

Cisco Firepower 管理中心升级指南，版本 6.0 – 7.0

首次发布日期: 2018 年 3 月 29 日

上次修改日期: 2023 年 4 月 14 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2018 – 2023 Cisco Systems, Inc. 保留所有权利。



目录

第 1 章 使用入门 1

本指南适用对象 1

功能历史记录 3

第 2 章 规划升级 9

升级规划阶段 9

当前版本和型号信息 10

升级路径 11

升级路径：Firepower 管理中心 12

升级路径：带有 FTD 逻辑设备和 FMC 的 14

升级路径：其他 Firepower 威胁防御 设备 18

升级路径：Firepower 7000/8000 系列 20

升级路径： ASA FirePOWER 22

升级路径：适用于 ASA FirePOWER 的 ASA 25

升级路径：NGIPSv 29

无响应的升级 31

时间和磁盘空间测试 32

下载升级包 33

Firepower 软件包 34

FXOS 软件包 35

ASA 软件包 36

上传 的 Firepower 软件升级包 37

上传到 Firepower 管理中心 37

上传到内部服务器（带有 FMC 的版本 6.6.0+ FTD） 38

复制到托管设备 39
Firepower 软件就绪性检查 40
通过 FMC 运行就绪性检查（版本 7.0.0+ FTD） 40
通过 FMC 运行就绪性检查（版本 6.7.0+） 40
通过 FMC 运行就绪性检查（版本 6.0.1 – 6.6.x） 41

第 3 章 升级 Firepower 管理中心 43
升级核对表：Firepower 管理中心 43
升级独立 Firepower 管理中心 46
升级高可用性 Firepower 管理中心 47

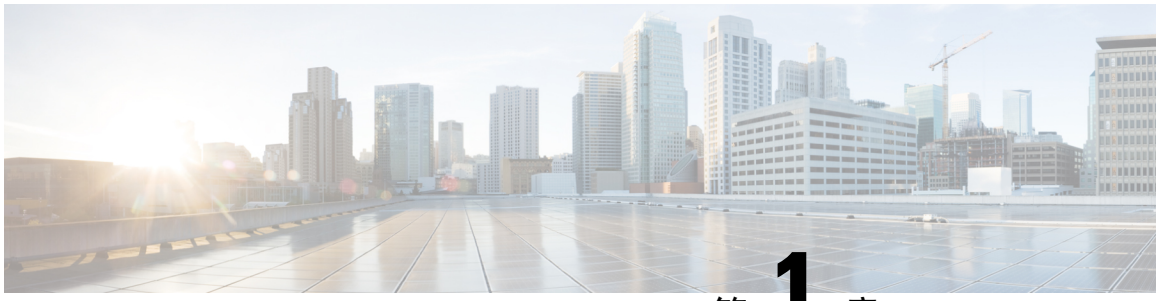
第 4 章 通过 Firepower 管理中心升级 Firepower 威胁防御 49
升级核对表：带有 FMC 的 Firepower 威胁防御 49
在带有 Firepower 威胁防御逻辑设备的 Firepower 4100/9300 上升级 FXOS 54
升级 FXOS：FTD 独立设备或机箱内集群 54
使用 Firepower 机箱管理器为独立 FTD 逻辑设备或 FTD 机箱内集群升级 FXOS 54
使用 FXOS CLI 为独立 FTD 逻辑设备或 FTD 机箱内集群升级 FXOS 55
升级 FXOS：FTD 高可用性对 58
使用 Firepower 机箱管理器升级 FTD 高可用性对上的 FXOS 58
使用 FXOS CLI 在 FTD 高可用性对上升级 FXOS 61
升级 FXOS：FTD 机箱内集群 65
使用 Firepower 机箱管理器升级 FXOS 和 FTD 机箱内集群 66
使用 FXOS CLI 在 FTD 机箱内集群上升级 FXOS 68
升级带有 FMC 的 Firepower 威胁防御（版本7.0.0） 71
升级带有 FMC 的 Firepower 威胁防御（版本6.0.1 – 6.7.0） 74

第 5 章 升级 Firepower 7000/8000 系列和 NGIPSv 77
升级核对表：带有 FMC 的 Firepower 7000/8000 系列和 NGIPSv 77
升级带有 FMC 的 Firepower 7000/8000 和 NGIPSv 80

第 6 章 升级具备 FirePOWER 服务的 ASA 83

升级核对表：带有 FMC 的 ASA FirePOWER 83
升级 ASA 87
升级独立设备 87
使用 CLI 升级独立设备 87
使用 ASDM 从本地计算机升级独立设备 89
使用 ASDM Cisco.com 向导升级独立设备 89
升级主用/备用故障转移对 91
使用 CLI 升级主用/备用故障转移对 91
使用 ASDM 升级主用/备用故障转移对 94
升级主用/主用故障转移对 95
使用 CLI 升级主用/主用故障转移对 95
使用 ASDM 升级主用/主用故障转移对 98
升级 ASA 集群 100
使用 CLI 升级 ASA 集群 100
使用 ASDM 升级 ASA 集群 105
升级带有 FMC 的 ASA FirePOWER 模块 107

第 7 章 卸载补丁 (Uninstall a Patch) 109
支持卸载的补丁 109
高可用性/可扩展性的卸载顺序 112
通过 FMC 卸载设备补丁 113
卸载独立 FMC 补丁 115
卸载高可用性 FMC 补丁 116



第 1 章

使用入门

- 本指南适用对象， 第 1 页
- 功能历史记录， 第 3 页

本指南适用对象

本指南介绍如何为以下对象准备并成功升级到 Firepower **7.0.x 或更早版本**：

- Firepower 管理中心 (FMC)
- 带有 FMC 的 Firepower 威胁防御 (FTD) 设备，包括适用于 Firepower 4100/9300 的 FXOS
- 带有 FMC 的 7000/8000 系列设备
- 带有 FMC 的 NGIPSv 设备
- 带有 FMC 的 ASA FirePOWER 设备，包括 ASA OS

其他资源

如果您要升级其他平台/组件或升级到其他版本，请参阅以下资源之一。

表 *1:* 升级 *FMC*

当前 **FMC** 版本	指南
云交付的管理中心（无版本）	无。我们负责更新。
7.2+	《适用于管理中心的 Cisco Secure Firewall Threat Defense 升级指南》中的升级管理中心。
7.1	《适用于 Firepower 管理中心版本 7.1 的 Cisco Firepower Threat Defense 升级指南》中的。
7.0 或更早版本	。

表 *2:* 通过 *FMC* 升级 *FTD*

当前 FMC 版本	指南
云交付的管理中心（无版本）	《适用于管理中心的 Cisco Secure Firewall Threat Defense 升级指南》中的。
7.2+	。
7.1	《适用于 Firepower 管理中心版本 7.1 的 Cisco Firepower Threat Defense 升级指南》中的。
7.0 或更早版本	。

表 *3:* 通过 *FDM* 升级 *FTD*

当前 FTD 版本	指南
7.2+	。
7.1	《适用于 Firepower 设备管理器版本 7.1 的 Cisco Firepower Threat Defense 升级指南》中的。
7.0 或更早版本	您的版本的《适用于 Firepower 设备管理器的 Cisco Firepower Threat Defense 配置指南》中的系统管理。 对于 Firepower 4100/9300，另请参阅《Cisco Firepower 4100/9300 升级指南》，FTD 6.0.1-7.0.x 或 ASA 9.4（1)-9.16(x)包括 FXOS 1.1.1-2.10.1中的 FXOS 升级说明。
版本 6.4+，带有 CDO	使用思科防御协调器管理 FDM 设备中的激活设备和服务。

表 *4:* 升级 *NGIPS* 设备

当前管理器版本	平台	指南
任意	Firepower 7000/8000 系列	。
任意	带有 FMC 的 ASA FirePOWER	。
任意	使用 ASDM 的 ASA FirePOWER	。

表 *5:* 升级其他组件

版本	组件	指南
任意	Firepower 4100/9300 上的 ASA 逻辑设备	Cisco Secure Firewall ASA 升级指南。
最新	用于 FMC 的 BIOS 和固件	Cisco Secure Firewall Threat Defense/Firepower Hotfix 版本说明。
最新	Firepower 4100/9300 的固件	Cisco Firepower 4100/9300 FXOS 固件升级指南
最新	ISA 3000 的 ROMMON 映像	Cisco Secure Firewall ASA 和 Secure Firewall Threat Defense 重新映像指南。

功能历史记录

表 *6:* 版本 *7.0.0* 功能

特性	说明
改进了 FTD 升级性能和状态报告。	FTD升级现在更容易、更快、更可靠，并且占用的磁盘空间更少。消息中心的新**升级**选项卡进一步增强了升级状态和错误报告功能。

特性	说明
FTD 设备易于遵循的升级工作流程。	FMC 上的新设备升级页面（**设备 (Devices) > 设备升级 (Device Upgrade)**）为升级版本 6.4+ FTD 设备提供了一个易于遵循的向导。它将引导您完成重要的升级前阶段，包括选择要升级的设备，将升级包复制到设备，以及兼容性和就绪性检查。 首先，请使用“设备管理”页面上的新 **升级 Firepower 软件** 操作（**设备 > 设备管理 > 选择操作**）。 继续操作时，系统会显示有关所选设备的基本信息以及当前的升级相关状态。这包括无法升级的任何原因。如果设备未在向导中“通过”某个阶段，则该阶段不会显示在下一阶段。 如果您离开向导，系统会保留您的进度，但具有管理员访问权限的其他用户可以重置、修改或继续向导。 **注释** 您仍必须使用 **系统**（⚙）> **更新 (Updates)** 来上传或指定FTD升级包的位置。您还必须使用“系统更新”页面升级 FMC 本身以及所有非 FTD 托管设备。 **注释** 在版本 7.0 中，向导无法正确显示集群或高可用性对中的设备。即使必须将这些设备作为一个单元进行选择和升级，向导也会将其显示为独立设备。设备状态和升级就绪性会逐个评估和报告。这意味着一台设备可能会“传递”到下一阶段，而另一台设备则不会。但是，这些设备仍然分组。因此，在一台设备上运行就绪性检查，所有设备上都会运行。在一台设备上启动升级，在所有设备上都会启动升级。 为避免可能的耗时升级失败，请手动确保所有组成员都已准备好继续执行向导的下一步，然后再点击 **下一步**。

特性	说明
一次升级更多 FTD 设备。	FTD 升级向导取消了以下限制： • 同步设备升级。 一次可以升级的设备数量现在受管理网络带宽的限制，而不是系统管理同步升级的能力。以前，我们建议不要一次升级超过五台设备。 **重要事项** 只有升级到 FTD 版本 6.7+ 才能看到此改进。如果您要将设备升级到较旧的FTD版本（即使您使用的是新的升级向导），我们仍建议您一次限制为五台设备。 • 按设备型号分组升级。 现在，只要系统有权访问相应的升级包，您就可以同时为所有 FTD 型号排队和调用升级。 以前，您需要选择一个升级包，然后使用该包选择要升级的设备。这意味着只有共享升级包时，您才能同时升级多台设备。例如，您可以同时升级两台 Firepower 2100 系列设备，但不能同时升级 Firepower 2100 系列和 Firepower 1000 系列。

表 *7:* 版本 *6.7.0* 功能

特性	说明
改进了 FTD 升级状态报告和取消/重试选项。	您现在可以在“设备管理”页面上查看 FTD 设备升级和就绪性检查的状态，以及升级成功/失败的 7 天历史记录。消息中心还提供增强的状态和错误消息。 在“设备管理”和“消息中心”中点击一下即可访问新的“升级状态”弹出窗口，其中显示详细的升级信息，包括剩余百分比/时间、特定升级阶段、成功/失败数据、升级日志等。 此外，在此弹出窗口中，您可以手动取消失败或正在进行的升级（**取消升级**），或重试失败的升级（**重试升级**）。取消升级会将设备恢复到升级前的状态。 **注释** 要能够手动取消或重试失败的升级，必须禁用新的自动取消选项：**升级失败时自动取消并回滚到以前的版本**。启用选项后，设备会在升级失败时自动恢复到升级前的状态。 补丁不支持自动取消。在高可用性或可扩展性部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。 新增/修改的屏幕： • **系统** > **更新** > **产品更新** > **可用更新** > **安装**FTD 升级包的 图标 • **设备** > **设备管理** > **升级** • **消息中心** > **任务** 新的 FTD CLI 命令： • **show upgrade status detail** • **show upgrade status continuous** • **show upgrade status** • **upgrade cancel** • **upgrade retry**
升级会删除 PCAP 文件以节省磁盘空间。	升级现在会删除本地存储的 PCAP 文件。要升级，您必须拥有足够的可用磁盘空间，否则升级会失败。

表 *8:* 版本 *6.6.0* 功能

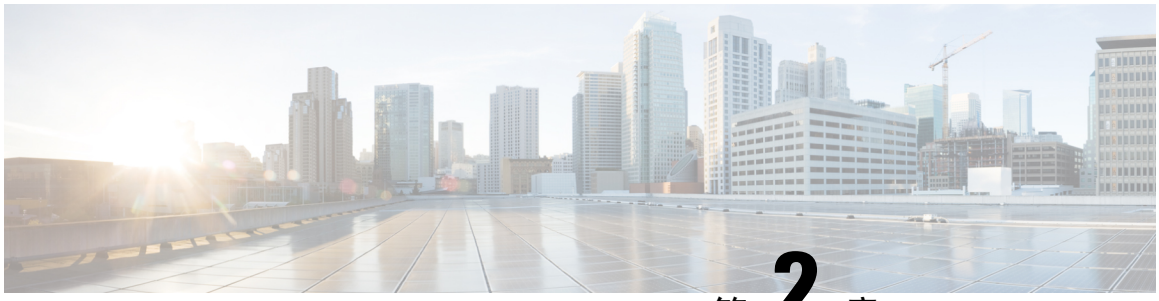
特性	说明
从内部 Web 服务器获取设备升级包。	设备现在可以从您自己的内部 Web 服务器而不是从 FMC 获取升级包。这在FMC及其设备之间的带宽有限时尤其有用。它还可以节省 FMC 上的空间。 新增/修改的屏幕：**系统 (System) > 更新 (Updates) > 上传更新 (Upload Update)** 按钮 > **指定软件更新源 (Specify software update source)** 选项
升级会推迟计划任务。	FMC升级流程现在会推迟计划任务。任何计划在升级期间开始的任务都将在升级后重新启动后五分钟开始。 **注释** 在开始任何升级之前，您仍必须确保运行任务已完成。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。 请注意，从受支持的版本进行的所有升级均支持此功能。这包括 6.4.0.10 及更高版本补丁、版本 6.6.3 及更高维护版本以及版本 6.7.0+。从不支持的版本升级到支持的版本时，不支持此功能。

表 *9:* 版本 *6.4.0* 功能

特性	说明
升级会推迟计划任务。	FMC升级流程现在会推迟计划任务。任何计划在升级期间开始的任务都将在升级后重新启动后五分钟开始。 **注释** 在开始任何升级之前，您仍必须确保运行任务已完成。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。 请注意，从受支持的版本进行的所有升级均支持此功能。这包括 6.4.0.10 及更高版本补丁、版本 6.6.3 及更高维护版本以及版本 6.7.0+。从不支持的版本升级到支持的版本时，不支持此功能。

表 *10:* 版本 *6.2.3* 的功能

特性	说明
升级前，将升级包复制到托管设备。	现在，您可以在运行实际升级之前，将升级软件包从 FMC 复制（或推送）到受管设备。这是非常有用的，因为您可以在“升级维护”窗口之外的低带宽使用时间内推送。 当您推送到高可用性、集群或可堆叠设备时，系统首先将升级软件包发送到活动/主要/首要设备，然后再发送到备用/数据/辅助设备。 新增/修改的屏幕： **系统 (System)** > **更新 (Updates)**



第 2 章

规划升级

- 升级规划阶段， 第 9 页
- 当前版本和型号信息， 第 10 页
- 升级路径， 第 11 页
- 无响应的升级， 第 31 页
- 时间和磁盘空间测试， 第 32 页
- 下载升级包， 第 33 页
- 上传 的 Firepower 软件升级包， 第 37 页
- Firepower 软件就绪性检查， 第 40 页

升级规划阶段

认真规划和准备可以帮助您避免失误。此表总结了升级规划流程。有关详细核对表和程序，请参阅相应升级或配置指南中的升级章节。

表 *11:* 升级规划阶段

规划阶段	包括
规划和可行性	评估部署。 计划升级路径。 阅读所有升级指南和计划配置更改。 检查设备访问。 检查带宽。 安排维护窗口。
备份	备份软件。 在 Firepower 4100/9300 上备份 FXOS。 备份适用于 ASA FirePOWER 的 ASA。

规划阶段	包括
升级程序包	从 Cisco 下载升级包。 将升级包上传到系统。
关联升级	升级虚拟部署中的虚拟主机。 升级 Firepower 4100/9300 的 FXOS。 升级适用于 ASA FirePOWER 的 ASA。
最终检查	检查配置。 检查 NTP 同步。 检查硬盘空间。 部署配置。 运行就绪性检查。 检查正在运行的任务。 检查部署运行状况和通信。

当前版本和型号信息

使用这些命令查找部署的当前版本和型号信息，

表 12:

组件	信息
Firepower 管理中心	在 FMC 上，选择**帮助 (Help)** > **关于 (About)**。
Firepower 托管设备	在 FMC 上，选择**设备 (Devices)** > **设备管理 (Device Management)**。
适用于 Firepower 4100/9300 的 FXOS	Firepower 机箱管理器：选择**概述 (Overview)**。 FXOS CLI：对于版本，请使用 **show version** 命令。对于型号，请输入 **scope chassis 1**，然后输入 **show inventory**。
具备 FirePOWER 服务的 ASA 的 ASA 操作系统	在 ASA CLI 上，使用 **show version** 命令。
虚拟托管环境	请参阅您的虚拟托管环境的相关文档。

升级路径

您的升级路径是您要升级的内容和时间的详细计划，包括虚拟托管环境和设备操作系统。您必须始终保持硬件、软件、操作系统和托管兼容性。

提示 本指南涵盖了 Firepower 7.0.x 及更早版本。请参阅本指南适用对象，第 1 页

当前版本是什么？

升级任何 Firepower 设备之前，请先确定部署的当前状态。除了当前版本和型号信息之外，请确定您的设备是否配置为高可用性/可扩展性，以及是否将它们作为 IPS、防火墙等进行被动部署。

请参阅当前版本和型号信息，第 10 页。

要升级到哪个版本？

既然您已经知道了自己当前的版本，请确保可以升级到想到的版本：

- 您的部署能否运行目标 Firepower 版本？
- 您的设备是否需要单独的操作系统升级才能运行目标 Firepower 版本？您的设备能否运行目标操作系统？
- 您的虚拟设备是否需要升级托管环境才能运行目标 Firepower 版本？

有关所有这些问题的答案，请参阅以下之一：

- Cisco Secure Firewall Management Center 兼容性指南
- Cisco Secure Firewall Threat Defense 兼容性指南
- Cisco Firepower 典型设备兼容性指南

如何达成目标？

确定设备可以运行目标版本后，请确保可以直接升级：

- 是否可以直接升级 Firepower 软件？
- Firepower 4100/9300 是否可以直接升级 FXOS？
- 具有 FirePOWER 服务的 ASA，是否可以直接升级 ASA？

有关所有这些问题的答案，请参阅本指南中提供的升级路径。

提示 需要中间版本的升级路径可能非常耗时。尤其是在大型 Firepower 部署中，您必须备用 FMC 和设备升级，请考虑重新映像旧设备而不是升级。首先，从 FMC 中删除设备。然后，升级 FMC，重新映像设备，并将其重新添加到 FMC。

是否可以保持部署兼容性？

您必须始终保持硬件、软件和操作系统兼容性：

- 我能否在 FMC 及其托管设备之间保持 Firepower 版本兼容性：Cisco Secure Firewall Management Center 兼容性指南。
- 我能否在 Firepower 4100/9300 上保持与逻辑设备的 FXOS 兼容性：Cisco Firepower 4100/9300 FXOS 兼容性。
- 具有 FirePOWER 服务的 ASA，我能否维护 ASA 与 ASA FirePOWER 模块的兼容性：Cisco Secure Firewall ASA 兼容性。

升级路径：Firepower 管理中心

此表提供了 FMC 的升级路径，包括 FMCv。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

注释 如果当前版本是在目标版本之后的某个日期发布的，则您可能无法如表中所列进行升级。在这些情况下，升级会快速失败并显示错误，说明两个版本之间存在数据存储不兼容问题。 当前和目标版本的会列出任何特定限制。

表 *13: FMC* 直接升级

当前版本	目标版本
7.0.0 7.0.x 最后支持 FMC 1000、2500 和 4500	→任何更高版本的 7.0.x 维护版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本

当前版本	目标版本
6.6.0 6.6.x 最后支持 FMC 2000 和 4000。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本 **注：**由于数据存储不兼容，您无法从版本 6.6.5+ 升级到版本 6.7.0。我们建议您直接升级到版本 7.0.0+。
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0 最后支持 FMC 750、1500 和 3500。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0
6.2.3	以下项中的任一个： →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3

当前版本	目标版本
6.2.1	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0
6.0.0	以下项中的任一个： → 6.0.1 需要预安装包：Firepower 系统发行说明版本 6.0.1 预安装。
5.4.1.1	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

升级路径：带有 FTD 逻辑设备和 FMC 的

此表提供由 Firepower 管理中心管理的具有 FTD 逻辑设备的 Firepower 4100/9300 的升级路径。

注释 如果要使用在单独的模块上运行的 FTD 和 ASA 逻辑设备升级 Firepower 9300 机箱，请参阅Cisco Firepower 4100/9300 升级指南，Firepower 6.0.1 – 7.0.x 或 ASA 9.4(1) – 9.16(x) 包括 FXOS 1.1.1 – 2.10.1。

在左列中查找您的当前版本组合。您可以升级到右列中列出的任何版本组合。这是一个多步骤过程：首先升级 FXOS，然后升级逻辑设备。

请注意，此表仅列出思科的特殊限定版本组合。由于您必须首先升级 FXOS，因此您将短暂运行受支持（但不推荐）的组合，其中 FXOS 位于逻辑设备之前。如需了解最小内部版本和其他详细的兼容性信息，请参阅Cisco Firepower 4100/9300 FXOS 兼容性。



注释 对于 FXOS 的早期版本，您必须升级到当前版本与目标版本之间的所有中间版本。到达 FXOS 2.2.2 后，您的升级选项会更广泛。

表 *14:* 升级路径：采用 *FTD* 逻辑设备的 *Firepower 4100/9300*

当前版本	目标设备
具有 FTD 6.7.0/6.7.x 的 FXOS 2.9.1	→ 具有 FTD 7.0.0/7.0.x 的 FXOS 2.10.1
具有 FTD 6.6.0/6.6.x 的 FXOS 2.8.1	以下项中的任一个： → 具有 FTD 7.0.0/7.0.x 的 FXOS 2.10.1 → 具有 FTD 6.7.x 的 FXOS 2.9.1
具有 FTD 6.5.0 的 FXOS 2.7.1	以下项中的任一个： → 具有 FTD 7.0.0/7.0.x 的 FXOS 2.10.1 → 具有 FTD 6.7.0/6.7.x 的 FXOS 2.9.1 → 具有 FTD 6.6.0/6.6.x 的 FXOS 2.8.1
具有 FTD 6.4.0 的 FXOS 2.6.1	以下项中的任一个： → 具有 FTD 7.0.0/7.0.x 的 FXOS 2.10.1 → 具有 FTD 6.7.0/6.7.x 的 FXOS 2.9.1 → 具有 FTD 6.6.0/6.6.x 的 FXOS 2.8.1 →具有 FTD 6.5.0 的 FXOS 2.7.1
具有 FTD 6.3.0 的 FXOS 2.4.1	以下项中的任一个： → 具有 FTD 6.7.0/6.7.x 的 FXOS 2.9.1 → 具有 FTD 6.6.0/6.6.x 的 FXOS 2.8.1 →具有 FTD 6.5.0 的 FXOS 2.7.1 →具有 FTD 6.4.0 的 FXOS 2.6.1

当前版本	目标设备
具有 FTD 6.2.3 的 FXOS 2.3.1	以下项中的任一个： → 具有 FTD 6.6.0/6.6.x 的 FXOS 2.8.1 →具有 FTD 6.5.0 的 FXOS 2.7.1 →具有 FTD 6.4.0 的 FXOS 2.6.1 →具有 FTD 6.3.0 的 FXOS 2.4.1
具有 FTD 6.2.2 的 FXOS 2.2.2	以下项中的任一个： →具有 FTD 6.4.0 的 FXOS 2.6.1 →具有 FTD 6.3.0 的 FXOS 2.4.1 → 具有 FTD 6.2.3 的 FXOS 2.3.1
具有 FTD 6.2.0 的 FXOS 2.2.2	以下项中的任一个： →具有 FTD 6.4.0 的 FXOS 2.6.1 →具有 FTD 6.3.0 的 FXOS 2.4.1 → 具有 FTD 6.2.3 的 FXOS 2.3.1 →具有 FTD 6.2.2 的 FXOS 2.2.2
具有 FTD 6.2.0 的 FXOS 2.2.1	→ 具有 FTD 6.2.0 的 FXOS 2.2.2（仅升级 FXOS） 另一种选择是使用 FTD 6.2.2 升级到 FXOS 2.2.2，这是推荐的组合。但是，如果您计划进一步升级您的部署，请不要打扰。现在您正在运行 FXOS 2.2.2，您可以使用 FTD 6.4.0 升级到 FXOS 2.6.1。
具有 FTD 6.2.0 的 FXOS 2.1.1	→具有 FTD 6.2.0 的 FXOS 2.2.1（仅升级 FXOS）
具有 FTD 6.1.0 的 FXOS 2.0.1	→ 具有 FTD 6.2.0 的 FXOS 2.1.1
具有 FTD 6.0.1 的 FXOS 1.1.4	→具有 FTD 6.1.0 的 FXOS 2.0.1

使用集群或 HA 对中的 FTD 逻辑设备升级 FXOS

在 Firepower 管理中心部署中，您可以将集群和高可用性 FTD 逻辑设备作为一个单元进行升级。然而，你可以单独在每个机箱上升级 FXOS。

表 *15: FXOS + FTD* 升级顺序

部署	升级顺序
独立设备 集群，同一机箱上的设备（仅限 Firepower 9300）	**1.** 升级 FXOS。 **2.** 升级 FTD。
低间断性	要最大限度地减少中断，请始终升级备用设备。 **1.** 在备用设备上升级 FXOS。 **2.** 切换角色。 **3.** 新的备用设备上升级 FXOS。 **4.** 升级 FTD。
集群，不同机箱上的设备 (6.2+)	为了最大限度地减少中断，请始终升级全数据单元机箱。例如，对于双机箱集群： **1.** 在全数据单元机箱上升级 FXOS。 **2.** 将控制模块切换到您刚刚升级的机箱。 **3.** 在全新全数据单元机箱上升级 FXOS。 **4.** 升级 FTD。

对于旧版本，无中断升级有一些额外要求。

表 *16:* 较旧版本的无中断升级

场景	详细信息
升级高可用性或集群设备，您当前正在运行以下任何设备： • FXOS 1.1.4.x 至 2.2.1.x • FXOS 2.2.2.17 至 FXOS 2.2.2.68 • FXOS 2.3.1.73 至 FXOS 2.3.1.111 具有： • FTD 6.0.1 至 6.2.2.x	流负载分流：由于在流负载分流功能中修复了漏洞，因此 FXOS 和 FTD 的一些组合不支持流负载分流；请参阅 Cisco Firepower 兼容性指南。执行无中断升级要求您始终运行兼容的组合。 如果您的升级路径包括将 FXOS 升级到 2.2.2.91、2.3.1.130 或更高版本（包括 FXOS 2.4.1. x、2.6.1. x 等），请使用此路径： 1. 将 FTD 升级到 6.2.2.2 或更高版本。 2. 将 FXOS 升级到 2.2.2.91、2.3.1.130 或更高版本。 3. 将 FTD 升级到您的最终版本。 例如，如果您运行的是 2.2.2.17/FTD 6.2.2.0，并且要升级到 FXOS 2.6.1/FTD 6.4.0，则可以执行以下操作： 1. 将 FTD 升级到 6.2.2.5。 2. 将 FXOS 升级到 2.6.1。 3. 将 FTD 升级到 6.4.0。
将高可用性设备升级到 FTD 版本 6.1.0	需要预安装软件包。有关详细信息，请参阅 Firepower 系统发行说明 6.1.0 版预安装包。

降级说明

官方不支持 FXOS 映像降级。思科唯一支持的 FXOS 映像版本降级方法是对设备执行完整的重新映像。

升级路径：其他 Firepower 威胁防御 设备

下表提供了由 FMC 管理的 FTD 设备的升级路径，您无需在其中更新操作系统：Firepower 1000/2100 系列、ASA 5500-X 系列、ISA 3000 和 Firepower 虚拟威胁防御。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

表 *17:* 升级路径：带有 *FMC* 的 *Firepower 1000/2100* 系列、*ASA 5500-X* 系列、*ISA 3000* 和 *Firepower* 虚拟威胁防御

当前版本	目标版本
7.0.0 7.0.x ASA 5508-X 和 5516-X 的最后 FTD 支持。	→任何更高版本的 7.0.x 维护版本

当前版本	目标版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本
6.6.0 6.6.x ASA 5525-X，5545-X 和 5555-X 的最后 FTD 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0 对 ASA 5515-X 最后的 FTD 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0
6.2.3 ASA 5506-X 系列的最新 FTD 支持。	以下项中的任一个： →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0

当前版本	目标版本
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 仅 Firepower 2100 系列。	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	→ 6.1.0

升级路径：Firepower 7000/8000 系列

此表提供了由 FMC 管理的 Firepowert 7000/8000 系列设备的升级路径。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

表 *18:* 升级路径：带有 *FMC* 的 *Firepower 7000/8000* 系列

当前版本	目标版本
6.4.0	无。 版本 6.4.0 是 Firepower 7000/8000 系列设备的最后一个主要版本。

当前版本	目标版本
6.3.0	以下项中的任一个： → 6.4.0
6.2.3	以下项中的任一个： → 6.4.0 → 6.3.0
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 此平台上不支持。	-
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0
6.0.0	以下项中的任一个： → 6.0.1
5.4.0.2	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

升级路径： ASA FirePOWER

此表提供由 FMC 管理的 ASA FirePOWER 模块 的升级路径。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

如果需要，您还可以升级 ASA。ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但通过升级，您可以利用新功能和已解决的问题。有关ASA升级路径，请参阅升级路径：适用于 ASA FirePOWER 的 ASA ， 第 25 页。

表 *19:* 升级路径：带有 *FMC* 的 *ASA FirePOWER*

当前版本	目标版本
7.0.0 7.0.x 在任何平台上最后支持的 ASA FirePOWER。	→任何更高版本的 7.0.x 维护版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本
6.6.0 6.6.x ASA 5525-X，5545-X 和 5555-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0 ASA 5585-X 系列和 ASA 5515-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0

当前版本	目标版本
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0
6.2.3 ASA 5506-X 系列和 ASA 5512-X 的最后 ASA FirePOWER 支持。	以下项中的任一个： →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3
6.2.1 此平台上不支持。	-
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0

当前版本	目标版本
6.0.0	以下项中的任一个： → 6.0.1
5.4.0.2 或 5.4.1.1	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

升级 ASA

ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但通过升级，您可以利用新功能和已解决的问题。有关详细的兼容性信息，请参阅 Cisco Secure Firewall ASA 兼容性。

即使已配置ASA集群或故障转移对，也应在每个设备上独立升级ASA。究竟何时升级ASA FirePOWER模块（在ASA重新加载之前或之后）取决于您的部署。下表概述了独立和HA/可扩展性部署的ASA升级顺序。有关详细说明，请参阅升级 ASA，第 87 页。

表 *20: ASA + ASA FirePOWER* 升级顺序

ASA 部署	升级顺序
独立设备	**1.** 升级 ASA，包括重新加载。 **2.** 升级 ASA FirePOWER。
ASA 故障转移：主用/备用	始终升级备用设备。 **1.** 在备用设备上升级 ASA，但不重新加载。 **2.** 在备用设备上升级 ASA FirePOWER。 **3.** 在备用设备上重新加载 ASA。 **4.** 故障转移。 **5.** 在新的备用设备上升级 ASA。 **6.** 在新的备用设备上升级 ASA FirePOWER。 **7.** 在新的备用备用上重新加载 ASA。

ASA 部署	升级顺序
ASA 故障转移：主用/主用	在未升级的设备上使两个故障转移组均处于活动状态。 **1.** 使两个故障转移组在主设备上均处于活动状态。 **2.** 在辅助设备上升级 ASA，但不重新加载。 **3.** 在辅助设备上升级 ASA FirePOWER。 **4.** 在辅助设备上重新加载 ASA。 **5.** 使两个故障转移组在辅助设备上均处于活动状态 **6.** 在主设备上升级 ASA，但不重新加载。 **7.** 在主设备上升级 ASA FirePOWER。 **8.** 在主设备上重新加载 ASA。
ASA 集群	升级前，在每个设备上禁用集群。一次升级一个设备，将控制单元留到最后。 **1.** 在从数据单元上禁用集群。 **2.** 在该数据单元上升级 ASA，但不重新加载。 **3.** 在设备上升级 ASA FirePOWER。 **4.** 重新加载 ASA。 **5.** 重新启用集群。等待单元重新加入集群。 **6.** 对每个从属数据单元上述操作。 **7.** 在控制单元上禁用集群。等待新的控制接管。 **8.** 在以前的控制单元上升级 ASA，但不重新加载。 **9.** 升级前控制单元上的 ASA FirePOWER。 **10.** 重新启用集群。

升级路径：适用于 ASA FirePOWER 的 ASA

下表提供具有 FirePOWER 服务的 ASA 上的 ASA 升级路径。 ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但通过升级，您可以利用新功能和已解决的问题。

在左列中查找您的当前 ASA 版本。您可以直接升级到列出的目标版本。建议的版本以**粗体显示**。

表 ***21:*** 升级路径：适用于 ***ASA FirePOWER*** 的 ***ASA***

当前版本	目标版本
9.15(x) Firepower 版本 7.0.x 在任何平台上的最后 ASA FirePOWER 支持。	→ **9.16(x)**
9.14(x) ASA 5525-X，ASA 5545-X和ASA 5555-X（含 Firepower 版本 6.6.x）的最后 ASA FirePOWER 支持。	以下项中的任一个： → **9.16(x)** → **9.15(x)**
9.13(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)**
9.12(x) ASA 5515-X 和 ASA 5585-X 的最新 ASA FirePOWER 最后支持，使用 Firepower 版本 6.4.0。	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)**
9.10(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x)

当前版本	目标版本
9.9(x) ASA 5506-X 系列和 ASA 5512-X 的最后一个 ASA FirePOWER Firepower 支持，使用 Firepower 版本 6.2.3。	以下项中的任一个： → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x)
9.8(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**
9.7(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)**

当前版本	目标版本
9.6(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.5(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.4(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

当前版本	目标版本
9.3(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)
9.2(x)	以下项中的任一个： → **9.16(x)** → **9.15(x)** → **9.14(x)** → **9.13(x)** → **9.12(x)** → 9.10(x) → 9.9(x) → **9.8(x)** → 9.6(x)

升级路径：NGIPSv

此表提供由 FMC 管理的 NGIPSv 的升级路径。

在左列中查找当前版本。您可以直接升级到右列中列出的任何版本。

表 *22:* 升级路径：带有 *FMC* 的 *NGIPSv*

当前版本	目标版本
7.0.0 7.0.x 最后的 NGIPSv 支持。	→任何更高版本的 7.0.x 维护版本

当前版本	目标版本
6.7.0 6.7.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.x 以后的任何维护版本
6.6.0 6.6.x	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.x 以后的任何维护版本
6.5.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本
6.4.0	以下项中的任一个： →7.0.0 或任何 7.0.x 维护版本 →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0
6.3.0	以下项中的任一个： →6.7.0 或任何 6.7.x 维护版本 →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0
6.2.3	以下项中的任一个： →6.6.0 或任何 6.6.x 维护版本 → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	以下项中的任一个： → 6.4.0 → 6.3.0

当前版本	目标版本
6.2.1 此平台上不支持。	-
6.2.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	以下项中的任一个： → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	以下项中的任一个： → 6.1.0
6.0.0	以下项中的任一个： → 6.0.1
5.4.1.1	以下项中的任一个： → 6.0.0 需要预安装包：FireSIGHT 系统发行说明版本 6.0.0 预安装。

无响应的升级

请勿在升级期间进行或部署配置更改。即使系统显示为非活动状态，也不要在升级过程中手动重新启动或关闭。您可以将系统置于不可用状态并要求重新映像。

无响应 FMC 或经典设备 升级

请勿重启正在进行的升级。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

无响应 FTD 升级

对于主要和维护升级，您可以手动取消失败或正在进行的升级，并重试失败的升级。在FMC上，使用“升级状态”(Upgrade Status) 弹出窗口，该窗口可从“设备管理”(Device Management) 页面和消息中心进行访问。您还可以使用 FTD CLI。



注释 默认情况下，在升级失败时FTD自动将其恢复到升级前的状态（“自动取消”）。要能够手动取消或重试失败的升级，请在启动升级时禁用自动取消选项。补丁不支持自动取消。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。

补丁或 6.6 及更早版本的升级不支持此功能。

时间和磁盘空间测试

出于参考目的，我们为 FMC 和设备软件升级提供内部时间和磁盘空间测试报告。 有关实际报告，请参阅目标版本的发行说明。

时间测试

我们会报告在特定平台/系列上测试的所有软件升级中最慢的测试时间。如下表所述，由于多种原因，您的升级所需的时间可能需要比所述的时间更长。我们建议您跟踪并记录自己的升级时间，以便将其用作未来的基准。



注意 请勿在升级期间进行或部署配置更改。即使系统显示为非活动状态，也不要手动重新启动或关闭。在大多数情况下，请勿重启正在进行的升级。您可以将系统置于不可用状态并要求重新映像。如果您遇到升级问题，包括升级失败或设备无响应，请参阅无响应的升级，第 31 页。

表 *23*: 软件升级的时间测试条件

情况	详细信息
部署	设备升级时间来自FMC部署中的测试。在类似条件下，远程和本地管理设备的原始升级时间相似。
版本	对于主要和维护版本，我们会测试所有先前符合条件的主版本的升级。对于补丁，我们会从基础版本测试升级。如果升级跳过版本，则升级时间通常会增加。
模式	大多数情况下，我们测试每个系列中的最低端型号，有时会对系列中的多个型号进行测试。
虚拟设备	我们使用内存和资源的默认设置进行测试。但请注意，虚拟部署中的升级时间很大程度上依赖于硬件。

情况	详细信息
高可用性/可扩展性	除非另有说明，否则我们将在独立设备上进行测试。 在高可用性或集群配置中，设备一次升级一个可保持操作的连续性，每个设备在升级时以维护模式运行。因此，升级一个设备对或整个集群所需的时间比升级独立设备所需的时间长。
配置	我们对具有最小配置和流量负载的设备进行了测试。 升级时间会随着配置的复杂性、事件数据库的大小以及这些事物是否/如何受到升级的影响而增加。例如，如果您使用大量访问控制规则并且升级需要对这些规则的存储方式进行后端更改，则升级可能需要更长时间。
组件	我们仅报告软件升级本身和随后的重启时间。这不包括操作系统升级、传输升级包、就绪性检查、VDB 和入侵规则 (SRU/LSP) 更新或部署配置的时间。

磁盘空间测试

我们会报告在特定平台/系列上测试的所有软件升级中使用最多磁盘空间的升级。这包括将升级包复制到设备所需的空间。

我们还报告了设备升级包在 FMC 上所需的空间（在 /Volume 或 /var 中）。如果您有 FTD 升级包的内部服务器，或者您正在使用 FDM，请忽略这些值。

当我们报告特定位置（例如，/var 或 /ngfw）的磁盘空间估计时，我们会报告该位置中安装的分区的磁盘空间估计值。在某些平台上，这些位置可能在同一个分区上。

如果可用磁盘空间不足，会导致升级失败。

表 *24:* 检查磁盘空间

平台	命令
FMC	选择**系统 (System)** > **监控 (Monitoring)** > **统计信息 (Statistics)**，然后选择 FMC。在磁盘使用情况下，展开“按分区”(By Partition) 详细信息。
具有 FTD的 FMC	选择**系统 (System)** > **监控 (Monitoring)** > **统计信息 (Statistics)**，然后选择您要检查的设备。在磁盘使用情况下，展开“按分区”(By Partition) 详细信息。

下载升级包

在开始升级之前，请从思科支持和下载站点下载升级包。根据具体的升级，您应将软件包放在本地计算机或设备可以访问到的服务器上。本指南中的各个检查清单和程序说明了您的选择。

注释 下载需要登录 Cisco.com，并签署服务合同。

Firepower 软件包

思科支持和下载站点上可以获取升级包。

- Firepower 管理中心，包括 Firepower Management Center Virtual：https://www.cisco.com/go/firepower-software
- Firepower 威胁防御 (ISA 3000)： https://www.cisco.com/go/isa3000-software
- Firepower 威胁防御（所有其他型号，包括 Firepower Threat Defense Virtual）：https://www.cisco.com/go/ftd-software
- Firepower 7000 系列： https://www.cisco.com/go/7000series-software
- Firepower 8000 系列： https://www.cisco.com/go/8000series-software
- 具备 FirePOWER 服务的 ASA（ASA 5500-X 系列）： https://www.cisco.com/go/asa-firepower-sw
- 具备 FirePOWER 服务的 ASA (ISA 3000)： https://www.cisco.com/go/isa3000-software
- NGIPSv： https://www.cisco.com/go/ngipsv-software

要查找升级包，请选择或搜索您的设备型号，然后浏览至当前版本的软件下载页面。列出了可用的升级包以及安装包、修复程序和其他适用的下载。

提示 可访问互联网的 Firepower 管理中心 可以直接从思科下载特定的版本，在发布后的一段时间内即可手动下载。延迟的长度取决于版本类型、版本采用情况和其他因素。

您对系列或系列中的所有型号使用相同的升级包。升级软件包文件名反映平台、软件包类型（升级、补丁、修复程序）和软件版本。 维护版本使用升级包类型。

例如：

- 软件包：`Cisco_Firepower_Mgmt_Center_Upgrade--999.sh.REL.tar`
- 平台：Firepower 管理中心
- 包类型：升级
- 版本和内部版本：-999
- 文件扩展名：sh.REL.tar

因此，系统可以证实您使用的是正确的文件，来自版本 6.2.1+ 的升级包是签名的 tar 档案 (.tar)。不要解压签名的 (.tar) 包。 并且，请勿通过邮件来传输升级包。

注释 上传签名的升级包后，Firepower管理中心GUI可能需要几分钟才能加载，因为系统需要对包进行验证。要加快显示速度，可删除不再需要的这些软件包。

Firepower 软件升级包

表 25:

平台	版本	数据包
FMC/FMCv	6.3.0+	Cisco_Firepower_Mgmt_Center
	5.4.0 至 6.2.3	Sourcefire_3D_Defense_Center_S3
Firepower 1000 系列	任意	Cisco_FTD_SSP-FP1K
Firepower 2100 系列	任意	Cisco_FTD_SSP-FP2K
Firepower 4100/9300	任意	Cisco_FTD_SSP
具备 FTD 的 ASA 5500-X 系列 使用 FTD 的 ISA 3000 FTDv	任意	Cisco_FTD
Firepower 7000/8000 系列 AMP 型号	6.3.0 至 6.4.0	Cisco_Firepower_NGIPS_Appliance
	5.4.0 至 6.2.3	Sourcefire_3D_Device_S3
ASA FirePOWER	任意	Cisco_Network_Sensor
NGIPSv	6.3.0+	Cisco_Firepower_NGIPS_Virtual
	6.2.2 至 6.2.3	Sourcefire_3D_Device_VMware
	5.4.0 至 6.2.0	Sourcefire_3D_Device_Virtual64_VMware

FXOS 软件包

思科支持和下载站点 上提供适用于 Firepower 4100/9300 的 FXOS 软件包。

- Firepower 4100 系列：http://www.cisco.com/go/firepower4100-software
- Firepower 9300：http://www.cisco.com/go/firepower9300-software

要查找 FXOS 软件包，请选择或搜索您的 Firepower 设备型号，然后浏览至目标版本的 Firepower 可扩展操作系统下载页面。

注释 如果计划使用 CLI 升级 FXOS，请将升级软件包复制到 Firepower 4100/9300 可以使用 SCP、SFTP、TFTP 或 FTP 访问的服务器。

表 *26:* 适用于 ***Firepower 4100/9300*** 的 ***FXOS*** 软件包

软件包类型	数据包
FXOS 映像	fxos-k9.版本**.SPA**
恢复 (kickstart)	fxos-k9-**kickstart**.版本**.SPA**
恢复（管理器）	fxos-k9-**manager**.版本**.SPA**
恢复（系统）	fxos-k9-**system**.版本**.SPA**
MIB	fxos-**mibs**-fp9k-fp4k.版本**.zip**
固件：Firepower 4100 系列	fxos-k9-fpr4k-**firmware**.版本**.SPA**
固件：Firepower 9300	fxos-k9-fpr9k-**firmware**.版本**.SPA**

ASA 软件包

ASA 软件在 思科支持和下载站点 上可用。

- 具备 FirePOWER 服务的 ASA（ASA 5500-X 系列）： https://www.cisco.com/go/asa-firepower-sw
- 具备 FirePOWER 服务的 ASA (ISA 3000)： https://www.cisco.com/go/isa3000-software

要查找 ASA 软件，请选择或搜索您的 Firepower 设备型号，然后浏览至相应的下载页面并选择一个版本。

注释 如果您正在使用 ASDM 升级向导，则不必预先下载。否则，请下载到本地计算机。对于 CLI 升级，您应将软件复制到设备可通过 ASA **copy** 命令支持的任何协议（包括 HTTP、FTP 和 SCP）来访问的服务器。

表 *27: ASA* 软件

下载页面	软件类型	数据包
自适应安全设备 (ASA) 软件	ASA 和 ASDM 升级	asa*version*-**lfbff-k8.SPA** 对于 ASA 5506-X、ASA 5508-X、ASA 5516-X 和 ISA 3000
		asa*version*-**smp-k8.bin** 对于 ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X 和 ASA 5585-X
自适应安全设备 (ASA) 设备管理器	仅 ASDM 升级	asdm-*version***.bin**
自适应安全设备 REST API 插件	ASA REST API	asa-restapi-*version*-**lfbff-k8.SPA**

上传 的 Firepower 软件升级包

要升级 Firepower 软件，必须在设备上安装软件升级包。

上传到 Firepower 管理中心

使用此程序可将用于其自身及其管理的设备的 Firepower 软件升级软件包手动上传到 Firepower 管理中心。

开始之前

如果您升级的是高可用性对中的备用 Firepower 管理中心，请暂停同步。

在 FMC 高可用性部署中，必须将 FMC 升级软件包上传到两个对等设备，在将软件包传输到备用设备之前暂停同步。要限制 HA 同步的中断，您可以在升级准备阶段将数据包传输到主用对等设备，并在暂停同步后将其作为实际升级过程的一部分传输到备用对等设备。

步骤 1 在 Firepower 管理中心Web 界面上，选择**系统** > **更新**。

步骤 2 点击**上传更新**。

提示 稍等片刻，当版本可以手动下载后，选择可以由Firepower管理中心 直接下载的升级包。延迟的长度取决于版本类型、版本采用情况和其他因素。如果您可以Firepower 管理中心访问互联网，则可以点击**下载更新 (Download Updates)** 下载适用于您的部署的所有符合条件的软件包，并根据需要下载最新的 VDB。

步骤 3 （版本 6.6.0+）对于**操作**，请点击**上传本地软件更新包**单选按钮。

步骤 4 点击**选择文件**。

步骤 5 浏览到升级包并点击**上传 (Upload)**。

上传到内部服务器（带有 FMC 的版本 6.6.0+ FTD）

从版本 6.6.0 开始，Firepower 威胁防御设备可以从内部 Web 服务器而不是从 FMC 获取升级软件包。这在 FMC 及其设备之间的带宽有限时尤其有用。它还可以节省 FMC 的空间。

注释 此功能仅支持运行版本 6.6.0+ 的 FTD 设备。它不支持升级到版本 6.6.0，也不支持 FMC 或经典设备。

要配置此功能，请保存指向升级包在 Web 服务器上的位置的指针 (URL)。然后，升级过程将从 Web 服务器而不是 FMC 获取升级软件包。或者，您可以使用 FMC 在升级之前复制软件包。

对于每个 FTD 升级包重复上述过程。每个升级包只能配置一个位置。

开始之前

- 从 思科支持和下载站点 下载相应的升级软件包，并将其复制到 FTD 设备可以访问的内部 Web 服务器。
- 对于安全 Web 服务器 (HTTPS)，获取服务器的数字证书（PEM 格式）。您应该能够从服务器的管理员处获取证书。您还可以使用浏览器或 OpenSSL 等工具查看服务器的证书详细信息，以及导出或复制证书。

步骤 1 在 FMC Web 界面上，选择 **系统** > **更新**。

步骤 2 点击**上传更新**。

选择此选项，即使您不会上传任何内容。下一页将提示您输入 URL。

步骤 3 对于**操作**，请点击**指定软件更新源**单选按钮。

步骤 4 输入升级软件包的**源 URL**。

提供协议 (HTTP/HTTPS) 和完整路径，例如：

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

升级软件包文件名反映平台、软件包类型（升级、补丁、修复程序）和要升级到的Firepower版本。确保输入正确的文件名。

步骤 5 对于 HTTPS 服务器，请提供 **CA 证书**。

这是您之前获得的服务器数字证书。复制整个文本块，包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。

步骤 6 点击**保存**。

您将返回到“产品更新”页面。上传的升级软件包和升级软件包 URL 一起列出，但有不同的标签。

复制到托管设备

要升级 Firepower 软件，升级软件包必须位于设备上。如果受支持，我们建议您在启动设备升级之前，使用此程序将软件包复制（推送）到托管设备。

注释 如果使用的是 Firepower 4100/9300，我们建议（有时需要）在开始所需的随附 FXOS 升级之前复制 Firepower Threat Defense 升级软件包。

支持情况因 Firepower 版本而异：

- 版本 6.2.2 及更早版本不支持预升级复制。

  当您开始设备升级时，系统会将升级包从 Firepower 管理中心 复制到设备作为第一个任务。

- 版本 6.2.3 增加了从手动将升级软件包从 Firepower 管理中心 复制到设备的功能。

  这样可以减少升级维护窗口的时长。

- 版本 6.6.0 增加了将升级软件包从内部 Web 服务器手动复制到 Firepower Threat Defense 设备的功能。

  如果 Firepower 管理中心与其 Firepower Threat Defense 设备之间的带宽有限，这种做法非常有用。它还可以节省 Firepower 管理中心 上的空间。

- 版本 7.0.0 引入了新的 Firepower Threat Defense 升级工作流程，提示您将升级包复制到 Firepower Threat Defense 设备。

  如果您的 Firepower 管理中心运行的是版本 7.0.0+，我们建议您使用“设备升级”页面将升级包复制到 FTD 设备；请参阅升级带有 FMC 的 Firepower 威胁防御（版本7.0.0），第 71 页。您仍必须使用此程序将较早部署中的升级软件包复制到经典设备（Firepower 7000/8000 系列、ASA FirePOWER、NGIPSv）。

请注意，手动复制时，每台设备都会从源获取升级软件包，即系统不会在集群、堆栈或 HA 成员设备之间复制升级软件包。

开始之前

确保管理网络具有执行大型数据传输的带宽。请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。

步骤 1 在 Firepower 管理中心Web 界面上，选择**系统** > **更新**。

步骤 2 将升级包放在设备可以拿到的地方。

- Firepower 管理中心：手动将软件包上传或直接检索到 FMC。
- 内部 Web 服务器（Firepower Threat Defense 版本 6.6.0+）：上传到内部 Web 服务器并配置 Firepower Threat Defense 设备以从该服务器获取软件包。

步骤 3 点击您想要推送的升级软件包旁边的**推送 (Push)**（6.5.0 及更早版本）或**推送或准备更新 (Push or Stage update)**（6.6.0 及以上版本）图标，然后选择目标设备。

如果您想要推送升级软件包的设备未列出，则表示您选择了错误的升级软件包。

步骤 4 推送数据包

- Firepower 管理中心：点击**推送 (Push)**。
- 内部 Web 服务器：点击**从来源将更新下载到设备 (Download Update to Device from Source)**。

Firepower 软件就绪性检查

就绪性检查旨在评估 Firepower 设备对于软件升级的准备程度。如果设备的就绪性检查失败，请纠正问题并再次运行就绪性检查。如果就绪性检查列出了您无法解决的问题，我们建议不要开始升级。

运行就绪性检查所需的时间因设备型号和数据库大小而异。更高的版本也具有更快的就绪性检查。

通过 FMC 运行就绪性检查（版本 7.0.0+ FTD）

如果 FMC 运行的是版本 7.0.0+，我们建议您使用“设备升级”页面在 FTD 设备上运行就绪性检查；请参阅升级带有 FMC 的 Firepower 威胁防御（版本7.0.0），第 71 页。

如果您符合以下条件，请参阅以下主题：

- 对 FMC 自身运行就绪性检查。
- 在受管设备上运行就绪性检查，并且您的 FMC 正在运行版本 6.7.x。
- 在受管设备上运行就绪性检查，并且您的 FMC 正在运行版本 6.6.x 或更早版本。

通过 FMC 运行就绪性检查（版本 6.7.0+）

此程序适用于当前运行版本 6.7.0+ 的 FMC 及其受管设备，包括运行较早版本 (6.3.0 – 6.6.x) 的设备，以及高可用性和可扩展性部署中的 FTD 设备。



重要事项 如果 FMC 运行的是版本 7.0.0+，我们建议您使用“设备升级”页面在 FTD 设备上运行就绪性检查；请参阅升级带有 FMC 的 Firepower 威胁防御（版本7.0.0），第 71 页。您仍必须使用此程序在 FMC 和任何经典设备上运行就绪性检查。

开始之前

- 将 FMC 升级到至少版本 6.7.0。如果您的 FMC 当前运行的是较早版本，请参阅通过 FMC 运行就绪性检查（版本 6.0.1 – 6.6.x），第 41 页。

- 为要检查的设备将升级软件包上传到FMC。如果要检查版本6.6.0+FTD设备，您也可以在内部Web服务器上指定升级包位置。这是必需的，因为就绪性检查包含在升级包中。
- （可选）如果要将经典设备升级到任何版本，或将FTD设备升级到版本6.3.0.1 – 6.6.x，请将升级包复制到设备。这样可以减少运行就绪性检查所需的时间。如果要将FTD设备升级到版本6.7.0+，可以跳过这一步。虽然我们仍然建议您在开始升级之前先将升级软件包复制到设备，但在运行就绪性检查之前，您无需再执行此操作。

步骤 1 在FMC Web界面上，选择 **系统** > **更新**。

步骤 2 在可用的升级下，点击相应升级软件包旁边的 **安装** 图标。

系统将显示符合条件的设备列表，以及其升级前兼容性检查结果。从版本6.7.0开始，FTD设备必须通过某些基本检查，然后才能运行更复杂的就绪性检查。此预先检查会捕获将会导致升级失败的问题，但现在我们会更早地捕获这些问题并阻止您继续操作。

步骤 3 选择要检查的设备，然后点击**检查就绪性 (Check Readiness)**。

如果您无法选择符合条件的设备，请确保其通过了兼容性检查。您可能需要升级操作系统或部署配置更改。

步骤 4 在消息中心中监控就绪性检查的进度。

如果检查失败，消息中心会提供失败日志。

下一步做什么

Z **系统 (System)** > **更新 (Updates)** 页面，点击**就绪性检查 (Readiness Checks)** 以查看FTD部署的就绪性检查状态，包括正在进行的检查和失败的检查。您还可以使用此页面在失败后轻松地重新运行检查。

通过 FMC 运行就绪性检查（版本 6.0.1 – 6.6.x）

此程序适用于当前运行版本6.0.1 – 6.6.x的FMC及其独立受管设备。

注释 对于集群设备、堆栈中的设备和高可用性对中的设备，您可以从Linux外壳（也称为专家模式）运行就绪性检查。要运行检查，您必须先将升级包推送或复制到每台设备上的正确位置，然后使用此命令：`sudo install_update.pl --detach --readiness-check /var/sf/updates/upgrade_package_name`。有关详细说明，请联系Cisco TAC。

开始之前

- （版本6.0.1）如果要在版本6.0.1→6.1.0升级上运行就绪性检查，请先安装版本6.1预安装软件包。您必须对FMC和受管设备执行此操作。请参阅：Firepower 系统发行说明版本 6.1.0 预安装包。

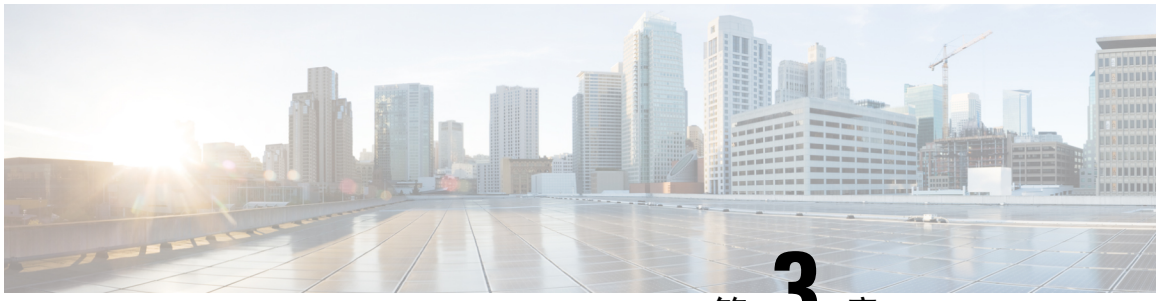
- 为要检查的设备将升级软件包上传到 FMC。如果要检查版本 6.6.x FTD 设备，您也可以在内部 Web 服务器上指定升级包位置。这是必需的，因为就绪性检查包含在升级包中。
- （可选，版本 6.2.3+）将升级包推送到受管设备。这样可以减少运行检查所需的时间。
- 将配置部署到其配置已过期的受管设备。否则，就绪性检查可能会失败。

步骤 1 在 FMC Web 界面上，选择**系统 (System)** > **更新 (Updates)**。

步骤 2 点击相应升级软件包旁边的**安装**图标。

步骤 3 选择要检查的设备，然后点击**启动就绪性检查 (Launch Readiness Check)**。

步骤 4 在消息中心中监控就绪性检查的进度。



第 3 章

升级 Firepower 管理中心

- 升级核对表：Firepower 管理中心，第 43 页
- 升级独立 Firepower 管理中心，第 46 页
- 升级高可用性 Firepower 管理中心，第 47 页

升级核对表：Firepower 管理中心

请在升级 FMC（包括 FMCv）之前填写此核对表。如果您在升级高可用性对，请对每个对等设备完成核对表。

注释 在此过程中的任何时候，请确保保持部署通信和运行状况。请勿重启正在进行的FMC升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

规划和可行性

认真规划和准备可以帮助您避免失误。

表 28:

	操作/检查
	计划升级路径。 这对于多设备部署、多跳升级或需要升级操作系统或托管环境，同时还要保持部署兼容性的情况尤其重要。始终了解已经完成的升级和即将执行的升级。 注释 在 FMC 部署中，通常先升级 FMC，然后再升级其受管设备。但是，在某些情况下，您可能需要先升级设备。 请参阅升级路径，第 11 页。

	操作/检查
	阅读所有升级指南和计划配置更改。 尤其是对于主要版本升级而言，升级可能会导致您或需要您在升级前或升级后的重大配置更改。从版本说明开始，版本说明包含重要且特定于版本的信息，包括升级警告、行为更改、新功能和弃用的功能以及已知问题。
	检查带宽。 确保管理网络具有执行大型数据传输的带宽。在 FMC 部署中，如果您在升级时将升级包传输到托管设备，则带宽不足会延长升级时间，甚至导致升级超时。如有可能，请在启动设备升级之前将升级软件包复制到受管设备。 请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。
	安排维护窗口。 考虑对流量和检查的任何影响以及升级可能需要的时间，将维护窗口安排在影响最小的时候。此外，还要考虑您必须在该维护窗口中执行的任务，以及可以提前执行的任务。例如，不要等到维护窗口将升级包复制到设备，运行就绪性检查，执行备份等操作。

升级程序包

思科支持和下载站点上可以获取升级包。

表 29:

	操作/检查
	上传升级包。 在 FMC 高可用性部署中，必须将 FMC 升级软件包上传到两个对等设备，在将软件包传输到备用设备之前暂停同步。要限制HA同步的中断，您可以在升级准备阶段将数据包传输到主用对等设备，并在暂停同步后将其作为实际升级过程的一部分传输到备用对等设备。 请参阅上传到 Firepower 管理中心， 第 37 页。

备份

灾难恢复能力是任何系统维护计划的重要组成部分。

备份和恢复可能是一个复杂的过程。您不想跳过任何步骤或忽略安全或许可问题。有关备份和恢复的要求、指南、限制和最佳实践的详细信息，请参阅适用于您的部署的配置指南。

⚠

注意 我们强烈建议在升级前和升级后，备份到安全的远程位置并验证传输是否成功。

表 *30:*

	操作/检查
	备份。 如果支持： • 升级前：如果升级失败是灾难性的，您可能必须重新映像并恢复。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。如果您有最近的备份，可以更快地恢复正常操作。 • 升级后：这会创建新升级的部署的快照。在 FMC 部署中，我们建议您在升级其受管设备后备份 FMC，以便新的 FMC 备份文件“知道”其设备已升级。

关联升级

由于操作系统和托管环境升级会影响流量和检查，因此请在维护窗口中执行。

表 *31:*

	操作/检查
	升级虚拟主机。 如果需要，请升级托管环境。如果需要执行此操作，通常是因为您运行的是旧版VMware并正在执行主要 FMC 升级。

最终检查

一系列最终检查可确保您已准备好升级。

表 *32:*

	操作/检查
	检查配置。 确保您已进行任何必要的升级前配置更改，并准备进行必要的升级后配置更改。
	检查 NTP 同步。 确保所有设备与您正在使用提供时间的 NTP 服务器进行同步。不同步可能会导致升级失败。在FMC部署中，如果时钟不同步超过10秒，运行状况模块会发出警报，但您仍应手动进行检查。 要检查时间，请执行以下操作： • FMC：选择**系统 > 配置 > 时间**。 • 设备：使用 **show time** CLI 命令。

	操作/检查
	检查硬盘空间。 运行磁盘空间检查进行软件升级。如果可用磁盘空间不足，会导致升级失败。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	部署配置。 在升级前部署配置可减少失败的可能性。在某些部署中，如果您的配置已过期，您可能会被阻止升级。在 FMC 高可用性部署中，您只需从主用对等设备进行部署。 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。 此外，部署某些配置会重启 Snort，这会中断流量检测，并且根据您的设备处理流量的方式，可能会中断流量，直至重启完成。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	运行就绪性检查。 如果 FMC 运行的是版本 6.1.0+，我们建议进行兼容性和就绪性检查。这些检查会评估您是否准备好进行软件升级。 请参阅 Firepower 软件就绪性检查，第 40 页。
	检查正在运行的任务。 确保在升级之前完成基本任务，包括最终部署。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。我们还建议您检查计划在升级期间运行的任务，并取消或推迟这些任务。 **注释** 在某些部署中，升级会自动推迟计划任务。任何计划在升级期间开始的任务都将在升级后重新启动后五分钟开始。 此功能目前支持 FMC 运行 6.4.0.10 及更高版本补丁、版本 6.6.3 及更高维护版本以及版本 6.7.0+。请注意，从受支持的版本进行的所有升级均支持此功能。从不支持的版本升级到支持的版本时，不支持此功能。

升级独立 Firepower 管理中心

使用此程序可升级独立的 Firepower 管理中心，包括 Firepower Management Center Virtual。

⚠

注意 升级 FMC 过程中，不要进行或部署配置更改、手动重启或关闭设备。请勿 重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

开始之前

完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。

步骤 1 选择**系统** > **更新**。

步骤 2 点击您想要使用的升级软件包旁边的安装图标，然后选择 FMC。

步骤 3 点击**安装 (Install)** 以开始升级。

确认您要升极和重启。

步骤 4 监控预检查进度，直到注销。在此期间，请勿更改配置。

步骤 5 在可以时登录回。

- 次要升级（补丁和热修复程序）：您可以在升级完成且重启后再次登录。
- 主要升级（补丁和热修复程序）：您可以在升级完成且重启后再次登录。系统会显示一个页面，供您用于监控升级进度，查看升级日志和任何错误消息。升级完成且系统重启时，您会再次注销。重新引导后，再次登录。

步骤 6 如果系统显示相应提示，则阅读并接受《最终用户许可协议 (EULA)》。

步骤 7 验证升级是否成功。

如果在您登录时系统未通知您升级成功，请选择**帮助** > **关于**以显示当前软件版本信息。

步骤 8 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 9 完成发行说明中所述的任何升级后配置更改。

步骤 10 重新部署配置。

重新部署到所有 受管设备。如果不部署到设备，其最终升级可能会失败，而且您可能需要对其重新映像。

升级高可用性 Firepower 管理中心

使用此程序可在高可用性对中的 FMC 上升级 Firepower 软件。

您需要逐一升级对等设备。在暂停同步的情况下，首先升级备用设备，然后升级主用设备。当备用开始预检查时，其状态从备用切换到主用，以便两个对等设备都处于主用状态。此临时状态称为 集群裂脑，仅 在升级期间受支持。请勿 在对处于集群脑裂的情况下执行或部署配置更改。重启同步后，您所做的更改将丢失。

⚠

注意 升级 FMC 过程中，不要进行或部署配置更改、手动重启或关闭设备。请勿 重启正在进行的升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

开始之前

完成两个对等设备的升级前检查表。确保部署中的设备保持正常运行，并且能够成功通信。

步骤 1 暂停同步。

a) 选择**系统** > **集成**。
b) 在**高可用性 (High Availability)**选项卡，点击**暂停同步 (Pause Synchronization)**。

步骤 2 将升级包上传到备用设备。

在 FMC 高可用性部署中，必须将 FMC 升级软件包上传到两个对等设备，在将软件包传输到备用设备之前暂停同步。要限制 HA 同步的中断，您可以在升级准备阶段将数据包传输到主用对等设备，并在暂停同步后将其作为实际升级过程的一部分传输到备用对等设备。

步骤 3 逐一升级对等体，先是备用设备，再是主用设备。

请按照升级独立 Firepower 管理中心，第 46 页中的说明进行操作，在验证每个对等体上的更新均成功后停止操作。总而言之，对于每个对等体：

a) 在**系统 (System)** > **更新 (Updates)**页面上，安装升级程序。
b) 监控进度，直到您注销，然后在可以时重新登录（在主要升级情况下这会发生两次）。
c) 验证升级是否成功。

请勿 在对处于集群脑裂的情况下执行或部署配置更改。

步骤 4 重启同步。

a) 登录到想到将其设置为主用对等体的 FMC。
b) 选择**系统** > **集成**。
c) 在**高可用性 (High Availability)**选项卡，点击**设为主用 (Make-Me-Active)**。
d) 等待直至同步重新开始，并且其他 FMC 切换到备用模式。

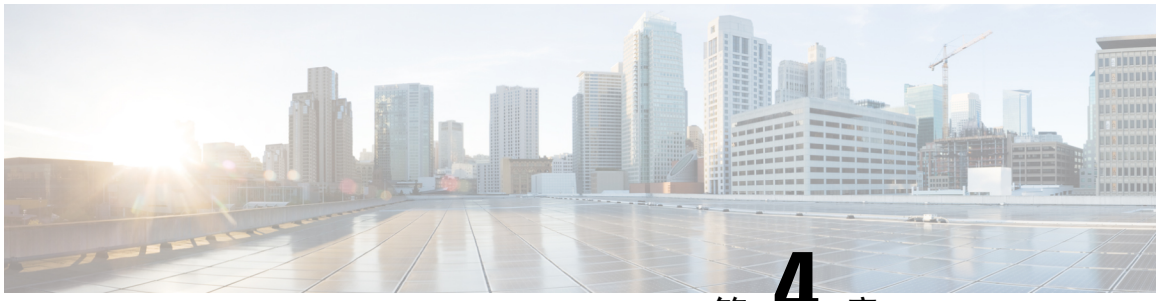
步骤 5 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 6 完成发行说明中所述的任何升级后配置更改。

步骤 7 重新部署配置。

重新部署到所有 受管设备。如果不部署到设备，其最终升级可能会失败，而且您可能需要对其重新映像。



第 4 章

通过 Firepower 管理中心升级 Firepower 威胁防御

- 升级核对表：带有 FMC 的 Firepower 威胁防御，第 49 页
- 在带有 Firepower 威胁防御逻辑设备的 Firepower 4100/9300 上升级 FXOS，第 54 页
- 升级带有 FMC 的 Firepower 威胁防御（版本7.0.0），第 71 页
- 升级带有 FMC 的 Firepower 威胁防御（版本6.0.1 – 6.7.0），第 74 页

升级核对表：带有 FMC 的 Firepower 威胁防御

请在升级 Firepower Threat Defense 之前填写此核对表。

注释 在此过程中的任何时候，请确保保持部署通信和运行状况。

在大多数情况下，请勿重启正在进行的升级。但是，从版本 6.7.0 的主要和维护 FTD 升级开始，您可以手动取消失败或正在进行的升级，并重试失败的升级；使用“升级状态”(Upgrade Status) 弹出窗口（可从“设备管理”(Device Management) 页面和消息中心访问），或使用 FTD CLI。请注意，默认情况下，在升级失败时 FTD 会自动将其恢复到升级前的状态（“自动取消”）。要能够手动取消或重试失败的升级，请在启动升级时禁用自动取消选项。请注意，补丁不支持自动取消。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。如果您已用尽所有选项，或者如果您的部署不支持取消/重试，请联系 Cisco TAC。

规划和可行性

认真规划和准备可以帮助您避免失误。

表 33:

	操作/检查
	计划升级路径。 这对于多设备部署、多跳升级或需要升级操作系统或托管环境，同时还要保持部署兼容性的情况尤其重要。始终了解已经完成的升级和即将执行的升级。 **注释** 在 FMC 部署中，通常先升级 FMC，然后再升级其受管设备。但是，在某些情况下，您可能需要先升级设备。 请参阅升级路径，第 11 页。
	阅读所有升级指南和计划配置更改。 尤其是对于主要版本升级而言，升级可能会导致您或需要您在升级前或升级后的重大配置更改。从版本说明开始，版本说明包含重要且特定于版本的信息，包括升级警告、行为更改、新功能和弃用的功能以及已知问题。
	检查设备访问。 设备可以在升级期间或在升级失败时停止传输流量（具体取决于接口配置）。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在 FMC 部署中，您还必须能够访问 FMC 管理界面而不遍历设备。
	检查带宽。 确保管理网络具有执行大型数据传输的带宽。在 FMC 部署中，如果您在升级时将升级包传输到托管设备，则带宽不足会延长升级时间，甚至导致升级超时。如有可能，请在启动设备升级之前将升级软件包复制到受管设备。 请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。
	安排维护窗口。 考虑对流量和检查的任何影响以及升级可能需要的时间，将维护窗口安排在影响最小的时候。此外，还要考虑您必须在该维护窗口中执行的任务，以及可以提前执行的任务。例如，不要等到维护窗口将升级包复制到设备，运行就绪性检查，执行备份等操作。

升级程序包

思科支持和下载站点上可以获取升级包。

表 *34:*

	操作/检查
	将升级软件包上传到 FMC 或内部 Web 服务器。 在版本 6.6.0+ 中，您可以配置一个内部 Web 服务器配置，而不是配置 FMC 作为 FTD 升级软件包的源。如果 FMC 及其设备之间的带宽有限，这会很有用，并且可以节省 FMC 上的空间。 请参阅上传到内部服务器（带有 FMC 的版本 6.6.0+ FTD），第 38 页。
	将升级包复制到设备。 当受支持时，我们建议您在启动设备升级之前将软件包复制（推送）到受管设备： • 版本 6.2.2 及更早版本不支持预升级复制。 • 版本 6.2.3 允许您从 FMC 手动复制升级软件包。 • 版本 6.6.0 添加了从内部 Web 服务器手动复制升级软件包的功能。 • 版本 7.0.0 添加了 FTD 升级工作流程，提示您复制升级软件包。 **注释** 对于 Firepower 4100/9300，我们建议（有时需要）您在开始所需的随附 FXOS 升级之前复制升级软件包。 请参阅复制到托管设备，第 39 页。

备份

灾难恢复能力是任何系统维护计划的重要组成部分。

备份和恢复可能是一个复杂的过程。您不想跳过任何步骤或忽略安全或许可问题。有关备份和恢复的要求、指南、限制和最佳实践的详细信息，请参阅适用于您的部署的配置指南。

注意 我们强烈建议在升级前和升级后，备份到安全的远程位置并验证传输是否成功。

表 35:

	操作/检查
	备份 FTD。 使用 FMC 来备份设备。并非所有 FTD 平台和配置都支持备份。需要版本 6.3.0+。 如果支持： • 升级前：如果升级失败是灾难性的，您可能必须重新映像并恢复。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。如果您有最近的备份，可以更快地恢复正常操作。 • 升级后：这会创建新升级的部署的快照。在 FMC 部署中，我们建议您在升级其受管设备后备份 FMC，以便新的 FMC 备份文件“知道”其设备已升级。
	在 Firepower 4100/9300 上备份 FXOS。 在升级前后使用 Firepower 机箱管理器或 FXOS CLI 导出机箱配置，包括逻辑设备和平台配置设置。

关联升级

由于操作系统和托管环境升级会影响流量和检查，因此请在维护窗口中执行。

表 36:

	操作/检查
	升级虚拟主机。 如果需要，请升级任何虚拟设备的托管环境。如果需要执行此操作，通常是因为您运行的是旧版 VMware 并正在执行主要设备升级。
	升级 Firepower 4100/9300 的 FXOS。 如果需要，请在升级 FTD 之前升级 FXOS。这通常是主要升级的要求，但很少用于 维护版本和补丁。为避免流量和检查出现中断，请在 FTD 高可用性对中升级 FXOS 以及在机箱内集群中一次升级一个机箱。 **注释** 在升级FXOS之前，请确保阅读所有升级指南并计划配置更改。首先是FXOS版本说明：Cisco Firepower 4100/9300 FXOS 发行说明。

最终检查

一系列最终检查可确保您已准备好升级。

表 *37:*

	操作/检查
	检查配置。 确保您已进行任何必要的升级前配置更改，并准备进行必要的升级后配置更改。
	检查 NTP 同步。 确保所有设备与您正在使用提供时间的 NTP 服务器进行同步。不同步可能会导致升级失败。在FMC部署中，如果时钟不同步超过10秒，运行状况模块会发出警报，但您仍应手动进行检查。 要检查时间，请执行以下操作： • FMC：选择**系统 > 配置 > 时间**。 • 设备：使用 **show time** CLI 命令。
	检查硬盘空间。 运行磁盘空间检查进行软件升级。如果可用磁盘空间不足，会导致升级失败。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	部署配置。 在升级前部署配置可减少失败的可能性。在某些部署中，如果您的配置已过期，您可能会被阻止升级。在 FMC 高可用性部署中，您只需从主用对等设备进行部署。 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。 此外，部署某些配置会重启 Snort，这会中断流量检测，并且根据您的设备处理流量的方式，可能会中断流量，直至重启完成。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	运行就绪性检查。 如果 FMC 运行的是版本 6.1.0+，我们建议进行兼容性和就绪性检查。这些检查会评估您是否准备好进行软件升级。版本 7.0.0 引入了新的 FTD 升级工作流程，提示您完成这些检查。 请参阅 Firepower 软件就绪性检查 ， 第 40 页。
	检查正在运行的任务。 在升级之前，请确保设备上的基本任务已完成，包括最终部署。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。我们还建议您检查计划在升级期间运行的任务，并取消或推迟这些任务。

在带有 Firepower 威胁防御逻辑设备的 Firepower 4100/9300 上升级 FXOS

在 Firepower 4100/9300 上，您可以在每个机箱上独立升级 FXOS，即使配置了 Firepower 机箱内集群或高可用性对也是如此。您可以使用 FXOS CLI 或 Firepower 机箱管理器。

升级 FXOS 会重启机箱。根据您的部署，流量可以不经过检查就丢弃或穿越网络；请参阅您所用版本的 CiscoFirepower 版本说明。

升级 FXOS：FTD 独立设备或机箱内集群

对于独立的 Firepower 威胁防御逻辑设备，或对于 FTD 机箱内集群（同一机箱上的设备），请先升级 FXOS 平台捆绑包，然后再升级 FTD 逻辑设备。使用 Firepower 管理中心将集群设备作为一个单元进行升级。

使用 Firepower 机箱管理器为独立 FTD 逻辑设备或 FTD 机箱内集群升级 FXOS

本部分介绍如何升级独立的 Firepower 4100/9300 机箱的 FXOS 平台捆绑包。

本部分介绍以下类型的设备的升级过程：

- Firepower 4100 系列 机箱，其配置了 逻辑设备且不是故障转移对或机箱内集群的一部分。
- Firepower 9300 机箱，其配置了不属于故障转移对或机箱内集群的一个或多个独立 逻辑设备。
- Firepower 9300机箱，其在机箱内集群中配置了 FTD 逻辑设备。

开始之前

开始升级之前，请确保您已完成以下操作：

- 将 FXOS 平台捆绑包软件包下载到您要升级的位置。
- 备份您的 FXOS 和 FTD 配置。

步骤 1 在 Firepower 机箱管理器中，选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 FXOS 平台捆绑包映像和应用映像列表。

步骤 2 上传新的平台捆绑包映像：

a) 点击**上传映像**，可打开“上传映像”对话框。
b) 点击**选择文件**，可导航到并选择想要上传的映像。
c) 点击**上传**。
所选映像将上传到 Firepower 4100/9300 机箱。
d) 对于某些软件映像，上传映像后，系统将显示一份最终用户许可协议。请按照系统提示接受这份最终用户许可协议。

步骤 3 成功上传新的平台捆绑包映像后，点击要升级到的 FXOS 平台捆绑包对应的**升级**。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的FXOS平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

步骤 4 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 5 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI监控升级过程：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

步骤 6 成功升级所有组件后，输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。
b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。
f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机。

使用 FXOS CLI 为独立 FTD 逻辑设备或 FTD 机箱内集群升级 FXOS

本部分介绍如何升级独立的 Firepower 4100/9300 机箱的 FXOS 平台捆绑包。

本部分介绍以下类型的设备的 FXOS 升级过程：

- Firepower 4100 系列 机箱，其配置了 逻辑设备且不是故障转移对或机箱内集群的一部分。
- Firepower 9300 机箱，其配置了不属于故障转移对或机箱内集群的一个或多个独立 FTD 设备。
- Firepower 9300机箱，其在机箱内集群中配置了 FTD 逻辑设备。

开始之前

开始升级之前，请确保您已完成以下操作：

- 将 FXOS 平台捆绑包软件包下载到您要升级的位置。
- 备份您的 FXOS 和 FTD 配置。
- 收集将软件映像下载到 Firepower 4100/9300 机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

步骤 1 连接到 FXOS CLI。

步骤 2 将新的平台捆绑包映像下载到 Firepower 4100/9300 机箱：

a) 进入固件模式：

Firepower-chassis-a # **scope firmware**

b) 下载 FXOS平台捆绑包软件映像：

Firepower-chassis-a /firmware # **download image** *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*:*port-num*/*path*/*image_name*

c) 要监控下载过程，请执行以下操作：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
```

```
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 3 如有必要，请返回到固件模式：

Firepower-chassis-a /firmware/download-task # **up**

步骤 4 进入自动安装模式：

Firepower-chassis-a /firmware # **scope auto-install**

步骤 5 安装 FXOS 平台捆绑包：

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number 是您正在安装的 FXOS平台捆绑包的版本号，例如 2.3(1.58)。

步骤 6 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的FXOS平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

输入 **yes**，确认您想要继续验证。

步骤 7 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 8 要监控升级流程，请执行以下操作：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
```

```
        Upgrade-Status: Ready
FP9300-A /system #
```

步骤 9 成功升级所有组件后，输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。
b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。
f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机。

升级 FXOS：FTD 高可用性对

在Firepower威胁防御高可用性部署中，请首先升级两个机箱上的FXOS平台捆绑包，然后再升级任一 FTD 逻辑设备。要最大限度地减少中断，请始终升级备用设备。

在 Firepower 管理中心部署中，您可以将逻辑设备作为一个单元进行升级：

1. 在备用设备上升级 FXOS。
2. 切换角色。
3. 新的备用设备上升级 FXOS。
4. 升级 FTD 逻辑设备。

使用 Firepower 机箱管理器升级 FTD 高可用性对上的 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 FTD 逻辑设备配置为高可用性对，请使用以下程序更新 Firepower 9300 或 Firepower 4100 系列安全设备上的 FXOS 平台捆绑包：

开始之前

开始升级之前，请确保您已完成以下操作：

- 将 FXOS 平台捆绑包软件包下载到您要升级的位置。
- 备份您的 FXOS 和 FTD 配置。

步骤 1 连接到包含备用 Firepower 威胁防御逻辑设备的 Firepower 安全设备上的 Firepower 机箱管理器：

步骤 2 在 Firepower 机箱管理器中，选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 FXOS 平台捆绑包映像和应用映像列表。

步骤 3 上传新的平台捆绑包映像：

a) 点击**上传映像**，可打开“上传映像”对话框。
b) 点击**选择文件**，可导航到并选择想要上传的映像。
c) 点击**上传**。
所选映像将上传到 Firepower 4100/9300 机箱。
d) 对于某些软件映像，上传映像后，系统将显示一份最终用户许可协议。请按照系统提示接受这份最终用户许可协议。

步骤 4 成功上传新的平台捆绑包映像后，点击要升级到的 FXOS 平台捆绑包对应的**升级**。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

步骤 5 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 6 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI监控升级过程：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

步骤 7 成功升级所有组件后，输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。
b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。

f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机。

步骤 8 将刚才升级的设备设为活动设备，以使流量流向已升级的设备：

a) 连接到 Firepower 管理中心。
b) 选择**设备** > **设备管理**。
c) 在要更改主用对等设备的高可用性对旁边，点击“切换主用对等设备”图标 ( )。
d) 点击**是**将使备用设备立即变成高可用性对中的主用设备。

步骤 9 连接到包含新的备用 Firepower 威胁防御逻辑设备的 Firepower 安全设备上的 Firepower 机箱管理器：

步骤 10 在 Firepower 机箱管理器中，选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 FXOS 平台捆绑包映像和应用映像列表。

步骤 11 上传新的平台捆绑包映像：

a) 点击**上传映像**，可打开“上传映像”对话框。
b) 点击**选择文件**，可导航到并选择想要上传的映像。
c) 点击**上传**。
所选映像将上传到 Firepower 4100/9300 机箱。
d) 对于某些软件映像，上传映像后，系统将显示一份最终用户许可协议。请按照系统提示接受这份最终用户许可协议。

步骤 12 成功上传新的平台捆绑包映像后，点击要升级到的 FXOS 平台捆绑包对应的**升级**。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

步骤 13 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。

系统打开捆绑包，升级/重新加载组件。升级过程最多可能需要 30 分钟才能完成。

步骤 14 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI监控升级过程：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
```

```
Package-Vers: 2.3(1.58)
Upgrade-Status: Ready
```

步骤 15 成功升级所有组件后，输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。
b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。
f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机。

步骤 16 将刚才升级的设备设为活动设备，同升级前一样：

a) 连接到 Firepower 管理中心。
b) 选择**设备** > **设备管理**。
c) 在要更改主用对等设备的高可用性对旁边，点击“切换主用对等设备”图标 ()。
d) 点击**是**将使备用设备立即变成高可用性对中的主用设备。

使用 FXOS CLI 在 FTD 高可用性对上升级 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 FTD 逻辑设备配置为高可用性对，请使用以下程序更新 Firepower 9300 或 Firepower 4100 系列安全设备上的 FXOS 平台捆绑包：

开始之前

开始升级之前，请确保您已完成以下操作：

- 将 FXOS 平台捆绑包软件包下载到您要升级的位置。
- 备份您的 FXOS 和 FTD 配置。
- 收集将软件映像下载到 Firepower 4100/9300 机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

步骤 1 连接到包含备用 Firepower 威胁防御逻辑设备的 Firepower 安全设备上的 FXOS CLI：

步骤 2 将新的平台捆绑包映像下载到 Firepower 4100/9300 机箱：

a) 进入固件模式：

Firepower-chassis-a # **scope firmware**

b) 下载 FXOS平台捆绑包软件映像：

Firepower-chassis-a /firmware # **download image** *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*:*port-num*/*path*/*image_name*

c) 要监控下载过程，请执行以下操作：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 3 如有必要，请返回到固件模式：

Firepower-chassis-a /firmware/download-task # **up**

步骤 4 进入自动安装模式：

Firepower-chassis-a /firmware # **scope auto-install**

步骤 5 安装 FXOS 平台捆绑包：

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number 是您正在安装的 FXOS平台捆绑包的版本号；例如 2.3(1.58)。

步骤 6 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

输入 **yes**，确认您想要继续验证。

步骤 7 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 8 要监控升级流程，请执行以下操作：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

步骤 9 成功升级所有组件后，输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。
b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。
f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机。

步骤 10 将刚才升级的设备设为活动设备，以使流量流向已升级的设备：

a) 连接到 Firepower 管理中心。
b) 选择**设备** > **设备管理**。
c) 在要更改主用对等设备的高可用性对旁边，点击“切换主用对等设备”图标 ( )。
d) 点击**是 (Yes)** 将使备用设备立即变成高可用性对中的主用设备。

步骤 11 连接到包含新备用 Firepower 威胁防御逻辑设备的 Firepower 安全设备上的 FXOS CLI：

步骤 12 将新的平台捆绑包映像下载到 Firepower 4100/9300 机箱：

a) 进入固件模式：

Firepower-chassis-a # **scope firmware**

b) 下载 FXOS平台捆绑包软件映像：

Firepower-chassis-a /firmware # **download image** *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*:*port-num*/*path*/*image_name*

c) 要监控下载过程，请执行以下操作：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 13 如有必要，请返回到固件模式：

Firepower-chassis-a /firmware/download-task # **up**

步骤 14 进入自动安装模式：

Firepower-chassis-a /firmware # **scope auto-install**

步骤 15 安装 FXOS 平台捆绑包：

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number 是您正在安装的 FXOS平台捆绑包的版本号；例如 2.3(1.58)。

步骤 16 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

输入 **yes**，确认您想要继续验证。

步骤 17 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 18 要监控升级流程，请执行以下操作：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

步骤 19 成功升级所有组件后，输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。
b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。
f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机。

步骤 20 将刚才升级的设备设为活动设备，同升级前一样：

a) 连接到 Firepower 管理中心。
b) 选择**设备** > **设备管理**。
c) 在要更改主用对等设备的高可用性对旁边，点击“切换主用对等设备”图标 ( )。
d) 点击**是 (Yes)** 将使备用设备立即变成高可用性对中的主用设备。

升级 FXOS：FTD 机箱内集群

对于Firepower威胁防御机箱内集群（不同机箱上的单元），请先升级所有机箱上的FXOS平台捆绑包，然后再升级FTD逻辑设备。为了最大限度地减少中断，请始终升级全数据单元机箱上的FXOS。然后，使用 Firepower 管理中心将逻辑设备作为一个单元进行升级。

例如，对于双机箱集群：

1. 在全数据单元机箱上升级 FXOS。
2. 将控制模块切换到您刚刚升级的机箱。
3. 在全新全数据单元机箱上升级 FXOS。
4. 升级 FTD 逻辑设备。

使用 Firepower 机箱管理器升级 FXOS 和 FTD 机箱内集群

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 FTD 逻辑设备配置为机箱内集群，请使用以下程序更新 Firepower 9300 或 Firepower 4100 系列安全设备上的 FXOS 平台捆绑包：

开始之前

开始升级之前，请确保您已完成以下操作：

- 将 FXOS 平台捆绑包软件包下载到您要升级的位置。
- 备份您的 FXOS 和 FTD 配置。

步骤 1 输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 连接到机箱 2（应该是没有控制单元的机箱）上的 FXOS CLI。
b) 输入 **top**。
c) 输入 **scope ssa**。
d) 输入 **show slot**。
e) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
f) 输入 **show app-instance**。
g) 验证机箱上安装的任何逻辑设备的运行状态是否为联机，且集群状态是否为集群内。另外，验证显示的运行版本是否为正确的 FTD 软件版本。

重要事项 确认主设备不在该机箱中。“集群角色”设置为主的任何 Firepower 威胁防御实例都不应存在。

h) 对于安装在 Firepower 9300 设备上的任何安全模块或 Firepower 4100 系列设备上的安全引擎，验证 FXOS 版本是否正确：

scope server 1/*slot_id*，其中 *slot_id* 对于 Firepower 4100 系列安全引擎为 1。

show version。

步骤 2 连接到机箱 2（应该是没有控制单元的机箱）上的 Firepower 机箱管理器。

步骤 3 在 Firepower 机箱管理器中，选择**系统 (System)** > **更新 (Updates)**。
“可用更新 (Available Updates)”页面显示机箱上可用的 FXOS 平台捆绑包映像和应用映像列表。

步骤 4 上传新的平台捆绑包映像：

a) 点击**上传映像 (Upload Image)**，可打开“上传映像”(Upload Image) 对话框。
b) 点击**选择文件 (Choose File)**，可导航到并选择想要上传的映像。
c) 点击**上传 (Upload)**。
所选映像将上传到 Firepower 4100/9300 机箱。
d) 对于某些软件映像，上传映像后，系统将显示一份最终用户许可协议。请按照系统提示接受这份最终用户许可协议。

步骤 5 成功上传新的平台捆绑包映像后，点击要升级到的 FXOS 平台捆绑包对应的**升级 (Upgrade)**。

系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

步骤 6 点击**是 (Yes)**，确认您想要继续安装，或者点击**否 (No)** 取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 7 Firepower 机箱管理器在升级期间将不可用。您可以使用 FXOS CLI监控升级过程：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

d) 输入 **top**。
e) 输入 **scope ssa**。
f) 输入 **show slot**。
g) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
h) 输入 **show app-instance**。
i) 验证机箱上安装的任何逻辑设备的运行状态是否为联机、集群状态是否为集群内，且集群角色是否为从属。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
```

```
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Profile Name Cluster
 State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                     In
Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                     In
Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                     Not
Applicable  None
FP9300-A /ssa #
```

步骤 8 将机箱 2 中的其中一个安全模块设为控制。

将机箱 2 上的某个安全模块设置为“控制”后，机箱 1 中则不再包含控制单元，现在即可对其进行升级。

步骤 9 对集群中的其他所有机箱重复步骤 1 到 7。

步骤 10 要将“控制”角色返还机箱 1，请将机箱 1 上的某个安全模块设置为“控制”。

使用 FXOS CLI 在 FTD 机箱内集群上升级 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 FTD 逻辑设备配置为机箱内集群，请使用以下程序更新 Firepower 9300 或 Firepower 4100 系列安全设备上的 FXOS 平台捆绑包：

开始之前

开始升级之前，请确保您已完成以下操作：

- 将 FXOS 平台捆绑包软件包下载到您要升级的位置。
- 备份您的 FXOS 和 FTD 配置。
- 收集将软件映像下载到 Firepower 4100/9300 机箱所需的以下信息：
  - 您从其复制映像的服务器的 IP 地址和身份验证凭证。
  - 映像文件的完全限定名称。

步骤 1 连接到机箱 2（应该是没有控制单元的机箱）上的 FXOS CLI。

步骤 2 输入以下命令以验证安全模块/安全引擎和任何已安装的应用的状态：

a) 输入 **top**。

b) 输入 **scope ssa**。
c) 输入 **show slot**。
d) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
e) 输入 **show app-instance**。
f) 验证机箱上安装的任何逻辑设备的运行状态是否为联机，且集群状态是否为集群内。另外，验证显示的运行版本是否为正确的 FTD 软件版本。

重要事项 确认主设备不在该机箱中。“集群角色”设置为主的任何 Firepower 威胁防御实例都不应存在。

g) 对于安装在 Firepower 9300 设备上的任何安全模块或 Firepower 4100 系列设备上的安全引擎，验证 FXOS 版本是否正确：

scope server 1/*slot_id*，其中 *slot_id* 对于 Firepower 4100 系列安全引擎为 1。

show version。

步骤 3 将新的平台捆绑包映像下载到 Firepower 4100/9300 机箱：

a) 输入 **top**。
b) 进入固件模式：

Firepower-chassis-a # **scope firmware**

c) 下载 FXOS平台捆绑包软件映像：

Firepower-chassis-a /firmware # **download image** *URL*

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

d) 要监控下载过程，请执行以下操作：

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

示例：

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
```

```
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

步骤 4 如有必要，请返回到固件模式：

Firepower-chassis-a /firmware/download-task # **up**

步骤 5 进入自动安装模式：

Firepower-chassis /firmware # **scope auto-install**

步骤 6 安装 FXOS 平台捆绑包：

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number 是您正在安装的 FXOS平台捆绑包的版本号，例如 2.3(1.58)。

步骤 7 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

输入 **yes**，确认您想要继续验证。

步骤 8 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

系统打开捆绑包，升级/重新加载组件。

步骤 9 要监控升级流程，请执行以下操作：

a) 输入 **scope system**。
b) 输入 **show firmware monitor**。
c) 等待所有组件（FPRM、交换矩阵互联和机箱）显示升级状态：就绪。

注释 升级 FPRM 组件后，系统将重启，然后继续升级其他组件。

d) 输入 **top**。
e) 输入 **scope ssa**。
f) 输入 **show slot**。
g) 验证 Firepower 4100 系列设备上的安全引擎或 Firepower 9300 设备上安装的任何安全模块的管理状态是否为正常，且操作状态是否为联机。
h) 输入 **show app-instance**。
i) 验证机箱上安装的任何逻辑设备的运行状态是否为联机、集群状态是否为集群内，且集群角色是否为从属。

示例：

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
```

```
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Profile Name Cluster
 State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                     In
Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                     In
Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                     Not
Applicable  None
FP9300-A /ssa #
```

步骤 10 将机箱 2 中的其中一个安全模块设为控制。

将机箱 2 上的某个安全模块设置为“控制”后，机箱 1 中则不再包含控制单元，现在即可对其进行升级。

步骤 11 对集群中的其他所有机箱重复步骤 1 到 9。

步骤 12 要将“控制”角色返还机箱 1，请将机箱 1 上的某个安全模块设置为“控制”。

升级带有 FMC 的 Firepower 威胁防御（版本7.0.0）

FMC 提供升级 FTD 的向导。您仍必须使用“系统更新”(System Updates)（**系统 (System) > 更新 (Updates)**）页面来上传或指定升级包的位置。您还必须使用“系统更新”页面升级 FMC 本身以及任何老版经典设备。

该向导将引导您完成重要的升级前阶段，包括选择要升级的设备，将升级包复制到设备，以及执行兼容性和就绪性检查。继续操作时，向导会显示有关所选设备的基本信息以及当前的升级相关状态。这包括无法升级的任何原因。如果设备未在向导中“通过”某个阶段，则该阶段不会显示在下一阶段。

如果您离开该向导，系统会保留您的进度，但其他具有管理员访问权限的用户可以重置、修改或继续工作流程（除非您使用 CAC 登录，在这种情况下，您的进度会在您注销后 24 小时清除）。您的进度也会在高可用性 FMC 之间同步。



注释 在版本 7.0.x，设备升级页面无法正确显示集群或高可用性对中的设备。即使必须将这些设备作为一个单元进行选择和升级，工作流程也会将其显示为独立设备。设备状态和升级就绪性会逐个评估和报告。这意味着一台设备可能会“传递”到下一阶段，而另一台设备则不会。但是，这些设备仍然分组。因此，在一台设备上运行就绪性检查，所有设备上都会运行。在一台设备上启动升级，在所有设备上都会启动升级。

为避免可能的耗时升级失败，请手动确保所有组成员都已准备好继续执行工作流程的下一步，然后再点击 **下一步**。



注意 请勿在升级期间进行或部署配置更改。即使系统显示为非活动状态，也不要手动重新启动或关闭。在大多数情况下，请勿重启正在进行的升级。但是，通过从版本 6.7.0 的主要和维护升级，您可以手动取消失败或正在进行的升级，并重试失败的升级；使用“升级状态”(Upgrade Status) 弹出窗口（可从“设备管理”(Device Management) 页面和消息中心访问），或使用 FTD CLI。

请注意，默认情况下，在升级失败时 FTD 会自动将其恢复到升级前的状态（“自动取消”）。要能够手动取消或重试失败的升级，请在启动升级时禁用自动取消选项。请注意，补丁不支持自动取消。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。如果您已用尽所有选项，或者如果您的部署不支持取消/重试，请联系 Cisco TAC。

开始之前

完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。

选择要升级的设备。

步骤 1 选择**设备 > 设备管理**。

步骤 2 选择想要升级的设备。

您可以一次升级多个设备。您必须同时升级设备集群和高可用性对的成员。

重要事项 由于性能问题，如果您将设备升级到（不是从）版本 6.4.0.x 到 6.6.x，我们强烈建议同时升级不超过五台设备。

步骤 3 从**选择操作**或**选择批量操作**菜单中，选择**升级 Firepower 软件**。

系统将显示“设备升级”（Device Upgrade）页面，指示您选择了多少台设备并提示您选择目标版本。该页面有两个窗格：左侧是设备选择，右侧是设备详细信息。点击设备选择中的设备链接（例如“4 台设备”）以显示这些设备的设备详细信息。

请注意，如果正在处理升级工作流程，则必须首先**合并设备**（将新选择的设备添加到之前选择的设备并继续）或**重置**（放弃之前的选择并仅使用新选择的设备）。

步骤 4 核对您的设备选择。

要选择其他设备，请返回“设备管理”页面，您的进度不会丢失。如需删除设备，点击**重置**清除设备选择并重新开始。

将升级软件包复制到设备。

步骤 5 从**升级到**菜单中，选择目标版本。

系统确定哪些所选设备可以升级到该版本。如果任何设备都不符合条件，您可以点击设备链接查看原因。如果您不想删除不符合条件的设备，则无需删除；它们将不会包含在下一步中。

请注意，**升级到**菜单中的选项对应于系统可用的设备升级软件包。如果您的目标版本未列出，请转至**系统**（**System**）**>更新**（**Updates**），并上传或指定正确升级包的位置。

步骤 6 对于仍需要升级软件包的所有设备，请点击**复制升级软件包**，然后确认选择。

要升级 FTD，必须在设备上安装软件升级包。在升级之前复制升级软件包可缩短升级维护窗口的长度。

执行兼容性、就绪性和其他最终检查。

步骤 7 对于需要通过就绪性检查的所有设备，请点击**运行就绪性检查**，然后确认您的选择。

虽然您可以通过禁用**需要通过兼容性和就绪性检查选项**来跳过检查，但我们建议不要使用此选项。通过所有检查可以大大降低升级失败的可能性。在运行就绪性检查时，请勿将更改部署到设备、手动重新启动或关闭设备。如果设备的就绪性检查失败，请纠正问题并再次运行就绪性检查。如果就绪性检查列出了您无法解决的问题，请不要开始升级，而是联系Cisco TAC寻求帮助。

请注意，兼容性检查是自动进行的。例如，如果您需要在Firepower 4100/9300 上升级 FXOS，或者如果您需要部署到托管设备，系统会立即发出警报。

步骤 8 执行最终的升级前检查。

重新查看预升级核对表。确保您已完成所有相关任务，尤其是最终检查。

步骤 9 如有必要，请返回“设备升级”页面。

您的进度应已保留。如果不是，则具有管理员访问权限的其他人可能已重置、修改或完成了此工作流程。

步骤 10 点击**下一步**。

升级。

步骤 11 核对您选择的设备和目标版本。

步骤 12 选择回滚选项。

对于主升级得维护升级，升级失败时，**系统将自动取消升级并回滚至上一版本**。启用此选项后，设备会在升级失败时自动返回到升级前的状态。如果您希望能够手动取消或重试失败的升级，请禁用此选项。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。

这些选项不支持打补丁。

步骤 13 点击**开始升级 (Start Upgrade)**，然后确认您要升级并重启设备。

您可以在消息中心监控升级进度。有关升级期间流量处理的信息，请参阅版本说明中的升级软件一章。

在更新过程中，设备可能会重新启动两次。这是预期行为。

验证成功并完成升级后任务。

步骤 14 验证升级是否成功。

升级过程完成后，选择**设备** > **设备管理**，并确认您升级的设备具有正确的软件版本。

步骤 15 （可选）在高可用性/可扩展性部署中，检查设备角色。

升级流程会切换设备角色，以便始终升级备用设备或数据单元。它不会将设备恢复到升级前的角色。如果您有特定设备的首选角色，请立即进行更改。

步骤 16 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 17 完成发行说明中所述的任何升级后配置更改。

步骤 18 将配置重新部署到将刚才升级的设备。

下一步做什么

（可选）通过返回“设备升级”（Device Upgrade）页面并点击“**完成**”（Finish）来清除向导。在执行此操作之前，“设备升级”页面将继续显示有关您刚刚执行的升级的详细信息。

升级带有 FMC 的 Firepower 威胁防御（版本6.0.1 – 6.7.0）

使用此程序通过 FMC 的“系统更新”(System Updates) 页面升级 FTD。在此页面上，如果多台设备使用相同的升级软件包，仅可一次性对这些设备同时进行升级。您必须同时升级设备集群和高可用性对的成员。

开始之前

- 决定是否要使用此程序。对于版本 7.0.x 的 FTD 升级，我们建议您改为使用升级向导；请参阅升级带有 FMC 的 Firepower 威胁防御（版本7.0.0），第 71 页。
- 完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。
- （可选）交换高可用性设备对的主用/备用角色。选择**设备 (Devices)** > **设备管理 (Device Management)**，点击对等设备旁边的**切换主用设备 (Switch Active Peer)** 图标并确认您的选择。

  首先升级高可用性对中的备用设备。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。

步骤 1 选择**系统** > **更新**。

步骤 2 点击您想要使用的升级软件包旁边的安装图标，然后选择要升级的设备。

如果您想要升级的设备未列出，则表示您选择了错误的升级软件包。

注释 我们强烈 建议同时从“系统更新”页面升级的设备数不超过五个。不能在所有选定设备完成升级过程之前停止升级。如果任何一个设备升级存在问题，则必须等待所有设备均完成升级，然后才可以解决该问题。

步骤 3 （版本 6.7.0+）选择回滚选项。

对于主升级得维护升级，升级失败时，**系统将自动取消升级并回滚至上一版本**。启用此选项后，设备会在升级失败时自动返回到升级前的状态。如果您希望能够手动取消或重试失败的升级，请禁用此选项。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。 补丁不支持自动取消。

步骤 4 点击**安装 (Install)**，然后确认您要升级并重启设备。

在升级过程中，一些设备可能会重启两次；这是预期行为。流量在整个升级过程中丢弃还是不进行检测就穿过网络，取决于您的设备的配置和部署方式。有关详细信息，请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。

步骤 5 监控升级进度。

注意 请勿将更改部署到正在升级的设备或部署更改到，手动重启正在升级的设备，或者关闭正在升级的设备。

在大多数情况下，请勿重启正在进行的升级。但是，从版本 6.7.0 的主要和维护 FTD 升级开始，您可以手动取消失败或正在进行的升级，并重试失败的升级；使用“升级状态”(Upgrade Status) 弹出窗口（可从“设备管理”(Device Management) 页面和消息中心访问），或使用 FTD CLI。请注意，默认情况下，在升级失败时 FTD 会自动将其恢复到升级前的状态（“自动取消”）。要能够手动取消或重试失败的升级，请在启动升级时禁用自动取消选项。请注意，补丁不支持自动取消。在高可用性或集群部署中，自动取消会单独应用于每个设备。也就是说，如果一台设备上的升级失败，则仅恢复该设备。如果您已用尽所有选项，或者如果您的部署不支持取消/重试，请联系 Cisco TAC。

步骤 6 验证升级是否成功。

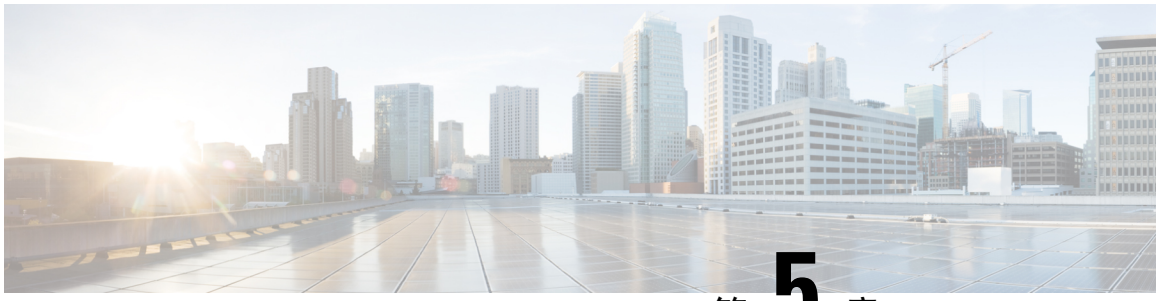
升级过程完成后，选择**设备** > **设备管理**，并确认您升级的设备具有正确的软件版本。

步骤 7 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 8 完成发行说明中所述的任何升级后配置更改。

步骤 9 将配置重新部署到将刚才升级的设备。



第 5 章

升级 Firepower 7000/8000 系列和 NGIPSv

- 升级核对表：带有 FMC 的 Firepower 7000/8000 系列和 NGIPSv，第 77 页
- 升级带有 FMC 的 Firepower 7000/8000 和 NGIPSv，第 80 页

升级核对表：带有 FMC 的 Firepower 7000/8000 系列和 NGIPSv

请在升级 Firepower 7000/8000 系列和 NGIPSv 设备之前填写此核对表。

注释 在此过程中的任何时候，请确保保持部署通信和运行状况。请勿重启正在进行的设备升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

规划和可行性

认真规划和准备可以帮助您避免失误。

表 38:

	操作/检查
	计划升级路径。 这对于多设备部署、多跳升级或需要升级操作系统或托管环境，同时还要保持部署兼容性的情况尤其重要。始终了解已经完成的升级和即将执行的升级。 **注释** 在 FMC 部署中，通常先升级 FMC，然后再升级其受管设备。但是，在某些情况下，您可能需要先升级设备。 请参阅升级路径，第 11 页。

	操作/检查
	阅读所有升级指南和计划配置更改。 尤其是对于主要版本升级而言，升级可能会导致您或需要您在升级前或升级后的重大配置更改。从版本说明开始，版本说明包含重要且特定于版本的信息，包括升级警告、行为更改、新功能和弃用的功能以及已知问题。
	检查设备访问。 设备可以在升级期间或在升级失败时停止传输流量（具体取决于接口配置）。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在 FMC 部署中，您还必须能够访问 FMC 管理界面而不遍历设备。
	检查带宽。 确保管理网络具有执行大型数据传输的带宽。在 FMC 部署中，如果您在升级时将升级包传输到托管设备，则带宽不足会延长升级时间，甚至导致升级超时。如有可能，请在启动设备升级之前将升级软件包复制到受管设备。 请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。
	安排维护窗口。 考虑对流量和检查的任何影响以及升级可能需要的时间，将维护窗口安排在影响最小的时候。此外，还要考虑您必须在该维护窗口中执行的任务，以及可以提前执行的任务。例如，不要等到维护窗口将升级包复制到设备，运行就绪性检查，执行备份等操作。

升级程序包

思科支持和下载站点上可以获取升级包。

表 39:

	操作/检查
	将升级包上传到 FMC。 请参阅上传到 Firepower 管理中心， 第 37 页。
	将升级包复制到设备。 如果 FMC 运行的是版本 6.2.3+，我们建议您在启动设备升级之前将软件包复制（推送）到受管设备。 请参阅复制到托管设备， 第 39 页。

备份

灾难恢复能力是任何系统维护计划的重要组成部分。

备份和恢复可能是一个复杂的过程。您不想跳过任何步骤或忽略安全或许可问题。有关备份和恢复的要求、指南、限制和最佳实践的详细信息，请参阅适用于您的部署的配置指南。



注意 我们强烈建议在升级前和升级后，备份到安全的远程位置并验证传输是否成功。

表 *40:*

	操作/检查
	备份 7000/8000 系列设备。 使用 FMC 备份 7000/8000 系列设备。NGIPSv 不支持备份。 如果支持： • 升级前：如果升级失败是灾难性的，您可能必须重新映像并恢复。重新映像会将大多数设置恢复为出厂默认设置，包括系统密码。如果您有最近的备份，可以更快地恢复正常操作。 • 升级后：这会创建新升级的部署的快照。在 FMC 部署中，我们建议您在升级其受管设备后备份 FMC，以便新的 FMC 备份文件“知道”其设备已升级。

关联升级

由于操作系统和托管环境升级会影响流量和检查，因此请在维护窗口中执行。

表 *41:*

	操作/检查
	升级虚拟主机。 如果需要，请升级任何虚拟设备的托管环境。如果需要执行此操作，通常是因为您运行的是旧版 VMware 并正在执行主要设备升级。

最终检查

一系列最终检查可确保您已准备好升级。

表 *42:*

	操作/检查
	检查配置。 确保您已进行任何必要的升级前配置更改，并准备进行必要的升级后配置更改。

	操作/检查
	检查 NTP 同步。 确保所有设备与您正在使用提供时间的 NTP 服务器进行同步。不同步可能会导致升级失败。在 FMC 部署中，如果时钟不同步超过 10 秒，运行状况模块会发出警报，但您仍应手动进行检查。 要检查时间，请执行以下操作： • FMC：选择**系统 > 配置 > 时间**。 • 设备：使用 **show time** CLI 命令。
	检查硬盘空间。 运行磁盘空间检查进行软件升级。如果可用磁盘空间不足，会导致升级失败。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	部署配置。 在升级前部署配置可减少失败的可能性。在某些部署中，如果您的配置已过期，您可能会被阻止升级。在 FMC 高可用性部署中，您只需从主用对等设备进行部署。 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。 此外，部署某些配置会重启 Snort，这会中断流量检测，并且根据您的设备处理流量的方式，可能会中断流量，直至重启完成。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	运行就绪性检查。 如果 FMC 运行的是版本 6.1.0+，我们建议进行兼容性和就绪性检查。这些检查会评估您是否准备好进行软件升级。 请参阅 Firepower 软件就绪性检查 ， 第 40 页。
	检查正在运行的任务。 在升级之前，请确保设备上的基本任务已完成，包括最终部署。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。我们还建议您检查计划在升级期间运行的任务，并取消或推迟这些任务。

升级带有 FMC 的 Firepower 7000/8000 和 NGIPSv

使用此程序升级 Firepower 7000/8000 系列和 NGIPSv 设备。如果多台设备使用相同的升级软件包，可一次性对这些设备同时进行升级。您必须同时升级设备堆叠和高可用性对的成员。

开始之前

完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。

步骤 1 （可选）交换执行交换/路由的高可用性设备对的主用/备用角色。

如果您部署高可用性对仅为了执行访问控制，请首先进行主用设备升级。升级完成后，主用设备和备用设备保持其原有角色。

但是，在路由或交换部署中，则先进行备用设备升级。设备会交换角色，然后新的备用设备进行升级。升级完成后，设备的角色保持交换后的状态。如果您想要保留主用/备用角色，请先手动交换角色，然后再进行升级。这样，升级流程会将它们交换回来。

选择**设备 (Devices)** > **设备管理 (Device Management)**，点击对等设备旁边的**切换主用设备 (Switch Active Peer)** 图标并确认您的选择。

步骤 2 选择**系统** > **更新**。

步骤 3 点击您想要使用的升级软件包旁边的安装图标，然后选择要升级的设备。

如果您想要升级的设备未列出，则表示您选择了错误的升级软件包。

注释 我们强烈 建议同时从“系统更新”页面升级的设备数不超过五个。不能在所有选定设备完成升级过程之前停止升级。如果任何一个设备升级存在问题，则必须等待所有设备均完成升级，然后才可以解决该问题。

步骤 4 点击**安装 (Install)**，然后确认您要升级并重启设备。

流量在整个升级过程中丢弃还是不进行检测就穿过网络，取决于您的设备的配置和部署方式。有关详细信息，请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。

步骤 5 监控升级进度。

注意 请勿将更改部署到正在升级的设备或部署更改到，手动重启正在升级的设备，或者关闭正在升级的设备。请勿重启正在进行的设备升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

步骤 6 验证升级是否成功。

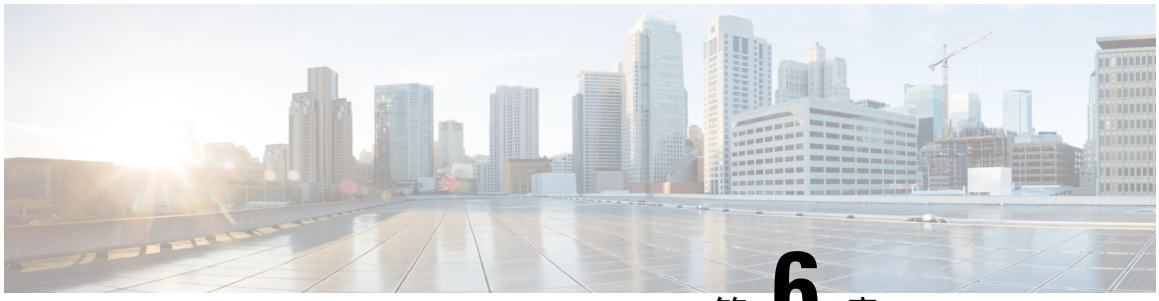
升级过程完成后，选择**设备** > **设备管理**，并确认您升级的设备具有正确的软件版本。

步骤 7 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 8 完成发行说明中所述的任何升级后配置更改。

步骤 9 将配置重新部署到将刚才升级的设备。



第 6 章

升级具备 FirePOWER 服务的 ASA

- 升级核对表：带有 FMC 的 ASA FirePOWER，第 83 页
- 升级 ASA，第 87 页
- 升级带有 FMC 的 ASA FirePOWER 模块，第 107 页

升级核对表：带有 FMC 的 ASA FirePOWER

请在升级 具备 FirePOWER 服务的 ASA 之前填写此核对表。



注释 在此过程中的任何时候，请确保保持部署通信和运行状况。请勿重启正在进行的 ASA FirePOWER 升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

规划和可行性

认真规划和准备可以帮助您避免失误。

表 *43:*

	操作/检查
	计划升级路径。 这对于多设备部署、多跳升级或需要升级操作系统或托管环境，同时还要保持部署兼容性的情况尤其重要。始终了解已经完成的升级和即将执行的升级。 **注释** 在 FMC 部署中，通常先升级 FMC，然后再升级其受管设备。但是，在某些情况下，您可能需要先升级设备。 请参阅升级路径，第 11 页。

	操作/检查
	阅读所有升级指南和计划配置更改。 尤其是对于主要版本升级而言，升级可能会导致您或需要您在升级前或升级后的重大配置更改。从版本说明开始，版本说明包含重要且特定于版本的信息，包括升级警告、行为更改、新功能和弃用的功能以及已知问题。
	检查设备访问。 设备可以在升级期间或在升级失败时停止传输流量（具体取决于接口配置）。升级之前，请确保来自您所在位置的流量不必遍历设备本身即可访问设备的管理界面。在 FMC 部署中，您还必须能够访问 FMC 管理界面而不遍历设备。
	检查带宽。 确保管理网络具有执行大型数据传输的带宽。在 FMC 部署中，如果您在升级时将升级包传输到托管设备，则带宽不足会延长升级时间，甚至导致升级超时。如有可能，请在启动设备升级之前将升级软件包复制到受管设备。 请参阅将数据从 Firepower 管理中心下载到受管设备的准则（故障排除技术说明）。
	安排维护窗口。 考虑对流量和检查的任何影响以及升级可能需要的时间，将维护窗口安排在影响最小的时候。此外，还要考虑您必须在该维护窗口中执行的任务，以及可以提前执行的任务。例如，不要等到维护窗口将升级包复制到设备，运行就绪性检查，执行备份等操作。

升级程序包

思科支持和下载站点上可以获取升级包。

表 44:

	操作/检查
	将升级包上传到 FMC。 请参阅上传到 Firepower 管理中心， 第 37 页。
	将升级包复制到设备。 如果 FMC 运行的是版本 6.2.3+，我们建议您在启动设备升级之前将软件包复制（推送）到受管设备。 请参阅复制到托管设备， 第 39 页。

备份

灾难恢复能力是任何系统维护计划的重要组成部分。

备份和恢复可能是一个复杂的过程。您不想跳过任何步骤或忽略安全或许可问题。有关备份和恢复的要求、指南、限制和最佳实践的详细信息，请参阅适用于您的部署的配置指南。



注意　我们强烈建议在升级前和升级后，备份到安全的远程位置并验证传输是否成功。

表 *45:*

	操作/检查
	备份 ASA。 在升级之前使用 ASDM 或 ASA CLI 备份配置和其他关键文件，尤其是在有 ASA 配置迁移的情况下。

关联升级

由于操作系统和托管环境升级会影响流量和检查，因此请在维护窗口中执行。

表 *46:*

	操作/检查
	升级具备 FirePOWER 服务的 。 如果需要，请升级 ASA。 ASA 与 ASA FirePOWER 版本之间有广泛的兼容性。但通过升级，您可以利用新功能和已解决的问题。 对于独立 ASA 设备，升级 ASA 后立即升级 ASA FirePOWER 模块，然后重新加载。 ASA 集群和故障转移对：为避免流量和检查出现中断，请逐一完全升级这些设备。在重新加载每个设备以升级 ASA 之前，使用升级 ASA FirePOWER 模块。 注释　在升级 ASA 之前，请确保阅读所有升级指南并计划配置更改。从 ASA 版本说明开始：Cisco ASA 发行说明。

最终检查

一系列最终检查可确保您已准备好升级。

表 *47:*

	操作/检查
	检查配置。 确保您已进行任何必要的升级前配置更改，并准备进行必要的升级后配置更改。

	操作/检查
	检查 NTP 同步。 确保所有设备与您正在使用提供时间的 NTP 服务器进行同步。不同步可能会导致升级失败。在 FMC 部署中，如果时钟不同步超过 10 秒，运行状况模块会发出警报，但您仍应手动进行检查。 要检查时间，请执行以下操作： • FMC：选择**系统 > 配置 > 时间**。 • 设备：使用 **show time** CLI 命令。
	检查硬盘空间。 运行磁盘空间检查进行软件升级。如果可用磁盘空间不足，会导致升级失败。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	部署配置。 在升级前部署配置可减少失败的可能性。在某些部署中，如果您的配置已过期，您可能会被阻止升级。在 FMC 高可用性部署中，您只需从主用对等设备进行部署。 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。 此外，部署某些配置会重启 Snort，这会中断流量检测，并且根据您的设备处理流量的方式，可能会中断流量，直至重启完成。 请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。
	在旧服务上禁用 ASA REST API。 在升级当前运行 6.3.0 或更早版本的 ASA FirePOWER 模块之前，确保禁用 ASA REST API。否则，升级可能会失败。从 ASA CLI：`no rest api agent`。可以在升级后重新启用：`rest-api agent`。
	运行就绪性检查。 如果 FMC 运行的是版本 6.1.0+，我们建议进行兼容性和就绪性检查。这些检查会评估您是否准备好进行软件升级。 请参阅 Firepower 软件就绪性检查，第 40 页。
	检查正在运行的任务。 在升级之前，请确保设备上的基本任务已完成，包括最终部署。在升级开始时运行的任务会停止，成为失败的任务，且不能恢复。我们还建议您检查计划在升级期间运行的任务，并取消或推迟这些任务。

升级 ASA

使用本部分中的程序为独立、故障转移或集群部署升级 ASA 和 ASDM。

升级独立设备

使用 CLI 或 ASDM 升级独立设备。

使用 CLI 升级独立设备

本部分介绍如何安装 ASDM 和 ASA 映像，以及何时升级 ASA FirePOWER 模块。

开始之前

此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

步骤 1 在特权 EXEC 模式下，将 ASA 软件复制到闪存。

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```

步骤 2 将 ASDM 映像复制到闪存中。

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

步骤 3 访问全局配置模式。

configure terminal

示例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

步骤 4 显示当前配置的启动映像（最多 4 个）：

show running-config boot system

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像URL。

示例：

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

步骤 5 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 6 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n***:/**[路径/]*asa_image_name*

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

示例：

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

步骤 7 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

示例：

```
ciscoasa(config)# asdm image disk0:/asdm-7121.bin
```

步骤 8 将新设置保存至启动配置：

write memory

步骤 9 重新加载 ASA：

reload

步骤 10 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则升级将失败。

no rest-api agent

您可以在升级后重新启用它：

rest-api agent

注释 如果您运行的是 FirePOWER 模块 6.0 或更高版本，则 ASA 5506-X 系列不支持 ASA REST API。

步骤 11 升级 ASA FirePOWER 模块。

使用 ASDM 从本地计算机升级独立设备

使用**本地计算机中的升级软件**工具，可将映像文件从计算机上传到闪存文件系统来升级 ASA。

步骤 1 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 2 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 3 在**本地文件路径**字段中，点击**浏览本地文件**以查找您的 PC 上的文件。

步骤 4 在**闪存文件系统路径**字段中，点击**浏览闪存**以在闪存文件系统中查找目录或文件。

步骤 5 点击**上传映像**。

上传过程可能需要数分钟。

步骤 6 系统会提示您将此映像设置为 ASDM 映像。点击**是**。

步骤 7 系统会提示您退出 ASDM 并保存配置。点击**确定**。

您会退出 **Upgrade** 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新连接到 ASDM。

步骤 8 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。您也可以使用此程序上传其他文件类型。

步骤 9 依次选择**工具** > **重新加载系统**以重新加载 ASA。

系统将显示新窗口，要求您确认重新加载的详细信息。

a) 点击**重新加载时保存运行配置**单选按钮（默认）。
b) 选择重新加载的时间（例如，默认值 **Now**）。
c) 点击**计划重新加载**。

重新加载开始后，系统将显示**重新加载状态**窗口，指示正在执行重新加载。系统还提供了退出 ASDM 的选项。

步骤 10 在 ASA 重新加载后，重启 ASDM。

您可以从控制台端口检查重新加载状态，也可以等待几分钟，并尝试使用 ASDM 进行连接，直到成功。

步骤 11 如果要升级 ASA FirePOWER 模块，请通过选择**工具** > **命令行界面**，然后输入 **no rest-api agent** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。您可以在升级后重新启用它：

rest-api agent

注释 如果您运行的是 FirePOWER 模块 6.0 或更高版本，则 ASA 5506-X 系列不支持 ASA REST API。

步骤 12 升级 ASA FirePOWER 模块。

使用 ASDM Cisco.com 向导升级独立设备

Cisco.com 向导中的升级软件工具允许您将 ASDM 和 ASA 自动升级至更加新的版本。

在此向导中，您可以执行以下操作：

- 选择 ASA 映像文件和/或 ASDM 映像文件以执行升级。



注释 ASDM 会下载最新的映像版本，其版本号包括内部版本号。例如，如果要下载 9.9(1)，则下载可能是 9.9(1.2)。这是预期行为，因此您可以继续执行计划的升级。

- 查看您所做的升级更改。
- 下载一个或多个映像，并进行安装。
- 查看安装的状态。
- 如果安装成功完成，请重新加载 ASA 以保存配置并完成升级。

开始之前

由于内部更改，此向导仅支持使用 ASDM 7.10(1) 及更高版本；此外，由于映像命名更改，您必须使用 ASDM 7.12(1) 或更高版本以升级到 ASA 9.10(1) 及更高版本。由于 ASDM 向后兼容较早的 ASA 版本，因此您可以升级 ASDM，无论您运行的是哪个 ASA 版本。

步骤 1 依次选择**工具** > **检查 ASA/ASDM 更新**。

在多情景模式中，从“系统”访问此菜单。

系统将显示 **Cisco.com 身份验证**对话框。

步骤 2 输入 Cisco.com 用户名和密码，然后点击 **Login**。

系统将显示 **Cisco.com 升级向导**。

注释 如果无可用升级，系统将显示对话框。点击**确定**退出向导。

步骤 3 点击**下一步**显示**选择软件**屏幕。

系统将显示当前的 ASA 版本和 ASDM 版本。

步骤 4 如要升级 ASA 版本和 ASDM 版本，请执行以下步骤：

a) 在 **ASA** 区域，选中**升级到**复选框，然后从下拉列表中选择要升级的目标 ASA 版本。

b) 在 **ASDM** 区域，选中**升级到**复选框，然后从下拉列表中选择要升级的目标 ASDM 版本。

步骤 5 点击**下一步**，显示**检查更改**屏幕。

步骤 6 请验证以下项目：

- 已下载的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
- 希望上传的文件是正确的 ASA 映像文件和/或 ASDM 映像文件。
- 已选择正确的 ASA 启动映像。

步骤 7 点击**下一步**，开始升级安装。

然后，您可以在升级安装过程中查看其状态。

系统将显示**结果**屏幕，其中提供详细信息，如升级安装状态（成功或失败）。

步骤 8 如果升级安装成功，为了使升级版本生效，请选中 **Save configuration and reload device now** 复选框来重新启动 ASA，然后重新启动 ASDM。

步骤 9 点击**完成**，退出向导，保存对配置的更改。

注释 如要升级到下一个较高版本（如可用），您必须重新启动向导。

步骤 10 在 ASA 重新加载后，重启 ASDM。

您可以从控制台端口检查重新加载状态，也可以等待几分钟，并尝试使用 ASDM 进行连接，直到成功。

步骤 11 如果要升级 ASA FirePOWER 模块，请通过选择**工具** > **命令行界面**，然后输入 **no rest-api agent** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。您可以在升级后重新启用它：

rest-api agent

注释 如果您运行的是 FirePOWER 模块 6.0 或更高版本，则 ASA 5506-X 系列不支持 ASA REST API。

步骤 12 升级 ASA FirePOWER 模块。

升级主用/备用故障转移对

使用 CLI 或 ASDM 升级主用/备用故障转移对，以实现零停机升级。

使用 CLI 升级主用/备用故障转移对

要升级主用/备用故障转移对，请执行以下步骤。

开始之前

- 在主用设备上执行以下步骤。对于 SSH 访问，请连接到主用 IP 地址；主用设备始终拥有此 IP 地址。当连接到 CLI 时，通过查看 ASA 提示符确定故障转移状态；您可以配置 ASA 提示符以显示故障转移状态和优先级（主设备或辅助设备），这可用于确定连接到的设备。请参阅 prompt 命令。或者，输入 **show failover** 命令，以查看此设备的状态和优先级（主设备或辅助设备）。
- 此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

步骤 1 在主用设备的特权 EXEC 模式下，将 ASA 软件复制到主用设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

步骤 2 将软件复制到备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
disk0:/asa9829-15-1-smp-k8.bin
```

步骤 3 将 ASDM 映像复制至主用设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.bin
```

步骤 4 将 ASDM 映像复制至备用设备；请确保指定与主用设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

步骤 5 如果您当前未处于全局配置模式，请访问全局配置模式：

configure terminal

步骤 6 显示当前配置的启动映像（最多 4 个）：

show running-config boot system

示例：

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像URL。

步骤 7 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 8 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/act(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

步骤 9 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act(config)# asdm image disk0:/asdm-77178271417151.bin
```

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

步骤 10 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到备用设备上。

步骤 11 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则升级将失败。

no rest-api agent

步骤 12 升级备用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成。

步骤 13 重新加载备用设备，以便启动新映像：

failover reload-standby

等待备用设备完成加载。使用 **show failover** 命令确认备用设备处于备用就绪状态。

步骤 14 强行要求主用设备故障转移至备用设备。

no failover active

如果您从 SSH 会话中断开连接，请重新连接到主 IP 地址（现位于新的主用/以前的备用设备上）。

步骤 15 升级以前主用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成。

步骤 16 在新的主用设备上，重新加载以前的主用设备（现为新的备用设备）。

failover reload-standby

示例：

```
asa/act# failover reload-standby
```

注释　如果连接到以前的主用设备控制台端口，应改为输入 **reload** 命令来重新加载以前的主用设备。

使用 ASDM 升级主用/备用故障转移对

要升级主用/备用故障转移对，请执行以下步骤。

开始之前

将 ASA 和 ASDM 映像放置在本地管理计算机上。

步骤 1　通过连接到备用 IP 地址，在备用 设备上启动 ASDM。

步骤 2　在主 ASDM 应用窗口中，依次选择**工具 (Tools)** > **从本地计算机升级软件 (Upgrade Software from Local Computer)**。

系统将显示**升级软件**对话框。

步骤 3　从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 4　在**本地文件路径 (Local File Path)** 字段中，输入指向计算机中文件的本地路径，或者点击**浏览本地文件 (Browse Local Files)** 在计算机中查找该文件。

步骤 5　在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在 Flash 文件系统中查找目录或文件。

步骤 6　点击**上传映像 (Upload Image)**。上传过程可能需要数分钟。

系统提示您将此映像设置为 ASDM 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 7　重复这些步骤，从**要上传的映像**下拉列表中选择 **ASA**。

当系统提示您将此映像设置为 ASA 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 8　通过连接到主 IP 地址，将 ASDM 连接到主用 设备，然后使用与您用于备用设备相同的文件位置上传 ASDM 软件。

步骤 9　当系统提示您将该映像设置为 ASDM 映像时，点击**是 (Yes)**。

系统会提示您退出 ASDM 并保存配置。点击**确定 (OK)**。您会退出 Upgrade 工具。**注意：**在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10　使用与备用设备相同的文件位置上传 ASA 软件。

步骤 11　当系统提示您将该映像设置为 ASA 映像时，点击**是 (Yes)**。

系统将提示您重新加载 ASA 以使用新映像。点击**确定 (OK)**。您会退出 Upgrade 工具。

步骤 12　点击工具栏上的**保存**图标，保存配置更改。

这些配置更改将自动保存在备用设备上。

步骤 13 如果要升级 ASA FirePOWER 模块，请选择**工具** > **命令行界面**，然后输入 **no rest-api enable** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。

步骤 14 升级备用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成后，将 ASDM 连接回主用设备。

步骤 15 通过依次选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**重新加载备用 (Reload Standby)**，重新加载备用设备。

留在**系统**窗格中，以监控备用设备何时重新加载。

步骤 16 重新加载备用设备后，强制主用设备执行故障转移到备用设备，方法为：选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**设为备用 (Make Standby)**。

ASDM 将自动重新连接到新主用设备。

步骤 17 升级以前主用设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到备用 管理 IP 地址。等待升级完成后，将 ASDM 连接回主用设备。

步骤 18 重新加载（新）备用设备，方法为：选择**监控 (Monitoring)** > **属性 (Properties)** > **故障转移 (Failover)** > **状态 (Status)**，然后点击**重新加载备用 (Reload Standby)**。

升级主用/主用故障转移对

使用 CLI 或 ASDM 升级主用/主用故障转移对，以实现零停机升级。

使用 CLI 升级主用/主用故障转移对

要升级主用/主用故障转移配置中的两台设备，请执行以下步骤。

开始之前

- 在主设备上执行这些步骤。
- 在系统执行空间中执行以下步骤。
- 此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

步骤 1 在主设备的特权 EXEC 模式下，将 ASA 软件复制到闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

步骤 2 将软件复制至辅助设备；请确保指定与主设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
 disk0:/asa9829-15-1-smp-k8.bin
```

步骤 3 将 ASDM 映像复制至主设备闪存：

copy ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

步骤 4 将 ASDM 映像复制到辅助设备中；务必指定与主设备相同的路径：

failover exec mate copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

步骤 5 如果您当前未处于全局配置模式，请访问全局配置模式：

configure terminal

步骤 6 显示当前配置的启动映像（最多 4 个）：

show running-config boot system

示例：

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像URL。

步骤 7 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n*:/[路径/]*asa_image_name*

示例：

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 8 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n*:/[路径/]*asa_image_name*

示例：

```
asa/act/pri(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

步骤 9 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n*:/[路径/]*asdm_image_name*

示例：

```
asa/act/pri(config)# asdm image disk0:/asdm-77178271417151.bin
```

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

步骤 10 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到辅助设备上。

步骤 11 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则升级将失败。

no rest-api agent

步骤 12 使两个故障转移组在主设备上均处于活动状态：

failover active group 1

failover active group 2

示例：

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

步骤 13 升级辅助设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成。

步骤 14 重新加载辅助设备，以便启动新映像：

failover reload-standby

等待辅助设备完成加载。使用 **show failover** 命令确认两个故障转移组均处于备用就绪状态。

步骤 15 强行要求两个故障转移组在辅助设备上变为活动状态：

no failover active group 1

no failover active group 2

示例：

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

如果您从 SSH 会话中断开连接，请重新连接到故障转移组 1 IP 地址（现位于辅助设备上）。

步骤 16 升级主设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成。

步骤 17 重新加载主设备：

failover reload-standby

示例：

```
asa/act/sec# failover reload-standby
```

注释　如果已连接到主设备控制台端口，应改为输入 **reload** 命令来重新加载主设备。

您可能从 SSH 会话中断开连接。

步骤 18 如果故障转移组配置了 **preempt** 命令，则抢占延迟过后，它们将在其指定设备上自动变为主用状态。

使用 ASDM 升级主用/主用故障转移对

要升级主用/主用故障转移配置中的两台设备，请执行以下步骤。

开始之前

- 在系统执行空间中执行以下步骤。
- 将 ASA 和 ASDM 映像放置在本地管理计算机上。

步骤 1 通过连接到故障转移组 2 中的管理地址，在辅助 设备上启动 ASDM。

步骤 2 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**升级软件**对话框。

步骤 3 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 4 在**本地文件路径 (Local File Path)** 字段中，输入指向计算机中文件的本地路径，或者点击**浏览本地文件 (Browse Local Files)** 在 PC 中查找文件。

步骤 5 在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在闪存文件系统中查找目录或文件。

步骤 6 点击**上传映像 (Upload Image)**。上传过程可能需要数分钟。

系统提示您将此映像设置为 ASDM 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 7 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。

当系统提示您将此映像设置为 ASA 映像时，点击**否 (No)**。您会退出 Upgrade 工具。

步骤 8 通过连接至故障转移组 1 中的管理 IP 地址，将 ASDM 连接至主设备，并使用辅助设备上所用的相同文件位置上传 ASDM 软件。

步骤 9 当系统提示您将该映像设置为 ASDM 映像时，点击**是 (Yes)**。

系统会提示您退出 ASDM 并保存配置。点击**确定 (OK)**。您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10 使用与辅助设备相同的文件位置上传 ASA 软件。

步骤 11 当系统提示您将该映像设置为 ASA 映像时，点击**是 (Yes)**。

系统将提示您重新加载 ASA 以使用新映像。点击**确定 (OK)**。您会退出 Upgrade 工具。

步骤 12 点击工具栏上的**保存**图标，保存配置更改。

这些配置更改在辅助设备上会自动保存。

步骤 13 如果要升级 ASA FirePOWER 模块，请选择**工具 > 命令行界面**，然后输入 **no rest-api enable** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。

步骤 14 通过选择**监控 (Monitoring) > 故障转移 (Failover) > 故障转移组号 (Failover Group #)**（其中**组号**是您要移动至主设备的故障转移组的编号）并点击**设为主用 (Make Active)**，使两个故障转移组在主设备上均处于活动状态。

步骤 15 升级辅助设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成后，将 ASDM 连接回主设备。

步骤 16 重新加载辅助设备，方法为：选择**监控 (Monitoring) > 故障转移 (Failover) > 系统 (System)**，然后点击**重新加载备用 (Reload Standby)**。

保持在**系统**窗格上，以监控辅助设备何时加载。

步骤 17 辅助设备启动后，通过选择**监控 (Monitoring) > 故障转移 (Failover) > 故障转移组号 (Failover Group #)**（其中**组号**是您要移动至辅助设备的故障转移组的编号）并点击**设为备用 (Make Standby)**，使两个故障转移组在辅助设备上均处于活动状态。

ASDM 将自动重新连接到辅助设备上的故障转移组 1 IP 地址。

步骤 18 升级主设备上的 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到故障转移组 1 或 2 的备用管理 IP 地址。等待升级完成后，将 ASDM 连接回辅助设备。

步骤 19 重新加载主设备，方法为：选择**监控 (Monitoring)** > **故障转移 (Failover)** > **系统 (System)**，然后点击**重新加载备用 (Reload Standby)**。

步骤 20 如果故障转移组被配置为“启用抢占”，在抢占延迟过后，它们会在其指定设备上自动变为活动状态。ASDM 将自动重新连接到主设备上的故障转移组 1 IP 地址。

升级 ASA 集群

使用 CLI 或 ASDM 升级 ASA 集群，以实现零停机升级。

使用 CLI 升级 ASA 集群

要升级 ASA 集群中的所有设备，请执行以下步骤。此程序使用 FTP。对于 TFTP、HTTP 或其他服务器类型，请参阅 ASA 命令参考中的 **copy** 命令。

开始之前

- 在控制单元上执行这些步骤。如果您还要升级 ASA FirePOWER 模块，则需要在每台数据单元上访问控制台或ASDM。您可以将ASA提示符配置为显示集群设备和状态（控制或数据），这些信息有助于确定您连接的目标设备。请参阅 prompt 命令。或者，输入 **show cluster info** 命令以查看每台设备的角色。
- 您必须使用控制台端口；不能通过远程 CLI 连接启用或禁用集群。
- 对于多情景模式，在系统执行空间中执行以下步骤。

步骤 1 在特权 EXEC 模式下，将控制单元的上的 ASA 软件复制到集群中的所有设备。

cluster exec copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asa_image_name* **disk***n***:/**[路径/]*asa_image_name*

示例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

步骤 2 将 ASDM 映像复制至集群中的所有设备：

cluster exec copy /noconfirm ftp://[[用户[**:**密码]**@**]服务器[/路径]/*asdm_image_name* **disk***n***:/**[路径/]*asdm_image_name*

示例：

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
 disk0:/asdm-77178271417151.bin
```

步骤 3 如果您当前未处于全局配置模式，请立即访问该模式。

configure terminal

示例：

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

步骤 4 显示当前配置的引导映像（最多 4 个）。

show running-config boot system

示例：

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

ASA 按列示顺序使用映像；如果第一个映像不可用，则使用下一个映像，以此类推。不能在列表顶部插入新映像URL；要将新的映像指定为第一个映像，必须删除所有现有条目，再根据后续步骤按所需顺序输入映像URL。

步骤 5 删除所有现有的引导映像配置，以便将新的引导映像作为首选输入：

no boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```

步骤 6 将 ASA 映像设置为引导映像（您刚上传的映像）：

boot system disk*n***:/**[路径/]*asa_image_name*

示例：

```
asa/unit1/master(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

如果此映像不可用，请对要使用的任何备份映像重复执行此命令。例如，您可以重新输入以前删除的映像。

步骤 7 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image disk*n***:/**[路径/]*asdm_image_name*

示例：

```
asa/unit1/master(config)# asdm image disk0:/asdm-77178271417151.bin
```

您只能配置一个要使用的 ASDM 映像，因此您不需要先删除现有配置。

步骤 8 将新设置保存至启动配置：

write memory

这些配置更改会自动保存到数据单元。

步骤 9 如果您要升级 ASA FirePOWER 模块，请禁用 ASA REST API，否则 ASA FirePOWER 模块升级将失败。

no rest-api agent

步骤 10 如果您要升级由 ASDM 管理的 ASA FirePOWER 模块，就需要将 ASDM 连接到单个 管理 IP 地址，因此您需要记下每台设备的 IP 地址。

show running-config interface *management_interface_id*

记下使用的 **cluster-pool** 池名称。

show ip[**v6**] **local pool** 池名称

记下集群设备的 IP 地址。

示例：

```
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin           End             Mask            Free     Held     In use
10.86.118.16    10.86.118.17    255.255.252.0       0        0        2

Cluster Unit                    IP Address Allocated
unit2                           10.86.118.16
unit1                           10.86.118.17
asa1/unit2/slave#
```

步骤 11 升级数据单元。

选择下面的程序，具体取决于您是否还要升级 ASA FirePOWER 模块。如果也需要升级 ASA FirePOWER 模块，ASA FirePOWER 程序可以最大限度地减少 ASA 重新加载的次数。您可以在执行这些程序时选用数据单元控制台或 ASDM。如果您还无权访问所有控制台端口，但可以通过网络访问 ASDM，则可能需要使用 ASDM 而不是控制台。

注释 在升级过程中，切勿使用 **cluster master unit** 命令强制将某个数据单元变为控制单元；否则可能导致网络连接和集群稳定相关的问题。您必须先升级并重新加载所有数据单元，然后继续此过程以确保从当前控制单元顺利地过渡到新的控制单元。

如果不进行 ASA FirePOWER 模块升级：

a) 在控制单元上，要查看成员名称，请输入 **cluster exec unit ?**，或输入 **show cluster info** 命令。

b) 重新加载数据单元。

cluster exec unit *data-unit* **reload noconfirm**

示例：

```
asa/unit1/master# cluster exec unit unit2 reload noconfirm
```

c) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备何时重新加入集群，请输入 **show cluster info**。

如果还要进行 ASA FirePOWER 模块升级（使用数据控制台）：

a) 连接到数据单元的控制台端口，然后进入全局配置模式。

enable

configure terminal

示例：

```
asa/unit2/slave> enable
Password:
asa/unit2/slave# configure terminal
asa/unit2/slave(config)#
```

b) 禁用集群。

cluster group *name*

no enable

不保存此配置；您希望在重新加载时启用集群。您需要禁用集群，以避免在升级过程中出现多次失败和重新加入；此设备应仅在所有升级和重新加载过程完成后才进行重新加入。

示例：

```
asa/unit2/slave(config)# cluster group cluster1
asa/unit2/slave(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#
```

c) 在此数据单元上升级 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到您之前记下的单个 管理 IP 地址。等待升级完成。

d) 重新加载数据单元。

reload noconfirm

e) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备何时重新加入集群，请输入 **show cluster info**。

如果还要进行 ASA FirePOWER 模块升级（使用 ASDM）：

a) 将 ASDM 连接到您之前记下的此数据单元的单个 管理 IP 地址。

b) 依次选择**配置** > **设备管理高可用性和可扩展性** > **ASA 集群** > **集群配置** > 。

c) 取消选中**加入 ASA 集群**复选框。

您需要禁用集群，以避免在升级过程中出现多次失败和重新加入；此设备应仅在所有升级和重新加载过程完成后才进行重新加入。

请勿取消选中**配置 ASA 集群设置**复选框，此操作会清除所有集群配置并关闭所有接口，包括 ASDM 连接到的管理接口。在此情况下，要恢复连接，您需要在控制台端口上访问 CLI。

注释 某些旧版本的 ASDM 不支持在此屏幕上禁用集群；在此情况下，请使用**工具** > **命令行界面**工具，点击**多行**单选按钮，然后输入 **cluster group** 名称 和 **no enable**。您可以在**主页** > **设置控制面板** > **设备信息** > **ASA 集群**区域中查看集群组名称。

d) 点击**应用**。

e) 系统会提示您退出 ASDM。将 ASDM 重新连接到相同的 IP 地址。

f) 升级 ASA FirePOWER 模块。

等待升级完成。

g) 在 ASDM 中，选择**工具** > **系统重新加载**。

h) 点击**重新加载而不保存运行配置**单选按钮。

请勿保存配置；在主设备重新加载后，您需要在其上启用集群。

i) 点击**计划重新加载**。

j) 请点击**是**继续重新加载。

k) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备重新加入集群的时间，请查看控制单元上的**监控** > **ASA 集群** > **集群摘要**窗格。

步骤 12 升级控制单元。

a) 禁用集群。

cluster group *name*

no enable

最多等待 5 分钟，以便选择新的控制单元且流量稳定下来。

不保存此配置；您希望在重新加载时启用集群。

我们建议在控制单元上手动禁用集群（如果可能），以便尽可能快速顺畅地选择新的控制单元。

示例：

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable
clustering or remove cluster group configuration.

Cluster unit unit1 transitioned from MASTER to DISABLED
```

```
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) 在此设备上升级 ASA FirePOWER 模块。

对于 ASDM 管理的 ASA FirePOWER 模块，请将 ASDM 连接到您之前记下的单个 管理 IP 地址。主集群 IP 地址现在属于新的控制单元；此以前的控制单元仍可通过其单独的管理 IP 地址进行访问。

等待升级完成。

c) 重新加载此设备。

reload noconfirm

当以前的控制单元重新加入集群时，它将成为数据单元。

使用 ASDM 升级 ASA 集群

要升级 ASA 集群中的所有设备，请执行以下步骤。

开始之前

- 在控制单元上执行这些步骤。如果您还要升级 ASA FirePOWER 模块，则需要 ASDM 访问每台数据单元。
- 对于多情景模式，在系统执行空间中执行以下步骤。
- 将 ASA 和 ASDM 映像放置在本地管理计算机上。

步骤 1 通过连接到主集群 IP 地址，在控制单元上启动 ASDM。

此 IP 地址始终属于控制单元。

步骤 2 在主 ASDM 应用窗口中，依次选择**工具** > **从本地计算机升级软件**。

系统将显示**从本地计算机升级软件**对话框。

步骤 3 点击**集群中的所有设备 (All devices in the cluster)** 单选按钮。

系统将显示**升级软件**对话框。

步骤 4 从**要上传的映像**下拉列表中选择 **ASDM**。

步骤 5 在**本地文件路径 (Local File Path)** 字段中，点击**浏览本地文件 (Browse Local Files)** 以查找您计算机上的文件。

步骤 6 （可选）在 **Flash 文件系统路径 (Flash File System Path)** 字段中，输入闪存文件系统的路径，或者点击**浏览 Flash (Browse Flash)** 在闪存文件系统中查找目录或文件。

默认情况下，此字段预先填充有以下路径：**disk0:/***filename*。

步骤 7 点击**上传映像 (Upload Image)**。上传过程可能需要数分钟。

步骤 8 系统会提示您将此映像设置为 ASDM 映像。点击**是 (Yes)**。

步骤 9 系统会提示您退出 ASDM 并保存配置。点击**确定 (OK)**。

您会退出 Upgrade 工具。**注意**：在升级 ASA 软件之后，您将保存配置并重新加载 ASDM。

步骤 10 重复上述步骤，从**要上传的映像**下拉列表中选择 **ASA**。

步骤 11 点击工具栏上的**保存**图标，保存配置更改。

这些配置更改会自动保存到数据单元。

步骤 12 请记下**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群** > **集群成员**上每个设备的单独管理 IP 地址，以便您以后可以将 ASDM 直接连接到数据单元。

步骤 13 如果要升级 ASA FirePOWER 模块，请选择**工具** > **命令行界面**，然后输入 **no rest-api enable** 以禁用 ASA REST API。

如果不禁用 REST API，ASA FirePOWER 模块升级将会失败。

步骤 14 升级数据单元。

选择下面的程序，具体取决于您是否还要升级 ASA FirePOWER 模块。ASA FirePOWER 程序最大程度减少了升级 ASA FirePOWER 模块时的 ASA 重新加载次数。

注释 在升级过程中，请勿使用**监控** > **ASA 集群** > **集群摘要**将控制单元更改为页面强制数据单元成为控制单元；否则会导致网络连接性和集群稳定性相关的问题。您必须先重新加载所有数据单元，然后继续此过程以确保从当前控制单元顺利地过渡到新的控制单元。

如果不进行 ASA FirePOWER 模块升级：

a) 在控制单元上，选择**工具** > **系统重新加载**。
b) 从**设备**下拉列表中，选择数据单元名称。
c) 点击**计划重新加载 (Schedule Reload)**。
d) 请点击**是 (Yes)** 继续重新加载。
e) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备重新加入集群的时间，请查看**监控** > **ASA 集群** > **集群摘要**窗格。

如果还要进行 ASA FirePOWER 模块升级：

a) 在控制单元上，选择**配置** > **设备管理** > **高可用性和稳定性** > **ASA 集群** > **集群成员**。
b) 选择要升级的数据单元，然后点击**删除 (Delete)**。
c) 点击**应用 (Apply)**。
d) 退出 ASDM，然后通过连接到您之前记下的单个管理 IP 地址，将 ASDM 连接到数据单元。
e) 升级 ASA FirePOWER 模块。

等待升级完成。

f) 在 ASDM 中，选择**工具** > **系统重新加载**。
g) 点击**重新加载而不保存运行配置 (Reload without saving the running configuration)** 单选按钮。

请勿保存配置；在主设备重新加载后，您需要在其上启用集群。

h) 点击**计划重新加载 (Schedule Reload)**。
i) 请点击**是 (Yes)** 继续重新加载。
j) 对每个从属数据单元上述操作。

为避免失去连接并使流量稳定下来，请等待每个设备恢复运行并重新加入集群（大约需要 5 分钟），然后再对下一个设备重复执行上述步骤。要查看设备重新加入集群的时间，请查看**监控** > **ASA 集群** > **集群摘要**窗格。

步骤 15 升级控制单元。

a) 在控制单元上的 ASDM 中，选择**配置** > **设备管理** > **高可用性和可扩展性** > **ASA 集群** > **集群配置**窗格。
b) 取消选中**加入 ASA 集群 (Participate in ASA cluster)** 复选框，然后点击**应用 (Apply)**。

系统会提示您退出 ASDM。

c) 最多等待 5 分钟，以便选择新的控制单元且流量稳定下来。

当以前的控制单元重新加入集群时，它将成为数据单元。

d) 通过连接到您之前记下的单个 管理 IP 地址，将 ASDM 重新连接到之前的控制单元。

主集群 IP 地址现在属于新的控制单元；此以前的控制单元仍可通过其单独的管理 IP 地址进行访问。

e) 升级 ASA FirePOWER 模块。

等待升级完成。

f) 依次选择**工具** > **重新加载系统**。
g) 点击**重新加载而不保存运行配置 (Reload without saving the running configuration)** 单选按钮。

请勿保存配置；在主设备重新加载后，您需要在其上启用集群。

h) 点击**计划重新加载 (Schedule Reload)**。
i) 请点击**是 (Yes)** 继续重新加载。

系统会提示您退出 ASDM。在主集群 IP 地址上重启 ASDM；您将重新连接到新的控制单元。

升级带有 FMC 的 ASA FirePOWER 模块

使用此程序升级由 FMC 管理的 ASA FirePOWER 模块。何时升级模块取决于是否升级 ASA，以及 ASA 部署。

- 独立 ASA 设备：如果您同时还在升级 ASA，请在升级 ASA 后立即升级 ASA FirePOWER 模块，然后重新加载。
- ASA 集群和故障转移对：为避免流量和检查出现中断，请逐一完全升级这些设备。如果还要升级 ASA，请在重新加载每个单元以升级 ASA 之前升级 ASA FirePOWER 模块。

有关详细信息，请参阅 升级路径： ASA FirePOWER，第 22 页 和 ASA 升级程序。

开始之前

完成预升级核对表。确保部署中的设备保持正常运行，并且能够成功通信。

步骤 1 选择**系统** > **更新**。

步骤 2 点击您想要使用的升级软件包旁边的安装图标，然后选择要升级的设备。

如果您想要升级的设备未列出，则表示您选择了错误的升级软件包。

注释 我们强烈 建议同时从“系统更新”页面升级的设备数不超过五个。不能在所有选定设备完成升级过程之前停止升级。如果任何一个设备升级存在问题，则必须等待所有设备均完成升级，然后才可以解决该问题。

步骤 3 点击**安装 (Install)**，然后确认您要升级并重启设备。

流量在整个升级过程中丢弃还是不进行检测就穿过网络，取决于您的设备的配置和部署方式。有关详细信息，请参阅目标版本的Cisco Firepower 发行说明中的升级软件一章。

步骤 4 监控升级进度。

注意 请勿将更改部署到正在升级的设备或部署更改到，手动重启正在升级的设备，或者关闭正在升级的设备。请勿重启正在进行的设备升级。升级过程在预检查期间可能会显示为非活动；这是预期行为。如果您遇到升级问题，升级失败的升级或无响应的设备，请联系 Cisco TAC。

步骤 5 验证升级是否成功。

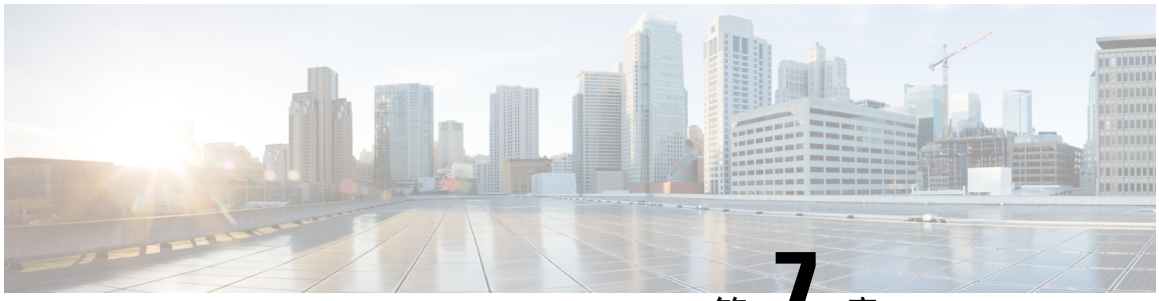
升级过程完成后，选择**设备** > **设备管理**，并确认您升级的设备具有正确的软件版本。

步骤 6 更新入侵规则 (SRU/LSP) 和漏洞数据库 (VDB)。

如果 思科支持和下载站点 上提供的组件比当前运行的版本新，请安装新版本。请注意，在更新入侵规则时，不需要自动重新应用策略。您可以稍后执行该操作。

步骤 7 完成发行说明中所述的任何升级后配置更改。

步骤 8 将配置重新部署到将刚才升级的设备。



第 7 章

卸载补丁 (Uninstall a Patch)

您可以卸载大多数补丁。如果您需要返回到较早的主版本或维护版本，则必须重新映像。

卸载补丁会返回到之前升级的版本，并且不会更改配置。由于FMC必须运行与其受管设备相同或更高的版本，因此请先从设备卸载补丁。修复程序不支持卸载。

- 支持卸载的补丁，第 109 页
- 高可用性/可扩展性的卸载顺序，第 112 页
- 通过 FMC 卸载设备补丁，第 113 页
- 卸载独立 FMC 补丁 ，第 115 页
- 卸载高可用性 FMC 补丁，第 116 页

支持卸载的补丁

卸载特定补丁可能会导致问题，即使卸载本身成功也是如此。这些问题包括：

- 卸载后无法部署配置更改。
- 操作系统与软件之间的不兼容性。
- 如果您在启用安全认证合规性的情况下安装补丁（CC/UCAPL模式），则设备重新启动时FSIC（文件系统完整性检查）失败。

⚠

注意 如果启用了安全认证合规性并且 FSIC 失败，则软件无法启动，远程 SSH 访问会被禁用，并且您只能通过本地控制台访问该设备。如果出现此情况，请联系Cisco TAC。

支持卸载的版本 7.0 补丁

对于所有版本 7.0 的补丁，目前都支持卸载。

支持卸载的 6.7 版补丁

对于所有版本 6.7 的补丁，目前都支持卸载。

支持卸载的 6.6 版补丁

对于所有版本 6.6 的补丁，目前都支持卸载。

支持卸载的 6.5 版补丁

此表列出了版本 6.5 补丁支持的卸载场景。卸载会使您返回到之前升级的补丁级别。如果卸载后的时间比支持的要长，我们建议您重新映像，然后再升级到所需的补丁级别。

表 *48:* 支持卸载的版本 *6.5.0* 补丁

当前版本	您应该卸载的最早版本		
	FTD/FTDv	**ASA FirePOWER** **NGIPSv**	**FMC/FMCv**
6.5.0.2+	6.5.0	6.5.0	6.5.0.1
6.5.0.1	6.5.0	6.5.0	—

支持卸载的版本 6.4 补丁

此表列出了版本 6.4 补丁支持的卸载场景。卸载会让您返回到之前升级的补丁级别。如果卸载后的时间比支持的要长，我们建议您重新映像，然后再升级到所需的补丁级别。

表 *49:* 支持卸载的版本 *6.4.0* 补丁

当前版本	您应该卸载的最早版本		
	FTD/FTDv	**Firepower 7000/8000** **ASA FirePOWER** **NGIPSv**	**FMC/FMCv**
6.4.0.5+	6.4.0.4	6.4.0.4	6.4.0.4
6.4.0.4	-	-	-
6.4.0.3	6.4.0	-	-
6.4.0.2	6.4.0	-	-
6.4.0.1	6.4.0	6.4.0	6.4.0

支持卸载的版本 6.3 补丁

此表列出了版本 6.3 补丁支持的卸载场景。卸载会使您返回到之前升级的补丁级别。如果卸载后的时间比支持的要长，我们建议您重新映像，然后再升级到所需的补丁级别。

表 *50:* 支持卸载的版本 *6.3.0* 补丁

当前版本	您应该卸载的最早版本
6.3.0.5	-
6.3.0.1 至 6.3.0.4	6.3.0

支持卸载的版本 6.2.3 补丁

此表列出了版本6.2.3 补丁支持的卸载场景。卸载会使您返回到之前升级的补丁级别。如果卸载后的时间比支持的要长，我们建议您重新映像，然后再升级到所需的补丁级别。

表 *51:* 支持卸载的版本 *6.2.3* 补丁

当前版本	您应该卸载的最早版本		
	FTD/FTDv	**Firepower 7000/8000** **ASA FirePOWER** **NGIPSv**	**FMC/FMCv**
6.2.3.16+	6.2.3.15	6.2.3.15	6.2.3.15
6.2.3.15	-	-	-
6.2.3.12 至 6.2.3.14	6.2.3	6.2.3.11	6.2.3.11
6.2.3.11	6.2.3	-	-
6.2.3.8 至 6.2.3.10	6.2.3	6.2.3.7	6.2.3.7
6.2.3.7	6.2.3	-	-
6.2.3.1 至 6.2.3.6	6.2.3	6.2.3	6.2.3

支持卸载的版本 6.2.2 补丁

此表列出了版本6.2.2 补丁支持的卸载场景。即使您是从更早的修补程序升级，卸载也会让您返回前一个修补程序。如果卸载后的时间比支持的要长，我们建议您重新映像，然后再升级到所需的补丁级别。

表 *52:* 支持卸载的版本 *6.2.2* 补丁

当前版本	您应该卸载的最早版本
6.2.2.3 至 6.2.2.5	6.2.2.2
6.2.2.2	-
6.2.2.1	6.2.2

高可用性/可扩展性的卸载顺序

在高可用性/可扩展性部署中，通过从设备逐一卸载来尽可能减少中断。与升级不同，系统不会为您执行此操作。等到补丁从一个设备完全卸载后，再转到下一个设备。

表 *53: FMC* 高可用性的卸载顺序

配置	卸载顺序
FMC 高可用性	同步暂停后（即一种称为裂脑的状态），从对等设备逐一卸载。请勿在对处于集群脑裂的情况下执行或部署配置更改。 **1.** 暂停同步（进入裂脑）。 **2.** 从备用设备卸载。 **3.** 从主用设备卸载。 **4.** 重启同步（退出裂脑）。

表 *54: FTD* 高可用性和集群的卸载顺序

配置	卸载顺序
FTD 高可用性	不能从配置为高可用性的设备卸载修补程序。必须先中断高可用性。 **1.** 中断高可用性。 **2.** 从先前的备用设备卸载。 **3.** 从先前的主用设备卸载。 **4.** 重新建立高可用性。
FTD 集群	从单元逐一卸载，将控制单元留到最后。卸载补丁时，集群单元在维护模式下运行。 **1.** 从数据模块逐一卸载。 **2.** 让其中一个数据模块成为新的控制模块。 **3.** 从以前的控制卸载。

表 *55: ASA* 故障转移对/集群中带 *FirePOWER* 服务的 *ASA* 的卸载顺序

配置	卸载顺序
ASA 主用/备用故障转移对，带 ASA FirePOWER	始终从备用设备卸载。 **1.** 从备用 ASA 设备上的 ASA FirePOWER 模块卸载。 **2.** 故障转移。 **3.** 从新备用 ASA 设备上的 ASA FirePOWER 模块卸载。
ASA 主用/主用故障转移对，带 ASA FirePOWER	在您未卸载的设备上使两个故障转移组均处于主用状态。 **1.** 使两个故障转移组在主要 ASA 设备上均处于主用状态。 **2.** 从辅助 ASA 设备上的 ASA FirePOWER 模块卸载。 **3.** 使两个故障转移组在辅助 ASA 设备上均处于主用状态。 **4.** 从主要 ASA 设备上的 ASA FirePOWER 模块卸载。
ASA 集群，带 ASA FirePOWER	卸载前，在每个单元上禁用集群。从单元逐一卸载，将控制单元留到最后。 **1.** 在从数据单元上禁用集群。 **2.** 从该单元上的 ASA FirePOWER 模块卸载。 **3.** 重新启用集群。等待单元重新加入集群。 **4.** 对每个从属数据单元上述操作。 **5.** 在控制单元上禁用集群。等待新的控制单元接管。 **6.** 从先前控制单元上的 ASA FirePOWER 模块卸载。 **7.** 重新启用集群。

通过 FMC 卸载设备补丁

使用 Linux shell（专家模式）卸载补丁。您必须能够以设备的管理员用户或者具有 CLI 配置访问权限的其他本地用户身份访问设备外壳程序。您无法使用 FMC 用户帐户。如果禁用了外壳程序访问，请联系 Cisco TAC 以撤销锁定。

⚠

注意 请勿在卸载期间进行或部署配置更改。即使系统显示为非活动状态，也不要手动重启、关闭或重新启动正在进行的卸载。您可以将系统置于不可用状态并要求重新映像。如果您遇到卸载问题，包括卸载失败或设备无响应，请联系 Cisco TAC。

开始之前

- 中断 FTD 高可用性对；请参阅高可用性/可扩展性的卸载顺序，第 112 页。
- 确保部署中保持正常运行，并且能够成功通信。

步骤 1 如果设备的配置过期，请立即从 FMC 部署。

在卸载之前进行部署可减少失败的可能性。 确保完成部署和其他基本任务。在卸载开始时运行的任务已停止，成为失败的任务，且不能恢复。您可以稍后手动删除具有失败状态的消息。

步骤 2 在设备上访问 Firepower CLI。使用配置访问权限作为管理员或其他 CLI 用户登录。

您可以通过 SSH 登录到设备的管理界面（主机名或 IP 地址），也可以使用控制台。如果使用控制台，有些设备默认使用操作系统 CLI，并且需要完成额外的步骤才能访问 Firepower CLI，如下表所列。

Firepower 1000 系列	`connect ftd`
Firepower 2100 系列	`connect ftd`
Firepower 4100/9300	连接模块 *slot_number* 控制台，然后连接 `ftd`（仅限首次登录）
ASA FirePOWER	`session sfr`

步骤 3 使用 `expert` 命令来访问 Linux shell。

步骤 4 验证卸载软件包是否在升级目录中。

```
ls /var/sf/updates
```

补丁卸载程序的名称与升级软件包类似，但文件名中包含 `Patch_Uninstaller` 而不是 `Patch`。在设备上安装补丁时，升级目录中会自动创建该补丁的卸载程序。如果没有卸载程序，请联系 Cisco TAC。

步骤 5 运行卸载命令，在系统提示时输入密码。

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

注意 系统不会要求您确认。输入此命令将启动卸载，其中包括设备重新启动。卸载期间的流量和检查中断与升级期间发生的中断相同。确保您已准备就绪。请注意，使用 `--detach` 选项可确保在 SSH 会话超时时卸载流程不会终止，这样会让设备处于不稳定状态。

步骤 6 监控卸载，直到您注销。

对于单独卸载，请使用 `tail` 或 `tailf` 来显示日志：

- FTD：`tail /ngfw/var/log/sf/update.status`
- ASA FirePOWER 和 NGIPSv：`tail /var/log/sf/update.status`

否则，请在控制台或终端中监控进度。

步骤 7 验证卸载是否成功。

在卸载完成后，确认设备的软件版本正确无误。在 FMC 上，选择**设备** > **设备管理**。

步骤 8 在高可用性/可扩展性部署中，对每个单元重复步骤 2 至 6。

对于集群，切勿从控制单元卸载。从所有数据单元卸载后，将其中一个单元设置为新控制，然后从以前的控制卸载。

步骤 9 重新部署配置。

例外：不要部署到混合版本的高可用性对或设备集群。首先部署，然后从第一个设备卸载，但在您从所有组成员卸载修补程序之前，不要再继续。

下一步做什么

- 要实现高可用性，请重新建立高可用性。
- 对于集群，如果您有特定设备的首选角色，请立即进行更改。

卸载独立 FMC 补丁

我们建议您使用 Web 界面来卸载 FMC 补丁。如果无法使用 Web 界面，可以作为外壳的管理员用户或者具有外壳访问权限的外部用户使用 Linux 外壳程序。如果禁用了外壳程序访问，请联系 Cisco TAC 以撤销锁定。

⚠

注意 请勿在卸载期间进行或部署配置更改。即使系统显示为非活动状态，也不要手动重启、关闭或重新启动正在进行的卸载。您可以将系统置于不可用状态并要求重新映像。如果您遇到卸载问题，包括卸载失败或设备无响应，请联系 Cisco TAC。

开始之前

- 如果卸载会使 FMC 的补丁级别低于其受管设备，请先从设备卸载补丁。
- 确保部署中保持正常运行，并且能够成功通信。

步骤 1 部署到其配置已过期的受管设备。

在卸载之前进行部署可减少失败的可能性。

步骤 2 点击您想要使用的卸载包旁边的 **安装** 图标，然后选择 FMC。

补丁卸载程序的名称与升级软件包类似，但文件名中包含 `Patch_Uninstaller` 而不是 `Patch`。在 FMC 上安装补丁时会自动创建该补丁的卸载程序。如果没有卸载程序，请联系 Cisco TAC。

步骤 3 点击**安装 (Install)**，然后确认要卸载并重新启动。

您可以在消息中心中监控进度，直到注销。

步骤 4 尽可能重新登录并验证卸载是否成功。

如果在您登录时系统未通知您卸载成功，请选择**帮助 (Help)** > **关于 (About)** 以显示当前软件版本信息。

步骤 5 将配置重新部署到所有托管设备。

卸载高可用性 FMC 补丁

我们建议您使用 Web 界面来卸载 FMC 补丁。如果无法使用 Web 界面，可以作为外壳的管理员用户或者具有外壳访问权限的外部用户使用 Linux 外壳程序。如果禁用了外壳程序访问，请联系 Cisco TAC 以撤销锁定。

从高可用性对逐一卸载。在暂停同步的情况下，首先从备用设备卸载，然后是主用设备。当备用设备开始卸载时，其状态从备用切换到主用，以便两个对等设备都处于主用状态。此临时状态称为裂脑，仅在升级和卸载期间受支持。

⚠

注意 请勿在对处于集群脑裂的情况下执行或部署配置更改。重启同步后，您所做的更改将丢失。 请勿在卸载期间进行或部署配置更改。即使系统显示为非活动状态，也不要手动重启、关闭或重新启动正在进行的卸载。您可以将系统置于不可用状态并要求重新映像。如果您遇到卸载问题，包括卸载失败或设备无响应，请联系 Cisco TAC。

开始之前

- 如果卸载会使 FMC 补丁级别低于其受管设备，请先从设备卸载补丁。
- 确保部署中保持正常运行，并且能够成功通信。

步骤 1 在主用 FMC上，部署到其配置已过期的受管设备。

在卸载之前进行部署可减少失败的可能性。

步骤 2 在主用 FMC，暂停同步。

a) 选择**系统** > **集成**。

b) 在**高可用性 (High Availability)**选项卡，点击**暂停同步 (Pause Synchronization)**。

步骤 3 从高可用性对逐一卸载补丁 - 先是备用设备，再是主用设备。

请按照卸载独立 FMC 补丁 ，第 115 页 中的说明进行操作，但省略初始部署，从而在验证每个对上的卸载均成功后停止。总而言之，对于每个对等体：

a) 在**系统 (System)** > **更新 (Updates)** 页面上卸载补丁。

b) 监控进度，直到您注销，然后在可以时重新登录。

c) 验证卸载是否成功。

步骤 4 在您想要设为主用对等设备的 FMC上，重新开始同步。

a) 选择**系统** > **集成**。
b) 在**高可用性 (High Availability)**选项卡，点击**设为主用 (Make-Me-Active)**。
c) 等待直至同步重新开始，并且其他 FMC 切换到备用模式。

步骤 5 将配置重新部署到所有托管设备。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。