



Firepower 管理中心升级指南

首次发布日期: 2018 年 3 月 29 日

上次修改日期: 2018 年 4 月 2 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



目录

第 1 章

使用入门 1

本指南适用对象 1

使用本指南 3

第 2 章

准备进行升级 5

评估部署 5

查找当前版本信息 6

计划升级路径 6

获取升级软件包 8

下载 Firepower 管理中心升级软件包 9

从 Cisco.com 下载软件 9

下载 Firepower 管理中心软件 10

下载 Firepower 威胁防御软件 11

下载 Firepower 7000/8000 系列和 NGIPSv 软件 13

下载 ASA FirePOWER 软件 14

下载 Firepower 4100/9300 机箱的 FXOS 15

下载高可用性 Firepower 管理中心准则 16

将升级软件包推送到受管设备 16

运行就绪性检查 17

从管理中心运行就绪性检查 18

从外壳运行就绪性检查 18

其他升级前的操作和检查 19

第 I 部分：

升级 Firepower 设备 21

第 3 章	升级 Firepower 管理中心	23
	Firepower 管理中心升级核对表	23
	升级独立 Firepower 管理中心	25
	升级高可用性 Firepower 管理中心	26

第 4 章	升级 Firepower 威胁防御 设备	29
	Firepower 威胁防御升级核对表	29
	升级 Firepower 威胁防御软件	31

第 5 章	升级 Firepower 威胁防御设备 - Firepower 4100/9300 系列	33
	Firepower 威胁防御升级核对表 - Firepower 4100/9300 机箱	33
	升级 FXOS - Firepower 4100/9300 机箱	35
	在独立 Firepower 4100/9300 机箱上升级 FXOS	35
	使用 Firepower 机箱管理器在独立 Firepower 4100/9300 机箱机箱上升级 FXOS	35
	使用 FXOS CLI 在独立 Firepower 4100/9300 机箱机箱上升级 FXOS	37
	在 Firepower 威胁防御高可用性对上升级 FXOS	40
	使用 Firepower 机箱管理器在 Firepower 威胁防御高可用性对上升级 FXOS	40
	使用 FXOS CLI 在 Firepower 威胁防御高可用性对上升级 FXOS	43
	在 Firepower 威胁防御机箱间集群上升级 FXOS	47
	使用 Firepower 机箱管理器在 Firepower 威胁防御机箱间集群上升级 FXOS	47
	使用 FXOS CLI 在 Firepower 威胁防御机箱间集群上升级 FXOS	50
	升级 Firepower 威胁防御软件 - Firepower 4100/9300 机箱	53

第 6 章	升级 Firepower 7000/8000 系列和 NGIPSv 设备	57
	Firepower 7000/8000 系列和 NGIPSv 升级核对表	57
	升级 Firepower 7000/8000 系列和 NGIPSv	59

第 7 章	升级具备 FirePOWER 服务的 ASA	61
	具备 FirePOWER 服务的 ASA 升级核对表	61
	升级 ASA	63

升级独立设备	63
使用 CLI 升级独立设备	63
使用 ASDM 从本地计算机升级独立设备	65
使用 ASDM Cisco.com 向导升级独立设备	66
升级主用/备用故障切换对	67
使用 CLI 升级主用/备用故障切换对	68
使用 ASDM 升级主用/备用故障切换对	70
升级主用/主用故障切换对	71
使用 CLI 升级主用/主用故障切换对	72
使用 ASDM 升级主用/主用故障切换对	75
升级 ASA 集群	76
使用 CLI 升级 ASA 集群	76
使用 ASDM 升级 ASA 集群	81
升级 ASA FirePOWER 模块 - 使用 Firepower 管理中心	84

 第 11 部分：

参考信息 87

 第 8 章

Firepower 设备的兼容性 89

Firepower 管理中心和受管设备版本兼容性	89
各型号的 Firepower 兼容性	91
Firepower 管理中心：物理	91
Firepower 管理中心：虚拟	92
Firepower 威胁防御设备	92
具备 Firepower 威胁防御的 Firepower 2100 系列	92
具有 Firepower 4100/9300 机箱的 Firepower 威胁防御	93
具有 ASA 5500-X 系列的 Firepower 威胁防御	94
具有 Firepower 威胁防御的 ISA 3000	94
Firepower 威胁防御虚拟	94
具备 FirePOWER 服务的 ASA 设备	95
具备 ASA FirePOWER 的 ASA 5500-X 系列	95
具备 ASA FirePOWER 的 ISA 3000	97

7000/8000 系列和传统设备 97

NGIPSv（虚拟受管设备） 98

第 9 章

升级途径 99

Firepower 管理中心升级路径 99

示例：升级高可用性 Firepower 管理中心 100

Firepower 威胁防御 升级路径 - 使用 Firepower 管理中心 101

示例：通过捆绑的操作系统升级 Firepower 威胁防御设备 102

示例：升级 Firepower 4100/9300 机箱（包括机箱内集群） 103

示例：升级 Firepower 4100/9300 机箱高可用性对 104

示例：升级 Firepower 威胁防御 4100/9300 机箱间集群 105

Firepower 7000/8000 系列和 NGIPSv 升级路径 - 使用 Firepower 管理中心 105

示例：升级虚拟部署 106

ASA FirePOWER 模块升级路径 - 使用 Firepower 管理中心 107

示例：升级具备 FirePOWER 服务的 ASA 108

Firepower 6.0 版预安装软件包 111

第 10 章

升级期间的流量、检查和设备行为 113

Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱 113

Firepower 威胁防御升级行为 115

Firepower 7000/8000 系列升级行为 117

ASA FirePOWER 升级行为 118

NGIPSv 升级行为 119

第 11 章

Firepower 软件升级的版本特定准则 121

影响多个版本的准则 121

6.2.3 版准则 121

6.2.2 版准则 122

6.2.0 版准则 122

6.1.0 版准则 124

6.0.0 版准则 125

Firepower 软件升级的时间和磁盘空间 127

- 6.2.3 版本时间和磁盘空间 127
- 6.2.2 版本时间和磁盘空间 128
 - 6.2.2.2 版本时间和磁盘空间 129
 - 6.2.2.1 版本时间和磁盘空间 130
- 6.2.0 版本时间和磁盘空间 130
 - 6.2.0.5 版本时间和磁盘空间 131
 - 6.2.0.4 版本时间和磁盘空间 132
 - 6.2.0.3 版本时间和磁盘空间 132
 - 6.2.0.2 版本时间和磁盘空间 133
 - 6.2.0.1 版本时间和磁盘空间 134
- 6.1.0 版本时间和磁盘空间 134
 - 6.1.0.6 版本时间和磁盘空间 135
 - 6.1.0.5 版本时间和磁盘空间 136
 - 6.1.0.4 版本时间和磁盘空间 136
 - 6.1.0.3 版本时间和磁盘空间 137
 - 6.1.0.2 版本时间和磁盘空间 138
 - 6.1.0.1 版本时间和磁盘空间 138
- 6.0.1 版本时间和磁盘空间 139
 - 6.0.1.4 版本时间和磁盘空间 139
 - 6.0.1.3 版本时间和磁盘空间 140
 - 6.0.1.2 版本时间和磁盘空间 141
 - 6.0.1.1 版本时间和磁盘空间 141
- 6.0 版本时间和磁盘空间 142
 - 6.0.0.1 版本时间和磁盘空间 142



第 1 章

使用入门

以下主题介绍如何开始升级 Firepower 管理中心部署。

- [本指南适用对象](#)，第 1 页
- [使用本指南](#)，第 3 页

本指南适用对象

本指南介绍如何准备并成功完成对 Firepower 管理中心部署的升级，该部署中，所有设备运行的最低 Firepower 版本为 5.4。如果您的部署不使用 Firepower 管理中心，或如果您需要全新安装 Firepower 软件，请使用以下资源。

升级单设备部署

以下指南介绍升级单设备部署。

- [思科 ASA 升级指南](#) - 使用 ASDM 升级 ASA FirePOWER 模块
- [适用于 Firepower 设备管理器的思科 Firepower 威胁防御配置指南](#) - 升级 Firepower 威胁防御设备

全新安装 Firepower 软件

以下表格列出了查找有关执行全新安装的相关说明的位置。安装软件包在 [Cisco.com](#) 上提供；请参阅[获取升级软件包](#)，第 8 页。请注意，思科不提供补丁的安装软件包。请安装最新的主要版本，然后进行升级。

表 1: Firepower 管理中心安装说明

设备	指南
MC750、1500、2000、3500、4000	750、1500、2000、3500 和 4000 型号的思科 Firepower 管理中心入门指南 - 将 Firepower 管理中心恢复为出厂默认设置
MC1000、2500、4500	1000、2500 和 4500 型号的思科 Firepower 管理中心入门指南 - 将 Firepower 管理中心恢复为出厂默认设置

设备	指南
虚拟: VMware	适用于 VMware 部署的思科虚拟 Firepower 管理中心快速入门指南
虚拟: KVM	适用于 KVM 部署的思科虚拟 Firepower 管理中心快速入门指南
虚拟: AWS	适用于 AWS 云的思科虚拟 Firepower 管理中心快速入门指南

表 2: Firepower 威胁防御安装说明

设备	指南
Firepower 2100 系列	重新映像思科 ASA 或 FirePOWER 威胁防御设备 和 适用于运行 Firepower 威胁防御的 Firepower 2100 系列的思科 FXOS 故障排除指南
Firepower 4100 系列 Firepower 9300	思科 FXOS CLI 配置指南 - Firepower 4100/9300 系列软件重新映像和灾难恢复程序
ASA 5500-X 系列 ISA 3000	重新映像思科 ASA 或 FirePOWER 威胁防御设备
虚拟: VMware	使用 Firepower 管理中心 适用于 VMware 部署的思科 Firepower 威胁防御虚拟快速入门指南
	使用 Firepower 设备管理器 使用面向 VMware 的 Firepower 设备管理器部署思科 Firepower 威胁防御虚拟设备快速入门指南
虚拟: KVM	使用 Firepower 管理中心 适用于 KVM 部署的思科 Firepower 威胁防御虚拟快速入门指南
	使用 Firepower 设备管理器 使用面向 KVM 的 Firepower 设备管理器部署思科 Firepower 威胁防御虚拟设备快速入门指南
虚拟: AWS	适用于 AWS 云的思科 Firepower 威胁防御虚拟快速入门指南
虚拟: Azure	适用于 Microsoft Azure 云的思科 Firepower 威胁防御虚拟快速入门指南

表 3: Firepower 7000/8000 系列、NGIPSv、ASA FirePOWER 安装说明

设备	指南
Firepower 7000 系列	思科 Firepower 7000 系列入门指南 - 将设备恢复为出厂默认设置
Firepower 8000 系列	思科 Firepower 8000 系列入门指南 - 将设备恢复为出厂默认设置
NGIPSv	适用于 VMware 的思科 Firepower NGIPSv 快速入门指南

设备	指南
具备 FirePOWER 服务的 ASA: <ul style="list-style-type: none"> • ASA 5500-X 系列 • ISA 3000 	重新映像思科 ASA 或 FirePOWER 威胁防御设备 和 ASDM 手册 2: 思科 ASA 系列防火墙 ASDM 配置指南 - 管理 ASA FirePOWER 模块

使用本指南

升级 Firepower 管理中心部署会是一个复杂的过程。认真规划和准备有助于避免步骤错误。在升级过程中，您应像实际执行调用升级脚本的机械步骤一样，考虑计划和准备。

最后，本指南包含三个主要部分：

- [准备进行升级，第 5 页](#)- 部署评估，升级路径计划，获取升级软件包，等等。
- [升级 Firepower 设备，第 21 页](#)- 描述升级 Firepower 设备的实际过程，包括在需要时进行操作系统升级。
- [参考信息，第 87 页](#)- 参考信息，可帮助您计划和执行 Firepower 升级。如果您已熟悉升级程序，这有助于快速解答最常见的问题。

升级核对表

本指南提供各种型号 Firepower 设备的升级核对表。这些核对表将引导您完成整个升级过程，包括计划和准备。



注意 每次升级时，请完成核对表。跳过步骤会导致升级失败。

设备	检查表
Firepower 管理中心包括: <ul style="list-style-type: none"> • Firepower 管理中心虚拟 • 高可用性对 	Firepower 管理中心升级核对表，第 23 页
Firepower 威胁防御: <ul style="list-style-type: none"> • Firepower 2100 系列 • ASA 5500-X 系列 • ISA 3000 • Firepower 威胁防御虚拟 	Firepower 威胁防御升级核对表，第 29 页

设备	检查表
Firepower 威胁防御： <ul style="list-style-type: none">• Firepower 4100 系列• Firepower 9300	Firepower 威胁防御升级核对表 - Firepower 4100/9300 机箱，第 33 页
NGIPS 软件： <ul style="list-style-type: none">• Firepower 7000 和 8000 系列• NGIPSv	Firepower 7000/8000 系列和 NGIPSv 升级核对表，第 57 页
具备 FirePOWER 服务的 ASA： <ul style="list-style-type: none">• ASA 5500-X 系列• ISA 3000	具备 FirePOWER 服务的 ASA 升级核对表，第 61 页



第 2 章

准备进行升级

升级 Firepower 管理中心部署会是一个复杂的过程。认真规划和准备有助于避免步骤错误。在升级过程中，您应像实际执行调用升级脚本的机械步骤一样，考虑计划和准备。

有关详情，请参阅：

- [评估部署，第 5 页](#)
- [计划升级路径，第 6 页](#)
- [获取升级软件包，第 8 页](#)
- [将升级软件包推送到受管设备，第 16 页](#)
- [运行就绪性检查，第 17 页](#)
- [其他升级前的操作和检查，第 19 页](#)

评估部署

升级任何 Firepower 设备之前，请先确定部署的当前状态。

您应思考如下问题：

- 您具有哪些设备，它们运行的是什么 Firepower 版本？您希望这些设备运行什么版本，它们是否可以运行该版本？
- 您是否有任何设备需要单独进行操作系统升级？或者，您是否希望仅升级操作系统？
- 您是否有虚拟设备需要进行托管环境升级？或者，您是否希望仅升级托管环境？
- 您使用的是独立 Firepower 管理中心，还是高可用性 Firepower 管理中心对？
- 您是使用独立设备，还是使用设备集群、堆叠和高可用性对？
- 您的设备是否是作为 IPS 或防火墙进行被动部署？
- 您要更换设备还是向您的部署添加新设备？

了解您当前的状态有助于确定如何达到目标。

查找当前版本信息

通过下表，您可以找到 Firepower 部署中可升级组件当前运行的版本的相关信息。

组件	设备	版本信息
Firepower 软件	Firepower 管理中心	在 Firepower 管理中心上，选择帮助 > 关于。
Firepower 软件	由 Firepower 管理中心管理的任何 Firepower 设备	在 Firepower 管理中心上，选择设备 > 设备管理。
FXOS	Firepower 4100/9300 机箱	在 FXOS CLI 中，使用 show version 命令。
ASA	具备 FirePOWER 服务的 ASA	在 ASA CLI 中，使用 show version 命令。
虚拟托管环境	任何 Firepower 虚拟设备	请参阅您的虚拟托管环境的相关文档。

计划升级路径

升级路径是有关您要升级的设备、要升级的组件以及升级顺序的详细计划。

如果您已评估部署，即您知道所拥有的内容和所需的内容，这就表示您已准备好构建升级路径。有关每种设备类型支持的升级路径，以及各种类型的部署的高级升级路径示例的快速参考，请参阅[升级途径，第 99 页](#)。

使用以下准则有助于构建升级路径。

了解 Firepower 主要版本/升级与补丁

Firepower 主要升级会更改版本的第一个、第二个或第三个数字。主要升级包括新特性和功能，并且可能包含对产品的大规模更改。对于要在其中单独升级操作系统的设备，主要 Firepower 升级很可能会伴有操作系统升级。



注释

在许多情况下，您无需升级 Firepower 软件即可升级设备的操作系统（或虚拟托管环境），反之亦然。例如，操作系统补丁可能会解决与 Firepower 软件无关的问题。或者，您可能希望利用新的 Firepower 功能，而不升级虚拟机监控程序。只需确保您要升级的组件的目标版本与您不希望升级的组件兼容即可。

Firepower 补丁会更改版本的第四个数字。补丁通常包含有限的修复程序。

如果您的升级路径跨多个主要 Firepower 版本（例如，从 6.0.1 版本到 6.2.3 版本），则可以跳过中间版本（6.1 版本）中的补丁。也就是说，您可以直接从一个主要版本升级到另一个主要版本。在达到目标主要版本后，应用最新的补丁。

保持管理器与设备的兼容性

单独升级 Firepower 管理中心及其设备。一次手动升级一个高可用性 Firepower 管理中心。

为保持管理器与设备的兼容性，以及根据您需要升级部署的程度，您可能需要：

- 执行中间升级。
- 在替代步骤中升级 Firepower 管理中心及其设备。

有关详细信息，请参阅[Firepower 管理中心和受管设备版本兼容性](#)，第 89 页。

包括 FXOS 升级（Firepower 4100/9300 机箱）

Firepower 4100 系列和 Firepower 9300 设备使用 FXOS 操作系统。

主要的 Firepower 版本具有随附的 FXOS 版本。在 Firepower 4100/9300 机箱上升级 Firepower 软件之前，您必须运行该随附版本的 FXOS。

在每个机箱上单独升级 FXOS，即使配置了 Firepower 威胁防御高可用性或集群也是如此。为了尽量减少中断，请始终升级高可用性对的备用设备或机箱间集群中的全从属机箱。

有关详细信息，请参阅[Firepower 威胁防御 升级路径 - 使用 Firepower 管理中心](#)，第 101 页。

包括 ASA 升级（具备 FirePOWER 服务的 ASA）

具备 FirePOWER 服务的 ASA 设备使用 ASA 操作系统。

ASA 与 ASA FirePOWER 版本之间没有广泛的兼容性。但是，即使并非严格要求进行 ASA 升级，但是解决问题可能需要升级到支持的最新版本。

在每个机箱上单独升级 ASA，即使已配置 ASA 集群或故障切换对也是如此。为尽量减少中断，先在每台设备上故障切换或禁用集群，然后再进行升级，在升级 ASA 时一次升级一个 ASA FirePOWER 模块。

有关详细信息，请参阅[ASA FirePOWER 模块升级路径 - 使用 Firepower 管理中心](#)，第 107 页。

包括虚拟托管环境升级

虚拟 Firepower 设备可在多种托管环境中运行。Firepower 软件必须保持与其托管环境的兼容。升级路径取决于兼容性：

- 先升级托管环境 - 例如，如果您在 VMware ESXi 5.0 上运行 NGIPSv 5.4.x 版本，则必须先将 VMware ESXi 升级到 5.1 或 5.5 版本，然后再将 NGIPSv 升级到 Firepower 6.0。
- 先升级 Firepower 软件 - 例如，如果您在 VMware ESXi 6.0 上运行 Firepower 威胁防御虚拟 6.1.x 版本，则先将 Firepower 软件升级到 6.2.3 版本，然后再将 VMware ESXi 升级到 6.5 版本。

确定何时添加新设备

如果您的升级路径包括添加新设备，则添加设备的时间取决于设备类型：

- 物理设备 - 确定设备当前正在运行的 Firepower 版本。尽快添加设备，然后在部署的其余部分中使用 Firepower 管理中心升级新设备。请勿将 Firepower 管理中心升级到无法再管理开箱即用设备的版本。
- 虚拟设备 - 在将 Firepower 管理中心升级到其目标版本后创建。当添加新虚拟设备时，永远不必执行主要升级，只需进行补丁升级。

确定其他主要任务

升级过程中的许多步骤可能需要大量时间。您应在计划中明确包含这些步骤。例如：

- 备份
- 下载和推送
- 就绪性检查
- 升级前和升级后配置更改

识别流量和检查中断

有关详细信息，请参阅[升级期间的流量、检查和设备行为](#)，第 113 页。

我应该从哪里着手？

请参阅您的部署评估。一般情况下，首先要执行的升级取决于受管设备正在运行的 Firepower 版本。

设备版本	首先升级此项	升级到此版本
所有设备均为 6.1 及更高版本。	Firepower 管理中心	任何主要版本，6.2 及更高版本。
部分或所有设备低于 6.1 版本，但运行的主要版本与 Firepower 管理中心相同。	Firepower 管理中心	下一个主要版本。
部分或所有设备低于 6.1 版本，但运行的主要版本低于 Firepower 管理中心。	设备	与 Firepower 管理中心相同的主要版本

获取升级软件包

要在 Firepower 管理中心或其管理的设备上升级 Firepower 软件，必须将适当的升级软件包上传到 Firepower 管理中心。将 Firepower 管理中心升级软件包（但不是受管设备软件包）上传到高可用性对中的两个对等设备。



注释 从 6.2.1 及更高版本进行升级的软件包经过签名，并在 `.sh.REL.tar` 而不是只是 `just.sh` 中终止。请勿解压已签名的升级软件包。

您可以使用 Firepower 管理中心 Web 界面从 Cisco.com 直接获取补丁和修补程序。但是，您必须自行从 Cisco.com 下载主要升级软件包，然后将它们上传到 Firepower 管理中心。

有关详情，请参阅：

下载 Firepower 管理中心升级软件包

您可以使用 Firepower 管理中心检索其自身以及其管理的设备的补丁和修补程序。

检索的升级软件包数量（以及检索它们所用的时间）取决于：

- 当前部署的新鲜程度 - 系统下载您的设备当前正在运行的版本所关联的每个补丁和修补程序的软件包。
- 您拥有的不同设备类型数 - 系统下载为每种设备类型下载不同的软件包。如果您的部署包括多个相同类型的设备（例如，10 个 Firepower 威胁防御设备），系统会下载单个软件包以对它们全部进行升级。

开始之前

- 请确保 Firepower 管理中心能够访问互联网。
- 如果您使用的是高可用性对中的备用 Firepower 管理中心，请暂停同步。有关详细信息，请参阅 [下载高可用性 Firepower 管理中心准则，第 16 页](#)。

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

步骤 2 点击下载更新。

从 Cisco.com 下载软件

您可以从 Cisco.com 下载任何升级软件包，但对于主要升级，必须执行该操作。请查看您的升级路径，以确定需要下载的升级软件包。

许多升级软件包名称类似，因此请确保下载正确的软件包。从支持站点直接下载。如果通过邮件传输升级软件包，可能会损坏该软件包。从 6.2.1 及更高版本进行升级的软件包经过签名，并在 `.sh.REL.tar` 而不是只是 `just.sh` 中终止。请勿解压已签名的升级软件包。

步骤 1 从 Cisco.com 找到相应的升级软件包，并将其下载到您的计算机。

下表提供了导航路径和升级软件包名称：

- 下载 Firepower 管理中心软件，第 10 页
- 下载 Firepower 威胁防御软件，第 11 页
- 下载 Firepower 7000/8000 系列和 NGIPSv 软件，第 13 页

步骤 2 在 Firepower 管理中心上，选择系统 > 更新。

步骤 3 点击上传更新，然后选择文件。浏览到更新并点击上传。

下载 Firepower 管理中心软件

本部分列出了 Firepower 管理中心的下载位置和软件包名称。

对于高可用性 Firepower 管理中心，将软件包上传到两个对等设备，在上传到辅助设备时暂停同步。有关详细信息，请参阅[下载高可用性 Firepower 管理中心准则](#)，第 16 页。

下载位置

浏览到 <https://www.cisco.com/web/go/firepower-software>。

选择型号 > **FireSIGHT 系统软件** > 版本。

软件包名称

从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。安装软件包仅用于全新安装（重新映像）。

型号	软件包类型	软件包名称
全部	升级	Sourcefire_3D_Defense_Center_S3_Upgrade-版本.sh Sourcefire_3D_Defense_Center_S3_Upgrade-版本.sh.REL.tar
	修补	Sourcefire_3D_Defense_Center_S3_Patch-版本.sh Sourcefire_3D_Defense_Center_S3_Patch-版本.sh.REL.tar
	修补程序	Sourcefire_3D_Defense_Center_S3_Hotfix_字母-版本.sh Sourcefire_3D_Defense_Center_S3_Hotfix_字母-版本.sh.REL.tar
750、1500、MC、MC、MC3500、MC2000、MC4000	预安装软件包（仅选择版本）	Sourcefire_3D_Defense_Center_S3_目标版本_Pre-install-当前版本.sh
	系统软件安装	Sourcefire_Defense_Center_S3-版本-Restore.iso

型号	软件包类型	软件包名称
MC1000、MC2500、MC4500	系统软件安装	Sourcefire_Defense_Center_M4-版本-Restore.iso
Firepower 管理中心虚拟	Firepower 软件安装: VMware	Cisco_Firepower_Management_Center_Virtual_VMware-版本.tar.gz
	Firepower 软件安装: KVM	Cisco_Firepower_Management_Center_Virtual-版本.qcow2
	Firepower 软件安装: AWS	登录到云服务并从市场部署。

下载 Firepower 威胁防御软件

本部分提供 Firepower 威胁防御设备的下载位置和软件包名称。

下载位置

浏览到:

- ISA 3000-<http://www.cisco.com/go/isa3000-software>
- 所有其他—<https://www.cisco.com/go/ftd-software>

选择型号 > **Firepower 威胁防御软件** > 版本。

软件包名称

从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。引导映像和安装软件包仅用于全新安装（重新映像）。

型号	软件包类型	软件包名称
Firepower 2100 系列	升级	Cisco_FTD_SSP_FP2K_Upgrade-版本.sh.REL.tar
	修补	Cisco_FTD_SSP-FP2K_Patch-版本.sh.REL.tar
	修补程序	Cisco_FTD_SSP-FP2K_Hotfix_字母-版本.sh.REL.tar
	系统软件安装	cisco-ftd-fp2k.版本.SPA

型号	软件包类型	软件包名称
Firepower 4100 系列 Firepower 9300	升级	Cisco_FTD_SSP_Upgrade-版本.sh Cisco_FTD_SSP_Upgrade-版本.sh.REL.tar
	修补	Cisco_FTD_SSP_Patch-版本.sh Cisco_FTD_SSP_Patch-版本.sh.REL.tar
	修补程序	Cisco_FTD_SSP_Hotfix_字母-版本.sh Cisco_FTD_SSP_Hotfix_字母-版本.sh.REL.tar
	Firepower 软件安装	cisco-ftd.版本.SPA.csp
	FXOS	请参阅 下载 Firepower 4100/9300 机箱的 FXOS ，第 15 页。
ASA 5500-X 系列 ISA 3000	升级	Cisco_FTD_Upgrade-版本.sh Cisco_FTD_Upgrade-版本.sh.REL.tar
	修补	Cisco_FTD_Patch-版本.sh Cisco_FTD_Patch-版本.sh.REL.tar
	修补程序	Cisco_FTD_Hotfix_字母-版本.sh Cisco_FTD_Hotfix_字母-版本.sh.REL.tar
	引导映像： 5506-X、08-X、16-X ISA 3000	ftd-boot-版本.lfbff
	引导映像： 5512-X、15-X、25-X、 45-X、55-X	ftd-boot-版本.cdisk
	Firepower 软件安装	ftd-版本.pkg

型号	软件包类型	软件包名称
Firepower 威胁防御虚拟 (NGFW 虚拟) : • VMware • KVM • AWS • Microsoft Azure	升级	Cisco_FTD_Upgrade-版本.sh Cisco_FTD_Upgrade-版本.sh.REL.tar
	修补	Cisco_FTD_Patch-版本.sh Cisco_FTD_Patch-版本.sh.REL.tar
	修补程序	Cisco_FTD_Hotfix_字母-版本.sh Cisco_FTD_Hotfix_字母-版本.sh.REL.tar
	Firepower 软件安装: VMware	Cisco_Firepower_Threat_Defense_Virtual-版本.tar.gz
	Firepower 软件安装: KVM	Cisco_Firepower_Threat_Defense_Virtual-版本.qcow2
	Firepower 软件安装: AWS、Azure	登录到云服务并从市场部署。

下载 Firepower 7000/8000 系列和 NGIPSv 软件

本部分提供 Firepower 7000/8000 系列和 NGIPSv 设备的下载位置和软件包名称。

下载位置

浏览到:

- 7000 系列—<https://www.cisco.com/go/7000series-software>
- 8000 系列—<https://www.cisco.com/go/8000series-software>
- NGIPSv—<http://www.cisco.com/go/ngipsv-software>

选择型号 > FireSIGHT 系统软件 > 版本。

软件包名称

从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。安装软件包仅用于全新安装（重新映像）。

表 4: Firepower 7000/8000 系列和 AMP 软件包名称

软件包类型	软件包名称
升级	Sourcefire_3D_Device_S3_Upgrade-版本.sh Sourcefire_3D_Device_S3_Upgrade-版本.sh.REL.tar

软件包类型	软件包名称
修补	Sourcefire_3D_Device_S3_Patch-版本.sh Sourcefire_3D_Device_S3_Patch-版本.sh.REL.tar
修补程序	Sourcefire_3D_Device_S3_Hotfix_字母-版本.sh Sourcefire_3D_Device_S3_Hotfix_字母-版本.sh.REL.tar
预安装软件包（仅选择版本）	Sourcefire_3D_Device_S3_目标版本_Pre-install-当前版本.sh
系统软件安装	Sourcefire_3D_Device_S3-版本-Restore.iso

表 5: NGIPSv 软件包名称

软件包类型	软件包名称
升级	Sourcefire_3D_Device_Virtual64_VMware_Upgrade-版本.sh Sourcefire_3D_Device_VMware_Upgrade-版本.sh.REL.tar
修补	Sourcefire_3D_Device_Virtual64_VMware_Patch-版本.sh Sourcefire_3D_Device_VMware_Patch-版本.sh.REL.tar
修补程序	Sourcefire_3D_Device_Virtual64_VMware_Hotfix_字母-版本.sh Sourcefire_3D_Device_VMware_Hotfix_字母-版本.sh.REL.tar
预安装软件包（仅选择版本）	Sourcefire_3D_Device_Virtual64_VMware_目标版本_Pre-install-当前版本.sh
Firepower 软件安装	Cisco_Firepower_NGIPSv_VMware-版本.tar.gz

下载 ASA FirePOWER软件

本部分提供 ASA FirePOWER 模块的下载位置和软件包名称。

下载位置

浏览到：

- ASA 5500-X 系列-<http://www.cisco.com/go/asa-firepower-sw>
- ISA 3000-<http://www.cisco.com/go/isa3000-software>

依次选择型号 > ASA FirePOWER服务软件 > 版本。

软件包名称

从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。引导映像和安装软件包仅用于全新安装（重新映像）。

型号	软件包类型	软件包名称
ASA 5500-X 系列	升级	Cisco_Network_Sensor_Upgrade-版本.sh Cisco_Network_Sensor_Upgrade-版本.sh.REL.tar
	修补	Cisco_Network_Sensor_Patch-版本.sh Cisco_Network_Sensor_Patch-版本.sh.REL.tar
	修补程序	Cisco_Network_Sensor_Hotfix_字母-版本.sh Cisco_Network_Sensor_Hotfix_字母-版本.sh.REL.tar
	预安装软件包（仅选择版本）	Cisco_Network_Sensor_目标版本_Pre-install-当前版本.sh
	引导映像： ASA 5506-X、 08-X、16-X ASA 5512-X、 15-X、25-X、 45-X、55-X	asasfr-boot-版本.img
	引导映像： ASA 5585-X	asasfr-boot-版本.img
	系统软件安装	asasfr-sys-版本.pkg
	ASA OS	请参阅 思科 ASA 升级指南 中的下载 ASA 软件。
ISA 3000	修补	Cisco_Network_Sensor_Patch-版本.sh
	修补程序	Cisco_Network_Sensor_Hotfix_字母-版本.sh
	引导映像	asasfr-ISA-3000-boot-版本.img
	系统软件安装	asasfr-sys-版本.pkg
	ASA OS	请参阅 思科 ASA 升级指南 中的下载 ASA 软件。

下载 Firepower 4100/9300 机箱的 FXOS

本部分提供 Firepower 4100/9300 机箱的 FXOS 操作系统的下载位置和软件包名称。

下载位置

浏览到:

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

选择型号 > **Firepower** 可扩展操作系统 > 版本。

软件包名称

软件包类型	软件包名称
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

下载高可用性 Firepower 管理中心准则

在高可用性配置中升级 Firepower 管理中心时, 您必须将软件包同时下载到主用/主 Firepower 管理中心和备用/辅助 Firepower 管理中心。

将软件包下载到主用/主 Firepower 管理中心时可以不暂停同步, 但在将软件包下载到备用/辅助 Firepower 管理中心之前, 必须暂停同步。

为了减少升级过程中高可用性同步的中断, 我们建议您:

- 在升级准备阶段为主用/主 Firepower 管理中心下载软件。
- 暂停同步后, 在执行升级步骤的过程中为备用/辅助 Firepower 管理中心下载软件。

有关详细信息, 请参阅[升级高可用性 Firepower 管理中心](#), 第 26 页。

将升级软件包推送到受管设备

在 6.2.3 及更高版本中, 您可以在实际运行升级之前, 将升级软件包复制 (或推送) 到受管设备。这有助于减少升级维护窗口的时长。(在版本 6.2.3 之前, Firepower 管理中心会在安装过程中将软件包复制到受管设备, 而且您不能分隔这些任务。)

将升级软件包推送到设备集群或堆叠时，Firepower管理中心首先推送到一台设备，然后再推送到其他设备。当您推送到高可用性对时，Firepower管理中心将推送到主设备，然后与辅助设备进行同步。

开始之前

- 获取适当的软件升级包，并将其上传到 Firepower 管理中心。请参阅[获取升级软件包](#)，第 8 页。
- 推送升级软件包的时间取决于管理网络的带宽。请确保您的带宽足以将大量数据从 Firepower 管理中心传输到设备。有关详细信息，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 依次选择系统 (System) > 更新 (Updates)。

步骤 2 点击您想要推送的升级软件包旁边的**推送**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 3 点击**推送**。

步骤 4 在信息中心监控推送进度。

运行就绪性检查

可选的就绪性检查会评估设备进行 Firepower 升级的就绪性情况。就绪性检查包含在升级软件包中，可识别数据库完整性、版本不一致和设备注册等问题。



注意

请勿在就绪性检查期间重启或关闭设备。如果您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，而是联系思科 TAC 寻求帮助。

就绪性检查准则和限制

- 仅检查 Firepower 软件就绪性 - 就绪性检查不评估入侵规则、VDB 或 GeoDB 更新的就绪性情况。
- 需要 6.1 及更高版本 - 就绪性检查在版本 6.1 中引入。对以版本 6.1 为目标的升级进行就绪性检查可能不会返回准确的结果。
- Web 界面与外壳 - 您可以使用 Firepower 管理中心 Web 界面仅对其自身及其独立的受管设备执行就绪性检查。对于集群设备、堆栈中的设备和高可用性对中的设备，请从每个设备的外壳运行就绪性检查。

- 时间要求 - 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。如果部署规模很大（例如，Firepower 管理中心管理超过 100 台设备），您可能会发现放弃就绪性检查是更好的做法。

从管理中心运行就绪性检查

您可以使用 Firepower 管理中心 Web 界面仅对它及其独立的受管设备执行就绪性检查。

开始之前

- 将您要检查其就绪性的 6.1 及更高版本设备的升级软件包上传到 Firepower 管理中心。升级软件包中包含就绪性检查。请注意，从 6.2.1 及更高版本进行升级的软件包经过签名，并在 `.sh.REL.tar` 而不是 `just.sh` 中终止。请勿在执行就绪性检查或升级之前，解压已签名的升级软件包。
- 将配置更改重新部署到任何受管设备。否则，就绪性检查可能会失败。

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

步骤 2 点击您希望就绪性检查评估的升级旁边的安装图标。

步骤 3 点击启动就绪性检查。

步骤 4 在消息中心中监控就绪性检查的进度。

就绪性检查完成后，系统会在“就绪性检查状态”页面报告成功或失败。

步骤 5 在 `/var/log/sf/$rpm_name/upgrade_readiness` 中访问完整的就绪性检查报告。

从外壳运行就绪性检查

您可以从任何 6.1 及更高版本的 Firepower 设备上的外壳运行就绪性检查。对于集群设备、堆叠设备和高可用性对中的设备，您必须使用外壳。



注意

我们建议您从控制台会话运行就绪性检查。如果您使用 SSH 访问设备，请确保您的连接不会超时。就绪性检查作为用户外壳的子进程运行。如果终止 SSH 连接，这些进程将被中止，检查会中断，而且设备可能处于不稳定状态。

开始之前

- 将升级软件包下载到要检查其就绪性的设备；请参阅[获取升级软件包](#)，第 8 页。升级软件包中包含就绪性检查。从 6.2.1 及更高版本进行升级的软件包经过签名，并在 `.sh.REL.tar` 而不是只是 `just.sh` 中终止。请勿解压已签名的升级软件包。
- 将配置部署到所有受管设备。否则，就绪性检查可能会失败。

步骤 1 以具有管理员权限的用户身份登录到外壳。

步骤 2 确保升级软件包位于设备上。

对于早于 6.2.3 版本的受管设备，使用设备外壳中的 SCP 将升级软件包复制到 `/var/sf/updates`。在 6.2.3 及更高版本中，您可以使用 SCP，也可以使用 Firepower 管理中心推送升级软件包。

对于 Firepower 管理中心，请使用 SCP 或 Web 界面。

步骤 3 以 root 用户身份运行以下命令：

```
sudo install_update.pl --readiness-check /var/sf/updates/update_package_name
```

步骤 4 就绪性检查完成后，在 `/var/log/sf/$rpm_name/upgrade_readiness` 中访问完整的就绪性检查报告。

其他升级前的操作和检查

以下升级前的操作和检查对于成功升级也是至关重要的。

验证设备通信和运行状况

在整个升级过程中，确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。及时解决不严重的问题，避免它们变为严重问题。

查看版本说明

务必要阅读版本说明，以了解重要信息和版本特定的信息：

- [Firepower 版本说明](#)
- [ASA 版本说明](#)
- [FXOS 版本说明](#)

制定升级计划之前和之后的配置更改

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必须解决重大配置更改。

例如，版本 6.0 删除了对 Firepower 管理中心高可用性的支持。在开始升级之前，必须拆分所有对。再举个例子，版本 6.2.3 会限制您可以在报告部分中使用或包括的结果数。升级过程可以降低结果限制和禁用 PDF 报告，具体取决于您的升级前配置。升级后，您可能希望调整报告模板，以容纳新的限制和重新启用 PDF 报告。

有关升级前和升级后配置更改的详细信息，请参阅版本说明以及 [Firepower 软件升级的版本特定准则](#)，第 121 页。

检查时间和磁盘空间

要升级 Firepower 设备，必须具有足够的可用磁盘空间，否则升级会失败。您还必须具有足够的时间来执行升级。根据您的部署，升级所需的时间可能超出提供的估计时间。例如，内存较低的设备 and 负载过多的设备可能需要更长的升级时间。此外，提供的估计时间不包括完成就绪性检查所需的时间。

有关每个版本的时间和磁盘空间的列表，请参阅[Firepower 软件升级的时间和磁盘空间](#)，第 127 页。

检查带宽

在版本 6.2.3 之前，Firepower 管理中心会在安装过程中将升级软件包复制到受管设备，而且您不能分隔这些任务。在 6.2.3 及更高版本中，您可以在实际运行升级之前，将升级软件包复制（或推送）到受管设备。这有助于减少升级维护窗口的时长。

不管是哪种情况，都必须确保您的带宽足以将大量数据从 Firepower 管理中心传输到设备。有关详细信息，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）。

备份配置和事件数据

在开始升级之前，将事件和配置数据备份到外部位置：

- Firepower 管理中心- 使用 Firepower 管理中心备份其自己的配置和事件数据。
- 大多数受管设备 - 使用 Firepower 管理中心备份来自受管设备的事件。对于大多数受管设备，无法创建单独的配置和事件备份文件。
- 仅限 7000 和 8000 系列设备 - 使用 Firepower 管理中心或本地设备 GUI 备份配置和事件数据。

有关详细信息，请参阅[Firepower 管理中心配置指南](#)。



注释

我们强烈建议备份到外部位置并验证传输是否成功。在升级 Firepower 管理中心时，它会清除本地存储的备份。

安排维护窗口

安排维护窗口时，请考虑升级对流量和检查的影响，以及升级可能需要的时间。此外，还要考虑您必须在该维护窗中执行的任务，以及可以提前执行的任务。通过精心的计划和准备，尽量减少中断。请勿等到维护窗口才获取和推送升级软件包、运行就绪性检查、创建备份等等。



第 I 部分

升级 Firepower 设备

- [升级 Firepower 管理中心，第 23 页](#)
- [升级 Firepower 威胁防御设备，第 29 页](#)
- [升级 Firepower 威胁防御设备 - Firepower 4100/9300 系列，第 33 页](#)
- [升级 Firepower 7000/8000 系列和 NGIPSv 设备，第 57 页](#)
- [升级具备 FirePOWER 服务的 ASA，第 61 页](#)



第 3 章

升级 Firepower 管理中心

- [Firepower 管理中心升级核对表](#)，第 23 页
- [升级独立 Firepower 管理中心](#)，第 25 页
- [升级高可用性 Firepower 管理中心](#)，第 26 页

Firepower 管理中心升级核对表

使用此核对表可升级 Firepower 管理中心，包括 Firepower 管理中心虚拟。如果您要在高可用性对中升级 Firepower 管理中心，请对每个对等设备完成核对表。

每次升级时，请完成核对表。跳过步骤会导致升级失败。在整个升级过程中，确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

制定升级计划

请正确地规划和遵循升级路径，以保持良好的部署兼容性。

	操作/检查	Details
	检查您在升级路径中所处的阶段，了解已经完成的升级和即将执行的升级。	计划升级路径 ，第 6 页
	检查 Firepower 管理中心上的当前版本和目标版本： <ul style="list-style-type: none">• Firepower 软件• 虚拟托管环境（Firepower 管理中心虚拟）	Firepower 管理中心：物理 ，第 91 页 Firepower 管理中心：虚拟 ，第 92 页
	检查 Firepower 管理中心在您对其升级后是否能够管理设备。如果不能，请修改您的升级路径，以便先升级设备。	Firepower 管理中心和受管设备版本兼容性 ，第 89 页
	阅读有关下一个/下一组升级的版本说明，应特别注意版本特定的准则。	Firepower 版本说明

升级前的操作和检查

通过在维护窗口外执行预检查，尽量减少中断。

	操作/检查	Details
	进行必要的升级前配置更改。 准备好进行必要的升级后配置更改。	Firepower 软件升级的版本特定准则， 第 121 页 Firepower 版本说明
	为 Firepower 软件升级运行初步磁盘空间检查。	Firepower 软件升级的时间和磁盘空间， 第 127 页
	获取正确的 Firepower 软件升级软件包，并将其上传到 Firepower 管理中心。 从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。	获取升级软件包，第 8 页
	运行就绪性检查。（可选，6.1 及更高版本）	运行就绪性检查，第 17 页
	备份事件和配置数据 备份到外部位置并验证传输是否成功。在升级 Firepower 管理中心时，它会清除本地存储的备份。	Firepower 管理中心配置指南
	从以下方面进行考虑，将维护窗口安排在影响最小的时间段： <ul style="list-style-type: none"> • 您必须在维护窗口执行的任务。 • 升级可能需要的最短时间。 	Firepower 软件升级的时间和磁盘空间， 第 127 页

升级 Firepower 管理中心

在维护窗口执行升级。

	操作/检查	Details
	如果需要，请升级托管环境（仅限 Firepower 管理中心虚拟）。	请参阅您的托管环境的相关文档。
	升级 Firepower 软件。	升级独立 Firepower 管理中心，第 25 页 升级高可用性 Firepower 管理中心，第 26 页

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 管理中心虚拟。



注意 请勿将更改部署到正在升级的设备或从其部署更改，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 思科 TAC。

开始之前

检查您在升级路径中所处的位置，包括托管环境和受管设备升级。请确保您已为此步骤做好充分的计划和准备。

步骤 1 部署到其配置已过期的受管设备。

在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。选择设备，然后再次点击**部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。

步骤 2 执行最终的升级前检查。

- 检查运行状况 - 使用消息中心（点击菜单栏上的系统状态图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务 - 此项也位于消息中心中，用于确保完成重要任务。在升级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。
- 检查磁盘空间 - 执行最终磁盘空间检查。如果可用磁盘空间不足，会导致升级失败。

步骤 3 依次选择系统 (System) > 更新 (Updates)。

步骤 4 点击您想要使用的升级软件包旁边的安装图标，然后选择 Firepower 管理中心。

步骤 5 点击**安装**以开始升级。

确认您要升级和重启 Firepower 管理中心。

步骤 6 在消息中心中监控预检查进度，直到注销。

在 Firepower 管理中心升级期间，不进行配置更改或部署到任何设备。即使消息中心在数分钟内不显示进度，或指示升级失败，请勿重新开始升级或重启 Firepower 管理中心。而是联系思科 TAC 寻求帮助。

步骤 7 在可以时，登录回 Firepower 管理中心。

- 次要升级（修补程序和修补程序） - 在升级完成且 Firepower 管理中心重启后，您可以登录。

- 主要升级 - 您可以在升级完成之前登录。Firepower 管理中心会显示一个页面，供您用于监控升级进度以及查看升级日志和任何错误消息。升级完成且 Firepower 管理中心重启时，您会再次注销。

步骤 8 (仅适用于主要升级) 登录回 Firepower 管理中心。

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)》。否则，您会被注销。

步骤 9 验证升级是否成功。

如果在您登录时 Firepower 管理中心未通知您升级成功，请选择 **帮助 > 关于** 以显示当前软件版本信息。

步骤 10 使用消息中心重新检查部署运行状况。

步骤 11 更新入侵规则和漏洞数据库 (VDB)。

如果支持站点上提供的入侵规则更新或 VDB 比当前运行的版本新，请安装新版本。有关详细信息，请参阅 [Firepower 管理中心配置指南](#)。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 12 完成版本说明中所述的任何升级后配置更改。

步骤 13 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 Firepower 管理中心上升级 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 Firepower 管理中心开始预检查时，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。请勿在对处于集群裂脑的情况下执行或部署配置更改。升级 Firepower 管理中心并重新开始同步后，您所做的更改将丢失。



注意

请勿将更改部署到正在升级的设备或从其部署更改，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 思科 TAC。

开始之前

检查您在升级路径中所处的位置，包括受管设备升级。请确保您已为此步骤做好充分的计划和准备。

步骤 1 在主用 Firepower 管理中心上，部署到其配置已过期的受管设备。

在 Firepower 管理中心菜单栏上，点击 **部署 (Deploy)**。选择设备，然后再次点击 **部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。

步骤 2 在暂停同步之前，使用信息中心检查部署运行状况。

点击 Firepower 管理中心菜单上的“系统状态”图标以显示信息中心。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 3 暂停同步。

- a) 选择系统 (System) > 集成 (Integration)。
- b) 在高可用性选项卡，点击暂停同步。

步骤 4 逐一升级 Firepower 管理中心。

- a) 升级备用设备。
- b) 升级主用设备。

要进行升级，请按照[升级独立 Firepower 管理中心](#)，第 25 页中的说明进行操作，但省略初始部署，并在验证每个 Firepower 管理中心上的更新均成功后停止。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 5 在您想要设为主用对等设备的 Firepower 管理中心上，重新开始同步。

- a) 选择系统 > 集成。
- b) 在高可用性选项卡，点击设为主用。
- c) 等待至高可用性同步重新开始，并且其他 Firepower 管理中心切换到备用模式。

步骤 6 使用信息中心重新检查部署运行状况。

步骤 7 更新入侵规则和漏洞数据库 (VDB)。

如果支持站点上提供的入侵规则更新或 VDB 比当前运行的版本新，请安装新版本。有关详细信息，请参阅[Firepower 管理中心配置指南](#)。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 完成版本说明中所述的任何升级后配置更改。

步骤 9 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

升级 Firepower 威胁防御设备

- [Firepower 威胁防御升级核对表](#)，第 29 页
- [升级 Firepower 威胁防御软件](#)，第 31 页

Firepower 威胁防御升级核对表

请使用此核对表升级 Firepower 2100 系列、ASA 5500-X 系列、ISA 3000 和 Firepower 威胁防御虚拟设备。

每次升级时，请完成核对表。跳过步骤会导致升级失败。在整个升级过程中，确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

制定升级计划

请正确地规划和遵循升级路径，以保持良好的部署兼容性。

操作/检查	详细信息
检查您在升级路径中所处的阶段，了解已经完成的升级和即将执行的升级。	计划升级路径 ，第 6 页 Firepower 威胁防御 升级路径 - 使用 Firepower 管理中心 ，第 101 页
检查设备上的当前版本和目标版本： <ul style="list-style-type: none">• Firepower 威胁防御 软件• 虚拟托管环境（Firepower 威胁防御虚拟）	Firepower 威胁防御设备 ，第 92 页
检查 Firepower 管理中心在您对其升级后是否能够管理设备。如果不能，请修改您的升级路径，以便先升级 Firepower 管理中心。	Firepower 管理中心和受管设备版本兼容性 ，第 89 页
阅读有关下一个/下一组升级的版本说明，应特别注意版本特定的准则。	Firepower 版本说明

升级前的操作和检查

通过在维护窗口外执行预检查，尽量减少中断。

操作/检查	详细信息
进行必要的升级前配置更改。 准备好进行必要的升级后配置更改。	Firepower 软件升级的版本特定准则 ， 第 121 页 Firepower 版本说明
为 Firepower 软件升级运行初步磁盘空间检查。	Firepower 软件升级的时间和磁盘空间 ， 第 127 页
获取正确的 Firepower 软件升级软件包，并将其上传到 Firepower 管理中心。 从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。	获取升级软件包 ，第 8 页
请确保您的带宽足以将大量数据从 Firepower 管理中心传输到设备。	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）
将 Firepower 软件升级软件包推送到设备。（可选，6.2.3 及更高版本）	将升级软件包推送到受管设备 ，第 16 页
运行就绪性检查。（可选，6.1 及更高版本）	运行就绪性检查 ，第 17 页
使用 Firepower 管理中心为设备备份事件数据。 备份到外部位置并验证传输是否成功。在升级 Firepower 管理中心时，它会清除本地存储的备份。	Firepower 管理中心配置指南
	其他升级前的操作和检查 ，第 19 页
从以下方面进行考虑，将维护窗口安排在影响最小的时间段： <ul style="list-style-type: none"> • 您必须在维护窗口执行的任务。 • 升级对流量和检查的影响。 • 升级可能需要的最短时间。 	Firepower 威胁防御升级行为 ，第 115 页 Firepower 软件升级的时间和磁盘空间 ，第 127 页

执行设备升级

由于升级可能会造成流量中断或检查中断，因此请在维护窗口执行升级。

	操作/检查	详细信息
	如果需要，请升级托管环境（仅限 Firepower 威胁防御虚拟）。	请参阅您的托管环境的相关文档。
	升级 Firepower 软件。	升级 Firepower 威胁防御软件，第 31 页

升级 Firepower 威胁防御软件

使用此程序可升级 Firepower 2100 系列、ASA 5500-X 系列、ISA 3000 和 Firepower 威胁防御虚拟设备。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。您必须同时升级高可用性对的成员。



注意 请勿将更改部署到正在升级的设备或从其部署更改，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 思科 TAC。

开始之前

检查您在升级路径中所处的位置，包括虚拟托管环境和 Firepower 管理中心升级。请确保您已为此步骤做好充分的计划和准备。

步骤 1 将配置部署到您要升级的设备。

在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。选择设备，然后再次点击**部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。有关详细信息，请参阅 [Firepower 威胁防御升级行为，第 115 页](#)。

步骤 2 执行最终的升级前检查。

- 检查运行状况 - 使用信息中心（点击菜单栏上的系统状态图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务 - 此项也位于信息中心中，用于确保完成重要任务。在升级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。
- 检查磁盘空间 - 执行最终磁盘空间检查。如果可用磁盘空间不足，会导致升级失败。

步骤 3 （可选，仅限高可用性）交换高可用性设备对的主用/备用角色。

首先升级高可用性对中的备用设备。设备切换角色，然后升级新的备用设备。升级完成后，设备的角色保持切换状态。如果不想改变主用/备用角色，请先手动切换角色，然后再进行升级。这样，升级过程会将它们切换回来。

选择**设备 > 设备管理**，点击对等设备旁边的**切换主用设备**图标并确认您的选择。

步骤 4 依次选择**系统 (System) > 更新 (Updates)**。

步骤 5 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 我们强烈建议同时升级的设备数不超过五个。Firepower 管理中心不允许在所有选定设备完成升级过程之前停止设备升级。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，然后您才可以解决该问题。

步骤 6 点击**安装**，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[Firepower 威胁防御升级行为](#)，第 115 页。

步骤 7 在消息中心监控升级进度。

在升级过程中，请勿将配置部署到设备。即使消息中心在数分钟内不显示进度，或指示升级失败，请勿重新开始升级或重启设备。而是联系思科 TAC 寻求帮助。

步骤 8 验证更新是否成功。

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。

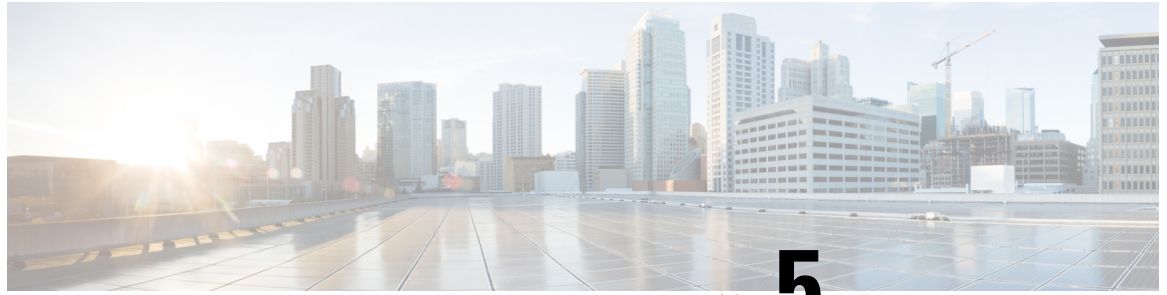
步骤 9 使用消息中心重新检查部署运行状况。

步骤 10 更新入侵规则和漏洞数据库 (VDB)。

如果支持站点上提供的入侵规则更新或 VDB 比当前运行的版本新，请安装新版本。有关详细信息，请参阅[Firepower 管理中心配置指南](#)。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 11 完成版本说明中所述的任何升级后配置更改。

步骤 12 将配置重新部署到将刚才升级的设备。



第 5 章

升级 Firepower 威胁防御设备 - Firepower 4100/9300 系列

- [Firepower 威胁防御升级核对表 - Firepower 4100/9300 机箱，第 33 页](#)
- [升级 FXOS - Firepower 4100/9300 机箱，第 35 页](#)
- [升级 Firepower 威胁防御软件 - Firepower 4100/9300 机箱，第 53 页](#)

Firepower 威胁防御升级核对表 - Firepower 4100/9300 机箱

请使用此核对表升级 Firepower 4100/9300 机箱。

每次升级时，请完成核对表。跳过步骤会导致升级失败。在整个升级过程中，确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

制定升级计划

请正确地规划和遵循升级路径，以保持良好的部署兼容性。

操作/检查	详细信息
检查您在升级路径中所处的阶段，了解已经完成的升级和即将执行的升级。	计划升级路径，第 6 页 Firepower 威胁防御 升级路径 - 使用 Firepower 管理中心，第 101 页
检查设备上的当前版本和目标版本： <ul style="list-style-type: none">• Firepower 软件• FXOS	具有 Firepower 4100/9300 机箱的 Firepower 威胁防御，第 93 页
检查 Firepower 管理中心在您对其升级后是否能够管理设备。如果不能，请修改您的升级路径，以便先升级 Firepower 管理中心。	Firepower 管理中心和受管设备版本兼容性，第 89 页

操作/检查	详细信息
阅读有关下一个/下一组升级的版本说明，应特别注意版本特定的准则。	Firepower 版本说明 FXOS 版本说明

升级前的操作和检查

通过在维护窗口外执行预检查，尽量减少中断。

操作/检查	详细信息
进行必要的升级前配置更改。 准备好进行必要的升级后配置更改。	Firepower 软件升级的版本特定准则 ， 第 121 页 Firepower 版本说明 FXOS 版本说明
为 Firepower 软件升级运行初步磁盘空间检查。	Firepower 软件升级的时间和磁盘空间 ， 第 127 页
获取正确的 Firepower 软件升级软件包，并将其上传到 Firepower 管理中心。 从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。	获取升级软件包 ，第 8 页
请确保您的带宽足以将大量数据从 Firepower 管理中心传输到设备。	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）
将 Firepower 软件升级软件包推送到设备。（可选，6.2.3 及更高版本）	将升级软件包推送到受管设备 ，第 16 页
运行就绪性检查。（可选，6.1 及更高版本）	运行就绪性检查 ，第 17 页
使用 Firepower 管理中心为设备备份事件数据。 备份到外部位置并验证传输是否成功。在升级 Firepower 管理中心时，它会清除本地存储的备份。	Firepower 管理中心配置指南
	其他升级前的操作和检查 ，第 19 页
从以下方面进行考虑，将维护窗口安排在影响最小的时间段： <ul style="list-style-type: none"> • 您必须在维护窗口执行的任务。 • 升级对流量和检查的影响。 • 升级可能需要的最短时间。 	Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱 ，第 113 页 Firepower 软件升级的时间和磁盘空间 ，第 127 页

执行设备升级

由于升级可能会造成流量中断或检查中断，因此请在维护窗口执行升级。

	操作/检查	详细信息
	如果需要，请升级 FXOS。 为避免流量和检查出现中断，请在高可用性对和机箱间集群中一次升级一个机箱。	升级 FXOS - Firepower 4100/9300 机箱，第 35 页
	升级 Firepower 软件。	升级 Firepower 威胁防御软件 - Firepower 4100/9300 机箱，第 53 页

升级 FXOS - Firepower 4100/9300 机箱

在 Firepower 4100/9300 机箱上，从 Firepower 软件单独升级 FXOS 操作系统。在每个机箱上独立升级 FXOS，即使配置了 Firepower 机箱间集群或高可用性对也是如此。

主要的 Firepower 版本具有随附的 FXOS 版本。在 Firepower 4100/9300 机箱上升级 Firepower 软件之前，您必须运行该随附版本的 FXOS。

升级 FXOS 会重启机箱。根据您的部署，流量可以不经检查就丢弃或穿越网络；请参阅 [Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱，第 113 页](#)。

在独立 Firepower 4100/9300 机箱上升级 FXOS

在将独立或机箱间集群 Firepower 威胁防御逻辑设备安装在设备上的 Firepower 4100/9300 系列安全设备上，使用 FXOS CLI 或 Firepower 机箱管理器升级 FXOS 平台捆绑包。

使用 Firepower 机箱管理器在独立 Firepower 4100/9300 机箱机箱上升级 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 Firepower 威胁防御逻辑设备且不是故障切换对或机箱间集群的一部分。
- Firepower 9300 机箱，其配置了不属于故障切换对或机箱间集群的一个或多个独立 Firepower 威胁防御逻辑设备。
- Firepower 9300 机箱，其在机箱内集群中配置了 Firepower 威胁防御逻辑设备。

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（请参阅[下载 Firepower 4100/9300 机箱的 FXOS](#)，第 15 页）。
- 备份您的 FXOS 和 Firepower 威胁防御配置。



注释 升级过程通常需要 20 到 30 分钟。在设备升级时，流量不会穿过设备。

步骤 1 在 Firepower 机箱管理器中，选择系统 > 更新。

“可用更新 (Available Updates)” 页面显示机箱上可用的 Firepower 可扩展操作系统 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：

- 点击**上传映像 (Upload Image)**，可打开“上传映像” (Upload Image) 对话框。
- 点击**选择文件**，可导航到并选择想要上传的映像。
- 点击**上传**。
已选中的映像被上传到 Firepower 4100/9300 机箱。
- 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。

Firepower 可扩展操作系统打开捆绑包，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 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：

- 输入 **scope system**。
- 输入 **show firmware monitor**。
- 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 systems
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 在独立 Firepower 4100/9300 机箱机箱上升级 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 Firepower 威胁防御逻辑设备且不是故障切换对或机箱间集群的一部分。
- Firepower 9300 机箱，其配置了不属于故障切换对或机箱间集群的一个或多个独立 Firepower 威胁防御设备。
- Firepower 9300 机箱，其在机箱内集群中配置了 Firepower 威胁防御逻辑设备。

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（请参阅[下载 Firepower 4100/9300 机箱的 FXOS](#)，第 15 页）。
- 备份您的 FXOS 和 Firepower 威胁防御配置。
- 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。



注释 升级过程通常需要 20 到 30 分钟。在设备升级时，流量不会穿过设备。

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**，可确认您想要继续安装，或者输入 **no**，可取消安装。

Firepower 可扩展操作系统打开捆绑包，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 systems
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。

在 Firepower 威胁防御高可用性对升级 FXOS

在将 Firepower 威胁防御逻辑设备配置为高可用性对的 Firepower 4100/9300 系列安全设备上，使用 FXOS CLI 或 Firepower 机箱管理器升级 FXOS 平台捆绑包。

使用 Firepower 机箱管理器在 Firepower 威胁防御高可用性对升级 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 Firepower 威胁防御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（请参阅[下载 Firepower 4100/9300 机箱的 FXOS，第 15 页](#)）。
- 备份您的 FXOS 和 Firepower 威胁防御配置。



注释 每个机箱的升级过程通常需要 20 到 30 分钟。

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 > 更新**。

“可用更新 (Available Updates)” 页面显示机箱上可用的 Firepower 可扩展操作系统 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：

- 点击**上传映像 (Upload Image)**，可打开“上传映像” (Upload Image) 对话框。
- 点击**选择文件**，可导航到并选择想要上传的映像。
- 点击**上传**。
已选中的映像被上传到 Firepower 4100/9300 机箱。
- 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。

Firepower 可扩展操作系统打开捆绑包，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 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：

- 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 systems
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 > 更新**。

“可用更新 (Available Updates)”页面显示机箱上可用的 Firepower 可扩展操作系统 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 (Upload Image)**，可打开“上传映像” (Upload Image) 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**。
已选中的映像被上传到 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。

Firepower 可扩展操作系统打开捆绑包，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 systems
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 Firepower 威胁防御高可用性对上升级 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 Firepower 威胁防御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（请参阅[下载 Firepower 4100/9300 机箱的 FXOS](#)，第 15 页）。
- 备份您的 FXOS 和 Firepower 威胁防御配置。
- 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。



注释 每个机箱的升级过程通常需要 20 到 30 分钟。

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 # scopeauto-install
```

步骤 5 安装 FXOS 平台捆绑包:

```
Firepower-chassis-a /firmware/auto-install # installplatformplatform-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**, 可确认您想要继续安装, 或者输入 **no**, 可取消安装。

Firepower 可扩展操作系统打开捆绑包, 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 # scopeauto-install
```

步骤 15 安装 FXOS 平台捆绑包:

```
Firepower-chassis-a /firmware/auto-install # installplatformplatform-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**, 可确认您想要继续安装, 或者输入 **no**, 可取消安装。

Firepower 可扩展操作系统打开捆绑包, 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 systems
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) 点击是将使备用设备立即变成高可用性对中的主用设备。

在 Firepower 威胁防御机箱间集群上升级 FXOS

在将 Firepower 威胁防御逻辑设备配置为机箱间集群的 Firepower 4100/9300 系列安全设备上，使用 FXOS CLI 或 Firepower 机箱管理器升级 FXOS 平台捆绑包。

使用 Firepower 机箱管理器在 Firepower 威胁防御机箱间集群上升级 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 Firepower 威胁防御逻辑设备配置为机箱间集群，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（请参阅[下载 Firepower 4100/9300 机箱的 FXOS](#)，第 15 页）。

- 备份您的 FXOS 和 Firepower 威胁防御配置。



注释 每个机箱的升级过程通常需要 20 到 30 分钟。

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（应该没有主设备的机箱）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 Firepower 威胁防御软件版本。

注释 验证主设备不在该机箱中。“集群角色”设置为主的所有 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（应该没有主设备的机箱）上的 Firepower 机箱管理器。

步骤 3 在 Firepower 机箱管理器中，选择系统 > 更新。

“可用更新”页面显示机箱上可用的 Firepower 可扩展操作系统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**，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**。
已选中的映像被上传到 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**。

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。

Firepower 可扩展操作系统打开捆绑包，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 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主。

将机箱 2 上的某个安全模块设置为“主”后，机箱 1 中则不再包含主设备，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“主”角色返还机箱 1，请将机箱 1 上的某个安全模块设置为“主”。

使用 FXOS CLI 在 Firepower 威胁防御机箱间集群上升级 FXOS

如果您的 Firepower 9300 或 Firepower 4100 系列安全设备将 Firepower 威胁防御逻辑设备配置为机箱间集群，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（请参阅[下载 Firepower 4100/9300 机箱的 FXOS，第 15 页](#)）。
- 备份您的 FXOS 和 Firepower 威胁防御配置。
- 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。



注释 每个机箱的升级过程通常需要 20 到 30 分钟。

步骤 1 连接到机箱 2（应该没有主设备的机箱）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 Firepower 威胁防御软件版本。

注释 验证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**
- **ftftp://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**，可确认您想要继续安装，或者输入 **no**，可取消安装。

Firepower 可扩展操作系统打开捆绑包，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
Cluster   Slave
ftd        2         Enabled    Online       6.2.2.81     6.2.2.81
Cluster   Slave
ftd        3         Disabled   Not Available 6.2.2.81
Applicable None
FP9300-A /ssa #

```

步骤 10 将机箱 2 中的其中一个安全模块设为主。

将机箱 2 上的某个安全模块设置为“主”后，机箱 1 中则不再包含主设备，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“主”角色返还机箱 1，请将机箱 1 上的某个安全模块设置为“主”。

升级 Firepower 威胁防御软件 - Firepower 4100/9300 机箱

使用此程序可在 Firepower 4100/9300 机箱上升级 Firepower 威胁防御软件。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。



注意 请勿将更改部署到正在升级的设备或从其部署更改，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 思科 TAC。

开始之前

检查您在升级路径中所处的位置，包括 FXOS 和 Firepower 管理中心升级。请确保您已为此步骤做好充分的计划和准备。

步骤 1 将配置部署到您要升级的设备。

在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。选择设备，然后再次点击**部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。有关详细信息，请参阅 [Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱，第 113 页](#)。

步骤 2 执行最终的升级前检查。

- 检查运行状况 - 使用信息中心（点击菜单栏上的系统状态图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务 - 此项也位于信息中心中，用于确保完成重要任务。在升级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。
- 检查磁盘空间 - 执行最终磁盘空间检查。如果可用磁盘空间不足，会导致升级失败。

步骤 3 （可选，仅限高可用性）交换高可用性设备对的主用/备用角色。

首先升级高可用性对中的备用设备。设备切换角色，然后升级新的备用设备。升级完成后，设备的角色保持切换状态。如果不想改变主用/备用角色，请先手动切换角色，然后再进行升级。这样，升级过程会将它们切换回来。

选择 **设备 > 设备管理**，点击对等设备旁边的 **切换主用设备** 图标并确认您的选择。

步骤 4 依次选择系统 (System) > 更新 (Updates)。

步骤 5 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 我们强烈建议同时升级的设备数不超过五个。Firepower 管理中心不允许在所有选定设备完成升级过程之前停止设备升级。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，然后您才可以解决该问题。

步骤 6 点击安装，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 [Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱，第 113 页](#)。

步骤 7 在信息中心监控升级进度。

在升级过程中，请勿将配置部署到设备。即使信息中心在数分钟内不显示进度，或指示升级失败，请勿重新开始升级或重启设备。而是联系思科 TAC 寻求帮助。

步骤 8 验证更新是否成功。

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 9 使用信息中心重新检查部署运行状况。

步骤 10 更新入侵规则和漏洞数据库 (VDB)。

如果支持站点上提供的入侵规则更新或 VDB 比当前运行的版本新，请安装新版本。有关详细信息，请参阅 [Firepower 管理中心配置指南](#)。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 11 完成版本说明中所述的任何升级后配置更改。

步骤 12 将配置重新部署到将刚才升级的设备。



第 6 章

升级 Firepower 7000/8000 系列和 NGIPSv 设备

- [Firepower 7000/8000 系列和 NGIPSv 升级核对表，第 57 页](#)
- [升级 Firepower 7000/8000 系列和 NGIPSv，第 59 页](#)

Firepower 7000/8000 系列和 NGIPSv 升级核对表

请使用此核对表升级 Firepower 7000/8000 系列和 NGIPSv 设备。

每次升级时，请完成核对表。跳过步骤会导致升级失败。在整个升级过程中，确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

制定升级计划

请正确地规划和遵循升级路径，以保持良好的部署兼容性。

操作/检查	详细信息
检查您在升级路径中所处的阶段，了解已经完成的升级和即将执行的升级。	计划升级路径，第 6 页 Firepower 7000/8000 系列和 NGIPSv 升级路径 - 使用 Firepower 管理中心，第 105 页
检查设备上的当前版本和目标版本： <ul style="list-style-type: none">• Firepower 软件• 虚拟托管环境 (NGIPSv)	7000/8000 系列和传统设备，第 97 页 NGIPSv (虚拟受管设备)，第 98 页
检查 Firepower 管理中心在您对其升级后是否能够管理设备。如果不能，请修改您的升级路径，以便先升级 Firepower 管理中心。	Firepower 管理中心和受管设备版本兼容性，第 89 页
阅读有关下一个/下一组升级的版本说明，应特别注意版本特定的准则。	Firepower 版本说明

升级前的操作和检查

通过在维护窗口外执行预检查，尽量减少中断。

操作/检查	详细信息
进行必要的升级前配置更改。 准备好进行必要的升级后配置更改。	Firepower 软件升级的版本特定准则 ， 第 121 页 Firepower 版本说明
为 Firepower 软件升级运行初步磁盘空间检查。	Firepower 软件升级的时间和磁盘空间 ， 第 127 页
获取正确的 Firepower 软件升级软件包，并将其上传到 Firepower 管理中心。 从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。	获取升级软件包 ，第 8 页
请确保您的带宽足以将大量数据从 Firepower 管理中心传输到设备。	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）
将 Firepower 软件升级软件包推送到设备。（可选，6.2.3 及更高版本）	将升级软件包推送到受管设备 ，第 16 页
运行就绪性检查。（可选，6.1 及更高版本）	运行就绪性检查 ，第 17 页
使用 Firepower 管理中心为设备备份事件数据。 备份到外部位置并验证传输是否成功。在升级 Firepower 管理中心时，它会清除本地存储的备份。	Firepower 管理中心配置指南
	其他升级前的操作和检查 ，第 19 页
从以下方面进行考虑，将维护窗口安排在影响最小的时间段： <ul style="list-style-type: none"> • 您必须在维护窗口执行的任务。 • 升级对流量和检查的影响。 • 升级可能需要的最短时间。 	升级期间的流量、检查和设备行为 ， 第 113 页 Firepower 软件升级的时间和磁盘空间 ， 第 127 页

执行设备升级

由于升级可能会造成流量中断或检查中断，因此请在维护窗口执行升级。

操作/检查	详细信息
如果需要，请升级托管环境（仅限 NGIPSv）。	请参阅您的托管环境的相关文档。

	操作/检查	详细信息
	升级 Firepower 软件。	升级 Firepower 7000/8000 系列和 NGIPSv，第 59 页

升级 Firepower 7000/8000 系列和 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。



注意 请勿将更改部署到正在升级的设备或从其部署更改，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 思科 TAC。

开始之前

检查您在升级路径中所处的位置，包括虚拟托管环境和 Firepower 管理中心升级。请确保您已为此步骤做好充分的计划和准备。

步骤 1 将配置部署到您要升级的设备。

在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。选择设备，然后再次点击**部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。有关详细信息，请参阅 [Firepower 7000/8000 系列升级行为，第 117 页](#)或 [NGIPSv 升级行为，第 119 页](#)。

步骤 2 将配置部署到您要升级的设备。

在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。选择设备，然后再次点击**部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。

步骤 3 执行最终的升级前检查。

- 检查运行状况 - 使用消息中心（点击菜单栏上的系统状态图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务 - 此项也位于消息中心中，用于确保完成重要任务。在升级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。
- 检查磁盘空间 - 执行最终磁盘空间检查。如果可用磁盘空间不足，会导致升级失败。

步骤 4 (可选, 仅限高可用性) 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。设备切换角色, 然后升级新的备用设备。升级完成后, 设备的角色保持切换状态。如果不想改变主用/备用角色, 请先手动切换角色, 然后再进行升级。这样, 升级过程会将它们切换回来。

选择**设备 > 设备管理**, 点击对等设备旁边的**切换主用设备**图标并确认您的选择。

步骤 5 依次选择**系统 (System) > 更新 (Updates)**。

步骤 6 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 我们强烈建议同时升级的设备数不超过五个。Firepower 管理中心不允许在所有选定设备完成升级过程之前停止设备升级。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, 然后您才可以解决该问题。

步骤 7 点击**安装**, 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[Firepower 7000/8000 系列升级行为, 第 117 页](#)或[NGIPSv 升级行为, 第 119 页](#)。

步骤 8 在消息中心监控升级进度。

在升级过程中, 请勿将配置部署到设备。即使消息中心在数分钟内不显示进度, 或指示升级失败, 请勿重新开始升级或重启设备。而是联系思科 TAC 寻求帮助。

步骤 9 验证更新是否成功。

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 10 使用消息中心重新检查部署运行状况。

步骤 11 更新入侵规则和漏洞数据库 (VDB)。

如果支持站点上提供的入侵规则更新或 VDB 比当前运行的版本新, 请安装新版本。有关详细信息, 请参阅[Firepower 管理中心配置指南](#)。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 12 完成版本说明中所述的任何升级后配置更改。

步骤 13 将配置重新部署到将刚才升级的设备。



第 7 章

升级具备 FirePOWER 服务的 ASA

- [具备 FirePOWER 服务的 ASA 升级核对表](#)，第 61 页
- [升级 ASA](#)，第 63 页
- [升级 ASA FirePOWER 模块 - 使用 Firepower 管理中心](#)，第 84 页

具备 FirePOWER 服务的 ASA 升级核对表

请使用此核对表升级 具备 FirePOWER 服务的 ASA。

每次升级时，请完成核对表。跳过步骤会导致升级失败。在整个升级过程中，确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

制定升级计划

请正确地规划和遵循升级路径，以保持良好的部署兼容性。

操作/检查	详细信息
检查您在升级路径中所处的阶段，了解已经完成的升级和即将执行的升级。	计划升级路径 ，第 6 页 ASA FirePOWER 模块升级路径 - 使用 Firepower 管理中心 ，第 107 页
检查设备上的当前版本和目标版本： <ul style="list-style-type: none">• ASA FirePOWER 模块• ASA OS	具备 FirePOWER 服务的 ASA 设备 ，第 95 页
检查 Firepower 管理中心在您对其升级后是否能够管理设备。如果不能，请修改您的升级路径，以便先升级 Firepower 管理中心。	Firepower 管理中心和受管设备版本兼容性 ，第 89 页
阅读有关下一个/下一组升级的版本说明，应特别注意版本特定的准则。	Firepower 版本说明 ASA 版本说明

升级前的操作和检查

通过在维护窗口外执行预检查，尽量减少中断。

操作/检查	详细信息
进行必要的升级前配置更改。 准备好进行必要的升级后配置更改。	Firepower 软件升级的版本特定准则 ， 第 121 页 思科 ASA 升级指南中的制定升级计划
为 Firepower 软件升级运行初步磁盘空间检查。	Firepower 软件升级的时间和磁盘空间 ， 第 127 页
获取正确的 Firepower 软件升级软件包，并将其上传到 Firepower 管理中心。 从 6.2.1 及更高版本进行升级的软件包经过签名，并在 .sh.REL.tar 而不是只是 just .sh 中终止。请勿解压已签名的升级软件包。	获取升级软件包 ，第 8 页
请确保您的带宽足以将大量数据从 Firepower 管理中心传输到设备。	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）
将 Firepower 软件升级软件包推送到设备。（可选，6.2.3 及更高版本）	将升级软件包推送到受管设备 ，第 16 页
运行就绪性检查。（可选，6.1 及更高版本）	运行就绪性检查 ，第 17 页
使用 Firepower 管理中心为设备备份事件数据。 备份到外部位置并验证传输是否成功。在升级 Firepower 管理中心时，它会清除本地存储的备份。	Firepower 管理中心配置指南
	其他升级前的操作和检查 ，第 19 页
从以下方面进行考虑，将维护窗口安排在影响最小的时间段： <ul style="list-style-type: none"> • 您必须在维护窗口执行的任务。 • 升级对流量和检查的影响。 • 升级可能需要的最短时间。 	ASA FirePOWER 升级行为 ，第 118 页 Firepower 软件升级的时间和磁盘空间 ，第 127 页

升级具备 FirePOWER 服务的 ASA

由于升级可能会造成流量中断或检查中断，因此请在维护窗口执行升级。

	操作/检查	详细信息
	在不需要 ASA 升级的设备上升级 ASA FirePOWER 模块。	升级 ASA FirePOWER 模块 - 使用 Firepower 管理中心 ，第 84 页
	在独立 ASA 设备上升级 ASA 和 ASA FirePOWER 模块。 在升级 ASA 并重新加载后，立即使用 Firepower 管理中心升级 ASA FirePOWER 模块。	升级独立设备 ，第 63 页 那么 升级 ASA FirePOWER 模块 - 使用 Firepower 管理中心 ，第 84 页
	在集群和故障切换对中的 ASA 设备上升级 ASA 和 ASA FirePOWER 模块。 为避免流量和检查出现中断，请逐一对设备进行完整升级。在重新加载每个设备以升级 ASA 之前，使用 Firepower 管理中心升级 ASA FirePOWER 模块。	以下任一项： 升级主用/备用故障切换对 ，第 67 页 升级主用/主用故障切换对 ，第 71 页 升级 ASA 集群 ，第 76 页 那么 升级 ASA FirePOWER 模块 - 使用 Firepower 管理中心 ，第 84 页

升级 ASA

使用本部分中的程序为独立、故障切换或集群部署升级 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://[user[:password]@]server[/path]/asa_image_name disk0:[/path]/asa_image_name
```

示例：

```
ciscoasa# copy ftp://jcrichon:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-smp-k8.bin
```

步骤 2 将 ASDM 映像复制到闪存中。

copy ftp://[[user[:password]@]server[/path]/asdm_image_namediskn:]/[path]/asdm_image_name

示例:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.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 diskn:]/[path]/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 diskn:]/[path]/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:/asa991-smp-k8.bin
```

步骤 7 设置要使用的 ASDM 映像（您刚上传的映像）：

asdm image diskn:]/[path]/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-771791.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 **Upgrade Software** 对话框。

步骤 2 从 **Image to Upload** 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 **Upload Image**。

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 **Yes**。

步骤 7 系统会提示您退出 ASDM 并保存配置。点击 **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连接到 ASDM。

步骤 8 重复上述步骤, 从 **Image to Upload** 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 **Save the running configuration at the time of reload** 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 **Schedule Reload**。

重新加载开始后，系统将显示 **Reload Status** 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 如果您要升级 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，如果您要下载 9.4(1)，实际下载的可能为 9.4(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，请重新启动 ASA 以保存配置并完成升级。

步骤 1 依次选择 **工具 > 检查 ASA/ASDM 更新**。

在多情景模式中，从 System 访问此菜单。

系统将显示 **Cisco.com Authentication** 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 Upgrade Wizard**。

注释 如果无可用升级，系统将显示对话框。点击 **OK** 退出向导。

步骤 3 点击 **Next** 显示 **Select Software** 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 **Upgrade to** 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 **Upgrade to** 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 **Next**，显示 **Review Changes** 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 **Next**，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 **Results** 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 **Finish**，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 如果您要升级 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/备用故障切换对

使用 CLI 或 ASDM 升级主用/备用故障切换对，以实现零停机升级。

使用 CLI 升级主用/备用故障切换对

要升级主用/备用故障切换对，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 提示符确定故障切换状态；您可以配置 ASA 提示符以显示故障切换状态和优先级（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://[[user[:password]@]server[/path]/asa_image_namediskn:[/path]/asa_image_name
```

示例：

```
asa/act# copy ftp://jcrichon:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-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://[[user[:password]@]server[/path]/asa_image_namediskn:[/path]/asa_image_name
```

示例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asa991-smp-k8.bin
disk0:/asa991-smp-k8.bin
```

步骤 3 将 ASDM 映像复制至主用设备闪存：

```
copy ftp://[[user[:password]@]server[/path]/asdm_image_namediskn:[/path]/asdm_image_name
```

示例：

```
asa/act# copy ftp://jcrichon:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.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://[[user[:password]@]server[/path]/asdm_image_namediskn:[/path]/asdm_image_name
```

示例：

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichon:aeryn@10.1.1.1/asdm-771791.bin
disk0:/asdm-771791.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 diskn:[path]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 diskn:[path]asa_image_name

示例：

```
asa/act(config)# boot system disk0://asa991-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 diskn:[path]asdm_image_name

示例：

```
asa/act(config)# asdm image disk0:/asdm-771791.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** 命令可验证备用设备是否处于备用就绪状态。

步骤 14 强行要求主用设备故障切换至备用设备。

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/备用故障切换对

要升级主用/备用故障切换对，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 连接到备用 IP 地址，以此在备用设备上启动 ASDM。

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

系统将显示 **Upgrade Software** 对话框。

步骤 3 从 **Image to Upload** 下拉列表中选择 **ASDM**。

步骤 4 在 **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 **Browse Local Files** 在计算机中查找该文件。

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

步骤 6 点击 **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 **No**。您会退出 Upgrade 工具。

- 步骤 7** 重复这些步骤，从 **Image to Upload** 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 **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 **Yes**。
- 系统会提示您退出 ASDM 并保存配置。点击 **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 **Yes**。
- 系统将提示您重新加载 ASA 以使用新映像。点击 **OK**。您会退出 Upgrade 工具。
- 步骤 12** 点击工具栏上的 **Save** 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** 如果您要升级 ASA FirePOWER 模块，请通过选择 **工具 > 命令行界面**，然后输入 **no rest-api 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 > 属性 > 故障切换 > 状态**，然后点击 **重新加载备用**，重新加载备用设备。
- 重新加载备用设备时，停留在系统窗格以进行监控。
- 步骤 16** 重新加载备用设备后，强制主用设备执行故障切换到备用设备，方法为：**选择监控 > 属性 > 故障切换 > 状态**，然后点击 **设为备用**。
- ASDM 将自动重新连接到新的主用设备。
- 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 > 属性 > 故障切换 > 状态**，然后点击 **重新加载备用**。

升级主用/主用故障切换对

使用 CLI 或 ASDM 升级主用/主用故障切换对，以实现零停机升级。

使用 CLI 升级主用/主用故障切换对

要升级主用/主用故障切换配置中的两台设备，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://[[user[:password]@]server[/path]/asa_image_name]diskn:[/path]/asa_image_name
```

示例：

```
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-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://[[user[:password]@]server[/path]/asa_image_name]diskn:[/path]/asa_image_name
```

示例：

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-smp-k8.bin
```

步骤 3 将 ASDM 映像复制至主设备闪存：

```
copy ftp://[[user[:password]@]server[/path]/asdm_image_name]diskn:[/path]/asdm_image_name
```

示例：

```
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.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://[[user[:password]@]server[/path]/asdm_image_name]diskn:[/path]/asdm_image_name
```

示例：

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin disk0:/asdm-771791.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 diskn:[path]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 diskn:[path]asa_image_name

示例：

```
asa/act/pri(config)# boot system disk0://asa991-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 diskn:[path]asdm_image_name

示例：

```
asa/act/pri(config)# asdm image disk0:/asdm-771791.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 使两个故障切换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 连接到故障切换组 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** 命令验证两个故障切换组是否处于备用就绪状态。

步骤 15 强行要求两个故障切换组在辅助设备变为活动状态：

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，请重新连接到故障切换组 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 连接到故障切换组 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 如果使用 **preempt** 命令配置故障切换组，则取代延迟过后，它们将在其专用设备上自动变为活动状态。

使用 ASDM 升级主用/主用故障切换对

要升级主用/主用故障切换配置中的两台设备，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** 通过连接到故障切换组 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 **Upgrade Software** 对话框。
- 步骤 3** 从 **Image to Upload** 下拉列表中选择 **ASDM**。
- 步骤 4** 在本地文件路径字段中，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** 在 PC 中查找文件。
- 步骤 5** 在 **Flash File System Path** 字段中，输入闪存文件系统的路径，或者点击 **Browse Flash** 在闪存文件系统中查找目录或文件。
- 步骤 6** 点击 **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 **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**。您会退出 Upgrade 工具。
- 步骤 8** 通过连接至故障切换组 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** 系统提示您将此映像设置为 ASDM 映像时，点击 **Yes**。
- 系统会提示您退出 ASDM 并保存配置。点击 **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** 系统提示您将此映像设置为 ASA 映像时，点击 **Yes**。
- 系统将提示您重新加载 ASA 以使用新映像。点击 **OK**。您会退出 Upgrade 工具。
- 步骤 12** 点击工具栏上的 **Save** 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** 如果您要升级 ASA FirePOWER 模块，请通过选择 **工具 > 命令行界面**，然后输入 **no rest-api 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** 通过依次选择 **监控 > 故障切换 > 故障切换编号**（该编号是您要移动至主设备的故障切换组的编号），然后点击 **设为主用** 来确保故障切换组在主设备上处于活动状态。

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 连接到故障切换组 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 > 故障切换 > 系统**，然后点击**重新加载备用**。

重新加载辅助设备时，停留在**系统**窗格以进行监控。

步骤 17 辅助设备启动后，通过依次选择**监控 > 故障切换 > 故障切换编号**（该编号是您要移动至辅助设备的故障切换组的编号），然后点击**设为备用**来确保故障切换组在辅助设备上处于活动状态。

ASDM 将自动重新连接到辅助设备上的故障切换组 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 连接到故障切换组 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 > 故障切换 > 系统**，然后点击**重新加载备用**。**步骤 20** 如果故障切换组被配置为 **Preempt Enabled**，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切换组 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

- 在主设备上执行这些步骤。如果您还要升级 ASA FirePOWER 模块，则需要每台从属设备上访问控制台或 ASDM。您可以将 ASA 提示符配置为显示集群设备和状态（主设备或从属设备），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，将主设备的上的 ASA 软件复制到集群中的所有设备。

cluster exec copy /noconfirm ftp://[[user[:password]@]server[/path]/asa_image_namediskn:]/[path]/asa_image_name
示例：

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa991-smp-k8.bin disk0:/asa991-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://[[user[:password]@]server[/path]/asdm_image_name]diskn:[/path]/asdm_image_name
```

示例：

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-771791.bin
disk0:/asdm-771791.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 diskn:[/path]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 diskn:[/path]asa_image_name
```

示例：

```
asa/unit1/master(config)# boot system disk0://asa991-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:/[path]/asdm_image_name
```

示例：

```
asa/unit1/master(config)# asdm image disk0:/asdm-771791.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从属设备。

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 升级从属设备。

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从属设备控制台或 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** 命令强制将某个从属设备变为主设备；否则可能导致网络连接和集群稳定相关的问题。您必须先升级和重新加载所有从属设备，然后继续此过程以确保从当前主设备顺利地过渡到新的主设备。

如果不进行 ASA FirePOWER 模块升级：

- a) 在主设备上，要查看成员名称，请输入 **cluster exec unit ?**，或者输入 **show cluster info** 命令。
- b) 重新加载从属设备。

cluster exec unit 从属设备 **reload noconfirm**

示例：

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

- c) 对每个从属设备重复上述操作。

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（使用从属设备控制台）：

- a) 连接到从属设备的控制台端口，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 名称

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) 在此从属设备上升级 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。等待升级完成。

- d) 重新加载从属设备。

reload noconfirm

- e) 对每个从属设备重复上述操作。

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从属设备的单个管理 IP 地址。
- b) 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 **Participate in ASA cluster** 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 **Configure ASA cluster settings** 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 **Apply**。
- 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 **Schedule Reload**。
- j) 请点击 **是继续重新加载**。
- k) 对每个从属设备重复上述操作。

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，请查看主设备上的监控 > ASA 集群 > 集群摘要窗格。

步骤 12 升级主设备。

- a) 禁用集群。

cluster group 名称

no enable

等待 5 分钟，以便选择新的主设备且流量稳定下来。

不保存此配置；您希望在重新加载时启用集群。

我们建议在主设备上手动禁用集群（如果可能），以便尽可能快速顺畅地选择新的主设备。

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 地址现在属于新的主设备；此以前的主设备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

当以前的主设备重新加入集群时，它将成为从属设备。

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

- 在主设备上执行这些步骤。如果您还要升级 ASA FirePOWER 模块，则需要 ASDM 访问每台从属设备。
- 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，在主设备上启动 ASDM。

此 IP 地址始终属于主设备。

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 **Upgrade Software from Local Computer** 对话框。

步骤 3 点击集群中的所有设备单选按钮。

系统将显示 **Upgrade Software** 对话框。

步骤 4 从 **Image to Upload** 下拉列表中选择 **ASDM**。

步骤 5 在本地文件路径字段中，点击浏览本地文件以查找您计算机上的文件。

步骤 6 （可选）在 **Flash File System Path** 字段中，输入闪存文件系统的路径，或者点击 **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 **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 **Yes**。

步骤 9 系统会提示您退出 ASDM 并保存配置。点击 **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 **Save** 图标，保存配置更改。

这些配置更改会自动保存到从属设备。

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 直接连接到从属设备。

步骤 13 如果您要升级 ASA FirePOWER 模块，请通过选择工具 > 命令行界面，然后输入 **no rest-api 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 升级从属设备。

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 > 将主设备更改为下拉列表强制辅助设备成为主设备；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从属设备，然后继续此过程以确保从当前主设备顺利地过渡到新的主设备。

如果不进行 **ASA FirePOWER 模块升级**：

- a) 在主设备上，选择工具 > 系统重新加载。
- b) 从设备下拉列表中，选择从属设备名称。
- c) 点击 **Schedule Reload**。
- d) 请点击是继续重新加载。
- e) 对每个从属设备重复上述操作。

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。

如果还进行 ASA FirePOWER 模块升级：

- a) 在主设备上，选择 **配置 > 设备管理 > 高可用性和稳定性 > ASA 集群 > 集群成员**。
- b) 选择要升级的从属设备，然后点击 **删除**。
- c) 点击 **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 连接到从属设备。
- 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** 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 **Schedule Reload**。
- i) 请点击 **是** 继续重新加载。
- j) 对每个从属设备重复上述操作。

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 升级主设备。

- a) 在主设备上的 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** 复选框，然后点击 **应用**。

系统会提示您退出 ASDM。

- c) 最多等待 5 分钟，以便选择新的主设备且流量稳定下来。

当以前的主设备重新加入集群时，它将成为从属设备。

- d) 通过连接到您之前记下的单个管理 IP 地址，将 ASDM 重新连接到之前的主设备。

主集群 IP 地址现在属于新的主设备；此以前的主设备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** 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 **Schedule Reload**。
- i) 请点击 **是** 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主设备。

升级 ASA FirePOWER 模块 - 使用 Firepower 管理中心

使用此程序升级由 Firepower 管理中心管理的 ASA FirePOWER 模块。

如果您要在独立 ASA 设备上升级 ASA 及 ASA FirePOWER 模块，请在升级 ASA 后升级模块并重新加载。如果您要在集群或故障切换 ASA 设备上升级 ASA 和 ASA FirePOWER 模块，请在重新加载每台设备之前升级每个模块。有关详细信息，请参阅[ASA FirePOWER 模块升级路径 - 使用 Firepower 管理中心](#)，第 107 页和 ASA 升级程序。

如果您不升级 ASA，则可以一同升级所有 ASA FirePOWER 模块，而不考虑 ASA 故障切换或集群配置。但是，您仍应请参阅 ASA 故障切换和集群升级程序，以便可以在模块升级之前在设备上执行故障切换或禁用集群，以避免流量丢失。



注意 请勿将更改部署到正在升级的设备或从其部署更改，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 思科 TAC。

开始之前

检查您在升级路径中所处的位置，包括 ASA 和 Firepower 管理中心升级。请确保您已为此步骤做好充分的计划和准备。

ASA 与 ASA FirePOWER 版本之间没有广泛的兼容性。但是，即使并非严格要求进行 ASA 升级，但是解决问题可能需要升级到支持的最新版本。

步骤 1 将配置部署到您要升级的设备。

在 Firepower 管理中心菜单栏上，点击**部署 (Deploy)**。选择设备，然后再次点击**部署**。如果现在不部署到过期设备，其最终升级可能会失败，而且您可能需要对其重新映像。

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 进程，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。有关详细信息，请参阅[ASA FirePOWER 升级行为](#)，第 118 页。

步骤 2 (升级到 6.1 及更高版本) 禁用 ASA REST API。

如果不禁用 REST API，升级将会失败。请注意，如果您还在运行 6.0 及更高版本的 ASA FirePOWER 模块，则 ASA 5506-X 系列设备不支持 ASA REST API。

在 ASA 上使用 CLI 以禁用 REST API:

```
no rest-api agent
```

您可以在升级后重新启用它：

rest-api agent

步骤 3 执行最终的升级前检查。

- 检查运行状况 - 使用信息中心（点击菜单栏上的系统状态图标）。确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。
- 正在运行的任务 - 此项也位于信息中心中，用于确保完成重要任务。在升级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。
- 检查磁盘空间 - 执行最终磁盘空间检查。如果可用磁盘空间不足，会导致升级失败。

步骤 4 依次选择系统 (System) > 更新 (Updates)。

步骤 5 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 我们强烈建议同时升级的设备数不超过五个。Firepower 管理中心不允许在所有选定设备完成升级过程之前停止设备升级。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，然后您才可以解决该问题。

步骤 6 点击**安装**，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[ASA FirePOWER升级行为，第 118 页](#)。

步骤 7 在信息中心监控升级进度。

在升级过程中，请勿将配置部署到设备。即使信息中心在数分钟内不显示进度，或指示升级失败，请勿重新开始升级或重启设备。而是联系思科 TAC 寻求帮助。

步骤 8 验证更新是否成功。

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 9 使用信息中心重新检查部署运行状况。

步骤 10 更新入侵规则和漏洞数据库 (VDB)。

如果支持站点上提供的入侵规则更新或 VDB 比当前运行的版本新，请安装新版本。有关详细信息，请参阅[Firepower 管理中心配置指南](#)。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 11 完成版本说明中所述的任何升级后配置更改。

步骤 12 将配置重新部署到将刚才升级的设备。



第 II 部分

参考信息

- [Firepower 设备的兼容性](#)，第 89 页
- [升级途径](#)，第 99 页
- [升级期间的流量、检查和设备行为](#)，第 113 页
- [Firepower 软件升级的版本特定准则](#)，第 121 页
- [Firepower 软件升级的时间和磁盘空间](#)，第 127 页



第 8 章

Firepower 设备的兼容性

以下主题提供了每个受支持的 Firepower 版本的思科 Firepower 软件和硬件兼容性，包括操作系统和托管环境要求。



注释 本指南提供与升级过程相关的兼容性信息。有关详细信息，请参阅 *Firepower* 系统兼容性指南。

- [Firepower 管理中心和受管设备版本兼容性，第 89 页](#)
- [各型号的 Firepower 兼容性，第 91 页](#)

Firepower 管理中心和受管设备版本兼容性

下表列出了 Firepower 管理中心与受管设备版本的兼容性。



注释 请记住，许多功能的可用性取决于在设备上运行的 Firepower 版本。即使 Firepower 管理中心是正在运行的特定版本，您的部署可能不支持其所有功能，直到您同时还将受管设备升级到该版本。

表 6: *Firepower* 管理中心和受管设备版本兼容性

Firepower 管理中心版本	受管设备版本
6.2.3	6.2.3
	6.2.2
	6.2.1 (仅限 firepower 2100)
	6.2.0
	6.1.0

Firepower 管理中心版本	受管设备版本
6.2.2	6.2.2 6.2.1 (仅限 firepower 2100) 6.2.0 6.1.0
6.2.1	6.2.1 (仅限 firepower 2100) 6.2.0 6.1.0
6.2.0	6.2.0 6.1.0
6.1.0	6.1.0 6.0.1 6.0.0 5.4.1 5.4.0
6.0.1	6.0.1 (第一个 Firepower 威胁防御版本) 6.0.0 5.4.1 5.4.0
6.0.0	6.0.0 5.4.1 5.4.0
5.4.1	5.4.1 (ASA 5506-X、5508-X 和 5516-X 上的第一个 ASA FirePOWER 模块版本) 5.4.0 5.3.1 5.3.0
5.4.0	5.4.0 5.3.1 5.3.0
5.3.1	5.3.1 (第一个 ASA FirePOWER 模块版本) 5.3.0

Firepower 管理中心版本	受管设备版本
5.3.0	5.3.0

各型号的 Firepower 兼容性

本部分的表格按型号列出了 Firepower 软件、平台和操作系统之间的兼容性。

Firepower 管理中心：物理

Firepower 版本	DC500 (EOL) DC1000 (EOL) DC3000 (EOL)	MC750 MC1500 MC3500	MC2000 MC4000	MC1000 MC2500 MC4500
6.2.3	-	是	是	是
6.2.2.x	-	是	是	是
6.2.1	-	是	是	是
6.2.0.x	-	是	是	是
6.1.x.x	-	是	是	-
6.0.1.x	-	是	是	-
6.0.0.x	-	是	是	-
5.4.1.x	是	是	是	-
5.4 仅限 5.4.0；使用 5.4.1.x 版本防御中心管理 5.4.x 设备。	是	是	是	-
5.3.1.x	是 5.3.1.4 - 5.3.1.7 除外	是	-	-
5.3.0.x 5.3.0.4 - 5.3.0.8 除外	是	是	-	-

Firepower 管理中心：虚拟

Firepower 版本	VMware vCloud Director	VMware vSphere/VMware ESXi					Amazon Web Services (AWS)	基于内核的虚拟机 (KVM)
	5.1	5.0	5.1	5.5	6.0	6.5	EC2/VPC	KVM
6.2.3	-	-	-	是	是	是	是	是
6.2.2.x	-	-	-	是	是	-	是	是
6.2.1	-	-	-	是	是	-	是	是
6.2.0.x	-	-	-	是	是	-	是	是
6.1.x.x	-	-	-	是	是	-	是	是
6.0.1.x	-	-	是	是	-	-	是	-
6.0.0.x	-	-	是	是	-	-	-	-
5.4.1.x	是	是	是	是	-	-	-	-
5.4 仅限 5.4.0；使用 5.4.1.x 版本防御中心管理 5.4.x 设备。	是	是	是	是	-	-	-	-
5.3.1.x	是 5.3.1 除外	是	是	-	-	-	-	-
5.3.0.x 5.3.0.4 - 5.3.0.8 除外	是	是	是	-	-	-	-	-

Firepower 威胁防御设备

下表列出了 Firepower 威胁防御与各种不同设备平台的兼容性。它们还包括对精选平台的 FXOS 要求以及虚拟实施的兼容托管环境。

具备 Firepower 威胁防御的 Firepower 2100 系列

Firepower 2100 系列设备使用 FXOS 操作系统。升级 Firepower 软件时会自动升级 FXOS。

Firepower 版本	Firepower 2110 Firepower 2120 Firepower 2130 Firepower 2140
6.2.3	是
6.2.2.x	是
6.2.1	是

具有 Firepower 4100/9300 机箱的 Firepower 威胁防御

运行 Firepower 软件的 Firepower 4100/9300 机箱使用 FXOS 操作系统。您必须从 Firepower 软件单独升级 FXOS。

以粗体显示的 FXOS 版本是 Firepower 版本的随附版本。要运行指定版本的 Firepower，请使用以粗体显示的 FXOS 版本。仅在升级情景中，才可将新版本的 FXOS 与旧版本的 Firepower 一起使用。

Firepower 版本	Firepower 9300	Firepower 4110 Firepower 4120 Firepower 4140	Firepower 4150
6.2.3	2.3.1.73 及更高版本	2.3.1.73 及更高版本	2.3.1.73 及更高版本
6.2.2.x	2.2.2.x 2.3.1.73 及更高版本	2.2.2.x 2.3.1.73 及更高版本	2.2.2.x 2.3.1.73 及更高版本
6.2.1	-	-	-
6.2.0.x	2.1.1.x 2.2.1.x 2.2.2.x 2.3.1.73 及更高版本	2.1.1.x 2.2.1.x 2.2.2.x 2.3.1.73 及更高版本	2.1.1.x 2.2.1.x 2.2.2.x 2.3.1.73 及更高版本
6.1.x.x	2.0.1.x 2.1.1.x 2.3.1.73 及更高版本	2.0.1.x 2.1.1.x 2.3.1.73 及更高版本	2.0.1.x 2.1.1.x 2.3.1.73 及更高版本
6.0.1.x	1.1.4.x 2.0.1.x (6.0.1.1 除外)	1.1.4.x 2.0.1.x (6.0.1.1 除外)	—

具有 ASA 5500-X 系列的 Firepower 威胁防御

Firepower 版本	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X
6.2.3	是	是
6.2.2.x	是	是
6.2.1	-	-
6.2.0.x	是	是
6.1.x.x	是	是
6.0.1.x	是	是

具有 Firepower 威胁防御的 ISA 3000

Firepower 版本	ISA 3000
6.2.3	是

Firepower 威胁防御虚拟

Firepower 版本	VMware vSphere/VMware ESXi				Amazon Web Services (AWS)	基于内核的虚拟机 (KVM)	Microsoft Azure
	5.1	5.5	6.0	6.5	EC2/VPC	KVM	Std.D3, D3_v2
6.2.3	-	是	是	是	是	是	是
6.2.2.x	-	是	是	-	是	是	是
6.2.1	-	-	-	-	-	-	-
6.2.0.x	-	是	是	-	是	是	是
6.1.x.x	-	是	是	-	是	是	-
6.0.1.x	是	是	-	-	是	-	-

具备 FirePOWER 服务的 ASA 设备

ASA FirePOWER 模块在 ASA 操作系统上运行。

对于具备 FirePOWER 服务的 ASA 设备，您必须从 ASA FirePOWER 模块单独升级 ASA（最好先升级）。

具备 ASA FirePOWER 的 ASA 5500-X 系列



注释 由于 [CSCuc91730](#)，我们建议您升级到 ASA 9.2(4.5) 及更高版本、9.3(3.8) 及更高版本或 9.4(2) 及更高版本。

表 7: 具备 ASA FirePOWER 6.x 版的 ASA 5500-X 系列

Firepower 版本	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5585-X	ASDM 管理
6.2.3	9.5(2)、9.5(3) - 5506 型号除外 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.9(2)
6.2.2.x	9.5(2)、9.5(3) - 5506 型号除外 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.8(2) 及更高版本
6.2.1	-			-
6.2.0.x	9.5(2)、9.5(3) - 5506 型号除外 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.7(1) 及更高版本

Firepower 版本	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5585-X	ASDM 管理
6.1.x.x	9.5(2)、9.5(3) - 5506 型号除外 9.6(x) 9.7(x) 9.8(x) 9.9(x)			7.6(2) 及更高版本
6.0.1.x	9.4(x) - 没有 ASDM 或强制门户 9.5(1.5) - 没有强制门户 9.5(2)、9.5(3) 9.6(x)			7.6(1) 及更高版本
6.0.0.x	9.4(x) - 没有 ASDM 或强制门户 9.5(1.5) - 没有强制门户 9.5(2)、9.5(3) 9.6(x)			7.5(1.112) 及更高版本

表 8: 具备 ASA 5500-X 系列 5.x 版的 ASA FirePOWER

Firepower 版本	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5585-X	ASDM 管理
5.4.1.x	9.3(2)、9.3(3) - 仅限 5506 型号 9.4(x) 9.5(1.5)、9.5(2)、9.5(3) 9.6(x) 9.7(x) 9.8(x) 9.9(x)	—		7.3(3) 及更高版本 - 仅限 5506 型号 7.4(1) 及更高版本

Firepower 版本	ASA 5506-X ASA 5506H-X ASA 5506W-X ASA 5508-X ASA 5516-X	ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	ASA 5585-X	ASDM 管理
5.4.0.x	—	9.2(2.4)、9.2(3)、9.2(4) - 仅限 5.4.0 版本 9.3(2)、9.3(3) 9.4(x) 9.5(1.5)、9.5(2)、9.5(3) 9.6(x) 9.7(x) 9.8(x) 9.9(x)	—	—
5.3.1.x	—	9.2(2.4)、9.2(3)、9.2(4)	—	—

具备 ASA FirePOWER 的 ISA 3000

Firepower 版本	ASA OS	ASDM 管理
5.4.1.7 及更高版本 仅限 5.4.1.x 序列	9.4(1.225) 9.5(2)、9.5(3) 9.6(x)	7.5(1.112) 及更高版本

7000/8000 系列和传统设备

Firepower 版本	7000 和 8000 系列，包括 AMP	系列2
6.2.3	是	-
6.2.2.x	是	-
6.2.1	-	-
6.2.0.x	是	-
6.1.x.x	是	-
6.0.x.x	是	-

NGIPSv (虚拟受管设备)

Firepower 版本	7000 和 8000 系列, 包括 AMP	系列2
5.4.0.x	是	是
5.3.0.x	是 3D7050、AMP 8150、AMP 8350 除外	是

NGIPSv (虚拟受管设备)

Firepower 版本	VMware vCloud Director	VMware vSphere/VMware ESXi				
	5.1	5.0	5.1	5.5	6.0	6.5
6.2.3	-	-	-	是	是	是
6.2.2.x	-	-	-	是	是	-
6.2.1	-	-	-	-	-	-
6.2.0.x	-	-	-	是	是	-
6.1.x.x	-	-	-	是	是	-
6.0.1.x	-	-	是	是	-	-
6.0.0.x	-	-	是	是	-	-
5.4.1.x	是	是	是	是	-	-
5.4.0.x	是	是	是	是	-	-
5.3.0.x	是	是	是	-	-	-



第 9 章

升级途径

以下主题提供 Firepower 设备支持的高级升级路径和升级路径示例。有关一般升级路径准则，请参阅计划升级路径，第 6 页。

- Firepower 管理中心升级路径，第 99 页
- Firepower 威胁防御 升级路径 - 使用 Firepower 管理中心，第 101 页
- Firepower 7000/8000 系列和 NGIPSv 升级路径 - 使用 Firepower 管理中心，第 105 页
- ASA FirePOWER 模块升级路径 - 使用 Firepower 管理中心，第 107 页
- Firepower 6.0 版预安装软件包，第 111 页

Firepower 管理中心升级路径

下表提供了 Firepower 管理中心的升级路径，包括 Firepower 管理中心虚拟。您必须升级到当前版本与目标版本之间的所有中间版本。

当前版本	升级路径		
6.2.2	→ 6.2.3		
6.2.1	→ 6.2.2 或 6.2.3		
6.2.0	→ 6.2.1 或 6.2.2 或 6.2.3		
6.1.0	→ 6.2.0 或 6.2.3		
6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3	
6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3
5.4.1.1	→ 6.0.0	→ 6.0.1	→ 6.1.0

示例：升级高可用性 Firepower 管理中心

一次手动升级一个高可用性 Firepower 管理中心。（升级过程对高可用性设备自动执行此操作。）在暂停同步的情况下，首先升级备用 Firepower 管理中心，然后升级主用设备。

虽然 Firepower 5.4.x 支持 Firepower 管理中心高可用性，但版本 6.0 会停止提供支持。要将您的部署从版本 5.4.x 升级至版本 6.0，必须拆分高可用性，而不仅仅是将其暂停。Firepower 管理中心高可用性支持将在版本 6.1 中恢复。重新配置高可用性后，不需要将其拆分即可进行后续升级。

本示例包括 Firepower 7000 和 8000 系列设备，它们是运行 NGIPS 软件的传统设备。您可以将它们配置为独立设备、高可用性对和堆栈。

部署

设备	当前	目标
Firepower 7000 和 8000 系列设备： <ul style="list-style-type: none"> • 独立设备 • 高可用性对 • 堆叠 	Firepower 5.4.0.x（各种版本）	Firepower 6.2.3
Firepower 管理中心高可用性对： <ul style="list-style-type: none"> • A（主用设备） • B（备用设备） 	Firepower 5.4.1.x	Firepower 6.2.3

升级路径

步骤	操作	设备	详细信息
1	安装 6.0 版预安装软件包	Firepower 设备	5.4.0.2 到 5.4.0.6 为必需项；对于更高版本为推荐项。
2	拆分高可用性，保持所有设备均注册到 A（主用）	Firepower 管理中心对	在 6.0 版本中停止支持高可用性。
3	安装 6.0 版预安装软件包	Firepower 管理中心 B	5.4.1.1 到 5.4.1.5 为必需项；对于更高版本为推荐项。
4	安装 6.0 版预安装软件包	Firepower 管理中心 A	5.4.1.1 到 5.4.1.5 为必需项；对于更高版本为推荐项。
5	升级	Firepower 管理中心 B	Firepower 5.4.1.x → 6.0
6	升级	Firepower 管理中心 A	Firepower 5.4.1.x → 6.0

步骤	操作	设备	详细信息
7	升级	Firepower 设备 使用相同的软件包一同升级。	Firepower 5.4.0.x → 6.0
8	升级	Firepower 管理中心 B	Firepower 6.0 → 6.1
9	升级	Firepower 管理中心 A	Firepower 6.0 → 6.1
10	重新配置高可用性，再次将 A 作为主用设备，将 B 作为备用设备	Firepower 管理中心对	在 6.1 版本中恢复支持高可用性。
11	升级	Firepower 设备 使用相同的软件包一同升级。	Firepower 6.0 → 6.1
12	暂停同步	Firepower 管理中心 A	进入集群脑裂。
13	升级	Firepower 管理中心 B	Firepower 6.1 → 6.2.3
14	升级	Firepower 管理中心 A	Firepower 6.1 → 6.2.3
15	重启同步	Firepower 管理中心 A	退出集群脑裂。
16	升级	Firepower 设备	Firepower 6.1 → 6.2.3

Firepower 威胁防御 升级路径 - 使用 Firepower 管理中心

下表提供了由 Firepower 管理中心管理的 Firepower 威胁防御设备的升级路径。您必须升级到当前版本与目标版本之间的所有中间版本。

当前版本	升级路径	
6.2.2	→ 6.2.3	
6.2.1（仅适用于 Firepower 2100 系列）	→ 6.2.2 或 6.2.3	
6.2.0	→ 6.2.2 或 6.2.3	
6.1.0	→ 6.2.0 或 6.2.3	
6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3

FXOS 升级序列（Firepower 4100/9300 机箱）

Firepower 4100/9300 机箱使用您从 Firepower 软件单独升级的 FXOS 操作系统。单独在每个机箱上升级 FXOS。

Firepower 威胁防御部署	升级序列
独立式 机箱内集群（仅限 Firepower 9300）	<ol style="list-style-type: none"> 1. 升级 FXOS。 2. 升级 Firepower 软件。
高可用性对	始终升级备用设备： <ol style="list-style-type: none"> 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. 在对上升级 Firepower 软件。
机箱间集群（6.2 及更高版本）	始终升级全从属机箱。例如，对于双机箱集群： <ol style="list-style-type: none"> 1. 在全从属机箱上升级 FXOS。 2. 将主模块切换到您刚刚升级的机箱。 3. 在新的全从属机箱上升级 FXOS。 4. 在集群上升级 Firepower 软件。

示例：通过捆绑的操作系统升级 Firepower 威胁防御设备

Firepower 6.0.1 引入了 Firepower 威胁防御。在某些平台上，升级 Firepower 软件会自动升级操作系统。您不需要单独执行这些任务。

部署

设备	当前	目标
具有 Firepower 威胁防御的 ASA 5500-X 系列	Firepower 6.0.1	Firepower 6.2.3
Firepower 2100 系列	Firepower 6.2.1（新加入，非托管）	Firepower 6.2.3
具有 ISA 3000 的 Firepower 威胁防御	Firepower 6.2.3（新加入，非托管）	Firepower 6.2.3
Firepower 管理中心	Firepower 6.0.1	Firepower 6.2.3

升级路径

步骤	操作	设备	详细信息
1	升级	Firepower 管理中心	Firepower 6.0.1 → 6.1
2	升级	ASA 5500-X 系列	Firepower 6.0.1 → 6.1
3	升级	Firepower 管理中心	Firepower 6.1 → 6.2.3
4	升级	ASA 5500-X 系列	Firepower 6.1 → 6.2.3
5	添加到部署	Firepower 2100 系列	添加设备的第一次机会。
6	升级	Firepower 2100 系列	Firepower 6.2.1 → 6.2.3
7	添加到部署	ISA 3000	添加设备的第一次机会。

示例：升级 Firepower 4100/9300 机箱（包括机箱内集群）

Firepower 6.0.1 在 Firepower 威胁防御上引入了 Firepower 4100/9300 机箱。单独在每个机箱上升级 FXOS。

部署

设备	当前	目标
带有三个安全模块的 Firepower 9300 机箱内集群	Firepower 6.0.1 FXOS 1.1.4	Firepower 6.2.3 FXOS 2.3.1
Firepower 4100 系列	Firepower 6.0.1 FXOS 1.1.4	Firepower 6.2.3 FXOS 2.3.1
Firepower 管理中心	Firepower 6.0.1	Firepower 6.2.3

升级路径

步骤	操作	设备	详细信息
1	升级	Firepower 管理中心	Firepower 6.0.1 → 6.1
2	升级 FXOS	Firepower 9300	FXOS 1.1.4 → 2.0.1
3	升级 FXOS	Firepower 4100 系列	FXOS 1.1.4 → 2.0.1
4	升级 Firepower 软件	Firepower 9300 和 4100 系列 使用相同的软件包一同升级。	Firepower 6.0.1 → 6.1
5	升级	Firepower 管理中心	Firepower 6.1 → 6.2.3

步骤	操作	设备	详细信息
6	升级 FXOS	Firepower 9300	FXOS 2.0.1 → 2.3.1
7	升级 FXOS	Firepower 4100 系列	FXOS 2.0.1 → 2.3.1
8	升级 Firepower 软件	Firepower 9300 和 4100 系列 使用相同的软件包一同升级。	Firepower 6.1 → 6.2.3

示例：升级 Firepower 4100/9300 机箱高可用性对

Firepower 6.0.1 在 Firepower 4100/9300 机箱上引入了 Firepower 威胁防御。在每个机箱上单独升级 FXOS，且始终升级备用机箱。

部署

设备	当前	目标
Firepower 4100 系列高可用性对： • A（主用设备） • B（备用设备）	Firepower 6.0.1 FXOS 1.1.4	Firepower 6.2.3 FXOS 2.3.1
Firepower 管理中心	Firepower 6.0.1	Firepower 6.2.3

升级路径

步骤	操作	设备	详细信息
1	升级	Firepower 管理中心	Firepower 6.0.1 → 6.1
2	升级 FXOS	设备 B（备用设备）	FXOS 1.1.4 → 2.0.1
3	切换角色	Firepower 4100 系列高可用性对	始终升级备用设备。
4	升级 FXOS	设备 A（新备用设备）	FXOS 1.1.4 → 2.0.1
5	升级 Firepower 软件	Firepower 4100 系列高可用性对	Firepower 6.0.1 → 6.1
6	升级	Firepower 管理中心	Firepower 6.1 → 6.2.3
7	升级 FXOS	设备 A（备用设备）	FXOS 2.0.1 → 2.3.1
8	切换角色	Firepower 4100 系列可用性对	始终升级备用设备。
9	升级 FXOS	设备 B（新备用设备）	FXOS 2.0.1 → 2.3.1

步骤	操作	设备	详细信息
10	升级 Firepower 软件	Firepower 4100 系列高可用性对	Firepower 6.1 → 6.2.3

示例：升级 Firepower 威胁防御 4100/9300 机箱间集群

Firepower 6.2 在 Firepower 4100/9300 机箱上引入了 Firepower 威胁防御机箱间集群。在每个机箱上单独升级 FXOS，且始终升级全从属机箱。

部署

设备	当前	目标
带两个机箱的 Firepower 9300 机箱间集群： <ul style="list-style-type: none"> • A（三个模块，包括主模块） • B（三个模块，全部为从属模块） 	Firepower 6.2 FXOS 2.1.1	Firepower 6.2.3 FXOS 2.3.1
Firepower 管理中心	Firepower 6.2	Firepower 6.2.3

升级路径

步骤	操作	设备	详细信息
1	升级	Firepower 管理中心	Firepower 6.2 → 6.2.3
2	升级 FXOS	机箱 B（全部为从属设备）	FXOS 2.1.1 → 2.3.1
3	将主模块切换到机箱 B	Firepower 9300 机箱间集群	始终升级全从属机箱。
4	升级 FXOS	机箱 A（全部为从属设备，因为主模块已移至机箱 B）	FXOS 2.1.1 → 2.3.1
5	升级 Firepower 软件	Firepower 9300 机箱间集群	Firepower 6.2 → 6.2.3

Firepower 7000/8000 系列和 NGIPSv 升级路径 - 使用 Firepower 管理中心

此表提供了由 Firepower 管理中心管理的 7000 系列、8000 系列和 NGIPSv 设备的升级路径。您必须升级到当前版本与目标版本之间的所有中间版本。

当前版本	升级路径		
6.2.2	→ 6.2.3		
6.2.1	在以下平台中不受支持		
6.2.0	→ 6.2.2 或 6.2.3		
6.1.0	→ 6.2.0 或 6.2.3		
6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3	
6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3
5.4.1.1	→ 6.0.0	→ 6.0.1	→ 6.1.0
5.4.0.2	→ 6.0.0	→ 6.0.1	→ 6.1.0

示例：升级虚拟部署

在虚拟部署中，请确保托管环境与虚拟设备的目标版本兼容。

部署

设备	当前	目标
NGIPSv	5.4.x（各种版本） VMware ESXi 5.0	Firepower 6.2.3 VMware ESXi 6.5
Firepower 管理中心虚拟	Firepower 6.0 VMware ESXi 5.5	Firepower 6.2.3 VMware ESXi 6.5

升级路径

步骤	操作	设备	详细信息
1	安装 6.0 版预安装软件包	NGIPSv (5.4.0.x)	5.4.0.2 到 5.4.0.6 为必需项；对于更高版本为推荐项。
2	安装 6.0 版预安装软件包	NGIPSv (5.4.1.x)	5.4.1.1 到 5.4.1.5 为必需项；对于更高版本为推荐项。
3	升级 VMware ESXi	NGIPSv	ESXi 5.0 → 5.5
4	升级 Firepower 软件	NGIPSv	Firepower 5.4.x → 6.0
5	升级 Firepower 软件	Firepower 管理中心虚拟	Firepower 6.0 → 6.1

步骤	操作	设备	详细信息
6	升级 Firepower 软件	NGIPSv	Firepower 6.0 → 6.1
7	升级 Firepower 软件	Firepower 管理中心虚拟	Firepower 6.1 → 6.2.3
8	升级 VMware ESXi	Firepower 管理中心虚拟	ESXi 5.5 → 6.5
9	升级 Firepower 软件	NGIPSv	Firepower 6.1 → 6.2.3
10	升级 VMware ESXi	NGIPSv	ESXi 5.5 → 6.5

ASA FirePOWER 模块升级路径 - 使用 Firepower 管理中心

下表提供了由 Firepower 管理中心管理的 ASA FirePOWER 模块的升级路径。您必须升级到当前版本与目标版本之间的所有中间版本。

当前版本	升级路径			
6.2.2	→ 6.2.3			
6.2.1	在此平台上不受支持			
6.2.0	→ 6.2.2 或 6.2.3			
6.1.0	→ 6.2.0 或 6.2.3			
6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3		
6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3	
5.4.1	→ 6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3
5.4.0.2	→ 6.0.0	→ 6.0.1	→ 6.1.0	→ 6.2.0 或 6.2.3

ASA 的升级序列

具备 FirePOWER 服务的 ASA 设备使用您从 Firepower 软件单独升级的 ASA 操作系统。ASA 与 ASA FirePOWER 版本之间没有广泛的兼容性。但是，即使并非严格要求进行 ASA 升级，但是解决问题可能需要升级到支持的最新版本。

您单独在每个机箱上升级 ASA。如果要在集群或故障切换 ASA 设备上升级 ASA 和 ASA FirePOWER 模块，请在升级 ASA 时一次升级一个 ASA FirePOWER 模块，如下表所示。

ASA 部署	升级序列
独立式	<ol style="list-style-type: none"> 1. 升级 ASA。 2. 升级 ASA FirePOWER 模块。

ASA 部署	升级序列
故障切换：主用/备用	<ol style="list-style-type: none"> 1. 在备用设备上升级 ASA。 2. 升级备用设备上的 ASA FirePOWER 模块。 3. 故障切换。 4. 在新的备用设备上升级 ASA。 5. 升级新备用设备上的 ASA FirePOWER 模块。
故障切换：主用/主用	<ol style="list-style-type: none"> 1. 使两个故障切换组在主设备上均处于活动状态。 2. 在辅助设备上升级 ASA。 3. 升级辅助设备上的 ASA FirePOWER 模块。 4. 使两个故障切换组在辅助设备上均处于活动状态 5. 升级主设备上的 ASA。 6. 升级主设备上的 ASA FirePOWER 模块。
集群	<p>对于每个设备：</p> <ol style="list-style-type: none"> 1. 从集群中删除设备。 首先升级从属设备。当您最后删除主设备时，请等待其他设备接管为主设备，然后再升级 ASA。 2. 升级已删除设备上的 ASA。 3. 升级已删除设备上的 ASA FirePOWER 模块。 4. 将设备恢复到集群（作为从属设备）。

示例：升级具备 FirePOWER 服务的 ASA

单独在每个机箱上升级 ASA。如果要在集群或故障切换 ASA 设备上升级 ASA 和 ASA FirePOWER 模块，请在升级 ASA 时一次升级一个 ASA FirePOWER 模块。

部署

设备	当前	目标
运行于各 ASA 5500-X 系列型号之上的具备 FirePOWER 服务的 ASA： <ul style="list-style-type: none"> • A 和 B（独立） • C 和 D（主用/备用故障切换对） • E 和 F（主用/主用故障切换对） • G、H、I（主/从属/从属集群） 	Firepower 5.4.x（各种版本） ASA 9.3(2)	Firepower 6.2.3 ASA 9.9(2)
Firepower 管理中心	Firepower 6.0	Firepower 6.2.3

升级路径

步骤	操作	设备	详细信息
1	安装 6.0 版预安装软件包	ASA FirePOWER 模块 (5.4.0.x)	对于 Firepower 5.4.0.2 至 5.4.0.6 为必需项；对于更高版本为推荐项。
2	安装 6.0 版预安装软件包	ASA FirePOWER 模块 (5.4.1.x)	Firepower 5.4.1.1 到 5.4.1.5 为必需项；对于更高版本为推荐项。
在独立设备上升级 ASA 和 ASA FirePOWER 模块：A 和 B			
3a	升级 ASA	设备 A（独立）	ASA 9.3(2) → 9.9(2)
3b	升级 ASA	设备 B（独立）	ASA 9.3(2) → 9.9(2)
3c	升级 ASA FirePOWER 模块	设备 A 和设备 B 使用相同的软件包一同升级。	Firepower 5.4.x → 6.0
在主用/备用故障切换对上升级 ASA 和 ASA FirePOWER 模块：C 和 D			
4a	升级 ASA	设备 D（主用/备用对中的备用设备）	ASA 9.3(2) → 9.9(2)
4b	升级 ASA FirePOWER 模块	设备 D	Firepower 5.4.x → 6.0
4c	故障切换	设备 C 和设备 D 对	始终升级备用设备。

步骤	操作	设备	详细信息
4d	升级 ASA	设备 C（新备用设备）	ASA 9.3(2) → 9.9(2)
4e	升级 ASA FirePOWER 模块	设备 C	Firepower 5.4.x → 6.0
在主用/主用故障切换对上升级 ASA 和 ASA FirePOWER 模块：E 和 F			
5a	使两个故障切换组在主设备上均处于活动状态	设备 E（主用/主用对中的主设备）	
5b	升级 ASA	设备 F（主用/主用对中的辅助设备）	ASA 9.3(2) → 9.9(2)
5c	升级 ASA FirePOWER 模块	设备 F	ASA 9.3(2) → 9.9(2)
5	使两个故障切换组在辅助设备上天均处于活动状态	设备 F	
5e	升级 ASA	设备 E	ASA 9.3(2) → 9.9(2)
5f	升级 ASA FirePOWER 模块	设备 E	Firepower 5.4.x → 6.0
升级 ASA 集群中的 ASA 和 ASA FirePOWER 模块：H、G 和 I			
6a	从集群中删除	设备 H（从属设备）	避免流量中断。
6b	升级 ASA	设备 H	ASA 9.3(2) → 9.9(2)
6c	升级 ASA FirePOWER 模块	设备 H	Firepower 5.4.x → 6.0
6d	返回集群	设备 H	继续处理流量。
6e	从集群中删除	设备 G（从属设备）	避免流量中断。
6f	升级 ASA	设备 G	ASA 9.3(2) → 9.9(2)
6g	升级 ASA FirePOWER 模块	设备 G	Firepower 5.4.x → 6.0
6	返回集群	设备 G	继续处理流量。
6i	从集群中删除	设备 G（主设备）	避免流量中断。
6j	升级 ASA	设备 G	ASA 9.3(2) → 9.9(2)
6k	升级 ASA FirePOWER 模块	设备 G	Firepower 5.4.x → 6.0
6l	返回集群	设备 G	继续处理流量。设备 G 作为从属设备返回。

步骤	操作	设备	详细信息
在不升级 ASA 的情况下升级 ASA FirePOWER 模块。			
7	升级	Firepower 管理中心	Firepower 6.0 → 6.0.1
8	升级 ASA FirePOWER 模块	ASA FirePOWER 模块s 使用相同的软件包一同升级。	Firepower 6.0 → 6.0.1
9	升级	Firepower 管理中心	Firepower 6.0.1 → 6.1
10	升级 ASA FirePOWER 模块	ASA FirePOWER 模块s 使用相同的软件包一同升级。	Firepower 6.0.1 → 6.1
11	升级	Firepower 管理中心	Firepower 6.1 → 6.2.3
12	升级 ASA FirePOWER 模块	ASA FirePOWER 模块s 使用相同的软件包一同升级。	Firepower 6.1 → 6.2.3

Firepower 6.0 版预安装软件包

对于从 5.4.x 版本到 6.x 版本的升级，思科提供可优化该升级的预安装软件包。

在某些情况下，您必须使用以下表中列出的预安装软件包。即使不要求这样做时，我们也强烈建议在升级路径中包含并使用 6.0 版本预安装软件包。

设备	要升级的最低版本	所需的预安装软件包	建议的预安装软件包
FireSIGHT Defense Center (Firepower 管理中心)	5.4.1.1	5.4.1.1 至 5.4.1.5	5.4.1.6 及更高版本
7000/8000 系列设备	5.4.0.2	5.4.0.2 至 5.4.0.6	
NGIPSv	5.4.0.2 5.4.1.1	5.4.0.2 至 5.4.0.6 5.4.1.1 至 5.4.1.5	5.4.1.6 及更高版本 5.4.0.7 及更高版本
ASA FirePOWER 模块 (5.4.1.x 序列中的型号)	5.4.1	5.4.1 5.4.1.1 至 5.4.1.5	5.4.1.6 及更高版本
ASA FirePOWER 模块 (5.4.0.x 序列中的型号)	5.4.0.2	5.4.0.2 至 5.4.0.6	5.4.0.7 及更高版本



第 10 章

升级期间的流量、检查和设备行为

- [Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱，第 113 页](#)
- [Firepower 威胁防御升级行为，第 115 页](#)
- [Firepower 7000/8000 系列升级行为，第 117 页](#)
- [ASA FirePOWER 升级行为，第 118 页](#)
- [NGIPSv 升级行为，第 119 页](#)

Firepower 威胁防御升级行为 - Firepower 4100/9300 机箱

本部分介绍在升级 Firepower 4100/9300 机箱时的设备和流量行为。

机箱：FXOS 升级

在每个机箱上独立升级 FXOS，即使配置了机箱间集群或高可用性对也是如此。您执行升级的方式会确定设备在 FXOS 升级期间处理流量的方式。

部署	方法	流量行为
独立式	—	被丢弃
高可用性	最佳实践： 在备用设备上更新 FXOS，切换主用对等设备，升级新的备用设备。	不受影响
	在备用设备完成升级之前，在主用对等设备上升级 FXOS。	被丢弃，直到一个对等设备处于在线状态
机箱间集群（6.2 及更高版本）	最佳实践： 一次升级一个机箱，以便至少有一个模块始终处于在线状态。	不受影响
	同时升级机箱，因此在某个时间所有模块都处于关闭状态。	被丢弃，直到至少一个模块处于在线状态

部署	方法	流量行为
机箱内集群（仅限 Firepower 9300）	已启用故障时自动绕过： 绕过：备用或强制绕过。 （6.1 及更高版本）	不检查直接通过
	已禁用故障时自动绕过： 绕过：已禁用。 （6.1 及更高版本）	被丢弃，直到至少一个模块处于在线状态
	没有故障时自动旁路模块。	被丢弃，直到至少一个模块处于在线状态

独立机箱：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 （切换接口也称为桥接组或透明接口）	被丢弃
仅限 IPS 接口	内联集，已启用故障时自动旁路： 绕过：备用或强制绕过。 （6.1 及更高版本）	可以为以下任意一项： <ul style="list-style-type: none"> 不检查直接通过（6.2.3 及更高版本） 被丢弃（6.1 至 6.2.2.x）
	内联集，已禁用故障时自动旁路： 绕过：已禁用。 （6.1 及更高版本）	被丢弃
	内联集，没有故障时自动旁路模块	被丢弃
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

高可用性对：Firepower 软件升级

在高可用性对中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，应一次升级一个设备。升级过程中，设备在维护模式下运行。

首先升级备用设备。设备切换角色，然后升级新的备用设备。升级完成后，设备的角色保持切换状态。如果不想改变主用/备用角色，请先手动切换角色，然后再进行升级。这样，升级过程会将它们切换回来。

集群：Firepower 软件升级

在 Firepower 威胁防御集群中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，应一次升级一个设备。升级过程中，设备在维护模式下运行。

首先升级一个或多个从属安全模块，然后升级主模块。升级时，安全模块在维护模式下运行。

在主安全模块升级期间，尽管流量检查和处理通常会继续，但系统会停止记录事件。升级完成后，在日志记录关闭期间处理的流量事件显示有不同步的时间戳。但是，如果日志记录关闭较长时间，则系统可能会删除最早事件，然后再记录事件。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 进程通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅 [Firepower 管理中心配置指南](#) 中的在部署或激活时重启 Snort 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检查而被丢弃。此外，重启 Snort 进程会中断 Firepower 威胁防御独立设备、高可用性对和集群上的流量检查。在中断期间，您的接口配置会确定是丢弃流量还是在检查的情况下允许流量通过。

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 (切换接口也称为桥接组或透明接口)	被丢弃
仅限 IPS 接口	内联集，已启用或禁用故障保护 (6.0.1-6.1.0.x)	不检查直接通过 如果已禁用故障保护，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
	内联集，Snort 故障时自动打开：关闭：已禁用（6.2 及更高版本）	被丢弃
	内联集，Snort 故障时自动打开：关闭：已启用（6.2 及更高版本）	不检查直接通过
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

Firepower 威胁防御升级行为

本部分介绍在升级 Firepower 2100 系列、ASA 5500-X 系列、ISA 3000 和 Firepower 威胁防御虚拟设备时的设备和流量行为。

独立设备：Firepower 软件升级

接口配置会确定在升级期间独立设备如何处理流量。

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 (切换接口也称为桥接组或透明接口)	被丢弃
仅限 IPS 接口	内联集	被丢弃
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

高可用性对：Firepower 软件升级

在高可用性对中的设备上升级 Firepower 软件时，流量或检查中不应出现中断。为确保操作的连续性，应一次升级一个设备。升级过程中，设备在维护模式下运行。

首先升级备用设备。设备切换角色，然后升级新的备用设备。升级完成后，设备的角色保持切换状态。如果不想改变主用/备用角色，请先手动切换角色，然后再进行升级。这样，升级过程会将它们切换回来。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 进程通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅 Firepower 管理中心配置指南中的在部署或激活时重启 Snort 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检查而被丢弃。此外，重启 Snort 进程会中断 Firepower 威胁防御独立设备和高可用性对上的流量检查。在中断期间，您的接口配置会确定是丢弃流量还是在检查的情况下允许流量通过。

接口配置		流量行为
防火墙接口	路由或交换，包括 EtherChannel、冗余、子接口 (切换接口也称为桥接组或透明接口)	被丢弃

接口配置		流量行为
仅限 IPS 接口	内联集，已启用或禁用故障保护 (6.0.1-6.1.0.x)	不检查直接通过 如果已禁用故障保护，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
	内联集，Snort 故障时自动打 开：关闭：已禁用（6.2 及更高版本）	被丢弃
	内联集，Snort 故障时自动打 开：关闭：已启用（6.2 及更高版本）	不检查直接通过
	内联集，分流模式	立即传出数据包，不检查副本
	被动，ERSPAN 被动	不中断，不检查

Firepower 7000/8000 系列升级行为

以下各部分介绍升级 Firepower 7000 和 8000 系列设备时的设备和流量行为。

独立设备：Firepower 软件升级

接口配置决定了独立设备在升级期间对流量的处理方式。

接口配置	流量行为
内联，已启用硬件绕过（绕过模式：绕过）	不检查直接通过，但是流量会在以下两个时间点短暂中断： <ul style="list-style-type: none"> 升级过程开始时，链路关闭并重新开启（振荡），网卡切换到硬件绕过模式。 升级完成后，链路再次出现振荡，网卡退出硬件绕过模式。终端重新连接并与设备接口重新建立链路后，检查会恢复。
内联，没有硬件绕过模块，或已禁用硬件绕过模式（绕过模式：非绕过）	被丢弃
内联，分流模式	立即传出数据包，不检查副本
被动	不中断，不检查
路由，交换	被丢弃

高可用性对：Firepower 软件升级

升级高可用性对中的设备（或设备堆叠）时，您应该不会感受到流量中断或检查中断。为确保操作的连续性，应一次升级一个设备。升级过程中，设备在维护模式下运行。

先升级哪个对等设备取决于您的部署：

- 路由或交换 - 优先升级备用设备。设备切换角色，然后升级新的备用设备。升级完成后，设备的角色保持切换状态。如果不想改变主用/备用角色，请先手动切换角色，然后再进行升级。这样，升级过程会将它们切换回来。
- 纯访问控制 - 优先升级主用设备。升级完成后，主用设备和备用设备保持其原有角色。

8000 系列堆栈：Firepower 软件升级

在 8000 系列堆栈中，设备同时进行升级。在主设备完成其升级并且堆栈恢复操作之前，流量都会受到影响，就像堆栈是一个独立设备一样。在所有设备完成升级之前，堆栈会在一个受限的混合版本状态下运行。

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 进程通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅 [Firepower 管理中心配置指南](#) 中的在部署或激活时重启 Snort 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检查而被丢弃。此外，重启 Snort 进程会中断 Firepower 独立设备、高可用性对和 8000 系列堆栈上的流量检查。在中断期间，您的接口配置会确定是丢弃流量还是在检查的情况下允许流量通过。

接口配置	重启流量行为
内联，故障保护已启用或已禁用	不检查直接通过 如果已禁用故障保护，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
内联，分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查
路由，交换	被丢弃

ASA FirePOWER升级行为

在 Firepower 软件升级期间（包括在您部署会导致 Snort 进程重启的某些配置时），模块处理流量的方式由用于将流量重定向到 ASA FirePOWER 模块的 ASA 服务策略决定。

流量重定向策略	流量行为
故障时自动打开 (sfr fail-open)	不检查直接通过

流量重定向策略	流量行为
故障时自动关闭 (sfr fail-close)	被丢弃
仅监控 (sfr {fail-close}{fail-open} monitor-only)	立即传出数据包，不检查副本

部署过程中的流量行为

Snort 进程重启时的流量行为与升级 ASA FirePOWER 模块时相同。升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 进程通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。

在部署时，资源需求可能会导致少量数据包未经检查而被丢弃。此外，重启 Snort 进程会中断流量检查。在中断期间，您的服务策略会确定是丢弃流量还是在检查的情况下允许流量通过。

NGIPSv升级行为

您的接口配置决定了 NGIPSv 在 Firepower 软件升级期间处理流量的方式。

接口配置	流量行为
内联	被丢弃
内联，分流模式	立即传出数据包，不检查副本
被动	不中断，不检查

部署过程中的流量行为

升级过程中，您需要多次部署配置。如果在升级后立即进行首次部署，Snort 进程通常会重启。该进程在其他部署期间不重启，除非您在部署之前修改特定策略或设备配置。有关详细信息，请参阅 [Firepower 管理中心配置指南](#) 中的在部署或激活时重启 Snort 进程的配置。

在部署时，资源需求可能会导致少量数据包未经检查而被丢弃。此外，重启 Snort 进程会中断流量检查。在中断期间，您的接口配置会确定是丢弃流量还是在检查的情况下允许流量通过。

接口配置	重启流量行为
内联，故障保护已启用或已禁用	不检查直接通过 如果已禁用故障保护，并且 Snort 处于繁忙而非关闭状态，则系统可能会丢弃一些数据包。
内联，分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查



第 11 章

Firepower 软件升级的版本特定准则

以下主题提供 Firepower 软件升级的重要且版本特定的信息。例如，您可能需要在任何升级之前或之后进行配置更改，或将许可重新应用到某些设备。

- [影响多个版本的准则](#)，第 121 页
- [6.2.3 版准则](#)，第 121 页
- [6.2.2 版准则](#)，第 122 页
- [6.2.0 版准则](#)，第 122 页
- [6.1.0 版准则](#)，第 124 页
- [6.0.0 版准则](#)，第 125 页

影响多个版本的准则

Firepower 威胁防御集群 (6.1.x): 在升级之前删除站点 ID

有效时间：从 Firepower 6.1.x 升级到 Firepower 6.2.3 及更高版本

6.2.3 版准则

在升级期间及升级之后与思科共享数据

版本 6.2.3 中的新功能包括与思科共享数据。

思科网络参与和思科成功网络会将使用情况信息和统计信息发送到思科，这些信息对于为您提供技术支持至关重要。在升级过程中，您可以接受或拒绝参与这些计划。您还可以随时选择加入或退出。

Web 分析跟踪会将非个人可识别使用情况数据发送到思科，包括但不限于查看的页面、在页面上停留的时间、浏览器版本、产品版本、用户位置以及您的 Firepower 管理中心的管理 IP 地址或主机名。



注释 在升级过程中，您不能选择退出 Web 分析。您可以在升级后禁用 Web 分析，或不安装升级。

在升级后编辑/重新保存访问控制策略

如果您配置仅在入侵策略变量集中使用的网络或端口对象，则在升级后部署关联的访问控制策略会失败。如果发生这种情况，请编辑访问控制策略，进行更改（例如编辑说明）、保存并重新部署。

报告中对结果限制的更改

版本 6.2.3 限制您可以在报告部分中使用或包括的结果数，如下所示。对于表格和详细信息视图，您可以在 PDF 报告中包括比 HTML/CSV 报告少的记录。

报告部分类型	最大记录数：HTML/CSV 报告部分	最大记录数：PDF 报告部分
条形图 饼图	100（顶部或底部）	100（顶部或底部）
表格视图	400,000	100,000
详细信息视图	1,000	500

如果在升级 Firepower 管理中心之前，报告模板中的某个部分指定了大于 HTML/CSV 最大值的结果数，则升级过程会将该设置降至新的最大值。

对于生成 PDF 报告的报告模板，如果在任何模板部分中超过 PDF 限制，升级过程会将输出格式更改为 HTML。要继续生成 PDF，请将结果限制降低到 PDF 最大值。如果您在升级后执行此操作，则将输出格式设置回 PDF。

6.2.2 版准则

在 8000 系列设备上禁用通用标准 (CC) 模式或 UCAPL 模式

思科建议不要在运行 6.2.2 版本的 8000 系列设备上启用通用标准 (CC) 或 UCAPL 模式。如果您在传感器上启用 CC 模式或 UCAPL 模式，则 8000 系列设备的文件系统完整性检查 (FSIC) 可能会失败，并且设备可能会变得不响应。如果在启用 CC 或 UCAPL 模式后设备变得不响应，则必须为设备设置基准以使设备正常工作。如果您需要启用 CC 模式或 UCAPL，请将 8000 系列设备更新为 6.2.2.1 版本，然后启用 CC 模式或 UCAPL 模式。

6.2.0 版准则

对关联策略的更新前修改

如果您要更新配置了关联策略的 Firepower 管理中心，请执行下面列出的规则修改。如果您重新映像 Firepower 管理中心而不对其更新，或者如果您没有配置关联策略，则不需要执行下面列出的规则修改。

版本 6.2.0 不再支持嵌套的关联规则。在以前的版本中，如果多个规则的基础事件类型相同，可以使用一个关联规则作为另一个关联规则的触发器。例如，如果您创建规则 A 和规则 B，这两个规则都

会触发入侵事件，则可以使用条件“规则 A 为真”作为规则 B 的限制。在此配置中，规则 A 被视为“嵌套”在规则 B 内。

更新过程通过将嵌套关联规则（规则 A）中的设置复制到嵌套关联规则（规则 B）并删除被嵌套规则，将某些被嵌套关联规则展平。更新过程会将嵌套规则中的主机配置文件/用户限定条件和暂停/非活动时段复制到嵌套规则。

对于除非活动时段外的所有这些设置，仅当嵌套规则中缺少相应设置时，系统才可将被嵌套规则中的设置复制到嵌套规则。系统将被嵌套规则中的非活动时段复制到嵌套规则时，它将保留嵌套规则中的非活动时段，以便生成的规则使用最初参与嵌套配置的两个规则中的设置。

如果被嵌套规则和嵌套规则具有特定类型的冲突，则更新无法展平被嵌套规则。在这些情况下，更新会失败。

为避免这种失败，请在运行更新之前按如下所示修改关联规则：

- 删除被嵌套规则或嵌套规则中的主机配置文件限定条件、用户限定条件和暂停时段设置，以便被嵌套配置中只有一个规则指定这些设置。
- 删除任何被嵌套规则中的连接跟踪器。
- 从不必为真的被嵌套规则中的主机配置文件限定文件、用户限定文件、暂停时段和非活动时段；也就是说，从被嵌套规则中删除使用 OR 运算符链接到嵌套规则中的其他规则条件的元素。

有关关联规则的信息，请参阅 [Firepower 管理中心配置指南](#)，6.2.0 版本。

更新期间对故障保护配置的自动修改

在 6.2.0 版本中，Snort 故障时自动打开的配置将取代由 Firepower 管理中心管理的 Firepower 威胁防御物理和虚拟设备上的故障保护选项。此新功能提供与故障保护选项相同的功能，但它还使您可以选择在 Snort 进程关闭时是否丢弃流量。

将 Firepower 管理中心更新为 6.2.0 版本时，故障保护在以下受管设备上仍受支持：

- 运行 6.1.x 版本的 Firepower 威胁防御设备
- 运行 6.2.0 版本的 7000 系列、8000 系列和 NGIPSv 设备

当您 Firepower 威胁防御设备更新为 6.2.0 版本时，更新过程会确定是否启用故障保护，如果启用，则将故障保护选项迁移至匹配的 Snort 故障时自动打开配置。我们强烈建议您先考虑是启用还是禁用故障保护，然后再更新 Firepower 威胁防御设备。

表 9: 将故障保护迁移至 Snort 故障时自动打开

如果 6.1 版本的故障保护为...	Snort 故障时自动打开设置为...	
	忙碌	关闭
已禁用（默认行为） 新的和现有的连接在 Snort 进程繁忙时丢弃，在 Snort 进程关闭时不检查直接通过。	禁用 新的和现有的连接在 Snort 进程繁忙时会丢弃。	启用 新的和现有的连接在 Snort 进程关闭时不检查直接通过。

如果 6.1 版本的故障保护为...	Snort 故障时自动打开设置为...	
	忙碌	关闭
启用 新的和现有的连接在 Snort 进程繁忙或关闭时不检查直接通过。	启用 新的和现有的连接在 Snort 进程繁忙时不检查直接通过。	启用 新的和现有的连接在 Snort 进程关闭时不检查直接通过。

有关详细信息，请参阅 6.2.0 版本的 [Firepower 管理中心配置指南](#) 中 [Firepower 系统上的内联集](#) 一章的故障保护部分。

6.1.0 版准则

在将 ASA FirePOWER 模块升级到 6.1 及更高版本之前禁用 ASA REST API

在将 ASA FirePOWER 模块升级到 6.1 及更高版本之前，请使用 ASA CLI 禁用 ASA REST API:

```
no rest-api agent
```

如果不禁用 REST API，升级将会失败。您可以在升级后重新启用它：

```
rest-api agent
```

请注意，如果您还在运行 6.0 及更高版本的 ASA FirePOWER 模块，则 ASA 5506-X 系列设备不支持 ASA REST API。

STIG 模式更改为 UCAPL 模式

在 6.1 版本中，称为安全技术实施指南 (STIG) 模式的安全认证合规性模式已重命名为统一功能获批产品列表 (UCAPL) 模式。

在 6.1 版本升级后，处于 STIG 模式下的 Firepower 设备将处于 UCAPL 模式。与 UCAPL 模式相关联所有系统功能限制和更改都将生效。

有关详细信息，包括有关加强系统 UCAPL 合规性的信息，请参阅 [Firepower 管理中心配置指南](#) 的安全认证合规性一章，以及由认证实体为此产品提供的准则。

在升级后恢复经典许可证

将 Firepower 管理中心升级到 6.1 版本可能会删除或禁用受管 NGIPSv、ASA FirePOWER、7000 系列和 8000 系列设备的经典许可证。

在开始更新之前，请联系 思科 TAC 以获取可以运行用来避免出现此问题的脚本。如果不运行升级前脚本，则在更新后：

- 检查并重新安装已删除的许可证 - 选择 **系统 > 许可证 > 经典许可证**。
- 编辑受影响的设备并重新启用许可证 - 选择 **设备 > 设备管理**。

6.0.0 版准则

术语和品牌

版本 6.0 包含重大术语和品牌更改，包括：

- FireSIGHT 系统 → Firepower
- FireSIGHT 防御中心 → Firepower 管理中心
- 系列 3 设备 → 7000 系列设备或 8000 系列设备
- 虚拟受管设备 → NGIPSv

有关详细信息，请参阅[思科 Firepower 术语指南](#)。

6.0 版预安装软件包

对于从 5.4.x 版本到 6.x 版本的升级，思科提供可优化该升级的预安装软件包。

在某些情况下，您必须使用以下表中列出的预安装软件包。即使不要求这样做时，我们也强烈建议在升级路径中包含并使用 6.0 版本预安装软件包。

设备	要升级的最低版本	所需的预安装软件包	建议的预安装软件包
FireSIGHT Defense Center (Firepower 管理中心)	5.4.1.1	5.4.1.1 至 5.4.1.5	5.4.1.6 及更高版本
7000/8000 系列设备	5.4.0.2	5.4.0.2 至 5.4.0.6	
NGIPSv	5.4.0.2 5.4.1.1	5.4.0.2 至 5.4.0.6 5.4.1.1 至 5.4.1.5	5.4.1.6 及更高版本 5.4.0.7 及更高版本
ASA FirePOWER 模块 (5.4.1.x 序列中的型号)	5.4.1	5.4.1 5.4.1.1 至 5.4.1.5	5.4.1.6 及更高版本
ASA FirePOWER 模块 (5.4.0.x 序列中的型号)	5.4.0.2	5.4.0.2 至 5.4.0.6	5.4.0.7 及更高版本

升级 DC750、DC1500、DC3500 和虚拟防御中心的内存

以下 FireSIGHT 防御中心型号可能需要额外内存来运行 6.0 版本：

- DC750
- DC1500

- DC3500
- 虚拟防御中心

由于思科产品要求增加内存，因此思科为有权在合格的 DC750 或 DC1500 上运行 6.0 版本的客户免费提供内存升级套件：

- 订购套件 - 请参阅[现场通告：FN - 64077 - 思科 FireSIGHT 和 Sourcefire 防御中心管理设备 - FirePOWER 软件 6.0 版及更高版本所需的内存升级](#)
- 升级内存 - 请参阅 *Firepower* 管理中心安装指南中的 [Firepower 管理中心内存升级说明](#)。

拆分防御中心高可用性对

6.0.x 版本不支持 Firepower 管理中心高可用性对。

您不能将防御中心的 5.4.x 版本高可用性对升级到 Firepower 管理中心的 6.0 版本高可用性对。您必须拆分高可用性对，并单独升级每个防御中心。您可以通过 6.1 版本重新建立高可用性对。

禁用“重试 URL 缓存未命中查找”选项

在管理运行 5.4.0.6 版本、5.4.1.5 版本或更早版本的设备时，将 Firepower 管理中心升级到 6.0 版本可能会导致流量中断和系统问题。

在升级防御中心之前，请禁用**重试 URL 缓存未命中查找**选项，该选项在部署到设备的访问控制策略中的“高级”选项卡上进行设置。然后，重新进行部署。在将受管设备升级到 5.4.0.7 及更高版本或 5.4.1.6 及更高版本（或 6.0 版本）后，可以重新启用该选项。

更新防御中心 HTTPS 证书

如果将使用以下 HTTPS 证书之一的 5.4.x 版本防御中心升级到 6.0 版本 Firepower 管理中心，您将无法登录，且必须联系思科 TAC：

- 使用 RSASSA-PSS 签名算法生成的证书。
在升级之前，请将通过 sha1WithRSAEncryption 或 sha256WithRSAEncryption 算法生成的证书替换为防御中心默认证书。重新启动。
- 使用大于 2048 位的公共服务器密钥生成的证书。
在升级之前，请替换为通过服务器证书请求 (CSR) 生成的证书。重新启动。

此外，请勿在升级后上传任一上述类型的证书。有关在 5.4.x 版本的设备上生成证书的信息，请参阅 5.4.1 版本 *FireSIGHT* 系统用户指南中的[使用自定义 HTTPS 证书](#)。

不支持 AMP 私有云

版本 6.0 不支持使用 AMP 私有云进行 AMP for Firepower 签名查找。在版本 6.0 中，系统会自动向 AMP 公共云提交 SHA-256 签名。如果您有 AMP 私有云且正在从终端接收事件，则无需对配置进行任何其他更改，版本 6.0 防御中心即可继续接收这些事件。



第 12 章

Firepower 软件升级的时间和磁盘空间

要升级 Firepower 设备，必须具有足够的可用磁盘空间，否则升级会失败。当使用 Firepower 管理中心升级受管设备时，Firepower 管理中心需要其 /Volume 分区中具有额外磁盘空间。

此外，您还必须具有足够的时间来执行升级。请注意，升级所需的时间可能超出估计的时间，具体取决于您的部署。例如，内存较低的设备 and 负载过多的设备可能需要更长的升级时间。这些估计时间还不包括完成就绪性检查所需的时间。

- [6.2.3 版本时间和磁盘空间，第 127 页](#)
- [6.2.2 版本时间和磁盘空间，第 128 页](#)
- [6.2.0 版本时间和磁盘空间，第 130 页](#)
- [6.1.0 版本时间和磁盘空间，第 134 页](#)
- [6.0.1 版本时间和磁盘空间，第 139 页](#)
- [6.0 版本时间和磁盘空间，第 142 页](#)

6.2.3 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	从 6.1.0 升级: 17 MB 从 6.2.0 升级: 24 MB 从 6.2.1 升级: 23 MB 从 6.2.2 升级: 24 MB	从 6.1.0 升级: 7415 MB 从 6.2.0 升级: 8863 MB 从 6.2.1 升级: 8263 MB 从 6.2.2 升级: 11860 MB	—	从 6.1.0 升级: 38 分钟 从 6.2.0 升级: 43 分钟 从 6.2.1 升级: 37 分钟 从 6.2.2 升级: 37 分钟
Firepower 管理中心虚拟	从 6.1.0 升级: 23 MB 从 6.2.0 升级: 28 MB 从 6.2.1 升级: 24 MB 从 6.2.2 升级: 24 MB	从 6.1.0 升级: 7993 MB 从 6.2.0 升级: 9320 MB 从 6.2.1 升级: 11571 MB 从 6.2.2 升级: 11487 MB	—	因硬件而异

6.2.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 2100 系列	从 6.2.1 升级: 7356 MB 从 6.2.2 升级: 11356 MB	从 6.2.1 升级: 7356 MB 从 6.2.2 升级: 11356 MB	1000 MB	从 6.2.1 升级: 15 分钟 从 6.2.2 升级: 15 分钟
Firepower 4100 系列 Firepower 9300	从 6.1.0 升级: 5593 MB 从 6.2.0 升级: 5122 MB 从 6.2.2 升级: 7498 MB	从 6.1.0 升级: 5593 MB 从 6.2.0 升级: 5122 MB 从 6.2.2 升级: 7498 MB	795 MB	从 6.1.0 升级: 10 分钟 从 6.2.0 升级: 12 分钟 从 6.2.2 升级: 15 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	从 6.1.0 升级: 0.88 MB 从 6.2.0 升级: 0.092 MB 从 6.2.2 升级: 0.88 MB	从 6.1.0 升级: 4322 MB 从 6.2.0 升级: 6421 MB 从 6.2.2 升级: 6450 MB	1000 MB	从 6.1.0 升级: 54 分钟 从 6.2.0 升级: 53 分钟 从 6.2.2 升级: 28 分钟
Firepower 威胁防御虚拟	从 6.1.0 升级: 0.076 MB 从 6.2.0 升级: 0.092 MB 从 6.2.2 升级: 0.092 MB	从 6.1.0 升级: 4225 MB 从 6.2.0 升级: 5179 MB 从 6.2.2 升级: 6450 MB	1000 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	从 6.1.0 升级: 18 MB 从 6.2.0 升级: 18 MB 从 6.2.2 升级: 18 MB	从 6.1.0 升级: 5145 MB 从 6.2.0 升级: 5732 MB 从 6.2.2 升级: 6752 MB	840 MB	从 6.1.0 升级: 29 分钟 从 6.2.0 升级: 31 分钟 从 6.2.2 升级: 31 分钟
ASA FirePOWER 模块	从 6.1.0 升级: 16 MB 从 6.2.0 升级: 16 MB 从 6.2.2 升级: 16 MB	从 6.1.0 升级: 7286 MB 从 6.2.0 升级: 7286 MB 从 6.2.2 升级: 10748 MB	从 6.1.0 升级: 1200 MB 从 6.2.0 升级: 1200 MB	从 6.1.0 升级: 94 分钟 从 6.2.0 升级: 104 分钟 从 6.2.2 升级: 96 分钟
NGIPSv	从 6.1.0 升级: 18 MB 从 6.2.0 升级: 19 MB 从 6.2.2 升级: 19 MB	从 6.1.0 升级: 4115 MB 从 6.2.0 升级: 5505 MB 从 6.2.2 升级: 5871 MB	741 MB	因硬件而异

6.2.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	从 6.2.0 升级: 22 MB 从 6.2.1 升级: 21 分钟	从 6.2.0 升级: 6467 MB 从 6.2.1 升级: 6916 MB	—	从 6.2.0 升级: 52 分钟 从 6.2.1 升级: 61 分钟

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心虚拟	从 6.2.0 升级: 24 MB 从 6.2.1 升级: 24 MB	从 6.2.0 升级: 6987 MB 从 6.2.1 升级: 5975 MB	—	因硬件而异
Firepower 2100 系列	5613 MB	5613 MB	925 MB	57 分钟
Firepower 4100 系列 Firepower 9300	4635 MB	4635 MB	743 MB	14 分钟
Firepower 威胁防御虚拟	0.92 MB	3586 MB	987 MB	因硬件而异
具备 Firepower 威胁防御的 ASA 5500-X 系列	0.16 MB	3683 MB	987 MB	80 分钟
Firepower 7000 系列 Firepower 8000 系列	18 MB	6745 MB	1300 MB	27 分钟
ASA FirePOWER 模块	16 MB	7021 MB	1200 MB	131 分钟
NGIPSv	18 MB	7261 MB	1300 MB	因硬件而异

6.2.2.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	18 MB	1656 MB	—	从 6.2.2 升级: 34 分钟 从 6.2.2.1 升级: 27 分钟
Firepower 管理中心虚拟	19 MB	2356 MB	—	因硬件而异
Firepower 2100 系列	2377 MB	2377 MB	497 MB	从 6.2.2 升级: 41 分钟 从 6.2.2.1 升级: 20 分钟
Firepower 4100 系列 Firepower 9300	561 MB	561 MB	41 MB	从 6.2.2 升级: 21 分钟 从 6.2.2.1 升级: 13 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	122 MB	984 MB	136 MB	从 6.2.2 升级: 110 分钟 从 6.2.2.1 升级: 70 分钟
Firepower 威胁防御虚拟	122 MB	984 MB	136 MB	因硬件而异

6.2.2.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 7000 系列 Firepower 8000 系列	16 MB	1706 MB	310 MB	从 6.2.2 升级: 56 分钟 从 6.2.2.1 升级: 40 分钟
ASA FirePOWER 模块	15 MB	1602 MB	190 MB	从 6.2.2 升级: 113 分钟 从 6.2.2.1 升级: 80 分钟
NGIPSv	17 MB	170 MB	16 MB	因硬件而异

6.2.2.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.2.2 升级的时间
Firepower 管理中心	18 MB	480 MB	—	52 分钟
Firepower 管理中心虚拟	30 MB	775 MB	—	因硬件而异
Firepower 2100 系列	1003 MB	1003 MB	47 MB	28 分钟
Firepower 4100 系列 Firepower 9300	299 MB	299 MB	47 MB	35 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	121 MB	674 MB	69 MB	72 分钟
Firepower 威胁防御虚拟	121 MB	674 MB	69 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	14 MB	664 MB	61 MB	33 分钟
ASA FirePOWER 模块	15 MB	758 MB	83 MB	90 分钟
NGIPSv	17 MB	106 MB	10 MB	因硬件而异

6.2.0 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	17 MB	10207 MB	—	57 分钟
Firepower 管理中心虚拟	17 MB	10207 MB	—	因硬件而异

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 4100 系列 Firepower 9300	5234 MB	5234 MB	734 MB	21 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	0.096 MB	5213 MB	938 MB	83 分钟
Firepower 威胁防御虚拟	1 MB	5663 MB	936 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	17 MB	6129 MB	1200 MB	27 分钟
ASA FirePOWER 模块	16 MB	6619 MB	1100 MB	165 分钟
NGIPSv	18 MB	7028 MB	1300 MB	因硬件而异

6.2.0.5 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	180 MB	6009 MB	—	从 6.2.0 升级：72 分钟 从 6.2.0.4 升级：34 分钟
Firepower 管理中心虚拟	20 MB	6943 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	3009 MB	3009 MB	441 MB	从 6.2.0 升级：28 分钟 从 6.2.0.4 升级：16 分钟
Firepower 威胁防御虚拟	135 MB	2805 MB	548 MB	因硬件而异
具备 Firepower 威胁防御的 ASA 5500-X 系列	135 MB	4316 MB	548 MB	从 6.2.0 升级：46 分钟 从 6.2.0.4 升级：22 分钟
Firepower 7000 系列 Firepower 8000 系列	18 MB	5806 MB	693 MB	从 6.2.0 升级：51 分钟 从 6.2.0.4 升级：18 分钟
ASA FirePOWER 模块	16 MB	5945 MB	703 MB	从 6.2.0 升级：66 分钟 从 6.2.0.4 升级：27 分钟

6.2.0.4 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
NGIPSv	18 MB	1301 MB	211 MB	因硬件而异

6.2.0.4 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	167 MB	5271 MB	—	从 6.2.0 升级：84 分钟 从 6.2.0.3 升级：50 分钟
Firepower 管理中心虚拟	20 MB	5346 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	1828 MB	1828 MB	325 MB	从 6.2.0 升级：23 分钟 从 6.2.0.3 升级：12 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	134 MB	3593 MB	448 MB	从 6.2.0 升级：2 小时 28 分钟 从 6.2.0.3 升级：69 分钟
Firepower 威胁防御虚拟	136 MB	275 MB	448 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	18 MB	4614 MB	608 MB	从 6.2.0 升级：45 分钟 从 6.2.0.3 升级：17 分钟
ASA FirePOWER 模块	16 MB	4585 MB	597 MB	从 6.2.0 升级：3 小时 34 分钟 从 6.2.0.3 升级：83 分钟
NGIPSv	18 MB	1067 MB	208 MB	因硬件而异

6.2.0.3 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	18 MB	3352 MB	—	从 6.2.0 升级：75 分钟 从 6.2.0.2 升级：37 分钟

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心虚拟	19 MB	3342 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	1355 MB	—	319 MB	从 6.2.0 升级: 18 分钟 从 6.2.0.2 升级: 12 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	2302 MB	131 MB	384 MB	从 6.2.0 升级: 118 分钟 从 6.2.0.2 升级: 76 分钟
Firepower 威胁防御虚拟	17 MB	842 MB	384 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	17 MB	3526 MB	554 MB	从 6.2.0 升级: 38 分钟 从 6.2.0.2 升级: 19 分钟
ASA FirePOWER 模块	3361 MB	15 MB	521 MB	从 6.2.0 升级: 3 小时 从 6.2.0.2 升级: 97 分钟
NGIPSv	17 MB	842 MB	202 MB	因硬件而异

6.2.0.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	35 MB	1665 MB	—	从 6.2.0 升级: 36 分钟 从 6.2.0.1 升级: 30 分钟
Firepower 管理中心虚拟	21 MB	2834 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	1060 MB	1060 MB	274 MB	从 6.2.0 升级: 12 分钟 从 6.2.0.1 升级: 9 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	144 MB	1808 MB	295 MB	从 6.2.0 升级: 95 分钟 从 6.2.0.1 升级: 59 分钟
Firepower 威胁防御虚拟	143 MB	998 MB	295 MB	因硬件而异

6.2.0.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 7000 系列 Firepower 8000 系列	17 MB	2110 MB	458 MB	从 6.2.0 升级: 54 分钟 从 6.2.0.1 升级: 35 分钟
ASA FirePOWER 模块	17 MB	2014 MB	383 MB	从 6.2.0 升级: 40 分钟 从 6.2.0.1 升级: 80 分钟
NGIPSv	19 MB	612 MB	195 MB	因硬件而异

6.2.0.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.2.0 升级的时间
Firepower 管理中心	50 MB	1237 MB	—	28 分钟
Firepower 管理中心虚拟	23 MB	1488 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	524 MB	524 MB	137 MB	12 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	144 MB	945 MB	159 MB	62 分钟
Firepower 威胁防御虚拟	10 MB	144 MB	159 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	18 MB	1134 MB	186 MB	22 分钟
ASA FirePOWER 模块	17 MB	97 MB	206 MB	69 分钟
NGIPSv	19 MB	721 MB	98 MB	因硬件而异

6.1.0 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	18 MB	10722 MB	—	47 分钟
Firepower 管理中心虚拟	17 MB	10128 MB	—	因硬件而异
具备 Firepower 威胁防御的 ASA 5500-X 系列	0.096 MB	5213 MB	914 MB	21 分钟

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 威胁防御虚拟	0.096 MB	5403 MB	914 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	61 MB	7108 MB	1740 MB	39 分钟
ASA FirePOWER 模块	47 MB	8392 MB	1300 MB	59 分钟
NGIPSv	54 MB	6368 MB	1229 MB	因硬件而异

6.1.0.6 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.1.0.5 升级的时间
Firepower 管理中心	215 MB	10503 MB	—	从 6.1.0 升级：66 分钟 从 6.1.0.5 升级：27 分钟
Firepower 管理中心虚拟	196 MB	1367 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	8140 MB	8140 MB	1126 MB	从 6.1.0 升级：270 分钟 从 6.1.0.5 升级：75 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	1034 MB	8540 MB	1229 MB	从 6.1.0 升级：40 分钟 从 6.1.0.5 升级：15 分钟
Firepower 威胁防御虚拟	1033 MB	7414 MB	1229 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	237 MB	12725 MB	1434 MB	从 6.1.0 升级：136 分钟 从 6.1.0.5 升级：34 分钟
ASA FirePOWER 模块	31 MB	11189 MB	1131 MB	从 6.1.0 升级：257 分钟 从 6.1.0.5 升级：60 分钟
NGIPSv	196 MB	4606 MB	644 MB	因硬件而异

6.1.0.5 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.1.0.4 升级的时间
Firepower 管理中心	46 MB	7673 MB	—	从 6.1.0 升级：56 分钟 从 6.1.0.4 升级：28 分钟
Firepower 管理中心虚拟	216 MB	10790 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	7680 MB	7680 MB	1060 MB	从 6.1.0 升级：30 分钟 从 6.1.0.4 升级：10 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	137 MB	7952 MB	1141 MB	从 6.1.0 升级：186 分钟 从 6.1.0.4 升级：70 分钟
Firepower 威胁防御虚拟	1140 MB	7453 MB	1141 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	259 MB	11877 MB	1403 MB	从 6.1.0 升级：115 分钟 从 6.1.0.4 升级：25 分钟
ASA FirePOWER 模块	34 MB	8955 MB	1217 MB	从 6.1.0 升级：208 分钟 从 6.1.0.4 升级：105 分钟
NGIPSv	215 MB	4298 MB	640 MB	因硬件而异

6.1.0.4 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	218808 MB	6739516 MB	—	从 6.1.0 升级：65 分钟 从 6.1.0.3 升级：30 分钟
Firepower 管理中心虚拟	200748 MB	675984 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	6010092 MB	6010092 MB	1020 MB	从 6.1.0 升级：26 分钟 从 6.1.0.3 升级：10 分钟

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
具备 Firepower 威胁防御的 ASA 5500-X 系列	1058968 MB	6155828 MB	1100 MB	从 6.1.0 升级: 49 分钟 从 6.1.0.3 升级: 20 分钟
Firepower 威胁防御虚拟	1059632 MB	1059632 MB	1100 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	240940 MB	8713068 MB	1200 MB	从 6.1.0 升级: 48 分钟 从 6.1.0.3 升级: 17 分钟
ASA FirePOWER 模块	31740 MB	7442808 MB	1100 MB	从 6.1.0 升级: 63 分钟 从 6.1.0.3 升级: 45 分钟
NGIPSv	20120 MB	3367536 MB	636 MB	因硬件而异

6.1.0.3 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	218676 MB	5537816 MB	—	从 6.1.0 升级: 46 分钟 从 6.1.0.2 升级: 35 分钟
Firepower 管理中心虚拟	200904 MB	6611148 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	5014020 MB	5014020 MB	929 MB	从 6.1.0 升级: 22 分钟 从 6.1.0.2 升级: 13 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	1057776 MB	1057776 MB	1000 MB	从 6.1.0 升级: 40 分钟 从 6.1.0.2 升级: 23 分钟
Firepower 威胁防御虚拟	1059932 MB	1059932 MB	1000 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	228728 MB	7357340 MB	1100 MB	从 6.1.0 升级: 43 分钟 从 6.1.0.2 升级: 25 分钟

6.1.0.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
ASA FirePOWER 模块	31792 MB	4782384 MB	1000 MB	从 6.1.0 升级: 160 分钟 从 6.1.0.2 升级: 80 分钟
NGIPSv	200896 MB	2710540 MB	635 MB	因硬件而异

6.1.0.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	235 MB	3872 MB	—	从 6.1.0 升级: 44 分钟 从 6.1.0.1 升级: 22 分钟
Firepower 管理中心虚拟	219 MB	3871 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	4046 MB	4046 MB	886 MB	从 6.1.0 升级: 20 分钟 从 6.1.0.1 升级: 14 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	96 MB	2291 MB	918 MB	从 6.1.0 升级: 74 分钟 从 6.1.0.1 升级: 106 分钟
Firepower 威胁防御虚拟	1137 MB	2797 MB	918 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	260 MB	4130 MB	965 MB	从 6.1.0 升级: 62 分钟 从 6.1.0.1 升级: 24 分钟
ASA FirePOWER 模块	40 MB	4549 MB	816 MB	从 6.1.0 升级: 139 分钟 从 6.1.0.1 升级: 34 分钟
NGIPSv	200896 MB	2710540 MB	635 MB	因硬件而异

6.1.0.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.1.0 升级的时间
Firepower 管理中心	140 MB	1893 MB	—	23 分钟

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.1.0 升级的时间
Firepower 管理中心虚拟	207 MB	2144 MB	—	因硬件而异
Firepower 4100 系列	580 MB	2580 MB	600 MB	15 分钟
Firepower 9300	1877 MB	1877 MB	600 MB	20 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	846 MB	1377 MB	600 MB	10 分钟
Firepower 威胁防御虚拟	846 MB	1377 MB	600 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	156 MB	2094 MB	513 MB	47 分钟
ASA FirePOWER 模块	34 MB	1728 MB	433 MB	76 分钟
NGIPSv	130 MB	793 MB	295 MB	因硬件而异

6.0.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	18 MB	8959 MB	—	66 分钟
Firepower 管理中心虚拟	-	-	-	-
Firepower 7000 系列 Firepower 8000 系列	227 MB	3683 MB	614 MB	30 分钟
ASA FirePOWER 模块	54 MB	2966 MB	429 MB	91 分钟
NGIPSv	196 MB	2090 MB	3050 MB	因硬件而异

6.0.1.4 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	201 MB	3428 MB	—	从 6.0.0 升级：92 分钟 从 6.0.1.3 升级：39 分钟
Firepower 管理中心虚拟	95 MB	3108 MB	—	因硬件而异

6.0.1.3 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 4100 系列	5237 MB	5237 MB	1000 MB	从 6.0.0 升级: 30 分钟 从 6.0.1.3 升级: 18 分钟
Firepower 9300	5434 MB	1360 MB	1000 MB	从 6.0.0 升级: 26 分钟 从 6.0.1.3 升级: 14 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	1017 MB	3416 MB	1000 MB	从 6.0.0 升级: 26 分钟 从 6.0.1.3 升级: 14 分钟
Firepower 威胁防御虚拟	1020 MB	3619 MB	1000 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	222 MB	7891 MB	1270 MB	从 6.0.0 升级: 47 分钟 从 6.0.1.3 升级: 23 分钟
ASA FirePOWER 模块	45 MB	6049 MB	990 MB	从 6.0.0 升级: 95 分钟 从 6.0.1.3 升级: 43 分钟
NGIPSv	192 MB	2916 MB	990 MB	因硬件而异

6.0.1.3 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	110 MB	2419 MB	—	58 分钟
Firepower 管理中心虚拟	101 MB	2419 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	2781 MB	2781 MB	473 MB	22 分钟
具备 Firepower 威胁防御的 ASA 5500-X 系列	813 MB	2641 MB	473 MB	24 分钟
Firepower 威胁防御虚拟	813 MB	2651 MB	473 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	125 MB	4757 MB	926 MB	55 分钟

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
ASA FirePOWER 模块	58 MB	3883 MB	685 MB	184 分钟
NGIPSv	107 MB	1695 MB	430 MB	因硬件而异

6.0.1.2 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	54 MB	272 MB	—	7 分钟
Firepower 管理中心虚拟	54 MB	368 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	56 MB	2101 MB	302 MB	16 分钟
具备 Firepower 威胁防 御的 ASA 5500-X 系列	807 MB	740 MB	302 MB	13 分钟
Firepower 威胁防御虚拟	56 MB	2101 MB	302 MB	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	63 MB	3190 MB	412 MB	17 分钟
ASA FirePOWER 模块	54 MB	2027 MB	577 MB	99 分钟
NGIPSv	56 MB	602 MB	243 MB	因硬件而异

6.0.1.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.0.1 升级的时间
Firepower 管理中心	54 MB	14 MB	—	23 分钟
Firepower 管理中心虚拟	54 MB	14 MB	—	因硬件而异
Firepower 4100 系列 Firepower 9300	54 MB	54 MB	2 MB	6 分钟
具备 Firepower 威胁防 御的 ASA 5500-X 系列	54 MB	54 MB	2 MB	7 分钟
Firepower 威胁防御虚拟	54 MB	14 MB	2 MB	因硬件而异

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.0.1 升级的时间
Firepower 7000 系列 Firepower 8000 系列	61 MB	944 MB	166 MB	39 分钟
ASA FirePOWER 模块	54 MB	824 MB	84 MB	46 分钟
NGIPSv	56 MB	54 MB	1 MB	因硬件而异

6.0 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	Time
Firepower 管理中心	16 MB	8022 MB	—	58 分钟
Firepower 管理中心虚拟	16 MB	8022 MB	—	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	16 MB	6496 MB	1200 MB	94 分钟
ASA FirePOWER 模块	32 MB	7644 MB	1200 MB	41 分钟
NGIPSv	17 MB	6046 MB	102000 MB	因硬件而异

6.0.0.1 版本时间和磁盘空间

设备	/ 上的空间	/Volume 上的空间	管理器上的空间	从 6.0 升级的时间
Firepower 管理中心	120 MB	976 MB	—	25 分钟
Firepower 管理中心虚拟	119 MB	969 MB	—	因硬件而异
Firepower 7000 系列 Firepower 8000 系列	134 MB	1568 MB	273 MB	25 分钟
ASA FirePOWER 模块	56 MB	1101 MB	181 MB	56 分钟
NGIPSv	26 MB	929 MB	174 MB	因硬件而异