



Cisco Nexus 9336C-FX2

Cluster and storage switches

NetApp
April 25, 2024

This PDF was generated from <https://docs.netapp.com/de-de/ontap-systems-switches/switch-cisco-9336c-fx2-storage/configure-switch-overview-9336c-storage.html> on April 25, 2024. Always check docs.netapp.com for the latest.

Inhalt

- Cisco Nexus 9336C-FX2 1
 - Überblick 1
 - Hardware installieren 5
 - Software konfigurieren 12
 - Ersetzen Sie einen Cisco Nexus 9336C-FX2 Storage-Switch 66

Cisco Nexus 9336C-FX2

Überblick

Überblick über die Installation und Konfiguration der Cisco Nexus 9336C-FX2 Storage-Switches

Der Cisco Nexus 9336C-FX2 Storage-Switch ist Teil der Cisco Nexus 9000 Plattform und kann in einem NetApp System-Rack installiert werden. Storage-Switches ermöglichen das Routen von Daten zwischen Servern und Storage Arrays in einem Storage Area Network (SAN).

Überblick über die Erstkonfiguration

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

1. ["Füllen Sie das Verkabelungsarbeitsblatt aus"](#).
2. ["Den Schalter einbauen"](#).
3. ["Konfigurieren Sie den Switch"](#).
4. ["Switch in NetApp-Schrank einbauen"](#).

Je nach Konfiguration können Sie den Cisco Nexus 9336C-FX2 Switch und die Pass-Through-Panel in einem NetApp Rack mit den im Lieferumfang des Switches enthaltenen Standardhalterungen installieren.

5. ["Bereiten Sie sich auf die Installation von NX-OS und RCF vor"](#).
6. ["Installieren Sie die NX-OS-Software"](#).
7. ["Installieren Sie die RCF-Konfigurationsdatei"](#).

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

Weitere Informationen

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

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

Konfigurationsanforderungen für Cisco Nexus 9336C-FX2 Storage Switches

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

ONTAP Support

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

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

Konfigurationsanforderungen

Für die Konfiguration benötigen Sie die entsprechende Anzahl und Art von Kabeln und Kabelanschlüssen für Ihre Switches.

Je nach Art des Switches, den Sie zunächst konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Switch-Konsolen-Port herstellen. Außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie die folgenden Netzwerkinformationen.

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

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

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

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

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

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

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

Dokumentationsanforderungen für Cisco Nexus 9336C-FX2 Storage-Switches

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

Switch-Dokumentation

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

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

Dokumenttitel	Beschreibung
<i>Nexus 9000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.
<i>Versionshinweise zur Cisco Nexus 9000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

Dokumentation der ONTAP Systeme

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

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

Schienensatz und Rack-Dokumentation

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

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

Anforderungen für Smart Call Home

Überprüfen Sie die folgenden Richtlinien, um die Smart Call Home-Funktion zu verwenden.

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

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

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

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

Hardware installieren

Installieren Sie den Speicherschalter 9336C-FX2

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

Was Sie benötigen

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

Schritte

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

Wenn Sie das installieren...	Dann...
Cisco Nexus 9336C-FX2 in einem NetApp Systemschrank	Siehe " Switch in NetApp-Schrank einbauen " Eine Anleitung zur Installation des Switches in einem NetApp-Schrank ist ebenfalls vorhanden.

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

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

Was kommt als Nächstes?

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

Konfigurieren Sie den Speicherschalter 9336C-FX2

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

Was Sie benötigen


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


Schritte

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

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

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit ja . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (ja/nein)	Antworten Sie mit ja . Die Standardeinstellung ist ja.

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

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

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

Was kommt als Nächstes?

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

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

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

Was Sie benötigen

- Für jeden Switch müssen Sie die acht 10-32- oder 12-24-Schrauben und Muttern bereitstellen, um die Halterungen und Gleitschienen an den vorderen und hinteren Schrankleisten zu befestigen.

- Sie müssen den Cisco Standard-Schienenensatz verwenden, um den Switch in einem NetApp Rack zu installieren.



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

Erforderliche Dokumentation

Lesen Sie die anfänglichen Vorbereitungsanforderungen, den Inhalt des Kits und die Sicherheitsvorkehrungen im ["Hardware-Installationsleitfaden Der Cisco Nexus 9000-Serie"](#).

Schritte

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

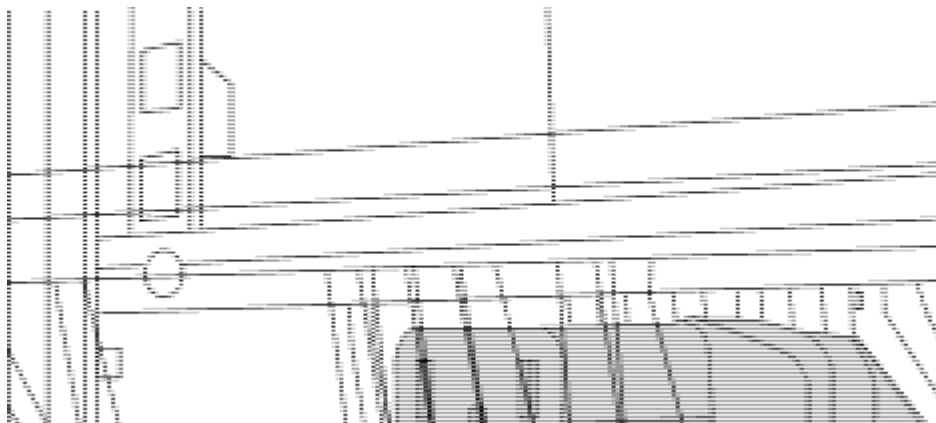
Die Pass-Through-Panel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

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

- Ein Durchlauf-Blindblech
- Vier 10-32 x 0,75 Schrauben
- Vier 10-32-Clip-Muttern
 - i. Stellen Sie die vertikale Position der Schalter und der Blindplatte im Schrank fest.

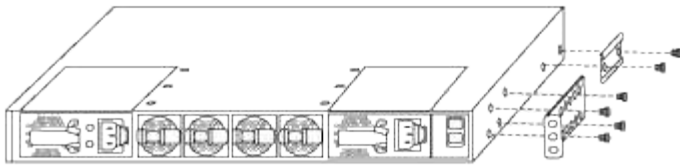
Bei diesem Verfahren wird die Blindplatte in U40 installiert.

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

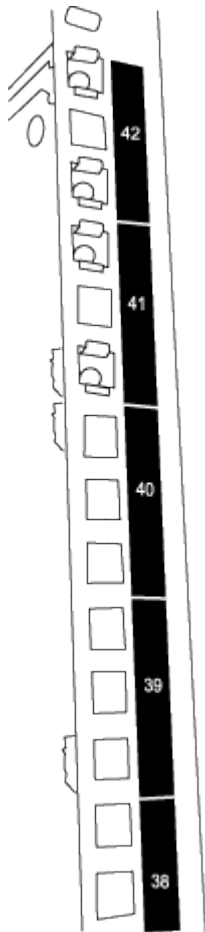


(1) *Buchsenleiste des Überbrückungskabels.*

2. Installieren Sie die Halterungen für die Rack-Montage am Switch-Gehäuse des Nexus 9336C-FX2.
 - a. Positionieren Sie eine vordere Rack-Mount-Halterung auf einer Seite des Switch-Gehäuses so, dass das Montagewinkel an der Gehäusefaceplate (auf der Netzteilseite oder Lüfterseite) ausgerichtet ist. Verwenden Sie dann vier M4-Schrauben, um die Halterung am Gehäuse zu befestigen.

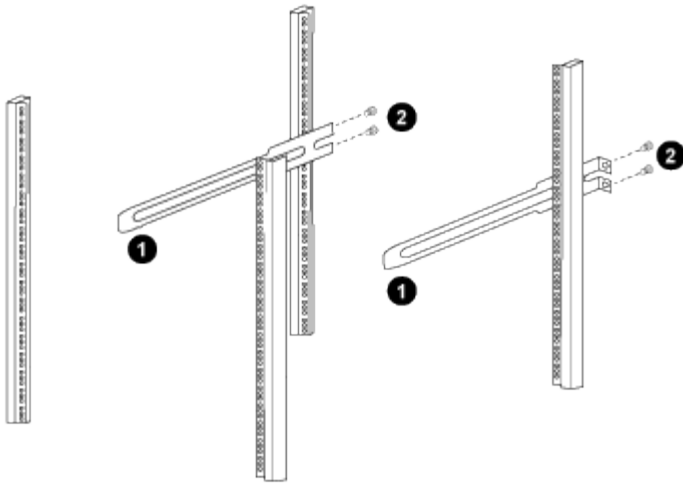


- b. Wiederholen Sie den Schritt 2 a Mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
 - c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.
 - d. Wiederholen Sie den Schritt 2c Mit der anderen hinteren Halterung für die Rackmontage auf der anderen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



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

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



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

(2) Schrauben der Gleitschienen an den Schrankleisten festziehen.

a. Wiederholen Sie den Schritt 4 a Für den hinteren Pfosten auf der rechten Seite.

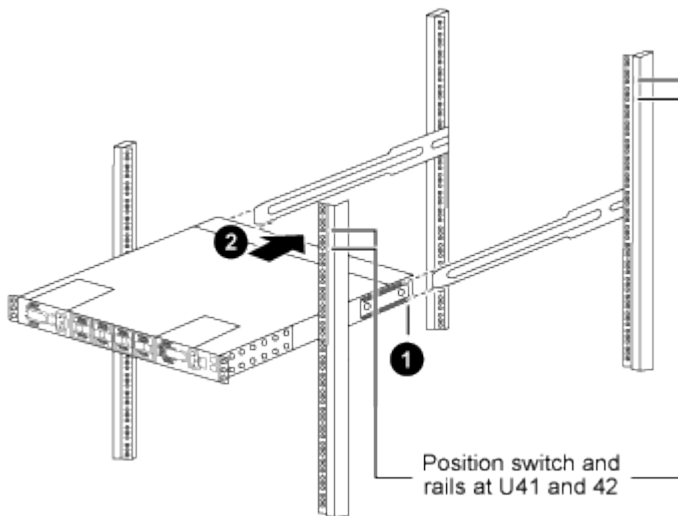
b. Wiederholen Sie die Schritte 4 a Und 4b An den RU41 Standorten auf dem Schrank.

5. Den Schalter in den Schrank einbauen.



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

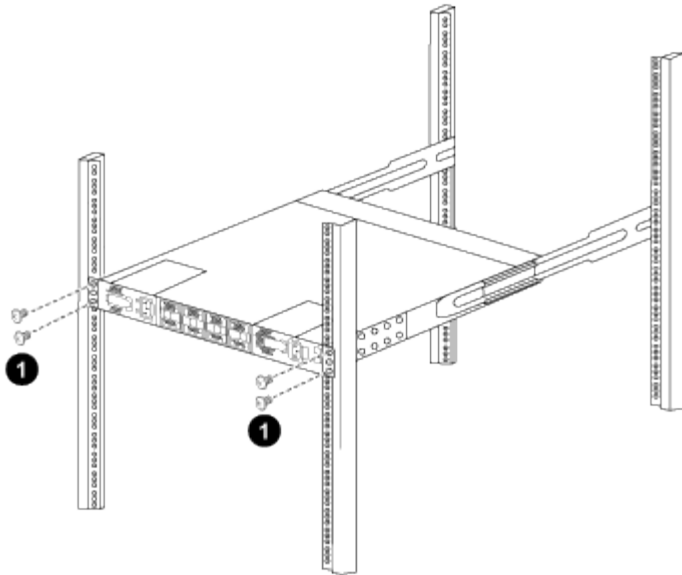
a. Positionieren Sie die Rückseite des Schalters an RU41.



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

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

b. Befestigen Sie den Schalter am Gehäuse.



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

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



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

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



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

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

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

Software konfigurieren

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

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

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

3. "Installieren Sie die RCF-Konfigurationsdatei".

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

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

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

Zu den Beispielen

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

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

Über diese Aufgabe

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

Schritte

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



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

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

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (`*>`) erscheint.

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

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

Beispiel anzeigen

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

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

4 entries were displayed.

4. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.

a. Zeigen Sie die Attribute des Netzwerkports an:

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


Beispiel anzeigen

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

Node: cluster1-02

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

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

4 entries were displayed.
```

b. Zeigt Informationen zu den LIFs an:

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

Beispiel anzeigen

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

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

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

4 entries were displayed.

5. Ping für die Remote-Cluster-LIFs:

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

Beispiel anzeigen

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

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

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

6. Vergewissern Sie sich, dass der automatische Zurücksetzen-Befehl auf allen Cluster-LIFs aktiviert ist:

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

Beispiel anzeigen

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

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

4 entries were displayed.

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

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

Beispiel anzeigen

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



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

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

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

Beispiel anzeigen

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

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

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

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

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

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

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

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

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

Enabling cluster switch log collection.

cluster1::*>
```



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

Was kommt als Nächstes?

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

Installieren Sie die NX-OS-Software

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

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

Prüfen Sie die Anforderungen

Was Sie benötigen

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

Zu den Beispielen

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

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

Installieren Sie die Software

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

Schritte

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

Beispiel anzeigen

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

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

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

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

Beispiel anzeigen

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

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

cs2# copy sftp: bootflash: vrf management

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

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

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

```
show version
```

Beispiel anzeigen

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

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

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

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

```
Last reset at 157524 usecs after Mon Nov  2 18:32:06 2020
```

```
Reason: Reset Requested by CLI command reload
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

```
cs2#
```

5. Installieren Sie das NX-OS Image.

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

Beispiel anzeigen

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

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

```
Installer is forced disruptive
```

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

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

```
Verifying image type.
```

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

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

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

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

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

```
Performing module support checks.
```

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

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

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

```
Compatibility check is done:
```

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

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

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

```
Switch will be reloaded for disruptive upgrade.
```

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

```
Install is in progress, please wait.
```

```
Performing runtime checks.
```

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

```
Setting boot variables.
```

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

```
Performing configuration copy.
```

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

```
Module 1: Refreshing compact flash and upgrading  
bios/loader/bootrom.
```

```
Warning: please do not remove or power off the module at this time.
```

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

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

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

```
show version
```

Beispiel anzeigen

```
cs2# show version
```

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

Software

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

Hardware

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

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

```
Last reset at 277524 usecs after Mon Nov  2 22:45:12 2020
```

```
Reason: Reset due to upgrade
```

```
System version: 9.3(4)
```

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

```
Active Package(s):
```

7. Aktualisieren Sie das EPLD-Bild, und starten Sie den Switch neu.

Beispiel anzeigen




```
cs2# show version module 1 epld
```

EPLD Device	Version
MI FPGA	0x7
IO FPGA	0x17
MI FPGA2	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2
GEM FPGA	0x2

```
cs2# install epld bootflash:n9000-epld.9.3.5.img module 1
```

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

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

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

8. Melden Sie sich nach dem Neustart des Switches erneut an, und überprüfen Sie, ob die neue EPLD-Version erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld
```

EPLD	Device	Version
MI	FPGA	0x7
IO	FPGA	0x19
MI	FPGA2	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2
GEM	FPGA	0x2

9. Wiederholen Sie die Schritte 1 bis 8, um die NX-OS-Software auf Switch cs1 zu installieren.

Was kommt als Nächstes?

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

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können den RCF nach dem ersten Einrichten des Nexus 9336C-FX2-Schalters installieren. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

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

Prüfen Sie die Anforderungen

Was Sie benötigen

- Ein aktuelles Backup der Switch-Konfiguration.
- Ein voll funktionsfähiges Cluster (keine Fehler in den Protokollen oder ähnlichen Problemen).
- Die aktuelle RCF-Datei.
- Eine Konsolenverbindung mit dem Switch, die bei der Installation des RCF erforderlich ist.

Vorgeschlagene Dokumentation

- ["Cisco Ethernet Switch Seite"](#) In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen. Beachten Sie, dass es Abhängigkeiten zwischen der Befehlssyntax im RCF und der in Versionen von NX-OS gibt.
- ["Switches Der Cisco Nexus 3000-Serie"](#). Ausführliche Dokumentation zu den Upgrade- und Downgrade-Verfahren für Cisco Switches finden Sie in den entsprechenden Software- und Upgrade-Leitfäden auf der Cisco Website.

Installieren Sie das RCF

Zu den Beispielen

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

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

Die Beispiele in diesem Verfahren verwenden zwei Knoten. Diese Nodes verwenden zwei 10-GbE-Cluster Interconnect-Ports e0a und e0b. Siehe "[Hardware Universe](#)" Um sicherzustellen, dass die korrekten Cluster-Ports auf Ihren Plattformen vorhanden sind.



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

Über diese Aufgabe

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

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



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein. Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritt 1: Vorbereitung für die Installation

1. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
           e0a    cs1                      Ethernet1/7      N9K-
C9336C
           e0d    cs2                      Ethernet1/7      N9K-
C9336C
cluster1-02/cdp
           e0a    cs1                      Ethernet1/8      N9K-
C9336C
           e0d    cs2                      Ethernet1/8      N9K-
C9336C
cluster1-03/cdp
           e0a    cs1                      Ethernet1/1/1    N9K-
C9336C
           e0b    cs2                      Ethernet1/1/1    N9K-
C9336C
cluster1-04/cdp
           e0a    cs1                      Ethernet1/1/2    N9K-
C9336C
           e0b    cs2                      Ethernet1/1/2    N9K-
C9336C
cluster1::*>
```

2. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.

a. Vergewissern Sie sich, dass alle Cluster-Ports **up** mit einem gesunden Status sind:

```
network port show -role cluster
```

Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::*>

b. Vergewissern Sie sich, dass sich alle Cluster-Schnittstellen (LIFs) im Home-Port befinden:

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

Beispiel anzeigen

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d true			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d true			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b true			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b true			
8 entries were displayed.				
cluster1::*>				

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

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

Beispiel anzeigen

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

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

3. Deaktivieren Sie die automatische Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

Schritt 2: Ports konfigurieren

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

Beispiel anzeigen

```
cs2(config)# interface eth1/1/1-2,eth1/7-8
cs2(config-if-range)# shutdown
```

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

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

Beispiel anzeigen

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0a true			
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0a false			
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0a true			
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0a false			
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0a true			
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0a false			
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0a true			
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0a false			
8 entries were displayed.				
cluster1::*>				

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

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
Node                Health Eligibility Epsilon
-----
cluster1-01         true   true      false
cluster1-02         true   true      false
cluster1-03         true   true       true
cluster1-04         true   true      false
4 entries were displayed.
cluster1::*>
```

4. Wenn Sie dies noch nicht getan haben, speichern Sie eine Kopie der aktuellen Switch-Konfiguration, indem Sie die Ausgabe des folgenden Befehls in eine Textdatei kopieren:

```
show running-config
```

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



Wenn Sie eine neue RCF aktualisieren oder anwenden, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

- a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

- b. Führen Sie einen Neustart des Switches aus:

Beispiel anzeigen

```
(cs2)# reload

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

6. Kopieren Sie die RCF auf den Bootflash von Switch cs2 mit einem der folgenden Übertragungsprotokolle: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Handbuch im ["Cisco Nexus 9000-Serie NX-OS Command Reference"](#) Leitfaden.

Beispiel anzeigen

Dieses Beispiel zeigt, dass TFTP zum Kopieren eines RCF auf den Bootflash auf Switch cs2 verwendet wird:

```
cs2# copy tftp: bootflash: vrf management
Enter source filename: Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt
Enter hostname for the tftp server: 172.22.201.50
Trying to connect to tftp server.....Connection to Server
Established.
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

7. Wenden Sie die RCF an, die zuvor auf den Bootflash heruntergeladen wurde.

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

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt Installation auf Schalter cs2:

```
cs2# copy Nexus_9336C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

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

Beispiel anzeigen

```
cs2# show banner motd

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

9. Vergewissern Sie sich, dass die RCF-Datei die richtige neuere Version ist:

```
show running-config
```

Wenn Sie die Ausgabe überprüfen, um zu überprüfen, ob Sie die richtige RCF haben, stellen Sie sicher, dass die folgenden Informationen richtig sind:

- Das RCF-Banner
- Die Node- und Port-Einstellungen
- Anpassungen

Die Ausgabe variiert je nach Konfiguration Ihres Standorts. Prüfen Sie die Porteinstellungen, und lesen Sie in den Versionshinweisen alle Änderungen, die für die RCF gelten, die Sie installiert haben.

10. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Switch-Einstellungen korrekt sind, kopieren Sie die Running-config-Datei in die Start-config-Datei.

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

Beispiel anzeigen

```
cs2# copy running-config startup-config
[#####] 100% Copy complete
```

11. Schalter cs2 neu starten. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

```
cs2# reload
This command will reboot the system. (y/n)? [n] y
```

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

- a. Vergewissern Sie sich, dass e0d-Ports über alle Nodes im Cluster hinweg ordnungsgemäß und ordnungsgemäß sind:

```
network port show -role cluster
```

Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

e0a	Cluster	Cluster		up	9000	auto/100000	
healthy	false						
e0d	Cluster	Cluster		up	9000	auto/100000	
healthy	false						

8 entries were displayed.

- a. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch cs2 an, da LIFs nicht auf e0d homed sind).

Beispiel anzeigen

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

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

cluster1-01/cdp			
	e0a	cs1	Ethernet1/7
N9K-C9336C			
	e0d	cs2	Ethernet1/7
N9K-C9336C			
cluster01-2/cdp			
	e0a	cs1	Ethernet1/8
N9K-C9336C			
	e0d	cs2	Ethernet1/8
N9K-C9336C			
cluster01-3/cdp			
	e0a	cs1	Ethernet1/1/1
N9K-C9336C			
	e0b	cs2	Ethernet1/1/1
N9K-C9336C			
cluster1-04/cdp			
	e0a	cs1	Ethernet1/1/2
N9K-C9336C			
	e0b	cs2	Ethernet1/1/2
N9K-C9336C			

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

Switch	Type	Address
Model		

cs1	cluster-network	10.233.205.90
NX9-C9336C		
Serial Number: FOCXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cisco Nexus Operating System (NX-OS)		
Software, Version		
9.3(5)		
Version Source: CDP		
cs2	cluster-network	10.233.205.91


```
NX9-C9336C
  Serial Number: FOCXXXXXXGS
    Is Monitored: true
      Reason: None
    Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
          9.3(5)
  Version Source: CDP

2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version können Sie die folgende Ausgabe auf der cs1-Switch-Konsole beobachten:

```
2020 Nov 17 16:07:18 cs1 %$ VDC-1 %$ %STP-2-UNBLOCK_CONSIST_PORT:
Unblocking port port-channel1 on VLAN0092. Port consistency
restored.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_PEER:
Blocking port-channel1 on VLAN0001. Inconsistent peer vlan.
2020 Nov 17 16:07:23 cs1 %$ VDC-1 %$ %STP-2-BLOCK_PVID_LOCAL:
Blocking port-channel1 on VLAN0092. Inconsistent local vlan.
```

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

Beispiel anzeigen

Im folgenden Beispiel wird die Ausgabe des Schnittstellenbeispiels verwendet:

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

14. Überprüfen Sie, ob die Cluster-LIFs zu den Ports migriert wurden, die auf dem Switch cs2 gehostet werden. Dies kann einige Sekunden dauern.

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

Beispiel anzeigen

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	false		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	false		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	false		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	false		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		
8 entries were displayed.				
cluster1::*>				

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

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
Node                Health    Eligibility    Epsilon
-----
cluster1-01         true     true          false
cluster1-02         true     true          false
cluster1-03         true     true           true
cluster1-04         true     true          false
4 entries were displayed.
cluster1::*>
```

16. Wiederholen Sie die Schritte 4 bis 11 am Schalter cs1.
17. Aktivieren Sie die Funktion zum automatischen Zurücksetzen auf den Cluster-LIFs.

Beispiel anzeigen

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

18. Schalter cs1 neu starten. Sie führen dies aus, um die Cluster-LIFs auszulösen, die auf die Home-Ports zurückgesetzt werden. Sie können die auf den Nodes gemeldeten Ereignisse „Cluster Ports down“ ignorieren, während der Switch neu gebootet wird.

Beispiel anzeigen

```
cs1# reload
This command will reboot the system. (y/n)? [n] y
```

Schritt 3: Überprüfen Sie die Konfiguration

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

```
show interface brief
```

Beispiel anzeigen

```
cs1# show interface brief | grep up
.
.
Eth1/1/1      1      eth  access up      none
10G(D)  --
Eth1/1/2      1      eth  access up      none
10G(D)  --
Eth1/7        1      eth  trunk  up      none
100G(D)  --
Eth1/8        1      eth  trunk  up      none
100G(D)  --
.
.
```

2. Überprüfen Sie, ob die erwarteten Nodes weiterhin verbunden sind:

```
show cdp neighbors
```

Beispiel anzeigen

```
cs1# show cdp neighbors

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-
Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1        133      H               FAS2980
e0a
node2              Eth1/2        133      H               FAS2980
e0a
cs2                 Eth1/35       175      R S I s         N9K-C9336C
Eth1/35
cs2                 Eth1/36       175      R S I s         N9K-C9336C
Eth1/36

Total entries displayed: 4
```

3. Überprüfen Sie mit den folgenden Befehlen, ob sich die Cluster-Nodes in den richtigen Cluster-VLANs befinden:

```
show vlan brief
```

```
show interface trunk
```

Beispiel anzeigen

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Pol, Eth1/1, Eth1/2, Eth1/3 Eth1/4, Eth1/5, Eth1/6, Eth1/7 Eth1/8, Eth1/35, Eth1/36 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
17	VLAN0017	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
18	VLAN0018	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4 Eth1/5, Eth1/6, Eth1/7, Eth1/8 Eth1/9/1, Eth1/9/2, Eth1/9/3 Eth1/9/4, Eth1/10/1, Eth1/10/2 Eth1/10/3, Eth1/10/4
31	VLAN0031	active	Eth1/11, Eth1/12, Eth1/13 Eth1/14, Eth1/15, Eth1/16 Eth1/17, Eth1/18, Eth1/19 Eth1/20, Eth1/21, Eth1/22
32	VLAN0032	active	Eth1/23, Eth1/24, Eth1/25

```

Eth1/28
Eth1/31
Eth1/34
33    VLAN0033          active  Eth1/11, Eth1/12,
Eth1/13
Eth1/16
Eth1/19
Eth1/22
34    VLAN0034          active  Eth1/23, Eth1/24,
Eth1/25
Eth1/28
Eth1/31
Eth1/34

```

```
cs1# show interface trunk
```

Port	Native Vlan	Status	Port Channel
Eth1/1	1	trunking	--
Eth1/2	1	trunking	--
Eth1/3	1	trunking	--
Eth1/4	1	trunking	--
Eth1/5	1	trunking	--
Eth1/6	1	trunking	--
Eth1/7	1	trunking	--
Eth1/8	1	trunking	--
Eth1/9/1	1	trunking	--
Eth1/9/2	1	trunking	--
Eth1/9/3	1	trunking	--
Eth1/9/4	1	trunking	--
Eth1/10/1	1	trunking	--
Eth1/10/2	1	trunking	--
Eth1/10/3	1	trunking	--
Eth1/10/4	1	trunking	--
Eth1/11	33	trunking	--

Eth1/12	33	trunking	--
Eth1/13	33	trunking	--
Eth1/14	33	trunking	--
Eth1/15	33	trunking	--
Eth1/16	33	trunking	--
Eth1/17	33	trunking	--
Eth1/18	33	trunking	--
Eth1/19	33	trunking	--
Eth1/20	33	trunking	--
Eth1/21	33	trunking	--
Eth1/22	33	trunking	--
Eth1/23	34	trunking	--
Eth1/24	34	trunking	--
Eth1/25	34	trunking	--
Eth1/26	34	trunking	--
Eth1/27	34	trunking	--
Eth1/28	34	trunking	--
Eth1/29	34	trunking	--
Eth1/30	34	trunking	--
Eth1/31	34	trunking	--
Eth1/32	34	trunking	--
Eth1/33	34	trunking	--
Eth1/34	34	trunking	--
Eth1/35	1	trnk-bndl	Pol
Eth1/36	1	trnk-bndl	Pol
Pol	1	trunking	--

Port	Vlans Allowed on Trunk
Eth1/1	1,17-18
Eth1/2	1,17-18
Eth1/3	1,17-18
Eth1/4	1,17-18
Eth1/5	1,17-18
Eth1/6	1,17-18
Eth1/7	1,17-18
Eth1/8	1,17-18
Eth1/9/1	1,17-18
Eth1/9/2	1,17-18
Eth1/9/3	1,17-18
Eth1/9/4	1,17-18
Eth1/10/1	1,17-18
Eth1/10/2	1,17-18
Eth1/10/3	1,17-18
Eth1/10/4	1,17-18

```
Eth1/11      31,33
Eth1/12      31,33
Eth1/13      31,33
Eth1/14      31,33
Eth1/15      31,33
Eth1/16      31,33
Eth1/17      31,33
Eth1/18      31,33
Eth1/19      31,33
Eth1/20      31,33
Eth1/21      31,33
Eth1/22      31,33
Eth1/23      32,34
Eth1/24      32,34
Eth1/25      32,34
Eth1/26      32,34
Eth1/27      32,34
Eth1/28      32,34
Eth1/29      32,34
Eth1/30      32,34
Eth1/31      32,34
Eth1/32      32,34
Eth1/33      32,34
Eth1/34      32,34
Eth1/35      1
Eth1/36      1
Po1          1
..
..
..
..
..
```



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

4. Stellen Sie sicher, dass die ISL zwischen cs1 und cs2 funktionsfähig ist:

```
show port-channel summary
```

Beispiel anzeigen

```
cs1# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        b - BFD Session Wait
        S - Switched      R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met

-----
-----
Group Port-          Type      Protocol  Member Ports      Channel
-----
-----
1      Pol (SU)      Eth      LACP      Eth1/35 (P)      Eth1/36 (P)
cs1#
```

5. Vergewissern Sie sich, dass die Cluster-LIFs auf ihren Home-Port zurückgesetzt wurden:

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

Beispiel anzeigen

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

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

Cluster				
	cluster1-01_clus1	up/up	169.254.3.4/23	
cluster1-01	e0d	true		
	cluster1-01_clus2	up/up	169.254.3.5/23	
cluster1-01	e0d	true		
	cluster1-02_clus1	up/up	169.254.3.8/23	
cluster1-02	e0d	true		
	cluster1-02_clus2	up/up	169.254.3.9/23	
cluster1-02	e0d	true		
	cluster1-03_clus1	up/up	169.254.1.3/23	
cluster1-03	e0b	true		
	cluster1-03_clus2	up/up	169.254.1.1/23	
cluster1-03	e0b	true		
	cluster1-04_clus1	up/up	169.254.1.6/23	
cluster1-04	e0b	true		
	cluster1-04_clus2	up/up	169.254.1.7/23	
cluster1-04	e0b	true		
8 entries were displayed.				
cluster1::*>				

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

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
Node           Health Eligibility  Epsilon
-----
cluster1-01    true   true       false
cluster1-02    true   true       false
cluster1-03    true   true        true
cluster1-04    true   true       false
4 entries were displayed.
cluster1::*>
```

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

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

Beispiel anzeigen

```
cluster1::*> cluster ping-cluster -node local
Host is cluster1-03
Getting addresses from network interface table...
Cluster cluster1-03_clus1 169.254.1.3 cluster1-03 e0a
Cluster cluster1-03_clus2 169.254.1.1 cluster1-03 e0b
Cluster cluster1-04_clus1 169.254.1.6 cluster1-04 e0a
Cluster cluster1-04_clus2 169.254.1.7 cluster1-04 e0b
Cluster cluster1-01_clus1 169.254.3.4 cluster1-01 e0a
Cluster cluster1-01_clus2 169.254.3.5 cluster1-01 e0d
Cluster cluster1-02_clus1 169.254.3.8 cluster1-02 e0a
Cluster cluster1-02_clus2 169.254.3.9 cluster1-02 e0d
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
.....
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
.....
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

Protokollerfassung der Ethernet-Switch-Statusüberwachung

Sie können die Protokollerfassungsfunktion verwenden, um Switch-bezogene Protokolldateien in ONTAP zu sammeln.

+

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

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie Ihre Umgebung mit dem Cluster-Switch 9336C-FX2 * CLI* eingerichtet haben.
- Die Switch-Statusüberwachung muss für den Switch aktiviert sein. Überprüfen Sie dies, indem Sie sicherstellen, dass die `Is Monitored:` Feld wird in der Ausgabe des auf **true** gesetzt `system switch ethernet show` Befehl.

Schritte

1. Erstellen Sie ein Passwort für die Protokollerfassungsfunktion der Ethernet-Switch-Statusüberwachung:

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

Beispiel anzeigen

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

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

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

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

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

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

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

2. Führen Sie zum Starten der Protokollerfassung den folgenden Befehl aus, um das GERÄT durch den im

vorherigen Befehl verwendeten Switch zu ersetzen. Damit werden beide Arten der Log-Erfassung gestartet: Die detaillierten **Support**-Protokolle und eine stündliche Erfassung von **Periodic**-Daten.

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

Beispiel anzeigen

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

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

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

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

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

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

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

```
system switch ethernet log show
```



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

Fehlerbehebung

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

Fehlerstatus der Protokollsammlung	* Auflösung*
RSA-Schlüssel nicht vorhanden	ONTAP-SSH-Schlüssel neu generieren. Wenden Sie sich an den NetApp Support.
Switch-Passwort-Fehler	Überprüfen Sie die Anmeldeinformationen, testen Sie die SSH-Konnektivität und regenerieren Sie ONTAP-SSH-Schlüssel. Lesen Sie die Switch-Dokumentation oder wenden Sie sich an den NetApp Support, um weitere Informationen zu erhalten.

ECDSA-Schlüssel für FIPS nicht vorhanden	Wenn der FIPS-Modus aktiviert ist, müssen ECDSA-Schlüssel auf dem Switch generiert werden, bevor Sie es erneut versuchen.
Bereits vorhandenes Log gefunden	Entfernen Sie die vorherige Protokollerfassungsdatei auf dem Switch.
Switch Dump Log Fehler	Stellen Sie sicher, dass der Switch-Benutzer über Protokollerfassungsberechtigungen verfügt. Beachten Sie die oben genannten Voraussetzungen.

Konfigurieren Sie SNMPv3

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

Über diese Aufgabe

Mit den folgenden Befehlen wird ein SNMPv3-Benutzername auf Cisco 9336C-FX2-Switches konfiguriert:

- Für **keine Authentifizierung**:

```
snmp-server user SNMPv3_USER NoAuth
```
- Für * MD5/SHA-Authentifizierung*:

```
snmp-server user SNMPv3_USER auth [md5|sha] AUTH-PASSWORD
```
- Für **MD5/SHA-Authentifizierung mit AES/DES-Verschlüsselung**:

```
snmp-server user SNMPv3_USER AuthEncrypt auth [md5|sha] AUTH-PASSWORD priv  
aes-128 PRIV-PASSWORD
```

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

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

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

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

Schritte

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

```
show snmp user
```


Beispiel anzeigen

```
(sw1) (Config)# snmp-server user SNMPv3User auth md5 <auth_password>
priv aes-128 <priv_password>
```

```
(sw1) (Config)# show snmp user
```

```
-----
-----
                                SNMP USERS
-----
-----
```

User	Auth	Priv(enforce)	Groups
acl_filter			
admin	md5	des(no)	network-admin
SNMPv3User	md5	aes-128(no)	network-operator

```
-----
-----
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
-----
-----
```

User	Auth	Priv

```
(sw1) (Config)#
```

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

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

Beispiel anzeigen

```
cluster1::*> system switch ethernet modify -device "sw1
(b8:59:9f:09:7c:22)" -is-monitoring-enabled-admin true

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

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

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

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

Enter the authentication protocol password again:

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

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

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

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

Beispiel anzeigen

```
cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv2c
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: cshml!
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored ?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

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

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

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

Beispiel anzeigen

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

cluster1::*> system switch ethernet show-all -device "sw1" -instance

Device Name: sw1
IP Address: 10.231.80.212
SNMP Version: SNMPv3
Is Discovered: true
SNMPv2c Community String or SNMPv3 Username: SNMPv3User
Model Number: N9K-C9336C-FX2
Switch Network: cluster-network
Software Version: Cisco Nexus
Operating System (NX-OS) Software, Version 9.3(7)
Reason For Not Monitoring: None <---- displays
when SNMP settings are valid
Source Of Switch Version: CDP/ISDP
Is Monitored?: true
Serial Number of the Device: QTFCU3826001C
RCF Version: v1.8X2 for

Cluster/HA/RDMA

cluster1::*>
```

Ersetzen Sie einen Cisco Nexus 9336C-FX2 Storage-Switch

Sie können einen defekten Nexus 9336C-FX2-Switch in einem Cluster-Netzwerk ersetzen. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

Was Sie benötigen

Stellen Sie vor der Installation der NX-OS-Software und der RCFs auf einem Cisco Nexus 9336C-FX2-Storage-Switch sicher, dass:

- Ihr System kann Cisco Nexus 9336C-FX2 Storage Switches unterstützen.
- Sie haben sich auf der Seite Cisco Ethernet Switch die Switch-Kompatibilitätstabelle für die unterstützten ONTAP-, NX-OS- und RCF-Versionen angehört.
- Sie haben die entsprechenden Leitfäden zu Software und Upgrades auf der Cisco Website zur Verfügung gestellt.

Switches Der Cisco Nexus 3000-Serie:

- Sie haben die entsprechenden RCFs heruntergeladen.

- Die vorhandene Netzwerkkonfiguration weist folgende Merkmale auf:
 - Auf der Seite Cisco Ethernet Switches befinden sich die neuesten RCF- und NX-OS-Versionen auf Ihren Switches.
 - Management-Konnektivität muss auf beiden Switches vorhanden sein.
- Der Cisco Nexus 9336C-FX2-Ersatzschalter weist folgende Merkmale auf:
 - Die Management-Netzwerk-Konnektivität ist funktionsfähig.
 - Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
 - Das entsprechende RCF- und NX-OS-Betriebssystemabbild wird auf den Switch geladen.
 - Die anfängliche Konfiguration des Schalters ist abgeschlossen.

Über diese Aufgabe

Dieses Verfahren ersetzt den zweiten Nexus 9336C-FX2 Storage Switch S2 durch den neuen 9336C-FX Switch NS2. Die beiden Knoten sind node1 und node2.

Schritte zur Fertigstellung:

- Vergewissern Sie sich, dass der zu ersetzende Schalter S2 ist.
- Trennen Sie die Kabel vom Schalter S2.
- Schließen Sie die Kabel wieder an den Schalter NS2 an.
- Überprüfen Sie alle Gerätekonfigurationen auf Switch NS2.



Es können Abhängigkeiten zwischen der Befehlssyntax für in der RCF- und NX-OS-Version bestehen.

Schritte

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

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

X ist die Dauer des Wartungsfensters in Stunden.

2. Überprüfen Sie den Integritätsstatus der Storage-Node-Ports, um sicherzustellen, dass eine Verbindung zum Storage-Switch S1 besteht:

```
storage port show -port-type ENET
```

Beispiel anzeigen

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID

node1	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

```
storage::*>
```

3. Stellen Sie sicher, dass der Speicherschalter S1 verfügbar ist:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol   Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
           e3a    S1                        Ethernet1/1 NX9336C
           e4a    node2                    e4a         AFF-A700
           e4e    node2                    e4e         AFF-A700
node1/lldp
           e3a    S1                        Ethernet1/1 -
           e4a    node2                    e4a         -
           e4e    node2                    e4e         -
node2/cdp
           e3a    S1                        Ethernet1/2 NX9336C
           e4a    node1                    e4a         AFF-A700
           e4e    node1                    e4e         AFF-A700
node2/lldp
           e3a    S1                        Ethernet1/2 -
           e4a    node1                    e4a         -
           e4e    node1                    e4e         -
storage::*>
```

4. Führen Sie die Show aus `lldp neighbors` Mit dem Befehl auf dem Arbeitsschalter bestätigen Sie, dass Sie beide Nodes und alle Shelves sehen können:

```
show lldp neighbors
```

Beispiel anzeigen

```
S1# show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID      Local Intf  Hold-time  Capability  Port ID
node1          Eth1/1     121        S           e3a
node2          Eth1/2     121        S           e3a
SHFGD2008000011 Eth1/5     121        S           e0a
SHFGD2008000011 Eth1/6     120        S           e0a
SHFGD2008000022 Eth1/7     120        S           e0a
SHFGD2008000022 Eth1/8     120        S           e0a
```

5. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-port
shelf    id  remote-port  remote-device
-----  --  -
3.20     0  Ethernet1/5  S1
3.20     1  -           -
3.20     2  Ethernet1/6  S1
3.20     3  -           -
3.30     0  Ethernet1/7  S1
3.20     1  -           -
3.30     2  Ethernet1/8  S1
3.20     3  -           -
storage::*>
```

6. Entfernen Sie alle Kabel, die am Lagerschalter S2 angeschlossen sind.

7. Schließen Sie alle Kabel wieder an den Ersatzschalter NS2 an.

8. Überprüfen Sie den Integritätsstatus der Speicher-Node-Ports erneut:

```
storage port show -port-type ENET
```

Beispiel anzeigen

```
storage::*> storage port show -port-type ENET
```

Node	Port	Type	Mode	Speed (Gb/s)	State	Status	VLAN ID
node1							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30
node2							
	e3a	ENET	storage	100	enabled	online	30
	e3b	ENET	storage	0	enabled	offline	30
	e7a	ENET	storage	0	enabled	offline	30
	e7b	ENET	storage	0	enabled	offline	30

```
storage::*>
```


9. Vergewissern Sie sich, dass beide Switches verfügbar sind:

```
network device-discovery show
```

Beispiel anzeigen

```
storage::*> network device-discovery show
Node/      Local Discovered
Protocol  Port  Device (LLDP: ChassisID)  Interface  Platform
-----
node1/cdp
          e3a  S1                        Ethernet1/1 NX9336C
          e4a  node2                     e4a         AFF-A700
          e4e  node2                     e4e         AFF-A700
          e7b  NS2                      Ethernet1/1 NX9336C
node1/lldp
          e3a  S1                        Ethernet1/1 -
          e4a  node2                     e4a         -
          e4e  node2                     e4e         -
          e7b  NS2                      Ethernet1/1 -
node2/cdp
          e3a  S1                        Ethernet1/2 NX9336C
          e4a  node1                     e4a         AFF-A700
          e4e  node1                     e4e         AFF-A700
          e7b  NS2                      Ethernet1/2 NX9336C
node2/lldp
          e3a  S1                        Ethernet1/2 -
          e4a  node1                     e4a         -
          e4e  node1                     e4e         -
          e7b  NS2                      Ethernet1/2 -
storage::*>
```

10. Überprüfen Sie die Shelf-Ports im Storage-System:

```
storage shelf port show -fields remote-device,remote-port
```

Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-  
port  
shelf    id    remote-port    remote-device  
-----  --    -  
3.20     0     Ethernet1/5    S1  
3.20     1     Ethernet1/5    NS2  
3.20     2     Ethernet1/6    S1  
3.20     3     Ethernet1/6    NS2  
3.30     0     Ethernet1/7    S1  
3.20     1     Ethernet1/7    NS2  
3.30     2     Ethernet1/8    S1  
3.20     3     Ethernet1/8    NS2  
storage::*>
```

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

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

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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