MetroCluster IP スイッチを設定します

ONTAP MetroCluster

NetApp
February 13, 2026

目次

MetroCluster IP スイッチを設定します

適切なMetroCluster IPスイッチ構成手順を選択する

バックエンドMetroCluster IP接続を提供するには、IPスイッチを設定する必要があります。手順はスイッチベンダーによって異なります。

- "Broadcom IP スイッチを設定します"
- "Cisco IP スイッチを設定する"
- "NVIDIA IPスイッチを設定します"

クラスタ相互接続とバックエンドMetroCluster IP 接続用にBroadcom IP スイッチを構成する

クラスタインターコネクトおよびバックエンド MetroCluster IP 接続用に Broadcom IP スイッチを設定する必要があります。

次のような場合は、構成に追加のライセンス（100Gbポートライセンス×6）が必要になります。

- ポート53および54を40GbpsまたはMetroCluster ISLとして使用します。
- ローカルクラスタインターフェイスとMetroCluster インターフェイスをポート49-52に接続するプラットフォームを使用します。

Broadcom IP スイッチを工場出荷時のデフォルトにリセット

新しいバージョンのスイッチソフトウェアと RCF をインストールする前に、 Broadcom スイッチの設定を消去し、基本的な設定を完了する必要があります。

このタスクについて

- この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソールを使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

手順

1. 昇格されたコマンドプロンプト (#):'enable' に変更します

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

2. スタートアップコンフィギュレーションを消去し、バナーを削除します

   a. スタートアップ設定を消去します。

*`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) #
```

このコマンドでは、バナーは消去されません。

b. バナーを削除します。

no set clibanner

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

3. スイッチを再起動します *(IP_switch_A_1)#reload *

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

スイッチをリロードする前に、未保存または変更された設定を保存するかどうかを確認するメッセージが表示された場合は、 **No** を選択します。

4. スイッチがリロードされるまで待ってから、スイッチにログインします。

デフォルトのユーザは「 admin 」で、パスワードは設定されていません。次のようなプロンプトが表示されます。

```
(Routing)>
```

5. 管理者特権のコマンドプロンプトに切り替えます。

「 enable 」を選択します

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

6. サービスポートプロトコルを「 none 」に設定します。

「サービスポートプロトコルなし」

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

(Routing) #
```

7. サービスポートに IP アドレスを割り当てます。

   'erviceport IP_address*netmask* gateway_

   次の例では、サービスポートに IP アドレス「 10.10.10.10 」が割り当てられています。サブネットは「 255.255.255.0 」、ゲートウェイは「 10.10.10.1 」です。

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

8. サービスポートが正しく設定されていることを確認します。

   'How serviceport

   次の例は、ポートが稼働しており、正しいアドレスが割り当てられていることを示しています。

```
(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. SSH サーバーを構成します。

   - RCF ファイルで Telnet プロトコルが無効になります。SSH サーバを設定しない場合は、シリアルポート接続を使用してブリッジにアクセスする必要があります。
   - ログ収集やその他の外部ツールを使用するには、SSH サーバーを構成する必要があります。

a. RSA キーを生成します。

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

b. DSA キーの生成（オプション）

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

c. FIPS 準拠バージョンの EFOS を使用している場合は、 ECDSA キーを生成します。次の例では、長さ521のキーを作成します。有効な値は、 256 、 384 、または 521 です。

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

d. SSH サーバを有効にします。

必要に応じて、設定コンテキストを終了します。

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

+

キーがすでに存在する場合は、それらを上書きするように求められることがあります。

10. 必要に応じて、ドメインとネームサーバを設定します。

「 configure 」を実行します

次に 'ip domain' コマンドと 'ip name server' コマンドの例を示します

```
(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. 必要に応じて、タイムゾーンと時刻の同期（ SNTP ）を設定します。

次に 'ntp' コマンドの例を示しますこの例では 'sntp サーバの IP アドレスと相対タイム・ゾーンを指定します

```
(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)#
```

EFOSバージョン3.10.0.3以降の場合は、 `ntp` 次の例に示すように、コマンドを実行します。

```
> (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. スイッチ名を設定します。

    'hostname ip_switch_a_1'

    スイッチのプロンプトに新しい名前が表示されます。

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. 設定を保存します。

    「メモリの書き込み」

    次の例のようなプロンプトと出力が表示されます。

```
(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. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

Broadcom スイッチの EFOS ソフトウェアのダウンロードとインストール

MetroCluster IP 構成の各スイッチにスイッチのオペレーティングシステムファイルと RCF ファイルをダウンロードする必要があります。

このタスクについて

このタスクは、 MetroCluster IP 構成内のスイッチごとに実行する必要があります。

- 次の点に注意してください。 *
- EFOS 3.x.x から EFOS 3.x.x 以降にアップグレードするときは、スイッチが EFOS 3.4.4.6 （または 3.4.x.x 以降のリリース）を実行している必要があります。それよりも前のリリースを実行している場合は、まずスイッチを EFOS 3.4.4.6 （または 3.4.x.x 以降のリリース）にアップグレードしてから、スイッチを EFOS 3.x.x 以降にアップグレードします。
- EFOS 3.x.x と 3.7.x.x 以降の設定は異なります。EFOS バージョンを 3.4.x.x から 3.7.x.x 以降、またはその逆に変更する場合は、スイッチを工場出荷時のデフォルトにリセットする必要があり、対応する EFOS バージョンの RCF ファイルが適用される（再適用される）必要があります。この手順には、シリアルコンソールポート経由でアクセスする必要があります。
- EFOS バージョン 3.7.x.x 以降では、 FIPS に準拠していないバージョンと FIPS に準拠したバージョンが提供されています。FIPS に準拠していないバージョンから FIPS に準拠したバージョンに移行する場合とその逆に移行する場合は、さまざまな手順があります。EFOS を FIPS 非準拠バージョンから FIPS 準拠バージョンに変更するか、その逆に変更すると、スイッチが工場出荷時のデフォルトにリセットされます。この手順には、シリアルコンソールポート経由でアクセスする必要があります。

手順

1. からスイッチファームウェアをダウンロードし"Broadcomサポートサイト"ます。
2. 「show fips status」コマンドを使用して、EFOSのバージョンがFIPSに準拠しているか、FIPSに準拠していないかを確認します。次の例では'ip_switch_a_1'はFIPS準拠のEFOSを使用しており'ip_switch_a_2'はFIPS非準拠のEFOSを使用しています

*例1 *

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

*例2 *

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

IP_switch_A_2 #
```

3. 次の表を参照して、実行する必要がある方法を確認してください。

* 手順 *	* 現在の EFOS バージョン *	* 新しい EFOS バージョン *	* 高レベルステップ *
FIPS に準拠している 2 つのバージョン間で EFOS をアップグレードする手順	3.4.x.x	3.4.x.x	方法 1 ）設定とライセンスの情報は保持されています
3.4.4.6 （または 3.4.x.x 以降）	3.7.x.x 以降の非 FIPS 準拠	方法 1 を使用して EFOS をアップグレードします。スイッチを工場出荷時のデフォルトにリセットして、 EFOS 3.x.x 以降の RCF ファイルを適用します	3.7.x.x 以降の非 FIPS 準拠
3.4.4.6 （または 3.4.x.x 以降）	方法 1 を使用して EFOS をダウングレードします。スイッチを工場出荷時のデフォルトにリセットして、 EFOS 3.x.x の RCF ファイルを適用します	3.7.x.x 以降の非 FIPS 準拠	
方法 1 を使用して新しい EFOS イメージをインストールします。構成とライセンスの情報は保持されます	3.7.x.x 以降の FIPS に準拠しています	3.7.x.x 以降の FIPS に準拠しています	方法 1 を使用して新しい EFOS イメージをインストールします。構成とライセンスの情報は保持されます

FIPS 準拠の EFOS バージョンへのアップグレード手順	FIPS に準拠していません	FIPS に準拠している	方法 2 を使用した EFOS イメージのインストールスイッチの設定とライセンス情報が失われます。

- 方法 1 ： ソフトウェアイメージをバックアップブートパーティションにダウンロードして EFOS をアップグレードする手順
- 方法 2 ： ONIE OS インストールを使用して EFOS をアップグレードする手順

ソフトウェアイメージをバックアップブートパーティションにダウンロードして **EFOS** をアップグレードする手順

次の手順を実行できるのは、両方の EFOS バージョンが FIPS 非準拠であるか、両方の EFOS バージョンが FIPS 準拠である場合のみです。

FIPS に準拠したバージョンで、もう一方のバージョンが FIPS に準拠していない場合は、次の手順を使用しないでください。

手順

1. スイッチソフトウェアをスイッチにコピーします :+copy sftp://user@50.50.50.50 /switchsoftware/efos-3.4.6.stk backup+`

   この例では、 efos-3.4.6.stk オペレーティングシステムファイルが SFTP サーバ（ 50.50.50 ）からバックアップパーティションにコピーされています。使用する TFTP / SFTP サーバの IP アドレスを指定し、インストールする必要がある RCF ファイルのファイル名を指定する必要があります。

```
(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. 次回リブート時にスイッチをバックアップパーティションからブートするように設定します。

   「ブート・システム・バックアップ」を参照してください

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

(IP_switch_A_1) #
```

3. 次回ブート時に新しいブートイメージがアクティブになることを確認します。

   'How 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. 設定を保存します。

   「メモリの書き込み」

```
(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. スイッチをリブートします。

   「再ロード」

```
(IP_switch_A_1) #reload

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

6. スイッチがリブートするまで待ちます。

まれに、スイッチが起動しないことがあります。に従ってください ONIE OS インストールを使用して EFOS をアップグレードする手順 新しいイメージをインストールします。

7. スイッチを EFOS 3.x.x から EFOS 3.x.x に変更した場合、またはその逆の場合は、次の 2 つの手順に従って正しい設定（ RCF ）を適用します。
   a. Broadcom IP スイッチを工場出荷時のデフォルトにリセット
   b. Broadcom の RCF ファイルのダウンロードとインストール
8. MetroCluster IP 構成の残りの 3 つの IP スイッチについて、上記の手順を繰り返します。

ONIE OS インストールを使用して **EFOS** をアップグレードする手順

一方の EFOS バージョンが FIPS に準拠していて、もう一方の EFOS バージョンが FIPS に準拠していない場合は、次の手順を実行できます。次の手順は、スイッチがブートに失敗した場合に、 ONIE から FIPS 非準拠または FIPS 準拠の EFOS 3.x.x イメージをインストールするために使用できます。

手順

1. スイッチを ONIE インストールモードで起動します。

   起動中に、次の画面が表示されたら ONIE を選択します。

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

   「 ONIE 」を選択すると、スイッチがロードされ、次の選択肢が表示されます。

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

スイッチが ONIE インストールモードで起動します。

2. ONIE の検出を停止し、イーサネットインターフェイスを設定します

   次のメッセージが表示されたら、 <ENTER> を押して ONIE コンソールを起動します。

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

   ONIE の検出は続行され、メッセージがコンソールに出力されます。

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

3. イーサネットインターフェイスを設定し、「 ifconfig eth0 <ipAddress> netmask <netmask> up 」および「 route add default gw <gatewayAddress> 」を使用してルートを追加します

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

4. ONIE インストールファイルをホストしているサーバにアクセスできることを確認します。

```
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. 新しいスイッチソフトウェアをインストールします

```
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.
```

ソフトウェアがスイッチをインストールし、リブートします。スイッチを通常どおりにリブートして新しい EFOS バージョンにします。

6. 新しいスイッチソフトウェアがインストールされていることを確認します

'How 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. インストールを完了します

   設定を適用せずにスイッチがリブートし、工場出荷時のデフォルトにリセットされます。2 つの手順に従ってスイッチの基本設定を行い、次の 2 つのドキュメントに記載されているように RCF ファイルを適用します。

   a. スイッチの基本設定を行います。手順 4 以降を実行します。 Broadcom IP スイッチを工場出荷時のデフォルトにリセット
   b. の説明に従って、 RCF ファイルを作成して適用します Broadcom の RCF ファイルのダウンロードとインストール

Broadcom の RCF ファイルのダウンロードとインストール

MetroCluster IP構成の各スイッチにスイッチのRCFファイルを生成してインストールする必要があります。

作業を開始する前に

この作業には、 FTP 、 TFTP 、 SFTP 、 SCP などのファイル転送ソフトウェアが必要です。 ファイルをスイッチにコピーします。

このタスクについて

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

RCF ファイルは 4 つあり、それぞれが MetroCluster IP 構成の 4 つの各スイッチに対応しています。使用するスイッチのモデルに対応した正しい RCF ファイルを使用する必要があります。

スイッチ	RCF ファイル
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

EFOS バージョン 3.4.4.6 以降の 3.4.x.x の RCF ファイルリリースと EFOS バージョン 3.7.0.4 は異なります。スイッチが実行されている EFOS バージョンの正しい RCF ファイルを作成したことを確認する必要があります。

EFOS バージョン	RCF ファイルのバージョン
3.4.x.x	V1.3 倍、 V1.4 倍
3.7.x.x	v2.x

手順

1. MetroCluster IP 用の Broadcom RCF ファイルを生成します。
   a. ダウンロード "MetroCluster IP 用の RcfFileGenerator"

b. RcfFileGenerator for MetroCluster IPを使用して、設定用のRCFファイルを生成します。

ダウンロード後にRCFファイルを変更することはできません。

2. RCF ファイルをスイッチにコピーします。

a. RCFファイルを最初のスイッチにコピーします。'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

この例では、「 BES-53248_v1.32_Switch-A1.txt 」 RCF ファイルを、 SFTP サーバの「 0.50.50.50 」からローカルブートフラッシュにコピーしています。使用する TFTP / SFTP サーバの IP アドレスを指定し、インストールする必要がある RCF ファイルのファイル名を指定する必要があります。

```
(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. RCF ファイルがスクリプトとして保存されたことを確認します。

「原稿リスト」

```
(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. RCF スクリプトを適用します。

「 script apply BES-53248 v1.32_Switch-A1.scr 」を参照してください

```
(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. 設定を保存します。

「メモリの書き込み」

```
(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. スイッチをリブートします。

「再ロード」

```
(IP_switch_A_1) #reload

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

a. 残りの 3 つのスイッチのそれぞれについて、同じ手順を繰り返します。それぞれのスイッチに対応する RCF ファイルをコピーするように注意してください。

3. スイッチをリロードします。

「再ロード」

```
IP_switch_A_1# reload
```

4. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

未使用のISLポートとポートチャネルを無効にする

NetAppでは、不要なヘルスアラートを回避するために、未使用のISLポートとポートチャネルを無効にすることを推奨します

1. RCFファイルのバナーを使用して、未使用のISLポートとポートチャネルを特定します。

ポートがブレークアウトモードの場合は、コマンドで指定するポート名がRCFバナーに表示される名前と異なることがあります。RCFケーブル接続ファイルを使用してポート名を検索することもできます。

ISLホオトノシヨウサイ

コマンドを実行します `show port all`。

ポートチャネルの詳細

コマンドを実行します `show port-channel all`。

2. 未使用のISLポートとポートチャネルを無効にします。

   特定された未使用のポートまたはポートチャネルごとに、次のコマンドを実行する必要があります。

```
(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
```

Cisco IP スイッチを設定する

クラスタ相互接続とバックエンド**MetroCluster IP** 接続用に**Cisco IP** スイッチを構成する

クラスタインターコネクトおよびバックエンド MetroCluster IP 接続用に Cisco IP スイッチを設定する必要があります。

このタスクについて

このセクションの手順のいくつかは独立した手順であり、実行する必要があるのは自分がタスクに指示された手順、またはタスクに関連する手順のみです。

Cisco IP スイッチを工場出荷時のデフォルトにリセットする

RCF ファイルをインストールする前に、 Cisco スイッチの設定を消去し、基本的な設定を完了する必要があります。この手順 は、以前のインストールに失敗したあとに同じ RCF ファイルを再インストールする場合、または新しいバージョンのファイルをインストールする場合に必要です。

このタスクについて

- この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソールを使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

手順

1. スイッチを工場出荷時のデフォルトにリセットします。

a. 既存の設定を消去します。

「 write erase 」を入力します

b. スイッチソフトウェアをリロードします。

「再ロード」

システムがリブートし、設定ウィザードが表示されます。起動中に「 Abort Auto Provisioning and continue with normal setup ？」というプロンプトが表示された場合は、(yes/no)[n]`" 、続行するには 'yes' と応答する必要があります。

c. 設定ウィザードで、スイッチの基本設定を入力します。

- 管理パスワード
- スイッチ名
- アウトオブバンド管理設定
- デフォルトゲートウェイ
- SSH サービス（ RSA ）

設定ウィザードが完了すると、スイッチがリブートします。

d. プロンプトが表示されたら、ユーザ名とパスワードを入力してスイッチにログインします。

次の例は、スイッチを設定する際のプロンプトとシステム応答を示しています。山括弧（「 <<<`) 」）は、情報を入力する場所を示します。

```
---- 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.
```

次の一連のプロンプトで、スイッチ名、管理アドレス、ゲートウェイなどの基本情報を入力し、 SSH with RSA を選択します。

この例は、RCFの設定に必要な最小限の情報を示しています。RCFの適用後に追加オプションを設定できます。たとえば、RCFを適用したあとにSNMPv3、NTP、またはSCP / SFTPを設定できます。

```
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]:
```

最後の一連のプロンプトで設定が完了します。

```
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. 設定を保存します。

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

3. スイッチをリブートし、スイッチがリロードされるまで待ちます。

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

4. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

Cisco スイッチの NX-OS ソフトウェアのダウンロードとインストール

MetroCluster IP 構成の各スイッチにスイッチのオペレーティングシステムファイルと RCF ファイルをダウンロードする必要があります。

このタスクについて

この作業には、 FTP 、 TFTP 、 SFTP 、 SCP などのファイル転送ソフトウェアが必要です。 ファイルをスイッチにコピーします。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

"NetApp Hardware Universe の略"

手順

1. サポートされている NX-OS ソフトウェアファイルをダウンロードします。

   "シスコソフトウェアのダウンロード"

2. スイッチソフトウェアをスイッチにコピーします。

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

   この例では、nxos.7.0.3.I4.6.bin ファイルと EPLD イメージが SFTP サーバ 10.10.99.99 からローカル ブートフラッシュにコピーされます。

```
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)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/n9000-epld.9.3.5.img  /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img                161MB   9.5MB/s   00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

3. 各スイッチの bootflash ディレクトリにスイッチの NX-OS ファイルがあることを確認します。

   「 IR bootflash: 」のように表示されます

   次の例は、 FC_switch_A_1 にファイルが存在することを示しています。

```
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. スイッチソフトウェアをインストールします。

   すべての nxos bootflash:nxos.version-number.bin をインストールします

   スイッチソフトウェアがインストールされると、スイッチは自動的にリロード（リブート）します。

   次の例は、 FC_switch_A_1 へのソフトウェアのインストールを示しています。

```
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. スイッチがリロードされるまで待ってから、スイッチにログインします。

スイッチがリブートされると、ログインプロンプトが表示されます。

```
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. スイッチソフトウェアがインストールされていることを確認します :+`show version`

次の例は、の出力を示しています。

```
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. EPLD イメージをアップグレードし、スイッチを再起動します。

```
IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module        Type         Upgradable    Impact      Reason
------  ------------------ ------------ ----------- -----------------
     1         SUP         Yes           disruptive  Module Upgradable

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

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

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

EPLDs upgraded.

Module 1 EPLD upgrade is successful.
```

8. [[step8] スイッチのリブート後に再度ログインし、新しいバージョンの EPLD が正常にロードされたことを確認します。

   ```
   show version module 1 epld
   ```

9. MetroCluster IP 構成の残りの 3 つの IP スイッチについて、上記の手順を繰り返します。

Cisco IP RCF ファイルのダウンロードとインストール

MetroCluster IP構成の各スイッチにRCFファイルを生成してインストールする必要があります。

このタスクについて

この作業には、 FTP 、 TFTP 、 SFTP 、 SCP などのファイル転送ソフトウェアが必要です。 ファイルをス

イッチにコピーします。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

"NetApp Hardware Universe の略"

QSFP / SFP+アダプタを使用している場合は、ISLポートをブレークアウト速度モードではなくネイティブ速度モードで設定する必要があります。ISLポートの速度モードについては、スイッチベンダーのドキュメントを参照してください。

RCF ファイルは 4 つあり、それぞれが MetroCluster IP 構成の 4 つの各スイッチに対応しています。使用するスイッチのモデルに対応した正しい RCF ファイルを使用する必要があります。

スイッチ	RCF ファイル
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

手順

1. MetroCluster IP用のCisco RCFファイルを生成します。
   a. ダウンロード "MetroCluster IP 用の RcfFileGenerator"
   b. RcfFileGenerator for MetroCluster IPを使用して、設定用のRCFファイルを生成します。

      ダウンロード後にRCFファイルを変更することはできません。

2. RCF ファイルをスイッチにコピーします。
   a. RCF ファイルを最初のスイッチにコピーします。

      'copy sftp://root@ftp-server-ip-address /tftpboot/switch-specific -RCF bootflash:vrf management`

      この例では、 NX3232_v1.80_Switch-A1.txt RCF ファイルを SFTP サーバの 10.10.99.99 からローカルブートフラッシュにコピーしています。使用する TFTP / SFTP サーバの IP アドレスと、インストールする必要がある RCF ファイルのファイル名を使用する必要があります。

```
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. 残りの 3 つのスイッチのそれぞれについて、同じ手順を繰り返します。それぞれのスイッチに対応する RCF ファイルをコピーするように注意してください。

3. 各スイッチの bootflash ディレクトリに RCF ファイルがあることを確認します。

「IR bootflash: 」のように表示されます

次の例は、 FC_switch_A_1 にファイルが存在することを示しています。

```
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. Cisco 3132Q-V および Cisco 3232C スイッチの TCAM リージョンを設定します。

Cisco 3132Q-V または Cisco 3232C スイッチを使用していない場合は、この手順を省略します。

a. Cisco 3132Q-V スイッチで、次の TCAM リージョンを設定します。

```
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. Cisco 3232C スイッチで、次の TCAM リージョンを設定します。

```
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. TCAM リージョンを設定したら、設定を保存してスイッチをリロードします。

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

5. 各スイッチで、対応する RCF ファイルをローカルブートフラッシュから実行中の設定にコピーします。

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

6. 各スイッチで、実行中の設定からスタートアップ設定に RCF ファイルをコピーします。

   'copy running-config startup-config

   次のような出力が表示されます。

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

7. スイッチをリロードします。

   「再ロード」

```
IP_switch_A_1# reload
```

8. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

25Gbps 接続を使用するシステムの前方誤り訂正の設定

25Gbps 接続を使用してシステムが設定されている場合は、 RCF ファイルの適用後に前方誤り訂正（ fec ）パラメータを手動で off に設定する必要があります。この設定は RCF ファイルでは適用されません。

このタスクについて

この手順を実行する前に、 25Gbps ポートがケーブル接続されている必要があります。

"Cisco 3232C スイッチまたは Cisco 9336C スイッチのプラットフォームポートの割り当て"

このタスクでは、 25Gbps 接続を使用する環境 プラットフォームのみを使用します。

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

このタスクは、 MetroCluster IP 構成の 4 つのスイッチすべてで実行する必要があります。

手順

1. コントローラモジュールに接続されている各 25Gbps ポートで fec パラメータを off に設定し、実行中の設定をスタートアップ設定にコピーします。

   a. 構成モードを開始します :config t

   b. 設定する 25Gbps インターフェイスを「 interface interface-Id 」と指定します

   c. fec を off に設定します

   d. スイッチの各 25Gbps ポートについて、上記の手順を繰り返します。

   e. 構成モードを終了します : exit

   次の例は、スイッチ IP_switch_A_1 のインターフェイス Ethernet1/25/1 に対するコマンドを示しています。

```
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. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

未使用のISLポートとポートチャネルを無効にする

NetAppでは、不要なヘルスアラートを回避するために、未使用のISLポートとポートチャネルを無効にすることを推奨します

1. 未使用のISLポートとポートチャネルを特定します。

   「インターフェイスの概要」

2. 未使用のISLポートとポートチャネルを無効にします。

   特定された未使用のポートまたはポートチャネルごとに、次のコマンドを実行する必要があります。

```
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.
```

MetroCluster IPサイト内のCisco 9336Cスイッチで MACsec暗号化を構成する

MACsec 暗号化は、 WAN ISL ポートにのみ適用できます。

Cisco 9336C スイッチに MACsec 暗号化を設定します

サイト間で実行される WAN ISL ポートにのみ MACsec 暗号化を設定する必要があります。正しい RCF ファイルを適用したあとに MACsec を設定する必要があります。

MACsec のライセンス要件

MACsec にはセキュリティライセンスが必要です。Cisco NX-OS ライセンス方式の詳細およびライセンスの取得方法と適用方法については、を参照してください "『 Cisco NX-OS Licensing Guide 』"

MetroCluster IP構成でCisco MACsec暗号化WAN ISLを有効にします

MetroCluster IP 構成では、 WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化をイネーブルにできます。

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. デバイスで MACsec と MKA を有効にします。

「 feature MACsec

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

3. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

MACsecキーチェーンとキーを設定します

MACsec キーチェーンまたはキーをコンフィギュレーションに作成できます。

- キーライフタイムと Hitless Key Rollover *

MACsec キーチェーンには、複数の Pre-Shared Key （ PSK; 事前共有キー）を設定できます。各 PSKs には、キー ID とオプションのライフタイムが設定されています。キーの有効期間は、キーがアクティブになって有効期限が切れるタイミングを指定します。ライフタイム設定がない場合、デフォルトのライフタイムは無制限です。ライフタイムが設定されている場合、ライフタイムが期限切れになると、 MKA はキーチェーン内で設定されている次の事前共有キーにロールオーバーします。キーのタイムゾーンは、 local または UTC です。デフォルトのタイムゾーンは UTC です。キーを同じキーチェーン内の 2 番目のキー（キーチェーン内）にロールオーバーして、最初のキーのライフタイムを設定することができます。最初のキーの有効期間が終了すると、自動的にリスト内の次のキーにロールオーバーされます。リンクの両側で同じキーが同時に設定されている場合、キーのロールオーバーはヒットレスになります（つまり、キーはトラフィックを中断することなくロールオーバーされます）。

手順

1. グローバルコンフィギュレーションモードを開始します。

「 configure terminal 」をクリックします

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

2. 暗号化されたキーオクテット文字列を非表示にするには、「 show running-config 」コマンドと「 show startup-config 」コマンドの出力で、文字列をワイルドカード文字に置き換えます。

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

オクテット文字列は、コンフィギュレーションをファイルに保存するときにも非表示になります。

デフォルトでは、 PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、 MACsec キーチェーンにのみ適用されます。

3. MACsec キーチェーンを作成して一連の MACsec キーを保持し、 MACsec キーチェーンコンフィギュレーションモードを開始します。

   キーチェーン名 MACsec

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

4. MACsec キーを作成し、 MACsec キーコンフィギュレーションモードを開始します。

   「 key key-id 」

   指定できる 16 進数のキー文字列の範囲は 1 ～ 32 で、最大サイズは 64 文字です。

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

5. キーのオクテット文字列を設定します。

   「 key-octet-string octet-string octet-string cryptographic-algorithm ae_128_CMAC | aes-256_CMAC 」という形式で指定します

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

   octet-string 引数には、最大 64 個の 16 進文字を含めることができます。オクテットキーは内部でエンコードされるため、クリアテキストのキーは、「 show running-config macsec 」コマンドの出力には表示されません。

6. キーの送信ライフタイムを設定します（秒単位）。

   「 send-lifetime start-time duration 」

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

   デフォルトでは、デバイスは開始時間を UTC として処理します。start-time 引数には、キーがアクティブになる時刻と日付を指定します。duration 引数は、ライフタイムの秒単位の長さです。最大値は 2147483646 秒（約 68 年）です。

7. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

   'copy running-config startup-config

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

8. キーチェーン設定を表示します。

   「鍵チェーン名」

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

MACsecポリシーを設定します

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. MACsec ポリシーを作成します。

   「 ACSEC ポリシー名」

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

3. 次のいずれかの暗号、 gcm-aes-128 、 gcm-aes-256 、 gcm-aes-xpN-128 、または gcm-aes-xpN-256 を設定します。

   「 cipher-site name 」

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

4. キー交換時にピア間の接続を解除するために、キーサーバの優先度を設定します。

   「 key-server -priority number 」と入力します

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

5. データおよび制御パケットの処理を定義するセキュリティポリシーを設定します。

   「セキュリティ・ポリシー・セキュリティ・ポリシー」を参照してください

次のオプションからセキュリティポリシーを選択します。

- must-secure — MACsec ヘッダーを伝送していないパケットはドロップされます
- must-secure — MACsec ヘッダーを伝送しないパケットは許可されます (これがデフォルト値です) 。

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

6. リプレイ保護ウィンドウを設定して、セキュアインターフェイスが設定されたウィンドウサイズより小さいパケットを受け入れないようにします。「 window-size number 」

> リプレイ保護ウィンドウのサイズは、 MACsec が受信して破棄されない最大アウトオブシーケンスフレーム数を表します。指定できる範囲は 0 ～ 596000000 です。

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

7. SAK キーの再生成を強制する時間を秒単位で設定します。

「 SAK-expiry-date time 」

このコマンドを使用して、予測可能な時間間隔にセッションキーを変更できます。デフォルトは 0 です。

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

8. 暗号化を開始するレイヤ 2 フレームで、次の機密性オフセットのいずれかを設定します。

「 conf-offsetconfidentiality offset 」を参照してください

次のいずれかのオプションを選択します。

- conf-offset-0 。
- conf-offset-30 。
- conf -offset-50 。

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

> このコマンドは、中間スイッチが MPLS タグのようなパケットヘッダー（ DMAC 、 smac 、 type ）を使用するために必要な場合があります。

9. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

10. MACsec ポリシー設定を表示します。

    「 MACsec ポリシー」

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

インターフェイス上で**Cisco MACsec**暗号化をイネーブルにします

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. MACsec暗号化で設定したインターフェイスを選択します。

   インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

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

3. インターフェイスに設定するキーチェーンとポリシーを追加して、MACsec設定を追加します。

   「MACsec keychain -name policy policy-name」という名前のキーチェーンがあります

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

4. MACsec暗号化を設定するすべてのインターフェイスで、ステップ1と2を繰り返します。
5. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

   'copy running-config startup-config

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

MetroCluster IP構成で**Cisco MACsec**暗号化**WAN ISL**をディセーブルにします

MetroCluster IP 構成では、 WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化を無効にする必要

がある場合があります。

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. デバイスの MACsec 設定を無効にします。

   「 ACSEC SHUTDOWN 」のようになります

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

   「 no 」オプションを選択すると、 MACsec 機能が復元されます。

3. MACsec で設定済みのインターフェイスを選択します。

   インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

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

4. インターフェイスに設定されているキーチェーンとポリシーを削除して、MACsec設定を削除します。

   「no MACsec keychain keychain -name policy policy-name」

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

5. MACsec が設定されているすべてのインターフェイスで、ステップ 3 と 4 を繰り返します。
6. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

   'copy running-config startup-config

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

MACsec 構成の確認

手順

1. コンフィギュレーション内の 2 番目のスイッチで上記の手順 * すべて * を繰り返して、 MACsec セッションを確立します。
2. 次のコマンドを実行して、両方のスイッチが正常に暗号化されたことを確認します。

   a. 「 How MACsec mka summary 」を実行します

   b. 実行 :'How MACsec mka session`

   c. 実行： 'How MACsec mka statistics （ MACsec mka 統計情報）

   MACsec 設定を確認するには、次のコマンドを使用します。

コマンドを実行します	表示される情報
'How MACsec mka session interface types/port number	特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッション
「鍵チェーン名」	キーチェーン設定
「 MACsec mka の概要」を参照してください	MACsec MKA 設定
'How MACsec policy policy-name' 」を参照してください	特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定

NVIDIA IPスイッチを設定します

クラスタ相互接続とバックエンド**MetroCluster IP** 接続用に**NVIDIA IP SN2100** スイッチを構成する

クラスタインターコネクトおよびバックエンドMetroCluster IP接続用にNVIDIA SN2100 IPスイッチを設定する必要があります。

[[Reset-The switch]] NVIDIA IP SN2100スイッチを工場出荷時のデフォルトにリセットします

スイッチを工場出荷時のデフォルト設定にリセットするには、次のいずれかの方法を選択します。

- RCFファイルオプションを使用してスイッチをリセットします
- Cumulusソフトウェアのダウンロードとインストール

[RCFファイルオプション]] RCFファイルオプションを使用してスイッチをリセットします

新しいRCF設定をインストールする前に、NVIDIAスイッチ設定をリバートする必要があります。

このタスクについて

スイッチをデフォルト設定に戻すには、「restoreDefaults」オプションを指定してRCFファイルを実行します。このオプションを選択すると、元のバックアップファイルが元の場所にコピーされ、スイッチがリブートされます。リブート後、スイッチを設定するためにRCFファイルを最初に実行したときに使用していた元の設定がスイッチにオンラインになります。

次の設定の詳細はリセットされません。

- ユーザおよびクレデンシャルの設定
- 管理ネットワークポートeth0の設定

RCFファイルの適用中に発生するその他の設定変更は、すべて元の設定にリバートされます。

作業を開始する前に

- に従ってスイッチを設定する必要があります NVIDIAのRCFファイルをダウンロードしてインストールします。この方法で設定していない場合やRCFファイルを実行する前に追加機能を設定している場合は、この手順 を使用できません。
- この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソール接続を使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

手順

1. 同じバージョンまたは互換性のあるRCFファイルを使用してRCF設定が正常に適用され、バックアップファイルが存在することを確認します。

出力には、バックアップファイル、保持されたファイル、またはその両方が表示されます。バックアップファイルまたは保存されたファイルが出力に表示されない場合は、この手順 を使用できません。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_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. デフォルトに戻すオプションを指定してRCFファイルを実行します。'restoreDefaults'

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_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. プロンプトに「yes」と入力します。スイッチが元の設定に戻り、リブートします。
4. スイッチがリブートするまで待ちます。

   スイッチがリセットされ、RCFファイルを適用する前の既存の管理ネットワーク設定や現在のクレデンシャルなどの初期設定が保持されます。リブート後、同じバージョンまたは別のバージョンのRCFファイルを使用して新しい設定を適用できます。

Cumulusソフトウェアのダウンロードとインストール

このタスクについて

Cumulus画像を適用してスイッチを完全にリセットするには、次の手順を実行します。

作業を開始する前に

- シリアルコンソール接続を使用してスイッチに接続する必要があります。
- Cumulusスイッチソフトウェアイメージには、HTTP経由でアクセスできます。

> Cumulus Linuxのインストールの詳細については、を参照してください。 "NVIDIA SN2100スイッチのインストールと設定の概要"

- コマンドへの「sudo」アクセス用のrootパスワードが必要です。

手順

1. Cumulusコンソールから、スイッチ・ソフトウェアのインストールを「ONIE-install-A-i」コマンドに続けてスイッチ・ソフトウェアへのファイル・パスを指定して、ダウンロードしてキューに入れます。

   この例では、ファームウェアファイル `cumulus-linux-4.4.3-mlx-amd64.bin` HTTPサーバ「50.50.50.50」からローカルスイッチにコピーされます。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.3-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.3-
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. イメージのダウンロードおよび確認時に'プロンプトにyと応答してインストールを確認します
3. 新しいソフトウェア「sudo reboot」をインストールするには、スイッチを再起動します

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

スイッチがリブートし、スイッチソフトウェアのインストールが開始されます。この処理にはしばらく時間がかかります。インストールが完了すると、スイッチがリブートし、「log-in」プロンプトが表示されたままになります。

4. スイッチの基本設定を行います
   a. スイッチがブートされ、ログインプロンプトでログインし、パスワードを変更します。

ユーザ名は「cumulus」で、デフォルトのパスワードは「cumulus」です。

```
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+cl4.4.3u1
(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. 管理ネットワークインターフェイスを設定

   使用するコマンドは、実行しているスイッチファームウェアのバージョンによって異なります。

   次に、ホスト名をIP_switch_A_1、IPアドレスを10.10.10.10、ネットマスクを255.255.255.0（24）、ゲートウェイアドレスを10.10.10.1に設定する例を示します。

クムルス**4.4.x**

次に、Cumulus 4.4.xを実行しているスイッチにホスト名、IPアドレス、ネットマスク、およびゲートウェイを設定する例を示します。

```
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:~$
```

Cumulus 5.4.x以降

次に、Cumulus 5.4.xを実行しているスイッチにホスト名、IPアドレス、ネットマスク、およびゲートウェイを設定する例を示します。以降が必要です。

```
cumulus@cumulus:mgmt:~$ nv set system hostname IP_switch_A_1

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip address
10.0.10.10/24

cumulus@cumulus:mgmt:~$ nv set interface eth0 ip gateway 10.10.10.1

cumulus@cumulus:mgmt:~$ nv config apply

cumulus@cumulus:mgmt:~$ nv config save
```

6. sudo rebootコマンドを使用してスイッチをリブートします。

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

スイッチがリブートしたら、の手順に従って新しい設定を適用できます NVIDIAのRCFファイルをダウンロードしてインストールします。

NVIDIA RCFファイルをダウンロードしてインストールします

MetroCluster IP構成の各スイッチにスイッチのRCFファイルを生成してインストールする必要があります。

作業を開始する前に

- コマンドへの「sudo」アクセス用のrootパスワードが必要です。
- スイッチソフトウェアがインストールされ、管理ネットワークが設定されている。
- 方法1または方法2のいずれかを使用して、スイッチを最初に設置する手順を実行しました。
- 初期インストール後に追加の設定を適用しなかった場合。

RCFファイルを適用する前にスイッチをリセットしたあとに以降の設定を実行する場合は、この手順 を使用できません。

このタスクについて

この手順は、MetroCluster IP構成（新規の設置）または交換用スイッチ（スイッチの交換）の各IPスイッチで実行する必要があります。

QSFP / SFP+アダプタを使用している場合は、ISLポートをブレークアウト速度モードではなくネイティブ速度モードで設定する必要があります。ISLポートの速度モードについては、スイッチベンダーのドキュメントを参照してください。

手順

1. MetroCluster IP用のNVIDIA RCFファイルを生成します。
   a. をダウンロードします "MetroCluster IP 用の RcfFileGenerator"。

b. RcfFileGenerator for MetroCluster IPを使用して、設定用のRCFファイルを生成します。

c. ホームディレクトリに移動します。「cumulus」として記録されている場合、ファイルパスは「/home/cumulus」です。

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

d. このディレクトリにRCFファイルをダウンロードします。 次に、SCPを使用してファイルをダウンロードする例を示します。 `SN2100_v2.0.0_IP_switch_A_1.txt` サーバ「50.50.50.50」からホームディレクトリに保存します。 `SN2100_v2.0.0_IP_switch_A_1.py`：

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_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:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. RCFファイルを実行します。RCFファイルでは、1つ以上の手順を適用するためのオプションが必要です。テクニカルサポートから指示がないかぎり、コマンドラインオプションを指定せずにRCFファイルを実行します。RCFファイルのさまざまな手順の完了ステータスを確認するには、オプション「-1」または「all」を使用してすべての（保留中の）手順を適用します。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_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 ...
```

3. 構成でDACケーブルを使用する場合は、スイッチポートでDACオプションを有効にします。

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0-X10_Switch-
A1.py runCmd <switchport> DacOption [enable | disable]
```

次に、ポートのDACオプションをイネーブルにする例を示します。 `swp7`：

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.00_Switch-A1.py
runCmd swp7 DacOption enable
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.00
    Running command: Enabling the DacOption for port swp7
    runCmd: 'nv set interface swp7 link fast-linkup on', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@IP_switch_A_1:mgmt:~$
```

4. スイッチポートでDACオプションを有効にしたら、スイッチをリブートします。

```
sudo reboot
```

> 複数のスイッチポートにDACオプションを設定する場合は、スイッチをリブートするだけで済みます。

25Gbps接続を使用するシステムの前方エラー修正の設定

25Gbps接続を使用するシステムの場合は、RCFの適用後に前方誤り訂正（FEC）パラメータを手動でoffに設定します。この設定はRCFでは適用されません。

このタスクについて

- このタスクは、25Gbps接続を使用するプラットフォームにのみ該当します。を参照してください "NVIDIAがサポートするSN2100 IPスイッチのプラットフォームポート割り当て"。
- このタスクは、 MetroCluster IP 構成の 4 つのスイッチすべてで実行する必要があります。
- 各スイッチポートは個別に更新する必要があります。コマンドで複数のポートまたはポート範囲を指定することはできません。

手順

1. 25Gbps接続を使用する最初のスイッチポートのパラメータをoffに設定し `fec`ます。

   ```
   sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport> fec off
   ```

2. コントローラモジュールに接続されている25Gbpsスイッチポートごとに、この手順を繰り返します。

MetroCluster IPインターフェイスのスイッチポート速度の設定

このタスクについて

- 次の手順を使用して、スイッチポート速度を100Gに設定します。
  - AFF A70、AFF A90、AFF A1K、AFF C80
  - AFF A30、AFF C30、AFF A50、AFF C60
  - FAS50、FAS70、FAS90
- 各スイッチポートは個別に更新する必要があります。コマンドで複数のポートまたはポート範囲を指定することはできません。

ステップ

1. 速度を設定するには、オプションを指定してRCFファイルを使用し `runCmd` ます。これにより、設定が適用され、設定が保存されます。

   次のコマンドは、MetroClusterインターフェイスおよびの速度を設定し `swp7` `swp8`ます。

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp7 speed 100
   ```

   ```
   sudo python3 SN2100_v2.20 _Switch-A1.py runCmd swp8 speed 100
   ```

   - 例 *

```
cumulus@Switch-A-1:mgmt:~$ sudo python3 SN2100_v2.20_Switch-A1.py runCmd
swp7 speed 100
[sudo] password for cumulus: <password>
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.20
    Running command: Setting switchport swp7 to 100G speed
    runCmd: 'nv set interface swp7 link auto-negotiate off', ret: 0
    runCmd: 'nv set interface swp7 link speed 100G', ret: 0
    runCmd: committed, ret: 0
    Completion: SUCCESS
cumulus@Switch-A-1:mgmt:~$
```

未使用の**ISL**ポートとポートチャネルを無効にする

NetAppでは、不要なヘルスアラートを回避するために、未使用のISLポートとポートチャネルを無効にすることを推奨します各ポートまたはポートチャネルを個別にディセーブルにする必要があります。コマンドで複数のポートまたはポート範囲を指定することはできません。

手順

1. RCFファイルのバナーを使用して、未使用のISLポートとポートチャネルを特定します。

> ポートがブレークアウトモードの場合は、コマンドで指定するポート名がRCFバナーに表示される名前と異なることがあります。RCFケーブル接続ファイルを使用してポート名を検索することもできます。

```
net show interface
```

2. RCFファイルを使用して、未使用のISLポートとポートチャネルを無効にします。

```
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:~$
```

次の例では、ポート「swp14」を無効にします。

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

特定された未使用のポートまたはポートチャネルごとに、この手順を繰り返します。

NVIDIA SN2100 MetroCluster IPスイッチ用のイーサネットスイッチヘルスモニター構成ファイルをインストールします。

NVIDIA イーサネット スイッチでイーサネット スイッチのヘルス モニタリングを構成するには、次の手順に従います。

これらの手順は、NVIDIA X190006-PEおよびX190006-PIスイッチが正しく検出されない場合に適用されます。これは、実行することで確認できます。 `system switch ethernet show`お使いのモデルに*OTHER*が表示されているかどうかを確認してください。NVIDIAスイッチのモデルを確認するには、コマンドで部品番号を検索してください。 `nv show platform hardware` NVIDIA CL 5.8以前または `nv show platform`それ以降のバージョンの場合。

以下のONTAPリリースでNVIDIA CL 5.11.xを使用する際に、ヘルスモニタリングとログ収集を意図したとおりに動作させたい場合にも、これらの手順を実行することをお勧めします。これらの手順を実行しなくてもヘルスモニタリングとログ収集は機能する可能性がありますが、実行することですべてが正しく動作することが保証されます。

- 9.10.1P20、9.11.1P18、9.12.1P16、9.13.1P8、9.14.1、9.15.1以降のパッチリリース

作業を開始する前に

- ONTAP クラスタが起動し、実行中であることを確認します。
- CSHM で利用可能なすべての機能を使用するには、スイッチで SSH を有効にします。
- すべてのノードでディレクトリをクリアし `/mroot/etc/cshm_nod/nod_sign/`ます。

a. ノードシェルに切り替えます。

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

b. advanced権限に切り替えます。

```
priv set advanced
```

c. ディレクトリ内の構成ファイルを一覧表示します `/etc/cshm_nod/nod_sign`。ディレクトリが存在し、構成ファイルが含まれている場合は、ファイル名がリストされます。

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

d. 接続されているスイッチモデルに対応する構成ファイルをすべて削除します。

不明な場合は、上記のサポートされているモデルのすべての構成ファイルを削除してから、それらの同じモデルの最新の構成ファイルをダウンロードしてインストールしてください。

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

a. 削除した構成ファイルがディレクトリに存在しないことを確認します。

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

手順

1. 対応するONTAPリリースバージョンに基づいて、イーサネットスイッチヘルスモニタ構成のzipファイルをダウンロードします。このファイルは、ページから入手でき "NVIDIAイーサネットスイッチ" ます。
   a. NVIDIA SN2100ソフトウェアのダウンロードページで、* Nvidia CSHMファイル*を選択します。
   b. [注意/必ずお読みください]ページで、同意するチェックボックスをオンにします。
   c. [End User License Agreement]ページで、同意するチェックボックスを選択し、*[Accept & Continue]*をクリックします。

d. Nvidia CSHM File - Download（Nvidia CSHMファイル-ダウンロード）ページで、適切な設定ファイルを選択します。次のファイルを使用できます。

ONTAP 9.15.1以降

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

ONTAP 9.11.1~9.14.1

- 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. 該当するzipファイルを内部Webサーバにアップロードします。
2. クラスタ内のいずれかのONTAPシステムからadvancedモード設定にアクセスします。

   「 advanced 」の権限が必要です

3. switch health monitor configureコマンドを実行します。

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

4. 使用しているONTAPのバージョンに応じて、コマンド出力の末尾が次のテキストになっていることを確認します。

ONTAP 9.15.1以降

イーサネットスイッチヘルスモニタに構成ファイルがインストールされました。

ONTAP 9.11.1~9.14.1

SHMは設定ファイルをインストールしました。

ONTAP 9.10.1

CSHMダウンロードパッケージが正常に処理されました。

エラーが発生した場合は、NetAppサポートにお問い合わせください。

1. を実行すると検出されたイーサネットスイッチヘルスモニタのポーリング間隔が最大2倍になるまで待って `system switch ethernet polling-interval show`から、次の手順を完了します。
2. コマンドを実行する `system switch ethernet configure-health-monitor show`ONTAPシステムで、監視対象フィールドが **True** に設定され、シリアル番号フィールドに **Unknown** が表示されていない状態でクラスタ スイッチが検出されていることを確認します。

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

構成ファイルを適用してもモデルに*その他*が表示される場合は、NetAppサポートにお問い合わせください。

参照 "システムスイッチイーサネットヘルスモニターの設定"詳細についてはコマンドを参照してください。

次の手順

"スイッチヘルス監視の設定"です。

著作権に関する情報

商標に関する情報