



# 設定**MetroCluster** 靜態IP交換器

## ONTAP MetroCluster

NetApp  
April 25, 2024

# 目錄

設定MetroCluster 靜態IP交換器 .....	1
設定Broadcom IP交換器 .....	1
設定Cisco IP交換器 .....	18
設定NVIDIA IP SN2100交換器 .....	38
設定 MetroCluster IP 交換器以進行健全狀況監控 .....	47

# 設定MetroCluster 靜態IP交換器

## 設定Broadcom IP交換器

您必須設定Broadcom IP交換器作為叢集互連和後端MetroCluster 的靜態IP連線。



您的組態在下列情況下需要額外授權（6個100-GB連接埠授權）：

- 您使用連接埠53和54做為40-Gbps或100-Gbps MetroCluster 的支援。
- 您所使用的平台將本機叢集和MetroCluster 功能區介面連接至連接埠49 - 52。

### 將Broadcom IP交換器重設為原廠預設值

在安裝新的交換器軟體版本和RCFs之前、您必須清除Broadcom交換器設定並執行基本組態。

#### 關於這項工作

- 您必須在MetroCluster 各個採用EIP組態的IP交換器上重複這些步驟。
- 您必須使用序列主控台連線至交換器。
- 此工作會重設管理網路的組態。

#### 步驟

1. 變更為提升命令提示字元（`#`）：「enable」

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

2. 清除啟動組態並移除橫幅

- a. 清除啟動組態：

「**erase**啟動組態」

```
(IP_switch_A_1) #erase startup-config

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

(IP_switch_A_1) #
```

此命令不會清除橫幅。

- b. 移除橫幅：

「**no set clibanner**」

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

3. 重新啟動交換器：(ip\_switch\_a\_1) #reboot

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



如果系統在重新載入交換器之前詢問是否要儲存未儲存或變更的組態、請選取\*否\*。

4. 等待交換器重新載入、然後登入交換器。

預設使用者為「admin」、未設定密碼。畫面會顯示類似下列的提示：

```
(Routing)>
```

5. 變更為提高權限的命令提示字元：

「啟用」

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

6. 將服務連接埠傳輸協定設為「無」：

'無服務傳輸協定'

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

(Routing) #
```

7. 將IP位址指派給服務連接埠：

「erviceport ip *ip-addressnetaskgateway*」

以下範例顯示指派IP位址「10.10.10.10」的服務連接埠、子網路為「255・255・255・0」、閘道為「10・10・10」：

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

## 8. 確認服務連接埠設定正確：

「How ServicePort」

下列範例顯示連接埠已啟動、且已指派正確的位址：

```
(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:bdf: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. 如有需要、請設定SSH伺服器。



RCF檔案會停用Telnet傳輸協定。如果您未設定SSH伺服器、則只能使用序列連接埠連線存取橋接器。

### a. 產生RSA金鑰。

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

### b. 產生DSA金鑰 (選用)

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

### c. 如果您使用的是FIPS相容版本的EFOS、請產生ECDSA金鑰。以下範例建立長度為 521 的金鑰。有效值為256、384或521。

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

d. 啟用SSH伺服器。

如有必要、請結束組態內容。

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

+



如果金鑰已經存在、系統可能會要求您覆寫金鑰。

10. 如有需要、請設定網域和名稱伺服器：

設定

以下範例顯示「IP網域」和「IP名稱伺服器」命令：

```
(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. 如有需要、請設定時區和時間同步（SNTP）。

以下範例顯示「shntp」命令、指定SNTP伺服器的IP位址和相對時區。

```
(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) #
```

若為 EFOS 3.10.0.3 版及更新版本、請使用 ntp 命令、如下列範例所示：

```
> (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. 設定交換器名稱：

「主機名稱ip\_switch\_a\_1」

交換器提示會顯示新名稱：

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. 儲存組態：

寫入記憶體

您會收到類似下列範例的提示和輸出：

```
(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. 在其他三個MetroCluster 交換器上重複上述步驟、以進行REIP組態設定。

## 下載並安裝Broadcom交換器EFOS軟體

您必須將交換器作業系統檔案和RCF檔案下載到MetroCluster 各個交換器、使其採用EWIP組態。

關於這項工作

此工作必須在MetroCluster 每個交換器上重複執行、且必須採用EIP組態。

請注意下列事項：

- 從EFOS 3.4.x.x升級至EFOS 3.7.x.x或更新版本時、交換器必須執行EFOS 3.4.4.6（或更新版本3.4.x.x）。如果您執行之前的版本、請先將交換器升級至EFOS 3.4.4.6（或更新版本3.4.x.x）、然後將交換器升級至EFOS 3.7.x.x或更新版本。
- EFOS 3.4.x.x和3.7.x.x或更新版本的組態不同。若要將EFOS版本從3.4.x.x變更為3.7.x.x或更新版本、或將其變更為3.7.x.x或更新版本、必須將交換器重設為原廠預設值、並套用對應EFOS版本的RCF檔案（重新）。此程序需要透過序列主控台連接埠存取。
- 從EFOS 3.7.x.x或更新版本開始、我們提供不符合FIPS標準的版本、以及符合FIPS標準的版本。從非FIPS相容的版本移至FIPS相容的版本時、會套用不同的步驟、反之亦然。將EFOS從非FIPS相容的版本變更為FIPS相容的版本、反之亦然、會將交換器重設為原廠預設值。此程序需要透過序列主控台連接埠存取。

## 步驟

1. 使用「show FIPS STATUS」命令檢查您的EFOS版本是否符合FIPS標準或不符合FIPS標準。在下列範例中、「ip\_switch\_a\_1」使用FIPS相容的EFOS、而「ip\_switch\_a\_2」使用的是非FIPS相容的EFOS。

### 範例1



```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

## 範例2

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

IP_switch_A_2 #
```

## 2. 請使用下表來判斷您必須遵循的方法：

程序	目前的EFOS版本	全新EFOS版本	高階步驟
在兩個（非）FIPS相容版本之間升級EFOS的步驟	3.4.x.x	3.4.x.x	使用方法1安裝新的EFOS映像）會保留組態與授權資訊
3.4.4.6（或更新版本3.4.x.x）	3.7.x.x或更新版本不符合FIPS標準	使用方法1升級EFOS。將交換器重設為原廠預設值、並套用EFOS 3.7.x.x或更新版本的RCF檔案	3.7.x.x或更新版本不符合FIPS標準
3.4.4.6（或更新版本3.4.x.x）	使用方法1降級EFOS。將交換器重設為原廠預設值、並套用EFOS 3.4.x.x的RCF檔案	3.7.x.x或更新版本不符合FIPS標準	
使用方法1安裝新的EFOS映像。系統會保留組態與授權資訊	3.7.x.x或更新版本符合FIPS標準	3.7.x.x或更新版本符合FIPS標準	使用方法1安裝新的EFOS映像。系統會保留組態與授權資訊
從FIPS相容EFOS版本升級至/升級的步驟	不符合FIPS標準	符合FIPS標準	使用方法2安裝EFOS映像。交換器組態和授權資訊將會遺失。

- 方法1：[將軟體映像下載到備份開機分割區、以升級EFOS的步驟](#)
- 方法2：[使用ONIE OS安裝來升級EFOS的步驟](#)

將軟體映像下載到備份開機分割區、以升級**EFOS**的步驟

只有在兩個EFOS版本皆不相容於FIPS或兩個EFOS版本皆符合FIPS標準時、您才能執行下列步驟。



如果某個版本符合FIPS標準、而另一個版本不符合FIPS標準、請勿使用這些步驟。

#### 步驟

1. 將交換器軟體複製到交換器：「複製sftp://user@50.50.50.50 /交換器軟體/EFOS-3.4.6.stk備份」

在此範例中、EFOS -3.4.6.stk作業系統檔案會從SFTP伺服器複製到備份分割區、檔位為50.50.50。您需要使用TFTP/SFTP伺服器的IP位址、以及需要安裝的RCF檔案名稱。

```
(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. 在下次交換器重新開機時、將交換器設定為從備份分割區開機：

「開機系統備份」

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

(IP_switch_A_1) #
```

3. 確認新的開機映像在下一次開機時會處於作用中狀態：

## 「如何啟動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. 儲存組態：

寫入記憶體

```
(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. 重新啟動交換器：

"重裝"

```
(IP_switch_A_1) #reload
```

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

6. 等待交換器重新開機。



在極少數情況下、交換器可能無法開機。請依照 [使用ONIE OS安裝來升級EFOS的步驟](#) 以安裝新映像。

7. 如果您將交換器從EFOS 3.4.x.x變更為EFOS 3.7.x.x或反之、請遵循下列兩個程序來套用正確的組態（RCF）：

- a. [將Broadcom IP交換器重設為原廠預設值](#)
- b. [下載並安裝Broadcom RCF檔案](#)

8. 在靜態IP組態的其餘三個IP交換器上重複上述步驟MetroCluster。

### 使用ONIE OS安裝來升級EFOS的步驟

如果其中一個EFOS版本符合FIPS標準、而另一個EFOS版本不符合FIPS標準、您可以執行下列步驟。這些步驟可用於在交換器無法開機時、從ONIE安裝非FIPS或FIPS相容的EFOS 3.7.x.x映像。

#### 步驟

1. 將交換器開機至ONIE安裝模式。

在開機期間、當下列畫面出現時、請選取ONIE：

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

選取「ONIE」之後、交換器就會載入並顯示下列選項：

```

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

```

現在、交換器將會開機進入ONIE安裝模式。

## 2. 停止ONIE探索並設定乙太網路介面

出現下列訊息後、按下<enter>以叫用ONIE主控台：

```

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

```



ONIE探索將會繼續、訊息將會列印到主控台。

```

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

```

## 3. 設定乙太網路介面、然後使用「ifconfigeth0 <ipaddress> netmask> up」和「route add default gW <gatewayAddress>」新增路由

```

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

```

## 4. 確認裝載ONIE安裝檔案的伺服器可連線：

```

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. 安裝新的交換器軟體

```

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.

```

軟體將會安裝、然後重新啟動交換器。讓交換器正常重新開機至新的EFOS版本。

## 6. 確認已安裝新的交換器軟體

### 「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. 完成安裝

交換器將在未套用組態的情況下重新開機、然後重設為原廠預設值。請依照下列兩份文件所述的兩個程序來設定交換器基本設定並套用RCF檔案：

- a. 設定交換器基本設定。請遵循步驟4及更新版本：[將Broadcom IP交換器重設為原廠預設值](#)
- b. 建立並套用RCF檔案、如所述 [下載並安裝Broadcom RCF檔案](#)

### 下載並安裝Broadcom RCF檔案

您必須將交換器RCF檔案下載並安裝到MetroCluster 各個交換器、以供採用此功能的介面IP組態。

#### 開始之前

此工作需要檔案傳輸軟體、例如FTP、TFTP、SFTP或scp。將檔案複製到交換器。

#### 關於這項工作

這些步驟必須重複執行MetroCluster 於各個採用EIP組態的IP交換器上。

共有四個RCF檔案、MetroCluster 每個檔案分別對應於整個EIP組態中的四個交換器。您必須針對所使用的交換器機型使用正確的RCF檔案。

交換器	RCF檔案
ip_switch_a_1.	v1.32_Switch-A1.txt
ip_switch_a_2	v1.32_Switch-A2.txt
IP交換器_B_1	v1.32_Switch-B1.txt
IP交換器_B_2	v1.32_Switch-B2.txt



EFOS 3.4.4.6版或更新版本3.4.x.x的RCF檔案版本與EFOS版本3.7.0.4不同。您必須確定已針對交換器執行的EFOS版本建立正確的RCF檔案。

EFOS版本	RCF檔案版本
3.4.x.x	v1.3x、v1.4x
3.7.x.x	v2.x

#### 步驟

1. 產生Broadcom RCF檔案MetroCluster 以利知識IP。
  - a. 下載 "[RcfFileGeneratorfor MetroCluster EflP](#)"
  - b. 使用RcfFileGeneratorfor MetroCluster EIP、為您的組態產生RCF檔案。



不支援下載後修改RCF檔案。

## 2. 將RCF檔案複製到交換器：

- a. 將RCF檔案複製到第一個交換器：「copy sftp://user@ft-server\_ip-address/rcfFiles/switch-specific-rCF/BES-53248\_v1.32\_Switch-A1.txt nvRAv:script bes-53241\_v1.32\_switch-a1.scr」

在此範例中、「Bes-53241\_v1.32\_Switch-a1.txt」RCF檔案會從SFTP伺服器複製到本機BootFlash、路徑為「50.50.50.50」。您需要使用TFTP/SFTP伺服器的IP位址、以及需要安裝的RCF檔案名稱。



```

(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. 確認RCF檔案已儲存為指令碼：

《記錄清單》

```
(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. 套用RCF指令碼：

「說明」 套用B2-53241\_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. 儲存組態：

## 寫入記憶體

```
(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. 重新啟動交換器：

"重裝"

```
(IP_switch_A_1) #reload

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

### a. 對其他三個交換器重複上述步驟、請務必將相符的RCF檔案複製到對應的交換器。

## 3. 重新載入交換器：

"重裝"

```
IP_switch_A_1# reload
```

## 4. 在其他三個MetroCluster 交換器上重複上述步驟、以進行REIP組態設定。

## 停用未使用的 ISL 連接埠和連接埠通道

NetApp 建議停用未使用的 ISL 連接埠和連接埠通道、以避免不必要的健全狀況警示。

### 1. 使用 RCF 檔案橫幅識別未使用的 ISL 連接埠和連接埠通道：



如果連接埠處於中斷連線模式、則您在命令中指定的連接埠名稱可能與 RCF 橫幅中指定的名稱不同。您也可以使用 RCF 纜線檔案來尋找連接埠名稱。

以取得 **ISL** 連接埠詳細資料

執行命令 `show port all`。

以取得連接埠通道詳細資料

執行命令 `show port-channel all`。

## 2. 停用未使用的 ISL 連接埠和連接埠通道。

您必須針對每個識別出的未使用連接埠或連接埠通道執行下列命令。

```
(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
```

# 設定Cisco IP交換器

## 設定Cisco IP交換器

您必須設定Cisco IP交換器作為叢集互連和後端MetroCluster 的靜態IP連線。

關於這項工作

本節中的幾個程序是獨立的程序、您只需要執行您被導向或與您的工作相關的程序。

### 將Cisco IP交換器重設為原廠預設值

在安裝任何RCF檔案之前、您必須先清除Cisco交換器組態並執行基本組態。如果您想在先前的安裝失敗之後重新安裝相同的RCF檔案、或是想要安裝新版RCF檔案、則需要執行此程序。

關於這項工作

- 您必須在MetroCluster 各個採用EIP組態的IP交換器上重複這些步驟。
- 您必須使用序列主控台連線至交換器。
- 此工作會重設管理網路的組態。

步驟

#### 1. 將交換器重設為原廠預設值：

##### a. 清除現有組態：

寫擦除

b. 重新載入交換器軟體：

"重裝"

系統會重新開機並進入組態精靈。在開機期間、如果出現「Abort Auto Provisioning and Continue with normalSetup（中止自動資源配置並繼續正常設定）」提示訊息、（是/否）[n]」、您應該回應「是」以繼續。

c. 在組態精靈中、輸入基本的交換器設定：

- 管理密碼
- 交換器名稱
- 頻外管理組態
- 預設閘道
- SSH服務（RSA）

完成組態精靈之後、交換器會重新開機。

d. 出現提示時、輸入使用者名稱和密碼以登入交換器。

以下範例顯示設定交換器時的提示和系統回應。角括弧（「<」）會顯示您輸入資訊的位置。

```
---- 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.
```

您可以在下一組提示中輸入基本資訊、包括交換器名稱、管理位址和閘道、然後選取SSH with RSA。

```

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]:

```

最後一組提示會完成組態設定：

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. 儲存組態：

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

## 3. 重新啟動交換器、然後等待交換器重新載入：

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

## 4. 在其他三個MetroCluster 交換器上重複上述步驟、以進行REIP組態設定。

## 下載並安裝Cisco交換器NX-OS軟體

您必須將交換器作業系統檔案和RCF檔案下載到MetroCluster 各個交換器、使其採用EWIP組態。

關於這項工作

此工作需要檔案傳輸軟體、例如FTP、TFTP、SFTP或scp。將檔案複製到交換器。

這些步驟必須重複執行MetroCluster 於各個採用EIP組態的IP交換器上。

您必須使用支援的交換器軟體版本。

### "NetApp Hardware Universe"

#### 步驟

1. 下載支援的NX-OS軟體檔案。

#### "Cisco軟體下載"

2. 將交換器軟體複製到交換器：

「copy sftp://root@server-ip-address/tftpboot/NX-os-name-name bootflash: VRF管理」

在此範例中、nxos.7.0.3.I4.6.bin檔案會從SFTP伺服器10.10.99.99複製到本機bootflash：

```
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. 在每個交換器上、確認交換器NX-OS檔案是否存在於每個交換器的bootflash目錄中：

《Dir bootflash:》

下列範例顯示檔案存在於ip\_switch\_a\_1上：



```

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. 安裝交換器軟體：

「安裝所有nxos bootflash:nxos.version、number.bin」

交換器軟體安裝完成後、交換器會自動重新載入（重新開機）。

下列範例顯示在ip\_switch\_a\_1上安裝軟體：

```

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. 等待交換器重新載入、然後登入交換器。

交換器重新開機後、會顯示登入提示：

```
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. 驗證是否已安裝交換器軟體：+「show version」（顯示版本）

下列範例顯示輸出：

```

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. 在靜態IP組態的其餘三個IP交換器上重複上述步驟MetroCluster。

#### 下載並安裝Cisco IP RCF檔案

您必須將RCF檔案下載MetroCluster 到各個交換器、以供使用。

#### 關於這項工作

此工作需要檔案傳輸軟體、例如FTP、TFTP、SFTP或scp。將檔案複製到交換器。

這些步驟必須重複執行MetroCluster 於各個採用EIP組態的IP交換器上。

您必須使用支援的交換器軟體版本。

"NetApp Hardware Universe"

共有四個RCF檔案、MetroCluster 每個檔案分別對應於整個EIP組態中的四個交換器。您必須針對所使用的交換器機型使用正確的RCF檔案。

交換器	RCF檔案
ip_switch_a_1.	NX3232_v1.80_Switch-A1.txt
ip_switch_a_2	NX3232_v1.80_Switch-A2.txt
IP交換器_B_1	NX3232_v1.80_Switch-B1.txt
IP交換器_B_2	NX3232_v1.80_Switch-B2.txt

步驟

- 1. 下載MetroCluster 《RCF》 檔案。



不支援下載後修改RCF檔案。

- 2. 將RCF檔案複製到交換器：
  - a. 將RCF檔案複製到第一個交換器：

```
「copy sftp ://root@ft-server-ip-address/tftpboot/switch-specif-rf bootflash: VRF management」
```

在此範例中、NX3232\_v1.80\_Switch-A1.txt RCF檔案會從位於10.10.99.99的SFTP伺服器複製到本機bootflash。您必須使用TFTP/SFTP伺服器的IP位址、以及需要安裝的RCF檔案名稱。

```

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. 對其他三個交換器重複上一個子步驟、請務必將相符的RCF檔案複製到對應的交換器。

3. 在每個交換器上、確認每個交換器的bootflash目錄中都有RCF檔案：

《Dir bootflash:》

下列範例顯示檔案存在於ip\_switch\_a\_1上：

```

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. 在Cisco 3132Q-V和Cisco 3232C交換器上設定TCAM區域。



如果您沒有Cisco 3132Q-V或Cisco 3232C交換器、請跳過此步驟。

a. 在Cisco 3132Q-V交換器上、設定下列TCAM區域：

```
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. 在Cisco 3232C交換器上、設定下列TCAM區域：

```
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. 設定「TCAM區域」之後、請儲存組態並重新載入交換器：

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

5. 將相符的RCF檔案從本機bootFlash複製到每個交換器上的執行組態：

「copy bootflash : switch-specific-RCF.txt執行組態」

6. 將RCF檔案從執行中的組態複製到每個交換器的啟動組態：

「copy running-config startup-config」

您應該會看到類似下列的輸出：

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

7. 重新載入交換器：

"重裝"

```
IP_switch_A_1# reload
```

8. 在其他三個MetroCluster 交換器上重複上述步驟、以進行REIP組態設定。

## 針對使用**25-Gbps**連線的系統設定轉送錯誤修正

如果您的系統設定為使用25-Gbps連線、則在套用RCF檔案之後、您需要手動將轉送錯誤修正（FEC）參數設定為關閉。RCF檔案不套用此設定。

關於這項工作

在執行此程序之前、必須先連接25 Gbps連接埠的纜線。

"Cisco 3232C或Cisco 9336C交換器的平台連接埠指派"

此工作僅適用於使用25-Gbps連線的平台：

- 部分A300 AFF
- zhTW 8200 FAS
- 500f FAS
- VA250 AFF

這項工作必須在MetroCluster 整個4台交換器上執行、且必須採用「靜態IP」組態。

步驟

1. 將連接至控制器模組的每個25-Gbps連接埠的FEC參數設為「Off」（關）、然後將執行組態複製到啟動組態：
  - a. 進入組態模式：「config t」
  - b. 指定要設定的25-Gbps介面：「interface interface-ID」
  - c. 將FEC設為關：「FEC關」
  - d. 針對交換器上的每個25-Gbps連接埠、重複上述步驟。
  - e. 退出組態模式：「exit」

以下範例顯示交換器ip\_switch\_a\_1上的乙太網路1/25/1命令：

```
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. 在其他三個MetroCluster 交換器上重複上述步驟、以進行「靜態IP」組態設定。

停用未使用的 **ISL** 連接埠和連接埠通道

NetApp 建議停用未使用的 ISL 連接埠和連接埠通道、以避免不必要的健全狀況警示。

1. 識別未使用的 ISL 連接埠和連接埠通道：



## 「How介面簡介」

### 2. 停用未使用的 ISL 連接埠和連接埠通道。

您必須針對每個識別出的未使用連接埠或連接埠通道執行下列命令。

```
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.
```

## 在Cisco 9336C交換器上設定Macsec加密



MAC秒加密只能套用至WAN ISL連接埠。

### 在Cisco 9336C交換器上設定Macsec加密

您只能在站台之間執行的WAN ISL連接埠上設定Macsec加密。套用正確的RCF檔案之後、您必須設定Macsec。

#### MAC的授權要求

Macsec需要安全授權。如需Cisco NX-OS授權方案的完整說明、以及如何取得及申請授權、請參閱 "[Cisco NX-OS授權指南](#)"

#### 在MetroCluster 不支援的IP組態中啟用Cisco Macsec Encryption WAN ISL

您可以在MetroCluster WAN ISL上的Cisco 9336C交換器上啟用MAC加密功能、以利執行支援。

#### 步驟

##### 1. 進入全域組態模式：

###### 設定終端機

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

##### 2. 在裝置上啟用Macsec和MKA：

《F精選Macsec》（功能MAC秒）

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

3. 將執行組態複製到啟動組態：

「copy running-config startup-config」

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

## 設定Macsec金鑰鏈和金鑰

您可以在組態上建立Macsec金鑰鏈或金鑰。

### 金鑰存留期與無中斷金鑰存留期

一個Macsec金鑰鏈可以有多個預先共用金鑰（PSK）、每個金鑰都設定有金鑰ID和選用的存留期。金鑰存留期指定金鑰啟動和過期的時間。如果沒有生命週期組態、則預設的生命週期是無限的。設定存留期後、MKA會在金鑰鏈中的下一個已設定的預先共用金鑰過期後、再繼續使用。金鑰的時區可以是本機或UTC。預設時區為UTC。如果您設定第二個金鑰（在金鑰鏈中）、並設定第一個金鑰的生命週期、金鑰就可以在同一個金鑰鏈內捲動到第二個金鑰。當第一個金鑰的存留期到期時、它會自動移至清單中的下一個金鑰。如果在連結的兩側同時設定相同的金鑰、則金鑰轉換是無雜訊的（也就是金鑰在不中斷流量的情況下自動移轉）。

### 步驟

1. 進入全域組態模式：

設定終端機

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

2. 若要隱藏加密金鑰字節字串、請在「show running-config」和「show startup-config」命令的輸出中、以萬用字元取代字串：

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



當您將組態儲存至檔案時、也會隱藏八位元字串。

根據預設、系統會以加密格式顯示PSKs金鑰、並可輕鬆解密。此命令僅適用於Macsec金鑰鏈。

3. 建立一組Macsec金鑰鏈以保留一組Macsec金鑰、然後進入Macsec金鑰鏈組態模式：

金鑰鏈名稱Macsec

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

4. 建立Macsec金鑰並進入Macsec金鑰組態模式：

「key key-id」

範圍為1到32個六位數的金鑰字串、最大大小為64個字元。

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

5. 設定金鑰的八位元組字串：

「key字節字節字串字節字節字串密碼編譯演算法AES-122\_CMAC | AES-256\_CMAC」

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



八位元字串引數最多可包含64個十六進位字元。八位元組金鑰是內部編碼的、因此純文字中的金鑰不會出現在「show running-config Macsec」命令的輸出中。

6. 設定金鑰的傳送壽命（以秒為單位）：

「終止生命週期開始時間持續時間」

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

依預設、裝置會將開始時間視為UTC。start-time引數是金鑰成為作用中的時間和日期。duration引數是以秒為單位的壽命長度。最大長度為2147483646秒（約68年）。

7. 將執行組態複製到啟動組態：

「copy running-config startup-config」

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

8. 顯示Keychain組態：

「如何輸入金鑰鏈名稱」

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

## 設定Macsec原則

### 步驟

1. 進入全域組態模式：

#### 設定終端機

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

2. 建立Macsec原則：

#### "Malaccec"原則名稱

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

3. 設定下列其中一個密碼：GCM-AES-128、GCM-AES-256、GCM-AES-XPB-128或GCM-AES-XPB-256：

#### 「密碼套件名稱」

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

4. 設定金鑰伺服器優先順序、以便在金鑰交換期間打破對等端點之間的關聯：

#### 「金鑰伺服器優先順序編號」

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

5. 設定安全性原則以定義資料處理和控制封包：

#### 「安全性原則」

從下列選項中選擇安全原則：

- 「必須安全」：不包含Macsec標頭的封包會被丟棄
- 應予保護：允許不含Macsec標頭的封包（這是預設值）

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

6. 設定重播保護視窗、使安全介面不接受小於設定視窗大小的封包：「視窗大小數字」



重播保護視窗大小代表Macsec接受且不捨棄的最大不連續框架數。範圍從0到596000000。

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

7. 設定強制SAK重新輸入的時間（以秒為單位）：

「過期時間」

您可以使用此命令將工作階段金鑰變更為可預測的時間間隔。預設值為0。

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

8. 在第2層框架中設定下列其中一項機密偏移、以開始加密：

「conf-offsetconfidentiality offset」

從下列選項中選擇：

- 會議偏移量為0。
- 會議偏移量：30。
- 會議偏移量-50。

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



中繼交換器可能需要使用此命令、才能像MPLS標記一樣使用封包標頭（DMAC、SMAC、etype）。

9. 將執行組態複製到啟動組態：

「copy running-config startup-config」

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

10. 顯示Macsec原則組態：

「How Macsec Policy」

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

在介面上啟用**Cisco Macsec**加密

1. 進入全域組態模式：

設定終端機

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

2. 選取您使用Macsec加密設定的介面。

您可以指定介面類型和身分識別。對於乙太網路連接埠、請使用乙太網路插槽/連接埠。

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

3. 新增要在介面上設定的金鑰鏈和原則、以新增Macsec組態：

"Malaccec keychain keychain keychain name policy police-name"

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

4. 在所有要設定Macsec加密的介面上重複步驟1和2。

5. 將執行組態複製到啟動組態：

「copy running-config startup-config」

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

在**MetroCluster** 不穩定的IP組態中停用**Cisco Macsec Encryption WAN ISL**

您可能需要在MetroCluster WAN ISL上針對Cisco 9336C交換器停用MAC加密、以利進行IP組態設定。

步驟

1. 進入全域組態模式：

設定終端機

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

2. 停用裝置上的Macsec組態：

## "Malaccec"關機

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



選取「no」選項可還原Macsec功能。

### 3. 選取您已使用Macsec設定的介面。

您可以指定介面類型和身分識別。對於乙太網路連接埠、請使用乙太網路插槽/連接埠。

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

### 4. 移除介面上設定的金鑰鏈和原則、以移除Macsec組態：

「沒有Macsec keychain keychain名稱policy原則名稱」

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

### 5. 在所有設定了Macsec的介面上重複步驟3和4。

### 6. 將執行組態複製到啟動組態：

「copy running-config startup-config」

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

## 驗證Macsec組態

### 步驟

1. 在組態內的第二個交換器上重複\*全部\*先前的程序、以建立一個Macsec工作階段。
2. 執行下列命令、確認兩台交換器都已成功加密：
  - a. RUN：「How Macsec mka Summary」
  - b. RUN：「How Macsec mka工作階段」
  - c. RUN：「How Macsec mka Statistics」

您可以使用下列命令來驗證Macsec組態：

命令	顯示有關...的資訊
「How Macsec mka工作階段介面類型/連接埠編號」	特定介面或所有介面的Macsec MKA工作階段

「如何輸入金鑰鍵名稱」	金鑰鍵組態
「MAC的摘要」	Macsec MKA組態
「How Macsec policy police-name」 （如何設定MAC原則名稱）	特定Macsec原則或所有Macsec原則的組態

## 設定NVIDIA IP SN2100交換器

您必須設定NVIDIA SN2100 IP交換器作為叢集互連和後端MetroCluster 的SIP連線。

### [Reset-the switch]將NVIDIA IP SN2100交換器重設為原廠預設值

您可以選擇下列方法、將交換器重設為原廠預設值。

- [使用RCF檔案選項重設交換器](#)
- [使用Cumulus安裝選項重設交換器](#)

#### 使用RCF檔案選項重設交換器

在安裝新的RCF組態之前、您必須還原NVIDIA交換器設定。

#### 關於這項工作

若要將交換器還原為預設設定、請使用「restoreDefaults」選項來執行RCF檔案。此選項會將原始備份檔案複製到原始位置、然後重新啟動交換器。重新開機之後、交換器會與您第一次執行RCF檔案來設定交換器時的原始組態一起上線。

下列組態詳細資料不會重設：

- 使用者與認證組態
- 管理網路連接埠eth0的組態



在應用RCF檔案期間發生的所有其他組態變更、都會還原為原始組態。

#### 開始之前

- 您必須根據設定交換器 [下載並安裝NVIDIA RCF檔案](#)。如果您尚未以這種方式設定、或是在執行RCF檔案之前已設定其他功能、則無法使用此程序。
- 您必須在MetroCluster 各個採用EIP組態的IP交換器上重複這些步驟。
- 您必須使用序列主控台連線連接至交換器。
- 此工作會重設管理網路的組態。

#### 步驟

1. 確認RCF組態已成功套用至相同或相容的RCF檔案版本、而且備份檔案已存在。





輸出內容可以顯示備份檔案、保留檔案或兩者。如果輸出中沒有出現備份檔案或保留的檔案、您就無法使用此程序。

```
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. 使用選項執行RCF檔案以還原預設值：「恢復預設值」

```
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. 對提示回應「是」。交換器會還原為原始組態並重新開機。

4. 等待交換器重新開機。

交換器會重設並保留初始組態、例如管理網路組態和目前認證、然後再套用RCF檔案。重新開機之後、您可以使用相同或不同版本的RCF檔案來套用新組態。

### 使用Cummuls安裝選項重設交換器

關於這項工作

如果您想要套用Cummuls映像來完全重設交換器、請使用這些步驟。

開始之前

- 您必須使用序列主控台連線連接至交換器。
- 可透過HTTP存取Cummulis交換器軟體映像。



如需安裝 Cumulus Linux 的詳細資訊、請參閱 "[NVIDIA SN2100交換器的安裝與組態總覽](#)"

- 您必須擁有root密碼才能存取命令。

步驟

1. 從Cummulo主控台下載交換器軟體、然後使用命令「onie-install -A -i」排入安裝佇列、接著再輸入交換器軟體的檔案路徑：

在此範例中、會將韌體檔案「累計至Linux -4.4.2-mlx-amd64.bin」從HTTP伺服器「50.50.50」複製到本機交換器。

```
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. 在下載並驗證映像時、請回應提示「y」以確認安裝。
3. 重新啟動交換器以安裝新軟體：「Udo reboot...」

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



交換器會重新開機並進入交換器軟體安裝、這需要一些時間。安裝完成後、交換器會重新開機、並保持「登入」提示。

#### 4. 設定基本交換器設定

- a. 當交換器開機並出現登入提示時、請登入並變更密碼。



使用者名稱為「累計」、預設密碼為「累計」。

```
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. 設定管理網路介面。



以下範例說明如何使用命令設定主機名稱 (ip\_switch\_a\_1)、IP位址 (10.10.10.10)、網路遮罩 (255 · 255 · 255 · 255 · 0 (24)) 和閘道 (10 · 10 · 10)：「net add hostname>」、「net add interface eth0 ip address<IPAddress/mask>」、「net add interface eth0 ip gateway <gateway>」（網路新增介面eth0 IP閘道<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. 使用「show reboot」命令重新啟動交換器。

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

當交換器重新開機時、您可以使用中的步驟套用新的組態 [下載並安裝NVIDIA RCF檔案](#)。

## [[Download-and -install]]下載並安裝NVIDIA RCF檔案

您必須將交換器RCF檔案下載並安裝到MetroCluster 各個交換器、以供採用此功能的介面IP組態。

開始之前

- 您必須擁有root密碼才能存取命令。
- 交換器軟體已安裝且管理網路已設定完成。

- 您依照步驟、使用方法1或方法2開始安裝交換器。
- 初始安裝之後、您並未套用任何其他組態。



如果您在重設交換器之後以及套用RCF檔案之前執行進一步的組態、則無法使用此程序。

#### 關於這項工作

您必須在MetroCluster 各個IP交換器上重複上述步驟（全新安裝）或更換交換器（更換交換器）。

#### 步驟

##### 1. 產生NVIDIA RCF檔案MetroCluster 以利知識IP。

- 下載 "[RcfFileGeneratorfor MetroCluster EfiP](#)"。
- 使用RcfFileGeneratorfor MetroCluster EsciP、為您的組態產生RCF檔案。
- 瀏覽至您的主目錄。如果您記錄為「累計」、則檔案路徑為「home/gumulus」。

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

- 將RCF檔案下載至此目錄。以下範例顯示、您可以使用scp將檔案「M f2 2100 v1.0」\_ip\_switch\_a\_1.txt' 從伺服器「50、50」下載到您的主目錄、並將其儲存為「M f2 2100、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:~$
```

- 執行RCF檔案。RCF檔案需要選項才能套用一或多個步驟。除非技術支援人員指示、否則請在不使用命令列選項的情況下執行RCF檔案。若要驗證RCF檔案各個步驟的完成狀態、請使用選項「-1」或「ALL」來套用

所有（擱置中）步驟。

```
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 ...
```

## 停用未使用的 ISL 連接埠和連接埠通道

NetApp 建議停用未使用的 ISL 連接埠和連接埠通道、以避免不必要的健全狀況警示。

1. 使用 RCF 檔案橫幅識別未使用的 ISL 連接埠和連接埠通道：



如果連接埠處於中斷連線模式、則您在命令中指定的連接埠名稱可能與 RCF 橫幅中指定的名稱不同。您也可以使用 RCF 纜線檔案來尋找連接埠名稱。

```
net show interface
```

2. 使用 RCF 檔案停用未使用的 ISL 連接埠和連接埠通道。



```

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:~$

```

下列範例命令會停用連接埠 "swp14"：

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

針對每個識別出未使用的連接埠或連接埠通道重複此步驟。

## 設定 MetroCluster IP 交換器以進行健全狀況監控

在 MetroCluster IP 組態中、您可以設定 SNMPv3 來監控 IP 交換器的健全狀況。

## 步驟 1：在 **MetroCluster IP** 交換器上設定 **SNMPv3** 使用者

請使用下列步驟在 MetroCluster IP 交換器上設定 SNMPv3 使用者。



您必須在命令中同時使用驗證和隱私權通訊協定。不支援不使用隱私權的驗證。

## 適用於 **Broadcom IP** 交換器

### 步驟

1. 如果「network-admin」使用者群組尚未存在、請建立：

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

2. 確認已建立「network-admin」群組：

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

3. 在 Broadcom IP 交換器上設定 SNMPv3 使用者：

```
(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>"
```

您必須在驗證和隱私權密碼上使用引號、如下列範例所示：

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

## 適用於 **Cisco IP** 交換器

### 步驟

1. 執行下列命令、在 Cisco IP 交換器上設定 SNMPv3 使用者：

```
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. 驗證是否已在交換器上設定 SNMPv3 使用者：

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

以下輸出範例顯示使用者 admin 已針對 SNMPv3 進行設定：

```
IP_switch_A_1(config)# show snmp user admin
User          Auth          Priv(enforce) Groups
acl_filter
_____
_____
admin          md5          aes-128(no)  network-admin
```

## 步驟 2：在 ONTAP 中設定 SNMPv3 使用者

請使用下列步驟在 ONTAP 中設定 SNMPv3 使用者。

1. 在 ONTAP 中設定 SNMPv3 使用者：

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

2. 設定交換器健全狀況監控、以使用新的 SNMPv3 使用者監控交換器：

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

3. 驗證將使用新建立的 SNMPv3 使用者監控的裝置序號是否正確：

- a. 顯示交換器健全狀況監控輪詢時間：

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

- b. 在輪詢時間結束後執行下列命令：

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

## 版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

## 商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。