



# Storage Switches

Install and maintain

NetApp

November 07, 2025

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

# Inhalt

- Storage Switches ..... 1
  - Cisco Nexus 9336C-FX2 oder 9336C-FX2-T ..... 1
    - Los geht's ..... 1
    - Installieren Sie die Hardware ..... 6
    - Konfigurieren der Software ..... 16
    - Ersetzen Sie die Speicher-Switches Cisco Nexus 9336C-FX2 und 9336C-FX2-T ..... 71
  - NVIDIA SN2100 ..... 77
    - Los geht's ..... 77
    - Hardware installieren ..... 80
    - Software konfigurieren ..... 89
    - Switches migrieren ..... 122
    - Ersetzen Sie einen NVIDIA SN2100 Storage-Switch ..... 132

# Storage Switches

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

### Los geht's

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

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

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

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

1

#### "Überprüfen der Konfigurationsanforderungen"

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

2

#### "Überprüfen Sie die Komponenten und Teilenummern"

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

3

#### "Überprüfen Sie die erforderlichen Unterlagen"

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

4

#### "Überprüfen Sie die Smart Call Home-Anforderungen"

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

5

#### "Installieren Sie die Hardware"

Installieren Sie die Switch-Hardware.

6

#### "Konfigurieren der Software"

Konfigurieren Sie die Switch-Software.

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

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

### ONTAP Support

#### ONTAP 9.9.1 und höher

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

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



Die Ethernet-Switch-Statusüberwachung unterstützt ONTAP 9.13.1P8 und früher und 9.14.1P3 und früher oder NX-OS Version 10.3(4a)(M) nicht.

#### ONTAP 9.10.1 und höher

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

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

### Konfigurationsanforderungen

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

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

### Netzwerkanforderungen

Für alle Switch-Konfigurationen benötigen Sie die folgenden Netzwerkinformationen.

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

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

### Was kommt als nächstes

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

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

Für die Installation und Wartung von Cisco Nexus 9336C-FX2 und 9336C-FX2-T Storage-Switches muss die Liste der Komponenten und Teilenummern überprüft werden.

In der folgenden Tabelle sind die Teilenummer und die Beschreibung der Speicherschalter, Lüfter und Netzteile 9336C-FX2 und 9336C-FX2-T aufgeführt:

Teilenummer	Beschreibung
X190200-CS-PE	Cluster-Switch, N9336C 36PT PTSX 10/25/40/100G
X190200-CS-PI	Cluster-Switch, N9336C 36 PT PSIN 10/25/40/100G
X190212-CS-PE	Cluster-Switch, N9336C, 12 PT (9336C-FX2-T), PTSX 10/25/40 G
X190212-CS-PI	Cluster-Switch, N9336C, 12 PT (9336C-FX2-T), PSIN 10/25/40 G
SW-N9K-FX2-24P-UPG	SW, Cisco 9336CFX2 POD-Lizenz mit 24 Anschlüssen
X190210-FE-PE	N9K-9336C, FTE, PTSX, 36PT 10/25/40/100GQSFP28
X190210-FE-PI	N9K-9336C, FTE, PSIN, 36PT 10/25/40/100GQSFP28
X190002	Zubehörkit X190001/X190003
X-NXA-PAC-1100W-PE2	N9K-9336C AC 1100 W Netzteil – Luftstrom am Port Side
X-NXA-PAC-1100W-PI2	N9K-9336C AC 1100 W Netzteil – Luftstrom für den seitlichen Ansauganschluss
X-NXA-LÜFTER-65CFM-PE	N9K-9336C 65 CFM, Luftstrom nach Anschlussseite
X-NXA-LÜFTER-65CFM-PI	N9K-9336C 65 CFM, Luftstrom zur Ansaugöffnung an der Seite des Ports

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

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

1. Erstellen Sie bei Bedarf ein neues Smart-Konto. Weitere Informationen finden Sie unter ["Erstellen Sie ein neues Smart-Konto"](#).
2. Zugriff auf ein vorhandenes Smart-Konto anfordern. Weitere Informationen finden Sie unter ["Zugriff auf ein vorhandenes Smart-Konto anfordern"](#).



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

## Was kommt als nächstes

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

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

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

### Switch-Dokumentation

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

Dokumenttitel	Beschreibung
Hardware-Installationshandbuch Der Serie <i>Nexus 9000</i>	Detaillierte Informationen zu Standortanforderungen, Hardwaredetails zu Switches und Installationsoptionen.
<i>Cisco Nexus 9000 Series Switch Software Configuration Guides</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Stellt Informationen zur Erstkonfiguration des Switches bereit, die Sie benötigen, bevor Sie den Switch für den ONTAP-Betrieb konfigurieren können.
<i>Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide</i> (wählen Sie das Handbuch für die auf Ihren Switches installierte NX-OS-Version)	Enthält Informationen zum Downgrade des Switch auf ONTAP unterstützte Switch-Software, falls erforderlich.
<i>Cisco Nexus 9000 Series NX-OS Command Reference Master Index</i>	Enthält Links zu den verschiedenen von Cisco bereitgestellten Befehlsreferenzen.
<i>Cisco Nexus 9000 MIBs Referenz</i>	Beschreibt die MIB-Dateien (Management Information Base) für die Nexus 9000-Switches.
<i>Nexus 9000 Series NX-OS System Message Reference</i>	Beschreibt die Systemmeldungen für Switches der Cisco Nexus 9000 Serie, Informationen und andere, die bei der Diagnose von Problemen mit Links, interner Hardware oder der Systemsoftware helfen können.
<i>Versionshinweise zur Cisco Nexus 9000-Serie NX-OS (wählen Sie die Hinweise für die auf Ihren Switches installierte NX-OS-Version aus)</i>	Beschreibt die Funktionen, Bugs und Einschränkungen der Cisco Nexus 9000 Serie.
Compliance- und Sicherheitsinformationen für die Cisco Nexus 9000-Serie	Bietet internationale Compliance-, Sicherheits- und gesetzliche Informationen für Switches der Serie Nexus 9000.

## Dokumentation der ONTAP Systeme

Um ein ONTAP-System einzurichten, benötigen Sie die folgenden Dokumente für Ihre Version des Betriebssystems von ["ONTAP 9"](#).

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

## Schienensatz und Rack-Dokumentation

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

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

## 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:

- Es muss ein E-Mail-Server vorhanden sein.
- Der Switch muss über eine IP-Verbindung zum E-Mail-Server verfügen.
- Der Name des Kontakts (SNMP-Serverkontakt), die Telefonnummer und die Adresse der Straße müssen konfiguriert werden. Dies ist erforderlich, um den Ursprung der empfangenen Nachrichten zu bestimmen.

- Eine CCO-ID muss mit einem entsprechenden Cisco SMARTnet-Servicevertrag für Ihr Unternehmen verknüpft sein.
- Cisco SMARTnet Service muss vorhanden sein, damit das Gerät registriert werden kann.

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

## Installieren Sie die Hardware

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

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

1

#### "Vervollständigen Sie das Verkabelungsarbeitsblatt"

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

2

#### "Den Schalter einbauen"

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

3

#### "Den Switch in einen NetApp-Schrank einbauen"

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

### Füllen Sie das Arbeitsblatt zur Verkabelung des Cisco Nexus 9336C-FX2 oder 9336C-FX2-T aus

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

Das Verkabelungsarbeitsblatt enthält Beispiele für empfohlene Port-Zuweisungen von den Switches zu den Controllern. Das leere Arbeitsblatt bietet eine Vorlage, die Sie beim Einrichten des Clusters verwenden können.

- [9336C-FX2 – Beispieldokument für Verkabelung](#)
- [9336C-FX2 Arbeitsblatt für leere Verkabelung](#)
- [Arbeitsblatt zur 9336C-FX2-T-Beispielverkabelung \(12 Anschlüsse\)](#)
- [Arbeitsblatt für die Verkabelung 9336C-FX2-T-Leereinschub \(12 Anschlüsse\)](#)

#### 9336C-FX2 – Beispieldokument für Verkabelung

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports



Cluster-Switch A		Cluster-Switch B	
1	4 x 100-GbE-Node 1	1	4 x 100-GbE-Node 1
2	4 x 100-GbE-Node 2	2	4 x 100-GbE-Node 2
3	4 x 100-GbE-Node 3	3	4 x 100-GbE-Node 3
4	4 x 100-GbE-Node 4	4	4 x 100-GbE-Node 4
5	4 x 100-GbE-Node 5	5	4 x 100-GbE-Node 5
6	4 x 100-GbE-Node 6	6	4 x 100-GbE-Node 6
7	4 x 100-GbE-Node 7	7	4 x 100-GbE-Node 7
8	4 x 100-GbE-Node 8	8	4 x 100-GbE-Node 8
9	4 x 100-GbE-Node 9	9	4 x 100-GbE-Node 9
10	4 x 100-GbE-Node 10	10	4 x 100-GbE-Node 10
11	4 x 100-GbE-Node 11	11	4 x 100-GbE-Node 11
12	4 x 100-GbE-Node 12	12	4 x 100-GbE-Node 12
13	4 x 100-GbE-Node 13	13	4 x 100-GbE-Node 13
14	4 x 100-GbE-Node 14	14	4 x 100-GbE-Node 14
15	4 x 100-GbE-Node 15	15	4 x 100-GbE-Node 15
16	4 x 100-GbE-Node 16	16	4 x 100-GbE-Node 16
17	4 x 100-GbE-Node 17	17	4 x 100-GbE-Node 17
18	4 x 100-GbE-Node 18	18	4 x 100-GbE-Node 18
19	4 x 100-GbE-Node 19	19	4 x 100-GbE-Node 19
20	4 x 100-GbE-Node 20	20	4 x 100-GbE-Node 20
21	4 x 100-GbE-Node 21	21	4 x 100-GbE-Node 21
22	4 x 100-GbE-Node 22	22	4 x 100-GbE-Node 22

Cluster-Switch A		Cluster-Switch B	
23	4 x 100-GbE-Node 23	23	4 x 100-GbE-Node 23
24	4 x 100-GbE-Node 24	24	4 x 100-GbE-Node 24
25	4 x 100-GbE-Node 25	25	4 x 100-GbE-Node 25
26	4 x 100-GbE-Node 26	26	4 x 100-GbE-Node 26
27	4 x 100-GbE-Node 27	27	4 x 100-GbE-Node 27
28	4 x 100-GbE-Node 28	28	4 x 100-GbE-Node 28
29	4 x 100-GbE-Node 29	29	4 x 100-GbE-Node 29
30	4 x 100-GbE-Node 30	30	4 x 100-GbE-Node 30
31	4 x 100-GbE-Node 31	31	4 x 100-GbE-Node 31
32	4 x 100-GbE-Node 32	32	4 x 100-GbE-Node 32
33	4 x 100-GbE-Node 33	33	4 x 100-GbE-Node 33
30	4 x 100-GbE-Node 30	30	4 x 100-GbE-Node 33
34	4 x 100-GbE-Node 34	34	4 x 100-GbE-Node 34
35	4 x 100-GbE-Node 35	35	4 x 100-GbE-Node 35
36	4 x 100-GbE-Node 36	36	4 x 100-GbE-Node 36

#### 9336C-FX2 Arbeitsblatt für leere Verkabelung

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden. Der Abschnitt „*supported Cluster Connections*“ des "[Hardware Universe](#)" Definiert die von der Plattform verwendeten Cluster-Ports.

Cluster-Switch A		Cluster-Switch B	
1		1	
2		2	
3		3	

Cluster-Switch A		Cluster-Switch B	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11		11	
12		12	
13		13	
14		14	
15		15	
16		16	
17		17	
18		18	
19		19	
20		20	
21		21	
22		22	
23		23	
24		24	
25		25	

Cluster-Switch A		Cluster-Switch B	
26		26	
27		27	
28		28	
29		29	
30		30	
31		31	
32		32	
33		33	
34		34	
35		35	
36		36	

#### Arbeitsblatt zur 9336C-FX2-T-Beispielverkabelung (12 Anschlüsse)

Die Beispielanschlussdefinition für jedes Switch-Paar lautet wie folgt:

Cluster-Switch A		Cluster-Switch B	
Switch-Port	Verwendung von Nodes und Ports	Switch-Port	Verwendung von Nodes und Ports
1	4 x 100-GbE-Node 1	1	4 x 100-GbE-Node 1
2	4 x 100-GbE-Node 2	2	4 x 100-GbE-Node 2
3	4 x 100-GbE-Node 3	3	4 x 100-GbE-Node 3
4	4 x 100-GbE-Node 4	4	4 x 100-GbE-Node 4
5	4 x 100-GbE-Node 5	5	4 x 100-GbE-Node 5
6	4 x 100-GbE-Node 6	6	4 x 100-GbE-Node 6
7	4 x 100-GbE-Node 7	7	4 x 100-GbE-Node 7

Cluster-Switch A		Cluster-Switch B	
8	4 x 100-GbE-Node 8	8	4 x 100-GbE-Node 8
9	4 x 100-GbE-Node 9	9	4 x 100-GbE-Node 9
10	4 x 100-GbE-Node 10	10	4 x 100-GbE-Node 10
11 bis 36	Erfordert Lizenz	11 bis 36	Erfordert Lizenz

#### Arbeitsblatt für die Verkabelung 9336C-FX2-T-Leereinschub (12 Anschlüsse)

Sie können das leere Verkabelungsarbeitsblatt verwenden, um die Plattformen zu dokumentieren, die als Nodes in einem Cluster unterstützt werden.

Cluster-Switch A		Cluster-Switch B	
1		1	
2		2	
3		3	
4		4	
5		5	
6		6	
7		7	
8		8	
9		9	
10		10	
11 bis 36	Erfordert Lizenz	11 bis 36	Erfordert Lizenz

Siehe ["Hardware Universe"](#) Weitere Informationen zu Switch-Ports.

#### Was kommt als nächstes

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

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

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

9336C-FX2-T zu installieren.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

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

### Schritte

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

Wenn Sie das installieren...	Dann...
Cisco Nexus 9336C-FX2 in einem NetApp Systemschrank	Siehe " <a href="#">Switch in NetApp-Schrank einbauen</a> " Eine Anleitung zur Installation des Switches in einem NetApp-Schrank ist ebenfalls vorhanden.
Geräte in einem Telco-Rack	Siehe die Verfahren in den Installationsleitfäden für die Switch-Hardware sowie in den Installations- und Setup-Anleitungen für NetApp.

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

### Was kommt als Nächstes?

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

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

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

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

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

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



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

### Erforderliche Dokumentation

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

### Schritte

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

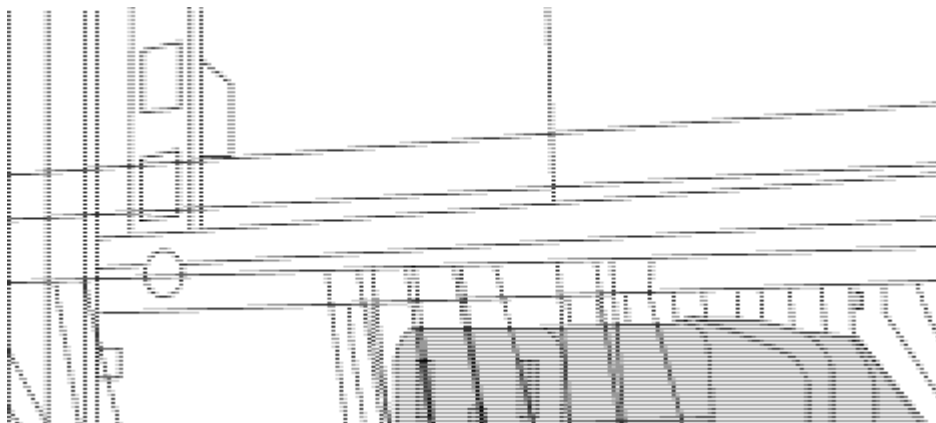
Die Pass-Through-Panel-Kit ist bei NetApp erhältlich (Teilenummer X8784-R6).

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

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

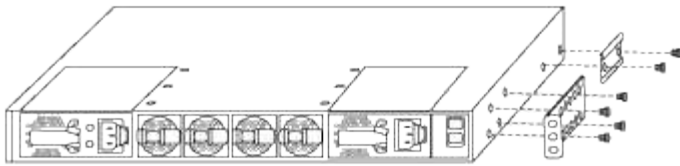
Bei diesem Verfahren wird die Blindplatte in U40 installiert.

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

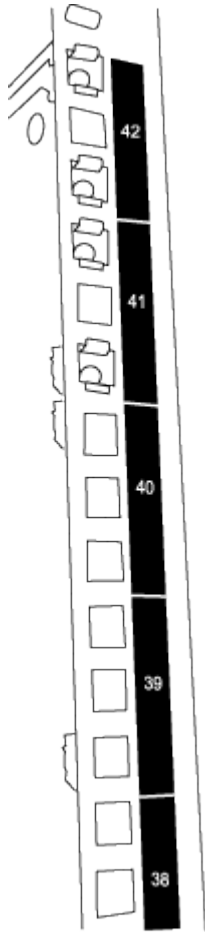


(1) *Buchsenleiste des Überbrückungskabels.*

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



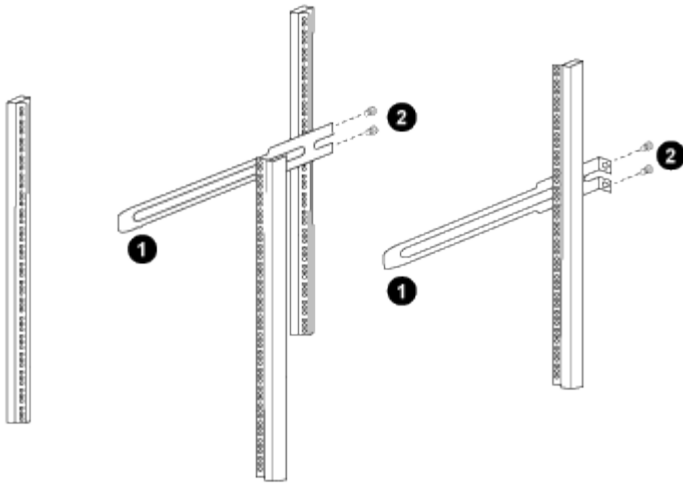
- b. Wiederholen Sie Schritt 2a mit der anderen vorderen Halterung für die Rackmontage auf der anderen Seite des Schalters.
  - c. Setzen Sie die hintere Rack-Halterung am Switch-Gehäuse ein.
  - d. Wiederholen Sie Schritt 2c mit der anderen hinteren Halterung für die Rackmontage auf der anderen Seite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



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

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





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

(2) *Schrauben der Gleitschienen an den Schrankleisten festziehen.*

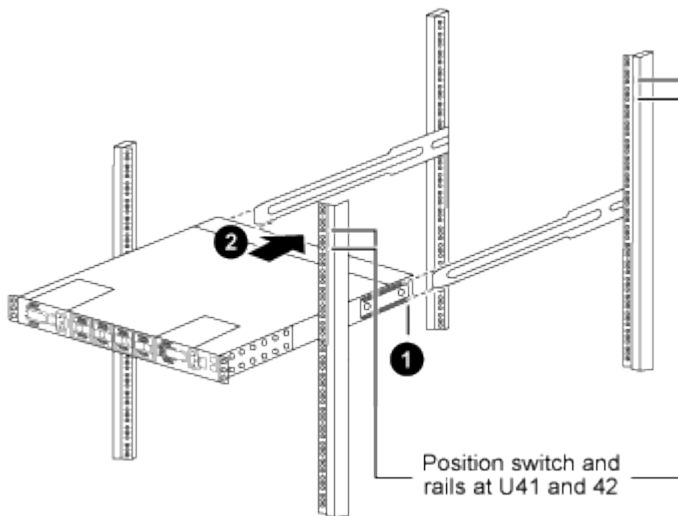
- a. Wiederholen Sie Schritt 4a für den hinteren Pfosten auf der rechten Seite.
- b. Wiederholen Sie die Schritte 4a und 4b an den RU41-Stellen im Schrank.

5. Den Schalter in den Schrank einbauen.



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

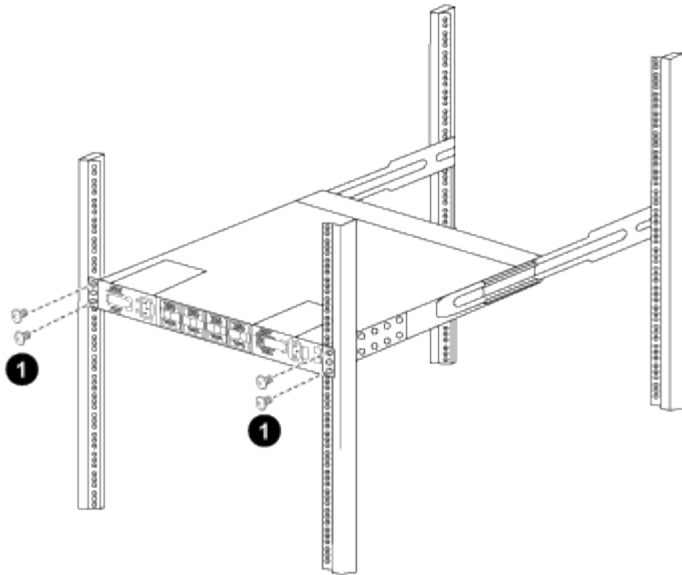
- a. Positionieren Sie die Rückseite des Schalters an RU41.



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

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

- b. Befestigen Sie den Schalter am Gehäuse.



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

- a. Wenn das Gehäuse nun ohne Unterstützung unterstützt wird, ziehen Sie die vorderen Schrauben fest an den Stützen.
- b. Wiederholen Sie die Schritte 5a bis 5c für den zweiten Schalter an der Position RU42.



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

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



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

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

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

### Was kommt als nächstes

Nachdem Sie die Switches im NetApp -Schrack installiert haben, können Sie ["Konfigurieren Sie die Cisco Nexus 9336C-FX2- und 9336C-FX2-T-Switches"](#) Die

## Konfigurieren der Software

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

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

1

### "Konfigurieren Sie den Switch"

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

2

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

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

3

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

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

4

### "Installieren oder aktualisieren Sie den RCF"

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

5

### "SSH-Konfiguration überprüfen"

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

6

### "Setzen Sie den Switch auf die Werkseinstellungen zurück"

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

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

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

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- Zugriff auf einen HTTP-, FTP- oder TFTP-Server auf der Installationswebsite zum Herunterladen der entsprechenden NX-OS- und RCF-Versionen (Reference Configuration File).
- Entsprechende NX-OS-Version, heruntergeladen von "[Cisco Software-Download](#)" Seite.
- Anwendbare Lizenzen, Netzwerk- und Konfigurationsinformationen und Kabel


- Abgeschlossen "[Verkabelungsarbeitsblätter](#)".
- Entsprechende RCFs für das NetApp Cluster-Netzwerk und das Management-Netzwerk, die von der NetApp Support Site unter heruntergeladen werden "[mysupport.netapp.com](https://mysupport.netapp.com)". Alle Netzwerk- und Management-Netzwerk-Switches von Cisco sind mit der Standardkonfiguration von Cisco geliefert. Diese Switches verfügen auch über die aktuelle Version der NX-OS-Software, aber nicht über die RCFs geladen.
- Erforderliche Switch-Dokumentation Siehe "[Erforderliche Dokumentation](#)" Finden Sie weitere Informationen.


## Schritte

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

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

Eingabeaufforderung	Antwort
Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/nein)	Antworten Sie mit <b>ja</b> . Der Standardwert ist Nein
Wollen Sie den sicheren Kennwortstandard durchsetzen? (ja/nein)	Antworten Sie mit <b>ja</b> . Die Standardeinstellung ist ja.
Geben Sie das Passwort für den Administrator ein.	Das Standardpasswort lautet „admin“. Sie müssen ein neues, starkes Passwort erstellen. Ein schwaches Kennwort kann abgelehnt werden.
Möchten Sie das Dialogfeld Grundkonfiguration aufrufen? (ja/nein)	Reagieren Sie mit <b>ja</b> bei der Erstkonfiguration des Schalters.
Noch ein Login-Konto erstellen? (ja/nein)	Ihre Antwort hängt von den Richtlinien Ihrer Site ab, die von alternativen Administratoren abhängen. Der Standardwert ist <b>no</b> .
Schreibgeschützte SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Lese-Schreib-SNMP-Community-String konfigurieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Geben Sie den Switch-Namen ein.	Der Switch-Name ist auf 63 alphanumerische Zeichen begrenzt.
Mit Out-of-Band-Management-Konfiguration (mgmt0) fortfahren? (ja/nein)	Beantworten Sie mit <b>ja</b> (der Standardeinstellung) bei dieser Aufforderung. Geben Sie an der Eingabeaufforderung mgmt0 IPv4 Adresse: ip_address Ihre IP-Adresse ein.

Eingabeaufforderung	Antwort
Standard-Gateway konfigurieren? (ja/nein)	Antworten Sie mit <b>ja</b> . Geben Sie an der IPv4-Adresse des Standard-Gateway: Prompt Ihren Standard_Gateway ein.
Erweiterte IP-Optionen konfigurieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Telnet-Dienst aktivieren? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
SSH-Dienst aktiviert? (ja/nein)	<p>Antworten Sie mit <b>ja</b>. Die Standardeinstellung ist ja.</p> <div>  <p>SSH wird empfohlen, wenn der Ethernet Switch Health Monitor (CSHM) für die Protokollerfassungsfunktionen verwendet wird. SSHv2 wird auch für erhöhte Sicherheit empfohlen.</p> </div>
Geben Sie den Typ des zu generierende SSH-Schlüssels ein (dsa/rsa/rsa1).	Der Standardwert ist <b>rsa</b> .
Geben Sie die Anzahl der Schlüsselbits ein (1024-2048).	Geben Sie die Anzahl der Schlüsselbits von 1024 bis 2048 ein.
Konfigurieren Sie den NTP-Server? (ja/nein)	Antworten Sie mit <b>Nein</b> . Der Standardwert ist Nein
Konfigurieren der Standard-Schnittstellenebene (L3/L2)	Antworten Sie mit <b>L2</b> . Der Standardwert ist L2.
Konfiguration des Status der Standard-Switch-Port-Schnittstelle (Shutter/noshut)	Antworten Sie mit <b>noshut</b> . Die Standardeinstellung ist noshut.
Konfiguration des CoPP-Systemprofils (streng/mittelmäßig/lenient/dense)	Reagieren Sie mit * Strict*. Die Standardeinstellung ist streng.
Möchten Sie die Konfiguration bearbeiten? (ja/nein)	Die neue Konfiguration sollte jetzt angezeigt werden. Überprüfen Sie die soeben eingegebene Konfiguration und nehmen Sie alle erforderlichen Änderungen vor. Wenn Sie mit der Konfiguration zufrieden sind, antworten Sie mit <b>No</b> an der Eingabeaufforderung. Beantworten Sie mit <b>ja</b> , wenn Sie Ihre Konfigurationseinstellungen bearbeiten möchten.

Eingabeaufforderung	Antwort
Verwenden Sie diese Konfiguration und speichern Sie sie? (ja/nein)	<p>Antworten Sie mit <b>ja</b>, um die Konfiguration zu speichern. Dadurch werden die Kickstart- und Systembilder automatisch aktualisiert.</p> <div>  <p>Wenn Sie die Konfiguration zu diesem Zeitpunkt nicht speichern, werden keine Änderungen beim nächsten Neustart des Switches wirksam.</p> </div>

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

### Was kommt als Nächstes?

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

### Bereiten Sie die Installation oder das Upgrade von NX-OS-Software und RCF vor

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

#### Zu den Beispielen

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

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

### Über diese Aufgabe

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

#### Schritte

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

Wobei x die Dauer des Wartungsfensters in Stunden ist.



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

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

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (\*>`Erscheint.

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

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

#### Beispiel anzeigen

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

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

4 entries were displayed.

4. Überprüfen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen.
- a. Zeigen Sie die Attribute des Netzwerkports an:

```
network port show -ipSpace Cluster
```

## Beispiel anzeigen

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
4 entries were displayed.
```

b. Zeigt Informationen zu den LIFs an:

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



## Beispiel anzeigen

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

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

4 entries were displayed.

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

## ONTAP 9.9.1 und höher

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

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

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

**HINWEIS:** Warten Sie einige Sekunden, bevor Sie den Befehl ausführen `show`, um die Details anzuzeigen.

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

Packet		Source	Destination
Node	Date	LIF	LIF
Loss			
-----			
-----			
node1			
	3/5/2024 19:21:18 -06:00	cluster1-01_clus2	cluster1-02-
clus1	none		
	3/5/2024 19:21:20 -06:00	cluster1-01_clus2	cluster1-
02_clus2	none		
node2			
	3/5/2024 19:21:18 -06:00	cluster1-02_clus2	cluster1-
01_clus1	none		
	3/5/2024 19:21:20 -06:00	cluster1-02_clus2	cluster1-
01_clus2	none		

## Alle ONTAP Versionen

Sie können für alle ONTAP Versionen auch den verwenden `cluster ping-cluster -node <name>` Befehl zum Überprüfen der Konnektivität:

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

```

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

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

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

```

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

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

## Beispiel anzeigen

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

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

4 entries were displayed.

### Was kommt als Nächstes?

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

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

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

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

### Prüfen Sie die Anforderungen

#### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

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

### Vorgeschlagene Dokumentation

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

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

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

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

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

Enthält Informationen zu störenden Upgrades/Downgrades für Cisco NX-OS-Software auf Switches der Nexus 9000-Serie  
Basierend auf Ihren aktuellen und Zielversionen.

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

### Zu den Beispielen

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

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

### Installieren Sie die Software

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

### Schritte

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

### Beispiel anzeigen

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

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

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

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

```
network device-discovery show
```

## Beispiel anzeigen

```
cluster1::*> network device-discovery show
Node/          Local  Discovered
Protocol      Port   Device (LLDP: ChassisID)  Interface
Platform
-----
-----
cluster1-01/cdp
          e0a    cs1                Ethernet1/7      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/7      N9K-
C9336C-FX2
cluster1-02/cdp
          e0a    cs1                Ethernet1/8      N9K-
C9336C-FX2
          e0d    cs2                Ethernet1/8      N9K-
C9336C-FX2
cluster1-03/cdp
          e0a    cs1                Ethernet1/1/1    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/1    N9K-
C9336C-FX2
cluster1-04/cdp
          e0a    cs1                Ethernet1/1/2    N9K-
C9336C-FX2
          e0b    cs2                Ethernet1/1/2    N9K-
C9336C-FX2
cluster1::*>
```

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

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

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

## Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

8 entries were displayed.

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

cluster1::\*>

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

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



## Beispiel anzeigen

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

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

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

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

## Beispiel anzeigen

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

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

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

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

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

## Beispiel anzeigen

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

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

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

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

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

```
show version
```

## Beispiel anzeigen

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

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

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

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

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

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

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

```
Service:
```

```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

```
cs2#
```

8. Installieren Sie das NX-OS Image.

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

## Beispiel anzeigen

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

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

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

```
Verifying image type.  
[] 100% -- SUCCESS
```

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

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

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

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

Compatibility check is done:

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

Images will be upgraded according to following table:

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

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

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

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

```
Performing runtime checks.
```

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

```
Setting boot variables.
```

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

```
Performing configuration copy.
```

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

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

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

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

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

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

```
show version
```

```
cs2# show version
```

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

### Software

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

### Hardware

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

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



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

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

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

```
Service:
```

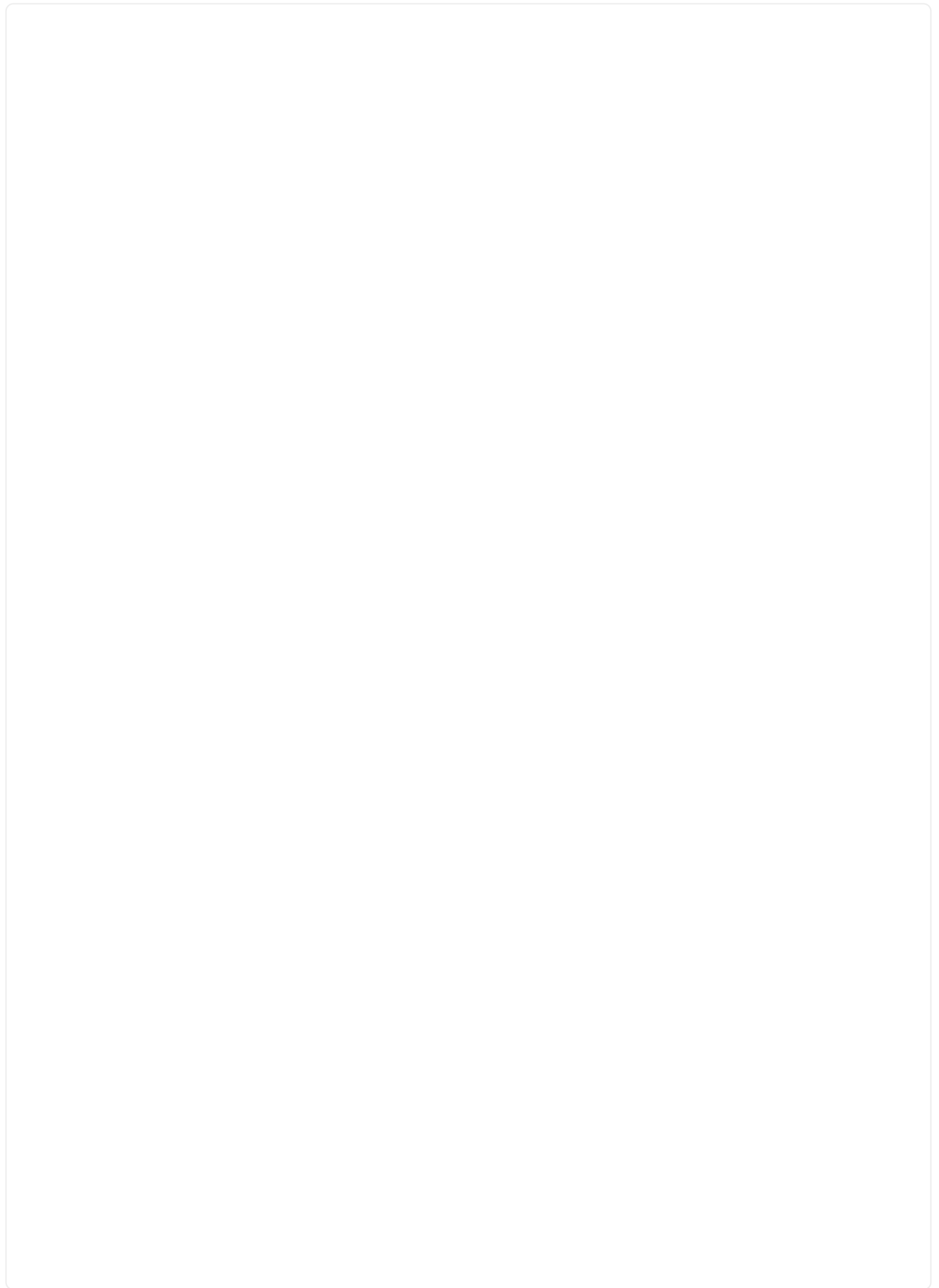
```
plugin
```

```
Core Plugin, Ethernet Plugin
```

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

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

**Beispiel anzeigen**



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

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

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

Compatibility check:

Module	Type	Upgradable	Impact	Reason
1	SUP	Yes	disruptive	Module Upgradable

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to following table:

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

The above modules require upgrade.

The switch will be reloaded at the end of the upgrade

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

Module 1 EPLD upgrade is successful.

Module	Type	Upgrade-Result
1	SUP	Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

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

**Beispiel anzeigen**

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

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

12. Überprüfen Sie den Systemzustand der Cluster-Ports auf dem Cluster.
- a. Vergewissern Sie sich, dass Cluster-Ports über alle Nodes im Cluster hinweg ordnungsgemäß hochaktiv sind:

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

## Beispiel anzeigen

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

```
Node: cluster1-01
```

```
Ignore
```

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

```
Node: cluster1-02
```

```
Ignore
```

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

```
Node: cluster1-03
```

```
Ignore
```

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

Node: cluster1-04

Ignore

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

8 entries were displayed.

b. Überprüfen Sie den Switch-Zustand vom Cluster.

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

## Beispiel anzeigen

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	
Platform				
-----				
-----				
cluster1-01/cdp				
	e0a	cs1	Ethernet1/7	N9K-
C9336C-FX2				
	e0d	cs2	Ethernet1/7	N9K-
C9336C-FX2				
cluster01-2/cdp				
	e0a	cs1	Ethernet1/8	N9K-
C9336C-FX2				
	e0d	cs2	Ethernet1/8	N9K-
C9336C-FX2				
cluster01-3/cdp				
	e0a	cs1	Ethernet1/1/1	N9K-
C9336C-FX2				
	e0b	cs2	Ethernet1/1/1	N9K-
C9336C-FX2				
cluster1-04/cdp				
	e0a	cs1	Ethernet1/1/2	N9K-
C9336C-FX2				
	e0b	cs2	Ethernet1/1/2	N9K-
C9336C-FX2				

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

Switch	Type	Address	
Model			
-----			
-----			
cs1	cluster-network	10.233.205.90	N9K-
C9336C-FX2			
Serial Number: FOCXXXXXXGD			
Is Monitored: true			
Reason: None			
Software Version: Cisco Nexus Operating System (NX-OS) Software,			
Version			
9.3(5)			
Version Source: CDP			
cs2	cluster-network	10.233.205.91	N9K-

```

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

2 entries were displayed.

```

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

```

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

```

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

```
cluster show
```

**Beispiel anzeigen**

```

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

```

14. Wiederholen Sie die Schritte 6 bis 13, um die NX-OS-Software auf Switch cs1 zu installieren.

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

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



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

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

#### Beispiel anzeigen

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

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

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

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

#### Was kommt als Nächstes?

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

#### Überprüfen Sie Ihre SSH-Konfiguration

Wenn Sie die Funktionen des Ethernet Switch Health Monitor (CSHM) und der Protokollsammlung verwenden, überprüfen Sie, ob SSH- und SSH-Schlüssel auf den

Cluster-Switches aktiviert sind.

### Schritte

1. Vergewissern Sie sich, dass 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
AAAAB3NzaC1yc2EAAAADAQABAAQGDINrD52Q586wTGJjFABjBlFaA23EpDrZ2sDCew
l7nwlloC6HBejxluIObAH8hrW8kR+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
AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAABmlzdHA1MjEAAACFBABJ+ZX5SFKhS57e
vkE273e0VoqZi4/32dt+f14fBuKv80MjMsmLfjKtCWylwgVt1Zi+C5TIBbugpzez529z
kFSF0ADb8JaGCoaAYe2HvWR/f6QLbKbqVlEwCdqWgxzrIY5BPP5GBdxQJMBiOwEdnHg1
u/9Pzh/Vz9cHDcCW9qGE780QHA==

bitcount:521
fingerprint:
SHA256:TFGe2hXn6QIpcs/vyHzftHJ7Dceg0vQaULYRA1ZeHwQ

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



Wenn Sie FIPS aktivieren, müssen Sie den Bitcount mit dem Befehl auf dem Switch auf 256 ändern `ssh key ecdsa 256 force`. ["Konfiguration der Netzwerksicherheit mit FIPS"](#) Weitere Informationen finden Sie unter.

### Was kommt als Nächstes?

Nachdem Sie Ihre SSH-Konfiguration überprüft haben, ["Konfigurieren der Switch-Integritätsüberwachung"](#).

Installieren oder aktualisieren Sie die Übersicht über die Referenzkonfigurationsdatei (RCF)

Die Referenzkonfigurationsdatei (RCF) wird nach der erstmaligen Einrichtung des

Speicherswitches Nexus 9336C-FX2 installiert. Sie aktualisieren Ihre RCF-Version, wenn auf Ihrem Switch eine vorhandene Version der RCF-Datei installiert ist.

Weitere Informationen zur Installation oder Aktualisierung Ihres RCF finden Sie im Knowledge Base-Artikel "[Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung](#)".

### Verfügbare RCF-Konfigurationen

In der folgenden Tabelle werden die für verschiedene Konfigurationen verfügbaren RCFs beschrieben. Wählen Sie den RCF aus, der für Ihre Konfiguration geeignet ist.

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

RCF-Name	Beschreibung
2-Cluster-HA-Breakout an	Unterstützt zwei ONTAP-Cluster mit mindestens acht Nodes, einschließlich Nodes, die gemeinsam genutzte Cluster + HA-Ports verwenden.
4-Cluster-HA-Breakout an	Unterstützt vier ONTAP-Cluster mit mindestens vier Knoten, einschließlich Knoten, die gemeinsam genutzte Cluster+HA-Ports verwenden.
1-Cluster-HA	Alle Ports sind für 40/100-GbE konfiguriert. Unterstützt Shared Cluster/HA-Datenverkehr auf Ports. Erforderlich für Systeme AFF A320, AFF A250 und FAS500f Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
1-Cluster-HA-Breakout an	Die Ports sind für 4x10-GbE-Breakout, 4x25-GbE-Breakout (RCF 1.6+ auf 100-GbE-Switches) und 40/100-GbE-Breakout konfiguriert. Unterstützt Shared-Cluster-/HA-Traffic auf Ports für Nodes, die Shared-Cluster/HA-Ports verwenden: AFF A320, AFF A250 und FAS500f Systeme. Darüber hinaus können alle Ports als dedizierte Cluster-Ports verwendet werden.
Cluster-HA-Storage	Die Ports sind für 40/100GbE für Cluster+HA, 4x10GbE Breakout für Cluster und 4x25GbE Breakout für Cluster+HA sowie 100GbE für jedes Storage-HA-Paar konfiguriert.
Cluster	Zwei Varianten von RCF mit unterschiedlicher Belegung von 4x10GbE-Ports (Breakout) und 40/100GbE-Ports. Alle FAS und AFF Knoten werden unterstützt, mit Ausnahme der Systeme AFF A320, AFF A250 und FAS500f .
Storage	Alle Ports sind für 100-GbE-NVMe-Storage-Verbindungen konfiguriert.

### Vorgeschlagene Dokumentation

- "[Cisco Ethernet-Switches](#)"

In der Tabelle zur Switch-Kompatibilität finden Sie Informationen zu den unterstützten ONTAP- und RCF-Versionen auf der NetApp Support-Website. Beachten Sie, dass es zwischen der Befehlssyntax in der RCF

und der Syntax in bestimmten Versionen von NX-OS Befehlssyntax bestehen kann.

- ["Switches Der Cisco Nexus 9000-Serie"](#)

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

### Zu den Beispielen

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

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

Siehe die ["Hardware Universe"](#) um die richtigen Ports auf Ihrer Plattform zu überprüfen.



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

### Verwendete Befehle

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

### Was kommt als Nächstes?

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

### Installieren Sie die Referenzkonfigurationsdatei

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

Weitere Informationen zur Installation des RCF finden Sie im Knowledge Base-Artikel ["Löschen der Konfiguration auf einem Cisco Interconnect Switch bei Beibehaltung der Remote-Verbindung"](#).

### Bevor Sie beginnen

Überprüfen Sie die folgenden Installationen und Verbindungen:

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

### Schritt 1: Installieren Sie die RCF auf den Schaltern

1. Melden Sie sich an, um cs1 über SSH oder über eine serielle Konsole zu wechseln.

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

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

#### Beispiel anzeigen

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

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

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

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

#### Beispiel anzeigen

Dieses Beispiel zeigt die RCF Nexus\_9336C\_RCF\_v1.6-Storage.txt, die auf Switch cs1 installiert wird:

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

4. Überprüfen Sie die Bannerausgabe des `show banner motd` Befehls. Sie müssen diese Anweisungen lesen und befolgen, um die richtige Konfiguration und den korrekten Betrieb des Switches sicherzustellen.

## Beispiel anzeigen

```
cs1# show banner motd
```

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

5. Stellen Sie sicher, dass der RCF die richtige neuere Version ist:

```
show running-config
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

10. Überprüfen Sie, ob die write\_erase.cfg Die Datei wird wie erwartet ausgefüllt:

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

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

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

13. Starten Sie den Switch cs1 neu.

```
cs1# reload
```

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

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

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

## Schritt 2: Überprüfen Sie die Switch-Verbindungen

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

```
show interface brief
```



## Beispiel anzeigen

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

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

```
show vlan brief
```

```
show interface trunk
```

## Beispiel anzeigen

```
cs1# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Po999
30	VLAN0030	active	Eth1/1, Eth1/2, Eth1/3, Eth1/4  Eth1/5, Eth1/6, Eth1/7, Eth1/8  Eth1/9, Eth1/10, Eth1/11  Eth1/12, Eth1/13, Eth1/14  Eth1/15, Eth1/16, Eth1/17  Eth1/18, Eth1/19, Eth1/20  Eth1/21, Eth1/22, Eth1/23  Eth1/24, Eth1/25, Eth1/26  Eth1/27, Eth1/28, Eth1/29  Eth1/30, Eth1/31, Eth1/32  Eth1/33, Eth1/34, Eth1/35  Eth1/36

```
cs1# show interface trunk
```

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

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

-----

-----

Port	Vlans Allowed on Trunk
------	------------------------

-----

-----

Eth1/1	30
Eth1/2	30
Eth1/3	30
Eth1/4	30
Eth1/5	30
Eth1/6	30
Eth1/7	30
Eth1/8	30
Eth1/9	30
Eth1/10	30
Eth1/11	30
Eth1/12	30

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

-----  
-----

Port	Vlans Err-disabled on Trunk
------	-----------------------------

-----  
-----

Eth1/1	none
Eth1/2	none
Eth1/3	none
Eth1/4	none
Eth1/5	none
Eth1/6	none
Eth1/7	none
Eth1/8	none
Eth1/9	none
Eth1/10	none
Eth1/11	none
Eth1/12	none
Eth1/13	none
Eth1/14	none
Eth1/15	none
Eth1/16	none

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

-----  
-----

Port	STP Forwarding
------	----------------

-----  
-----

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

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

```

-----
-----
Port          Vlans in spanning tree forwarding state and not pruned
-----
-----

```

Eth1/1	Feature VTP is not enabled
none	
Eth1/2	Feature VTP is not enabled
none	
Eth1/3	Feature VTP is not enabled
none	
Eth1/4	Feature VTP is not enabled
none	
Eth1/5	Feature VTP is not enabled
none	
Eth1/6	Feature VTP is not enabled
none	
Eth1/7	Feature VTP is not enabled
none	
Eth1/8	Feature VTP is not enabled
none	
Eth1/9	Feature VTP is not enabled
none	
Eth1/10	Feature VTP is not enabled
none	
Eth1/11	Feature VTP is not enabled
30	
Eth1/12	Feature VTP is not enabled
30	

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

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



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

### Schritt 3: Richten Sie Ihren ONTAP-Cluster ein

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

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

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

#### Was kommt als Nächstes?

Nach der Installation Ihres RCF können Sie ["Überprüfen Sie die SSH-Konfiguration"](#)

#### Aktualisieren der Referenzkonfigurationsdatei (RCF)

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

#### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

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

Wenn Sie die Startkonfiguration ändern müssen, um die aktuellen Startabbilder zu berücksichtigen, müssen Sie dies vor dem erneuten Anwenden des RCF tun, damit die korrekte Version bei zukünftigen Neustarts instanziiert wird.



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



Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Switch-Einstellungen löschen und die Grundkonfiguration durchführen. Sie müssen über die serielle Konsole mit dem Switch verbunden sein oder grundlegende Konfigurationsinformationen beibehalten haben, bevor Sie die Switch-Einstellungen löschen.



## Schritt 1: Bereiten Sie sich auf das Upgrade vor

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

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

Wobei x die Dauer des Wartungsfensters in Stunden angibt.

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

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (\*>) wird angezeigt.

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

```
network device-discovery show
```

### Beispiel anzeigen

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

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

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

## Beispiel anzeigen

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

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

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

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

## Schritt 2: Ports konfigurieren

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

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



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

2. Überprüfen Sie, ob für die Cluster-LIFs ein Failover auf die auf Switch cs1 gehosteten Ports durchgeführt wurde. Dies kann einige Sekunden dauern.

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

### Beispiel anzeigen

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

	Logical	Status	Network	Current
Current Is				
Vserver	Interface	Admin/Oper	Address/Mask	Node
Port	Home			
-----	-----	-----	-----	
-----	-----			
Cluster				
	node1-01_clus1	up/up	169.254.36.44/16	node1-01
e7a	true			
	node1-01_clus2	up/up	169.254.7.5/16	node1-01
e7b	true			
	node1-02_clus1	up/up	169.254.197.206/16	node1-02
e7a	true			
	node1-02_clus2	up/up	169.254.195.186/16	node1-02
e7b	true			
	node1-03_clus1	up/up	169.254.192.49/16	node1-03
e7a	true			
	node1-03_clus2	up/up	169.254.182.76/16	node1-03
e7b	true			
	node1-04_clus1	up/up	169.254.59.49/16	node1-04
e7a	true			
	node1-04_clus2	up/up	169.254.62.244/16	node1-04
e7b	true			

```
8 entries were displayed.
```

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

```
cluster show
```

## Beispiel anzeigen

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

4 entries were displayed.
```

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

```
show running-config
```

- Notieren Sie alle benutzerdefinierten Ergänzungen zwischen dem aktuellen `running-config` und die verwendete RCF-Datei (z. B. eine SNMP-Konfiguration für Ihre Organisation).
  - Für NX-OS 10.2 und höher verwenden Sie die `show diff running-config` Befehl zum Vergleich mit der gespeicherten RCF-Datei im Bootflash. Alternativ können Sie ein Vergleichstool eines Drittanbieters verwenden.
5. Speichern Sie grundlegende Konfigurationsdetails im `write_erase.cfg` Datei auf dem Bootflash.



Stellen Sie sicher, dass Sie Folgendes konfigurieren:

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

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

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

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

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

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

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

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

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

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

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

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

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

```
cs1# write erase
```

Warning: This command will erase the startup-configuration.

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

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

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

10. Starten Sie den Switch neu:

```
cs1# reload
```

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

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

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

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

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

### Beispiel anzeigen

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

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

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

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

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

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



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

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

```
show running-config
```

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

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

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

15. Wenden Sie alle vorherigen Anpassungen erneut auf die Switch-Konfiguration an.
16. Nachdem Sie die RCF-Versionen, benutzerdefinierten Ergänzungen und Schaltereinstellungen überprüft haben, kopieren Sie die `running-config` Datei in die `startup-config` Datei.

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

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

```
[ ] 100% Copy complete
```

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

```
cs1# reload
```

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

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

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

#### Beispiel anzeigen

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

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

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

```
cluster show
```

#### Beispiel anzeigen

```
cluster1::*> cluster show
```

Node	Health	Eligibility	Epsilon
-----	-----	-----	-----
node1-01	true	true	false
node1-02	true	true	false
node1-03	true	true	true
node1-04	true	true	false

4 entries were displayed.

20. Wiederholen Sie die Schritte 4 bis 19 auf Switch cs2.

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

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

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

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

```
show interface brief
```

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

```
show cdp neighbors
```

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

```
show vlan brief
```

```
show interface trunk
```

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

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

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

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

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

```
cluster show
```

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

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

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

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



der Konnektivität:

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

### Was kommt als Nächstes?

Nach dem Upgrade Ihres RCF können Sie ["Überprüfen Sie die SSH-Konfiguration"](#) Die

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

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

### Über diese Aufgabe

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

### Schritte

1. Löschen Sie die vorhandene Konfiguration:

```
write erase
```

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

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

2. Laden Sie die Switch-Software neu:

```
reload
```

```
(cs2)# reload
```

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

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

### Was kommt als nächstes

Nachdem Sie Ihre Schalter zurückgesetzt haben, können Sie ["neu konfigurieren"](#) sie nach Bedarf.

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

Sie können defekte Nexus 9336C-FX2- und 9336C-FX2-T-Switches in einem

Clusternetzwerk ersetzen. Dies ist ein unterbrechungsfreies Verfahren.

### Bevor Sie beginnen

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

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

Switches Der Cisco Nexus 3000-Serie:

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

### Über diese Aufgabe

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

Schritte zur Fertigstellung:

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



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

### Schritte

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

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

X ist die Dauer des Wartungsfensters in Stunden.

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

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

#### Beispiel anzeigen

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

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

```
storage::*>
```

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

```
network device-discovery show
```

## Beispiel anzeigen

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

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

```
show lldp neighbors
```

## Beispiel anzeigen

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

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

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

**Beispiel anzeigen**

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

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

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

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

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

**Beispiel anzeigen**

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

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

```
network device-discovery show
```

**Beispiel anzeigen**

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

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

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

## Beispiel anzeigen

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

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

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

### Was kommt als Nächstes?

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

## NVIDIA SN2100

### Los geht's

#### Installations- und Einrichtungsworkflow für NVIDIA SN2100-Switches

Der NVIDIA SN2100 ist ein Ethernet Switch, mit dem Sie Daten zwischen Controllern und Platten-Shelves wechseln können.

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

1

#### "Überprüfen der Konfigurationsanforderungen"

Überprüfen Sie die Konfigurationsanforderungen für den SN2100-Speicherswitch.

2

#### "Überprüfen Sie die Komponenten und Teilenummern"

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

**3**

### "Überprüfen Sie die erforderlichen Unterlagen"

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

**4**

### "Installieren Sie die Hardware"

Installieren Sie die Switch-Hardware.

**5**

### "Konfigurieren der Software"

Konfigurieren Sie die Switch-Software.

## Konfigurationsanforderungen für NVIDIA SN2100 Switches

Prüfen Sie bei Installation und Wartung von NVIDIA SN2100-Switches alle Anforderungen.

### Installationsvoraussetzungen

Wenn Sie ONTAP Cluster mit mehr als zwei Nodes erstellen möchten, sind zwei unterstützte Cluster-Netzwerk-Switches erforderlich. Sie können zusätzliche, optionale Management Switches verwenden.

Sie installieren den NVIDIA SN2100-Switch (X190006/X190106) im NVIDIA-Dual/Single-Switch-Gehäuse mit den im Lieferumfang des Switches enthaltenen Standardhalterungen.

Richtlinien zur Verkabelung finden Sie unter "[Überlegungen zur Verkabelung und Konfiguration](#)".

### ONTAP und Linux Unterstützung

Der NVIDIA SN2100 Switch ist ein 10/25/40/100 GB Ethernet-Switch mit Cumulus Linux. Der Switch unterstützt Folgendes:

- ONTAP 9.10.1P3. Der SN2100 Switch dient Cluster- und Speicheranwendungen in ONTAP 9.10.1P3 über verschiedene Switch-Paare. Ab ONTAP 9.10.1P3 können Sie mit NVIDIA SN2100 Switches Storage- und Cluster-Funktionen in einer gemeinsamen Switch-Konfiguration kombinieren.
- Cumulus Linux (CL) OS-Version 4.4.3. Aktuelle Informationen zur Kompatibilität finden Sie im "[NVIDIA Ethernet-Switches](#)" Informationsseite.
- Sie können Cumulus Linux installieren, wenn auf dem Switch Cumulus Linux oder ONIE ausgeführt wird.

### Was kommt als nächstes

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

## Komponenten und Teilenummern für NVIDIA SN2100-Switches

Lesen Sie bei der Installation und Wartung von NVIDIA SN2100-Switches die Liste der Komponenten und Teilenummern für Schrank und Schienensatz.



## Rack-Details

Sie installieren den NVIDIA SN2100-Switch (X190006/X190106) im NVIDIA-Dual/Single-Switch-Gehäuse mit den im Lieferumfang des Switches enthaltenen Standardhalterungen.

## Einzelheiten zum Schienensatz

In der folgenden Tabelle sind die Teilenummer und Beschreibung der MSN2100-Switches und Schienen-Kits aufgeführt:

Teilenummer	Beschreibung
X190006-PE	Cluster Switch, NVIDIA SN2100, 16 PT 100 G, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16 PT 100 G, PSIN
X190106-FE-PE	Switch, NVIDIA SN2100, 16 PT 100 G, PTSX, Frontend
X190106-FE-PI	Switch, NVIDIA SN2100, 16 PT 100G, PSIN, Front End
X-MTEF-KIT-D	Rail Kit, NVIDIA Dual Switch Seite an Seite
X-MTEF-KIT-E	Rail Kit, NVIDIA Single Switch, kurze Tiefe



Weitere Informationen finden Sie in der NVIDIA-Dokumentation auf ["Installieren Sie den SN2100-Switch und den Schienen-Kit"](#).

## Was kommt als nächstes

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

## Dokumentationsanforderungen für NVIDIA SN2100-Switches

Überprüfen Sie bei Installation und Wartung von NVIDIA SN2100-Switches alle empfohlenen Dokumente.

In der folgenden Tabelle ist die Dokumentation für die NVIDIA SN2100-Switches aufgeführt.

Titel	Beschreibung
<a href="#">"NVIDIA SN2100 Switches einrichten und konfigurieren"</a>	Hier wird beschrieben, wie Sie Ihre NVIDIA SN2100-Switches einrichten und konfigurieren, einschließlich der Installation von Cumulus Linux und entsprechenden RCFs.
<a href="#">"Migration von einem Cisco -Speicherswitch zu einem NVIDIA SN2100-Speicherswitch"</a>	Beschreibt, wie Sie von Umgebungen, die Cisco -Speicher-Switches verwenden, zu Umgebungen migrieren, die NVIDIA SN2100-Speicher-Switches verwenden.

Titel	Beschreibung
<a href="#">"Migration zu einem Cluster mit zwei Nodes und NVIDIA SN2100 Cluster Switches"</a>	Hier wird die Migration zu einer Switch-Umgebung mit zwei Nodes mit NVIDIA SN2100-Cluster-Switches beschrieben.
<a href="#">"Einen NVIDIA SN2100-Storage-Switch ersetzen"</a>	Beschreibt das Verfahren zum Austausch eines defekten NVIDIA SN2100-Speicherschalters und Herunterladen von Cumulus Linux und Referenzkonfigurationsdatei.

## Hardware installieren

### Workflow zur Hardwareinstallation für NVIDIA SN2100-Speicherswitches

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

**1**

#### ["Installieren Sie die Hardware"](#)

Installieren Sie die Switch-Hardware.

**2**

#### ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#)

Prüfen Sie die Anforderungen für optische Verbindungen, den QSA-Adapter und die Switch-Port-Geschwindigkeit.

**3**

#### ["Die NS224-Regale verkabeln"](#)

Befolgen Sie die Verkabelungsverfahren, wenn Sie über ein System verfügen, in dem die NS224-Laufwerk-Shelves als Switch-Attached Storage (kein Direct-Attached Storage) verkabelt werden müssen.

### Installieren Sie die Hardware für den NVIDIA SN2100 Switch

Informationen zur Installation der SN2100-Hardware finden Sie in der NVIDIA-Dokumentation.

#### Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen unter ["NVIDIA Switch Installation Guide"](#).

#### Was kommt als Nächstes?

Nachdem Sie Ihre Hardware installiert haben, können Sie ["Verkabelung und Konfiguration überprüfen"](#) Anforderungen.

### Prüfen Sie die Verkabelung und Konfigurationsüberlegungen

Lesen Sie vor der Konfiguration des NVIDIA SN2100-Switches die folgenden Punkte.

## Details zum NVIDIA-Port

Switch-Ports	Verwendung von Ports
Swp1s0-3	4 x 10 GbE Breakout-Cluster-Port-Nodes
Swp2s0-3	4 x 25-GbE-Breakout-Cluster-Port-Nodes
Swp3-14	40/100-GbE-Cluster-Port-Nodes
Swp15-16	100-GbE-Inter-Switch Link-Ports (ISL

Siehe "[Hardware Universe](#)" Weitere Informationen zu Switch-Ports.

## Verbindungsverzögerungen mit optischen Verbindungen

Wenn Sie Verbindungsverzögerungen von mehr als fünf Sekunden haben, bietet Cumulus Linux 5.4 und höher Unterstützung für eine schnelle Verbindungsaufnahme. Sie können die Verknüpfungen mit konfigurieren `nv set` Befehl wie folgt:

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

## Beispiel anzeigen

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

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

Only switchd reload required
```

## Unterstützung für Kupferverbindungen

Die folgenden Konfigurationsänderungen sind erforderlich, um dieses Problem zu beheben.

### Cumulus Linux 4.4.3

1. Benennen Sie die einzelnen Schnittstellen, die 40-GbE-/100-GbE-Kupferkabel verwenden, wie folgt:

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

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

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

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

Beispiel:

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

3. Starten Sie den neu switchd Dienst:

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

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

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

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

## Cumulus Linux 5.x

1. Benennen Sie die einzelnen Schnittstellen, die 40-GbE-/100-GbE-Kupferkabel verwenden, wie folgt:

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

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

2. Konfigurieren Sie die Verknüpfungen mit `nv set` Befehl wie folgt:

- ° `nv set interface <interface-id> link fast-linkup on`
- ° `nv config apply`
- ° Laden Sie den neu switchd Service

Beispiel:

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

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

```
Only switchd reload required
```

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

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

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

[https://kb.netapp.com/Advice\\_and\\_Troubleshooting/Data\\_Storage\\_Systems/Fabric\\_Interconnect\\_and\\_Management\\_Switches/NVIDIA\\_SN2100\\_switch\\_fails\\_to\\_connect\\_using\\_40\\_100GbE\\_copper\\_cable](https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Systems/Fabric_Interconnect_and_Management_Switches/NVIDIA_SN2100_switch_fails_to_connect_using_40_100GbE_copper_cable)["SN2100-Switch stellt keine Verbindung über 40/100-GbE-Kupferkabel her"^]Weitere Informationen finden Sie im Knowledge Base-Artikel.

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

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

#### QSA-Adapter

Wenn ein QSA-Adapter für die Verbindung mit den 10 GbE/25 GbE-Cluster-Ports auf einer Plattform verwendet wird, wird die Verbindung möglicherweise nicht hergestellt.

Gehen Sie wie folgt vor, um dieses Problem zu beheben:

- Stellen Sie bei 10GbE die Verbindungsgeschwindigkeit swp1s0-3 manuell auf 10000 und stellen Sie die automatische Aushandlung auf aus.
- Stellen Sie für 25 GbE die Verbindungsgeschwindigkeit swp2s0-3 manuell auf 25000 ein, und stellen Sie die automatische Aushandlung auf aus.



Wenn Sie 10-GbE-QSA-Adapter verwenden, fügen Sie sie in Breakout-GbE-/100-GbE-Ports (swp3-swp14) ein. Setzen Sie den QSA-Adapter nicht in einen Port ein, der für einen Breakout konfiguriert ist.

#### Stellen Sie die Schnittstellengeschwindigkeit an Breakout-Ports ein

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

### Cumulus Linux 4.4.3

Beispiel:

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

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

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

Überprüfen Sie die Schnittstelle und den Port-Status, um zu überprüfen, ob die Einstellungen angewendet werden:

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

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

## Cumulus Linux 5.x

Beispiel:



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

```
link
```

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

Überprüfen Sie die Schnittstelle und den Port-Status, um zu überprüfen, ob die Einstellungen angewendet werden:

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

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

### Was kommt als Nächstes?

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

### Verkabelung der NS224 Shelves als Switch-Attached Storage

Wenn Sie über ein System verfügen, bei dem die NS224 Laufwerk-Shelves als Switch-Attached Storage verkabelt werden müssen (kein Direct-Attached Storage), verwenden Sie die hier bereitgestellten Informationen.

- Kabel-NS224-Laufwerk-Shelfs über Storage-Switches:

["Informationen zu Verkabelung-Switch-Attached NS224-Laufwerk-Shelfs"](#)

- Installieren Sie Ihre Speicher-Switches:

["Dokumentation zu den Switches von AFF und FAS"](#)

- Bestätigen Sie die unterstützte Hardware, z. B. die Storage-Switches und Kabel, für Ihr Plattformmodell:

["NetApp Hardware Universe"](#)

## Software konfigurieren

### Workflow für die Softwareinstallation von NVIDIA SN2100 Storage-Switches

So installieren und konfigurieren Sie die Software für einen NVIDIA SN2100-Switch:

1

#### ["Konfigurieren Sie den Switch"](#)

Konfigurieren Sie den NVIDIA SN2100-Switch.

2

#### ["Installieren Sie Cumulus Linux im Cumulus-Modus"](#)

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

3

#### ["Installieren Sie Cumulus Linux im ONIE-Modus"](#)

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

4

#### ["Installieren Sie das RCF-Skript \(Reference Configuration File\)"](#)

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Das Verfahren für jedes ist gleich.

5

#### ["Installieren Sie die CSHM-Datei"](#)

Sie können die entsprechende Konfigurationsdatei für die Statusüberwachung von NVIDIA-Cluster-Switches des Ethernet-Switches installieren.

6

#### ["Setzen Sie den Switch auf die Werkseinstellungen zurück"](#)

Löschen Sie die Einstellungen des SN2100-Speicherschalters.

## Konfigurieren Sie den NVIDIA SN2100-Switch

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

### Schritte

1. Überprüfen Sie die ["Konfigurationsanforderungen"](#).
2. Befolgen Sie die Anweisungen unter ["NVIDIA System Bring-up:"](#).

### Was kommt als Nächstes?

Nachdem Sie Ihre Schalter konfiguriert haben, können Sie ["Cumulus Linux im Cumulus-Modus installieren"](#) oder ["Cumulus Linux im ONIE-Modus installieren"](#) Die

## Installieren Sie Cumulus Linux im Cumulus-Modus

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



Cumulus Linux (CL) kann entweder installiert werden, wenn der Switch Cumulus Linux oder ONIE ausführt (siehe ["Im ONIE-Modus installieren"](#)).

### Bevor Sie beginnen

Stellen Sie sicher, dass Folgendes verfügbar ist:

- Linux-Wissen auf mittlerer Ebene.
- Vertrautheit mit grundlegender Textbearbeitung, UNIX-Dateiberechtigungen und Prozessüberwachung. Eine Vielzahl von Texteditoren sind vorinstalliert, einschließlich `vi` und `nano`.
- Zugriff auf eine Linux oder UNIX Shell. Wenn Sie Windows verwenden, verwenden Sie eine Linux-Umgebung als Kommandozeilen-Tool für die Interaktion mit Cumulus Linux.
- Die Baudrate muss auf dem seriellen Konsolen-Switch für den Zugriff auf die NVIDIA SN2100 Switch-Konsole auf 115200 eingestellt werden:
  - 115200 Baud
  - 8 Datenbits
  - 1 Stoppbit
  - Parität: Keine
  - Flusskontrolle: Keine

### Über diese Aufgabe

Beachten Sie Folgendes:



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.



Das Standardpasswort für das Cumulus-Benutzerkonto lautet **Cumulus**. Wenn Sie sich das erste Mal bei Cumulus Linux anmelden, müssen Sie dieses Standardpasswort ändern. Aktualisieren Sie alle Automatisierungsskripts, bevor Sie ein neues Image installieren. Cumulus Linux bietet Befehlszeilenoptionen zum automatischen Ändern des Standardpassworts während des Installationsvorgangs.

## Beispiel 1. Schritte

### Cumulus Linux 4.4.3

1. Melden Sie sich beim Switch an.

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

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

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

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

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standard-Gateway. Der neue Hostname wird erst nach dem Neustart der Konsole/SSH-Sitzung wirksam.



Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0`. Diese Schnittstelle wurde speziell für den Out-of-Band-Management-Einsatz entwickelt. Standardmäßig verwendet die Managementoberfläche DHCPv4 für Adressierung.



Verwenden Sie keine Unterstriche (\_), Apostroph (') oder nicht-ASCII-Zeichen im Hostnamen.

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

Dieser Befehl ändert beide `/etc/hostname` Und `/etc/hosts` Dateien:

4. Vergewissern Sie sich, dass der Hostname, die IP-Adresse, die Subnetzmaske und das Standard-Gateway aktualisiert wurden.

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

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

5. Legen Sie Datum, Uhrzeit, Zeitzone und NTP-Server auf dem Switch fest.

- a. Überprüfen Sie die aktuelle Zeitzone:

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

- b. Auf die neue Zeitzone aktualisieren:

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

- c. Überprüfen Sie Ihre aktuelle Zeitzone:

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

- d. Führen Sie den folgenden Befehl aus, um die Zeitzone mit dem Assistenten festzulegen:

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

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

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

- f. Stellen Sie den aktuellen Wert der Softwareuhr auf die Hardware-Uhr ein:

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

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

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

- h. Überprüfen Sie, ob ntpd auf dem System ausgeführt wird:

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

- i. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig ist die von NTP verwendete Quellschnittstelle eth0. Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

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



6. Installieren Sie Cumulus Linux 4.4.3:

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

Das Installationsprogramm startet den Download. Geben Sie bei Aufforderung \* y\* ein.

7. Starten Sie den NVIDIA SN2100-Switch neu:

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

8. Die Installation wird automatisch gestartet, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Wählen Sie bitte \* nicht\* aus.

- Cumulus-Linux GNU/Linux
- ONIE: Installieren des Betriebssystems
- CUMULUS EINBAUEN
- Cumulus-Linux GNU/Linux

9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.

10. Überprüfen Sie, ob die Cumulus Linux-Version 4.4.3 lautet: `net show version`

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

11. Erstellen Sie einen neuen Benutzer, und fügen Sie diesen Benutzer dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

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

```

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

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

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

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

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

```

## Cumulus Linux 5.4.0

1. Melden Sie sich beim Switch an.

Wenn Sie sich zum ersten Mal am Switch anmelden, benötigen Sie den Benutzernamen/das

Passwort von **cumulus/cumulus** mit **sudo** Berechtigungen.

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

2. Prüfen Sie die Cumulus Linux-Version: **nv show system**

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

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.3.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standard-Gateway. Der neue Hostname wird erst nach dem Neustart der Konsole/SSH-Sitzung wirksam.



Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens **eth0**. Diese Schnittstelle wurde speziell für den Out-of-Band-Management-Einsatz entwickelt. Standardmäßig verwendet die Managementoberfläche DHCPv4 für Adressierung.



Verwenden Sie keine Unterstriche (**\_**), Apostroph (**'**) oder nicht-ASCII-Zeichen im Hostnamen.

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

Dieser Befehl ändert beide **/etc/hostname** Und **/etc/hosts** Dateien:

4. Vergewissern Sie sich, dass der Hostname, die IP-Adresse, die Subnetzmaske und das Standard-Gateway aktualisiert wurden.

```

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

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

```

5. Legen Sie Zeitzone, Datum, Uhrzeit und NTP-Server auf dem Switch fest.

a. Zeitzone einstellen:

```

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

```

b. Überprüfen Sie Ihre aktuelle Zeitzone:

```

cumulus@switch:~$ date +%Z

```

c. Führen Sie den folgenden Befehl aus, um die Zeitzone mit dem Assistenten festzulegen:

```

cumulus@sw1:~$ sudo dpkg-reconfigure tzdata

```

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

```

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

```

e. Stellen Sie den aktuellen Wert der Softwareuhr auf die Hardware-Uhr ein:

```

cumulus@sw1:~$ sudo hwclock -w

```

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

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

Lesen Sie den Knowledge Base-Artikel ["Die NTP-Serverkonfiguration funktioniert nicht mit NVIDIA SN2100-Switches"](#) für weitere Details.

g. Überprüfen Sie, ob ntpd auf dem System ausgeführt wird:

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

h. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig ist die von NTP verwendete Quellschnittstelle eth0 . Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

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

6. Installieren Sie Cumulus Linux 5.4.0:

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

Das Installationsprogramm startet den Download. Geben Sie bei Aufforderung \* y\* ein.

7. Starten Sie den NVIDIA SN2100-Switch neu:

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

8. Die Installation wird automatisch gestartet, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Wählen Sie bitte \* nicht\* aus.

- Cumulus-Linux GNU/Linux
- ONIE: Installieren des Betriebssystems
- CUMULUS EINBAUEN
- Cumulus-Linux GNU/Linux

9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.

10. Stellen Sie sicher, dass die Cumulus Linux-Version 5.4 ist: `nv show system`

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

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 13:37:36	system uptime
timezone	Etc/UTC	system time zone

11. Stellen Sie sicher, dass die Nodes jeweils über eine Verbindung zu jedem Switch verfügen:

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

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

12. Erstellen Sie einen neuen Benutzer, und fügen Sie diesen Benutzer dem hinzu `sudo` Gruppieren. Dieser Benutzer wird erst wirksam, nachdem die Konsole/SSH-Sitzung neu gestartet wurde.

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

```

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

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

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

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

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

```

13. Fügen Sie zusätzliche Benutzergruppen hinzu, auf die der Admin-Benutzer zugreifen kann `nv` Befehl:

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

Siehe ["NVIDIA Benutzerkonten"](#) Finden Sie weitere Informationen.

## Cumulus Linux 5.11.0

### 1. Melden Sie sich beim Switch an.

Wenn Sie sich zum ersten Mal beim Switch anmelden, benötigt er den Benutzernamen/das Passwort von **cumulus/cumulus** mit `sudo` Privileges.

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

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

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

operational	applied	description
hostname	cumulus	cumulus
build	Cumulus Linux 5.4.0	system build version
uptime	6 days, 8:37:36	system uptime
timezone	Etc/UTC	system time zone

### 3. Konfigurieren Sie den Hostnamen, die IP-Adresse, die Subnetzmaske und das Standard-Gateway. Der neue Hostname wird erst nach dem Neustart der Konsole/SSH-Sitzung wirksam.



Ein Cumulus Linux-Switch bietet mindestens einen dedizierten Ethernet-Management-Port namens `eth0`. Diese Schnittstelle wurde speziell für den Out-of-Band-Management-Einsatz entwickelt. Standardmäßig verwendet die Managementoberfläche DHCPv4 für Adressierung.



Verwenden Sie keine Unterstriche (`_`), Apostroph (`'`) oder nicht-ASCII-Zeichen im Hostnamen.



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

Dieser Befehl ändert beide /etc/hostname Und /etc/hosts Dateien:

4. Vergewissern Sie sich, dass der Hostname, die IP-Adresse, die Subnetzmaske und das Standard-Gateway aktualisiert wurden.

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

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

5. Legen Sie Zeitzone, Datum, Uhrzeit und NTP-Server auf dem Switch fest.

- a. Zeitzone einstellen:

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

- b. Überprüfen Sie Ihre aktuelle Zeitzone:

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

- c. Führen Sie den folgenden Befehl aus, um die Zeitzone mit dem Assistenten festzulegen:

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

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

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

- e. Stellen Sie den aktuellen Wert der Softwareuhr auf die Hardware-Uhr ein:

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

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

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

Lesen Sie den Knowledge Base-Artikel ["Die NTP-Serverkonfiguration funktioniert nicht mit NVIDIA SN2100-Switches"](#) für weitere Details.

- g. Überprüfen Sie, ob ntpd auf dem System ausgeführt wird:

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

- h. Geben Sie die NTP-Quellschnittstelle an. Standardmäßig ist die von NTP verwendete Quellschnittstelle eth0 . Sie können eine andere NTP-Quellschnittstelle wie folgt konfigurieren:

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

6. Installieren Sie Cumulus Linux 5.11.0:

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

Das Installationsprogramm startet den Download. Geben Sie bei Aufforderung \* y\* ein.

7. Starten Sie den NVIDIA SN2100-Switch neu:

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

8. Die Installation wird automatisch gestartet, und die folgenden GRUB-Bildschirmoptionen werden angezeigt. Wählen Sie bitte \* nicht\* aus.
  - Cumulus-Linux GNU/Linux
  - ONIE: Installieren des Betriebssystems
  - CUMULUS EINBAUEN
  - Cumulus-Linux GNU/Linux
9. Wiederholen Sie die Schritte 1 bis 4, um sich anzumelden.
10. Überprüfen Sie, ob die Cumulus Linux-Version 5.11.0 lautet:

```
nv show system
```

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

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

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

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

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

Weitere Informationen finden Sie unter ["NVIDIA Benutzerkonten"](#) .

### Was kommt als Nächstes?

Nach der Installation von Cumulus Linux im Cumulus-Modus können Sie ["Installieren oder aktualisieren Sie das RCF-Skript"](#) Die

### Installieren Sie Cumulus Linux im ONIE-Modus

Gehen Sie folgendermaßen vor, um Cumulus Linux (CL) OS zu installieren, wenn der Switch im ONIE-Modus ausgeführt wird.



Cumulus Linux (CL) kann entweder installiert werden, wenn der Switch Cumulus Linux oder ONIE ausführt (siehe ["Im Cumulus-Modus installieren"](#)).

### Über diese Aufgabe

Sie können Cumulus Linux unter Verwendung der Open Network Install Environment (ONIE) installieren, die die automatische Erkennung eines Network Installer-Images ermöglicht. Dies erleichtert das Systemmodell der Sicherung von Schaltern mit einem Betriebssystem, wie Cumulus Linux. Die einfachste Möglichkeit, Cumulus Linux mit ONIE zu installieren, ist mit lokaler HTTP-Erkennung.



Wenn Ihr Host IPv6 aktiviert ist, stellen Sie sicher, dass er einen Webserver ausführt. Wenn der Host IPv4 aktiviert ist, stellen Sie sicher, dass er zusätzlich zu einem Webserver DHCP ausführt.

Dieses Verfahren zeigt, wie Cumulus Linux nach dem Start des Administrators in ONIE aktualisiert werden kann.

## Schritte

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Benennen Sie diese Datei um `onie-installer`.
2. Verbinden Sie den Host über ein Ethernet-Kabel mit dem Management-Ethernet-Port des Switches.
3. Schalten Sie den Schalter ein. Der Switch lädt das ONIE-Image-Installationsprogramm herunter und startet. Nach Abschluss der Installation wird die Cumulus Linux-Anmeldeaufforderung im Terminalfenster angezeigt.



Jedes Mal, wenn Cumulus Linux installiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut.

4. Starten Sie den SN2100-Schalter neu:

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

5. Drücken Sie die Taste **Esc** auf dem GNU GRUB-Bildschirm, um den normalen Bootvorgang zu unterbrechen, wählen Sie **ONIE** und drücken Sie **Enter**.
6. Wählen Sie auf dem nächsten Bildschirm **ONIE: Install OS** aus.
7. Der Vorgang zur Erkennung des ONIE-Installers führt die Suche nach der automatischen Installation durch. Drücken Sie **Enter**, um den Vorgang vorübergehend zu beenden.
8. Wenn der Erkennungsvorgang angehalten wurde:

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

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

```
ifconfig eth0
```

## Beispiel anzeigen

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

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

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

10. Wenn das IP-Adressschema manuell definiert ist, gehen Sie wie folgt vor:

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

11. Wiederholen Sie Schritt 9, um zu überprüfen, ob die statischen Informationen korrekt eingegeben wurden.

12. Cumulus Linux Installieren:

```
ONIE:/ # route
```

```
Kernel IP routing table
```

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

```
Stopping: discover... done.
```

```
Info: Attempting
```

```
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-4.4.3-mlx-amd64.bin ...
```

```
Connecting to 10.60.132.97 (10.60.132.97:80)
```

```
installer          100% |*|    552M  0:00:00 ETA
```

```
...
```

```
...
```

13. Nach Abschluss der Installation melden Sie sich beim Switch an:

#### Beispiel anzeigen

```
cumulus login: cumulus
```

```
Password: cumulus
```

```
You are required to change your password immediately (administrator enforced)
```

```
Changing password for cumulus.
```

```
Current password: cumulus
```

```
New password: <new_password>
```

```
Retype new password: <new_password>
```

14. Überprüfen Sie die Cumulus Linux-Version:

```
net show version
```

#### Beispiel anzeigen

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

```
NCLU_VERSION=1.0-cl4.4.3u4
```

```
DISTRIB_ID="Cumulus Linux"
```

```
DISTRIB_RELEASE=4.4.3
```

```
DISTRIB_DESCRIPTION="Cumulus Linux 4.4.3"
```

Was kommt als Nächstes?

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

## Installieren oder aktualisieren Sie das RCF-Skript

Gehen Sie wie folgt vor, um das RCF-Skript zu installieren oder zu aktualisieren.

### Bevor Sie beginnen

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

- Cumulus Linux 4.4.3 ist installiert.
- IP-Adresse, Subnetzmaske und Standard-Gateway über DHCP oder manuell konfiguriert definiert.

### Aktuelle RCF-Skriptversionen

Für Clustering- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. Das Verfahren für jedes ist gleich.

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



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



Die Befehlsausgabe des Switch-Management verwendet die Switch-Management-IP-Adresse 10.233.204.71, die Netmask 255.255.254.0 und das Standard-Gateway 10.233.204.1.

### Schritte

1. Zeigen Sie die verfügbaren Schnittstellen am SN2100-Schalter an:

```
net show interface all
```



## Beispiel anzeigen

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

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

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

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

3. Anwenden des RCF-Python-Skripts **MSN2100-RCF-v1.8-Cluster**:

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

Das RCF-Skript führt die oben aufgeführten Schritte durch.



Für Probleme mit RCF-Python-Skripts, die nicht behoben werden können, wenden Sie sich an ["NetApp Support"](#) Für weitere Unterstützung.

4. Wenden Sie alle vorherigen Anpassungen erneut auf die Switch-Konfiguration an. ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#) Weitere Informationen zu erforderlichen Änderungen finden Sie unter.
5. Überprüfen Sie die Konfiguration nach dem Neustart:

```
net show interface all
```

## Beispiel anzeigen

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

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

```

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

```

```
cumulus@cumulus:mgmt:~$ net show roce config
```

```
RoCE mode..... lossless
```

```
Congestion Control:
```

```
Enabled SPs.... 0 2 5
```

```
Mode..... ECN
```

```
Min Threshold.. 150 KB
```

```
Max Threshold.. 1500 KB
```

```
PFC:
```

```
Status..... enabled
```

```
Enabled SPs.... 2 5
```

```
Interfaces..... swp10-16,swp1s0-3,swp2s0-3,swp3-9
```

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

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

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

```
net show interface pluggables
```

### Beispiel anzeigen

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

Interface	Identifier	Vendor Name	Vendor PN	Vendor SN
Vendor Rev				
swp3	0x11 (QSFP28)	Amphenol	112-00574	
APF20379253516	B0			
swp4	0x11 (QSFP28)	AVAGO	332-00440	AF1815GU05Z
A0				
swp15	0x11 (QSFP28)	Amphenol	112-00573	
APF21109348001	B0			
swp16	0x11 (QSFP28)	Amphenol	112-00573	
APF21109347895	B0			

7. Stellen Sie sicher, dass die Nodes jeweils über eine Verbindung zu jedem Switch verfügen:

```
net show lldp
```

### Beispiel anzeigen

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

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

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

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

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

## Beispiel anzeigen

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

Node: node1

Ignore

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

Node: node2

Ignore

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

- a. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den Switch sw2 an, da LIFs nicht auf e0d homed sind).

## Beispiel anzeigen

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

Node/	Local	Discovered		
Protocol	Port	Device (LLDP: ChassisID)	Interface	Platform
-----	-----	-----	-----	-----
node1/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp3	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp3	-
node2/lldp				
	e3a	sw1 (b8:ce:f6:19:1a:7e)	swp4	-
	e3b	sw2 (b8:ce:f6:19:1b:96)	swp4	-

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

Switch	Type	Address
Model		
-----	-----	-----
sw1	cluster-network	10.233.205.90
MSN2100-CB2RC		
Serial Number: MNXXXXXXGD		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 4.4.3 running on Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		
sw2	cluster-network	10.233.205.91
MSN2100-CB2RC		
Serial Number: MNCXXXXXXGS		
Is Monitored: true		
Reason: None		
Software Version: Cumulus Linux version 4.4.3 running on Mellanox		
Technologies Ltd. MSN2100		
Version Source: LLDP		

### Was kommt als Nächstes?

Nach der Installation oder Aktualisierung des RCF können Sie ["Installieren Sie die CSHM-Datei"](#) Die

## Installieren Sie die Konfigurationsdatei des Ethernet Switch Health Monitor

Gehen Sie wie folgt vor, um die entsprechende Konfigurationsdatei für die Statusüberwachung von NVIDIA-Cluster-Switches über Ethernet-Switches zu installieren. Folgende Modelle werden unterstützt:

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



Dieses Installationsverfahren gilt für ONTAP 9.10.1 und höher.

### Bevor Sie beginnen

- Überprüfen Sie, ob Sie die Konfigurationsdatei herunterladen müssen, indem Sie ausführen `system switch ethernet show` und prüfen, ob **ANDERE** für Ihr Modell angezeigt wird.

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

- Stellen Sie sicher, dass das ONTAP Cluster betriebsbereit ist und ausgeführt wird.
- Aktivieren Sie SSH, um alle in CSHM verfügbaren Funktionen zu verwenden.
- Löschen Sie das `/mroot/etc/cshm_nod/nod_sign/` Verzeichnis auf allen Knoten:

- a. Betreten Sie die Nodeshell:

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

- b. Zu erweiterten Berechtigungen wechseln:

```
priv set advanced
```

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

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

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

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

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

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

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

### Schritte



1. Laden Sie die ZIP-Datei für die Konfiguration der Ethernet-Switch-Systemzustandsüberwachung basierend auf der entsprechenden ONTAP-Version herunter. Diese Datei ist auf der Seite verfügbar "[NVIDIA Ethernet-Switches](#)".
  - a. Wählen Sie auf der Download-Seite der NVIDIA SN2100-Software **Nvidia CSHM-Datei** aus.
  - b. Aktivieren Sie auf der Seite Achtung/muss gelesen werden das Kontrollkästchen, um zuzustimmen.
  - c. Aktivieren Sie auf der Seite Endbenutzer-Lizenzvereinbarung das Kontrollkästchen, um zuzustimmen, und klicken Sie auf **Akzeptieren und Fortfahren**.
  - d. Wählen Sie auf der Seite Nvidia CSHM File - Download die entsprechende Konfigurationsdatei aus. Folgende Dateien sind verfügbar:

#### **ONTAP 9.15.1 und höher**

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

#### **ONTAP 9.11.1 bis 9.14.1**

- MSN2100-CB2FC\_PRIOR\_R9.15.1-v1.4.zip
- MSN2100-CB2RC\_PRIOR\_R9.15.1-v1.4.zip
- X190006-PE\_PRIOR\_9.15.1-v1.4.zip
- X190006-PI\_PRIOR\_9.15.1-v1.4.zip

1. Laden Sie die entsprechende ZIP-Datei auf Ihren internen Webserver hoch.
2. Greifen Sie von einem der ONTAP-Systeme im Cluster aus auf den erweiterten Modus zu.

```
set -privilege advanced
```

3. Führen Sie den Befehl Switch Health Monitor configure aus.

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

4. Überprüfen Sie, ob die Befehlsausgabe mit dem folgenden Text für Ihre ONTAP-Version endet:

#### **ONTAP 9.15.1 und höher**

Die Konfigurationsdatei wurde von der Statusüberwachung des Ethernet-Switches installiert.

#### **ONTAP 9.11.1 bis 9.14.1**

SHM hat die Konfigurationsdatei installiert.

#### **ONTAP 9.10.1**

Das heruntergeladene CSHM-Paket wurde erfolgreich verarbeitet.

Sollte ein Fehler auftreten, wenden Sie sich an den NetApp Support.

1. Warten Sie bis zu zweimal das Abfrageintervall der Ethernet-Switch-Integritätsüberwachung, das durch Ausführen gefunden ``system switch ethernet polling-interval show`` wird, bevor Sie den nächsten Schritt abschließen.
2. Führen Sie den Befehl aus `system switch ethernet configure-health-monitor show` Stellen Sie im ONTAP -System sicher, dass die Cluster-Switches erkannt werden, wobei das überwachte Feld auf **True** gesetzt ist und das Feld für die Seriennummer nicht **Unknown** anzeigt.

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

### Was kommt als Nächstes?

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

### Setzen Sie den SN2100-Speicherschalter auf die Werkseinstellungen zurück

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

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

### Über diese Aufgabe

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



Weitere Informationen zur Installation von Cumulus Linux finden Sie unter "[Workflow für die Softwareinstallation von NVIDIA SN2100-Switches](#)".

## Beispiel 2. Schritte

### Cumulus Linux 5.10 und früher

1. Laden Sie die Switch-Softwareinstallation von der Cumulus-Konsole herunter und stellen Sie sie mit dem Befehl in die Warteschlange. `onie-install -a -i http://<web-server>/<path>/cumulus-linux-5.10.0-mlx-amd64.bin`

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

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

```
sudo reboot
```

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



Der Switch startet neu und beginnt mit der Installation der Switch-Software, was einige Zeit in Anspruch nimmt. Wenn die Installation abgeschlossen ist, startet der Switch neu und bleibt auf dem `log-in` prompt.

### Cumulus Linux 5.11 und höher

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

```
nv action reset system factory-default
```

Beispiel:

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

```
This operation will reset the system configuration, delete the log files and reboot the switch.
```

```
Type [y] continue.
```

```
Type [n] to abort.
```

```
Do you want to continue? [y/n] y
```

Sehen Sie sich die NVIDIA "[Werksreset](#)" Weitere Einzelheiten finden Sie in der Dokumentation.

### Was kommt als nächstes

Nachdem Sie Ihre Schalter zurückgesetzt haben, können Sie "[neu konfigurieren](#)" sie nach Bedarf.

## Switches migrieren

### Migrieren Sie von einem Cisco Storage Switch auf einen NVIDIA SN2100 Storage-Switch

Sie können ältere Cisco Switches für ein ONTAP Cluster zu NVIDIA SN2100 Storage Switches migrieren. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

#### Prüfen Sie die Anforderungen

Folgende Storage-Switches werden unterstützt:

- Cisco Nexus 9336C-FX2
- Cisco Nexus 3232C
- Siehe "[Hardware Universe](#)" Erhalten Sie ausführliche Informationen zu den unterstützten Ports und deren Konfigurationen.

#### Bevor Sie beginnen

Stellen Sie sicher, dass Sie über Folgendes verfügen:

- Das vorhandene Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Storage-Ports befinden sich im Status up, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die NVIDIA SN2100-Speicherschalter sind konfiguriert und funktionieren unter der richtigen Version von Cumulus Linux, die mit der verwendeten Referenzkonfigurationsdatei (RCF) installiert wird.
- Die vorhandene Speichernetzwerkconfiguration verfügt über folgende Merkmale:
  - Ein redundantes und voll funktionsfähiges NetApp Cluster unter Verwendung beider älteren Cisco Switches.
  - Management-Konnektivität und Konsolenzugriff auf die älteren Cisco Switches und die neuen Switches.
  - Alle Cluster-LIFs im Status „up“ mit den Cluster-LIFs befinden sich auf den Home-Ports.
  - ISL-Ports aktiviert und zwischen den älteren Cisco Switches und zwischen den neuen Switches verkabelt.
- Siehe "[Hardware Universe](#)" Erhalten Sie ausführliche Informationen zu den unterstützten Ports und deren Konfigurationen.
- Einige der Ports sind auf NVIDIA SN2100-Switches für 100 GbE konfiguriert.
- Sie haben 100-GbE-Konnektivität von Nodes zu NVIDIA SN2100 Storage-Switches geplant, migriert und dokumentiert.

#### Migrieren Sie die Switches

##### Zu den Beispielen

In diesem Verfahren werden Cisco Nexus 9336C-FX2 Storage-Switches zum Beispiel Befehle und Ausgänge verwendet.

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

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

- Die Knoten sind *node1* und *node2*.
- Die Cluster-LIFs sind auf Node 1 *\_clus1\_* und *node1\_clus2* und *node2\_clus1* bzw. *node2\_clus2* auf Knoten 2.
- Der `cluster1::*>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Netzwerk-Ports sind *e5a* und *e5b*.
- Breakout-Ports haben das Format *swp1s0-3*. Zum Beispiel sind vier Breakout-Ports auf *swp1 swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.
- Schalter S2 wird zuerst durch Schalter *sw2* ersetzt und dann Schalter S1 durch Schalter *sw1* ersetzt.
  - Die Verkabelung zwischen den Knoten und S2 wird dann von S2 getrennt und wieder mit *sw2* verbunden.
  - Die Verkabelung zwischen den Knoten und S1 wird dann von S1 getrennt und wieder mit *sw1* verbunden.

### Schritt: Bereiten Sie sich auf die Migration vor

1. Wenn AutoSupport aktiviert ist, unterdrücken Sie die automatische Erstellung eines Cases durch Aufrufen einer AutoSupport Meldung:

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

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

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

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung (*\*>*) wird angezeigt.

3. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Storage-Schnittstellen fest:

Jeder Port sollte für aktiviert angezeigt werden *Status*.

### Schritt: Kabel und Ports konfigurieren

1. Zeigen Sie die Attribute des Netzwerkports an:

```
storage port show
```

## Beispiel anzeigen

```
cluster1::*> storage port show
```

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

```
cluster1::*>
```

2. Überprüfen Sie mithilfe des Befehls, ob die Storage-Ports auf jedem Node (aus Sicht der Nodes) auf folgende Weise mit vorhandenen Storage-Switches verbunden sind:

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

## Beispiel anzeigen

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

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

3. Stellen Sie am Schalter S1 und S2 sicher, dass die Speicheranschlüsse und -Schalter (aus der Perspektive der Switches) mit dem Befehl wie folgt verbunden sind:

```
show lldp neighbors
```

## Beispiel anzeigen

S1# **show lldp neighbors**

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS  
Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

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

S2# **show lldp neighbors**

Capability Codes: (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS  
Cable Device,

(W) WLAN Access Point, (P) Repeater, (S) Station

(O) Other

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

4. Fahren Sie beim Switch sw2 die mit den Storage-Ports und den Nodes der Festplatten-Shelfs verbundenen Ports herunter.

#### Beispiel anzeigen

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

5. Verschieben Sie die Node Storage Ports des Controllers und der Festplatten-Shelfs vom alten Switch S2 auf den neuen Switch sw2. Verwenden Sie dazu die geeignete Verkabelung, die von NVIDIA SN2100 unterstützt wird.
6. Stellen Sie beim Switch sw2 die Ports bereit, die mit den Speicherports der Knoten und der Festplatten-Shelfs verbunden sind.

#### Beispiel anzeigen

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

7. Vergewissern Sie sich, dass die Storage-Ports auf jedem Node aus Sicht der Nodes nun auf folgende Weise mit den Switches verbunden sind:

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

#### Beispiel anzeigen

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

Node/ Protocol	Local Port	Discovered Device (LLDP: ChassisID)	Interface	Platform
-----				
node1	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	S1 (7c:ad:4f:98:6d:f0)	Eth1/2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-



8. Überprüfen Sie die Netzwerkanschlussattribute:

```
storage port show
```

**Beispiel anzeigen**

```
cluster1::*> storage port show
```

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

9. Vergewissern Sie sich bei Switch sw2, dass alle Knoten Speicher-Ports aktiv sind:

```
net show interface
```

### Beispiel anzeigen

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

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

10. Fahren Sie beim Switch sw1 die Ports herunter, die mit den Speicherports der Knoten und der Platten-Shelves verbunden sind.

### Beispiel anzeigen

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

11. Verschieben Sie die Node Storage Ports des Controllers und der Festplatten-Shelves vom alten Switch S1 zum neuen Switch sw1. Verwenden Sie dazu die geeignete Verkabelung, die von NVIDIA SN2100 unterstützt wird.
12. Bringen Sie am Switch sw1 die Ports auf, die mit den Speicherports der Knoten und den Platten-Shelves verbunden sind.

### Beispiel anzeigen

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

13. Vergewissern Sie sich, dass die Storage-Ports auf jedem Node aus Sicht der Nodes nun auf folgende Weise mit den Switches verbunden sind:

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

### Beispiel anzeigen

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

Node/ Protocol Platform	Local Port	Discovered Device (LLDP: ChassisID)	Interface	
-----				
node1	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp1	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp1	-
node2	/lldp			
	e0c	sw1 (b8:ce:f6:19:1b:96)	swp2	-
	e5b	sw2 (b8:ce:f6:19:1a:7e)	swp2	-

## Schritt 3: Überprüfen Sie die Konfiguration

1. Überprüfen der endgültigen Konfiguration:

```
storage port show
```

Jeder Port sollte für aktiviert angezeigt werden State Und aktiviert für Status.

## Beispiel anzeigen

```
cluster1::*> storage port show
```

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

```
cluster1::*>
```

2. Vergewissern Sie sich bei Switch sw2, dass alle Knoten Speicher-Ports aktiv sind:

```
net show interface
```

## Beispiel anzeigen

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

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

3. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

## Beispiel anzeigen

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

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

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

4. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

5. Wenn Sie die automatische Erstellung eines Cases unterdrückten, können Sie sie erneut aktivieren, indem Sie eine AutoSupport Meldung aufrufen:

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

## Was kommt als Nächstes?

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

## Ersetzen Sie einen NVIDIA SN2100 Storage-Switch

Sie können einen defekten NVIDIA SN2100 Storage Switch ersetzen. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

### Bevor Sie beginnen

Stellen Sie vor der Installation der Cumulus-Software und der RCFs auf einem NVIDIA SN2100-Speicherschalter Folgendes sicher:

- Ihr System kann NVIDIA SN2100 Storage Switches unterstützen.
- Sie haben die entsprechenden RCFs heruntergeladen.

Der "[Hardware Universe](#)" Ausführliche Informationen zu unterstützten Ports und deren Konfigurationen erhalten Sie im Detail.

Die vorhandene Netzwerkkonfiguration muss die folgenden Merkmale aufweisen:

- Führen Sie alle Schritte zur Fehlerbehebung durch, um zu bestätigen, dass Sie Ihren Switch ersetzen müssen.
- Stellen Sie sicher, dass auf beiden Switches eine Verwaltungskonnektivität besteht.



Stellen Sie sicher, dass alle Fehlerbehebungsschritte durchgeführt wurden, um zu bestätigen, dass Ihr Switch ausgetauscht werden muss.

Der Ersatz-NVIDIA SN2100-Switch muss die folgenden Eigenschaften aufweisen:

- Die Management-Netzwerk-Konnektivität ist funktionsfähig.
- Sie können über die Konsole auf den Ersatzschalter zugreifen.
- Das entsprechende RCF- und Cumulus-Betriebssystemabbild wird auf den Switch geladen.
- Die anfängliche Anpassung des Schalters ist abgeschlossen.

### Zusammenfassung der Vorgehensweise

Dieses Verfahren ersetzt den zweiten NVIDIA SN2100 Storage Switch sw2 durch den neuen NVIDIA SN2100 Switch nsw2. Die beiden Knoten sind node1 und node2.

Schritte zur Fertigstellung:

- Vergewissern Sie sich, dass der zu ersetzende Schalter sw2 ist.
- Trennen Sie die Kabel vom Schalter sw2.
- Schließen Sie die Kabel wieder an den Schalter nsw2 an.
- Überprüfen Sie alle Gerätekonfigurationen am Switch nsw2.

### Schritte

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

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

X ist die Dauer des Wartungsfensters in Stunden.

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

```
set -privilege advanced
```

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

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

## Beispiel anzeigen

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

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

```
cluster1::*>
```

4. Stellen Sie sicher, dass der Speicherschalter sw1 verfügbar ist:

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



## Beispiel anzeigen

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

5. Führen Sie die aus `net show interface` Mit dem Befehl auf dem Arbeitsschalter bestätigen Sie, dass Sie beide Nodes und alle Shelves sehen können:

```
net show interface
```

## Beispiel anzeigen

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

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

### 6. Überprüfen Sie die Shelf-Ports im Storage-System:

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

## Beispiel anzeigen

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

7. Entfernen Sie alle Kabel, die am Speicherschalter sw2 angeschlossen sind.
8. Schließen Sie alle Kabel wieder an den Ersatzschalter nsw2 an.
9. Überprüfen Sie den Integritätsstatus der Speicher-Node-Ports erneut:

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

## Beispiel anzeigen

```
cluster1::*> storage port show -port-type ENET  
  
Node      Port Type  Mode   Speed      State   Status   VLAN  
-----  -  
node1  
          e3a  ENET   storage 100    enabled online   30  
          e3b  ENET   storage 0      enabled offline  30  
          e7a  ENET   storage 0      enabled offline  30  
          e7b  ENET   storage 100   enabled online   30  
node2  
          e3a  ENET   storage 100   enabled online   30  
          e3b  ENET   storage 0      enabled offline  30  
          e7a  ENET   storage 0      enabled offline  30  
          e7b  ENET   storage 100   enabled online   30  
cluster1::*>
```

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

```
net device-discovery show -protocol lldp
```

## Beispiel anzeigen

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

### 11. Überprüfen Sie die Shelf-Ports im Storage-System:

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

## Beispiel anzeigen

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

12. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

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

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

## Was kommt als Nächstes?

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

## Copyright-Informationen

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

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

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

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

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

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

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

## Markeninformationen

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