



Tauschen Sie die Schalter aus

Cluster and storage switches

NetApp
April 25, 2024

Inhalt

- Tauschen Sie die Schalter aus 1
 - Anforderungen für den Austausch von Cisco Nexus 3132Q-V Cluster Switches 1
 - Ersetzen Sie die Cisco Nexus 3132Q-V Cluster Switches. 4
 - Austausch von Cisco Nexus 3132Q-V Cluster-Switches durch Verbindungen ohne Switches 31

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, 1/2/2/3, 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/QSFP28 optische 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      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.

```

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					
		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				

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)
```

	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.

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.

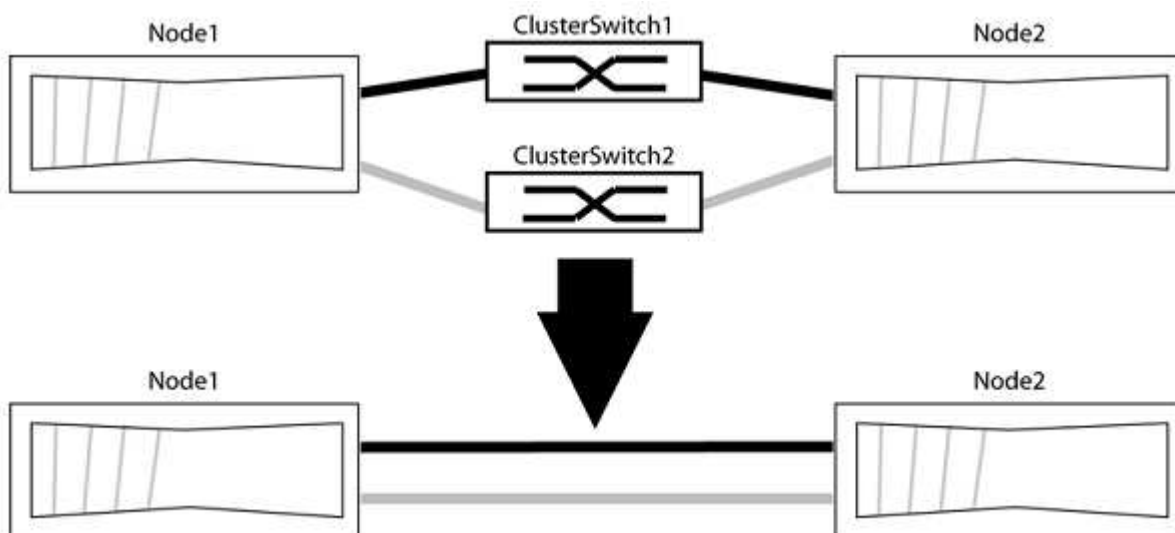
Was Sie benötigen

- 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 `*>` 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

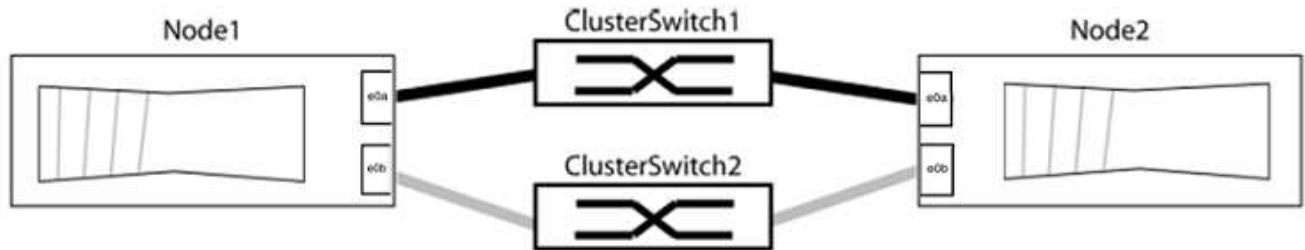
```
cluster::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

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.

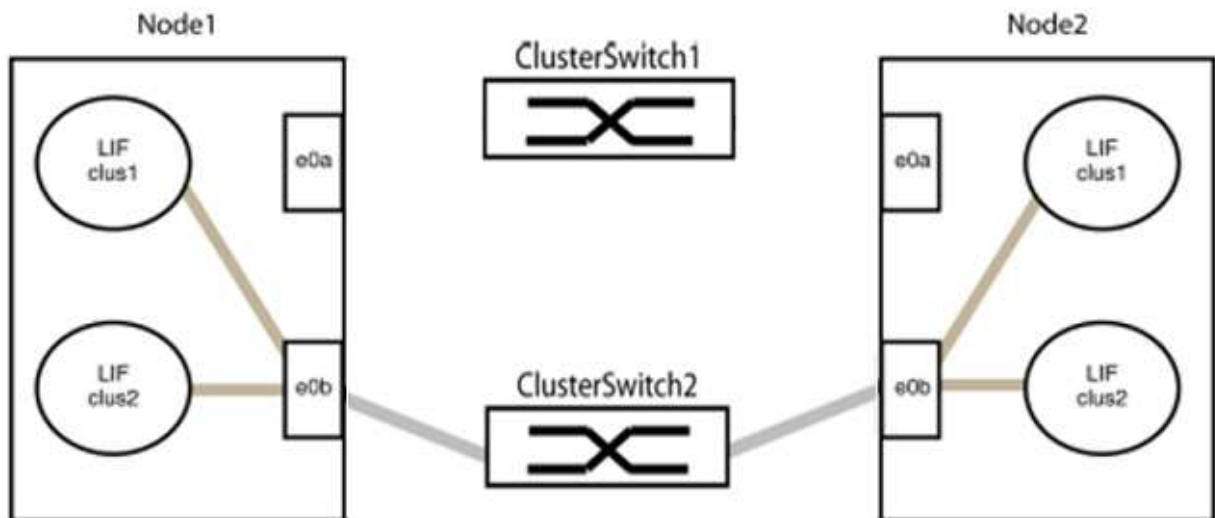
8. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



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**.

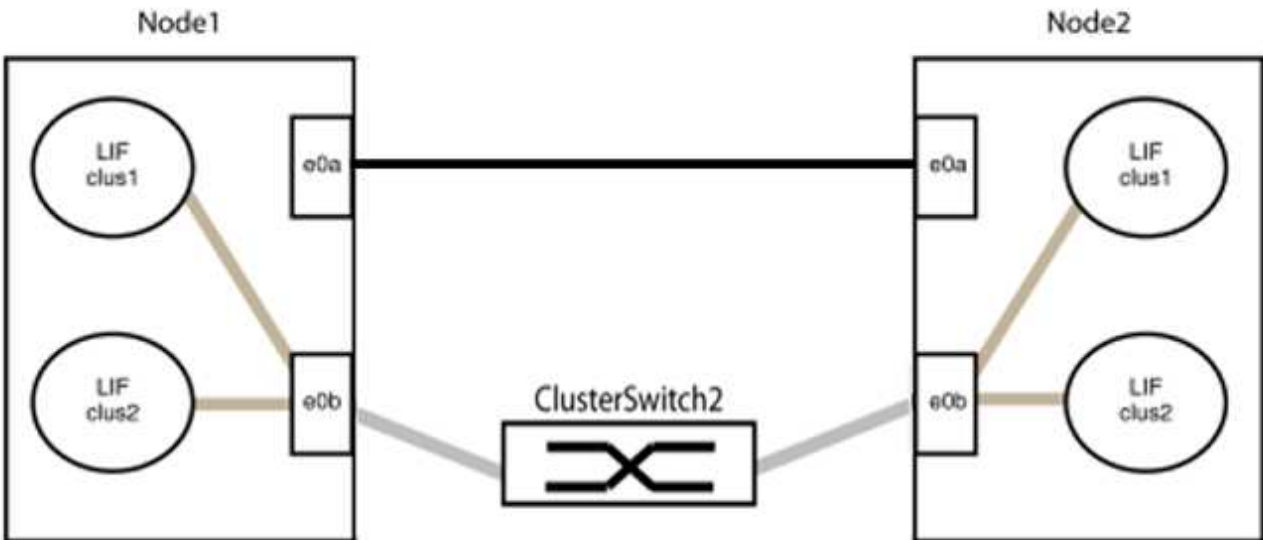
a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group1 ab.

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.

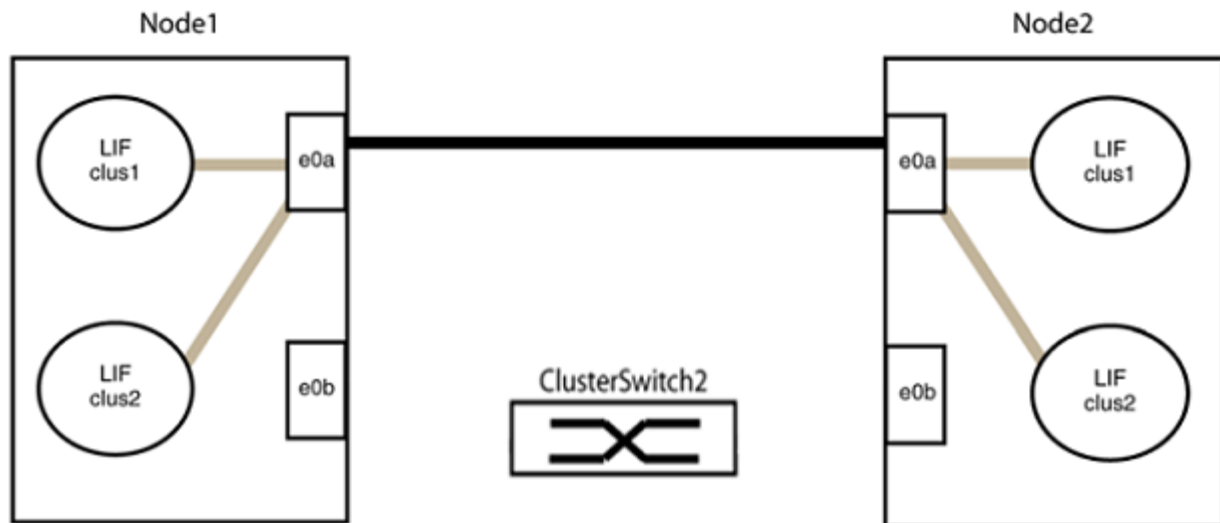
11. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



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**.

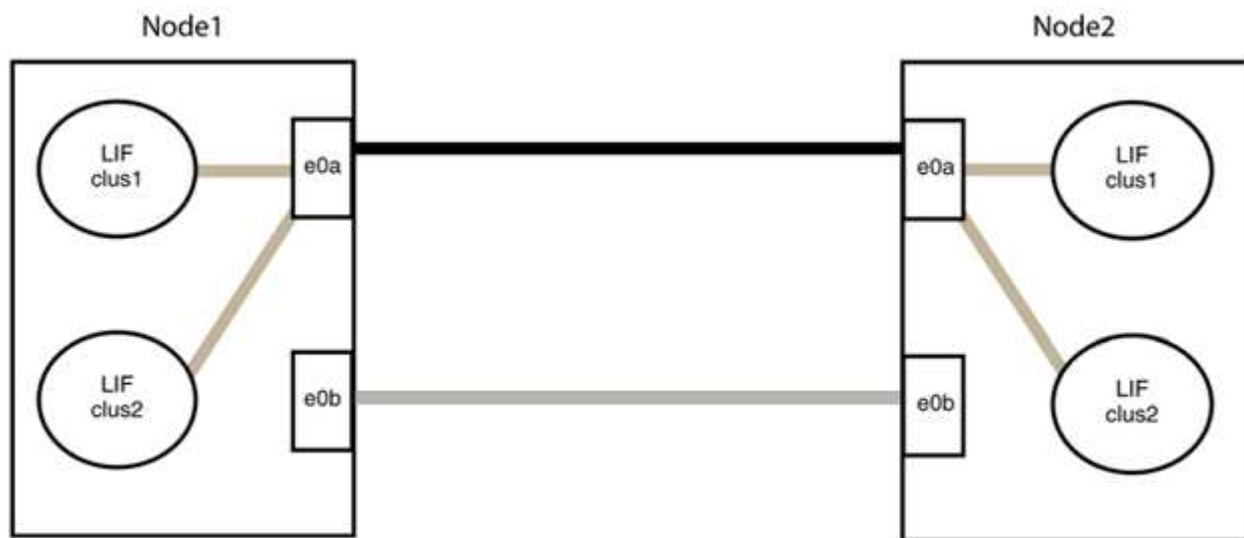
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in `Groupp2` ab.

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 unterdrücken, 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
```

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.