Configuration des commutateurs IP MetroCluster

ONTAP MetroCluster

NetApp
February 13, 2026

Sommaire

Configuration des commutateurs IP MetroCluster . . . 1
- Choisissez la procédure de configuration du commutateur IP MetroCluster appropriée . . . 1
- Configurer les commutateurs IP Broadcom pour l'interconnexion de cluster et la connectivité IP MetroCluster backend . . . 1
  - Réinitialisation des paramètres d'usine du commutateur IP Broadcom . . . 1
  - Téléchargement et installation du logiciel du commutateur Broadcom EFOS . . . 6
  - Téléchargement et installation des fichiers RCF Broadcom . . . 14
  - Désactivez les ports ISL et les canaux de port inutilisés . . . 18
- Configuration des commutateurs IP Cisco . . . 19
  - Configurer les commutateurs IP Cisco pour l'interconnexion des clusters et la connectivité IP MetroCluster backend . . . 19
  - Configurer le cryptage MACsec sur les commutateurs Cisco 9336C dans un site IP MetroCluster . . . 34
- Configurez les commutateurs IP NVIDIA . . . 41
  - Configurer le commutateur NVIDIA IP SN2100 pour l'interconnexion de cluster et la connectivité IP MetroCluster backend . . . 41
  - Installer le fichier de configuration Ethernet Switch Health Monitor pour un commutateur IP NVIDIA SN2100 MetroCluster . . . 54

Configuration des commutateurs IP MetroCluster

Choisissez la procédure de configuration du commutateur IP MetroCluster appropriée

Vous devez configurer les switchs IP pour assurer la connectivité IP MetroCluster back-end. La procédure à suivre dépend de votre fournisseur de commutateur.

- "Configurez les commutateurs IP Broadcom"
- "Configuration des commutateurs IP Cisco"
- "Configurez les commutateurs IP NVIDIA"

Configurer les commutateurs IP Broadcom pour l'interconnexion de cluster et la connectivité IP MetroCluster backend

Vous devez configurer les commutateurs IP Broadcom pour qu'ils servent d'interconnexion de cluster et pour la connectivité IP MetroCluster de back-end.

Votre configuration nécessite des licences supplémentaires (6 licences de port de 100 Go) dans les scénarios suivants :

- Vous utilisez les ports 53 et 54 en tant que MetroCluster ISL de 40 Gbits/s ou 100 Gbits/s.
- Vous utilisez une plate-forme qui connecte le cluster local et les interfaces MetroCluster aux ports 49 - 52.

Réinitialisation des paramètres d'usine du commutateur IP Broadcom

Avant d'installer une nouvelle version du logiciel de commutation et des RCFs, vous devez effacer les paramètres du commutateur Broadcom et effectuer une configuration de base.

Description de la tâche

- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur à l'aide de la console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Passez à l'invite de commande surélevée (`#`) : `enable`

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

2. Effacez la configuration de démarrage et supprimez la bannière

   a. Effacez la configuration de démarrage :

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) #
```

Cette commande n'efface pas la bannière.

b. Supprimer la bannière :

no set clibanner

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

3. Redémarrez le commutateur :*`(IP_switch_A_1) #reload*`

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

Si le système vous demande si vous souhaitez enregistrer la configuration non enregistrée ou modifiée avant de recharger le commutateur, sélectionnez **non**.

4. Attendre que le commutateur se recharge, puis se connecter au commutateur.

L'utilisateur par défaut est « admin » et aucun mot de passe n'est défini. Une invite similaire à la commande suivante s'affiche :

```
(Routing)>
```

5. Passer à l'invite de commande surélevée :

`enable`

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

6. Définissez le protocole du port de service sur `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. Attribuez l'adresse IP au port de service :

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

   L'exemple suivant montre l'adresse IP 10.10.10.10 attribuée à un port de service avec le sous-réseau 255.255.255.0 et la passerelle 10.10.10.1 :

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

8. Vérifiez que le port de service est correctement configuré :

   `show serviceport`

   L'exemple suivant indique que le port est activé et que les adresses correctes ont été attribuées :

```
(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. Configurez le serveur SSH.

   - Le fichier RCF désactive le protocole Telnet. Si vous ne configurez pas le serveur SSH, vous pouvez uniquement accéder au pont à l'aide de la connexion du port série.
   - Vous devez configurer le serveur SSH afin d'utiliser la collecte de journaux et d'autres outils externes.

a. Générer des clés RSA.

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

b. Générer des clés DSA (facultatif)

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

c. Si vous utilisez la version conforme FIPS de EFOS, générez les clés ECDSA. L'exemple suivant crée les clés d'une longueur de 521. Les valeurs valides sont 256, 384 ou 521.

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

d. Activez le serveur SSH.

Si nécessaire, quittez le contexte de configuration.

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

+

Si des clés existent déjà, il peut vous être demandé de les remplacer.

10. Si vous le souhaitez, configurez le domaine et le serveur de noms :

`configure`

L'exemple suivant montre le `ip domain` et `ip name server` commandes :

```
(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. Si vous le souhaitez, configurez le fuseau horaire et la synchronisation de l'heure (SNTP).

L'exemple suivant montre le `sntp` Commandes, en spécifiant l'adresse IP du serveur SNTP et le fuseau horaire relatif.

```
(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)#
```

Pour EFOS version 3.10.0.3 et ultérieure, utilisez le `ntp` comme indiqué dans l'exemple suivant :

```
> (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. Configurer le nom du commutateur :

    `hostname IP_switch_A_1`

    L'invite du commutateur affiche le nouveau nom :

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Enregistrez la configuration :

    `write memory`

    Vous recevez des invites et des valeurs de sortie similaires à l'exemple suivant :

```
(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. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Téléchargement et installation du logiciel du commutateur Broadcom EFOS

Vous devez télécharger le fichier du système d'exploitation du switch et le fichier RCF sur chaque commutateur de la configuration IP de MetroCluster.

Description de la tâche

Cette tâche doit être répétée sur chaque commutateur de la configuration IP de MetroCluster.

Notez ce qui suit :

- Lors de la mise à niveau de EFOS 3.4.x.x vers EFOS 3.7.x.x ou version ultérieure, le commutateur doit exécuter EFOS 3.4.4.6 (ou version 3.4.x.x ultérieure). Si vous exécutez une version antérieure à celle-ci, mettez d'abord le commutateur à niveau vers EFOS 3.4.4.6 (ou version ultérieure 3.4.x.x), puis mettez-le à niveau vers EFOS 3.7.x.x ou version ultérieure.
- La configuration de EFOS 3.4.x.x et 3.7.x.x ou ultérieure est différente. Pour changer la version EFOS de 3.4.x.x à 3.7.x.x ou ultérieure, ou vice versa, le commutateur doit être réinitialisé aux valeurs par défaut et les fichiers RCF pour la version EFOS correspondante doivent être (ré)appliqués. Cette procédure nécessite un accès via le port série console.
- À partir de la version 3.7.x.x ou ultérieure de EFOS, une version non conforme à la norme FIPS et une version conforme à la norme FIPS sont disponibles. Différentes étapes sont appliquées lorsque vous passez d'une version non conforme à FIPS à une version conforme FIPS ou inversement. Le fait de remplacer EFOS d'une version non conforme à la norme FIPS par une version conforme à la norme FIPS ou vice versa réinitialise les paramètres par défaut du commutateur. Cette procédure nécessite un accès via le port série console.

Étapes

1. Téléchargez le micrologiciel du commutateur à partir du "Site de support Broadcom".
2. Vérifiez si votre version de EFOS est conforme à la norme FIPS ou non conforme à la norme FIPS à l'aide du `show fips status` commande. Dans les exemples suivants, `IP_switch_A_1` Utilise EFOS et conforme à la norme FIPS `IP_switch_A_2` Utilise EFOS non conforme à la norme FIPS.

Exemple 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Exemple 2

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

IP_switch_A_2 #
```

3. Utilisez le tableau suivant pour déterminer la méthode à suivre :

Procédure	Version actuelle de EFOS	Nouvelle version EFOS	Pas de niveau élevé
Procédure de mise à niveau de EFOS entre deux versions (non conformes à la norme FIPS	3.4.x.x	3.4.x.x	Installer la nouvelle image EFOS à l'aide de la méthode 1) les informations de configuration et de licence sont conservées
3.4.4.6 (ou version ultérieure 3.4.x.x)	3.7.x.x ou version ultérieure non conforme FIPS	Mettre à niveau EFOS à l'aide de la méthode 1. Réinitialisez le commutateur sur les paramètres par défaut et appliquez le fichier RCF pour EFOS 3.7.x.x ou version ultérieure	3.7.x.x ou version ultérieure non conforme FIPS
3.4.4.6 (ou version ultérieure 3.4.x.x)	Rétrograder EFOS à l'aide de la méthode 1. Réinitialisez le commutateur sur les paramètres par défaut et appliquez le fichier RCF pour EFOS 3.4.x.x	3.7.x.x ou version ultérieure non conforme FIPS	

Installez la nouvelle image EFOS à l'aide de la méthode 1. Les informations de configuration et de licence sont conservées	Conforme à la norme FIPS 3.7.x.x ou ultérieure	Conforme à la norme FIPS 3.7.x.x ou ultérieure	Installez la nouvelle image EFOS à l'aide de la méthode 1. Les informations de configuration et de licence sont conservées
Procédure de mise à niveau vers/à partir d'une version conforme à la norme FIPS EFOS	Non conforme à la norme FIPS	Conforme à la norme FIPS	Installation de l'image EFOS à l'aide de la méthode 2. La configuration du commutateur et les informations de licence seront perdues.

- Méthode 1 : Procédure de mise à niveau de EFOS en téléchargeant l'image logicielle dans la partition de démarrage de sauvegarde
- Méthode 2 : Procédure de mise à niveau de EFOS à l'aide de l'installation ONIE OS

Procédure de mise à niveau de EFOS en téléchargeant l'image logicielle dans la partition de démarrage de sauvegarde

Vous ne pouvez effectuer les étapes suivantes que si les deux versions EFOS ne sont pas conformes à la norme FIPS ou si les deux versions EFOS sont conformes à la norme FIPS.

N'utilisez pas ces étapes si une version est conforme à la norme FIPS et que l'autre est non conforme à la norme FIPS.

Étapes

1. Copier le logiciel du commutateur sur le commutateur : `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   Dans cet exemple, le fichier système d'exploitation efos-3.4.4.6.stk est copié du serveur SFTP à 50.50.50.50 vers la partition de sauvegarde. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
(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. Configurez le commutateur pour qu'il démarre à partir de la partition de sauvegarde lors du prochain redémarrage du commutateur :

   `boot system backup`

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

(IP_switch_A_1) #
```

3. Vérifiez que la nouvelle image de démarrage sera active au prochain démarrage :

   `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. Enregistrez la configuration :

   `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. Redémarrez le commutateur :

   `reload`

```
(IP_switch_A_1) #reload

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

6. Attendez que le commutateur redémarre.

Dans de rares cas, le commutateur peut ne pas démarrer. Suivez le Procédure de mise à niveau de EFOS à l'aide de l'installation ONIE OS pour installer la nouvelle image.

7. Si vous passez de EFOS 3.4.x.x à EFOS 3.7.x.x ou vice versa, suivez les deux procédures suivantes pour appliquer la configuration correcte (RCF) :
   a. Réinitialisation des paramètres d'usine du commutateur IP Broadcom
   b. Téléchargement et installation des fichiers RCF Broadcom
8. Répétez ces étapes sur les trois commutateurs IP restants de la configuration IP MetroCluster.

Procédure de mise à niveau de EFOS à l'aide de l'installation ONIE OS

Vous pouvez effectuer les étapes suivantes si une version de EFOS est conforme à la norme FIPS et que l'autre version de EFOS n'est pas compatible FIPS. Ces étapes peuvent être utilisées pour installer l'image EFOS 3.7.x.x non conforme à la norme FIPS ou à la norme FIPS à partir d'ONIE si le commutateur ne parvient pas à démarrer.

Étapes

1. Démarrez le commutateur en mode d'installation ONIE.

   Au cours du démarrage, sélectionnez ONIE lorsque l'écran suivant s'affiche :

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

   Après avoir sélectionné « ONIE », le commutateur se charge et vous présente les choix suivants :

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

Le commutateur démarre maintenant en mode d'installation ONIE.

2. Arrêtez la détection ONIE et configurez l'interface ethernet

   Lorsque le message suivant s'affiche, appuyez sur <ENTER> pour appeler la console ONIE :

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

   La détection ONIE se poursuit et les messages sont imprimés sur la console.

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

3. Configurez l'interface ethernet et ajoutez la route à l'aide de `ifconfig eth0 <ipAddress> netmask <netmask> up` et `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. Vérifiez que le serveur hébergeant le fichier d'installation ONIE est accessible :

```
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. Installez le nouveau logiciel du commutateur

```
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.
```

Le logiciel va installer puis redémarrer le commutateur. Laissez le commutateur redémarrer normalement dans la nouvelle version de EFOS.

6. Vérifier que le nouveau logiciel de commutateur est installé

`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. Terminez l'installation

   Le commutateur redémarre sans configuration appliquée et rétablit les paramètres par défaut. Suivez les deux procédures pour configurer les paramètres de base du commutateur et appliquer le fichier RCF comme indiqué dans les deux documents suivants :

   a. Configurer les paramètres de base du commutateur. Suivez l'étape 4 et les versions ultérieures : Réinitialisation des paramètres d'usine du commutateur IP Broadcom
   b. Créez et appliquez le fichier RCF comme indiqué dans Téléchargement et installation des fichiers RCF Broadcom

Téléchargement et installation des fichiers RCF Broadcom

Vous devez générer et installer le fichier RCF des switchs sur chaque switch de configuration MetroCluster IP.

Avant de commencer

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Description de la tâche

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Il existe quatre fichiers RCF, un par pour chacun des quatre commutateurs de la configuration MetroCluster IP. Vous devez utiliser les fichiers RCF appropriés pour le modèle de commutateur que vous utilisez.

Commutateur	Fichier 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

Fichiers RCF pour EFOS version 3.4.4.6 ou ultérieure 3.4.x.x. La version et la version 3.7.0.4 de EFOS sont différentes. Vous devez vous assurer que vous avez créé les fichiers RCF appropriés pour la version EFOS que le commutateur est en cours d'exécution.

Version EFOS	Version du fichier RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Étapes

1. Générez les fichiers RCF Broadcom pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP"
   b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

Les modifications apportées aux fichiers RCF après le téléchargement ne sont pas prises en charge.

2. Copier les fichiers RCF sur les commutateurs :

   a. Copier les fichiers RCF sur le premier commutateur : `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`

      Dans cet exemple, le fichier RCF "BES-53248_v1.32_Switch-A1.txt" est copié du serveur SFTP à "50.50.50.50" vers le bootflash local. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
(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. Vérifiez que le fichier RCF est enregistré comme 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. Appliquer le 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. Enregistrez la configuration :

```
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. Redémarrez le commutateur :

```
reload
```

```
(IP_switch_A_1) #reload

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

a. Répétez les étapes précédentes pour chacun des trois autres commutateurs en veillant à copier le fichier RCF correspondant sur le commutateur correspondant.

3. Recharger l'interrupteur :

```
reload
```

```
IP_switch_A_1# reload
```

4. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifiez les ports ISL et les canaux de port inutilisés à l'aide de la bannière du fichier RCF :

> Si le port est en mode écorché, le nom de port que vous spécifiez dans la commande peut être différent du nom indiqué dans la bannière RCF. Vous pouvez également utiliser les fichiers de câblage RCF pour trouver le nom du port.

Pour plus de détails sur le port ISL

Lancer la commande `show port all`.

Pour plus d'informations sur les canaux de port

Lancer la commande `show port-channel all`.

2. Désactivez les ports ISL et les canaux de port inutilisés.

   Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

```
(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
```

Configuration des commutateurs IP Cisco

Configurer les commutateurs IP Cisco pour l'interconnexion des clusters et la connectivité IP MetroCluster backend

Vous devez configurer les switchs IP Cisco pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Description de la tâche

Plusieurs procédures de cette section sont des procédures indépendantes et vous n'avez qu'à exécuter celles que vous êtes dirigé vers ou qui sont pertinentes pour votre tâche.

Réinitialisation des paramètres d'usine du commutateur IP Cisco

Avant d'installer un fichier RCF, vous devez effacer la configuration du commutateur Cisco et effectuer une configuration de base. Cette procédure est obligatoire lorsque vous souhaitez réinstaller le même fichier RCF après l'échec d'une installation précédente ou si vous souhaitez installer une nouvelle version d'un fichier RCF.

Description de la tâche

- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur à l'aide de la console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Rétablir les paramètres d'usine du commutateur :

   a. Effacez la configuration existante :

      `write erase`

b. Recharger le logiciel du contacteur :

```
reload
```

Le système redémarre et entre dans l'assistant de configuration. Au cours du démarrage, si vous recevez l'invite « abandonner la mise en service automatique et poursuivre la configuration normale ? (oui/non)", you should respond `yes pour continuer.

c. Dans l'assistant de configuration, entrez les paramètres de base du commutateur :

- Mot de passe d'administrateur
- Nom du commutateur
- Configuration de gestion hors bande
- Passerelle par défaut
- Service SSH (RSA)

Une fois l'assistant de configuration terminé, le commutateur redémarre.

d. Lorsque vous y êtes invité, entrez le nom d'utilisateur et le mot de passe pour vous connecter au commutateur.

L'exemple suivant montre les invites et les réponses système lors de la configuration du commutateur. Les supports d'angle (<<<) indique où vous saisissez les informations.

```
---- 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.
```

Vous entrez des informations de base dans les invites suivantes, notamment le nom du commutateur, l'adresse de gestion et la passerelle, et sélectionnez SSH avec RSA.

Cet exemple montre les informations minimales requises pour configurer la FCR. Des options supplémentaires peuvent être configurées une fois la FCR appliquée. Par exemple, vous pouvez configurer SNMPv3, NTP ou SCP/SFTP après avoir appliqué le 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]:
```

Le jeu d’invites final termine la configuration :

```
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. Enregistrez la configuration :

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

3. Redémarrez le commutateur et attendez que le commutateur se recharge :

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

4. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Téléchargement et installation du logiciel du commutateur Cisco NX-OS

Vous devez télécharger le fichier du système d'exploitation du switch et le fichier RCF sur chaque commutateur de la configuration IP de MetroCluster.

Description de la tâche

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Étapes

1. Téléchargez le fichier logiciel NX-OS pris en charge.

   "Téléchargement de logiciels Cisco"

2. Copier le logiciel du commutateur sur le commutateur :

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

   Dans cet exemple, le fichier nxos.7.0.3.I4.6.bin et l'image EPLD sont copiés du serveur SFTP 10.10.99.99 vers le bootflash local :

```
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. Vérifiez sur chaque commutateur que les fichiers de commutateur NX-OS sont présents dans le répertoire bootflash de chaque commutateur :

   `dir bootflash:`

   L'exemple suivant montre que les fichiers sont présents sur 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. Installez le logiciel du commutateur :

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

   Le commutateur se recharge automatiquement (redémarre) après l'installation du logiciel du commutateur.

   L'exemple suivant montre l'installation du logiciel sur 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. Attendre que le commutateur se recharge, puis se connecter au commutateur.

   Une fois le commutateur redémarré, l'invite de connexion s'affiche :

```
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. Vérifier que le logiciel du commutateur a été installé :
   `show version`

   L'exemple suivant montre la sortie :

```
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. Mettre à niveau l’image EPLD et redémarrer le commutateur.

```
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. après le redémarrage du commutateur, reconnectez-vous et vérifiez que la nouvelle version de EPLD a été chargée avec succès.

   ```
   show version module 1 epld
   ```

9. Répétez ces étapes sur les trois commutateurs IP restants de la configuration IP MetroCluster.

Téléchargement et installation des fichiers Cisco IP RCF

Vous devez générer et installer le fichier RCF sur chaque switch de configuration MetroCluster IP.

Description de la tâche

Cette tâche nécessite un logiciel de transfert de fichiers, tel que FTP, TFTP, SFTP ou SCP, pour copier les fichiers sur les commutateurs.

Ces étapes doivent être répétées sur chacun des commutateurs IP de la configuration MetroCluster IP.

Vous devez utiliser la version du logiciel de commutation prise en charge.

"NetApp Hardware Universe"

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

Il existe quatre fichiers RCF, un par pour chacun des quatre commutateurs de la configuration MetroCluster IP. Vous devez utiliser les fichiers RCF appropriés pour le modèle de commutateur que vous utilisez.

Commutateur	Fichier 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

Étapes

1. Générez les fichiers RCF Cisco pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP"
   b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

   > Les modifications apportées aux fichiers RCF après le téléchargement ne sont pas prises en charge.

2. Copier les fichiers RCF sur les commutateurs :
   a. Copier les fichiers RCF sur le premier commutateur :

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

      Dans cet exemple, le fichier RCF NX3232_v1.80_Switch-A1.txt est copié du serveur SFTP à 10.10.99.99 vers le bootflash local. Vous devez utiliser l'adresse IP de votre serveur TFTP/SFTP et le nom du fichier RCF que vous devez installer.

```
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. Répétez la sous-étape précédente pour chacun des trois autres commutateurs en étant sûr de copier le fichier RCF correspondant sur le commutateur correspondant.

3. Vérifiez sur chaque commutateur que le fichier RCF est présent dans le répertoire bootflash de chaque commutateur :

   `dir bootflash:`

   L'exemple suivant montre que les fichiers sont présents sur 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. Configurez les régions TCAM sur les switchs Cisco 3132Q-V et Cisco 3232C.

   Ignorez cette étape si vous ne disposez pas de switchs Cisco 3132Q-V ou Cisco 3232C.

   a. Sur le commutateur Cisco 3132Q-V, définissez les régions TCAM suivantes :

```
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. Sur le switch Cisco 3232C, définissez les régions TCAM suivantes :

```
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. Après avoir défini les régions du TCAM, enregistrez la configuration et rechargez le commutateur :

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

5. Copiez le fichier RCF correspondant de la mémoire bootflash locale vers la configuration en cours d'exécution sur chaque commutateur :

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

6. Copiez les fichiers RCF de la configuration en cours d'exécution vers la configuration de démarrage de chaque commutateur :

   `copy running-config startup-config`

   Vous devez voir les résultats similaires à ce qui suit :

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

7. Recharger l'interrupteur :

   `reload`

```
IP_switch_A_1# reload
```

8. Répétez les étapes précédentes sur les trois autres commutateurs de la configuration MetroCluster IP.

Définition de la correction d'erreurs de renvoi pour les systèmes utilisant une connectivité à 25 Gbit/s.

Si votre système est configuré avec une connectivité 25 Gbit/s, vous devez définir manuellement le paramètre fec (Forward Error correction) sur Off après avoir appliqué le fichier RCF. Le fichier RCF n'applique pas ce paramètre.

Description de la tâche

Les ports 25 Gbit/s doivent être câblés avant d'effectuer cette procédure.

"Affectation des ports de plateforme pour les switchs Cisco 3232C ou Cisco 9336C"

Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s :

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

Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.

Étapes

1. Définissez le paramètre fec sur Off sur chaque port 25 Gbit/s connecté à un module de contrôleur, puis copiez la configuration en cours d'exécution sur la configuration de démarrage :

   a. Passer en mode configuration : `config t`

   b. Spécifiez l'interface 25 Gbit/s à configurer : `interface interface-ID`

   c. Réglez fec sur Arrêt : `fec off`

   d. Répétez les étapes précédentes pour chaque port 25 Gbit/s du commutateur.

   e. Quitter le mode de configuration : `exit`

   L'exemple suivant montre les commandes de l'interface Ethernet1/25/1 sur le commutateur 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. Répétez l'étape précédente sur les trois autres commutateurs de la configuration MetroCluster IP.

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles.

1. Identifier les ports ISL et les canaux de port inutilisés :

```
show interface brief
```

2. Désactivez les ports ISL et les canaux de port inutilisés.

   Vous devez exécuter les commandes suivantes pour chaque port ou canal de port non utilisé identifié.

```
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.
```

Configurer le cryptage MACsec sur les commutateurs Cisco 9336C dans un site IP MetroCluster

Le cryptage MACsec ne peut être appliqué qu'aux ports WAN ISL.

Configurez le cryptage MACsec sur les commutateurs Cisco 9336C

Vous devez uniquement configurer le cryptage MACsec sur les ports WAN ISL qui s'exécutent entre les sites. Vous devez configurer MACsec après avoir appliqué le fichier RCF correct.

Conditions de licence pour MACsec

MACsec nécessite une licence de sécurité. Pour une explication complète du schéma de licence Cisco NX-OS et de la manière d'obtenir et de demander des licences, consultez le "Guide des licences Cisco NX-OS"

Activez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous pouvez activer le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL WAN dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

```
configure terminal
```

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

2. Activer MACsec et MKA sur le périphérique :

```
feature macsec
```

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

3. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

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

Configurer une chaîne de clé MACsec et des clés

Vous pouvez créer une chaîne de clés MACsec ou des clés sur votre configuration.

Key Lifetime et hitless Key Rollover

Un trousseau MACsec peut avoir plusieurs clés pré-partagées (PSK), chacune configurée avec un ID de clé et une durée de vie facultative. La durée de vie d'une clé indique à quel moment la clé s'active et expire. En l'absence d'une configuration à vie, la durée de vie par défaut est illimitée. Lorsqu'une durée de vie est configurée, MKA passe à la prochaine clé pré-partagée configurée dans le trousseau une fois la durée de vie écoulée. Le fuseau horaire de la clé peut être local ou UTC. Le fuseau horaire par défaut est UTC. Une clé peut se déployer sur une seconde clé dans le même trousseau si vous configurez la seconde clé (dans le trousseau) et configurez une durée de vie pour la première clé. Lorsque la durée de vie de la première clé expire, elle passe automatiquement à la clé suivante de la liste. Si la même clé est configurée sur les deux côtés de la liaison en même temps, le basculement de la clé est sans arrêt (c'est-à-dire, la clé se replace sans interruption de la circulation).

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

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

2. Pour masquer la chaîne d'octet de clé cryptée, remplacez la chaîne par un caractère générique dans la sortie du `show running-config` et `show startup-config` commandes :

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

> La chaîne octet est également masquée lorsque vous enregistrez la configuration dans un fichier.

   Par défaut, les clés PSK sont affichées au format crypté et peuvent être déchiffrées facilement. Cette commande ne s'applique qu'aux chaînes de clés MACsec.

3. Créer une chaîne de clés MACsec pour contenir un jeu de clés MACsec et entrer le mode de configuration de la chaîne de clés MACsec :

```
key chain name macsec
```

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

4. Créer une clé MACsec et entrer le mode de configuration de la clé MACsec :

```
key key-id
```

La plage est comprise entre 1 et 32 caractères hexadécimaux, et la taille maximale est de 64 caractères.

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

5. Configurez la chaîne d'octet pour la clé :

```
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'argument octet-chaîne peut contenir jusqu'à 64 caractères hexadécimaux. La clé octet est codée en interne, de sorte que la clé en texte clair n'apparaît pas dans la sortie du `show running-config macsec` commande.

6. Configurer une durée de vie d'envoi pour la clé (en secondes) :

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

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

Par défaut, l'appareil traite l'heure de début comme UTC. L'argument heure de début correspond à l'heure et à la date auxquelles la clé devient active. L'argument de durée est la durée de vie en secondes. La longueur maximale est de 2147483646 secondes (environ 68 ans).

7. Copier la configuration en cours d'exécution dans la configuration de démarrage :

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

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

8. Affiche la configuration du trousseau :

   `show key chain name`

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

Configurez une stratégie MACsec

Étapes

1. Passer en mode de configuration globale :

   `configure terminal`

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

2. Créer une stratégie MACsec :

   `macsec policy name`

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

3. Configurez l'un des chiffrements suivants : GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 ou GCM-AES-XPN-256 :

   `cipher-suite name`

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

4. Configurez la priorité du serveur de clés pour rompre le lien entre les pairs lors d'un échange de clés :

   `key-server-priority number`

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

5. Configurez la stratégie de sécurité pour définir le traitement des données et des paquets de contrôle :

   `security-policy security policy`

   Choisissez une stratégie de sécurité parmi les options suivantes :

   - Doit-Secure — les paquets qui ne portent pas les en-têtes MACsec sont supprimés

- Devrait-Secure — les paquets qui ne portent pas d'en-têtes MACsec sont autorisés (il s'agit de la valeur par défaut)

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

6. Configurez la fenêtre de protection de relecture de sorte que l'interface sécurisée n'accepte pas un paquet dont la taille de fenêtre configurée est inférieure à celle de la fenêtre : `window-size number`

> La taille de la fenêtre de protection de relecture représente le nombre maximum de trames hors séquence que MACsec accepte et ne sont pas supprimées. La plage va de 0 à 596000000.

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

7. Configurer le temps en secondes pour forcer une nouvelle touche SAK :

   `sak-expiry-time time`

   Vous pouvez utiliser cette commande pour remplacer la clé de session par un intervalle de temps prévisible. La valeur par défaut est 0.

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

8. Configurez l'un des décalages de confidentialité suivants dans la trame de couche 2 où le chiffrement commence :

   `conf-offsetconfidentiality offset`

   Choisissez parmi les options suivantes :

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

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

> Cette commande peut être nécessaire pour que les commutateurs intermédiaires utilisent des en-têtes de paquets (dmac, smac, etype) comme des balises MPLS.

9. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

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

10. Afficher la configuration de la stratégie MACsec :

    `show macsec policy`

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

Activez le cryptage Cisco MACsec sur les interfaces

1. Passer en mode de configuration globale :

    `configure terminal`

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

2. Sélectionnez l'interface que vous avez configurée avec le cryptage MACsec.

    Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

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

3. Ajoutez le trousseau et la stratégie à configurer sur l'interface pour ajouter la configuration MACsec :

    `macsec keychain keychain-name policy policy-name`

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

4. Répétez les étapes 1 et 2 sur toutes les interfaces où le cryptage MACsec doit être configuré.
5. Copier la configuration en cours d'exécution dans la configuration de démarrage :

    `copy running-config startup-config`

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

Désactivez les liens ISL de Cisco MACsec dans les configurations IP de MetroCluster

Vous devrez peut-être désactiver le cryptage MACsec pour les commutateurs Cisco 9336C sur les liens ISL du réseau étendu dans une configuration IP MetroCluster.

Étapes

1. Passer en mode de configuration globale :

`configure terminal`

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

2. Désactivez la configuration MACsec sur le périphérique :

   `macsec shutdown`

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

   La sélection de l'option « non » restaure la fonction MACsec.

3. Sélectionnez l'interface que vous avez déjà configurée avec MACsec.

   Vous pouvez spécifier le type et l'identité de l'interface. Pour un port Ethernet, utilisez le logement/port ethernet.

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

4. Supprimez le trousseau et la stratégie configurés sur l'interface pour supprimer la configuration MACsec :

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

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

5. Répétez les étapes 3 et 4 sur toutes les interfaces où MACsec est configuré.
6. Copier la configuration en cours d'exécution dans la configuration de démarrage :

   `copy running-config startup-config`

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

Vérification de la configuration MACsec

Étapes

1. Répétez **tous** des procédures précédentes sur le deuxième commutateur de la configuration pour établir une session MACsec.
2. Exécutez les commandes suivantes pour vérifier que les deux commutateurs sont chiffrés :

   a. Exécuter : `show macsec mka summary`

b. Exécuter : `show macsec mka session`

c. Exécuter : `show macsec mka statistics`

Vous pouvez vérifier la configuration MACsec à l'aide des commandes suivantes :

Commande	Affiche des informations sur…
`show macsec mka session interface typeslot/port number`	La session MKA de MACsec pour une interface spécifique ou pour toutes les interfaces
`show key chain name`	La configuration de la chaîne de clés
`show macsec mka summary`	La configuration MACsec MKA
`show macsec policy policy-name`	Configuration d'une stratégie MACsec spécifique ou de toutes les politiques MACsec

Configurez les commutateurs IP NVIDIA

Configurer le commutateur NVIDIA IP SN2100 pour l'interconnexion de cluster et la connectivité IP MetroCluster backend

Vous devez configurer les switchs IP NVIDIA SN2100 pour une utilisation en tant qu'interconnexion de cluster et pour la connectivité IP MetroCluster back-end.

Réinitialiser les valeurs par défaut du commutateur NVIDIA IP SN2100

Vous pouvez choisir parmi les méthodes suivantes pour réinitialiser un commutateur sur les paramètres par défaut.

- Réinitialisez le commutateur à l'aide de l'option de fichier RCF
- Téléchargez et installez le logiciel Cumulus

Réinitialiser le commutateur à l'aide de l'option de fichier RCF

Avant d'installer une nouvelle configuration RCF, vous devez rétablir les paramètres du commutateur NVIDIA.

Description de la tâche

Pour restaurer les paramètres par défaut du commutateur, exécutez le fichier RCF avec le `restoreDefaults` option. Cette option copie les fichiers d'origine sauvegardés à leur emplacement d'origine, puis redémarre le commutateur. Après le redémarrage, le switch est en ligne avec la configuration d'origine qui existait au moment d'avoir exécuté le fichier RCF pour configurer le switch.

Les détails de configuration suivants ne sont pas réinitialisés :

- Configuration utilisateur et informations d'identification
- Configuration du port réseau de gestion, eth0

Toutes les autres modifications de configuration qui se produisent pendant l'application du fichier RCF sont rétablies à la configuration d'origine.

Avant de commencer

- Vous devez configurer le commutateur conformément à Téléchargez et installez le fichier RCF NVIDIA. Si vous n'avez pas configuré cette méthode ou si des fonctionnalités supplémentaires ont été configurées avant d'exécuter le fichier RCF, vous ne pouvez pas suivre cette procédure.
- Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration MetroCluster IP.
- Vous devez être connecté au commutateur par une connexion de console série.
- Cette tâche réinitialise la configuration du réseau de gestion.

Étapes

1. Vérifiez que la configuration RCF a été appliquée avec succès avec la même version ou une version de fichier RCF compatible et que les fichiers de sauvegarde sont bien en place.

Le résultat de cette commande peut afficher les fichiers de sauvegarde, les fichiers conservés, ou les deux. Si les fichiers de sauvegarde ou les fichiers conservés n'apparaissent pas dans le résultat, vous ne pouvez pas utiliser cette procédure.

```
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. Exécutez le fichier RCF avec la possibilité de restaurer les valeurs par défaut : `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. Répondez « oui » à l'invite. Le commutateur revient à la configuration d'origine et redémarre.
4. Attendez que le commutateur redémarre.

   Le commutateur est réinitialisé et conserve la configuration initiale, telle que la configuration du réseau de gestion et les identifiants actuels qu'ils existaient avant d'appliquer le fichier RCF. Après le redémarrage, vous pouvez appliquer une nouvelle configuration en utilisant la même version ou une version différente du fichier RCF.

Téléchargez et installez le logiciel Cumulus

Description de la tâche

Suivez ces étapes pour réinitialiser complètement le commutateur en appliquant l'image Cumulus.

Avant de commencer

- Vous devez être connecté au commutateur par une connexion de console série.
- L'image logicielle du commutateur Cumulus est accessible via HTTP.

> Pour plus d'informations sur l'installation de Cumulus Linux, voir "Présentation de l'installation et de la configuration des switchs NVIDIA SN2100"

- Vous devez avoir le mot de passe root pour `sudo` accès aux commandes.

Étapes

1. À partir de la console Cumulus, téléchargez et mettez en file d'attente l'installation du logiciel du commutateur avec la commande `onie-install -a -i` suivi du chemin du fichier vers le logiciel du commutateur :

   Dans cet exemple, le fichier du micrologiciel `cumulus-linux-4.4.3-mlx-amd64.bin` Est copié du serveur HTTP '50.50.50.50' sur le commutateur local.

```
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. Répondez `y` à l'invite pour confirmer l'installation lors du téléchargement et de la vérification de l'image.
3. Redémarrez le commutateur pour installer le nouveau logiciel : `sudo reboot`

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

> Le commutateur redémarre et entre dans l'installation du logiciel du commutateur, ce qui prend un certain temps. Une fois l'installation terminée, le commutateur redémarre et reste à l'invite de connexion.

4. Configurer les paramètres de base du commutateur
   a. Lorsque le commutateur est démarré et que vous êtes invité à ouvrir une session, connectez-vous et modifiez le mot de passe.

> Le nom d'utilisateur est 'cumulus' et le mot de passe par défaut est 'cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.3u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configuration de l'interface réseau de gestion

   Les commandes que vous utilisez dépendent de la version du micrologiciel du commutateur que vous exécutez.

   L'exemple de commandes suivant configure le nom d'hôte en tant que IP_Switch_A_1, l'adresse IP en tant que 10.10.10.10, le masque de réseau en tant que 255.255.255.0 (24) et l'adresse de la passerelle en tant que 10.10.10.1.

Cumulus 4.4.x

L'exemple de commandes suivant configure le nom d'hôte, l'adresse IP, le masque de réseau et la passerelle sur un commutateur exécutant 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@cumulus:mgmt:~$
```

Cumulus 5.4.x et versions ultérieures

L'exemple de commandes suivant configure le nom d'hôte, l'adresse IP, le masque de réseau et la passerelle sur un commutateur exécutant Cumulus 5.4.x. ou ultérieure.

```
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. Redémarrez le commutateur à l'aide du `sudo reboot` commande.

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

Lorsque le commutateur redémarre, vous pouvez appliquer une nouvelle configuration en suivant les étapes de la section Téléchargez et installez le fichier RCF NVIDIA.

Télécharger et installer les fichiers RCF NVIDIA

Vous devez générer et installer le fichier RCF des switchs sur chaque switch de configuration MetroCluster IP.

Avant de commencer

- Vous devez avoir le mot de passe root pour `sudo` accès aux commandes.
- Le logiciel du commutateur est installé et le réseau de gestion est configuré.
- Vous avez suivi les étapes d'installation initiale du commutateur à l'aide de la méthode 1 ou de la méthode 2.
- Vous n'avez appliqué aucune configuration supplémentaire après l'installation initiale.

> Si vous effectuez une autre configuration après la réinitialisation du commutateur et avant d'appliquer le fichier RCF, cette procédure ne peut pas être utilisée.

Description de la tâche

Vous devez répéter ces étapes sur chacun des commutateurs IP de la configuration IP MetroCluster (nouvelle installation) ou sur le commutateur de remplacement (remplacement du commutateur).

Si vous utilisez une carte QSFP-to-SFP+, vous devrez peut-être configurer le port ISL en mode de vitesse natif au lieu du mode de vitesse d'arrachage. Consultez la documentation du fournisseur du commutateur pour déterminer le mode de vitesse du port ISL.

Étapes

1. Générer les fichiers RCF NVIDIA pour MetroCluster IP.
   a. Téléchargez le "RcfFileGenerator pour MetroCluster IP".

b. Générez le fichier RCF pour votre configuration à l'aide de RcfFileGenerator pour MetroCluster IP.

c. Accédez à votre répertoire personnel. Si vous êtes enregistré en tant que 'culus', le chemin du fichier est `/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. Téléchargez le fichier RCF dans ce répertoire. L'exemple suivant montre que vous utilisez SCP pour télécharger le fichier `SN2100_v2.0.0_IP_switch_A_1.txt` du serveur '50.50.50.50' à votre répertoire personnel et enregistrez-le sous `SN2100_v2.0.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/SN2100_v2.0.0_IP_switch_A_1.txt
./SN2100_v2.0.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
**********************************************************************
**
Banner of the SCP server
**********************************************************************
**
username@50.50.50.50's password:
SN2100_v2.0.0_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Exécutez le fichier RCF. Le fichier RCF requiert une option permettant d'appliquer une ou plusieurs étapes. Sauf instruction contraire du support technique, exécutez le fichier RCF sans l'option de ligne de commande. Pour vérifier l'état d'achèvement des différentes étapes du fichier RCF, utilisez l'option '-1' ou 'All' pour appliquer toutes les étapes (en attente).

```
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. Si votre configuration utilise des câbles DAC, activez l'option DAC sur les ports de commutateur :

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

L'exemple suivant active l'option DAC pour le port `swp7`:

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

4. Redémarrez le commutateur après avoir activé l'option DAC sur les ports de commutateur :

```
sudo reboot
```

> Lorsque vous définissez l'option DAC pour plusieurs ports de commutateur, vous ne devez redémarrer le commutateur qu'une seule fois.

Définissez la correction d'erreur de transfert pour les systèmes utilisant une connectivité de 25 Gbit/s.

Si votre système est configuré avec une connectivité de 25 Gbit/s, définissez manuellement le paramètre correction d'erreur de transfert (fec) sur Désactivé après l'application de la FCR. La FCR n'applique pas ce paramètre.

Description de la tâche

- Cette tâche s'applique uniquement aux plates-formes utilisant une connectivité 25 Gbit/s. Reportez-vous à la "Affectations des ports de plateforme pour les switchs IP SN2100 pris en charge par NVIDIA".
- Cette tâche doit être effectuée sur les quatre commutateurs de la configuration IP MetroCluster.
- Vous devez mettre à jour chaque port de commutateur individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étapes

1. Définissez le `fec` paramètre sur Off pour le premier port de commutateur qui utilise une connectivité 25 Gbit/s :

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

2. Répétez l'étape pour chaque port de commutateur 25 Gbit/s connecté à un module de contrôleur.

Définissez la vitesse du port de commutateur pour les interfaces IP MetroCluster

Description de la tâche

- Utilisez cette procédure pour régler la vitesse du port de commutation sur 100 G pour les systèmes suivants :
  - AFF A70, AFF A90, AFF A1K, AFF C80
  - AFF A30, AFF C30, AFF A50, AFF C60
  - FAS50, FAS70, FAS90
- Vous devez mettre à jour chaque port de commutateur individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étape

1. Utilisez le fichier RCF avec `runCmd` l'option pour définir la vitesse. Ceci applique le paramètre et enregistre la configuration.

   Les commandes suivantes définissent la vitesse des interfaces MetroCluster `swp7` et `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
   ```

   Exemple

```
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:~$
```

Désactivez les ports ISL et les canaux de port inutilisés

NetApp recommande de désactiver les ports ISL et les canaux de port inutilisés afin d'éviter les alertes d'intégrité inutiles. Vous devez désactiver chaque port ou canal de port individuellement. Vous ne pouvez pas spécifier plusieurs ports ou plages de ports dans la commande.

Étapes

1. Identifiez les ports ISL et les canaux de port inutilisés à l'aide de la bannière du fichier RCF :

   Si le port est en mode écorché, le nom de port que vous spécifiez dans la commande peut être différent du nom indiqué dans la bannière RCF. Vous pouvez également utiliser les fichiers de câblage RCF pour trouver le nom du port.

   ```
   net show interface
   ```

2. Désactivez les ports ISL et les canaux de port inutilisés à l'aide du fichier 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:~$
```

L'exemple de commande suivant désactive le port « swp14 » :

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

Répétez cette étape pour chaque port ou canal de port non utilisé identifié.

Installer le fichier de configuration Ethernet Switch Health Monitor pour un commutateur IP NVIDIA SN2100 MetroCluster

Pour configurer la surveillance de l'état du commutateur Ethernet sur les commutateurs Ethernet NVIDIA, suivez cette procédure.

Ces instructions s'appliquent si les commutateurs NVIDIA X190006-PE et X190006-PI ne sont pas détectés

correctement, ce qui peut être confirmé en exécutant `system switch ethernet show` et vérifiez si **AUTRE** est affiché pour votre modèle. Pour identifier votre modèle de commutateur NVIDIA, recherchez sa référence à l'aide de la commande `nv show platform hardware` pour NVIDIA CL 5.8 et versions antérieures ou `nv show platform` pour les versions ultérieures.

> Ces étapes sont également recommandées si vous souhaitez que la surveillance de l'intégrité et la collecte des journaux fonctionnent correctement lors de l'utilisation de NVIDIA CL 5.11.x avec les versions ONTAP suivantes. Bien que la surveillance de l'intégrité et la collecte des journaux puissent fonctionner sans ces étapes, leur respect garantit le bon fonctionnement de l'ensemble.
>
> - 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 et versions ultérieures des correctifs

Avant de commencer

- Assurez-vous que le cluster ONTAP est opérationnel.
- Activez SSH sur le commutateur pour utiliser toutes les fonctionnalités disponibles dans CSHM.
- Effacez le `/mroot/etc/cshm_nod/nod_sign/` répertoire sur tous les nœuds :

  a. Entrez le nodeshell :

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

  b. Passer au privilège avancé :

     ```
     priv set advanced
     ```

  c. Répertoriez les fichiers de configuration dans le `/etc/cshm_nod/nod_sign` répertoire. Si le répertoire existe et contient des fichiers de configuration, il répertorie les noms des fichiers.

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

  d. Supprimez tous les fichiers de configuration correspondant à vos modèles de commutateurs connectés.

     Si vous n'êtes pas sûr, supprimez tous les fichiers de configuration pour les modèles pris en charge répertoriés ci-dessus, puis téléchargez et installez les derniers fichiers de configuration pour ces mêmes modèles.

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

  a. Vérifiez que les fichiers de configuration supprimés ne se trouvent plus dans le répertoire :

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

Étapes

1. Téléchargez le fichier zip de configuration du moniteur d'état du commutateur Ethernet basé sur la version ONTAP correspondante. Ce fichier est disponible à partir de la "Switchs Ethernet NVIDIA" page.
   a. Sur la page de téléchargement du logiciel NVIDIA SN2100, sélectionnez **Nvidia CSHM File**.
   b. Sur la page attention/doit lire, cochez la case pour accepter.

c. Sur la page Contrat de licence utilisateur final, cochez la case accepter et cliquez sur **accepter et continuer**.

d. Sur la page Nvidia CSHM File - Download, sélectionnez le fichier de configuration applicable. Les fichiers suivants sont disponibles :

ONTAP 9.15.1 et versions ultérieures

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

ONTAP 9.11.1 à 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. chargez le fichier zip applicable sur votre serveur Web interne.
2. Accédez au paramètre de mode avancé à partir d'un des systèmes ONTAP du cluster.

   ```
   set -privilege advanced
   ```

3. Exécutez la commande switch Health Monitor configure.

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

4. Vérifiez que le résultat de la commande se termine par le texte suivant pour votre version de ONTAP :

ONTAP 9.15.1 et versions ultérieures

La surveillance de l'état du commutateur Ethernet a installé le fichier de configuration.

ONTAP 9.11.1 à 9.14.1

SHM a installé le fichier de configuration.

ONTAP 9.10.1

Le package CSHM téléchargé a été traité avec succès.

En cas d'erreur, contactez le support NetApp.

1. attendez jusqu'à deux fois l'intervalle d'interrogation du moniteur d'état du commutateur Ethernet, détecté en exécutant `system switch ethernet polling-interval show`, avant de terminer l'étape suivante.
2. Exécutez la commande `system switch ethernet configure-health-monitor show` sur le système ONTAP et assurez-vous que les commutateurs du cluster sont détectés avec le champ surveillé

défini sur **Vrai** et le champ du numéro de série n'affichant pas **Inconnu**.

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

Si votre modèle affiche toujours **OTHER** après avoir appliqué le fichier de configuration, contactez le support NetApp.

Voir le "configuration-santé-surveillance du commutateur Ethernet du système" commande pour plus de détails.

Et la suite ?

"Configurer la surveillance de l'état des commutateurs".

Informations sur le copyright

Informations sur les marques commerciales