

firepowerアプライアンスでのFTD HAペアのアップグレード

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[タスク 1.前提条件の確認](#)

[タスク 2.ソフトウェアイメージのアップロード](#)

[タスク 3.最初のFXOSシャーシのアップグレード](#)

[タスク 4. FTD フェールオーバーの状態のスワップ](#)

[タスク 5.2つ目のFXOSシャーシのアップグレード](#)

[タスク 6.FMC ソフトウェアのアップグレード](#)

[タスク 7.FTD HA ペアのアップグレード](#)

[タスク 8.FTD HA ペアへのポリシーの展開](#)

[関連情報](#)

はじめに

このドキュメントでは、Firepowerアプライアンスのハイアベイラビリティ(HA)モードでのFirepower Threat Defense(FTD)のアップグレードプロセスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Firepower Management Center (FMC)
- FTD
- Firepowerアプライアンス(FXOS)

使用するコンポーネント

- FPR4150 X 2
- 1 X FS4000
- PC X 1

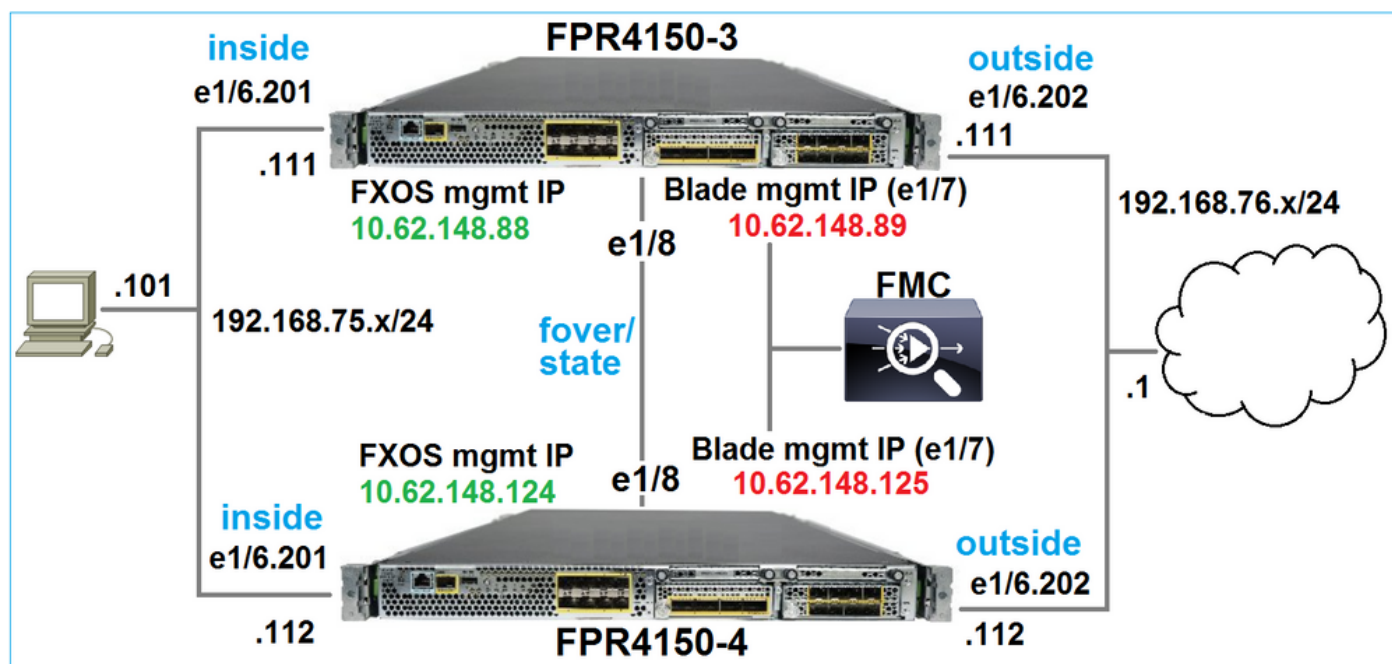
アップグレード前のソフトウェアイメージのバージョン

- 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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していません。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



アクションプラン

作業1：前提条件の確認

タスク2:FMCおよびSSPへのイメージのアップロード

タスク3：最初のFXOSシャーシのアップグレード(2.0.1-37 -> 2.0.1-86)

タスク4:FTDフェールオーバーの切り替え

タスク5:2番目のFXOSシャーシのアップグレード(2.0.1-37 -> 2.0.1-86)

タスク6:FMCのアップグレード(6.1.0-330 -> 6.1.0.1)

タスク7:FTD HAペアのアップグレード(6.1.0-330 -> 6.1.0.1)


タスク8:FMCからFTD HAペアへのポリシーの導入

タスク 1.前提条件の確認

次の間の互換性を確認するには、『FXOS Compatibility Guide』を参照してください。


- ターゲット FTD ソフトウェア バージョンと FXOS ソフトウェア バージョン
- Firepower HW プラットフォームと FXOS ソフトウェア バージョン

[CiscoFirepower4100/9300 FXOSの互換性](#)

 注：この手順は、FP21xx以前のプラットフォームには適用されません。

FXOSのアップグレードパスを確認するには、ターゲットバージョンのFXOSリリースノートを確認します。

[CiscoFirepower4100/9300 FXOSリリースノート、2.0\(1\)](#)

 注：この手順は、FP21xx以前のプラットフォームには適用されません。

FTDのアップグレードパスを確認するには、FTDターゲットバージョンのリリースノートを参照してください。

[Firepower システム リリース ノート、バージョン 6.0.1.2](#)


タスク 2.ソフトウェアイメージのアップロード


2つのFCMで、FXOSイメージ(fxos-k9.2.0.1.86.SPA)をアップロードします。

FMCで、FMCとFTDのアップグレードパッケージをアップロードします。

- FMCのアップグレード：Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- FTDのアップグレード：Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

タスク 3.最初のFXOSシャーシのアップグレード

 注:FXOSを1.1.4.xから2.xにアップグレードする場合は、最初にFTD論理アプライアンスをシャットダウンし、FXOSをアップグレードしてから再度有効にします。

 注：この手順は、FP21xx以前のプラットフォームには適用されません。

アップグレード前：

<#root>

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

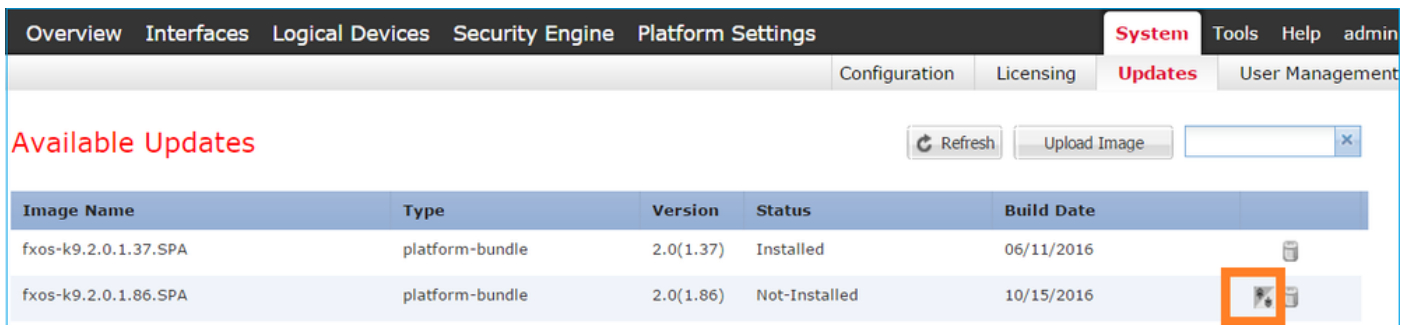
Chassis 1:

Server 1:

Package-Vers: 2.0(1.37)

Upgrade-Status: Ready

FXOS アップグレードを開始します。



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のアップグレードには、シャーシのリブートが必要です。

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 FXOS アップグレードをモニタできます。3つのコンポーネント (FPRM、ファブリックインターコネクト、およびシャーシ) はすべてアップグレードする必要があります。

```
<#root>
```

```
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てから数分後に、FXOS CLIとGUIの両方から切断されます。数分後に再度ログインできます。

約5分後に、FPRMコンポーネントのアップグレードが完了します。

```
<#root>
```

```
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
```

約10分後に、FXOSアップグレードプロセスの一部として、Firepowerデバイスが再起動します。

```
<#root>
```

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

```
...
```

```
Restarting system.
```

再起動後にアップグレードプロセスが再開します。

```
<#root>
```

```
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
```

合計で約30分が経過すると、FXOSのアップグレードが完了します。

<#root>

```
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
```

タスク 4. FTD フェールオーバーの状態のスワップ

 注：この手順は、FP21xx以前のプラットフォームには適用されません。

フェールオーバーの状態を切り替える前に、シャーシのFTDモジュールが完全にUPになっていることを確認します。

```
<#root>
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 フェールオーバーの状態をスワップします。アクティブな FTD CLI から次のコマンドを入力します。

```

<#root>
>
no failover active


```

Switching to Standby

>

タスク 5.2つ目のFXOSシャーシのアップグレード

タスク2と同様に、新しいスタンバイFTDがインストールされているFXOSアプライアンスをアップグレードします。この処理には約30分以上かかります。

 注：この手順は、FP21xx以前のプラットフォームには適用されません。

タスク 6.FMC ソフトウェアのアップグレード

このシナリオでは、FMC を 6.1.0-330 から 6.1.0.1 にアップグレードします。

タスク 7.FTD HA ペアのアップグレード

アップグレード前：

```
<#root>
```

```
>
```

```
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

```

...

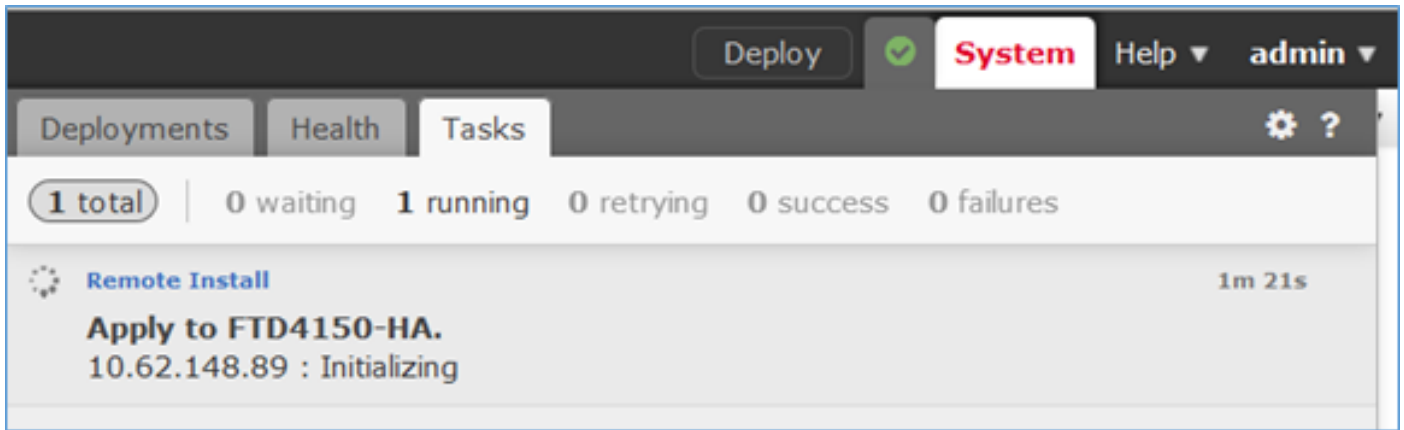
FMCのSystem > Updatesメニューから、FTD HAアップグレードプロセスを開始します。

The screenshot shows the Cisco FMC System > Updates menu. The top navigation bar includes Overview, Analysis, Policies, Devices, Objects, AMP, Deploy, System, Help, and admin. The main menu has Configuration, Users, Domains, Integration, Updates, Licenses, Health, Monitoring, and Tools. Under Updates, there are tabs for Product Updates, Rule Updates, and Geolocation Updates. A button for 'Upload Update' is visible. The current software version is 6.1.0. The Updates table lists three updates: Sourcefire Vulnerability And Fingerprint Database Updates, Cisco FTD Patch, and Cisco FTD SSP Patch. The Cisco FTD SSP Patch is highlighted with an orange box. Below the table, a list of devices is shown under 'Ungrouped (1 total)'. The list includes FTD4150-HA (Cisco Firepower 4150 Threat Defense Cluster) and two active FTD4150-4 and FTD4150-3 devices. Each device has a 'Health Policy' section with a link to 'Initial Health Policy 2016-11-21 12:21:09' and a green checkmark. At the bottom right, there are three buttons: 'Launch Readiness Check', 'Install' (highlighted with an orange box), and 'Cancel'.

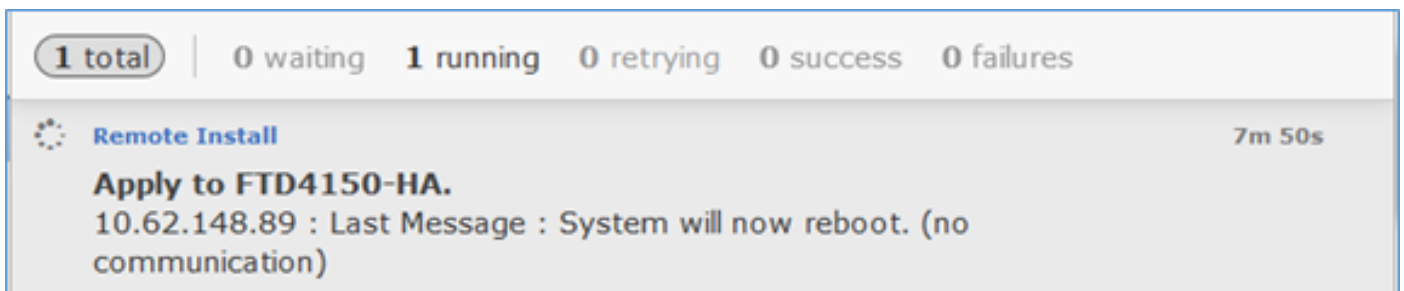
Type	Version	Date	Release Notes	Reboot
Sourcefire Vulnerability And Fingerprint Database Updates	275	Wed Nov 16 16:50:43 UTC 2016		No
Cisco FTD Patch	6.1.0.1-53	Fri Dec 2 17:36:27 UTC 2016		Yes
Cisco FTD SSP Patch	6.1.0.1-53	Fri Dec 2 17:37:52 UTC 2016		Yes

Device	Health Policy
FTD4150-4 (active) 10.62.148.125 - Cisco Firepower 4150 Threat Defense v6.1.0	Initial Health Policy 2016-11-21 12:21:09 X ✓
FTD4150-3 10.62.148.89 - Cisco Firepower 4150 Threat Defense v6.1.0	Initial Health Policy 2016-11-21 12:21:09 X ✓

まず、プライマリ/スタンバイFTDがアップグレードされます。



スタンバイ FTD モジュールが新しいイメージでリブートされます。



FXOS BootCLI モードから FTD のステータスを確認できます。

```
<#root>
```

```
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の不一致による警告メッセージを表示します。

```
<#root>
```

```
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 には、FTD デバイスが正常にアップグレードされたことが表示されます。

1 total		1 waiting	0 running	0 retrying	0 success	0 failures
Remote Install 16m 1s						
Apply to FTD4150-HA. 10.62.148.89 : Device successfully upgraded						

セカンダリ FTD モジュールのアップグレードが開始されます。

1 total		0 waiting	1 running	0 retrying	0 success	0 failures
Remote Install 17m 22s						
Apply to FTD4150-HA. 10.62.148.125 : [1%] Running script 000_start/101_run_pruning.pl...						

プロセスの最後に、FTDは新しいイメージでブートします。

Deploy		✔	System	Help ▾	admin	
Deployments	Health	Tasks	⚙️ ?			
2 total		0 waiting	1 running	0 retrying	1 success	0 failures
Remote Install 24m 55s						
Apply to FTD4150-HA. 10.62.148.125 : Last Message : System will now reboot. (no communication)						

バックグラウンドでは、FMCは内部ユーザenable_1を使用してFTDフェールオーバー状態をスワップし、FTDからフェールオーバー設定を一時的に削除します。

<#root>

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 failo

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 co
```

```
Dec 17 2016 16:41:19: %ASA-5-111008: User 'enable_1' executed the 'copy /noconfirm running-config disk0
```

```
Dec 17 2016 16:41:19: %ASA-5-111010: User 'enable_1', running 'N/A' from IP 0.0.0.0, executed 'copy /no
```

```
disk0:/modified-config.cfg'
```

```
firepower#
```

```
Switching to Standby
```

```
firepower#
```

この場合、FTDのアップグレード全体（両方のユニット）に約30分かかりました。

検証

次の例は、プライマリFTDデバイスからのFTD CLIの検証を示しています。

```
<#root>
```

```
>
```

```
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
```

```
...
>
```

次の例は、セカンダリ/スタンバイFTDデバイスからのFTD CLIの検証を示しています。

```
<#root>
```

```
>
```

```
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)
```

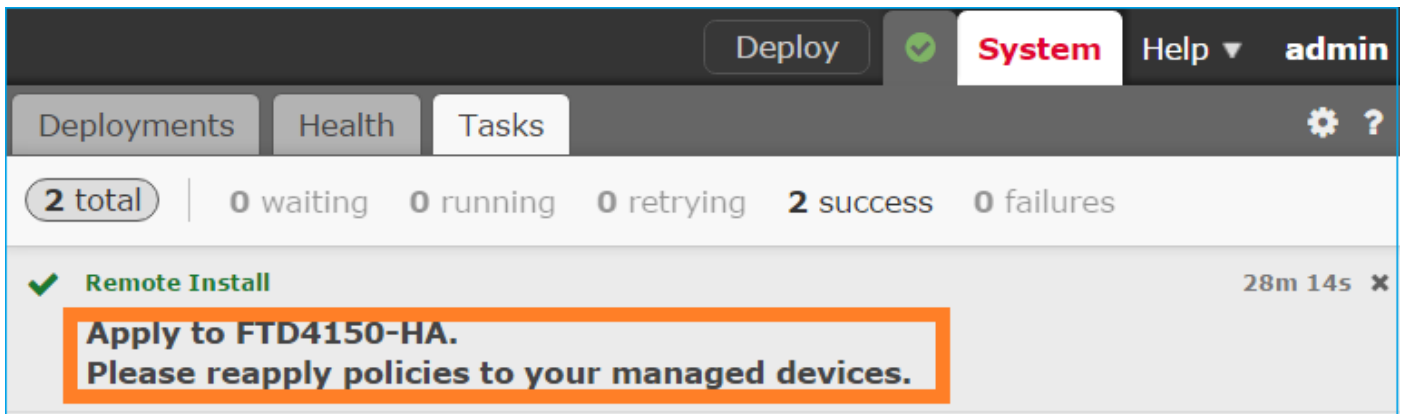
Stateful Failover Logical Update Statistics

```
Link : FOVER Ethernet1/8 (up)
Stateful Obj  xmit      xerr      rcv      rerr
General      38          0         41       0
```

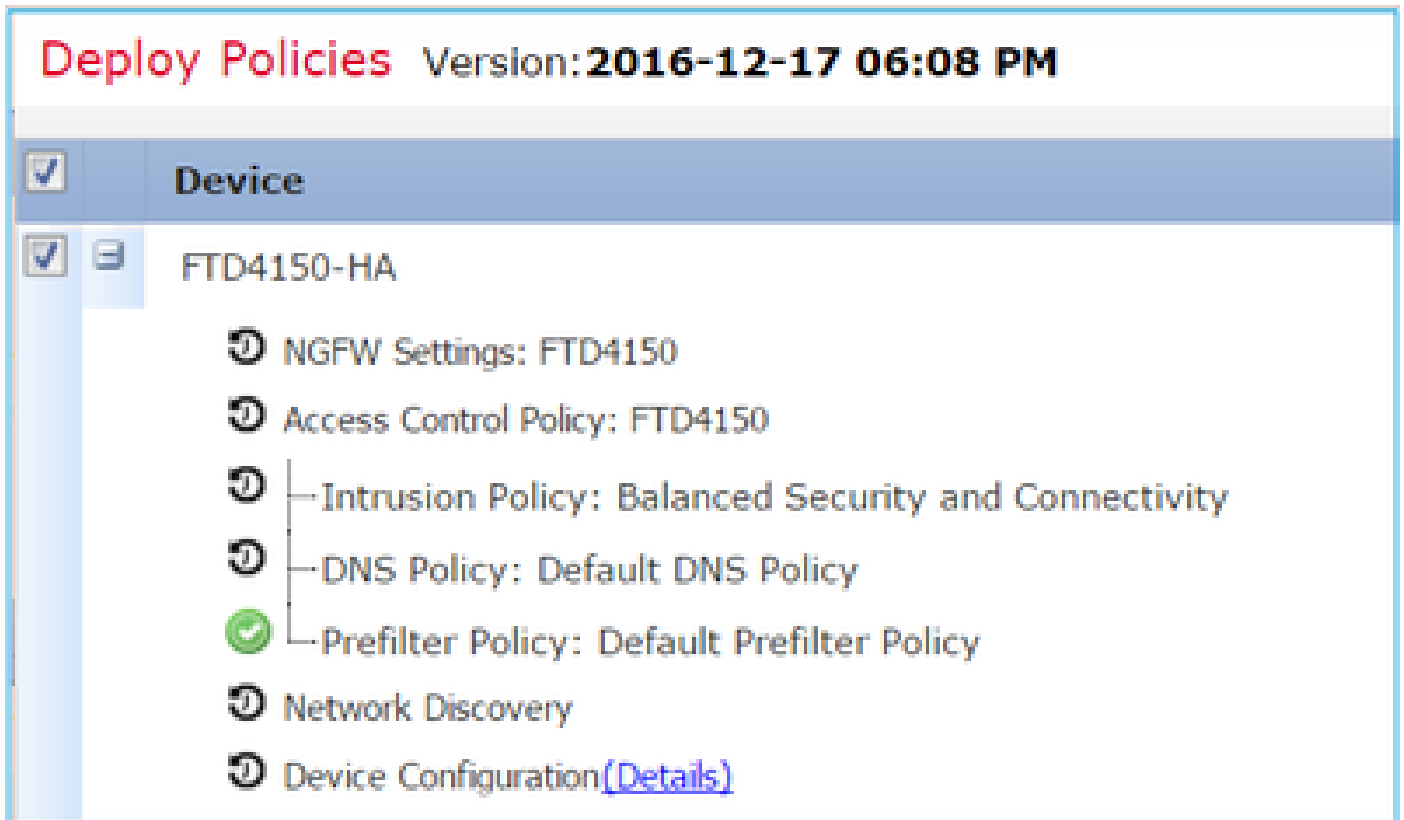
```
...
>
```

タスク 8.FTD HA ペアへのポリシーの展開

アップグレードが完了したら、HAペアにポリシーを導入する必要があります。FMC UI にその旨が表示されます。



ポリシーを展開します。



検証

FMC UI に表示されたアップグレード済みの HTD 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 に表示されたアップグレード済みの 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: 13fbc60-c378

関連情報

- [Cisco Firepower NGFW](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。