升级FTD HA请配对在Firepower设备

目录

简介
目标
实验室组件
拓扑
FTD HA升级进程
步骤 1：检查前提条件
步骤 2： 上载镜像
步骤 3： 升级第二FXO
步骤 4： 交换FTD故障切换状态
步骤 5：升级主要的FXO设备
步骤 6：升级FMC软件
步骤 7：升级FTD HA对
步骤 8:实施策略对FTD HA对
相关文档

简介

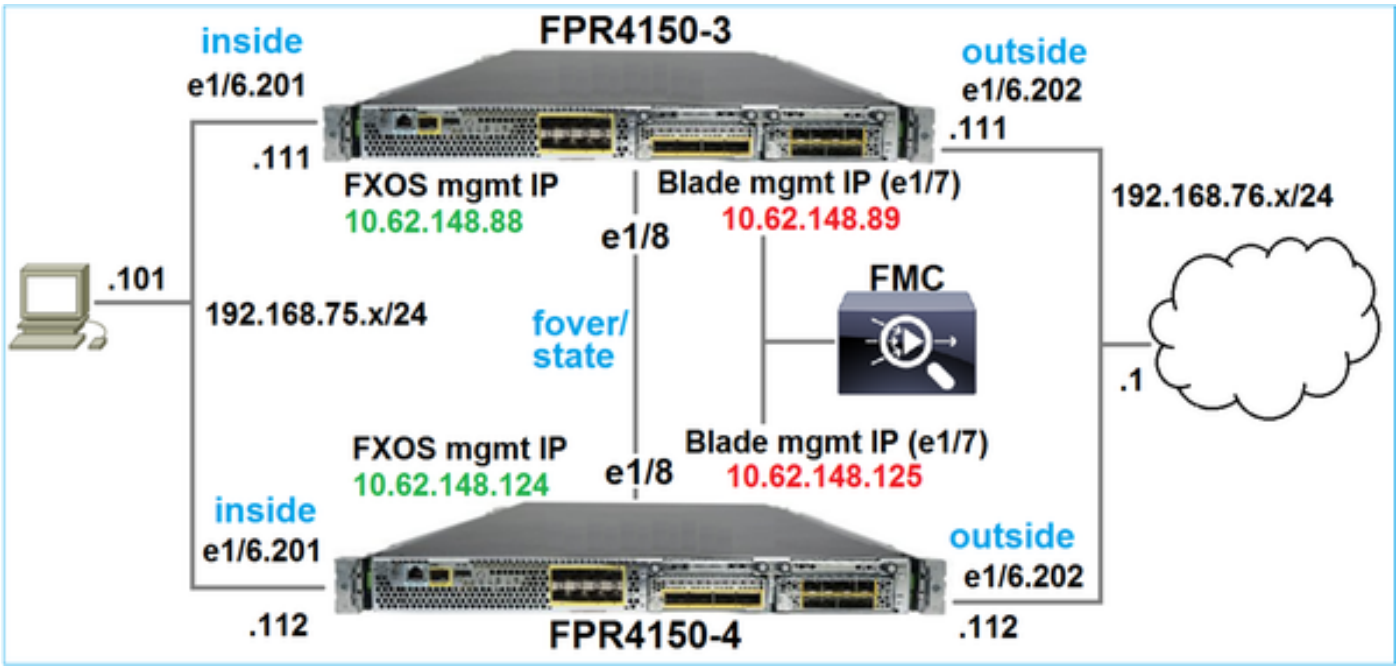
目标

本文目标是展示升级进程Firepower威胁防御(FTD)在Firepower设备的高性能的模式。

实验室组件

- 2 x FP4150
- 1个x FS4000
- 1个PC

拓扑



在开始活动前的软件镜像版本：

- Firepower管理中心(FMC) 6.1.0-330
- FTD主要的6.1.0-330
- FTD第二6.1.0-330
- FXO主要的2.0.1-37
- FXO第二2.0.1-37

行动计划

步骤 1：检查前提条件

步骤 2：上载镜像对FMC和SSP

步骤 3：升级第二FXO 2.0.1-37 - > 2.0.1-86

步骤 4：交换FTD故障切换(您将有主要的/待机、第二/激活)

步骤 5：升级主要的FXO 2.0.1-37 - > 2.0.1-86

步骤 6：升级FMC 6.1.0-330 - > 6.1.0.1

步骤 7：升级FTD HA对6.1.0-330 - > 6.1.0.1

步骤 8:实施从FMC的一项策略到FTD HA对

FTD HA升级进程

步骤 1：检查前提条件

参见FXO兼容性指南确定兼容性之间：

- 瞄准FTD软件版本和FXO软件版本
- Firepower HW平台和FXO软件版本

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

检查目标版本的FXO版本注释确定FXO升级路径：

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

参见FTD目标版本版本注释确定FTD升级路径：

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

步骤 2：上载镜像

在2 FCMs上传FXO制作镜像(fxos-k9.2.0.1.86.SPA)

在FMC加载FMC和FTD升级包：

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

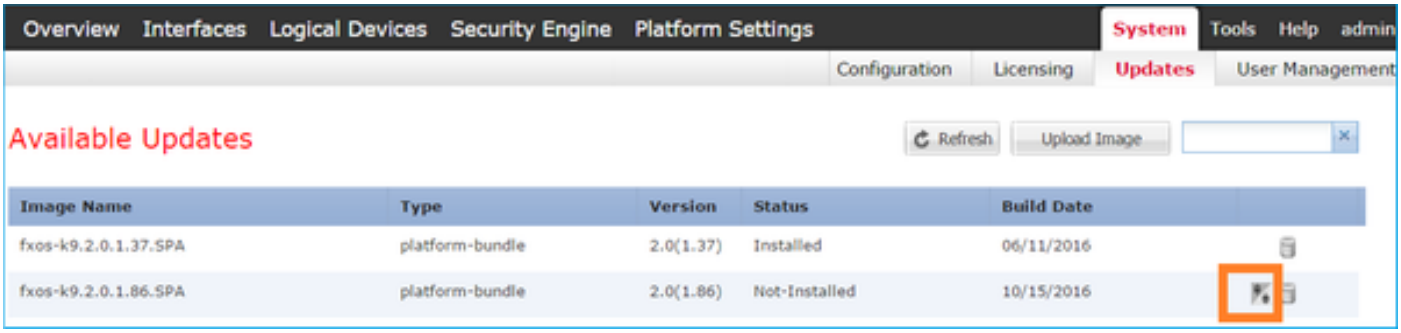
步骤 3：升级第二FXO

在升级前：

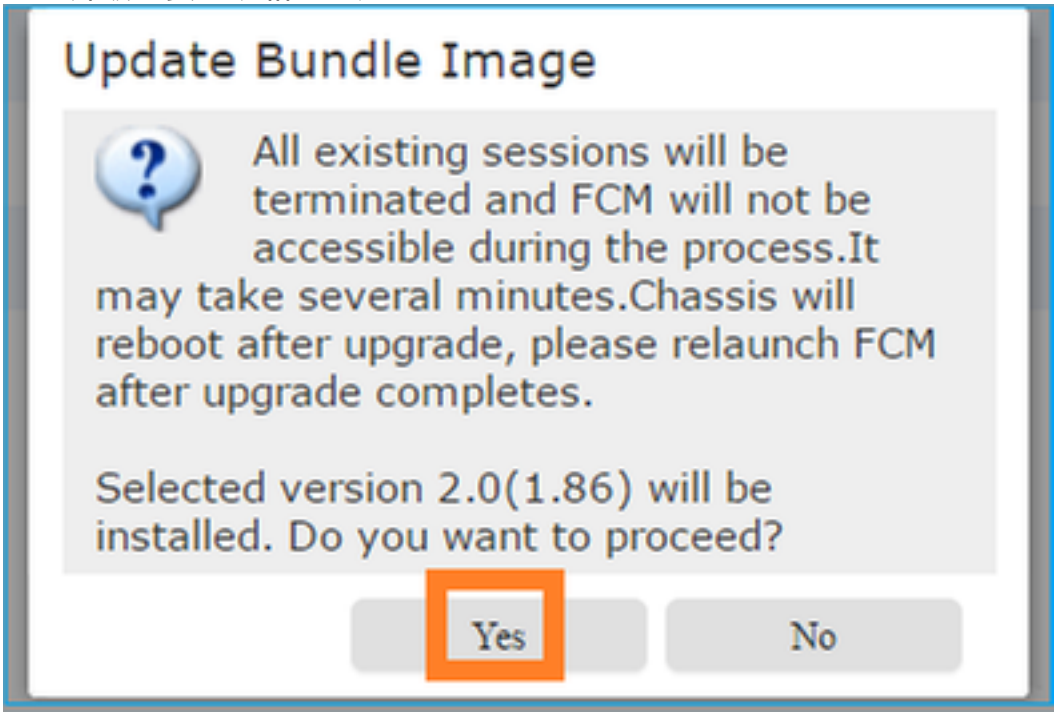
```
FPR4100-4-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.0(1.37)
    Upgrade-Status: Ready

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
```

开始FXO升级：



FXO升级将要求机箱重新启动：



您能监控从FXO CLI的FXO升级。全部3个组件(FPRM、结构互连和机箱)必须升级：

```
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
```

注意–在开始FXO升级进程以后的少量分钟您也许从FXO CLI和GUI被断开。您应该能在少量秒钟之后再登陆。

在~5分钟之后FPRM组分升级完成：

```
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
```

在~10分钟之后和作为FXO升级进程的部分第二Firepower设备重新启动：

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

在重新启动以后升级进程恢复：

```
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
```

在总计~30分钟以后FXO升级完成：

```
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
```

步骤 4：交换FTD故障切换状态

在交换前failver状态确保，在附属机箱的FTD模块充分地上升：

```
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
      ...
```

交换FTD故障切换状态。从激活FTD CLI ：

```
> no failover active
        Switching to Standby

>
```

注意-这时您也许安排~1数据包FTD中转流量丢弃

步骤 5：升级主要的FXO设备

类似于步骤2升级主要的FTD安装的FXO设备-此步骤能采取~30分钟或更多完成。

步骤 6：升级FMC软件

升级FMC，在从6.1.0-330的此方案到6.1.0.1。

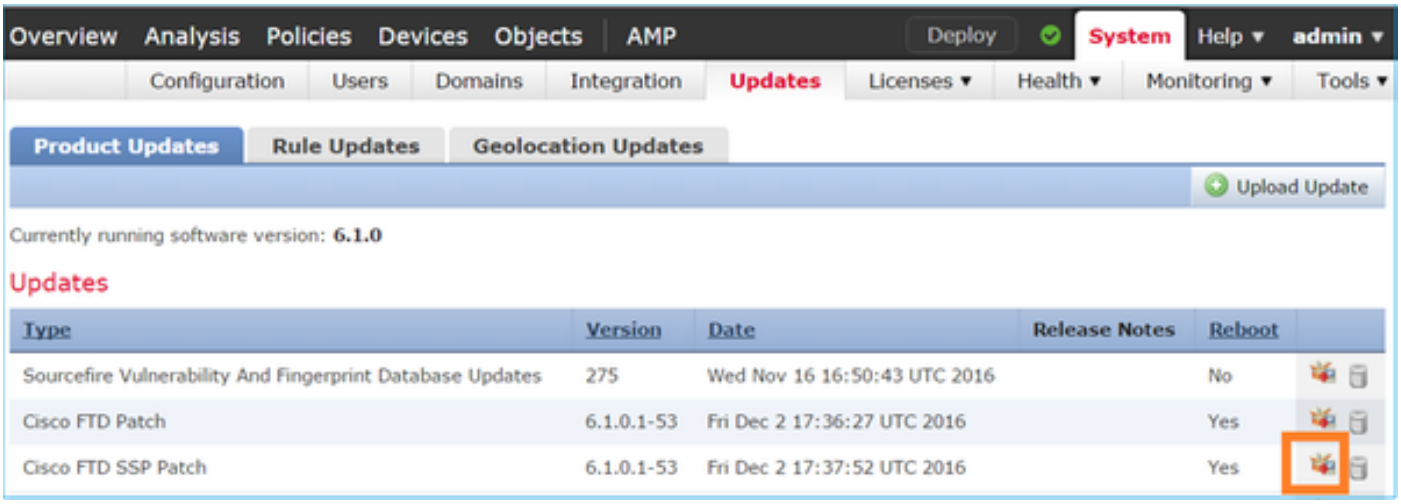
步骤 7：升级FTD HA对

在升级前：

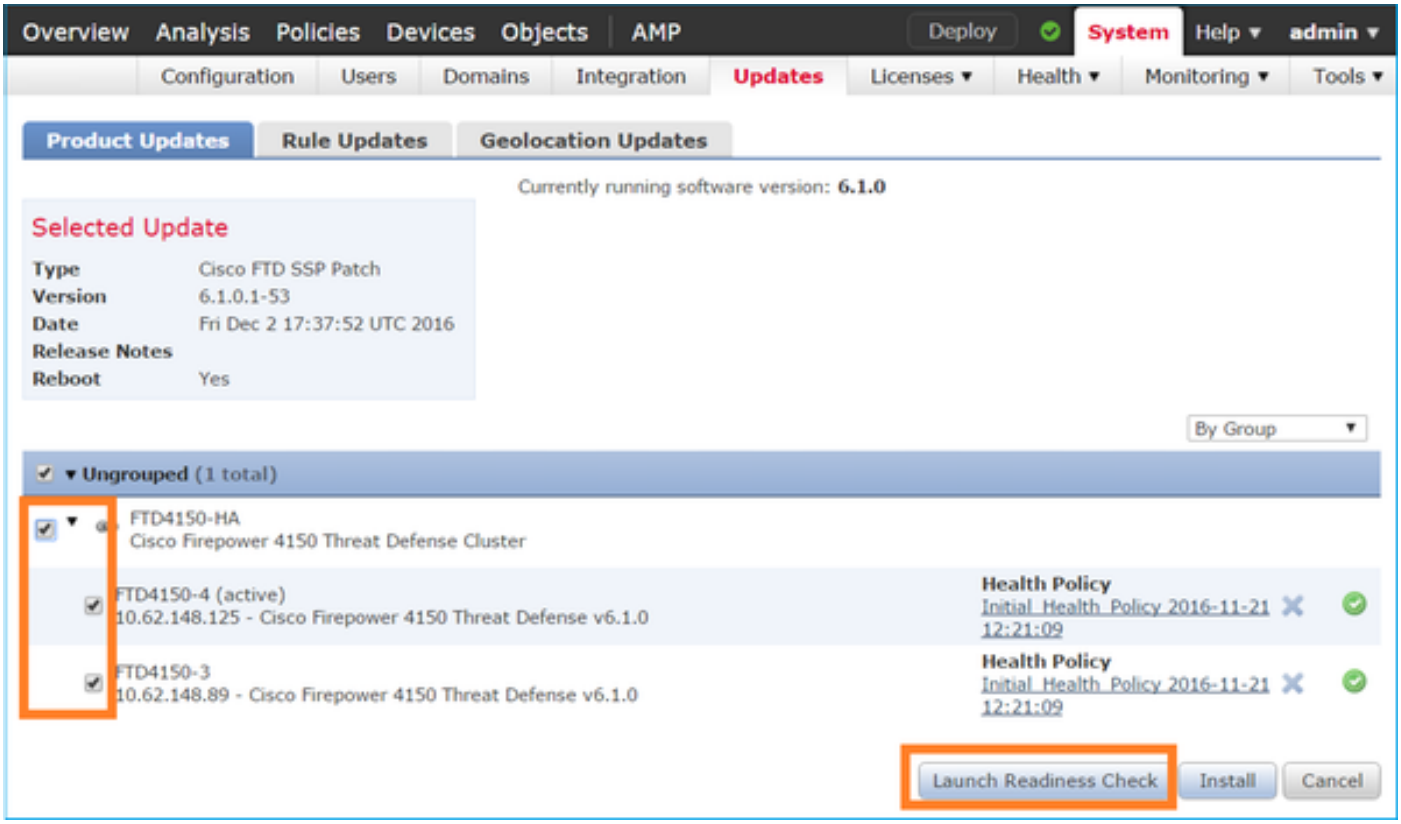
```
> show high-availability config
Failover On
Failover unit Primary
```

```
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
...
```

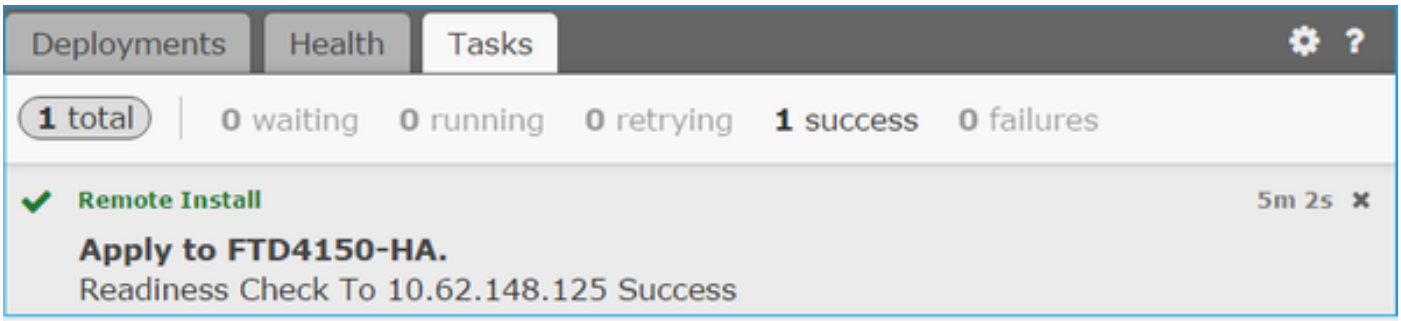
从FMC**系统>更新**菜单请开始FTD HA升级进程：



随意地您能启动包括FTD DB完整性检查的FTD升级准备检查：

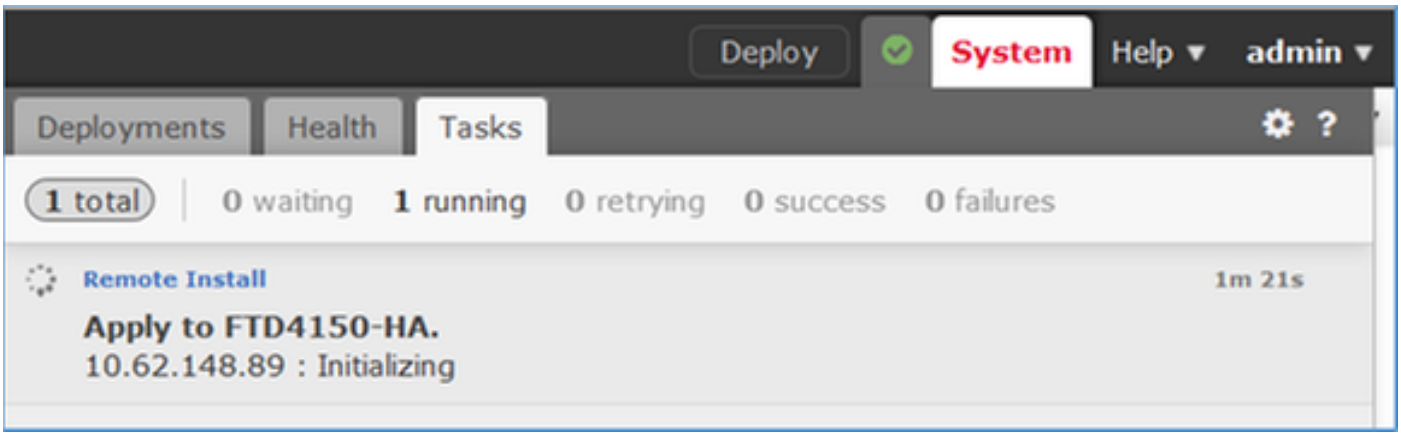


检查采取了~5分钟并且是成功的：

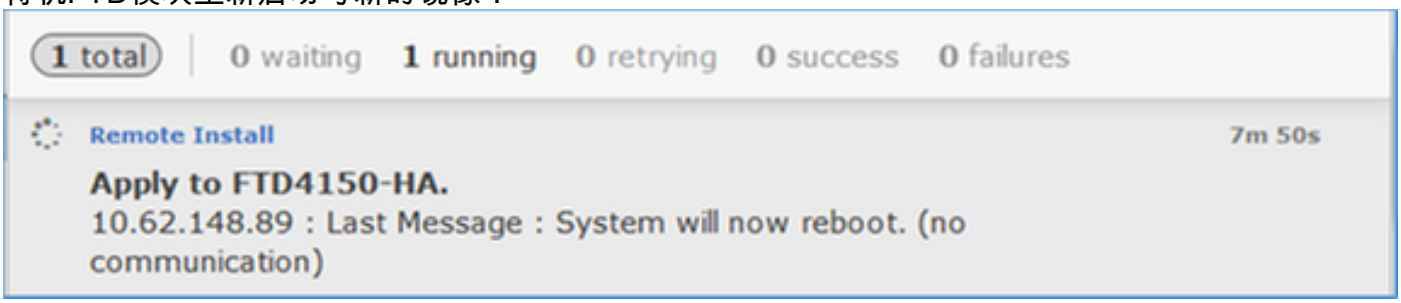


开始安装过程：

首先主要的/待机FTD升级：



待机FTD模块重新启动与新的镜像：



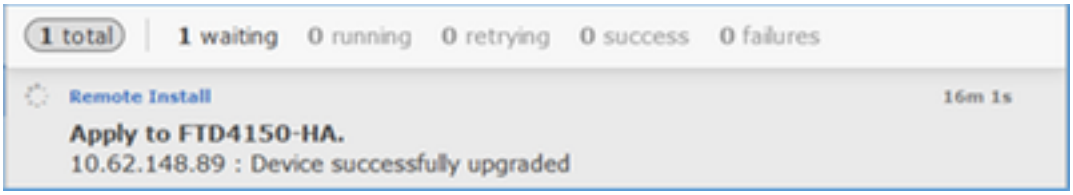
您能验证从FXO BootCLI模式的FTD状态：

```
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
```

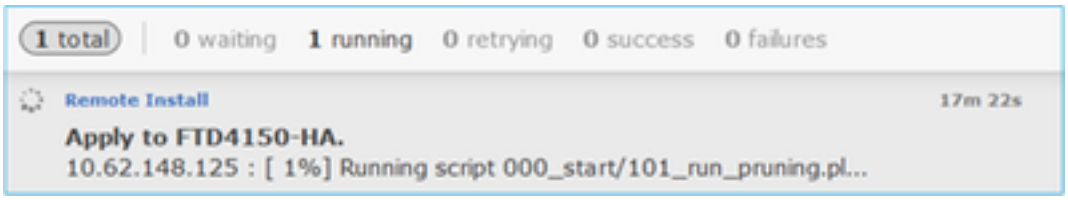
附属/激活FTD CLI表示警告消息由于FTD模块之间的软件版本不匹配：

```
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
```

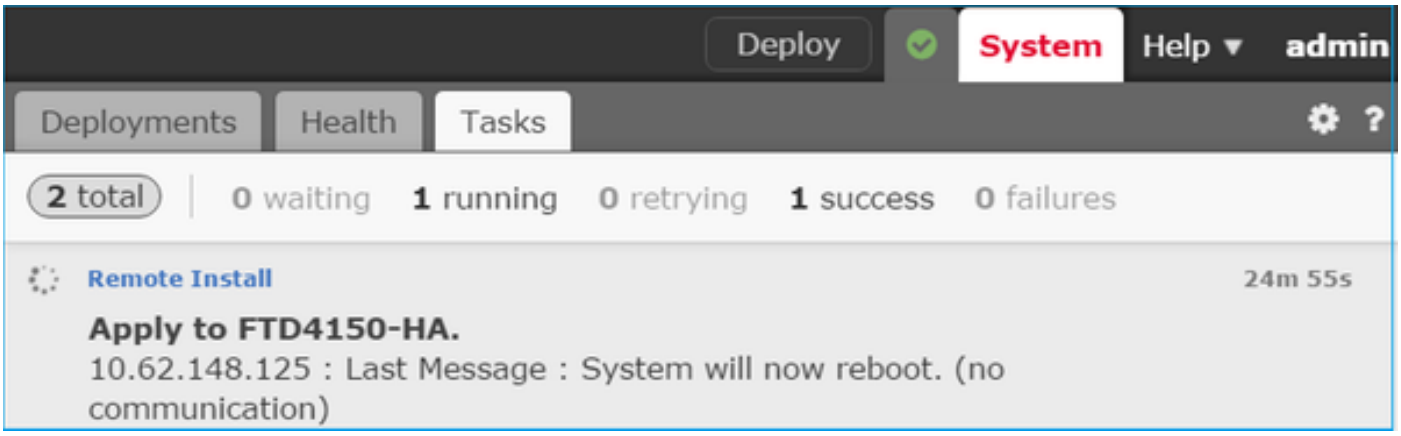
FMC显示FTD设备顺利地升级：



第二个FTD模块的升级开始：



在进程结束时第二FTD启动与新的镜像：



在背景FMC，使用内部用户“enable_1’，交换FTD故障切换状态和从第二FTD临时地删除故障切换配置：

```
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#
```

注意-这时您也许发现~1丢包由于故障切换状态交换

在这种情况下全部的FTD升级(两个单元)花费了~30分钟：

验证

FTD从主要的FTD设备的CLI验证：

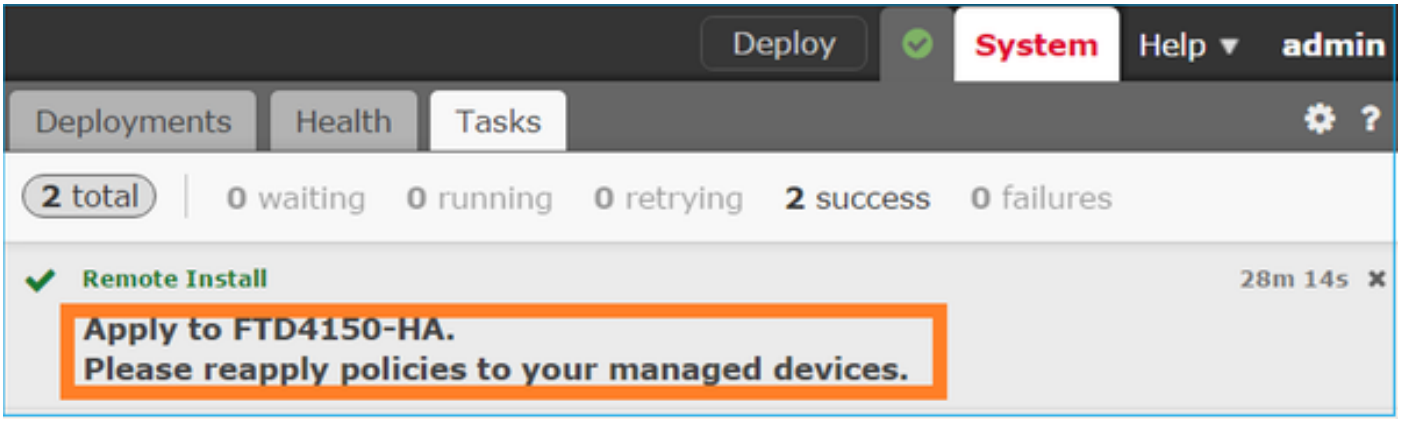
```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1041 maximum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

从第二FTD设备：

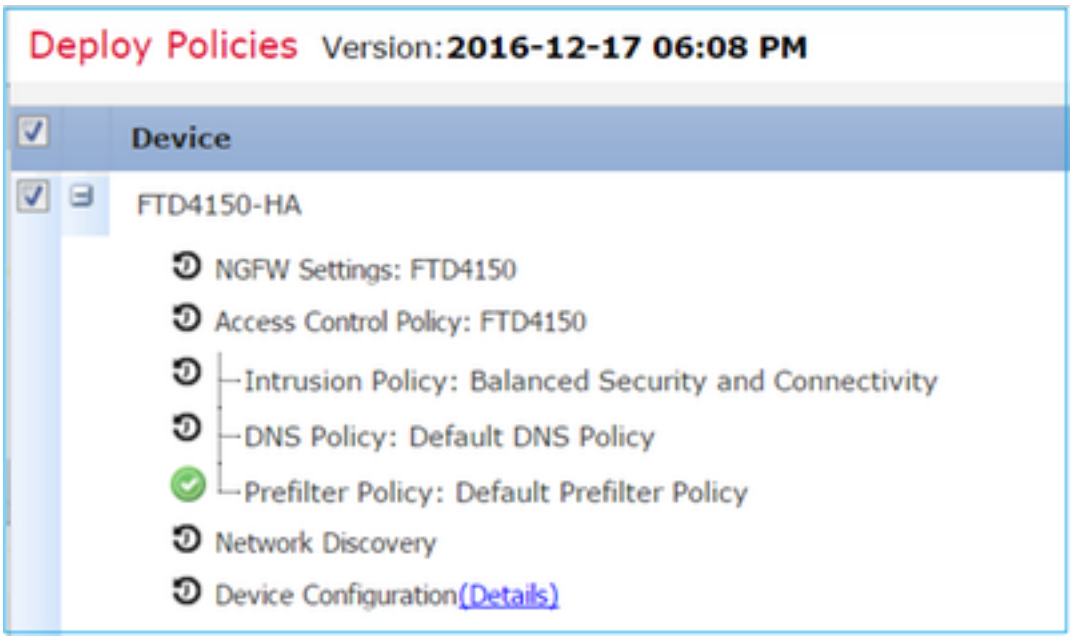
```
> show high-availability config
Failover On
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1041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

步骤 8::实施策略对FTD HA对

在升级完成后有需要实施策略到HA对。这在FMC UI显示：

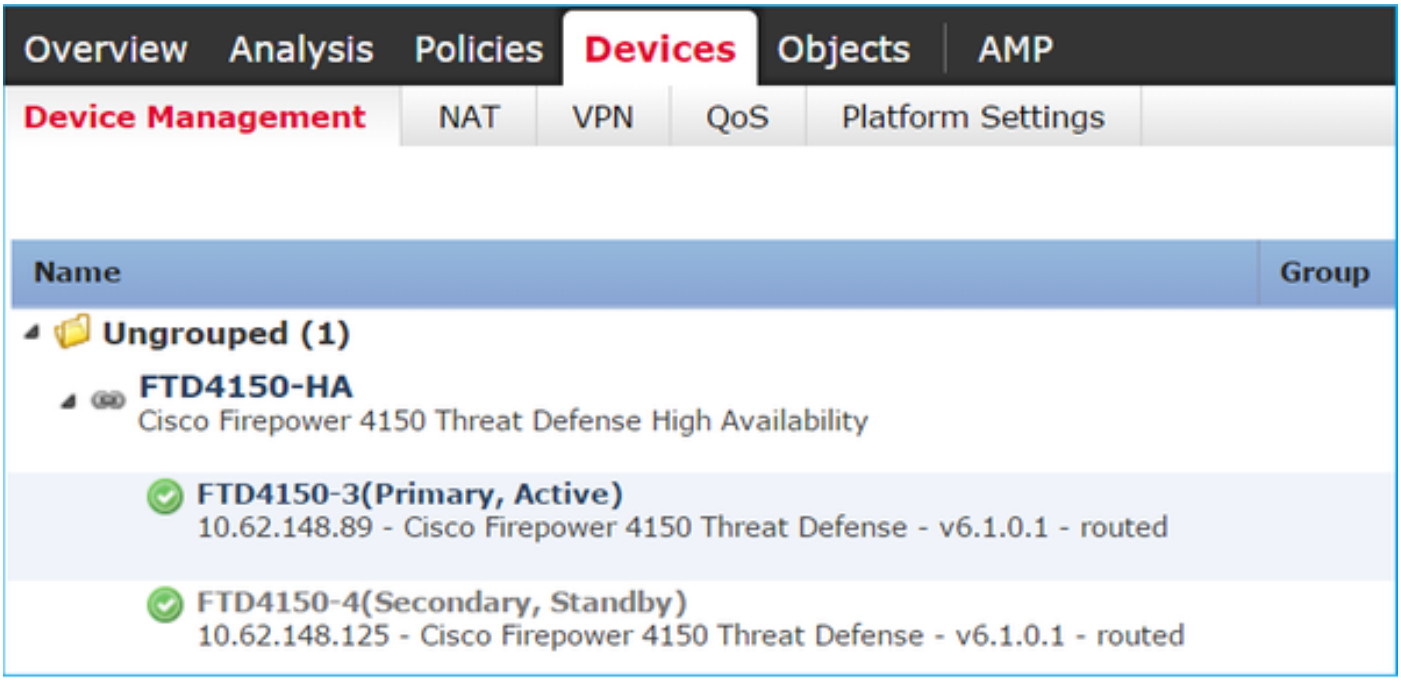


实施策略：

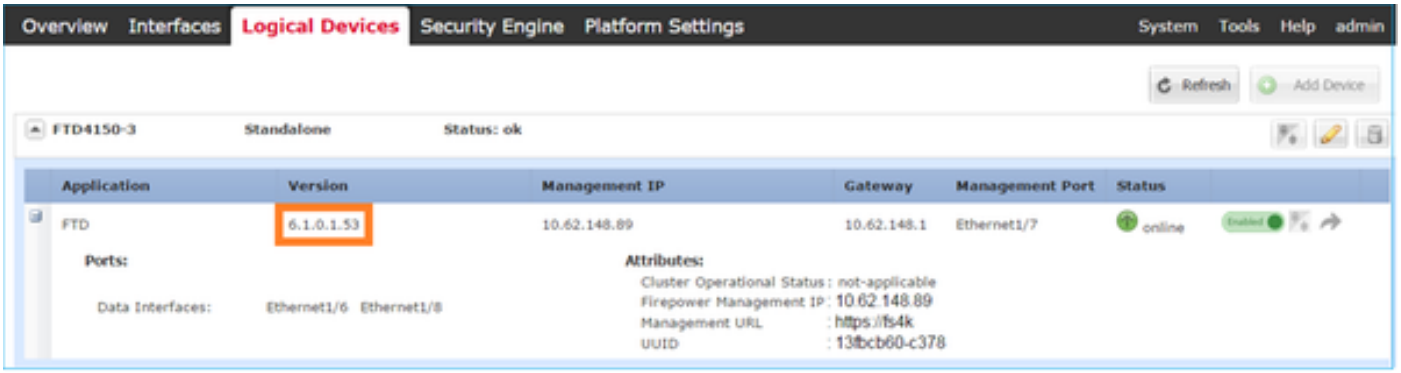


验证

升级的FTD HA对作为从FMC UI看到的它：



升级的FTD HA对作为从FCM UI看到的它：



相关文档

[思科Firepower NGFW]