche Probleme auftreten).
- Die Erstkonfiguration der Cisco Nexus 9336C-FX2 Switches ist abgeschlossen, sodass:
  - Auf den Switches vom Typ 9336C-FX2 läuft die neueste empfohlene Softwareversion.
  - Bevor Sie die LIFs auf die neuen Switches migrieren, vergewissern Sie sich, dass die Referenzkonfigurationsdateien (RCFs) vollständig auf alle neuen Switches angewendet wurden.
  - Prüfen Sie vor der Umleitung des Netzwerkverkehrs die laufenden und Startkonfigurationen beider Switches.
  - Sämtliche Standortanpassungen, wie z. B. DNS, NTP, SMTP, SNMP und SSH, werden auf den neuen Switches konfiguriert.
- Sie haben Zugriff auf die Switch-Kompatibilitätstabelle auf dem "Cisco Ethernet-Switches" Seite für die unterstützten ONTAP, NX-OS- und RCF-Versionen.
- Sie haben die entsprechenden Software- und Upgrade-Anleitungen auf der Cisco -Website für die Upgrade- und Downgrade-Verfahren von Cisco Switches geprüft. "Cisco Nexus 9000 Series Switches Unterstützung" Seite.

> Wenn Sie die Portgeschwindigkeit der Cluster-Ports e0a und e1a auf AFF A800 oder AFF C800 Systemen ändern, kann es nach der Geschwindigkeitsumwandlung zu fehlerhaften Paketen kommen. Sehen "Bug 1570339" und der Artikel in der Wissensdatenbank "CRC-Fehler an T6-Ports nach der Umstellung von 40GbE auf 100GbE" zur Orientierung.

Migrieren Sie die Schalter

Zu den Beispielen

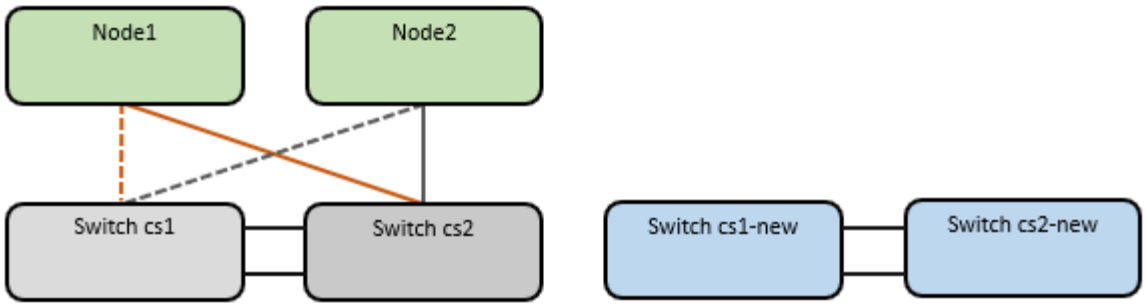
Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Knoten nutzen zwei 10GbE-Cluster-Verbindungsports e0a und e0b. Siehe die "Hardware Universe" um die korrekten Cluster-Ports auf Ihren Plattformen zu überprüfen. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Weitere Informationen zu den Installationsanforderungen des Schalters finden Sie hier.

> Die Befehlsausgaben können je nach ONTAP Version variieren.

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

- Die Namen der beiden vorhandenen Cisco Switches lauten **cs1** und **cs2**.
- Die neuen Cluster-Switches Nexus 9336C-FX2 sind **cs1-new** und **cs2-new**.
- Die Knotennamen lauten **node1** und **node2**.
- Die Cluster-LIF-Namen lauten **node1_clus1** und **node1_clus2** für Knoten 1 sowie **node2_clus1** und **node2_clus2** für Knoten 2.
- Die Eingabeaufforderung **cluster1::>*** zeigt den Namen des Clusters an.

Beachten Sie bei diesem Vorgang das folgende Beispiel:



Informationen zu diesem Vorgang

Das Verfahren erfordert die Verwendung sowohl von ONTAP -Befehlen als auch von "Switches der Nexus 9000-Serie" Befehle; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Dieses Verfahren umfasst folgendes Szenario:

- Der Schalter cs2 wird zuerst durch den Schalter cs2-new ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
    - Alle Cluster-LIFs werden auf den neuen Switch cs2-new umgeschaltet.
  - Die Verkabelung zwischen den Knoten und cs2 wird dann von cs2 getrennt und wieder mit cs2-new verbunden.
- Der Schalter cs1 wird durch den Schalter cs1-new ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
    - Alle Cluster-LIFs schalten auf den neuen Switch cs1-new um.
  - Die Verkabelung zwischen den Knoten und cs1 wird dann von cs1 getrennt und wieder mit cs1-new verbunden.

> 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, wird während der Ausführung der Schritte auf dem Ziel-Switch ein Failover aller Cluster-LIFs auf den operativen Partner-Switch durchgeführt.

Schritt 1: Vorbereitung auf die Migration

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.

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.

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Prüfen Sie an den neuen Switches, ob die ISL-Verbindung zwischen den Switches cs1-new und cs2-new hergestellt und funktionsfähig ist:

   ```
   show port-channel summary
   ```

Beispiel anzeigen

```
cs1-new# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

cs2-new# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

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

   `network device-discovery show`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e0a    cs1                       Ethernet1/1        N5K-
C5596UP
            e0b    cs2                       Ethernet1/2        N5K-
C5596UP
node2      /cdp
            e0a    cs1                       Ethernet1/1        N5K-
C5596UP
            e0b    cs2                       Ethernet1/2        N5K-
C5596UP
```

3. Ermitteln Sie den administrativen oder operativen Status für jeden Cluster-Port.

   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: node1

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

Node: node2

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

b. Überprüfen Sie, ob alle Cluster-Schnittstellen (LIFs) an ihren jeweiligen Heimatports 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
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0b     true
```

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

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
---------------
cs1                         cluster-network    10.233.205.92    N5K-
C5596UP
      Serial Number: FOXXXXXXXGS
       Is Monitored: true
             Reason: None
   Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                     9.3(4)
     Version Source: CDP

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

4. Automatische Rücksetzung der Cluster-LIFs deaktivieren.

   Durch Deaktivierung der automatischen Rückstellung für diesen Vorgang werden die Cluster-LIFs nicht automatisch zu ihrem Heimatport zurückbewegt. Sie bleiben im derzeitigen Hafen, solange dieser in Betrieb ist.

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

   Durch Deaktivieren der automatischen Rücksetzung wird sichergestellt, dass ONTAP nur dann auf die Cluster-LIFs zurückgreift, wenn die Switch-Ports später heruntergefahren werden.

5. Schalten Sie auf dem Cluster-Switch cs2 die Ports ab, die mit den Cluster-Ports **aller** Knoten verbunden sind, um ein Failover der Cluster-LIFs zu erzwingen:

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

6. Überprüfen Sie, ob die Cluster-LIFs auf die Ports des Cluster-Switches cs1 umgeschaltet haben. Dies kann einige Sekunden dauern.

   `network interface show -vserver Cluster`

   Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------ ----------
------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/16     node1
e0a     true
            node1_clus2   up/up      169.254.3.5/16     node1
e0a     false
            node2_clus1   up/up      169.254.3.8/16     node2
e0a     true
            node2_clus2   up/up      169.254.3.9/16     node2
e0a     false
```

7. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   `cluster show`

   Beispiel anzeigen

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

8. Wenn die Cluster-LIFs auf Switch cs1 umgeschaltet haben und der Cluster fehlerfrei ist, fahren Sie mit folgendem fort:Schritt. 10 Die Falls einige Cluster-LIFs nicht fehlerfrei sind oder der Cluster insgesamt fehlerhaft ist, können Sie die Konnektivität zum Switch cs2 wie folgt wiederherstellen:

   a. Aktivieren Sie die Ports, die mit den Cluster-Ports **aller** Knoten verbunden sind:

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

   b. Überprüfen Sie, ob die Cluster-LIFs auf die Ports des Cluster-Switches cs1 umgeschaltet haben. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ------------- ---------- ------------------
---------- ------- ----
Cluster
            node1_clus1   up/up      169.254.3.4/16     node1
e0a     true
            node1_clus2   up/up      169.254.3.5/16     node1
e0a     false
            node2_clus1   up/up      169.254.3.8/16     node2
e0a     true
            node2_clus2   up/up      169.254.3.9/16     node2
e0a     false
```

   c. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

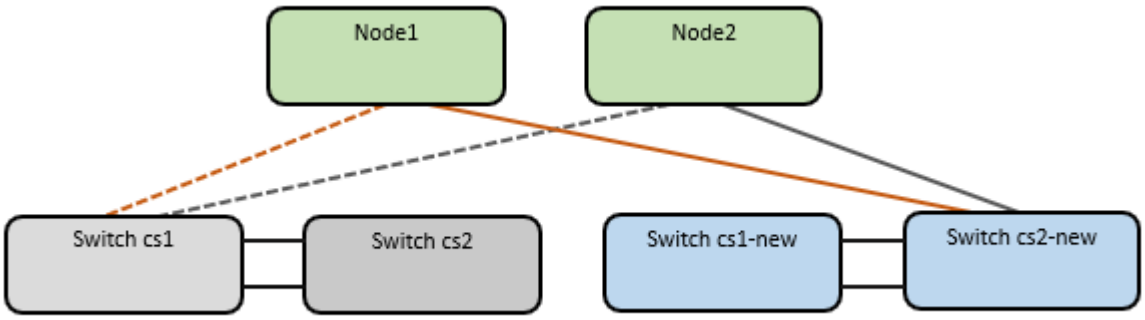
```
cluster show
```

Beispiel anzeigen

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

9. Sobald Sie LIF und die Clusterintegrität wiederhergestellt haben, starten Sie den Prozess neu.Schritt. 4 Die
10. Verlegen Sie alle Cluster-Knotenverbindungskabel vom alten cs2-Switch zum neuen cs2-new-Switch.

Die Verbindungskabel der Clusterknoten wurden an den Switch cs2-new angeschlossen.



11. Bestätigen Sie den Zustand der nach cs2-new verschobenen Netzwerkverbindungen:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

Alle verschobenen Cluster-Ports sollten nun aktiv sein.

12. Überprüfen Sie die Nachbarinformationen an den Cluster-Ports:

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

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- -------------
--------------
node1      /cdp
            e0a    cs1                       Ethernet1/1    N5K-
C5596UP
            e0b    cs2-new                   Ethernet1/1/1  N9K-
C9336C-FX2

node2      /cdp
            e0a    cs1                       Ethernet1/2    N5K-
C5596UP
            e0b    cs2-new                   Ethernet1/1/2  N9K-
C9336C-FX2
```

Überprüfen Sie, ob die verschobenen Cluster-Ports den Switch cs2-new als Nachbarn erkennen.

13. Prüfen Sie die Switch-Port-Verbindungen aus der Perspektive des Switches cs2-new:

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

14. Um ein Failover der Cluster-LIFs durchzuführen, müssen auf dem Cluster-Switch cs1 die mit den Cluster-Ports **aller** Knoten verbundenen Ports abgeschaltet werden.

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

Alle Cluster-LIFs schalten auf den Switch cs2-new um.

15. Überprüfen Sie, ob die Cluster-LIFs auf die Ports des Switches cs2-new umgeschaltet haben. Dies kann einige Sekunden dauern:

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

Beispiel anzeigen

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

16. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

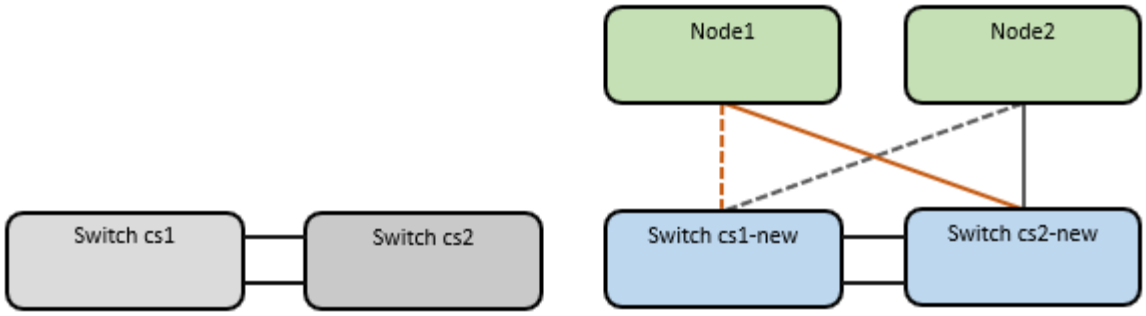
    `cluster show`

    Beispiel anzeigen

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

17. Verlegen Sie die Cluster-Knoten-Verbindungskabel von cs1 zum neuen Switch cs1-new.

    Die Verbindungskabel der Clusterknoten wurden an den Switch cs1-new angeschlossen.



18. Prüfen Sie den Zustand der Netzwerkverbindungen, die nach cs1-new verschoben wurden:

    `network port show -ipspace Cluster`

    Beispiel anzeigen

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

Node: node1

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

Node: node2

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

Alle verschobenen Cluster-Ports sollten nun aktiv sein.

19. Überprüfen Sie die Nachbarinformationen an den Cluster-Ports:

    `network device-discovery show`

    Beispiel anzeigen

    ```
    cluster1::*> network device-discovery show -protocol cdp
    Node/       Local  Discovered
    Protocol    Port   Device (LLDP: ChassisID)  Interface
    Platform
    ----------- ------ ------------------------- --------------
    --------------
    node1      /cdp
                e0a    cs1-new                   Ethernet1/1/1   N9K-
    C9336C-FX2
                e0b    cs2-new                   Ethernet1/1/2   N9K-
    C9336C-FX2

    node2      /cdp
                e0a    cs1-new                   Ethernet1/1/1   N9K-
    C9336C-FX2
                e0b    cs2-new                   Ethernet1/1/2   N9K-
    C9336C-FX2
    ```

    Überprüfen Sie, ob die verschobenen Cluster-Ports den Switch cs1-new als Nachbarn erkennen.

20. Prüfen Sie die Switch-Port-Verbindungen aus der Perspektive des Switches cs1-new:

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

21. Überprüfen Sie, ob die ISL-Verbindung zwischen cs1-new und cs2-new noch funktioniert:

    `show port-channel summary`

Beispiel anzeigen

```
cs1-new# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

cs2-new# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

2. Auf Switch cs2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

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

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

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

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

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

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

4. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster show
   ```

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
```

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

```
cluster1::*> network interface check cluster-connectivity show
                                  Source          Destination
Packet
Node   Date                       LIF             LIF
Loss
------ -------------------------- --------------- -----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2_clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none

node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Wenn Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen: `system node autosupport invoke -node * -type all -message MAINT=END`

Wie geht es weiter?

Nach der Migration der Switches können Sie"Konfigurieren der Switch-Integritätsüberwachung" Die

Migration zu einem Zwei-Knoten-Switched-Cluster

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

Der Migrationsprozess funktioniert für alle Knoten, die optische oder Twinax-Anschlüsse verwenden, wird jedoch von diesem Switch nicht unterstützt, wenn die Knoten Onboard-10Gb BASE-T RJ45-Anschlüsse für die Cluster-Netzwerkanschlüsse verwenden.

Überprüfungsanforderungen

Was du brauchst

- Für die schalterlose Zwei-Knoten-Konfiguration:

- Die Zwei-Knoten-Konfiguration ohne Schalter ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**.
- Alle logischen Schnittstellen (LIFs) des Clusters befinden sich im Status **up** und sind an ihren jeweiligen Ports angeschlossen.
- Sehen "Hardware Universe" für alle unterstützten ONTAP Versionen.

- Für die Konfiguration des Cisco Nexus 9336C-FX2 Switches:
  - Beide Switches verfügen über eine Management-Netzwerkanbindung.
  - Es besteht Konsolenzugriff auf die Cluster-Switches.
  - Knoten-zu-Knoten-Switch- und Switch-zu-Switch-Verbindungen des Nexus 9336C-FX2 verwenden Twinax- oder Glasfaserkabel.

    Sehen "Hardware Universe" Weitere Informationen zur Verkabelung finden Sie hier.
- Inter-Switch Link (ISL)-Kabel sind an die Ports 1/35 und 1/36 beider 9336C-FX2-Switches angeschlossen.
- Die erste Anpassung beider 9336C-FX2-Schalter ist abgeschlossen, sodass:
  - Die Switches vom Typ 9336C-FX2 verwenden die neueste Softwareversion.
  - Referenzkonfigurationsdateien (RCFs) werden auf die Switches angewendet. Sämtliche Standortanpassungen, wie z. B. SMTP, SNMP und SSH, werden auf den neuen Switches konfiguriert.

Zu den Beispielen

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

- Die Bezeichnungen der 9336C-FX2-Schalter lauten cs1 und cs2.
- Die Namen der Cluster-SVMs lauten node1 und node2.
- Die Namen der LIFs lauten node1_clus1 und node1_clus2 auf Knoten 1 bzw. node2_clus1 und node2_clus2 auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e0a und e0b.

Sehen "Hardware Universe" Informationen zu den Cluster-Ports für Ihre Plattformen finden Sie hier. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Weitere Informationen zu den Installationsanforderungen des Schalters finden Sie hier.

Migrieren Sie die Schalter

Schritt 1: Vorbereitung auf die Migration

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.

2. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung(`*>`) erscheint.

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Deaktivieren Sie alle zum Knoten führenden Ports (außer ISL-Ports) an den beiden neuen Cluster-Switches cs1 und cs2.

   Deaktivieren Sie die ISL-Ports nicht.

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass die dem Knoten zugewandten Ports 1 bis 34 am Switch cs1 deaktiviert sind:

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

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden 9336C-FX2 Switches cs1 und cs2 an den Ports 1/35 und 1/36 aktiv sind:

   ```
   show port-channel summary
   ```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs1 aktiv sind:

```
cs1# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs2 aktiv sind:

```
(cs2)# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)
```

3. Liste der benachbarten Geräte anzeigen:

`show cdp neighbors`

Dieser Befehl liefert Informationen über die mit dem System verbundenen Geräte.

Beispiel anzeigen

Das folgende Beispiel listet die benachbarten Geräte am Switch cs1 auf:

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 2
```

Das folgende Beispiel listet die benachbarten Geräte am Switch cs2 auf:

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

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

Total entries displayed: 2
```

4. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

   `network port show -ipspace Cluster`

   Jeder Port sollte angezeigt werden für `Link` und gesund für `Health Status` Die

   Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

5. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind:

   `network interface show -vserver Cluster`

   Jeder Cluster-LIF sollte Folgendes anzeigen `true` für `Is Home` und haben `Status Admin/Oper` von oben/hoch.

Beispiel anzeigen

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

6. Automatische Wiederherstellung auf allen Cluster-LIFs deaktivieren:

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

   Beispiel anzeigen

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

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

4 entries were displayed.
```

7. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 1 und verbinden Sie dann e0a mit Port 1 des Cluster-Switches cs1 unter Verwendung der von den 9336C-FX2-Switches unterstützten geeigneten

Verkabelung.

Der "Hardware Universe – Schalter" enthält weitere Informationen zur Verkabelung.

"Hardware Universe – Schalter"

8. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 2 und verbinden Sie dann e0a mit Port 2 des Cluster-Switches cs1 unter Verwendung der von den 9336C-FX2-Switches unterstützten geeigneten Verkabelung.
9. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs1.

Beispiel anzeigen

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

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

10. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf node1 und node2 aktiv sind:

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

         Logical      Status     Network            Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask       Node         Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
         node1_clus1  up/up      169.254.209.69/16  node1        e0b
false
         node1_clus2  up/up      169.254.49.125/16  node1        e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2        e0b
false
         node2_clus2  up/up      169.254.19.183/16  node2        e0b
true

4 entries were displayed.
```

11. Informationen über den Status der Knoten im Cluster anzeigen:

    `cluster show`

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster an:

```
cluster1::*> cluster show

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

2 entries were displayed.
```

12. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 1 und verbinden Sie dann e0b mit Port 1 auf Cluster-Switch cs2. Verwenden Sie dazu die von den 9336C-FX2-Switches unterstützten Kabel.

13. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 2 und verbinden Sie dann e0b mit Port 2 des Cluster-Switches cs2 unter Verwendung der von den 9336C-FX2-Switches unterstützten geeigneten Verkabelung.
14. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs2.

    Beispiel anzeigen

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

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

15. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports auf Knoten 1 und Knoten 2 aktiv sind:

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

2. Auf Switch cs2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

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

(Wait for 5-10 seconds before re-enabling the ports)

cs2(config-if-range)# no shutdown

(After executing the no shutdown command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)

cs2(config-if-range)# exit
cs2(config)# exit
cs2#
```

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

   `network interface show -vserver Cluster`

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

   `network interface revert -vserver Cluster -lif *`

4. Überprüfen Sie, ob alle Schnittstellen den Wert „true“ anzeigen. `Is Home` :

   `network interface show -vserver Cluster`

   Dieser Vorgang kann mehrere Minuten dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf Knoten 1 und Knoten 2 aktiv sind und dass `Is Home` Die Ergebnisse sind korrekt:

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

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true

4 entries were displayed.
```

5. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

   `show cdp neighbors`

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
(cs1)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         133    H           FAS2980
e0a
node2              Eth1/2         133    H           FAS2980
e0a
cs2                Eth1/35        175    R S I s     N9K-C9336C
Eth1/35
cs2                Eth1/36        175    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4

(cs2)# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

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

Total entries displayed: 4
```

6. Informationen zu den in Ihrem Cluster gefundenen Netzwerkgeräten anzeigen:

   `network device-discovery show -protocol cdp`

   Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C9336C
            e0b    cs2                       0/2               N9K-
C9336C
node1      /cdp
            e0a    cs1                       0/1               N9K-
C9336C
            e0b    cs2                       0/1               N9K-
C9336C

4 entries were displayed.
```

7. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

   `network options switchless-cluster show`

   > Die Ausführung des Befehls kann mehrere Minuten dauern. Warten Sie auf die Ansage „Noch 3 Minuten bis zum Ablauf der Gültigkeitsdauer“.

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

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

8. Überprüfen Sie den Status der Knoten im Cluster:

   `cluster show`

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster:

```
cluster1::*> cluster show

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

9. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

2. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Ersetzen Sie die Schalter

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

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

Überprüfungsanforderungen

Bevor Sie den Schalter austauschen, stellen Sie sicher, dass Folgendes passiert:

- Sie haben die Seriennummer des Schalters überprüft, um sicherzustellen, dass der richtige Schalter ausgetauscht wird.
- Zur bestehenden Cluster- und Netzwerkinfrastruktur:
  - Der bestehende Cluster wurde als voll funktionsfähig verifiziert, wobei mindestens ein Cluster-Switch vollständig angeschlossen ist.
  - Alle Cluster-Ports sind **aktiv**.
  - Alle logischen Schnittstellen (LIFs) des Clusters sind aktiv und an ihren jeweiligen Ports angeschlossen.
  - Das ONTAP `cluster ping-cluster -node node1` Der Befehl muss anzeigen, dass die grundlegende Konnektivität und die Kommunikation über eine PMTU hinaus auf allen Pfaden erfolgreich sind.
- Zum Ersatzschalter des Nexus 9336C-FX2:
  - Die Management-Netzwerkanbindung des Ersatz-Switches ist funktionsfähig.
  - Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
  - Die Knotenverbindungen sind die Ports 1/1 bis 1/34.
  - Alle Inter-Switch Link (ISL)-Ports sind an den Ports 1/35 und 1/36 deaktiviert.
  - Die gewünschte Referenzkonfigurationsdatei (RCF) und das NX-OS-Betriebssystem-Image werden auf den Switch geladen.
  - Die erste Anpassung des Schalters ist abgeschlossen, wie in folgendem Abschnitt detailliert beschrieben:"Konfigurieren des Cluster-Switches 9336C-FX2" Die

    Alle zuvor vorgenommenen Anpassungen am Standort, wie z. B. STP, SNMP und SSH, werden auf den neuen Switch kopiert.
- Sie haben den Befehl zum Migrieren eines Cluster-LIF von dem Knoten ausgeführt, auf dem der Cluster-LIF gehostet wird.

Konsolenprotokollierung aktivieren

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

- Lassen Sie AutoSupport während der Wartungsarbeiten aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs AutoSupport aus, um die Fallerstellung für die Dauer der Wartung zu deaktivieren. Siehe diesen Wissensdatenbankartikel "SU92: Wie man die automatische Fallerstellung während geplanter Wartungsfenster unterdrückt" für weitere Einzelheiten.
- Aktivieren Sie die Sitzungsprotokollierung für alle CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Wissensdatenbankartikel. "Wie konfiguriert man PuTTY für eine optimale Verbindung zu ONTAP -Systemen?" Die

Tauschen Sie den Schalter aus.

Zu den Beispielen

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

- Die Namen der vorhandenen Nexus 9336C-FX2 Switches lauten cs1 und cs2.
- Der neue Switch Nexus 9336C-FX2 trägt den Namen newcs2.
- Die Knotennamen lauten Knoten1 und Knoten2.
- Die Cluster-Ports auf jedem Knoten tragen die Namen e0a und e0b.
- Die Cluster-LIF-Namen lauten node1_clus1 und node1_clus2 für Knoten 1 sowie node2_clus1 und node2_clus2 für Knoten 2.
- Die Aufforderung zum Ändern aller Clusterknoten lautet cluster1::*>

Informationen zu diesem Vorgang

Das folgende Verfahren basiert auf der folgenden Cluster-Netzwerktopologie:

Beispiel anzeigen

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

Node: node1

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

Node: node2

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



cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
```

```
true
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true
4 entries were displayed.



cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C9336C
            e0b    cs2                       Eth1/2            N9K-
C9336C
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C9336C
            e0b    cs2                       Eth1/1            N9K-
C9336C
4 entries were displayed.



cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2                Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
cs2(FDO220329V5)   Eth1/36        176    R S I s     N9K-C9336C
Eth1/36

Total entries displayed: 4
```

```
cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

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

Total entries displayed: 4
```

Schritt 1: Vorbereitung auf den Austausch

1. Wenn AutoSupport 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.

2. Installieren Sie die entsprechende RCF-Datei und das Image auf dem Switch newcs2 und treffen Sie alle notwendigen Vorbereitungen vor Ort.

   Prüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und NX-OS-Software für den neuen Switch. Wenn Sie überprüft haben, dass der neue Switch korrekt eingerichtet ist und keine Aktualisierungen der RCF- und NX-OS-Software erforderlich sind, fahren Sie mit Schritt 2 fort.

   a. Gehen Sie auf der NetApp Support-Website zur Seite „NetApp Cluster and Management Network Switches Reference Configuration File Description Page“.
   b. Klicken Sie auf den Link zur *Kompatibilitätsmatrix für Cluster- und Managementnetzwerke* und notieren Sie sich anschließend die erforderliche Switch-Softwareversion.
   c. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Beschreibungsseite zurückzukehren, klicken Sie auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und gehen Sie dann zur Downloadseite.
   d. Folgen Sie den Anweisungen auf der Downloadseite, um die korrekten RCF- und NX-OS-Dateien für die Version der ONTAP -Software herunterzuladen, die Sie installieren.

3. Melden Sie sich auf dem neuen Switch als Administrator an und fahren Sie alle Ports herunter, die mit den Knotenclusterschnittstellen verbunden werden (Ports 1/1 bis 1/34).

Wenn der zu ersetzende Schalter nicht funktionsfähig und ausgeschaltet ist, fahren Sie mit Schritt 4 fort. Die LIFs auf den Clusterknoten sollten bereits für jeden Knoten auf den anderen Clusterport umgeschaltet haben.

Beispiel anzeigen

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

4. Überprüfen Sie, ob für alle Cluster-LIFs die automatische Rücksetzung aktiviert ist:

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

   Beispiel anzeigen

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

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

4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Schritt 2: Kabel und Anschlüsse konfigurieren

1. Schalten Sie die ISL-Ports 1/35 und 1/36 am Switch Nexus 9336C-FX2 cs1 ab.

   Beispiel anzeigen

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

2. Entfernen Sie alle Kabel vom Nexus 9336C-FX2 cs2-Switch und schließen Sie sie dann an dieselben Ports am Nexus C9336C-FX2 newcs2-Switch an.
3. Aktivieren Sie die ISL-Ports 1/35 und 1/36 zwischen den Switches cs1 und newcs2 und überprüfen Sie dann den Betriebsstatus des Portkanals.

   Port-Channel sollte Po1(SU) und Member Ports sollten Eth1/35(P) und Eth1/36(P) anzeigen.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/35 und 1/36 und zeigt die Port-Kanal-Zusammenfassung auf Switch cs1 an:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/35-36
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member       Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/35(P)   Eth1/36(P)

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

4. Überprüfen Sie, ob Port e0b auf allen Knoten aktiv ist:

   `network port show ipspace Cluster`

Beispiel anzeigen

Die Ausgabe sollte in etwa wie folgt aussehen:

```
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/auto   -
false

4 entries were displayed.
```

5. Auf demselben Knoten, den Sie im vorherigen Schritt verwendet haben, stellen Sie die Cluster-LIF, die dem Port im vorherigen Schritt zugeordnet ist, mit dem Befehl network interface revert wieder her.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert Home true ist und der Port e0b lautet.

Die folgenden Befehle geben LIF zurück. `node1_clus2` An `node1` zum Heimathafen `e0a` und zeigt Informationen über die LIFs auf beiden Knoten an. Das Hochfahren des ersten Knotens ist erfolgreich, wenn die Spalte „Is Home“ für beide Cluster-Schnittstellen den Wert „true“ aufweist und die korrekten Portzuweisungen angezeigt werden. `e0a` Und `e0b` auf Knoten1.

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false

4 entries were displayed.
```

6. Informationen über die Knoten in einem Cluster anzeigen:

`cluster show`

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Knotenstatus für Knoten 1 und Knoten 2 in diesem Cluster „true“ ist:

```
cluster1::*> cluster show

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

7. Überprüfen Sie, ob alle physischen Cluster-Ports aktiv sind:

   `network port show ipspace Cluster`

   Beispiel anzeigen

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

Node node1
Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e0a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e0b       Cluster     Cluster           up    9000  auto/10000
healthy  false

Node: node2

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

4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Schritt 3: Konfiguration überprüfen

1. Bestätigen Sie die folgende Cluster-Netzwerkkonfiguration:

   ```
   network port show
   ```

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
```

```
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.

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

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

4 entries were displayed.


cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e0a
node2                Eth1/2         145    H           FAS2980
e0a
newcs2               Eth1/35        176    R S I s     N9K-C9336C
Eth1/35
newcs2               Eth1/36        176    R S I s     N9K-C9336C
```

```
Eth1/36

Total entries displayed: 4


cs2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

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

Total entries displayed: 4
```

2. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nachdem Sie Ihre Schalter ausgetauscht haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

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

Für ONTAP 9.3 und höher können Sie von einem Cluster mit einem Switched-Cluster-Netzwerk zu einem Cluster migrieren, in dem zwei Knoten direkt miteinander verbunden sind.

Überprüfungsanforderungen

Richtlinien

Bitte beachten Sie die folgenden Richtlinien:

- Die Migration zu einer Zwei-Knoten-Clusterkonfiguration ohne Switches ist ein unterbrechungsfreier Vorgang. Die meisten Systeme verfügen über zwei dedizierte Cluster-Interconnect-Ports pro Knoten. Dieses Verfahren kann aber auch für Systeme mit einer größeren Anzahl dedizierter Cluster-Interconnect-Ports pro Knoten angewendet werden, beispielsweise vier, sechs oder acht.
- Die Funktion „Switchless Cluster Interconnect“ kann nicht mit mehr als zwei Knoten verwendet werden.
- Wenn Sie über einen bestehenden Zwei-Knoten-Cluster verfügen, der Cluster-Interconnect-Switches verwendet und auf dem ONTAP 9.3 oder höher läuft, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Knoten ersetzen.

Bevor Sie beginnen

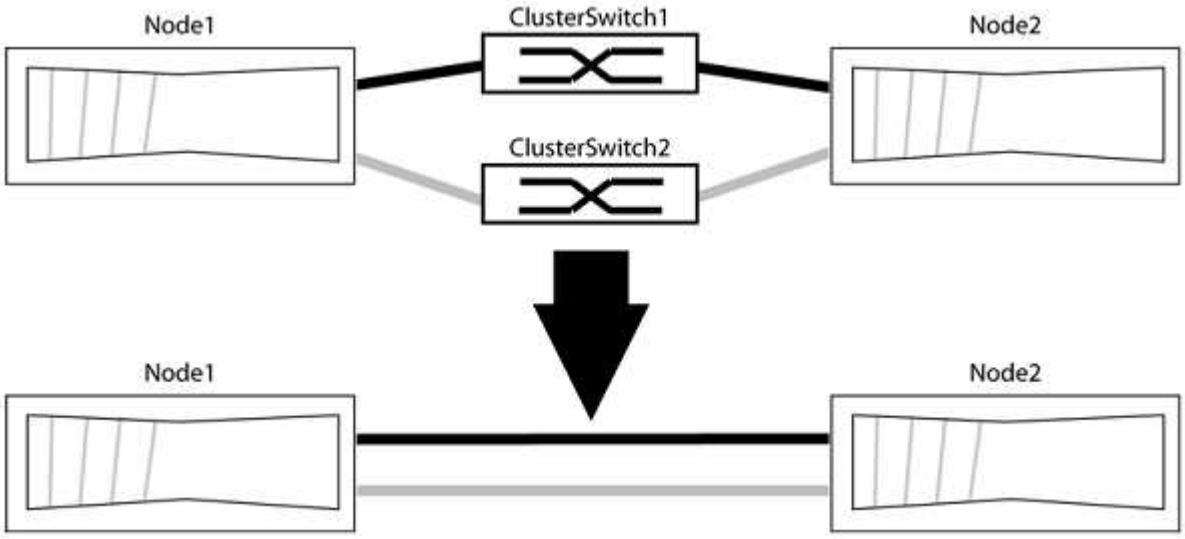
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesunder Cluster, der aus zwei Knoten besteht, die über Cluster-Switches verbunden sind. Auf den Knoten muss die gleiche ONTAP Version laufen.
- Jeder Knoten verfügt über die erforderliche Anzahl dedizierter Cluster-Ports, die redundante Cluster-Verbindungen bereitstellen, um Ihre Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster-Verbindungsports auf jedem Knoten.

Migrieren Sie die Schalter

Informationen zu diesem Vorgang

Das folgende Verfahren entfernt die Cluster-Switches in einem Zwei-Knoten-Cluster und ersetzt jede Verbindung zum Switch durch eine direkte Verbindung zum Partnerknoten.



Zu den Beispielen

Die Beispiele im folgenden Verfahren zeigen Knoten, die "e0a" und "e0b" als Cluster-Ports verwenden. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.

Schritt 1: Vorbereitung auf die Migration

1. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

Die erweiterte Aufforderung `*>` erscheint.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von switchlosen Clustern, die standardmäßig aktiviert ist.

   Sie können überprüfen, ob die Erkennung von Clustern ohne Switch aktiviert ist, indem Sie den Befehl mit erweiterten Berechtigungen ausführen:

   `network options detect-switchless-cluster show`

   Beispiel anzeigen

   Die folgende Beispielausgabe zeigt, ob die Option aktiviert ist.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Wenn "Schalterlose Clustererkennung aktivieren" `false` Wenden Sie sich an den NetApp Support.

3. 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=<number_of_hours>h`

   Wo `h` ist die Dauer des Wartungsfensters in Stunden. Die Meldung informiert den technischen Support über diese Wartungsaufgabe, damit dieser die automatische Fallerstellung während des Wartungsfensters unterdrücken kann.

   Im folgenden Beispiel unterdrückt der Befehl die automatische Fallerstellung für zwei Stunden:

   Beispiel anzeigen

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

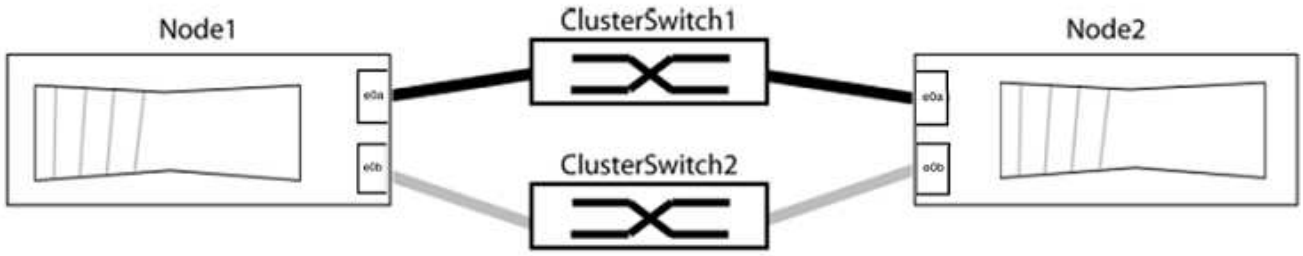
Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen ein, sodass die Cluster-Ports in Gruppe 1 an Cluster-Switch 1 und die Cluster-Ports in Gruppe 2 an Cluster-Switch 2 angeschlossen werden. Diese Gruppen werden im weiteren Verlauf des Verfahrens benötigt.
2. Identifizieren Sie die Cluster-Ports und überprüfen Sie den Verbindungsstatus und die Integrität:

   `network port show -ipspace Cluster`

   Im folgenden Beispiel für Knoten mit Cluster-Ports „e0a“ und „e0b“ wird eine Gruppe als „node1:e0a“ und

„node2:e0a“ und die andere Gruppe als „node1:e0b“ und „node2:e0b“ identifiziert. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



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

Beispiel anzeigen

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Vergewissern Sie sich, dass alle Cluster-LIFs an ihren jeweiligen Heimatports angeschlossen sind.

   Überprüfen Sie, ob die Spalte „is-home“ `true` für jeden der Cluster-LIFs:

   ```
   network interface show -vserver Cluster -fields is-home
   ```

   Beispiel anzeigen

   ```
   cluster::*> net int show -vserver Cluster -fields is-home
   (network interface show)
   vserver  lif          is-home
   -------- ------------ --------
   Cluster  node1_clus1  true
   Cluster  node1_clus2  true
   Cluster  node2_clus1  true
   Cluster  node2_clus2  true
   4 entries were displayed.
   ```

   Falls Cluster-LIFs vorhanden sind, die sich nicht auf ihren Heimatports befinden, werden diese LIFs wieder auf ihre Heimatports zurückgesetzt:

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

4. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

5. Überprüfen Sie, ob alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

   In der Spalte „Erkanntes Gerät“ sollte der Name des Cluster-Switches stehen, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports "e0a" und "e0b" korrekt mit den Cluster-Switches "cs1" und "cs2" verbunden sind.

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 7]] Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster ring show
   ```

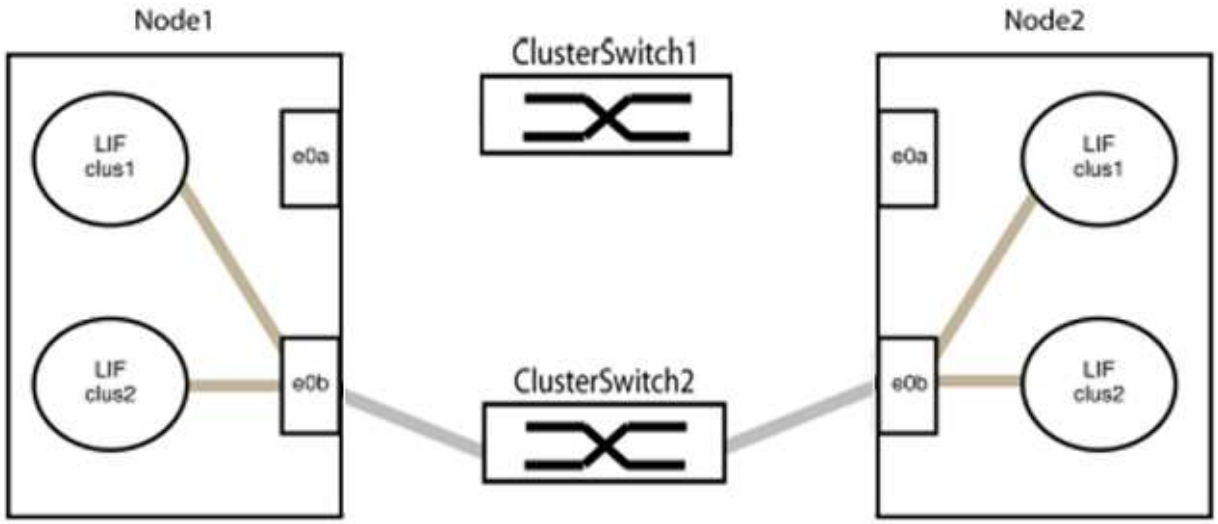
   Alle Einheiten müssen entweder Master- oder Sekundäreinheiten sein.

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

   > Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe1 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

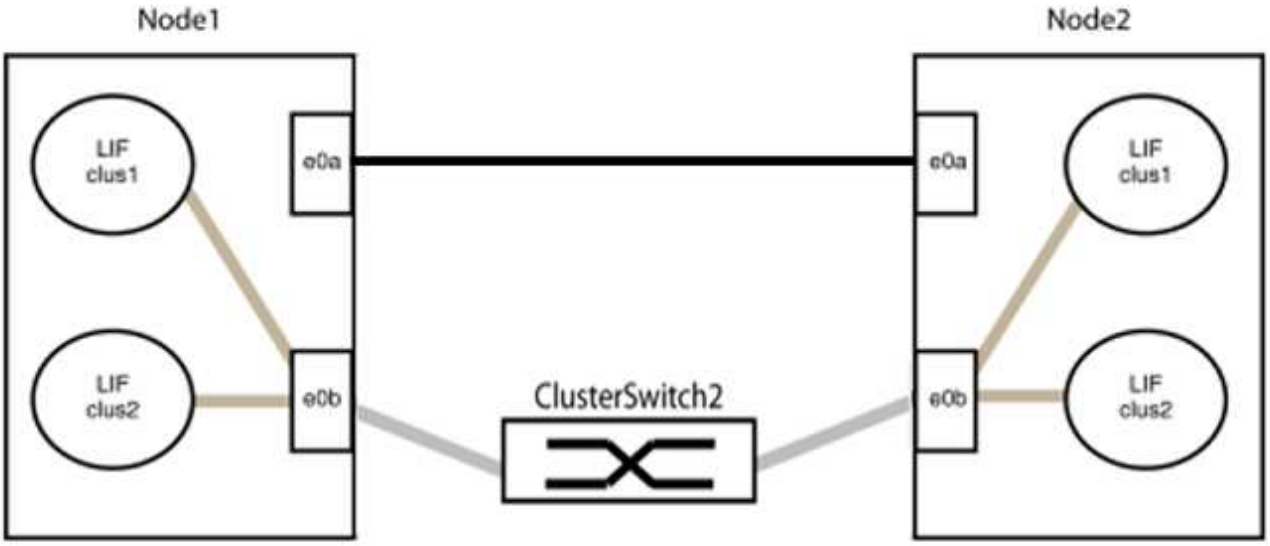
   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

      Im folgenden Beispiel werden die Kabel an Port „e0a“ auf jedem Knoten getrennt, und der Cluster-Datenverkehr wird weiterhin über den Switch und Port „e0b“ auf jedem Knoten abgewickelt:



b. Verbinden Sie die Ports in Gruppe 1 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden:



3. Die Option für ein schalterloses Clusternetzwerk wechselt von `false` Zu `true` Die Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „Schalterlos“ aktiviert ist. `true` :

`network options switchless-cluster show`

Das folgende Beispiel zeigt, dass der switchlose Cluster aktiviert ist:

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

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

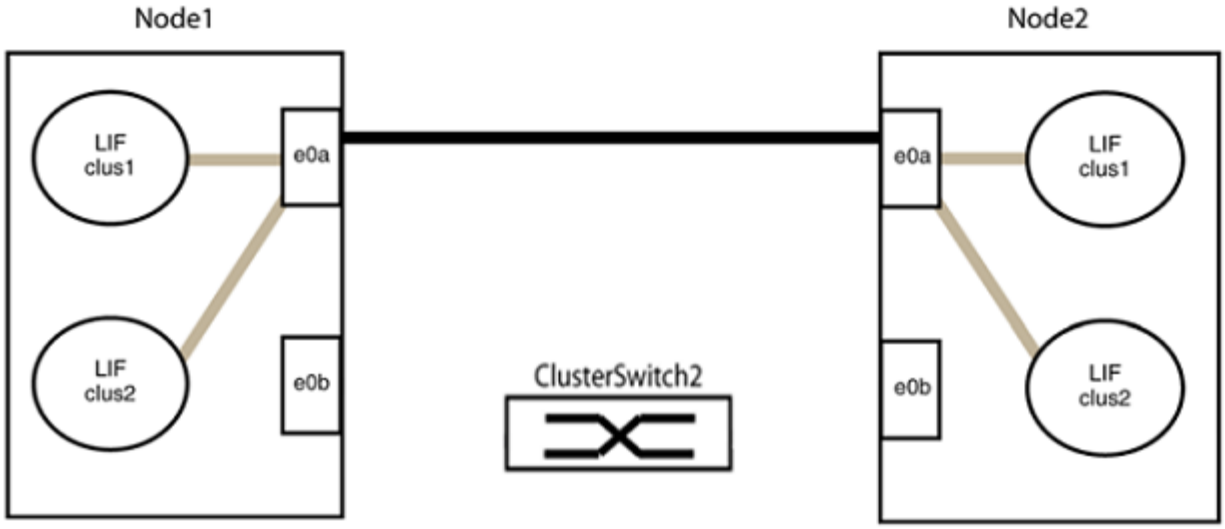
Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung in Gruppe 1 zu bestätigen.

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

   Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe 2 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 2.

      Im folgenden Beispiel werden die Kabel von Port "e0b" an jedem Knoten getrennt, und der Cluster-Datenverkehr wird über die direkte Verbindung zwischen den Ports "e0a" fortgesetzt:



b. Verbinden Sie die Ports in Gruppe 2 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden und "e0b" auf Knoten 1 ist mit "e0b" auf Knoten 2 verbunden:

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie, ob die Ports an beiden Knoten korrekt verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port des Cluster-Partners verbunden sind:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Automatische Rücksetzung für die Cluster-LIFs wieder aktivieren:

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

3. Überprüfen Sie, ob alle LIFs zu Hause sind. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „Ist zu Hause“ den Wert „Ist zu Hause“ aufweist. `true` , wie gezeigt für `node1_clus2` Und `node2_clus2` im folgenden Beispiel:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif          curr-port is-home
-------- ------------ --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

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

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

4. Überprüfen Sie den Clusterstatus der Knoten über die Systemkonsole eines der beiden Knoten:

   `cluster show`

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass epsilon an beiden Knoten gleich ist. `false` :

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Falls Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

   Weitere Informationen finden Sie unter "NetApp KB-Artikel 1010449: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster".

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

NVIDIA SN2100

Erste Schritte

Installations- und Einrichtungsworkflow für NVIDIA SN2100-Switches

Der NVIDIA SN2100 ist ein Cluster-Switch, mit dem Sie ONTAP -Cluster mit mehr als zwei Knoten aufbauen können.

Befolgen Sie diese Arbeitsschritte, um Ihre NVIDIA SN2100-Switches zu installieren und einzurichten.

1. **"Überprüfen der Konfigurationsanforderungen"**

Überprüfen Sie die Konfigurationsanforderungen für den SN2100-Cluster-Switch.

2. **"Überprüfen Sie die Komponenten und Teilenummern"**

Überprüfen Sie die Komponenten und Teilenummern für den Cluster-Switch SN2100.

3. **"Überprüfen Sie die erforderlichen Unterlagen"**

Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre SN2100-Switches und den ONTAP Cluster einzurichten.

4. **"Installieren Sie die Hardware"**

Installieren Sie die Switch-Hardware.

5. **"Konfigurieren der Software"**

Konfigurieren Sie die Switch-Software.

Konfigurationsanforderungen für NVIDIA SN2100-Switches

Für die Installation und Wartung des NVIDIA SN2100 Switches sollten Sie unbedingt alle Konfigurationsanforderungen beachten.

Installationsvoraussetzungen

Wenn Sie ONTAP -Cluster mit mehr als zwei Knoten aufbauen möchten, benötigen Sie zwei unterstützte Cluster-Netzwerk-Switches. Sie können zusätzliche Management-Schalter verwenden, die optional sind.

Sie installieren den NVIDIA SN2100 Switch (X190006) im NVIDIA Dual/Single Switch Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Richtlinien zur Verkabelung finden Sie unter"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Die

ONTAP und Linux-Unterstützung

Der NVIDIA SN2100 Switch ist ein 10/25/40/100GbE Switch, auf dem Cumulus Linux läuft. Der Schalter unterstützt Folgendes:

- ONTAP 9.10.1P3 und höher

  Der SN2100-Switch dient Cluster- und Speicheranwendungen in ONTAP 9.10.1P3 und späteren Versionen über verschiedene Switch-Paare.

- Cumulus Linux (CL) Betriebssystemversionen

- Bestimmte CL-Versionen sind von NetApp qualifiziert und werden unterstützt. Aktuelle Informationen zur Kompatibilität finden Sie unter"Informationen zu NVIDIA Ethernet-Switches" Seite oder die"NetApp Hardware Universe" Die
- Um die SN2100 Cumulus-Software von NVIDIA herunterzuladen, benötigen Sie Anmeldeinformationen für den Zugriff auf das Enterprise Support Portal von NVIDIA. Siehe den Artikel in der Wissensdatenbank. "So registrieren Sie sich bei NVIDIA für den Zugriff auf das Enterprise-Supportportal" Die

- Sie können Cumulus Linux installieren, wenn auf dem Switch Cumulus Linux oder ONIE läuft.

Wie geht es weiter?

Nachdem Sie die Konfigurationsanforderungen geprüft haben, können Sie Ihre "Komponenten und Teilenummern"Die

Komponenten und Teilenummern für NVIDIA SN2100-Schalter

Für die Installation und Wartung des NVIDIA SN2100 Switches sollten Sie unbedingt die Liste der Komponenten und die Teilenummern für das Gehäuse und das Schienenset überprüfen.

Schrankdetails

Sie installieren den NVIDIA SN2100 Switch (X190006) im NVIDIA Dual/Single Switch Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Details zum Schienenbausatz

Die folgende Tabelle listet die Teilenummer und die Beschreibung für die SN2100-Weichen und Schienensätze auf:

Teilenummer	Beschreibung
X190006-PE	Cluster-Switch, NVIDIA SN2100, 16PT 100GbE, PTSX
X190006-PI	Cluster-Switch, NVIDIA SN2100, 16PT 100GbE, PSIN
X-MTEF-KIT-D	Schienen-Kit, NVIDIA Dual-Schalter nebeneinander
X-MTEF-KIT-E	Schienensatz, NVIDIA Einzelschalter kurze Tiefe

Weitere Informationen finden Sie in der NVIDIA Dokumentation. "Installation Ihres SN2100-Weichen- und Schienensatzes" Die

Wie geht es weiter?

Nachdem Sie Ihre Komponenten und Teilenummern bestätigt haben, können Sie die folgenden überprüfen: "erforderliche Dokumentation"Die

Dokumentationsanforderungen für NVIDIA SN2100-Switches

Für die Installation und Wartung des NVIDIA SN2100 Switches sollten Sie unbedingt die

gesamte empfohlene Dokumentation lesen.

Titel	Beschreibung
"NVIDIA Switch Installationsanleitung"	Beschreibt die Installation Ihrer NVIDIA SN2100 Switches.
"NS224 NVMe-Laufwerksgehäuse-Verkabelungsleitfaden"	Übersicht und Abbildungen zur Konfiguration der Verkabelung von Laufwerksschächten.
"NetApp Hardware Universe"	Ermöglicht es Ihnen, die für Ihr Plattformmodell unterstützte Hardware, wie z. B. Speicherschalter und Kabel, zu bestätigen.

Installieren Sie die Hardware

Workflow zur Hardwareinstallation für NVIDIA SN2100-Switches

Um die Hardware für einen SN2100-Cluster-Switch zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

1. **"Installieren Sie die Hardware"**

Installieren Sie die Switch-Hardware.

2. **"Überprüfung der Verkabelung und Konfigurationsüberlegungen"**

Überprüfen Sie die Anforderungen an optische Verbindungen, den QSA-Adapter und die Switchport-Geschwindigkeit.

3. **"Verkabeln Sie die NS224-Regale"**

Befolgen Sie die Verkabelungsprozeduren, wenn Sie ein System haben, in dem die NS224-Laufwerksschächte als Switch-Attached Storage (nicht als Direct-Attached Storage) verkabelt werden müssen.

Installieren Sie die Hardware für den NVIDIA SN2100-Switch.

Zur Installation der SN2100-Hardware konsultieren Sie bitte die Dokumentation von NVIDIA.

Schritte

1. Überprüfen Sie die"Konfigurationsanforderungen" Die
2. Befolgen Sie die Anweisungen in "NVIDIA Switch Installationsanleitung" Die

Wie geht es weiter?

Nachdem Sie Ihre Hardware installiert haben, können Sie"Verkabelung und Konfiguration überprüfen" Anforderungen.

Überprüfung der Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren NVIDIA SN2100 Switch konfigurieren, beachten Sie bitte die folgenden Hinweise.

NVIDIA -Portdetails

Switch-Ports	Portnutzung
swp1s0-3	4x10GbE Breakout-Cluster-Portknoten
swp2s0-3	4x25GbE Breakout-Cluster-Portknoten
swp3-14	40/100GbE-Cluster-Portknoten
swp15-16	100GbE Inter-Switch Link (ISL)-Ports

Siehe die "Hardware Universe" Weitere Informationen zu Switch-Ports finden Sie hier.

Verbindungsverzögerungen bei optischen Verbindungen

Falls Sie Verbindungsverzögerungen von mehr als fünf Sekunden feststellen, bietet Cumulus Linux 5.4 und spätere Versionen Unterstützung für schnelles Verbindungsaufbauen. Sie können die Links mithilfe der folgenden Funktion konfigurieren: `nv set` Befehl wie folgt:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Beispiel anzeigen

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Unterstützung für Kupferverbindungen

Um dieses Problem zu beheben, sind folgende Konfigurationsänderungen erforderlich.

Cumulus Linux 4.4.3

1. Ermitteln Sie die Bezeichnung für jede Schnittstelle, die 40GbE/100GbE-Kupferkabel verwendet:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Fügen Sie die folgenden zwei Zeilen hinzu: `/etc/cumulus/switchd.conf` Datei für jeden Port (swp<n>), der 40GbE/100GbE-Kupferkabel verwendet:

   - `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
   - `interface.swp<n>.enable_short_tuning=TRUE`

   Beispiel:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Starten Sie das Gerät neu. `switchd` Service:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Vergewissern Sie sich, dass die Ports aktiv sind:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
UP     swp3      100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                      Master:
bridge(UP)
```

Cumulus Linux 5.x

1. Ermitteln Sie die Bezeichnung für jede Schnittstelle, die 40GbE/100GbE-Kupferkabel verwendet:

```
cumulus@cumulus:mgmt:~$ nv show interface --view=pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Konfigurieren Sie die Links mithilfe der `nv set` Befehl wie folgt:
   - `nv set interface <interface-id> link fast-linkup on`
   - `nv config apply`
   - Laden Sie die `switchd` Service

     Beispiel:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Vergewissern Sie sich, dass die Ports aktiv sind:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode        LLDP                Summary
-----  --------- ----  -----  ----------  ------------------  --------
UP     swp3      100G  9216   Trunk/L2                        Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                        Master:
bridge(UP)
```

Siehe den Artikel in der Wissensdatenbank."Der SN2100-Switch kann keine Verbindung über 40/100GbE-Kupferkabel herstellen." für weitere Einzelheiten.

Unter Cumulus Linux 4.4.2 werden Kupferverbindungen auf SN2100-Switches mit X1151A NIC, X1146A NIC oder integrierten 100GbE-Ports nicht unterstützt. Beispiel:

- AFF A800 an den Ports e0a und e0b
- AFF A320 an den Ports e0g und e0h

QSA-Modul

Bei Verwendung von QSFP+ (40GbE) zu SFP+ (10GbE) Adaptern oder QSFP28 (100GbE) zu SFP28 (25GbE) Adaptern (QSA) stecken Sie diese in nicht-breakout 40GbE/100GbE Switch-Ports (swp3-swp14). Stecken Sie das QSA-Modul nicht in einen Port, der für Breakout konfiguriert ist.

Wenn ein QSA-Modul verwendet wird, um eine Verbindung zu den 10GbE/25GbE-Cluster-Ports einer Plattform herzustellen, kann es vorkommen, dass die Verbindung nicht zustande kommt.

Um dieses Problem zu beheben, gehen Sie wie folgt vor:

- Bei 10GbE stellen Sie die Verbindungsgeschwindigkeit manuell auf 10000 ein und deaktivieren die automatische Aushandlung.
- Bei 25GbE stellen Sie die Verbindungsgeschwindigkeit manuell auf 25000 ein und deaktivieren Sie die automatische Aushandlung.

Einstellen der Schnittstellengeschwindigkeit an Breakout-Ports

Je nach Transceiver im Switch-Port müssen Sie möglicherweise die Geschwindigkeit an der Switch-Schnittstelle auf eine feste Geschwindigkeit einstellen. Bei Verwendung von 10GbE- und 25GbE-Breakout-Ports oder eines QSA-Moduls überprüfen Sie, ob die automatische Aushandlung deaktiviert ist und stellen Sie die Schnittstellengeschwindigkeit am Switch ein.

Cumulus Linux 4.4.3

Beispiel:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces     2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000  <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
     alias 10G Intra-Cluster Node
-    link-autoneg off
+    link-autoneg on
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp2s0
iface swp2s0
     alias 25G Intra-Cluster Node
     link-autoneg off
     link-speed 25000 <---- port speed set
```

Überprüfen Sie den Schnittstellen- und Portstatus, um sicherzustellen, dass die Einstellungen angewendet wurden:

```
cumulus@cumulus:mgmt:~$ net show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Cumulus Linux 5.x

Beispiel:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3

link

  auto-negotiate        off                   off
off
  duplex                full                  full
full
  speed                 10G                   10G
10G
  fec                   auto                  auto
auto
  mtu                   9216                  9216
9216
[breakout]

  state                 up                    up
up
```

Überprüfen Sie den Schnittstellen- und Portstatus, um sicherzustellen, dass die Einstellungen angewendet wurden:

```
cumulus@cumulus:mgmt:~$ nv show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Siehe die "Hardware Universe"und der Artikel in der Wissensdatenbank "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" für weitere Informationen.

Wie geht es weiter?

Nachdem Sie Ihre Verkabelungs- und Konfigurationsanforderungen überprüft haben, können Sie"Verkabeln Sie die NS224-Regale als schaltergebundene Aufbewahrung." Die

Verkabeln Sie die NS224-Regale als schaltergebundene Aufbewahrungslösung.

Falls Sie ein System haben, in dem die NS224-Laufwerksschächte als Switch-Attached Storage (nicht als Direct-Attached Storage) verkabelt werden müssen, verwenden Sie die hier bereitgestellten Informationen.

- Kabel NS224 treibt Regale über Speicherschalter an:

  "Kabelumschalter-angeschlossene NS224-Laufwerksschächte"

- Prüfen Sie, ob Ihre Plattformmodelle mit unterstützter Hardware wie Speicherschaltern und Kabeln kompatibel sind:

  "NetApp Hardware Universe"

Wie geht es weiter?

Nachdem Sie Ihre Regale verkabelt haben, können Sie"Konfigurieren Sie den Switch" Die

Konfigurieren der Software

Softwareinstallations-Workflow für NVIDIA SN2100-Switches

Um die Software für einen NVIDIA SN2100 Switch zu installieren und zu konfigurieren, befolgen Sie diese Schritte:

1. **"Konfigurieren Sie den Schalter"**

   Konfigurieren Sie den NVIDIA SN2100-Switch.

2. **"Installieren Sie Cumulus Linux im Cumulus-Modus"**

   Sie können das Betriebssystem Cumulus Linux (CL) installieren, wenn auf dem Switch Cumulus Linux ausgeführt wird.

3. **"Installieren Sie Cumulus Linux im ONIE-Modus"**

   Alternativ können Sie das Betriebssystem Cumulus Linux (CL) installieren, wenn auf dem Switch Cumulus Linux im ONIE-Modus ausgeführt wird.

4. **"Aktualisieren Sie Ihre Cumulus Linux-Version nach Bedarf"**

   Sie können Ihr Cumulus Linux (CL)-Betriebssystem nach Bedarf aktualisieren.

5. **"Installieren oder aktualisieren Sie das Skript der Referenzkonfigurationsdatei (RCF)."**

   Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Die Vorgehensweise ist für alle Fälle gleich.

6 **"Installieren Sie die CSHM-Datei"**

Sie können die entsprechende Konfigurationsdatei für die Zustandsüberwachung von Ethernet-Switches in NVIDIA -Cluster-Switches installieren.

7 **"Setzen Sie den Schalter auf die Werkseinstellungen zurück."**

Löschen Sie die Einstellungen des SN2100-Cluster-Switches.

Konfigurieren Sie den NVIDIA SN2100-Switch

Informationen zur Konfiguration des SN2100-Switches finden Sie in der Dokumentation von NVIDIA.

Schritte

1. Überprüfen Sie die"Konfigurationsanforderungen" Die
2. Befolgen Sie die Anweisungen in "NVIDIA -Systemstart." Die

Wie geht es weiter?

Nachdem Sie Ihren Switch konfiguriert haben, können Sie"Cumulus Linux im Cumulus-Modus installieren" oder"Cumulus Linux im ONIE-Modus installieren" Die

Installieren Sie Cumulus Linux im Cumulus-Modus

Führen Sie diese Schritte aus, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im Cumulus-Modus läuft.

ⓘ Cumulus Linux (CL) OS kann entweder installiert werden, wenn auf dem Switch Cumulus Linux oder ONIE läuft (siehe"Installation im ONIE-Modus").

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Linux-Kenntnisse auf mittlerem Niveau.
- Kenntnisse in grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren ist vorinstalliert, darunter `vi` Und `nano` Die
- Zugriff auf eine Linux- oder UNIX-Shell. Wenn Sie Windows verwenden, nutzen Sie eine Linux-Umgebung als Befehlszeilentool für die Interaktion mit Cumulus Linux.
- Die Baudratenanforderung für den seriellen Konsolen-Switch für den Konsolenzugriff des NVIDIA SN2100-Switches ist wie folgt auf 115200 eingestellt:
  - 115200 Baud
  - 8 Datenbits
  - 1 Stoppbit
  - Parität: keine
  - Flusssteuerung: keine

Informationen zu diesem Vorgang

Beachten Sie Folgendes:

Bei jeder Neuinstallation von Cumulus Linux wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

Das Standardpasswort für das Cumulus-Benutzerkonto lautet **cumulus**. Beim ersten Anmelden bei Cumulus Linux müssen Sie dieses Standardpasswort ändern. Aktualisieren Sie unbedingt alle Automatisierungsskripte, bevor Sie ein neues Image installieren. Cumulus Linux bietet Befehlszeilenoptionen, um das Standardpasswort während des Installationsprozesses automatisch zu ändern.

Beispiel 1. Schritte

Cumulus Linux 4.4.3

1. Melden Sie sich am Switch an.

   Für die erstmalige Anmeldung am Switch werden der Benutzername und das Passwort **cumulus** /**cumulus** benötigt. `sudo` Privilegien.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Überprüfen Sie die Cumulus Linux-Version: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standardgateway. Der neue Hostname wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

   Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0` Die Diese Schnittstelle ist speziell für die Out-of-Band-Verwaltung vorgesehen. Standardmäßig verwendet die Verwaltungsschnittstelle DHCPv4 zur Adressierung.

Verwenden Sie im Hostnamen keinen Unterstrich (_), keinen Apostroph (') und keine Nicht-ASCII-Zeichen.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Dieser Befehl ändert beides `/etc/hostname` Und `/etc/hosts` Dateien.

4. Prüfen Sie, ob Hostname, IP-Adresse, Subnetzmaske und Standardgateway aktualisiert wurden.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Stellen Sie Datum, Uhrzeit, Zeitzone und NTP-Server am Switch ein.
   a. Überprüfen Sie die aktuelle Zeitzone:

```
cumulus@sw1:~$ cat /etc/timezone
```

   b. Aktualisierung auf die neue Zeitzone:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Überprüfen Sie Ihre aktuelle Zeitzone:

```
cumulus@switch:~$ date +%Z
```

d. Um die Zeitzone mithilfe des geführten Assistenten einzustellen, führen Sie folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Stellen Sie die Softwareuhr entsprechend der konfigurierten Zeitzone ein:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Den aktuellen Wert der Softwareuhr auf den Wert der Hardwareuhr setzen:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Fügen Sie bei Bedarf einen NTP-Server hinzu:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>
iburst
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

h. Überprüfen Sie, ob `ntpd` läuft auf dem System:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

i. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig verwendet NTP die folgende Quellschnittstelle: `eth0` Die Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

```
cumulus@sw1:~$ net add time ntp source <src_int>
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

6. Installieren Sie Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie dazu aufgefordert werden.

7. Starten Sie den NVIDIA SN2100 Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation startet automatisch, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Treffen Sie **keine** Auswahlen.
   - Cumulus-Linux GNU/Linux
   - ONIE: Betriebssystem installieren
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.
10. Überprüfen Sie, ob die Cumulus Linux-Version 4.4.3 ist: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

    `sudo adduser --ingroup netedit admin`

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

Cumulus Linux 5.4.0

1. Melden Sie sich am Switch an.

   Für die erstmalige Anmeldung am Switch werden der Benutzername und das Passwort **cumulus**

/**cumulus** benötigt. `sudo` Privilegien.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standardgateway. Der neue Hostname wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0` Die Diese Schnittstelle ist speziell für die Out-of-Band-Verwaltung vorgesehen. Standardmäßig verwendet die Verwaltungsschnittstelle DHCPv4 zur Adressierung.

Verwenden Sie im Hostnamen keinen Unterstrich (_), keinen Apostroph (') und keine Nicht-ASCII-Zeichen.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Dieser Befehl ändert beides `/etc/hostname` Und `/etc/hosts` Dateien.

4. Prüfen Sie, ob Hostname, IP-Adresse, Subnetzmaske und Standardgateway aktualisiert wurden.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Stellen Sie Zeitzone, Datum, Uhrzeit und NTP-Server am Switch ein.
   a. Zeitzone einstellen:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Überprüfen Sie Ihre aktuelle Zeitzone:

```
cumulus@switch:~$ date +%Z
```

   c. Um die Zeitzone mithilfe des geführten Assistenten einzustellen, führen Sie folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

   d. Stellen Sie die Softwareuhr entsprechend der konfigurierten Zeitzone ein:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

   e. Den aktuellen Wert der Softwareuhr auf den Wert der Hardwareuhr setzen:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Fügen Sie bei Bedarf einen NTP-Server hinzu:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Siehe den Artikel in der Wissensdatenbank."Die NTP-Serverkonfiguration funktioniert nicht mit NVIDIA SN2100-Switches." für weitere Einzelheiten.

g. Überprüfen Sie, ob `ntpd` läuft auf dem System:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig verwendet NTP die folgende Quellschnittstelle: `eth0` Die Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installieren Sie Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie dazu aufgefordert werden.

7. Starten Sie den NVIDIA SN2100 Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation startet automatisch, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Treffen Sie **keine** Auswahlen.
   - Cumulus-Linux GNU/Linux
   - ONIE: Betriebssystem installieren
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.

10. Überprüfen Sie, ob die Cumulus Linux-Version 5.4.0 ist: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 13:37:36     system uptime
timezone            Etc/UTC              system time zone
```

11. Überprüfen Sie, ob jeder Knoten eine Verbindung zu jedem Switch hat:

```
cumulus@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ----------------------------------
-----------
eth0       100M   Mgmt        mgmt-sw1
Eth110/1/29
swp2s1     25G    Trunk/L2    node1
e0a
swp15      100G   BondMember  sw2
swp15
swp16      100G   BondMember  sw2
swp16
```

12. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Fügen Sie dem Administrator weitere Benutzergruppen hinzu, auf die er zugreifen kann. `nv` Befehle:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user 'admin' to group 'nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Cumulus Linux 5.11.0

1. Melden Sie sich am Switch an.

   Wenn Sie sich zum ersten Mal am Switch anmelden, benötigen Sie den Benutzernamen/das Passwort **cumulus**/**cumulus** mit `sudo` Privilegien.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standardgateway. Der neue Hostname wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

   Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0` Die Diese Schnittstelle ist speziell für die Out-of-Band-Verwaltung vorgesehen. Standardmäßig verwendet die Verwaltungsschnittstelle DHCPv4 zur Adressierung.

   Verwenden Sie im Hostnamen keinen Unterstrich (_), keinen Apostroph (') und keine Nicht-ASCII-Zeichen.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Dieser Befehl ändert beides `/etc/hostname` Und `/etc/hosts` Dateien.

4. Prüfen Sie, ob Hostname, IP-Adresse, Subnetzmaske und Standardgateway aktualisiert wurden.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Stellen Sie Zeitzone, Datum, Uhrzeit und NTP-Server am Switch ein.
   a. Zeitzone einstellen:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Überprüfen Sie Ihre aktuelle Zeitzone:

```
cumulus@switch:~$ date +%Z
```

   c. Um die Zeitzone mithilfe des geführten Assistenten einzustellen, führen Sie folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

d. Stellen Sie die Softwareuhr entsprechend der konfigurierten Zeitzone ein:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Den aktuellen Wert der Softwareuhr auf den Wert der Hardwareuhr setzen:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Fügen Sie bei Bedarf einen NTP-Server hinzu:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Siehe den Artikel in der Wissensdatenbank."Die NTP-Serverkonfiguration funktioniert nicht mit NVIDIA SN2100-Switches." für weitere Einzelheiten.

g. Überprüfen Sie, ob `ntpd` läuft auf dem System:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig verwendet NTP die folgende Quellschnittstelle: `eth0` Die Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installieren Sie Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie dazu aufgefordert werden.

7. Starten Sie den NVIDIA SN2100 Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation startet automatisch, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Treffen Sie **keine** Auswahlen.
   - Cumulus-Linux GNU/Linux
   - ONIE: Betriebssystem installieren
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.
10. Überprüfen Sie, ob die Cumulus Linux-Version 5.11.0 ist:

    `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied                 description
------------------- ----------------------- --------------------
build               Cumulus Linux 5.11.0
uptime              153 days, 2:44:16
hostname            cumulus                 cumulus
product-name        Cumulus Linux
product-release     5.11.0
platform            x86_64-mlnx_x86-r0
system-memory       2.76 GB used / 2.28 GB free / 7.47 GB total
swap-memory         0 Bytes used / 0 Bytes free / 0 Bytes total
health-status       not OK
date-time           2025-04-23 09:55:24
status              N/A
timezone            Etc/UTC
maintenance
  mode              disabled
  ports             enabled
version
  kernel            6.1.0-cl-1-amd64
  build-date        Thu Nov 14 13:06:38 UTC 2024
  image             5.11.0
  onie              2019.11-5.2.0020-115200
```

11. Überprüfen Sie, ob jeder Knoten mit jedem Switch verbunden ist:

```
cumulus@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   eth   mgmt-sw1
Eth110/1/14
swp2s1     25G    Trunk/L2    node1
e0a
swp1s1     10G    swp   sw2
e0a
swp9       100G   swp   sw3
e4a
swp10      100G   swp   sw4
e4a
swp15      100G   swp   sw5
swp15
swp16      100G   swp   sw6
swp16
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Wie geht es weiter?

Nachdem Sie Cumulus Linux im Cumulus-Modus installiert haben, "Installieren Sie das Skript der Referenzkonfigurationsdatei (RCF)."Die

Installieren Sie Cumulus Linux im ONIE-Modus

Gehen Sie wie folgt vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im ONIE-Modus läuft.

> Cumulus Linux (CL) OS kann entweder installiert werden, wenn auf dem Switch ONIE oder Cumulus Linux läuft (siehe"Installation im Cumulus-Modus").

Informationen zu diesem Vorgang

Sie können Cumulus Linux mithilfe der Open Network Install Environment (ONIE) installieren, die die automatische Erkennung eines Netzwerkinstallationsabbilds ermöglicht. Dies erleichtert das Systemmodell der Absicherung von Switches durch die Wahl eines Betriebssystems, wie beispielsweise Cumulus Linux. Cumulus Linux lässt sich am einfachsten mit ONIE über die lokale HTTP-Erkennung installieren.

> Wenn Ihr Host IPv6-fähig ist, stellen Sie sicher, dass darauf ein Webserver läuft. Wenn Ihr Host IPv4-fähig ist, stellen Sie sicher, dass er zusätzlich zu einem Webserver auch DHCP ausführt.

Dieses Verfahren zeigt, wie man Cumulus Linux aktualisiert, nachdem der Administrator in ONIE gestartet hat.

Beispiel 2. Schritte

Cumulus Linux 4.4.3

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Benennen Sie diese Datei um in: `onie-installer` Die
2. Verbinden Sie Ihren Host mithilfe eines Ethernet-Kabels mit dem Management-Ethernet-Port des Switches.
3. Den Schalter einschalten.

   Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der Installation erscheint die Cumulus Linux-Anmeldeaufforderung im Terminalfenster.

   > Bei jeder Neuinstallation von Cumulus Linux wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Switch neu:

   ```
   cumulus@cumulus:mgmt:~$ sudo reboot
   ```

5. Drücken Sie auf dem GNU GRUB-Bildschirm die **Esc**-Taste, um den normalen Bootvorgang zu unterbrechen, wählen Sie **ONIE** aus und drücken Sie **Enter**.
6. Im nächsten Bildschirm wählen Sie **ONIE: Betriebssystem installieren**.
7. Der ONIE-Installer-Erkennungsprozess wird ausgeführt und sucht nach der automatischen Installation. Drücken Sie die **Eingabetaste**, um den Vorgang vorübergehend zu unterbrechen.
8. Wenn der Ermittlungsprozess abgeschlossen ist:

   ```
   ONIE:/ # onie-stop
   discover: installer mode detected.
   Stopping: discover...start-stop-daemon: warning: killing process
   427:
   No such process done.
   ```

9. Wenn der DHCP-Dienst in Ihrem Netzwerk ausgeführt wird, überprüfen Sie, ob die IP-Adresse, die Subnetzmaske und das Standardgateway korrekt zugewiesen sind:

   ```
   ifconfig eth0
   ```

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface

default         10.233.204.1    0.0.0.0         UG    0      0
0   eth0
10.233.204.0    *               255.255.254.0   U     0      0
0   eth0
```

10. Wenn das IP-Adressierungsschema manuell definiert wurde, gehen Sie wie folgt vor:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Wiederholen Sie Schritt 9, um zu überprüfen, ob die statischen Informationen korrekt eingegeben wurden.
12. Installieren Sie Cumulus Linux:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-4.4.3-
mlx-amd64.bin
```

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-4.4.3-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-
4.4.3-mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

13. Nach Abschluss der Installation melden Sie sich am Switch an.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

14. Überprüfen Sie die Cumulus Linux-Version: `net show version`

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3”
```

Cumulus Linux 5.x

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Benennen Sie diese Datei um in: `onie-installer` Die
2. Verbinden Sie Ihren Host mithilfe eines Ethernet-Kabels mit dem Management-Ethernet-Port des Switches.
3. Den Schalter einschalten.

   Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der

Installation erscheint die Cumulus Linux-Anmeldeaufforderung im Terminalfenster.

> Bei jeder Neuinstallation von Cumulus Linux wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Switch neu:

```
cumulus@cumulus:mgmt:~$ sudo reboot
.
.
GNU GRUB version 2.06-3
+-------------------------------------------------------------------------
------+
| Cumulus-Linux GNU/Linux
|
| Advanced options for Cumulus-Linux GNU/Linux
|
| ONIE
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
|
+-------------------------------------------------------------------------
------+
```

5. Drücken Sie auf dem GNU GRUB-Bildschirm die Esc-Taste, um den normalen Bootvorgang zu unterbrechen, wählen Sie ONIE aus und drücken Sie Enter.

```
.
.
Loading ONIE ...

GNU GRUB version 2.02
+-------------------------------------------------------------------------
------+
| ONIE: Install OS
|
| ONIE: Rescue
|
| ONIE: Uninstall OS
|
| ONIE: Update ONIE
|
| ONIE: Embed ONIE
|
|
|
|
|
|
|
|
|
|
|
+-------------------------------------------------------------------------
------+
```

ONIE auswählen: **Betriebssystem installieren.**

6. Der ONIE-Installer-Erkennungsprozess wird ausgeführt und sucht nach der automatischen Installation. Drücken Sie die **Eingabetaste**, um den Vorgang vorübergehend zu unterbrechen.
7. Wenn der Ermittlungsprozess abgeschlossen ist:

```
ONIE:/ # onie-stop
discover: installer mode detected.
Stopping: discover...start-stop-daemon: warning: killing process
427:
No such process done.
```

8. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und das Standardgateway:

```
ifconfig eth0
```

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff
ONIE:/ #
ONIE:/ # ifconfig eth0 10.228.140.27 netmask 255.255.248.0
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet HWaddr B8:CE:F6:5E:05:E6
       inet addr:10.228.140.27 Bcast:10.228.143.255
Mask:255.255.248.0
       inet6 addr: fd20:8b1e:b255:822b:bace:f6ff:fe5e:5e6/64
Scope:Global
       inet6 addr: fe80::bace:f6ff:fe5e:5e6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
       RX packets:18813 errors:0 dropped:1418 overruns:0 frame:0
       TX packets:491 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:1339596 (1.2 MiB) TX bytes:49379 (48.2 KiB)
       Memory:dfc00000-dfc1ffff
ONIE:/ # route add default gw 10.228.136.1
ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface

default         10.228.136.1    0.0.0.0         UG    0      0
0   eth0
10.228.136.1    *               255.255.248.0   U     0      0
0   eth0
```

9. Installieren Sie Cumulus Linux 5.4:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-5.4-mlx-
amd64.bin
```

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-5.4-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-5.4-
mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

10. Nach Abschluss der Installation melden Sie sich am Switch an.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

11. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 13:37:36     system uptime
timezone            Etc/UTC              system time zone
```

12. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

    ```
    sudo adduser --ingroup netedit admin
    ```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Fügen Sie dem Administrator weitere Benutzergruppen hinzu, auf die er zugreifen kann. `nv` Befehle:

```
cumulus@cumulus:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user `admin' to group `nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Wie geht es weiter?

Nach der Installation von Cumulus Linux im ONIE-Modus können Sie"Installieren Sie das Skript der Referenzkonfigurationsdatei (RCF)." Die

Cumulus Linux-Versionen aktualisieren

Führen Sie die folgenden Schritte aus, um Ihre Cumulus Linux-Version bei Bedarf zu aktualisieren.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Linux-Kenntnisse auf mittlerem Niveau.
- Kenntnisse in grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren ist vorinstalliert, darunter `vi` Und `nano` Die
- Zugriff auf eine Linux- oder UNIX-Shell. Wenn Sie Windows verwenden, nutzen Sie eine Linux-Umgebung als Befehlszeilentool für die Interaktion mit Cumulus Linux.
- Die Baudratenanforderung für den seriellen Konsolen-Switch für den Konsolenzugriff des NVIDIA SN2100-Switches ist wie folgt auf 115200 eingestellt:
  - 115200 Baud
  - 8 Datenbits
  - 1 Stoppbit
  - Parität: keine
  - Flusssteuerung: keine

Informationen zu diesem Vorgang

Beachten Sie Folgendes:

> Bei jedem Upgrade von Cumulus Linux wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut. Ihre bestehende Konfiguration wird gelöscht. Sie müssen Ihre Switch-Konfiguration speichern und protokollieren, bevor Sie Cumulus Linux aktualisieren.

Das Standardpasswort für das Cumulus-Benutzerkonto lautet **cumulus**. Beim ersten Anmelden bei Cumulus Linux müssen Sie dieses Standardpasswort ändern. Vor der Installation eines neuen Images müssen Sie alle Automatisierungsskripte aktualisieren. Cumulus Linux bietet Befehlszeilenoptionen, um das Standardpasswort während des Installationsprozesses automatisch zu ändern.

Sehen "Installation eines neuen Cumulus Linux-Images" für weitere Informationen.

Beispiel 3. Schritte

Cumulus Linux 4.4.x zu Cumulus Linux 5.4.0

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem Cumulus Linux und RCF gehostet werden.
3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

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 -role cluster
      ```

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

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

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

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

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

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

6. Überprüfen Sie die aktuelle Cumulus Linux-Version und die angeschlossenen Ports:

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox

cumulus@cumulus:mgmt:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  ----------------------
--------------------
.
.
UP     swp1    100G  9216   Trunk/L2    node1 (e5b)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2    node2 (e5b)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2    SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2    SHFFG1826000102 (e0b)
Master: bridge(UP))
.
.
```

7. Laden Sie das Cumulux Linux 5.4.0-Image herunter:

```
cumulus@cumulus:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Starten Sie den Switch neu:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

9. Ändern Sie das Passwort:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
           operational    applied
---------- -------------- ----------
hostname   cumulus        cumulus
build      Cumulus Linux 5.4.0
uptime     14:07:08
timezone   Etc/UTC
```

11. Ändern Sie den Hostnamen:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Melden Sie sich vom Switch ab und wieder an, um den aktualisierten Switch-Namen in der Eingabeaufforderung zu sehen:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)


ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. IP-Adresse festlegen:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

15. Fügen Sie dem Administrator weitere Benutzergruppen hinzu, auf die er zugreifen kann. `nv` Befehle:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user `admin' to group `nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Cumulus Linux 5.x zu Cumulus Linux 5.4.0

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem Cumulus Linux und RCF gehostet werden.
3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

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 -role cluster
      ```

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

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

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

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

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

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

6. Überprüfen Sie die aktuelle Cumulus Linux-Version und die angeschlossenen Ports:

```
cumulus@sw1:mgmt:~$ nv show system
                    operational          applied
------------------- -------------------- -----------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0
uptime              6 days, 8:37:36
timezone            Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------- ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01                e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                      swp15
swp
+ swp16      9216 100G    up sw2                      swp16
swp
```

7. Laden Sie das Cumulux Linux 5.4.0-Image herunter:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Starten Sie den Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Ändern Sie das Passwort:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational    applied
-------------- ----------------
hostname       cumulus cumulus
build          Cumulus Linux 5.4.0
uptime         14:07:08
timezone       Etc/UTC
```

11. Ändern Sie den Hostnamen:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Melden Sie sich vom Switch ab und wieder an, um den aktualisierten Switch-Namen in der Eingabeaufforderung zu sehen:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)


ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. IP-Adresse festlegen:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

    ```
    sudo adduser --ingroup netedit admin
    ```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

15. Fügen Sie dem Administrator weitere Benutzergruppen hinzu, auf die er zugreifen kann. `nv` Befehle:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user `admin' to group `nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Cumulus Linux 5.4.0 bis Cumulus Linux 5.11.0

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem Cumulus Linux und RCF gehostet werden.
3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

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 -role cluster
      ```

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

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

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

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

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

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

6. Überprüfen Sie die aktuelle Cumulus Linux-Version und die angeschlossenen Ports:

```
cumulus@sw1:mgmt:~$ nv show system
                    operational          applied
------------------- -------------------- -----------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0
uptime              6 days, 8:37:36
timezone            Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------- ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01                e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                      swp15
swp
+ swp16      9216 100G    up sw2                      swp16
swp
```

7. Laden Sie das Cumulux Linux 5.11.0-Image herunter:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.11.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.11.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.
.
.
.
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Starten Sie den Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

9. Ändern Sie das Passwort:

```
cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

10. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational    applied
-------------- ----------------
hostname       cumulus cumulus
build          Cumulus Linux 5.11.0
uptime         14:07:08
timezone       Etc/UTC
```

11. Ändern Sie den Hostnamen:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Melden Sie sich vom Switch ab und wieder an, um den aktualisierten Switch-Namen in der Eingabeaufforderung zu sehen:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)


ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. IP-Adresse festlegen:

```
cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

Wie geht es weiter?

Nach dem Upgrade Ihrer Cumulus Linux-Version können Sie"Installieren oder aktualisieren Sie das RCF-Skript" Die

Installieren oder aktualisieren Sie das Skript der Referenzkonfigurationsdatei (RCF).

Folgen Sie dieser Vorgehensweise, um das RCF-Skript zu installieren oder zu aktualisieren.

Bevor Sie beginnen

Vor der Installation oder Aktualisierung des RCF-Skripts stellen Sie sicher, dass Folgendes auf dem Switch verfügbar ist:

- Cumulus Linux ist installiert. Siehe die "Hardware Universe" für unterstützte Versionen.
- IP-Adresse, Subnetzmaske und Standardgateway werden per DHCP definiert oder manuell konfiguriert.

Sie müssen im RCF (zusätzlich zum Administratorbenutzer) einen Benutzer angeben, der speziell für die Protokollerfassung verwendet werden soll.

Kundenkonfigurationen

Folgende Referenzkonfigurationskategorien stehen zur Verfügung:

Cluster	Bei Ports, die für 4x10GbE-Breakout konfiguriert sind, ist ein Port für 4x25GbE-Breakout und die anderen Ports für 40/100GbE konfiguriert. Unterstützt gemeinsam genutzten Cluster-/HA-Verkehr auf Ports für Knoten, die gemeinsam genutzte Cluster-/HA-Ports verwenden. Die Plattformtabelle finden Sie im Knowledge-Base-Artikel. "Welche AFF, ASA und FAS -Plattformen verwenden gemeinsam genutzte Cluster- und HA-Ethernet-Ports?" Die Alle Ports können auch als dedizierte Cluster-Ports verwendet werden.
Storage	Alle Ports sind für 100GbE NVMe-Speicherverbindungen konfiguriert.

Aktuelle RCF-Skriptversionen

Für Cluster- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. RCFs herunterladen von "NVIDIA SN2100 Software-Download" Seite. Die Vorgehensweise ist für alle Fälle gleich.

- Cluster: **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP**
- Speicher: **MSN2100-RCF-v1.*x*-Speicher**

Zu den Beispielen

Das folgende Beispielverfahren zeigt, wie das RCF-Skript für Cluster-Switches heruntergeladen und angewendet wird.

Beispielausgabe des Befehls verwendet die Switch-Management-IP-Adresse 10.233.204.71, die Netzmaske 255.255.254.0 und das Standardgateway 10.233.204.1.

Beispiel 4. Schritte

Cumulus Linux 4.4.3

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung zum Server, auf dem Cumulus Linux und RCF gehostet werden.
3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

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 -role cluster
      ```

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

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

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

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

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

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

- Wenn Sie Ihr RCF aktualisieren, müssen Sie für diesen Schritt die automatische Wiederherstellung deaktivieren.
- Wenn Sie Ihre Cumulus Linux-Version gerade erst aktualisiert haben, brauchen Sie die automatische Wiederherstellung für diesen Schritt nicht zu deaktivieren, da sie bereits deaktiviert ist.

1. Die verfügbaren Schnittstellen des SN2100-Switches anzeigen:

```
admin@sw1:mgmt:~$ net show interface all

State  Name    Spd  MTU    Mode          LLDP                 Summary
-----  -----   ---  -----  -----------   ------------------
--------------
...
...
ADMDN  swp1    N/A  9216   NotConfigured
ADMDN  swp2    N/A  9216   NotConfigured
ADMDN  swp3    N/A  9216   NotConfigured
ADMDN  swp4    N/A  9216   NotConfigured
ADMDN  swp5    N/A  9216   NotConfigured
ADMDN  swp6    N/A  9216   NotConfigured
ADMDN  swp7    N/A  9216   NotConfigured
ADMDN  swp8    N/A  9216   NotConfigured
ADMDN  swp9    N/A  9216   NotConfigured
ADMDN  swp10   N/A  9216   NotConfigured
ADMDN  swp11   N/A  9216   NotConfigured
ADMDN  swp12   N/A  9216   NotConfigured
ADMDN  swp13   N/A  9216   NotConfigured
ADMDN  swp14   N/A  9216   NotConfigured
ADMDN  swp15   N/A  9216   NotConfigured
ADMDN  swp16   N/A  9216   NotConfigured
```

2. Kopiere das RCF-Python-Skript auf den Switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP         100% 8607
111.2KB/s         00:00
```

Während `scp` Wird im Beispiel verwendet, können Sie Ihre bevorzugte Methode der Dateiübertragung nutzen, zum Beispiel SFTP, HTTPS oder FTP.

3. Wenden Sie das RCF-Python-Skript **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP** an.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Das RCF-Skript führt die im obigen Beispiel aufgeführten Schritte aus.

> Im obigen Schritt 3 **Aktualisieren der MOTD-Datei** wird der Befehl verwendet. `cat /etc/motd` wird ausgeführt. Dies ermöglicht es Ihnen, den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner zu überprüfen.

> Bei Problemen mit RCF-Python-Skripten, die nicht behoben werden können, wenden Sie sich bitte an [Kontaktinformationen einfügen]. "NetApp Support" um Unterstützung zu erhalten.

4. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
5. Überprüfen Sie die Konfiguration nach dem Neustart:

```
admin@sw1:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
...
...
DN     swp1s0    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp1s1    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp1s2    N/A   9216   Trunk/L2                      Master:
```

```
bridge(UP)
DN     swp1s3    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s0    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s1    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s2    N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp2s3    N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp3      100G  9216   Trunk/L2                    Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                    Master:
bridge(UP)
DN     swp5      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp6      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp7      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp8      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp9      N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp10     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp11     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp12     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp13     N/A   9216   Trunk/L2                    Master:
bridge(UP)
DN     swp14     N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp15     N/A   9216   BondMember                  Master:
bond_15_16(UP)
UP     swp16     N/A   9216   BondMember                  Master:
bond_15_16(UP)
...
...

admin@sw1:mgmt:~$ net show roce config
RoCE mode.......... lossless
Congestion Control:
  Enabled SPs.... 0 2 5
```

```
  Mode........... ECN
  Min Threshold.. 150 KB
  Max Threshold.. 1500 KB
PFC:
  Status......... enabled
  Enabled SPs.... 2 5
  Interfaces......... swp10-16,swp1s0-3,swp2s0-3,swp3-9

DSCP                     802.1p  switch-priority
-----------------------  ------  ---------------
0 1 2 3 4 5 6 7               0                0
8 9 10 11 12 13 14 15         1                1
16 17 18 19 20 21 22 23       2                2
24 25 26 27 28 29 30 31       3                3
32 33 34 35 36 37 38 39       4                4
40 41 42 43 44 45 46 47       5                5
48 49 50 51 52 53 54 55       6                6
56 57 58 59 60 61 62 63       7                7

switch-priority  TC  ETS
---------------  --  --------
0 1 3 4 6 7       0  DWRR 28%
2                 2  DWRR 28%
5                 5  DWRR 43%
```

6. Überprüfen Sie die Informationen für den Transceiver in der Schnittstelle:

```
admin@sw1:mgmt:~$ net show interface pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor SN
    Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp3       0x11 (QSFP28)  Amphenol     112-00574
APF20379253516  B0
swp4       0x11 (QSFP28)  AVAGO        332-00440        AF1815GU05Z
    A0
swp15      0x11 (QSFP28)  Amphenol     112-00573
APF21109348001  B0
swp16      0x11 (QSFP28)  Amphenol     112-00573
APF21109347895  B0
```

7. Überprüfen Sie, ob jeder Knoten eine Verbindung zu jedem Switch hat:

```
admin@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost              RemotePort
---------  -----  ----------  ----------------------  -----------
swp3       100G   Trunk/L2    sw1                     e3a
swp4       100G   Trunk/L2    sw2                     e3b
swp15      100G   BondMember  sw13                    swp15
swp16      100G   BondMember  sw14                    swp16
```

8. 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:

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

   b. Überprüfen Sie den Zustand des Switches vom Cluster aus (dabei wird möglicherweise Switch sw2 nicht angezeigt, da LIFs nicht auf e0d liegen).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

9. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster show
   ```

10. Wiederholen Sie die Schritte 1 bis 14 am zweiten Schalter.
11. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung zum Server, auf dem Cumulus Linux und RCF gehostet werden.
3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

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 -role cluster
      ```

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

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

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

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

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

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

- Wenn Sie Ihr RCF aktualisieren, müssen Sie für diesen Schritt die automatische Wiederherstellung deaktivieren.
- Wenn Sie Ihre Cumulus Linux-Version gerade erst aktualisiert haben, brauchen Sie die automatische Wiederherstellung für diesen Schritt nicht zu deaktivieren, da sie bereits deaktiviert ist.

1. Die verfügbaren Schnittstellen des SN2100-Switches anzeigen:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------ ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1           Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp
```

2. Kopiere das RCF-Python-Skript auf den Switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s         00:00
```

> Während `scp` Wird im Beispiel verwendet, können Sie Ihre bevorzugte Methode der Dateiübertragung nutzen, zum Beispiel SFTP, HTTPS oder FTP.

3. Wenden Sie das RCF-Python-Skript **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP** an.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Das RCF-Skript führt die im obigen Beispiel aufgeführten Schritte aus.

> Im obigen Schritt 3 **Aktualisieren der MOTD-Datei** wird der Befehl verwendet. `cat /etc/issue.net` wird ausgeführt. Dies ermöglicht es Ihnen, den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner zu überprüfen.

Beispiel:

```
admin@sw1:mgmt:~$ cat /etc/issue.net
**********************************************************************
**********
*
* NetApp Reference Configuration File (RCF)
* Switch       : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1      : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2      : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14  : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16 : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
**********************************************************************
**********
```

Bei Problemen mit RCF-Python-Skripten, die nicht behoben werden können, wenden Sie sich bitte an [Kontaktinformationen einfügen]. "NetApp Support" um Unterstützung zu erhalten.

4. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
5. Überprüfen Sie die Konfiguration nach dem Neustart:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------- ----- ----- ----- ------------------- ------------
```

```
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                   operational  applied   description
-----------------  -----------  ---------
----------------------------------------
enable             on                     Turn feature 'on' or
'off'. This feature is disabled by default.
mode               lossless     lossless  Roce Mode
congestion-control
  congestion-mode   ECN,RED                Congestion config mode
  enabled-tc        0,2,5                  Congestion config enabled
Traffic Class
  max-threshold     195.31 KB              Congestion config max-
threshold
  min-threshold     39.06 KB               Congestion config min-
threshold
  probability       100
lldp-app-tlv
  priority          3                      switch-priority of roce
  protocol-id       4791                   L4 port number
  selector          UDP                    L4 protocol
pfc
  pfc-priority      2, 5                   switch-prio on which PFC
is enabled
  rx-enabled        enabled                PFC Rx Enabled status
  tx-enabled        enabled                PFC Tx Enabled status
```

```
trust
  trust-mode        pcp,dscp                Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations
========================================
        pcp  dscp                     switch-prio
    --  ---  -----------------------  -----------
    0   0    0,1,2,3,4,5,6,7          0
    1   1    8,9,10,11,12,13,14,15    1
    2   2    16,17,18,19,20,21,22,23  2
    3   3    24,25,26,27,28,29,30,31  3
    4   4    32,33,34,35,36,37,38,39  4
    5   5    40,41,42,43,44,45,46,47  5
    6   6    48,49,50,51,52,53,54,55  6
    7   7    56,57,58,59,60,61,62,63  7

RoCE SP->TC mapping and ETS configurations
==========================================
        switch-prio  traffic-class  scheduler-weight
    --  -----------  -------------  ----------------
    0   0            0              DWRR-28%
    1   1            0              DWRR-28%
    2   2            2              DWRR-28%
    3   3            0              DWRR-28%
    4   4            0              DWRR-28%
    5   5            5              DWRR-43%
    6   6            0              DWRR-28%
    7   7            0              DWRR-28%

RoCE pool config
================
        name                    mode     size  switch-priorities
traffic-class
    --  ----------------------  -------  ----  -----------------
-------------
    0   lossy-default-ingress   Dynamic  50%   0,1,3,4,6,7        -
    1   roce-reserved-ingress   Dynamic  50%   2,5                -
    2   lossy-default-egress    Dynamic  50%   -                  0
    3   roce-reserved-egress    Dynamic  inf   -                  2,5

Exception List
==============
        description
    --
---------------------------------------------------------------------
```

```
---…
    1   RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
    2   Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
    3   Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
    4   Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
    5   Congestion Config max-threshold Mismatch.Expected max-
threshold:
        1500000.
    6   Scheduler config mismatch for traffic-class mapped to
switch-prio0.
        Expected scheduler-weight: DWRR-50%.
    7   Scheduler config mismatch for traffic-class mapped to
switch-prio1.
        Expected scheduler-weight: DWRR-50%.
    8   Scheduler config mismatch for traffic-class mapped to
switch-prio2.
        Expected scheduler-weight: DWRR-50%.
    9   Scheduler config mismatch for traffic-class mapped to
switch-prio3.
        Expected scheduler-weight: DWRR-50%.
    10  Scheduler config mismatch for traffic-class mapped to
switch-prio4.
        Expected scheduler-weight: DWRR-50%.
    11  Scheduler config mismatch for traffic-class mapped to
switch-prio5.
        Expected scheduler-weight: DWRR-50%.
    12  Scheduler config mismatch for traffic-class mapped to
switch-prio6.
        Expected scheduler-weight: strict-priority.
    13  Scheduler config mismatch for traffic-class mapped to
switch-prio7.
        Expected scheduler-weight: DWRR-50%.
    14  Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
    15  Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
    16  Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
    17  Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
    18  Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
    19  Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

```
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

```
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

Die aufgeführten Ausnahmen haben keinen Einfluss auf die Leistung und können getrost ignoriert werden.

6. Überprüfen Sie die Informationen für den Transceiver in der Schnittstelle:

```
admin@sw1:mgmt:~$ nv show interface --view=pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor
SN       Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp1s0     0x00 None
swp1s1     0x00 None
swp1s2     0x00 None
swp1s3     0x00 None
swp2s0     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s1     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s2     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s3     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp3       0x00 None
swp4       0x00 None
swp5       0x00 None
swp6       0x00 None
.
.
.
swp15      0x11 (QSFP28)  Amphenol     112-00595
APF20279210117  B0
swp16      0x11 (QSFP28)  Amphenol     112-00595
APF20279210166  B0
```

7. Überprüfen Sie, ob jeder Knoten eine Verbindung zu jedem Switch hat:

```
admin@sw1:mgmt:~$ nv show interface --view=lldp

LocalPort  Speed  Mode        RemoteHost                RemotePort
---------  -----  ----------  ------------------------  -----------
eth0       100M   Mgmt        mgmt-sw1                  Eth110/1/29
swp2s1     25G    Trunk/L2    node1                     e0a
swp15      100G   BondMember  sw2                       swp15
swp16      100G   BondMember  sw2                       swp16
```

8. 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:

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

   b. Überprüfen Sie den Zustand des Switches vom Cluster aus (dabei wird möglicherweise Switch sw2 nicht angezeigt, da LIFs nicht auf e0d liegen).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

9. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster show
   ```

10. Wiederholen Sie die Schritte 1 bis 14 am zweiten Schalter.
11. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung zum Server, auf dem Cumulus Linux und RCF gehostet werden.
3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

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 -role cluster
      ```

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

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

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

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

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

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

- Wenn Sie Ihr RCF aktualisieren, müssen Sie für diesen Schritt die automatische Wiederherstellung deaktivieren.
- Wenn Sie Ihre Cumulus Linux-Version gerade erst aktualisiert haben, brauchen Sie die automatische Wiederherstellung für diesen Schritt nicht zu deaktivieren, da sie bereits deaktiviert ist.

1. Die verfügbaren Schnittstellen des SN2100-Switches anzeigen:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------ ----- ----- ----- ------------------ ------------
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1           Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp
```

2. Kopiere das RCF-Python-Skript auf den Switch.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100% 8607
111.2KB/s         00:00
```

> Obwohl `scp` Wird im Beispiel verwendet, können Sie Ihre bevorzugte Methode der Dateiübertragung nutzen, zum Beispiel SFTP, HTTPS oder FTP.

3. Wenden Sie das RCF-Python-Skript **MSN2100-RCF-v1.*x*-Cluster-HA-Breakout-LLDP** an.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[sudo] password for cumulus:
.
.
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Das RCF-Skript führt die im obigen Beispiel aufgeführten Schritte aus.

> Im oben genannten Schritt 3 **Aktualisieren der MOTD-Datei** wird der Befehl `cat /etc/issue.net` ausgeführt. Dies ermöglicht es Ihnen, den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner zu überprüfen.

Beispiel:

```
admin@sw1:mgmt:~$ cat /etc/issue.net
**********************************************************************
**********
*
* NetApp Reference Configuration File (RCF)
* Switch       : Mellanox MSN2100
* Filename     : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version      : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1      : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2      : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14  : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16 : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
**********************************************************************
**********
```

Bei Problemen mit RCF-Python-Skripten, die nicht behoben werden können, wenden Sie sich bitte an [Kontaktinformationen einfügen]. "NetApp Support" um Unterstützung zu erhalten.

4. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
5. Überprüfen Sie die Konfiguration nach dem Neustart:

```
admin@sw1:mgmt:~$ nv show interface
Interface     MTU   Speed State Remote Host         Remote Port-
Type      Summary
------------- ----- ----- ----- ------------------ ------------
```

```
--------- -------------
+ cluster_isl 9216  200G  up
bond
+ eth0        1500  100M  up    mgmt-sw1            Eth105/1/14
eth       IP Address: 10.231.80 206/22
  eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo          65536       up
loopback  IP Address: 127.0.0.1/8
  lo
IP Address: ::1/128
+ swp1s0      9216 10G    up cluster01               e0b
swp
.
.
.
+ swp15      9216 100G    up sw2                     swp15
swp
+ swp16      9216 100G    up sw2                     swp16
swp

admin@sw1:mgmt:~$ nv show qos roce
                   operational  applied   description
-----------------  -----------  ---------
----------------------------------------
enable             on                     Turn feature 'on' or
'off'. This feature is disabled by default.
mode               lossless     lossless  Roce Mode
congestion-control
  congestion-mode   ECN,RED                Congestion config mode
  enabled-tc        0,2,5                  Congestion config enabled
Traffic Class
  max-threshold     195.31 KB              Congestion config max-
threshold
  min-threshold     39.06 KB               Congestion config min-
threshold
  probability       100
lldp-app-tlv
  priority          3                      switch-priority of roce
  protocol-id       4791                   L4 port number
  selector          UDP                    L4 protocol
pfc
  pfc-priority      2, 5                   switch-prio on which PFC
is enabled
  rx-enabled        enabled                PFC Rx Enabled status
  tx-enabled        enabled                PFC Tx Enabled status
```

```
trust
  trust-mode        pcp,dscp               Trust Setting on the port
for packet classification

RoCE PCP/DSCP->SP mapping configurations
========================================
        pcp  dscp                    switch-prio
    --  ---  ----------------------  -----------
    0   0    0,1,2,3,4,5,6,7         0
    1   1    8,9,10,11,12,13,14,15   1
    2   2    16,17,18,19,20,21,22,23 2
    3   3    24,25,26,27,28,29,30,31 3
    4   4    32,33,34,35,36,37,38,39 4
    5   5    40,41,42,43,44,45,46,47 5
    6   6    48,49,50,51,52,53,54,55 6
    7   7    56,57,58,59,60,61,62,63 7

RoCE SP->TC mapping and ETS configurations
==========================================
        switch-prio  traffic-class  scheduler-weight
    --  -----------  -------------  ----------------
    0   0            0              DWRR-28%
    1   1            0              DWRR-28%
    2   2            2              DWRR-28%
    3   3            0              DWRR-28%
    4   4            0              DWRR-28%
    5   5            5              DWRR-43%
    6   6            0              DWRR-28%
    7   7            0              DWRR-28%

RoCE pool config
================
        name                    mode     size  switch-priorities
traffic-class
    --  ----------------------  -------  ----  -----------------
-------------
    0   lossy-default-ingress   Dynamic  50%   0,1,3,4,6,7        -
    1   roce-reserved-ingress   Dynamic  50%   2,5                -
    2   lossy-default-egress    Dynamic  50%   -                  0
    3   roce-reserved-egress    Dynamic  inf   -                  2,5

Exception List
==============
        description
    --
---------------------------------------------------------------------
```

```
---…
    1   RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
    2   Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
    3   Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
    4   Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
    5   Congestion Config max-threshold Mismatch.Expected max-
threshold:
        1500000.
    6   Scheduler config mismatch for traffic-class mapped to
switch-prio0.
        Expected scheduler-weight: DWRR-50%.
    7   Scheduler config mismatch for traffic-class mapped to
switch-prio1.
        Expected scheduler-weight: DWRR-50%.
    8   Scheduler config mismatch for traffic-class mapped to
switch-prio2.
        Expected scheduler-weight: DWRR-50%.
    9   Scheduler config mismatch for traffic-class mapped to
switch-prio3.
        Expected scheduler-weight: DWRR-50%.
    10  Scheduler config mismatch for traffic-class mapped to
switch-prio4.
        Expected scheduler-weight: DWRR-50%.
    11  Scheduler config mismatch for traffic-class mapped to
switch-prio5.
        Expected scheduler-weight: DWRR-50%.
    12  Scheduler config mismatch for traffic-class mapped to
switch-prio6.
        Expected scheduler-weight: strict-priority.
    13  Scheduler config mismatch for traffic-class mapped to
switch-prio7.
        Expected scheduler-weight: DWRR-50%.
    14  Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
    15  Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
    16  Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
    17  Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
    18  Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
    19  Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

```
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```
```
Incomplete Command: set interface swp3-16 link fast-linkupp3-16 link
fast-linkup
```

> Die aufgeführten Ausnahmen haben keinen Einfluss auf die Leistung und können getrost ignoriert werden.

6. Überprüfen Sie die Informationen für den Transceiver in der Schnittstelle:

```
admin@sw1:mgmt:~$ nv show platform transceiver
Interface  Identifier     Vendor Name  Vendor PN        Vendor
SN       Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp1s0     0x00 None
swp1s1     0x00 None
swp1s2     0x00 None
swp1s3     0x00 None
swp2s0     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s1     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s2     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp2s3     0x11 (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ     00
swp3       0x00 None
swp4       0x00 None
swp5       0x00 None
swp6       0x00 None
.
.
.
swp15      0x11 (QSFP28)  Amphenol     112-00595
APF20279210117  B0
swp16      0x11 (QSFP28)  Amphenol     112-00595
APF20279210166  B0
```

7. Überprüfen Sie, ob jeder Knoten eine Verbindung zu jedem Switch hat:

```
admin@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost                RemotePort
---------  -----  ----------  ------------------------  -----------
eth0       100M   Mgmt        mgmt-sw1                  Eth110/1/29
swp2s1     25G    Trunk/L2    node1                     e0a
swp15      100G   BondMember  sw2                       swp15
swp16      100G   BondMember  sw2                       swp16
```

8. 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:

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

   b. Überprüfen Sie den Zustand des Switches vom Cluster aus (dabei wird möglicherweise Switch sw2 nicht angezeigt, da LIFs nicht auf e0d liegen).

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 5.4.0 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

9. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster show
   ```

10. Wiederholen Sie die Schritte 1 bis 14 am zweiten Schalter.
11. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

Wie geht es weiter?

Nach der Installation des RCF können Sie "Installieren Sie die CSHM-Datei"Die

Installieren Sie die Konfigurationsdatei für den Ethernet Switch Health Monitor.

Um die Zustandsüberwachung von Ethernet-Switches auf NVIDIA Ethernet-Switches zu konfigurieren, gehen Sie wie folgt vor.

Diese Anweisungen gelten, wenn die NVIDIA -Switches X190006-PE und X190006-PI nicht ordnungsgemäß erkannt werden. Dies kann durch Ausführen des Befehls überprüft werden. `system switch ethernet show` und prüfen, ob für Ihr Modell **ANDERE** angezeigt wird. Um Ihr NVIDIA Switch-Modell zu identifizieren, ermitteln Sie die Teilenummer mit dem Befehl `nv show platform hardware` für NVIDIA CL 5.8 und früher oder `nv show platform` für spätere Versionen.

> Diese Schritte werden auch empfohlen, wenn Sie möchten, dass die Zustandsüberwachung und die Protokollerfassung bei Verwendung von NVIDIA CL 5.11.x mit den folgenden ONTAP Versionen wie vorgesehen funktionieren. Auch wenn die Gesundheitsüberwachung und die Protokollerfassung möglicherweise auch ohne diese Schritte funktionieren, stellt deren Befolgung sicher, dass alles ordnungsgemäß funktioniert.
>
> - Patch-Versionen 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 und spätere Versionen

Bevor Sie beginnen

- Stellen Sie sicher, dass der ONTAP -Cluster betriebsbereit ist.
- Aktivieren Sie SSH auf dem Switch, um alle in CSHM verfügbaren Funktionen nutzen zu können.
- Räumen Sie die `/mroot/etc/cshm_nod/nod_sign/` Verzeichnis auf allen Knoten:

  a. Geben Sie die NodeShell ein:

  ```
  system node run -node <name>
  ```

  b. Änderung zu erweiterten Berechtigungen:

  ```
  priv set advanced
  ```

  c. Listen Sie die Konfigurationsdateien im folgenden Verzeichnis auf: `/etc/cshm_nod/nod_sign` Verzeichnis. Wenn das Verzeichnis existiert und Konfigurationsdateien enthält, werden die Dateinamen aufgelistet.

  ```
  ls /etc/cshm_nod/nod_sign
  ```

  d. Löschen Sie alle Konfigurationsdateien, die zu Ihren angeschlossenen Switch-Modellen gehören.

  Wenn Sie sich nicht sicher sind, entfernen Sie alle Konfigurationsdateien für die oben aufgeführten unterstützten Modelle und laden Sie anschließend die neuesten Konfigurationsdateien für dieselben Modelle herunter und installieren Sie diese.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

a. Vergewissern Sie sich, dass die gelöschten Konfigurationsdateien nicht mehr im Verzeichnis vorhanden sind:

```
ls /etc/cshm_nod/nod_sign
```

Schritte

1. Laden Sie die Konfigurations-ZIP-Datei für den Ethernet-Switch-Integritätsmonitor entsprechend der zugehörigen ONTAP Version herunter. Diese Datei ist verfügbar unter "NVIDIA Ethernet-Switches" Seite.
   a. Auf der Downloadseite der NVIDIA SN2100 Software wählen Sie **Nvidia CSHM-Datei** aus.
   b. Auf der Seite „Vorsicht/Unbedingt lesen“ das Kontrollkästchen aktivieren, um zuzustimmen.
   c. Auf der Seite „Endbenutzer-Lizenzvereinbarung“ das Kontrollkästchen aktivieren, um zuzustimmen, und auf **Akzeptieren & Fortfahren** klicken.
   d. Auf der Seite „Nvidia CSHM File - Download“ wählen Sie die entsprechende Konfigurationsdatei aus. Folgende Dateien sind verfügbar:

ONTAP 9.15.1 und höher

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 bis 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Laden Sie die entsprechende ZIP-Datei auf Ihren internen Webserver hoch.
2. Die Einstellungen für den erweiterten Modus können Sie von einem der ONTAP -Systeme im Cluster aus aufrufen.

```
set -privilege advanced
```

3. Führen Sie den Befehl „switch health monitor configure“ aus.

```
cluster1::> system switch ethernet configure-health-monitor
```

4. Vergewissern Sie sich, dass die Befehlsausgabe für Ihre ONTAP Version mit folgendem Text endet:

ONTAP 9.15.1 und höher

Die Zustandsüberwachung des Ethernet-Switches hat die Konfigurationsdatei installiert.

ONTAP 9.11.1 bis 9.14.1

SHM hat die Konfigurationsdatei installiert.

ONTAP 9.10.1

Das heruntergeladene CSHM-Paket wurde erfolgreich verarbeitet.

Im Fehlerfall wenden Sie sich bitte an den NetApp Support.

1. Warten Sie bis zum Doppelten des Abfrageintervalls des Ethernet-Switch-Integritätsmonitors, das durch Ausführen von `system switch ethernet polling-interval show` , bevor der nächste Schritt ausgeführt wird.
2. Führen Sie den Befehl aus `system switch ethernet configure-health-monitor show` Stellen Sie im ONTAP -System sicher, dass die Cluster-Switches erkannt werden, wobei das überwachte Feld auf **True** gesetzt ist und das Feld für die Seriennummer nicht **Unknown** anzeigt.

```
cluster1::> system switch ethernet configure-health-monitor show
```

Falls Ihr Modell nach Anwendung der Konfigurationsdatei immer noch **ANDERE** anzeigt, wenden Sie sich bitte an den NetApp -Support.

Siehe die "System-Switch-Ethernet-Konfigurations-Health-Monitor" Befehl für weitere Details.

Wie geht es weiter?

Nach der Installation der CSHM-Datei können Sie"Konfigurieren der Switch-Integritätsüberwachung" Die

Setzen Sie den SN2100-Cluster-Switch auf die Werkseinstellungen zurück

So setzen Sie den SN2100-Cluster-Switch auf die Werkseinstellungen zurück:

- Für Cumulus Linux 5.10 und früher wenden Sie das Cumulus-Image an.
- Für Cumulus Linux 5.11 und höher verwenden Sie die `nv action reset system factory-default` Befehl.

Informationen zu diesem Vorgang

- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Sie müssen über das Root-Passwort verfügen, um per Sudo auf die Befehle zugreifen zu können.

Weitere Informationen zur Installation von Cumulus Linux finden Sie unter"Softwareinstallations-Workflow für NVIDIA SN2100-Switches" Die

Beispiel 5. Schritte

Cumulus Linux 5.10 und früher

1. Laden Sie über die Cumulus-Konsole die Installation der Switch-Software mit dem Befehl herunter und stellen Sie sie in die Warteschlange. `onie-install -a -i` gefolgt vom Dateipfad zur Switch-Software, zum Beispiel:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie aufgefordert werden, die Installation zu bestätigen, nachdem das Image heruntergeladen und überprüft wurde.
3. Starten Sie den Switch neu, um die neue Software zu installieren.

   `sudo reboot`

```
cumulus@sw1:mgmt:~$ sudo reboot
```

> Der Switch startet neu und beginnt mit der Installation der Switch-Software, was einige Zeit in Anspruch nimmt. Nach Abschluss der Installation startet der Switch neu und verbleibt im aktuellen Zustand. `log-in` prompt.

Cumulus Linux 5.11 und höher

1. Um den Switch auf die Werkseinstellungen zurückzusetzen und alle Konfigurations-, System- und Protokolldateien zu entfernen, führen Sie Folgendes aus:

   `nv action reset system factory-default`

   Beispiel:

```
cumulus@switch:~$ nv action reset system factory-default

This operation will reset the system configuration, delete the log
files and reboot the switch.
Type [y] continue.
Type [n] to abort.
Do you want to continue? [y/n] y
```

Siehe NVIDIA "Werksreset" Weitere Einzelheiten finden Sie in der Dokumentation.

Was kommt als nächstes

Nachdem Sie Ihre Schalter zurückgesetzt haben, können Sie"neu konfigurieren" sie nach Bedarf.

Migrieren Sie die Schalter

Migration von CN1610-Cluster-Switches zu NVIDIA SN2100-Cluster-Switches

Sie können NetApp CN1610 Cluster-Switches für einen ONTAP Cluster auf NVIDIA SN2100 Cluster-Switches migrieren. Dies ist ein unterbrechungsfreies Verfahren.

Überprüfungsanforderungen

Beim Austausch von NetApp CN1610 Cluster-Switches durch NVIDIA SN2100 Cluster-Switches müssen Sie bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen beachten. Sehen"Übersicht über Installation und Konfiguration von NVIDIA SN2100-Switches" .

Unterstützte Schalter

Folgende Cluster-Switches werden unterstützt:

- NetApp CN1610
- NVIDIA SN2100

Einzelheiten zu den unterstützten Ports und deren Konfigurationen finden Sie unter "Hardware Universe" Die

Bevor Sie beginnen

Bitte prüfen Sie, ob Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Der bestehende Cluster ist korrekt eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die NVIDIA SN2100 Cluster-Switches sind konfiguriert und arbeiten unter der korrekten Version von Cumulus Linux, auf der die Referenzkonfigurationsdatei (RCF) angewendet wurde.
- Die bestehende Cluster-Netzwerkkonfiguration weist folgende Merkmale auf:
  - Ein redundanter und voll funktionsfähiger NetApp Cluster mit CN1610-Switches.
  - Management-Konnektivität und Konsolenzugriff sowohl auf die CN1610-Switches als auch auf die neuen Switches.
  - Alle Cluster-LIFs befinden sich im aktiven Zustand und sind an ihren Heimatports angeschlossen.
  - ISL-Ports wurden zwischen den CN1610-Switches und zwischen den neuen Switches aktiviert und verkabelt.
- Einige der Ports sind auf NVIDIA SN2100 Switches für den Betrieb mit 40GbE oder 100GbE konfiguriert.
- Sie haben die 40GbE- und 100GbE-Konnektivität von den Knoten zu den NVIDIA SN2100 Cluster-Switches geplant, migriert und dokumentiert.

Migrieren Sie die Schalter

Zu den Beispielen

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

- Die vorhandenen CN1610 Cluster-Switches sind *c1* und *c2*.
- Die neuen NVIDIA SN2100 Cluster-Switches sind *sw1* und *sw2*.
- Die Knoten heißen *node1* und *node2*.

- Die Cluster-LIFs sind *node1_clus1* und *node1_clus2* auf Knoten 1 bzw. *node2_clus1* und *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben folgendes Format: swp[Port]s[Breakout-Port 0-3]. Beispielsweise gibt es vier Breakout-Ports auf swp1: *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

Informationen zu diesem Vorgang

Dieses Verfahren umfasst folgendes Szenario:

- Der Schalter c2 wird zuerst durch den Schalter sw2 ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
  - Die Verkabelung zwischen den Knoten und c2 wird dann von c2 getrennt und wieder mit sw2 verbunden.
- Der Schalter c1 wird durch den Schalter sw1 ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
  - Die Verkabelung zwischen den Knoten und c1 wird dann von c1 getrennt und wieder mit sw1 verbunden.

> 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.

Schritt 1: Vorbereitung auf die Migration

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.

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. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ermitteln Sie den administrativen oder operativen Status jeder Clusterschnittstelle.

   Jeder Port sollte angezeigt werden für `Link` Und `healthy` für `Health Status` Die

   a. Netzwerkportattribute anzeigen:

      `network port show -ipspace Cluster`

      Beispiel anzeigen

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

      Node: node1

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

      Node: node2

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

   b. Informationen zu den LIFs und ihren jeweiligen Heimatknoten anzeigen:

      `network interface show -vserver Cluster`

      Jedes LIF sollte anzeigen `up/up` für `Status Admin/Oper` Und `true` für `Is Home` Die

Beispiel anzeigen

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3b     true
```

2. Die Cluster-Ports auf jedem Knoten werden (aus Sicht der Knoten) folgendermaßen mit vorhandenen Cluster-Switches verbunden:

   `network device-discovery show -protocol`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /cdp
            e3a    c1 (6a:ad:4f:98:3b:3f)    0/1               -
            e3b    c2 (6a:ad:4f:98:4c:a4)    0/1               -
node2      /cdp
            e3a    c1 (6a:ad:4f:98:3b:3f)    0/2               -
            e3b    c2 (6a:ad:4f:98:4c:a4)    0/2               -
```

3. Die Cluster-Ports und Switches werden (aus Sicht der Switches) mit folgendem Befehl verbunden:

   `show cdp neighbors`

Beispiel anzeigen

```
c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 0/1           124     H          AFF-A400
e3a
node2                 0/2           124     H          AFF-A400
e3a
c2                    0/13          179     S I s      CN1610
0/13
c2                    0/14          175     S I s      CN1610
0/14
c2                    0/15          179     S I s      CN1610
0/15
c2                    0/16          175     S I s      CN1610
0/16

c2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 0/1           124    H           AFF-A400
e3b
node2                 0/2           124    H           AFF-A400
e3b
c1                    0/13          175    S I s       CN1610
0/13
c1                    0/14          175    S I s       CN1610
0/14
c1                    0/15          175    S I s       CN1610
0/15
c1                    0/16          175    S I s       CN1610
0/16
```

4. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e3a
Cluster node1_clus2 169.254.49.125 node1     e3b
Cluster node2_clus1 169.254.47.194 node2     e3a
Cluster node2_clus2 169.254.19.183 node2     e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Schalten Sie auf Switch c2 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen.

```
(c2)# configure
(c2)(Config)# interface 0/1-0/12
(c2)(Interface 0/1-0/12)# shutdown
(c2)(Interface 0/1-0/12)# exit
(c2)(Config)# exit
(c2)#
```

2. Verschieben Sie die Knotencluster-Ports vom alten Switch c2 auf den neuen Switch sw2 unter Verwendung geeigneter, von NVIDIA SN2100 unterstützter Kabel.
3. Netzwerkportattribute anzeigen:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

   `network device-discovery show -protocol`

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   0/1               -
            e3b    sw2 (b8:ce:f6:19:1a:7e)   swp3              -
node2      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   0/2               -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4              -
```

5. Überprüfen Sie an Switch sw2, ob alle Ports des Knotenclusters aktiv sind:

   `net show interface`

Beispiel anzeigen

```
cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

6. Schalten Sie auf Switch c1 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen.

```
(c1)# configure
(c1)(Config)# interface 0/1-0/12
(c1)(Interface 0/1-0/12)# shutdown
(c1)(Interface 0/1-0/12)# exit
(c1)(Config)# exit
(c1)#
```

7. Verschieben Sie die Knotencluster-Ports vom alten Switch c1 auf den neuen Switch sw1 unter Verwendung geeigneter, von NVIDIA SN2100 unterstützter Kabel.
8. Überprüfen Sie die endgültige Konfiguration des Clusters:

   `network port show -ipspace Cluster`

   Jeder Port sollte Folgendes anzeigen `up` für `Link` Und `healthy` für `Health Status` Die

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

9. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

   `network device-discovery show -protocol`

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3           -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4           -
```

10. Überprüfen Sie an den Switches sw1 und sw2, ob alle Ports des Knotenclusters aktiv sind:

    `net show interface`

Beispiel anzeigen

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw2 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw2 (swp16)
Master: cluster_isl(UP)


cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

11. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

    `net show lldp`

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3a
swp4       100G   Trunk/L2    node2               e3a
swp15      100G   BondMember  sw2                 swp15
swp16      100G   BondMember  sw2                 swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3b
swp4       100G   Trunk/L2    node2               e3b
swp15      100G   BondMember  sw1                 swp15
swp16      100G   BondMember  sw1                 swp16
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

2. Auf Switch sw2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit

(Wait for 5-10 seconds before re-enabling the ports)

cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit

(After executing the link state up command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)
```

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface

(Wait for 5-10 seconds before re-enabling the ports)

cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface

(After executing the link state up command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)
```

1. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihre ursprünglichen Ports zurückgekehrt sind (dies kann eine Minute dauern):

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

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

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

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

3. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Migration von einem Cisco Cluster-Switch zu einem NVIDIA SN2100 Cluster-Switch

Sie können Cisco -Cluster-Switches für einen ONTAP Cluster auf NVIDIA SN2100-Cluster-Switches migrieren. Dies ist ein unterbrechungsfreies Verfahren.

Überprüfungsanforderungen

Beim Austausch älterer Cisco -Cluster-Switches durch NVIDIA SN2100-Cluster-Switches müssen Sie bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen beachten. Sehen"Übersicht über Installation und Konfiguration von NVIDIA SN2100-Switches" .

Unterstützte Schalter

Folgende Cisco Cluster-Switches werden unterstützt:

- Nexus 9336C-FX2
- Nexus 92300YC
- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Einzelheiten zu den unterstützten Ports und deren Konfigurationen finden Sie unter "Hardware Universe" Die

Was du brauchst

Stellen Sie sicher, dass:

- Der bestehende Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die NVIDIA SN2100 Cluster-Switches sind konfiguriert und arbeiten unter der richtigen Version von Cumulus Linux, auf der die Referenzkonfigurationsdatei (RCF) angewendet wurde.
- Die bestehende Cluster-Netzwerkkonfiguration weist folgende Merkmale auf:
  - Ein redundanter und voll funktionsfähiger NetApp Cluster, der beide ältere Cisco Switches nutzt.
  - Management-Konnektivität und Konsolenzugriff sowohl auf die älteren Cisco Switches als auch auf die neuen Switches.
  - Alle Cluster-LIFs befinden sich im aktiven Zustand und sind an ihren Heimatports angeschlossen.
  - ISL-Ports wurden aktiviert und zwischen den älteren Cisco Switches sowie zwischen den neuen Switches verkabelt.
- Einige der Ports sind auf NVIDIA SN2100 Switches für den Betrieb mit 40 GbE oder 100 GbE konfiguriert.
- Sie haben die 40-GbE- und 100-GbE-Konnektivität von den Knoten zu den NVIDIA SN2100 Cluster-Switches geplant, migriert und dokumentiert.

Wenn Sie die Portgeschwindigkeit der Cluster-Ports e0a und e1a auf AFF A800 oder AFF C800 Systemen ändern, kann es nach der Geschwindigkeitsumwandlung zu fehlerhaften Paketen kommen. Sehen "Bug 1570339" und der Artikel in der Wissensdatenbank "CRC-Fehler an T6-Ports nach der Umstellung von 40GbE auf 100GbE" zur Orientierung.

Migrieren Sie die Schalter

Zu den Beispielen

In diesem Verfahren werden Cisco Nexus 3232C Cluster-Switches als Beispiel für Befehle und Ausgaben verwendet.

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

- Die vorhandenen Cisco Nexus 3232C Cluster-Switches sind *c1* und *c2*.
- Die neuen NVIDIA SN2100 Cluster-Switches sind *sw1* und *sw2*.
- Die Knoten heißen *node1* und *node2*.
- Die Cluster-LIFs sind *node1_clus1* und *node1_clus2* auf Knoten 1 bzw. *node2_clus1* und *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben folgendes Format: swp[Port]s[Breakout-Port 0-3]. Beispielsweise gibt es vier Breakout-Ports auf swp1: *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

Informationen zu diesem Vorgang

Dieses Verfahren umfasst folgendes Szenario:

- Der Schalter c2 wird zuerst durch den Schalter sw2 ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
  - Die Verkabelung zwischen den Knoten und c2 wird dann von c2 getrennt und wieder mit sw2 verbunden.
- Der Schalter c1 wird durch den Schalter sw1 ersetzt.
  - Schalten Sie die Ports zu den Clusterknoten ab. Um eine Instabilität des Clusters zu vermeiden, müssen alle Ports gleichzeitig abgeschaltet werden.
  - Die Verkabelung zwischen den Knoten und c1 wird dann von c1 getrennt und wieder mit sw1 verbunden.

Schritt 1: Vorbereitung auf die Migration

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.

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. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ermitteln Sie den administrativen oder operativen Status jeder Clusterschnittstelle.

   Jeder Port sollte angezeigt werden für `Link` und gesund für `Health Status` Die

   a. Netzwerkportattribute anzeigen:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

b. Informationen über die logischen Schnittstellen und ihre jeweiligen Heimatknoten anzeigen:

`network interface show -vserver Cluster`

Jedes LIF sollte anzeigen `up/up` für `Status Admin/Oper` und wahr für `Is Home` Die

Beispiel anzeigen

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- -----------  ---------- ------------------ -----------
------- ----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e3b     true
```

2. Die Cluster-Ports an jedem Knoten sind folgendermaßen mit den vorhandenen Cluster-Switches verbunden (aus Sicht der Knoten):

   `network device-discovery show -protocol lldp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1 (6a:ad:4f:98:3b:3f)    Eth1/1            -
            e3b    c2 (6a:ad:4f:98:4c:a4)    Eth1/1            -
node2      /lldp
            e3a    c1 (6a:ad:4f:98:3b:3f)    Eth1/2            -
            e3b    c2 (6a:ad:4f:98:4c:a4)    Eth1/2            -
```

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

   `show cdp neighbors`

Beispiel anzeigen

```
c1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1         124   H           AFF-A400
e3a
node2                 Eth1/2         124   H           AFF-A400
e3a
c2                    Eth1/31        179   S I s       N3K-C3232C
Eth1/31
c2                    Eth1/32        175   S I s       N3K-C3232C
Eth1/32

c2# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute


Device-ID             Local Intrfce Hldtme Capability  Platform
Port ID
node1                 Eth1/1        124    H           AFF-A400
e3b
node2                 Eth1/2        124    H           AFF-A400
e3b
c1                    Eth1/31       175    S I s       N3K-C3232C
Eth1/31
c1                    Eth1/32       175    S I s       N3K-C3232C
Eth1/32
```

4. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e3a
Cluster node1_clus2 169.254.49.125 node1     e3b
Cluster node2_clus1 169.254.47.194 node2     e3a
Cluster node2_clus2 169.254.19.183 node2     e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
................
Detected 9000 byte MTU on 4 path(s):
    Local 169.254.19.183 to Remote 169.254.209.69
    Local 169.254.19.183 to Remote 169.254.49.125
    Local 169.254.47.194 to Remote 169.254.209.69
    Local 169.254.47.194 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Schalten Sie auf Switch c2 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen.

```
(c2)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c2)(Config)# interface
(c2)(config-if-range)# shutdown <interface_list>
(c2)(config-if-range)# exit
(c2)(Config)# exit
(c2)#
```

2. Verschieben Sie die Knotencluster-Ports vom alten Switch c2 auf den neuen Switch sw2 unter Verwendung geeigneter, von NVIDIA SN2100 unterstützter Kabel.
3. Netzwerkportattribute anzeigen:

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

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   Eth1/1            -
            e3b    sw2 (b8:ce:f6:19:1a:7e)   swp3              -
node2      /lldp
            e3a    c1  (6a:ad:4f:98:3b:3f)   Eth1/2            -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4              -
```

5. Überprüfen Sie an Switch sw2, ob alle Ports des Knotenclusters aktiv sind:

   `net show interface`

Beispiel anzeigen

```
cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

6. Schalten Sie auf Switch c1 die mit den Cluster-Ports der Knoten verbundenen Ports ab, um ein Failover der Cluster-LIFs zu erzwingen.

```
(c1)# configure
Enter configuration commands, one per line. End with CNTL/Z.

(c1)(Config)# interface
(c1)(config-if-range)# shutdown <interface_list>
(c1)(config-if-range)# exit
(c1)(Config)# exit
(c1)#
```

7. Verschieben Sie die Knotencluster-Ports vom alten Switch c1 auf den neuen Switch sw1 unter Verwendung geeigneter, von NVIDIA SN2100 unterstützter Kabel.
8. Überprüfen Sie die endgültige Konfiguration des Clusters:

   `network port show -ipspace Cluster`

   Jeder Port sollte Folgendes anzeigen `up` für `Link` und gesund für `Health Status` Die

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

9. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3           -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4           -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4           -
```

10. Überprüfen Sie an den Switches sw1 und sw2, ob alle Ports des Knotenclusters aktiv sind:

    `net show interface`

Beispiel anzeigen

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3a
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw2 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw2 (swp16)
Master: cluster_isl(UP)


cumulus@sw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2    e3b
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

11. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

    `net show lldp`

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3a
swp4       100G   Trunk/L2    node2               e3a
swp15      100G   BondMember  sw2                 swp15
swp16      100G   BondMember  sw2                 swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost          RemotePort
---------  -----  ----------  ------------------  -----------
swp3       100G   Trunk/L2    node1               e3b
swp4       100G   Trunk/L2    node2               e3b
swp15      100G   BondMember  sw1                 swp15
swp16      100G   BondMember  sw1                 swp16
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

2. Auf Switch sw2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit

(Wait for 5-10 seconds before re-enabling the ports)

cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit

(After executing the link state up command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)
```

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface

(Wait for 5-10 seconds before re-enabling the ports)

cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface

(After executing the link state up command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)
```

1. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihre ursprünglichen Ports zurückgekehrt sind (dies kann eine Minute dauern):

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

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

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

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

3. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Migration zu einem Zwei-Knoten-Switch-Cluster mit NVIDIA SN2100 Cluster-Switches

Wenn Sie bereits eine switchlose Clusterumgebung mit zwei Knoten besitzen, können Sie mithilfe von NVIDIA SN2100 Switches auf eine switchierte Clusterumgebung mit zwei Knoten migrieren, um die Anzahl der Knoten im Cluster auf über zwei zu erweitern.

Die Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerkanschlüsse oder an jedem Controller einen einzelnen Clusteranschluss haben. Der dokumentierte Prozess funktioniert für alle Knoten, die optische oder Twinax-Ports verwenden, wird jedoch auf diesem Switch nicht unterstützt, wenn die Knoten Onboard-10GBASE-T-RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

Überprüfungsanforderungen

Zwei-Knoten-Schalterlose Konfiguration

Stellen Sie sicher, dass:

- Die beiden schalterlosen Knoten sind ordnungsgemäß eingerichtet und funktionieren.
- Auf den Knoten läuft ONTAP 9.10.1P3 oder höher.
- Alle Cluster-Ports befinden sich im Status **up**.
- Alle logischen Schnittstellen (LIFs) des Clusters befinden sich im Status **up** und sind an ihren jeweiligen Ports angeschlossen.

NVIDIA SN2100 Cluster-Switch-Konfiguration

Stellen Sie sicher, dass:

- Beide Switches verfügen über eine Management-Netzwerkanbindung.
- Es besteht Konsolenzugriff auf die Cluster-Switches.
- Die Knoten-zu-Knoten- und Switch-zu-Switch-Verbindungen des NVIDIA SN2100 verwenden Twinax- oder Glasfaserkabel.

> Sehen"Überprüfung der Verkabelung und Konfigurationsüberlegungen" für Einschränkungen und weitere Details. Der "Hardware Universe – Schalter" Enthält außerdem weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel sind an die Ports swp15 und swp16 beider NVIDIA SN2100 Switches angeschlossen.
- Die erste Anpassung beider SN2100-Schalter ist abgeschlossen, sodass:
  - Die SN2100-Switches laufen mit der neuesten Version von Cumulus Linux.
  - Referenzkonfigurationsdateien (RCFs) werden auf die Schalter angewendet.
  - Sämtliche Standortanpassungen, wie z. B. SMTP, SNMP und SSH, werden auf den neuen Switches konfiguriert.

    Der "Hardware Universe" Enthält die aktuellsten Informationen zu den tatsächlichen Cluster-Ports für

Ihre Plattformen.

Migrieren Sie die Schalter

Zu den Beispielen

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

- Die Namen der SN2100-Schalter lauten *sw1* und *sw2*.
- Die Namen der Cluster-SVMs lauten *node1* und *node2*.
- Die Namen der LIFs lauten *node1_clus1* und *node1_clus2* auf Knoten 1 bzw. *node2_clus1* und *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben folgendes Format: swp[Port]s[Breakout-Port 0-3]. Beispielsweise gibt es vier Breakout-Ports auf swp1: *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

Schritt 1: Vorbereitung auf die Migration

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.

2. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren: `set -privilege advanced`

   Die erweiterte Aufforderung(`*>`) erscheint.

Schritt 2: Anschlüsse und Verkabelung konfigurieren

Cumulus Linux 4.4.x

1. Deaktivieren Sie alle zum Knoten führenden Ports (nicht die ISL-Ports) an den beiden neuen Cluster-Switches sw1 und sw2.

   Die ISL-Ports dürfen nicht deaktiviert werden.

   Die folgenden Befehle deaktivieren die zum Knoten führenden Ports der Switches sw1 und sw2:

   ```
   cumulus@sw1:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit

   cumulus@sw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw2:~$ net pending
   cumulus@sw2:~$ net commit
   ```

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden SN2100-Switches sw1 und sw2 an den Ports swp15 und swp16 aktiv sind:

   ```
   net show interface
   ```

   Die folgenden Befehle zeigen, dass die ISL-Ports an den Switches sw1 und sw2 aktiv sind:

```
cumulus@sw1:~$ net show interface

State  Name       Spd   MTU    Mode        LLDP         Summary
-----  ---------  ----  -----  ----------  -----------
-----------------------
...
...
UP     swp15      100G  9216   BondMember  sw2 (swp15)  Master:
cluster_isl(UP)
UP     swp16      100G  9216   BondMember  sw2 (swp16)  Master:
cluster_isl(UP)

cumulus@sw2:~$ net show interface

State  Name       Spd   MTU    Mode        LLDP         Summary
-----  ---------  ----  -----  ----------  -----------
-----------------------
...
...
UP     swp15      100G  9216   BondMember  sw1 (swp15)  Master:
cluster_isl(UP)
UP     swp16      100G  9216   BondMember  sw1 (swp16)  Master:
cluster_isl(UP)
```

Cumulus Linux 5.x

1. Deaktivieren Sie alle zum Knoten führenden Ports (nicht die ISL-Ports) an den beiden neuen Cluster-Switches sw1 und sw2.

   Die ISL-Ports dürfen nicht deaktiviert werden.

   Die folgenden Befehle deaktivieren die zum Knoten führenden Ports der Switches sw1 und sw2:

   ```
   cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
   down
   cumulus@sw1:~$ nv config apply
   cumulus@sw1:~$ nv config save

   cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
   down
   cumulus@sw2:~$ nv config apply
   cumulus@sw2:~$ nv config save
   ```

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden SN2100-Switches sw1 und sw2 an den Ports swp15 und swp16 aktiv sind:

`nv show interface`

Die folgenden Beispiele zeigen, dass die ISL-Ports an den Switches sw1 und sw2 aktiv sind:

```
cumulus@sw1:~$ nv show interface

Interface     MTU    Speed  State  Remote Host  Remote Port
Type    Summary
------------ ------ -----  ------ ------------
------------------------------------ ------- -------
...
...
+ swp14       9216          down
swp
+ swp15       9216   100G   up     ossg-rcf1    Intra-Cluster Switch
ISL Port swp15  swp
+ swp16       9216   100G   up     ossg-rcf2    Intra-Cluster Switch
ISL Port swp16  swp


cumulus@sw2:~$ nv show interface

Interface     MTU    Speed  State  Remote Host  Remote Port
Type    Summary
------------ ------ -----  ------ ------------
------------------------------------ ------- -------
...
...
+ swp14       9216          down
swp
+ swp15       9216   100G   up     ossg-rcf1    Intra-Cluster Switch
ISL Port swp15  swp
+ swp16       9216   100G   up     ossg-rcf2    Intra-Cluster Switch
ISL Port swp16  swp
```

1. [[Schritt 3]] Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

   `network port show`

   Jeder Port sollte Folgendes anzeigen `up` für `Link` und gesund für `Health Status` Die

Beispiel anzeigen

```
cluster1::*> network port show

Node: node1


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

Node: node2


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

2. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind:

   `network interface show`

   Jeder Cluster-LIF sollte „true“ anzeigen für `Is Home` und haben `Status Admin/Oper` von `up/up` Die

Beispiel anzeigen

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e3a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e3b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e3a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e3b     true
```

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

   Beispiel anzeigen

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

          Logical
Vserver   Interface     Auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   false
          node1_clus2   false
          node2_clus1   false
          node2_clus2   false
```

4. Trennen Sie das Kabel vom Cluster-Port e3a auf Knoten 1 und verbinden Sie dann e3a mit Port 3 des Cluster-Switches sw1. Verwenden Sie dazu die von den SN2100-Switches unterstützten geeigneten Kabel.

   Der "Hardware Universe – Schalter" enthält weitere Informationen zur Verkabelung.

5. Trennen Sie das Kabel vom Cluster-Port e3a auf Knoten 2 und verbinden Sie dann e3a mit Port 4 auf

Cluster-Switch sw1. Verwenden Sie dazu die von den SN2100-Switches unterstützten geeigneten Kabel.

Cumulus Linux 4.4.x

1. Aktivieren Sie auf Switch sw1 alle zum Knoten hin ausgerichteten Ports.

   Die folgenden Befehle aktivieren alle zum Knoten hin ausgerichteten Ports am Switch sw1.

   ```
   cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit
   ```

2. Überprüfen Sie am Switch sw1, ob alle Ports aktiv sind:

   ```
   net show interface all
   ```

```
cumulus@sw1:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP             Summary
-----  --------- ----  -----  ---------- ---------------- --------
...
DN     swp1s0    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s1    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s2    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp1s3    10G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s0    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s1    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s2    25G   9216   Trunk/L2                    Master:
br_default(UP)
DN     swp2s3    25G   9216   Trunk/L2                    Master:
br_default(UP)
UP     swp3      100G  9216   Trunk/L2    node1 (e3a)     Master:
br_default(UP)
UP     swp4      100G  9216   Trunk/L2    node2 (e3a)     Master:
br_default(UP)
...
...
UP     swp15     100G  9216   BondMember  swp15           Master:
cluster_isl(UP)
UP     swp16     100G  9216   BondMember  swp16           Master:
cluster_isl(UP)
...
```

Cumulus Linux 5.x

1. Aktivieren Sie auf Switch sw1 alle zum Knoten hin ausgerichteten Ports.

   Die folgenden Befehle aktivieren alle zum Knoten hin ausgerichteten Ports am Switch sw1.

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
up
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

2. [[Schritt 9]] Überprüfen Sie am Switch sw1, ob alle Ports aktiv sind:

```
nv show interface
```

```
cumulus@sw1:~$ nv show interface

Interface    State  Speed  MTU    Type      Remote Host
Remote Port  Summary
-----------  -----  -----  -----  --------
--------------------------  -----------  ----------
...
...
swp1s0       up     10G    9216   swp       odq-a300-1a
e0a
swp1s1       up     10G    9216   swp       odq-a300-1b
e0a
swp1s2       down   10G    9216   swp
swp1s3       down   10G    9216   swp
swp2s0       down   25G    9216   swp
swp2s1       down   25G    9216   swp
swp2s2       down   25G    9216   swp
swp2s3       down   25G    9216   swp
swp3         down          9216   swp
swp4         down          9216   swp
...
...
swp14        down          9216   swp
swp15        up     100G   9216   swp       ossg-int-rcf10
swp15
swp16        up     100G   9216   swp       ossg-int-rcf10
swp16
```

1. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports auf Knoten 1 und Knoten 2 aktiv sind:

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

Node: node1

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

Node: node2

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

2. Informationen über den Status der Knoten im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster an:

```
cluster1::*> cluster show

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

3. Trennen Sie das Kabel vom Cluster-Port e3b auf Knoten 1 und verbinden Sie dann e3b mit Port 3 des Cluster-Switches sw2. Verwenden Sie dazu die von den SN2100-Switches unterstützten Kabel.
4. Trennen Sie das Kabel vom Cluster-Port e3b auf Knoten 2 und verbinden Sie dann e3b mit Port 4 auf Cluster-Switch sw2. Verwenden Sie dazu die von den SN2100-Switches unterstützten Kabel.

Cumulus Linux 4.4.x

1. Aktivieren Sie auf Switch sw2 alle zum Knoten hin ausgerichteten Ports.

   Die folgenden Befehle aktivieren die zum Knoten hin ausgerichteten Ports am Switch sw2:

   ```
   cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@sw2:~$ net pending
   cumulus@sw2:~$ net commit
   ```

2. Überprüfen Sie am Switch sw2, ob alle Ports aktiv sind:

   ```
   net show interface all
   ```

```
cumulus@sw2:~$ net show interface all

State  Name      Spd   MTU    Mode        LLDP             Summary
-----  --------- ----  -----  ----------- ---------------- --------
...
DN     swp1s0    10G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp1s1    10G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp1s2    10G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp1s3    10G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp2s0    25G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp2s1    25G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp2s2    25G   9216   Trunk/L2                     Master:
br_default(UP)
DN     swp2s3    25G   9216   Trunk/L2                     Master:
br_default(UP)
UP     swp3      100G  9216   Trunk/L2    node1 (e3b)      Master:
br_default(UP)
UP     swp4      100G  9216   Trunk/L2    node2 (e3b)      Master:
br_default(UP)
...
...
UP     swp15     100G  9216   BondMember  swp15            Master:
cluster_isl(UP)
UP     swp16     100G  9216   BondMember  swp16            Master:
cluster_isl(UP)
...
```

3. Überprüfen Sie an beiden Switches sw1 und sw2, ob jeder Knoten genau eine Verbindung zu jedem Switch hat:

   `net show lldp`

   Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter sw1 und sw2:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  sw2                swp15
swp16      100G   BondMember  sw2                swp16

cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3b
swp4       100G   Trunk/L2    node2              e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

Cumulus Linux 5.x

1. Aktivieren Sie auf Switch sw2 alle zum Knoten hin ausgerichteten Ports.

   Die folgenden Befehle aktivieren die zum Knoten hin ausgerichteten Ports am Switch sw2:

   ```
   cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
   up
   cumulus@sw2:~$ nv config apply
   cumulus@sw2:~$ nv config save
   ```

2. Überprüfen Sie am Switch sw2, ob alle Ports aktiv sind:

   ```
   nv show interface
   ```

```
cumulus@sw2:~$ nv show interface

Interface    State  Speed  MTU    Type      Remote Host
Remote Port  Summary
-----------  -----  -----  -----  --------
--------------------------  -----------  ----------
...
...
swp1s0       up     10G    9216   swp       odq-a300-1a
e0a
swp1s1       up     10G    9216   swp       odq-a300-1b
e0a
swp1s2       down   10G    9216   swp
swp1s3       down   10G    9216   swp
swp2s0       down   25G    9216   swp
swp2s1       down   25G    9216   swp
swp2s2       down   25G    9216   swp
swp2s3       down   25G    9216   swp
swp3         down          9216   swp
swp4         down          9216   swp
...
...
swp14        down          9216   swp
swp15        up     100G   9216   swp       ossg-int-rcf10
swp15
swp16        up     100G   9216   swp       ossg-int-rcf10
swp16
```

3. Überprüfen Sie an beiden Switches sw1 und sw2, ob jeder Knoten genau eine Verbindung zu jedem Switch hat:

   `nv show interface --view=lldp`

   Die folgenden Beispiele zeigen die entsprechenden Ergebnisse für beide Schalter sw1 und sw2:

```
cumulus@sw1:~$ nv show interface --view=lldp

Interface    Speed  Type      Remote Host
Remote Port
-----------  -----  --------  ---------------------------------
-----------
...
...
swp1s0       10G    swp       odq-a300-1a
e0a
```

```
swp1s1       10G    swp       odq-a300-1b
e0a
swp1s2       10G    swp
swp1s3       10G    swp
swp2s0       25G    swp
swp2s1       25G    swp
swp2s2       25G    swp
swp2s3       25G    swp
swp3                swp
swp4                swp
...
...
swp14               swp
swp15        100G   swp       ossg-int-rcf10
swp15
swp16        100G   swp       ossg-int-rcf10
swp16

cumulus@sw2:~$ nv show interface --view=lldp

Interface    Speed  Type      Remote Host
Remote Port
-----------  -----  --------  ---------------------------------
-----------
...
...
swp1s0       10G    swp       odq-a300-1a
e0a
swp1s1       10G    swp       odq-a300-1b
e0a
swp1s2       10G    swp
swp1s3       10G    swp
swp2s0       25G    swp
swp2s1       25G    swp
swp2s2       25G    swp
swp2s3       25G    swp
swp3                swp
swp4                swp
...
...
swp14               swp
swp15        100G   swp       ossg-int-rcf10
swp15
swp16        100G   swp       ossg-int-rcf10
swp16
```

1. Informationen zu den in Ihrem Cluster gefundenen Netzwerkgeräten anzeigen:

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

   Beispiel anzeigen

   ```
   cluster1::*> network device-discovery show -protocol lldp
   Node/       Local  Discovered
   Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
   ----------- ------ ------------------------- ------------
   ----------------
   node1      /lldp
               e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3          -
               e3b    sw2 (b8:ce:f6:19:1b:96)   swp3          -
   node2      /lldp
               e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4          -
               e3b    sw2 (b8:ce:f6:19:1b:96)   swp4          -
   ```

2. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports auf Knoten 1 und Knoten 2 aktiv sind:

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

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       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
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung auf allen Cluster-LIFs aktivieren:

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

Beispiel anzeigen

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

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

2. Auf Switch sw2 müssen alle Cluster-Ports heruntergefahren und neu gestartet werden, um eine automatische Rücksetzung aller Cluster-LIFs auszulösen, die sich nicht an ihren Home-Ports befinden.

Cumulus 4.4.3

```
cumulus@sw2:mgmt:~$ net add interface swp1-14 link down
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit

(Wait for 5-10 seconds before re-enabling the ports)

cumulus@sw2:mgmt:~$ net add interface swp1-14 link up
cumulus@sw2:mgmt:~$ net pending
cumulus@sw2:mgmt:~$ net commit

(After executing the link state up command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)
```

Cumulus 5.x

```
cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state down
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface

(Wait for 5-10 seconds before re-enabling the ports)

cumulus@sw2:mgmt:~$ nv set interface swp1-14 link state up
cumulus@sw2:mgmt:~$ nv config apply
cumulus@sw2:mgmt:~$ nv show interface

(After executing the link state up command, the nodes detect the change
and begin to auto-revert the cluster LIFs to their home ports)
```

1. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihre ursprünglichen Ports zurückgekehrt sind (dies kann eine Minute dauern):

   `network interface show -vserver Cluster`

   Falls eine der Cluster-LIFs nicht auf ihren Heimatport zurückgesetzt wurde, setzen Sie sie manuell zurück. Sie müssen eine Verbindung zur jeweiligen Node-Management-LIF- oder SP/ BMC -Systemkonsole des lokalen Knotens herstellen, dem die LIF gehört:

   `network interface revert -vserver Cluster -lif *`

2. Überprüfen Sie, ob alle Schnittstellen angezeigt werden. `true` für `Is Home` :

   `net interface show -vserver Cluster`

   Dieser Vorgang kann eine Minute dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf Knoten 1 und Knoten 2 aktiv sind und dass `Is Home` Die Ergebnisse sind korrekt:

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

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e3a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e3b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e3a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e3b
true
```

3. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

   `network options switchless-cluster show`

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

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

4. Überprüfen Sie den Status der Knoten im Cluster:

   `cluster show`

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 8]]Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

2. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Ersetzen Sie die Schalter

Ersetzen Sie einen NVIDIA SN2100 Cluster-Switch

Gehen Sie wie folgt vor, um einen defekten NVIDIA SN2100-Switch in einem Clusternetzwerk auszutauschen. Dies ist ein unterbrechungsfreies Verfahren (NDU).

Überprüfungsanforderungen

Vorhandene Cluster- und Netzwerkinfrastruktur

Stellen Sie sicher, dass:

- Es wurde überprüft, dass die vorhandenen Cluster voll funktionsfähig sind und mindestens ein Cluster-Switch vollständig angeschlossen ist.
- Alle Cluster-Ports sind aktiv.
- Alle logischen Schnittstellen (LIFs) des Clusters sind aktiv und an ihren jeweiligen Ports angeschlossen.
- Das ONTAP `cluster ping-cluster -node node1` Der Befehl zeigt an, dass die grundlegende Konnektivität und die Kommunikation über PMTU hinaus auf allen Pfaden erfolgreich sind.

NVIDIA SN2100 Ersatzschalter

Stellen Sie sicher, dass:

- Die Management-Netzwerkanbindung des Ersatz-Switches ist funktionsfähig.
- Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
- Die Knotenverbindungen sind die Ports swp1 bis swp14.
- Alle Inter-Switch Link (ISL)-Ports sind an den Ports swp15 und swp16 deaktiviert.
- Die gewünschte Referenzkonfigurationsdatei (RCF) und das Cumulus-Betriebssystem-Image werden auf den Switch geladen.
- Die erste Konfiguration des Schalters ist abgeschlossen.

Achten Sie außerdem darauf, dass alle zuvor vorgenommenen Anpassungen am Standort, wie z. B. STP, SNMP und SSH, auf den neuen Switch kopiert werden.

> Sie müssen den Befehl zur Migration eines Cluster-LIF von dem Knoten ausführen, auf dem der Cluster-LIF gehostet wird.

Konsolenprotokollierung aktivieren

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

- Lassen Sie AutoSupport während der Wartungsarbeiten aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs AutoSupport aus, um die Fallerstellung für die Dauer der Wartung zu deaktivieren. Siehe diesen Wissensdatenbankartikel "SU92: Wie man die automatische Fallerstellung während geplanter Wartungsfenster unterdrückt" für weitere Einzelheiten.
- Aktivieren Sie die Sitzungsprotokollierung für alle CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Wissensdatenbankartikel. "Wie konfiguriert man PuTTY für eine optimale Verbindung zu ONTAP -Systemen?" Die

Tauschen Sie den Schalter aus.

Zu den Beispielen

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

- Die Namen der vorhandenen NVIDIA SN2100-Switches lauten *sw1* und *sw2*.

- Der Name des neuen NVIDIA SN2100 Switches lautet *nsw2*.
- Die Knotennamen lauten *node1* und *node2*.
- Die Cluster-Ports auf jedem Knoten tragen die Namen *e3a* und *e3b*.
- Die Cluster-LIF-Namen lauten *node1_clus1* und *node1_clus2* für Knoten 1 sowie *node2_clus1* und *node2_clus2* für Knoten 2.
- Die Aufforderung zur Änderung aller Clusterknoten lautet: `cluster1::*>`
- Breakout-Ports haben folgendes Format: swp[Port]s[Breakout-Port 0-3]. Beispielsweise gibt es vier Breakout-Ports auf swp1: *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

Über die Cluster-Netzwerktopologie

Dieses Verfahren basiert auf folgender Cluster-Netzwerktopologie:

Beispieltopologie anzeigen

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

Node: node1

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

Node: node2

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


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e3a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e3b
true
```

```
            node2_clus1  up/up    169.254.47.194/16  node2         e3a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e3b
true


cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3          -
node2      /lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4          -
```

+

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    sw2                e3a
swp4       100G   Trunk/L2    sw2                e3a
swp15      100G   BondMember  sw2                swp15
swp16      100G   BondMember  sw2                swp16


cumulus@sw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    sw1                e3b
swp4       100G   Trunk/L2    sw1                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

Schritt 1: Vorbereitung auf den Austausch

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.

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. Installieren Sie die entsprechende RCF-Datei und das Image auf dem Switch nsw2 und treffen Sie alle notwendigen Vorbereitungen vor Ort.

   Prüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und Cumulus-Software für den neuen Switch.

   a. Sie können die passende Cumulus-Software für Ihre Cluster-Switches von der NVIDIA Support-Website herunterladen. Folgen Sie den Anweisungen auf der Downloadseite, um Cumulus Linux für die Version der ONTAP -Software herunterzuladen, die Sie installieren.

   b. Die entsprechende RCF ist erhältlich bei der"NVIDIA Cluster- und Speicher-Switches" Seite. Folgen Sie den Anweisungen auf der Downloadseite, um die richtige RCF-Datei für die Version der ONTAP -Software herunterzuladen, die Sie installieren.

Schritt 2: Anschlüsse und Verkabelung konfigurieren

Cumulus Linux 4.4.3

1. Melden Sie sich auf dem neuen Switch nsw2 als Administrator an und deaktivieren Sie alle Ports, die mit den Schnittstellen des Knotenclusters verbunden werden (Ports swp1 bis swp14).

   Die LIFs auf den Clusterknoten sollten bereits für jeden Knoten auf den anderen Clusterport umgeschaltet haben.

   ```
   cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
   down
   cumulus@nsw2:~$ net pending
   cumulus@nsw2:~$ net commit
   ```

2. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

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

   Warning: Disabling the auto-revert feature of the cluster logical
   interface may effect the availability of your cluster network. Are
   you sure you want to continue? {y|n}: y
   ```

3. Überprüfen Sie, ob die automatische Rücksetzung für alle Cluster-LIFs deaktiviert ist:

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

4. Schalten Sie die ISL-Ports swp15 und swp16 am SN2100-Switch sw1 ab.

   ```
   cumulus@sw1:~$ net add interface swp15-16 link down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit
   ```

5. Entfernen Sie alle Kabel vom SN2100 sw1 Switch und schließen Sie sie dann an die gleichen Ports am SN2100 nsw2 Switch an.
6. Aktivieren Sie die ISL-Ports swp15 und swp16 zwischen den Switches sw1 und nsw2.

   Die folgenden Befehle aktivieren die ISL-Ports swp15 und swp16 auf Switch sw1:

   ```
   cumulus@sw1:~$ net del interface swp15-16 link down
   cumulus@sw1:~$ net pending
   cumulus@sw1:~$ net commit
   ```

   Das folgende Beispiel zeigt, dass die ISL-Ports am Switch sw1 aktiv sind:

```
cumulus@sw1:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP           Summary
-----  -----------  ----  -----  ----------  -------------
----------------------
...
...
UP     swp15        100G  9216   BondMember  nsw2 (swp15)   Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  nsw2 (swp16)   Master:
cluster_isl(UP)
```

Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch nsw2 aktiv sind:

```
cumulus@nsw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP           Summary
-----  -----------  ----  -----  ----------  -------------
----------------------
...
...
UP     swp15        100G  9216   BondMember  sw1 (swp15)    Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)    Master:
cluster_isl(UP)
```

7. Überprüfen Sie, ob der Port `e3b` ist auf allen Knoten aktiv:

   `network port show -ipspace Cluster`

   Die Ausgabe sollte in etwa wie folgt aussehen:

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

Node: node1

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


Node: node2

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

8. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp3          -
node2      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp4          -
```

9. Überprüfen Sie, ob alle Ports des Knotenclusters aktiv sind:

   `net show interface`

```
cumulus@nsw2:~$ net show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

10. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

    `net show lldp`

    Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  nsw2               swp15
swp16      100G   BondMember  nsw2               swp16


cumulus@nsw2:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1                e3b
swp4       100G   Trunk/L2    node2                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

11. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

12. Schalten Sie auf Switch nsw2 die Ports ein, die mit den Netzwerkports der Knoten verbunden sind.

    ```
    cumulus@nsw2:~$ net del interface swp1-14 link down
    cumulus@nsw2:~$ net pending
    cumulus@nsw2:~$ net commit
    ```

13. Informationen über die Knoten in einem Cluster anzeigen:

    ```
    cluster show
    ```

    Dieses Beispiel zeigt, dass der Knotenstatus für Knoten 1 und Knoten 2 in diesem Cluster „true“ ist:

    ```
    cluster1::*> cluster show

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

14. Überprüfen Sie, ob alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

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

Node node1
Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e3a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e3b       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
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e3a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up    9000  auto/10000
healthy  false
```

Cumulus Linux 5.x

1. Melden Sie sich auf dem neuen Switch nsw2 als Administrator an und deaktivieren Sie alle Ports, die mit den Schnittstellen des Knotenclusters verbunden werden (Ports swp1 bis swp14).

   Die LIFs auf den Clusterknoten sollten bereits für jeden Knoten auf den anderen Clusterport umgeschaltet haben.

   ```
   cumulus@nsw2:~$ nv set interface swp15-16 link state down
   cumulus@nsw2:~$ nv config apply
   ```

2. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

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

Warning: Disabling the auto-revert feature of the cluster logical
interface may effect the availability of your cluster network. Are
you sure you want to continue? {y|n}: y
```

3. Überprüfen Sie, ob die automatische Rücksetzung für alle Cluster-LIFs deaktiviert ist:

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

4. Schalten Sie die ISL-Ports swp15 und swp16 am SN2100-Switch sw1 ab.

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

5. Entfernen Sie alle Kabel vom SN2100 sw1 Switch und schließen Sie sie dann an die gleichen Ports am SN2100 nsw2 Switch an.
6. Aktivieren Sie die ISL-Ports swp15 und swp16 zwischen den Switches sw1 und nsw2.

   Die folgenden Befehle aktivieren die ISL-Ports swp15 und swp16 auf Switch sw1:

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

   Das folgende Beispiel zeigt, dass die ISL-Ports am Switch sw1 aktiv sind:

```
cumulus@sw1:~$ nv show interface

State  Name         Spd   MTU    Mode        LLDP            Summary
-----  -----------  ----  -----  ----------  --------------
----------------------
...
...
UP     swp15        100G  9216   BondMember  nsw2 (swp15)    Master:
cluster_isl(UP)
UP     swp16        100G  9216   BondMember  nsw2 (swp16)    Master:
cluster_isl(UP)
```

   Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch nsw2 aktiv sind:

```
cumulus@nsw2:~$ nv show interface

State  Name          Spd   MTU    Mode         LLDP            Summary
-----  ------------  ----  -----  ----------  -------------
-----------------------
...
...
UP     swp15         100G  9216   BondMember  sw1 (swp15)     Master:
cluster_isl(UP)
UP     swp16         100G  9216   BondMember  sw1 (swp16)     Master:
cluster_isl(UP)
```

7. Überprüfen Sie, ob der Port `e3b` ist auf allen Knoten aktiv:

   `network port show -ipspace Cluster`

   Die Ausgabe sollte in etwa wie folgt aussehen:

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

Node: node1

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


Node: node2

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

8. Die Cluster-Ports auf jedem Knoten sind nun, aus Sicht der Knoten, folgendermaßen mit den Cluster-Switches verbunden:

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface     Platform
----------- ------ ------------------------- ------------
----------------
node1      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp3          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp3          -
node2      /lldp
            e3a    sw1  (b8:ce:f6:19:1a:7e)   swp4          -
            e3b    nsw2 (b8:ce:f6:19:1b:b6)   swp4          -
```

9. Überprüfen Sie, ob alle Ports des Knotenclusters aktiv sind:

   `nv show interface`

```
cumulus@nsw2:~$ nv show interface

State  Name         Spd   MTU    Mode        LLDP
Summary
-----  -----------  ----  -----  ----------  -----------------
----------------------
...
...
UP     swp3         100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp4         100G  9216   Trunk/L2
Master: bridge(UP)
UP     swp15        100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl(UP)
UP     swp16        100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl(UP)
```

10. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

    `nv show interface lldp`

    Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
cumulus@sw1:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1              e3a
swp4       100G   Trunk/L2    node2              e3a
swp15      100G   BondMember  nsw2               swp15
swp16      100G   BondMember  nsw2               swp16


cumulus@nsw2:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost         RemotePort
---------  -----  ----------  -----------------  -----------
swp3       100G   Trunk/L2    node1                e3b
swp4       100G   Trunk/L2    node2                e3b
swp15      100G   BondMember  sw1                swp15
swp16      100G   BondMember  sw1                swp16
```

11. Automatische Wiederherstellung der Cluster-LIFs aktivieren:

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

12. Schalten Sie auf Switch nsw2 die Ports ein, die mit den Netzwerkports der Knoten verbunden sind.

    ```
    cumulus@nsw2:~$ nv set interface swp1-14 link state up
    cumulus@nsw2:~$ nv config apply
    ```

13. Informationen über die Knoten in einem Cluster anzeigen:

    ```
    cluster show
    ```

    Dieses Beispiel zeigt, dass der Knotenstatus für Knoten 1 und Knoten 2 in diesem Cluster „true“ ist:

    ```
    cluster1::*> cluster show

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

14. Überprüfen Sie, ob alle physischen Cluster-Ports aktiv sind:

    ```
    network port show ipspace Cluster
    ```

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

Node node1
Ignore
                                                        Speed(Mbps)
Health   Health
Port      IPspace     Broadcast Domain  Link  MTU   Admin/Oper
Status   Status
--------- ----------- ----------------- ----- ----- -----------
-------- ------
e3a       Cluster     Cluster           up    9000  auto/10000
healthy  false
e3b       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
--------- ------------ ---------------- ----- ----- -----------
-------- ------
e3a       Cluster      Cluster          up    9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up    9000  auto/10000
healthy  false
```

Schritt 3: Konfiguration überprüfen

Cumulus Linux 4.4.3

1. Überprüfen Sie, ob das Clusternetzwerk fehlerfrei funktioniert.

```
cumulus@sw1:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost      RemotePort
---------  -----  ----------  --------------  -----------
swp3       100G   Trunk/L2    node1           e3a
swp4       100G   Trunk/L2    node2           e3a
swp15      100G   BondMember  nsw2            swp15
swp16      100G   BondMember  nsw2            swp16
```

Cumulus Linux 5.x

1. Überprüfen Sie, ob das Clusternetzwerk fehlerfrei funktioniert.

```
cumulus@sw1:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost      RemotePort
---------  -----  ----------  --------------  -----------
swp3       100G   Trunk/L2    node1           e3a
swp4       100G   Trunk/L2    node2           e3a
swp15      100G   BondMember  nsw2            swp15
swp16      100G   BondMember  nsw2            swp16
```

1. [[Schritt 2]] Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

2. Wenn Sie die automatische Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

Nachdem Sie Ihre Schalter ausgetauscht haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Ersetzen Sie die NVIDIA SN2100 Cluster-Switches durch switchlose Verbindungen.

Für ONTAP 9.3 und höher können Sie von einem Cluster mit einem Switched-Cluster-Netzwerk zu einem Cluster migrieren, in dem zwei Knoten direkt miteinander verbunden sind.

Überprüfungsanforderungen

Richtlinien

Bitte beachten Sie die folgenden Richtlinien:

- Die Migration zu einer Zwei-Knoten-Clusterkonfiguration ohne Switches ist ein unterbrechungsfreier Vorgang. Die meisten Systeme verfügen über zwei dedizierte Cluster-Interconnect-Ports pro Knoten. Dieses Verfahren kann aber auch für Systeme mit einer größeren Anzahl dedizierter Cluster-Interconnect-Ports pro Knoten angewendet werden, beispielsweise vier, sechs oder acht.
- Die Funktion „Switchless Cluster Interconnect“ kann nicht mit mehr als zwei Knoten verwendet werden.
- Wenn Sie über einen bestehenden Zwei-Knoten-Cluster verfügen, der Cluster-Interconnect-Switches verwendet und auf dem ONTAP 9.3 oder höher läuft, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Knoten ersetzen.

Bevor Sie beginnen

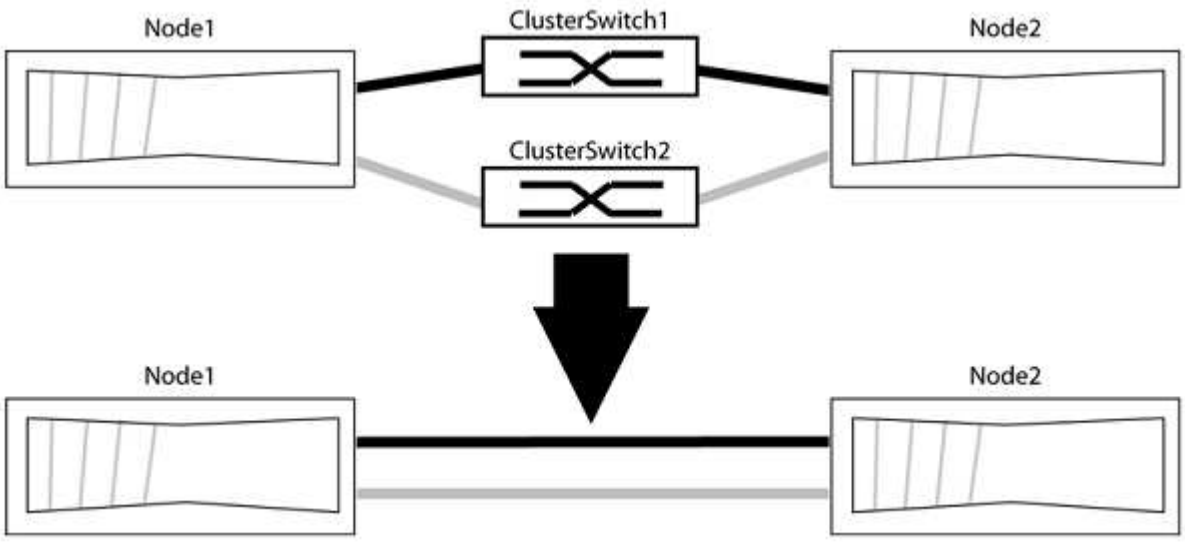
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesunder Cluster, der aus zwei Knoten besteht, die über Cluster-Switches verbunden sind. Auf den Knoten muss die gleiche ONTAP Version laufen.
- Jeder Knoten verfügt über die erforderliche Anzahl dedizierter Cluster-Ports, die redundante Cluster-Verbindungen bereitstellen, um Ihre Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster-Verbindungsports auf jedem Knoten.

Migrieren Sie die Schalter

Informationen zu diesem Vorgang

Das folgende Verfahren entfernt die Cluster-Switches in einem Zwei-Knoten-Cluster und ersetzt jede Verbindung zum Switch durch eine direkte Verbindung zum Partnerknoten.



Zu den Beispielen

Die Beispiele im folgenden Verfahren zeigen Knoten, die "e0a" und "e0b" als Cluster-Ports verwenden. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.

Schritt 1: Vorbereitung auf die Migration

1. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung `*>` erscheint.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von switchlosen Clustern, die standardmäßig aktiviert ist.

   Sie können überprüfen, ob die Erkennung von Clustern ohne Switch aktiviert ist, indem Sie den Befehl mit erweiterten Berechtigungen ausführen:

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

   Beispiel anzeigen

   Die folgende Beispielausgabe zeigt, ob die Option aktiviert ist.

   ```
   cluster::*> network options detect-switchless-cluster show
      (network options detect-switchless-cluster show)
   Enable Switchless Cluster Detection: true
   ```

   Wenn "Schalterlose Clustererkennung aktivieren" `false` Wenden Sie sich an den NetApp Support.

3. 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=<number_of_hours>h
   ```

   Wo `h` ist die Dauer des Wartungsfensters in Stunden. Die Meldung informiert den technischen Support über diese Wartungsaufgabe, damit dieser die automatische Fallerstellung während des Wartungsfensters unterdrücken kann.

   Im folgenden Beispiel unterdrückt der Befehl die automatische Fallerstellung für zwei Stunden:

   Beispiel anzeigen

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

Schritt 2: Anschlüsse und Verkabelung konfigurieren

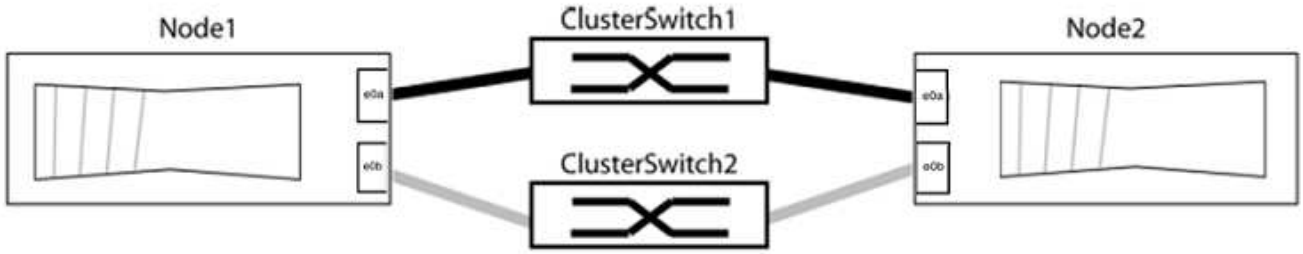
1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen ein, sodass die Cluster-Ports in Gruppe 1 an Cluster-Switch 1 und die Cluster-Ports in Gruppe 2 an Cluster-Switch 2 angeschlossen werden. Diese

Gruppen werden im weiteren Verlauf des Verfahrens benötigt.

2. Identifizieren Sie die Cluster-Ports und überprüfen Sie den Verbindungsstatus und die Integrität:

   `network port show -ipspace Cluster`

   Im folgenden Beispiel für Knoten mit Cluster-Ports „e0a“ und „e0b“ wird eine Gruppe als „node1:e0a“ und „node2:e0a“ und die andere Gruppe als „node1:e0b“ und „node2:e0b“ identifiziert. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



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

Beispiel anzeigen

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Vergewissern Sie sich, dass alle Cluster-LIFs an ihren jeweiligen Heimatports angeschlossen sind.

   Überprüfen Sie, ob die Spalte „is-home“ `true` für jeden der Cluster-LIFs:

   `network interface show -vserver Cluster -fields is-home`

Beispiel anzeigen

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Falls Cluster-LIFs vorhanden sind, die sich nicht auf ihren Heimatports befinden, werden diese LIFs wieder auf ihre Heimatports zurückgesetzt:

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

4. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

5. Überprüfen Sie, ob alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

   In der Spalte „Erkanntes Gerät“ sollte der Name des Cluster-Switches stehen, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports "e0a" und "e0b" korrekt mit den Cluster-Switches "cs1" und "cs2" verbunden sind.

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 7]] Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster ring show
   ```

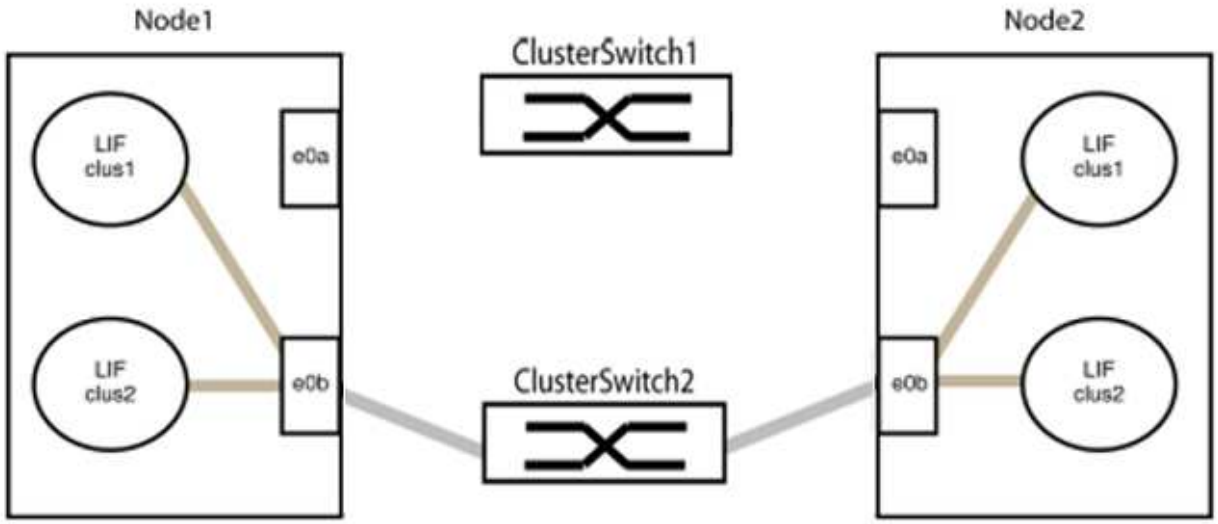
   Alle Einheiten müssen entweder Master- oder Sekundäreinheiten sein.

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

   > Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe1 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

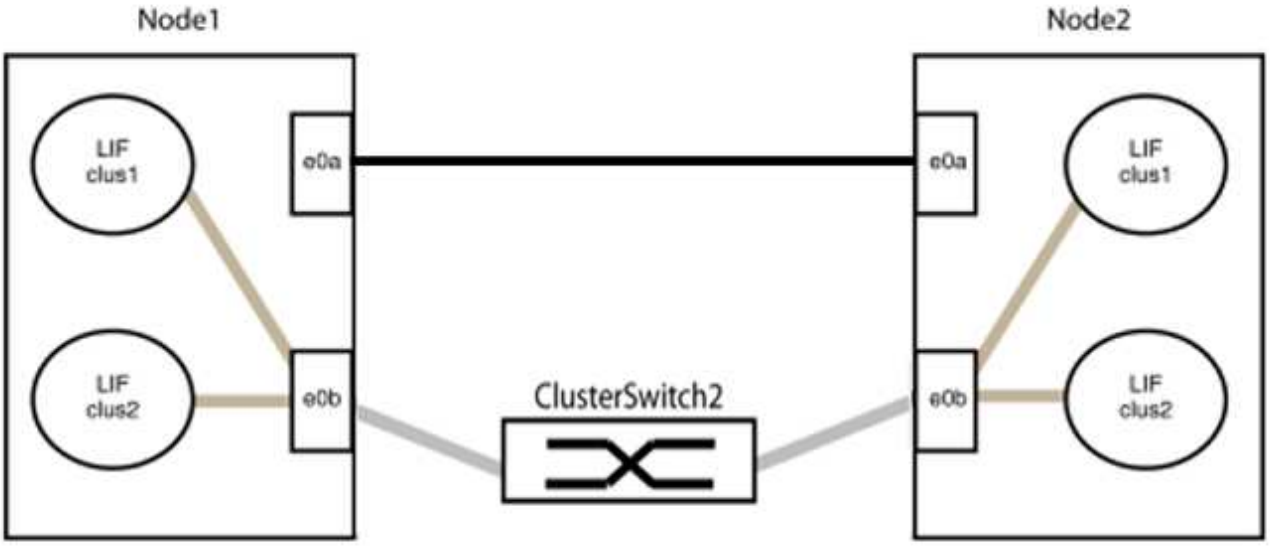
   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

      Im folgenden Beispiel werden die Kabel an Port „e0a“ auf jedem Knoten getrennt, und der Cluster-Datenverkehr wird weiterhin über den Switch und Port „e0b“ auf jedem Knoten abgewickelt:



b. Verbinden Sie die Ports in Gruppe 1 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden:



3. Die Option für ein schalterloses Clusternetzwerk wechselt von `false` Zu `true` Die Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „Schalterlos“ aktiviert ist. `true` :

`network options switchless-cluster show`

Das folgende Beispiel zeigt, dass der switchlose Cluster aktiviert ist:

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

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

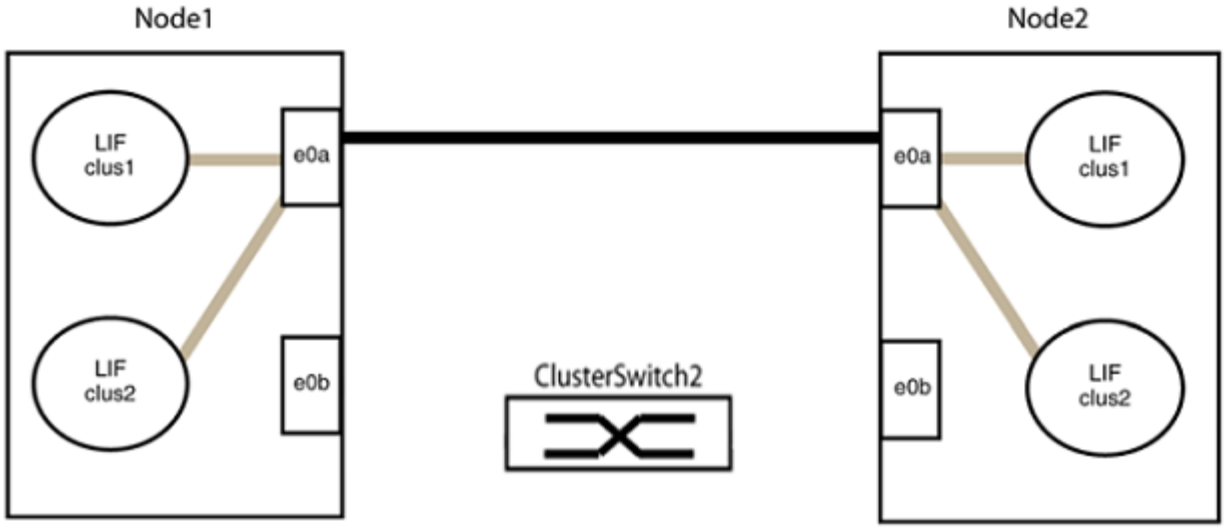
Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung in Gruppe 1 zu bestätigen.

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

   Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe 2 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 2.

      Im folgenden Beispiel werden die Kabel von Port "e0b" an jedem Knoten getrennt, und der Cluster-Datenverkehr wird über die direkte Verbindung zwischen den Ports "e0a" fortgesetzt:



b. Verbinden Sie die Ports in Gruppe 2 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden und "e0b" auf Knoten 1 ist mit "e0b" auf Knoten 2 verbunden:

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie, ob die Ports an beiden Knoten korrekt verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port des Cluster-Partners verbunden sind:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Automatische Rücksetzung für die Cluster-LIFs wieder aktivieren:

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

3. Überprüfen Sie, ob alle LIFs zu Hause sind. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „Ist zu Hause“ den Wert „Ist zu Hause“ aufweist. `true` , wie gezeigt für `node1_clus2` Und `node2_clus2` im folgenden Beispiel:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif          curr-port is-home
-------- ------------ --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

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

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

4. Überprüfen Sie den Clusterstatus der Knoten über die Systemkonsole eines der beiden Knoten:

   `cluster show`

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass epsilon an beiden Knoten gleich ist. `false` :

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 entries were displayed.
   ```

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

ONTAP 9.9.1 und höher

Sie können 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
------ ------------------------- ---------------- ----------------
-----------
node1
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)

Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Falls Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

   Weitere Informationen finden Sie unter "NetApp KB-Artikel 1010449: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster".

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

Wie geht es weiter?

Nachdem Sie Ihre Schalter ausgetauscht haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die