Actualizando un FTD HA empareje en los dispositivos de FirePOWER

Contenido

Introducción

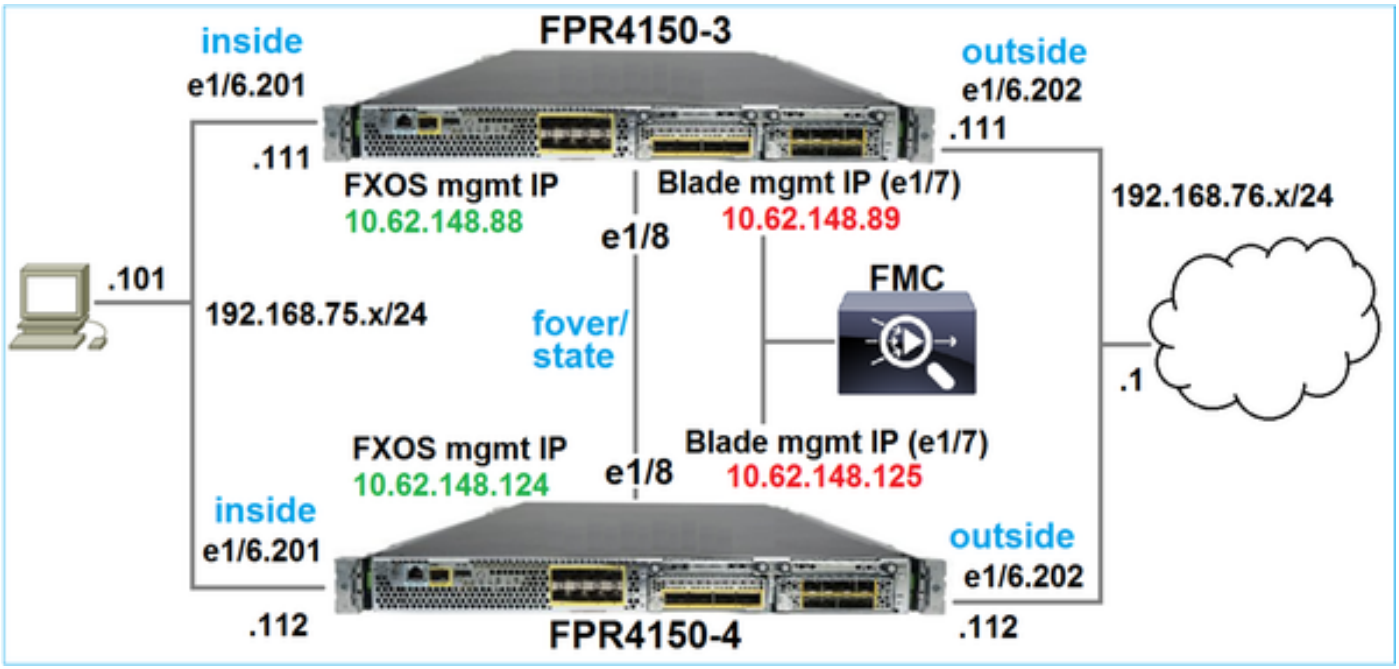
Meta

La meta de este documento es demostrar el proceso de actualización de la defensa de la amenaza de FirePOWER (FTD) en el modo de gran disponibilidad en los dispositivos de FirePOWER.

Componentes del laboratorio

- 2 x FP4150
- 1 x FS4000
- 1 PC

Topología



Las versiones de la imagen del software antes de comenzar la actividad:

- Centro de administración de FirePOWER (FMC) 6.1.0-330
- FTD 6.1.0-330 primarios
- FTD 6.1.0-330 secundarios
- FXO 2.0.1-37 primarios
- FXO 2.0.1-37 secundarios

Plan de acción

Paso 1: Marque los requisitos previos

Paso 2: Cargue las imágenes a FMC y al SSP

Paso 3: Actualice los FXO secundarios 2.0.1-37 - > 2.0.1-86

Paso 4: Intercambie la Conmutación por falla FTD (usted tendrá primario/el recurso seguro, secundario/Active)

Paso 5: Actualice los FXO primarios 2.0.1-37 - > 2.0.1-86

Paso 6: Actualice el FMC 6.1.0-330 - > 6.1.0.1

Paso 7: Actualice los pares 6.1.0-330 FTD HA - > 6.1.0.1

Paso 8: Despliegue una directiva de FMC a los pares FTD HA

El proceso de actualización FTD HA

Paso 1: Marque los requisitos previos

Consulte la guía de la compatibilidad FXO para determinar la compatibilidad en medio:

- Apunte la versión de software FTD y la versión de software FXO
- Plataforma de FirePOWER HW y versión de software FXO

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

Marque los Release Note FXO de la versión de destino para determinar el trayecto de actualización FXO:

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

Consulte los Release Note de la versión de destino FTD para determinar el trayecto de actualización FTD:

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

Paso 2: Cargue las imágenes

En los 2 FCMs carga las imágenes FXO (fxos-k9.2.0.1.86.SPA)

En la carga FMC paquetes de la actualización FMC y FTD:

- Para la actualización FMC: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- Para la actualización FTD: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

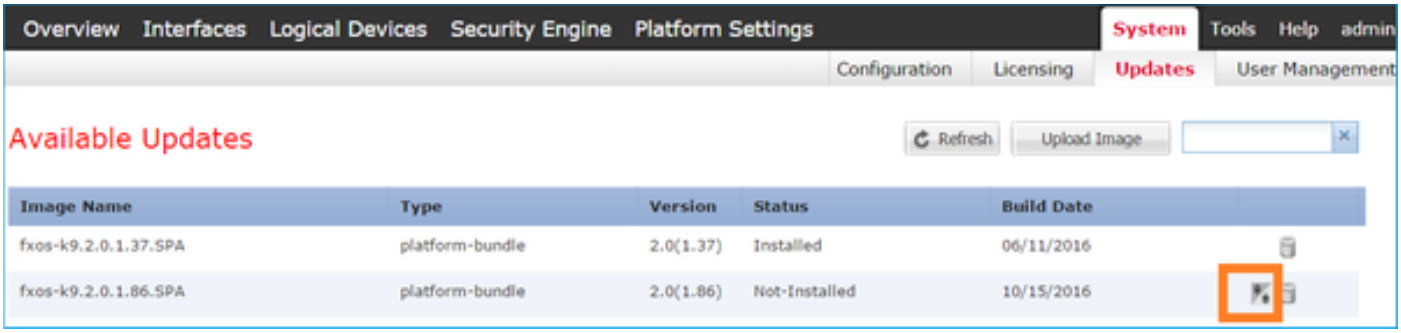
Paso 3: Actualice los FXO secundarios

Antes de la actualización:

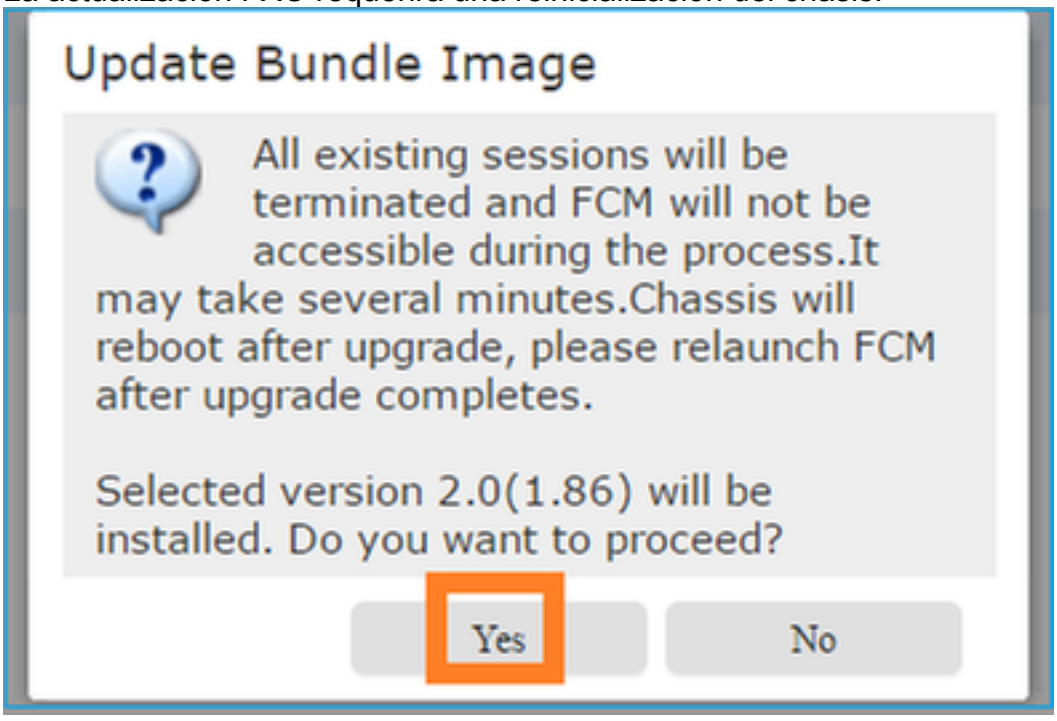
```
FPR4100-4-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.0(1.37)
```

```
    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
```

Comience la actualización FXO:



La actualización FXO requerirá una reinicialización del chasis:



Usted puede monitorear la actualización FXO de los FXO CLI. Los 3 componentes (FPRM, interconexión de la tela y chasis) tienen que ser actualizados:

```
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
```

Nota – Pocos minutos después de comenzar el proceso de actualización FXO usted puede ser que sea disconnected de FXO CLI y del GUI. Usted debe poder iniciar sesión otra vez después de pocos segundos.

Después del minuto ~5 la actualización componente FPRM completa:

```
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
```

Después de ~10 mínimos y como parte del proceso de actualización FXO que el dispositivo secundario de FirePOWER recomienza:

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

Después del reinicio los curriculums vitae del proceso de actualización:

```
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
```

Después del total del minuto ~30 la actualización FXO completa:

```
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
```

Paso 4: Intercambie los estados de la Conmutación por falla FTD

Antes de intercambiar los estados del failver aseegurese que el módulo FTD en el chasis secundario está completamente PARA ARRIBA:

```
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
      ...
```

Intercambie los estados de la Conmutación por falla FTD. Del FTD activo CLI:

```
> no failover active
        Switching to Standby

>
```

Nota - En este momento usted puede ser que haga el paquete ~1 de tráfico de tránsito FTD caer

Paso 5: Actualice el dispositivo primario FXO

Similar a la actualización del paso 2 el dispositivo FXO donde el FTD primario está instalado - este paso puede tomar ~30 minutos o más para completar.

Paso 6: Actualice el software FMC

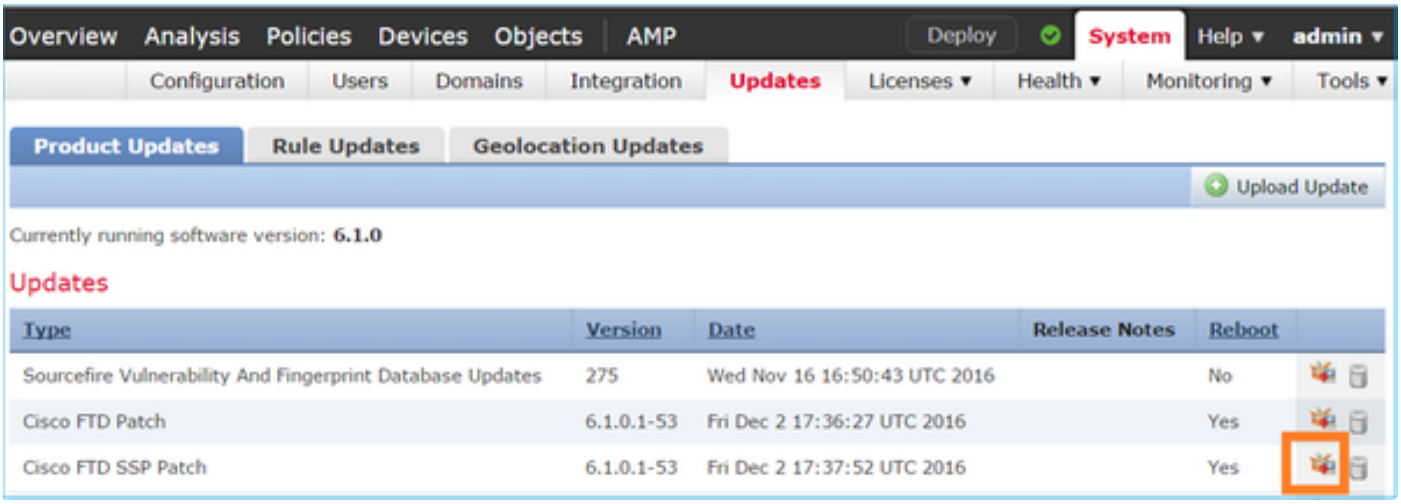
Actualice el FMC, en este escenario a partir del 6.1.0-330 a 6.1.0.1.

Paso 7: Actualice los pares FTD HA

Antes de la actualización:

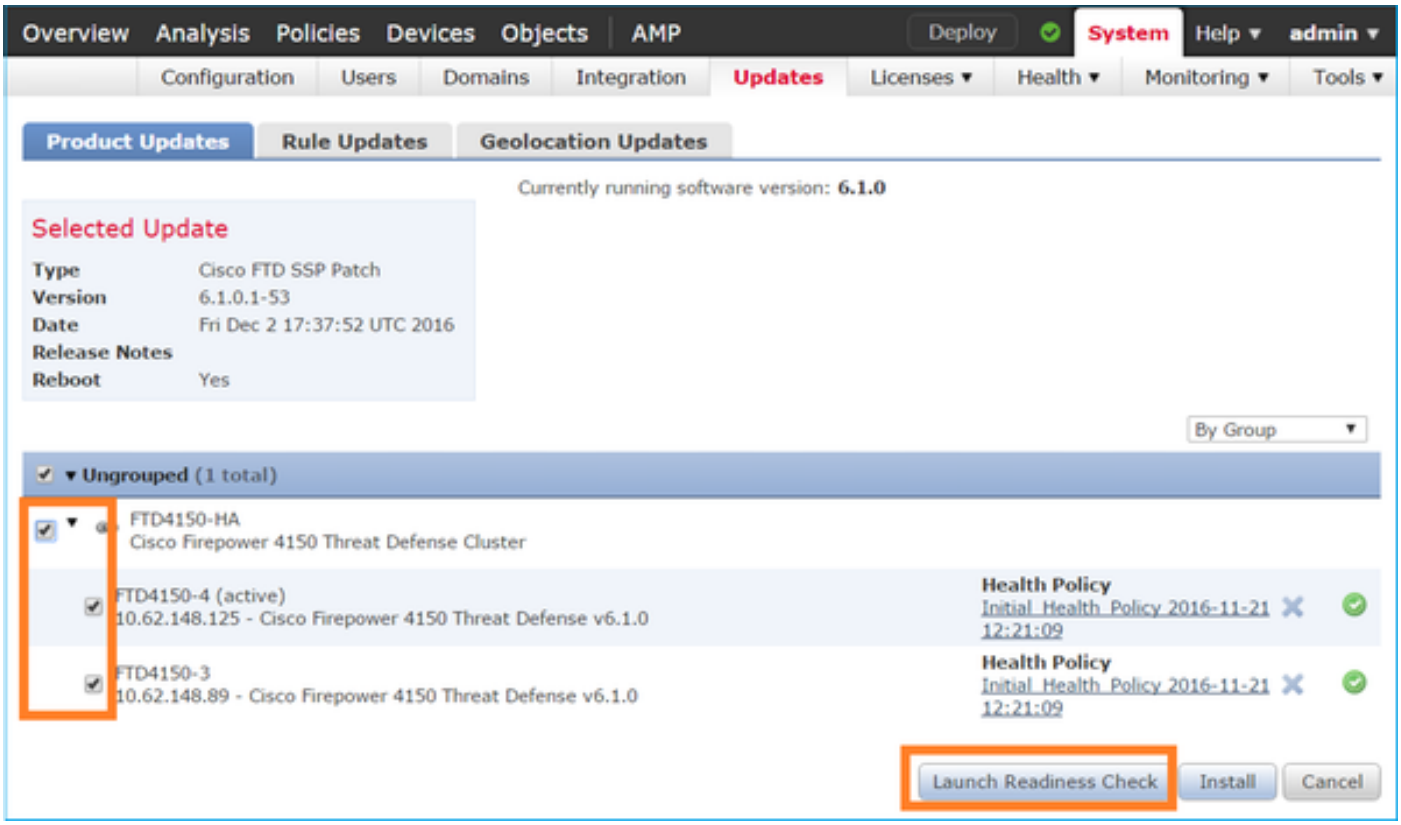
```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1041 maximum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

Del menú del **sistema > de las actualizaciones** FMC inicie el proceso de actualización FTD HA:

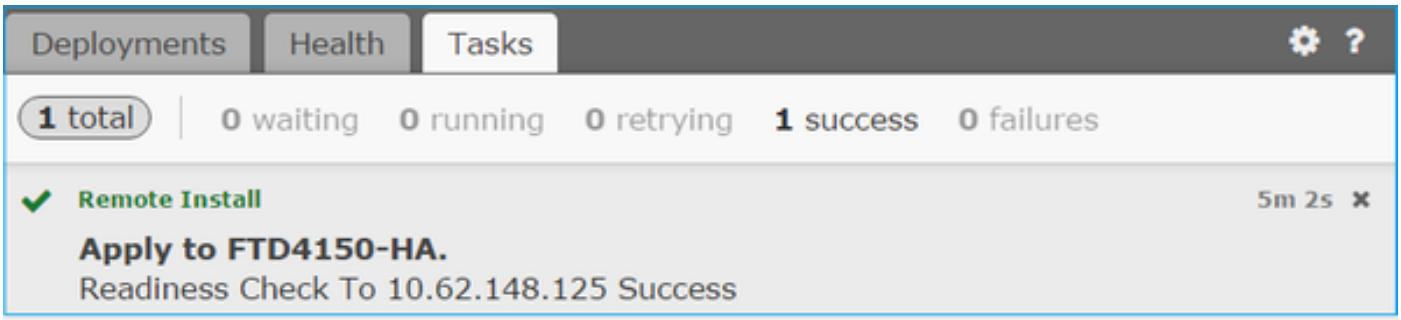


Usted puede poner en marcha opcionalmente el control de la disposición de la actualización FTD

que incluye una verificación de la integridad FTD DB:

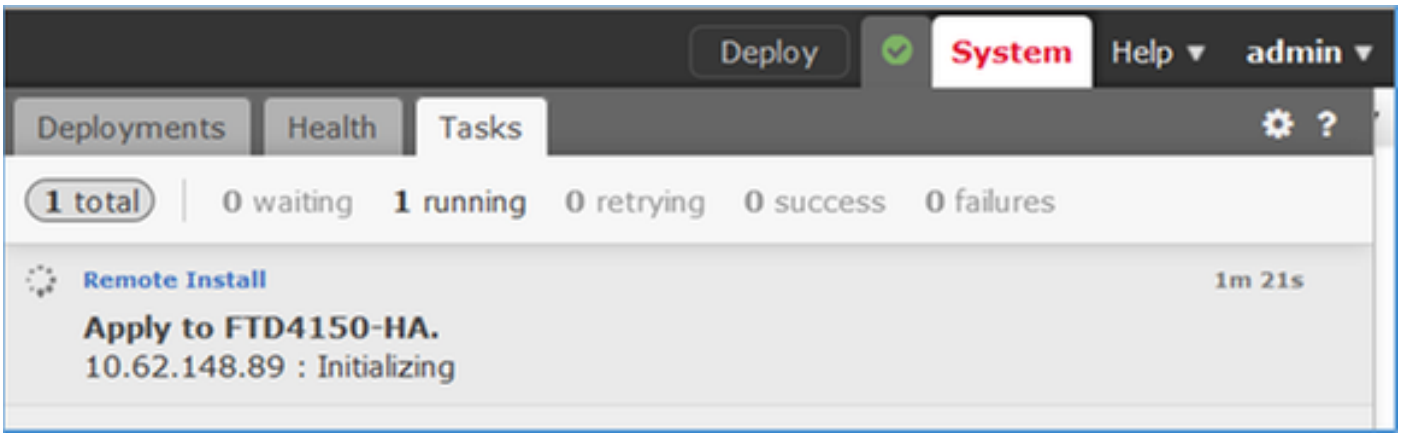


El control tomó ~5 mínimos y era acertado:

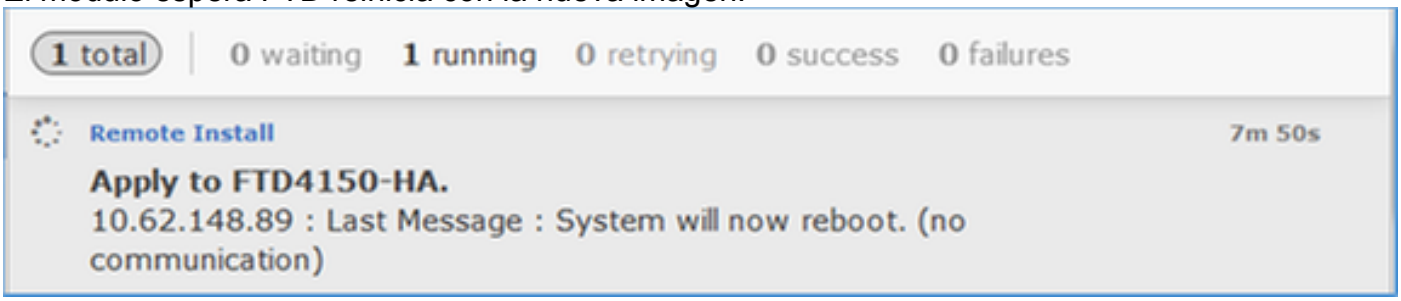


Inicie el proceso de instalación:

Se actualiza el FTD primero primario/espera:



El módulo espera FTD reinicia con la nueva imagen:



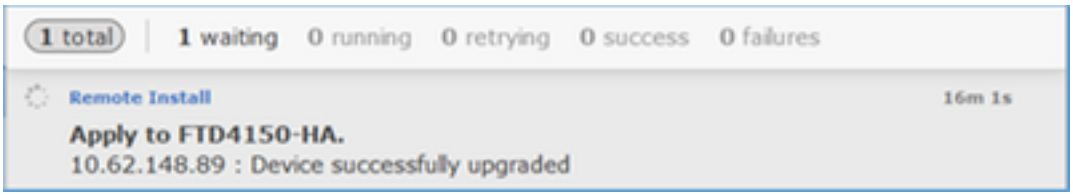
Usted puede verificar el estatus FTD del modo FXO BootCLI:

```
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
```

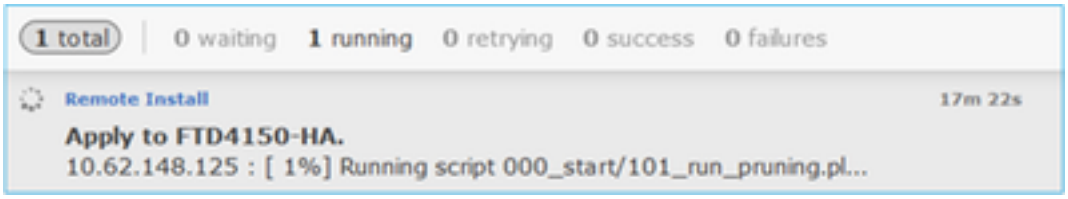
El FTD secundario/activo CLI muestra un mensaje de advertencia debido a la discordancía de la versión de software entre los módulos FTD:

```
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
```

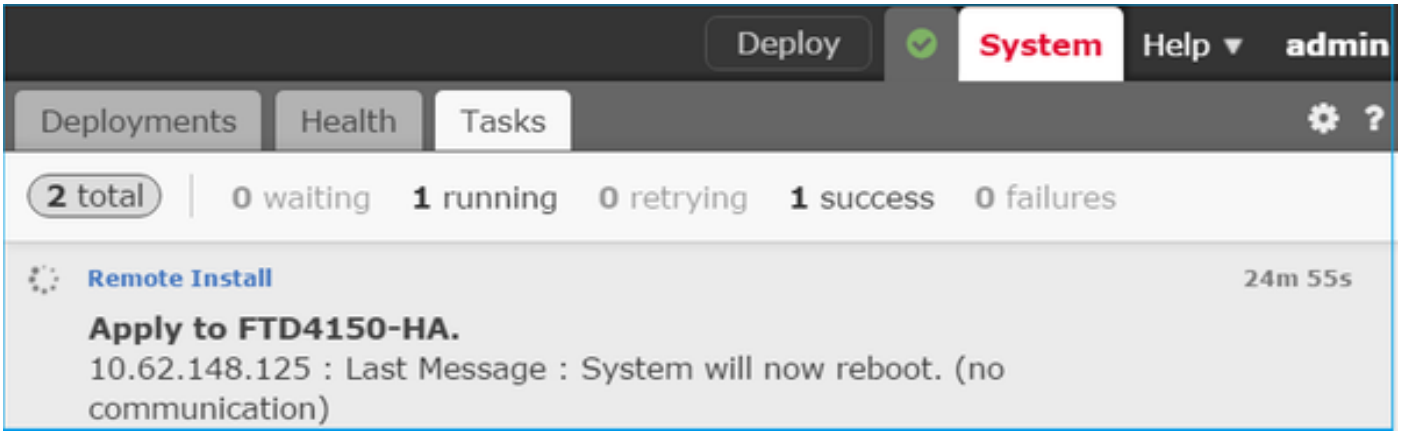
El FMC muestra que el dispositivo FTD fue actualizado con éxito:



La actualización del segundo módulo FTD comienza:



En el final del proceso el FTD secundario inicia con la nueva imagen:



En el fondo el FMC, usando el usuario interno “enable_1”, intercambia los estados de la Conmutación por falla FTD y quita temporalmente la configuración de failover del FTD secundario:

```
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#
```

Nota - En este momento usted puede ser que vea la caída de paquetes ~1 debido al intercambio del estado de la Conmutación por falla

En este caso la actualización entera FTD (ambas unidades) tardó ~30 minutos:

Verificación

Verificación FTD CLI del dispositivo primario FTD:

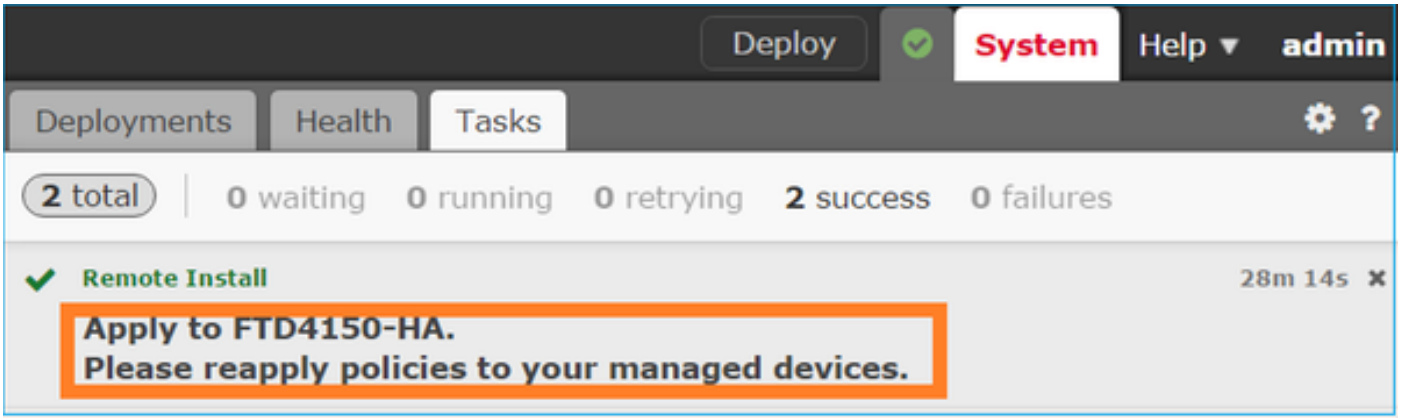
```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1041 maximum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

Del dispositivo secundario FTD:

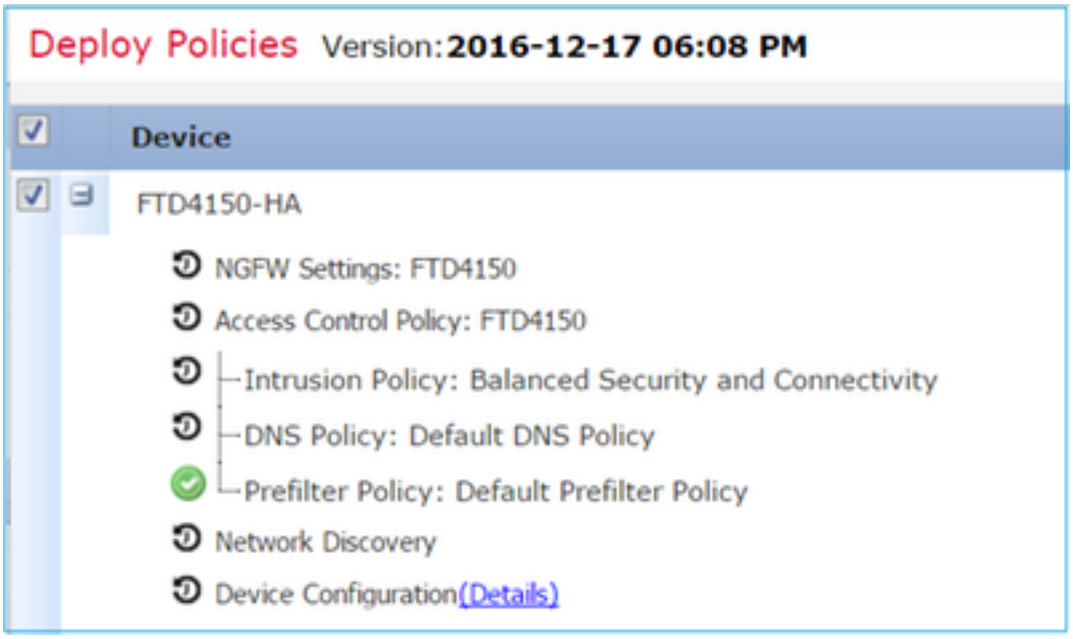
```
> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1041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

Paso 8: Despliegue una directiva a los pares FTD HA

Después de que se complete la actualización hay necesidad de desplegar una directiva a los pares HA. Esto se muestra en el FMC UI:

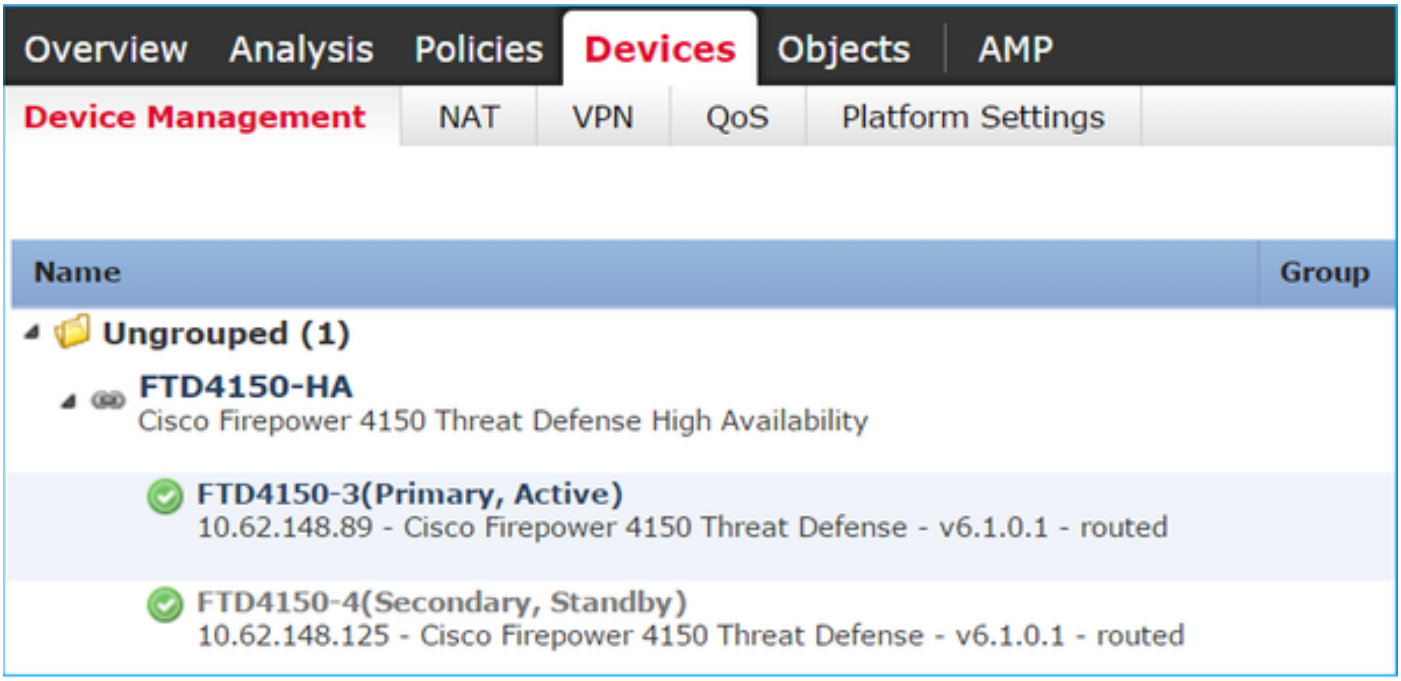


Despliegue las directivas:

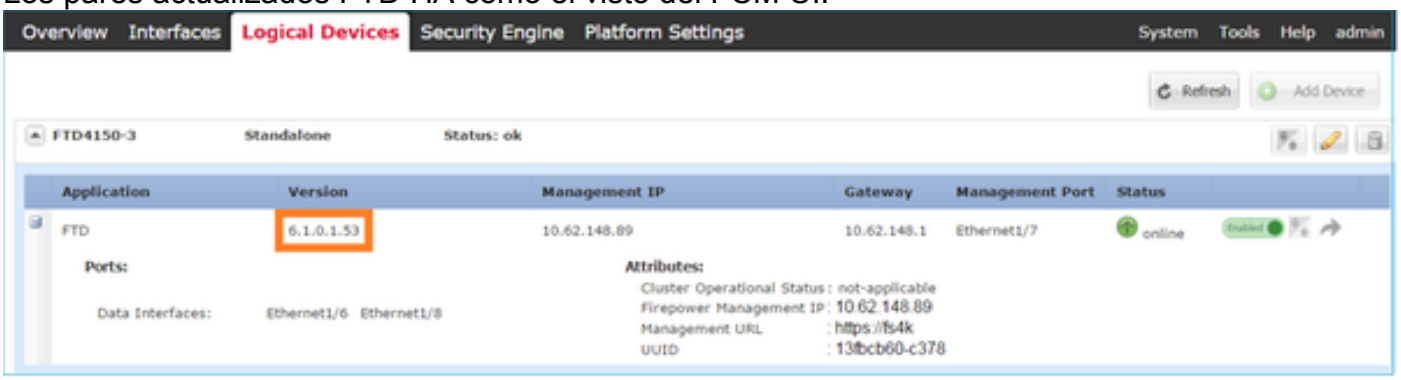


Verificación

Los pares actualizados FTD HA como ella vista del FMC UI:



Los pares actualizados FTD HA como él visto del FCM UI:



Documentos Relacionados

Cisco FirePOWER NGFW