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

Install and maintain

NetApp
February 13, 2026

Inhalt

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

Erste Schritte

Installations- und Einrichtungsworkflow für Cisco Nexus 9336C-FX2 9336C-FX2-T-Speicherswitches

Die Cisco Nexus 9336C-FX2 und 9336C-FX2-T Switches sind Teil der Cisco Nexus 9000 Plattform und können in einem NetApp Systemschrank installiert werden.

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

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

1. **"Überprüfen der Konfigurationsanforderungen"**

Überprüfen Sie die Konfigurationsanforderungen für die Speicher-Switches 9336C-FX2 und 9336C-FX2-T.

2. **"Überprüfen Sie die Komponenten und Teilenummern"**

Überprüfen Sie die Komponenten und Teilenummern für die Speicher-Switches 9336C-FX2 und 9336C-FX2-T.

3. **"Überprüfen Sie die erforderlichen Unterlagen"**

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

4. **"Überprüfen Sie die Smart Call Home-Anforderungen"**

Überprüfen Sie die Anforderungen für die Cisco Smart Call Home-Funktion, die zur Überwachung der Hardware- und Softwarekomponenten in Ihrem Netzwerk verwendet wird.

5. **"Installieren Sie die Hardware"**

Installieren Sie die Switch-Hardware.

6. **"Konfigurieren der Software"**

Konfigurieren Sie die Switch-Software.

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

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

ONTAP-Unterstützung

ONTAP 9.9.1 und höher

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

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

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

ONTAP 9.10.1 und höher

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

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

Konfigurationsanforderungen

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

Je nach Art des Switches, den Sie initial konfigurieren, müssen Sie mit dem mitgelieferten Konsolenkabel eine Verbindung zum Konsolenport des Switches herstellen; außerdem müssen Sie spezifische Netzwerkinformationen angeben.

Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie folgende Netzwerkinformationen.

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

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

Was kommt als nächstes

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

Teilenummern"Die

Komponenten und Teilenummern für Cisco Nexus 9336C-FX2 und 9336C-FX2-T Speicherswitches

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

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

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

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

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

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

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

Was kommt als nächstes

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

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

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

Switch-Dokumentation

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

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

Dokumenttitel	Beschreibung
Cisco Nexus 9000 Series NX-OS Versionshinweise (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)	Beschreibt die Funktionen, Fehler und Einschränkungen der Cisco Nexus 9000-Serie.
Informationen zur Einhaltung gesetzlicher Bestimmungen und zur Sicherheit für die Cisco Nexus 9000-Serie	Bietet Informationen zur Einhaltung internationaler behördlicher Vorschriften, zur Sicherheit und zu gesetzlichen Bestimmungen für die Switches der Serie Nexus 9000.

ONTAP-Systemdokumentation

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

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

Dokumentation für Schienenbausatz und Schrank

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

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

Anforderungen für Smart Call Home

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

Smart Call Home überwacht die Hardware- und Softwarekomponenten in Ihrem Netzwerk. Wenn eine kritische

Systemkonfiguration auftritt, wird eine E-Mail-Benachrichtigung generiert und ein Alarm an alle Empfänger gesendet, die in Ihrem Zielprofil konfiguriert sind.

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

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

- Ein E-Mail-Server muss vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Kontaktname (SNMP-Server-Kontakt), die Telefonnummer und die Straßenadresse müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu ermitteln.
- Eine CCO-ID muss mit einem passenden Cisco SMARTnet Servicevertrag für Ihr Unternehmen verknüpft sein.
- Für die Registrierung des Geräts muss der Cisco SMARTnet-Dienst eingerichtet sein.

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

Installieren Sie die Hardware

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

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

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

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

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

Installieren Sie die Speicher-Switches 9336C-FX2 und 9336C-FX2-T.

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

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

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

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

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

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

9336C-FX2 Beispiel-Verkabelungsarbeitsblatt

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

Clusterschalter A		**Clusterschalter B**	
Switch-Port	Knoten- und Portnutzung	Switch-Port	Knoten- und Portnutzung
1	4x100GbE-Knoten 1	1	4x100GbE-Knoten 1
2	4x100GbE-Knoten 2	2	4x100GbE-Knoten 2
3	4x100GbE-Knoten 3	3	4x100GbE-Knoten 3
4	4x100GbE-Knoten 4	4	4x100GbE-Knoten 4
5	4x100GbE-Knoten 5	5	4x100GbE-Knoten 5
6	4x100GbE-Knoten 6	6	4x100GbE-Knoten 6
7	4x100GbE-Knoten 7	7	4x100GbE-Knoten 7
8	4x100GbE-Knoten 8	8	4x100GbE-Knoten 8
9	4x100GbE-Knoten 9	9	4x100GbE-Knoten 9
10	4x100GbE-Knoten 10	10	4x100GbE-Knoten 10
11	4x100GbE-Knoten 11	11	4x100GbE-Knoten 11
12	4x100GbE-Knoten 12	12	4x100GbE-Knoten 12
13	4x100GbE-Knoten 13	13	4x100GbE-Knoten 13
14	4x100GbE-Knoten 14	14	4x100GbE-Knoten 14
15	4x100GbE-Knoten 15	15	4x100GbE-Knoten 15

Clusterschalter A		Clusterschalter B	
16	4x100GbE-Knoten 16	16	4x100GbE-Knoten 16
17	4x100GbE-Knoten 17	17	4x100GbE-Knoten 17
18	4x100GbE-Knoten 18	18	4x100GbE-Knoten 18
19	4x100GbE-Knoten 19	19	4x100GbE-Knoten 19
20	4x100GbE-Knoten 20	20	4x100GbE-Knoten 20
21	4x100GbE-Knoten 21	21	4x100GbE-Knoten 21
22	4x100GbE-Knoten 22	22	4x100GbE-Knoten 22
23	4x100GbE-Knoten 23	23	4x100GbE-Knoten 23
24	4x100GbE-Knoten 24	24	4x100GbE-Knoten 24
25	4x100GbE-Knoten 25	25	4x100GbE-Knoten 25
26	4x100GbE-Knoten 26	26	4x100GbE-Knoten 26
27	4x100GbE-Knoten 27	27	4x100GbE-Knoten 27
28	4x100GbE-Knoten 28	28	4x100GbE-Knoten 28
29	4x100GbE-Knoten 29	29	4x100GbE-Knoten 29
30	4x100GbE-Knoten 30	30	4x100GbE-Knoten 30
31	4x100GbE-Knoten 31	31	4x100GbE-Knoten 31
32	4x100GbE-Knoten 32	32	4x100GbE-Knoten 32
33	4x100GbE-Knoten 33	33	4x100GbE-Knoten 33
30	4x100GbE-Knoten 30	30	4x100GbE-Knoten 33
34	4x100GbE-Knoten 34	34	4x100GbE-Knoten 34
35	4x100GbE-Knoten 35	35	4x100GbE-Knoten 35
36	4x100GbE-Knoten 36	36	4x100GbE-Knoten 36

9336C-FX2 leeres Verkabelungs-Arbeitsblatt

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

Clusterschalter A		Clusterschalter B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	

Clusterschalter A		Clusterschalter B	
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	

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

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

Clusterschalter A		Clusterschalter B	
Switch-Port	Knoten- und Portnutzung	Switch-Port	Knoten- und Portnutzung
1	4x100GbE-Knoten 1	1	4x100GbE-Knoten 1

Clusterschalter A		Clusterschalter B	
2	4x100GbE-Knoten 2	2	4x100GbE-Knoten 2
3	4x100GbE-Knoten 3	3	4x100GbE-Knoten 3
4	4x100GbE-Knoten 4	4	4x100GbE-Knoten 4
5	4x100GbE-Knoten 5	5	4x100GbE-Knoten 5
6	4x100GbE-Knoten 6	6	4x100GbE-Knoten 6
7	4x100GbE-Knoten 7	7	4x100GbE-Knoten 7
8	4x100GbE-Knoten 8	8	4x100GbE-Knoten 8
9	4x100GbE-Knoten 9	9	4x100GbE-Knoten 9
10	4x100GbE-Knoten 10	10	4x100GbE-Knoten 10
11 bis 36	Lizenz erforderlich	11 bis 36	Lizenz erforderlich

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

Mithilfe des leeren Verkabelungsarbeitsblatts können Sie die Plattformen dokumentieren, die als Knoten in einem Cluster unterstützt werden.

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

Clusterschalter A		Clusterschalter B	
10		10	
11 bis 36	Lizenz erforderlich	11 bis 36	Lizenz erforderlich

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

Was kommt als nächstes

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

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

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

Schritte

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

Wenn Sie Ihr… installieren	Dann…
Cisco Nexus 9336C-FX2 in einem NetApp -Systemschrank	Sehen"Switch im NetApp Schrank installieren" Anweisungen zur Installation des Switches in einem NetApp -Schrank finden Sie hier.
Ausrüstung in einem Telekommunikationsrack	Beachten Sie die in den Hardware-Installationshandbüchern für Switches und den Installations- und Einrichtungsanweisungen von NetApp beschriebenen Vorgehensweisen.

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

Wie geht es weiter?

Optional können Sie "Installieren Sie einen Cisco Nexus 9336C-FX2 Switch in einem NetApp Schrank"Die Ansonsten gehen Sie zu "Konfigurieren Sie den Switch"Die

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Für jeden Schalter müssen Sie die acht 10-32 oder 12-24 Schrauben und Clipmuttern zur Montage der Halterungen und Gleitschienen an den vorderen und hinteren Schrankpfosten bereitstellen.
- Sie müssen das Cisco Standard-Schienenkit verwenden, um den Switch in einem NetApp -Schrank zu installieren.

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

Erforderliche Dokumentation

Überprüfen Sie die anfänglichen Vorbereitungsanforderungen, den Inhalt des Kits und die Sicherheitsvorkehrungen in der "Hardware-Installationshandbuch für die Cisco Nexus 9000-Serie" Die

Schritte

1. Installieren Sie die Durchgangsabdeckung im NetApp -Schrank.

   Das Durchgangspanel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

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

   - Eine Durchgangs-Blindplatte
   - Vier 10-32 x 0,75 Schrauben
   - Vier 10-32 Clipmuttern

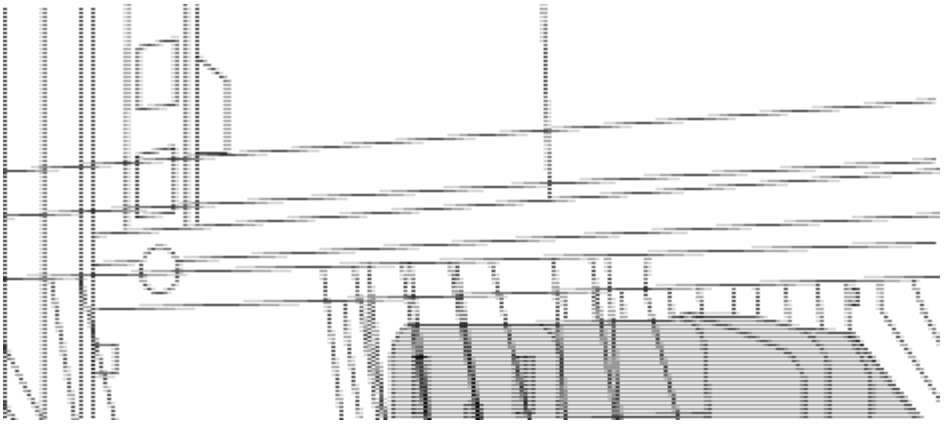
     i. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

     Bei diesem Verfahren wird die Abdeckplatte in U40 installiert.

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

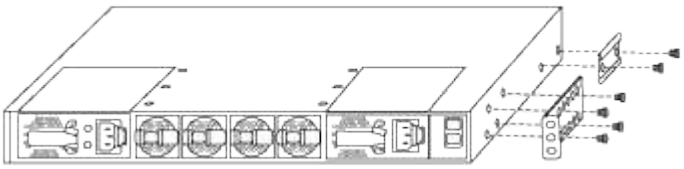
     iii. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.

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

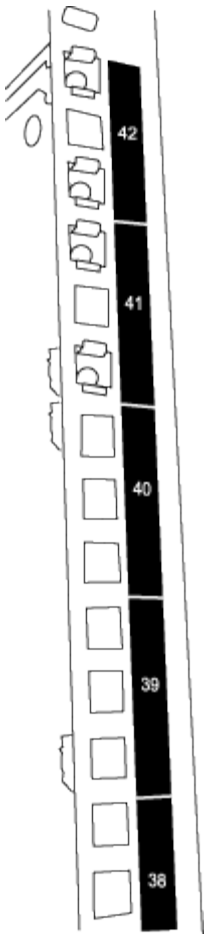


(1) Weiblicher Stecker des Überbrückungskabels.

2. Montieren Sie die Rack-Montagehalterungen am Nexus 9336C-FX2 Switch-Gehäuse.
   a. Positionieren Sie eine vordere Rackmontagehalterung auf einer Seite des Switch-Gehäuses, sodass die Montageöse mit der Gehäusefrontplatte (auf der Netzteil- oder Lüfterseite) ausgerichtet ist, und befestigen Sie die Halterung dann mit vier M4-Schrauben am Gehäuse.



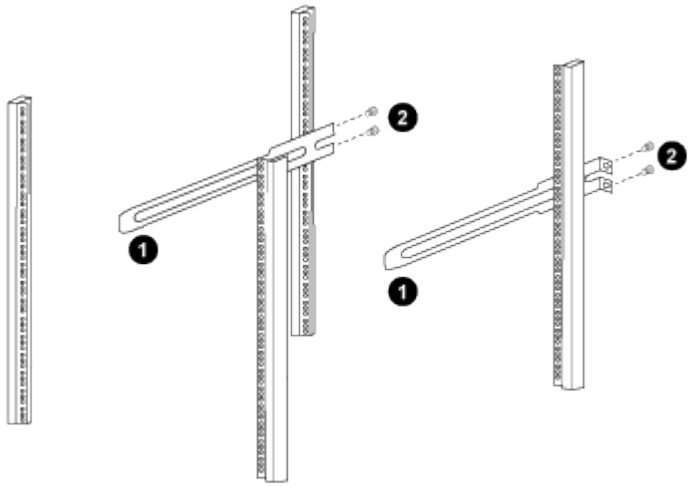
   b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.
   c. Installieren Sie die hintere Rackmontagehalterung am Switch-Gehäuse.
   d. Wiederholen Sie Schritt 2c mit der anderen hinteren Rackmontagehalterung auf der anderen Seite des Switches.
3. Installieren Sie die Clipmuttern in den quadratischen Lochpositionen für alle vier IEA-Pfosten.



Die beiden 9336C-FX2-Switches werden immer in den oberen 2 HE des Schranks RU41 und 42 montiert.

4. Montieren Sie die Gleitschienen im Schrank.

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



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

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

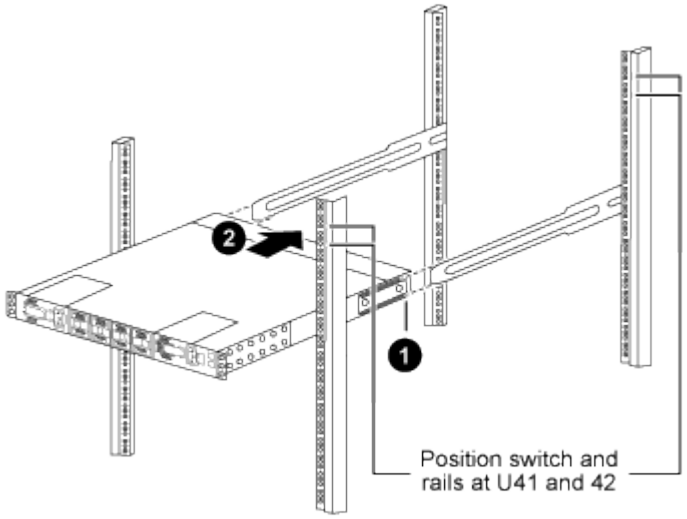
a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.

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

5. Bauen Sie den Schalter in den Schrank ein.

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

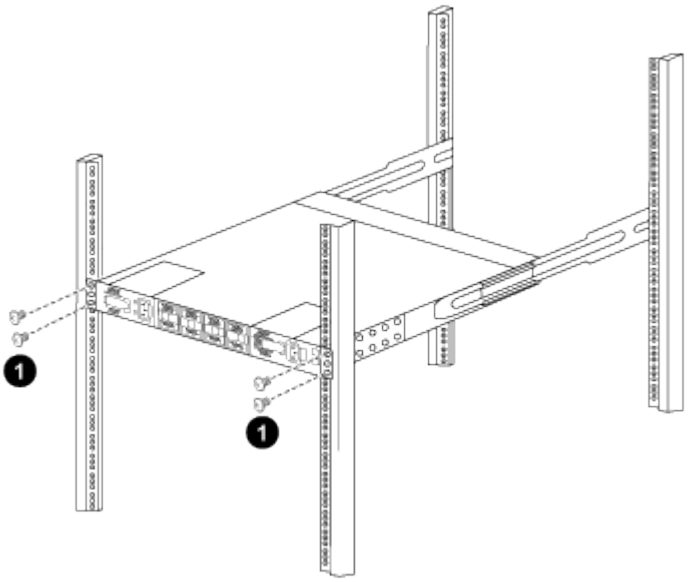
a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



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

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

b. Befestigen Sie den Schalter am Gehäuse.



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

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

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

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

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

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

8. Verbinden Sie den Management-Port jedes 9336C-FX2-Switches mit einem der Management-Switches (falls bestellt) oder verbinden Sie diese direkt mit Ihrem Management-Netzwerk.

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

Was kommt als nächstes

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

Konfigurieren der Software

Workflow zur Softwareinstallation für die Speicherswitches Cisco Nexus 9336C-FX2 und 9336C-FX2-T

Gehen Sie folgendermaßen vor, um Software für die Speicher-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T zu installieren und zu konfigurieren:

1 **"Konfigurieren Sie den Schalter"**

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

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

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

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

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

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

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

5 **"SSH-Konfiguration überprüfen"**

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

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

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

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

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

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

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

Schritte

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

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

Prompt	Antwort
Automatische Bereitstellung abbrechen und mit normaler Einrichtung fortfahren? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Nein.

Prompt	Antwort
Wollen Sie einen sicheren Passwortstandard erzwingen? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Ja.
Geben Sie das Passwort für den Administrator ein.	Das Standardpasswort lautet “admin”; Sie müssen ein neues, sicheres Passwort erstellen. Ein schwaches Passwort kann abgelehnt werden.
Möchten Sie den Dialog zur Basiskonfiguration aufrufen? (ja/nein)	Antworten Sie bei der Erstkonfiguration des Switches mit **ja**.
Ein weiteres Benutzerkonto erstellen? (ja/nein)	Die Antwort hängt von den Richtlinien Ihrer Website bezüglich alternativer Administratoren ab. Die Standardeinstellung ist **nein**.
SNMP-Community-String schreibgeschützt konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
SNMP-Community-Zeichenfolge für Lese- und Schreibzugriffe konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
Geben Sie den Namen des Schalters ein.	Der Name des Schalters ist auf 63 alphanumerische Zeichen beschränkt.
Mit der Out-of-Band-Managementkonfiguration (mgmt0) fortfahren? (ja/nein)	Antworten Sie bei dieser Eingabeaufforderung mit **ja** (Standardeinstellung). Geben Sie an der Eingabeaufforderung mgmt0 IPv4 address: Ihre IP-Adresse ein: ip_address.
Standardgateway konfigurieren? (ja/nein)	Antworten Sie mit **ja**. Geben Sie an der IPv4-Adresse des Standardgateways Ihre Standardgateway-Adresse ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
Den Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit **nein**. Die Standardeinstellung ist Nein.
SSH-Dienst aktiviert? (ja/nein)	Antworten Sie mit **ja**. Die Standardeinstellung ist Ja.  Bei der Verwendung von Ethernet Switch Health Monitor (CSHM) wird SSH aufgrund seiner Protokollierungsfunktionen empfohlen. Für erhöhte Sicherheit wird auch SSHv2 empfohlen.

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

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

Wie geht es weiter?

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

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

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

Zu den Beispielen

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

- Die Namen der beiden Cisco Switches lauten cs1 und cs2.
- Die Knotennamen lauten cluster1-01 und cluster1-02.
- Die Cluster-LIF-Namen lauten cluster1-01_clus1 und cluster1-01_clus2 für Cluster1-01 sowie cluster1-02_clus1 und cluster1-02_clus2 für Cluster1-02.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

Informationen zu diesem Vorgang

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

Schritte

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

   wobei x die Dauer des Wartungsfensters in Stunden ist.

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

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

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung(`*>`) erscheint.

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

   ```
   network device-discovery show -protocol lldp
   ```

Beispiel anzeigen

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

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

4 entries were displayed.
```

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

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

Beispiel anzeigen

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

Node: cluster1-02

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

Node: cluster1-01

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

4 entries were displayed.
```

b. Informationen zu den LIFs anzeigen:

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

Beispiel anzeigen

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

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

4 entries were displayed.
```

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

ONTAP 9.9.1 und höher

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
node1
       3/5/2024 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2024 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
node2
       3/5/2024 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2024 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Alle ONTAP Versionen

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

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

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

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

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

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

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

Beispiel anzeigen

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

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

Wie geht es weiter?

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

Installieren oder aktualisieren Sie die NX-OS-Software.

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

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

Überprüfungsanforderungen

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes tun:

- Führen Sie den `show install all impact nxos bootflash:<image_name>.bin` Befehl auf dem Switch aus, um die Auswirkungen der Installation oder Aktualisierung des neuen NX-OS-Software-Images zu überprüfen. Dabei werden die Integrität des Images, erforderliche Neustarts, die Hardwarekompatibilität und ausreichend Speicherplatz geprüft.
- Lesen Sie die Versionshinweise für die Zielversion der NX-OS-Software, um auf spezifische Anforderungen zu prüfen.
- Vergewissern Sie sich, dass Sie eine aktuelle Sicherung der Switch-Konfiguration haben.
- Vergewissern Sie sich, dass Sie einen voll funktionsfähigen Cluster haben (keine Fehler in den Protokollen oder ähnliche Probleme).

Empfohlene Dokumentation

- "Cisco Ethernet-Switch-Seite"

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

- "Anleitungen für Software-Upgrades und -Downgrades"

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

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

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

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

Zu den Beispielen

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

- Die Namen der beiden Cisco Switches lauten cs1 und cs2.
- Die Knotennamen sind cluster1-01, cluster1-02, cluster1-03 und cluster1-04.
- Die Cluster-LIF-Namen lauten cluster1-01_clus1, cluster1-01_clus2, cluster1-02_clus1, cluster1-02_clus2, cluster1-03_clus1, cluster1-03_clus2, cluster1-04_clus1 und cluster1-04_clus2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

Installieren Sie die Software

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

Schritte

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

   Beispiel anzeigen

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

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

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

3. Zeigen Sie die Cluster-Ports auf jedem Knoten an, die mit den Cluster-Switches verbunden sind:

   ```
   network device-discovery show
   ```

Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2
cluster1::*>
```

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

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

      `network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

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

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

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

Beispiel anzeigen

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

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

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

Beispiel anzeigen

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

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

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

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

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

Beispiel anzeigen

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

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


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

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

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

   ```
   show version
   ```

Beispiel anzeigen

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

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


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

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

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

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):


cs2#
```

8. Installieren Sie das NX-OS-Image.

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

Beispiel anzeigen

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

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

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

Verifying image type.
[] 100% -- SUCCESS

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

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

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

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



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



Images will be upgraded according to following table:

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

```
Switch will be reloaded for disruptive upgrade.

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

Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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

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

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

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version

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

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


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

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

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

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

10. Aktualisieren Sie das EPLD-Image und starten Sie den Switch neu.

Beispiel anzeigen

```
cs2# show version module 1 epld

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

cs2# install epld bootflash:n9000-epld.9.3.5.img module all
Compatibility check:
Module        Type         Upgradable        Impact    Reason
------  ------------------ ----------------- --------- -----------
     1         SUP         Yes       disruptive  Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------- ------ ----------------- ----------------- ------------
------------
     1  SUP    MI FPGA           0x07              0x07         No
     1  SUP    IO FPGA           0x17              0x19         Yes
     1  SUP    MI FPGA2          0x02              0x02         No
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (     64 of      64
sectors)
Module 1 EPLD upgrade is successful.
Module   Type  Upgrade-Result
-------- ----- --------------
     1   SUP   Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

11. Nach dem Neustart des Switches melden Sie sich erneut an und überprüfen Sie, ob die neue Version von EPLD erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld

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

12. Überprüfen Sie den Zustand der Cluster-Ports im Cluster.

    a. Überprüfen Sie, ob die Cluster-Ports auf allen Knoten im Cluster aktiv und fehlerfrei sind:

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

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0b       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

b. Überprüfen Sie den Zustand der Switches im Cluster.

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

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------------
cluster1-01/cdp
            e0a    cs1                       Ethernet1/7       N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/7       N9K-
C9336C-FX2
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/8       N9K-
C9336C-FX2
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/1     N9K-
C9336C-FX2
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C9336C-FX2
            e0b    cs2                       Ethernet1/1/2     N9K-
C9336C-FX2

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

cs2                         cluster-network    10.233.205.91    N9K-
```

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

2 entries were displayed.
```

Je nach der zuvor auf dem Switch geladenen RCF-Version kann die folgende Ausgabe auf der cs1-Switch-Konsole angezeigt werden:

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

13. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

    `cluster show`

    Beispiel anzeigen

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

14. Wiederholen Sie die Schritte 6 bis 13, um die NX-OS-Software auf Switch cs1 zu installieren.
15. Überprüfen Sie die Konnektivität der Remote-Cluster-Schnittstellen, bevor Sie die automatische Rücksetzung auf den Cluster-LIFs aktivieren:

ONTAP 9.9.1 und höher

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

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

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

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

```
cluster1::*> network interface check cluster-connectivity show
                                  Source               Destination
Packet
Node   Date                       LIF                  LIF
Loss
------ -------------------------- -------------------
------------------ -----------
cluster1-01
       3/5/2022 19:21:18 -06:00   cluster1-01_clus2    cluster1-02-
clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-01_clus2    cluster1-
02_clus2   none
cluster1-02
       3/5/2022 19:21:18 -06:00   cluster1-02_clus2    cluster1-
01_clus1   none
       3/5/2022 19:21:20 -06:00   cluster1-02_clus2    cluster1-
01_clus2   none
```

Alle ONTAP Versionen

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

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

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

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

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

1. Automatische Rücksetzung der Cluster-LIFs aktivieren.

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

2. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihren Heimatport zurückgekehrt sind:

   network interface show -vserver Cluster

Beispiel anzeigen

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

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

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

Wie geht es weiter?

Nach der Installation oder Aktualisierung der NX-OS-Software können Sie"Installieren oder aktualisieren Sie RCF" Die

Installieren oder aktualisieren Sie die RCF

Übersicht zur Installation oder Aktualisierung der Referenzkonfigurationsdatei (RCF).

Die Referenzkonfigurationsdatei (RCF) wird nach der erstmaligen Einrichtung des Speicherswitches Nexus 9336C-FX2 installiert. Sie aktualisieren Ihre RCF-Version, wenn auf Ihrem Switch eine vorhandene Version der RCF-Datei installiert ist.

Siehe den Artikel in der Wissensdatenbank."Wie man die Konfiguration eines Cisco Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält" Weitere Informationen zur Installation oder Aufrüstung Ihres RCF erhalten Sie bei Bedarf.

Verfügbare RCF-Konfigurationen

Die folgende Tabelle beschreibt die für verschiedene Konfigurationen verfügbaren RCFs. Wählen Sie den für Ihre Konfiguration passenden RCF aus. Sehen"Cisco Ethernet-Switches" für weitere Informationen.

Für spezifische Details zur Port- und VLAN-Nutzung verweisen wir auf den Abschnitt „Banner und wichtige Hinweise“ in Ihrem RCF.

RCF-Name	Beschreibung
2-Cluster-HA-Ausbruch	Unterstützt zwei ONTAP -Cluster mit mindestens acht Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
4-Cluster-HA-Ausbruch	Unterstützt vier ONTAP -Cluster mit mindestens vier Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
1-Cluster-HA	Alle Ports sind für 40/100GbE konfiguriert. Unterstützt gemeinsam genutzten Cluster-/HA-Datenverkehr auf Ports. Erforderlich für die Systeme AFF A320, AFF A250 und FAS500f . Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
1-Cluster-HA-Ausbruch	Die Ports sind für 4x10GbE Breakout, 4x25GbE Breakout (RCF 1.6+ auf 100GbE Switches) und 40/100GbE konfiguriert. Unterstützt gemeinsam genutzten Cluster-/HA-Datenverkehr auf Ports für Knoten, die gemeinsam genutzte Cluster-/HA-Ports verwenden: AFF A320, AFF A250 und FAS500f Systeme. Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
Cluster-HA-Speicher	Die Ports sind für 40/100GbE für Cluster+HA, 4x10GbE Breakout für Cluster und 4x25GbE Breakout für Cluster+HA sowie 100GbE für jedes Storage-HA-Paar konfiguriert.
Cluster	Zwei Varianten von RCF mit unterschiedlicher Belegung von 4x10GbE-Ports (Breakout) und 40/100GbE-Ports. Alle FAS und AFF Knoten werden unterstützt, mit Ausnahme der Systeme AFF A320, AFF A250 und FAS500f .
Storage	Alle Ports sind für 100GbE NVMe-Speicherverbindungen konfiguriert.

Verfügbare RCFs

Die folgende Tabelle listet die verfügbaren RCFs für die Switches 9336C-FX2 und 9336C-FX2-T auf. Wählen Sie die für Ihre Konfiguration passende RCF-Version aus. Sehen"Cisco Ethernet-Switches" für weitere Informationen.

RCF-Name
Cluster-HA-Breakout RCF 1.*xx*
Cluster-HA-Storage RCF 1.*xx*
Speicher RCF 1.*xx*
MultiCluster-HA RCF 1.*xx*

Empfohlene Dokumentation

- "Cisco Ethernet-Switches"

  Auf der NetApp Support-Website finden Sie die Tabelle zur Switch-Kompatibilität, in der die unterstützten ONTAP und RCF-Versionen aufgeführt sind. Beachten Sie, dass zwischen der Befehlssyntax in der RCF und der Syntax in bestimmten Versionen von NX-OS Befehlsabhängigkeiten bestehen können.

- "Cisco Nexus 9000 Series Switches"

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

Zu den Beispielen

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

- Die Namen der beiden Cisco Switches lauten cs1 und cs2.
- Die Knotennamen sind node1-01, node1-02, node1-03 und node1-04.
- Die Cluster-LIF-Namen sind node1-01_clus1, node1-01_clus2, node1-02_clus1, node1-02_clus2, node1-03_clus1, node1-03_clus2, node1-04_clus1 und node1-04_clus2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

Siehe die "Hardware Universe" um die korrekten Ports auf Ihrer Plattform zu überprüfen.

Die Befehlsausgaben können je nach ONTAP Version variieren.

verwendete Befehle

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

Wie geht es weiter?

Nachdem Sie die Installations- oder Aktualisierungsprozedur für RCF durchgelesen haben, können Sie"Installieren Sie den RCF" oder"Aktualisieren Sie Ihren RCF" nach Bedarf.

Installieren Sie die Referenzkonfigurationsdatei

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Speicher-Switches Nexus 9336C-FX2 und 9336C-FX2-T zum ersten Mal eingerichtet haben.

Siehe den Artikel in der Wissensdatenbank."Wie man die Konfiguration eines Cisco Interconnect-Switches

löscht und gleichzeitig die Remote-Konnektivität beibehält" Weitere Informationen zur Installation Ihres RCF erhalten Sie bei Bedarf.

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Eine Konsolenverbindung zum Switch. Die Konsolenverbindung ist optional, wenn Sie Fernzugriff auf den Switch haben.
- Die Switches cs1 und cs2 sind eingeschaltet und die Ersteinrichtung der Switches ist abgeschlossen (die Management-IP-Adresse und SSH sind eingerichtet).
- Die gewünschte NX-OS-Version wurde installiert.
- Die Ports des ONTAP Knotenclusters sind nicht verbunden.

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich über SSH oder über eine serielle Konsole am Switch cs1 an.
2. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs1: FTP, TFTP, SFTP oder SCP.

   Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" .

   Beispiel anzeigen

   Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches cs1 zu kopieren:

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

3. Wenden Sie die zuvor heruntergeladene RCF-Datei auf den Bootflash an.

   Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" .

Beispiel anzeigen

Dieses Beispiel zeigt die RCF `Nexus_9336C_RCF_v1.6-Storage.txt` wird auf Switch CS1 installiert:

```
cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-
commands
```

4. Untersuchen Sie die Bannerausgabe von `show banner motd` Befehl. Sie müssen diese Anweisungen lesen und befolgen, um die korrekte Konfiguration und den ordnungsgemäßen Betrieb des Schalters sicherzustellen.

Beispiel anzeigen

```
cs1# show banner motd

**********************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch    : Nexus N9K-C9336C-FX2
* Filename  : Nexus_9336C_RCF_v1.6-Storage.txt
* Date      : 10-23-2020
* Version   : v1.6
*
* Port Usage : Storage configuration
* Ports  1-36: 100GbE Controller and Shelf Storage Ports
**********************************************************************
**********
```

5. Überprüfen Sie, ob es sich bei der RCF um die korrekte, neuere Version handelt:

`show running-config`

Wenn Sie die Ausgabe überprüfen, um sicherzustellen, dass Sie die richtige RCF-Datei haben, achten Sie darauf, dass die folgenden Informationen korrekt sind:

- Das RCF-Banner
- Die Knoten- und Porteinstellungen
- Anpassungen

  Das Ergebnis variiert je nach Ihrer Website-Konfiguration. Prüfen Sie die Port-Einstellungen und beachten Sie die Versionshinweise, um sich über etwaige Änderungen zu informieren, die speziell für die von Ihnen installierte RCF-Version gelten.

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

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

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

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

9. Bei der Installation von RCF Version 1.12 und höher führen Sie die folgenden Befehle aus:

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

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

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

   Siehe den Artikel in der Wissensdatenbank."Wie man die Konfiguration eines Cisco Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält" für weitere Einzelheiten.

10. Überprüfen Sie, ob die `write_erase.cfg` Die Datei ist wie erwartet gefüllt:

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

11. Stellen Sie die `write erase` Befehl zum Löschen der aktuell gespeicherten Konfiguration:

```
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 Basiskonfiguration in die Startkonfiguration.

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

13. Neustart des Switches cs1.

```
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. Überprüfen Sie, ob die mit den Cluster-Ports verbundenen Switch-Ports **aktiv** sind.

```
show interface brief
```

Beispiel anzeigen

```
cs1# show interface brief | grep up
mgmt0  --           up     <mgmt ip address>
1000    1500
Eth1/11         1       eth  trunk  up      none
100G(D) --
Eth1/12         1       eth  trunk  up      none
100G(D) --
Eth1/13         1       eth  trunk  up      none
100G(D) --
Eth1/14         1       eth  trunk  up      none
100G(D) --
Eth1/15         1       eth  trunk  up      none
100G(D) --
Eth1/16         1       eth  trunk  up      none
100G(D) --
Eth1/17         1       eth  trunk  up      none
100G(D) --
Eth1/18         1       eth  trunk  up      none
100G(D) --
Eth1/23         1       eth  trunk  up      none
100G(D) --
Eth1/24         1       eth  trunk  up      none
100G(D) --
Eth1/25         1       eth  trunk  up      none
100G(D) --
Eth1/26         1       eth  trunk  up      none
100G(D) --
Eth1/27         1       eth  trunk  up      none
100G(D) --
Eth1/28         1       eth  trunk  up      none
100G(D) --
Eth1/29         1       eth  trunk  up      none
100G(D) --
Eth1/30         1       eth  trunk  up      none
100G(D) --
```

2. Überprüfen Sie mithilfe der folgenden Befehle, ob sich die Clusterknoten in den richtigen Cluster-VLANs befinden:

   `show vlan brief`

   `show interface trunk`

Beispiel anzeigen

```
cs1# show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- ---------
------------------------------
1    default                           active    Po999
30   VLAN0030                          active    Eth1/1, Eth1/2,
Eth1/3, Eth1/4
                                                 Eth1/5, Eth1/6,
Eth1/7, Eth1/8
                                                 Eth1/9, Eth1/10,
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,
Eth1/26
                                                 Eth1/27, Eth1/28,
Eth1/29
                                                 Eth1/30, Eth1/31,
Eth1/32
                                                 Eth1/33, Eth1/34,
Eth1/35
                                                 Eth1/36

cs1# show interface trunk

----------------------------------------------------
Port          Native  Status        Port
              Vlan                  Channel
----------------------------------------------------
Eth1/1        1       trunking      --
Eth1/2        1       trunking      --
Eth1/3        1       trunking      --
Eth1/4        1       trunking      --
Eth1/5        1       trunking      --
Eth1/6        1       trunking      --
Eth1/7        1       trunking      --
Eth1/8        1       trunking      --
```

```
Eth1/9        1       trunking      --
Eth1/10       1       trunking      --
Eth1/11       1       trunking      --
Eth1/12       1       trunking      --
Eth1/13       1       trunking      --
Eth1/14       1       trunking      --
Eth1/15       1       trunking      --
Eth1/16       1       trunking      --
Eth1/17       1       trunking      --
Eth1/18       1       trunking      --
Eth1/19       1       trunking      --
Eth1/20       1       trunking      --
Eth1/21       1       trunking      --
Eth1/22       1       trunking      --
Eth1/23       1       trunking      --
Eth1/24       1       trunking      --
Eth1/25       1       trunking      --
Eth1/26       1       trunking      --
Eth1/27       1       trunking      --
Eth1/28       1       trunking      --
Eth1/29       1       trunking      --
Eth1/30       1       trunking      --
Eth1/31       1       trunking      --
Eth1/32       1       trunking      --
Eth1/33       1       trunking      --
Eth1/34       1       trunking      --
Eth1/35       1       trunking      --
Eth1/36       1       trunking      --

--------------------------------------------------------------------------
------------
Port          Vlans Allowed on Trunk
--------------------------------------------------------------------------
------------
Eth1/1        30
Eth1/2        30
Eth1/3        30
Eth1/4        30
Eth1/5        30
Eth1/6        30
Eth1/7        30
Eth1/8        30
Eth1/9        30
Eth1/10       30
Eth1/11       30
Eth1/12       30
```

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

--------------------------------------------------------------------------
------------
Port          Vlans Err-disabled on Trunk
--------------------------------------------------------------------------
------------
Eth1/1        none
Eth1/2        none
Eth1/3        none
Eth1/4        none
Eth1/5        none
Eth1/6        none
Eth1/7        none
Eth1/8        none
Eth1/9        none
Eth1/10       none
Eth1/11       none
Eth1/12       none
Eth1/13       none
Eth1/14       none
Eth1/15       none
Eth1/16       none
```

```
Eth1/17       none
Eth1/18       none
Eth1/19       none
Eth1/20       none
Eth1/21       none
Eth1/22       none
Eth1/23       none
Eth1/24       none
Eth1/25       none
Eth1/26       none
Eth1/27       none
Eth1/28       none
Eth1/29       none
Eth1/30       none
Eth1/31       none
Eth1/32       none
Eth1/33       none
Eth1/34       none
Eth1/35       none
Eth1/36       none

--------------------------------------------------------------------------
------------
Port          STP Forwarding
--------------------------------------------------------------------------
------------
Eth1/1        none
Eth1/2        none
Eth1/3        none
Eth1/4        none
Eth1/5        none
Eth1/6        none
Eth1/7        none
Eth1/8        none
Eth1/9        none
Eth1/10       none
Eth1/11       30
Eth1/12       30
Eth1/13       30
Eth1/14       30
Eth1/15       30
Eth1/16       30
Eth1/17       30
Eth1/18       30
Eth1/19       none
Eth1/20       none
```

```
Eth1/21       none
Eth1/22       none
Eth1/23       30
Eth1/24       30
Eth1/25       30
Eth1/26       30
Eth1/27       30
Eth1/28       30
Eth1/29       30
Eth1/30       30
Eth1/31       none
Eth1/32       none
Eth1/33       none
Eth1/34       none
Eth1/35       none
Eth1/36       none

--------------------------------------------------------------------------------
Port          Vlans in spanning tree forwarding state and not pruned
--------------------------------------------------------------------------------
Eth1/1        Feature VTP is not enabled
none
Eth1/2        Feature VTP is not enabled
none
Eth1/3        Feature VTP is not enabled
none
Eth1/4        Feature VTP is not enabled
none
Eth1/5        Feature VTP is not enabled
none
Eth1/6        Feature VTP is not enabled
none
Eth1/7        Feature VTP is not enabled
none
Eth1/8        Feature VTP is not enabled
none
Eth1/9        Feature VTP is not enabled
none
Eth1/10       Feature VTP is not enabled
none
Eth1/11       Feature VTP is not enabled
30
Eth1/12       Feature VTP is not enabled
30
```

```
Eth1/13       Feature VTP is not enabled
30
Eth1/14       Feature VTP is not enabled
30
Eth1/15       Feature VTP is not enabled
30
Eth1/16       Feature VTP is not enabled
30
Eth1/17       Feature VTP is not enabled
30
Eth1/18       Feature VTP is not enabled
30
Eth1/19       Feature VTP is not enabled
none
Eth1/20       Feature VTP is not enabled
none
Eth1/21       Feature VTP is not enabled
none
Eth1/22       Feature VTP is not enabled
none
Eth1/23       Feature VTP is not enabled
30
Eth1/24       Feature VTP is not enabled
30
Eth1/25       Feature VTP is not enabled
30
Eth1/26       Feature VTP is not enabled
30
Eth1/27       Feature VTP is not enabled
30
Eth1/28       Feature VTP is not enabled
30
Eth1/29       Feature VTP is not enabled
30
Eth1/30       Feature VTP is not enabled
30
Eth1/31       Feature VTP is not enabled
none
Eth1/32       Feature VTP is not enabled
none
Eth1/33       Feature VTP is not enabled
none
Eth1/34       Feature VTP is not enabled
none
Eth1/35       Feature VTP is not enabled
none
```

```
Eth1/36       Feature VTP is not enabled
none
```

Für spezifische Details zur Port- und VLAN-Nutzung verweisen wir auf den Abschnitt „Banner und wichtige Hinweise“ in Ihrem RCF.

Schritt 3: Richten Sie Ihren ONTAP Cluster ein.

NetApp empfiehlt, neue Cluster mit dem System Manager einzurichten.

System Manager bietet einen einfachen und unkomplizierten Workflow für die Einrichtung und Konfiguration von Clustern, einschließlich der Zuweisung einer Knotenverwaltungs-IP-Adresse, der Initialisierung des Clusters, der Erstellung einer lokalen Ebene, der Konfiguration von Protokollen und der Bereitstellung des anfänglichen Speichers.

Gehe zu "Konfigurieren Sie ONTAP auf einem neuen Cluster mit System Manager" für Installationsanweisungen.

Wie geht es weiter?

Nach der Installation Ihres RCF können Sie"Überprüfen Sie die SSH-Konfiguration"

Aktualisieren Sie Ihre Referenzkonfigurationsdatei (RCF)

Sie aktualisieren Ihre RCF-Version, wenn auf Ihren betriebsbereiten Switches bereits eine Version der RCF-Datei installiert ist.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Der aktuelle RCF.
- Wenn Sie Ihre RCF-Version aktualisieren, benötigen Sie eine Boot-Konfiguration in der RCF, die die gewünschten Boot-Images widerspiegelt.

  Wenn Sie die Bootkonfiguration ändern müssen, um die aktuellen Boot-Images widerzuspiegeln, müssen Sie dies tun, bevor Sie die RCF erneut anwenden, damit bei zukünftigen Neustarts die richtige Version instanziiert wird.

Während dieses Vorgangs ist kein betriebsbereiter Inter-Switch-Link (ISL) erforderlich. Dies ist beabsichtigt, da RCF-Versionsänderungen die ISL-Konnektivität vorübergehend beeinträchtigen können. Um einen unterbrechungsfreien Clusterbetrieb zu gewährleisten, migriert das folgende Verfahren alle Cluster-LIFs zum operativen Partner-Switch, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Vor der Installation einer neuen Switch-Softwareversion und neuer RCFs müssen Sie die Switch-Einstellungen löschen und eine Basiskonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein oder grundlegende Konfigurationsinformationen gesichert haben, bevor Sie die Switch-Einstellungen löschen.

Schritt 1: Vorbereitung auf das Upgrade

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

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

   Wobei *x* die Dauer des Wartungsfensters in Stunden angibt.

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

   ```
   set -privilege advanced
   ```

   Die erweiterte Eingabeaufforderung (*>) wird angezeigt.

3. Zeigen Sie die Ports auf jedem Knoten an, die mit den Switches verbunden sind:

   ```
   network device-discovery show
   ```

   Beispiel anzeigen

   ```
   cluster1::*> network device-discovery show
   Node/       Local  Discovered
   Protocol    Port   Device (LLDP: ChassisID) Interface       Platform
   ----------- ------ ----------------------- ---------------
   ---------
   node1-01/cdp
               e3a    cs1                      Ethernet1/7     N9K-
   C9336C
               e3b    cs2                      Ethernet1/7     N9K-
   C9336C
   node1-02/cdp
               e3a    cs1                      Ethernet1/8     N9K-
   C9336C
               e3b    cs2                      Ethernet1/8     N9K-
   C9336C
   .
   .
   .
   ```

4. Überprüfen Sie, ob alle Speicherports aktiv sind und einen fehlerfreien Status aufweisen:

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

Beispiel anzeigen

```
cluster1::*> storage port show -port-type ENET


                                    Speed
Node                Port Type  Mode    (Gb/s) State    Status
------------------ ---- ----- ------- ------ -------- -----------
node1-01
                    e3a ENET  -         100   enabled  online
                    e3b ENET  -         100   enabled  online
                    e7a ENET  -         100   enabled  online
                    e7b ENET  -         100   enabled  online
node1-02
                    e3a ENET  -         100   enabled  online
                    e3b ENET  -         100   enabled  online
                    e7a ENET  -         100   enabled  online
                    e7b ENET  -         100   enabled  online
.
.
.
```

5. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

Schritt 2: Ports konfigurieren

1. Fahren Sie auf Switch CS1 die Ports herunter, die mit allen Ports der Knoten verbunden sind.

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

Stellen Sie sicher, dass Sie **alle** verbundenen Ports herunterfahren, um Probleme mit der Netzwerkverbindung zu vermeiden. Siehe den Artikel in der Wissensdatenbank. "Knoten außerhalb des Quorums bei Migration des Cluster-LIF während des Switch-OS-Upgrades" für weitere Einzelheiten.

2. Überprüfen Sie, ob für die Cluster-LIFs ein Failover auf die auf 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
            node1-01_clus1  up/up      169.254.36.44/16   node1-01
e7a     true
            node1-01_clus2  up/up      169.254.7.5/16     node1-01
e7b     true
            node1-02_clus1  up/up      169.254.197.206/16 node1-02
e7a     true
            node1-02_clus2  up/up      169.254.195.186/16 node1-02
e7b     true
            node1-03_clus1  up/up      169.254.192.49/16  node1-03
e7a     true
            node1-03_clus2  up/up      169.254.182.76/16  node1-03
e7b     true
            node1-04_clus1  up/up      169.254.59.49/16   node1-04
e7a     true
            node1-04_clus2  up/up      169.254.62.244/16  node1-04
e7b     true

8 entries were displayed.
```

3. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  -------
node1-01             true    true          false
node1-02             true    true          false
node1-03             true    true          true
node1-04             true    true          false

4 entries were displayed.
```

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

   `show running-config`

   a. Alle benutzerdefinierten Ergänzungen zwischen dem aktuellen `running-config` und die verwendete RCF-Datei (z. B. eine SNMP-Konfiguration für Ihre Organisation).

   b. Für NX-OS 10.2 und höher verwenden Sie die `show diff running-config` Befehl zum Vergleich mit der gespeicherten RCF-Datei im Bootflash. Alternativ können Sie ein Vergleichstool eines Drittanbieters verwenden.

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

   Stellen Sie sicher, dass Sie Folgendes konfigurieren:

   - Benutzername und Passwort
   - Verwaltungs-IP-Adresse
   - Standardgateway
   - Schaltername

```
cs1# show run | i "username admin password" > bootflash:write_erase.cfg

cs1# show run | section "vrf context management" >> bootflash:write_erase.cfg

cs1# show run | section "interface mgmt0" >> bootflash:write_erase.cfg

cs1# show run | section "switchname" >> bootflash:write_erase.cfg
```

6. Beim Upgrade auf RCF Version 1.12 und höher führen Sie die folgenden Befehle aus:

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

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

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

Siehe den Artikel in der Wissensdatenbank."Wie man die Konfiguration eines Cisco Interconnect-Switches löscht und gleichzeitig die Remote-Konnektivität beibehält" für weitere Einzelheiten.

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

   `show file bootflash:write_erase.cfg`

8. Stellen Sie die `write erase` Befehl zum Löschen der aktuell gespeicherten Konfiguration:

   ```
   cs1# write erase

   Warning: This command will erase the startup-configuration.

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

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

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

10. Starten Sie den Switch neu:

    ```
    cs1# reload

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

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

    Möglicherweise müssen Sie die Einträge in der Host-Datei aktualisieren, die mit den SSH-Schlüsseln zusammenhängen.

12. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs1: FTP, TFTP, SFTP oder SCP.

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" Führer.

Beispiel anzeigen

Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches cs1 zu kopieren:

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

13. Wenden Sie die zuvor heruntergeladene RCF-Datei auf den Bootflash an.

    Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" Führer.

    Dieses Beispiel zeigt die RCF-Datei. `NX9336C-FX2-RCF-v1.13-1-Storage.txt` wird auf Switch CS1 installiert:

    ```
    cs1# copy Nexus_9336C_RCF_v1.6-Storage.txt running-config echo-commands
    ```

    Lesen Sie die Abschnitte **Installationshinweise**, **Wichtige Hinweise** und **Banner** Ihres RCF gründlich durch. Sie müssen diese Anweisungen lesen und befolgen, um die ordnungsgemäße Konfiguration und den ordnungsgemäßen Betrieb des Switches sicherzustellen.

14. Überprüfen Sie, ob es sich bei der RCF-Datei um die korrekte, neuere Version handelt:

    `show running-config`

    Wenn Sie die Ausgabe überprüfen, um sicherzustellen, dass Sie die richtige RCF-Datei haben, achten Sie darauf, dass die folgenden Informationen korrekt sind:

    - Das RCF-Banner
    - Die Knoten- und Porteinstellungen
    - Anpassungen

      Das Ergebnis variiert je nach Ihrer Website-Konfiguration. Prüfen Sie die Port-Einstellungen und beachten Sie die Versionshinweise, um sich über etwaige Änderungen zu informieren, die speziell für die von Ihnen installierte RCF-Version gelten.

15. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an.
16. Nachdem Sie überprüft haben, ob die RCF-Versionen, die benutzerdefinierten Erweiterungen und die Schaltereinstellungen korrekt sind, kopieren Sie die `running-config` Datei an die `startup-config` Datei.

Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 9000 Serie NX-OS Befehlsreferenz" Führer.

```
cs1# copy running-config startup-config

[] 100% Copy complete
```

17. Neustart des Switches cs1. Sie können die Warnungen „`cluster switch health monitor`“ und die Ereignisse „`cluster ports down`“, die auf den Knoten während des Neustarts des Switches gemeldet werden, ignorieren.

```
cs1# reload

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

18. Überprüfen Sie, ob alle Speicherports aktiv sind und einen fehlerfreien Status aufweisen:

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

Beispiel anzeigen

```
cluster1::*> storage port show -port-type ENET


                                  Speed
Node                Port Type  Mode    (Gb/s) State    Status
------------------- ---- ----- ------- ------ -------- -----------
node1-01
                    e3a  ENET  -          100 enabled  online
                    e3b  ENET  -          100 enabled  online
                    e7a  ENET  -          100 enabled  online
                    e7b  ENET  -          100 enabled  online
node1-02
                    e3a  ENET  -          100 enabled  online
                    e3b  ENET  -          100 enabled  online
                    e7a  ENET  -          100 enabled  online
                    e7b  ENET  -          100 enabled  online
.
.
.
```

19. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

Beispiel anzeigen

```
cluster1::*> cluster show
Node                 Health   Eligibility   Epsilon
-------------------- -------- ------------- -------
node1-01             true     true          false
node1-02             true     true          false
node1-03             true     true          true
node1-04             true     true          false

4 entries were displayed.
```

20. Wiederholen Sie die Schritte 4 bis 19 auf Switch cs2.
21. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

Schritt 3: Überprüfen Sie die Clusternetzwerkkonfiguration und den Clusterzustand.

1. Überprüfen Sie, ob die mit den Cluster-Ports verbundenen Switch-Ports **aktiv** sind.

```
show interface brief
```

2. Überprüfen Sie, ob die erwarteten Knoten noch verbunden sind:

```
show cdp neighbors
```

3. Überprüfen Sie mithilfe der folgenden Befehle, ob sich die Clusterknoten in den richtigen Cluster-VLANs befinden:

```
show vlan brief
```

```
show interface trunk
```

4. Überprüfen Sie, ob die Cluster-LIFs wieder auf ihren Heimatport zurückgekehrt sind:

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

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

```
network interface revert -vserver vserver_name -lif <lif-name>
```

5. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

```
cluster show
```

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

   a. Sie können die `network interface check cluster-connectivity show` Befehl zum Anzeigen der Details einer Zugriffsprüfung für die Clusterkonnektivität:

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

   b. Alternativ können Sie die `cluster ping-cluster -node <node-name>` Befehl zum Überprüfen der Verbindung:

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

Wie geht es weiter?

Nach dem Upgrade Ihres RCF können Sie"Überprüfen Sie die SSH-Konfiguration" Die

Überprüfen Sie Ihre SSH-Konfiguration

Wenn Sie die Funktionen Ethernet Switch Health Monitor (CSHM) und Protokollerfassung verwenden, überprüfen Sie, ob SSH und SSH-Schlüssel auf den Cluster-Switches aktiviert sind.

Schritte

1. Überprüfen Sie, ob SSH aktiviert ist:

```
(switch) show ssh server
ssh version 2 is enabled
```

2. Überprüfen Sie, ob die SSH-Schlüssel aktiviert sind:

```
show ssh key
```

Beispiel anzeigen

```
(switch)# show ssh key

rsa Keys generated:Fri Jun 28 02:16:00 2024

ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQDiNrD52Q586wTGJjFAbjBlFaA23EpDrZ2sDCew
l7nwlioC6HBejxluIObAH8hrW8kR+gj0ZAfPpNeLGTg3APj/yiPTBoIZZxbWRShywAM5
PqyxWwRb7kp9Zt1YHzVuHYpSO82KUDowKrL6lox/YtpKoZUDZjrZjAp8hTv3JZsPgQ==

bitcount:1024
fingerprint:
SHA256:aHwhpzo7+YCDSrp3isJv2uVGz+mjMMokqdMeXVVXfdo

could not retrieve dsa key information

ecdsa Keys generated:Fri Jun 28 02:30:56 2024

ecdsa-sha2-nistp521
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWy1wgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVIewCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRAlZeHwQ

(switch)# show feature | include scpServer
scpServer             1          enabled
(switch)# show feature | include ssh
sshServer             1          enabled
(switch)#
```

Wenn Sie FIPS aktivieren, müssen Sie die Bitanzahl am Switch mithilfe des Befehls auf 256 ändern. `ssh key ecdsa 256 force` Die Sehen "Konfigurieren Sie die Netzwerksicherheit mithilfe von FIPS." Weitere Einzelheiten.

Wie geht es weiter?

Nachdem Sie Ihre SSH-Konfiguration überprüft haben,"Konfigurieren der Switch-Integritätsüberwachung" Die

Setzen Sie die Speicher-Switches 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurück

Um die Speicherschalter 9336C-FX2 und 9336C-FX2-T auf die Werkseinstellungen zurückzusetzen, müssen Sie die Schaltereinstellungen 9336C-FX2 und 9336C-FX2-T löschen.

Informationen zu diesem Vorgang

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

Schritte

1. Löschen Sie die vorhandene Konfiguration:

   `write erase`

   ```
   (cs2)# write erase

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

2. Laden Sie die Switch-Software neu:

   `reload`

   ```
   (cs2)# reload

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

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

Was kommt als nächstes

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

Ersetzen Sie die Speicher-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T

Sie können defekte Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem Clusternetzwerk ersetzen. Dies ist ein unterbrechungsfreies Verfahren.

Bevor Sie beginnen

Stellen Sie vor der Installation der NX-OS-Software und RCFs auf den Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Speicher-Switches Folgendes sicher:

- Ihr System kann die Speicher-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T unterstützen.
- Sie haben die Switch-Kompatibilitätstabelle auf der Cisco Ethernet Switch-Seite konsultiert, um die unterstützten ONTAP, NX-OS- und RCF-Versionen zu ermitteln.
- Sie haben die entsprechenden Software- und Upgrade-Anleitungen auf der Cisco -Website konsultiert.

Cisco Nexus 3000 Series Switches:

- Sie haben die entsprechenden RCFs heruntergeladen.
- Die bestehende Netzwerkkonfiguration weist folgende Merkmale auf:
  - Auf der Cisco Ethernet Switches-Seite finden Sie die neuesten RCF- und NX-OS-Versionen für Ihre Switches.
  - Die Management-Konnektivität muss auf beiden Switches vorhanden sein.
- Der Ersatz-Switch Cisco Nexus 9336C-FX2 weist folgende Merkmale auf:
  - Die Managementnetzwerkanbindung ist funktionsfähig.
  - Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
  - Das entsprechende RCF- und NX-OS-Betriebssystemabbild wird auf den Switch geladen.
  - Die Erstkonfiguration des Schalters ist abgeschlossen.

Informationen zu diesem Vorgang

Bei diesem Verfahren wird der zweite Nexus 9336C-FX2 Speicherswitch S2 durch den neuen 9336C-FX Switch NS2 ersetzt. Die beiden Knoten sind Knoten1 und Knoten2.

Zu erledigende Schritte:

- Bestätigen Sie, dass es sich bei dem auszutauschenden Schalter um S2 handelt.
- Die Kabel vom Schalter S2 abziehen.
- Schließen Sie die Kabel wieder an den Schalter NS2 an.
- Überprüfen Sie alle Gerätekonfigurationen auf dem Switch NS2.

> Zwischen der Befehlssyntax in den RCF- und NX-OS-Versionen können Abhängigkeiten bestehen.

Schritte

1. Wenn AutoSupport auf diesem Cluster aktiviert ist, unterdrücken Sie die automatische Fallerstellung durch Aufruf einer AutoSupport -Nachricht:

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

   x ist die Dauer des Wartungsfensters in Stunden.

2. Überprüfen Sie den Gesundheitszustand der Speicherknotenports, um sicherzustellen, dass eine Verbindung zum Speicherswitch S1 besteht:

   ```
   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
               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. Prüfen Sie, ob 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. Leite die Show `lldp neighbors` Führen Sie einen Befehl auf dem funktionierenden Switch aus, um zu bestätigen, dass Sie beide Knoten und alle Regale 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 Regalanschlüsse im Lagersystem:

   ```
   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 Speicherschalter S2 angeschlossen sind.
7. Schließen Sie alle Kabel wieder an den Ersatzschalter NS2 an.
8. Überprüfen Sie erneut den Gesundheitszustand der Speicherknotenports:

   ```
   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
                     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 Schalter 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 Regalanschlüsse im Lagersystem:

    ```
    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 Fallerstellung unterdrückt haben, können Sie sie durch Aufruf einer AutoSupport Nachricht wieder aktivieren:

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

Wie geht es weiter?

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