Upgrading an FTD HA pair on Firepower appliances

Contents

Introduction

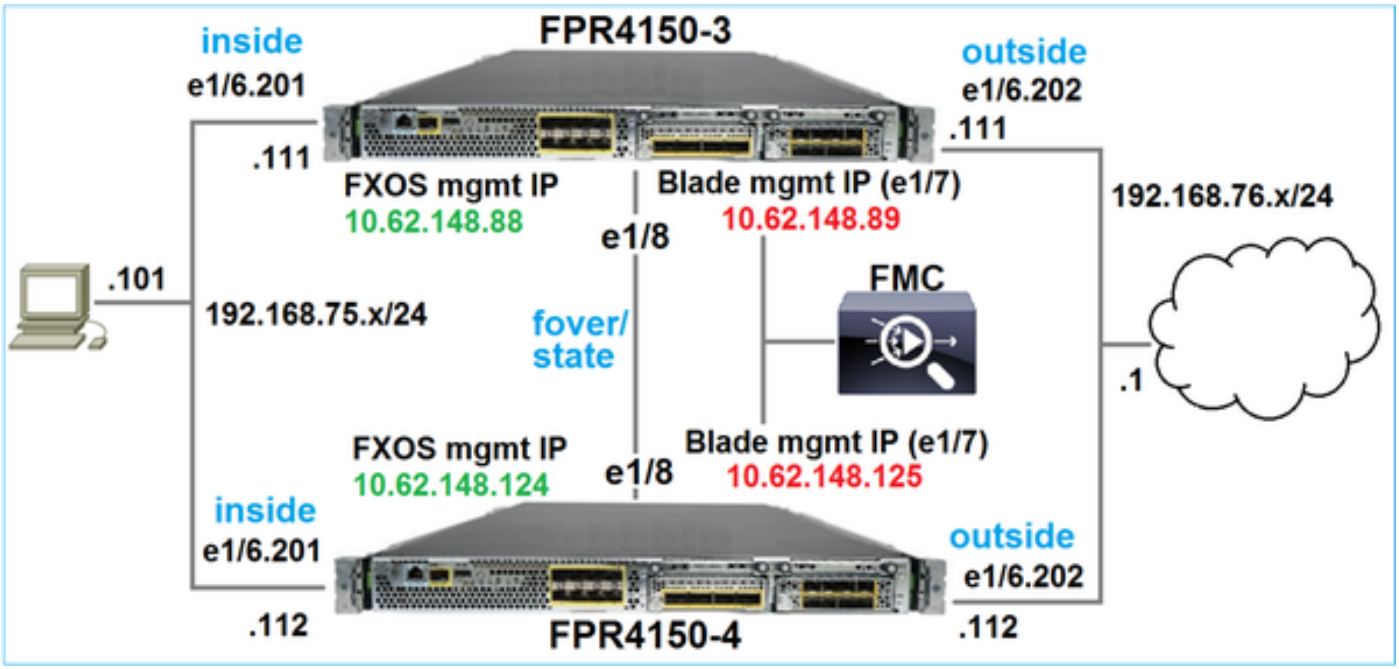
Goal

The goal of this document is to demonstrate the upgrade process of Firepower Threat Defense (FTD) in High Availability mode on Firepower appliances.

Lab components

- 2 x FP4150
- 1 x FS4000
- 1 PC

Topology



The software Image versions before starting the activity:

- Firepower Management Center (FMC) 6.1.0-330
- FTD primary 6.1.0-330
- FTD secondary 6.1.0-330
- FXOS primary 2.0.1-37
- FXOS secondary 2.0.1-37

Action Plan

Step 1: Check the prerequisites

Step 2: Upload the images to FMC and SSP

Step 3: Upgrade the Secondary FXOS 2.0.1-37 -> 2.0.1-86

Step 4: Swap the FTD failover (you will have Primary/Standby, Secondary/Active)

Step 5: Upgrade the Primary FXOS 2.0.1-37 -> 2.0.1-86

Step 6: Upgrade the FMC 6.1.0-330 -> 6.1.0.1

Step 7: Upgrade the FTD HA pair 6.1.0-330 -> 6.1.0.1

Step 8: Deploy a policy from FMC to the FTD HA pair

The FTD HA upgrade process

Step 1: Check the prerequisites

Consult the FXOS Compatibility Guide to determine the compatibility between:

- Target FTD software version and FXOS software version
- Firepower HW platform and FXOS software version

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

Check the FXOS Release Notes of the target version to determine the FXOS upgrade path:

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

Consult the FTD target version Release Notes to determine the FTD upgrade path:

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

Step 2: Upload the images

On the 2 FCMs upload the FXOS images (fxos-k9.2.0.1.86.SPA)

On the FMC upload the FMC and FTD upgrade packages:

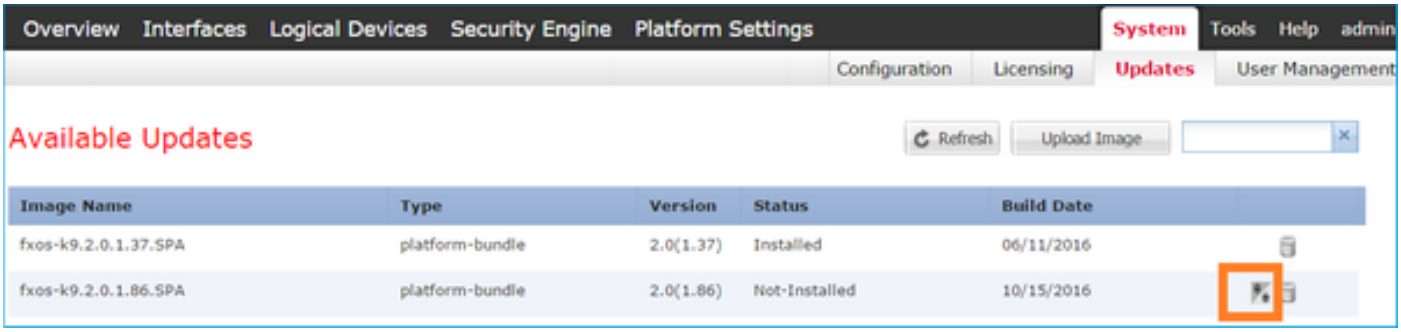
- For the FMC upgrade: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- For the FTD upgrade: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

Step 3: Upgrade the Secondary FXOS

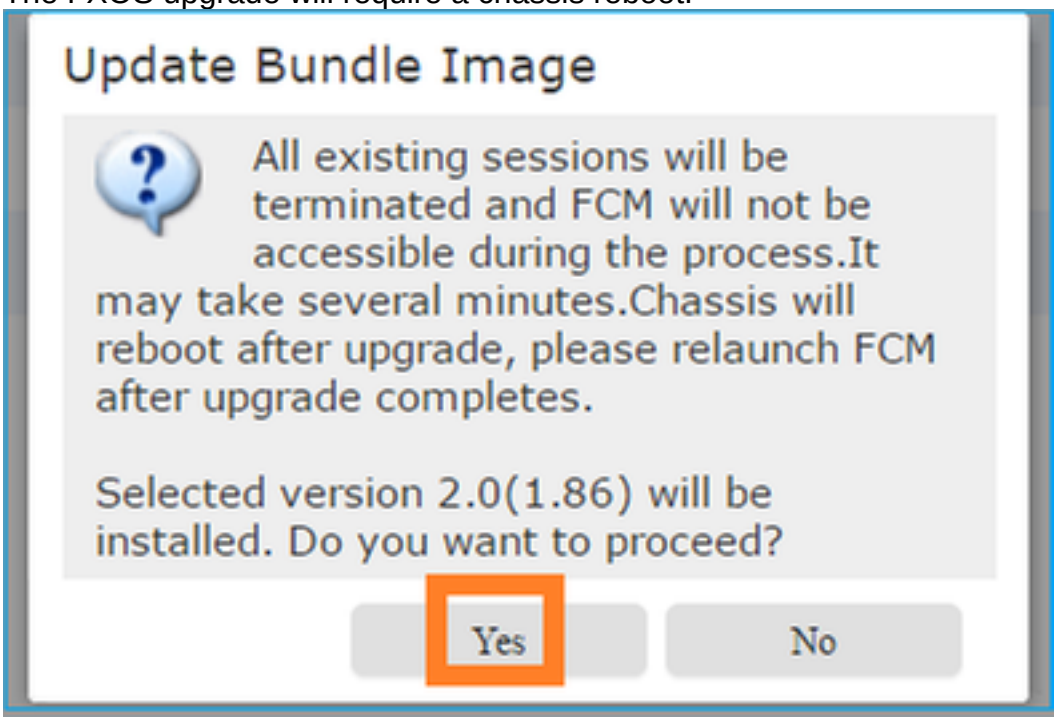
Before the upgrade:

```
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
```

Start the FXOS upgrade:



The FXOS upgrade will require a chassis reboot:



You can monitor the FXOS upgrade from the FXOS CLI. All 3 components (FPRM, Fabric interconnect and Chassis) have to be upgraded:

```
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
```

Note – Few minutes after starting the FXOS upgrade process you might be disconnected from both FXOS CLI and GUI. You should be able to login again after few seconds.

After ~5 min the FPRM component upgrade completes:

```
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
```

After ~10 min and as a part of the FXOS upgrade process the Secondary Firepower device

restarts:

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

After the restart the upgrade process resumes:

```
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
```

After total of ~30 min the FXOS upgrade completes:

```
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
```

Step 4: Swap the FTD failover states

Before swapping the failver states make sure that the FTD module on the Secondary chassis is fully UP:

```
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 ...
```

Swap the FTD failover states. From the Active FTD CLI:

```
> no failover active Switching to Standby >
```

Note - At this point you might have ~1 packet of FTD transit traffic dropped

Step 5: Upgrade the Primary FXOS appliance

Similar to Step 2 upgrade the FXOS appliance where the Primary FTD is installed - This step can take ~30 minutes or more to complete.

Step 6: Upgrade the FMC software

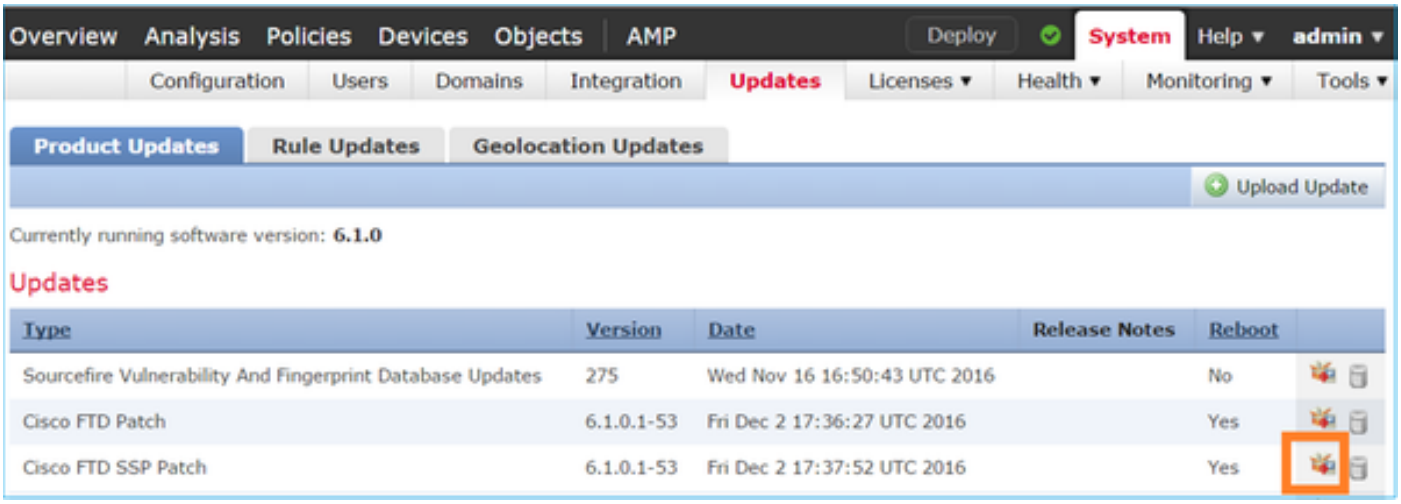
Upgrade the FMC, in this scenario from 6.1.0-330 to 6.1.0.1.

Step 7: Upgrade the FTD HA pair

Before the upgrade:

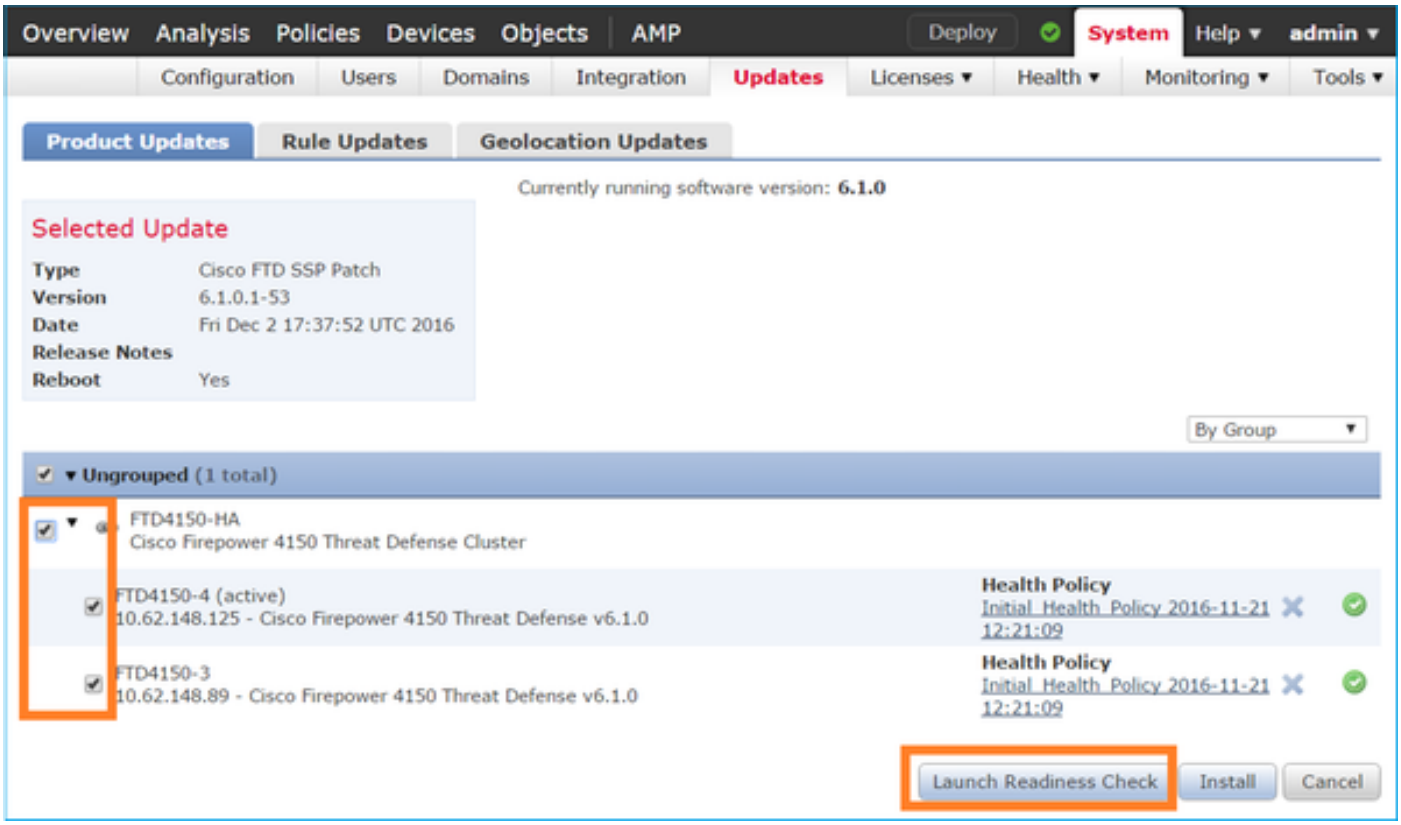
```
> show high-availability config Failover On Failover unit Primary Failover LAN Interface: FOVER
Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces
3 of 1041 maximum 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
...
```

From the FMC **System > Updates** menu initiate the FTD HA upgrade process:

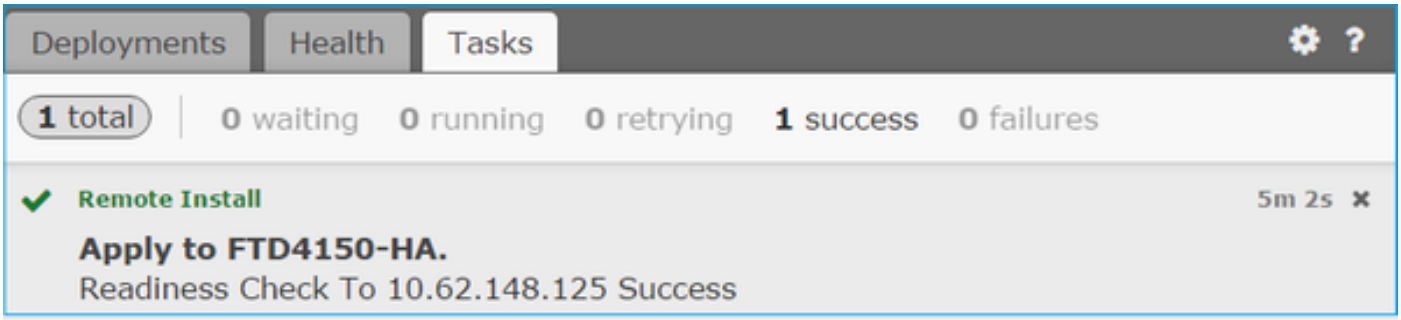


Optionally you can launch the FTD upgrade Readiness Check which includes an FTD DB integrity

check:

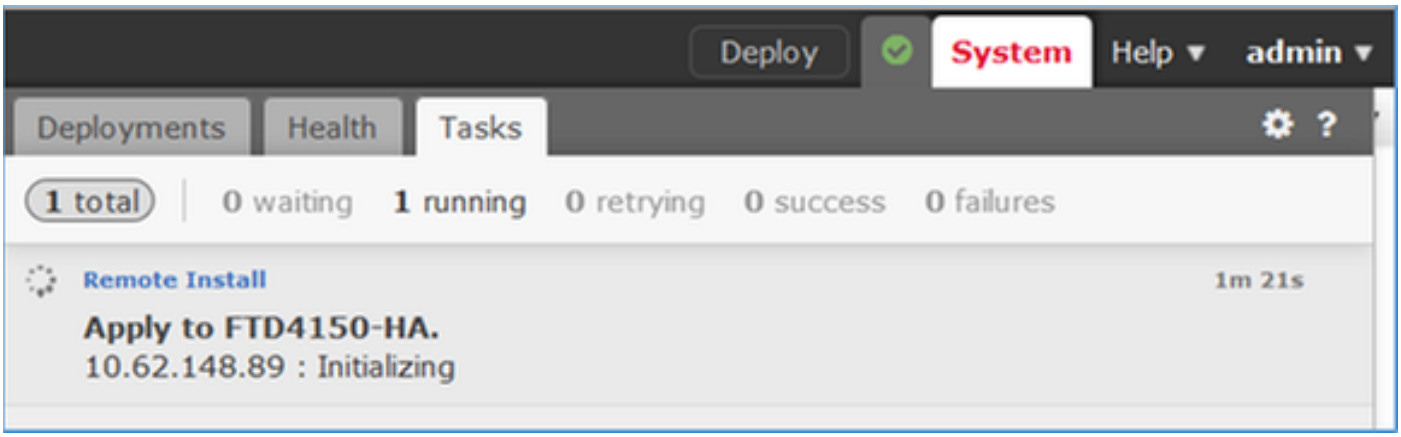


The check took ~5 min and was successful:

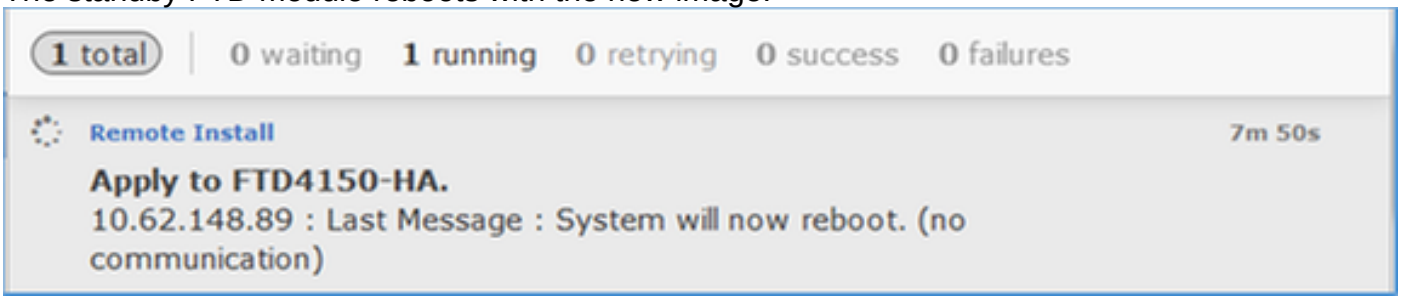


Initiate the installation process:

First the Primary/Standby FTD is upgraded:



The standby FTD module reboots with the new image:



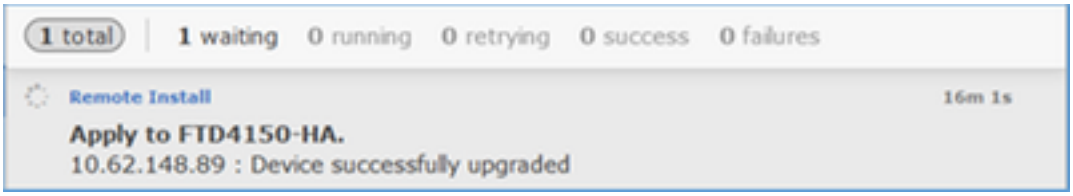
You can verify the FTD status from the FXOS BootCLI mode:

```
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
```

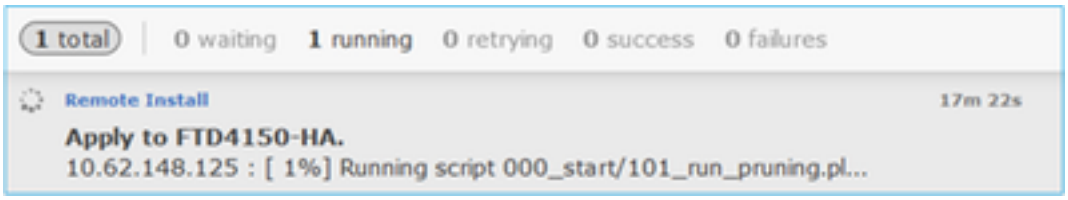
The Secondary/Active FTD CLI shows a warning message due to software version mismatch between the FTD modules:

```
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
```

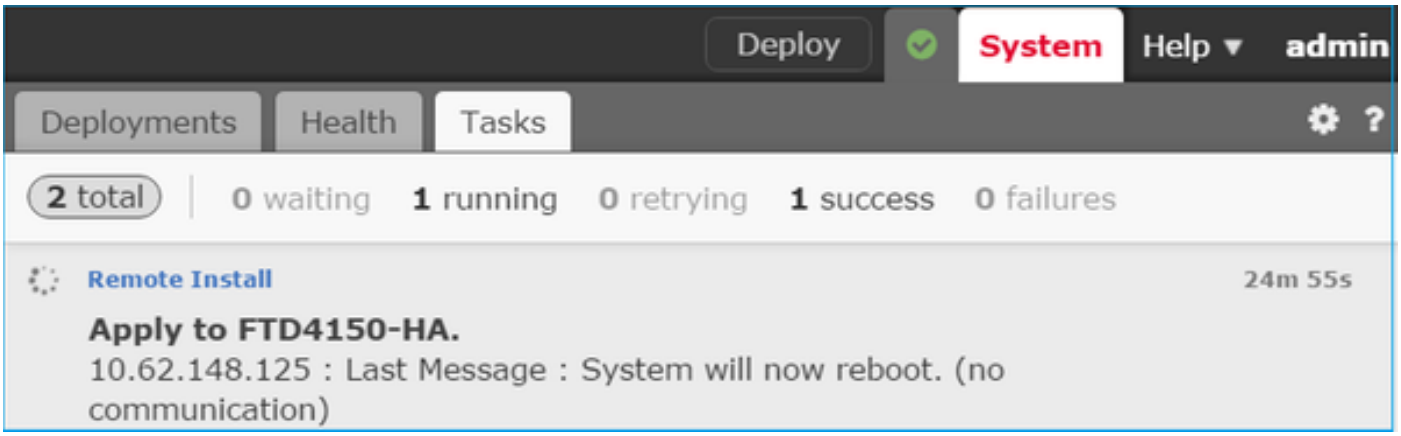
The FMC shows that the FTD device was successfully upgraded:



The upgrade of the second FTD module starts:



At the end of the process the Secondary FTD boots with the new image:



At the background the FMC, using the internal user ‘enable_1’, swaps the FTD failover states and temporarily removes the failover configuration from the Secondary FTD:

```
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#
```

Note - At this point you might see ~1 packet drop due to failover state swapping

In this case the whole FTD upgrade (both units) took ~30 minutes:

Verification

FTD CLI verification from the Primary FTD device:

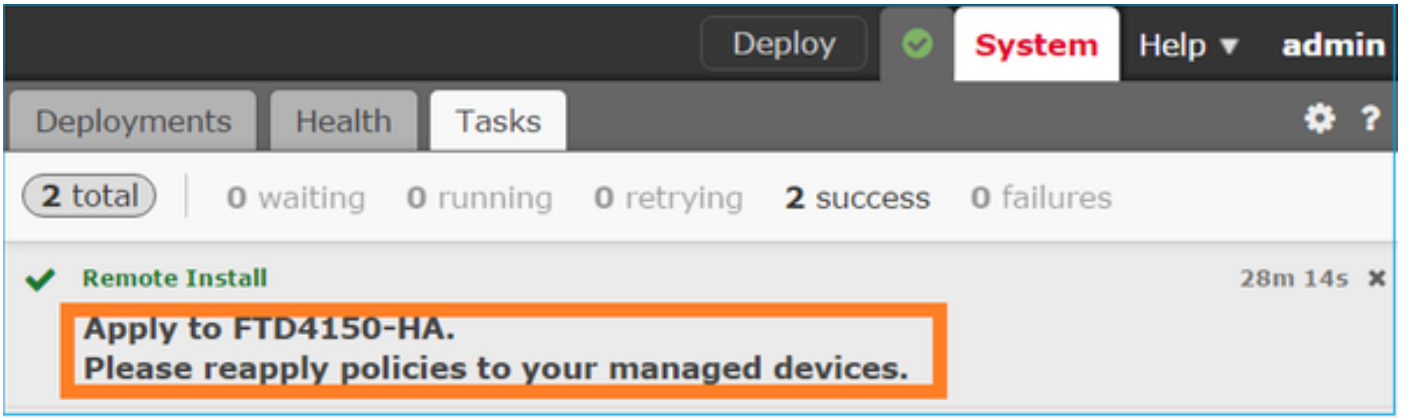
```
> show high-availability config Failover On Failover unit Primary Failover LAN Interface: FOVER Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 1041 maximum 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 ... >
```

From the Secondary FTD device:

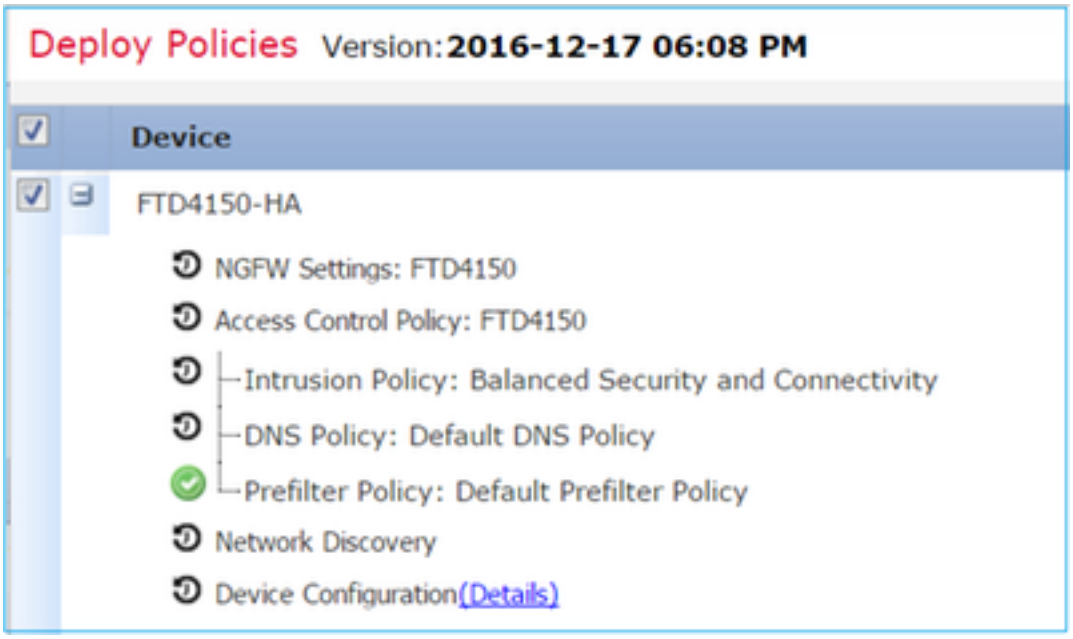
```
> show high-availability config Failover On Failover unit Secondary Failover LAN Interface: FOVER Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 1041 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
... >
```

Step 8: Deploy a policy to the FTD HA pair

After the upgrade is completed there is need to deploy a policy to the HA pair. This is shown in the FMC UI:

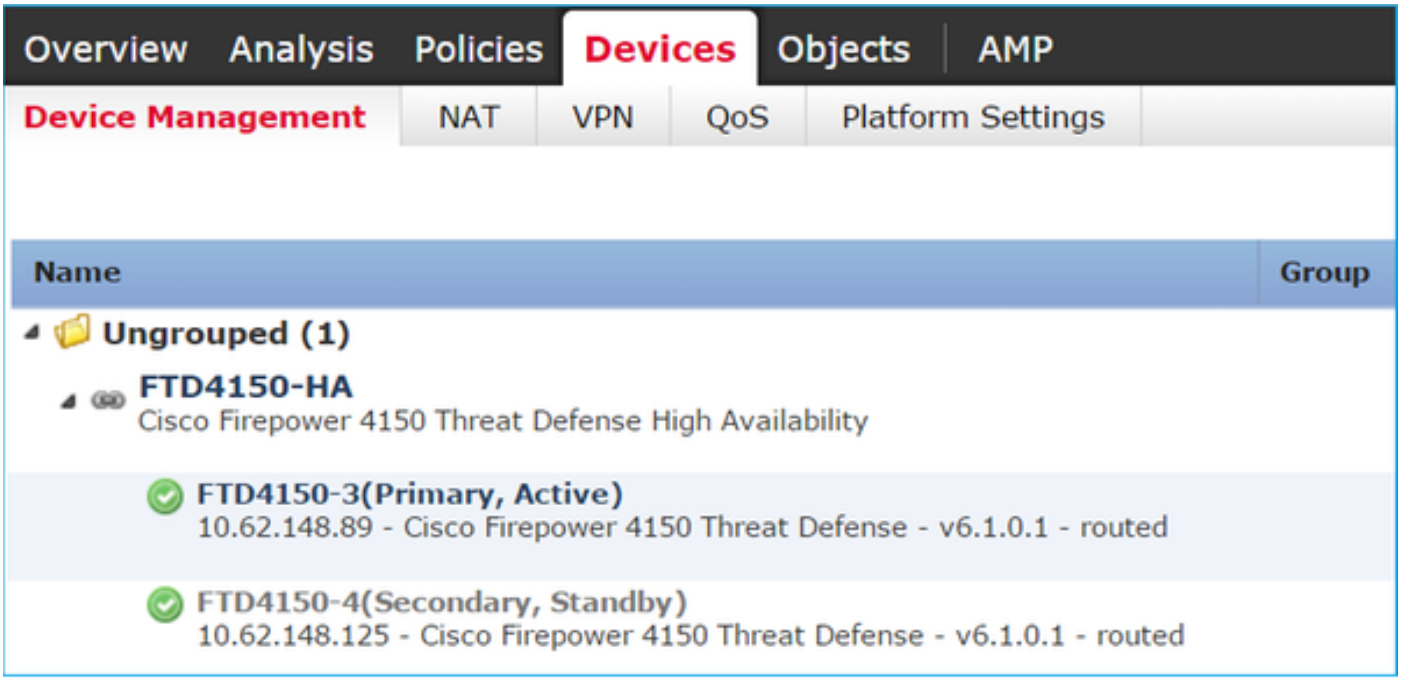


Deploy the policies:

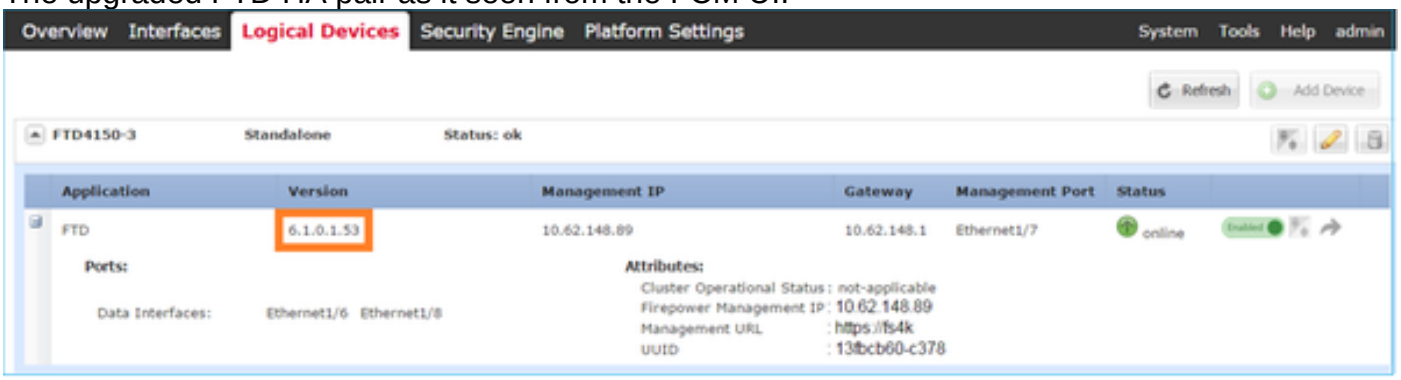


Verification

The upgraded FTD HA pair as it seen from the FMC UI:



The upgraded FTD HA pair as it seen from the FCM UI:



Related Documents

[Cisco Firepower NGFW]