

通过由FMC管理的CLI升级FTD HA

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[准备升级](#)

[检查故障转移状态](#)

[上传升级包](#)

[就绪性检查](#)

[升级安装](#)

[验证](#)

简介

本文档介绍通过命令行界面(CLI)升级Cisco Firepower威胁防御(FTD)设备的详细过程。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙管理中心(FMC)
- 思科安全防火墙威胁防御(FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全防火墙管理中心v7.2.8
- 适用于VMWare v7.2.2的思科Firepower威胁防御

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。

背景信息

本文档的具体要求包括：

- 运行版本7.2或更高版本的思科安全防火墙威胁防御
- 运行版本7.2或更高版本的Cisco安全防火墙管理中心

配置

通过CLI升级一对FTD设备需要升级软件包文件存在于设备上。无需将任何待处理的部署作为通过CLI成功升级的先决条件，这一点至关重要。

准备升级



警告：检查升级顺序“备用/活动”以避免任何流量中断。

-
1. 从配置为备用设备的设备开始。
 2. 在专家模式下输入expert，然后在clish模式下输入sudo su以访问CLI。确认设备密码以提升权限

并进入专家模式。

```
Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.  
Cisco is a registered trademark of Cisco Systems, Inc.  
All other trademarks are property of their respective owners.
```

```
Cisco Firepower Extensible Operating System (FX-OS) v2.12.0 (build 1104)  
Cisco Firepower Threat Defense for VMware v7.2.2 (build 54)
```

```
> expert  
admin@firepower:~$ sudo su
```

```
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:
```

- #1) Respect the privacy of others.
- #2) Think before you type.
- #3) With great power comes great responsibility.

```
Password:  
root@firepower:/home/admin#  
root@firepower:/home/admin# cd  
root@firepower:~#  
root@firepower:~#
```

检查故障转移状态

验证故障切换状态，以确保这些步骤应用于辅助FTD（可显示为“辅助就绪”和“备用就绪”）。

```
firepower#  
firepower# sh failover state
```

	State	Last Failure Reason	Date/Time
This host -	Secondary Standby Ready	None	
Other host -	Primary Active	None	

```
====Configuration State====  
    Sync Done - STANDBY  
====Communication State====  
    Mac set
```

```
firepower#  
firepower#
```

上传升级包

导航到设置>更新>产品更新>上传本地软件更新包，通过FMC将升级包上传到两个设备。从software.cisco.com选择先前下载的软件包，然后选择Upload。

在FMC上上传Firepower数据包后，请继续使用Upgrade按钮。

Firewall Management Center
System / Product Upgrades

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒

Product Upgrades

System Overview

Management Center: 7.2.8-25
Already running latest version.
Last upgrade performed: 7.2.5-208 → 7.2.8-25

Threat Defense: 1 cluster/HA pair
Visit [Device Management](#) to view your devices.
Upgrade: Initiated (7.2.2-54) [View](#)

Available Upgrade Packages

These are the downloadable upgrades that apply to your current deployment, and the upgrade packages you have manually uploaded or configured. [Upgrade Guide](#)

Upgrade	Release Date	Required Minimum Version	Availability	Actions
> 7.2.8-25	2024-05-31	6.6.0	Downloaded	...
▼ 7.2.7-500	2024-04-27	6.6.0	Downloaded	Upgrade ...
Firepower Threat Defense for ASA/ISA/FTDv				Downloaded ...
> 7.2.2-54	2022-11-22	6.6.0	Downloaded	...
> 6.6.5-81	2021-07-28	6.2.3	Downloaded	...

升级按钮

在升级向导中，您需要选择FTD HA设备，然后选择设备，并点击Add to Selection。

Firewall Management Center
Devices / Upgrade / Threat Defense Upgrade

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒

Threat Defense Upgrade

1 Copy Upgrade Packages to Devices — 2 Compatibility and Readiness Checks — 3 Upgrade — 4 Upgrade Status

Upgrade to: 7.2.7-500 [Manage Upgrade Packages](#) [Unattended Mode](#)

Device Selection **Action**

1 cluster/HA pair is a candidate to add to your upgrade list.

No devices selected. Use the Device Details pane to select devices to upgrade to the selected version. Or, use [Device Management](#) to select more devices.

Device Details

1 cluster/HA pair is a candidate to add to your upgrade list.

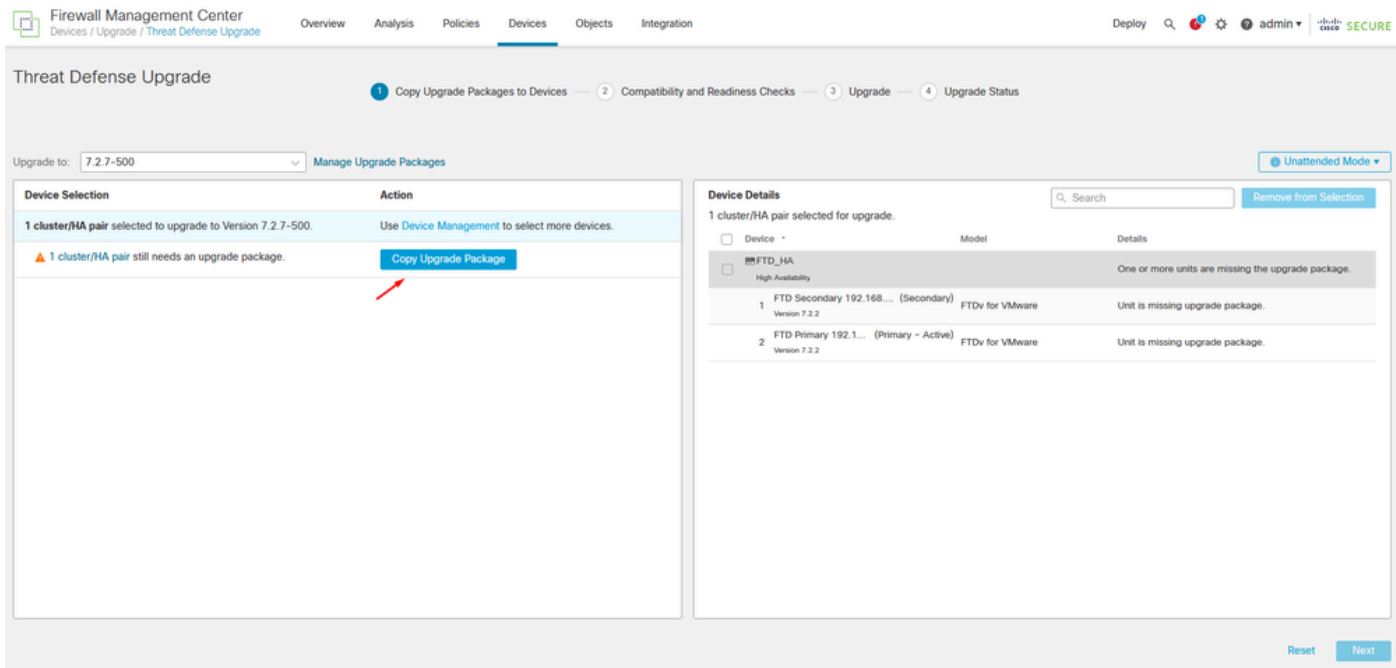
Device	Model	Details
<input checked="" type="checkbox"/> FTD_HA High Availability		
FTD Primary 192.168.192.13 (Primary)	FTDv for VMware	Version 7.2.2
FTD Secondary 192.168.192.14 (Secondary)	FTDv for VMware	Version 7.2.2

[Add to Selection](#)

[Reset](#) [Next](#)

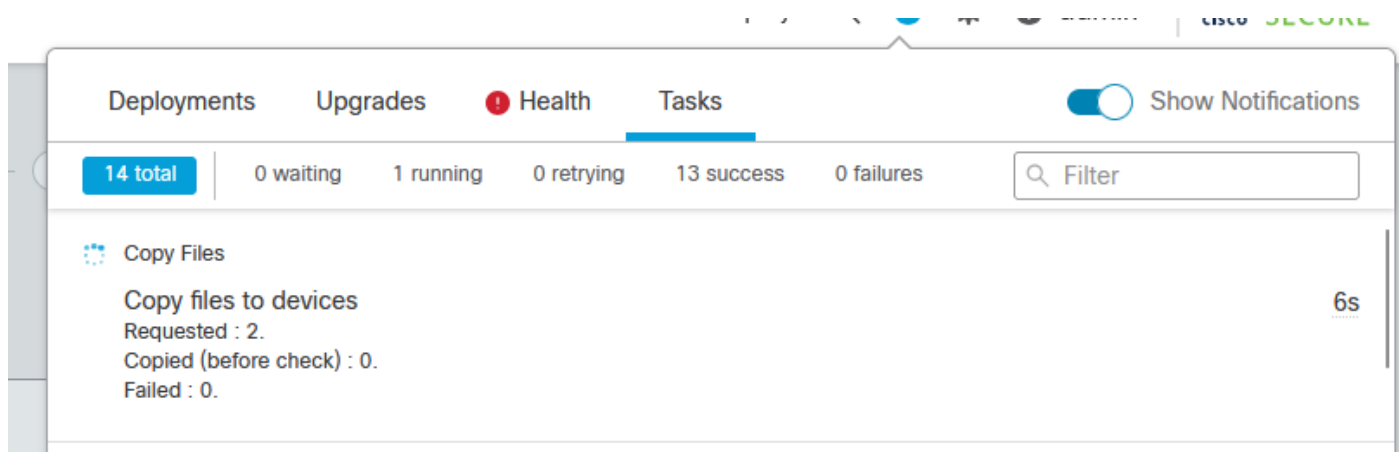
添加到选定内容

然后，您可以在设备上复制升级包，系统将显示一条消息，以继续升级包。



复制升级包按钮

在“通知”任务中，您可以找到将文件复制到设备的作业。任务完成后，即会完成并成功。



将文件复制到设备的任务

您可以验证软件包是否已上传到以下路径上的设备：

```

root@firepower:/ngfw/var/sf/updates#
root@firepower:/ngfw/var/sf/updates# ls -l
total 2181772
-rw-r--r-- 1 root root 1110405120 Jul 18 01:08 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar
-rw-r--r-- 1 root root 815 Jul 18 01:23 Cisco_FTD_Upgrade-7.2.2-54.sh.REL.tar.METADATA
-rw-r--r-- 1 root root 1123706880 Jul 18 02:36 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
-rw-r--r-- 1 root root 854 Jul 18 02:37 Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar.METADATA
root@firepower:/ngfw/var/sf/updates#

```

就绪性检查

使用命令，从辅助设备上的CLI执行就绪性检查：

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
```

例如：

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach --readiness-check /ngfw/var/sf/updates/
ARGV[0] = --detach
ARGV[1] = --readiness-check
ARGV[2] = /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
[Readiness-Info]filename : /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar at /usr/local/sf/lib
This was not run through the SF::System APIs at /usr/local/sf/lib/perl/5.24.4/SF/System/Wrappers.pm line
MakeSelf GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/MakeSelf.pm 1
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade_Readiness-7.2.7-500.sh at /usr/local/
root@firepower:/ngfw/var/sf/updates#
```

通过以下路径监控就绪性检查流程：

```
root@firepower : /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness
```

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness# cat upgrade_readiness_status
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 0% MESSAGE:Running script 000_start/000_00_run_cli_kic
TIMESTAMP:Thu Jul 18 02:43:05 UTC 2024 PERCENT: 5% MESSAGE:Running script 000_start/000_check_platform
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:10% MESSAGE:Running script 000_start/100_start_messages
TIMESTAMP:Thu Jul 18 02:43:06 UTC 2024 PERCENT:14% MESSAGE:Running script 000_start/101_run_pruning.pl
TIMESTAMP:Thu Jul 18 02:43:41 UTC 2024 PERCENT:19% MESSAGE:Running script 000_start/105_check_model_nu
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:24% MESSAGE:Running script 000_start/106_check_HA_state
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:29% MESSAGE:Running script 000_start/107_version_check.
TIMESTAMP:Thu Jul 18 02:43:42 UTC 2024 PERCENT:33% MESSAGE:Running script 000_start/108_clean_user_sta
TIMESTAMP:Thu Jul 18 02:43:43 UTC 2024 PERCENT:38% MESSAGE:Running script 000_start/110_DB_integrity_c
TIMESTAMP:Thu Jul 18 02:43:47 UTC 2024 PERCENT:43% MESSAGE:Running script 000_start/113_EO_integrity_c
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:48% MESSAGE:Running script 000_start/250_check_system_f
TIMESTAMP:Thu Jul 18 02:43:50 UTC 2024 PERCENT:52% MESSAGE:Running script 000_start/410_check_disk_spa
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:57% MESSAGE:Running script 200_pre/001_check_reg.pl...
TIMESTAMP:Thu Jul 18 02:43:55 UTC 2024 PERCENT:62% MESSAGE:Running script 200_pre/002_check_mounts.sh.
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:67% MESSAGE:Running script 200_pre/004_check_deploy_pac
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:71% MESSAGE:Running script 200_pre/005_check_manager.pl
TIMESTAMP:Thu Jul 18 02:43:56 UTC 2024 PERCENT:76% MESSAGE:Running script 200_pre/006_check_snort.sh..
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:81% MESSAGE:Running script 200_pre/007_check_sru_instal
TIMESTAMP:Thu Jul 18 02:43:57 UTC 2024 PERCENT:86% MESSAGE:Running script 200_pre/009_check_snort_prep
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:90% MESSAGE:Running script 200_pre/011_check_self.sh...
TIMESTAMP:Thu Jul 18 02:43:58 UTC 2024 PERCENT:95% MESSAGE:Running script 200_pre/015_verify_rpm.sh...
TIMESTAMP:Thu Jul 18 02:44:00 UTC 2024 PERCENT:100% MESSAGE:Readiness Check completed successfully.
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_readiness#
```

如果就绪性检查失败，请联系思科TAC。

升级安装

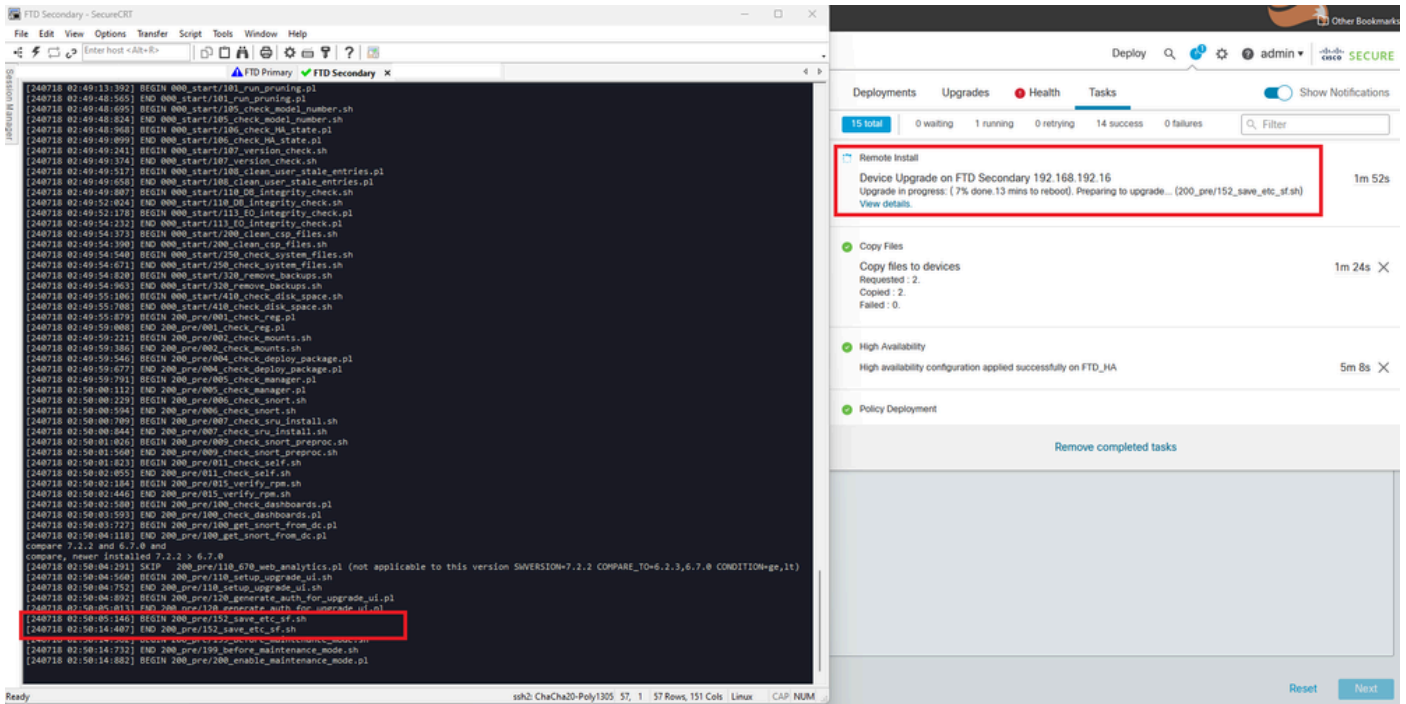
在辅助FTD上继续升级安装。导航到包含升级文件的文件夹并执行安装命令：

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach <FTD_Upgrade_Package.sh.REL.tar>
```

一旦执行升级，就会出现如下所示的输出：

```
root@firepower:/ngfw/var/sf/updates# install_update.pl --detach Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
ARGV[0] = Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
bundle_filepath: Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
updated absolute bundle_filepath: /ngfw/var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
install_update.pl begins. bundle_filepath: /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.REL.tar
Makeself GetUpdate Info params FILEPATH : /var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr/
FILEPATH directory name /var/tmp/upgrade-patch at /usr/local/sf/lib/perl/5.24.4/SF/Update/Makeself.pm 1
Inside GetInfo FILEPATH :/var/tmp/upgrade-patch/Cisco_FTD_Upgrade-7.2.7-500.sh at /usr/local/sf/lib/per
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value in string at /usr/local/sf/lib/perl/5.24.4/SF/Update/StatusProc.pm line 196.
Use of uninitialized value $in_container in string eq at /usr/local/sf/lib/perl/5.24.4/SF/Update/Status
Verifying archive integrity... All good.
Uncompressing Cisco FTD Upgrade / Sat Apr 27 04:09:29 UTC 2024.....
Entering is_fmc_managed
Device is FMC Managed
[240718 02:48:13:868] Found original ftd upgrade file /var/sf/updates/Cisco_FTD_Upgrade-7.2.7-500.sh.RE
[240718 02:48:16:990] MAIN_UPGRADE_SCRIPT_START
[240718 02:48:17:006] #####
[240718 02:48:17:007] # UPGRADE STARTING
[240718 02:48:17:008] #####
compare 7.2.2 and 6.2.3 and
compare, newer installed 7.2.2 > 6.2.3
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/var/sf/sync/updates_status_logs
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/var/sf/sync/updates_s
Link to JSON upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json created i
Running [ln -f /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/var/sf/sync/updates_st
Link to log upgrade status file /ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log created in
[240718 02:48:17:229] BEGIN 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:421] END 000_start/000_00_run_cli_kick_start.sh
[240718 02:48:18:525] BEGIN 000_start/000_00_run_troubleshoot.sh
```

在FMC上，有一个任务在辅助设备运行升级：



在FMC上运行的任务

使用以下路径监控升级状态：

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-X.X.X# tail -f upgrade_status.log
```

以下是输出示例：

```
root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7# tail -f upgrade_status.log
TIMESTAMP:Thu Jul 18 02:50:25 UTC 2024 PERCENT: 7% MESSAGE:Running script 200_pre/202_disable_syncd.sh
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT: 7% MESSAGE:Running script 200_pre/400_restrict_rpc.sh
TIMESTAMP:Thu Jul 18 02:50:26 UTC 2024 PERCENT: 7% MESSAGE:Running script 200_pre/500_stop_system.sh..
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14% MESSAGE:Running script 200_pre/501_recovery.sh... T
TIMESTAMP:Thu Jul 18 02:50:53 UTC 2024 PERCENT:14% MESSAGE:Running script 200_pre/505_revert_prep.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14% MESSAGE:Running script 200_pre/999_enable_sync.sh..
TIMESTAMP:Thu Jul 18 02:51:46 UTC 2024 PERCENT:14% MESSAGE:Running script 300_os/001_verify_bundle.sh.
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14% MESSAGE:Running script 300_os/002_set_auto_neg.pl..
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14% MESSAGE:Running script 300_os/060_fix_fstab.sh... T
TIMESTAMP:Thu Jul 18 02:51:47 UTC 2024 PERCENT:14% MESSAGE:Running script 300_os/100_install_Fire_Linu
```

辅助设备上的升级完成后，您将看到以下消息：

```
240718 13:40:58:872] Attempting to remove upgrade lock
[240718 13:40:58:873] Success, removed upgrade lock
Upgrade lock /ngfw/tmp/upgrade.lock removed successfully.
[240718 13:40:58:882]
[240718 13:40:58:883] #####
[240718 13:40:58:885] # UPGRADE COMPLETE #
```



```
[240718 13:40:58:887] #####
Entering create_upgrade_status_links...
Create upgrade_status.json and upgrade_status.log link in /ngfw/Volume/root/ngfw/var/sf/sync/updates_st
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.json /ngfw/Volum
Link to JSON upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_stat
Running [ln -f /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_status.log /ngfw/Volum
Link to log upgrade status file /ngfw/Volume/root/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.7/upgrade_statu
Process 10677 exited.I am going away.
RC: 0
Update package reports success: almost finished...
Scheduling a reboot to occur in 5 seconds...
Process 12153 exited.I am going away.
root@firepower:/ngfw/var/sf/updates#
Broadcast message from root@firepower (Thu Jul 18 13:41:05 2024):

The system is going down for reboot NOW!
```

从备用设备完成升级后，设备将重新启动。设备启动后，请检查故障切换状态，确保一切保持最初配置的状态。

在活动FTD上，您可以找到以下内容：

```
firepower# show failover state

This host - State Primary Last Failure Reason None Date/Time
            Active
Other host - State Secondary Last Failure Reason Comm Failure Date/Time
            Standby Ready 13:24:46 UTC Jul 18 2024

====Configuration State====
      Sync Done
====Communication State====
      Mac set

firepower#
```

在备用FTD上，您会发现：

```
firepower#
firepower# sh failover state

This host - State Secondary Last Failure Reason None Date/Time
            Standby Ready
Other host - State Primary Last Failure Reason None Date/Time
            Active

====Configuration State====
      Sync Skipped - STANDBY
====Communication State====
      Mac set
```

firepower#

将会出现一则消息，显示版本不同。

```
firepower#  
*****WARNING****WARNING****WARNING*****  
    Mate version 9.18(4)201 is not identical with ours 9.18(2)200  
*****WARNING****WARNING****WARNING*****
```

在备用设备上，使用命令failover active通过CLI手动执行故障切换。现在，备用设备变为主用设备。



警告：此时，发生故障切换时流量会短暂中断。

```
firepower#
firepower# failover active

Switching to Active
firepower#
firepower#
firepower# sh fail
firepower# sh failover state
```

	State	Last Failure Reason	Date/Time
This host -	Secondary Active	None	
Other host -	Primary Standby Ready	None	

```
====Configuration State====
Sync Skipped
====Communication State====
Mac set
```

```
firepower#
```

故障转移完成后，您可以继续升级其他设备。对于之前处于活动状态现在处于备用状态的设备，请使用本文档开头介绍的相同步骤。

现在两台设备都已升级。您可以通过Lina端的show version命令看到。对于主设备：

```
firepower#
firepower# show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary Standby Ready	None	
Other host -	Secondary Active	None	

```
====Configuration State====
Sync Skipped - STANDBY
====Communication State====
Mac set
```

```
firepower#
```

对于辅助设备：

```
firepower#
firepower# sh failover state
```

	State	Last Failure Reason	Date/Time
This host -	Secondary Active	None	
Other host -	Primary Standby Ready	Comm Failure	14:03:06 UTC Jul 18 2024

```
====Configuration State====
      Sync Skipped
====Communication State====
      Mac set
```

```
firepower#
```

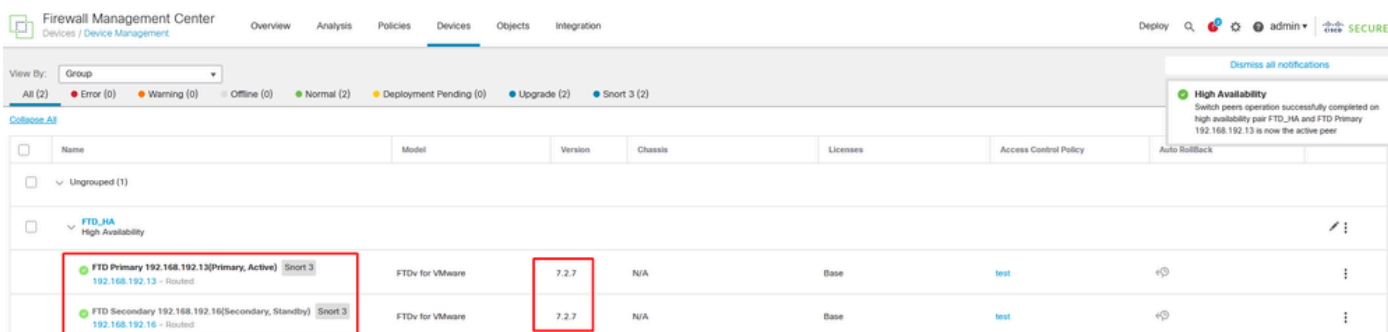
此时，您可以像在开始时一样从FMC切换设备。

验证

成功升级两个设备后，使用show version命令验证FMC内和两个FTD的状态。

```
firepower# show version
-----[ firepower ]-----
Model          : Cisco Firepower Threat Defense for VMware (75) Version 7.2.7 (Build 500)
UUID           : 0edf9f22-78e6-11ea-8ed0-e0e5abf334e2
LSP version    : lsp-rel-20240306-2015
VDB version    : 353
-----
```

在FMC上，您可以看到版本更新，并准备像在开始时一样进行切换。



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
FTD Primary 192.168.192.13(Primary, Active) Snort 3 192.168.192.13 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	↔
FTD Secondary 192.168.192.16(Secondary, Standby) Snort 3 192.168.192.16 - Routed	FTDv for VMware	7.2.7	N/A	Base	test	↔

来自FMC的交换对等体

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）。