



# **NVIDIA SN2100**

## Cluster and storage switches

NetApp  
August 29, 2025

This PDF was generated from <https://docs.netapp.com/de-de/ontap-systems-switches/switch-nvidia-sn2100/configure-overview-sn2100-cluster.html> on August 29, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

NVIDIA SN2100 .....	1
Überblick .....	1
Installations- und Einrichtungsworkflow für NVIDIA SN2100-Switches .....	1
Konfigurationsanforderungen für NVIDIA SN2100 Switches .....	1
Komponenten und Teilenummern für NVIDIA SN2100-Switches .....	2
Dokumentationsanforderungen für NVIDIA SN2100-Switches .....	3
Installieren Sie die Hardware .....	3
Workflow zur Hardwareinstallation für NVIDIA SN2100-Switches .....	3
Installieren Sie die Hardware für den NVIDIA SN2100 Switch .....	3
Prüfen Sie die Verkabelung und Konfigurationsüberlegungen .....	4
Verbinden Sie die NS224-Shelfs als Switch-Attached Storage .....	12
Konfigurieren der Software .....	13
Workflow für die Softwareinstallation von NVIDIA SN2100-Switches .....	13
Konfigurieren Sie den NVIDIA SN2100-Switch .....	14
Installieren Sie Cumulus Linux im Cumulus-Modus .....	14
Installieren Sie Cumulus Linux im ONIE-Modus .....	30
Aktualisieren Sie Cumulus Linux-Versionen .....	39
Installieren oder aktualisieren Sie das RCF-Skript (Reference Configuration File) .....	56
Installieren Sie die Konfigurationsdatei des Ethernet Switch Health Monitor .....	85
Setzen Sie den SN2100-Cluster-Switch auf die Werkseinstellungen zurück .....	87
Migrieren Sie die Switches .....	88
Migrieren Sie von einem Cisco Cluster-Switch zu einem NVIDIA SN2100 Cluster-Switch .....	89
Migrieren Sie mit NVIDIA SN2100-Cluster-Switches zu einem Cluster mit zwei Nodes .....	104
Ersetzen Sie die Schalter .....	128
Ersetzen Sie einen NVIDIA SN2100-Cluster-Switch .....	128
Ersetzen Sie NVIDIA SN2100-Cluster-Switches durch Switch-lose Verbindungen .....	146

# NVIDIA SN2100

## Überblick

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

Die NVIDIA SN2100 ist ein Cluster-Switch, mit dem Sie ONTAP Cluster mit mehr als zwei Knoten erstellen können.

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

1

#### "Überprüfen der Konfigurationsanforderungen"

Überprüfen Sie die Konfigurationsanforderungen für den SN2100-Cluster-Switch.

2

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

Überprüfen Sie die Komponenten und Teilenummern für den Cluster-Switch SN2100.

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 der Installation und Wartung von NVIDIA SN2100-Switches alle Konfigurationsanforderungen.

#### 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) in einem NVIDIA Dual/Single-Switch-Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

Hinweise zur Verkabelung finden Sie unter ["Prüfen Sie die Verkabelung und Konfigurationsüberlegungen"](#).

## ONTAP und Linux Unterstützung

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

- ONTAP 9.10.1P3 und höher

Der SN2100-Switch dient Cluster- und Speicheranwendungen in ONTAP 9.10.1P3 und höher über verschiedene Switch-Paare.

- Cumulus Linux (CL) OS-Versionen

- Bestimmte CL-Versionen werden von NetApp qualifiziert und unterstützt. Aktuelle Informationen zur Kompatibilität finden Sie auf der "["Informationen zu NVIDIA-Ethernet-Switches"](#) Seite oder im "["NetApp Hardware Universe"](#)".
- Um die SN2100 Cumulus Software von NVIDIA herunterzuladen, müssen Sie über Anmeldedaten verfügen, um auf das Enterprise Support Portal von NVIDIA zugreifen zu können. Siehe Knowledge Base-Artikel "["Registrierung bei NVIDIA für Enterprise Support Portal Access"](#)".

- Sie können Cumulus Linux installieren, wenn auf dem Switch Cumulus Linux oder ONIE ausgeführt wird.

### Was kommt als Nächstes?

["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) in einem NVIDIA Dual/Single-Switch-Schrank mit den Standardhalterungen, die im Lieferumfang des Switches enthalten sind.

### Einzelheiten zum Schienensatz

In der folgenden Tabelle sind die Teilenummer und Beschreibung der SN2100-Switches und Schienen-Kits aufgeführt:

Teilenummer	Beschreibung
X190006-PE	Cluster-Switch, NVIDIA SN2100, 16 PT 100 GbE, PTSX
X190006-PI	Cluster Switch, NVIDIA SN2100, 16 PT 100 GbE, PSIN
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?

"Erforderliche Dokumentation" .

## Dokumentationsanforderungen für NVIDIA SN2100-Switches

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

Titel	Beschreibung
"NVIDIA Switch Installation Guide"	Beschreibt die Installation Ihrer NVIDIA SN2100-Switches.
"Shelf-Verkabelung bei NS224 NVMe-Laufwerken"	Überblick und Abbildungen zeigen die Konfiguration der Verkabelung für Laufwerk-Shelves.
"NetApp Hardware Universe"	Ermöglicht die Bestätigung der unterstützten Hardware wie Storage-Switches und -Kabel für Ihr Plattformmodell.

## Installieren Sie die Hardware

### Workflow zur Hardwareinstallation für NVIDIA SN2100-Switches

Um die Hardware für einen SN2100-Cluster-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?

["Überprüfung der Verkabelung und Konfiguration"](#).

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

2. Fügen Sie die folgenden 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 --view=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.

## Einstellen der Schnittstellengeschwindigkeit an Breakout-Ports

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:~$ 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
@0 -37,21 +37,21 @0
    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:~$ net show interface
```

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

## Cumulus Linux 5.x

Beispiel:

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

link

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

Überprüfen Sie 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 br_default(UP)	10G	9216	Trunk/L2	cs07 (e4c)	Master:
UP	swp1s1 br_default(UP)	10G	9216	Trunk/L2	cs07 (e4d)	Master:
UP	swp1s2 br_default(UP)	10G	9216	Trunk/L2	cs08 (e4c)	Master:
UP	swp1s3 br_default(UP)	10G	9216	Trunk/L2	cs08 (e4d)	Master:
.						
.						
UP	swp3 br_default(UP)	40G	9216	Trunk/L2	cs03 (e4e)	Master:
UP	swp4 br_default(UP)	40G	9216	Trunk/L2	cs04 (e4e)	Master:
DN	swp5 br_default(UP)	N/A	9216	Trunk/L2		Master:
DN	swp6 br_default(UP)	N/A	9216	Trunk/L2		Master:
DN	swp7 br_default(UP)	N/A	9216	Trunk/L2		Master:
.						
.						
UP	swp15 cluster_isl(UP)	100G	9216	BondMember	cs01 (swp15)	Master:
UP	swp16 cluster_isl(UP)	100G	9216	BondMember	cs01 (swp16)	Master:
.						
.						

## Was kommt als Nächstes?

["Verkabelung der NS224 Shelves als Switch-Attached Storage".](#)

## Verbinden Sie die 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-Shelves über Storage-Switches:  
["Verkabelung, Switch-Attached NS224 Laufwerk-Shelves"](#)
- Bestätigen Sie die unterstützte Hardware, z. B. die Storage-Switches und Kabel, für Ihr Plattformmodell:  
["NetApp Hardware Universe"](#)

#### Was kommt als Nächstes?

"Konfigurieren Sie den Switch".

## Konfigurieren der Software

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

Gehen Sie wie folgt vor, um die Software für einen NVIDIA SN2100-Switch zu installieren und zu konfigurieren:

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

#### ["Aktualisieren Sie Ihre Cumulus Linux-Version nach Bedarf"](#)

Sie können Ihr Cumulus Linux (CL)-Betriebssystem nach Bedarf aktualisieren.

5

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

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

6

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

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

7

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

Löschen Sie die Einstellungen des SN2100-Cluster-Switches.

## 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?

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

## 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 Sie Folgendes haben:

- 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 Baud-Rate-Anforderung ist auf 115200 am seriellen Konsolen-Switch für den Zugriff auf die NVIDIA SN2100-Switch-Konsole eingestellt, wie folgt:
  - 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
10.233.204.71/24
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 0xdxfc00000-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.

- Überprüfen Sie die aktuelle Zeitzone:

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

- 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@cycrh6sv101 ~]$ 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+cl4.4.1ul
(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 0xdxfc00000-dfc1ffff

cumulus@sw1:~$ 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@cycrh6sv101 ~]$ 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 0xdxfc00000-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?

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

### 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 ONIE oder Cumulus Linux 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.

## Beispiel 2. Schritte

### Cumulus Linux 4.4.3

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Diese Datei umbenennen in: `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
```

```

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

```

```
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,sv1/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. Melden Sie sich nach Abschluss der Installation beim Switch an.

```
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`

```
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"
```

### Cumulus Linux 5.x

1. Laden Sie die Cumulus Linux-Installationsdatei in das Stammverzeichnis des Webservers herunter. Diese Datei umbenennen in: `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-Anmeldeanforderung 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:

5. Drücken Sie die Esc-Taste auf dem GNU GRUB-Bildschirm, um den normalen Bootvorgang zu unterbrechen, wählen Sie ONIE aus, und drücken Sie die Eingabetaste.

## Wählen Sie ONIE: OS installieren.

6. Der Vorgang zur Erkennung des ONIE-Installers führt die Suche nach der automatischen Installation durch. Drücken Sie **Enter**, um den Vorgang vorübergehend zu beenden.
7. Wenn der Erkennungsvorqang angehalten wurde:

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

8. Konfigurieren Sie die IP-Adresse, die Subnetzmaske und das Standard-Gateway:

```
ifconfig eth0
```

```

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:/ #
ONIE:/ # ifconfig eth0 10.228.140.27 netmask 255.255.248.0
ONIE:/ # ifconfig eth0
eth0      Link encap:Ethernet  HWaddr B8:CE:F6:5E:05:E6
          inet  addr:10.228.140.27  Bcast:10.228.143.255
          Mask:255.255.248.0
                  inet6 addr: fd20:8b1e:b255:822b:bace:f6ff:fe5e:5e6/64
          Scope:Global
                  inet6 addr: fe80::bace:f6ff:fe5e:5e6/64 Scope:Link
                      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                      RX packets:18813 errors:0 dropped:1418 overruns:0 frame:0
                      TX packets:491 errors:0 dropped:0 overruns:0 carrier:0
                      collisions:0 txqueuelen:1000
                      RX bytes:1339596 (1.2 MiB)  TX bytes:49379 (48.2 KiB)
                      Memory:dfc00000-dfc1ffff

ONIE:/ # route add default gw 10.228.136.1
ONIE:/ # route
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref
Use  Iface

default          10.228.136.1    0.0.0.0        UG      0      0
0    eth0
10.228.136.1    *              255.255.248.0  U      0      0
0    eth0

```

## 9. Installieren Sie Cumulus Linux 5.4:

```
# onie-nos-install http://<web-server>/<path>/cumulus-linux-5.4-mlx-
amd64.bin
```

```

ONIE:/ # route

Kernel IP routing table

ONIE:/ # onie-nos-install http://<web-server>/<path>/cumulus-
linux-5.4-mlx-amd64.bin

Stopping: discover... done.
Info: Attempting
http://10.60.132.97/x/eng/testbedN,svl/nic/files/cumulus-linux-5.4-
mlx-amd64.bin ...
Connecting to 10.60.132.97 (10.60.132.97:80)
installer          100% |*| 552M 0:00:00 ETA
...
...

```

10. Melden Sie sich nach Abschluss der Installation beim Switch an.

```

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>

```

11. Überprüfen Sie die Cumulus Linux-Version: **nv show system**

```

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

```

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@cycrh6sv101 ~]$ 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@cumulus:~$ 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.

## Was kommt als Nächstes?

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

## Aktualisieren Sie Cumulus Linux-Versionen

Gehen Sie wie folgt vor, um Ihre Cumulus Linux-Version bei Bedarf zu aktualisieren.

### Bevor Sie beginnen

Stellen Sie sicher, dass Sie Folgendes haben:

- 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 Baud-Rate-Anforderung ist auf 115200 am seriellen Konsolen-Switch für den Zugriff auf die NVIDIA SN2100-Switch-Konsole eingestellt, wie folgt:
  - 115200 Baud
  - 8 Datenbits
  - 1 Stoppbit
  - Parität: Keine
  - Flusskontrolle: Keine

### Über diese Aufgabe

Beachten Sie Folgendes:



Jedes Mal, wenn Cumulus Linux aktualisiert wird, wird die gesamte Dateisystemstruktur gelöscht und neu aufgebaut. Ihre bestehende Konfiguration wird gelöscht. Sie müssen Ihre Switch-Konfiguration speichern und aufzeichnen, bevor Sie Cumulus Linux aktualisieren.



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

Weitere Informationen finden Sie unter "["Installieren eines neuen Cumulus Linux-Images"](#)".

### Beispiel 3. Schritte

#### Cumulus Linux 4.4.x bis Cumulus Linux 5.4.0

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem Cumulus Linux und RCF gehostet werden.
3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
  - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

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

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

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

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

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. Überprüfen Sie die aktuelle Version von Cumulus Linux und die angeschlossenen Ports:

```
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
```

```
cumulus@cumulus:mgmt:~$ 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) )					
.	.	.	.	.	.

7. Laden Sie das Cumulux Linux 5.4.0-Image herunter:

```
cumulus@cumulus:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.

.
.
.

Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Starten Sie den Switch neu:

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

9. Ändern Sie das Passwort:

```
cumulus login: cumulus
Password:
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>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

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

```
cumulus@cumulus:mgmt:~$ nv show system
      operational      applied
-----
hostname      cumulus      cumulus
build        Cumulus Linux 5.4.0
uptime        14:07:08
timezone     Etc/UTC
```

11. Ändern Sie den Hostnamen:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
```

12. Melden Sie sich ab, und melden Sie sich erneut beim Switch an, um den aktualisierten Switch-Namen an der Eingabeaufforderung anzuzeigen:

```
cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Legen Sie die IP-Adresse fest:

```
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. 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@cycrh6sv101 ~]$ 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:~$
```

15. 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.x bis Cumulus Linux 5.4.0**

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem Cumulus Linux und RCF gehostet werden.
3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
  - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

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

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

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

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

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. Überprüfen Sie die aktuelle Version von Cumulus Linux und die angeschlossenen Ports:

```

cumulus@sw1:mgmt:~$ nv show system
                           operational      applied
-----
hostname              cumulus          cumulus
build                Cumulus Linux 5.3.0
uptime               6 days, 8:37:36
timezone             Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface      MTU   Speed State Remote Host      Remote Port-
Type          Summary
-----
----- -----
+ cluster_isl  9216   200G  up
bond
+ eth0         1500   100M  up      mgmt-sw1      Eth105/1/14
eth          IP Address: 10.231.80 206/22
  eth0
  IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo           65536    up
loopback    IP Address: 127.0.0.1/8
  lo
  IP Address: ::1/128
+ swp1s0      9216 10G   up  cluster01      e0b
swp
  .
  .
  .
+ swp15      9216 100G   up  sw2          swp15
swp
+ swp16      9216 100G   up  sw2          swp16
swp

```

## 7. Laden Sie das Cumulux Linux 5.4.0-Image herunter:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.4.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.4.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.

.
.
.

Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Starten Sie den Switch neu:

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

9. Ändern Sie das Passwort:

```
cumulus login: cumulus
Password:
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>
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

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

```
cumulus@cumulus:mgmt:~$ nv show system
operational applied
-----
hostname      cumulus cumulus
build         Cumulus Linux 5.4.0
uptime         14:07:08
timezone      Etc/UTC
```

11. Ändern Sie den Hostnamen:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Melden Sie sich ab, und melden Sie sich erneut beim Switch an, um den aktualisierten Switch-Namen an der Eingabeaufforderung anzuzeigen:

```

cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.10.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

13. Legen Sie die IP-Adresse fest:

```

cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

14. Erstellen Sie einen neuen Benutzer, und fügen Sie diesen Benutzer dem `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@cycrh6sv101 ~]$ 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:~$
```

15. 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 5.4.0 bis Cumulus Linux 5.11.0**

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie den Ping-Befehl, um die Verbindung zum Server zu überprüfen, auf dem Cumulus Linux und RCF gehostet werden.
3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
  - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

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

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

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

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

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. Überprüfen Sie die aktuelle Version von Cumulus Linux und die angeschlossenen Ports:

```

cumulus@sw1:mgmt:~$ nv show system
                           operational      applied
-----
hostname              cumulus          cumulus
build                Cumulus Linux 5.4.0
uptime               6 days, 8:37:36
timezone             Etc/UTC

cumulus@sw1:mgmt:~$ nv show interface
Interface      MTU   Speed State Remote Host      Remote Port-
Type          Summary
-----
----- -----
+ cluster_isl  9216   200G  up
bond
+ eth0         1500   100M  up      mgmt-sw1      Eth105/1/14
eth          IP Address: 10.231.80 206/22
  eth0
  IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo           65536    up
loopback    IP Address: 127.0.0.1/8
  lo
  IP Address: ::1/128
+ swp1s0      9216 10G    up  cluster01      e0b
swp
  .
  .
  .
+ swp15      9216 100G   up  sw2          swp15
swp
+ swp16      9216 100G   up  sw2          swp16
swp

```

7. Laden Sie das Cumulux Linux 5.11.0-Image herunter:

```
cumulus@sw1:mgmt:~$ sudo onie-install -a -i http://<ip-to-
webserver>/path/to/cumulus-linux-5.11.0-mlx-amd64.bin
[sudo] password for cumulus:
Fetching installer: http://<ip-to-webserver>/path/to/cumulus-linux-
5.11.0-mlx-amd64.bin
Downloading URL: http://<ip-to-webserver>/path/to/cumulus-linux-
5.11.0-mlx-amd64.bin
# 100.0%
Success: HTTP download complete.
EFI variables are not supported on this system
Warning: SecureBoot is not available.
Image is signed.

.
.
.

Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
```

8. Starten Sie den Switch neu:

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

9. Ändern Sie das Passwort:

```
cumulus login: cumulus
Password:
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>
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'
```

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

```
cumulus@cumulus:mgmt:~$ nv show system
operational applied
-----
hostname      cumulus cumulus
build         Cumulus Linux 5.11.0
uptime         14:07:08
timezone      Etc/UTC
```

11. Ändern Sie den Hostnamen:

```
cumulus@cumulus:mgmt:~$ nv set system hostname sw1
cumulus@cumulus:mgmt:~$ nv config apply
Warning: The following files have been changed since the last save,
and they WILL be overwritten.
- /etc/nsswitch.conf
- /etc/synced/synced.conf
.
.
```

12. Melden Sie sich ab und erneut beim Switch an, um den aktualisierten Switch-Namen in der Eingabeaufforderung anzuzeigen:

```

cumulus@cumulus:mgmt:~$ exit
logout

Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
Last login: Tue Dec 15 21:43:13 UTC 2020 on ttyS0
Linux cumulus 5.11.0-cl-1-amd64 #1 SMP Debian 5.10.162-1+cl5.4.0u1
(2023-01-20) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

ZTP in progress. To disable, do 'ztp -d'

cumulus@sw1:mgmt:~$
```

### 13. Legen Sie die IP-Adresse fest:

```

cumulus@sw1:mgmt:~$ nv unset interface eth0 ip address dhcp
cumulus@sw1:mgmt:~$ nv set interface eth0 ip address
10.231.80.206/22
cumulus@sw1:mgmt:~$ nv set interface eth0 ip gateway 10.231.80.1
cumulus@sw1:mgmt:~$ nv config apply
applied [rev_id: 2]
cumulus@sw1:mgmt:~$ ip route show vrf mgmt
default via 10.231.80.1 dev eth0 proto kernel
unreachable default metric 4278198272
10.231.80.0/22 dev eth0 proto kernel scope link src 10.231.80.206
127.0.0.0/8 dev mgmt proto kernel scope link src 127.0.0.1
```

### Was kommt als Nächstes?

["Installieren oder aktualisieren Sie das RCF-Skript".](#)

## Installieren oder aktualisieren Sie das RCF-Skript (Reference Configuration File)

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 ist installiert. Siehe "[Hardware Universe](#)" Für unterstützte Versionen.

- IP-Adresse, Subnetzmaske und Standard-Gateway über DHCP oder manuell konfiguriert definiert.



Sie müssen im RCF (zusätzlich zum Admin-Benutzer) einen Benutzer angeben, der speziell für die Protokollerfassung verwendet werden soll.

## Kundenkonfigurationen

Folgende Referenzkonfigurationskategorien stehen zur Verfügung:

Cluster	Bei Ports, die für 4x10GbE-Breakout konfiguriert sind, ist ein Port für 4x25GbE-Breakout und die anderen Ports für 40/100GbE konfiguriert. Unterstützt gemeinsam genutzten Cluster-/HA-Verkehr auf Ports für Knoten, die gemeinsam genutzte Cluster-/HA-Ports verwenden. Die Plattformtabelle finden Sie im Knowledge Base-Artikel. <a href="#">"Welche AFF, ASA und FAS -Plattformen verwenden gemeinsam genutzte Cluster- und HA-Ethernet-Ports?"</a> . Alle Ports können auch als dedizierte Cluster-Ports verwendet werden.
Storage	Alle Ports sind für 100GbE NVMe-Speicherverbindungen konfiguriert.

## Aktuelle RCF-Skriptversionen

Für Cluster- und Speicheranwendungen stehen zwei RCF-Skripte zur Verfügung. RCFs von Seite herunterladen ["NVIDIA SN2100 Software-Download"](#). Das Verfahren für jedes ist gleich.

- Cluster: **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**
- Speicher: **MSN2100-RCF-v1.x-Speicher**

## Zu den Beispielen

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.

## Beispiel 4. Schritte

### Cumulus Linux 4.4.3

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die ping Befehl zum Überprüfen der Konnektivität mit dem Server, auf dem Cumulus Linux und RCF gehostet werden.
3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
  - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

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

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

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

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

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
```

- Wenn Sie Ihr RCF aktualisieren, müssen Sie für diesen Schritt die automatische Rücksetzung deaktivieren.
- Wenn Sie Ihre Cumulus Linux-Version gerade aktualisiert haben, müssen Sie die automatische Wiederherstellung für diesen Schritt nicht deaktivieren, da sie bereits deaktiviert ist.

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

```
admin@sw1: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  NotConfigured
  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.

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host>/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LLDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP          100%  8607
111.2KB/s          00:00
```



Während `scp` Im Beispiel wird „<http://www.sftp.org/docs/file...>

3. Wenden Sie das Skript RCF Python an **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LLDP**.

```

cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LLDP
[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 im obigen Beispiel aufgeführten Schritte durch.

- i In Schritt 3 **Aktualisierung der MOTD-Datei** oben, der Befehl `cat /etc/motd` wird ausgeführt. Dadurch können Sie den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner überprüfen.
- i 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:

```

admin@sw1: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
bridge (UP)
DN      swp2s1      N/A    9216    Trunk/L2
bridge (UP)
DN      swp2s2      N/A    9216    Trunk/L2
bridge (UP)
DN      swp2s3      N/A    9216    Trunk/L2
bridge (UP)
UP      swp3         100G   9216    Trunk/L2
bridge (UP)
UP      swp4         100G   9216    Trunk/L2
bridge (UP)
DN      swp5         N/A    9216    Trunk/L2
bridge (UP)
DN      swp6         N/A    9216    Trunk/L2
bridge (UP)
DN      swp7         N/A    9216    Trunk/L2
bridge (UP)
DN      swp8         N/A    9216    Trunk/L2
bridge (UP)
DN      swp9         N/A    9216    Trunk/L2
bridge (UP)
DN      swp10        N/A    9216    Trunk/L2
bridge (UP)
DN      swp11        N/A    9216    Trunk/L2
bridge (UP)
DN      swp12        N/A    9216    Trunk/L2
bridge (UP)
DN      swp13        N/A    9216    Trunk/L2
bridge (UP)
DN      swp14        N/A    9216    Trunk/L2
bridge (UP)
UP      swp15        N/A    9216    BondMember
bond_15_16 (UP)
UP      swp16        N/A    9216    BondMember
bond_15_16 (UP)
...
...

```

```

admin@sw1: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:

```

admin@sw1: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:

```
admin@sw1: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 Cluster-Ports über alle Nodes im Cluster hinweg ordnungsgemäß hochaktiv sind:

```
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
```

- Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den

Switch sw2 an, da LIFs nicht auf e0d homed sind.)

```
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
```

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

```
cluster show
```

10. Wiederholen Sie die Schritte 1 bis 14 am zweiten Schalter.

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

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

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die ping Befehl zum Überprüfen der Konnektivität mit dem Server, auf dem Cumulus Linux und RCF gehostet werden.
3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
  - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

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

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

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

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

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
```

- Wenn Sie Ihr RCF aktualisieren, müssen Sie für diesen Schritt die automatische Rücksetzung deaktivieren.
- Wenn Sie Ihre Cumulus Linux-Version gerade aktualisiert haben, müssen Sie die automatische Wiederherstellung für diesen Schritt nicht deaktivieren, da sie bereits deaktiviert ist.

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

```
admin@sw1:mgmt:~$ nv show interface
Interface      MTU   Speed State Remote Host          Remote Port-
Type          Summary
-----  -----  -----  -----  -----  -----
-----  -----
+ cluster_isl  9216   200G   up
bond
+ eth0         1500   100M   up      mgmt-sw1      Eth105/1/14
eth          IP Address: 10.231.80 206/22
  eth0
  IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo           65536    up
loopback    IP Address: 127.0.0.1/8
  lo
  IP Address: ::1/128
+ swp1s0       9216 10G    up  cluster01      e0b
swp
.
.
.
+ swp15       9216 100G   up  sw2          swp15
swp
+ swp16       9216 100G   up  sw2          swp16
swp
```

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

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host>/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LDP          100% 8607
111.2KB/s          00:00
```



Während scp Im Beispiel wird „<http://www.sftp.org/docs/file...>

3. Wenden Sie das Skript RCF Python an **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LDP
[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 im obigen Beispiel aufgeführten Schritte durch.



In Schritt 3 **Aktualisieren der MOTD-Datei** oben, der Befehl `cat /etc/issue.net` ausgeführt wird. Dadurch können Sie den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner überprüfen.

Beispiel:

```

admin@sw1:mgmt:~$ cat /etc/issue.net
*****
*****
*
* NetApp Reference Configuration File (RCF)
* Switch      : Mellanox MSN2100
* Filename    : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LLDP
* Release Date : 13-02-2023
* Version     : 1._x_-Cluster-HA-Breakout-LLDP
*
* Port Usage:
* Port 1      : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2      : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14   : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16  : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
*****
*****

```



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:

```

admin@sw1:mgmt:~$ nv show interface
Interface      MTU      Speed State Remote Host          Remote Port-
Type          Summary
-----  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----

```

```

+ cluster_isl 9216 200G up
bond
+ eth0 1500 100M up mgmt-sw1 Eth105/1/14
eth IP Address: 10.231.80 206/22
eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo 65536 up
loopback IP Address: 127.0.0.1/8
lo
IP Address: ::1/128
+ swp1s0 9216 10G up cluster01 e0b
swp
.
.
.
+ swp15 9216 100G up sw2 swp15
swp
+ swp16 9216 100G up sw2 swp16
swp

```

```

admin@sw1:mgmt:~$ nv show qos roce
              operational applied description
-----  -----  -----
enable          on          Turn feature 'on' or
'off'. This feature is disabled by default.
mode           lossless    lossless Roce Mode
congestion-control
  congestion-mode  ECN,RED          Congestion config mode
  enabled-tc       0,2,5          Congestion config enabled
Traffic Class
  max-threshold   195.31 KB      Congestion config max-
threshold
  min-threshold   39.06 KB       Congestion config min-
threshold
  probability      100
lldp-app-tlv
  priority         3          switch-priority of roce
  protocol-id     4791        L4 port number
  selector         UDP         L4 protocol
pfc
  pfc-priority    2, 5        switch-prio on which PFC
is enabled
  rx-enabled       enabled      PFC Rx Enabled status
  tx-enabled       enabled      PFC Tx Enabled status
trust

```

trust-mode pcp,dscp Trust Setting on the port  
for packet classification

RoCE PCP/DSCP->SP mapping configurations

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

RoCE SP->TC mapping and ETS configurations

	switch-prio	traffic-class	scheduler-weight
0	0	0	DWRR-28%
1	1	0	DWRR-28%
2	2	2	DWRR-28%
3	3	0	DWRR-28%
4	4	0	DWRR-28%
5	5	5	DWRR-43%
6	6	0	DWRR-28%
7	7	0	DWRR-28%

RoCE pool config

traffic-class	name	mode	size	switch-priorities	
0	lossy-default-ingress	Dynamic	50%	0,1,3,4,6,7	-
1	roce-reserved-ingress	Dynamic	50%	2,5	-
2	lossy-default-egress	Dynamic	50%	-	0
3	roce-reserved-egress	Dynamic	inf	-	2,5

Exception List

description

--

---

```
1  RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
2  Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
3  Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
4  Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
5  Congestion Config max-threshold Mismatch.Expected max-
threshold:
1500000.
6  Scheduler config mismatch for traffic-class mapped to
switch-prio0.
Expected scheduler-weight: DWRR-50%.
7  Scheduler config mismatch for traffic-class mapped to
switch-prio1.
Expected scheduler-weight: DWRR-50%.
8  Scheduler config mismatch for traffic-class mapped to
switch-prio2.
Expected scheduler-weight: DWRR-50%.
9  Scheduler config mismatch for traffic-class mapped to
switch-prio3.
Expected scheduler-weight: DWRR-50%.
10 Scheduler config mismatch for traffic-class mapped to
switch-prio4.
Expected scheduler-weight: DWRR-50%.
11 Scheduler config mismatch for traffic-class mapped to
switch-prio5.
Expected scheduler-weight: DWRR-50%.
12 Scheduler config mismatch for traffic-class mapped to
switch-prio6.
Expected scheduler-weight: strict-priority.
13 Scheduler config mismatch for traffic-class mapped to
switch-prio7.
Expected scheduler-weight: DWRR-50%.
14 Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
15 Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
16 Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
17 Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
18 Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
19 Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkup3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkup3-16 link
```

```
fast-linkup
```

```
Incomplete Command: set interface swp3-16 link fast-linkup swp3-16 link  
fast-linkup
```



Die aufgeführten Ausnahmen haben keine Auswirkungen auf die Leistung und können sicher ignoriert werden.

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

```
admin@sw1:mgmt:~$ nv show interface --view=pluggables
Interface Identifier      Vendor Name  Vendor PN      Vendor
SN      Vendor Rev
-----  -----  -----  -----
-----  -----  -----  -----
swp1s0    0x00  None
swp1s1    0x00  None
swp1s2    0x00  None
swp1s3    0x00  None
swp2s0    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp2s1    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp2s2    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp2s3    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp3      0x00  None
swp4      0x00  None
swp5      0x00  None
swp6      0x00  None
.
.
.
swp15    0x11  (QSFP28)  Amphenol      112-00595
APF20279210117  B0
swp16    0x11  (QSFP28)  Amphenol      112-00595
APF20279210166  B0
```

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

```
admin@sw1:mgmt:~$ nv show interface --view=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

8. 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:

```
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
```

b. Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den

Switch sw2 an, da LIFs nicht auf e0d homed sind.)

```
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 5.4.0 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 5.4.0 running on
  Mellanox
  Technologies Ltd. MSN2100
  Version Source: LLDP
```

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

```
cluster show
```

10. Wiederholen Sie die Schritte 1 bis 14 am zweiten Schalter.

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

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

1. Verbinden Sie den Cluster-Switch mit dem Managementnetzwerk.
2. Verwenden Sie die ping Befehl zum Überprüfen der Konnektivität mit dem Server, auf dem Cumulus Linux und RCF gehostet werden.
3. Anzeigen der Cluster-Ports an jedem Node, der mit den Cluster-Switches verbunden ist:

```
network device-discovery show
```

4. Überprüfen Sie den Administrations- und Betriebsstatus der einzelnen Cluster-Ports.
  - a. Vergewissern Sie sich, dass alle Cluster-Ports einen ordnungsgemäßen Status aufweisen:

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

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

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

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

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

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
```

- Wenn Sie Ihr RCF aktualisieren, müssen Sie für diesen Schritt die automatische Rücksetzung deaktivieren.
- Wenn Sie Ihre Cumulus Linux-Version gerade aktualisiert haben, müssen Sie die automatische Wiederherstellung für diesen Schritt nicht deaktivieren, da sie bereits deaktiviert ist.

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

```
admin@sw1:mgmt:~$ nv show interface
Interface      MTU   Speed State Remote Host      Remote Port-
Type          Summary
-----  -----  -----  -----  -----  -----
-----  -----
+ cluster_isl  9216   200G   up
bond
+ eth0         1500   100M   up      mgmt-sw1      Eth105/1/14
eth          IP Address: 10.231.80.206/22
    eth0
    IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo           65536    up
loopback    IP Address: 127.0.0.1/8
    lo
    IP Address: ::1/128
+ swp1s0       9216 10G   up  cluster01      e0b
swp
.
.
.
+ swp15       9216 100G   up  sw2          swp15
swp
+ swp16       9216 100G   up  sw2          swp16
swp
```

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

```
cumulus@cumulus:mgmt:~$ cd /tmp
cumulus@cumulus:mgmt:/tmp$ scp <user>@<host>/<path>/MSN2100-RCF-v1.x
-Cluster-HA-Breakout-LDP .
ssologin@10.233.204.71's password:
MSN2100-RCF-v1.x-Cluster-HA-Breakout-LDP          100% 8607
111.2KB/s          00:00
```



Obwohl scp im Beispiel wird „http://www.sftp.org/docs/file ...“

3. Wenden Sie das Skript RCF Python an **MSN2100-RCF-v1.x-Cluster-HA-Breakout-LDP**.

```
cumulus@cumulus:mgmt:/tmp$ sudo python3 MSN2100-RCF-v1.x-Cluster-HA
-Breakout-LDP
[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 im obigen Beispiel aufgeführten Schritte durch.



In Schritt 3 **Aktualisieren der MOTD-Datei** oben wird der Befehl „cat /etc/issue.net“ ausgeführt. Dadurch können Sie den RCF-Dateinamen, die RCF-Version, die zu verwendenden Ports und andere wichtige Informationen im RCF-Banner überprüfen.

Beispiel:

```

admin@sw1:mgmt:~$ cat /etc/issue.net
*****
*****
*
* NetApp Reference Configuration File (RCF)
* Switch      : Mellanox MSN2100
* Filename    : MSN2100-RCF-1._x_-Cluster-HA-Breakout-LDP
* Release Date : 13-02-2023
* Version     : 1._x_-Cluster-HA-Breakout-LDP
*
* Port Usage:
* Port 1      : 4x10G Breakout mode for Cluster+HA Ports, swp1s0-3
* Port 2      : 4x25G Breakout mode for Cluster+HA Ports, swp2s0-3
* Ports 3-14   : 40/100G for Cluster+HA Ports, swp3-14
* Ports 15-16  : 100G Cluster ISL Ports, swp15-16
*
* NOTE:
*   RCF manually sets swp1s0-3 link speed to 10000 and
*   auto-negotiation to off for Intel 10G
*   RCF manually sets swp2s0-3 link speed to 25000 and
*   auto-negotiation to off for Chelsio 25G
*
*
* IMPORTANT: Perform the following steps to ensure proper RCF
installation:
* - Copy the RCF file to /tmp
* - Ensure the file has execute permission
* - From /tmp run the file as sudo python3 <filename>
*
*****
*****

```



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:

```

admin@sw1:mgmt:~$ nv show interface
Interface      MTU      Speed State Remote Host          Remote Port-
Type          Summary
-----  -----  -----  -----  -----  -----
-----  -----  -----  -----  -----  -----

```

```

+ cluster_isl 9216 200G up
bond
+ eth0          1500 100M up mgmt-sw1                         Eth105/1/14
eth      IP Address: 10.231.80 206/22
eth0
IP Address: fd20:8b1e:f6ff:fe31:4a0e/64
+ lo           65536      up
loopback  IP Address: 127.0.0.1/8
lo
IP Address: ::1/128
+ swp1s0       9216 10G up cluster01                         e0b
swp
.
.
.
+ swp15       9216 100G up sw2                            swp15
swp
+ swp16       9216 100G up sw2                            swp16
swp

```

```

admin@sw1:mgmt:~$ nv show qos roce
              operational applied description
-----  -----  -----
enable          on                      Turn feature 'on' or
'off'. This feature is disabled by default.
mode           lossless      lossless  Roce Mode
congestion-control
  congestion-mode  ECN,RED          Congestion config mode
  enabled-tc       0,2,5           Congestion config enabled
Traffic Class
  max-threshold   195.31 KB        Congestion config max-
threshold
  min-threshold   39.06 KB         Congestion config min-
threshold
  probability      100
lldp-app-tlv
  priority         3                  switch-priority of roce
  protocol-id     4791              L4 port number
  selector         UDP                L4 protocol
pfc
  pfc-priority    2, 5              switch-prio on which PFC
is enabled
  rx-enabled       enabled            PFC Rx Enabled status
  tx-enabled       enabled            PFC Tx Enabled status
trust

```

trust-mode pcp,dscp Trust Setting on the port  
for packet classification

RoCE PCP/DSCP->SP mapping configurations

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

RoCE SP->TC mapping and ETS configurations

	switch-prio	traffic-class	scheduler-weight
0	0	0	DWRR-28%
1	1	0	DWRR-28%
2	2	2	DWRR-28%
3	3	0	DWRR-28%
4	4	0	DWRR-28%
5	5	5	DWRR-43%
6	6	0	DWRR-28%
7	7	0	DWRR-28%

RoCE pool config

traffic-class	name	mode	size	switch-priorities	
0	lossy-default-ingress	Dynamic	50%	0,1,3,4,6,7	-
1	roce-reserved-ingress	Dynamic	50%	2,5	-
2	lossy-default-egress	Dynamic	50%	-	0
3	roce-reserved-egress	Dynamic	inf	-	2,5

Exception List

description

--

---

```
1  RoCE PFC Priority Mismatch.Expected pfc-priority: 3.
2  Congestion Config TC Mismatch.Expected enabled-tc: 0,3.
3  Congestion Config mode Mismatch.Expected congestion-mode:
ECN.
4  Congestion Config min-threshold Mismatch.Expected min-
threshold: 150000.
5  Congestion Config max-threshold Mismatch.Expected max-
threshold:
1500000.
6  Scheduler config mismatch for traffic-class mapped to
switch-prio0.
Expected scheduler-weight: DWRR-50%.
7  Scheduler config mismatch for traffic-class mapped to
switch-prio1.
Expected scheduler-weight: DWRR-50%.
8  Scheduler config mismatch for traffic-class mapped to
switch-prio2.
Expected scheduler-weight: DWRR-50%.
9  Scheduler config mismatch for traffic-class mapped to
switch-prio3.
Expected scheduler-weight: DWRR-50%.
10 Scheduler config mismatch for traffic-class mapped to
switch-prio4.
Expected scheduler-weight: DWRR-50%.
11 Scheduler config mismatch for traffic-class mapped to
switch-prio5.
Expected scheduler-weight: DWRR-50%.
12 Scheduler config mismatch for traffic-class mapped to
switch-prio6.
Expected scheduler-weight: strict-priority.
13 Scheduler config mismatch for traffic-class mapped to
switch-prio7.
Expected scheduler-weight: DWRR-50%.
14 Invalid reserved config for ePort.TC[2].Expected 0 Got 1024
15 Invalid reserved config for ePort.TC[5].Expected 0 Got 1024
16 Invalid traffic-class mapping for switch-priority 2.Expected
0 Got 2
17 Invalid traffic-class mapping for switch-priority 3.Expected
3 Got 0
18 Invalid traffic-class mapping for switch-priority 5.Expected
0 Got 5
19 Invalid traffic-class mapping for switch-priority 6.Expected
6 Got 0
Incomplete Command: set interface swp3-16 link fast-linkup3-16 link
fast-linkup
Incomplete Command: set interface swp3-16 link fast-linkup3-16 link
```

fast-linkup

Incomplete Command: set interface swp3-16 link fast-linkup swp3-16 link fast-linkup



Die aufgeführten Ausnahmen haben keine Auswirkungen auf die Leistung und können sicher ignoriert werden.

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

```
admin@sw1:mgmt:~$ nv show platform transceiver
Interface Identifier      Vendor Name  Vendor PN      Vendor
SN      Vendor Rev
-----  -----  -----  -----
-----  -----  -----  -----
swp1s0    0x00  None
swp1s1    0x00  None
swp1s2    0x00  None
swp1s3    0x00  None
swp2s0    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp2s1    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp2s2    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp2s3    0x11  (QSFP28)  CISCO-LEONI  L45593-D278-D20
LCC2321GTTJ    00
swp3      0x00  None
swp4      0x00  None
swp5      0x00  None
swp6      0x00  None
.
.
.
swp15    0x11  (QSFP28)  Amphenol      112-00595
APF20279210117  B0
swp16    0x11  (QSFP28)  Amphenol      112-00595
APF20279210166  B0
```

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

```
admin@sw1:mgmt:~$ nv show interface 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

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

- Vergewissern Sie sich, dass Cluster-Ports über alle Nodes im Cluster hinweg ordnungsgemäß hochaktiv sind:

```
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
```

- Überprüfen Sie den Switch-Systemzustand des Clusters (dies zeigt möglicherweise nicht den

Switch sw2 an, da LIFs nicht auf e0d homed sind.)

```
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 5.4.0 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 5.4.0 running on
  Mellanox
  Technologies Ltd. MSN2100
  Version Source: LLDP
```

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

```
cluster show
```

10. Wiederholen Sie die Schritte 1 bis 14 am zweiten Schalter.

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

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

### Was kommt als Nächstes?

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

## Installieren Sie die Konfigurationsdatei des Ethernet Switch Health Monitor

Um die Integritätsüberwachung von Ethernet-Switches auf NVIDIA-Ethernet-Switches zu konfigurieren, befolgen Sie dieses Verfahren.

Diese Anweisungen gelten, wenn NVIDIA X190006-PE und X190006-PI Switches nicht richtig erkannt werden. Dies kann durch Ausführen von `system switch ethernet show` und prüfen Sie, ob **OTHER** für Ihr Modell angezeigt wird. Um Ihr NVIDIA-Switch-Modell zu identifizieren, suchen Sie die Teilenummer mit dem Befehl `nv show platform hardware` für NVIDIA CL 5.8 und früher oder `nv show platform` für spätere Versionen.

Diese Schritte werden auch empfohlen, wenn Sie möchten, dass die Integritätsüberwachung und Protokollerfassung bei Verwendung von NVIDIA CL 5.11.x mit den folgenden ONTAP-Versionen wie vorgesehen funktioniert. Auch ohne diese Schritte funktionieren Integritätsüberwachung und Protokollerfassung möglicherweise weiterhin, aber durch deren Befolgeung wird sichergestellt, dass alles ordnungsgemäß funktioniert.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 und spätere Patch-Versionen

### Bevor Sie beginnen

- Stellen Sie sicher, dass das ONTAP Cluster betriebsbereit ist und ausgeführt wird.
- Aktivieren Sie SSH auf dem Switch, um alle in CSHM verfügbaren Funktionen zu nutzen.
- 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
```

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 auf dem ONTAP-System aus `system switch ethernet show`, und stellen Sie sicher, dass die Cluster-Switches erkannt werden, wobei das überwachte Feld auf **true** und das Seriennummernfeld nicht **Unknown** anzeigt.

```
cluster1::> system switch ethernet show
```



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

Siehe die "[System-Switch-Ethernet-Konfigurations-Health-Monitor](#)" Befehl für weitere Details.

#### Was kommt als Nächstes?

["Konfigurieren Sie die Überwachung des Switch-Systemzustands".](#)

## Setzen Sie den SN2100-Cluster-Switch auf die Werkseinstellungen zurück

So setzen Sie den SN2100-Cluster-Switch 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 5. 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` gefolgt vom Dateipfad zur Switch-Software, zum Beispiel:

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

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

```
sudo reboot
```

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



Der Switch startet neu und beginnt mit der Installation der Switch-Software, was einige Zeit in Anspruch nimmt. 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.

## Migrieren Sie die Switches

## Migrieren Sie von einem Cisco Cluster-Switch zu einem NVIDIA SN2100 Cluster-Switch

Sie können Cisco Cluster Switches für ein ONTAP Cluster zu NVIDIA SN2100 Cluster Switches migrieren. Hierbei handelt es sich um ein unterbrechungsfreies Verfahren.

### Prüfen Sie die Anforderungen

Sie müssen bestimmte Konfigurationsinformationen, Portverbindungen und Verkabelungsanforderungen beachten, wenn Sie einige ältere Cisco Cluster Switches durch NVIDIA SN2100 Cluster Switches ersetzen. Siehe "[Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches](#)".

### Unterstützte Switches

Folgende Cisco Cluster-Switches werden unterstützt:

- Nexus 9336C-FX2
- Nexus 92300YC
- Nexus 5596UP
- Nexus 3232C
- Nexus 3132Q-V

Weitere Informationen zu unterstützten Ports und deren Konfigurationen finden Sie im "[Hardware Universe](#)".

### Was Sie benötigen

Stellen Sie sicher, dass:

- Das vorhandene Cluster ist ordnungsgemäß eingerichtet und funktioniert.
- Alle Cluster-Ports befinden sich im Status **up**, um einen unterbrechungsfreien Betrieb zu gewährleisten.
- Die NVIDIA SN2100-Cluster-Switches sind konfiguriert und funktionieren unter der richtigen Version von Cumulus Linux, die mit der verwendeten Referenzkonfigurationsdatei (RCF) installiert wird.
- Die vorhandene Cluster-Netzwerkkonfiguration 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.
- Einige der Ports sind auf NVIDIA SN2100-Switches für 40 GbE oder 100 GbE konfiguriert.
- Sie haben 40-GbE- und 100-GbE-Konnektivität von den Nodes zu NVIDIA SN2100 Cluster Switches geplant, migriert und dokumentiert.

 Wenn Sie die Portgeschwindigkeit der e0a- und e1a-Cluster-Ports auf AFF A800- oder AFF C800-Systemen ändern, können Sie beobachten, wie fehlerhafte Pakete nach der Geschwindigkeitskonvertierung empfangen werden. Siehe "[Bug 1570339](#)" Und den Knowledge Base Artikel "["CRC-Fehler auf T6-Ports nach der Konvertierung von 40GbE zu 100GbE"](#)" Für eine Anleitung.

## Migrieren Sie die Switches

### Zu den Beispielen

In diesem Verfahren werden Cisco Nexus 3232C-Cluster-Switches beispielsweise Befehle und Ausgaben verwendet.

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

- Die vorhandenen Cisco Nexus 3232C Cluster-Switches sind *c1* und *c2*.
- Die neuen NVIDIA SN2100-Cluster-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 Cluster-Ports sind *e3a* und *e3b*.
- Breakout-Ports haben das Format *swp[Port]s[Breakout-Port 0-3]*. Beispielsweise sind vier Breakout-Ports auf *swp1* *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

### Über diese Aufgabe

Dieses Verfahren umfasst das folgende Szenario:

- Schalter *c2* wird zuerst durch Schalter *sw2* ersetzt.
  - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
  - Die Verkabelung zwischen den Knoten und *c2* wird dann von *c2* getrennt und wieder mit *sw2* verbunden.
- Schalter *c1* wird durch Schalter *sw1* ersetzt.
  - Fahren Sie die Ports zu den Cluster-Nodes herunter. Alle Ports müssen gleichzeitig heruntergefahren werden, um eine Instabilität von Clustern zu vermeiden.
  - Die Verkabelung zwischen den Knoten und *c1* wird dann von *c1* getrennt und wieder mit *sw1* verbunden.

### Schritt: Bereiten Sie sich auf die Migration 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 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. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

#### Schritt: Ports und Verkabelung konfigurieren

1. Legen Sie den Administrations- oder Betriebsstatus der einzelnen Cluster-Schnittstellen fest.

Jeder Port sollte für angezeigt werden Link Und gesund für Health Status.

- a. Zeigen Sie die Attribute des Netzwerkports an:

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

#### Beispiel anzeigen

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

Node: node1

Ignore                                                 Speed (Mbps)

Health     Health
Port       IPspace     Broadcast Domain Link MTU     Admin/Oper
Status     Status
-----  -----
-----  -----
e3a       Cluster     Cluster           up    9000  auto/100000
healthy   false
e3b       Cluster     Cluster           up    9000  auto/100000
healthy   false

Node: node2

Ignore                                                 Speed (Mbps)

Health     Health
Port       IPspace     Broadcast Domain Link MTU     Admin/Oper
Status     Status
-----  -----
-----  -----
e3a       Cluster     Cluster           up    9000  auto/100000
healthy   false
e3b       Cluster     Cluster           up    9000  auto/100000
healthy   false
```

- b. Informationen zu den logischen Schnittstellen und den zugehörigen Home-Nodes anzeigen:

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

Jede LIF sollte angezeigt werden up/up Für Status Admin/Oper Und zwar für Is Home.

#### Beispiel anzeigen

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

          Logical      Status      Network      Current
Current Is
Vserver      Interface      Admin/Oper  Address/Mask      Node
Port        Home
-----  -----  -----  -----
-----  -----
Cluster
          node1_clus1  up/up      169.254.209.69/16  node1
e3a        true
          node1_clus2  up/up      169.254.49.125/16  node1
e3b        true
          node2_clus1  up/up      169.254.47.194/16  node2
e3a        true
          node2_clus2  up/up      169.254.19.183/16  node2
e3b        true
```

2. Die Cluster-Ports auf jedem Node sind auf folgende Weise (aus Sicht der Nodes) mit vorhandenen Cluster-Switches verbunden:

```
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
          e3a    c1 (6a:ad:4f:98:3b:3f)      Eth1/1      -
          e3b    c2 (6a:ad:4f:98:4c:a4)      Eth1/1      -
node2      /lldp
          e3a    c1 (6a:ad:4f:98:3b:3f)      Eth1/2      -
          e3b    c2 (6a:ad:4f:98:4c:a4)      Eth1/2      -
```

3. Die Cluster-Ports und Switches sind (aus Sicht der Switches) wie folgt verbunden:

```
show cdp neighbors
```

#### Beispiel anzeigen

```
c1# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,  
V - VoIP-Phone, D - Remotely-Managed-Device,  
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3a	Eth1/1	124	H	AFF-A400
node2 e3a	Eth1/2	124	H	AFF-A400
c2 Eth1/31	Eth1/31	179	S I s	N3K-C3232C
c2 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

```
c2# show cdp neighbors
```

Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge

S - Switch, H - Host, I - IGMP, r - Repeater,  
V - VoIP-Phone, D - Remotely-Managed-Device,  
s - Supports-STP-Dispute

Device-ID Port ID	Local Intrfce	Hldtme	Capability	Platform
node1 e3b	Eth1/1	124	H	AFF-A400
node2 e3b	Eth1/2	124	H	AFF-A400
c1 Eth1/31	Eth1/31	175	S I s	N3K-C3232C
c1 Eth1/32	Eth1/32	175	S I s	N3K-C3232C

4. 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 anzeigen:

```
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 anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date                LIF          LIF
Loss
-----
-----
node1
      3/5/2022 19:21:18 -06:00  node1_clus2      node2-clus1
none
      3/5/2022 19:21:20 -06:00  node1_clus2      node2_clus2
none
node2
      3/5/2022 19:21:18 -06:00  node2_clus2      node1_clus1
none
      3/5/2022 19:21:20 -06:00  node2_clus2      node1_clus2
none
```

## Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1      e3a
Cluster node1_clus2 169.254.49.125 node1      e3b
Cluster node2_clus1 169.254.47.194 node2      e3a
Cluster node2_clus2 169.254.19.183 node2      e3b
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. bei Switch c2 fahren Sie die mit den Cluster-Ports der Knoten verbundenen Ports herunter, um ein Failover der Cluster-LIFs durchzuführen.

```

(c2) # configure
Enter configuration commands, one per line. End with CNTL/Z.

(c2) (Config) # interface
(c2) (config-if-range) # shutdown <interface_list>
(c2) (config-if-range) # exit
(c2) (Config) # exit
(c2) #

```

2. Verschieben Sie die Node-Cluster-Ports vom alten Switch c2 auf den neuen Switch sw2, indem Sie die entsprechende Verkabelung verwenden, die von NVIDIA SN2100 unterstützt wird.
3. Zeigen Sie die Attribute des Netzwerkports an:

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

## Beispiel anzeigen

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

Node: node1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----
e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false

Node: node2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----
e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false
```

4. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

### Beispiel anzeigen

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

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

-----
-----
node1      /lldp
          e3a    c1  (6a:ad:4f:98:3b:3f)  Eth1/1      -
          e3b    sw2  (b8:ce:f6:19:1a:7e)  swp3       -
node2      /lldp
          e3a    c1  (6a:ad:4f:98:3b:3f)  Eth1/2      -
          e3b    sw2  (b8:ce:f6:19:1b:96)  swp4       -
```

5. Vergewissern Sie sich beim Switch sw2, dass alle Knoten-Cluster-Ports aktiv sind:

```
net show interface
```

### Beispiel anzeigen

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

State  Name          Spd   MTU    Mode      LLDP
Summary
-----  -----  -----  -----  -----  -----
-----
...
...
UP      swp3          100G  9216   Trunk/L2   e3b
Master: bridge (UP)
UP      swp4          100G  9216   Trunk/L2   e3b
Master: bridge (UP)
UP      swp15          100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl (UP)
UP      swp16          100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl (UP)
```

6. Fahren Sie auf Switch c1 die Ports herunter, die mit den Cluster-Ports der Nodes verbunden sind, um ein Failover der Cluster LIFs zu ermöglichen.

```
(c1) # configure
Enter configuration commands, one per line. End with CNTL/Z.

(c1) (Config) # interface
(c1) (config-if-range) # shutdown <interface_list>
(c1) (config-if-range) # exit
(c1) (Config) # exit
(c1) #
```

7. Verschieben Sie die Knoten-Cluster-Ports vom alten Switch c1 auf den neuen Switch sw1, mit der entsprechenden Verkabelung unterstützt von NVIDIA SN2100.
8. Überprüfen der endgültigen Konfiguration des Clusters:

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

Jeder Port sollte angezeigt werden **up** Für Link Und gesund für Health Status.

## Beispiel anzeigen

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

Node: node1

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----



e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false

Node: node2

Ignore

Health
Port      IPspace      Broadcast Domain Link MTU      Admin/Oper      Status
Status

-----
-----



e3a      Cluster      Cluster          up      9000  auto/100000
healthy  false
e3b      Cluster      Cluster          up      9000  auto/100000
healthy  false
```

9. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

## 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	-

10. Vergewissern Sie sich bei den Switches sw1 und sw2, dass alle Knoten-Cluster-Ports aktiv sind:

```
net show interface
```

## Beispiel anzeigen

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

State	Name	Spd	MTU	Mode	LLDP
Summary					
---	-----	---	-----	-----	-----
---					
...					
...					
UP	swp3	100G	9216	Trunk/L2	e3a
Master:	bridge (UP)				
UP	swp4	100G	9216	Trunk/L2	e3a
Master:	bridge (UP)				
UP	swp15	100G	9216	BondMember	sw2 (swp15)
Master:	cluster_isl (UP)				
UP	swp16	100G	9216	BondMember	sw2 (swp16)
Master:	cluster_isl (UP)				

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

State	Name	Spd	MTU	Mode	LLDP
Summary					
---	-----	---	-----	-----	-----
---					
...					
...					
UP	swp3	100G	9216	Trunk/L2	e3b
Master:	bridge (UP)				
UP	swp4	100G	9216	Trunk/L2	e3b
Master:	bridge (UP)				
UP	swp15	100G	9216	BondMember	sw1 (swp15)
Master:	cluster_isl (UP)				
UP	swp16	100G	9216	BondMember	sw1 (swp16)
Master:	cluster_isl (UP)				

11. 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
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

## Schritt 3: Überprüfen Sie die Konfiguration

1. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

2. Vergewissern Sie sich, dass alle Cluster-Netzwerk-LIFs wieder an ihren Home-Ports sind:

```
network interface show
```

## Beispiel anzeigen

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

      Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----  -----  -----  -----  -----
-----  -----
Cluster
      node1_clus1  up/up    169.254.209.69/16  node1
e3a      true
      node1_clus2  up/up    169.254.49.125/16  node1
e3b      true
      node2_clus1  up/up    169.254.47.194/16  node2
e3a      true
      node2_clus2  up/up    169.254.19.183/16  node2
e3b      true
```

3. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

4. 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?

["Konfigurieren Sie die Überwachung des Switch-Systemzustands".](#)

## Migrieren Sie mit NVIDIA SN2100-Cluster-Switches zu einem Cluster mit zwei Nodes

Wenn Sie eine bestehende Cluster-Umgebung mit zwei Nodes ohne Switches nutzen, können Sie mit NVIDIA SN2100 Switches zu einer Switch-basierten Cluster-Umgebung mit zwei Nodes migrieren. So können Sie eine Skalierung über zwei Nodes im Cluster hinaus vornehmen.

Die von Ihnen verwendete Vorgehensweise hängt davon ab, ob Sie an jedem Controller zwei dedizierte Cluster-Netzwerk-Ports oder einen einzelnen Cluster-Port haben. Der dokumentierte Prozess funktioniert bei allen Knoten über optische oder Twinax-Ports, wird bei diesem Switch jedoch nicht unterstützt, wenn Knoten integrierte 10GBASE-T RJ45-Ports für die Cluster-Netzwerk-Ports verwenden.

## Prüfen Sie die Anforderungen

### Konfiguration mit zwei Nodes ohne Switches

Stellen Sie sicher, dass:

- Die Konfiguration mit zwei Nodes ohne Switches ist ordnungsgemäß eingerichtet und funktionsfähig.
- Auf den Knoten wird ONTAP 9.10.1P3 und höher ausgeführt.
- Alle Cluster-Ports haben den Status **up**.
- Alle logischen Cluster-Schnittstellen (LIFs) befinden sich im **up**-Zustand und auf ihren Home-Ports.

### Konfiguration des NVIDIA SN2100-Cluster-Switches

Stellen Sie sicher, dass:

- Beide Switches verfügen über Management-Netzwerk-Konnektivität.
- Auf die Cluster-Switches kann über eine Konsole zugegriffen werden.
- Bei NVIDIA SN2100, Node-to-Node-Switch und Switch-to-Switch-Verbindungen werden Twinax- oder Glasfaserkabel verwendet.



Siehe "[Prüfen Sie die Verkabelung und Konfigurationsüberlegungen](#)" Bei Einschränkungen und weiteren Details. Der "[Hardware Universe – Switches](#)" Enthält auch weitere Informationen über Verkabelung.

- Inter-Switch Link (ISL)-Kabel werden an die Anschlüsse `swp15` und `swp16` an beiden NVIDIA SN2100-Switches angeschlossen.
- Die Erstanpassung der beiden SN2100-Switches erfolgt so:
  - SN2100-Switches führen die neueste Version von Cumulus Linux aus
  - Auf die Switches werden Referenzkonfigurationsdateien (RCFs) angewendet
  - Auf den neuen Switches werden alle Site-Anpassungen wie SMTP, SNMP und SSH konfiguriert.

Der "[Hardware Universe](#)" Enthält die neuesten Informationen über die tatsächlichen Cluster-Ports für Ihre Plattformen.

## Migrieren Sie die Switches

### Zu den Beispielen

In den Beispielen dieses Verfahrens wird die folgende Terminologie für Cluster-Switch und Node verwendet:

- Die Namen der SN2100-Schalter lauten `sw1` und `sw2`.
- Die Namen der Cluster SVMs sind `node1` und `node2`.
- Die Namen der LIFs sind `_node1_clus1_` und `_node1_clus2` auf Knoten 1, und `_node2_clus1` und `_node2_clus2` auf Knoten 2.
- Der `cluster1::>` Eine Eingabeaufforderung gibt den Namen des Clusters an.
- Die in diesem Verfahren verwendeten Cluster-Ports sind `e3a` und `e3b`.
- Breakout-Ports haben das Format `swp[Port]s[Breakout-Port 0-3]`. Beispielsweise sind vier Breakout-Ports auf `swp1` `swp1s0`, `swp1s1`, `swp1s2` und `swp1s3`.

#### **Schritt: Bereiten Sie sich auf die Migration 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 ist.

2. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben y Wenn Sie dazu aufgefordert werden, fortfahren: `set -privilege advanced`

Die erweiterte Eingabeaufforderung ('\*>`Erscheint.

#### **Schritt: Ports und Verkabelung konfigurieren**

## Cumulus Linux 4.4.x

1. Deaktivieren Sie alle Node-Ports (keine ISL-Ports) auf den neuen Cluster-Switches sw1 und sw2.

Sie dürfen die ISL-Ports nicht deaktivieren.

Mit den folgenden Befehlen werden die Knotenanschlüsse an den Switches sw1 und sw2 deaktiviert:

```
cumulus@sw1:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit

cumulus@sw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw2:~$ net pending
cumulus@sw2:~$ net commit
```

2. Stellen Sie sicher, dass sich die ISL und die physischen Ports auf der ISL zwischen den beiden SN2100-Switches sw1 und sw2 auf den Ports swp15 und swp16 befinden:

```
net show interface
```

Die folgenden Befehle zeigen, dass die ISL-Ports bei den Switches sw1 und sw2 aktiviert sind:

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

State  Name      Spd  MTU  Mode      LLDP      Summary
-----  -----  -----  -----  -----  -----
...
...
UP      swp15    100G  9216  BondMember  sw2  (swp15)  Master:
cluster_isl (UP)
UP      swp16    100G  9216  BondMember  sw2  (swp16)  Master:
cluster_isl (UP)
```

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

```
State  Name      Spd  MTU  Mode      LLDP      Summary
-----  -----  -----  -----  -----  -----
...
...
UP      swp15    100G  9216  BondMember  sw1  (swp15)  Master:
cluster_isl (UP)
UP      swp16    100G  9216  BondMember  sw1  (swp16)  Master:
cluster_isl (UP)
```

## Cumulus Linux 5.x

1. Deaktivieren Sie alle an den Node ausgerichteten Ports (nicht ISL-Ports) auf den neuen Cluster-Switches sw1 und sw2.

Sie dürfen die ISL-Ports nicht deaktivieren.

Mit den folgenden Befehlen werden die Knotenanschlüsse an den Switches sw1 und sw2 deaktiviert:

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
down
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save

cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
down
cumulus@sw2:~$ nv config apply
cumulus@sw2:~$ nv config save
```

2. Stellen Sie sicher, dass sich die ISL und die physischen Ports auf der ISL zwischen den beiden SN2100-Switches sw1 und sw2 auf den Ports swp15 und swp16 befinden:

```
nv show interface
```

Die folgenden Beispiele zeigen, dass die ISL-Ports auf den Switches sw1 und sw2 aktiviert sind:

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

Interface Type	MTU Summary	Speed	State	Remote Host	Remote Port
...					
...					
+ swp14 swp	9216		down		
+ swp15 ISL Port	9216	100G	up	ossg-rcf1	Intra-Cluster Switch
swp15 ISL Port	swp				
+ swp16 ISL Port	9216	100G	up	ossg-rcf2	Intra-Cluster Switch
swp16 ISL Port	swp				

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

Interface Type	MTU Summary	Speed	State	Remote Host	Remote Port
...					
...					
+ swp14 swp	9216		down		
+ swp15 ISL Port	9216	100G	up	ossg-rcf1	Intra-Cluster Switch
swp15 ISL Port	swp				
+ swp16 ISL Port	9216	100G	up	ossg-rcf2	Intra-Cluster Switch
swp16 ISL Port	swp				

1. Überprüfen Sie, ob alle Cluster-Ports hochgefahren sind:

```
network port show
```

Jeder Port sollte angezeigt werden **up** Für Link Und gesund für Health Status.

## Beispiel anzeigen

```
cluster1::*> network port show
```

Node: node1

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

Node: node2

Ignore

Health	Health					Speed (Mbps)
Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper
Status	Status					
-----	-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----	-----
e3a	Cluster	Cluster		up	9000	auto/100000
healthy	false					
e3b	Cluster	Cluster		up	9000	auto/100000
healthy	false					

2. Vergewissern Sie sich, dass alle Cluster-LIFs betriebsbereit sind und betriebsbereit sind:

```
network interface show
```

Jede LIF im Cluster sollte für „true“ anzeigen Is Home Und ich habe ein Status Admin/Oper Von up/up.

## Beispiel anzeigen

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

          Logical      Status      Network      Current
Current Is
Vserver      Interface  Admin/Oper  Address/Mask      Node
Port      Home
-----
-----
Cluster
      node1_clus1  up/up      169.254.209.69/16  node1
e3a      true
      node1_clus2  up/up      169.254.49.125/16  node1
e3b      true
      node2_clus1  up/up      169.254.47.194/16  node2
e3a      true
      node2_clus2  up/up      169.254.19.183/16  node2
e3b      true
```

3. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

## Beispiel anzeigen

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

          Logical
Vserver      Interface      Auto-revert
-----
Cluster
      node1_clus1  false
      node1_clus2  false
      node2_clus1  false
      node2_clus2  false
```

4. Trennen Sie das Kabel vom Cluster-Port e3a auf node1, und verbinden sie dann e3a mit Port 3 am Cluster-Switch sw1. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.

Der "[Hardware Universe – Switches](#)" Enthält weitere Informationen zur Verkabelung.

5. Trennen Sie das Kabel vom Cluster-Port e3a auf node2, und verbinden sie dann e3a mit Port 4 am Cluster-Switch sw1. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.

### Cumulus Linux 4.4.x

1. bei Switch sw1 aktivieren Sie alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden alle an den Knoten ausgerichteten Ports auf Switch sw1 aktiviert.

```
cumulus@sw1:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

2. bei Switch sw1 überprüfen Sie, ob alle Ports aktiviert sind:

```
net show interface all
```

State	Name	Spd	MTU	Mode	LLDP	Summary
DN	swp1s0	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s1	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s2	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s3	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s0	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s1	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s2	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s3	25G	9216	Trunk/L2		Master:
br_default(UP)						
UP	swp3	100G	9216	Trunk/L2	node1 (e3a)	Master:
br_default(UP)						
UP	swp4	100G	9216	Trunk/L2	node2 (e3a)	Master:
br_default(UP)						
...						
...						
UP	swp15	100G	9216	BondMember	swp15	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	swp16	Master:
cluster_isl(UP)						
...						

Cumulus Linux 5.x

1. bei Switch sw1 aktivieren Sie alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden alle an den Knoten ausgerichteten Ports auf Switch sw1 aktiviert

```
cumulus@sw1:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
up
cumulus@sw1:~$ nv config apply
cumulus@sw1:~$ nv config save
```

2. bei Switch sw1 überprüfen Sie, ob alle Ports aktiviert sind:

```
nv show interface
```

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

Interface      State   Speed   MTU      Type      Remote Host
Remote Port    Summary
-----  -----  -----  -----  -----
-----  -----  -----  -----  -----
...
...
swp1s0          up     10G     9216    swp      odq-a300-1a
e0a
swp1s1          up     10G     9216    swp      odq-a300-1b
e0a
swp1s2          down   10G     9216    swp
swp1s3          down   10G     9216    swp
swp2s0          down   25G     9216    swp
swp2s1          down   25G     9216    swp
swp2s2          down   25G     9216    swp
swp2s3          down   25G     9216    swp
swp3            down   9216    swp
swp4            down   9216    swp
...
...
swp14            down   9216    swp
swp15            up     100G    9216    swp      ossg-int-rcf10
swp15
swp16            up     100G    9216    swp      ossg-int-rcf10
swp16
```

1. Überprüfen Sie, ob alle Cluster-Ports hochgefahren sind:

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

## Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

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

Node: node1

Ignore

Health      Health
Port        IPspace      Broadcast Domain Link MTU Admin/Oper
Status      Status

-----
-----
e3a         Cluster      Cluster          up    9000  auto/100000
healthy    false
e3b         Cluster      Cluster          up    9000  auto/100000
healthy    false

Node: node2

Ignore

Health      Health
Port        IPspace      Broadcast Domain Link MTU Admin/Oper
Status      Status

-----
-----
e3a         Cluster      Cluster          up    9000  auto/100000
healthy    false
e3b         Cluster      Cluster          up    9000  auto/100000
healthy    false
```

## 2. Informationen zum Status der Nodes im Cluster anzeigen:

```
cluster show
```

## Beispiel anzeigen

Im folgenden Beispiel werden Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster angezeigt:

```
cluster1::*> cluster show

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

3. Trennen Sie das Kabel vom Cluster-Port e3b auf node1, und verbinden sie e3b mit Port 3 am Cluster-Switch sw2. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.
4. Trennen Sie das Kabel vom Cluster-Port e3b auf node2, und verbinden sie e3b mit Port 4 am Cluster-Switch sw2. Verwenden Sie dazu die geeignete Verkabelung, die von den SN2100-Switches unterstützt wird.

## Cumulus Linux 4.4.x

1. aktivieren Sie auf Switch sw2 alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden die Node-Ports am Switch sw2 aktiviert:

```
cumulus@sw2:~$ net del interface swp1s0-3, swp2s0-3, swp3-14 link  
down  
cumulus@sw2:~$ net pending  
cumulus@sw2:~$ net commit
```

2. bei Switch sw2 überprüfen Sie, ob alle Ports aktiviert sind:

```
net show interface all
```

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

State	Name	Spd	MTU	Mode	LLDP	Summary
---	---	---	---	---	---	---
...						
DN	swp1s0	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s1	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s2	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp1s3	10G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s0	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s1	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s2	25G	9216	Trunk/L2		Master:
br_default(UP)						
DN	swp2s3	25G	9216	Trunk/L2		Master:
br_default(UP)						
UP	swp3	100G	9216	Trunk/L2	node1 (e3b)	Master:
br_default(UP)						
UP	swp4	100G	9216	Trunk/L2	node2 (e3b)	Master:
br_default(UP)						
...						
...						
UP	swp15	100G	9216	BondMember	swp15	Master:
cluster_isl(UP)						
UP	swp16	100G	9216	BondMember	swp16	Master:
cluster_isl(UP)						
...						

3. Überprüfen Sie bei beiden Switches sw1 und sw2, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Schalter sw1 und sw2:

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

## Cumulus Linux 5.x

1. aktivieren Sie auf Switch sw2 alle nach Knoten gerichteten Ports.

Mit den folgenden Befehlen werden die Node-Ports am Switch sw2 aktiviert:

```
cumulus@sw2:~$ nv set interface swp1s0-3,swp2s0-3,swp3-14 link state
up
cumulus@sw2:~$ nv config apply
cumulus@sw2:~$ nv config save
```

2. bei Switch sw2 überprüfen Sie, ob alle Ports aktiviert sind:

```
nv show interface
```

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

Interface      State   Speed   MTU      Type      Remote Host
Remote Port    Summary
-----  -----  -----  -----  -----
...
...
swp1s0          up     10G    9216    swp       odq-a300-1a
e0a
swp1s1          up     10G    9216    swp       odq-a300-1b
e0a
swp1s2          down   10G    9216    swp
swp1s3          down   10G    9216    swp
swp2s0          down   25G    9216    swp
swp2s1          down   25G    9216    swp
swp2s2          down   25G    9216    swp
swp2s3          down   25G    9216    swp
swp3            down   9216   swp
swp4            down   9216   swp
...
...
swp14            down   9216   swp
swp15            up     100G   9216   swp       ossg-int-rcf10
swp15
swp16            up     100G   9216   swp       ossg-int-rcf10
swp16
```

3. Überprüfen Sie bei beiden Switches sw1 und sw2, ob beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
nv show interface --view=lldp
```

Die folgenden Beispiele zeigen die entsprechenden Ergebnisse für beide Schalter sw1 und sw2:

```
cumulus@sw1:~$ nv show interface --view=lldp

Interface      Speed   Type      Remote Host
Remote Port
-----  -----  -----  -----
...
...
swp1s0          10G    swp       odq-a300-1a
e0a
```

swp1s1	10G	swp	odq-a300-1b
e0a			
swp1s2	10G	swp	
swp1s3	10G	swp	
swp2s0	25G	swp	
swp2s1	25G	swp	
swp2s2	25G	swp	
swp2s3	25G	swp	
swp3		swp	
swp4		swp	
...			
...			
swp14		swp	
swp15	100G	swp	ossg-int-rcf10
swp15			
swp16	100G	swp	ossg-int-rcf10
swp16			

cumulus@sw2:~\$ **nv show interface --view=lldp**

Interface Remote Port	Speed	Type	Remote Host
-----	-----	-----	-----
...			
...			
swp1s0	10G	swp	odq-a300-1a
e0a			
swp1s1	10G	swp	odq-a300-1b
e0a			
swp1s2	10G	swp	
swp1s3	10G	swp	
swp2s0	25G	swp	
swp2s1	25G	swp	
swp2s2	25G	swp	
swp2s3	25G	swp	
swp3		swp	
swp4		swp	
...			
...			
swp14		swp	
swp15	100G	swp	ossg-int-rcf10
swp15			
swp16	100G	swp	ossg-int-rcf10
swp16			

1. zeigt Informationen über die erkannten Netzwerkgeräte im Cluster an:

```
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
          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        -
```

2. Vergewissern Sie sich, dass alle Cluster-Ports aktiv sind:

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

## Beispiel anzeigen

Im folgenden Beispiel werden alle Cluster-Ports auf node1 und node2 angezeigt:

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

Node: node1

Ignore

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

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
```

### Schritt 3: Überprüfen Sie die Konfiguration

1. Aktivieren Sie das automatische Zurücksetzen auf allen Cluster-LIFs:

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

## Beispiel anzeigen

```
cluster1::*> net interface modify -vserver Cluster -lif * -auto
-revert true

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

2. Vergewissern Sie sich, dass alle Schnittstellen angezeigt werden true Für Is Home:

```
net interface show -vserver Cluster
```



Dies kann eine Minute dauern.

## Beispiel anzeigen

Das folgende Beispiel zeigt, dass alle LIFs auf node1 und node2 liegen und dass Is Home Die Ergebnisse sind wahr:

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

      Logical      Status      Network      Current
Current Is
Vserver  Interface      Admin/Oper  Address/Mask      Node      Port
Home
-----  -----
-----  -----
Cluster
      node1_clus1  up/up      169.254.209.69/16  node1      e3a
true
      node1_clus2  up/up      169.254.49.125/16  node1      e3b
true
      node2_clus1  up/up      169.254.47.194/16  node2      e3a
true
      node2_clus2  up/up      169.254.19.183/16  node2      e3b
true
```

3. Vergewissern Sie sich, dass die Einstellungen deaktiviert sind:

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

#### Beispiel anzeigen

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

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

4. Überprüfen Sie den Status der Node-Mitglieder im Cluster:

```
cluster show
```

#### Beispiel anzeigen

Das folgende Beispiel zeigt Informationen über den Systemzustand und die Berechtigung der Nodes im Cluster:

```
cluster1::*> cluster show

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

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 anzeigen:

```
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 anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date                LIF          LIF
Loss
-----
-----
node1
      3/5/2022 19:21:18 -06:00  node1_clus2      node2-clus1
none
      3/5/2022 19:21:20 -06:00  node1_clus2      node2_clus2
none
node2
      3/5/2022 19:21:18 -06:00  node2_clus2      node1_clus1
none
      3/5/2022 19:21:20 -06:00  node2_clus2      node1_clus2
none
```

## Alle ONTAP Versionen

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 node1
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e3a
Cluster node1_clus2 169.254.49.125 node1 e3b
Cluster node2_clus1 169.254.47.194 node2 e3a
Cluster node2_clus2 169.254.19.183 node2 e3b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

```

1. Ändern Sie die Berechtigungsebene zurück zu admin:

```
set -privilege admin
```

2. 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?

["Konfigurieren Sie die Überwachung des Switch-Systemzustands".](#)

## Ersetzen Sie die Schalter

### Ersetzen Sie einen NVIDIA SN2100-Cluster-Switch

Gehen Sie folgendermaßen vor, um einen defekten NVIDIA SN2100-Switch in einem Cluster-Netzwerk zu ersetzen. Dies ist ein NDU (Non Disruptive Procedure, NDU).

## Prüfen Sie die Anforderungen

### Bestehende Cluster- und Netzwerkinfrastruktur

Stellen Sie sicher, dass:

- Das vorhandene Cluster wird mit mindestens einem vollständig verbundenen Cluster-Switch als voll funktionsfähig geprüft.
- Alle Cluster-Ports sind aktiv.
- Alle logischen Cluster-Schnittstellen (LIFs) laufen und auf ihren Home-Ports.
- Das `ONTAP cluster ping-cluster -node node1` Der Befehl gibt an, dass grundlegende und größere Verbindungen als PMTU auf allen Pfaden erfolgreich sind.

### NVIDIA SN2100-Ersatzschalter

Stellen Sie sicher, dass:

- Die Konnektivität des Managementnetzwerks am Ersatz-Switch funktioniert.
- Der Konsolenzugriff auf den Ersatz-Switch erfolgt.
- Die Knotenverbindungen sind die Anschlüsse `swp1` bis `swp14`.
- Alle Inter-Switch Link (ISL)-Ports sind an den Ports `swp15` und `swp16` deaktiviert.
- Die gewünschte Referenzkonfigurationsdatei (RCF) und der Bildschalter des Betriebssystems Cumulus werden auf den Switch geladen.
- Die anfängliche Anpassung des Schalters ist abgeschlossen.

Vergewissern Sie sich außerdem, dass alle Änderungen an früheren Standorten, wie STP, SNMP und SSH, auf den neuen Switch kopiert werden.



Sie müssen den Befehl zum Migrieren einer Cluster-LIF von dem Node ausführen, auf dem die Cluster-LIF gehostet wird.

### Aktivieren Sie die Konsolenprotokollierung

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

- Lassen Sie AutoSupport während der Wartung aktiviert.
- Lösen Sie vor und nach der Wartung einen Wartungs-AutoSupport aus, um die Case-Erstellung für die Dauer der Wartung zu deaktivieren. Lesen Sie diesen Knowledge Base-Artikel "["SU92: Unterdrücken der automatischen Case-Erstellung während geplanter Wartungsfenster"](#)" Entnehmen.
- Aktivieren Sie die Sitzungsprotokollierung für beliebige CLI-Sitzungen. Anweisungen zum Aktivieren der Sitzungsprotokollierung finden Sie im Abschnitt „Protokollierung der Sitzungsausgabe“ in diesem Knowledge Base Artikel "["So konfigurieren Sie PuTTY für optimale Konnektivität zu ONTAP-Systemen"](#)".

### Tauschen Sie den Schalter aus

#### Zu den Beispielen

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

- Die Namen der vorhandenen NVIDIA SN2100-Switches lauten `sw1` und `sw2`.

- Der Name des neuen NVIDIA SN2100 Switch lautet *nsw2*.
- Die Knotennamen sind *node1* und *node2*.
- Die Cluster-Ports auf jedem Node lauten *e3a* und *e3b*.
- Die Cluster LIF-Namen sind *node1\_clus1* und *node1\_clus2* für *node1*, und *node2\_clus1* und *node2\_clus2* für *node2*.
- Die Eingabeaufforderung für Änderungen an allen Cluster-Nodes lautet `cluster1::*`
- Breakout-Ports haben das Format *swp[Port]s[Breakout-Port 0-3]*. Beispielsweise sind vier Breakout-Ports auf *swp1* *swp1s0*, *swp1s1*, *swp1s2* und *swp1s3*.

### Allgemeines zur Cluster-Netzwerktopologie

Dieses Verfahren basiert auf der folgenden Cluster-Netzwerktopologie:

## Beispieltopologie anzeigen

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

Node: node1

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	Health	Speed (Mbps)	Health
e3a	Cluster	Cluster		up	9000	auto/100000	healthy			
false										
e3b	Cluster	Cluster		up	9000	auto/100000	healthy			
false										

Node: node2

Port	IPspace	Broadcast	Domain	Link	MTU	Admin/Oper	Status	Health	Speed (Mbps)	Health
e3a	Cluster	Cluster		up	9000	auto/100000	healthy			
false										
e3b	Cluster	Cluster		up	9000	auto/100000	healthy			
false										

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

Current	Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port	
Cluster	node1_clus1	up/up	169.254.209.69/16	node1	e3a	
true	node1_clus2	up/up	169.254.49.125/16	node1	e3b	
true						

```

node2_clus1  up/up      169.254.47.194/16  node2      e3a
true
node2_clus2  up/up      169.254.19.183/16  node2      e3b
true

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      -

```

+

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw2	e3a
swp4	100G	Trunk/L2	sw2	e3a
swp15	100G	BondMember	sw2	swp15
swp16	100G	BondMember	sw2	swp16

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	sw1	e3b
swp4	100G	Trunk/L2	sw1	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

### Schritt 1: Vorbereitung auf den Austausch

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 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. Installieren Sie das entsprechende RCF und das entsprechende Image auf dem Switch, nsw2, und treffen Sie die erforderlichen Standortvorbereitungen.

Überprüfen, laden und installieren Sie gegebenenfalls die entsprechenden Versionen der RCF- und Cumulus-Software für den neuen Switch.

- a. Sie können die entsprechende Cumulus-Software für Ihre Cluster-Switches von der Seite *NVIDIA Support* herunterladen. Folgen Sie den Schritten auf der Download-Seite, um das Cumulus Linux für die Version der ONTAP Software, die Sie installieren, herunterzuladen.
- b. Das entsprechende RCF ist im erhältlich "[NVIDIA Cluster und Storage Switches](#)" Seite. Befolgen Sie die Schritte auf der Download-Seite, um den korrekten RCF für die Version der von Ihnen installierenden ONTAP-Software herunterzuladen.

#### **Schritt: Ports und Verkabelung konfigurieren**

### Cumulus Linux 4.4.3

1. Melden Sie sich beim neuen Switch nsw2 als admin an und fahren Sie alle Ports herunter, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports swp1 bis swp14).

Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt haben.

```
cumulus@nsw2:~$ net add interface swp1s0-3, swp2s0-3, swp3-14 link
down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

2. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

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

Warning: Disabling the auto-revert feature of the cluster logical interface may effect the availability of your cluster network. Are you sure you want to continue? {y|n}: **y**

3. Stellen Sie sicher, dass die automatische Rücksetzung bei allen Cluster-LIFs deaktiviert ist:

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

4. Schließen Sie die ISL-Ports swp15 und swp16 am SN2100-Switch sw1 ab.

```
cumulus@sw1:~$ net add interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

5. Entfernen Sie alle Kabel vom SN2100 sw1-Switch, und verbinden Sie sie dann mit den gleichen Ports am SN2100 nsw2-Switch.

6. Die ISL-Ports swp15 und swp16 zwischen den Switches sw1 und nsw2.

Die folgenden Befehle ermöglichen ISL-Ports swp15 und swp16 auf Switch sw1:

```
cumulus@sw1:~$ net del interface swp15-16 link down
cumulus@sw1:~$ net pending
cumulus@sw1:~$ net commit
```

Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch sw1 aufstehen:

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

  State  Name          Spd   MTU    Mode          LLDP          Summary
  -----  -----  -----  -----  -----  -----
  ...
  ...
  UP      swp15        100G  9216  BondMember  nsw2 (swp15)  Master:
  cluster_isl (UP)
  UP      swp16        100G  9216  BondMember  nsw2 (swp16)  Master:
  cluster_isl (UP)
```

Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch nsw2 aktiv sind:

```
cumulus@nsw2:~$ net show interface

  State  Name          Spd   MTU    Mode          LLDP          Summary
  -----  -----  -----  -----  -----  -----
  ...
  ...
  UP      swp15        100G  9216  BondMember  sw1 (swp15)  Master:
  cluster_isl (UP)
  UP      swp16        100G  9216  BondMember  sw1 (swp16)  Master:
  cluster_isl (UP)
```

7. Überprüfen Sie diesen Port e3b Ist auf allen Knoten aktiv:

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

Die Ausgabe sollte wie folgt aussehen:

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

Node: node1

Ignore

Health      Health
Port        IPspace      Broadcast Domain Link MTU      Admin/Oper
Status      Status

-----
-----
e3a         Cluster      Cluster          up      9000  auto/100000
healthy    false
e3b         Cluster      Cluster          up      9000  auto/100000
healthy    false
```

Node: node2

```
Ignore

Health      Health
Port        IPspace      Broadcast Domain Link MTU      Admin/Oper
Status      Status

-----
-----
e3a         Cluster      Cluster          up      9000  auto/100000
healthy    false
e3b         Cluster      Cluster          up      9000  auto/100000
healthy    false
```

8. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

```
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    nsw2 (b8:ce:f6:19:1b:b6)  swp3          -
node2      /lldp
          e3a    sw1  (b8:ce:f6:19:1a:7e)  swp4          -
          e3b    nsw2 (b8:ce:f6:19:1b:b6)  swp4          -
```

9. Vergewissern Sie sich, dass alle Node-Cluster-Ports aktiv sind:

```
net show interface
```

```
cumulus@nsw2:~$ net show interface

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)
UP      swp15         100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl (UP)
UP      swp16         100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl (UP)
```

10. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
net show lldp
```

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

```
cumulus@nsw2:~$ net show lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

11. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

12. Bringen Sie auf Switch nsw2 die Ports an, die mit den Netzwerkports der Knoten verbunden sind.

```
cumulus@nsw2:~$ net del interface swp1-14 link down
cumulus@nsw2:~$ net pending
cumulus@nsw2:~$ net commit
```

13. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

```
cluster1::*> cluster show

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

14. Vergewissern Sie sich, dass alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

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

## Cumulus Linux 5.x

1. Melden Sie sich beim neuen Switch nsw2 als admin an und fahren Sie alle Ports herunter, die mit den Node-Cluster-Schnittstellen verbunden werden (Ports swp1 bis swp14).

Die LIFs auf den Cluster-Nodes sollten für jeden Node bereits ein Failover auf den anderen Cluster-Port durchgeführt haben.

```
cumulus@nsw2:~$ nv set interface swp15-16 link state down
cumulus@nsw2:~$ nv config apply
```

2. Deaktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

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

Warning: Disabling the auto-revert feature of the cluster logical interface may effect the availability of your cluster network. Are you sure you want to continue? {y|n}: **y**

3. Stellen Sie sicher, dass die automatische Rücksetzung bei allen Cluster-LIFs deaktiviert ist:

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

4. Schließen Sie die ISL-Ports swp15 und swp16 am SN2100-Switch sw1 ab.

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

5. Entfernen Sie alle Kabel vom SN2100 sw1-Switch, und verbinden Sie sie dann mit den gleichen Ports am SN2100 nsw2-Switch.
6. Die ISL-Ports swp15 und swp16 zwischen den Switches sw1 und nsw2.

Die folgenden Befehle ermöglichen ISL-Ports swp15 und swp16 auf Switch sw1:

```
cumulus@sw1:~$ nv set interface swp15-16 link state down
cumulus@sw1:~$ nv config apply
```

Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch sw1 aufstehen:

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

State	Name	Spd	MTU	Mode	LLDP	Summary
-----	-----	---	-----	-----	-----	-----
...						
...						
UP	swp15	100G	9216	BondMember	nsw2 (swp15)	Master:
	cluster_isl (UP)					
UP	swp16	100G	9216	BondMember	nsw2 (swp16)	Master:
	cluster_isl (UP)					

Das folgende Beispiel zeigt, dass die ISL-Ports auf Switch nsw2 aktiv sind:

```

cumulus@nsw2:~$ nv show interface

  State  Name          Spd    MTU    Mode          LLDP          Summary
  ----  -----  -----  -----  -----  -----  -----
  ...
  ...
  UP      swp15        100G  9216  BondMember  sw1 (swp15)  Master:
  cluster_isl (UP)
  UP      swp16        100G  9216  BondMember  sw1 (swp16)  Master:
  cluster_isl (UP)

```

7. Überprüfen Sie diesen Port e3b Ist auf allen Knoten aktiv:

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

Die Ausgabe sollte wie folgt aussehen:

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

Node: node1

Ignore

Health      Health
Port        IPspace      Broadcast Domain Link MTU      Admin/Oper
Status      Status

-----
-----
e3a         Cluster      Cluster          up      9000  auto/100000
healthy    false
e3b         Cluster      Cluster          up      9000  auto/100000
healthy    false
```

Node: node2

```
Ignore

Health      Health
Port        IPspace      Broadcast Domain Link MTU      Admin/Oper
Status      Status

-----
-----
e3a         Cluster      Cluster          up      9000  auto/100000
healthy    false
e3b         Cluster      Cluster          up      9000  auto/100000
healthy    false
```

8. Die Cluster-Ports auf jedem Node sind nun aus Sicht der Nodes mit Cluster-Switches auf die folgende Weise verbunden:

```
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    nsw2 (b8:ce:f6:19:1b:b6)  swp3          -
node2      /lldp
          e3a    sw1  (b8:ce:f6:19:1a:7e)  swp4          -
          e3b    nsw2 (b8:ce:f6:19:1b:b6)  swp4          -
```

9. Vergewissern Sie sich, dass alle Node-Cluster-Ports aktiv sind:

```
nv show interface
```

```
cumulus@nsw2:~$ nv show interface

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)
UP      swp15         100G  9216   BondMember  sw1 (swp15)
Master: cluster_isl (UP)
UP      swp16         100G  9216   BondMember  sw1 (swp16)
Master: cluster_isl (UP)
```

10. Vergewissern Sie sich, dass beide Knoten jeweils eine Verbindung zu jedem Switch haben:

```
nv show interface lldp
```

Das folgende Beispiel zeigt die entsprechenden Ergebnisse für beide Switches:

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

```
cumulus@nsw2:~$ nv show interface lldp
```

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3b
swp4	100G	Trunk/L2	node2	e3b
swp15	100G	BondMember	sw1	swp15
swp16	100G	BondMember	sw1	swp16

11. Aktivieren Sie die automatische Zurücksetzung auf den Cluster-LIFs:

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

12. Bringen Sie auf Switch nsw2 die Ports an, die mit den Netzwerkports der Knoten verbunden sind.

```
cumulus@nsw2:~$ nv set interface swp1-14 link state up
cumulus@nsw2:~$ nv config apply
```

13. Zeigen Sie Informationen über die Nodes in einem Cluster an:

```
cluster show
```

Dieses Beispiel zeigt, dass der Zustand des Node für Node 1 und node2 in diesem Cluster „true“ lautet:

```
cluster1::*> cluster show

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

14. Vergewissern Sie sich, dass alle physischen Cluster-Ports aktiv sind:

```
network port show ipspace Cluster
```

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

Node node1

Ignore

Health	Health					Speed (Mbps)
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

Health	Health					Speed (Mbps)
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					

### Schritt 3: Überprüfen Sie die Konfiguration

### Cumulus Linux 4.4.3

1. Vergewissern Sie sich, dass das Cluster-Netzwerk ordnungsgemäß funktioniert.

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

### Cumulus Linux 5.x

1. Vergewissern Sie sich, dass das Cluster-Netzwerk ordnungsgemäß funktioniert.

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

LocalPort	Speed	Mode	RemoteHost	RemotePort
swp3	100G	Trunk/L2	node1	e3a
swp4	100G	Trunk/L2	node2	e3a
swp15	100G	BondMember	nsw2	swp15
swp16	100G	BondMember	nsw2	swp16

1. Ändern Sie die Berechtigungsebene zurück zu admin:

```
set -privilege admin
```

2. 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?

["Konfigurieren Sie die Überwachung des Switch-Systemzustands".](#)

## Ersetzen Sie NVIDIA SN2100-Cluster-Switches durch Switch-lose Verbindungen

Sie können von einem Cluster mit einem Switch-Cluster-Netzwerk zu einem migrieren, mit dem zwei Nodes direkt für ONTAP 9.3 und höher verbunden sind.

## Prüfen Sie die Anforderungen

### Richtlinien

Lesen Sie sich die folgenden Richtlinien durch:

- Die Migration auf eine Cluster-Konfiguration mit zwei Nodes ohne Switches ist ein unterbrechungsfreier Betrieb. Die meisten Systeme verfügen auf jedem Node über zwei dedizierte Cluster Interconnect Ports, jedoch können Sie dieses Verfahren auch für Systeme mit einer größeren Anzahl an dedizierten Cluster Interconnect Ports auf jedem Node verwenden, z. B. vier, sechs oder acht.
- Sie können die Cluster Interconnect-Funktion ohne Switches nicht mit mehr als zwei Nodes verwenden.
- Wenn Sie bereits über ein zwei-Node-Cluster mit Cluster Interconnect Switches verfügen und ONTAP 9.3 oder höher ausgeführt wird, können Sie die Switches durch direkte Back-to-Back-Verbindungen zwischen den Nodes ersetzen.

### Bevor Sie beginnen

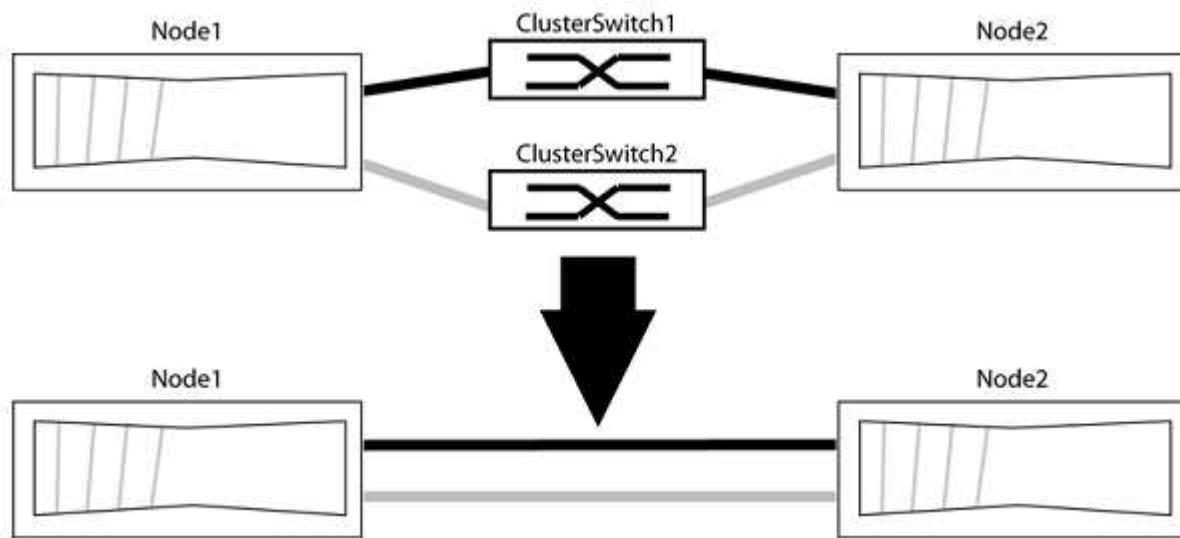
Stellen Sie sicher, dass Sie Folgendes haben:

- Ein gesundes Cluster, das aus zwei durch Cluster-Switches verbundenen Nodes besteht. Auf den Nodes muss dieselbe ONTAP Version ausgeführt werden.
- Jeder Node mit der erforderlichen Anzahl an dedizierten Cluster-Ports, die redundante Cluster Interconnect-Verbindungen bereitstellen, um die Systemkonfiguration zu unterstützen. Beispielsweise gibt es zwei redundante Ports für ein System mit zwei dedizierten Cluster Interconnect Ports auf jedem Node.

## Migrieren Sie die Switches

### Über diese Aufgabe

Durch das folgende Verfahren werden die Cluster-Switches in einem 2-Node-Cluster entfernt und jede Verbindung zum Switch durch eine direkte Verbindung zum Partner-Node ersetzt.



### Zu den Beispielen

Die Beispiele in dem folgenden Verfahren zeigen Nodes, die „e0a“ und „e0b“ als Cluster-Ports verwenden. Ihre Nodes verwenden möglicherweise unterschiedliche Cluster-Ports, je nach System.

## Schritt: Bereiten Sie sich auf die Migration vor

1. Ändern Sie die Berechtigungsebene in erweitert, indem Sie eingeben y Wenn Sie dazu aufgefordert werden, fortzufahren:

```
set -privilege advanced
```

Die erweiterte Eingabeaufforderung \*> Angezeigt.

2. ONTAP 9.3 und höher unterstützt die automatische Erkennung von Clustern ohne Switches, die standardmäßig aktiviert sind.

Sie können überprüfen, ob die Erkennung von Clustern ohne Switch durch Ausführen des Befehls „Advanced Privilege“ aktiviert ist:

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

### Beispiel anzeigen

Die folgende Beispielausgabe zeigt, ob die Option aktiviert ist.

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

Wenn „Switch less Cluster Detection aktivieren“ lautet `false`, Wen Sie sich an den NetApp Support.

3. 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=<number_of_hours>h
```

Wo `h` Dies ist die Dauer des Wartungsfensters von Stunden. Die Meldung wird vom technischen Support dieser Wartungsaufgabe benachrichtigt, damit die automatische Case-Erstellung während des Wartungsfensters unterdrückt werden kann.

Im folgenden Beispiel unterdrückt der Befehl die automatische Case-Erstellung für zwei Stunden:

### Beispiel anzeigen

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

## Schritt: Ports und Verkabelung konfigurieren

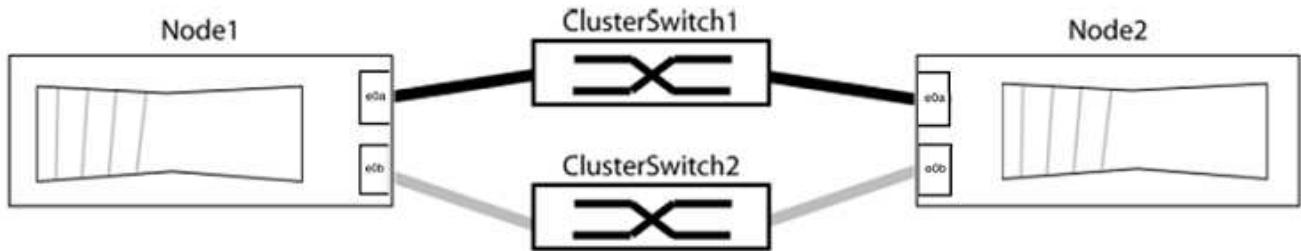
1. Ordnen Sie die Cluster-Ports an jedem Switch in Gruppen, so dass die Cluster-Ports in `grp1` zu Cluster-Switch 1 wechseln und die Cluster-Ports in `grp2` zu Cluster-Switch 2 wechseln. Diese Gruppen sind

später im Verfahren erforderlich.

## 2. Ermitteln der Cluster-Ports und Überprüfen von Verbindungsstatus und Systemzustand:

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

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



Überprüfen Sie, ob die Ports einen Wert von haben `up` Für die Spalte „Link“ und einen Wert von `healthy` Für die Spalte „Integritätsstatus“.

## Beispiel anzeigen

3. Vergewissern Sie sich, dass alle Cluster-LIFs auf ihren Home-Ports sind.

Vergewissern Sie sich, dass die Spalte „ist-Home“ angezeigt wird true Für jedes der Cluster-LIFs:

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

## Beispiel anzeigen

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

Wenn Cluster-LIFs sich nicht auf ihren Home-Ports befinden, setzen Sie die LIFs auf ihre Home-Ports zurück:

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

4. Deaktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs:

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

5. Vergewissern Sie sich, dass alle im vorherigen Schritt aufgeführten Ports mit einem Netzwerk-Switch verbunden sind:

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

Die Spalte „ermittelte Geräte“ sollte der Name des Cluster-Switch sein, mit dem der Port verbunden ist.

## Beispiel anzeigen

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

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

6. 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 anzeigen:

```
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 anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date                LIF          LIF
Loss
-----
-----
node1
      3/5/2022 19:21:18 -06:00  node1_clus2      node2-clus1
none
      3/5/2022 19:21:20 -06:00  node1_clus2      node2_clus2
none
node2
      3/5/2022 19:21:18 -06:00  node2_clus2      node1_clus1
none
      3/5/2022 19:21:20 -06:00  node2_clus2      node1_clus2
none
```

## Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

```

1. Überprüfen Sie, ob das Cluster ordnungsgemäß ist:

```
cluster ring show
```

Alle Einheiten müssen entweder Master oder sekundär sein.

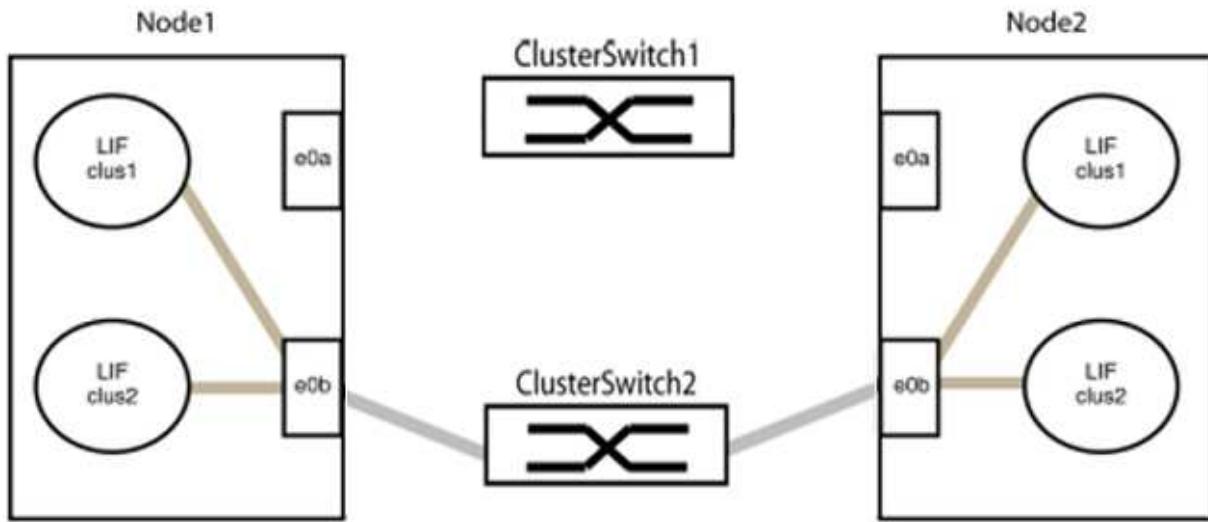
2. Richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 1 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von group1 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

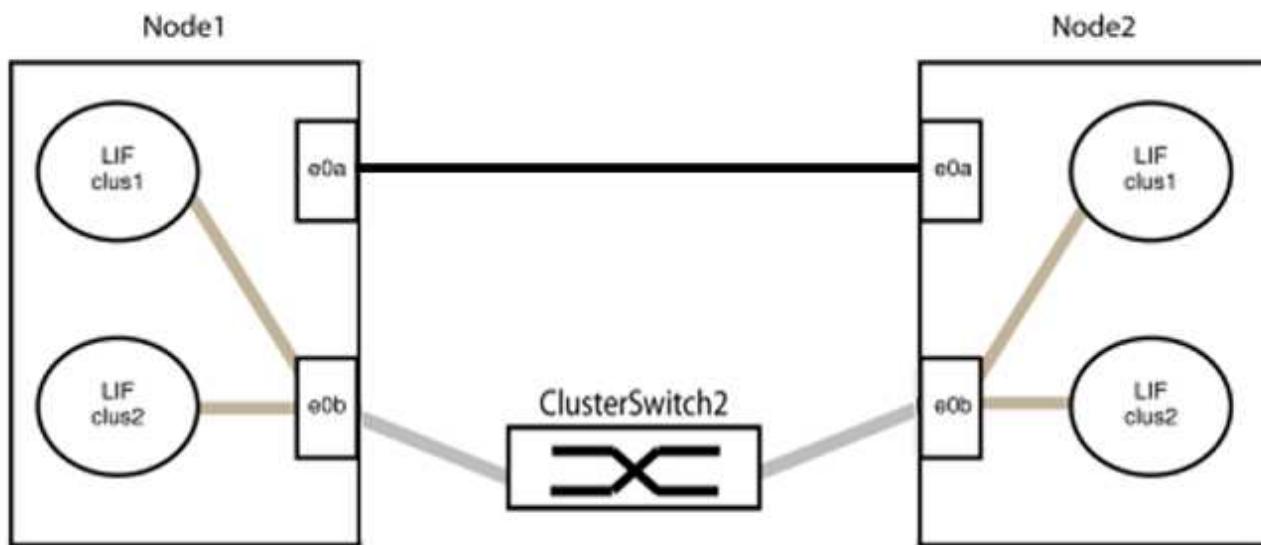
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Grupp1 ab.

Im folgenden Beispiel werden die Kabel von Port „e0a“ auf jeden Node getrennt, und der Cluster-Traffic wird auf jedem Node durch den Switch und Port „e0b“ fortgesetzt:



b. Schließen Sie die Anschlüsse in der Gruppe p1 zurück an die Rückseite an.

Im folgenden Beispiel ist „e0a“ auf node1 mit „e0a“ auf node2 verbunden:



3. Die Cluster-Netzwerkoption ohne Switches wechselt von `false` Bis `true`. Dies kann bis zu 45 Sekunden dauern. Vergewissern Sie sich, dass die Option „ohne Switch“ auf eingestellt ist `true`:

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

Das folgende Beispiel zeigt, dass das Cluster ohne Switches aktiviert ist:

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

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

## ONTAP 9.9.1 und höher

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

```
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 anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date                LIF          LIF
Loss
-----
-----
node1
      3/5/2022 19:21:18 -06:00  node1_clus2      node2-clus1
none
      3/5/2022 19:21:20 -06:00  node1_clus2      node2_clus2
none
node2
      3/5/2022 19:21:18 -06:00  node2_clus2      node1_clus1
none
      3/5/2022 19:21:20 -06:00  node2_clus2      node1_clus2
none
```

## Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

```



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

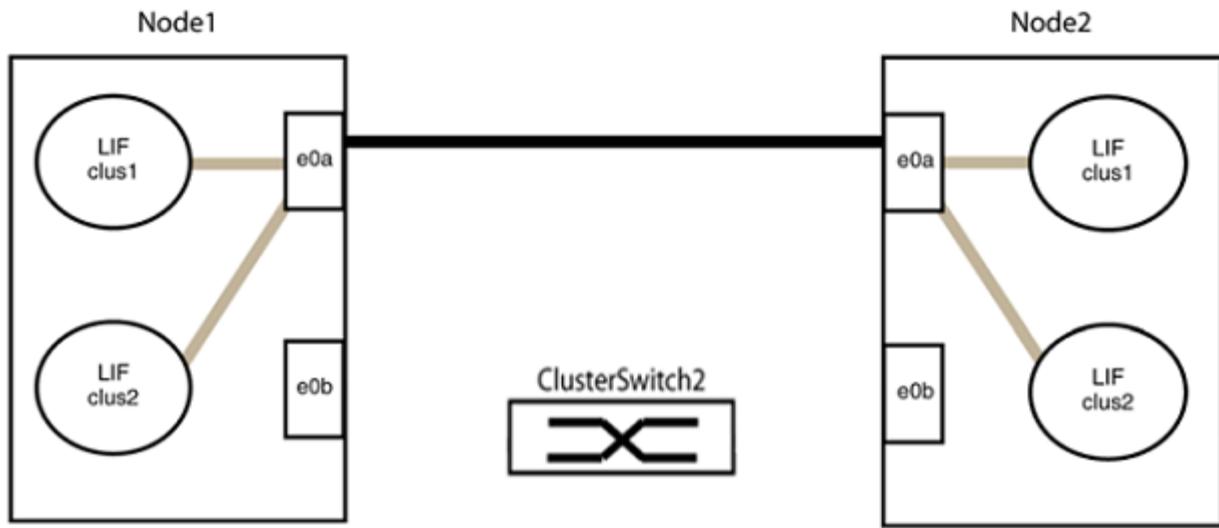
1. richten Sie die Konfiguration ohne Switches für die Ports in Gruppe 2 ein.



Um mögliche Netzwerkprobleme zu vermeiden, müssen Sie die Ports von groerp2 trennen und sie so schnell wie möglich wieder zurückverbinden, z. B. **in weniger als 20 Sekunden**.

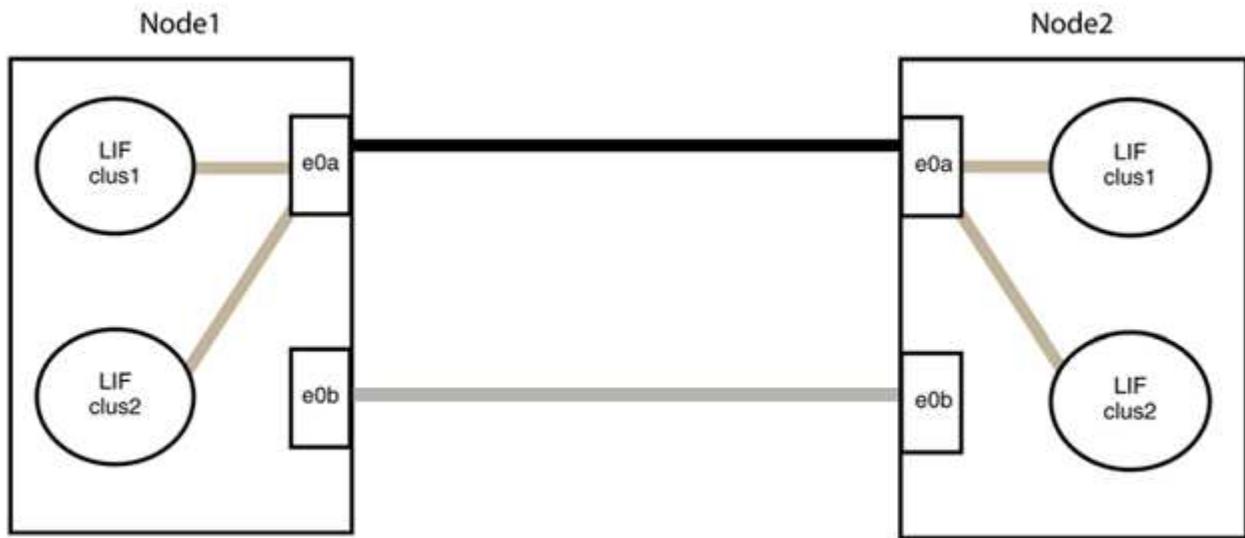
- a. Ziehen Sie alle Kabel gleichzeitig von den Anschlüssen in Group2 ab.

Im folgenden Beispiel werden die Kabel von Port „e0b“ auf jedem Node getrennt, und der Cluster-Datenverkehr wird durch die direkte Verbindung zwischen den „e0a“-Ports fortgesetzt:



b. Verkabeln Sie die Anschlüsse in der Rückführung von Group2.

Im folgenden Beispiel wird „e0a“ auf node1 mit „e0a“ auf node2 verbunden und „e0b“ auf node1 ist mit „e0b“ auf node2 verbunden:



### Schritt 3: Überprüfen Sie die Konfiguration

1. Vergewissern Sie sich, dass die Ports auf beiden Nodes ordnungsgemäß verbunden sind:

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

## Beispiel anzeigen

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

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

2. Aktivieren Sie die automatische Zurücksetzung für die Cluster-LIFs erneut:

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

3. Vergewissern Sie sich, dass alle LIFs Zuhause sind. Dies kann einige Sekunden dauern.

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

## Beispiel anzeigen

Die LIFs wurden zurückgesetzt, wenn die Spalte „ist Home“ lautet `true`, Wie gezeigt für `node1_clus2` Und `node2_clus2` Im folgenden Beispiel:

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

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
```

4. Überprüfen Sie den Cluster-Status der Nodes von der Systemkonsole eines der beiden Nodes:

```
cluster show
```

## Beispiel anzeigen

Das folgende Beispiel zeigt das Epsilon auf beiden Knoten `false`:

```
Node  Health  Eligibility Epsilon
-----
node1 true    true        false
node2 true    true        false
2 entries were displayed.
```

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

## ONTAP 9.9.1 und höher

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

```
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 anzeigen.

```
cluster1::*> network interface check cluster-connectivity show
                                         Source          Destination
Packet
Node    Date                LIF          LIF
Loss
-----
-----
node1
      3/5/2022 19:21:18 -06:00  node1_clus2      node2-clus1
none
      3/5/2022 19:21:20 -06:00  node1_clus2      node2_clus2
none
node2
      3/5/2022 19:21:18 -06:00  node2_clus2      node1_clus1
none
      3/5/2022 19:21:20 -06:00  node2_clus2      node1_clus2
none
```

## Alle ONTAP Versionen

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 node2
Getting addresses from network interface table...
Cluster node1_clus1 169.254.209.69 node1 e0a
Cluster node1_clus2 169.254.49.125 node1 e0b
Cluster node2_clus1 169.254.47.194 node2 e0a
Cluster node2_clus2 169.254.19.183 node2 e0b
Local = 169.254.47.194 169.254.19.183
Remote = 169.254.209.69 169.254.49.125
Cluster Vserver Id = 4294967293
Ping status:

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

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

```

1. Wenn Sie die automatische Fällerstellung unterdrückt haben, aktivieren Sie sie erneut, indem Sie eine AutoSupport-Meldung aufrufen:

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

Weitere Informationen finden Sie unter ["NetApp KB Artikel 1010449: Wie kann die automatische Case-Erstellung während geplanter Wartungszeiten unterdrückt werden"](#).

2. Ändern Sie die Berechtigungsebene zurück in den Administrator:

```
set -privilege admin
```

## 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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER 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.