Konfigurieren Sie die MetroCluster IP-Switches

ONTAP MetroCluster

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap-metrocluster/install-ip/task_switch_config_broadcom.html on April 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

Konfigurieren Sie die MetroCluster IP-Switches . . . 1
Konfigurieren von Broadcom IP-Switches . . . 1
Konfigurieren Sie Cisco IP-Switches . . . 19
Konfigurieren Sie den NVIDIA IP SN2100-Switch . . . 39
Konfigurieren Sie MetroCluster IP-Switches für die Zustandsüberwachung . . . 50

Konfigurieren Sie die MetroCluster IP-Switches

Konfigurieren von Broadcom IP-Switches

Sie müssen die Broadcom IP-Switches für die Verwendung als Cluster-Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

> Ihre Konfiguration erfordert zusätzliche Lizenzen (6 x 100-GB-Port-Lizenz) in den folgenden Szenarien:

- Die Ports 53 und 54 werden als MetroCluster-ISL mit 40 Gbit/s oder 100 Gbit/s verwendet.
- Sie verwenden eine Plattform, die das lokale Cluster und MetroCluster-Schnittstellen mit den Ports 49 - 52 verbindet.

Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen

Bevor Sie eine neue Switch-Softwareversion und RCFs installieren, müssen Sie die Broadcom-Switch-Einstellungen löschen und eine grundlegende Konfiguration durchführen.

Über diese Aufgabe

- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Wechseln Sie zur erhöhten Eingabeaufforderung (`#`): `enable`

   ```
   (IP_switch_A_1)> enable
   (IP_switch_A_1) #
   ```

2. Löschen Sie die Startkonfiguration, und entfernen Sie das Banner

   a. Löschen der Startkonfiguration:

      `erase startup-config`

      ```
      (IP_switch_A_1) #erase startup-config

      Are you sure you want to clear the configuration? (y/n) y

      (IP_switch_A_1) #
      ```

      Dieser Befehl löscht das Banner nicht.

   b. Entfernen Sie das Banner:

no set clibanner

```
(IP_switch_A_1) #configure
(IP_switch_A_1)(Config) # no set clibanner
(IP_switch_A_1)(Config) #
```

3. Starten Sie den Switch neu:*`(IP_switch_A_1) #reload*`

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

> Wenn das System fragt, ob die nicht gespeicherte oder geänderte Konfiguration vor dem erneuten Laden des Switches gespeichert werden soll, wählen Sie **Nein** aus.

4. Warten Sie, bis der Schalter neu geladen wurde, und melden Sie sich dann am Switch an.

   Der Standardbenutzer lautet „`admin`“, und es ist kein Passwort festgelegt. Es wird eine Eingabeaufforderung wie die folgende angezeigt:

```
(Routing)>
```

5. Zur erhöhten Eingabeaufforderung wechseln:

   `enable`

```
Routing)> enable
(Routing) #
```

6. Legen Sie das Service-Port-Protokoll auf fest `none`:

   `serviceport protocol none`

```
(Routing) #serviceport protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

(Routing) #
```

7. Weisen Sie die IP-Adresse dem Service-Port zu:

   `serviceport ip` *`ip-address netmask gateway`*

   Das folgende Beispiel zeigt eine dem Service-Port zugewiesene IP-Adresse „10.10.10.10“ mit dem Subnetz „255.255.255.0“ und dem Gateway „10.10.10.1“:

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Überprüfen Sie, ob der Service-Port ordnungsgemäß konfiguriert ist:

   ```
   show serviceport
   ```

   Das folgende Beispiel zeigt, dass der Port als aktiv ist und die richtigen Adressen zugewiesen wurden:

   ```
   (Routing) #show serviceport

   Interface Status............................... Up
   IP Address..................................... 10.10.10.10
   Subnet Mask.................................... 255.255.255.0
   Default Gateway................................ 10.10.10.1
   IPv6 Administrative Mode....................... Enabled
   IPv6 Prefix is ................................
   fe80::dac4:97ff:fe56:87d7/64
   IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
   Configured IPv4 Protocol....................... None
   Configured IPv6 Protocol....................... None
   IPv6 AutoConfig Mode........................... Disabled
   Burned In MAC Address.......................... D8:C4:97:56:87:D7

   (Routing) #
   ```

9. Konfigurieren Sie auf Wunsch den SSH-Server.

   > Die RCF-Datei deaktiviert das Telnet-Protokoll. Wenn Sie den SSH-Server nicht konfigurieren, können Sie nur über die serielle Port-Verbindung auf die Bridge zugreifen.

   a. Generieren von RSA-Schlüsseln.

      ```
      (Routing) #configure
      (Routing) (Config)#crypto key generate rsa
      ```

   b. DSA-Schlüssel generieren (optional)

      ```
      (Routing) #configure
      (Routing) (Config)#crypto key generate dsa
      ```

   c. Wenn Sie die FIPS-konforme Version von EFOS verwenden, generieren Sie die ECDSA-Schlüssel. Im folgenden Beispiel werden die Schlüssel mit einer Länge von 521 erstellt. Gültige Werte sind 256, 384 oder 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Aktivieren Sie den SSH-Server.

Schließen Sie bei Bedarf den Konfigurationskontext.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+

> Wenn Schlüssel bereits vorhanden sind, werden Sie möglicherweise aufgefordert, sie zu überschreiben.

10. Konfigurieren Sie bei Bedarf die Domäne und den Namensserver:

`configure`

Das folgende Beispiel zeigt die `ip domain` Und `ip name server` Befehl:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. Konfigurieren Sie auf Wunsch die Zeitzone und die Zeitsynchronisierung (SNTP).

Das folgende Beispiel zeigt die `sntp` Befehle, die IP-Adresse des SNTP-Servers und der relativen Zeitzone angeben.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

Verwenden Sie für EFOS Version 3.10.0.3 und höher den `ntp` Befehl, wie im folgenden Beispiel dargestellt:

```
> (Config)# ntp ?

authenticate             Enables NTP authentication.
authentication-key       Configure NTP authentication key.
broadcast                Enables NTP broadcast mode.
broadcastdelay           Configure NTP broadcast delay in microseconds.
server                   Configure NTP server.
source-interface         Configure the NTP source-interface.
trusted-key              Configure NTP authentication key number for
trusted time source.
vrf                      Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. Konfigurieren Sie den Switch-Namen:

    ```
    hostname IP_switch_A_1
    ```

    In der Switch-Eingabeaufforderung wird der neue Name angezeigt:

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Konfiguration speichern:

    ```
    write memory
    ```

    Sie erhalten Eingabeaufforderungen und Ausgabe ähnlich dem folgenden Beispiel:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

14. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Broadcom-Switch EFOS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe muss bei jedem Switch in der MetroCluster IP-Konfiguration wiederholt werden.

Beachten Sie Folgendes:

- Beim Upgrade von EFOS 3.4.x.x auf EFOS 3.7.x.x oder höher muss auf dem Switch EFOS 3.4.4.6 (oder höher 3.4.x.x-Version) ausgeführt werden. Wenn Sie vor dieser Version eine Version ausführen, aktualisieren Sie zuerst den Switch auf EFOS 3.4.4.6 (oder höher 3.4.x.x Version), und aktualisieren Sie dann den Switch auf EFOS 3.7.x.x oder höher.
- Die Konfiguration für EFOS 3.4.x.x und 3.7.x.x oder höher ist unterschiedlich. Wenn Sie die EFOS-Version von 3.4.x.x auf 3.7.x.x oder höher ändern oder umgekehrt, müssen Sie den Switch auf die Werkseinstellungen zurücksetzen und die RCF-Dateien für die entsprechende EFOS-Version werden (neu) angewendet. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.
- Ab EFOS Version 3.7.x.x oder höher ist eine FIPS-konforme Version und eine FIPS-konforme Version verfügbar. Verschiedene Schritte gelten für den Wechsel von einem nicht FIPS-konformen auf eine FIPS-konforme Version oder umgekehrt. Wenn EFOS von einer nicht FIPS-konformen Version oder umgekehrt geändert wird, wird der Switch auf die Werkseinstellungen zurückgesetzt. Für dieses Verfahren ist ein Zugriff über den seriellen Konsolen-Port erforderlich.

Schritte

1. Überprüfen Sie, ob Ihre EFOS-Version FIPS-konform oder nicht-FIPS-konform ist, indem Sie die verwenden `show fips status` Befehl. In den folgenden Beispielen: `IP_switch_A_1` Verwendet FIPS-konformes EFOS und `IP_switch_A_2` Verwendet ein nicht FIPS-konformes EFOS.

   Beispiel 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Beispiel 2

```
IP_switch_A_2 #show fips status
                     ^
% Invalid input detected at `^` marker.

IP_switch_A_2 #
```

2. Bestimmen Sie anhand der folgenden Tabelle, welche Methode Sie befolgen müssen:

Verfahren	**Aktuelle EFOS-Version**	* Neue EFOS-Version*	**Hohe Stufen**
Schritte zur Aktualisierung von EFOS zwischen zwei (nicht) FIPS-konformen Versionen	3.4.x.x	3.4.x.x	Installieren Sie das neue EFOS-Image mit Methode 1) die Konfigurations- und Lizenzinformationen bleiben erhalten
3.4.4.6 (oder höher 3.4.x.x)	3.7.x.x oder höher ohne FIPS-konform	EFOS mit Methode 1 aktualisieren. Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.7.x.x oder höher an	3.7.x.x oder höher ohne FIPS-konform
3.4.4.6 (oder höher 3.4.x.x)	EFOS mit Methode 1 abstufen. Setzen Sie den Schalter auf die Werkseinstellungen zurück, und wenden Sie die RCF-Datei für EFOS 3.4.x.x an	3.7.x.x oder höher ohne FIPS-konform	
Installieren Sie das neue EFOS-Image mit Methode 1. Die Konfigurations- und Lizenzdaten bleiben erhalten	3.7.x.x oder höher FIPS-konform	3.7.x.x oder höher FIPS-konform	Installieren Sie das neue EFOS-Image mit Methode 1. Die Konfigurations- und Lizenzdaten bleiben erhalten

Schritte zum Upgrade auf/von einer FIPS-konformen EFOS-Version	Nicht FIPS-konform	FIPS-konform	Installation des EFOS-Images unter Verwendung von Methode 2. Informationen zur Switch-Konfiguration und -Lizenz gehen verloren.

- Methode 1: Schritte zum Aktualisieren von EFOS beim Herunterladen des Software-Images auf die Backup-Boot-Partition
- Methode 2: Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation

Schritte zum Aktualisieren von EFOS beim Herunterladen des Software-Images auf die Backup-Boot-Partition

Die folgenden Schritte können nur ausgeführt werden, wenn beide EFOS-Versionen nicht FIPS-konform sind oder beide EFOS-Versionen FIPS-konform sind.

> Führen Sie diese Schritte nicht aus, wenn eine Version FIPS-konform ist und die andere Version nicht FIPS-konform ist.

Schritte

1. Kopieren Sie die Switch-Software auf den Switch: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   In diesem Beispiel wird die betriebssystemdatei efos-3.4.4.6.stk vom SFTP-Server unter 50.50.50.50 auf die Sicherungspartition kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode........................................... SFTP
Set Server IP.................................. 50.50.50.50
Path........................................... /switchsoftware/
Filename....................................... efos-3.4.4.6.stk
Data Type...................................... Code
Destination Filename........................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Legen Sie beim nächsten Neustart des Switches den Switch fest, der von der Backup-Partition aus gestartet werden soll:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Vergewissern Sie sich, dass das neue Startabbild beim nächsten Start aktiv ist:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Konfiguration speichern:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Starten Sie den Switch neu:

   `reload`

```
(IP_switch_A_1) #reload

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

6. Warten Sie, bis der Schalter neu gestartet wurde.

> In seltenen Fällen kann der Switch nicht booten. Folgen Sie den Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation Um das neue Image zu installieren.

7. Wenn Sie den Switch von EFOS 3.4.x.x auf EFOS 3.7.x.x oder umgekehrt umstellen, befolgen Sie die folgenden beiden Verfahren, um die korrekte Konfiguration (RCF) anzuwenden:
   a. Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen
   b. Herunterladen und Installieren der Broadcom RCF-Dateien
8. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Schritte zum Aktualisieren von EFOS mit der ONIE OS-Installation

Sie können die folgenden Schritte durchführen, wenn eine EFOS-Version FIPS-konform ist und die andere EFOS-Version nicht FIPS-konform ist. Mit diesen Schritten kann das nicht-FIPS- oder FIPS-konforme EFOS 3.7.x.x-Image von ONIE installiert werden, wenn der Switch nicht startet.

Schritte

1. Starten Sie den Schalter in den ONIE-Installationsmodus.

   Wählen Sie während des Startvorgangs ONIE aus, wenn der folgende Bildschirm angezeigt wird:

```
+-----------------------------------------------------------------------+
|EFOS                                                                   |
|*ONIE                                                                  |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
+-----------------------------------------------------------------------+
```

   Nach der Auswahl von „ONIE“ wird der Schalter geladen und Ihnen folgende Auswahlmöglichkeiten zur Verfügung stehen:

```
 +-----------------------------------------------------------------------+
 |*ONIE: Install OS                                                      |
 | ONIE: Rescue                                                          |
 | ONIE: Uninstall OS                                                    |
 | ONIE: Update ONIE                                                     |
 | ONIE: Embed ONIE                                                      |
 | DIAG: Diagnostic Mode                                                 |
 | DIAG: Burn-In Mode                                                    |
 |                                                                       |
 |                                                                       |
 |                                                                       |
 |                                                                       |
 |                                                                       |
 +-----------------------------------------------------------------------+
```

Der Schalter startet nun in den ONIE-Installationsmodus.

2. Beenden Sie die ONIE-Erkennung, und konfigurieren Sie die ethernet-Schnittstelle

   Sobald die folgende Meldung angezeigt wird, drücken Sie <ENTER>, um die ONIE-Konsole zu öffnen:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

   Die ONIE-Erkennung wird fortgesetzt, und Meldungen werden auf die Konsole gedruckt.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Konfigurieren Sie die ethernet-Schnittstelle und fügen Sie die Route mit hinzu `ifconfig eth0 <ipAddress> netmask <netmask> up` Und `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Stellen Sie sicher, dass der Server, der die ONIE-Installationsdatei hostet, erreichbar ist:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Installieren Sie die neue Switch-Software

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

Die Software wird installiert und startet den Switch dann neu. Lassen Sie den Switch normal in die neue EFOS-Version neu starten.

6. Vergewissern Sie sich, dass die neue Switch-Software installiert ist

`show bootvar`

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Schließen Sie die Installation ab

   Der Switch wird neu gestartet, ohne dass die Konfiguration angewendet wurde, und setzt die Werkseinstellungen zurück. Befolgen Sie die beiden Verfahren, um die Grundeinstellungen des Switches zu konfigurieren und die RCF-Datei anzuwenden, wie in den folgenden beiden Dokumenten beschrieben:

   a. Konfigurieren Sie die Grundeinstellungen des Switches. Befolgen Sie Schritt 4 und höher: Zurücksetzen des Broadcom IP-Switches auf die Werkseinstellungen
   b. Erstellen und wenden Sie die RCF-Datei wie in beschrieben an Herunterladen und Installieren der Broadcom RCF-Dateien

Herunterladen und Installieren der Broadcom RCF-Dateien

Sie müssen die RCF-Datei des Switch auf jedem Switch der MetroCluster IP-Konfiguration herunterladen und installieren.

Bevor Sie beginnen

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Über diese Aufgabe

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Es gibt vier RCF-Dateien, eine für jeden der vier Schalter in der MetroCluster IP-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
IP_Switch_A_1	v1.32_Switch-A1.txt
IP_Switch_A_2	v1.32_Switch-A2.txt
IP_Switch_B_1	v1.32_Switch-B1.txt
IP_Switch_B_2	v1.32_Switch-B2.txt

Die RCF-Dateien für EFOS Version 3.4.4.6 oder höher 3.4.x.x Version und EFOS Version 3.7.0.4 sind unterschiedlich. Sie müssen sicherstellen, dass Sie die richtigen RCF-Dateien für die EFOS-Version erstellt haben, auf der der Switch ausgeführt wird.

EFOS-Version	RCF-Dateiversion
3.4.x.x	V1.3x, v1.4x
3.7.x.x	v2.x

Schritte

1. Generieren Sie die Broadcom RCF-Dateien für die MetroCluster-IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP"
   b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.

Änderungen an den RCF-Dateien nach dem Download werden nicht unterstützt.

2. Kopieren Sie die RCF-Dateien auf die Switches:

   a. Kopieren Sie die RCF-Dateien auf den ersten Switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

      In diesem Beispiel wird die RCF-Datei „BES-53248_v1.32_Switch-A1.txt“ vom SFTP-Server unter „50.50.50.50“ in den lokalen Bootflash kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode........................................... SFTP
Set Server IP.................................. 50.50.50.50
Path........................................... /RcfFiles/
Filename....................................... BES-
53248_v1.32_Switch-A1.txt
Data Type...................................... Config Script
Destination Filename........................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"*******************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248



...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Überprüfen Sie, ob die RCF-Datei als Skript gespeichert ist:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr             852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Anwenden des RCF-Skripts:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"*********************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Konfiguration speichern:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Starten Sie den Switch neu:

   `reload`

```
(IP_switch_A_1) #reload

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

a. Wiederholen Sie die vorherigen Schritte für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Schalter neu laden:

   `reload`

```
IP_switch_A_1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe des RCF-Datei-Banners:

> Wenn sich der Port im Breakout-Modus befindet, kann der im Befehl angegebene Portname von dem im RCF-Banner angegebenen Namen abweichen. Sie können auch die RCF-Verkabelungsdateien verwenden, um den Portnamen zu finden.

Für Details zum ISL-Port

Führen Sie den Befehl aus `show port all`.

Für Port-Channel-Details

Führen Sie den Befehl aus `show port-channel all`.

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle.

   Sie müssen die folgenden Befehle für jeden identifizierten nicht verwendeten Port oder Port-Kanal ausführen.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

Konfigurieren Sie Cisco IP-Switches

Konfigurieren von Cisco IP-Switches

Sie müssen die Cisco IP Switches für die Verwendung als Cluster Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

Über diese Aufgabe

Einige der Verfahren in diesem Abschnitt sind unabhängige Verfahren, und Sie müssen nur diejenigen ausführen, die Sie an Ihre Aufgabe gerichtet sind oder für Ihre Aufgabe relevant sind.

Zurücksetzen des Cisco IP-Switches auf die Werkseinstellungen

Bevor Sie eine RCF-Datei installieren, müssen Sie die Cisco Switch-Konfiguration löschen und die grundlegende Konfiguration durchführen. Dieses Verfahren ist erforderlich, wenn Sie dieselbe RCF-Datei nach einer vorherigen Installation neu installieren möchten oder wenn Sie eine neue Version einer RCF-Datei installieren möchten.

Über diese Aufgabe

- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über die serielle Konsole mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Setzen Sie den Schalter auf die werkseitigen Standardeinstellungen zurück:

   a. Löschen Sie die vorhandene Konfiguration:

```
write erase
```

b. Laden Sie die Switch-Software neu:

```
reload
```

Das System startet neu und wechselt in den Konfigurationsassistenten. Wenn Sie während des Startvorgangs die Eingabeaufforderung „`Automatische Bereitstellung abbrechen und mit der normalen Einrichtung fortfahren? (ja/Nein)[n]`", you should respond `yes` Fortfahren.

c. Geben Sie im Konfigurationsassistenten die grundlegenden Switch-Einstellungen ein:
   - Admin-Passwort
   - Switch-Name
   - Out-of-Band-Managementkonfiguration
   - Standard-Gateway
   - SSH-Service (RSA)

   Nach Abschluss des Konfigurationsassistenten wird der Switch neu gestartet.

d. Geben Sie bei entsprechender Aufforderung den Benutzernamen und das Kennwort ein, um sich beim Switch anzumelden.

Das folgende Beispiel zeigt die Eingabeaufforderungen und Systemantworten bei der Konfiguration des Switches. Die Winkelklammern (`<<<`Geben Sie an, wo Sie die Informationen eingeben.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
  Confirm the password for "admin": password
         ---- Basic System Configuration Dialog VDC: 1 ----

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

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

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

Sie geben grundlegende Informationen in die nächsten Eingabeaufforderungen ein, einschließlich Switch-Name, Managementadresse und Gateway, und wählen SSH mit RSA aus.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

Die letzte Reihe von Eingabeaufforderungen vervollständigt die Konfiguration:

```
The following configuration will be applied:
  password strength-check
  switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
  no feature telnet
  ssh key rsa 1024 force
  feature ssh
  system default switchport
  system default switchport shutdown
  copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown

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

Use this configuration and save it? (yes/no) [y]:
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.

[##########################################] 100%
Copy complete.

User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Konfiguration speichern:

```
IP_switch-A-1# copy running-config startup-config
```

3. Starten Sie den Switch neu, und warten Sie, bis der Schalter neu geladen wurde:

```
IP_switch-A-1# reload
```

4. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco Switch NX-OS-Software

Sie müssen die Betriebssystemdatei und die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Schritte

1. Laden Sie die unterstützte NX-OS-Softwaredatei herunter.

   "Cisco Software-Download"

2. Kopieren Sie die Switch-Software auf den Switch:

   ```
   copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf
   management
   ```

   In diesem Beispiel wird die Datei nxos.7.0.3.I4.6.bin vom SFTP-Server 10.10.99.99 auf den lokalen Bootflash kopiert:

   ```
   IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
   bootflash: vrf management
   root@10.10.99.99's password: password
   sftp> progress
   Progress meter enabled
   sftp> get   /tftpboot/nxos.7.0.3.I4.6.bin
   /bootflash/nxos.7.0.3.I4.6.bin
   Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
   /tftpboot/nxos.7.0.3.I4.6.bin                 100%  666MB   7.2MB/s
   01:32
   sftp> exit
   Copy complete, now saving to disk (please wait)...
   ```

3. Überprüfen Sie auf jedem Switch, ob die NX-OS-Dateien des Switches im Bootflash-Verzeichnis jedes Switches vorhanden sind:

   ```
   dir bootflash:
   ```

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

```
IP_switch_A_1# dir bootflash:
                  .
                  .
                  .
  698629632    Jun 13 21:37:44 2017  nxos.7.0.3.I4.6.bin
                  .
                  .
                  .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#
```

4. Installieren der Switch-Software:

   ```
   install all nxos bootflash:nxos.version-number.bin
   ```

   Der Switch wird automatisch neu geladen (neu gestartet), nachdem die Switch-Software installiert wurde.

   Das folgende Beispiel zeigt die Softwareinstallation auf IP_Switch_A_1:

```
IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

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

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[####################] 100% -- SUCCESS       [####################] 100%
-- SUCCESS

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

Notifying services about system upgrade.     [####################] 100%
```

```
-- SUCCESS



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



Images will be upgraded according to following table:
Module       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     1        nxos                7.0(3)I4(1)         7.0(3)I4(6)   yes
     1        bios         v04.24(04/21/2016)  v04.24(04/21/2016)   no


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


Install is in progress, please wait.

Performing runtime checks.         [####################] 100%    --
SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

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


Finishing the upgrade, switch will reboot in 10 seconds.
IP_switch_A_1#
```

5. Warten Sie, bis der Schalter neu geladen ist, und melden Sie sich dann am Schalter an.

   Nach dem Neustart des Switches wird die Eingabeaufforderung für die Anmeldung angezeigt:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Überprüfen Sie, ob die Switch-Software installiert wurde:
   `show version`

   Das folgende Beispiel zeigt die Ausgabe:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time:  04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time:  3/9/2017 22:00:00 [03/10/2017 07:05:18]


Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash:   14900224 kB
  usb1:               0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after  Mon Jun 10 21:43:52 2017

  Reason: Reset due to upgrade
  System version: 7.0(3)I4(1)
  Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Wiederholen Sie diese Schritte für die verbleibenden drei IP-Switches in der MetroCluster IP-Konfiguration.

Herunterladen und Installieren der Cisco IP RCF-Dateien

Sie müssen die RCF-Datei auf jeden Switch in der MetroCluster IP-Konfiguration herunterladen.

Über diese Aufgabe

Diese Aufgabe erfordert Dateiübertragungssoftware, wie FTP, TFTP, SFTP oder SCP, Um die Dateien auf die

Switches zu kopieren.

Diese Schritte müssen bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholt werden.

Sie müssen die unterstützte Switch-Softwareversion verwenden.

"NetApp Hardware Universe"

Es gibt vier RCF-Dateien, eine für jeden der vier Schalter in der MetroCluster IP-Konfiguration. Sie müssen die richtigen RCF-Dateien für das Switch-Modell verwenden, das Sie verwenden.

Switch	RCF-Datei
IP_Switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_Switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_Switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_Switch_B_2	NX3232_v1.80_Switch-B2.txt

Schritte

1. Laden Sie die MetroCluster IP RCF-Dateien herunter.

   Änderungen an den RCF-Dateien nach dem Download werden nicht unterstützt.

2. Kopieren Sie die RCF-Dateien auf die Switches:

   a. Kopieren Sie die RCF-Dateien auf den ersten Switch:

      ```
      copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
      bootflash: vrf management
      ```

      In diesem Beispiel wird die RCF-Datei NX3232_v1.80_Switch-A1.txt vom SFTP-Server unter 10.10.99.99 auf den lokalen Bootflash kopiert. Sie müssen die IP-Adresse Ihres TFTP/SFTP-Servers und den Dateinamen der RCF-Datei verwenden, die Sie installieren müssen.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Wiederholen Sie den vorherigen Unterschritt für jeden der anderen drei Schalter, wobei Sie sicherstellen müssen, dass die entsprechende RCF-Datei auf den entsprechenden Switch kopiert wird.

3. Überprüfen Sie bei jedem Switch, ob die RCF-Datei im Bootflash-Verzeichnis jedes Switches vorhanden ist:

   ```
   dir bootflash:
   ```

   Das folgende Beispiel zeigt, dass die Dateien auf IP_Switch_A_1 vorhanden sind:

   ```
   IP_switch_A_1# dir bootflash:
                     .
                     .
                     .
   5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                     .
                     .
                     .

   Usage for bootflash://sup-local
   1779363840 bytes used
   13238841344 bytes free
   15018205184 bytes total
   IP_switch_A_1#
   ```

4. Konfigurieren Sie die TCAM-Regionen auf Cisco Switches 3132Q-V und Cisco 3232C-Switches.

   Überspringen Sie diesen Schritt, wenn Cisco 3132Q-V oder Cisco 32Q-V Switches nicht vorhanden sind.

a. Stellen Sie auf dem Cisco Switch 3132Q-V die folgenden TCAM-Bereiche ein:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. Legen Sie auf dem Cisco 3232C Switch die folgenden TCAM-Regionen fest:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Speichern Sie nach dem Einstellen der TCAM-Bereiche die Konfiguration, und laden Sie den Schalter neu:

```
copy running-config startup-config
reload
```

5. Kopieren Sie die passende RCF-Datei vom lokalen Bootflash auf jeden Switch in die laufende Konfiguration:

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Kopieren Sie die RCF-Dateien von der ausgeführten Konfiguration auf die Startkonfiguration auf jedem Switch:

   `copy running-config startup-config`

   Sie sollten eine Ausgabe wie die folgende sehen:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Schalter neu laden:

   `reload`

```
IP_switch_A_1# reload
```

8. Wiederholen Sie die vorherigen Schritte auf den anderen drei Switches in der MetroCluster IP-Konfiguration.

Einstellen der Vorwärtskorrektur für Systeme mit 25-Gbit/s-Konnektivität

Wenn Ihr System mit 25-Gbit/s-Konnektivität konfiguriert ist, müssen Sie den fec-Parameter (Forward Error Correction) nach Anwendung der RCF-Datei manuell auf OFF setzen. Die RCF-Datei wendet diese Einstellung nicht an.

Über diese Aufgabe

Die 25-Gbps-Ports müssen vor Durchführung dieses Verfahrens verkabelt werden.

"Plattform-Port-Zuweisungen für Cisco 3232C- oder Cisco 9336C-Switches"

Diese Aufgabe gilt nur für Plattformen mit 25-Gbit/s-Konnektivität:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Diese Aufgabe muss an allen vier Switches der MetroCluster IP-Konfiguration ausgeführt werden.

Schritte

1. Stellen Sie den fec-Parameter auf aus für jeden 25-Gbit/s-Port, der mit einem Controller-Modul verbunden ist, und kopieren Sie dann die laufende Konfiguration in die Startkonfiguration:

   a. Konfigurationsmodus aufrufen: `config t`

   b. Geben Sie die zu konfigurierende 25-Gbit/s-Schnittstelle an: `interface interface-ID`

   c. fec auf aus stellen: `fec off`

   d. Wiederholen Sie die vorherigen Schritte für jeden 25-Gbit/s-Port am Switch.

   e. Konfigurationsmodus beenden: `exit`

   Im folgenden Beispiel werden die Befehle für Interface ethernet1/25/1 auf Switch IP_Switch_A_1 angezeigt:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Wiederholen Sie den vorherigen Schritt auf den anderen drei Switches der MetroCluster IP-Konfiguration.

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle:

   ```
   show interface brief
   ```

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle.

   Sie müssen die folgenden Befehle für jeden identifizierten nicht verwendeten Port oder Port-Kanal ausführen.

   ```
   SwitchA_1# config t
   Enter configuration commands, one per line. End with CNTL/Z.
   SwitchA_1(config)# int Eth1/14
   SwitchA_1(config-if)# shutdown
   SwitchA_12(config-if)# exit
   SwitchA_1(config-if)# copy running-config startup-config
   [########################################] 100%
   Copy complete, now saving to disk (please wait)...
   Copy complete.
   ```

Konfigurieren Sie die MACsec-Verschlüsselung auf Cisco 9336C-Switches

Auf Wunsch können Sie die MACsec-Verschlüsselung für die WAN-ISL-Ports konfigurieren, die zwischen den Standorten ausgeführt werden. Sie müssen MACsec konfigurieren, nachdem Sie die korrekte RCF-Datei angewendet haben.

> Die MACsec-Verschlüsselung kann nur auf die WAN-ISL-Ports angewendet werden.

Konfigurieren Sie die MACsec-Verschlüsselung auf Cisco 9336C-Switches

Sie müssen die MACsec-Verschlüsselung nur für die WAN-ISL-Ports konfigurieren, die zwischen den Standorten ausgeführt werden. Sie müssen MACsec konfigurieren, nachdem Sie die korrekte RCF-Datei angewendet haben.

Lizenzierungsanforderungen für MACsec

MACsec erfordert eine Sicherheitslizenz. Eine vollständige Erläuterung des Cisco NX-OS-Lizenzschemas und der Beschaffung und Anwendung von Lizenzen finden Sie im "Cisco NX-OS Licensing Guide"

Aktivierung von Cisco MACs Encryption WAN-ISLs in MetroCluster IP-Konfigurationen

Sie können die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration aktivieren.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Aktivieren Sie MACsec und MKA auf dem Gerät:

```
feature macsec
```

```
IP_switch_A_1(config)# feature macsec
```

3. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Konfigurieren Sie eine MACsec-Schlüsselkette und -Tasten

Sie können eine MACsec-Schlüsselkette oder Schlüssel für Ihre Konfiguration erstellen.

- Key Lifetime und Hitless Key Rollover*

Eine MACsec-Schlüsselkette kann über mehrere vorinstallierte PSKs (Preshared Keys) verfügen, die jeweils mit einer Schlüssel-ID und einer optionalen Lebensdauer konfiguriert sind. Eine Schlüssellebensdauer legt fest, zu welcher Zeit die Taste aktiviert und abläuft. Wenn keine lebenslange Konfiguration vorhanden ist, ist die Standardlebensdauer unbegrenzt. Wenn eine Lebensdauer konfiguriert ist, rollt MKA nach Ablauf der Lebensdauer zum nächsten konfigurierten vorfreigegebenen Schlüssel in der Schlüsselkette um. Die Zeitzone des Schlüssels kann lokal oder UTC sein. Die Standardzeitzone ist UTC. Ein Schlüssel kann auf einen zweiten Schlüssel innerhalb derselben Schlüsselkette übertragen werden, wenn Sie den zweiten Schlüssel (in der Schlüsselkette) konfigurieren und eine Lebensdauer für den ersten Schlüssel konfigurieren. Wenn die Lebensdauer der ersten Taste abläuft, wird automatisch die nächste Taste in der Liste angezeigt. Wenn dieselbe Taste auf beiden Seiten des Links gleichzeitig konfiguriert ist, ist der Schlüsselüberschlag ohne Unterbrechung des Datenverkehrs aktiviert (d. h. der Schlüssel wird ohne Unterbrechung des Datenverkehrs überrollt).

Schritte

1. Den globalen Konfigurationsmodus aufrufen:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Um den verschlüsselten Schlüsselzeichenkette auszublenden, ersetzen Sie den String in der Ausgabe des durch ein Platzhalterzeichen `show running-config` Und `show startup-config` Befehl:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

> Die Oktett-Zeichenfolge wird ebenfalls ausgeblendet, wenn Sie die Konfiguration in einer Datei speichern.

Standardmäßig werden PSK-Schlüssel im verschlüsselten Format angezeigt und können einfach entschlüsselt werden. Dieser Befehl gilt nur für MACsec-Schlüsselketten.

3. Erstellen Sie eine MACsec-Schlüsselkette, um eine Reihe von MACsec-Schlüsseln zu halten und den MACsec-Konfigurationsmodus für die Schlüsselkette aufzurufen:

   `key chain name macsec`

   ```
   IP_switch_A_1(config)# key chain 1 macsec
   IP_switch_A_1(config-macseckeychain)#
   ```

4. Erstellen Sie eine MACsec-Taste, und rufen Sie den MACsec-Key-Konfigurationsmodus auf:

   `key key-id`

   Der Bereich liegt zwischen 1 und 32 hex-stelligen Schlüsselzeichenfolge und die maximale Größe beträgt 64 Zeichen.

   ```
   IP_switch_A_1 switch(config-macseckeychain)# key 1000
   IP_switch_A_1 (config-macseckeychain-macseckey)#
   ```

5. Konfigurieren Sie die Oktett-Zeichenfolge für den Schlüssel:

   `key-octet-string octet-string cryptographic-algorithm AES_128_CMAC | AES_256_CMAC`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
   abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
   cryptographic-algorithm AES_256_CMAC
   ```

   > Das Argument Octet-string kann bis zu 64 hexadezimale Zeichen enthalten. Der Oktett-Schlüssel wird intern kodiert, so dass der Schlüssel im Klartext nicht in der Ausgabe des angezeigt wird `show running-config macsec` Befehl.

6. Konfigurieren einer Sendezeit für die Taste (in Sekunden):

   `send-lifetime start-time duration duration`

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

Standardmäßig behandelt das Gerät die Startzeit als UTC. Das Argument Start-Time ist die Uhrzeit und das Datum, zu der der Schlüssel aktiv wird. Das Argument „Dauer“ ist die Länge der Lebensdauer in Sekunden. Die maximale Länge beträgt 2147483646 Sekunden (ca. 68 Jahre).

7. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

8. Zeigt die Schlüsselkettenkonfiguration an:

   `show key chain name`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
   ```

Konfigurieren einer MACsec-Richtlinie

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Erstellen einer MACsec-Richtlinie:

   `macsec policy name`

   ```
   IP_switch_A_1(config)# macsec policy abc
   IP_switch_A_1(config-macsec-policy)#
   ```

3. Konfigurieren Sie eine der folgenden Chiffren GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 oder GCM-AES-XPN-256:

   `cipher-suite name`

   ```
   IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
   ```

4. Konfigurieren Sie die zentrale Serverpriorität, um die Verbindung zwischen Peers während eines Schlüsselaustauschs zu unterbrechen:

   `key-server-priority number`

   ```
   switch(config-macsec-policy)# key-server-priority 0
   ```

5. Konfigurieren Sie die Sicherheitsrichtlinie, um den Umgang mit Daten und Kontrollpaketen zu definieren:

   `security-policy security policy`

   Wählen Sie aus den folgenden Optionen eine Sicherheitsrichtlinie aus:

   - Must-Secure — Pakete, die keine MACsec-Header tragen, werden verworfen
   - Sollte-sicher — Pakete, die keine MACsec-Header tragen, sind zulässig (dies ist der Standardwert)

   ```
   IP_switch_A_1(config-macsec-policy)# security-policy should-secure
   ```

6. Konfigurieren Sie das Replay Protection-Fenster, damit die gesicherte Schnittstelle kein Paket akzeptiert, das kleiner als die konfigurierte Fenstergröße ist: `window-size number`

   > Die Größe des Replay Protection Window stellt die maximale Anzahl von Frames dar, die von MACsec akzeptiert und nicht verworfen werden. Der Bereich liegt zwischen 0 und 596000000.

   ```
   IP_switch_A_1(config-macsec-policy)# window-size 512
   ```

7. Konfigurieren Sie die Zeit in Sekunden, um einen SAK-Rekey zu erzwingen:

   `sak-expiry-time time`

   Sie können mit diesem Befehl den Sitzungsschlüssel in ein vorhersehbares Zeitintervall ändern. Der Standardwert ist 0.

   ```
   IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
   ```

8. Konfigurieren Sie einen der folgenden Vertraulichkeitsvereinbarungen im Layer 2-Frame, in dem die Verschlüsselung beginnt:

   `conf-offsetconfidentiality offset`

   Wählen Sie eine der folgenden Optionen:

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

> Dieser Befehl kann erforderlich sein, damit zwischen den Zwischenschaltern Paketheader (dmac, smac, etype) wie MPLS-Tags verwendet werden können.

9. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

10. Die MACsec-Richtlinienkonfiguration anzeigen:

    `show macsec policy`

    ```
    IP_switch_A_1(config-macsec-policy)# show macsec policy
    ```

Aktivieren Sie die Verschlüsselung von Cisco MACsec an den Schnittstellen

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Wählen Sie die Schnittstelle aus, die Sie mit MACsec-Verschlüsselung konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

3. Fügen Sie die Schlüsselanhänger und die Richtlinie, die auf der Schnittstelle konfiguriert werden sollen, hinzu, um die MACsec-Konfiguration hinzuzufügen:

   `macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# macsec keychain 1 policy abc
   ```

4. Wiederholen Sie die Schritte 1 und 2 auf allen Schnittstellen, für die die MACsec-Verschlüsselung

konfiguriert werden soll.

5. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Deaktivieren Sie Cisco MACs Verschlüsselungs-WAN-ISLs in MetroCluster IP-Konfigurationen

Möglicherweise müssen Sie die MACsec-Verschlüsselung für Cisco 9336C-Switches auf WAN-ISLs in einer MetroCluster IP-Konfiguration deaktivieren.

Schritte

1. Globalen Konfigurationsmodus aufrufen:

   `configure terminal`

   ```
   IP_switch_A_1# configure terminal
   IP_switch_A_1(config)#
   ```

2. Deaktivieren Sie die MACsec-Konfiguration auf dem Gerät:

   `macsec shutdown`

   ```
   IP_switch_A_1(config)# macsec shutdown
   ```

   Durch Auswahl der Option „`no`“ wird die MACsec-Funktion wiederhergestellt.

3. Wählen Sie die Schnittstelle aus, die Sie bereits mit MACsec konfiguriert haben.

   Sie können den Schnittstellentyp und die Identität angeben. Verwenden Sie für einen Ethernet-Port ethernet-Steckplatz/Ethernet-Port.

   ```
   IP_switch_A_1(config)# interface ethernet 1/15
   switch(config-if)#
   ```

4. Entfernen Sie die auf der Schnittstelle konfigurierte Schlüsselanhänger und Richtlinie, um die MACsec-Konfiguration zu entfernen:

   `no macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
   ```

5. Wiederholen Sie die Schritte 3 und 4 auf allen Schnittstellen, für die MACsec konfiguriert ist.
6. Kopieren Sie die laufende Konfiguration in die Startkonfiguration:

   `copy running-config startup-config`

   ```
   IP_switch_A_1(config)# copy running-config startup-config
   ```

Überprüfen der MACsec-Konfiguration

Schritte

1. Wiederholen Sie * alle* der vorherigen Vorgänge auf dem zweiten Schalter innerhalb der Konfiguration, um eine MACsec-Sitzung einzurichten.
2. Führen Sie die folgenden Befehle aus, um zu überprüfen, ob beide Switches erfolgreich verschlüsselt sind:

   a. Ausführen: `show macsec mka summary`

   b. Ausführen: `show macsec mka session`

   c. Ausführen: `show macsec mka statistics`

   Sie können die MACsec-Konfiguration mit den folgenden Befehlen überprüfen:

Befehl	Zeigt Informationen über… an.
`show macsec mka session interface typeslot/port number`	Die MKA-Sitzung von MACsec für eine bestimmte Schnittstelle oder für alle Schnittstellen
`show key chain name`	Konfiguration der Schlüsselkette
`show macsec mka summary`	Die MKA-Konfiguration von MACsec
`show macsec policy policy-name`	Die Konfiguration für eine bestimmte MACsec-Richtlinie oder für alle MACsec-Richtlinien

Konfigurieren Sie den NVIDIA IP SN2100-Switch

Sie müssen die NVIDIA SN2100 IP-Switches für die Verwendung als Cluster-Interconnect und für die Back-End-MetroCluster-IP-Konnektivität konfigurieren.

[[Reset-the-Switch] setzt den NVIDIA IP SN2100-Schalter auf die Werkseinstellungen zurück

Sie können eine der folgenden Methoden auswählen, um einen Schalter auf die werkseitigen Standardeinstellungen zurückzusetzen.

- Setzen Sie den Switch mithilfe der RCF-Dateioption zurück

- Setzen Sie den Schalter mithilfe der Cumulus-Installationsoption zurück

Zurücksetzen des Switches mit der RCF-Dateioption

Bevor Sie eine neue RCF-Konfiguration installieren, müssen Sie die NVIDIA-Switch-Einstellungen zurücksetzen.

Über diese Aufgabe

Um den Switch auf die Standardeinstellungen zurückzusetzen, führen Sie die RCF-Datei mit dem aus `restoreDefaults` Option. Mit dieser Option werden die ursprünglichen gesicherten Dateien an den ursprünglichen Speicherort kopiert und anschließend der Switch neu gestartet. Nach dem Neustart wird der Switch mit der ursprünglichen Konfiguration online geschaltet, die bei der ersten Ausführung der RCF-Datei zum Konfigurieren des Switches existierte.

Die folgenden Konfigurationsdetails werden nicht zurückgesetzt:

- Konfiguration von Benutzern und Anmeldeinformationen
- Konfiguration des Management-Netzwerk-Ports, eth0

> Alle anderen Konfigurationsänderungen, die während der Anwendung der RCF-Datei auftreten, werden auf die ursprüngliche Konfiguration zurückgesetzt.

Bevor Sie beginnen

- Sie müssen den Switch gemäß konfigurieren Laden Sie die NVIDIA RCF-Datei herunter, und installieren Sie sie. Wenn Sie auf diese Weise nicht konfiguriert haben oder vor der Ausführung der RCF-Datei zusätzliche Funktionen konfiguriert haben, können Sie dieses Verfahren nicht verwenden.
- Sie müssen diese Schritte bei jedem der IP-Switches in der MetroCluster IP-Konfiguration wiederholen.
- Sie müssen über eine serielle Konsolenverbindung mit dem Switch verbunden sein.
- Mit dieser Aufgabe wird die Konfiguration des Managementnetzwerks zurückgesetzt.

Schritte

1. Überprüfen Sie, ob die RCF-Konfiguration erfolgreich mit derselben oder einer kompatiblen RCF-Dateiversion angewendet wurde und ob die Sicherungsdateien vorhanden sind.

   > Die Ausgabe kann Backup-Dateien, erhaltene Dateien oder beides anzeigen. Wenn Sicherungsdateien oder nicht vorhandene Dateien nicht in der Ausgabe angezeigt werden, können Sie dieses Verfahren nicht verwenden.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
  Backup files exist.
    Preserved files exist.
    Listing completion of the steps:
        Success: Step: 1: Performing Backup and Restore
        Success: Step: 2: updating MOTD file
        Success: Step: 3: Disabling apt-get
        Success: Step: 4: Disabling cdp
        Success: Step: 5: Adding lldp config
        Success: Step: 6: Creating interfaces
        Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
        Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
        Success: Step: 9: Configuring switch basic settings: ecn
        Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
        Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
        Success: Step: 12: Configuring switch basic settings: traffic
classification
        Success: Step: 13: Configuring LAG load balancing policies
        Success: Step: 14: Configuring the VLAN bridge
        Success: Step: 15: Configuring local cluster ISL ports
        Success: Step: 16: Configuring MetroCluster ISL ports
        Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
        Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
        Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
        Success: Step: 20: Configuring L2FC for MetroCluster interfaces
        Success: Step: 21: Configuring the interface to UP
        Success: Step: 22: Final commit
        Success: Step: 23: Final reboot of the switch
    Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Führen Sie die RCF-Datei mit der Option zum Wiederherstellen der Standardeinstellungen aus: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_2.py
restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Beantworten Sie die Eingabeaufforderung mit „Ja“. Der Switch wird auf die ursprüngliche Konfiguration zurückgesetzt und startet neu.
4. Warten Sie, bis der Schalter neu gestartet wurde.

   Der Switch wird zurückgesetzt und behält die ursprüngliche Konfiguration wie z. B. die Konfiguration des Managementnetzwerks und die aktuellen Zugangsdaten vor dem Anwenden der RCF-Datei bei. Nach dem Neustart können Sie eine neue Konfiguration mit der gleichen oder einer anderen Version der RCF-Datei anwenden.

Reset the Switch using the Cumulus install Option

Über diese Aufgabe

Verwenden Sie diese Schritte, wenn Sie den Schalter vollständig zurücksetzen möchten, indem Sie das Cumulus-Bild anwenden.

Bevor Sie beginnen

- Sie müssen über eine serielle Konsolenverbindung mit dem Switch verbunden sein.
- Das Cumulus Switch-Softwarebild ist über HTTP zugänglich.

> Weitere Informationen zur Installation von Cumulus Linux finden Sie unter "Überblick über Installation und Konfiguration von NVIDIA SN2100-Switches"

- Sie müssen das Root-Passwort für haben `sudo` Zugriff auf die Befehle.

Schritte

1. Von der Cumulus-Konsole herunterladen und die Switch-Software-Installation mit dem Befehl in Warteschlange stellen `onie-install -a -i` Anschließend folgt der Dateipfad zur Switch-Software:

   In diesem Beispiel die Firmware-Datei `cumulus-linux-4.4.2-mlx-amd64.bin` Wird vom HTTP-Server '50.50.50.50' auf den lokalen Switch kopiert.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.2-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.2-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.2-
mlx-amd64.bin
##################################################################
# 100.0%
```

```
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
```

```
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
future
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.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Antworten `y` Um die Eingabeaufforderung zur Bestätigung der Installation zu bestätigen, wenn das Image heruntergeladen und verifiziert wurde.
3. Starten Sie den Switch neu, um die neue Software zu installieren: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```

> Der Switch startet neu und wechselt in die Switch-Software-Installation, was einige Zeit in Anspruch nimmt. Nach Abschluss der Installation wird der Switch neu gestartet und bleibt an der Eingabeaufforderung „Login“.

4. Konfigurieren Sie die grundlegenden Switch-Einstellungen
   a. Wenn der Switch gestartet wird und in der Anmeldeaufforderung angezeigt wird, melden Sie sich an, und ändern Sie das Passwort.

   > Der Benutzername ist 'Cumulus' und das Standardpasswort lautet 'Cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.2u1
(2021-12-18) 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.

cumulus@cumulus:mgmt:~$
```

5. Konfigurieren Sie die Managementoberfläche.

> Das folgende Beispiel zeigt, wie der Hostname (IP_Switch_A_1), die IP-Adresse (10.10.10.10), die Netmask (255.255.255.0 (24)) und das Gateway (10.10.10.1) mit den Befehlen konfiguriert werden: `net add hostname <hostname>`, `net add interface eth0 ip address <IPAddress/mask>`, und `net add interface eth0 ip gateway <Gateway>`.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address 10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


net add/del commands since the last "net commit"


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

6. Starten Sie den Switch mithilfe des neu `sudo reboot` Befehl.

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

Wenn der Switch neu startet, können Sie eine neue Konfiguration mit den Schritten unter anwenden Laden Sie die NVIDIA RCF-Datei herunter, und installieren Sie sie.

Laden Sie die NVIDIA RCF-Dateien herunter und installieren Sie sie

Sie müssen die RCF-Datei des Switch auf jedem Switch der MetroCluster IP-Konfiguration herunterladen und installieren.

Bevor Sie beginnen

- Sie müssen das Root-Passwort für haben `sudo` Zugriff auf die Befehle.

- Die Switch-Software wird installiert und das Managementnetzwerk konfiguriert.
- Sie haben die ersten Schritte zur Installation des Switches mit der Methode 1 oder Methode 2 ausgeführt.
- Nach der Erstinstallation haben Sie keine zusätzliche Konfiguration angewendet.

> Wenn Sie nach dem Zurücksetzen des Switches und vor dem Anwenden der RCF-Datei eine weitere Konfiguration durchführen, können Sie dieses Verfahren nicht verwenden.

Über diese Aufgabe

Sie müssen diese Schritte bei jedem der IP-Schalter in der MetroCluster IP-Konfiguration (neue Installation) oder am Ersatzschalter (Switch-Austausch) wiederholen.

Schritte

1. Generieren Sie die NVIDIA RCF-Dateien für MetroCluster IP.
   a. Laden Sie die herunter "RCfFileGenerator für MetroCluster-IP".
   b. Generieren Sie die RCF-Datei für Ihre Konfiguration mit dem RcfFileGenerator für MetroCluster IP.
   c. Navigieren Sie zu Ihrem Home Directory. Wenn Sie als 'cumulus' angemeldet sind, lautet der Dateipfad `/home/cumulus`.

```
cumulus@IP_switch_A_1:mgmt:~$ cd ~
cumulus@IP_switch_A_1:mgmt:~$ pwd
/home/cumulus
cumulus@IP_switch_A_1:mgmt:~$
```

   d. Laden Sie die RCF-Datei in dieses Verzeichnis herunter. Das folgende Beispiel zeigt, dass Sie die Datei mit SCP herunterladen `MSN2100_v1.0_IP_switch_A_1.txt` Von Server '50.50.50.50' in Ihr Home-Verzeichnis und speichern Sie es als `MSN2100_v1.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/MSN2100_v1.0_IP_switch_A_1.txt
./MSN2100_v1.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*********************************************************************
**
Banner of the SCP server
*********************************************************************
**
username@50.50.50.50's password:
MSN2100_v1.0-X2_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Ausführen der RCF-Datei. Die RCF-Datei erfordert eine Option zum Anwenden eines oder mehrerer Schritte. Führen Sie die RCF-Datei ohne die Befehlszeilenoption aus, sofern Sie nicht vom technischen Support dazu aufgefordert werden. Um den Abschlussstatus der verschiedenen Schritte der RCF-Datei zu überprüfen, verwenden Sie die Option '-1' oder 'all', um alle (ausstehenden) Schritte anzuwenden.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

Deaktivieren Sie nicht verwendete ISL-Ports und Port-Kanäle

NetApp empfiehlt, nicht verwendete ISL-Ports und Port-Kanäle zu deaktivieren, um unnötige Integritätswarnungen zu vermeiden.

1. Identifizieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe des RCF-Datei-Banners:

> Wenn sich der Port im Breakout-Modus befindet, kann der im Befehl angegebene Portname von dem im RCF-Banner angegebenen Namen abweichen. Sie können auch die RCF-Verkabelungsdateien verwenden, um den Portnamen zu finden.

```
net show interface
```

2. Deaktivieren Sie die nicht verwendeten ISL-Ports und Port-Kanäle mithilfe der RCF-Datei.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

Mit dem folgenden Beispielbefehl wird der Port „swp14“ deaktiviert:

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Wiederholen Sie diesen Schritt für jeden identifizierten nicht verwendeten Port oder Port-Kanal.

Konfigurieren Sie MetroCluster IP-Switches für die Zustandsüberwachung

In MetroCluster IP-Konfigurationen können Sie SNMPv3 zur Überwachung des Funktionszustands von IP-Switches konfigurieren.

Schritt 1: Konfigurieren Sie den SNMPv3-Benutzer auf MetroCluster IP-Switches

Führen Sie die folgenden Schritte aus, um den SNMPv3-Benutzer auf den MetroCluster IP-Switches zu konfigurieren.

> Sie müssen in den Befehlen sowohl die Authentifizierungs- als auch die Datenschutzprotokolle verwenden. Die Verwendung von Authentifizierung ohne Datenschutz wird nicht unterstützt.

Für Broadcom IP-Switches

Schritte

1. Wenn die Benutzergruppe „Network-admin“ nicht bereits vorhanden ist, erstellen Sie sie:

   ```
   (IP_switch_1) (Config)# snmp-server group network-admin v3 auth read
   "Default"
   ```

2. Bestätigen Sie, dass die Gruppe „Network-admin“ erstellt wurde:

   ```
   (IP_switch_1) (Config)# show snmp group
   ```

3. Konfigurieren Sie den SNMPv3-Benutzer auf Broadcom IP-Switches:

   ```
   (IP_switch_1)# config
   (IP_switch_1) (Config)# snmp-server user <user_name> network-admin
   [auth-md5/auth-sha/noauth] "<auth_password>" [priv-aes128/priv-des]
   "<priv_password>"
   ```

   Sie müssen Anführungszeichen für die Authentifizierungs- und Datenschutzkennwörter verwenden, wie im folgenden Beispiel gezeigt:

   ```
   snmp-server user admin1 network-admin auth-md5 "password" priv-des
   "password"
   ```

Für Cisco IP-Switches

Schritte

1. Führen Sie die folgenden Befehle aus, um den SNMPv3-Benutzer auf einem Cisco IP-Switch zu konfigurieren:

   ```
   IP_switch_A_1 # configure terminal
   IP_switch_A_1 (config) # snmp-server user <user_name>  auth
   [md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
   ```

2. Überprüfen Sie, ob der SNMPv3-Benutzer auf dem Switch konfiguriert ist:

   ```
   IP_switch_A_1(config) # show snmp user <user_name>
   ```

   Das folgende Beispiel zeigt, dass der Benutzer `admin` Ist für SNMPv3 konfiguriert:

```
IP_switch_A_1(config)# show snmp user admin
User                Auth      Priv(enforce) Groups
acl_filter

____                ____      _____________ ______
__________

admin               md5       aes-128(no)   network-admin
```

Schritt 2: Konfigurieren Sie den SNMPv3-Benutzer in ONTAP

Führen Sie die folgenden Schritte aus, um den SNMPv3-Benutzer in ONTAP zu konfigurieren.

1. Konfigurieren Sie den SNMPv3-Benutzer in ONTAP:

   ```
   security login create -user-or-group-name <user_name> -application snmp
   -authentication-method usm -remote-switch-ipaddress <ip_address>
   ```

2. Konfigurieren Sie die Switch-Statusüberwachung, um den Switch mithilfe des neuen SNMPv3-Benutzers zu überwachen:

   ```
   system switch ethernet modify -device <device_id> -snmp-version SNMPv3
   -community-or-username <user_name>
   ```

3. Überprüfen Sie, ob die Seriennummer des Geräts, die mit dem neu erstellten SNMPv3-Benutzer überwacht wird, korrekt ist:

   a. Den Abfragezeitraum für die Überwachung des Switch-Funktionszustands anzeigen:

      ```
      system switch ethernet polling-interval show
      ```

   b. Führen Sie den folgenden Befehl aus, nachdem der Abfragezeitraum abgelaufen ist:

      ```
      system switch ethernet show-all -instance -device <device_serial_number>
      ```

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN 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.