Configure os switches IP MetroCluster

ONTAP MetroCluster

NetApp
January 10, 2025

Índice

Configure os switches IP MetroCluster

Configuração de switches IP Broadcom

Você deve configurar os switches IP Broadcom para uso como interconexão de cluster e para conetividade IP MetroCluster de back-end.

A sua configuração requer licenças adicionais (6 licença de porta de 100 GB) nos seguintes cenários:

- Você usa as portas 53 e 54 como um ISL MetroCluster de 40 Gbps ou 100 Gbps.
- Você usa uma plataforma que coneta o cluster local e as interfaces MetroCluster às portas 49 - 52.

Redefinindo o switch IP Broadcom para os padrões de fábrica

Antes de instalar uma nova versão do software do switch e RCFs, você deve apagar as configurações do switch Broadcom e executar a configuração básica.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Mude para o prompt de comando elevado (`#`): `enable`

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

2. Apague a configuração de inicialização e remova o banner

   a. Apagar a configuração de arranque:

   `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) #
```

   Este comando não apaga o banner.

   b. Remova o banner:

no set clibanner

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

3. Reinicie o switch: **(IP_switch_A_1) #reload**

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

Se o sistema perguntar se deseja salvar a configuração não salva ou alterada antes de recarregar o switch, selecione **não**.

4. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   O usuário padrão é "'admin'", e nenhuma senha é definida. É apresentado um aviso semelhante ao seguinte:

```
(Routing)>
```

5. Mude para o prompt de comando elevado:

   `enable`

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

6. Defina o protocolo da porta de serviço como `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. Atribua o endereço IP à porta de serviço:

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

   O exemplo a seguir mostra um endereço IP atribuído à porta de serviço "10.10.10.10" com a sub-rede "255.255.255.0" e o gateway "10.10.10.1":

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

8. Verifique se a porta de serviço está configurada corretamente:

   ```
   show serviceport
   ```

   O exemplo a seguir mostra que a porta está ativa e os endereços corretos foram atribuídos:

```
(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. Se desejar, configure o servidor SSH.

   O arquivo RCF desativa o protocolo Telnet. Se você não configurar o servidor SSH, você só poderá acessar a ponte usando a conexão de porta serial.

   a. Gerar chaves RSA.

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

   b. Gerar chaves DSA (opcional)

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

   c. Se você estiver usando a versão compatível com FIPS do EFOS, gere as chaves ECDSA. O exemplo a seguir cria as teclas com um comprimento de 521. Os valores válidos são 256, 384 ou 521.

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

d. Ative o servidor SSH.

Se necessário, saia do contexto de configuração.

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

+

Se as chaves já existem, então você pode ser solicitado a sobrescrevê-las.

10. Se desejar, configure o domínio e o servidor de nomes:

`configure`

O exemplo a seguir mostra `ip domain` os comandos e `ip name server`:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. Se desejar, configure o fuso horário e a sincronização de horário (SNTP).

O exemplo a seguir mostra os `sntp` comandos, especificando o endereço IP do servidor SNTP e o fuso horário relativo.

```
(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)#
```

Para o EFOS versão 3.10.0.3 e posterior, use o `ntp` comando, como mostrado no exemplo a seguir:

```
> (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. Configure o nome do switch:

    `hostname IP_switch_A_1`

    O prompt do switch exibirá o novo nome:

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. Guardar a configuração:

    `write memory`

    Você recebe prompts e saída semelhantes ao seguinte exemplo:

```
(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. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Download e instalação do software Broadcom switch EFOS

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa deve ser repetida em cada switch na configuração IP do MetroCluster.

Observe o seguinte:

- Ao atualizar do EFOS 3,4.x.x para o EFOS 3,7.x.x ou posterior, o switch deve estar executando o EFOS 3.4.4.6 (ou versão 3,4.x.x posterior). Se você estiver executando uma versão antes disso, atualize o switch para EFOS 3.4.4.6 (ou versão posterior 3,4.x.x) primeiro, então atualize o switch para EFOS 3,7.x.x ou posterior.
- A configuração para o EFOS 3,4.x.x e 3,7.x.x ou posterior é diferente. Alterar a versão do EFOS de 3,4.x.x para 3,7.x.x ou posterior, ou vice-versa, requer que o switch seja redefinido para os padrões de fábrica e os arquivos RCF para que a versão do EFOS correspondente seja (re)aplicada. Este procedimento requer acesso através da porta do console serial.
- A partir da versão 3,7.x.x do EFOS ou posterior, uma versão não compatível com FIPS e compatível com FIPS está disponível. Diferentes etapas se aplicam ao passar de uma versão não compatível com FIPS para uma versão compatível com FIPS ou vice-versa. Alterar o EFOS de uma versão não compatível com FIPS para uma versão compatível com FIPS ou vice-versa redefinirá o switch para os padrões de fábrica. Este procedimento requer acesso através da porta do console serial.

Passos

1. Transfira o firmware do switch a partir do "Site de suporte da Broadcom".
2. Verifique se sua versão do EFOS é compatível com FIPS ou não compatível com FIPS usando o `show fips status` comando. Nos exemplos a seguir `IP_switch_A_1`, está usando EFOS compatível com FIPS e `IP_switch_A_2` está usando EFOS não compatível com FIPS.

   Exemplo 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Exemplo 2

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

IP_switch_A_2 #
```

3. Use a tabela a seguir para determinar qual método você deve seguir:

Procedimento	Versão atual do EFOS	Nova versão EFOS	Passos de alto nível
Etapas para atualizar o EFOS entre duas versões (não) compatíveis com FIPS	3.4.x.x	3.4.x.x	Instale a nova imagem EFOS utilizando o método 1) as informações de configuração e licença são mantidas
3.4.4.6 (ou posterior 3,4.x.x)	3,7.x.x ou posterior não compatível com FIPS	Atualize o EFOS usando o método 1. Redefina o switch para os padrões de fábrica e aplique o arquivo RCF para EFOS 3,7.x.x ou posterior	3,7.x.x ou posterior não compatível com FIPS
3.4.4.6 (ou posterior 3,4.x.x)	Downgrade EFOS usando o método 1. Redefina o switch para os padrões de fábrica e aplique o arquivo RCF para EFOS 3,4.x.x	3,7.x.x ou posterior não compatível com FIPS	
Instale a nova imagem EFOS usando o método 1. As informações de configuração e licença são mantidas	3,7.x.x ou posterior compatível com FIPS	3,7.x.x ou posterior compatível com FIPS	Instale a nova imagem EFOS usando o método 1. As informações de configuração e licença são mantidas

Passos para atualizar para/a partir de uma versão EFOS compatível com FIPS	Não compatível com FIPS	Compatível com FIPS	Instalação da imagem EFOS usando o método 2. A configuração do switch e as informações da licença serão perdidas.

- Método 1: Passos para atualizar o EFOS com o download da imagem de software para a partição de inicialização de backup
- Método 2: Etapas para atualizar o EFOS usando a instalação do ONIE os

Passos para atualizar o EFOS com o download da imagem de software para a partição de inicialização de backup

Só pode executar as seguintes etapas se ambas as versões do EFOS forem não compatíveis com FIPS ou ambas as versões do EFOS forem compatíveis com FIPS.

Não utilize estes passos se uma versão for compatível com FIPS e a outra não for compatível com FIPS.

Passos

1. Copie o software do interrutor para o interrutor: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   Neste exemplo, o arquivo do sistema operacional efos-3,4.4,6.stk é copiado do servidor SFTP em 50.50.50.50 para a partição de backup. Você precisa usar o endereço IP do seu servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
(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. Configure o switch para inicializar a partir da partição de backup na próxima reinicialização do switch:

   ```
   boot system backup
   ```

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

(IP_switch_A_1) #
```

3. Verifique se a nova imagem de inicialização estará ativa na próxima inicialização:

   ```
   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. Guardar a configuração:

   `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. Reinicie o switch:

   `reload`

```
(IP_switch_A_1) #reload

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

6. Aguarde até que o switch seja reiniciado.

Em cenários raros, o switch pode falhar ao inicializar. Siga o Etapas para atualizar o EFOS usando a instalação do ONIE os para instalar a nova imagem.

7. Se alterar a mudança de EFOS 3,4.x.x para EFOS 3,7.x.x ou vice-versa, siga os dois procedimentos a seguir para aplicar a configuração correta (RCF):
   a. Redefinindo o switch IP Broadcom para os padrões de fábrica
   b. Download e instalação dos arquivos RCF Broadcom
8. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Etapas para atualizar o EFOS usando a instalação do ONIE os

Pode executar as seguintes etapas se uma versão do EFOS for compatível com FIPS e a outra versão do EFOS não for compatível com FIPS. Estas etapas podem ser usadas para instalar a imagem EFOS 3,7.x.x não compatível com FIPS do ONIE se o switch não inicializar.

Passos

1. Inicialize o switch no modo de instalação ONIE.

   Durante a inicialização, selecione ONIE quando a seguinte tela for exibida:

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

   Depois de selecionar "ONIE", o switch irá então carregar e apresentar-lhe as seguintes opções:

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

O switch agora será inicializado no modo de instalação ONIE.

2. Pare a descoberta ONIE e configure a interface ethernet

   Quando a seguinte mensagem for exibida, pressione <enter> para chamar o console ONIE:

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

   A descoberta ONIE continuará e as mensagens serão impressas no console.

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

3. Configure a interface ethernet e adicione a rota utilizando `ifconfig eth0 <ipAddress> netmask <netmask> up` e. `route add default gw <gatewayAddress>`

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

4. Verifique se o servidor que hospeda o arquivo de instalação ONIE está acessível:

```
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. Instale o novo software do interrutor

```
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.
```

O software irá instalar e, em seguida, reiniciar o interrutor. Deixe o switch reiniciar normalmente para a nova versão do EFOS.

6. Verifique se o novo software do switch está instalado

`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. Conclua a instalação

   O switch reiniciará sem nenhuma configuração aplicada e redefinirá os padrões de fábrica. Siga os dois procedimentos para configurar as configurações básicas do switch e aplicar o arquivo RCF conforme descrito nos dois documentos a seguir:

   a. Configure as definições básicas do interrutor. Siga o passo 4 e posterior: Redefinindo o switch IP Broadcom para os padrões de fábrica
   b. Crie e aplique o arquivo RCF conforme descrito em Download e instalação dos arquivos RCF Broadcom

Download e instalação dos arquivos RCF Broadcom

Você deve gerar e instalar o arquivo RCF do switch em cada switch na configuração IP do MetroCluster.

Antes de começar

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Sobre esta tarefa

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Existem quatro arquivos RCF, um para cada um dos quatro switches na configuração IP do MetroCluster. Você deve usar os arquivos RCF corretos para o modelo de switch que você está usando.

Interrutor	Ficheiro 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

Os arquivos RCF para EFOS versão 3.4.4.6 ou posterior versão 3,4.x.x. e EFOS versão 3.7.0.4 são diferentes. Você precisa ter certeza de que criou os arquivos RCF corretos para a versão EFOS em que o switch está sendo executado.

Versão de EFOS	Versão do ficheiro RCF
3.4.x.x	v1.3x, v1.4x
3.7.x.x	v2.x

Passos

1. Gere os arquivos RCF Broadcom para MetroCluster IP.
   a. Transfira o. "RcfFileGenerator para MetroCluster IP"
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.

As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:

   a. Copie os arquivos RCF para o primeiro switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

      Neste exemplo, o arquivo RCF "BES-53248_v1,32_Switch-A1.txt" é copiado do servidor SFTP em "50.50.50.50" para o flash de inicialização local. Você precisa usar o endereço IP do seu servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
(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. Verifique se o arquivo RCF está salvo como um 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. Aplicar o 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. Guardar a configuração:

```
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. Reinicie o switch:

```
reload
```

```
(IP_switch_A_1) #reload

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

a. Repita os passos anteriores para cada uma das outras três centrais, certificando-se de copiar o ficheiro RCF correspondente para o comutador correspondente.

3. Recarregue o interrutor:

```
reload
```

```
IP_switch_A_1# reload
```

4. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identifique as portas ISL e os canais de portas não utilizados usando o banner de arquivo RCF:

> Se a porta estiver no modo de divisão, o nome da porta que você especificar no comando pode ser diferente do nome indicado no banner RCF. Você também pode usar os arquivos de cabeamento RCF para encontrar o nome da porta.

Para detalhes da porta ISL

Executar o comando `show port all`.

Para obter detalhes do canal da porta

Executar o comando `show port-channel all`.

2. Desative as portas ISL e os canais de portas não utilizados.

   Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

```
(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
```

Configurar switches IP Cisco

Configurar switches IP Cisco

Você deve configurar os switches IP Cisco para uso como interconexão de cluster e para conetividade IP do MetroCluster de back-end.

Sobre esta tarefa

Vários dos procedimentos nesta seção são procedimentos independentes e você só precisa executar aqueles para os quais você é direcionado ou é relevante para a sua tarefa.

Repor as predefinições de fábrica do interrutor IP do Cisco

Antes de instalar qualquer arquivo RCF, você deve apagar a configuração do switch Cisco e executar a configuração básica. Este procedimento é necessário quando você deseja reinstalar o mesmo arquivo RCF depois de uma instalação anterior falhar, ou se você quiser instalar uma nova versão de um arquivo RCF.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Repor as predefinições de fábrica do interrutor:

   a. Apagar a configuração existente:

      `write erase`

b. Recarregue o software do switch:

```
reload
```

O sistema reinicia e entra no assistente de configuração. Durante a inicialização, se você receber o prompt "'Cancelar provisionamento automático e continuar com a configuração normal? (sim/não)", `you should respond `yes` para continuar.

c. No assistente de configuração, introduza as definições básicas do interrutor:

- Palavra-passe de administrador
- Mudar nome
- Configuração de gerenciamento fora da banda
- Gateway predefinido
- Serviço SSH (RSA)

Depois de concluir o assistente de configuração, o switch reinicia.

d. Quando solicitado, introduza o nome de utilizador e a palavra-passe para iniciar sessão no comutador.

O exemplo a seguir mostra os prompts e as respostas do sistema ao configurar o switch. Os colchetes de ângulo (<<<) mostram onde você insere as informações.

```
---- 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.
```

Você insere informações básicas no próximo conjunto de prompts, incluindo o nome do switch, endereço de gerenciamento e gateway, e seleciona SSH com 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]:
```

O conjunto final de prompts completa a configuração:

```
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. Guardar a configuração:

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

3. Reinicie o switch e aguarde até que o switch recarregue:

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

4. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Transferir e instalar o software Cisco switch NX-os

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Passos

1. Transfira o ficheiro de software NX-os suportado.

   "Transferência do software Cisco"

2. Copie o software do interrutor para o interrutor:

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

   Neste exemplo, o arquivo nxos.7.0.3.I4.6.bin é copiado do servidor SFTP 10.10.99.99 para o flash de inicialização 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)...
   ```

3. Verifique em cada switch se os arquivos NX-os estão presentes no diretório bootflash de cada switch:

   ```
   dir bootflash:
   ```

   O exemplo a seguir mostra que os arquivos estão presentes no 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. Instale o software do interrutor:

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

   O interrutor recarregará (reiniciará) automaticamente após a instalação do software do interrutor.

   O exemplo a seguir mostra a instalação do software em 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. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   Depois que o switch reiniciar, o prompt de login é exibido:

```
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. Verifique se o software do switch foi instalado `show version`

   O exemplo a seguir mostra a saída:

```
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. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Transferir e instalar os ficheiros Cisco IP RCF

Você deve gerar e instalar o arquivo RCF em cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os

arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Existem quatro arquivos RCF, um para cada um dos quatro switches na configuração IP do MetroCluster. Você deve usar os arquivos RCF corretos para o modelo de switch que você está usando.

Interrutor	Ficheiro 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

Passos

1. Gerar os arquivos RCF do Cisco para MetroCluster IP.
   a. Transfira o. "RcfFileGenerator para MetroCluster IP"
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.

      As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:
   a. Copie os arquivos RCF para o primeiro switch:

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

      Neste exemplo, o arquivo RCF NX3232_v1.80_Switch-A1.txt é copiado do servidor SFTP em 10.10.99.99 para o flash de inicialização local. Você deve usar o endereço IP do servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
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. Repita a subetapa anterior para cada uma das outras três centrais, certificando-se de copiar o arquivo RCF correspondente para a central correspondente.

3. Verifique em cada switch se o arquivo RCF está presente no diretório bootflash de cada switch:

   `dir bootflash:`

   O exemplo a seguir mostra que os arquivos estão presentes no 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. Configure as regiões TCAM nos switches Cisco 3132Q-V e Cisco 3232C.

   Ignore esta etapa se você não tiver switches Cisco 3132Q-V ou Cisco 3232C.

   a. No interrutor Cisco 3132Q-V, defina as seguintes regiões 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. No switch Cisco 3232C, defina as seguintes regiões 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. Depois de definir as regiões TCAM, salve a configuração e recarregue o switch:

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

5. Copie o arquivo RCF correspondente do flash de inicialização local para a configuração em execução em cada switch:

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

6. Copie os arquivos RCF da configuração em execução para a configuração de inicialização em cada switch:

   `copy running-config startup-config`

   Você deve ver saída semelhante ao seguinte:

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

7. Recarregue o interrutor:

   `reload`

```
IP_switch_A_1# reload
```

8. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Definição de correção de erro de avanço para sistemas que utilizam conetividade de 25 Gbps

Se o sistema estiver configurado usando conetividade de 25 Gbps, você precisará definir manualmente o parâmetro Correção de erros de Avanço (fec) para Desativado após a aplicação do arquivo RCF. O ficheiro RCF não aplica esta definição.

Sobre esta tarefa

As portas de 25 Gbps devem ser cabeadas antes de executar este procedimento.

"Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C"

Esta tarefa aplica-se apenas a plataformas que utilizam conetividade de 25 Gbps:

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

Esta tarefa deve ser executada em todos os quatro switches na configuração IP do MetroCluster.

Passos

1. Defina o parâmetro fec como Desligado em cada porta de 25 Gbps conetada a um módulo de controladora e copie a configuração em execução para a configuração de inicialização:

   a. Entre no modo de configuração: `config t`

   b. Especifique a interface de 25 Gbps para configurar: `interface interface-ID`

   c. Defina fec para Off (Desligado): `fec off`

   d. Repita as etapas anteriores para cada porta de 25 Gbps no switch.

   e. Sair do modo de configuração: `exit`

   O exemplo a seguir mostra os comandos da interface Ethernet1/25/1 no 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. Repita a etapa anterior nos outros três switches na configuração IP do MetroCluster.

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identificar as portas ISL e os canais de portas não utilizados:

```
show interface brief
```

2. Desative as portas ISL e os canais de portas não utilizados.

   Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

```
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.
```

Configure a criptografia MACsec em switches Cisco 9336C

A criptografia MACsec só pode ser aplicada às portas ISL WAN.

Configure a criptografia MACsec em switches Cisco 9336C

Você só deve configurar a criptografia MACsec nas portas ISL WAN executadas entre os sites. Você deve configurar o MACsec depois de aplicar o arquivo RCF correto.

Requisitos de licenciamento para MACsec

MACsec requer uma licença de segurança. Para obter uma explicação completa do esquema de licenciamento do Cisco NX-os e como obter e solicitar licenças, consulte a. "Guia de licenciamento do Cisco NX-os"

Habilite ISLs WAN de criptografia MACsec Cisco em configurações IP MetroCluster

Você pode ativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

```
configure terminal
```

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

2. Ativar MACsec e MKA no dispositivo:

```
feature macsec
```

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

3. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

Configure uma cadeia de chaves e chaves MACsec

Você pode criar uma cadeia de chaves MACsec ou chaves em sua configuração.

Key Lifetime e Hitless Key Rollover

Um chaveiro MACsec pode ter várias chaves pré-compartilhadas (PSKs), cada uma configurada com um ID de chave e uma vida útil opcional. Uma vida útil da chave especifica a hora em que a chave ativa e expira. Na ausência de uma configuração vitalícia, o tempo de vida padrão é ilimitado. Quando uma vida útil é configurada, o MKA passa para a próxima chave pré-compartilhada configurada no chaveiro após a expiração da vida útil. O fuso horário da chave pode ser local ou UTC. O fuso horário padrão é UTC. Uma chave pode rolar para uma segunda chave dentro do mesmo chaveiro se você configurar a segunda chave (no chaveiro) e configurar uma vida útil para a primeira chave. Quando o tempo de vida da primeira tecla expira, ela passa automaticamente para a próxima chave na lista. Se a mesma chave for configurada em ambos os lados do link ao mesmo tempo, a rolagem da chave será sem hitless (ou seja, a chave rolará sem interrupção de tráfego).

Passos

1. Entre no modo de configuração global:

   `configure terminal`

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

2. Para ocultar a cadeia de carateres octeto de chave criptografada, substitua a cadeia por um caractere curinga na saída `show running-config` dos comandos e `show startup-config`:

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

> A cadeia de carateres octeto também é oculta quando você salva a configuração em um arquivo.

   Por padrão, as chaves PSK são exibidas em formato criptografado e podem ser facilmente descriptografadas. Este comando aplica-se apenas às cadeias de chaves MACsec.

3. Crie uma cadeia de chaves MACsec para manter um conjunto de chaves MACsec e entrar no modo de configuração da cadeia de chaves MACsec:

`key chain name macsec`

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

4. Crie uma chave MACsec e entre no modo de configuração da chave MACsec:

   `key key-id`

   O intervalo é de 1 a 32 carateres de chave de dígitos hexadecimais e o tamanho máximo é de 64 carateres.

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

5. Configure a cadeia de carateres octeto para a chave:

   `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
```

   O argumento octet-string pode conter até 64 carateres hexadecimais. A chave octeto é codificada internamente, portanto a chave em texto claro não aparece na saída do `show running-config macsec` comando.

6. Configure uma vida útil de envio para a chave (em segundos):

   `send-lifetime start-time duration duration`

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

   Por padrão, o dispositivo trata a hora de início como UTC. O argumento de hora de início é a hora do dia e a data em que a chave se torna ativa. O argumento duração é o comprimento do tempo de vida em segundos. A duração máxima é de 2147483646 segundos (aproximadamente 68 anos).

7. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

8. Exibe a configuração do keychain:

   `show key chain name`

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

Configurar uma política MACsec

Passos

1. Entre no modo de configuração global:

   `configure terminal`

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

2. Criar uma política MACsec:

   `macsec policy name`

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

3. Configure uma das seguintes cifras, 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. Configure a prioridade do servidor de chaves para quebrar o vínculo entre pares durante uma troca de chaves:

   `key-server-priority number`

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

5. Configure a política de segurança para definir o processamento de dados e pacotes de controle:

   `security-policy security policy`

   Escolha uma política de segurança das seguintes opções:

   - Must-Secure — os pacotes que não transportam cabeçalhos MACsec são descartados

- Should-secure - pacotes que não transportam cabeçalhos MACsec são permitidos (este é o valor padrão)

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

6. Configure a janela de proteção de repetição para que a interface protegida não aceite um pacote que seja menor do que o tamanho da janela configurado: `window-size number`

   O tamanho da janela de proteção de repetição representa o máximo de quadros fora de sequência que o MACsec aceita e não são descartados. O intervalo é de 0 a 596000000.

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

7. Configure o tempo em segundos para forçar um SAK rechavear:

   `sak-expiry-time time`

   Você pode usar este comando para alterar a chave da sessão para um intervalo de tempo previsível. A predefinição é 0.

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

8. Configure uma das seguintes compensações de confidencialidade no quadro da camada 2 onde a criptografia começa:

   `conf-offsetconfidentiality offset`

   Escolha entre as seguintes opções:

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

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

   Esse comando pode ser necessário para que os switches intermediários usem cabeçalhos de pacotes (dmac, smac, etype) como tags MPLS.

9. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

10. Apresentar a configuração da política MACsec:

    `show macsec policy`

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

Ative a criptografia Cisco MACsec nas interfaces

1. Entre no modo de configuração global:

    `configure terminal`

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

2. Selecione a interface que você configurou com criptografia MACsec.

    Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

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

3. Adicione o chaveiro e a política a serem configurados na interface para adicionar a configuração MACsec:

    `macsec keychain keychain-name policy policy-name`

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

4. Repita as etapas 1 e 2 em todas as interfaces onde a criptografia MACsec deve ser configurada.
5. Copie a configuração em execução para a configuração de inicialização:

    `copy running-config startup-config`

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

Desative os ISLs de WAN de criptografia Cisco MACsec em configurações IP do MetroCluster

Talvez seja necessário desativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

`configure terminal`

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

2. Desative a configuração MACsec no dispositivo:

`macsec shutdown`

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

Selecionar a opção "não" restaura o recurso MACsec.

3. Selecione a interface que você já configurou com o MACsec.

Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

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

4. Remova o chaveiro e a política configurados na interface para remover a configuração MACsec:

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

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

5. Repita as etapas 3 e 4 em todas as interfaces onde o MACsec está configurado.
6. Copie a configuração em execução para a configuração de inicialização:

`copy running-config startup-config`

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

Verificando a configuração do MACsec

Passos

1. Repita **All** dos procedimentos anteriores no segundo switch dentro da configuração para estabelecer uma sessão MACsec.
2. Execute os seguintes comandos para verificar se ambos os switches estão criptografados com êxito:
   a. Executar: `show macsec mka summary`
   b. Executar: `show macsec mka session`

c. Executar: `show macsec mka statistics`

Você pode verificar a configuração do MACsec usando os seguintes comandos:

Comando	Exibe informações sobre…
`show macsec mka session interface typeslot/port number`	A sessão MACsec MKA para uma interface específica ou para todas as interfaces
`show key chain name`	A configuração da cadeia de chaves
`show macsec mka summary`	A configuração MACsec MKA
`show macsec policy policy-name`	A configuração para uma política MACsec específica ou para todas as políticas MACsec

Configure o switch NVIDIA IP SN2100

Você deve configurar os switches IP NVIDIA SN2100 para uso como interconexão de cluster e para conetividade IP MetroCluster de back-end.

Reponha o switch NVIDIA IP SN2100 para os padrões de fábrica

Você pode escolher entre os seguintes métodos para redefinir um switch para as configurações padrão de fábrica.

- Reponha o interrutor utilizando a opção de ficheiro RCF
- Baixe e instale o software Cumulus

Reponha o switch usando a opção de arquivo RCF

Antes de instalar uma nova configuração RCF, você deve reverter as configurações do switch NVIDIA.

Sobre esta tarefa

Para restaurar o switch para as configurações padrão, execute o arquivo RCF com a `restoreDefaults` opção. Esta opção copia os ficheiros de cópia de segurança originais para a sua localização original e, em seguida, reinicia o interrutor. Após a reinicialização, o switch fica online com a configuração original que existia quando você executou o arquivo RCF pela primeira vez para configurar o switch.

Os seguintes detalhes de configuração não são redefinidos:

- Configuração de usuário e credencial
- Configuração da porta de rede de gerenciamento, eth0

Todas as outras alterações de configuração que ocorrem durante a aplicação do ficheiro RCF são revertidas para a configuração original.

Antes de começar

- Tem de configurar o interrutor de acordo Baixe e instale o arquivo NVIDIA RCFcom . Se não tiver configurado desta forma ou tiver configurado funcionalidades adicionais antes de executar o ficheiro RCF, não pode utilizar este procedimento.
- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch com uma conexão de console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Verifique se a configuração do RCF foi aplicada com sucesso com a mesma ou uma versão de arquivo RCF compatível e se os arquivos de backup existem.

   A saída pode mostrar arquivos de backup, arquivos preservados ou ambos. Se arquivos de backup ou arquivos preservados não aparecerem na saída, você não poderá usar este procedimento.

```
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. Execute o arquivo RCF com a opção para restaurar os padrões: `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. Responda "sim" ao prompt. O interrutor reverte para a configuração original e reinicializa.
4. Aguarde até que o switch seja reiniciado.

   O switch é redefinido e mantém a configuração inicial, como configuração de rede de gerenciamento e credenciais atuais, conforme existiam antes de aplicar o arquivo RCF. Após a reinicialização, você pode aplicar uma nova configuração usando a mesma ou uma versão diferente do arquivo RCF.

Baixe e instale o software Cumulus

Sobre esta tarefa

Siga estas etapas se você quiser redefinir completamente o switch aplicando a imagem Cumulus.

Antes de começar

- Você deve estar conetado ao switch com uma conexão de console serial.
- A imagem do software Cumulus switch é acessível através de HTTP.

> Para obter mais informações sobre a instalação do Cumulus Linux, consulte "Visão geral da instalação e configuração dos switches NVIDIA SN2100"

- Você deve ter a senha raiz para `sudo` acesso aos comandos.

Passos

1. A partir do download do console Cumulus e coloque em fila a instalação do software do switch com o comando `onie-install -a -i` seguido do caminho do arquivo para o software do switch:

   Neste exemplo, o arquivo de firmware `cumulus-linux-4.4.3-mlx-amd64.bin` é copiado do servidor HTTP '50.50.50.50' para o switch 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. Responda `y` ao aviso para confirmar a instalação quando a imagem é transferida e verificada.
3. Reinicie o switch para instalar o novo software: `sudo reboot`

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

> O interrutor reinicia e entra na instalação do software do interrutor, o que demora algum tempo. Quando a instalação estiver concluída, o interrutor reinicializa e permanece no prompt de 'login'.

4. Configure as definições básicas do interrutor
   a. Quando o switch é inicializado e no prompt de login, faça login e altere a senha.

> O nome de usuário é 'Cumulus' e a senha padrão é '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. Configure a interface de rede de gerenciamento.

   Os comandos que você usa dependem da versão do firmware do switch que você está executando.

   > Os comandos de exemplo a seguir configuram o nome do host como IP_switch_A_1, o endereço IP como 10.10.10.10, a máscara de rede como 255.255.255.0 (24) e o endereço de gateway como 10.10.10.1.

Cumulus 4,4.x

Os comandos de exemplo a seguir configuram o nome do host, endereço IP, máscara de rede e gateway em um switch executando 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 e posterior

Os comandos de exemplo a seguir configuram o nome de host, endereço IP, máscara de rede e gateway em um switch executando Cumulus 5,4.x. ou posterior.

```
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. Reinicie o switch usando o `sudo reboot` comando.

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

Quando o switch for reinicializado, você poderá aplicar uma nova configuração usando as etapas em Baixe e instale o arquivo NVIDIA RCF.

Baixe e instale os arquivos RCF do NVIDIA

Você deve gerar e instalar o arquivo RCF do switch em cada switch na configuração IP do MetroCluster.

Antes de começar

- Você deve ter a senha raiz para `sudo` acesso aos comandos.
- O software do switch está instalado e a rede de gerenciamento está configurada.
- Você seguiu os passos para instalar inicialmente o switch usando o método 1 ou o método 2.
- Você não aplicou nenhuma configuração adicional após a instalação inicial.

> Se efetuar uma configuração adicional depois de reiniciar o comutador e antes de aplicar o ficheiro RCF, não poderá utilizar este procedimento.

Sobre esta tarefa

Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster (nova instalação) ou no comutador de substituição (substituição do comutador).

Passos

1. Gerar os arquivos RCF do NVIDIA para MetroCluster IP.
   a. Faça download do "RcfFileGenerator para MetroCluster IP".
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.
   c. Navegue para o seu diretório inicial. Se você estiver logado como 'Cumulus', o caminho do arquivo é `/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. Transfira o ficheiro RCF para este diretório. O exemplo a seguir mostra que você usa SCP para baixar o arquivo `SN2100_v2.0.0_IP_switch_A_1.txt` do servidor '50.50.50.50' para o diretório principal e salvá-lo como `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. Execute o arquivo RCF. O arquivo RCF requer uma opção para aplicar uma ou mais etapas. A menos que instruído pelo suporte técnico, execute o arquivo RCF sem a opção de linha de comando. Para verificar o estado de conclusão dos vários passos do ficheiro RCF, utilize a opção '-1' ou 'All' para aplicar todos os passos (pendentes).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3
SN2100_v2.0.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

3. Se a sua configuração utilizar cabos DAC, ative a opção DAC nas portas do switch:

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

O exemplo a seguir ativa a opção DAC para a porta `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. Reinicie o switch depois de ativar a opção DAC nas portas do switch:

```
sudo reboot
```

> Ao definir a opção DAC para várias portas de switch, você só precisa reiniciar o switch uma vez.

Defina a velocidade da porta do switch para as interfaces IP do MetroCluster

Sobre esta tarefa

Use este procedimento para definir a velocidade da porta do switch para 100g para os seguintes sistemas:

- AFF A70
- AFF A90
- AFF A1K

Passo

1. Utilize o ficheiro RCF com a `runCmd` opção para definir a velocidade. Isso aplica a configuração e salva a configuração.

   Os comandos a seguir definem a velocidade para as interfaces MetroCluster `swp7` e `swp8`:

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

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

   Exemplo

   ```
   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:~$
   ```

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identifique as portas ISL e os canais de portas não utilizados usando o banner de arquivo RCF:

   > Se a porta estiver no modo de divisão, o nome da porta que você especificar no comando pode ser diferente do nome indicado no banner RCF. Você também pode usar os arquivos de cabeamento RCF para encontrar o nome da porta.

   ```
   net show interface
   ```

2. Desative as portas ISL e os canais de portas não utilizados usando o arquivo 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:~$
```

O seguinte comando de exemplo desativa a porta "swp14":

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

Repita esta etapa para cada porta ou canal de porta não utilizado identificado.

Configurar switches IP MetroCluster para monitoramento de integridade

Nas configurações IP do MetroCluster, você pode configurar o SNMPv3 para monitorar a

integridade dos switches IP.

Passo 1: Configure o usuário SNMPv3 em switches IP MetroCluster

Siga as etapas a seguir para configurar o usuário SNMPv3 nos switches IP do MetroCluster.

Você deve usar os protocolos de autenticação e privacidade nos comandos. O uso de autenticação sem privacidade não é suportado.

Para switches IP Broadcom

Passos

1. Se o grupo de utilizadores 'network-admin' ainda não existir, crie-o:

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

2. Confirme se o grupo 'network-admin' foi criado:

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

3. Configure o usuário SNMPv3 em switches IP Broadcom:

```
(IP_switch_1)# config
(IP_switch_1) (Config)# snmp-server user <user_name> network-admin
auth-sha priv-aes128
```

Digite a senha de autenticação quando solicitado.

```
#snmp-server user admin1 network-admin auth-sha priv-aes128

Enter Authentication Password:
```

Para switches IP Cisco

Passos

1. Execute os seguintes comandos para configurar o usuário SNMPv3 em um switch IP Cisco:

```
IP_switch_A_1 # configure terminal
IP_switch_A_1 (config) # snmp-server user <user_name>  auth
[md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
```

2. Verifique se o usuário SNMPv3 está configurado no switch:

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

A saída de exemplo a seguir mostra que o usuário `admin` está configurado para SNMPv3:

```
IP_switch_A_1(config)# show snmp user admin
User                 Auth      Priv(enforce) Groups
acl_filter

____                 ____      _____________ ______
__________

admin                md5       aes-128(no)   network-admin
```

Passo 2: Configure o usuário SNMPv3 no ONTAP

Siga as etapas a seguir para configurar o usuário SNMPv3 no ONTAP.

1. Configure o usuário SNMPv3 no ONTAP:

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

2. Configure a monitorização do estado do comutador para monitorizar o comutador utilizando o novo utilizador SNMPv3:

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

3. Verifique se o número de série do dispositivo que será monitorado com o usuário SNMPv3 recém-criado está correto:
   a. Apresentar o período de tempo de polling da monitorização do estado do interrutor:

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

   b. Execute o seguinte comando após o período de tempo de polling ter decorrido:

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

Informações sobre direitos autorais

Informações sobre marcas comerciais