



MetroCluster IP 스위치를 구성합니다

ONTAP MetroCluster

NetApp
February 13, 2026

목차

| | |
|---|----|
| MetroCluster IP 스위치를 구성합니다 | 1 |
| 올바른 MetroCluster IP 스위치 구성 절차를 선택하세요 | 1 |
| 클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 Broadcom IP 스위치 구성 | 1 |
| Broadcom IP 스위치를 출하 시 기본값으로 재설정합니다 | 1 |
| Broadcom 스위치 EFOS 소프트웨어 다운로드 및 설치 | 6 |
| Broadcom RCF 파일 다운로드 및 설치 | 13 |
| 사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다 | 17 |
| Cisco IP 스위치를 구성합니다 | 18 |
| 클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 Cisco IP 스위치 구성 | 18 |
| MetroCluster IP 사이트의 Cisco 9336C 스위치에서 MACsec 암호화 구성 | 33 |
| NVIDIA IP 스위치를 구성합니다 | 40 |
| 클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 NVIDIA IP SN2100 스위치 구성 | 40 |
| NVIDIA SN2100 MetroCluster IP 스위치용 이더넷 스위치 상태 모니터 구성 파일을 설치합니다 | 53 |

MetroCluster IP 스위치를 구성합니다

올바른 MetroCluster IP 스위치 구성 절차를 선택하세요

백엔드 MetroCluster IP 연결을 제공하도록 IP 스위치를 구성해야 합니다. 따라야 할 절차는 스위치 공급업체에 따라 다릅니다.

- "Broadcom IP 스위치를 구성합니다"
- "Cisco IP 스위치를 구성합니다"
- "NVIDIA IP 스위치를 구성합니다"

클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 Broadcom IP 스위치 구성

클러스터 상호 연결 및 백엔드 MetroCluster IP 연결에 사용할 Broadcom IP 스위치를 구성해야 합니다.



다음과 같은 경우 구성에 추가 라이선스(6 x 100-Gb 포트 라이선스)가 필요합니다.

- 포트 53과 54를 40Gbps 또는 100Gbps MetroCluster ISL로 사용합니다.
- 로컬 클러스터와 MetroCluster 인터페이스를 포트 49-52에 연결하는 플랫폼을 사용합니다.

Broadcom IP 스위치를 출하 시 기본값으로 재설정합니다

새 스위치 소프트웨어 버전과 RCFs를 설치하기 전에 Broadcom 스위치 설정을 지우고 기본 구성을 수행해야 합니다.

이 작업에 대해

- MetroCluster IP 구성의 각 IP 스위치에서 이 단계를 반복해야 합니다.
- 직렬 콘솔을 사용하여 스위치에 연결해야 합니다.
- 이 작업은 관리 네트워크의 구성을 재설정합니다.

단계

1. 상승된 권한의 명령 프롬프트('#')로 변경합니다

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

2. 시작 구성을 지우고 배너를 제거합니다

a. 시작 구성을 지웁니다.

- '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) #
```

+ 이 명령은 배너를 지우지 않습니다.

b. 배너 제거:

"세트 피너 없음" *

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

3. 스위치를 재부팅합니다. * `(ip_switch_a_1) #reload` *

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



스위치를 다시 로드하기 전에 저장되지 않은 구성이나 변경된 구성을 저장할지 묻는 메시지가 나타나면 * No * 를 선택합니다.

4. 스위치가 다시 로드될 때까지 기다린 다음 스위치에 로그인합니다.

기본 사용자는 ""admin""이고 암호가 설정되어 있지 않습니다. 다음과 유사한 프롬프트가 표시됩니다.

```
(Routing) >
```

5. 상승된 권한의 명령 프롬프트로 변경합니다.

"활성화"를 선택합니다

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

6. service port protocol을 none으로 설정한다.

'저빙항프로토콜 없음

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

(Routing) #
```

7. IP 주소를 서비스 포트에 할당합니다.

```
'erviceport IP_IP-addressnetmaskgateway_'
```

다음 예에서는 서브넷 "255.255.255.0" 및 게이트웨이 "10.10.10.1"이 있는 서비스 포트에 할당된 IP 주소 "10.10.10.10"을 보여 줍니다.

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

8. 서비스 포트가 올바르게 구성되었는지 확인합니다.

서비스서비스

다음 예에서는 포트가 작동 가능하며 올바른 주소가 할당되었음을 보여 줍니다.

```
(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:bddf: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. SSH 서버를 구성합니다.



- RCF 파일은 텔넷 프로토콜을 비활성화합니다. SSH 서버를 구성하지 않으면 직렬 포트 연결을 통해서만 브리지에 액세스할 수 있습니다.
- 로그 수집 및 기타 외부 도구를 사용하려면 SSH 서버를 구성해야 합니다.

a. RSA 키를 생성합니다.

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

b. DSA 키 생성(선택 사항)

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

c. FIPS 호환 버전의 EFOS를 사용하는 경우 ECDSA 키를 생성합니다. 다음 예제에서는 길이가 521인 키를 만듭니다. 유효한 값은 256, 384 또는 521입니다.

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

d. SSH 서버를 활성화합니다.

필요한 경우 구성 컨텍스트를 종료합니다.

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

+



키가 이미 있으면 덮어쓸지 묻는 메시지가 나타날 수 있습니다.

10. 필요한 경우 도메인 및 이름 서버를 구성합니다.

'설정'을 클릭합니다

다음 예에서는 IP domain과 IP name server 명령을 보여 줍니다.

```
(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. 필요한 경우 시간대 및 시간 동기화(SNTP)를 구성합니다.

다음 예에서는 SNTP 서버의 IP 주소와 상대 시간대 등을 지정하는 'sntp' 명령어를 보여준다.

```
(Routing) #
(Routing) (Config)#ntp client mode unicast
(Routing) (Config)#ntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

EFOS 버전 3.10.0.3 이상에서는 를 사용합니다 ntp 명령을 입력합니다.

```
> (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. 스위치 이름 구성:

호스트 이름 IP_SWITCH_A_1

스위치 프롬프트에는 새 이름이 표시됩니다.

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. 구성을 저장합니다.

쓰기 메모리

다음 예와 유사한 프롬프트 및 출력이 표시됩니다.

```
(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. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

Broadcom 스위치 EFOS 소프트웨어 다운로드 및 설치

MetroCluster IP 구성의 각 스위치에 스위치 운영 체제 파일과 RCF 파일을 다운로드해야 합니다.

이 작업에 대해

이 작업은 MetroCluster IP 구성의 각 스위치에서 반복해야 합니다.

- 다음 사항에 유의하십시오. *
- EFOS 3.4.x.x에서 EFOS 3.7.x.x 이상으로 업그레이드할 경우 스위치에서 EFOS 3.4.4.6(또는 이후 3.4.x.x 릴리즈)이 실행되고 있어야 합니다. 그 전에 릴리즈를 실행 중인 경우 먼저 스위치를 EFOS 3.4.4.6(또는 그 이상 3.4.x.x 릴리즈)로 업그레이드한 다음 스위치를 EFOS 3.7.x.x 이상으로 업그레이드하십시오.
- EFOS 3.4.x.x 및 3.7.x.x 이상의 구성은 다릅니다. EFOS 버전을 3.4.x.x에서 3.7.x.x 이상으로 변경하거나 그 반대로 변경하려면 스위치를 출고 시 기본값으로 재설정하고 해당 EFOS 버전의 RCF 파일을 (다시) 적용해야 합니다. 이 절차를 수행하려면 직렬 콘솔 포트를 통해 액세스해야 합니다.
- EFOS 버전 3.7.x.x 이상부터는 FIPS를 준수하지 않는 버전과 FIPS 호환 버전을 사용할 수 있습니다. FIPS를 준수하지 않는 버전에서 로 이동하거나 FIPS를 준수하는 버전으로 전환할 때 다른 단계가 적용됩니다. FIPS를 준수하지 않는 버전에서 FIPS를 준수하는 버전으로 또는 그 반대로 EFOS를 변경하면 스위치가 공장 출하 시 기본값으로 재설정됩니다. 이 절차를 수행하려면 직렬 콘솔 포트를 통해 액세스해야 합니다.

단계

1. 에서 스위치 펌웨어를 "[Broadcom 지원 사이트](#)" 다운로드합니다.
2. 'show FIPS status' 명령을 사용하여 사용자의 EFOS 버전이 FIPS 호환 버전인지 또는 비 FIPS 호환 버전인지 확인합니다. 다음 예에서는 IP_SWITCH_A_1이 FIPS 호환 EFOS를 사용하고 있으며 IP_SWITCH_A_2는 FIPS 비호환 EFOS를 사용하고 있습니다.

◦ 예 1 *

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

◦ 예 2 *

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

IP_switch_A_2 #
```

3. 다음 표를 사용하여 어떤 방법을 따라야 하는지 확인하십시오.

| * 절차 * | * 현재 EFOS 버전 * | * 새로운 EFOS 버전 * | * 고급 단계 * |
|---|---|---|---|
| FIPS를 준수하지 않는 두 버전 간에 EFOS를 업그레이드하는 단계 | 3.4.x.x | 3.4.x.x | 방법 1을 사용하여 새 EFOS 이미지 설치) 구성 및 라이선스 정보가 보존됩니다 |
| 3.4.4.6(또는 그 이상 3.4.x.x) | 3.7.x.x 이상 비 FIPS 규격 | 방법 1을 사용하여 EFOS를 업그레이드합니다. 스위치를 출고 시 기본값으로 재설정하고 EFOS 3.7.x.x 이상에 RCF 파일을 적용합니다 | 3.7.x.x 이상 비 FIPS 규격 |
| 3.4.4.6(또는 그 이상 3.4.x.x) | 방법 1을 사용하여 EFOS를 다운그레이드합니다. 스위치를 출고 시 기본값으로 재설정하고 EFOS 3.4.x.x의 RCF 파일을 적용합니다 | 3.7.x.x 이상 비 FIPS 규격 | |
| 방법 1을 사용하여 새 EFOS 이미지를 설치합니다. 구성 및 라이선스 정보가 유지됩니다 | 3.7.x.x 이상 FIPS 규격 | 3.7.x.x 이상 FIPS 규격 | 방법 1을 사용하여 새 EFOS 이미지를 설치합니다. 구성 및 라이선스 정보가 유지됩니다 |

| | | | |
|----------------------------|----------|---------|---|
| FIPS 호환 EFOS 버전으로 업그레이드 단계 | FIPS 비호환 | FIPS 규격 | 방법 2를 사용하여 EFOS 이미지 설치 스위치 구성 및 라이선스 정보가 손실됩니다. |
|----------------------------|----------|---------|---|

- 방법 1: 백업 부팅 파티션에 소프트웨어 이미지를 다운로드하여 EFOS를 업그레이드하는 단계입니다
- 방법 2: ONIE OS 설치를 사용하여 EFOS를 업그레이드하는 단계

백업 부팅 파티션에 소프트웨어 이미지를 다운로드하여 **EFOS**를 업그레이드하는 단계입니다

두 EFOS 버전이 FIPS를 준수하지 않거나 두 EFOS 버전이 모두 FIPS를 준수하는 경우에만 다음 단계를 수행할 수 있습니다.



한 버전이 FIPS를 준수하고 다른 버전이 FIPS를 준수하지 않는 경우 이 단계를 사용하지 마십시오.

단계

1. 스위치 소프트웨어를 스위치에 복사합니다. (+ copy sftp://user@50.50.50.50 /switchsoftware/efos-3.4.4.6.stk backup+)

이 예에서 efos-3.4.4.6.stk 운영 체제 파일은 SFTP 서버에서 50.50.50으로 백업 파티션으로 복사됩니다. TFTP/SFTP 서버의 IP 주소와 설치해야 하는 RCF 파일의 파일 이름을 사용해야 합니다.

```
(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. 다음 스위치 재부팅의 백업 파티션에서 부팅하도록 스위치를 설정합니다.

부팅 시스템 백업

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

(IP_switch_A_1) #
```

3. 새 부팅 이미지가 다음 부팅 시 활성화되는지 확인합니다.

'How bootvar'입니다

```
(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. 구성을 저장합니다.

쓰기 메모리

```
(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. 스위치를 재부팅합니다.

다시 로드

```
(IP_switch_A_1) #reload
```

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

6. 스위치가 재부팅될 때까지 기다립니다.



드문 경우지만 스위치가 부팅되지 않을 수 있습니다. 를 따릅니다 [ONIE OS 설치를 사용하여 EFOS를 업그레이드하는 단계](#) 새 이미지를 설치합니다.

7. 스위치를 EFOS 3.4.x.x에서 EFOS 3.7.x.x로 변경하거나 그 반대로 변경할 경우 다음 두 절차를 따라 올바른 구성(RCF)을 적용하십시오.

- a. [Broadcom IP 스위치를 출하 시 기본값으로 재설정합니다](#)
- b. [Broadcom RCF 파일 다운로드 및 설치](#)

8. MetroCluster IP 구성의 나머지 3개 IP 스위치에 대해 이 단계를 반복합니다.

ONIE OS 설치를 사용하여 EFOS를 업그레이드하는 단계

한 EFOS 버전이 FIPS를 준수하고 다른 EFOS 버전이 FIPS를 준수하지 않는 경우 다음 단계를 수행할 수 있습니다. 이러한 단계는 스위치가 부팅되지 않는 경우 ONIE에서 비 FIPS 또는 FIPS 호환 EFOS 3.7.x.x 이미지를 설치하는 데 사용할 수 있습니다.

단계

1. 스위치를 ONIE 설치 모드로 부팅합니다.

부팅 중에 다음 화면이 나타나면 ONIE를 선택합니다.

```

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

```

"ONIE"를 선택하면 스위치가 로드되고 다음 선택 사항이 표시됩니다.

```

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

```

이제 스위치가 ONIE 설치 모드로 부팅됩니다.

2. ONIE 검색을 중지하고 이더넷 인터페이스를 구성합니다

다음 메시지가 나타나면 <ENTER> 키를 눌러 ONIE 콘솔을 호출합니다.

```

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

```



ONIE 검색이 계속 진행되어 메시지가 콘솔에 인쇄됩니다.

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

3. 이더넷 인터페이스를 구성하고 'ifconfig eth0 <IPAddress> netmask <netmask> up' 및 'route add default GW <gatewayAddress>'를 사용하여 라우트를 추가합니다

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

4. ONIE 설치 파일을 호스팅하는 서버에 연결할 수 있는지 확인합니다.

```
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. 새 스위치 소프트웨어를 설치합니다

```
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.
```

소프트웨어가 설치되고 스위치를 재부팅합니다. 스위치가 새 EFOS 버전으로 정상적으로 재부팅되도록 합니다.

6. 새 스위치 소프트웨어가 설치되었는지 확인합니다

'How 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. 설치를 완료합니다

구성이 적용되지 않고 스위치가 재부팅되고 출하 시 기본값으로 재설정됩니다. 다음 두 절차에 따라 스위치 기본 설정을 구성하고 다음 두 문서에 설명된 대로 RCF 파일을 적용합니다.

- 스위치 기본 설정을 구성합니다. 4단계 이후 단계를 따릅니다. [Broadcom IP 스위치를 출하 시 기본값으로 재설정합니다](#)
- 에 설명된 대로 RCF 파일을 생성하고 적용합니다 [Broadcom RCF 파일 다운로드 및 설치](#)

Broadcom RCF 파일 다운로드 및 설치

스위치 RCF 파일을 생성하고 MetroCluster IP 구성의 각 스위치에 설치해야 합니다.

시작하기 전에

이 작업에는 FTP, TFTP, SFTP 또는 SCP와 같은 파일 전송 소프트웨어가 필요합니다. 스위치에 파일을 복사합니다.

이 작업에 대해

이러한 단계는 MetroCluster IP 구성의 각 IP 스위치에서 반복해야 합니다.

RCF 파일은 MetroCluster IP 구성의 4개 스위치당 하나씩 4개의 파일로 구성됩니다. 사용 중인 스위치 모델에 적합한 RCF 파일을 사용해야 합니다.

| 스위치 | RCF 파일 |
|---------------|---------------------|
| 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 |



EFOS 버전 3.4.4.6 이상 3.4.x.x.x용 RCF 파일 릴리즈 버전과 EFOS 버전 3.7.0.4는 다릅니다. 스위치가 실행 중인 EFOS 버전에 맞는 RCF 파일을 생성했는지 확인해야 합니다.

| EFOS 버전입니다 | RCF 파일 버전 |
|------------|--------------|
| 3.4.x.x | v1.3x, v1.4x |
| 3.7.x.x | V2.x |

단계

1. MetroCluster IP용 Broadcom RCF 파일을 생성합니다.
 - a. 를 다운로드하십시오 "[MetroCluster IP용 RcfFileGenerator입니다](#)"
 - b. MetroCluster IP용 RcfFileGenerator를 사용하여 구성에 대한 RCF 파일을 생성합니다.



다운로드 후 RCF 파일을 수정할 수 없습니다.

2. RCF 파일을 스위치에 복사합니다.
 - a. RCF 파일을 첫 번째 스위치에 복사합니다. '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'

이 예에서 "BES-53248_v1.32_Switch-A1.txt" RCF 파일은 SFTP 서버에서 "50.50.50"의 로컬 bootflash로 복사됩니다. TFTP/SFTP 서버의 IP 주소와 설치해야 하는 RCF 파일의 파일 이름을 사용해야 합니다.

```
(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. RCF 파일이 스크립트로 저장되었는지 확인합니다.

'스크립트 목록'

```
(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. RCF 스크립트 적용:

'cript 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. 구성을 저장합니다.

쓰기 메모리

```
(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. 스위치를 재부팅합니다.

다시 로드

```
(IP_switch_A_1) #reload

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

a. 일치하는 RCF 파일을 해당 스위치에 복사하도록 나머지 세 스위치 각각에 대해 이전 단계를 반복합니다.

3. 스위치를 다시 로드하십시오.

다시 로드

```
IP_switch_A_1# reload
```

4. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다

불필요한 상태 경고를 방지하기 위해 사용하지 않는 ISL 포트 및 포트 채널을 비활성화하는 것이 좋습니다 NetApp.

1. RCF 파일 배너를 사용하여 사용되지 않는 ISL 포트 및 포트 채널을 식별합니다.



포트가 브레이크아웃 모드인 경우 명령에서 지정하는 포트 이름은 RCF 배너에 지정된 이름과 다를 수 있습니다. RCF 케이블 연결 파일을 사용하여 포트 이름을 찾을 수도 있습니다.

ISL 포트 세부 정보를 참조하십시오

명령을 실행합니다 show port all.

포트 채널 세부 정보는 을 참조하십시오

명령을 실행합니다 show port-channel all.

2. 사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다.

식별된 미사용 포트 또는 포트 채널에 대해 다음 명령을 실행해야 합니다.

```
(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
```

Cisco IP 스위치를 구성합니다

클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 Cisco IP 스위치 구성

클러스터 인터커넥트 및 백엔드 MetroCluster IP 연결에 사용할 Cisco IP 스위치를 구성해야 합니다.

이 작업에 대해

이 섹션의 절차 중 일부는 독립 절차이며, 사용자가 직접 수행했거나 작업과 관련된 절차만 실행해야 합니다.

Cisco IP 스위치를 출하 시 기본값으로 재설정합니다

RCF 파일을 설치하기 전에 Cisco 스위치 구성을 지우고 기본 구성을 수행해야 합니다. 이전 설치가 실패한 후 동일한 RCF 파일을 다시 설치하거나 새 버전의 RCF 파일을 설치하려는 경우 이 절차가 필요합니다.

이 작업에 대해

- MetroCluster IP 구성의 각 IP 스위치에서 이 단계를 반복해야 합니다.
- 직렬 콘솔을 사용하여 스위치에 연결해야 합니다.
- 이 작업은 관리 네트워크의 구성을 재설정합니다.

단계

1. 스위치를 출하 시 기본값으로 재설정합니다.

a. 기존 구성을 지웁니다.

쓰기 지우기

b. 스위치 소프트웨어를 다시 로드합니다.

다시 로드

시스템이 재부팅되고 구성 마법사가 시작됩니다. 부팅 중에 "자동 프로비저닝 중단"이라는 메시지가 표시되면 일반 설정으로 계속 진행하시겠습니까? (예/아니요) [n]", 계속하려면 "예"라고 답해야 합니다.

c. 구성 마법사에서 기본 스위치 설정을 입력합니다.

- 관리자 암호입니다
- 스위치 이름
- 대역외 관리 구성
- 기본 게이트웨이
- SSH 서비스(RSA)

구성 마법사를 완료하면 스위치가 재부팅됩니다.

d. 메시지가 표시되면 사용자 이름과 암호를 입력하여 스위치에 로그인합니다.

다음 예에서는 스위치를 구성할 때 프롬프트 및 시스템 응답을 보여 줍니다. 꺾쇠 괄호(<<<<)는 사용자가 정보를 입력하는 위치를 표시합니다.

```
---- 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.
```

스위치 이름, 관리 주소 및 게이트웨이를 포함하여 다음 프롬프트 세트에 기본 정보를 입력하고 SSH with RSA를 선택합니다.

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. 구성을 저장합니다.

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

3. 스위치를 재부팅하고 스위치가 다시 로드될 때까지 기다립니다.

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

4. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

Cisco 스위치 NX-OS 소프트웨어 다운로드 및 설치

MetroCluster IP 구성의 각 스위치에 스위치 운영 체제 파일과 RCF 파일을 다운로드해야 합니다.

이 작업에 대해

이 작업에는 FTP, TFTP, SFTP 또는 SCP와 같은 파일 전송 소프트웨어가 필요합니다. 스위치에 파일을 복사합니다.

이러한 단계는 MetroCluster IP 구성의 각 IP 스위치에서 반복해야 합니다.

지원되는 스위치 소프트웨어 버전을 사용해야 합니다.

["NetApp Hardware Universe를 참조하십시오"](#)

단계

1. 지원되는 NX-OS 소프트웨어 파일을 다운로드합니다.

["Cisco 소프트웨어 다운로드"](#)

2. 스위치 소프트웨어를 스위치에 복사합니다.

```
'copy sftp://root@server-ip-address/tftpboot/nx-os-file-name bootflash:vrf management'
```

이 예에서 nxos.7.0.3.l4.6.bin 파일과 EPLD 이미지는 SFTP 서버 10.10.99.99에서 로컬 부트플래시로 복사됩니다.

```

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. 각 스위치에서 스위치 NX-OS 파일이 각 스위치의 bootflash 디렉토리에 있는지 확인합니다.

```
'dir bootflash:'
```

다음 예제는 파일이 IP_SWITCH_A_1에 있음을 보여줍니다.

```

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. 스위치 소프트웨어를 설치합니다.

nxos bootflash: nxos.version-number.bin을 모두 설치합니다

스위치 소프트웨어가 설치되면 스위치는 자동으로 다시 로드(재부팅)됩니다.

다음 예에서는 IP_SWITCH_A_1에 설치된 소프트웨어를 보여 줍니다.

```

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. 스위치가 다시 로드될 때까지 기다린 다음 스위치에 로그인합니다.

스위치가 재부팅되면 로그인 프롬프트가 표시됩니다.

```
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. 스위치 소프트웨어가 설치되어 있는지 확인합니다

다음 예는 출력을 보여줍니다.

```
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. EPLD 이미지를 업그레이드하고 스위치를 reboot한다.

```

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.

```

- 스위치 재부팅 후 다시 로그인하여 새 버전의 EPLD가 성공적으로 로드되었는지 확인합니다.

```
show version module 1 epld
```

- MetroCluster IP 구성의 나머지 3개 IP 스위치에 대해 이 단계를 반복합니다.

Cisco IP RCF 파일 다운로드 및 설치

MetroCluster IP 구성의 각 스위치에 RCF 파일을 생성하고 설치해야 합니다.

이 작업에 대해

이 작업에는 FTP, TFTP, SFTP 또는 SCP와 같은 파일 전송 소프트웨어가 필요합니다. 스위치에 파일을 복사합니다.

이러한 단계는 MetroCluster IP 구성의 각 IP 스위치에서 반복해야 합니다.

지원되는 스위치 소프트웨어 버전을 사용해야 합니다.

["NetApp Hardware Universe를 참조하십시오"](#)

QSFP-SFP+ 어댑터를 사용하는 경우 ISL 포트를 브레이크아웃 속도 모드 대신 기본 속도 모드로 구성해야 할 수 있습니다. ISL 포트 속도 모드를 확인하려면 스위치 공급업체의 설명서를 참조하십시오.

RCF 파일은 MetroCluster IP 구성의 4개 스위치당 하나씩 4개의 파일로 구성됩니다. 사용 중인 스위치 모델에 적합한 RCF 파일을 사용해야 합니다.

| 스위치 | RCF 파일 |
|---------------|----------------------------|
| 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 |

단계

1. MetroCluster IP에 대한 Cisco RCF 파일을 생성합니다.
 - a. 를 다운로드하십시오 ["MetroCluster IP용 RcfFileGenerator입니다"](#)
 - b. MetroCluster IP용 RcfFileGenerator를 사용하여 구성에 대한 RCF 파일을 생성합니다.



다운로드 후 RCF 파일을 수정할 수 없습니다.

2. RCF 파일을 스위치에 복사합니다.
 - a. RCF 파일을 첫 번째 스위치에 복사합니다.

복사 `sftp://root@ftp-server-ip-address/tftpboot/switch-specific-bootRCF flash:vrf management`

이 예에서 NX3232_v1.80_Switch-A1.txt RCF 파일은 SFTP 서버(10.10.99.99)에서 로컬 bootflash로 복사됩니다. TFTP/SFTP 서버의 IP 주소와 설치해야 하는 RCF 파일의 파일 이름을 사용해야 합니다.

```

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. 일치하는 RCF 파일을 해당 스위치에 복사하도록 나머지 세 스위치 각각에 대해 이전 하위 단계를 반복합니다.
3. 각 스위치에서 RCF 파일이 각 스위치의 bootflash 디렉토리에 있는지 확인합니다.

'dir bootflash:'

다음 예제는 파일이 IP_SWITCH_A_1에 있음을 보여줍니다.

```

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. Cisco 3132Q-V 및 Cisco 3232C 스위치에서 TCAM 영역을 구성합니다.



Cisco 3132Q-V 또는 Cisco 3232C 스위치가 없는 경우 이 단계를 건너뛰십시오.

- a. Cisco 3132Q-V 스위치에서 다음 TCAM 영역을 설정합니다.

```
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. Cisco 3232C 스위치에서 다음 TCAM 영역을 설정합니다.

```
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. TCAM 영역을 설정한 후 구성을 저장하고 스위치를 다시 로드합니다.

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

5. 로컬 bootflash에서 각 스위치의 실행 구성으로 일치하는 RCF 파일을 복사합니다.

bootflash: switch-specific-RCF.txt running-config를 복사합니다

6. RCF 파일을 실행 중인 구성에서 각 스위치의 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

다음과 유사한 출력이 표시됩니다.

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

7. 스위치를 다시 로드하십시오.

다시 로드

```
IP_switch_A_1# reload
```

8. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

25Gbps 연결을 사용하는 시스템에 대한 Forward Error Correction 설정

시스템이 25Gbps 연결을 사용하여 구성된 경우 RCF 파일을 적용한 후 FEC(Forward Error Correction) 매개변수를 수동으로 OFF로 설정해야 합니다. RCF 파일은 이 설정을 적용하지 않습니다.

이 작업에 대해

이 절차를 수행하기 전에 25Gbps 포트를 케이블로 연결해야 합니다.

"Cisco 3232C 또는 Cisco 9336C 스위치에 대한 플랫폼 포트 할당"

이 작업은 25Gbps 연결을 사용하는 플랫폼에만 적용됩니다.

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

이 작업은 MetroCluster IP 구성의 4개 스위치 모두에서 수행해야 합니다.

단계

1. 컨트롤러 모듈에 연결된 각 25Gbps 포트에서 FEC 매개변수를 OFF로 설정한 다음 실행 중인 구성을 시작 구성으로 복사합니다.
 - a. 설정 모드 'config t'로 진입한다
 - b. 구성할 25Gbps interface를 지정한다:'interface-id'
 - c. FEC를 OFF: FEC OFF로 설정한다
 - d. 스위치의 각 25Gbps 포트에 대해 이전 단계를 반복합니다.
 - e. 설정 모드 종료: '종료'

다음 예에서는 스위치 IP_SWITCH_A_1의 인터페이스 Ethernet1/25/1에 대한 명령을 보여 줍니다.

```
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. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다

불필요한 상태 경고를 방지하기 위해 사용하지 않는 ISL 포트 및 포트 채널을 비활성화하는 것이 좋습니다 NetApp.

1. 사용되지 않는 ISL 포트 및 포트 채널 식별:

인터페이스 요약

2. 사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다.

식별된 미사용 포트 또는 포트 채널에 대해 다음 명령을 실행해야 합니다.

```
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.
```

MetroCluster IP 사이트의 Cisco 9336C 스위치에서 MACsec 암호화 구성



MACsec 암호화는 WAN ISL 포트에만 적용할 수 있습니다.

Cisco 9336C 스위치에서 MACsec 암호화를 구성합니다

사이트 간에 실행되는 WAN ISL 포트에서만 MACsec 암호화를 구성해야 합니다. 올바른 RCF 파일을 적용한 후 MACsec을 구성해야 합니다.

MACsec에 대한 라이선스 요구 사항

MACsec에는 보안 라이선스가 필요합니다. Cisco NX-OS 라이선스 체계에 대한 전체 설명 및 라이선스 취득 및 적용 방법은 [참조하십시오 "Cisco NX-OS 라이선스 가이드 를 참조하십시오"](#)

MetroCluster IP 구성에서 Cisco MACsec 암호화 WAN ISL을 활성화합니다

MetroCluster IP 구성에서 WAN ISL의 Cisco 9336C 스위치에 대해 MACsec 암호화를 설정할 수 있습니다.

단계

1. 글로벌 구성 모드 시작:

'터미널 구성'을 선택합니다

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

2. 장치에서 MACsec 및 MKA 활성화:

피처 MACsec

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

3. 실행 중인 구성을 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

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

MACsec 키 체인 및 키를 구성합니다

구성에 MACsec 키 체인 또는 키를 만들 수 있습니다.

- 키 수명 및 Hitless 키 롤오버 *

MACsec 키 체인은 미리 공유된 여러 키(PSK)를 가질 수 있으며, 각 키는 키 ID와 수명(옵션)으로 구성됩니다. 키 수명은 키가 활성화되고 만료되는 시간을 지정합니다. 수명 구성이 없을 경우 기본 수명은 무제한입니다. 수명이 구성되면 MKA는 수명이 만료된 후 키체인에 구성된 다음 사전 공유 키로 롤오버합니다. 키의 표준 시간대는 로컬 또는 UTC입니다. 기본 표준 시간대는 UTC입니다. 두 번째 키(키 체인)를 구성하고 첫 번째 키의 수명을 구성하면 동일한 키 체인 내의 두 번째 키로 키를 롤오버할 수 있습니다. 첫 번째 키의 수명이 만료되면 목록의 다음 키로 자동 롤오버됩니다. 같은 키가 링크의 양쪽에서 동시에 구성된 경우 키 롤오버는 무단위(즉, 키가 트래픽 중단 없이 롤오버됨)입니다.

단계

1. 글로벌 구성 모드로 들어갑니다.

'터미널 구성'을 선택합니다

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

2. 암호화된 키 옥텟 문자열을 숨기려면 'show running-config' 및 'show startup-config' 명령의 출력에서 문자열을 와일드카드 문자로 바꿉니다.

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



설정을 파일에 저장할 때 옥텟 문자열도 숨겨집니다.

기본적으로 PSK 키는 암호화된 형식으로 표시되며 쉽게 해독할 수 있습니다. 이 명령은 MACsec 키 체인에만 적용됩니다.

3. MACsec 키 세트를 보류하고 MACsec 키 체인 구성 모드로 전환하기 위해 MACsec 키 체인을 생성합니다.

키 체인 이름 MACsec

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

4. MACsec 키를 만들고 MACsec 키 구성 모드를 입력합니다.

키 ID

범위는 1 ~ 32자의 16진수 키 문자열이며 최대 크기는 64자입니다.

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

5. 키에 대한 옥텟 문자열을 구성합니다.

'key-octet-string octet-string 암호화 알고리즘 AES_128_CMAC|AES_256_CMAC'

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



8진수 문자열 인수는 최대 64자의 16진수 문자를 포함할 수 있습니다. 옥텟키는 내부적으로 인코딩되므로 'show running-config MACsec' 명령의 출력에는 일반 텍스트의 키가 나타나지 않는다.

6. 키의 전송 수명 구성(초):

'수명 종료 시작-시간 지속 기간'을 선택합니다

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

기본적으로 장치는 시작 시간을 UTC로 처리합니다. start-time 인수는 키가 활성화되는 날짜와 시간입니다. duration 인수는 초 단위의 수명 길이입니다. 최대 길이는 2147483646초(약 68년)입니다.

7. 실행 중인 구성을 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

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

8. 키 체인 구성을 표시합니다.

키 체인 이름

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

MACsec 정책을 구성합니다

단계

1. 글로벌 구성 모드 시작:

'터미널 구성'을 선택합니다

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

2. MACsec 정책 만들기:

'macsec policy name'입니다

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

3. GCM-AES-128, GCM-AES-256, GCM-AES-XPB-128 또는 GCM-AES-XPB-256 중 하나를 구성합니다.

암호-스위트 이름

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

4. 키 교환 중에 피어 간의 연결을 끊도록 키 서버 우선 순위를 구성합니다.

키-서버-우선 순위 번호

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

5. 데이터 처리 및 제어 패킷을 정의할 수 있도록 보안 정책을 구성합니다.

보안정책

다음 옵션 중에서 보안 정책을 선택합니다.

- 필수 보안 — MACsec 헤더를 전달하지 않는 패킷은 삭제됩니다
- 보안 — MACsec 헤더를 전달하지 않는 패킷이 허용됩니다(기본값).

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

6. 보안된 인터페이스가 설정된 윈도우 크기보다 작은 패킷을 허용하지 않도록 재생 보호 윈도우를 설정한다



재생 보호 창 크기는 MACsec이 수락하고 폐기하지 않는 최대 시퀀스 초과 프레임을 나타냅니다. 범위는 0에서 596000000 사이입니다.

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

7. SAK 키를 강제로 다시 입력하다

'AK-expiry-time'입니다

이 명령을 사용하여 세션 키를 예측 가능한 시간 간격으로 변경할 수 있습니다. 기본값은 0입니다.

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

8. 암호화가 시작되는 계층 2 프레임에서 다음 기밀 오프셋 중 하나를 구성합니다.

'conf-offset기밀성 오프셋'

다음 옵션 중에서 선택합니다.

- conf-offset-0.
- conf-offset-30
- conf-offset-50.

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



이 명령은 MPLS 태그와 같은 패킷 헤더(dmac, smac, etype)를 사용하기 위해 중간 스위치에 필요할 수 있습니다.

9. 실행 중인 구성을 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

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

10. MACsec 정책 구성을 표시합니다.

마초 정책

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

인터페이스에서 **Cisco MACsec** 암호화를 활성화합니다

1. 글로벌 구성 모드 시작:

'터미널 구성'을 선택합니다

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

2. MACsec 암호화로 구성된 인터페이스를 선택합니다.

인터페이스 유형 및 ID를 지정할 수 있습니다. 이더넷 포트의 경우 이더넷 슬롯/포트를 사용합니다.

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

3. 인터페이스에서 구성할 키 체인 및 정책을 추가하여 MACsec 구성을 추가합니다.

macsec keychain-name policy-name'입니다

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

4. MACsec 암호화를 구성할 모든 인터페이스에서 1단계와 2단계를 반복합니다.
5. 실행 중인 구성을 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

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

MetroCluster IP 구성에서 **Cisco MACsec** 암호화 **WAN ISL**을 비활성화합니다

MetroCluster IP 구성에서 WAN ISL의 Cisco 9336C 스위치에 대한 MACsec 암호화를 비활성화해야 할 수 있습니다.

단계

1. 글로벌 구성 모드 시작:

'터미널 구성'을 선택합니다

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

2. 장치에서 MACsec 구성 비활성화:

'시스템 종료'

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



""아니오"" 옵션을 선택하면 MACsec 기능이 복원됩니다.

3. MACsec로 이미 구성한 인터페이스를 선택합니다.

인터페이스 유형 및 ID를 지정할 수 있습니다. 이더넷 포트의 경우 이더넷 슬롯/포트를 사용합니다.

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

4. MACsec 구성을 제거하기 위해 인터페이스에 구성된 키 체인 및 정책을 제거합니다.

MACsec keychain keychain-name policy-name 없음

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

5. MACsec이 구성된 모든 인터페이스에서 3단계와 4단계를 반복합니다.

6. 실행 중인 구성을 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

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

MACsec 구성을 확인하는 중입니다

단계

1. MACsec 세션을 설정하려면 구성 내 두 번째 스위치에 대한 이전 절차의 *ALL* 을 반복합니다.

2. 다음 명령을 실행하여 두 스위치가 모두 성공적으로 암호화되었는지 확인합니다.

- a. 'How MACsec MKA summary'를 실행합니다
- b. 'How MACsec MKA SESSION'을 실행하십시오
- c. 'How MACsec MKA statistics'를 실행합니다

다음 명령을 사용하여 MACsec 구성을 확인할 수 있습니다.

| | |
|----|-------------------|
| 명령 | 다음에 대한 정보를 표시합니다. |
|----|-------------------|

| | |
|---|--|
| 'How MACsec MKA session interface typeslot/port number' | 특정 인터페이스 또는 모든 인터페이스에 대한 MACsec MKA 세션 |
| 키 체인 이름 | 키 체인 구성 |
| '하세초 MKA 요약 정보 | MACsec MKA 구성 |
| 마초 정책 정책 이름 | 특정 MACsec 정책 또는 모든 MACsec 정책의 구성 |

NVIDIA IP 스위치를 구성합니다

클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 NVIDIA IP SN2100 스위치 구성

클러스터 인터커넥트 및 백엔드 MetroCluster IP 연결에 사용할 NVIDIA SN2100 IP 스위치를 구성해야 합니다.

NVIDIA IP SN2100 스위치를 출하 시 기본값으로 재설정합니다

다음 방법 중 하나를 선택하여 스위치를 공장 출하시 기본 설정으로 재설정할 수 있습니다.

- [RCF 파일 옵션을 사용하여 스위치를 재설정합니다](#)
- [Cumulus 소프트웨어를 다운로드하고 설치합니다](#)

RCF 파일 옵션을 사용하여 스위치를 재설정합니다

새 RCF 구성을 설치하기 전에 NVIDIA 스위치 설정을 되돌려야 합니다.

이 작업에 대해

스위치를 기본 설정으로 복원하려면 RestoreDefaults 옵션을 사용하여 RCF 파일을 실행합니다. 이 옵션은 원래 백업된 파일을 원래 위치로 복사한 다음 스위치를 재부팅합니다. 재부팅 후, 스위치는 RCF 파일을 처음 실행하여 스위치를 구성할 때 있던 원래 구성과 함께 온라인 상태로 제공됩니다.

다음 구성 세부 정보는 재설정되지 않습니다.

- 사용자 및 자격 증명 구성
- 관리 네트워크 포트 eth0 구성



RCF 파일을 적용하는 동안 발생하는 다른 모든 구성 변경은 원래 구성으로 되돌려집니다.

시작하기 전에

- 예 따라 스위치를 구성해야 합니다 [NVIDIA RCF 파일을 다운로드하고 설치합니다](#). 이 방법으로 를 구성하지 않았거나 RCF 파일을 실행하기 전에 추가 기능을 구성한 경우 이 절차를 사용할 수 없습니다.
- MetroCluster IP 구성의 각 IP 스위치에서 이 단계를 반복해야 합니다.
- 직렬 콘솔 연결을 사용하여 스위치에 연결해야 합니다.

- 이 작업은 관리 네트워크의 구성을 재설정합니다.

단계

1. RCF 구성이 동일하거나 호환되는 RCF 파일 버전으로 성공적으로 적용되었으며 백업 파일이 있는지 확인하십시오.



출력에는 백업 파일, 보존된 파일 또는 이 두 가지 모두가 표시될 수 있습니다. 백업 파일 또는 보존된 파일이 출력에 표시되지 않으면 이 절차를 사용할 수 없습니다.

```

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. RCF 파일을 실행하여 기본값 복원: RestoreDefaults 옵션을 사용합니다

```

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. 프롬프트에 '예'로 응답합니다. 스위치가 원래 구성으로 되돌아가고 재부팅됩니다.
4. 스위치가 재부팅될 때까지 기다립니다.

RCF 파일을 적용하기 전에 스위치가 재설정되고 관리 네트워크 구성 및 현재 자격 증명과 같은 초기 구성이 그대로 유지됩니다. 재부팅 후 동일한 또는 다른 버전의 RCF 파일을 사용하여 새 구성을 적용할 수 있습니다.

Cumulus 소프트웨어를 다운로드하고 설치합니다

이 작업에 대해

Cumulus 이미지를 적용하여 스위치를 완전히 재설정하려면 다음 단계를 사용하십시오.

시작하기 전에

- 직렬 콘솔 연결을 사용하여 스위치에 연결해야 합니다.
- Cumulus 스위치 소프트웨어 이미지는 HTTP를 통해 액세스할 수 있습니다.



Cumulus Linux 설치에 대한 자세한 내용은 [여기](#)를 참조하십시오 **"NVIDIA SN2100 스위치의 설치 및 구성 개요"**

- 명령에 대한 'SUDO'에 대한 루트 암호가 있어야 합니다.

단계

1. Cumulus 콘솔에서 스위치 소프트웨어 설치를 "onie-install-a-i" 명령과 함께 스위치 소프트웨어의 파일 경로를 다운로드하고 대기하십시오.

이 예에서는 펌웨어 파일입니다 cumulus-linux-4.4.3-mlx-amd64.bin HTTP 서버 '50.50.50.50'에서 로컬 스위치로 복사됩니다.

```

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. 이미지 다운로드 및 확인 시 설치 확인을 위해 프롬프트에 "y"를 응답합니다.
3. 스위치를 재부팅하여 새 소프트웨어 'SUDO 재부팅'을 설치합니다

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



스위치가 재부팅되고 스위치 소프트웨어 설치 상태로 전환되며, 이 과정에서 시간이 다소 소요됩니다. 설치가 완료되면 스위치가 재부팅되고 '로그인' 메시지가 표시됩니다.

4. 기본 스위치 설정을 구성합니다
 - a. 스위치가 부팅되고 로그인 프롬프트에서 로그인하고 암호를 변경합니다.



사용자 이름은 'cumulus'이고 기본 암호는 'cumulus'입니다.

```
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. 관리 네트워크 인터페이스를 구성합니다.

사용하는 명령은 실행 중인 스위치 펌웨어 버전에 따라 다릅니다.



다음 예제 명령에서는 호스트 이름을 IP_SWITCH_A_1로, IP 주소는 10.10.10.10으로, 넷마스크 255.255.255.0(24), 게이트웨이 주소는 10.10.10.10.1로 구성합니다.

Cumulus 4.4.x입니다

다음 명령은 Cumulus 4.4.x를 실행하는 스위치에서 호스트 이름, IP 주소, 넷마스크 및 게이트웨이를 구성합니다

```
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 이상

다음 명령은 Cumulus 5.4.x를 실행하는 스위치에서 호스트 이름, IP 주소, 넷마스크 및 게이트웨이를 구성합니다 이상.

```

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. 'SUDO reboot' 명령어를 사용하여 스위치를 reboot 한다.

```

cumulus@cumulus:~$ sudo reboot

```

스위치가 재부팅되면 의 단계를 사용하여 새 구성을 적용할 수 있습니다 [NVIDIA RCF 파일을 다운로드하고 설치합니다.](#)

[[다운로드 및 설치]] NVIDIA RCF 파일을 다운로드하여 설치합니다

스위치 RCF 파일을 생성하고 MetroCluster IP 구성의 각 스위치에 설치해야 합니다.

시작하기 전에

- 명령에 대한 'SUDO'에 대한 루트 암호가 있어야 합니다.
- 스위치 소프트웨어가 설치되고 관리 네트워크가 구성됩니다.
- 방법 1 또는 방법 2를 사용하여 스위치를 처음 설치하는 단계를 따랐습니다.
- 초기 설치 후 추가 구성을 적용하지 않았습니다.



스위치를 재설정 후 RCF 파일을 적용하기 전에 추가 구성을 수행할 경우 이 절차를 사용할 수 없습니다.

이 작업에 대해

MetroCluster IP 구성(새 설치) 또는 교체 스위치(스위치 교체)의 각 IP 스위치에 대해 이러한 단계를 반복해야 합니다.

QSFP-SFP+ 어댑터를 사용하는 경우 ISL 포트를 브레이크아웃 속도 모드 대신 기본 속도 모드로 구성해야 할 수 있습니다. ISL 포트 속도 모드를 확인하려면 스위치 공급업체의 설명서를 참조하십시오.

단계

1. MetroCluster IP용 NVIDIA RCF 파일을 생성합니다.
 - a. 를 다운로드합니다 "[MetroCluster IP용 RcfFileGenerator입니다.](#)"
 - b. MetroCluster IP용 RcfFileGenerator를 사용하여 구성에 사용할 RCF 파일을 생성합니다.

c. 홈 디렉토리로 이동합니다. '누적'으로 기록되면 파일 경로는 '/home/cumulus'입니다.

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

d. RCF 파일을 이 디렉토리에 다운로드합니다. 다음 예에서는 SCP를 사용하여 파일을 다운로드하는 방법을 보여 줍니다 SN2100_v2.0.0_IP_switch_A_1.txt 서버 '50.50.50.50'에서 홈 디렉토리로 이동한 후 로 저장합니다 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. RCF 파일을 실행합니다. RCF 파일에는 하나 이상의 단계를 적용하는 옵션이 필요합니다. 기술 지원 부서의 지시가 없는 한, RCF 파일을 명령줄 옵션 없이 실행합니다. RCF 파일의 다양한 단계 완료 상태를 확인하려면 '-1' 또는 '모두' 옵션을 사용하여 모든 단계(보류 중)를 적용합니다.

```

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. 구성에서 DAC 케이블을 사용하는 경우 스위치 포트에서 DAC 옵션을 활성화합니다.

```

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

```

다음 예에서는 포트에 대해 DAC 옵션을 활성화합니다 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. 스위치 포트에서 DAC 옵션을 활성화한 후 스위치를 재부팅합니다.

```
sudo reboot
```



여러 스위치 포트에 대해 DAC 옵션을 설정하면 스위치를 한 번만 재부팅하면 됩니다.

25Gbps 연결을 사용하는 시스템에 대해 Forward Error Correction(전달 오류 수정)을 설정합니다

25Gbps 연결을 사용하여 시스템을 구성한 경우 RCF를 적용한 후 FEC(Forward Error Correction) 매개변수를 OFF(꺼짐)로 수동으로 설정합니다. RCF는 이 설정을 적용하지 않습니다.

이 작업에 대해

- 이 작업은 25Gbps 연결을 사용하는 플랫폼에만 적용됩니다. 을 "[NVIDIA 지원 SN2100 IP 스위치를 위한 플랫폼 포트 할당](#)"참조하십시오.
- 이 작업은 MetroCluster IP 구성의 4개 스위치 모두에서 수행해야 합니다.
- 각 스위치 포트를 개별적으로 업데이트해야 하며 명령에서 여러 포트 또는 포트 범위를 지정할 수 없습니다.

단계

1. 25Gbps 연결을 사용하는 첫 번째 스위치 포트에 대해 매개 변수를 off로 설정합니다 fec.

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

2. 컨트롤러 모듈에 연결된 각 25Gbps 스위치 포트에 대해 이 단계를 반복합니다.

MetroCluster IP 인터페이스의 스위치 포트 속도를 설정합니다

이 작업에 대해

- 다음 시스템의 스위치 포트 속도를 100G로 설정하려면 다음 절차를 수행하십시오.
 - AFF A70, AFF A90, AFF A1K, AFF C80의 약어입니다
 - AFF A30, AFF C30, AFF A50, AFF C60의 약어입니다
 - FAS50, FAS70, FAS90
- 각 스위치 포트를 개별적으로 업데이트해야 하며 명령에서 여러 포트 또는 포트 범위를 지정할 수 없습니다.

단계

1. 속도를 설정하려면 옵션과 함께 RCF 파일을 runCmd 사용합니다. 이렇게 하면 설정이 적용되고 구성이 저장됩니다.

다음은 MetroCluster 인터페이스 및 의 속도를 설정하는 명령입니다. swp7 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
```

- 예 *

```

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:~$

```

사용되지 않는 **ISL** 포트 및 포트 채널을 비활성화합니다

불필요한 상태 경고를 방지하기 위해 사용하지 않는 ISL 포트 및 포트 채널을 비활성화하는 것이 좋습니다 NetApp. 각 포트 또는 포트 채널을 개별적으로 사용하지 않도록 설정해야 하며 명령에서 여러 포트 또는 포트 범위를 지정할 수 없습니다.

단계

1. RCF 파일 배너를 사용하여 사용되지 않는 ISL 포트 및 포트 채널을 식별합니다.



포트가 브레이크아웃 모드인 경우 명령에서 지정하는 포트 이름은 RCF 배너에 지정된 이름과 다를 수 있습니다. RCF 케이블 연결 파일을 사용하여 포트 이름을 찾을 수도 있습니다.

```
net show interface
```

2. RCF 파일을 사용하여 사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다.

```

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:~$

```

다음 명령 예에서는 "swp14" 포트를 비활성화합니다.

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

식별된 각 사용되지 않은 포트 또는 포트 채널에 대해 이 단계를 반복합니다.

NVIDIA SN2100 MetroCluster IP 스위치용 이더넷 스위치 상태 모니터 구성 파일을 설치합니다.

NVIDIA 이더넷 스위치에서 이더넷 스위치 상태 모니터링을 구성하려면 다음 절차를 따르세요.

이 지침은 NVIDIA X190006-PE 및 X190006-PI 스위치가 제대로 감지되지 않은 경우 적용되며 다음을 실행하여

확인할 수 있습니다. `system switch ethernet show` 모델에 *OTHER*가 표시되는지 확인하세요. NVIDIA 스위치 모델을 식별하려면 다음 명령을 사용하여 부품 번호를 찾으세요. `nv show platform hardware NVIDIA CL 5.8` 및 이전 버전용 또는 `nv show platform` 이후 버전용.



다음 ONTAP 릴리스에서 NVIDIA CL 5.11.x를 사용할 때 상태 모니터링 및 로그 수집이 의도한 대로 작동하도록 하려면 이 단계를 따르는 것이 좋습니다. 이 단계를 따르지 않아도 상태 모니터링 및 로그 수집이 작동할 수 있지만, 모든 것이 제대로 작동하는지 확인하려면 이 단계를 따르세요.

- 9.10.1P20, 9.11.1P18, 9.12.1P16, 9.13.1P8, 9.14.1, 9.15.1 및 이후 패치 릴리스

시작하기 전에

- ONTAP 클러스터가 작동 중이고 실행 중인지 확인합니다.
- CSHM에서 제공하는 모든 기능을 사용하려면 스위치에서 SSH를 활성화하세요.
- 모든 노드에서 디렉토리를 지웁니다 `/mroot/etc/cshm_nod/nod_sign/`.

- a. 노드 셸을 입력합니다.

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

- b. 고급 권한으로 변경:

```
priv set advanced
```

- c. 디렉터리의 구성 파일을 `/etc/cshm_nod/nod_sign` 나열합니다. 디렉터리가 있고 구성 파일이 포함되어 있으면 파일 이름이 나열됩니다.

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

- d. 연결된 스위치 모델에 해당하는 모든 구성 파일을 삭제합니다.

확실하지 않은 경우 위에 나열된 지원 모델에 대한 모든 구성 파일을 제거한 다음 해당 모델에 대한 최신 구성 파일을 다운로드하여 설치합니다.

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

- a. 삭제된 구성 파일이 더 이상 디렉터리에 없는지 확인합니다.

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

단계

1. 해당 ONTAP 릴리스 버전을 기반으로 이더넷 스위치 상태 모니터 구성 zip 파일을 다운로드합니다. 이 파일은 페이지에서 사용할 수 ["NVIDIA 이더넷 스위치"](#) 있습니다.
 - a. NVIDIA SN2100 소프트웨어 다운로드 페이지에서 * Nvidia CSHM File * 을 선택합니다.
 - b. 주의/읽어야 함 페이지에서 동의할 확인란을 선택합니다.
 - c. 최종 사용자 사용권 계약 페이지에서 동의할 확인란을 선택하고 * Accept & Continue * 를 클릭합니다.
 - d. Nvidia CSHM 파일 - 다운로드 페이지에서 해당 구성 파일을 선택합니다. 다음 파일을 사용할 수 있습니다.

ONTAP 9.15.1 이상

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

ONTAP 9.11.1 ~ 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. 해당 zip 파일을 내부 웹 서버에 업로드합니다.
2. 클러스터의 ONTAP 시스템 중 하나에서 고급 모드 설정에 액세스합니다.

세트 프리빌리지 고급

3. switch 상태 monitor configure 명령을 실행합니다.

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

4. 명령 출력이 ONTAP 버전에 대한 다음 텍스트로 끝나는지 확인합니다.

ONTAP 9.15.1 이상

이더넷 스위치 상태 모니터링이 구성 파일을 설치했습니다.

ONTAP 9.11.1 ~ 9.14.1

shm이 구성 파일을 설치했습니다.

ONTAP 9.10.1

CSHM 다운로드 패키지가 성공적으로 처리되었습니다.

오류가 발생하면 NetApp 지원 팀에 문의하십시오.

1. 다음 단계를 완료하기 전에 를 실행하여 찾은 이더넷 스위치 상태 모니터 폴링 간격을 최대 2배까지 기다립니다
system switch ethernet polling-interval show.
2. 명령을 실행하세요 system switch ethernet configure-health-monitor show ONTAP 시스템에서 클러스터 스위치가 모니터링 필드가 *True*로 설정되어 있고 일련 번호 필드에 *Unknown*이 표시되지 않는지 확인합니다.

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



구성 파일을 적용한 후에도 모델에 * 기타 * 가 계속 표시되면 NetApp 지원에 문의하십시오.

를 참조하십시오 "시스템 스위치 이더넷 구성-상태-모니터" 자세한 내용은 명령을 참조하세요.

다음 단계

"스위치 상태 모니터링을 구성합니다"..

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.