

Firepower アプライアンス上での FTD HA ペアのアップグレード

目次

[はじめに](#)

[目標](#)

[ラボのコンポーネント](#)

[トポロジ](#)

[FTD HA アップグレード プロセス](#)

[ステップ 1: 前提条件の確認](#)

[ステップ 2: イメージのアップロード](#)

[ステップ 3: セカンダリ FXOS のアップグレード](#)

[ステップ 4: FTD フェールオーバーの状態のスワップ](#)

[ステップ 5: プライマリ FXOS アプライアンスのアップグレード](#)

[ステップ 6: FMC ソフトウェアのアップグレード](#)

[ステップ 7: FTD HA ペアのアップグレード](#)

[ステップ 8: FTD HA ペアへのポリシーの展開](#)

[関連資料](#)

概要

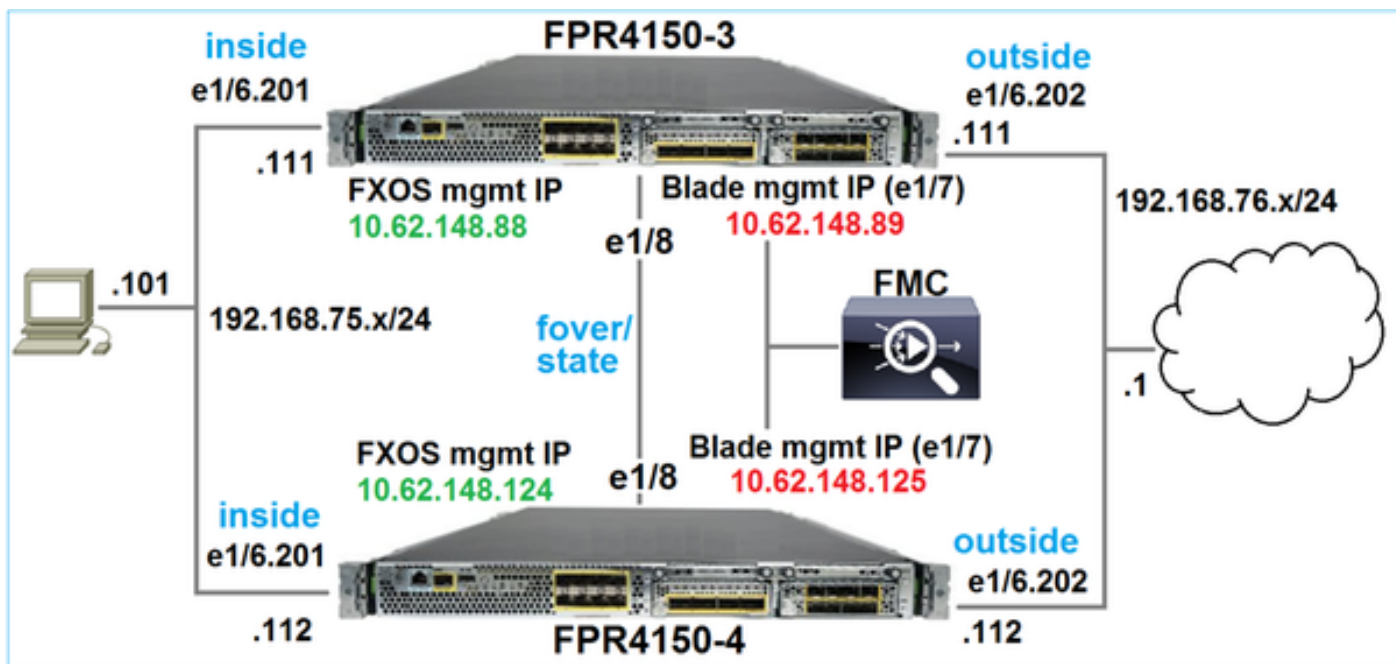
目標

このドキュメントは、Firepower アプライアンスで Firepower Threat Defense (FTD) を高可用性モードでアップグレードするプロセスを説明することを目的としています。

ラボのコンポーネント

- 2 X FP4150
- 1 X FS4000
- 1 PC

トポロジ



アクティビティ開始前のソフトウェア イメージのバージョンは次のとおりです。

- 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： 前提条件の確認

ステップ 2： FMC と SSP へのイメージのアップロード

ステップ 3： 2.0.1-37 から 2.0.1-86 へのセカンダリ FXOS のアップグレード

ステップ 4： FTD //

ステップ 5： 2.0.1-37 から 2.0.1-86 へのプライマリ FXOS のアップグレード

ステップ 6： 6.1.0-330 から 6.1.0.1 への FMC の アップグレード

ステップ 7： 6.1.0-330 から 6.1.0.1 への FTD HA ペア のアップグレード

ステップ 8： FMC から FTD HA ペアへのポリシーの展開

FTD HA アップグレード プロセス

ステップ 1： 前提条件の確認

次のバージョン間の互換性を特定するには、『FXOS 互換性ガイド』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

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

FXOS のアップグレード パスを特定するには、ターゲット バージョンの FXOS リリース ノートを確認してください。

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

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。

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

ステップ 2： 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 のアップグレードの場合： Sourcefire_3D_Defense_Center_S3_Patch-6.1.0.1-53.sh
- FTD のアップグレードの場合： Cisco_FTD_SSP_Patch-6.1.0.1-53.sh

ステップ 3： セカンダリ FXOS のアップグレード

アップグレード前：

```
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ます。

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 のアップグレードでは、シャーシをリブートする必要があります。

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 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すべて (FPRM、ファブリック インターコネクト、およびシャーシ) をアップグレードする必要があります。

```
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 のアップグレード プロセスの開始後数分で、FXOS CLI と GUI の両方から切断される場合がありますが、数秒後に再度ログインできるようになります。

5 分以内に FPRM コンポーネントのアップグレードが完了します。

```
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
```

10 分以内に、FXOS アップグレード プロセスの一環として、セカンダリ Firepower デバイスが再起動します。

```
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。

```
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 30 分以内に FXOS のアップグレードが完了します。

```
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 フェールオーバーの状態のスワップ

フェールオーバーの状態をスワップする前に、セカンダリ シャーシの FTD モジュールが完全に稼働していることを確認します。

```
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。

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

```
>
```

注：この時点で、最大 1 つの FTD 中継トラフィックがドロップされている場合があります。

ステップ 5：プライマリ FXOS アプライアンスのアップグレード

ステップ 2 のアップグレードと同様に、プライマリ FTD がインストールされている FXOS をアップグレードします。このステップは完了までに 30 分以上かかる可能性があります。

ステップ 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。

ステップ 7：FTD HA ペアのアップグレード

アップグレード前 :

```
> 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)
```

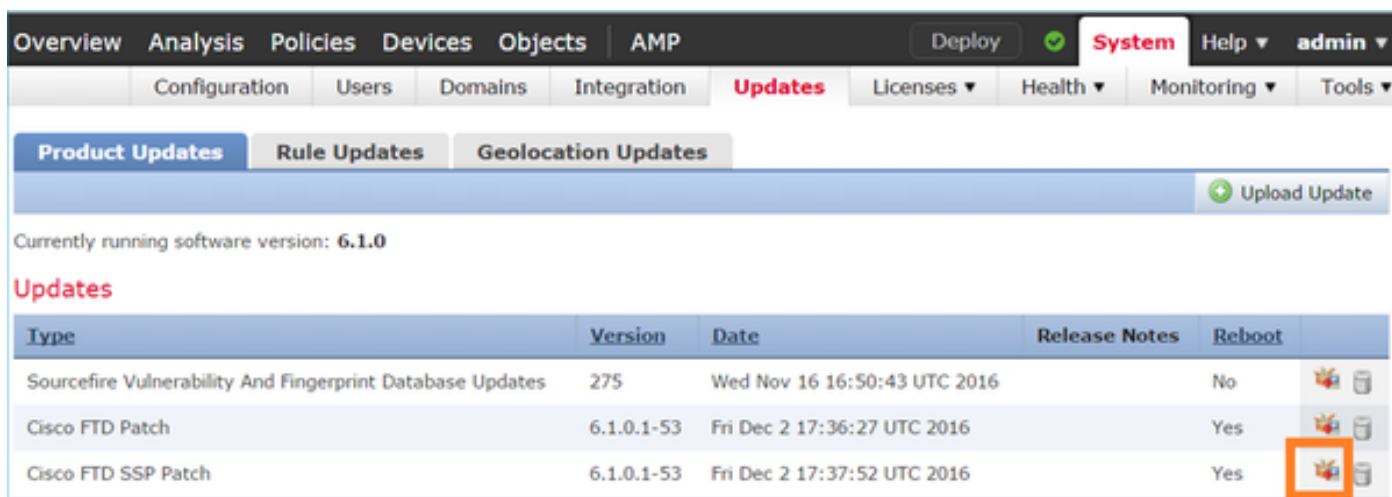
Stateful Obj	xmit	xerr	rcv	rerr
--------------	------	------	-----	------

General	6	0	9	0
---------	---	---	---	---

sys cmd	6	0	6	0
---------	---	---	---	---

...

FMC から [System] > [Update] メニューに移動し、FTD HA アップグレード プロセスを開始します。









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	 

必要に応じて、FTD アップグレードの Readiness Check を起動します。これには、FTD DB の整合性チェックが含まれています。

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

Currently running software version: 6.1.0

Selected Update

Type Cisco FTD SSP Patch
Version 6.1.0.1-53
Date Fri Dec 2 17:37:52 UTC 2016
Release Notes
Reboot Yes

By Group

Ungrouped (1 total)

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

Launch Readiness Check Install Cancel

このチェックの所要時間は 5 分以下で、このケースでは正常に終了しました。

Deployments Health Tasks

1 total | 0 waiting | 0 running | 0 retrying | 1 success | 0 failures

Remote Install 5m 2s

Apply to FTD4150-HA.
Readiness Check To 10.62.148.125 Success

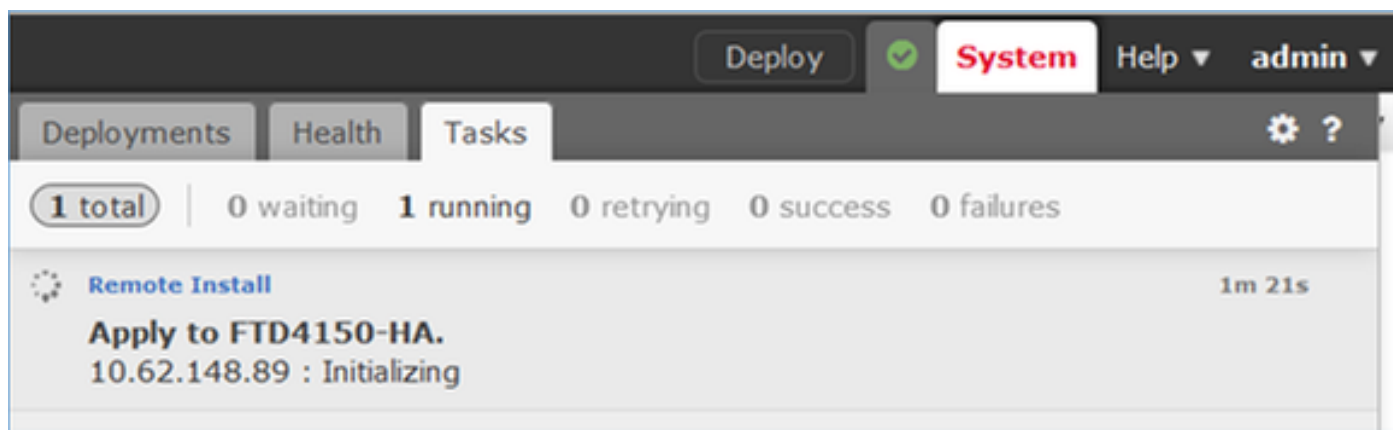
インストール プロセスを開始します。

Ungrouped (1 total)

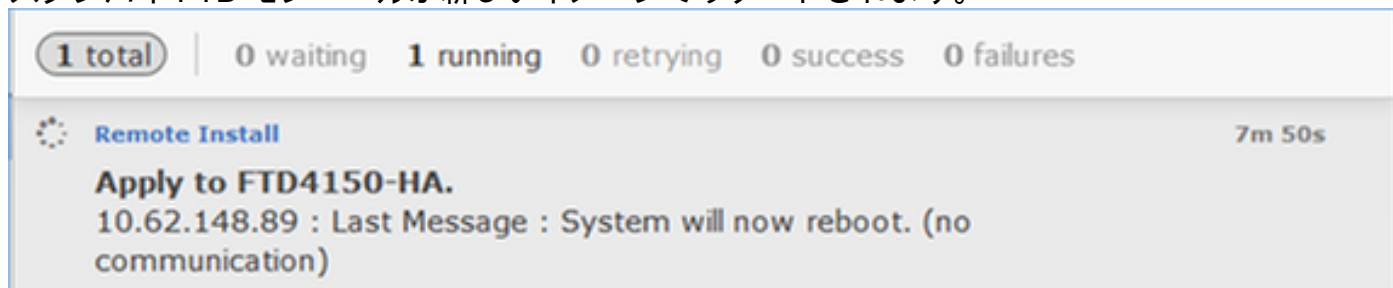
Device	Health Policy	Status
FTD4150-HA Cisco Firepower 4150 Threat Defense Cluster		
FTD4150-4 (active) 10.62.148.125 - Cisco Firepower 4150 Threat Defense v6.1.0	Initial Health Policy 2016-11-21 12:21:09	Success
FTD4150-3 10.62.148.89 - Cisco Firepower 4150 Threat Defense v6.1.0	Initial Health Policy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

Launch Readiness Check Install Cancel

最初に、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。



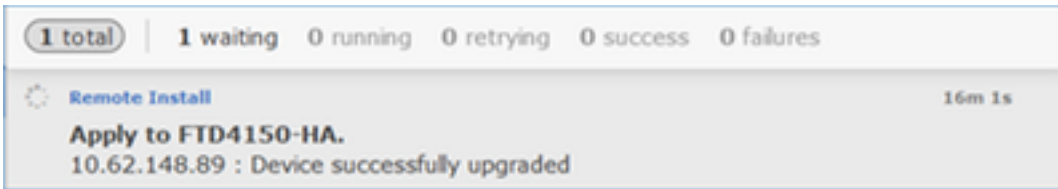
FXOS BootCLI モードから FTD のステータスを確認できます。

```
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
```

セカンダリ/アクティブ FTD CLI に、FTD モジュール間でのソフトウェア バージョンの不一致による警告メッセージが表示されます。

```
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 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。

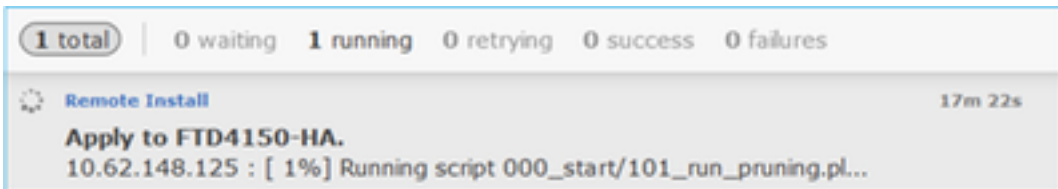


1 total | 1 waiting 0 running 0 retrying 0 success 0 failures

Remote Install 16m 1s

Apply to FTD4150-HA.
10.62.148.89 : Device successfully upgraded

FTD モジュールのアップグレードが開始されます。

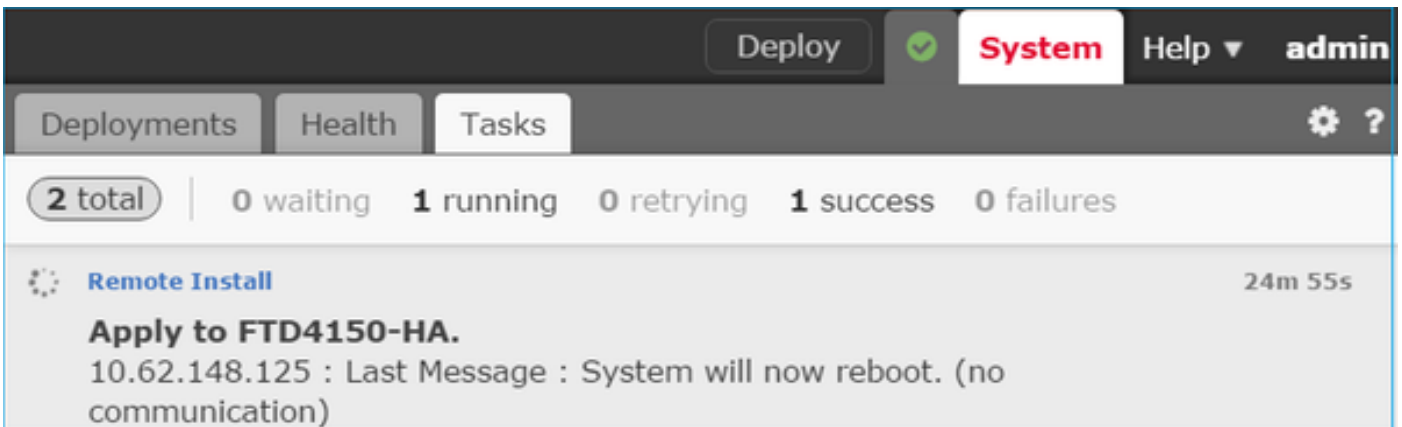


1 total | 0 waiting 1 running 0 retrying 0 success 0 failures

Remote Install 17m 22s

Apply to FTD4150-HA.
10.62.148.125 : [1%] Running script 000_start/101_run_pruning.pl...

プロセス終了時に、セカンダリ FTD が新しいイメージでブートされます。



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、FMC は内部ユーザ 'enable_1' を使用して FTD フェールオーバーの状態をスワップし、セカンダリ FTD からフェールオーバー設定を一時的に削除します。

```
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、フェールオーバーの状態のスワップにより、最大1つのパケットがドロップされていることが判明する場合があります。

このケースでは、FTD のアップグレード全体 (両方のユニット) は最大で 30 分かかりました。

検証

プライマリ FTD デバイスから FTD CLI を使用して検証します。

```
> 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 デバイスから次のコマンドを入力します。

```
> 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 ペアへのポリシーの展開

アップグレード完了後は、ポリシーを HA ペアに展開する必要があります。FMC UI にその旨が表示されます。

Deploy System Help admin

Deployments Health Tasks ?

2 total | 0 waiting 0 running 0 retrying 2 success 0 failures

✓ Remote Install 28m 14s ✕

Apply to FTD4150-HA.
Please reapply policies to your managed devices.

ポリシーを展開します。

Deploy Policies Version: 2016-12-17 06:08 PM

<input checked="" type="checkbox"/>	Device
<input checked="" type="checkbox"/>	FTD4150-HA <ul style="list-style-type: none">🔄 NGFW Settings: FTD4150🔄 Access Control Policy: FTD4150🔄 Intrusion Policy: Balanced Security and Connectivity🔄 DNS Policy: Default DNS Policy✓ Prefilter Policy: Default Prefilter Policy🔄 Network Discovery🔄 Device Configuration (Details)

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 : 13fcb60-c378

関連資料

[Cisco Firepower NGFW](#)