



Switch-Dokumentation für ONTAP Hardwaresysteme

Cluster and storage switches

NetApp
April 25, 2024

Inhalt

Switch-Dokumentation für ONTAP Hardwaresysteme	1
Los geht's	2
Was ist neu für Schalter	2
Erfahren Sie mehr über Cluster, Storage und Shared Switches	3
Die Systeme sind betriebsbereit mit Cluster, Storage und Shared Switches	4
Cluster-Switches	7
Von Broadcom unterstützte BES-53248	7
Cisco Nexus 9336C-FX2	147
NVIDIA SN2100	304
Storage Switches	456
Cisco Nexus 9336C-FX2	456
NVIDIA SN2100	527
Shared-Switches	579
Cisco Nexus 9336C-FX2	579
Switches für das Ende der Verfügbarkeit	702
End-of-Verfügbarkeit	702
Cisco Nexus 3232C	702
Cisco Nexus 3132Q-V	913
Cisco Nexus 92300YC	1111
NetApp CN1610	1235
Rechtliche Hinweise	1318
Urheberrecht	1318
Marken	1318
Patente	1318
Datenschutzrichtlinie	1318

Switch-Dokumentation für ONTAP Hardwaresysteme

Los geht's

Was ist neu für Schalter

Erfahren Sie mehr über die neuen Switches für FAS und AFF Systeme.

Unterstützung für neue Switches

Schalter	Beschreibung	Verfügbar ab
"100 GbE Cisco Switch mit 36 Ports (X190200)"	Unterstützung einer Shared IT-Infrastruktur (Cluster, HA und Switch-Attached Storage) auf demselben Paar Cisco Nexus 9336C-FX2 Switches, einschließlich Unterstützung für MetroCluster IP-Konfigurationen.	ONTAP 9.9.1
"100-GbE-Cisco-Switch mit 36 Ports (X190200 und X190210)"	Cisco Nexus 9336C-FX2 Cluster-Interconnect-Switch und Storage-Switch-Unterstützung für All Flash FAS/FAS Controller sowie für Front-End-Konnektivität für Daten	ONTAP 9.8
"Broadcom BES-53248 Switch (X190005 und X190005R)"	Unterstützung von Broadcom BES-53248 Cluster-Interconnect-Switches für All Flash FAS/FAS Controller mit 40/100-GbE-Ports	ONTAP 9.8
"100 GbE Cisco Switch mit 36 Ports (X190200)" "100 GbE Cisco Switch mit 32 Ports (X190100 und X190100R)"	Cisco Nexus 100 GbE Switch kann als dedizierter Storage-Switch verwendet werden, um NS224 NVMe Laufwerk-Shelfs mit folgenden Plattformen zu verbinden: <ul style="list-style-type: none">• AFF A800/AFF ASA A800• AFF A700/AFF ASA A700• AFF A400/AFF ASA A400• AFF A320	ONTAP 9.8
"Broadcom BES-53248 Switch (X190005 und X190005R)"	Unterstützung von Broadcom BES-53248 Cluster-Interconnect-Switches für All Flash FAS/FAS Controller mit 10/25-GbE-Ports	ONTAP 9.5P8

Erfahren Sie mehr über Cluster, Storage und Shared Switches

NetApp bietet Cluster-, Storage- und Shared-Switches, die interne Kommunikation mit der Möglichkeit bieten, Daten und Netzwerkschnittstellen innerhalb des Clusters unterbrechungsfrei zu verschieben.

Die „Front-End“-Switches sorgen für Konnektivität mit Host Storage, während die „Back-End“-Cluster-Switches Verbindungen zwischen zwei oder mehr NetApp Controllern ermöglichen.



Es werden nur von NetApp validierte Back-End Switches (im Auftrag von NetApp) unterstützt.

Cluster-Switches

Dank Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Nodes erstellen. Von NetApp unterstützte Cluster-Switches:

- Broadcom BES-53248
- Cisco Nexus 9336C-FX2
- NVIDIA SN2100

Storage Switches

Storage-Switches ermöglichen das Routen von Daten zwischen Servern und Storage Arrays in einem Storage Area Network (SAN). Von NetApp unterstützte Cluster-Switches:

- Cisco Nexus 9336C-FX2
- NVIDIA SN2100

Shared-Switches

Mit Shared Switches können Sie Cluster- und Storage-Funktionen zu einer Shared-Switch-Konfiguration kombinieren, indem Sie gemeinsam genutzte Cluster- und Storage-RCFs unterstützen. Der von NetApp unterstützte Shared-Switch ist:

- Cisco Nexus 9336C-FX2

End-of-Verfügbarkeit

Folgende Storage Switches sind nicht mehr erhältlich. Sie werden jedoch weiterhin unterstützt:

- Cisco Nexus 3232C
- Cisco Nexus 3132Q-V
- Cisco Nexus 92300YC
- NetApp CN1610

Die Systeme sind betriebsbereit mit Cluster, Storage und Shared Switches

Um Cluster-, Storage- und Shared-Switches in Betrieb zu nehmen, installieren Sie Hardwarekomponenten und konfigurieren Ihren Switch.

Die Bereitstellung des Switches umfasst den folgenden Workflow.

1

Installieren Sie AFF/FAS Controller

Installieren Sie Ihre All Flash FAS/FAS Controller im Rack oder Schrank. Installations- und Setup-Anleitung für Ihr All Flash FAS/FAS Plattformmodell erhalten Sie hier.

AFF Systeme	FAS Systeme	
<ul style="list-style-type: none">• "AFF C 190"• "AFF A220"• "AFF A250"• "AFF A400"• "AFF A700"• "AFF A800"• "AFF A900"	<ul style="list-style-type: none">• "FAS500f"• "FAS8300"• "FAS8700"• "FAS9000"• "FAS9500"	

2

Die Switch-Hardware einbauen

Installieren Sie Ihre Switches im Rack oder Schrank. Lesen Sie die folgenden Anweisungen für Ihr Switch-Modell.

Cluster-Switches	Storage Switches	Shared-Switches
<ul style="list-style-type: none">• "Installieren Sie den BES-53248-Switch"• "Installieren Sie den Cisco Nexus 9336C-FX2 Switch"• "Installieren Sie den NVIDIA SN2100-Switch"	<ul style="list-style-type: none">• "Installieren Sie den Cisco Nexus 9336C-FX2 Switch"• "Installieren Sie den NVIDIA SN2100-Switch"	<ul style="list-style-type: none">• "Installieren Sie den Cisco Nexus 9336C-FX2 Switch"

3

Verkabeln Sie die Switches mit den Controllern

Die Installations- und Setup-Anleitung für AFF/FAS enthält Anweisungen zur Verkabelung der Controller-Ports mit dem Switch. Wenn Sie jedoch Listen mit unterstützten Kabeln und Transceivern sowie detaillierte Informationen zu den Host-Ports für Ihren Switch benötigen, greifen Sie auf die folgenden Anweisungen für Ihr Switch-Modell zu.

	Cluster-Switches <ul style="list-style-type: none"> • "BES-53248-Schalter verkabeln" • "Cisco Nexus 9336C-FX2-Switch verkabeln" • "Verkabeln Sie den NVIDIA SN2100-Switch" 	Storage Switches <ul style="list-style-type: none"> • "Cisco Nexus 9336C-FX2-Switch verkabeln" • "Verkabeln Sie den NVIDIA SN2100-Switch" 	Shared-Switches <ul style="list-style-type: none"> • "Cisco Nexus 9336C-FX2-Switch verkabeln"
--	--	--	---

4

Konfigurieren Sie den Switch

Führen Sie eine Ersteinrichtung Ihrer Switches durch. Lesen Sie die folgenden Anweisungen für Ihr Switch-Modell.

	Cluster-Switches <ul style="list-style-type: none"> • "Konfigurieren Sie den BES-53248-Switch" • "Konfigurieren Sie den Cisco Nexus 9336C-FX2 Switch" • "Konfigurieren Sie den NVIDIA SN2100-Switch" 	Storage Switches <ul style="list-style-type: none"> • "Konfigurieren Sie den Cisco Nexus 9336C-FX2 Switch" • "Konfigurieren Sie den NVIDIA SN2100-Switch" 	Shared-Switches <ul style="list-style-type: none"> • "Konfigurieren Sie den Cisco Nexus 9336C-FX2 Switch"
--	--	--	---

5

Installation der Switch-Software

Um die Software auf Ihrem Switch zu installieren und zu konfigurieren, folgen Sie dem Workflow für die Softwareinstallation Ihres Switch-Modells.

	Cluster-Switches <ul style="list-style-type: none"> • "Installation der Software für BES-53248-Switches" • "Installieren Sie Software für Cisco Nexus 9336C-FX2 Switch" • "Software für NVIDIA SN2100-Switch installieren" 	Storage Switches <ul style="list-style-type: none"> • "Installieren Sie Software für Cisco Nexus 9336C-FX2 Switch" • "Software für NVIDIA SN2100-Switch installieren" 	Shared-Switches <ul style="list-style-type: none"> • "Installieren Sie Software für Cisco Nexus 9336C-FX2 Switch"
--	--	--	---

6

Schließen Sie die System-Einrichtung ab

Nachdem die Switches konfiguriert und die erforderliche Software installiert wurden, rufen Sie die Installations- und Setup-Anleitung für das All Flash FAS/FAS Plattformmodell auf, um das System vollständig einzurichten.

	AFF Systeme <ul style="list-style-type: none"> • "AFF C 190" • "AFF A220" • "AFF A250" • "AFF A400" • "AFF A700" • "AFF A800" • "AFF A900" 	FAS Systeme <ul style="list-style-type: none"> • "FAS500f" • "FAS8300" • "FAS8700" • "FAS9000" • "FAS9500" 	
--	--	--	--

7

Schließen Sie die ONTAP-Konfiguration ab

Nachdem die All Flash FAS/FAS Controller und Switches installiert und eingerichtet wurden, müssen Sie die Konfiguration des Storage in ONTAP abschließen. Greifen Sie entsprechend der Bereitstellungskonfiguration auf die folgenden Anweisungen zu.

- Informationen zu ONTAP-Implementierungen finden Sie unter ["Konfigurieren Sie ONTAP"](#).
- Informationen zu ONTAP mit MetroCluster Implementierungen finden Sie unter ["Konfigurieren Sie MetroCluster mit ONTAP"](#).

Cluster-Switches

Von Broadcom unterstützte BES-53248

Überblick

Überblick über die Installation und Konfiguration von BES-53248-Switches

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

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen BES-53248-Cluster-Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Installieren Sie die Hardware für den BES-53248 Cluster-Switch"](#).

Anweisungen hierzu finden Sie im Installationshandbuch für den Cluster Switch *Broadcom-unterstützte BES-53248 Cluster Switch*.

2. ["Konfigurieren Sie den BES-53248 Cluster-Switch"](#).

Führen Sie eine Ersteinrichtung des BES-53248-Cluster-Switch durch.

3. ["Installieren Sie die EFOS-Software"](#).

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

4. ["Installation von Lizenzen für BES-53248 Cluster-Switches"](#).

Optional können Sie neue Ports durch den Kauf und die Installation weiterer Lizenzen hinzufügen. Das Switch-Basismodell ist für 16 10-GbE- oder 25-GbE-Ports und zwei 100-GbE-Ports lizenziert.

5. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)."](#)

Installieren oder aktualisieren Sie die RCF auf dem BES-53248 Cluster-Switch und überprüfen Sie nach der Anwendung des RCF die Ports für eine zusätzliche Lizenz.

6. ["Installieren Sie die Konfigurationsdatei des Cluster Switch Health Monitor \(CSHM\)"](#).

Installieren Sie die entsprechende Konfigurationsdatei für das Monitoring des Clusterstatus.

7. ["Aktivieren Sie SSH bei BES-53248 Cluster-Switches"](#).

Wenn Sie den Cluster Switch Health Monitor (CSHM) und die Funktionen zur Protokollerfassung verwenden, aktivieren Sie SSH auf den Switches.

8. ["Aktivieren Sie die Protokollerfassungsfunktion"](#).

Verwenden Sie die Protokollerfassungsfunktionen, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)

Konfigurationsanforderungen für BES-53248 Cluster Switches

Für die Installation und Wartung von BES-53248-Switches müssen die Support- und Konfigurationsanforderungen für EFOS und ONTAP überprüft werden.

EFOS- und ONTAP-Unterstützung

Siehe ["NetApp Hardware Universe"](#) Und ["Kompatibilitätsmatrix für Broadcom Switches"](#) Für Informationen zur EFOS- und ONTAP-Kompatibilität mit BES-53248-Switches. Die Unterstützung von EFOS und ONTAP kann je nach Maschinentyp des BES-53248-Switches variieren. Weitere Informationen zu allen BES-52348-Schaltmaschinentypen finden Sie unter ["Komponenten und Teilenummern für BES-53248 Cluster-Switches"](#).

Konfigurationsanforderungen

Zum Konfigurieren eines Clusters benötigen Sie die entsprechende Anzahl und den entsprechenden Kabeltyp und Kabelanschlüsse für die Cluster-Switches. Je nach Art des zu Beginn konfiguriert-Cluster-Switch müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen.

Zuweisung von Cluster-Switch-Ports

Sie können die von Broadcom unterstützte Tabelle zur Konfiguration des Clusters für die Zuweisung von BES-53248-Cluster-Switches als Leitfaden verwenden.

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

Siehe ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

Einschränkung bei der Geschwindigkeit der Port-Gruppe

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

Zusätzlichen Anforderungen

- Informationen zum Erwerb zusätzlicher Lizenzen finden Sie unter ["Aktivieren Sie neu lizenzierende Ports"](#) Für Details, wie sie aktiviert werden.
- Wenn SSH aktiv ist, müssen Sie es nach dem Ausführen des Befehls manuell erneut aktivieren `erase startup-config` Und den Switch neu zu starten.

Komponenten und Teilenummern für BES-53248 Cluster-Switches

Prüfen Sie für die Installation und Wartung von BES-53248-Switches die Liste der Komponenten und Teilenummern.

In der folgenden Tabelle sind die Teilenummer, die Beschreibung und die Mindestversionen von EFOS und ONTAP für die Komponenten des BES-53248-Cluster-Switches aufgeführt, einschließlich Details zum Rack-Befestigungsschienen-Kit.



Für die Teilenummern **X190005-B** und **X190005R-B** ist eine EFOS-Mindestversion von **3.10.0.3** erforderlich.

Teilenummer	Beschreibung	Minimale EFOS-Version	Minimale ONTAP-Version
X190005-B	BES-53248-B/IX8, CLSW, 16PT10/25GB, PTSX (PTSX = Port Side Exhaust)	3.10.0.3	9.8
X190005R-B	BES-53248-B/IX8, CLSW, 16PT10/25 GB, PSIN (PSIN = Port Side Intake)	3.10.0.3	9.8
X190005	BES-53248, CLSW, 16PT10/25 GB, PTSX, BRDCM-SUPPORT	3.4.4.6	9.5P8
X190005R	BES-53248, CLSW, 16PT10/25 GB, PSIN, BRDCM-SUPPORT	3.4.4.6	9.5P8
X-RAIL-4POST-190005	Rack Mount Rail Kit Ozeki 4 Post 19 Zoll	1. A.	1. A.



Beachten Sie die folgenden Informationen bezüglich Maschinentypen:

Maschinentyp	EFOS-Version
BES-53248A1	3.4.4.6
BES-53248A2	3.10.0.3
BES-53248A3	3.10.0.3

Sie können Ihren spezifischen Maschinentyp mit dem folgenden Befehl bestimmen: `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..... QTCU225xxxxx  
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  
.  
.  
.
```

Dokumentationsanforderungen für BES-53248-Cluster-Switches

Überprüfen Sie für BES-53248-Switch-Installation und -Wartung die spezifische Switch- und Controller-Dokumentation.

Broadcom-Dokumentation

Zum Einrichten des BES-53248-Cluster-Switches benötigen Sie die folgenden Dokumente, die über die Broadcom Support Site verfügbar sind: ["Produkte Der Broadcom Ethernet-Switches-Reihe"](#)

Dokumenttitel	Beschreibung
<i>EFOS Administratorhandbuch</i> v3.4.3	Enthält Beispiele für die Verwendung des BES-53248-Switches in einem typischen Netzwerk.
<i>EFOS CLI Command Reference</i> v3.4.3	Beschreibt die Befehle der Befehlszeilenschnittstelle (CLI), mit denen Sie die BES-53248-Software anzeigen und konfigurieren können.
<i>EFOS Handbuch erste Schritte</i> v3.4.3	Enthält detaillierte Informationen zum BES-53248-Switch.
<i>EFOS SNMP-Referenzhandbuch</i> v3.4.3	Enthält Beispiele für die Verwendung des BES-53248-Switches in einem typischen Netzwerk.

Dokumenttitel	Beschreibung
<i>EFOS-Skalierungsparameter und Werte v3.4.3</i>	Beschreibt die Standard-Skalierungsparameter, mit denen EFOS-Software auf den unterstützten Plattformen bereitgestellt und validiert wird.
<i>EFOS Funktionsspezifikationen v3.4.3</i>	Beschreibt die Spezifikationen für die EFOS-Software auf den unterstützten Plattformen.
<i>EFOS Release Notes Version 3.4.3</i>	Enthält Release-spezifische Informationen zur BES-53248-Software.
<i>Kompatibilitätsmatrix für Cluster-Netzwerk und Management-Netzwerk</i>	Bietet Informationen zur Netzwerkkompatibilität. Die Matrix ist über die BES-53248 Switch Download-Site unter erhältlich "Broadcom Cluster-Switches" .

Dokumentation zu ONTAP Systemen und KB-Artikel

Um ein ONTAP System einzurichten, benötigen Sie die folgenden Dokumente über die NetApp Support Site unter ["mysupport.netapp.com"](https://mysupport.netapp.com) Oder die Knowledgebase (KB)-Website unter ["kb.netapp.com"](https://kb.netapp.com).

Name	Beschreibung
"NetApp Hardware Universe"	Beschreibt die Anforderungen an Stromversorgung und Standort für die gesamte NetApp Hardware, einschließlich System-Cabinets, und bietet Informationen zu den entsprechenden Anschlüssen und Kabeloptionen zur Verwendung zusammen mit den Teilenummern.
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP 9	Enthält ausführliche Informationen zu allen Aspekten der Version ONTAP 9.
<i>Hinzufügen zusätzlicher Portlizenzen für den von Broadcom unterstützten BES-53248 Switch</i>	Enthält detaillierte Informationen zum Hinzufügen von Portlizenzen. Wechseln Sie zum "KB-Artikel" .

Hardware installieren

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

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

Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen im ["Von Broadcom unterstützte Installationshandbuch für den BES-53248 Cluster Switch"](#).

Was kommt als Nächstes?

["Konfigurieren Sie den Switch"](#).

Konfigurieren Sie den BES-53248 Cluster-Switch

Führen Sie diese Schritte aus, um eine Ersteinrichtung des BES-53248-Cluster-Switches durchzuführen.

Bevor Sie beginnen

- Die Hardware wird installiert, wie in beschrieben ["Installieren Sie die Hardware"](#).
- Sie haben die folgenden Punkte überprüft:
 - ["Konfigurationsanforderungen"](#)
 - ["Komponenten und Teilenummern"](#)
 - ["Dokumentationsanforderungen"](#)

Zu den Beispielen

In den Beispielen der Konfigurationsverfahren wird die folgende Nomenklatur für Switches und Knoten verwendet:

- Die NetApp Switch-Namen sind `cs1` Und `cs2`. Das Upgrade beginnt auf dem zweiten Switch, `cs2`.
- Die LIF-Namen des Clusters sind `node1_clus1` Und `node1_clus2` Für Node1, und `node2_clus1` Und `node2_clus2` Für Knoten 2.
- Der IPspace Name ist der Cluster.
- Der `cluster1 :>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die Cluster-Ports an jedem Node werden mit benannt `e0a` Und `e0b`. Siehe ["NetApp Hardware Universe"](#) Für die tatsächlichen Cluster-Ports, die auf Ihrer Plattform unterstützt werden.
- Die von NetApp Switches unterstützten Inter-Switch Links (ISLs) sind die Ports 0/55 und 0/56.
- Die für NetApp Switches unterstützten Node-Verbindungen sind die Ports 0/1 bis 0/16 mit Standardlizenz.
- Die Beispiele verwenden zwei Nodes, Sie können jedoch bis zu 24 Nodes in einem Cluster haben.

Schritte

1. Verbinden Sie den seriellen Port mit einem Host oder einem seriellen Port.
2. Verbinden Sie den Verwaltungsport (den RJ-45-Schraubenschlüssel-Port auf der linken Seite des Switches) mit dem gleichen Netzwerk, in dem sich Ihr TFTP-Server befindet.
3. Legen Sie an der Konsole die seriellen Host-Einstellungen fest:
 - 115200 Baud
 - 8 Datenbits
 - 1 Stoppbit
 - Parität: Keine
 - Flusskontrolle: Keine
4. Melden Sie sich beim Switch an `admin` Und drücken Sie **Enter**, wenn Sie zur Eingabe eines Kennworts aufgefordert werden. Der Standard-Switch-Name lautet **Routing**. Geben Sie an der Eingabeaufforderung ein `enable`. Dadurch haben Sie Zugriff auf den privilegierten EXEC-Modus für die Switch-Konfiguration.

Beispiel anzeigen

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

5. Ändern Sie den Switch-Namen in **cs2**.

Beispiel anzeigen

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

6. Verwenden Sie zum Festlegen einer statischen IP-Adresse das `serviceport protocol`, `network protocol`, und `serviceport ip` Befehle, wie im Beispiel gezeigt.

für den serviceport ist standardmäßig DHCP verwendet. Die IP-Adresse, die Subnetzmaske und die Standard-Gateway-Adresse werden automatisch zugewiesen.

Beispiel anzeigen

```
(cs2) # serviceport protocol none  
(cs2) # network protocol none  
(cs2) # serviceport ip ipaddr netmask gateway
```

7. Überprüfen Sie die Ergebnisse mit dem Befehl:

```
show serviceport
```

Beispiel anzeigen

```
(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
```

8. Konfigurieren Sie die Domäne und den Namensserver:

configure

Beispiel anzeigen

```
(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) (Config)#
```

9. Konfigurieren Sie den NTP-Server.

a. Konfigurieren der Zeitzone und der Zeitsynchronisierung (SNTP):

sntp

Beispiel anzeigen

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

Verwenden Sie für EFOS Version 3.10.0.3 und höher den Befehl `ntp`.

`ntp`

Beispiel anzeigen

```
(cs2) configure  
(cs2) (Config) # ntp ?  
  
authenticate          Enables NTP authentication.  
authentication-key     Configure NTP authentication key.  
broadcast             Enables NTP broadcast mode.  
broadcastdelay        Configure NTP broadcast delay in  
microseconds.  
server               Configure NTP server.  
source-interface      Configure the NTP source-interface.  
trusted-key          Configure NTP authentication key number  
for trusted time source.  
vrf                  Configure the NTP VRF.  
  
(cs2) (Config) # ntp server ?  
  
ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address  
or hostname.  
  
(cs2) (Config) # ntp server 10.99.99.5
```

b. Konfigurieren Sie die Zeit manuell:

`clock`

Beispiel anzeigen

```
(cs2)# config
(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 10/20/2020

(cs2) (Config)# show clock

07:00:11 EST(UTC-5:00) Oct 20 2020
No time source

(cs2) (Config)# exit

(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!
```

Was kommt als Nächstes?

["Installieren Sie die EFOS-Software".](#)

Software konfigurieren

Workflow für die Softwareinstallation für BES-53248-Switches

Gehen Sie wie folgt vor, um die Software für einen BES-53248 Cluster-Switch zu installieren und zu konfigurieren:

1. ["Installieren Sie die EFOS-Software".](#)

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

2. ["Installation von Lizenzen für BES-53248 Cluster-Switches".](#)

Optional können Sie neue Ports durch den Kauf und die Installation weiterer Lizenzen hinzufügen. Das

Switch-Basismodell ist für 16 10-GbE- oder 25-GbE-Ports und zwei 100-GbE-Ports lizenziert.

3. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)".](#)

Installieren oder aktualisieren Sie die RCF auf dem BES-53248 Cluster-Switch und überprüfen Sie nach der Anwendung des RCF die Ports für eine zusätzliche Lizenz.

4. ["Installieren Sie die Konfigurationsdatei des Cluster Switch Health Monitor \(CSHM\)".](#)

Installieren Sie die entsprechende Konfigurationsdatei für das Monitoring des Clusterstatus.

5. ["Aktivieren Sie SSH bei BES-53248 Cluster-Switches".](#)

Wenn Sie den Cluster Switch Health Monitor (CSHM) und die Funktionen zur Protokollerfassung verwenden, aktivieren Sie SSH auf den Switches.

6. ["Aktivieren Sie die Protokollerfassungsfunktion".](#)

Verwenden Sie diese Funktion, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

Installieren Sie die EFOS-Software

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

EFOS Software umfasst eine Reihe erweiterter Netzwerkfunktionen und Protokolle für die Entwicklung von Ethernet- und IP-Infrastruktursystemen. Diese Softwarearchitektur ist für jedes Netzwerkorganisationsgerät geeignet, das Anwendungen verwendet, die eine gründliche Paketinspektion oder -Trennung erfordern.

Installation vorbereiten

Bevor Sie beginnen

- Laden Sie die entsprechende Broadcom EFOS-Software für Ihre Cluster-Switches von [herunter](#) ["Unterstützung Für Broadcom Ethernet-Switches"](#) Standort.
- Lesen Sie die folgenden Hinweise zu EFOS-Versionen.


Beachten Sie Folgendes:

- Beim Upgrade von EFOS 3.4.x.x auf EFOS 3.7.x.x oder höher muss auf dem Switch EFOS 3.4.4.6 (oder höher 3.4.x.x-Version) ausgeführt werden. Wenn Sie vor dieser Version eine Version ausführen, aktualisieren Sie zuerst den Switch auf EFOS 3.4.4.6 (oder höher 3.4.x.x Version), und aktualisieren Sie dann den Switch auf EFOS 3.7.x.x oder höher.
- Die Konfiguration für EFOS 3.4.x.x und 3.7.x.x oder höher ist unterschiedlich. Wenn Sie die EFOS-Version von 3.4.x.x auf 3.7.x.x oder höher ändern oder umgekehrt, müssen Sie den Switch auf die Werkseinstellungen zurücksetzen und die RCF-Dateien für die entsprechende EFOS-Version werden (neu) angewendet. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.
- Ab EFOS Version 3.7.x.x oder höher ist eine FIPS-konforme Version und eine FIPS-konforme Version verfügbar. Verschiedene Schritte gelten für den Wechsel von einer nicht FIPS-konformen Version auf eine FIPS-konforme Version oder umgekehrt. Wenn EFOS von einer nicht FIPS-konformen Version oder umgekehrt geändert wird, wird der Switch auf die Werkseinstellungen zurückgesetzt. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.

Verfahren	Aktuelle EFOS-Version	* Neue EFOS-Version*	Hohe Stufen
Schritte zur Aktualisierung von EFOS zwischen zwei (nicht) FIPS-konformen Versionen	3.4.x.x	3.4.x.x	Installieren Sie das neue EFOS-Image mit Methode 1: EFOS installieren . Die Konfigurations- und Lizenzdaten bleiben erhalten.
3.4.4.6 (oder höher 3.4.x.x)	3.7.x.x oder höher ohne FIPS-konform	Aktualisieren von EFOS mit Methode 1: EFOS installieren . Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.7.x.x oder höher an.	3.7.x.x oder höher ohne FIPS-konform
3.4.4.6 (oder höher 3.4.x.x)	EFOS mit herabstufen Methode 1: EFOS installieren . Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.4.x.x an	3.7.x.x oder höher ohne FIPS-konform	
Installieren Sie das neue EFOS-Image mit Methode 1: EFOS installieren . Die Konfigurations- und Lizenzdaten bleiben erhalten.	3.7.x.x oder höher FIPS-konform	3.7.x.x oder höher FIPS-konform	Installieren Sie das neue EFOS-Image mit Methode 1: EFOS installieren . Die Konfigurations- und Lizenzdaten bleiben erhalten.
Schritte zum Upgrade auf/von einer FIPS-konformen EFOS-Version	Nicht FIPS-konform	FIPS-konform	Installation des EFOS-Images mit Methode 2: Aktualisieren von EFOS mit der ONIE OS-Installation . Informationen zur Switch-Konfiguration und -Lizenz 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.

- Ein-Schalter IP_Switch_a1:



```
IP_switch_a1 # *show fips status*

System running in FIPS mode
```

- Ein-Schalter IP_Switch_a2:

```
IP_switch_a2 # *show fips status*
                ^
% Invalid input detected at ``^` marker.
```

Installieren Sie die Software

Verwenden Sie eine der folgenden Methoden:

- [Methode 1: EFOS installieren](#). Verwenden Sie für die meisten Fälle (siehe Tabelle oben).
- [Methode 2: Aktualisieren von EFOS mit der ONIE OS-Installation](#). Verwenden Sie diese Option, wenn eine EFOS-Version FIPS-konform ist und die andere EFOS-Version nicht FIPS-konform ist.

Methode 1: EFOS installieren

Führen Sie die folgenden Schritte durch, um die EFOS-Software zu installieren oder zu aktualisieren.



Beachten Sie, dass nach dem Upgrade von BES-53248-Cluster-Switches von EFOS 3.3.x.x oder 3.4.x.x auf EFOS 3.7.0.4 oder 3.8.0.2 Inter-Switch Links (ISLs) und Port Channel im Status **Down** markiert sind. Lesen Sie diesen KB-Artikel: ["NDU für Cluster-Switch BES-53248 konnte nicht auf EFOS 3.7.0.4 und höher aktualisiert werden"](#) Entnehmen.

Schritte

1. Verbinden Sie den BES-53248-Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung mit dem Server, der EFOS, Lizenzen und der RCF-Datei hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch mit der IP-Adresse 172.19.2 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. Sichern Sie das aktuelle aktive Bild auf cs2:

```
show bootvar
```

Beispiel anzeigen

```
(cs2)# show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.3.3	Q.10.22.1	3.4.3.3	3.4.3.3

```
(cs2)# copy active backup
```

Copying active to backup

Management access will be blocked for the duration of the operation

Copy operation successful

```
(cs2)# show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.3.3	3.4.3.3	3.4.3.3	3.4.3.3

```
(cs2)#
```

4. Überprüfen Sie die laufende Version der EFOS-Software:

```
show version
```

Beispiel anzeigen

```
(cs2)# show version
```

```
Switch: 1
```

```
System Description..... BES-53248A1,
3.4.3.3, Linux 4.4.117-ceeeb99d, 2016.05.00.05
Machine Type..... BES-53248A1
Machine Model..... BES-53248
Serial Number..... QTFCU38260014
Maintenance Level..... A
Manufacturer..... 0xbc00
Burned In MAC Address..... D8:C4:97:71:12:3D
Software Version..... 3.4.3.3
Operating System..... Linux 4.4.117-
ceeeb99d
Network Processing Device..... BCM56873_A0
CPLD Version..... 0xff040c03

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

5. Laden Sie die Bilddatei auf den Switch herunter.

Durch Kopieren der Bilddatei auf das aktive Image wird bei einem Neustart die aktuell ausgeführte EFOS-Version erstellt. Das vorherige Bild bleibt als Backup verfügbar.

Beispiel anzeigen

```
(cs2)# copy sftp://root@172.19.2.1//tmp/EFOS-3.4.4.6.stk active
Remote Password:**

Mode..... SFTP
Set Server IP..... 172.19.2.1
Path..... //tmp/
Filename..... EFOS-3.4.4.6.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.
```

6. Anzeigen der Boot-Images für die aktive und die Backup-Konfiguration:

```
show bootvar
```

Beispiel anzeigen

```
(cs2)# show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash
-----
unit      active      backup      current-active      next-active
-----
1         3.4.3.3      3.4.3.3      3.4.3.3             3.4.4.6
```

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!
```

```
System will now restart!
```

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

```
show version
```

Beispiel anzeigen

```
(cs2)# show version
```

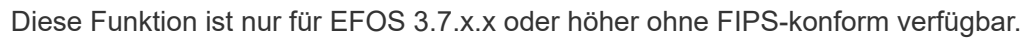
```
Switch: 1
```

```
System Description..... BES-53248A1,  
3.4.4.6, 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..... 3.4.4.6  
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
```

"Installation von Lizenzen für BES-53248 Cluster-Switches".

Sie können die folgenden Schritte durchführen, wenn eine EFOS-Version FIPS-konform ist und die andere EFOS-Version nicht FIPS-konform ist. Mit diesen Schritten kann das nicht-FIPS- oder FIPS-konforme EFOS 3.7.x.x-Image von ONIE installiert werden, wenn der Switch nicht startet.



1. Starten Sie den Schalter in den ONIE-Installationsmodus.

Beispiel anzeigen

EFOS

*ONIE

Nachdem Sie **ONIE** ausgewählt haben, lädt der Schalter und bietet Ihnen mehrere Auswahlmöglichkeiten. 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 Schalter startet in den ONIE-Installationsmodus.

2. Beenden Sie die ONIE-Erkennung, und konfigurieren Sie die Ethernet-Schnittstelle.

Wenn die folgende Meldung angezeigt wird, 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 an der Konsole gedruckt.

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

3. Konfigurieren Sie die Ethernet-Schnittstelle und fügen Sie die Route mit hinzu `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
```

4. Stellen Sie sicher, dass der Server, der die ONIE-Installationsdatei hostet, 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:/ #
```

5. 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 wird installiert und startet den Switch anschließend neu. Lassen Sie den Switch normal in die neue EFOS-Version neu starten.

6. Vergewissern Sie sich, dass 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         3.7.0.4
(cs2) #
```

7. Schließen Sie die Installation ab.

Der Switch wird neu gestartet, ohne dass die Konfiguration angewendet wurde, und setzt die Werkseinstellungen zurück.

Was kommt als Nächstes?

["Installation von Lizenzen für BES-53248 Cluster-Switches".](#)

Installation von Lizenzen für BES-53248 Cluster-Switches

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

Prüfen Sie verfügbare Lizenzen

Die folgenden Lizenzen sind zur Verwendung auf dem BES-53248 Cluster-Switch verfügbar:

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 10G25G-Lizenzschlüssel mit 8 Anschlüssen, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248A2-6P-40-100G	Broadcom 40G100G-Lizenzschlüssel mit 6 Anschlüssen, X190005/R	EFOS 3.4.4.6 und höher

Ältere Lizenzen

In der folgenden Tabelle sind die älteren Lizenzen aufgeführt, die für den BES-53248-Cluster-Switch 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 6Port 40G100G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248-8P-10G25G-LIC	Broadcom 8-Port 10 G25 G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher

Lizenztyp	Lizenzdetails	Unterstützte Firmware-Version
SW-BES53248-16P-1025G-LIC	Broadcom 16-Port 10-G25-G-Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher
SW-BES53248-24P-1025G-LIC	Broadcom 24Port 10G25G Lizenzschlüssel, X190005/R	EFOS 3.4.4.6 und höher



Für die Basiskonfiguration ist keine Lizenz erforderlich.

Installieren Sie Lizenzdateien

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

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung mit dem Server, der EFOS, Lizenzen und der RCF-Datei hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch mit der IP-Adresse 172.19.2 verbunden ist:

```
(cs2)# ping 172.19.2.1
Pingung 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 Lizenzverwendung 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 verschiedene Schlüsselindizes zu verwenden.

Beispiel anzeigen

Im folgenden Beispiel wird SFTP verwendet, um eine Lizenzdatei in 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 sich den Lizenzstatus, bevor Switch cs2 neu gestartet wird:

```
show license
```

Beispiel anzeigen

```
(cs2)# show license

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

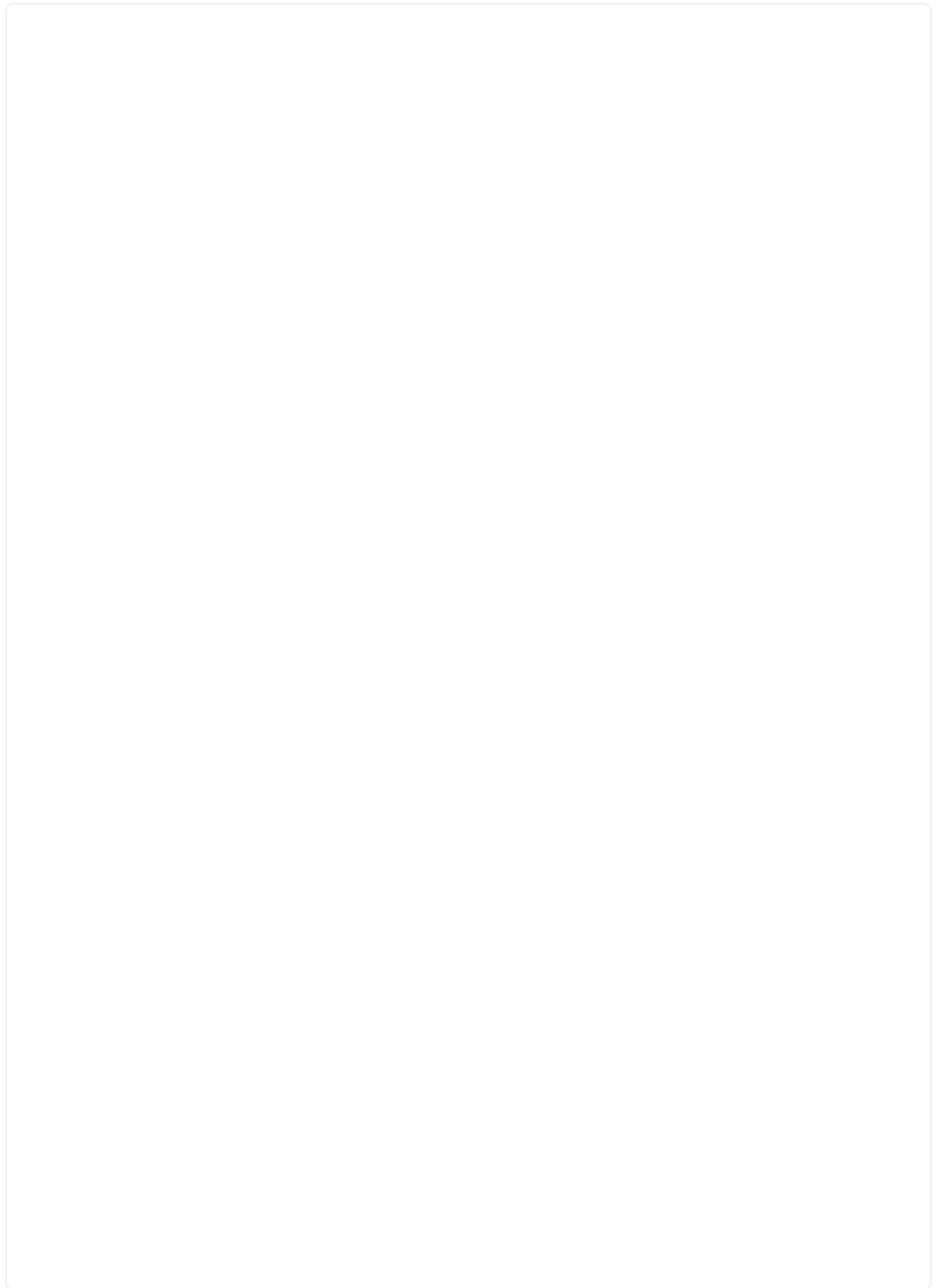
License Index  License Type      Status
-----
1              Port              License valid but not applied
```

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
```

Actor		Admin	Physical	Physical	Link	Link	LACP
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. Überprüfen Sie, ob die neue Lizenz aktiv ist, und beachten 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. Stellen Sie sicher, dass alle neuen Ports verfügbar sind:

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

Beispiel anzeigen

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

Actor		Admin	Physical	Physical	Link	Link	LACP
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					



Wenn Sie zusätzliche Lizenzen installieren, müssen Sie die neuen Schnittstellen manuell konfigurieren. Wenden Sie einen RCF nicht auf einen vorhandenen funktionierenden Produktionsschalter an.

Beheben Sie Probleme bei der Installation

Wenn beim Installieren einer Lizenz Probleme auftreten, führen Sie die folgenden Debug-Befehle aus, bevor Sie den ausführen `copy` Befehl erneut.

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 den ausführen `copy` Befehl mit dem `debug transfer` Und `debug license` Aktivierte Optionen, die Protokollausgabe wird 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.
```

Überprüfen Sie bei der Debug-Ausgabe auf Folgendes:

- Überprüfen Sie, ob die Seriennummer übereinstimmt: Serial number QTFCU38290012 matched.
- Überprüfen Sie, ob das Switch-Modell mit folgenden Punkten übereinstimmt: Model BES-53248 matched.
- Überprüfen Sie, ob der angegebene Lizenzindex zuvor nicht verwendet wurde. Wenn bereits ein Lizenzindex verwendet wird, wird der folgende Fehler zurückgegeben: License file /mnt/download//license.dat.1 already exists.
- Eine Port-Lizenz ist keine Feature-Lizenz. Daher wird folgende Aussage erwartet: Feature not found in license file with index = 1.

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


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



Wenn Sie die Switch-Software von Version 3.4.4.6 herunterstufen müssen, werden die Lizenzen entfernt. Dieses Verhalten ist zu erwarten.

Bevor Sie auf eine ältere Softwareversion zurücksetzen, müssen Sie eine entsprechende ältere Lizenz installieren.

Aktivieren Sie neu lizenzierte Ports

Um neue lizenzierte Ports zu aktivieren, müssen Sie die neueste Version des RCF bearbeiten und die entsprechenden Portdetails abkommentieren.

Die Standardlizenz aktiviert die Ports 0/1 bis 0/16 und 0/55 bis 0/56, während die neu lizenzierten Ports je nach Typ und Anzahl der verfügbaren Lizenzen zwischen den Ports 0/17 bis 0/54 liegen. Zum Beispiel, um die SW-BES54248-40-100G-LIC-Lizenz zu aktivieren, müssen Sie den folgenden Abschnitt im RCF entkommentieren:

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 High-Speed-Ports zwischen 0/49 und 0/54 inklusiv, deaktivieren Sie jeden Port, aber lösen Sie nur eine **Speed**-Leitung in der RCF für jeden dieser Anschlüsse, entweder: **Speed 100G Vollduplex** oder **Speed 40G Vollduplex** wie im Beispiel gezeigt. Bei Low-Speed-Ports zwischen 0/17 und 0/48 inklusive, deaktivieren Sie den gesamten Abschnitt mit 8 Ports, wenn eine entsprechende Lizenz aktiviert wurde.

Was kommt als Nächstes?

"[Installieren Sie die Referenzkonfigurationsdatei \(RCF\)](#)".

Installieren Sie die Referenzkonfigurationsdatei (RCF).

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

Wenn Sie ein RCF von einer älteren Version aktualisieren, müssen Sie die Broadcom-Switch-Einstellungen zurücksetzen und die Grundkonfiguration durchführen, um das RCF erneut anzuwenden. Sie müssen diesen Vorgang jedes Mal durchführen, wenn Sie ein RCF aktualisieren oder ändern möchten. Siehe "[KB-Artikel](#)" Entsprechende Details.

Prüfen Sie die Anforderungen

Bevor Sie beginnen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle RCF-Datei, die im verfügbar ist "[Broadcom Cluster-Switches](#)" Seite.
- Eine Startkonfiguration im RCF, die die gewünschten Startabbilder widerspiegelt, ist erforderlich, wenn Sie nur EFOS installieren und die aktuelle RCF-Version beibehalten. Wenn Sie die Startkonfiguration ändern müssen, um die aktuellen Startabbilder zu berücksichtigen, müssen Sie dies vor dem erneuten Anwenden des RCF tun, damit die korrekte Version bei zukünftigen Neustarts instanziiert wird.
- Eine Konsolenverbindung zum Switch, die erforderlich ist, wenn die RCF aus dem werkseitigen Standardzustand installiert wird. Diese Anforderung ist optional, wenn Sie den Knowledge Base-Artikel verwendet haben "[Löschen der Konfiguration auf einem Broadcom-Interconnect-Switch bei Beibehaltung der Remote-Konnektivität](#)" Um die Konfiguration vorher zu löschen.

Vorgeschlagene Dokumentation

- In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Siehe "[Download der EFOS-Software](#)" Seite. Beachten Sie, dass es zwischen der Befehlssyntax im RCF und der in EFOS-Versionen gefundenen Befehlssyntax bestehen kann.
- Weitere Informationen finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der "[Broadcom](#)" Website für vollständige Dokumentation über die Upgrade- und Downgrade-Verfahren für

Installieren Sie die Konfigurationsdatei

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden BES-53248-Switches lauten cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Namen der Cluster-LIF 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: :*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die Beispiele in diesem Verfahren verwenden vier Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster-Interconnect-Ports e0a Und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Über diese Aufgabe

Für das Verfahren müssen sowohl ONTAP-Befehle als auch Broadcom-Switch-Befehle verwendet werden. ONTAP-Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Mit dem folgenden Verfahren werden alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden, um einen unterbrechungsfreien Cluster-Betrieb zu gewährleisten.



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, verwenden Sie die "[KB: Löschen der Konfiguration auf einem Broadcom-Interconnect-Switch bei Beibehaltung der Remote-Konnektivität](#)". Wenn Sie die Switch-Einstellungen vollständig löschen müssen, müssen Sie die Grundkonfiguration erneut durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein, da durch eine vollständige Löschung der Konfiguration die Konfiguration des Managementnetzwerks zurückgesetzt wird.

Schritt 1: Vorbereitung für die Installation

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster1::*> system node autosupport invoke -node \* -type all -message  
MAINT=2h
```

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist: `network device-discovery show`

Beispiel anzeigen

```
cluster1::*> network device-discovery show  
Node/      Local  Discovered  
Protocol   Port   Device (LLDP: ChassisID)  Interface  
Platform  
-----  
-----  
cluster1-01/cdp  
          e0a    cs1                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 Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

- a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen 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					
e0b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

- b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden: `network interface show -role cluster`

Beispiel anzeigen

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

	Logical	Status	Network	
Current	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	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. Vergewissern Sie sich, dass im Cluster Informationen für beide Cluster-Switches angezeigt werden.

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie den 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 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009			
Is Monitored: true			
Reason: None			
Software Version: 3.10.0.3			
Version Source: CDP/ISDP			

```
cluster1::*>
```

ONTAP 9.7 und früher

Verwenden Sie für ONTAP 9.7 und frühere Versionen den 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 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```
cluster1::*>
```

1. Automatische Wiederherstellung auf den Cluster-LIFs deaktiviert.

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

Schritt 2: Ports konfigurieren

1. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

```
(cs2) (Config) # interface 0/1-0/16
(cs2) (Interface 0/1-0/16) # shutdown
```

2. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a	false		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0a	false		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0a	false		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0a	false		

```
cluster1::*>
```

3. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet: `cluster show`

Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

4. Wenn Sie dies noch nicht getan haben, speichern Sie die aktuelle Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Protokolldatei kopieren: `show running-config`

5. Reinigen Sie die Konfiguration am Schalter cs2, und führen Sie eine grundlegende Einrichtung durch.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein, um die Switch-Einstellungen zu löschen.

a. SSH in den Switch.

Fahren Sie nur fort, wenn alle Cluster-LIFs aus den Ports am Switch entfernt wurden und der Switch bereit ist, die Konfiguration zu löschen.

b. Aktivieren des Berechtigungsmodus:

```
(cs2)> enable
```

```
(cs2) #
```

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

Beispiel anzeigen

```
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. Speichern Sie die laufende Konfiguration in der Startkonfiguration:

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!
```

e. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload
```

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

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

6. Wenn zusätzliche Portlizenzen auf dem Switch installiert wurden, müssen Sie den RCF ändern, um die zusätzlichen lizenzierten Ports zu konfigurieren. Siehe ["Aktivieren Sie neu lizenzierte Ports"](#) Entsprechende Details.
7. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP.

Dieses Beispiel zeigt SFTP, mit dem eine RCF in den Bootflash auf Switch cs2 kopiert wird:

Beispiel anzeigen

```
(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.
```

8. Überprüfen Sie, ob das Skript heruntergeladen und auf dem Dateinamen gespeichert wurde, den Sie ihm gegeben haben:

```
script list
```

Beispiel anzeigen

```
(cs2)# script list
```

Configuration Script Name Modification	Size(Bytes)	Date of
BES-53248_RCF_v1.9-Cluster-HA.scr 05:41:00	2241	2020 09 30

1 configuration script(s) found.

9. Das Skript auf den Switch anwenden:

```
script apply
```

Beispiel anzeigen

```
(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.
```

10. Untersuchen Sie die Bannerausgabe aus dem `show clibanner` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

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
```

11. Überprüfen Sie auf dem Switch, ob die zusätzlichen lizenzierten Ports nach der Anwendung des RCF angezeigt werden:

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

Beispiel anzeigen

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

LACP	Actor	Admin	Physical	Physical	Link	Link
Intf	Type	Mode	Mode	Status	Status	Trap
Mode	Timeout					

0/1		Enable	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				

12. Überprüfen Sie auf dem Switch, ob Ihre Änderungen vorgenommen wurden:

```
show running-config
```

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

13. Speichern Sie die laufende Konfiguration, damit sie die Startkonfiguration wird, wenn Sie den Switch neu starten:

```
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!
```

14. Starten Sie den Switch neu und vergewissern Sie sich, dass die laufende Konfiguration korrekt ist:

```
reload
```

Beispiel anzeigen

```
(cs2)# reload
```

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

```
System will now restart!
```

15. Aktivieren Sie bei Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports.

```
(cs2) (Config)# interface 0/1-0/16
```

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

16. Überprüfen Sie die Ports auf Switch cs2: `show interfaces status all | exclude Detach`

Beispiel anzeigen

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

Media	Flow	Link	Physical	Physical	
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				

17. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

a. Überprüfen Sie, ob e0b Ports über alle Nodes im Cluster hinweg ordnungsgemäß eingerichtet 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					
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 Switch-Zustand vom Cluster.

Beispiel anzeigen

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

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

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			

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie den Befehl: `system switch ethernet show -is-monitoring-enabled -enabled-operational true`

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

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

```
cluster1::*>
```

ONTAP 9.7 und früher

Verwenden Sie für ONTAP 9.7 und frühere Versionen den 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 53248	cluster-network	10.228.143.200	BES-
Serial Number: QTWCU22510008 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			
cs2 53248	cluster-network	10.228.143.202	BES-
Serial Number: QTWCU22510009 Is Monitored: true Reason: None Software Version: 3.10.0.3 Version Source: CDP/ISDP			

```

cluster1::*>

```

1. fahren Sie bei Cluster-Switch cs1 die mit den Cluster-Ports der Knoten verbundenen Ports herunter.

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels verwendet:

```

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

```

2. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf dem Switch cs2 gehostet werden. Dies kann einige Sekunden dauern.
`network interface show -role cluster`

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet: `cluster show`

Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

4. Wiederholen Sie die Schritte 4 bis 14 am Schalter cs1.

5. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

6. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die Ereignisse „Cluster Ports down“ ignorieren, die auf den Knoten gemeldet wurden, während der Switch neu startet.

Beispiel anzeigen

```
(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: Überprüfen Sie die Konfiguration

1. Stellen Sie bei Switch cs1 sicher, dass die mit den Cluster-Ports verbundenen Switch-Ports **up** sind.

Beispiel anzeigen

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

Media	Flow	Link	Physical	Physical	
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 zwischen den Switches 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. Vergewissern Sie sich, dass die Cluster-LIFs auf ihren Home-Port zurückgesetzt wurden: `network interface show -role cluster`

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet: `cluster show`

Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

5. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität: `cluster ping-cluster -node local`

Beispiel anzeigen

```
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)
```

6. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

7. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine

AutoSupport Meldung aufrufen:

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

Was kommt als Nächstes?

["Installieren Sie die CSHM-Konfigurationsdatei".](#)

Aktivieren Sie SSH bei BES-53248 Cluster-Switches

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

Schritte

1. Vergewissern Sie sich, dass 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
```

2. Generieren der 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

(switch) (Config)# aaa authorization commands "noCmdAuthList" none
(switch) (Config)# exit
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
(switch)# write mem

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!
```



Stellen Sie sicher, dass SSH deaktiviert ist, bevor Sie die Schlüssel ändern. Andernfalls wird eine Warnung auf dem Switch gemeldet.

3. Starten Sie den Switch neu:

```
reload
```

4. Vergewissern Sie sich, dass 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
```

Was kommt als Nächstes?

["Aktivieren Sie die Protokollerfassung"](#).

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Um die Protokollerfassungsfunktion zu aktivieren, müssen Sie ONTAP Version 9.12.1 oder höher und EFOS 3.8.0.2 oder höher ausführen.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um Anweisungen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Broadcom BES-53248-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3UserNoAuth NETWORK-OPERATOR noauth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3UserAuth NETWORK-OPERATOR [auth-md5|auth-sha]
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3UserAuthEncrypt NETWORK-OPERATOR [auth-md5|auth-sha]
[priv-aes128|priv-des]
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp status
```


Beispiel anzeigen

```
(sw1) (Config)# snmp-server user <username> network-admin auth-md5
<password> priv-aes128 <password>

(cs1) (Config)# show snmp user snmp
```

Name	Group Name	Auth Meth	Priv Meth	Remote Engine ID
<username>	network-admin	MD5	AES128	8000113d03d8c497710bee

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Beispiel anzeigen

```
cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance
Device Name: sw1
IP Address: 10.228.136.24
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: <username>
Model Number: BES-53248
Switch Network: cluster-network
Software Version: 3.9.0.2
Reason For Not Monitoring: None <---- should
display this if SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for
Cluster/HA/RDMA
```

Aktualisieren der Switches

Überblick über den Upgrade-Prozess für BES-53248-Switches

Überprüfen Sie vor der Konfiguration von BES-53248-Cluster-Switches für ein Upgrade die Konfigurationsübersicht.

Führen Sie zum Upgrade eines BES-53248-Cluster-Switches die folgenden Schritte aus:

1. ["Vorbereiten des BES-53248-Cluster-Switch für ein Upgrade"](#). Bereiten Sie den Controller vor, und installieren Sie anschließend die EFOS-Software, Lizenzen und die Referenzkonfigurationsdatei (RCF). Überprüfen Sie abschließend die Konfiguration.
2. ["Installieren Sie die EFOS-Software"](#). Laden Sie die Ethernet Fabric OS (EFOS)-Software auf dem BES-53248-Cluster-Switch herunter und installieren Sie sie.
3. ["Installation von Lizenzen für BES-53248 Cluster-Switches"](#). Optional können Sie neue Ports durch den Kauf und die Installation weiterer Lizenzen hinzufügen. Das Switch-Basismodell ist für 16 10-GbE- oder 25-GbE-Ports und zwei 100-GbE-Ports lizenziert.
4. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)"](#). Installieren oder aktualisieren Sie die RCF auf dem BES-53248 Cluster-Switch und überprüfen Sie nach der Anwendung des RCF die Ports für eine zusätzliche Lizenz.
5. ["Installieren Sie die Konfigurationsdatei des Cluster Switch Health Monitor \(CSHM\)"](#). Installieren Sie die entsprechende Konfigurationsdatei für das Monitoring des Clusterstatus.

6. ["Aktivieren Sie SSH bei BES-53248 Cluster-Switches"](#). Wenn Sie den Cluster Switch Health Monitor (CSHM) und die Funktionen zur Protokollerfassung verwenden, aktivieren Sie SSH auf den Switches.
7. ["Aktivieren Sie die Protokollerfassungsfunktion"](#). Verwenden Sie diese Funktion, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.
8. ["Überprüfen Sie die Konfiguration"](#). Mithilfe der empfohlenen Befehle können Sie die Vorgänge nach einem Upgrade eines BES-53248-Cluster-Switches überprüfen.

Aktualisieren Sie den BES-53248 Cluster-Switch

Führen Sie diese Schritte aus, um einen BES-53248-Cluster-Switch zu aktualisieren.

Dieser Vorgang gilt für ein funktionierendes Cluster und ermöglicht eine unterbrechungsfreie Upgrade- (NDU) und eine unterbrechungsfreie Betriebsumgebung (Non-Disruptive Operations, NDO). Weitere Informationen finden Sie im Knowledge Base-Artikel ["Vorbereiten von ONTAP auf ein Cluster-Switch-Upgrade"](#).

Prüfen Sie die Anforderungen

Vor der Installation der EFOS Software, der Lizenzen und der RCF-Datei auf einem vorhandenen NetApp BES-53248 Cluster-Switch stellen Sie sicher, dass:

- Das Cluster ist ein voll funktionsfähiges Cluster (keine Fehlermeldungen oder andere Probleme).
- Das Cluster enthält keine fehlerhaften Cluster-Netzwerkkarten (NICs).
- Alle verbundenen Ports auf beiden Cluster-Switches funktionieren ordnungsgemäß.
- Alle Cluster-Ports sind aktiv.
- Alle Cluster-LIFs sind administrativ und betrieblich und auf ihren Home-Ports aktiv.
- Die ersten beiden Cluster-LIFs an jedem Node sind auf separaten NICs konfiguriert und mit separaten Cluster-Switch-Ports verbunden.
- Das ONTAP `cluster ping-cluster -node node1` Der Befehl „Advanced Privilege“ zeigt das an `larger than PMTU communication` Ist auf allen Pfaden erfolgreich.



Zwischen der Befehlssyntax in der RCF- und EFOS-Version kann es zu Befehlsabhängigkeiten kommen.



Informationen zur Switch-Kompatibilität finden Sie in der Kompatibilitätstabelle auf der ["Broadcom Cluster-Switches"](#) Seite für die unterstützten EFOS-, RCF- und ONTAP-Versionen.

Bereiten Sie den Controller vor

Gehen Sie folgendermaßen vor, um den Controller für ein Upgrade des BES-53248-Cluster-Switches vorzubereiten.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Mit dem Ping-Befehl können Sie die Verbindung zum Server, der EFOS, Lizenzen und RCF hostet, überprüfen.

Wenn es sich um ein Problem handelt, verwenden Sie ein nicht geroutetes Netzwerk, und konfigurieren Sie den Service-Port mithilfe der IP-Adresse 192.168.x oder 172.19.x Sie können den Service-Port später an die Produktionsmanagement-IP-Adresse neu konfigurieren.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch mit der IP-Adresse 172.19.2 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, ob die Cluster-Ports ordnungsgemäß sind und über einen Link verfügen. Verwenden Sie dazu den Befehl:

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

Beispiel anzeigen

Das folgende Beispiel zeigt die Art der Ausgabe, in der alle Ports mit einem verfügen Link Wert von up und a Health Status Für gesund:

```
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							

- Überprüfen Sie mithilfe des Befehls, dass die Cluster-LIFs administrativ und betrieblich sind und sich in ihren Home Ports befinden:

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

Beispiel anzeigen

In diesem Beispiel ist der `-vserver` Mit dem Parameter werden Informationen zu den LIFs angezeigt, die den Cluster-Ports zugeordnet sind. Status Admin/Oper Muss up-und sein Is Home Muss wahr sein:

```
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			

Software installieren

Befolgen Sie diese Anweisungen, um die Software zu installieren.

1. ["Installieren Sie die EFOS-Software"](#). Laden Sie die Ethernet Fabric OS (EFOS)-Software auf dem BES-53248-Cluster-Switch herunter und installieren Sie sie.
2. ["Installation von Lizenzen für BES-53248 Cluster-Switches"](#). Optional können Sie neue Ports durch den Kauf und die Installation weiterer Lizenzen hinzufügen. Das Switch-Basismodell ist für 16 10-GbE- oder 25-GbE-Ports und zwei 100-GbE-Ports lizenziert.
3. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)"](#). Installieren oder aktualisieren Sie die RCF auf dem BES-53248 Cluster-Switch und überprüfen Sie nach der Anwendung des RCF die Ports für eine zusätzliche Lizenz.
4. ["Installieren Sie die Konfigurationsdatei des Cluster Switch Health Monitor \(CSHM\)"](#). Installieren Sie die entsprechende Konfigurationsdatei für das Monitoring des Clusterstatus.
5. ["Aktivieren Sie SSH bei BES-53248 Cluster-Switches"](#). Wenn Sie den Cluster Switch Health Monitor (CSHM) und die Funktionen zur Protokollerfassung verwenden, aktivieren Sie SSH auf den Switches.
6. ["Aktivieren Sie die Protokollerfassungsfunktion"](#). Verwenden Sie diese Funktion, um Switch-bezogene

Protokolldateien in ONTAP zu sammeln.

Überprüfen Sie die Konfiguration nach einem Upgrade eines BES-53248 Cluster-Switches

Mithilfe empfohlener Befehle können Sie die Vorgänge nach einem Upgrade von BES-53248-Cluster-Switches überprüfen.

Schritte

1. Zeigen Sie mit dem Befehl Informationen zu den Netzwerk-Ports auf dem Cluster an:

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

Link Muss den Wert haben up Und Health Status Muss sein healthy.

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Befehls angezeigt:

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

Node: node1

Ignore

Speed (Mbps) Health

Health

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	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
------	---------	-----------	--------	------	-----	------------	--------

e0a	Cluster	Cluster		up	9000	auto/10000	healthy
-----	---------	---------	--	----	------	------------	---------

false							
e0b	Cluster	Cluster		up	9000	auto/10000	healthy

false

2. Überprüfen Sie dies für jede LIF Is Home Ist true Und Status Admin/Oper Ist up Auf beiden Nodes, mit dem 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 das Health Status Von jedem Node ist true Verwenden des Befehls:

```
cluster show
```

Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon

node1	true	true	false
node2	true	true	false

Switches migrieren

Migrieren Sie CN1610 Cluster-Switches zu BES-53248 Cluster-Switches

Um die CN1610-Cluster-Switches in einem Cluster zu von Broadcom unterstützten BES-53248-Cluster-Switches zu migrieren, die Migrationsanforderungen zu prüfen und anschließend den Migrationsvorgang zu befolgen.

Folgende Cluster-Switches werden unterstützt:

- CN1610
- BES-53248

Prüfen Sie die Anforderungen

Stellen Sie sicher, dass Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Einige der Ports auf BES-53248-Switches sind für den Betrieb mit 10 GbE konfiguriert.
- Die 10-GbE-Konnektivität von den Nodes zu BES-53248 Cluster-Switches wurde geplant, migriert und dokumentiert.
- Das Cluster funktioniert voll (es sollten keine Fehler in den Protokollen oder ähnlichen Problemen geben).
- Die erste Anpassung der BES-53248-Switches ist abgeschlossen, so dass:
 - BES-53248-Switches verwenden die neueste empfohlene Version der EFOS-Software.
 - Auf die Switches wurden Referenzkonfigurationsdateien (RCFs) angewendet.
 - Anpassung von Websites, z. B. DNS, NTP, SMTP, SNMP, Und SSH werden auf den neuen Switches konfiguriert.

Node-Verbindungen

Die Cluster-Switches unterstützen die folgenden Node-Verbindungen:

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



Zusätzliche Ports können durch den Kauf von Portlizenzen aktiviert werden.

ISL-Ports

Bei den Cluster-Switches werden die folgenden Inter-Switch-Link-Ports (ISL) verwendet:

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

Der "[NetApp Hardware Universe](#)" Enthält Informationen zur ONTAP-Kompatibilität, zu unterstützter EFOS-Firmware und zur Verkabelung mit BES-53248-Cluster-Switches.

ISL-Verkabelung

Die entsprechende ISL-Verkabelung lautet wie folgt:

- **Beginn:** für CN1610 bis CN1610 (SFP+ auf SFP+), vier SFP+-Glasfaserkabel oder Kupfer-Direct-Attach-Kabel.
- **Endfassung:** für BES-53248 bis BES-53248 (QSFP28 zu QSFP28), zwei optische QSFP28-Transceiver/Glasfaser oder Kupfer-Direct-Attach-Kabel.

Migrieren Sie die Switches

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

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Beispiele verwenden zwei Nodes, die jeweils zwei 10-GbE-Cluster-Interconnect-Ports implementieren: e0a Und e0b.
- Die Ausgaben für die Befehle können je nach Versionen der ONTAP Software variieren.
- Die zu ersetzenden CN1610-Schalter sind CL1 Und CL2.
- Die BES-53248-Switches als Ersatz für die CN1610-Switches sind cs1 Und cs2.
- Die Nodes sind node1 Und node2.
- Der Schalter CL2 wird zuerst durch cs2 ersetzt, gefolgt von CL1 durch cs1.
- Die BES-53248-Switches sind mit den unterstützten Versionen von Reference Configuration File (RCF) und Ethernet Fabric OS (EFOS) vorinstalliert, wobei ISL-Kabel an den Ports 55 und 56 angeschlossen sind.
- Die LIF-Namen des Clusters sind node1_clus1 Und node1_clus2 Für Node1, und node2_clus1 Und node2_clus2 Für Knoten 2.

Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Zu Beginn des Clusters sind zwei mit zwei CN1610 Cluster-Switches verbundene Nodes verbunden.
- CN1610-Switch CL2 wird durch BES-53248-Schalter cs2 ersetzt:
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Trennen Sie die Kabel von allen Cluster-Ports auf allen mit CL2 verbundenen Nodes, und schließen Sie die Ports mit den unterstützten Kabeln wieder an den neuen Cluster-Switch cs2 an.
- CN1610-Schalter CL1 wird durch BES-53248-Schalter cs1 ersetzt:
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Trennen Sie die Kabel von allen Cluster-Ports auf allen mit CL1 verbundenen Nodes, und schließen Sie die Ports mit den unterstützten Kabeln wieder an den neuen Cluster-Switch cs1 an.



Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster1::*> system node autosupport invoke -node * -type all -message  
MAINT=2h
```

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

Schritt: Ports und Verkabelung konfigurieren

1. Vergewissern Sie sich bei den neuen Switches, dass die ISL zwischen den Switches cs1 und cs2 verkabelt und ordnungsgemäß funktioniert:

```
show port-channel
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports **up** auf Switch cs1 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 **up** auf Switch cs2 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 Node an, der mit den vorhandenen Cluster-Switches verbunden ist:

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

Beispiel anzeigen

Im folgenden Beispiel wird angezeigt, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster-Interconnect-Switch konfiguriert wurden:

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface
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. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

a. Vergewissern Sie sich, dass alle Cluster-Ports vorhanden sind up Mit einem healthy Status:

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

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

Node: node1

Ignore

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

Node: node2

Ignore

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

- b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) auf ihren Home-Ports befinden:

```
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. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie den Befehl: `system switch ethernet show -is-monitoring-enabled -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

Verwenden Sie für ONTAP 9.7 und frühere Versionen den 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. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs.

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

2. Fahren Sie bei Cluster-Switch CL2 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster-LIFs zu ermöglichen:

```
(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. Vergewissern Sie sich, dass für die Cluster-LIFs ein Failover zu den auf dem Cluster-Switch CL1 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
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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

Beispiel anzeigen

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

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

5. Verschieben Sie alle Clusterknoten-Verbindungskabel vom alten CL2-Switch auf den neuen cs2-Switch.
6. Bestätigen Sie den Funktionszustand der Netzwerkverbindungen, die zu cs2 verschoben wurden:

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

Beispiel anzeigen

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

Node: node1

Ignore

						Speed(Mbps)	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
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						

Es sollten alle verschobenen Cluster-Ports verwendet werden up.

7. Überprüfen Sie die „Neighbor“-Informationen auf 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
53248			BES-
node1	/cdp		
	e0a	CL1	0/1
CN1610			
	e0b	cs2	0/1
53248			BES-

8. Vergewissern Sie sich, dass die Switch-Port-Verbindungen aus Sicht von Switch cs2 ordnungsgemäß sind:

```
cs2# show port all
cs2# show isdp neighbors
```

9. Fahren Sie bei Cluster-Switch CL1 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster-LIFs zu ermöglichen:

```
(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) #
```

Bei allen Cluster-LIFs wird ein Failover zum cs2-Switch durchgeführt.

10. Vergewissern Sie sich, dass für die Cluster-LIFs ein Failover zu den 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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

Beispiel anzeigen

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

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

12. Verschieben Sie die Verbindungskabel des Clusterknoten von CL1 zum neuen cs1-Switch.
13. Bestätigen Sie den Funktionszustand 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						

Es sollten alle verschobenen Cluster-Ports verwendet werden up.

14. Überprüfen Sie die „Neighbor“-Informationen auf 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
53248			BES-
	e0b	cs2	0/1
53248			BES-
node2	/cdp		
	e0a	cs1	0/2
53248			BES-
	e0b	cs2	0/2
53248			BES-

15. Vergewissern Sie sich, dass die Switch-Port-Verbindungen aus Sicht von Switch cs1 ordnungsgemäß sind:

```
cs1# show port all
cs1# show isdp neighbors
```

16. Vergewissern Sie sich, dass die ISL zwischen cs1 und cs2 weiterhin funktionsfähig ist:

```
show port-channel
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports **up** auf Switch cs1 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 **up** auf Switch cs2 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 ausgetauschten CN1610-Switches aus der Switch-Tabelle des Clusters, wenn sie nicht

automatisch entfernt werden:

ONTAP 9.8 und höher

Ab ONTAP 9.8 verwenden Sie den 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

Verwenden Sie für ONTAP 9.7 und frühere Versionen den 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: Überprüfen Sie die Konfiguration

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

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

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

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

Wenn die Cluster-LIFs nicht auf ihren Home-Port zurückgesetzt wurden, setzen Sie sie manuell zurück:

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

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

```
cluster show
```

4. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

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

Beispiel anzeigen

```
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 169.254.47.194 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)
```

5. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

6. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

Do you want to modify the cluster switch log collection
configuration?

{y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

Do you want to modify the cluster switch log collection
configuration?

{y|n}: [n] **y**

Enabling cluster switch log collection.

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

7. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

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

Migration zu einer NetApp Cluster-Umgebung mit Switch

Wenn Sie über eine vorhandene Cluster-Umgebung mit zwei Nodes (ohne Switch) verfügen, können Sie mit den von Broadcom unterstützten BES-53248 Cluster-Switches zu einer 2-Node-*Switched*-Cluster-Umgebung migrieren. Dadurch können Sie eine Skalierung über zwei Nodes im Cluster hinaus vornehmen.

Der Migrationsprozess funktioniert bei allen Cluster Node-Ports mit optischen oder Twinax-Ports, wird bei diesem Switch jedoch nicht unterstützt, wenn Knoten integrierte 10GBASE-T RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

Prüfen Sie die Anforderungen

Prüfen Sie die folgenden Anforderungen für die Cluster-Umgebung.

- Beachten Sie, dass die meisten Systeme auf jedem Controller zwei dedizierte Cluster-Netzwerk-Ports benötigen.
- Vergewissern Sie sich, dass der BES-53248-Cluster-Switch wie unter beschrieben eingerichtet ist ["Anforderungen ersetzen"](#) Bevor Sie mit diesem Migrationsprozess beginnen.
- Bei der Konfiguration mit zwei Nodes ohne Switches stellen Sie Folgendes sicher:
 - Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
 - Auf den Knoten wird ONTAP 9.5P8 und höher ausgeführt. Die Unterstützung für 40/100-GbE-Cluster-Ports beginnt mit der EFOS-Firmware-Version 3.4.4.6 und höher.
 - Alle Cluster-Ports haben den Status **up**.
 - Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren Home-Ports.
- Stellen Sie für die von Broadcom unterstützte Konfiguration von BES-53248 Cluster-Switches Folgendes sicher:
 - Der BES-53248 Cluster-Switch funktioniert bei beiden Switches vollständig.
 - Beide Switches verfügen über Management-Netzwerk-Konnektivität.
 - Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
 - BES-53248 Node-to-Node-Switch und Switch-to-Switch-Verbindungen verwenden Twinax- oder Glasfaserkabel.

Der ["NetApp Hardware Universe"](#) Enthält Informationen zur ONTAP-Kompatibilität, zu unterstützter EFOS-Firmware und zur Verkabelung mit BES-53248-Switches.

- Inter-Switch Link (ISL)-Kabel sind an beiden BES-53248-Switches mit den Ports 0/55 und 0/56 verbunden.
- Die Erstinstallation der BES-53248 Switches ist damit abgeschlossen. Dadurch erreichen Sie Folgendes:
 - Bei BES-53248-Switches wird die neueste Softwareversion ausgeführt.
 - Beim Kauf von BES-53248 Switches sind optionale Portlizenzen installiert.
 - Auf die Switches werden Referenzkonfigurationsdateien (RCFs) angewendet.
- Auf den neuen Switches werden alle Site-Anpassungen (SMTP, SNMP und SSH) konfiguriert.

Geschwindigkeitsbeschränkungen der Portgruppe

- Die 48 10/25-GbE-Ports (SFP28/SFP+) werden wie folgt in 12 x 4-Port-Gruppen kombiniert: 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 Port-Geschwindigkeit von SFP28/SFP+ muss für alle Ports der 4-Port-Gruppe gleich (10 GbE oder 25 GbE) sein.
- Wenn die Geschwindigkeiten in einer 4-Port-Gruppe unterschiedlich sind, funktionieren die Switch-Ports nicht ordnungsgemäß.

In Cluster-Umgebung migrieren

Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der BES-53248-Switches lauten `cs1` Und `cs2`.

- Die Namen der Cluster-SVMs lauten `node1` Und `node2`.
- Die Namen der LIFs sind `node1_clus1` Und `node1_clus2` Auf Node 1, und `node2_clus1` Und `node2_clus2` Auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind `e0a` Und `e0b`.

Der "[NetApp Hardware Universe](#)" Enthält die neuesten Informationen über die tatsächlichen Cluster-Ports für Ihre Plattformen.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster1::*> system node autosupport invoke -node \* -type all -message MAINT=2h
```

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (``*>``) erscheint.

Schritt: Ports und Verkabelung konfigurieren

1. Deaktivieren Sie alle aktivierten Node-Ports (keine ISL-Ports) auf beiden neuen Cluster-Switches **cs1** und **cs2**.



Sie dürfen die ISL-Ports nicht deaktivieren.

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 16 auf 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 auf der ISL zwischen den beiden BES-53248-Switches cs1 und cs2 aktiviert sind:

```
show port-channel
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports auf 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 auf 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 enthält Informationen zu den Geräten, die mit dem System verbunden sind.

Beispiel anzeigen

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs1 aufgeführt:

```
(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

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs2 aufgeführt:

```
(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. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

```
network port show -ip space Cluster
```

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

5. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind 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. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

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

7. Trennen Sie das Kabel vom Cluster-Port e0a auf node1, und verbinden sie e0a mit Port 1 am Cluster-Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von den BES-53248-Switches unterstützt wird.

Der "[NetApp Hardware Universe](#)" Enthält weitere Informationen zur Verkabelung.

8. Trennen Sie das Kabel vom Cluster-Port e0a auf node2 und verbinden sie e0a mit Port 2 am Cluster-Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von den BES-53248-Switches unterstützt wird.
9. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs1.

Das folgende Beispiel zeigt, dass die Ports 1 bis 16 auf 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. Vergewissern Sie sich, dass 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. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind 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
false					
	node1_clus2	up/up	169.254.49.125/16	node1	e0b
true					
	node2_clus1	up/up	169.254.47.194/16	node2	e0a
false					
	node2_clus2	up/up	169.254.19.183/16	node2	e0b
true					

12. Informationen zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

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

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

13. Trennen Sie das Kabel von Cluster-Port e0b auf node1, und verbinden Sie dann e0b mit Port 1 am Cluster-Switch cs2. Verwenden Sie dazu die entsprechende Verkabelung, die von den BES-53248-Switches unterstützt wird.
14. Trennen Sie das Kabel von Cluster-Port e0b auf node2, und verbinden Sie dann e0b mit Port 2 am Cluster-Switch cs2. Verwenden Sie dazu die entsprechende Verkabelung, die von den BES-53248-Switches unterstützt wird.
15. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs2.

Das folgende Beispiel zeigt, dass die Ports 1 bis 16 auf 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. Vergewissern Sie sich, dass 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: Überprüfen Sie die Konfiguration

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

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

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

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

Wenn die Cluster-LIFs nicht auf ihren Home-Port zurückgesetzt wurden, setzen Sie sie manuell zurück:

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

3. Vergewissern Sie sich, dass alle Schnittstellen angezeigt werden `true` Für Is Home:

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



Dies kann einige Minuten dauern.

Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current	
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. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
show isdp neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
(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

5. Zeigen Sie Informationen zu den erkannten Netzwerkgeräten im Cluster an:

```
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
53248			BES-
	e0b	cs2	0/2
53248			BES-
node1	/cdp		
	e0a	cs1	0/1
53248			BES-
	e0b	cs2	0/1
53248			BES-

6. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

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



Es kann einige Minuten dauern, bis der Befehl abgeschlossen ist. Warten Sie, bis die Ankündigung „3 Minuten Lebensdauer abläuft“ abläuft.

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

```
cluster1::*> network options switchless-cluster show
```

Enable Switchless Cluster: false

7. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

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

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

8. Überprüfen Sie mit dem Befehl, ob das Cluster-Netzwerk vollständig verbunden ist:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node local
```

```
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 192.168.168.26 node1 e0a
Cluster node1_clus2 192.168.168.27 node1 e0b
Cluster node2_clus1 192.168.168.28 node2 e0a
Cluster node2_clus2 192.168.168.29 node2 e0b
Local = 192.168.168.28 192.168.168.29
Remote = 192.168.168.26 192.168.168.27
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 4 path(s):
    Local 192.168.168.28 to Remote 192.168.168.26
    Local 192.168.168.28 to Remote 192.168.168.27
    Local 192.168.168.29 to Remote 192.168.168.26
    Local 192.168.168.29 to Remote 192.168.168.27
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)
```

9. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

10. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

```
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 KB-Artikel: Wie kann die automatische Case-Erstellung während geplanter Wartungszeitfenster unterdrückt werden"](#)

Was kommt als Nächstes?

Nach Abschluss der Migration müssen Sie möglicherweise die erforderliche Konfigurationsdatei installieren, um den Ethernet Switch Health Monitor (CSHM) für BES-53248-Cluster-Switches zu unterstützen. Siehe ["Aktivieren Sie die Protokollerfassung"](#).

Tauschen Sie die Schalter aus

Ersatzanforderungen

Stellen Sie vor dem Austausch des Switches sicher, dass die folgenden Bedingungen in der aktuellen Umgebung und am Ersatzschalter erfüllt sind.

Bestehende Cluster- und Netzwerkinfrastruktur

Stellen Sie sicher, dass:

- Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
- Alle Cluster-Ports sind **up**.
- Alle Cluster-logischen Schnittstellen (LIFs) sind administrativ und betrieblich **up** und auf ihren Home-Ports.
- 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 Austausch-Cluster-Switch

Stellen Sie sicher, dass:

- Das Management-Netzwerk-Konnektivität auf dem Ersatz-Switch ist funktionsfähig.
- Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
- Die Node-Verbindungen sind die Ports 0/1 bis 0/16 bei der Standardlizenzierung.

- Alle Inter-Switch Link (ISL)-Ports sind an den Ports 0/55 und 0/56 deaktiviert.
- Die gewünschte Referenzkonfigurationsdatei (RCF) und das Switch-Image des EFOS-Betriebssystems werden auf den Switch geladen.
- Die Erstanpassung des Schalters ist abgeschlossen, wie in beschrieben "[Konfigurieren Sie den BES-53248 Cluster-Switch](#)".

Alle zuvor erstellten Site-Anpassungen wie STP, SNMP und SSH werden auf den neuen Switch kopiert.

Finden Sie weitere Informationen

- "[NetApp Support Website](#)"
- "[NetApp Hardware Universe](#)"

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

Führen Sie diese Schritte aus, um einen defekten Broadcom-unterstützten BES-53248-Cluster-Switch in einem Cluster-Netzwerk zu ersetzen. Dies ist ein NDU (Non Disruptive Procedure, NDU).

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der vorhandenen BES-53248-Switches lauten `cs1` Und `cs2`.
- Der Name des neuen BES-53248-Switch lautet `newcs2`.
- Die Node-Namen sind `node1` Und `node2`.
- Die Cluster-Ports an jedem Node werden mit benannt `e0a` Und `e0b`.
- Die LIF-Namen des Clusters sind `node1_clus1` Und `node1_clus2` Für Node1, und `node2_clus1` Und `node2_clus2` Für Knoten 2.
- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet `cluster1::>`

Allgemeines zur Topologie

Dieses Verfahren basiert auf der folgenden 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/ Protocol	Local Port	Discovered 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 Port ID	Intf	Holdtime	Capability	Platform
node1 e0a	0/1	175	H	FAS2750
node2 e0a	0/2	152	H	FAS2750
cs2 0/55	0/55	179	R	BES-53248
cs2 0/56	0/56	179	R	BES-53248

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

Schritte

1. Überprüfen Sie die ["Ersatzanforderungen"](#).
2. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

3. Installieren Sie die entsprechende Referenzkonfigurationsdatei (RCF) und das entsprechende Image auf dem Switch, newcs2, und nehmen Sie die erforderlichen Standortvorbereitungen vor.

Überprüfen, 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 benötigt, fahren Sie mit Schritt 2 fort.

- a. Sie können die entsprechende Broadcom EFOS-Software für Ihre Cluster-Switches von [herunterladen "Unterstützung Für Broadcom Ethernet-Switches"](#) Standort. Befolgen Sie die Schritte auf der Download-Seite, um die EFOS-Datei für die Version der zu installierenden ONTAP-Software herunterzuladen.
 - b. Das entsprechende RCF ist im erhältlich ["Broadcom Cluster-Switches"](#) Seite. Befolgen Sie die Schritte auf der Download-Seite, um den korrekten RCF für die Version der von Ihnen installierenden ONTAP-Software herunterzuladen.
4. Beim neuen Switch melden Sie sich als `admin` Fahren Sie außerdem alle Ports herunter, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports 1 zu 16).



Wenn Sie zusätzliche Lizenzen für zusätzliche Ports erworben haben, fahren Sie diese Ports auch herunter.

Wenn der Switch, den Sie ersetzen, nicht funktionsfähig und heruntergefahren ist, sollten die LIFs auf den Cluster-Nodes bereits ein Failover zum anderen Cluster-Port für jeden Node durchgeführt haben.



Zur Eingabe 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. Vergewissern Sie sich, dass alle Cluster-LIFs über diesen verfügen `auto-revert` Aktiviert:

```
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. Fahren Sie die ISL-Ports 0/55 und 0/56 auf dem BES-53248-Switch cs1 herunter:

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 verbinden Sie sie dann mit den gleichen Ports am BES-53248 newc2 Switch.
8. Bringen Sie die ISLs-Ports 0/55 und 0/56 zwischen den switches cs1 und newcs2 auf, und überprüfen Sie dann den Betriebsstatus des Port-Kanals.

Der Link-Status für Port-Kanal 1/1 sollte **up** sein und alle Mitgliedsports sollten unter der Überschrift Port Active wahr sein.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 0/55 und 0/56 und zeigt den Link-Status für Port-Channel 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. Aktivieren Sie auf dem neuen Switch newcs2 alle Ports, die mit den Knoten-Cluster-Schnittstellen verbunden sind (Ports 1 bis 16).



Wenn Sie zusätzliche Lizenzen für zusätzliche Ports erworben haben, fahren Sie diese Ports auch herunter.

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. Vergewissern Sie sich, dass Port e0b **up** ist:

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

Beispiel anzeigen

Die Ausgabe sollte wie folgt aussehen:

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

Node: node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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. Auf dem gleichen Node, den Sie im vorherigen Schritt verwendet haben, warten Sie, bis der Cluster LIF node1_clus2 on node1 die automatische Wiederherstellung ermöglicht.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn er umgekehrt wurde Is Home Ist true Und der Hafen ist e0b.

Mit dem folgenden Befehl werden Informationen zu den LIFs auf beiden Nodes angezeigt. Wenn das Einrichten des ersten Node erfolgreich ist Is Home Ist true In diesem Beispiel werden für beide Cluster-Schnittstellen und sie die richtigen Port-Zuweisungen zeigen e0a Und e0b Auf Knoten 1.

```
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. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

Beispiel anzeigen

In diesem Beispiel wird der Systemzustand des Node für angegeben node1 Und node2 In diesem Cluster befindet sich true:

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

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

13. Bestätigen Sie die folgende Clusternetzwerkconfiguration:

```
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					

```
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.
```

+

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	144	H	FAS2980
node2 e0a	Eth1/2	145	H	FAS2980
newcs2 (FDO296348FU) Eth1/65	Eth1/65	176	R S I s	N9K-C92300YC
newcs2 (FDO296348FU) Eth1/66	Eth1/66	176	R S I s	N9K-C92300YC

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 (FDO220329KU) Eth1/65	Eth1/65	178	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	178	R S I s	N9K-C92300YC

14. Vergewissern Sie sich, dass das Cluster-Netzwerk ordnungsgemäß ist:

```
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 Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Was kommt als Nächstes?

Siehe "[Aktivieren Sie die Protokollerfassungsfunktion](#)" Für die Schritte, die erforderlich sind, um die Protokollerfassung des Cluster-Zustandsschalters zu aktivieren, die zum Erfassen von Switch-bezogenen Protokolldateien verwendet wird.

Ersetzen Sie Broadcom BES-53248-Cluster-Switches durch Switch-lose Verbindungen

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

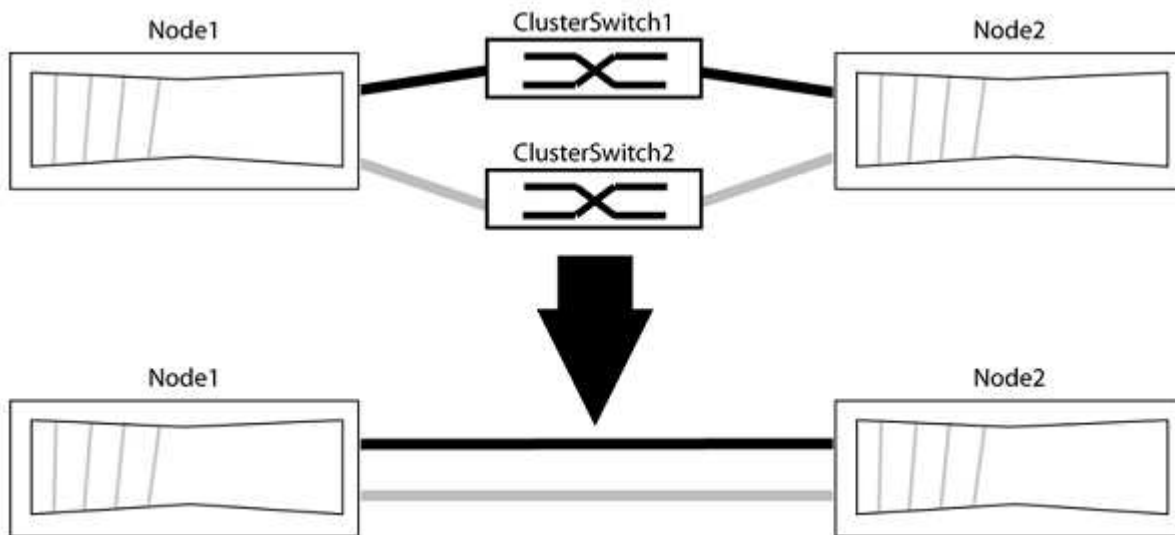
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Angezeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

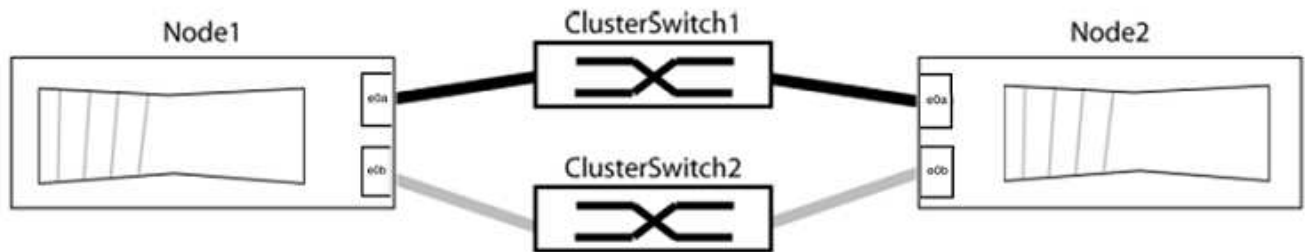
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Schritt: Ports und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in `grop1` zu Cluster-Switch 1 wechseln und die Cluster-Ports in `grop2` zu Cluster-Switch 2 wechseln. Diese Gruppen sind später im Verfahren erforderlich.
2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



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

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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

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

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

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

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

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

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

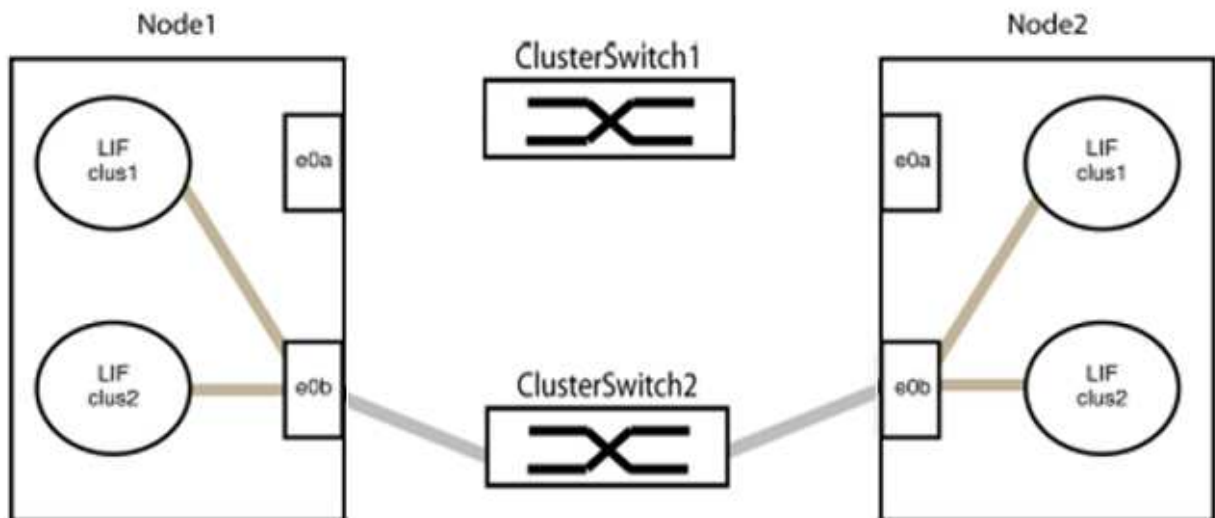
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

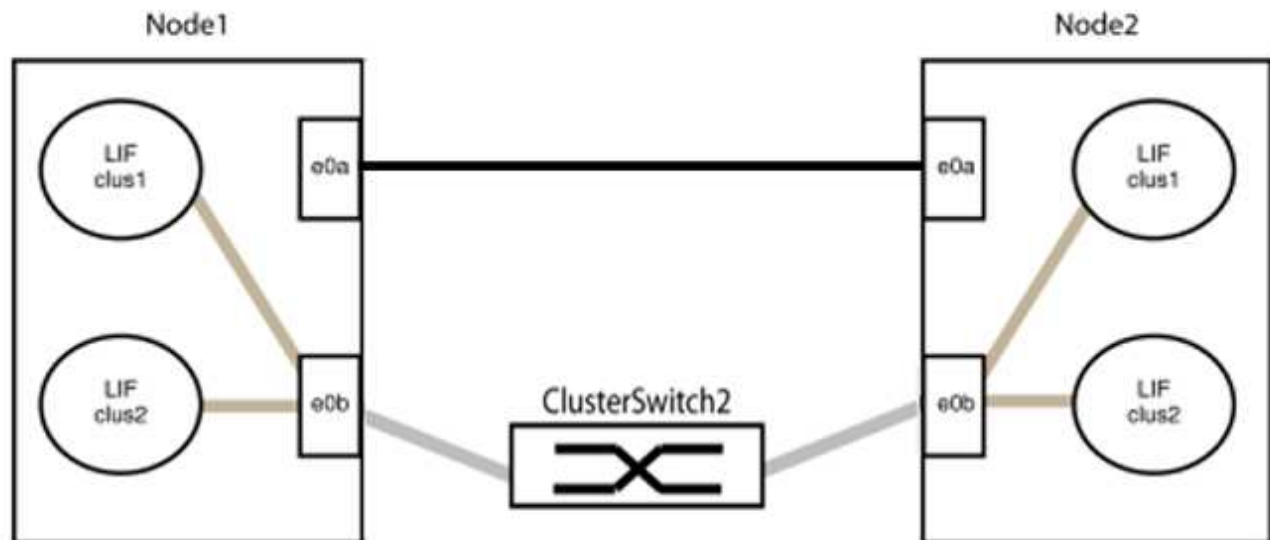
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

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

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

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

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:

```
cluster ping-cluster -node local
```



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

11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

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

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

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

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

Cisco Nexus 9336C-FX2

Überblick

Überblick über Installation und Konfiguration von Cisco Nexus 9336C-FX2 Cluster-Switches

Der Cisco Nexus 9336C-FX2 Cluster-Switch ist Teil der Cisco Nexus 9000 Plattform und kann in einem NetApp System-Rack installiert werden. Dank Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Nodes erstellen.

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen Cisco Nexus 9336C-FX2 Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Füllen Sie das Cisco Nexus 9336C-FX2-Verkabelungsarbeitsblatt aus"](#). Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.
2. ["Den Schalter einbauen"](#). Richten Sie die Switch-Hardware ein.
3. ["Konfigurieren Sie den Cluster-Switch 9336C-FX2"](#). Richten Sie den Cisco Nexus 9336C-FX2 Switch ein.
4. ["Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack"](#). Je nach Konfiguration können Sie den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Panel in einem NetApp Rack mit den im Lieferumfang des Switches enthaltenen Standardhalterungen installieren.
5. ["Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor"](#). Befolgen Sie die vorbereitenden Verfahren zur Installation der Cisco NX-OS-Software und der Referenzkonfigurationsdateien (RCFs).
6. ["Installieren Sie die NX-OS-Software"](#). Installieren Sie die NX-OS-Software auf dem Nexus 9336C-FX2 Cluster Switch.
7. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)."](#) Installieren Sie den RCF, nachdem Sie den Nexus 9336C-FX2-Schalter zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)
- ["Anforderungen für Smart Call Home"](#)

Konfigurationsanforderungen für Cisco Nexus 9336C-FX2 Cluster Switches

Prüfen Sie bei der Installation und Wartung von Cisco Nexus 9336C-FX2 Switches die Konfigurations- und Netzwerkanforderungen.

ONTAP Support

Ab ONTAP 9.9 können Sie mithilfe von Cisco Nexus 9336C-FX2 Switches Storage- und Cluster-Funktionen in einer gemeinsamen Switch-Konfiguration kombinieren.

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Netzwerk-Switches erforderlich.

Konfigurationsanforderungen

Stellen Sie sicher, dass:

- Sie verfügen über die entsprechende Anzahl und den entsprechenden Kabeltyp und Kabelstecker für Ihre Switches. Siehe "[Hardware Universe](#)".
- Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie die folgenden Netzwerkinformationen.

- IP-Subnetz für den Management-Netzwerkdatenverkehr
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700s Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.
- Siehe "[Hardware Universe](#)" Aktuelle Informationen.

Weitere Informationen zur Erstkonfiguration des Switches finden Sie im folgenden Handbuch: "[Cisco Nexus 9336C-FX2 – Installations- und Upgrade-Leitfaden](#)".

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

Informationen zur Installation und Wartung von Cisco Nexus 9336C-FX2 Switches finden Sie in der Liste der Komponenten und Teilenummern.

In der folgenden Tabelle sind die Teilenummer und Beschreibung für den Switch 9336C-FX2, die Lüfter und die Netzteile aufgeführt:

Teilenummer	Beschreibung
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Zubehörkit X190001/X190003

Teilenummer	Beschreibung
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W Netzteil – Luftstrom am Port Side
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W Netzteil – Luftstrom für den seitlichen Ansauganschluss
X-NXA-LÜFTER-65CFM-PE	N9K-9336C 65 CFM, Luftstrom nach Anschlussseite
X-NXA-LÜFTER-65CFM-PI	N9K-9336C 65 CFM, Luftstrom zur Ansaugöffnung an der Seite des Ports

Dokumentationsanforderungen für Cisco Nexus 9336C-FX2-Switches

Überprüfen Sie bei der Installation und Wartung des Cisco Nexus 9336C-FX2 Switches spezielle Switch- und Controller-Dokumentation, um Ihre Cisco 9336-FX2-Switches und das ONTAP-Cluster einzurichten.

Switch-Dokumentation

Zum Einrichten der Cisco Nexus 9336C-FX2-Switches benötigen Sie die folgende Dokumentation über das ["Switches Der Cisco Nexus 9000-Serie Unterstützen"](#) Seite:

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie <i>Nexus 9000</i>	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 9000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.
<i>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 9000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 9000-Switches.
<i>Nexus 9000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.

Dokumenttitel	Beschreibung
<i>Versionshinweise zur Cisco Nexus 9000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Betriebssystemversion über das ["ONTAP 9 Dokumentationszentrum"](#).

Name	Beschreibung
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP-Dokumentation	Dieser Service bietet detaillierte Informationen zu allen Aspekten der ONTAP Versionen.
"Hardware Universe"	Liefert Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Schienensatz und Rack-Dokumentation

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

Name	Beschreibung
"42-HE-System-Cabinet, Deep Guide"	Beschreibt die FRUs, die dem 42U-Systemschrank zugeordnet sind, und bietet Anweisungen für Wartung und FRU-Austausch.
"Installation eines Cisco 9336-FX2 Switch in einem NetApp Rack"	Beschreibt die Installation eines Cisco Nexus 9336C-FX2 Switches in einem NetApp Rack mit vier Pfosten.

Anforderungen für Smart Call Home

Gehen Sie wie folgt vor, um die Smart Call Home-Funktion zu verwenden.

Smart Call Home überwacht die Hardware- und Softwarekomponenten Ihres Netzwerks. Wenn eine kritische Systemkonfiguration auftritt, generiert es eine E-Mail-basierte Benachrichtigung und gibt eine Warnung an alle Empfänger aus, die im Zielfprofil konfiguriert sind. Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch konfigurieren, um per E-Mail mit dem Smart Call Home-System kommunizieren zu können. Darüber hinaus können Sie optional Ihren Cluster-Netzwerk-Switch einrichten, um die integrierte Smart Call Home-Support-Funktion von Cisco zu nutzen.

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

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.
- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.
- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

Der "[Cisco Support-Website](#)" Enthält Informationen zu den Befehlen zum Konfigurieren von Smart Call Home.

Hardware installieren

Füllen Sie das Cisco Nexus 9336C-FX2-Verkabelungsarbeitsblatt aus

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

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

Beispiel für eine Verkabelung

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	4 x 10-GbE-Node 1	1	4 x 10-GbE-Node 1
2	4 x 10-GbE-Node 2	2	4 x 10-GbE-Node 2
3	4x10 GbE Node 3	3	4x10 GbE Node 3
4	4 x 25-GbE-Node 4	4	4 x 25-GbE-Node 4
5	4 x 25-GbE-Node 5	5	4 x 25-GbE-Node 5
6	4 x 25-GbE-Node 6	6	4 x 25-GbE-Node 6
7	40/100-GbE-Node 7	7	40/100-GbE-Node 7
8	40/100-GbE-Node 8	8	40/100-GbE-Node 8

Cluster-Switch A		Cluster-Switch B	
9	40/100-GbE-Node 9	9	40/100-GbE-Node 9
10	40/100-GbE-Node 10	10	40/100-GbE-Node 10
11	40/100-GbE-Node 11	11	40/100-GbE-Node 11
12	40/100-GbE-Node 12	12	40/100-GbE-Node 12
13	40/100-GbE-Node 13	13	40/100-GbE-Node 13
14	40/100-GbE-Node 14	14	40/100-GbE-Node 14
15	40/100-GbE-Node 15	15	40/100-GbE-Node 15
16	40/100-GbE-Node 16	16	40/100-GbE-Node 16
17	40/100-GbE-Node 17	17	40/100-GbE-Node 17
18	40/100-GbE-Node 18	18	40/100-GbE-Node 18
19	40/100-GbE-Node 19	19	40/100-GbE-Node 19
20	40/100-GbE-Node 20	20	40/100-GbE-Node 20
21	40/100-GbE-Node 21	21	40/100-GbE-Node 21
22	40/100-GbE-Node 22	22	40/100-GbE-Node 22
23	40/100-GbE-Node 23	23	40/100-GbE-Node 23
24	40/100-GbE-Node 24	24	40/100-GbE-Node 24
25 bis 34	Reserviert	25 bis 34	Reserviert
35	100-GbE-ISL zu Switch B-Port 35	35	100-GbE-ISL für Switch A-Port 35
36	100-GbE-ISL zu Switch B-Port 36	36	100-GbE-ISL für Switch A-Port 36

Leeres Verkabelungsarbeitsblatt

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des ["Hardware"](#)

Universe" Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	

Cluster-Switch A		Cluster-Switch B	
22		22	
23		23	
24		24	
25 bis 34	Reserviert	25 bis 34	Reserviert
35	100-GbE-ISL zu Switch B-Port 35	35	100-GbE-ISL für Switch A-Port 35
36	100-GbE-ISL zu Switch B-Port 36	36	100-GbE-ISL für Switch A-Port 36

Siehe ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

Installieren Sie den Cluster-Switch 9336C-FX2

Gehen Sie wie folgt vor, um den Cisco Nexus 9336C-FX2 Switch einzurichten und zu konfigurieren.

Was Sie benötigen

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von ["Cisco Software-Download"](#) Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossen ["Verkabelungsarbeitsblätter"](#).
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden ["mysupport.netapp.com"](#). Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- ["Erforderliche Switch- und ONTAP-Dokumentation"](#).

Schritte

1. Rack-Aufbau des Cluster-Netzwerks und der Management-Netzwerk-Switches und -Controller

Wenn Sie den installieren...	Dann...
Cisco Nexus 9336C-FX2 in einem NetApp Systemschrank	Anweisungen zur Installation des Switches in einem NetApp Rack sind im Dokument _Installation eines Cisco Nexus 9336C-FX2 Cluster-Switch und Pass-Through-Panel in einem NetApp Rack enthalten.

Wenn Sie den installieren...	Dann...
Geräte in einem Telco-Rack	Siehe die Verfahren in den Installationsleitfäden für die Switch-Hardware sowie in den Installations- und Setup-Anleitungen für NetApp.

2. Verkabeln Sie die Switches für das Cluster-Netzwerk und das Management-Netzwerk mithilfe der ausgefüllten Verkabelungsarbeitsblätter mit den Controllern.
3. Schalten Sie das Cluster-Netzwerk sowie die Switches und Controller des Managementnetzwerks ein.

Was kommt als Nächstes?

Gehen Sie zu ["Konfigurieren Sie den Cisco Nexus 9336C-FX2 Switch"](#).

Konfigurieren Sie den Cluster-Switch 9336C-FX2

Gehen Sie folgendermaßen vor, um den Cisco Nexus 9336C-FX2-Switch zu konfigurieren.

Was Sie benötigen


- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von ["Cisco Software-Download"](#) Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossen ["Verkabelungsarbeitsblätter"](#).
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden ["mysupport.netapp.com"](#). Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- ["Erforderliche Switch- und ONTAP-Dokumentation"](#).


Schritte

1. Initiale Konfiguration der Cluster-Netzwerk-Switches durchführen.

Geben Sie beim ersten Booten des Switches die folgenden Einrichtungsfragen entsprechend an. Die Sicherheitsrichtlinie Ihres Standorts definiert die zu erstellenden Antworten und Services.

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit ja . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (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, starkes Passwort erstellen. Ein schwaches Kennwort kann abgelehnt werden.

Eingabeaufforderung	Antwort
Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)	Reagieren Sie mit ja bei der Erstkonfiguration des Schalters.
Noch ein Login-Konto erstellen? (ja/nein)	Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen. Der Standardwert ist no .
Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Geben Sie den Switch-Namen ein.	Geben Sie den Switch-Namen ein, der auf 63 alphanumerische Zeichen begrenzt ist.
Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)	Beantworten Sie mit ja (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein.
Standard-Gateway konfigurieren? (ja/nein)	Antworten Sie mit ja . Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit ja. Die Standardeinstellung ist ja.</p> <div>  <p>SSH wird empfohlen, wenn Sie Cluster Switch Health Monitor (CSHM) für seine Protokollerfassung verwenden. SSHv2 wird auch für erhöhte Sicherheit empfohlen.</p> </div>
Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1).	Der Standardwert ist rsa .
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits von 1024 bis 2048 ein.
Konfigurieren Sie den NTP-Server? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein

Eingabeaufforderung	Antwort
Konfigurieren der Standard-Schnittstellenebene (L3/L2)	Antworten Sie mit L2 . Der Standardwert ist L2.
Konfiguration des Status der Standard-Switch-Port-Schnittstelle (Shutter/noshut)	Antworten Sie mit noshut . Die Standardeinstellung ist noshut.
Konfiguration des CoPP-Systemprofils (streng/mittelmäßig/lenient/dense)	Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, antworten Sie mit No an der Eingabeaufforderung. Beantworten Sie mit ja , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)	<p>Antworten Sie mit ja, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert.</p> <div>  <p>Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam.</p> </div>

- Überprüfen Sie die Konfigurationseinstellungen, die Sie am Ende der Einrichtung in der Anzeige vorgenommen haben, und stellen Sie sicher, dass Sie die Konfiguration speichern.
- Überprüfen Sie die Version der Cluster-Netzwerk-Switches und laden Sie bei Bedarf die von NetApp unterstützte Version der Software von auf die Switches von herunter "[Cisco Software-Download](#)" Seite.

Was kommt als Nächstes?

Optional können Sie "[Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack](#)". Andernfalls fahren Sie mit fort "[Bereiten Sie sich auf die Installation von NX-OS und RCF vor](#)".

Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack

Je nach Konfiguration müssen Sie möglicherweise den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Tafel in einem NetApp Rack installieren. Standardhalterungen sind im Lieferumfang des Schalters enthalten.

Was Sie benötigen

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

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

- Ein Durchlauf-Blindblech
- Vier 10-32 x 0,75 Schrauben

- Vier 10-32-Clip-Muttern
- Für jeden Schalter sind acht 10-32 oder 12-24 Schrauben und Muttern zu befestigen, um die Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten zu befestigen.
- Den Cisco Standard-Schienensatz zur Installation des Switch in einem NetApp Rack



Die Jumper-Kabel sind nicht im Lieferumfang des Pass-Through-Kits enthalten und sollten in Ihrem Switch enthalten sein. Wenn die Switches nicht im Lieferumfang enthalten sind, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

- Informationen zu den anfänglichen Vorbereitungsanforderungen, zum Inhalt des Kits und zu Sicherheitsvorkehrungen finden Sie unter "[Hardware-Installationsleitfaden Der Cisco Nexus 9000-Serie](#)".

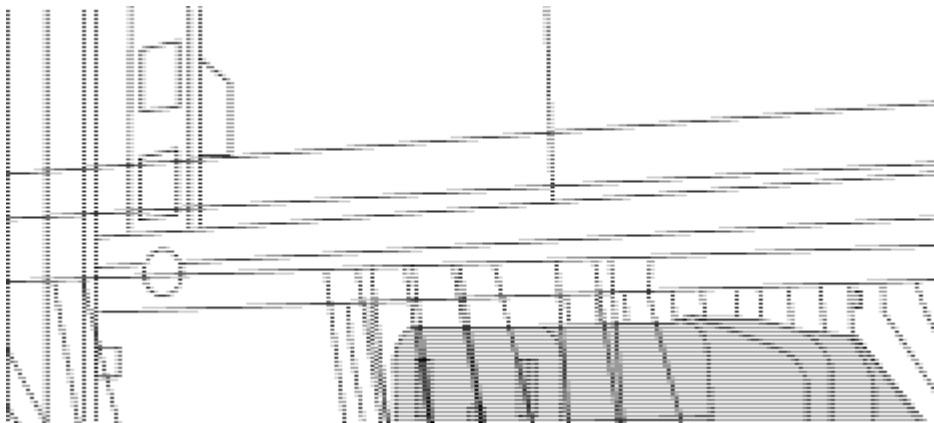
Schritte

1. Die Pass-Through-Blindplatte in den NetApp-Schrank einbauen.

- Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

Bei diesem Verfahren ist die Blindplatte in U40 installiert.

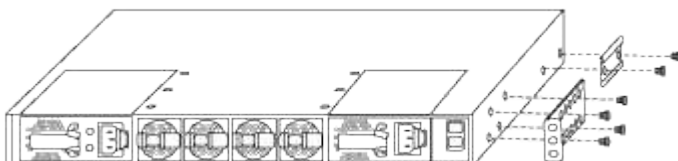
- Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
- Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
- Stecken Sie die Buchsen der beiden 48-Zoll-Jumper-Kabel von der Rückseite der Abdeckung und durch die Bürstenbaugruppe.



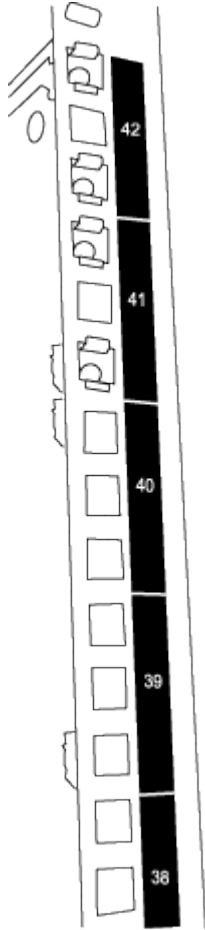
(1) Buchsenleiste des Überbrückungskabels.

2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Gehäuse des Nexus 9336C-FX2.

- Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.

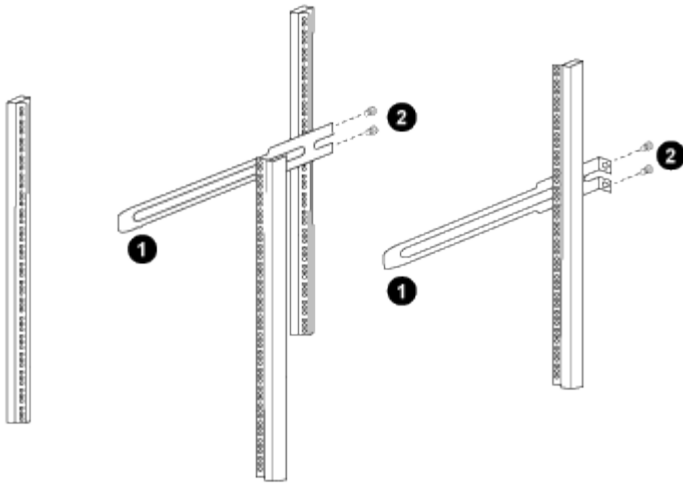


- b. Wiederholen Sie den Schritt [2 a](#) Mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
 - c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.
 - d. Wiederholen Sie den Schritt [2c](#) Mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite des Schalters.
3. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



Die beiden 9336C-FX2 Schalter sind immer in der oberen 2 HE des Schrankes RU41 und 42 montiert.

4. Installieren Sie die Gleitschienen im Schrank.
 - a. Positionieren Sie die erste Gleitschiene an der RU42-Markierung auf der Rückseite des hinteren linken Pfosten, legen Sie die Schrauben mit dem entsprechenden Gewindetyp ein und ziehen Sie die Schrauben mit den Fingern fest.



(1) beim sanften Schieben der Gleitschiene richten Sie sie an den Schraubenbohrungen im Rack aus.

(2) Schrauben der Gleitschienen an den Schrankleisten festziehen.

a. Wiederholen Sie den Schritt 4 a Für die hintere Säule auf der rechten Seite.

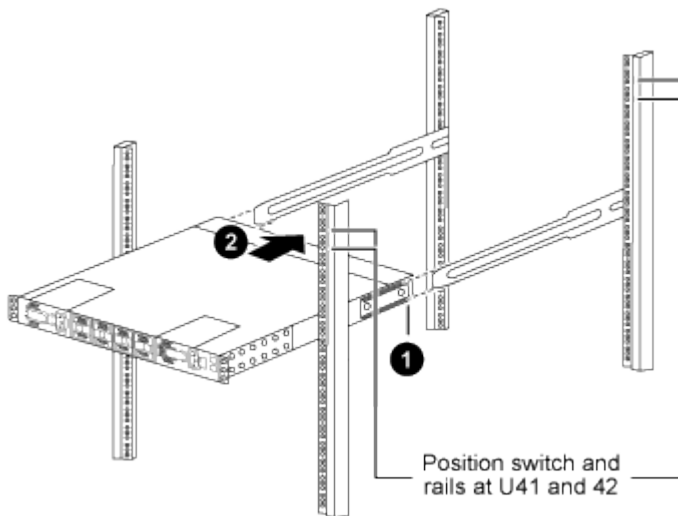
b. Wiederholen Sie die Schritte 4 a Und 4b An den RU41 Standorten auf dem Schrank.

5. Den Schalter in den Schrank einbauen.



Für diesen Schritt sind zwei Personen erforderlich: Eine Person muss den Schalter von vorne und von der anderen in die hinteren Gleitschienen führen.

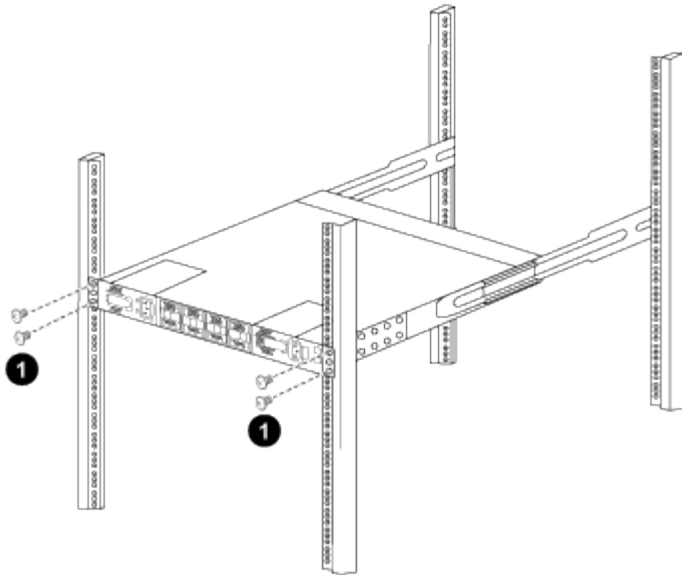
a. Positionieren Sie die Rückseite des Schalters an RU41.



(1) Da das Gehäuse in Richtung der hinteren Pfosten geschoben wird, richten Sie die beiden hinteren Rackmontageführungen an den Gleitschienen aus.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Halterungen der Rackmontage bündig mit den vorderen Pfosten sind.

b. Befestigen Sie den Schalter am Gehäuse.



(1) mit einer Person, die die Vorderseite des Chassis hält, sollte die andere Person die vier hinteren Schrauben vollständig an den Schrankpfosten festziehen.

- a. Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- b. Wiederholen Sie die Schritte [5a](#) Bis [5c](#) Für den zweiten Schalter an der RU42-Position.



Durch die Verwendung des vollständig installierten Schalters als Unterstützung ist es nicht erforderlich, während des Installationsvorgangs die Vorderseite des zweiten Schalters zu halten.

6. Wenn die Switches installiert sind, verbinden Sie die Jumper-Kabel mit den Switch-Netzeinkabeln.
7. Verbinden Sie die Stecker beider Überbrückungskabel mit den am nächsten verfügbaren PDU-Steckdosen.



Um Redundanz zu erhalten, müssen die beiden Kabel mit verschiedenen PDUs verbunden werden.

8. Verbinden Sie den Management Port an jedem 9336C-FX2 Switch mit einem der Management-Switches (falls bestellt) oder verbinden Sie sie direkt mit dem Management-Netzwerk.

Der Management-Port ist der oben rechts gelegene Port auf der PSU-Seite des Switch. Das CAT6-Kabel für jeden Switch muss über die Passthrough-Leiste geführt werden, nachdem die Switches zur Verbindung mit den Management-Switches oder dem Management-Netzwerk installiert wurden.

Was kommt als Nächstes?

["Konfigurieren Sie den Cisco Nexus 9336C-FX2 Switch".](#)

Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 9336C-FX2-Switch konfigurieren, gehen Sie die folgenden Überlegungen durch.

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

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 Switch-Port-Geschwindigkeit fest kodieren.

```
(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 "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

Anforderungen für 25 GbE FEC

FAS2820 e0a/e0b-Ports

FAS2820 e0a und e0b Ports erfordern Änderungen der FEC-Konfiguration, um über 9336C-FX2 Switch-Ports verbunden zu werden.

Für die Switch-Ports e0a und e0b ist die fec-Einstellung auf festgelegt `rs-cons16`.

```
(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
```

Software konfigurieren

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

So installieren und konfigurieren Sie die Software für einen Cisco Nexus 9336C-FX2 Switch:

1. "[Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor](#)".
2. "[Installieren Sie die NX-OS-Software](#)".
3. "[Installieren Sie die Referenzkonfigurationsdatei \(RCF\)](#)".

Installieren Sie den RCF, nachdem Sie den Nexus 9336C-FX2-Schalter zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Verfügbare RCF-Konfigurationen

In der folgenden Tabelle werden die für verschiedene Konfigurationen verfügbaren RCFs beschrieben. Wählen Sie den RCF aus, der für Ihre Konfiguration geeignet ist.

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

RCF-Name	Beschreibung
2-Cluster-HA-Breakout an	Unterstützt zwei ONTAP-Cluster mit mindestens acht Nodes, einschließlich Nodes, die gemeinsam genutzte Cluster + HA-Ports verwenden.
4-Cluster-HA-Breakout an	Unterstützt vier ONTAP-Cluster mit mindestens vier Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
1-Cluster-HA	Alle Ports sind für 40/100-GbE konfiguriert. Unterstützt Shared Cluster/HA-Datenverkehr auf Ports. Erforderlich für Systeme AFF A320, AFF A250 und FAS500f Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
1-Cluster-HA-Breakout an	Die Ports sind für 4x10-GbE-Breakout, 4x25-GbE-Breakout (RCF 1.6+ auf 100-GbE-Switches) und 40/100-GbE-Breakout konfiguriert. Unterstützt Shared-Cluster-/HA-Traffic auf Ports für Nodes, die Shared-Cluster/HA-Ports verwenden: AFF A320, AFF A250 und FAS500f Systeme. Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
Cluster-HA-Storage	Die Ports sind für 40/100 GbE für Cluster+HA, 4 x 10 GbE Breakout für Cluster und 4 x 25 GbE Breakout für Cluster+HA und 100 GbE für jedes Storage HA-Paar konfiguriert.
Cluster	Zwei RCF-Varianten mit unterschiedlichen Zuweisungen von 4x10GbE-Ports (Breakout) und 40/100-GbE-Ports. Alle FAS/AFF Nodes werden unterstützt, außer AFF A320, AFF A250 und FAS500f Systeme.
Storage	Alle Ports sind für 100-GbE-NVMe-Storage-Verbindungen konfiguriert.

Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor

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

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.

- Die Node-Namen sind cluster1-01 und cluster1-02.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1 und cluster1-01_clus2 für cluster1-01 und cluster1-02_clusions1 und cluster1-02_clus2 für cluster1-02.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=x h`

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

Beispiel anzeigen

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

```
`network port show -ip space Cluster`
```

Beispiel anzeigen

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

```
Node: cluster1-02
```

Health					Speed (Mbps)	
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
```

Health					Speed (Mbps)	
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. Zeigt Informationen zu den LIFs an:

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


Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
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. Ping für die Remote-Cluster-LIFs:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node cluster1-02
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)
```

6. Vergewissern Sie sich, dass der automatische Zurücksetzen-Befehl 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
```

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

4 entries were displayed.

7. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password Und system switch ethernet log enable-collection
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

8. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

system cluster-switch log setup-password Und system cluster-switch log enable-collection

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Was kommt als Nächstes?

["Installieren Sie die NX-OS-Software"](#).

Installieren Sie die NX-OS-Software

Gehen Sie folgendermaßen vor, um die NX-OS-Software auf dem Nexus 9336C-FX2-Cluster-Switch zu installieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- ["Cisco Ethernet Switch Seite"](#). In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.
- Entsprechende Leitfäden für Software und Upgrades auf der Cisco Website für die Upgrade- und Downgrade-Verfahren von Cisco Switches. Siehe ["Switches Der Cisco Nexus 9000-Serie"](#).

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clusions1, cluster1-02_clus2 , cluster1-03_clug1, Cluster1-03_clus2, cluster1-04_clut1, und cluster1-04_clus2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Installieren Sie die Software

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Überprüfen Sie mit dem Ping-Befehl die Verbindung zum Server, der die NX-OS-Software und die RCF hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

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

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

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

Beispiel anzeigen

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

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

cs2# copy sftp: bootflash: vrf management

Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

4. 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#
```

5. Installieren Sie das NX-OS Image.

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

Beispiel anzeigen

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

```
Installer will perform compatibility check first. Please wait.
```

```
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
```

```
[#####] 100% -- SUCCESS
```

```
Verifying image type.
```

```
[#####] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Performing module support checks.
```

```
[#####] 100% -- SUCCESS
```

```
Notifying services about system upgrade.
```

```
[#####] 100% -- SUCCESS
```

```
Compatibility check is done:
```

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

```
Images will be upgraded according to following table:
```

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

```
Switch will be reloaded for disruptive upgrade.

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

Install is in progress, please wait.

Performing runtime checks.
[#####] 100% -- SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

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

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

6. 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:
```

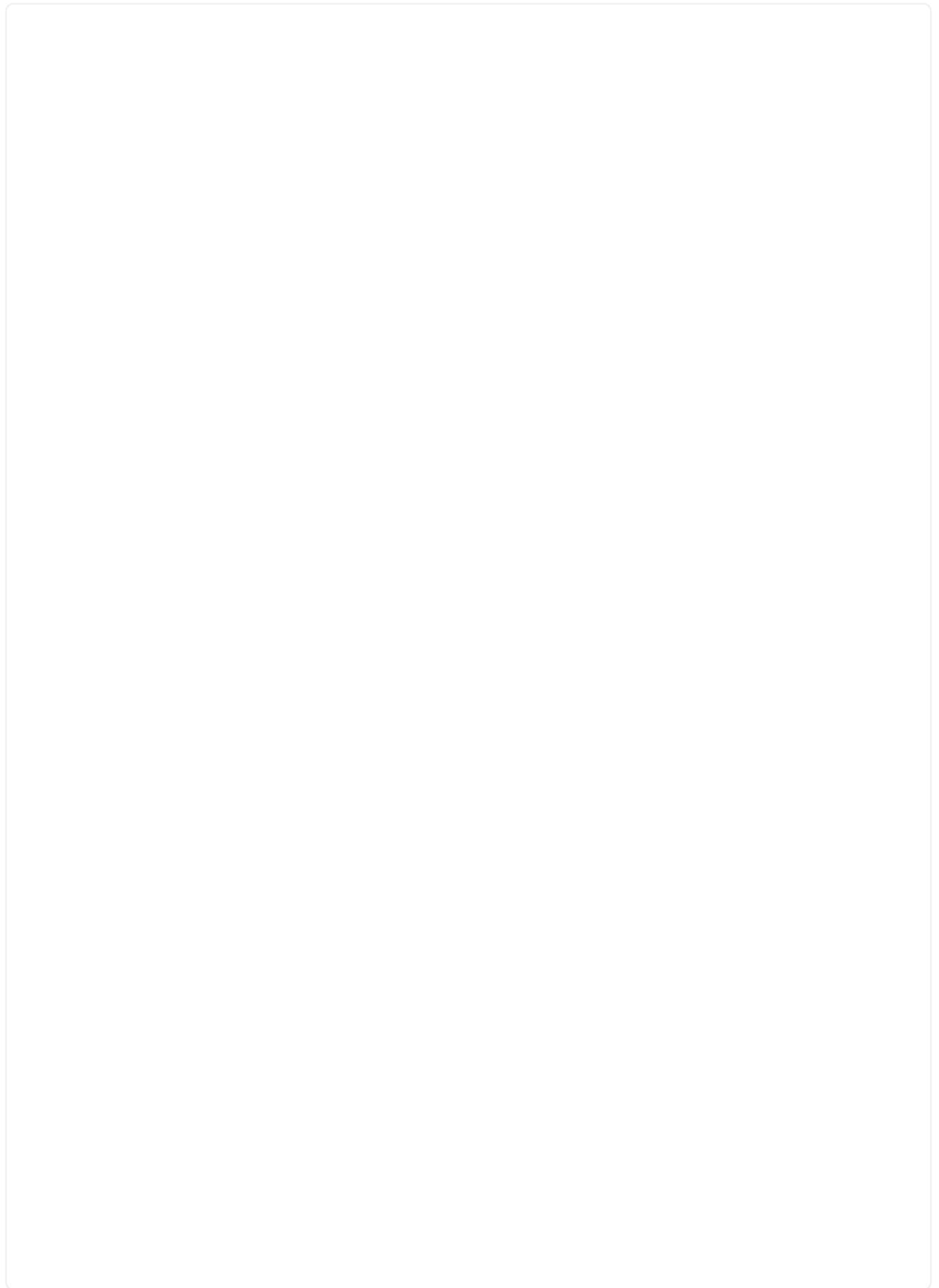
```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen



```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	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.

8. Melden Sie sich nach dem Neustart des Switches erneut an, und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

9. Wiederholen Sie die Schritte 1 bis 8, um die NX-OS-Software auf Switch cs1 zu installieren.

Was kommt als Nächstes?

["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)."](#)

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können die Referenzkonfigurationsdatei (RCF) installieren, nachdem Sie den Nexus 9336C-FX2-Switch zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).

Weitere Informationen zu den verfügbaren RCF-Konfigurationen finden Sie unter ["Workflow für die Softwareinstallation"](#).

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle RCF-Datei.
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.

Vorgeschlagene Dokumentation

- ["Cisco Ethernet Switch Seite"](#) In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.

- "[Switches Der Cisco Nexus 3000-Serie](#)". Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie das RCF

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clusions1, cluster1-02_clus2, cluster1-03_clug1, Cluster1-03_clus2, cluster1-04_clut1, und cluster1-04_clus2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster Interconnect-Ports e0a und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein. Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritt 1: Vorbereitung für die Installation

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N9K-
C9336C
          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 Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports **up** mit einem gesunden Status sind:

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

Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

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

	Logical	Status	Network	
Current	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.90      N9K-
C9336C
    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. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

Schritt 2: Ports konfigurieren

1. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

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

2. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```


Beispiel anzeigen

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

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

```
show running-config
```

5. Reinigen Sie die Konfiguration am Schalter cs2, und führen Sie eine grundlegende Einrichtung durch.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload

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

6. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

```
cs2# 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)...
```

7. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt Installation auf Schalter cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

8. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

Beispiel anzeigen

```
cs2# 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
*
*****
*****
```

9. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

10. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

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

11. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

12. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß 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.

- a. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

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 können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
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. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels verwendet:

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

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

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


Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

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

```
cluster show
```

Beispiel anzeigen

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

16. Wiederholen Sie die Schritte 4 bis 11 am Schalter cs1.
17. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

18. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

Schritt 3: Überprüfen Sie die Konfiguration

1. Stellen Sie sicher, dass die mit den Cluster-Ports verbundenen Switch-Ports **up** sind.

```
show interface brief
```

Beispiel anzeigen

```
cs1# show interface brief | grep up
.
.
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 Nodes weiterhin 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
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
```

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

```
show vlan brief
```

```
show interface trunk
```

Beispiel anzeigen

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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
..
..
..
..
..
```



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

4. Stellen Sie sicher, dass die ISL 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      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
```

```
cs1#
```

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	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::*>				

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

```
cluster show
```

Beispiel anzeigen

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

7. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

```
cluster ping-cluster -node local
```

Beispiel anzeigen

```
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)
```

Aktivieren Sie SSH auf Cisco 9336C-FX2 Cluster-Switches

Wenn Sie Cluster Switch Health Monitor (CSHM) und Funktionen zur Protokollerfassung verwenden, müssen Sie SSH-Schlüssel generieren und dann SSH auf den Cluster-

Switches aktivieren.

Schritte

1. Vergewissern Sie sich, dass 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
```

2. Generieren der 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

(switch) (Config)# aaa authorization commands "noCmdAuthList" none
(switch) (Config)# exit
(switch)# ip ssh server enable
(switch)# ip scp server enable
(switch)# ip ssh pubkey-auth
(switch)# write mem

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!
```

3. Starten Sie den Switch neu:

```
reload
```

4. Vergewissern Sie sich, dass 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
```

Was kommt als Nächstes?

["Aktivieren Sie die Protokollerfassung"](#).

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung mit dem Cluster-Switch 9336C-FX2 * CLI* eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```


Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 9336C-FX2-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                        SNMP USERS
-----
-----

User                Auth                Priv(enforce)    Groups
acl_filter
-----
-----
admin                md5                des(no)          network-admin
SNMPv3User           md5                aes-128(no)      network-operator
-----
-----

      NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User                Auth                Priv
-----
-----

(sw1) (Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Switches migrieren

Migration von einem NetApp CN1610 Cluster-Switch zu einem Cisco 9336C-FX2 Cluster-Switch

Sie können NetApp CN1610-Cluster-Switches für ein ONTAP-Cluster zu Cisco 9336C-FX2 Cluster-Switches migrieren. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Wenn Sie NetApp CN1610-Cluster-Switches durch Cisco 9336C-FX2 Cluster-Switches ersetzen, müssen Sie sich über bestimmte Konfigurationsdaten, Port-Verbindungen und Verkabelungsanforderungen im Klaren sein.

Unterstützte Switches

Folgende Cluster-Switches werden unterstützt:

- NetApp CN1610
- Cisco 9336C-FX2

Weitere Informationen zu unterstützten Ports und deren Konfigurationen finden Sie im ["Hardware Universe"](#).

Was Sie benötigen

Stellen Sie sicher, dass Ihre Konfiguration die folgenden Anforderungen erfüllt:

- Der vorhandene Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die Cisco 9336C-FX2 Cluster-Switches werden unter der richtigen NX-OS-Version konfiguriert und betrieben, die mit der angewendeten Referenzkonfigurationsdatei (RCF) installiert ist.
- Die vorhandene Cluster-Netzwerkconfiguration verfügt über folgende Merkmale:
 - Ein redundantes und voll funktionsfähiges NetApp Cluster mit NetApp CN1610 Switches.
 - Managementkonnektivität und Konsolenzugriff sowohl auf die NetApp CN1610-Switches als auch auf die neuen Switches.
 - Alle Cluster-LIFs im Status „up“ mit den Cluster-LIFs befinden sich auf den Home-Ports.
- Einige der Ports sind auf Cisco 9336C-FX2 Switches konfiguriert, um mit 40 GbE oder 100 GbE zu laufen.
- Sie haben die 40-GbE- und 100-GbE-Konnektivität von Nodes zu Cisco 9336C-FX2 Cluster-Switches geplant, migriert und dokumentiert.

Migrieren Sie die Switches

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen CN1610 Cluster Switches sind *C1* und *C2*.
- Die neuen Cluster-Switches 9336C-FX2 sind *cs1* und *cs2*.
- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node 1 *_clus1_* und *node1_clus2* und *node2_clus1* bzw. *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.

Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Schalter C2 wird zuerst durch Schalter cs2 ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und C2 wird dann von C2 getrennt und wieder mit cs2 verbunden.
- Switch C1 wird durch Switch cs1 ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und C1 wird dann von C1 getrennt und wieder mit cs1 verbunden.



Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

3. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

Schritt: Ports und Verkabelung konfigurieren

1. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

Jeder Port sollte für angezeigt werden `Link Und healthy Für Health Status`.

- a. Zeigen Sie die Attribute des Netzwerkports an:

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


Beispiel anzeigen

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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. Zeigt Informationen zu den LIFs und ihren zugewiesenen Home-Nodes an:

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

Jede LIF sollte angezeigt werden up/up Für Status Admin/Oper Und true Für Is Home.

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
	true			
e3b	node1_clus2	up/up	169.254.49.125/16	node1
	true			
e3a	node2_clus1	up/up	169.254.47.194/16	node2
	true			
e3b	node2_clus2	up/up	169.254.19.183/16	node2
	true			

2. Die Cluster-Ports auf jedem Node sind mit vorhandenen Cluster-Switches auf die folgende Weise (aus Sicht der Nodes) verbunden. Verwenden Sie dazu den Befehl:

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

Beispiel anzeigen

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

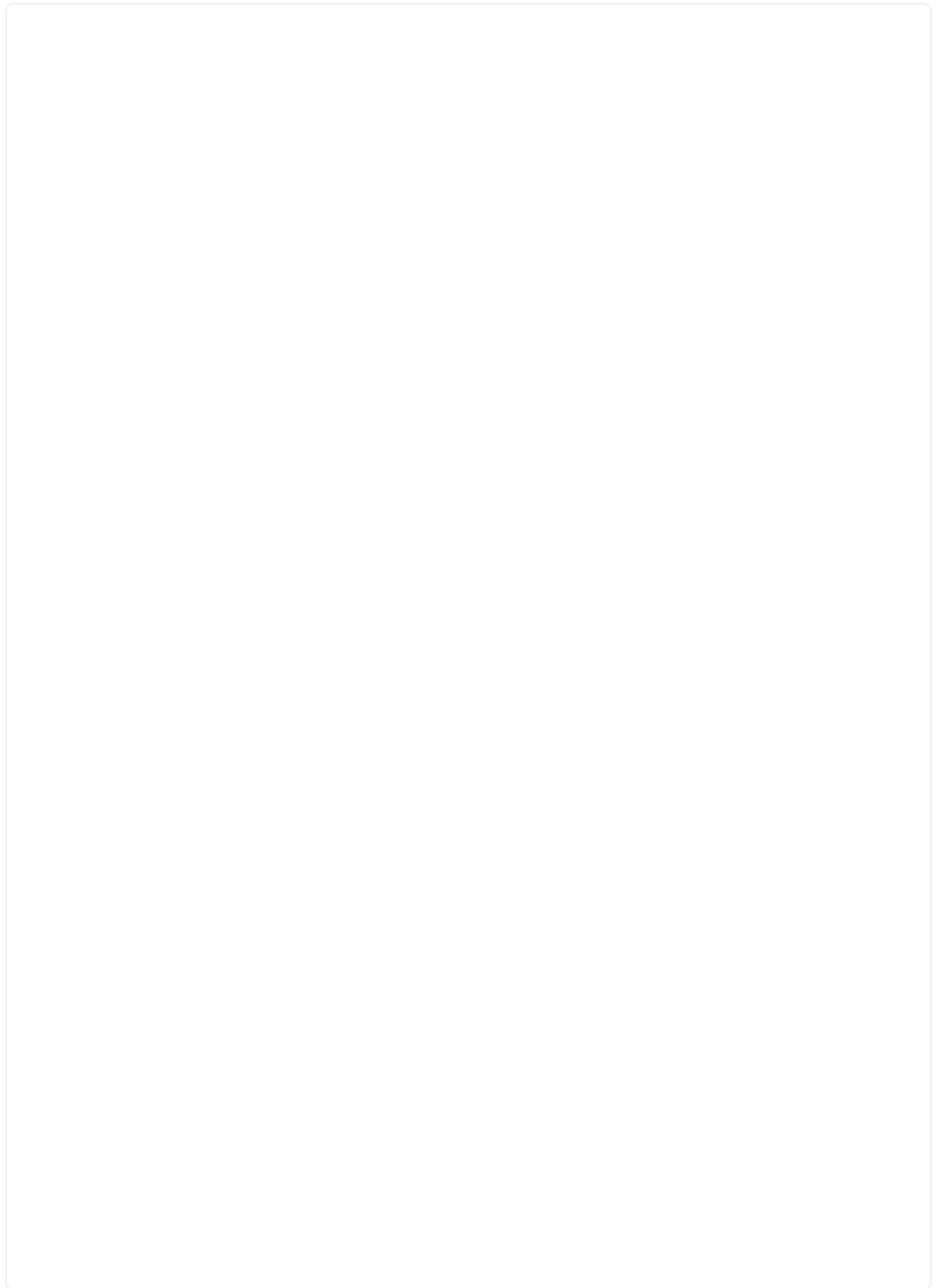
Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

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 sind (aus Sicht der Switches) folgendermaßen 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
C2 0/13	0/13	179	S I s	CN1610
C2 0/14	0/14	175	S I s	CN1610
C2 0/15	0/15	179	S I s	CN1610
C2 0/16	0/16	175	S I s	CN1610

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
C1 0/13	0/13	175	S I s	CN1610
C1 0/14	0/14	175	S I s	CN1610
C1 0/15	0/15	175	S I s	CN1610
C1 0/16	0/16	175	S I s	CN1610

4. Überprüfen Sie mit dem Befehl, ob das Cluster-Netzwerk vollständig verbunden ist:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node node2

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)
```

5. Fahren Sie auf Switch C2 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster-LIFs durchzuführen.

```
(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
```

6. Verschieben Sie die Knoten-Cluster-Ports vom alten Switch C2 auf den neuen Switch cs2. Verwenden Sie dabei die entsprechende Verkabelung, die von Cisco 9336C-FX2 unterstützt wird.
7. Zeigen Sie die Attribute des Netzwerkports an:

```
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						

8. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

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

Beispiel anzeigen

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

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

9. Überprüfen Sie bei Switch cs2, ob alle Node-Cluster-Ports aktiviert sind:

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

Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
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			

10. Fahren Sie auf Switch C1 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster LIFs zu ermöglichen.

```
(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
```

11. Verschieben Sie die Knoten-Cluster-Ports vom alten Switch C1 auf den neuen Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von Cisco 9336C-FX2 unterstützt wird.
12. Überprüfen der endgültigen Konfiguration des Clusters:

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

Jeder Port sollte angezeigt werden up Für Link Und healthy Für Health Status.

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						

13. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

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

Beispiel anzeigen

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

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

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				

14. Überprüfen Sie auf den Switches cs1 und cs2, ob alle Node-Cluster-Ports aktiviert sind:

```
network port show -ip space 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						

15. Vergewissern Sie sich, dass 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 Switches:

```
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: Führen Sie den Vorgang durch

1. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

2. Vergewissern Sie sich, dass alle Cluster-Netzwerk-LIFs wieder an ihren Home-Ports sind:

```
network interface show
```

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. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

4. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung erfolgreich war mit dem folgenden Befehl:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

5. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

6. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Migrieren Sie von einem älteren Cisco Switch zu einem Cisco Nexus 9336C-FX2 Cluster Switch

Eine unterbrechungsfreie Migration von einem älteren Cisco Cluster-Switch zu einem Cisco Nexus 9336C-FX2 Cluster-Netzwerk-Switch ist möglich.

Prüfen Sie die Anforderungen

Stellen Sie sicher, dass:

- Einige der Ports auf Nexus 9336C-FX2-Switches sind für 10-GbE- oder 40-GbE-Betrieb konfiguriert.
- Die 10GbE- und 40-GbE-Konnektivität von den Nodes zu Nexus 9336C-FX2 Cluster-Switches wurde geplant, migriert und dokumentiert.

- Das Cluster funktioniert voll (es sollten keine Fehler in den Protokollen oder ähnlichen Problemen geben).
- Die anfängliche Anpassung der Cisco Nexus 9336C-FX2 Switches lautet folgendermaßen:
 - 9336C-FX2-Switches führen die neueste empfohlene Version der Software aus.
 - Auf die Switches wurden Referenzkonfigurationsdateien (RCFs) angewendet.
 - Anpassung von Websites, z. B. DNS, NTP, SMTP, SNMP, Und SSH werden auf den neuen Switches konfiguriert.
- Sie haben Zugriff auf die Switch-Kompatibilitätstabelle auf der "[Cisco Ethernet-Switches](#)" Seite für die unterstützten ONTAP-, NX-OS- und RCF-Versionen.
- Sie haben die entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website für die Upgrade- und Downgrade-Verfahren von Cisco Switches unter geprüft "[Switches Der Cisco Nexus 9000-Serie Unterstützen](#)" Seite.



Wenn Sie die Portgeschwindigkeit der e0a- und e1a-Cluster-Ports auf AFF A800- oder AFF C800-Systemen ändern, können Sie beobachten, wie fehlerhafte Pakete nach der Geschwindigkeitskonvertierung empfangen werden. Siehe "[Bug 1570339](#)" Und den Knowledge Base Artikel "[CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE](#)" Für eine Anleitung.

Migrieren Sie die Switches

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster Interconnect-Ports e0a und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.

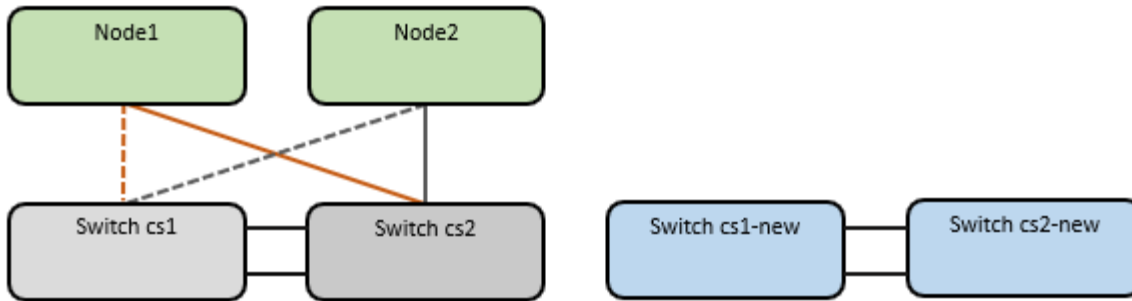


Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden vorhandenen Cisco Switches sind **cs1** und **cs2**
- Die neuen Nexus 9336C-FX2 Cluster Switches sind **cs1-neu** und **cs2-neu**.
- Die Knotennamen sind **node1** und **node2**.
- Die Cluster-LIF-Namen sind **node1_clus1** und **node1_clus2** für Knoten 1, und **node2_clus1** und **node2_clus2** für Knoten 2.
- Die Eingabeaufforderung **cluster1::>*** gibt den Namen des Clusters an.

Beachten Sie während dieses Verfahrens das folgende Beispiel:



Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP-Befehlen und "Switches Der Nexus 9000 Serie" Befehle; ONTAP-Befehle werden verwendet, sofern nicht anders angegeben.

Dieses Verfahren umfasst das folgende Szenario:

- Schalter cs2 wird zuerst durch Schalter cs2-New ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und cs2 wird dann von cs2 getrennt und wieder mit cs2-New verbunden.
- Switch cs1 wird durch Switch cs1-New ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und cs1 wird dann von cs1 getrennt und wieder mit cs1-New verbunden.



Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=xh`

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

Schritt: Ports und Verkabelung konfigurieren

1. Vergewissern Sie sich bei den neuen Switches, dass die ISL zwischen den Switches cs1-New und cs2-New verkabelt und ordnungsgemäß 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)
```

2. Anzeigen der Cluster-Ports an jedem Node, der mit den vorhandenen Cluster-Switches verbunden ist:

```
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
C5596UP			N5K-
	e0b	cs2	Ethernet1/2
C5596UP			N5K-
node2	/cdp		
	e0a	cs1	Ethernet1/1
C5596UP			N5K-
	e0b	cs2	Ethernet1/2
C5596UP			N5K-

3. Legen Sie den Administrations- oder Betriebsstatus für jeden Cluster-Port fest.

a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

Beispiel anzeigen

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

Node: node1

Ignore

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

Node: node2

Ignore

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

- b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) auf ihren Home-Ports befinden:

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

Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	node1_clus1	up/up	169.254.209.69/16	node1
e0b	true			
e0a	node1_clus2	up/up	169.254.49.125/16	node1
e0b	true			
e0a	node2_clus1	up/up	169.254.47.194/16	node2
e0b	true			
e0a	node2_clus2	up/up	169.254.19.183/16	node2
e0b	true			

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

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

Switch Model	Type	Address	
cs1 C5596UP	cluster-network	10.233.205.92	N5K-
Serial Number: FOXXXXXXXXGS			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(4)			
Version Source: CDP			
cs2 C5596UP	cluster-network	10.233.205.93	N5K-
Serial Number: FOXXXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(4)			
Version Source: CDP			

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

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



Durch die Deaktivierung der automatischen Zurücksetzung wird sichergestellt, dass ONTAP nur ein Failover der Cluster-LIFs übernimmt, wenn die Switch-Ports später heruntergefahren werden.

5. Fahren Sie auf Cluster-Switch cs2 die Ports herunter, die mit den Cluster-Ports von **all** Nodes verbunden sind, um ein Failover der Cluster-LIFs zu ermöglichen:

```
cs2(config)# interface eth1/1-1/2
cs2(config-if-range)# shutdown
```

6. Vergewissern Sie sich, dass für die Cluster-LIFs ein Failover zu den auf Cluster-Switch cs1 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	169.254.3.4/16	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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

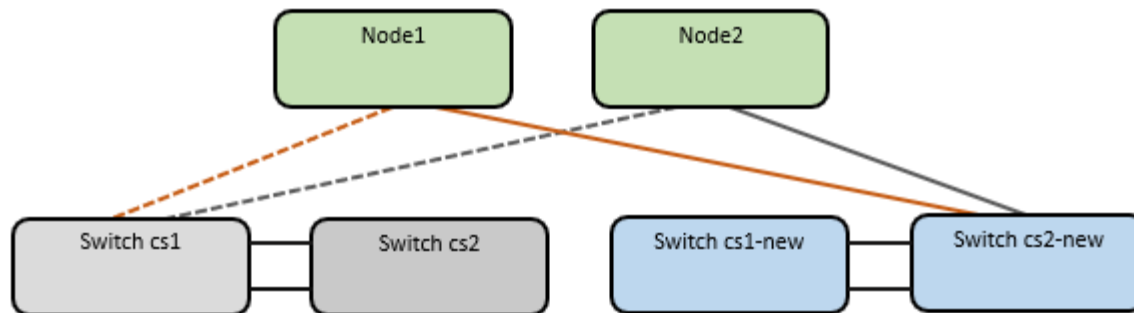
Beispiel anzeigen

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

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

8. Verschieben Sie alle Clusterknoten-Verbindungskabel vom alten cs2-Switch auf den neuen cs2-New-Switch.

Clusterknoten-Verbindungskabel wurden auf den cs2-New Switch verlegt



9. Überprüfen Sie den Zustand der zu cs2-New übergewechselt 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 nach oben erfolgen.

10. Überprüfen Sie die „Neighbor“-Informationen auf den Cluster-Ports:

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

Beispiel anzeigen

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

Node/ Protocol	Local Port	Discovered 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				

Vergewissern Sie sich, dass der cs2-neue Switch von den verschobenen Cluster-Ports als „Nachbarn“ angezeigt wird.

11. Bestätigen Sie die Switch-Port-Verbindungen aus der Perspektive von Switch cs2-New:

```
cs2-new# show interface brief
cs2-new# show cdp neighbors
```

12. Fahren Sie auf Cluster-Switch cs1 die Ports herunter, die mit den Cluster-Ports von **all** Nodes verbunden sind, um ein Failover der Cluster-LIFs durchzuführen.

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

Alle Cluster-LIFs führen einen Failover zum cs2-neuen Switch durch.

13. Überprüfen Sie, ob für die Cluster-LIFs ein Failover zu den auf Switch cs2-New 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	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			

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

```
cluster show
```

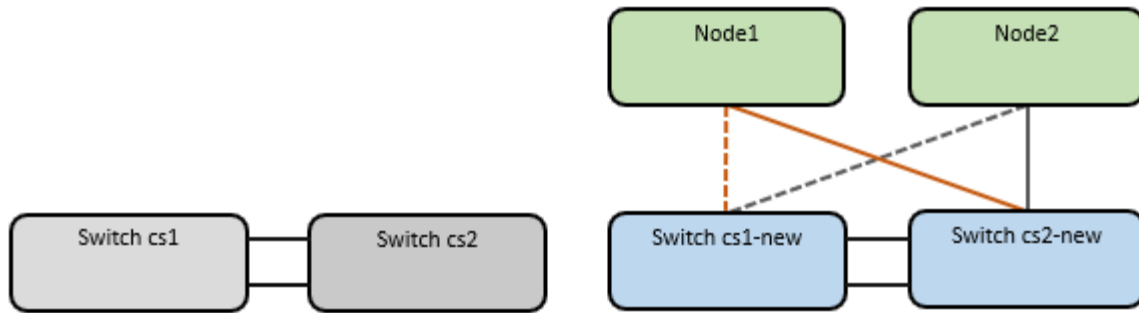
Beispiel anzeigen

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

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

15. Verschieben Sie die Verbindungskabel des Clusterknoten von cs1 zum neuen cs1-New-Switch.

Clusterknoten-Verbindungskabel wurden auf den cs1-New Switch verlegt



16. Überprüfen Sie den Zustand der zu cs1-New übergewechselt Netzwerkverbindungen:

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

Beispiel anzeigen

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

Node: node1

Ignore

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

Node: node2

Ignore

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

Alle verschobenen Cluster-Ports sollten nach oben erfolgen.

17. Überprüfen Sie die „Neighbor“-Informationen auf 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			

Vergewissern Sie sich, dass die verschobenen Cluster-Ports den cs1-neuen Switch als Nachbarn sehen.

18. Bestätigen Sie die Switch-Port-Verbindungen aus der Perspektive von Switch cs1-New:

```
cs1-new# show interface brief
cs1-new# show cdp neighbors
```

19. Vergewissern Sie sich, dass die ISL zwischen cs1-New und cs2-New weiterhin betriebsbereit 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)
```

Schritt 3: Überprüfen Sie die Konfiguration

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

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

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

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

Wenn die Cluster-LIFs nicht auf ihren Home-Port zurückgesetzt wurden, setzen Sie sie manuell zurück:

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

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

```
cluster show
```

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

ONTAP 9.9.1 und höher

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

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

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

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

```
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

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

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



```

cluster1::*> cluster ping-cluster -node 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. Aktivieren Sie die Protokollaufnahmefunktion für die Statusüberwachung des Ethernet-Switches, um Switch-bezogene Protokolldateien zu erfassen.

ONTAP 9.8 und höher

Aktivieren Sie die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden beiden Befehle:

```
system switch ethernet log setup-password Und system switch ethernet log enable-collection
```

HINWEIS: Sie benötigen das Passwort für den **admin**-Benutzer auf den Switches.

Geben Sie Ein: `system switch ethernet log setup-password`

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1-new
cs2-new

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1-new
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <password of switch's admin user>
Enter the password again: <password of switch's admin user>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2-new
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <password of switch's admin user>
Enter the password again: <password of switch's admin user>
```

Gefolgt von: `system switch ethernet log enable-collection`

```
cluster1::*> system switch ethernet log enable-collection
```

Do you want to enable cluster log collection for all nodes in the cluster?

```
{y|n}: [n] y
```

Enabling cluster switch log collection.

```
cluster1::*>
```

HINWEIS: Wenn einer dieser Befehle einen Fehler zurückgibt, wenden Sie sich an den NetApp Support.

ONTAP veröffentlicht 9.5P16, 9.6P12 und 9.7P10 sowie neuere Patch-Releases

Aktivieren Sie die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung mithilfe der Befehle, um Switch-bezogene Protokolldateien zu erfassen: `system cluster-switch log setup-password` und `system cluster-switch log enable-collection`

HINWEIS: Sie benötigen das Passwort für den **admin**-Benutzer auf den Switches.

Geben Sie Ein: `system cluster-switch log setup-password`

```
cluster1::*> system cluster-switch log setup-password
```

Enter the switch name: <return>

The switch name entered is not recognized.

Choose from the following list:

cs1-new

cs2-new

```
cluster1::*> system cluster-switch log setup-password
```

Enter the switch name: **cs1-new**

RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc

Do you want to continue? {y|n}::[n] **y**

Enter the password: <password of switch's admin user>

Enter the password again: <password of switch's admin user>

```
cluster1::*> system cluster-switch log setup-password
```

Enter the switch name: **cs2-new**

RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1

Do you want to continue? {y|n}:: [n] **y**

Enter the password: <password of switch's admin user>

Enter the password again: <password of switch's admin user>

Gefolgt von: `system cluster-switch log enable-collection`

```
cluster1::*> system cluster-switch log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```

HINWEIS: Wenn einer dieser Befehle einen Fehler zurückgibt, wenden Sie sich an den NetApp Support.

1. Wenn Sie die automatische Fehlerstellung unterdrückt haben, aktivieren Sie sie erneut, indem Sie eine AutoSupport-Meldung aufrufen: `system node autosupport invoke -node * -type all -message MAINT=END`

Migration auf Cluster mit zwei Nodes

Wenn Sie eine vorhandene Cluster-Umgebung mit zwei Nodes ohne oder ohne Switches nutzen, können Sie mithilfe von Cisco Nexus 9336C-FX2 zu einer *2-Node-Switched* -Cluster-Umgebung migrieren.

Der Migrationsprozess funktioniert bei allen Knoten mit optischen oder Twinax-Ports, wird von diesem Switch jedoch nicht unterstützt, wenn die Nodes integrierte 10 GB BASE-T RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Bei der Konfiguration mit zwei Nodes ohne Switches:
 - Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
 - Alle Cluster-Ports haben den Status **up**.
 - Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren Home-Ports.
 - Siehe "[Hardware Universe](#)" Für alle unterstützten ONTAP-Versionen.
- Für die Switch-Konfiguration des Cisco Nexus 9336C-FX2:
 - Beide Switches verfügen über Management-Netzwerk-Konnektivität.
 - Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
 - Bei den Nexus 9336C-FX2 Nodes-zu-Node-Switches und Switch-zu-Switch-Verbindungen werden Twinax- oder Glasfaserkabel verwendet.

Siehe "[Hardware Universe](#)" Weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel werden an den Anschlüssen 1/35 und 1/36 an beiden 9336C-FX2-Switches angeschlossen.

- Die anfängliche Anpassung der beiden 9336C-FX2-Switches erfolgt so, dass:
 - 9336C-FX2-Switches führen die neueste Version der Software aus.
 - Auf die Switches werden Referenzkonfigurationsdateien (RCFs) angewendet. Bei den neuen Switches werden alle Site-Anpassungen wie SMTP, SNMP und SSH konfiguriert.

Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der Schalter 9336C-FX2 lauten cs1 und cs2.
- Die Namen der Cluster SVMs sind node1 und node2.
- Die Namen der LIFs sind node1_clug1 und node1_clus2 auf Knoten 1, und node2_clus1 bzw. node2_clus2 auf Knoten 2.
- Der `cluster1 : *` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e0a und e0b.

Siehe "[Hardware Universe](#)" Weitere Informationen zu den Cluster-Ports für Ihre Plattformen.

Migrieren Sie die Switches

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y` Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

Schritt: Ports und Verkabelung konfigurieren

1. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches cs1 und cs2.

Deaktivieren Sie die ISL-Ports nicht.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 34 auf 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. Stellen Sie sicher, dass ISL und die physischen Ports auf der ISL zwischen den beiden 9336C-FX2-Switches cs1 und cs2 über die Ports 1/35 und 1/36 verfügen:

```
show port-channel summary
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports auf 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 auf 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 enthält Informationen zu den Geräten, die mit dem System verbunden sind.

Beispiel anzeigen

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs1 aufgeführt:

```
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
```

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs2 aufgeführt:

```
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. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

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

Jeder Port sollte für angezeigt werden Link Und gesund für Health Status.

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4 entries were displayed.

5. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

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

Jede Cluster-LIF sollte angezeigt werden true Für Is Home Und ich habe ein Status Admin/Oper Von up/Up.

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. Vergewissern Sie sich, dass die automatische Umrüstung 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		
	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

7. Trennen Sie das Kabel vom Cluster-Port e0a auf node1, und verbinden Sie dann e0a mit Port 1 am Cluster Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von den 9336C-FX2-Switches

unterstützt wird.

Der "[Hardware Universe – Switches](#)" Enthält weitere Informationen zur Verkabelung.

"Hardware Universe – Switches"

8. Trennen Sie das Kabel vom Cluster Port e0a auf node2, und verbinden Sie dann e0a mit Port 2 am Cluster Switch cs1. Verwenden Sie dabei die entsprechende Verkabelung, die von den 9336C-FX2 Switches unterstützt wird.
9. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/34 auf 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. Vergewissern Sie sich, dass alle Cluster-LIFs aktiv und betriebsbereit sind und als angezeigt werden `true`
Für Is Home:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs sich auf node1 und node2 befinden und dass Is Home Die Ergebnisse sind wahr:

```
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.

11. Informationen zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

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

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

2 entries were displayed.

12. Trennen Sie das Kabel von Cluster-Port e0b auf node1, und verbinden Sie dann e0b mit Port 1 am Cluster

Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den 9336C-FX2 Switches unterstützt wird.

13. Trennen Sie das Kabel von Cluster-Port e0b auf node2, und verbinden Sie dann e0b mit Port 2 am Cluster Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den 9336C-FX2 Switches unterstützt wird.
14. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs2.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/34 auf 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. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

```
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: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass alle Schnittstellen für „true“ anzeigen Is Home:

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



Dies kann einige Minuten dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf node1 und node2 liegen und dass Is Home Die Ergebnisse sind wahr:

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

Current Is	Logical	Status	Network	Current	
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.

2. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
show cdp neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
(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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs2 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs2 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	133	H	FAS2980
node2 e0b	Eth1/2	133	H	FAS2980
cs1 Eth1/35	Eth1/35	175	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	175	R S I s	N9K-C9336C

Total entries displayed: 4

3. Zeigen Sie Informationen zu den erkannten Netzwerkgeräten im Cluster an:

```
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.
```

4. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

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



Es kann einige Minuten dauern, bis der Befehl abgeschlossen ist. Warten Sie, bis die Ankündigung „3 Minuten Lebensdauer abläuft“ abläuft.

Beispiel anzeigen

Die falsche Ausgabe im folgenden Beispiel zeigt an, dass die Konfigurationseinstellungen deaktiviert sind:

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

5. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

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

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

6. Vergewissern Sie sich, dass das Cluster-Netzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
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 169.254.47.194 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)

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

8. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password Und system switch ethernet log  
enable-collection
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

9. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

system cluster-switch log setup-password **Und** system cluster-switch log enable-collection

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

10. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem

Sie eine AutoSupport Meldung aufrufen:

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

Tauschen Sie die Schalter aus

Ersetzen Sie einen Cisco Nexus 9336C-FX2 Cluster-Switch

Führen Sie diese Schritte aus, um einen defekten Nexus 9336C-FX2-Switch in einem Cluster-Netzwerk zu ersetzen. Dies ist ein NDU (Non Disruptive Procedure, NDU).

Prüfen Sie die Anforderungen

Stellen Sie vor dem Austausch des Switches Folgendes sicher:

- In dem vorhandenen Cluster und der Netzwerkinfrastruktur:
 - Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
 - Alle Cluster-Ports sind **up**.
 - Alle logischen Cluster-Schnittstellen (LIFs) sind **up** und auf ihren Home-Ports.
 - Das ONTAP `cluster ping-cluster -node node1` Der Befehl muss angeben, dass grundlegende und größere Verbindungen als die PMTU-Kommunikation auf allen Pfaden erfolgreich sind.
- Auf dem Nexus 9336C-FX2-Ersatzschalter:
 - Das Management-Netzwerk-Konnektivität auf dem Ersatz-Switch ist funktionsfähig.
 - Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
 - Die Node-Verbindungen sind 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 den NX-OS-Bildschalter werden auf den Switch geladen.
 - Die Erstanpassung des Schalters ist abgeschlossen, wie in beschrieben "[Konfigurieren Sie den Cluster-Switch 9336C-FX2](#)".

Alle zuvor erstellten Site-Anpassungen wie STP, SNMP und SSH werden auf den neuen Switch kopiert.
- Sie haben den Befehl zum Migrieren einer Cluster-LIF von dem Node ausgeführt, auf dem die Cluster-LIF gehostet wird.

Tauschen Sie den Schalter aus

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der vorhandenen Nexus 9336C-FX2 Switches lauten cs1 und cs2.
- Der Name des neuen Nexus 9336C-FX2 Switch lautet newc2.
- Die Node-Namen sind node1 und node2.

- Die Cluster-Ports auf jedem Node lauten e0a und e0b.
- Die Cluster-LIF-Namen sind node1_clug1 und node1_clus2 für node1, und node2_clus1 und node2_clus2 für node2.
- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet cluster1:*>

Über diese Aufgabe

Die folgende Vorgehensweise 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 (FD0220329V5)	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 in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Installieren Sie das entsprechende RCF und Image auf dem Switch, newcs2, und nehmen Sie die erforderlichen Standortvorbereitungen vor.

Überprüfen, 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 für die RCF- und NX-OS-Software benötigen, fahren Sie mit Schritt 2 fort.

- a. Wechseln Sie auf der NetApp Support Site zur Referenzkonfigurationsdatei *Seite* der Referenzkonfiguration für NetApp Cluster und Management-Netzwerk-Switches.
 - b. Klicken Sie auf den Link für die Kompatibilitätsmatrix *Cluster Network and Management Network*, und notieren Sie anschließend die erforderliche Switch-Softwareversion.
 - c. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Seite Beschreibung zurückzukehren, klicken Sie auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung, und gehen Sie dann zur Download-Seite.
 - d. Befolgen Sie die Schritte auf der Download-Seite, um die korrekten RCF- und NX-OS-Dateien für die Version der installierten ONTAP-Software herunterzuladen.
3. Bei dem neuen Switch melden Sie sich als Administrator an und fahren Sie alle Ports ab, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports 1/1 zu 1/34).

Wenn der Schalter, den Sie ersetzen, nicht funktionsfähig ist und ausgeschaltet ist, fahren Sie mit Schritt 4 fort. Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt 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. Vergewissern Sie sich, dass für alle Cluster-LIFs die automatische Zurücksetzung aktiviert ist:

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

Beispiel anzeigen

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

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

```
4 entries were displayed.
```

5. Vergewissern Sie sich, dass alle Cluster-LIFs kommunizieren können:

```
cluster ping-cluster
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster node1

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: Kabel und Ports konfigurieren

1. Fahren Sie die ISL-Ports 1/35 und 1/36 auf dem Nexus 9336C-FX2 Switch cs1 herunter.

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 verbinden Sie sie dann mit den gleichen Ports am Nexus C9336C-FX2 newc2 Switch.

3. Bringen Sie die ISLs-Ports 1/35 und 1/36 zwischen den switches cs1 und newcs2 auf, und überprüfen Sie dann den Betriebsstatus des Port-Kanals.

Port-Channel sollte PO1(SU) angeben und Mitgliedsports sollten eth1/35(P) und eth1/36(P) angeben.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/35 und 1/36 und zeigt die Zusammenfassung des Port-Kanals am 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. Vergewissern Sie sich, dass Port e0b auf allen Nodes aktiviert ist:

```
network port show ipspace Cluster
```

Beispiel anzeigen

Die Ausgabe sollte wie folgt aussehen:

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

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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. Setzen Sie auf demselben Node, den Sie im vorherigen Schritt verwendet haben, die Cluster-LIF, die dem Port im vorherigen Schritt zugeordnet ist, mithilfe des Befehls „Netzwerkschnittstelle revert“ zurück.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert für „Home“ wahr ist und der Port e0b ist.

Die folgenden Befehle geben LIF zurück node1_clus2 Ein node1 Zu Home Port e0a Und zeigt Informationen zu den LIFs auf beiden Nodes an. Das Einrichten des ersten Node ist erfolgreich, wenn die Spalte IS Home für beide Clusterschnittstellen wahr ist und in diesem Beispiel die korrekten Port-Zuweisungen angezeigt werden e0a Und e0b Auf Knoten 1.

```
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. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

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

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

7. Vergewissern Sie sich, dass alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```


Beispiel anzeigen

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

Node node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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. Vergewissern Sie sich, dass alle Cluster-LIFs kommunizieren können:

```
cluster ping-cluster
```

Beispiel anzeigen

```
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 169.254.47.194 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)
```

9. Bestätigen Sie die folgende Clusternetzwerkconfiguration:

```
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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C
cs1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C

Total entries displayed: 4

Schritt 3: Überprüfen Sie die Konfiguration

1. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password Und system switch ethernet log  
enable-collection
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

2. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

system cluster-switch log setup-password **Und** system cluster-switch log enable-collection

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

3. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine

AutoSupport Meldung aufrufen:

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

Ersetzen Sie Cisco Nexus 9336C-FX2 Cluster-Switches durch Switch-lose Verbindungen

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

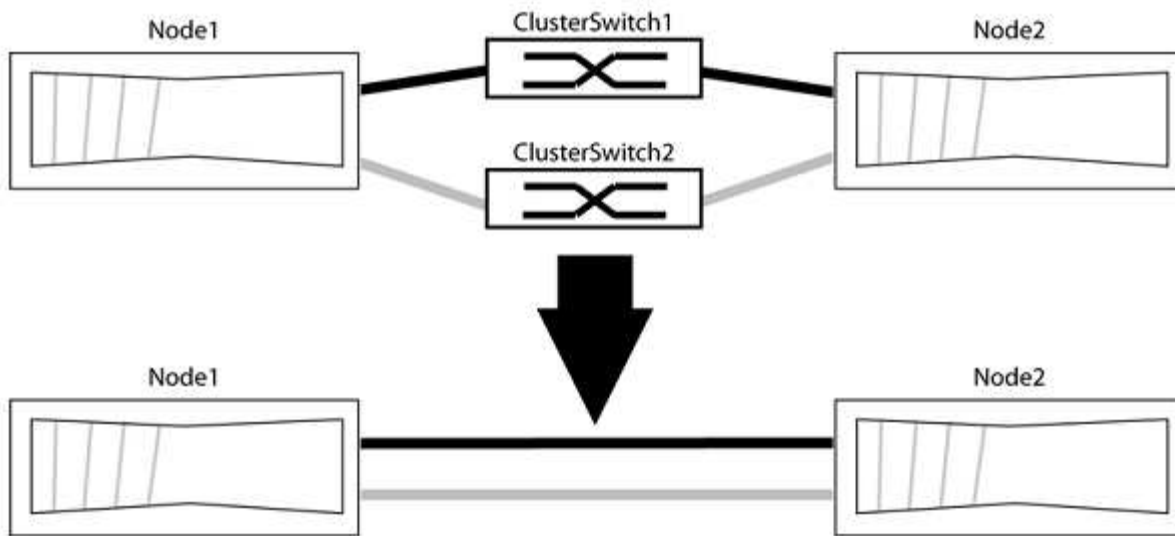
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Anzeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message  
MAINT=<number_of_hours>h
```

Wo h Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

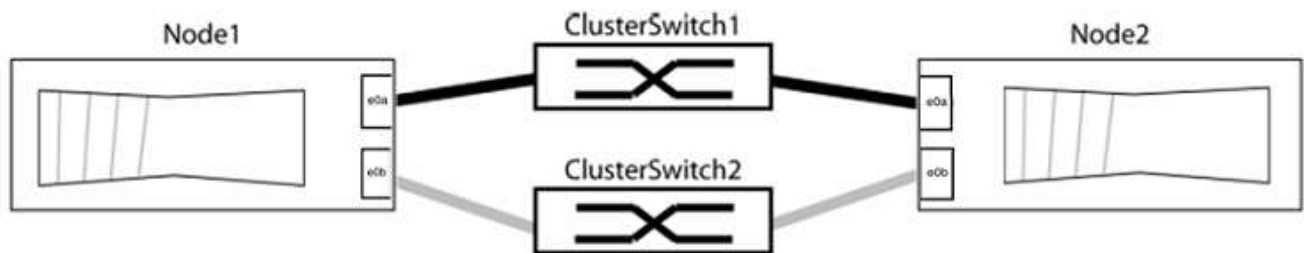
```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Schritt: Ports und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in grop1 zu Cluster-Switch 1 wechseln und die Cluster-Ports in grop2 zu Cluster-Switch 2 wechseln. Diese Gruppen sind später im Verfahren erforderlich.
2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



Überprüfen Sie, ob die Ports einen Wert von `up` Für die Spalte „Link“ und einen Wert von `healthy` Für die Spalte „Integritätsstatus“.

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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

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

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

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

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

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

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

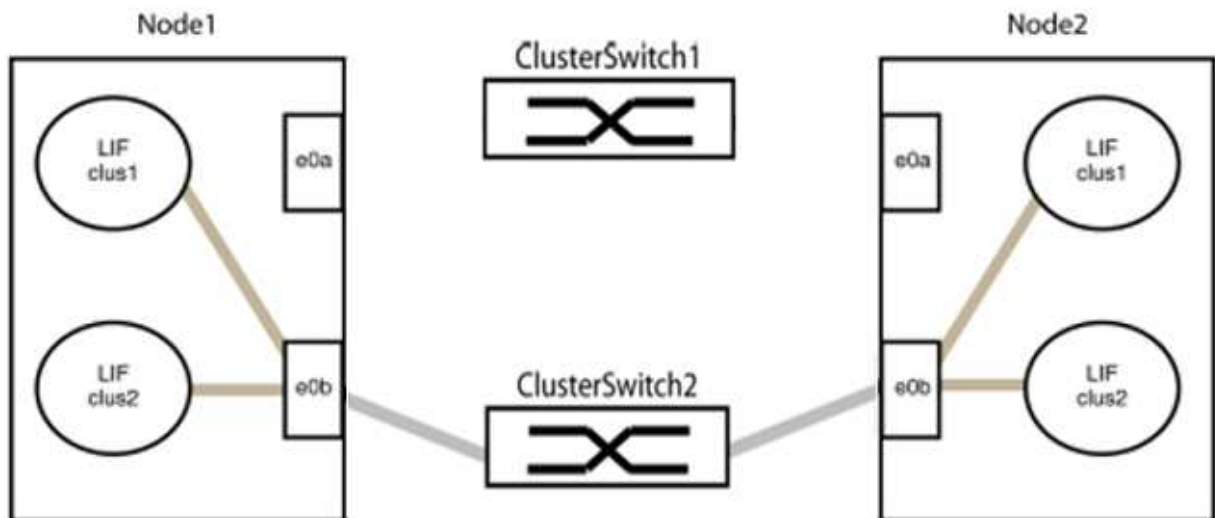
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

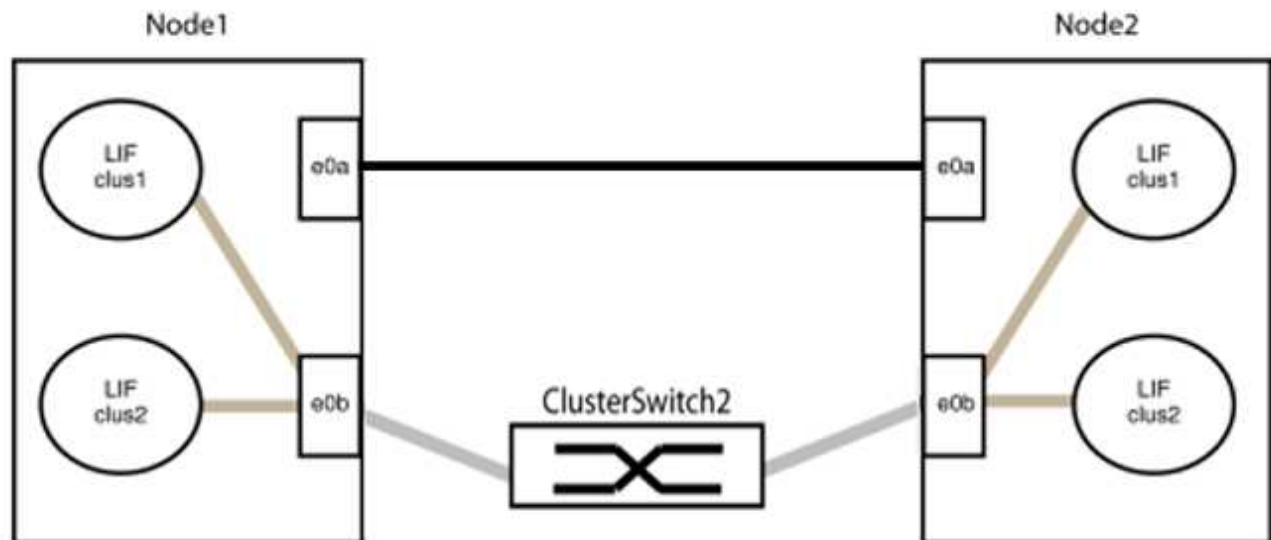
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

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

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

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

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:

```
cluster ping-cluster -node local
```



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

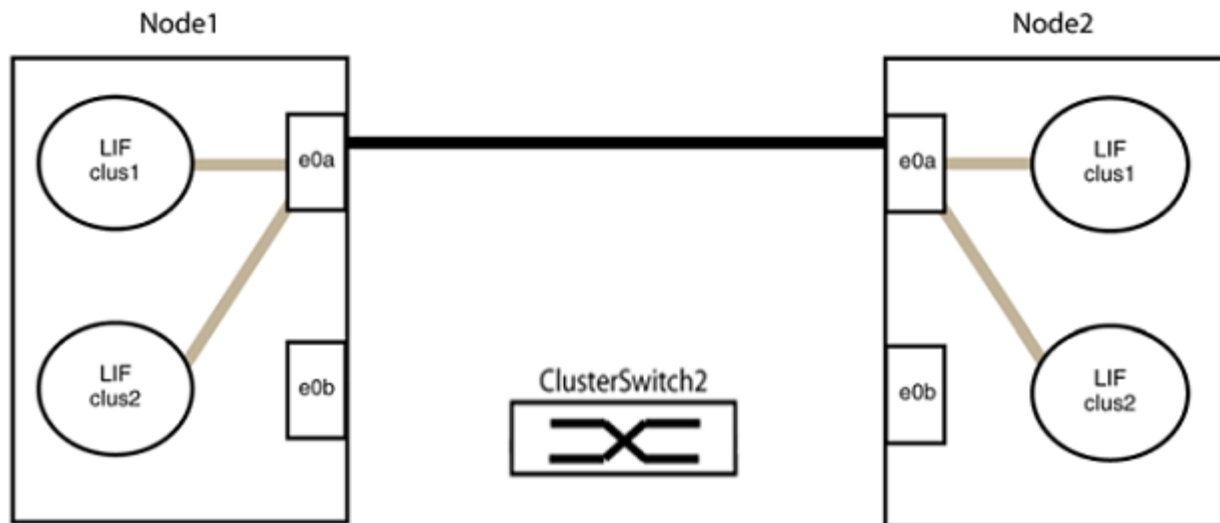
11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

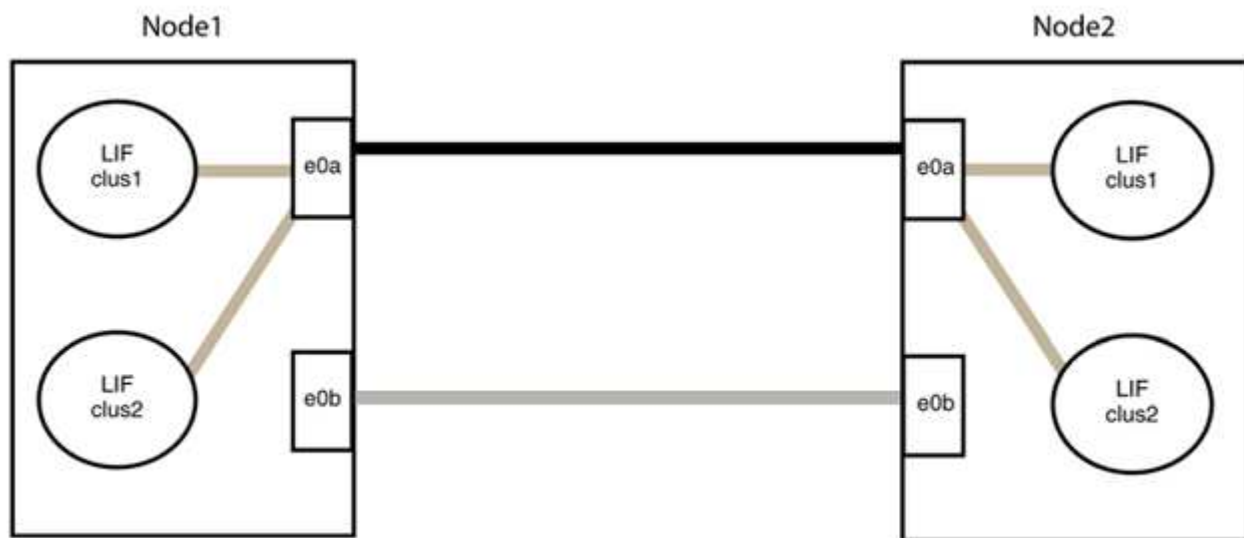
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

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

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

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


Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

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

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

NVIDIA SN2100

Überblick

Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches

Die NVIDIA SN2100 ist ein Cluster-Switch, mit dem Sie ONTAP Cluster mit mehr als zwei Knoten erstellen können.

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen NVIDIA SN2100-Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Installieren Sie die Hardware für den NVIDIA SN2100 Switch"](#).

Anweisungen hierzu finden Sie im *NVIDIA Switch Installation Guide*.

2. ["Konfigurieren Sie den Switch"](#).

Anweisungen sind in der NVIDIA-Dokumentation verfügbar.

3. ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#).

Prüfen Sie die Anforderungen für optische Verbindungen, den QSA-Adapter und die Switch-Port-Geschwindigkeit.

4. ["Verbinden Sie die NS224-Shelfs als Switch-Attached Storage"](#).

Befolgen Sie die Verkabelungsverfahren, wenn Sie über ein System verfügen, in dem die NS224-Laufwerk-Shelfs als Switch-Attached Storage (kein Direct-Attached Storage) verkabelt werden müssen.

5. ["Installieren Sie Cumulus Linux im Cumulus-Modus"](#) Oder ["Installieren Sie Cumulus Linux im ONIE-Modus"](#).

Sie können Cumulus Linux (CL) OS installieren, wenn der Switch Cumulus Linux oder ONIE ausführt.

6. ["Installieren Sie das RCF-Skript \(Reference Configuration File\)"](#).

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Das Verfahren für jedes ist gleich.

7. ["Konfigurieren Sie SNMPv3 für die Switch-Protokollerfassung"](#).

Diese Version umfasst Unterstützung für SNMPv3 für die Erfassung von Switch-Protokollen und für Switch Health Monitoring (SHM).

Die Verfahren verwenden Network Command Line Utility (NCLU), eine Befehlszeilenoberfläche, die sicherstellt, dass Cumulus Linux für alle zugänglich ist. Der NET-Befehl ist das Wrapper-Dienstprogramm, mit dem Sie Aktionen von einem Terminal aus ausführen.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)
- ["Hardware Universe"](#) Für alle unterstützten ONTAP-Versionen.

Konfigurationsanforderungen für NVIDIA SN2100 Switches

Prüfen Sie bei der Installation und Wartung von NVIDIA SN2100-Switches alle Konfigurationsanforderungen.

Installationsvoraussetzungen

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Cluster-Netzwerk-Switches erforderlich. Sie können zusätzliche, optionale Management Switches verwenden.

Sie installieren den NVIDIA SN2100-Switch (X190006) in einem NVIDIA Dual/Single-Switch-Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Hinweise zur Verkabelung finden Sie unter ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#).

ONTAP und Linux Unterstützung

Der NVIDIA SN2100-Switch ist ein 10/25/40/100-GbE-Switch mit Cumulus Linux. Der Switch unterstützt Folgendes:

- ONTAP 9.10.1P3.

Der SN2100 Switch dient Cluster- und Speicheranwendungen in ONTAP 9.10.1P3 über verschiedene Switch-Paare.

- Cumulus Linux (CL) OS-Version.

Um die SN2100 Cumulus Software von NVIDIA herunterzuladen, müssen Sie über Anmeldedaten verfügen, um auf das Enterprise Support Portal von NVIDIA zugreifen zu können. Weitere Informationen finden Sie im Knowledge Base-Artikel ["Registrierung bei NVIDIA für Enterprise Support Portal Access"](#). Aktuelle Informationen zur Kompatibilität finden Sie im ["NVIDIA Ethernet-Switches"](#) Informationsseite.

- Sie können Cumulus Linux installieren, wenn auf dem Switch Cumulus Linux oder ONIE ausgeführt wird.

Komponenten und Teilenummern für NVIDIA SN2100-Switches

Lesen Sie bei der Installation und Wartung von NVIDIA SN2100-Switches die Liste der Komponenten und Teilenummern für Schrank und Schienensatz.

Rack-Details

Sie installieren den NVIDIA SN2100-Switch (X190006) in einem NVIDIA Dual/Single-Switch-Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Einzelheiten zum Schienensatz

In der folgenden Tabelle sind die Teilenummer und Beschreibung der SN2100-Switches und Schienen-Kits aufgeführt:

Teilenummer	Beschreibung
X190006-PE	Cluster-Switch, NVIDIA SN2100, 16 PT 100 GbE, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16 PT 100 GbE, PSIN
X-MTEF-KIT-D	Rail Kit, NVIDIA Dual Switch Seite an Seite
X-MTEF-KIT-E	Rail Kit, NVIDIA Single Switch, kurze Tiefe



Weitere Informationen finden Sie in der NVIDIA-Dokumentation auf ["Installieren Sie den SN2100-Switch und den Schienen-Kit"](#).

Dokumentationsanforderungen für NVIDIA SN2100-Switches

Überprüfen Sie bei Installation und Wartung von NVIDIA SN2100-Switches alle empfohlenen Dokumente.

Titel	Beschreibung
"NVIDIA Switch Installation Guide"	Beschreibt die Installation Ihrer NVIDIA SN2100-Switches.
"Shelf-Verkabelung bei NS224 NVMe-Laufwerken"	Überblick und Abbildungen zeigen die Konfiguration der Verkabelung für Laufwerk-Shelfs.
"NetApp Hardware Universe"	Ermöglicht die Bestätigung der unterstützten Hardware wie Storage-Switches und -Kabel für Ihr Plattformmodell.

Hardware installieren

Installieren Sie die Hardware für den NVIDIA SN2100 Switch

Informationen zur Installation der SN2100-Hardware finden Sie in der NVIDIA-Dokumentation.

Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen unter ["NVIDIA Switch Installation Guide"](#).

Was kommt als Nächstes?

["Konfigurieren Sie den Switch"](#).

Konfigurieren Sie den NVIDIA SN2100-Switch

Informationen zur Konfiguration des SN2100-Switch finden Sie in der NVIDIA-Dokumentation.

Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen unter ["NVIDIA System Bring-up:"](#).

Was kommt als Nächstes?

["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#).

Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Lesen Sie vor der Konfiguration des NVIDIA SN2100-Switches die folgenden Punkte.

Details zum NVIDIA-Port

Switch-Ports	Verwendung von Ports
Swp1s0-3	4 x 10 GbE Breakout-Cluster-Port-Nodes
Swp2s0-3	4 x 25-GbE-Breakout-Cluster-Port-Nodes
Swp3-14	40/100-GbE-Cluster-Port-Nodes
Swp15-16	40/100-GbE-Inter-Switch Link (ISL)-Ports

Siehe ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

Verbindungsverzögerungen mit optischen Verbindungen

Wenn Sie Verbindungsverzögerungen von mehr als fünf Sekunden haben, bietet Cumulus Linux 5.4 und höher Unterstützung für eine schnelle Verbindungsaufnahme. Sie können die Verknüpfungen mit 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

Die folgenden Konfigurationsänderungen sind erforderlich, um dieses Problem zu beheben.

Cumulus Linux 4.4.3

1. Benennen Sie die einzelnen Schnittstellen, die 40-GbE-/100-GbE-Kupferkabel verwenden, wie folgt:

```
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 beiden Zeilen zum hinzu `/etc/cumulus/switchd.conf` Datei für jeden Port (swpp <n>), der 40 GbE/100 GbE 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 den neu switchd Dienst:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Vergewissern Sie sich, dass die Ports hochgefahren 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. Benennen Sie die einzelnen Schnittstellen, die 40-GbE-/100-GbE-Kupferkabel verwenden, wie folgt:

```
cumulus@cumulus:mgmt:~$ nv 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. Konfigurieren Sie die Verknüpfungen mit `nv set` Befehl wie folgt:

- ° `nv set interface <interface-id> link fast-linkup on`
- ° `nv config apply`
- ° Laden Sie den neu 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 hochgefahren 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 "[Diesen KB](#)" Entnehmen.

Auf Cumulus Linux 4.4.2 werden Kupferverbindungen nicht auf SN2100-Switches mit X1151A NIC, X1146A NIC oder integrierten 100-GbE-Ports unterstützt. Beispiel:

- AFF A800 auf den Ports e0a und e0b
- AFF A320 an den Ports e0g und e0h

QSA-Adapter

Wenn ein QSA-Adapter für die Verbindung mit den 10 GbE/25 GbE-Cluster-Ports auf einer Plattform verwendet wird, wird die Verbindung möglicherweise nicht hergestellt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Stellen Sie bei 10GbE die Verbindungsgeschwindigkeit swp1s0-3 manuell auf 10000 und stellen Sie die automatische Aushandlung auf aus.
- Stellen Sie für 25 GbE die Verbindungsgeschwindigkeit swp2s0-3 manuell auf 25000 ein, und stellen Sie die automatische Aushandlung auf aus.



Wenn Sie 10-GbE-QSA-Adapter verwenden, fügen Sie sie in Breakout-GbE-/100-GbE-Ports (swp3-swp14) ein. Setzen Sie den QSA-Adapter nicht in einen Port ein, der für einen Breakout konfiguriert ist.

Einstellen der Schnittstellengeschwindigkeit an Breakout-Ports

Je nach Transceiver im Switch-Port müssen Sie die Geschwindigkeit an der Switch-Schnittstelle möglicherweise auf eine feste Geschwindigkeit einstellen. Bei Verwendung von 10-GbE- und 25-GbE-Breakout-Ports überprüfen Sie, ob die automatische Aushandlung deaktiviert ist, und legen Sie die Schnittstellengeschwindigkeit auf dem Switch fest.

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 die Schnittstelle und den Port-Status, um zu überprüfen, ob die Einstellungen angewendet werden:

```
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
duplex	full	full
speed	10G	10G
fec	auto	auto
mtu	9216	9216
[breakout]		
state	up	up

Überprüfen Sie die Schnittstelle und den Port-Status, um zu überprüfen, ob die Einstellungen angewendet werden:

```
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)						
.						
.						

Was kommt als Nächstes?

"Verkabelung der NS224 Shelves als Switch-Attached Storage".

Verbinden Sie die NS224-Shelves als Switch-Attached Storage

Wenn Sie über ein System verfügen, bei dem die NS224 Laufwerk-Shelves als Switch-Attached Storage verkabelt werden müssen (kein Direct-Attached Storage), verwenden Sie die hier bereitgestellten Informationen.

- Kabel-NS224-Laufwerk-Shelfs über Storage-Switches:

["Verkabelung, Switch-Attached NS224 Laufwerk-Shelfs"](#)

- Bestätigen Sie die unterstützte Hardware, z. B. die Storage-Switches und Kabel, für Ihr Plattformmodell:

["NetApp Hardware Universe"](#)

Was kommt als Nächstes?

["Installieren Sie Cumulus Linux im Cumulus-Modus"](#) Oder ["Installieren Sie Cumulus Linux im ONIE-Modus"](#).

Software konfigurieren

Workflow für die Softwareinstallation von NVIDIA SN2100-Switches

Gehen Sie wie folgt vor, um die Software für einen NVIDIA SN2100-Switch zu installieren und zu konfigurieren:

1. ["Installieren Sie Cumulus Linux im Cumulus-Modus"](#) Oder ["Installieren Sie Cumulus Linux im ONIE-Modus"](#).

Sie können Cumulus Linux (CL) OS installieren, wenn der Switch Cumulus Linux oder ONIE ausführt.

2. ["Installieren Sie das RCF-Skript \(Reference Configuration File\)"](#).

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Das Verfahren für jedes ist gleich.

3. ["Konfigurieren Sie SNMPv3 für die Switch-Protokollerfassung"](#).

Diese Version umfasst Unterstützung für SNMPv3 für die Erfassung von Switch-Protokollen und für Switch Health Monitoring (SHM).

Die Verfahren verwenden Network Command Line Utility (NCLU), eine Befehlszeilenoberfläche, die sicherstellt, dass Cumulus Linux für alle zugänglich ist. Der NET-Befehl ist das Wrapper-Dienstprogramm, mit dem Sie Aktionen von einem Terminal aus ausführen.

Installieren Sie Cumulus Linux im Cumulus-Modus

Gehen Sie folgendermaßen vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im Cumulus-Modus läuft.



Cumulus Linux (CL) kann entweder installiert werden, wenn der Switch Cumulus Linux oder ONIE ausführt (siehe ["Im ONIE-Modus installieren"](#)).

Was Sie benötigen

- Linux-Wissen auf mittlerer Ebene.
- Vertrautheit mit grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren sind vorinstalliert, einschließlich `vi` und `nano`.
- Zugriff auf eine Linux oder UNIX Shell. Wenn Sie Windows verwenden, verwenden Sie eine Linux-Umgebung als Kommandozeilen-Tool für die Interaktion mit Cumulus Linux.

- Die Baud-Rate-Anforderung ist auf 115200 am seriellen Konsolen-Switch für den Zugriff auf die NVIDIA SN2100-Switch-Konsole eingestellt, wie folgt:
 - 115200 Baud
 - 8 Datenbits
 - 1 Stoppbit
 - Parität: Keine
 - Flusskontrolle: Keine

Über diese Aufgabe

Beachten Sie Folgendes:



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.



Das Standardpasswort für das Cumulus-Benutzerkonto lautet **Cumulus**. Wenn Sie sich das erste Mal bei Cumulus Linux anmelden, müssen Sie dieses Standardpasswort ändern. Aktualisieren Sie alle Automatisierungsskripts, bevor Sie ein neues Image installieren. Cumulus Linux bietet Befehlszeilenoptionen zum automatischen Ändern des Standardpassworts während des Installationsvorgangs.

Beispiel 1. Schritte

Cumulus Linux 4.4.3

1. Melden Sie sich beim Switch an.

Wenn Sie sich zum ersten Mal am Switch anmelden, benötigen Sie den Benutzernamen/das Passwort von **cumulus/cumulus** mit `sudo` Berechtigungen.

```
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. Prüfen 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 Standard-Gateway. Der neue Hostname wird erst nach dem Neustart der Konsole/SSH-Sitzung wirksam.



Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0`. Diese Schnittstelle wurde speziell für den Out-of-Band-Management-Einsatz entwickelt. Standardmäßig verwendet die Managementoberfläche DHCPv4 für Adressierung.



Verwenden Sie keine Unterstriche (_), Apostroph (') oder nicht-ASCII-Zeichen im Hostnamen.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
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 beide `/etc/hostname` Und `/etc/hosts` Dateien:

4. Vergewissern Sie sich, dass der Hostname, die IP-Adresse, die Subnetzmaske und das Standard-Gateway 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. Konfigurieren Sie die Zeitzone mithilfe des interaktiven NTP-Modus.

- a. Führen Sie auf einem Terminal den folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- b. Folgen Sie den Menüoptionen auf dem Bildschirm, um den geografischen Bereich und die Region auszuwählen.
- c. Um die Zeitzone für alle Dienste und Dämonen einzustellen, starten Sie den Switch neu.
- d. Überprüfen Sie, ob das Datum und die Uhrzeit auf dem Switch korrekt sind, und aktualisieren Sie

ggf..

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 bei Aufforderung * y* ein.

7. Starten Sie den NVIDIA SN2100-Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation wird automatisch gestartet, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Wählen Sie bitte * nicht* aus.

- Cumulus-Linux GNU/Linux
- ONIE: Installieren des Betriebssystems
- CUMULUS EINBAUEN
- 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 lautet: `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 dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

```
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.x

1. Melden Sie sich beim Switch an.

Wenn Sie sich zum ersten Mal am Switch anmelden, benötigen Sie den Benutzernamen/das

Passwort von **cumulus/cumulus** mit **sudo** Berechtigungen.

```
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. Prüfen 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 Standard-Gateway. Der neue Hostname wird erst nach dem Neustart der Konsole/SSH-Sitzung wirksam.



Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0`. Diese Schnittstelle wurde speziell für den Out-of-Band-Management-Einsatz entwickelt. Standardmäßig verwendet die Managementoberfläche DHCPv4 für Adressierung.



Verwenden Sie keine Unterstriche (`_`), Apostroph (`'`) oder nicht-ASCII-Zeichen im Hostnamen.

```
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 beide `/etc/hostname` Und `/etc/hosts` Dateien:

4. Vergewissern Sie sich, dass der Hostname, die IP-Adresse, die Subnetzmaske und das Standard-Gateway 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. Konfigurieren Sie die Zeitzone mithilfe des interaktiven NTP-Modus.

- a. Führen Sie auf einem Terminal den folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- b. Folgen Sie den Menüoptionen auf dem Bildschirm, um den geografischen Bereich und die Region auszuwählen.
- c. Um die Zeitzone für alle Dienste und Dämonen einzustellen, starten Sie den Switch neu.
- d. Überprüfen Sie, ob das Datum und die Uhrzeit auf dem Switch korrekt sind, und aktualisieren Sie ggf..

6. Installieren Sie Cumulus Linux 5.4:

```
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 bei Aufforderung * y* ein.

7. Starten Sie den NVIDIA SN2100-Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation wird automatisch gestartet, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Wählen Sie bitte * nicht* aus.

- Cumulus-Linux GNU/Linux

- ONIE: Installieren des Betriebssystems
- CUMULUS EINBAUEN
- 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 lautet: `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. Stellen Sie sicher, dass die Nodes jeweils über eine Verbindung zu jedem Switch verfügen:

```
cumulus@sw1:mgmt:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost
Eth110/1/29			
swp2s1	25G	Trunk/L2	node1
e0a			
swp15	100G	BondMember	sw2
swp16	100G	BondMember	sw2

12. Erstellen Sie einen neuen Benutzer, und fügen Sie diesen Benutzer dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

```
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 zusätzliche Benutzergruppen hinzu, auf die der Admin-Benutzer zugreifen kann `nv` Befehl:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user 'admin' to group 'nvshow' ...
Adding user admin to group nvshow
Done.
```

Siehe "[NVIDIA Benutzerkonten](#)" Finden Sie weitere Informationen.

Was kommt als Nächstes?

"[Installieren Sie das RCF-Skript \(Reference Configuration File\)](#)".

Installieren Sie Cumulus Linux im ONIE-Modus

Gehen Sie folgendermaßen vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im ONIE-Modus ausgeführt wird.



Cumulus Linux (CL) kann entweder installiert werden, wenn der Switch ONIE oder Cumulus Linux ausführt (siehe "[Im Cumulus-Modus installieren](#)").

Über diese Aufgabe

Sie können Cumulus Linux unter Verwendung der Open Network Install Environment (ONIE) installieren, die die automatische Erkennung eines Network Installer-Images ermöglicht. Dies erleichtert das Systemmodell der Sicherung von Schaltern mit einem Betriebssystem, wie Cumulus Linux. Die einfachste Möglichkeit, Cumulus Linux mit ONIE zu installieren, ist mit lokaler HTTP-Erkennung.



Wenn Ihr Host IPv6 aktiviert ist, stellen Sie sicher, dass er einen Webserver ausführt. Wenn der Host IPv4 aktiviert ist, stellen Sie sicher, dass er zusätzlich zu einem Webserver DHCP ausführt.

Dieses Verfahren zeigt, wie Cumulus Linux nach dem Start des Administrators in ONIE aktualisiert werden kann.

Beispiel 2. Schritte

Cumulus Linux 4.4.3

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webserver herunter. Diese Datei umbenennen in: `onie-installer`.
2. Verbinden Sie den Host über ein Ethernet-Kabel mit dem Management-Ethernet-Port des Switches.
3. Schalten Sie den Schalter ein.

Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der Installation wird die Cumulus Linux-Anmeldeaufforderung im Terminalfenster angezeigt.



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Schalter neu:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Drücken Sie die Taste **Esc** auf dem GNU GRUB-Bildschirm, um den normalen Bootvorgang zu unterbrechen, wählen Sie **ONIE** und drücken Sie **Enter**.
6. Wählen Sie auf dem nächsten Bildschirm **ONIE: Install OS** aus.
7. Der Vorgang zur Erkennung des ONIE-Installers führt die Suche nach der automatischen Installation durch. Drücken Sie **Enter**, um den Vorgang vorübergehend zu beenden.
8. Wenn der Erkennungsvorgang angehalten wurde:

```
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 Standard-Gateway 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-Adressschema manuell definiert ist, 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. Cumulus Linux Installieren:

```
# 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. Melden Sie sich nach Abschluss der Installation beim 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 Webserver herunter. Diese Datei umbenennen in: `onie-installer`.
2. Verbinden Sie den Host über ein Ethernet-Kabel mit dem Management-Ethernet-Port des Switches.
3. Schalten Sie den Schalter ein.

Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der Installation wird die Cumulus Linux-Anmeldeaufforderung im Terminalfenster angezeigt.



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Schalter 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 die Esc-Taste auf dem GNU GRUB-Bildschirm, um den normalen Bootvorgang zu unterbrechen, wählen Sie ONIE aus, und drücken Sie die Eingabetaste.

```

.
.
Loading ONIE ...

GNU GRUB version 2.02
+-----+
-----+
| ONIE: Install OS
|
| ONIE: Rescue
|
| ONIE: Uninstall OS
|
| ONIE: Update ONIE
|
| ONIE: Embed ONIE
|
|
|
|
|
|
|
|
|
|
|
|
+-----+
-----+

```

Wählen Sie ONIE: **OS installieren**.

6. Der Vorgang zur Erkennung des ONIE-Installers führt die Suche nach der automatischen Installation durch. Drücken Sie **Enter**, um den Vorgang vorübergehend zu beenden.
7. Wenn der Erkennungsvorgang angehalten wurde:

```

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 Standard-Gateway:

```
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. Melden Sie sich nach Abschluss der Installation beim 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 dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

```
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 zusätzliche Benutzergruppen hinzu, auf die der Admin-Benutzer zugreifen kann `nv` Befehl:


```
cumulus@cumulus:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Siehe ["NVIDIA Benutzerkonten"](#) Finden Sie weitere Informationen.

Was kommt als Nächstes?

["Installieren Sie das RCF-Skript \(Reference Configuration File\)"](#).

Installieren Sie das RCF-Skript (Reference Configuration File)

Gehen Sie folgendermaßen vor, um das RCF-Skript zu installieren.

Was Sie benötigen

Stellen Sie vor der Installation des RCF-Skripts sicher, dass auf dem Switch folgende Funktionen verfügbar sind:

- Cumulus Linux ist installiert. Siehe ["Hardware Universe"](#) Für unterstützte Versionen.
- IP-Adresse, Subnetzmaske und Standard-Gateway über DHCP oder manuell konfiguriert definiert.



Sie müssen im RCF (zusätzlich zum Admin-Benutzer) einen Benutzer angeben, der speziell für die Protokollerfassung verwendet werden soll.

Aktuelle RCF-Skriptversionen

Für Cluster- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Laden Sie RCFs von [hier](#) herunter. Das Verfahren für jedes ist gleich.

- Cluster: **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**
- Speicher: **MSN2100-RCF-v1.x-Speicher**

Zu den Beispielen

Das folgende Beispiel zeigt, wie das RCF-Skript für Cluster-Switches heruntergeladen und angewendet wird.

Die Befehlsausgabe des Switch-Management verwendet die Switch-Management-IP-Adresse 10.233.204.71, die Netmask 255.255.254.0 und das Standard-Gateway 10.233.204.1.

Beispiel 3. Schritte

Cumulus Linux 4.4.3

1. Zeigen Sie die verfügbaren Schnittstellen am SN2100-Schalter an:

```
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. Kopieren Sie das RCF-Python-Skript auf den Switch.

```
admin@sw1:mgmt:~$ pwd
/home/cumulus
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 in dem Beispiel verwendet, können Sie Ihre bevorzugte Methode der Dateiübertragung verwenden.

3. Wenden Sie das Skript RCF Python an **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```
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 durch.



In Schritt 3 **Aktualisierung der MOTD-Datei** oben, der Befehl `cat /etc/motd` Wird ausgeführt. Dadurch können Sie den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner überprüfen.



Für Probleme mit RCF-Python-Skripts, die nicht behoben werden können, wenden Sie sich an "[NetApp Support](#)" Für weitere Unterstützung.

4. 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%

5. 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				

6. Stellen Sie sicher, dass die Nodes jeweils über eine Verbindung zu jedem Switch verfügen:

```
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

7. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß 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 Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den

Switch sw2 an, da LIFs nicht auf e0d homed sind).

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

Node/ Protocol	Local Port	Discovered 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 Model	Type	Address

sw1 MSN2100-CB2RC	cluster-network	10.233.205.90
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 MSN2100-CB2RC	cluster-network	10.233.205.91
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		

Cumulus Linux 5.x

1. Zeigen Sie die verfügbaren Schnittstellen am SN2100-Schalter an:

```

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. Kopieren Sie das RCF-Python-Skript auf den Switch.

```

admin@sw1:mgmt:~$ pwd
/home/cumulus
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 in dem Beispiel verwendet, können Sie Ihre bevorzugte Methode der Dateiübertragung verwenden.

3. Wenden Sie das Skript RCF Python an **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.


```
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 durch.



In Schritt 3 **Aktualisierung der MOTD-Datei** oben, der Befehl `cat /etc/issue` Wird ausgeführt. Dadurch können Sie den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner überprüfen.

Beispiel:

```

admin@sw1:mgmt:~$ cat /etc/issue
*****
*****
*
* 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>
*
*****
*****

```



Für Probleme mit RCF-Python-Skripts, die nicht behoben werden können, wenden Sie sich an "[NetApp Support](#)" Für weitere Unterstützung.

4. 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 RTP-LF01-410G38.rtp.eng.netapp.com Eth105/1/14
eth IP Address: 10.231.80.206/22

```

```

eth0 IP Address: fd20:8b1e:b255:85a0:bace:f6ff:fe31:4a0e/64
+ lo 65536 up loopback IP Address: 127.0.0.1/8
lo IP Address: ::1/128
+ swp1s0 9216 10G up cumulus1 e0b swp
.
.
.
+ swp15 9216 100G up cumulus swp15 swp

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         pcsp,dscp              Trust Setting on the port
for packet classification

```

RoCE PCP/DSCP->SP mapping configurations

```

=====
      pcsp  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 keine Auswirkungen auf die Leistung und können sicher ignoriert werden.

5. 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			

6. Stellen Sie sicher, dass die Nodes jeweils über eine Verbindung zu jedem Switch verfügen:

```
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

7. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß 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 Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch sw2 an, da LIFs nicht auf e0d homed sind).


```

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

```

Was kommt als Nächstes?

"Konfigurieren Sie die Switch-Protokollerfassung".

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Der Benutzer für die Protokollerfassung muss angegeben werden, wenn die Referenzkonfigurationsdatei (RCF) angewendet wird. Standardmäßig ist dieser Benutzer auf „admin“ eingestellt. Wenn Sie einen anderen Benutzer verwenden möchten, müssen Sie dies im Abschnitt `*# SHM-Benutzer*s` des RCF angeben.
- Der Benutzer muss Zugriff auf die Befehle **nv show** haben. Dies kann durch Ausführen hinzugefügt werden `sudo adduser USER nv show` Und BENUTZER durch den Benutzer für die Protokollerfassung ersetzen.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Sammlung gestartet: Die detaillierte Support Protokolle und eine stündliche Erfassung von Periodic Daten:

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um Anweisungen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie das vorherige Verzeichnis der Protokollsammlung und die Datei '.tar' unter /tmp/shm_log Auf dem Schalter.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf NVIDIA SN2100-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
net add snmp-server username SNMPv3_USER auth-none
```
- Für * MD5/SHA-Authentifizierung*:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-PASSWORD
[encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
net show snmp status
```

Beispiel anzeigen

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status                active (running)
Reload Status                 enabled
Listening IP Addresses        all vrf mgmt
Main snmpd PID                4318
Version 1 and 2c Community String Configured
Version 3 Usernames           Not Configured
-----

cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf      2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf 2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
# Auto-generated config file: do not edit. #
agentaddress udp:@mgmt:161
agentxperms 777 777 snmp snmp
agentxsocket /var/agentx/master
createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
ifmib_max_num_ifaces 500
iquerysecname _snmptrapusernameX
master agentx
monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
```

```

rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syssservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

=====

User	Timestamp	Command
-----	-----	-----
-----	-----	-----
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username SNMPv3User auth-md5 <password> encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames     Configured    <---- Configured
here
-----
cumulus@sw1:~$

```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```

security login create -user-or-group-name SNMPv3User -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212

```

Beispiel anzeigen

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)" -instance
```


Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 4.4.3 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums detaillierten Seriennummer identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 4.4.3 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Aktualisieren Sie Cumulus Linux-Versionen

Gehen Sie wie folgt vor, um Ihre Cumulus Linux-Version bei Bedarf zu aktualisieren.

Was Sie benötigen

- Linux-Wissen auf mittlerer Ebene.
- Vertrautheit mit grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren sind vorinstalliert, einschließlich `vi` und `nano`.
- Zugriff auf eine Linux oder UNIX Shell. Wenn Sie Windows verwenden, verwenden Sie eine Linux-Umgebung als Kommandozeilen-Tool für die Interaktion mit Cumulus Linux.
- Die Baud-Rate-Anforderung ist auf 115200 am seriellen Konsolen-Switch für den Zugriff auf die NVIDIA SN2100-Switch-Konsole eingestellt, wie folgt:
 - 115200 Baud
 - 8 Datenbits
 - 1 Stoppbit
 - Parität: Keine

- Flusskontrolle: Keine

Über diese Aufgabe

Beachten Sie Folgendes:



Jedes Mal, wenn Cumulus Linux aktualisiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut. Ihre bestehende Konfiguration wird gelöscht. Sie müssen Ihre Switch-Konfiguration speichern und aufzeichnen, bevor Sie Cumulus Linux aktualisieren.



Das Standardpasswort für das Cumulus-Benutzerkonto lautet **Cumulus**. Wenn Sie sich das erste Mal bei Cumulus Linux anmelden, müssen Sie dieses Standardpasswort ändern. Sie müssen Automatisierungsskripts aktualisieren, bevor Sie ein neues Image installieren. Cumulus Linux bietet Befehlszeilenoptionen zum automatischen Ändern des Standardpassworts während des Installationsvorgangs.

Beispiel 4. Schritte

Von Cumulus Linux 4.4.x auf Cumulus Linux 5.x

1. Überprüfen Sie die aktuelle Version von Cumulus Linux und die angeschlossenen Ports:

```
admin@sw1: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

admin@sw1: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)
.
.
```

2. Laden Sie das Cumulux Linux 5.x-Image herunter:

```
admin@sw1:mgmt:~$ sudo onie-install -a -i
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/cumulus-
linux-5.4.0-mlx-amd64.bin/
[sudo] password for cumulus:
Fetching installer:
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/cumulus-
linux-5.4.0-mlx-amd64.bin
Downloading URL:
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/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.
```

3. Starten Sie den Switch neu:

```
admin@sw1:mgmt:~$ sudo onie-install -a -i
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/cumulus-
linux-5.4.0-mlx-amd64.bin/
sudo reboot
```

4. 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'
```

5. Prüfen 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	

6. 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/syncd/syncd.conf
.
.
```

7. Melden Sie sich ab, und melden Sie sich erneut beim Switch an, um den aktualisierten Switch-Namen an der Eingabeaufforderung anzuzeigen:

```
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:~$
```

8. Legen Sie die IP-Adresse fest:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address 10.231.80.206
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
```

9. Erstellen Sie einen neuen Benutzer, und fügen Sie diesen Benutzer dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

```
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:~$

```

10. Fügen Sie zusätzliche Benutzergruppen hinzu, auf die der Admin-Benutzer zugreifen kann `nv` Befehl:


```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Siehe ["NVIDIA Benutzerkonten"](#) Finden Sie weitere Informationen.

Von Cumulus Linux 5.x auf Cumulus Linux 5.x

1. Überprüfen Sie die aktuelle Version von Cumulus Linux und die angeschlossenen Ports:

```
admin@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	

```
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. Laden Sie das Cumulux Linux 5.4.0-Image herunter:

```
admin@sw1:mgmt:~$ sudo onie-install -a -i
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/cumulus-
linux-5.4.0-mlx-amd64.bin/
[sudo] password for cumulus:
Fetching installer:
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/cumulus-
linux-5.4.0-mlx-amd64.bin
Downloading URL:
http://10.60.132.97/x/eng/testbedN,svl/nic/files/NVIDIA/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.
```

3. Starten Sie den Switch neu:

```
admin@sw1:mgmt:~$ sudo reboot
```

4. 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'
```

5. Prüfen 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
```

6. 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/syncd/syncd.conf
.
.
```

7. Melden Sie sich ab, und melden Sie sich erneut beim Switch an, um den aktualisierten Switch-Namen an der Eingabeaufforderung anzuzeigen:

```
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:~$
```

8. Legen Sie die IP-Adresse fest:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address 10.231.80.206
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
```

9. Erstellen Sie einen neuen Benutzer, und fügen Sie diesen Benutzer dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

```
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:~$

```

10. Fügen Sie zusätzliche Benutzergruppen hinzu, auf die der Admin-Benutzer zugreifen kann `nv` Befehl:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
[sudo] password for cumulus:
Adding user `admin' to group `nvshow' ...
Adding user admin to group nvshow
Done.
```

Siehe ["NVIDIA Benutzerkonten"](#) Finden Sie weitere Informationen.

Was kommt als Nächstes?

["Installieren Sie das RCF-Skript \(Reference Configuration File\)"](#).

Switches migrieren

Migrieren Sie CN1610-Cluster-Switches zu NVIDIA SN2100-Cluster-Switches

Sie können NetApp CN1610 Cluster Switches für ein ONTAP Cluster zu NVIDIA SN2100 Cluster Switches migrieren. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Wenn Sie NetApp CN1610-Cluster-Switches durch NVIDIA SN2100-Cluster-Switches ersetzen, müssen Sie sich über bestimmte Konfigurationsdaten, Port-Verbindungen und Verkabelungsanforderungen im Klaren sein. Siehe ["Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches"](#).

Unterstützte Switches

Folgende Cluster-Switches werden unterstützt:

- NetApp CN1610
- NVIDIA SN2100

Weitere Informationen zu unterstützten Ports und deren Konfigurationen finden Sie im ["Hardware Universe"](#).

Was Sie benötigen

Stellen Sie sicher, dass Sie die folgenden Anforderungen für die Konfiguration erfüllen:

- Der vorhandene 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 werden unter der richtigen Version von Cumulus Linux konfiguriert und betrieben, die mit der angewendeten Referenzkonfigurationsdatei (RCF) installiert ist.
- Die vorhandene Cluster-Netzwerkconfiguration verfügt über folgende Merkmale:
 - Ein redundantes und voll funktionsfähiges NetApp Cluster mit CN1610-Switches.
 - Managementkonnektivität und Konsolenzugriff auf die CN1610-Switches und die neuen Switches.
 - Alle Cluster-LIFs befinden sich im Zustand „up“, wobei die Cluster-LIFs an ihren Home-Ports vorhanden sind.

- ISL-Ports aktiviert und zwischen den CN1610-Switches und zwischen den neuen Switches verkabelt.
- Einige Ports sind auf NVIDIA SN2100-Switches konfiguriert, um mit 40 GbE oder 100 GbE zu laufen.
- Die 40-GbE- und 100-GbE-Konnektivität von Nodes zu NVIDIA SN2100-Cluster-Switches wurde geplant, migriert und dokumentiert.

Migrieren Sie die Switches

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen CN1610 Cluster Switches sind *c1* und *c2*.
- Die neuen NVIDIA SN2100-Cluster-Switches sind *sw1* und *sw2*.
- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node 1 *_clus1_* und *node1_clus2* und *node2_clus1* bzw. *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben das Format `swp[Port]s[Breakout-Port 0-3]`. Beispielsweise sind vier Breakout-Ports auf `swp1 swp1s0, swp1s1, swp1s2 und swp1s3`.

Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Schalter c2 wird zuerst durch Schalter sw2 ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und c2 wird dann von c2 getrennt und wieder mit sw2 verbunden.
- Schalter c1 wird durch Schalter sw1 ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und c1 wird dann von c1 getrennt und wieder mit sw1 verbunden.



Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

3. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

Schritt: Ports und Verkabelung konfigurieren

1. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

Jeder Port sollte für angezeigt werden `Link Und healthy` Für `Health Status`.

- a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show -ipSPACE Cluster
```


Beispiel anzeigen

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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. Zeigt Informationen zu den LIFs und ihren zugewiesenen Home-Nodes an:

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

Jede LIF sollte angezeigt werden up/up Für Status Admin/Oper Und true Für Is Home.

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 Node sind mit vorhandenen Cluster-Switches auf die folgende Weise (aus Sicht der Nodes) verbunden. Verwenden Sie dazu den Befehl:

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

Beispiel anzeigen

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

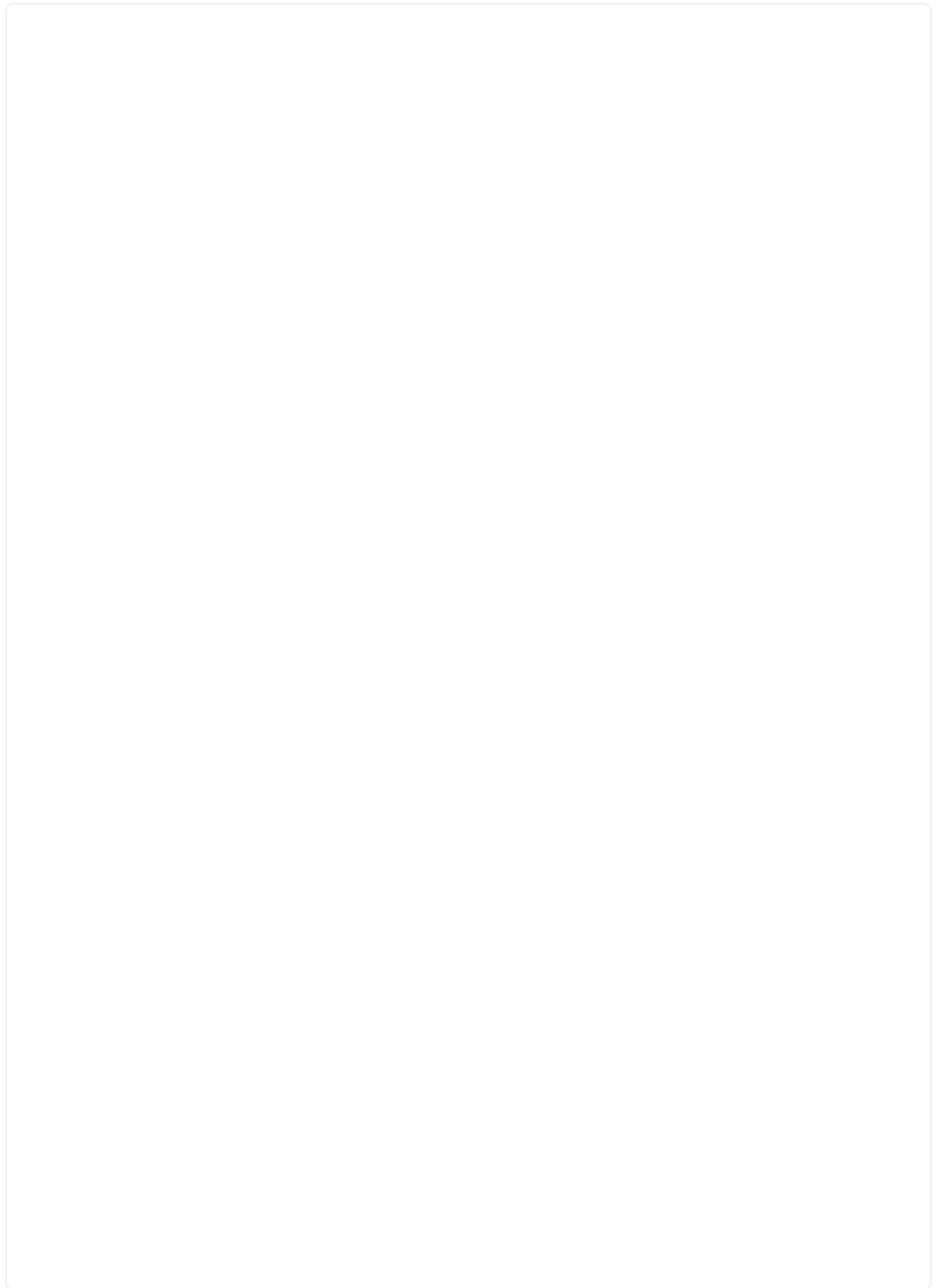
Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				

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 sind (aus Sicht der Switches) folgendermaßen 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	0/1	124	H	AFF-A400
node2 e3a	0/2	124	H	AFF-A400
c2 0/13	0/13	179	S I s	CN1610
c2 0/14	0/14	175	S I s	CN1610
c2 0/15	0/15	179	S I s	CN1610
c2 0/16	0/16	175	S I s	CN1610

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	0/1	124	H	AFF-A400
node2 e3b	0/2	124	H	AFF-A400
c1 0/13	0/13	175	S I s	CN1610
c1 0/14	0/14	175	S I s	CN1610
c1 0/15	0/15	175	S I s	CN1610
c1 0/16	0/16	175	S I s	CN1610

4. Vergewissern Sie sich, dass das Cluster-Netzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node node2

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)
```

5. Fahren Sie auf Switch c2 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster-LIFs durchzuführen.

```
(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)#
```

6. Verschieben Sie die Node-Cluster-Ports vom alten Switch c2 auf den neuen Switch sw2, indem Sie die entsprechende Verkabelung verwenden, die von NVIDIA SN2100 unterstützt wird.

7. Zeigen Sie die Attribute des Netzwerkports an:

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

Beispiel anzeigen

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

Node: node1

Ignore

						Speed (Mbps)	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
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 Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise 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	-

9. Vergewissern Sie sich beim Switch sw2, dass alle Knoten-Cluster-Ports 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)					

10. Fahren Sie auf Switch c1 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster LIFs zu ermöglichen.

```
(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)#
```

11. Verschieben Sie die Knoten-Cluster-Ports vom alten Switch c1 auf den neuen Switch sw1, mit der entsprechenden Verkabelung unterstützt von NVIDIA SN2100.
12. Überprüfen der endgültigen Konfiguration des Clusters:

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

Jeder Port sollte angezeigt werden up Für Link Und healthy Für Health Status.

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						

13. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

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

Beispiel anzeigen

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

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

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	-

14. Vergewissern Sie sich bei den Switches sw1 und sw2, dass alle Knoten-Cluster-Ports 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)					

15. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
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: Führen Sie den Vorgang durch

1. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

2. Vergewissern Sie sich, dass alle Cluster-Netzwerk-LIFs wieder an ihren Home-Ports sind:

```
network interface show
```

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. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

4. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log show  
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	cs1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	cs2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

5. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

6. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Migrieren Sie von einem Cisco Cluster-Switch zu einem NVIDIA SN2100 Cluster-Switch

Sie können Cisco Cluster Switches für ein ONTAP Cluster zu NVIDIA SN2100 Cluster Switches migrieren. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Sie müssen bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen beachten, wenn Sie einige ältere Cisco Cluster Switches durch NVIDIA SN2100 Cluster Switches ersetzen. Siehe ["Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches"](#).

Unterstützte Switches

Folgende Cisco Cluster-Switches werden unterstützt:

- Nexus 9336C-FX2
- Nexus 92300YC
- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Weitere Informationen zu unterstützten Ports und deren Konfigurationen finden Sie im ["Hardware Universe"](#).

Was Sie benötigen

Stellen Sie sicher, dass:

- Das vorhandene 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 funktionieren unter der richtigen Version von Cumulus Linux, die mit der verwendeten Referenzkonfigurationsdatei (RCF) installiert wird.
- Die vorhandene Cluster-Netzwerkkonfiguration verfügt über folgende Merkmale:
 - Ein redundantes und voll funktionsfähiges NetApp Cluster unter Verwendung beider älteren Cisco Switches.
 - Management-Konnektivität und Konsolenzugriff auf die älteren Cisco Switches und die neuen Switches.
 - Alle Cluster-LIFs im Status „up“ mit den Cluster-LIFs befinden sich auf den Home-Ports.
 - ISL-Ports aktiviert und zwischen den älteren Cisco Switches und zwischen den neuen Switches verkabelt.
- Einige der Ports sind auf NVIDIA SN2100-Switches für 40 GbE oder 100 GbE konfiguriert.
- Sie haben 40-GbE- und 100-GbE-Konnektivität von den Nodes zu NVIDIA SN2100 Cluster Switches geplant, migriert und dokumentiert.



Wenn Sie die Portgeschwindigkeit der e0a- und e1a-Cluster-Ports auf AFF A800- oder AFF C800-Systemen ändern, können Sie beobachten, wie fehlerhafte Pakete nach der Geschwindigkeitskonvertierung empfangen werden. Siehe ["Bug 1570339"](#) Und den Knowledge Base Artikel ["CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE"](#) Für eine Anleitung.

Migrieren Sie die Switches

Zu den Beispielen

In diesem Verfahren werden Cisco Nexus 3232C-Cluster-Switches beispielsweise Befehle und Ausgaben verwendet.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen Cisco Nexus 3232C Cluster-Switches sind *c1* und *c2*.
- Die neuen NVIDIA SN2100-Cluster-Switches sind *sw1* und *sw2*.
- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node 1 *clus1_* und *node1_clus2* und *node2_clus1* bzw. *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben das Format `swp[Port]s[Breakout-Port 0-3]`. Beispielsweise sind vier Breakout-Ports auf *swp1 swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Schalter c2 wird zuerst durch Schalter sw2 ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und c2 wird dann von c2 getrennt und wieder mit sw2 verbunden.
- Schalter c1 wird durch Schalter sw1 ersetzt.
 - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
 - Die Verkabelung zwischen den Knoten und c1 wird dann von c1 getrennt und wieder mit sw1 verbunden.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

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

3. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

Schritt: Ports und Verkabelung konfigurieren

1. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

Jeder Port sollte für angezeigt werden `Link` Und gesund für `Health Status`.

- a. Zeigen Sie die Attribute des Netzwerkports an:

```
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
Status	Status			Admin/Oper	
-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

Node: node2

Ignore

					Speed (Mbps)
Health	Health				
Port	IPspace	Broadcast	Domain	Link	MTU
Status	Status			Admin/Oper	
-----	-----	-----	-----	-----	-----
-----	-----				
e3a	Cluster	Cluster		up	9000
healthy	false				auto/100000
e3b	Cluster	Cluster		up	9000
healthy	false				auto/100000

- b. Informationen zu den logischen Schnittstellen und den zugehörigen Home-Nodes anzeigen:

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

Jede LIF sollte angezeigt werden up/up Für Status Admin/Oper Und zwar für Is Home.

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e3a	node1_clus1	up/up	169.254.209.69/16	node1
e3b	node1_clus2	up/up	169.254.49.125/16	node1
e3a	node2_clus1	up/up	169.254.47.194/16	node2
e3b	node2_clus2	up/up	169.254.19.183/16	node2

- Die Cluster-Ports auf jedem Node sind auf folgende Weise (aus Sicht der Nodes) mit vorhandenen Cluster-Switches verbunden:

```
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 (aus Sicht der Switches) wie folgt 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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
c2 Eth1/31	Eth1/31	179	S I s	N3K-C3232C
c2 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
c1 Eth1/31	Eth1/31	175	S I s	N3K-C3232C
c1 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

4. Stellen Sie sicher, dass das Clusternetzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node node2

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)
```

5. Fahren Sie auf Switch c2 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster-LIFs durchzuführen.

```
(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)#
```

6. Verschieben Sie die Node-Cluster-Ports vom alten Switch c2 auf den neuen Switch sw2, indem Sie die entsprechende Verkabelung verwenden, die von NVIDIA SN2100 unterstützt wird.
7. Zeigen Sie die Attribute des Netzwerkports an:

```
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

8. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise 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	-

9. Vergewissern Sie sich beim Switch sw2, dass alle Knoten-Cluster-Ports 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)					

10. Fahren Sie auf Switch c1 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster LIFs zu ermöglichen.

```
(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)#
```

11. Verschieben Sie die Knoten-Cluster-Ports vom alten Switch c1 auf den neuen Switch sw1, mit der entsprechenden Verkabelung unterstützt von NVIDIA SN2100.
12. Überprüfen der endgültigen Konfiguration des Clusters:

```
network port show -ip space Cluster
```

Jeder Port sollte angezeigt werden up Für Link Und gesund für Health Status.

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						

13. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

Beispiel anzeigen

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

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

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	-

14. Vergewissern Sie sich bei den Switches sw1 und sw2, dass alle Knoten-Cluster-Ports 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)					

15. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
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: Führen Sie den Vorgang durch

1. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

2. Vergewissern Sie sich, dass alle Cluster-Netzwerk-LIFs wieder an ihren Home-Ports sind:

```
network interface show
```

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. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

4. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device sw1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device sw2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log show  
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	sw1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	sw2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

5. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

6. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Migrieren Sie mit NVIDIA SN2100-Cluster-Switches zu einem Cluster mit zwei Nodes

Wenn Sie eine bestehende Cluster-Umgebung mit zwei Nodes ohne Switches nutzen, können Sie mit NVIDIA SN2100 Switches zu einer Switch-basierten Cluster-Umgebung mit zwei Nodes migrieren. So können Sie eine Skalierung über zwei Nodes im Cluster hinaus vornehmen.

Die von Ihnen verwendete Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerk-Ports oder einen einzelnen Cluster-Port haben. Der dokumentierte Prozess funktioniert bei allen Knoten über optische oder Twinax-Ports, wird bei diesem Switch jedoch nicht unterstützt, wenn Knoten integrierte 10GBASE-T RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

Prüfen Sie die Anforderungen

Konfiguration mit zwei Nodes ohne Switches

Stellen Sie sicher, dass:

- Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
- Auf den Knoten wird ONTAP 9.10.1P3 und höher ausgeführt.
- Alle Cluster-Ports haben den Status **up**.
- Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren Home-Ports.

Konfiguration des NVIDIA SN2100-Cluster-Switches

Stellen Sie sicher, dass:

- Beide Switches verfügen über Management-Netzwerk-Konnektivität.
- Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
- Bei NVIDIA SN2100, Node-to-Node-Switch und Switch-to-Switch-Verbindungen werden Twinax- oder Glasfaserkabel verwendet.



Siehe "[Prüfen Sie die Verkabelung und Konfigurationsüberlegungen](#)" Bei Einschränkungen und weiteren Details. Der "[Hardware Universe – Switches](#)" Enthält auch weitere Informationen über Verkabelung.

- Inter-Switch Link (ISL)-Kabel werden an die Anschlüsse swp15 und swp16 an beiden NVIDIA SN2100-Switches angeschlossen.
- Die Erstanpassung der beiden SN2100-Switches erfolgt so:
 - SN2100-Switches führen die neueste Version von Cumulus Linux aus
 - Auf die Switches werden Referenzkonfigurationsdateien (RCFs) angewendet
 - Auf den neuen Switches werden alle Site-Anpassungen wie SMTP, SNMP und SSH konfiguriert.

Der "[Hardware Universe](#)" Enthält die neuesten Informationen über die tatsächlichen Cluster-Ports für Ihre Plattformen.

Migrieren Sie die Switches

Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der SN2100-Schalter lauten *sw1* und *sw2*.
- Die Namen der Cluster SVMs sind *node1* und *node2*.
- Die Namen der LIFs sind *_node1_clus1_* und *node1_clus2* auf Knoten 1, und *node2_clus1* und *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben das Format `swp[Port]s[Breakout-Port 0-3]`. Beispielsweise sind vier Breakout-Ports auf *swp1* *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=xh`

Wobei *x* die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben *y* Wenn Sie dazu aufgefordert werden, fortzufahren: `set -privilege advanced`

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

Schritt: Ports und Verkabelung konfigurieren

Cumulus Linux 4.4.x

1. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches sw1 und sw2.

Sie dürfen die ISL-Ports nicht deaktivieren.

Mit den folgenden Befehlen werden die Knotenanschlüsse an den Switches sw1 und sw2 deaktiviert:

```
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. Stellen Sie sicher, dass sich die ISL und die physischen Ports auf der ISL zwischen den beiden SN2100-Switches sw1 und sw2 auf den Ports swp15 und swp16 befinden:

```
net show interface
```

Die folgenden Befehle zeigen, dass die ISL-Ports bei den Switches sw1 und sw2 aktiviert 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 an den Node ausgerichteten Ports (nicht ISL-Ports) auf den neuen Cluster-Switches sw1 und sw2.

Sie dürfen die ISL-Ports nicht deaktivieren.

Mit den folgenden Befehlen werden die Knotenanschlüsse an den Switches sw1 und sw2 deaktiviert:

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
down  
cumulus@sw1:~$ nv config apply  
cumulus@sw1:~$ nv save  
  
cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state  
down  
cumulus@sw2:~$ nv config apply  
cumulus@sw2:~$ nv save
```

2. Stellen Sie sicher, dass sich die ISL und die physischen Ports auf der ISL zwischen den beiden SN2100-Switches sw1 und sw2 auf den Ports swp15 und swp16 befinden:

```
nv show interface
```

Die folgenden Beispiele zeigen, dass die ISL-Ports auf den Switches sw1 und sw2 aktiviert sind:

```
cumulus@sw1:~$ nv show interface
```

Interface	MTU	Speed	State	Remote Host	Remote Port
Type	Summary				

...					
...					
+ swp14	9216		down		
swp					
+ swp15	9216	100G	up	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-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	oss-g-rcf1	Intra-Cluster Switch
ISL Port swp15 swp					
+ swp16	9216	100G	up	oss-g-rcf2	Intra-Cluster Switch
ISL Port swp16 swp					

1. Überprüfen Sie, ob alle Cluster-Ports hochgefahren sind:

```
network port show
```

Jeder Port sollte angezeigt werden up Für Link Und gesund für Health Status.

Beispiel anzeigen

```
cluster1::*> network port show
```

Node: node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

```
network interface show
```

Jede LIF im Cluster sollte für „true“ anzeigen Is Home Und ich habe ein Status Admin/Oper Von up/up.

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. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

```
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 node1, und verbinden sie dann e3a mit Port 3 am Cluster-Switch sw1. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.

Der ["Hardware Universe – Switches"](#) Enthält weitere Informationen zur Verkabelung.

5. Trennen Sie das Kabel vom Cluster-Port e3a auf node2, und verbinden sie dann e3a mit Port 4 am Cluster-Switch sw1. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.

Cumulus Linux 4.4.x

1. bei Switch sw1 aktivieren Sie alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden alle an den Knoten ausgerichteten Ports auf Switch sw1 aktiviert.

```
cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw1:~$ net pending  
cumulus@sw1:~$ net commit
```

2. bei Switch sw1 überprüfen Sie, ob alle Ports aktiviert 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. bei Switch sw1 aktivieren Sie alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden alle an den Knoten ausgerichteten Ports auf Switch sw1 aktiviert.

```
cumulus@sw1:~$ nv unset interface swp1s0-3,swp2s0-3,swp3-14 link
state down
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

2. bei Switch sw1 überprüfen Sie, ob alle Ports aktiviert 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	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

1. Überprüfen Sie, ob alle Cluster-Ports hochgefahren sind:

```
network port show -ip space Cluster
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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 zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

```
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 node1, und verbinden sie e3b mit Port 3 am Cluster-Switch sw2. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.
4. Trennen Sie das Kabel vom Cluster-Port e3b auf node2, und verbinden sie e3b mit Port 4 am Cluster-Switch sw2. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.

Cumulus Linux 4.4.x

1. aktivieren Sie auf Switch sw2 alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden die Node-Ports am Switch sw2 aktiviert:

```
cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw2:~$ net pending  
cumulus@sw2:~$ net commit
```

2. bei Switch sw2 überprüfen Sie, ob alle Ports aktiviert 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)						
...						

- Überprüfen Sie bei beiden Switches sw1 und sw2, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
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 nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden die Node-Ports am Switch sw2 aktiviert:

```
cumulus@sw2:~$ nv unset interface swp1s0-3,swp2s0-3,swp3-14 link  
state down  
cumulus@sw2:~$ nv config apply  
cumulus@sw2:~$ nv config save
```

2. bei Switch sw2 überprüfen Sie, ob alle Ports aktiviert 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	ossq-int-rcf10
swp15					
swp16	up	100G	9216	swp	ossq-int-rcf10
swp16					

3. Überprüfen Sie bei beiden Switches sw1 und sw2, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
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. zeigt Informationen über die erkannten Netzwerkgeräte im Cluster an:

```
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. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

```
network port show -ipSpace Cluster
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

```
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: Führen Sie den Vorgang durch

1. Aktivieren Sie das automatische Zurücksetzen auf allen Cluster-LIFs:

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

Beispiel anzeigen

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

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

2. Vergewissern Sie sich, dass alle Schnittstellen angezeigt werden true Für Is Home:

```
net interface show -vserver Cluster
```



Dies kann eine Minute dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf node1 und node2 liegen und dass Is Home Die Ergebnisse sind wahr:

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

Current Is	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Port
Home	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. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

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

Beispiel anzeigen

Die falsche Ausgabe im folgenden Beispiel zeigt an, dass die Konfigurationseinstellungen deaktiviert sind:

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

4. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

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

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

5. Vergewissern Sie sich, dass das Cluster-Netzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node node1
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)
```

6. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

7. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device sw1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device sw2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log show  
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
1	sw1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	sw2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

8. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

9. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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


Tauschen Sie die Schalter aus

Ersetzen Sie einen NVIDIA SN2100-Cluster-Switch

Gehen Sie folgendermaßen vor, um einen defekten NVIDIA SN2100-Switch in einem Cluster-Netzwerk zu ersetzen. Dies ist ein NDU (Non Disruptive Procedure, NDU).

Prüfen Sie die Anforderungen

Bestehende Cluster- und Netzwerkinfrastruktur

Stellen Sie sicher, dass:

- Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
- Alle Cluster-Ports sind aktiv.
- Alle logischen Cluster-Schnittstellen (LIFs) laufen und auf ihren Home-Ports.
- Das ONTAP `cluster ping-cluster -node node1` Der Befehl gibt an, dass grundlegende und größere Verbindungen als PMTU auf allen Pfaden erfolgreich sind.

NVIDIA SN2100-Ersatzschalter

Stellen Sie sicher, dass:

- Die Konnektivität des Managementnetzwerks am Ersatz-Switch funktioniert.
- Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
- Die Knotenverbindungen sind die Anschlüsse swp1 bis swp14.
- Alle Inter-Switch Link (ISL)-Ports sind an den Ports swp15 und swp16 deaktiviert.
- Die gewünschte Referenzkonfigurationsdatei (RCF) und der Bildschalter des Betriebssystems Cumulus werden auf den Switch geladen.
- Die anfängliche Anpassung des Schalters ist abgeschlossen.

Vergewissern Sie sich außerdem, dass alle Änderungen an früheren Standorten, wie STP, SNMP und SSH, auf den neuen Switch kopiert werden.



Sie müssen den Befehl zum Migrieren einer Cluster-LIF von dem Node ausführen, auf dem die Cluster-LIF gehostet wird.

Tauschen Sie den Schalter aus

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der vorhandenen NVIDIA SN2100-Switches lauten *sw1* und *sw2*.
- Der Name des neuen NVIDIA SN2100 Switch lautet *nsw2*.
- Die Knotennamen sind *node1* und *node2*.
- Die Cluster-Ports auf jedem Node lauten *e3a* und *e3b*.
- Die Cluster LIF-Namen sind *node1_clus1* und *node1_clus2* für node1, und *node2_clus1* und *node2_clus2* für node2.

- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet `cluster1::*>`
- Breakout-Ports haben das Format `swp[Port]s[Breakout-Port 0-3]`. Beispielsweise sind vier Breakout-Ports auf `swp1` `swp1s0`, `swp1s1`, `swp1s2` und `swp1s3`.

Allgemeines zur Cluster-Netzwerktopologie

Dieses Verfahren basiert auf der folgenden 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 in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

3. Installieren Sie das entsprechende RCF und das entsprechende Image auf dem Switch, nsw2, und treffen Sie die erforderlichen Standortvorbereitungen.

Überprüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und Cumulus-Software für den neuen Switch.

- a. Sie können die entsprechende Cumulus-Software für Ihre Cluster-Switches von der Seite *NVIDIA Support* herunterladen. Folgen Sie den Schritten auf der Download-Seite, um das Cumulus Linux für die Version der ONTAP Software, die Sie installieren, herunterzuladen.
- b. Das entsprechende RCF ist im erhältlich "[NVIDIA Cluster und Storage Switches](#)" Seite. Befolgen Sie die Schritte auf der Download-Seite, um den korrekten RCF für die Version der von Ihnen installierenden ONTAP-Software herunterzuladen.

Schritt: Ports und Verkabelung konfigurieren

1. Melden Sie sich beim neuen Switch nsw2 als admin an und fahren Sie alle Ports herunter, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports swp1 bis swp14).

Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt haben.

Beispiel anzeigen

```
cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@nsw2:~$ net pending  
cumulus@nsw2:~$ net commit
```

2. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

Beispiel anzeigen

```
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. Vergewissern Sie sich, dass für alle Cluster-LIFs die automatische Zurücksetzung aktiviert ist:

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

4. Schließen Sie die ISL-Ports swp15 und swp16 am SN2100-Switch sw1 ab.

Beispiel anzeigen

```
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 verbinden Sie sie dann mit den gleichen Ports am SN2100 nsw2-Switch.
6. Die ISL-Ports swp15 und swp16 zwischen den Switches sw1 und nsw2.

Beispiel anzeigen

Die folgenden Befehle ermöglichen 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 auf Switch sw1 aufstehen:

```
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 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 diesen Port e3b Ist auf allen Knoten aktiv:

```
network port show -ipSpace Cluster
```

Beispiel anzeigen

Die Ausgabe sollte 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 Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise 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	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. Vergewissern Sie sich, dass alle Node-Cluster-Ports aktiv sind:

```
net show interface
```

Beispiel anzeigen

```
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. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
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. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

12. Bringen Sie auf Switch nsw2 die Ports an, die mit den Netzwerkports der Knoten verbunden sind.

Beispiel anzeigen

```
cumulus@nsw2:~$ net del interface swp1-14 link down  
cumulus@nsw2:~$ net pending  
cumulus@nsw2:~$ net commit
```

13. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

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

Node	Health	Eligibility
-----	-----	-----
node1	true	true
node2	true	true

14. Vergewissern Sie sich, dass alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

Beispiel anzeigen

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

Node node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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: Führen Sie den Vorgang durch

1. Vergewissern Sie sich, dass das Cluster-Netzwerk ordnungsgemäß funktioniert.

Beispiel anzeigen

```
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

2. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs1
```

```
Would you like to specify a user other than admin for log  
collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs2
```

```
Would you like to specify a user other than admin for log  
collection? {y|n}: n
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

3. Aktivieren Sie die Funktion zur Statusüberwachung des Ethernet-Switches.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log show  
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	cs1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	cs2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

4. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

5. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Ersetzen Sie NVIDIA SN2100-Cluster-Switches durch Switch-lose Verbindungen

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

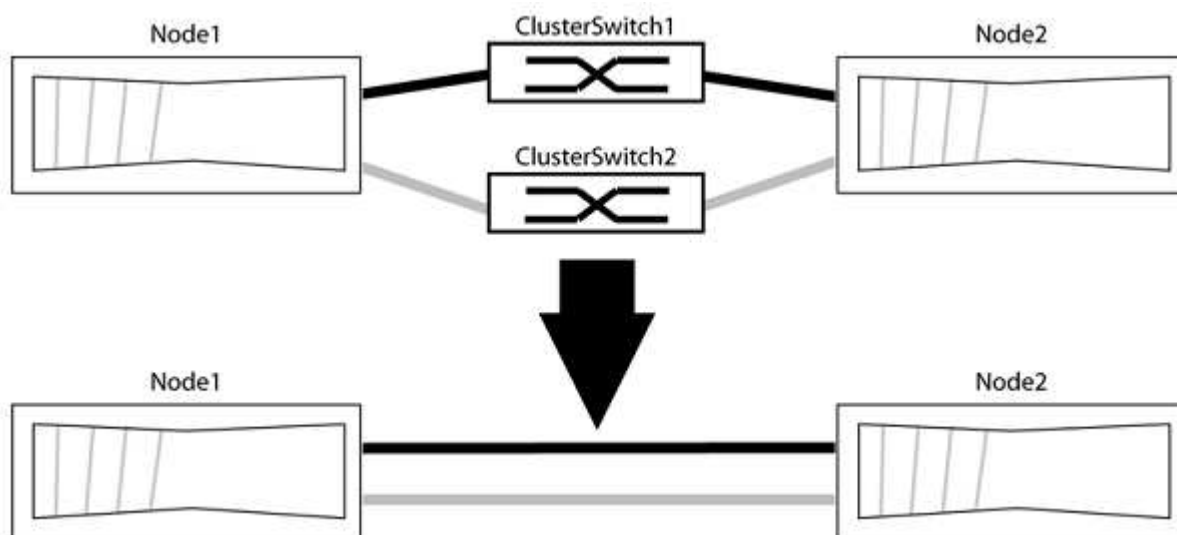
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Anzeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

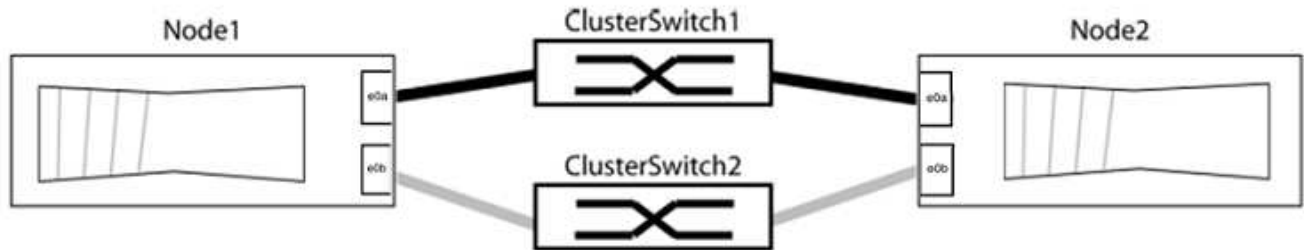
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```


Schritt: Ports und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in grop1 zu Cluster-Switch 1 wechseln und die Cluster-Ports in grop2 zu Cluster-Switch 2 wechseln. Diese Gruppen sind später im Verfahren erforderlich.
2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
network port show -ip space 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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



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

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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

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

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

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

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

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

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

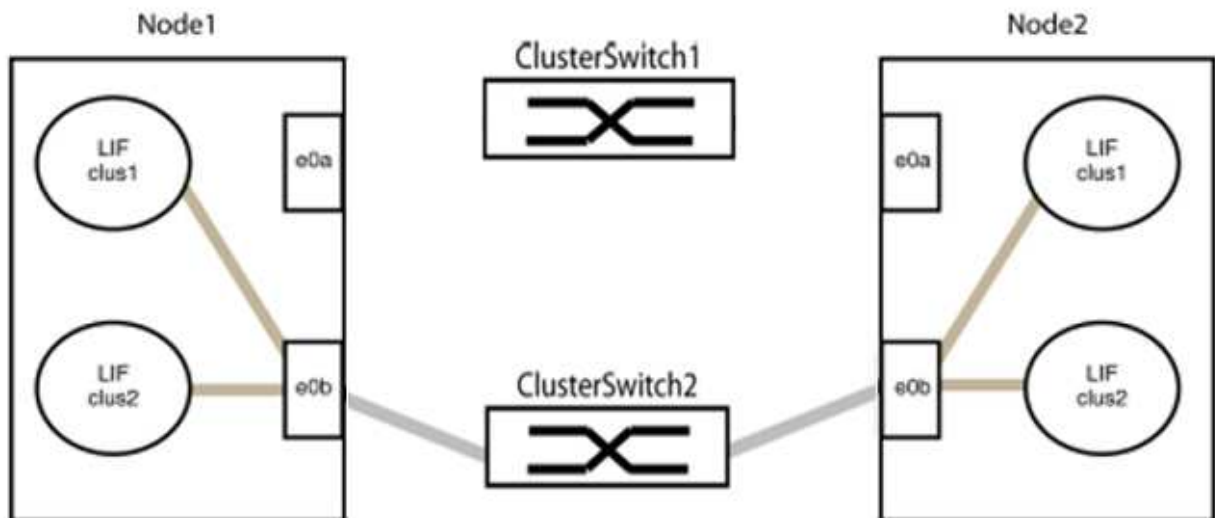
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

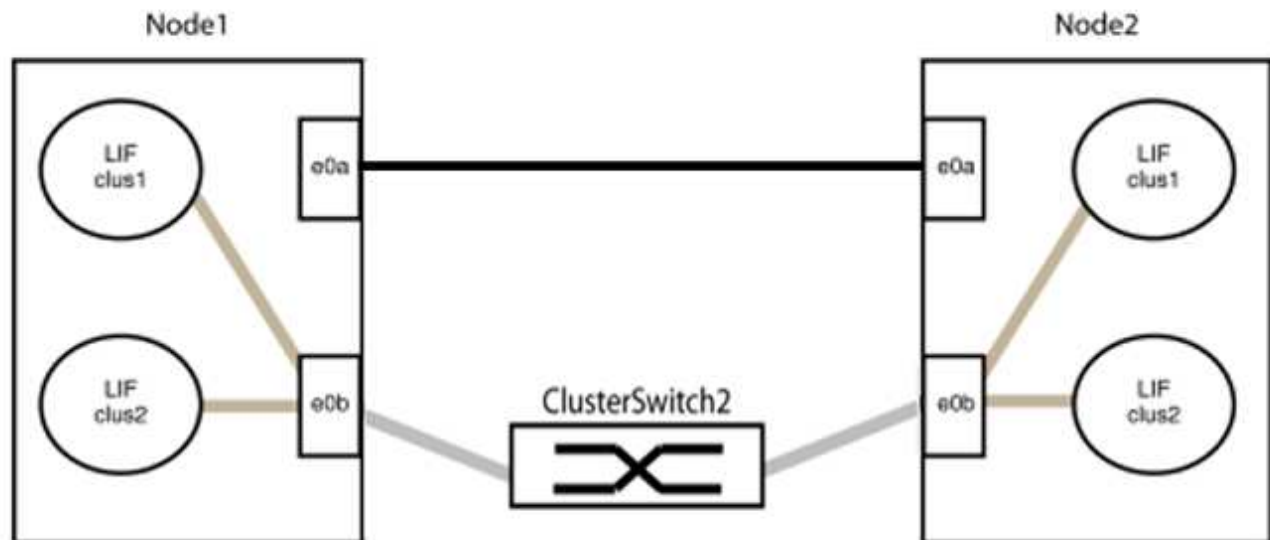
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

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

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

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

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:

```
cluster ping-cluster -node local
```



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

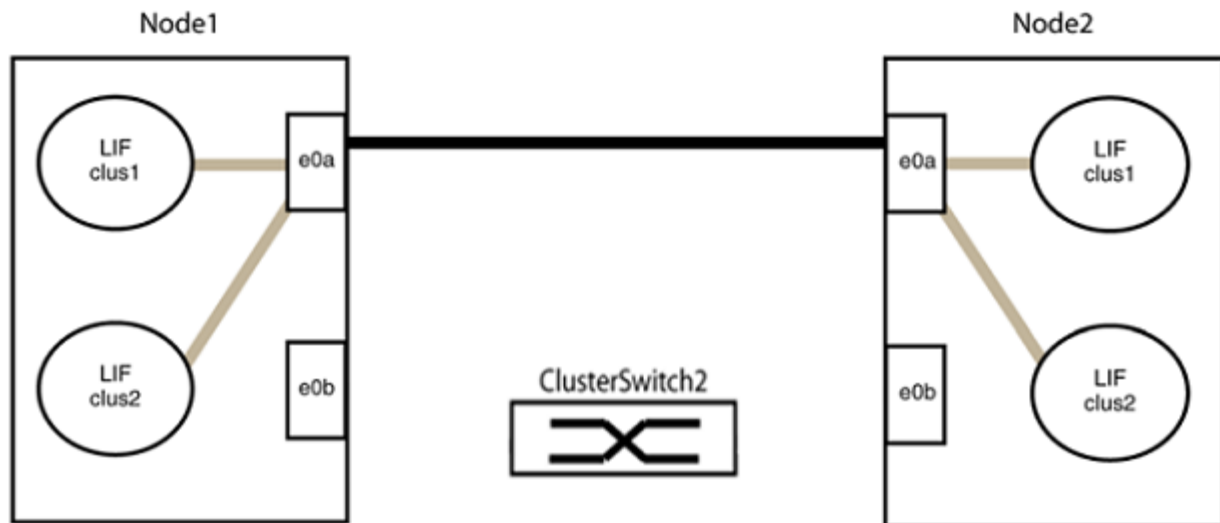
11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

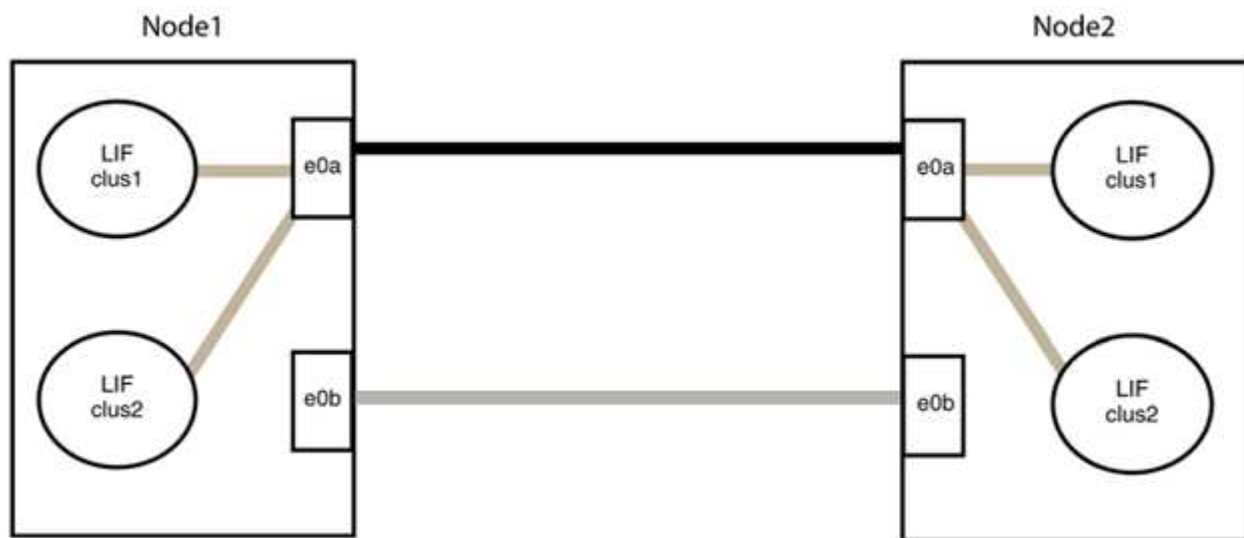
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

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

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

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

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

Storage Switches

Cisco Nexus 9336C-FX2

Überblick

Überblick über die Installation und Konfiguration der Cisco Nexus 9336C-FX2 Storage-Switches

Der Cisco Nexus 9336C-FX2 Storage-Switch ist Teil der Cisco Nexus 9000 Plattform und kann in einem NetApp System-Rack installiert werden. Storage-Switches ermöglichen das Routen von Daten zwischen Servern und Storage Arrays in einem Storage Area Network (SAN).

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen Cisco Nexus 9336C-FX2 Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Füllen Sie das Verkabelungsarbeitsblatt aus"](#).
2. ["Den Schalter einbauen"](#).
3. ["Konfigurieren Sie den Switch"](#).
4. ["Switch in NetApp-Schrank einbauen"](#).

Je nach Konfiguration können Sie den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Panel in einem NetApp Rack mit den im Lieferumfang des Switches enthaltenen Standardhalterungen installieren.

5. ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).
6. ["Installieren Sie die NX-OS-Software"](#).
7. ["Installieren Sie die RCF-Konfigurationsdatei"](#).

Installieren Sie den RCF, nachdem Sie den Nexus 9336C-FX2-Schalter zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)
- ["Anforderungen für Smart Call Home"](#)

Konfigurationsanforderungen für Cisco Nexus 9336C-FX2 Storage Switches

Prüfen Sie bei der Installation und Wartung von Cisco Nexus 9336C-FX2 Switches die Konfigurations- und Netzwerkanforderungen.

ONTAP Support

Ab ONTAP 9.9 können Sie mithilfe von Cisco Nexus 9336C-FX2 Switches Storage- und Cluster-Funktionen in einer gemeinsamen Switch-Konfiguration kombinieren.

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Netzwerk-Switches erforderlich.

Konfigurationsanforderungen

Für die Konfiguration benötigen Sie die entsprechende Anzahl und Art von Kabeln und Kabelanschlüssen für Ihre Switches.

Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie die folgenden Netzwerkinformationen.

- IP-Subnetz für den Management-Netzwerkdatenverkehr
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700s Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.
- Siehe "[Hardware Universe](#)" Aktuelle Informationen.

Weitere Informationen zur Erstkonfiguration des Switches finden Sie im folgenden Handbuch: "[Cisco Nexus 9336C-FX2 – Installations- und Upgrade-Leitfaden](#)".

Komponenten und Teilenummern für Cisco Nexus 9336C-FX2 Storage Switches

Informationen zur Installation und Wartung von Cisco Nexus 9336C-FX2 Switches finden Sie in der Liste der Komponenten und Teilenummern.

In der folgenden Tabelle sind die Teilenummer und Beschreibung für den Switch 9336C-FX2, die Lüfter und die Netzteile aufgeführt:

Teilenummer	Beschreibung
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT10/25/40/100GQSFP28
X190002	Zubehörkit X190001/X190003

Teilenummer	Beschreibung
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W Netzteil – Luftstrom am Port Side
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W Netzteil – Luftstrom für den seitlichen Ansauganschluss
X-NXA-LÜFTER-65CFM-PE	N9K-9336C 65 CFM, Luftstrom nach Anschlussseite
X-NXA-LÜFTER-65CFM-PI	N9K-9336C 65 CFM, Luftstrom zur Ansaugöffnung an der Seite des Ports

Dokumentationsanforderungen für Cisco Nexus 9336C-FX2 Storage-Switches

Überprüfen Sie bei der Installation und Wartung des Cisco Nexus 9336C-FX2 Switches spezielle Switch- und Controller-Dokumentation, um Ihre Cisco 9336-FX2-Switches und das ONTAP-Cluster einzurichten.

Switch-Dokumentation

Zum Einrichten der Cisco Nexus 9336C-FX2-Switches benötigen Sie die folgende Dokumentation über das ["Switches Der Cisco Nexus 9000-Serie Unterstützen"](#) Seite:

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie <i>Nexus 9000</i>	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 9000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.
<i>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 9000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 9000-Switches.
<i>Nexus 9000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.

Dokumenttitel	Beschreibung
<i>Versionshinweise zur Cisco Nexus 9000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Betriebssystemversion über das ["ONTAP 9 Dokumentationszentrum"](#).

Name	Beschreibung
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP-Dokumentation	Dieser Service bietet detaillierte Informationen zu allen Aspekten der ONTAP Versionen.
"Hardware Universe"	Liefert Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Schienensatz und Rack-Dokumentation

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

Name	Beschreibung
"42-HE-System-Cabinet, Deep Guide"	Beschreibt die FRUs, die dem 42U-Systemschrank zugeordnet sind, und bietet Anweisungen für Wartung und FRU-Austausch.
"Installation eines Cisco 9336-FX2 Switch in einem NetApp Rack"	Beschreibt die Installation eines Cisco Nexus 9336C-FX2 Switches in einem NetApp Rack mit vier Pfosten.

Anforderungen für Smart Call Home

Überprüfen Sie die folgenden Richtlinien, um die Smart Call Home-Funktion zu verwenden.

Smart Call Home überwacht die Hardware- und Softwarekomponenten Ihres Netzwerks. Wenn eine kritische Systemkonfiguration auftritt, generiert es eine E-Mail-basierte Benachrichtigung und gibt eine Warnung an alle Empfänger aus, die im Zielprofil konfiguriert sind. Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch konfigurieren, um per E-Mail mit dem Smart Call Home-System kommunizieren zu können. Darüber hinaus können Sie optional Ihren Cluster-Netzwerk-Switch einrichten, um die integrierte

Smart Call Home-Support-Funktion von Cisco zu nutzen.

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

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.
- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.
- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

Der "[Cisco Support-Website](#)" Enthält Informationen zu den Befehlen zum Konfigurieren von Smart Call Home.

Hardware installieren

Installieren Sie den Speicherschalter 9336C-FX2

Gehen Sie folgendermaßen vor, um den Cisco Nexus 9336C-FX2 Storage-Switch zu installieren.

Was Sie benötigen

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von "[Cisco Software-Download](#)" Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossen "[Verkabelungsarbeitsblätter](#)".
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden "[mysupport.netapp.com](#)". Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- Erforderliche Switch-Dokumentation Siehe "[Erforderliche Dokumentation](#)" Finden Sie weitere Informationen.

Schritte

1. Rack-Aufbau des Cluster-Netzwerks und der Management-Netzwerk-Switches und -Controller

Wenn Sie das installieren...	Dann...
Cisco Nexus 9336C-FX2 in einem NetApp Systemschrank	Siehe " Switch in NetApp-Schrank einbauen " Eine Anleitung zur Installation des Switches in einem NetApp-Schrank ist ebenfalls vorhanden.
Geräte in einem Telco-Rack	Siehe die Verfahren in den Installationsleitfäden für die Switch-Hardware sowie in den Installations- und Setup-Anleitungen für NetApp.

2. Verkabeln Sie die Switches für das Cluster-Netzwerk und das Management-Netzwerk mithilfe der

ausgefüllten Verkabelungsarbeitsblätter mit den Controllern.

3. Schalten Sie das Cluster-Netzwerk sowie die Switches und Controller des Managementnetzwerks ein.

Was kommt als Nächstes?

Gehen Sie zu ["Konfigurieren Sie den Cisco Nexus 9336C-FX2 Storage-Switch"](#).

Konfigurieren Sie den Speicherschalter 9336C-FX2

Gehen Sie folgendermaßen vor, um den Cisco Nexus 9336C-FX2-Switch zu konfigurieren.

Was Sie benötigen


- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von ["Cisco Software-Download"](#) Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossen ["Verkabelungsarbeitsblätter"](#).
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden ["mysupport.netapp.com"](#). Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- Erforderliche Switch-Dokumentation Siehe ["Erforderliche Dokumentation"](#) Finden Sie weitere Informationen.


Schritte

1. Initiale Konfiguration der Cluster-Netzwerk-Switches durchführen.

Geben Sie beim ersten Booten des Switches die folgenden Einrichtungsfragen entsprechend an. Die Sicherheitsrichtlinie Ihres Standorts definiert die zu erstellenden Antworten und Services.

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit ja . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (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, starkes Passwort erstellen. Ein schwaches Kennwort kann abgelehnt werden.
Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)	Reagieren Sie mit ja bei der Erstkonfiguration des Schalters.

Eingabeaufforderung	Antwort
Noch ein Login-Konto erstellen? (ja/nein)	Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen. Der Standardwert ist no .
Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Geben Sie den Switch-Namen ein.	Der Switch-Name ist auf 63 alphanumerische Zeichen begrenzt.
Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)	Beantworten Sie mit ja (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein.
Standard-Gateway konfigurieren? (ja/nein)	Antworten Sie mit ja . Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit ja. Die Standardeinstellung ist ja.</p> <div>  <p>SSH wird empfohlen, wenn Sie Cluster Switch Health Monitor (CSHM) für seine Protokollerfassung verwenden. SSHv2 wird auch für erhöhte Sicherheit empfohlen.</p> </div>
Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1).	Der Standardwert ist rsa .
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits von 1024 bis 2048 ein.
Konfigurieren Sie den NTP-Server? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Konfigurieren der Standard-Schnittstellenebene (L3/L2)	Antworten Sie mit L2 . Der Standardwert ist L2.

Eingabeaufforderung	Antwort
Konfiguration des Status der Standard-Switch-Port-Schnittstelle (Shutter/noshut)	Antworten Sie mit noshut . Die Standardeinstellung ist noshut.
Konfiguration des CoPP-Systemprofils (streng/mittelmäßig/lenient/dense)	Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, antworten Sie mit No an der Eingabeaufforderung. Beantworten Sie mit ja , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)	<p>Antworten Sie mit ja, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert.</p> <div>  <p>Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam.</p> </div>

- Überprüfen Sie die Konfigurationseinstellungen, die Sie am Ende der Einrichtung in der Anzeige vorgenommen haben, und stellen Sie sicher, dass Sie die Konfiguration speichern.
- Überprüfen Sie die Version der Cluster-Netzwerk-Switches und laden Sie bei Bedarf die von NetApp unterstützte Version der Software von auf die Switches von herunter "[Cisco Software-Download](#)" Seite.

Was kommt als Nächstes?

Optional können Sie "[Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack](#)". Andernfalls fahren Sie mit fort "[Bereiten Sie sich auf die Installation von NX-OS und RCF vor](#)".

Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack

Je nach Konfiguration müssen Sie möglicherweise den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Tafel in einem NetApp Rack installieren. Standardhalterungen sind im Lieferumfang des Schalters enthalten.

Was Sie benötigen

- Für jeden Switch müssen Sie die acht 10-32- oder 12-24-Schrauben und Muttern bereitstellen, um die Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten zu befestigen.
- Sie müssen den Cisco Standard-Schienenensatz verwenden, um den Switch in einem NetApp Rack zu installieren.



Die Jumper-Kabel sind nicht im Lieferumfang des Pass-Through-Kits enthalten und sollten in Ihrem Switch enthalten sein. Wenn die Switches nicht im Lieferumfang enthalten sind, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

Erforderliche Dokumentation

Lesen Sie die anfänglichen Vorbereitungsanforderungen, den Inhalt des Kits und die Sicherheitsvorkehrungen im ["Hardware-Installationsleitfaden Der Cisco Nexus 9000-Serie"](#).

Schritte

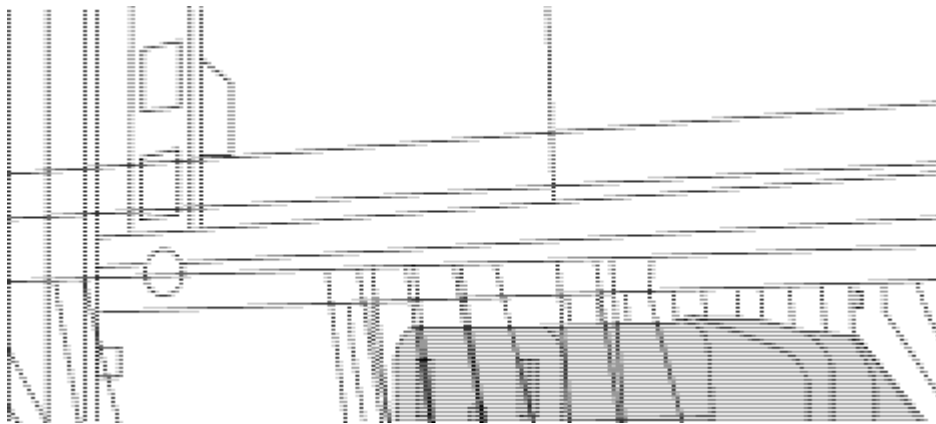
1. Die Pass-Through-Blindplatte in den NetApp-Schrank einbauen.

Die Pass-Through-Panel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

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

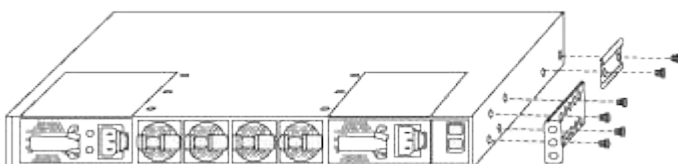
- Ein Durchlauf-Blindblech
- Vier 10-32 x 0,75 Schrauben
- Vier 10-32-Clip-Muttern
 - i. Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

Bei diesem Verfahren wird die Blindplatte in U40 installiert.
 - ii. Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
 - iii. Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
 - iv. Stecken Sie die Buchsen der beiden 48-Zoll-Jumper-Kabel von der Rückseite der Abdeckung und durch die Bürstenbaugruppe.



(1) *Buchsenleiste des Überbrückungskabels.*

2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Gehäuse des Nexus 9336C-FX2.
 - a. Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.



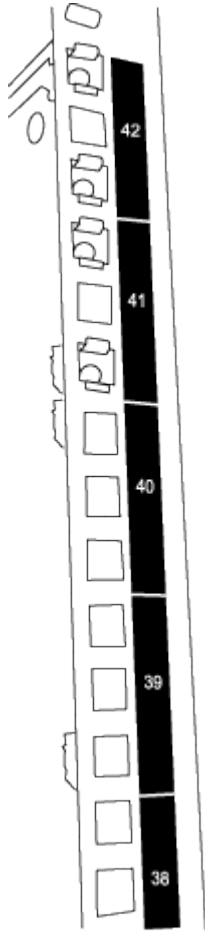
- b. Wiederholen Sie den Schritt [2 a](#) Mit der anderen vorderen Halterung für die Rackmontage auf der

anderen Seite des Schalters.

c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.

d. Wiederholen Sie den Schritt [2c](#) Mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite des Schalters.

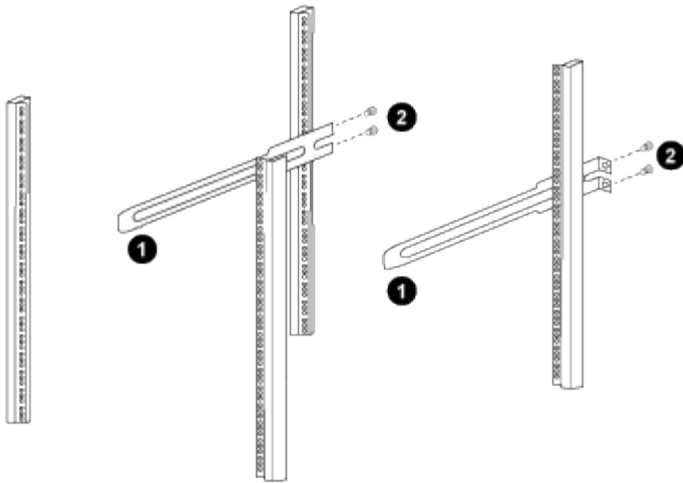
3. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



Die beiden 9336C-FX2 Schalter werden immer in der oberen 2 HE des Schrankes RU41 und 42 montiert.

4. Installieren Sie die Gleitschienen im Schrank.

a. Positionieren Sie die erste Gleitschiene an der RU42-Markierung auf der Rückseite des hinteren linken Pfosten, legen Sie die Schrauben mit dem entsprechenden Gewindetyp ein und ziehen Sie die Schrauben mit den Fingern fest.



(1) *beim sanften Schieben der Gleitschiene richten Sie sie an den Schraubenbohrungen im Rack aus.*

(2) *Schrauben der Gleitschienen an den Schrankleisten festziehen.*

a. Wiederholen Sie den Schritt 4 a Für den hinteren Pfosten auf der rechten Seite.

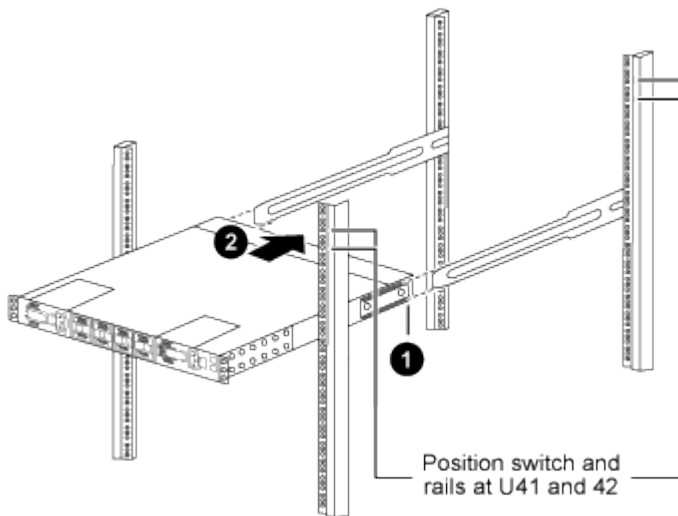
b. Wiederholen Sie die Schritte 4 a Und 4b An den RU41 Standorten auf dem Schrank.

5. Den Schalter in den Schrank einbauen.



Für diesen Schritt sind zwei Personen erforderlich: Eine Person muss den Schalter von vorne und von der anderen in die hinteren Gleitschienen führen.

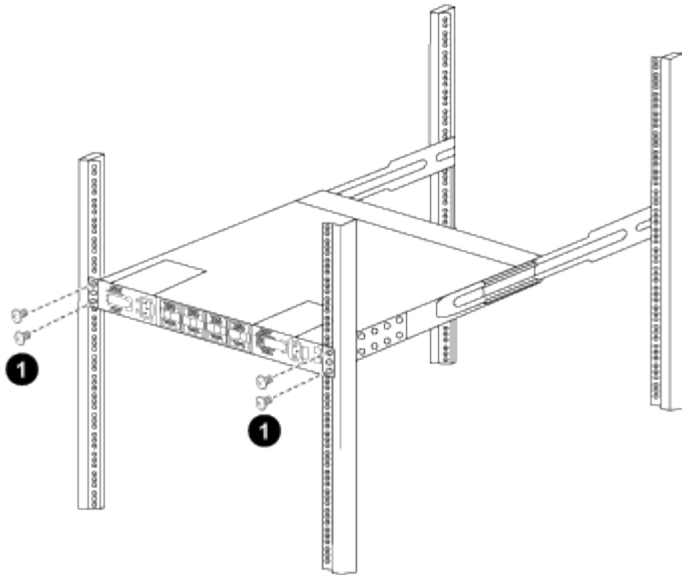
a. Positionieren Sie die Rückseite des Schalters an RU41.



(1) *Da das Gehäuse in Richtung der hinteren Pfosten geschoben wird, richten Sie die beiden hinteren Rackmontageführungen an den Gleitschienen aus.*

(2) *Schieben Sie den Schalter vorsichtig, bis die vorderen Halterungen der Rackmontage bündig mit den vorderen Pfosten sind.*

b. Befestigen Sie den Schalter am Gehäuse.



(1) mit einer Person, die die Vorderseite des Chassis hält, sollte die andere Person die vier hinteren Schrauben vollständig an den Schrankpfosten festziehen.

- a. Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- b. Wiederholen Sie die Schritte [5a](#) Bis [5c](#) Für den zweiten Schalter an der RU42-Position.



Durch die Verwendung des vollständig installierten Schalters als Unterstützung ist es nicht erforderlich, während des Installationsvorgangs die Vorderseite des zweiten Schalters zu halten.

6. Wenn die Switches installiert sind, verbinden Sie die Jumper-Kabel mit den Switch-Netzeinkabeln.
7. Verbinden Sie die Stecker beider Überbrückungskabel mit den am nächsten verfügbaren PDU-Steckdosen.



Um Redundanz zu erhalten, müssen die beiden Kabel mit verschiedenen PDUs verbunden werden.

8. Verbinden Sie den Management Port an jedem 9336C-FX2 Switch mit einem der Management-Switches (falls bestellt) oder verbinden Sie sie direkt mit dem Management-Netzwerk.

Der Management-Port ist der oben rechts gelegene Port auf der PSU-Seite des Switch. Das CAT6-Kabel für jeden Switch muss über die Passthrough-Leiste geführt werden, nachdem die Switches zur Verbindung mit den Management-Switches oder dem Management-Netzwerk installiert wurden.

Software konfigurieren

Workflow zur Softwareinstallation für Cisco Nexus 9336C-FX2 Storage-Switches

So installieren und konfigurieren Sie Software für einen Cisco Nexus 9336C-FX2 Switch:

1. ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).
2. ["Installieren Sie die NX-OS-Software"](#).

3. "Installieren Sie die RCF-Konfigurationsdatei".

Installieren Sie den RCF, nachdem Sie den Nexus 9336C-FX2-Schalter zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor

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

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01 und cluster1-02.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1 und cluster1-01_clus2 für cluster1-01 und cluster1-02_clusions1 und cluster1-02_clus2 für cluster1-02.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=x h`

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

Beispiel anzeigen

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

```
`network port show -ip space 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. Zeigt Informationen zu den LIFs an:

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


Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
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. Ping für die Remote-Cluster-LIFs:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node cluster1-02
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)
```

6. Vergewissern Sie sich, dass der automatische Zurücksetzen-Befehl 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
```

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

4 entries were displayed.

7. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password Und system switch ethernet log enable-collection
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

8. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

system cluster-switch log setup-password Und system cluster-switch log enable-collection

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Was kommt als Nächstes?

["Installieren Sie die NX-OS-Software".](#)

Installieren Sie die NX-OS-Software

Gehen Sie folgendermaßen vor, um die NX-OS-Software auf dem Nexus 9336C-FX2-Cluster-Switch zu installieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- ["Cisco Ethernet Switch Seite"](#). In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.
- Entsprechende Leitfäden für Software und Upgrades auf der Cisco Website für die Upgrade- und Downgrade-Verfahren von Cisco Switches. Siehe ["Switches Der Cisco Nexus 9000-Serie"](#).

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clusions1, cluster1-02_clus2 , cluster1-03_clug1, Cluster1-03_clus2, cluster1-04_clut1, und cluster1-04_clus2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Installieren Sie die Software

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Überprüfen Sie mit dem Ping-Befehl die Verbindung zum Server, der die NX-OS-Software und die RCF hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

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

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

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

Beispiel anzeigen

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

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

cs2# copy sftp: bootflash: vrf management

Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

4. 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#
```

5. Installieren Sie das NX-OS Image.

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

Beispiel anzeigen

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

```
Installer will perform compatibility check first. Please wait.
```

```
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.5.bin for boot variable "nxos".
```

```
[#####] 100% -- SUCCESS
```

```
Verifying image type.
```

```
[#####] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.5.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.5.bin.
```

```
[#####] 100% -- SUCCESS
```

```
Performing module support checks.
```

```
[#####] 100% -- SUCCESS
```

```
Notifying services about system upgrade.
```

```
[#####] 100% -- SUCCESS
```

```
Compatibility check is done:
```

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

```
Images will be upgraded according to following table:
```

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

```
Switch will be reloaded for disruptive upgrade.

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

Install is in progress, please wait.

Performing runtime checks.
[#####] 100% -- SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

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

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

6. 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:
```

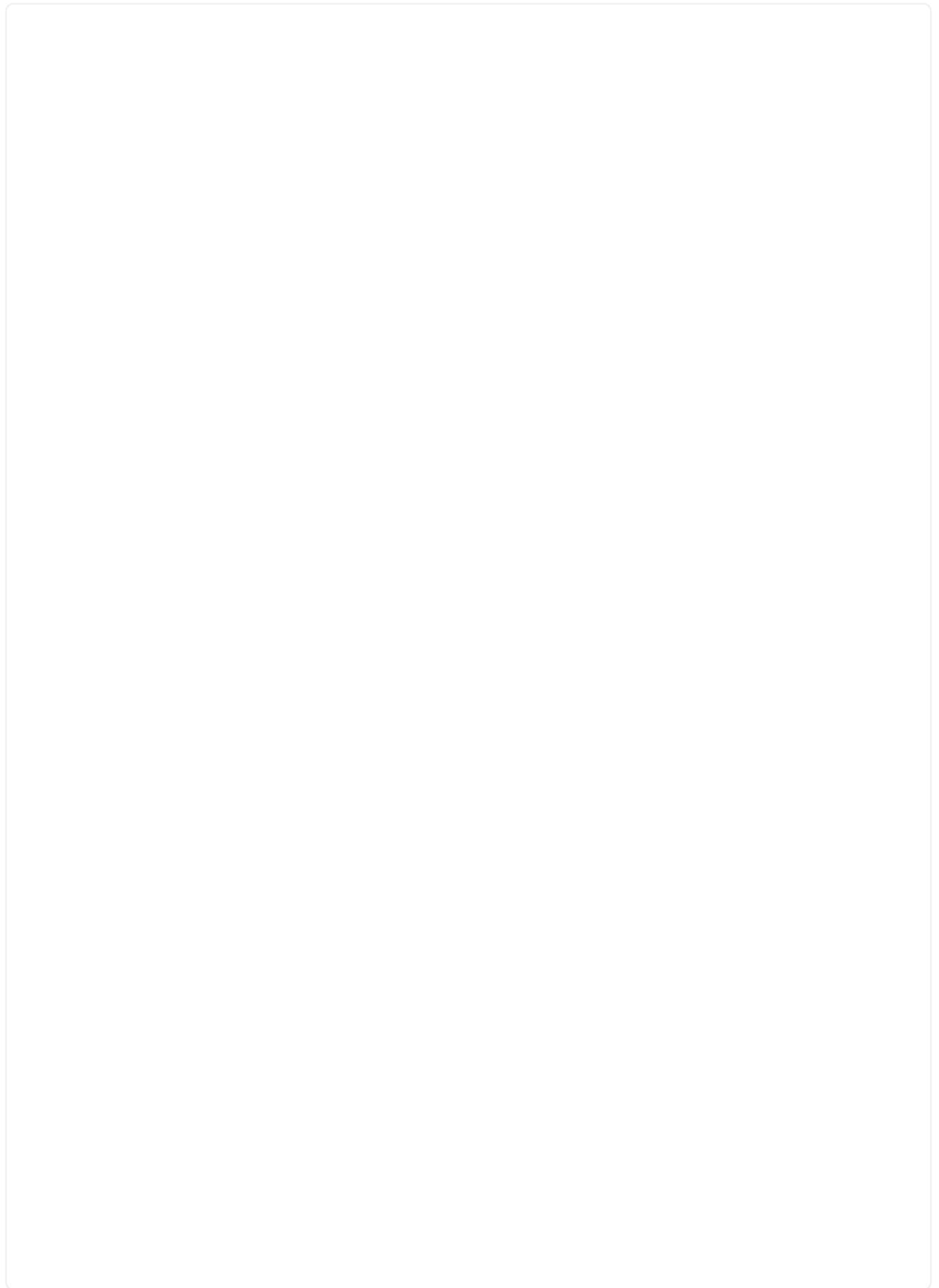
```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen



```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	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.

8. Melden Sie sich nach dem Neustart des Switches erneut an, und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

9. Wiederholen Sie die Schritte 1 bis 8, um die NX-OS-Software auf Switch cs1 zu installieren.

Was kommt als Nächstes?

["Installieren Sie die RCF-Konfigurationsdatei"](#).

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können den RCF nach dem ersten Einrichten des Nexus 9336C-FX2-Schalters installieren. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle RCF-Datei.
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.

Vorgeschlagene Dokumentation

- ["Cisco Ethernet Switch Seite"](#) In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie das RCF

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clusions1, cluster1-02_clus2, cluster1-03_clug1, Cluster1-03_clus2, cluster1-04_clut1, und cluster1-04_clus2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster Interconnect-Ports e0a und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein. Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritt 1: Vorbereitung für die Installation

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N9K-
C9336C
          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 Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports **up** mit einem gesunden Status sind:

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

Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

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

	Logical	Status	Network	
Current	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
-----
cs1                                     cluster-network      10.233.205.90      N9K-
C9336C
    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. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

Schritt 2: Ports konfigurieren

1. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

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

2. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```


Beispiel anzeigen

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

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

```
show running-config
```

5. Reinigen Sie die Konfiguration am Schalter cs2, und führen Sie eine grundlegende Einrichtung durch.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload

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

6. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

```
cs2# 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)...
```

7. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt Installation auf Schalter cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

8. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

Beispiel anzeigen

```
cs2# 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
*
*****
*****
```

9. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

10. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

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

11. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

12. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß 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.

- a. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

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 können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
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. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels verwendet:

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

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

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


Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

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

```
cluster show
```

Beispiel anzeigen

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

16. Wiederholen Sie die Schritte 4 bis 11 am Schalter cs1.
17. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

18. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

Schritt 3: Überprüfen Sie die Konfiguration

1. Stellen Sie sicher, dass die mit den Cluster-Ports verbundenen Switch-Ports **up** sind.

```
show interface brief
```

Beispiel anzeigen

```
cs1# show interface brief | grep up
.
.
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 Nodes weiterhin 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
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
```

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

```
show vlan brief
```

```
show interface trunk
```

Beispiel anzeigen

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
Eth1/34

```

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--
Eth1/9/1	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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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
Pol	1
..	
..	
..	
..	
..	



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

4. Stellen Sie sicher, dass die ISL 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      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	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::*>				

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

```
cluster show
```

Beispiel anzeigen

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

7. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

```
cluster ping-cluster -node local
```

Beispiel anzeigen

```
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)
```

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

+

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung mit dem Cluster-Switch 9336C-FX2 * CLI* eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im

vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-log-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-log-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.

ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.
Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 9336C-FX2-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                                SNMP USERS
-----
-----

User                Auth                Priv(enforce)    Groups
acl_filter
-----
-----
admin                md5                des(no)          network-admin
SNMPv3User           md5                aes-128(no)      network-operator
-----
-----

NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User                Auth                Priv
-----
-----

(sw1) (Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```


Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

                                Device Name: sw1
                                IP Address: 10.231.80.212
                                SNMP Version: SNMPv2c
                                Is Discovered: true
                                SNMPv2c Community String or SNMPv3 Username: cshml!
                                Model Number: N9K-C9336C-FX2
                                Switch Network: cluster-network
                                Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
                                Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
                                Source Of Switch Version: CDP/ISDP
                                Is Monitored ?: true
                                Serial Number of the Device: QTFCU3826001C
                                RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Ersetzen Sie einen Cisco Nexus 9336C-FX2 Storage-Switch

Sie können einen defekten Nexus 9336C-FX2-Switch in einem Cluster-Netzwerk ersetzen. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Was Sie benötigen

Stellen Sie vor der Installation der NX-OS-Software und der RCFs auf einem Cisco Nexus 9336C-FX2-Storage-Switch sicher, dass:

- Ihr System kann Cisco Nexus 9336C-FX2 Storage Switches unterstützen.
- Sie haben sich auf der Seite Cisco Ethernet Switch die Switch-Kompatibilitätstabelle für die unterstützten ONTAP-, NX-OS- und RCF-Versionen angehört.
- Sie haben die entsprechenden Leitfäden zu Software und Upgrades auf der Cisco Website zur Verfügung gestellt.

Switches Der Cisco Nexus 3000-Serie:

- Sie haben die entsprechenden RCFs heruntergeladen.
- Die vorhandene Netzwerkkonfiguration weist folgende Merkmale auf:

- Auf der Seite Cisco Ethernet Switches befinden sich die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.
- Management-Konnektivität muss auf beiden Switches vorhanden sein.
- Der Cisco Nexus 9336C-FX2-Ersatzschalter weist folgende Merkmale auf:
 - Die Management-Netzwerk-Konnektivität ist funktionsfähig.
 - Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
 - Das entsprechende RCF- und NX-OS-Betriebssystemabbild wird auf den Switch geladen.
 - Die anfängliche Konfiguration des Schalters ist abgeschlossen.

Über diese Aufgabe

Dieses Verfahren ersetzt den zweiten Nexus 9336C-FX2 Storage Switch S2 durch den neuen 9336C-FX Switch NS2. Die beiden Knoten sind node1 und node2.

Schritte zur Fertigstellung:

- Vergewissern Sie sich, dass der zu ersetzende Schalter S2 ist.
- Trennen Sie die Kabel vom Schalter S2.
- Schließen Sie die Kabel wieder an den Schalter NS2 an.
- Überprüfen Sie alle Gerätekonfigurationen auf Switch NS2.



Es können Abhängigkeiten zwischen der Befehlssyntax für in der RCF- und NX-OS-Version bestehen.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.

2. Überprüfen Sie den Integritätsstatus der Storage-Node-Ports, um sicherzustellen, dass eine Verbindung zum Storage-Switch S1 besteht:

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

Beispiel anzeigen

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

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

```
storage::*>
```

3. Stellen Sie sicher, dass der Speicherschalter S1 verfügbar ist:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e3a   S1                        Ethernet1/1 NX9336C
          e4a   node2                    e4a         AFF-A700
          e4e   node2                    e4e         AFF-A700
node1/lldp
          e3a   S1                        Ethernet1/1 -
          e4a   node2                    e4a         -
          e4e   node2                    e4e         -
node2/cdp
          e3a   S1                        Ethernet1/2 NX9336C
          e4a   node1                    e4a         AFF-A700
          e4e   node1                    e4e         AFF-A700
node2/lldp
          e3a   S1                        Ethernet1/2 -
          e4a   node1                    e4a         -
          e4e   node1                    e4e         -
storage::*>
```

4. Führen Sie die Show aus `lldp neighbors` Mit dem Befehl auf dem Arbeitsschalter bestätigen Sie, dass Sie beide Nodes und alle Shelves sehen können:

```
show lldp neighbors
```

Beispiel anzeigen

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf  Hold-time  Capability  Port ID
node1          Eth1/1     121        S           e3a
node2          Eth1/2     121        S           e3a
SHFGD2008000011 Eth1/5     121        S           e0a
SHFGD2008000011 Eth1/6     120        S           e0a
SHFGD2008000022 Eth1/7     120        S           e0a
SHFGD2008000022 Eth1/8     120        S           e0a
```

5. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf    id  remote-port  remote-device  
-----  --  -  
3.20     0  Ethernet1/5  S1  
3.20     1  -            -  
3.20     2  Ethernet1/6  S1  
3.20     3  -            -  
3.30     0  Ethernet1/7  S1  
3.20     1  -            -  
3.30     2  Ethernet1/8  S1  
3.20     3  -            -  
storage::*>
```

6. Entfernen Sie alle Kabel, die am Lagerschalter S2 angeschlossen sind.

7. Schließen Sie alle Kabel wieder an den Ersatzschalter NS2 an.

8. Überprüfen Sie den Integritätsstatus der Speicher-Node-Ports erneut:

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

Beispiel anzeigen

```
storage::*> storage port show -port-type ENET  
  
Node          Port Type  Mode    Speed      State   Status  VLAN  
-----  ----  ----  -  
node1  
          e3a  ENET  storage 100    enabled  online   30  
          e3b  ENET  storage  0    enabled  offline  30  
          e7a  ENET  storage  0    enabled  offline  30  
          e7b  ENET  storage  0    enabled  offline  30  
node2  
          e3a  ENET  storage 100    enabled  online   30  
          e3b  ENET  storage  0    enabled  offline  30  
          e7a  ENET  storage  0    enabled  offline  30  
          e7b  ENET  storage  0    enabled  offline  30  
storage::*>
```

9. Vergewissern Sie sich, dass beide Switches verfügbar sind:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----  -
node1/cdp
          e3a  S1                        Ethernet1/1 NX9336C
          e4a  node2                    e4a         AFF-A700
          e4e  node2                    e4e         AFF-A700
          e7b  NS2                      Ethernet1/1 NX9336C
node1/lldp
          e3a  S1                        Ethernet1/1 -
          e4a  node2                    e4a         -
          e4e  node2                    e4e         -
          e7b  NS2                      Ethernet1/1 -
node2/cdp
          e3a  S1                        Ethernet1/2 NX9336C
          e4a  node1                    e4a         AFF-A700
          e4e  node1                    e4e         AFF-A700
          e7b  NS2                      Ethernet1/2 NX9336C
node2/lldp
          e3a  S1                        Ethernet1/2 -
          e4a  node1                    e4a         -
          e4e  node1                    e4e         -
          e7b  NS2                      Ethernet1/2 -
storage::*>
```

10. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device,remote-port
```


Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf    id    remote-port    remote-device  
-----  --    -  
3.20     0     Ethernet1/5    S1  
3.20     1     Ethernet1/5    NS2  
3.20     2     Ethernet1/6    S1  
3.20     3     Ethernet1/6    NS2  
3.30     0     Ethernet1/7    S1  
3.20     1     Ethernet1/7    NS2  
3.30     2     Ethernet1/8    S1  
3.20     3     Ethernet1/8    NS2  
storage::*>
```

11. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

NVIDIA SN2100

Überblick

Überblick über den Konfigurationsprozess für NVIDIA SN2100 Storage Switches

Die NVIDIA SN2100 ist ein Storage Switch, über den Sie Daten zwischen Servern und Storage Arrays in einem Storage Area Network (SAN) weiterleiten können.

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen NVIDIA SN2100-Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Installieren Sie die Hardware für den NVIDIA SN2100 Switch"](#).

Anweisungen hierzu finden Sie im *NVIDIA Switch Installation Guide*.

2. ["Konfigurieren Sie den Switch"](#).

Anweisungen finden Sie in der NVIDIA-Dokumentation.

3. ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#).

Prüfen Sie die Anforderungen für optische Verbindungen, den QSA-Adapter und die Switch-Port-Geschwindigkeit.

4. ["Verkabelung der NS224 Shelves als Switch-Attached Storage"](#).

Befolgen Sie diese Anweisungen, wenn Sie über ein System verfügen, in dem die NS224-Laufwerk-Shelfs als Switch-Attached Storage (nicht als Direct-Attached Storage) verkabelt werden müssen.

5. ["Installieren Sie Cumulus Linux im Cumulus-Modus"](#) Oder ["Installieren Sie Cumulus Linux im ONIE-Modus"](#).

Sie können Cumulus Linux (CL) OS installieren, wenn der Switch Cumulus Linux oder ONIE ausführt.

6. ["Installieren Sie das Skript für die Referenzkonfigurationsdatei"](#).

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung.

7. ["Konfigurieren Sie SNMPv3 für die Switch-Protokollerfassung"](#).

Diese Version umfasst Unterstützung für SNMPv3 für die Erfassung von Switch-Protokollen und für Switch Health Monitoring (SHM).

Die Verfahren verwenden Network Command Line Utility (NCLU), eine Befehlszeilenoberfläche, die sicherstellt, dass Cumulus Linux für alle zugänglich ist. Der NET-Befehl ist das Wrapper-Dienstprogramm, mit dem Sie Aktionen von einem Terminal aus ausführen.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)

Konfigurationsanforderungen für NVIDIA SN2100 Switches

Prüfen Sie bei Installation und Wartung von NVIDIA SN2100-Switches alle Anforderungen.

Installationsvoraussetzungen

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Cluster-Netzwerk-Switches erforderlich. Sie können zusätzliche, optionale Management Switches verwenden.

Sie installieren den NVIDIA SN2100-Switch (X190006/X190106) im NVIDIA-Dual/Single-Switch-Gehäuse mit den im Lieferumfang des Switches enthaltenen Standardhalterungen.

Hinweise zur Verkabelung finden Sie unter ["Überlegungen zur Verkabelung und Konfiguration"](#).

ONTAP und Linux Unterstützung

Der NVIDIA SN2100 Switch ist ein 10/25/40/100 GB Ethernet-Switch mit Cumulus Linux. Der Switch unterstützt Folgendes:

- ONTAP 9.10.1P3. Der SN2100 Switch dient Cluster- und Speicheranwendungen in ONTAP 9.10.1P3 über verschiedene Switch-Paare. Ab ONTAP 9.10.1P3 können Sie mit NVIDIA SN2100 Switches Storage- und Cluster-Funktionen in einer gemeinsamen Switch-Konfiguration kombinieren.
- Cumulus Linux (CL) OS-Version 4.4.3. Aktuelle Informationen zur Kompatibilität finden Sie im ["NVIDIA"](#)

[Ethernet-Switches](#)" Informationsseite.

- Sie können Cumulus Linux installieren, wenn auf dem Switch Cumulus Linux oder ONIE ausgeführt wird.

Komponenten und Teilenummern für NVIDIA SN2100-Switches

Lesen Sie bei der Installation und Wartung von NVIDIA SN2100-Switches die Liste der Komponenten und Teilenummern für Schrank und Schienensatz.

Rack-Details

Sie installieren den NVIDIA SN2100-Switch (X190006/X190106) im NVIDIA-Dual/Single-Switch-Gehäuse mit den im Lieferumfang des Switches enthaltenen Standardhalterungen.

Einzelheiten zum Schienensatz

In der folgenden Tabelle sind die Teilenummer und Beschreibung der MSN2100-Switches und Schienen-Kits aufgeführt:

Teilenummer	Beschreibung
X190006-PE	Cluster Switch, NVIDIA SN2100, 16 PT 100 G, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16 PT 100 G, PSIN
X190106-FE-PE	Switch, NVIDIA SN2100, 16 PT 100 G, PTSX, Frontend
X190106-FE-PI	Switch, NVIDIA SN2100, 16 PT 100G, PSIN, Front End
X-MTEF-KIT-D	Rail Kit, NVIDIA Dual Switch Seite an Seite
X-MTEF-KIT-E	Rail Kit, NVIDIA Single Switch, kurze Tiefe



Weitere Informationen finden Sie in der NVIDIA-Dokumentation auf "[Installieren Sie den SN2100-Switch und den Schienen-Kit](#)".

Dokumentationsanforderungen für NVIDIA SN2100-Switches

Überprüfen Sie bei Installation und Wartung von NVIDIA SN2100-Switches alle empfohlenen Dokumente.

In der folgenden Tabelle ist die Dokumentation für die NVIDIA SN2100-Switches aufgeführt.

Titel	Beschreibung
"NVIDIA SN2100 Switches einrichten und konfigurieren"	Hier wird beschrieben, wie Sie Ihre NVIDIA SN2100-Switches einrichten und konfigurieren, einschließlich der Installation von Cumulus Linux und entsprechenden RCFs.

Titel	Beschreibung
"Von einem Cisco Cluster-Switch zu einem NVIDIA SN2100 Cluster-Switch migrieren"	Eine Beschreibung der Migration von Umgebungen, in denen Cisco Cluster Switches verwendet werden, in Umgebungen, die NVIDIA SN2100 Cluster-Switches verwenden.
"Von einem Cisco Storage Switch zu einem NVIDIA Storage Switch migrieren"	Eine Beschreibung der Migration von Umgebungen, die Cisco Storage Switches in Umgebungen verwenden, die NVIDIA SN2100 Storage-Switches verwenden.
"Migration zu einem Cluster mit zwei Nodes und NVIDIA SN2100 Cluster Switches"	Hier wird die Migration zu einer Switch-Umgebung mit zwei Nodes mit NVIDIA SN2100-Cluster-Switches beschrieben.
"Ersetzen Sie einen NVIDIA SN2100-Cluster-Switch"	Beschreibt das Verfahren zum Ersetzen eines defekten NVIDIA SN2100-Switch in einem Cluster und Herunterladen von Cumulus Linux und Referenzkonfigurationsdatei.
"Einen NVIDIA SN2100-Storage-Switch ersetzen"	Beschreibt das Verfahren zum Austausch eines defekten NVIDIA SN2100-Speicherschalters und Herunterladen von Cumulus Linux und Referenzkonfigurationsdatei.

Hardware installieren

Installieren Sie die Hardware für den NVIDIA SN2100 Switch

Informationen zur Installation der SN2100-Hardware finden Sie in der NVIDIA-Dokumentation.

Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen unter ["NVIDIA Switch Installation Guide"](#).

Was kommt als Nächstes?

["Konfigurieren Sie den Switch"](#).

Konfigurieren Sie den NVIDIA SN2100-Switch

Informationen zur Konfiguration des SN2100-Switch finden Sie in der NVIDIA-Dokumentation.

Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen unter ["NVIDIA System Bring-up:"](#).

Was kommt als Nächstes?

["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#).

Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Lesen Sie vor der Konfiguration des NVIDIA SN2100-Switches die folgenden Punkte.

Details zum NVIDIA-Port

Switch-Ports	Verwendung von Ports
Swp1s0-3	Nodes mit 10/40 Cluster-Ports
Swp2s0-3	Nodes mit 25/100 Cluster-Ports
Swp3-14 40/100-Cluster-Port-Knoten	Swp15-16 40/100 Inter-Switch Link (ISL)-Ports

Siehe "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

Optische Verbindungen

Nur optische Verbindungen werden auf SN2100-Switches mit X1151A NIC, X1146A NIC oder integrierten 100-GbE-Ports unterstützt. Beispiel:

- AFF A800 auf den Ports e0a und e0b
- AFF A320 an den Ports e0g und e0h

QSA-Adapter

Wenn ein QSA-Adapter für die Verbindung mit den integrierten Intel-Cluster-Ports auf einer Plattform verwendet wird, werden nicht alle Verbindungen hergestellt. Beispielsweise sind die Plattformen FAS2750, AFF A300 und FAS8200 (alle 10G) und AFF A250 (25G).

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

1. Stellen Sie bei Intel 10G die Verbindungsgeschwindigkeit swp1s0-3 manuell auf 10000 ein und setzen Sie die automatische Aushandlung auf aus.
2. Stellen Sie für Chelsio 25G die Verbindungsgeschwindigkeit swp2s0-3 manuell auf 25000 ein und setzen Sie die automatische Aushandlung auf aus.



Verwenden Sie die nicht-Breakout-40/100G-Ports mit 10G/25G QSA. Setzen Sie den QSA-Adapter nicht in Ports ein, die für Breakout konfiguriert sind.

Switch-Port-Geschwindigkeit

Je nach Sender/Empfänger im Switchport müssen Sie die Geschwindigkeit am Switchport möglicherweise auf eine feste Geschwindigkeit einstellen. Wenn Sie 10G- und 25G-Breakout-Ports verwenden, stellen Sie sicher, dass die automatische Aushandlung nicht erfolgt und stellen Sie die Port-Geschwindigkeit auf dem Switch fest. Beispiel:

```

cumulus@cumulus:mgmt:~$ net add int swpls3 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 swpls3
iface swpls3
    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

```

Was kommt als Nächstes?

["Verkabelung der NS224 Shelves als Switch-Attached Storage".](#)

Verkabelung der NS224 Shelves als Switch-Attached Storage

Wenn Sie über ein System verfügen, bei dem die NS224 Laufwerk-Shelves als Switch-Attached Storage verkabelt werden müssen (kein Direct-Attached Storage), verwenden Sie die hier bereitgestellten Informationen.

- Kabel-NS224-Laufwerk-Shelves über Storage-Switches:

["Informationen zu Verkabelung-Switch-Attached NS224-Laufwerk-Shelves"](#)

- Installieren Sie Ihre Speicher-Switches:

["Dokumentation zu den Switches von AFF und FAS"](#)

- Bestätigen Sie die unterstützte Hardware, z. B. die Storage-Switches und Kabel, für Ihr Plattformmodell:

Software konfigurieren

Workflow für die Softwareinstallation von NVIDIA SN2100 Storage-Switches

So installieren und konfigurieren Sie die Software für einen NVIDIA SN2100-Switch:

1. ["Installieren Sie Cumulus Linux im Cumulus-Modus"](#) Oder ["Installieren Sie Cumulus Linux im ONIE-Modus"](#).

Sie können Cumulus Linux (CL) OS installieren, wenn der Switch Cumulus Linux oder ONIE ausführt.

2. ["Installieren Sie das Skript für die Referenzkonfigurationsdatei"](#).

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung.

3. ["Konfigurieren Sie SNMPv3 für die Switch-Protokollerfassung"](#).

Diese Version umfasst Unterstützung für SNMPv3 für die Erfassung von Switch-Protokollen und für Switch Health Monitoring (SHM).

Die Verfahren verwenden Network Command Line Utility (NCLU), eine Befehlszeilenoberfläche, die sicherstellt, dass Cumulus Linux für alle zugänglich ist. Der NET-Befehl ist das Wrapper-Dienstprogramm, mit dem Sie Aktionen von einem Terminal aus ausführen.

Installieren Sie Cumulus Linux im Cumulus-Modus

Gehen Sie folgendermaßen vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im Cumulus-Modus läuft.



Cumulus Linux (CL) kann entweder installiert werden, wenn der Switch Cumulus Linux oder ONIE ausführt (siehe ["Im ONIE-Modus installieren"](#)).

Was Sie benötigen

- Linux-Wissen auf mittlerer Ebene.
- Vertrautheit mit grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren sind vorinstalliert, einschließlich `vi` und `nano`.
- Zugriff auf eine Linux oder UNIX Shell. Wenn Sie Windows verwenden, verwenden Sie eine Linux-Umgebung als Kommandozeilen-Tool für die Interaktion mit Cumulus Linux.
- Die Baudrate muss auf dem seriellen Konsolen-Switch für den Zugriff auf die NVIDIA SN2100 Switch-Konsole auf 115200 eingestellt werden:
 - 115200 Baud
 - 8 Datenbits
 - 1 Stoppbit
 - Parität: Keine
 - Flusskontrolle: Keine

Über diese Aufgabe

Beachten Sie Folgendes:



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.



Das Standardpasswort für das Cumulus-Benutzerkonto lautet **Cumulus**. Wenn Sie sich das erste Mal bei Cumulus Linux anmelden, müssen Sie dieses Standardpasswort ändern. Aktualisieren Sie alle Automatisierungsskripts, bevor Sie ein neues Image installieren. Cumulus Linux bietet Befehlszeilenoptionen zum automatischen Ändern des Standardpassworts während des Installationsvorgangs.

Schritte

1. Melden Sie sich beim Switch an.

Wenn Sie sich zum ersten Mal am Switch anmelden, benötigen Sie den Benutzernamen/das Passwort von **cumulus/cumulus** mit `sudo` Berechtigungen.

Beispiel anzeigen

```
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. Prüfen Sie die Cumulus Linux-Version:

```
net show system
```


Beispiel anzeigen

```
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 Standard-Gateway. Der neue Hostname wird erst nach dem Neustart der Konsole/SSH-Sitzung wirksam.



Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0`. Diese Schnittstelle wurde speziell für den Out-of-Band-Management-Einsatz entwickelt. Standardmäßig verwendet die Managementoberfläche DHCPv4 für Adressierung.



Verwenden Sie keine Unterstriche (`_`), Apostroph (`'`) oder nicht-ASCII-Zeichen im Hostnamen.

Beispiel anzeigen

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
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 beide `/etc/hostname` Und `/etc/hosts` Dateien:

4. Vergewissern Sie sich, dass der Hostname, die IP-Adresse, die Subnetzmaske und das Standard-Gateway aktualisiert wurden.

Beispiel anzeigen

```
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. Konfigurieren Sie die Zeitzone mithilfe des interaktiven NTP-Modus.

- a. Führen Sie auf einem Terminal den folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

- b. Folgen Sie den Menüoptionen auf dem Bildschirm, um den geografischen Bereich und die Region auszuwählen.
- c. Um die Zeitzone für alle Dienste und Dämonen einzustellen, starten Sie den Switch neu.
- d. Überprüfen Sie, ob das Datum und die Uhrzeit auf dem Switch korrekt sind, und aktualisieren Sie ggf..

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 bei Aufforderung *y* ein.

7. Starten Sie den NVIDIA SN2100-Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation wird automatisch gestartet, und die folgenden GRUB-Bildschirme werden angezeigt. Wählen Sie * nicht* aus:
 - Cumulus-Linux GNU/Linux
 - ONIE: Installieren des Betriebssystems
 - CUMULUS EINBAUEN
 - 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 lautet:

```
net show version
```

Beispiel anzeigen

```
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 dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

```
sudo adduser --ingroup netedit admin
```

Beispiel anzeigen

```
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+cl4.4.3u1
(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:~$
```

Was kommt als Nächstes?

"Installieren Sie das RCF-Skript".

Installieren Sie Cumulus Linux im ONIE-Modus

Gehen Sie folgendermaßen vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im ONIE-Modus ausgeführt wird.



Cumulus Linux (CL) kann entweder installiert werden, wenn der Switch Cumulus Linux oder ONIE ausführt (siehe ["Im Cumulus-Modus installieren"](#)).

Über diese Aufgabe

Sie können Cumulus Linux unter Verwendung der Open Network Install Environment (ONIE) installieren, die die automatische Erkennung eines Network Installer-Images ermöglicht. Dies erleichtert das Systemmodell der Sicherung von Schaltern mit einem Betriebssystem, wie Cumulus Linux. Die einfachste Möglichkeit, Cumulus Linux mit ONIE zu installieren, ist mit lokaler HTTP-Erkennung.



Wenn Ihr Host IPv6 aktiviert ist, stellen Sie sicher, dass er einen Webserver ausführt. Wenn der Host IPv4 aktiviert ist, stellen Sie sicher, dass er zusätzlich zu einem Webserver DHCP ausführt.

Dieses Verfahren zeigt, wie Cumulus Linux nach dem Start des Administrators in ONIE aktualisiert werden kann.

Schritte

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Benennen Sie diese Datei um `onie-installer`.
2. Verbinden Sie den Host über ein Ethernet-Kabel mit dem Management-Ethernet-Port des Switches.
3. Schalten Sie den Schalter ein. Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der Installation wird die Cumulus Linux-Anmeldeaufforderung im Terminalfenster angezeigt.



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Schalter neu:

```
cumulus@cumulus:mgmt:~$ sudo reboot
```

5. Drücken Sie die Taste **Esc** auf dem GNU GRUB-Bildschirm, um den normalen Bootvorgang zu unterbrechen, wählen Sie **ONIE** und drücken Sie **Enter**.
6. Wählen Sie auf dem nächsten Bildschirm **ONIE: Install OS** aus.
7. Der Vorgang zur Erkennung des ONIE-Installers führt die Suche nach der automatischen Installation durch. Drücken Sie **Enter**, um den Vorgang vorübergehend zu beenden.
8. Wenn der Erkennungsvorgang angehalten wurde:

```
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 Standard-Gateway korrekt zugewiesen sind:

```
ifconfig eth0
```

Beispiel anzeigen

```
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-Adressschema manuell definiert ist, 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. Cumulus Linux Installieren:

```
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 beim Switch an:

Beispiel anzeigen

```
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
```

Beispiel anzeigen

```
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"
```

Was kommt als Nächstes?

["Installieren Sie das RCF-Skript".](#)

Installieren Sie das RCF-Skript

Gehen Sie folgendermaßen vor, um das RCF-Skript zu installieren.

Was Sie benötigen

Stellen Sie vor der Installation des RCF-Skripts sicher, dass auf dem Switch folgende Funktionen verfügbar sind:

- Cumulus Linux 4.4.3 ist installiert.
- IP-Adresse, Subnetzmaske und Standard-Gateway über DHCP oder manuell konfiguriert definiert.

Aktuelle RCF-Skriptversionen

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Das Verfahren für jedes ist gleich.

- Clustering: **MSN2100-RCF-v1.8-Cluster**
- Storage: **MSN2100-RCF-v1.8-Storage**



Das folgende Beispiel zeigt, wie das RCF-Skript für Cluster-Switches heruntergeladen und angewendet wird.



Die Befehlsausgabe des Switch-Management verwendet die Switch-Management-IP-Adresse 10.233.204.71, die Netmask 255.255.254.0 und das Standard-Gateway 10.233.204.1.

Schritte

1. Zeigen Sie die verfügbaren Schnittstellen am SN2100-Schalter an:

```
net show interface all
```


Beispiel anzeigen

```
cumulus@cumulus: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	NotConfigure		
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. Kopieren Sie das RCF-Python-Skript auf den Switch:

```
cumulus@cumulus:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt: /tmp$ scp <user>@<host>:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster          100% 8607    111.2KB/s
00:00
```

3. Anwenden des RCF-Python-Skripts **MSN2100-RCF-v1.8-Cluster**:

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[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 oben aufgeführten Schritte durch.



Für Probleme mit RCF-Python-Skripts, die nicht behoben werden können, wenden Sie sich an ["NetApp Support"](#) Für weitere Unterstützung.

4. Überprüfen Sie die Konfiguration nach dem Neustart:

```
net show interface all
```

Beispiel anzeigen

```
cumulus@cumulus: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)
...
...

```

```
cumulus@cumulus: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%

5. Überprüfen Sie die Informationen für den Transceiver in der Schnittstelle:

```
net show interface pluggables
```

Beispiel anzeigen

```
cumulus@cumulus: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			

6. Stellen Sie sicher, dass die Nodes jeweils über eine Verbindung zu jedem Switch verfügen:

```
net show lldp
```

Beispiel anzeigen

```
cumulus@cumulus: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

7. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß sind:

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

Beispiel anzeigen

```
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						

- a. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch sw2 an, da LIFs nicht auf e0d homed sind).

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	-


```
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		

Was kommt als Nächstes?

"Konfigurieren Sie die Switch-Protokollerfassung".

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Der Benutzer für die Protokollerfassung muss angegeben werden, wenn die Referenzkonfigurationsdatei (RCF) angewendet wird. Standardmäßig ist dieser Benutzer auf „admin“ eingestellt. Wenn Sie einen anderen Benutzer verwenden möchten, müssen Sie dies im Abschnitt `*# SHM-Benutzer*s` des RCF angeben.
- Der Benutzer muss Zugriff auf die Befehle **nv show** haben. Dies kann durch Ausführen hinzugefügt werden `sudo adduser USER nv show` Und BENUTZER durch den Benutzer für die Protokollerfassung ersetzen.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```


Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Sammlung gestartet: Die detaillierte Support Protokolle und eine stündliche Erfassung von Periodic Daten:

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true
```

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log
-request true
```

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um Anweisungen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie das vorherige Verzeichnis der Protokollsammlung und die Datei '.tar' unter /tmp/shm_log Auf dem Schalter.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf NVIDIA SN2100-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
net add snmp-server username SNMPv3_USER auth-none
```
- Für * MD5/SHA-Authentifizierung*:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
net add snmp-server username SNMPv3_USER [auth-md5|auth-sha] AUTH-PASSWORD
[encrypt-aes|encrypt-des] PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
net show snmp status
```

Beispiel anzeigen

```
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status                active (running)
Reload Status                 enabled
Listening IP Addresses        all vrf mgmt
Main snmpd PID                4318
Version 1 and 2c Community String Configured
Version 3 Usernames           Not Configured
-----

cumulus@sw1:~$
cumulus@sw1:~$ net add snmp-server username SNMPv3User auth-md5
<password> encrypt-aes <password>
cumulus@sw1:~$ net commit
--- /etc/snmp/snmpd.conf      2020-08-02 21:09:34.686949282 +0000
+++ /run/nclu/snmp/snmpd.conf 2020-08-11 00:13:51.826126655 +0000
@@ -1,26 +1,28 @@
# Auto-generated config file: do not edit. #
agentaddress udp:@mgmt:161
agentxperms 777 777 snmp snmp
agentxsocket /var/agentx/master
createuser _snmptrapusernameX
+createuser SNMPv3User MD5 <password> AES <password>
ifmib_max_num_ifaces 500
iquerysecname _snmptrapusernameX
master agentx
monitor -r 60 -o laNames -o laErrMessage "laTable" laErrorFlag != 0
pass -p 10 1.3.6.1.2.1.1.1 /usr/share/snmp/sysDescr_pass.py
pass_persist 1.2.840.10006.300.43
/usr/share/snmp/ieee8023_lag_pp.py
pass_persist 1.3.6.1.2.1.17 /usr/share/snmp/bridge_pp.py
pass_persist 1.3.6.1.2.1.31.1.1.1.18
/usr/share/snmp/snmpifAlias_pp.py
pass_persist 1.3.6.1.2.1.47 /usr/share/snmp/entity_pp.py
pass_persist 1.3.6.1.2.1.99 /usr/share/snmp/entity_sensor_pp.py
pass_persist 1.3.6.1.4.1.40310.1 /usr/share/snmp/resq_pp.py
pass_persist 1.3.6.1.4.1.40310.2
/usr/share/snmp/cl_drop_cntrs_pp.py
pass_persist 1.3.6.1.4.1.40310.3 /usr/share/snmp/cl_poe_pp.py
pass_persist 1.3.6.1.4.1.40310.4 /usr/share/snmp/bgpun_pp.py
pass_persist 1.3.6.1.4.1.40310.5 /usr/share/snmp/cumulus-status.py
pass_persist 1.3.6.1.4.1.40310.6 /usr/share/snmp/cumulus-sensor.py
pass_persist 1.3.6.1.4.1.40310.7 /usr/share/snmp/vrf_bgpun_pp.py
+rocommunity cshml! default
```

```

rouser _snmptrapusernameX
+rouser SNMPv3User priv
sysobjectid 1.3.6.1.4.1.40310
syssservices 72
-rocommunity cshml! default

```

net add/del commands since the last "net commit"

=====

User	Timestamp	Command
-----	-----	-----
-----	-----	-----
SNMPv3User	2020-08-11 00:13:51.826987	net add snmp-server username SNMPv3User auth-md5 <password> encrypt-aes <password>

```

cumulus@sw1:~$
cumulus@sw1:~$ net show snmp status
Simple Network Management Protocol (SNMP) Daemon.
-----
Current Status          active (running)
Reload Status           enabled
Listening IP Addresses  all vrf mgmt
Main snmpd PID          24253
Version 1 and 2c Community String Configured
Version 3 Usernames     Configured    <---- Configured
here
-----
cumulus@sw1:~$

```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```

security login create -user-or-group-name SNMPv3User -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212

```

Beispiel anzeigen

```
cluster1::*> security login create -user-or-group-name SNMPv3User  
-application snmp -authentication-method usm -remote-switch  
-ipaddress 10.231.80.212
```

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha, sha2-256)

[none]: **md5**

Enter the authentication protocol password (minimum 8 characters long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)

[none]: **aes128**

Enter privacy protocol password (minimum 8 characters long):

Enter privacy protocol password again:

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1 (b8:59:9f:09:7c:22)" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: cshml!
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 4.4.3 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored ?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -snmp-version SNMPv3 -community-or-username
SNMPv3User
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums detaillierten Seriennummer identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1
(b8:59:9f:09:7c:22)" -instance

Device Name: sw1
(b8:59:9f:09:7c:22)
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
DEPRECATED-Community String or SNMPv3 Username: -
Community String or SNMPv3 Username: SNMPv3User
Model Number: MSN2100-CB2FC
Switch Network: cluster-network
Software Version: Cumulus Linux
version 4.4.3 running on Mellanox Technologies Ltd. MSN2100
Reason For Not Monitoring: None
Source Of Switch Version: LLDP
Is Monitored?: true
Serial Number of the Device: MT2110X06399 <----
serial number to check
RCF Version: MSN2100-RCF-v1.9X6-
Cluster-LLDP Aug-18-2022
```

Switches migrieren

Migrieren Sie von einem Cisco Storage Switch auf einen NVIDIA SN2100 Storage-Switch

Sie können ältere Cisco Switches für ein ONTAP Cluster zu NVIDIA SN2100 Storage Switches migrieren. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Folgende Storage-Switches werden unterstützt:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Siehe "[Hardware Universe](#)" Erhalten Sie ausführliche Informationen zu den unterstützten Ports und deren Konfigurationen.

Was Sie benötigen

Stellen Sie sicher, dass:

- Das vorhandene Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Storage-Ports befinden sich im Status up, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die NVIDIA SN2100-Speicherschalter sind konfiguriert und funktionieren unter der richtigen Version von Cumulus Linux, die mit der verwendeten Referenzkonfigurationsdatei (RCF) installiert wird.
- Die vorhandene Speichernetzwerkconfiguration verfügt über folgende Merkmale:
 - Ein redundantes und voll funktionsfähiges NetApp Cluster unter Verwendung beider älteren Cisco Switches.
 - Management-Konnektivität und Konsolenzugriff auf die älteren Cisco Switches und die neuen Switches.
 - Alle Cluster-LIFs im Status „up“ mit den Cluster-LIFs befinden sich auf den Home-Ports.
 - ISL-Ports aktiviert und zwischen den älteren Cisco Switches und zwischen den neuen Switches verkabelt.
- Siehe "[Hardware Universe](#)" Erhalten Sie ausführliche Informationen zu den unterstützten Ports und deren Konfigurationen.
- Einige der Ports sind auf NVIDIA SN2100-Switches für 100 GbE konfiguriert.
- Sie haben 100-GbE-Konnektivität von Nodes zu NVIDIA SN2100 Storage-Switches geplant, migriert und dokumentiert.

Migrieren Sie die Switches

Zu den Beispielen

In diesem Verfahren werden Cisco Nexus 9336C-FX2 Storage-Switches zum Beispiel Befehle und Ausgänge verwendet.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen Cisco Nexus 9336C-FX2 Storage Switches sind *S1* und *S2*.
- Die neuen NVIDIA SN2100 Storage-Switches sind *sw1* und *sw2*.
- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node *1_clus1_* und *node1_clus2* und *node2_clus1* bzw. *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Netzwerk-Ports sind *e5a* und *e5b*.
- Breakout-Ports haben das Format *swp1s0-3*. Zum Beispiel sind vier Breakout-Ports auf *swp1 swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.
- Schalter *S2* wird zuerst durch Schalter *sw2* ersetzt und dann Schalter *S1* durch Schalter *sw1* ersetzt.
 - Die Verkabelung zwischen den Knoten und *S2* wird dann von *S2* getrennt und wieder mit *sw2* verbunden.
 - Die Verkabelung zwischen den Knoten und *S1* wird dann von *S1* getrennt und wieder mit *sw1* verbunden.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport aktiviert ist, unterdrücken Sie die automatische Erstellung eines Cases durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

3. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Storage-Schnittstellen fest:

Jeder Port sollte für aktiviert angezeigt werden `Status`.

Schritt: Kabel und Ports konfigurieren

1. Zeigen Sie die Attribute des Netzwerkports an:

```
storage port show
```

Beispiel anzeigen

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

2. Überprüfen Sie mithilfe des Befehls, ob die Storage-Ports auf jedem Node (aus Sicht der Nodes) auf folgende Weise mit vorhandenen Storage-Switches verbunden sind:

```
network device-discovery show -protocol lldp
```

Beispiel anzeigen

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

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

node1	/lldp		
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1 -
	e5b	S2 (7c:ad:4f:98:8e:3c)	Eth1/1 -
node2	/lldp		
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2 -
	e5b	S2 (7c:ad:4f:98:8e:3c)	Eth1/2 -

3. Stellen Sie am Schalter S1 und S2 sicher, dass die Speicheranschlüsse und -Schalter (aus der Perspektive der Switches) mit dem Befehl wie folgt verbunden sind:

```
show lldp neighbors
```

Beispiel anzeigen

S1# **show lldp neighbors**

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

Device-ID Port ID	Local Intf	Holdtime	Capability
node1 e0c	Eth1/1	121	S
node2 e0c	Eth1/2	121	S
SHFGD1947000186 e0a	Eth1/10	120	S
SHFGD1947000186 e0a	Eth1/11	120	S
SHFGB2017000269 e0a	Eth1/12	120	S
SHFGB2017000269 e0a	Eth1/13	120	S

S2# **show lldp neighbors**

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

Device-ID Port ID	Local Intf	Holdtime	Capability
node1 e5b	Eth1/1	121	S
node2 e5b	Eth1/2	121	S
SHFGD1947000186 e0b	Eth1/10	120	S
SHFGD1947000186 e0b	Eth1/11	120	S
SHFGB2017000269 e0b	Eth1/12	120	S
SHFGB2017000269 e0b	Eth1/13	120	S

4. Fahren Sie beim Switch sw2 die mit den Storage-Ports und den Nodes der Festplatten-Shelfs verbundenen Ports herunter.

Beispiel anzeigen

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Verschieben Sie die Node Storage Ports des Controllers und der Festplatten-Shelfs vom alten Switch S2 auf den neuen Switch sw2. Verwenden Sie dazu die geeignete Verkabelung, die von NVIDIA SN2100 unterstützt wird.
6. Stellen Sie beim Switch sw2 die Ports bereit, die mit den Speicherports der Knoten und der Festplatten-Shelfs verbunden sind.

Beispiel anzeigen

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Vergewissern Sie sich, dass die Storage-Ports auf jedem Node aus Sicht der Nodes nun auf folgende Weise mit den Switches verbunden sind:

```
network device-discovery show -protocol lldp
```

Beispiel anzeigen

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

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

node1	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

8. Überprüfen Sie die Netzwerkanschlussattribute:

```
storage port show
```

Beispiel anzeigen

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2							
	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

9. Vergewissern Sie sich bei Switch sw2, dass alle Knoten Speicher-Ports aktiv sind:

```
net show interface
```

Beispiel anzeigen

```
cumulus@sw2:~$ 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)					
...					
...					

10. Fahren Sie beim Switch sw1 die Ports herunter, die mit den Speicherports der Knoten und der Platten-Shelves verbunden sind.

Beispiel anzeigen

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Verschieben Sie die Node Storage Ports des Controllers und der Festplatten-Shelves vom alten Switch S1 zum neuen Switch sw1. Verwenden Sie dazu die geeignete Verkabelung, die von NVIDIA SN2100 unterstützt wird.
12. Bringen Sie am Switch sw1 die Ports auf, die mit den Speicherports der Knoten und den Platten-Shelves verbunden sind.

Beispiel anzeigen

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Vergewissern Sie sich, dass die Storage-Ports auf jedem Node aus Sicht der Nodes nun auf folgende Weise mit den Switches verbunden sind:

```
network device-discovery show -protocol lldp
```

Beispiel anzeigen

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

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

node1	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

14. Überprüfen der endgültigen Konfiguration:

```
storage port show
```

Jeder Port sollte für aktiviert angezeigt werden State Und aktiviert für Status.

Beispiel anzeigen

```
cluster1::*> storage port show
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID

node1	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30
node2	e0c	ENET	storage	100	enabled	online	30
	e0d	ENET	storage	0	enabled	offline	30
	e5a	ENET	storage	0	enabled	offline	30
	e5b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

15. Vergewissern Sie sich bei Switch sw2, dass alle Knoten Speicher-Ports aktiv sind:

```
net show interface
```

Beispiel anzeigen

```
cumulus@sw2:~$ 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)					
...					
...					

16. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
cumulus@sw1:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
...				
swp1	100G	Trunk/L2	node1	e0c
swp2	100G	Trunk/L2	node2	e0c
swp3	100G	Trunk/L2	SHFFG1826000112	e0a
swp4	100G	Trunk/L2	SHFFG1826000112	e0a
swp5	100G	Trunk/L2	SHFFG1826000102	e0a
swp6	100G	Trunk/L2	SHFFG1826000102	e0a

```
cumulus@sw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
-----	-----	-----	-----	-----
...				
swp1	100G	Trunk/L2	node1	e5b
swp2	100G	Trunk/L2	node2	e5b
swp3	100G	Trunk/L2	SHFFG1826000112	e0b
swp4	100G	Trunk/L2	SHFFG1826000112	e0b
swp5	100G	Trunk/L2	SHFFG1826000102	e0b
swp6	100G	Trunk/L2	SHFFG1826000102	e0b

Schritt 3: Führen Sie den Vorgang durch

1. Aktivieren Sie die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den beiden Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

```
system switch ethernet log setup-password Und system switch ethernet log  
enable-collection
```

Geben Sie Ein: system switch ethernet log setup-password

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sw1
sw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: sw2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

Gefolgt von:

```
system switch ethernet log enable-collection
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

2. Initiieren der Switch-Protokollerfassung:

```
system switch ethernet log collect -device *
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung erfolgreich war mit dem folgenden Befehl:

```
system switch ethernet log show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log show
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	sw1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	sw2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete

3. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

4. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Ersetzen Sie einen NVIDIA SN2100 Storage-Switch

Beim Austausch von NVIDIA SN2100 Storage Switches müssen Sie bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen kennen.

Bevor Sie beginnen

Vor der Installation der Cumulus-Software und der RCFs auf einem NVIDIA SN2100-Speicherschalter müssen Sie überprüfen, ob die folgenden Bedingungen vorliegen:

- Ihr System kann NVIDIA SN2100 Storage Switches unterstützen.
- Sie müssen die entsprechenden RCFs heruntergeladen haben.
- Der "[Hardware Universe](#)" Ausführliche Informationen zu unterstützten Ports und deren Konfigurationen erhalten Sie im Detail.

Über diese Aufgabe

Die vorhandene Netzwerkkonfiguration muss die folgenden Merkmale aufweisen:

- Stellen Sie sicher, dass alle Fehlerbehebungsschritte durchgeführt wurden, um zu bestätigen, dass Ihr Switch ausgetauscht werden muss.
- Management-Konnektivität muss auf beiden Switches vorhanden sein.



Stellen Sie sicher, dass alle Fehlerbehebungsschritte durchgeführt wurden, um zu bestätigen, dass Ihr Switch ausgetauscht werden muss.

Der Ersatz-NVIDIA SN2100-Switch muss die folgenden Eigenschaften aufweisen:

- Die Konnektivität des Managementnetzwerks muss funktionsfähig sein.
- Der Konsolenzugriff auf den Ersatzschalter muss vorhanden sein.
- Das entsprechende RCF- und Cumulus-Betriebssystemabbild muss auf den Switch geladen werden.
- Die anfängliche Anpassung des Schalters muss abgeschlossen sein.

Zusammenfassung der Vorgehensweise

Dieses Verfahren ersetzt den zweiten NVIDIA SN2100 Storage Switch sw2 durch den neuen NVIDIA SN2100 Switch nsw2. Die beiden Knoten sind node1 und node2.

Schritte zur Fertigstellung:

- Vergewissern Sie sich, dass der zu ersetzende Schalter sw2 ist.
- Trennen Sie die Kabel vom Schalter sw2.
- Schließen Sie die Kabel wieder an den Schalter nsw2 an.
- Überprüfen Sie alle Gerätekonfigurationen am Switch nsw2.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren: `set -privilege advanced`
3. Überprüfen Sie den Integritätsstatus der Storage-Node-Ports, um sicherzustellen, dass eine Verbindung zum Storage-Switch S1 besteht:

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

Beispiel anzeigen

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

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	100	enabled	online	30

```
cluster1::*>
```

4. Stellen Sie sicher, dass der Speicherschalter sw1 verfügbar ist:

```
network device-discovery show
```

Beispiel anzeigen

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
node1/lldp				
	e3a	sw1 (b8:ce:f6:19:1b:42)	swp3	-
node2/lldp				
	e3a	sw1 (b8:ce:f6:19:1b:42)	swp4	-

```
cluster1::*>
```

5. Führen Sie die aus

`net show interface` Mit dem Befehl auf dem Arbeitsschalter bestätigen Sie, dass Sie beide Nodes und alle Shelves sehen können:

```
net show interface
```

Beispiel anzeigen

```
cumulus@sw1:~$ net show interface
```

State	Name	Spd	MTU	Mode	LLDP
Summary					

...					
...					
UP	swp1	100G	9216	Trunk/L2	node1 (e3a)
Master: bridge(UP)					
UP	swp2	100G	9216	Trunk/L2	node2 (e3a)
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)					
...					
...					

6. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device, remote-port
```


Beispiel anzeigen

```
cluster1::*> storage shelf port show -fields remote-device, remote-  
port  
shelf    id  remote-port  remote-device  
-----  --  -  
3.20     0   swp3         sw1  
3.20     1   -           -  
3.20     2   swp4         sw1  
3.20     3   -           -  
3.30     0   swp5         sw1  
3.20     1   -           -  
3.30     2   swp6         sw1  
3.20     3   -           -  
cluster1::*>
```

7. Entfernen Sie alle Kabel, die am Speicherschalter sw2 angeschlossen sind.

8. Schließen Sie alle Kabel wieder an den Ersatzschalter nsw2 an.

9. Überprüfen Sie den Integritätsstatus der Speicher-Node-Ports erneut:

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

Beispiel anzeigen

```
cluster1::*> storage port show -port-type ENET  
  
Node      Port Type  Mode   Speed      State   Status   VLAN  
-----  -  
node1  
          e3a  ENET  storage 100    enabled  online   30  
          e3b  ENET  storage 0     enabled  offline  30  
          e7a  ENET  storage 0     enabled  offline  30  
          e7b  ENET  storage 100   enabled  online   30  
node2  
          e3a  ENET  storage 100    enabled  online   30  
          e3b  ENET  storage 0     enabled  offline  30  
          e7a  ENET  storage 0     enabled  offline  30  
          e7b  ENET  storage 100   enabled  online   30  
cluster1::*>
```

10. Vergewissern Sie sich, dass beide Switches verfügbar sind:

```
net device-discovery show
```

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:f6:19:1b:96)   swp1       -
          e7b  nsw2 (b8:ce:f6:19:1a:7e)  swp1       -
node2/lldp
          e3a  sw1 (b8:ce:f6:19:1b:96)   swp2       -
          e7b  nsw2 (b8:ce:f6:19:1a:7e)  swp2       -
cluster1::*>
```

11. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device, remote-port
```

Beispiel anzeigen

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf  id  remote-port  remote-device
-----  --  -
3.20   0   swp3         sw1
3.20   1   swp3         nsw2
3.20   2   swp4         sw1
3.20   3   swp4         nsw2
3.30   0   swp5         sw1
3.20   1   swp5         nsw2
3.30   2   swp6         sw1
3.20   3   swp6         nsw2
cluster1::*>
```

12. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sw1
nsw2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: csw1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: nsw2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

13. Aktivieren Sie die Funktion zur Statusüberwachung des Ethernet-Switches.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] **y**

Enabling cluster switch log collection.

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log show  
Log Collection Enabled: true
```

Index	Switch	Log Timestamp	Status
-----	-----	-----	-----
1	sw1 (b8:ce:f6:19:1b:42)	4/29/2022 03:05:25	complete
2	nsw2 (b8:ce:f6:19:1b:96)	4/29/2022 03:07:42	complete



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

14. Ändern Sie die Berechtigungsebene zurück in den Administrator: `set -privilege admin`
15. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:
`system node autosupport invoke -node * -type all -message MAINT=END`

Shared-Switches

Cisco Nexus 9336C-FX2

Überblick

Überblick über Installation und Konfiguration für gemeinsame Cisco Nexus 9336C-FX2-Switches

Der gemeinsame Switch der Cisco Nexus 9336C-FX2 ist Teil der Cisco Nexus 9000 Plattform und kann in einem NetApp Systemschrank installiert werden. Gemeinsam genutzte Switches ermöglichen es Ihnen, Cluster- und Storage-Funktionen in einer gemeinsamen Switch-Konfiguration zu kombinieren, indem Sie gemeinsam genutzte Cluster- und Speicherreferenzkonfigurationsdateien unterstützen.

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen Cisco Nexus 9336C-FX2 Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Füllen Sie das Verkabelungsarbeitsblatt aus"](#).

Verwenden Sie die Verkabelungsabbilder, um die Verkabelung zwischen den Controllern und den Switches abzuschließen.

2. ["Den Schalter einbauen"](#).
3. ["Konfigurieren Sie den Switch"](#).
4. ["Switch in NetApp-Schrank einbauen"](#).

Je nach Konfiguration können Sie den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Panel in einem NetApp Rack mit den im Lieferumfang des Switches enthaltenen Standardhalterungen installieren.

5. ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).
6. ["Installieren Sie die NX-OS-Software"](#).
7. ["Installieren Sie die RCF-Konfigurationsdatei"](#).

Installieren Sie den RCF, nachdem Sie den Nexus 9336C-FX2-Schalter zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)

Konfigurationsanforderungen für gemeinsame Cisco Nexus 9336C-FX2 Switches

Prüfen Sie bei der Installation und Wartung von Cisco Nexus 9336C-FX2 Switches die

Konfigurations- und Netzwerkanforderungen.

ONTAP Support

Ab ONTAP 9.9 können Sie mithilfe von Cisco Nexus 9336C-FX2 Switches Storage- und Cluster-Funktionen in einer gemeinsamen Switch-Konfiguration kombinieren.

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Netzwerk-Switches erforderlich.

Konfigurationsanforderungen

Für die Konfiguration benötigen Sie die entsprechende Anzahl und Art von Kabeln und Kabelanschlüssen für Ihre Switches.

Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie die folgenden Netzwerkinformationen.

- IP-Subnetz für den Management-Netzwerkdatenverkehr
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700s Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.
- Siehe "[Hardware Universe](#)" Aktuelle Informationen.

Weitere Informationen zur Erstkonfiguration des Switches finden Sie im folgenden Handbuch: "[Cisco Nexus 9336C-FX2 – Installations- und Upgrade-Leitfaden](#)".

Komponenten und Teilenummern für gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches

Informationen zur Installation und Wartung von Cisco Nexus 9336C-FX2 Switches finden Sie in der Liste der Komponenten und Teilenummern.

In der folgenden Tabelle sind die Teilenummer und Beschreibung für den Switch 9336C-FX2, die Lüfter und die Netzteile aufgeführt:

Teilenummer	Beschreibung
X190200-CS-PE	N9K-9336C-FX2, CS, PTSX, 36PT10/25/40/100GQSFP28
X190200-CS-PI	N9K-9336C-FX2, CS, PSIN, 36PT10/25/40/100GQSFP28
X190002	Zubehörkit X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W Netzteil – Luftstrom am Port Side

Teilenummer	Beschreibung
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W Netzteil – Luftstrom für den seitlichen Ansauganschluss
X-NXA-LÜFTER-65CFM-PE	N9K-9336C 65 CFM, Luftstrom nach Anschlussseite
X-NXA-LÜFTER-65CFM-PI	N9K-9336C 65 CFM, Luftstrom zur Ansaugöffnung an der Seite des Ports

Dokumentationsanforderungen für Cisco Nexus 9336C-FX2 Shared-Switches

Überprüfen Sie bei der Installation und Wartung des Cisco Nexus 9336C-FX2 Switches spezielle Switch- und Controller-Dokumentation, um Ihre Cisco 9336-FX2-Switches und das ONTAP-Cluster einzurichten.

Informationen zum Einrichten der gemeinsamen Cisco Nexus 9336C-FX2-Switches finden Sie im ["Switches Der Cisco Nexus 9000-Serie Unterstützen"](#) Seite.

Dokumenttitel	Beschreibung
"Hardware-Installationsleitfaden Der Nexus 9000-Serie"	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
"Cisco Nexus 9000-Serie Switch – Software-Konfigurationsleitfaden" (Im Leitfaden für die auf den Switches installierte NX-OS Version finden)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.
"Cisco Nexus 9000 Serie NX-OS Software-Upgrade und Downgrade Guide" (Im Leitfaden für die auf den Switches installierte NX-OS Version finden)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
"Cisco Nexus 9000-Serie NX-OS Command Reference Master Index"	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
"Cisco Nexus 9000 MIBs Referenz"	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 9000-Switches.
"Nachrichtenreferenz für das NX-OS-System der Serie Nexus 9000"	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.
"Versionshinweise für die Cisco Nexus 9000-Serie NX-OS" (Wählen Sie die Hinweise für die NX-OS Version, die auf Ihren Switches installiert ist.)	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
"Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie"	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

Hardware installieren

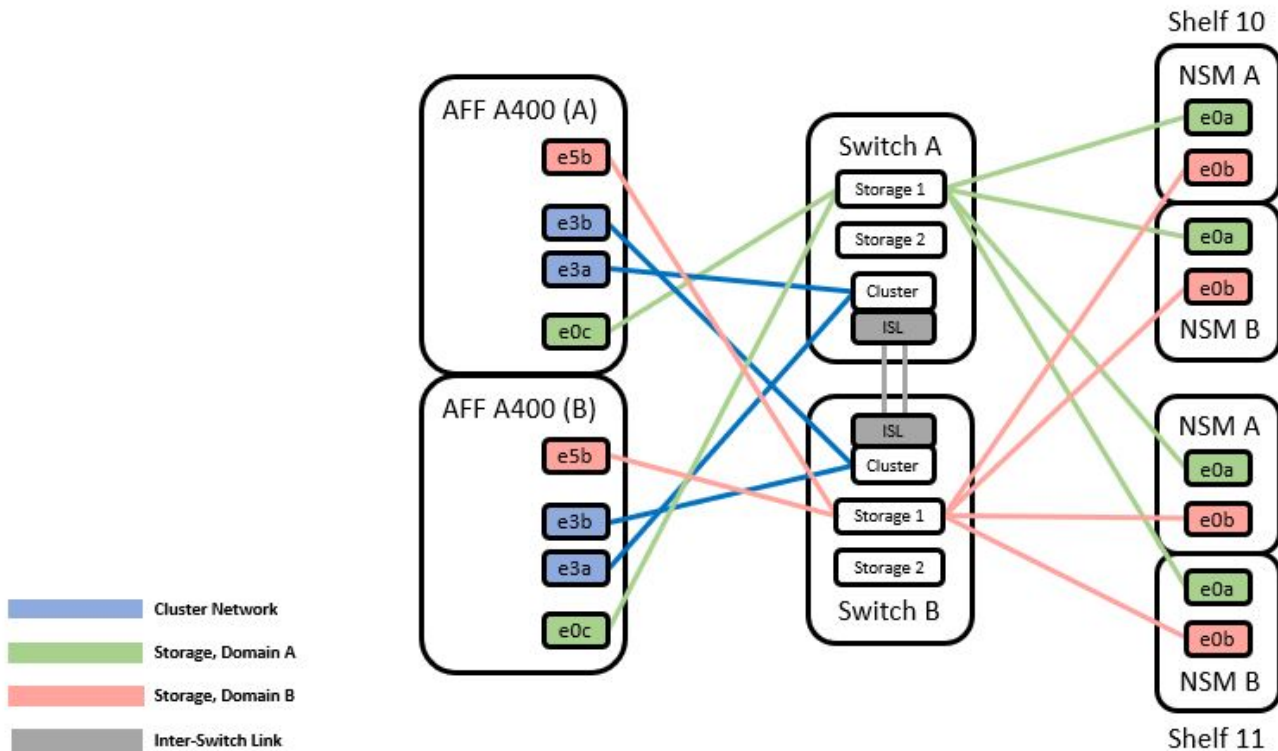
Füllen Sie das Cisco Nexus 9336C-FX2-Verkabelungsarbeitsblatt aus

Verwenden Sie die folgenden Verkabelungsabbilder, um die Verkabelung zwischen den Controllern und den Switches abzuschließen.

Kabel NS224 Speicher als Switch-Attached

Wenn Sie NS224-Speicher als Switch-Attached verkabeln möchten, folgen Sie dem Schaltplan:

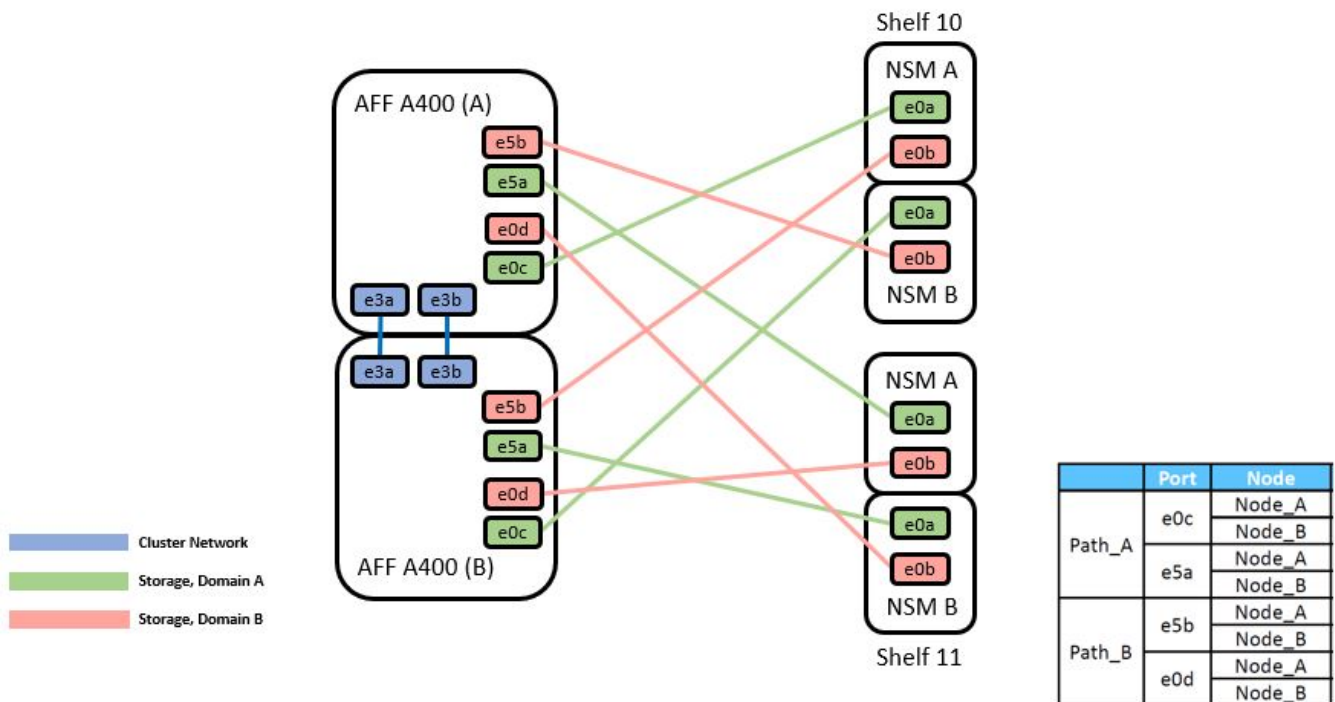
Switch Attached



Siehe "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

Kabel-NS224-Speicher als Direct-Attached

Wenn Sie NS224-Speicher als Direct-Attached anstatt die Shared Switch-Speicherports verkabeln möchten, folgen Sie dem direkt angeschlossenen Diagramm:



Siehe "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

Cisco Nexus 9336C-FX2 – Verkabelungsarbeitsblatt

Wenn Sie die unterstützten Plattformen dokumentieren möchten, müssen Sie das leere Verkabelungsarbeitsblatt ausfüllen, indem Sie als Anleitung ein ausgefülltes Beispiel-Verkabelungsarbeitsblatt verwenden.

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Switch A			Switch B		
Switch Port	Port Role	Port Usage	Switch Port	Port Role	Port Usage
1	Cluster	40/100GbE	1	Cluster	40/100GbE
2	Cluster	40/100GbE	2	Cluster	40/100GbE
3	Cluster	40/100GbE	3	Cluster	40/100GbE
4	Cluster	40/100GbE	4	Cluster	40/100GbE
5	Cluster	40/100GbE	5	Cluster	40/100GbE
6	Cluster	40/100GbE	6	Cluster	40/100GbE
7	Cluster	40/100GbE	7	Cluster	40/100GbE
8	Cluster	40/100GbE	8	Cluster	40/100GbE
9	Cluster	40GbE w/4x10GbE b/o	9	Cluster	40GbE w/4x10GbE b/o
10	Cluster	100GbE w/4x25GbE b/o	10	Cluster	100GbE w/4x25GbE b/o
11	Storage	100GbE	11	Storage	100GbE
12	Storage	100GbE	12	Storage	100GbE
13	Storage	100GbE	13	Storage	100GbE
14	Storage	100GbE	14	Storage	100GbE
15	Storage	100GbE	15	Storage	100GbE
16	Storage	100GbE	16	Storage	100GbE
17	Storage	100GbE	17	Storage	100GbE
18	Storage	100GbE	18	Storage	100GbE
19	Storage	100GbE	19	Storage	100GbE
20	Storage	100GbE	20	Storage	100GbE
21	Storage	100GbE	21	Storage	100GbE
22	Storage	100GbE	22	Storage	100GbE
23	Storage	100GbE	23	Storage	100GbE
24	Storage	100GbE	24	Storage	100GbE
25	Storage	100GbE	25	Storage	100GbE
26	Storage	100GbE	26	Storage	100GbE
27	Storage	100GbE	27	Storage	100GbE
28	Storage	100GbE	28	Storage	100GbE
29	Storage	100GbE	29	Storage	100GbE
30	Storage	100GbE	30	Storage	100GbE
31	Storage	100GbE	31	Storage	100GbE
32	Storage	100GbE	32	Storage	100GbE
33	Storage	100GbE	33	Storage	100GbE
34	Storage	100GbE	34	Storage	100GbE
35	ISL	100GbE	35	ISL	100GbE
36	ISL	100GbE	36	ISL	100GbE

Wo?

- 100-GB-ISL für Switch A-Port 35
- 100-GB-ISL für Switch A-Port 36
- 100-GB-ISL zu Switch B-Port 35
- 100-GB-ISL zu Switch B-Port 36

Leeres Verkabelungsarbeitsblatt

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Die Tabelle der unterstützten Cluster-Verbindungen der Hardware Universe definiert die von der Plattform verwendeten Cluster-Ports.

Switch Port	Switch A Port Role	Port Usage	Switch Port	Switch B Port Role	Port Usage
1			1		
2			2		
3			3		
4			4		
5			5		
6			6		
7			7		
8			8		
9			9		
10			10		
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			25		
26			26		
27			27		
28			28		
29			29		
30			30		
31			31		
32			32		
33			33		
34			34		
35			35		
36			36		

Wo?

- 100-GB-ISL für Switch A-Port 35
- 100-GB-ISL für Switch A-Port 36
- 100-GB-ISL zu Switch B-Port 35
- 100-GB-ISL zu Switch B-Port 36

Installieren Sie gemeinsam genutzte Cisco Nexus 9336C-FX2 Switches

Befolgen Sie diese Anweisungen, um gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches zu konfigurieren.

Was Sie benötigen

- Erforderliche Dokumentation für gemeinsamen Switch, Controller-Dokumentation und ONTAP-Dokumentation Siehe "[Dokumentationsanforderungen für Cisco Nexus 9336C-FX2 Shared-Switches](#)" Und "[NetApp ONTAP-Dokumentation](#)".
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossene Verkabelungsarbeitsblätter. Siehe "[Füllen Sie das Cisco Nexus 9336C-FX2-Verkabelungsarbeitsblatt aus](#)". Weitere Informationen zur Verkabelung finden Sie im "[Hardware Universe](#)".

Schritte

1. Racks für Switches, Controller und NS224 NVMe Storage-Shelfs

Siehe "[Anweisungen zum Rack](#)" Erfahren Sie, wie Sie den Switch in einem NetApp Rack unterbringen.

2. Schalten Sie die Switches, Controller und NS224 NVMe Storage-Shelfs ein.

Was kommt als Nächstes?

Gehen Sie zu "[Konfigurieren Sie den gemeinsamen Cisco Nexus 9336C-FX2 Switch](#)".

Konfigurieren Sie gemeinsam genutzte Cisco Nexus 9336C-FX2 Switches

Befolgen Sie diese Anweisungen, um gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches zu konfigurieren.

Was Sie benötigen

- Erforderliche Dokumentation für gemeinsamen Switch, Controller-Dokumentation und ONTAP-Dokumentation Siehe "[Dokumentationsanforderungen für Cisco Nexus 9336C-FX2 Shared-Switches](#)" Und "[NetApp ONTAP-Dokumentation](#)".
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossene Verkabelungsarbeitsblätter. Siehe "[Füllen Sie das Cisco Nexus 9336C-FX2-Verkabelungsarbeitsblatt aus](#)". Weitere Informationen zur Verkabelung finden Sie im "[Hardware Universe](#)".

Schritte

1. eine Erstkonfiguration der Switches durchführen.

Für die Konfiguration benötigen Sie die entsprechende Anzahl und Art von Kabeln und Kabelanschlüssen für Ihre Switches.

Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

2. Starten Sie den Switch.

Geben Sie beim ersten Booten des Switches die entsprechenden Antworten auf die folgenden Einrichtungsfragen an.

Die Sicherheitsrichtlinie Ihres Standorts definiert die zu erstellenden Antworten und Services.

- a. Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)

Antworten Sie mit **ja**. Der Standardwert ist Nein

b. Wollen Sie den sicheren Kennwortstandard durchsetzen? (ja/nein)

Antworten Sie mit **ja**. Die Standardeinstellung ist ja.

c. Geben Sie das Passwort für den Administrator ein.

Das Standardpasswort lautet admin. Sie müssen ein neues, starkes Passwort erstellen.

Ein schwaches Kennwort kann abgelehnt werden.

d. Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)

Reagieren Sie mit **ja** bei der Erstkonfiguration des Schalters.

e. Noch ein Login-Konto erstellen? (ja/nein)

Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen.
Der Standardwert ist Nein

f. Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)

Antworten Sie mit **Nein**. Der Standardwert ist Nein

g. Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)

Antworten Sie mit **Nein**. Der Standardwert ist Nein

h. Geben Sie den Switch-Namen ein.

Der Switch-Name ist auf 63 alphanumerische Zeichen begrenzt.

i. Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)

Beantworten Sie mit **ja** (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein

j. Standard-Gateway konfigurieren? (ja/nein)

Antworten Sie mit **ja**. Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.

k. Erweiterte IP-Optionen konfigurieren? (ja/nein)

Antworten Sie mit **Nein**. Der Standardwert ist Nein

l. Telnet-Dienst aktivieren? (ja/nein)

Antworten Sie mit **Nein**. Der Standardwert ist Nein

m. SSH-Dienst aktivieren? (ja/nein)

Antworten Sie mit **ja**. Die Standardeinstellung ist ja.



SSH wird empfohlen, wenn Sie Cluster Switch Health Monitor (CSHM) für seine Protokollerfassung verwenden. SSHv2 wird auch für erhöhte Sicherheit empfohlen.

- a. Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1). Die Standardeinstellung ist rsa.
- b. Geben Sie die Anzahl der Schlüsselbits ein (1024- 2048).
- c. Konfigurieren Sie den NTP-Server? (ja/nein)

Antworten Sie mit **Nein**. Der Standardwert ist Nein

- d. Standard-Schnittstellenebene konfigurieren (L3/L2):

Antworten Sie mit **L2**. Der Standardwert ist L2.

- e. Konfigurieren Sie den Status der Switch-Schnittstelle (shut/noshut) als Standard-Switch-Port:

Antworten Sie mit **noshut**. Die Standardeinstellung ist noshut.

- f. Konfiguration des CoPP-Systemprofils (streng/mittel/lenient/dense):

Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.

- g. Möchten Sie die Konfiguration bearbeiten? (ja/nein)

Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, beantworten Sie mit Nein. Beantworten Sie mit **ja**, wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.

- h. Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)

Antworten Sie mit **ja**, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert.

3. Überprüfen Sie die Konfigurationseinstellungen, die Sie am Ende der Einrichtung in der Anzeige vorgenommen haben, und stellen Sie sicher, dass Sie die Konfiguration speichern.



Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam.

4. Überprüfen Sie die Version der Cluster-Netzwerk-Switches und laden Sie bei Bedarf die von NetApp unterstützte Version der Software von auf die Switches von herunter "[Cisco Software-Download](#)" Seite.

Was kommt als Nächstes?

Je nach Konfiguration können Sie dies tun "[Switch in NetApp-Schrank einbauen](#)". Andernfalls fahren Sie mit fort "[Bereiten Sie sich auf die Installation von NX-OS und RCF vor](#)".

Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack

Je nach Konfiguration müssen Sie möglicherweise den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Tafel in einem NetApp Rack installieren. Standardhalterungen sind im Lieferumfang des Schalters enthalten.

Was Sie benötigen

- Für jeden Switch müssen Sie die acht 10-32- oder 12-24-Schrauben und Muttern bereitstellen, um die Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten zu befestigen.

- Sie müssen den Cisco Standard-Schienensatz verwenden, um den Switch in einem NetApp Rack zu installieren.



Die Jumper-Kabel sind nicht im Lieferumfang des Pass-Through-Kits enthalten und sollten in Ihrem Switch enthalten sein. Wenn die Switches nicht im Lieferumfang enthalten sind, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

Erforderliche Dokumentation

Lesen Sie die anfänglichen Vorbereitungsanforderungen, den Inhalt des Kits und die Sicherheitsvorkehrungen im ["Hardware-Installationsleitfaden Der Cisco Nexus 9000-Serie"](#).

Schritte

1. Die Pass-Through-Blindplatte in den NetApp-Schrank einbauen.

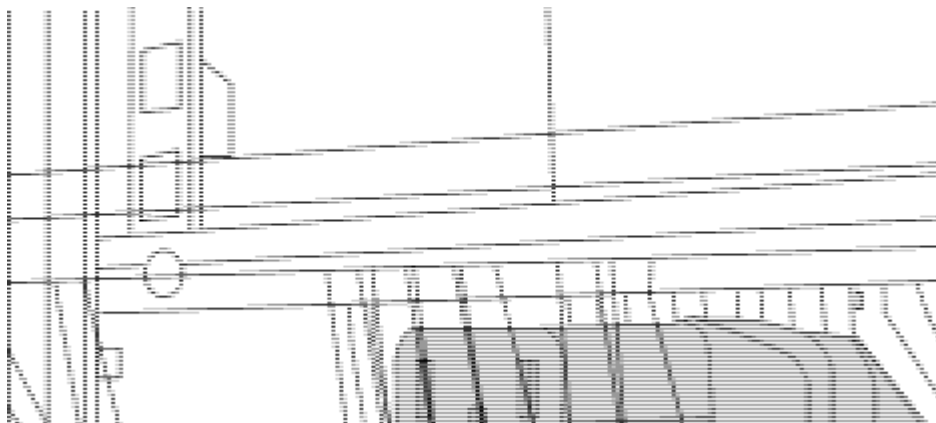
Die Pass-Through-Panel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

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

- Ein Durchlauf-Blindblech
- Vier 10-32 x 0,75 Schrauben
- Vier 10-32-Clip-Muttern
 - i. Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

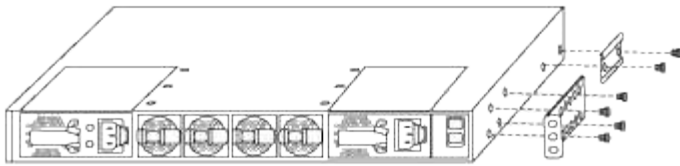
Bei diesem Verfahren wird die Blindplatte in U40 installiert.

- ii. Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
- iii. Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
- iv. Stecken Sie die Buchsen der beiden 48-Zoll-Jumper-Kabel von der Rückseite der Abdeckung und durch die Bürstenbaugruppe.

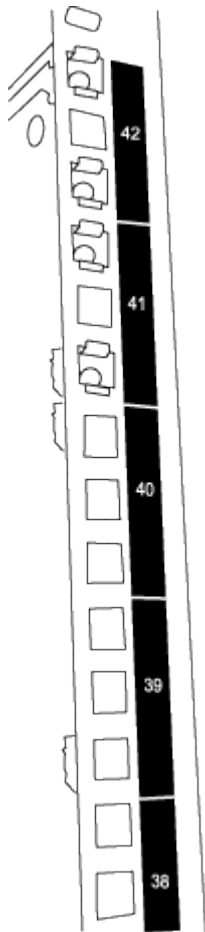


(1) *Buchsenleiste des Überbrückungskabels.*

2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Gehäuse des Nexus 9336C-FX2.
 - a. Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.

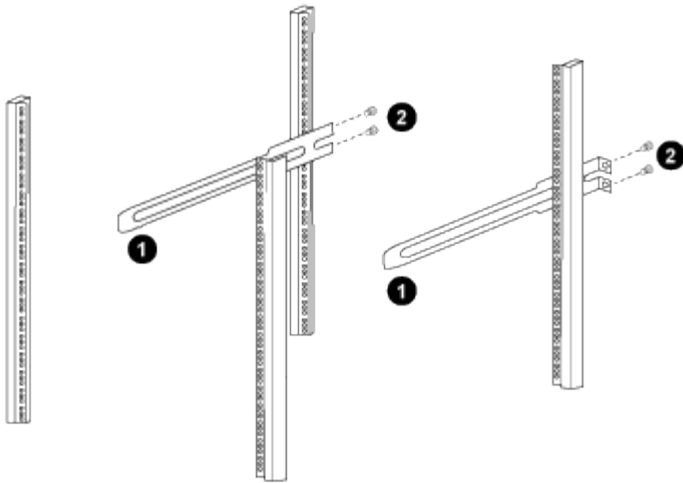


- b. Wiederholen Sie den Schritt [2 a](#) Mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
 - c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.
 - d. Wiederholen Sie den Schritt [2c](#) Mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite des Schalters.
3. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



Die beiden 9336C-FX2 Schalter werden immer in der oberen 2 HE des Schrankes RU41 und 42 montiert.

4. Installieren Sie die Gleitschienen im Schrank.
 - a. Positionieren Sie die erste Gleitschiene an der RU42-Markierung auf der Rückseite des hinteren linken Pfosten, legen Sie die Schrauben mit dem entsprechenden Gewindetyp ein und ziehen Sie die Schrauben mit den Fingern fest.



(1) beim sanften Schieben der Gleitschiene richten Sie sie an den Schraubenbohrungen im Rack aus.

(2) Schrauben der Gleitschienen an den Schrankleisten festziehen.

a. Wiederholen Sie den Schritt 4 a Für den hinteren Pfosten auf der rechten Seite.

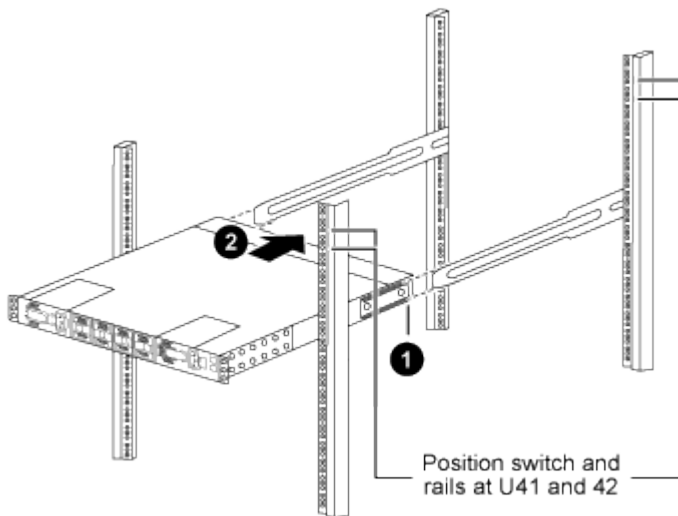
b. Wiederholen Sie die Schritte 4 a Und 4b An den RU41 Standorten auf dem Schrank.

5. Den Schalter in den Schrank einbauen.



Für diesen Schritt sind zwei Personen erforderlich: Eine Person muss den Schalter von vorne und von der anderen in die hinteren Gleitschienen führen.

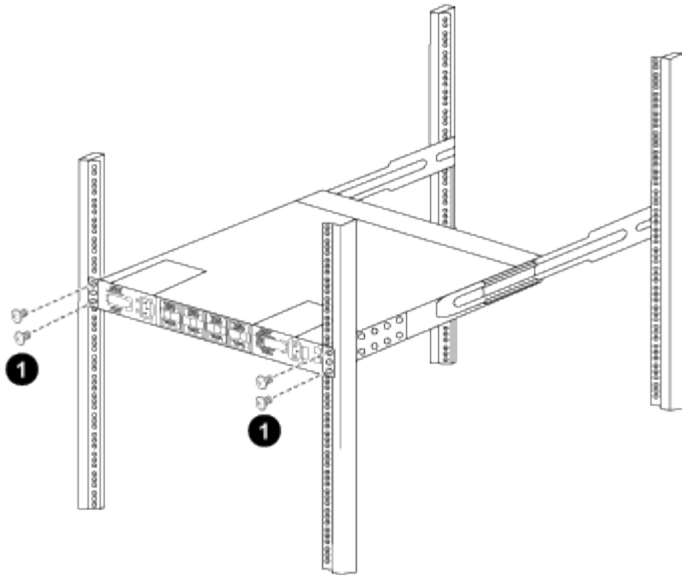
a. Positionieren Sie die Rückseite des Schalters an RU41.



(1) Da das Gehäuse in Richtung der hinteren Pfosten geschoben wird, richten Sie die beiden hinteren Rackmontageführungen an den Gleitschienen aus.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Halterungen der Rackmontage bündig mit den vorderen Pfosten sind.

b. Befestigen Sie den Schalter am Gehäuse.



(1) mit einer Person, die die Vorderseite des Chassis hält, sollte die andere Person die vier hinteren Schrauben vollständig an den Schrankpfosten festziehen.

- a. Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- b. Wiederholen Sie die Schritte [5a](#) Bis [5c](#) Für den zweiten Schalter an der RU42-Position.



Durch die Verwendung des vollständig installierten Schalters als Unterstützung ist es nicht erforderlich, während des Installationsvorgangs die Vorderseite des zweiten Schalters zu halten.

6. Wenn die Switches installiert sind, verbinden Sie die Jumper-Kabel mit den Switch-Netzeinkabeln.
7. Verbinden Sie die Stecker beider Überbrückungskabel mit den am nächsten verfügbaren PDU-Steckdosen.



Um Redundanz zu erhalten, müssen die beiden Kabel mit verschiedenen PDUs verbunden werden.

8. Verbinden Sie den Management Port an jedem 9336C-FX2 Switch mit einem der Management-Switches (falls bestellt) oder verbinden Sie sie direkt mit dem Management-Netzwerk.

Der Management-Port ist der oben rechts gelegene Port auf der PSU-Seite des Switch. Das CAT6-Kabel für jeden Switch muss über die Passthrough-Leiste geführt werden, nachdem die Switches zur Verbindung mit den Management-Switches oder dem Management-Netzwerk installiert wurden.

Software konfigurieren

Workflow für die Softwareinstallation für gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches

So installieren und konfigurieren Sie Software für einen Cisco Nexus 9336C-FX2 Switch:

1. ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).
2. ["Installieren Sie die NX-OS-Software"](#).

3. "Installieren Sie das RCF".

Installieren Sie den RCF, nachdem Sie den Nexus 9336C-FX2-Schalter zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor

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

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01 und cluster1-02.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1 und cluster1-01_clus2 für cluster1-01 und cluster1-02_clusions1 und cluster1-02_clus2 für cluster1-02.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=x h`

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

Beispiel anzeigen

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
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. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

```
`network port show -ip space Cluster`
```

Beispiel anzeigen

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

```
Node: cluster1-02
```

Health					Speed (Mbps)	
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
```

Health					Speed (Mbps)	
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. Zeigt Informationen zu den LIFs an:

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

Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
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. Ping für die Remote-Cluster-LIFs:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node cluster1-02
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)
```

6. Vergewissern Sie sich, dass der automatische Zurücksetzen-Befehl 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
```

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

4 entries were displayed.

7. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password Und system switch ethernet log enable-collection
```


Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

8. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

system cluster-switch log setup-password **Und** system cluster-switch log enable-collection

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Was kommt als Nächstes?

["Installieren Sie die NX-OS-Software"](#).

Installieren Sie die NX-OS-Software

Gehen Sie folgendermaßen vor, um die NX-OS-Software auf dem gemeinsamen Switch Nexus 9336C-FX2 zu installieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- ["Cisco Ethernet Switch Seite"](#). In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.
- Entsprechende Leitfäden für Software und Upgrades auf der Cisco Website für die Upgrade- und Downgrade-Verfahren von Cisco Switches. Siehe ["Switches Der Cisco Nexus 9000-Serie"](#).

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clusions1, cluster1-02_clus2 , cluster1-03_clug1, Cluster1-03_clus2, cluster1-04_clut1, und cluster1-04_clus2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Installieren Sie die Software

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Überprüfen Sie mit dem Ping-Befehl die Verbindung zum Server, der die NX-OS-Software und die RCF hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

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

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

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

Beispiel anzeigen

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

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

cs2# copy sftp: bootflash: vrf management

Enter source filename: /code/n9000-epld.9.3.5.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

4. 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#
```

5. Installieren Sie das NX-OS Image.

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

Beispiel anzeigen

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

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

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

```
Verifying image type.  
[#####] 100% -- SUCCESS
```

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

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

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

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

Compatibility check is done:

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

Images will be upgraded according to following table:

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


```
Switch will be reloaded for disruptive upgrade.

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

Install is in progress, please wait.

Performing runtime checks.
[#####] 100% -- SUCCESS

Setting boot variables.
[#####] 100% -- SUCCESS

Performing configuration copy.
[#####] 100% -- SUCCESS

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

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

6. 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):
```

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen



```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	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.

8. Melden Sie sich nach dem Neustart des Switches erneut an, und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

9. Wiederholen Sie die Schritte 1 bis 8, um die NX-OS-Software auf Switch cs1 zu installieren.

Was kommt als Nächstes?

["Installieren Sie die RCF-Konfigurationsdatei"](#)

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können den RCF nach dem ersten Einrichten des Nexus 9336C-FX2-Schalters installieren. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Bevor Sie beginnen, führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle RCF-Datei.
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.

Vorgeschlagene Dokumentation

- ["Cisco Ethernet Switch Seite"](#) In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie das RCF

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches sind cs1 und cs2.
- Die Node-Namen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen sind Cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clusions1, cluster1-02_clus2, cluster1-03_clug1, Cluster1-03_clus2, cluster1-04_clut1, und cluster1-04_clus2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster Interconnect-Ports e0a und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein. Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritt 1: Vorbereitung für die Installation

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
cluster1-01/cdp
              e0a    cs1                      Ethernet1/7      N9K-
C9336C
              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 Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports **up** mit einem gesunden Status sind:

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


Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
Home				

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

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

```
cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                                     Type                Address
Model
-----
-----
cs1                                     cluster-network     10.233.205.90      N9K-
C9336C
    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. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

Schritt 2: Ports konfigurieren

1. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

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

2. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

Beispiel anzeigen

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

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

```
show running-config
```

5. Reinigen Sie die Konfiguration am Schalter cs2, und führen Sie eine grundlegende Einrichtung durch.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload

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

6. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

```
cs2# 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)...
```

7. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt Installation auf Schalter cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

8. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

Beispiel anzeigen

```
cs2# 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
*
*****
*****
```

9. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```


Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

10. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

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

11. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

12. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß 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.

- a. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

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 können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
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. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels verwendet:

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

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

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

```
cluster show
```

Beispiel anzeigen

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

16. Wiederholen Sie die Schritte 4 bis 11 am Schalter cs1.
17. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

18. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

Schritt 3: Überprüfen Sie die Konfiguration

1. Stellen Sie sicher, dass die mit den Cluster-Ports verbundenen Switch-Ports **up** sind.

```
show interface brief
```

Beispiel anzeigen

```
cs1# show interface brief | grep up
.
.
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 Nodes weiterhin 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
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
```


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

```
show vlan brief
```

```
show interface trunk
```

Beispiel anzeigen

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, 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

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
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	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	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
..
..
..
..
..
```



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

4. Stellen Sie sicher, dass die ISL 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      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	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::*>				

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

```
cluster show
```

Beispiel anzeigen

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

7. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

```
cluster ping-cluster -node local
```


Beispiel anzeigen

```
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)
```

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

+

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung mit dem Cluster-Switch 9336C-FX2 * CLI* eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im

vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*> system switch ethernet log modify -device cs2 -log
-request true

Do you want to modify the cluster switch log collection
configuration? {y|n}: [n] y

Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.

ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.
Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 9336C-FX2-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config)# show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv

```
(sw1) (Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Switches migrieren

Migrieren Sie von einem Cluster ohne Switches mit Direct-Attached Storage

Sie können von einem Cluster ohne Switches mit Direct-Attached Storage durch Hinzufügen von zwei neuen Shared-Switches migrieren.

Die von Ihnen verwendete Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerk-Ports oder einen einzelnen Cluster-Port haben. Der dokumentierte Prozess funktioniert für alle Nodes mit optischen oder Twinax-Ports, wird auf diesem Switch jedoch nicht unterstützt, wenn die Nodes für die Cluster-Netzwerk-Ports integrierte 10-Gbit-BASE-T RJ45-Ports verwenden.

Die meisten Systeme benötigen an jedem Controller zwei dedizierte Cluster-Netzwerk-Ports. Siehe "[Cisco Ethernet-Switches](#)" Finden Sie weitere Informationen.

Falls Sie eine bestehende Cluster-Umgebung mit zwei Nodes ohne Switches nutzen, können Sie mit Cisco Nexus 9336C-FX2 Switches zu einer Switch-basierten Cluster-Umgebung mit zwei Nodes migrieren. So können Sie auf mehr als zwei Nodes im Cluster skalieren.

Prüfen Sie die Anforderungen

Stellen Sie sicher, dass:

- Bei der Konfiguration mit zwei Nodes ohne Switches:
 - Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
 - Auf den Knoten wird ONTAP 9.8 und höher ausgeführt.
 - Alle Cluster-Ports haben den Status **up**.
 - Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren **Home**-Ports.
- Für die Switch-Konfiguration des Cisco Nexus 9336C-FX2:
 - Beide Switches verfügen über Management-Netzwerk-Konnektivität.
 - Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
 - Bei den Nexus 9336C-FX2 Nodes-zu-Node-Switches und Switch-zu-Switch-Verbindungen werden Twinax- oder Glasfaserkabel verwendet.
 - Das NetApp "[Hardware Universe](#)" Enthält weitere Informationen zur Verkabelung.
 - Inter-Switch Link (ISL)-Kabel werden an den Anschlüssen 1/35 und 1/36 an beiden 9336C-FX2-Switches angeschlossen.
- Die Erstanpassung der Switches 9336C-FX2 ist abgeschlossen. So werden die:
 - 9336C-FX2-Switches führen die neueste Version der Software aus
 - Auf die Switches wurden Referenzkonfigurationsdateien (RCFs) angewendet
 - Auf den neuen Switches werden alle Site-Anpassungen wie SMTP, SNMP und SSH konfiguriert.

Migrieren Sie die Switches

Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der Schalter 9336C-FX2 lauten *cs1* und *cs2*.
- Die Namen der Cluster SVMs sind *node1* und *node2*.
- Die Namen der LIFs sind *_node1_clus1_* und *node1_clus2* auf Knoten 1, und *node2_clus1* und *node2_clus2* auf Knoten 2.
- Die Eingabeaufforderung des Cluster1::*> gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports lauten *e3a* und *e3b* gemäß AFF A400-Controller. Der "[Hardware Universe](#)" Enthält die neuesten Informationen über die tatsächlichen Cluster-Ports für Ihre Plattformen.

Schritt 1: Migration von einem Cluster ohne Switches mit Direct-Attached Storage

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=xh`.

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

1. Ändern Sie die Berechtigungsebene in Erweitert, geben Sie y ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

2. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches cs1 und cs2. Sie dürfen die ISL-Ports nicht deaktivieren.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 34 auf Switch cs1 deaktiviert sind:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# shutdown
```

3. Überprüfen Sie, ob die ISL und die physischen Ports auf der ISL zwischen den beiden 9336C-FX2-Switches cs1 und cs2 auf den Ports 1/35 und 1/36 stehen:

```
show port-channel summary
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports auf 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 auf 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)
```

4. Liste der benachbarten Geräte anzeigen:

```
show cdp neighbors
```

Dieser Befehl enthält Informationen zu den Geräten, die mit dem System verbunden sind.

Beispiel anzeigen

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs1 aufgeführt:

```
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
```

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs2 aufgeführt:

```
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
```

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

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

Jeder Port sollte für „Link“ und „OK“ für den Integritätsstatus angezeigt werden.

Beispiel anzeigen

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

Node: node1

Health					Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy						
e3b	Cluster	Cluster		up	9000	auto/100000
healthy						

Node: node2

Health					Speed (Mbps)	
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status						
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy						
e3b	Cluster	Cluster		up	9000	auto/100000
healthy						

4 entries were displayed.

6. Überprüfung, ob alle Cluster-LIFs betriebsbereit sind:

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

Jede LIF im Cluster sollte für „true“ anzeigen Is Home Und haben einen Status Admin/Oper von up/up.

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			

4 entries were displayed.

7. Überprüfung, ob die automatische Umrüstung 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		
	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

8. Trennen Sie das Kabel vom Cluster-Port e3a auf node1, und verbinden sie dann e3a mit Port 1 am Cluster-Switch cs1. Verwenden Sie dabei die geeignete Verkabelung, die von den Switches 9336C-FX2 unterstützt wird.

Das NetApp "[Hardware Universe](#)" Enthält weitere Informationen zur Verkabelung.

9. Trennen Sie das Kabel vom Cluster-Port e3a auf node2, und verbinden sie dann e3a mit Port 2 am Cluster-Switch cs1. Verwenden Sie dazu die geeignete Verkabelung, die von den Switches 9336C-FX2 unterstützt wird.
10. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/34 auf Switch cs1 aktiviert sind:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-34
cs1(config-if-range)# no shutdown
```

11. [[step 12]]Überprüfen Sie, ob alle Cluster-LIFs **up**, betriebsbereit und als wahr angezeigt werden Is Home:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs **up** auf node1 und node2 sind und dass Is Home Die Ergebnisse sind **wahr**:

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

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
Cluster				
true	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

4 entries were displayed.

12. Informationen zum Status der Knoten im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      false
node2          true   true      false
2 entries were displayed.
```

13. Trennen Sie das Kabel vom Cluster-Port e3b auf node1, und verbinden sie dann e3b mit Port 1 am Cluster-Switch cs2. Verwenden Sie dazu die entsprechende Verkabelung, die von den Switches 9336C-FX2 unterstützt wird.
14. Trennen Sie das Kabel vom Cluster-Port e3b auf node2, und verbinden sie dann e3b mit Port 2 am Cluster-Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den Switches 9336C-FX2 unterstützt wird.
15. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs2.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/34 auf Switch cs2 aktiviert sind:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-34
cs2(config-if-range)# no shutdown
```

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

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


Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

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

Node: node1

Ignore

Health	Health				Speed (Mbps)	
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

Health	Health				Speed (Mbps)	
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 entries were displayed.

17. Überprüfen Sie, ob alle Schnittstellen für wahr angezeigt werden Is Home:

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



Dies kann einige Minuten dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs **up** auf node1 und node2 sind und dass Is Home Die Ergebnisse sind wahr:

```
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					

4 entries were displayed.

18. 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 Switches:

```
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              AFFA400
e3a
node2          Eth1/2      133    H              AFFA400
e3a
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              AFFA400
e3b
node2          Eth1/2      133    H              AFFA400
e3b
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
```

19. Informationen über die erkannten Netzwerkgeräte in Ihrem Cluster 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
           e3a    cs1                      0/2          N9K-
C9336C
           e3b    cs2                      0/2          N9K-
C9336C
node1      /cdp
           e3a    cs1                      0/1          N9K-
C9336C
           e3b    cs2                      0/1          N9K-
C9336C
4 entries were displayed.
```

20. Überprüfen Sie, ob die Speicherkonfiguration von HA-Paar 1 (und HA-Paar 2) korrekt und fehlerfrei ist:

```
system switch ethernet show
```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                               Address
Model
-----
sh1
                                     storage-network                     172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                9.3(5)
    Version Source: CDP
sh2
                                     storage-network                     172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    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.
storage::*>
```

21. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

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



Es kann einige Minuten dauern, bis der Befehl abgeschlossen ist. Warten Sie, bis die Ankündigung „3-Minuten-Lebensdauer abläuft“ abläuft.

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

Beispiel anzeigen

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

22. Überprüfen Sie den Status der Knotenmitglieder im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

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

23. Stellen Sie sicher, dass das Clusternetzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node node2
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 169.254.47.194 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)
```

24. Ändern Sie die Berechtigungsebene zurück in admin:

```
set -privilege admin
```

25. Aktivieren Sie die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung mithilfe der Befehle, um Switch-bezogene Protokolldateien zu erfassen:

- ° system switch ethernet log setup-password
- ° system switch ethernet log enable-collection

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.

Choose from the following list:
cs1
cs2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster? {y|n}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```

Schritt 2: Richten Sie den gemeinsamen Schalter ein

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden gemeinsamen Schalter sind *sh1* und *sh2*.
- Die Knoten sind *node1* und *node2*.



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

1. Überprüfen Sie, ob die Storage-Konfiguration von HA-Paar 1 (und HA-Paar 2) richtig und fehlerfrei ist:

```
system switch ethernet show
```


Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                                     Address
Model
-----
sh1
                                     storage-network                             172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(5)
    Version Source: CDP
sh2
                                     storage-network                             172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    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.
storage::*>
```

2. Vergewissern Sie sich, dass die Storage-Node-Ports ordnungsgemäß und betriebsbereit sind:

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

Beispiel anzeigen

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

VLAN				Speed		
Node	Port	Type	Mode	(Gb/s)	State	Status
ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online

3. Bewegen Sie das HA-Paar 1, den Pfad A des NSM224-Pfads in den Bereich der sh1-Ports 11-22.
4. Installieren Sie ein Kabel von HA-Paar 1, node1, Pfad A zu sh1-Port-Bereich 11-22. Beispiel: Der Pfad Ein Speicherport an einer AFF A400 ist e0c.
5. Installieren Sie ein Kabel von HA-Paar 1, node2, Pfad A zu sh1-Port-Bereich 11-22.
6. Vergewissern Sie sich, dass die Node-Ports ordnungsgemäß und betriebsbereit sind:

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

Beispiel anzeigen

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

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	0	enabled	offline
30	e5a	ENET	storage	0	enabled	offline
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	0	enabled	offline
30	e5a	ENET	storage	0	enabled	offline
30	e5b	ENET	storage	100	enabled	online

7. Vergewissern Sie sich, dass es keine Probleme mit dem Storage Switch oder der Verkabelung beim Cluster gibt:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

8. Verschieben Sie die Anschlüsse für HA-Paar 1 und NSM224 Pfad B in den Bereich der sh2-Ports 11-22.
9. Installieren Sie ein Kabel von HA-Paar 1, node1, Pfad B bis sh2-Port-Bereich 11-22. Beispiel: Der Speicherport Pfad B auf einer AFF A400 ist e5b.
10. Installieren Sie ein Kabel zwischen HA-Paar 1, node2, Pfad B und sh2-Port-Bereich 11-22.

11. Vergewissern Sie sich, dass die Node-Ports ordnungsgemäß und betriebsbereit sind:

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

Beispiel anzeigen

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

VLAN					Speed		
Node	Port	Type	Mode	(Gb/s)	State	Status	
ID							

node1							
30	e0c	ENET	storage	100	enabled	online	
30	e0d	ENET	storage	0	enabled	offline	
30	e5a	ENET	storage	0	enabled	offline	
30	e5b	ENET	storage	100	enabled	online	
node2							
30	e0c	ENET	storage	100	enabled	online	
30	e0d	ENET	storage	0	enabled	offline	
30	e5a	ENET	storage	0	enabled	offline	
30	e5b	ENET	storage	100	enabled	online	

12. Überprüfen Sie, ob die Storage-Konfiguration von HA-Paar 1 korrekt ist und fehlerfrei ist:

```
system switch ethernet show
```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                                     Address
Model
-----
sh1
                                     storage-network                             172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(5)
    Version Source: CDP
sh2
                                     storage-network                             172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    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.
storage::*>
```

13. Konfigurieren Sie die ungenutzten sekundären (Controller) Storage-Ports auf HA-Paar 1 vom Storage bis zum Netzwerk neu. Wenn mehr als eine NS224 direkt angeschlossen war, gibt es Ports, die neu konfiguriert werden sollten.

Beispiel anzeigen

```
storage port modify -node [node name] -port [port name] -mode
network
```

So platzieren Sie Storage-Ports in einer Broadcast-Domäne:

- ° network port broadcast-domain create (Um bei Bedarf eine neue Domäne zu erstellen)

- `network port broadcast-domain add-ports` (Zum Hinzufügen von Ports zu einer vorhandenen Domäne)

14. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Migration von einer Switched-Konfiguration mit Direct-Attached Storage

Sie können von einer Switched-Konfiguration mit Direct-Attached Storage durch Hinzufügen von zwei neuen Shared-Switches migrieren.

Unterstützte Switches

Folgende Switches werden unterstützt:

- Nexus 9336C-FX2
- Nexus 3232C

Die in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen finden sich auf der Seite [Cisco Ethernet Switches](#). Siehe "[Cisco Ethernet Switches](#)".

Verbindungs-Ports

Die Switches verwenden die folgenden Ports, um eine Verbindung zu den Nodes herzustellen:

- Nexus 9336C-FX2:
 - Ports 1 - 3: Breakout-Modus (4X10G) Intra-Cluster-Ports, int e1/1/1-4, e1/2/1-4, e1/3/1-4
 - Ports 4- 6: Breakout-Modus (4X25G) Intra-Cluster/HA-Ports, int e1/4/1-4, e1/5/1-4, e1/6/1-4
 - Ports 7–34: 40 GbE Intra-Cluster/HA-Ports, int e1/7-34
- Nexus 3232C:
 - 1–30 Ports: 10/40/100 GbE
- Bei den Switches werden die folgenden Inter-Switch Link (ISL)-Ports verwendet:
 - Anschlüsse in e1/35-36: Nexus 9336C-FX2
 - Ports e1/31-32: Nexus 3232C

Der "[Hardware Universe](#)" Die enthält Informationen über die unterstützte Verkabelung aller Cluster Switches.

Was Sie benötigen

- Stellen Sie sicher, dass Sie die folgenden Aufgaben ausgeführt haben:
 - Konfiguration einiger Ports auf Nexus 9336C-FX2-Switches für 100 GbE.
 - Geplante, migrierte und dokumentierte 100-GbE-Konnektivität von Nodes zu Nexus 9336C-FX2 Switches.
 - Unterbrechungsfreie Migration anderer Cisco Cluster Switches von einem ONTAP Cluster zu Cisco Nexus 9336C-FX2 Netzwerk-Switches
- Das vorhandene Switch-Netzwerk ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.

- Die Nexus 9336C-FX2 Switches sind unter der entsprechenden Version des installierten NX-OS und angewendete Referenzkonfigurationsdatei (RCF) konfiguriert und betrieben.
- Die vorhandene Netzwerkkonfiguration verfügt über folgende Merkmale:
 - Ein redundantes und voll funktionsfähiges NetApp Cluster unter Verwendung beider älteren Cisco Switches.
 - Management-Konnektivität und Konsolenzugriff auf die älteren Cisco Switches und die neuen Switches.
 - Alle Cluster-LIFs im Status **up** mit den Cluster-LIFs befinden sich auf ihren Home-Ports.
 - ISL-Ports aktiviert und zwischen den anderen Cisco Switches und zwischen den neuen Switches verkabelt.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen Cisco Nexus 3232C Cluster-Switches sind *c1* und *c2*.
- Die neuen Nexus 9336C-FX2 Switches sind *sh1* und *sh2*.
- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node 1_clus1_ und *node1_clus2* und *node2_clus1* bzw. *node2_clus2* auf Knoten 2.
- Schalter c2 wird zuerst durch Schalter sh2 ersetzt und dann wird der Schalter c1 durch den Schalter sh1 ersetzt.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
3. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

Beispiel anzeigen

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

```
Node: node1
```

```
Ignore
```

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Ope	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 entries were displayed.

```
cluster1::*>
```

4. Stellen Sie sicher, dass sich alle Cluster-Schnittstellen (LIFs) auf dem Home-Port befinden:

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


Beispiel anzeigen

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

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
-----	----				
Cluster					
node1_clus1	up/up	169.254.3.4/23	node1	e3a	
true					
node1_clus2	up/up	169.254.3.5/23	node1	e3b	
true					
node2_clus1	up/up	169.254.3.8/23	node2	e3a	
true					
node2_clus2	up/up	169.254.3.9/23	node2	e3b	
true					
4 entries were displayed.					
cluster1::*>					

5. Überprüfen Sie, ob auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

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

Switch	Type	Address	Model
sh1	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			
sh2	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::*>
```

6. Automatische Wiederherstellung auf den Cluster-LIFs deaktiviert.

Beispiel anzeigen

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

7. Schalten Sie den c2-Schalter aus.

Beispiel anzeigen

```
c2# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
c2(config)# interface ethernet <int range>  
c2(config)# shutdown
```

8. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert haben, die auf dem Cluster-Switch sh1 gehostet werden:

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

Dies kann einige Sekunden dauern.

Beispiel anzeigen

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

Current	Logical	Status	Network	Current	
Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
Cluster					
	node1_clus1	up/up	169.254.3.4/23	node1	e3a
true					
	node1_clus2	up/up	169.254.3.5/23	node1	e3a
false					
	node2_clus1	up/up	169.254.3.8/23	node2	e3a
true					
	node2_clus2	up/up	169.254.3.9/23	node2	e3a
false					

4 entries were displayed.
cluster1::*>

9. Schalter c2 durch den neuen Schalter sh2 ersetzen und den neuen Schalter neu verkabeln.
10. Vergewissern Sie sich, dass die Anschlüsse auf sh2 gesichert sind. **Hinweis** dass die LIFs noch auf Switch c1 sind.
11. Schalten Sie den c1-Schalter aus.

Beispiel anzeigen

```
c1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
c1(config)# interface ethernet <int range>
c1(config)# shutdown
```

12. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf Cluster-Switch sh2 gehostet wurden. Dies kann einige Sekunden dauern.

Beispiel anzeigen

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

Is	Logical	Status	Network	Current	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

Cluster					
true	node1_clus1	up/up	169.254.3.4/23	node1	e3a
false	node1_clus2	up/up	169.254.3.5/23	node1	e3a
true	node2_clus1	up/up	169.254.3.8/23	node2	e3a
false	node2_clus2	up/up	169.254.3.9/23	node2	e3a

4 entries were displayed.
cluster1::*>

- Schalter c1 durch den neuen Schalter sh1 ersetzen und den neuen Schalter neu verkabeln.
- Überprüfen Sie, ob die Anschlüsse auf sh1 gesichert sind. **Hinweis** dass sich die LIFs noch auf Schalter c2 befinden.
- Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

Beispiel anzeigen

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

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

```
cluster show
```

Beispiel anzeigen

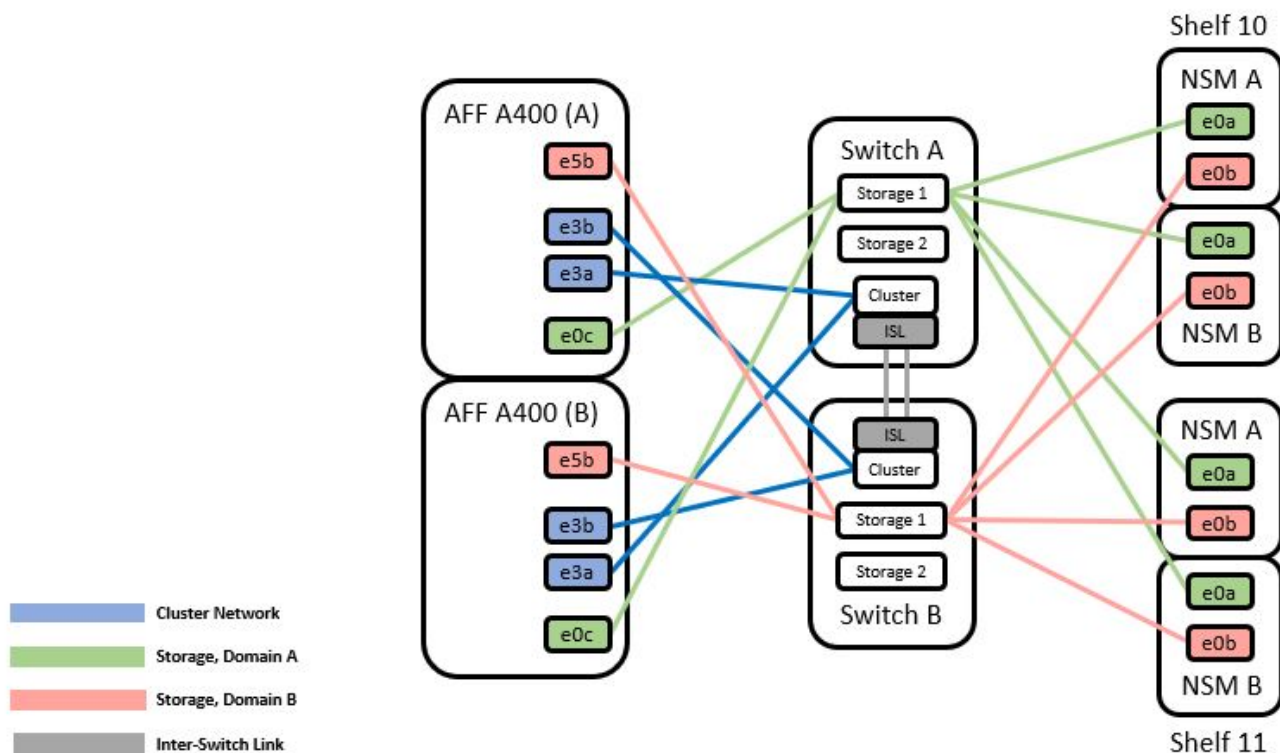
```
cluster1::*> cluster show
Node           Health Eligibility Epsilon
-----
node1          true   true      false
node2          true   true      false
2 entries were displayed.
cluster1::*>
```

Migrieren Sie mit der erneuten Nutzung der Storage-Switches von einer Konfiguration ohne Switches mit Switch-Attached Storage

Sie können die Storage-Switches von einer Konfiguration ohne Switches mit dem Switch-Attached Storage migrieren.

Durch die Wiederverwendung der Storage-Switches werden die Storage Switches von HA-Paar 1 zu den Shared Switches, wie in der folgenden Abbildung dargestellt.

Switch Attached



Schritte

1. Überprüfen Sie, ob die Storage-Konfiguration von HA-Paar 1 (und HA-Paar 2) richtig und fehlerfrei ist:

```
system switch ethernet show
```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                                     Address
Model
-----
sh1
                                     storage-network                             172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: none
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(5)
    Version Source: CDP
sh2
                                     storage-network                             172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    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.
storage::*>
```

2. Überprüfung, ob die Node-Ports ordnungsgemäß und betriebsbereit sind:

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

Beispiel anzeigen

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

Speed

VLAN	Port	Type	Mode	Speed (Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online

3. Verschieben Sie das HA-Paar 1, den Pfad A von NSM2224 vom Storage Switch A zu den gemeinsamen NS224 Storage-Ports für HA-Paar 1, Pfad A auf Storage Switch A
4. Verschieben Sie das Kabel von HA-Paar 1, Node A, Pfad A zu dem gemeinsamen Storage Port für HA-Paar 1, Node A auf Storage Switch A
5. Bewegen Sie das Kabel von HA-Paar 1, Node B, Pfad A zum gemeinsamen Storage Port für HA-Paar 1, Node B auf Storage Switch A
6. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage Switch A in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

7. Ersetzen Sie die Speicher-RCF auf Shared Switch A durch die gemeinsam genutzte RCF-Datei. Siehe ["Installieren Sie das RCF auf einem gemeinsamen Cisco Nexus 9336C-FX2 Switch"](#) Entnehmen.
8. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage-Switch B in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

9.] Verschieben Sie die Kabel HA-Paar 1 und NSM224 Pfad B vom Storage Switch B zu den gemeinsamen NS224 Storage-Ports für HA-Paar 1, Pfad B zum Storage Switch B
10. Bewegen Sie das Kabel von HA-Paar 1, Node A, Pfad B zum gemeinsamen Storage Port für HA-Paar 1, Node A, Pfad B auf Storage Switch B.
11. Bewegen Sie das Kabel von HA-Paar 1, Node B, Pfad B zu dem gemeinsamen Storage Port für HA-Paar 1, Node B, Pfad B auf Storage Switch B
12. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage-Switch B in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

13. [[step 13]] Ersetzen Sie die Speicher-RCF-Datei auf Shared Switch B durch die gemeinsam genutzte RCF-Datei. Siehe ["Installieren Sie das RCF auf einem gemeinsamen Cisco Nexus 9336C-FX2 Switch"](#) Entnehmen.
14. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage-Switch B in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```


Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

15. [[step 15]]ISLs zwischen Shared Switch A und Shared Switch B installieren:

Beispiel anzeigen

```
sh1# configure  
Enter configuration commands, one per line. End with CNTL/Z.  
sh1 (config)# interface e1/35-36  
sh1 (config-if-range)# no lldp transmit  
sh1 (config-if-range)# no lldp receive  
sh1 (config-if-range)# switchport mode trunk  
sh1 (config-if-range)# no spanning-tree bpduguard enable  
sh1 (config-if-range)# channel-group 101 mode active  
sh1 (config-if-range)# exit  
sh1 (config)# interface port-channel 101  
sh1 (config-if)# switchport mode trunk  
sh1 (config-if)# spanning-tree port type network  
sh1 (config-if)# exit  
sh1 (config)# exit
```

16. Konvertieren Sie HA-Paar 1 von einem Cluster ohne Switches zu einem Cluster mit Switches. Verwenden Sie die vom gemeinsamen RCF definierten Cluster-Port-Zuweisungen. Siehe "[Installieren der NX-OS-Software und der Referenzkonfigurationsdateien \(RCFs\)](#)"Entnehmen.
17. Vergewissern Sie sich, dass die Switch-Netzwerkconfiguration gültig ist:

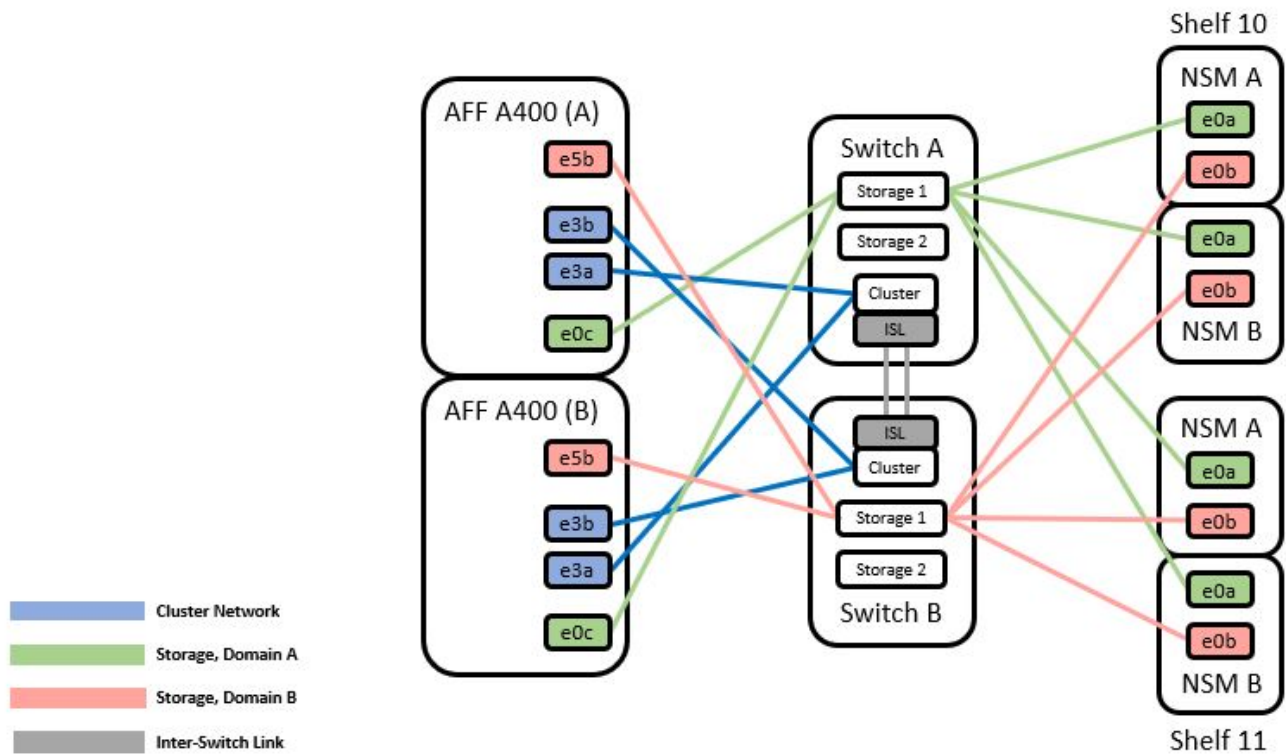
```
network port show
```

Migration von einem Switch-basierten Cluster mit Switch-Attached Storage

Sie können die Storage-Switches von einem Switch-Attached Storage-Cluster mit Switch-Attached Storage migrieren.

Durch die Wiederverwendung der Storage-Switches werden die Storage Switches von HA-Paar 1 zu den Shared Switches, wie in der folgenden Abbildung dargestellt.

Switch Attached



Schritte

1. Überprüfen Sie, ob die Storage-Konfiguration von HA-Paar 1 (und HA-Paar 2) richtig und fehlerfrei ist:

```
system switch ethernet show
```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                               Type                Address             Model
-----
sh1
                                storage-network    172.17.227.5       C9336C

    Serial Number: FOC221206C2
      Is Monitored: true
        Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                        9.3(5)
      Version Source: CDP
sh2
                                storage-network    172.17.227.6       C9336C

    Serial Number: FOC220443LZ
      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.
storage::*>
```

2. HA-Paar 1, NSM224 Pfad-A-Kabel vom Storage Switch A zu den NSM224 Storage-Ports für HA-Paar 1, Pfad A auf Storage Switch A
3. Verschieben Sie das Kabel von HA-Paar 1, Node A, Pfad A zum Storage Port NSM2224 für HA-Paar 1, Node A auf Storage Switch A
4. Bewegen Sie das Kabel von HA-Paar 1, Node B, Pfad A zum Storage Port NSM2224 für HA-Paar 1, Node B auf Storage Switch A
5. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage Switch A in einem ordnungsgemäßen Zustand ist:

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

Beispiel anzeigen

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

				Speed		
VLAN	Port	Type	Mode	(Gb/s)	State	Status
Node ID						

node1						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online
node2						
30	e0c	ENET	storage	100	enabled	online
30	e0d	ENET	storage	100	enabled	online
30	e5a	ENET	storage	100	enabled	online
30	e5b	ENET	storage	100	enabled	online

- Ersetzen Sie die Speicher-RCF auf Shared Switch A durch die gemeinsam genutzte RCF-Datei. Siehe ["Installieren Sie das RCF auf einem gemeinsamen Cisco Nexus 9336C-FX2 Switch"](#) Entnehmen.
- Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage Switch A in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance
```

There are no entries matching your query.

-] Verschieben Sie die Kabel HA-Paar 1, NSM224 Pfad B vom Storage Switch B zu den gemeinsamen NS224 Storage-Ports für HA-Paar 1, Pfad B zum Storage Switch B

9. Bewegen Sie das Kabel von HA-Paar 1, Node A, Pfad B zum gemeinsamen Storage Port für HA-Paar 1, Node A, Pfad B auf Storage Switch B.
10. Bewegen Sie das Kabel von HA-Paar 1, Node B, Pfad B zu dem gemeinsamen Storage Port für HA-Paar 1, Node B, Pfad B auf Storage Switch B
11. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage-Switch B in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

12. [[step 12]] ersetzen Sie die Speicher-RCF-Datei auf Shared-Switch B durch die gemeinsam genutzte RCF-Datei. Siehe "[Installieren Sie das RCF auf einem gemeinsamen Cisco Nexus 9336C-FX2 Switch](#)" Entnehmen.
13. Überprüfen Sie, ob der mit HA-Paar 1 verbundene Storage-Switch B in einem ordnungsgemäßen Zustand ist:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance  
There are no entries matching your query.
```

14. Überprüfung der Speicherkonfiguration von HA-Paar 1 ist richtig und fehlerfrei:

```
system switch ethernet show
```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                                     Address
Model
-----
sh1
                                     storage-network                             172.17.227.5
C9336C
    Serial Number: FOC221206C2
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(5)
    Version Source: CDP
sh2
                                     storage-network                             172.17.227.6
C9336C
    Serial Number: FOC220443LZ
    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.
storage::*>
```

15. [[step 15]]ISLs zwischen Shared Switch A und Shared Switch B installieren:

Beispiel anzeigen

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# interface e1/35-36*
sh1 (config-if-range)# no lldp transmit
sh1 (config-if-range)# no lldp receive
sh1 (config-if-range)# switchport mode trunk
sh1 (config-if-range)# no spanning-tree bpduguard enable
sh1 (config-if-range)# channel-group 101 mode active
sh1 (config-if-range)# exit
sh1 (config)# interface port-channel 101
sh1 (config-if)# switchport mode trunk
sh1 (config-if)# spanning-tree port type network
sh1 (config-if)# exit
sh1 (config)# exit
```

16. Migrieren Sie das Clusternetzwerk von den vorhandenen Cluster-Switches auf die gemeinsam genutzten Switches, indem Sie das Switch-Austauschverfahren und den gemeinsamen RCF verwenden. Der neue gemeinsam genutzte Schalter A ist „cs1“. Der neue gemeinsam genutzte Schalter B ist „cs2“. Siehe ["Ersetzen Sie einen gemeinsamen Cisco Nexus 9336C-FX2 Switch"](#) Und ["Installieren Sie das RCF auf einem gemeinsamen Cisco Nexus 9336C-FX2 Switch"](#) Entnehmen.
17. Vergewissern Sie sich, dass die Switch-Netzwerkconfiguration gültig ist:

```
network port show
```

18. Entfernen Sie die nicht verwendeten Cluster-Switches.
19. Entfernen Sie die nicht verwendeten Speicherschalter.

Ersetzen Sie einen gemeinsamen Cisco Nexus 9336C-FX2 Switch

Sie können einen defekten Nexus 9336C-FX2 Shared Switch ersetzen. Dies ist ein NDU (Non Disruptive Procedure, NDU).

Was Sie benötigen

Stellen Sie vor dem Austausch des Switches Folgendes sicher:

- In dem vorhandenen Cluster und der Netzwerkinfrastruktur:
 - Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
 - Alle Cluster-Ports sind **up**.
 - Alle logischen Cluster-Schnittstellen (LIFs) sind **up** und auf ihren Home-Ports.
 - Der ONTAP-Cluster ping-Cluster -Node node1 Befehl muss angeben, dass die grundlegende Konnektivität und die PMTU-Kommunikation auf allen Pfaden erfolgreich sind.
- Für den Nexus 9336C-FX2-Ersatzschalter:

- Das Management-Netzwerk-Konnektivität auf dem Ersatz-Switch ist funktionsfähig.
- Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
- Die Node-Verbindungen sind 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 den NX-OS-Bildschalter werden auf den Switch geladen.
- Alle zuvor erstellten Site-Anpassungen wie STP, SNMP und SSH sollten auf den neuen Switch kopiert werden.

Zu den Beispielen

Sie müssen den Befehl zum Migrieren einer Cluster-LIF von dem Node ausführen, auf dem die Cluster-LIF gehostet wird.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der vorhandenen Nexus 9336C-FX2-Schalter sind *sh1* und *sh2*.
- Der Name der neuen Nexus 9336C-FX2 Switches lautet *newsh1* und *newsh2*.
- Die Knotennamen sind *node1* und *node2*.
- Die Cluster-Ports auf jedem Node lauten *e3a* und *e3b*.
- Die LIF-Namen des Clusters sind *node1_clus1* Und *node1_clus2* Für Node1, und *node2_clus1* Und *node2_clus2* Für Knoten 2.
- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet *cluster1:*>*.



Die folgende Vorgehensweise basiert auf der folgenden 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							

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	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
4 entries were displayed.

```

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
node2	/cdp			
	e3a	sh1	Eth1/2	N9K-
C9336C				
	e3b	sh2	Eth1/2	N9K-
C9336C				
node1	/cdp			
	e3a	sh1	Eth1/1	N9K-
C9336C				
	e3b	sh2	Eth1/1	N9K-
C9336C				

4 entries were displayed.

sh1# **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	e3a
node2	Eth1/2	145	H	FAS2980	e3a
sh2	Eth1/35	176	R S I s	N9K-C9336C	
Eth1/35					
sh2 (FDO220329V5)	Eth1/36	176	R S I s	N9K-C9336C	
Eth1/36					

Total entries displayed: 4

sh2# **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      eb
node2          Eth1/2          124      H          FAS2980      eb
sh1            Eth1/35         178      R S I s    N9K-C9336C
Eth1/35
sh1            Eth1/36         178      R S I s    N9K-C9336C
Eth1/36
Total entries displayed: 4

```

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.

2. Optional: Installieren Sie die entsprechenden RCF und das entsprechende Bild auf dem Switch, newsh2, und machen Sie alle erforderlichen Standortvorbereitungen.
 - a. Überprüfen, 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 benötigt, fahren Sie fort [Schritt 3](#).
 - b. Rufen Sie die Seite „Referenzkonfigurationsdatei“ der NetApp Support-Website auf der Seite „NetApp Cluster- und Management-Netzwerk-Switches“ auf.
 - c. Klicken Sie auf den Link für die Cluster-Netzwerk- und Management-Netzwerk-Kompatibilitätsmatrix, und notieren Sie anschließend die erforderliche Switch-Softwareversion.
 - d. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Seite Beschreibung zurückzukehren. Klicken Sie auf WEITER, akzeptieren Sie die Lizenzvereinbarung und gehen Sie dann zur Download-Seite.
 - e. Befolgen Sie die Schritte auf der Download-Seite, um die korrekten RCF- und NX-OS-Dateien für die Version der installierten ONTAP-Software herunterzuladen.
3. beim neuen Switch melden Sie sich als Administrator an und fahren Sie alle Ports ab, die mit den Node-Cluster-Schnittstellen verbunden werden sollen (Ports 1/1 bis 1/34). Wenn der Schalter, den Sie ersetzen, nicht funktionsfähig ist und ausgeschaltet ist, fahren Sie mit fort [Schritt 4](#). Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt haben.

Beispiel anzeigen

```

newsh2# config
Enter configuration commands, one per line. End with CNTL/Z.
newsh2(config)# interface e1/1-34
newsh2(config-if-range)# shutdown

```

4. Überprüfen Sie, ob für alle Cluster-LIFs die automatische Zurücksetzung aktiviert ist.

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

Beispiel anzeigen

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

Vserver	Logical 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, ob alle Cluster-LIFs kommunizieren können:

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

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster node2
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 169.254.47.194 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)
```

6. Schalten Sie die ISL-Ports 1/35 und 1/36 am Nexus 9336C-FX2-Switch sh1 ab.

Beispiel anzeigen

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1(config)# interface e1/35-36
sh1(config-if-range)# shutdown
```

7. Entfernen Sie alle Kabel vom Nexus 9336C-FX2 sh2 Switch und verbinden Sie sie dann mit den gleichen Ports am Nexus C9336C-FX2 newsh2 Switch.
8. Bringen Sie die ISLs-Ports 1/35 und 1/36 zwischen den switches sh1 und newsh2 auf, und überprüfen Sie dann den Betriebsstatus des Port-Kanals.

Port-Channel sollte PO1(SU) angeben und Mitgliedsports sollten eth1/35(P) und eth1/36(P) angeben.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/35 und 1/36 und zeigt die Zusammenfassung des Port-Kanals am Switch sh1 an.

```
sh1# configure
Enter configuration commands, one per line. End with CNTL/Z.
sh1 (config)# int e1/35-36
sh1 (config-if-range)# no shutdown
sh1 (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)

sh1 (config-if-range)#
```

9. Überprüfen Sie, ob der Port e3b auf allen Knoten verfügbar ist:

```
network port show ipspace Cluster
```

Beispiel anzeigen

Die Ausgabe sollte wie folgt aussehen:

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

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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/auto
false
4 entries were displayed.
```

10. auf demselben Node, den Sie im vorherigen Schritt verwendet haben, setzen Sie die dem Port zugeordnete Cluster-LIF im vorherigen Schritt zurück, indem Sie den Befehl zur Zurücksetzen der Netzwerkschnittstelle verwenden.

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert „Home“ lautet und der Port e3b ist.

Die folgenden Befehle geben LIF node1_clus2 on node1 an den Home Port e3a zurück und zeigen

Informationen über die LIFs auf beiden Knoten an. Das Aufbringen des ersten Knotens ist erfolgreich, wenn die Spalte IS Home für beide Cluster-Schnittstellen **true** lautet und sie die korrekten Port-Zuweisungen zeigen, in diesem Beispiel e3a und e3b auf node1.

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
e3a	false			
4 entries were displayed.				

11. Informationen über die Knoten in einem Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

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

Node	Health	Eligibility
node1	false	true
node2	true	true

12.] 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					
-----	-----	-----	-----	-----	-----	-----
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 entries were displayed.

13. Stellen Sie sicher, dass alle Cluster-LIFs kommunizieren können:

```
cluster ping-cluster
```


Beispiel anzeigen

```
cluster1::~*> cluster ping-cluster -node node2
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 169.254.47.194 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)
```

14. Bestätigen Sie die folgende Clusternetzwerkconfiguration:

```
network port show
```

Beispiel anzeigen

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

Node: node1

Ignore

Health	Health			Speed (Mbps)		
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

Health	Health			Speed (Mbps)		
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 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
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
```

```
4 entries were displayed.
```

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

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

node2	/cdp			
	e3a	sh1 0/2	N9K-C9336C	
	e3b	newsh2	0/2	N9K-
C9336C				
node1	/cdp			
	e3a	sh1	0/1	N9K-
C9336C				
	e3b	newsh2	0/1	N9K-
C9336C				

```
4 entries were displayed.
```

```
sh1# 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
e3a					
node2		Eth1/2	145	H	FAS2980
e3a					
newsh2		Eth1/35	176	R S I s	N9K-C9336C
Eth1/35					
newsh2		Eth1/36	176	R S I s	N9K-C9336C
Eth1/36					

```
Total entries displayed: 4
```

```
sh2# 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
e3b				
node2	Eth1/2	124	H	FAS2980
eb				
sh1	Eth1/35	178	R S I s	N9K-C9336C
Eth1/35				
sh1	Eth1/36	178	R S I s	N9K-C9336C
Eth1/36				
Total entries displayed: 4				

15. Aktivieren Sie die Protokollerfassung für die Integritätsüberwachung des Ethernet Switch, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:
- ° system switch ethernet log setup password
 - ° system switch ethernet log enable-collection

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
sh1
sh2
cluster1::*> system switch ethernet log setup-password
Enter the switch name: sh1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log setup-password
Enter the switch name: sh2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y
Enter the password: <enter switch password>
Enter the password again: <enter switch password>
cluster1::*> system switch ethernet log enable-collection
Do you want to enable cluster log collection for all nodes in the
cluster? y|n}: [n] y
Enabling cluster switch log collection.
cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

1. Bewegen Sie die Speicherports vom alten Switch sh2 zum neuen Switch newsh2.
2. Überprüfen Sie, ob der mit dem HA-Paar 1 verbundene Speicher, der gemeinsam genutzte Switch newsh2 in einem ordnungsgemäßen Zustand ist.
3. Überprüfen Sie, ob der an HA-Paar 2 angeschlossene Speicher, der gemeinsam genutzte Switch newsh2 in einem ordnungsgemäßen Zustand ist:

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

Beispiel anzeigen

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

VLAN				Speed		
Node	Port	Type	Mode	(Gb/s)	State	Status
ID						

node1						
30	e3a	ENET	storage	100	enabled	online
30	e3b	ENET	storage	0	enabled	offline
30	e7a	ENET	storage	0	enabled	offline
30	e7b	ENET	storage	100	enabled	online
node2						
30	e3a	ENET	storage	100	enabled	online
30	e3b	ENET	storage	0	enabled	offline
30	e7a	ENET	storage	0	enabled	offline
30	e7b	ENET	storage	100	enabled	online

4. Stellen Sie sicher, dass die Shelves ordnungsgemäß verkabelt sind:

```
storage shelf port show -fields remote- device,remote-port
```

Beispiel anzeigen

```
cluster1::*> storage shelf port show -fields remote-device,remote-  
port  
shelf id remote-port  remote-device  
-----  
3.20  0  Ethernet1/13  sh1  
3.20  1  Ethernet1/13  newsh2  
3.20  2  Ethernet1/14  sh1  
3.20  3  Ethernet1/14  newsh2  
3.30  0  Ethernet1/15  sh1  
3.30  1  Ethernet1/15  newsh2  
3.30  2  Ethernet1/16  sh1  
3.30  3  Ethernet1/16  newsh2  
8 entries were displayed.
```

5. Entfernen Sie den alten Schalter sh2.
6. Wiederholen Sie diese Schritte für den Schalter sh1 und den neuen Schalter newsh1.
7. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Switches für das Ende der Verfügbarkeit

End-of-Verfügbarkeit

Die folgenden Switches sind nicht mehr zum Kauf erhältlich, werden aber weiterhin unterstützt.

- ["Cisco Nexus 3232C"](#)
- ["Cisco Nexus 3132Q-V"](#)
- ["Cisco Nexus 92300YC"](#)
- ["NetApp CN1610"](#)

Cisco Nexus 3232C

Überblick

Überblick über Installation und Konfiguration von Cisco Nexus 3232c-Switches

Cisco Nexus 3232C Switches können als Cluster-Switches in Ihrem AFF oder FAS Cluster verwendet werden. Dank Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Nodes erstellen.

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen Cisco Nexus 3232c Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Füllen Sie das Cisco Nexus 3232C-Verkabelungsarbeitsblatt aus"](#). Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.
2. ["Installieren Sie einen Cisco Nexus 3232C Cluster Switch in einem NetApp Rack"](#). Installieren Sie den Cisco Nexus 3232C-Cluster-Switch und die Pass-Through-Panel in einem NetApp-Schrank mit den im Switch enthaltenen Standardhalterungen.
3. ["Konfigurieren Sie den 3232C-Cluster-Switch"](#). Richten Sie den Cisco Nexus 3232C Switch ein und konfigurieren Sie ihn.
4. ["Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei vor"](#). Bereiten Sie die Installation der NX-OS-Software und der Referenz-Konfigurationsdatei (RCF) vor.
5. ["Installieren Sie die NX-OS-Software"](#). Installieren Sie die NX-OS-Software auf dem Nexus 3232C-Cluster-Switch.
6. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)."](#) Installieren Sie den RCF, nachdem Sie den Nexus 3232C-Switch zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)

- ["Erforderliche Dokumentation"](#)
- ["Anforderungen für Smart Call Home"](#)

Konfigurationsanforderungen für Cisco Nexus 3232C Switches

Für die Installation und Wartung von Cisco Nexus 3232C Switches sollten die Konfigurations- und Netzwerkanforderungen geprüft werden.

Konfigurationsanforderungen

Zum Konfigurieren des Clusters benötigen Sie die entsprechende Anzahl und den entsprechenden Kabeltyp und Kabelanschlüsse für Ihre Switches. Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

Netzwerkanforderungen

Sie benötigen die folgenden Netzwerkinformationen für alle Switch-Konfigurationen:

- IP-Subnetz für den Management-Netzwerkdatenverkehr
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700 Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.

Siehe ["Hardware Universe"](#) Aktuelle Informationen.

Dokumentationsanforderungen für Cisco Nexus 3232C-Switches

Lesen Sie bei der Installation und Wartung von Cisco Nexus 3232C Switches alle empfohlenen Dokumente.

Switch-Dokumentation

Zum Einrichten der Cisco Nexus 3232C-Switches wird die folgende Dokumentation von benötigt ["Switches Der Cisco Nexus 3000-Serie Unterstützen"](#) Seite.

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie <i>Nexus 3000</i>	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 3000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.

Dokumenttitel	Beschreibung
<i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 3000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 3000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 3000-Switches.
<i>Nexus 3000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 3000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.
<i>Versionshinweise zur Cisco Nexus 3000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 3000 Serie.
Gesetzliche Vorschriften, Compliance und Sicherheitsinformationen für die Cisco Nexus 6000, Cisco Nexus 5000 Serie, Cisco Nexus 3000 Serie und Cisco Nexus 2000 Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 3000.

Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Betriebssystemversion über das ["ONTAP 9 Dokumentationszentrum"](#).

Name	Beschreibung
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP-Dokumentation	Dieser Service bietet detaillierte Informationen zu allen Aspekten der ONTAP Versionen.
"Hardware Universe"	Liefert Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Schienenansatz und Rack-Dokumentation

Informationen zur Installation eines Cisco Switch der 3232C-Serie in einem NetApp Rack finden Sie in der folgenden Hardware-Dokumentation.

Name	Beschreibung
"42-HE-System-Cabinet, Deep Guide"	Beschreibt die FRUs, die dem 42U-Systemschrank zugeordnet sind, und bietet Anweisungen für Wartung und FRU-Austausch.
"Installieren Sie einen Cisco Nexus 3232C Switch in einem NetApp Rack"	Beschreibt die Installation eines Cisco Nexus 3232C-Switch in einem NetApp Rack mit vier Pfosten.

Anforderungen für Smart Call Home

Überprüfen Sie die folgenden Richtlinien, um die Smart Call Home-Funktion zu verwenden.

Smart Call Home überwacht die Hardware- und Softwarekomponenten Ihres Netzwerks. Wenn eine kritische Systemkonfiguration auftritt, generiert es eine E-Mail-basierte Benachrichtigung und gibt eine Warnung an alle Empfänger aus, die im Zielprofil konfiguriert sind. Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch konfigurieren, um per E-Mail mit dem Smart Call Home-System kommunizieren zu können. Darüber hinaus können Sie optional Ihren Cluster-Netzwerk-Switch einrichten, um die integrierte Smart Call Home-Support-Funktion von Cisco zu nutzen.

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

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.
- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.
- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

Der ["Cisco Support-Website"](#) Enthält Informationen zu den Befehlen zum Konfigurieren von Smart Call Home.

Hardware installieren

Füllen Sie das Cisco Nexus 3232C-Verkabelungsarbeitsblatt aus

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

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

Jeder Switch kann als einzelner 100-GbE-, 40-GbE-Port oder 4-x-GbE-Ports konfiguriert werden.

Beispiel für eine Verkabelung

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	1	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
2	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	2	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
3	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	3	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
4	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	4	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
5	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	5	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
6	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	6	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
7	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	7	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
8	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	8	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
9	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	9	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
10	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	10	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
11	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	11	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
12	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	12	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
13	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	13	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
14	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	14	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node

Cluster-Switch A		Cluster-Switch B	
15	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	15	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
16	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	16	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
17	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	17	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
18	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node	18	4 x 10 GbE/4x25 GbE oder 40/100-GbE-Node
19	40 G/100-GbE-Node 19	19	40 G/100-GbE-Node 19
20	40 G/100-GbE-Node 20	20	40 G/100-GbE-Node 20
21	40 G/100-GbE-Node 21	21	40 G/100-GbE-Node 21
22	40 G/100-GbE-Node 22	22	40 G/100-GbE-Node 22
23	40 G/100-GbE-Node 23	23	40 G/100-GbE-Node 23
24	40 G/100-GbE-Node 24	24	40 G/100-GbE-Node 24
25 bis 30	Reserviert	25 bis 30	Reserviert
31	100-GbE-ISL zu Switch B- Port 31	31	100-GbE-ISL für Switch A-Port 31
32	100-GbE-ISL zu Switch B- Port 32	32	100-GbE-ISL für Switch A-Port 32

Leeres Verkabelungsarbeitsblatt

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des "[Hardware Universe](#)" Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Node-/Port-Verwendung	Switch-Port	Node-/Port-Verwendung
1		1	
2		2	

Cluster-Switch A		Cluster-Switch B	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
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	

Cluster-Switch A		Cluster-Switch B	
25 bis 30	Reserviert	25 bis 30	Reserviert
31	100-GbE-ISL zu Switch B-Port 31	31	100-GbE-ISL für Switch A-Port 31
32	100-GbE-ISL zu Switch B-Port 32	32	100-GbE-ISL für Switch A-Port 32

Konfigurieren Sie den 3232C-Cluster-Switch

Befolgen Sie diese Anweisungen, um den Cisco Nexus 3232C Switch einzurichten und zu konfigurieren.

Was Sie benötigen

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von "[Cisco Software-Download](#)" Seite.
- Erforderliche Dokumentation für das Cluster-Netzwerk und den Switch des Management-Netzwerks

Siehe "[Erforderliche Dokumentation](#)" Finden Sie weitere Informationen.

- Erforderliche Controller-Dokumentation und ONTAP-Dokumentation

["NetApp Dokumentation"](#)

- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossene Verkabelungsarbeitsblätter.
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden "[mysupport.netapp.com](#)" Für die Switches, die Sie empfangen. Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, haben aber die RCFs nicht geladen.

Schritte

1. Rack-Aufbau des Cluster-Netzwerks und der Management-Netzwerk-Switches und -Controller

Wenn Sie das installieren...	Dann...
Cisco Nexus 3232C in einem NetApp System-Rack	Anweisungen zur Installation des Switches in einem NetApp Schrank sind im Abschnitt _Installieren eines Cisco Nexus 3232C-Cluster-Switch und Pass-Through-Panel in einem NetApp Rack verfügbar.
Geräte in einem Telco-Rack	Siehe die Verfahren in den Installationsleitfäden für die Switch-Hardware sowie in den Installations- und Setup-Anleitungen für NetApp.

2. Verkabeln Sie die Switches für das Cluster-Netzwerk und das Management-Netzwerk mithilfe der

ausgefüllten Verkabelungsarbeitsblätter mit den Controllern.

3. Schalten Sie das Cluster-Netzwerk sowie die Switches und Controller des Managementnetzwerks ein.
4. Initiale Konfiguration der Cluster-Netzwerk-Switches durchführen.

Geben Sie beim ersten Booten des Switches die folgenden Einrichtungsfragen entsprechend an. Die Sicherheitsrichtlinie Ihres Standorts definiert die zu erstellenden Antworten und Services.

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit ja . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (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, starkes Passwort erstellen. Ein schwaches Kennwort kann abgelehnt werden.
Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)	Reagieren Sie mit ja bei der Erstkonfiguration des Schalters.
Noch ein Login-Konto erstellen? (ja/nein)	Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen. Der Standardwert ist no .
Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Geben Sie den Switch-Namen ein.	Der Switch-Name ist auf 63 alphanumerische Zeichen begrenzt.
Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)	Beantworten Sie mit ja (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein.
Standard-Gateway konfigurieren? (ja/nein)	Antworten Sie mit ja . Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein

Eingabeaufforderung	Antwort
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit ja. Die Standardeinstellung ist ja.</p> <div>  <p>SSH wird empfohlen, wenn Sie Cluster Switch Health Monitor (CSHM) für seine Protokollerfassung verwenden. SSHv2 wird auch für erhöhte Sicherheit empfohlen.</p> </div>
Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1).	Der Standardwert ist rsa .
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits von 1024-2048 ein.
Konfigurieren Sie den NTP-Server? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Standard-Schnittstellenebene konfigurieren (L3/L2):	Antworten Sie mit L2 . Der Standardwert ist L2.
Konfigurieren Sie den Status der Switch-Schnittstelle (shut/noshut) als Standard-Switch-Port:	Antworten Sie mit noshut . Die Standardeinstellung ist noshut.
Konfiguration des CoPP-Systemprofils (streng/mittel/lenient/dense):	Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, antworten Sie mit No an der Eingabeaufforderung. Beantworten Sie mit ja , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)	<p>Antworten Sie mit ja, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert.</p> <div>  <p>Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam.</p> </div>

- Überprüfen Sie die Konfigurationseinstellungen, die Sie am Ende der Einrichtung in der Anzeige vorgenommen haben, und stellen Sie sicher, dass Sie die Konfiguration speichern.
- Überprüfen Sie die Version der Cluster-Netzwerk-Switches und laden Sie bei Bedarf die von NetApp unterstützte Version der Software von auf die Switches von herunter "[Cisco Software-Download](#)" Seite.

Was kommt als Nächstes?

"Bereiten Sie sich auf die Installation von NX-OS und RCF vor".

Installieren Sie einen Cisco Nexus 3232C Cluster Switch in einem NetApp Rack

Je nach Konfiguration müssen möglicherweise der Cisco Nexus 3232C Cluster-Switch und die Pass-Through-Panel in einem NetApp Rack mit den im Switch enthaltenen Standardhalterungen installiert werden.

Was Sie benötigen

- Die anfänglichen Vorbereitungsanforderungen, Inhalt des Kits und Sicherheitsvorkehrungen im ["Hardware-Installationsleitfaden Der Cisco Nexus 3000-Serie"](#).
- Die acht 10-32- oder 12-24-Schrauben und Muttern für jeden Schalter, um die Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten zu befestigen.
- Cisco Standard-Schienensatz zur Installation des Switches in einem NetApp Rack



Die Jumper-Kabel sind nicht im Lieferumfang des Pass-Through-Kits enthalten und sollten in Ihrem Switch enthalten sein. Wenn die Switches nicht im Lieferumfang enthalten sind, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

Schritte

1. Die Pass-Through-Blindplatte in den NetApp-Schrank einbauen.

Die Pass-Through-Panel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

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

- Ein Durchlauf-Blindblech
- Vier 10-32 x 0,75 Schrauben
- Vier 10-32-Clip-Muttern
 - i. Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

Bei diesem Verfahren wird die Blindplatte in U40 installiert.

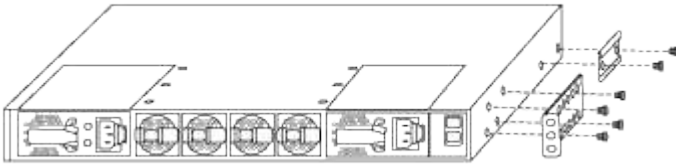
- ii. Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
- iii. Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
- iv. Stecken Sie die Buchsen der beiden 48-Zoll-Jumper-Kabel von der Rückseite der Abdeckung und durch die Bürstenbaugruppe.



(1) Buchsenleiste des Überbrückungskabels.

1. Installieren Sie die Rack-Mount-Halterungen am Nexus 3232C-Switch-Chassis.

- a. Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.



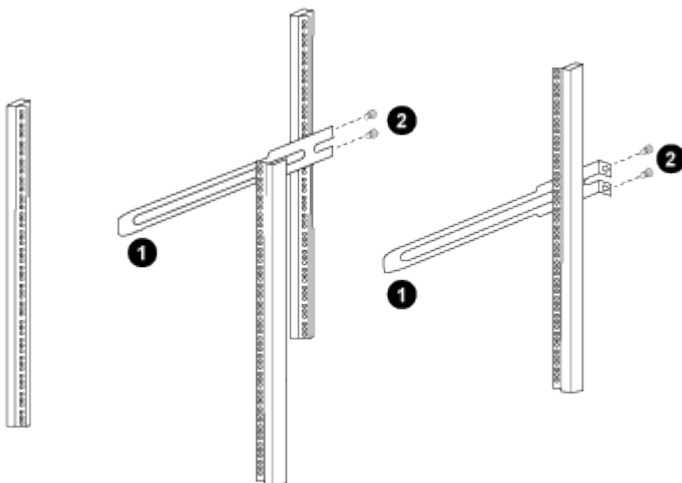
- b. Wiederholen Sie Schritt 2a mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
 - c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.
 - d. Wiederholen Sie Schritt 2c mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite des Schalters.
2. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



Die beiden 3232C-Schalter werden immer in den oberen 2 HE des Schrankes RU41 und 42 montiert.

3. Installieren Sie die Gleitschienen im Schrank.

- a. Positionieren Sie die erste Gleitschiene an der RU42-Markierung auf der Rückseite des hinteren linken Pfosten, legen Sie die Schrauben mit dem entsprechenden Gewindetyp ein und ziehen Sie die Schrauben mit den Fingern fest.



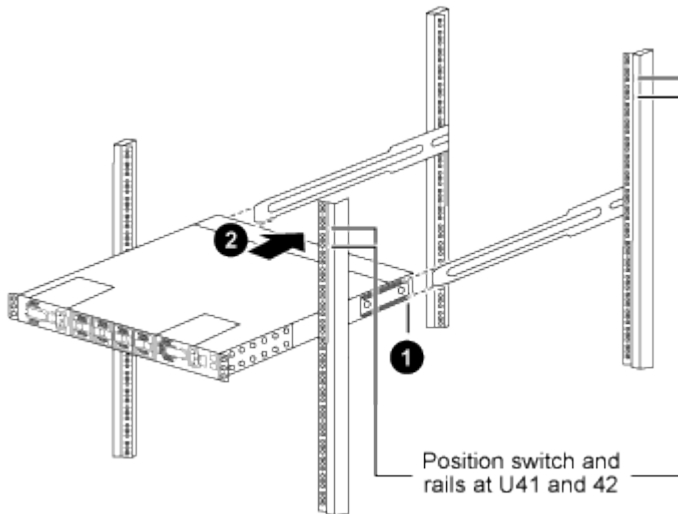
(1) beim sanften Schieben der Gleitschiene richten Sie sie an den Schraubenbohrungen im Rack aus. + (2) ziehen Sie die Schrauben der Gleitschienen an den Schrankleisten fest.

- a. Wiederholen Sie Schritt 4a für den hinteren Pfosten auf der rechten Seite.
 - b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Stellen im Schrank.
4. Den Schalter in den Schrank einbauen.



Für diesen Schritt sind zwei Personen erforderlich: Eine Person muss den Schalter von vorne und von der anderen in die hinteren Gleitschienen führen.

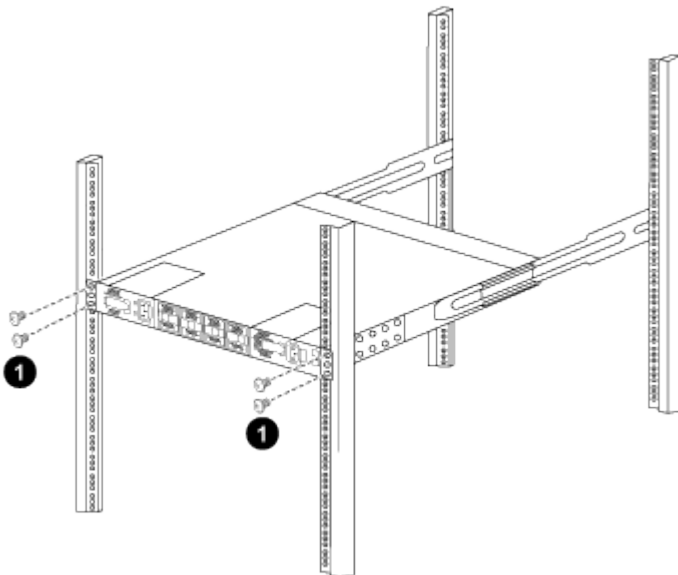
- a. Positionieren Sie die Rückseite des Schalters an RU41.



(1) Da das Gehäuse in Richtung der hinteren Pfosten geschoben wird, richten Sie die beiden hinteren Rackmontageführungen an den Gleitschienen aus.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Halterungen der Rackmontage bündig mit den vorderen Pfosten sind.

- b. Befestigen Sie den Schalter am Gehäuse.



(1) mit einer Person, die die Vorderseite des Chassis hält, sollte die andere Person die vier hinteren Schrauben vollständig an den Schrankpfosten festziehen.

- a. Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- b. Wiederholen Sie die Schritte 5a bis 5c für den zweiten Schalter an der Position RU42.



Durch die Verwendung des vollständig installierten Schalters als Unterstützung ist es nicht erforderlich, während des Installationsvorgangs die Vorderseite des zweiten Schalters zu halten.

5. Wenn die Switches installiert sind, verbinden Sie die Jumper-Kabel mit den Switch-Netzeinkabeln.
6. Verbinden Sie die Stecker beider Überbrückungskabel mit den am nächsten verfügbaren PDU-Steckdosen.



Um Redundanz zu erhalten, müssen die beiden Kabel mit verschiedenen PDUs verbunden werden.

7. Verbinden Sie den Management-Port auf jedem 3232C-Switch mit einem der Management-Switches (falls bestellt) oder verbinden Sie sie direkt mit dem Managementnetzwerk.

Der Management-Port ist der oben rechts gelegene Port auf der PSU-Seite des Switch. Das CAT6-Kabel für jeden Switch muss über die Passthrough-Leiste geführt werden, nachdem die Switches zur Verbindung mit den Management-Switches oder dem Management-Netzwerk installiert wurden.

Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 3232C-Switch konfigurieren, lesen Sie die folgenden Überlegungen.

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

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 Switch-Port-Geschwindigkeit fest kodieren.

```
(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 ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

Software konfigurieren

Vorbereiten der Installation der NX-OS-Software und der Referenzkonfigurationsdatei (RCF)

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

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster-Interconnect-Ports e0a Und e0b.

Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Switch- und Node-Terminologie

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` Und `cs2`.
- Die Node-Namen sind `cluster1-01` Und `cluster1-02`.
- Die LIF-Namen des Clusters sind `cluster1-01_clus1` Und `cluster1-01_clus2` Für Clustered 1-01 und `cluster1-02_clus1` Und `cluster1-02_clus2` Für Clustered 1-02.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (``*>``) erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

Beispiel anzeigen

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp	e0a	cs1	Eth1/2	N3K-
C3232C	e0b	cs2	Eth1/2	N3K-
C3232C				
cluster1-01/cdp	e0a	cs1	Eth1/1	N3K-
C3232C	e0b	cs2	Eth1/1	N3K-
C3232C				

4 entries were displayed.

4. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

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


Beispiel anzeigen

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

```
Node: cluster1-02
```

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

```
Node: cluster1-01
```

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

```
4 entries were displayed.
```

a. Zeigt Informationen zu den LIFs an:

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

Beispiel anzeigen

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

Current Vserver Port	Logical Current Is Interface Home	Status Admin/Oper	Network Address/Mask	Node

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. Ping für die Remote-Cluster-LIFs:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node cluster1-02
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)
```

6. Überprüfen Sie das `auto-revert` Befehl ist für alle Cluster-LIFs aktiviert:
`network interface show -vserver Cluster -fields auto-revert`

Beispiel anzeigen

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

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

4 entries were displayed.

7. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die Ethernet Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password
```

```
system switch ethernet log enable-collection
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue*? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

8. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Installieren Sie die NX-OS-Software

Mithilfe dieser Vorgehensweise können Sie die NX-OS-Software auf dem Nexus 3232C-Cluster-Switch installieren.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- ["Cisco Ethernet Switch Seite"](#). In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie die Software

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#), Und dann folgen Sie den Schritten unten.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung mit dem Server, der die NX-OS-Software und die RCF hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

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

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

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

Beispiel anzeigen

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

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

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

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

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

```
show version
```


Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FO?????GD

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

  Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
```

```
Reason: Reset Requested by CLI command reload
```

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Installieren Sie das NX-OS Image.

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

Beispiel anzeigen

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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

Compatibility check is done:
Module  bootable          Impact          Install-type  Reason
-----
      1      yes          disruptive          reset          default
upgrade is not hitless

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

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

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[] 100% -- SUCCESS
```

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

```
cs2#
```

6. 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 08.37
  NXOS: version 9.3(4)
  BIOS compile time: 01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FO?????GD

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

  Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
```

Reason: Reset due to upgrade

System version: 9.3(3)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

cs2#

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD Device	Version
-------------	---------

MI FPGA	0x12
IO FPGA	0x11

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
--------	------	------	-----------------	-------------	--------------

1	SUP	MI FPGA	0x12	0x12	No
---	-----	---------	------	------	----

1	SUP	IO FPGA	0x11	0x12	Yes
---	-----	---------	------	------	-----

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
--------	------	----------------

1	SUP	Success
---	-----	---------

Module 1 EPLD upgrade is successful.

```
cs2#
```

8. Melden Sie sich nach dem Neustart des Switches erneut an, aktualisieren Sie das goldene EPLD-Bild und starten Sie den Switch erneut.

Beispiel anzeigen

```
cs2# install epld bootflash:n9000-epld.9.3.4.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module          Type          Upgradable          Impact          Reason
-----
1              SUP              Yes              disruptive      Module
Upgradable

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

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

9. Melden Sie sich nach dem Neustart des Switches an, um zu überprüfen, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x12
IO	FPGA	0x12

Was kommt als Nächstes?

["Installieren Sie die RCF-Konfigurationsdatei"](#)

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Gehen Sie folgendermaßen vor, um den RCF nach dem ersten Einrichten des Nexus 3232C-Switch zu installieren.

Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren. Weitere Informationen finden Sie im Knowledge Base-Artikel ["Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung"](#) Weitere Informationen zum Upgrade Ihres RCF.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle Referenzkonfigurationsdatei (RCF).
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.
- ["Cisco Ethernet Switch Seite"](#) In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie die Datei

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` und `cs2`.
- Die Node-Namen sind `cluster1-01`, `cluster1-02`, `cluster1-03`, und `cluster1-04`.
- Die LIF-Namen des Clusters 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::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Führen Sie den Vorgang in durch ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#), Und dann folgen Sie den Schritten unten.

Schritte

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N3K-
C3232C
          e0d    cs2                Ethernet1/7      N3K-
C3232C
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N3K-
C3232C
          e0d    cs2                Ethernet1/8      N3K-
C3232C
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N3K-
C3232C
          e0b    cs2                Ethernet1/1/1    N3K-
C3232C
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N3K-
C3232C
          e0b    cs2                Ethernet1/1/2    N3K-
C3232C
cluster1::*>
```

2. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen 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

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

cluster1::*>

- b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

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

	Logical	Status	Network	
Current	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

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

Switch Model	Type	Address
cs1 NX3232C	cluster-network	10.233.205.92
Serial Number: FOXXXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
9.3(4)		
Version Source: CDP		
cs2 NX3232C	cluster-network	10.233.205.93
Serial Number: FOXXXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
9.3(4)		
Version Source: CDP		

2 entries were displayed.

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

Beispiel anzeigen

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

4. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

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

5. Überprüfen Sie, ob die Cluster-Ports zu den Ports migriert wurden, die auf Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	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::*>				

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

```
cluster show
```


Beispiel anzeigen

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

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

```
show running-config
```

8. Reinigen Sie die Konfiguration auf Switch cs2, und starten Sie den Switch neu.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Starten Sie den Switch neu:

Beispiel anzeigen

```
(cs2)# reload

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

9. Führen Sie eine grundlegende Einrichtung des Switches durch. Siehe ["Konfigurieren Sie den 3232C-Cluster-Switch"](#) Entsprechende Details.

10. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 3000-Serie NX-OS Command Reference](#)" Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

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

11. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

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

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt Installation auf Schalter cs2:

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

12. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen die Anweisungen unter **wichtige Hinweise** lesen und befolgen, um sicherzustellen, dass der Schalter ordnungsgemäß konfiguriert und betrieben wird.

Beispiel anzeigen

```
cs2# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Cisco Nexus 3232C
* Filename    : Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date       : Oct-20-2020
* Version    : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 3: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25GbE) Intra-Cluster/HA Ports, int
e1/4/1-4,
* e1/5/1-4, e1/6/1-4
* Ports 7-30: 40/100GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
* Ports 33-34: 10GbE Intra-Cluster 10GbE Ports, int e1/33-34
*
* IMPORTANT NOTES
* - Load Nexus_3232C_RCF_v1.6-Cluster-HA.txt for non breakout config
*
* - This RCF utilizes QoS and requires TCAM re-configuration,
requiring RCF
*   to be loaded twice with the Cluster Switch rebooted in between.
*
* - Perform the following 4 steps to ensure proper RCF installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class IPv4
ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
```

```
*
* (4) Save running-configuration again
*****
*****
```



Beim ersten Anwenden des RCF wird die Meldung **ERROR: Failed to write VSH** befehlt erwartet und kann ignoriert werden.

13. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

14. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

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

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

15. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

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

16. Wenden Sie dieselbe RCF an, und speichern Sie die ausgeführte Konfiguration ein zweites Mal.

Beispiel anzeigen

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands  
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

17. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß sind:

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

Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

8 entries were displayed.

- b. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

Beispiel anzeigen

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

Node/	Local	Discovered	
Protocol	Port	Device (LLDP: ChassisID)	Interface
Platform			
cluster1-01/cdp			
	e0a	cs1	Ethernet1/7
N3K-C3232C			
	e0d	cs2	Ethernet1/7
N3K-C3232C			
cluster01-2/cdp			
	e0a	cs1	Ethernet1/8
N3K-C3232C			
	e0d	cs2	Ethernet1/8
N3K-C3232C			
cluster01-3/cdp			
	e0a	cs1	Ethernet1/1/1
N3K-C3232C			
	e0b	cs2	Ethernet1/1/1
N3K-C3232C			
cluster1-04/cdp			
	e0a	cs1	Ethernet1/1/2
N3K-C3232C			
	e0b	cs2	Ethernet1/1/2
N3K-C3232C			

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

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


```
N3K-C3232C
  Serial Number: FOXXXXXXXXGS
    Is Monitored: true
      Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                9.3(4)
  Version Source: CDP

2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten



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



Es kann bis zu 5 Minuten dauern, bis die Cluster-Nodes einen ordnungsgemäßen Zustand melden.

18. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels aus Schritt 1 verwendet:

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

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

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

```
cluster show
```

Beispiel anzeigen

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

21. Wiederholen Sie die Schritte 7 bis 15 am Schalter cs1.
22. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

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

23. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

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

24. Vergewissern Sie sich, dass die mit den Cluster-Ports verbundenen Switch-Ports aktiv sind.

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) --
.
.
```

25. Stellen Sie sicher, dass die ISL zwischen cs1 und cs2 funktionsfähig ist:

```
show port-channel summary
```

Beispiel anzeigen

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

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

Wenn keine Cluster-LIFS an die Home-Ports zurückgegeben wurden, setzen Sie sie manuell zurück:

```
network interface revert -vserver vserver_name -lif lif_name
```

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

```
cluster show
```

Beispiel anzeigen

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

28. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

```
cluster ping-cluster -node local
```

Beispiel anzeigen

```
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)
```

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung über den Cisco 3232C Cluster Switch * CLI * eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```


2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.

ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.
Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 3232C-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config)# show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv

```
(sw1) (Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N3K-C3232C
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N3K-C3232C
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Switches migrieren

Migrationsanforderungen für Cisco Nexus 3232C Cluster Switches

Vor der Migration zu Cisco Nexus 3232C Cluster-Switches. Überprüfen Sie die Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen.

Migrationsanforderungen für CN1610

Die Cluster-Switches unterstützen die folgenden Node-Verbindungen:

- NetApp CN1610: 0/1 bis 0/12 (10 GbE)
- Cisco Nexus 3232C – Ports e1/1-30 (40 oder 100 oder 4x10 GbE)

Bei den Cluster-Switches werden die folgenden Inter-Switch-Link-Ports (ISL) verwendet.

- NetApp CN1610: 0/13 bis 0/16 (10 GbE)
- Cisco Nexus 3232C – 31-32 Ports (100 GbE)



Auf dem Cisco Nexus 3232C Cluster Switch müssen 4X10G-Breakout-Kabel verwendet werden.

Die folgende Tabelle zeigt die in der jeweiligen Phase erforderlichen Verkabelungsverbindungen beim Umstieg von NetApp CN1610-Switches auf Cisco Nexus 3232C-Cluster-Switches:

Stufe	Beschreibung	Erforderliche Kabel
Initial	CN1610 bis CN1610 (SFP+ auf SFP+)	4 SFP+-Glasfaserkabel oder Kupfer-Direct-Attached-Kabel
Übergang	CN1610 bis 3232C (QSFP zu SFP+)	1 QSFP- und 4 SFP+-Glasfaserkabel oder Kupferkabel
Endgültig	3232C auf 3232C (QSFP zu QSFP)	2 QSFP-Glasfaserkabel oder Kupfer-Direct-Attach-Kabel

Sie müssen die entsprechenden Referenzkonfigurationsdateien (RCFs) heruntergeladen haben. Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren RCFs definiert "[Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen](#)" Seite.

Die in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen finden Sie auf der "[Seite zu Cisco Ethernet Switches](#)".

Die in diesem Verfahren unterstützten ONTAP- und FASTPATH-Versionen werden auf der aufgeführt "[Seite zu den NetApp CN1601 und CN1610 Switches](#)".

CN5596 Anforderungen

Die Cluster-Switches verwenden die folgenden Ports für Verbindungen zu den Nodes:

- Ports e1/1-40 (10 GbE): Nexus 5596
- Ports e1/1-30 (10/40/100 GbE): Nexus 3232C
 - Bei den Cluster-Switches werden die folgenden Inter-Switch Link (ISL)-Ports verwendet:
- Ports e1/41-48 (10 GbE): Nexus 5596
- Ports e1/31-32 (40/100 GbE): Nexus 3232C
 - Der "[Hardware Universe](#)" Hier finden Sie Informationen zur unterstützten Verkabelung zu Nexus 3232C-Switches:
- Nodes mit 10 GbE-Cluster-Verbindungen erfordern QSFP zu SFP+-Breakout-Kabel oder QSFP zu SFP+-Kupfer-Breakout-Kabel.
- Nodes mit 40/100 GbE-Cluster-Verbindungen erfordern unterstützte QSFP/QSFP28 optische Module mit Glasfaserkabeln oder QSFP/QSFP28 Kupfer-Direct-Attach-Kabeln.
 - Die Cluster-Switches verwenden die entsprechende ISL-Verkabelung:
- Anfang Nexus 5596 (SFP+ auf SFP+)
 - 8 x SFP+-Glasfaserkabel oder Kupfer-Direct-Attached-Kabel
- Interim: Nexus 5596 auf Nexus 3232C (QSFP zu 4xSFP+ Breakout-out)
 - 1x Kabel für QSFP zu SFP+-Ausbruchkabel oder Kupferausbruch

- Final: Nexus 3232C auf Nexus 3232C (QSFP28 zu QSFP28)
 - 2 QSFP28 Glasfaserkabel oder Kupfer-Direct-Attach-Kabel
 - Bei Nexus 3232C Switches können QSFP/QSFP28-Ports entweder im 40/100-Gigabit-Ethernet- oder im 4 x 10-Gigabit-Ethernet-Modus betrieben werden.

Standardmäßig sind im 40/100-Gigabit-Ethernet-Modus 32 Ports vorhanden. Diese 40-Gigabit-Ethernet-Ports werden in einer 2-tupel-Namenskonvention nummeriert. So wird beispielsweise der zweite 40-Gigabit-Ethernet-Port mit der Nummer 1/2 nummeriert. Der Prozess der Änderung der Konfiguration von 40 Gigabit Ethernet zu 10 Gigabit Ethernet wird *Breakout* genannt und der Prozess der Änderung der Konfiguration von 10 Gigabit Ethernet zu 40 Gigabit Ethernet wird *break* genannt. Wenn Sie einen 40/100-Gigabit-Ethernet-Port in 10 Gigabit-Ethernet-Ports untergliedern, werden die resultierenden Ports mit einer 3-tupel-Namenskonvention nummeriert. Beispielsweise werden die Ausbruchanschlüsse des zweiten 40/100-Gigabit-Ethernet-Ports mit den Nummern 1/2/1, 1/2/2/2, 1/2/3 und 1/2/4 nummeriert.

- Auf der linken Seite der Nexus 3232C-Switches sind 2 SFP+-Ports, genannt 1/33 und 1/34.
- Sie haben einige der Ports auf Nexus 3232C-Switches für 10-GbE- oder 40/100-GbE-Ausführung konfiguriert.



Sie können die ersten sechs Ports mit dem in den 4x10 GbE-Modus versetzen `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Auf ähnliche Weise können Sie die ersten sechs QSFP+-Ports aus Breakout-Konfiguration mit dem neu gruppieren `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie haben die Planung, Migration und die erforderliche Dokumentation auf 10-GbE- und 40/100-GbE-Konnektivität zwischen den Nodes zu Nexus 3232C-Cluster-Switches gelesen.
- Die in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen befinden sich auf dem ["Seite zu Cisco Ethernet Switches"](#).

Migrieren Sie einen CN1610 Cluster-Switch zu einem Cisco Nexus 3232C Cluster-Switch

Um die vorhandenen CN1610-Cluster-Switches in einem Cluster durch Cisco Nexus 3232C-Cluster-Switches zu ersetzen, müssen Sie eine bestimmte Sequenz von Aufgaben durchführen.

Prüfen Sie die Anforderungen

Vor der Migration sollten Sie unbedingt prüfen ["Migrationsanforderungen"](#).



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Weitere Informationen finden Sie bei Bedarf im folgenden Dokument:

- ["Beschreibungsseite zu NetApp CN1601 und CN1610"](#)
- ["Beschreibungsseite für den Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Migrieren Sie die Switches

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden vier Nodes: Zwei Nodes verwenden vier 10-GbE-Cluster-Interconnect-Ports: e0a, e0b, e0c und e0d. Die anderen beiden Knoten verwenden zwei 40 GbE Cluster Interconnect Glasfaserkabel: e4a und e4e. Der "[Hardware Universe](#)" Enthält Informationen zu den Glasfaserkabeln des Clusters auf den Plattformen.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Knoten sind n1, n2, n3 und n4.
- Die Ausgaben für die Befehle können je nach Versionen der ONTAP Software variieren.
- Die zu ersetzenden CN1610-Schalter sind CL1 und CL2.
- Die Switches der Nexus 3232C-Serie als Ersatz für die CN1610-Switches sind C1 und C2.
- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die mit Cluster-Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- n1_clus2 ist die erste Cluster-LIF, die mit Cluster Switch 2 (CL2 oder C2) für Node n1 verbunden ist.
- n1_clus3 ist die zweite logische Schnittstelle, die mit Cluster Switch 2 (CL2 oder C2) für Knoten n1 verbunden ist.
- n1_clus4 ist die zweite logische Schnittstelle, die mit Cluster Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert "[Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen](#)" Seite.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.



Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit während des Wartungsfensters die automatische Case-Erstellung unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device-discovery show
```

Beispiel anzeigen

Im folgenden Beispiel wird angezeigt, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster-Interconnect-Switch konfiguriert wurden:

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	CL1	0/1	CN1610
	e0b	CL2	0/1	CN1610
	e0c	CL2	0/2	CN1610
	e0d	CL1	0/2	CN1610
n2	/cdp			
	e0a	CL1	0/3	CN1610
	e0b	CL2	0/3	CN1610
	e0c	CL2	0/4	CN1610
	e0d	CL1	0/4	CN1610

8 entries were displayed.

3. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

a. Zeigt die Attribute des Cluster-Netzwerk-Ports an:

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

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

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

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

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

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	
e0d	cluster	cluster	up	9000	auto/10000	-	

8 entries were displayed.

b. Informationen zu den logischen Schnittstellen anzeigen:

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

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current      Current
Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
-----
Cluster
true      n1_clus1      up/up      10.10.0.1/24      n1      e0a
true      n1_clus2      up/up      10.10.0.2/24      n1      e0b
true      n1_clus3      up/up      10.10.0.3/24      n1      e0c
true      n1_clus4      up/up      10.10.0.4/24      n1      e0d
true      n2_clus1      up/up      10.10.0.5/24      n2      e0a
true      n2_clus2      up/up      10.10.0.6/24      n2      e0b
true      n2_clus3      up/up      10.10.0.7/24      n2      e0c
true      n2_clus4      up/up      10.10.0.8/24      n2      e0d

8 entries were displayed.
```

c. Informationen über die erkannten Cluster-Switches anzeigen:

```
system cluster-switch show
```

Beispiel anzeigen

Im folgenden Beispiel werden die Cluster-Switches, die dem Cluster bekannt sind, sowie ihre Management-IP-Adressen angezeigt:

```
cluster::> system cluster-switch show
```

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

2 entries displayed.

4. Vergewissern Sie sich, dass die entsprechenden RCF und das entsprechende Image auf den neuen 3232C-Switches installiert sind, wenn dies für Ihre Anforderungen erforderlich ist, und nehmen Sie alle wesentlichen Standortanpassungen vor.

Sie sollten beide Switches derzeit vorbereiten. Wenn Sie ein RCF- und Image-Upgrade durchführen müssen, müssen Sie folgende Schritte ausführen:

- a. Siehe "[Cisco Ethernet Switch](#)" Auf der NetApp Support Site finden.
 - b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
 - c. Laden Sie die entsprechende Version des RCF herunter.
 - d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
 - e. Laden Sie die entsprechende Version der Bildsoftware unter herunter "[Cisco® Cluster und Management Network Switch Referenzkonfigurationsdatei herunterladen](#)".
5. Migrieren Sie die LIFs, die dem zweiten CN1610 Switch zugeordnet sind, den Sie ersetzen möchten:

```
network interface migrate -vserver vserver-name -lif lif-name -source-node  
source-node-name destination-node destination-node-name -destination-port  
destination-port-name
```

Beispiel anzeigen

Sie müssen jede LIF individuell wie im folgenden Beispiel gezeigt migrieren:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2
-source-node n1
-destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver cluster -lif n1_clus3
-source-node n1
-destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver cluster -lif n2_clus2
-source-node n2
-destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver cluster -lif n2_clus3
-source-node n2
-destination-node n2 -destination-port e0d
```

6. Überprüfen Sie den Systemzustand des Clusters:

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

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current  Current  Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
Cluster
true      n1_clus1    up/up      10.10.0.1/24  n1        e0a
false     n1_clus2    up/up      10.10.0.2/24  n1        e0a
false     n1_clus3    up/up      10.10.0.3/24  n1        e0d
true      n1_clus4    up/up      10.10.0.4/24  n1        e0d
true      n2_clus1    up/up      10.10.0.5/24  n2        e0a
false     n2_clus2    up/up      10.10.0.6/24  n2        e0a
false     n2_clus3    up/up      10.10.0.7/24  n2        e0d
true      n2_clus4    up/up      10.10.0.8/24  n2        e0d

8 entries were displayed.
```

Schritt: Ersetzen Sie den Cluster-Switch CL2 durch C2

1. Fahren Sie die Cluster-Interconnect-Ports herunter, die physisch mit dem Switch CL2 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Im folgenden Beispiel werden die vier Cluster-Interconnect-Ports für Knoten n1 und Knoten n2 heruntergefahren:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

2. Pingen Sie die Remote-Cluster-Schnittstellen, und führen Sie dann eine Remote-Prozedur Call-Server überprüfen:

```
cluster ping-cluster -node node-name
```


Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

3. Fahren Sie die ISL-Ports 13 bis 16 am aktiven CN1610-Switch CL1 mit dem entsprechenden Befehl herunter.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Im folgenden Beispiel werden die ISL-Ports 13 bis 16 am CN1610-Switch CL1 heruntergefahren:

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

4. Temporäres ISL zwischen CL1 und C2 aufbauen:

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt eine temporäre ISL, die zwischen CL1 (Ports 13-16) und C2 (Ports e1/24/1-4) mit Cisco aufgebaut wird `switchport mode trunk` Befehl:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

5. Entfernen Sie die Kabel, die an allen Knoten am CN1610-Switch CL2 angeschlossen sind.

Unter Verwendung der unterstützten Verkabelung müssen Sie die getrennten Ports auf allen Nodes mit dem Nexus 3232C Switch C2 verbinden.

6. Entfernen Sie vier ISL-Kabel von den Ports 13 bis 16 am CN1610-Switch CL1.

Sie müssen die entsprechenden Cisco QSFP28 an SFP+ Breakout-Kabel anschließen, die Port 1/24 am neuen Cisco 3232C Switch C2 an die Ports 13 bis 16 des vorhandenen CN1610-Switch CL1 anschließen.



Beim erneuten Verbinden aller Kabel mit dem neuen Cisco 3232C Switch müssen entweder optische oder Cisco Twinax-Kabel verwendet werden.

7. Stellen Sie die ISL-Dynamik her, indem Sie die ISL-Schnittstelle 3/1 auf dem aktiven CN1610-Switch konfigurieren, um den statischen Modus zu deaktivieren.

Diese Konfiguration entspricht der ISL-Konfiguration auf dem 3232C-Switch C2, wenn die ISLs auf beiden Switches aufgerufen werden.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Schnittstelle 3/1 für die ISL-Dynamik konfiguriert ist:

```
(CL1) # configure
(CL1) (Config) # interface 3/1
(CL1) (Interface 3/1) # no port-channel static
(CL1) (Interface 3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

8. ISLs 13 bis 16 auf dem aktiven CN1610-Switch CL1 bringen.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Im folgenden Beispiel werden die ISL-Ports 13 bis 16 über die Port-Channel-Schnittstelle 3/1 aufgerufen:

```
(CL1) # configure
(CL1) (Config) # interface 0/13-0/16,3/1
(CL1) (Interface 0/13-0/16,3/1) # no shutdown
(CL1) (Interface 0/13-0/16,3/1) # exit
(CL1) (Config) # exit
(CL1) #
```

9. Überprüfen Sie, ob es sich bei den ISLs um handelt `up` Am CN1610-Schalter CL1.

Der „Verbindungsstatus“ sollte sein `Up`, "Typ" sollte sein `Dynamic`, Und die Spalte "Port Active" sollte sein

True Für Ports 0/13 bis 0/16.

Beispiel anzeigen

Im folgenden Beispiel werden die ISLs angezeigt, die als verifiziert werden up Am CN1610-Schalter CL1:

```
(CL1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed      Active
-----
0/13      actor/long    10 Gb Full  True
          partner/long
0/14      actor/long    10 Gb Full  True
          partner/long
0/15      actor/long    10 Gb Full  True
          partner/long
0/16      actor/long    10 Gb Full  True
          partner/long
```

10. Überprüfen Sie, ob es sich bei den ISLs um handelt up Am 3232C-Switch C2:

```
show port-channel summary
```

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Die Ports eth1/24/1 bis eth1/24/4 sollten angegeben werden (P) , Das bedeutet, dass alle vier ISL-Ports im Port-Kanal aktiv sind. Eth1/31 und eth1/32 sollten angegeben werden (D) Da sie nicht verbunden sind.

Beispiel anzeigen

Im folgenden Beispiel werden die ISLs angezeigt, die als verifiziert werden up Am 3232C-Switch C2:

```
C2# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth      LACP      Eth1/31 (D)  Eth1/32 (D)
2      Po2 (SU)       Eth      LACP      Eth1/24/1 (P) Eth1/24/2 (P)
Eth1/24/3 (P)
                                   Eth1/24/4 (P)
```

11. Alle Cluster-Interconnect-Ports, die auf allen Knoten mit dem 3232C-Switch C2 verbunden sind, werden verfügbar:

```
network port modify -node node-name -port port-name -up-admin true
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die mit dem 3232C-Switch C2 verbundenen Cluster-Interconnect-Ports geöffnet werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

12. Zurücksetzen aller migrierten Cluster-Interconnect-LIFs, die auf allen Nodes mit C2 verbunden sind:

```
network interface revert -vserver cluster -lif lif-name
```

Beispiel anzeigen

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2  
cluster::*> network interface revert -vserver cluster -lif n1_clus3  
cluster::*> network interface revert -vserver cluster -lif n2_clus2  
cluster::*> network interface revert -vserver cluster -lif n2_clus3
```

13. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports auf die Home-Ports zurückgesetzt werden:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die LIFs auf clu2 auf ihre Home-Ports zurückgesetzt werden. Die LIFs werden erfolgreich zurückgesetzt, wenn die Ports in der Spalte „Current Port“ den Status von aufweisen `true` in der Spalte „is Home“. Wenn der Wert „ist zu Hause“ lautet `false`, Dann ist das LIF nicht zurückgesetzt.

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current      Current      Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
-----
Cluster
true      n1_clus1      up/up      10.10.0.1/24      n1      e0a
true      n1_clus2      up/up      10.10.0.2/24      n1      e0b
true      n1_clus3      up/up      10.10.0.3/24      n1      e0c
true      n1_clus4      up/up      10.10.0.4/24      n1      e0d
true      n2_clus1      up/up      10.10.0.5/24      n2      e0a
true      n2_clus2      up/up      10.10.0.6/24      n2      e0b
true      n2_clus3      up/up      10.10.0.7/24      n2      e0c
true      n2_clus4      up/up      10.10.0.8/24      n2      e0d

8 entries were displayed.
```

14. Vergewissern Sie sich, dass alle Cluster-Ports verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt die Ausgabe, bei der alle Cluster Interconnects überprüft werden up:

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

```
(network port show)
```

Node: n1

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

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

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

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	
e0d	cluster	cluster	up	9000	auto/10000	-	

8 entries were displayed.

15. Pingen Sie die Remote-Cluster-Schnittstellen und führen Sie dann eine Remote-Prozedur aus Rufen Sie den Server an:

```
cluster ping-cluster -node node-name
```


Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

16. Migrieren Sie die LIFs, die mit dem ersten CN1610 Switch CL1 verbunden sind:

```
network interface migrate -vserver cluster -lif lif-name -source-node node-name
```

Beispiel anzeigen

Sie müssen jede Cluster-LIF individuell zu den entsprechenden Cluster-Ports migrieren, die auf Cluster-Switch C2 gehostet werden, wie im folgenden Beispiel dargestellt:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1  
-source-node n1  
-destination-node n1 -destination-port e0b  
cluster::*> network interface migrate -vserver cluster -lif n1_clus4  
-source-node n1  
-destination-node n1 -destination-port e0c  
cluster::*> network interface migrate -vserver cluster -lif n2_clus1  
-source-node n2  
-destination-node n2 -destination-port e0b  
cluster::*> network interface migrate -vserver cluster -lif n2_clus4  
-source-node n2  
-destination-node n2 -destination-port e0c
```

Schritt 3: Ersetzen Sie den Cluster-Switch CL1 durch C1

1. Überprüfen Sie den Status des Clusters:

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

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, dass die erforderlichen Cluster-LIFs zu den entsprechenden Cluster-Ports migriert wurden, die auf Cluster-Switch gehostet werden.C2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current      Current      Is
Vserver Interface  Admin/Oper  Address/Mask  Node         Port
Home
-----
-----
Cluster
false      n1_clus1      up/up      10.10.0.1/24  n1           e0b
true       n1_clus2      up/up      10.10.0.2/24  n1           e0b
true       n1_clus3      up/up      10.10.0.3/24  n1           e0c
false      n1_clus4      up/up      10.10.0.4/24  n1           e0c
false      n2_clus1      up/up      10.10.0.5/24  n2           e0b
false      n2_clus2      up/up      10.10.0.6/24  n2           e0b
true       n2_clus3      up/up      10.10.0.7/24  n2           e0c
true       n2_clus4      up/up      10.10.0.8/24  n2           e0c
false

8 entries were displayed.
```

2. Fahren Sie die Node-Ports, die auf allen Nodes mit CL1 verbunden sind, herunter:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Im folgenden Beispiel werden bestimmte Ports an den Knoten n1 und n2 heruntergefahren:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

3. Fahren Sie die ISL-Ports 24, 31 und 32 am aktiven 3232C-Switch C2 herunter.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt, dass ISLs 24, 31 und 32 am aktiven 3232C-Switch C2 heruntergefahren werden:

```
C2# configure
C2(config)# interface ethernet 1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
C2#
```

4. Entfernen Sie die Kabel, die an allen Knoten am CN1610-Switch CL1 angeschlossen sind.

Mithilfe der entsprechenden Verkabelung müssen Sie die getrennten Ports auf allen Nodes wieder an den Nexus 3232C Switch C1 anschließen.

5. Entfernen Sie die QSFP28-Kabel vom Nexus 3232C C2-Port e1/24.

Sie müssen die Ports e1/31 und e1/32 an C1 mit den Ports e1/31 und e1/32 auf C2 verbinden, die die unterstützten Cisco QSFP28-Glasfaserkabel oder Direct-Attach-Kabel verwenden.

6. Stellen Sie die Konfiguration an Port 24 wieder her, und entfernen Sie den temporären Port-Kanal 2 auf C2:

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt die running-configuration Datei, die in die kopiert wird startup-configuration Datei:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 100GbE/40GbE Node Port
C2(config-if)# spanning-tree port type edge
Edge port type (portfast) should only be enabled on ports connected
to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet 1/24 but
will only
have effect when the interface is in a non-trunking mode.

C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

7. ISL-Ports 31 und 32 auf C2, dem aktiven 3232C-Switch, herausholen.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt, dass ISLs 31 und 32 auf den 3232C-Switch C2 gebracht werden:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

8. Stellen Sie sicher, dass die ISL-Verbindungen sind up Am 3232C-Switch C2.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt die zu prüfenden ISL-Verbindungen. Die Ports eth1/31 und eth1/32 werden angezeigt (P), Was bedeutet, dass beide ISL-Ports sind `up` Im Port-Kanal:

```
C1# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
```

```
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
```

```
C2# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
```

```
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
```

9. Alle mit dem neuen 3232C-Switch C1 verbundenen Cluster-Interconnect-Ports auf allen Knoten:

```
network port modify -node node-name -port port-name -up-admin true
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Interconnect-Ports angezeigt, die mit dem neuen 3232C-Switch C1 verbunden sind.

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

10. Überprüfen Sie den Status des Cluster-Node-Ports:

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


Beispiel anzeigen

Das folgende Beispiel zeigt die Ausgabe, die überprüft, ob die Cluster-Interconnect-Ports an den Knoten n1 und n2 auf dem neuen 3232C-Switch C1 sind up:

```
cluster::*> network port show -role cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status                                     Admin/Open    Status    Health
-----
-----
e0a   cluster  cluster    up    9000  auto/10000    -       -
e0b   cluster  cluster    up    9000  auto/10000    -       -
e0c   cluster  cluster    up    9000  auto/10000    -       -
e0d   cluster  cluster    up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status                                     Admin/Open    Status    Health
-----
-----
e0a   cluster  cluster    up    9000  auto/10000    -       -
e0b   cluster  cluster    up    9000  auto/10000    -       -
e0c   cluster  cluster    up    9000  auto/10000    -       -
e0d   cluster  cluster    up    9000  auto/10000    -       -

8 entries were displayed.
```

Schritt 4: Führen Sie den Vorgang durch

1. Zurücksetzen aller migrierten Cluster-Interconnect-LIFs, die ursprünglich auf allen Knoten mit C1 verbunden waren:

```
network interface revert -server cluster -lif lif-name
```

Beispiel anzeigen

Sie müssen jede LIF individuell wie im folgenden Beispiel gezeigt migrieren:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n1_clus4
cluster::*> network interface revert -vserver cluster -lif n2_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus4
```

2. Vergewissern Sie sich, dass die Schnittstelle jetzt die Startseite ist:

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

Beispiel anzeigen

Im folgenden Beispiel wird der Status von Cluster-Interconnect-Schnittstellen angezeigt up Und „IS Home“ für Knoten n1 und n2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current      Current      Is
Vserver Interface Admin/Oper Address/Mask Node      Port
Home
-----
-----
Cluster
true      n1_clus1      up/up      10.10.0.1/24      n1      e0a
true      n1_clus2      up/up      10.10.0.2/24      n1      e0b
true      n1_clus3      up/up      10.10.0.3/24      n1      e0c
true      n1_clus4      up/up      10.10.0.4/24      n1      e0d
true      n2_clus1      up/up      10.10.0.5/24      n2      e0a
true      n2_clus2      up/up      10.10.0.6/24      n2      e0b
true      n2_clus3      up/up      10.10.0.7/24      n2      e0c
true      n2_clus4      up/up      10.10.0.8/24      n2      e0d

8 entries were displayed.
```

3. Pingen Sie die Remote-Cluster-Schnittstellen und führen Sie dann eine Remote-Prozedur aus Rufen Sie den Server an:

```
cluster ping-cluster -node host-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
3  paths up, 0 paths down (udp check)
```

4. Erweitern Sie den Cluster durch Hinzufügen von Nodes zu den Nexus 3232C Cluster-Switches.

5. Zeigen Sie die Informationen zu den Geräten in Ihrer Konfiguration an:

- ° `network device-discovery show`
- ° `network port show -role cluster`
- ° `network interface show -role cluster`
- ° `system cluster-switch show`

Beispiel anzeigen

Die folgenden Beispiele zeigen die Nodes n3 und n4 mit 40-GbE-Cluster-Ports, die mit den Ports e1/7 bzw. e1/8 verbunden sind, auf beiden Nexus 3232C-Cluster-Switches. Beide Nodes sind dem Cluster verbunden. Die 40 GbE Cluster Interconnect Ports sind e4a und e4e.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0d	C1	Ethernet1/1/2	N3K-C3232C
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
n3	/cdp			
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
	e4a	C1	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4e	C2	Ethernet1/7	N3K-C3232C
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

12 entries were displayed.

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

```
(network port show)
```

Node: n1

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

e0a	cluster	cluster	up	9000	auto/10000	-	
e0b	cluster	cluster	up	9000	auto/10000	-	
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
e0a	cluster	cluster	up	9000	auto/10000	-
e0b	cluster	cluster	up	9000	auto/10000	-
e0c	cluster	cluster	up	9000	auto/10000	-
e0d	cluster	cluster	up	9000	auto/10000	-

Node: n3

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					
-----	-----	-----	-----	-----	-----	-----
e4a	cluster	cluster	up	9000	auto/40000	-
e4e	cluster	cluster	up	9000	auto/40000	-

Node: n4

		Broadcast			Speed (Mbps)	Health
Ignore						
Port	IPspace	Domain	Link	MTU	Admin/Open	Status
Health	Status					
-----	-----	-----	-----	-----	-----	-----
e4a	cluster	cluster	up	9000	auto/40000	-
e4e	cluster	cluster	up	9000	auto/40000	-

12 entries were displayed.

cluster::*> **network interface show -role cluster**

(network interface show)

		Logical	Status	Network	Current	Current
Is						
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	
Home						

Cluster						
true	n1_clus1	up/up	10.10.0.1/24	n1	e0a	
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	

```

true
      n1_clus3   up/up      10.10.0.3/24   n1      e0c
true
      n1_clus4   up/up      10.10.0.4/24   n1      e0d
true
      n2_clus1   up/up      10.10.0.5/24   n2      e0a
true
      n2_clus2   up/up      10.10.0.6/24   n2      e0b
true
      n2_clus3   up/up      10.10.0.7/24   n2      e0c
true
      n2_clus4   up/up      10.10.0.8/24   n2      e0d
true
      n3_clus1   up/up      10.10.0.9/24   n3      e4a
true
      n3_clus2   up/up      10.10.0.10/24  n3      e4e
true
      n4_clus1   up/up      10.10.0.11/24  n4      e4a
true
      n4_clus2   up/up      10.10.0.12/24  n4      e4e
true

```

12 entries were displayed.

cluster::> **system cluster-switch show**

Switch	Type	Address	Model
-----	-----	-----	

C1	cluster-network	10.10.1.103	
NX3232C			

Serial Number: FOX000001

Is Monitored: true

Reason:

Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version

7.0(3)I6(1)

Version Source: CDP

C2	cluster-network	10.10.1.104	
NX3232C			

Serial Number: FOX000002

Is Monitored: true

Reason:


```

Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
              7.0(3)I6(1)
Version Source: CDP
CL1              cluster-network  10.10.1.101    CN1610

Serial Number: 01234567
Is Monitored: true
Reason:
Software Version: 1.2.0.7
Version Source: ISDP
CL2              cluster-network  10.10.1.102
CN1610

Serial Number: 01234568
Is Monitored: true
Reason:
Software Version: 1.2.0.7
Version Source: ISDP 4 entries were displayed.

```

6. Entfernen Sie die ausgetauschten CN1610-Schalter, wenn sie nicht automatisch entfernt werden:

```
system cluster-switch delete -device switch-name
```

Beispiel anzeigen

Sie müssen beide Geräte einzeln löschen, wie im folgenden Beispiel gezeigt:

```

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

```

7. Überprüfen Sie, ob die richtigen Cluster-Switches überwacht werden:

```
system cluster-switch show
```

Beispiel anzeigen

Im folgenden Beispiel werden die Cluster-Switches C1 und C2 überwacht:

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.104
Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP		

2 entries were displayed.

8. Aktivieren Sie die Protokollerfassung für die Cluster Switch-Systemzustandsüberwachung zum Erfassen von Switch-bezogenen Protokolldateien:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

9. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Migration von einem Cisco Nexus 5596 Cluster-Switch zu einem Cisco Nexus 3232C-Cluster-Switch

So migrieren Sie vorhandene Cisco Nexus 5596 Cluster-Switches in einem Cluster mit Nexus 3232C-Cluster-Switches.

Prüfen Sie die Anforderungen

Vor der Migration sollten Sie unbedingt prüfen ["Migrationsanforderungen"](#).



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Weitere Informationen finden Sie unter:

- ["Beschreibungsseite für den Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Migrieren Sie den Switch

Zu den Beispielen

Die Beispiele in diesem Verfahren beschreiben, wie Cisco Nexus 5596 Switches durch Cisco Nexus 3232C-Switches ersetzt werden. Sie können diese Schritte (mit Änderungen) für andere ältere Cisco Switches (z. B. 3132Q-V) verwenden.

Weiterhin verwendet das Verfahren die folgende Nomenklatur für Switches und Nodes:

- Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.
- Die zu ersetzenden Nexus 5596 Switches sind CL1 und CL2.
- Die Switches der Nexus 3232C-Serie als Ersatz für die Nexus 5596-Switches sind C1 und C2.
- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die mit Cluster-Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- n1_clus2 ist die erste Cluster-LIF, die mit Cluster-Switch 2 (CL2 oder C2) für Node n1 verbunden ist.
- n1_clus3 ist die zweite logische Schnittstelle, die mit Cluster Switch 2 (CL2 oder C2) für Knoten n1 verbunden ist.
- n1_clus4 ist die zweite logische Schnittstelle, die mit Cluster Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.-
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert ["Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen"](#) Seite.
- Die Knoten sind n1, n2, n3 und n4.

Die Beispiele in diesem Verfahren verwenden vier Knoten:

- Zwei Nodes verwenden vier 10-GbE-Cluster-Interconnect-Ports: e0a, e0b, e0c und e0d.
- Die anderen beiden Knoten verwenden zwei 40 GbE Cluster Interconnect Ports: e4a, e4e. Der ["Hardware Universe"](#) Listet die tatsächlichen Cluster-Ports auf Ihren Plattformen auf.

Szenarien

Dieses Verfahren umfasst folgende Szenarien:

- Das Cluster beginnt mit zwei verbundenen Nodes und funktioniert in zwei Nexus 5596-Cluster-Switches.
- Der zu ersetzende Cluster-Switch CL2 (Schritt 1 bis 19):
 - Der Traffic auf allen Cluster-Ports und LIFs auf allen mit CL2 verbundenen Nodes wird zu den ersten Cluster-Ports migriert und mit CL1 verbundene LIFs.
 - Trennen Sie die Verkabelung von allen Cluster-Ports auf allen mit CL2 verbundenen Nodes, und verwenden Sie dann die unterstützte Breakout-Verkabelung, um die Ports wieder mit dem neuen Cluster-Switch C2 zu verbinden.
 - Trennen Sie die Verkabelung zwischen ISL-Ports zwischen CL1 und CL2, und verwenden Sie dann die unterstützte Breakout-Verkabelung, um die Ports von CL1 an C2 wiederherzustellen.
 - Der Datenverkehr auf allen Cluster-Ports und LIFs, die mit C2 verbunden sind, wird auf allen Nodes zurückgesetzt.
- Der Cluster-Switch CL2, der durch C2 ersetzt werden soll.
 - Der Datenverkehr aller Cluster-Ports oder LIFs auf allen mit CL1 verbundenen Nodes wird zu den zweiten Cluster-Ports oder zu LIFs migriert, die mit C2 verbunden sind.
 - Trennen Sie die Verkabelung von allen Cluster-Ports auf allen mit CL1 verbundenen Knoten, und verbinden Sie sie über unterstützte Breakout-Kabel mit dem neuen Cluster-Switch C1.
 - Trennen Sie die Verkabelung zwischen ISL-Ports zwischen CL1 und C2, und schließen Sie sie über unterstützte Kabel von C1 bis C2 wieder an.
 - Der Verkehr auf allen Cluster-Ports oder LIFs, die mit C1 auf allen Nodes verbunden sind, wird zurückgesetzt.
- Zwei FAS9000 Nodes wurden dem Cluster hinzugefügt, wobei Beispiele für Cluster-Details zeigen.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device-discovery show
```

Beispiel anzeigen

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

```
cluster::> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform
-----	-----	-----	-----	-----
n1	/cdp			
	e0a	CL1	Ethernet1/1	N5K-C5596UP
	e0b	CL2	Ethernet1/1	N5K-C5596UP
	e0c	CL2	Ethernet1/2	N5K-C5596UP
	e0d	CL1	Ethernet1/2	N5K-C5596UP
n2	/cdp			
	e0a	CL1	Ethernet1/3	N5K-C5596UP
	e0b	CL2	Ethernet1/3	N5K-C5596UP
	e0c	CL2	Ethernet1/4	N5K-C5596UP
	e0d	CL1	Ethernet1/4	N5K-C5596UP

8 entries were displayed.

3. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

a. Zeigen Sie die Attribute des Netzwerkports an:

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

Beispiel anzeigen

Im folgenden Beispiel werden die Netzwerkanschlussattribute an den Knoten n1 und n2 angezeigt:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e0a         Cluster      Cluster      up    9000  auto/10000  -
-
e0b         Cluster      Cluster      up    9000  auto/10000  -
-
e0c         Cluster      Cluster      up    9000  auto/10000  -
-
e0d         Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e0a         Cluster      Cluster      up    9000  auto/10000  -
-
e0b         Cluster      Cluster      up    9000  auto/10000  -
-
e0c         Cluster      Cluster      up    9000  auto/10000  -
-
e0d         Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

b. Informationen zu den logischen Schnittstellen anzeigen:

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

Beispiel anzeigen

Im folgenden Beispiel werden die allgemeinen Informationen zu allen LIFs auf dem Cluster, einschließlich ihrer aktuellen Ports, angezeigt:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask  Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3      up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3      up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

c. Informationen über die erkannten Cluster-Switches anzeigen:

```
system cluster-switch show
```


Beispiel anzeigen

Im folgenden Beispiel werden die aktiven Cluster-Switches angezeigt:

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

2 entries were displayed.

4. Vergewissern Sie sich, dass die entsprechenden RCF und das entsprechende Image auf den neuen 3232C-Switches installiert sind, wenn dies für Ihre Anforderungen erforderlich ist, und nehmen Sie die wesentlichen Änderungen an der Website vor, z. B. Benutzer und Passwörter, Netzwerkadressen und andere Anpassungen.



Sie müssen beide Switches derzeit vorbereiten.

Wenn Sie ein RCF- und Image-Upgrade durchführen müssen, müssen Sie die folgenden Schritte ausführen:

- a. Wechseln Sie auf der NetApp Support Site zur Seite *Cisco Ethernet Switches*.

["Cisco Ethernet-Switches"](#)

- b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.

- c. Laden Sie die entsprechende Version des RCF herunter.
- d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
- e. Laden Sie die entsprechende Version der Bildsoftware herunter.

Besuchen Sie die Seite *ONTAP 8.x oder höher Referenzkonfigurationsdateien für Cluster und Netzwerk-Management-Switches* herunterladen, und klicken Sie dann auf die entsprechende Version.

Informationen zur richtigen Version finden Sie auf der Download-Seite „ONTAP 8.x“ oder höher für Cluster-Netzwerk-Switch.

5. Migrieren Sie die LIFs, die mit dem zweiten Nexus 5596 Switch verbunden sind, der ersetzt werden soll:

```
network interface migrate -vserver vserver-name -lif lif-name -source-node
source-node-name - destination-node node-name -destination-port destination-
port-name
```

Beispiel anzeigen

Das folgende Beispiel zeigt die LIFs, die für die Knoten n1 und n2 migriert werden; die LIF-Migration muss auf allen Knoten durchgeführt werden:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

6. Überprüfen Sie den Systemzustand des Clusters:

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

Beispiel anzeigen

Im folgenden Beispiel wird der aktuelle Status jedes Clusters angezeigt:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
e0a      n1_clus1      up/up      10.10.0.1/24      n1
      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0a      false
      n1_clus3      up/up      10.10.0.3/24      n1
e0d      false
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0a      false
      n2_clus3      up/up      10.10.0.7/24      n2
e0d      false
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

Schritt 2: Ports konfigurieren

1. Fahren Sie die Cluster-Interconnect-Ports herunter, die physisch mit dem Switch CL2 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Die folgenden Befehle fahren die angegebenen Ports auf n1 und n2 herunter, die Ports müssen jedoch auf allen Knoten heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

2. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

3. Schließen Sie ISLs 41 bis 48 auf CL1, dem aktiven Nexus 5596 Switch mit Cisco `shutdown` Befehl.

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass ISLs 41 bis 48 am Nexus 5596-Switch CL1 heruntergefahren werden:

```
(CL1) # configure
(CL1) (Config) # interface e1/41-48
(CL1) (config-if-range) # shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

4. Mithilfe der entsprechenden Cisco Befehle können Sie eine temporäre ISL zwischen CL1 und C2 erstellen.

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass ein temporärer ISL zwischen CL1 und C2 eingerichtet wird:

```
C2# configure
C2 (config) # interface port-channel 2
C2 (config-if) # switchport mode trunk
C2 (config-if) # spanning-tree port type network
C2 (config-if) # mtu 9216
C2 (config-if) # interface breakout module 1 port 24 map 10g-4x
C2 (config) # interface e1/24/1-4
C2 (config-if-range) # switchport mode trunk
C2 (config-if-range) # mtu 9216
C2 (config-if-range) # channel-group 2 mode active
C2 (config-if-range) # exit
C2 (config-if) # exit
```

5. Entfernen Sie auf allen Knoten alle Kabel, die am Nexus 5596 Switch CL2 angeschlossen sind.

Verbinden Sie bei der unterstützten Verkabelung die getrennten Ports aller Nodes mit dem Nexus 3232C Switch C2.

6. Entfernen Sie alle Kabel vom Nexus 5596 Switch CL2.

Verbinden Sie die entsprechenden Cisco QSFP mit SFP+ Breakout-Kabel, die Port 1/24 am neuen Cisco 3232C Switch C2 an die Anschlüsse 45 bis 48 des vorhandenen Nexus 5596, CL1 anschließen.

- ISLs-Ports 45 bis 48 auf dem aktiven Nexus 5596 Switch CL1 wechseln

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISLs-Ports 45 bis 48 aufgerufen werden:

```
(CL1) # configure
(CL1) (Config) # interface e1/45-48
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

- Überprüfen Sie, ob es sich bei den ISLs um handelt ^{up} Beim Nexus 5596 Switch CL1.

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

Beispiel anzeigen

Das folgende Beispiel zeigt die Ports eth1/45 bis eth1/48 an, was bedeutet, dass die ISL-Ports laufen up im Port-Kanal.

```
CL1# 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
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth     LACP      Eth1/41 (D)  Eth1/42 (D)
Eth1/43 (D)
                                   Eth1/44 (D)  Eth1/45 (P)
Eth1/46 (P)
                                   Eth1/47 (P)  Eth1/48 (P)
```

9. Vergewissern Sie sich, dass die Schnittstellen eth1/45-48 bereits `Channel-Group 1 Mode Active` in ihrer laufenden Konfiguration aufweisen.
10. Auf allen Knoten alle Cluster-Interconnect-Ports anzeigen, die mit dem 3232C-Switch C2 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin true
```

Beispiel anzeigen

Im folgenden Beispiel werden die angegebenen Ports angezeigt, die auf den Knoten n1 und n2 aufgerufen werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

11. Stellen Sie auf allen Nodes alle migrierten Cluster-Interconnect-LIFs zurück, die mit C2 verbunden sind:

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


Beispiel anzeigen

Im folgenden Beispiel werden die migrierten Cluster-LIFs, die auf die Home-Ports zurückgesetzt werden:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

12. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports nun auf ihr Home zurückgesetzt werden:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die LIFs auf Fa.2 auf ihre Home-Ports zurückgesetzt werden und zeigt, dass die LIFs erfolgreich zurückgesetzt werden, wenn die Ports in der Spalte „Current Port“ den Status aufweisen true Im Is Home Spalte. Wenn der Is Home Wert ist false, Das LIF wurde nicht zurückgesetzt.

```
cluster::*> *network interface show -role cluster*
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3      up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3      up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

13. Vergewissern Sie sich, dass die Cluster-Ports verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt das Ergebnis des vorherigen `network port modify` Befehl, Überprüfung der Cluster Interconnects up:

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

```
Node: n2
```

```
Ignore
```

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

```
8 entries were displayed.
```

14. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

15. Migrieren Sie bei jedem Node im Cluster die Schnittstellen, die mit dem ersten Nexus 5596 Switch CL1 verbunden sind, der ersetzt werden soll:

```
network interface migrate -vserver vserver-name -lif lif-name -source-node  
source-node-name  
-destination-node destination-node-name -destination-port destination-port-  
name
```

Beispiel anzeigen

Im folgenden Beispiel werden die Ports oder LIFs angezeigt, die auf den Nodes n1 und n2 migriert werden:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1  
-source-node n1 -  
destination-node n1 -destination-port e0b  
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4  
-source-node n1 -  
destination-node n1 -destination-port e0c  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1  
-source-node n2 -  
destination-node n2 -destination-port e0b  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4  
-source-node n2 -  
destination-node n2 -destination-port e0c
```

16. Überprüfen Sie den Status des Clusters:

```
network interface show
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, dass die erforderlichen Cluster-LIFs zu geeigneten Cluster-Ports migriert wurden, die auf dem Cluster-Switch gehostet werden.C2:

```
cluster::*> network interface show
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0b	false			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0c	false			
	n2_clus1	up/up	10.10.0.5/24	n2
e0b	false			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0c	false			
8 entries were displayed.				
-----	-----	----		

17. Fahren Sie auf allen Nodes die Node-Ports herunter, die mit CL1 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Das folgende Beispiel zeigt die angegebenen Anschlüsse, die auf den Knoten n1 und n2 heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

18. Fahren Sie ISL 24, 31 und 32 am aktiven 3232C-Switch C2 herunter.

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

Beispiel anzeigen

Im folgenden Beispiel werden die ISLs beim Herunterfahren angezeigt:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if)# exit
C2#
```

19. Entfernen Sie auf allen Knoten alle Kabel, die am Nexus 5596 Switch CL1 angeschlossen sind.

Schließen Sie bei der unterstützten Verkabelung die getrennten Ports auf allen Knoten wieder an den Nexus 3232C Switch C1 an.

20. Entfernen Sie das QSFP-Breakout-Kabel von den Nexus 3232C C2-Ports e1/24.

Verbinden Sie die Ports e1/31 und e1/32 auf C1 mit den Ports e1/31 und e1/32 auf C2 unter Verwendung der unterstützten Cisco QSFP-Glasfaserkabel oder Direct-Attached-Kabel.

21. Stellen Sie die Konfiguration an Port 24 wieder her, und entfernen Sie den temporären Port Channel 2 auf C2.

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

Beispiel anzeigen

Das folgende Beispiel zeigt die Konfiguration an Port m24, die mit den entsprechenden Cisco Befehlen wiederhergestellt wird:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[] 100%
Copy Complete.
```

22. Holen Sie die ISL-Ports 31 und 32 auf C2, dem aktiven 3232C-Switch, indem Sie den folgenden Cisco-Befehl eingeben: `no shutdown`

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

Beispiel anzeigen

Im folgenden Beispiel werden die Befehle von Cisco angezeigt `switchname configure` Einschalten des 3232C-Switch C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
```

23. Stellen Sie sicher, dass die ISL-Verbindungen sind up Am 3232C-Switch C2.

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

Die Ports eth1/31 und eth1/32 sollten (P) angeben, was bedeutet, dass beide ISL-Ports im Port-Channel oben sind

Beispiel anzeigen

```
C1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

24. Auf allen Knoten alle Cluster-Interconnect-Ports anzeigen, die mit dem neuen 3232C-Switch C1 verbunden sind:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt alle Cluster-Interconnect-Ports, die für n1 und n2 auf dem 3232C-Switch C1 aufgerufen werden:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

25. Überprüfen Sie den Status des Cluster-Node-Ports:

```
network port show
```

Beispiel anzeigen

Im folgenden Beispiel wird überprüft, ob alle Cluster-Interconnect-Ports auf allen Nodes des neuen 3232C-Switch C1 aktiviert sind:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

26. Setzen Sie auf allen Nodes die spezifischen Cluster-LIFs auf ihre Home-Ports zurück:

```
network interface revert -server Cluster -lif lif-name
```

Beispiel anzeigen

Im folgenden Beispiel werden die spezifischen Cluster-LIFs angezeigt, die auf ihre Home-Ports auf den Nodes n1 und n2 zurückgesetzt werden:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1  
cluster::*> network interface revert -vserver Cluster -lif n1_clus4  
cluster::*> network interface revert -vserver Cluster -lif n2_clus1  
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

27. Vergewissern Sie sich, dass die Schnittstelle Home ist:

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

Beispiel anzeigen

Im folgenden Beispiel wird der Status von Cluster-Interconnect-Schnittstellen angezeigt up Und Is Home Für n1 und n2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3      up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3      up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

28. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

29. Erweitern Sie den Cluster durch Hinzufügen von Nodes zu den Nexus 3232C Cluster-Switches.

In den folgenden Beispielen werden die Nodes n3 und n4 mit 40-GbE-Cluster-Ports verbunden, die mit den Ports e1/7 und e1/8 verbunden sind und beide Nodes dem Cluster verbunden sind. Die 40 GbE Cluster Interconnect Ports sind e4a und e4e.

Zeigen Sie die Informationen zu den Geräten in Ihrer Konfiguration an:

- ° `network device-discovery show`
- ° `network port show -role cluster`
- ° `network interface show -role cluster`
- ° `system cluster-switch show`

Beispiel anzeigen

```
cluster::> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

12 entries were displayed.

+

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a       Cluster      Cluster      up    9000  auto/10000  -
-
e0b       Cluster      Cluster      up    9000  auto/10000  -
-
e0c       Cluster      Cluster      up    9000  auto/10000  -
-
e0d       Cluster      Cluster      up    9000  auto/10000  -
```


-

Node: n2

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	-----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n3

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	-----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

Node: n4

Ignore

						Speed (Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	-----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-

-
12 entries were displayed.

+

```
cluster::*> network interface show -role cluster
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

12 entries were displayed.

+

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

```
4 entries were displayed.
```

30. Entfernen Sie den ausgetauschten Nexus 5596 mit dem `system cluster-switch delete` Befehl, wenn er nicht automatisch entfernt wird:

```
system cluster-switch delete -device switch-name
```

Beispiel anzeigen

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

Schritt 3: Führen Sie den Vorgang durch

1. Überprüfen Sie, ob die richtigen Cluster-Switches überwacht werden:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

2. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

3. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Migrieren Sie mit Cisco Nexus 3232C Cluster-Switches von einem Cluster mit zwei Nodes ohne Switches zu einem Cluster

Wenn Sie über einen 2-Node-Switch-Cluster verfügen, können Sie zu einem Switched Cluster mit zwei Nodes migrieren, der Cisco Nexus 3232C-Cluster-Netzwerk-Switches enthält. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Migrationsanforderungen

Vor der Migration sollten Sie unbedingt prüfen ["Migrationsanforderungen"](#).

Was Sie benötigen

Stellen Sie sicher, dass:

- Für Node-Verbindungen sind Ports verfügbar. Die Cluster-Switches verwenden die Inter-Switch-Link-Ports (ISL) e1/31-32.
- Sie verfügen über die entsprechenden Kabel für Cluster-Verbindungen:
 - Die Nodes mit 10 GbE-Cluster-Verbindungen erfordern optische QSFP-Module mit Breakout-Glasfaserkabeln oder QSFP zu SFP+ Kupfer-Breakout-Kabeln.
 - Die Nodes mit 40/100 GbE-Cluster-Verbindungen erfordern unterstützte optische QSFP/QSFP28-Module mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direct-Attach-Kabeln.
 - Die Cluster-Switches erfordern die entsprechende ISL-Verkabelung: 2 QSFP28-Glasfaser- oder Kupfer-Direct-Attached-Kabel.
- Die Konfigurationen sind ordnungsgemäß eingerichtet und funktionieren ordnungsgemäß.

Die beiden Nodes müssen verbunden und in einer 2-Node-Cluster-Einstellung ohne Switches funktionieren.

- Alle Cluster-Ports haben den Status **up**.
- Der Cisco Nexus 3232C Cluster-Switch wird unterstützt.
- Die vorhandene Cluster-Netzwerkconfiguration verfügt über folgende Merkmale:
 - Eine redundante und voll funktionsfähige Nexus 3232C-Cluster-Infrastruktur auf beiden Switches
 - Die neuesten RCF- und NX-OS-Versionen auf Ihren Switches
 - Management-Konnektivität auf beiden Switches
 - Konsolenzugriff auf beide Switches
 - Alle Cluster-logischen Schnittstellen (LIFs) im Status **up** ohne migriert zu haben
 - Erstanpassung des Schalters
 - Alle ISL-Ports sind aktiviert und verkabelt

Migrieren Sie die Switches

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Nexus 3232C Cluster Switches, C1 und C2.
- Die Knoten sind n1 und n2.

Die Beispiele in diesem Verfahren verwenden zwei Knoten, von denen jeder zwei 40 GbE Cluster Interconnect Ports e4a und e4e nutzt. Der "[Hardware Universe](#)" Enthält Details zu den Cluster-Ports auf Ihren Plattformen.

- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die für Knoten n1 mit Cluster-Switch C1 verbunden werden soll.
- n1_clus2 ist die erste Cluster-LIF, die für Node n1 mit Cluster-Switch C2 verbunden wird.
- n2_clus1 ist die erste Cluster-LIF, die für Knoten n2 mit Cluster-Switch C1 verbunden wird.
- n2_clus2 ist die zweite Cluster-LIF, die für Knoten n2 an Cluster-Switch C2 angeschlossen werden soll.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert "[Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen](#)" Seite.



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritt: Physische und logische Ports anzeigen und migrieren

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Legen Sie den Administrations- oder Betriebsstatus für jede Cluster-Schnittstelle fest:

- a. Zeigen Sie die Attribute des Netzwerkports an:

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


Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health
Port        IPspace    Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster    Cluster    up    9000 auto/40000 -
e4e         Cluster    Cluster    up    9000 auto/40000 -
-
Node: n2

Ignore

Health      Health
Port        IPspace    Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster    Cluster    up    9000 auto/40000 -
e4e         Cluster    Cluster    up    9000 auto/40000 -
4 entries were displayed.
```

- b. Informationen zu den logischen Schnittstellen und den zugehörigen Home-Nodes anzeigen:

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

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true

4 entries were displayed.
```

- c. Überprüfen Sie mithilfe des erweiterten Berechtigungsbefehls, ob die Cluster-Erkennung ohne Switch aktiviert ist:

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

Beispiel anzeigen

Die Ausgabe im folgenden Beispiel zeigt, dass die Cluster-Erkennung ohne Switches aktiviert ist:

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

3. Vergewissern Sie sich, dass die entsprechenden RCs und das entsprechende Image auf den neuen 3232C-Switches installiert sind und nehmen Sie alle erforderlichen Standortanpassungen vor, z. B. das Hinzufügen von Benutzern, Passwörtern und Netzwerkadressen.

Sie müssen beide Switches derzeit vorbereiten. Wenn Sie die RCF- und Bildsoftware aktualisieren müssen, müssen Sie folgende Schritte ausführen:

- a. Wechseln Sie auf der NetApp Support Site zur Seite *Cisco Ethernet Switches*.

["Cisco Ethernet-Switches"](#)

- b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
- c. Laden Sie die entsprechende RCF-Version herunter.
- d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
- e. Laden Sie die entsprechende Version der Bildsoftware herunter.

["Download-Seite für die Referenzkonfigurationsdatei für den Cisco Cluster- und Management-Netzwerk-Switch"](#)

- 4. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
- 5. Bei den Nexus 3232C-Switches C1 und C2 deaktivieren Sie alle Ports C1 und C2 für Knoten, deaktivieren Sie aber nicht die ISL-Ports e1/31-32.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt die Ports 1 bis 30, die bei Nexus 3232C-Cluster-Switches C1 und C2 unter Verwendung einer in RCF unterstützten Konfiguration deaktiviert sind
NX3232_RCF_v1.0_24p10g_24p100g.txt:

```
C1# copy running-config startup-config
[] 100% Copy complete.
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# shutdown
C1(config-if-range)# exit
C1(config)# exit
C2# copy running-config startup-config
[] 100% Copy complete.
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
```

- 6. Verbinden Sie die Ports 1/31 und 1/32 auf C1 mit den gleichen Ports auf C2, indem Sie die unterstützten Kabel verwenden.
- 7. Überprüfen Sie, ob die ISL-Ports auf C1 und C2 funktionsfähig sind:

```
show port-channel summary
```

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-](#)

Beispiel anzeigen

Das folgende Beispiel zeigt Cisco `show port-channel summary` Mit diesem Befehl wird sichergestellt, dass die ISL-Ports auf C1 und C2 funktionsfähig sind:

```
C1# 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
      S - Switched      R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
      Port-
Group Channel          Type    Protocol  Member Ports
-----
-----
1      Po1 (SU)        Eth    LACP      Eth1/31 (P)  Eth1/32 (P)

C2# 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
      S - Switched      R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----

Group Port-          Type    Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)        Eth    LACP      Eth1/31 (P)  Eth1/32 (P)
```

8. Zeigen Sie die Liste der benachbarten Geräte auf dem Switch an.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Im folgenden Beispiel wird der Befehl Cisco angezeigt `show cdp neighbors` Wird zur Anzeige der benachbarten Geräte auf dem Switch verwendet:

```
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
C2                  Eth1/31       174      R S I s          N3K-C3232C
Eth1/31
C2                  Eth1/32       174      R S I s          N3K-C3232C
Eth1/32
Total entries displayed: 2
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
C1                  Eth1/31       178      R S I s          N3K-C3232C
Eth1/31
C1                  Eth1/32       178      R S I s          N3K-C3232C
Eth1/32
Total entries displayed: 2
```

9. Zeigen Sie die Cluster-Port-Konnektivität auf jedem Node an:

```
network device-discovery show
```

Beispiel anzeigen

Im folgenden Beispiel wird die Cluster-Port-Konnektivität für eine Konfiguration mit zwei Nodes ohne Switches angezeigt:

```
cluster::*> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e4a	n2	e4a	FAS9000
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	n1	e4a	FAS9000
	e4e	n1	e4e	FAS9000

10. Migrieren Sie die LIFs n1_clus1 und n2_clug1 zu den physischen Ports ihrer Ziel-Knoten:

```
network interface migrate -vserver vserver-name -lif lif-name source-node  
source-node-name -destination-port destination-port-name
```

Beispiel anzeigen

Sie müssen den Befehl für jeden lokalen Node ausführen, wie im folgenden Beispiel gezeigt:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus1  
-source-node n1  
-destination-node n1 -destination-port e4e  
cluster::*> network interface migrate -vserver cluster -lif n2_clus1  
-source-node n2  
-destination-node n2 -destination-port e4e
```

Schritt 2: Schalten Sie die neu zugeordneten LIFs ab und trennen Sie die Kabel

1. Überprüfen Sie, ob die Cluster-Schnittstellen erfolgreich migriert wurden:

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

Beispiel anzeigen

Das folgende Beispiel zeigt den Status „is Home“ für die LIFs n1_clus1 und n2_clug1 ist nach Abschluss der Migration „false“ geworden:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4e      false
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4e      false
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

2. Beenden Sie die Cluster-Ports für die LIFs n1_clus1 und n2_clue1, die in Schritt 9 migriert wurden:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Sie müssen den Befehl für jeden Port ausführen, wie im folgenden Beispiel gezeigt:

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

3. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::*> cluster ping-cluster -node n1

Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e4a      10.10.0.1
Cluster n1_clus2 n1          e4e      10.10.0.2
Cluster n2_clus1 n2          e4a      10.10.0.3
Cluster n2_clus2 n2          e4e      10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
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 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

4. Trennen Sie das Kabel von e4a am Knoten n1.

Sie können sich auf die laufende Konfiguration beziehen und den ersten 40-GbE-Port am Switch C1 (Port 1/7 in diesem Beispiel) mit e4a auf n1 verbinden, indem die Verkabelung unterstützt für Nexus 3232C-Switches.

Schritt 3: Aktivieren Sie die Cluster-Ports

1. Trennen Sie das Kabel von e4a auf Knoten n2.

Sie können sich auf die laufende Konfiguration beziehen und e4a mit dem nächsten verfügbaren 40 GbE-Port von C1, Port 1/8, über unterstützte Verkabelung verbinden.

2. Aktivieren Sie alle Ports, die an Knoten gerichtet sind, auf C1.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Das folgende Beispiel zeigt die Ports 1 bis 30, die bei Nexus 3232C-Cluster-Switches C1 und C2 unter Verwendung der in RCF unterstützten Konfiguration aktiviert sind

NX3232_RCF_v1.0_24p10g_26p100g.txt:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

3. Aktivieren Sie den ersten Cluster-Port e4a auf jedem Knoten:

```
network port modify -node node-name -port port-name -up-admin true
```

Beispiel anzeigen

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

4. Vergewissern Sie sich, dass die Cluster auf beiden Nodes aktiv sind:

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

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a       Cluster      Cluster      up    9000 auto/40000 -
e4e       Cluster      Cluster      up    9000 auto/40000 -
-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a       Cluster      Cluster      up    9000 auto/40000 -
e4e       Cluster      Cluster      up    9000 auto/40000 -

4 entries were displayed.
```

5. Setzen Sie für jeden Node alle migrierten Cluster Interconnect LIFs zurück:

```
network interface revert -vserver cluster -lif lif-name
```

Beispiel anzeigen

Sie müssen jede LIF einzeln wie im folgenden Beispiel gezeigt auf ihren Home-Port zurücksetzen:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus1
cluster::*> network interface revert -vserver cluster -lif n2_clus1
```

6. Vergewissern Sie sich, dass alle LIFs nun auf ihre Home-Ports zurückgesetzt werden:

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

Der Is Home Spalte sollte einen Wert von anzeigen true Für alle im aufgeführten Ports Current Port Spalte. Wenn der angezeigte Wert lautet false, Der Hafen wurde nicht zurückgesetzt.

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

Schritt 4: Aktivieren Sie die neu signierten LIFs

1. Zeigen Sie die Cluster-Port-Konnektivität auf jedem Node an:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster::*> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	n1	e4e	FAS9000

2. Migrieren von Fazit 2 zu Port e4a auf der Konsole jedes Knotens:

```
network interface migrate cluster -lif lif-name -source-node source-node-name  
-destination-node destination-node-name -destination-port destination-port-  
name
```

Beispiel anzeigen

Sie müssen jede LIF individuell wie im folgenden Beispiel dargestellt zu ihrem Home Port migrieren:

```
cluster::*> network interface migrate -vserver cluster -lif n1_clus2  
-source-node n1  
-destination-node n1 -destination-port e4a  
cluster::*> network interface migrate -vserver cluster -lif n2_clus2  
-source-node n2  
-destination-node n2 -destination-port e4a
```

3. Herunterfahren von Cluster-Ports clu2 LIF auf beiden Knoten:

```
network port modify
```

Beispiel anzeigen

Im folgenden Beispiel werden die angegebenen Ports angezeigt, die auf festgelegt sind false, Herunterfahren der Ports auf beiden Nodes:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false  
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

4. Überprüfen Sie den LIF-Status des Clusters:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4a      false
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4a      false
4 entries were displayed.
```

5. Trennen Sie das Kabel von e4e am Knoten n1.

Sie können auf die laufende Konfiguration verweisen und den ersten 40-GbE-Port am Switch C2 (Port 1/7 in diesem Beispiel) mit e4e am Node n1 verbinden. Dabei wird die entsprechende Verkabelung für das Nexus 3232C-Switch-Modell verwendet.

6. Trennen Sie das Kabel von e4e am Knoten n2.

Sie können sich auf die laufende Konfiguration beziehen und e4e mithilfe der entsprechenden Verkabelung für das Nexus 3232C-Switch-Modell mit dem nächsten verfügbaren 40 GbE-Port auf C2, Port 1/8 verbinden.

7. Aktivieren Sie alle Anschlüsse für Knoten auf C2.

Beispiel anzeigen

Das folgende Beispiel zeigt die Ports 1 bis 30, die bei Nexus 3132Q-V Cluster Switches C1 und C2 aktiviert sind und eine in RCF unterstützte Konfiguration verwenden
NX3232C_RCF_v1.0_24p10g_26p100g.txt:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

8. Aktivieren Sie den zweiten Cluster-Port e4e auf jedem Node:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass der zweite Cluster-Port e4e auf jedem Node hochgebracht wird:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> *network port modify -node n2 -port e4e -up-admin true*s
```

9. Setzen Sie für jeden Node alle migrierten Cluster Interconnect LIFs zurück: `network interface revert`

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die migrierten LIFs auf die Home-Ports zurückgesetzt werden.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

10. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports jetzt auf die Home-Ports zurückgesetzt werden:

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

Der Is Home Spalte sollte einen Wert von anzeigen true Für alle im aufgeführten Ports Current Port Spalte. Wenn der angezeigte Wert lautet false, Der Hafen wurde nicht zurückgesetzt.

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e4a      n1_clus1    up/up      10.10.0.1/24      n1
      true
e4e      n1_clus2    up/up      10.10.0.2/24      n1
      true
e4a      n2_clus1    up/up      10.10.0.3/24      n2
      true
e4e      n2_clus2    up/up      10.10.0.4/24      n2
      true
4 entries were displayed.
```

11. Vergewissern Sie sich, dass sich alle Cluster-Interconnect-Ports im befinden up Bundesland:

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

12. Zeigen Sie die Port-Nummern des Cluster-Switches an, über die jeder Cluster-Port mit jedem Node verbunden ist: network device-discovery show

Beispiel anzeigen

```
cluster::*> network device-discovery show
      Local   Discovered
Node      Port   Device      Interface      Platform
-----
n1      /cdp
      e4a    C1          Ethernet1/7     N3K-C3232C
      e4e    C2          Ethernet1/7     N3K-C3232C
n2      /cdp
      e4a    C1          Ethernet1/8     N3K-C3232C
      e4e    C2          Ethernet1/8     N3K-C3232C
```

13. Anzeige ermittelte und überwachte Cluster-Switches:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3232CV Serial Number: FOX000001 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP	cluster-network	10.10.1.101
C2 NX3232CV Serial Number: FOX000002 Is Monitored: true Reason: Software Version: Cisco Nexus Operating System (NX-OS) Software, Version 7.0(3)I6(1) Version Source: CDP 2 entries were displayed.	cluster-network	10.10.1.102

14. Vergewissern Sie sich, dass die Cluster-Erkennung ohne Switches die Switch-Option deaktiviert hat:

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

15. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```


Beispiel anzeigen

```
cluster::*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e4a    10.10.0.1
Cluster n1_clus2 n1          e4e    10.10.0.2
Cluster n2_clus1 n2          e4a    10.10.0.3
Cluster n2_clus2 n2          e4e    10.10.0.4
Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
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 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s) RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

16. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

17. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Tauschen Sie die Schalter aus

Austausch eines Cisco Nexus 3232C-Cluster-Switch

Befolgen Sie diese Schritte, um einen defekten Cisco Nexus 3232C Switch in einem Cluster zu ersetzen. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Was Sie benötigen

Stellen Sie sicher, dass die vorhandene Cluster- und Netzwerkkonfiguration folgende Merkmale aufweist:

- Die Nexus 3232C-Cluster-Infrastruktur ist redundant und funktioniert auf beiden Switches vollständig.

Auf der Seite Cisco Ethernet Switches befinden sich die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.

- Alle Cluster-Ports müssen den Status **up** aufweisen.
- Management-Konnektivität muss auf beiden Switches vorhanden sein.
- Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und werden nicht migriert.

Der Ersatz-Switch der Cisco Nexus 3232C-Serie weist folgende Merkmale auf:

- Die Management-Netzwerk-Konnektivität ist funktionsfähig.
- Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
- Das entsprechende RCF- und NX-OS-Betriebssystemabbild wird auf den Switch geladen.
- Die anfängliche Anpassung des Schalters ist abgeschlossen.

Finden Sie weitere Informationen

Siehe folgendes:

- ["Beschreibungsseite für den Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Tauschen Sie den Schalter aus

Über diese Aufgabe

Dieses Austauschverfahren beschreibt das folgende Szenario:

- Der Cluster ist zunächst mit vier Nodes mit zwei Nexus 3232C-Cluster-Switches CL1 und CL2 verbunden.
- Sie planen, den Cluster-Switch CL2 durch C2 zu ersetzen (Schritte 1 bis 21):
 - Sie migrieren bei jedem Node die mit Cluster-Switch CL2 verbundenen Cluster-LIFs zu Cluster-Ports, die mit Cluster-Switch CL1 verbunden sind.
 - Sie trennen die Verkabelung von allen Ports am Cluster-Switch CL2, und schließen die Verkabelung wieder an die gleichen Ports am Switch C2 an.
 - Sie setzen die migrierten Cluster-LIFs auf jedem Node zurück.

Zu den Beispielen

Durch diesen Austausch wird der zweite Nexus 3232C Cluster Switch CL2 durch den neuen 3232C Switch C2

ersetzt.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vier Knoten sind n1, n2, n3 und n4.
- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die für Knoten n1 mit Cluster-Switch C1 verbunden ist.
- n1_clus2 ist die erste Cluster-LIF, die mit Cluster-Switch CL2 oder C2 für Node n1 verbunden ist.
- n1_clus3 ist die zweite logische Schnittstelle, die mit Cluster-Switch C2 für Knoten n1 verbunden ist.-
- n1_clus4 ist die zweite logische Schnittstelle, die mit Cluster-Switch CL1 für Node n1 verbunden ist.

Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert "[Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen](#)" Seite.

Die Beispiele in diesem Ersatzverfahren verwenden vier Knoten. Zwei der Nodes verwenden vier 10 GB Cluster Interconnect Ports: e0a, e0b, e0c und e0d. Die anderen beiden Knoten verwenden zwei 40 GB Cluster Interconnect Ports: e4a und e4e. Siehe "[Hardware Universe](#)" Um zu überprüfen, welche Cluster-Ports für Ihre Plattform korrekt sind.

Schritt 1: Anzeigen und migrieren Sie die Cluster-Ports auf den Switch

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3232C
	e0b	CL2	Ethernet1/1/1	N3K-C3232C
	e0c	CL2	Ethernet1/1/2	N3K-C3232C
n2	e0d	CL1	Ethernet1/1/2	N3K-C3232C
	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3232C
	e0b	CL2	Ethernet1/1/3	N3K-C3232C
n3	e0c	CL2	Ethernet1/1/4	N3K-C3232C
	e0d	CL1	Ethernet1/1/4	N3K-C3232C
	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3232C
n4	e4e	CL2	Ethernet1/7	N3K-C3232C
	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3232C
	e4e	CL2	Ethernet1/8	N3K-C3232C

3. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

a. Zeigen Sie die Attribute des Netzwerkports an:

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

```

cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed (Mbps)

Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper
Status Status
-----
-----
e0a Cluster Cluster up 9000 auto/10000 -
e0b Cluster Cluster up 9000 auto/10000 -
e0c Cluster Cluster up 9000 auto/10000 -
e0d Cluster Cluster up 9000 auto/10000 -
-

Node: n2

Ignore

Speed (Mbps)

Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper
Status Status
-----
-----
e0a Cluster Cluster up 9000 auto/10000 -
e0b Cluster Cluster up 9000 auto/10000 -
e0c Cluster Cluster up 9000 auto/10000 -
e0d Cluster Cluster up 9000 auto/10000 -
-

Node: n3

Ignore

Speed (Mbps)

Health Health
Port IPspace Broadcast Domain Link MTU Admin/Oper
Status Status
-----
-----
e4a Cluster Cluster up 9000 auto/40000 -
-
e4e Cluster Cluster up 9000 auto/40000 -

```

```

-

Node: n4

Ignore

Health      Health      Speed (Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
e4e         Cluster      Cluster      up    9000 auto/40000 -

```

b. Anzeigen von Informationen zu den logischen Schnittstellen (LIFs):

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

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e0a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e0e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e0a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e0e	true			

c. Zeigen Sie die erkannten Cluster-Switches an:

```
system cluster-switch show
```


Beispiel anzeigen

Im folgenden Ausgabebeispiel werden die Cluster-Switches angezeigt:

```
cluster::> system cluster-switch show
Switch                                     Type                Address
Model
-----
CL1                                     cluster-network     10.10.1.101
NX3232C
    Serial Number: FOX000001
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version 7.0(3)I6(1)
    Version Source: CDP

CL2                                     cluster-network     10.10.1.102
NX3232C
    Serial Number: FOX000002
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
    Software, Version 7.0(3)I6(1)
    Version Source: CDP
```

4. Vergewissern Sie sich, dass die entsprechenden RCF und das entsprechende Image auf dem neuen Nexus 3232C Switch installiert sind und nehmen Sie die erforderlichen Anpassungen am Standort vor.
 - a. Rufen Sie die NetApp Support Site auf.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- b. Gehen Sie zur Seite **Cisco Ethernet Switches** und notieren Sie sich die erforderlichen Softwareversionen in der Tabelle.

["Cisco Ethernet-Switches"](#)

- c. Laden Sie die entsprechende Version des RCF herunter.
 - d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und navigieren Sie dann zur Seite **Download**.
 - e. Laden Sie die richtige Version der Bildsoftware von der Seite * Cisco® Cluster und Management Network Switch Reference Configuration File Download* herunter.

["Cisco® Cluster und Management Network Switch Referenzkonfigurationsdatei herunterladen"](#)

5. Migrieren Sie die Cluster-LIFs auf die physischen Node-Ports, die mit dem Ersatz-Switch verbunden

sind.C2:

```
network interface migrate -vserver vservice-name -lif lif-name -source-node  
node-name -destination-node node-name -destination-port port-name
```

Beispiel anzeigen

Sie müssen alle Cluster-LIFs individuell migrieren, wie im folgenden Beispiel gezeigt:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2  
-source-node n1 -destination-  
node n1 -destination-port e0a  
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3  
-source-node n1 -destination-  
node n1 -destination-port e0d  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2  
-source-node n2 -destination-  
node n2 -destination-port e0a  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3  
-source-node n2 -destination-  
node n2 -destination-port e0d  
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2  
-source-node n3 -destination-  
node n3 -destination-port e4a  
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2  
-source-node n4 -destination-  
node n4 -destination-port e4a
```

6. Überprüfen Sie den Status der Cluster-Ports und ihrer Home-Bezeichnungen:

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

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0a      false
      n1_clus3      up/up      10.10.0.3/24      n1
e0d      false
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0a      false
      n2_clus3      up/up      10.10.0.7/24      n2
e0d      false
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
      n3_clus1      up/up      10.10.0.9/24      n3
e4a      true
      n3_clus2      up/up      10.10.0.10/24      n3
e4a      false
      n4_clus1      up/up      10.10.0.11/24      n4
e4a      true
      n4_clus2      up/up      10.10.0.12/24      n4
e4a      false
```

7. Fahren Sie die Cluster-Interconnect-Ports herunter, die physisch mit dem ursprünglichen Switch CL2 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin false
```

Beispiel anzeigen

Im folgenden Beispiel werden die Cluster-Interconnect-Ports auf allen Nodes heruntergefahren:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e0a    10.10.0.1
Cluster n1_clus2 n1          e0b    10.10.0.2
Cluster n1_clus3 n1          e0c    10.10.0.3
Cluster n1_clus4 n1          e0d    10.10.0.4
Cluster n2_clus1 n2          e0a    10.10.0.5
Cluster n2_clus2 n2          e0b    10.10.0.6
Cluster n2_clus3 n2          e0c    10.10.0.7
Cluster n2_clus4 n2          e0d    10.10.0.8
Cluster n3_clus1 n4          e0a    10.10.0.9
Cluster n3_clus2 n3          e0e    10.10.0.10
Cluster n4_clus1 n4          e0a    10.10.0.11
Cluster n4_clus2 n4          e0e    10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11
10.10.0.12 Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) .....
Detected 9000 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
```

```
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
8 paths up, 0 paths down (udp check)
```

Schritt: ISLs auf Switch CL1 und C2 migrieren

1. Fahren Sie die Ports 1/31 und 1/32 am Cluster-Switch CL1 herunter.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1) (config-if-range) # shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

2. Entfernen Sie alle Kabel, die am Cluster-Switch CL2 angeschlossen sind, und schließen Sie sie für alle Nodes an den Austausch-Switch C2 an.
3. Entfernen Sie die ISL-Kabel (Inter-Switch Link) von den Ports e1/31 und e1/32 am Cluster-Switch CL2, und schließen Sie sie an die gleichen Ports am Ersatzschalter C2 an.
4. ISL-Ports 1/31 und 1/32 auf dem Cluster-Switch CL1 heraufholen.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

```
(CL1) # configure
(CL1) (Config) # interface e1/31-32
(CL1) (config-if-range) # no shutdown
(CL1) (config-if-range) # exit
(CL1) (Config) # exit
(CL1) #
```

5. Überprüfen Sie, ob die ISLs auf CL1 verfügbar sind.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Die Ports eth1/31 und eth1/32 sollten angegeben werden (P), Was bedeutet, dass die ISL-Ports im Port-Channel aktiv sind:

Beispiel anzeigen

```
CL1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

6. Vergewissern Sie sich, dass die ISLs auf Cluster-Switch C2 verfügbar sind.

Weitere Informationen zu Cisco-Befehlen finden Sie in den Handbüchern im ["Referenzen für NX-OS-Befehle der Cisco Nexus 3000-Serie"](#).

Beispiel anzeigen

Die Ports eth1/31 und eth1/32 sollten (P) angeben, was bedeutet, dass beide ISL-Ports im Port-Channel hochgefahren sind.

```
C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

7. Führen Sie auf allen Knoten alle Cluster-Interconnect-Ports aus, die mit dem Ersatz-Switch C2 verbunden sind:

```
network port modify -node node-name -port port-name -up-admin true
```

Beispiel anzeigen

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
cluster::*> network port modify -node n3 -port e4e -up-admin true
cluster::*> network port modify -node n4 -port e4e -up-admin true
```

Schritt 3: Zurücksetzen aller LIFs auf die ursprünglich zugewiesenen Ports

1. Zurücksetzen aller migrierten Cluster-Interconnect-LIFs auf allen Nodes:

```
network interface revert -vserver cluster -lif lif-name
```


Beispiel anzeigen

Sie müssen alle Cluster-Interconnect-LIFs einzeln zurücksetzen, wie im folgenden Beispiel dargestellt:

```
cluster::*> network interface revert -vserver cluster -lif n1_clus2
cluster::*> network interface revert -vserver cluster -lif n1_clus3
cluster::*> network interface revert -vserver cluster -lif n2_clus2
cluster::*> network interface revert -vserver cluster -lif n2_clus3
Cluster::*> network interface revert -vserver cluster -lif n3_clus2
Cluster::*> network interface revert -vserver cluster -lif n4_clus2
```

2. Vergewissern Sie sich, dass die Cluster-Interconnect-Ports jetzt nach Hause zurückgesetzt werden:

```
network interface show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs erfolgreich zurückgesetzt wurden, da die Ports unter aufgeführt sind `Current Port` Spalte hat den Status von `true` Im `Is Home` Spalte. Wenn ein Port einen Wert von `false` hat, Das LIF wurde nicht zurückgesetzt.

```
cluster::*> network interface show -role cluster
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

3. Vergewissern Sie sich, dass die Cluster-Ports verbunden sind:

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

Beispiel anzeigen

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

```
Speed(Mbps) Health
```

```
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
```

```
-----
```

```
-----
```

```
e0a      Cluster      Cluster      up    9000  auto/10000  -
```

```
e0b      Cluster      Cluster      up    9000  auto/10000  -
```

```
e0c      Cluster      Cluster      up    9000  auto/10000  -
```

```
e0d      Cluster      Cluster      up    9000  auto/10000  -
```

```
-
```

```
Node: n2
```

```
Ignore
```

```
Speed(Mbps) Health
```

```
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
```

```
-----
```

```
-----
```

```
e0a      Cluster      Cluster      up    9000  auto/10000  -
```

```
e0b      Cluster      Cluster      up    9000  auto/10000  -
```

```
e0c      Cluster      Cluster      up    9000  auto/10000  -
```

```
e0d      Cluster      Cluster      up    9000  auto/10000  -
```

```
-
```

```
Node: n3
```

```
Ignore
```

```
Speed(Mbps) Health
```

```
Health
```

```
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
```

```
-----
```

```
-----
```

```
e4a      Cluster      Cluster      up    9000  auto/40000  -
```

```
e4e      Cluster      Cluster      up    9000  auto/40000  -
```

```
-
```

```
Node: n4
```

Ignore

Speed (Mbps) Health

Health

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
------	---------	-----------	--------	------	-----	------------	--------

e4a	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

e4e	Cluster	Cluster		up	9000	auto/40000	-
-----	---------	---------	--	----	------	------------	---

-

4. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

Im folgenden Beispiel wird Node n1 beflügelt und der RPC-Status danach angezeigt:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1 Getting addresses from network interface table...
Cluster n1_clus1 n1          e0a      10.10.0.1
Cluster n1_clus2 n1          e0b      10.10.0.2
Cluster n1_clus3 n1          e0c      10.10.0.3
Cluster n1_clus4 n1          e0d      10.10.0.4
Cluster n2_clus1 n2          e0a      10.10.0.5
Cluster n2_clus2 n2          e0b      10.10.0.6
Cluster n2_clus3 n2          e0c      10.10.0.7
Cluster n2_clus4 n2          e0d      10.10.0.8
Cluster n3_clus1 n3          e0a      10.10.0.9
Cluster n3_clus2 n3          e0e      10.10.0.10
Cluster n4_clus1 n4          e0a      10.10.0.11
Cluster n4_clus2 n4          e0e      10.10.0.12
Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293 Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s) .....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
```

```
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
```

```
Larger than PMTU communication succeeds on 32 path(s) RPC status:
8 paths up, 0 paths down (tcp check)
8  paths up, 0 paths down (udp check)
```

Schritt 4: Überprüfen, ob alle Ports und LIF korrekt migriert sind

1. Geben Sie die folgenden Befehle ein, um Informationen über die Geräte in Ihrer Konfiguration anzuzeigen:

Sie können die folgenden Befehle in beliebiger Reihenfolge ausführen:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

Beispiel anzeigen

```
cluster::> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3232C
	e0b	C2	Ethernet1/1/1	N3K-C3232C
	e0c	C2	Ethernet1/1/2	N3K-C3232C
	e0d	C1	Ethernet1/1/2	N3K-C3232C
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3232C
	e0b	C2	Ethernet1/1/3	N3K-C3232C
	e0c	C2	Ethernet1/1/4	N3K-C3232C
	e0d	C1	Ethernet1/1/4	N3K-C3232C
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3232C
	e4e	C2	Ethernet1/7	N3K-C3232C
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3232C
	e4e	C2	Ethernet1/8	N3K-C3232C

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

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

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

e0a	Cluster	Cluster		up	9000	auto/10000 -
e0b	Cluster	Cluster		up	9000	auto/10000 -
e0c	Cluster	Cluster		up	9000	auto/10000 -
e0d	Cluster	Cluster		up	9000	auto/10000 -

```
Node: n2
```

```
Ignore
```

					Speed(Mbps)	Health
Health						

```

Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a       Cluster      Cluster      up    9000  auto/10000  -
e0b       Cluster      Cluster      up    9000  auto/10000  -
e0c       Cluster      Cluster      up    9000  auto/10000  -
e0d       Cluster      Cluster      up    9000  auto/10000  -

Node: n3

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a       Cluster      Cluster      up    9000  auto/40000  -
e4e       Cluster      Cluster      up    9000  auto/40000  -

Node: n4

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a       Cluster      Cluster      up    9000  auto/40000  -
e4e       Cluster      Cluster      up    9000  auto/40000  -

cluster::*> network interface show -role cluster

Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
-----
Cluster
nm1_clus1 up/up 10.10.0.1/24 n1
e0a true
n1_clus2 up/up 10.10.0.2/24 n1
e0b true

```


	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

cluster::*> **system cluster-switch show**

Switch	Type	Address
Model		
-----	-----	-----
CL1	cluster-network	10.10.1.101
NX3232C		
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
CL2	cluster-network	10.10.1.102
NX3232C		
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2	cluster-network	10.10.1.103
NX3232C		
Serial Number: FOX000003		

```
Is Monitored: true
```

```
Reason: None
```

```
Software Version: Cisco Nexus Operating System (NX-OS)
```

```
Software, Version 7.0(3)I6(1)
```

```
Version Source: CDP 3 entries were displayed.
```

2. Löschen Sie den ersetzten Cluster-Switch CL2, wenn er nicht automatisch entfernt wurde:

```
system cluster-switch delete -device cluster-switch-name
```

3. Überprüfen Sie, ob die richtigen Cluster-Switches überwacht werden:

```
system cluster-switch show
```

Beispiel anzeigen

Im folgenden Beispiel werden die Cluster-Switches überwacht, da der Is Monitored Status lautet true.

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3232C	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		
C2 NX3232C	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version 7.0(3)I6(1)		
Version Source: CDP		

4. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password  
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password  
Enter the switch name: <return>  
The switch name entered is not recognized.  
Choose from the following list:  
CL1  
C2  
  
cluster::*> system cluster-switch log setup-password  
  
Enter the switch name: CL1  
RSA key fingerprint is  
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc  
Do you want to continue? {y|n}::[n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster::*> system cluster-switch log setup-password  
  
Enter the switch name: C2  
RSA key fingerprint is  
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1  
Do you want to continue? {y|n}: [n] y  
  
Enter the password: <enter switch password>  
Enter the password again: <enter switch password>  
  
cluster::*> system cluster-switch log enable-collection  
  
Do you want to enable cluster log collection for all nodes in the  
cluster?  
{y|n}: [n] y  
  
Enabling cluster switch log collection.  
  
cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

5. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Einen Cisco Nexus 3232C Storage-Switch austauschen

Befolgen Sie diese Schritte, um einen fehlerhaften Cisco Nexus 3232C Storage Switch zu ersetzen. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Prüfen Sie die Anforderungen

Die vorhandene Netzwerkkonfiguration muss die folgenden Merkmale aufweisen:

- Auf der Seite Cisco Ethernet Switches befinden sich die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.
- Management-Konnektivität muss auf beiden Switches vorhanden sein.



Stellen Sie sicher, dass alle Fehlerbehebungsschritte durchgeführt wurden, um zu bestätigen, dass Ihr Switch ausgetauscht werden muss.

Der Cisco Nexus 3232C Switch muss folgende Merkmale aufweisen:

- Die Konnektivität des Managementnetzwerks muss funktionsfähig sein.
- Der Konsolenzugriff auf den Ersatzschalter muss vorhanden sein.
- Das entsprechende RCF- und NX-OS-Betriebssystemabbild muss auf den Switch geladen werden.
- Die anfängliche Anpassung des Schalters muss abgeschlossen sein.

Tauschen Sie den Schalter aus

Dieses Verfahren ersetzt den zweiten Nexus 3232C Storage Switch S2 durch den neuen 3232C Switch NS2. Die beiden Knoten sind node1 und node2.

Schritt 1: Bestätigen Sie, dass der zu ersetzende Schalter S2 ist

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Überprüfen Sie den Integritätsstatus der Storage-Node-Ports, um sicherzustellen, dass eine Verbindung zum Storage-Switch S1 besteht:

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

Beispiel anzeigen

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

Node	Port	Type	Mode	Speed		Status	VLAN
				(Gb/s)	State		ID

node1	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

3. Stellen Sie sicher, dass der Speicherschalter S1 verfügbar ist:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
```

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

node1/cdp	e3a	S1	Ethernet1/1	
NX3232C	e4a	node2	e4a	AFF-
A700	e4e	node2	e4e	AFF-
A700				
node1/lldp	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
node2/cdp	e3a	S1	Ethernet1/2	
NX3232C	e4a	node1	e4a	AFF-
A700	e4e	node1	e4e	AFF-
A700				
node2/lldp	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-

4. Führen Sie die aus `show lldp neighbors` Mit dem Befehl auf dem Arbeitsschalter bestätigen Sie, dass Sie beide Nodes und alle Shelves sehen können:

```
show lldp neighbors
```

Beispiel anzeigen

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID                Local Intf          Hold-time  Capability  Port
ID
node1                    Eth1/1             121        S           e3a
node2                    Eth1/2             121        S           e3a
SHFGD2008000011          Eth1/5             121        S           e0a
SHFGD2008000011          Eth1/6             120        S           e0a
SHFGD2008000022          Eth1/7             120        S           e0a
SHFGD2008000022          Eth1/8             120        S           e0a
```

Schritt: Verkabelung konfigurieren

1.]Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-
port

shelf  id  remote-port  remote-device
----- --  -
3.20   0  Ethernet1/5  S1
3.20   1  -            -
3.20   2  Ethernet1/6  S1
3.20   3  -            -
3.30   0  Ethernet1/7  S1
3.20   1  -            -
3.30   2  Ethernet1/8  S1
3.20   3  -            -
```

2. Entfernen Sie alle Kabel, die am Lagerschalter S2 angeschlossen sind.
3. Schließen Sie alle Kabel wieder an den Ersatzschalter NS2 an.

Schritt 3: Überprüfen Sie alle Gerätekonfigurationen am Switch NS2

1. Überprüfen Sie den Funktionsstatus der Storage-Node-Ports:

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

Beispiel anzeigen

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

		Speed				
VLAN	Node	Port	Type	Mode	(Gb/s)	State
ID						Status

node1						
		e3a	ENET	storage	100	enabled online
30		e3b	ENET	storage	0	enabled offline
30		e7a	ENET	storage	0	enabled offline
30		e7b	ENET	storage	100	enabled online
30						
node2						
		e3a	ENET	storage	100	enabled online
30		e3b	ENET	storage	0	enabled offline
30		e7a	ENET	storage	0	enabled offline
30		e7b	ENET	storage	100	enabled online
30						

2. Vergewissern Sie sich, dass beide Switches verfügbar sind:

```
network device-discovery show
```


Beispiel anzeigen

```
storage::*> network device-discovery show
```

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

node1/cdp	e3a	S1	Ethernet1/1	
NX3232C	e4a	node2	e4a	AFF-
A700	e4e	node2	e4e	AFF-
A700	e7b	NS2	Ethernet1/1	
NX3232C				
node1/lldp	e3a	S1	Ethernet1/1	-
	e4a	node2	e4a	-
	e4e	node2	e4e	-
	e7b	NS2	Ethernet1/1	-
node2/cdp	e3a	S1	Ethernet1/2	
NX3232C	e4a	node1	e4a	AFF-
A700	e4e	node1	e4e	AFF-
A700	e7b	NS2	Ethernet1/2	
NX3232C				
node2/lldp	e3a	S1	Ethernet1/2	-
	e4a	node1	e4a	-
	e4e	node1	e4e	-
	e7b	NS2	Ethernet1/2	-

3. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf id remote-port remote-device  
-----  
3.20 0 Ethernet1/5 S1  
3.20 1 Ethernet1/5 NS2  
3.20 2 Ethernet1/6 S1  
3.20 3 Ethernet1/6 NS2  
3.30 0 Ethernet1/7 S1  
3.20 1 Ethernet1/7 NS2  
3.30 2 Ethernet1/8 S1  
3.20 3 Ethernet1/8 NS2
```

4. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Ersetzen Sie Cisco Nexus 3232C-Cluster-Switches durch Verbindungen ohne Switches

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

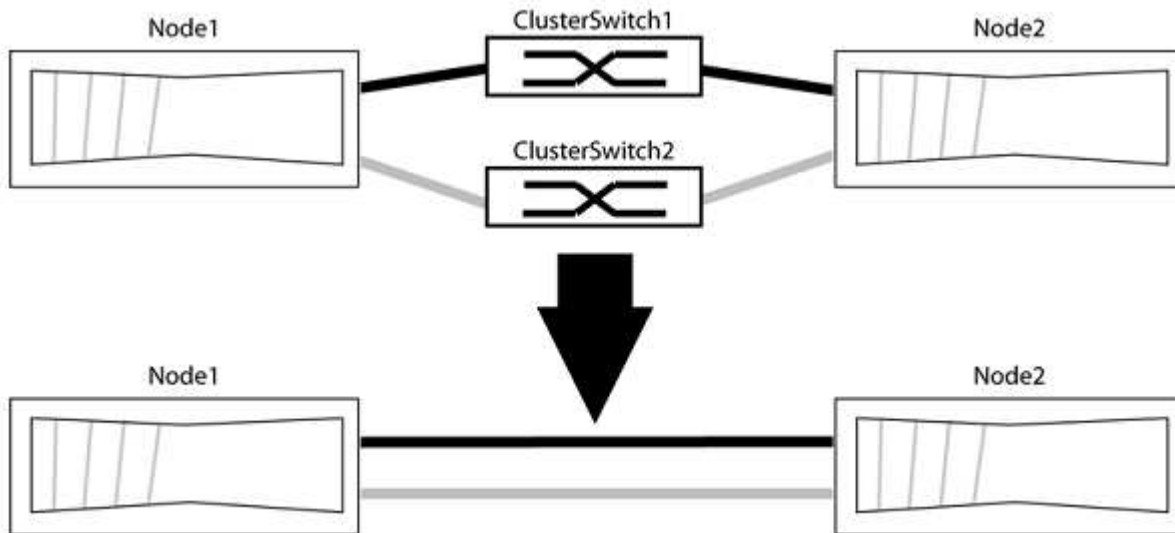
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Angezeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

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

Schritt: Ports und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in `grop1` zu Cluster-Switch 1 wechseln und die Cluster-Ports in `grop2` zu Cluster-Switch 2 wechseln. Diese Gruppen sind später im Verfahren erforderlich.
2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



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

Beispiel anzeigen

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

```
Node: node1
```

```
Ignore
```

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

```
Node: node2
```

```
Ignore
```

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

```
4 entries were displayed.
```

3. Vergewissern Sie sich, dass alle Cluster-LIFs auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

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

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

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

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

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

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

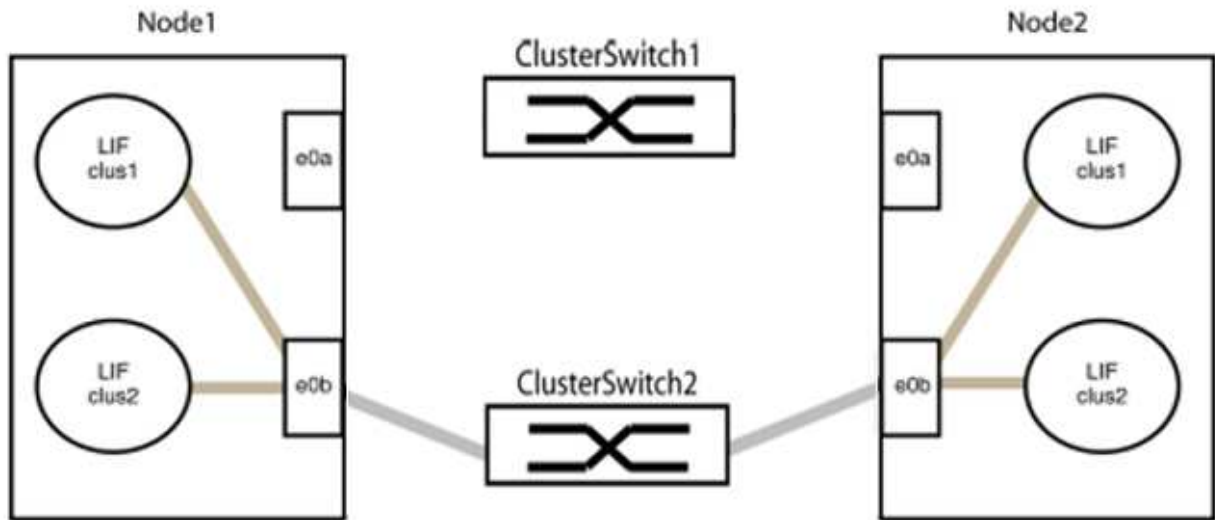
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

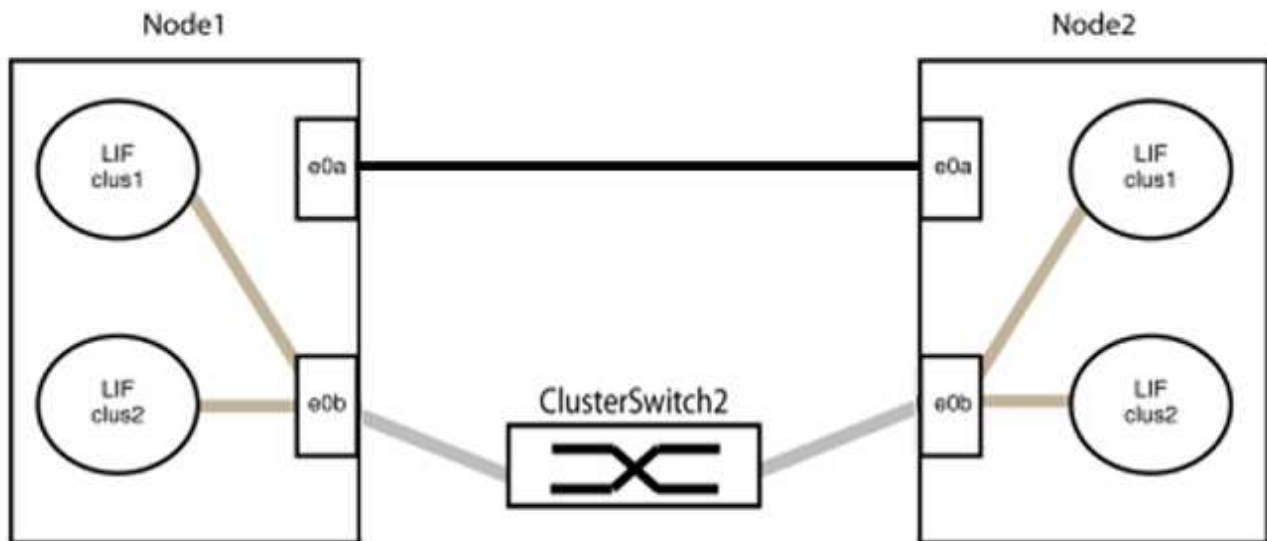
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

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

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

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

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:


```
cluster ping-cluster -node local
```



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

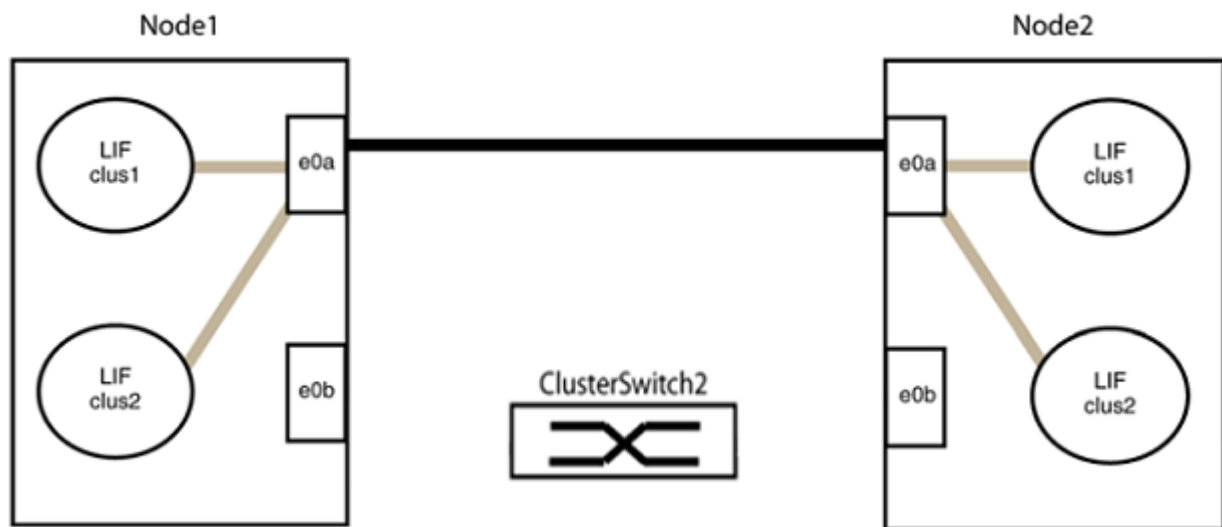
11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

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

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet 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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

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

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten false:

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

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

Aktualisieren eines Cisco Nexus 3232C Storage Switch

Führen Sie diese Schritte aus, um die Cisco NX-OS Software und die RCF (Referenz-Konfigurationsdateien) auf Cisco Nexus 3232C-Switches zu aktualisieren.

Prüfen Sie die Anforderungen

Was Sie benötigen

Stellen Sie vor dem Upgrade der NX-OS-Software und der RCFs auf dem Storage-Switch sicher, dass die folgenden Bedingungen erfüllt sind:

- Der Switch funktioniert voll (es sollten keine Fehler in den Protokollen oder ähnlichen Problemen geben).
- Sie haben die gewünschten Boot-Variablen im RCF aktiviert oder gesetzt, um die gewünschten Boot-Images zu reflektieren, wenn Sie nur NX-OS installieren und Ihre aktuelle RCF-Version behalten.

Wenn Sie die Boot-Variablen ändern müssen, um die aktuellen Startabbilder zu berücksichtigen, müssen Sie dies vor der erneuten Anwendung der RCF tun, damit die korrekte Version bei zukünftigen Neustarts instanziiert wird.

- Sie haben die entsprechenden Leitfäden zu Software und Upgrades auf der bezogenen ["Switches Der Cisco Nexus 3000-Serie"](#) Seite für vollständige Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Storage.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert ["Cisco Ethernet-Switches"](#) Seite.

Tauschen Sie den Schalter aus

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Speicherschalter lauten S1 und S2.
- Die Knoten sind node1 und node2.

Die Beispiele in diesem Verfahren verwenden zwei Nodes; Knoten1 mit zwei Storage-Ports und Knoten2 mit zwei Storage-Ports. Siehe ["Hardware Universe"](#) Um die korrekten Speicherports auf Ihren Plattformen zu überprüfen.



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben. Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.

Schritt 1: Prüfen Sie den Funktionszustand von Switches und Ports

1. Wenn AutoSupport aktiviert ist, unterdrücken Sie die automatische Erstellung eines Cases durch Aufrufen einer AutoSupport Meldung:

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

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Prüfen Sie, ob die Speicherschalter verfügbar sind:

```
system switch ethernet show
```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                Address
Model
-----
S1
                                     storage-network      172.17.227.5
NX3232C
  Serial Number: FOC221206C2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(3)
  Version Source: CDP

S2
                                     storage-network      172.17.227.6
NX3232C
  Serial Number: FOC220443LZ
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(3)
  Version Source: CDP

2 entries were displayed.
storage::*>
```

3. Vergewissern Sie sich, dass die Node-Ports ordnungsgemäß und betriebsbereit sind:

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

Beispiel anzeigen

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

		Speed				
VLAN	Node	Port	Type	Mode	(Gb/s)	State
ID						Status

node1						
		e3a	ENET	storage	100	enabled online
30						
		e3b	ENET	storage	0	enabled offline
30						
		e7a	ENET	storage	0	enabled offline
30						
		e7b	ENET	storage	100	enabled online
30						
node2						
		e3a	ENET	storage	100	enabled online
30						
		e3b	ENET	storage	0	enabled offline
30						
		e7a	ENET	storage	0	enabled offline
30						
		e7b	ENET	storage	100	enabled online
30						

4. Prüfen Sie, ob es keine Probleme mit dem Storage Switch oder der Verkabelung gibt:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance
```

There are no entries matching your query.

Schritt: Kopieren Sie den RCF auf Cisco Switch S2

1. Kopieren Sie den RCF auf Switch S2 mit einem der folgenden Übertragungsprotokolle auf den Switch Bootflash: FTP, HTTP, TFTP, SFTP oder SCP.

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

Beispiel anzeigen

Im folgenden Beispiel wird HTTP zum Kopieren eines RCF auf den Bootflash auf Switch S2 verwendet:

```
S2# copy http://172.16.10.1//cfg/Nexus_3232C_RCF_v1.6-Storage.txt
bootflash: vrf management
% Total      % Received % Xferd  Average   Speed    Time     Time
Time                               Current          Dload    Upload  Total   Spent
Left                               Speed
 100          3254      100    3254      0         0      8175      0
--:--:-- --:--:-- --:--:--    8301
Copy complete, now saving to disk (please wait)...
Copy complete.
S2#
```

2. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde:

```
copy bootflash:
```

Beispiel anzeigen

Das folgende Beispiel zeigt die RCF-Datei Nexus_3232C_RCF_v1.6-Storage.txt Installation auf Schalter S2:

```
S2# copy Nexus_3232C_RCF_v1.6-Storage.txt running-config echo-
commands
```

3. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.



In der Bannerausgabe aus dem `show banner motd` Befehl, Sie müssen lesen und befolgen Sie die Anweisungen im Abschnitt *** WICHTIGE HINWEISE***, um die richtige Konfiguration und den Betrieb des Switches zu gewährleisten.

+

.Beispiel anzeigen

```
S2# show banner motd
```

```
*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Cisco Nexus 3232C
* Filename  : Nexus_3232C_RCF_v1.6-Storage.txt
* Date      : Oct-20-2020
* Version   : v1.6
*
* Port Usage : Storage configuration
* Ports 1-32: Controller and Shelf Storage Ports
* Ports 33-34: Disabled
*
* IMPORTANT NOTES*
* - This RCF utilizes QoS and requires TCAM re-configuration,
  requiring RCF
*   to be loaded twice with the Storage Switch rebooted in between.
*
* - Perform the following 4 steps to ensure proper RCF installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
  ports...
*       - TCAM region is not configured for feature QoS class IPv4
  ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
  following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
*
*   (4) Save running-configuration again
*****
*****
S2#
```

+



Beim ersten Anwenden des RCF wird die Meldung **ERROR: Failed to write VSH** befiehlt erwartet und kann ignoriert werden.

4. Nachdem Sie sich vergewissern, dass die Software-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie den `running-config` Datei in der `startup-config` Datei auf Schalter S2.

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

Beispiel anzeigen

Das folgende Beispiel zeigt die `running-config` Datei erfolgreich in kopiert `startup-config` Datei:

```
S2# copy running-config startup-config
[#####] 100% Copy complete.
```

Schritt 3: Kopieren Sie das NX-OS-Image auf Cisco Switch S2 und starten Sie neu

1. Kopieren Sie das NX-OS-Image auf Switch S2.

Beispiel anzeigen

```
S2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

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

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

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

2. Installieren Sie das System-Image so, dass die neue Version beim nächsten Neustart von Switch S2 geladen wird.

Der Schalter wird in 10 Sekunden neu gestartet, wobei das neue Bild wie in der folgenden Ausgabe dargestellt ist:

Beispiel anzeigen

```
S2# install all nxos bootflash:nxos.9.3.4.bin
```

```
Installer will perform compatibility check first. Please wait.
```

```
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
```

```
[ ] 100% -- SUCCESS
```

```
Verifying image type.
```

```
[ ] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
```

```
[ ] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
```

```
[ ] 100% -- SUCCESS
```

```
Performing module support checks.
```

```
[ ] 100% -- SUCCESS
```

```
Notifying services about system upgrade.
```

```
[ ] 100% -- SUCCESS
```

```
Compatibility check is done:
```

Module	bootable	Impact	Install-type	Reason
-----	-----	-----	-----	-----
1	yes	disruptive	reset	default upgrade is not hitless

```
Images will be upgraded according to following table:
```

Module	Image	Running-Version(pri:alt)
New-Version	Upg-Required	
-----	-----	-----
1	nxos	9.3(3)
9.3(4)	yes	
1	bios	v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)	no	

```
Switch will be reloaded for disruptive upgrade.
```

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

```
input string too long
```

```
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.
S2#
```

3. Speichern Sie die Konfiguration.

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

Sie werden aufgefordert, das System neu zu booten.

Beispiel anzeigen

```
S2# copy running-config startup-config
[] 100% Copy complete.
S2# reload
This command will reboot the system. (y/n)? [n] y
```

4. Vergewissern Sie sich, dass sich die neue NX-OS-Versionsnummer auf dem Switch befindet:

Beispiel anzeigen

S2# **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 Nexus3000 C3232C Chassis (Nexus 9000 Series)

Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of memory.

Processor Board ID FOC20291J6K

Device name: S2

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 due to upgrade
```

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
S2#
```

Schritt 4: Überprüfen Sie den Funktionszustand von Switches und Ports

1. Überprüfen Sie erneut, ob die Speicherschalter nach dem Neustart verfügbar sind:

```
system switch ethernet show
```


Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                                     Type                Address
Model
-----
S1
                                     storage-network      172.17.227.5
NX3232C
  Serial Number: FOC221206C2
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(4)
  Version Source: CDP

S2
                                     storage-network      172.17.227.6
NX3232C
  Serial Number: FOC220443LZ
  Is Monitored: true
  Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                                     9.3(4)
  Version Source: CDP

2 entries were displayed.
storage::*>
```

2. Vergewissern Sie sich nach dem Neustart, dass die Switch-Ports ordnungsgemäß und betriebsbereit sind:

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

Beispiel anzeigen

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

		Speed				
VLAN	Node	Port	Type	Mode	(Gb/s)	State
ID						Status

node1						
		e3a	ENET	storage	100	enabled online
30		e3b	ENET	storage	0	enabled offline
30		e7a	ENET	storage	0	enabled offline
30		e7b	ENET	storage	100	enabled online
30						
node2						
		e3a	ENET	storage	100	enabled online
30		e3b	ENET	storage	0	enabled offline
30		e7a	ENET	storage	0	enabled offline
30		e7b	ENET	storage	100	enabled online
30						

3. Überprüfen Sie erneut, ob es keine Probleme mit dem Storage Switch oder der Verkabelung beim Cluster gibt:

```
system health alert show -instance
```

Beispiel anzeigen

```
storage::*> system health alert show -instance
```

```
There are no entries matching your query.
```

4. Wiederholen Sie das Verfahren, um die NX-OS-Software und die RCF am Switch S1 zu aktualisieren.
5. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

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

Cisco Nexus 3132Q-V

Überblick

Überblick über die Installation und Konfiguration von Cisco Nexus 3132Q-V Switches

Die Cisco Nexus 3132Q-V Switches können als Cluster Switches in Ihrem AFF oder FAS Cluster verwendet werden. Dank Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Nodes erstellen.

Überblick über die Erstkonfiguration

Gehen Sie wie folgt vor, um einen Cisco Nexus 3132Q-V Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Füllen Sie das Cisco Nexus 3132Q-V-Verkabelungsarbeitsblatt aus"](#). Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.
2. ["Installieren Sie einen Cisco Nexus 3132Q-V Cluster Switch in einem NetApp Rack"](#). Installieren Sie den Cisco Nexus 3132Q-V Switch und die Pass-Through-Panel in einem NetApp Rack mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.
3. ["Konfigurieren Sie den Cisco Nexus 3132Q-V Switch"](#). Richten Sie den Cisco Nexus 3132Q-V Switch ein und konfigurieren Sie ihn.
4. ["Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei \(RCF\) vor"](#). Bereiten Sie die Installation der NX-OS-Software und der Referenz-Konfigurationsdatei (RCF) vor.
5. ["Installieren Sie die NX-OS-Software"](#). Gehen Sie folgendermaßen vor, um die NX-OS-Software auf dem Nexus 3132Q-V Cluster Switch zu installieren.
6. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)"](#). Gehen Sie folgendermaßen vor, um den RCF nach dem ersten Einrichten des Nexus 3132Q-V-Schalters zu installieren. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Erforderliche Dokumentation"](#)
- ["Anforderungen für Smart Call Home"](#)

Konfigurationsanforderungen für Cisco Nexus 3132Q-V Switches

Prüfen Sie die Netzwerk- und Konfigurationsanforderungen für die Installation und Wartung von Cisco Nexus 3132Q-V Switches.

Konfigurationsanforderungen

Zum Konfigurieren des Clusters benötigen Sie die entsprechende Anzahl und den entsprechenden Kabeltyp und Kabelanschlüsse für Ihre Switches. Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

Netzwerkanforderungen

Sie benötigen die folgenden Netzwerkinformationen für alle Switch-Konfigurationen:

- IP-Subnetz für den Management-Netzwerkdatenverkehr.
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches.
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700 Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.

Siehe "[Hardware Universe](#)" Aktuelle Informationen.

Dokumentationsanforderungen für Cisco Nexus 3132Q-V-Switches

Prüfen Sie für die Installation und Wartung von Cisco Nexus 3132Q-V Switches die empfohlene Dokumentation.

Switch-Dokumentation

Zum Einrichten der Cisco Nexus 3132Q-V Switches benötigen Sie die folgende Dokumentation von "[Switches Der Cisco Nexus 3000-Serie Unterstützen](#)" Seite.

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie <i>Nexus 3000</i>	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 3000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.
<i>Cisco Nexus 3000 Series NX-OS Software Upgrade and Downgrade Guide</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 3000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 3000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 3000-Switches.
<i>Nexus 3000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 3000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.

Dokumenttitel	Beschreibung
<i>Versionshinweise zur Cisco Nexus 3000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 3000 Serie.
Gesetzliche Vorschriften, Compliance und Sicherheitsinformationen für die Cisco Nexus 6000, Cisco Nexus 5000 Serie, Cisco Nexus 3000 Serie und Cisco Nexus 2000 Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 3000.

Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Betriebssystemversion über das ["ONTAP 9 Dokumentationszentrum"](#).

Name	Beschreibung
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP-Dokumentation	Dieser Service bietet detaillierte Informationen zu allen Aspekten der ONTAP Versionen.
"Hardware Universe"	Liefert Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Schienensatz und Rack-Dokumentation

Informationen zur Installation eines 33132Q-V Cisco Switch in einem NetApp Rack finden Sie in der folgenden Hardware-Dokumentation.

Name	Beschreibung
"42-HE-System-Cabinet, Deep Guide"	Beschreibt die FRUs, die dem 42U-Systemschrank zugeordnet sind, und bietet Anweisungen für Wartung und FRU-Austausch.
"Installation des Cisco Nexus 3132Q-V Switch in einem NetApp Rack"	Beschreibt die Installation eines Cisco Nexus 3132Q-V Switches in einem NetApp Rack mit vier Pfosten.

Anforderungen für Smart Call Home

Überprüfen Sie die folgenden Richtlinien, um die Smart Call Home-Funktion zu verwenden.

Smart Call Home überwacht die Hardware- und Softwarekomponenten Ihres Netzwerks. Wenn eine kritische

Systemkonfiguration auftritt, generiert es eine E-Mail-basierte Benachrichtigung und gibt eine Warnung an alle Empfänger aus, die im Zielprofil konfiguriert sind. Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch konfigurieren, um per E-Mail mit dem Smart Call Home-System kommunizieren zu können. Darüber hinaus können Sie optional Ihren Cluster-Netzwerk-Switch einrichten, um die integrierte Smart Call Home-Support-Funktion von Cisco zu nutzen.

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

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.
- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.
- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

Der "[Cisco Support-Website](#)" Enthält Informationen zu den Befehlen zum Konfigurieren von Smart Call Home.

Hardware installieren

Füllen Sie das Cisco Nexus 3132Q-V-Verkabelungsarbeitsblatt aus

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

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

Jeder Switch kann als einzelner 40-GbE-Port oder als 4-x-GbE-Ports konfiguriert werden.

Beispiel für eine Verkabelung

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	4 x 10 GB/40 GB Node	1	4 x 10 GB/40 GB Node
2	4 x 10 GB/40 GB Node	2	4 x 10 GB/40 GB Node
3	4 x 10 GB/40 GB Node	3	4 x 10 GB/40 GB Node
4	4 x 10 GB/40 GB Node	4	4 x 10 GB/40 GB Node
5	4 x 10 GB/40 GB Node	5	4 x 10 GB/40 GB Node

Cluster-Switch A		Cluster-Switch B	
6	4 x 10 GB/40 GB Node	6	4 x 10 GB/40 GB Node
7	4 x 10 GB/40 GB Node	7	4 x 10 GB/40 GB Node
8	4 x 10 GB/40 GB Node	8	4 x 10 GB/40 GB Node
9	4 x 10 GB/40 GB Node	9	4 x 10 GB/40 GB Node
10	4 x 10 GB/40 GB Node	10	4 x 10 GB/40 GB Node
11	4 x 10 GB/40 GB Node	11	4 x 10 GB/40 GB Node
12	4 x 10 GB/40 GB Node	12	4 x 10 GB/40 GB Node
13	4 x 10 GB/40 GB Node	13	4 x 10 GB/40 GB Node
14	4 x 10 GB/40 GB Node	14	4 x 10 GB/40 GB Node
15	4 x 10 GB/40 GB Node	15	4 x 10 GB/40 GB Node
16	4 x 10 GB/40 GB Node	16	4 x 10 GB/40 GB Node
17	4 x 10 GB/40 GB Node	17	4 x 10 GB/40 GB Node
18	4 x 10 GB/40 GB Node	18	4 x 10 GB/40 GB Node
19	40 G-Node 19	19	40 G-Node 19
20	40 G-Node 20	20	40 G-Node 20
21	40 G-Node 21	21	40 G-Node 21
22	40 G-Node 22	22	40 G-Node 22
23	40 G-Node 23	23	40 G-Node 23
24	40 G-Node 24	24	40 G-Node 24
25 bis 30	Reserviert	25 bis 30	Reserviert
31	40 Gbit ISL für Switch B Port 31	31	40 Gbit ISL für Switch A Port 31

Cluster-Switch A		Cluster-Switch B	
32	40 Gbit ISL für Switch B Port 32	32	40 Gbit ISL für Switch A Port 32

Leeres Verkabelungsarbeitsblatt

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des "[Hardware Universe](#)" Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Node-/Port-Verwendung	Switch-Port	Node-/Port-Verwendung
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	

Cluster-Switch A		Cluster-Switch B	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25 bis 30	Reserviert	25 bis 30	Reserviert
31	40 Gbit ISL für Switch B Port 31	31	40 Gbit ISL für Switch A Port 31
32	40 Gbit ISL für Switch B Port 32	32	40 Gbit ISL für Switch A Port 32

Konfigurieren Sie den Cisco Nexus 3132Q-V Switch

Gehen Sie folgendermaßen vor, um den Cisco Nexus 3132Q-V Switch zu konfigurieren.

Was Sie benötigen

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von "[Cisco Software-Download](#)" Seite.
- Erforderliche Dokumentation für den Netzwerk-Switch, Controller-Dokumentation und ONTAP-Dokumentation Weitere Informationen finden Sie unter "[Erforderliche Dokumentation](#)".
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel
- Abgeschlossene Verkabelungsarbeitsblätter. Siehe "[Füllen Sie das Cisco Nexus 3132Q-V-Verkabelungsarbeitsblatt aus](#)".
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden "[mysupport.netapp.com](#)" Für die Switches, die Sie empfangen. Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, haben aber die RCFs nicht geladen.

Schritte


1. Rack-Aufbau des Cluster-Netzwerks und der Management-Netzwerk-Switches und -Controller


Wenn Sie das installieren...	Dann...
Cisco Nexus 3132Q-V in einem NetApp System-Rack	Anweisungen zur Installation des Switches in einem NetApp Schrank finden Sie im Dokument _Installation eines Cisco Nexus 3132Q-V Cluster-Switch und Pass-Through-Panel in einem NetApp Rack .
Geräte in einem Telco-Rack	Siehe die Verfahren in den Installationsleitfäden für die Switch-Hardware sowie in den Installations- und Setup-Anleitungen für NetApp.

2. Verkabeln Sie die Switches für das Cluster-Netzwerk und das Management-Netzwerk mithilfe des vollständigen Verkabelungsarbeitsblatts mit den Controllern, wie in beschrieben ["Füllen Sie das Cisco Nexus 3132Q-V-Verkabelungsarbeitsblatt aus"](#).
3. Schalten Sie das Cluster-Netzwerk sowie die Switches und Controller des Managementnetzwerks ein.
4. Initiale Konfiguration der Cluster-Netzwerk-Switches durchführen.

Geben Sie beim ersten Booten des Switches die folgenden Einrichtungsfragen entsprechend an. Die Sicherheitsrichtlinie Ihres Standorts definiert die zu erstellenden Antworten und Services.

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit ja . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (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, starkes Passwort erstellen. Ein schwaches Kennwort kann abgelehnt werden.
Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)	Reagieren Sie mit ja bei der Erstkonfiguration des Schalters.
Noch ein Login-Konto erstellen? (ja/nein)	Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen. Der Standardwert ist no .
Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein

Eingabeaufforderung	Antwort
Geben Sie den Switch-Namen ein.	Der Switch-Name ist auf 63 alphanumerische Zeichen begrenzt.
Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)	Beantworten Sie mit ja (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein.
Standard-Gateway konfigurieren? (ja/nein)	Antworten Sie mit ja . Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit ja. Die Standardeinstellung ist ja.</p> <div>  <p>SSH wird empfohlen, wenn Sie Cluster Switch Health Monitor (CSHM) für seine Protokollerfassung verwenden. SSHv2 wird auch für erhöhte Sicherheit empfohlen.</p> </div>
Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1).	Der Standardwert ist rsa .
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Schlüsselbits von 1024-2048 ein.
Konfigurieren Sie den NTP-Server? (ja/nein)	Antworten Sie mit Nein . Der Standardwert ist Nein
Standard-Schnittstellenebene konfigurieren (L3/L2):	Antworten Sie mit L2 . Der Standardwert ist L2.
Konfigurieren Sie den Status der Switch-Schnittstelle (shut/noshut) als Standard-Switch-Port:	Antworten Sie mit noshut . Die Standardeinstellung ist noshut.
Konfiguration des CoPP-Systemprofils (streng/mittel/lenient/dense):	Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.

Eingabeaufforderung	Antwort
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, antworten Sie mit No an der Eingabeaufforderung. Beantworten Sie mit ja , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.
Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)	<div> Antworten Sie mit ja, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert. </div> <div>  Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam. </div>

- Überprüfen Sie die Konfigurationseinstellungen, die Sie am Ende der Einrichtung in der Anzeige vorgenommen haben, und stellen Sie sicher, dass Sie die Konfiguration speichern.
- Überprüfen Sie die Version der Cluster-Netzwerk-Switches und laden Sie bei Bedarf die von NetApp unterstützte Version der Software von auf die Switches von herunter "[Cisco Software-Download](#)" Seite.

Was kommt als Nächstes?

"[Bereiten Sie sich auf die Installation von NX-OS und RCF vor](#)".

Installieren Sie einen Cisco Nexus 3132Q-V Cluster Switch in einem NetApp Rack

Je nach Konfiguration müssen Sie möglicherweise den Cisco Nexus 3132Q-V Switch und die Pass-Through-Panel in einem NetApp Rack mit den im Lieferumfang des Switches enthaltenen Standardhalterungen installieren.

Was Sie benötigen

- Die anfänglichen Vorbereitungsanforderungen, Inhalt des Kits und Sicherheitsvorkehrungen im "[Hardware-Installationsleitfaden Der Cisco Nexus 3000-Serie](#)". Lesen Sie diese Dokumente, bevor Sie mit dem Verfahren beginnen.
- Das Pass-Through-Panel-Kit, erhältlich von NetApp (Teilenummer X8784-R6). Das NetApp Pass-Through-Panel-Kit enthält die folgende Hardware:
 - Ein Durchlauf-Blindblech
 - Vier 10-32 x 0,75 Schrauben
 - Vier 10-32-Clip-Muttern
- Acht 10-32 oder 12-24 Schrauben und Befestigungsmuttern für die Befestigung der Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten.
- Cisco Standard-Schienensatz zur Installation des Switches in einem NetApp Rack



Die Jumper-Kabel sind nicht im Lieferumfang des Pass-Through-Kits enthalten und sollten in Ihrem Switch enthalten sein. Wenn die Switches nicht im Lieferumfang enthalten sind, können Sie sie bei NetApp bestellen (Teilenummer X1558A-R6).

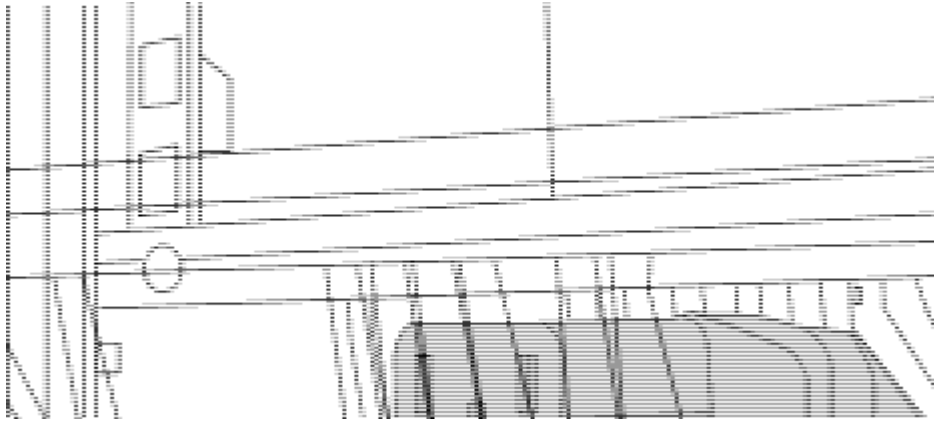
Schritte

1. Die Pass-Through-Blindplatte in den NetApp-Schrank einbauen.

- a. Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

Bei diesem Verfahren wird die Blindplatte in U40 installiert.

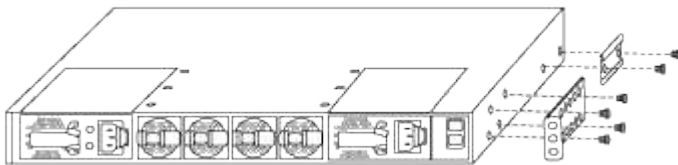
- b. Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
- c. Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
- d. Stecken Sie die Buchsen der beiden 48-Zoll-Jumper-Kabel von der Rückseite der Abdeckung und durch die Bürstenbaugruppe.



(1) Buchsenleiste des Überbrückungskabels.

2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Chassis des Nexus 3132Q-V.

- a. Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.



- b. Wiederholen Sie Schritt 2a mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
- c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.
- d. Wiederholen Sie Schritt 2c mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite des Schalters.

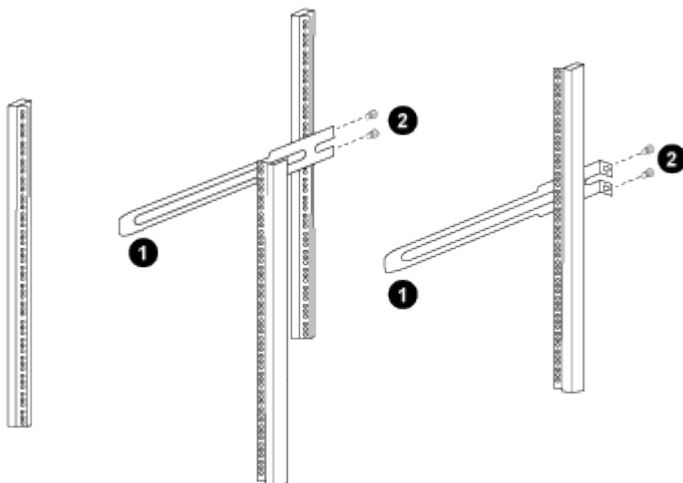
3. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



Die beiden 3132Q-V Schalter werden immer in den oberen 2 HE des Schrankes RU41 und 42 montiert.

4. Installieren Sie die Gleitschienen im Schrank.

- a. Positionieren Sie die erste Gleitschiene an der RU42-Markierung auf der Rückseite des hinteren linken Pfosten, legen Sie die Schrauben mit dem entsprechenden Gewindetyp ein und ziehen Sie die Schrauben mit den Fingern fest.



(1) beim sanften Schieben der Gleitschiene richten Sie sie an den Schraubenbohrungen im Rack aus.

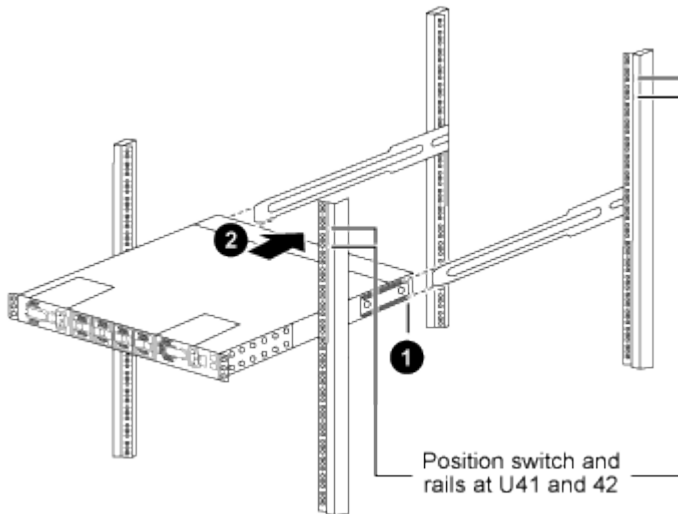
(2) Schrauben der Gleitschienen an den Schrankleisten festziehen.

- a. Wiederholen Sie Schritt 4a für den hinteren Pfosten auf der rechten Seite.
 - b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Stellen im Schrank.
5. Den Schalter in den Schrank einbauen.



Für diesen Schritt sind zwei Personen erforderlich: Eine Person muss den Schalter von vorne und von der anderen in die hinteren Gleitschienen führen.

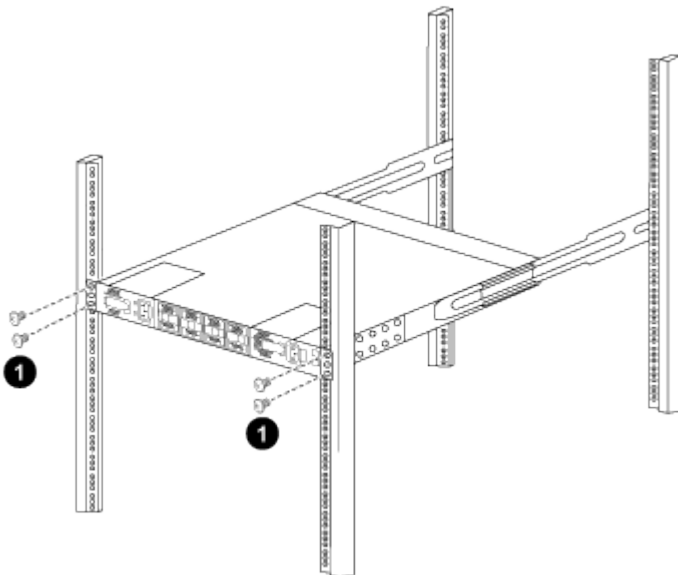
- a. Positionieren Sie die Rückseite des Schalters an RU41.



(1) Da das Gehäuse in Richtung der hinteren Pfosten geschoben wird, richten Sie die beiden hinteren Rackmontageführungen an den Gleitschienen aus.

(2) Schieben Sie den Schalter vorsichtig, bis die vorderen Halterungen der Rackmontage bündig mit den vorderen Pfosten sind.

- b. Befestigen Sie den Schalter am Gehäuse.



(1) mit einer Person, die die Vorderseite des Chassis hält, sollte die andere Person die vier hinteren Schrauben vollständig an den Schrankpfosten festziehen.

- a. Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- b. Wiederholen Sie die Schritte 5a bis 5c für den zweiten Schalter an der Position RU42.



Wenn Sie den vollständig installierten Switch als Support verwenden, müssen Sie während der Installation nicht die Vorderseite des zweiten Schalters halten.

6. Wenn die Switches installiert sind, verbinden Sie die Jumper-Kabel mit den Switch-Netzeinkabeln.
7. Verbinden Sie die Stecker beider Überbrückungskabel mit den am nächsten verfügbaren PDU-Steckdosen.



Um Redundanz zu erhalten, müssen die beiden Kabel mit verschiedenen PDUs verbunden werden.

8. Schließen Sie den Management Port an jedem 3132Q-V Switch an einen der Management Switches an (sofern bestellt), oder verbinden Sie sie direkt mit Ihrem Management-Netzwerk.

Der Management-Port ist der oben rechts gelegene Port auf der PSU-Seite des Switch. Das CAT6-Kabel für jeden Switch muss über die Passthrough-Leiste geführt werden, nachdem die Switches zur Verbindung mit den Management-Switches oder dem Management-Netzwerk installiert wurden.

Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 3132Q-V-Switch konfigurieren, gehen Sie die folgenden Überlegungen durch.

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

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 Switch-Port-Geschwindigkeit fest kodieren.

```
(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 ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

Software konfigurieren

Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei vor

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

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster-Interconnect-Ports e0a Und e0b.

Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` Und `cs2`.
- Die Node-Namen sind `cluster1-01` Und `cluster1-02`.
- Die LIF-Namen des Clusters sind `cluster1-01_clus1` Und `cluster1-01_clus2` Für Clustered 1-01 und `cluster1-02_clus1` Und `cluster1-02_clus2` Für Clustered 1-02.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritte

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind:

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

Beispiel anzeigen

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
cluster1-02/cdp	e0a	cs1	Eth1/2	N3K-
C3132Q-V	e0b	cs2	Eth1/2	N3K-
C3132Q-V				
cluster1-01/cdp	e0a	cs1	Eth1/1	N3K-
C3132Q-V	e0b	cs2	Eth1/1	N3K-
C3132Q-V				

4. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

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

```
Node: cluster1-02
```

						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						

b. Zeigt Informationen zu den LIFs an:

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

Beispiel anzeigen

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

Current Is	Logical	Status	Network	Current
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			

5. Ping für die Remote-Cluster-LIFs:

```
cluster ping-cluster -node local
```

Beispiel anzeigen

```
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)
```

6. Überprüfen Sie das `auto-revert` Befehl ist für alle Cluster-LIFs aktiviert:

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

Beispiel anzeigen

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

Vserver	Logical Interface	Auto-revert
Cluster	cluster1-01_clus1	true
	cluster1-01_clus2	true
	cluster1-02_clus1	true
	cluster1-02_clus2	true

Was kommt als Nächstes?

["Installation der NX-OS Software"](#).

Installieren Sie die NX-OS-Software

Gehen Sie folgendermaßen vor, um die NX-OS-Software auf dem Nexus 3132Q-V Cluster Switch zu installieren.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).

Vorgeschlagene Dokumentation

- ["Cisco Ethernet Switch"](#). In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Die entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website finden Sie in der vollständigen Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches.

Installieren Sie die Software

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Führen Sie den Vorgang in durch ["Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei vor"](#), Und dann folgen Sie den Schritten unten.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.

2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung mit dem Server, der die NX-OS-Software und die RCF hostet.

Beispiel anzeigen

```
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. Kopieren Sie die NX-OS-Software mit einem der folgenden Übertragungsprotokolle auf den Nexus 3132Q-V-Switch: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch unter ["Cisco Nexus 3000 Series NX-OS Command Reference Guides"](#).

Beispiel anzeigen

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

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

4. 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 04.25
  NXOS: version 9.3(3)
    BIOS compile time: 01/28/2020
    NXOS image file is: bootflash:///nxos.9.3.3.bin
      NXOS compile time: 12/22/2019 2:00:00 [12/22/2019
14:00:37]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```



```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
```

```
Reason: Reset Requested by CLI command reload
```

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Installieren Sie das NX-OS Image.

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

Beispiel anzeigen

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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

Compatibility check is done:
Module  bootable          Impact          Install-type  Reason
-----  -
      1      yes          disruptive          reset          default
upgrade is not hitless

Images will be upgraded according to following table:
Module      Image      Running-Version(pri:alt)
New-Version      Upg-Required
-----  -
      1      nxos      9.3(3)
9.3(4)          yes
      1      bios      v04.25(01/28/2020):v04.25(10/18/2016)
v04.25(01/28/2020)  no

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

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

```
[] 100% -- SUCCESS
```

```
Setting boot variables.
```

```
[] 100% -- SUCCESS
```

```
Performing configuration copy.
```

```
[] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

```
[] 100% -- SUCCESS
```

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

```
cs2#
```

6. 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 04.25
  NXOS: version 9.3(4)
  BIOS compile time: 05/22/2019
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time: 4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
  cisco Nexus 3132QV Chassis (Nexus 9000 Series)
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16399900 kB of memory.
  Processor Board ID FOxxxxxxx23

  Device name: cs2
  bootflash: 15137792 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 79 day(s), 10 hour(s), 23 minute(s), 53 second(s)
```

```
Last reset at 663500 usecs after Mon Nov  2 10:50:33 2020
Reason: Reset Requested by CLI command reload
System version: 9.3(4)
Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s) :

cs2#
```

Was kommt als Nächstes?

["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)."](#)

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Gehen Sie folgendermaßen vor, um den RCF nach dem ersten Einrichten des Nexus 3132Q-V-Schalters zu installieren. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle Referenzkonfigurationsdatei (RCF).
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.
- ["Cisco Ethernet Switch"](#). In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Die entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website finden Sie in der vollständigen Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches.

Installieren Sie die Datei

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` und `cs2`.
- Die Node-Namen sind `cluster1-01`, `cluster1-02`, `cluster1-03`, und `cluster1-04`.
- Die LIF-Namen des Clusters 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::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Führen Sie den Vorgang in durch ["Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei vor"](#), Und dann folgen Sie den Schritten unten.

Schritt 1: Überprüfen Sie den Portstatus

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
           e0a    cs1                      Ethernet1/7      N3K-
C3132Q-V
           e0d    cs2                      Ethernet1/7      N3K-
C3132Q-V
cluster1-02/cdp
           e0a    cs1                      Ethernet1/8      N3K-
C3132Q-V
           e0d    cs2                      Ethernet1/8      N3K-
C3132Q-V
cluster1-03/cdp
           e0a    cs1                      Ethernet1/1/1    N3K-
C3132Q-V
           e0b    cs2                      Ethernet1/1/1    N3K-
C3132Q-V
cluster1-04/cdp
           e0a    cs1                      Ethernet1/1/2    N3K-
C3132Q-V
           e0b    cs2                      Ethernet1/1/2    N3K-
C3132Q-V
cluster1::*>
```

2. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen 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

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

cluster1::*>

b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

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

Current	Logical	Status	Network	
Vserver	Current Is			
Port	Interface	Admin/Oper	Address/Mask	Node
Home				

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

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

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

Beispiel anzeigen

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

cs2                                     cluster-network     10.0.0.2
NX3132QV
    Serial Number: FOXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                        9.3(4)
    Version Source: CDP

2 entries were displayed.
```



Verwenden Sie für ONTAP 9.8 und höher den Befehl `system switch ethernet show -is-monitoring-enabled-operational true`.

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

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

Stellen Sie sicher, dass die automatische Umrüstung deaktiviert ist, nachdem Sie diesen Befehl ausgeführt haben.

4. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

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

- Überprüfen Sie, ob die Cluster-Ports zu den Ports migriert wurden, die auf 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::*>
```

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

```
cluster show
```

Beispiel anzeigen

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

Schritt 2: Konfigurieren und überprüfen Sie das Setup

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

```
show running-config
```

2. Reinigen Sie die Konfiguration am Schalter cs2, und führen Sie eine grundlegende Einrichtung durch.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload

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

3. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im ["Cisco Nexus 3000-Serie NX-OS Command Reference"](#) Leitfäden.

Beispiel anzeigen

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

4. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

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

Beispiel anzeigen

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

5. Untersuchen Sie die Bannerausgabe aus dem `show banner motd` Befehl. Sie müssen die Anweisungen unter **wichtige Hinweise** lesen und befolgen, um die korrekte Konfiguration und den korrekten Betrieb des Schalters zu gewährleisten.

Beispiel anzeigen

```
cs2# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch    : Cisco Nexus 3132Q-V
* Filename  : Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt
* Date      : Nov-02-2020
* Version   : v1.6
*
* Port Usage : Breakout configuration
* Ports 1- 6: Breakout mode (4x10GbE) Intra-Cluster Ports, int
e1/1/1-4,
* e1/2/1-4, e1/3/1-4,int e1/4/1-4, e1/5/1-4, e1/6/1-4
* Ports 7-30: 40GbE Intra-Cluster/HA Ports, int e1/7-30
* Ports 31-32: Intra-Cluster ISL Ports, int e1/31-32
*
* IMPORTANT NOTES
* - Load Nexus_3132QV_RCF_v1.6-Cluster-HA.txt for non breakout
config
*
* - This RCF utilizes QoS and requires specific TCAM configuration,
requiring
*   cluster switch to be rebooted before the cluster becomes
operational.
*
* - Perform the following steps to ensure proper RCF installation:
*
*   (1) Apply RCF, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class
IPv4...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*
*   (4) Save running-configuration again
*
```

```

* - If running NX-OS versions 9.3(5) 9.3(6), 9.3(7), or 9.3(8)
*   - Downgrade the NX-OS firmware to version 9.3(5) or earlier if
*     NX-OS using a version later than 9.3(5).
*   - Do not upgrade NX-OS prior to applying v1.9 RCF file.
*   - After the RCF is applied and switch rebooted, then proceed to
upgrade
*     NX-OS to version 9.3(5) or later.
*
* - If running 9.3(9) 10.2(2) or later the RCF can be applied to the
switch
*   after the upgrade.
*
* - Port 1 multiplexed H/W configuration options:
*   hardware profile front portmode qsfp      (40G H/W port 1/1 is
active - default)
*   hardware profile front portmode sfp-plus  (10G H/W ports 1/1/1
- 1/1/4 are active)
*   hardware profile front portmode qsfp      (To reset to QSFP)
*
*****
*****

```

6. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteeinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.



Wie Sie Ihre 10-GbE-Ports nach einem Upgrade des RCF online schalten können, erfahren Sie in dem Knowledge Base Artikel ["10-GbE-Ports auf einem Cisco 3132Q Cluster-Switch werden nicht online geschaltet"](#).

7. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

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

Beispiel anzeigen

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

8. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

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

9. Wenden Sie dieselbe RCF an, und speichern Sie die ausgeführte Konfiguration ein zweites Mal.

Beispiel anzeigen

```
cs2# copy Nexus_3132QV_RCF_v1.6-Cluster-HA-Breakout.txt running-  
config echo-commands  
cs2# copy running-config startup-config  
[#####] 100% Copy complete
```

10. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.
- a. Vergewissern Sie sich, dass Cluster-Ports über alle Nodes im Cluster hinweg ordnungsgemäß hochaktiv sind:

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

Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

Health	Health					Speed (Mbps)
Port	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					

b. Überprüfen Sie den Switch-Zustand vom Cluster.

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

Beispiel anzeigen

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

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

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

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

Switch	Type	Address
Model		

cs1	cluster-network	10.233.205.90
N3K-C3132Q-V		
Serial Number: FOXXXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
9.3(4)		
Version Source: CDP		
cs2	cluster-network	10.233.205.91

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

2 entries were displayed.
```



Verwenden Sie für ONTAP 9.8 und höher den Befehl `system switch ethernet show -is-monitoring-enabled-operational true`.

Je nach der zuvor auf dem Switch geladenen RCF-Version können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:



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

+



Es kann bis zu 5 Minuten dauern, bis die Cluster-Nodes einen ordnungsgemäßen Zustand melden.

11. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	false		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

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

```
cluster show
```

Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```
4 entries were displayed.  
cluster1::*>
```

14. Wiederholen Sie die Schritte 1 bis 10 am Schalter cs1.
15. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

16. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

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

Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die mit den Cluster-Ports verbundenen Switch-Ports aktiv sind.

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

Beispiel anzeigen

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

2. Stellen Sie sicher, dass die ISL zwischen cs1 und cs2 funktionsfähig ist:

```
show port-channel summary
```

Beispiel anzeigen

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
cs1#
```

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

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


Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		

```
cluster1::*>
```

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

```
cluster show
```

Beispiel anzeigen

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

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
cluster1-01	true	true	false
cluster1-02	true	true	false
cluster1-03	true	true	true
cluster1-04	true	true	false

```
cluster1::*>
```

5. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

```
cluster ping-cluster -node local
```

Beispiel anzeigen

```
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)
```

6. Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassungsfunktion für die

Systemzustandsüberwachung Ethernet Switch, um Switch-bezogene Protokolldateien zu erfassen. Verwenden Sie dazu die folgenden Befehle:

```
system switch ethernet log setup-password
```

```
system switch ethernet log enable-collection
```

a. Geben Sie Ein: `system switch ethernet log setup-password`

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

b. Geben Sie Ein: `system switch ethernet log enable-collection`

Beispiel anzeigen

```
cluster1::*> system switch ethernet log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

7. Aktivieren Sie bei Patch-Releases von ONTAP Releases 9.5P16, 9.6P12 und 9.7P10 sowie höher die Protokollerfassung der Ethernet Switch-Systemzustandsüberwachung mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien:

```
system cluster-switch log setup-password Und
```

```
system cluster-switch log enable-collection
```

- a. Geben Sie Ein: `system cluster-switch log setup-password`

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

b. Geben Sie Ein: `system cluster-switch log enable-collection`

Beispiel anzeigen

```
cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung mit dem Cisco 3132Q-V Cluster Switch * CLI* eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und prüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 3132Q-V-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```

Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>

(sw1) (Config)# show snmp user

-----
-----
                        SNMP USERS
-----
-----

User                Auth                Priv(enforce)    Groups
acl_filter
-----
-----
admin                md5                des(no)          network-admin
SNMPv3User           md5                aes-128(no)      network-operator
-----
-----

      NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----

User                Auth                Priv
-----
-----

(sw1) (Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N3K-C3132Q-V
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N3K-C3132Q-V
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Switches migrieren

Migrieren Sie einen Cisco Nexus 5596 Cluster-Switch auf einen Cisco Nexus 3132Q-V Cluster-Switch

Gehen Sie folgendermaßen vor, um einen vorhandenen Nexus 5596 Cluster Switch durch einen Nexus 3132Q-V Cluster Switch zu ersetzen.

Prüfen Sie die Anforderungen

Prüfen Sie die Cisco Nexus 5596-Anforderungen in ["Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster Switches"](#).

Weitere Informationen finden Sie unter:

- ["Beschreibungsseite für den Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Tauschen Sie den Schalter aus

Zu den Beispielen

Die Beispiele in diesem Verfahren beschreiben den Austausch von Nexus 5596 Switches durch Nexus 3132Q-V Switches. Mit diesen Schritten (durch Änderungen) können andere ältere Cisco Switches ersetzt werden.

Für das Verfahren wird die folgende Nomenklatur von Switches und Nodes verwendet:

- Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.
- Die zu ersetzenden Nexus 5596 Switches sind CL1 und CL2.
- Die Nexus 3132Q-V-Switches als Ersatz für die Nexus 5596-Switches sind C1 und C2.
- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die mit Cluster-Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- n1_clus2 ist die erste Cluster-LIF, die mit Cluster-Switch 2 (CL2 oder C2) für Node n1 verbunden ist.
- n1_clus3 ist die zweite logische Schnittstelle, die mit Cluster Switch 2 (CL2 oder C2) für Knoten n1 verbunden ist.
- n1_clus4 ist die zweite logische Schnittstelle, die mit Cluster Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- Die Knoten sind n1, n2, n3 und n4.
- Die Beispiele in diesem Verfahren verwenden vier Nodes: Zwei Nodes verwenden vier 10-GbE-Cluster-Interconnect-Ports: e0a, e0b, e0c und e0d. Die anderen beiden Knoten verwenden zwei 40/100 GbE Cluster Interconnect Ports: e4a, e4e. Der ["Hardware Universe"](#) Listet die tatsächlichen Cluster-Ports auf Ihren Plattformen auf.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert ["Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen"](#) Seite.



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Über diese Aufgabe

Dieses Verfahren umfasst folgende Szenarien:

- Das Cluster beginnt mit zwei verbundenen Nodes und funktioniert in einem 2 Nexus 5596 Cluster-Switch.
- Der zu ersetzende Cluster-Switch CL2 durch C2 ([Schritt 1 - 19](#))
 - Der Traffic auf allen Cluster-Ports und LIFs auf allen mit CL2 verbundenen Nodes wird zu den ersten Cluster-Ports migriert und mit CL1 verbundene LIFs.
 - Trennen Sie die Verkabelung von allen Cluster-Ports auf allen mit CL2 verbundenen Nodes, und verwenden Sie dann die unterstützte Breakout-Verkabelung, um die Ports wieder mit dem neuen Cluster-Switch C2 zu verbinden.
 - Trennen Sie die Verkabelung zwischen ISL-Ports zwischen CL1 und CL2, und verwenden Sie dann die unterstützte Breakout-Verkabelung, um die Ports von CL1 an C2 wiederherzustellen.
 - Der Datenverkehr auf allen Cluster-Ports und LIFs, die mit C2 verbunden sind, wird auf allen Nodes zurückgesetzt.
- Der Cluster-Switch CL2, der durch C2 ersetzt werden soll
 - Der Datenverkehr aller Cluster-Ports oder LIFs auf allen mit CL1 verbundenen Nodes wird zu den zweiten Cluster-Ports oder zu LIFs migriert, die mit C2 verbunden sind.
 - Trennen Sie die Verkabelung von allen Cluster-Ports auf allen mit CL1 verbundenen Knoten, und verbinden Sie sie über unterstützte Breakout-Kabel mit dem neuen Cluster-Switch C1.

- Trennen Sie die Verkabelung zwischen ISL-Ports zwischen CL1 und C2, und schließen Sie sie über unterstützte Kabel von C1 bis C2 wieder an.
- Der Verkehr auf allen Cluster-Ports oder LIFs, die mit C1 auf allen Nodes verbunden sind, wird zurückgesetzt.
- Zwei FAS9000 Nodes wurden dem Cluster hinzugefügt, wobei Beispiele für Cluster-Details zeigen.

Schritt 1: Vorbereitung auf den Austausch

Um einen vorhandenen Nexus 5596 Cluster Switch durch einen Nexus 3132Q-V Cluster-Switch zu ersetzen, müssen Sie eine bestimmte Sequenz von Aufgaben durchführen.

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=xh`

X ist die Dauer des Wartungsfensters in Stunden.



Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit während des Wartungsfensters die automatische Case-Erstellung unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device-discovery show
```

Beispiel anzeigen

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

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	CL1	Ethernet1/1	N5K-C5596UP
	e0b	CL2	Ethernet1/1	N5K-C5596UP
	e0c	CL2	Ethernet1/2	N5K-C5596UP
	e0d	CL1	Ethernet1/2	N5K-C5596UP
n2	/cdp			
	e0a	CL1	Ethernet1/3	N5K-C5596UP
	e0b	CL2	Ethernet1/3	N5K-C5596UP
	e0c	CL2	Ethernet1/4	N5K-C5596UP
	e0d	CL1	Ethernet1/4	N5K-C5596UP

8 entries were displayed.

3. Legen Sie den Administrations- oder Betriebsstatus für jede Cluster-Schnittstelle fest:

a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show
```


Beispiel anzeigen

Im folgenden Beispiel werden die Netzwerkanschlussattribute auf einem System angezeigt:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

8 entries were displayed.
```

a. Informationen zu den logischen Schnittstellen anzeigen:

```
network interface show
```

Beispiel anzeigen

Im folgenden Beispiel werden die allgemeinen Informationen zu allen LIFs auf Ihrem System angezeigt:

```
cluster::*> network interface show -role cluster
(network interface show)

Current Is      Logical      Status      Network      Current
Vserver      Interface  Admin/Oper  Address/Mask  Node
Port      Home
-----
Cluster
e0a      true      n1_clus1   up/up         10.10.0.1/24   n1
e0b      true      n1_clus2   up/up         10.10.0.2/24   n1
e0c      true      n1_clus3   up/up         10.10.0.3/24   n1
e0d      true      n1_clus4   up/up         10.10.0.4/24   n1
e0a      true      n2_clus1   up/up         10.10.0.5/24   n2
e0b      true      n2_clus2   up/up         10.10.0.6/24   n2
e0c      true      n2_clus3   up/up         10.10.0.7/24   n2
e0d      true      n2_clus4   up/up         10.10.0.8/24   n2
8 entries were displayed.
```

b. Informationen über die erkannten Cluster-Switches anzeigen:

```
system cluster-switch show
```

Beispiel anzeigen

Im folgenden Beispiel werden die Cluster-Switches, die dem Cluster bekannt sind, mit ihren Management-IP-Adressen angezeigt:

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

2 entries were displayed.

4. Stellen Sie die ein `-auto-revert` Parameter an `false` Auf Cluster LIFs `clu1` und `clu2` zu beiden Knoten:

```
network interface modify
```

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto  
-revert false  
cluster::*> network interface modify -vserver node1 -lif clus2 -auto  
-revert false  
cluster::*> network interface modify -vserver node2 -lif clus1 -auto  
-revert false  
cluster::*> network interface modify -vserver node2 -lif clus2 -auto  
-revert false
```

5. Überprüfen Sie, ob die entsprechenden RCF und das entsprechende Image auf den neuen 3132Q-V-Switches installiert sind, wenn dies für Ihre Anforderungen erforderlich ist, und nehmen Sie die wesentlichen Standortanpassungen vor, z. B. Benutzer und Passwörter, Netzwerkadressen usw.

Sie müssen beide Switches derzeit vorbereiten. Gehen Sie wie folgt vor, wenn Sie ein Upgrade für RCF und Image durchführen müssen:

- Wechseln Sie zum ["Cisco Ethernet-Switches"](#) Auf der NetApp Support Site finden.
- Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
- Laden Sie die entsprechende Version des RCF herunter.
- Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
- Laden Sie die entsprechende Version der Bildsoftware herunter.

Besuchen Sie die Seite *ONTAP 8.x oder höher Referenzkonfigurationsdateien für Cluster und Netzwerk-Management-Switches*Download, und klicken Sie dann auf die entsprechende Version.

Informationen zur richtigen Version finden Sie auf der Download-Seite „*ONTAP 8.x“ oder höher für Cluster-Netzwerk-Switch*.

6. Migrieren Sie die LIFs, die mit dem zweiten Nexus 5596 Switch verbunden sind, der ersetzt werden soll:

```
network interface migrate
```

Beispiel anzeigen

Das folgende Beispiel zeigt n1 und n2, die LIF-Migration muss jedoch auf allen Knoten durchgeführt werden:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -
destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -
destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -
destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -
destination-node n2 -destination-port e0d
```

7. Überprüfen Sie den Systemzustand des Clusters:

```
network interface show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Ergebnis des vorherigen `network interface migrate` Befehl:

```
cluster::*> network interface show -role cluster
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0a	false			
	n1_clus3	up/up	10.10.0.3/24	n1
e0d	false			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0a	false			
	n2_clus3	up/up	10.10.0.7/24	n2
e0d	false			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			

8 entries were displayed.

8. Fahren Sie die Cluster-Interconnect-Ports herunter, die physisch mit dem Switch CL2 verbunden sind:

```
network port modify
```

Beispiel anzeigen

Die folgenden Befehle fahren die angegebenen Ports auf n1 und n2 herunter, die Ports müssen jedoch auf allen Knoten heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie Sie die Remote-Cluster-Schnittstellen pingen:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```


10. Fahren Sie die ISL-Ports 41 bis 48 am aktiven Nexus 5596-Switch CL1 herunter:

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die ISL-Ports 41 bis 48 auf dem Nexus 5596-Switch CL1 heruntergefahren werden:

```
(CL1)# configure
(CL1) (Config)# interface e1/41-48
(CL1) (config-if-range)# shutdown
(CL1) (config-if-range)# exit
(CL1) (Config)# exit
(CL1) #
```

Wenn Sie einen Nexus 5010 oder 5020 ersetzen, geben Sie die entsprechenden Portnummern für ISL an.

11. Stellen Sie eine temporäre ISL zwischen CL1 und C2 her.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass ein temporärer ISL zwischen CL1 und C2 eingerichtet wird:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

Schritt 2: Ports konfigurieren

1. Entfernen Sie auf allen Knoten alle Kabel, die am Nexus 5596 Switch CL2 angeschlossen sind.

Schließen Sie bei der unterstützten Verkabelung die getrennten Ports aller Knoten wieder an den Nexus 3132Q-V Switch C2 an.

2. Entfernen Sie alle Kabel vom Nexus 5596 Switch CL2.

Verbinden Sie die entsprechenden Cisco QSFP-Kabel mit SFP+-Breakout-Kabel, die Port 1/24 am neuen Cisco 3132Q-V Switch C2 an die Anschlüsse 45 bis 48 auf dem vorhandenen Nexus 5596, CL1

anschließen.

3. Vergewissern Sie sich, dass die Schnittstellen eth1/45-48 bereits vorhanden sind `channel-group 1 mode active` in ihrer laufenden Konfiguration.
4. ISLs-Ports 45 bis 48 auf dem aktiven Nexus 5596 Switch CL1 wechseln

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISLs-Ports 45 bis 48 aufgerufen werden:

```
(CL1)# configure
(CL1)(Config)# interface e1/45-48
(CL1)(config-if-range)# no shutdown
(CL1)(config-if-range)# exit
(CL1)(Config)# exit
(CL1)#
```

5. Überprüfen Sie, ob es sich bei den ISLs um handelt `up` Beim Nexus 5596 Switch CL1:

```
show port-channel summary
```

Beispiel anzeigen

Die Ports eth1/45 bis eth1/48 sollten (P) angeben, was bedeutet, dass die ISL-Ports laufen `up` Im Port-Kanal:

Example

```
CL1# 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
       S - Switched      R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type   Protocol  Member Ports
      Channel
-----
-----
1      Po1 (SU)      Eth    LACP      Eth1/41 (D)  Eth1/42 (D)
Eth1/43 (D)
                                   Eth1/44 (D)  Eth1/45 (P)
Eth1/46 (P)
                                   Eth1/47 (P)  Eth1/48 (P)
```

6. Überprüfen Sie, ob es sich bei den ISLs um handelt `up` Am 3132Q-V Schalter C2:

```
show port-channel summary
```

Beispiel anzeigen

Die Ports eth1/24/1, eth1/24/2, eth1/24/3 und eth1/24/4 sollten (P) angeben, d. h. die ISL-Ports sind up im Port-Kanal:

```
C2# 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
      S - Switched      R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (D)  Eth1/32 (D)
2      Po2 (SU)       Eth     LACP      Eth1/24/1 (P) Eth1/24/2 (P)
Eth1/24/3 (P)
                                   Eth1/24/4 (P)
```

7. Fahren Sie auf allen Knoten alle Cluster-Interconnect-Ports ein, die mit dem 3132Q-V Switch C2 verbunden sind.

```
network port modify
```

Beispiel anzeigen

Im folgenden Beispiel werden die angegebenen Ports angezeigt, die auf den Knoten n1 und n2 aufgerufen werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

8. Stellen Sie auf allen Nodes alle migrierten Cluster-Interconnect-LIFs zurück, die mit C2 verbunden sind:

```
network interface revert
```

Beispiel anzeigen

Im folgenden Beispiel werden die migrierten Cluster-LIFs angezeigt, die auf ihre Home-Ports auf den Nodes n1 und n2 zurückgesetzt werden:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

9. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports nun auf ihr Home zurückgesetzt werden:

```
network interface show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die LIFs auf Fa.2 auf ihre Home-Ports zurückgesetzt werden und zeigt, dass die LIFs erfolgreich zurückgesetzt werden, wenn die Ports in der Spalte „Current Port“ den Status aufweisen `true` Im `Is Home` Spalte. Wenn der `Is Home` Wert ist `false`, Das LIF wurde nicht zurückgesetzt.

```
cluster::*> network interface show -role cluster
(network interface show)

Current Is      Logical   Status   Network   Current
Vserver      Interface Admin/Oper Address/Mask Node
Port        Home
-----
Cluster
e0a          true      n1_clus1 up/up     10.10.0.1/24 n1
e0b          true      n1_clus2 up/up     10.10.0.2/24 n1
e0c          true      n1_clus3 up/up     10.10.0.3/24 n1
e0d          true      n1_clus4 up/up     10.10.0.4/24 n1
e0a          true      n2_clus1 up/up     10.10.0.5/24 n2
e0b          true      n2_clus2 up/up     10.10.0.6/24 n2
e0c          true      n2_clus3 up/up     10.10.0.7/24 n2
e0d          true      n2_clus4 up/up     10.10.0.8/24 n2
8 entries were displayed.
```

10. Vergewissern Sie sich, dass die Cluster-Ports verbunden sind:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Ergebnis des vorherigen `network port modify` Befehl, Überprüfung der Cluster Interconnects up:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

11. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster
```


Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie Sie die Remote-Cluster-Schnittstellen pingen:

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

12. Migrieren Sie bei jedem Node im Cluster die Schnittstellen, die mit dem ersten Nexus 5596 Switch CL1 verbunden sind, der ersetzt werden soll:

```
network interface migrate
```

Beispiel anzeigen

Im folgenden Beispiel werden die Ports oder LIFs angezeigt, die auf den Nodes n1 und n2 migriert werden:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1
-source-node n1 -
destination-node n1 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4
-source-node n1 -
destination-node n1 -destination-port e0c
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1
-source-node n2 -
destination-node n2 -destination-port e0b
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4
-source-node n2 -
destination-node n2 -destination-port e0c
```

13. Überprüfen Sie den Cluster-Status:

```
network interface show
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, dass die erforderlichen Cluster-LIFs zu geeigneten Cluster-Ports migriert wurden, die auf Cluster-Switch gehostet werden.C2:

```
(network interface show)

Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e0b n1_clus1 up/up 10.10.0.1/24 n1
false
e0b n1_clus2 up/up 10.10.0.2/24 n1
true
e0c n1_clus3 up/up 10.10.0.3/24 n1
true
e0c n1_clus4 up/up 10.10.0.4/24 n1
false
e0b n2_clus1 up/up 10.10.0.5/24 n2
false
e0b n2_clus2 up/up 10.10.0.6/24 n2
true
e0c n2_clus3 up/up 10.10.0.7/24 n2
true
e0c n2_clus4 up/up 10.10.0.8/24 n2
false
8 entries were displayed.

-----
```

14. Fahren Sie auf allen Nodes die Node-Ports herunter, die mit CL1 verbunden sind:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt die angegebenen Anschlüsse, die auf den Knoten n1 und n2 heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

15. Fahren Sie die ISL-Ports 24, 31 und 32 am aktiven Switch 3132Q-V C2 herunter.

shutdown

Beispiel anzeigen

Das folgende Beispiel zeigt, wie ISLs 24, 31 und 32 heruntergefahren werden:

```
C2# configure
C2(Config)# interface e1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config-if)# exit
C2#
```

16. Entfernen Sie auf allen Knoten alle Kabel, die am Nexus 5596 Switch CL1 angeschlossen sind.

Schließen Sie bei der unterstützten Verkabelung die getrennten Ports aller Knoten wieder an den Nexus 3132Q-V Switch C1 an.

17. Entfernen Sie das QSFP-Breakout-Kabel von den Nexus 3132Q-V C2-Ports e1/24.

Verbinden Sie die Ports e1/31 und e1/32 auf C1 mit den Ports e1/31 und e1/32 auf C2 unter Verwendung der unterstützten Cisco QSFP-Glasfaserkabel oder Direct-Attached-Kabel.

18. Stellen Sie die Konfiguration an Port 24 wieder her, und entfernen Sie den temporären Port Channel 2 auf C2:

```

C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# int e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.

```

19. ISL-Ports 31 und 32 auf C2, dem aktiven 3132Q-V Switch: no shutdown

Beispiel anzeigen

Das folgende Beispiel zeigt, wie ISLs 31 und 32 auf dem 3132Q-V Switch C2:

```

C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.

```

Schritt 3: Überprüfen Sie die Konfiguration

1. Stellen Sie sicher, dass die ISL-Verbindungen sind up Am 3132Q-V Schalter C2:

```
show port-channel summary
```

Beispiel anzeigen

Die Ports eth1/31 und eth1/32 sollten angegeben werden (P), Was bedeutet, dass beide ISL-Ports sind up Im Port-Kanal:

```
C1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

2. Bringen Sie auf allen Knoten alle Cluster Interconnect Ports an, die mit dem neuen 3132Q-V Switch C1 verbunden sind:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt alle Cluster-Interconnect-Ports, die für n1 und n2 auf dem 3132Q-V-Switch C1 aufgerufen werden:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

3. Überprüfen Sie den Status des Cluster-Node-Ports:

```
network port show
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Interconnect-Ports auf allen Knoten des neuen Switch C1 3132Q-V überprüft up:

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-

Node: n2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e0a        Cluster      Cluster      up    9000  auto/10000  -
-
e0b        Cluster      Cluster      up    9000  auto/10000  -
-
e0c        Cluster      Cluster      up    9000  auto/10000  -
-
e0d        Cluster      Cluster      up    9000  auto/10000  -
-
8 entries were displayed.
```

4. Setzen Sie auf allen Nodes die spezifischen Cluster-LIFs auf ihre Home-Ports zurück:

```
network interface revert
```

Beispiel anzeigen

Im folgenden Beispiel werden die spezifischen Cluster-LIFs angezeigt, die auf ihre Home-Ports auf den Nodes n1 und n2 zurückgesetzt werden:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Vergewissern Sie sich, dass die Schnittstelle Home ist:

```
network interface show
```


Beispiel anzeigen

Im folgenden Beispiel wird der Status von Cluster-Interconnect-Schnittstellen angezeigt up Und Is home Für n1 und n2:

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e0a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e0b      true
      n1_clus3      up/up      10.10.0.3/24      n1
e0c      true
      n1_clus4      up/up      10.10.0.4/24      n1
e0d      true
      n2_clus1      up/up      10.10.0.5/24      n2
e0a      true
      n2_clus2      up/up      10.10.0.6/24      n2
e0b      true
      n2_clus3      up/up      10.10.0.7/24      n2
e0c      true
      n2_clus4      up/up      10.10.0.8/24      n2
e0d      true
8 entries were displayed.
```

6. Pingen Sie die Remote-Cluster-Schnittstellen und führen Sie dann eine Remote-Prozedur aus Rufen Sie den Server an:

```
cluster ping-cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie Sie die Remote-Cluster-Schnittstellen pingen:

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8
Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)
```

7. Erweitern Sie das Cluster durch Hinzufügen von Nodes zu den Nexus 3132Q-V Cluster Switches.

8. Zeigen Sie die Informationen zu den Geräten in Ihrer Konfiguration an:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

Beispiel anzeigen

Die folgenden Beispiele zeigen die Nodes n3 und n4 mit 40-GbE-Cluster-Ports, die mit den Ports e1/7 und e1/8 verbunden sind, bzw. auf den Nexus 3132Q-V Cluster-Switches, und beide Nodes haben sich dem Cluster angeschlossen. Die 40 GbE Cluster Interconnect Ports sind e4a und e4e.

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-
C3132Q-V	e0b	C2	Ethernet1/1/1	N3K-
C3132Q-V	e0c	C2	Ethernet1/1/2	N3K-
C3132Q-V	e0d	C1	Ethernet1/1/2	N3K-
C3132Q-V				
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-
C3132Q-V	e0b	C2	Ethernet1/1/3	N3K-
C3132Q-V	e0c	C2	Ethernet1/1/4	N3K-
C3132Q-V	e0d	C1	Ethernet1/1/4	N3K-
C3132Q-V				
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-
C3132Q-V	e4e	C2	Ethernet1/7	N3K-
C3132Q-V				
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-
C3132Q-V	e4e	C2	Ethernet1/8	N3K-
C3132Q-V				

12 entries were displayed.

```
cluster::*> network port show -role cluster
(network port show)
Node: n1
```

Ignore

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

e0a	Cluster	Cluster		up	9000	auto/10000 -
-						
e0b	Cluster	Cluster		up	9000	auto/10000 -
-						
e0c	Cluster	Cluster		up	9000	auto/10000 -
-						
e0d	Cluster	Cluster		up	9000	auto/10000 -
-						

Node: n2

Ignore

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

e0a	Cluster	Cluster		up	9000	auto/10000 -
-						
e0b	Cluster	Cluster		up	9000	auto/10000 -
-						
e0c	Cluster	Cluster		up	9000	auto/10000 -
-						
e0d	Cluster	Cluster		up	9000	auto/10000 -
-						

Node: n3

Ignore

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

e4a	Cluster	Cluster		up	9000	auto/40000 -
-						
e4e	Cluster	Cluster		up	9000	auto/40000 -

```

-

Node: n4

Ignore

Health      Health      Speed (Mbps)
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e4a      Cluster      Cluster      up      9000 auto/40000 -
-
e4e      Cluster      Cluster      up      9000 auto/40000 -
-
12 entries were displayed.

```

```
cluster::*> network interface show -role cluster
```

```
(network interface show)
```

		Logical	Status	Network	Current
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask		Node
Port	Home				

Cluster					
		n1_clus1	up/up	10.10.0.1/24	n1
e0a	true				
		n1_clus2	up/up	10.10.0.2/24	n1
e0b	true				
		n1_clus3	up/up	10.10.0.3/24	n1
e0c	true				
		n1_clus4	up/up	10.10.0.4/24	n1
e0d	true				
		n2_clus1	up/up	10.10.0.5/24	n2
e0a	true				
		n2_clus2	up/up	10.10.0.6/24	n2
e0b	true				
		n2_clus3	up/up	10.10.0.7/24	n2
e0c	true				
		n2_clus4	up/up	10.10.0.8/24	n2
e0d	true				
		n3_clus1	up/up	10.10.0.9/24	n3
e4a	true				
		n3_clus2	up/up	10.10.0.10/24	n3
e4e	true				
		n4_clus1	up/up	10.10.0.11/24	n4
e4a	true				
		n4_clus2	up/up	10.10.0.12/24	n4
e4e	true				

```
12 entries were displayed.
```

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL1 NX5596	cluster-network	10.10.1.101
Serial Number: 01234567		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		
CL2 NX5596	cluster-network	10.10.1.102
Serial Number: 01234568		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
7.1(1)N1(1)		
Version Source: CDP		

4 entries were displayed.

9. Entfernen Sie den ausgetauschten Nexus 5596, wenn sie nicht automatisch entfernt werden:

```
system cluster-switch delete
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Nexus 5596 entfernt wird:

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

10. Konfigurieren Sie Cluster clue1 und clu2, um jeden Knoten automatisch zurückzusetzen und zu bestätigen.

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto  
-revert true  
cluster::*> network interface modify -vserver node1 -lif clus2 -auto  
-revert true  
cluster::*> network interface modify -vserver node2 -lif clus1 -auto  
-revert true  
cluster::*> network interface modify -vserver node2 -lif clus2 -auto  
-revert true
```

11. Überprüfen Sie, ob die richtigen Cluster-Switches überwacht werden:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

12. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
**RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

13. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

Migration von CN1610 Cluster-Switches zu Cisco Nexus 3132Q-V Cluster-Switches

Gehen Sie folgendermaßen vor, um die vorhandenen CN1610 Cluster Switches durch Cisco Nexus 3132Q-V Cluster Switches zu ersetzen.

Prüfen Sie die Anforderungen

Überprüfen Sie die Anforderungen der NetApp CN1610 in ["Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster Switches"](#).

Weitere Informationen finden Sie unter:

- ["Beschreibungsseite zu NetApp CN1601 und CN1610"](#)
- ["Beschreibungsseite für den Cisco Ethernet Switch"](#)
- ["Hardware Universe"](#)

Tauschen Sie den Schalter aus

Switch- und Node-Terminologie

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Ausgaben für die Befehle können je nach Versionen der ONTAP Software variieren.
- Die zu ersetzenden CN1610-Schalter sind CL1 und CL2.
- Die Nexus 3132Q-V-Switches als Ersatz für die CN1610-Switches sind C1 und C2.
- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die mit Cluster-Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- n1_clus2 ist die erste Cluster-LIF, die mit Cluster Switch 2 (CL2 oder C2) für Node n1 verbunden ist.
- n1_clus3 ist die zweite logische Schnittstelle, die mit Cluster Switch 2 (CL2 oder C2) für Knoten n1 verbunden ist.
- n1_clus4 ist die zweite logische Schnittstelle, die mit Cluster Switch 1 (CL1 oder C1) für Knoten n1 verbunden ist.
- Die Knoten sind n1, n2, n3 und n4.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert ["Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen"](#) Seite.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden vier Knoten:

- Zwei Nodes verwenden vier 10-GbE-Cluster-Interconnect-Ports: e0a, e0b, e0c und e0d.
- Die anderen beiden Knoten verwenden zwei 40/100 GbE Cluster Interconnect Glasfaserkabel: e4a und e4e.

Der ["Hardware Universe"](#) Enthält Informationen zu den Glasfaserkabeln des Clusters auf den Plattformen.

Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Zu Beginn des Clusters sind zwei mit zwei CN1610 Cluster-Switches verbundene Nodes verbunden.

- Cluster-Switch CL2 wird durch C2 ersetzt
 - Der Traffic auf allen Cluster-Ports und LIFs auf allen mit CL2 verbundenen Nodes wird zu den ersten Cluster-Ports migriert und mit CL1 verbundene LIFs.
 - Trennen Sie die Verkabelung von allen Cluster-Ports auf allen mit CL2 verbundenen Nodes, und verwenden Sie anschließend die unterstützten Breakout-Kabel, um die Ports wieder mit dem neuen Cluster-Switch C2 zu verbinden.
 - Trennen Sie die Verkabelung zwischen den ISL-Ports CL1 und CL2, und verwenden Sie dann die unterstützten Breakout-Kabel, um die Ports von CL1 nach C2 wiederherzustellen.
 - Der Datenverkehr auf allen Cluster-Ports und LIFs, die mit C2 verbunden sind, wird auf allen Nodes zurückgesetzt.
- Cluster-Switch CL1 wird durch C1 ersetzt
 - Der Datenverkehr aller Cluster-Ports und LIFs auf allen mit CL1 verbundenen Nodes wird zu den zweiten Cluster-Ports und LIFs migriert, die mit C2 verbunden sind.
 - Trennen Sie die Verkabelung von allen Cluster-Ports auf allen mit CL1 verbundenen Nodes, und verwenden Sie dann die unterstützten Breakout-Kabel, um die Ports wieder mit dem neuen Cluster-Switch C1 zu verbinden.
 - Trennen Sie die Verkabelung zwischen den ISL-Ports CL1 und C2, und verwenden Sie dann die unterstützten Breakout-Kabel, um die Ports von C1 nach C2 wiederherzustellen.
 - Der Datenverkehr auf allen migrierten Cluster-Ports und LIFs, die auf allen Nodes mit C1 verbunden sind, wird zurückgesetzt.



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

Schritt 1: Vorbereitung auf den Austausch

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device-discovery show
```

Beispiel anzeigen

Im folgenden Beispiel wird angezeigt, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster-Interconnect-Switch konfiguriert wurden:

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	CL1	0/1	CN1610
	e0b	CL2	0/1	CN1610
	e0c	CL2	0/2	CN1610
	e0d	CL1	0/2	CN1610
n2	/cdp			
	e0a	CL1	0/3	CN1610
	e0b	CL2	0/3	CN1610
	e0c	CL2	0/4	CN1610
	e0d	CL1	0/4	CN1610

8 entries were displayed.

3. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

a. Zeigt die Attribute des Cluster-Netzwerk-Ports an:

```
network port show
```

Beispiel anzeigen

Im folgenden Beispiel werden die Netzwerkanschlussattribute auf einem System angezeigt:

```
cluster::*> network port show -role Cluster
(network port show)

Node: n1

      Broadcast
Port  IPspace  Domain  Link  MTU  Speed (Mbps)  Health Ignore
Status                               Status Health
-----
-----
e0a   cluster  cluster  up    9000  auto/10000    -      -
e0b   cluster  cluster  up    9000  auto/10000    -      -
e0c   cluster  cluster  up    9000  auto/10000    -      -
e0d   cluster  cluster  up    9000  auto/10000    -      -

Node: n2

      Broadcast
Port  IPspace  Domain  Link  MTU  Speed (Mbps)  Health Ignore
Status                               Status Health
-----
-----
e0a   cluster  cluster  up    9000  auto/10000    -      -
e0b   cluster  cluster  up    9000  auto/10000    -      -
e0c   cluster  cluster  up    9000  auto/10000    -      -
e0d   cluster  cluster  up    9000  auto/10000    -      -

8 entries were displayed.
```

b. Informationen zu den logischen Schnittstellen anzeigen:

```
network interface show
```

Beispiel anzeigen

Im folgenden Beispiel werden die allgemeinen Informationen zu allen LIFs auf Ihrem System angezeigt:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

	Logical	Status	Network	Current	Current
Is	Interface	Admin/Oper	Address/Mask	Node	Port
Vserver					
Home					
-----	-----	-----	-----	-----	-----

Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true					
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true					
	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true					
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true					
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true					
	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true					
	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true					
	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true					

8 entries were displayed.

c. Informationen über die erkannten Cluster-Switches anzeigen:

```
system cluster-switch show
```


Beispiel anzeigen

Im folgenden Beispiel werden die Cluster-Switches, die dem Cluster bekannt sind, mit ihren Management-IP-Adressen angezeigt:

```
cluster::> system cluster-switch show
```

Switch	Type	Address	Model
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	CN1610
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

2 entries were displayed.

4. Stellen Sie die ein `-auto-revert` Parameter to false on Cluster LIFs `clusie1` und `clu4` zu beiden Nodes:

```
network interface modify
```

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto  
-revert false  
cluster::*> network interface modify -vserver node1 -lif clus4 -auto  
-revert false  
cluster::*> network interface modify -vserver node2 -lif clus1 -auto  
-revert false  
cluster::*> network interface modify -vserver node2 -lif clus4 -auto  
-revert false
```

5. Überprüfen Sie, ob die entsprechenden RCF und das entsprechende Image auf den neuen 3132Q-V-Switches installiert sind, wenn dies für Ihre Anforderungen erforderlich ist, und nehmen Sie alle wesentlichen Standortanpassungen vor, z. B. Benutzer und Passwörter, Netzwerkadressen usw.

Sie müssen beide Switches derzeit vorbereiten. Gehen Sie wie folgt vor, wenn Sie ein Upgrade für RCF und Image durchführen müssen:

- a. Siehe "[Cisco Ethernet-Switches](#)" Auf der NetApp Support Site finden.
- b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
- c. Laden Sie die entsprechende Version des RCF herunter.
- d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
- e. Laden Sie die entsprechende Version der Bildsoftware herunter.

["Cisco® Cluster und Management Network Switch Referenzkonfigurationsdatei herunterladen"](#)

6. Migrieren Sie die LIFs, die mit dem zweiten CN1610 Switch verbunden sind, der ersetzt werden soll:

```
network interface migrate
```



Sie müssen die Cluster-LIFs von einer Verbindung zum Node migrieren, entweder über den Service-Prozessor oder die Node-Managementoberfläche, zu der die zu migrierende Cluster-LIF gehört.

Beispiel anzeigen

Das folgende Beispiel zeigt n1 und n2, die LIF-Migration muss jedoch auf allen Knoten durchgeführt werden:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-destination-node n2 -destination-port e0d
```

7. Überprüfen Sie den Systemzustand des Clusters:

```
network interface show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Ergebnis des vorherigen `network interface migrate` Befehl:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	-----
Cluster						
true	n1_clus1	up/up	10.10.0.1/24	n1	e0a	
false	n1_clus2	up/up	10.10.0.2/24	n1	e0a	
false	n1_clus3	up/up	10.10.0.3/24	n1	e0d	
true	n1_clus4	up/up	10.10.0.4/24	n1	e0d	
true	n2_clus1	up/up	10.10.0.5/24	n2	e0a	
false	n2_clus2	up/up	10.10.0.6/24	n2	e0a	
false	n2_clus3	up/up	10.10.0.7/24	n2	e0d	
true	n2_clus4	up/up	10.10.0.8/24	n2	e0d	

8 entries were displayed.

8. Fahren Sie die Cluster-Interconnect-Ports herunter, die physisch mit dem Switch CL2 verbunden sind:

```
network port modify
```

Beispiel anzeigen

Die folgenden Befehle fahren die angegebenen Ports auf n1 und n2 herunter, die Ports müssen jedoch auf allen Knoten heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
```

9. Pingen Sie die Remote-Cluster-Schnittstellen, und führen Sie dann eine Remote-Prozedur Call-Server überprüfen:

```
cluster ping-cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie Sie die Remote-Cluster-Schnittstellen pingen:

```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)

```

10. Fahren Sie die ISL-Ports 13 bis 16 am aktiven CN1610-Switch CL1 herunter:

shutdown

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die ISL-Ports 13 bis 16 am CN1610-Switch CL1 heruntergefahren werden:

```
(CL1)# configure
(CL1)(Config)# interface 0/13-0/16
(CL1)(Interface 0/13-0/16)# shutdown
(CL1)(Interface 0/13-0/16)# exit
(CL1)(Config)# exit
(CL1)#
```

11. Temporäres ISL zwischen CL1 und C2 aufbauen:

Beispiel anzeigen

Im folgenden Beispiel wird eine temporäre ISL zwischen CL1 (Ports 13-16) und C2 (Ports e1/24/1-4) erstellt:

```
C2# configure
C2(config)# interface port-channel 2
C2(config-if)# switchport mode trunk
C2(config-if)# spanning-tree port type network
C2(config-if)# mtu 9216
C2(config-if)# interface breakout module 1 port 24 map 10g-4x
C2(config)# interface e1/24/1-4
C2(config-if-range)# switchport mode trunk
C2(config-if-range)# mtu 9216
C2(config-if-range)# channel-group 2 mode active
C2(config-if-range)# exit
C2(config-if)# exit
```

Schritt 2: Ports konfigurieren

1. Entfernen Sie auf allen Knoten die Kabel, die am CN1610 Switch CL2 angeschlossen sind.

Bei der unterstützten Verkabelung müssen Sie die getrennten Ports auf allen Knoten wieder an den Nexus 3132Q-V Switch C2 anschließen.

2. Entfernen Sie vier ISL-Kabel von den Ports 13 bis 16 am CN1610-Switch CL1.

Sie müssen geeignete Cisco QSFP an SFP+-Breakout-Kabel anschließen, die Port 1/24 am neuen Cisco 3132Q-V Switch C2 an die Ports 13 bis 16 am vorhandenen CN1610-Switch CL1 anschließen.



Beim erneuten Anschließen von Kabeln an den neuen Cisco 3132Q-V Switch müssen Sie entweder eine Glasfaser oder ein Cisco Twinax-Kabel verwenden.

- Um die ISL dynamisch zu machen, konfigurieren Sie die ISL-Schnittstelle 3/1 auf dem aktiven CN1610-Switch, um den statischen Modus zu deaktivieren: `no port-channel static`

Diese Konfiguration entspricht der ISL-Konfiguration auf dem 3132Q-V Switch C2, wenn die ISLs in Schritt 11 an beiden Switches aufgerufen werden

Beispiel anzeigen

Das folgende Beispiel zeigt die Konfiguration der ISL-Schnittstelle 3/1 mit dem `no port-channel static` Befehl für die ISL-Dynamik:

```
(CL1)# configure
(CL1)(Config)# interface 3/1
(CL1)(Interface 3/1)# no port-channel static
(CL1)(Interface 3/1)# exit
(CL1)(Config)# exit
(CL1)#
```

- ISLs 13 bis 16 auf dem aktiven CN1610-Switch CL1 bringen.

Beispiel anzeigen

Das folgende Beispiel veranschaulicht, wie die ISL-Ports 13 bis 16 auf die Port-Channel-Schnittstelle 3/1 gebracht werden:

```
(CL1)# configure
(CL1)(Config)# interface 0/13-0/16,3/1
(CL1)(Interface 0/13-0/16,3/1)# no shutdown
(CL1)(Interface 0/13-0/16,3/1)# exit
(CL1)(Config)# exit
(CL1)#
```

- Überprüfen Sie, ob es sich bei den ISLs um handelt `up` Am CN1610-Schalter CL1:

```
show port-channel
```

Der „Verbindungsstatus“ sollte sein `Up`, "Typ" sollte sein `Dynamic`, Und die Spalte "Port Active" sollte sein `True` Für Ports 0/13 bis 0/16:

Beispiel anzeigen

```
(CL1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Dynamic
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr Ports	Device/ Timeout	Port Speed	Port Active
-----	-----	-----	-----
0/13	actor/long partner/long	10 Gb Full	True
0/14	actor/long partner/long	10 Gb Full	True
0/15	actor/long partner/long	10 Gb Full	True
0/16	actor/long partner/long	10 Gb Full	True

6. Überprüfen Sie, ob es sich bei den ISLs um handelt up Am 3132Q-V Schalter C2:

```
show port-channel summary
```

Beispiel anzeigen

Die Ports eth1/24/1 bis eth1/24/4 sollten angegeben werden (P) , Das bedeutet, dass alle vier ISL-Ports im Port-Channel aktiv sind. Eth1/31 und eth1/32 sollten angegeben werden (D) Da sie nicht verbunden sind:

```
C2# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```
-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)      Eth      LACP      Eth1/31 (D)  Eth1/32 (D)
2      Po2 (SU)      Eth      LACP      Eth1/24/1 (P) Eth1/24/2 (P)
Eth1/24/3 (P)
                                   Eth1/24/4 (P)
```

7. Alle Cluster-Interconnect-Ports, die an allen Knoten mit dem 3132Q-V Switch C2 verbunden sind, werden angezeigt:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Cluster Interconnect Ports, die mit dem 3132Q-V Switch C2 verbunden sind, geöffnet werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
```

8. Zurücksetzen aller migrierten Cluster-Interconnect-LIFs, die auf allen Nodes mit C2 verbunden sind:

```
network interface revert
```

Beispiel anzeigen

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
```

9. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports auf die Home-Ports zurückgesetzt werden:

```
network interface show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die LIFs auf clu2 auf ihre Home-Ports zurückgesetzt werden und zeigt an, dass die LIFs erfolgreich zurückgesetzt werden, wenn die Ports in der Spalte „Current Port“ den Status von aufweisen `true` in der Spalte „is Home“. Wenn der Wert „Home“ lautet `false`, Dann ist das LIF nicht zurückgesetzt.

```
cluster::*> network interface show -role cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
Cluster	n1_clus1	up/up	10.10.0.1/24	n1	e0a	true
	n1_clus2	up/up	10.10.0.2/24	n1	e0b	true
	n1_clus3	up/up	10.10.0.3/24	n1	e0c	true
	n1_clus4	up/up	10.10.0.4/24	n1	e0d	true
	n2_clus1	up/up	10.10.0.5/24	n2	e0a	true
	n2_clus2	up/up	10.10.0.6/24	n2	e0b	true
	n2_clus3	up/up	10.10.0.7/24	n2	e0c	true
	n2_clus4	up/up	10.10.0.8/24	n2	e0d	true

8 entries were displayed.

10. Vergewissern Sie sich, dass alle Cluster-Ports verbunden sind:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Ergebnis des vorherigen `network port modify` Befehl, um sicherzustellen, dass alle Cluster Interconnects vorhanden sind up:

```
cluster::*> network port show -role Cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain                               Admin/Open  Status  Health
-----  -----  -
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Domain                               Admin/Open  Status  Health
-----  -----  -
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

8 entries were displayed.
```

11. Pingen Sie die Remote-Cluster-Schnittstellen und führen Sie dann eine Remote-Prozedur aus Rufen Sie den Server an:

```
cluster ping-cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie Sie die Remote-Cluster-Schnittstellen pingen:

```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a    10.10.0.1
Cluster n1_clus2 n1      e0b    10.10.0.2
Cluster n1_clus3 n1      e0c    10.10.0.3
Cluster n1_clus4 n1      e0d    10.10.0.4
Cluster n2_clus1 n2      e0a    10.10.0.5
Cluster n2_clus2 n2      e0b    10.10.0.6
Cluster n2_clus3 n2      e0c    10.10.0.7
Cluster n2_clus4 n2      e0d    10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
    Local 10.10.0.3 to Remote 10.10.0.7
    Local 10.10.0.3 to Remote 10.10.0.8
    Local 10.10.0.4 to Remote 10.10.0.5
    Local 10.10.0.4 to Remote 10.10.0.6
    Local 10.10.0.4 to Remote 10.10.0.7
    Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)

```

12. Migrieren Sie bei jedem Node im Cluster die Schnittstellen, die dem ersten CN1610 Switch CL1

zugeordnet sind, der ersetzt werden soll:

```
network interface migrate
```

Beispiel anzeigen

Im folgenden Beispiel werden die Ports oder LIFs angezeigt, die auf den Nodes n1 und n2 migriert werden:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1  
-destination-node n1 -destination-port e0b  
cluster::*> network interface migrate -vserver Cluster -lif n1_clus4  
-destination-node n1 -destination-port e0c  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1  
-destination-node n2 -destination-port e0b  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus4  
-destination-node n2 -destination-port e0c
```

13. Überprüfen Sie den Cluster-Status:

```
network interface show
```


Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, dass die erforderlichen Cluster-LIFs zu den entsprechenden Cluster-Ports migriert wurden, die auf Cluster-Switch gehostet werden.C2:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	-----
Cluster						
false	n1_clus1	up/up	10.10.0.1/24	n1	e0b	
true	n1_clus2	up/up	10.10.0.2/24	n1	e0b	
true	n1_clus3	up/up	10.10.0.3/24	n1	e0c	
false	n1_clus4	up/up	10.10.0.4/24	n1	e0c	
false	n2_clus1	up/up	10.10.0.5/24	n2	e0b	
true	n2_clus2	up/up	10.10.0.6/24	n2	e0b	
true	n2_clus3	up/up	10.10.0.7/24	n2	e0c	
false	n2_clus4	up/up	10.10.0.8/24	n2	e0c	

8 entries were displayed.

14. Fahren Sie die Node-Ports, die auf allen Nodes mit CL1 verbunden sind, herunter:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die angegebenen Ports an den Knoten n1 und n2 heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0a -up-admin false
cluster::*> network port modify -node n1 -port e0d -up-admin false
cluster::*> network port modify -node n2 -port e0a -up-admin false
cluster::*> network port modify -node n2 -port e0d -up-admin false
```

15. Fahren Sie die ISL-Ports 24, 31 und 32 am aktiven Switch 3132Q-V C2 herunter.

shutdown

Beispiel anzeigen

Das folgende Beispiel zeigt, wie ISLs 24, 31 und 32 auf dem aktiven Switch 3132Q-V C2 heruntergefahren werden:

```
C2# configure
C2(config)# interface ethernet 1/24/1-4
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
C2#
```

16. Entfernen Sie die Kabel, die an allen Knoten am CN1610-Switch CL1 angeschlossen sind.

Bei der unterstützten Verkabelung müssen Sie die getrennten Ports auf allen Knoten wieder an den Nexus 3132Q-V Switch C1 anschließen.

17. Entfernen Sie die QSFP-Kabel vom Nexus 3132Q-V C2-Port e1/24.

Sie müssen die Ports e1/31 und e1/32 auf C1 mit den Ports e1/31 und e1/32 auf C2 verbinden, die von unterstützten Cisco QSFP-Glasfaserkabeln oder Direct-Attach-Kabeln verwendet werden.

18. Stellen Sie die Konfiguration an Port 24 wieder her, und entfernen Sie den temporären Port-Kanal 2 auf C2, indem Sie den kopieren `running-configuration` Datei in der `startup-configuration` Datei:

Beispiel anzeigen

Im folgenden Beispiel wird das kopiert running-configuration Datei in der startup-configuration Datei:

```
C2# configure
C2(config)# no interface breakout module 1 port 24 map 10g-4x
C2(config)# no interface port-channel 2
C2(config-if)# interface e1/24
C2(config-if)# description 40GbE Node Port
C2(config-if)# spanning-tree port type edge
C2(config-if)# spanning-tree bpduguard enable
C2(config-if)# mtu 9216
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.
```

19. ISL-Ports 31 und 32 auf C2, dem aktiven 3132Q-V Switch:

```
no shutdown
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie ISLs 31 und 32 auf dem 3132Q-V Switch C2:

```
C2# configure
C2(config)# interface ethernet 1/31-32
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
C2# copy running-config startup-config
[#####] 100%
Copy Complete.
```

Schritt 3: Überprüfen Sie die Konfiguration

1. Stellen Sie sicher, dass die ISL-Verbindungen sind up Am 3132Q-V Schalter C2:

```
show port-channel summary
```

Die Ports eth1/31 und eth1/32 sollten angegeben werden (P), Was bedeutet, dass beide ISL-Ports sind up Im Port-Kanal.

Beispiel anzeigen

```
C1# 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
        S - Switched      R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth      LACP      Eth1/31 (P)  Eth1/32 (P)
```

2. Alle Cluster-Interconnect-Ports, die an den neuen 3132Q-V Switch C1 angeschlossen sind, können auf allen Knoten angezeigt werden:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie alle Cluster Interconnect Ports, die mit dem neuen Switch C1 3132Q-V verbunden sind, verbunden sind:

```
cluster::*> network port modify -node n1 -port e0a -up-admin true
cluster::*> network port modify -node n1 -port e0d -up-admin true
cluster::*> network port modify -node n2 -port e0a -up-admin true
cluster::*> network port modify -node n2 -port e0d -up-admin true
```

3. Überprüfen Sie den Status des Cluster-Node-Ports:

```
network port show
```

Beispiel anzeigen

Im folgenden Beispiel wird überprüft, ob alle Cluster-Interconnect-Ports an n1 und n2 auf dem neuen 3132Q-V-Switch C1 sind up:

```
cluster::*> network port show -role Cluster
(network port show)

Node: n1

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Admin/Open  Status  Health
-----
-----
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

Node: n2

Port  IPspace  Broadcast  Link  MTU  Speed (Mbps)  Health  Ignore
Status  Admin/Open  Status  Health
-----
-----
e0a    cluster  cluster    up    9000  auto/10000    -       -
e0b    cluster  cluster    up    9000  auto/10000    -       -
e0c    cluster  cluster    up    9000  auto/10000    -       -
e0d    cluster  cluster    up    9000  auto/10000    -       -

8 entries were displayed.
```

4. Zurücksetzen aller migrierten Cluster-Interconnect-LIFs, die ursprünglich auf allen Knoten mit C1 verbunden waren:

```
network interface revert
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie die migrierten Cluster-LIFs auf die Home-Ports zurückgesetzt werden:

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n1_clus4
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus4
```

5. Vergewissern Sie sich, dass die Schnittstelle jetzt die Startseite ist:

```
network interface show
```

Beispiel anzeigen

Im folgenden Beispiel wird der Status von Cluster-Interconnect-Schnittstellen angezeigt up Und Is home Für n1 und n2:

```
cluster::*> network interface show -role Cluster
(network interface show)
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is
Home						
-----	-----	-----	-----	-----	-----	-----
Cluster						
true	n1_clus1	up/up	10.10.0.1/24	n1	e0a	
true	n1_clus2	up/up	10.10.0.2/24	n1	e0b	
true	n1_clus3	up/up	10.10.0.3/24	n1	e0c	
true	n1_clus4	up/up	10.10.0.4/24	n1	e0d	
true	n2_clus1	up/up	10.10.0.5/24	n2	e0a	
true	n2_clus2	up/up	10.10.0.6/24	n2	e0b	
true	n2_clus3	up/up	10.10.0.7/24	n2	e0c	
true	n2_clus4	up/up	10.10.0.8/24	n2	e0d	

8 entries were displayed.

6. Pingen Sie die Remote-Cluster-Schnittstellen und führen Sie dann eine Remote-Prozedur aus Rufen Sie den Server an:

```
cluster ping-cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird gezeigt, wie Sie die Remote-Cluster-Schnittstellen pingen:


```

cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a      10.10.0.1
Cluster n1_clus2 n1      e0b      10.10.0.2
Cluster n1_clus3 n1      e0c      10.10.0.3
Cluster n1_clus4 n1      e0d      10.10.0.4
Cluster n2_clus1 n2      e0a      10.10.0.5
Cluster n2_clus2 n2      e0b      10.10.0.6
Cluster n2_clus3 n2      e0c      10.10.0.7
Cluster n2_clus4 n2      e0d      10.10.0.8

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 16 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 16 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
  Local 10.10.0.3 to Remote 10.10.0.7
  Local 10.10.0.3 to Remote 10.10.0.8
  Local 10.10.0.4 to Remote 10.10.0.5
  Local 10.10.0.4 to Remote 10.10.0.6
  Local 10.10.0.4 to Remote 10.10.0.7
  Local 10.10.0.4 to Remote 10.10.0.8

Larger than PMTU communication succeeds on 16 path(s)
RPC status:
4 paths up, 0 paths down (tcp check)
4 paths up, 0 paths down (udp check)

```

7. Erweitern Sie das Cluster durch Hinzufügen von Nodes zu den Nexus 3132Q-V Cluster Switches.

8. Zeigen Sie die Informationen zu den Geräten in Ihrer Konfiguration an:

- ° `network device-discovery show`
- ° `network port show -role cluster`
- ° `network interface show -role cluster`
- ° `system cluster-switch show`

Beispiel anzeigen

Die folgenden Beispiele zeigen die Nodes n3 und n4 mit 40-GbE-Cluster-Ports, die mit den Ports e1/7 und e1/8 verbunden sind, bzw. auf den Nexus 3132Q-V Cluster-Switches, und beide Nodes haben sich dem Cluster angeschlossen. Die 40 GbE Cluster Interconnect Ports sind e4a und e4e.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
n3	/cdp			
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

12 entries were displayed.

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1		Broadcast		Speed (Mbps)		Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						

e0a	cluster	cluster	up	9000	auto/10000	-	-
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n2

		Broadcast			Speed (Mbps)	Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						
-----	-----	-----	-----	-----	-----	-----	-----
-----	-----						
e0a	cluster	cluster	up	9000	auto/10000	-	-
e0b	cluster	cluster	up	9000	auto/10000	-	-
e0c	cluster	cluster	up	9000	auto/10000	-	-
e0d	cluster	cluster	up	9000	auto/10000	-	-

Node: n3

		Broadcast			Speed (Mbps)	Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						
-----	-----	-----	-----	-----	-----	-----	

e4a	cluster	cluster	up	9000	auto/40000	-	-
e4e	cluster	cluster	up	9000	auto/40000	-	-

Node: n4

		Broadcast			Speed (Mbps)	Health	
Ignore							
Port	IPspace	Domain	Link	MTU	Admin/Open	Status	
Health	Status						
-----	-----	-----	-----	-----	-----	-----	-----

e4a	cluster	cluster	up	9000	auto/40000	-	-
e4e	cluster	cluster	up	9000	auto/40000	-	-

12 entries were displayed.

```
cluster::*> network interface show -role Cluster
(network interface show)
```

Is	Logical	Status	Network	Current	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----

Cluster					
	n1_clus1	up/up	10.10.0.1/24	n1	e0a
true					
	n1_clus2	up/up	10.10.0.2/24	n1	e0b
true					
	n1_clus3	up/up	10.10.0.3/24	n1	e0c
true					
	n1_clus4	up/up	10.10.0.4/24	n1	e0d
true					
	n2_clus1	up/up	10.10.0.5/24	n2	e0a
true					
	n2_clus2	up/up	10.10.0.6/24	n2	e0b
true					
	n2_clus3	up/up	10.10.0.7/24	n2	e0c
true					
	n2_clus4	up/up	10.10.0.8/24	n2	e0d
true					
	n3_clus1	up/up	10.10.0.9/24	n3	e4a
true					
	n3_clus2	up/up	10.10.0.10/24	n3	e4e
true					
	n4_clus1	up/up	10.10.0.11/24	n4	e4a
true					
	n4_clus2	up/up	10.10.0.12/24	n4	e4e
true					

```
12 entries were displayed.
```

```
cluster::> system cluster-switch show
```

Switch	Type	Address	Model

C1	cluster-network	10.10.1.103	
NX3132V			
Serial Number: FOX000001			
Is Monitored: true			
Reason:			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
7.0(3)I4(1)			
Version Source: CDP			
C2	cluster-network	10.10.1.104	
NX3132V			
Serial Number: FOX000002			
Is Monitored: true			
Reason:			
Software Version: Cisco Nexus Operating System (NX-OS)			
Software, Version			
7.0(3)I4(1)			
Version Source: CDP			
CL1	cluster-network	10.10.1.101	CN1610
Serial Number: 01234567			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			
CL2	cluster-network	10.10.1.102	
CN1610			
Serial Number: 01234568			
Is Monitored: true			
Reason:			
Software Version: 1.2.0.7			
Version Source: ISDP			

4 entries were displayed.

9. Entfernen Sie die ausgetauschten CN1610-Schalter, wenn sie nicht automatisch entfernt werden:

```
system cluster-switch delete
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die CN1610-Switches entfernt werden:

```
cluster::> system cluster-switch delete -device CL1  
cluster::> system cluster-switch delete -device CL2
```

10. Konfigurieren Sie Cluster clue1 und clus4 to `-auto-revert` Auf jedem Knoten und bestätigen:

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto  
-revert true  
cluster::*> network interface modify -vserver node1 -lif clus4 -auto  
-revert true  
cluster::*> network interface modify -vserver node2 -lif clus1 -auto  
-revert true  
cluster::*> network interface modify -vserver node2 -lif clus4 -auto  
-revert true
```

11. Überprüfen Sie, ob die richtigen Cluster-Switches überwacht werden:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address

C1 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.104
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

12. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```


Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

13. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie sie erneut, indem Sie eine AutoSupport-Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Migrieren Sie von einem Cluster ohne Switch auf ein Cluster mit zwei Nodes

Wenn Sie über einen 2-Node-Cluster ohne Switches verfügen, können Sie dieses Verfahren durchführen, um zu einem Switch-basierten Cluster mit zwei Nodes zu migrieren, der Cisco Nexus 3132Q-V Cluster-Netzwerk-Switches umfasst. Beim Austausch handelt es sich um einen unterbrechungsfreien Vorgang (Non-Disruptive Procedure, NDO).

Prüfen Sie die Anforderungen

Ports und Node-Verbindungen

Wenn Sie zu einem Switch mit zwei Nodes und Cisco Nexus 3132Q-V Cluster Switches migrieren, sollten Sie die Verbindungen zu Ports und Nodes und die Verkabelungsanforderungen verstehen.

- Die Cluster-Switches verwenden die Inter-Switch-Link-Ports (ISL) e1/31-32.
- Der "[Hardware Universe](#)" Enthält Informationen über die unterstützten Kabel zu Nexus 3132Q-V Switches:
 - Die Nodes mit 10 GbE-Cluster-Verbindungen erfordern optische QSFP-Module mit Breakout-Glasfaserkabeln oder QSFP zu SFP+ Kupfer Breakout-Kabel.
 - Die Nodes mit 40/100 GbE-Cluster-Verbindungen erfordern unterstützte QSFP/QSFP28 optische Module mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direct-Attach-Kabeln.
 - Die Cluster-Switches verwenden die entsprechenden ISL-Kabel: 2 QSFP28-Glasfaser- oder Kupfer-Direct-Attach-Kabel.
- Bei Nexus 3132Q-V können Sie QSFP-Ports entweder als 40/100-GB-Ethernet- oder als 4 x 10-GB-Ethernet-Modus betreiben.

Standardmäßig befinden sich im 40/100-GB-Ethernet-Modus 32 Ports. Diese 40-GB-Ethernet-Ports werden in einer 2-tupel-Namenskonvention nummeriert. Beispielsweise wird der zweite 40-GB-Ethernet-Port mit der Nummer 1/2 nummeriert. Der Prozess der Änderung der Konfiguration von 40 GB Ethernet zu 10 GB Ethernet wird *Breakout* genannt und der Prozess der Änderung der Konfiguration von 10 GB Ethernet zu 40 GB Ethernet wird *break* genannt. Wenn Sie einen 40/100-GB-Ethernet-Port in 10-GB-Ethernet-Ports umwandeln, werden die resultierenden Ports mit einer 3-tupel-Namenskonvention nummeriert. Die Breakout-Ports des zweiten 40/100-GB-Ethernet-Ports werden beispielsweise als 1/2/1, 1/2/2/2/3, 1/2/4 nummeriert.

- Auf der linken Seite von Nexus 3132Q-V befindet sich ein Satz von vier SFP+ Ports, die auf den ersten QSFP-Port multipliziert werden.

Standardmäßig ist der RCF so strukturiert, dass der erste QSFP-Port verwendet wird.

Mit dem können Sie vier SFP+-Ports anstelle eines QSFP-Ports für Nexus 3132Q-V aktivieren `hardware profile front portmode sfp-plus` Befehl. Auf ähnliche Weise können Sie Nexus 3132Q-V zurücksetzen, um einen QSFP-Port anstelle von vier SFP+-Ports mit dem zu verwenden `hardware profile front portmode qsfp` Befehl.

- Stellen Sie sicher, dass Sie einige der Ports auf Nexus 3132Q-V für 10 GbE oder 40/100 GbE konfiguriert haben.

Sie können die ersten sechs Ports mit dem in den 4x10 GbE-Modus eingliedern `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Auf ähnliche Weise können Sie die ersten sechs QSFP+-Ports aus Breakout-Konfiguration mit dem neu gruppieren `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert ["Referenzkonfigurationsdatei Für Cisco® Cluster-Switch Herunterladen"](#) Seite.

Was Sie benötigen

- Konfiguration ordnungsgemäß eingerichtet und funktionsfähig.
- Nodes mit ONTAP 9.4 oder höher.
- Alle Cluster-Ports in `up` Bundesland.
- Der Cisco Nexus 3132Q-V Cluster-Switch wird unterstützt.
- Die vorhandene Cluster-Netzwerkconfiguration verfügt über:
 - Die Nexus 3132 Cluster-Infrastruktur ist redundant und auf beiden Switches voll funktionsfähig.
 - Die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.

Der ["Cisco Ethernet-Switches"](#) Die Seite enthält Informationen zu den in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen.

- Management-Konnektivität auf beiden Switches.
- Konsolenzugriff auf beide Switches.
- Alle logischen Cluster-Schnittstellen (LIFs) im `up` Zustand ohne Migration.
- Erstanpassung des Schalters.
- Alle ISL-Ports sind aktiviert und verkabelt.

Darüber hinaus müssen die erforderlichen Dokumentationen für 10-/25-GbE- und 40/100-GbE-Konnektivität von den Nodes auf Nexus 3132Q-V Cluster Switches geplant, migriert und gelesen werden.

Migrieren Sie die Switches

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Nexus 3132Q-V Cluster Switches, C1 und C2.
- Die Knoten sind n1 und n2.



Die Beispiele in diesem Verfahren verwenden zwei Knoten, von denen jeder zwei 40/100 GbE Cluster Interconnect Ports e4a und e4e nutzt. Der ["Hardware Universe"](#) Enthält Details zu den Cluster-Ports auf Ihren Plattformen.

Über diese Aufgabe

Dieses Verfahren umfasst folgende Szenarien:

- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die für Knoten n1 mit Cluster-Switch C1 verbunden werden soll.
- n1_clus2 ist die erste Cluster-LIF, die für Node n1 mit Cluster-Switch C2 verbunden wird.
- n2_clus1 ist die erste Cluster-LIF, die für Knoten n2 mit Cluster-Switch C1 verbunden wird.
- n2_clus2 ist die zweite Cluster-LIF, die für Knoten n2 an Cluster-Switch C2 angeschlossen werden soll.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren

Referenzkonfigurationsdateien (RCFs) definiert ["Referenzkonfigurationsdatei Für Cisco® Cluster-Switch Herunterladen"](#) Seite.



Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 3000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben.

- Das Cluster beginnt mit zwei verbundenen Nodes und funktioniert in einer zwei-Node-Cluster-Einstellung ohne Switches.
- Der erste Cluster Port ist nach C1 verschoben.
- Der zweite Cluster-Port wird auf C2 verschoben.
- Die Option für einen Cluster mit zwei Nodes ohne Switches ist deaktiviert.

Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Legen Sie den Administrations- oder Betriebsstatus für jede Cluster-Schnittstelle fest:
 - a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
-
e4e         Cluster      Cluster      up    9000 auto/40000 -
-

Node: n2

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
-----
e4a         Cluster      Cluster      up    9000 auto/40000 -
-
e4e         Cluster      Cluster      up    9000 auto/40000 -
-

4 entries were displayed.
```

b. Informationen zu den logischen Schnittstellen anzeigen:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e4a          n1_clus1    up/up      10.10.0.1/24      n1
true
e4e          n1_clus2    up/up      10.10.0.2/24      n1
true
e4a          n2_clus1    up/up      10.10.0.3/24      n2
true
e4e          n2_clus2    up/up      10.10.0.4/24      n2
true
4 entries were displayed.
```

3. Vergewissern Sie sich, dass die entsprechenden RCF- und Image-Einstellungen auf den neuen 3132Q-V-Switches installiert sind, wenn dies für Ihre Anforderungen erforderlich ist, und nehmen Sie alle wesentlichen Standortanpassungen vor, z. B. Benutzer und Passwörter, Netzwerkadressen usw.

Sie müssen beide Switches derzeit vorbereiten. Wenn Sie die RCF- und Bildsoftware aktualisieren müssen, müssen Sie folgende Schritte ausführen:

- Wechseln Sie zum "[Cisco Ethernet-Switches](#)" Auf der NetApp Support Site finden.
 - Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
 - Laden Sie die entsprechende RCF-Version herunter.
 - Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
 - Laden Sie die entsprechende Version der Bildsoftware herunter.
4. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.

Schritt 2: Verschieben Sie den ersten Cluster-Port nach C1

- Bei Nexus 3132Q-V Switches C1 und C2 sollten Sie alle an Nodes ausgerichteten Ports C1 und C2 deaktivieren, aber die ISL-Ports nicht deaktivieren.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1 bis 30 bei den Nexus 3132Q-V Cluster Switches C1 und C2 deaktiviert sind und eine in RCF unterstützte Konfiguration verwenden

NX3132_RCF_v1.1_24p10g_26p40g.txt:

```
C1# copy running-config startup-config
[#####] 100%
Copy complete.
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C1(config-if-range)# shutdown
C1(config-if-range)# exit
C1(config)# exit

C2# copy running-config startup-config
[#####] 100%
Copy complete.
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-
4,e1/7-30
C2(config-if-range)# shutdown
C2(config-if-range)# exit
C2(config)# exit
```

2. Verbinden Sie die Ports 1/31 und 1/32 auf C1 mit den gleichen Ports auf C2, indem Sie die unterstützten Kabel verwenden.
3. Überprüfen Sie, ob die ISL-Ports auf C1 und C2 funktionsfähig sind:

```
show port-channel summary
```

Beispiel anzeigen

```
C1# 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
      S - Switched        R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1(SU)        Eth     LACP      Eth1/31(P)  Eth1/32(P)

C2# 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
      S - Switched        R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1(SU)        Eth     LACP      Eth1/31(P)  Eth1/32(P)
```

4. Anzeigen der Liste der benachbarten Geräte auf dem Switch:

```
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
C2                  Eth1/31        174      R S I s         N3K-C3132Q-V
Eth1/31
C2                  Eth1/32        174      R S I s         N3K-C3132Q-V
Eth1/32

Total entries displayed: 2

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
C1                  Eth1/31        178      R S I s         N3K-C3132Q-V
Eth1/31
C1                  Eth1/32        178      R S I s         N3K-C3132Q-V
Eth1/32

Total entries displayed: 2
```

5. Zeigen Sie die Cluster-Port-Konnektivität auf jedem Node an:

```
network device-discovery show
```

Beispiel anzeigen

Das folgende Beispiel zeigt eine Konfiguration eines Clusters mit zwei Nodes ohne Switches.

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e4a	n2	e4a	FAS9000
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	n1	e4a	FAS9000
	e4e	n1	e4e	FAS9000

6. Migrieren Sie die Faclu1-Schnittstelle in den physischen Port, der hostet, Fa.2:

```
network interface migrate
```

Führen Sie diesen Befehl von jedem lokalen Knoten aus.

Beispiel anzeigen

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus1  
-source-node n1  
-destination-node n1 -destination-port e4e  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus1  
-source-node n2  
-destination-node n2 -destination-port e4e
```

7. Überprüfen Sie, ob die Migration der Cluster-Schnittstellen durchgeführt wird:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4e      false
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4e      false
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

8. Fahren Sie Cluster-Ports herunter und schließen Sie LIF auf beiden Knoten an:

```
network port modify
```

```
cluster::*> network port modify -node n1 -port e4a -up-admin false
cluster::*> network port modify -node n2 -port e4a -up-admin false
```

9. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster
```

Beispiel anzeigen

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e4a 10.10.0.1
Cluster n1_clus2 n1      e4e 10.10.0.2
Cluster n2_clus1 n2      e4a 10.10.0.3
Cluster n2_clus2 n2      e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

10. Trennen Sie das Kabel von e4a am Knoten n1.

Sie können sich auf die laufende Konfiguration beziehen und den ersten 40-GbE-Port am Switch C1 (Port 1/7 in diesem Beispiel) mit e4a auf n1 verbinden, indem Sie die unterstützte Verkabelung auf Nexus 3132Q-V. verwenden



Beim erneuten Anschließen von Kabeln an einen neuen Cisco Cluster Switch müssen die verwendeten Kabel entweder Glasfaser oder Verkabelung sein, die von Cisco unterstützt wird.

11. Trennen Sie das Kabel von e4a auf Knoten n2.

Sie können sich auf die laufende Konfiguration beziehen und e4a mit dem nächsten verfügbaren 40 GbE-Port von C1, Port 1/8, über unterstützte Verkabelung verbinden.

12. Aktivieren Sie alle Ports, die an Knoten gerichtet sind, auf C1.

Beispiel anzeigen

Das folgende Beispiel zeigt die Ports 1 bis 30, die bei Nexus 3132Q-V Cluster Switches C1 und C2 aktiviert sind und die in RCF unterstützt werden NX3132_RCF_v1.1_24p10g_26p40g.txt:

```
C1# configure
C1(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C1(config-if-range)# no shutdown
C1(config-if-range)# exit
C1(config)# exit
```

13. Aktivieren Sie den ersten Cluster-Port e4a auf jedem Knoten:

```
network port modify
```

Beispiel anzeigen

```
cluster::*> network port modify -node n1 -port e4a -up-admin true
cluster::*> network port modify -node n2 -port e4a -up-admin true
```

14. Vergewissern Sie sich, dass die Cluster auf beiden Nodes aktiv sind:

```
network port show
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

4 entries were displayed.
```

15. Setzen Sie für jeden Node alle migrierten Cluster Interconnect LIFs zurück:

```
network interface revert
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die migrierten LIFs auf die Home-Ports zurückgesetzt werden.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus1
cluster::*> network interface revert -vserver Cluster -lif n2_clus1
```

16. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports jetzt auf die Home-Ports zurückgesetzt werden:

```
network interface show
```

Der Is Home Spalte sollte einen Wert von `true` Für alle im aufgeführten Ports Current Port Spalte. Wenn der angezeigte Wert lautet `false`, Der Hafen wurde nicht zurückgesetzt.

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
Current Is Logical Status Network Current
Vserver Interface Admin/Oper Address/Mask Node
Port Home
-----
Cluster
e4a n1_clus1 up/up 10.10.0.1/24 n1
true n1_clus2 up/up 10.10.0.2/24 n1
e4e true n2_clus1 up/up 10.10.0.3/24 n2
e4a true n2_clus2 up/up 10.10.0.4/24 n2
e4e true
4 entries were displayed.
```

Schritt 3: Zweiten Cluster-Port auf C2 verschieben

1. Zeigen Sie die Cluster-Port-Konnektivität auf jedem Node an:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster::*> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform

n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	n2	e4e	FAS9000
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	n1	e4e	FAS9000

2. Migrieren Sie auf der Konsole jedes Knotens cluden2 zu Port e4a:

```
network interface migrate
```

Beispiel anzeigen

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2  
-source-node n1  
-destination-node n1 -destination-port e4a  
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2  
-source-node n2  
-destination-node n2 -destination-port e4a
```

3. Herunterfahren von Cluster-Ports clu2 LIF auf beiden Knoten:

```
network port modify
```

Im folgenden Beispiel werden die angegebenen Ports angezeigt, die auf beiden Nodes heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e4e -up-admin false  
cluster::*> network port modify -node n2 -port e4e -up-admin false
```

4. Überprüfen Sie den LIF-Status des Clusters:

```
network interface show
```


Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4a      false
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4a      false
4 entries were displayed.
```

5. Trennen Sie das Kabel von e4e am Knoten n1.

Sie können sich auf die laufende Konfiguration beziehen und den ersten 40-GbE-Port am Switch C2 (Port 1/7 in diesem Beispiel) mit e4e auf n1 verbinden, indem Sie die unterstützte Verkabelung auf Nexus 3132Q-V. verwenden

6. Trennen Sie das Kabel von e4e am Knoten n2.

Sie können sich auf die laufende Konfiguration beziehen und e4e mithilfe der unterstützten Verkabelung an den nächsten verfügbaren 40-GbE-Port auf C2, Port 1/8 anschließen.

7. Aktivieren Sie alle Anschlüsse für Knoten auf C2.

Beispiel anzeigen

Das folgende Beispiel zeigt die Ports 1 bis 30, die bei Nexus 3132Q-V Cluster Switches C1 und C2 aktiviert sind und eine in RCF unterstützte Konfiguration verwenden

NX3132_RCF_v1.1_24p10g_26p40g.txt:

```
C2# configure
C2(config)# int e1/1/1-4,e1/2/1-4,e1/3/1-4,e1/4/1-4,e1/5/1-4,e1/6/1-4,e1/7-30
C2(config-if-range)# no shutdown
C2(config-if-range)# exit
C2(config)# exit
```

8. Aktivieren Sie den zweiten Cluster-Port e4e auf jedem Node:

```
network port modify
```

Im folgenden Beispiel werden die angegebenen Ports angezeigt:

```
cluster::*> network port modify -node n1 -port e4e -up-admin true
cluster::*> network port modify -node n2 -port e4e -up-admin true
```

9. Setzen Sie für jeden Node alle migrierten Cluster Interconnect LIFs zurück:

```
network interface revert
```

Das folgende Beispiel zeigt, dass die migrierten LIFs auf die Home-Ports zurückgesetzt werden.

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

10. Vergewissern Sie sich, dass alle Cluster-Interconnect-Ports jetzt auf die Home-Ports zurückgesetzt werden:

```
network interface show
```

Der Is Home Spalte sollte einen Wert von anzeigen true Für alle im aufgeführten Ports Current Port Spalte. Wenn der angezeigte Wert lautet false, Der Hafen wurde nicht zurückgesetzt.

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
      n1_clus1      up/up      10.10.0.1/24      n1
e4a      true
      n1_clus2      up/up      10.10.0.2/24      n1
e4e      true
      n2_clus1      up/up      10.10.0.3/24      n2
e4a      true
      n2_clus2      up/up      10.10.0.4/24      n2
e4e      true
4 entries were displayed.
```

11. Vergewissern Sie sich, dass sich alle Cluster-Interconnect-Ports im befinden up Bundesland.

```
network port show -role cluster
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
Node: n1

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

Node: n2

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000  -
-
e4e      Cluster      Cluster      up    9000 auto/40000  -
-

4 entries were displayed.
```

Schritt 4: Deaktivieren Sie die 2-Node-Cluster-Option ohne Switches

1. Zeigen Sie die Port-Nummern des Cluster-Switches an, mit denen jeder Cluster-Port auf jedem Node verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster::*> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform

n1	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n2	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

2. Anzeige ermittelte und überwachte Cluster-Switches:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
C1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

3. Deaktivieren Sie die Konfigurationseinstellungen mit zwei Nodes ohne Switches auf jedem Node:

```
network options switchless-cluster
```

```
network options switchless-cluster modify -enabled false
```

4. Überprüfen Sie das switchless-cluster Die Option wurde deaktiviert.

```
network options switchless-cluster show
```

Schritt 5: Überprüfen Sie die Konfiguration

1. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster
```

Beispiel anzeigen

```
cluster::*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e4a 10.10.0.1
Cluster n1_clus2 n1      e4e 10.10.0.2
Cluster n2_clus1 n2      e4a 10.10.0.3
Cluster n2_clus2 n2      e4e 10.10.0.4

Local = 10.10.0.1 10.10.0.2
Remote = 10.10.0.3 10.10.0.4
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.3
    Local 10.10.0.1 to Remote 10.10.0.4
    Local 10.10.0.2 to Remote 10.10.0.3
    Local 10.10.0.2 to Remote 10.10.0.4
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
1 paths up, 0 paths down (tcp check)
1 paths up, 0 paths down (ucp check)
```

2. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> **system cluster-switch log setup-password**
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

3. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```


Tauschen Sie die Schalter aus

Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster Switches

Stellen Sie sicher, dass Sie die Konfigurationsanforderungen, Port-Verbindungen und Verkabelungsanforderungen kennen, wenn Sie Cluster Switches ersetzen.

Anforderungen für Cisco Nexus 3132Q-V

- Der Cisco Nexus 3132Q-V Cluster-Switch wird unterstützt.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert "[Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen](#)" Seite.
- Die Cluster-Switches verwenden die Inter-Switch-Link-Ports (ISL) e1/31-32.
- Der "[Hardware Universe](#)" Enthält Informationen über die unterstützten Kabel zu Nexus 3132Q-V Switches:
 - Die Nodes mit 10 GbE-Cluster-Verbindungen erfordern optische QSFP-Module mit Breakout-Glasfaserkabeln oder QSFP zu SFP+ Kupfer Breakout-Kabel.
 - Die Nodes mit 40/100 GbE-Cluster-Verbindungen erfordern unterstützte QSFP/QSFP28 optische Module mit Glasfaserkabeln oder QSFP/QSFP28-Kupfer-Direct-Attach-Kabeln.
 - Die Cluster-Switches verwenden die entsprechenden ISL-Kabel: 2 QSFP28-Glasfaser- oder Kupfer-Direct-Attach-Kabel.
- Bei Nexus 3132Q-V können Sie QSFP-Ports entweder als 40/100-GB-Ethernet- oder als 4 x 10-GB-Ethernet-Modus betreiben.

Standardmäßig befinden sich im 40/100-GB-Ethernet-Modus 32 Ports. Diese 40-GB-Ethernet-Ports werden in einer 2-tupel-Namenskonvention nummeriert. Beispielsweise wird der zweite 40-GB-Ethernet-Port mit der Nummer 1/2 nummeriert. Der Prozess der Änderung der Konfiguration von 40 GB Ethernet zu 10 GB Ethernet wird *Breakout* genannt und der Prozess der Änderung der Konfiguration von 10 GB Ethernet zu 40 GB Ethernet wird *break* genannt. Wenn Sie einen 40/100-GB-Ethernet-Port in 10-GB-Ethernet-Ports umwandeln, werden die resultierenden Ports mit einer 3-tupel-Namenskonvention nummeriert. Die Breakout-Ports des zweiten 40/100-GB-Ethernet-Ports werden beispielsweise als 1/2/1, 1/2/2/2/3, 1/2/4 nummeriert.

- Auf der linken Seite von Nexus 3132Q-V befindet sich ein Satz von vier SFP+ Ports, die auf den ersten QSFP-Port multipliziert werden.

Standardmäßig ist der RCF so strukturiert, dass der erste QSFP-Port verwendet wird.

Mit dem können Sie vier SFP+-Ports anstelle eines QSFP-Ports für Nexus 3132Q-V aktivieren `hardware profile front portmode sfp-plus` Befehl. Auf ähnliche Weise können Sie Nexus 3132Q-V zurücksetzen, um einen QSFP-Port anstelle von vier SFP+-Ports mit dem zu verwenden `hardware profile front portmode qsfp` Befehl.

- Sie müssen einige der Ports auf Nexus 3132Q-V für 10 GbE oder 40/100 GbE konfiguriert haben.

Sie können die ersten sechs Ports mit dem in den 4x10 GbE-Modus eingliedern `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Auf ähnliche Weise können Sie die ersten sechs QSFP+-Ports aus Breakout-Konfiguration mit dem neu gruppieren `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie müssen die Planung, Migration und die erforderliche Dokumentation zu 10- GbE- und 40/100-GbE-Konnektivität von den Nodes zu den Nexus 3132Q-V Cluster Switches gelesen haben.

Der "[Cisco Ethernet-Switches](#)" Die Seite enthält Informationen zu den in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen.

Anforderungen für Cisco Nexus 5596

- Folgende Cluster-Switches werden unterstützt:
 - Nexus 5596
 - Nexus 3132Q-V
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert "[Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen](#)" Seite.
- Die Cluster-Switches verwenden die folgenden Ports für Verbindungen zu den Nodes:
 - Ports e1/1-40 (10 GbE): Nexus 5596
 - Ports e1/1-30 (40/100 GbE): Nexus 3132Q-V
- Bei den Cluster-Switches werden die folgenden Inter-Switch Link (ISL)-Ports verwendet:
 - Ports e1/41-48 (10 GbE): Nexus 5596
 - Ports e1/31-32 (40/100 GbE): Nexus 3132Q-V
- Der "[Hardware Universe](#)" Enthält Informationen über die unterstützten Kabel zu Nexus 3132Q-V Switches:
 - Nodes mit 10 GbE-Cluster-Verbindungen erfordern QSFP zu SFP+-Breakout-Kabel oder QSFP zu SFP+-Kupfer-Breakout-Kabel.
 - Nodes mit 40/100 GbE-Cluster-Verbindungen erfordern unterstützte QSFP/QSFP28optische Module mit Glasfaserkabeln oder QSFP/QSFP28 Kupfer-Direct-Attach-Kabeln.
- Die Cluster-Switches verwenden die entsprechende ISL-Verkabelung:
 - Anfang: Nexus 5596 bis Nexus 5596 (SFP+ auf SFP+)
 - 8 x SFP+-Glasfaserkabel oder Kupfer-Direct-Attached-Kabel
 - Zwischenzeit: Nexus 5596 auf Nexus 3132Q-V (QSFP auf 4xSFP+ Breakout-out)
 - 1x Kabel für QSFP zu SFP+-Ausbruchkabel oder Kupferausbruch
 - Finale: Nexus 3132Q-V auf Nexus 3132Q-V (QSFP28 zu QSFP28)
 - 2 QSFP28 Glasfaserkabel oder Kupfer-Direct-Attach-Kabel
- Bei Nexus-Switches 3132Q-V können Sie QSFP/QSFP28-Ports entweder als 40/100-Gigabit-Ethernet- oder als 4-x10-Gigabit-Ethernet-Modus betreiben.

Standardmäßig sind im 40/100-Gigabit-Ethernet-Modus 32 Ports vorhanden. Diese 40-Gigabit-Ethernet-Ports werden in einer 2-tupel-Namenskonvention nummeriert. So wird beispielsweise der zweite 40-Gigabit-Ethernet-Port mit der Nummer 1/2 nummeriert. Der Prozess der Änderung der Konfiguration von 40 Gigabit Ethernet zu 10 Gigabit Ethernet wird *Breakout* genannt und der Prozess der Änderung der Konfiguration von 10 Gigabit Ethernet zu 40 Gigabit Ethernet wird *break* genannt. Wenn Sie einen 40/100-Gigabit-Ethernet-Port in 10 Gigabit-Ethernet-Ports untergliedern, werden die resultierenden Ports mit einer 3-tupel-Namenskonvention nummeriert. Beispielsweise werden die Ausbruchanschlüsse des zweiten 40-Gigabit-Ethernet-Ports mit den Nummern 1/2/1, 1/2/2/2, 1/2/3 und 1/2/4 nummeriert.

- Auf der linken Seite der Nexus 3132Q-V Switches befindet sich ein Satz von 4 SFP+ Ports, die mit diesem

QSFP28-Port multipliziert wurden.

Das RCF ist standardmäßig so strukturiert, dass es den QSFP28-Port verwendet.



Mit dem können Sie 4 SFP+-Ports anstelle eines QSFP-Ports für Nexus 3132Q-V-Switches aktivieren `hardware profile front portmode sfp-plus` Befehl. Auf ähnliche Weise können Sie Nexus 3132Q-V-Switches zurücksetzen, um einen QSFP-Port anstelle von 4 SFP+-Ports mit dem zu verwenden `hardware profile front portmode qsfp` Befehl.

- Sie haben einige der Ports auf Nexus 3132Q-V Switches für 10 GbE oder 40/100 GbE konfiguriert.



Sie können die ersten sechs Ports mit dem in den 4x10 GbE-Modus versetzen `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Auf ähnliche Weise können Sie die ersten sechs QSFP+-Ports aus Breakout-Konfiguration mit dem neu gruppieren `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie haben die Planung, Migration und die erforderliche Dokumentation zu 10-GbE- und 40/100-GbE-Konnektivität von den Nodes zu den Nexus 3132Q-V Cluster Switches gelesen.
- Die in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen befinden sich auf dem "[Cisco Ethernet-Switches](#)" Seite.

Anforderungen von NetApp CN1610

- Folgende Cluster-Switches werden unterstützt:
 - NetApp CN1610
 - Cisco Nexus 3132Q-V
- Die Cluster-Switches unterstützen die folgenden Node-Verbindungen:
 - NetApp CN1610: 0/1 bis 0/12 (10 GbE)
 - Cisco Nexus 3132Q-V: Ports e1/1-30 (40/100 GbE)
- Bei den Cluster-Switches werden die folgenden Inter-Switch-Link-Ports (ISL) verwendet:
 - NetApp CN1610: 0/13 bis 0/16 (10 GbE)
 - Cisco Nexus 3132Q-V: Ports e1/31-32 (40/100 GbE)
- Der "[Hardware Universe](#)" Enthält Informationen über die unterstützten Kabel zu Nexus 3132Q-V Switches:
 - Nodes mit 10 GbE-Cluster-Verbindungen erfordern QSFP zu SFP+-Breakout-Kabel oder QSFP zu SFP+-Kupfer-Breakout-Kabel
 - Nodes mit 40/100 GbE-Cluster-Verbindungen erfordern unterstützte QSFP/QSFP28 optische Module mit optischen Faserkabeln oder QSFP/QSFP28-Kupfer-Direct-Attach-Kabeln
- Die entsprechende ISL-Verkabelung lautet wie folgt:
 - Anfang: Bei CN1610 bis CN1610 (SFP+ zu SFP+), vier SFP+-Glasfaserkabeln oder Direct-Attached-Kabeln für Kupfer
 - Interim: Für CN1610 auf Nexus 3132Q-V (QSFP zu vier SFP+ Breakout), ein QSFP zu SFP+ Glasfaserkabel oder Kupferkabel
 - Finale: Für Nexus 3132Q-V auf Nexus 3132Q-V (QSFP28 zu QSFP28), zwei QSFP28-Glasfaserkabel oder Kupfer-Direct-Attach-Kabel
- NetApp Twinax-Kabel sind nicht kompatibel mit Cisco Nexus 3132Q-V Switches.

Wenn bei Ihrer aktuellen CN1610-Konfiguration NetApp Twinax-Kabel für Cluster-Node-to-Switch-Verbindungen oder ISL-Verbindungen verwendet werden und Sie Twinax-Lösungen in Ihrer Umgebung verwenden möchten, müssen Sie Cisco Twinax-Kabel beschaffen. Alternativ können Sie für die ISL-Verbindungen und die Cluster-Node-to-Switch-Verbindungen Glasfaserkabel verwenden.

- Bei Nexus-Switches 3132Q-V können Sie QSFP/QSFP28-Ports entweder als 40/100-GB-Ethernet- oder als 4x 10-GB-Ethernet-Modi verwenden.

Standardmäßig befinden sich im 40/100-GB-Ethernet-Modus 32 Ports. Diese 40-GB-Ethernet-Ports werden in einer 2-tupel-Namenskonvention nummeriert. Beispielsweise wird der zweite 40-GB-Ethernet-Port mit der Nummer 1/2 nummeriert. Der Prozess der Änderung der Konfiguration von 40 GB Ethernet zu 10 GB Ethernet wird *Breakout* genannt und der Prozess der Änderung der Konfiguration von 10 GB Ethernet zu 40 GB Ethernet wird *break* genannt. Wenn Sie einen 40/100-GB-Ethernet-Port in 10-GB-Ethernet-Ports umwandeln, werden die resultierenden Ports mit einer 3-tupel-Namenskonvention nummeriert. Die Breakout-Ports des zweiten 40-GB-Ethernet-Ports werden beispielsweise als 1/2/1, 1/2/2/2, 1/3 und 1/2/4 nummeriert.

- Auf der linken Seite von Nexus 3132Q-V Switches befindet sich ein Satz von vier SFP+ Ports, die auf den ersten QSFP-Port multipliziert werden.

Standardmäßig ist die Referenzkonfigurationsdatei (RCF) so strukturiert, dass der erste QSFP-Port verwendet wird.

Mit dem können Sie vier SFP+-Ports anstelle eines QSFP-Ports für Nexus 3132Q-V-Switches aktivieren `hardware profile front portmode sfp-plus` Befehl. Auf ähnliche Weise können Sie Nexus 3132Q-V-Switches zurücksetzen, um einen QSFP-Port anstelle von vier SFP+-Ports mit dem zu verwenden `hardware profile front portmode qsfp` Befehl.



Wenn Sie die ersten vier SFP+-Ports verwenden, wird der erste 40-GbE-QSFP-Port deaktiviert.

- Sie müssen einige der Ports auf Nexus 3132Q-V Switches für 10 GbE oder 40/100 GbE konfiguriert haben.

Die ersten sechs Ports können mit dem in den 4-mal 10-GbE-Modus versetzt werden `interface breakout module 1 port 1-6 map 10g-4x` Befehl. Auf ähnliche Weise können Sie die ersten sechs QSFP+-Ports aus *Breakout*-Konfiguration mit dem neu gruppieren `no interface breakout module 1 port 1-6 map 10g-4x` Befehl.

- Sie müssen die Planung, Migration und die erforderliche Dokumentation zu 10- GbE- und 40/100-GbE-Konnektivität von den Nodes zu den Nexus 3132Q-V Cluster Switches gelesen haben.
- Die in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen finden Sie auf der "[Cisco Ethernet-Switches](#)" Seite.
- Die in diesem Verfahren unterstützten ONTAP- und FASTPATH-Versionen werden auf der aufgeführt "[NetApp CN1601 und CN1610 Switches](#)" Seite.

Ersetzen Sie die Cisco Nexus 3132Q-V Cluster Switches

Befolgen Sie diese Vorgehensweise, um einen fehlerhaften Cisco Nexus 3132Q-V Switch in einem Cluster-Netzwerk zu ersetzen. Beim Austausch handelt es sich um einen unterbrechungsfreien Vorgang (Non-Disruptive Procedure, NDO).

Prüfen Sie die Anforderungen

Switch-Anforderungen

Überprüfen Sie die ["Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster Switches"](#).

Was Sie benötigen

- Die vorhandene Cluster- und Netzwerkkonfiguration verfügt über:
 - Die Nexus 3132Q-V Cluster-Infrastruktur ist redundant und funktioniert vollständig auf beiden Switches.
 - Der ["Cisco Ethernet Switch"](#) Die Seite hat die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.
 - Alle Cluster-Ports befinden sich im `up` Bundesland.
 - Management-Konnektivität ist auf beiden Switches vorhanden.
 - Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im `up` Zustand und wurden migriert.
- Stellen Sie beim Nexus 3132Q-V-Ersatzschalter Folgendes sicher:
 - Das Management-Netzwerk-Konnektivität auf dem Ersatz-Switch ist funktionsfähig.
 - Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
 - Der gewünschte RZF- und NX-OS-Betriebssystem-Bildschalter wird auf den Switch geladen.
 - Die anfängliche Anpassung des Schalters ist abgeschlossen.
- ["Hardware Universe"](#)

Tauschen Sie den Schalter aus

Bei diesem Verfahren wird der zweite Nexus 3132Q-V Cluster Switch CL2 durch den neuen 3132Q-V Switch C2 ersetzt.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- n1_clus1 ist die erste logische Clusterschnittstelle (LIF), die für Knoten n1 mit Cluster-Switch C1 verbunden ist.
- n1_clus2 ist die erste Cluster-LIF, die mit Cluster-Switch CL2 oder C2 für Node n1 verbunden ist.
- n1_clus3 ist die zweite logische Schnittstelle, die mit Cluster-Switch C2 für Node n1 verbunden ist.
- n1_clus4 ist die zweite logische Schnittstelle, die mit Cluster-Switch CL1 für Node n1 verbunden ist.
- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den auf der verfügbaren Referenzkonfigurationsdateien (RCFs) definiert ["Cisco® Cluster Network Switch Referenzkonfigurationsdatei Herunterladen"](#) Seite.
- Die Knoten sind n1, n2, n3 und n4. - Die Beispiele in diesem Verfahren verwenden vier Knoten: Zwei Knoten verwenden vier 10 GB Cluster Interconnect Ports: e0a, e0b, e0c und e0d. Die anderen beiden Knoten verwenden zwei 40 GB Cluster Interconnect Ports: e4a und e4e. Siehe ["Hardware Universe"](#) Für die tatsächlichen Cluster-Ports auf Ihren Plattformen.

Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Das Cluster beginnt mit vier Nodes, die mit zwei Nexus 3132Q-V Cluster Switches, CL1 und CL2 verbunden sind.

- Cluster-Switch CL2 ist durch C2 zu ersetzen
 - Bei jedem Node werden mit CL2 verbundene Cluster-LIFs auf Cluster-Ports migriert, die mit CL1 verbunden sind.
 - Trennen Sie die Verkabelung von allen Anschlüssen am CL2, und schließen Sie die Verkabelung wieder an die gleichen Ports am Switch C2 an.
 - Auf jedem Node werden die migrierten Cluster-LIFs zurückgesetzt.

Schritt 1: Vorbereitung auf den Austausch

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster::> network device-discovery show
```

	Local	Discovered		
Node	Port	Device	Interface	Platform
-----	-----	-----	-----	
n1	/cdp			
	e0a	CL1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	CL2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	CL1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	CL1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	CL2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	CL2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	CL1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	CL1	Ethernet1/7	N3K-C3132Q-V
	e4e	CL2	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4a	CL1	Ethernet1/8	N3K-C3132Q-V
	e4e	CL2	Ethernet1/8	N3K-C3132Q-V

```
12 entries were displayed
```

3. Legen Sie den Administrations- oder Betriebsstatus für jede Cluster-Schnittstelle fest:

a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

Ignore

		Speed (Mbps)				
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000 -
-						
e0b	Cluster	Cluster		up	9000	auto/10000 -
-						
e0c	Cluster	Cluster		up	9000	auto/10000 -
-						
e0d	Cluster	Cluster		up	9000	auto/10000 -
-						

Node: n2

Ignore

		Speed (Mbps)				
Health	Health					
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	----	----	----	-----
-----	-----					
e0a	Cluster	Cluster		up	9000	auto/10000 -
-						
e0b	Cluster	Cluster		up	9000	auto/10000 -
-						
e0c	Cluster	Cluster		up	9000	auto/10000 -
-						
e0d	Cluster	Cluster		up	9000	auto/10000 -
-						

Node: n3

Ignore

		Speed (Mbps)				
Health	Health					

Port Status	IPspace Status	Broadcast	Domain	Link	MTU	Admin/Oper	
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

Node: n4

Ignore

Speed (Mbps)

Health Port Status	Health IPspace Status	Broadcast	Domain	Link	MTU	Admin/Oper	
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

12 entries were displayed.

b. Informationen zu den logischen Schnittstellen anzeigen:

network interface show

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	n1_clus1	up/up	10.10.0.1/24	n1
e0b	n1_clus2	up/up	10.10.0.2/24	n1
e0c	n1_clus3	up/up	10.10.0.3/24	n1
e0d	n1_clus4	up/up	10.10.0.4/24	n1
e0a	n2_clus1	up/up	10.10.0.5/24	n2
e0b	n2_clus2	up/up	10.10.0.6/24	n2
e0c	n2_clus3	up/up	10.10.0.7/24	n2
e0d	n2_clus4	up/up	10.10.0.8/24	n2
e0a	n3_clus1	up/up	10.10.0.9/24	n3
e0e	n3_clus2	up/up	10.10.0.10/24	n3
e0a	n4_clus1	up/up	10.10.0.11/24	n4
e0e	n4_clus2	up/up	10.10.0.12/24	n4

12 entries were displayed.

c. Zeigen Sie die Informationen auf den erkannten Cluster-Switches an:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL2 NX3132V	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

4. Vergewissern Sie sich, dass die entsprechenden RCF und das entsprechende Image auf dem neuen Nexus 3132Q-V Switch installiert sind, je nach Ihren Anforderungen, und nehmen Sie alle wesentlichen Standortanpassungen vor.

Sie müssen den Ersatzschalter zu diesem Zeitpunkt vorbereiten. Wenn Sie die RCF und das Image aktualisieren müssen, müssen Sie folgende Schritte ausführen:

- a. Wechseln Sie auf der NetApp Support Site zum "[Cisco Ethernet Switch](#)" Seite.
 - b. Notieren Sie sich Ihren Switch und die erforderlichen Softwareversionen in der Tabelle auf dieser Seite.
 - c. Laden Sie die entsprechende Version des RCF herunter.
 - d. Klicken Sie auf der Seite **Beschreibung** auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und befolgen Sie dann die Anweisungen auf der Seite **Download**, um die RCF herunterzuladen.
 - e. Laden Sie die entsprechende Version der Bildsoftware herunter.
5. Migrieren Sie die LIFs für die mit Switch C2 verbundenen Cluster-Ports:

```
network interface migrate
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass die LIF-Migration auf allen Nodes durchgeführt wird:

```
cluster::*> network interface migrate -vserver Cluster -lif n1_clus2
-source-node n1 -destination-node n1 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n1_clus3
-source-node n1 -destination-node n1 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n2_clus2
-source-node n2 -destination-node n2 -destination-port e0a
cluster::*> network interface migrate -vserver Cluster -lif n2_clus3
-source-node n2 -destination-node n2 -destination-port e0d
cluster::*> network interface migrate -vserver Cluster -lif n3_clus2
-source-node n3 -destination-node n3 -destination-port e4a
cluster::*> network interface migrate -vserver Cluster -lif n4_clus2
-source-node n4 -destination-node n4 -destination-port e4a
```

6. Überprüfen Sie den Systemzustand des Clusters:

```
network interface show
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
(network interface show)
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
e0a	n1_clus1	up/up	10.10.0.1/24	n1
e0a	n1_clus2	up/up	10.10.0.2/24	n1
e0d	n1_clus3	up/up	10.10.0.3/24	n1
e0d	n1_clus4	up/up	10.10.0.4/24	n1
e0a	n2_clus1	up/up	10.10.0.5/24	n2
e0a	n2_clus2	up/up	10.10.0.6/24	n2
e0d	n2_clus3	up/up	10.10.0.7/24	n2
e0d	n2_clus4	up/up	10.10.0.8/24	n2
e4a	n3_clus1	up/up	10.10.0.9/24	n3
e4a	n3_clus2	up/up	10.10.0.10/24	n3
e4a	n4_clus1	up/up	10.10.0.11/24	n4
e4a	n4_clus2	up/up	10.10.0.12/24	n4

12 entries were displayed.

7. Fahren Sie die Cluster-Interconnect-Ports herunter, die physisch mit dem Switch CL2 verbunden sind:

```
network port modify
```

Beispiel anzeigen

In diesem Beispiel werden die angegebenen Ports angezeigt, die auf allen Nodes heruntergefahren werden:

```
cluster::*> network port modify -node n1 -port e0b -up-admin false
cluster::*> network port modify -node n1 -port e0c -up-admin false
cluster::*> network port modify -node n2 -port e0b -up-admin false
cluster::*> network port modify -node n2 -port e0c -up-admin false
cluster::*> network port modify -node n3 -port e4e -up-admin false
cluster::*> network port modify -node n4 -port e4e -up-admin false
```

8. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster
```

Beispiel anzeigen

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8
Cluster n3_clus1 n4      e0a 10.10.0.9
Cluster n3_clus2 n3      e0e 10.10.0.10
Cluster n4_clus1 n4      e0a 10.10.0.11
Cluster n4_clus2 n4      e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
    Local 10.10.0.1 to Remote 10.10.0.5
    Local 10.10.0.1 to Remote 10.10.0.6
    Local 10.10.0.1 to Remote 10.10.0.7
    Local 10.10.0.1 to Remote 10.10.0.8
    Local 10.10.0.1 to Remote 10.10.0.9
    Local 10.10.0.1 to Remote 10.10.0.10
    Local 10.10.0.1 to Remote 10.10.0.11
    Local 10.10.0.1 to Remote 10.10.0.12
    Local 10.10.0.2 to Remote 10.10.0.5
    Local 10.10.0.2 to Remote 10.10.0.6
    Local 10.10.0.2 to Remote 10.10.0.7
    Local 10.10.0.2 to Remote 10.10.0.8
    Local 10.10.0.2 to Remote 10.10.0.9
    Local 10.10.0.2 to Remote 10.10.0.10
    Local 10.10.0.2 to Remote 10.10.0.11
    Local 10.10.0.2 to Remote 10.10.0.12
    Local 10.10.0.3 to Remote 10.10.0.5
    Local 10.10.0.3 to Remote 10.10.0.6
```

```
Local 10.10.0.3 to Remote 10.10.0.7
Local 10.10.0.3 to Remote 10.10.0.8
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
```

Larger than PMTU communication succeeds on 32 path(s)

RPC status:

8 paths up, 0 paths down (tcp check)

8 paths up, 0 paths down (udp check)

9. Fahren Sie bei CL1 die Ports 1/31 und 1/32 herunter, und schalten Sie den aktiven Nexus 3132Q-V Switch ein:

shutdown

Beispiel anzeigen

In diesem Beispiel werden die ISL-Ports 1/31 und 1/32 am Switch CL1 heruntergefahren:

```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1(config-if-range)# shutdown
(CL1(config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

Schritt 2: Ports konfigurieren

1. Entfernen Sie alle Kabel, die am Nexus 3132Q-V Switch CL2 angeschlossen sind, und schließen Sie sie an allen Knoten an den Ersatzschalter C2 an.
2. Entfernen Sie die ISL-Kabel von den Ports e1/31 und e1/32 am CL2, und schließen Sie sie an die gleichen Ports am Ersatzschalter C2 an.
3. ISLs-Ports 1/31 und 1/32 auf dem Nexus 3132Q-V Switch CL1:


```
(CL1)# configure
(CL1) (Config)# interface e1/31-32
(CL1(config-if-range)# no shutdown
(CL1(config-if-range)# exit
(CL1) (Config)# exit
(CL1)#
```

4. Überprüfen Sie, ob die ISLs auf CL1 verfügbar sind:

```
show port-channel
```

Die Ports eth1/31 und eth1/32 sollten angegeben werden (P) , Was bedeutet, dass die ISL-Ports im Port-Channel aktiv sind.

Beispiel anzeigen

```
CL1# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member
Ports
      Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

5. Überprüfen Sie, ob die ISLs auf C2:

```
show port-channel summary
```

Die Ports eth1/31 und eth1/32 sollten angegeben werden (P) , Was bedeutet, dass beide ISL-Ports im Port-Channel aktiv sind.

Beispiel anzeigen

```
C2# 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
      S - Switched       R - Routed
      U - Up (port-channel)
      M - Not in use. Min-links not met

-----
-----
Group Port-          Type   Protocol  Member Ports
Channel
-----
-----
1      Po1 (SU)       Eth     LACP      Eth1/31 (P)  Eth1/32 (P)
```

6. Fahren Sie auf allen Knoten alle mit dem Nexus 3132Q-V Switch verbundenen Cluster-Interconnect-Ports C2:

```
network port modify
```

Beispiel anzeigen

```
cluster::*> network port modify -node n1 -port e0b -up-admin true
cluster::*> network port modify -node n1 -port e0c -up-admin true
cluster::*> network port modify -node n2 -port e0b -up-admin true
cluster::*> network port modify -node n2 -port e0c -up-admin true
cluster::*> network port modify -node n3 -port e4e -up-admin true
cluster::*> network port modify -node n4 -port e4e -up-admin true
```

7. Setzen Sie für alle Nodes alle migrierten Cluster Interconnect LIFs zurück:

```
network interface revert
```

Beispiel anzeigen

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n1_clus3
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus3
Cluster::*> network interface revert -vserver Cluster -lif n3_clus2
Cluster::*> network interface revert -vserver Cluster -lif n4_clus2
```

8. Vergewissern Sie sich, dass die Cluster-Interconnect-Ports jetzt nach Hause zurückgesetzt werden:

```
network interface show
```

Beispiel anzeigen

In diesem Beispiel wird angezeigt, dass alle LIFs erfolgreich zurückgesetzt werden, da die Ports unter aufgeführt sind Current Port Spalte hat den Status von true Im Is Home Spalte. Wenn der Is Home Spaltenwert ist false, Das LIF wurde nicht zurückgesetzt.

```
cluster::*> network interface show -role cluster
(network interface show)
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

12 entries were displayed.

9. Vergewissern Sie sich, dass die Cluster-Ports verbunden sind:

```
network port show
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
(network port show)
```

Node: n1

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----	-----	----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n3

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status

```

Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000 -
-
e4e      Cluster      Cluster      up    9000 auto/40000 -
-

Node: n4

Ignore

Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
-----
-----
e4a      Cluster      Cluster      up    9000 auto/40000 -
-
e4e      Cluster      Cluster      up    9000 auto/40000 -
-

12 entries were displayed.

```

10. Anpingen der Remote-Cluster-Schnittstellen und Durchführen einer RPC-Server-Prüfung:

```
cluster ping-cluster
```

Beispiel anzeigen

```
cluster::~*> cluster ping-cluster -node n1
Host is n1
Getting addresses from network interface table...
Cluster n1_clus1 n1      e0a 10.10.0.1
Cluster n1_clus2 n1      e0b 10.10.0.2
Cluster n1_clus3 n1      e0c 10.10.0.3
Cluster n1_clus4 n1      e0d 10.10.0.4
Cluster n2_clus1 n2      e0a 10.10.0.5
Cluster n2_clus2 n2      e0b 10.10.0.6
Cluster n2_clus3 n2      e0c 10.10.0.7
Cluster n2_clus4 n2      e0d 10.10.0.8
Cluster n3_clus1 n3      e0a 10.10.0.9
Cluster n3_clus2 n3      e0e 10.10.0.10
Cluster n4_clus1 n4      e0a 10.10.0.11
Cluster n4_clus2 n4      e0e 10.10.0.12

Local = 10.10.0.1 10.10.0.2 10.10.0.3 10.10.0.4
Remote = 10.10.0.5 10.10.0.6 10.10.0.7 10.10.0.8 10.10.0.9
10.10.0.10 10.10.0.11 10.10.0.12
Cluster Vserver Id = 4294967293
Ping status:
....
Basic connectivity succeeds on 32 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 1500 byte MTU on 32 path(s):
  Local 10.10.0.1 to Remote 10.10.0.5
  Local 10.10.0.1 to Remote 10.10.0.6
  Local 10.10.0.1 to Remote 10.10.0.7
  Local 10.10.0.1 to Remote 10.10.0.8
  Local 10.10.0.1 to Remote 10.10.0.9
  Local 10.10.0.1 to Remote 10.10.0.10
  Local 10.10.0.1 to Remote 10.10.0.11
  Local 10.10.0.1 to Remote 10.10.0.12
  Local 10.10.0.2 to Remote 10.10.0.5
  Local 10.10.0.2 to Remote 10.10.0.6
  Local 10.10.0.2 to Remote 10.10.0.7
  Local 10.10.0.2 to Remote 10.10.0.8
  Local 10.10.0.2 to Remote 10.10.0.9
  Local 10.10.0.2 to Remote 10.10.0.10
  Local 10.10.0.2 to Remote 10.10.0.11
  Local 10.10.0.2 to Remote 10.10.0.12
  Local 10.10.0.3 to Remote 10.10.0.5
  Local 10.10.0.3 to Remote 10.10.0.6
```

```
Local 10.10.0.3 to Remote 10.10.0.7
Local 10.10.0.3 to Remote 10.10.0.8
Local 10.10.0.3 to Remote 10.10.0.9
Local 10.10.0.3 to Remote 10.10.0.10
Local 10.10.0.3 to Remote 10.10.0.11
Local 10.10.0.3 to Remote 10.10.0.12
Local 10.10.0.4 to Remote 10.10.0.5
Local 10.10.0.4 to Remote 10.10.0.6
Local 10.10.0.4 to Remote 10.10.0.7
Local 10.10.0.4 to Remote 10.10.0.8
Local 10.10.0.4 to Remote 10.10.0.9
Local 10.10.0.4 to Remote 10.10.0.10
Local 10.10.0.4 to Remote 10.10.0.11
Local 10.10.0.4 to Remote 10.10.0.12
```

Larger than PMTU communication succeeds on 32 path(s)

RPC status:

8 paths up, 0 paths down (tcp check)

8 paths up, 0 paths down (udp check)

Schritt 3: Überprüfen Sie die Konfiguration

1. Zeigen Sie die Informationen zu den Geräten in Ihrer Konfiguration an:

- ° network device-discovery show
- ° network port show -role cluster
- ° network interface show -role cluster
- ° system cluster-switch show

Beispiel anzeigen

```
cluster::> network device-discovery show
```

Node	Local Port	Discovered Device	Interface	Platform
n1	/cdp			
	e0a	C1	Ethernet1/1/1	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/1	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/2	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/2	N3K-C3132Q-V
n2	/cdp			
	e0a	C1	Ethernet1/1/3	N3K-C3132Q-V
	e0b	C2	Ethernet1/1/3	N3K-C3132Q-V
	e0c	C2	Ethernet1/1/4	N3K-C3132Q-V
	e0d	C1	Ethernet1/1/4	N3K-C3132Q-V
n3	/cdp			
	e4a	C1	Ethernet1/7	N3K-C3132Q-V
	e4e	C2	Ethernet1/7	N3K-C3132Q-V
n4	/cdp			
	e4a	C1	Ethernet1/8	N3K-C3132Q-V
	e4e	C2	Ethernet1/8	N3K-C3132Q-V

12 entries were displayed.

```
cluster::*> network port show -role cluster
```

```
(network port show)
```

```
Node: n1
```

```
Ignore
```

Health	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper	Speed(Mbps)	Health Status
	e0a	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0b	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0c	Cluster	Cluster	up	9000	auto/10000	-	
	-							
	e0d	Cluster	Cluster	up	9000	auto/10000	-	
	-							

Node: n2

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e0a	Cluster	Cluster		up	9000	auto/10000	-
-							
e0b	Cluster	Cluster		up	9000	auto/10000	-
-							
e0c	Cluster	Cluster		up	9000	auto/10000	-
-							
e0d	Cluster	Cluster		up	9000	auto/10000	-
-							

Node: n3

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

Node: n4

Ignore

						Speed(Mbps)	Health
Health							
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status
Status							
-----	-----	-----		----	----	-----	
-----	-----						
e4a	Cluster	Cluster		up	9000	auto/40000	-
-							
e4e	Cluster	Cluster		up	9000	auto/40000	-
-							

12 entries were displayed.

```
cluster::*> network interface show -role cluster
```

```
(network interface show)
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	-----
-----	----			
Cluster				
	n1_clus1	up/up	10.10.0.1/24	n1
e0a	true			
	n1_clus2	up/up	10.10.0.2/24	n1
e0b	true			
	n1_clus3	up/up	10.10.0.3/24	n1
e0c	true			
	n1_clus4	up/up	10.10.0.4/24	n1
e0d	true			
	n2_clus1	up/up	10.10.0.5/24	n2
e0a	true			
	n2_clus2	up/up	10.10.0.6/24	n2
e0b	true			
	n2_clus3	up/up	10.10.0.7/24	n2
e0c	true			
	n2_clus4	up/up	10.10.0.8/24	n2
e0d	true			
	n3_clus1	up/up	10.10.0.9/24	n3
e4a	true			
	n3_clus2	up/up	10.10.0.10/24	n3
e4e	true			
	n4_clus1	up/up	10.10.0.11/24	n4
e4a	true			
	n4_clus2	up/up	10.10.0.12/24	n4
e4e	true			

12 entries were displayed.

```
cluster::*> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
CL2 NX3132V	cluster-network	10.10.1.102
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000003		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

3 entries were displayed.

2. Entfernen Sie den ausgetauschten Nexus 3132Q-V-Schalter, wenn er nicht bereits automatisch entfernt wird:

```
system cluster-switch delete
```

```
cluster::*> system cluster-switch delete -device CL2
```

3. Überprüfen Sie, ob die richtigen Cluster-Switches überwacht werden:

```
system cluster-switch show
```

Beispiel anzeigen

```
cluster::> system cluster-switch show
```

Switch Model	Type	Address
CL1 NX3132V	cluster-network	10.10.1.101
Serial Number: FOX000001		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		
C2 NX3132V	cluster-network	10.10.1.103
Serial Number: FOX000002		
Is Monitored: true		
Reason:		
Software Version: Cisco Nexus Operating System (NX-OS) Software, Version		
7.0(3)I4(1)		
Version Source: CDP		

2 entries were displayed.

4. Aktivieren Sie die Protokollerfassungsfunktion für die Cluster-Switch-Systemzustandsüberwachung, um Switch-bezogene Protokolldateien zu erfassen:

```
system cluster-switch log setup-password
```

```
system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
C1
C2

cluster::*> system cluster-switch log setup-password

Enter the switch name: C1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log setup-password

Enter the switch name: C2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

5. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Austausch von Cisco Nexus 3132Q-V Cluster-Switches durch Verbindungen ohne Switches

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

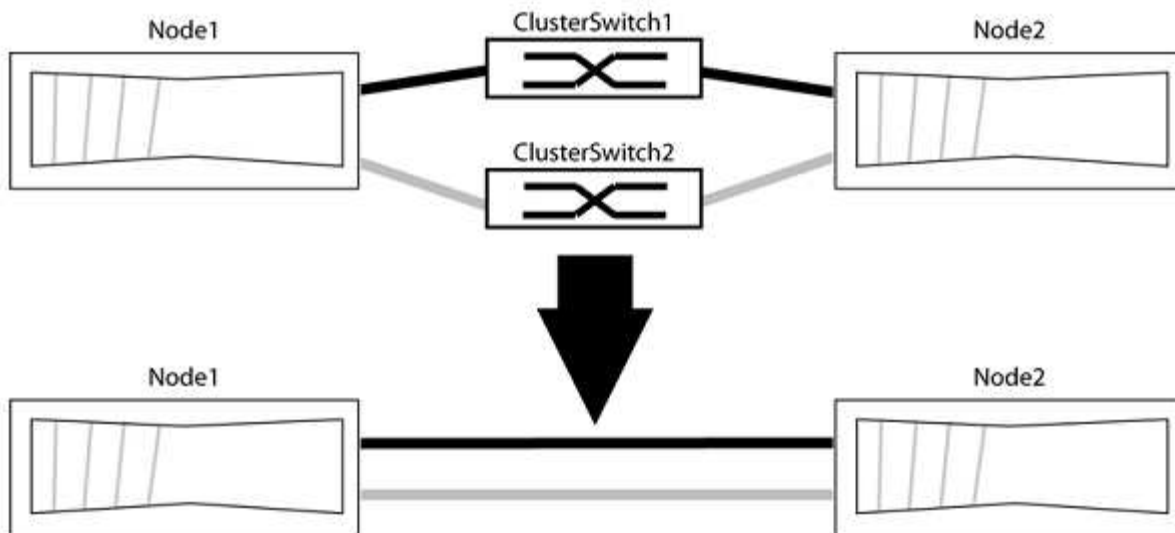
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Angezeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Schritt: Ports und Verkabelung konfigurieren

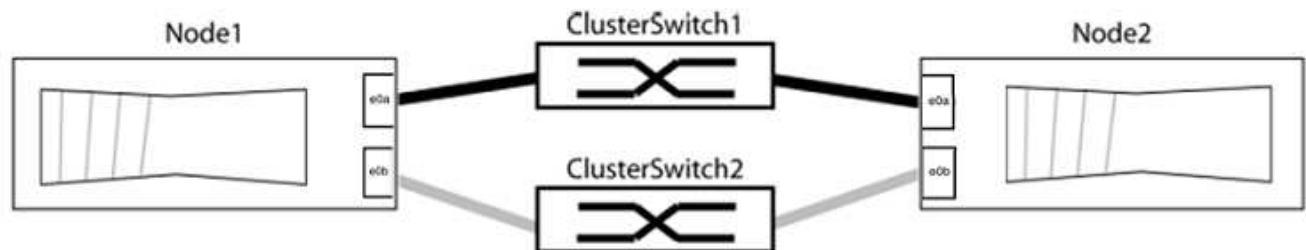
1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in `grp1` zu Cluster-Switch 1 wechseln und die Cluster-Ports in `grp2` zu Cluster-Switch 2 wechseln. Diese Gruppen sind

später im Verfahren erforderlich.

2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



Überprüfen Sie, ob die Ports einen Wert von `up` für die Spalte „Link“ und einen Wert von `healthy` für die Spalte „Integritätsstatus“.

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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

```
network interface revert -vserver Cluster -lif *
```

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

```
network device-discovery show -port cluster_port
```

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

7. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

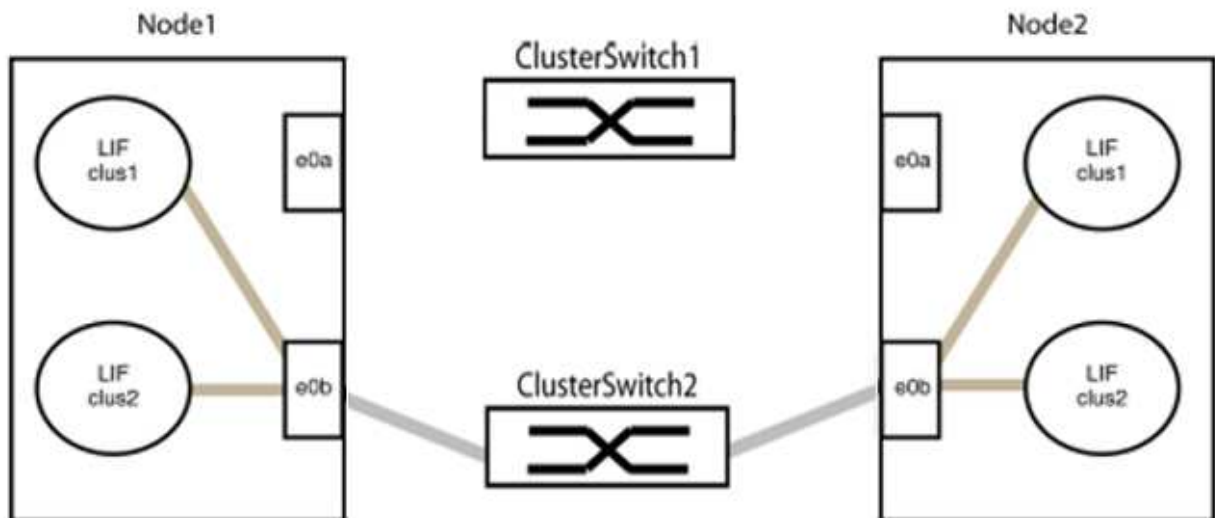
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

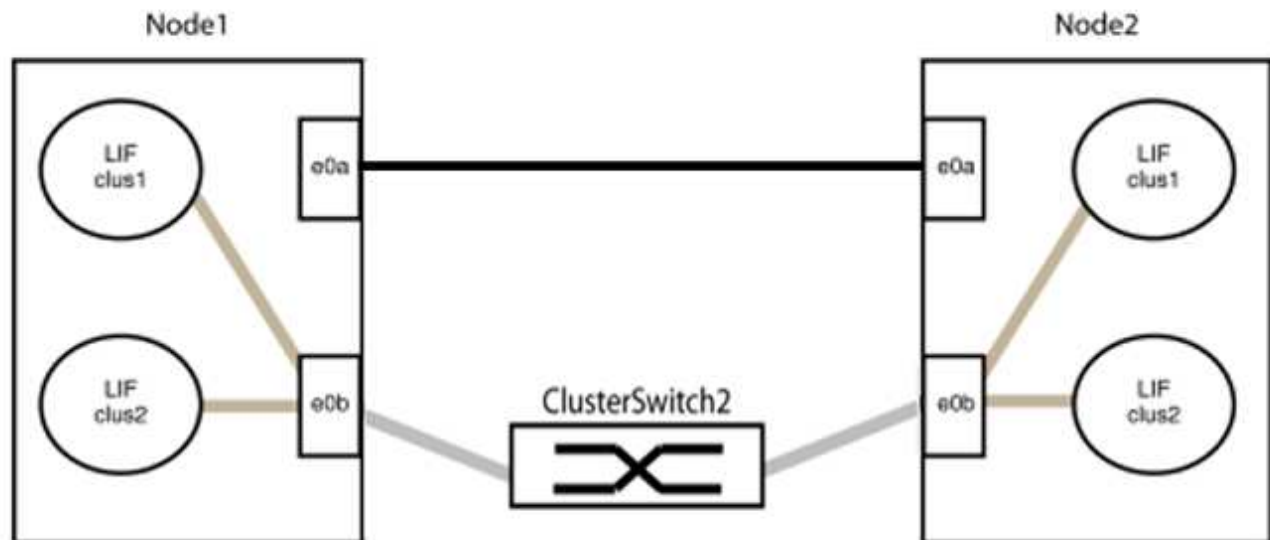
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

```
network options switchless-cluster show
```

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:

```
cluster ping-cluster -node local
```



Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung für Gruppe 1 zu bestätigen.

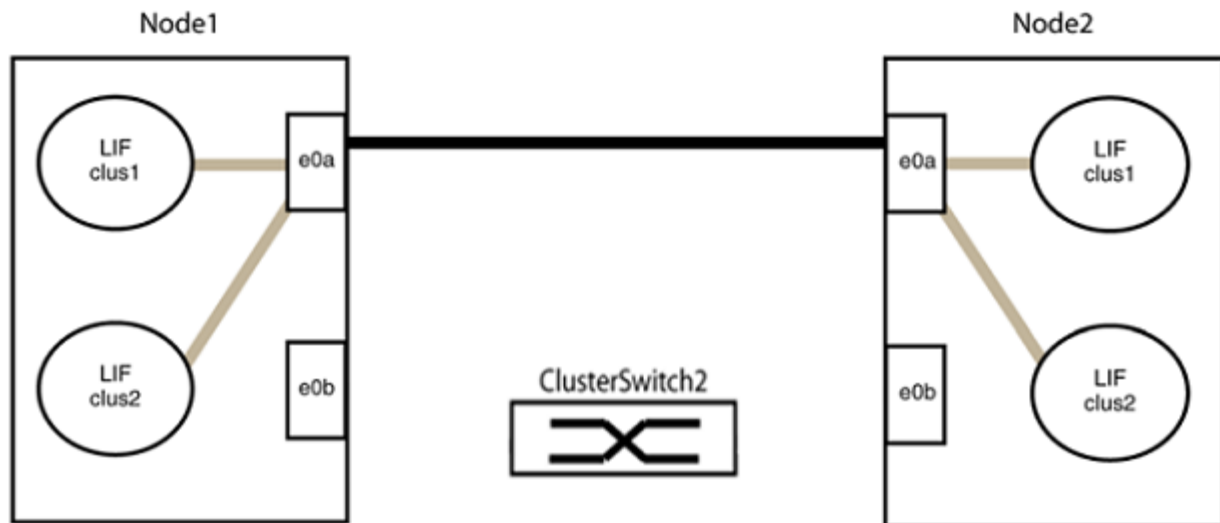
11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

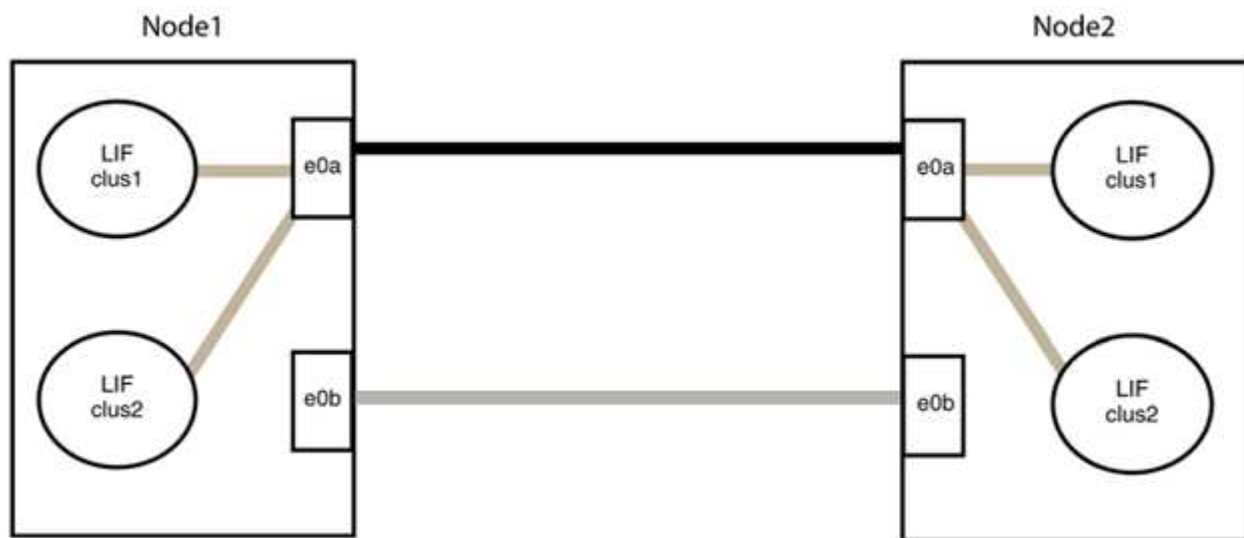
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

```
network device-discovery show -port cluster_port
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

```
network interface show -vserver Cluster -lif lif_name
```

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

Cisco Nexus 92300YC

Überblick

Überblick über die Installation und Konfiguration von Cisco Nexus 92300YC Switches

Lesen Sie vor der Konfiguration von Cisco Nexus 92300YC-Switches die Verfahrensübersicht durch.

Gehen Sie wie folgt vor, um einen Cisco Nexus 92300YC-Switch auf Systemen mit ONTAP zu konfigurieren:

1. ["Füllen Sie das Cisco Nexus 92300YC-Verkabelungsarbeitsblatt aus"](#). Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.
2. ["Konfigurieren Sie den Cisco Nexus 92300YC-Switch"](#). Cisco Nexus 92300YC-Switch einrichten und konfigurieren.
3. ["Vorbereiten der Installation der NX-OS-Software und der Referenzkonfigurationsdatei \(RCF\)"](#). Bereiten Sie sich auf die Installation der NX-OS-Software und der Referenzkonfigurationsdatei (RCF) vor.
4. ["Installieren Sie die NX-OS-Software"](#). Installieren Sie die NX-OS-Software auf dem Nexus 92300YC-Switch. Bei NX-OS handelt es sich um ein Netzwerkbetriebssystem für die Ethernet Switches der Nexus Serie und die MDS Serie mit Fibre Channel (FC) Storage Area Network Switches von Cisco Systems.
5. ["Installieren Sie die Referenzkonfigurationsdatei \(RCF\)"](#). Installieren Sie das RCF, nachdem Sie den Nexus 92300YC-Switch zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.
6. ["Installieren Sie die Konfigurationsdatei des Cluster Switch Health Monitor \(CSHM\)"](#). Installieren Sie die entsprechende Konfigurationsdatei für die Integritätsüberwachung des Cluster Switch bei Nexus 92300YC Cluster Switches.

Weitere Informationen

Bevor Sie mit der Installation oder Wartung beginnen, überprüfen Sie bitte die folgenden Punkte:

- ["Konfigurationsanforderungen"](#)
- ["Komponenten und Teilenummern"](#)
- ["Erforderliche Dokumentation"](#)
- ["Anforderungen für Smart Call Home"](#)

Konfigurationsanforderungen für Cisco Nexus 92300YC Switches

Für die Installation und Wartung von Cisco Nexus 92300YC-Switches müssen alle Konfigurations- und Netzwerkanforderungen geprüft werden.

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Cluster-Netzwerk-Switches erforderlich. Sie können zusätzliche, optionale Management Switches verwenden.

Konfigurationsanforderungen

Zum Konfigurieren des Clusters benötigen Sie die entsprechende Anzahl und den entsprechenden Kabeltyp und Kabelanschlüsse für Ihre Switches. Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

Netzwerkanforderungen

Sie benötigen die folgenden Netzwerkinformationen für alle Switch-Konfigurationen:

- IP-Subnetz für den Management-Netzwerkdatenverkehr
- Host-Namen und IP-Adressen für jeden Storage-System-Controller und alle entsprechenden Switches
- Die meisten Storage-System-Controller werden über die Schnittstelle E0M verwaltet durch eine Verbindung zum Ethernet-Service-Port (Symbol Schraubenschlüssel). Auf AFF A800 und AFF A700 Systemen verwendet die E0M Schnittstelle einen dedizierten Ethernet-Port.

Siehe "[Hardware Universe](#)" Aktuelle Informationen.

Komponenten für Cisco Nexus 92300YC Switches

Prüfen Sie bei der Installation und Wartung von Cisco Nexus 92300YC-Switches alle Switch-Komponenten und Teilenummern. Siehe "[Hardware Universe](#)" Entsprechende Details.

In der folgenden Tabelle sind die Teilenummer und Beschreibung für den 92300YC-Switch, die Lüfter und die Netzteile aufgeführt:

Teilenummer	Beschreibung
190003	Cisco 92300YC, CLSW, 48 Pt10/25 GB, 18 Pt100G, PTSX (PTSX = Port Side Exhaust)
190003R	Cisco 92300YC, CLSW, 48Pt10/25 GB, 18Pt100G, PSIN (PSIN = Port Side Intake)
X-NXA-LÜFTER-35CFM-B	Lüfter, Luftstrom für den seitlichen Cisco N9K-Anschluss
X-NXA-LÜFTER-35CFM-F	Lüfter, seitlicher Luftstrom des Cisco N9K-Ports
X-NXA-PAC-650W-B	Netzteil, Cisco 650W - Anschlusseingang
X-NXA-PAC-650W-F	Netzteil, Cisco 650W - Anschlussseite Auspuff

Details zum Luftstrom des Cisco Nexus 92300YC-Switches:

- Port-Side Abluftstrom (Standardluft) — Kühle Luft dringt durch die Lüfter- und Stromversorgungsmodule im Kaltgang in das Gehäuse ein und auspufft durch das Anschlussende des Gehäuses im heißen Gang. Port-Side Abluftstrom mit blauer Färbung.
- Port-Side Ansaugluftstrom (Rückwärtsluft) — Kühle Luft dringt durch das Anschlussende im kalten Gang in

das Gehäuse ein und entgastet durch die Lüfter- und Stromversorgungsmodule im heißen Gang. Port-Side-Luftstrom mit Burgunder Färbung.

Dokumentationsanforderungen für Cisco Nexus 92300YC-Switches

Prüfen Sie für die Installation und Wartung von Cisco Nexus 92300YC-Switches die empfohlene Dokumentation.

Switch-Dokumentation

Zum Einrichten der Cisco Nexus 92300YC Switches benötigen Sie die folgende Dokumentation von "[Switches Der Cisco Nexus 9000-Serie Unterstützen](#)" Seite:

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie <i>Nexus 9000</i>	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 9000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.
<i>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 9000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 9000-Switches.
<i>Nexus 9000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.
<i>Versionshinweise zur Cisco Nexus 9000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Betriebssystemversion über das ["ONTAP 9 Dokumentationszentrum"](#).

Name	Beschreibung
Controller-spezifisch <i>Installations- und Setup-Anleitung</i>	Beschreibt die Installation von NetApp Hardware.
ONTAP-Dokumentation	Dieser Service bietet detaillierte Informationen zu allen Aspekten der ONTAP Versionen.
"Hardware Universe"	Liefert Informationen zur NetApp Hardwarekonfiguration und -Kompatibilität.

Schienensatz und Rack-Dokumentation

Informationen zur Installation eines Cisco Nexus 92300YC Switch in einem NetApp-Schrank finden Sie in der folgenden Hardware-Dokumentation.

Name	Beschreibung
"42-HE-System-Cabinet, Deep Guide"	Beschreibt die FRUs, die dem 42U-Systemschrank zugeordnet sind, und bietet Anweisungen für Wartung und FRU-Austausch.
"[Installieren Sie einen Cisco Nexus 92300YC Switch in einem NetApp Cabinet]"	Beschreibt die Installation eines Cisco Nexus 92300YC Switches in einem NetApp Rack mit vier Säulen.

Anforderungen für Smart Call Home

Überprüfen Sie die folgenden Richtlinien, um die Smart Call Home-Funktion zu verwenden.

Smart Call Home überwacht die Hardware- und Softwarekomponenten Ihres Netzwerks. Wenn eine kritische Systemkonfiguration auftritt, generiert es eine E-Mail-basierte Benachrichtigung und gibt eine Warnung an alle Empfänger aus, die im Zielprofil konfiguriert sind. Um Smart Call Home zu verwenden, müssen Sie einen Cluster-Netzwerk-Switch konfigurieren, um per E-Mail mit dem Smart Call Home-System kommunizieren zu können. Darüber hinaus können Sie optional Ihren Cluster-Netzwerk-Switch einrichten, um die integrierte Smart Call Home-Support-Funktion von Cisco zu nutzen.

Bevor Sie Smart Call Home verwenden können, beachten Sie die folgenden Punkte:

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.
- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.

- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

Der "[Cisco Support-Website](#)" Enthält Informationen zu den Befehlen zum Konfigurieren von Smart Call Home.

Hardware installieren

Füllen Sie das Cisco Nexus 92300YC-Verkabelungsarbeitsblatt aus

Wenn Sie die unterstützten Plattformen dokumentieren möchten, laden Sie eine PDF-Datei dieser Seite herunter, und füllen Sie das Verkabelungsarbeitsblatt aus.

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

Beispiel für eine Verkabelung

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	10/25-GbE-Node	1	10/25-GbE-Node
2	10/25-GbE-Node	2	10/25-GbE-Node
3	10/25-GbE-Node	3	10/25-GbE-Node
4	10/25-GbE-Node	4	10/25-GbE-Node
5	10/25-GbE-Node	5	10/25-GbE-Node
6	10/25-GbE-Node	6	10/25-GbE-Node
7	10/25-GbE-Node	7	10/25-GbE-Node
8	10/25-GbE-Node	8	10/25-GbE-Node
9	10/25-GbE-Node	9	10/25-GbE-Node
10	10/25-GbE-Node	10	10/25-GbE-Node
11	10/25-GbE-Node	11	10/25-GbE-Node
12	10/25-GbE-Node	12	10/25-GbE-Node
13	10/25-GbE-Node	13	10/25-GbE-Node

Cluster-Switch A		Cluster-Switch B	
14	10/25-GbE-Node	14	10/25-GbE-Node
15	10/25-GbE-Node	15	10/25-GbE-Node
16	10/25-GbE-Node	16	10/25-GbE-Node
17	10/25-GbE-Node	17	10/25-GbE-Node
18	10/25-GbE-Node	18	10/25-GbE-Node
19	10/25-GbE-Node	19	10/25-GbE-Node
20	10/25-GbE-Node	20	10/25-GbE-Node
21	10/25-GbE-Node	21	10/25-GbE-Node
22	10/25-GbE-Node	22	10/25-GbE-Node
23	10/25-GbE-Node	23	10/25-GbE-Node
24	10/25-GbE-Node	24	10/25-GbE-Node
25	10/25-GbE-Node	25	10/25-GbE-Node
26	10/25-GbE-Node	26	10/25-GbE-Node
27	10/25-GbE-Node	27	10/25-GbE-Node
28	10/25-GbE-Node	28	10/25-GbE-Node
29	10/25-GbE-Node	29	10/25-GbE-Node
30	10/25-GbE-Node	30	10/25-GbE-Node
31	10/25-GbE-Node	31	10/25-GbE-Node
32	10/25-GbE-Node	32	10/25-GbE-Node
33	10/25-GbE-Node	33	10/25-GbE-Node
34	10/25-GbE-Node	34	10/25-GbE-Node
35	10/25-GbE-Node	35	10/25-GbE-Node

Cluster-Switch A		Cluster-Switch B	
36	10/25-GbE-Node	36	10/25-GbE-Node
37	10/25-GbE-Node	37	10/25-GbE-Node
38	10/25-GbE-Node	38	10/25-GbE-Node
39	10/25-GbE-Node	39	10/25-GbE-Node
40	10/25-GbE-Node	40	10/25-GbE-Node
41	10/25-GbE-Node	41	10/25-GbE-Node
42	10/25-GbE-Node	42	10/25-GbE-Node
43	10/25-GbE-Node	43	10/25-GbE-Node
44	10/25-GbE-Node	44	10/25-GbE-Node
45	10/25-GbE-Node	45	10/25-GbE-Node
46	10/25-GbE-Node	46	10/25-GbE-Node
47	10/25-GbE-Node	47	10/25-GbE-Node
48	10/25-GbE-Node	48	10/25-GbE-Node
49	40/100-GbE-Node	49	40/100-GbE-Node
50	40/100-GbE-Node	50	40/100-GbE-Node
51	40/100-GbE-Node	51	40/100-GbE-Node
52	40/100-GbE-Node	52	40/100-GbE-Node
53	40/100-GbE-Node	53	40/100-GbE-Node
54	40/100-GbE-Node	54	40/100-GbE-Node
55	40/100-GbE-Node	55	40/100-GbE-Node
56	40/100-GbE-Node	56	40/100-GbE-Node
57	40/100-GbE-Node	57	40/100-GbE-Node

Cluster-Switch A		Cluster-Switch B	
58	40/100-GbE-Node	58	40/100-GbE-Node
59	40/100-GbE-Node	59	40/100-GbE-Node
60	40/100-GbE-Node	60	40/100-GbE-Node
61	40/100-GbE-Node	61	40/100-GbE-Node
62	40/100-GbE-Node	62	40/100-GbE-Node
63	40/100-GbE-Node	63	40/100-GbE-Node
64	40/100-GbE-Node	64	40/100-GbE-Node
65	100-GbE-ISL für Switch B-Port 65	65	100-GbE-ISL für Switch A-Port 65
66	100-GbE-ISL für Switch B-Port 66	66	100-GbE-ISL für Switch A-Port 65

Leeres Verkabelungsarbeitsblatt

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des "[Hardware Universe](#)" Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Node-/Port-Verwendung	Switch-Port	Node-/Port-Verwendung
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	

Cluster-Switch A		Cluster-Switch B	
9		9	
10		10	
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		25	
26		26	
27		27	
28		28	
29		29	
30		30	

Cluster-Switch A		Cluster-Switch B	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	

Cluster-Switch A		Cluster-Switch B	
53		53	
54		54	
55		55	
56		56	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL zu Switch B Port 65	65	ISL für Switch A Port 65
66	ISL zu Switch B Port 66	66	ISL für Switch A Port 66

Konfigurieren Sie den Cisco Nexus 92300YC-Switch

Gehen Sie wie folgt vor, um den Cisco Nexus 92300YC-Switch einzurichten und zu konfigurieren.

Schritte

1. Verbinden Sie den seriellen Port mit einem Host oder einem seriellen Port.
2. Verbinden Sie den Verwaltungsport (auf der Seite des Switches ohne Port) mit dem gleichen Netzwerk, in dem sich der SFTP-Server befindet.
3. Legen Sie an der Konsole die seriellen Einstellungen der Host-Seite fest:
 - 9600 Baud
 - 8 Datenbits
 - 1 Stoppbit
 - Parität: Keine

- Flusskontrolle: Keine

4. Beim ersten Booten oder Neustart nach dem Löschen der laufenden Konfiguration wird der Nexus 92300YC-Switch in einem Boot-Zyklus ausgeführt. Unterbrechen Sie diesen Zyklus, indem Sie **yes** eingeben, um das Einschalten der automatischen Provisionierung abubrechen.

Das Setup des Systemadministratorkontos wird angezeigt.

Beispiel anzeigen

```
$ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
[yes - continue with normal setup, skip - bypass password and basic
configuration, no - continue with Power On Auto Provisioning]
(yes/skip/no) [no]: y
Disabling POAP.....Disabling POAP
2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
wait... (This may take 5-15 minutes)

      ---- System Admin Account Setup ----

Do you want to enforce secure password standard (yes/no) [y]:
```

5. Geben Sie ***y*** ein, um den sicheren Kennwortstandard durchzusetzen:

```
Do you want to enforce secure password standard (yes/no) [y]: y
```

6. Geben Sie das Passwort für den Benutzer admin ein und bestätigen Sie es:

```
Enter the password for "admin":
Confirm the password for "admin":
```

7. Geben Sie **yes** ein, um das Dialogfeld Grundkonfiguration des Systems aufzurufen.

Beispiel anzeigen

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

Please register Cisco Nexus9000 Family devices promptly with your supplier. Failure to register may affect response times for initial service calls. Nexus9000 devices must be registered to receive entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):

8. Ein weiteres Anmeldekonto erstellen:

Create another login account (yes/no) [n]:

9. Konfigurieren Sie die SNMP-Community-Strings Read-Only und read-write:

Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:

10. Konfigurieren Sie den Namen des Cluster-Switches:

Enter the switch name : **cs2**

11. Konfigurieren Sie die Out-of-Band-Managementoberfläche:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Erweiterte IP-Optionen konfigurieren:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Telnet-Dienste konfigurieren:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Konfigurieren von SSH-Diensten und SSH-Schlüsseln:

```
Enable the ssh service? (yes/no) [y]: y

Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Weitere Einstellungen konfigurieren:

```
Configure the ntp server? (yes/no) [n]: n

Configure default interface layer (L3/L2) [L2]: L2

Configure default switchport interface state (shut/noshut) [noshut]:
noshut

Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Bestätigen Sie die Switch-Informationen und speichern Sie die Konfiguration:

```
Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Was kommt als Nächstes?

["Bereiten Sie sich auf die Installation der NX-OS-Software und der RCF vor"](#).

Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 92300YC-Switch konfigurieren, gehen Sie die folgenden Überlegungen durch.

Unterstützung für NVIDIA CX6-, CX6-DX- und CX7-Ethernet-Ports

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 Switch-Port-Geschwindigkeit fest kodieren.

```
(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 ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

Software konfigurieren

Vorbereiten der Installation der NX-OS-Software und der Referenzkonfigurationsdatei (RCF)

Bevor Sie die NX-OS-Software und die RCF-Datei (Reference Configuration File) installieren, gehen Sie wie folgt vor:

Was Sie benötigen

- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Entsprechende Leitfäden für Software und Upgrades, die bei verfügbar sind ["Switches Der Cisco Nexus 9000-Serie"](#).

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster-Interconnect-Ports e0a Und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` Und `cs2`.
- Die Node-Namen sind `node1` Und `node2`.
- Die LIF-Namen des Clusters sind `node1_clus1` Und `node1_clus2` Für Node1 und `node2_clus1` Und `node2_clus2` Für Knoten 2.
- Der `cluster1: :*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.

Über diese Aufgabe

Das Verfahren erfordert die Verwendung von ONTAP Befehlen und den Switches der Cisco Nexus 9000 Serie. ONTAP Befehle werden verwendet, sofern nicht anders angegeben. Die Ausgaben für die Befehle können je nach verschiedenen Versionen von ONTAP variieren.

Schritte

1. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (``*>``) erscheint.

2. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster1:> **system node autosupport invoke -node * -type all -message  
MAINT=2h**
```

3. Zeigen Sie an, wie viele Cluster-Interconnect-Schnittstellen in jedem Node für jeden Cluster Interconnect-Switch konfiguriert sind: `network device-discovery show -protocol cdp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	Eth1/2	N9K-
C92300YC				
	e0b	cs2	Eth1/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	Eth1/1	N9K-
C92300YC				
	e0b	cs2	Eth1/1	N9K-
C92300YC				

4 entries were displayed.

4. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.
 - a. Zeigen Sie die Attribute des Netzwerkports an: `network port show -ip space Cluster`

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
```

Node: node2

Health					Speed (Mbps)	
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: node1

Health					Speed (Mbps)	
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. Zeigt Informationen zu den LIFs an: `network interface show -vserver Cluster`

Beispiel anzeigen

```
cluster1::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	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. Ping für die Remote-Cluster-LIFs:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
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)
```

6. Vergewissern Sie sich, dass der automatische Zurücksetzen-Befehl 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
```

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

7. Aktivieren Sie für ONTAP 9.4 und höher die Protokollerfassungsfunktion für die Cluster Switch-Systemzustandsüberwachung, um mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien zu gelangen:

```
system cluster-switch log setup-password Und system cluster-switch log enable-collection
```

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Was kommt als Nächstes?

["Installieren Sie die NX-OS-Software".](#)

Installieren Sie die NX-OS-Software

Gehen Sie folgendermaßen vor, um die NX-OS-Software auf dem Nexus 92300YC-Switch zu installieren.

Bei NX-OS handelt es sich um ein Netzwerkbetriebssystem für die Ethernet Switches der Nexus Serie und die MDS Serie mit Fibre Channel (FC) Storage Area Network Switches von Cisco Systems.

Prüfen Sie die Anforderungen

Unterstützte Ports und Node-Verbindungen

- Die Inter-Switch Links (ISLs) werden für Nexus 92300YC Switches unterstützt; die Ports 1/65 und 1/66.
- Die für Nexus 92300YC-Switches unterstützten Node-Verbindungen sind die Ports 1/1 bis 1/66.

Was Sie benötigen

- Anwendbare NetApp Cisco NX-OS Software für Ihre Switches über die NetApp Support Site, erhältlich über "mysupport.netapp.com"
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- "[Cisco Ethernet Switch Seite](#)". In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.

Installieren Sie die Software

Die Beispiele in diesem Verfahren verwenden zwei Nodes, Sie können jedoch bis zu 24 Nodes in einem Cluster haben.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Switch-Namen des Nexus 92300YC sind `cs1` Und `cs2`.
- Das in diesem Verfahren verwendete Beispiel startet das Upgrade auf dem zweiten Schalter `*cs2*`.
- Die LIF-Namen des Clusters sind `node1_clus1` Und `node1_clus2` Für Node1, und `node2_clus1` Und `node2_clus2` Für Knoten 2.
- Der IPspace-Name lautet `Cluster`.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die Cluster-Ports an jedem Node werden mit benannt `e0a` Und `e0b`.

Siehe "[Hardware Universe](#)" Für die tatsächlichen Cluster-Ports, die auf Ihrer Plattform unterstützt werden.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung mit dem Server, der die NX-OS-Software und die RCF hostet.

Beispiel anzeigen

In diesem Beispiel wird überprüft, ob der Switch den Server unter der IP-Adresse 172.19.2 erreichen kann:

```
cs2# ping 172.19.2.1  
Pinging 172.19.2.1 with 0 bytes of data:  
  
Reply From 172.19.2.1: icmp_seq = 0. time= 5910 usec.
```

3. Kopieren Sie die NX-OS-Software und EPLD-Bilder auf den Nexus 92300YC-Switch.

Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.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.9.2.2.bin /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.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.9.2.2.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.9.2.2.img /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img 100% 161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

4. 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) 2002-2018, 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 05.31
  NXOS: version 9.2(1)
  BIOS compile time: 05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time: 7/17/2018 16:00:00 [07/18/2018 00:21:19]

Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

  Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
System version: 9.2(1)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Installieren Sie das NX-OS Image.

Durch die Installation der Image-Datei wird sie bei jedem Neustart des Switches geladen.

Beispiel anzeigen

```
cs2# install all nxos bootflash:nxos.9.2.2.bin
```

```
Installer will perform compatibility check first. Please wait.  
Installer is forced disruptive
```

```
Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".  
[] 100% -- SUCCESS
```

```
Verifying image type.  
[] 100% -- SUCCESS
```

```
Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.  
[] 100% -- SUCCESS
```

```
Preparing "bios" version info using image bootflash:/nxos.9.2.2.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	9.2(1)	
9.2(2)	yes		
1	bios	v05.31(05/17/2018):v05.28(01/18/2018)	
v05.33(09/08/2018)	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
```

```
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:  
Successfully deactivated virtual service 'guestshell+'
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
```

6. 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) 2002-2018, 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 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]
```

Hardware

```
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash: 115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)
```

```
Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

Reason: Reset due to upgrade

System version: 9.2(1)

Service:

plugin

Core Plugin, Ethernet Plugin

Active Package(s):

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.2.2.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
1	SUP	MI FPGA	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	IO FPGA	Success

1 SUP Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. Melden Sie sich nach dem Neustart des Switches erneut an, und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# *show version module 1 epld*
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x19
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

Was kommt als Nächstes?

["Installieren Sie die Referenzkonfigurationsdatei"](#)

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können den RCF installieren, nachdem Sie den Nexus 92300YC-Switch zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

Über diese Aufgabe

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der beiden Cisco Switches lauten `cs1` Und `cs2`.
- Die Node-Namen sind `node1` Und `node2`.
- Die LIF-Namen des Clusters sind `node1_clus1`, `node1_clus2`, `node2_clus1`, und `node2_clus2`.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.



- Das Verfahren erfordert die Verwendung von ONTAP-Befehlen und "[Switches Der Cisco Nexus 9000-Serie](#)"; ONTAP-Befehle werden verwendet, sofern nicht anders angegeben.
- Bevor Sie dieses Verfahren durchführen, stellen Sie sicher, dass Sie über eine aktuelle Sicherung der Switch-Konfiguration verfügen.
- Bei diesem Verfahren ist keine betriebsbereite ISL (Inter Switch Link) erforderlich. Dies ist von Grund auf so, dass Änderungen der RCF-Version die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, werden mit dem folgenden Verfahren alle Cluster-LIFs auf den betriebsbereiten Partner-Switch migriert, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Schritte

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> *network device-discovery show*
Node/          Local   Discovered
Protocol       Port   Device (LLDP: ChassisID)  Interface
Platform
-----
node1/cdp
      e0a      cs1                Ethernet1/1/1      N9K-
C92300YC
      e0b      cs2                Ethernet1/1/1      N9K-
C92300YC
node2/cdp
      e0a      cs1                Ethernet1/1/2      N9K-
C92300YC
      e0b      cs2                Ethernet1/1/2      N9K-
C92300YC
cluster1::*>
```

2. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
 - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

```
network port show -ip space Cluster
```

Beispiel anzeigen

```
cluster1::*> *network port show -ipspace Cluster*

Node: node1

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e0c         Cluster      Cluster      up    9000  auto/100000
healthy false
e0d         Cluster      Cluster      up    9000  auto/100000
healthy false

Node: node2

Ignore

Health      Health      Speed(Mbps)
Port        IPspace      Broadcast Domain Link MTU  Admin/Oper
Status      Status
-----
e0c         Cluster      Cluster      up    9000  auto/100000
healthy false
e0d         Cluster      Cluster      up    9000  auto/100000
healthy false
cluster1::*>
```

- b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:
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
e0c      true      node1_clus1      up/up      169.254.3.4/23      node1
e0d      true      node1_clus2      up/up      169.254.3.5/23      node1
e0c      true      node2_clus1      up/up      169.254.3.8/23      node2
e0d      true      node2_clus2      up/up      169.254.3.9/23      node2
cluster1::*>
```

- c. Vergewissern Sie sich, dass auf dem Cluster Informationen für beide Cluster-Switches angezeigt werden:

```
system cluster-switch show -is-monitoring-enabled-operational true
```

Beispiel anzeigen

```
cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                                     Type                Address
Model
-----
cs1                                     cluster-network     10.233.205.92
N9K-C92300YC
    Serial Number: FOXXXXXXXXGS
    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
N9K-C92300YC
    Serial Number: FOXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                        9.3(4)
    Version Source: CDP

2 entries were displayed.
```

3. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert false
```

4. Fahren Sie beim Cluster-Switch cs2 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Überprüfen Sie, ob die Cluster-Ports zu den Ports migriert wurden, die auf 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
      node1_clus1      up/up      169.254.3.4/23      node1
e0c      true
      node1_clus2      up/up      169.254.3.5/23      node1
e0c      false
      node2_clus1      up/up      169.254.3.8/23      node2
e0c      true
      node2_clus2      up/up      169.254.3.9/23      node2
e0c      false
cluster1::*>
```

6. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> *cluster show*

Node      Health      Eligibility      Epsilon
-----
node1      true      true      false
node2      true      true      false
cluster1::*>
```

7. Wenn Sie dies noch nicht getan haben, speichern Sie eine Kopie der aktuellen Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Textdatei kopieren:

```
show running-config
```

8. Reinigen Sie die Konfiguration am Schalter cs2, und führen Sie eine grundlegende Einrichtung durch.



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase
```

```
Warning: This command will erase the startup-configuration.
```

```
Do you wish to proceed anyway? (y/n) [n] y
```

b. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload
```

```
Are you sure you would like to reset the system? (y/n) y
```

9. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im ["Switches Der Cisco Nexus 9000-Serie"](#) Leitfäden.

Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

```
cs2# copy tftp: bootflash: vrf management  
Enter source filename: /code/Nexus_92300YC_RCF_v1.0.2.txt  
Enter hostname for the tftp 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:  
tftp> progress  
Progress meter enabled  
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin  
/code/Nexus_92300YC_R 100% 9687 530.2KB/s 00:00  
tftp> exit  
Copy complete, now saving to disk (please wait)...  
Copy complete.
```

10. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im ["Switches Der Cisco Nexus 9000-Serie"](#) Leitfäden.

Dieses Beispiel zeigt die RCF-Datei Nexus_92300YC_RCF_v1.0.2.txt Installation auf Schalter cs2:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands
```

Disabling ssh: as its enabled right now:

generating ecdsa key(521 bits).....

generated ecdsa key

Enabling ssh: as it has been disabled

this command enables edge port type (portfast) by default on all interfaces. You

should now disable edge port type (portfast) explicitly on switched ports leading to hubs,

switches and bridges as they may create temporary bridging loops.

Edge port type (portfast) should only be enabled on ports connected to a single

host. Connecting hubs, concentrators, switches, bridges, etc... to this

interface when edge port type (portfast) is enabled, can cause temporary bridging loops.

Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet1/1 but will only

have effect when the interface is in a non-trunking mode.

...

Copy complete, now saving to disk (please wait)...

Copy complete.

11. Überprüfen Sie auf dem Switch, ob die RCF erfolgreich zusammengeführt wurde:

```
show running-config
```



```

cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJlRtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1 - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*

```



Beim ersten Anwenden des RCF wird die Meldung **ERROR: Failed to write VSH** befiehlt erwartet und kann ignoriert werden.

1. Überprüfen Sie, ob die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

2. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im ["Switches Der Cisco Nexus 9000-Serie"](#) Leitfäden.

```
cs2# copy running-config startup-config  
[] 100% Copy complete
```

3. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

```
cs2# reload  
This command will reboot the system. (y/n)? [n] y
```

4. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.
 - a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß sind:

```
network port show -ipspace Cluster
```

Beispiel anzeigen

```
cluster1::*> *network port show -ipspace Cluster*

Node: node1

Ignore

Health      Health      Speed (Mbps)
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

Health      Health      Speed (Mbps)
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 den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

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
N9K-C92300YC
          e0b    cs2                      Ethernet1/1
N9K-C92300YC
node2/cdp
          e0a    cs1                      Ethernet1/2
N9K-C92300YC
          e0b    cs2                      Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch          Type          Address
Model
-----
cs1              cluster-network  10.233.205.90
N9K-C92300YC
    Serial Number: FOXXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                9.3(4)
    Version Source: CDP

cs2              cluster-network  10.233.205.91
N9K-C92300YC
    Serial Number: FOXXXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                9.3(4)
    Version Source: CDP

2 entries were displayed.

```

Je nach der zuvor auf dem Switch geladenen RCF-Version können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten



```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-
UNBLOCK_CONSIST_PORT: 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.
```

5. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels aus Schritt 1 verwendet:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

6. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf dem 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
e0d      node1_clus1      up/up      169.254.3.4/23      node1
false
e0d      node1_clus2      up/up      169.254.3.5/23      node1
true
e0d      node2_clus1      up/up      169.254.3.8/23      node2
false
e0d      node2_clus2      up/up      169.254.3.9/23      node2
true
cluster1::*>
```

7. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node           Health   Eligibility   Epsilon
-----
node1          true    true         false
node2          true    true         false
cluster1::*>
```

8. Wiederholen Sie die Schritte 7 bis 14 am Schalter cs1.
9. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

```
cluster1::*> network interface modify -vserver Cluster -lif * -auto
-revert True
```

10. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

```
cs1# reload
This command will reboot the system. (y/n)? [n] y
```

11. Vergewissern Sie sich, dass die mit den Cluster-Ports verbundenen Switch-Ports aktiv sind.

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1      eth  access up    none
10G(D) --
Ethernet1/2      1      eth  access up    none
10G(D) --
Ethernet1/3      1      eth  trunk  up    none
100G(D) --
Ethernet1/4      1      eth  trunk  up    none
100G(D) --
.
.
```

12. Stellen Sie sicher, dass die ISL 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      Eth1/65 (P)  Eth1/66 (P)
cs1#
```

13. Vergewissern Sie sich, dass die Cluster-LIFs auf ihren Home-Port zurückgesetzt wurden:

```
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      169.254.3.4/23  node1
e0d       true
          node1_clus2  up/up      169.254.3.5/23  node1
e0d       true
          node2_clus1  up/up      169.254.3.8/23  node2
e0d       true
          node2_clus2  up/up      169.254.3.9/23  node2
e0d       true
cluster1::*>
```


14. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node           Health Eligibility  Epsilon
-----
node1          true   true       false
node2          true   true       false
```

15. Ping für die Remote-Cluster-Schnittstellen zur Überprüfung der Konnektivität:

```
cluster ping-cluster -node local
```

Beispiel anzeigen

```
cluster1::*> *cluster ping-cluster -node local*
Host is node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 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)
```

Für ONTAP 9.8 und höher

Aktivieren Sie für ONTAP 9.8 und höher die Protokollerfassung der Cluster Switch-Systemzustandsüberwachung zum Erfassen von Switch-bezogenen Protokolldateien mithilfe der Befehle:
system switch ethernet log setup-password Und system switch ethernet log enable-collection

Geben Sie Ein: system switch ethernet log setup-password

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs1
```

```
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
```

```
Do you want to continue? {y|n}::[n] y
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

```
cluster1::*> system switch ethernet log setup-password
```

```
Enter the switch name: cs2
```

```
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
```

```
Do you want to continue? {y|n}:: [n] y
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

Gefolgt von: system switch ethernet log enable-collection

```
cluster1::*> system switch ethernet log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```

Für ONTAP 9.4 und höher

Aktivieren Sie für ONTAP 9.4 und höher die Protokollerfassungsfunktion für die Cluster Switch-Systemzustandsüberwachung, um mit den Befehlen zum Erfassen von Switch-bezogenen Protokolldateien zu gelangen:

```
system cluster-switch log setup-password Und system cluster-switch log enable-collection
```

Geben Sie Ein: `system cluster-switch log setup-password`

```
cluster1::*> system cluster-switch log setup-password
```

```
Enter the switch name: <return>
```

```
The switch name entered is not recognized.
```

```
Choose from the following list:
```

```
cs1
```

```
cs2
```

```
cluster1::*> system cluster-switch log setup-password
```

```
Enter the switch name: cs1
```

```
RSA key fingerprint is e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
```

```
Do you want to continue? {y|n}::[n] y
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

```
cluster1::*> system cluster-switch log setup-password
```

```
Enter the switch name: cs2
```

```
RSA key fingerprint is 57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
```

```
Do you want to continue? {y|n}:: [n] y
```

```
Enter the password: <enter switch password>
```

```
Enter the password again: <enter switch password>
```

Gefolgt von: `system cluster-switch log enable-collection`

```
cluster1::*> system cluster-switch log enable-collection
```

```
Do you want to enable cluster log collection for all nodes in the  
cluster?
```

```
{y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Die Ethernet-Switch-Integritätsüberwachung (CSHM) ist für die Sicherstellung des Betriebszustands von Cluster- und Speichernetzwerk-Switches und das Sammeln von Switch-Protokollen für Debugging-Zwecke verantwortlich. Dieses Verfahren führt Sie durch den Prozess der Einrichtung und Inbetriebnahme der Sammlung von detaillierten **Support**-Protokollen vom Switch und startet eine stündliche Erfassung von **periodischen** Daten, die von AutoSupport gesammelt werden.

Schritte

1. Führen Sie zum Einrichten der Protokollsammlung den folgenden Befehl für jeden Switch aus. Sie werden aufgefordert, den Switch-Namen, den Benutzernamen und das Kennwort für die Protokollerfassung einzugeben.

```
system switch ethernet log setup-password
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs1
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system switch ethernet log setup-password

Enter the switch name: cs2
Would you like to specify a user other than admin for log
collection? {y|n}: n

Enter the password: <enter switch password>
Enter the password again: <enter switch password>
```

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

```
system switch ethernet log modify -device <switch-name> -log-request true
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet log modify -device cs1 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

```
cluster1::*> system switch ethernet log modify -device cs2 -log  
-request true
```

```
Do you want to modify the cluster switch log collection  
configuration? {y|n}: [n] y
```

```
Enabling cluster switch log collection.
```

Warten Sie 10 Minuten, und überprüfen Sie dann, ob die Protokollsammlung abgeschlossen ist:

```
system switch ethernet log show
```



Wenn einer dieser Befehle einen Fehler zurückgibt oder die Protokollsammlung nicht abgeschlossen ist, wenden Sie sich an den NetApp Support.

Fehlerbehebung

Wenn einer der folgenden Fehlerzustände auftritt, die von der Protokollerfassungsfunktion gemeldet werden (sichtbar in der Ausgabe von `system switch ethernet log show`), versuchen Sie die entsprechenden Debug-Schritte:

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um Anweisungen zu erhalten.
ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.

Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

Gehen Sie wie folgt vor, um SNMPv3 zu konfigurieren, das die Statusüberwachung des Ethernet-Switches (CSHM) unterstützt.

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 92300YC-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

Mit dem folgenden Befehl wird ein SNMPv3-Benutzername auf der ONTAP-Seite konfiguriert:

```
cluster1::*> security login create -user-or-group-name SNMPv3_USER -application  
snmp -authentication-method usm -remote-switch-ipaddress ADDRESS
```

Mit dem folgenden Befehl wird der SNMPv3-Benutzername mit CSHM eingerichtet:

```
cluster1::*> system switch ethernet modify -device DEVICE -snmp-version SNMPv3  
-community-or-username SNMPv3_USER
```

Schritte

1. Richten Sie den SNMPv3-Benutzer auf dem Switch so ein, dass Authentifizierung und Verschlüsselung verwendet werden:

```
show snmp user
```


Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config)# show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv

```
(sw1) (Config)#
```

2. Richten Sie den SNMPv3-Benutzer auf der ONTAP-Seite ein:

```
security login create -user-or-group-name <username> -application snmp
-authentication-method usm -remote-switch-ipaddress 10.231.80.212
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

cluster1::*> security login create -user-or-group-name <username>
-application snmp -authentication-method usm -remote-switch
-ipaddress 10.231.80.212

Enter the authoritative entity's EngineID [remote EngineID]:

Which authentication protocol do you want to choose (none, md5, sha,
sha2-256)
[none]: md5

Enter the authentication protocol password (minimum 8 characters
long):

Enter the authentication protocol password again:

Which privacy protocol do you want to choose (none, des, aes128)
[none]: aes128

Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

3. Konfigurieren Sie CSHM für die Überwachung mit dem neuen SNMPv3-Benutzer:

```
system switch ethernet show-all -device "sw1" -instance
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C92300YC
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
cluster1::*> system switch ethernet modify -device "sw1" -snmp
-version SNMPv3 -community-or-username <username>
cluster1::*>
```

4. Stellen Sie sicher, dass die Seriennummer, die mit dem neu erstellten SNMPv3-Benutzer abgefragt werden soll, mit der im vorherigen Schritt nach Abschluss des CSHM-Abfragezeitraums enthaltenen identisch ist.

```
system switch ethernet polling-interval show
```

Beispiel anzeigen

```
cluster1::*> system switch ethernet polling-interval show
Polling Interval (in minutes): 5

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C92300YC
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Switches migrieren

Migrieren Sie zu einem Switch mit zwei Knoten und einem Cisco Nexus 92300YC Switch

Wenn Sie über eine bestehende Cluster-Umgebung mit zwei Nodes (*witched*) verfügen, können Sie mit Cisco Nexus 92300YC-Switches zu einer 2-Node_Switched_Cluster-Umgebung migrieren, um eine Skalierung über zwei Nodes im Cluster durchzuführen.

Die von Ihnen verwendete Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerk-Ports oder einen einzelnen Cluster-Port haben. Der dokumentierte Prozess funktioniert für alle Knoten mit optischen oder Twinax-Ports, wird aber auf diesem Switch nicht unterstützt, wenn Knoten integrierte 10-Gbit-BASE-T-RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

Die meisten Systeme benötigen an jedem Controller zwei dedizierte Cluster-Netzwerk-Ports.



Nach Abschluss der Migration müssen Sie möglicherweise die erforderliche Konfigurationsdatei installieren, um den Cluster Switch Health Monitor (CSHM) für 92300YC Cluster Switches zu unterstützen. Siehe ["Installieren Sie den Cluster Switch Health Monitor \(CSHM\)".](#)

Prüfen Sie die Anforderungen

Was Sie benötigen

Stellen Sie bei einer Konfiguration mit zwei Nodes ohne Switches Folgendes sicher:

- Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
- Auf den Knoten wird ONTAP 9.6 und höher ausgeführt.
- Alle Cluster-Ports haben den Status **up**.
- Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren Home-Ports.

Für die Switch-Konfiguration des Cisco Nexus 92300YC:

- Beide Switches verfügen über Management-Netzwerk-Konnektivität.
- Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
- Nexus 92300YC Node-to-Node-Switch und Switch-to-Switch-Verbindungen verwenden Twinax- oder Glasfaserkabel.

["Hardware Universe – Switches"](#) Enthält weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel werden an den Ports 1/65 und 1/66 an beiden 92300YC-Switches angeschlossen.
- Initiale Anpassung der beiden 92300YC-Switches wird abgeschlossen. So werden die:
 - 92300YC-Switches verwenden die neueste Version der Software
 - RCFs (Reference Configuration Files) werden auf die Switches angewendet. Auf den neuen Switches werden alle Site-Anpassungen wie SMTP, SNMP und SSH konfiguriert.

Migrieren Sie den Switch

Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der 92300YC-Switches lauten cs1 und cs2.
- Die Namen der Cluster SVMs sind node1 und node2.
- Die Namen der LIFs sind node1_clug1 und node1_clus2 auf Knoten 1, und node2_clus1 bzw. node2_clus2 auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e0a und e0b.

["Hardware Universe"](#) Enthält die neuesten Informationen über die tatsächlichen Cluster-Ports für Ihre Plattformen.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y` Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

2. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Beispiel anzeigen

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster1::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Schritt: Kabel und Ports konfigurieren

1. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches cs1 und cs2.

Sie dürfen die ISL-Ports nicht deaktivieren.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 64 auf Switch cs1 deaktiviert sind:

```
cs1# config  
Enter configuration commands, one per line. End with CNTL/Z.  
cs1(config)# interface e/1-64  
cs1(config-if-range)# shutdown
```

2. Stellen Sie sicher, dass ISL und die physischen Ports auf der ISL zwischen den beiden 92300YC-Switches cs1 und cs2 auf den Ports 1/65 und 1/66 vorhanden sind:

```
show port-channel summary
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports auf 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      Eth1/65 (P)  Eth1/66 (P)
```

+ das folgende Beispiel zeigt, dass die ISL-Ports auf Switch cs2 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      Eth1/65 (P)  Eth1/66 (P)
```

3. Liste der benachbarten Geräte anzeigen:

```
show cdp neighbors
```

Dieser Befehl enthält Informationen zu den Geräten, die mit dem System verbunden sind.

Beispiel anzeigen

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs1 aufgeführt:

```
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 Port ID	Local Intfrc	Hldtme	Capability	Platform
cs2 (FDO220329V5) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs2 (FDO220329V5) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 2

+ im folgenden Beispiel werden die benachbarten Geräte auf Switch cs2 aufgelistet:

+

```
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 Port ID	Local Intfrc	Hldtme	Capability	Platform
cs1 (FDO220329KU) Eth1/65	Eth1/65	177	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	177	R S I s	N9K-C92300YC

Total entries displayed: 2

4. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

```
network port show -ip space Cluster
```

Jeder Port sollte für angezeigt werden Link Und gesund für Health Status.

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Port	IPspace	Broadcast Domain	Link	MTU	Speed(Mbps) Admin/Oper	Health Status
e0a	Cluster	Cluster	up	9000	auto/10000	healthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy

Node: node2

Port	IPspace	Broadcast Domain	Link	MTU	Speed(Mbps) Admin/Oper	Health Status
e0a	Cluster	Cluster	up	9000	auto/10000	healthy
e0b	Cluster	Cluster	up	9000	auto/10000	healthy

4 entries were displayed.

5. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

```
network interface show -vserver Cluster
```

Jede LIF im Cluster sollte für „true“ anzeigen Is Home Und ich habe ein Status Admin/Oper Von up/Up

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. Vergewissern Sie sich, dass die automatische Umrüstung 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		
	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

7. Trennen Sie das Kabel vom Cluster Port e0a auf node1, und verbinden Sie dann e0a mit Port 1 auf Cluster Switch cs1, wobei die entsprechende Verkabelung verwendet wird, die von den 92300YC Switches

unterstützt wird.

Der "[Hardware Universe - Schalter](#)" Enthält weitere Informationen zur Verkabelung.

8. Trennen Sie das Kabel vom Cluster Port e0a auf node2, und verbinden Sie dann e0a mit Port 2 auf Cluster Switch cs1, unter Verwendung der entsprechenden Verkabelung, die von den 92300YC Switches unterstützt wird.
9. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/64 auf Switch cs1 aktiviert sind:

```
cs1# config  
Enter configuration commands, one per line. End with CNTL/Z.  
cs1(config)# interface e1/1-64  
cs1(config-if-range)# no shutdown
```

10. Vergewissern Sie sich, dass alle Cluster-LIFs bereit, funktionsfähig und als wahr angezeigt werden Is Home:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs sich auf node1 und node2 befinden und dass Is Home Die Ergebnisse sind wahr:

```
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.					

11. Informationen zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false
2 entries were displayed.			

12. Trennen Sie das Kabel von Cluster Port e0b auf node1, und verbinden Sie dann e0b mit Port 1 am Cluster

Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den 92300YC Switches unterstützt wird.

13. Trennen Sie das Kabel von Cluster Port e0b auf node2, und verbinden Sie dann e0b mit Port 2 am Cluster Switch cs2. Verwenden Sie dazu die geeignete Verkabelung, die von den 92300YC Switches unterstützt wird.
14. Aktivieren Sie alle Ports für Knoten auf Cluster-Switch cs2.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/64 auf Switch cs2 aktiviert sind:

```
cs2# config
Enter configuration commands, one per line. End with CNTL/Z.
cs2(config)# interface e1/1-64
cs2(config-if-range)# no shutdown
```

Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

```
network port show -ipspace Cluster
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

```
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.

2. Vergewissern Sie sich, dass alle Schnittstellen für „true“ anzeigen Is Home:

```
network interface show -vserver Cluster
```



Dies kann einige Minuten dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf node1 und node2 liegen und dass Is Home Die Ergebnisse sind wahr:

```
cluster1::*> network interface show -vserver Cluster
```

Current Is	Logical	Status	Network	Current	
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.

3. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
show cdp neighbors
```


Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
(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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	133	H	FAS2980
node2 e0a	Eth1/2	133	H	FAS2980
cs2 (FDO220329V5) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs2 (FDO220329V5) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	133	H	FAS2980
node2 e0b	Eth1/2	133	H	FAS2980
cs1 (FDO220329KU) Eth1/65	Eth1/65	175	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	175	R S I s	N9K-C92300YC

Total entries displayed: 4

4. Zeigen Sie Informationen zu den erkannten Netzwerkgeräten im Cluster an:

```
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-
C92300YC
           e0b    cs2                      0/2      N9K-
C92300YC
node1      /cdp
           e0a    cs1                      0/1      N9K-
C92300YC
           e0b    cs2                      0/1      N9K-
C92300YC

4 entries were displayed.
```

5. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

```
network options switchless-cluster show
```



Es kann einige Minuten dauern, bis der Befehl abgeschlossen ist. Warten Sie, bis die Ankündigung „3 Minuten Lebensdauer abläuft“ abläuft.

Beispiel anzeigen

Die falsche Ausgabe im folgenden Beispiel zeigt an, dass die Konfigurationseinstellungen deaktiviert sind:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

6. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
node1	true	true	false
node2	true	true	false

7. Vergewissern Sie sich, dass das Cluster-Netzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
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 169.254.47.194 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)

8. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Beispiel anzeigen

```
cluster1::*> system node autosupport invoke -node * -type all  
-message MAINT=END
```

9. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

10. Aktivieren Sie für ONTAP 9.4 und höher die Protokollerfassung der Cluster Switch-Systemzustandsüberwachung zum Erfassen von Switch-bezogenen Protokolldateien mithilfe der Befehle:

```
system cluster-switch log setup-password Und system cluster-switch log enable-  
collection
```

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Migrieren Sie von einem Cisco Switch zu einem Cisco Nexus 92300YC Switch

Sie können ältere Cisco Cluster Switches für einen ONTAP Cluster unterbrechungsfrei zu

Cisco Nexus 92300YC Cluster Network Switches migrieren.



Nach Abschluss der Migration müssen Sie möglicherweise die erforderliche Konfigurationsdatei installieren, um den Cluster Switch Health Monitor (CSHM) für 92300YC Cluster Switches zu unterstützen. Siehe "[Installieren Sie den Cluster Switch Health Monitor \(CSHM\)](#)".

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein vorhandenes Cluster mit vollem Funktionsumfang.
- 10-GbE- und 40-GbE-Konnektivität zwischen Nodes und Nexus 92300YC Cluster-Switches.
- Alle Cluster-Ports sind im Status up, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Korrekte Version von NX-OS und Referenzkonfigurationsdatei (RCF) auf den Nexus 92300YC Cluster Switches installiert.
- Ein redundantes und voll funktionsfähiges NetApp Cluster unter Verwendung beider älteren Cisco Switches.
- Management-Konnektivität und Konsolenzugriff auf die älteren Cisco Switches und die neuen Switches.
- Alle Cluster-LIFs im Status „up“ mit den Cluster-LIFs befinden sich auf den Home-Ports.
- ISL-Ports aktiviert und zwischen den älteren Cisco Switches und zwischen den neuen Switches verkabelt.

Migrieren Sie den Switch

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die vorhandenen Cisco Nexus 5596UP Cluster-Switches sind c1 und c2.
- Die neuen Nexus 92300YC Cluster Switches sind cs1 und cs2.
- Die Knoten sind node1 und node2.
- Die Cluster-LIFs sind node1_clut1 und node1_clus2 on Node 1, und node2_clus1 bzw. node2_clus2 on Node 2.
- Schalter c2 wird zuerst durch Schalter cs2 ersetzt und dann Schalter c1 durch Schalter cs1 ersetzt.
 - Ein temporäres ISL basiert auf cs1, das c1 mit cs1 verbindet.
 - Die Verkabelung zwischen den Knoten und c2 wird dann von c2 getrennt und wieder mit cs2 verbunden.
 - Die Verkabelung zwischen den Knoten und c1 wird dann von c1 getrennt und wieder mit cs1 verbunden.
 - Die temporäre ISL zwischen c1 und cs1 wird dann entfernt.

Für Verbindungen verwendete Ports

- Einige der Ports sind auf Nexus 92300YC Switches konfiguriert, um mit 10 GbE oder 40 GbE zu laufen.
- Die Cluster-Switches verwenden die folgenden Ports für Verbindungen zu den Nodes:
 - Ports e1/1-48 (10/25 GbE), e1/49-64 (40/100 GbE): Nexus 92300YC
 - Ports e1/1-40 (10 GbE): Nexus 5596UP
 - Ports e1/1-32 (10 GbE): Nexus 5020

- Ports e1/1-12, e2/1-6 (10 GbE): Nexus 5010 mit Erweiterungsmodul
- Bei den Cluster-Switches werden die folgenden Inter-Switch Link (ISL)-Ports verwendet:
 - Ports e1/65-66 (100 GbE): Nexus 92300YC
 - Ports e1/41-48 (10 GbE): Nexus 5596UP
 - Ports e1/33-40 (10 GbE): Nexus 5020
 - Ports e1/13-20 (10 GbE): Nexus 5010
- ["Hardware Universe – Switches"](#) Die enthält Informationen über die unterstützte Verkabelung aller Cluster Switches.
- Die in diesem Verfahren unterstützten ONTAP- und NX-OS-Versionen befinden sich auf dem ["Cisco Ethernet-Switches"](#) Seite.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in Erweitert, und geben Sie **y** ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

2. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

Wobei x die Dauer des Wartungsfensters in Stunden ist.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Beispiel anzeigen

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster1::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

3. Vergewissern Sie sich, dass die automatische Umrüstung 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
```

Vserver	Logical Interface	Auto-revert
Cluster	node1_clus1	true
	node1_clus2	true
	node2_clus1	true
	node2_clus2	true

4 entries were displayed.

4. Legen Sie den Administrations- oder Betriebsstatus für jede Cluster-Schnittstelle fest:

Jeder Port sollte für angezeigt werden Link Und gesund für Health Status.

a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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.

- b. Informationen zu den logischen Schnittstellen und den zugehörigen Home-Nodes anzeigen:

```
network interface show -vserver Cluster
```

Jedes LIF sollte für angezeigt werden Status Admin/Oper Und zwar für Is Home.

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.

5. Überprüfen Sie mithilfe des Befehls, ob die Cluster-Ports auf jedem Node mit vorhandenen Cluster-Switches auf folgende Weise (aus Sicht der Nodes) verbunden 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			

node2	/cdp		
	e0a	c1	0/2 N5K-
C5596UP			
	e0b	c2	0/2 N5K-
C5596UP			
node1	/cdp		
	e0a	c1	0/1 N5K-
C5596UP			
	e0b	c2	0/1 N5K-
C5596UP			

4 entries were displayed.

6. Überprüfen Sie mithilfe des Befehls, ob die Cluster-Ports und -Switches (aus Sicht der Switches) auf folgende Weise verbunden sind:

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0a	Eth1/1	124	H	FAS2750
node2 e0a	Eth1/2	124	H	FAS2750
c2 (FOX2025GEFC) Eth1/41	Eth1/41	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/42	Eth1/42	175	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/43	Eth1/43	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/44	Eth1/44	175	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/45	Eth1/45	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/46	Eth1/46	179	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/47	Eth1/47	175	S I s	N5K-C5596UP
c2 (FOX2025GEFC) Eth1/48	Eth1/48	179	S I s	N5K-C5596UP

Total entries displayed: 10

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	124	H	FAS2750
node2 e0b	Eth1/2	124	H	FAS2750
c1 (FOX2025GEEX) Eth1/41	Eth1/41	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/42	Eth1/42	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/43	Eth1/43	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/44	Eth1/44	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/45	Eth1/45	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/46	Eth1/46	175	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/47	Eth1/47	176	S I s	N5K-C5596UP
c1 (FOX2025GEEX) Eth1/48	Eth1/48	176	S I s	N5K-C5596UP

7. Überprüfen Sie mit dem Befehl, ob das Cluster-Netzwerk vollständig verbunden ist:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
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)
```

Schritt: Kabel und Ports konfigurieren

1. Konfigurieren Sie eine temporäre ISL an den CS1on-Ports e1/41-48 zwischen c1 und cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die neue ISL auf c1 und cs1 konfiguriert ist:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/41-48
cs1(config-if-range)# description temporary ISL between Nexus 5596UP
and Nexus 92300YC
cs1(config-if-range)# no lldp transmit
cs1(config-if-range)# no lldp receive
cs1(config-if-range)# switchport mode trunk
cs1(config-if-range)# no spanning-tree bpduguard enable
cs1(config-if-range)# channel-group 101 mode active
cs1(config-if-range)# exit
cs1(config)# interface port-channel 101
cs1(config-if)# switchport mode trunk
cs1(config-if)# spanning-tree port type network
cs1(config-if)# exit
cs1(config)# exit
```

2. Entfernen Sie ISL-Kabel von den Ports e1/41-48 von c2, und verbinden Sie die Kabel mit den Ports e1/41-48 an cs1.
3. Vergewissern Sie sich, dass die ISL-Ports und der Port-Channel betriebsbereit sind, die C1 und cs1 verbinden:

```
show port-channel summary
```


Beispiel anzeigen

Das folgende Beispiel zeigt, dass der Cisco show Port-Channel summary Befehl verwendet wird, um zu überprüfen, ob die ISL Ports auf c1 und cs1 funktionsfähig sind:

c1# **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      Eth1/41(P)  Eth1/42(P)  
Eth1/43(P)  
Eth1/44(P)  Eth1/45(P)  
Eth1/46(P)  
Eth1/47(P)  Eth1/48(P)
```

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      Eth1/65(P)  Eth1/66(P)  
101    Po101(SU)  Eth      LACP      Eth1/41(P)  Eth1/42(P)  
Eth1/43(P)  
Eth1/44(P)  Eth1/45(P)  
Eth1/46(P)  
Eth1/47(P)  Eth1/48(P)
```

4. Trennen Sie bei Node1 das Kabel von e1/1 auf c2, und schließen Sie das Kabel anschließend an e1/1 auf cs2 an. Verwenden Sie dazu die geeignete Verkabelung, die von Nexus 92300YC unterstützt wird.
5. Trennen Sie bei node2 das Kabel von e1/2 auf c2, und schließen Sie das Kabel anschließend an e1/2 auf cs2 an. Verwenden Sie dazu die geeignete Verkabelung, die von Nexus 92300YC unterstützt wird.
6. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

```
network device-discovery show -protocol cdp
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
```

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	c1	0/2	N5K-
C5596UP				
	e0b	cs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	c1	0/1	N5K-
C5596UP				
	e0b	cs2	0/1	N9K-
C92300YC				

4 entries were displayed.

7. Trennen Sie bei Node1 das Kabel von e1/1 auf c1, und schließen Sie das Kabel anschließend an e1/1 am cs1 an. Verwenden Sie dazu die geeignete Verkabelung, die von Nexus 92300YC unterstützt wird.
8. Trennen Sie bei node2 das Kabel von e1/2 auf c1, und verbinden Sie das Kabel mit e1/2 am cs1. Verwenden Sie dazu die geeignete Verkabelung, die von Nexus 92300YC unterstützt wird.
9. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

```
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
C92300YC			N9K-
	e0b	cs2	0/2
C92300YC			N9K-
node1	/cdp		
	e0a	cs1	0/1
C92300YC			N9K-
	e0b	cs2	0/1
C92300YC			N9K-

4 entries were displayed.

10. Löschen Sie die temporäre ISL zwischen cs1 und c1.

Beispiel anzeigen

```
cs1(config)# no interface port-channel 10
cs1(config)# interface e1/41-48
cs1(config-if-range)# lldp transmit
cs1(config-if-range)# lldp receive
cs1(config-if-range)# no switchport mode trunk
cs1(config-if-range)# no channel-group
cs1(config-if-range)# description 10GbE Node Port
cs1(config-if-range)# spanning-tree bpduguard enable
cs1(config-if-range)# exit
cs1(config)# exit
```

Schritt 3: Beenden Sie die Migration

1. Überprüfen der endgültigen Konfiguration des Clusters:

```
network port show -ip space Cluster
```

Jeder Port sollte für angezeigt werden Link Und gesund für Health Status.

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
```

Node: node1

Ignore

						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

Ignore

						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.

```
cluster1::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Cluster	node1_clus1	up/up	169.254.209.69/16	node1

```

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/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
node2	/cdp			
	e0a	cs1	0/2	N9K-
C92300YC				
	e0b	cs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C92300YC				
	e0b	cs2	0/1	N9K-
C92300YC				

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1	Eth1/1	124	H	FAS2750
e0a				
node2	Eth1/2	124	H	FAS2750
e0a				
cs2 (FD0220329V5)	Eth1/65	179	R S I s	N9K-C92300YC
Eth1/65				

```
cs2(FDO220329V5)    Eth1/66    179    R S I s    N9K-C92300YC
Eth1/66
```

```
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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	124	H	FAS2750
node2 e0b	Eth1/2	124	H	FAS2750
cs1(FDO220329KU) Eth1/65	Eth1/65	179	R S I s	N9K-C92300YC
cs1(FDO220329KU) Eth1/66	Eth1/66	179	R S I s	N9K-C92300YC

Total entries displayed: 4

2. Vergewissern Sie sich, dass das Cluster-Netzwerk über vollständige Konnektivität verfügt:

```
cluster ping-cluster -node node-name
```

Beispiel anzeigen

```
cluster1::*> set -priv advanced
```

Warning: These advanced commands are potentially dangerous; use them only when

directed to do so by NetApp personnel.

Do you want to continue? {y|n}: **y**

```
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)

```
cluster1::*> set -privilege admin
```

```
cluster1::*>
```

3. Aktivieren Sie für ONTAP 9.4 und höher die Protokollerfassung der Cluster Switch-Systemzustandsüberwachung zum Erfassen von Switch-bezogenen Protokolldateien mithilfe der Befehle:

```
system cluster-switch log setup-password Und system cluster-switch log enable-collection
```


Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Tauschen Sie die Schalter aus

Ersetzen Sie einen Cisco Nexus 92300YC-Switch

Der Austausch eines defekten Nexus 92300YC Switches in einem Cluster-Netzwerk ist eine unterbrechungsfreie Prozedur (NDU).

Prüfen Sie die Anforderungen

Was Sie benötigen

Stellen Sie vor dem Austausch des Switches Folgendes sicher:

- In dem vorhandenen Cluster und der Netzwerkinfrastruktur:
 - Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
 - Alle Cluster-Ports sind aktiv.
 - Alle logischen Cluster-Schnittstellen (LIFs) laufen und auf ihren Home-Ports.
 - Der ONTAP-Cluster ping-Cluster -Node node1 Befehl muss angeben, dass die grundlegende Konnektivität und die PMTU-Kommunikation auf allen Pfaden erfolgreich sind.
- Für den Nexus 92300YC-Ersatzschalter:
 - Die Konnektivität des Managementnetzwerks am Ersatz-Switch funktioniert.
 - Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
 - Die Node-Verbindungen sind Ports 1/1 bis 1/64.
 - Alle Inter-Switch Link (ISL)-Ports sind an den Ports 1/65 und 1/66 deaktiviert.
 - Die gewünschte Referenzkonfigurationsdatei (RCF) und der NX-OS-Bildschalter werden auf den Switch geladen.
 - Die anfängliche Anpassung des Switches ist abgeschlossen, wie in beschrieben: ["Konfigurieren Sie den Cisco Nexus 92300YC-Switch"](#).

Alle zuvor erstellten Site-Anpassungen wie STP, SNMP und SSH werden auf den neuen Switch kopiert.

Tauschen Sie den Schalter aus

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die Namen der vorhandenen Nexus 92300YC Switches sind cs1 und cs2.
- Der Name des neuen Nexus 92300YC Switches lautet newc2.
- Die Node-Namen sind node1 und node2.
- Die Cluster-Ports auf jedem Node lauten e0a und e0b.
- Die Cluster-LIF-Namen sind node1_clug1 und node1_clus2 für node1, und node2_clus1 und node2_clus2 für node2.
- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet cluster1:*>

Über diese Aufgabe

Sie müssen den Befehl zum Migrieren einer Cluster-LIF von dem Node ausführen, auf dem die Cluster-LIF gehostet wird.

Die folgende Vorgehensweise basiert auf der folgenden Cluster-Netzwerktopologie:

Topologie 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-	
C92300YC					
	e0b	cs2	Eth1/2	N9K-	
C92300YC					
node1	/cdp				
	e0a	cs1	Eth1/1	N9K-	
C92300YC					
	e0b	cs2	Eth1/1	N9K-	
C92300YC					

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 (FD0220329V5)	Eth1/65	176	R S I s	N9K-C92300YC	
Eth1/65					
cs2 (FD0220329V5)	Eth1/66	176	R S I s	N9K-C92300YC	
Eth1/66					

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 ID	Local Intrfce	Hldtme	Capability	Platform	Port
node1	Eth1/1	139	H	FAS2980	e0b
node2	Eth1/2	124	H	FAS2980	e0b
cs1 (FDO220329KU)	Eth1/65	178	R S I s	N9K-C92300YC	
Eth1/65					
cs1 (FDO220329KU)	Eth1/66	178	R S I s	N9K-C92300YC	
Eth1/66					

Total entries displayed: 4

Schritt 1: Vorbereitung auf den Austausch

1. Installieren Sie das entsprechende RCF und Image auf dem Switch, newcs2, und nehmen Sie die erforderlichen Standortvorbereitungen vor.

Überprüfen, 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 für die RCF- und NX-OS-Software benötigen, fahren Sie mit Schritt 2 fort.

- a. Wechseln Sie auf der NetApp Support Site zur Referenzkonfigurationsdatei *Seite* der Referenzkonfiguration für NetApp Cluster und Management-Netzwerk-Switches.
 - b. Klicken Sie auf den Link für die Kompatibilitätsmatrix *Cluster Network and Management Network*, und notieren Sie anschließend die erforderliche Switch-Softwareversion.
 - c. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur Seite **Beschreibung** zurückzukehren, klicken Sie auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und gehen Sie dann zur Seite **Download**.
 - d. Befolgen Sie die Schritte auf der Download-Seite, um die korrekten RCF- und NX-OS-Dateien für die Version der installierten ONTAP-Software herunterzuladen.
2. Bei dem neuen Switch melden Sie sich als Administrator an und fahren Sie alle Ports ab, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports 1/1 zu 1/64).

Wenn der Schalter, den Sie ersetzen, nicht funktionsfähig ist und ausgeschaltet ist, fahren Sie mit Schritt 4 fort. Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt haben.

Beispiel anzeigen

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

3. Vergewissern Sie sich, dass für alle Cluster-LIFs die automatische Zurücksetzung 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.
```

4. Vergewissern Sie sich, dass alle Cluster-LIFs kommunizieren können:

```
cluster ping-cluster
```

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster node1

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: Kabel und Ports konfigurieren

1. Fahren Sie die ISL-Ports 1/65 und 1/66 auf dem Nexus 92300YC-Switch cs1 herunter:

Beispiel anzeigen

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/65-66
cs1(config-if-range)# shutdown
cs1(config-if-range)#
```

2. Entfernen Sie alle Kabel vom Nexus 92300YC cs2 Switch, und verbinden Sie sie dann mit den gleichen Ports auf dem Nexus 92300YC newc2 Switch.

3. Bringen Sie die ISLs-Ports 1/65 und 1/66 zwischen den switches cs1 und newcs2 auf, und überprüfen Sie dann den Betriebsstatus des Port-Kanals.

Port-Channel sollte PO1(SU) angeben und Mitgliedsports sollten eth1/65(P) und eth1/66(P) angeben.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/65 und 1/66 und zeigt die Zusammenfassung des Port-Kanals am Switch cs1 an:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
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      Eth1/65 (P)  Eth1/66 (P)

cs1(config-if-range)#
```

4. Vergewissern Sie sich, dass Port e0b auf allen Nodes aktiviert ist:

```
network port show ipspace Cluster
```

Beispiel anzeigen

Die Ausgabe sollte 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. Setzen Sie auf demselben Node, den Sie im vorherigen Schritt verwendet haben, die Cluster-LIF, die dem Port im vorherigen Schritt zugeordnet ist, mithilfe des Befehls „Netzwerkschnittstelle revert“ zurück.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert für „Home“ wahr ist und der Port e0b ist.

Die folgenden Befehle geben LIF zurück node1_clus2 Ein node1 Zu Home Port e0a Und zeigt Informationen zu den LIFs auf beiden Nodes an. Das Einrichten des ersten Node ist erfolgreich, wenn die Spalte IS Home für beide Clusterschnittstellen wahr ist und in diesem Beispiel die korrekten Port-Zuweisungen angezeigt werden e0a Und e0b Auf Knoten 1.

```
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. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

```
cluster1::*> cluster show
```

Node	Health	Eligibility
-----	-----	-----
node1	false	true
node2	true	true

7. Vergewissern Sie sich, dass 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.
```

Schritt 3: Führen Sie den Vorgang durch

1. Vergewissern Sie sich, dass alle Cluster-LIFs kommunizieren können:

```
cluster ping-cluster
```

Beispiel anzeigen

```
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 169.254.47.194 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)
```

2. Bestätigen Sie die folgende Clusternetzwerkconfiguration:

```
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-
C92300YC				
	e0b	newcs2	0/2	N9K-
C92300YC				
node1	/cdp			
	e0a	cs1	0/1	N9K-
C92300YC				
	e0b	newcs2	0/1	N9K-
C92300YC				

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 (FDO296348FU)	Eth1/65	176	R S I s	N9K-C92300YC
Eth1/65				
newcs2 (FDO296348FU)	Eth1/66	176	R S I s	N9K-C92300YC

Eth1/66

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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e0b	Eth1/1	139	H	FAS2980
node2 e0b	Eth1/2	124	H	FAS2980
cs1 (FDO220329KU) Eth1/65	Eth1/65	178	R S I s	N9K-C92300YC
cs1 (FDO220329KU) Eth1/66	Eth1/66	178	R S I s	N9K-C92300YC

Total entries displayed: 4

3. Aktivieren Sie für ONTAP 9.4 und höher die Protokollerfassung des Cluster Switch Health Monitor zur Erfassung von Switch-bezogenen Protokolldateien mithilfe von gthe Commamnds:

system cluster-switch log setup-password Und system cluster-switch log enable-collection

Beispiel anzeigen

```
cluster1::*> system cluster-switch log setup-password
Enter the switch name: <return>
The switch name entered is not recognized.
Choose from the following list:
cs1
cs2

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs1
RSA key fingerprint is
e5:8b:c6:dc:e2:18:18:09:36:63:d9:63:dd:03:d9:cc
Do you want to continue? {y|n}::[n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log setup-password

Enter the switch name: cs2
RSA key fingerprint is
57:49:86:a1:b9:80:6a:61:9a:86:8e:3c:e3:b7:1f:b1
Do you want to continue? {y|n}:: [n] y

Enter the password: <enter switch password>
Enter the password again: <enter switch password>

cluster1::*> system cluster-switch log enable-collection

Do you want to enable cluster log collection for all nodes in the
cluster?
{y|n}: [n] y

Enabling cluster switch log collection.

cluster1::*>
```



Wenn einer dieser Befehle einen Fehler sendet, wenden Sie sich an den NetApp Support.

Austausch von Cisco Nexus 92300YC Cluster Switches durch Verbindungen ohne Switches

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren,

mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

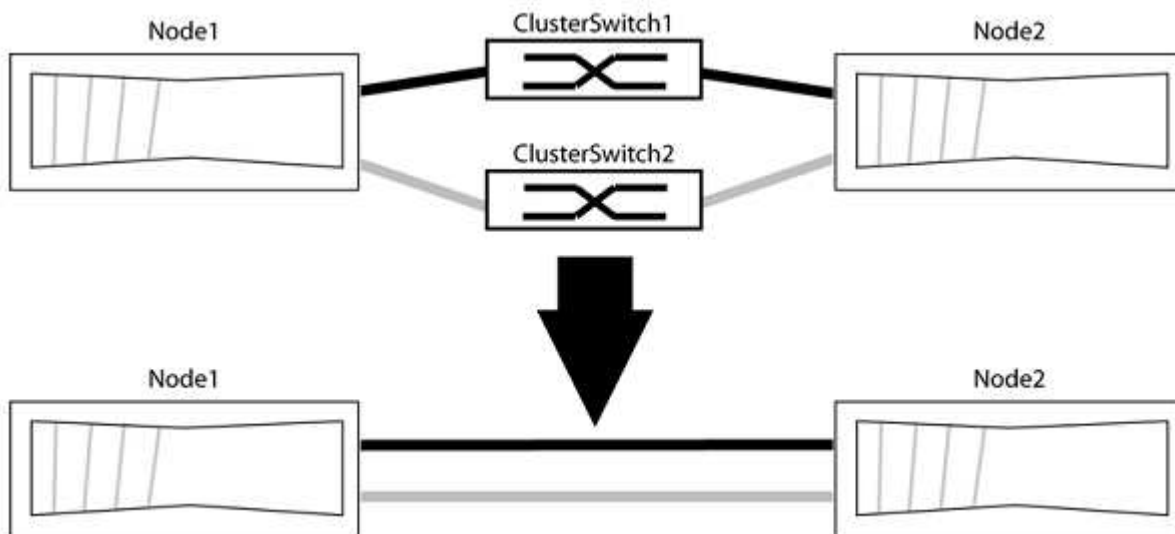
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Angezeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Schritt: Ports und Verkabelung konfigurieren

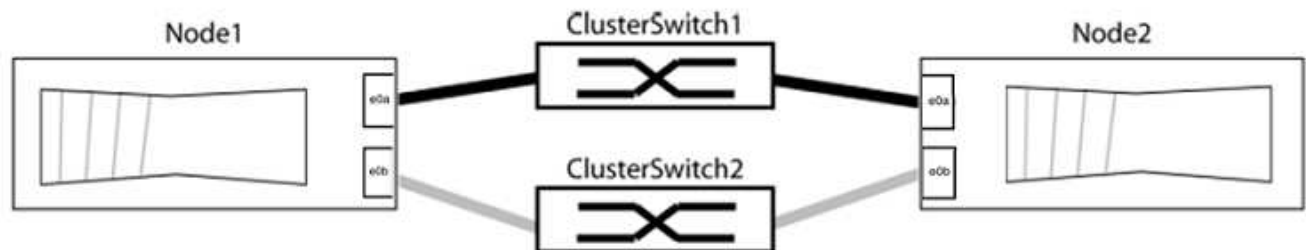
1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in `grp1` zu Cluster-Switch 1 wechseln und die Cluster-Ports in `grp2` zu Cluster-Switch 2 wechseln. Diese Gruppen sind

später im Verfahren erforderlich.

2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



Überprüfen Sie, ob die Ports einen Wert von `up` für die Spalte „Link“ und einen Wert von `healthy` für die Spalte „Integritätsstatus“.

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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

```
network interface revert -vserver Cluster -lif *
```

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

```
network device-discovery show -port cluster_port
```

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

7. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

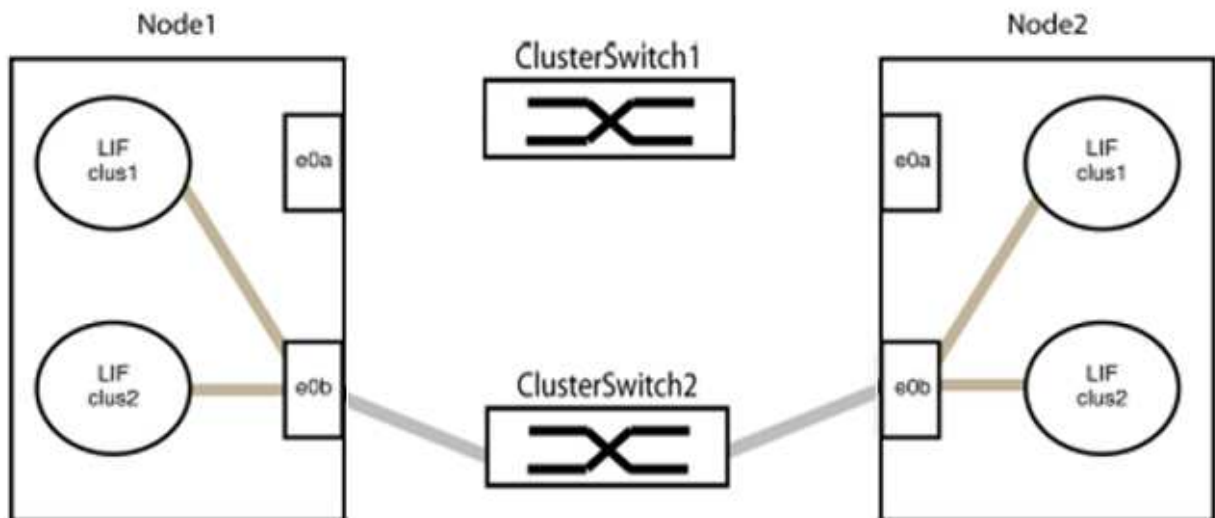
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

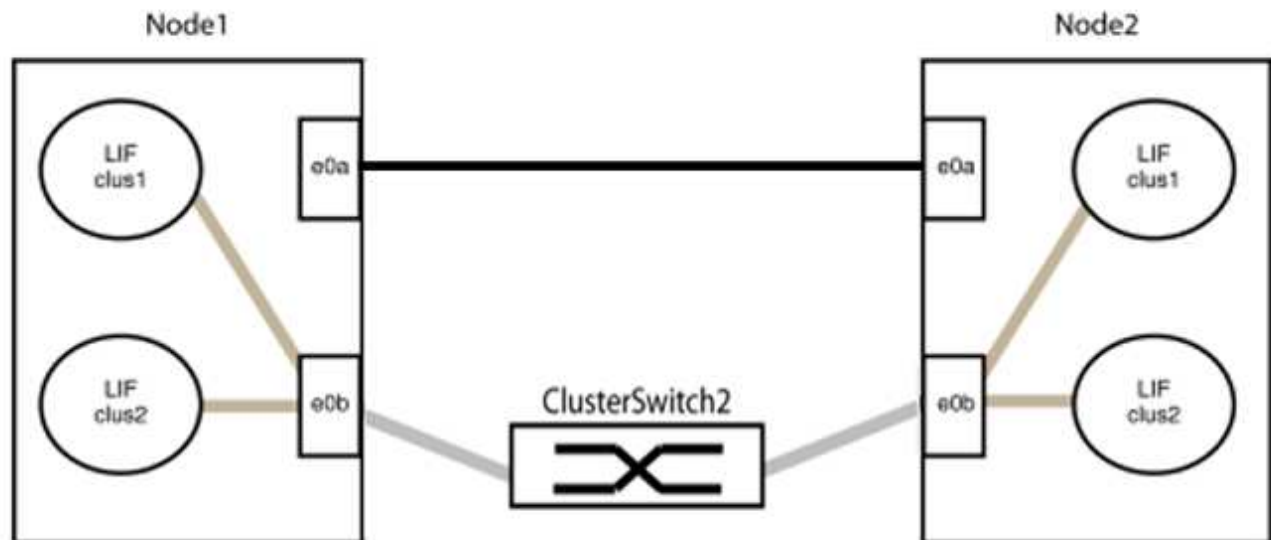
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

```
network options switchless-cluster show
```

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:

```
cluster ping-cluster -node local
```



Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung für Gruppe 1 zu bestätigen.

11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von `groerp2` trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in `Groupp2` ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

```
network device-discovery show -port cluster_port
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

```
network interface show -vserver Cluster -lif lif_name
```

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true        false  
node2 true    true        false  
2 entries were displayed.
```

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

NetApp CN1610

Überblick über die Installation und Konfiguration der NetApp CN1610 Switches

Beim CN1610 handelt es sich um einen Managed Layer 2 Switch mit hoher Bandbreite, der über 16 10-Gigabit SFP+ (Small Form-Factor Pluggable Plus)-Ports verfügt.

Der Switch umfasst redundante Netzteile und Lüftereinschübe, die Hot Swapping für hohe Verfügbarkeit unterstützen. Dieser 1-HE-Switch kann in einem standardmäßigen 19 NetApp 42U-Systemschrank oder Schrank von Drittanbietern installiert werden.

Der Switch unterstützt die lokale Verwaltung über den Konsolen-Port oder die Remote-Verwaltung über eine Netzwerkverbindung mit Telnet oder SSH. Die CN1610 umfasst einen dedizierten 1-Gigabit Ethernet RJ45 Management-Port für Out-of-Band-Switch-Management. Sie können den Switch verwalten, indem Sie Befehle in die Befehlszeilenschnittstelle (CLI) eingeben oder über ein SNMP-basiertes Netzwerk-Management System (NMS).

Workflow für NetApp CN1610-Switches installieren und konfigurieren

Gehen Sie wie folgt vor, um einen NetApp CN1610 Switch auf Systemen mit ONTAP zu installieren und zu konfigurieren:

1. ["Hardware installieren"](#)
2. ["INSTALLIEREN Sie DIE FASTPATH Software"](#)
3. ["Installieren Sie die Referenzkonfigurationsdatei"](#)

Wenn auf den Switches ONTAP 8.3.1 oder höher ausgeführt wird, befolgen Sie die Anweisungen unter ["INSTALLIEREN SIE FASTPATH und RCFs auf Switches mit ONTAP 8.3.1 und höher."](#)

4. ["Konfigurieren Sie den Switch"](#)

Dokumentationsanforderungen für NetApp CN1610-Switches

Überprüfen Sie bei der Installation und Wartung von NetApp CN1610 Switches alle empfohlenen Dokumente.

Dokumenttitel	Beschreibung
"1G Installationshandbuch"	Ein Überblick über die Hardware- und Softwarefunktionen und den Installationsprozess des CN1601 Switch.
"10G-Installationsanleitung"	Ein Überblick über die Hardware- und Softwarefunktionen für CN1610 Switches und beschreibt die Funktionen für die Installation des Switches und den Zugriff auf die CLI.

Dokumenttitel	Beschreibung
"Installations- und Konfigurationshandbuch für CN1601 und CN1610-Switch"	Hier erfahren Sie, wie Sie die Switch-Hardware und -Software für Ihre Cluster-Umgebung konfigurieren.
Administratorhandbuch für den CN1601-Switch	<p>Enthält Beispiele für die Verwendung des CN1601-Switches in einem typischen Netzwerk.</p> <ul style="list-style-type: none"> • "Administratorhandbuch" • "Administratorhandbuch, Version 1.1.x.x" • "Administratorhandbuch, Version 1.2.x.x"
CN1610 Network Switch CLI Command Reference	<p>Enthält detaillierte Informationen zu den CLI-Befehlen (Command-Line Interface), mit denen Sie die CN1601-Software konfigurieren.</p> <ul style="list-style-type: none"> • "Befehlsreferenz" • "Befehlsreferenz, Version 1.1.x.x" • "Befehlsreferenz, Version 1.2.x.x"

Installieren und konfigurieren

Installieren Sie die Hardware für den NetApp CN1610 Switch

Verwenden Sie zur Installation der NetApp CN1610 Switch-Hardware die Anweisungen in einem der folgenden Leitfäden.

- ["1G Installationshandbuch"](#).

Ein Überblick über die Hardware- und Softwarefunktionen und den Installationsprozess des CN1601 Switch.

- ["10G-Installationsanleitung"](#)

Ein Überblick über die Hardware- und Softwarefunktionen für CN1610 Switches und beschreibt die Funktionen für die Installation des Switches und den Zugriff auf die CLI.

INSTALLIEREN Sie DIE FASTPATH Software

Wenn Sie die FASTPATH Software auf Ihren NetApp Switches installieren, müssen Sie das Upgrade mit dem zweiten Switch cs2 beginnen.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen und keine fehlerhaften Cluster Network Interface Cards (NICs) oder ähnlichen Problemen).

- Voll funktionsfähige Portverbindungen am Cluster-Switch.
- Es sind alle Cluster-Ports eingerichtet.
- Einrichtung aller logischen Cluster-Schnittstellen (LIFs) (darf nicht migriert worden sein)
- Ein erfolgreicher Kommunikationspfad: Der ONTAP (Privilege: Erweitert) `cluster ping-cluster -node node1` Der Befehl muss das angeben `larger than PMTU communication` Ist auf allen Pfaden erfolgreich.
- Eine unterstützte Version von FASTPATH und ONTAP.

Beachten Sie unbedingt die Kompatibilitätstabelle für Switches auf der ["NetApp CN1601 und CN1610 Switches"](#) Seite für die unterstützten FASTPATH und ONTAP Versionen.

INSTALLIEREN Sie FASTPATH

Im folgenden Verfahren wird die Syntax „Clustered Data ONTAP 8.2“ verwendet. Aus diesem Grund unterscheiden sich der Cluster-Vserver, LIF-Namen und die CLI-Ausgabe von denen in Data ONTAP 8.3.

Zwischen der Befehlssyntax für „RCF“ und „FASTPATH“-Versionen kann eine Befehlssyntax bestehen.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die beiden NetApp-Switches sind cs1 und cs2.
- Die beiden Cluster LIFs sind „Schlussfolgerungen 1“ und „schluss2“.
- Die Vserver sind vs1 und vs2.
- Der `cluster::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Node lauten e1a und e2a.

["Hardware Universe"](#) Bietet weitere Informationen zu den tatsächlichen, auf Ihrer Plattform unterstützten Cluster-Ports.

- Die unterstützten Inter-Switch Links (ISLs) sind die Ports 0/13 bis 0/16.
- Die unterstützten Node-Verbindungen sind die Ports 0/1 bis 0/12.

Schritt 1: Migration des Clusters

1. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

2. Melden Sie sich als Administrator beim Switch an. Standardmäßig ist kein Passwort vorhanden. Am (cs2) # Geben Sie die ein `enable` Befehl. Auch hier gibt es standardmäßig kein Passwort. Dadurch haben Sie Zugriff auf den privilegierten EXEC-Modus, mit dem Sie die Netzwerkschnittstelle konfigurieren können.

Beispiel anzeigen

```
(cs2) # enable
Password (Enter)
(cs2) #
```

3. Migrieren Sie auf der Konsole jedes Knotens Fazit 2 zu Port e1a:

```
network interface migrate
```

Beispiel anzeigen

```
cluster::*> network interface migrate -vserver vs1 -lif clus2
-destnode node1 -dest-port e1a
cluster::*> network interface migrate -vserver vs2 -lif clus2
-destnode node2 -dest-port e1a
```

4. Vergewissern Sie sich an der Konsole jedes Node, dass die Migration stattgefunden hat:

```
network interface show
```

Das folgende Beispiel zeigt, dass Faclu2 auf beiden Knoten zu Port e1a migriert hat:

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
```

Vserver	Logical Interface	Status Admin/Open	Network Address/Mask	Current Node	Current Port	Is Home
vs1						
	clus1	up/up	10.10.10.1/16	node1	e1a	true
	clus2	up/up	10.10.10.2/16	node1	e1a	
false						
vs2						
	clus1	up/up	10.10.10.1/16	node2	e1a	true
	clus2	up/up	10.10.10.2/16	node2	e1a	
false						

Schritt: FASTPATH Software installieren

1. Fahren Sie Cluster-Port e2a auf beiden Nodes herunter:


```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e2a auf beiden Nodes heruntergefahren wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin  
false  
cluster::*> network port modify -node node2 -port e2a -up-admin  
false
```

2. Vergewissern Sie sich, dass Port e2a auf beiden Knoten heruntergefahren wird:

```
network port show
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
-----	----	-----	----	-----	-----	-----	-----

node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

3. Fahren Sie die Inter-Switch Link (ISL)-Ports auf cs1, den aktiven NetApp Switch, herunter:

Beispiel anzeigen

```
(cs1) # configure  
(cs1)(config) # interface 0/13-0/16  
(cs1)(Interface 0/13-0/16) # shutdown  
(cs1)(Interface 0/13-0/16) # exit  
(cs1)(config) # exit
```

4. Sichern Sie das aktuelle aktive Bild auf cs2.

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions .

  active:
  backup:

Images currently available on Flash

-----
--
  unit          active      backup      current-active      next-
active
-----
--

      1          1.1.0.3      1.1.0.1          1.1.0.3              1.1.0.3

(cs2) # copy active backup
Copying active to backup
Copy operation successful

(cs2) #
```

5. Laden Sie die Bilddatei auf den Switch herunter.

Durch Kopieren der Bilddatei auf das aktive Bild wird beim Neustart die laufende FASTPATH-Version erstellt. Das vorherige Bild bleibt als Backup verfügbar.

Beispiel anzeigen

```
(cs2) # copy tftp://10.0.0.1/NetApp_CN1610_1.1.0.5.stk active

Mode..... TFTP
Set Server IP..... 10.0.0.1
Path..... ./
Filename..... NetApp_CN1610_1.1.0.5.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
TFTP Code transfer starting...

File transfer operation completed successfully.
```

6. Überprüfen Sie die laufende Version der FASTPATH-Software.

```
show version
```

Beispiel anzeigen

```
(cs2) # show version
```

```
Switch: 1
```

```
System Description..... Broadcom Scorpion 56820
                           Development System - 16 TENGIG,
                           1.1.0.3, Linux 2.6.21.7
Machine Type.....       Broadcom Scorpion 56820
                           Development System - 16TENGIG
Machine Model.....       BCM-56820
Serial Number.....       10611100004
FRU Number.....
Part Number.....         BCM56820
Maintenance Level.....   A
Manufacturer.....        0xbc00
Burned In MAC Address..... 00:A0:98:4B:A9:AA
Software Version.....    1.1.0.3
Operating System.....    Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Additional Packages.....  FASTPATH QOS
                           FASTPATH IPv6 Management
```

7. Zeigen Sie die Boot-Images für die aktive und die Backup-Konfiguration an.

```
show bootvar
```

Beispiel anzeigen

```
(cs2) # show bootvar

Image Descriptions

  active :
  backup :

  Images currently available on Flash

-----
--
  unit          active      backup      current-active      next-
active
-----
--

      1          1.1.0.3      1.1.0.3          1.1.0.3          1.1.0.5
```

8. Starten Sie den Switch neu.

reload

Beispiel anzeigen

```
(cs2) # reload

Are you sure you would like to reset the system? (y/n)  y

System will now restart!
```

Schritt 3: Installation validieren

1. Melden Sie sich erneut an und überprüfen Sie die neue Version der FASTPATH Software.

show version

Beispiel anzeigen

```
(cs2) # show version

Switch: 1

System Description..... Broadcom Scorpion 56820
                          Development System - 16
TENGIG,
                          1.1.0.5, Linux 2.6.21.7
Machine Type.....      Broadcom Scorpion 56820
                          Development System - 16TENGIG
Machine Model.....      BCM-56820
Serial Number.....      10611100004
FRU Number.....
Part Number.....        BCM56820
Maintenance Level.....  A
Manufacturer.....       0xbc00
Burned In MAC Address... 00:A0:98:4B:A9:AA
Software Version.....    1.1.0.5
Operating System.....    Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Additional Packages.....  FASTPATH QOS
                          FASTPATH IPv6 Management
```

2. ISL-Ports an cs1, dem aktiven Switch, herauf.

```
configure
```

Beispiel anzeigen

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (Interface 0/13-0/16) # no shutdown
(cs1) (Interface 0/13-0/16) # exit
(cs1) (config) # exit
```

3. Vergewissern Sie sich, dass die ISLs betriebsbereit sind:

```
show port-channel 3/1
```

Das Feld „Verbindungsstatus“ sollte angezeigt werden Up.

Beispiel anzeigen

```
(cs2) # show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports   Timeout      Speed     Active
-----
0/13    actor/long      10G Full  True
        partner/long
0/14    actor/long      10G Full  True
        partner/long
0/15    actor/long      10G Full  True
        partner/long
0/16    actor/long      10G Full  True
        partner/long
```

4. Kopieren Sie die running-config Datei in der startup-config Datei, wenn Sie mit den Software-Versionen und Switch-Einstellungen zufrieden sind.

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. Aktivieren Sie den zweiten Cluster-Port e2a auf jedem Node:

```
network port modify
```

Beispiel anzeigen

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> **network port modify -node node2 -port e2a -up-admin
true**
```

6. Fazit 2 zurücksetzen, der Port e2a zugeordnet ist:

```
network interface revert
```

Das LIF ist möglicherweise automatisch zurückgesetzt, je nach Ihrer Version der ONTAP Software.

Beispiel anzeigen

```
cluster::*> network interface revert -vserver Cluster -lif n1_clus2
cluster::*> network interface revert -vserver Cluster -lif n2_clus2
```

7. Vergewissern Sie sich, dass das LIF jetzt die Startseite ist (`true`) Auf beiden Knoten:

```
network interface show -role cluster
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	----
vs1						
	clus1	up/up	10.10.10.1/24	node1	e1a	true
	clus2	up/up	10.10.10.2/24	node1	e2a	true
vs2						
	clus1	up/up	10.10.10.1/24	node2	e1a	true
	clus2	up/up	10.10.10.2/24	node2	e2a	true

8. Status der Nodes anzeigen:

```
cluster show
```


Beispiel anzeigen

```
cluster::> cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

9. Wiederholen Sie die vorherigen Schritte, um DIE FASTPATH-Software auf dem anderen Switch, cs1, zu installieren.
10. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Installieren Sie eine Referenzkonfigurationsdatei auf einem CN1610-Switch

Gehen Sie folgendermaßen vor, um eine RCF (Reference Configuration File) zu installieren.

Vor dem Installieren eines RCF müssen Sie zuerst die Cluster-LIFs vom Switch cs2 weg migrieren. Nachdem die RCF installiert und validiert wurde, können die LIFs zurück migriert werden.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen und keine fehlerhaften Cluster Network Interface Cards (NICs) oder ähnlichen Problemen).
- Voll funktionsfähige Portverbindungen am Cluster-Switch.
- Es sind alle Cluster-Ports eingerichtet.
- Einrichtung aller logischen Cluster-Schnittstellen (LIFs)
- Ein erfolgreicher Kommunikationspfad: Der ONTAP (Privilege: Erweitert) `cluster ping-cluster -node node1` Der Befehl muss das angeben `larger than PMTU communication` Ist auf allen Pfaden erfolgreich.
- Eine unterstützte Version von RCF und ONTAP.

Beachten Sie unbedingt die Kompatibilitätstabelle für Switches auf der ["NetApp CN1601 und CN1610 Switches"](#) Seite für die unterstützten RCF- und ONTAP-Versionen.

Installieren Sie das RCF

Im folgenden Verfahren wird die Syntax „Clustered Data ONTAP 8.2“ verwendet. Aus diesem Grund unterscheiden sich der Cluster-Vserver, LIF-Namen und die CLI-Ausgabe von denen in Data ONTAP 8.3.

Zwischen der Befehlssyntax für „RCF“ und „FASTPATH“-Versionen kann eine Befehlssyntax bestehen.



In RCF Version 1.2 wurde die Unterstützung für Telnet explizit aufgrund von Sicherheitsbedenken deaktiviert. Um Verbindungsprobleme bei der Installation von RCF 1.2 zu vermeiden, vergewissern Sie sich, dass Secure Shell (SSH) aktiviert ist. Der ["Administratorleitfaden für den NetApp CN1610 Switch"](#) hat weitere Informationen über SSH.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die beiden NetApp-Switches sind cs1 und cs2.
- Die beiden Cluster LIFs sind „Schlussfolgerungen 1“ und „schluss2“.
- Die Vserver sind vs1 und vs2.
- Der `cluster: :*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Node lauten e1a und e2a.

["Hardware Universe"](#) Bietet weitere Informationen zu den tatsächlichen, auf Ihrer Plattform unterstützten Cluster-Ports.

- Die unterstützten Inter-Switch Links (ISLs) sind die Ports 0/13 bis 0/16.
- Die unterstützten Node-Verbindungen sind die Ports 0/1 bis 0/12.
- Eine unterstützte Version von FASTPATH, RCF und ONTAP.

Beachten Sie unbedingt die Kompatibilitätstabelle für Switches auf der ["NetApp CN1601 und CN1610 Switches"](#) Seite für die unterstützten FASTPATH-, RCF- und ONTAP-Versionen.

Schritt 1: Migration des Clusters

1. Aktuelle Switch-Konfigurationsinformationen speichern:

```
write memory
```

Beispiel anzeigen

Das folgende Beispiel zeigt die aktuelle Switch-Konfiguration, die in der Startkonfiguration gespeichert wird (`startup-config`) Datei auf Schalter cs2:

```
(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!
```

2. Migrieren Sie auf der Konsole jedes Knotens Fazit 2 zu Port e1a:

```
network interface migrate
```

Beispiel anzeigen

```
cluster::~*> network interface migrate -vserver vs1 -lif clus2
-source-node node1 -destnode node1 -dest-port e1a

cluster::~*> network interface migrate -vserver vs2 -lif clus2
-source-node node2 -destnode node2 -dest-port e1a
```

3. Vergewissern Sie sich an der Konsole jedes Node, dass die Migration aufgetreten ist:

```
network interface show -role cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Faclu2 auf beiden Knoten zu Port e1a migriert hat:

```
cluster::~*> network port show -role cluster
      clus1      up/up      10.10.10.1/16      node2      e1a      true
      clus2      up/up      10.10.10.2/16      node2      e1a
false
```

4. Fahren Sie den Port e2a auf beiden Knoten herunter:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e2a auf beiden Nodes heruntergefahren wird:

```
cluster::~*> network port modify -node node1 -port e2a -up-admin
false
cluster::~*> network port modify -node node2 -port e2a -up-admin
false
```

5. Vergewissern Sie sich, dass Port e2a auf beiden Knoten heruntergefahren wird:

```
network port show
```

Beispiel anzeigen

```
cluster::*> network port show -role cluster
```

(Mbps)					Auto-Negot	Duplex	Speed
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	Admin/Oper
-----	-----	-----	----	-----	-----	-----	-----
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	down	9000	true/true	full/full	auto/10000

6. Fahren Sie die ISL-Ports auf cs1, dem aktiven NetApp Switch, herunter.

Beispiel anzeigen

```
(cs1) # configure
(cs1) (config) # interface 0/13-0/16
(cs1) (interface 0/13-0/16) # shutdown
(cs1) (interface 0/13-0/16) # exit
(cs1) (config) # exit
```

Schritt 2: Installieren Sie RCF

1. Kopieren Sie den RCF auf den Switch.



Sie müssen die einstellen `.scr` Erweiterung als Teil des Dateinamens vor dem Aufrufen des Skripts. Diese Erweiterung ist die Erweiterung für DAS FASTPATH-Betriebssystem.

Der Switch überprüft das Skript automatisch, wenn es auf den Switch heruntergeladen wird, und die Ausgabe wird zur Konsole gehen.

Beispiel anzeigen

```
(cs2) # copy tftp://10.10.0.1/CN1610_CS_RCF_v1.1.txt nvram:script
CN1610_CS_RCF_v1.1.scr

[the script is now displayed line by line]
Configuration script validated.
File transfer operation completed successfully.
```

2. Überprüfen Sie, ob das Skript heruntergeladen und mit dem Dateinamen gespeichert wurde, den Sie ihm gegeben haben.

Beispiel anzeigen

```
(cs2) # script list
Configuration Script Name          Size(Bytes)
-----
running-config.scr                6960
CN1610_CS_RCF_v1.1.scr            2199

2 configuration script(s) found.
6038 Kbytes free.
```

3. Das Skript validieren.



Das Skript wird während des Downloads validiert, um sicherzustellen, dass jede Zeile eine gültige Switch-Befehlszeile ist.

Beispiel anzeigen

```
(cs2) # script validate CN1610_CS_RCF_v1.1.scr
[the script is now displayed line by line]
Configuration script 'CN1610_CS_RCF_v1.1.scr' validated.
```

4. Das Skript auf den Switch anwenden.

Beispiel anzeigen

```
(cs2) #script apply CN1610_CS_RCF_v1.1.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.1.scr' applied.
```

5. Überprüfen Sie, ob Ihre Änderungen auf dem Switch implementiert wurden.

```
(cs2) # show running-config
```

Im Beispiel wird das angezeigt `running-config` Datei auf dem Switch. Sie müssen die Datei mit dem RCF vergleichen, um zu überprüfen, ob die Parameter, die Sie eingestellt haben, wie Sie erwarten.

6. Speichern Sie die Änderungen.
7. Stellen Sie die ein `running-config` Als Standarddatei.

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.
```

8. Starten Sie den Switch neu, und überprüfen Sie, ob der `running-config` Die Datei ist korrekt.

Nach Abschluss des Neubootens müssen Sie sich anmelden, zeigen Sie die an `running-config` Datei, und suchen Sie dann nach der Beschreibung auf Schnittstelle 3/64, die die Versionsbezeichnung für die RCF ist.

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!
```

9. ISL-Ports an cs1, dem aktiven Switch, herauf.

Beispiel anzeigen

```
(cs1) # configure
(cs1) (config)# interface 0/13-0/16
(cs1) (Interface 0/13-0/16)# no shutdown
(cs1) (Interface 0/13-0/16)# exit
(cs1) (config)# exit
```

10. Vergewissern Sie sich, dass die ISLs betriebsbereit sind:

```
show port-channel 3/1
```

Das Feld „Verbindungsstatus“ sollte angezeigt werden Up.

Beispiel anzeigen

```
(cs2) # show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports    Timeout      Speed     Active
-----
0/13     actor/long      10G Full  True
         partner/long
0/14     actor/long      10G Full  True
         partner/long
0/15     actor/long      10G Full  True
         partner/long
0/16     actor/long      10G Full  True
         partner/long
```

11. Bringen Sie e2a des Cluster-Ports auf beiden Nodes in das System:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e2a auf node1 und node2 hochgestellt wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

Schritt 3: Installation validieren

1. Vergewissern Sie sich, dass Port e2a auf beiden Knoten aktiv ist:

```
network port show -role cluster
```


Beispiel anzeigen

```
cluster::*> network port show -role cluster
```

Node	Port	Role	Link	MTU	Auto-Negot Admin/Oper	Duplex Admin/Oper	Speed (Mbps) Admin/Oper
-----	----	-----	----	----	-----	-----	-----
node1							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	up	9000	true/true	full/full	auto/10000
node2							
	e1a	cluster	up	9000	true/true	full/full	auto/10000
	e2a	cluster	up	9000	true/true	full/full	auto/10000

2. Stellen Sie auf beiden Knoten clu2 zurück, der mit Port e2a verknüpft ist:

```
network interface revert
```

Das LIF ist möglicherweise automatisch zurückgesetzt, je nach Ihrer Version von ONTAP.

Beispiel anzeigen

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```

3. Vergewissern Sie sich, dass das LIF jetzt die Startseite ist (true) Auf beiden Knoten:

```
network interface show -role cluster
```

Beispiel anzeigen

```
cluster::*> network interface show -role cluster
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
-----	-----	-----	-----	-----	-----	----
vs1						
	clus1	up/up	10.10.10.1/24	node1	e1a	true
	clus2	up/up	10.10.10.2/24	node1	e2a	true
vs2						
	clus1	up/up	10.10.10.1/24	node2	e1a	true
	clus2	up/up	10.10.10.2/24	node2	e2a	true

4. Anzeigen des Status der Node-Mitglieder:

```
cluster show
```

Beispiel anzeigen

```
cluster::> cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

5. Kopieren Sie die running-config Datei in der startup-config Datei, wenn Sie mit den Software-Versionen und Switch-Einstellungen zufrieden sind.

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!
```

6. Wiederholen Sie die vorherigen Schritte, um die RCF auf dem anderen Schalter, cs1, zu installieren.

Installieren SIE FASTPATH Software und RCs für ONTAP 8.3.1 und höher

Folgen Sie diesem Verfahren, um FASTPATH-Software und RCFs für ONTAP 8.3.1 und höher zu installieren.

Bei den NetApp CN1601 Management Switches und CN1610 Cluster Switches mit ONTAP 8.3.1 oder höher sind die Installationsschritte identisch. Die beiden Modelle benötigen jedoch unterschiedliche Software und RCFs.

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.

- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen und keine fehlerhaften Cluster Network Interface Cards (NICs) oder ähnlichen Problemen).
- Voll funktionsfähige Portverbindungen am Cluster-Switch.
- Es sind alle Cluster-Ports eingerichtet.
- Einrichtung aller logischen Cluster-Schnittstellen (LIFs) (darf nicht migriert worden sein)
- Ein erfolgreicher Kommunikationspfad: Der ONTAP (Privilege: Erweitert) `cluster ping-cluster -node node1` Der Befehl muss das angeben `larger than PMTU communication` Ist auf allen Pfaden erfolgreich.
- Eine unterstützte Version von FASTPATH, RCF und ONTAP.

Beachten Sie unbedingt die Kompatibilitätstabelle für Switches auf der "[NetApp CN1601 und CN1610 Switches](#)" Seite für die unterstützten FASTPATH-, RCF- und ONTAP-Versionen.

Installieren Sie die FASTPATH Software

Im folgenden Verfahren wird die Syntax „Clustered Data ONTAP 8.2“ verwendet. Aus diesem Grund unterscheiden sich der Cluster-Vserver, LIF-Namen und die CLI-Ausgabe von denen in Data ONTAP 8.3.

Zwischen der Befehlssyntax für „RCF“ und „FASTPATH“-Versionen kann eine Befehlssyntax bestehen.



In RCF Version 1.2 wurde die Unterstützung für Telnet explizit aufgrund von Sicherheitsbedenken deaktiviert. Um Verbindungsprobleme bei der Installation von RCF 1.2 zu vermeiden, vergewissern Sie sich, dass Secure Shell (SSH) aktiviert ist. Der "[Administratorleitfaden für den NetApp CN1610 Switch](#)" Hat weitere Informationen über SSH.

Zu den Beispielen

Die Beispiele in diesem Verfahren verwenden die folgende Nomenklatur für Switches und Knoten:

- Die beiden NetApp Switch-Namen sind cs1 und cs2.
- Die Namen der Cluster Logical Interface (LIF) sind node1_clus1 und node1_clus2 für node1, und node2_clus1 und node2_clus2 für node2. (Ein Cluster kann bis zu 24 Nodes enthalten.)
- Der Name der Storage Virtual Machine (SVM) lautet „Cluster“.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Node lauten e0a und e0b.

"[Hardware Universe](#)" Bietet weitere Informationen zu den tatsächlichen, auf Ihrer Plattform unterstützten Cluster-Ports.

- Die unterstützten Inter-Switch Links (ISLs) sind die Ports 0/13 bis 0/16.
- Die unterstützten Node-Verbindungen sind die Ports 0/1 bis 0/12.

Schritt 1: Migration des Clusters

1. Zeigen Sie Informationen zu den Netzwerkports auf dem Cluster an:

```
network port show -ipspace cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird der Ausgabebetyp aus dem Befehl angezeigt:

```
cluster1::> network port show -ipspace cluster
```

					Speed
(Mbps)					
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----	-----	-----	-----	-----	-----
node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					

4 entries were displayed.

2. Zeigt Informationen zu den LIFs auf dem Cluster an:

```
network interface show -role cluster
```

Beispiel anzeigen

Im folgenden Beispiel werden die logischen Schnittstellen auf dem Cluster angezeigt. In diesem Beispiel die `-role` Mit dem Parameter werden Informationen zu den LIFs angezeigt, die den Cluster-Ports zugeordnet sind:

```
cluster1::> network interface show -role cluster
(network interface show)
      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
Cluster
e0a      node1_clus1  up/up      10.254.66.82/16    node1
      true
e0b      node1_clus2  up/up      10.254.206.128/16  node1
      true
e0a      node2_clus1  up/up      10.254.48.152/16   node2
      true
e0b      node2_clus2  up/up      10.254.42.74/16    node2
      true
4 entries were displayed.
```

3. Migrieren Sie auf jedem entsprechenden Knoten mithilfe einer Knoten-Management-LIF `node1_clus2` zu `e0a` auf `node1` und `node2_clus2` zu `e0a` auf `node2`:

```
network interface migrate
```

Sie müssen die Befehle an den Controller-Konsolen eingeben, die über die jeweiligen Cluster-LIFs verfügen.

Beispiel anzeigen

```
cluster1::> network interface migrate -vserver Cluster -lif
node1_clus2 -destination-node node1 -destination-port e0a
cluster1::> network interface migrate -vserver Cluster -lif
node2_clus2 -destination-node node2 -destination-port e0a
```



Für diesen Befehl wird die Groß-/Kleinschreibung des Clusters beachtet, und der Befehl sollte auf jedem Node ausgeführt werden. Dieser Befehl kann nicht in der allgemeinen Cluster LIF ausgeführt werden.

4. Stellen Sie sicher, dass die Migration mit dem durchgeföhrt wurde `network interface show` Befehl auf einem Node.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass `clus2` zu Port `e0a` auf Nodes `node1` und `node2` migriert hat:

```
cluster1::> **network interface show -role cluster**

      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper Address/Mask      Node
Port      Home
-----
-----
Cluster
e0a          node1_clus1  up/up      10.254.66.82/16   node1
e0a          true
              node1_clus2  up/up      10.254.206.128/16 node1
e0a          false
              node2_clus1  up/up      10.254.48.152/16  node2
e0a          true
              node2_clus2  up/up      10.254.42.74/16  node2
e0a          false
4 entries were displayed.
```

5. Ändern Sie die Berechtigungsebene in Erweitert. Geben Sie Y ein, wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) wird angezeigt.

6. Fahren Sie Cluster-Port `e0b` auf beiden Nodes herunter:

```
network port modify -node node_name -port port_name -up-admin false
```

Sie müssen die Befehle an den Controller-Konsolen eingeben, die über die jeweiligen Cluster-LIFs verfügen.

Beispiel anzeigen

Im folgenden Beispiel werden die Befehle zum Herunterfahren von Port e0b auf allen Nodes angezeigt:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin  
false  
cluster1::*> network port modify -node node2 -port e0b -up-admin  
false
```

7. Vergewissern Sie sich, dass Port e0b auf beiden Nodes heruntergefahren wird:

```
network port show
```

Beispiel anzeigen

```
cluster1::*> network port show -role cluster
```

(Mbps)					Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					
-----	-----	-----	-----	-----	-----
node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	down	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	down	9000
auto/10000					
4 entries were displayed.					

8. Fahren Sie die Inter-Switch Link (ISL)-Ports auf cs1 herunter.

Beispiel anzeigen

```
(cs1) #configure
(cs1) (Config)#interface 0/13-0/16
(cs1) (Interface 0/13-0/16)#shutdown
(cs1) (Interface 0/13-0/16)#exit
(cs1) (Config)#exit
```

9. Sichern Sie das aktuelle aktive Bild auf cs2.

Beispiel anzeigen

```
(cs2) # show bootvar
```

Image Descriptions

active :

backup :

Images currently available on Flash

unit	active	backup	current-active	next-active
1	1.1.0.5	1.1.0.3	1.1.0.5	1.1.0.5

```
(cs2) # copy active backup
Copying active to backup
Copy operation successful
```

Schritt: INSTALLIEREN Sie die FASTPATH-Software und RCF

1. Überprüfen Sie die laufende Version der FASTPATH-Software.

Beispiel anzeigen

```
(cs2) # show version

Switch: 1

System Description..... NetApp CN1610,
1.1.0.5, Linux
                               2.6.21.7
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 20211200106
Burned In MAC Address..... 00:A0:98:21:83:69
Software Version..... 1.1.0.5
Operating System..... Linux 2.6.21.7
Network Processing Device..... BCM56820_B0
Part Number..... 111-00893

--More-- or (q)uit

Additional Packages..... FASTPATH QOS
                               FASTPATH IPv6
Management
```

2. Laden Sie die Bilddatei auf den Switch herunter.

Durch Kopieren der Bilddatei auf das aktive Bild wird beim Neustart die laufende FASTPATH-Version erstellt. Das vorherige Bild bleibt als Backup verfügbar.

Beispiel anzeigen

```
(cs2) #copy
sftp://root@10.22.201.50//tftpboot/NetApp_CN1610_1.2.0.7.stk active
Remote Password:*****

Mode..... SFTP
Set Server IP..... 10.22.201.50
Path..... /tftpboot/
Filename.....
NetApp_CN1610_1.2.0.7.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.
```

3. Aktuelle und nächste aktive Bootabbilde bestätigen:

```
show bootvar
```

Beispiel anzeigen

```
(cs2) #show bootvar

Image Descriptions

active :
backup :

Images currently available on Flash

-----
unit      active      backup      current-active      next-active
-----
1         1.1.0.8      1.1.0.8      1.1.0.8              1.2.0.7
```

4. Installieren Sie den kompatiblen RCF für die neue Bildversion auf dem Switch.

Wenn die RCF-Version bereits korrekt ist, die ISL-Ports heraufbringen.

Beispiel anzeigen

```
(cs2) #copy tftp://10.22.201.50//CN1610_CS_RCF_v1.2.txt nvram:script
CN1610_CS_RCF_v1.2.scr

Mode..... TFTP
Set Server IP..... 10.22.201.50
Path..... /
Filename.....
CN1610_CS_RCF_v1.2.txt
Data Type..... Config Script
Destination Filename.....
CN1610_CS_RCF_v1.2.scr

File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

Validating configuration script...
[the script is now displayed line by line]

Configuration script validated.
File transfer operation completed successfully.
```



Der .scr Die Erweiterung muss als Teil des Dateinamens festgelegt werden, bevor das Skript aufgerufen wird. Diese Erweiterung gilt für DAS FASTPATH-Betriebssystem.

Der Switch überprüft das Skript automatisch, wenn es auf den Switch heruntergeladen wird. Die Ausgabe geht zur Konsole.

5. Überprüfen Sie, ob das Skript heruntergeladen und auf dem Dateinamen gespeichert wurde, den Sie ihm gegeben haben.

Beispiel anzeigen

```
(cs2) #script list

Configuration Script Name          Size(Bytes)
-----
CN1610_CS_RCF_v1.2.scr            2191

1 configuration script(s) found.
2541 Kbytes free.
```

6. Das Skript auf den Switch anwenden.

Beispiel anzeigen

```
(cs2) #script apply CN1610_CS_RCF_v1.2.scr

Are you sure you want to apply the configuration script? (y/n) y
[the script is now displayed line by line]...

Configuration script 'CN1610_CS_RCF_v1.2.scr' applied.
```

7. Überprüfen Sie, ob die Änderungen auf den Switch angewendet wurden, und speichern Sie sie:

```
show running-config
```

Beispiel anzeigen

```
(cs2) #show running-config
```

8. Speichern Sie die laufende Konfiguration, damit sie die Startkonfiguration wird, wenn Sie den Switch neu starten.

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!
```

9. Starten Sie den Switch neu.

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!
```

Schritt 3: Installation validieren

1. Melden Sie sich erneut an, und überprüfen Sie dann, ob auf dem Switch die neue Version der FASTPATH-Software ausgeführt wird.

Beispiel anzeigen

```
(cs2) #show version

Switch: 1

System Description..... NetApp CN1610,
1.2.0.7,Linux
                               3.8.13-4ce360e8
Machine Type..... NetApp CN1610
Machine Model..... CN1610
Serial Number..... 20211200106
Burned In MAC Address..... 00:A0:98:21:83:69
Software Version..... 1.2.0.7
Operating System..... Linux 3.8.13-
4ce360e8
Network Processing Device..... BCM56820_B0
Part Number..... 111-00893
CPLD version..... 0x5

Additional Packages..... FASTPATH QOS
                               FASTPATH IPv6
Management
```

Nach Abschluss des Neubootens müssen Sie sich anmelden, um die Bildversion zu überprüfen, die laufende Konfiguration anzuzeigen, und nach der Beschreibung auf der Schnittstelle 3/64 suchen, die die Versionsbezeichnung für die RCF ist.

2. ISL-Ports an cs1, dem aktiven Switch, herauf.

Beispiel anzeigen

```
(cs1) #configure
(cs1) (Config) #interface 0/13-0/16
(cs1) (Interface 0/13-0/16) #no shutdown
(cs1) (Interface 0/13-0/16) #exit
(cs1) (Config) #exit
```

3. Vergewissern Sie sich, dass die ISLs betriebsbereit sind:

```
show port-channel 3/1
```

Das Feld „Verbindungsstatus“ sollte angezeigt werden Up.

Beispiel anzeigen

```
(cs1) #show port-channel 3/1

Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)

Mbr      Device/      Port      Port
Ports   Timeout      Speed     Active
-----
0/13     actor/long      10G Full  True
         partner/long
0/14     actor/long      10G Full  True
         partner/long
0/15     actor/long      10G Full  False
         partner/long
0/16     actor/long      10G Full  True
         partner/long
```

4. Bringen Sie Cluster Port e0b auf allen Nodes hinzu:

```
network port modify
```

Sie müssen die Befehle an den Controller-Konsolen eingeben, die über die jeweiligen Cluster-LIFs verfügen.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e0b auf node1 und node2 gebracht wird:

```
cluster1::*> network port modify -node node1 -port e0b -up-admin
true
cluster1::*> network port modify -node node2 -port e0b -up-admin
true
```

5. Vergewissern Sie sich, dass der Port e0b auf allen Nodes aktiviert ist:

```
network port show -ipSPACE cluster
```

Beispiel anzeigen

```
cluster1::*> network port show -ipspace cluster
```

(Mbps)					Speed
Node	Port	IPspace	Broadcast Domain	Link	MTU
Admin/Oper					

node1					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					
node2					
	e0a	Cluster	Cluster	up	9000
auto/10000					
	e0b	Cluster	Cluster	up	9000
auto/10000					

4 entries were displayed.

6. Vergewissern Sie sich, dass das LIF jetzt die Startseite ist (`true`) Auf beiden Knoten:

```
network interface show -role cluster
```


Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
```

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			

Cluster				
	node1_clus1	up/up	169.254.66.82/16	node1
e0a	true			
	node1_clus2	up/up	169.254.206.128/16	node1
e0b	true			
	node2_clus1	up/up	169.254.48.152/16	node2
e0a	true			
	node2_clus2	up/up	169.254.42.74/16	node2
e0b	true			
4 entries were displayed.				

7. Zeigt den Status der Node-Mitglieder an:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1	true	true	false
node2	true	true	false
2 entries were displayed.			

8. Zurück zur Administratorberechtigungsebene:

```
set -privilege admin
```

9. Wiederholen Sie die vorherigen Schritte, um DIE FASTPATH-Software und RCF auf dem anderen Switch, cs1, zu installieren.

Konfigurieren Sie die Hardware für den NetApp CN1610 Switch

Informationen zur Konfiguration der Switch-Hardware und -Software für Ihre Cluster-Umgebung finden Sie im ["Installations- und Konfigurationshandbuch für CN1601 und CN1610-Switch"](#).

Switches migrieren

Migration von einer Cluster-Umgebung ohne Switches zu einer Switch-basierten NetApp CN1610 Cluster-Umgebung

Wenn Sie eine vorhandene Cluster-Umgebung mit zwei Nodes ohne Switches nutzen, können Sie mit CN1610 Cluster-Netzwerk-Switches zu einer Switch-basierten Cluster-Umgebung mit zwei Nodes migrieren. So können Sie eine Skalierung über zwei Nodes hinaus vornehmen.

Prüfen Sie die Anforderungen

Was Sie benötigen

Stellen Sie bei einer Konfiguration mit zwei Nodes ohne Switches Folgendes sicher:

- Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
- Auf den Knoten wird ONTAP 8.2 oder höher ausgeführt.
- Alle Cluster-Ports befinden sich im `up` Bundesland.
- Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im `up` Geben Sie den Staat und die Anschlüsse zu Hause an.

Bei der Switch-Konfiguration des CN1610-Cluster:

- Die CN1610 Cluster-Switch-Infrastruktur funktioniert bei beiden Switches voll und ganz.
- Beide Switches verfügen über Management-Netzwerk-Konnektivität.
- Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
- Bei Node-to-Node-Switch und Switch-to-Switch-Verbindungen bei CN1610 werden Twinax- oder Glasfaserkabel verwendet.

Der ["Hardware Universe"](#) Enthält weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel sind an beiden CN1610 Switches mit den Ports 13 bis 16 verbunden.
- Die Erstanpassung der beiden CN1610 Switches ist abgeschlossen.

Alle Anpassungen der vorherigen Site, wie SMTP, SNMP und SSH, sollten auf die neuen Switches kopiert werden.

Verwandte Informationen

- ["Hardware Universe"](#)
- ["Beschreibungsseite zu NetApp CN1601 und CN1610"](#)
- ["Installations- und Konfigurationshandbuch für CN1601 und CN1610-Switch"](#)

- ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#)

Migrieren Sie die Switches

Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der CN1610-Switches lauten cs1 und cs2.
- Die Namen der LIFs sind Faclu1 und clut2.
- Die Namen der Nodes sind node1 und node2.
- Der `cluster::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind e1a und e2a.

Der ["Hardware Universe"](#) Enthält die neuesten Informationen über die tatsächlichen Cluster-Ports für Ihre Plattformen.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y` Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) wird angezeigt.

2. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message MAINT=xh
```

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

Beispiel anzeigen

Mit dem folgenden Befehl wird die automatische Case-Erstellung für zwei Stunden unterdrückt:

```
cluster::*> system node autosupport invoke -node * -type all  
-message MAINT=2h
```

Schritt 2: Ports konfigurieren

1. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches cs1 und cs2.

Sie dürfen die ISL-Ports nicht deaktivieren.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 12 auf Switch cs1 deaktiviert sind:

```
(cs1)> enable
(cs1)# configure
(cs1) (Config)# interface 0/1-0/12
(cs1) (Interface 0/1-0/12)# shutdown
(cs1) (Interface 0/1-0/12)# exit
(cs1) (Config)# exit
```

Das folgende Beispiel zeigt, dass die Node-Ports 1 bis 12 auf Switch cs2 deaktiviert sind:

```
(c2)> enable
(cs2)# configure
(cs2) (Config)# interface 0/1-0/12
(cs2) (Interface 0/1-0/12)# shutdown
(cs2) (Interface 0/1-0/12)# exit
(cs2) (Config)# exit
```

2. Stellen Sie sicher, dass ISL und die physischen Ports auf der ISL zwischen den beiden CN1610 Cluster-Switches cs1 und cs2 liegen up:

```
show port-channel
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass es sich um die ISL-Ports handelt up Schalter cs1 ein:

```
(cs1)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr Ports	Device/ Timeout	Port Speed	Port Active
-----	-----	-----	-----
0/13	actor/long partner/long	10G Full	True
0/14	actor/long partner/long	10G Full	True
0/15	actor/long partner/long	10G Full	True
0/16	actor/long partner/long	10G Full	True

Das folgende Beispiel zeigt, dass es sich um die ISL-Ports handelt up Schalter cs2 ein:

```
(cs2)# show port-channel 3/1
Local Interface..... 3/1
Channel Name..... ISL-LAG
Link State..... Up
Admin Mode..... Enabled
Type..... Static
Load Balance Option..... 7
(Enhanced hashing mode)
```

Mbr	Device/ Ports	Port Timeout	Port Speed	Port Active
-----	-----	-----	-----	-----
0/13	actor/long partner/long	10G Full	True	
0/14	actor/long partner/long	10G Full	True	
0/15	actor/long partner/long	10G Full	True	
0/16	actor/long partner/long	10G Full	True	

3. Liste der benachbarten Geräte anzeigen:

```
show isdp neighbors
```

Dieser Befehl enthält Informationen zu den Geräten, die mit dem System verbunden sind.

Beispiel anzeigen

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs1 aufgeführt:

```
(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                0/13          11        S           CN1610
0/13
cs2                0/14          11        S           CN1610
0/14
cs2                0/15          11        S           CN1610
0/15
cs2                0/16          11        S           CN1610
0/16
```

Im folgenden Beispiel sind die benachbarten Geräte auf Switch cs2 aufgeführt:

```
(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
-----
cs1                0/13          11        S           CN1610
0/13
cs1                0/14          11        S           CN1610
0/14
cs1                0/15          11        S           CN1610
0/15
cs1                0/16          11        S           CN1610
0/16
```

4. Zeigt die Liste der Cluster-Ports an:

```
network port show
```

Beispiel anzeigen

Im folgenden Beispiel werden die verfügbaren Cluster-Ports angezeigt:


```
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						
e0c	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4b	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						
e0c	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4a	Cluster	Cluster		up	9000	auto/10000	
healthy	false						
e4b	Cluster	Cluster		up	9000	auto/10000	
healthy	false						

```
12 entries were displayed.
```

5. Vergewissern Sie sich, dass jeder Cluster-Port mit dem entsprechenden Port auf seinem Partner-Cluster-Node verbunden ist:

```
run * cdpd show-neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports e1a und e2a mit demselben Port auf ihrem Cluster-Partner-Node verbunden sind:

```
cluster::*> run * cdpd show-neighbors
2 entries were acted on.
```

Node: node1

Local Remote	Remote	Remote	Remote	Hold
Port Device	Interface	Platform	Time	
Capability				

e1a	node2	e1a	FAS3270	137
H				
e2a	node2	e2a	FAS3270	137
H				

Node: node2

Local Remote	Remote	Remote	Remote	Hold
Port Device	Interface	Platform	Time	
Capability				

e1a	node1	e1a	FAS3270	161
H				
e2a	node1	e2a	FAS3270	161
H				

6. Vergewissern Sie sich, dass alle Cluster-LIFs sind up Und in Betrieb:

```
network interface show -vserver Cluster
```

Jede Cluster-LIF sollte angezeigt werden true In der Spalte „is Home“.

Beispiel anzeigen

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	
node1					
true	clus1	up/up	10.10.10.1/16	node1	e1a
true	clus2	up/up	10.10.10.2/16	node1	e2a
node2					
true	clus1	up/up	10.10.11.1/16	node2	e1a
true	clus2	up/up	10.10.11.2/16	node2	e2a

4 entries were displayed.



Die folgenden Änderungs- und Migrationsbefehle in den Schritten 10 bis 13 müssen vom lokalen Node aus ausgeführt werden.

7. Vergewissern Sie sich, dass alle Cluster-Ports vorhanden sind up:

```
network port show -ipspace Cluster
```

Beispiel anzeigen

```
cluster::*> network port show -ipspace Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	up	9000	true/true	full/full	
	auto/10000						
	e2a	clus2	up	9000	true/true	full/full	
	auto/10000						
node2							
	e1a	clus1	up	9000	true/true	full/full	
	auto/10000						
	e2a	clus2	up	9000	true/true	full/full	
	auto/10000						

4 entries were displayed.

8. Stellen Sie die ein `-auto-revert` Parameter an `false` Auf Cluster LIFs `clus1` und `clus2` zu beiden Knoten:

```
network interface modify
```

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto-revert false
cluster::*> network interface modify -vserver node1 -lif clus2 -auto-revert false
cluster::*> network interface modify -vserver node2 -lif clus1 -auto-revert false
cluster::*> network interface modify -vserver node2 -lif clus2 -auto-revert false
```



Verwenden Sie für Version 8.3 und höher den folgenden Befehl: `network interface modify -vserver Cluster -lif * -auto-revert false`

9. Ping für die Cluster-Ports zur Überprüfung der Cluster-Konnektivität:

```
cluster ping-cluster local
```

Die Befehlsausgabe zeigt die Verbindung zwischen allen Cluster-Ports an.

10. Faclu1 zu Port e2a auf der Konsole jedes Knotens migrieren:

```
network interface migrate
```

Beispiel anzeigen

Das folgende Beispiel zeigt den Prozess der Migration von Faclu1 zu Anschluss e2a auf node1 und node2:

```
cluster::*> network interface migrate -vserver node1 -lif clus1  
-source-node node1 -dest-node node1 -dest-port e2a  
cluster::*> network interface migrate -vserver node2 -lif clus1  
-source-node node2 -dest-node node2 -dest-port e2a
```



Verwenden Sie für Version 8.3 und höher den folgenden Befehl: `network interface migrate -vserver Cluster -lif clus1 -destination-node node1 -destination-port e2a`

11. Vergewissern Sie sich, dass die Migration stattgefunden hat:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird überprüft, ob Faclu1 zu Port e2a auf node1 und node2 migriert wird:

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
false	clus1	up/up	10.10.10.1/16	node1	e2a
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2					
false	clus1	up/up	10.10.11.1/16	node2	e2a
	clus2	up/up	10.10.11.2/16	node2	e2a
true					

4 entries were displayed.

12. Fahren Sie Cluster-Port e1a auf beiden Knoten herunter:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e1a auf node1 und node2 heruntergefahren wird:

```
cluster::*> network port modify -node node1 -port e1a -up-admin  
false  
cluster::*> network port modify -node node2 -port e1a -up-admin  
false
```

13. Überprüfen Sie den Portstatus:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass der Anschluss e1a lautet down Auf Knoten 1 und Knoten 2:

```
cluster::*> network port show -role cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							

node1							
	e1a	clus1	down	9000	true/true	full/full	
	auto/10000						
	e2a	clus2	up	9000	true/true	full/full	
	auto/10000						
node2							
	e1a	clus1	down	9000	true/true	full/full	
	auto/10000						
	e2a	clus2	up	9000	true/true	full/full	
	auto/10000						

4 entries were displayed.

14. Trennen Sie das Kabel vom Cluster-Port e1a in Node1, und verbinden sie dann e1a mit Port 1 am Cluster-Switch cs1. Verwenden Sie dabei die geeignete Verkabelung, die von den CN1610-Switches unterstützt wird.

Der "[Hardware Universe](#)" Enthält weitere Informationen zur Verkabelung.

15. Trennen Sie das Kabel vom Cluster-Port e1a auf node2, und verbinden sie dann e1a mit Port 2 am Cluster-Switch cs1. Verwenden Sie dabei die geeignete Verkabelung, die von den CN1610-Switches unterstützt wird.
16. Aktivieren Sie alle Node-Ports auf Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1 bis 12 auf Switch cs1 aktiviert sind:

```
(cs1)# configure
(cs1)(Config)# interface 0/1-0/12
(cs1)(Interface 0/1-0/12)# no shutdown
(cs1)(Interface 0/1-0/12)# exit
(cs1)(Config)# exit
```

17. Aktivieren Sie den ersten Cluster-Port e1a auf jedem Knoten:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e1a auf node1 und node2 aktiviert wird:

```
cluster::*> network port modify -node node1 -port e1a -up-admin true
cluster::*> network port modify -node node2 -port e1a -up-admin true
```

18. Vergewissern Sie sich, dass alle Cluster-Ports vorhanden sind up:

```
network port show -ipSPACE Cluster
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports angezeigt up Auf Knoten 1 und Knoten 2:

```
cluster::*> network port show -ipSPACE Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							
-----	-----	-----	----	-----	-----	-----	-----

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	up	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

19. Fazit 1 (der zuvor migriert wurde) auf beiden Knoten zu e1a zurücksetzen:

```
network interface revert
```


Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Anschluss Nr. 1 und Nr. 2 auf den Port e1a zurückgesetzt wird:

```
cluster::*> network interface revert -vserver node1 -lif clus1
cluster::*> network interface revert -vserver node2 -lif clus1
```



Verwenden Sie für Version 8.3 und höher den folgenden Befehl: `network interface revert -vserver Cluster -lif <nodename_clus<N>>`

20. Vergewissern Sie sich, dass alle Cluster-LIFs sind up, Betrieb, und Anzeige als true In der Spalte „is Home“:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs sind up Auf node1 und node2 und dass die "is Home" Spalte Ergebnisse sind true:

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true					
	clus2	up/up	10.10.10.2/16	node1	e2a
true					
node2					
	clus1	up/up	10.10.11.1/16	node2	e1a
true					
	clus2	up/up	10.10.11.2/16	node2	e2a
true					

4 entries were displayed.

21. Informationen zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true    true         false
node2                true    true         false
```

22. Fazit 2 auf Port e1a auf der Konsole jedes Knotens migrieren:

```
network interface migrate
```

Beispiel anzeigen

Das folgende Beispiel zeigt den Prozess für die Migration von Fak2 auf Port e1a in Node1 und node2:

```
cluster::*> network interface migrate -vserver node1 -lif clus2
-source-node node1 -dest-node node1 -dest-port e1a
cluster::*> network interface migrate -vserver node2 -lif clus2
-source-node node2 -dest-node node2 -dest-port e1a
```



Verwenden Sie für Version 8.3 und höher den folgenden Befehl: `network interface migrate -vserver Cluster -lif node1_clus2 -dest-node node1 -dest-port e1a`

23. Vergewissern Sie sich, dass die Migration stattgefunden hat:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

Im folgenden Beispiel wird überprüft, ob Faclu2 in den Anschluss e1a in den Knoten 1 und node2 migriert wird:

```
cluster::*> network interface show -vserver Cluster
```

	Logical	Status	Network	Current	
Current Is					
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					

node1					
	clus1	up/up	10.10.10.1/16	node1	e1a
true					
	clus2	up/up	10.10.10.2/16	node1	e1a
false					
node2					
	clus1	up/up	10.10.11.1/16	node2	e1a
true					
	clus2	up/up	10.10.11.2/16	node2	e1a
false					

4 entries were displayed.

24. Fahren Sie Cluster-Port e2a auf beiden Nodes herunter:

```
network port modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e2a auf node1 und node2 heruntergefahren wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin  
false  
cluster::*> network port modify -node node2 -port e2a -up-admin  
false
```

25. Überprüfen Sie den Portstatus:

```
network port show
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Port e2a ist down Auf Knoten 1 und Knoten 2:

```
cluster::*> network port show -role cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)							
Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper	
Admin/Oper							
-----	-----	-----	----	-----	-----	-----	-----

node1							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	down	9000	true/true	full/full	
auto/10000							
node2							
	e1a	clus1	up	9000	true/true	full/full	
auto/10000							
	e2a	clus2	down	9000	true/true	full/full	
auto/10000							

4 entries were displayed.

26. Trennen Sie das Kabel vom Cluster-Port e2a auf node1, und verbinden sie dann e2a mit Port 1 am Cluster-Switch cs2. Verwenden Sie dabei die geeignete Verkabelung, die von den CN1610-Switches unterstützt wird.
27. Trennen Sie das Kabel vom Cluster-Port e2a auf node2, und verbinden sie dann e2a mit Port 2 am Cluster-Switch cs2. Verwenden Sie dabei die geeignete Verkabelung, die von den CN1610-Switches unterstützt wird.
28. Aktivieren Sie alle Node-Ports auf Cluster-Switch cs2.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1 bis 12 auf Switch cs2 aktiviert sind:

```
(cs2)# configure
(cs2)(Config)# interface 0/1-0/12
(cs2)(Interface 0/1-0/12)# no shutdown
(cs2)(Interface 0/1-0/12)# exit
(cs2)(Config)# exit
```

29. Aktivieren Sie den zweiten Cluster-Port e2a auf jedem Knoten.

Beispiel anzeigen

Das folgende Beispiel zeigt, wie der Port e2a auf node1 und node2 aktiviert wird:

```
cluster::*> network port modify -node node1 -port e2a -up-admin true
cluster::*> network port modify -node node2 -port e2a -up-admin true
```

30. Vergewissern Sie sich, dass alle Cluster-Ports vorhanden sind up:

```
network port show -ipspace Cluster
```

Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports angezeigt up Auf Knoten 1 und Knoten 2:

```
cluster::*> network port show -ipspace Cluster
```

					Auto-Negot	Duplex	Speed
(Mbps)	Node	Port	Role	Link	MTU	Admin/Oper	Admin/Oper
Admin/Oper							
-----	-----	-----	-----	-----	-----	-----	-----
node1							
		e1a	clus1	up	9000	true/true	full/full
auto/10000							
		e2a	clus2	up	9000	true/true	full/full
auto/10000							
node2							
		e1a	clus1	up	9000	true/true	full/full
auto/10000							
		e2a	clus2	up	9000	true/true	full/full
auto/10000							

4 entries were displayed.

31. Schluss2 (der zuvor migriert wurde) auf beiden Knoten zu e2a zurücksetzen:

```
network interface revert
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie man clu2 auf den Port e2a auf node1 und node2 zurücksetzt:

```
cluster::*> network interface revert -vserver node1 -lif clus2
cluster::*> network interface revert -vserver node2 -lif clus2
```



Für Release 8.3 und höher lauten die Befehle:

```
cluster::*> network interface revert -vserver Cluster -lif
node1_clus2 Und
```

```
cluster::*> network interface revert -vserver Cluster -lif
node2_clus2
```

Schritt 3: Schließen Sie die Konfiguration ab

1. Vergewissern Sie sich, dass alle Schnittstellen angezeigt werden `true` In der Spalte „is Home“:

```
network interface show -vserver Cluster
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs sind up Auf node1 und node2 und dass die "is Home" Spalte Ergebnisse sind `true`:

```
cluster::*> network interface show -vserver Cluster
```

Current	Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node	
Port	Home				
-----	-----	-----	-----	-----	-----
node1					
		clus1	up/up	10.10.10.1/16	node1
e1a	true				
		clus2	up/up	10.10.10.2/16	node1
e2a	true				
node2					
		clus1	up/up	10.10.11.1/16	node2
e1a	true				
		clus2	up/up	10.10.11.2/16	node2
e2a	true				

2. Ping für die Cluster-Ports zur Überprüfung der Cluster-Konnektivität:

```
cluster ping-cluster local
```

Die Befehlsausgabe zeigt die Verbindung zwischen allen Cluster-Ports an.

3. Vergewissern Sie sich, dass beide Nodes zwei Verbindungen zu jedem Switch haben:

```
show isdp neighbors
```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

```
(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            132       H           FAS3270
e1a
node2              0/2            163       H           FAS3270
e1a
cs2                0/13           11        S           CN1610
0/13
cs2                0/14           11        S           CN1610
0/14
cs2                0/15           11        S           CN1610
0/15
cs2                0/16           11        S           CN1610
0/16

(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            132       H           FAS3270
e2a
node2              0/2            163       H           FAS3270
e2a
cs1                0/13           11        S           CN1610
0/13
cs1                0/14           11        S           CN1610
0/14
cs1                0/15           11        S           CN1610
0/15
cs1                0/16           11        S           CN1610
0/16
```


4. Informationen zu den Geräten in Ihrer Konfiguration anzeigen:

```
network device discovery show
```

5. Deaktivieren Sie die Konfigurationseinstellungen mit zwei Nodes ohne Switches auf beiden Nodes mithilfe des erweiterten Befehls „Privilege“:

```
network options detect-switchless modify
```

Beispiel anzeigen

Das folgende Beispiel zeigt, wie die Konfigurationseinstellungen ohne Switches deaktiviert werden:

```
cluster::*> network options detect-switchless modify -enabled false
```



überspringen Sie diesen Schritt für Version 9.2 und höher, da die Konfiguration automatisch konvertiert wird.

6. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

```
network options detect-switchless-cluster show
```

Beispiel anzeigen

Der false Die Ausgabe im folgenden Beispiel zeigt, dass die Konfigurationseinstellungen deaktiviert sind:

```
cluster::*> network options detect-switchless-cluster show  
Enable Switchless Cluster Detection: false
```



Für Version 9.2 und höher, warten Sie bis Enable Switchless Cluster Ist auf FALSE gesetzt. Dies kann bis zu drei Minuten dauern.

7. Konfigurieren Sie Cluster clue1 und clu2, um jeden Knoten automatisch zurückzusetzen und zu bestätigen.

Beispiel anzeigen

```
cluster::*> network interface modify -vserver node1 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node1 -lif clus2 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus1 -auto
-revert true
cluster::*> network interface modify -vserver node2 -lif clus2 -auto
-revert true
```



Verwenden Sie für Version 8.3 und höher den folgenden Befehl: `network interface modify -vserver Cluster -lif * -auto-revert true` Um die automatische Umrüstung auf allen Nodes im Cluster zu aktivieren.

8. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

```
cluster::*> cluster show
Node                Health  Eligibility  Epsilon
-----
node1                true   true         false
node2                true   true         false
```

9. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Beispiel anzeigen

```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=END
```

10. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

Tauschen Sie die Schalter aus

Ersetzen Sie einen NetApp CN1610 Cluster Switch

Führen Sie diese Schritte aus, um einen defekten NetApp CN1610-Switch in einem Cluster-Netzwerk auszutauschen. Dies ist ein unterbrechungsfreies Verfahren (Nondisruptive Procedure, NDU).

Was Sie benötigen

Bevor Sie den Switch austauschen, müssen die folgenden Bedingungen erfüllt sein, bevor Sie den Switch in der aktuellen Umgebung und am Ersatz-Switch für das vorhandene Cluster und die Netzwerkinfrastruktur austauschen:

- Das vorhandene Cluster muss mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig verifiziert werden.
- Alle Cluster-Ports müssen **up** sein.
- Alle logischen Cluster-Schnittstellen (LIFs) müssen aktiviert sein und dürfen nicht migriert worden sein.
- Dem ONTAP Cluster `ping-cluster -node node1` Befehl muss angegeben, dass die grundlegende Konnektivität und die Kommunikation größer als PMTU auf allen Pfaden erfolgreich ist.

Über diese Aufgabe

Sie müssen den Befehl zum Migrieren einer Cluster-LIF von dem Node ausführen, auf dem die Cluster-LIF gehostet wird.

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der beiden CN1610 Cluster-Switches lauten `cs1` und `cs2`.
- Der Name des zu ersetzenden CN1610-Schalters (der defekte Schalter) lautet `old_cs1`.
- Der Name des neuen CN1610-Schalters (der Ersatzschalter) lautet `new_cs1`.
- Der Name des Partner-Switches, der nicht ersetzt wird, lautet `cs2`.

Schritte

1. Vergewissern Sie sich, dass die Startkonfigurationsdatei mit der ausgeführten Konfigurationsdatei übereinstimmt. Sie müssen diese Dateien lokal speichern, um sie während des Austauschs verwenden zu können.

Die Konfigurationsbefehle im folgenden Beispiel gelten für FASTPATH 1.2.0.7:

Beispiel anzeigen

```
(old_cs1) >enable
(old_cs1) #show running-config
(old_cs1) #show startup-config
```

2. Erstellen Sie eine Kopie der ausgeführten Konfigurationsdatei.

Der Befehl im folgenden Beispiel ist für FASTPATH 1.2.0.7:

Beispiel anzeigen

```
(old_cs1) #show running-config filename.scr  
Config script created successfully.
```



Sie können jeden Dateinamen außer verwenden CN1610_CS_RCF_v1.2.scr. Der Dateiname muss die Erweiterung **.SCR** haben.

1. Speichern Sie die laufende Konfigurationsdatei des Switches auf einem externen Host, um den Austausch vorzubereiten.

Beispiel anzeigen

```
(old_cs1) #copy nvram:script filename.scr  
scp://<Username>@<remote_IP_address>/path_to_file/filename.scr
```

2. Überprüfen Sie, ob die Switch- und ONTAP-Versionen in der Kompatibilitätsmatrix übereinstimmen. Siehe ["NetApp CN1601 und CN1610 Switches"](#) Für Details.
3. Von ["Seite „Software-Downloads“"](#) Wählen Sie auf der NetApp Support Website NetApp Cluster Switches aus, um die entsprechenden RCF- und FASTPATH-Versionen herunterzuladen.
4. Richten Sie einen TFTP-Server (Trivial File Transfer Protocol) mit DER FASTPATH-, RCF- und gespeicherten Konfiguration ein .scr Datei zur Verwendung mit dem neuen Switch.
5. Verbinden Sie den seriellen Port (der RJ-45-Anschluss mit der Bezeichnung „IOIOIOI“ auf der rechten Seite des Switches) mit einem verfügbaren Host mit Terminalemulation.
6. Stellen Sie auf dem Host die Einstellungen für die serielle Terminalverbindung ein:
 - a. 9600 Baud
 - b. 8 Datenbits
 - c. 1 Stoppbit
 - d. Parität: Keine
 - e. Flusskontrolle: Keine
7. Verbinden Sie den Verwaltungsport (den RJ-45-Schraubenschlüssel-Port auf der linken Seite des Switches) mit dem gleichen Netzwerk, in dem sich Ihr TFTP-Server befindet.
8. Bereiten Sie sich auf die Netzwerkverbindung mit dem TFTP-Server vor.

Wenn Sie DHCP (Dynamic Host Configuration Protocol) verwenden, müssen Sie derzeit keine IP-Adresse für den Switch konfigurieren. Der Service-Port ist standardmäßig auf DHCP eingestellt. Der Netzwerkverwaltungsport ist für die IPv4- und IPv6-Protokolleinstellungen auf none festgelegt. Wenn der Schlüsselport mit einem Netzwerk verbunden ist, das über einen DHCP-Server verfügt, werden die Servereinstellungen automatisch konfiguriert.

Um eine statische IP-Adresse festzulegen, sollten Sie die Befehle serviceport-Protokoll, Netzwerkprotokoll und serviceport ip verwenden.

Beispiel anzeigen

```
(new_cs1) #serviceport ip <ipaddr> <netmask> <gateway>
```

9. Wenn sich der TFTP-Server auf einem Laptop befindet, schließen Sie den CN1610-Switch optional über ein Standard-Ethernet-Kabel an den Laptop an, und konfigurieren Sie dann den Netzwerkanschluss im gleichen Netzwerk mit einer alternativen IP-Adresse.

Sie können das verwenden `ping` Befehl zum Verifizieren der Adresse. Wenn Sie die Verbindung nicht herstellen können, sollten Sie ein nicht geroutetes Netzwerk verwenden und den Service-Port mit IP 192.168.x oder 172.16.x konfigurieren Sie können den Service-Port zu einem späteren Zeitpunkt auf die Produktions-Management-IP-Adresse neu konfigurieren.

10. Überprüfen und installieren Sie optional die entsprechenden Versionen der RCF- und FASTPATH-Software für den neuen Switch. Wenn Sie überprüft haben, ob der neue Switch korrekt eingerichtet ist und keine Updates für die RCF- und FASTPATH-Software erforderlich sind, fahren Sie mit Schritt 13 fort.
 - a. Überprüfen Sie die neuen Schaltereinstellungen.

Beispiel anzeigen

```
(new_cs1) >*enable*  
(new_cs1) #show version
```

- b. Laden Sie den RCF auf den neuen Switch herunter.

Beispiel anzeigen

```
(new_cs1) #copy tftp://<server_ip_address>/CN1610_CS_RCF_v1.2.txt
nvram:script CN1610_CS_RCF_v1.2.scr
Mode.      TFTP
Set Server IP. 172.22.201.50
Path.      /
Filename.....
CN1610_CS_RCF_v1.2.txt
Data Type..... Config Script
Destination Filename.....
CN1610_CS_RCF_v1.2.scr
File with same name already exists.
WARNING:Continuing with this command will overwrite the existing
file.

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...
Validating configuration script...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script validated.
File transfer operation completed successfully.
```

- c. Stellen Sie sicher, dass der RCF auf den Switch heruntergeladen wurde.

Beispiel anzeigen

```
(new_cs1) #script list
Configuration Script Nam    Size(Bytes)
-----
CN1610_CS_RCF_v1.1.scr      2191
CN1610_CS_RCF_v1.2.scr      2240
latest_config.scr           2356

4 configuration script(s) found.
2039 Kbytes free.
```

11. Den RCF auf den CN1610-Schalter auftragen.

Beispiel anzeigen

```
(new_cs1) #script apply CN1610_CS_RCF_v1.2.scr
Are you sure you want to apply the configuration script? (y/n) y
...
(the entire script is displayed line by line)
...
description "NetApp CN1610 Cluster Switch RCF v1.2 - 2015-01-13"
...
Configuration script 'CN1610_CS_RCF_v1.2.scr' applied. Note that the
script output will go to the console.
After the script is applied, those settings will be active in the
running-config file. To save them to the startup-config file, you
must use the write memory command, or if you used the reload answer
yes when asked if you want to save the changes.
```

- a. Speichern Sie die laufende Konfigurationsdatei, damit sie beim Neustart des Switches zur Startkonfigurationsdatei wird.

Beispiel anzeigen

```
(new_cs1) #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!
```

- b. Laden Sie das Bild auf den Switch CN1610 herunter.

Beispiel anzeigen

```
(new_cs1) #copy
tftp://<server_ip_address>/NetApp_CN1610_1.2.0.7.stk active
Mode.      TFTP
Set Server IP.  tftp_server_ip_address
Path.        /
Filename.....
NetApp_CN1610_1.2.0.7.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

TFTP Code transfer starting...

File transfer operation completed successfully.
```

- c. Führen Sie das neue aktive Startabbild durch, indem Sie den Switch neu starten.

Der Switch muss neu gestartet werden, damit der Befehl in Schritt 6 das neue Image widerspiegelt. Es gibt zwei mögliche Ansichten für eine Antwort, die Sie nach Eingabe des Befehls reload möglicherweise sehen werden.

Beispiel anzeigen

```
(new_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!
.
.
.
Cluster Interconnect Infrastructure

User:admin Password: (new_cs1) >*enable*
```


- a. Kopieren Sie die gespeicherte Konfigurationsdatei vom alten Switch auf den neuen Switch.

Beispiel anzeigen

```
(new_cs1) #copy tftp://<server_ip_address>/<filename>.scr  
nvram:script <filename>.scr
```

- b. Wenden Sie die zuvor gespeicherte Konfiguration auf den neuen Switch an.

Beispiel anzeigen

```
(new_cs1) #script apply <filename>.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!
```

- c. Speichern Sie die laufende Konfigurationsdatei in der Startkonfigurationsdatei.

Beispiel anzeigen

```
(new_cs1) #write memory
```

12. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all - message MAINT=xh
```

X ist die Dauer des Wartungsfensters in Stunden.



Die AutoSupport Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt wird.

13. Melden Sie sich beim neuen Switch New_cs1 als Admin-Benutzer an, und fahren Sie alle Ports herunter, die mit den Node-Cluster-Schnittstellen (Ports 1 bis 12) verbunden sind.

Beispiel anzeigen

```
User:*admin*
Password:
(new_cs1) >*enable*
(new_cs1) #

(new_cs1) config
(new_cs1) (config) interface 0/1-0/12
(new_cs1) (interface 0/1-0/12) shutdown
(new_cs1) (interface 0/1-0/12) exit
(new_cs1) #write memory
```

14. Migrieren Sie die Cluster-LIFs von den Ports, die mit dem Switch old_cs1 verbunden sind.

Sie müssen jede LIF des Clusters von der Managementoberfläche des aktuellen Node migrieren.

Beispiel anzeigen

```
cluster::> set -privilege advanced
cluster::> network interface migrate -vserver <vserver_name> -lif
<Cluster_LIF_to_be_moved> - sourcenode <current_node> -dest-node
<current_node> -dest-port <cluster_port_that_is_UP>
```

15. Vergewissern Sie sich, dass alle Cluster-LIFs auf den entsprechenden Cluster-Port auf jedem Node verschoben wurden.

Beispiel anzeigen

```
cluster::> network interface show -role cluster
```

16. Fahren Sie die Cluster-Ports herunter, die an den Switch angeschlossen sind, den Sie ausgetauscht haben.

Beispiel anzeigen

```
cluster::*> network port modify -node <node_name> -port
<port_to_admin_down> -up-admin false
```

17. Überprüfen Sie den Systemzustand des Clusters.

Beispiel anzeigen

```
cluster::*> cluster show
```

18. Vergewissern Sie sich, dass die Ports ausgefallen sind.

Beispiel anzeigen

```
cluster::*> cluster ping-cluster -node <node_name>
```

19. Fahren Sie auf dem Switch cs2 die ISL-Ports 13 bis 16 herunter.

Beispiel anzeigen

```
(cs2) config  
(cs2)(config) interface 0/13-0/16  
(cs2)(interface 0/13-0/16) #shutdown  
(cs2) #show port-channel 3/1
```

20. Überprüfen Sie, ob der Speicheradministrator für den Austausch des Switches bereit ist.
21. Entfernen Sie alle Kabel vom Switch old_cs1, und schließen Sie dann die Kabel an dieselben Ports am Switch New_cs1 an.
22. Aktivieren Sie auf dem cs2-Switch die ISL-Ports 13 bis 16.

Beispiel anzeigen

```
(cs2) config  
(cs2)(config) interface 0/13-0/16  
(cs2)(interface 0/13-0/16) #no shutdown
```

23. Aktivieren Sie die Ports auf dem neuen Switch, der den Clusterknoten zugeordnet ist.

Beispiel anzeigen

```
(cs2) config  
(cs2)(config) interface 0/1-0/12  
(cs2)(interface 0/13-0/16) #no shutdown
```

24. Rufen Sie auf einem einzelnen Node den Clusterknoten-Port auf, der mit dem ausgetauschten Switch verbunden ist, und bestätigen Sie anschließend, dass die Verbindung hergestellt ist.

Beispiel anzeigen

```
cluster::*> network port modify -node node1 -port  
<port_to_be_onlined> -up-admin true  
cluster::*> network port show -role cluster
```

25. Setzen Sie die Cluster-LIFs zurück, die dem Port in Schritt 25 auf demselben Node zugeordnet sind.

In diesem Beispiel werden die LIFs auf node1 erfolgreich zurückgesetzt, wenn die Spalte „is Home“ den Wert „true“ lautet.

Beispiel anzeigen

```
cluster::*> network interface revert -vserver node1 -lif  
<cluster_lif_to_be_reverted>  
cluster::*> network interface show -role cluster
```

26. Wenn die Cluster-LIF des ersten Node hochgefahren ist und auf den Home Port zurückgesetzt wird, wiederholen Sie die Schritte 25 und 26, um die Cluster-Ports hochzuschalten und die Cluster-LIFs auf den anderen Nodes im Cluster zurückzusetzen.
27. Zeigt Informationen zu den Nodes im Cluster an.

Beispiel anzeigen

```
cluster::*> cluster show
```

28. Vergewissern Sie sich, dass die Startkonfigurationsdatei und die laufende Konfigurationsdatei auf dem ersetzten Switch korrekt sind. Diese Konfigurationsdatei sollte mit der Ausgabe in Schritt 1 übereinstimmen.

Beispiel anzeigen

```
(new_cs1) >*enable*  
(new_cs1) #show running-config  
(new_cs1) #show startup-config
```

29. Wenn Sie die automatische Case-Erstellung unterdrückt haben, aktivieren Sie es erneut, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Ersetzen Sie NetApp CN1610 Cluster Switches durch Verbindungen ohne Switches

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

Prüfen Sie die Anforderungen

Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

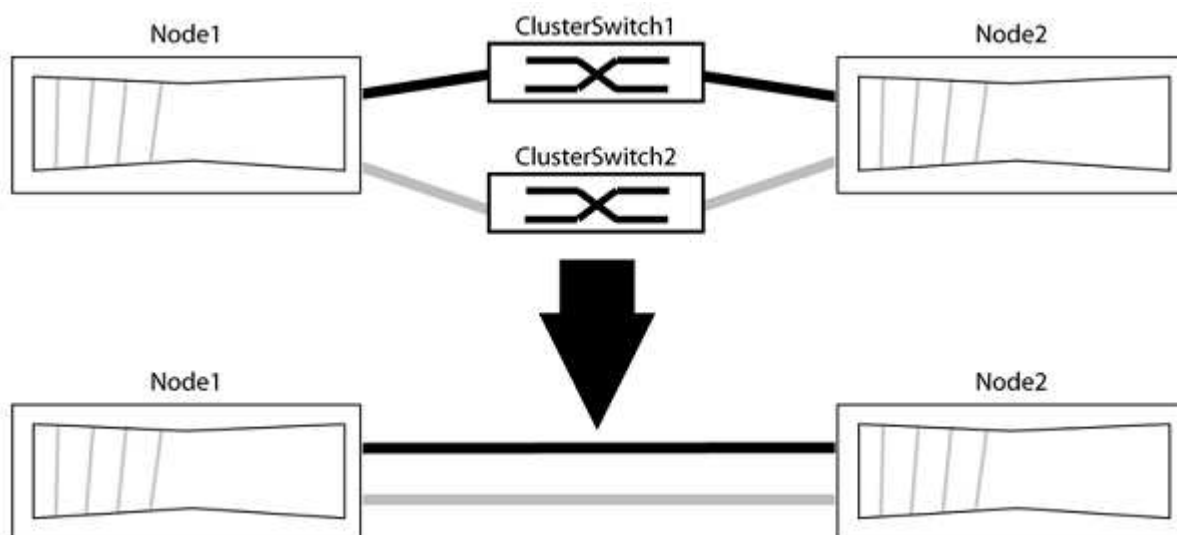
Was Sie benötigen

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

Migrieren Sie die Switches

Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben `y`. Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung `*>` Anzeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

```
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 „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. Wenn AutoSupport in diesem Cluster aktiviert ist, unterdrücken Sie die automatische Erstellung eines Falls durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message
MAINT=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

Beispiel anzeigen

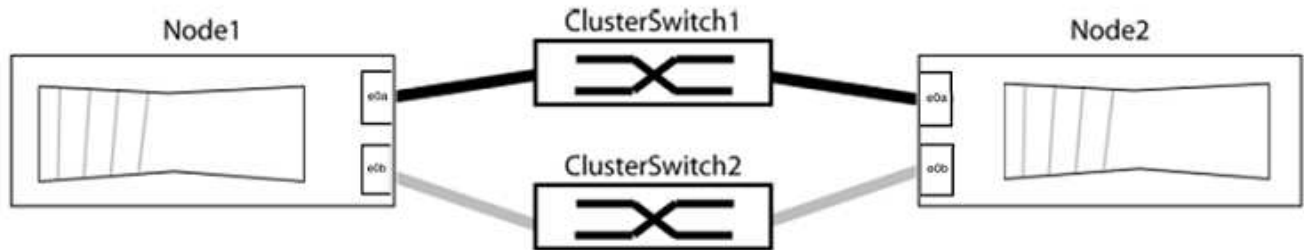
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Schritt: Ports und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in grop1 zu Cluster-Switch 1 wechseln und die Cluster-Ports in grop2 zu Cluster-Switch 2 wechseln. Diese Gruppen sind später im Verfahren erforderlich.
2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

```
network port show -ip space 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 Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



Überprüfen Sie, ob die Ports einen Wert von `up` für die Spalte „Link“ und einen Wert von `healthy` für die Spalte „Integritätsstatus“.

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 auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird `true` Für jedes 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.
```

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

```
network interface revert -vserver Cluster -lif *
```

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

```
network interface modify -vserver Cluster -lif * -auto-revert false
```

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

```
network device-discovery show -port cluster_port
```

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit 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 Cluster-Konnektivität:

```
cluster ping-cluster -node local
```

7. Vergewissern Sie sich, dass das Cluster sich in einem ordnungsgemäßen Zustand befindet:

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

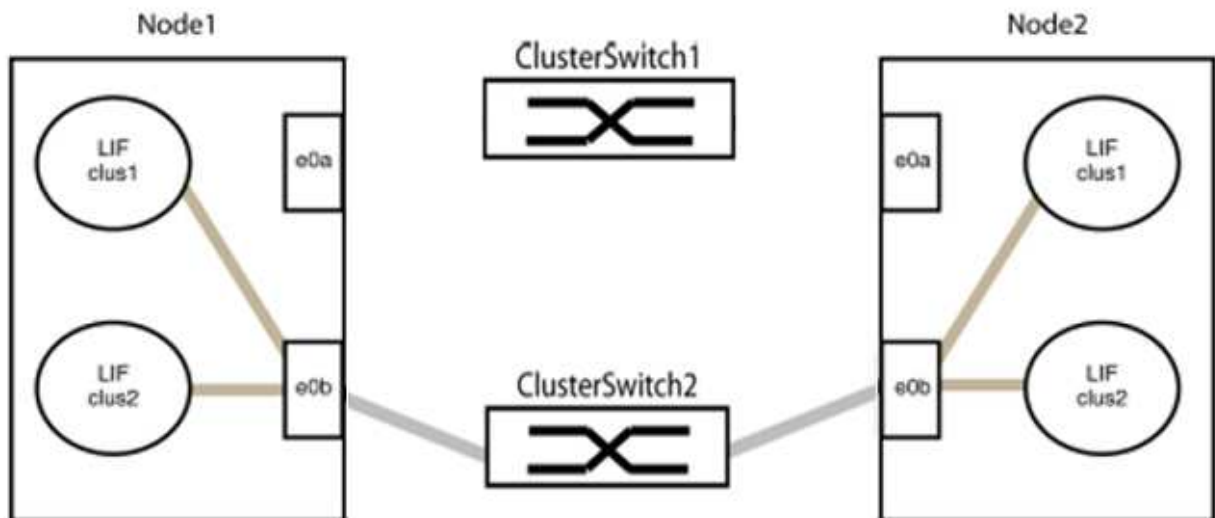
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

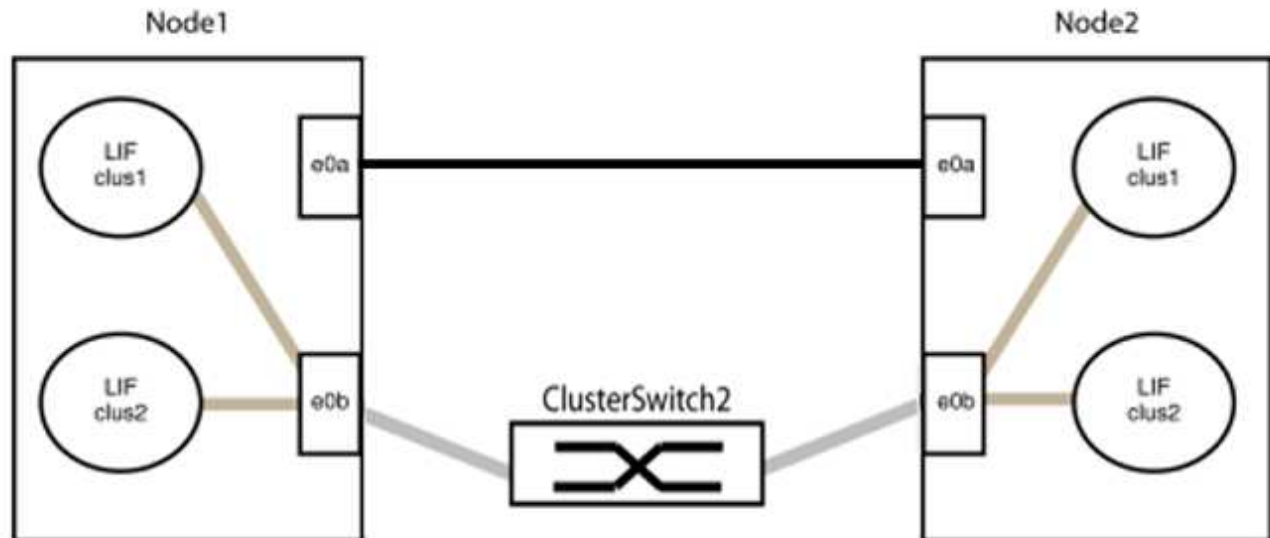
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



9. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

```
network options switchless-cluster show
```

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

10. Vergewissern Sie sich, dass das Cluster-Netzwerk nicht unterbrochen wird:

```
cluster ping-cluster -node local
```



Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung für Gruppe 1 zu bestätigen.

11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von `groerp2` trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in `Groupp2` ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

```
network device-discovery show -port cluster_port
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port auf dem Cluster-Partner 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. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

```
network interface modify -vserver Cluster -lif * -auto-revert true
```

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

```
network interface show -vserver Cluster -lif lif_name
```

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `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.
```

Wenn Cluster-LIFS nicht an die Home Ports zurückgegeben haben, setzen Sie sie manuell vom lokalen Node zurück:

```
network interface revert -vserver Cluster -lif lif_name
```

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

```
Node  Health  Eligibility Epsilon  
-----  
node1 true    true       false  
node2 true    true       false  
2 entries were displayed.
```

5. Bestätigen Sie die Verbindung zwischen den Cluster-Ports:

```
cluster ping-cluster local
```

6. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

7. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marken

NetApp, das NETAPP Logo und die auf der NetApp Markenseite aufgeführten Marken sind Marken von NetApp Inc. Andere Firmen- und Produktnamen können Marken der jeweiligen Eigentümer sein.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Datenschutzrichtlinie

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.