Configurare gli switch IP Cisco

ONTAP MetroCluster

NetApp
April 25, 2024

Sommario

Configurare gli switch IP Cisco

Configurazione degli switch IP Cisco

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 (<<<) mostra 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.

```
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 viene copiato 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)...
   ```

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

Download e installazione dei file Cisco IP RCF

È necessario scaricare il file RCF su ogni 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"

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. Scaricare i file MetroCluster IP RCF.

   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

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 precondivisa configurata 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-macseckeychain)#
   ```

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 esadecimali e la dimensione massima è di 64 caratteri.

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

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

   > L'argomento ottet-string può contenere fino a 64 caratteri esadecimali. 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-macseckeychain-macseckey)# 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-macseckeychain-macseckey)# 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