Firepower 어플라이언스에서 FTD HA 페어 업그레이드

목차

소개

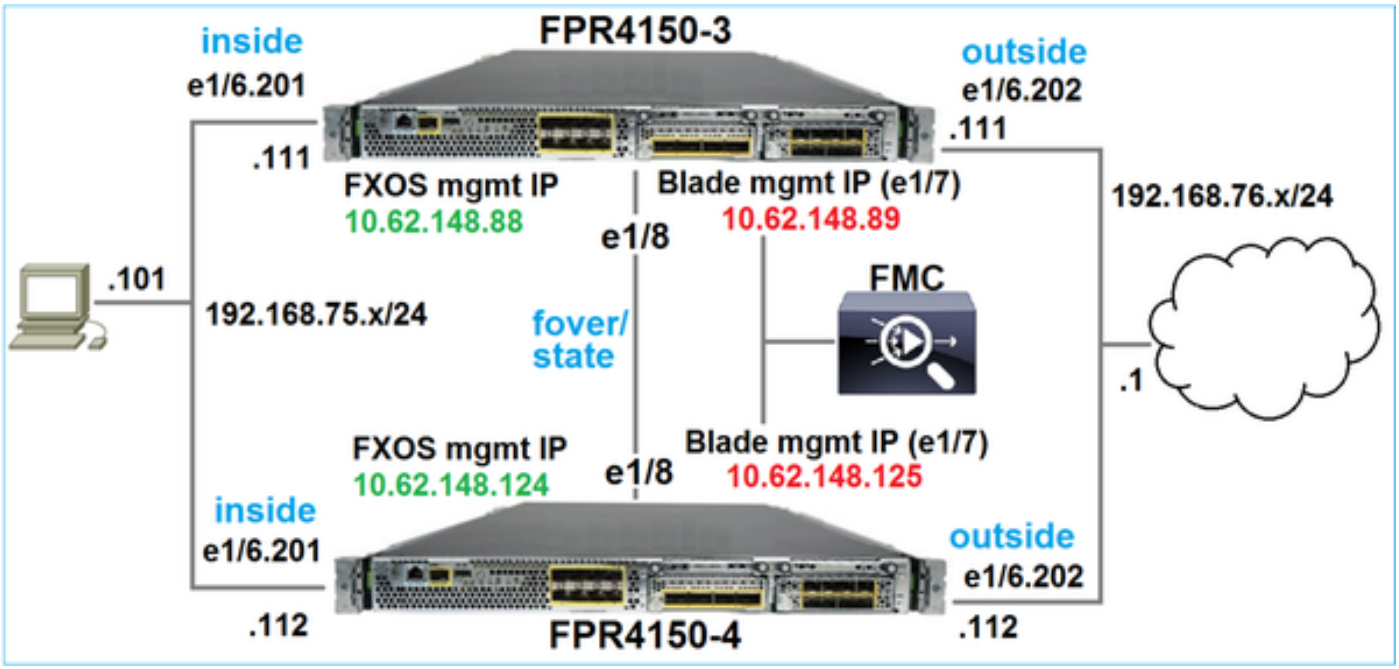
목표

이 문서의 목표는 Firepower 어플라이언스에서 고가용성 모드로 FTD(Firepower Threat Defense) 업그레이드 프로세스를 수행하는 방법을 설명하는 것입니다.

랩 구성 요소

- FP4150 2대
- FS4000 2대
- PC 1대

토폴로지



활동을 시작하기 전의 소프트웨어 이미지 버전은 다음과 같습니다.

- FMC(Firepower Management Center) 6.1.0-330
- 기본 FTD 6.1.0-330
- 보조 FTD 6.1.0-330
- 기본 FXOS 2.0.1-37
- 보조 FXOS 2.0.1-37

실행 계획

1단계: 사전 요구 사항 확인

2단계: FMC 및 SSP에 이미지 업로드

3단계: 보조 FXOS를 2.0.1-37 -> 2.0.1-86으로 업그레이드

4단계: FTD 장애 조치 교체(기본/스탠바이, 보조/액티브 상태로 설정됨)

5단계: 기본 FXOS를 2.0.1-37 -> 2.0.1-86으로 업그레이드

6단계: FMC를 6.1.0-330 -> 6.1.0.1로 업그레이드

7단계: FTD HA 페어를 6.1.0-330 -> 6.1.0.1로 업그레이드

8단계: FMC에서 FTD HA 페어로 정책 구축

FTD HA 업그레이드 프로세스

1단계: 사전 요구 사항 확인

FXOS 호환성 가이드를 참조하여 다음 항목 간의 호환성을 확인합니다.

- 타깃 FTD 소프트웨어 버전과 FXOS 소프트웨어 버전
- Firepower HW 플랫폼과 FXOS 소프트웨어 버전

http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html#pgfId-136544

타깃 버전의 FXOS 릴리스 노트를 확인하여 FXOS 업그레이드 경로를 결정합니다.

http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/fxos201/release/notes/fxos201_rn.html#pgfId-141076

FTD 타깃 버전 릴리스 노트를 참조하여 FTD 업그레이드 경로를 결정합니다.

http://www.cisco.com/c/en/us/td/docs/security/firepower/601/6012/relnotes/firepower-system-release-notes-version-6012.html#pgfId-378288

2단계: 이미지 업로드

FCM 2대에서 FXOS 이미지(fxos-k9.2.0.1.86.SPA)를 업로드합니다.

FMC에서 FMC 및 FTD 업그레이드 패키지를 업로드합니다.

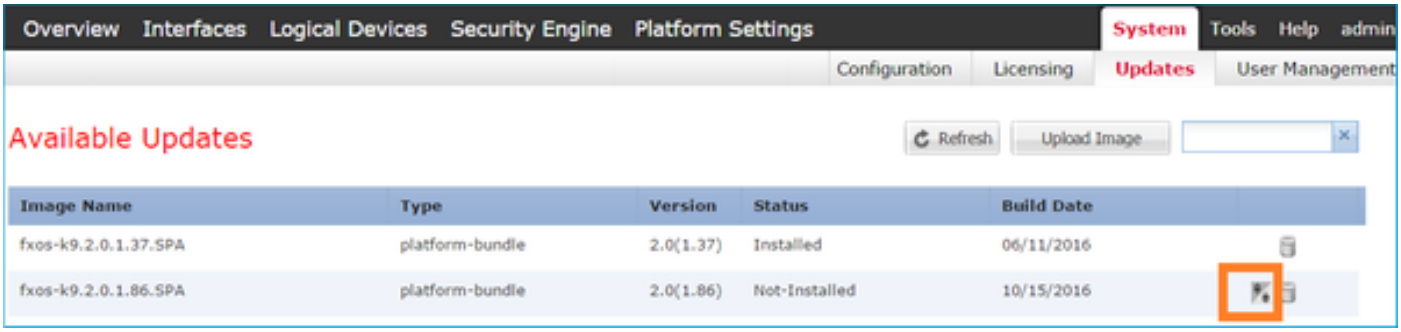
- FMC 업그레이드용: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- FTD 업그레이드용: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

3단계: 보조 FXOS 업그레이드

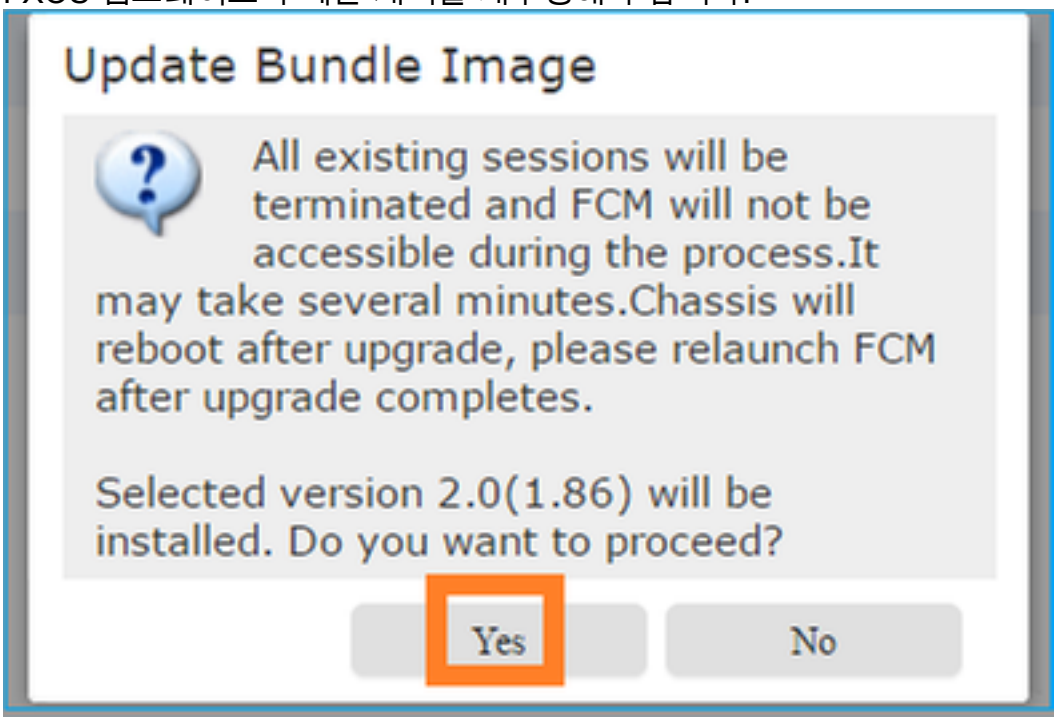
업그레이드 전에 다음을 수행합니다.

```
FPR4100-4-A /system # show firmware monitor FPRM: Package-Vers: 2.0(1.37) Upgrade-Status: Ready
Fabric Interconnect A: Package-Vers: 2.0(1.37) Upgrade-Status: Ready Chassis 1: Server 1:
Package-Vers: 2.0(1.37) Upgrade-Status: Ready
```

FXOS 업그레이드를 시작합니다.



FXOS 업그레이드 후에는 섀시를 재부팅해야 합니다.



FXOS CLI에서 FXOS 업그레이드를 모니터링할 수 있습니다. 3개 구성 요소(FPRM, 패브릭 인터커넥트 및 섀시)를 모두 업그레이드해야 합니다.

```
FPR4100-4-A# scope system FPR4100-4-A /system # show firmware monitor FPRM: Package-Vers: 2.0(1.37) Upgrade-Status: Upgrading Fabric Interconnect A: Package-Vers: 2.0(1.37) Upgrade-Status: Ready Chassis 1: Server 1: Package-Vers: 2.0(1.37) Upgrade-Status: Ready
```

참고 - FXOS 업그레이드 프로세스를 시작하고 나서 몇 분 후에 FXOS CLI와 GUI 연결이 모두 끊길 수 있습니다. 이 경우 몇 초 후에 다시 로그인할 수 있습니다.

FPRM 구성 요소 업그레이드는 5분 이내에 완료됩니다.

```
FPR4100-4-A /system # show firmware monitor FPRM: Package-Vers: 2.0(1.86) Upgrade-Status: Ready Fabric Interconnect A: Package-Vers: 2.0(1.37) Upgrade-Status: Upgrading Chassis 1: Server 1: Package-Vers: 2.0(1.37) Upgrade-Status: Upgrading
```

10분 이내에 FXOS 업그레이드 프로세스의 일부분으로 보조 Firepower 디바이스가 재시작됩니다.

Please stand by while rebooting the system...
... Restarting system.

디바이스가 재시작되고 나면 업그레이드 프로세스가 재시작됩니다.

FPR4100-4-A /system # **show firmware monitor** FPRM: Package-Vers: **2.0(1.86)** Upgrade-Status: **Ready** Fabric Interconnect A: Package-Vers: 2.0(1.37) Upgrade-Status: **Upgrading** Chassis 1: Server 1: Package-Vers: 2.0(1.37) Upgrade-Status: **Upgrading**

FXOS 업그레이드는 총 30분 이내에 완료됩니다.

FPR4100-4-A /system # **show firmware monitor** FPRM: Package-Vers: **2.0(1.86)** Upgrade-Status: **Ready** Fabric Interconnect A: Package-Vers: **2.0(1.86)** Upgrade-Status: **Ready** Chassis 1: Server 1: Package-Vers: **2.0(1.86)**,2.0(1.37) Upgrade-Status: **Ready**

4단계: FTD 장애 조치 상태 교체

장애 조치 상태를 교체하기 전에 보조 섀시의 FTD 모듈이 완전히 가동되고 있는지 확인합니다.

FPR4100-4-A# **connect module 1 console** Firepower-module1>**connect ftd** Connecting to ftd console... enter exit to return to bootCLI > **show high-availability config** Failover On Failover unit Secondary Failover LAN Interface: FOVER Ethernet1/8 (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 3 of 1041 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.6(2), Mate 9.6(2) Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U Last Failover at: 15:08:47 UTC Dec 17 2016 **This host: Secondary - Standby Ready** Active time: 0 (sec) slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)) status (Up Sys) Interface inside (192.168.75.112): **Normal** (Monitored) Interface outside (192.168.76.112): **Normal** (Monitored) Interface diagnostic (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) **status** (**up**) slot 2: diskstatus rev (1.0) **status** (**up**) **Other host: Primary - Active** Active time: 5163 (sec) Interface inside (192.168.75.111): **Normal** (Monitored) Interface outside (192.168.76.111): **Normal** (Monitored) Interface diagnostic (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) **status** (**up**) slot 2: diskstatus rev (1.0) **status** (**up**) Stateful Failover Logical Update Statistics Link : FOVER Ethernet1/8 (up) Stateful Obj xmit xerr rcv rerr General 65 0 68 4 sys cmd 65 0 65 0 **...**

FTD 장애 조치 상태를 교체합니다. 활성화된 FTD CLI에서 다음 명령을 실행합니다.

> **no failover active Switching to Standby** >

참고 - 이 시점에서 FTP 통과 트래픽의 패킷 1개가 삭제될 수 있습니다.

5단계: 기본 FXOS 어플라이언스 업그레이드

2단계와 같은 방식으로 기본 FTD가 설치된 FXOS 어플라이언스를 업그레이드합니다. 이 단계를 완료하려면 30분 이상이 걸릴 수 있습니다.

6단계: FMC 소프트웨어 업그레이드

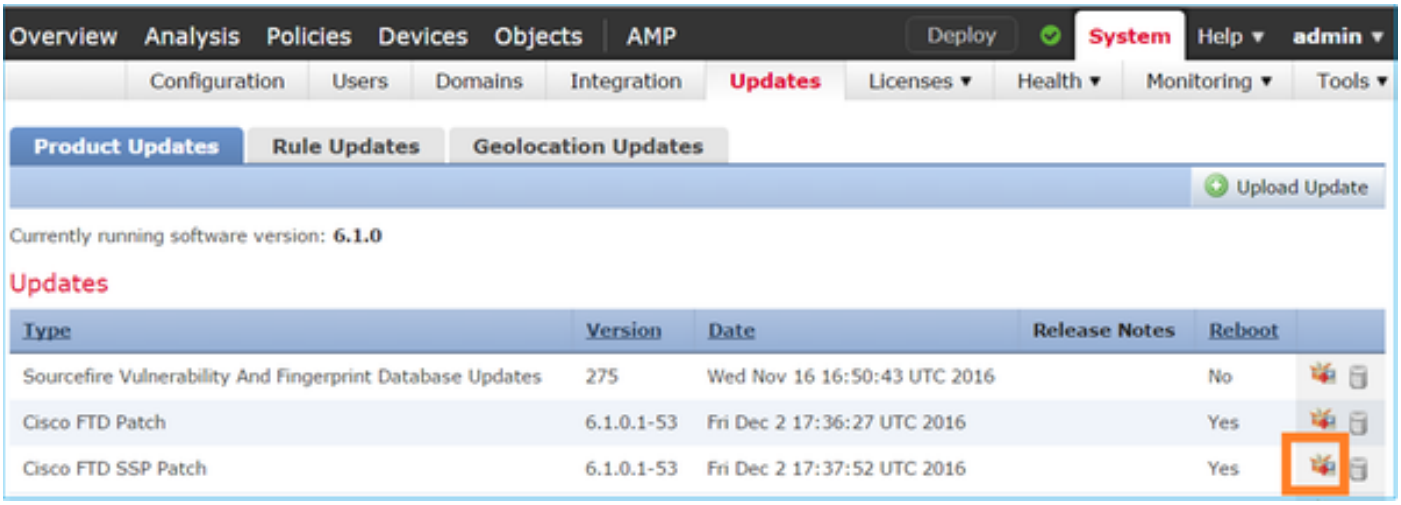
FMC를 업그레이드합니다. 이 시나리오에서는 6.1.0-330에서 6.1.0.1로 업그레이드합니다.

7단계: FTD HA 페어 업그레이드

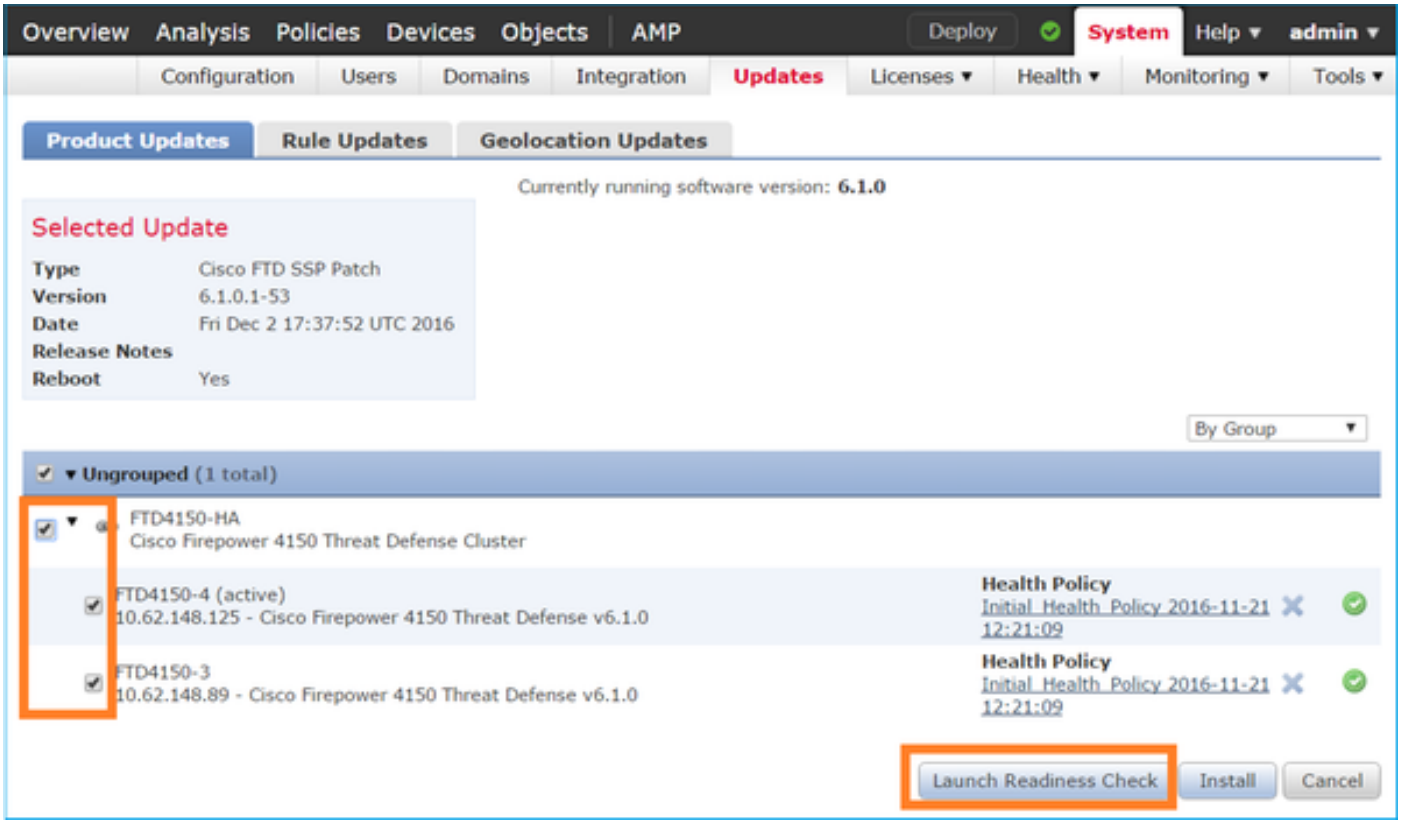
업그레이드 전에 다음을 수행합니다.

```
> show high-availability config Failover On Failover unit Primary Failover LAN Interface: FOVER
Ethernet1/8 (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
3 of 1041 maximum MAC Address Move Notification Interval not set failover replication http
Version: Ours 9.6(2), Mate 9.6(2) Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW Last
Failover at: 15:51:08 UTC Dec 17 2016 This host: Primary - Standby Ready Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)) status (Up Sys) Interface inside (192.168.75.112):
Normal (Monitored) Interface outside (192.168.76.112): Normal (Monitored) Interface diagnostic
(0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0)
status (up) Other host: Secondary - Active Active time: 1724 (sec) Interface inside
(192.168.75.111): Normal (Monitored) Interface outside (192.168.76.111): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2:
diskstatus rev (1.0) status (up) Stateful Failover Logical Update Statistics Link : FOVER
Ethernet1/8 (up) Stateful Obj xmit xerr rcv rerr General 6 0 9 0 sys cmd 6 0 6 0
...
```

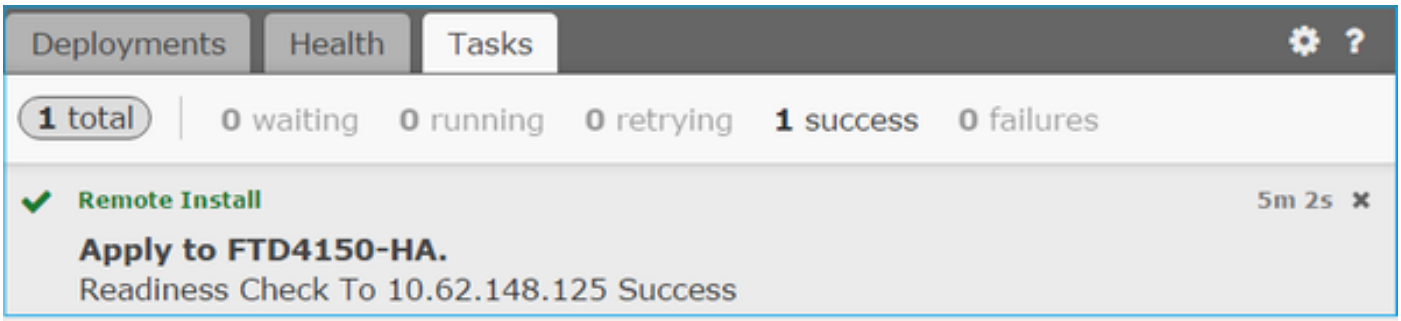
FMC **System(시스템) > Updates(업데이트)** 메뉴에서 FTD HA 업그레이드 프로세스를 시작합니다.



원하는 경우 FTD DB 무결성 검사가 포함되는 FTD 업그레이드 준비 상태 점검을 시작할 수 있습니다.

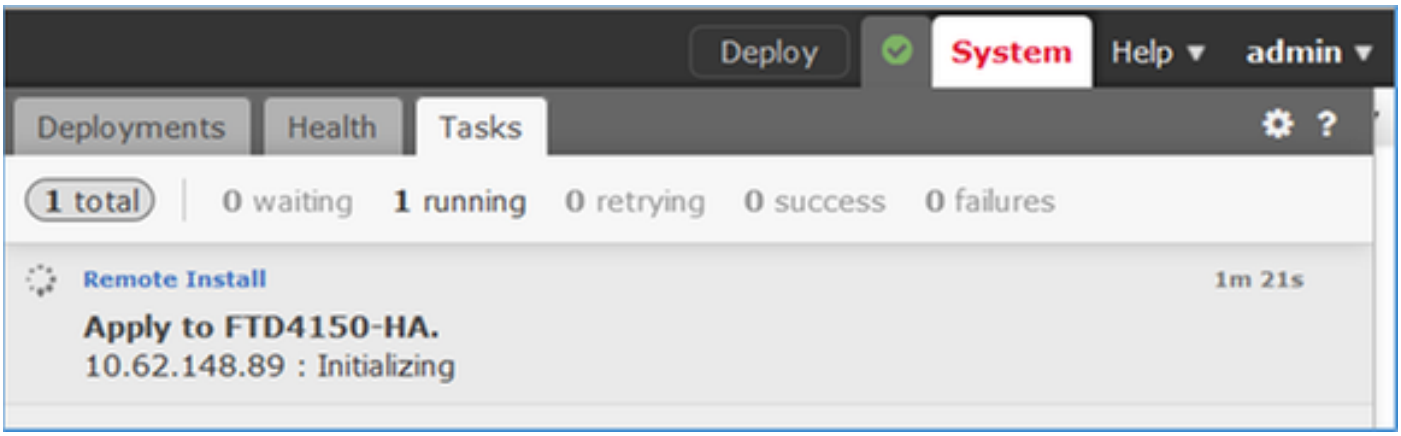


이 예에서는 점검이 5분 이내에 정상적으로 완료되었습니다.

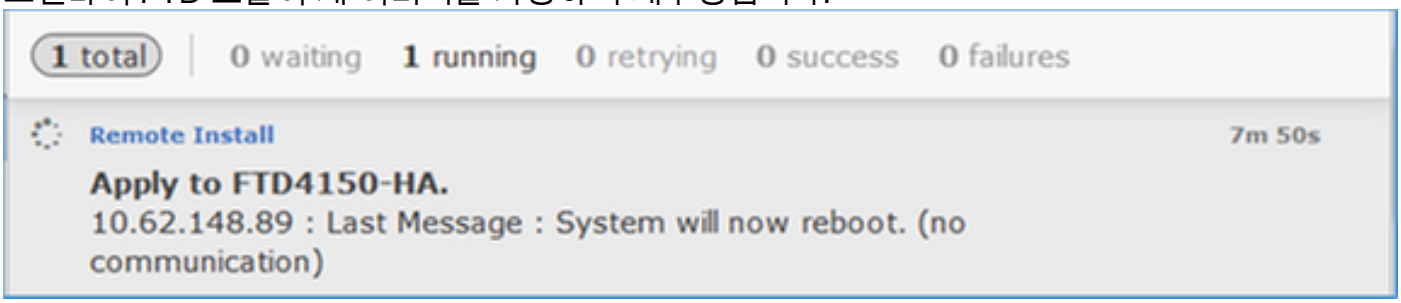


설치 프로세스를 시작합니다.

먼저 기본/스탠바이 FTD를 업그레이드합니다.



스탠바이 FTD 모듈이 새 이미지를 사용하여 재부팅됩니다.



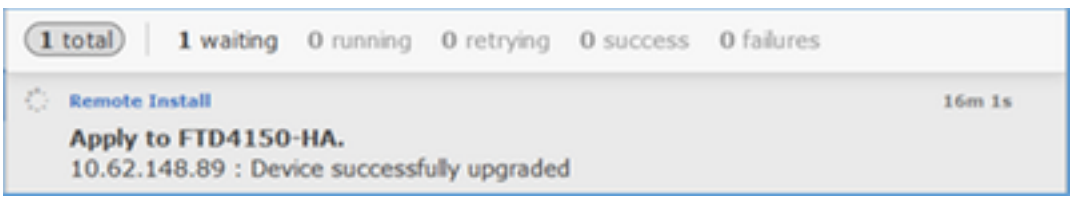
FXOS BootCLI 모드에서 FTD 상태를 확인할 수 있습니다.

```
FPR4100-3-A# connect module 1 console Firepower-module1> show services status Services currently running: Feature | Instance ID | State | Up Since ----------------------------------------------
------------ ftd | 001_JAD201200R4WLYCWO6 | RUNNING | :00:00:33
```

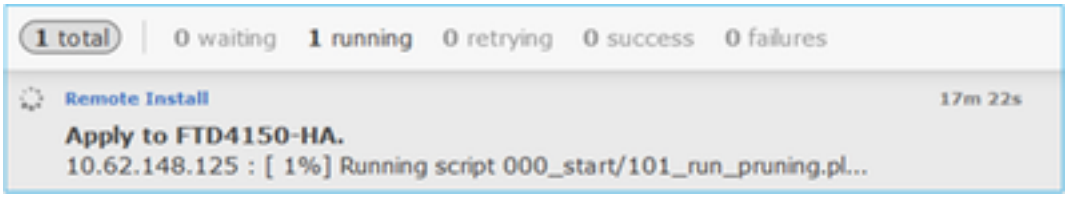
FTD 모듈 간의 소프트웨어 버전 불일치로 인해 보조/액티브 FTD CLI에 경고 메시지가 표시됩니다.

```
firepower#
************WARNING****WARNING****WARNING*******************************
Mate version 9.6(2) is not identical with ours 9.6(2)4
************WARNING****WARNING****WARNING******************************* Beginning
configuration replication: Sending to mate. End Configuration Replication to mate
```

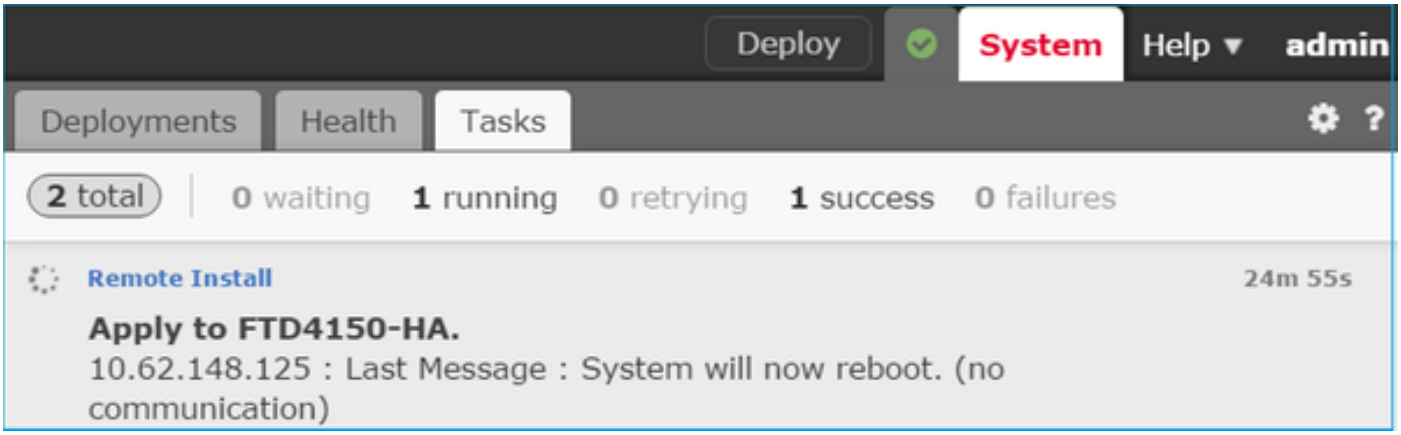
FMC에는 FTD 디바이스가 정상적으로 업그레이드되었음이 표시됩니다.



두 번째 FTD 모듈의 업그레이드가 시작됩니다.



프로세스가 끝나면 보조 FTD가 새 이미지를 사용하여 부팅됩니다.



백그라운드에서 FMC는 내부 사용자 'enable_1'을 사용하여 FTD 장애 조치 상태를 교체하고 보조 FTD에서 장애 조치 컨피그레이션을 임시로 제거합니다.

```
firepower# show logging Dec 17 2016 16:40:14: %ASA-5-111008: User 'enable_1' executed the 'no failover active' command. Dec 17 2016 16:40:14: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'no failover active' Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'clear configure failover' command. Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'clear configure failover' Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'copy /noconfirm running-config disk0:/modified-config.cfg' command. Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'copy /noconfirm running-config disk0:/modified-config.cfg' firepower# Switching to Standby firepower#
```

참고 - 이 시점에서 장애 조치 상태 교체로 인해 패킷 1개가 삭제될 수 있습니다.

이 예의 경우에는 전체 FTD 업그레이드(두 장치 모두)가 30분 이내에 완료되었습니다.

확인

기본 FTD 디바이스에서 FTD CLI를 확인합니다.

```
> show high-availability config Failover On Failover unit Primary Failover LAN Interface: FOVER Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds
```

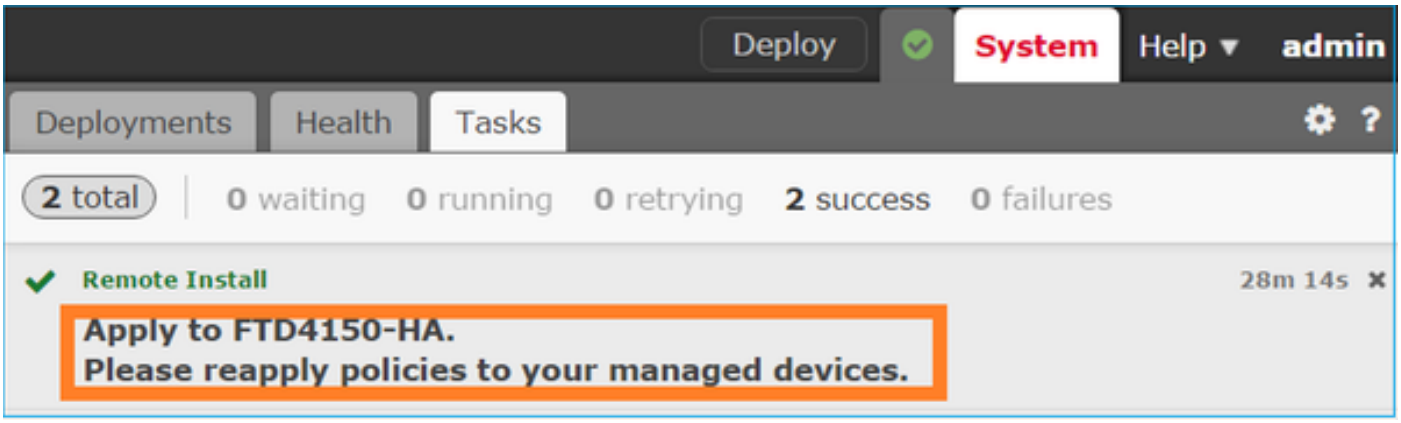
```
Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces
3 of 1041 maximum MAC Address Move Notification Interval not set failover replication http
Version: Ours 9.6(2)4, Mate 9.6(2)4 Serial Number: Ours FLM2006EN9U, Mate FLM2006EQFW Last
Failover at: 16:40:14 UTC Dec 17 2016 This host: Primary - Active Active time: 1159 (sec) slot
0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys) Interface inside (192.168.75.111):
Normal (Monitored) Interface outside (192.168.76.111): Normal (Monitored) Interface diagnostic
(0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0)
status (up) Other host: Secondary - Standby Ready Active time: 0 (sec) slot 0: UCSB-B200-M3-U
hw/sw rev (0.0/9.6(2)4) status (Up Sys) Interface inside (192.168.75.112): Normal (Monitored)
Interface outside (192.168.76.112): Normal (Monitored) Interface diagnostic (0.0.0.0): Normal
(Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Stateful
Failover Logical Update Statistics Link : FOVER Ethernet1/8 (up) Stateful Obj xmit xerr rcv rerr
General 68 0 67 0 ... >
```

보조 FTD 디바이스에서 FTD CLI를 확인합니다.

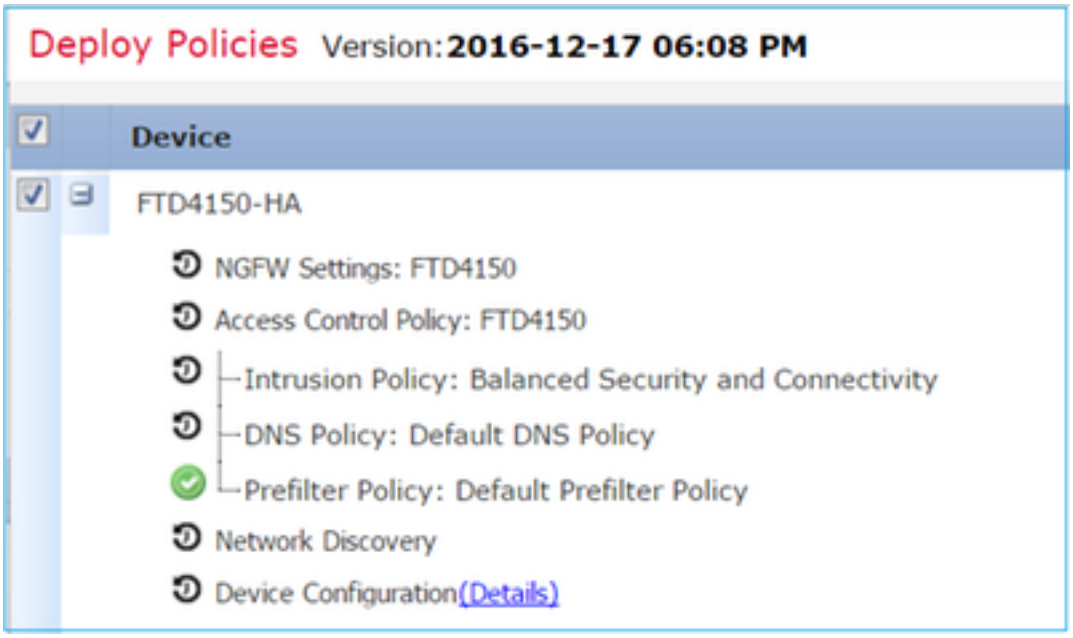
```
> show high-availability config Failover On Failover unit Secondary Failover LAN Interface:
FOVER Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15
seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored
Interfaces 3 of 1041 maximum MAC Address Move Notification Interval not set failover replication
http Version: Ours 9.6(2)4, Mate 9.6(2)4 Serial Number: Ours FLM2006EQFW, Mate FLM2006EN9U Last
Failover at: 16:52:43 UTC Dec 17 2016 This host: Secondary - Standby Ready Active time: 0 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(2)4) status (Up Sys) Interface inside
(192.168.75.112): Normal (Monitored) Interface outside (192.168.76.112): Normal (Monitored)
Interface diagnostic (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2:
diskstatus rev (1.0) status (up) Other host: Primary - Active Active time: 1169 (sec) Interface
inside (192.168.75.111): Normal (Monitored) Interface outside (192.168.76.111): Normal
(Monitored) Interface diagnostic (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up) Stateful Failover Logical Update Statistics Link :
FOVER Ethernet1/8 (up) Stateful Obj xmit xerr rcv rerr General 38 0 41 0
... >
```

8단계: FTD HA 페어에 정책 구축

업그레이드가 완료되고 나면 HA 페어에 정책을 구축해야 합니다. FMC UI에 이 내용이 표시됩니다.

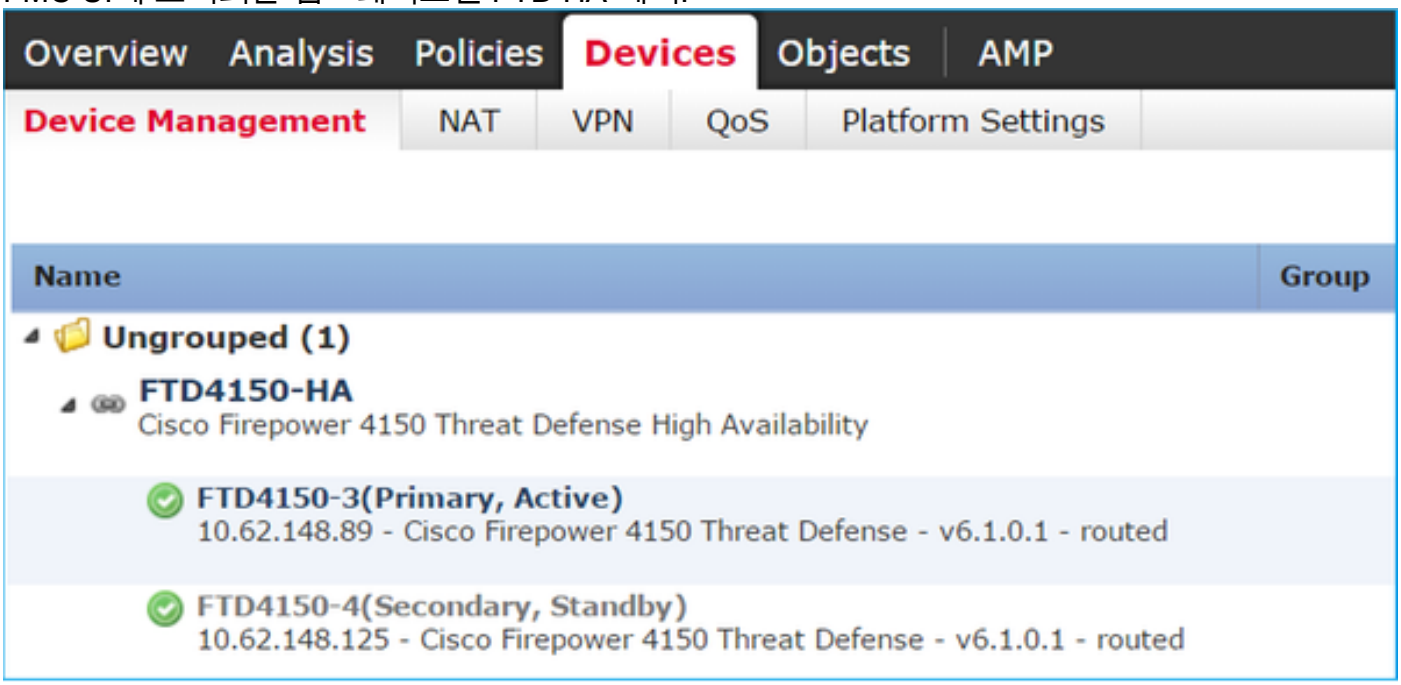


정책을 구축합니다.

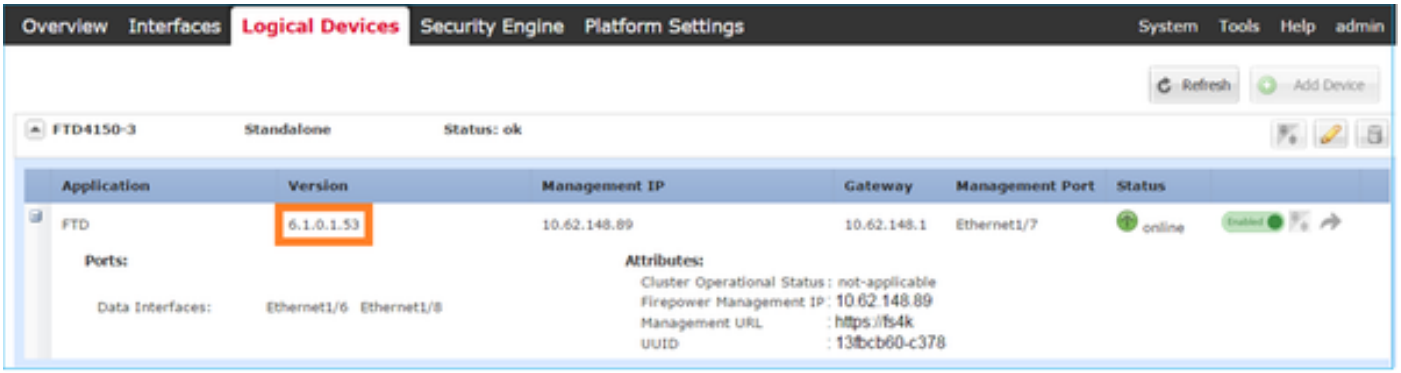


확인

FMC UI에 표시되는 업그레이드된 FTD HA 페어:



FCM UI에 표시되는 업그레이드된 FTD HA 페어:



관련 문서

Cisco Firepower NGFW