



Shared-Switches

Install and maintain

NetApp
November 07, 2025

This PDF was generated from <https://docs.netapp.com/de-de/ontap-systems-switches/switch-cisco-9336c-fx2-shared/configure-switch-overview-9336c-shared.html> on November 07, 2025. Always check docs.netapp.com for the latest.

Inhalt

Shared-Switches	1
Cisco Nexus 9336C-FX2	1
Los geht's	1
Installieren Sie die Hardware	3
Konfigurieren der Software	12
Switches migrieren	81
Ersetzen Sie einen gemeinsamen Cisco Nexus 9336C-FX2 Switch	120

Shared-Switches

Cisco Nexus 9336C-FX2

Los geht's

Installations- und Einrichtungsworkflow für gemeinsam genutzte 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.

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

1

"Überprüfen der Konfigurationsanforderungen"

Überprüfen Sie die Konfigurationsanforderungen für den gemeinsam genutzten Switch 9336C-FX2.

2

"Überprüfen Sie die Komponenten und Teilenummern"

Überprüfen Sie die Komponenten und Teilenummern für den gemeinsam genutzten Switch 9336C-FX2.

3

"Überprüfen Sie die erforderlichen Unterlagen"

Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 9336C-FX2-Switches und den ONTAP Cluster einzurichten.

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"](#).

Was kommt als nächstes

Nachdem Sie die Konfigurationsanforderungen geprüft haben, können Sie Ihre ["Komponenten und Teilenummern"](#)Die

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
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

Was kommt als nächstes

Nachdem Sie Ihre Komponenten und Teilenummern bestätigt haben, können Sie die folgenden überprüfen: ["erforderliche Dokumentation"](#)Die

Dokumentationsanforderungen für Cisco Nexus 9336C-FX2 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-Konfigurationsleitfäden" (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.

Installieren Sie die Hardware

Workflow zur Hardwareinstallation für gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches

Um die Hardware für einen gemeinsam genutzten Switch 9336C-FX2 zu installieren und zu konfigurieren, führen Sie die folgenden Schritte aus:

1

["Vervollständigen Sie das Verkabelungsarbeitsblatt"](#)

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"

Installieren Sie den Schalter 9336C-FX2.

3

"Den Switch in einen NetApp-Schrank einbauen"

Installieren Sie den 9336C-FX2-Switch und das Durchgangspanel nach Bedarf in einem NetApp Schrank.

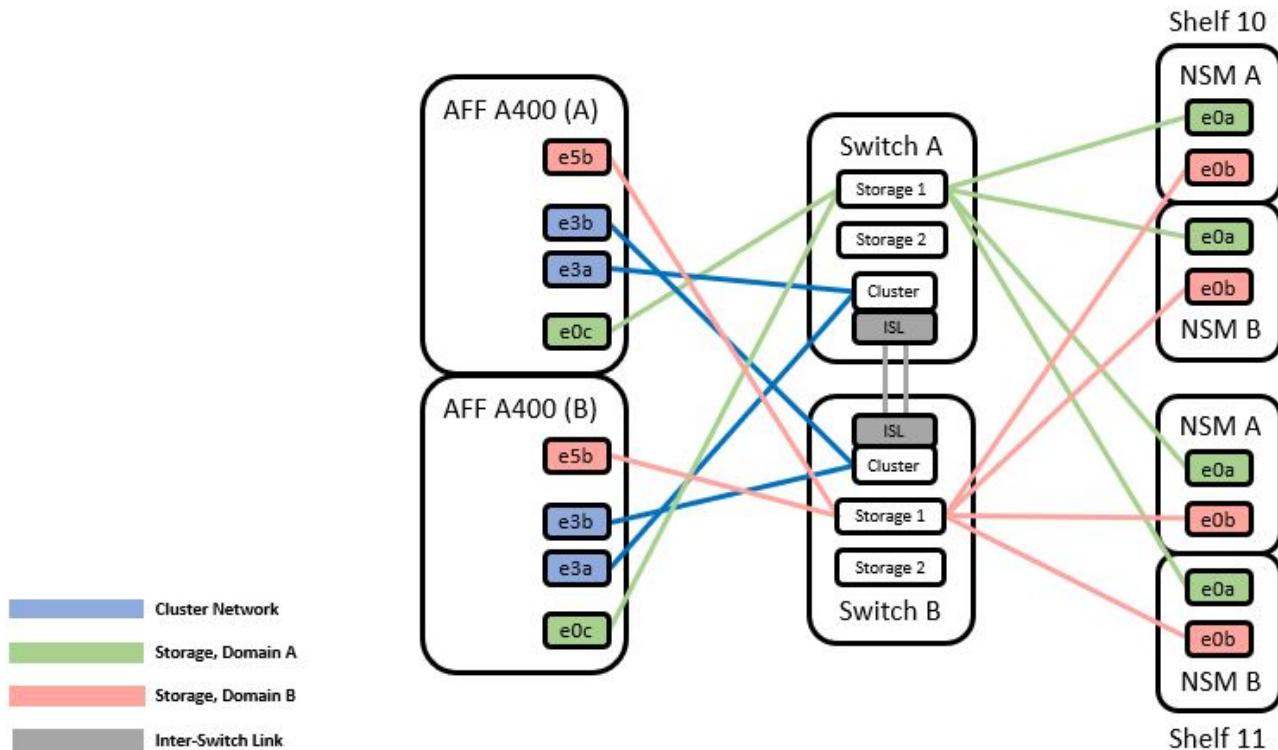
Füllen Sie das Cisco Nexus 9336C-FX2-Verkabelungsarbeitsblatt aus

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

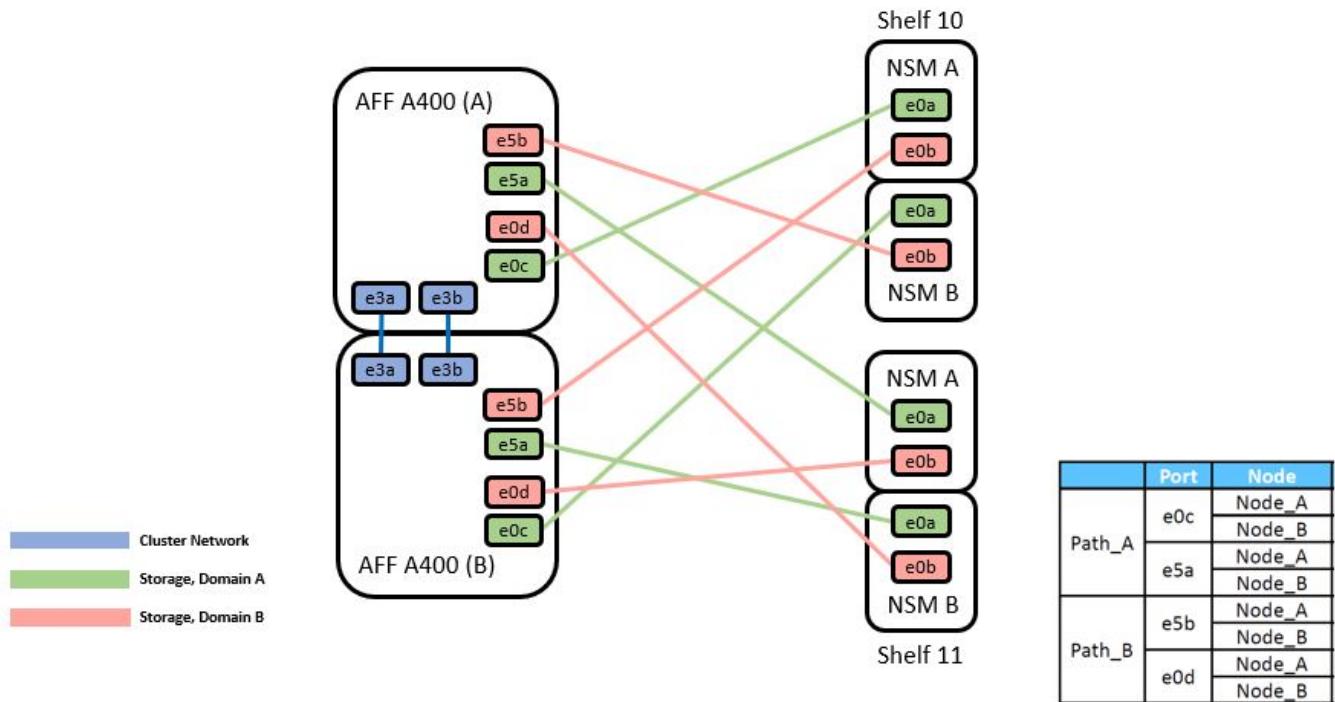


Siehe "Hardware Universe" Weitere Informationen zu Switch-Ports.

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:

Direct Attached



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		Switch Port	Switch B	
	Port Role	Port Usage		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

Was kommt als nächstes

Nachdem Sie Ihre Verkabelungsarbeitsblätter ausgefüllt haben, können Sie ["Installieren Sie den Schalter"](#) Die

Installieren Sie gemeinsam genutzte Cisco Nexus 9336C-FX2 Switches

Befolgen Sie diese Anweisungen, um gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches zu konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- 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

Im "[Anweisungen zum Rack](#)" erfahren Sie, wie Sie den Switch in einem NetApp-Schrank einmontieren.

2. Schalten Sie die Switches, Controller und NS224 NVMe Storage-Shelfs ein.

Was kommt als Nächstes?

Optional können Sie "[Installation eines Cisco Nexus 9336C-FX2 Switch in einem NetApp Rack](#)" . Andernfalls gehen Sie zu "[Konfigurieren Sie den Switch](#)".

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.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- 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).

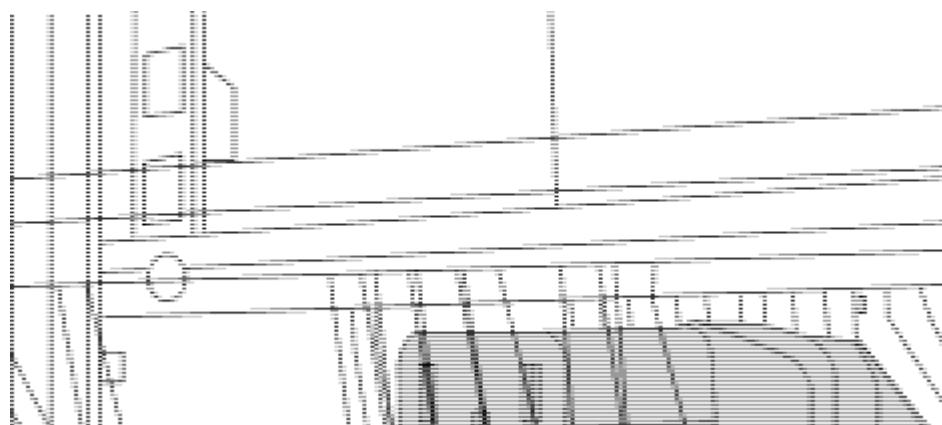
Das NetApp Pass-Through-Panel-Kit enthält die folgende Hardware:

- 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.

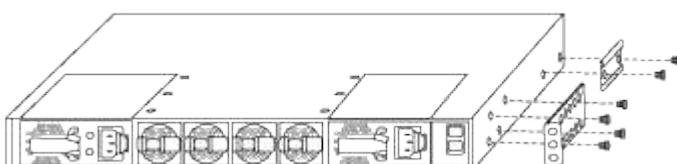
- ii. Bringen Sie an jeder Seite zwei Klemmmuttern an den entsprechenden quadratischen Löchern für die vorderen Schrankschienen an.
- iii. Zentrieren Sie die Abdeckung senkrecht, um ein Eindringen in den benachbarten Rack zu verhindern, und ziehen Sie die Schrauben fest.
- iv. Stecken Sie die Buchsen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



(1) Buchsenleiste des Überbrückungskabels.

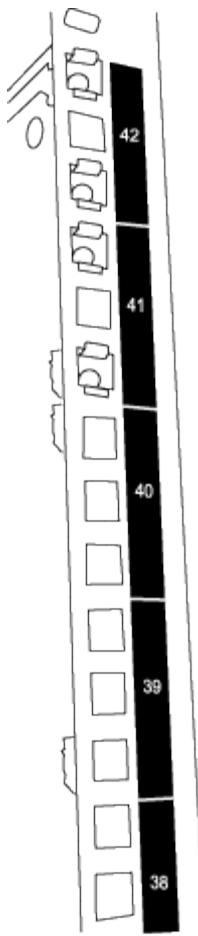
2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Gehäuse des Nexus 9336C-FX2.

- 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 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.

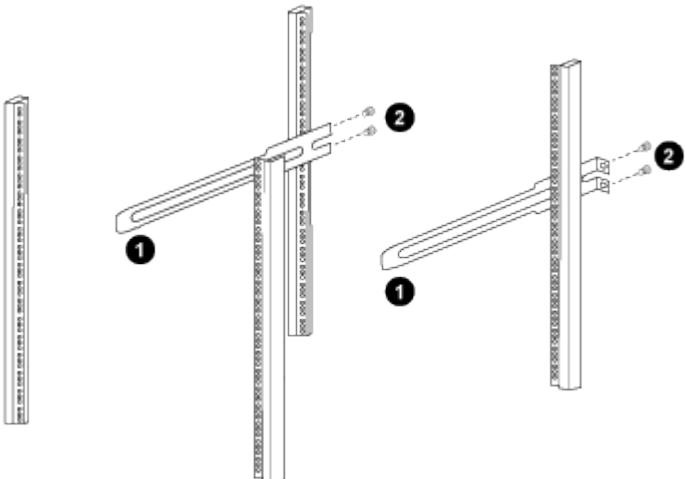
3. Die Klemmmuttern für alle vier IEA-Stützen an den Stellen der quadratischen Bohrung anbringen.



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

4. Installieren Sie die Gleitschienen im Schrank.

- 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.

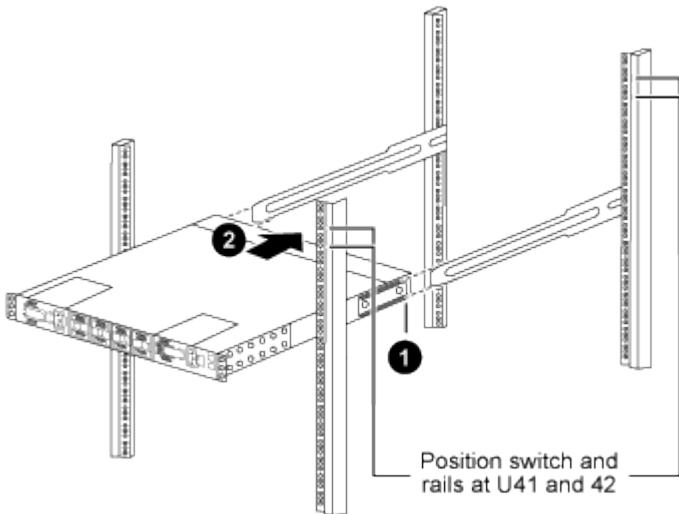
(2) Schrauben der Gleitschienen an den Schrankleisten festziehen.

- 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.

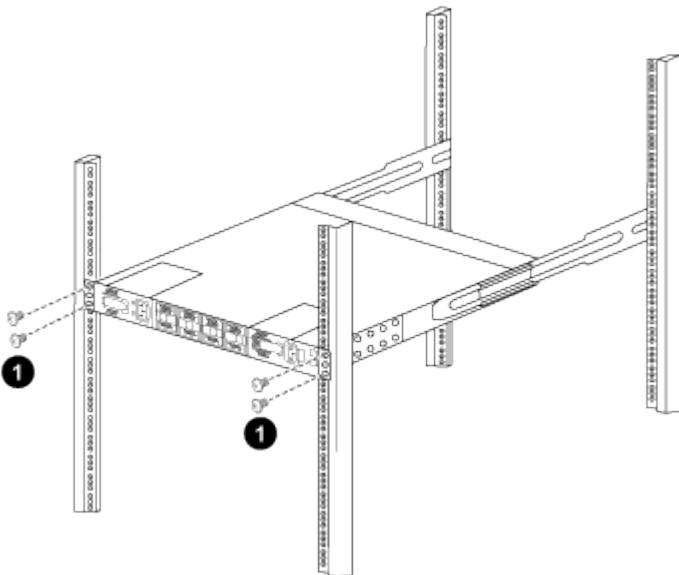
- a. Positionieren Sie die Rückseite des Schalters an RU41.



(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.



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.

Konfigurieren der Software

Workflow für die Softwareinstallation für gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches

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

1

"Konfigurieren Sie den Switch"

Konfigurieren Sie den gemeinsam genutzten Switch 9336C-FX2.

2

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

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

3

"Installieren oder aktualisieren Sie die NX-OS-Software"

Laden Sie die NX-OS-Software herunter und installieren oder aktualisieren Sie sie auf dem gemeinsam genutzten Cisco 9336C-FX2-Switch.

4

"Installieren Sie das RCF"

Installieren Sie das RCF, nachdem Sie den gemeinsam genutzten Cisco 9336C-FX2-Switch zum ersten Mal eingerichtet haben.

5

"Aktualisieren Sie Ihren RCF"

Aktualisieren Sie Ihre RCF-Version, wenn auf Ihren Betriebs-Switches eine vorhandene Version der RCF-Datei installiert ist.

6

"Setzen Sie den Switch auf die Werkseinstellungen zurück"

Löschen Sie die Einstellungen des gemeinsam genutzten Switches 9336C-FX2.

Konfigurieren Sie gemeinsam genutzte Cisco Nexus 9336C-FX2 Switches

Befolgen Sie diese Anweisungen, um gemeinsam genutzte Cisco Nexus 9336C-FX2-Switches zu konfigurieren.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- 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 erstellenenden 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 der Ethernet Switch Health Monitor (CSHM) für die Protokollerfassungsfunktionen verwendet wird. 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?

Nachdem Sie Ihre Schalter konfiguriert haben, können Sie ["Bereiten Sie die Installation von NX-OS und RCF vor"](#) Die

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:

Vorgeschlagene Dokumentation

- ["Cisco Ethernet Switch Seite"](#)

In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.

- ["Software-Upgrade- und Downgrade-Anleitungen"](#)

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

- ["Cisco Nexus 9000 und 3000 Upgrade und ISSU Matrix"](#)

Bietet Informationen zu disruptiven Upgrades/Downgrades für die Cisco NX-OS-Software auf Nexus 9000 Series Switches basierend auf Ihren aktuellen und Zielversionen.

Wählen Sie auf der Seite **Disruptive Upgrade** aus, und wählen Sie aus der Dropdown-Liste Ihr aktuelles Release und Ihr Ziel-Release aus.

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_clus1 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/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform

-----
-----  

cluster1-02/cdp
      e0a    cs1          Eth1/2      N9K-
C9336C
      e0b    cs2          Eth1/2      N9K-
C9336C
cluster1-01/cdp
      e0a    cs1          Eth1/1      N9K-
C9336C
      e0b    cs2          Eth1/1      N9K-
C9336C

4 entries were displayed.
```

4. 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

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
        cluster1-01_clus1  up/up      169.254.209.69/16
cluster1-01  e0a      true
        cluster1-01_clus2  up/up      169.254.49.125/16
cluster1-01  e0b      true
        cluster1-02_clus1  up/up      169.254.47.194/16
cluster1-02  e0a      true
        cluster1-02_clus2  up/up      169.254.19.183/16
cluster1-02  e0b      true

4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
                                         LIF           LIF
Packet
Node   Date
Loss
-----
```

Node	Date	Source	Destination
node1	3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-clus1
	3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
node2	3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
	3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2

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

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

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

```

1. Stellen Sie sicher, dass der Befehl zum automatischen Zurücksetzen auf allen Cluster-LIFs aktiviert ist:

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

Beispiel anzeigen

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

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

Was kommt als Nächstes?

Nachdem Sie die Installation der NX-OS-Software und von RCF vorbereitet haben, können Sie "["Installieren Sie die NX-OS-Software"](#) Die

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

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).

Vorgeschlagene Dokumentation

- "["Cisco Ethernet Switch Seite"](#)

In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und NX-OS-Versionen.

- "["Software-Upgrade- und Downgrade-Anleitungen"](#)

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

- "["Cisco Nexus 9000 und 3000 Upgrade und ISSU Matrix"](#)

Enthält Informationen zu störenden Upgrades/Downgrades für Cisco NX-OS-Software auf Switches der

Nexus 9000-Serie

Basierend auf Ihren aktuellen und Zielversionen.

Wählen Sie auf der Seite **Disruptive Upgrade** aus, und wählen Sie aus der Dropdown-Liste Ihr aktuelles Release und Ihr Ziel-Release aus.

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_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.

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 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. 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
C9336C-FX2
    e0d    cs2
C9336C-FX2
cluster1-02/cdp
    e0a    cs1
C9336C-FX2
    e0d    cs2
C9336C-FX2
cluster1-03/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1-04/cdp
    e0a    cs1
C9336C-FX2
    e0b    cs2
C9336C-FX2
cluster1::*>
```

4. 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

          Speed (Mbps)

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

```

- b. 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
  Port        Home
  Admin/Oper  Address/Mask      Node
  -----
  -----
  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-FX2
    Serial Number: FOCXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
          9.3(5)
    Version Source: CDP

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

5. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs. Die Cluster-LIFs führen ein Failover zum Partner-Cluster-Switch durch und bleiben dort, während Sie das Upgrade-Verfahren für den Ziel-Switch durchführen:

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

6. 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.
```

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

```
show version
```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own

licenses, such as open source. This software is provided "as is,"
and unless

otherwise stated, there is no warranty, express or implied,
including but not

limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/library.txt.
```

Software

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

Hardware

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

Processor Board ID FOC20291J6K
```

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

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

  plugin
    Core Plugin, Ethernet Plugin

  Active Package(s):

cs2#
```

8. Installieren Sie das NX-OS Image.

Durch die Installation der Image-Datei wird 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.
```

9. Überprüfen Sie nach dem Neustart des Switches die neue Version der NX-OS-Software:

```
show version
```

Beispiel anzeigen

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source. This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.

Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.

A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
BIOS: version 05.33
NXOS: version 9.3(5)
BIOS compile time: 09/08/2018
NXOS image file is: bootflash:///nxos.9.3.5.bin
NXOS compile time: 11/4/2018 21:00:00 [11/05/2018 06:11:06]

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

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

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
  Reason: Reset due to upgrade
  System version: 9.3(4)
  Service:

  plugin
    Core Plugin, Ethernet Plugin

  Active Package(s):
```

10. Aktualisieren Sie das EPLD-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

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module all
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

Module Required	Type	EPLD	Running-Version	New-Version	Upg-
1	SUP	MI FPGA	0x07	0x07	No
1	SUP	IO FPGA	0x17	0x19	Yes
1	SUP	MI FPGA2	0x02	0x02	No

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

Do you want to continue (y/n) ? [n] **y**

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

11. 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
```

12. 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 -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-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      N9K-
C9336C-FX2
    e0d    cs2                      Ethernet1/7      N9K-
C9336C-FX2
cluster01-2/cdp
    e0a    cs1                      Ethernet1/8      N9K-
C9336C-FX2
    e0d    cs2                      Ethernet1/8      N9K-
C9336C-FX2
cluster01-3/cdp
    e0a    cs1                      Ethernet1/1/1    N9K-
C9336C-FX2
    e0b    cs2                      Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
    e0a    cs1                      Ethernet1/1/2    N9K-
C9336C-FX2
    e0b    cs2                      Ethernet1/1/2    N9K-
C9336C-FX2

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

-----
-----
cs1                   cluster-network  10.233.205.90  N9K-
C9336C-FX2
    Serial Number: FOCXXXXXXXGD
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
    9.3 (5)
    Version Source: CDP

cs2                   cluster-network  10.233.205.91  N9K-
```

```
C9336C-FX2
```

```
    Serial Number: FOCXXXXXXGS
    Is Monitored: true
    Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
        9.3(5)
    Version Source: CDP
```

```
2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version 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:
Unlocking 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. 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 6 bis 13, um die NX-OS-Software auf Switch cs1 zu installieren.

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

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

16. 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 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>
```

Was kommt als Nächstes?

Nach der Installation der NX-OS-Software können Sie ["Installieren Sie den RCF"](#) Die

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können die Referenzkonfigurationsdatei (RCF) nach dem ersten Einrichten des Nexus 9336C-FX2-Switches installieren.

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

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Eine Konsolenverbindung zum Switch. Die Konsolenverbindung ist optional, wenn Sie Remote-Zugriff auf den Switch haben.
- Switch cs1 und Switch cs2 werden eingeschaltet und die Ersteinrichtung des Switches ist abgeschlossen (die Management-IP-Adresse und SSH sind eingerichtet).
- Die gewünschte NX-OS-Version wurde installiert.
- ISL-Verbindungen (Inter-Switch Link) zwischen Switches sind angeschlossen.
- Die ONTAP Node-Cluster-Ports sind nicht verbunden.

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich an, um cs1 über SSH oder über eine serielle Konsole zu wechseln.
2. Kopieren Sie den RCF mit einem der folgenden Übertragungsprotokolle auf den Bootflash von Switch cs1: FTP, TFTP, SFTP oder SCP.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)".

Beispiel anzeigen

Dieses Beispiel zeigt TFTP, mit dem eine RCF in den Bootflash auf Switch cs1 kopiert wird:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

3. Wenden Sie die 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](#)".

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` Installation auf Switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

4. 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

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date        : 10-23-2020
* Version     : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in config
mode:
* no interface breakout module 1 port <range> map 10g-4x
* no interface breakout module 1 port <range> map 25g-4x
* interface Ethernet <interfaces taken out of breakout mode>
* inherit port-profile 40-100G
* priority-flow-control mode auto
* service-policy input HA
* exit
*
*****
*****
```

5. 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.

6. Notieren Sie alle benutzerdefinierten Ergänzungen zwischen dem aktuellen `running-config` Datei und die verwendete RCF-Datei.
7. Nachdem Sie überprüft haben, dass die RCF-Versionen und Schaltereinstellungen korrekt sind, kopieren Sie die `running-config` Datei in die `startup-config` Datei.

```
cs1# copy running-config startup-config
[#####] 100% Copy complete
```

8. Speichern Sie grundlegende Konfigurationsdetails im `write_erase.cfg` Datei auf dem Bootflash.

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Führen Sie für RCF Version 1.12 und höher die folgenden Befehle aus:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg

cs1# echo "hardware access-list tcam region ing-l2-qos 1280" >>
bootflash:write_erase.cfg
```

Siehe den Knowledge Base-Artikel "[Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung](#)" für weitere Details.

10. Überprüfen Sie, ob die `write_erase.cfg` Die Datei wird wie erwartet ausgefüllt:

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

11. Führen Sie den Befehl zum Löschen des Schreibvorgangs aus, um die aktuell gespeicherte Konfiguration zu löschen:

```
cs1# write erase
```

```
Warning: This command will erase the startup-configuration.
```

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

12. Kopieren Sie die zuvor gespeicherte Grundkonfiguration in die Startkonfiguration.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

13. Starten Sie den Switch cs1 neu.

```
cs1# reload
```

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

14. Wiederholen Sie die Schritte 1 bis 13 auf Switch cs2.

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

Schritt 2: Überprüfen Sie die Switch-Verbindungen

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 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	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
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, Eth1/23, Eth1/24, Eth1/25

Eth1/28			Eth1/26, Eth1/27,
Eth1/31			Eth1/29, Eth1/30,
Eth1/34			Eth1/32, Eth1/33,
33 VLAN0033	active		Eth1/11, Eth1/12,
Eth1/13			Eth1/14, Eth1/15,
Eth1/16			Eth1/17, Eth1/18,
Eth1/19			Eth1/20, Eth1/21,
Eth1/22			Eth1/23, Eth1/24,
34 VLAN0034	active		Eth1/26, Eth1/27,
Eth1/25			Eth1/29, Eth1/30,
Eth1/28			Eth1/32, Eth1/33,
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
Po1	1
..	
..	
..	
..	
..	



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

3. 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      Eth1/35 (P)    Eth1/36 (P)
cs1#
```

Schritt 3: Richten Sie Ihren ONTAP-Cluster ein

NetApp empfiehlt, zum Einrichten neuer Cluster System Manager zu verwenden.

System Manager bietet einen einfachen und einfachen Workflow für die Cluster-Einrichtung und -Konfiguration einschließlich der Zuweisung einer Node-Management-IP-Adresse, Initialisierung des Clusters, Erstellung eines lokalen Tiers, Konfiguration von Protokollen und Bereitstellung des anfänglichen Storage.

Gehen Sie zu "[Konfigurieren Sie ONTAP mit System Manager in einem neuen Cluster](#)" Für Setup-Anweisungen.

Was kommt als Nächstes?

Nach der Installation des RCF können Sie "[Konfigurieren der Switch-Integritätsüberwachung](#)" Die

Aktualisieren der Referenzkonfigurationsdatei (RCF)

Sie aktualisieren Ihre RCF-Version, wenn auf Ihren Betriebsschaltern eine vorhandene Version der RCF-Datei installiert ist.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Der aktuelle RZB.
- Wenn Sie Ihre RCF-Version aktualisieren, benötigen Sie eine Startkonfiguration im RCF, die die gewünschten Startabbilder widerspiegelt.

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 instanziert wird.

 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 oder grundlegende Konfigurationsinformationen beibehalten haben, bevor Sie die Switch-Einstellungen löschen.

Schritt 1: Bereiten Sie sich auf das Upgrade vor

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
C9336C
    e0d    cs2
C9336C
cluster1-02/cdp
    e0a    cs1
C9336C
    e0d    cs2
C9336C
cluster1-03/cdp
    e0a    cs1
C9336C
    e0b    cs2
C9336C
cluster1-04/cdp
    e0a    cs1
C9336C
    e0b    cs2
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

          Speed (Mbps)

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

```

- b. 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
  Port        Home
  Admin/Oper  Address/Mask      Node
  -----
  -----
  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.

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

Schritt 2: Ports konfigurieren

1. Fahren Sie beim Cluster-Switch cs1 die mit den Cluster-Ports der Nodes verbundenen Ports herunter.

```
cs1(config)# interface eth1/1/1-2,eth1/7-8
```

```
cs1(config-if-range)# shutdown
```

 Stellen Sie sicher, dass Sie **alle** verbundenen Cluster-Ports herunterfahren, um Probleme mit der Netzwerkverbindung zu vermeiden. ["Kein Quorum mehr aus dem Node bei der Migration von LIF auf Cluster während des Upgrades des Switch-Betriebssystems"](#) Weitere Informationen finden Sie im Knowledge Base-Artikel.

2. 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 -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
```

- a. Notieren Sie alle benutzerdefinierten Ergänzungen zwischen der aktuellen Running-config und der verwendeten RCF-Datei (z. B. eine SNMP-Konfiguration für Ihr Unternehmen).
- b. Verwenden Sie für NX-OS 10.2 und höher den Befehl, show diff running-config um mit der gespeicherten RCF-Datei im Bootflash zu vergleichen. Verwenden Sie andernfalls ein diff- oder Vergleichstool eines Drittanbieters.

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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg
cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg
cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

6. Führen Sie für RCF Version 1.12 und höher die folgenden Befehle aus:

```
cs1# echo "hardware access-list tcam region ing-racl 1024" >>
bootflash:write_erase.cfg
cs1# echo "hardware access-list tcam region egr-racl 1024" >>
bootflash:write_erase.cfg
cs1# echo "hardware access-list tcam region ing-12-qos 1280" >>
bootflash:write_erase.cfg
```

Siehe den Knowledge Base-Artikel "["Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung"](#)" für weitere Details.

7. Überprüfen Sie, ob die Datei write_erase.cfg wie erwartet gefüllt ist:

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

8. Führen Sie den Befehl zum Löschen des Schreibvorgangs aus, um die aktuell gespeicherte Konfiguration zu löschen:

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

9. Kopieren Sie die zuvor gespeicherte Grundkonfiguration in die Startkonfiguration.

```
cs1# copy bootflash:write_erase.cfg startup-config
```

10. Führen Sie einen Neustart des Switches aus:

```
switch# reload
```

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

11. Nachdem die Management-IP-Adresse wieder erreichbar ist, melden Sie sich über SSH beim Switch an.

Möglicherweise müssen Sie die Einträge der Host-Datei im Zusammenhang mit den SSH-Schlüsseln aktualisieren.

12. Kopieren Sie den RCF mit einem der folgenden Übertragungsprotokolle auf den Bootflash von Switch cs1: FTP, TFTP, SFTP oder SCP.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im "[Cisco Nexus 9000-Serie NX-OS Command Reference](#)" Leitfäden.

Beispiel anzeigen

Dieses Beispiel zeigt TFTP, mit dem eine RCF in den Bootflash auf Switch cs1 kopiert wird:

```
cs1# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

13. Wenden Sie die 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](#)" Leitfäden.

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei `Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt` Installation auf Switch cs1:

```
cs1# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

14. 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

```
cs1# show banner motd

*****
*****
* NetApp Reference Configuration File (RCF)
*
* Switch      : Nexus N9K-C9336C-FX2
* Filename    : Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
* Date        : 10-23-2020
* Version     : v1.6
*
* Port Usage:
* Ports 1- 3: Breakout mode (4x10G) Intra-Cluster Ports, int
e1/1/1-4, e1/2/1-4
, e1/3/1-4
* Ports 4- 6: Breakout mode (4x25G) Intra-Cluster/HA Ports, int
e1/4/1-4, e1/5/
1-4, e1/6/1-4
* Ports 7-34: 40/100GbE Intra-Cluster/HA Ports, int e1/7-34
* Ports 35-36: Intra-Cluster ISL Ports, int e1/35-36
*
* Dynamic breakout commands:
* 10G: interface breakout module 1 port <range> map 10g-4x
* 25G: interface breakout module 1 port <range> map 25g-4x
*
* Undo breakout commands and return interfaces to 40/100G
configuration in config
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
*
*****
*****
```

15. 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.

16. Wenden Sie alle vorherigen Anpassungen erneut auf die Switch-Konfiguration an.
17. Nachdem Sie überprüft haben, ob die RCF-Versionen, die benutzerdefinierten Ergänzungen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Startup-config-Datei.

Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im ["Cisco Nexus 9000-Serie NX-OS Command Reference"](#) Leitfäden.

```
cs1# copy running-config startup-config  
[] 100% Copy complete
```

18. Starten Sie den Switch cs1 neu. Sie können die Warnmeldungen „Cluster-Switch-Systemzustandsüberwachung“ und die Ereignisse „Cluster-Ports ausgefallen“, die von den Nodes gemeldet werden, ignorieren, während der Switch neu gebootet wird.

```
cs1# reload
```

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

19. 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 -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-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      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:
Unlocking 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.
```

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 1 bis 20 am Schalter cs2.

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

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

Schritt 3: Überprüfen Sie die Cluster-Netzwerkkonfiguration und den Zustand des Clusters

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
cs1            Eth1/35      175      R S I s      N9K-C9336C
Eth1/35
cs1            Eth1/36      175      R S I s      N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Überprüfen Sie 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    Po1, Eth1/1, Eth1/2,
                                              Eth1/3
                                              Eth1/4, Eth1/5,
                                              Eth1/6, Eth1/7
                                              Eth1/8, Eth1/35,
                                              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
                                              Eth1/23, Eth1/24,
32     VLAN0032                          active    Eth1/25
```

Eth1/28			Eth1/26, Eth1/27,
Eth1/31			Eth1/29, Eth1/30,
Eth1/34			Eth1/32, Eth1/33,
33 VLAN0033	active		Eth1/11, Eth1/12,
Eth1/13			Eth1/14, Eth1/15,
Eth1/16			Eth1/17, Eth1/18,
Eth1/19			Eth1/20, Eth1/21,
Eth1/22			Eth1/23, Eth1/24,
34 VLAN0034	active		Eth1/26, Eth1/27,
Eth1/25			Eth1/29, Eth1/30,
Eth1/28			Eth1/32, Eth1/33,
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
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      Po1 (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::*>
```

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

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

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. 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 anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
                                         LIF           LIF
Packet
Node   Date
Loss
-----
```

Node	Date	Source	Destination
node1	3/5/2022 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-clus1
	3/5/2022 19:21:20 -06:00	cluster1-01_clus2	cluster1-02_clus2
node2	3/5/2022 19:21:18 -06:00	cluster1-02_clus2	cluster1-01_clus1
	3/5/2022 19:21:20 -06:00	cluster1-02_clus2	cluster1-01_clus2

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 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)

```

Was kommt als Nächstes?

Nach dem Upgrade des RCF können Sie ["Konfigurieren der Switch-Integritätsüberwachung"](#) Die

Setzen Sie den gemeinsam genutzten Switch 9336C-FX2 auf die Werkseinstellungen zurück

Um den gemeinsam genutzten Switch 9336C-FX2 auf die Werkseinstellungen

zurückzusetzen, müssen Sie die Switch-Einstellungen 9336C-FX2 löschen.

Über diese Aufgabe

- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Löschen Sie die vorhandene Konfiguration:

```
write erase
```

```
(cs2) # write erase
```

```
Warning: This command will erase the startup-configuration.  
Do you wish to proceed anyway? (y/n) [n] y
```

2. Laden Sie die Switch-Software neu:

```
reload
```

```
(cs2) # reload
```

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

Das System wird neu gestartet und der Konfigurationsassistent wird aufgerufen. Wenn Sie während des Startvorgangs die Aufforderung „Auto Provisioning abbrechen und mit der normalen Einrichtung fortfahren?“ erhalten, (ja/nein)[n]“, sollten Sie mit **ja** antworten, um fortfahren.

Was kommt als nächstes

Nachdem Sie Ihre Schalter zurückgesetzt haben, können Sie "neu konfigurieren" sie nach Bedarf.

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

                                         Speed (Mbps)
Health
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

                                         Speed (Mbps)
Health
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
      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.
```

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                                         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.
```

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.

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. 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 anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
                                         LIF           LIF
Packet
Node    Date
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 local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. Ändern Sie die Berechtigungsebene zurück zu admin:

```
set -privilege admin
```

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
                                         Speed
VLAN
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
30
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
30
```

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
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
30
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
30
```

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
                                         Speed
VLAN
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
30
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
30
```

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
```

Was kommt als Nächstes?

Nach der Migration Ihrer Switches können Sie "[Konfigurieren der Switch-Integritätsüberwachung](#)" Die

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
      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      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
      Logical          Status      Network      Current      Current
  Is
  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::*
```

13. Schalter c1 durch den neuen Schalter sh1 ersetzen und den neuen Schalter neu verkabeln.
14. Überprüfen Sie, ob die Anschlüsse auf sh1 gesichert sind. **Hinweis** dass sich die LIFs noch auf Schalter c2 befinden.
15. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

Beispiel anzeigen

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

16. 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::*>
```

Was kommt als Nächstes?

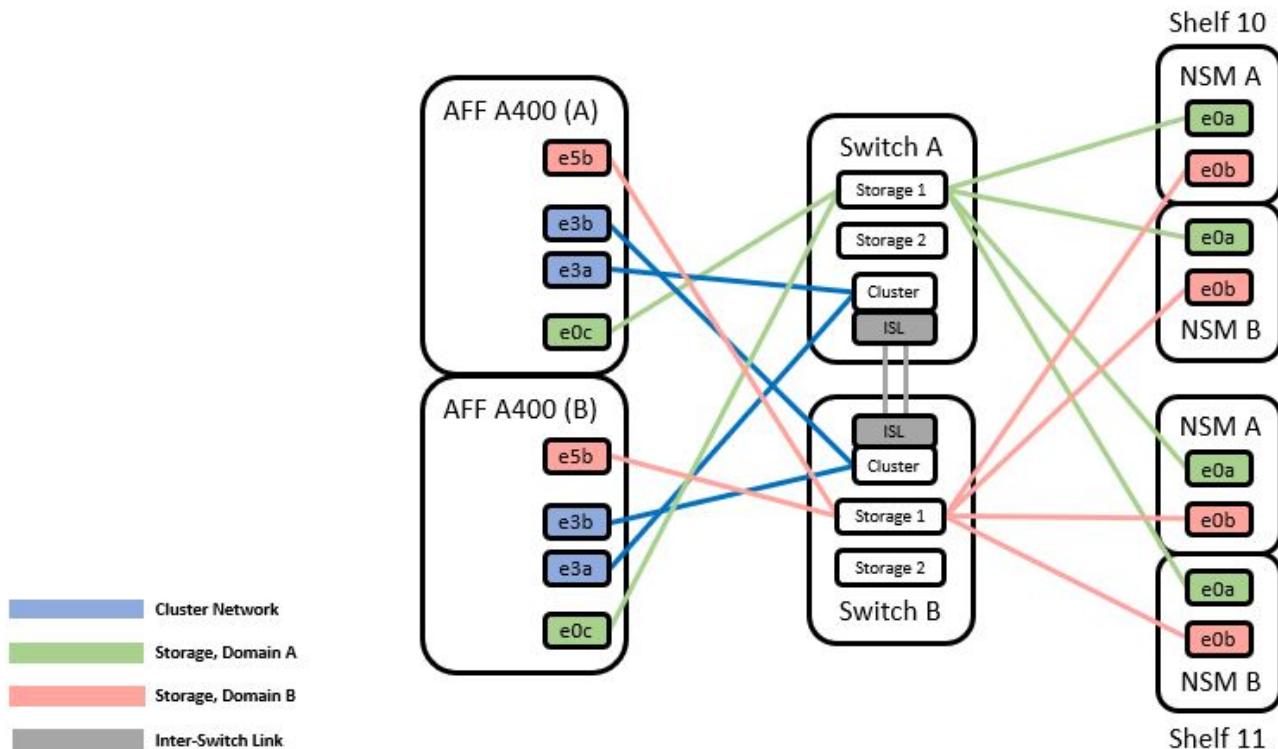
Nach der Migration Ihrer Switches können Sie ["Konfigurieren der Switch-Integritätsüberwachung"](#) Die

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
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
30
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
30
```

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-Netzwerkkonfiguration gültig ist:

```
network port show
```

Was kommt als Nächstes?

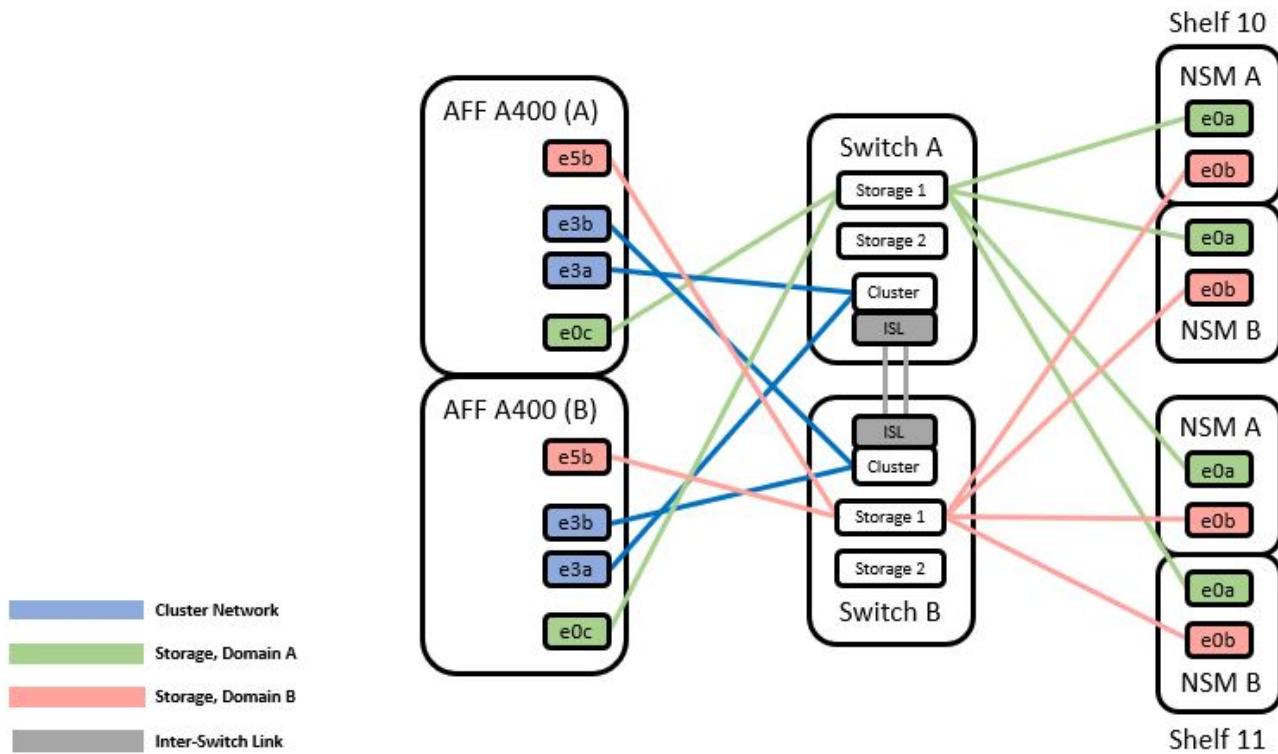
Nach der Migration Ihrer Switches können Sie "["Konfigurieren der Switch-Integritätsüberwachung"](#)Die

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
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
30
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
30
```

6. 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.
7. 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.
```

8.] 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-Netzwerkkonfiguration gültig ist:

```
network port show
```

18. Entfernen Sie die nicht verwendeten Cluster-Switches.
19. Entfernen Sie die nicht verwendeten Speicherschalter.

Was kommt als Nächstes?

Nach der Migration Ihrer Switches können Sie ["Konfigurieren der Switch-Integritätsüberwachung"](#) Die

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).

Bevor Sie beginnen

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

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	Health	Speed (Mbps)	Health
e3a	Cluster	Cluster		up	9000	auto/100000	healthy			
false										
e3b	Cluster	Cluster		up	9000	auto/100000	healthy			
false										

Node: node2

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

Current	Is	Logical	Status	Network	Current	
Vserver	Home	Interface	Admin/Oper	Address/Mask	Node	Port
Cluster		node1_clus1	up/up	169.254.209.69/16	node1	e3a
true		node1_clus2	up/up	169.254.49.125/16	node1	e3b

```

        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
          e3b    sh2
C9336C
          e3a    sh1
          e3b    sh2
C9336C
          e3a    sh1
          e3b    sh2
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
              Logical
Vserver       Interface      Auto-revert
-----
Cluster       node1_clus1    true
Cluster       node1_clus2    true
Cluster       node2_clus1    true
Cluster       node2_clus2    true
4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

Sie können das verwenden `network interface check cluster-connectivity` Befehl, um eine Zugriffsprüfung für die Cluster-Konnektivität zu starten und dann Details anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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 local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)

```

1. 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

```

2. 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.
3. 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) #
```

4. 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
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
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.
```

5. 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.
```

6. 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
```

7.] Überprüfen Sie, ob alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

Beispiel anzeigen

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

Node node1
Ignore

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

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.
```

8. 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 anzeigen:

```
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 ausführen `show`, um die Details anzeigen.

```
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 local
Host is node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 4 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 4 path(s):
Local 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Bestätigen Sie die folgende Clusternetzwerkkonfiguration:

```
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
-----  -----
-----  -----
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      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 Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	139	H	FAS2980
node2 eb	Eth1/2	124	H	FAS2980
sh1 Eth1/35	Eth1/35	178	R S I s	N9K-C9336C
sh1 Eth1/36	Eth1/36	178	R S I s	N9K-C9336C
Total entries displayed: 4				

2. Verschieben Sie die Speicherports vom alten Switch sh2 auf den neuen Switch news2.
3. Überprüfen Sie, ob der mit dem HA-Paar 1 verbundene Speicher, der gemeinsam genutzte Switch newsh2 in einem ordnungsgemäßen Zustand ist.
4. 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
                                         Speed
VLAN
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
30

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
30
```

5. Überprüfen Sie, ob die Shelves richtig 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.
```

6. Entfernen Sie den alten Schalter sh2.
7. Wiederholen Sie diese Schritte für den Schalter sh1 und den neuen Schalter newsh1.
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
```

Was kommt als Nächstes?

Nachdem Sie Ihre Schalter ausgetauscht haben, können Sie ["Konfigurieren der Switch-Integritätsüberwachung"](#) Die

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER 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.