Обновление FTD HA пара на устройствах Огневой мощи

Содержание

Введение

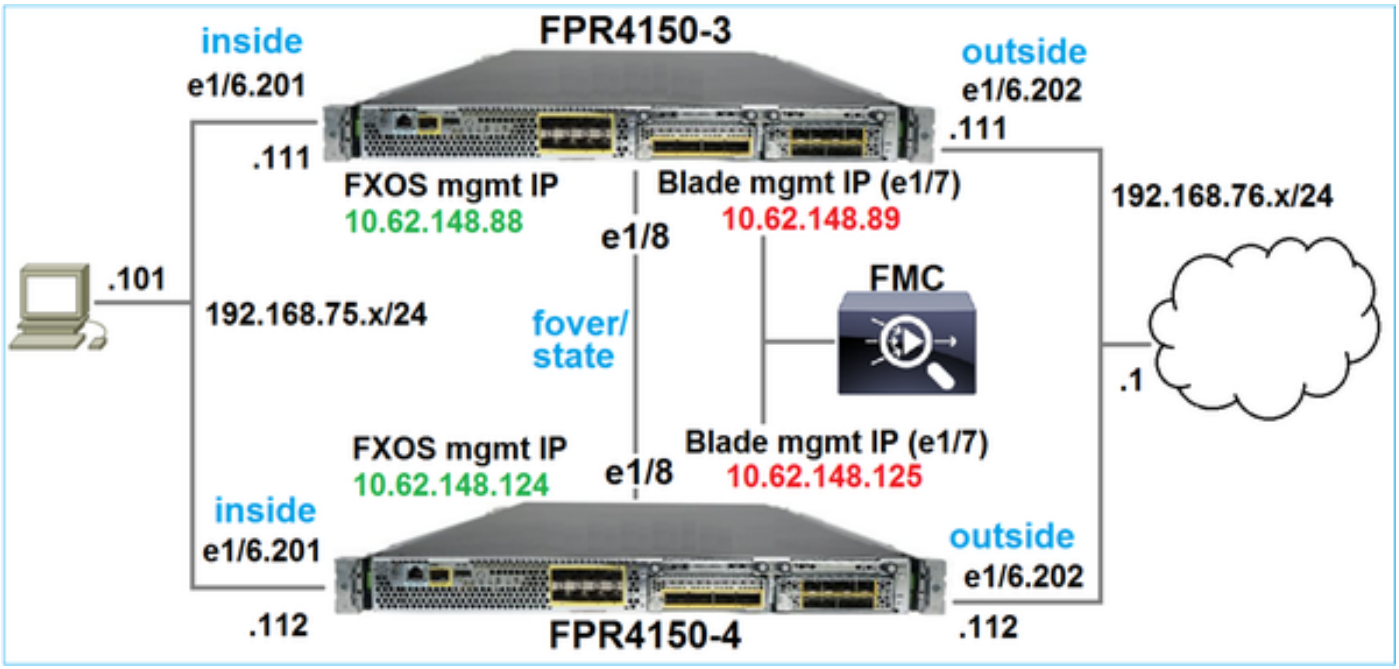
Цель

Цель этого документа состоит в том, чтобы продемонстрировать процесс обновления Защиты угрозы огневой мощи (FTD) в режиме Высокой доступности на устройствах Огневой мощи.

Компоненты лабораторной работы

- 2 x FP4150
- 1 x FS4000
- 1 пк

Топология



Версии образа программы прежде, чем запустить действие:

- Центр управления огневой мощи (FMC) 6.1.0-330
- FTD основные 6.1.0-330
- FTD вторичные 6.1.0-330
- FXOS основные 2.0.1-37
- FXOS вторичные 2.0.1-37

План действий

Шаг 1: Проверьте предварительные условия

Шаг 2: Загрузите образы к FMC и SSP

Шаг 3: Обновите Вторичный FXOS 2.0.1-37-> 2.0.1-86

Шаг 4. : Подкачайте аварийное переключение FTD (вы будете иметь Основным/Резервным, Вторичным/Активным),

Шаг 5. : Обновите Основной FXOS 2.0.1-37-> 2.0.1-86

Шаг 6: Обновите FMC 6.1.0-330-> 6.1.0.1

Шаг 7: Обновите FTD HA пара 6.1.0-330-> 6.1.0.1

Шаг 8: Разверните политику от FMC до FTD HA пара

FTD HA процесс обновления

Шаг 1: Проверьте предварительные условия

Консультируйтесь с Руководством по совместимости FXOS для определения совместимости между:

- Предназначайтесь для версии программного обеспечения FTD и версии программного обеспечения FXOS
- Платформа HW огневой мощи и версия программного обеспечения FXOS

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

Проверьте Комментарии к выпуску FXOS нужной версии для определения пути повышения FXOS:

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

Консультируйтесь с Комментариями к выпуску нужной версии FTD для определения пути повышения FTD:

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

Шаг 2: Загрузите образы

На 2 FCMs загружают образы FXOS (fxos-k9.2.0.1.86. SPA)

На FMC загружают FMC и пакеты обновления FTD:

- Для обновления FMC: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- Для обновления FTD: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

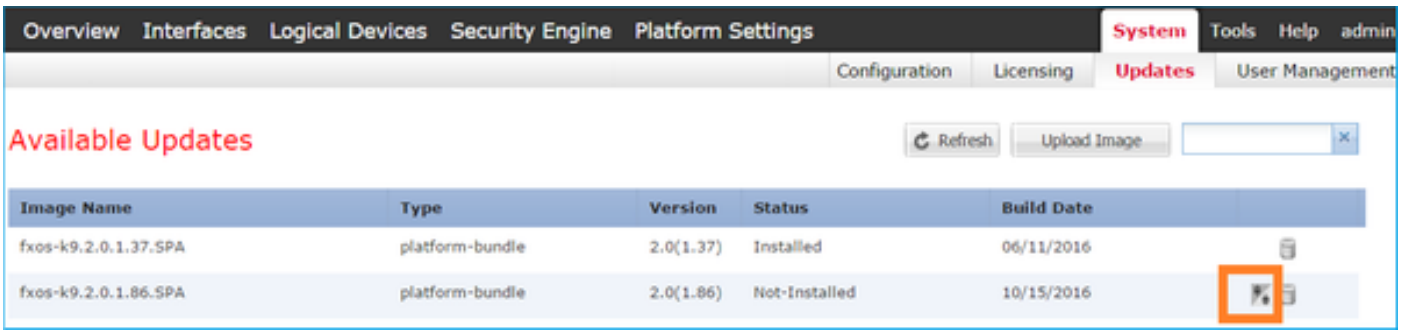
Шаг 3: Обновите вторичный FXOS

Перед обновлением:

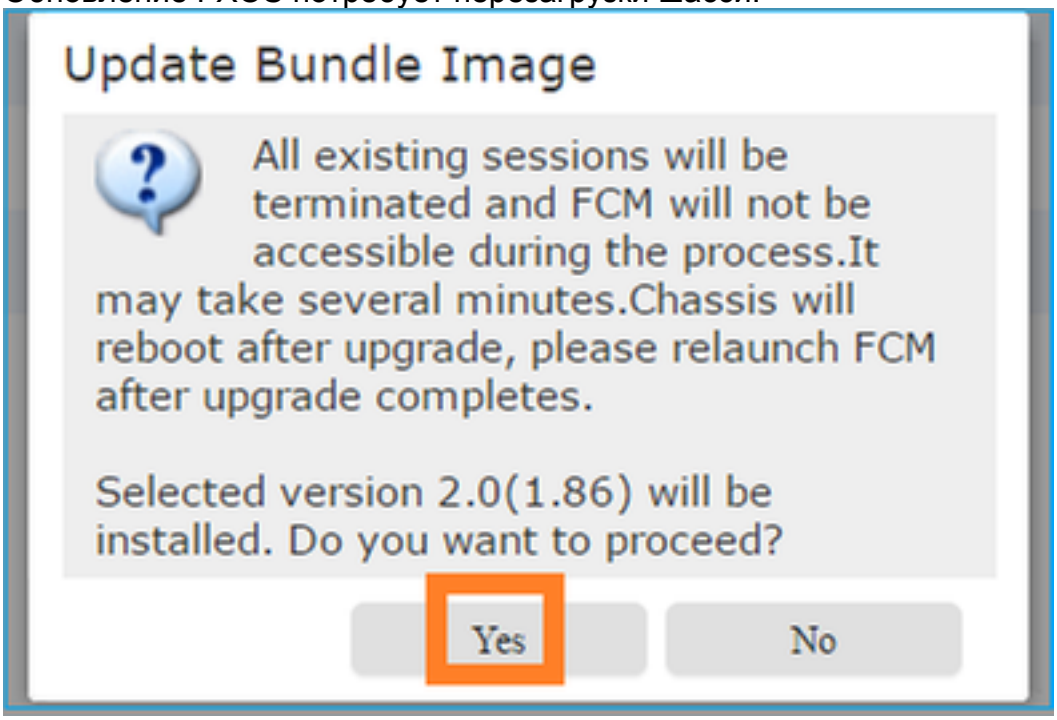
```
FPR4100-4-A /system # show firmware monitor FPRM: Package-Vers: 2.0(1.37) Upgrade-Status: Ready
Fabric Interconnect A: Package-Vers: 2.0(1.37) Upgrade-Status: Ready Chassis 1: Server 1:
```

```
Package-Vers: 2.0(1.37) Upgrade-Status: Ready
```

Запустите обновление FXOS:



Обновление FXOS потребует перезагрузки шасси:



Можно контролировать обновление FXOS от CLI FXOS. Должны быть обновлены все 3 компонента (FPRM, Центральное устройство и Шасси):

```
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
```

Обратите внимание – Спустя несколько минут после начала процесса обновления FXOS, вы могли бы быть разъединены и от CLI FXOS и от GUI. Должна существовать возможность входить снова после нескольких секунд.

После ~5 min обновление компонента FPRM завершает:

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**

После ~10 min и как часть процесса обновления FXOS Вторичные перезапуски устройства Огневой мощи:

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

После перезапуска резюме процесса обновления:

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**

После общего количества ~30 min обновление FXOS завершает:

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**

Шаг 4. : Подкачайте состояния аварийного переключения FTD

Прежде, чем подкачать состояния failver удостоверяются, что модуль FTD на Вторичном шасси подключен полностью 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 **...**

Подкачайте состояния аварийного переключения FTD. От Активного CLI FTD:

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

Обратите внимание - На этом этапе у вас мог бы быть ~1 пакет отброшенного транзитного трафика FTD

Шаг 5. : Обновите Основное устройство FXOS

Подобный Шагу 2 обновляют устройство FXOS, где Основной FTD установлен - Этот шаг может занять ~30 минут или больше завершить.

Шаг 6: Обновите программное обеспечение FMC

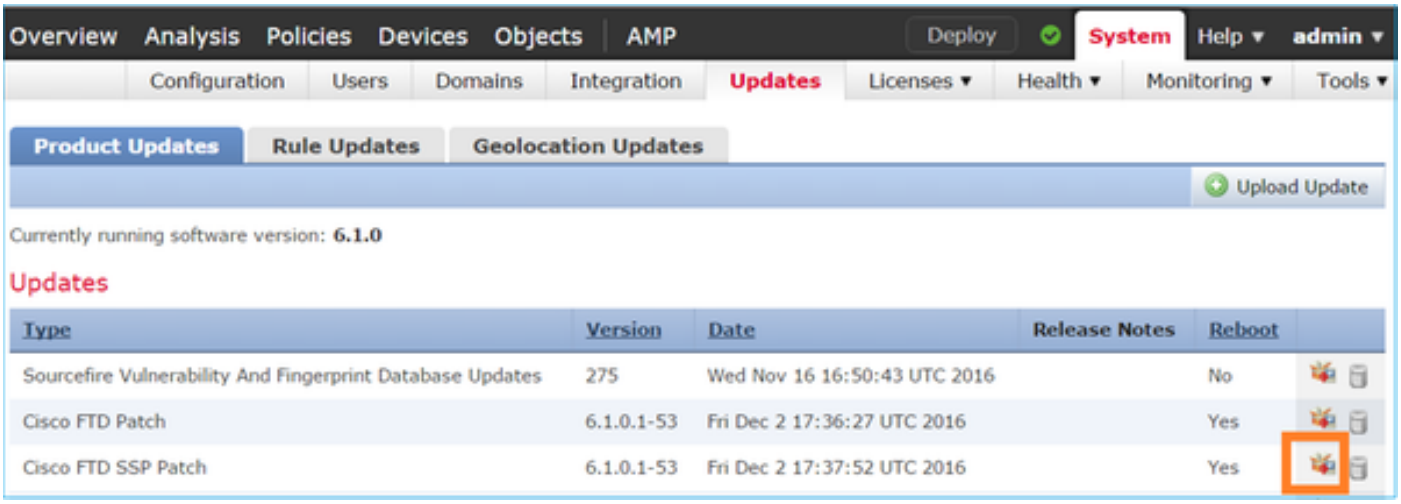
Обновите FMC в этом сценарии от 6.1.0-330 до 6.1.0.1.

Шаг 7: Обновите FTD HA пара

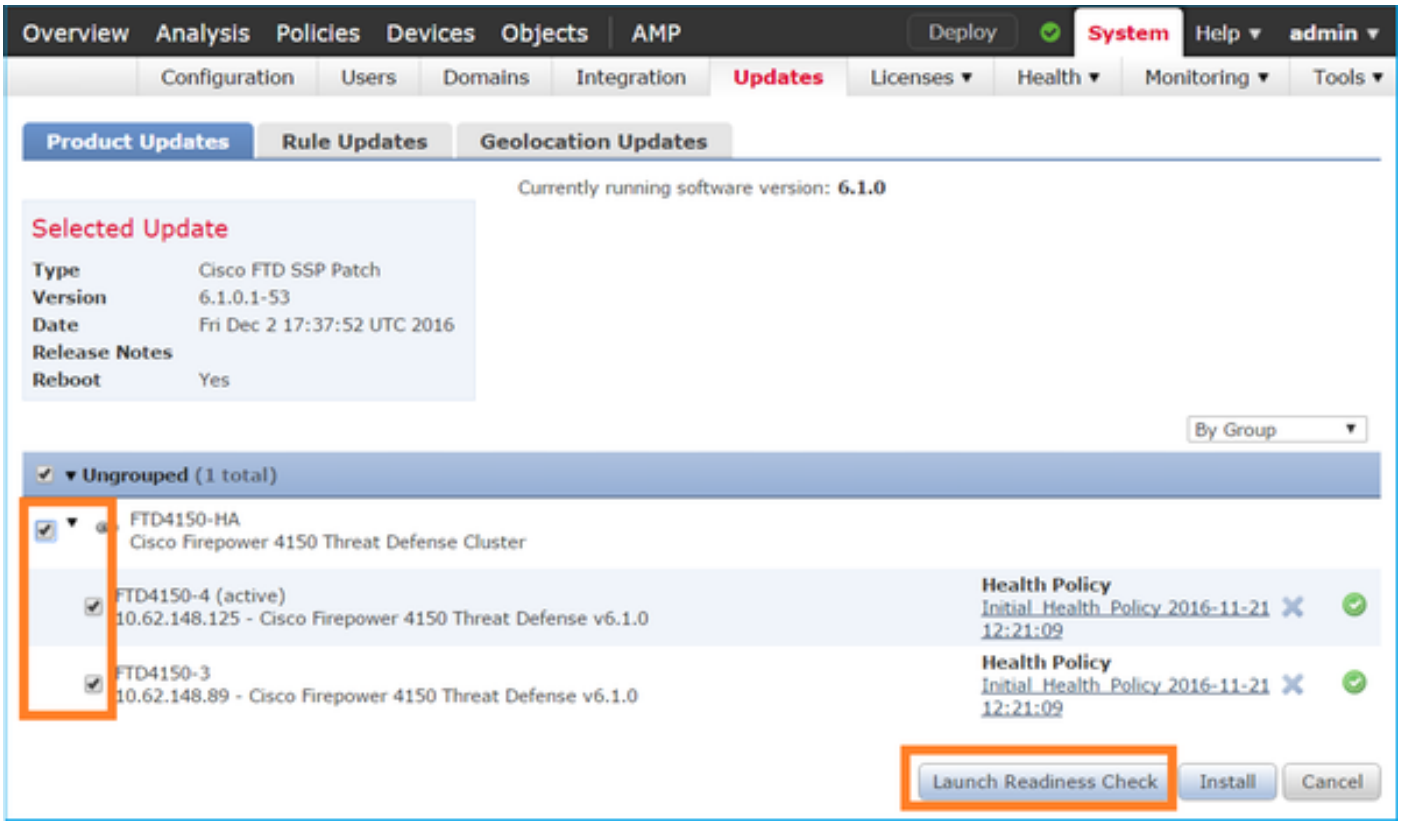
Перед обновлением:

```
> 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
...
```

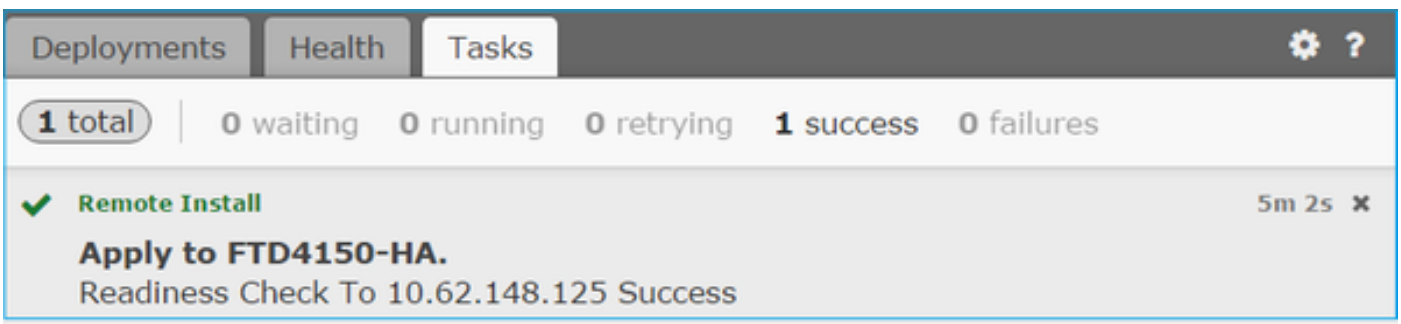
От **FMC System> Updates** меню инициируют FTD HA процесс обновления:



Дополнительно можно запустить Проверку Готовности обновления FTD, которая включает проверку целостности БД FTD:

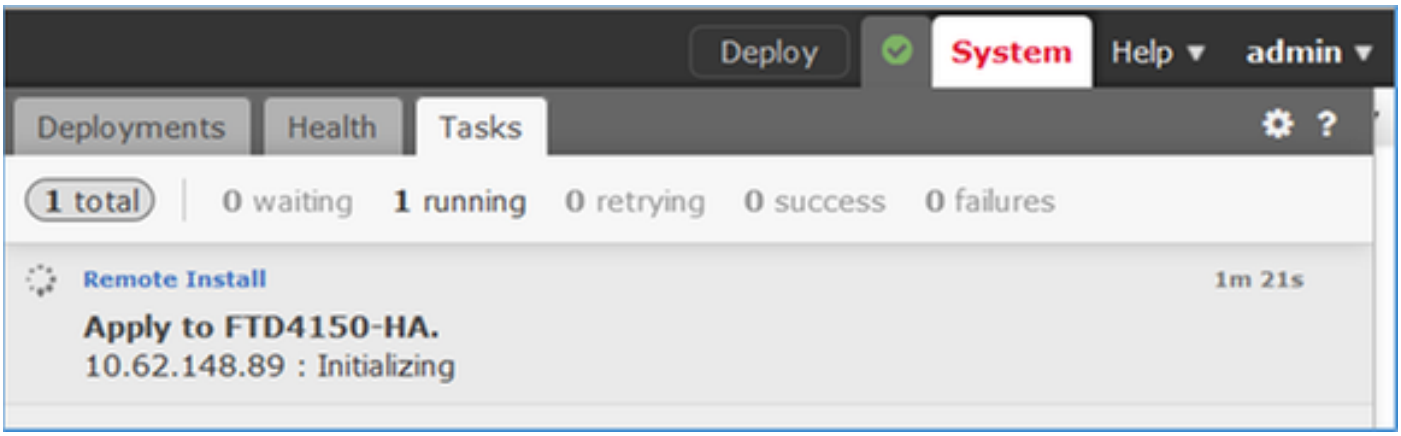


Проверка заняла ~5 min и была успешна:

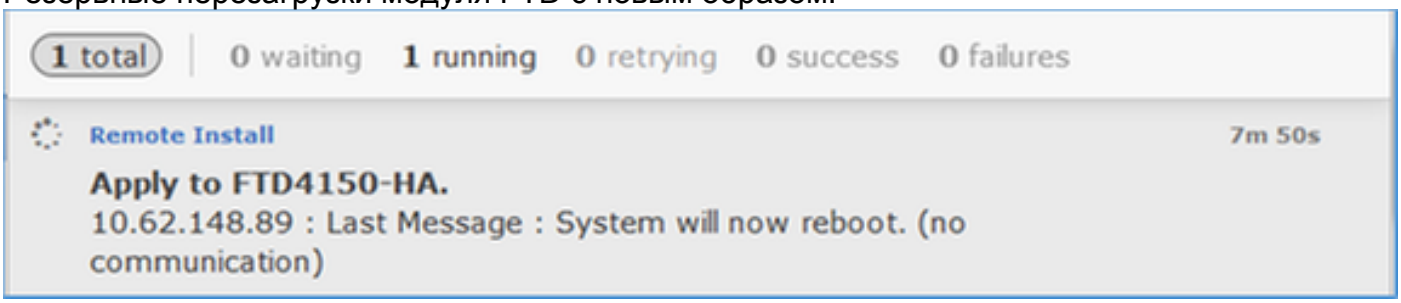


Инициируйте процесс установки:

Сначала Основной/Резервный FTD обновлен:



Резервные перезагрузки модуля FTD с новым образом:



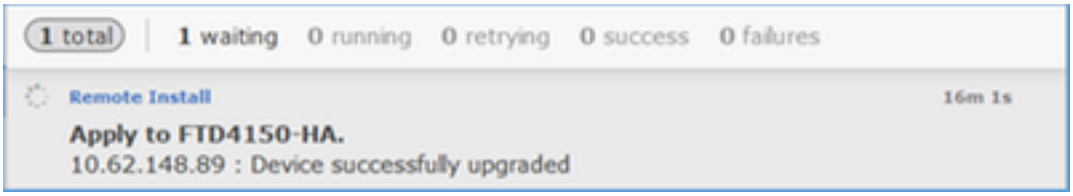
Можно проверить статус FTD от режима FXOS BootCLI:

```
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
```

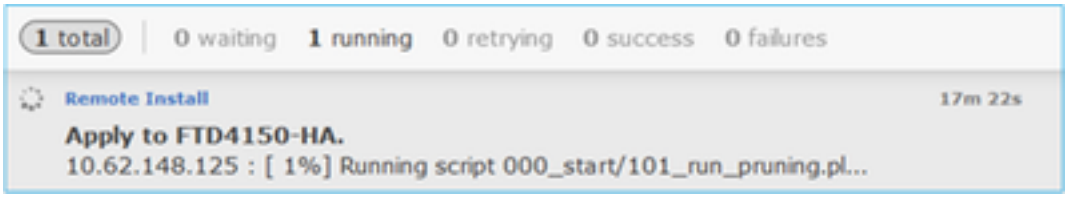
Вторичный/Активный CLI FTD показывает предупреждающее сообщение из-за несоответствия версии программного обеспечения между модулями FTD:

```
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
```

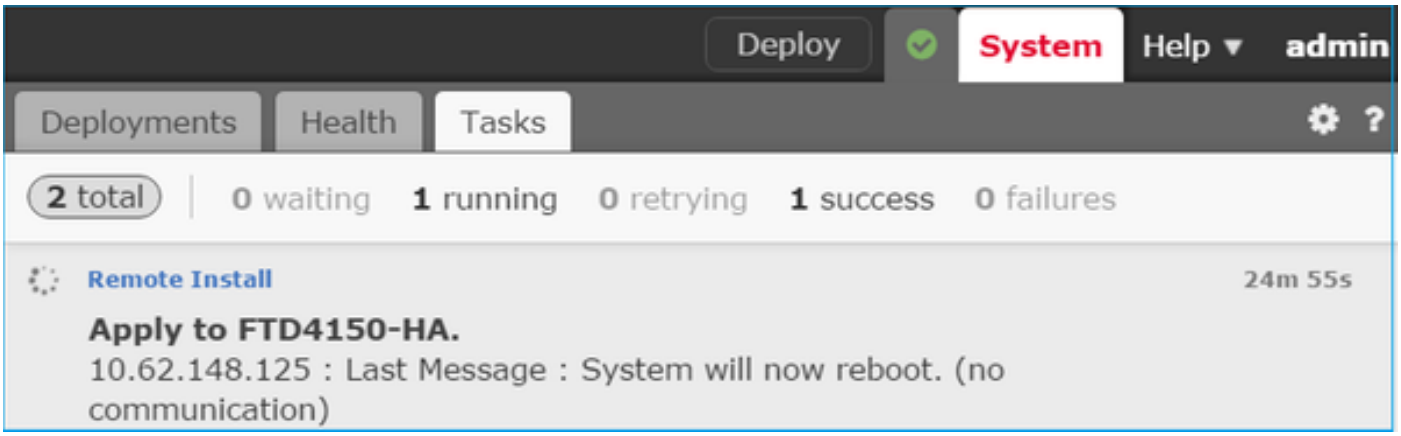
FMC показывает, что было успешно обновлено устройство FTD:



Обновление второго модуля FTD запускается:



В конце процесса Вторичный FTD загружается с новым образом:



В общих сведениях FMC, с помощью внутреннего пользователя ‘enable_1’, подкачивает состояния аварийного переключения FTD и временно удаляет конфигурацию аварийного переключения из Вторичного 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#

Обратите внимание - На этом этапе вы могли бы видеть ~1 отбрасывание пакета из-за свопинга состояния аварийного переключения

В этом случае целое обновление FTD (оба модуля) заняло ~30 минут:

Проверка

Проверка CLI FTD от Основного устройства FTD:

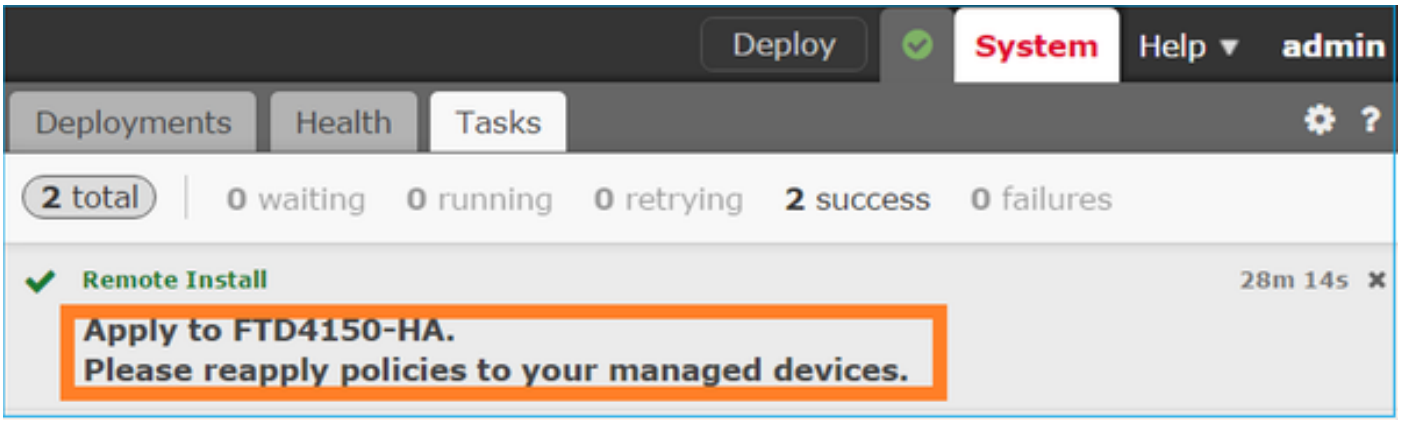
> **show high-availability config** Failover On Failover unit Primary Failover LAN Interface: FOVER Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 1041 maximum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

От Вторичного устройства FTD:

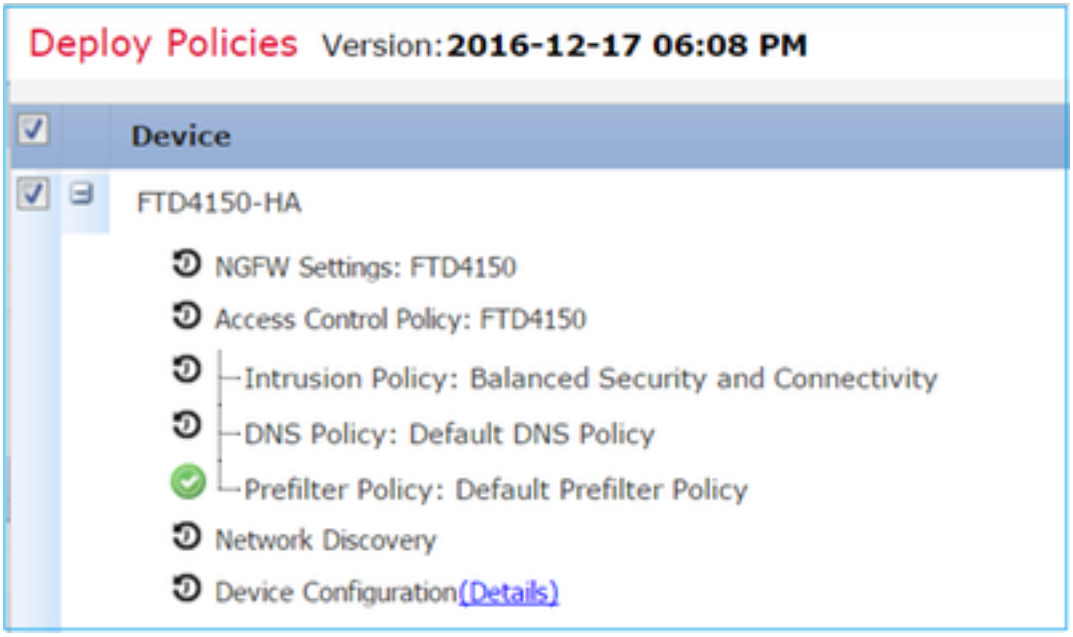
> **show high-availability config** Failover On **Failover unit Secondary** Failover LAN Interface: FOVER Ethernet1/8 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of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

Шаг 8: Разверните политику на FTD HA пара

После того, как обновление завершено существует потребность развернуть политику на паре HA. Это показывают в UI FMC:

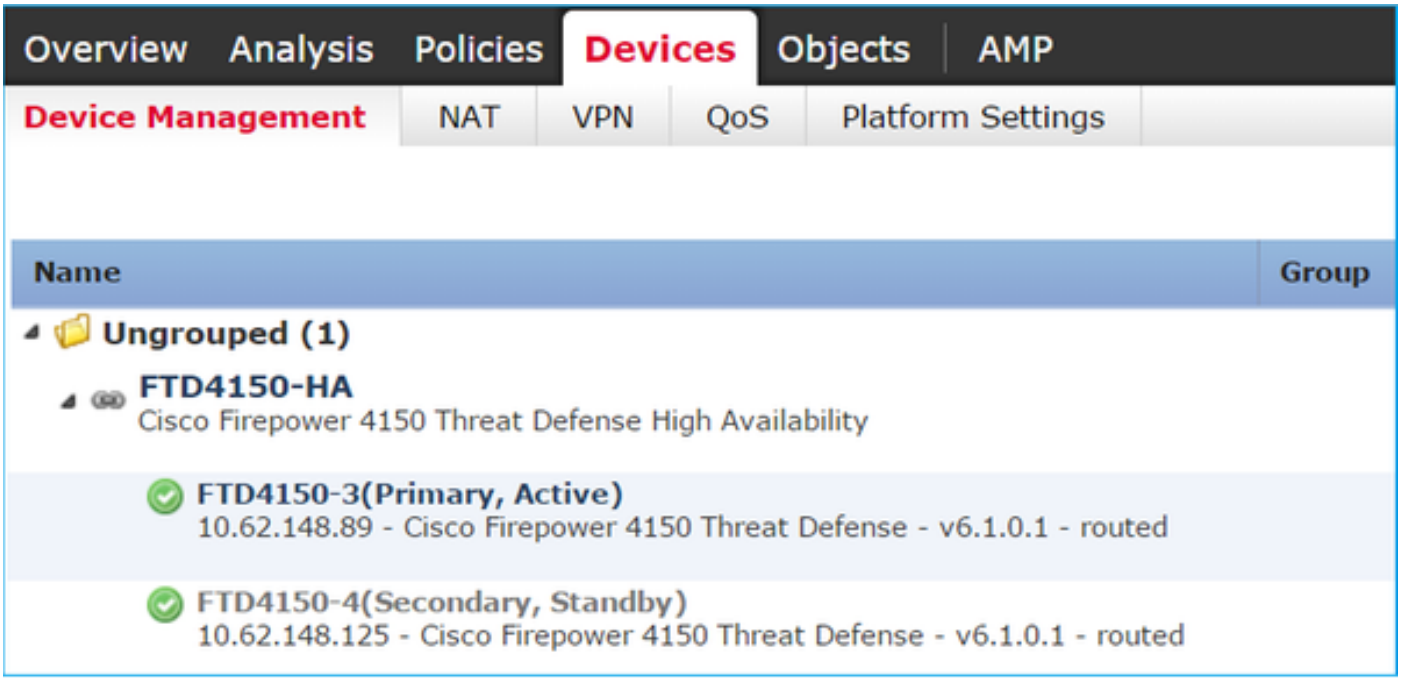


Разверните политику:

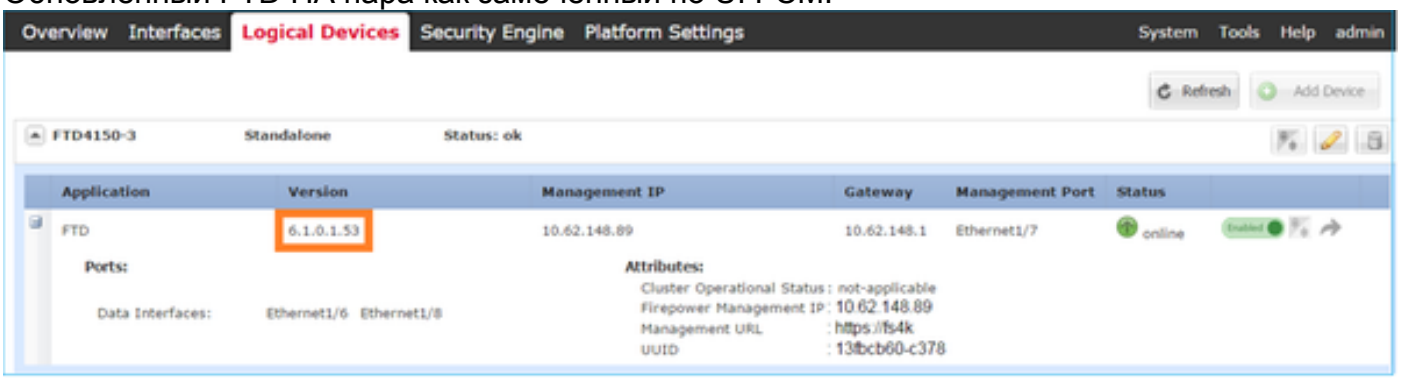


Проверка

Обновленный FTD HA пара как замеченный по UI FMC:



Обновленный FTD HA пара как замеченный по UI FCM:



Дополнительная документация

[Огневая мощь Cisco NGFW]