



Configurare gli switch IP di MetroCluster

ONTAP MetroCluster

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/it-it/ontap-metrocluster/install-ip/task_install_and_cable_the_mcc_components.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Configurare gli switch IP di MetroCluster	1
Scegli la procedura corretta di configurazione dello switch IP MetroCluster	1
Configurare gli switch IP Broadcom per l'interconnessione del cluster e la connettività IP MetroCluster backend	1
Ripristino delle impostazioni predefinite dello switch IP Broadcom	1
Download e installazione del software EFOS dello switch Broadcom	6
Download e installazione dei file RCF Broadcom	14
Disattivare le porte e i canali delle porte ISL non utilizzati	18
Configurare gli switch IP Cisco	19
Configurare gli switch IP Cisco per l'interconnessione del cluster e la connettività IP MetroCluster back-end	19
Configurare la crittografia MACsec sugli switch Cisco 9336C in un sito IP MetroCluster	34
Configurare gli switch NVIDIA IP	41
Configurare lo switch NVIDIA IP SN2100 per l'interconnessione del cluster e la connettività IP MetroCluster backend	41
Installa il file di configurazione Ethernet Switch Health Monitor per uno switch IP NVIDIA SN2100 MetroCluster	54

Configurare gli switch IP di MetroCluster

Scegli la procedura corretta di configurazione dello switch IP MetroCluster

È necessario configurare gli switch IP per fornire connettività MetroCluster IP back-end. La procedura da seguire dipende dal fornitore dello switch.

- ["Configurare gli switch IP Broadcom"](#)
- ["Configurare gli switch IP Cisco"](#)
- ["Configurare gli switch NVIDIA IP"](#)

Configurare gli switch IP Broadcom per l'interconnessione del cluster e la connettività IP MetroCluster backend

È necessario configurare gli switch IP Broadcom per l'utilizzo come interconnessione del cluster e per la connettività IP MetroCluster back-end.



La configurazione richiede licenze aggiuntive (6 licenze per porte da 100 GB) nei seguenti scenari:

- Le porte 53 e 54 vengono utilizzate come ISL MetroCluster a 40 Gbps o 100 Gbps.
- Si utilizza una piattaforma che connette il cluster locale e le interfacce MetroCluster alle porte 49 - 52.

Ripristino delle impostazioni predefinite dello switch IP Broadcom

Prima di installare una nuova versione del software dello switch e gli RCF, è necessario cancellare le impostazioni dello switch Broadcom ed eseguire la configurazione di base.

A proposito di questa attività

- È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.
- È necessario essere collegati allo switch mediante la console seriale.
- Questa attività ripristina la configurazione della rete di gestione.

Fasi

1. Passare al prompt dei comandi con privilegi elevati (#): enable

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

2. Cancellare la configurazione di avvio e rimuovere il banner

- a. Cancellare la configurazione di avvio:

```
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) #
```

Questo comando non cancella il banner.

b. Rimuovere lo striscione:

```
no set clibanner
```

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

3. Riavviare lo switch:
(IP_switch_A_1) #reload

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



Se il sistema chiede se salvare la configurazione non salvata o modificata prima di ricaricare lo switch, selezionare **No**.

4. Attendere che lo switch si ricarichi, quindi accedere allo switch.

L'utente predefinito è “admin” e non è stata impostata alcuna password. Viene visualizzato un prompt simile al seguente:

```
(Routing) >
```

5. Passare al prompt dei comandi con privilegi elevati:

```
enable
```

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

6. Impostare il protocollo della porta di servizio su none:

```
serviceport protocol none
```

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

7. Assegnare l'indirizzo IP alla porta di servizio:

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

L'esempio seguente mostra un indirizzo IP assegnato alla porta di servizio "10.10.10.10" con la subnet "255.255.255.0" e il gateway "10.10.10.1":

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

8. Verificare che la porta di servizio sia configurata correttamente:

```
show serviceport
```

L'esempio seguente mostra che la porta è attiva e che sono stati assegnati gli indirizzi corretti:

```
(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. Configurare il server SSH.



- Il file RCF disattiva il protocollo Telnet. Se non si configura il server SSH, è possibile accedere al bridge solo utilizzando la connessione alla porta seriale.
- Per poter utilizzare la raccolta dei log e altri strumenti esterni è necessario configurare il server SSH.

a. Generare chiavi RSA.

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

b. Generare chiavi DSA (opzionale)

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

c. Se si utilizza la versione conforme a FIPS di EFOS, generare le chiavi ECDSA. Nell'esempio seguente vengono create le chiavi con una lunghezza di 521. I valori validi sono 256, 384 o 521.

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

d. Abilitare il server SSH.

Se necessario, uscire dal contesto di configurazione.

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

+



Se le chiavi sono già presenti, potrebbe essere richiesto di sovrascriverle.

10. Se lo si desidera, configurare il dominio e il server dei nomi:

configure

Nell'esempio riportato di seguito viene illustrato il ip domain e. ip name server comandi:

```
(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. Se lo si desidera, configurare il fuso orario e la sincronizzazione dell'ora (SNTP).

Nell'esempio riportato di seguito viene illustrato il sntp Che specifica l'indirizzo IP del server SNTP e il relativo fuso orario.

```
(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) #
```

Per EFOS versione 3.10.0.3 e successive, utilizzare `ntp` comando, come illustrato nell'esempio seguente:

```
> (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. Configurare il nome dello switch:

```
hostname IP_switch_A_1
```

Il prompt di switch visualizza il nuovo nome:

```
(Routing) # hostname IP_switch_A_1
(IP_switch_A_1) #
```

13. Salvare la configurazione:

```
write memory
```

Si ricevono messaggi e output simili al seguente esempio:

```
(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. Ripetere i passaggi precedenti sugli altri tre switch nella configurazione IP MetroCluster.

Download e installazione del software EFOS dello switch Broadcom

È necessario scaricare il file del sistema operativo dello switch e il file RCF su ciascun switch nella configurazione IP MetroCluster.

A proposito di questa attività

Questa attività deve essere ripetuta su ogni switch nella configurazione IP MetroCluster.

Nota:

- Quando si esegue l'aggiornamento da EFOS 3.4.x.x a EFOS 3.7.x.x o versioni successive, lo switch deve eseguire EFOS 3.4.4.6 (o versioni successive 3.4.x.x). Se si esegue una release precedente, aggiornare prima lo switch a EFOS 3.4.4.6 (o versione successiva 3.4.x.x), quindi aggiornare lo switch a EFOS 3.7.x.x o versione successiva.
- La configurazione per EFOS 3.4.x.x e 3.7.x.x o versioni successive è diversa. Se si modifica la versione di EFOS da 3.4.x.x a 3.7.x.x o successiva o viceversa, è necessario ripristinare le impostazioni predefinite dello switch e applicare nuovamente i file RCF per la versione di EFOS corrispondente. Questa procedura richiede l'accesso tramite la porta seriale della console.
- A partire dalla versione EFOS 3.7.x.x o successiva, è disponibile una versione non conforme a FIPS e una conforme a FIPS. Quando si passa da una versione non conforme a FIPS a una versione conforme a FIPS o viceversa, si applicano diverse procedure. Se si cambia EFOS da una versione non conforme a FIPS a una conforme a FIPS o viceversa, si ripristinano le impostazioni predefinite dello switch. Questa procedura richiede l'accesso tramite la porta seriale della console.

Fasi

1. Scaricare il firmware dello switch dal "[Sito di supporto Broadcom](#)".
2. Verificare che la versione di EFOS in uso sia conforme a FIPS o non conforme a FIPS utilizzando `show fips status` comando. Negli esempi seguenti, IP_switch_A_1 Utilizza EFOS conforme a FIPS e. IP_switch_A_2 Utilizza EFOS non conforme a FIPS.

Esempio 1

```
IP_switch_A_1 #show fips status
```

```
System running in FIPS mode
```

```
IP_switch_A_1 #
```

Esempio 2

```
IP_switch_A_2 #show fips status
```

```
^
```

```
% Invalid input detected at `^` marker.
```

```
IP_switch_A_2 #
```

3. Utilizzare la seguente tabella per determinare il metodo da seguire:

Procedura	Versione EFOS corrente	Nuova versione EFOS	Fasi di alto livello
Procedura per l'aggiornamento di EFOS tra due versioni (non) conformi a FIPS	3.4.x.x	3.4.x.x	Installare la nuova immagine EFOS utilizzando il metodo 1) le informazioni di configurazione e licenza vengono conservate
3.4.4.6 (o versione successiva 3.4.x.x)	3.7.x.x o versioni successive non conformi a FIPS	Aggiornare EFOS utilizzando il metodo 1. Ripristinare le impostazioni predefinite dello switch e applicare il file RCF per EFOS 3.7.x.x o versioni successive	3.7.x.x o versioni successive non conformi a FIPS
3.4.4.6 (o versione successiva 3.4.x.x)	Eseguire il downgrade di EFOS utilizzando il metodo 1. Ripristinare le impostazioni predefinite dello switch e applicare il file RCF per EFOS 3.4.x.x.	3.7.x.x o versioni successive non conformi a FIPS	

Installare la nuova immagine EFOS utilizzando il metodo 1. Le informazioni di configurazione e licenza vengono conservate	3.7.x.x o successivo conforme a FIPS	3.7.x.x o successivo conforme a FIPS	Installare la nuova immagine EFOS utilizzando il metodo 1. Le informazioni di configurazione e licenza vengono conservate
Procedura per l'aggiornamento a/da una versione EFOS conforme a FIPS	Non conforme a FIPS	Conforme a FIPS	Installazione dell'immagine EFOS con il metodo 2. La configurazione dello switch e le informazioni sulla licenza andranno perse.

- Metodo 1: [Procedura per l'aggiornamento di EFOS con il download dell'immagine software nella partizione di boot di backup](#)
- Metodo 2: [Procedura per aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE](#)

Procedura per l'aggiornamento di EFOS con il download dell'immagine software nella partizione di boot di backup

È possibile eseguire i seguenti passaggi solo se entrambe le versioni di EFOS non sono conformi a FIPS o se entrambe le versioni di EFOS sono conformi a FIPS.



Non seguire questa procedura se una versione è conforme a FIPS e l'altra non è conforme a FIPS.

Fasi

1. Copiare il software dello switch sullo switch: copy

```
sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup
```

In questo esempio, il file del sistema operativo efos-3.4.4.6.stk viene copiato dal server SFTP all'indirizzo 50.50.50.50 nella partizione di backup. È necessario utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

```
(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. Impostare lo switch per l'avvio dalla partizione di backup al successivo riavvio dello switch:

```
boot system backup
```

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

```
(IP_switch_A_1) #
```

3. Verificare che la nuova immagine di avvio sia attiva al prossimo avvio:

```
show bootvar
```

```
(IP_switch_A_1) #show bootvar
```

Image Descriptions

```
active :  
backup :
```

Images currently available on Flash

unit	active	backup	current-active	next-active
1	3.4.4.2	3.4.4.6	3.4.4.2	3.4.4.6

```
(IP_switch_A_1) #
```

4. Salvare la configurazione:

```
write memory
```

```
(IP_switch_A_1) #write memory
```

This operation may take a few minutes.

Management interfaces will not be available during this time.

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

Configuration Saved!

```
(IP_switch_A_1) #
```

5. Riavviare lo switch:

```
reload
```

```
(IP_switch_A_1) #reload
```

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

6. Attendere il riavvio dello switch.



In rari casi, lo switch potrebbe non avviarsi. Seguire la [Procedura per aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE](#) per installare la nuova immagine.

7. Se si cambia lo switch da EFOS 3.4.x.x a EFOS 3.7.x.x o viceversa, seguire le due procedure seguenti per applicare la configurazione corretta (RCF):
 - a. [Ripristino delle impostazioni predefinite dello switch IP Broadcom](#)
 - b. [Download e installazione dei file RCF Broadcom](#)
8. Ripetere questa procedura sui tre switch IP rimanenti nella configurazione IP MetroCluster.

Procedura per aggiornare EFOS utilizzando l'installazione del sistema operativo ONIE

Se una versione di EFOS è conforme a FIPS e l'altra non è conforme a FIPS, eseguire le seguenti operazioni. Questa procedura può essere utilizzata per installare l'immagine EFOS 3.7.x.x non conforme a FIPS o FIPS da ONIE in caso di mancato avvio dello switch.

Fasi

1. Avviare lo switch in modalità di installazione ONIE.

Durante l'avvio, selezionare ONIE quando viene visualizzata la seguente schermata:

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

Dopo aver selezionato "ONIE", lo switch si carica e presenta le seguenti opzioni:

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

Lo switch si avvia in modalità di installazione ONIE.

2. Interrompere il rilevamento ONIE e configurare l'interfaccia ethernet

Una volta visualizzato il seguente messaggio, premere Invio per richiamare la console ONIE:

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



Il rilevamento ONIE continua e i messaggi vengono stampati sulla console.

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

3. Configurare l'interfaccia ethernet e aggiungere il percorso utilizzando `ifconfig eth0 <ipAddress>` `netmask <netmask>` `up` e `route add default gw <gatewayAddress>`

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

4. Verificare che il server che ospita il file di installazione ONIE sia raggiungibile:

```

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. Installare il nuovo software dello switch

```

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.

```

Il software installerà e riavvierà lo switch. Lasciare che lo switch si riavvii normalmente nella nuova versione di EFOS.

6. Verificare che il nuovo software dello switch sia installato

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. Completare l'installazione

Lo switch si riavvia senza alcuna configurazione applicata e ripristina le impostazioni predefinite. Seguire le due procedure per configurare le impostazioni di base dello switch e applicare il file RCF come indicato nei due documenti seguenti:

- a. Configurare le impostazioni di base dello switch. Seguire i passaggi 4 e successivi: [Ripristino delle impostazioni predefinite dello switch IP Broadcom](#)
- b. Creare e applicare il file RCF come descritto in [Download e installazione dei file RCF Broadcom](#)

Download e installazione dei file RCF Broadcom

È necessario generare e installare il file RCF dello switch in ogni switch nella configurazione IP di MetroCluster.

Prima di iniziare

Questa attività richiede un software per il trasferimento dei file, ad esempio FTP, TFTP, SFTP o SCP, per copiare i file sui centralini.

A proposito di questa attività

Questa procedura deve essere ripetuta su ciascuno switch IP nella configurazione IP di MetroCluster.

Sono disponibili quattro file RCF, uno per ciascuno dei quattro switch nella configurazione IP di MetroCluster. È necessario utilizzare i file RCF corretti per il modello di switch in uso.

Switch	File RCF
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



File RCF per EFOS versione 3.4.4.6 o successiva 3.4.x.x. La release e la versione 3.7.0.4 di EFOS sono diverse. Assicurarsi di aver creato i file RCF corretti per la versione EFOS in esecuzione sullo switch.

Versione EFOS	Versione del file RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Fasi

1. Generare i file RCF Broadcom per l'IP MetroCluster.
 - a. Scaricare ["RcfFileGenerator per MetroCluster IP"](#)
 - b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.



Le modifiche apportate ai file RCF dopo il download non sono supportate.

2. Copiare i file RCF sugli switch:

- a. Copiare i file RCF sul primo switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

In questo esempio, il file RCF "BES-53248_v1.32_Switch-A1.txt" viene copiato dal server SFTP in "50.50.50.50" al bootflash locale. È necessario utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

```
(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. Verificare che il file RCF sia salvato come script:

```
script list
```

```
(IP_switch_A_1) #script list

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

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

c. Applicare lo script RCF:

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

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

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

```
config
```

```
set clibanner
```

```
*****
```

```
*****
```

```
* NetApp Reference Configuration File (RCF)
```

```
*
```

```
* Switch      : BES-53248
```

```
...
```

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

```
...
```

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

```
(IP_switch_A_1) #
```

d. Salvare la configurazione:

```
write memory
```

```
(IP_switch_A_1) #write memory

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

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

Configuration Saved!

(IP_switch_A_1) #
```

e. Riavviare lo switch:

```
reload
```

```
(IP_switch_A_1) #reload

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

- a. Ripetere i passaggi precedenti per ciascuno degli altri tre switch, assicurandosi di copiare il file RCF corrispondente sullo switch corrispondente.

3. Ricaricare lo switch:

```
reload
```

```
IP_switch_A_1# reload
```

4. Ripetere i passaggi precedenti sugli altri tre switch nella configurazione IP MetroCluster.

Disattivare le porte e i canali delle porte ISL non utilizzati

NetApp consiglia di disattivare le porte ISL e i canali delle porte inutilizzati per evitare avvisi di integrità non necessari.

1. Identificare le porte ISL e i canali delle porte non utilizzati utilizzando il banner del file RCF:



Se la porta è in modalità breakout, il nome della porta specificato nel comando potrebbe essere diverso dal nome indicato nell'intestazione RCF. È inoltre possibile utilizzare i file di cablaggio RCF per individuare il nome della porta.

Per informazioni dettagliate sulla porta ISL

Eseguire il comando show port all.

Per i dettagli del canale della porta

Eseguire il comando show port-channel all.

2. Disattivare le porte ISL e i canali delle porte non utilizzati.

È necessario eseguire i seguenti comandi per ogni porta o canale di porta non utilizzato identificato.

```
(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
```

Configurare gli switch IP Cisco

Configurare gli switch IP Cisco per l'interconnessione del cluster e la connettività IP MetroCluster back-end

È necessario configurare gli switch IP Cisco per l'utilizzo come interconnessione del cluster e per la connettività IP MetroCluster back-end.

A proposito di questa attività

Molte delle procedure descritte in questa sezione sono procedure indipendenti ed è necessario eseguire solo quelle a cui si è indirizzati o che sono pertinenti al proprio compito.

Ripristino delle impostazioni predefinite dello switch IP Cisco

Prima di installare qualsiasi file RCF, è necessario cancellare la configurazione dello switch Cisco ed eseguire la configurazione di base. Questa procedura è necessaria quando si desidera reinstallare lo stesso file RCF dopo un'installazione precedente non riuscita o se si desidera installare una nuova versione di un file RCF.

A proposito di questa attività

- È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.
- È necessario essere collegati allo switch mediante la console seriale.
- Questa attività ripristina la configurazione della rete di gestione.

Fasi**1. Ripristinare le impostazioni predefinite dello switch:**

- a. Cancellare la configurazione esistente:

```
write erase
```

b. Ricaricare il software dello switch:

```
reload
```

Il sistema viene riavviato e viene avviata la configurazione guidata. Durante l'avvio, se viene visualizzato il messaggio "Interrompi provisioning automatico e continua con la normale configurazione? (sì/no)[n]", you should respond yes per procedere.

c. Nella configurazione guidata, immettere le impostazioni di base dello switch:

- Password amministratore
- Nome dello switch
- Configurazione della gestione fuori banda
- Gateway predefinito
- Servizio SSH (RSA)

Al termine della configurazione guidata, lo switch si riavvia.

d. Quando richiesto, immettere il nome utente e la password per accedere allo switch.

L'esempio seguente mostra i prompt e le risposte del sistema durante la configurazione dello switch. Le staffe angolari (<<<) mostrano dove inserire le informazioni.

```
---- 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.

Inserire le informazioni di base nel successivo set di prompt, inclusi nome dello switch, indirizzo di gestione e gateway, quindi selezionare SSH con RSA.



Questo esempio mostra le informazioni minime necessarie per configurare l'RCF; è possibile configurare opzioni aggiuntive dopo l'applicazione dell'RCF. Ad esempio, è possibile configurare SNMPv3, NTP o SCP/SFTP dopo aver applicato l'RCF.

```
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]:
```

L'ultimo set di prompt completa la configurazione:

```
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. Salvare la configurazione:

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

3. Riavviare lo switch e attendere che lo switch si ricarichi:

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

4. Ripetere i passaggi precedenti sugli altri tre switch nella configurazione IP MetroCluster.

Download e installazione del software NX-OS dello switch Cisco

È necessario scaricare il file del sistema operativo dello switch e il file RCF su ciascun switch nella configurazione IP MetroCluster.

A proposito di questa attività

Questa attività richiede un software per il trasferimento dei file, ad esempio FTP, TFTP, SFTP o SCP, per copiare i file sui centralini.

Questa procedura deve essere ripetuta su ciascuno switch IP nella configurazione IP di MetroCluster.

È necessario utilizzare la versione del software dello switch supportata.

"NetApp Hardware Universe"

Fasi

1. Scaricare il file software NX-OS supportato.

"Download del software Cisco"

2. Copiare il software dello switch sullo switch:

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

In questo esempio, il file nxos.7.0.3.I4.6.bin e l'immagine EPLD vengono copiati dal server SFTP 10.10.99.99 al bootflash locale:

```
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. Verificare su ogni switch che i file NX-OS dello switch siano presenti nella directory bootflash di ogni switch:

```
dir bootflash:
```

Il seguente esempio mostra che i file sono presenti su IP_switch_A_1:

```

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. Installare il software dello switch:

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

Lo switch viene ricaricato (riavviato) automaticamente dopo l'installazione del software dello switch.

L'esempio seguente mostra l'installazione del software su IP_switch_A_1:

```

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

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

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

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

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

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

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

```

```
-- SUCCESS
```

```
Compatibility check is done:
```

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

```
Images will be upgraded according to following table:
```

Module Required	Image	Running-Version(pri:alt)	New-Version	Upg-
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. Attendere che lo switch si ricarichi, quindi accedere allo switch.

Una volta riavviato lo switch, viene visualizzato il prompt di login:

```
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. Verificare che il software dello switch sia stato installato:

```
show version
```

L'esempio seguente mostra l'output:

```
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. Aggiornare l'immagine EPLD e riavviare lo switch.

```

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. dopo il riavvio dello switch, accedere nuovamente e verificare che la nuova versione di EPLD sia stata caricata correttamente.

```
show version module 1 epld
```

9. Ripetere questa procedura sui tre switch IP rimanenti nella configurazione IP MetroCluster.

Download e installazione dei file Cisco IP RCF

È necessario generare e installare il file RCF in ogni switch nella configurazione IP di MetroCluster.

A proposito di questa attività

Questa attività richiede un software per il trasferimento dei file, ad esempio FTP, TFTP, SFTP o SCP, per copiare i file sui centralini.

Questa procedura deve essere ripetuta su ciascuno switch IP nella configurazione IP di MetroCluster.

È necessario utilizzare la versione del software dello switch supportata.

"NetApp Hardware Universe"

Se si utilizza un adattatore QSFP-SFP+, potrebbe essere necessario configurare la porta ISL in modalità di velocità nativa invece che in modalità di velocità breakout. Per determinare la modalità di velocità della porta ISL, consultare la documentazione fornita con lo switch.

Sono disponibili quattro file RCF, uno per ciascuno dei quattro switch nella configurazione IP di MetroCluster. È necessario utilizzare i file RCF corretti per il modello di switch in uso.

Switch	File RCF
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

Fasi

1. Generare i file Cisco RCF per MetroCluster IP.
 - a. Scaricare "[RcfFileGenerator per MetroCluster IP](#)"
 - b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.



Le modifiche apportate ai file RCF dopo il download non sono supportate.

2. Copiare i file RCF sugli switch:

- a. Copiare i file RCF sul primo switch:

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

In questo esempio, il file RCF NX3232_v1.80_Switch-A1.txt viene copiato dal server SFTP all'indirizzo 10.10.99.99 alla flash di avvio locale. Utilizzare l'indirizzo IP del server TFTP/SFTP e il nome file del file RCF da installare.

```

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. Ripetere il passaggio precedente per ciascuno degli altri tre switch, assicurandosi di copiare il file RCF corrispondente sullo switch corrispondente.
3. Verificare su ogni switch che il file RCF sia presente nella directory bootflash di ogni switch:

dir bootflash:

Il seguente esempio mostra che i file sono presenti su IP_switch_A_1:

```

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. Configurare le regioni TCAM sugli switch Cisco 3132Q-V e Cisco 3232C.



Saltare questo passaggio se non si dispone di switch Cisco 3132Q-V o Cisco 3232C.

- a. Sullo switch Cisco 3132Q-V, impostare le seguenti regioni TCAM:

```
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. Sullo switch Cisco 3232C, impostare le seguenti regioni TCAM:

```
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. Dopo aver impostato le regioni TCAM, salvare la configurazione e ricaricare lo switch:

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

5. Copiare il file RCF corrispondente dalla flash di avvio locale alla configurazione in esecuzione su ogni switch:

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

6. Copiare i file RCF dalla configurazione in esecuzione alla configurazione di avvio su ciascun switch:

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

L'output dovrebbe essere simile a quanto segue:

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

7. Ricaricare lo switch:

```
reload
```

```
IP_switch_A_1# reload
```

8. Ripetere i passaggi precedenti sugli altri tre switch nella configurazione IP MetroCluster.

Impostazione della correzione degli errori di inoltro per i sistemi che utilizzano la connettività a 25 Gbps

Se il sistema è configurato utilizzando la connettività a 25 Gbps, è necessario impostare manualmente il parametro fec (Forward Error Correction) su Off dopo aver applicato il file RCF. Il file RCF non applica questa impostazione.

A proposito di questa attività

Le porte a 25 Gbps devono essere cablate prima di eseguire questa procedura.

[**"Assegnazioni delle porte della piattaforma per switch Cisco 3232C o Cisco 9336C"**](#)

Questa attività si applica solo alle piattaforme che utilizzano la connettività a 25 Gbps:

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

Questa attività deve essere eseguita su tutti e quattro gli switch nella configurazione IP di MetroCluster.

Fasi

1. Impostare il parametro fec su Off su ciascuna porta a 25 Gbps collegata a un modulo controller, quindi copiare la configurazione in esecuzione nella configurazione di avvio:
 - a. Accedere alla modalità di configurazione: config t
 - b. Specificare l'interfaccia a 25 Gbps da configurare: interface interface-ID
 - c. Impostare fec su Off: fec off
 - d. Ripetere i passaggi precedenti per ciascuna porta a 25 Gbps dello switch.
 - e. Uscire dalla modalità di configurazione: exit

L'esempio seguente mostra i comandi per l'interfaccia Ethernet1/25/1 sullo switch IP_switch_A_1:

```
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. Ripetere il passaggio precedente sugli altri tre switch della configurazione IP MetroCluster.

Disattivare le porte e i canali delle porte ISL non utilizzati

NetApp consiglia di disattivare le porte ISL e i canali delle porte inutilizzati per evitare avvisi di integrità non necessari.

1. Identificare le porte ISL e i canali delle porte non utilizzati:

```
show interface brief
```

2. Disattivare le porte ISL e i canali delle porte non utilizzati.

È necessario eseguire i seguenti comandi per ogni porta o canale di porta non utilizzato identificato.

```
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.
```

Configurare la crittografia MACsec sugli switch Cisco 9336C in un sito IP MetroCluster



La crittografia MACsec può essere applicata solo alle porte ISL WAN.

Configurare la crittografia MACsec sugli switch Cisco 9336C

È necessario configurare la crittografia MACsec solo sulle porte ISL WAN in esecuzione tra i siti. È necessario configurare MACsec dopo aver applicato il file RCF corretto.

Requisiti di licenza per MACsec

MACsec richiede una licenza di sicurezza. Per una spiegazione completa dello schema di licenza di Cisco NX-OS e su come ottenere e richiedere le licenze, consultare la "[Guida alle licenze di Cisco NX-OS](#)"

Abilitare gli ISL WAN con crittografia Cisco MACsec nelle configurazioni IP di MetroCluster

È possibile attivare la crittografia MACsec per gli switch Cisco 9336C sugli ISL WAN in una configurazione IP MetroCluster.

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Abilitare MACsec e MKA sul dispositivo:

```
feature macsec
```

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

3. Copiare la configurazione in esecuzione nella configurazione di avvio:

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

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

Configurare una catena di chiavi MACsec e le chiavi

È possibile creare una o più chiavi MACsec nella configurazione.

Key Lifetime e Hitless Key Rollover

Un portachiavi MACsec può avere più chiavi pre-condivise (PSK), ciascuna configurata con un ID chiave e una durata opzionale. La durata della chiave specifica l'ora di attivazione e scadenza della chiave. In assenza di una configurazione a vita, la durata predefinita è illimitata. Quando viene configurata una vita utile, l'MKA passa alla successiva chiave precondizionata nel portachiavi dopo la scadenza della vita utile. Il fuso orario del tasto può essere locale o UTC. Il fuso orario predefinito è UTC. Un tasto può passare a un secondo tasto all'interno dello stesso portachiavi se configuri il secondo tasto (nel portachiavi) e configuri una durata per il primo tasto. Quando la durata della prima chiave scade, passa automaticamente alla chiave successiva nell'elenco. Se la stessa chiave viene configurata su entrambi i lati del collegamento contemporaneamente, il rollover della chiave è hitless (ovvero, il tasto viene rollover senza interruzione del traffico).

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Per nascondere la stringa di ottetti della chiave crittografata, sostituire la stringa con un carattere jolly nell'output di show running-config e show startup-config comandi:

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



La stringa di ottetti viene nascosta anche quando si salva la configurazione in un file.

Per impostazione predefinita, le chiavi PSK vengono visualizzate in formato crittografato e possono essere facilmente decifrate. Questo comando si applica solo alle catene di chiavi MACsec.

3. Creare una catena di chiavi MACsec per contenere una serie di chiavi MACsec e accedere alla modalità di configurazione della catena di chiavi MACsec:

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec  
IP_switch_A_1(config-macseckeckeychain)#[/pre>
```

4. Creare una chiave MACsec e accedere alla modalità di configurazione della chiave MACsec:

```
key key-id
```

L'intervallo è compreso tra 1 e 32 caratteri esadecimale e la dimensione massima è di 64 caratteri.

```
IP_switch_A_1 switch(config-macseckeckeychain)# key 1000  
IP_switch_A_1 (config-macseckeckeychain-macseckeckey)#[/pre>
```

5. Configurare la stringa di ottetti per la chiave:

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

```
IP_switch_A_1 (config-macseckeckeychain-macseckeckey) # key-octet-string  
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789  
cryptographic-algorithm AES_256_CMAC
```



L'argomento ottet-string può contenere fino a 64 caratteri esadecimale. La chiave octet viene codificata internamente, quindi la chiave in testo non viene visualizzata nell'output di show running-config macsec comando.

6. Configurare una durata di invio per la chiave (in secondi):

```
send-lifetime start-time duration duration
```

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

Per impostazione predefinita, il dispositivo considera l'ora di inizio come UTC. L'argomento relativo all'ora di inizio indica l'ora e la data in cui la chiave diventa attiva. L'argomento duration è la durata della vita in secondi. La lunghezza massima è di 2147483646 secondi (circa 68 anni).

7. Copiare la configurazione in esecuzione nella configurazione di avvio:

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

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

8. Visualizza la configurazione del portachiavi:

```
show key chain name
```

```
IP_switch_A_1(config-macseckeckeychain-macseckeckey)# show key chain 1
```

Configurare un criterio MACsec

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Creare un criterio MACsec:

```
macsec policy name
```

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

3. Configurare una delle seguenti crittografia, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 o GCM-AES-XPN-256:

```
cipher-suite name
```

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

4. Configurare la priorità del server chiave per interrompere il legame tra i peer durante uno scambio di chiavi:

```
key-server-priority number
```

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

5. Configurare il criterio di protezione per definire la gestione dei dati e dei pacchetti di controllo:

```
security-policy security policy
```

Scegliere una policy di sicurezza tra le seguenti opzioni:

- Must-Secure — i pacchetti che non trasportano intestazioni MACsec vengono eliminati
- Dovrebbe-sicuro — sono consentiti pacchetti che non trasportano intestazioni MACsec (questo è il valore predefinito)

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

6. Configurare la finestra di protezione dalla riproduzione in modo che l'interfaccia protetta non accetti un pacchetto inferiore alle dimensioni della finestra configurata: window-size number



La dimensione della finestra di protezione dalla riproduzione rappresenta il numero massimo di frame fuori sequenza che MACsec accetta e non vengono scartati. L'intervallo va da 0 a 596000000.

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

7. Configurare il tempo in secondi per forzare una riskey SAK:

```
sak-expiry-time time
```

È possibile utilizzare questo comando per impostare la chiave di sessione su un intervallo di tempo prevedibile. Il valore predefinito è 0.

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

8. Configurare uno dei seguenti offset di riservatezza nel frame Layer 2 in cui inizia la crittografia:

```
conf-offsetconfidentiality offset
```

Scegliere una delle seguenti opzioni:

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

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



Questo comando potrebbe essere necessario affinché gli switch intermedi utilizzino intestazioni di pacchetti (dmac, smac, etype) come tag MPLS.

9. Copiare la configurazione in esecuzione nella configurazione di avvio:

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

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

10. Visualizzare la configurazione del criterio MACsec:

```
show macsec policy
```

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

Abilitare la crittografia Cisco MACsec sulle interfacce

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Selezionare l'interfaccia configurata con la crittografia MACsec.

È possibile specificare il tipo di interfaccia e l'identità. Per una porta Ethernet, utilizzare slot/porta ethernet.

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

3. Aggiungere il portachiavi e il criterio da configurare sull'interfaccia per aggiungere la configurazione MACsec:

```
macsec keychain keychain-name policy policy-name
```

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

4. Ripetere i passaggi 1 e 2 su tutte le interfacce in cui deve essere configurata la crittografia MACsec.

5. Copiare la configurazione in esecuzione nella configurazione di avvio:

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

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

Disattivare gli ISL WAN con crittografia Cisco MACsec nelle configurazioni IP di MetroCluster

Potrebbe essere necessario disattivare la crittografia MACsec per gli switch Cisco 9336C sugli ISL WAN in una configurazione IP MetroCluster.

Fasi

1. Accedere alla modalità di configurazione globale:

```
configure terminal
```

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

2. Disattivare la configurazione MACsec sul dispositivo:

```
macsec shutdown
```

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



Selezionando l'opzione “no” si ripristina la funzione MACsec.

3. Selezionare l'interfaccia già configurata con MACsec.

È possibile specificare il tipo di interfaccia e l'identità. Per una porta Ethernet, utilizzare slot/porta ethernet.

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

4. Rimuovere il portachiavi e il criterio configurati sull'interfaccia per rimuovere la configurazione MACsec:

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

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

5. Ripetere i passaggi 3 e 4 su tutte le interfacce in cui è configurato MACsec.

6. Copiare la configurazione in esecuzione nella configurazione di avvio:

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

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

Verifica della configurazione MACsec

Fasi

1. Ripetere **tutte** le procedure precedenti sul secondo switch all'interno della configurazione per stabilire una sessione MACsec.
2. Eseguire i seguenti comandi per verificare che entrambi gli switch siano crittografati correttamente:
 - a. Esecuzione: show macsec mka summary
 - b. Esecuzione: show macsec mka session
 - c. Esecuzione: show macsec mka statistics

È possibile verificare la configurazione MACsec utilizzando i seguenti comandi:

Comando	Visualizza informazioni su...
show macsec mka session interface typeslot/port number	La sessione MACsec MKA per un'interfaccia specifica o per tutte le interfacce
show key chain name	La configurazione della catena di chiavi
show macsec mka summary	La configurazione MACsec MKA
show macsec policy policy-name	La configurazione per un criterio MACsec specifico o per tutti i criteri MACsec

Configurare gli switch NVIDIA IP

Configurare lo switch NVIDIA IP SN2100 per l'interconnessione del cluster e la connettività IP MetroCluster backend

È necessario configurare gli switch IP NVIDIA SN2100 per l'utilizzo come interconnessione del cluster e per la connettività IP MetroCluster back-end.

Ripristina le impostazioni predefinite dello switch NVIDIA IP SN2100

Per ripristinare le impostazioni predefinite di uno switch, è possibile scegliere tra i seguenti metodi.

- [Ripristinare lo switch utilizzando l'opzione del file RCF](#)
- [Scaricare e installare il software Cumulus](#)

ripristinare lo switch utilizzando l'opzione del file RCF

Prima di installare una nuova configurazione RCF, è necessario ripristinare le impostazioni dello switch NVIDIA.

A proposito di questa attività

Per ripristinare le impostazioni predefinite dello switch, eseguire il file RCF con `restoreDefaults` opzione. Questa opzione copia i file di backup originali nella posizione originale e riavvia lo switch. Dopo il riavvio, lo switch viene fornito online con la configurazione originale esistente al momento della prima esecuzione del file RCF per configurare lo switch.

I seguenti dettagli di configurazione non vengono ripristinati:

- Configurazione utente e credenziale
- Configurazione della porta di rete di gestione, eth0



Tutte le altre modifiche di configurazione che si verificano durante l'applicazione del file RCF vengono ripristinate alla configurazione originale.

Prima di iniziare

- È necessario configurare lo switch in base a. [Scaricare e installare il file NVIDIA RCF](#). Se la configurazione non è stata eseguita in questo modo o se sono state configurate funzionalità aggiuntive prima di eseguire il file RCF, non è possibile utilizzare questa procedura.
- È necessario ripetere questa procedura su ciascuno switch IP nella configurazione IP di MetroCluster.
- È necessario essere connessi allo switch con una connessione seriale alla console.
- Questa attività ripristina la configurazione della rete di gestione.

Fasi

1. Verificare che la configurazione RCF sia stata applicata correttamente con la stessa versione del file RCF o compatibile e che i file di backup esistano.



L'output può mostrare file di backup, file conservati o entrambi. Se i file di backup o i file conservati non vengono visualizzati nell'output, non è possibile utilizzare questa procedura.

```

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. Eseguire il file RCF con l'opzione per ripristinare le impostazioni predefinite: `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. Rispondere "sì" al prompt. Lo switch torna alla configurazione originale e si riavvia.
4. Attendere il riavvio dello switch.

Lo switch viene ripristinato e conserva la configurazione iniziale, ad esempio la configurazione della rete di gestione e le credenziali correnti, così come esistevano prima dell'applicazione del file RCF. Dopo il riavvio, è possibile applicare una nuova configurazione utilizzando la stessa versione o una versione diversa del file RCF.

scaricare e installare il software Cumulus

A proposito di questa attività

Seguire questa procedura se si desidera ripristinare completamente lo switch applicando l'immagine Cumulus.

Prima di iniziare

- È necessario essere connessi allo switch con una connessione seriale alla console.
- L'immagine software dello switch Cumulus è accessibile tramite HTTP.



Per ulteriori informazioni sull'installazione di Cumulus Linux, vedere "[Panoramica dell'installazione e della configurazione degli switch NVIDIA SN2100](#)"

- È necessario disporre della password root per `sudo` accesso ai comandi.

Fasi

1. Dalla console di Cumulus scaricare e mettere in coda l'installazione del software dello switch con il comando `onie-install -a -i` seguito dal percorso del file per il software dello switch:

In questo esempio, il file del firmware `cumulus-linux-4.4.3-mlx-amd64.bin` viene copiato dal server HTTP '50.50.50.50' allo switch locale.

```
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. Rispondere `y` alla richiesta di conferma dell'installazione quando l'immagine viene scaricata e verificata.
3. Riavviare lo switch per installare il nuovo software: `sudo reboot`

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



Lo switch si riavvia e viene avviata l'installazione del software dello switch, operazione che richiede un certo tempo. Al termine dell'installazione, lo switch si riavvia e rimane visualizzato il prompt di accesso.

4. Configurare le impostazioni di base dello switch

- a. All'avvio dello switch e al prompt di accesso, accedere e modificare la password.



Il nome utente è 'cumulus' e la password predefinita è 'cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+c14.4.3u1
(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 worldwide
basis.

cumulus@cumulus:mgmt:~\$

5. Configurare l'interfaccia di rete di gestione.

I comandi utilizzati dipendono dalla versione del firmware dello switch in uso.



I seguenti comandi di esempio configurano il nome host come IP_switch_A_1, l'indirizzo IP come 10.10.10.10, la maschera di rete come 255.255.255.0 (24) e l'indirizzo del gateway come 10.10.10.1.

Cumulus 4,4.x

I seguenti comandi di esempio configurano il nome host, l'indirizzo IP, la maschera di rete e il gateway su uno switch che esegue Cumulus 4,4.x

```
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 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 e successivi

I seguenti comandi di esempio configurano il nome host, l'indirizzo IP, la maschera di rete e il gateway su uno switch che esegue Cumulus 5,4.x o versioni successive.

```
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. Riavviare lo switch utilizzando `sudo reboot` comando.

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

Al riavvio dello switch, è possibile applicare una nuova configurazione seguendo la procedura descritta in [Scaricare e installare il file NVIDIA RCF](#).

Scarica e installa i file NVIDIA RCF

È necessario generare e installare il file RCF dello switch in ogni switch nella configurazione IP di MetroCluster.

Prima di iniziare

- È necessario disporre della password root per `sudo` accesso ai comandi.
- Il software dello switch è installato e la rete di gestione è configurata.
- È stata eseguita la procedura per installare inizialmente lo switch utilizzando il metodo 1 o il metodo 2.
- Non è stata applicata alcuna configurazione aggiuntiva dopo l'installazione iniziale.



Se si esegue un'ulteriore configurazione dopo aver reimpostato lo switch e prima di applicare il file RCF, non è possibile utilizzare questa procedura.

A proposito di questa attività

Ripetere questa procedura su ciascuno switch IP nella configurazione MetroCluster IP (nuova installazione) o sullo switch sostitutivo (sostituzione dello switch).

Se si utilizza un adattatore QSFP-SFP+, potrebbe essere necessario configurare la porta ISL in modalità di velocità nativa invece che in modalità di velocità breakout. Per determinare la modalità di velocità della porta ISL, consultare la documentazione fornita con lo switch.

Fasi

1. Generare i file NVIDIA RCF per MetroCluster IP.
 - a. Scaricare il ["RcfFileGenerator per MetroCluster IP"](#).

- b. Generare il file RCF per la configurazione utilizzando RcfFileGenerator per MetroCluster IP.
- c. Accedere alla home directory. Se si è registrati come 'cumulo', il percorso del file è /home/cumulus.

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

- d. Scaricare il file RCF in questa directory. L'esempio seguente mostra che si utilizza SCP per scaricare il file SN2100_v2.0.0_IP_switch_A_1.txt dal server '50.50.50.50' alla home directory e salvarlo con nome 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's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Eseguire il file RCF. Il file RCF richiede un'opzione per applicare uno o più passaggi. Se non richiesto dal supporto tecnico, eseguire il file RCF senza l'opzione della riga di comando. Per verificare lo stato di completamento delle varie fasi del file RCF, utilizzare l'opzione '-1' o 'all' per applicare tutte le fasi (in sospeso).

```
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. Se la configurazione utilizza cavi DAC, attivare l'opzione DAC sulle porte dello switch:

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

Nell'esempio seguente viene attivata l'opzione DAC per la porta `swp7`:

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 SN2100_v2.0.0_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. Riavviare lo switch dopo aver attivato l'opzione DAC sulle porte dello switch:

```
sudo reboot
```



Quando si imposta l'opzione DAC per più porte dello switch, è necessario riavviare lo switch una sola volta.

Impostare la correzione degli errori in avanti per i sistemi che utilizzano la connettività a 25 Gbps

Se il sistema è configurato utilizzando una connettività a 25 Gbps, impostare manualmente il parametro Forward Error Correction (fec) su Off dopo aver applicato l'RCF. L'RCF non applica questa impostazione.

A proposito di questa attività

- Questa attività si applica solo alle piattaforme che utilizzano la connettività a 25 Gbps. Fare riferimento alla "[Assegnazioni delle porte della piattaforma per gli switch IP SN2100 supportati da NVIDIA](#)".
- Questa attività deve essere eseguita su tutti e quattro gli switch nella configurazione IP di MetroCluster.
- È necessario aggiornare ogni porta dello switch singolarmente, non è possibile specificare più porte o intervalli di porte nel comando.

Fasi

1. Impostare il `fec` parametro su Off per la prima porta dello switch che utilizza la connettività a 25 Gbps:

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

2. Ripetere l'operazione per ogni porta dello switch a 25 Gbps collegata a un modulo controller.

Impostare la velocità della porta dello switch per le interfacce IP MetroCluster

A proposito di questa attività

- Utilizzare questa procedura per impostare la velocità della porta dello switch su 100g per i seguenti sistemi:
 - AFF A70, AFF A90, AFF A1K, AFF C80
 - AFF A30, AFF C30, AFF A50, AFF C60
 - FAS50, FAS70, FAS90
- È necessario aggiornare ogni porta dello switch singolarmente, non è possibile specificare più porte o intervalli di porte nel comando.

Fase

1. Utilizzare il file RCF con l' `runCmd` opzione per impostare la velocità. Questa operazione applica l'impostazione e salva la configurazione.

I seguenti comandi impostano la velocità per le interfacce MetroCluster `swp7` e `swp8`:

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

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

Esempio

```
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:~$
```

Disattivare le porte e i canali delle porte ISL non utilizzati

NetApp consiglia di disattivare le porte ISL e i canali delle porte inutilizzati per evitare avvisi di integrità non necessari. È necessario disattivare ogni porta o canale porta individualmente, non è possibile specificare più porte o intervalli di porte nel comando.

Fasi

1. Identificare le porte ISL e i canali delle porte non utilizzati utilizzando il banner del file RCF:



Se la porta è in modalità breakout, il nome della porta specificato nel comando potrebbe essere diverso dal nome indicato nell'intestazione RCF. È inoltre possibile utilizzare i file di cablaggio RCF per individuare il nome della porta.

```
net show interface
```

2. Disattivare le porte ISL e i canali delle porte non utilizzati utilizzando il file RCF.

```

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:~$
```

Il seguente comando di esempio disattiva la porta "swp14":

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

Ripetere questo passaggio per ogni porta o canale di porta non utilizzato identificato.

Installare il file di configurazione Ethernet Switch Health Monitor per uno switch IP NVIDIA SN2100 MetroCluster

Per configurare il monitoraggio dello stato dello switch Ethernet sugli switch Ethernet NVIDIA, seguire questa procedura.

Queste istruzioni si applicano se gli switch NVIDIA X190006-PE e X190006-PI non vengono rilevati

correttamente, il che può essere confermato eseguendo `system switch ethernet show` e controlla se **OTHER** è visualizzato per il tuo modello. Per identificare il modello del tuo switch NVIDIA, trova il codice prodotto con il comando `nv show platform hardware` per NVIDIA CL 5.8 e precedenti o `nv show platform` per le versioni successive.

 Questi passaggi sono consigliati anche se si desidera che il monitoraggio dello stato e la raccolta dei log funzionino correttamente quando si utilizza NVIDIA CL 5.11.x con le seguenti release di ONTAP. Sebbene il monitoraggio dello stato e la raccolta dei log possano comunque funzionare anche senza questi passaggi, seguirli garantisce il corretto funzionamento di tutto.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 e versioni successive

Prima di iniziare

- Assicurarsi che il cluster ONTAP sia attivo e in esecuzione.
- Abilitare SSH sullo switch per utilizzare tutte le funzionalità disponibili in CSHM.
- Cancellare la `/mroot/etc/cshm_nod/nod_sign/` directory su tutti i nodi:

- a. Immettere la notoresella:

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

- b. Modifica dei privilegi avanzati:

```
priv set advanced
```

- c. Elencare i file di configurazione nella `/etc/cshm_nod/nod_sign` directory. Se la directory esiste e contiene file di configurazione, elenca i nomi dei file.

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

- d. Eliminare tutti i file di configurazione corrispondenti ai modelli di switch collegati.

In caso di dubbi, rimuovere tutti i file di configurazione per i modelli supportati elencati sopra, quindi scaricare e installare i file di configurazione più recenti per gli stessi modelli.

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

- a. Verificare che i file di configurazione eliminati non siano più nella directory:

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

Fasi

1. Scaricare il file zip di configurazione dello switch Ethernet Health monitor in base alla versione di ONTAP corrispondente. Questo file è disponibile nella "[Switch Ethernet NVIDIA](#)" pagina .
 - a. Nella pagina di download del software NVIDIA SN2100, selezionare **Nvidia CSHM file**.
 - b. Nella pagina attenzione/da leggere, selezionare la casella di controllo per accettare.
 - c. Nella pagina Contratto di licenza con l'utente finale, selezionare la casella di controllo Accetto e fare clic su **Accetta e continua**.
 - d. Nella pagina file Nvidia CSHM - Download, selezionare il file di configurazione appropriato. Sono disponibili i seguenti file:

ONTAP 9.15.1 e versioni successive

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

ONTAP da 9.11.1 a 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. caricare il file zip applicabile sul server Web interno.
2. Accedi alle impostazioni della modalità avanzata da uno dei sistemi ONTAP nel cluster.

```
set -privilege advanced
```

3. Eseguire il comando di configurazione dello switch Health monitor.

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

4. Verificare che l'output del comando termini con il seguente testo per la versione di ONTAP in uso:

ONTAP 9.15.1 e versioni successive

Il monitoraggio dello stato dello switch Ethernet ha installato il file di configurazione.

ONTAP da 9.11.1 a 9.14.1

SHM ha installato il file di configurazione.

ONTAP 9.10.1

Pacchetto scaricato CSHM elaborato correttamente.

In caso di errore, contattare il supporto NetApp.

1. attendere fino a due volte l'intervallo di polling del monitor dello stato dello switch Ethernet, rilevato eseguendo `system switch ethernet polling-interval show`, prima di completare il passaggio successivo.
2. Esegui il comando `system switch ethernet configure-health-monitor show` sul sistema ONTAP e assicurarsi che gli switch del cluster vengano rilevati con il campo monitorato impostato su **True** e che il campo del numero di serie non mostri **Unknown**.

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



Se il modello mostra ancora **ALTRO** dopo aver applicato il file di configurazione, contattare il supporto NetApp.

Vedi il "[switch di sistema ethernet configura-monitor-stato](#)" comando per ulteriori dettagli.

Quali sono le prossime novità?

["Configurare il monitoraggio dello stato dello switch"](#).

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.