

FTD HA のアップグレード手順 Firepower アプライアンスで組み合わせて下さい

目次

[概要](#)

[目的](#)

[ラボ コンポーネント](#)

[トポロジ](#)

[FTD HA アップグレード プロセス](#)

[ステップ 1: 前提条件をチェックして下さい](#)

[ステップ 2: イメージをアップロードして下さい](#)

[ステップ 3: セカンダリ FXOS をアップグレードして下さい](#)

[ステップ 4: FTD フェールオーバー状態を交換して下さい](#)

[ステップ 5: プライマリ FXOS アプライアンスをアップグレードして下さい](#)

[ステップ 6: FMC ソフトウェアをアップグレードして下さい](#)

[ステップ 7: FTD HA ペアをアップグレードして下さい](#)

[ステップ 8: FTD HA ペアにポリシーを展開して下さい](#)

[関連資料](#)

概要

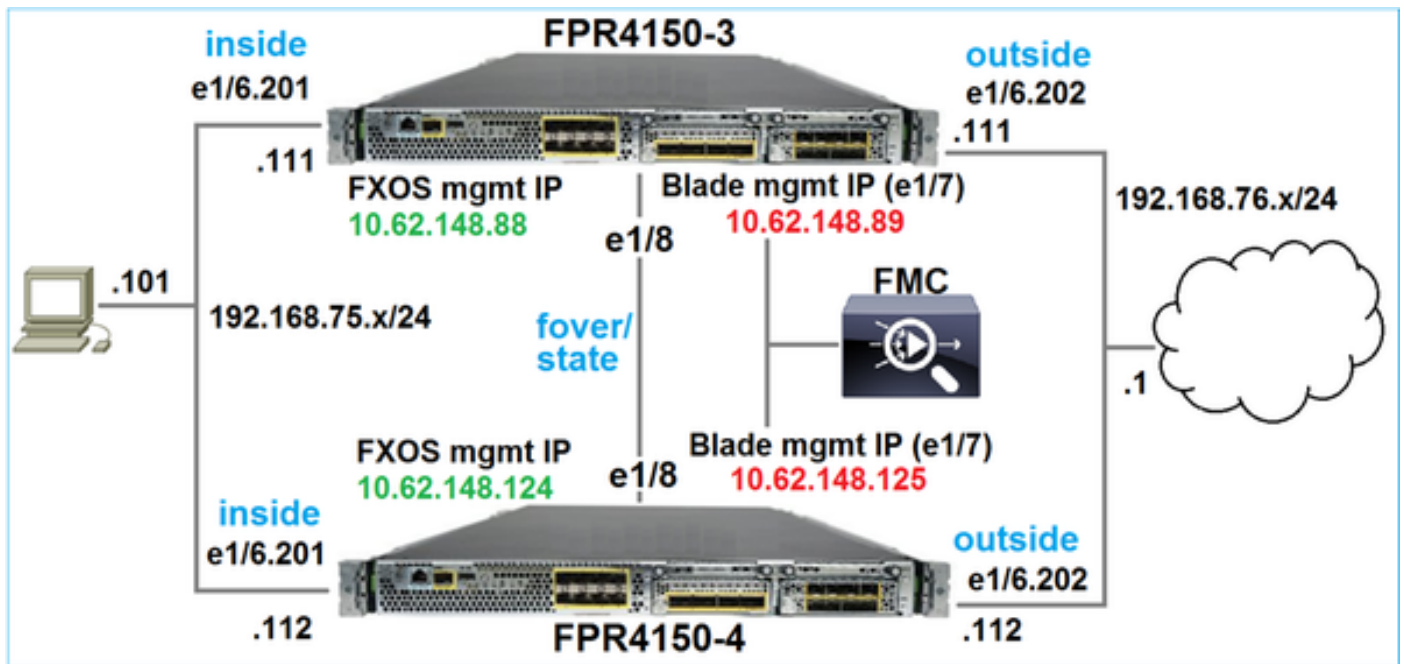
目標

この資料の目標は Firepower アプライアンスの高可用性のモードの Firepower Threat Defense (FTD) のアップグレード プロセスを示すことです。

ラボ コンポーネント

- 2 x FP4150
- 1 つの x FS4000
- 1 PC

トポロジ



アクティビティを開始する前のソフトウェア イメージバージョン:

- Firepower Management Center (FMC) 6.1.0-330
- FTD プライマリ 6.1.0-330
- FTD セカンダリ 6.1.0-330
- FXOS プライマリ 2.0.1-37
- FXOS セカンダリ 2.0.1-37

アクションプラン

ステップ 1: 前提条件をチェックして下さい

ステップ 2: FMC および SSP にイメージをアップロードして下さい

手順 3: セカンダリ FXOS 2.0.1-37 を -> 2.0.1-86 アップグレードして下さい

ステップ 4: 交換して下さい FTD フェールオーバー (プライマリ/スタンバイ、セカンダリ/アクティブがあります) を

ステップ 5: プライマリ FXOS 2.0.1-37 を -> 2.0.1-86 アップグレードして下さい

ステップ 6: FMC 6.1.0-330 を -> 6.1.0.1 アップグレードして下さい

ステップ 7: FTD HA ペア 6.1.0-330 を -> 6.1.0.1 アップグレードして下さい

ステップ 8: FMC から FTD HA ペアにポリシーを展開して下さい

FTD HA アップグレード プロセス

ステップ 1： 前提条件をチェックして下さい

互換性をその間判別するために FXOS 互換性 ガイドを参照して下さい:

- FTD ソフトウェア バージョンおよび FXOS ソフトウェア バージョンを目標として下さい
- Firepower HW プラットフォームおよび FXOS ソフトウェア バージョン

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

FXOS アップグレード パスを判別するためにターゲットバージョンの FXOS リリース ノートをチェックして下さい:

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

FTD アップグレード パスを判別するために FTD ターゲットバージョン リリース ノートを参照して下さい:

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

ステップ 2： イメージをアップロードして下さい

2 で FCMs はアップロードします FXOS イメージ (fxos-k9.2.0.1.86.SPA) を

FMC アップロード FMC および FTD アップグレード パッケージ:

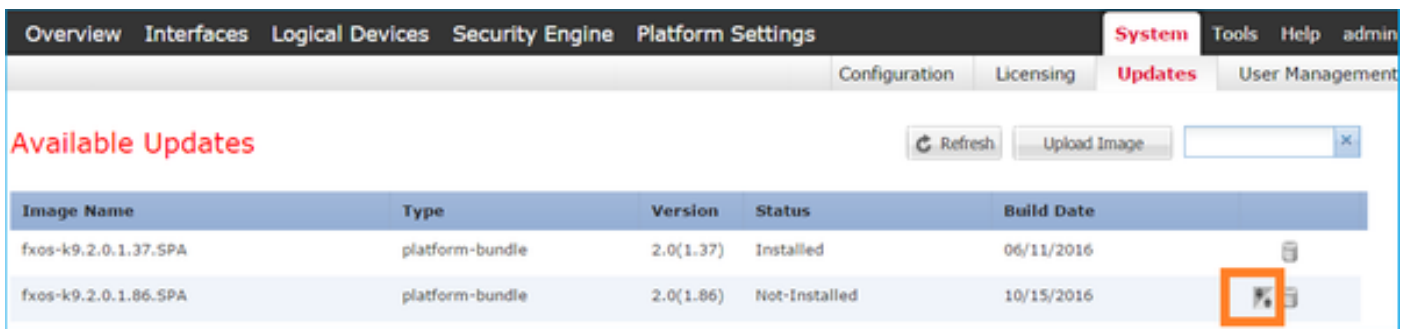
- FMC アップグレードに関しては: Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- FTD アップグレードに関しては: Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

ステップ 3： セカンダリ FXOS をアップグレードして下さい

アップグレードの前:

```
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
```

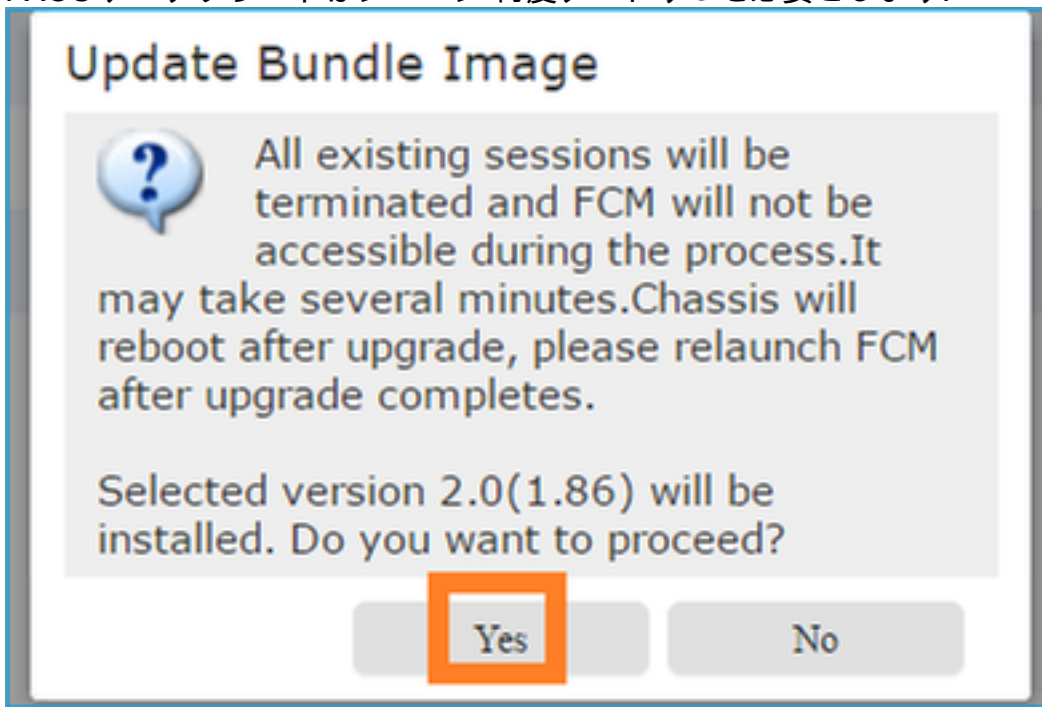
FXOS アップグレードを開始して下さい:



Available Updates

Image Name	Type	Version	Status	Build Date
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Installed	06/11/2016
fxos-k9.2.0.1.86.SPA	platform-bundle	2.0(1.86)	Not-Installed	10/15/2016

FXOS アップグレードはシャーシ 再度ブートするを必要とします:



Update Bundle Image

All existing sessions will be terminated and FCM will not be accessible during the process. It may take several minutes. Chassis will reboot after upgrade, please relaunch FCM after upgrade completes.

Selected version 2.0(1.86) will be installed. Do you want to proceed?

Yes No

FXOS CLI からの FXOS アップグレードを監視できます。3つのコンポーネントすべて (FPRM、ファブリック相互接続およびシャーシ) はアップグレードされなければなりません:

```
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- FXOS アップグレード プロセスを開始した後数分 FXOS CLI および GUI 両方から切断されるかもしれません。数秒後に再度ログインできるはずで。

~5 最小値以降に FPRM コンポーネント アップグレードは完了します:

```
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
```

として ~10 最小値以降におよび FXOS アップグレード プロセスの一部セカンダリ Firepower デバイスは再起動します:

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

再始動の後アップグレード プロセス再開:

```
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
```

合計 ~30 最小値の後で FXOS アップグレードは完了します:

```
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
```

ステップ 4 : FTD フェールオーバー状態を交換して下さい

failver 状態を交換する前にセカンダリ シャーシの FTD モジュールが十分にアップすることを確かめて下さい:

```
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 フェールオーバー状態を交換して下さい。 アクティブ FTD CLI から:

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

注-この時点で FTD トランジットトラフィックの ~1 パケットを廃棄してもらうかもしれません

ステップ 5：プライマリ FXOS アプライアンスをアップグレードして下さい

ステップ 2 アップグレードに類似したプライマリ FTD がインストールされている FXOS アプライアンスは完了するために-このステップ ~30 分または多くを奪取できます。

ステップ 6：FMC ソフトウェアをアップグレードして下さい

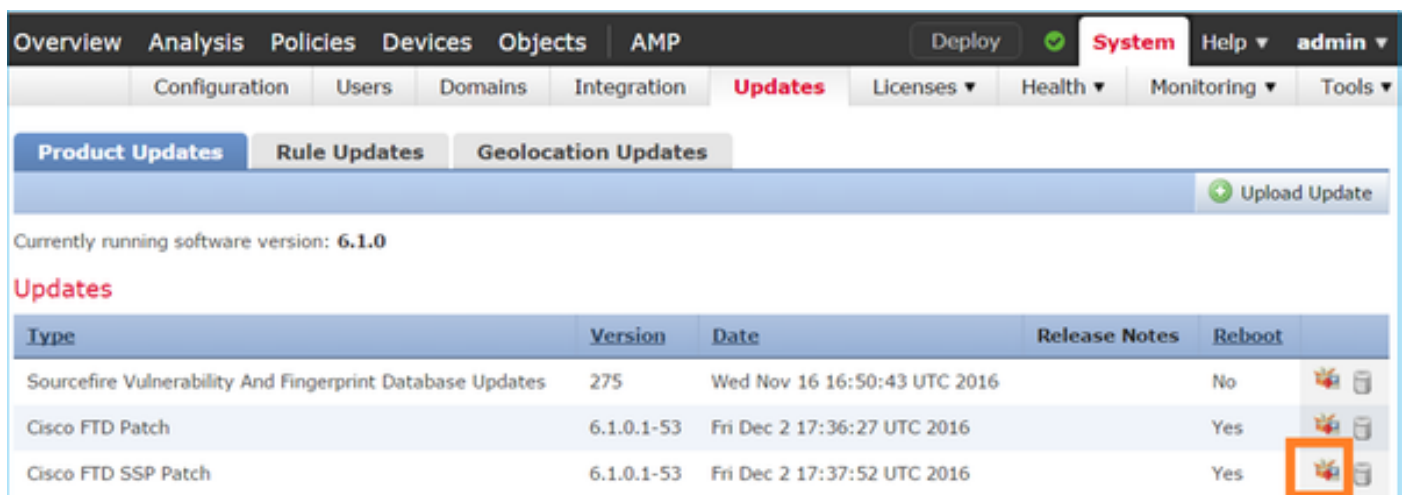
6.1.0-330 から 6.1.0.1 にこのシナリオの FMC を、アップグレードして下さい。

ステップ 7：FTD HA ペアをアップグレードして下さい

アップグレードの前:

```
> 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
...
```

FMC システム > Updates メニューから FTD HA アップグレード プロセスを開始して下さい:



Overview Analysis Policies Devices Objects AMP Deploy System Help admin

Configuration Users Domains Integration Updates Licenses Health Monitoring Tools

Product Updates Rule Updates Geolocation Updates Upload Update

Currently running software version: 6.1.0

Updates

Type	Version	Date	Release Notes	Reboot
Sourcefire Vulnerability And Fingerprint Database Updates	275	Wed Nov 16 16:50:43 UTC 2016		No
Cisco FTD Patch	6.1.0.1-53	Fri Dec 2 17:36:27 UTC 2016		Yes
Cisco FTD SSP Patch	6.1.0.1-53	Fri Dec 2 17:37:52 UTC 2016		Yes

任意で FTD DB 健全性チェックが含まれている FTD アップグレード準備チェックを起動できません:

The screenshot shows the Cisco FTD management console interface. At the top, there are navigation tabs: Overview, Analysis, Policies, Devices, Objects, AMP, Deploy, System, Help, and admin. Below these are sub-tabs: Configuration, Users, Domains, Integration, Updates, Licenses, Health, Monitoring, and Tools. The 'Updates' section is active, showing 'Product Updates', 'Rule Updates', and 'Geolocation Updates'. The current software version is 6.1.0. A 'Selected Update' box displays details for a Cisco FTD SSP Patch (version 6.1.0.1-53, released on Dec 2, 2016, requiring a reboot). Below this, a list of devices is shown under 'Ungrouped (1 total)'. The devices are FTD4150-HA (Cisco Firepower 4150 Threat Defense Cluster), FTD4150-4 (active) at 10.62.148.125, and FTD4150-3 at 10.62.148.89. Each device has a 'Health Policy' status of 'Initial Health Policy 2016-11-21 12:21:09' with a green checkmark. At the bottom right, there is a 'Launch Readiness Check' button, an 'Install' button, and a 'Cancel' button.

チェックは ~5 最小値を奪取し、正常でした:

The screenshot shows the 'Tasks' section of the Cisco FTD management console. The top navigation bar includes 'Deployments', 'Health', and 'Tasks'. Below the navigation bar, there is a summary of tasks: '1 total', '0 waiting', '0 running', '0 retrying', '1 success', and '0 failures'. A task titled 'Remote Install' is shown with a green checkmark and a duration of '5m 2s'. The task description is 'Apply to FTD4150-HA. Readiness Check To 10.62.148.125 Success'.

インストールプロセスを開始して下さい:

最初にプライマリ/スタンバイ FTD はアップグレードされます:

スタンバイ FTD モジュールは新しいイメージとリブートします:

FXOS BootCLI モードからの FTD ステータスを確認できます:

```

FPR4100-3-A# connect module 1 console Firepower-module1> show services status
Services currently
running: Feature | Instance ID | State | Up Since -----
----- ftd | 001_JAD201200R4WLYCW06 | RUNNING | :00:00:33

```

セカンダリ/アクティブ FTD CLI は FTD モジュール間のソフトウェア バージョン ミスマッチによる警告メッセージを表示します:

```

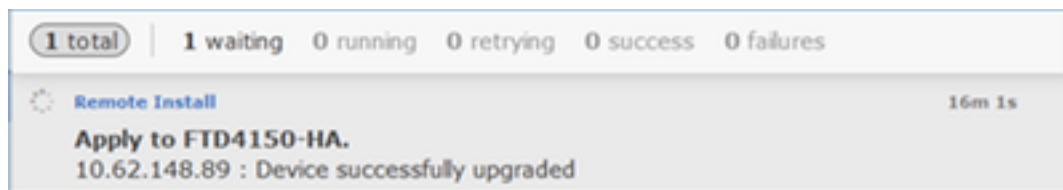
firepower#
*****WARNING*****WARNING*****WARNING*****

```

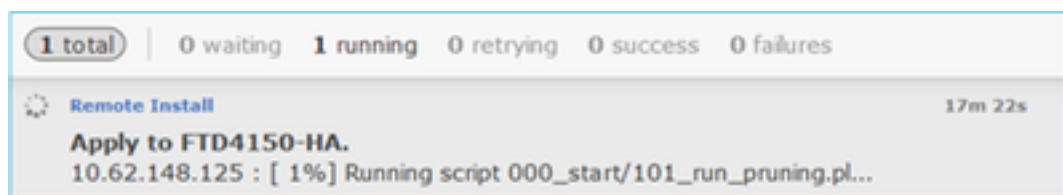

Mate version 9.6(2) is not identical with ours 9.6(2)4

*****WARNING*****WARNING*****WARNING***** Beginning configuration replication: Sending to mate. End Configuration Replication to mate

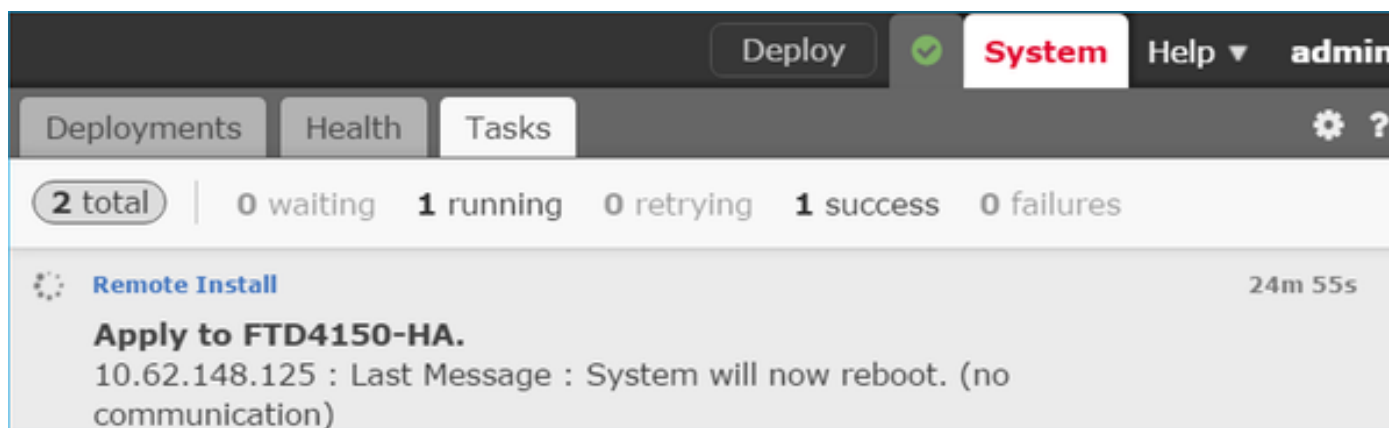
FMC は FTD デバイスがアップグレードに成功したことを示します:



第 2 FTD モジュールのアップグレードは開始します:



プロセスの終わりにセカンダリは新しいイメージと FTD 起動します:



バックグラウンドで内部ユーザ「enable_1」を使用して FMC は、FTD フェールオーバー状態を交換し、セカンダリ FTD から一時的にフェールオーバー 設定を取除きます:

```
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-この時点でフェールオーバー状態スワップによる ~1 パケット破棄を参照するかもしれません

この場合全 FTD アップグレード (両方のユニット) は ~30 分かかりました:

確認

プライマリ FTD デバイスからの FTD CLI 確認:

```
> 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 ... >
```

セカンダリ FTD デバイスから:

```
> 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
... >
```

ステップ 8 : FTD HA ペアにポリシーを展開して下さい

アップグレードが完了した後 HA ペアにポリシーを展開する必要があります。これは FMC UI で

示されています:

The screenshot shows the FMC System page. At the top, there is a 'Deploy' button with a green checkmark, a 'System' tab, and a 'Help' dropdown menu. Below this, there are tabs for 'Deployments', 'Health', and 'Tasks'. The 'Tasks' tab is active, showing a summary of 2 total tasks: 0 waiting, 0 running, 0 retrying, 2 success, and 0 failures. A specific task, 'Remote Install', is highlighted with a green checkmark and a duration of 28m 14s. The task details are displayed in a box with an orange border, stating: 'Apply to FTD4150-HA. Please reapply policies to your managed devices.'

ポリシーを展開して下さい:

The screenshot shows the 'Deploy Policies' page for device FTD4150-HA. The page title is 'Deploy Policies Version: 2016-12-17 06:08 PM'. The device is selected, and a list of policies is shown with expandable icons (circles with a right-pointing arrow). The policies are: NGFW Settings: FTD4150, Access Control Policy: FTD4150, Intrusion Policy: Balanced Security and Connectivity, DNS Policy: Default DNS Policy, Prefilter Policy: Default Prefilter Policy (which has a green checkmark next to it), Network Discovery, and Device Configuration (Details).

確認

FMC UI から見られるそれとしてアップグレードされた FTD HA ペア:

Overview Analysis Policies **Devices** Objects AMP

Device Management NAT VPN QoS Platform Settings

Name	Group
<ul style="list-style-type: none"> Ungrouped (1) <ul style="list-style-type: none"> FTD4150-HA <ul style="list-style-type: none"> Cisco Firepower 4150 Threat Defense High Availability <ul style="list-style-type: none"> FTD4150-3(Primary, Active) <ul style="list-style-type: none"> 10.62.148.89 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed FTD4150-4(Secondary, Standby) <ul style="list-style-type: none"> 10.62.148.125 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed 	

FCM UI から見られるそれとしてアップグレードされた FTD HA ペア:

Overview Interfaces **Logical Devices** Security Engine Platform Settings System Tools Help admin

Refresh Add Device

FTD4150-3 Standalone Status: ok

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.1.0.1.53	10.62.148.89	10.62.148.1	Ethernet1/7	online

Ports:

Data Interfaces: Ethernet1/6 Ethernet1/8

Attributes:

Cluster Operational Status: not-applicable
 Firepower Management IP: 10.62.148.89
 Management URL : https://fs4k
 UUID : 13fcb60-c378

関連資料

[Cisco Firepower NGFW](#)