Speicherschalter

Install and maintain

NetApp
February 13, 2026

Inhalt

Speicherschalter

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.

"Überprüfen der Konfigurationsanforderungen"

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

"Überprüfen Sie die Komponenten und Teilenummern"

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

"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.

"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.

"Installieren Sie die Hardware"

Installieren Sie die Switch-Hardware.

"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.
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.

Dokumenttitel	Beschreibung
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
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

Clusterschalter A		Clusterschalter B	
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	

Clusterschalter A		Clusterschalter B	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	

Clusterschalter A		Clusterschalter B	
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
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

Clusterschalter A		Clusterschalter B	
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	
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:

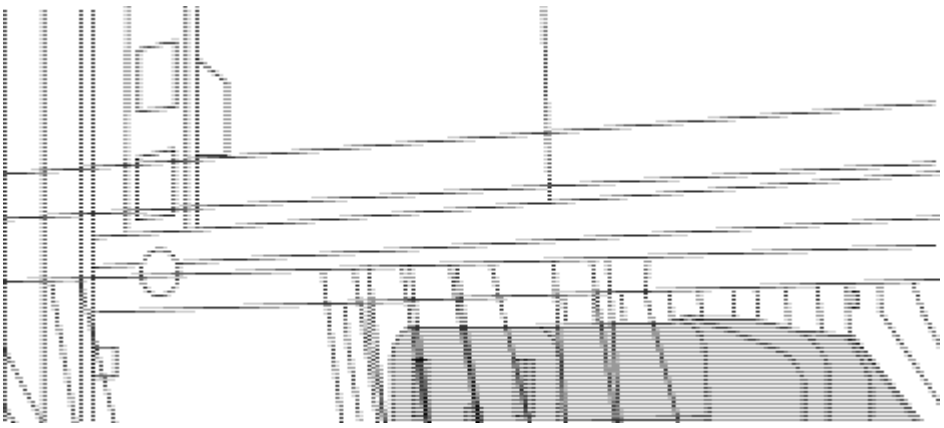
   - Eine Durchgangs-Blindplatte
   - Vier 10-32 x 0,75 Schrauben
   - Vier 10-32 Clipmuttern
     i. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

     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.

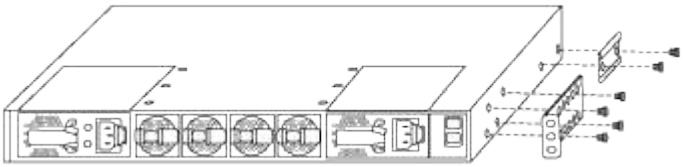
     iv. Führen Sie die weiblichen Stecker beider 48-Zoll-Überbrückungskabel von der Rückseite des Bedienfelds durch die Bürstenbaugruppe.



(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.

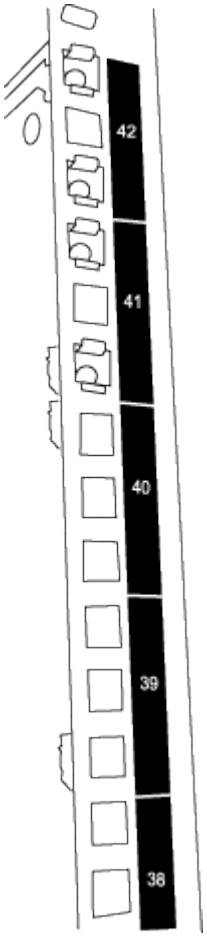


b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.

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.

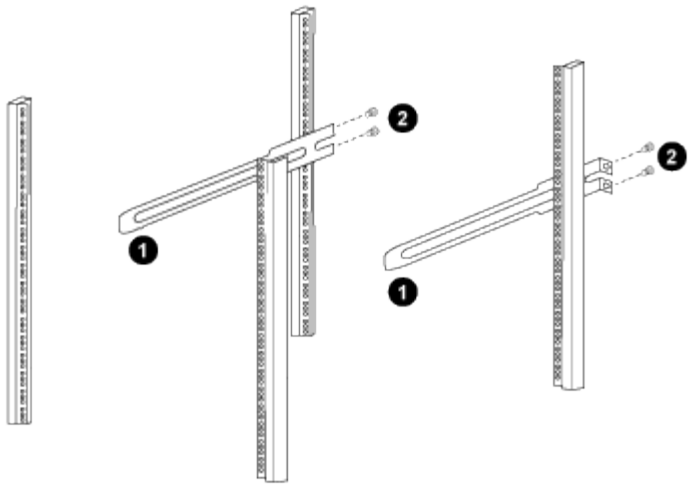
3. Installieren Sie die Clipmuttern in den quadratischen Lochpositionen für alle vier IEA-Pfosten.



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.

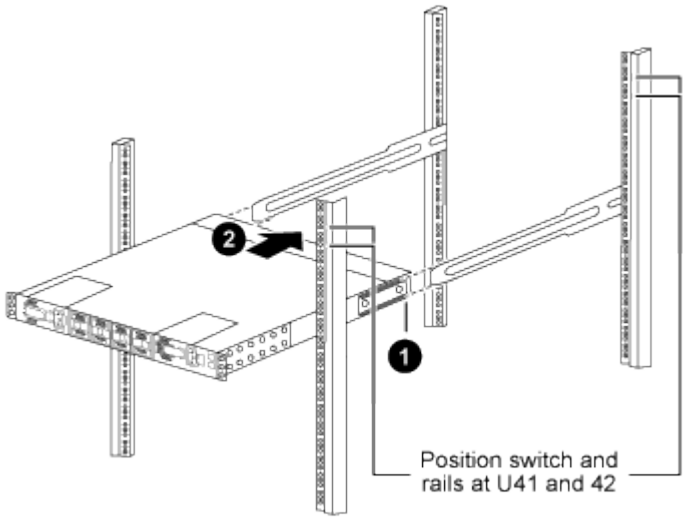
a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.

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.

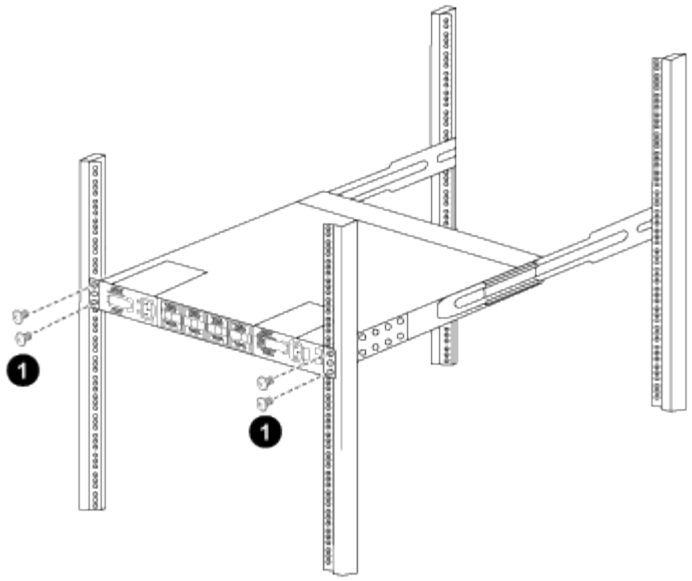
a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(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.
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.

Prompt	Antwort
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.
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.

Prompt	Antwort
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

Cisco Nexus 3232C

Erste Schritte

Installations- und Einrichtungsworkflow für Cisco Nexus 3232C Storage Switches

Die Cisco Nexus 3232C Switches sind Teil der Cisco Nexus 9000 Plattform und können in einem NetApp Systemschrank installiert werden.

Befolgen Sie diese Arbeitsschritte, um Ihre Cisco 3232C Switches zu installieren und einzurichten.

1. **"Überprüfen der Konfigurationsanforderungen"**

Prüfen Sie die Konfigurationsanforderungen für die 3232C storage switches.

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

Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 3232C-Switches und den ONTAP Cluster einzurichten.

3 **"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.

4 **"Installieren Sie die Hardware"**

Installieren Sie die Switch-Hardware.

5 **"Konfigurieren der Software"**

Konfigurieren Sie die Switch-Software.

Konfigurationsanforderungen für Cisco Nexus 3232C Storage Switches

Bei der Installation und Wartung des Cisco Nexus 3232C Switches sollten Sie unbedingt die Konfigurations- und Netzwerkanforderungen überprüfen.

Konfigurationsanforderungen

Sie benötigen die passende Anzahl und Art von Kabeln und Kabelsteckern für Ihre Switches. Je nach Typ des Switches, den Sie zunächst konfigurieren, müssen Sie den Konsolenport des Switches mit dem mitgelieferten Konsolenkabel verbinden; außerdem müssen Sie spezifische Netzwerkinformationen bereitstellen.

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 A700 verwendet die e0M-Schnittstelle einen dedizierten Ethernet-Anschluss.

Siehe die "Hardware Universe" für die aktuellsten Informationen. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

Was kommt als nächstes

Nachdem Sie Ihre Konfigurationsanforderungen bestätigt haben, können Sie die "erforderliche Dokumentation" überprüfen.

Dokumentationsanforderungen für Cisco Nexus 3232C Storage Switches

Für die Installation und Wartung des Cisco Nexus 3232C Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation lesen.

Switch-Dokumentation

Für die Einrichtung der Cisco Nexus 3232C Switches benötigen Sie die folgende Dokumentation von "Cisco

Nexus 3000 Series Switches Unterstützung" Seite.

Dokumenttitel	Beschreibung
Hardware-Installationsanleitung für die Nexus 3000-Serie	Bietet detaillierte Informationen zu Standortanforderungen, Hardware-Details der Schalter und Installationsoptionen.
Softwarekonfigurationshandbücher für Cisco Nexus 3000 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 3000 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 3000 Serie NX-OS Befehlsreferenz – Masterindex	Bietet Links zu den verschiedenen Befehlsreferenzen von Cisco.
Cisco Nexus 3000 MIBs-Referenz	Beschreibt die Management Information Base (MIB)-Dateien für die Nexus 3000 Switches.
Referenz der NX-OS-Systemmeldungen der Nexus 3000-Serie	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 3000-Serie, sowohl die informativen als auch die, die bei der Diagnose von Problemen mit Verbindungen, interner Hardware oder der Systemsoftware hilfreich sein können.
Cisco Nexus 3000 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 3000-Serie.
Informationen zu Vorschriften, Konformität und Sicherheit für die Cisco Nexus 6000-, Cisco Nexus 5000-, Cisco Nexus 3000- und Cisco Nexus 2000-Serie	Bietet Informationen zur Einhaltung internationaler behördlicher Vorschriften, zur Sicherheit und zu gesetzlichen Bestimmungen für die Switches der Nexus 3000-Serie.

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 3232C 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 Nexus 3232C Switch in einem NetApp -Schrank"	Beschreibt die Installation eines Cisco Nexus 3232C 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 der Hardware

Workflow zur Hardwareinstallation für Cisco Nexus 3232C-Switches

Um die Hardware für einen 3232C-Speicherswitch zu installieren und zu konfigurieren, führen Sie die folgenden Schritte aus:

1. **"Installieren Sie den Schalter"**
Installieren Sie den 3232C-Speicherschalter.

2. **"Installieren Sie den Switch in einem NetApp -Schrank."**
Installieren Sie den 3232C-Speicherschalter und die Durchgangsplatte in einem NetApp-Schrank nach Bedarf.

Installieren Sie den 3232C-Speicherschalter

Führen Sie dieses Verfahren aus, um den Cisco Nexus 3232C Storage-Switch einzurichten und 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.
- 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 Switch- und ONTAP Dokumentation".

Schritte

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

Wenn Sie die… installieren	Dann…
Cisco Nexus 3232C in einem NetApp -Systemschrank	Anweisungen zum Einbau des Switches in einen NetApp -Schrank finden Sie im Leitfaden *Installing a Cisco Nexus 3232C cluster switch and pass-through panel in a NetApp cabinet*.
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?

Nachdem Sie den 3232C Speicherschalter installiert haben, können Sie dann "Installieren Sie den Schalter in einem NetApp cabinet".

Installieren Sie einen Cisco Nexus 3232C Storage-Switch in einem NetApp Schrank

Je nach Konfiguration müssen Sie den Cisco Nexus 3232C Storage-Switch und das Passthrough-Panel möglicherweise in einem NetApp cabinet mit den standardmäßigen Halterungen installieren, die im Lieferumfang des Switches enthalten sind.

Bevor Sie beginnen

Vergewissern Sie sich, dass Sie Folgendes haben: * Die anfänglichen Vorbereitungsanforderungen, den Kit-Inhalt und die Sicherheitshinweise in der "Hardware-Installationshandbuch für die Cisco Nexus 3000-Serie". * Für jeden Switch die acht 10-32- oder 12-24-Schrauben und Clipmuttern zur Montage der Halterungen und Gleitschienen an den vorderen und hinteren Schrankpfosten. * Cisco Standard-Schienenkit zur Installation des Switches in einem NetApp Schrank.

> 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).

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

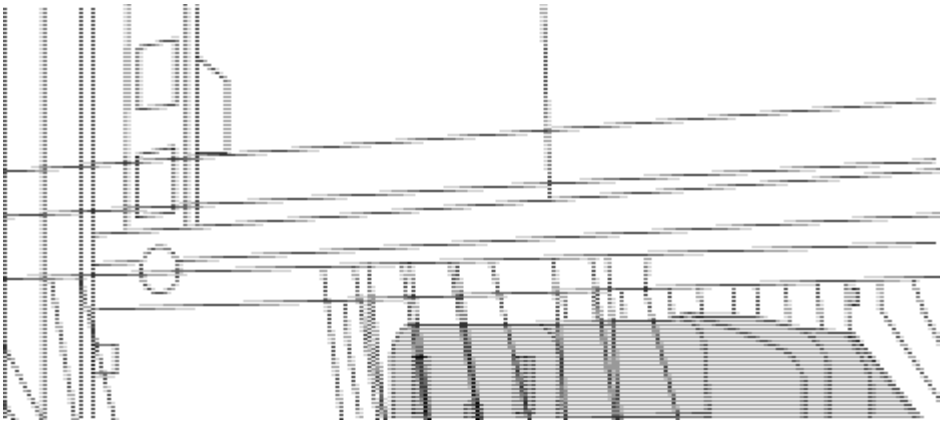
     i. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

     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.

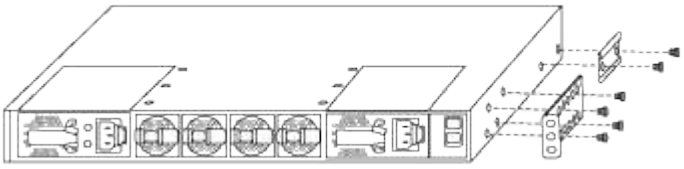
     iii. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.

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

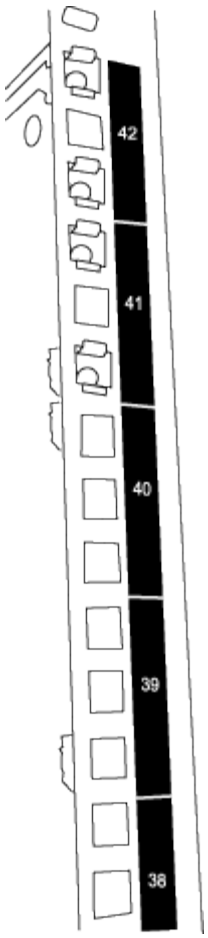


(1) Weiblicher Stecker des Überbrückungskabels.

1. Montieren Sie die Rack-Montagehalterungen am Gehäuse des Nexus 3232C Storage Switch.
   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.



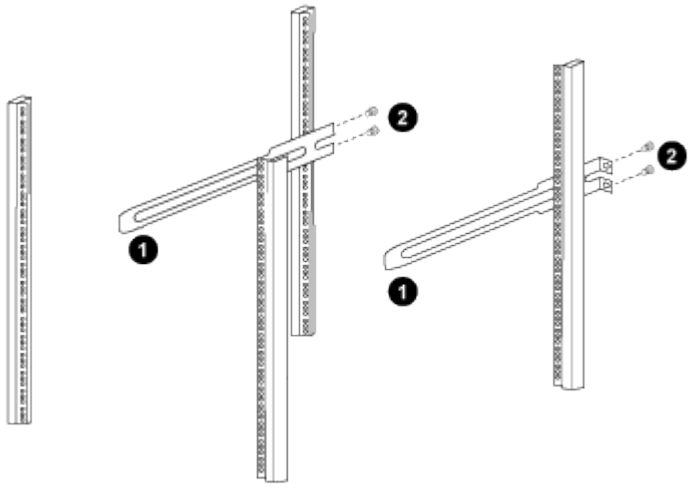
   b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.
   c. Installieren Sie die hintere Rackmontagehalterung am Switch-Gehäuse.
   d. Wiederholen Sie Schritt 2c mit der anderen hinteren Rackmontagehalterung auf der anderen Seite des Switches.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



Die beiden 3232C-Switches werden immer in den oberen 2 HE des Schranks RU41 und 42 montiert.

3. 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) Schieben 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.

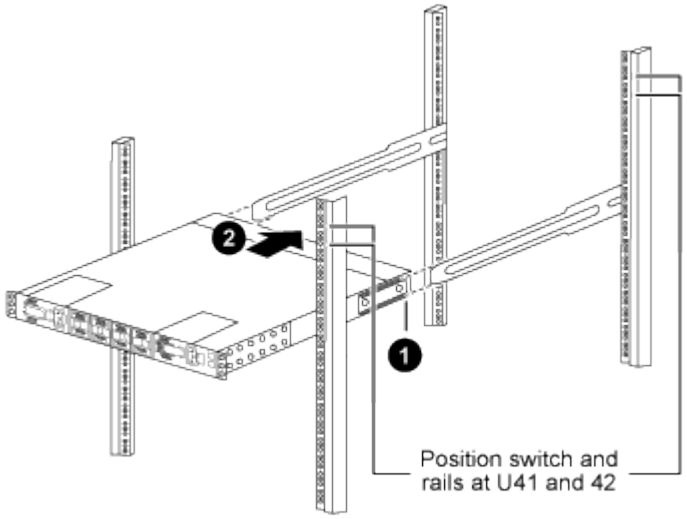
a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.

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

4. 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.

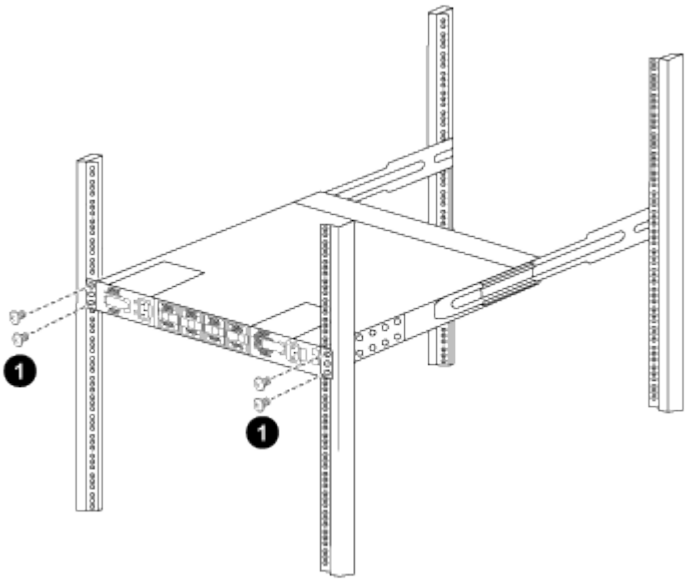
a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(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.

5. Wenn die Schalter installiert sind, schließen Sie die Überbrückungskabel an die Stromeingänge der Schalter an.
6. 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.

7. Verbinden Sie den Management-Port jedes 3232C-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.

Software konfigurieren

Software-Installations-Workflow für Cisco Nexus 3232C Storage Switches

Um die Software für einen Cisco Nexus 3232C-Switch zu installieren und zu konfigurieren und die Referenzkonfigurationsdatei (RCF) zu installieren oder zu aktualisieren, gehen Sie wie folgt vor:

1. **"Konfigurieren Sie den Schalter"**

Konfigurieren Sie den 3232C Speicherswitch.

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

Die Cisco NX-OS Software und die Referenzkonfigurationsdateien (RCFs) müssen auf Cisco 3232C Storage-Switches installiert sein.

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

Laden Sie die NX-OS-Software auf dem Cisco 3232C Storage-Switch herunter und installieren oder aktualisieren Sie sie.

4. **"Installieren Sie den RCF"**

Installieren Sie das RCF, nachdem Sie den Cisco 3232C Storage-Switch zum ersten Mal eingerichtet haben.

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 3232C-Speicherschalter-Einstellungen.

Konfigurieren Sie den 3232C-Speicherschalter

Gehen Sie wie folgt vor, um den Cisco Nexus 3232C Switch einzurichten und zu konfigurieren.

Bevor Sie beginnen

- 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.
- Erforderliche Dokumentation zum Cluster-Netzwerk und zum Management-Netzwerk-Switch.

  Siehe "Erforderliche Dokumentation" für weitere Informationen.

- Erforderliche Controller-Dokumentation und ONTAP Dokumentation.

  "NetApp Dokumentation"

- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen sowie Kabel.
- Ausgefüllte Verkabelungs-Arbeitsblätter.
- Anwendbare NetApp Clusternetzwerk- und Managementnetzwerk-RCFs, heruntergeladen von der NetApp Support-Website unter "mysupport.netapp.com" für die Schalter, die Sie erhalten. Alle Cisco Cluster-Netzwerk- und Management-Netzwerk-Switches werden mit der standardmäßigen Cisco -Werkskonfiguration ausgeliefert. Auf diesen Switches ist auch die aktuelle Version der NX-OS-Software installiert, allerdings sind die RCFs nicht geladen.

Schritte

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

Wenn Sie Ihr… installieren	Dann…
Cisco Nexus 3232C in einem NetApp -Systemschrank	Siehe die Anleitung *Installing a Cisco Nexus 3232C switch and pass-through panel in a NetApp cabinet* für Anweisungen zum Einbau des Switches in einen NetApp Schrank.
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.
4. 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.
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.

Prompt	Antwort
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.
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 im Bereich von 1024 bis 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.

5. 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.
6. Prüfen Sie die Version auf den Cluster-Netzwerk-Switches und laden Sie gegebenenfalls die von NetApp unterstützte Version der Software von der "Cisco -Software-Download" Seite auf die Switches herunter.

Wie geht es weiter?

Nachdem Sie Ihre Switches konfiguriert haben, können Sie "Bereiten Sie die Installation von NX-OS und RCF vor.".

Bereiten Sie die Installation der NX-OS-Software und der Referenzkonfigurationsdatei (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 zwei Knoten. Diese Knoten nutzen zwei 10GbE-Cluster-Verbindungsports. `e0a` Und `e0b` Die

Siehe die"Hardware Universe" um die korrekten Cluster-Ports auf Ihren Plattformen zu überprüfen. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

Die Befehlsausgaben können je nach ONTAP Version variieren.

Nomenklatur von Schaltern und Knoten

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

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

Informationen zu diesem Vorgang

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 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 cdp
```

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
--------
cluster1-02/cdp
            e0a    cs1                       Eth1/2            N3K-
C3232C
            e0b    cs2                       Eth1/2            N3K-
C3232C
cluster1-01/cdp
            e0a    cs1                       Eth1/1            N3K-
C3232C
            e0b    cs2                       Eth1/1            N3K-
C3232C

4 entries were displayed.
```

4. 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
                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

Node: cluster1-01
                                                  Speed(Mbps) Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
--------- ------------ ---------------- ---- ---- ----------- ------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

a. 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
------ -------------------------- ------------------
------------------ -----------
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. [[Schritt 6]]Überprüfen Sie, ob die `auto-revert` Der Befehl ist auf allen Cluster-LIFs aktiviert: `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 des RCF vorbereitet haben, können Sie "Installieren Sie die NX-OS-Software".

Installieren Sie die NX-OS-Software

Mit diesem Verfahren können Sie die NX-OS-Software auf dem Nexus 3232C Storage Switch installieren.

Überprüfungsanforderungen

Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben: * Eine aktuelle Sicherung der Switch-Konfiguration. * Einen voll funktionsfähigen Cluster (keine Fehler in den Protokollen oder ähnliche Probleme). * "Cisco Ethernet-Switch-Seite". Konsultieren Sie die Switch-Kompatibilitätstabelle für die unterstützten ONTAP und NX-OS Versionen. * "Cisco Nexus 3000 Series Switches". Lesen Sie die entsprechenden Software- und Upgrade-Anleitungen auf der Cisco Website, um die vollständige Dokumentation zu den Cisco Switch Upgrade- und Downgrade-Verfahren zu erhalten.

Installieren Sie die Software

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

Führen Sie die Prozedur in "Bereiten Sie die Installation von NX-OS und RCF vor." durch und befolgen Sie dann die folgenden Schritte.

Schritte

1. Verbinden Sie den Cluster-Switch mit dem Management-Netzwerk.
2. Verwenden Sie die `ping` Befehl zum Überprüfen der Verbindung zum Server, 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
   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       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster1-02/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster1-03/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C
cluster1::*>
```

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 -role cluster`

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

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

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

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

Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network
Current      Current Is
Vserver     Interface          Admin/Oper Address/Mask      Node
Port    Home
----------- ------------------ ---------- -----------------
------------ ------- ----
Cluster
            cluster1-01_clus1  up/up     169.254.3.4/23
cluster1-01  e0a     true
            cluster1-01_clus2  up/up     169.254.3.5/23
cluster1-01  e0d     true
            cluster1-02_clus1  up/up     169.254.3.8/23
cluster1-02  e0a     true
            cluster1-02_clus2  up/up     169.254.3.9/23
cluster1-02  e0d     true
            cluster1-03_clus1  up/up     169.254.1.3/23
cluster1-03  e0a     true
            cluster1-03_clus2  up/up     169.254.1.1/23
cluster1-03  e0b     true
            cluster1-04_clus1  up/up     169.254.1.6/23
cluster1-04  e0a     true
            cluster1-04_clus2  up/up     169.254.1.7/23
cluster1-04  e0b     true
8 entries were displayed.
cluster1::*>
```

c. 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    N3K-
C3232C
     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    N3K-
C3232C
     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 3232C-Switch.

Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.


cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.4.img  /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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) 2002-2019, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.37
  NXOS: version 9.3(3)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.3.bin
  NXOS compile time:  12/22/2019 2:00:00 [12/22/2019 14:00:37]

Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGD

  Device name: cs2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 36 second(s)

Last reset at 74117 usecs after Tue Nov 24 06:24:23 2020
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

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

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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


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


Images will be upgraded according to following table:
Module       Image       Running-Version(pri:alt)
New-Version          Upg-Required
------------ ----------- ----------------------------------------
-------------------- ------------
     1       nxos        9.3(3)
9.3(4)               yes
     1       bios        v08.37(01/28/2020):v08.32(10/18/2016)
v08.37(01/28/2020)   no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y
```

```
Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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


Finishing the upgrade, switch will reboot in 10 seconds.
cs2#
```

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 08.37
  NXOS: version 9.3(4)
  BIOS compile time:  01/28/2020
  NXOS image file is: bootflash:///nxos.9.3.4.bin
  NXOS compile time:  4/28/2020 21:00:00 [04/29/2020 06:28:31]

Hardware
 cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOCXXXXXXGS

  Device name: rtpnpi-mcc01-8200-ms-A1
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 14 second(s)

Last reset at 196755 usecs after Tue Nov 24 06:37:36 2020
  Reason: Reset due to upgrade
```

```
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

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                            0x12
IO   FPGA                            0x11

cs2# install epld bootflash:n9000-epld.9.3.4.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  -----------------  ----------    ----------
-----------------
     1         SUP         Yes           Disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type   EPLD              Running-Version   New-Version  Upg-
Required
------  ----  -----------------  ---------------   -----------
------------
     1   SUP   MI FPGA                0x12         0x12         No
     1   SUP   IO FPGA                0x11         0x12         Yes
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.
cs2#
```

11. Wenn Sie auf NX-OS Version 9.3(11) aktualisieren, müssen Sie auch das EPLD aktualisieren. `golden` Image erstellen und den Switch erneut starten. Andernfalls fahren Sie mit Schritt 12 fort.

Sehen "EPLD-Upgrade-Versionshinweise, Version 9.3(11)" für weitere Einzelheiten.

Beispiel anzeigen

```
cs2# install epld bootflash:n9000-epld.9.3.11.img module 1 golden
Digital signature verification is successful
Compatibility check:
Module        Type         Upgradable     Impact      Reason
------  -----------------  ------------  ----------
-----------------
     1        SUP          Yes            Disruptive  Module
Upgradable

Retrieving EPLD versions.... Please wait.
The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ?  [n] y

Proceeding to upgrade Modules.

 Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
cs2#
```

12. Nach dem Neustart des Switches melden Sie sich an, um zu überprüfen, ob die neue Version von EPLD erfolgreich geladen wurde.

Beispiel anzeigen

```
cs2# show version module 1 epld

EPLD Device                      Version
---------------------------------------
MI   FPGA                         0x12
IO   FPGA                         0x12
```

13. 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 -role cluster
    ```

Beispiel anzeigen

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

Node: cluster1-01

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

Node: cluster1-02

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

Node: cluster1-03

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

```
Node: cluster1-04

Ignore
                                                          Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0a       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false
8 entries were displayed.
```

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       N3K-
C3232C
            e0d    cs2                       Ethernet1/7       N3K-
C3232C
cluster01-2/cdp
            e0a    cs1                       Ethernet1/8       N3K-
C3232C
            e0d    cs2                       Ethernet1/8       N3K-
C3232C
cluster01-3/cdp
            e0a    cs1                       Ethernet1/1/1     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/1     N3K-
C3232C
cluster1-04/cdp
            e0a    cs1                       Ethernet1/1/2     N3K-
C3232C
            e0b    cs2                       Ethernet1/1/2     N3K-
C3232C

cluster1::*> system cluster-switch show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ---------------
----------
cs1                         cluster-network    10.233.205.90    N3K-
C3232C
     Serial Number: 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    N3K-
```

```
C3232C
     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.
```

14. 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::*>
```

15. Wiederholen Sie die Schritte 6 bis 14 auf Switch cs1.
16. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

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

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

Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

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 der NX-OS-Software können Sie "Installieren oder aktualisieren Sie die Referenzkonfigurationsdatei (RCF).".

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie installieren die Referenzkonfigurationsdatei (RCF), nachdem Sie die Nexus 3232C-Switches zum ersten Mal eingerichtet haben.

Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

- Eine aktuelle Sicherungskopie der Switch-Konfiguration.
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Der aktuelle RCF.
- Eine Konsolenverbindung zum Switch, dies ist erforderlich, wenn das RCF installiert wird.

Informationen zu diesem Vorgang

Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben.

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 ermöglichen, migriert das folgende Verfahren alle Cluster-LIFs auf den operativen Partner-Switch, während die Schritte auf dem Ziel-Switch ausgeführt werden.

Führen Sie die Prozedur in "Bereiten Sie die Installation von NX-OS und RCF vor." durch und befolgen Sie dann die folgenden Schritte.

Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich per SSH oder über eine serielle Konsole bei Switch CS2 an.
2. Kopieren Sie die RCF mit einem der folgenden Übertragungsprotokolle in den Bootflash des Switches cs2: FTP, TFTP, SFTP oder SCP. Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 3000 Serie NX-OS Befehlsreferenz" .

   Beispiel anzeigen

   Dieses Beispiel zeigt, wie TFTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches CS2 zu kopieren:

   ```
   cs2# copy tftp: bootflash: vrf management
   Enter source filename: Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt
   Enter hostname for the tftp server: 172.22.201.50
   Trying to connect to tftp server......Connection to Server
   Established.
   TFTP get operation was successful
   Copy complete, now saving to disk (please wait)...
   ```

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 3000 Serie NX-OS Befehlsreferenz" .

Beispiel anzeigen

Dieses Beispiel zeigt die RCF-Datei. `Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt` wird auf Switch CS2 installiert:

```
cs2# copy Nexus_3232C_RCF_v1.6-Cluster-HA-Breakout.txt running-
config echo-commands
```

Lesen Sie unbedingt die Abschnitte **Installationshinweise**, **Wichtige Hinweise** und **Banner** Ihrer RCF sorgfältig durch. Sie müssen diese Anweisungen lesen und befolgen, um die korrekte Konfiguration und den ordnungsgemäßen Betrieb des Switches zu überprüfen.

4. Untersuchen Sie die Bannerausgabe von `show banner motd` Befehl. Um die korrekte Konfiguration und den ordnungsgemäßen Betrieb des Schalters sicherzustellen, müssen Sie die Anweisungen unter **Wichtige Hinweise** lesen und befolgen.
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. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an.
7. 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 * Standard-Gateway * Switch-Name

   ```
   cs2# show run | section "switchname" > bootflash:write_erase.cfg

   cs2# show run | section "hostname" >> bootflash:write_erase.cfg

   cs2# show run | i "username admin password" >> bootflash:write_erase.cfg

   cs2# show run | section "vrf context management" >> bootflash:write_erase.cfg

   cs2# show run | section "interface mgmt0" >> bootflash:write_erase.cfg
   ```
8. Bei der Installation von RCF Version 1.12 und höher führen Sie die folgenden Befehle aus:

```
cs2# echo "hardware access-list tcam region racl-lite 512" >>
bootflash:write_erase.cfg

cs2# echo "hardware access-list tcam region qos 256" >>
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.

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

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

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

```
cs2# write erase

Warning: This command will erase the startup-configuration.

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

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

```
cs2# copy bootflash:write_erase.cfg startup-config
```

12. Neustartschalter cs2:

```
cs2# reload

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

13. Wiederholen Sie die Schritte 1 bis 12 auf Switch cs1.
14. 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 | grep up
```

Beispiel anzeigen

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

2. Überprüfen Sie, ob die ISL-Verbindung zwischen cs1 und cs2 funktionsfähig ist:

   `show port-channel summary`

Beispiel anzeigen

```
cs1# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/31(P)   Eth1/32(P)
cs1#
```

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

   `network interface show -role cluster`

Beispiel anzeigen

```
cluster1::*> network interface show -role cluster
            Logical            Status     Network            Current
Current Is
Vserver     Interface          Admin/Oper Address/Mask       Node
Port    Home
----------- ------------------ ---------- ------------------
------------------- ------- ----
Cluster
            cluster1-01_clus1  up/up      169.254.3.4/23
cluster1-01         e0d     true
            cluster1-01_clus2  up/up      169.254.3.5/23
cluster1-01         e0d     true
            cluster1-02_clus1  up/up      169.254.3.8/23
cluster1-02         e0d     true
            cluster1-02_clus2  up/up      169.254.3.9/23
cluster1-02         e0d     true
            cluster1-03_clus1  up/up      169.254.1.3/23
cluster1-03         e0b     true
            cluster1-03_clus2  up/up      169.254.1.1/23
cluster1-03         e0b     true
            cluster1-04_clus1  up/up      169.254.1.6/23
cluster1-04         e0b     true
            cluster1-04_clus2  up/up      169.254.1.7/23
cluster1-04         e0b     true
8 entries were displayed.
cluster1::*>
```

Wenn Cluster-LIFS nicht zu ihren Home-Ports zurückgekehrt sind, setzen Sie sie manuell zurück: `network interface revert -vserver <vserver_name> -lif <lif_name>`

4. 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::*>
```

Schritt 3: Richten Sie Ihren ONTAP Cluster ein.

NetApp empfiehlt, neue Cluster mit dem System Manager einzurichten.

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

Siehe "Konfigurieren Sie ONTAP auf einem neuen Cluster mit System Manager" für Einrichtungsanweisungen.

Wie geht es weiter?

Nach der Installation des 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, können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Setzen Sie den 3232C-Speicherschalter auf die Werkseinstellungen zurück

Um den 3232C Speicherschalter auf die Werkseinstellungen zurückzusetzen, müssen Sie die 3232C Speicherschalter-Einstellungen 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

Nach dem Zurücksetzen des Schalters können Sie "neu konfigurieren" ihn entsprechend Ihren Anforderungen konfigurieren.

Ersetzen Sie einen Cisco Nexus 3232C Speicherswitch

Befolgen Sie diese Schritte, um einen defekten Cisco Nexus 3232C Storage-Switch auszutauschen. Dies ist ein unterbrechungsfreies Verfahren.

Überprüfungsanforderungen

Die bestehende Netzwerkkonfiguration muss folgende Eigenschaften aufweisen:

- 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.

Stellen Sie sicher, dass alle Schritte zur Fehlerbehebung abgeschlossen sind, um zu bestätigen, dass Ihr Schalter ausgetauscht werden muss.

Der Ersatz-Switch Cisco Nexus 3232C muss folgende Eigenschaften aufweisen:

- Die Managementnetzwerkanbindung muss funktionsfähig sein.
- Der Zugang zum Ersatzschalter über die Konsole muss gewährleistet sein.
- Das entsprechende RCF- und NX-OS-Betriebssystemabbild muss auf den Switch geladen werden.
- Die Erstkonfiguration des Schalters muss abgeschlossen sein.

Tauschen Sie den Schalter aus.

Bei diesem Verfahren wird der zweite Nexus 3232C Speicherschalter S2 durch den neuen 3232C Schalter NS2 ersetzt. Die beiden Knoten sind Knoten1 und Knoten2.

Schritt 1: Prüfen Sie, ob es sich bei dem auszutauschenden Schalter um S2 handelt.

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.

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

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
```

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
NX3232C
            e4a    node2                     e4a               AFF-
A700
            e4e    node2                     e4e               AFF-
A700
node1/lldp
            e3a    S1                        Ethernet1/1       -
            e4a    node2                     e4a               -
            e4e    node2                     e4e               -
node2/cdp
            e3a    S1                        Ethernet1/2
NX3232C
            e4a    node1                     e4a               AFF-
A700
            e4e    node1                     e4e               AFF-
A700
node2/lldp
            e3a    S1                        Ethernet1/2       -
            e4a    node1                     e4a               -
            e4e    node1                     e4e               -
```

4. Führe 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
```

Schritt 2: Verkabelung konfigurieren

1. Überprüfen Sie die Regalanschlüsse im Speichersystem:

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

   Beispiel anzeigen

```
storage::*> storage shelf port show -fields remote-device,remote-
port

shelf  id  remote-port  remote-device
-----  --  -----------  -------------
3.20   0   Ethernet1/5  S1
3.20   1   -            -
3.20   2   Ethernet1/6  S1
3.20   3   -            -
3.30   0   Ethernet1/7  S1
3.20   1   -            -
3.30   2   Ethernet1/8  S1
3.20   3   -            -
```

2. Entfernen Sie alle Kabel, die am Speicherschalter S2 angeschlossen sind.
3. Schließen Sie alle Kabel wieder an den Ersatzschalter NS2 an.

Schritt 3: Überprüfen Sie alle Gerätekonfigurationen auf dem Switch NS2.

1. Überprüfen Sie 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    100 enabled  online
30
node2
                    e3a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
```

2. Vergewissern Sie sich, dass beide 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
NX3232C
            e4a    node2                     e4a               AFF-
A700
            e4e    node2                     e4e               AFF-
A700
            e7b    NS2                       Ethernet1/1
NX3232C
node1/lldp
            e3a    S1                        Ethernet1/1       -
            e4a    node2                     e4a               -
            e4e    node2                     e4e               -
            e7b    NS2                       Ethernet1/1       -
node2/cdp
            e3a    S1                        Ethernet1/2
NX3232C
            e4a    node1                     e4a               AFF-
A700
            e4e    node1                     e4e               AFF-
A700
            e7b    NS2                       Ethernet1/2
NX3232C
node2/lldp
            e3a    S1                        Ethernet1/2       -
            e4a    node1                     e4a               -
            e4e    node1                     e4e               -
            e7b    NS2                       Ethernet1/2       -
```

3. Überprüfen Sie die 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
```

4. 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 Ihren Schalter ausgetauscht haben, können Sie "Konfigurieren der Switch-Integritätsüberwachung".

Upgrade eines Cisco Nexus 3232C Speicherswitch

Führen Sie diese Schritte aus, um die Cisco NX-OS-Software und die Referenzkonfigurationsdateien (RCF) auf Cisco Nexus 3232C-Switches zu aktualisieren.

Überprüfungsanforderungen

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Bedingungen erfüllt sind, bevor Sie die NX-OS-Software und die RCFs auf dem Speichersystem aktualisieren:

- Der Schalter funktioniert einwandfrei (es sollten keine Fehler in den Protokollen oder ähnliche Probleme auftreten).
- Sie haben die gewünschten Boot-Variablen in der RCF-Datei überprüft oder so eingestellt, dass sie die gewünschten Boot-Images widerspiegeln, wenn Sie nur NX-OS installieren und Ihre aktuelle RCF-Version beibehalten.

  Wenn Sie die Bootvariablen 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.

- Sie haben die entsprechenden Software- und Upgrade-Anleitungen auf der "Cisco Nexus 3000 Series Switches" Seite für die vollständige Dokumentation zu den Cisco Speicher-Upgrade- und Downgrade-Verfahren konsultiert.

- Die Anzahl der 10-GbE- und 40/100-GbE-Ports ist in den Referenzkonfigurationsdateien (RCFs) definiert, die auf der "Cisco Ethernet-Switches" Seite verfügbar sind.

Tauschen Sie den Schalter aus.

Zu den Beispielen

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

- Die Namen der beiden Speicherschalter lauten S1 und S2.
- Die Knoten sind Knoten1 und Knoten2.

Die Beispiele in diesem Verfahren verwenden zwei Knoten; Knoten 1 mit zwei Speicheranschlüssen und Knoten 2 mit zwei Speicheranschlüssen. Siehe die"Hardware Universe" um die korrekten Speicherports auf Ihren Plattformen zu überprüfen. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Für weitere Informationen zu den Installationsanforderungen des Schalters.

> Für dieses Verfahren werden sowohl ONTAP -Befehle als auch Cisco Nexus 3000 Series Switches-Befehle benötigt; es werden ONTAP -Befehle verwendet, sofern nicht anders angegeben. Die Befehlsausgaben können je nach ONTAP Version variieren.

Schritt 1: Überprüfen Sie den Gesundheitszustand der Switches und Ports.

1. Wenn AutoSupport 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.

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

2. Prüfen Sie, ob die Speicherschalter verfügbar sind:

   `system switch ethernet show`

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                       Type               Address
Model
---------------------------- ------------------ ----------------
---------------
S1
                             storage-network    172.17.227.5
NX3232C
     Serial Number: FOC221206C2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(3)
    Version Source: CDP

S2
                             storage-network    172.17.227.6
NX3232C
     Serial Number: FOC220443LZ
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(3)
    Version Source: CDP

2 entries were displayed.
storage::*>
```

3. Überprüfen Sie, ob die Knotenports intakt und betriebsbereit sind:

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

Beispiel anzeigen

```
storage::*> storage port show -port-type ENET
                                      Speed
VLAN
Node                Port Type  Mode    (Gb/s) State    Status
ID
------------------ ---- ----- ------- ------ -------- -----------
----
node1
                    e3a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
node2
                    e3a  ENET  storage    100 enabled  online
30
                    e3b  ENET  storage      0 enabled  offline
30
                    e7a  ENET  storage      0 enabled  offline
30
                    e7b  ENET  storage    100 enabled  online
30
```

4. Prüfen Sie, ob es keine Probleme mit dem Speicherschalter oder der Verkabelung gibt:

   `system health alert show -instance`

   Beispiel anzeigen

```
storage::*> system health alert show -instance
There are no entries matching your query.
```

Schritt 2: Kopieren Sie die RCF-Datei auf den Cisco -Switch S2

1. Kopieren Sie die RCF-Datei auf Switch S2 mithilfe eines der folgenden Übertragungsprotokolle in den Bootflash-Speicher des Switches: FTP, HTTP, TFTP, SFTP oder SCP.

   Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Leitfaden in der "Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen".

Beispiel anzeigen

Das folgende Beispiel zeigt, wie HTTP verwendet wird, um eine RCF-Datei in den Bootflash des Switches S2 zu kopieren:

```
S2# copy http://172.16.10.1//cfg/Nexus_3232C_RCF_v1.6-Storage.txt
bootflash: vrf management
% Total    % Received % Xferd  Average  Speed   Time    Time
Time                           Current
                                Dload    Upload  Total   Spent
Left                           Speed
  100        3254       100    3254     0       0       8175     0
--:--:-- --:--:-- --:--:-   8301
Copy complete, now saving to disk (please wait)...
Copy complete.
S2#
```

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

   `copy bootflash:`

   Beispiel anzeigen

   Das folgende Beispiel zeigt die RCF-Datei. `Nexus_3232C_RCF_v1.6-Storage.txt` wird auf Switch S2 installiert:

   ```
   S2# copy Nexus_3232C_RCF_v1.6-Storage.txt running-config echo-
   commands
   ```

3. 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.

Im Banner-Output von `show banner motd` Um den korrekten Betrieb des Schalters sicherzustellen, müssen Sie die Anweisungen im Abschnitt **WICHTIGE HINWEISE** lesen und befolgen.

+
.Beispiel anzeigen

```
S2# show banner motd

*********************************************************************
**********
* NetApp Reference Configuration File (RCF)
*
* Switch   : Cisco Nexus 3232C
* Filename : Nexus_3232C_RCF_v1.6-Storage.txt
* Date     : Oct-20-2020
* Version  : v1.6
*
* Port Usage : Storage configuration
* Ports  1-32: Controller and Shelf Storage Ports
* Ports 33-34: Disabled
*
* IMPORTANT NOTES*
* - This RCF utilizes QoS and requires TCAM re-configuration,
requiring RCF
*   to be loaded twice with the Storage Switch rebooted in between.
*
* - Perform the following 4 steps to ensure proper RCF installation:
*
*   (1) Apply RCF first time, expect following messages:
*       - Please save config and reload the system...
*       - Edge port type (portfast) should only be enabled on
ports...
*       - TCAM region is not configured for feature QoS class IPv4
ingress...
*
*   (2) Save running-configuration and reboot Cluster Switch
*
*   (3) After reboot, apply same RCF second time and expect
following messages:
*       - % Invalid command at '^' marker
*       - Syntax error while parsing...
*
*   (4) Save running-configuration again
*********************************************************************
**********
S2#
```

+

Bei der erstmaligen Anwendung des RCF ist die Fehlermeldung **ERROR: Failed to write VSH commands** zu erwarten und kann ignoriert werden.

4. Nachdem Sie überprüft haben, ob die Softwareversionen und die Schaltereinstellungen korrekt sind, kopieren Sie die `running-config` Datei an die `startup-config` Datei auf Switch S2.

   Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Leitfaden in der "Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen".

   Beispiel anzeigen

   Das folgende Beispiel zeigt die `running-config` Datei erfolgreich kopiert nach `startup-config` Datei:

   ```
   S2# copy running-config startup-config
   [########################################] 100% Copy complete.
   ```

Schritt 3: Kopieren Sie das NX-OS-Image auf den Cisco -Switch S2 und starten Sie ihn neu.

1. Kopieren Sie das NX-OS-Image auf Switch S2.

Beispiel anzeigen

```
S2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.3.4.bin
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/nxos.9.3.4.bin  /bootflash/nxos.9.3.4.bin
/code/nxos.9.3.4.bin  100% 1261MB   9.3MB/s   02:15
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/n9000-epld.9.3.4.img
Enter hostname for the sftp server: 172.19.2.1
Enter username: user1

Outbound-ReKey for 172.19.2.1:22
Inbound-ReKey for 172.19.2.1:22
user1@172.19.2.1's password:
sftp> progress
Progress meter enabled
sftp> get   /code/n9000-epld.9.3.4.img  /bootflash/n9000-
epld.9.3.4.img
/code/n9000-epld.9.3.4.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

2. Installieren Sie das Systemabbild, damit die neue Version beim nächsten Neustart des Switches S2 geladen wird.

   Der Switch wird in 10 Sekunden mit dem neuen Image neu gestartet, wie in der folgenden Ausgabe dargestellt:

Beispiel anzeigen

```
S2# install all nxos bootflash:nxos.9.3.4.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.4.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.4.bin.
[] 100% -- SUCCESS

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

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


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


Images will be upgraded according to following table:
Module       Image                 Running-Version(pri:alt)
New-Version  Upg-Required
------  ----------  ----------------------------------------
--------------------  ------------
     1        nxos                                      9.3(3)
9.3(4)           yes
     1        bios     v08.37(01/28/2020):v08.23(09/23/2015)
v08.38(05/29/2020)            no


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y
input string too long
```

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

Install is in progress, please wait.

Performing runtime checks.
[] 100% -- SUCCESS

Setting boot variables.
[] 100% -- SUCCESS

Performing configuration copy.
[] 100% -- SUCCESS

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


Finishing the upgrade, switch will reboot in 10 seconds.
S2#
```

3. Konfiguration speichern.

   Weitere Informationen zu Cisco-Befehlen finden Sie im entsprechenden Leitfaden in der "Cisco Nexus 3000 Serie NX-OS Befehlsreferenzen".

   Sie werden aufgefordert, das System neu zu starten.

   Beispiel anzeigen

```
S2# copy running-config startup-config
[] 100% Copy complete.
S2# reload
This command will reboot the system. (y/n)?  [n] y
```

4. Vergewissern Sie sich, dass die neue NX-OS-Versionsnummer auf dem Switch eingestellt ist:

Beispiel anzeigen

```
S2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2020, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their
own
licenses, such as open source.  This software is provided "as is,"
and unless
otherwise stated, there is no warranty, express or implied,
including but not
limited to warranties of merchantability and fitness for a
particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

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


Hardware
  cisco Nexus3000 C3232C Chassis (Nexus 9000 Series)
  Intel(R) Xeon(R) CPU E5-2403 v2 @ 1.80GHz with 8154432 kB of
memory.
  Processor Board ID FOC20291J6K

  Device name: S2
  bootflash:   53298520 kB
Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 42 second(s)

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

```
  Reason: Reset due to upgrade
  System version: 9.3(3)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

S2#
```

Schritt 4: Überprüfen Sie erneut den Gesundheitszustand der Switches und Ports.

1. Überprüfen Sie nach dem Neustart, ob die Speicherschalter verfügbar sind:

   ```
   system switch ethernet show
   ```

Beispiel anzeigen

```
storage::*> system switch ethernet show
Switch                       Type               Address
Model
---------------------------- ------------------ ----------------
---------------
S1
                             storage-network    172.17.227.5
NX3232C
     Serial Number: FOC221206C2
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP

S2
                             storage-network    172.17.227.6
NX3232C
     Serial Number: FOC220443LZ
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS) Software,
Version
                    9.3(4)
    Version Source: CDP

2 entries were displayed.
storage::*>
```

2. Überprüfen Sie nach dem Neustart, ob die Switch-Ports einwandfrei funktionieren:

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

3. Überprüfen Sie erneut, ob es Probleme mit dem Speicherschalter oder der Verkabelung des Clusters gibt:

   `system health alert show -instance`

   Beispiel anzeigen

   ```
   storage::*> system health alert show -instance
   There are no entries matching your query.
   ```

4. Wiederholen Sie den Vorgang, um die NX-OS-Software und RCF auf Switch S1 zu aktualisieren.
5. 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?

Nach dem Upgrade Ihres Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung".

NVIDIA SN2100

Erste Schritte

Installations- und Einrichtungsworkflow für NVIDIA SN2100-Switches

Der NVIDIA SN2100 ist ein Ethernet-Switch, mit dem Daten zwischen Controllern und Festplattengehäusen umgeschaltet werden können.

Befolgen Sie diese Arbeitsschritte, um Ihre SN2100-Switches zu installieren und einzurichten.

1. **"Überprüfen der Konfigurationsanforderungen"**

   Überprüfen Sie die Konfigurationsanforderungen für den SN2100-Speicherswitch.

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

   Überprüfen Sie die Komponenten und Teilenummern für den SN2100-Speicherschalter.

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

   Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre SN2100-Switches und den ONTAP Cluster einzurichten.

4. **"Installieren Sie die Hardware"**

   Installieren Sie die Switch-Hardware.

5. **"Konfigurieren der Software"**

   Konfigurieren Sie die Switch-Software.

Konfigurationsanforderungen für NVIDIA SN2100-Switches

Für die Installation und Wartung des NVIDIA SN2100 Switches sollten Sie unbedingt alle Anforderungen beachten.

Installationsvoraussetzungen

Wenn Sie ONTAP -Cluster mit mehr als zwei Knoten aufbauen möchten, benötigen Sie zwei unterstützte Cluster-Netzwerk-Switches. Sie können zusätzliche Management-Schalter verwenden, die optional sind.

Sie installieren den NVIDIA SN2100 Switch (X190006/X190106) im NVIDIA Dual-/Single-Switch-Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Richtlinien zur Verkabelung finden Sie unter"Überlegungen zu Verkabelung und Konfiguration" Die

ONTAP und Linux-Unterstützung

Der NVIDIA SN2100 Switch ist ein 10/25/40/100-Gb-Ethernet-Switch, auf dem Cumulus Linux läuft. Der Schalter unterstützt Folgendes:

- ONTAP 9.10.1P3. Der SN2100-Switch dient Cluster- und Speicheranwendungen in ONTAP 9.10.1P3 über verschiedene Switch-Paare. Ab ONTAP 9.10.1P3 können Sie NVIDIA SN2100 Switches verwenden, um Speicher- und Clusterfunktionen in einer gemeinsamen Switch-Konfiguration zu kombinieren.
- Cumulus Linux (CL) Betriebssystemversion 4.4.3. Aktuelle Informationen zur Kompatibilität finden Sie unter "NVIDIA Ethernet-Switches" Informationsseite.
- Sie können Cumulus Linux installieren, wenn auf dem Switch Cumulus Linux oder ONIE läuft.

Was kommt als nächstes

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

Komponenten und Teilenummern für NVIDIA SN2100-Schalter

Für die Installation und Wartung des NVIDIA SN2100 Switches sollten Sie unbedingt die Liste der Komponenten und die Teilenummern für das Gehäuse und das Schienenset überprüfen.

Schrankdetails

Sie installieren den NVIDIA SN2100 Switch (X190006/X190106) im NVIDIA Dual-/Single-Switch-Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Details zum Schienenbausatz

Die folgende Tabelle listet die Teilenummer und die Beschreibung für die MSN2100-Weichen und Schienensätze auf:

Teilenummer	Beschreibung
X190006-PE	Cluster-Switch, NVIDIA SN2100, 16PT 100G, PTSX
X190006-PI	Cluster-Switch, NVIDIA SN2100, 16PT 100G, PSIN
X190106-FE-PE	Switch, NVIDIA SN2100, 16PT 100G, PTSX, Front End
X190106-FE-PI	Switch, NVIDIA SN2100, 16PT 100G, PSIN, Front End
X-MTEF-KIT-D	Schienen-Kit, NVIDIA Dual-Schalter nebeneinander
X-MTEF-KIT-E	Schienensatz, NVIDIA Einzelschalter kurze Tiefe

Weitere Informationen finden Sie in der NVIDIA Dokumentation. "Installation Ihres SN2100-Weichen- und Schienensatzes" Die

Was kommt als nächstes

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

Dokumentationsanforderungen für NVIDIA SN2100-Switches

Für die Installation und Wartung des NVIDIA SN2100 Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation lesen.

Die folgende Tabelle listet die für die NVIDIA SN2100 Switches verfügbare Dokumentation auf.

Titel	Beschreibung
"*Einrichten und Konfigurieren Ihrer NVIDIA SN2100-Switches*"	Beschreibt, wie Sie Ihre NVIDIA SN2100 Switches einrichten und konfigurieren, einschließlich der Installation von Cumulus Linux und den entsprechenden RCFs.
"*Migration von einem Cisco -Speicherswitch zu einem NVIDIA SN2100-Speicherswitch*"	Beschreibt, wie Sie von Umgebungen, die Cisco -Speicher-Switches verwenden, zu Umgebungen migrieren, die NVIDIA SN2100-Speicher-Switches verwenden.
"*Migration zu einem Zwei-Knoten-Switch-Cluster mit NVIDIA SN2100 Cluster-Switches*"	Beschreibt, wie man mit NVIDIA SN2100 Cluster-Switches auf eine Zwei-Knoten-Switch-Umgebung migriert.
"NVIDIA SN2100 Speicherswitch austauschen_"	Beschreibt das Vorgehen zum Austausch eines defekten NVIDIA SN2100 Speicherswitches und zum Herunterladen von Cumulus Linux und der zugehörigen Konfigurationsdatei.

Installieren der Hardware

Workflow zur Hardwareinstallation für NVIDIA SN2100-Speicherswitches

Um die Hardware für einen SN2100-Speicher-Switch zu installieren und zu konfigurieren, gehen Sie wie folgt vor:

1. **"Installieren Sie die Hardware"**
   Installieren Sie die Switch-Hardware.

2. **"Überprüfung der Verkabelung und Konfigurationsüberlegungen"**
   Überprüfen Sie die Anforderungen an optische Verbindungen, den QSA-Adapter und die Switchport-Geschwindigkeit.

3. **"Verkabeln Sie die NS224-Regale"**
   Befolgen Sie die Verkabelungsprozeduren, wenn Sie ein System haben, in dem die NS224-Laufwerksschächte

als Switch-Attached Storage (nicht als Direct-Attached Storage) verkabelt werden müssen.

Installieren Sie die Hardware für den NVIDIA SN2100-Switch.

Zur Installation der SN2100-Hardware konsultieren Sie bitte die Dokumentation von NVIDIA.

Schritte

1. Überprüfen Sie die"Konfigurationsanforderungen" Die
2. Befolgen Sie die Anweisungen in "NVIDIA Switch Installationsanleitung" Die

Wie geht es weiter?

Nachdem Sie Ihre Hardware installiert haben, können Sie"Verkabelung und Konfiguration überprüfen" Anforderungen.

Überprüfung der Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren NVIDIA SN2100 Switch konfigurieren, beachten Sie bitte die folgenden Hinweise.

NVIDIA -Portdetails

Switch-Ports	Portnutzung
swp1s0-3	4x10GbE Breakout-Cluster-Portknoten
swp2s0-3	4x25GbE Breakout-Cluster-Portknoten
swp3-14	40/100GbE-Cluster-Portknoten
swp15-16	100GbE Inter-Switch Link (ISL)-Ports

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

Verbindungsverzögerungen bei optischen Verbindungen

Falls Sie Verbindungsverzögerungen von mehr als fünf Sekunden feststellen, bietet Cumulus Linux 5.4 und spätere Versionen Unterstützung für schnelles Verbindungsaufbauen. Sie können die Links mithilfe der folgenden Funktion konfigurieren: `nv set` Befehl wie folgt:

```
nv set interface <interface-id> link fast-linkup on
nv config apply
reload the switchd
```

Beispiel anzeigen

```
cumulus@cumulus-cs13:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus-cs13:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

Unterstützung für Kupferverbindungen

Um dieses Problem zu beheben, sind folgende Konfigurationsänderungen erforderlich.

Cumulus Linux 4.4.3

1. Ermitteln Sie die Bezeichnung für jede Schnittstelle, die 40GbE/100GbE-Kupferkabel verwendet:

```
cumulus@cumulus:mgmt:~$ net show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Fügen Sie die folgenden zwei Zeilen hinzu: `/etc/cumulus/switchd.conf` Datei für jeden Port (swp<n>), der 40GbE/100GbE-Kupferkabel verwendet:

   - `interface.swp<n>.enable_media_depended_linkup_flow=TRUE`
   - `interface.swp<n>.enable_short_tuning=TRUE`

   Beispiel:

```
cumulus@cumulus:mgmt:~$ sudo nano /etc/cumulus/switchd.conf
.
.
interface.swp3.enable_media_depended_linkup_flow=TRUE
interface.swp3.enable_short_tuning=TRUE
interface.swp4.enable_media_depended_linkup_flow=TRUE
interface.swp4.enable_short_tuning=TRUE
```

3. Starten Sie das Gerät neu. `switchd` Service:

```
cumulus@cumulus:mgmt:~$ sudo systemctl restart switchd.service
```

4. Vergewissern Sie sich, dass die Ports aktiv sind:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
UP     swp3      100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                      Master:
bridge(UP)
```

Cumulus Linux 5.x

1. Ermitteln Sie die Bezeichnung für jede Schnittstelle, die 40GbE/100GbE-Kupferkabel verwendet:

```
cumulus@cumulus:mgmt:~$ nv show interface pluggables

Interface  Identifier     Vendor Name     Vendor PN    Vendor SN
Vendor Rev
---------  -------------  --------------  -----------  -------------
----------
swp3       0x11 (QSFP28)  Molex           112-00576    93A2229911111
B0
swp4       0x11 (QSFP28)  Molex           112-00576    93A2229922222
B0
```

2. Konfigurieren Sie die Links mithilfe der `nv set` Befehl wie folgt:
   - `nv set interface <interface-id> link fast-linkup on`
   - `nv config apply`
   - Laden Sie die `switchd` Service

     Beispiel:

```
cumulus@cumulus:mgmt:~$ nv set interface swp5 link fast-linkup on
cumulus@cumulus:mgmt:~$ nv config apply
switchd need to reload on this config change

Are you sure? [y/N] y
applied [rev_id: 22]

Only switchd reload required
```

3. Vergewissern Sie sich, dass die Ports aktiv sind:

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name       Spd   MTU    Mode        LLDP                 Summary
-----  ---------- ----  -----  ----------- -------------------- --------
UP     swp3       100G  9216   Trunk/L2                         Master:
bridge(UP)
UP     swp4       100G  9216   Trunk/L2                         Master:
bridge(UP)
```

Siehe den Artikel in der Wissensdatenbank. "Der SN2100-Switch kann keine Verbindung über 40/100GbE-Kupferkabel herstellen." für weitere Einzelheiten.

Unter Cumulus Linux 4.4.2 werden Kupferverbindungen auf SN2100-Switches mit X1151A NIC, X1146A NIC oder integrierten 100GbE-Ports nicht unterstützt. Beispiel:

- AFF A800 an den Ports e0a und e0b
- AFF A320 an den Ports e0g und e0h

QSA-Adapter

Wenn ein QSA-Adapter verwendet wird, um eine Verbindung zu den 10GbE/25GbE-Cluster-Ports einer Plattform herzustellen, kann es vorkommen, dass die Verbindung nicht zustande kommt.

Um dieses Problem zu beheben, gehen Sie wie folgt vor:

- Für 10GbE stellen Sie die Verbindungsgeschwindigkeit von swp1s0-3 manuell auf 10000 ein und deaktivieren Sie die automatische Aushandlung.
- Für 25GbE stellen Sie die Verbindungsgeschwindigkeit swp2s0-3 manuell auf 25000 ein und deaktivieren Sie die automatische Aushandlung.

> Bei Verwendung von 10GbE/25GbE QSA-Adaptern stecken Sie diese in nicht-breakout 40GbE/100GbE-Ports (swp3-swp14). Stecken Sie den QSA-Adapter nicht in einen Port, der für Breakout konfiguriert ist.

Schnittstellengeschwindigkeit an Breakout-Ports einstellen

Je nach Transceiver im Switch-Port müssen Sie möglicherweise die Geschwindigkeit an der Switch-Schnittstelle auf eine feste Geschwindigkeit einstellen. Bei Verwendung von 10GbE- und 25GbE-Breakout-Ports überprüfen Sie, ob die automatische Aushandlung deaktiviert ist, und stellen Sie die Schnittstellengeschwindigkeit am Switch ein.

Cumulus Linux 4.4.3

Beispiel:

```
cumulus@cumulus:mgmt:~$ net add int swp1s3 link autoneg off && net com
--- /etc/network/interfaces     2019-11-17 00:17:13.470687027 +0000
+++ /run/nclu/ifupdown2/interfaces.tmp  2019-11-24 00:09:19.435226258
+0000
@@ -37,21 +37,21 @@
     alias 10G Intra-Cluster Node
     link-autoneg off
     link-speed 10000  <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp1s3
iface swp1s3
     alias 10G Intra-Cluster Node
-    link-autoneg off
+    link-autoneg on
     link-speed 10000 <---- port speed set
     mstpctl-bpduguard yes
     mstpctl-portadminedge yes
     mtu 9216

auto swp2s0
iface swp2s0
     alias 25G Intra-Cluster Node
     link-autoneg off
     link-speed 25000 <---- port speed set
```

Überprüfen Sie den Schnittstellen- und Portstatus, um sicherzustellen, dass die Einstellungen angewendet wurden:

```
cumulus@cumulus:mgmt:~$ net show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Cumulus Linux 5.x

Beispiel:

```
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link auto-negotiate off
cumulus@cumulus:mgmt:~$ nv set interface swp1s3 link speed 10G
cumulus@cumulus:mgmt:~$ nv show interface swp1s3

link

  auto-negotiate        off                   off
off
  duplex                full                  full
full
  speed                 10G                   10G
10G
  fec                   auto                  auto
auto
  mtu                   9216                  9216
9216
[breakout]

  state                 up                    up
up
```

Überprüfen Sie den Schnittstellen- und Portstatus, um sicherzustellen, dass die Einstellungen angewendet wurden:

```
cumulus@cumulus:mgmt:~$ nv show interface

State  Name       Spd    MTU    Mode         LLDP              Summary
-----  --------   -----  -----  ----------   ---------------
-------------------------------------
.
.
UP     swp1s0     10G    9216   Trunk/L2     cs07 (e4c)        Master:
br_default(UP)
UP     swp1s1     10G    9216   Trunk/L2     cs07 (e4d)        Master:
br_default(UP)
UP     swp1s2     10G    9216   Trunk/L2     cs08 (e4c)        Master:
br_default(UP)
UP     swp1s3     10G    9216   Trunk/L2     cs08 (e4d)        Master:
br_default(UP)
.
.
UP     swp3       40G    9216   Trunk/L2     cs03 (e4e)        Master:
br_default(UP)
UP     swp4       40G    9216   Trunk/L2     cs04 (e4e)        Master:
br_default(UP)
DN     swp5       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp6       N/A    9216   Trunk/L2                       Master:
br_default(UP)
DN     swp7       N/A    9216   Trunk/L2                       Master:
br_default(UP)
.
.
UP     swp15      100G   9216   BondMember   cs01 (swp15)      Master:
cluster_isl(UP)
UP     swp16      100G   9216   BondMember   cs01 (swp16)      Master:
cluster_isl(UP)
.
.
```

Wie geht es weiter?

Nachdem Sie Ihre Verkabelungs- und Konfigurationsanforderungen überprüft haben, können Sie"Verkabeln Sie die NS224-Regale als schaltergebundene Aufbewahrung." Die

Kabelablagen NS224 als am Schalter befestigte Aufbewahrung

Falls Sie ein System haben, in dem die NS224-Laufwerksschächte als Switch-Attached Storage (nicht als Direct-Attached Storage) verkabelt werden müssen, verwenden Sie die hier bereitgestellten Informationen.

- Kabel NS224 treibt Regale über Speicherschalter an:

  "Informationen zur Verkabelung von NS224-Laufwerksschächten mit Switch-Anschluss."

- Installieren Sie Ihre Speicherschalter:

  "AFF und FAS Schalterdokumentation"

- Prüfen Sie, ob Ihre Plattformmodelle mit unterstützter Hardware wie Speicherschaltern und Kabeln kompatibel sind:

  "NetApp Hardware Universe"

Software konfigurieren

Workflow für die Softwareinstallation der NVIDIA SN2100 Speicherschalter

Um die Software für einen NVIDIA SN2100 Switch zu installieren und zu konfigurieren, befolgen Sie diese Schritte:

1. **"Konfigurieren Sie den Schalter"**

   Konfigurieren Sie den NVIDIA SN2100-Switch.

2. **"Installieren Sie Cumulus Linux im Cumulus-Modus"**

   Sie können das Betriebssystem Cumulus Linux (CL) installieren, wenn auf dem Switch Cumulus Linux ausgeführt wird.

3. **"Installieren Sie Cumulus Linux im ONIE-Modus"**

   Alternativ können Sie das Betriebssystem Cumulus Linux (CL) installieren, wenn auf dem Switch Cumulus Linux im ONIE-Modus ausgeführt wird.

4. **"Installieren Sie das Skript für die Referenzkonfigurationsdatei (RCF)."**

   Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Die Vorgehensweise ist für alle Fälle gleich.

5. **"Installieren Sie die CSHM-Datei"**

   Sie können die entsprechende Konfigurationsdatei für die Zustandsüberwachung von Ethernet-Switches in NVIDIA -Cluster-Switches installieren.

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

   Löschen Sie die Einstellungen des SN2100-Speicherschalters.

Konfigurieren Sie den NVIDIA SN2100-Switch

Informationen zur Konfiguration des SN2100-Switches finden Sie in der Dokumentation von NVIDIA.

Schritte

1. Überprüfen Sie die"Konfigurationsanforderungen" Die
2. Befolgen Sie die Anweisungen in "NVIDIA -Systemstart." Die

Wie geht es weiter?

Nachdem Sie Ihre Schalter konfiguriert haben, können Sie"Cumulus Linux im Cumulus-Modus installieren" oder"Cumulus Linux im ONIE-Modus installieren" Die

Installieren Sie Cumulus Linux im Cumulus-Modus

Führen Sie diese Schritte aus, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im Cumulus-Modus läuft.

Cumulus Linux (CL) OS kann entweder installiert werden, wenn auf dem Switch Cumulus Linux oder ONIE läuft (siehe"Installation im ONIE-Modus").

Bevor Sie beginnen

Stellen Sie sicher, dass Folgendes verfügbar ist:

- Linux-Kenntnisse auf mittlerem Niveau.
- Kenntnisse in grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren ist vorinstalliert, darunter `vi` Und `nano` Die
- Zugriff auf eine Linux- oder UNIX-Shell. Wenn Sie Windows verwenden, nutzen Sie eine Linux-Umgebung als Befehlszeilentool für die Interaktion mit Cumulus Linux.
- Die Baudrate muss am seriellen Konsolenschalter für den Konsolenzugriff des NVIDIA SN2100-Switches wie folgt auf 115200 eingestellt werden:
  - 115200 Baud
  - 8 Datenbits
  - 1 Stoppbit
  - Parität: keine
  - Flusssteuerung: keine

Informationen zu diesem Vorgang

Beachten Sie Folgendes:

Bei jeder Neuinstallation von Cumulus Linux wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

Das Standardpasswort für das Cumulus-Benutzerkonto lautet **cumulus**. Beim ersten Anmelden bei Cumulus Linux müssen Sie dieses Standardpasswort ändern. Aktualisieren Sie unbedingt alle Automatisierungsskripte, bevor Sie ein neues Image installieren. Cumulus Linux bietet Befehlszeilenoptionen, um das Standardpasswort während des Installationsprozesses automatisch zu ändern.

Beispiel 1. Schritte

Cumulus Linux 4.4.3

1. Melden Sie sich am Switch an.

   Für die erstmalige Anmeldung am Switch werden der Benutzername und das Passwort **cumulus** /**cumulus** benötigt. `sudo` Privilegien.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Überprüfen Sie die Cumulus Linux-Version: `net show system`

```
cumulus@cumulus:mgmt:~$ net show system
Hostname..... cumulus
Build..... Cumulus Linux 4.4.3
Uptime..... 0:08:20.860000
Model..... Mlnx X86
CPU..... x86_64 Intel Atom C2558 2.40GHz
Memory..... 8GB
Disk..... 14.7GB
ASIC..... Mellanox Spectrum MT52132
Ports..... 16 x 100G-QSFP28
Part Number..... MSN2100-CB2FC
Serial Number.... MT2105T05177
Platform Name.... x86_64-mlnx_x86-r0
Product Name..... MSN2100
ONIE Version..... 2019.11-5.2.0020-115200
Base MAC Address. 04:3F:72:43:92:80
Manufacturer..... Mellanox
```

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standardgateway. Der neue Hostname wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

> Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0` Die Diese Schnittstelle ist speziell für die Out-of-Band-Verwaltung vorgesehen. Standardmäßig verwendet die Verwaltungsschnittstelle DHCPv4 zur Adressierung.

Verwenden Sie im Hostnamen keinen Unterstrich (_), keinen Apostroph (') und keine Nicht-ASCII-Zeichen.

```
cumulus@cumulus:mgmt:~$ net add hostname sw1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address
10.233.204.71
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ net pending
cumulus@cumulus:mgmt:~$ net commit
```

Dieser Befehl ändert beides `/etc/hostname` Und `/etc/hosts` Dateien.

4. Prüfen Sie, ob Hostname, IP-Adresse, Subnetzmaske und Standardgateway aktualisiert wurden.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Stellen Sie Datum, Uhrzeit, Zeitzone und NTP-Server am Switch ein.
   a. Überprüfen Sie die aktuelle Zeitzone:

```
cumulus@sw1:~$ cat /etc/timezone
```

   b. Aktualisierung auf die neue Zeitzone:

```
cumulus@sw1:~$ sudo dpkg-reconfigure --frontend noninteractive
tzdata
```

c. Überprüfen Sie Ihre aktuelle Zeitzone:

```
cumulus@switch:~$ date +%Z
```

d. Um die Zeitzone mithilfe des geführten Assistenten einzustellen, führen Sie folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

e. Stellen Sie die Softwareuhr entsprechend der konfigurierten Zeitzone ein:

```
cumulus@switch:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

f. Den aktuellen Wert der Softwareuhr auf den Wert der Hardwareuhr setzen:

```
cumulus@switch:~$ sudo hwclock -w
```

g. Fügen Sie bei Bedarf einen NTP-Server hinzu:

```
cumulus@sw1:~$ net add time ntp server <cumulus.network.ntp.org>
iburst
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

h. Überprüfen Sie, ob `ntpd` läuft auf dem System:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

i. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig verwendet NTP die folgende Quellschnittstelle: `eth0` Die Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

```
cumulus@sw1:~$ net add time ntp source <src_int>
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

6. Installieren Sie Cumulus Linux 4.4.3:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-server>/<path>/cumulus-linux-4.4.3-mlx-amd64.bin
```

Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie dazu aufgefordert werden.

7. Starten Sie den NVIDIA SN2100 Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation startet automatisch, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Treffen Sie **keine** Auswahlen.
   - Cumulus-Linux GNU/Linux
   - ONIE: Betriebssystem installieren
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.
10. Überprüfen Sie, ob die Cumulus Linux-Version 4.4.3 ist: `net show version`

```
cumulus@sw1:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u0
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

11. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

    ```
    sudo adduser --ingroup netedit admin
    ```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

Cumulus Linux 5.4.0

1. Melden Sie sich am Switch an.

   Für die erstmalige Anmeldung am Switch werden der Benutzername und das Passwort **cumulus**

/**cumulus** benötigt. `sudo` Privilegien.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.3.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standardgateway. Der neue Hostname wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0` Die Diese Schnittstelle ist speziell für die Out-of-Band-Verwaltung vorgesehen. Standardmäßig verwendet die Verwaltungsschnittstelle DHCPv4 zur Adressierung.

Verwenden Sie im Hostnamen keinen Unterstrich (_), keinen Apostroph (') und keine Nicht-ASCII-Zeichen.

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Dieser Befehl ändert beides `/etc/hostname` Und `/etc/hosts` Dateien.

4. Prüfen Sie, ob Hostname, IP-Adresse, Subnetzmaske und Standardgateway aktualisiert wurden.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Stellen Sie Zeitzone, Datum, Uhrzeit und NTP-Server am Switch ein.
   a. Zeitzone einstellen:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Überprüfen Sie Ihre aktuelle Zeitzone:

```
cumulus@switch:~$ date +%Z
```

   c. Um die Zeitzone mithilfe des geführten Assistenten einzustellen, führen Sie folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

   d. Stellen Sie die Softwareuhr entsprechend der konfigurierten Zeitzone ein:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

   e. Den aktuellen Wert der Softwareuhr auf den Wert der Hardwareuhr setzen:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Fügen Sie bei Bedarf einen NTP-Server hinzu:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Siehe den Artikel in der Wissensdatenbank."Die NTP-Serverkonfiguration funktioniert nicht mit NVIDIA SN2100-Switches." für weitere Einzelheiten.

g. Überprüfen Sie, ob `ntpd` läuft auf dem System:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig verwendet NTP die folgende Quellschnittstelle: `eth0` Die Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installieren Sie Cumulus Linux 5.4.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.4-mlx-amd64.bin
```

Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie dazu aufgefordert werden.

7. Starten Sie den NVIDIA SN2100 Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation startet automatisch, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Treffen Sie **keine** Auswahlen.
   - Cumulus-Linux GNU/Linux
   - ONIE: Betriebssystem installieren
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.

10. Überprüfen Sie, ob die Cumulus Linux-Version 5.4.0 ist: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 13:37:36     system uptime
timezone            Etc/UTC              system time zone
```

11. Überprüfen Sie, ob jeder Knoten eine Verbindung zu jedem Switch hat:

```
cumulus@sw1:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ----------------------------------
-----------
eth0       100M   Mgmt        mgmt-sw1
Eth110/1/29
swp2s1     25G    Trunk/L2    node1
e0a
swp15      100G   BondMember  sw2
swp15
swp16      100G   BondMember  sw2
swp16
```

12. Erstellen Sie einen neuen Benutzer und fügen Sie diesen Benutzer der folgenden Gruppe hinzu: `sudo` Gruppe. Dieser Benutzer wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

```
sudo adduser --ingroup netedit admin
```

```
cumulus@sw1:mgmt:~$ sudo adduser --ingroup netedit admin
[sudo] password for cumulus:
Adding user 'admin' ...
Adding new user 'admin' (1001) with group `netedit' ...
Creating home directory '/home/admin' ...
Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for admin
Enter the new value, or press ENTER for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y

cumulus@sw1:mgmt:~$ sudo adduser admin sudo
[sudo] password for cumulus:
Adding user `admin' to group `sudo' ...
Adding user admin to group sudo
Done.
cumulus@sw1:mgmt:~$ exit
logout
Connection to 10.233.204.71 closed.

[admin@cycrh6svl01 ~]$ ssh admin@10.233.204.71
admin@10.233.204.71's password:
Linux sw1 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.1u1
(2021-09-09) x86_64
Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense
from LMI, the exclusive licensee of Linus Torvalds, owner of the
mark on a world-wide basis.
admin@sw1:mgmt:~$
```

13. Fügen Sie dem Administrator weitere Benutzergruppen hinzu, auf die er zugreifen kann. `nv` Befehle:

```
cumulus@sw1:mgmt:~$ sudo adduser admin nvshow
     [sudo] password for cumulus:
     Adding user 'admin' to group 'nvshow' ...
     Adding user admin to group nvshow
     Done.
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Cumulus Linux 5.11.0

1. Melden Sie sich am Switch an.

   Wenn Sie sich zum ersten Mal am Switch anmelden, benötigen Sie den Benutzernamen/das Passwort **cumulus**/**cumulus** mit `sudo` Privilegien.

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

2. Überprüfen Sie die Cumulus Linux-Version: `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied              description
------------------- -------------------- --------------------
hostname            cumulus              cumulus
build               Cumulus Linux 5.4.0  system build version
uptime              6 days, 8:37:36      system uptime
timezone            Etc/UTC              system time zone
```

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standardgateway. Der neue Hostname wird erst nach einem Neustart der Konsolen-/SSH-Sitzung wirksam.

   Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0` Die Diese Schnittstelle ist speziell für die Out-of-Band-Verwaltung vorgesehen. Standardmäßig verwendet die Verwaltungsschnittstelle DHCPv4 zur Adressierung.

   Verwenden Sie im Hostnamen keinen Unterstrich (_), keinen Apostroph (') und keine Nicht-ASCII-Zeichen.

```
cumulus@cumulus:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.233.204.71/24
cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway
10.233.204.1
cumulus@cumulus:mgmt:~$ nv config apply
cumulus@cumulus:mgmt:~$ nv config save
```

Dieser Befehl ändert beides `/etc/hostname` Und `/etc/hosts` Dateien.

4. Prüfen Sie, ob Hostname, IP-Adresse, Subnetzmaske und Standardgateway aktualisiert wurden.

```
cumulus@sw1:mgmt:~$ hostname sw1
cumulus@sw1:mgmt:~$ ifconfig eth0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
inet 10.233.204.71  netmask 255.255.254.0  broadcast 10.233.205.255
inet6 fe80::bace:f6ff:fe19:1df6  prefixlen 64  scopeid 0x20<link>
ether b8:ce:f6:19:1d:f6  txqueuelen 1000  (Ethernet)
RX packets 75364  bytes 23013528 (21.9 MiB)
RX errors 0  dropped 7  overruns 0  frame 0
TX packets 4053  bytes 827280 (807.8 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0 device
memory 0xdfc00000-dfc1ffff

cumulus@sw1::mgmt:~$ ip route show vrf mgmt
default via 10.233.204.1 dev eth0
unreachable default metric 4278198272
10.233.204.0/23 dev eth0 proto kernel scope link src 10.233.204.71
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

5. Stellen Sie Zeitzone, Datum, Uhrzeit und NTP-Server am Switch ein.
   a. Zeitzone einstellen:

```
cumulus@sw1:~$ nv set system timezone US/Eastern
cumulus@sw1:~$ nv config apply
```

   b. Überprüfen Sie Ihre aktuelle Zeitzone:

```
cumulus@switch:~$ date +%Z
```

   c. Um die Zeitzone mithilfe des geführten Assistenten einzustellen, führen Sie folgenden Befehl aus:

```
cumulus@sw1:~$ sudo dpkg-reconfigure tzdata
```

d. Stellen Sie die Softwareuhr entsprechend der konfigurierten Zeitzone ein:

```
cumulus@sw1:~$ sudo date -s "Tue Oct 28 00:37:13 2023"
```

e. Den aktuellen Wert der Softwareuhr auf den Wert der Hardwareuhr setzen:

```
cumulus@sw1:~$ sudo hwclock -w
```

f. Fügen Sie bei Bedarf einen NTP-Server hinzu:

```
cumulus@sw1:~$ nv set service ntp mgmt listen eth0
cumulus@sw1:~$ nv set service ntp mgmt server <server> iburst on
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

Siehe den Artikel in der Wissensdatenbank."Die NTP-Serverkonfiguration funktioniert nicht mit NVIDIA SN2100-Switches." für weitere Einzelheiten.

g. Überprüfen Sie, ob `ntpd` läuft auf dem System:

```
cumulus@sw1:~$ ps -ef | grep ntp
ntp       4074     1  0 Jun20 ?        00:00:33 /usr/sbin/ntpd -p
/var/run/ntpd.pid -g -u 101:102
```

h. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig verwendet NTP die folgende Quellschnittstelle: `eth0` Die Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

```
cumulus@sw1:~$ nv set service ntp default listen <src_int>
cumulus@sw1:~$ nv config apply
```

6. Installieren Sie Cumulus Linux 5.11.0:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.11.0-mlx-amd64.bin
```

Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie dazu aufgefordert werden.

7. Starten Sie den NVIDIA SN2100 Switch neu:

```
cumulus@sw1:mgmt:~$ sudo reboot
```

8. Die Installation startet automatisch, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Treffen Sie **keine** Auswahlen.
   - Cumulus-Linux GNU/Linux
   - ONIE: Betriebssystem installieren
   - CUMULUS-INSTALL
   - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.
10. Überprüfen Sie, ob die Cumulus Linux-Version 5.11.0 ist:

    `nv show system`

```
cumulus@cumulus:mgmt:~$ nv show system
operational         applied                 description
------------------- ----------------------- --------------------
build               Cumulus Linux 5.11.0
uptime              153 days, 2:44:16
hostname            cumulus                 cumulus
product-name        Cumulus Linux
product-release     5.11.0
platform            x86_64-mlnx_x86-r0
system-memory       2.76 GB used / 2.28 GB free / 7.47 GB total
swap-memory         0 Bytes used / 0 Bytes free / 0 Bytes total
health-status       not OK
date-time           2025-04-23 09:55:24
status              N/A
timezone            Etc/UTC
maintenance
  mode              disabled
  ports             enabled
version
  kernel            6.1.0-cl-1-amd64
  build-date        Thu Nov 14 13:06:38 UTC 2024
  image             5.11.0
  onie              2019.11-5.2.0020-115200
```

11. Überprüfen Sie, ob jeder Knoten mit jedem Switch verbunden ist:

```
cumulus@sw1:mgmt:~$ nv show interface lldp

LocalPort  Speed  Mode        RemoteHost
RemotePort
---------  -----  ----------  ---------------------------------
-----------
eth0       100M   eth   mgmt-sw1
Eth110/1/14
swp2s1     25G    Trunk/L2    node1
e0a
swp1s1     10G    swp   sw2
e0a
swp9       100G   swp   sw3
e4a
swp10      100G   swp   sw4
e4a
swp15      100G   swp   sw5
swp15
swp16      100G   swp   sw6
swp16
```

Sehen "NVIDIA Benutzerkonten" für weitere Informationen.

Wie geht es weiter?

Nach der Installation von Cumulus Linux im Cumulus-Modus können Sie"Installieren oder aktualisieren Sie das RCF-Skript" Die

Installieren Sie Cumulus Linux im ONIE-Modus

Gehen Sie wie folgt vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im ONIE-Modus läuft.

Cumulus Linux (CL) OS kann entweder installiert werden, wenn auf dem Switch Cumulus Linux oder ONIE läuft (siehe"Installation im Cumulus-Modus").

Informationen zu diesem Vorgang

Sie können Cumulus Linux mithilfe der Open Network Install Environment (ONIE) installieren, die die automatische Erkennung eines Netzwerkinstallationsabbilds ermöglicht. Dies erleichtert das Systemmodell der Absicherung von Switches durch die Wahl eines Betriebssystems, wie beispielsweise Cumulus Linux. Cumulus Linux lässt sich am einfachsten mit ONIE über die lokale HTTP-Erkennung installieren.

Wenn Ihr Host IPv6-fähig ist, stellen Sie sicher, dass darauf ein Webserver läuft. Wenn Ihr Host IPv4-fähig ist, stellen Sie sicher, dass er zusätzlich zu einem Webserver auch DHCP ausführt.

Dieses Verfahren zeigt, wie man Cumulus Linux aktualisiert, nachdem der Administrator in ONIE gestartet hat.

Schritte

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Benennen Sie diese Datei um `onie-installer` Die
2. Verbinden Sie Ihren Host mithilfe eines Ethernet-Kabels mit dem Management-Ethernet-Port des Switches.
3. Den Schalter einschalten. Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der Installation erscheint die Cumulus Linux-Anmeldeaufforderung im Terminalfenster.

   Bei jeder Neuinstallation von Cumulus Linux wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Switch neu:

   ```
   cumulus@cumulus:mgmt:~$ sudo reboot
   ```

5. Drücken Sie auf dem GNU GRUB-Bildschirm die **Esc**-Taste, um den normalen Bootvorgang zu unterbrechen, wählen Sie **ONIE** aus und drücken Sie **Enter**.
6. Im nächsten angezeigten Bildschirm wählen Sie **ONIE: Betriebssystem installieren**.
7. Der ONIE-Installer-Erkennungsprozess wird ausgeführt und sucht nach der automatischen Installation. Drücken Sie die **Eingabetaste**, um den Vorgang vorübergehend zu unterbrechen.
8. Wenn der Ermittlungsprozess abgeschlossen ist:

   ```
   ONIE:/ # onie-stop
   discover: installer mode detected.
   Stopping: discover...start-stop-daemon: warning: killing process 427:
   No such process done.
   ```

9. Wenn der DHCP-Dienst in Ihrem Netzwerk ausgeführt wird, überprüfen Sie, ob die IP-Adresse, die Subnetzmaske und das Standardgateway korrekt zugewiesen sind:

   ```
   ifconfig eth0
   ```

Beispiel anzeigen

```
ONIE:/ # ifconfig eth0
eth0   Link encap:Ethernet  HWaddr B8:CE:F6:19:1D:F6
       inet addr:10.233.204.71  Bcast:10.233.205.255
Mask:255.255.254.0
       inet6 addr: fe80::bace:f6ff:fe19:1df6/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:21344 errors:0 dropped:2135 overruns:0 frame:0
       TX packets:3500 errors:0 dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:6119398 (5.8 MiB)  TX bytes:472975 (461.8 KiB)
       Memory:dfc00000-dfc1ffff

ONIE:/ # route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref
Use Iface

default         10.233.204.1    0.0.0.0         UG    0      0
0   eth0
10.233.204.0    *               255.255.254.0   U     0      0
0   eth0
```

10. Wenn das IP-Adressierungsschema manuell definiert wurde, gehen Sie wie folgt vor:

```
ONIE:/ # ifconfig eth0 10.233.204.71 netmask 255.255.254.0
ONIE:/ # route add default gw 10.233.204.1
```

11. Wiederholen Sie Schritt 9, um zu überprüfen, ob die statischen Informationen korrekt eingegeben wurden.
12. Installieren Sie Cumulus Linux:

```
ONIE:/ # route

  Kernel IP routing table

  ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-linux-
4.4.3-mlx-amd64.bin

  Stopping: discover... done.
  Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.3-
mlx-amd64.bin ...
  Connecting to 10.60.132.97 (10.60.132.97:80)
  installer            100% |*|   552M  0:00:00 ETA
  ...
  ...
```

13. Sobald die Installation abgeschlossen ist, melden Sie sich am Switch an:

Beispiel anzeigen

```
cumulus login: cumulus
Password: cumulus
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password: cumulus
New password: <new_password>
Retype new password: <new_password>
```

14. Überprüfen Sie die Cumulus Linux-Version:

```
net show version
```

Beispiel anzeigen

```
cumulus@cumulus:mgmt:~$ net show version
NCLU_VERSION=1.0-cl4.4.3u4
DISTRIB_ID="Cumulus Linux"
DISTRIB_RELEASE=4.4.3
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3”
```

Wie geht es weiter?

Nach der Installation von Cumulus Linux im ONIE-Modus können Sie"Installieren oder aktualisieren Sie das RCF-Skript" Die

Installieren oder aktualisieren Sie das RCF-Skript.

Folgen Sie dieser Vorgehensweise, um das RCF-Skript zu installieren oder zu aktualisieren.

Bevor Sie beginnen

Vor der Installation oder Aktualisierung des RCF-Skripts stellen Sie sicher, dass Folgendes auf dem Switch verfügbar ist:

- Cumulus Linux 4.4.3 ist installiert.
- IP-Adresse, Subnetzmaske und Standardgateway werden per DHCP definiert oder manuell konfiguriert.

Aktuelle RCF-Skriptversionen

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Die Vorgehensweise ist für alle Fälle gleich.

- Clustering: **MSN2100-RCF-v1.*x*-Cluster**
- Speicher: **MSN2100-RCF-v1.*x*-Speicher**

Das folgende Beispielverfahren zeigt, wie das RCF-Skript für Cluster-Switches heruntergeladen und angewendet wird.

Beispielausgabe des Befehls verwendet die Switch-Management-IP-Adresse 10.233.204.71, die Netzmaske 255.255.254.0 und das Standardgateway 10.233.204.1.

Schritte

1. Die verfügbaren Schnittstellen des SN2100-Switches anzeigen:

```
net show interface all
```

Beispiel anzeigen

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name   Spd  MTU    Mode          LLDP                 Summary
-----  -----  ---  -----  ------------  -------------------
--------------
...
...
ADMDN  swp1   N/A  9216   NotConfigured
ADMDN  swp2   N/A  9216   NotConfigured
ADMDN  swp3   N/A  9216   NotConfigured
ADMDN  swp4   N/A  9216   NotConfigured
ADMDN  swp5   N/A  9216   NotConfigured
ADMDN  swp6   N/A  9216   NotConfigured
ADMDN  swp7   N/A  9216   NotConfigure
ADMDN  swp8   N/A  9216   NotConfigured
ADMDN  swp9   N/A  9216   NotConfigured
ADMDN  swp10  N/A  9216   NotConfigured
ADMDN  swp11  N/A  9216   NotConfigured
ADMDN  swp12  N/A  9216   NotConfigured
ADMDN  swp13  N/A  9216   NotConfigured
ADMDN  swp14  N/A  9216   NotConfigured
ADMDN  swp15  N/A  9216   NotConfigured
ADMDN  swp16  N/A  9216   NotConfigured
```

2. Kopieren Sie das RCF-Python-Skript auf den Switch:

```
admin@sw1:mgmt:~$ pwd
/home/cumulus
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host:/<path>/MSN2100-RCF-v1.8-
Cluster
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.8-Cluster                 100% 8607   111.2KB/s
00:00
```

3. Wenden Sie das RCF-Python-Skript **MSN2100-RCF-v1.8-Cluster** an:

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.8-Cluster
[sudo] password for cumulus:
...
Step 1: Creating the banner file
Step 2: Registering banner message
Step 3: Updating the MOTD file
Step 4: Ensuring passwordless use of cl-support command by admin
Step 5: Disabling apt-get
Step 6: Creating the interfaces
Step 7: Adding the interface config
Step 8: Disabling cdp
Step 9: Adding the lldp config
Step 10: Adding the RoCE base config
Step 11: Modifying RoCE Config
Step 12: Configure SNMP
Step 13: Reboot the switch
```

Das RCF-Skript führt die oben aufgeführten Schritte aus.

> Bei Problemen mit RCF-Python-Skripten, die nicht behoben werden können, wenden Sie sich bitte an [Kontaktinformationen einfügen]. "NetApp Support" um Unterstützung zu erhalten.

4. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
5. Überprüfen Sie die Konfiguration nach dem Neustart:

   ```
   net show interface all
   ```

Beispiel anzeigen

```
cumulus@cumulus:mgmt:~$ net show interface all

State  Name      Spd   MTU    Mode       LLDP               Summary
-----  --------- ----  -----  ---------- ------------------ --------
...
...
DN     swp1s0    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp1s1    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp1s2    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp1s3    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp2s0    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp2s1    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp2s2    N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp2s3    N/A   9216   Trunk/L2                      Master:
bridge(UP)
UP     swp3      100G  9216   Trunk/L2                      Master:
bridge(UP)
UP     swp4      100G  9216   Trunk/L2                      Master:
bridge(UP)
DN     swp5      N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp6      N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp7      N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp8      N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp9      N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp10     N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp11     N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp12     N/A   9216   Trunk/L2                      Master:
bridge(UP)
DN     swp13     N/A   9216   Trunk/L2                      Master:
bridge(UP)
```

```
DN     swp14     N/A   9216   Trunk/L2                    Master:
bridge(UP)
UP     swp15     N/A   9216   BondMember                  Master:
bond_15_16(UP)
UP     swp16     N/A   9216   BondMember                  Master:
bond_15_16(UP)
...
...

cumulus@cumulus:mgmt:~$ net show roce config
RoCE mode..... lossless
Congestion Control:
  Enabled SPs.... 0 2 5
  Mode..... ECN
  Min Threshold.. 150 KB
  Max Threshold.. 1500 KB
PFC:
  Status..... enabled
  Enabled SPs.... 2 5
  Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9

DSCP                    802.1p  switch-priority
----------------------  ------  ---------------
0 1 2 3 4 5 6 7              0                0
8 9 10 11 12 13 14 15        1                1
16 17 18 19 20 21 22 23      2                2
24 25 26 27 28 29 30 31      3                3
32 33 34 35 36 37 38 39      4                4
40 41 42 43 44 45 46 47      5                5
48 49 50 51 52 53 54 55      6                6
56 57 58 59 60 61 62 63      7                7

switch-priority  TC  ETS
---------------  --  --------
0 1 3 4 6 7       0  DWRR 28%
2                 2  DWRR 28%
5                 5  DWRR 43%
```

6. Überprüfen Sie die Informationen für den Transceiver in der Schnittstelle:

   ```
   net show interface pluggables
   ```

Beispiel anzeigen

```
cumulus@cumulus:mgmt:~$ net show interface pluggables
Interface  Identifier     Vendor Name  Vendor PN        Vendor SN
    Vendor Rev
---------  -------------  -----------  ---------------
--------------  ----------
swp3       0x11 (QSFP28)  Amphenol     112-00574
APF20379253516  B0
swp4       0x11 (QSFP28)  AVAGO        332-00440        AF1815GU05Z
    A0
swp15      0x11 (QSFP28)  Amphenol     112-00573
APF21109348001  B0
swp16      0x11 (QSFP28)  Amphenol     112-00573
APF21109347895  B0
```

7. Überprüfen Sie, ob jeder Knoten eine Verbindung zu jedem Switch hat:

   `net show lldp`

Beispiel anzeigen

```
cumulus@cumulus:mgmt:~$ net show lldp

LocalPort  Speed  Mode        RemoteHost              RemotePort
---------  -----  ----------  ----------------------  -----------
swp3       100G   Trunk/L2    sw1                     e3a
swp4       100G   Trunk/L2    sw2                     e3b
swp15      100G   BondMember  sw13                    swp15
swp16      100G   BondMember  sw14                    swp16
```

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

   a. Überprüfen Sie, ob die e0d-Ports auf allen Knoten im Cluster aktiv und fehlerfrei sind:

      `network port show -role cluster`

Beispiel anzeigen

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

Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false

Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e3a       Cluster      Cluster          up   9000  auto/10000
healthy  false
e3b       Cluster      Cluster          up   9000  auto/10000
healthy  false
```

a. Überprüfen Sie den Zustand des Switches vom Cluster aus (dabei wird möglicherweise Switch sw2 nicht angezeigt, da LIFs nicht auf e0d liegen).

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface Platform
----------- ------ ------------------------- --------- ----------
node1/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp3      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp3      -

node2/lldp
            e3a    sw1 (b8:ce:f6:19:1a:7e)   swp4      -
            e3b    sw2 (b8:ce:f6:19:1b:96)   swp4      -


cluster1::*> system switch ethernet show -is-monitoring-enabled
-operational true
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
-----
sw1                         cluster-network    10.233.205.90
MSN2100-CB2RC
     Serial Number: MNXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP

sw2                         cluster-network    10.233.205.91
MSN2100-CB2RC
     Serial Number: MNCXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cumulus Linux version 4.4.3 running on
Mellanox
                    Technologies Ltd. MSN2100
    Version Source: LLDP
```

Wie geht es weiter?

Nach der Installation oder Aktualisierung des RCF können Sie"Installieren Sie die CSHM-Datei" Die

Installieren Sie die Konfigurationsdatei für den Ethernet Switch Health Monitor.

Gehen Sie wie folgt vor, um die entsprechende Konfigurationsdatei für die Zustandsüberwachung von Ethernet-Switches in NVIDIA Cluster-Switches zu installieren. Unterstützte Modelle sind:

- MSN2100-CB2FC
- MSN2100-CB2RC
- X190006-PE
- X190006-PI

Dieses Installationsverfahren gilt für ONTAP 9.10.1 und höher.

Bevor Sie beginnen

- Überprüfen Sie durch Ausführen des folgenden Befehls, ob Sie die Konfigurationsdatei herunterladen müssen. `system switch ethernet show` und prüfen, ob für Ihr Modell **ANDERE** angezeigt wird.

  Falls Ihr Modell nach Anwendung der Konfigurationsdatei immer noch **ANDERE** anzeigt, wenden Sie sich bitte an den NetApp -Support.

- Stellen Sie sicher, dass der ONTAP -Cluster betriebsbereit ist.
- Aktivieren Sie SSH, um alle in CSHM verfügbaren Funktionen nutzen zu können.
- Räumen Sie die `/mroot/etc/cshm_nod/nod_sign/` Verzeichnis auf allen Knoten:

  a. Geben Sie die NodeShell ein:

     ```
     system node run -node <name>
     ```

  b. Änderung zu erweiterten Berechtigungen:

     ```
     priv set advanced
     ```

  c. Listen Sie die Konfigurationsdateien im folgenden Verzeichnis auf: `/etc/cshm_nod/nod_sign` Verzeichnis. Wenn das Verzeichnis existiert und Konfigurationsdateien enthält, werden die Dateinamen aufgelistet.

     ```
     ls /etc/cshm_nod/nod_sign
     ```

  d. Löschen Sie alle Konfigurationsdateien, die zu Ihren angeschlossenen Switch-Modellen gehören.

     Wenn Sie sich nicht sicher sind, entfernen Sie alle Konfigurationsdateien für die oben aufgeführten unterstützten Modelle und laden Sie anschließend die neuesten Konfigurationsdateien für dieselben Modelle herunter und installieren Sie diese.

```
rm /etc/cshm_nod/nod_sign/<filename>
```

  a. Vergewissern Sie sich, dass die gelöschten Konfigurationsdateien nicht mehr im Verzeichnis vorhanden sind:

     ```
     ls /etc/cshm_nod/nod_sign
     ```

Schritte

1. Laden Sie die Konfigurations-ZIP-Datei für den Ethernet-Switch-Integritätsmonitor entsprechend der zugehörigen ONTAP Version herunter. Diese Datei ist verfügbar unter "NVIDIA Ethernet-Switches" Seite.
   a. Auf der Downloadseite der NVIDIA SN2100 Software wählen Sie **Nvidia CSHM-Datei** aus.
   b. Auf der Seite „Vorsicht/Unbedingt lesen“ das Kontrollkästchen aktivieren, um zuzustimmen.
   c. Auf der Seite „Endbenutzer-Lizenzvereinbarung“ das Kontrollkästchen aktivieren, um zuzustimmen, und auf **Akzeptieren & Fortfahren** klicken.
   d. Auf der Seite „Nvidia CSHM File - Download“ wählen Sie die entsprechende Konfigurationsdatei aus. Folgende Dateien sind verfügbar:

ONTAP 9.15.1 und höher

- MSN2100-CB2FC-v1.4.zip
- MSN2100-CB2RC-v1.4.zip
- X190006-PE-v1.4.zip
- X190006-PI-v1.4.zip

ONTAP 9.11.1 bis 9.14.1

- MSN2100-CB2FC_PRIOR_R9.15.1-v1.4.zip
- MSN2100-CB2RC_PRIOR_R9.15.1-v1.4.zip
- X190006-PE_PRIOR_9.15.1-v1.4.zip
- X190006-PI_PRIOR_9.15.1-v1.4.zip

1. Laden Sie die entsprechende ZIP-Datei auf Ihren internen Webserver hoch.
2. Die Einstellungen für den erweiterten Modus können Sie von einem der ONTAP -Systeme im Cluster aus aufrufen.

   ```
   set -privilege advanced
   ```

3. Führen Sie den Befehl „switch health monitor configure“ aus.

   ```
   cluster1::> system switch ethernet configure-health-monitor
   ```

4. Vergewissern Sie sich, dass die Befehlsausgabe für Ihre ONTAP Version mit folgendem Text endet:

ONTAP 9.15.1 und höher

Die Zustandsüberwachung des Ethernet-Switches hat die Konfigurationsdatei installiert.

ONTAP 9.11.1 bis 9.14.1

SHM hat die Konfigurationsdatei installiert.

ONTAP 9.10.1

Das heruntergeladene CSHM-Paket wurde erfolgreich verarbeitet.

Im Fehlerfall wenden Sie sich bitte an den NetApp Support.

1. Warten Sie bis zum Doppelten des Abfrageintervalls des Ethernet-Switch-Integritätsmonitors, das durch Ausführen von `system switch ethernet polling-interval show` , bevor der nächste Schritt ausgeführt wird.
2. Führen Sie den Befehl aus `system switch ethernet configure-health-monitor show` Stellen Sie im ONTAP -System sicher, dass die Cluster-Switches erkannt werden, wobei das überwachte Feld auf **True** gesetzt ist und das Feld für die Seriennummer nicht **Unknown** anzeigt.

```
cluster1::> system switch ethernet configure-health-monitor show
```

Wie geht es weiter?

Nach der Installation der CSHM-Datei können Sie"Konfigurieren der Switch-Integritätsüberwachung" Die

Setzen Sie den SN2100-Speicherschalter auf die Werkseinstellungen zurück

So setzen Sie den SN2100-Speicherschalter auf die Werkseinstellungen zurück:

- Für Cumulus Linux 5.10 und früher wenden Sie das Cumulus-Image an.
- Für Cumulus Linux 5.11 und höher verwenden Sie die `nv action reset system factory-default` Befehl.

Informationen zu diesem Vorgang

- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Sie müssen über das Root-Passwort verfügen, um per Sudo auf die Befehle zugreifen zu können.

Weitere Informationen zur Installation von Cumulus Linux finden Sie unter"Softwareinstallations-Workflow für NVIDIA SN2100-Switches" Die

Beispiel 2. Schritte

Cumulus Linux 5.10 und früher

1. Laden Sie über die Cumulus-Konsole die Installation der Switch-Software mit dem Befehl herunter und stellen Sie sie in die Warteschlange. `onie-install -a -i` gefolgt vom Dateipfad zur Switch-Software, zum Beispiel:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<web-
server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin
```

2. Das Installationsprogramm startet den Download. Geben Sie **y** ein, wenn Sie aufgefordert werden, die Installation zu bestätigen, nachdem das Image heruntergeladen und überprüft wurde.
3. Starten Sie den Switch neu, um die neue Software zu installieren.

   `sudo reboot`

```
cumulus@sw1:mgmt:~$ sudo reboot
```

> Der Switch startet neu und beginnt mit der Installation der Switch-Software, was einige Zeit in Anspruch nimmt. Nach Abschluss der Installation startet der Switch neu und verbleibt im aktuellen Zustand. `log-in` prompt.

Cumulus Linux 5.11 und höher

1. Um den Switch auf die Werkseinstellungen zurückzusetzen und alle Konfigurations-, System- und Protokolldateien zu entfernen, führen Sie Folgendes aus:

   `nv action reset system factory-default`

   Beispiel:

```
cumulus@switch:~$ nv action reset system factory-default

This operation will reset the system configuration, delete the log
files and reboot the switch.
Type [y] continue.
Type [n] to abort.
Do you want to continue? [y/n] y
```

Siehe NVIDIA "Werksreset" Weitere Einzelheiten finden Sie in der Dokumentation.

Was kommt als nächstes

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

Schalter migrieren

Migration von einem Cisco -Speicher-Switch zu einem NVIDIA SN2100-Speicher-Switch

Ältere Cisco Switches für einen ONTAP Cluster können auf NVIDIA SN2100-Speicher-Switches migriert werden. Dies ist ein unterbrechungsfreies Verfahren.

Überprüfungsanforderungen

Folgende Speichersysteme werden unterstützt:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Siehe die "Hardware Universe" Für detaillierte Informationen zu den unterstützten Ports und deren Konfigurationen.

Bevor Sie beginnen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Der bestehende Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Speicheranschlüsse sind aktiviert, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die NVIDIA SN2100 Speicherswitches sind konfiguriert und arbeiten unter der richtigen Version von Cumulus Linux, auf der die Referenzkonfigurationsdatei (RCF) angewendet wurde.
- Die bestehende Speichernetzwerkkonfiguration weist folgende Merkmale auf:
  - Ein redundanter und voll funktionsfähiger NetApp Cluster, der beide ältere Cisco Switches nutzt.
  - Management-Konnektivität und Konsolenzugriff sowohl auf die älteren Cisco Switches als auch auf die neuen Switches.
  - Alle Cluster-LIFs befinden sich im aktiven Zustand und sind an ihren Heimatports angeschlossen.
  - ISL-Ports wurden aktiviert und zwischen den älteren Cisco Switches sowie zwischen den neuen Switches verkabelt.
- Siehe die "Hardware Universe" Für detaillierte Informationen zu den unterstützten Ports und deren Konfigurationen.
- Einige der Ports sind auf NVIDIA SN2100 Switches für den Betrieb mit 100 GbE konfiguriert.
- Sie haben die 100-GbE-Konnektivität von den Knoten zu den NVIDIA SN2100-Speicher-Switches geplant, migriert und dokumentiert.

Migrieren Sie die Schalter

Zu den Beispielen

In diesem Verfahren werden Cisco Nexus 9336C-FX2 Storage-Switches als Beispiel für Befehle und Ausgaben verwendet.

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

- Die vorhandenen Cisco Nexus 9336C-FX2 Storage-Switches sind *S1* und *S2*.
- Die neuen NVIDIA SN2100 Speicherschalter sind *sw1* und *sw2*.
- Die Knoten heißen *node1* und *node2*.

- Die Cluster-LIFs sind *node1_clus1* und *node1_clus2* auf Knoten 1 bzw. *node2_clus1* und *node2_clus2* auf Knoten 2.
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Netzwerkanschlüsse sind *e5a* und *e5b*.
- Die Breakout-Ports haben folgendes Format: swp1s0-3. Beispielsweise gibt es vier Breakout-Ports auf swp1: *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.
- Zuerst wird Schalter S2 durch Schalter sw2 ersetzt, dann wird Schalter S1 durch Schalter sw1 ersetzt.
  - Die Verkabelung zwischen den Knoten und S2 wird dann von S2 getrennt und wieder mit sw2 verbunden.
  - Die Verkabelung zwischen den Knoten und S1 wird dann von S1 getrennt und wieder mit sw1 verbunden.

Schritt 1: Vorbereitung auf die Migration

1. Wenn AutoSupport 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 ist.

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. Ermitteln Sie den administrativen oder betrieblichen Status jeder Speicherschnittstelle:

   Jeder Port sollte als aktiviert angezeigt werden `Status` Die

Schritt 2: Kabel und Anschlüsse konfigurieren

1. Netzwerkportattribute anzeigen:

   ```
   storage port show
   ```

Beispiel anzeigen

```
cluster1::*> storage port show
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

2. Überprüfen Sie mithilfe des folgenden Befehls, ob die Speicherports an jedem Knoten wie folgt mit den vorhandenen Speicherswitches verbunden sind (aus Sicht der Knoten):

   `network device-discovery show -protocol lldp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1           -
            e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/1           -
node2      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2           -
            e5b    S2 (7c:ad:4f:98:8e:3c)    Eth1/2           -
```

3. Stellen Sie an den Switches S1 und S2 mithilfe des folgenden Befehls sicher, dass die Speicherports und Switches wie folgt verbunden sind (aus Sicht der Switches):

   `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     Holdtime    Capability
Port ID
node1                 Eth1/1         121         S
e0c
node2                 Eth1/2         121         S
e0c
SHFGD1947000186       Eth1/10        120         S
  e0a
SHFGD1947000186       Eth1/11        120         S
  e0a
SHFGB2017000269       Eth1/12        120         S
  e0a
SHFGB2017000269       Eth1/13        120         S
  e0a

S2# show lldp neighbors

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS
Cable Device,
                  (W) WLAN Access Point, (P) Repeater, (S) Station
(O) Other

Device-ID             Local Intf     Holdtime    Capability
Port ID
node1                 Eth1/1         121         S
e5b
node2                 Eth1/2         121         S
e5b
SHFGD1947000186       Eth1/10        120         S
 e0b
SHFGD1947000186       Eth1/11        120         S
 e0b
SHFGB2017000269       Eth1/12        120         S
 e0b
SHFGB2017000269       Eth1/13        120         S
 e0b
```

4. Schalten Sie am Switch sw2 die Ports ab, die mit den Speicherports und Knoten der Disk-Shelches verbunden sind.

Beispiel anzeigen

```
cumulus@sw2:~$ net add interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

5. Verlegen Sie die Speicherknotenanschlüsse des Controllers und der Festplattengehäuse vom alten Switch S2 auf den neuen Switch sw2. Verwenden Sie dazu geeignete Kabel, die von NVIDIA SN2100 unterstützt werden.
6. Schalten Sie am Switch sw2 die Ports ein, die mit den Speicherports der Knoten und den Festplattengehäusen verbunden sind.

Beispiel anzeigen

```
cumulus@sw2:~$ net del interface swp1-16 link down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

7. Überprüfen Sie aus Sicht der Knoten, ob die Speicheranschlüsse an jedem Knoten nun wie folgt mit den Switches verbunden sind:

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

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface      Platform
----------- ------ ------------------------- -------------
----------------
node1      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/1         -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp1           -

node2      /lldp
            e0c    S1 (7c:ad:4f:98:6d:f0)    Eth1/2         -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp2           -
```

8. Überprüfen Sie die Netzwerkportattribute:

   `storage port show`

   Beispiel anzeigen

```
cluster1::*> storage port show
                                  Speed                      VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

9. Überprüfen Sie am Switch sw2, ob alle Speicherports der Knoten aktiv sind:

   `net show interface`

Beispiel anzeigen

```
cumulus@sw2:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e5b)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e5b)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

10. Schalten Sie am Schalter sw1 die Ports ab, die mit den Speicherports der Knoten und den Festplattengehäusen verbunden sind.

Beispiel anzeigen

```
cumulus@sw1:~$ net add interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

11. Verlegen Sie die Speicherknotenanschlüsse des Controllers und die Festplattengehäuse vom alten Switch S1 zum neuen Switch sw1. Verwenden Sie dazu geeignete Kabel, die von NVIDIA SN2100 unterstützt werden.
12. Schalten Sie am Switch sw1 die Ports ein, die mit den Speicherports der Knoten und den Festplattengehäusen verbunden sind.

Beispiel anzeigen

```
cumulus@sw1:~$ net del interface swp1-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

13. Überprüfen Sie aus Sicht der Knoten, ob die Speicheranschlüsse an jedem Knoten nun wie folgt mit den Switches verbunden sind:

    `network device-discovery show -protocol lldp`

Beispiel anzeigen

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- --------------
----------------
node1      /lldp
            e0c    sw1 (b8:ce:f6:19:1b:96)   swp1            -
            e5b    sw2 (b8:ce:f6:19:1a:7e)   swp1            -

node2      /lldp
            e0c    sw1  (b8:ce:f6:19:1b:96)  swp2            -
            e5b    sw2  (b8:ce:f6:19:1a:7e)  swp2            -
```

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie die endgültige Konfiguration:

   `storage port show`

   Jeder Port sollte als aktiviert angezeigt werden `State` und aktiviert für `Status` Die

Beispiel anzeigen

```
cluster1::*> storage port show
                                  Speed                       VLAN
Node           Port Type  Mode    (Gb/s) State    Status       ID
-------------- ---- ----- ------- ------ -------- --------- ----
node1
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
node2
               e0c  ENET  storage  100   enabled  online       30
               e0d  ENET  storage    0   enabled  offline      30
               e5a  ENET  storage    0   enabled  offline      30
               e5b  ENET  storage  100   enabled  online       30
cluster1::*>
```

2. Überprüfen Sie am Switch sw2, ob alle Speicherports der Knoten aktiv sind:

   `net show interface`

Beispiel anzeigen

```
cumulus@sw2:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e5b)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e5b)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

3. Überprüfen Sie, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

   ```
   net show lldp
   ```

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
cumulus@sw1:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost              RemotePort
---------  -----  --------  ----------------------  -----------
...
swp1       100G   Trunk/L2  node1                   e0c
swp2       100G   Trunk/L2  node2                   e0c
swp3       100G   Trunk/L2  SHFFG1826000112        e0a
swp4       100G   Trunk/L2  SHFFG1826000112        e0a
swp5       100G   Trunk/L2  SHFFG1826000102        e0a
swp6       100G   Trunk/L2  SHFFG1826000102        e0a

cumulus@sw2:~$ net show lldp
LocalPort  Speed  Mode      RemoteHost              RemotePort
---------  -----  --------  ----------------------  -----------
...
swp1       100G   Trunk/L2  node1                   e5b
swp2       100G   Trunk/L2  node2                   e5b
swp3       100G   Trunk/L2  SHFFG1826000112        e0b
swp4       100G   Trunk/L2  SHFFG1826000112        e0b
swp5       100G   Trunk/L2  SHFFG1826000102        e0b
swp6       100G   Trunk/L2  SHFFG1826000102        e0b
```

4. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

5. 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?

Nach der Migration Ihrer Switches können Sie "Konfigurieren der Switch-Integritätsüberwachung"Die

Ersetzen Sie einen NVIDIA SN2100 Speicherschalter

Sie können einen defekten NVIDIA SN2100 Speicherschalter austauschen. Dies ist ein unterbrechungsfreies Verfahren.

Bevor Sie beginnen

Bevor Sie die Cumulus-Software und die RCFs auf einem NVIDIA SN2100-Speicher-Switch installieren, stellen Sie Folgendes sicher:

- Ihr System unterstützt NVIDIA SN2100 Speicherswitches.
- Sie haben die entsprechenden RCFs heruntergeladen.

Der "Hardware Universe" Enthält detaillierte Informationen zu den unterstützten Ports und deren Konfigurationen.

Die bestehende Netzwerkkonfiguration muss folgende Eigenschaften aufweisen:

- Führen Sie alle Schritte zur Fehlerbehebung durch, um zu bestätigen, dass Sie Ihren Schalter austauschen müssen.
- Stellen Sie sicher, dass auf beiden Switches eine Management-Verbindung besteht.

> Stellen Sie sicher, dass alle Schritte zur Fehlerbehebung abgeschlossen sind, um zu bestätigen, dass Ihr Schalter ausgetauscht werden muss.

Der Ersatz-Switch NVIDIA SN2100 muss folgende Eigenschaften aufweisen:

- Die Managementnetzwerkanbindung ist funktionsfähig.
- Sie können über die Konsole auf den Ersatzschalter zugreifen.
- Das entsprechende RCF- und Cumulus-Betriebssystemabbild wird auf den Switch geladen.
- Die erste Konfiguration des Schalters ist abgeschlossen.

Verfahrensübersicht

Bei diesem Verfahren wird der zweite NVIDIA SN2100 Speicherschalter sw2 durch den neuen NVIDIA SN2100 Schalter nsw2 ersetzt. Die beiden Knoten sind Knoten1 und Knoten2.

Zu erledigende Schritte:

- Bestätigen Sie, dass es sich bei dem auszutauschenden Schalter um SW2 handelt.
- Trennen Sie die Kabel vom Schalter sw2.
- Schließen Sie die Kabel wieder an den Schalter NSW2 an.
- Überprüfen Sie alle Gerätekonfigurationen auf Switch nsw2.

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

   ```
   set -privilege advanced
   ```

3. Überprüfen Sie den Gesundheitszustand der Speicherknotenports, um die Verbindung zum Speicherswitch S1 zu bestätigen:

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

Beispiel anzeigen

```
cluster1::*> 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 100    enabled  online       30
node2
               e3a  ENET  storage 100    enabled  online       30
               e3b  ENET  storage   0    enabled  offline      30
               e7a  ENET  storage   0    enabled  offline      30
               e7b  ENET  storage 100    enabled  online       30
cluster1::*>
```

4. Prüfen Sie, ob der Speicherschalter sw1 verfügbar ist:

   `network device-discovery show -protocol lldp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1/lldp
            e0M    sw1 (00:ea:bd:68:6a:e8)   Eth1/46           -
            e0b    sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16      -
            e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                                             e0a               -
            e0e    sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18      -
            e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                             e0b               -
            e0g    sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11      -
            e0h    sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22      -
            e1a    sw6 (00:f6:63:10:be:7c)   Ethernet1/33      -
            e1b    sw7 (00:f6:63:10:be:7d)   Ethernet1/34      -
            e2a    sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35      -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

5. Führe die `net show interface` Führen Sie einen Befehl auf dem funktionierenden Switch aus, um zu bestätigen, dass Sie beide Knoten und alle Regale sehen können:

   `net show interface`

Beispiel anzeigen

```
cumulus@sw1:~$ net show interface

State  Name    Spd   MTU    Mode        LLDP
Summary
-----  ------  ----  -----  ----------  --------------------
--------------------
...
...
UP     swp1    100G  9216   Trunk/L2   node1 (e3a)
Master: bridge(UP)
UP     swp2    100G  9216   Trunk/L2   node2 (e3a)
Master: bridge(UP)
UP     swp3    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp4    100G  9216   Trunk/L2   SHFFG1826000112 (e0b)
Master: bridge(UP)
UP     swp5    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP)
UP     swp6    100G  9216   Trunk/L2   SHFFG1826000102 (e0b)
Master: bridge(UP))
...
...
```

6. Überprüfen Sie die Regalanschlüsse im Lagersystem:

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

Beispiel anzeigen

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf   id  remote-port   remote-device
-----   --  -----------   -------------
3.20    0   swp3          sw1
3.20    1   -             -
3.20    2   swp4          sw1
3.20    3   -             -
3.30    0   swp5          sw1
3.20    1   -             -
3.30    2   swp6          sw1
3.20    3   -             -
cluster1::*>
```

7. Entfernen Sie alle Kabel, die am Speicherschalter sw2 angeschlossen sind.
8. Schließen Sie alle Kabel wieder an den Ersatzschalter NSW2 an.
9. Überprüfen Sie erneut den Gesundheitszustand der Speicherknotenports:

   `storage port show -port-type ENET`

   Beispiel anzeigen

```
cluster1::*> 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 100    enabled  online      30
node2
                  e3a  ENET  storage 100    enabled  online      30
                  e3b  ENET  storage   0    enabled  offline     30
                  e7a  ENET  storage   0    enabled  offline     30
                  e7b  ENET  storage 100    enabled  online      30
cluster1::*>
```

10. Vergewissern Sie sich, dass beide Schalter verfügbar sind:

    `net device-discovery show -protocol lldp`

Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node1/lldp
            e0M    sw1 (00:ea:bd:68:6a:e8)   Eth1/46           -
            e0b    sw2 (6c:b2:ae:5f:a5:b2)   Ethernet1/16      -
            e0c    SHFFG1827000286 (d0:39:ea:1c:16:92)
                                             e0a               -
            e0e    sw3 (6c:b2:ae:5f:a5:ba)   Ethernet1/18      -
            e0f    SHFFG1827000286 (00:a0:98:fd:e4:a9)
                                             e0b               -
            e0g    sw4 (28:ac:9e:d5:4a:9c)   Ethernet1/11      -
            e0h    sw5 (6c:b2:ae:5f:a5:ca)   Ethernet1/22      -
            e1a    sw6 (00:f6:63:10:be:7c)   Ethernet1/33      -
            e1b    sw7 (00:f6:63:10:be:7d)   Ethernet1/34      -
            e2a    sw8 (b8:ce:f6:91:3d:88)   Ethernet1/35      -
Press <space> to page down, <return> for next line, or 'q' to
quit...
10 entries were displayed.
```

11. Überprüfen Sie die Regalanschlüsse im Lagersystem:

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

Beispiel anzeigen

```
cluster1::*> storage shelf port show -fields remote-device, remote-
port
shelf   id    remote-port     remote-device
-----   --    -----------     -------------
3.20    0     swp3            sw1
3.20    1     swp3            nsw2
3.20    2     swp4            sw1
3.20    3     swp4            nsw2
3.30    0     swp5            sw1
3.20    1     swp5            nsw2
3.30    2     swp6            sw1
3.20    3     swp6            nsw2
cluster1::*>
```

12. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

    ```
    set -privilege admin
    ```

13. 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