firepower Threat Defense 고가용성 문제 해결

목차

소개

firepower 이 문서에서는 FTD(Availability Threat Defense)에서 HA(High Availability)의 운영, 확인 및 문제 해결 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- FTD 및 ASA 플랫폼
- FTD 어플라이언스에서 패킷 캡처

이 문서에 설명된 개념을 더 잘 이해하려면 Firepower 컨피그레이션 가이드(Configuration Guide) Firepower 어플라이언스에서 FTD 고가용성 구성을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD
- Cisco FMC(Firepower 관리 센터)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

정보 및 예는 FTD를 기반으로 하지만 대부분의 개념은 ASA(Adaptive Security Appliance)에도 완벽하게 적용됩니다.

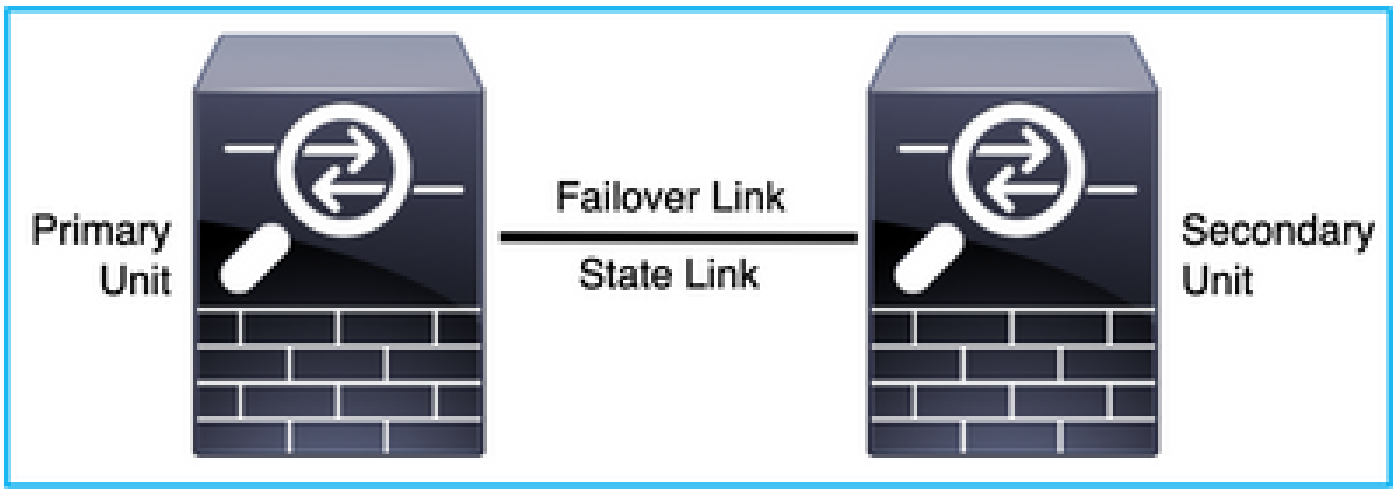
FTD는 두 가지 기본 관리 모드를 지원합니다.

- FMC를 통한 오프박스(off-box) - 원격 관리라고도 함
- FDM(Firepower 장치 관리자)을 통한 온박스 - 로컬 관리라고도 함

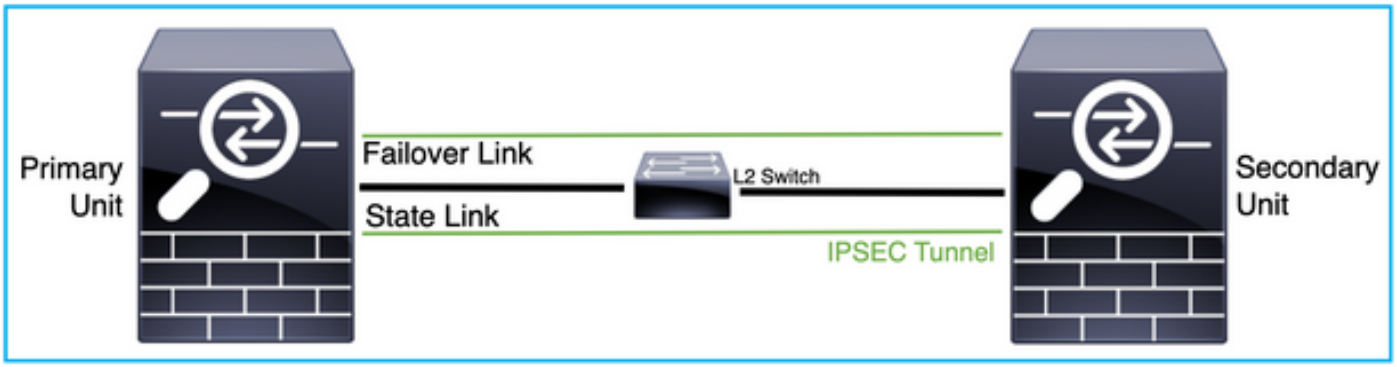
참고: FDM을 통해 관리되는 FTD는 Firepower 버전 코드 v6.3.0 이상에서 고가용성에 추가할 수 있습니다.

설계 옵션

FTD의 설계 관점에서 이 이미지에 표시된 것처럼 직접 연결할 수 있습니다.



또는 이 이미지에 표시된 대로 레이어 2(L2) 스위치를 통해 연결할 수 있습니다.



HA 용어

활성	활성 ASA는 모든 트래픽 흐름을 수신하고 모든 네트워크 트래픽을 필터링합니다. 컨피그레이션이 활성 ASA에서 변경됩니다.
HA 링크	장애 조치 쌍의 두 유닛은 장애 조치 링크를 통해 지속적으로 통신하면서 각 유닛의 운영 상태를 확인하고 컨피그레이션 변경 사항을 동기화합니다. 링크를 통해 공유되는 정보는 다음과 같습니다. • 유닛 상태(액티브 또는 스탠바이) • Hello 메시지(keep-alive) • 네트워크 링크 상태 • MAC 주소 교환 • 구성 복제 및 동기화
기본	HA를 생성할 때 일반적으로 먼저 구성되는 유닛입니다. 이 기능의 중요성은 ASA HA의 두 디바이스가 동일한 순간에 함께 작동되는 경우 기본 디바이스가 활성 역할을 맡는다는 것입니다.

보조	HA를 생성할 때 일반적으로 두 번째로 구성된 유닛입니다. 이 기능의 중요성은 ASA HA의 두 디바이스가 동일한 순간에 함께 작동하면 보조 디바이스가 대기 역할을 맡는다는 것입니다.
대기	스탠바이 ASA는 라이브 트래픽을 처리하지 않으며, 활성 디바이스의 연결 및 컨피그레이션을 동기화하며, 장애 조치 시 활성 역할을 수행합니다.
상태 링크	액티브 유닛은 상태 링크를 사용하여 연결 상태 정보를 스탠바이 디바이스에 전달합니다. 따라서 스탠바이 유닛에서는 특정 유형의 연결을 유지 관리할 수 있으며 사용자에게 영향을 주지 않습니다. 이 정보는 스탠바이 유닛이 장애 조치 발생 시 존재하는 연결을 유지하는 데 도움이 됩니다. NB: 장애 조치 및 상태 기반 장애 조치에 동일한 링크를 사용할 경우 인터페이스를 가장 잘 보존합니다. 그러나 대규모 컨피그레이션과 높은 트래픽 네트워크가 있는 경우 상태 링크 및 장애 조치 링크에 대한 전용 인터페이스를 고려해야 합니다. 스테이트풀 장애 조치 링크의 대역폭은 디바이스에서 데이터 인터페이스의 최대 대역폭과 일치해야 합니다.

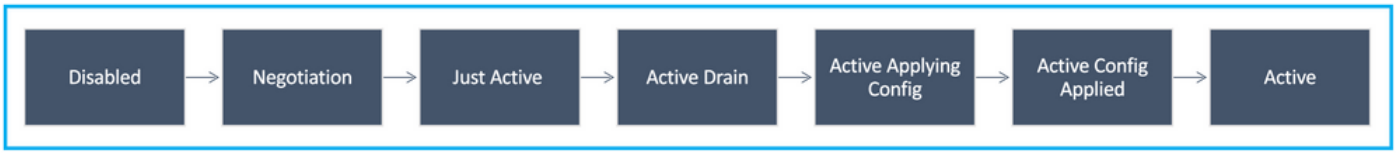
HA 상태

활성	디바이스는 현재 네트워크의 라이브 트래픽을 처리하며, 수행해야 하는 모든 컨피그레이션 변경 사항이 이 디바이스에서 수행됩니다.
앱 동기화	이 상태의 디바이스는 활성 디바이스의 컨피그레이션을 동기화합니다.
대량 동기화	이 상태의 디바이스는 활성 디바이스의 컨피그레이션을 동기화합니다.
비활성화됨	유닛의 장애 조치가 비활성화되었습니다(명령: 장애 조치 없음).
협상	디바이스가 활성 디바이스의 가용성을 확인하고 활성 디바이스가 대기 상태로 준비되지 않은 경우 활성 역할을 수행합니다.
스탠바이 준비	디바이스는 현재 트래픽을 처리하지 않지만 활성 디바이스에 상태 확인 문제가 표시되는 경우 활성 역할을 수행합니다.
동기화 구성	컨피그레이션이 액티브 디바이스에서 스탠바이 디바이스로 복제됩니다.
콜드 스탠바이	디바이스는 장애 조치 시 액티브 상태로 전환되지만 연결 이벤트를 복제하

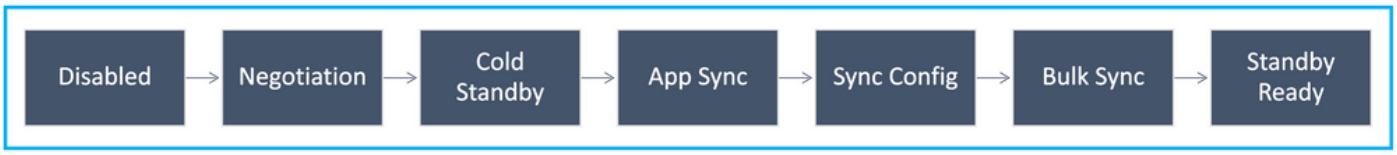
	지는 않습니다.

HA 상태 흐름도

기본(연결된 피어 없음):



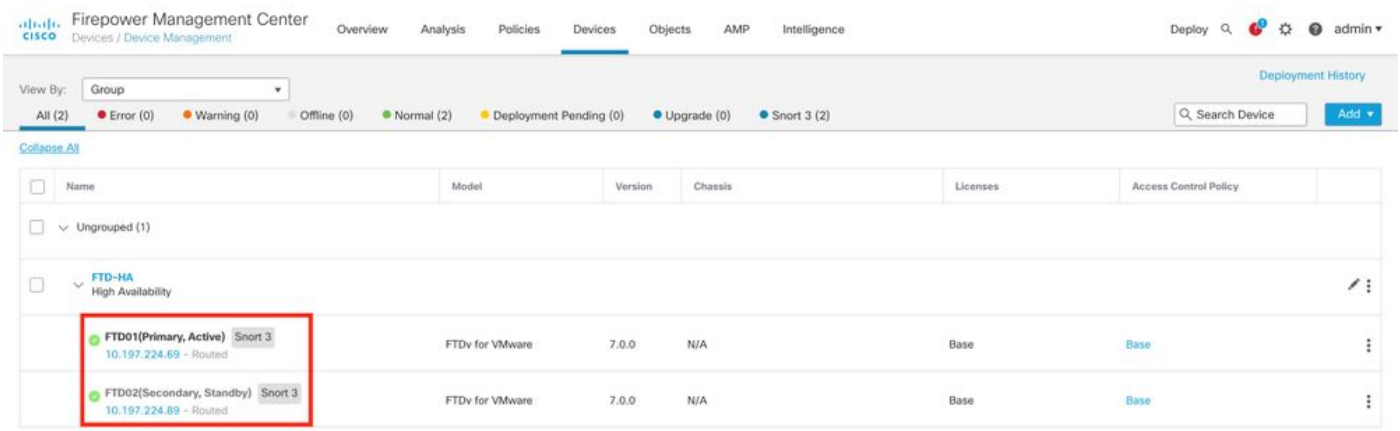
보조(활성 연결 피어 포함):



UI 확인

Firepower Management Center 관리 FTD HA

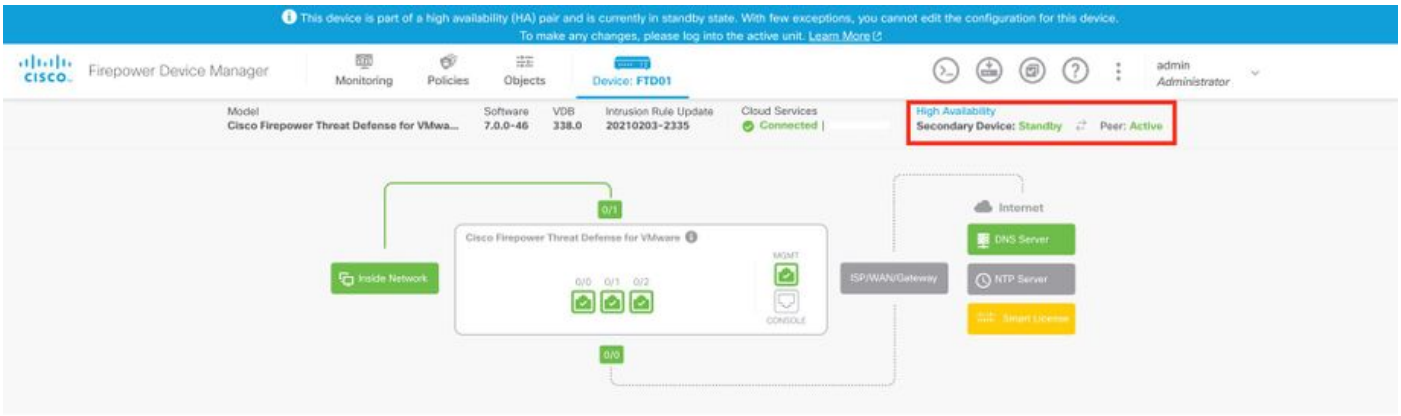
다음 이미지에 표시된 대로 Device > Device Management(디바이스 관리)로 이동하면 FMC UI에서 FTD HA 상태를 확인할 수 있습니다.



FDM 관리 FTD HA

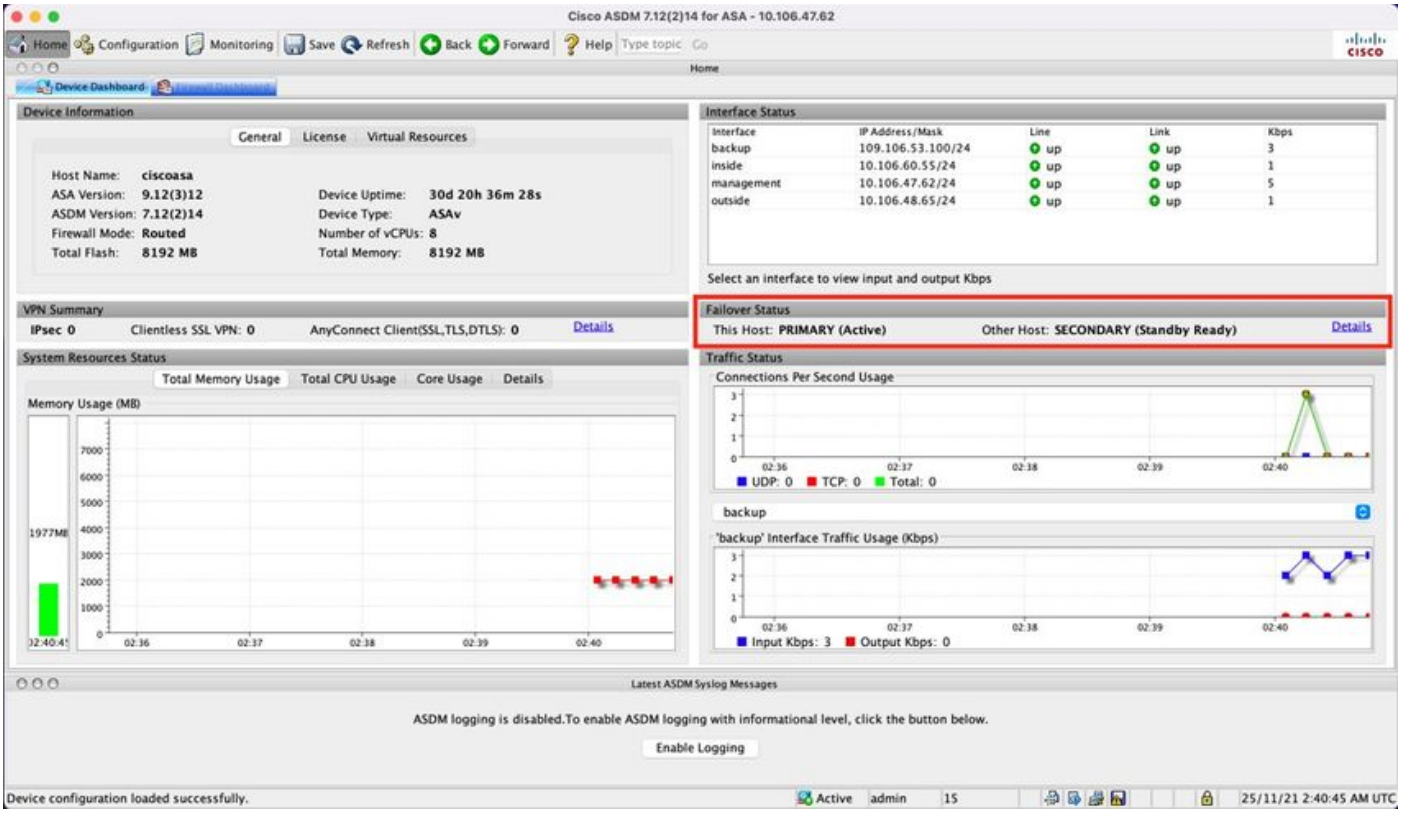
기본 FDM 개요 페이지:

보조 FDM 개요 페이지:

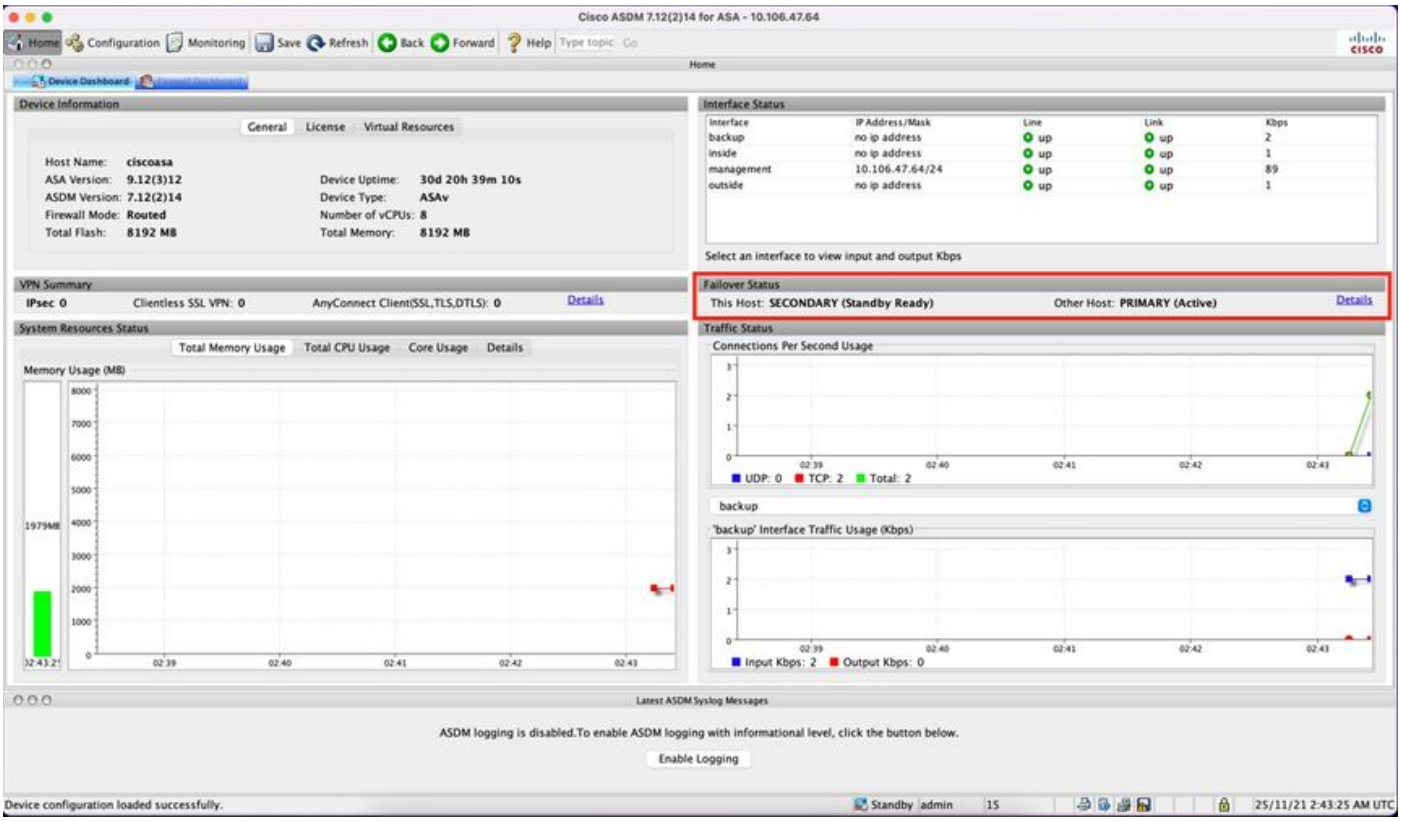


ASDM 관리 ASA HA

기본 ASA에 대한 ASDM 홈 페이지:

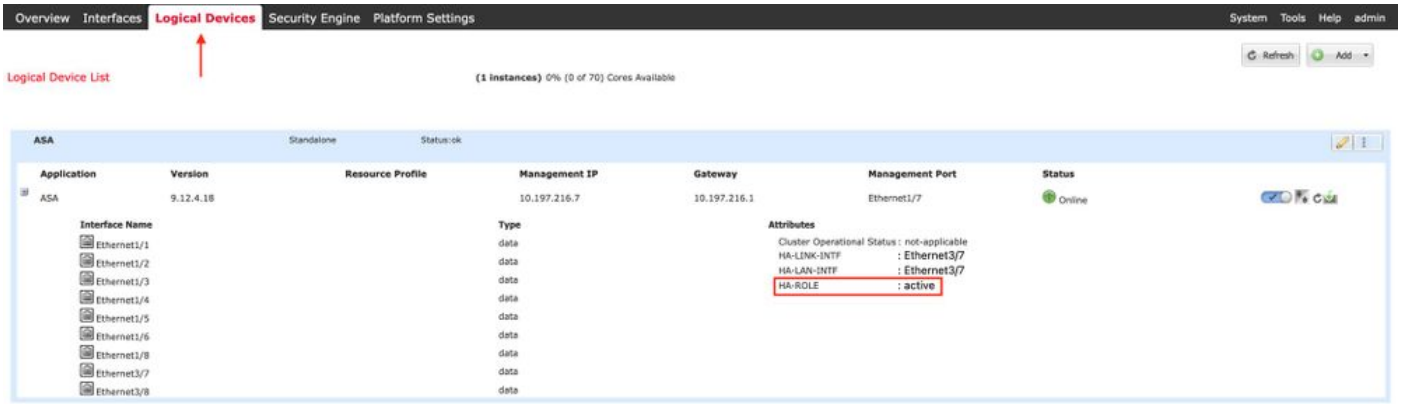


보조 ASA에 대한 ASDM 홈 페이지:

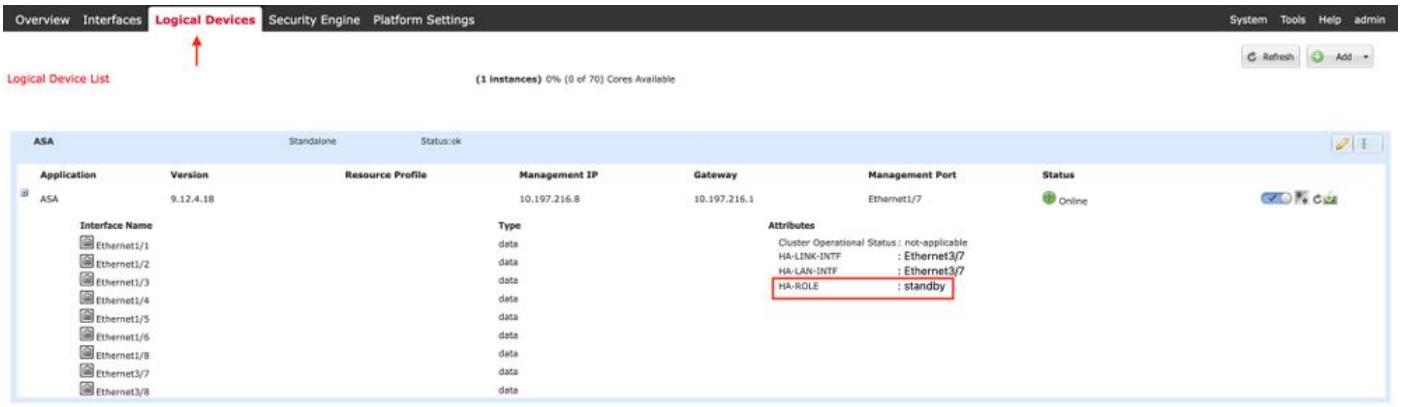


FTD/ASA HA를 실행하는 4100/9300용 firepower 섀시 관리자

기본 FCM 논리적 디바이스 페이지:



보조 FCM 논리적 디바이스 페이지:



CLI 확인

<#root>

>

show running-config failover

```
failover
failover lan unit secondary
failover lan interface failover-link GigabitEthernet0/2
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89
```

여기서 고려해야 할 중요한 사항은 다음과 같습니다.

장애 조치
장애 조치 lan 유닛 보조 —> 유닛이 기본 유닛인지 보조 유닛인지 여부
장애 조치 lan 인터페이스 failover-link GigabitEthernet0/2 —> 디바이스의 장애 조치 링크 물리적 인터페이스
장애 조치(failover) 복제 http
장애 조치 링크 장애 조치 링크 GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 —> primary 및 standby device failover link ip address.

<#root>

>

show failover

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
Monitored Interfaces 0 of 311 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(0)26, Mate 9.16(0)26
Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12
Last Failover at: 01:18:19 UTC Nov 25 2021
    This host: Secondary - Standby Ready
        Active time: 0 (sec)
        slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.2): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)
    Other host: Primary - Active
        Active time: 707216 (sec)
        Interface outside (0.0.0.0): Normal (Not-Monitored)
        Interface inside (192.168.45.1): Normal (Not-Monitored)
        Interface diagnostic (0.0.0.0): Normal (Not-Monitored)
        slot 1: snort rev (1.0) status (up)
        slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
    Link : failover-link GigabitEthernet0/2 (up)
    Stateful Obj        xmit       xerr          rcv          rerr
    General             95752       0           115789          0
    sys cmd             95752       0            95752          0
    up time               0         0              0            0
    RPC services          0         0              0            0
    TCP conn              0         0              0            0
    UDP conn              0         0              0            0
    ARP tbl               0         0            20036          0
    Xlate_Timeout         0         0              0            0
    IPv6 ND tbl           0         0              0            0
    VPN IKEv1 SA          0         0              0            0
    VPN IKEv1 P2          0         0              0            0
    VPN IKEv2 SA          0         0              0            0
    VPN IKEv2 P2          0         0              0            0
    VPN CTCP upd          0         0              0            0
    VPN SDI upd           0         0              0            0
    VPN DHCP upd          0         0              0            0
    SIP Session           0         0              0            0
    SIP Tx                0         0              0            0
    SIP Pinhole           0         0              0            0
    Route Session         0         0              0            0
    Router ID             0         0              0            0
    User-Identity         0         0              1            0
    CTS SGTNAME           0         0              0            0
    CTS PAC               0         0              0            0
    TrustSec-SXP          0         0              0            0
    IPv6 Route            0         0              0            0
    STS Table             0         0              0            0
    Rule DB B-Sync        0         0              0            0
    Rule DB P-Sync        0         0              0            0
    Rule DB Delete        0         0              0            0

    Logical Update Queue Information
       Cur   Max    Total
Recv Q: 0     5     504656
Xmit Q: 0     1     95752
```

장애 조치 켜짐: 장애 조치가 활성화되었거나 비활성화되었습니다.

이 호스트: Secondary - Standby Ready. 이 디바이스의 역할 및 인터페이스의 상태.

기타 호스트: Primary - Active. 다른 장치는 활성 상태이고 현재 장치와 통신합니다.

<#root>

>

show failover history

```
==========================================================================
From State                 To State                       Reason
==========================================================================
01:18:14 UTC Nov 25 2021
Not Detected               Negotiation                    No Error

01:18:27 UTC Nov 25 2021
Negotiation                Just Active                    No Active unit found

01:18:27 UTC Nov 25 2021
Just Active                Active Drain                   No Active unit found

01:18:27 UTC Nov 25 2021
Active Drain               Active Applying Config         No Active unit found

01:18:27 UTC Nov 25 2021
Active Applying Config     Active Config Applied          No Active unit found

01:18:27 UTC Nov 25 2021
Active Config Applied         Active                      No Active unit found
==========================================================================
```

디바이스의 기록 상태 및 이러한 상태가 변경된 이유를 확인하려면 이 옵션을 사용합니다.

<#root>

>

show failover state

```
               State              Last Failure Reason      Date/Time
This host -    Secondary
               Standby Ready          None
Other host -   Primary
               Active                 None

====Configuration State===
    Sync Done - STANDBY
====Communication State===
    Mac set
```

디바이스의 현재 상태 및 마지막 장애 조치 이유를 확인합니다.

필드	설명
컨피그레이션 상태	컨피그레이션 동기화 상태를 표시합니다. 스탠바이 유닛에 대해 가능한 컨피그레이션 상태: • Config Syncing - STANDBY — 동기화된 컨피그레이션이 실행되는 동안 설정됩니다. • 인터페이스 구성 동기화 - 대기 • Sync Done - STANDBY — 스탠바이 유닛이 액티브 유닛에서 컨피그레이션 동기화를 완료한 경우에 설정합니다. 활성 유닛에 대해 가능한 컨피그레이션 상태: • 컨피그레이션 동기화 — 액티브 유닛에서 스탠바이 유닛에 컨피그레이션 동기화를 수행할 때 설정됩니다. • 인터페이스 구성 동기화 • Sync Done(동기화 완료) - 액티브 유닛에서 스탠바이 유닛으로의 컨피그레이션 동기화를 성공적으로 완료한 경우에 설정합니다. • Ready for Config Sync(컨피그레이션 동기화 준비) - 스탠바이 유닛에서 컨피그레이션 동기화를 수신할 준비가 되었다는 신호를 보낼 때 활성 유닛에서 설정합니다.
통신 상태	MAC 주소 동기화의 상태를 표시합니다. • Mac set - MAC 주소가 피어 유닛에서 이 유닛으로 동기화되었습니다. • Updated Mac(업데이트된 Mac) - MAC 주소가 업데이트되어 다른 유닛과 동기화해야 할 때 사용합니다. 디바이스가 피어 디바이스에서 동기화된 로컬 MAC 주소를 업데이트하는 전환 시에도 사용됩니다.
날짜/시간	실패의 날짜 및 타임스탬프를 표시합니다.
마지막 실패 사유	마지막으로 보고된 실패의 이유를 표시합니다. 이 정보는 실패 조건이 지워진 경우에도 지워지지 않습니다. 이 정보는 장애 조치가 발생할 때만 변경됩니다. 가능한 실패 이유:

필드	설명
	• 인터페이스 오류 — 장애가 발생한 인터페이스 수가 장애 조치 기준을 충족하여 장애 조치를 유발했습니다. • 통신 실패 — 장애 조치 링크에 장애가 발생했거나 피어가 다운되었습니다. • 백플레인 오류
상태	유닛의 Primary/Secondary 및 Active/Standby 상태를 표시합니다.
이 호스트/기타 호스트	이 호스트는 명령이 실행된 디바이스에 대한 정보를 나타냅니다. 다른 호스트는 장애 조치 쌍의 다른 디바이스에 대한 정보를 나타냅니다.

<#root>

>

show failover descriptor

```
outside send: 00020000ffff0000 receive: 00020000ffff0000
inside send: 00020100ffff0000 receive: 00020100ffff0000
diagnostic send: 01020000ffff0000 receive: 01020000ffff0000
```

문제 해결

디버그

<#root>

>

debug fover ?

```
cable          Failover LAN status
cmd-exec       Failover EXEC command execution
fail           Failover internal exception
fmsg           Failover message
ifc            Network interface status trace
open           Failover device open
rx             Failover Message receive
rxdmp          Failover recv message dump (serial console only)
rxip           IP network failover packet recv
snort          Failover NGFW mode snort processing
switch         Failover Switching status
```

```
sync          Failover config/command replication
tx            Failover Message xmit
txdmp         Failover xmit message dump (serial console only)
txip          IP network failover packet xmit
verify        Failover message verify
```

캡처:

장애 조치 인터페이스는 다음을 캡처합니다.

이 캡처를 참조하여 대체작동 hello 패킷이 전송되는 속도로 대체작동 링크에서 전송되는지 확인할 수 있습니다.

<#root>

>

show capture

```
capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
```

>

show capture capfail

```
15 packets captured

1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

장애 조치 링크의 ARP 캡처:

이 캡처를 통해 피어에 ARP 테이블에 Mac 항목이 있는지 확인할 수 있습니다.

<#root>

```
>
```

show capture

```
capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes]
>
```

show capture caparp

```
22 packets captured

1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
>
```

시나리오

피어 유닛이 HA 그룹에 가입하지 못하거나 활성 유닛에서 변경 사항을 구축하는 동안 실패한 경우, 실패한 유닛에 로그인하고 High Availability 페이지로 이동한 다음 Failover History 링크를 클릭합니다.

APP-SYNC 실패

show failover history 출력에 App Sync 실패가 표시되는 경우 HA 검증 단계 시 문제가 발생했습니다. 시스템에서 유닛이 고가용성 그룹으로 올바르게 작동할 수 있는지 확인합니다.

From State is App Sync(시작 상태가 앱 동기화인 경우) 메시지가 표시되고 노드가 Standby Ready(대기 준비) 상태로 이동합니다.

검증 실패가 발생하면 피어가 Disabled(실패) 상태로 전환됩니다. 문제를 해결하여 피어가 다시 고가용성 그룹으로 작동하도록 합니다.

앱 동기화 오류를 수정하고 활성 유닛을 변경하는 경우 이를 배포한 다음 피어 노드가 참여할 수 있도록 HA를 다시 시작해야 합니다.

이 메시지는 문제를 해결하는 방법에 대한 설명과 함께 실패를 나타냅니다. 이러한 오류는 노드 조인 및 각 후속 구축에서 발생할 수 있습니다.

노드 조인 시 시스템은 활성 유닛에서 마지막으로 구축된 컨피그레이션에 대해 검사를 수행합니다.

스탠바이 노드가 "CD 앱 동기화 오류: 앱 구성 적용 실패"로 HA에 조인하지 못함

Standby FTD 명령줄에서 /ngfw/var/log/action_queue.log에 컨피그레이션 실패 사유가 있어야 합니다.
교정: 컨피그레이션 오류를 식별하고 필요한 변경 사항을 사후 생성하면 HA를 다시 시작할 수 있습니다.
Cisco 버그 IDCSCvu15611을 참조하십시오.

<#root>

```
================================================================================
From State                  To State                    Reason
================================================================================
15:10:16 CDT Sep 28 2021
Not Detected               Disabled                    No Error
15:10:18 CDT Sep 28 2021
Disabled                   Negotiation                 Set by the config command
15:10:24 CDT Sep 28 2021
Negotiation                Cold Standby                Detected an Active mate
15:10:25 CDT Sep 28 2021
Cold Standby               App Sync                    Detected an Active mate
15:10:55 CDT Sep 28 2021
App Sync                   Disabled
```

CD App Sync error is App Config Apply Failed

```
================================================================================
```

스탠바이 노드가 "HA 상태 진행이 APP SYNC 시간 초과로 인해 실패함"으로 HA에 조인하지 못함

Standby FTD 명령줄에서 /ngfw/var/log/ngfwmanager.log에는 app-sync 시간 초과에 대한 이유가 있어야 합니다.
이 단계에서는 액티브 유닛에서 앱 동기화가 아직 진행 중이라고 생각하기 때문에 정책 배포도 실패합니다.
정책 배포에서 오류가 발생합니다. "newNode 조인/AppSync 프로세스가 진행 중이므로 구성 변경이 허용되지 않으므로 배포 요청을 거부합니다. 잠시 후에 배포를 다시 시도하십시오."
교정: 대기 노드에서 고가용성을 재개할 때 문제를 해결할 수 있는 경우가 있습니다.
Cisco 버그 ID CSCvt를 참조하십시오48941
Cisco 버그 ID CSCvx를 참조하십시오11636

<#root>

```
==========================================================================
From State                  To State                    Reason
==========================================================================
19:07:01 EST MAY 31 2021
Not Detected               Disabled                    No Error
19:07:04 EST MAY 31 2021
Disabled                   Negotiation                 Set by the config command
19:07:06 EST MAY 31 2021
Negotiation                Cold Standby                Detected an Active mate
19:07:07 EST MAY 31 2021
Cold Standby               App Sync                    Detected an Active mate
21:11:18 EST Jun 30 2021
App Sync                   Disabled
```

HA state progression failed due to APP SYNC timeout

```
==========================================================================
```

스탠바이 노드가 "CD 앱 동기화 오류가 스탠바이 시 SSP 구성을 적용하지 못함"으로 HA에 조인하지 못함

Standby FTD 명령행에서 /ngfw/var/log/ngfwmanager.log에 장애에 대한 정확한 원인이 있어야 합니다.

교정: 경우에 따라 대기 노드에서 고가용성을 다시 시작 할 때 문제를 해결 할 수 있습니다.

Cisco 버그 ID 참조 CSCvy04965

<#root>

```
==========================================================================
From State                  To State                    Reason
==========================================================================
04:15:15 UTC Apr 17 2021
Not Detected               Disabled                    No Error
04:15:24 UTC Apr 17 2021
Disabled                   Negotiation                 Set by the config command
04:16:12 UTC Apr 17 2021
Negotiation                Cold Standby                Detected an Active mate
04:16:13 UTC Apr 17 2021
Cold Standby               App Sync                    Detected an Active mate
04:17:44 UTC Apr 17 2021
App Sync                   Disabled
```

CD App Sync error is Failed to apply SSP config on standby

```
==========================================================================
```

상태 검사 실패

"HELLO not heard from mate"는 메이트가 오프라인이거나 장애 조치 링크에서 HELLO 킵얼라이브 메시지를 전달하지 않음을 의미합니다.

SSH가 작동하지 않을 경우 다른 디바이스에 로그인하여 콘솔 액세스 권한을 얻은 다음 디바이스가 작동 중인지 아니면 오프라인 상태인지 확인하십시오.

작동 중인 경우, 명령을 사용하여 장애의 원인을 파악하고 장애 조치 상태를 표시합니다.

작동하지 않으면 정상 재부팅을 시도하고 콘솔에 부팅 로그가 표시되는지 확인하십시오. 그렇지 않으면 디바이스가 하드웨어 오류로 간주될 수 있습니다.

<#root>

```
==========================================================================
From State                To State                  Reason
==========================================================================
04:53:36 UTC Feb 6 2021
Failed                    Standby Ready

Interface check


02:12:46 UTC Jul 11 2021
Standby Ready             Just Active               HELLO not heard from mate
02:12:46 UTC Jul 11 2021
Active Config Applied     Active                    HELLO not heard from mate
==========================================================================
```

Snort Down 또는 디스크 장애

FTD에서 "디스크 오류로 인한 검사 엔진 오류 감지"라는 오류를 표시할 경우 2가지 가능성이 있습니다.

탐지 엔진(SNORT 인스턴스)이 다운되었습니다.

이는 Linux 측의 명령인 pmtool 상태를 사용하여 확인할 수 있습니다 | grep -i de,

교정: 인스턴스 중 하나라도 다운된 경우 /ngfw/var/log/messages를 확인하고 원인을 파악합니다.

디바이스에 높은 디스크 사용률이 표시됨

Linux 측의 df -Th 명령을 사용하여 유효성을 검사할 수 있습니다.

교정: 대부분의 디스크를 사용하는 디렉토리를 식별하고 TAC에 문의하여 원치 않는 파일을 삭제합니다.

<#root>

```
==========================================================================
From State                To State                  Reason
```

```
==========================================================================
Active Config Applied      Active                    No Active unit found
16:07:18 UTC Dec 5 2020
Active                     Standby Ready             Other unit wants me Standby
16:07:20 UTC Dec 5 2020
Standby Ready              Failed

Detect Inspection engine failure due to disk failure


16:07:29 UTC Dec 5 2020
Failed                     Standby Ready             My Inspection engine is as good as peer due to di
==========================================================================
```

서비스 카드 오류

이러한 문제는 일반적으로 ASA 5500-X 디바이스의 Firepower 모듈 장애로 인해 보고됩니다. show module sfr 세부 정보를 통해 모듈의 온전성을 확인하십시오.

교정: 장애 발생 시점에 ASA Syslog를 수집하며, 여기에는 제어 또는 데이터 플레인 장애와 같은 세부사항이 포함될 수 있습니다.

이는 SFR 모듈의 다양한 이유로 인해 발생할 수 있습니다. IPS에서 이 문제의 근본 원인을 찾으려면 TAC를 여는 것이 좋습니다.

<#root>

```
==========================================================================
From State                 To State                  Reason
==========================================================================
21:48:19 CDT Aug 1 2021
Active                     Standby Ready             Set by the config command
21:48:19 CDT Aug 1 2021
Standby Ready              Just Active

Service card in other unit has failed


21:48:19 CDT Aug 1 2021
Active Config Applied      Active                    Service card in other unit has failed
==========================================================================
```

MIO 하트비트 실패

Firepower Threat Defense/ASA가 FPR1K, 2K, 4K, 9K에서 "MIO-blade 하트비트 오류"로 인한 오류를 보고합니다.

Cisco 버그 ID 참조 CSCvy14484
Cisco 버그 ID 참조 CSCvh26447

<#root>

```
==========================================================================
From State                  To State                    Reason
==========================================================================
20:14:45 EDT Apr 14 2021
Active Config Applied      Active                      No Active unit found
20:15:18 EDT Apr 14 2021
Active                     Failed
```

MIO-blade heartbeat failure

```
20:15:19 EDT Apr 14 2021
Failed                     Negotiation                 MIO-blade heartbeat recovered
==========================================================================
```

관련 정보

- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html
- https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.