Cisco Nexus 92300YC

Install and maintain

NetApp
February 13, 2026

Inhalt

Cisco Nexus 92300YC

Erste Schritte

Installations- und Einrichtungsworkflow für Cisco Nexus 92300YC-Switches

Cisco Nexus 92300YC-Switches können als Cluster-Switches in Ihrem AFF oder FAS Cluster verwendet werden. Mit Cluster-Switches können Sie ONTAP Cluster mit mehr als zwei Knoten erstellen.

Befolgen Sie diese Arbeitsschritte, um Ihren Cisco Nexus 92300YC-Switch zu installieren und einzurichten.

1. **"Konfigurationsanforderungen"**
   Prüfen Sie die Konfigurationsanforderungen für den Cluster-Switch 92300YC.

2. **"Erforderliche Dokumentation"**
   Lesen Sie die spezifische Switch- und Controller-Dokumentation, um Ihre 92300YC-Switches und den ONTAP Cluster einzurichten.

3. **"Anforderungen für Smart Call Home"**
   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 92300YC-Switches

Bei der Installation und Wartung des Cisco Nexus 92300YC Switches sollten Sie unbedingt alle Konfigurations- und Netzwerkanforderungen überprüfen.

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.

Konfigurationsanforderungen

Zur Konfiguration Ihres Clusters 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 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?" Weitere Informationen zu den Installationsanforderungen des Schalters finden Sie hier.

Was kommt als nächstes

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

Komponenten und Teilenummern für Cisco Nexus 92300YC-Switches

Bei der Installation und Wartung des Cisco Nexus 92300YC Switches sollten Sie unbedingt alle Switch-Komponenten und Teilenummern überprüfen. Siehe die "Hardware Universe" für Details. 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 folgende Tabelle listet die Teilenummer und Beschreibung für den Schalter 92300YC, die Lüfter und die Netzteile auf:

Teilenummer	Beschreibung
190003	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PTSX (PTSX = Port Side Exhaust)
190003R	Cisco 92300YC, CLSW, 48Pt10/25GB, 18Pt100G, PSIN (PSIN = Port Side Intake)
X-NXA-FAN-35CFM-B	Lüfter, Cisco N9K, seitlicher Lufteinlass
X-NXA-FAN-35CFM-F	Lüfter, Cisco N9K, seitlicher Luftauslass
X-NXA-PAC-650W-B	Netzteil, Cisco 650W - Einlass an der Portseite
X-NXA-PAC-650W-F	Netzteil, Cisco 650W - Auslassöffnung an der Portseite

Details zum Luftstrom des Cisco Nexus 92300YC Switches:

- Abluftstrom auf der Backbordseite (Standardluft) — Kühle Luft strömt durch die Lüfter- und Netzteilmodule im Kaltgang in das Gehäuse und wird durch das Backbordende des Gehäuses im Warmgang wieder ausgestoßen. Abluftstrom auf der Backbordseite mit blauer Färbung.
- Luftansaugung an der Backbordseite (umgekehrte Luftführung) — Kühle Luft strömt durch die Backbordseite im Kaltgang in das Gehäuse und wird durch die Lüfter- und Stromversorgungsmodule im Warmgang wieder ausgestoßen. Lufteinlass auf der Backbordseite mit bordeauxroter Färbung.

Was kommt als nächstes

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

Dokumentationsanforderungen für Cisco Nexus 92300YC-Switches

Für die Installation und Wartung des Cisco Nexus 92300YC Switches sollten Sie unbedingt die gesamte empfohlene Dokumentation durchlesen.

Switch-Dokumentation

Für die Einrichtung der Cisco Nexus 92300YC Switches benötigen Sie die folgende Dokumentation von "Cisco Nexus 9000 Series Switches Unterstützung" Seite:

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

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

ONTAP-Systemdokumentation

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

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

Dokumentation für Schienenbausatz und Schrank

Informationen zur Installation eines Cisco Nexus 92300YC 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 92300YC Switch in einem NetApp -Schrank"	Beschreibt die Installation eines Cisco Nexus 92300YC 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 92300YC-Switches

Gehen Sie folgendermaßen vor, um die Hardware für einen 92300YC-Cluster-Switch zu installieren und zu konfigurieren:

"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.

"Installieren Sie den Schalter"

Installieren Sie den Schalter 92300YC.

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

Installieren Sie den 92300YC-Switch und das Durchgangspanel nach Bedarf in einem NetApp Schrank.

"Kabel und Konfiguration prüfen"

Überprüfen Sie die Unterstützung für NVIDIA -Ethernet-Ports.

Vollständiges Verkabelungs-Arbeitsblatt für Cisco Nexus 92300YC

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.

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	10/25 GbE-Knoten	1	10/25 GbE-Knoten
2	10/25 GbE-Knoten	2	10/25 GbE-Knoten
3	10/25 GbE-Knoten	3	10/25 GbE-Knoten
4	10/25 GbE-Knoten	4	10/25 GbE-Knoten
5	10/25 GbE-Knoten	5	10/25 GbE-Knoten
6	10/25 GbE-Knoten	6	10/25 GbE-Knoten
7	10/25 GbE-Knoten	7	10/25 GbE-Knoten
8	10/25 GbE-Knoten	8	10/25 GbE-Knoten
9	10/25 GbE-Knoten	9	10/25 GbE-Knoten
10	10/25 GbE-Knoten	10	10/25 GbE-Knoten
11	10/25 GbE-Knoten	11	10/25 GbE-Knoten
12	10/25 GbE-Knoten	12	10/25 GbE-Knoten
13	10/25 GbE-Knoten	13	10/25 GbE-Knoten
14	10/25 GbE-Knoten	14	10/25 GbE-Knoten
15	10/25 GbE-Knoten	15	10/25 GbE-Knoten
16	10/25 GbE-Knoten	16	10/25 GbE-Knoten
17	10/25 GbE-Knoten	17	10/25 GbE-Knoten

Clusterschalter A		Clusterschalter B	
18	10/25 GbE-Knoten	18	10/25 GbE-Knoten
19	10/25 GbE-Knoten	19	10/25 GbE-Knoten
20	10/25 GbE-Knoten	20	10/25 GbE-Knoten
21	10/25 GbE-Knoten	21	10/25 GbE-Knoten
22	10/25 GbE-Knoten	22	10/25 GbE-Knoten
23	10/25 GbE-Knoten	23	10/25 GbE-Knoten
24	10/25 GbE-Knoten	24	10/25 GbE-Knoten
25	10/25 GbE-Knoten	25	10/25 GbE-Knoten
26	10/25 GbE-Knoten	26	10/25 GbE-Knoten
27	10/25 GbE-Knoten	27	10/25 GbE-Knoten
28	10/25 GbE-Knoten	28	10/25 GbE-Knoten
29	10/25 GbE-Knoten	29	10/25 GbE-Knoten
30	10/25 GbE-Knoten	30	10/25 GbE-Knoten
31	10/25 GbE-Knoten	31	10/25 GbE-Knoten
32	10/25 GbE-Knoten	32	10/25 GbE-Knoten
33	10/25 GbE-Knoten	33	10/25 GbE-Knoten
34	10/25 GbE-Knoten	34	10/25 GbE-Knoten
35	10/25 GbE-Knoten	35	10/25 GbE-Knoten
36	10/25 GbE-Knoten	36	10/25 GbE-Knoten
37	10/25 GbE-Knoten	37	10/25 GbE-Knoten
38	10/25 GbE-Knoten	38	10/25 GbE-Knoten
39	10/25 GbE-Knoten	39	10/25 GbE-Knoten

Clusterschalter A		Clusterschalter B	
40	10/25 GbE-Knoten	40	10/25 GbE-Knoten
41	10/25 GbE-Knoten	41	10/25 GbE-Knoten
42	10/25 GbE-Knoten	42	10/25 GbE-Knoten
43	10/25 GbE-Knoten	43	10/25 GbE-Knoten
44	10/25 GbE-Knoten	44	10/25 GbE-Knoten
45	10/25 GbE-Knoten	45	10/25 GbE-Knoten
46	10/25 GbE-Knoten	46	10/25 GbE-Knoten
47	10/25 GbE-Knoten	47	10/25 GbE-Knoten
48	10/25 GbE-Knoten	48	10/25 GbE-Knoten
49	40/100-GbE-Knoten	49	40/100-GbE-Knoten
50	40/100-GbE-Knoten	50	40/100-GbE-Knoten
51	40/100-GbE-Knoten	51	40/100-GbE-Knoten
52	40/100-GbE-Knoten	52	40/100-GbE-Knoten
53	40/100-GbE-Knoten	53	40/100-GbE-Knoten
54	40/100-GbE-Knoten	54	40/100-GbE-Knoten
55	40/100-GbE-Knoten	55	40/100-GbE-Knoten
56	40/100-GbE-Knoten	56	40/100-GbE-Knoten
57	40/100-GbE-Knoten	57	40/100-GbE-Knoten
58	40/100-GbE-Knoten	58	40/100-GbE-Knoten
59	40/100-GbE-Knoten	59	40/100-GbE-Knoten
60	40/100-GbE-Knoten	60	40/100-GbE-Knoten
61	40/100-GbE-Knoten	61	40/100-GbE-Knoten

Clusterschalter A		Clusterschalter B	
62	40/100-GbE-Knoten	62	40/100-GbE-Knoten
63	40/100-GbE-Knoten	63	40/100-GbE-Knoten
64	40/100-GbE-Knoten	64	40/100-GbE-Knoten
65	100-GbE-ISL-zu-Switch-B-Port 65	65	100-GbE-ISL-zu-Switch-A-Port 65
66	100-GbE-ISL-zu-Switch-B-Port 66	66	100-GbE-ISL-zu-Switch-A-Port 65

Leeres Verkabelungsarbeitsblatt

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	
Switch-Port	Knoten-/Portnutzung	Switch-Port	Knoten-/Portnutzung
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	

Clusterschalter A		Clusterschalter B	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	

Clusterschalter A		Clusterschalter B	
35		35	
36		36	
37		37	
38		38	
39		39	
40		40	
41		41	
42		42	
43		43	
44		44	
45		45	
46		46	
47		47	
48		48	
49		49	
50		50	
51		51	
52		52	
53		53	
54		54	
55		55	
56		56	

Clusterschalter A		Clusterschalter B	
57		57	
58		58	
59		59	
60		60	
61		61	
62		62	
63		63	
64		64	
65	ISL zum Schalter B Port 65	65	ISL zum Umschalten von Port 65
66	ISL zum Schalter B Port 66	66	ISL zum Umschalten von Port 66

Was kommt als nächstes

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

Installieren Sie den Cluster-Switch 92300YC

Gehen Sie wie folgt vor, um den Cisco Nexus 92300YC 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.
- 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 Switch- und ONTAP Dokumentation".

Schritte

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

Wenn Sie die… installieren	Dann…
Cisco Nexus 92300YC in einem NetApp -Systemschrank	Anweisungen zur Installation des Switches in einem NetApp -Schrank finden Sie im Handbuch „Installieren eines Cisco Nexus 92300YC-Cluster-Switches und Pass-Through-Panels in einem 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.

Wie geht es weiter?

Optional können Sie "Installieren Sie einen Cisco Nexus 3223C-Switch in einem NetApp -Schrank"Die Ansonsten gehen Sie zu "Kabel und Konfiguration prüfen"Die

Installieren Sie einen Cisco Nexus 92300YC-Cluster-Switch in einem NetApp Schrank

Abhängig von Ihrer Konfiguration müssen Sie den Cisco Nexus 92300YC-Cluster-Switch und das Pass-Through-Panel möglicherweise mit den im Lieferumfang des Switches enthaltenen Standardhalterungen in einem NetApp -Schrank installieren.

Bevor Sie beginnen

- Die anfänglichen Vorbereitungsanforderungen, der Inhalt des Kits und die Sicherheitsvorkehrungen im"Hardware-Installationshandbuch für die Cisco Nexus 9000-Serie" Die
- Für jeden Schalter werden die acht 10-32 oder 12-24 Schrauben und Clipmuttern benötigt, um die Halterungen und Gleitschienen an den vorderen und hinteren Gehäusepfosten zu befestigen.
- 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

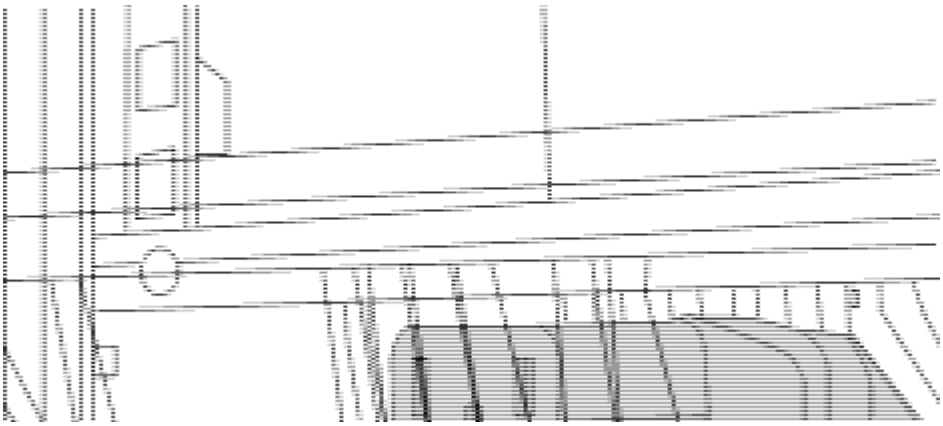
- Vier 10-32 Clipmuttern
  i. Ermitteln Sie die vertikale Position der Schalter und der Abdeckplatte im Gehäuse.

     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.

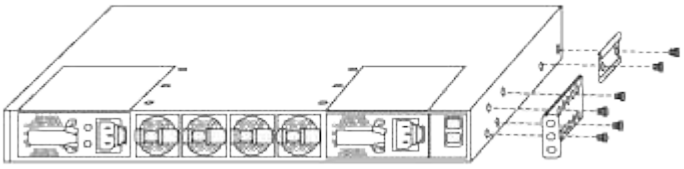
  iii. Zentrieren Sie das Panel vertikal, um ein Eindringen in den angrenzenden Rack-Bereich zu verhindern, und ziehen Sie dann die Schrauben fest.

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

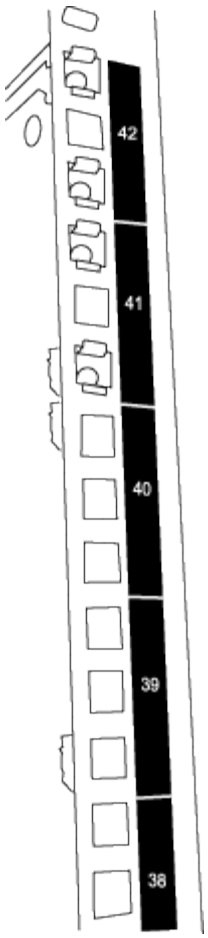


(1) Weiblicher Stecker des Überbrückungskabels.

1. Installieren Sie die Rackmontagehalterungen am Nexus 92300YC-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.



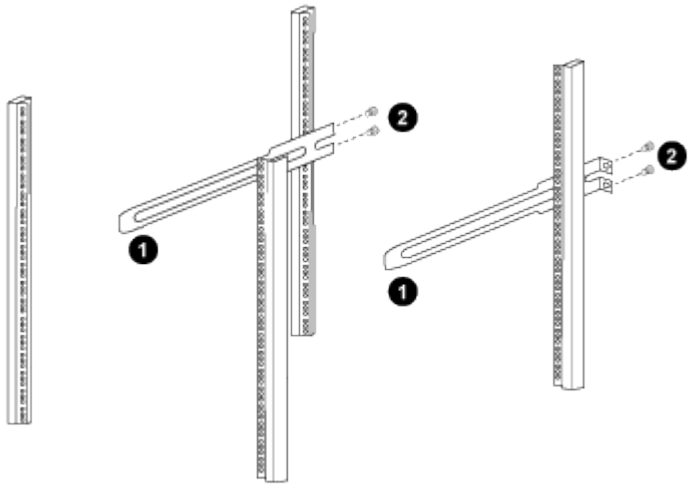
   b. Wiederholen Sie Schritt 2a mit der anderen vorderen Rackmontagehalterung auf der anderen Seite des Switches.
   c. Installieren Sie die hintere Rackmontagehalterung am Switch-Gehäuse.
   d. Wiederholen Sie Schritt 2c mit der anderen hinteren Rackmontagehalterung auf der anderen Seite des Switches.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



Die beiden 92300YC-Switches werden immer in den oberen 2 HE der Schränke 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.

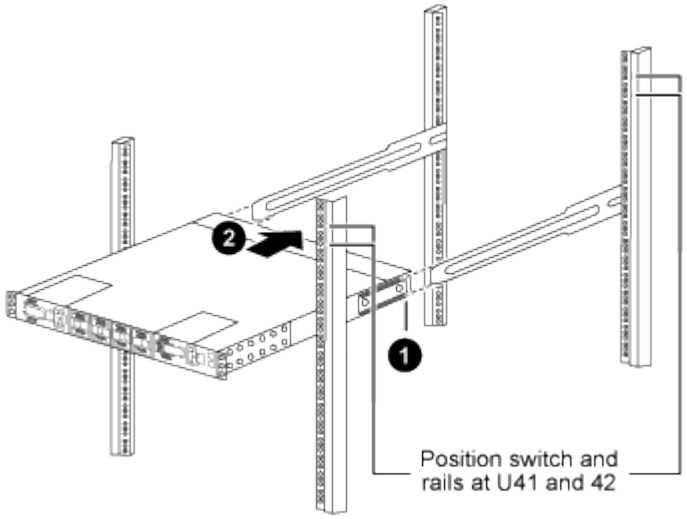
a. Wiederholen Sie Schritt 4a für den rechten hinteren Pfosten.

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.

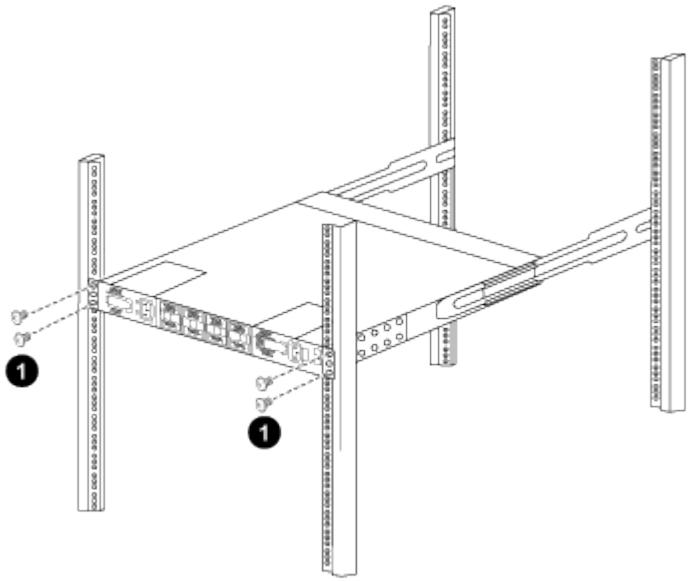
a. Positionieren Sie die Rückseite des Schalters an der RU41-Schiene.



(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 Verwaltungsport an jedem 92300YC-Switch mit einem der Verwaltungsswitches (falls bestellt) oder verbinden Sie sie direkt mit Ihrem Verwaltungsnetzwerk.

   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 den Switch" Die

Überprüfung der Verkabelung und Konfigurationsüberlegungen

Bevor Sie Ihren Cisco 92300YC Switch konfigurieren, beachten Sie bitte die folgenden Hinweise.

Unterstützung für NVIDIA CX6-, CX6-DX- und CX7-Ethernet-Anschlüsse

Wenn Sie einen Switch-Port mit einem ONTAP Controller über NVIDIA ConnectX-6 (CX6), ConnectX-6 Dx (CX6-DX) oder ConnectX-7 (CX7) NIC-Ports verbinden, müssen Sie die Geschwindigkeit des Switch-Ports fest codieren.

```
(cs1)(config)# interface Ethernet1/19
For 100GbE speed:
(cs1)(config-if)# speed 100000
For 40GbE speed:
(cs1)(config-if)# speed 40000
(cs1)(config-if)# no negotiate auto
(cs1)(config-if)# exit
(cs1)(config)# exit
Save the changes:
(cs1)# copy running-config startup-config
```

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

Konfigurieren der Software

Workflow zur Softwareinstallation für Cisco Nexus 92300YC-Cluster-Switches

Um die Software für einen Cisco Nexus 92300YC-Switch zu installieren und zu konfigurieren und die Referenzkonfigurationsdatei (RCF) zu installieren oder zu aktualisieren, gehen Sie wie folgt vor:

"Konfigurieren Sie den Schalter"

Konfigurieren Sie den Cluster-Switch 92300YC.

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

Die Cisco NX-OS-Software und Referenzkonfigurationsdateien (RCFs) müssen auf Cisco 92300YC-Cluster-Switches installiert werden.

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

Laden Sie die NX-OS-Software herunter und installieren oder aktualisieren Sie sie auf dem Cisco 392300YC-Cluster-Switch.

"Installieren Sie den RCF"

Installieren Sie das RCF, nachdem Sie den Cisco 92300YC-Switch zum ersten Mal eingerichtet haben.

"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.

Konfigurieren Sie den Cisco Nexus 92300YC-Switch

Gehen Sie wie folgt vor, um den Cisco Nexus 92300YC Switch einzurichten und zu konfigurieren.

Schritte

1. Verbinden Sie den seriellen Port mit einem Host oder einem seriellen Port.
2. Verbinden Sie den Management-Port (auf der Nicht-Port-Seite des Switches) mit demselben Netzwerk, in dem sich Ihr SFTP-Server befindet.
3. Nehmen Sie an der Konsole die seriellen Einstellungen auf dem Host vor:
    - 9600 Baud

- 8 Datenbits
- 1 Stoppbit
- Parität: keine
- Flusssteuerung: keine

4. Beim erstmaligen Hochfahren oder beim Neustart nach dem Löschen der laufenden Konfiguration gerät der Switch Nexus 92300YC in eine Boot-Schleife. Unterbrechen Sie diesen Vorgang, indem Sie **ja** eingeben, um die automatische Stromversorgung abzubrechen.

   Die Einrichtung des Systemadministratorkontos wird angezeigt.

   Beispiel anzeigen

   ```
   $ VDC-1 %$ %POAP-2-POAP_INFO:   - Abort Power On Auto Provisioning
   [yes - continue with normal setup, skip - bypass password and basic
   configuration, no - continue with Power On Auto Provisioning]
   (yes/skip/no)[no]: y
   Disabling POAP.......Disabling POAP
   2019 Apr 10 00:36:17 switch %$ VDC-1 %$ poap: Rolling back, please
   wait... (This may take 5-15 minutes)

             ---- System Admin Account Setup ----

   Do you want to enforce secure password standard (yes/no) [y]:
   ```

5. Geben Sie **y** ein, um den sicheren Passwortstandard zu erzwingen:

   ```
   Do you want to enforce secure password standard (yes/no) [y]: y
   ```

6. Geben Sie das Passwort für den Benutzer „admin“ ein und bestätigen Sie es:

   ```
   Enter the password for "admin":
   Confirm the password for "admin":
   ```

7. Geben Sie **ja** ein, um den Dialog „Systemgrundkonfiguration“ aufzurufen.

Beispiel anzeigen

```
This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus9000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus9000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no):
```

8. Erstellen Sie ein weiteres Benutzerkonto:

```
Create another login account (yes/no) [n]:
```

9. Konfigurieren von schreibgeschützten und Lese-/Schreib-SNMP-Community-Strings:

```
Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:
```

10. Konfigurieren Sie den Cluster-Switch-Namen:

```
Enter the switch name : cs2
```

11. Konfigurieren Sie die Out-of-Band-Managementschnittstelle:

```
Continue with Out-of-band (mgmt0) management configuration? (yes/no)
[y]: y

Mgmt0 IPv4 address : 172.22.133.216

Mgmt0 IPv4 netmask : 255.255.224.0

Configure the default gateway? (yes/no) [y]: y

IPv4 address of the default gateway : 172.22.128.1
```

12. Erweiterte IP-Optionen konfigurieren:

```
Configure advanced IP options? (yes/no) [n]: n
```

13. Telnet-Dienste konfigurieren:

```
Enable the telnet service? (yes/no) [n]: n
```

14. Konfigurieren von SSH-Diensten und SSH-Schlüsseln:

```
Enable the ssh service? (yes/no) [y]: y

       Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa

       Number of rsa key bits <1024-2048> [1024]: 2048
```

15. Konfigurieren Sie weitere Einstellungen:

```
Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L2]: L2

  Configure default switchport interface state (shut/noshut) [noshut]:
noshut

  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]: strict
```

16. Schalterinformationen bestätigen und Konfiguration speichern:

```
Would you like to edit the configuration? (yes/no) [n]: n

Use this configuration and save it? (yes/no) [y]: y

[] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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 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.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- Geeignete Software und Upgrade-Anleitungen sind erhältlich bei "Cisco Nexus 9000 Series Switches" Die

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.

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 `node1` Und `node2` Die
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.
- 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. Die Befehlsausgaben können je nach ONTAP Version variieren.

Schritte

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

   ```
   set -privilege advanced
   ```

Die erweiterte Aufforderung(`*>`) erscheint.

2. 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 ist.

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

   Der folgende Befehl unterdrückt die automatische Fallerstellung für zwei Stunden:

   ```
   cluster1:> **system node autosupport invoke -node * -type all -message
   MAINT=2h**
   ```

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
   ----------- ------ ------------------------- ----------------
   ----------------
   node2      /cdp
               e0a    cs1                       Eth1/2            N9K-
   C92300YC
               e0b    cs2                       Eth1/2            N9K-
   C92300YC
   node1      /cdp
               e0a    cs1                       Eth1/1            N9K-
   C92300YC
               e0b    cs2                       Eth1/1            N9K-
   C92300YC

   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: node2
                                                  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: node1
                                                  Speed(Mbps)
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
--------- ------------ ---------------- ---- ---- -----------
--------
e0a       Cluster      Cluster          up   9000  auto/10000
healthy
e0b       Cluster      Cluster          up   9000  auto/10000
healthy

4 entries were displayed.
```

b. 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
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1     e0a
Cluster node1_clus2 169.254.49.125 node1     e0b
Cluster node2_clus1 169.254.47.194 node2     e0a
Cluster node2_clus2 169.254.19.183 node2     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
          node1_clus1   true
          node1_clus2   true
          node2_clus1   true
          node2_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 Sie die NX-OS-Software"Die

Installieren Sie die NX-OS-Software

Gehen Sie wie folgt vor, um die NX-OS-Software auf dem Switch Nexus 92300YC zu installieren.

NX-OS ist ein Netzwerkbetriebssystem für die Nexus-Serie von Ethernet-Switches und die MDS-Serie von Fibre Channel (FC) Storage Area Network Switches von Cisco Systems.

Überprüfungsanforderungen

Unterstützte Ports und Knotenverbindungen

- Die für die Nexus 92300YC Switches unterstützten Inter-Switch Links (ISLs) sind die Ports 1/65 und 1/66.
- Die für die Nexus 92300YC Switches unterstützten Knotenverbindungen sind die Ports 1/1 bis 1/66.

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Die passende NetApp Cisco NX-OS-Software für Ihre Switches finden Sie auf der NetApp Support-Website. "mysupport.netapp.com"
- Ein voll funktionsfähiger Cluster (keine Fehler in den Protokollen oder ähnliche Probleme).
- "Cisco Ethernet-Switch-Seite". In der Switch-Kompatibilitätstabelle finden Sie die unterstützten ONTAP und NX-OS-Versionen.

Installieren Sie die Software

Die Beispiele in diesem Verfahren verwenden zwei Knoten, aber ein Cluster kann bis zu 24 Knoten umfassen.

Zu den Beispielen

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

- Die Bezeichnungen der Nexus 92300YC-Switches lauten: `cs1` Und `cs2` Die
- Das in diesem Verfahren verwendete Beispiel startet das Upgrade auf dem zweiten Switch, **cs2*.*
- Die Cluster-LIF-Namen sind `node1_clus1` Und `node1_clus2` für Knoten1 und `node2_clus1` Und `node2_clus2` für Knoten 2.
- Der IPspace-Name lautet: `Cluster` Die
- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.
- Die Cluster-Ports auf jedem Knoten sind benannt `e0a` Und `e0b` Die

  Siehe die"Hardware-Universum^_" für die tatsächlich von Ihrer Plattform unterstützten Cluster-Ports. Sehen "Welche zusätzlichen Informationen benötige ich für die Installation meiner Geräte, die nicht in HWU enthalten sind?" Weitere Informationen zu den Installationsanforderungen des Schalters finden Sie hier.

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. Kopieren Sie die NX-OS-Software und die EPLD-Images auf den Nexus 92300YC-Switch.

Beispiel anzeigen

```
cs2# copy sftp: bootflash: vrf management
Enter source filename: /code/nxos.9.2.2.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.9.2.2.bin  /bootflash/nxos.9.2.2.bin
/code/nxos.9.2.2.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.9.2.2.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.9.2.2.img  /bootflash/n9000-
epld.9.2.2.img
/code/n9000-epld.9.2.2.img  100%  161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

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

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, 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 05.31
  NXOS: version 9.2(1)
  BIOS compile time:  05/17/2018
  NXOS image file is: bootflash:///nxos.9.2.1.bin
  NXOS compile time:  7/17/2018 16:00:00 [07/18/2018 00:21:19]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
Kernel uptime is 0 day(s), 4 hour(s), 23 minute(s), 11 second(s)

Last reset at 271444 usecs after Wed Apr 10 00:25:32 2019
  Reason: Reset Requested by CLI command reload
```

```
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):

cs2#
```

5. 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.9.2.2.bin

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

Verifying image bootflash:/nxos.9.2.2.bin for boot variable "nxos".
[] 100% -- SUCCESS

Verifying image type.
[] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.2.2.bin.
[] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.2.2.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                                   9.2(1)
9.2(2)         yes
  1       bios    v05.31(05/17/2018):v05.28(01/18/2018)
v05.33(09/08/2018)       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
2019 Apr 10 04:59:35 cs2 %$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE:
Successfully deactivated virtual service 'guestshell+'

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

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

   ```
   show version
   ```

Beispiel anzeigen

```
cs2# show version

Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2018, 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 9.2(2)
  BIOS compile time:  09/08/2018
  NXOS image file is: bootflash:///nxos.9.2.2.bin
  NXOS compile time:  11/4/2018 21:00:00 [11/05/2018 06:11:06]


Hardware
  cisco Nexus9000 C92300YC Chassis
  Intel(R) Xeon(R) CPU D-1526 @ 1.80GHz with 16337884 kB of memory.
  Processor Board ID FDO220329V5

  Device name: cs2
  bootflash:  115805356 kB
  Kernel uptime is 0 day(s), 0 hour(s), 3 minute(s), 52 second(s)

Last reset at 182004 usecs after Wed Apr 10 04:59:48 2019
```

```
  Reason: Reset due to upgrade
  System version: 9.2(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin

Active Package(s):
```

7. 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.9.2.2.img module 1
Compatibility check:
Module        Type         Upgradable        Impact   Reason
------  -----------------  ----------    ----------   ------
     1            SUP           Yes       disruptive  Module
Upgradable

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

```
     1          SUP          Success


EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. 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
```

Wie geht es weiter?

Nach der Installation der NX-OS-Software können Sie "Installieren Sie die Referenzkonfigurationsdatei"Die

Installieren Sie die Referenzkonfigurationsdatei (RCF).

Sie können die RCF-Datei installieren, nachdem Sie den Switch Nexus 92300YC zum ersten Mal eingerichtet haben. Sie können dieses Verfahren auch verwenden, um Ihre RCF-Version zu aktualisieren.

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.

Informationen zu diesem Vorgang

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 `node1` Und `node2` Die
- Die Cluster-LIF-Namen sind `node1_clus1` , `node1_clus2` , `node2_clus1` , Und `node2_clus2` Die

- Der `cluster1::*>` Die Eingabeaufforderung zeigt den Namen des Clusters an.

- Das Verfahren erfordert die Verwendung sowohl von ONTAP -Befehlen als auch von "Cisco Nexus 9000 Series Switches" Sofern nicht anders angegeben, werden ONTAP -Befehle verwendet.
- Bevor Sie diese Prozedur durchführen, stellen Sie sicher, dass Sie über eine aktuelle Sicherungskopie der Switch-Konfiguration verfügen.
- 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.

Schritte

1. 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
----------- ------ ------------------------- ----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1/1     N9K-
C92300YC
            e0b    cs2                       Ethernet1/1/1     N9K-
C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/1/2     N9K-
C92300YC
            e0b    cs2                       Ethernet1/1/2     N9K-
C92300YC
cluster1::*>
```

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

   a. Überprüfen Sie, ob alle Cluster-Ports aktiv und fehlerfrei sind: `network port show -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
healthy false

Node: node2

Ignore
                                                  Speed(Mbps)
Health   Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status   Status
--------- ------------ ---------------- ---- ---- -----------
-------- ------
e0c       Cluster      Cluster          up   9000  auto/100000
healthy false
e0d       Cluster      Cluster          up   9000  auto/100000
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
            node1_clus1        up/up      169.254.3.4/23    node1
e0c     true
            node1_clus2        up/up      169.254.3.5/23    node1
e0d     true
            node2_clus1        up/up      169.254.3.8/23    node2
e0c     true
            node2_clus2        up/up      169.254.3.9/23    node2
e0d     true
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    10.233.205.92
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.93
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      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.
```

3. Automatische Wiederherstellung der Cluster-LIFs deaktivieren.

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

4. Schalten Sie auf dem Cluster-Switch cs2 die Ports ab, die mit den Cluster-Ports der Knoten verbunden sind.

```
cs2(config)# interface e1/1-64
cs2(config-if-range)# shutdown
```

5. Überprüfen Sie, ob die Cluster-Ports auf die Ports migriert wurden, die auf dem Cluster-Switch cs1 gehostet werden. Dies kann einige Sekunden dauern. `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
            node1_clus1       up/up      169.254.3.4/23     node1
e0c     true
            node1_clus2       up/up      169.254.3.5/23     node1
e0c     false
            node2_clus1       up/up      169.254.3.8/23     node2
e0c     true
            node2_clus2       up/up      169.254.3.9/23     node2
e0c     false
cluster1::*>
```

6. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert: `cluster show`

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node           Health  Eligibility   Epsilon
-------------- ------- ------------  -------
node1          true    true          false
node2          true    true          false
cluster1::*>
```

7. 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`

8. Bereinigen Sie die Konfiguration auf Switch CS2 und führen Sie eine grundlegende Einrichtung durch.

Beim Aktualisieren oder Anwenden eines neuen RCF müssen Sie die Schaltereinstellungen löschen und eine grundlegende Konfiguration durchführen. Sie müssen mit dem seriellen Konsolenport des Switches verbunden sein, um den Switch erneut einzurichten.

a. Konfiguration bereinigen:

Beispiel anzeigen

```
(cs2)# write erase

Warning: This command will erase the startup-configuration.

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

b. Führen Sie einen Neustart des Switches durch:

Beispiel anzeigen

```
(cs2)# reload

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

9. 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 9000 Series Switches" Führer.

   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: /code/Nexus_92300YC_RCF_v1.0.2.txt
Enter hostname for the tftp 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:
tftp> progress
Progress meter enabled
tftp> get /code/Nexus_92300YC_RCF_v1.0.2.txt /bootflash/nxos.9.2.2.bin
/code/Nexus_92300YC_R  100% 9687   530.2KB/s   00:00
tftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

10. 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

Series Switches" Führer.

Dieses Beispiel zeigt die RCF-Datei. `Nexus_92300YC_RCF_v1.0.2.txt` wird auf Switch CS2 installiert:

```
cs2# copy Nexus_92300YC_RCF_v1.0.2.txt running-config echo-commands

Disabling ssh: as its enabled right now:
 generating ecdsa key(521 bits).....
generated ecdsa key

Enabling ssh: as it has been disabled
 this command enables edge port type (portfast) by default on all
interfaces. You
 should now disable edge port type (portfast) explicitly on switched
ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.

Edge port type (portfast) should only be enabled on ports connected to a
single
 host. Connecting hubs, concentrators, switches, bridges, etc...  to
this
 interface when edge port type (portfast) is enabled, can cause
temporary bridging loops.
 Use with CAUTION

Edge Port Type (Portfast) has been configured on Ethernet1/1 but will
only
 have effect when the interface is in a non-trunking mode.

...

Copy complete, now saving to disk (please wait)...
Copy complete.
```

11. Überprüfen Sie auf dem Switch, ob die RCF-Datei erfolgreich zusammengeführt wurde:

    `show running-config`

```
cs2# show running-config
!Command: show running-config
!Running configuration last done at: Wed Apr 10 06:32:27 2019
!Time: Wed Apr 10 06:36:00 2019

version 9.2(2) Bios:version 05.33
switchname cs2
vdc cs2 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 511
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

feature lacp

no password strength-check
username admin password 5
$5$HY9Kk3F9$YdCZ8iQJ1RtoiEFa0sKP5IO/LNG1k9C4lSJfi5kesl
6  role network-admin
ssh key ecdsa 521

banner motd #

*
*
*  Nexus 92300YC Reference Configuration File (RCF) v1.0.2 (10-19-2018)
*
*
*
*  Ports 1/1  - 1/48: 10GbE Intra-Cluster Node Ports
*
*  Ports 1/49 - 1/64: 40/100GbE Intra-Cluster Node Ports
*
*  Ports 1/65 - 1/66: 40/100GbE Intra-Cluster ISL Ports
*
*
*
```

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

1. Überprüfen Sie, ob die RCF-Datei die richtige neuere Version ist: `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.

2. Wenden Sie alle zuvor vorgenommenen Anpassungen auf die Switch-Konfiguration erneut an. Siehe"Überprüfung der Verkabelung und Konfigurationsüberlegungen" Einzelheiten zu etwaigen weiteren erforderlichen Änderungen.
3. Nachdem Sie überprüft haben, ob die RCF-Versionen und die Schaltereinstellungen korrekt sind, kopieren Sie die Running-Config-Datei in die Startup-Config-Datei.

   Weitere Informationen zu Cisco -Befehlen finden Sie im entsprechenden Handbuch im "Cisco Nexus 9000 Series Switches" Führer.

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

4. Neustart des Switches CS2. Sie können die auf den Knoten gemeldeten Ereignisse vom Typ „Cluster-Ports ausgefallen“ ignorieren, während der Switch neu startet.

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

5. 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 -ipspace Cluster`

Beispiel anzeigen

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

Node: node1

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

Node: node2

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

b. Überprüfen Sie den Zustand des Switches vom Cluster aus (dabei wird möglicherweise der Switch cs2 nicht angezeigt, da LIFs nicht auf e0d liegen).

Beispiel anzeigen

```
cluster1::*> *network device-discovery show -protocol cdp*
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- -----------------
------------
node1/cdp
            e0a    cs1                       Ethernet1/1
N9K-C92300YC
            e0b    cs2                       Ethernet1/1
N9K-C92300YC
node2/cdp
            e0a    cs1                       Ethernet1/2
N9K-C92300YC
            e0b    cs2                       Ethernet1/2
N9K-C92300YC

cluster1::*> *system cluster-switch show -is-monitoring-enabled
-operational true*
Switch                      Type               Address
Model
--------------------------- ------------------ ----------------
------------
cs1                         cluster-network    10.233.205.90
N9K-C92300YC
     Serial Number: FOXXXXXXXGD
      Is Monitored: true
            Reason: None
  Software Version: Cisco Nexus Operating System (NX-OS)
Software, Version
                    9.3(4)
    Version Source: CDP

cs2                         cluster-network    10.233.205.91
N9K-C92300YC
     Serial Number: FOXXXXXXXGS
      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.
```

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.
```

6. Schalten Sie auf dem Cluster-Switch cs1 die Ports ab, die mit den Cluster-Ports der Knoten verbunden sind.

   Das folgende Beispiel verwendet die Ausgabe des Schnittstellenbeispiels aus Schritt 1:

```
cs1(config)# interface e1/1-64
cs1(config-if-range)# shutdown
```

7. Überprüfen Sie, ob die Cluster-LIFs auf die Ports migriert wurden, die auf Switch cs2 gehostet werden. Dies kann einige Sekunden dauern. `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
            node1_clus1      up/up      169.254.3.4/23     node1
e0d     false
            node1_clus2      up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1      up/up      169.254.3.8/23     node2
e0d     false
            node2_clus2      up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

8. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert: `cluster show`

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node           Health   Eligibility   Epsilon
-------------- -------- ------------- -------
node1          true     true          false
node2          true     true          false
cluster1::*>
```

9. Wiederholen Sie die Schritte 7 bis 14 auf Switch cs1.
10. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

11. Neustart des Switches cs1. Dadurch werden die Cluster-LIFs veranlasst, zu ihren ursprünglichen Ports zurückzukehren. Sie können die auf den Knoten gemeldeten Ereignisse vom Typ „Cluster-Ports ausgefallen“ ignorieren, während der Switch neu startet.

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

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

```
cs1# show interface brief | grep up
.
.
Ethernet1/1      1       eth  access up      none
10G(D) --
Ethernet1/2      1       eth  access up      none
10G(D) --
Ethernet1/3      1       eth  trunk  up      none
100G(D) --
Ethernet1/4      1       eth  trunk  up      none
100G(D) --
.
.
```

13. 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      Eth1/65(P)   Eth1/66(P)
cs1#
```

14. 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
            node1_clus1   up/up      169.254.3.4/23     node1
e0d     true
            node1_clus2   up/up      169.254.3.5/23     node1
e0d     true
            node2_clus1   up/up      169.254.3.8/23     node2
e0d     true
            node2_clus2   up/up      169.254.3.9/23     node2
e0d     true
cluster1::*>
```

15. Überprüfen Sie, ob der Cluster fehlerfrei funktioniert: `cluster show`

Beispiel anzeigen

```
cluster1::*> *cluster show*
Node            Health  Eligibility   Epsilon
--------------- ------- ------------- -------
node1           true    true          false
node2           true    true          false
```

16. 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.3.4 node1 e0a
Cluster node1_clus2 169.254.3.5 node1 e0b
Cluster node2_clus1 169.254.3.8 node2 e0a
Cluster node2_clus2 169.254.3.9 node2 e0b
Local = 169.254.1.3 169.254.1.1
Remote = 169.254.1.6 169.254.1.7 169.254.3.4 169.254.3.5 169.254.3.8
169.254.3.9
Cluster Vserver Id = 4294967293
Ping status:
............
Basic connectivity succeeds on 12 path(s)
Basic connectivity fails on 0 path(s)
................................................
Detected 9000 byte MTU on 12 path(s):
    Local 169.254.1.3 to Remote 169.254.1.6
    Local 169.254.1.3 to Remote 169.254.1.7
    Local 169.254.1.3 to Remote 169.254.3.4
    Local 169.254.1.3 to Remote 169.254.3.5
    Local 169.254.1.3 to Remote 169.254.3.8
    Local 169.254.1.3 to Remote 169.254.3.9
    Local 169.254.1.1 to Remote 169.254.1.6
    Local 169.254.1.1 to Remote 169.254.1.7
    Local 169.254.1.1 to Remote 169.254.3.4
    Local 169.254.1.1 to Remote 169.254.3.5
    Local 169.254.1.1 to Remote 169.254.3.8
    Local 169.254.1.1 to Remote 169.254.3.9
Larger than PMTU communication succeeds on 12 path(s)
RPC status:
6 paths up, 0 paths down (tcp check)
6 paths up, 0 paths down (udp check)
```

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

Schalter migrieren

Migrieren Sie zu einem Zwei-Knoten-Switch-Cluster mit einem Cisco Nexus 92300YC-Switch

Wenn Sie bereits eine *switchlose* Clusterumgebung mit zwei Knoten besitzen, können Sie mithilfe von Cisco Nexus 92300YC Switches zu einer *switched* Clusterumgebung mit zwei Knoten migrieren, um die Anzahl der Knoten im Cluster auf mehr als zwei zu erhöhen.

Die Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerkanschlüsse oder an jedem Controller einen einzelnen Clusteranschluss haben. Der dokumentierte Prozess funktioniert für alle Knoten, die optische oder Twinax-Anschlüsse verwenden, wird jedoch von diesem Switch nicht unterstützt, wenn die Knoten Onboard-10Gb BASE-T RJ45-Anschlüsse für die Cluster-Netzwerkanschlüsse verwenden.

Die meisten Systeme benötigen zwei dedizierte Cluster-Netzwerkanschlüsse an jedem Controller.

Nach Abschluss der Migration müssen Sie möglicherweise die erforderliche Konfigurationsdatei installieren, um den Cluster Switch Health Monitor (CSHM) für 92300YC Cluster-Switches zu unterstützen. Sehen"Switch-Zustandsüberwachung (CSHM)" .

Überprüfungsanforderungen

Bevor Sie beginnen

Bitte stellen Sie sicher, dass Sie Folgendes haben:

Bei einer schalterlosen Konfiguration mit zwei Knoten ist Folgendes sicherzustellen:

- Die Zwei-Knoten-Konfiguration ohne Schalter ist ordnungsgemäß eingerichtet und funktioniert.
- Auf den Knoten läuft ONTAP 9.6 oder höher.
- Alle Cluster-Ports befinden sich im Status **up**.
- Alle logischen Schnittstellen (LIFs) des Clusters befinden sich im Status **up** und sind an ihren jeweiligen Ports angeschlossen.

Für die Konfiguration des Cisco Nexus 92300YC Switches:

- Beide Switches verfügen über eine Management-Netzwerkanbindung.
- Es besteht Konsolenzugriff auf die Cluster-Switches.
- Die Knoten-zu-Knoten- und Schalter-zu-Schalter-Verbindungen des Nexus 92300YC verwenden Twinax- oder Glasfaserkabel.

"Hardware Universe – Schalter"enthält weitere Informationen zur Verkabelung.

- Inter-Switch Link (ISL)-Kabel sind an die Ports 1/65 und 1/66 beider 92300YC-Switches angeschlossen.
- Die erste Anpassung beider 92300YC-Switches ist abgeschlossen. Damit die:
  - Auf den 92300YC-Switches läuft die neueste Softwareversion.
  - Referenzkonfigurationsdateien (RCFs) werden auf die Switches angewendet. Jegliche standortspezifische Anpassung, wie z. B. SMTP, SNMP und SSH, wird auf den neuen Switches konfiguriert.

Den Schalter migrieren

Zu den Beispielen

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

- Die Bezeichnungen der 92300YC-Switches lauten cs1 und cs2.
- Die Namen der Cluster-SVMs lauten node1 und node2.
- Die Namen der LIFs lauten 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 Cluster-Ports sind e0a und e0b.

  "Hardware Universe"Enthält die aktuellsten Informationen zu den tatsächlichen Cluster-Ports für Ihre Plattformen.

Schritt 1: Vorbereitung auf die Migration

1. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung(`*>`) erscheint.

2. 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 ist.

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

Beispiel anzeigen

Der folgende Befehl unterdrückt die automatische Fallerstellung für zwei Stunden:

```
cluster1::*> system node autosupport invoke -node * -type all
-message MAINT=2h
```

Schritt 2: Kabel und Anschlüsse konfigurieren

1. Deaktivieren Sie alle zum Knoten führenden Ports (außer ISL-Ports) an den beiden neuen Cluster-Switches cs1 und cs2.

   Die ISL-Ports dürfen nicht deaktiviert werden.

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass die dem Knoten zugewandten Ports 1 bis 64 am Switch cs1 deaktiviert sind:

   ```
   cs1# config
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e/1-64
   cs1(config-if-range)# shutdown
   ```

2. Überprüfen Sie, ob die ISL und die physischen Ports der ISL zwischen den beiden 92300YC-Switches cs1 und cs2 an den Ports 1/65 und 1/66 aktiv sind:

   ```
   show port-channel summary
   ```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die ISL-Ports am Switch cs1 aktiv sind:

```
cs1# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

+ Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch cs2 aktiv sind:

+

```
(cs2)# show port-channel summary

Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)
```

3. Liste der benachbarten Geräte anzeigen:

   ```
   show cdp neighbors
   ```

   Dieser Befehl liefert Informationen über die mit dem System verbundenen Geräte.

Beispiel anzeigen

Das folgende Beispiel listet die benachbarten Geräte am Switch cs1 auf:

```
cs1# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

+ Das folgende Beispiel listet die benachbarten Geräte am Switch cs2 auf:

+

```
cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
cs1(FDO220329KU)    Eth1/65        177    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)    Eth1/66        177    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 2
```

4. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Jeder Port sollte angezeigt werden für `Link` und gesund für `Health Status` Die

Beispiel anzeigen

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

Node: node1

                                                  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: node2

                                                  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.
```

5. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind:

   `network interface show -vserver Cluster`

   Jeder Cluster-LIF sollte „true“ anzeigen für `Is Home` und haben `Status Admin/Oper` von oben/aufwärts

Beispiel anzeigen

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

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- -----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true
4 entries were displayed.
```

6. Automatische Wiederherstellung auf allen Cluster-LIFs deaktivieren:

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

   Beispiel anzeigen

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

          Logical
Vserver   Interface     auto-revert
--------- ------------- ------------
Cluster
          node1_clus1   false
          node1_clus2   false
          node2_clus1   false
          node2_clus2   false

4 entries were displayed.
```

7. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 1 und verbinden Sie dann e0a mit Port 1 auf dem Cluster-Switch cs1. Verwenden Sie dazu die von den 92300YC-Switches unterstützten geeigneten Kabel.

Der "*Hardware Universe - Schalter*" enthält weitere Informationen zur Verkabelung.

8. Trennen Sie das Kabel vom Cluster-Port e0a auf Knoten 2 und verbinden Sie dann e0a mit Port 2 auf Cluster-Switch cs1. Verwenden Sie dazu die von den 92300YC-Switches unterstützten Kabel.
9. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs1.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/64 am Switch cs1 aktiviert sind:

```
cs1# config
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# interface e1/1-64
cs1(config-if-range)# no shutdown
```

10. Überprüfen Sie, ob alle Cluster-LIFs aktiv und betriebsbereit sind und als „true“ angezeigt werden. `Is Home` :

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf Knoten 1 und Knoten 2 aktiv sind und dass `Is Home` Die Ergebnisse sind korrekt:

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

         Logical      Status     Network            Current
Current Is
Vserver  Interface    Admin/Oper Address/Mask       Node         Port
Home
-------- ------------ ---------- ------------------ -----------
------- ----
Cluster
         node1_clus1  up/up      169.254.209.69/16  node1        e0a
true
         node1_clus2  up/up      169.254.49.125/16  node1        e0b
true
         node2_clus1  up/up      169.254.47.194/16  node2        e0a
true
         node2_clus2  up/up      169.254.19.183/16  node2        e0b
true

4 entries were displayed.
```

11. Informationen über den Status der Knoten im Cluster anzeigen:

    ```
    cluster show
    ```

    Beispiel anzeigen

    Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster an:

    ```
    cluster1::*> cluster show

    Node                 Health  Eligibility   Epsilon
    -------------------- ------- ------------  ------------
    node1                true    true          false
    node2                true    true          false

    2 entries were displayed.
    ```

12. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 1 und verbinden Sie dann e0b mit Port 1 auf Cluster-Switch cs2. Verwenden Sie dazu die von den 92300YC-Switches unterstützten geeigneten Kabel.
13. Trennen Sie das Kabel vom Cluster-Port e0b auf Knoten 2 und verbinden Sie dann e0b mit Port 2 des Cluster-Switches cs2 unter Verwendung der von den 92300YC-Switches unterstützten geeigneten Verkabelung.
14. Aktivieren Sie alle zum Knoten hin ausgerichteten Ports am Cluster-Switch cs2.

    Beispiel anzeigen

    Das folgende Beispiel zeigt, dass die Ports 1/1 bis 1/64 am Switch cs2 aktiviert sind:

    ```
    cs2# config
    Enter configuration commands, one per line. End with CNTL/Z.
    cs2(config)# interface e1/1-64
    cs2(config-if-range)# no shutdown
    ```

Schritt 3: Konfiguration überprüfen

1. Automatische Wiederherstellung der Cluster-LIFs aktivieren.

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

2. Überprüfen Sie, ob alle Cluster-Ports aktiv sind:

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

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle Cluster-Ports auf Knoten 1 und Knoten 2 aktiv sind:

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

3. Überprüfen Sie, ob alle Schnittstellen den Wert „true“ anzeigen. `Is Home` :

   `network interface show -vserver Cluster`

   Dieser Vorgang kann mehrere Minuten dauern.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf Knoten 1 und Knoten 2 aktiv sind und dass `Is Home` Die Ergebnisse sind korrekt:

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

          Logical      Status     Network            Current
Current Is
Vserver   Interface    Admin/Oper Address/Mask       Node       Port
Home
--------- ------------ ---------- ------------------ ----------
------- ----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1      e0a
true
          node1_clus2  up/up      169.254.49.125/16  node1      e0b
true
          node2_clus1  up/up      169.254.47.194/16  node2      e0a
true
          node2_clus2  up/up      169.254.19.183/16  node2      e0b
true

4 entries were displayed.
```

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

   `show cdp neighbors`

Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter:

```
(cs1)# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0a
node2               Eth1/2         133    H         FAS2980
e0a
cs2(FDO220329V5)    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs2(FDO220329V5)    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4


(cs2)# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1               Eth1/1         133    H         FAS2980
e0b
node2               Eth1/2         133    H         FAS2980
e0b
cs1(FDO220329KU)
                    Eth1/65        175    R S I s   N9K-C92300YC
Eth1/65
cs1(FDO220329KU)
                    Eth1/66        175    R S I s   N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

5. Informationen zu den in Ihrem Cluster gefundenen Netzwerkgeräten anzeigen:

   `network device-discovery show -protocol cdp`

   Beispiel anzeigen

```
cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    cs2                       0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    cs2                       0/1               N9K-
C92300YC

4 entries were displayed.
```

6. Überprüfen Sie, ob die Einstellungen deaktiviert sind:

   `network options switchless-cluster show`

   Die Ausführung des Befehls kann mehrere Minuten dauern. Warten Sie auf die Ansage „Noch 3 Minuten bis zum Ablauf der Gültigkeitsdauer“.

   Beispiel anzeigen

   Die falsche Ausgabe im folgenden Beispiel zeigt, dass die Konfigurationseinstellungen deaktiviert sind:

```
cluster1::*> network options switchless-cluster show
Enable Switchless Cluster: false
```

7. Überprüfen Sie den Status der Knoten im Cluster:

   `cluster show`

Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Zustand und die Eignung der Knoten im Cluster:

```
cluster1::*> cluster show

Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  --------
node1                true    true          false
node2                true    true          false
```

8. 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Falls Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

   Beispiel anzeigen

   ```
   cluster1::*> system node autosupport invoke -node * -type all
   -message MAINT=END
   ```

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```

Wie geht es weiter?

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

Schalter austauschen

Ersetzen Sie einen Cisco Nexus 92300YC-Switch

Der Austausch eines defekten Nexus 92300YC-Switches in einem Clusternetzwerk ist ein nicht-unterbrechendes Verfahren (NDU).

Überprüfungsanforderungen

Bevor Sie beginnen

Vor dem Austausch des Schalters stellen Sie bitte Folgendes sicher:

- In der bestehenden Cluster- und Netzwerkinfrastruktur:
  - Der bestehende Cluster wurde als voll funktionsfähig verifiziert, wobei mindestens ein Cluster-Switch vollständig angeschlossen ist.
  - Alle Cluster-Ports sind aktiv.
  - Alle logischen Schnittstellen (LIFs) des Clusters sind aktiv und an ihren jeweiligen Ports angeschlossen.
  - Der Befehl ONTAP cluster ping-cluster -node node1 muss anzeigen, dass die grundlegende Konnektivität und die Kommunikation größer als PMTU auf allen Pfaden erfolgreich sind.
- Für den Ersatzschalter Nexus 92300YC:
  - Die Management-Netzwerkanbindung des Ersatz-Switches ist funktionsfähig.
  - Der Konsolenzugriff auf den Ersatzschalter ist eingerichtet.
  - Die Knotenverbindungen sind die Ports 1/1 bis 1/64.
  - Alle Inter-Switch Link (ISL)-Ports sind an den Ports 1/65 und 1/66 deaktiviert.
  - Die gewünschte Referenzkonfigurationsdatei (RCF) und das NX-OS-Betriebssystem-Image werden auf den Switch geladen.
  - Die erste Anpassung des Schalters ist abgeschlossen, wie in der folgenden Beschreibung detailliert aufgeführt:"Konfigurieren Sie den Cisco Nexus 92300YC-Switch" Die

    Alle zuvor vorgenommenen Anpassungen am Standort, wie z. B. STP, SNMP und SSH, werden auf den neuen Switch kopiert.

Konsolenprotokollierung aktivieren

NetApp empfiehlt dringend, die Konsolenprotokollierung auf den verwendeten Geräten zu aktivieren und beim Austausch Ihres Switches die folgenden Maßnahmen zu ergreifen:

- Lassen Sie AutoSupport während der Wartungsarbeiten aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs AutoSupport aus, um die Fallerstellung für die Dauer der Wartung zu deaktivieren. Siehe diesen Wissensdatenbankartikel "SU92: Wie man die automatische Fallerstellung während geplanter Wartungsfenster unterdrückt" für weitere Einzelheiten.
- Aktivieren Sie die Sitzungsprotokollierung für alle CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Wissensdatenbankartikel. "Wie konfiguriert man PuTTY für eine optimale Verbindung zu ONTAP -Systemen?" Die

Tauschen Sie den Schalter aus.

Zu den Beispielen

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

- Die Namen der vorhandenen Nexus 92300YC Switches lauten cs1 und cs2.
- Der neue Switch Nexus 92300YC trägt den Namen newcs2.
- Die Knotennamen lauten Knoten1 und Knoten2.
- Die Cluster-Ports auf jedem Knoten tragen die Namen e0a und e0b.
- Die Cluster-LIF-Namen lauten node1_clus1 und node1_clus2 für Knoten 1 sowie node2_clus1 und node2_clus2 für Knoten 2.
- Die Aufforderung zum Ändern aller Clusterknoten lautet cluster1::*>

Informationen zu diesem Vorgang

Sie müssen den Befehl zur Migration eines Cluster-LIF von dem Knoten ausführen, auf dem der Cluster-LIF gehostet wird.

Das folgende Verfahren basiert auf der folgenden Cluster-Netzwerktopologie:

Topologie anzeigen

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

Node: node1

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

Node: node2

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



cluster1::*> network interface show -vserver Cluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1         e0a
true
            node1_clus2  up/up    169.254.49.125/16  node1         e0b
```

```
true
            node2_clus1  up/up    169.254.47.194/16  node2         e0a
true
            node2_clus2  up/up    169.254.19.183/16  node2         e0b
true
4 entries were displayed.



cluster1::*> network device-discovery show -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       Eth1/2            N9K-
C92300YC
            e0b    cs2                       Eth1/2            N9K-
C92300YC
node1      /cdp
            e0a    cs1                       Eth1/1            N9K-
C92300YC
            e0b    cs2                       Eth1/1            N9K-
C92300YC
4 entries were displayed.



cs1# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         144    H           FAS2980       e0a
node2              Eth1/2         145    H           FAS2980       e0a
cs2(FDO220329V5)   Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
cs2(FDO220329V5)   Eth1/66        176    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

```
cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform      Port
ID
node1              Eth1/1         139    H           FAS2980       e0b
node2              Eth1/2         124    H           FAS2980       e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

Schritt 1: Vorbereitung auf den Austausch

1. Installieren Sie die entsprechende RCF-Datei und das Image auf dem Switch newcs2 und treffen Sie alle notwendigen Vorbereitungen vor Ort.

   Prüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und NX-OS-Software für den neuen Switch. Wenn Sie überprüft haben, dass der neue Switch korrekt eingerichtet ist und keine Aktualisierungen der RCF- und NX-OS-Software erforderlich sind, fahren Sie mit Schritt 2 fort.

   a. Gehen Sie auf der NetApp Support-Website zur Seite „NetApp Cluster and Management Network Switches Reference Configuration File Description Page“.

   b. Klicken Sie auf den Link zur *Kompatibilitätsmatrix für Cluster- und Managementnetzwerke* und notieren Sie sich anschließend die erforderliche Switch-Softwareversion.

   c. Klicken Sie auf den Zurück-Pfeil Ihres Browsers, um zur **Beschreibungsseite** zurückzukehren, klicken Sie auf **WEITER**, akzeptieren Sie die Lizenzvereinbarung und gehen Sie dann zur **Download**-Seite.

   d. Folgen Sie den Anweisungen auf der Downloadseite, um die korrekten RCF- und NX-OS-Dateien für die Version der ONTAP -Software herunterzuladen, die Sie installieren.

2. Melden Sie sich auf dem neuen Switch als Administrator an und fahren Sie alle Ports herunter, die mit den Knotenclusterschnittstellen verbunden werden (Ports 1/1 bis 1/64).

   Wenn der zu ersetzende Schalter nicht funktionsfähig und ausgeschaltet ist, fahren Sie mit Schritt 4 fort. Die LIFs auf den Clusterknoten sollten bereits für jeden Knoten auf den anderen Clusterport umgeschaltet haben.

Beispiel anzeigen

```
newcs2# config
Enter configuration commands, one per line. End with CNTL/Z.
newcs2(config)# interface e1/1-64
newcs2(config-if-range)# shutdown
```

3. Überprüfen Sie, ob für alle Cluster-LIFs die automatische Rücksetzung aktiviert ist:

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

Beispiel anzeigen

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

             Logical
Vserver      Interface     Auto-revert
------------ ------------- -------------
Cluster      node1_clus1   true
Cluster      node1_clus2   true
Cluster      node2_clus1   true
Cluster      node2_clus2   true

4 entries were displayed.
```

4. 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

Schritt 2: Kabel und Anschlüsse konfigurieren

1. Schalten Sie die ISL-Ports 1/65 und 1/66 am Switch Nexus 92300YC cs1 ab:

   Beispiel anzeigen

   ```
   cs1# configure
   Enter configuration commands, one per line. End with CNTL/Z.
   cs1(config)# interface e1/65-66
   cs1(config-if-range)# shutdown
   cs1(config-if-range)#
   ```

2. Entfernen Sie alle Kabel vom Nexus 92300YC cs2-Switch und schließen Sie sie dann an dieselben Ports am Nexus 92300YC newcs2-Switch an.
3. Aktivieren Sie die ISL-Ports 1/65 und 1/66 zwischen den Switches cs1 und newcs2 und überprüfen Sie dann den Betriebsstatus des Portkanals.

   Port-Channel sollte Po1(SU) und Member Ports sollten Eth1/65(P) und Eth1/66(P) anzeigen.

Beispiel anzeigen

Dieses Beispiel aktiviert die ISL-Ports 1/65 und 1/66 und zeigt die Port-Kanal-Zusammenfassung auf Switch cs1 an:

```
cs1# configure
Enter configuration commands, one per line. End with CNTL/Z.
cs1(config)# int e1/65-66
cs1(config-if-range)# no shutdown

cs1(config-if-range)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------
------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------
------------
1     Po1(SU)     Eth      LACP      Eth1/65(P)   Eth1/66(P)

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

4. Überprüfen Sie, ob Port e0b auf allen Knoten aktiv ist:

   ```
   network port show ipspace Cluster
   ```

Beispiel anzeigen

Die Ausgabe sollte in etwa wie folgt aussehen:

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

5. Auf demselben Knoten, den Sie im vorherigen Schritt verwendet haben, stellen Sie die Cluster-LIF, die dem Port im vorherigen Schritt zugeordnet ist, mit dem Befehl network interface revert wieder her.

Beispiel anzeigen

In diesem Beispiel wird LIF node1_clus2 auf node1 erfolgreich zurückgesetzt, wenn der Wert Home true ist und der Port e0b lautet.

Die folgenden Befehle geben LIF zurück. `node1_clus2` An `node1` zum Heimathafen `e0a` und zeigt Informationen über die LIFs auf beiden Knoten an. Das Hochfahren des ersten Knotens ist erfolgreich, wenn die Spalte „Is Home“ für beide Cluster-Schnittstellen den Wert „true“ aufweist und die korrekten Portzuweisungen angezeigt werden. `e0a` Und `e0b` auf Knoten1.

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

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ------------ ---------- ------------------ ----------
------- -----
Cluster
            node1_clus1  up/up      169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up      169.254.49.125/16  node1
e0b     true
            node2_clus1  up/up      169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up      169.254.19.183/16  node2
e0a     false

4 entries were displayed.
```

6. Informationen über die Knoten in einem Cluster anzeigen:

   `cluster show`

Beispiel anzeigen

Dieses Beispiel zeigt, dass der Knotenstatus für Knoten 1 und Knoten 2 in diesem Cluster „true“ ist:

```
cluster1::*> cluster show

Node          Health  Eligibility
------------- ------- ------------
node1         false   true
node2         true    true
```

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

   `network port show ipspace Cluster`

   Beispiel anzeigen

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

Node: node1

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

Node: node2

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

4 entries were displayed.
```

Schritt 3: Schließen Sie den Vorgang ab.

1. 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Bestätigen Sie die folgende Cluster-Netzwerkkonfiguration:

```
network port show
```

Beispiel anzeigen

```
cluster1::*> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

4 entries were displayed.


cluster1::*> network interface show -vserver Cluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            node1_clus1  up/up    169.254.209.69/16  node1
e0a     true
            node1_clus2  up/up    169.254.49.125/16  node1
```

```
e0b     true
            node2_clus1  up/up    169.254.47.194/16  node2
e0a     true
            node2_clus2  up/up    169.254.19.183/16  node2
e0b     true

4 entries were displayed.

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

Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface
Platform
----------- ------ ------------------------- ----------------
----------------
node2      /cdp
            e0a    cs1                       0/2               N9K-
C92300YC
            e0b    newcs2                    0/2               N9K-
C92300YC
node1      /cdp
            e0a    cs1                       0/1               N9K-
C92300YC
            e0b    newcs2                    0/1               N9K-
C92300YC

4 entries were displayed.


cs1# show cdp neighbors

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

Device-ID            Local Intrfce  Hldtme Capability  Platform
Port ID
node1                Eth1/1         144    H           FAS2980
e0a
node2                Eth1/2         145    H           FAS2980
e0a
newcs2(FDO296348FU)  Eth1/65        176    R S I s     N9K-C92300YC
Eth1/65
newcs2(FDO296348FU)  Eth1/66        176    R S I s     N9K-C92300YC
```

```
Eth1/66


Total entries displayed: 4


cs2# show cdp neighbors

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

Device-ID          Local Intrfce  Hldtme Capability  Platform
Port ID
node1              Eth1/1         139    H           FAS2980
e0b
node2              Eth1/2         124    H           FAS2980
e0b
cs1(FDO220329KU)   Eth1/65        178    R S I s     N9K-C92300YC
Eth1/65
cs1(FDO220329KU)   Eth1/66        178    R S I s     N9K-C92300YC
Eth1/66

Total entries displayed: 4
```

Wie geht es weiter?

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

Ersetzen Sie Cisco Nexus 92300YC Cluster-Switches durch switchlose Verbindungen.

Für ONTAP 9.3 und höher können Sie von einem Cluster mit einem Switched-Cluster-Netzwerk zu einem Cluster migrieren, in dem zwei Knoten direkt miteinander verbunden sind.

Überprüfungsanforderungen

Richtlinien

Bitte beachten Sie die folgenden Richtlinien:

- Die Migration zu einer Zwei-Knoten-Clusterkonfiguration ohne Switches ist ein unterbrechungsfreier Vorgang. Die meisten Systeme verfügen über zwei dedizierte Cluster-Interconnect-Ports pro Knoten. Dieses Verfahren kann aber auch für Systeme mit einer größeren Anzahl dedizierter Cluster-Interconnect-

Ports pro Knoten angewendet werden, beispielsweise vier, sechs oder acht.

- Die Funktion „Switchless Cluster Interconnect“ kann nicht mit mehr als zwei Knoten verwendet werden.
- Wenn Sie über einen bestehenden Zwei-Knoten-Cluster verfügen, der Cluster-Interconnect-Switches verwendet und auf dem ONTAP 9.3 oder höher läuft, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Knoten ersetzen.

Bevor Sie beginnen

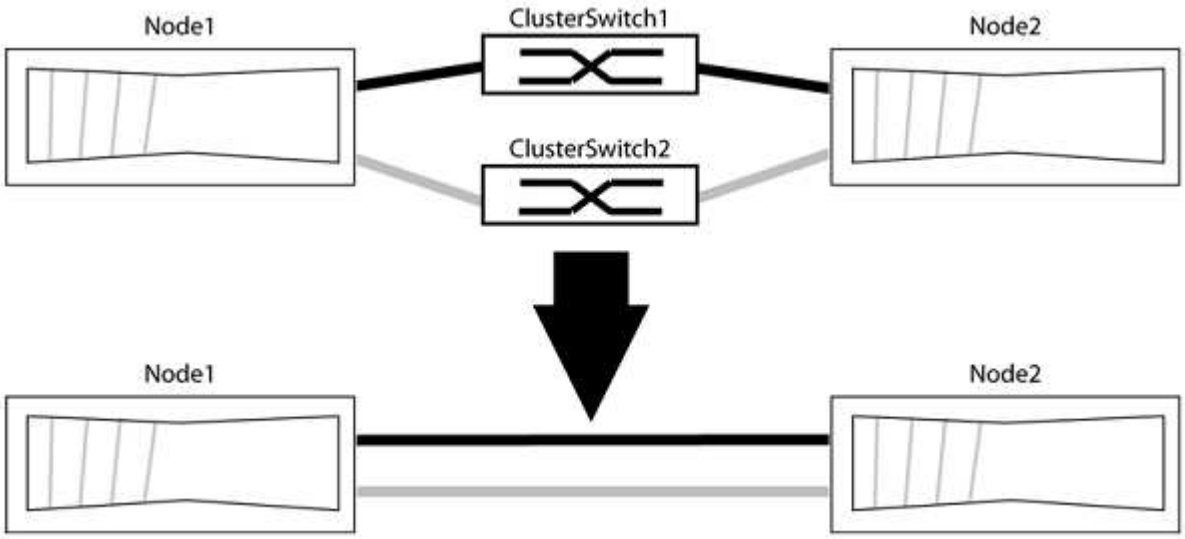
Bitte stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesunder Cluster, der aus zwei Knoten besteht, die über Cluster-Switches verbunden sind. Auf den Knoten muss die gleiche ONTAP Version laufen.
- Jeder Knoten verfügt über die erforderliche Anzahl dedizierter Cluster-Ports, die redundante Cluster-Verbindungen bereitstellen, um Ihre Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster-Verbindungsports auf jedem Knoten.

Migrieren Sie die Schalter

Informationen zu diesem Vorgang

Das folgende Verfahren entfernt die Cluster-Switches in einem Zwei-Knoten-Cluster und ersetzt jede Verbindung zum Switch durch eine direkte Verbindung zum Partnerknoten.



Zu den Beispielen

Die Beispiele im folgenden Verfahren zeigen Knoten, die "e0a" und "e0b" als Cluster-Ports verwenden. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.

Schritt 1: Vorbereitung auf die Migration

1. Ändern Sie die Berechtigungsstufe auf „Erweitert“, indem Sie Folgendes eingeben `y` wenn Sie aufgefordert werden, fortzufahren:

   ```
   set -privilege advanced
   ```

   Die erweiterte Aufforderung `*>` erscheint.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von switchlosen Clustern, die

standardmäßig aktiviert ist.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch aktiviert ist, indem Sie den Befehl mit erweiterten Berechtigungen ausführen:

```
network options detect-switchless-cluster show
```

Beispiel anzeigen

Die folgende Beispielausgabe zeigt, ob die Option aktiviert ist.

```
cluster::*> network options detect-switchless-cluster show
   (network options detect-switchless-cluster show)
Enable Switchless Cluster Detection: true
```

Wenn "Schalterlose Clustererkennung aktivieren" `false` Wenden Sie sich an den NetApp Support.

3. 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=<number_of_hours>h
   ```

   Wo `h` ist die Dauer des Wartungsfensters in Stunden. Die Meldung informiert den technischen Support über diese Wartungsaufgabe, damit dieser die automatische Fallerstellung während des Wartungsfensters unterdrücken kann.

   Im folgenden Beispiel unterdrückt der Befehl die automatische Fallerstellung für zwei Stunden:

   Beispiel anzeigen

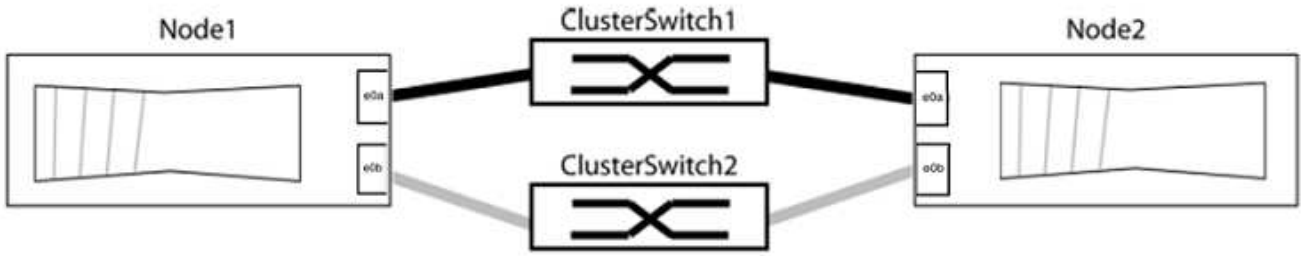
   ```
   cluster::*> system node autosupport invoke -node * -type all
   -message MAINT=2h
   ```

Schritt 2: Anschlüsse und Verkabelung konfigurieren

1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen ein, sodass die Cluster-Ports in Gruppe 1 an Cluster-Switch 1 und die Cluster-Ports in Gruppe 2 an Cluster-Switch 2 angeschlossen werden. Diese Gruppen werden im weiteren Verlauf des Verfahrens benötigt.
2. Identifizieren Sie die Cluster-Ports und überprüfen Sie den Verbindungsstatus und die Integrität:

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

   Im folgenden Beispiel für Knoten mit Cluster-Ports „e0a“ und „e0b“ wird eine Gruppe als „node1:e0a“ und „node2:e0a“ und die andere Gruppe als „node1:e0b“ und „node2:e0b“ identifiziert. Ihre Knoten verwenden möglicherweise unterschiedliche Cluster-Ports, da diese je nach System variieren.



Überprüfen Sie, ob die Ports den Wert haben. `up` für die Spalte „Link“ und einen Wert von `healthy` für die Spalte „Gesundheitszustand“.

Beispiel anzeigen

```
cluster::> network port show -ipspace Cluster
Node: node1

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

Node: node2

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

3. Vergewissern Sie sich, dass alle Cluster-LIFs an ihren jeweiligen Heimatports angeschlossen sind.

Überprüfen Sie, ob die Spalte „is-home“ `true` für jeden der Cluster-LIFs:

```
network interface show -vserver Cluster -fields is-home
```

Beispiel anzeigen

```
cluster::*> net int show -vserver Cluster -fields is-home
(network interface show)
vserver  lif          is-home
-------- ------------ --------
Cluster  node1_clus1  true
Cluster  node1_clus2  true
Cluster  node2_clus1  true
Cluster  node2_clus2  true
4 entries were displayed.
```

Falls Cluster-LIFs vorhanden sind, die sich nicht auf ihren Heimatports befinden, werden diese LIFs wieder auf ihre Heimatports zurückgesetzt:

```
network interface revert -vserver Cluster -lif *
```

4. Automatische Wiederherstellung der Cluster-LIFs deaktivieren:

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

5. Überprüfen Sie, ob alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

   ```
   network device-discovery show -port cluster_port
   ```

   In der Spalte „Erkanntes Gerät“ sollte der Name des Cluster-Switches stehen, mit dem der Port verbunden ist.

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports "e0a" und "e0b" korrekt mit den Cluster-Switches "cs1" und "cs2" verbunden sind.

```
cluster::> network device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/     Local  Discovered
Protocol  Port   Device (LLDP: ChassisID)  Interface  Platform
--------- ------ ------------------------- ---------- ----------
node1/cdp
          e0a    cs1                       0/11       BES-53248
          e0b    cs2                       0/12       BES-53248
node2/cdp
          e0a    cs1                       0/9        BES-53248
          e0b    cs2                       0/9        BES-53248
4 entries were displayed.
```

6. Überprüfen Sie die 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. [[Schritt 7]] Überprüfen Sie, ob der Cluster fehlerfrei funktioniert:

   ```
   cluster ring show
   ```

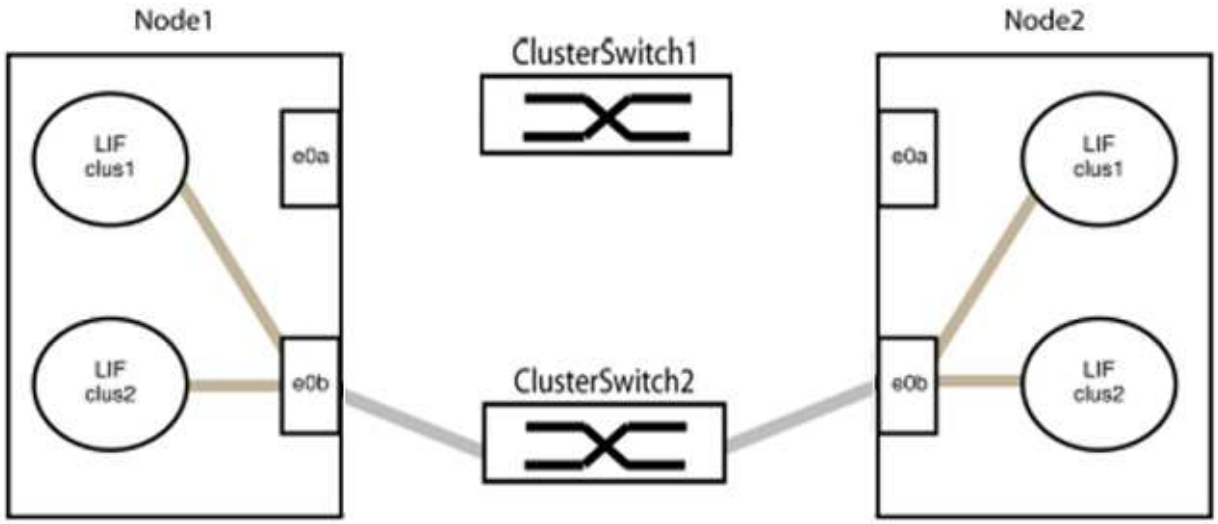
   Alle Einheiten müssen entweder Master- oder Sekundäreinheiten sein.

2. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 1 ein.

   > Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe1 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

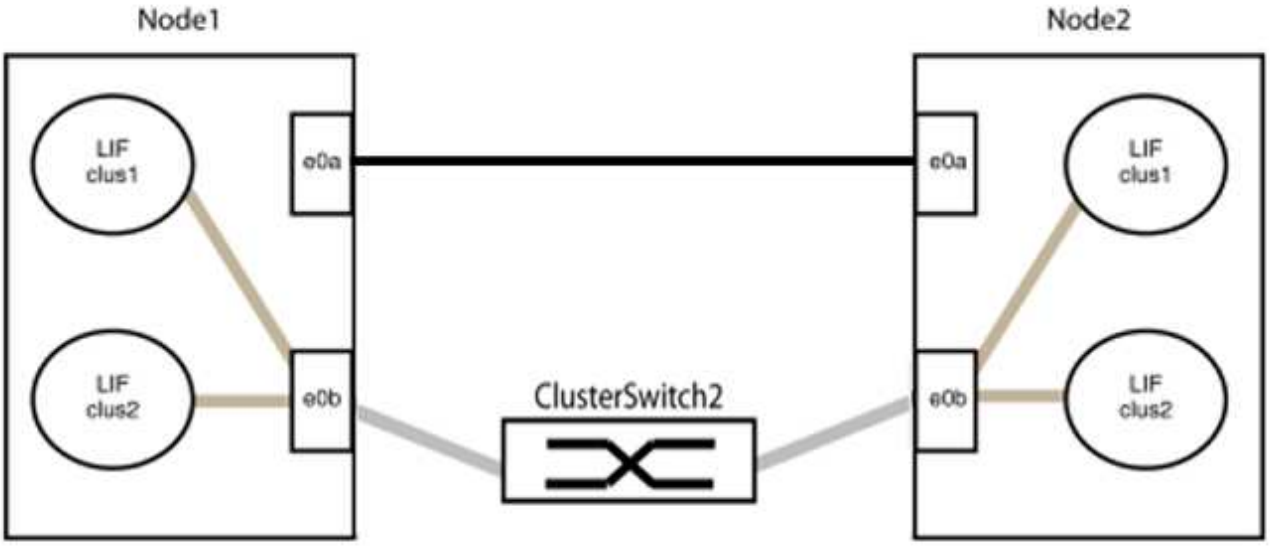
   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 1.

      Im folgenden Beispiel werden die Kabel an Port „e0a“ auf jedem Knoten getrennt, und der Cluster-Datenverkehr wird weiterhin über den Switch und Port „e0b“ auf jedem Knoten abgewickelt:



b. Verbinden Sie die Ports in Gruppe 1 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden:



3. Die Option für ein schalterloses Clusternetzwerk wechselt von `false` Zu `true` Die Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „Schalterlos“ aktiviert ist. `true` :

`network options switchless-cluster show`

Das folgende Beispiel zeigt, dass der switchlose Cluster aktiviert ist:

```
cluster::*> network options switchless-cluster show
Enable Switchless Cluster: true
```

4. 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

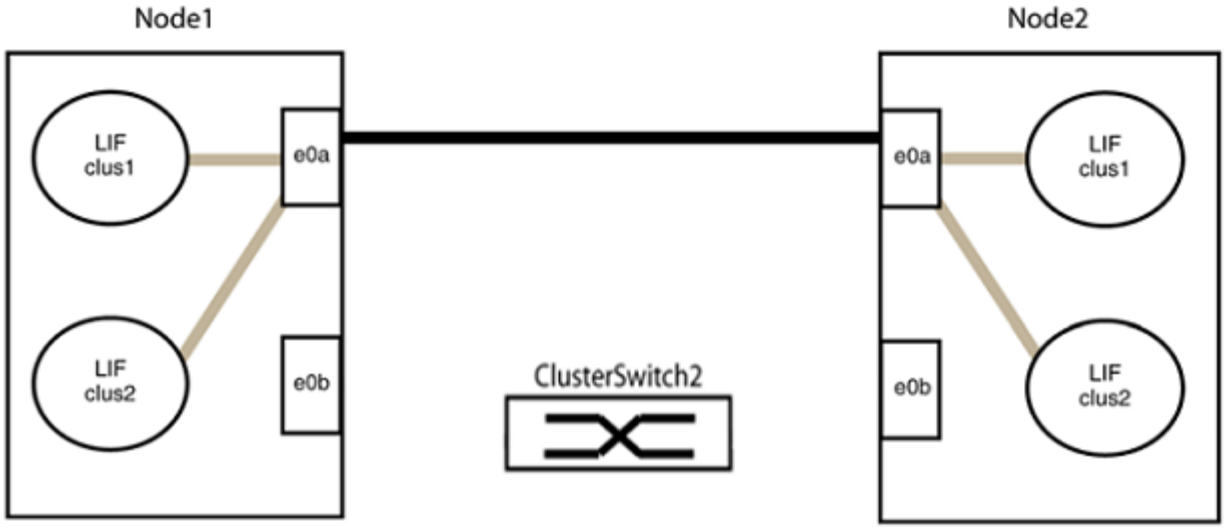
Bevor Sie mit dem nächsten Schritt fortfahren, müssen Sie mindestens zwei Minuten warten, um eine funktionierende Back-to-Back-Verbindung in Gruppe 1 zu bestätigen.

1. Richten Sie die switchlose Konfiguration für die Ports in Gruppe 2 ein.

   Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von Gruppe 2 trennen und sie so schnell wie möglich wieder direkt miteinander verbinden, zum Beispiel **in weniger als 20 Sekunden**.

   a. Trennen Sie gleichzeitig alle Kabel von den Anschlüssen in Gruppe 2.

      Im folgenden Beispiel werden die Kabel von Port "e0b" an jedem Knoten getrennt, und der Cluster-Datenverkehr wird über die direkte Verbindung zwischen den Ports "e0a" fortgesetzt:



b. Verbinden Sie die Ports in Gruppe 2 Rücken an Rücken.

Im folgenden Beispiel ist "e0a" auf Knoten 1 mit "e0a" auf Knoten 2 verbunden und "e0b" auf Knoten 1 ist mit "e0b" auf Knoten 2 verbunden:

Schritt 3: Konfiguration überprüfen

1. Überprüfen Sie, ob die Ports an beiden Knoten korrekt verbunden sind:

```
network device-discovery show -port cluster_port
```

Beispiel anzeigen

Das folgende Beispiel zeigt, dass die Cluster-Ports „e0a“ und „e0b“ korrekt mit dem entsprechenden Port des Cluster-Partners verbunden sind:

```
cluster::> net device-discovery show -port e0a|e0b
  (network device-discovery show)
Node/      Local  Discovered
Protocol   Port   Device (LLDP: ChassisID)  Interface  Platform
---------- ------ ------------------------- ---------- ----------
node1/cdp
           e0a    node2                     e0a        AFF-A300
           e0b    node2                     e0b        AFF-A300
node1/lldp
           e0a    node2 (00:a0:98:da:16:44) e0a        -
           e0b    node2 (00:a0:98:da:16:44) e0b        -
node2/cdp
           e0a    node1                     e0a        AFF-A300
           e0b    node1                     e0b        AFF-A300
node2/lldp
           e0a    node1 (00:a0:98:da:87:49) e0a        -
           e0b    node1 (00:a0:98:da:87:49) e0b        -
8 entries were displayed.
```

2. Automatische Rücksetzung für die Cluster-LIFs wieder aktivieren:

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

3. Überprüfen Sie, ob alle LIFs zu Hause sind. Dies kann einige Sekunden dauern.

   `network interface show -vserver Cluster -lif` *`lif_name`*

Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „Ist zu Hause“ den Wert „Ist zu Hause“ aufweist. `true` , wie gezeigt für `node1_clus2` Und `node2_clus2` im folgenden Beispiel:

```
cluster::> network interface show -vserver Cluster -fields curr-
port,is-home
vserver  lif          curr-port is-home
-------- ------------ --------- -------
Cluster  node1_clus1   e0a       true
Cluster  node1_clus2   e0b       true
Cluster  node2_clus1   e0a       true
Cluster  node2_clus2   e0b       true
4 entries were displayed.
```

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`*

4. Überprüfen Sie den Clusterstatus der Knoten über die Systemkonsole eines der beiden Knoten:

   `cluster show`

   Beispiel anzeigen

   Das folgende Beispiel zeigt, dass epsilon an beiden Knoten gleich ist. `false` :

   ```
   Node  Health  Eligibility Epsilon
   ----- ------- ----------- --------
   node1 true    true        false
   node2 true    true        false
   2 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
       3/5/2022 19:21:18 -06:00   node1_clus2      node2-clus1
none
       3/5/2022 19:21:20 -06:00   node1_clus2      node2_clus2
none
node2
       3/5/2022 19:21:18 -06:00   node2_clus2      node1_clus1
none
       3/5/2022 19:21:20 -06:00   node2_clus2      node1_clus2
none
```

Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 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 169.254.47.194 to Remote 169.254.209.69
Local 169.254.47.194 to Remote 169.254.49.125
Local 169.254.19.183 to Remote 169.254.209.69
Local 169.254.19.183 to Remote 169.254.49.125
Larger than PMTU communication succeeds on 4 path(s)
RPC status:
2 paths up, 0 paths down (tcp check)
2 paths up, 0 paths down (udp check)
```

1. Falls Sie die automatische Fallerstellung unterdrückt haben, aktivieren Sie sie wieder, indem Sie eine AutoSupport Nachricht aufrufen:

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

   Weitere Informationen finden Sie unter "NetApp KB-Artikel 1010449: So unterdrücken Sie die automatische Fallerstellung während geplanter Wartungsfenster".

2. Ändern Sie die Berechtigungsstufe wieder auf Administrator:

   ```
   set -privilege admin
   ```