

升级Firepower设备上的FTD HA对

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[任务1.检验必备条件](#)

[任务2.上传软件映像](#)

[任务3.升级第一个FXOS机箱](#)

[任务4.交换FTD故障切换状态](#)

[任务5.升级第二个FXOS机箱](#)

[任务6.升级FMC软件](#)

[任务7.升级FTD HA对](#)

[任务8.将策略部署到FTD HA对](#)

[相关信息](#)

简介

本文档介绍Firepower设备在高可用性(HA)模式下进行Firepower威胁防御(FTD)升级的过程。

先决条件

要求

建议掌握下列主题的相关知识：

- Firepower Management Center (FMC)
- FTD
- Firepower设备(FXOS)

使用的组件

- 2个FPR4150
- 1个FS4000
- 1台PC

升级前的软件映像版本：

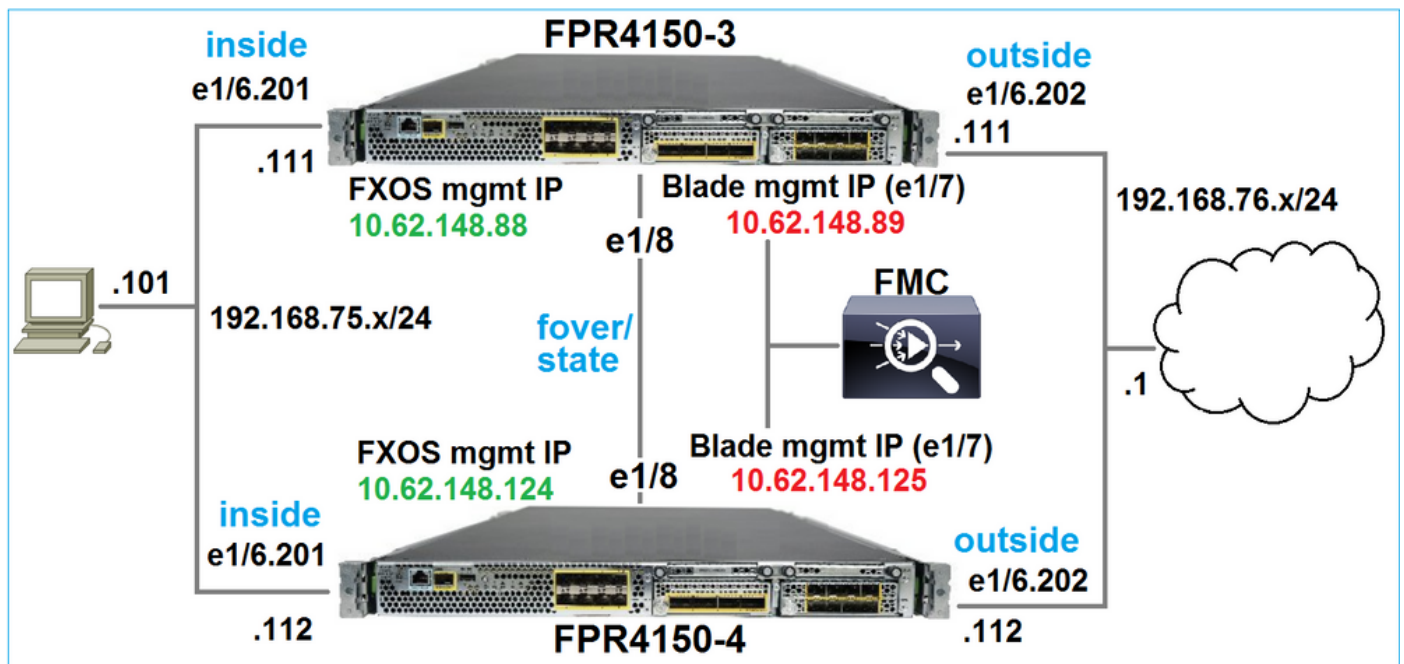
- FMC 6.1.0-330

- FTD主6.1.0-330
- FTD辅助6.1.0-330
- FXOS主2.0.1-37
- FXOS辅助2.0.1-37

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



行动计划

任务1：验证必备条件

任务2：将映像上传到FMC和SSP

任务3：升级第一个FXOS机箱(2.0.1-37 -> 2.0.1-86)

任务4：交换FTD故障切换

任务5：升级第二个FXOS机箱(2.0.1-37 -> 2.0.1-86)

任务6：升级FMC(6.1.0-330 -> 6.1.0.1)

任务7：升级FTD高可用性对(6.1.0-330 -> 6.1.0.1)


任务8：将策略从FMC部署到FTD HA对

任务1.检验必备条件

请查阅FXOS兼容性指南，以确定以下各项之间的兼容性：

- 目标FTD软件版本和FXOS软件版本
- Firepower硬件平台和FXOS软件版本

[Cisco Firepower 4100/9300 FXOS兼容性](#)

 注：此步骤不适用于FP21xx和更早的平台。

检查目标版本的FXOS发行版本注释以确定FXOS升级路径：

[Cisco Firepower 4100/9300 FXOS版本说明，2.0\(1\)](#)

 注：此步骤不适用于FP21xx和更早的平台。

请参阅FTD目标版本发行说明，以确定FTD升级路径：

[Firepower系统版本说明，版本6.0.1.2](#)


任务2.上传软件映像


在两个FCM上，上传FXOS映像(fxos-k9.2.0.1.86.SPA)。

在FMC上，上传FMC和FTD升级包：

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

任务3.升级第一个FXOS机箱

 注意：如果您将FXOS从1.1.4.x升级到2.x，请首先关闭FTD逻辑设备，升级FXOS，然后重新启用它。

 注：此步骤不适用于FP21xx和更早的平台。

升级前：

```
<#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

启动FXOS升级：

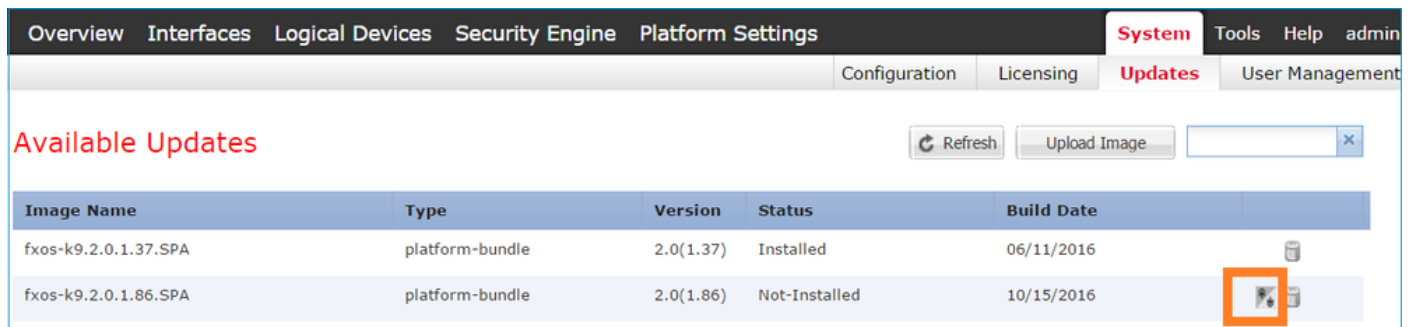



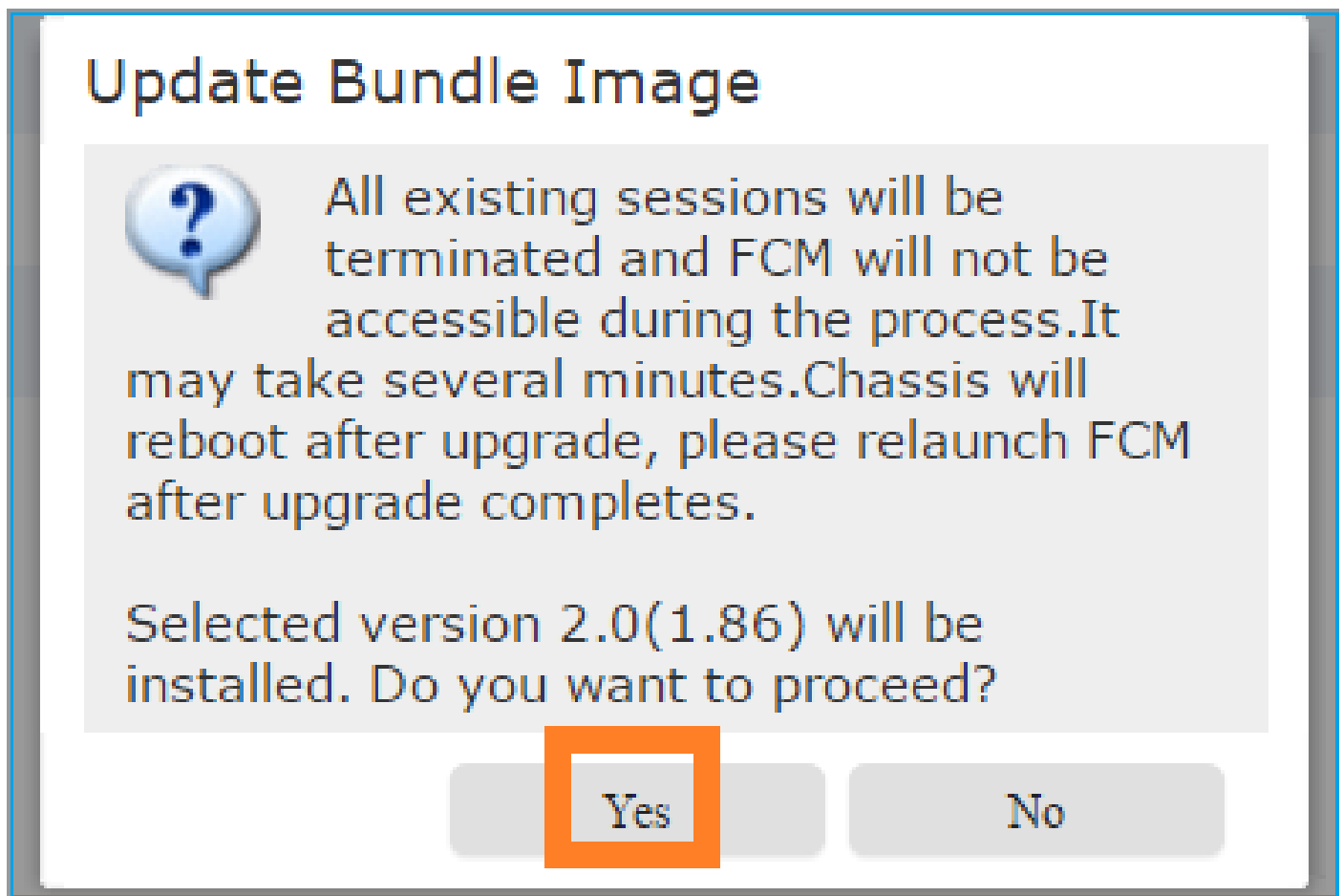



Image Name	Type	Version	Status	Build Date	
fxos-k9.2.0.1.37.SPA	platform-bundle	2.0(1.37)	Installed	06/11/2016	
fxos-k9.2.0.1.86.SPA	platform-bundle	2.0(1.86)	Not-Installed	10/15/2016	 

FXOS升级需要重新启动机箱：



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?

您可以从FXOS CLI监控FXOS升级。所有三个组件（FPRM、交换矩阵互联和机箱）都必须升级：

```
<#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
```

 **注意：**启动FXOS升级过程几分钟后，您将从FXOS CLI和GUI断开连接。几分钟后必须能够重新登录。

大约五分钟后，FPRM组件升级完成：

```
<#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
```

约10分钟后，作为FXOS升级过程的一部分，Firepower设备会重新启动：

```
<#root>
```

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

```
...
```

```
Restarting system.
```

重新启动后，升级过程将恢复：

```
<#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
```

在总共大约30分钟后，FXOS升级完成：

```
<#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

任务4.交换FTD故障切换状态

 注：此步骤不适用于FP21xx和更早的平台。

在交换故障切换状态之前，请确保机箱上的FTD模块完全打开：

```
<#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
...

```

交换FTD故障切换状态。从活动FTD CLI:

```

<#root>
>
no failover active


Switching to Standby

>

```

任务5.升级第二个FXOS机箱

类似于任务2，升级安装了新备用FTD的FXOS设备。完成此过程大约需要30分钟或更长时间。

 注：此步骤不适用于FP21xx和更早的平台。

任务6.升级FMC软件

将FMC从6.1.0-330升级到6.1.0.1。

任务7.升级FTD HA对

升级前：

```

<#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

...

从FMC System > Updates菜单，启动FTD HA升级过程：

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

Ungrouped (1 total)

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

Buttons: Launch Readiness Check, **Install**, Cancel

首先，升级主/备用FTD:

Deploy System Help admin

Deployments Health **Tasks** ?

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

Remote Install 1m 21s

Apply to FTD4150-HA.
10.62.148.89 : Initializing

备用FTD模块使用新映像重新启动：

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

Remote Install 7m 50s

Apply to FTD4150-HA.
10.62.148.89 : Last Message : System will now reboot. (no communication)

您可以从FXOS BootCLI模式验证FTD状态：

```
<#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

辅助/主用FTD CLI显示由于FTD模块之间的软件版本不匹配导致的警告消息：

<#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显示FTD设备已成功升级：

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

第二个FTD模块的升级开始：

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...

在该过程结束时，FTD将使用新映像启动：

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)

在后台，FMC使用内部用户enable_1，交换FTD故障切换状态，并暂时从FTD中删除故障切换配置：

```
<#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#
```

在本例中，整个FTD升级（两台设备）大约需要30分钟。

确认

此示例显示来自自主FTD设备的FTD CLI验证：

```
<#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

...
>

此示例显示从辅助/备用FTD设备的FTD CLI验证：

<#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)
```

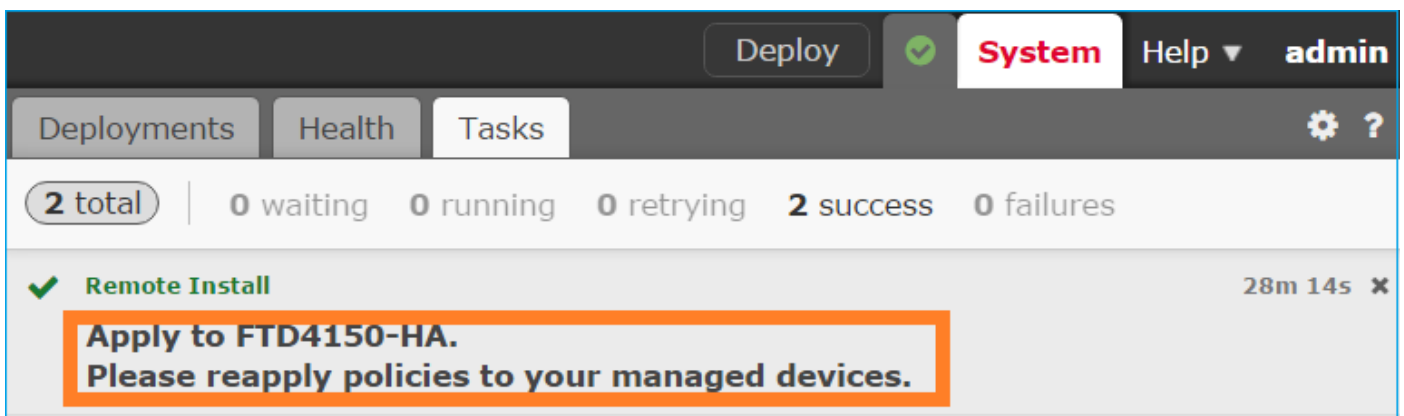
Stateful Failover Logical Update Statistics

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

...
>

任务8.将策略部署到FTD HA对

升级完成后，您需要将策略部署到HA对。FMC UI中显示以下内容：



部署策略：

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

Device

- FTD4150-HA
 - 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 [\(Details\)](#)

确认

从FMC UI看到的已升级的FTD HA对：

Overview	Analysis	Policies	Devices	Objects	AMP	
Device Management	NAT	VPN	QoS	Platform Settings		
Name						Group
Ungrouped (1)						
FTD4150-HA Cisco Firepower 4150 Threat Defense High Availability						
FTD4150-3(Primary, Active) 10.62.148.89 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed						
FTD4150-4(Secondary, Standby) 10.62.148.125 - Cisco Firepower 4150 Threat Defense - v6.1.0.1 - routed						

从FCM UI看到的已升级的FTD HA对：

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

相关信息

- [Cisco Firepower NGFW](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。