



思科 Firepower 4100/9300 FXOS Firepower 机箱管理器配置指南， 2.4(1)

首次发布日期: 2018 年 10 月 25 日

上次修改日期: 2019 年 2 月 12 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

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。© 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

本文档的所有打印副本和复制的电子副本均被视为非受控副本。最新版本请参阅当前在线版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址和电话号码。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此 URL：[www.cisco.com go trademarks](http://www.cisco.com/go/trademarks)。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1721R)

© 2018 - 2019 Cisco Systems, Inc. 保留所有权利。



目录

第 1 章	Firepower 安全设备简介 1
	关于 Firepower 安全设备 1
	Firepower 机箱管理器 概况 1
	监控机箱状态 2

第 2 章	使用入门 5
	任务流 5
	初始配置 6
	登录或注销 Firepower 机箱管理器 8
	访问 FXOS CLI 9

第 3 章	ASA 的许可证管理 11
	关于智能软件许可 11
	适用于 ASA 的智能软件许可 11
	智能软件管理器和账户 12
	离线管理 12
	永久许可证预留 12
	卫星服务器 12
	按虚拟账户管理的许可证和设备 13
	评估许可证 13
	智能软件管理器通信 13
	设备注册和令牌 13
	与许可证颁发机构的定期通信 14
	不合规状态 14

Smart Call Home 基础设施	14
智能软件许可必备条件	14
智能软件许可准则	15
智能软件许可的默认设置	15
配置定期智能软件许可	15
(可选) 配置 HTTP 代理	15
(可选) 删除 Call Home URL	16
向许可证颁发机构注册 Firepower 安全设备	16
配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱	17
配置永久许可证预留	18
安装永久许可证	18
(可选) 返还永久许可证	19
智能软件许可历史记录	20

第 4 章

用户管理	21
用户账户	21
面向用户名的指导原则	22
密码的指导原则	23
远程身份验证指导原则	24
用户角色	26
本地身份验证用户的密码配置文件	26
配置用户设置	27
配置会话超时	29
配置绝对会话超时	30
设置最大尝试登录次数	31
查看和清除用户锁定状态	32
配置最小密码长度检查	33
创建本地用户账户	34
删除本地用户账户	35
激活或停用本地用户账户	35
清除本地身份验证的用户的密码历史记录	36

第 5 章	映像管理 37
	关于映像管理 37
	从 Cisco.com 下载映像 38
	将映像上传到 Firepower 安全设备 38
	验证映像的完整性 39
	升级 Firepower 可扩展操作系统平台捆绑包 39
	更新逻辑设备的映像版本 40
	固件升级 41

第 6 章	安全认证合规性 45
	安全认证合规性 45
	生成 SSH 主机密钥 46
	配置 IPSec 安全通道 47
	配置信任点静态 CRL 52
	关于证书撤销吊销列表检查 53
	配置 CRL 定期下载 56
	设置 LDAP 密钥环证书 58
	启用客户端证书身份验证 59

第 7 章	系统管理 61
	导致 Firepower 机箱管理器会话关闭的系统更改 61
	更改管理 IP 地址 62
	更改应用管理 IP 63
	更改 Firepower 4100/9300 机箱名称 66
	登录前横幅 67
	创建登录前横幅 67
	修改登录前横幅 68
	删除登录前横幅 69
	重新启动 Firepower 4100/9300 机箱 70
	关闭 Firepower 4100/9300 机箱电源 70

恢复出厂默认配置	70
安装受信任身份证书	71

第 8 章

平台设置 79

启用 NTP 服务器身份验证	79
设置日期和时间	80
查看配置的日期和时间	80
设置时区	81
使用 NTP 设置日期和时间	81
删除 NTP 服务器	82
手动设置日期和时间	82
配置 SSH	83
配置 TLS	84
配置 Telnet	85
配置 SNMP	86
关于 SNMP	86
SNMP 通知	87
SNMP 安全级别和权限	87
支持的 SNMP 安全模型和级别组合	88
SNMPv3 安全功能	88
SNMP 支持	88
启用 SNMP 并配置 SNMP 属性	89
创建 SNMP 陷阱	90
删除 SNMP 陷阱	91
创建 SNMPv3 用户	91
删除 SNMPv3 用户	93
配置 HTTPS	93
证书、密钥环和受信任点	94
创建密钥环	94
重新生成默认密钥环	95
创建密钥环的证书请求	96

使用基本选项创建密钥环证书请求	96
使用高级选项创建密钥环的证书请求	97
创建受信任点	99
将证书导入密钥环	100
配置 HTTPS	102
更改 HTTPS 端口	103
删除密钥环	104
删除受信任点	104
禁用 HTTPS	105
配置 AAA	105
关于 AAA	106
配置 LDAP 提供程序	107
配置 LDAP 提供程序的属性	107
创建 LDAP 提供程序	108
删除 LDAP 提供程序	110
配置 RADIUS 提供程序	110
配置 RADIUS 提供程序的属性	110
创建 RADIUS 提供程序	110
删除 RADIUS 提供程序	112
配置 TACACS+ 提供程序	112
配置 TACACS+ 提供程序的属性	112
创建 TACACS+ 提供程序	112
删除 TACACS+ 提供程序	113
配置系统日志	114
配置 DNS 服务器	117
启用 FIPS 模式	117
启用通用标准模式	118
配置 IP 访问列表	119
为容器实例接口添加 MAC 池前缀，并查看其 MAC 地址	119
为容器实例添加资源配置文件	120
配置机箱 URL	121

第 9 章

接口管理 123

- 关于 Firepower 接口 123
 - 机箱管理接口 123
 - 接口类型 123
 - 机箱和应用中的独立接口状态 124
 - 硬件旁路对 124
 - 巨帧支持 125
 - 共享接口可扩展性 125
 - 共享接口最佳实践 126
 - 共享接口使用示例 126
 - 查看共享接口资源 135
 - Firepower 威胁防御的内联集链路状态传播 136
- Firepower 接口的准则和限制 136
- 配置接口 138
 - 启用或禁用接口 138
 - 配置物理接口 139
 - 添加 EtherChannel（端口通道） 139
 - 为容器实例添加 VLAN 子接口 141
 - 配置分支电缆 143
- 监控接口 144
- 排除接口故障 145
- 接口历史 151

第 10 章

逻辑设备 153

- 关于逻辑设备 153
 - 独立和集群逻辑设备 153
 - 容器实例和本地实例 154
 - 容器实例接口 154
 - 机箱如何将数据包分类 154
 - 分类示例 155

级联容器实例	158
典型多实例部署	159
容器实例接口的自动 MAC 地址	160
容器实例资源管理	161
容器实例与高可用性	161
逻辑设备的要求和必备条件	161
集群要求和必备条件	161
容器实例的要求和必备条件	163
适用于逻辑设备的准则和限制	164
一般准则和限制	164
集群准则和限制	165
添加独立的逻辑设备	169
添加独立 ASA	169
添加独立的 Firepower 威胁防御	170
添加高可用性对	173
添加集群	174
关于集群 Firepower 4100/9300 机箱	174
主设备角色和辅助设备角色	175
集群控制链接	175
管理网络	176
管理接口	176
跨网络 EtherChannel	177
站点间集群	177
添加 ASA 集群	178
创建 ASA 集群	178
添加更多集群成员	181
添加 Firepower 威胁防御集群	182
创建 Firepower 威胁防御集群	182
添加更多集群成员	185
配置 Radware DefensePro	187
关于 Radware DefensePro	187

Radware DefensePro 的必备条件	187
服务链准则	187
在独立逻辑设备上配置 Radware DefensePro	188
在机箱内集群上配置 Radware DefensePro	189
开放 UDP/TCP 端口和启用 vDP Web 服务	191
管理逻辑设备	191
连接到应用控制台	191
删除逻辑设备	193
删除与逻辑设备不关联的应用实例	194
更改 Firepower 威胁防御逻辑设备上的接口	194
更改 ASA 逻辑设备上的接口	195
修改或恢复逻辑设备的引导程序设置	196
“逻辑设备 (Logical Devices)” 页面	197
站点间集群示例	199
跨网络 EtherChannel 透明模式南北站点间集群示例	199
跨网络 EtherChannel 透明模式东西站点间集群示例	200
逻辑设备的历史记录	202

第 11 章

安全模块/引擎管理	207
关于 FXOS 安全模块/安全引擎	207
停用/重新启用安全模块	209
确认安全模块/引擎	209
重置安全模块/引擎	210
重新初始化安全模块/引擎	210
使网络模块离线或在线	211
关闭/开启安装的模块/引擎	212

第 12 章

配置导入/导出	213
关于配置导入/导出	213
导出 FXOS 配置文件	214
计划自动配置导出	214

设置配置导出提醒 215

导入配置文件 216

第 13 章

故障排除 219

数据包捕获 219

背板端口映射 219

数据包捕获准则和限制 220

创建或编辑数据包捕获会话 220

配置数据包捕获的过滤器 222

启动和停止数据包捕获会话 223

下载数据包捕获文件 223

删除数据包捕获会话 224

测试网络连接 224

确定端口通道状态 226

从软件故障中恢复 228

从损坏的文件系统中恢复 233

Firepower 威胁防御集群成员的灾难恢复 242



第 1 章

Firepower 安全设备简介

- [关于 Firepower 安全设备，第 1 页](#)
- [Firepower 机箱管理器 概况，第 1 页](#)
- [监控机箱状态，第 2 页](#)

关于 Firepower 安全设备

思科 Firepower 4100/9300 机箱是网络和内容安全解决方案的下一代平台。Firepower 4100/9300 机箱是思科以应用为中心的基础设施 (ACI) 安全解决方案的一部分，并且提供一种灵活、开放、安全的平台，用于实现可扩展性、一致控制和简化管理。

Firepower 4100/9300 机箱具有以下特点：

- 基于机箱的模块化安全系统 - 提供高性能、灵活的输入/输出配置和可扩展性。
- Firepower 机箱管理器- 图形用户界面可简单、直观地显示当前机箱状态并支持简化的机箱功能配置。
- FXOS CLI- 提供基于命令的接口，用于配置各种功能，监控机箱状态和访问高级故障排除功能。
- FXOS REST API- 允许用户以编程方式配置和管理其机箱。

Firepower 机箱管理器 概况

Firepower 可扩展操作系统提供 Web 界面，让您轻松配置平台设置和接口，调配设备，以及监控系统状态。用户界面顶部的导航栏提供到下列页面的访问：

- 概述 (Overview) - 从“概述 (Overview)”页面，您可以轻松监控 Firepower 机箱的状态。有关详细信息，请参阅[监控机箱状态，第 2 页](#)。
- 接口 (Interfaces) - 从“接口 (Interfaces)”页面，您可以查看机箱上安装的接口的状态，编辑接口属性，启用或禁用接口，以及创建端口通道。有关详细信息，请参阅[接口管理，第 123 页](#)。

- 逻辑设备 (Logical Devices) - 在“逻辑设备 (Logical Devices)”页面中，您可以创建、编辑和删除逻辑设备。您还可以查看现有逻辑设备的当前状态。有关详细信息，请参阅[逻辑设备](#)，第 153 页。
- 安全模块/安全引擎 - 从“安全模块/安全引擎”页面，您可以查看安全模块/引擎的状态并执行各种功能，例如电源重启、重新初始化、确认和解除授权。有关详细信息，请参阅[安全模块/引擎管理](#)，第 207 页。
- 平台设置 (Platform Settings) - 从“平台设置 (Platform Settings)”页面，您可以配置机箱的下列设置：日期和时间、SSH、SNMP、HTTPS、AAA、系统日志和 DNS。有关详细信息，请参阅[平台设置](#)，第 79 页。
- 系统设置 (System Settings) - 从“系统 (System)”菜单，您可以管理下列设置：
 - 许可 (Licensing) - 从“许可 (Licensing)”页面，您可以配置 Smart Call Home 设置，向许可证颁发机构注册 Firepower 机箱。有关详细信息，请参阅[ASA 的许可证管理](#)，第 11 页。
 - 更新 (Updates) - 从“更新 (Updates)”页面，您可以将平台捆绑包和应用映像上传到 Firepower 机箱。有关详细信息，请参阅[映像管理](#)，第 37 页。
 - 用户管理 - 从“用户管理”页面，您可以为 Firepower 4100/9300 机箱配置用户设置和定义用户账户。有关详细信息，请参阅[用户管理](#)，第 21 页。

监控机箱状态

在“概述 (Overview)”页面上，您可以轻松监控 Firepower 4100/9300 机箱的状态。“概述 (Overview)”页面提供下列元素：

- 设备信息 (Device Information) - “概述 (Overview)”页面顶部包含下列有关 Firepower 4100/9300 机箱的信息：
 - 机箱名称 (Chassis name) - 显示初始配置期间为机箱分配的名称。
 - IP 地址 (IP address) - 显示初始配置期间为机箱分配的管理 IP 地址。
 - 型号 - 显示 Firepower 4100/9300 机箱型号。
 - 版本 - 显示机箱上运行的 FXOS 版本。
 - 运行状态 (Operational State) - 显示机箱的可操作状态。
 - 机箱正常运行时间 (Chassis uptime) - 显示自从系统上次重新启动后经过的时间。
 - “关闭 (Shutdown)”按钮 - 正常关闭 Firepower 4100/9300 机箱（请参阅[关闭 Firepower 4100/9300 机箱电源](#)，第 70 页）。



注释 您可以在“安全模块/安全引擎 (Security Modules/Security Engine)”页面上打开/关闭安全模块/引擎的电源（请参阅[关闭/开启安装的模块/引擎](#)，第 212 页）。

- “重新启动 (Reboot)”按钮 - 正常关闭 Firepower 4100/9300 机箱（请参阅[重新启动 Firepower 4100/9300 机箱](#)，第 70 页）。



注释 您可以在“安全模块/安全引擎 (Security Modules/Security Engine)”页面上重置安全模块/引擎（请参阅[重置安全模块/引擎](#)，第 210 页）。

- “运行时间信息 (Uptime Information)”图标 - 将光标悬停在该图标上可查看机箱和任何已安装的安全模块/引擎的运行时间。
- 直观状态显示 (Visual Status Display) - “设备信息 (Device Information)”部分下面是机箱的直观展示图，显示机箱中安装的组件，并提供这些组件的常规状态。您可以将光标悬停在“直观状态显示 (Visual Status Display)”中显示的端口上，以获取更多信息，例如接口名称、速度、类型、管理状态和运行状态。对于带有多个安全模块的型号，您可以将光标悬停在“直观状态显示 (Visual Status Display)”中显示的安全模块上，以获取更多信息，例如设备名称、模板类型、管理状态和运行状态。如果在该安全模块上安装了逻辑设备，您还可以查看管理 IP 地址、软件版本和逻辑设备模式。
- 详细状态信息 (Detailed Status Information) - “直观状态显示 (Visual Status Display)”下面有一个表，其中包含机箱的详细状态信息。状态信息分为五个部分：“故障 (Faults)”、“接口 (Interfaces)”、“设备 (Devices)”、“许可证 (License)”和“资产 (Inventory)”。您可以看到上面各个部分的摘要，点击您想要查看信息的摘要区域，可以看到每个部分的更多详细信息。

系统为机箱提供以下详细状态信息：

- 故障 (Faults) - 列出系统中发生的故障。故障按严重性排序：“严重 (Critical)”、“主要 (Major)”、“次要 (Minor)”、“警告 (Warning)”和“信息 (Info)”。对于所列的每个故障，可以查看严重性、故障说明、原因、出现次数以及最新出现时间。您还可以查看是否已确认故障。

点击任何故障，可查看故障的更多详细信息或确认故障。要确认多个故障，请点击您想要确认的每个故障旁边的复选框，然后点击**确认**。可以使用**选择所有故障**和**取消选定的故障**按钮快速选择或取消选择多个故障。



注释 在消除了故障根源后，系统会在下个轮询间隔内自动将故障从列表中清除。如果用户正在想办法解决特定故障，他们可以确认故障，以便让其他用户了解当前正在处理故障。

- 接口 - 列出系统中安装的接口。所有接口选项卡显示接口名称、运行状态、管理状态、接收的字节数和传输的字节数。硬件绕行选项卡仅显示 FTD 应用上支持硬件绕行功能的接口对。对于每个接口对，显示运行状态：被禁用（没有为该对配置硬件绕行）、备用（配置了硬件绕行，但当前未处于活动状态）和旁路（在硬件绕行中处于活动状态）。
- 设备和网络 - 列出系统中配置的逻辑设备，并为每个逻辑设备提供以下详细信息（将光标悬停在某个条上即可显示）：设备名称、状态、映像版本、管理 IP 地址和核心数量。您还可以在页面底部查看容器实例转发表和 VLAN 组表。
- 许可证 - （对于 ASA 逻辑设备）显示是否启用智能许可，提供 Firepower 许可证的当前注册状态信息，并显示机箱的许可证授权信息。
- 资产 (Inventory) - 列出机箱中安装的组件，提供这些组件的相关详细信息，例如：组件名称、核心数量、安装位置、运行状态、互通性、容量、功率、温度、序列号、型号、部件号和供应商。



第 2 章

使用入门

- [任务流](#)，第 5 页
- [初始配置](#)，第 6 页
- [登录或注销 Firepower 机箱管理器](#)，第 8 页
- [访问 FXOS CLI](#)，第 9 页

任务流

以下程序显示配置 Firepower 4100/9300 机箱时应当完成的基本任务。

过程

- 步骤 1** 配置 Firepower 4100/9300 机箱硬件（请参阅[思科 Firepower 安全设备硬件安装指南](#)）。
 - 步骤 2** 完成初始配置（请参阅[初始配置](#)，第 6 页）。
 - 步骤 3** 登录 Firepower 机箱管理器（请参阅[登录或注销 Firepower 机箱管理器](#)，第 8 页）。
 - 步骤 4** 设置日期和时间（请参阅[设置日期和时间](#)，第 80 页）。
 - 步骤 5** 配置 DNS 服务器（请参阅[配置 DNS 服务器](#)，第 117 页）。
 - 步骤 6** 注册产品许可证（请参阅[ASA 的许可证管理](#)，第 11 页）。
 - 步骤 7** 配置用户（请参阅[用户管理](#)，第 21 页）。
 - 步骤 8** 按需执行软件更新（请参阅[映像管理](#)，第 37 页）。
 - 步骤 9** 配置其他平台设置（请参阅[平台设置](#)，第 79 页）。
 - 步骤 10** 配置接口（请参阅[接口管理](#)，第 123 页）。
 - 步骤 11** 创建逻辑设备（请参阅[逻辑设备](#)，第 153 页）。
-

初始配置

在可以使用 Firepower 机箱管理器或 FXOS CLI 配置和管理系统之前，必须使用通过控制台端口访问的 FXOS CLI 执行一些初始配置任务。当第一次使用 FXOS CLI 访问 Firepower 4100/9300 机箱时，您将会看到安装向导，可以用它来配置系统。

您可以选择从现有的备份文件恢复系统配置，或者遍历安装向导手动设置系统。如果选择恢复系统，备份文件必须可从管理网络访问。

您必须为 Firepower 4100/9300 机箱上的单一管理端口指定一个 IPv4 地址、网关和子网掩码，或者一个 IPv6 地址、网关和网络前缀。您可以为管理端口 IP 地址配置 IPv4 或 IPv6 地址。

开始之前

1. 在 Firepower 4100/9300 机箱上验证下列物理连接：

- 控制台端口以物理方式连接到计算机终端或控制台服务器。
- 1 Gbps 以太网管理端口连接到外部集线器、交换机或路由器。

有关详细信息，请参阅[思科 Firepower 安全设备硬件安装指南](#)。

2. 验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否如下所示：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

过程

步骤 1 连接到控制台端口。

步骤 2 打开 Firepower 4100/9300 机箱 的电源。

在 Firepower 4100/9300 机箱启动时，您将看到开机自检消息。

步骤 3 当未配置的系统启动时，安装向导将提示您输入配置系统所需的下列信息：

- 设置模式（从完整系统备份或初始设置中恢复）
- 强密码执行策略（对于强密码准则，请参阅[用户账户](#)，第 21 页）
- 管理员密码
- 系统名称
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀

- 默认网关 IPv4 或 IPv6 地址
- 用于 SSH 访问的 IP 块地址
- 用于 SSH 访问的 IPv4 或 IPv6 块子网掩码
- 用于 HTTPS 访问的 IP 块地址
- 用于 HTTPS 访问的 IPv4 或 IPv6 块子网掩码
- DNS 服务器 IPv4 或 IPv6 地址
- 默认域名

步骤 4 检查安装摘要，输入 **yes**，保存并应用设置，或者输入 **no**，再次遍历安装向导更改某些设置。

如果选择再次遍历安装向导，您之前输入的值将显示在括号中。要接受之前输入的值，请按 **Enter** 键。

示例

以下示例使用 IPv4 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
  SSH IPv4 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
  HTTPS IP block address: 0.0.0.0
  HTTPS IPv4 block netmask: 0.0.0.0
Configure the DNS Server IP address (yes/no) [n]:y
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: y
  Default domain name: domainname.com
Following configurations will be applied:
Switch Fabric=A
System Name=foo
Enforce Strong Password=no
Physical Switch Mgmt0 IP Address=192.168.10.10
Physical Switch Mgmt0 IP Netmask=255.255.255.0
Default Gateway=192.168.10.1
IPv6 value=0
SSH Access Configured=yes
  SSH IP Address=0.0.0.0
  SSH IP Netmask=0.0.0.0
HTTPS Access Configured=yes
  HTTPS IP Address=0.0.0.0
  HTTPS IP Netmask=0.0.0.0
DNS Server=20.10.20.10
```

```
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

以下示例使用 IPv6 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address : 2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Do you want to configure IP block for ssh access? (yes/no) [y]: y
SSH IPv6 block netmask: 0.0.0.0
Do you want to configure IP block for https access? (yes/no) [y]: y
HTTPS IP block address: 0.0.0.0
HTTPS IPv6 block netmask: 0.0.0.0
Configure the DNS Server IPv6 address? (yes/no) [n]: y
DNS IP address: 2001::101
Configure the DNS Server IP address (yes/no) [n]:
Configure the default domain name? (yes/no) [n]: y
Default domain name: domainname.com
Following configurations will be applied:
Switch Fabric=A
System Name=foo
Enforced Strong Password=no
Physical Switch Mgmt0 IPv6 Address=2001::107
Physical Switch Mgmt0 IPv6 Prefix=64
Default Gateway=2001::1
Ipv6 value=1
SSH Access Configured=yes
SSH IP Address=0.0.0.0
SSH IP Netmask=0.0.0.0
HTTPS Access Configured=yes
HTTPS IP Address=0.0.0.0
HTTPS IP Netmask=0.0.0.0
DNS Server=2001::101
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

登录或注销 Firepower 机箱管理器

在您使用 Firepower 机箱管理器配置 Firepower 4100/9300 机箱之前，必须使用有效的用户账户登录。有关用户账户的详细信息，请参阅[用户管理](#)，第 21 页。

如果在特定时间段内没有任何活动，系统会自动将您注销。默认情况下，此自动注销超时时间为 10 分钟。要配置此超时设置，请参阅[配置会话超时](#)，第 29 页。另外，您还可以配置一个绝对超时设置，使系统在经过特定时间后强制注销登录用户（即使用户会话处于活动状态）。要配置绝对超时设置，请参阅[配置绝对会话超时](#)，第 30 页。

有关会导致您自动从 Firepower 机箱管理器系统注销的所有系统更改列表，请参阅[导致 Firepower 机箱管理器会话关闭的系统更改](#)，第 61 页。



注释 您可以选择将 Firepower 机箱管理器配置为只允许一定数量的不成功登录尝试，然后，用户会被系统锁定一段指定的时间长度。有关详细信息，请参阅 [设置最大尝试登录次数](#)，第 31 页。

过程

步骤 1 要登录 Firepower 机箱管理器，请按以下步骤操作：

a) 使用支持的浏览器，在地址栏中输入以下 URL：

```
https://<chassis_mgmt_ip_address>
```

其中 <chassis_mgmt_ip_address> 是您在初始配置期间输入的 Firepower 4100/9300 机箱 IP 地址或主机名。

注释 有关受支持的浏览器的信息，请参阅您使用的版本的版本说明（请参阅 <http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html>）。

b) 输入您的用户名和密码。

c) 点击 **Login**。

您已登录，Firepower 机箱管理器打开以显示“概述 (Overview)”页面。

步骤 2 要注销 Firepower 机箱管理器，请指向导航栏中的用户名，然后选择注销。

您已注销 Firepower 机箱管理器，并返回登录屏幕。

访问 FXOS CLI

您可以使用插入到控制台端口中的终端来连接到 FXOS CLI。验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否为如下所示：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

您也可以使用 SSH 和 Telnet 连接到 FXOS CLI。Firepower 可扩展操作系统最多支持八个 SSH 并发连接。要使用 SSH 进行连接，您需要知道 Firepower 4100/9300 机箱的主机名或 IP 地址。

使用以下语法示例之一来通过 SSH、Telnet 或 Putty 进行登录：



注释 SSH 登录区分大小写。

使用 SSH 从 Linux 终端登录:

- **ssh ucs-auth-domain\username@{UCSM-ip-address | UCMS-ipv6-address}**

```
ssh ucs-example\jsmith@192.0.20.11
ssh ucs-example\jsmith@2001::1
```
- **ssh -l ucs-auth-domain\username {UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name}**

```
ssh -l ucs-example\jsmith 192.0.20.11
ssh -l ucs-example\jsmith 2001::1
```
- **ssh {UCSM-ip-address | UCSM-ipv6-address | UCSM-host-name} -l ucs-auth-domain\username**

```
ssh 192.0.20.11 -l ucs-example\jsmith
ssh 2001::1 -l ucs-example\jsmith
```
- **ssh ucs-auth-domain\username@{UCSM-ip-address | UCSM-ipv6-address}**

```
ssh ucs-ldap23\jsmith@192.0.20.11
ssh ucs-ldap23\jsmith@2001::1
```

使用 Telnet 从 Linux 终端登录:



注释 默认情况下，会禁用 Telnet。有关启用 Telnet 的说明，请参阅[配置 Telnet](#)，第 85 页。

- **telnet ucs-UCSM-host-name ucs-auth-domain\username**

```
telnet ucs-qa-10
login: ucs-ldap23\bladmin
```
- **telnet ucs-{UCSM-ip-address | UCSM-ipv6-address} ucs-auth-domain\username**

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\bladmin
```

从 Putty 客户端登录:

- 登录方式: **ucs-auth-domain\username**

```
Login as: ucs-example\jsmith
```



注释 如果默认身份验证设置为本地，并且控制台身份验证设置为 LDAP，您可以使用 **ucs-local\admin** 从 Putty 客户端登录交换矩阵互联，其中 admin 是本地账户名称。



第 3 章

ASA 的许可证管理

通过思科智能软件许可，您可以集中购买和管理许可证池。您可以轻松部署或停用设备，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。



注释 本节仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。

- [关于智能软件许可，第 11 页](#)
- [智能软件许可必备条件，第 14 页](#)
- [智能软件许可准则，第 15 页](#)
- [智能软件许可的默认设置，第 15 页](#)
- [配置定期智能软件许可，第 15 页](#)
- [配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱，第 17 页](#)
- [配置永久许可证预留，第 18 页](#)
- [智能软件许可历史记录，第 20 页](#)

关于智能软件许可

本部分介绍智能软件许可的工作原理。



注释 本节仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。

适用于 ASA 的智能软件许可

对于 Firepower 4100/9300 机箱上的 ASA 应用，智能软件许可配置分为两部分，分别在 Firepower 4100/9300 机箱管理引擎和应用中进行。

- Firepower 4100/9300 机箱- 所有智能软件许可基础设施均在管理引擎中配置，包括用于与许可证颁发机构进行通信的参数。Firepower 4100/9300 机箱本身无需任何许可证即可运行。



注释 机箱间集群需要您在集群的每个机箱上启用相同的智能许可方法。

- ASA 应用 - 配置应用中的所有许可证授权。

智能软件管理器和账户

在为设备购买一个或多个许可证时，可在思科智能软件管理器中对其进行管理：

<https://software.cisco.com/#module/SmartLicensing>

通过智能软件管理器，您可以为组织创建一个主账户。



注释 如果您还没有账户，请点击链接[设置新账户](#)。通过智能软件管理器，您可以为组织创建一个主账户。

默认情况下，许可证分配给主账户下的默认虚拟账户。作为账户管理员，您可以选择创建其他虚拟账户；例如，您可以为区域、部门或子公司创建账户。通过多个虚拟账户，您可以更轻松地管理大量许可证和设备。

离线管理

如果您的设备无法访问互联网且无法注册到许可证颁发机构，可以配置离线许可。

永久许可证预留

如果您的设备出于安全原因而无法访问互联网，您可以选择为每个ASA请求永久许可证。永久许可证不需要定期访问许可证颁发机构。与PAK许可证一样，您将为ASA购买一个许可证并安装许可证密钥。与PAK许可证不同的是，您将通过智能软件管理器获取和管理许可证。您可以在定期智能许可模式与永久许可证预留模式之间轻松切换。

您可以获取启用所有功能的许可证：具有最多安全环境的标准层级许可证和运营商许可证。许可证在Firepower 4100/9300机箱上管理，但您还需要请求ASA配置授权，以便ASA允许使用它们。

卫星服务器

如果您的设备出于安全原因无法访问互联网，您可以选择以虚拟机(VM)形式安装本地智能软件管理器卫星服务器。该卫星提供智能软件管理器功能的子集，并允许您为所有本地设备提供必要的许可服务。只有卫星需要定期连接到主许可证颁发机构以同步您的许可证使用。您可以按时间表执行同步，也可以手动同步。

一旦下载并部署该卫星应用之后，即可在不使用互联网将数据发送到思科SSM的情况下执行以下功能：

- 激活或注册许可证
- 查看公司的许可证
- 在公司实体之间传输许可证

有关详细信息，请参阅[智能账户管理器卫星](#)上的智能软件管理器卫星安装和配置指南。

按虚拟账户管理的许可证和设备

仅当虚拟账户可以使用分配给该账户的许可证时，才能按虚拟账户对许可证和设备进行管理。如果您需要其他许可证，则可以从另一个虚拟账户传输未使用的许可证。您还可以在虚拟账户之间迁移设备。

仅 Firepower 4100/9300 机箱会注册为设备，而机箱中的 ASA 应用会请求自己的许可证。例如，对于配有 3 个安全模块的 Firepower 9300 机箱，机箱计为一个设备，但模块使用 3 个单独的许可证。

评估许可证

Firepower 4100/9300 机箱支持两种类型的评估许可证：

- 机箱级评估模式 - 在 Firepower 4100/9300 机箱向许可证颁发机构注册之前，会在评估模式下运行 90 天（总使用量）。ASA 在此模式下无法请求特定授权，只能启用默认授权。当此期限结束时，Firepower 4100/9300 机箱会变为不合规。
- 基于授权的评估模式 - 在 Firepower 4100/9300 机箱向许可证颁发机构注册之后，您可以获取基于时间的评估许可证，并可将这些许可证分配给 ASA。在 ASA 中，可照常请求授权。当该基于时间的许可证到期时，您需要续订基于时间的许可证或获取永久许可证。



注释 您无法获得针对强密码 (3DES/AES) 的评估许可证；仅永久许可证支持此授权。

智能软件管理器通信

本部分介绍您的设备如何与智能软件管理器通信。

设备注册和令牌

对于每个虚拟账户，您可以创建注册令牌。默认情况下，此令牌有效期为 30 天。当部署每个机箱或注册现有机箱时，请输入此令牌 ID 以及授权级别。如果现有令牌已过期，则可以创建新的令牌。

在完成部署后或在现有机箱上手动配置这些参数后启动时，该机箱会向思科许可证颁发机构进行注册。当机箱向令牌注册时，许可证颁发机构会颁发一张 ID 证书，用于机箱与许可证颁发机构之间的通信。此证书有效期为 1 年，但需要每 6 个月续签一次。

与许可证颁发机构的定期通信

设备每30天与许可证颁发机构进行通信。如果您在智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。或者，也可以等待设备按计划通信。

您可以随意配置 HTTP 代理。

Firepower 4100/9300 机箱 必须可以直接访问互联网，或者至少可每 90 天通过 HTTP 代理访问互联网。常规许可证通信每 30 天进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。在宽限期后，您必须联系许可证颁发机构，否则您将无法对需要特殊许可证的功能进行配置更改，但操作则不受影响。

不合规状态

设备在以下情况下可能会处于不合规状态：

- 过度使用 - 当设备使用不可用的许可证时。
- 许可证到期 - 当基于时间的许可证到期时。
- 通信不畅 - 当设备无法访问许可证颁发机构以重新获得授权时。

要验证您的账户是否处于或接近不合规状态，必须将 Firepower 4100/9300 机箱当前正在使用的授权与智能账户中的授权进行比较。

在不合规状态下，无法更改需要特殊许可证的功能配置，但操作不受影响。例如，基于标准许可证限制的现有环境可以继续运行，您可以修改它们的配置，但无法添加新环境。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件位于指定许可证颁发机构 URL 的 FXOS 配置中。不能移除此配置文件。请注意，许可证配置文件的唯一可配置选项是许可证颁发机构的地址 URL。除非获得 Cisco TAC 的指示，否则不应更改许可证颁发机构 URL。

智能软件许可必备条件

- 请注意，本章仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。
- 在思科智能软件管理器上创建主账户：
<https://software.cisco.com/#module/SmartLicensing>
如果您还没有账户，请点击此链接以 [设置新账户](#)。通过智能软件管理器，您可以为组织创建一个主账户。
- 通过 [思科商务工作空间](#) 购买 1 个或多个许可证。在主页上，通过 [查找产品](#) 和 [解决方案](#) 搜索字段搜索您的平台。有些许可证是免费的，但您仍需要将它们添加到智能软件许可账户。
- 确保可从机箱访问互联网或访问 HTTP 代理，以使机箱能够访问许可证颁发机构。

- 配置 DNS 服务器，以使机箱能够解析许可证颁发机构的名称。
- 设置机箱的时间。
- 在配置 ASA 许可授权之前，请在 Firepower 4100/9300 机箱上配置智能软件许可基础设施。

智能软件许可准则

ASA 故障切换和集群指南

每个 Firepower 4100/9300 机箱都必须注册到许可证颁发机构或卫星服务器中。辅助设备不会产生额外成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。

智能软件许可的默认设置

Firepower 4100/9300 机箱默认配置包括名为“SLProf”的 Smart Call Home 配置文件，该文件用于指定许可颁发机构的 URL。

配置定期智能软件许可

要与思科许可证颁发机构通信，您可以选择配置 HTTP 代理。要向许可证颁发机构注册，必须在 Firepower 4100/9300 机箱上输入您从智能软件许可证账户获得的注册令牌 ID。

过程

- 步骤 1 (可选) 配置 HTTP 代理，第 15 页。
- 步骤 2 向许可证颁发机构注册 Firepower 安全设备，第 16 页。

(可选) 配置 HTTP 代理

如果您的网络使用 HTTP 代理进行互联网访问，则必须为智能软件许可配置代理地址。此代理一般也用于 Smart Call Home。



注释 不支持认证的 HTTP 代理。

过程

步骤 1 选择系统 (System) > 许可 (Licensing) > Call Home。

Call Home 页面提供用于配置许可证颁发机构的目的地 URL 以及配置 HTTP 代理的字段。

注释 除非获得思科 TAC 的指示，否则不应更改许可证颁发机构 URL。

步骤 2 在“服务器启用 (Server Enable)”下拉列表中，选择开 (on)。

步骤 3 在服务器 URL (Server URL) 和服务器端口 (Server Port) 字段中输入代理 IP 地址和端口。例如，为 HTTPS 服务器输入端口 443。

步骤 4 点击保存 (Save)。

(可选) 删除 Call Home URL

使用以下程序删除先前配置的 Call Home URL。

过程

步骤 1 选择系统 (System) > 许可 (Licensing) > Call Home。

步骤 2 在 Call home 配置 (Call home Configuration) 区域中，选择删除 (Delete)。

向许可证颁发机构注册 Firepower 安全设备

当注册 Firepower 4100/9300 机箱时，许可证颁发机构会为 Firepower 4100/9300 机箱与许可证颁发机构之间的通信颁发 ID 证书。它还会将 Firepower 4100/9300 机箱分配到相应的虚拟账户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于诸如通信问题等原因而到期，则稍后可能需要重新注册 Firepower 4100/9300 机箱。

过程

步骤 1 在智能软件管理器或智能软件管理器卫星中，为要将此 Firepower 4100/9300 机箱添加到的虚拟账户请求并复制注册令牌。

有关如何使用智能软件管理器卫星请求注册令牌的详细信息，请参阅《思科智能软件管理器卫星用户指南》(<https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html>)。

步骤 2 在 Firepower 机箱管理器中，选择系统 (System) > 许可 (Licensing) > 智能许可证 (Smart License)。

步骤 3 在输入产品实例注册令牌 (Enter Product Instance Registration Token) 字段中输入注册令牌。

步骤 4 点击 Register。

Firepower 4100/9300 机箱尝试向许可证颁发机构注册。

要取消注册设备，请点击**取消注册 (Unregister)**。

取消注册 Firepower 4100/9300 机箱会从账户中删除设备。系统会删除设备上的所有许可证授权和证书。您可能希望取消注册来为新的 Firepower 4100/9300 机箱释放许可证。或者，也可以从智能软件管理器删除设备。

配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱

以下程序显示如何配置 Firepower 4100/9300 机箱以使用智能许可证卫星服务器。

开始之前

- 满足**智能软件许可必备条件**，第 14 页中列出的所有必要条件。
- 部署和设置智能软件卫星服务器：

从 Cisco.com 下载**智能许可证卫星 OVA** 文件，并在 VMware ESXi 服务器上安装和配置此文件。有关详细信息，请参阅《**智能软件管理器卫星安装指南**》。

- 验证智能软件卫星服务器的 FQDN 是否可以被您的内部 DNS 服务器解析。
- 验证卫星信任点是否已存在：

scope security

show trustpoint

请注意，FXOS 版本 2.4(1) 及更高版本中默认添加信任点。如果信任点不存在，则必须采用以下步骤手动添加一个信任点：

1. 转至 <http://www.cisco.com/security/pki/certs/clrca.cer>，并将完整的 SSL 证书正文（从“-----BEGIN CERTIFICATE-----”到“-----END CERTIFICATE-----”）复制到您在配置期间可访问的某个位置。

2. 进入安全模式：

scope security

3. 创建并命名信任点：

create trustpoint trustpoint_name

4. 为信任点指定证书信息。注意：证书必须采用 Base64 编码 X.509 (CER) 格式。

set certchain certchain

对于 *certchain* 变量，粘贴您在步骤 1 中复制的证书文本。

如果在命令中未指定证书信息，系统会提示您输入证书或定义根证书颁发机构 (CA) 的证书路径的一系列信任点。在您输入信息的下一行，键入 **ENDOFBUF** 以完成操作。

5. 提交配置：

commit-buffer

过程

-
- 步骤 1** 选择系统 (System) > 许可 (Licensing) > Call Home。
- 步骤 2** 在 Call home 配置区域中，采用在此程序必备条件中收集的信息，将地址字段中的默认 URL 替换为智能软件卫星服务器的 URL，格式如下：**https://[FQDN of Satellite server]/Transportgateway/services/DeviceRequestHandler**
- 步骤 3** 向许可证颁发机构注册 Firepower 安全设备，第 16 页。请注意，必须从智能许可证管理器卫星请求和复制注册令牌。
-

配置永久许可证预留

您可以为 Firepower 4100/9300 机箱分配一个永久许可证。此通用预留允许您在设备上不受计数限制地使用任何授权。



注释 在开始之前，您必须购买永久许可证，才能在智能软件管理器中使用。并非所有账户都被批准使用永久许可证预留。在您尝试配置此功能之前，请确保已获得思科批准。

安装永久许可证

以下程序介绍如何为您的 Firepower 4100/9300 机箱分配永久许可证。

过程

-
- 步骤 1** 选择 System > Licensing > Permanent License。
- 步骤 2** 点击 **Generate** 生成预留申请代码。将预留申请代码复制到剪贴板。
- 步骤 3** 转至思科智能软件管理器门户的“智能软件管理器库存”屏幕，点击 **Licenses** 选项卡：
<https://software.cisco.com/#SmartLicensing-Inventory>
- Licenses** 选项卡显示与您的账户相关的所有现有许可证（普通类型和永久类型）。
- 步骤 4** 点击 **License Reservation**，并将生成的预留申请代码粘贴到框中。
- 步骤 5** 点击 **Reserve License**。
- 智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您未看到**License Reservation**按钮，则您的账户无权使用永久许可证预留。在这种情况下，您应禁用永久许可证预留并重新输入普通的智能许可证命令。

步骤 6 在 Firepower 机箱管理器中，向**Authorization Code**文本框中输入生成的授权代码。

步骤 7 点击 **Install**。

在您的 Firepower 4100/9300 机箱完全获得 PLR 许可后，“永久许可证”页面将显示您的许可证状态，并提供返还永久许可证的选项。

步骤 8 在 ASA 逻辑设备上启用功能授权。请参阅 [ASA 授权章节](#)以启用授权。

(可选) 返还永久许可证

如果不再需要永久许可证，您必须使用以下程序将其正式返还给智能软件管理器。如果不遵循所有步骤，许可证将保持使用状态，无法在其他地方使用。

过程

步骤 1 选择**System > Licensing > Permanent License**。

步骤 2 点击**Return**生成返还代码。将返还代码复制到剪贴板。

Firepower 4100/9300 机箱会立即变成未获许可并转变为“评估”状态。

步骤 3 访问“智能软件管理器库存”屏幕，点击**Product Instances**选项卡：

<https://software.cisco.com/#SmartLicensing-Inventory>

步骤 4 使用通用设备标识符 (UDI) 搜索您的 Firepower 4100/9300 机箱。

步骤 5 选择**Actions > Remove**，并将生成的返还代码粘贴到框中。

步骤 6 点击 **Remove Product Instance**。

永久许可证被返还到可用池。

步骤 7 重启系统。有关如何重新引导您的 Firepower 4100/9300 机箱的详细信息，请参阅[重新启动 Firepower 4100/9300 机箱](#)，第 70 页。

智能软件许可历史记录

功能名称	平台版本	描述
面向 Firepower 4100/9300 机箱的思科智能软件许可	1.1(1)	<p>通过智能软件许可，您可以购买和管理许可证池。智能许可证不与特定序列号关联。您可以轻松部署或停用设备，而不必管理每台设备的许可密钥。通过智能软件许可，您还可以直观地了解许可证使用情况和需求。智能软件许可配置划分为 Firepower 4100/9300 机箱管理引擎和安全模块两部分。</p> <p>引入了以下屏幕：</p> <p>系统 > 许可 > Call Home</p> <p>系统 > 许可 > 智能许可证</p>



第 4 章

用户管理

- [用户账户，第 21 页](#)
- [面向用户名的指导原则，第 22 页](#)
- [密码的指导原则，第 23 页](#)
- [远程身份验证指导原则，第 24 页](#)
- [用户角色，第 26 页](#)
- [本地身份验证用户的密码配置文件，第 26 页](#)
- [配置用户设置，第 27 页](#)
- [配置会话超时，第 29 页](#)
- [配置绝对会话超时，第 30 页](#)
- [设置最大尝试登录次数，第 31 页](#)
- [查看和清除用户锁定状态，第 32 页](#)
- [配置最小密码长度检查，第 33 页](#)
- [创建本地用户账户，第 34 页](#)
- [删除本地用户账户，第 35 页](#)
- [激活或停用本地用户账户，第 35 页](#)
- [清除本地身份验证的用户的密码历史记录，第 36 页](#)

用户账户

用户账户用于访问系统。您最多可配置 48 个本地用户账户。每个用户账户必须具有唯一的用户名和密码。

管理员账户

管理员账户是默认用户账户，并且无法修改或删除。此账户是系统管理员或超级用户账户并具有完整权限。管理员账户没有已分配的默认密码；您必须在初始系统设置中选择密码。

管理员账户始终处于活动状态，并且不会到期。无法将管理员账户配置为非活动状态。

本地身份验证的用户账户

本地身份验证用户账户直接通过机箱进行身份验证，并且可以由具有管理员或 AAA 权限的任何用户来启用或禁用。一旦本地用户账户被禁用，该用户将无法登录。已禁用本地用户账户的详细配置信息不会被数据库删除。如果重新启用已禁用的本地用户账户，此账户将再次处于活动状态，且采用现有配置（包括用户名和密码）。

远程身份验证的用户账户

远程身份验证的用户账户是指任何通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的用户账户。

如果用户同时持有本地用户账户和远程用户账户，则在本地用户账户中定义的角色将覆盖在远程用户账户中持有的角色。

有关远程身份验证指导原则以及如何配置和删除远程身份验证提供程序的详细信息，请参阅以下主题：

- [远程身份验证指导原则，第 24 页](#)
- [配置 LDAP 提供程序，第 107 页](#)
- [配置 RADIUS 提供程序，第 110 页](#)
- [配置 TACACS+ 提供程序，第 112 页](#)

用户账户的到期

您可以配置用户账户在预定时间过期。当到达到期时间时，系统将会禁用用户账户。

默认情况下，用户账户不会到期。

使用到期日期配置用户账户后，无法将该账户重新配置为不到期。然而，您可以为账户配置可用的最新过期日期。

面向用户名的指导原则

用户名还用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。将登录 ID 分配到用户账户时，请考虑以下指导原则和限制：

- 登录 ID 可以包含 1 到 32 个字符，包括以下字符：
 - 任何字母字符
 - 任何数字
 - _（下划线）
 - -（连字符）
 - .（圆点）
- 登录 ID 必须唯一。

- 登录 ID 必须以字母字符开头，而不能以数字或特殊字符开头，例如下划线。
- 登录 ID 区分大小写。
- 无法创建全数字登录 ID。
- 创建用户账户后，无法更改登录 ID。必须删除该用户账户，创建新的用户账户。

密码的指导原则

密码对于每个本地认证的用户账户都是必需的。具有管理员或 AAA 权限的用户可以配置系统，以对用户密码执行密码强度检查。如果密码强度检查已启用，则每个用户必须使用强密码。

建议每个用户都使用强密码。如果对本地身份验证的用户启用密码强度检查，则 Firepower 可扩展操作系统将拒绝不符合以下要求的任何密码：

- 必须包含最少 8 个字符，最多 80 个字符。



注释 您可以选择在系统上配置 15 个字符（最小密码长度）的密码，以符合通用标准需求。有关详细信息，请参阅[配置最小密码长度检查](#)，第 33 页。

- 必须包含至少一个大写字母字符。
- 必须包含至少一个小写字母字符。
- 必须包含至少一个非字母数字（特殊）字符。
- 不能包含连续重复 3 次的字符，例如 aaabbb。
- 不得包含三个以任何顺序排列的连续数字或字母，例如 passwordABC 或 password321。
- 不能与用户名相同，或与用户名正好相反。
- 必须通过密码字典检查。例如，密码不可以是标准的词典单词。
- 不得包含以下符号：\$（美元符号）、?（问号）和 =（等号）。



注释 无论密码强度检查是否启用，此限制均适用。

- 本地用户和管理员账户的密码不得为空。

远程身份验证指导原则

如果为支持的远程身份验证服务之一配置系统，则必须创建用于为该服务的创建提供程序，以确保 Firepower 4100/9300 机箱 能够与系统进行通信。下列指导原则影响用户授权：

远程身份验证服务中的用户账户

用户账户可能存在于 Firepower 4100/9300 机箱本地或远程身份验证服务器中。

您可以查看通过 Firepower 机箱管理器或 FXOS CLI 中的远程身份验证服务登录的用户的临时会话。

远程身份验证服务中的用户角色

如果在远程身份验证服务器中创建用户账户，则必须确保账户包括用户在 Firepower 4100/9300 机箱中工作所需的角色，并且这些角色的名称与 FXOS 中使用的名称相匹配。基于角色策略，可能不允许用户进行登录，也可能仅授予用户只读权限。

远程身份验证提供程序中的用户属性

对于 RADIUS 和 TACAS+ 配置，您必须在用户用于登录 Firepower 机箱管理器或 FXOS CLI 的每个远程身份验证提供程序中为 Firepower 4100/9300 机箱配置一个用户属性。此用户属性存储分配给各用户的角色和区域设置信息。

用户登录后，FXOS 执行以下操作：

1. 查询远程身份验证服务。
2. 验证用户。
3. 如果对用户进行了验证，则检查分配给该用户的角色和区域设置。

下表包含 FXOS 支持的远程身份验证提供程序的用户属性要求比较：

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
LDAP	可选	您可以选择执行以下操作之一： <ul style="list-style-type: none"> • 请不要扩展 LDAP 方案，配置符合要求的现有的未使用属性。 • 扩展 LDAP 方案，使用唯一名称（例如，CiscoAVPair）创建自定义属性。 	思科 LDAP 实施需要 unicode 类型属性。 如果选择创建 CiscoAVPair 自定义属性，请使用以下属性 ID： 1.3.6.1.4.1.9.287247.1 以下部分提供示例 OID。

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
RADIUS	可选	<p>您可以选择执行以下操作之一：</p> <ul style="list-style-type: none"> • 请不要扩展 RADIUS 方案，并使用符合要求的现有的未使用属性。 • 扩展 RADIUS 方案，使用唯一名称（例如，<code>cisco-avpair</code>）创建自定义属性。 	<p>思科 RADIUS 实施的供应商 ID 为 009，属性的供应商 ID 为 001。</p> <p>以下语法示例显示，如果选择创建 <code>cisco-avpair</code> 属性，如何指定多个用户角色和区域： <code>shell:roles="admin,aaa"</code> <code>shell:locales="L1,abc"</code>。 使用逗号 “,” 作为分隔多个值的分隔符。</p>
TACACS+	必要	<p>必须扩展方案，并使用名称 <code>cisco-av-pair</code> 创建自定义属性。</p>	<p><code>cisco-av-pair</code> 名称是为 TACACS+ 提供程序提供属性 ID 的字符串。</p> <p>以下语法示例显示如何在创建 <code>cisco-av-pair</code> 属性时指定多个用户角色和区域： <code>cisco-av-pair=shell:roles="admin,aaa"</code> <code>shell:locales*"L1,abc"</code>。在 <code>cisco-av-pair</code> 属性语法中使用星号 (*) 将区域标记为可选项，以避免使用相同身份验证配置文件的其他思科设备的身份验证失败。使用空格作为分隔符来分隔多个值。</p>

LDAP 用户属性的示例 OID

以下是自定义 `CiscoAVPair` 属性的示例 OID：

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
```

```
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
LDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

用户角色

系统包含以下用户角色：

管理员

完成对整个系统的读写访问。默认情况，下会向默认管理员账户分配此角色，并且不能对其进行更改。

只读

对系统配置进行只读访问，但无权修改系统状态。

运营

对 NTP 配置、用于智能许可的 Smart Call Home 配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。

AAA 管理员

对用户、角色和 AAA 配置的读写访问。对系统其余部分的读取访问。

本地身份验证用户的密码配置文件

密码配置文件包含所有本地身份验证用户的密码历史记录和密码更改时间间隔属性。不能为每个本地身份验证的用户指定其他密码配置文件。

密码历史记录计数

借助密码历史记录计数，您可以阻止本地身份验证的用户反复使用同一密码。配置此属性后，Firepower 机箱最多可以存储本地身份验证的用户先前使用的 15 个密码。密码存储的顺序与时间顺序正好相反，最近的密码在前，这样可确保当达到历史记录计数阈值后仅重复使用最旧的密码。

用户必须创建和使用在密码历史记录计数中配置的密码数量，然后才能重新使用密码。例如，如果您将密码历史记录计数设置为 8，本地身份验证用户无法重新使用第一个密码，直至第九个密码过期为止。

默认情况下，密码历史记录设置为 0。该值禁用历史记录计数，允许用户随时重新使用以前的密码。

如有必要，可以清除本地身份验证的用户的密码历史记录计数并支持重复使用先前的密码。

密码更改间隔

通过密码更改间隔，可以限制本地身份验证的用户在特定小时数内能够进行的密码更改次数。下表介绍密码更改间隔的两个配置选项。

间隔配置	说明	示例
不允许密码更改 (No password change allowed)	此选项不允许在密码更改后的指定小时数内更改本地身份验证的用户的密码。 可以指定介于 1 和 745 小时之间的无更改间隔。默认情况下，无更改间隔为 24 小时。	例如，要在本地身份验证用户更改其密码后 48 小时内阻止更改密码，请进行以下设置： <ul style="list-style-type: none"> • 将在间隔期间更改设置为禁用 • 将无更改间隔设置为 48
更改间隔内允许密码更改 (Password changes allowed within change interval)	此选项指定本地身份验证的用户的密码在预定义间隔内可以更改的最大次数。 可以指定介于 1 和 745 小时之间的更改间隔，以及介于 0 和 10 之间的最大密码更改次数。默认情况下，允许本地身份验证的用户在 48 小时间隔内最多更改 2 次密码。	例如，要在本地身份验证用户更改其密码后 24 小时内最多允许一次密码更改，请进行以下设置： <ul style="list-style-type: none"> • 将在间隔期间更改设置为启用 • 将更改计数设置为 1 • 将更改间隔设置为 24

配置用户设置

过程

步骤 1 选择系统 (System) > 用户管理 (User Management)。

步骤 2 点击设置 (Settings) 选项卡。

步骤 3 使用必填信息填写下列字段：

名称	说明
默认身份验证字段	<p>在远程登录期间，对用户进行身份验证的默认方式。这可以是以下其中一项：</p> <ul style="list-style-type: none"> • 本地 (Local) - 必须在 Firepower 机箱本地定义用户账户。 • Radius - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户账户。 • TACACS - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户账户。 • LDAP - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户账户。 • 无 (None) - 如果用户账户是 Firepower 机箱的本地账户，当用户在远程登录时，不需要密码。
控制台身份验证字段	<p>通过控制台端口连接到 FXOS CLI 时用于用户身份验证的方法。这可以是以下其中一项：</p> <ul style="list-style-type: none"> • 本地 (Local) - 必须在 Firepower 机箱本地定义用户账户。 • Radius - 必须在为 Firepower 机箱指定的 RADIUS 服务器上定义用户账户。 • TACACS - 必须在为 Firepower 机箱指定的 TACACS+ 服务器上定义用户账户。 • LDAP - 必须在为 Firepower 机箱指定的 LDAP/MS-AD 服务器上定义用户账户。 • 无 (None) - 如果用户账户是 Firepower 机箱的本地账户，则在用户使用控制台端口连接至 FXOS CLI 时无需密码。
远程用户设置	
远程用户角色策略	<p>控制当用户尝试登录并且远程身份验证提供程序不向用户角色提供身份验证信息时发生的事情：</p> <ul style="list-style-type: none"> • 分配默认角色 (Assign Default Role) - 允许用户使用只读用户角色登录。 • 无登录 (No-Login) - 不允许用户登录系统，即使用户名和密码正确也是如此。
本地用户设置	
密码强度检查 (Password Strength Check) 复选框	<p>如果选中，所有本地用户密码都必须符合强密码准则（请参阅密码的指导原则，第 23 页）。</p>

名称	说明
历史记录计数字段	<p>用户在重新使用先前使用的密码之前必须创建的唯一密码的数量。历史记录计数的顺序与时间顺序正好相反，最近的密码在前，这样可确保当达到历史记录计数阈值后仅重复使用最旧的密码。</p> <p>该值可以是介于 0 和 15 之间的任意值。</p> <p>您可以将历史记录计数 (History Count) 字段设置为 0，这表示禁用历史记录计数，使用户随时都能够重复使用之前已使用的密码。</p>
间隔期间更改字段	<p>控制本地验证用户何时能够更改其密码。该字段可以是：</p> <ul style="list-style-type: none"> • 启用 (Enable)-本地身份验证用户可以根据“更改间隔 (Change Interval)”和“更改计数 (Change Count)”设置更改其密码。 • 禁用 (Disable)-本地身份验证用户不能在为“无更改间隔 (No Change Interval)”指定的期限内更改其密码。
更改间隔字段	<p>在其期间执行在更改计数 (Change Count) 字段中指定的密码更改次数的小时数。</p> <p>该值可以是介于 1 和 745 小时之间的任意值。</p> <p>例如，如果该字段设置为 48，更改计数 (Change Count) 字段设置为 2，那么本地身份验证用户在 48 小时内执行的密码更改不能超过 2 次。</p>
更改计数字段	<p>本地身份验证用户能够在“更改间隔 (Change Interval)”内更改其密码的最大次数。</p> <p>该值可以是介于 0 和 10 之间的任意值。</p>
无更改间隔字段	<p>本地身份验证用户在更改新建密码之前必须等待的最少小时数。</p> <p>该值可以是介于 1 和 745 小时之间的任意值。</p> <p>如果未将间隔期间更改 (Change During Interval) 属性设置为禁用 (Disable)，该时间间隔将被忽略。</p>

步骤 4 点击保存。

配置会话超时

您可以使用 FXOS CLI 来指定 Firepower 4100/9300 机箱在关闭用户会话之前允许用户不活动的时间段。您可以为控制台会话以及 HTTPS、SSH 和 Telnet 会话配置不同的设置。

超时值最大可设置为 3600 秒（60 分钟）。默认值为 600 秒。要禁用此设置，请将会话超时值设置为 0。

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 进入默认授权安全模式：

```
Firepower-chassis /security # scope default-auth
```

步骤 3 设置 HTTPS、SSH 和 Telnet 会话的空闲超时：

```
Firepower-chassis /security/default-auth # set session-timeout seconds
```

步骤 4 （可选）设置控制台会话的空闲超时：

```
Firepower-chassis /security/default-auth # set con-session-timeout seconds
```

步骤 5 （可选）查看会话和绝对会话超时设置：

```
Firepower-chassis /security/default-auth # show detail
```

示例：

```
Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No
```

配置绝对会话超时

Firepower 4100/9300 机箱具有绝对会话超时设置，即系统会在绝对会话超时期限已过后关闭用户会话，而不考虑会话是否在使用。此绝对超时功能具全局性，适用于所有形式的访问（包括串行控制台、SSH 和 HTTPS）。

您可以为串行控制台会话单独配置绝对会话超时。这允许针对调试需求禁用串行控制台绝对会话超时，同时保持其他访问形式的超时。

绝对超时值默认为 3600 秒（60 分钟），可使用 FXOS CLI 进行更改。要禁用此设置，请将绝对会话超时值设为 0。

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 进入默认授权安全模式：

```
Firepower-chassis /security # scope default-auth
```

步骤 3 设置绝对会话超时：

```
Firepower-chassis /security/default-auth # set absolute-session-timeout seconds
```

步骤 4 （可选）设置单独的控制台绝对会话超时：

```
Firepower-chassis /security/default-auth # set con-absolute-session-timeout seconds
```

步骤 5 （可选）查看会话和绝对会话超时设置：

```
Firepower-chassis /security/default-auth # show detail
```

示例：

```
Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Idle Session timeout (in secs) for web, ssh, telnet sessions: 600
Absolute Session timeout (in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No
```

设置最大尝试登录次数

您可配置在将用户您可配置允许用户尝试登录的最大失败次数，如果超过该次数，用户会被 Firepower 4100/9300 机箱 锁定一段指定的时间长度之前允许用户尝试登录的最大失败次数。锁定一段指定的时间长度。如果用户超过设置的最大尝试登录次数，用户会被系统锁定。系统不会显示表明用户被锁定的通知。在这种情况下，用户必须等待一段指定的时间长度，然后才能尝试登录。

执行以下步骤，以配置最大登录尝试次数。

**注释**

- 在超过最大尝试登录次数后，所有类型的用户账户（包括管理员账户）均被锁定。
- 默认的最大尝试登录失败次数为 0。在超过最大尝试登录次数后，用户被系统锁定的默认时间长度为 30 分钟（1800 秒）。
- 有关查看用户锁定状态和清除用户锁定状态的步骤，请参阅[查看和清除用户锁定状态](#)，第 32 页。

这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅[安全认证合规性](#)，第 45 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

```
scope security
```

步骤 2 设置最大尝试登录失败次数。

```
set max-login-attempts num_attempts
```

num_attempts 值可以是 0 到 10 之间的任何整数。

步骤 3 指定在达到最大尝试登录次数后用户应被系统锁定的时间长度（以秒为单位）：

```
set user-account-unlock-time
```

```
unlock_time
```

步骤 4 提交配置：

```
commit-buffer
```

查看和清除用户锁定状态

对于超过 Maximum Number of Login Attempts CLI 设置中指定的最大失败登录尝试次数之后被 Firepower 4100/9300 机箱锁定的用户，管理员用户可查看和清除其锁定状态。有关详细信息，请参阅[设置最大尝试登录次数](#)，第 31 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

```
scope security
```


步骤 2 显示相关用户的用户信息（包括锁定状态）：

```
Firepower-chassis /security # show local-user user detail
```

示例：

```
Local User user:
First Name:
Last Name:
Email:
Phone:
Expiration: Never
Password:
User lock status: Locked
Account status: Active
User Roles:
Name: read-only
User SSH public key:
```

步骤 3 （可选）清除用户锁定状态：

```
Firepower-chassis /security # scope local-user user
```

```
Firepower-chassis /security/local-user # clear lock-status
```

配置最小密码长度检查

如果启用最小密码长度检查，则必须使用指定的最小数目的字符创建密码。例如，如果将 *min_length* 选项设为 15，则用户必须使用 15 个或更多字符创建密码。此选项是在系统上用于实施通用标准认证合规性的众多选项之一。有关详细信息，请参阅[安全认证合规性，第 45 页](#)。

执行以下步骤，以配置最小密码长度检查。

过程

步骤 1 从 FXOS CLI 进入安全模式：

```
scope security
```

步骤 2 指定最小密码长度：

```
set min-password-length min_length
```

步骤 3 提交配置：

```
commit-buffer
```

创建本地用户账户

过程

- 步骤 1** 选择系统 (System) > 用户管理 (User Management)。
- 步骤 2** 点击本地用户 (Local Users) 选项卡。
- 步骤 3** 点击添加用户 (Add User)，可打开添加用户 (Add User) 对话框。
- 步骤 4** 使用关于用户的必填信息，填写下列字段：

名称	说明
用户名字段	登录此账户时使用的账户名称。此名称必须唯一，并满足用户账户名称的准则和限制（请参阅 面向用户名的指导原则，第 22 页 ）。 保存用户后，不能更改登录 ID。必须删除该用户账户，创建新的用户账户。
名字字段	用户的名字。该字段最多包含 32 个字符。
姓氏字段	用户的姓氏。该字段最多包含 32 个字符。
邮件字段	用户的邮件地址。
电话号码字段	用户的电话号码。
密码字段	与此账户关联的密码。如果启用了密码强度检查，则用户的密码必须为强密码，Firepower 可扩展操作系统会拒绝任何不满足强度检查要求的密码（请参阅 密码的指导原则，第 23 页 ）。 注释 密码不得包含以下符号：\$（美元符号）、?（问号）和 =（等号）。无论密码强度检查是否启用，此限制均适用。
确认密码字段	第二次用于确认目的的密码。
账户状态字段	如果状态设置为 活动 (Active) ，用户可以登录使用此登录 ID 和密码登录 Firepower 机箱管理器和 FXOS CLI。

名称	说明
用户角色 列表	<p>代表要分配给用户账户的权限的角色（请参阅用户角色，第 26 页）。</p> <p>所有用户均默认分配了“只读 (Read-Only)”角色，并且此角色无法取消选择。要分配多个角色，请按住 Ctrl 键并点击所需角色。</p> <p>注释 用户角色和权限的更改在用户下一次登录之后才会生效。如果在向用户账户分配新角色或从中删除现有角色时用户已登录，则活动会话将继续使用上一个角色和权限。</p>
账户到期复选框	<p>如果选中，在到期日期 (Expiration Date) 字段中指定的日期过后，此账户将到期且无法使用。</p> <p>注释 在为用户账户配置过期日期后，无法将账户重新配置为不过期。然而，您可以为账户配置可用的最新过期日期。</p>
到期日期字段	<p>账户到期日期。日期格式应为 yyyy-mm-dd。</p> <p>点击此字段末尾的日历图标，查看您可以用来选择到期日期的日历。</p>

步骤 5 点击 **Add**。

删除本地用户账户

过程

- 步骤 1 依次选择系统 (**System**) > 用户管理 (**User Management**)。
- 步骤 2 点击本地用户 (**Local Users**) 选项卡。
- 步骤 3 在与您想要删除的用户账户对应的行中，点击删除 (**Delete**)。
- 步骤 4 在确认 (**Confirm**) 对话框中，点击是 (**Yes**)。

激活或停用本地用户账户

您必须是拥有管理员或 AAA 权限的用户，才能激活或停用本地用户账户。

过程

步骤 1 依次选择 **System > User Management**。

步骤 2 点击本地用户 (**Local Users**) 选项卡。

步骤 3 在您要激活或停用的用户账户所在的行中，点击编辑 (**Edit**) (铅笔图标)。

步骤 4 在编辑用户 (**Edit User**) 对话框中，执行以下操作之一：

- 要激活用户账户，请点击账户状态 (**Account Status**) 字段中的活动 (**Active**) 单选按钮。
- 要停用用户账户，请点击账户状态 (**Account Status**) 字段中的非活动 (**Inactive**) 单选按钮。

管理员用户账户始终设置为活动。不能修改。

步骤 5 点击保存 (**Save**)。

清除本地身份验证的用户的密码历史记录

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 进入已指定用户账户的本地用户安全模式：

```
Firepower-chassis /security # scope local-user user-name
```

步骤 3 清除已指定用户账户的密码历史记录：

```
Firepower-chassis /security/local-user # clear password-history
```

步骤 4 将任务提交到系统配置：

```
Firepower-chassis /security/local-user # commit-buffer
```

示例

以下示例将清除密码历史记录并提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```



第 5 章

映像管理

- 关于映像管理，第 37 页
- 从 Cisco.com 下载映像，第 38 页
- 将映像上传到 Firepower 安全设备，第 38 页
- 验证映像的完整性，第 39 页
- 升级 Firepower 可扩展操作系统平台捆绑包，第 39 页
- 更新逻辑设备的映像版本，第 40 页
- 固件升级，第 41 页

关于映像管理

Firepower 4100/9300 机箱使用的映像分为两个基本类型：



注释

所有映像都可通过安全启动进行数字签名和验证。请勿以任何方式修改映像，否则系统会报告验证错误。

- 平台捆绑包 (Platform Bundle) - Firepower 平台捆绑包是一系列运行在 Firepower 管理引擎和 Firepower 安全模块/引擎上的多个独立映像。平台捆绑包是 Firepower 可扩展操作系统软件包。
- 应用 (Application) - 应用是您想在安全模块/引擎的 Firepower 4100/9300 机箱上部署的软件映像。应用映像作为思科安全数据包文件 (CSP) 进行交付，一直存储在管理引擎上，直至创建逻辑设备的过程中，或者在为稍后创建逻辑设备执行准备的过程中，再部署到安全模块/引擎中。您可以在 Firepower 管理引擎上存储相同应用映像类型的多个不同版本。



注释

如果您正在升级平台捆绑包映像和一个或多个应用映像，必须首先升级平台捆绑包。

从 Cisco.com 下载映像

从 Cisco.com 下载 FXOS 和应用映像，以便将其上传到 Firepower 机箱。

开始之前

您必须有 Cisco.com 账户。

过程

-
- 步骤 1** 使用网络浏览器导航至<http://www.cisco.com/go/firepower9300-software>或<http://www.cisco.com/go/firepower4100-software>。
系统将在浏览器中打开 Firepower 4100/9300 机箱 的软件下载页面：
- 步骤 2** 查找适当的软件映像，然后将其下载到本地计算机。
-

将映像上传到 Firepower 安全设备

您可以将 FXOS 和应用映像上传到机箱。

开始之前

确保您要上传的映像在本地计算机上可用。

过程

-
- 步骤 1** 依次选择系统 (**System**) > 更新 (**Updates**)。
“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** 点击上传映像 (**Upload Image**)，可打开“上传映像” (Upload Image) 对话框。
- 步骤 3** 点击选择文件，可导航到并选择想要上传的映像。
- 步骤 4** 点击上传。
所选映像将上传到 Firepower 4100/9300 机箱。上传映像时，系统会显示进度条，指示上传完成百分比。
- 步骤 5** 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。
-

验证映像的完整性

将新的映像添加至 Firepower 4100/9300 机箱后，系统自动验证映像的完整性。如果需要，您可以使用以下过程手动验证映像的完整性。

过程

步骤 1 依次选择系统 (System) > 更新 (Updates)。

“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 点击与您要验证映像相对应的验证 (Verify) (复选标记图标)。

系统将验证映像的完整性并在“映像完整性 (Image Integrity)” 字段中显示状态。

升级 Firepower 可扩展操作系统平台捆绑包

开始之前

从 Cisco.com 下载平台捆绑包软件映像 (请参阅[从 Cisco.com 下载映像](#)，第 38 页)，然后将此映像上传到 Firepower 4100/9300 机箱 (请参阅[将映像上传到 Firepower 安全设备](#)，第 38 页)。



注释 升级过程通常需要 20 到 30 分钟。

如果要升级运行独立逻辑设备的 Firepower 9300 或 Firepower 4100 系列安全设备，或者如果要升级运行机箱内集群的 Firepower 9300 安全设备，则升级期间流量不会通过该设备。

如果要升级属于某机箱间集群的 Firepower 9300 或 Firepower 4100 系列安全设备，则升级期间流量不会通过正在升级的设备。但是，该集群中的其他设备仍然会通过流量。

过程

步骤 1 依次选择系统 (System) > 更新 (Updates)。

“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 点击想要升级到的 FXOS 平台捆绑包所对应的升级 (Upgrade)。

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

步骤 3 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。

更新逻辑设备的映像版本

使用此程序将 ASA 应用映像升级到新版本，或将 Firepower 威胁防御应用映像设为将在灾难恢复场景中使用的重新启动版本。

当您使用 Firepower 机箱管理器或 FXOS CLI 更改 Firepower 威胁防御逻辑设备上的启动版本时，应用不会立即升级至新版本。逻辑设备启动版本是 Firepower 威胁防御在灾难恢复场景中重新安装到的目标版本。有关详细信息，请参阅 [Firepower 威胁防御集群成员的灾难恢复，第 242 页](#)。在初始创建 FTD 逻辑设备后，您将无法使用 Firepower 机箱管理器或 FXOS CLI 升级 FTD 逻辑设备。要升级 FTD 逻辑设备，您必须使用 Firepower 管理中心。有关详细信息，请参阅《Firepower 系统版本说明》：<http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>。

另请注意，FTD 逻辑设备的任何更新都不会反映在 Firepower 机箱管理器的 **Logical Devices > Edit** 和 **System > Updates** 页面上。这些页面中显示的版本是指创建 FTD 逻辑设备所用的软件版本（CSP 映像）。

在您更改 ASA 逻辑设备上的启动版本时，ASA 会升级至该版本并恢复所有配置。根据您的配置，使用以下工作流程来更改 ASA 启动版本：

ASA 高可用性 -

1. 更改备用设备上的逻辑设备映像版本。
2. 激活备用设备。
3. 更改另一台设备上的应用版本。

ASA 机箱间集群 -

1. 更改从属设备上的启动版本。
2. 使从属设备成为主设备。
3. 更改原始主设备（现在的从属设备）上的启动版本。

开始之前

从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅 [从 Cisco.com 下载映像，第 38 页](#)），然后将该映射上传到 Firepower 4100/9300 机箱（请参阅 [将映像上传到 Firepower 安全设备，第 38 页](#)）。

如果您正在升级平台捆绑包映像和一个或多个应用映像，必须首先升级平台捆绑包。

过程

- 步骤 1** 选择逻辑设备 (**Logical Devices**) 打开“逻辑设备” (**Logical Devices**) 页面。
“逻辑设备” (**Logical Devices**) 页面显示在机箱上配置的逻辑设备列表。如果尚未配置任何逻辑设备，则系统将显示一条表明此情况的消息。
- 步骤 2** 点击想要更新的逻辑设备对应的**更新版本 (Update Version)**，可打开**更新映像版本 (Update Image Version)** 对话框。
- 步骤 3** 对于**新版本**，选择软件版本。
- 步骤 4** 点击 **OK**。

固件升级

使用以下操作步骤升级 Firepower 4100/9300 机箱上的固件。

过程

- 步骤 1** 使用网络浏览器导航至 <http://www.cisco.com/go/firepower9300-software> 或 <http://www.cisco.com/go/firepower4100-software>。
系统将在浏览器中打开 Firepower 4100/9300 机箱 的软件下载页面：
- 步骤 2** 从 Cisco.com 查找，然后将合适的固件包下载到您可从 Firepower 4100/9300 机箱访问的服务器。
- 步骤 3** 在 Firepower 4100/9300 机箱上，进入固件模式：
`Firepower-chassis # scope firmware`
- 步骤 4** 将 FXOS 固件映像下载到 Firepower 4100/9300 机箱：
`Firepower-chassis /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`
 - `scp:// username@hostname / path`
 - `sftp:// username@hostname / path`
 - `tftp:// hostname : port-num / path`
- 步骤 5** 要监控下载过程，请执行以下操作：
`Firepower-chassis /firmware # show download-task image_name detail`
- 步骤 6** 下载完成后，可输入以下命令查看固件包的内容：
`Firepower-chassis /firmware # show package image_name expand`

步骤 7 可输入以下命令查看固件包的版本号：

```
Firepower-chassis /firmware # show package
```

当安装固件包时，在以下步骤中使用此版本号：

步骤 8 要安装固件包：

a) 进入固件安装模式：

```
Firepower-chassis /firmware # scope firmware-install
```

b) 安装固件包：

```
Firepower-chassis /firmware/firmware-install # install firmware pack-version version_number
```

系统将验证固件包，并通知您验证过程可能需要几分钟才能完成。

c) 输入**yes**继续验证。

固件包验证完成后，系统将通知您安装过程可能需要几分钟才能完成，并且系统在更新过程中将重启。

d) 输入**yes**继续安装。升级流程中请勿重启 Firepower 4100/9300 机箱。

步骤 9 要监控升级流程，请执行以下操作：

```
Firepower-chassis /firmware/firmware-install # show detail
```

步骤 10 安装完成后，可输入以下命令查看当前固件版本：

```
top
```

```
scope chassis 1
```

```
show sup version
```

```
show nm-fpga-version
```

示例：

```
Firepower-chassis /firmware/firmware-install # top
```

```
Firepower-chassis# scope chassis 1
```

```
Firepower-chassis /chassis # show sup version
```

```
SUP FIRMWARE:
```

```
  ROMMON:
```

```
    Running-Vers: 1.0.14
```

```
    Package-Vers: 0.0
```

```
    Activate-Status: Ready
```

```
  FPGA:
```

```
    Running-Vers: 1.06
```

```
    Package-Vers: 0.0
```

```
    Activate-Status: Ready
```

```
Firepower-chassis /chassis # show nm-fpga-version
```

```
Network Module Version:
```

```
  Network Module Slot Running-Vers Package-Vers Activate-Status
```

```
  -----
```

```
                2 1.2.0          1.0.17          Ready
```

示例

下面的示例将固件升级到了版本 1.0.10:

```
Firepower-chassis# scope firmware
Firepower-chassis /firmware # download image
tftp://10.10.10.1/fxos-k9-fpr9k-firmware.1.0.10.SPA
Firepower-chassis /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.10.SPA detail

Download task:
  File Name: fxos-k9-fpr9k-firmware.1.0.10.SPA
  Protocol: Tftp
  Server: 10.10.10.1
  Port: 0
  Userid:
  Path:
  Downloaded Image Size (KB): 2104
  Time stamp: 2015-12-04T23:51:57.846
  State: Downloading
  Transfer Rate (KB/s): 263.000000
  Current Task: unpacking image fxos-k9-fpr9k-firmware.1.0.10.SPA on primary(
FSM-STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal)

Firepower-chassis /firmware # show package fxos-k9-fpr9k-firmware.1.0.10.SPA expand

Package fxos-k9-fpr9k-firmware.1.0.10.SPA:
  Images:
    fxos-k9-fpr9k-fpga.1.0.5.bin
    fxos-k9-fpr9k-rommon.1.0.10.bin

Firepower-chassis /firmware # show package

Name                                     Version
-----
fxos-k9-fpr9k-firmware.1.0.10.SPA      1.0.10

Firepower-chassis /firmware # scope firmware-install
Firepower-chassis /firmware/firmware-install # install firmware pack-version 1.0.10

Verifying FXOS firmware package 1.0.10. Verification could take several minutes.
Do you want to proceed? (yes/no):yes

FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA  : Upgrade from 1.04 to 1.05

This operation upgrades SUP firmware on Security Platform.
Here is the checklist of things that are recommended before starting the install operation
(1) Review current critical/major faults
(2) Initiate a configuration backup

Attention:
  The system will be reboot to upgrade the SUP firmware.
  The upgrade operation will take several minutes to complete.
  PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.
Do you want to proceed? (yes/no):yes

Upgrading FXOS SUP firmware software package version 1.0.10

command executed
```




第 6 章

安全认证合规性

- [安全认证合规性](#)，第 45 页
- [生成 SSH 主机密钥](#)，第 46 页
- [配置 IPSec 安全通道](#)，第 47 页
- [配置信任点静态 CRL](#)，第 52 页
- [关于证书撤销吊销列表检查](#)，第 53 页
- [配置 CRL 定期下载](#)，第 56 页
- [设置 LDAP 密钥环证书](#)，第 58 页
- [启用客户端证书身份验证](#)，第 59 页

安全认证合规性

美国联邦政府机构有时需要仅使用符合由美国国防部和全球认证组织建立的安全标准的设备和软件。Firepower 4100/9300 机箱支持符合其中若干安全认证标准。

请参阅以下主题，了解支持符合这些标准的功能的启用步骤：

- [启用 FIPS 模式](#)，第 117 页
- [启用通用标准模式](#)，第 118 页
- [配置 IPSec 安全通道](#)，第 47 页
- [配置信任点静态 CRL](#)，第 52 页
- [关于证书撤销吊销列表检查](#)，第 53 页
- [配置 CRL 定期下载](#)，第 56 页
- [启用 NTP 服务器身份验证](#)，第 79 页
- [设置 LDAP 密钥环证书](#)，第 58 页
- [配置 IP 访问列表](#)，第 119 页
- [启用客户端证书身份验证](#)，第 59 页
- [配置最小密码长度检查](#)，第 33 页

- [设置最大尝试登录次数，第 31 页](#)



注释 请注意，这些主题只讨论在 Firepower 4100/9300 机箱上启用认证合规性。在 Firepower 4100/9300 机箱上启用认证合规性不会将合规性自动传播到它连接的任何逻辑设备。

生成 SSH 主机密钥

在 FXOS 版本 2.0.1 之前，设备初始设置期间创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥并生成新的主机密钥。有关详细信息，请参阅 [启用 FIPS 模式，第 117 页](#) 或 [启用通用标准模式，第 118 页](#)。

执行以下步骤，以销毁旧的 SSH 主机密钥并生成新的符合认证证书要求的主机密钥。

过程

步骤 1 从 FXOS CLI 进入服务模式：

```
scope system
```

```
scope services
```

步骤 2 删除 SSH 主机密钥：

```
delete ssh-server host-key
```

步骤 3 提交配置：

```
commit-buffer
```

步骤 4 将 SSH 主机密钥长度设置为 2048 位：

```
set ssh-server host-key rsa 2048
```

步骤 5 提交配置：

```
commit-buffer
```

步骤 6 创建新的 SSH 主机密钥：

```
create ssh-server host-key
```

```
commit-buffer
```

步骤 7 确认新的主机密钥长度：

```
show ssh-server host-key
```

主机密钥长度：2048

配置 IPSec 安全通道

您可以在 Firepower 4100/9300 机箱上配置 IPSec，对通过公用网络的数据包提供端到端数据加密和身份验证服务。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅[安全认证合规性，第 45 页](#)。



注释

- 如果您在 FIPS 模式下使用 IPSec 安全通道，则 IPSec 对等体必须支持 RFC 7427。
- 如果选择配置执行 IKE 和 SA 连接间加密密钥强度的匹配（在以下步骤中将 `sa-strength-enforcement` 设为 `yes`）：

启用 SA 执行后：	在 IKE 协商的密钥大小小于 ESP 协商的密钥大小时，连接失败。 IKE 协商的密钥大小大于或等于 ESP 协商的密钥大小时，SA 执行检查通过并且连接成功。
禁用 SA 执行后：	SA 执行检查通过且连接成功。

执行以下步骤，以配置 IPSec 安全通道。

过程

- 步骤 1** 从 FXOS CLI 进入安全模式：
`scope security`
- 步骤 2** 创建密钥环：
`enter keyring ssp`
`! create certreq subject-name subject-name ip ip`
- 步骤 3** 输入关联的证书请求信息：
`enter certreq`
- 步骤 4** 设置国家/地区：
`set country country`
- 步骤 5** 设置 DNS：
`set dns dns`
- 步骤 6** 设置邮件：
`set e-mail 邮件`

步骤 7 设置 IP 信息:

```
set fi-a-ip fi-a-ip  
set fi-a-ipv6 fi-a-ipv6  
set fi-b-ip fi-b-ip  
set fi-b-ipv6 fi-b-ipv6  
set ipv6 ipv6
```

步骤 8 设置位置:

```
set locality locality
```

步骤 9 设置组织名称:

```
set org-name org-name
```

步骤 10 设置组织单位名称:

```
set org-unit-name org-unit-name
```

步骤 11 设置密码:

```
! set password
```

步骤 12 设置状态:

```
set state state
```

步骤 13 设置 certreq 的主题名称:

```
set subject-name subject-name
```

步骤 14 退出:

```
exit
```

步骤 15 设置模数:

```
set modulus modulus
```

步骤 16 设置证书请求的重新生成:

```
set regenerate { yes | no }
```

步骤 17 设置信任点:

```
set trustpoint interca
```

步骤 18 退出:

```
exit
```

步骤 19 输入新创建的信任点:

```
enter trustpoint interca
```

步骤 20 生成证书签名请求:

set certchain

示例:

```

-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2lyZ28xDTALBgNV
BAsMBFNUQIUxZCzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3Bac3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJhFw0yNjEyMDYxOTMzNTJhMHAcCzAJBgNVBAYTAIVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMAAsG
A1UECwwEU1RCVTELMakGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWc3Nzc3Bz3Au
bmV0MIICLjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCGKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/0RBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6y13nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLdkss1nO
xP9+1+Lc690V18/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FIRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QliGYSetlSHj18087o5s/pmQAWWRGkKpfDv3oH
cMPgl2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMODwBdeMG3EihxEEOUPTD
Fdu0HrTM51vwb+vr5wE9HsAiMj8UuujmHqH5mlwyy3Me+cEDH00hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLPrsVqSfJsAuVI/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDexvd0qbORWb31H32yS1
lla6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZIO4jcSlvtdizbbT8u5B4VcLKIC
x0vkkjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEA2ukWyMLQuLqTvhq7
W7DRmszPUWQ7edor7yxuQzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWVWxpo
pFahRhZyxVZ10DhKlzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DlpBQ29yweCbUkc9qiHKA0lbnvAxoroHwMBlD
94LrJCggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwrSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+Ukfp89hvJt/fluJ+s/VJSVZWK4tAWvR7w1
QngCKRjW6FypzeyNBetiJ07wO+Wt4e3KhIjJdyvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSa6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CgnViptn0w+uJ1Irr1oulk+/ZyPtBvFHUKFrhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBJn+BXgxmMg8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2lyZ28xDTALBgNV
BAsMBFNUQIUxZCzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3Bac3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTM0NTRaMHAcCzAJBgNVBAYTAIVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDADAuZXZzdGd1
MRMwEYQYDVQQDDAAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFHlpbmRlcm0xLWNh
QGluDGVybTEtY2EubmV0MIICLjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCGKCAgEA
wLpNnyEx514P8uDoWkWF3IZsegjhlANSodxuAumhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXI3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNVkfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipC/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfGUq11stkIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMAk/t8kCqhtGXfuLII
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFPcLCS9o5S5O2B6QfGcTZ
yKR6hsmwe22wpK8QI7/5oWNXl0lb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfh0IdPA28xlnfIBlazCmMmdPcBO6cbUQfCj5hSmk3StVQKglCjaujz55TGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLIZgJ5txSaVUIgrgVCJaf6/jrRRWoRjwT
AzvznYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T

```

```

BAUwAwEB/zAvBgNVHR8EKDAmMCSglqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybsS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbdZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWoc3lZlOi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyD79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgeurZxOpR+NwPwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCeI6aROIgDp/Hwvb0/+uThle89g8WZ0djTKFUM8uBO3f+Hl
/cbuyBO1+JrDMq8NkAjsxKIJlp1c3WbfCue/qcwtcfUBYZ4i53a56UNF5Ef0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF

```

步骤 21 显示证书签名请求：

show certreq

示例：

```

Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIICwTCCAakCAQAwVTELMakGA1UEBhMCVVMx CzAJBgNVBAgMAkNBMQwwCgYDVQQH
DANTSkmxDjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3t0laoxPbfE
p/ITK6rxFhPqSSbtm6sXer//VZFiDTWODockDIuf4Kja215mlS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClK/tsIxsPkV0
6OduZYXk2bnsLW6tNk3uzOIT2Q0FcZ1ET66C8fyyKwTrmVcZjDjkMm2nDFsPIX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvw4BF8vzwRpHWTdjU5YnRl
qiR4q7j1RmzVFxCdY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAAGJzAlBqkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEARTBoInXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZl03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMl9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbxPuHkj28kXAVczmTxXEkJBFLVduWNo6
DT3u0xImiPR1sqW1jpMwbhC+ZGdtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----

```

步骤 22 进入 IPsec 模式：

scope ipsec

步骤 23 设置日志冗长级别：

```
set log-level log_level
```

步骤 24 创建并输入一个 IPSec 连接：

```
enter connection connection_name
```

步骤 25 将 IPSec 模式设置为隧道或传输：

```
set mode tunnel_or_transport
```

步骤 26 设置本地 IP 地址：

```
set local-addr ip_address
```

步骤 27 设置远程 IP 地址：

```
set remote-addr ip_address
```

步骤 28 如果使用隧道模式，则设置远程子网：

```
set remote-subnet ip/mask
```

步骤 29 （可选）设置远程身份：

```
set remote-ike-ident remote_identity_name
```

步骤 30 设置密钥环名称：

```
set keyring-name name
```

步骤 31 （可选）设置密钥环密码：

```
set keyring-passwd passphrase
```

步骤 32 （可选）设置 IKE-SA 生命周期（分钟）：

```
set ike-rekey-time minutes
```

minutes 值可以是 60-1440（包含在内）之间的任何整数。

步骤 33 （可选）设置子 SA 生命周期（分钟）(30-480)：

```
set esp-rekey-time 分钟
```

minutes 值可以是 30-480（包含在内）之间的任何整数。

步骤 34 （可选）设置初次连接期间重新传输序列的执行次数：

```
set keyringtries retry_number
```

retry_number 值可以是 1-5（包含在内）之间的任何整数。

步骤 35 （可选）启用或禁用证书吊销列表检查：

```
set revoke-policy { relaxed | strict }
```

步骤 36 启用连接：

```
set admin-state enable
```

步骤 37 重新加载所有连接:

```
reload-conns
```

步骤 38 (可选) 将现有信任点名称添加至 IPsec:

```
create authority trustpoint_name
```

步骤 39 配置执行 IKE 和 SA 连接间加密密钥强度的匹配:

```
set sa-strength-enforcement yes_or_no
```

配置信任点静态 CRL

已吊销证书保留在证书吊销列表 (CRL) 中。客户端应用使用 CRL 检查服务器的身份验证。服务器应用利用 CRL 授予或拒绝来自不再受信任的客户端应用的访问请求。

您可配置 Firepower 4100/9300 机箱以使用证书吊销列表 (CRL) 信息验证对等证书。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅[安全认证合规性，第 45 页](#)。

执行这些步骤以使用 CRL 信息验证对等证书。

过程

步骤 1 从 FXOS CLI 进入安全模式:

```
scope security
```

步骤 2 进入信任点模式:

```
scope trustpoint trustname
```

步骤 3 进入吊销模式:

```
scope revoke
```

步骤 4 下载 CRL 文件:

```
import crl protocol://user_id@CA_or_CRL_issuer_IP/tmp/DoDCA1CRL1.crl
```

步骤 5 (可选) 显示 CRL 信息的导入过程状态:

```
show import-task detail
```

步骤 6 将证书撤销方法设置为仅限于 CRL:

```
set certrevoke method {crl}
```

关于证书撤销吊销列表检查

您可以在 IPSec、HTTPS 和安全 LDAP 连接中将证书吊销列表 (CRL) 检查模式配置为“严格”或“宽松”。

动态（非静态）CRL 信息从 X.509 证书的 CDP 信息中获取，并指示动态 CRL 信息。静态 CRL 信息由系统管理人员手动下载，并指示 FXOS 系统中的本地 CRL 信息。动态 CRL 信息的处理仅特定于证书链中当前正在处理的证书；静态 CRL 信息则应用于整个对等证书链。

有关启用或禁用对安全 IPSec、LDAP 和 HTTPS 连接的证书吊销检查的具体步骤，请参阅[配置 IPSec 安全通道](#)，第 47 页、[创建 LDAP 提供程序](#)，第 108 页和[配置 HTTPS](#)，第 102 页。



注释

- 如果“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“严格 (Strict)”，则仅当对等证书链具有级别 1 或更高级别时，静态 CRL 才适用。（例如，当对等证书链仅包含根 CA 证书和根 CA 证书签名的对等证书时。）
- 为 IPSec 配置静态 CRL 时，导入的 CRL 文件中必须具有“授权密钥标识符 (authkey) (Authority Key Identifier [authkey])”字段。否则，IPSec 会将其视为无效。
- 静态 CRL 优先于来自同一颁发者的动态 CRL。验证对等证书时，如果存在同一颁发者的有效（已确定）静态 CRL，则对等证书中的 CDP 会被忽略。
- 默认在以下场景中启用严格 CRL 检查：
 - 新创建的安全 LDAP 提供程序连接、IPSec 连接或客户端证书条目
 - 新部署的 FXOS 机箱管理器（使用 FXOS 2.3.1.x 或更高版本的初始启动版本部署）

下表说明了连接结果，具体取决于证书吊销列表检查设置和证书验证。

表 1: 无本地静态 CRL 时将“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“严格 (Strict)”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	需要完整的证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链	需要完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
某个 CDP 缺少对等证书链	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
某个 CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接失败，系统显示系统日志消息
无法下载对等证书链中的任何 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，但 CDP 服务器已关闭	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
证书具有 CDP，服务器已启动且 CRL 在 CDP 上具有 CRL，但 CRL 具有无效签名	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息

表 2: 具有本地静态 CRL 时将“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“严格 (Strict)”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	需要完整的证书链	需要完整的证书链
检查对等证书链中的 CDP	需要完整的证书链	需要完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
一个 CDP 缺少对等证书链（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功

具有本地静态 CRL	LDAP 连接	IPSec 连接
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有 CDP，连接会失败并生成系统日志消息

表 3: 无本地静态 CRL 时将“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“释放 (Relaxed)”

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
检查对等证书链	完整的证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链	完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用	是
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
某个 CDP 缺少对等证书链	连接成功	连接成功	连接失败，系统显示系统日志消息
某个 CDP CRL 在具有有效签名的对等证书链中为空	连接成功	连接成功	连接成功
无法下载对等证书链中的任何 CDP	连接成功	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭	连接成功	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名	连接成功	连接成功	连接成功

表 4. 具有本地静态 CRL 时将“证书撤销检查模式 (Certificate Revocation Check Mode)”设置为“释放 (Relaxed)”

具有本地静态 CRL	LDAP 连接	IPSec 连接
检查对等证书链	完整的证书链	完整的证书链
检查对等证书链中的 CDP	完整的证书链	完整的证书链
针对对等证书链的根 CA 证书执行 CDP 检查	是	不适用
对等证书链中的任何证书验证失败	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
在对等证书链中撤销了任何证书	连接失败，系统显示系统日志消息	连接失败，系统显示系统日志消息
一个 CDP 缺少对等证书链（证书链级别为 1）	连接成功	连接成功
对等证书链中的一个 CDP CRL 为空（证书链级别为 1）	连接成功	连接成功
无法下载对等证书链中的任何 CDP（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，但 CDP 服务器已关闭（证书链级别为 1）	连接成功	连接成功
证书具有 CDP，服务器已启动且 CRL 在 CDP 上，但 CRL 具有无效签名（证书链级别为 1）	连接成功	连接成功
对等证书链级别高于 1	连接失败，系统显示系统日志消息	如果与 CDP 结合，连接会成功 如果没有 CDP，连接会失败并生成系统日志消息

配置 CRL 定期下载

您可将系统配置为定期下载 (CRL)，以便每隔 1 至 24 小时使用新的 CRL 验证证书。

您可将以下协议和接口用于该功能：

- FTP
- SCP
- SFTP

- TFTP
- USB



注释

- 不支持 SCEP 和 OCSP。
- 每个 CRL 仅可配置一个定期下载。
- 每个信任点支持一个 CRL。



注释

您仅可以一小时为间隔配置周期。您只能以一小时为间隔配置周期。

执行以下步骤，以配置 CRL 定期下载。

开始之前

确保您已配置 Firepower 4100/9300 机箱以使用 (CRL) 信息验证对等证书。有关详细信息，请参阅[配置信任点静态 CRL](#)，第 52 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

```
scope security
```

步骤 2 进入信任点模式：

```
scope trustpoint
```

步骤 3 进入吊销模式：

```
scope revoke
```

步骤 4 编辑吊销配置：

```
sh config
```

步骤 5 设置首选配置：

示例：

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
```

```
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

步骤 6 退出配置文件:

```
exit
```

步骤 7 (可选) 通过下载新 CRL 测试新配置:

示例:

```
Firepower-chassis /security/trustpoint/ revoke # sh import-task

Import task:
File Name Protocol Server      Port  Userid  State
-----
rootCA.crl Scp      182.23.33.113  0     myname  Downloading
```

设置 LDAP 密钥环证书

您可配置安全的 LDAP 客户端密钥环证书，以便在支持 Firepower 4100/9300 机箱上的支持 TLS 连接。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅[安全认证合规性，第 45 页](#)。



注释 如果启用“通用标准 (Common Criteria)”模式，则必须启用 SSL，且必须使用服务器 DNS 信息创建密钥环证书。

如果为 LDAP 服务器条目启用 SSL，则系统会在建立连接时引用和检查密钥环信息。

LDAP 服务器信息必须是 CC 模式下用于安全 LDAP 连接（启用 SSL）的 DNS 信息。

执行以下步骤，以配置安全的 LDAP 客户端密钥环证书:

过程

步骤 1 从 FXOS CLI 进入安全模式:

```
scope security
```

步骤 2 进入 LDAP 模式:

```
scope ldap
```

步骤 3 进入 LDAP 服务器模式:

```
enter server {server_ip|server_dns}
```

步骤 4 设置 LDAP 密钥环:

```
set keyring keyring_name
```

步骤 5 提交配置：

```
commit-buffer
```

启用客户端证书身份验证

您可使系统将客户端证书与 LDAP 结合使用，对 HTTPS 访问用户进行身份验证。Firepower 4100/9300 机箱上的默认身份验证配置基于凭据。



注释 启用证书身份验证后，这是允许用于 HTTPS 的唯一一种身份验证形式。

客户端证书身份验证功能的 FXOS 2.1.1 版本不支持证书吊销检查。

客户端证书必须满足以下要求，才能使用此功能：

- 用户名必须包含在 X509 属性“证书持有者备用名称 - 邮件 (Subject Alternative Name - Email)”中。
- 客户端证书必须由已将其证书导入到管理引擎上的信任点的根 CA 进行签名。客户端证书必须由已将其证书导入到管理引擎上的信任点的根 CA 签名。

过程

步骤 1 从 FXOS CLI 进入服务模式：

```
scope system
```

```
scope services
```

步骤 2 （可选）查看 HTTPS 身份验证选项：

```
set https auth-type
```

示例：

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

步骤 3 将 HTTPS 身份验证设为基于客户端：

```
set https auth-type cert-auth
```

步骤 4 提交配置：

commit-buffer



第 7 章

系统管理

- [导致 Firepower 机箱管理器会话关闭的系统更改](#)，第 61 页
- [更改管理 IP 地址](#)，第 62 页
- [更改应用管理 IP](#)，第 63 页
- [更改 Firepower 4100/9300 机箱名称](#)，第 66 页
- [登录前横幅](#)，第 67 页
- [重新启动 Firepower 4100/9300 机箱](#)，第 70 页
- [关闭 Firepower 4100/9300 机箱电源](#)，第 70 页
- [恢复出厂默认配置](#)，第 70 页
- [安装受信任身份证书](#)，第 71 页

导致 Firepower 机箱管理器会话关闭的系统更改

以下系统更改可能会导致您自动从 Firepower 机箱管理器系统中注销：

- 对系统时间的改动超过 10 分钟
- 使用 Firepower 机箱管理器或 FXOS CLI 重新启动或关闭系统
- 在 Firepower 4100/9300 机箱上升级 FXOS 版本
- 启用或禁用 FIPS 或通用标准模式



注释

除上述更改外，如果在特定时间段内没有任何活动，您也会自动从系统中注销。默认情况下，此自动注销超时时间为 10 分钟。要配置此超时设置，请参阅[配置会话超时](#)，第 29 页。另外，您还可以配置一个绝对超时设置，使系统在经过特定时间后强制注销登录用户（即使用户会话处于活动状态）。要配置绝对超时设置，请参阅[配置绝对会话超时](#)，第 30 页。

更改管理 IP 地址

开始之前

您可以从 FXOS CLI 更改 Firepower 4100/9300 机箱上的管理 IP 地址。



注释 更改管理 IP 地址后，您需要使用新地址重新建立到 Firepower 机箱管理器或 FXOS CLI 的任何连接。

过程

步骤 1 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)，第 9 页）。

步骤 2 要配置 IPv4 管理 IP 地址，请执行以下操作：

- a) 设置交换矩阵互联 a 的范围：

```
Firepower-chassis# scope fabric-interconnect a
```

- b) 要查看当前管理 IP 地址，请输入以下命令：

```
Firepower-chassis /fabric-interconnect # show
```

- c) 输入以下命令，配置新的管理 IP 地址和网关：

```
Firepower-chassis /fabric-interconnect # set out-of-band ip ip_address netmask network_mask gw gateway_ip_address
```

- d) 将任务提交到系统配置：

```
Firepower-chassis /fabric-interconnect* # commit-buffer
```

步骤 3 要配置 IPv6 管理 IP 地址，请执行以下操作：

- a) 设置交换矩阵互联 a 的范围：

```
Firepower-chassis# scope fabric-interconnect a
```

- b) 设置管理 IPv6 配置的范围：

```
Firepower-chassis /fabric-interconnect # scope ipv6-config
```

- c) 要查看当前管理 IPv6 地址，请输入以下命令：

```
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if
```

- d) 输入以下命令，配置新的管理 IP 地址和网关：

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 ipv6_address ipv6-prefix prefix_length ipv6-gw gateway_address
```

- e) 将任务提交到系统配置：

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
```

示例

以下示例配置 IPv4 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
  ID   OOB IP Addr   OOB Gateway   OOB Netmask   OOB IPv6 Address OOB IPv6 Gateway
  Prefix Operability
  -----
  A    192.0.2.112   192.0.2.1     255.255.255.0  ::              ::
  64   Operable
Firepower-chassis /fabric-interconnect # set out-of-band ip 192.0.2.111 netmask 255.255.255.0
gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

以下示例配置 IPv6 管理接口和网关：

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
  IPv6 Address           Prefix   IPv6 Gateway
  -----
  2001::8998             64      2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band ipv6 2001::8999
ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

更改应用管理 IP

您可以从 FXOS CLI 更改连接到 Firepower 4100/9300 机箱的应用上的管理 IP 地址。为此，您必须首先在 FXOS 平台级别更改 IP 信息，然后在应用级别更改 IP 信息。



注释

尝试使用 Firepower 机箱管理器进行更改可能导致服务中断。为了避免任何可能的服务中断，您必须使用 FXOS CLI 执行这些更改。

过程

步骤 1 连接到 FXOS CLI。（请参阅[访问 FXOS CLI](#)，第 9 页）。

步骤 2 将范围设置为逻辑设备：

scope ssa

scope logical-device *logical_device_name*

步骤 3 将范围设置为管理引导程序，并配置新的管理引导程序参数。请注意，配置之间存在差异：

对于 ASA 逻辑设备的独立配置：

a) 输入逻辑设备管理引导程序：

scope mgmt-bootstrap *asa*

b) 输入插槽的 IP 模式：

scope ipv4_or_6 slot_number default

c) （仅限 IPv4）设置新的 IP 地址：

set ip *ipv4_address* **mask** *network_mask*

d) （仅限 IPv6）设置新的 IP 地址：

set ip *ipv6_address* **prefix-length** *prefix_length_number*

e) 设置网关地址：

set gateway *gateway_ip_address*

f) 提交配置：

commit-buffer

对于 ASA 逻辑设备的集群配置：

a) 输入集群管理引导程序：

scope cluster-bootstrap *asa*

b) （仅限 IPv4）设置新的虚拟 IP：

set virtual ipv4 *ip_address* **mask** *network_mask*

c) （仅限 IPv6）设置新的虚拟 IP：

set virtual ipv6 *ipv6_address* **prefix-length** *prefix_length_number*

d) 设置新的 IP 池：

set ip pool *start_ip* *end_ip*

e) 设置网关地址：

set gateway *gateway_ip_address*

f) 提交配置：

commit-buffer

对于 Firepower 威胁防御的独立和集群配置：

- a) 输入逻辑设备管理引导程序：

```
scope mgmt-bootstrap ftd
```

- b) 输入插槽的 IP 模式：

```
scope ipv4_or_6 slot_number firepower
```

- c) （仅限 IPv4）设置新的 IP 地址：

```
set ip ipv4_address mask network_mask
```

- d) （仅限 IPv6）设置新的 IP 地址：

```
set ip ipv6_address prefix-length prefix_length_number
```

- e) 设置网关地址：

```
set gateway gateway_ip_address
```

- f) 提交配置：

```
commit-buffer
```

注释 对于集群配置，您必须为连接到 Firepower 4100/9300 机箱的每个应用设置新的 IP 地址。如果您有机箱间集群或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

步骤 4 为每个应用清除管理引导程序信息：

- a) 将范围设置为 ssa 模式：

```
scope ssa
```

- b) 将范围设置为插槽：

```
scope slot slot_number
```

- c) 将范围设置为应用实例：

```
scope app-instance asa_or_ftd
```

- d) 清除管理引导程序信息：

```
clear mgmt-bootstrap
```

- e) 提交配置：

```
commit-buffer
```

步骤 5 禁用应用：

```
disable
```

```
commit-buffer
```

注释 对于集群配置，您必须清除并禁用连接到 Firepower 4100/9300 机箱的每个应用的管理引导程序信息。如果您有机箱间集群或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

步骤 6 当应用离线且插槽恢复在线时，重新启用应用。

a) 将范围重置为 ssa 模式：

scope ssa

b) 将范围设置为插槽：

scope slot slot_number

c) 将范围设置为应用实例：

scope app-instance asa_or_fid

d) 启用应用：

enable

e) 提交配置：

commit-buffer

注释 对于集群配置，您必须重复执行这些步骤以重新启用连接到 Firepower 4100/9300 机箱的每个应用。如果您有机箱间集群或 HA 配置，则必须对两个机箱上的每个应用重复这些步骤。

更改 Firepower 4100/9300 机箱名称

您可以在 FXOS CLI 中更改用于 Firepower 4100/9300 机箱的名称。

过程

步骤 1 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)，第 9 页）。

步骤 2 进入系统模式：

Firepower-chassis-A# **scope system**

步骤 3 查看当前名称：

Firepower-chassis-A /system # **show**

步骤 4 配置新名称：

Firepower-chassis-A /system # **set name device_name**

步骤 5 将任务提交到系统配置：

```
Firepower-chassis-A /fabric-interconnect* # commit-buffer
```

示例

以下示例将更改设备名称：

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
  Name           Mode           System IP Address System IPv6 Address
  -----
  New-name      Stand Alone  192.168.100.10   ::
New-name-A /system #
```

登录前横幅

如果配置了登录前横幅，当用户登录到 Firepower 机箱管理器时，系统将显示横幅文本，用户必须在消息屏幕上点击**确定**，然后系统才会提示输入用户名和密码。如果未配置登录前横幅，系统会直接进入用户名和密码输入提示屏幕。

当用户登录到 FXOS CLI 时，系统显示横幅文本（如已配置），然后提示输入密码。

创建登录前横幅

过程

步骤 1 连接到 FXOS CLI（请参阅[访问 FXOS CLI，第 9 页](#)）。

步骤 2 进入安全模式：

```
Firepower-chassis# scope security
```

步骤 3 进入横幅安全模式：

```
Firepower-chassis /security # scope banner
```

步骤 4 输入以下命令创建登录前横幅：

```
Firepower-chassis /security/banner # create pre-login-banner
```

步骤 5 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 应向用户显示的消息：

```
Firepower-chassis /security/banner/pre-login-banner* # set message
```

启动一个对话框，用于输入登录前横幅消息文本。

步骤 6 在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。

在您输入信息的下一行，键入 **ENDOFBUF** 并按 **Enter** 键以完成操作。

按 **Ctrl** 和 **C** 键取消设置消息对话框。

步骤 7 将任务提交到系统配置：

```
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
```

示例

以下示例创建登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

修改登录前横幅

过程

步骤 1 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)，第 9 页）。

步骤 2 进入安全模式：

```
Firepower-chassis# scope security
```

步骤 3 进入横幅安全模式：

```
Firepower-chassis /security # scope banner
```

步骤 4 进入登录前横幅安全模式：

```
Firepower-chassis /security/banner # scope pre-login-banner
```

步骤 5 指定在用户登录 Firepower 机箱管理器或 FXOS CLI 前 FXOS 应向用户显示的消息：

```
Firepower-chassis /security/banner/pre-login-banner # set message
```

启动一个对话框，用于输入登录前横幅消息文本。

步骤 6 在提示符处，键入登录前横幅消息。您可以在此字段中输入任何标准 ASCII 字符。您可以输入多行文本，每行最多 192 个字符。按 **Enter** 键换行。

在您输入信息的下一行，键入 **ENDOFBUF** 并按 **Enter** 键以完成操作。

按 **Ctrl** 和 **C** 键取消设置消息对话框。

步骤 7 将任务提交到系统配置：

```
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
```

示例

以下示例修改登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

删除登录前横幅

过程

步骤 1 连接到 FXOS CLI（请参阅[访问 FXOS CLI](#)，第 9 页）。

步骤 2 进入安全模式：

```
Firepower-chassis# scope security
```

步骤 3 进入横幅安全模式：

```
Firepower-chassis /security # scope banner
```

步骤 4 从系统中删除登录前横幅：

```
Firepower-chassis /security/banner # delete pre-login-banner
```

步骤 5 将任务提交到系统配置：

```
Firepower-chassis /security/banner* # commit-buffer
```

示例

以下示例删除登录前横幅：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

重新启动 Firepower 4100/9300 机箱

过程

-
- 步骤 1** 选择概览 (Overview) 打开“概览 (Overview)”页面。
 - 步骤 2** 点击“概览 (Overview)”页面右上角“机箱运行时间 (Chassis Uptime)”旁边的**重新启动 (Reboot)**。
 - 步骤 3** 点击**是 (Yes)**确认您要关闭 Firepower 4100/9300 机箱。
系统将正常关闭系统上配置的任何逻辑设备，然后关闭每个安全模块/引擎，最后关闭并重新启动 Firepower 4100/9300 机箱。此过程大约需要 15-20 分钟。
-

关闭 Firepower 4100/9300 机箱电源

过程

-
- 步骤 1** 选择概览 (Overview) 打开“概览 (Overview)”页面。
 - 步骤 2** 点击“概览 (Overview)”页面右上角“机箱运行时间 (Chassis Uptime)”旁边的**关闭 (Shutdown)**。
 - 步骤 3** 点击**是**确认您要关闭 Firepower 4100/9300 机箱。
系统将正常关闭系统上配置的任何逻辑设备，然后关闭每个安全模块/引擎，最后关闭 Firepower 4100/9300 机箱。
-

恢复出厂默认配置

您可以使用 FXOS CLI 将您的 Firepower 4100/9300 机箱恢复至出厂默认配置。



注释 此过程将从机箱中清除所有用户配置，包括所有逻辑设备配置。完成此程序后，您需要连接到 Firepower 4100/9300 机箱上的控制台端口，以使用设置向导重新配置系统（请参阅[初始配置](#)，第 6 页）。

过程

步骤 1 （可选） **erase configuration** 命令不会从机箱中删除智能许可证配置。如果您还想要删除智能许可证配置，请执行以下步骤：

scope license

deregister

取消注册 Firepower 4100/9300 机箱会从账户中删除设备。系统会删除设备上的所有许可证授权和证书。

步骤 2 连接到本地管理：

connect local-mgmt

步骤 3 输入以下命令，从您的 Firepower 4100/9300 机箱中清除所有用户配置，并将机箱恢复到其原始出厂默认配置：

erase configuration

系统将提示您确认，是否确定想要清除所有用户配置。

步骤 4 通过在命令提示符后输入 **yes**，确认您想要清除配置。

系统将从您的 Firepower 4100/9300 机箱中清除所有用户配置，然后重启系统。

安装受信任身份证书

在完成初始配置后，系统将生成自签名 SSL 证书以供 Firepower 4100/9300 机箱 Web 应用使用。由于该证书是自签名证书，客户端浏览器不会自动信任它。新的客户端浏览器首次访问 Firepower 4100/9300 机箱 Web 界面时，浏览器会抛出 SSL 警告，要求用户在访问 Firepower 4100/9300 机箱之前接受证书。您可以使用以下程序，使用 FXOS CLI 生成证书签名请求 (CSR)，并安装得到的身份证书以供 Firepower 4100/9300 机箱使用。此身份证书允许客户端浏览器信任连接，并直接启动 Web 界面而无警告。

过程

步骤 1 连接到 FXOS CLI。（请参阅[访问 FXOS CLI](#)，第 9 页）。

步骤 2 输入安全模块：

scope security

步骤 3 创建密钥环:

```
create keyring keyring_name
```

步骤 4 设置私钥的模数大小:

```
set modulus size
```

步骤 5 提交配置:

```
commit-buffer
```

步骤 6 配置 CSR 字段。可以使用基本选项（例如，主题名称）生成证书，也可以选择允许将信息（例如，区域和组织）嵌入证书的更高级选项。请注意，在您配置 CSR 字段时，系统会提示输入证书密码。

```
create certreq certreq subject_name
```

```
password
```

```
set country country
```

```
set state state
```

```
set locality locality
```

```
set org-name organization_name
```

```
set org-unit-name organization_unit_name
```

```
set subject-name subject_name
```

步骤 7 提交配置:

```
commit-buffer
```

步骤 8 导出 CSR，将其提供给您的证书颁发机构。证书颁发机构使用 CSR 来创建您的身份证书。

a) 显示完整 CSR:

```
show certreq
```

b) 复制从（并包含）“-----BEGIN CERTIFICATE REQUEST-----”到（并包含）“-----END CERTIFICATE REQUEST-----”的输出:

示例:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbgG1mb3JuaWEw
ETAPBgNVBACMCFNhbiBKb3N1MRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
VQQLDANUQUxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxyY2F5MIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUgk/EyrVq3B+u2DsopVq76mTm8BwYmGhbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIZoavU6d1tB9rnyxgGth5dPV0dhQIDAQABOC8wLQYJ
KoZIHvcNAQkOMSAwHjAcBgNVHREEFtAtghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAAZUfCbwx9vt5aVdCL+tATu5xFE3LA310ck6Gj1Nv6W/6r
jBNLxusYilrZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ10Ikyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLflG1dxWf1xAxLzF5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
```



```
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXyDjEXp7rCx9
+6bvD1ln70JCegHdCWtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

步骤 9 退出证书请求模式：

```
exit
```

步骤 10 退出密钥环模式：

```
exit
```

步骤 11 根据证书颁发机构的注册流程，向证书颁发机构提供 CSR 输出。如果请求成功，证书颁发机构将发回一份已使用 CA 的私钥进行数字签名的身份证书。

步骤 12 注释 所有身份证书必须采用 Base64 格式才能导入到 FXOS。如果从证书颁发机构接收到的身份证书链采用的是其他格式，您必须先使用 SSL 工具（例如，OpenSSL）进行转换。

创建新的信任点以保存身份证书链。

```
create trustpoint trustpoint_name
```

步骤 13 按照屏幕上的说明，输入您在第 11 步中从证书颁发机构接收到的身份证书链。

注释 对于使用中间证书的证书颁发机构，必须对根证书和中间证书进行组合。在文本文件中，将根证书粘贴在顶部，然后是链中的每一个中间证书，包括所有 BEGIN CERTIFICATE 和 END CERTIFICATE 标记。将整个文本块复制并粘贴到信任点。

```
set certchain
```

示例：

```
firepower /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDTCcAbOgAwIBAgIQYIutxPDfW6BOP3uKNgJHZDAKBggqhkJOPQDAjBTMRUw
>EwYKZImiZPyLQBGryFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMjUwNzI4MTc1NjU2
>WhcNMjUwNzI4MTgwNjU2WjBTMRUwEwYKZImiZPyLQBGryFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkJOPQIBBggqhkJOPQMBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUKmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIkoZiZj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYh1sv1gCxsQVOW0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

步骤 14 提交配置：

```
commit-buffer
```

步骤 15 退出信任点模式：

```
exit
```

步骤 16 进入密钥环模式:

```
scope keyring keyring_name
```

步骤 17 将在第 13 步中创建的信任点与为 CSR 创建的密钥环关联:

```
set trustpoint trustpoint_name
```

步骤 18 导入服务器的签名身份证书。

```
set cert
```

步骤 19 粘贴证书颁发机构提供的身份证书的内容:

示例:

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIe8DCCBjAgAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQDAjBT
>MRUwEwYKcZImiZPyLGQBGRYFbG9jYWwxGDAWBoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHcNMTYwNDI4MTMw
>OTU0WhcNMTgWNDI4MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBGGA1UEAxMRZnAOMTIwLnRlc3QubG9jYjYwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+Lg1UQA0b7tga
>BwdudS3sulXIwKGco48mMHCRCw1ADWZCxFANxsnbfb+wR8xKfKo4vvnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNyTzzIS9XAFs1MSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujob0hNsSvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2H109XR2FAGMB
>AAGjggJYMICVDacBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/lWpstiEYExs8D1ZWcuHzwPt5QwHwYDVR0jBBgwFoAUyInbDHPfFwEEBcbx
>GSgQW7pOVikwgdwGA1UdHwSB1DCB0TCBzqCBY6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0E0sQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmXpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYjYw/Y2VydGlmawNhdGVsZXZvY2F0aW9uTG1z
>dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBGgrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE1OLVBDLUNBLENOPUFJQSxDTj1QdWJsaW1mJmJmJmJmJmJmJmJmJmJmJmJm
>Tj1TZXJ2aW1mJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJmJm
>P2NBQ2VydGlmawNhdGU/YmFzZT9vYmplY3RDbGFzZj1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQGbjUAgQUUhIAVwB1AGIAUwB1AHIAAdgB1AHIAIdgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQOMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtfRvxyjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

步骤 20 退出密钥环模式:

```
exit
```

步骤 21 退出安全模式:

```
exit
```

步骤 22 进入系统模式:

```
scope system
```

步骤 23 进入服务模式:

```
scope services
```

步骤 24 配置 FXOS Web 服务以使用新证书:

```
set https keyring keyring_name
```

步骤 25 提交配置:

```
commit-buffer
```

步骤 26 显示与 HTTPS 服务器关联的密钥环。它应显示在本程序的第 3 步中创建的密钥环名称。如果屏幕输出显示默认的密钥环名称, 则 HTTPS 服务器尚未更新, 不能使用新证书:

```
show https
```

示例:

```
fp4120 /system/services # show https
Name: https
  Admin State: Enabled
  Port: 443
  Operational port: 443
  Key Ring: firepower_cert
  Cipher suite mode: Medium Strength
  Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

步骤 27 显示导入的证书的内容, 确认**Certificate Status**值显示为**Valid**:

```
scope security
```

```
show keyring keyring_name detail
```

示例:

```
fp4120 /security # scope security
fp4120 /security # show keyring firepower_cert detail
Keyring firepower_cert:
  RSA key modulus: Mod2048
  Trustpoint CA: firepower_chain
Certificate status: Valid
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number:
    45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:0a
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
  Validity
    Not Before: Apr 28 13:09:54 2016 GMT
    Not After : Apr 28 13:09:54 2018 GMT
  Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
  CN=fp4120.test.local
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
      0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
      a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
      50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
```

```

fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
1d:85
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Alternative Name:
  DNS:fp4120.test.local
X509v3 Subject Key Identifier:
  FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
X509v3 Authority Key Identifier:
  keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
X509v3 CRL Distribution Points:
  Full Name:
    URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
      CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
      DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

Authority Information Access:
  CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
    CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
    DC=local?cACertificate?base?objectClass=certificationAuthority
1.3.6.1.4.1.311.20.2:
  ..W.e.b.S.e.r.v.e.r
X509v3 Key Usage: critical
  Digital Signature, Key Encipherment
X509v3 Extended Key Usage:
  TLS Web Server Authentication
Signature Algorithm: ecdsa-with-SHA256
30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c
-----BEGIN CERTIFICATE-----
MIIe8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkJOPQQDAjBT
MRUwEwYKcZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rr
bjEgMB4GA1UEAxMXbWFnZDh0aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMzQ2F5
aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBGNVBAoTDUNpc2NvIFN5c3Rl
bXN5bWVudDQwOTU0WjB3MQswCQYDVQGEwJVUzETMBEGA1UECBMzQ2F5aWZvcn5p
YTERMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGC048mMHCQRw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVikdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2uflGAA2H109XR2FAGMB
AAGjggJYMIICVDAcBgNVHREEFtATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8D1ZwcuHzwPtU5QwHwYDVR0jBBgwFoAUyInbDHPFrFwEEBcbx
GSgQW7pOVIkwgdwGAlUdHwSB1DCB0TCBzqCBY6CBYIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40aW40
YmXpYyUyMEtleSUyMFN1cnZpY2VzLENOPVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW40aW40REM9bG9jYWw/Y2VydGlmawNhdGV5ZXZvY2F0aW9uTG1z
dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50MIHMBGgrBgEF
BQcBAQBvCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B

```

```
QVVTVE10LVBDLUNBLENOPUFJQSxDtj1QdWJsaWM1MjBLZXk1MjBTZXJ2aWN1cyxD
Tj1TZXJ2aWN1cyxDtj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGhmaWNhdGU/YmFzZT9vYmplY3RDbGFzZcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCsGAQQBgjcUAQQUHhIAVwBLAGIAUwBIAHIAHgBIAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvxyjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
sgoIK60akbjotOTvUdUd9b6K1Uw=
-----END CERTIFICATE-----
```

Zeroized: No

下一步做什么

要验证显示的证书是新的受信任证书，请通过在 Web 浏览器的地址栏输入 `https://<FQDN_or_IP>/` 转至 Firepower 机箱管理器。



注释

浏览器还根据地址栏中的输入验证证书的主题名称。如果证书颁发给完全限定域名，则必须在浏览器中以相应方式访问它。如果通过 IP 地址访问，将引发其他 SSL 错误（公用名无效 [Common Name Invalid]），即使使用的是受信任证书。



第 8 章

平台设置

- 启用 NTP 服务器身份验证，第 79 页
- 设置日期和时间，第 80 页
- 配置 SSH，第 83 页
- 配置 TLS，第 84 页
- 配置 Telnet，第 85 页
- 配置 SNMP，第 86 页
- 配置 HTTPS，第 93 页
- 配置 AAA，第 105 页
- 配置系统日志，第 114 页
- 配置 DNS 服务器，第 117 页
- 启用 FIPS 模式，第 117 页
- 启用通用标准模式，第 118 页
- 配置 IP 访问列表，第 119 页
- 为容器实例接口添加 MAC 池前缀，并查看其 MAC 地址，第 119 页
- 为容器实例添加资源配置文件，第 120 页
- 配置机箱 URL，第 121 页

启用 NTP 服务器身份验证

执行以下步骤以在 Firepower 4100/9300 机箱上启用 NTP 服务器身份验证。



注释

- 启用时，NTP 身份验证功能全局应用于所有已配置的服务器。
- 仅支持使用 SHA1 进行 NTP 服务器身份验证。
- 您需要密钥 ID 和密钥值，才能进行服务器身份验证。密钥 ID 用于告知客户端和服务器在计算消息摘要时要使用哪个密钥值。密钥值是使用 `ntp-keygen` 得出的固定值。

过程

-
- 步骤 1 下载 ntp 4.2.8p8。
 - 步骤 2 **ntpd openssl** 启用时安装 NTP 服务器。
 - 步骤 3 生成 NTP 密钥 ID 和密钥值：
ntp-keygen -M
使用这些生成的密钥执行以下步骤。
 - 步骤 4 以管理员用户身份登录 Firepower 4100/9300 机箱。
 - 步骤 5 选择 **Platform Settings** 以打开“平台设置”页面。
 - 步骤 6 在“设置时间来源”区域，点击 **Use NTP server** 单选按钮。
 - 步骤 7 使用生成的 SHA1 字符串和密钥添加 NTP 服务器。
 - 步骤 8 点击 **Save** 保存 NTP 服务器配置。
 - 步骤 9 选中 **Enable ntp-authentication** 复选框。
 - 步骤 10 点击 **Save**。
-

设置日期和时间

使用 NTP 页面在系统上配置网络时间协议 (NTP)，手动设置日期和时间，或者查看当前系统时间。

NTP 设置在 Firepower 4100/9300 机箱与机箱上安装的任何逻辑设备之间自动同步。



注释 如果您在 Firepower 4100/9300 机箱上部署 Firepower 威胁防御，则必须在 Firepower 4100/9300 机箱上配置 NTP，使智能许可正常工作并确保设备注册的时间戳正确。应对 Firepower 4100/9300 机箱和 Firepower 管理中心使用相同 NTP 服务器。

如果您使用的是 NTP，则可以在 **当前时间 (Current Time)** 选项卡上查看整体同步状态，或者也可以通过 **时间同步 (Time Synchronization)** 选项卡上 **NTP 服务器 (NTP Server)** 表中的“服务器状态 (Server Status)”字段查看每个已配置的 NTP 服务器的同步状态。如果系统无法与特定 NTP 服务器同步，您可以将光标悬停在“服务器状态 (Server Status)”旁边的信息图标上获取更多信息。

查看配置的日期和时间

过程

-
- 步骤 1 选择平台设置 (**Platform Settings**) > **NTP**。
 - 步骤 2 点击当前时间 (**Current Time**) 选项卡。

系统显示设备上配置 的日期、时间和时区。

如果您使用 NTP，您还可以在**当前时间 (Current Time)** 选项卡上查看整体同步状态。您可以通过**时间同步 (Time Synchronization)** 选项卡上的**NTP 服务器 (NTP Server)** 表中的“服务器状态 (Server Status)”字段查看每台已配置的 NTP 服务器的同步状态。如果系统无法与特定 NTP 服务器同步，您可以将光标悬停在“服务器状态 (Server Status)”旁边的信息图标上获取更多信息。

设置时区

过程

- 步骤 1** 选择平台设置 (**Platform Settings**) > **NTP**。
- 步骤 2** 点击**当前时间 (Current Time)** 选项卡。
- 步骤 3** 从**时区 (Time Zone)** 下拉列表中为 Firepower 机箱选择适当的时区。

使用 NTP 设置日期和时间

NTP 用于实施分层服务器系统，可在网络系统中提供精确的同步时间。时间敏感性操作需要这种精确度，例如验证 CRL，其包括精确时间戳。您最多可以配置 4 个 NTP 服务器。



注释 FXOS 2.2(2) 及更高版本使用 NTP 版本 3。

过程

- 步骤 1** 选择平台设置 (**Platform Settings**) > **NTP**。
- 步骤 2** 点击**时间同步 (Time Synchronization)** 选项卡。
- 步骤 3** 在**设置时间来源 (Set Time Source)** 下面，点击**使用 NTP 服务器 (Use NTP Server)**。
- 步骤 4** 对于您要使用的每个 NTP 服务器（最多 4 个），请在**NTP 服务器 (NTP Server)** 字段中输入 NTP 服务器的 IP 地址或主机名，点击**添加 (Add)**。
- 步骤 5** 点击**保存 (Save)**。

使用指定的 NTP 服务器信息配置 Firepower 机箱。

您可以通过**NTP 服务器 (NTP Server)** 表中的“服务器状态 (Server Status)”字段查看每台服务器的同步状态。如果系统无法与特定 NTP 服务器同步，您可以将光标悬停在“服务器状态 (Server Status)”旁边的信息图标上获取更多信息。

注释 如果系统时间修改超过 10 分钟，系统会将您注销，稍后，您需要再次登录 Firepower 机箱管理器。

删除 NTP 服务器

过程

- 步骤 1** 选择平台设置 (Platform Settings) > NTP。
 - 步骤 2** 点击时间同步 (Time Synchronization) 选项卡。
 - 步骤 3** 对于您要删除的每台 NTP 服务器，请在 NTP 服务器 (NTP Server) 表中点击该服务器所对应的删除 (Delete) 图标。
 - 步骤 4** 点击保存 (Save)。
-

手动设置日期和时间

本部分介绍如何在 Firepower 机箱上手动设置日期和时间。

过程

- 步骤 1** 选择平台设置 (Platform Settings) > NTP。
- 步骤 2** 点击时间同步 (Time Synchronization) 选项卡。
- 步骤 3** 在设置时间来源 (Set Time Source) 下面，点击手动设置时间 (Set Time Manually)。
- 步骤 4** 点击日期 (Date) 下拉列表，显示日历，然后使用日历中的可用控件设置日期。
- 步骤 5** 使用对应的下拉列表将时间指定为小时、分钟和 AM/PM。

提示 您可以点击获取系统时间 (Get System Time)，设置日期和时间，以匹配您正在用来连接到 Firepower 机箱管理器的系统上所配置的日期和时间。

- 步骤 6** 点击保存 (Save)。

使用指定的日期和时间配置 Firepower 机箱。

注释 如果系统时间修改超过 10 分钟，系统会将您注销，稍后，您需要再次登录 Firepower 机箱管理器。

配置 SSH

以下程序说明如何启用或禁用对 Firepower 机箱的 SSH 访问，以及如何将 FXOS 机箱作为 SSH 客户端启用。默认情况下，SSH 处于启用状态。

过程

- 步骤 1** 依次选择平台设置 > SSH > SSH 服务器。
- 步骤 2** 要启用到 Firepower 机箱的 SSH 访问，请选中启用 **SSH (Enable SSH)** 复选框。要禁用 SSH 访问，请取消勾选启用 **SSH (Enable SSH)** 复选框。
- 步骤 3** 对于服务器加密算法，请勾选每个允许的加密算法的复选框。
注释 通用标准中不支持 3des-cbc。如果在 FXOS 机箱上启用了通用标准模式，则不能使用 3des-cbc 作为加密算法。
- 步骤 4** 对于服务器密钥交换算法，请勾选每个允许的 Diffie-Hellman (DH) 密钥交换的复选框。DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。
- 步骤 5** 对于服务器 **Mac 算法 (Mac Algorithm)**，请勾选允许的每种完整性算法所对应的复选框。
- 步骤 6** 对于服务器主机密钥，请输入 RSA 密钥对的模块大小。
模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。
- 步骤 7** 对于服务器密钥更新数量限制，请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。
- 步骤 8** 对于服务器密钥更新时间限制，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。
- 步骤 9** 点击保存 (Save)。
- 步骤 10** 点击 **SSH 客户端 (SSH Client)** 选项卡，以自定义 FXOS 机箱 SSH 客户端。
- 步骤 11** 对于严格主机密钥检查，可选择启用、禁用或提示来控制 SSH 主机密钥检查。
 - **启用** - 如果 FXOS 已知的主机文件中未包含主机密钥，连接将被拒绝。您必须在 FXOS CLI 中使用系统/服务范围的 **enter ssh-host** 命令手动添加主机。
 - **提示** - 对于机箱中未存储的主机密钥，系统会提示您接受或拒绝该主机密钥。
 - **禁用** - （默认）机箱将自动接受以前未存储的主机密钥。
- 步骤 12** 对于客户端加密算法，请勾选每个允许的加密算法的复选框。
注释 通用标准中不支持 3des-cbc。如果在 FXOS 机箱上启用了通用标准模式，则不能使用 3des-cbc 作为加密算法。

- 步骤 13** 对于客户端密钥交换算法，请勾选每个允许的 Diffie-Hellman (DH) 密钥交换的复选框。DH 密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。
- 步骤 14** 对于客户端 **Mac** 算法，请勾选每个允许的完整性算法的复选框。
- 步骤 15** 对于客户端密钥更新数量限制，请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。
- 步骤 16** 对于客户端密钥更新时间限制，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。
- 步骤 17** 点击保存 (Save)。

配置 TLS

传输层安全 (TLS) 协议在两个通信的应用之间确保隐私安全和数据完整性。您可以使用 FXOS CLI 来配置 FXOS 机箱与外部设备通信时允许的最低 TLS 版本。较新的 TLS 版本可提供更安全的通信，而较旧的 TLS 版本则能向后兼容较旧的应用。

例如，如果您的 FXOS 机箱上配置的最低 TLS 版本为 1.1 版，而且客户端浏览器配置为仅运行 1.0 版，那么客户端将无法通过 HTTPS 打开与 FXOS 机箱管理器的连接。因此，必须适当地配置对等应用和 LDAP 服务器。

以下程序显示了如何配置和查看 FXOS 机箱与外部设备之间的通信所允许的最低 TLS 版本。



注释

- 截至 FXOS 2.3(1) 版本，FXOS 机箱的默认最低 TLS 版本为 v1.1。

过程

步骤 1 进入系统模式：

```
Firepower-chassis# scope system
```

步骤 2 查看您的系统中可用的 TLS 版本选项：

```
Firepower-chassis /system # set services tls-ver
```

示例：

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver
    v1_0  v1.0
    v1_1  v1.1
    v1_2  v1.2
```

步骤 3 设置最低 TLS 版本：

```
Firepower-chassis /system # set services tls-ver version
```

示例:

```
Firepower-chassis /system #
Firepower-chassis /system # set services tls-ver v1_2
```

步骤 4 提交配置:

```
Firepower-chassis /system # commit-buffer
```

步骤 5 显示在您的系统上配置的最低 TLS 版本:

```
Firepower-chassis /system # scope services
```

```
Firepower-chassis /system/services # show
```

示例:

```
Firepower-chassis /system/services # show
Name: ssh
  Admin State: Enabled
  Port: 22
  Kex Algo: Diffie Hellman Group1 Sha1,Diffie Hellman Group14 Sha1
  Mac Algo: Hmac Sha1,Hmac Sha1 96,Hmac Sha2 512,Hmac Sha2 256
  Encrypt Algo: 3des Cbc,Aes256 Cbc,Aes128 Cbc,Aes192 Cbc,Aes256 Ctr,Aes128 Ctr,Aes192 Ctr
  Auth Algo: Rsa
    Host Key Size: 2048
  Volume: None Time: None
Name: telnet
  Admin State: Disabled
  Port: 23
Name: https
  Admin State: Enabled
  Port: 443
  Operational port: 443
  Key Ring: default
  Cipher suite mode: Medium Strength
  Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
  Https authentication type: Cert Auth
  Crl mode: Relaxed
TLS:
  TLS version: v1.2
```

配置 Telnet

以下程序介绍如何启用或禁用对 Firepower 机箱的 Telnet 访问。默认情况下，Telnet 处于禁用状态。



注释

目前，Telnet 配置只有在使用 CLI 时才可使用。

过程

步骤 1 进入系统模式：

```
Firepower-chassis # scope system
```

步骤 2 进入系统服务模式：

```
Firepower-chassis /system # scope services
```

步骤 3 要配置对 Firepower 机箱的 Telnet 访问，请执行以下操作之一：

- 要允许对 Firepower 机箱进行 Telnet 访问，请输入以下命令：

```
Firepower-chassis /system/services # enable telnet-server
```

- 要禁止对 Firepower 机箱进行 Telnet 访问，请输入以下命令：

```
Firepower-chassis /system/services # disable telnet-server
```

步骤 4 将任务提交到系统配置：

```
Firepower /system/services # commit-buffer
```

示例

以下示例启用 Telnet 并且提交任务：

```
Firepower-chassis# scope system  
Firepower-chassis /system # scope services  
Firepower-chassis /services # enable telnet-server  
Firepower-chassis /services* # commit-buffer  
Firepower-chassis /services #
```

配置 SNMP

使用 SNMP 页面，在 Firepower 机箱上配置简单网络管理协议 (SNMP)。有关详细信息，请参阅以下主题：

关于 SNMP

简单网络管理协议 (SNMP) 是一个应用层协议，用于为 SNMP 管理器和代理之间的通信提供消息格式。SNMP 提供用于监控和管理网络中的设备的标准化框架和通用语言。

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来控制 and 监控网络设备的活动的系统。

- SNMP 代理 - Firepower 机箱内的软件组件，用于维护 Firepower 机箱的数据并根据需要向 SNMP 管理器报告数据。Firepower 机箱包含代理和 MIB 集合。要启用 SNMP 代理并创建管理器和代理之间的关系，请在 Firepower 机箱管理器或 FXOS CLI 中启用并配置 SNMP。
- 管理信息库 (MIB) - SNMP 代理上的受管对象集合。

Firepower 机箱支持 SNMPv1、SNMPv2c 和 SNMPv3。SNMPv1 和 SNMPv2c 都使用基于社区形式的安全性。有关 SNMP 的定义，请参阅以下标准：

- RFC 3410 (<http://tools.ietf.org/html/rfc3410>)
- RFC 3411 (<http://tools.ietf.org/html/rfc3411>)
- RFC 3412 (<http://tools.ietf.org/html/rfc3412>)
- RFC 3413 (<http://tools.ietf.org/html/rfc3413>)
- RFC 3414 (<http://tools.ietf.org/html/rfc3414>)
- RFC 3415 (<http://tools.ietf.org/html/rfc3415>)
- RFC 3416 (<http://tools.ietf.org/html/rfc3416>)
- RFC 3417 (<http://tools.ietf.org/html/rfc3417>)
- RFC 3418 (<http://tools.ietf.org/html/rfc3418>)
- RFC 3584 (<http://tools.ietf.org/html/rfc3584>)

SNMP 通知

SNMP 的一个关键功能是可以生成来自 SNMP 代理的通知。这些通知不要求从 SNMP 管理器发送请求。通知可以指示不恰当的用户验证、重新启动、连接断开、到相邻路由器的连接丢失或其他重要事件。

Firepower 机箱将 SNMP 通知生成陷阱或通知。陷阱不如通知可靠，因为 SNMP 管理器在收到陷阱时不发送任何确认，并且 Firepower 机箱无法确定是否已收到陷阱。收到通告请求的 SNMP 管理器使用一个 SNMP 响应协议数据单元 (PDU) 来确认消息。如果 Firepower 机箱不接收 PDU，则其可以再次发送通知请求。

SNMP 安全级别和权限

SNMPv1、SNMPv2c 和 SNMPv3 分别表示不同的安全模型。安全模型与所选安全级别结合来确定处理 SNMP 消息时应用的安全机制。

安全级别确定查看与 SNMP 陷阱关联的消息时所需的权限。权限级别确定是否需要防范消息泄露或免受身份验证。受支持的安全级别取决于实施的安全模式。SNMP 安全级别支持以下一个或多个权限：

- noAuthNoPriv - 无身份验证或加密

- authNoPriv - 身份验证，但无加密
- authPriv - 身份验证和加密

SNMPv3 同时提供了安全模型和安全级别。安全模型是为用户和用户所处的角色设置的身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别相结合来确定在处理 SNMP 数据包时采用的安全机制。

支持的 SNMP 安全模型和级别组合

下表确定安全模型和级别的组合含义。

表 5: SNMP 安全模型和级别

型号	级别	身份验证	加密	状况
v1	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。
v2c	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。
V3	noAuthNoPriv	用户名	否	使用用户名匹配进行身份验证。
V3	authNoPriv	HMAC-SHA	否	提供基于 HMAC 安全散列算法 (SHA) 的身份验证。
V3	authPriv	HMAC-SHA	DES	提供基于 HMAC-SHA 算法的身份验证。除基于密码块链 (CBC) DES (DES-56) 标准的身份验证外，还提供数据加密标准 (DES) 56 位加密。

SNMPv3 安全功能

SNMPv3 通过将在网络上对帧进行身份验证和加密相结合来提供对设备的安全接入。SNMPv3 仅按已配置的用户来授权管理操作，并会加密 SNMP 消息。SNMPv3 基于用户的安全模型 (USM) 是指 SNMP 消息级别安全，并提供以下服务：

- 消息完整性 - 确保消息未在未经授权的情况下进行修改或销毁，并且数据序列未修改至超出可以非恶意形式出现的程度。
- 消息来源身份验证 - 确保对用户（系统代表该用户发出此已接收数据）的声明身份进行确认。
- 消息机密性和加密 - 确保不向未经授权的个人、实体或流程提供或披露信息。

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

针对 MIB 的支持

Firepower 机箱支持对 MIB 的只读访问。

有关可用的特定 MIB 和在何处获取这些 MIB 的信息，请参阅《思科 FXOS MIB 参考指南》。

适用于 SNMPv3 用户的身份验证协议

Firepower 机箱针对 SNMPv3 用户支持 HMAC-SHA-96 (SHA) 身份验证协议。

适用于 SNMPv3 用户的 AES 隐私协议

Firepower 机箱使用高级加密标准 (AES) 作为用于 SNMPv3 消息加密的隐私协议之一并符合 RFC 3826。

隐私密码或 `priv` 选项提供对 DES 或 128 位 AES 加密的选择，以进行 SNMP 安全加密。如果启用 AES-128 配置并包含 SNMPv3 用户的隐私密码，则 Firepower 机箱使用该隐私密码来生成 128 位 AES 密钥。AES 隐私密码至少可具有八个字符。如果口令用明文指定，您可以指定最多 64 个字符。

启用 SNMP 并配置 SNMP 属性

过程

步骤 1 选择平台设置 (Platform Settings) > SNMP。

步骤 2 在 SNMP 区域中，填写以下字段：

名称	说明
管理状态 (Admin State) 复选框	SNMP 已启用还是已禁用。仅当系统包含与 SNMP 服务器的集成时才启用此服务。
端口字段	Firepower 机箱与 SNMP 主机通信时使用的端口。无法更改默认端口。
社区/用户名 (Community/Username) 字段	<p>在 SNMP v1 和 v2 中用于轮询的社区字符串。</p> <p>请注意，此字段不适用于 SNMP v3。</p> <p>输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @ (at 号)、\ (反斜线)、" (双引号)、? (问号) 或空格。默认值为 public。</p> <p>请注意，如果社区/用户名 (Community/Username) 字段已设置，空字段右侧会显示文本 已设置：是 (Set: Yes)。如果社区/用户名 (Community/Username) 字段尚未填充值，空字段右侧会显示文本 已设置：否 (Set: No)。</p>

名称	说明
系统管理员名称 (System Administrator Name) 字段	负责 SNMP 实施的联系人。 输入一个字符串，最多 255 个字符，例如邮件地址或姓名和电话号码。
位置字段	SNMP 代理（服务器）运行所在的主机的位置。 输入一个字母数字字符串，最多 510 个字符。

步骤 3 点击保存 (Save)。

下一步做什么

创建 SNMP 陷阱和用户。

创建 SNMP 陷阱

过程

步骤 1 选择平台设置 (Platform Settings) > SNMP。

步骤 2 在 SNMP 陷阱 (SNMP Traps) 区域中，点击添加 (Add)。

步骤 3 在添加 SNMP 陷阱 (Add SNMP Trap) 对话框中，填写以下字段：

名称	说明
主机名 (Host Name) 字段	Firepower 机箱应向其发送陷阱的 SNMP 主机的主机名或 IP 地址。
社区/用户名 (Community/Username) 字段	向 SNMP 主机发送陷阱时，Firepower 机箱包含的 SNMP v1 或 v2 社区名或 SNMP v3 用户名。这必须与为 SNMP 服务配置的社区或用户名相同。 输入介于 1 和 32 个字符之间的字母数字字符串。请勿使用 @（at 号）、\（反斜线）、"（双引号）、?（问号）或空格。
端口字段	Firepower 机箱与 SNMP 主机通信以布设陷阱时使用的端口。 输入一个介于 1 和 65535 之间的整数。
版本 字段	用于陷阱的 SNMP 版本和型号。这可以是以下其中一项： <ul style="list-style-type: none"> • V1 • V2 • V3

名称	说明
类型字段	<p>如果为版本选择 V2 或 V3，则是要发送的陷阱类型。这可以是以下其中一项：</p> <ul style="list-style-type: none"> • 陷阱 (Traps) • 告知 (Informs)
v3 权限 (v3 Privilege) 字段	<p>如果为版本选择 V3，与陷阱相关联的权限。这可以是以下其中一项：</p> <ul style="list-style-type: none"> • 身份验证 (Auth) - 有身份验证，但没有加密 • 无身份验证 (Noauth) - 没有身份验证和加密 • 权限 (Priv) - 有身份验证和加密

步骤 4 点击确定 (**OK**)，可关闭添加 SNMP 陷阱 (**Add SNMP Trap**) 对话框。

步骤 5 点击保存 (**Save**)。

删除 SNMP 陷阱

过程

步骤 1 选择平台设置 (**Platform Settings**) > **SNMP**。

步骤 2 在 **SNMP 陷阱 (SNMP Traps)** 区域中，在与您想要删除的陷阱对应的表的行中点击删除 (**Delete**) 图标。

创建 SNMPv3 用户

过程

步骤 1 选择平台设置 (**Platform Settings**) > **SNMP**。

步骤 2 在 **SNMP 用户 (SNMP Users)** 区域中，点击添加 (**Add**)。

步骤 3 在添加 SNMP 用户 (**Add SNMP User**) 对话框中，填写以下字段：

名称	说明
名称 (Name) 字段	分配给 SNMP 用户的用户名。 最多输入32个字符。名称必须以字母开头。有效字符包括字母、数字、_（下划线）、.（句点）、@（邮箱符号）和-（连字符）。
授权类型 (Auth Type) 字段	授权类型： SHA 。
使用 AES-128 (Use AES-128) 复选框	如果选中此复选框，则此用户使用 AES-128 加密。
密码字段	此用户的密码。 Firepower 可扩展操作系统 拒绝任何不满足以下要求的密码： <ul style="list-style-type: none"> • 必须包含最少 8 个字符，最多 80 个字符。 • 必须仅包含字母、数字和以下字符： ~!@#%^&*()_+{}[]\ :;'"<>./ • 不得包含以下符号：\$（美元符号）、?（问号）或=（等号）。 • 必须包含至少 5 个不同的字符。 • 不得包含过多连续递增或递减数字或字母。例如，字符串“12345”包含四个此类字符，字符串“ZYXW”包含三个此类字符。如果此类字符的总数超过某个限值（通常约大于 4 至 6 个字符），则简单性检查将会失败。 注释 在使用的非递增或递减字符数介于两者之间时，系统不会重置连续递增或递减字符计数。例如，abcd&!21 将致使密码检查失败，但abcd&!25 不会。
确认密码 (Confirm Password) 字段	用于再次确认的密码。

名称	说明
隐私密码 (Privacy Password) 字段	<p>此用户的隐私密码。</p> <p>Firepower 可扩展操作系统 拒绝任何不满足以下要求的密码：</p> <ul style="list-style-type: none"> • 必须包含最少 8 个字符，最多 80 个字符。 • 必须仅包含字母、数字和以下字符： ~!@#%^&*()_+{}[]\:"'<>./ • 不得包含以下符号：\$（美元符号）、?（问号）或 =（等号）。 • 必须包含至少 5 个不同的字符。 • 不得包含过多连续递增或递减数字或字母。例如，字符串“12345”包含四个此类字符，字符串“ZYXW”包含三个此类字符。如果此类字符的总数超过某个限值（通常约大于 4 至 6 个字符），则简单性检查将会失败。 <p>注释 在使用的非递增或递减字符数介于两者之间时，系统不会重置连续递增或递减字符计数。例如，abcd&!21 将致使密码检查失败，但 abcd&!25 不会。</p>
确认隐私密码 (Confirm Privacy Password) 字段	用于再次确认的隐私密码。

步骤 4 点击确定 (OK)，可关闭添加 SNMP 用户 (Add SNMP User) 对话框。

步骤 5 点击保存 (Save)。

删除 SNMPv3 用户

过程

步骤 1 选择平台设置 (Platform Settings) > SNMP。

步骤 2 在 SNMP 用户 (SNMP Users) 区域中，在与您想要删除的用户对应的表的行中点击删除 (Delete) 图标。

配置 HTTPS

本节介绍如何在 Firepower 4100/9300 机箱上配置 HTTPS。



注释 您可以使用 Firepower 机箱管理器或 FXOS CLI 更改 HTTPS 端口。所有其他 HTTPS 配置仅可使用 FXOS CLI 完成。

证书、密钥环和受信任点

HTTPS 使用公钥基础设施 (PKI) 的组件在两个设备（例如客户端浏览器和 Firepower 4100/9300 机箱）之间建立安全通信。

加密密钥和密钥环

每个 PKI 设备具有一对非对称 Rivest-Shamir-Adleman (RSA) 加密密钥（其中一个保持为私有，另一个公开），存储在内部密钥环中。用任一密钥加密的消息均可用另一密钥解密。要发送加密消息，发送方使用接收方的公钥加密消息，接收方使用自己的私钥解密消息。发送方也可以通过使用其自有私钥加密（也称为“签名”）已知消息来证明其对公钥的所有权。如果接收方可使用上述公钥成功解密消息，则发送方对相应私钥的所有权得以证明。加密密钥长度可以不同，典型的长度为 512 位至 2048 位。一般来说，密钥长度越长，安全性就越高。FXOS 提供一个默认密钥环，带有 2048 位的初始密钥对，并允许创建更多密钥环。

如果集群名称更改或证书过期，则必须手动重新生成默认密钥环证书。

证书

作为安全通信前的准备，两台设备首先会交换数字证书。证书是包含设备的公钥以及有关设备身份的签名信息的文件。要仅支持加密通信，设备可生成自己的密钥对和自签名证书。远程用户连接至显示自签名证书的设备时，用户无法轻易验证设备身份，且用户浏览器最初会显示身份验证警告。默认情况下，FXOS 包含内置的自签名证书，其中包含来自默认密钥环的公钥。

受信任点

要为 FXOS 提供更强的身份验证，您可从受信任来源或信任点获取并安装确认设备身份的第三方证书。第三方证书由颁发证书的受信任点签署，该受信任点可以是根证书颁发机构 (CA)，也可以是中间 CA 或信任锚（通向根 CA 的信任链一部分）。要获取新证书，您必须通过 FXOS 生成证书请求，并将请求提交至受信任点。



重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

创建密钥环

FXOS 最多支持 8 个密钥环，包括默认密钥环。

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 创建并命名密钥环：

```
Firepower-chassis # create keyring keyring-name
```

步骤 3 设置 SSL 密钥长度（以位为单位）：

```
Firepower-chassis # set modulus {mod1024 | mod1536 | mod2048 | mod512}
```

步骤 4 提交任务：

```
Firepower-chassis # commit-buffer
```

示例

以下示例创建密钥大小为 1024 位的密钥环：

```
Firepower-chassis# scope security  
Firepower-chassis /security # create keyring kr220  
Firepower-chassis /security/keyring* # set modulus mod1024  
Firepower-chassis /security/keyring* # commit-buffer  
Firepower-chassis /security/keyring #
```

下一步做什么

创建该密钥环证书请求。为该密钥环创建证书请求。

重新生成默认密钥环

如果集群名称更改或证书过期，则必须手动重新生成默认密钥环证书。

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 进入默认密钥环的密钥环安全模式：

```
Firepower-chassis /security # scope keyring default
```

步骤 3 重新生成默认密钥环：

```
Firepower-chassis /security/keyring # set regenerate yes
```

步骤 4 提交任务:

```
Firepower-chassis # commit-buffer
```

示例

以下示例重新生成默认密钥环:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

创建密钥环的证书请求

使用基本选项创建密钥环证书请求使用基本选项创建密钥环的证书请求

过程**步骤 1** 进入安全模式:

```
Firepower-chassis # scope security
```

步骤 2 进入密钥环配置模式:

```
Firepower-chassis /security # scope keyring keyring-name
```

步骤 3 使用指定 IPv4 或 IPv6 地址或交换矩阵互联的名称创建证书请求。系统将提示您输入证书请求的密码。

```
Firepower-chassis /security/keyring # create certreq {ip [ipv4-addr | ipv6-v6] | subject-name name}
```

步骤 4 提交任务:

```
Firepower-chassis /security/keyring/certreq # commit-buffer
```

步骤 5 显示您可以复制并发送至信任锚或证书颁发机构的证书请求:

```
Firepower-chassis /security/keyring # show certreq
```

示例

以下示例使用基本选项为密钥环创建并显示具有 IPv4 地址的证书请求:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
```



```

Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKnlt8qMZO4UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtX1WsyLwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNlceCsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWicTWgHhH8BimOb/00KuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXpc5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #

```

下一步做什么

- 复制证书请求文本（包括开始 [BEGIN] 和结束 [END] 行），并将其保存到文件中。将带有证书请求的文件发送至信任锚或证书颁发机构，以获取密钥环证书。
- 创建受信任点并设置从信任锚接收的信任证书的证书链。创建受信任点并为从信任锚接收的信任证书设置证书链。

使用高级选项创建密钥环的证书请求

过程

步骤 1 进入安全模式:

```
Firepower-chassis # scope security
```

步骤 2 进入密钥环配置模式:

```
Firepower-chassis /security # scope keyring keyring-name
```

步骤 3 创建证书请求:

```
Firepower-chassis /security/keyring # create certreq
```

步骤 4 指定公司所在国家/地区的国家/地区代码:

```
Firepower-chassis /security/keyring/certreq* # set country country name
```

步骤 5 指定与请求相关联的域名服务器 (DNS) 地址:

```
Firepower-chassis /security/keyring/certreq* # set dns DNS Name
```

步骤 6 指定与证书请求相关联的邮件地址:

```
Firepower-chassis /security/keyring/certreq* # set e-mail E-mail name
```

步骤 7 指定 Firepower 4100/9300 机箱的 IP 地址:

```
Firepower-chassis /security/keyring/certreq* # set ip {certificate request ip-address|certificate request ip6-address }
```

步骤 8 指定请求此证书的公司总部所在的城市或城镇:

```
Firepower-chassis /security/keyring/certreq* # set locality locality name (eg, city)
```

步骤 9 指定请求证书的组织:

```
Firepower-chassis /security/keyring/certreq* # set org-name organization name
```

步骤 10 指定组织单位:

```
Firepower-chassis /security/keyring/certreq* # set org-unit-name organizational unit name
```

步骤 11 为证书请求指定可选密码:

```
Firepower-chassis /security/keyring/certreq* # set password certificate request password
```

步骤 12 指定请求此证书的公司总部所在的省、市或自治区:

```
Firepower-chassis /security/keyring/certreq* # set state state, province or county
```

步骤 13 指定 Firepower 4100/9300 机箱的完全限定域名:

```
Firepower-chassis /security/keyring/certreq* # set subject-name certificate request name
```

步骤 14 提交任务:

```
Firepower-chassis /security/keyring/certreq # commit-buffer
```

步骤 15 显示您可以复制并发送至信任锚或证书颁发机构的证书请求:

```
Firepower-chassis /security/keyring # show certreq
```

示例

以下示例使用高级选项为密钥环创建并显示具有 IPv4 地址的证书请求:

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* # set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
```

```

Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKnl8qMZO4UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtX1WsyLwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGAl4sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQOMA6CBnNhbWMwNlECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXpC5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring/certreq #

```

下一步做什么

- 复制证书请求文本（包括开始 [BEGIN] 和结束 [END] 行），并将其保存到文件中。将带有证书请求的文件发送至信任锚或证书颁发机构，以获取密钥环证书。
- 创建受信任点并设置从信任锚接收的信任证书的证书链。创建受信任点并为从信任锚接收的信任证书设置证书链。

创建受信任点

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 创建受信任点：

```
Firepower-chassis /security # create trustpoint name
```

步骤 3 为此受信任点指定证书信息：

```
Firepower-chassis /security/trustpoint # set certchain [certchain ]
```

如果不在命令中指定证书信息，系统将提示您输入证书或信任点列表，定义到根证书授权(CA)的证书路径。在您输入信息的下一行，键入 **ENDOFBUF** 以完成操作。

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

步骤 4 提交任务：

```
Firepower-chassis /security/trustpoint # commit-buffer
```

示例

以下示例创建受信点并提供为受信点提供证书：

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBGNVBAsT
> ClRlc3QgR3JvdXAxGTAXBGNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWZHVzZXJAZXhhbXBsZS5jb20wZGZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayV1QjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAGMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl90306Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtlv1WvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3n04MIGeBgNVHSMGgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3n04oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> ClNhbnRhIENsYXhMRswGQYDVQQKEwJ0dW92YSBTeXN0ZW1zIEluYy4xZDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZkN0Q0GCAQAwdAYDVVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wr4pYiO4z42/j9Ijenh75tCKMhW51az8cop1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6idlavt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

下一步做什么

从信任锚或证书颁发机构获取密钥环证书并将其导入密钥环。

将证书导入密钥环

开始之前

- 配置包含密钥环证书的证书链的信任点。
- 从信任锚或证书颁发机构获取密钥环证书。

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 进入将接收证书的密钥环的配置模式：

```
Firepower-chassis /security # scope keyring keyring-name
```

步骤 3 为从其中获取密钥环证书的信任锚或证书颁发机构指定受信点：

```
Firepower-chassis /security/keyring # set trustpoint name
```

步骤 4 启动用于输入和上传密钥环证书的对话框：

```
Firepower-chassis /security/keyring # set cert
```

在提示符后，粘贴从信任锚或证书颁发机构接收到的证书文本。在证书后的下一行，键入 **ENDOFBUF** 完成证书输入。

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

步骤 5 提交任务：

```
Firepower-chassis /security/keyring # commit-buffer
```

示例

以下示例指定信任点并将证书导入密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAQgCAQAwwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJQTEVMBGMA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YcCYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GmbkPayV1Qjbg4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl90306Mg51zqlzXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNldvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

下一步做什么

使用密钥环配置 HTTPS 服务。

配置 HTTPS



注意 完成 HTTPS 配置（包括更改将由 HTTPS 使用的端口和密钥环）后，一旦保存或提交任务，所有当前 HTTP 和 HTTPS 会话都将关闭，而不显示警告。

过程

步骤 1 进入系统模式：

```
Firepower-chassis# scope system
```

步骤 2 进入系统服务模式：

```
Firepower-chassis /system # scope services
```

步骤 3 启用 HTTPS 服务：

```
Firepower-chassis /system/services # enable https
```

步骤 4 （可选）指定要用于 HTTPS 连接的端口：

```
Firepower-chassis /system/services # set https port port-num
```

步骤 5 （可选）指定创建用于 HTTPS 的密钥环名称：

```
Firepower-chassis /system/services # set https keyring keyring-name
```

步骤 6 （可选）指定域使用的 Cipher Suite 安全级别：

```
Firepower-chassis /system/services # set https cipher-suite-mode cipher-suite-mode
```

cipher-suite-mode 可以是以下关键字之一：

- **high-strength**
- **medium-strength**
- **low-strength**
- **custom**- 允许您指定用户定义的 Cipher Suite 规格规范字符串。

步骤 7 （可选）如果将 **cipher-suite-mode** 设为 **custom**，请指定域的 Cipher Suite 安全性自定义级别：

```
Firepower-chassis /system/services # set https cipher-suite cipher-suite-spec-string
```

cipher-suite-spec-string 可以包含最多 256 个字符，并且必须符合 OpenSSL Cipher Suite 规范。不得使用任何空格或特殊字符，！（感叹号）、+（加号）、-（连字符）和:（冒号）除外。有关详细信息，请参阅 http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslcipher-suite。

例如，默认情况下，FXOS 使用的中强度规范字符串为：

```
ALL: !ADH: !EXPORT56: !LOW: RC4+RSA: +HIGH: +MEDIUM: +EXP: +eNULL
```

注释 如果将 **cipher-suite-mode** 设置为除 **custom** 之外的任何其他值，则忽略此选项。

步骤 8 （可选） 启用或禁用证书吊销列表检查：

```
set revoke-policy { relaxed | strict }
```

步骤 9 将任务提交到系统配置：

```
Firepower-chassis /system/services # commit-buffer
```

示例

以下示例启用 HTTPS，将端口号设置为 443，将密钥环名称设为 kring7984，将 Cipher Suite 安全级别设置为高，并提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

更改 HTTPS 端口

默认情况下，在端口 443 上启用 HTTPS 服务。您无法禁用 HTTPS，但可以更改端口，将其用于 HTTPS 连接。

过程

步骤 1 选择平台设置 (Platform Settings) > HTTPS。

步骤 2 在端口 (Port) 字段中输入要用于 HTTPS 连接的端口。指定一个介于 1 和 65535 之间的整数。默认情况下，在端口 443 上启用此服务。

步骤 3 点击保存 (Save)。

使用指定的 HTTPS 端口配置 Firepower 机箱。

更改 HTTPS 端口后，所有当前 HTTPS 会话都将关闭。用户需要使用新端口重新登录 Firepower 机箱管理器，如下所示：

```
https://<chassis_mgmt_ip_address>:<chassis_mgmt_port>
```

其中 `<chassis_mgmt_ip_address>` 是您在初始配置期间输入的 Firepower 机箱的 IP 地址或主机名，`<chassis_mgmt_port>` 是您刚刚配置的 HTTPS 端口。

删除密钥环

过程

步骤 1 进入安全模式：

```
Firepower-chassis # scope security
```

步骤 2 删除指定密钥环：

```
Firepower-chassis /security # delete keyring name
```

步骤 3 提交任务：

```
Firepower-chassis /security # commit-buffer
```

示例

以下示例删除密钥环：

```
Firepower-chassis# scope security  
Firepower-chassis /security # delete keyring key10  
Firepower-chassis /security* # commit-buffer  
Firepower-chassis /security #
```

删除受信任点

开始之前

确保密钥环未使用受信任点。

过程

步骤 1 进入安全模式：

```
Firepower-chassis# scope security
```

步骤 2 删除指定受信任点：

```
Firepower-chassis /security # delete trustpoint name
```


步骤 3 提交任务:

```
Firepower-chassis /security # commit-buffer
```

示例

以下示例删除受信点:

```
Firepower-chassis# scope security  
Firepower-chassis /security # delete trustpoint tPoint10  
Firepower-chassis /security* # commit-buffer  
Firepower-chassis /security #
```

禁用 HTTPS

过程

步骤 1 进入系统模式:

```
Firepower-chassis# scope system
```

步骤 2 进入系统服务模式:

```
Firepower-chassis /system # scope services
```

步骤 3 禁用 HTTPS 服务:

```
Firepower-chassis /system/services # disable https
```

步骤 4 将任务提交到系统配置:

```
Firepower-chassis /system/services # commit-buffer
```

示例

以下示例禁用 HTTPS 并提交任务:

```
Firepower-chassis# scope system  
Firepower-chassis /system # scope services  
Firepower-chassis /system/services # disable https  
Firepower-chassis /system/services* # commit-buffer  
Firepower-chassis /system/services #
```

配置 AAA

本部分介绍身份验证、授权和记账。有关详细信息，请参阅以下主题:

关于 AAA

AAA 是一组服务，用于控制对计算机资源的访问、实施策略、评估使用情况并提供对服务进行计费所需的信息。这些过程对于高效进行网络管理和安全性而言至关重要。

身份验证

身份验证提供了一种识别用户的方法，这种方法通常先请用户输入有效用户名和有效密码，然后再授予访问权限。AAA 服务器将用户的身份验证凭证与数据库中存储的其他用户凭证进行比较。如果凭证匹配，则允许用户访问网络。如果凭证不匹配，则身份验证失败，并拒绝网络访问。

您可以将 Firepower 4100/9300 机箱配置对机箱的管理连接进行身份验证，包括以下会话：

- HTTPS
- SSH
- 串行控制台

授权

授权是执行策略的过程：确定允许用户访问哪些类型的活动、资源或服务。对用户进行身份验证后，可能会授权该用户执行各种类型的访问或活动。

会计

记账用于测量用户在访问期间使用的资源量，这可以包括系统时间长度或者用户在会话期间发送或接收的数据量。记账是通过记录会话统计信息和使用量信息来执行的，这些信息用于进行授权控制、计费、趋势分析、资源利用率和容量规划活动。

身份验证、授权和记账之间的交互

您可以单独使用身份验证功能，也可以将其与授权和记账功能配合使用。授权始终要求先对用户进行身份验证。您可以单独使用记账功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器

AAA 服务器是用于进行访问控制的网络服务器。身份验证用于识别用户。授权用于实施策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记账对时间和数据资源进行追踪，这些资源用于计费和分析。

本地数据库支持

Firepower 机箱维护可用用户配置文件填充的本地数据库。您可以使用本地数据库代替 AAA 服务器来提供用户身份验证、授权和记账。

配置 LDAP 提供程序

配置 LDAP 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，则 Firepower 可扩展操作系统将使用该设置并忽略默认设置。

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户账户以绑定 Firepower 可扩展操作系统。此账户应具有永不过期的密码。

过程

步骤 1 选择平台设置 (Platform Settings) > AAA。

步骤 2 点击 LDAP 选项卡。

步骤 3 在属性 (Properties) 区域中，填写以下字段：

名称	说明
超时字段	在系统超时之前，系统尝试连接 LDAP 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 30 秒。该属性为必填项。
属性字段	LDAP 属性，存储用户角色值和区域设置值。此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。
基础 DN 字段	LDAP 层级结构中的特定区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索。基础 DN 的长度可以设置为最大 255 个字符减去 CN=\$userid 的长度，其中，\$userid 标识尝试使用 LDAP 身份验证访问 Firepower 机箱的远程用户。 该属性为必填项。如果您没有在此选项卡上指定基础 DN，则必须为自己定义的每个 LDAP 提供程序指定一个基础 DN。
过滤器字段	LDAP 搜索仅限于那些匹配已定义过滤器的用户名。 该属性为必填项。如果您没有在此选项卡上指定过滤器，则必须为自己定义的每个 LDAP 提供程序指定一个过滤器。

步骤 4 点击保存 (Save)。

下一步做什么

创建 LDAP 提供程序。

创建 LDAP 提供程序

Firepower 可扩展操作系统最多支持 16 个 LDAP 提供程序。

开始之前

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户账户以绑定 Firepower 可扩展操作系统。此账户应具有永不过期的密码。

过程

步骤 1 选择平台设置 (Platform Settings) > AAA.

步骤 2 点击 LDAP 选项卡。

步骤 3 对于要添加的每个 LDAP 提供程序：

- a) 在 LDAP 提供程序 (LDAP Providers) 区域中，点击添加 (Add)。
- b) 在添加 LDAP 提供程序 (Add LDAP Provider) 对话框中，填写以下字段：

名称	说明
主机名/FDQN（或 IP 地址）字段	LDAP 提供程序所驻留的主机名或 IP 地址。如果启用了 SSL，此字段必须精确匹配 LDAP 数据库安全认证中的通用名称 (CN)。
顺序字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 中定义的其他提供程序分配下一个可用顺序。
绑定 DN 字段	LDAP 数据库账户的区别名 (DN)，对基础 DN 下的所有对象拥有读取和搜索权限。 支持的最大字符串长度为 255 个 ASCII 字符。
基础 DN 字段	LDAP 层级结构中的特定区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索。基础 DN 的长度可以设置为最大长度 255 个字符减去 CN=\$userid 的长度，其中 \$userid 标识尝试使用 LDAP 身份验证访问 Firepower 机箱管理器或 FXOS CLI 的远程用户。 该值为必填项，除非已在 LDAP 选项卡上设置了默认基础 DN。
端口字段	Firepower 机箱管理器或 FXOS CLI 与 LDAP 数据库进行通信所使用的端口。标准端口号为 389。

名称	说明
启用 SSL 复选框	如果选中，需要对与 LDAP 数据库之间的通信进行加密。如果取消选中，身份验证信息将以明文发送。 LDAP 使用 STARTTLS。这允许使用端口 389 进行加密通信。
过滤器字段	LDAP 搜索仅限于那些匹配已定义过滤器的用户名。 该值为必填项，除非已在 LDAP 选项卡上设置了默认过滤器。
属性字段	LDAP 属性，存储用户角色值和区域设置值。此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。 该值为必填项，除非已在 LDAP 选项卡上设置了默认属性。
密钥字段	在绑定 DN (Bind DN) 字段中指定的 LDAP 数据库账户的密码。您可以输入任意标准 ASCII 字符，但空格、§ (分节号)、? (问号) 或 = (等号) 除外。
确认密钥字段	重复用于确认目的的 LDAP 数据库密码。
超时字段	在系统超时之前，系统尝试连接 LDAP 数据库时应花费的时间 (以秒为单位)。 输入一个介于 1 和 60 秒之间的整数，或者输入 0 (零)，以使用在 LDAP 选项卡上指定的全局超时值。默认值为 30 秒。
供应商字段	此选择标识提供 LDAP 提供程序或服务器详细信息的供应商： <ul style="list-style-type: none"> • 如果 LDAP 提供程序是 Microsoft Active Directory，请选择 MS AD。 • 如果 LDAP 提供程序不是 Microsoft Active Directory，请选择打开 LDAP (Open LDAP)。 默认值为打开 LDAP (Open LDAP)。

c) 点击确定 (OK)，可关闭添加 LDAP 提供程序 (Add LDAP Provider) 对话框。

步骤 4 点击保存 (Save)。

步骤 5 (可选) 启用证书吊销列表检查：

```
Firepower-chassis /security/ldap/server # set revoke-policy {strict | relaxed}
```

注释 此配置仅在启用 SSL 连接后才生效。

删除 LDAP 提供程序

过程

-
- 步骤 1 选择平台设置 (Platform Settings) > AAA.
 - 步骤 2 点击 LDAP 选项卡。
 - 步骤 3 在 LDAP 提供程序 (LDAP Providers) 区域中，在与您想要删除的 LDAP 提供程序对应的表的行中点击删除 (Delete) 图标。
-

配置 RADIUS 提供程序

配置 RADIUS 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，则 Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

-
- 步骤 1 选择平台设置 (Platform Settings) > AAA。
 - 步骤 2 点击 RADIUS 选项卡。
 - 步骤 3 在属性 (Properties) 区域中，填写以下字段：

名称	说明
超时字段	在系统超时之前，系统尝试连接 RADIUS 数据库时应花费的时间（以秒为单位）。 请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。 该属性为必填项。
重试字段	请求被视为失败之前的连接重试次数。

- 步骤 4 点击保存 (Save)。
-

下一步做什么

创建 RADIUS 提供程序。

创建 RADIUS 提供程序

Firepower 可扩展操作系统最多支持 16 个 RADIUS 提供程序。

过程

步骤 1 选择平台设置 (Platform Settings) > AAA。

步骤 2 点击 RADIUS 选项卡。

步骤 3 对于要添加的每个 RADIUS 提供程序：

- a) 在 RADIUS 提供程序 (RADIUS Providers) 区域中，点击添加 (Add)。
- b) 在添加 RADIUS 提供程序 (Add RADIUS Provider) 对话框中，填写以下字段：

名称	说明
主机名/FDQN（或 IP 地址）字段	RADIUS 提供程序所驻留的主机名或 IP 地址。
顺序字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 中定义的其他提供程序分配下一个可用顺序。
密钥字段	数据库 SSL 加密密钥。
确认密钥字段	反复用于确认目的的 SSL 加密密钥。
授权端口字段	Firepower 机箱管理器或 FXOS CLI 与 RADIUS 数据库进行通信所使用的端口。有效范围为 1 至 65535。标准端口号为 1700。
超时字段	在系统超时之前，系统尝试连接 RADIUS 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），使用在 RADIUS 选项卡上指定的全局超时值。默认值为 5 秒。
重试字段	请求被视为失败之前的连接重试次数。 如果需要，请输入一个介于 0 和 5 之间的整数。如果不指定该值，Firepower 机箱管理器将使用在 RADIUS 选项卡上指定的值。

- c) 点击确定 (OK)，可关闭添加 RADIUS 提供程序 (Add RADIUS Provider) 对话框。

步骤 4 点击保存 (Save)。

删除 RADIUS 提供程序

过程

-
- 步骤 1 选择平台设置 (Platform Settings) > AAA。
 - 步骤 2 点击 RADIUS 选项卡。
 - 步骤 3 在 RADIUS 提供程序 (RADIUS Providers) 区域中，在与您想要删除的 RADIUS 提供程序对应的表的行中点击删除 (Delete) 图标。
-

配置 TACACS+ 提供程序

配置 TACACS+ 提供程序的属性

在此任务中配置的属性对于此类型的所有提供程序连接而言是默认设置。如果单个提供程序包括任何这些属性的设置，则 Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

-
- 步骤 1 选择平台设置 (Platform Settings) > AAA。
 - 步骤 2 点击 TACACS 选项卡。
 - 步骤 3 在属性 (Properties) 区域中，填写以下字段：

名称	说明
超时字段	<p>在系统超时之前，系统尝试连接 TACACS+ 数据库时应花费的时间（以秒为单位）。</p> <p>请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。</p> <p>该属性为必填项。</p>

- 步骤 4 点击保存 (Save)。
-

下一步做什么

创建 TACACS+ 提供程序。

创建 TACACS+ 提供程序

Firepower 可扩展操作系统最多支持 16 个 TACACS+ 提供程序。

过程

步骤 1 选择平台设置 (Platform Settings) > AAA。

步骤 2 点击 TACACS 选项卡。

步骤 3 对于您要添加的每个 TACACS+ 提供程序：

- a) 在 TACACS 提供程序 (TACACS Providers) 区域中，点击添加 (Add)。
- b) 在添加 TACACS 提供程序 (Add TACACS Provider) 对话框中，填写以下字段：

名称	说明
主机名/FDQN（或 IP 地址）字段	TACACS+ 提供程序所驻留的主机名或 IP 地址。
顺序字段	Firepower 可扩展操作系统使用此提供程序对用户进行身份验证的顺序。 输入一个介于 1 和 16 之间的整数，或者输入最低可用值或 0（零），前提是您想让 Firepower 可扩展操作系统根据在 Firepower 机箱管理器或 FXOS CLI 中定义的其他提供程序分配下一个可用顺序。
密钥字段	数据库 SSL 加密密钥。
确认密钥字段	反复用于确认目的的 SSL 加密密钥。
端口字段	Firepower 机箱管理器或 FXOS CLI 与 TACACS+ 数据库进行通信所使用的端口。 输入一个介于 1 和 65535 之间的整数。默认端口为 49。
超时字段	在系统超时之前，系统尝试连接 TACACS+ 数据库时应花费的时间（以秒为单位）。 输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），以使用在 TACACS+ 选项卡上指定的全局超时值。默认值为 5 秒。

- c) 点击确定 (OK)，可关闭添加 TACACS 提供程序 (Add TACACS Provider) 对话框。

步骤 4 点击保存 (Save)。

删除 TACACS+ 提供程序

过程

步骤 1 选择平台设置 (Platform Settings) > AAA。

步骤 2 点击 **TACACS** 选项卡。

步骤 3 在 **TACACS 提供程序 (TACACS Providers)** 区域中，在与您想要删除的 TACACS+ 提供程序对应的表的行中点击删除 (**Delete**) 图标。

配置系统日志

系统日志记录是将来自设备的消息收集到运行系统日志后台守护程序的服务器的方法。记录到中央系统日志服务器有助于汇聚日志和警报。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件打印消息。以这种形式记录日志可为日志提供受保护的长期存储。日志对常规故障排除及事件处理均有帮助。

过程

步骤 1 选择平台设置 (**Platform Settings**) > 系统日志 (**Syslog**)。

步骤 2 配置本地目的：

- a) 点击本地目的 (**Local Destinations**) 选项卡。
- b) 在本地目的 (**Local Destinations**) 选项卡上，填写以下字段：

名称	说明
控制台 (Console) 部分	
管理状态 (Admin State) 字段	Firepower 机箱是否在控制台上显示系统日志消息。 如果您想在控制台上显示系统日志消息并将这些日志消息添加到日志中，请选中启用 (Enable) 复选框。如果取消选中启用 (Enable) 复选框，系统日志消息将会添加到日志中，但不会显示在控制台上。
级别 (Level) 字段	如果选中了控制台 - 管理状态 (Console - Admin State) 的启用 (Enable) 复选框，请选择您想在控制台上显示的最低消息级别。Firepower 机箱在控制台上显示此级别及以上消息。这可以是以下其中一项： <ul style="list-style-type: none"> • 紧急 (Emergencies) • 提醒 • 严重
监视器 (Monitor) 部分	

名称	说明
管理状态 (Admin State) 字段	Firepower 机箱是否在监视器上显示系统日志消息。 如果您想在监视器上显示系统日志消息并将这些日志消息添加到日志中，请选中启用 (Enable) 复选框。如果取消选中启用 (Enable) 复选框，系统日志消息将会添加到日志中，但不会显示在监视器上。
级别 (Level) 下拉列表	如果选中了 监视器 - 管理状态 (Monitor - Admin State) 的启用 (Enable) 复选框，请选择您想在监视器上显示的最低消息级别。系统在监视器上显示此级别及以上消息。这可以是以下其中一项： <ul style="list-style-type: none"> • 紧急 (Emergencies) • Alerts (提醒) • Critical (严重) • 错误 (Error) • 警告 (Warnings) • 通知 (Notifications) • 信息 (Information) • 调试 (Debugging)

c) 点击保存 (Save)。

步骤 3 配置远程目的：

- a) 点击远程目的 (Remote Destinations) 选项卡。
- b) 在远程目的 (Remote Destinations) 选项卡上，为最多三个外部日志填写下列字段，这些日志可以存储 Firepower 机箱生成的消息：

通过将系统日志消息发送到远程目的，您可以根据外部系统日志服务器上的可用磁盘空间存档消息，并在保存日志记录数据后对其进行处理。例如，可以指定在记录特定类型的系统日志消息后要执行的操作，从日志提取数据并将记录保存到其他文件以进行报告，或者使用特定于站点的脚本跟踪统计信息。

名称	说明
管理状态 (Admin State) 字段	如果您想在远程日志文件中存储系统日志消息，请选中启用 (Enable) 复选框。

名称	说明
级别 (Level) 下拉列表	<p>选择您想让系统存储的最低消息级别。系统在远程文件中存储此级别及以上消息。这可以是以下其中一项：</p> <ul style="list-style-type: none"> • 紧急 (Emergencies) • Alerts(提醒) • Critical(严重) • 错误 (Error) • 警告 (Warnings) • Notifications(通知) • Information(信息) • 调试(Debugging)
主机名/IP 地址 (Hostname/IP Address) 字段	<p>远程日志文件所驻留的主机名或 IP 地址。</p> <p>注释 如果使用主机名而不使用 IP 地址，必须配置 DNS 服务器。</p>
设备 (Facility) 下拉列表	<p>为系统日志服务器选择要用作文件消息基础的系统日志设备。这可以是以下其中一项：</p> <ul style="list-style-type: none"> • Local0 • Local1 • Local2 • Local3 • Local4 • Local5 • Local6 • Local7

c) 点击保存 (Save)。

步骤 4 配置本地来源：

- a) 点击本地来源 (Local Sources) 选项卡。
- b) 在本地源 (Local Sources) 选项卡上，填写以下字段：

名称	说明
故障管理状态 (Faults Admin State) 字段	是否启用系统故障日志记录。如果选中启用 (Enable) 复选框，Firepower 机箱将记录所有系统故障。
审核管理状态 (Audits Admin State) 字段	是否启用审核日志记录。如果选中启用 (Enable) 复选框，Firepower 机箱将记录所有审核日志事件。
事件管理状态 (Events Admin State) 字段	是否启用系统事件日志记录。如果选中启用 (Enable) 复选框，Firepower 机箱将记录所有系统事件。

c) 点击保存 (Save)。

配置 DNS 服务器

如果系统要求将主机名解析为 IP 地址，您需要指定 DNS 服务器。例如，如果不配置 DNS 服务器，当您在 Firepower 机箱上配置设置时，不能使用 `www.cisco.com` 等名称。您可能需要使用服务器的 IP 地址，其可以是 IPv4 或 IPv6 地址。您最多可以配置 4 个 DNS 服务器。



注释 配置多个 DNS 服务器时，系统仅以任意随机顺序搜索服务器。如果本地管理命令要求 DNS 服务器查询，它只能以随机顺序搜索 3 个 DNS 服务器。

过程

- 步骤 1** 选择平台设置 (Platform Settings) > DNS。
- 步骤 2** 选中启用 DNS 服务器 (Enable DNS Server) 复选框。
- 步骤 3** 对于您要添加的每个 DNS 服务器（最多 4 个），请在 DNS 服务器 (DNS Server) 字段中输入 DNS 服务器的 IP 地址，点击添加 (Add)。
- 步骤 4** 点击保存 (Save)。

启用 FIPS 模式

执行以下步骤，以在 Firepower 4100/9300 机箱上启用 FIPS 模式。

过程

- 步骤 1** 以管理员用户身份登录 Firepower 4100/9300 机箱。
 - 步骤 2** 选择 **Platform Settings** 以打开“平台设置”页面。
 - 步骤 3** 选择 **FIPS/CC mode** 以打开“FIPS 和常用标准”窗口。
 - 步骤 4** 选中 FIPS 所对应的 **Enable** 复选框。
 - 步骤 5** 点击 **Save** 保存配置。
 - 步骤 6** 按照提示重新启动系统。
-

下一步做什么

在 FXOS 版本 2.0.1 之前，首次设置设备时创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥，并使用 [生成 SSH 主机密钥](#)，第 46 页中的详细操作步骤生成新的主机密钥。如果不执行这些附加步骤，则在 FIPS 模式启用的情况下，设备重新启动后，将无法使用 SSH 连接到主控管理引擎。如果您使用 FXOS 2.0.1 或更高版本执行初始设置，则无需生成新的主机密钥。

启用通用标准模式

执行以下步骤，在 Firepower 4100/9300 机箱上启用通用标准模式。

过程

- 步骤 1** 以管理员用户身份登录 Firepower 4100/9300 机箱。
 - 步骤 2** 选择 **Platform Settings** 以打开“平台设置”页面。
 - 步骤 3** 选择 **FIPS/CC mode** 以打开“FIPS 和常用标准”窗口。
 - 步骤 4** 选中“通用标准”所对应的 **Enable** 复选框。
 - 步骤 5** 点击 **Save** 保存配置。
 - 步骤 6** 按照提示重新启动系统。
-

下一步做什么

在 FXOS 版本 2.0.1 之前，首次设置设备时创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥，并使用 [生成 SSH 主机密钥](#)，第 46 页中的详细操作步骤生成新的主机密钥。如果不执行这些附加步骤，则在“通用标准 (Common Criteria)”模式启用的情况下，设备重新启动后，将无法使用 SSH 连接到管理引擎。如果您使用 FXOS 2.0.1 或更高版本执行初始设置，则无需生成新的主机密钥。

配置 IP 访问列表

默认情况下，Firepower 4100/9300 机箱拒绝对本地 Web 服务器的所有访问。您必须使用每个 IP 块的允许服务列表配置 IP 访问列表。

IP 访问列表支持以下协议：

- HTTPS
- SNMP
- SSH

对于各 IP 地址块（v4 或 v6），可为各服务配置最多 25 个不同子网。子网 0 和前缀 0 允许无限制无限访问服务。

过程

步骤 1 以管理员用户身份登录 Firepower 4100/9300 机箱。

步骤 2 选择 **Platform Settings** 以打开“平台设置”页面。

步骤 3 选择 **Access List**，以打开“访问列表”区域。

步骤 4 在此区域中，您可以查看、添加和删除 IP 访问列表中列出的 IPv4 和 IPv6 地址。

要添加 IPv4 块，必须输入有效的 IPv4 IP 地址（前缀 [0-32] 长度）并选择协议。

要添加 IPv6 块，必须输入有效的 IPv6 IP 地址（前缀 [0-128] 长度）并选择协议。

为容器实例接口添加 MAC 池前缀，并查看其 MAC 地址

FXOS 机箱会自动为容器实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一的 MAC 地址。FXOS 机箱使用以下格式生成 MAC 地址：

A2xx.yyzz.zzzz

其中，xx.yy 是用户定义的前缀或系统定义的前缀，zz.zzzz 是由机箱生成的内部计数器。系统定义的前缀与 IDPROM 中的固化 MAC 地址池中第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

有关详细信息，请参阅 [容器实例接口的自动 MAC 地址](#)，第 160 页。

此程序介绍如何查看 MAC 地址，以及如何选择性地定义生成所使用的前缀。



注释 如果您在部署逻辑设备后更改了 MAC 地址前缀，则可能会遇到流量中断现象。

过程

步骤 1 选择平台设置 > MAC 池。

此页面显示以及容器实例和使用 MAC 地址的接口生成的 MAC 地址。

步骤 2（可选）添加生成 MAC 地址时所使用的 MAC 地址前缀。

a) 点击添加前缀。

系统将显示设置 MAC 池前缀对话框。

a) 输入一个介于 1 和 65535 之间的十进制值。此前缀会转换为一个四位数的十六进制数字，并用作 MAC 地址的一部分。

如何使用前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (yyxx)。在 MAC 地址中使用时，该前缀会反转 (xxyy)，以便与机箱的本地形式匹配：

A24D.00zz.zzzz

对于前缀 1009 (03F1)，MAC 地址为：

A2F1.03zz.zzzz

b) 点击确定。

系统会生成并分配使用该前缀的新 MAC 地址。当前前缀和生成的十六进制值则显示在表格上方。

为容器实例添加资源配置文件

要指定每个容器实例的资源使用情况，请创建一个或多个资源配置文件。部署逻辑设备/应用实例时，请指定想要使用的资源配置文件。资源配置文件会设置 CPU 核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

- 最小核心数量为 6。
- 由于内部架构原因，无法指定 8 个核心。
- 您可以分配偶数（6、10、12、14 等）个核心，乃至最大值。
- 最大可用核心数取决于安全模块/机箱型号，请参阅[容器实例的要求和必备条件](#)，第 163 页。

机箱包括一个命名为 "Default-Small" 的默认资源配置文件，此文件包括最小核心数。您可以更改此配置文件定义，甚至可在未使用情况下将其删除。请注意，此配置文件在机箱重新加载且系统上不存在任何其他配置文件时创建而成。

如果当前正在使用，则无法更改资源配置文件设置。必须禁用使用此文件的任何实例，然后更改资源配置文件，最后重新启用该实例。如果调整已建立高可用性对中实例的大小，稍后应尽可能快地确保所有成员大小一致。

如果在将 FTD 实例添加到 FMC 后更改资源配置文件设置，稍后应在 **设备 > 设备管理 > 设备 > 系统 > 库存** 对话框上更新每个设备的库存。

过程

步骤 1 选择 **平台设置 > 资源配置文件**，然后点击 **添加**。

系统将显示 **添加资源配置文件** 对话框。

步骤 2 设置以下参数。

- **Name** - 设置介于 1 和 64 个字符之间的配置文件名称。请注意，此配置文件名称添加后无法更改。
- **Description** - 设置最多 510 个字符的配置文件说明。
- **Number of Cores** - 设置介于 6 和最大值之间的配置文件核心数（偶数），具体取决于机箱。无法指定 8 个核心。

步骤 3 点击 **确定**。

配置机箱 URL

可以指定管理 URL，以便直接从 FMC 轻松打开 FTD 实例的 Firepower 机箱管理器。如果未指定机箱管理 URL，则使用机箱名称。

如果在将 FTD 实例添加到 FMC 后更改机箱 URL 设置，稍后应在 **设备 > 设备管理 > 设备 > 系统 > 库存** 对话框上更新每个设备的库存。

过程

步骤 1 选择 **平台设置 > 机箱 URL**。

步骤 2 设置以下参数。

- **机箱名称** - 设置介于 1 至 60 个字符之间的机箱名称。
- **机箱 URL** - 设置 FMC 应该用于连接到 Firepower 机箱管理器中 FTD 实例的 URL。URL 必须以 `https://` 开头。如果未指定机箱管理 URL，则使用机箱名称。

步骤 3 点击更新。



第 9 章

接口管理

- [关于 Firepower 接口，第 123 页](#)
- [Firepower 接口的准则和限制，第 136 页](#)
- [配置接口，第 138 页](#)
- [监控接口，第 144 页](#)
- [排除接口故障，第 145 页](#)
- [接口历史，第 151 页](#)

关于 Firepower 接口

Firepower 4100/9300 机箱支持物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口。EtherChannel 接口最多可以包含同一类型的 16 个成员接口。

机箱管理接口

机箱管理接口用于通过 SSH 或 Firepower 机箱管理器来管理 FXOS 机箱。此接口在接口选项卡顶部显示为 **MGMT**，您只可在接口选项卡上启用或禁用此接口。此接口独立于分配给应用管理用逻辑设备的 MGMT 型接口。

要配置此接口参数，必须从 CLI 进行配置。另请参阅[更改管理 IP 地址，第 62 页](#)。要在 FXOS CLI 中查看此接口，请连接到本地管理并显示管理端口：

```
Firepower # connect local-mgmt
```

```
Firepower(local-mgmt) # show mgmt-port
```

请注意，即使将物理电缆或小型封装热插拔模块拔下，或者执行了 **mgmt-port shut** 命令，机箱管理接口仍会保持正常运行状态。

接口类型

每个接口可以是以下类型之一：

- 数据 - 不能在逻辑设备之间共享数据接口。

- 数据共享 - 仅容器实例支持这些数据接口，可由一个或多个逻辑设备/容器实例（仅限 FTD）共享。每个容器实例都可通过背板与共享此接口的所有其他实例通信。共享的接口可能会影响您可以部署容器实例的数量；请参阅[共享接口可扩展性](#)，第 125 页。共享接口不支持用于桥接组成员接口（在透明模式或路由模式下）、内联集、被动接口或故障切换链路。
- Mgmt - 管理接口用于管理应用实例。这些管理接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。只能为每个逻辑设备分配一个管理接口。有关独立机箱管理接口的信息，请参阅[机箱管理接口](#)，第 123 页。

在 FTD 应用内，物理管理接口由诊断逻辑接口和管理逻辑接口共用。管理逻辑接口与设备上的其他接口分离。它用于设置设备并将其注册到 Firepower 管理中心。它会使用自己的本地身份验证、IP 地址和静态路由。请参阅《Firepower 管理中心配置指南》“系统配置”一章中的“管理接口”部分。

诊断逻辑接口可以连同其余数据接口一起在 FMC 设备 > 设备管理 > 接口屏幕上进行配置。使用诊断接口是可选的。诊断接口只允许管理流量，而不允许通过流量。

- Firepower 事件 - 此接口是 FTD 设备的辅助管理接口。要使用此接口，您必须在 FTD CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅 Firepower 管理中心配置指南系统配置一章中的“管理接口”部分。Firepower 事件接口可以由一个或多个逻辑设备共享，以访问外部主机；逻辑设备无法通过此接口与共享接口的其他逻辑设备通信。
- 集群 - 用于集群逻辑设备的特殊接口类型。此类型自动分配到集群控制链路以进行设备间集群通信。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。

机箱和应用中的独立接口状态

您可以从管理上启用和禁用机箱和应用中的接口。必须在两个操作系统中都启用能够正常运行的接口。由于接口状态可独立控制，因此机箱与应用之间可能出现不匹配的情况。

应用内接口的默认状态取决于接口类型。例如，在应用内，默认禁用物理接口或 EtherChannel，但默认启用于接口。

硬件旁路对

对于 FTD，Firepower 9300 和 4100 系列上的某些接口模块允许您启用硬件绕行功能。硬件绕行可确保流量在停电期间继续在内联接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。

硬件绕行功能在 FTD 应用中进行配置。您不需要将这些接口用作硬件绕行对；它们可用作 ASA 和 FTD 应用的常规接口。请注意，不可为分支端口配置具有硬件绕行功能的接口。如果您想使用硬件绕行功能，请勿将端口配置为 EtherChannel；否则，您可将这些接口作为常规接口模式下的 EtherChannel 成员。

对于以下型号上特定网络模块的接口对，FTD 支持 硬件绕行：

- Firepower 9300

- Firepower 4100 系列

这些型号的受支持 硬件绕行 网络包括：

- Firepower 6 端口 1G SX FTW 单位宽网络模块 (FPR-NM-6X1SX-F)
- Firepower 6 端口 10G SR FTW 单位宽网络模块 (FPR-NM-6X10SR-F)
- Firepower 6 端口 10G LR FTW 单位宽网络模块 (FPR-NM-6X10LR-F)
- Firepower 2 端口 40G SR FTW 单位宽网络模块 (FPR-NM-2X40G-F)
- Firepower 8 端口 1G 铜 FTW 单位宽网络模块 (FPR-NM-8X1G-F)

硬件绕行 仅可使用以下端口对：

- 1、2
- 3、4
- 5、6
- 7、8

巨帧支持

Firepower 4100/9300 机箱默认启用巨帧支持。要在 Firepower 4100/9300 机箱上安装的特定逻辑设备上启用巨帧支持，您将需要为逻辑设备上的接口配置合适的 MTU 设置。

Firepower 4100/9300 机箱 上应用支持的最大 MTU 为 9184。

共享接口可扩展性

容器实例可以共享数据共享型接口。此功能允许您保存物理接口的使用情况，以及支持灵活的网络部署。当您共享接口时，机箱会使用唯一 MAC 地址将流量转发至适当实例。然而，由于需要在机箱内实现全网状拓扑，因此共享接口将导致转发表规模扩大（每个实例都必须能够与共享同一接口的所有其他实例进行通信）。因此，您可以共享的接口存在数量限制。

除转发表外，机箱还维护用于 VLAN 子接口转发的 VLAN 组表。您可以创建最多 500 个 VLAN 子接口，具体取决于父接口数量和其他部署决策。

请参阅共享接口分配的以下限制：

- 每个共享接口最多 14 个实例。例如，您可以将以太网接口 1/1 分配至实例 1 至实例 14。
- 每个实例最多 10 个共享接口。例如，您可以将以太网接口 1/1.1 至以太网接口 1/1.10 分配至实例 1。

共享接口最佳实践

为确保转发表的最佳可扩展性，请共享尽可能少的接口。相反，您可以在一个或多个物理接口上创建最多 500 个 VLAN 子接口，然后在容器实例之间划分 VLAN。

共享接口时，请按照可扩展性从高到低的顺序遵循这些最佳实践：

1. 最佳 - 共享单父项下的子接口，并结合使用相同集合的子接口和同组逻辑设备。

例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口：端口通道 1.100、200 和 300 而不是端口通道 1、端口通道 2 和端口通道 3。与跨父项共享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

如果未与一组逻辑设备共享相同集合的子接口，则配置会提高资源使用率（更多 VLAN 组）。例如，与逻辑设备 1、2 和 3 共享端口通道 1.100 和 200（一个 VLAN 组），而不是与逻辑设备 1 和 2 共享端口通道 1.100，同时与逻辑设备 2 和 3 共享端口通道 1.200（两个 VLAN 组）。

2. 一般 - 跨父项共享子接口。

例如，共享端口通道 1.100、端口通道 2.200 和端口通道 3.300 而不是端口通道 1、端口通道 2 和端口通道 3。虽然这种使用方法的效率低于仅共享同一父项上的子接口，但仍可利用 VLAN 组。

3. 最差 - 共享单个父接口（物理或 EtherChannel）。

此方法使用的转发表条目最多。

共享接口使用示例

有关接口共享示例和可扩展性，请参阅下表。以下情景假设使用一个在所有实例中共享的物理/EtherChannel 接口来实现管理，和另一个设有专用子接口的物理或 EtherChannel 接口，用于实现高可用性。

- [表 6: Firepower 9300（设有三个 SM-44）上的物理/EtherChannel 接口和实例，第 127 页](#)
- [表 7: Firepower 9300（设有三个 SM-44）上的一个父接口的子接口和实例，第 129 页](#)
- [表 8: Firepower 9300（设有一个 SM-44）上的物理/EtherChannel 接口和实例，第 132 页](#)
- [表 9: Firepower 9300（设有一个 SM-44）上的一个父接口的子接口和实例，第 134 页](#)

Firepower 9300（设有三个 SM-44）

下表适用于仅使用物理接口或 Etherchannel 的 9300 上的三个 SM-44 安全模块。在未设子接口的情况下，接口的最大数量受限。此外，与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 6: Firepower 9300 (设有三个 SM-44) 上的物理/EtherChannel 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	0	4: <ul style="list-style-type: none"> • 实例 1 • 实例 2 • 实例 3 • 实例 4 	16%
30: <ul style="list-style-type: none"> • 15 • 15 	0	2: <ul style="list-style-type: none"> • 实例 1 • 实例 2 	14%
14: <ul style="list-style-type: none"> • 14 (每个实例 1 个专用接口) 	1	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
33: <ul style="list-style-type: none"> • 11 (每个实例 1 个专用接口) • 11 (每个实例 1 个专用接口) • 11 (每个实例 1 个专用接口) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	33: <ul style="list-style-type: none"> • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33 	98%

专用接口	共享接口	实例数	转发表使用百分比
33: <ul style="list-style-type: none"> • 11 (每个实例 1 个专用接口) • 11 (每个实例 1 个专用接口) • 12 (每个实例 1 个专用接口) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	34: <ul style="list-style-type: none"> • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 34 	102% 禁止使用
30: <ul style="list-style-type: none"> • 30 (每个实例 1 个专用接口) 	1	6: <ul style="list-style-type: none"> • 实例 1 实例 6 	25%
30: <ul style="list-style-type: none"> • 10 (每个实例 5 个专用接口) • 10 (每个实例 5 个专用接口) • 10 (每个实例 5 个专用接口) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	6: <ul style="list-style-type: none"> • 实例 1 至实例 2 • 实例 2 至实例 4 • 实例 5 至实例 6 	23%
30: <ul style="list-style-type: none"> • 30 (每个实例 6 个专用接口) 	2	5: <ul style="list-style-type: none"> • 实例 1 至实例 5 	28%

专用接口	共享接口	实例数	转发表使用百分比
30: <ul style="list-style-type: none"> • 12（每个实例 6 个专用接口） • 18（每个实例 6 个专用接口） 	4: <ul style="list-style-type: none"> • 2 • 2 	5: <ul style="list-style-type: none"> • 实例 1 至实例 2 • 实例 2 至实例 5 	26%
24: <ul style="list-style-type: none"> • 6 • 6 • 6 • 6 	7	4: <ul style="list-style-type: none"> • 实例 1 • 实例 2 • 实例 3 • 实例 4 	44%
24: <ul style="list-style-type: none"> • 12（每个实例 6 个专用接口） • 12（每个实例 6 个专用接口） 	14: <ul style="list-style-type: none"> • 7 • 7 	4: <ul style="list-style-type: none"> • 实例 1 至实例 2 • 实例 2 至实例 4 	41%

下表适用于使用单父项物理接口上子接口的 9300 的三个 SM-44 安全模块。例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

每个 SM-44 模块最多可支持 14 个实例。如有必要，系统会拆分模块之间的实例，以将实例数维持在限值范围内。

表 7: Firepower 9300（设有三个 SM-44）上的一个父接口的子接口和实例

专用子接口	共享子接口	实例数	转发表使用百分比
168: <ul style="list-style-type: none"> • 168（每个实例 4 个专用子接口） 	0	42: <ul style="list-style-type: none"> • 实例 1 至实例 42 	33%

专用子接口	共享子接口	实例数	转发表使用百分比
224: <ul style="list-style-type: none"> • 224 (每个实例 16 个专用子接口) 	0	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	27%
14: <ul style="list-style-type: none"> • 14 (每个实例 1 个专用子接口) 	1	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
33: <ul style="list-style-type: none"> • 11 (每个实例 1 个专用子接口) • 11 (每个实例 1 个专用子接口) • 11 (每个实例 1 个专用子接口) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	33: <ul style="list-style-type: none"> • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33 	98%
70: <ul style="list-style-type: none"> • 70 (每个实例 5 个专用子接口) 	1	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
165: <ul style="list-style-type: none"> • 55 (每个实例 5 个专用子接口) • 55 (每个实例 5 个专用子接口) • 55 (每个实例 5 个专用子接口) 	3: <ul style="list-style-type: none"> • 1 • 1 • 1 	33: <ul style="list-style-type: none"> • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33 	98%

专用子接口	共享子接口	实例数	转发表使用百分比
70: <ul style="list-style-type: none"> • 70 (每个实例 5 个专用子接口) 	2	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
165: <ul style="list-style-type: none"> • 55 (每个实例 5 个专用子接口) • 55 (每个实例 5 个专用子接口) • 55 (每个实例 5 个专用子接口) 	6: <ul style="list-style-type: none"> • 2 • 2 • 2 	33: <ul style="list-style-type: none"> • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33 	98%
70: <ul style="list-style-type: none"> • 70 (每个实例 5 个专用子接口) 	10	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
165: <ul style="list-style-type: none"> • 55 (每个实例 5 个专用子接口) • 55 (每个实例 5 个专用子接口) • 55 (每个实例 5 个专用子接口) 	30: <ul style="list-style-type: none"> • 10 • 10 • 10 	33: <ul style="list-style-type: none"> • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33 	102% 禁止使用

Firepower 9300 (设有一个 SM-44)

下表适用于仅使用物理接口或 Etherchannel 的 Firepower 9300 (设一个 SM-44)。在未设子接口的情况下,接口的最大数量受限。此外,与共享多个子接口相比,共享多个物理接口所使用的转发表资源更多。

Firepower Firepower 9300 (设有一个 SM-44) 最多可支持 14 个实例。

表 8: Firepower 9300 (设有一个 SM-44) 上的物理/EtherChannel 接口和实例

专用接口	共享接口	实例数	转发表使用百分比
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	0	4: <ul style="list-style-type: none"> • 实例 1 • 实例 2 • 实例 3 • 实例 4 	16%
30: <ul style="list-style-type: none"> • 15 • 15 	0	2: <ul style="list-style-type: none"> • 实例 1 • 实例 2 	14%
14: <ul style="list-style-type: none"> • 14 (每个实例 1 个专用接口) 	1	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
14: <ul style="list-style-type: none"> • 7 (每个实例 1 个专用接口) • 7 (每个实例 1 个专用接口) 	2: <ul style="list-style-type: none"> • 1 • 1 	14: <ul style="list-style-type: none"> • 实例 1 至实例 7 • 实例 8 至实例 14 	37%
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	1	4: <ul style="list-style-type: none"> • 实例 1 • 实例 2 • 实例 3 • 实例 4 	21%
32: <ul style="list-style-type: none"> • 16 (每个实例 8 个专用接口) • 16 (每个实例 8 个专用接口) 	2	4: <ul style="list-style-type: none"> • 实例 1 至实例 2 • 实例 3 至实例 4 	20%

专用接口	共享接口	实例数	转发表使用百分比
32: <ul style="list-style-type: none"> • 8 • 8 • 8 • 8 	2	4: <ul style="list-style-type: none"> • 实例 1 • 实例 2 • 实例 3 • 实例 4 	25%
32: <ul style="list-style-type: none"> • 16 (每个实例 8 个专用接口) • 16 (每个实例 8 个专用接口) 	4: <ul style="list-style-type: none"> • 2 • 2 	4: <ul style="list-style-type: none"> • 实例 1 至实例 2 • 实例 3 至实例 4 	24%
24: <ul style="list-style-type: none"> • 8 • 8 • 8 	8	3: <ul style="list-style-type: none"> • 实例 1 • 实例 2 • 实例 3 	37%
10: <ul style="list-style-type: none"> • 10 (每个实例 2 个专用接口) 	10	5: <ul style="list-style-type: none"> • 实例 1 至实例 5 	69%
10: <ul style="list-style-type: none"> • 6 (每个实例 2 个专用接口) • 4 (每个实例 2 个专用接口) 	20: <ul style="list-style-type: none"> • 10 • 10 	5: <ul style="list-style-type: none"> • 实例 1 至实例 3 • 实例 4 至实例 5 	59%
14: <ul style="list-style-type: none"> • 12 (每个实例 2 个专用接口) 	10	7: <ul style="list-style-type: none"> • 实例 1 至实例 7 	109% 禁止使用

下表适用于使用单父项物理接口上子接口的 Firepower 9300（设有一个 SM-44）。例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口。与共享多个子接口相比，共享多个物理接口所使用的转发表资源更多。

Firepower 9300（设有一个 SM-44）最多可支持 14 个实例。

表 9: Firepower 9300（设有一个 SM-44）上的一个父接口的子接口和实例

专用子接口	共享子接口	实例数	转发表使用百分比
112: <ul style="list-style-type: none"> • 112（每个实例 8 个专用子接口） 	0	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	17%
224: <ul style="list-style-type: none"> • 224（每个实例 16 个专用子接口） 	0	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	17%
14: <ul style="list-style-type: none"> • 14（每个实例 1 个专用子接口） 	1	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
14: <ul style="list-style-type: none"> • 7（每个实例 1 个专用子接口） • 7（每个实例 1 个专用子接口） 	2: <ul style="list-style-type: none"> • 1 • 1 	14: <ul style="list-style-type: none"> • 实例 1 至实例 7 • 实例 8 至实例 14 	37%
112: <ul style="list-style-type: none"> • 112（每个实例 8 个专用子接口） 	1	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%

专用子接口	共享子接口	实例数	转发表使用百分比
112: <ul style="list-style-type: none"> • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口） 	2: <ul style="list-style-type: none"> • 1 • 1 	14: <ul style="list-style-type: none"> • 实例 1 至实例 7 • 实例 8 至实例 14 	37%
112: <ul style="list-style-type: none"> • 112（每个实例 8 个专用子接口） 	2	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
112: <ul style="list-style-type: none"> • 56（每个实例 8 个专用子接口） • 56（每个实例 8 个专用子接口） 	4: <ul style="list-style-type: none"> • 2 • 2 	14: <ul style="list-style-type: none"> • 实例 1 至实例 7 • 实例 8 至实例 14 	37%
140: <ul style="list-style-type: none"> • 140（每个实例 10 个专用子接口） 	10	14: <ul style="list-style-type: none"> • 实例 1 至实例 14 	46%
140: <ul style="list-style-type: none"> • 70（每个实例 10 个专用子接口） • 70（每个实例 10 个专用子接口） 	20: <ul style="list-style-type: none"> • 10 • 10 	14: <ul style="list-style-type: none"> • 实例 1 至实例 7 • 实例 8 至实例 14 	37%

查看共享接口资源

要查看转发表和 VLAN 组使用情况，请在 `scope fabric-interconnect` 项下输入 `show detail` 命令。例如：

```
Firepower# scope fabric-interconnect
DFirepower /fabric-interconnect # show detail

Fabric Interconnect:
  ID: A
  Product Name: Cisco FPR9K-SUP
  PID: FPR9K-SUP
  VID: V02
  Vendor: Cisco Systems, Inc.
  Serial (SN): JAD104807YN
  HW Revision: 0
  Total Memory (MB): 16185
  OOB IP Addr: 10.10.5.14
  OOB Gateway: 10.10.5.1
  OOB Netmask: 255.255.255.0
  OOB IPv6 Address: ::
  OOB IPv6 Gateway: ::
  Prefix: 64
  Operability: Operable
  Thermal Status: Ok
  Ingress VLAN Group Entry Count (Current/Max): 0/500
  Switch Forwarding Path Entry Count (Current/Max): 16/1021
  Current Task 1:
  Current Task 2:
  Current Task 3:
```

Firepower 威胁防御的内联集链路状态传播

内联集类似于导线上的凹凸，用于将两个接口绑定在一起插入到现有网络中。此功能使系统可以安装在任何网络环境中，而无需配置相邻网络设备。内联接口无条件接收所有流量，但是，除非已明确丢弃，否则这些接口上接收的所有流量将在内联集外重传。

当您在 FTD 应用中配置内联集并启用链路状态传播时，FTD 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。当被关闭的接口恢复运行时，第二个接口也将自动恢复运行。换句话说，如果一个接口的链路状态更改，机箱会感知该更改并更新其他接口的链路状态以与其匹配。请注意，机箱最多需要 4 秒即可传播链路状态更改。在将路由器配置为在处于故障状态的网络设备上自动重新路由流量的弹性网络环境中，链路状态传播特别有用。

Firepower 接口的准则和限制

VLAN 子接口

- 您可以使用最多 500 个 VLAN ID 为每个机箱创建 250 至 500 个子接口，具体取决于网络部署。
- 仅支持在数据或数据共享型接口上创建子接口。
- 子接口（和父接口）仅可分配至容器实例。



注释 如果将父接口分配至容器实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。

- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
 - 不得将子接口用于 FTD 内联集或用作被动接口。
 - 如果将子接口用于故障切换链路，则该父接口及其上的所有子接口仅限于用作故障切换链路。不得将某些子接口用作故障切换链路，而将某些用作常规数据接口。

数据共享接口

- 每个共享接口最多 14 个实例。例如，您可以将以太网接口 1/1 分配至实例 1 至实例 14。
- 每个实例最多 10 个共享接口。例如，您可以将以太网接口 1/1.1 至以太网接口 1/1.10 分配至实例 1。
- 不得结合使用数据共享接口和本地实例。
- 请参阅逻辑设备应用中的以下限制；规划接口分配时，请谨记这些限制。
 - 不得结合使用数据共享接口和透明防火墙模式设备。
 - 不得结合数据共享接口和 FTD 内联集或被动接口。
 - 不得将数据共享接口用于故障切换链路。

FTD 的内联集

- 支持物理接口（常规端口和分支端口）和 Etherchannel。不支持子接口。
- 支持链路状态传播。

硬件绕行

- 支持 FTD；可以将它们用作 ASA 的常规接口。
- FTD 仅支持包含内联集的硬件绕行。
- 不可为分支端口配置具有硬件绕行功能的接口。
- 不得包含 EtherChannel 中的硬件绕行接口包含在并将它们用于硬件绕行；可以将它们用作 EtherChannel 中的常规接口。

默认 MAC 地址

对于本地实例：

默认 MAC 地址分配取决于接口类型。

- 物理接口 - 物理接口使用已刻录的 MAC 地址。
- EtherChannel - 对于 EtherChannel，属于通道组的所有接口均共享相同 MAC 地址。此功能使 EtherChannel 对网络应用和用户透明，因为他们只看到一个逻辑连接；而不知道各个链路。端口通道接口使用来自池中的唯一 MAC 地址；接口成员资格不影响 MAC 地址。

对于容器实例：

- 所有接口的 MAC 地址均取自一个 MAC 地址池。请参阅[容器实例接口的自动 MAC 地址](#)，第 160 页。

配置接口

默认情况下，物理接口处于禁用状态。可以启用接口，添加 Etherchannel，添加 VLAN 子接口，编辑接口属性，配置分支端口。



注释 如果在 FXOS 中删除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中删除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

启用或禁用接口

可以将每个接口的**管理状态**更改为启用或禁用。默认情况下，物理接口处于禁用状态。对于 VLAN 子接口，其管理状态继承自父接口。

过程

步骤 1 选择接口 (**Interfaces**) 打开 Interfaces 页面。

“接口 (Interfaces)” 页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 要启用接口，请点击已禁用 滑块 ()，使其更改为已启用 滑块 ()。

点击是 (**Yes**)，确认更改。以直观展示图表现的对应接口从灰色变为绿色。

步骤 3 要禁用接口，请点击已启用 滑块 ()，使其更改为已禁用 滑块 ()。

点击是 (**Yes**)，确认更改。以直观展示图表现的对应接口从绿色变为灰色。

配置物理接口

您可以通过物理方式启用和禁用接口，并设置接口速度和双工。要使用某一接口，必须在 FXOS 中以物理方式启用它，并在应用中以逻辑方式启用它。

开始之前

- 不能单独修改已经是 EtherChannel 成员的接口。务必在将接口添加到 EtherChannel 之前为其配置设置。

过程

步骤 1 选择接口 (**Interfaces**) 打开 Interfaces 页面。

“接口 (Interfaces)” 页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 在您要编辑的接口所对应的行中点击 **编辑 (Edit)**，可打开 **编辑接口 (Edit Interface)** 对话框。

步骤 3 要启用接口，请选中 **启用 (Enable)** 复选框。要禁用接口，请取消选中 **启用 (Enable)** 复选框。

步骤 4 选择接口类型：**数据、数据共享、管理、Firepower 事件或集群**。

请勿选择 **集群** 类型；默认情况下，系统会自动在端口通道 48 上创建集群控制链路。

步骤 5 (可选) 从 **速度** 下拉列表中选择接口的速度。

步骤 6 (可选) 如果您的接口支持 **自动协商**，请点击 **是** 或 **否** 单选按钮。

步骤 7 (可选) 从 **双工** 下拉列表中选择接口双工。

步骤 8 点击 **OK**。

添加 EtherChannel (端口通道)

EtherChannel (也称为端口通道) 最多可以包含 16 个同一类型的成员接口。链路汇聚控制协议 (LACP) 将在两个网络设备之间交换链路汇聚控制协议数据单元 (LACPDU)，进而汇聚接口。

您可以将 EtherChannel 中的每个物理数据或数据共享接口配置为：

- **Active** - 发送和接收 LACP 更新。主用 EtherChannel 可以与主用或备用 EtherChannel 建立连接。除非您需要最大限度地减少 LACP 流量，否则应使用主用模式。
- **开启** - EtherChannel 始终开启，并且不使用 LACP。“开启”的 EtherChannel 只能与另一个“开启”的 EtherChannel 建立连接。

非数据接口仅支持主用模式。

LACP 将协调自动添加和删除指向 EtherChannel 的链接，而无需用户干预。LACP 还会处理配置错误，并检查成员接口的两端是否连接到正确的通道组。如果接口发生故障且未检查连接和配置，“开启”模式将不能使用通道组中的备用接口。

当 Firepower 4100/9300 机箱创建 EtherChannel 时，EtherChannel 将处于挂起 (**Suspended**) 状态，直到您将其分配给逻辑设备，即使物理链路是连通的。EtherChannel 在以下情况下将退出挂起 (**Suspended**) 状态：

- 将 EtherChannel 添加为独立逻辑设备的数据或管理端口
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的管理接口或集群控制链路
- 将 EtherChannel 添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个单元已加入该集群

请注意，EtherChannel 在您将它分配到逻辑设备前不会正常工作。如果从逻辑设备移除 EtherChannel 或删除逻辑设备，EtherChannel 将恢复为挂起 (**Suspended**) 状态。

过程

步骤 1 选择接口 (**Interfaces**) 打开 Interfaces 页面。

“接口 (Interfaces)” 页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

步骤 2 点击接口表上方的添加端口通道 (**Add Port Channel**)，可打开添加端口通道 (**Add Port Channel**) 对话框。

步骤 3 在端口通道 ID (**Port Channel ID**) 字段中输入端口通道 ID。有效值介于 1 与 47 之间。

部署集群逻辑设备时，端口通道 48 为集群控制链路预留。如果不想将端口通道 48 用于集群控制链路，您可以为 EtherChannel 配置不同的 ID，为接口选择“集群 (Cluster)”类型。不要将任何接口分配给集群 EtherChannel。

步骤 4 要启用端口通道，请选中启用 (**Enable**) 复选框。要禁用端口通道，请取消选中启用 (**Enable**) 复选框。

步骤 5 选择接口类型：数据、数据共享、管理、Firepower 事件或集群。

请勿选择集群类型，除非要将此端口通道用作集群控制链路，而不是默认设置。

步骤 6 从下拉列表设置成员接口的管理速度。

步骤 7 对于数据或数据共享接口，选择 LACP 端口通道模式、主用或保持。

对于非数据或数据共享接口，模式始终是主用模式。

步骤 8 设置管理双工、全双工或半双工。

步骤 9 要将接口添加到端口通道，请在可用接口 (**Available Interface**) 列表中选择该接口，点击添加接口 (**Add Interface**)，将接口移动至“成员 ID (Member ID)”列表。您最多可以添加 16 个同一类型和速度的接口。

提示 一次可添加多个接口。要选择多个独立接口，请点击所需的接口，同时按住 **Ctrl** 键。要选择一个接口范围，请选择范围中的第一个接口，然后，在按住 **Shift** 键的同时，点击选择范围中的最后一个接口。

步骤 10 要从端口通道删除接口，请点击“成员 ID (Member ID)”列表中接口右侧的删除 (**Delete**) 按钮。

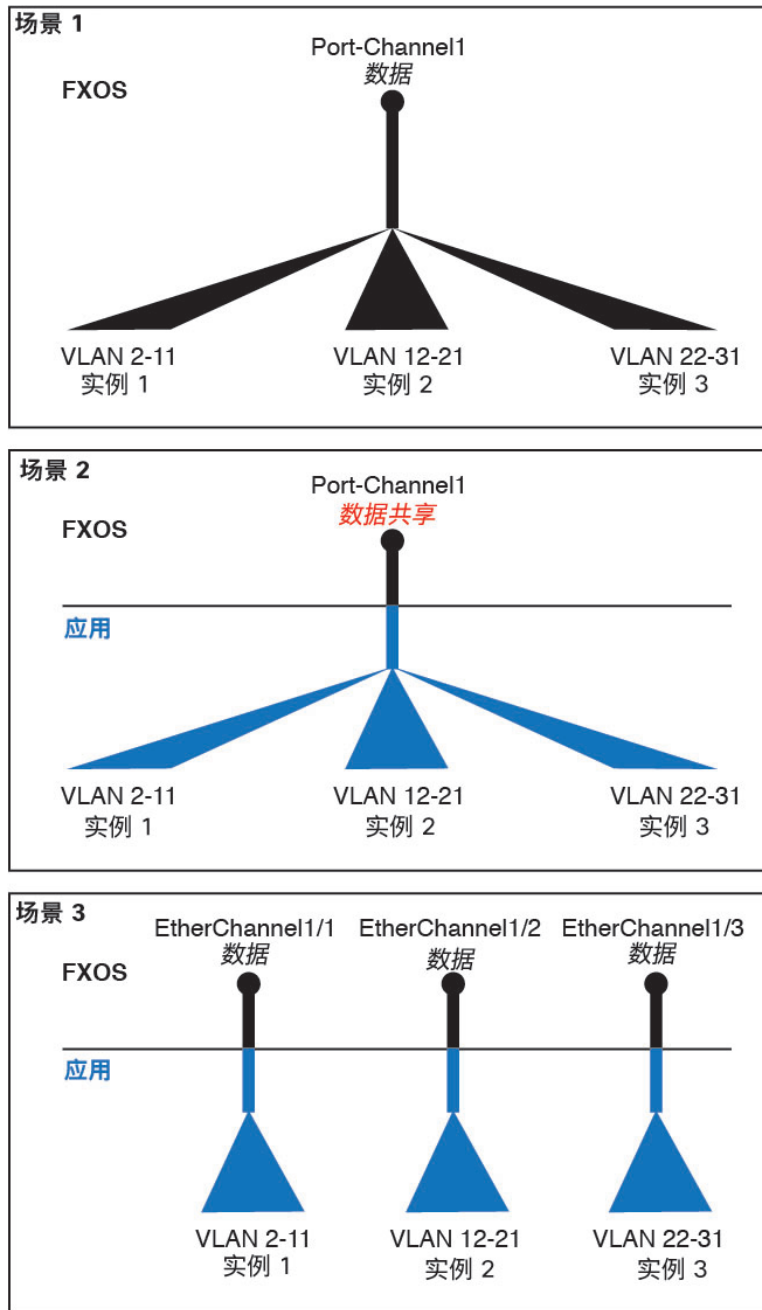
步骤 11 点击确定 (OK)。

为容器实例添加 VLAN 子接口

您可以向机箱添加 250 至 500 个 VLAN 子接口，具体取决于网络部署。

每个接口的 VLAN ID 都必须具有唯一性，并且在容器实例内，VLAN ID 在所有已分配接口上也必须具有唯一性。只要系统将 VLAN ID 分配至不同的容器实例，您就可以在单独接口上重新使用它们。然而，即使每个子接口使用相同的 ID，这些子接口仍将计入限值。

对于本地实例，您仅可在应用内创建 VLAN 子接口。对于容器实例，您还可以在不含所定义 FXOS VLAN 子接口的接口上的应用内创建 VLAN 子接口，这些子接口不受 FXOS 限值限制。选择在哪个操作系统创建子接口取决于网络部署和个人偏好。例如，要共享子接口，必须在 FXOS 中创建子接口。偏好 FXOS 子接口的另一种场景包含将单个接口上的单独子接口组分配至多个实例。例如，您想要结合使用端口通道 1 与实例 A 上的 VLAN 2-11、实例 B 上的 VLAN 12-21 和实例 C 上的 VLAN 22-31。如果您在应用内创建这些子接口，则必须在 FXOS 中共享父接口，但这可能并不合适。有关可以用于实现这种场景的三种方法，请参阅下图：



过程

步骤 1 选择接口打开所有接口选项卡。

页面顶部的所有接口选项卡显示当前已安装的接口的直观展示图，并在下表中提供已安装接口列表。

步骤 2 点击添加新 > 子接口打开添加子接口对话框。

步骤 3 选择接口类型：数据或数据共享。

仅支持在数据或数据共享型接口上创建子接口。此类型独立于父接口类型；例如，您可以设数据共享父接口和数据子接口。

步骤 4 从下拉列表选择父接口。

不得将子接口添加到当前已分配至逻辑设备的物理接口。如果系统已分配父接口的其他子接口，只要未分配此父接口，您就可以添加新的子接口。

步骤 5 输入一个介于 1 和 4294967295 之间的子接口 ID。

此 ID 将附加到父接口 ID，作为 *interface_id.subinterface_id*。例如，如果您将子接口添加到 ID 为 100 的以太网接口 1/1，则子接口 ID 将为：以太网接口 1/1.100。尽管可以出于方便目的将此 ID 和 VLAN ID 设置为相互匹配，但两者始终不同。

步骤 6 设置介于 1 和 4095 之间的 VLAN ID。

步骤 7 点击确定。

展开父接口查看其项下所有子接口。

配置分支电缆

以下程序介绍如何配置分支线缆以供 Firepower 4100/9300 机箱使用。您可以使用分支线缆提供 4 个 10 Gbps 端口，代替单个 40 Gbps 端口。

开始之前

不可为分支端口配置具有硬件绕行功能的接口。

过程

步骤 1 选择接口 (**Interfaces**) 打开 Interfaces 页面。

“接口 (**Interfaces**)” 页面顶部显示当前已安装的接口的直观展示图，在下表中提供已安装接口列表。

接口对应的行中的“分支端口 (**Breakout Port**)” 图标表示能够支持分支线缆但当前未配置为支持的接口。对于已配置为使用分支线缆的接口，分别列出各个分支接口（例如，以太网 2/1/1、2/1/2、2/1/3 和 2/1/4）。

步骤 2 要将 40 Gbps 接口转换为 4 个 10 Gbps 接口，请执行以下操作：

a) 点击您想转换的接口所对应的分支端口 (**Breakout Port**) 图标。

“创建分支端口 (**Breakout Port Creation**)” 对话框打开，要求您确认是否想要继续，并警告您机箱将被重启。

b) 点击是进行确认。

Firepower 机箱重启，指定接口转换为 4 个 10 Gbps 接口。

步骤 3 要将 4 个 10 Gbps 分支接口转换回单个 40 Gbps 接口，请执行以下操作：

- a) 点击任意分支接口所对应的 **删除 (Delete)**。

确认对话框打开，要求您确认是否想要继续，并警告您全部 4 个分支接口都将被删除，机箱将重启。

- b) 点击是进行确认。

Firepower 机箱重启，指定的接口转换为单个 40 Gbps 接口。

监控接口

从 Firepower 机箱管理器的“接口 (Interfaces)”页面，您可以查看机箱上已安装的接口的状态，编辑接口属性，启用或禁用接口，以及创建端口通道。

“接口 (Interfaces)”页面由两部分组成：

- 上面部分显示 Firepower 机箱中安装的接口的直观表示。您可以将鼠标悬停在任何接口上方，以获取有关该接口的其他信息。

接口带有色标，表示其当前状态：

- 绿色 - 已安装并启用接口。
- 深灰色 - 已安装但禁用接口。
- 红色 - 接口的运行状态有问题。
- 浅灰色 - 未安装接口。



注释 此列表中不包含在端口通道中充当端口的接口。

- 下半部分包含两个选项卡：**所有接口**和**硬件绕行**。在**所有接口**选项卡上：对于每个接口，您可以启用或禁用接口。您也可以点击**编辑 (Edit)**编辑接口属性，例如速度和接口类型。有关**硬件绕行**，请参阅[硬件旁路对](#)，第 124 页。



注释 如果端口通道 48 集群类型接口不包括任何成员接口，则该接口的**运行状态 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

排除接口故障

错误：交换机转发路径条目数为 **1076**，超出限值 **1024**。如果要添加接口，请减少分配至逻辑设计的共享接口的数量，减少共享接口的逻辑设备的数量或改为使用非共享子接口。如果要删除子接口，您将看到此消息，因为系统不再优化剩余配置以适应交换机转发路径表。有关使用案例删除的故障排除信息，请参阅 **FXOS** 配置指南。使用“交换矩阵互联”项下的“显示详细信息”查看当前交换机转发路径条目计数。

如果在尝试从逻辑设备删除共享子接口时看到此错误，则是因为新配置未遵循此准则中有关共享子接口的相关规定：结合使用相同集合的子接口和同组逻辑设备。如果从一个逻辑设备删除共享子接口，则最终可能生成更多 VLAN 组，并因此降低转发表的使用效率。要解决此问题，需要使用 CLI 同时添加和删除共享子接口，以便维护同组逻辑设备的相同集合的子接口。

有关详细信息，请参阅以下场景。这些场景从以下接口和逻辑设备开始：

- 同一父接口上设置的共享子接口：端口通道 1.100 (VLAN 100)、端口通道 1.200 (VLAN 200)、端口通道 1.300 (VLAN 300)
- 逻辑设备组：LD1、LD2、LD3 和 LD4

场景 1：从一个逻辑设备上删除子接口，但将其分配至其他逻辑设备

不删除子接口。相反，只需在应用配置中禁用此子接口即可。如果必须删除子接口，一般情况下需要减少共享接口的数量，以继续适应转发表。

场景 2：从一个逻辑设备上删除集合中的所有子接口

从 CLI 上的逻辑设备上删除集合中的所有子接口，然后保存配置以同步删除信息。

1. 查看 VLAN 组（供参考）。在以下输出中，组 1 包括 VLAN 100、200 和 300，表示 3 个共享子接口。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status      INTF      Vlan Status
1    1         configured  100      100 present
      200      200 present
      300      300 present
2048 512       configured  0        0 present
2049 511       configured  0        0 present
firepower(fxos)# exit
firepower#
```

2. 查看分配至要更改的逻辑设备的共享子接口。

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # show external-port-link
```

External-Port Link:				
Name	Description	Port or Port Channel Name	Port Type	App Name
Ethernet14_ftd		Ethernet1/4	Mgmt	ftd
PC1.100_ftd		Port-channel1.100	Data Sharing	ftd
PC1.200_ftd		Port-channel1.200	Data Sharing	ftd
PC1.300_ftd		Port-channel1.300	Data Sharing	ftd

3. 从逻辑设备上删除子接口，然后保存配置。

```
firepower /ssa/logical-device # delete external-port-link PC1.100_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.200_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

如果您在操作过程中提交了配置，则最终将生成 2 个 VLAN 组，这可能产生交换机转发路径错误并阻止您保存配置。

场景 3：从组中的所有逻辑设备上删除子接口

从 CLI 上组中的所有逻辑设备上删除子接口，然后保存配置以同步删除信息。例如：

1. 查看 VLAN 组（供参考）。在以下输出中，组 1 包括 VLAN 100、200 和 300，表示 3 个共享子接口。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status      INTF          Vlan Status
1    1         configured  100           100 present
      200       200 present
      300       300 present
2048 512       configured  0             0 present
2049 511       configured  0             0 present
```

2. 查看分配至每个逻辑设备的接口，并注意通用共享子接口。如果这些子接口在同一父接口上，则它们属于一个 VLAN 组，应与 **show ingress-vlan-groups** 列表相匹配。在 Firepower 机箱管理器中，您可以将鼠标悬停在每个共享子接口上，以查看这些子接口分配至哪些实例。

图 1: 每个共享接口的实例数

Interface	Type	Admin Speed	Operational Speed	Instances	VLAN
MGMT	Management				
Port-channel1	data	1gbps	1gbps		
Port-channel1.100	data-sharing			LD4...	100
Port-channel1.200	data-sharing			LD4...	
Port-channel1.300	data-sharing			LD4...	300
Ethernet1/3					
Port-channel2	data	1gbps	1gbps		

Interface is shared by 4 instances:
LD4
LD3
LD2
LD1

在 CLI 上，可以查看所有逻辑设备的特征，包括已分配的接口。

```
firepower# scope ssa
firepower /ssa # show logical-device expand

Logical Device:
  Name: LD1
  Description:
  Slot ID: 1
  Mode: Standalone
  Oper State: Ok
  Template Name: ftd

  External-Port Link:
    Name: Ethernet14_ftd
    Port or Port Channel Name: Ethernet1/4
    Port Type: Mgmt
    App Name: ftd
    Description:

    Name: PC1.100_ftd
    Port or Port Channel Name: Port-channel1.100
    Port Type: Data Sharing
    App Name: ftd
    Description:

    Name: PC1.200_ftd
    Port or Port Channel Name: Port-channel1.200
    Port Type: Data Sharing
    App Name: ftd
    Description:

  System MAC address:
    Mac Address
    -----
    A2:F0:B0:00:00:25

    Name: PC1.300_ftd
    Port or Port Channel Name: Port-channel1.300
    Port Type: Data Sharing
    App Name: ftd
    Description:

[...]

  Name: LD2
```

```
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:

  System MAC address:
    Mac Address
    -----
    A2:F0:B0:00:00:28

  Name: PC1.300_ftd
  Port or Port Channel Name: Port-channel1.300
  Port Type: Data Sharing
  App Name: ftd
  Description:
```

[...]

```
Name: LD3
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:
```

```

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:2B

Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:

[...]

Name: LD4
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
Name: Ethernet14_ftd
Port or Port Channel Name: Ethernet1/4
Port Type: Mgmt
App Name: ftd
Description:

Name: PC1.100_ftd
Port or Port Channel Name: Port-channel1.100
Port Type: Data Sharing
App Name: ftd
Description:

Name: PC1.200_ftd
Port or Port Channel Name: Port-channel1.200
Port Type: Data Sharing
App Name: ftd
Description:

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:2E

Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:

[...]

```

3. 从每个逻辑设备上删除子接口，然后保存配置。

```

firepower /ssa # scope logical device LD1
firepower /ssa/logical-device # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD2
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD3
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd

```

```

firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD4
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #

```

如果您在操作过程中提交了配置，则最终将生成 2 个 VLAN 组，这可能产生交换机转发路径错误并阻止您保存配置。

场景 4：将子接口添加至一个或多个逻辑设备

在 CLI 中将子接口添加至组中的所有逻辑设备，然后保存配置以同步添加信息。

1. 将子接口添加至每个逻辑设备，然后保存配置。

```

firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channell.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD2
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channell.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD3
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channell.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD4
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channell.400
ftd
firepower /ssa/logical-device/external-port-link* # commit-buffer
firepower /ssa/logical-device/external-port-link #

```

如果您在操作过程中提交了配置，则最终将生成 2 个 VLAN 组，这可能产生交换机转发路径错误并阻止您保存配置。

2. 您可以检查端口通道 1.400 VLAN ID 已添加至 VLAN 组 1。

```

firepower /ssa/logical-device/external-port-link # connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID   Status      INTF          Vlan Status
1    1          configured  200 present
100  present
300  present
400  present
2048 512        configured  0 present
2049 511        configured  0 present
firepower(fxos)# exit
firepower /ssa/logical-device/external-port-link #

```

接口历史

功能名称	平台版本	功能信息
用于容器实例的 VLAN 子接口	2.4.1	<p>要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。</p> <p>注释 要求使用 6.3 或更高版本的 FTD。</p> <p>新增/修改的菜单项： 接口 > 所有接口 > 添加新下拉菜单 > 子接口</p> <p>新增/修改的 Firepower 管理中心菜单项： 设备 > 设备管理 > 编辑图标 > 接口选项卡</p>
用于容器实例的数据共享接口	2.4.1	<p>要确保灵活使用物理接口，可以在多个实例之间共享接口。</p> <p>注释 要求使用 6.3 或更高版本的 FTD。</p> <p>新增/修改的菜单项： 接口 > 所有接口 > 类型</p>
支持保存模式下的数据 Etherchannel	2.4.1	<p>现在可以将数据和数据共享 Etherchannel 设置为“主用” LACP 模式或“保持”模式。其他类型 Etherchannel 仅支持“主用”模式。</p> <p>新增/修改的菜单项： 接口 > 所有接口 > 编辑端口通道 > 模式</p>
支持 FTD 内联集中的 Etherchannel	2.1.1	<p>现在可以使用 FTD 内联集中的 EtherChannel。</p>
FTD 支持的内联集链路状态传播	2.0.1	<p>当您在 FTD 应用中配置内联集并启用链路状态传播时，FTD 会向 FXOS 机箱发送内联集成员身份。链路状态传播意味着，当内联集的一个接口断开时，机箱将自动关闭内联接口对的第二个接口。</p>

功能名称	平台版本	功能信息
FTD 支持的硬件绕行网络模块	2.0.1	<p>硬件绕行确保流量在断电期间继续在接口对之间流动。在软件或硬件发生故障时，此功能可用于维持网络连接性。</p> <p>新增/修改的 Firepower 管理中心菜单项： 设备 > 设备管理 > 接口 > 编辑物理接口</p>
用于 FTD 的 Firepower 事件类型接口	1.1.4	<p>可以将接口指定为用于 FTD 的 Firepower 事件接口。此接口是 FTD 设备的辅助管理接口。要使用此接口，您必须在 FTD CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅《Firepower 管理中心配置指南》“系统配置”一章中的“管理接口”部分。</p> <p>新增/修改的 Firepower 机箱管理器菜单项： 接口 > 所有接口 > 类型</p>



第 10 章

逻辑设备

- 关于逻辑设备，第 153 页
- 逻辑设备的要求和必备条件，第 161 页
- 适用于逻辑设备的准则和限制，第 164 页
- 添加独立的逻辑设备，第 169 页
- 添加高可用性对，第 173 页
- 添加集群，第 174 页
- 配置 Radware DefensePro，第 187 页
- 管理逻辑设备，第 191 页
- “逻辑设备 (Logical Devices)” 页面，第 197 页
- 站点间集群示例，第 199 页
- 逻辑设备的历史记录，第 202 页

关于逻辑设备

逻辑设备允许您运行一个应用实例（ASA 或 Firepower 威胁防御）和一个可选修饰器应用 (Radware DefensePro) 以形成服务链。

当您添加逻辑设备时，还应定义应用实例类型和版本，分配接口，并配置推送至应用配置的引导程序设置。



注释

对于 Firepower 9300，必须在机箱中的所有模块上都安装同一类型的应用实例（ASA 或 FTD）机箱，目前不支持不同类型的应用实例。请注意，模块可以运行一种应用实例类型的不同版本。

独立和集群逻辑设备

您可以添加以下类型的逻辑设备：

- 独立 - 独立逻辑设备作为独立单元或高可用性对中的单元运行。

- 集群 - 集群逻辑设备允许您将多个单元集合在一起，具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。对于 Firepower 9300，所有三个模块应用实例都属于单个逻辑设备。



注释 对于 Firepower 9300，所有模块都必须属于该集群。不能在一个安全模块上创建独立逻辑设备，而使用剩余的 2 个安全模块创建集群。

容器实例和本地实例

应用实例在以下类型部署中运行：

- 本地实例 - 本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此您仅可安装一个本地实例。
- 容器实例 - 容器实例使用安全模块/引擎的部分资源，因此您可以安装多个容器实例。仅 Firepower 威胁防御支持多实例功能；ASA 对此不予支持。



注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全 Firepower 威胁防御功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。Firepower 威胁防御不支持多情景模式。

对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。

容器实例接口

要确保灵活使用容器实例的物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口（VLAN 或物理接口）。本地实例不得使用 VLAN 子接口或共享接口。请参阅[共享接口可扩展性](#)，第 125 页和[为容器实例添加 VLAN 子接口](#)，第 141 页。

机箱如何将数据包分类

必须对进入机箱的每个数据包进行分类，以便机箱能够确定将数据包发送到哪个实例。

- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。
- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一 MAC 地址的实例。在应用内配置每个接口时，您也可以手动设置 MAC

地址。然而，即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类正确。

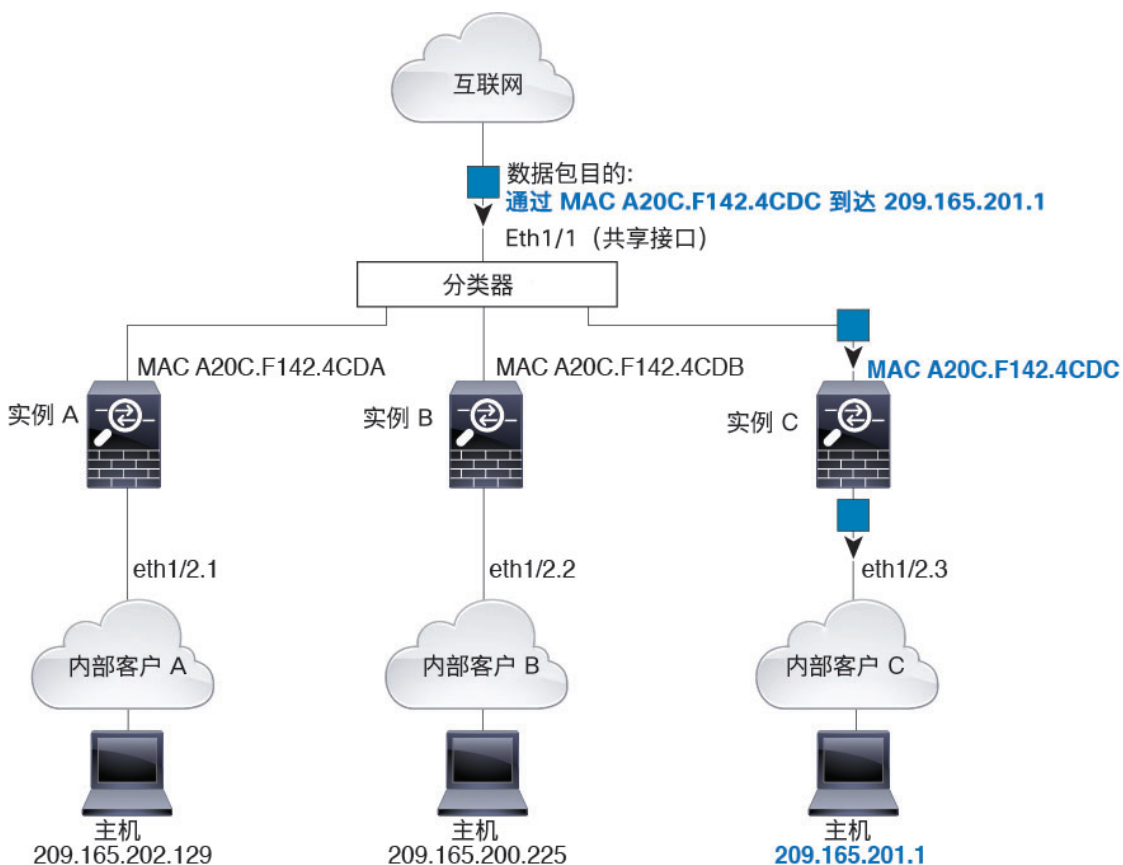


注释 如果目的 MAC 地址为组播或广播 MAC 地址，则数据包会复制并传递到每个实例。

分类示例

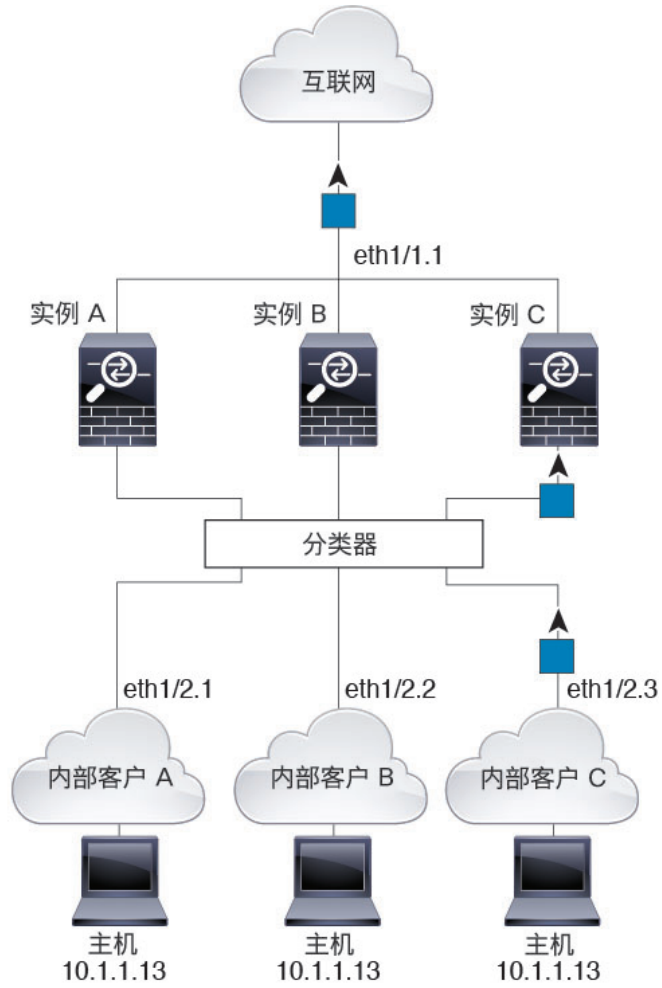
下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

图 2: 使用 **MAC** 地址通过共享接口进行数据包分类



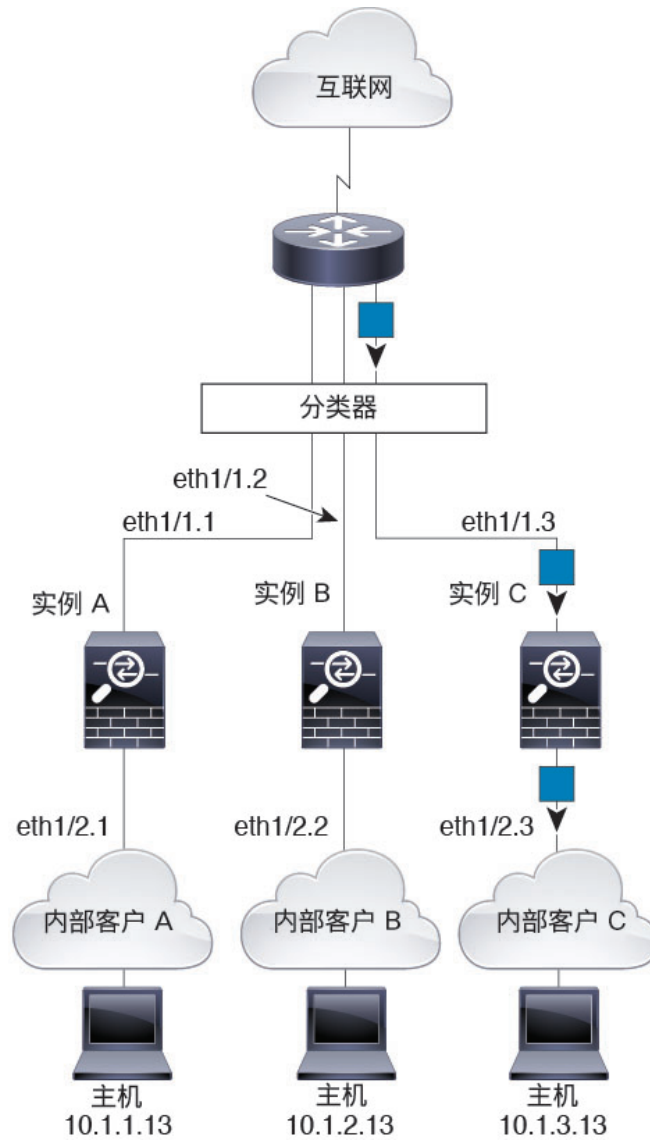
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

图 3: 来自内部网络的传入流量



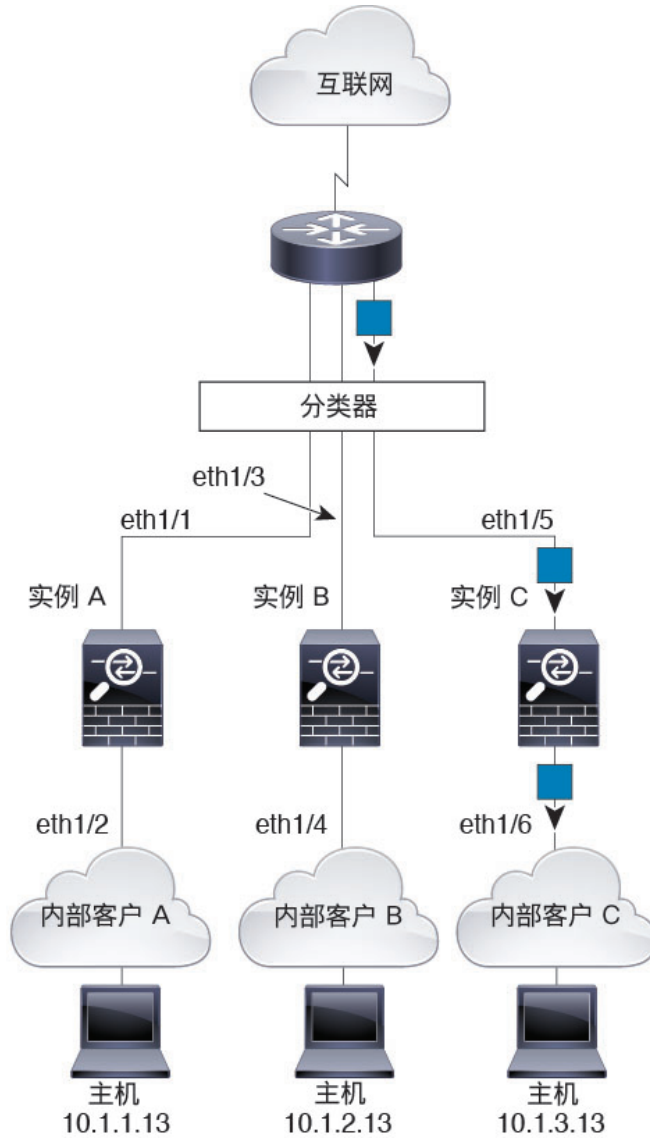
对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

图 4: 透明防火墙实例



对于内联集，必须使用唯一接口，并且这些接口必须为物理接口或 Etherchannel 接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/5，因此分类器会将数据包分配至实例 C。

图 5: FTD 的内联集

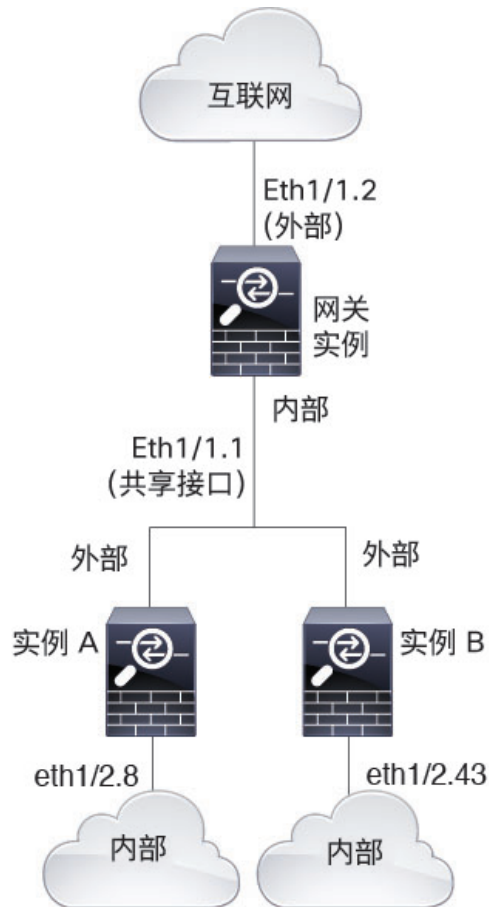


级联容器实例

直接在一个容器实例前面放置另一个实例的行为称为级联容器实例；一个实例的外部接口与另一个实例的内部接口完全相同。如果您希望通过在顶级实例中配置共享参数，从而简化某些实例的配置，则可能要使用级联实例。

下图显示了在网关后有两个实例的网关实例。

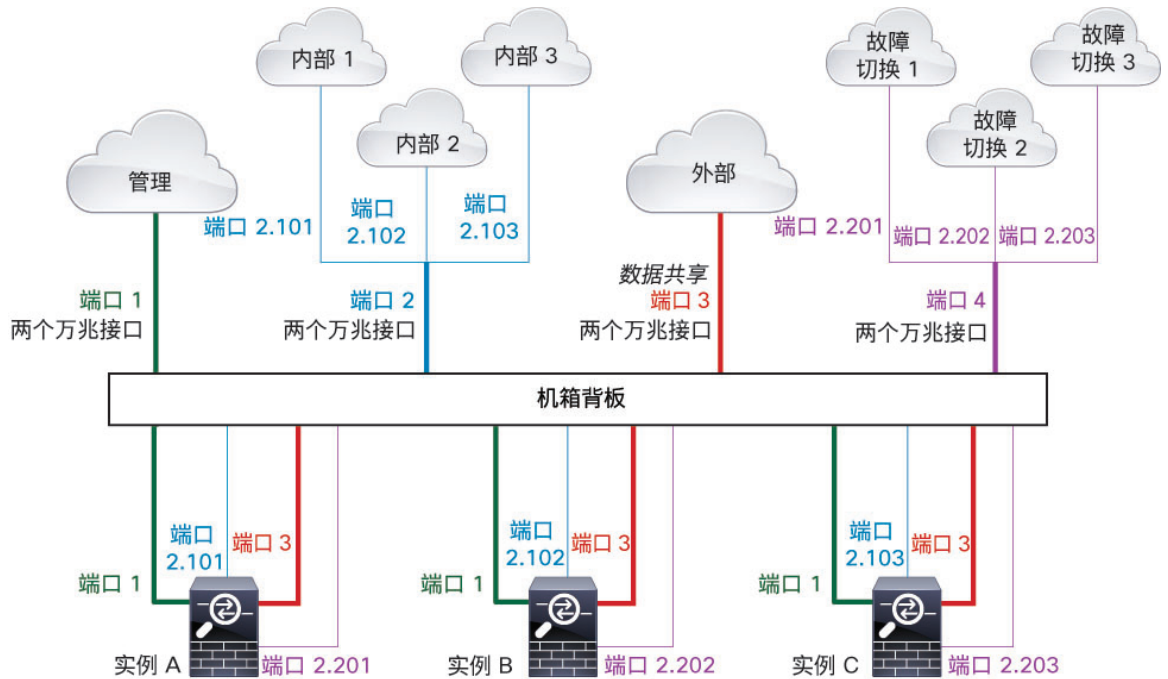
图 6: 级联容器实例



典型多实例部署

以下示例包括路由防火墙模式下的三个容器实例。这三个容器实例包括以下接口：

- 管理 - 所有实例都使用端口通道 1 接口（管理类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一管理网络上的唯一 IP 地址。
- 内部 - 每个实例使用端口通道 2 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。
- 外部 - 所有实例都使用端口通道 3 接口（数据共享类型）。此 EtherChannel 包括两个万兆以太网接口。在每个应用内，该接口都使用同一管理网络上的唯一 IP 地址。
- 故障切换 - 每个实例都使用端口通道 4 上的子接口（数据类型）。此 EtherChannel 包括两个万兆以太网接口。每个子接口位于独立的网络中。



容器实例接口的自动 MAC 地址

FXOS 机箱会自动为容器实例接口自动生成 MAC 地址，以确保各个实例中的共享接口使用唯一的 MAC 地址。

如果您手动为应用中的共享接口分配了一个 MAC 地址，则使用手动分配的 MAC 地址。如果您随后删除了手动 MAC 地址，则会使用自动生成的地址。在出现生成的 MAC 地址与网络中的另一个专用 MAC 地址冲突这种极少发生的情况下，我们建议您在应用中对接口手动设置 MAC 地址。

由于自动生成的地址以 A2 开头，因此您不应该分配以 A2 开头的手动 MAC 地址，以避免出现地址重叠。



注释 即使您未共享子接口，如果您手动配置 MAC 地址，请确保您为同一父接口上的所有子接口使用唯一 MAC 地址，从而确保分类得当。

FXOS 机箱使用以下格式生成 MAC 地址：

A2xx.yyzz.zzzz

其中，xx.yy 是用户定义的前缀或系统定义的前缀，zz.zzzz 是由机箱生成的内部计数器。系统定义的前缀与 IDPROM 中的固化 MAC 地址池中第一个 MAC 地址的 2 个低位字节相匹配。使用 **connect fxos**，然后通过 **show module** 查看 MAC 地址池。例如，如果显示的适用于模块 1 的 MAC 地址范围为 b0aa.772f.f0b0 至 b0aa.772f.f0bf，则系统前缀将是 f0b0。

用户定义的前缀是转换为十六进制的整数。如何使用用户自定义前缀的示例如下：如果将前缀设置为 77，则机箱会将 77 转换为十六进制值 004D (yyxx)。在 MAC 地址中使用时，该前缀会反转 (xxyy)，以便与机箱的本地形式匹配：

A24D.00zz.zzzz

对于前缀 1009 (03F1), MAC 地址为:

A2F1.03zz.zzzz

容器实例资源管理

要指定每个容器实例的资源使用情况,请在 FXOS 中创建一个或多个资源配置文件。部署逻辑设备/应用实例时,请指定想要使用的资源配置文件。资源配置文件会设置 CPU 核心数量;系统会根据核心数量动态分配 RAM,并将每个实例的磁盘空间设为 40 GB。要查看每个型号的可用资源,请参阅[容器实例的要求和必备条件,第 163 页](#)。要添加资源配置文件,请参阅[为容器实例添加资源配置文件,第 120 页](#)。

容器实例与高可用性

您可以在 2 个独立机箱上使用容器实例来实现高可用性;例如,如果您有 2 个机箱,每个机箱设 10 个实例,您可以创建 10 个高可用性对。请注意,不得在 FXOS 中配置高可用性;在应用管理器中配置每个高可用性对。

每个单元都必须使用相同的资源配置文件属性。

每个高可用性对都要求使用专用故障切换链路,并且您不得使用数据共享接口。我们建议您在父接口上创建子接口,并为每个实例分配子接口以用作故障切换链路。



注释 不支持集群。

逻辑设备的要求和必备条件

有关要求 and 必备条件,请参阅以下章节。

集群要求和必备条件

集群型号支持

- Firepower 9300 上的 ASA - 最多 16 个机箱,最多 16 个模块。支持机箱内、机箱间和站点间集群。
- Firepower 4100 系列上的 ASA - 最多 16 个机箱。支持机箱间和站点间集群。
- Firepower 9300 上的 FTD - 最多 6 个机箱,最多 6 个模块。支持机箱内和机箱间集群。
- Firepower 4100 系列上的 FTD - 最多 6 个机箱,最多 6 个模块。支持机箱间集群。
- Radware DefensePro - 对于包含 ASA 的机箱内集群受支持。
- Radware DefensePro - 支持包含 FTD 的机箱内集群。

机箱间集群硬件和软件要求

集群中的所有机箱：

- 对于 Firepower 4100 系列：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 除进行映像升级外，必须运行完全相同的 FXOS 软件。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨网络 EtherChannel 中。请注意，所有数据接口必须是机箱间集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从从属设备开始，到主设备结束。
- 必须使用同一台 NTP 服务器。对于 Firepower 威胁防御，Firepower 管理中心也必须使用同一 NTP 服务器。请勿手动设置时间。
- ASA：每个 FXOS 机箱都必须注册到许可证颁发机构或卫星服务器。从属设备不会产生额外成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。对于 Firepower 威胁防御，所有许可由 Firepower 管理中心处理。

机箱间集群交换机必备条件

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱上配置集群。
- 有关受支持的交换机列表，请参阅《[思科 FXOS 兼容性](#)》。

调整站点间集群的数据中心互联

您应在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{每个站点的集群成员数量}}{2} \times \text{每个成员的集群控制链路大小}$$

如果各站点的成员数不同，请使用较大的数量进行计算。DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 4 个站点的 2 个成员：
 - 总共 4 个集群成员
 - 每个站点 2 个成员
 - 每个成员 5 Gbps 集群控制链路

保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。

- 对位于 3 个站点的 6 个成员而言，规格加大：
 - 总共 6 个集群成员
 - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
 - 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。

- 位于 2 个站点的 2 个成员：
 - 总共 2 个集群成员
 - 每个站点 1 个成员
 - 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 10 Gbps (1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps))。

容器实例的要求和必备条件

受支持应用类型

- Firepower 威胁防御

FTD：每个型号的最大容器实例数和资源容量

对于每个容器实例，您可以指定要分配至实例的 CPU 核心数量。系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。

表 10: 每个型号的最大容器实例数和资源容量

型号	最大容器实例数	可用 CPU 核心	可用 RAM	可用磁盘空间
Firepower 4110	3	22	53 GB	125.6 GB
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4150	7	86	222 GB	311.8 GB
Firepower 9300 SM-24 安全模块	7	46	226 GB	656.4 GB
Firepower 9300 SM-36 安全模块	11	70	222 GB	640.4 GB
Firepower 9300 SM-44 安全模块	14	86	218 GB	628.4 GB

适用于逻辑设备的准则和限制

有关准则和限制，请参阅以下章节。

一般准则和限制

防火墙模式

您可以在 FTD 和 ASA 的引导程序配置中将防火墙模式设置为路由或透明模式。

高可用性

- 在应用配置中配置高可用性。
- 可以将任何数据接口用作故障切换和状态链路。不支持数据共享接口。
- 有关详细信息，请参阅“高可用性”的应用配置指南一章

多实例和情景模式

- 仅 ASA 支持多情景模式。
- 部署后，请在 ASA 中启用多情景模式。
- 包含容器实例的多实例功能仅适用于 FTD。
- 对于容器实例，您可以将每个共享接口分配至最多 14 个容器实例。
- 对于给定的容器实例，您可以分配最多 10 个共享接口。
- 对于 FTD 容器实例，单个 Firepower 管理中心必须管理安全模块/引擎上的所有实例。
- 对于 FTD 容器实例，不支持以下功能：
 - SSL 硬件加速
 - 集群
 - Radware DefensePro 链路修饰器
 - FMC 备份和恢复
 - FMC UCAPL/CC 模式

集群准则和限制

机箱间集群的交换机

- 对于 ASR 9006，如果要设置非默认 MTU，请将 ASR 接口 MTU 设置为高于集群设备 MTU 14 个字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 ASR IPv4 MTU 匹配。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。
- 当发现交换机上跨网络 EtherChannel 的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。
- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 有些交换机不支持 LACP 动态端口优先级（活动链路和备用链路）。您可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。
- 集群控制链路路径上的交换机不应验证第 4 层校验和。集群控制链路上的重定向流量没有正确的第 4 层校验和。交换机验证第 4 层校验和可能导致流量被丢弃。
- 端口通道绑定中断时间不得超过配置的 **keepalive** 间隔。
- 在 Supervisor 2T EtherChannel 上，默认的散列值分配算法是自适应算法。为了避免 VSS 设计中的非对称流量，请将连接到集群设备的端口通道上的散列算法更改为固定：

```
router(config)# port-channel id hash-distribution fixed
```

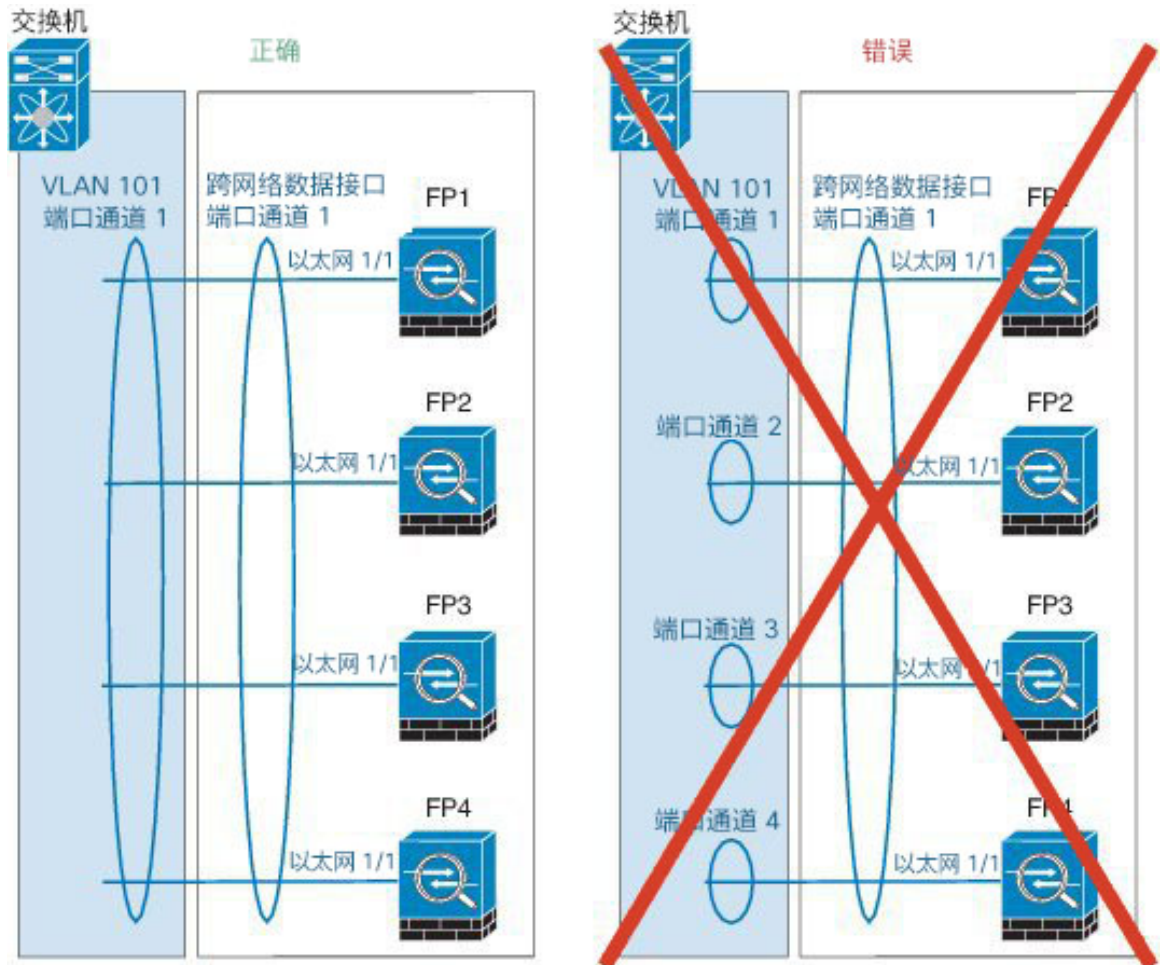
请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

机箱间集群的 EtherChannel

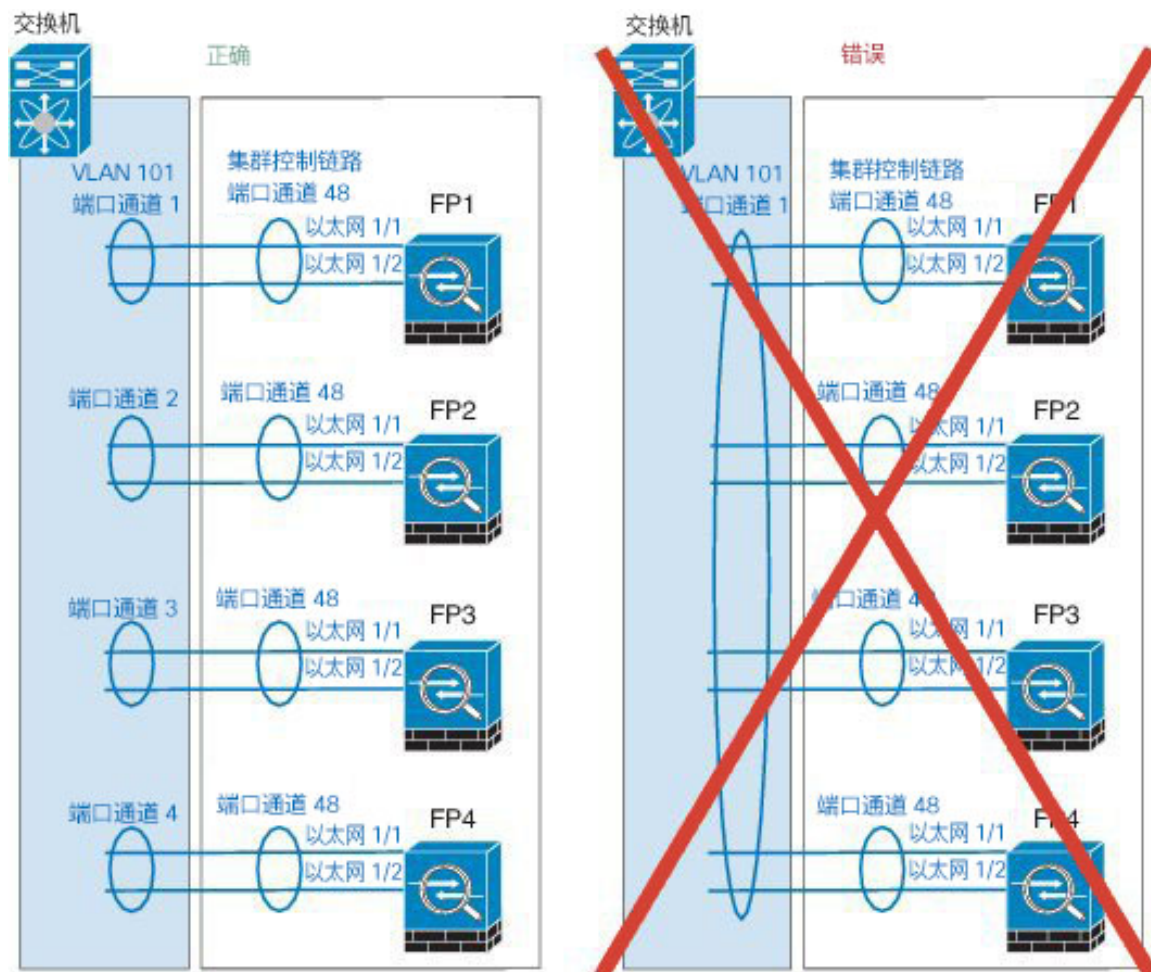
- 为了连接交换机，请将 EtherChannel 模式设置为 Active；Firepower 4100/9300 机箱不支持 ON 模式，甚至对于集群控制链路也是如此。
- 默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。
- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接集群设备 EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac**

persistent timer 命令设置为足够大的值，以将重载时间计算在内；例如，可将其设置为 8 分钟，或设置为 0 以表示无穷大。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。

- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨网络 EtherChannel 和设备本地 EtherChannel 适当地配置交换机。
- 跨网络 EtherChannel - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



站点间集群

请参阅有关站点间集群的以下准则：

- 集群控制链路的延迟必须小于 20 微秒往返时间 (RTT)。
- 集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，您应使用专用链路。
- 请勿配置连接再均衡；您不需要将连接再均衡到位于不同站点的集群成员。
- 对于传入连接而言，位于多个站点的成员之间的集群实施没有区别；因此，给定连接的角色可以跨越所有站点。这是预期行为。但是，如果您启用导向器本地化，系统将始终从连接所有者所在同一站点选择本地导向器角色（根据站点 ID）。此外，如果原始所有者发生故障，本地导向器将在同一站点选择新的连接所有者（注意：如果不同站点间的流量非对称，且原始所有者发生故障后远程站点继续发出流量，则远程站点设备可能成为新的所有者，但条件是该设备在重新托管期间接收到数据包。）。
- 对于导向器本地化，以下流量类型不支持本地化：NAT 或 PAT 流量；SCTP 检查的流量；分段所有者查询。

- 对于透明模式，如果集群布置于内部和外部路由器对之间（AKA 南北插入），您必须确保两个内部路由器共享一个 MAC 地址，两个外部路由器共享一个 MAC 地址。当位于站点 1 的集群成员将连接转发到位于站点 2 的成员时，目的 MAC 地址会被保留。如果该 MAC 地址与位于站点 1 的路由器相同，则数据包只会到达位于站点 2 的路由器。
- 对于透明模式，如果集群布置于每个站点上的数据网络和网关路由器之间，用作内部网络之间的防火墙（AKA 东西插入），则每个网关路由器都应使用 HSRP 等第一跳冗余协议 (FHRP) 在每个站点提供相同的虚拟 IP 和 MAC 目的地址。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术扩展到多个站点。您需要创建过滤器，阻止发往本地网关路由器的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的网关路由器，则您需要删除所有过滤器，使流量能够成功到达另一站点的网关。
- 对于使用跨网络 EtherChannel 的路由模式，请配置站点特定的 MAC 地址。使用 OTV 或类似技术跨站点扩展数据 VLAN。您需要创建过滤器，阻止发往全局 MAC 地址的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群，则您需要删除所有过滤器，使流量能够成功到达另一站点的集群设备。当站点间集群作为扩展网段的第一跳路由器时，不支持动态路由。

其他规定

- 将设备添加到现有集群时或重新加载设备时，会有限地暂时丢弃数据包/断开连接；这是预期行为。在某些情况下，丢弃的数据包可能会挂起连接；例如，丢弃 FTP 连接的 FIN/ACK 数据包会使 FTP 客户端挂起。在此情况下，您需要重新建立 FTP 连接。
- 如果使用连接到跨网络 EtherChannel 接口的 Windows 2003 服务器，当系统日志服务器端口关闭且服务器未限制 ICMP 错误消息时，会有大量 ICMP 消息被发回集群。这些消息可能会导致集群的某些设备出现高 CPU 问题，从而可能影响性能。因此，我们建议您限制 ICMP 错误信息。
- 我们建议将 EtherChannel 连接到 VSS 或 vPC，以实现冗余。
- 在机箱内，您不能对某些安全模块进行集群，也不能在单机模式下运行其他安全模块；必须在集群内包含所有安全模块。

默认值

- 默认情况下，集群运行状况检查功能处于启用状态，保持时间为 3 秒。默认情况下，在所有接口上启用接口运行状况监控。
- 出现故障的集群控制链路的集群自动重新加入功能设置为无限次尝试，每隔 5 分钟进行一次。
- 出现故障的数据接口的集群自动重新加入功能设置为尝试 3 次，每 5 分钟一次，递增间隔设置为 2。
- 对于 HTTP 流量，默认启用 5 秒的连接复制延迟。

添加独立的逻辑设备

独立逻辑设备可以单独或作为高可用性单元使用。有关高可用性的详细信息，请参阅[添加高可用性对](#)，第 173 页。

添加独立 ASA

独立逻辑设备可单独使用，也可在高可用性对中使用。在 Firepower 9300 等多模块设备上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

您可以通过 Firepower 4100/9300 机箱部署一个路由或透明防火墙模式的 ASA。

对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅[从 Cisco.com 下载映像](#)，第 38 页），然后将映像上传到 Firepower 4100/9300 机箱（请参阅[将映像上传到 Firepower 安全设备](#)，第 38 页）。



注释 对于 Firepower 9300，必须在机箱中的所有模块上都安装同一类型的应用实例（ASA 或 FTD）机箱，目前不支持不同类型的应用实例。请注意，模块可以运行一种应用实例类型的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口（并且在[接口选项卡](#)的顶部显示为 **MGMT**）不同。

过程

步骤 1 选择逻辑设备。

逻辑设备页面显示机箱上的逻辑设备列表。

步骤 2 点击 **Add Device**（添加设备）。

系统将显示 **Add Device** 对话框。

步骤 3 对于设备名称 (**Device Name**)，请为逻辑设备提供一个名称。

此名称由 Firepower 4100/9300 机箱 管理引擎用于配置管理设置和分配接口；它不是在 安全模块/引擎 配置中使用的设备名称。

步骤 4 对于模板 (**Template**)，请选择思科自适应安全设备 (**Cisco Adaptive Security Appliance**)。

步骤 5 选择映像版本。

步骤 6 在设备模式 (**Device Mode**) 中，点击独立 (**Standalone**) 单选按钮。

步骤 7 点击确定 (**OK**)。

屏幕会显示调配 - 设备名称 (*Provisioning - device name*) 窗口。

步骤 8 展开数据端口 (**Data Ports**) 区域，然后点击要分配给设备的每个端口。

步骤 9 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。出于正常运行目的，可以更改应用 CLI 配置中的大多数数值。

步骤 10 在一般信息 (**General Information**) 选项卡上，完成下列操作：

- a) (在 Firepower 9300 等多模块设备上) 在安全模块选择下，点击您想用于此逻辑设备的安全模块。
- b) 选择管理接口。
- c) 选择管理接口：地址类型、仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- d) 配置管理 IP 地址。
- e) 输入网络掩码 (**Network Mask**) 或前缀长度 (**Prefix Length**)。
- f) 输入网络网关 (**Network Gateway**) 地址。

步骤 11 点击设置选项卡。

步骤 12 输入并确认管理员用户和启用密码的密码。

预配置的 ASA 管理员用户和启用密码在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

步骤 13 选择防火墙模式：路由 或透明。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

步骤 14 点击确定 (**OK**) 关闭配置对话框。

步骤 15 点击保存 (**Save**)。

机箱通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定的安全模块/引擎来部署逻辑设备。

步骤 16 部署逻辑设备后，您可以选择安装第三方 Radware DefensePro 虚拟平台，作为位于设备前面的 DDoS 检测和缓解服务，请参阅[关于 Radware DefensePro](#)，第 187 页。

添加独立的 Firepower 威胁防御

独立逻辑设备可单独使用，也可在高可用性对中使用。在 Firepower 9300 等多模块设备上，可以配置集群或独立设备。集群必须使用所有模块，因此无法将双模块集群和独立设备进行混用和搭配。

可以在某些模块上使用本地实例，在其他模块上使用容器实例。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅[从 Cisco.com 下载映像](#)，第 38 页），然后将映像上传到 Firepower 4100/9300 机箱（请参阅[将映像上传到 Firepower 安全设备](#)，第 38 页）。



注释 对于 Firepower 9300，必须在机箱中的所有模块上都安装同一类型的应用实例（ASA 或 FTD）机箱，目前不支持不同类型的应用实例。请注意，模块可以运行一种应用实例类型的不同版本。

- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口（并且在[接口](#)选项卡的顶部显示为 **MGMT**）不同。
- 您还必须至少配置一个数据类型的接口。或者，您也可以创建 Firepower 事件接口，传输所有事件流量（例如 Web 事件）。有关详细信息，请参阅[接口类型](#)，第 123 页。
- 对于容器实例，如果您不想使用默认配置文件，则请根据[为容器实例添加资源配置文件](#)，第 120 页添加资源配置文件。
- 对于容器实例，在首次安装容器实例之前，必须重新初始化安全模块/引擎，以保证磁盘具有正确的格式。选择[安全模块](#)或[安全引擎](#)，然后点击[重新初始化安全模块/引擎](#)图标。首先删除现有逻辑设备，然后将其重新安装为新设备，这会丢失任何本地应用配置。如果要使用容器实例替换本地实例，则在任何情况下都需要删除本地实例。无法自动将本地实例迁移到容器实例。有关详细信息，请参阅[重新初始化安全模块/引擎](#)，第 210 页。

过程

步骤 1 选择逻辑设备。

逻辑设备页面显示机箱上的逻辑设备列表。

步骤 2 点击 **Add Device**（添加设备）。

系统将显示 **Add Device** 对话框。

步骤 3 对于设备名称 (Device Name)，请为逻辑设备提供一个名称。

此名称由 Firepower 4100/9300 机箱 管理引擎用于配置管理设置和分配接口；它不是在 [安全模块/引擎](#) 配置中使用的设备名称。

步骤 4 对于模板 (Template)，请选择思科 **Firepower 威胁防御 (Cisco Firepower Threat Defense)**。

步骤 5 选择映像版本。


步骤 6 选择实例类型：容器或本地。


步骤 7 在设备模式 (Device Mode) 中，点击独立 (Standalone) 单选按钮。

步骤 8 点击确定 (OK)。

屏幕会显示调配 - 设备名称 (*Provisioning - device name*) 窗口。

步骤 9 展开数据端口区域，然后点击要分配给设备的每个接口。

仅可向一个容器实例分配最多 10 个数据共享接口。此外，可以将每个数据共享接口分配至最多 14 个容器实例。数据共享接口以共享图标（）表示。

具有硬件绕行功能的端口使用以下图标显示：。如果您未同时分配一个硬件绕行对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件绕行功能，因此如果您愿意，可以分配单个接口。

步骤 10 点击屏幕中心的设备图标。

系统将显示对话框，可以在该对话框中配置初始引导程序设置。这些设置仅用于仅初始部署或灾难恢复。出于正常运行目的，可以更改应用 CLI 配置中的大多数值。

步骤 11 在一般信息 (General Information) 选项卡上，完成下列操作：

- （在 Firepower 9300 等多模块设备上）在安全模块选择下，点击您想用于此逻辑设备的安全模块。
- 选择管理接口。
- 对于容器实例，指定资源配置文件。

如果您稍后分配一个不同的资源配置文件，则实例将重新加载，这可能需要大约 5 分钟的时间。请注意，对于已建立的高可用性对，如果分配不同大小的资源配置文件，请务必尽快确保所有成员大小一致。

- 选择管理接口：地址类型、仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- 配置管理 IP 地址。
- 输入网络掩码 (Network Mask) 或前缀长度 (Prefix Length)。
- 输入网络网关 (Network Gateway) 地址。

步骤 12 在设置 (Settings) 选项卡上，完成下列操作：

- 在注册密钥 (Registration Key) 字段中，输入 Firepower 管理中心和设备在注册期间共享的密钥。
- 在密码 (Password) 字段中，输入设备密码。
- 在 Firepower 管理中心 IP (Firepower Management Center IP) 字段中，输入执行管理的 Firepower 管理中心的 IP 地址。
- 是否允许 FTD SSH 会话专家模式：是或否。专家模式提供 FTD shell 访问权限以确保实现高级故障排除。

对于此选项，如果您选择是，拥有直接从 SSH 会话访问容器实例的权限的用户可以输入专家模式。如果您选择否，只有拥有从 FXOS CLI 访问容器实例的权限的用户可以输入专家模式。我们建议选择否以加强实例之间的隔离。

仅当书面程序指出必须使用或思科技术支持中心要求使用专家模式时，才使用专家模式。要进入此模式下，请在 FTD CLI 中使用 **expert** 命令。

- 在搜索域 (Search Domains) 字段中，输入设备的搜索域列表（用逗号隔开）。
- 选择防火墙模式：透明或路由。
- 在 DNS 服务器 (DNS Servers) 字段中，输入设备使用的 DNS 服务器列表，用逗号隔开。
- 在完全限定主机名 (Fully Qualified Hostname) 字段中，输入威胁防御设备的完全限定名称。
- 选择应该发送 Firepower 事件的事件接口。如果未指定，将使用管理接口。

要指定发送 Firepower 事件所用的接口，必须将接口配置为 *firepower-eventing* 接口。有关详细信息，请参阅[关于 Firepower 接口](#)，第 123 页。

步骤 13 在协议 (Agreement) 选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 14 点击**确定 (OK)** 关闭配置对话框。

步骤 15 点击**保存 (Save)**。

机箱通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定的安全模块/引擎来部署逻辑设备。

步骤 16 部署逻辑设备后，您可以选择安装第三方 Radware DefensePro 虚拟平台，作为位于设备前面的 DDoS 检测和缓解服务，请参阅[关于 Radware DefensePro](#)，第 187 页。

容器实例不支持 Radware DefensePro。

添加高可用性对

Firepower 威胁防御或 ASA 高可用性（也称为故障切换）是在应用中配置，而不是在 FXOS 中配置。但为了让您的机箱做好配置高可用性的准备，请参阅以下步骤。

开始之前

- 有关高可用性系统要求，请参阅“高可用性”的应用配置指南一章。

过程

步骤 1 每个逻辑设备应位于单独的机箱上；不建议为 Firepower 9300 配置机箱内高可用性，而且可能不支持此功能。

步骤 2 将相同的接口分配给各个逻辑设备。

步骤 3 为故障切换和状态链路分配 1 个或 2 个数据接口。

这些接口用于交换 2 个机箱之间的高可用性流量。我们建议您将一个 10 GB 数据接口用于组合的故障切换和状态链路。如果您有可用的接口，可以使用单独的故障切换和状态链路；状态链路需要的带宽最多。不能将管理类型的接口用于故障切换或状态链路。我们建议您在机箱之间使用一个交换机，并且不将同一网段中的其他任何设备作为故障切换接口。

对于容器实例，故障切换链路不支持数据共享接口。我们建议您在父接口或 EtherChannel 上创建子接口，并为每个实例分配子接口以用作故障切换链路。请注意，您必须将同一父接口上的所有子接口用作故障切换链路。不得将一个子接口用作故障切换链路，然后将其他子接口（或父接口）用作常规数据接口。

步骤 4 在逻辑设备上启用高可用性。

步骤 5 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在主用设备上执行更改。

注释 对于 ASA，如果在 FXOS 中移除一个接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中移除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

添加集群

通过集群，您可以将多台设备组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。包含多个模块的 Firepower 9300 支持机箱内集群，在此，即您可以将单个机箱中的所有模块分组到一个集群中。您还可使用将多个机箱组合在一起的机箱间集群；机箱间集群是单模块设备（例如 Firepower 4100 系列）的唯一选择。

关于集群 Firepower 4100/9300 机箱

集群由充当单一逻辑单元的多个设备组成。在 Firepower 4100/9300 机箱上部署集群时，它执行以下操作：

- 为设备间通信创建集群控制链路（默认情况下，使用端口通道 48）。对于机箱内集群（仅限 Firepower 9300），此链路利用 Firepower 9300 背板进行集群通信。对于机箱间集群，需要手动将物理接口分配到此 EtherChannel 以进行机箱间通信。
- 在应用中创建集群引导程序配置。

在部署集群时，Firepower 4100/9300 机箱管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。如果您需要自定义集群环境，可以在应用内对引导程序配置的某些用户可配置部分进行配置。

- 将数据接口作为跨网络接口分配给集群。

对于机箱内集群，跨网络接口不仅限于 EtherChannel，与机箱间集群类似。Firepower 9300 管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。对于机箱间集群，必须对所有数据接口使用跨网络 EtherChannel。



注释 除管理接口以外，不支持单个接口。

- 向集群中的所有设备分配管理接口。

以下部分提供有关集群概念和实施的更多详细信息。

主设备角色和辅助设备角色

集群的一个成员是主设备。系统自动确定主设备。所有其他成员都是辅助设备。

您必须仅在主设备上执行所有配置；然后，配置将复制到辅助设备。

集群控制链接

集群控制链路使用端口通道 48 接口自动进行创建。对于机箱内集群，此接口未设任何成员接口。对于机箱间集群，必须将一个或多个接口添加到 EtherChannel。此集群类型 EtherChannel 利用 Firepower 9300 背板进行机箱内集群的集群通信。

对于包含 2 个成员的机箱间集群，请勿直接将集群控制链路从一个机箱连接到另一个机箱。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

集群控制链路流量包括控制流量和数据流量。

设定机箱间集群的集群控制链路大小

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

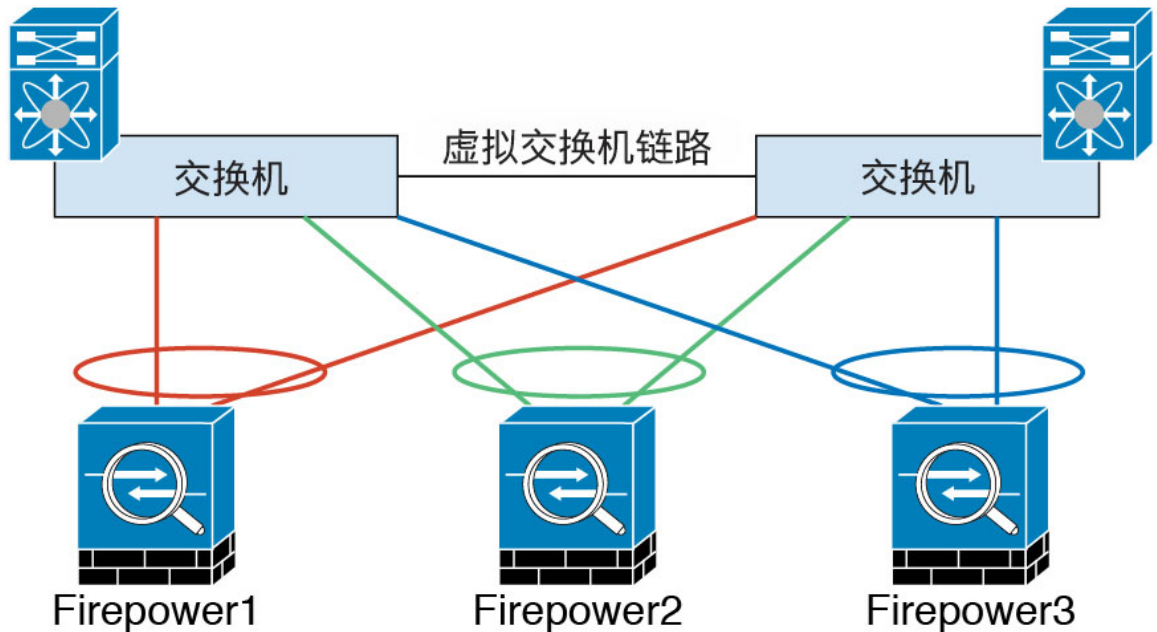
带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。



注释 如果集群中存在大量不对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

机箱间集群的集群控制链路冗余

下图显示了如何在虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。当交换机是 VSS 或 vPC 的一部分时，可以将同一 EtherChannel 中的 Firepower 4100/9300 机箱接口连接到 VSS 或 vPC 中的不同交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台不同的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



机箱间集群的集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成集群控制链路接口 IP 地址：127.2.chassis_id.slot_id。当您部署集群时，您可以自定义此 IP 地址。集群控制链路网络不能包括设备之间的任何路由器；仅可执行第 2 层交换。对于站点间流量，思科建议使用重叠传输虚拟化 (OTV)。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理接口

必须为集群分配管理类型的接口。此接口是相对于跨网络 (Spanned) 接口的特殊单独接口。通过管理接口，可以直接连接到每个设备。

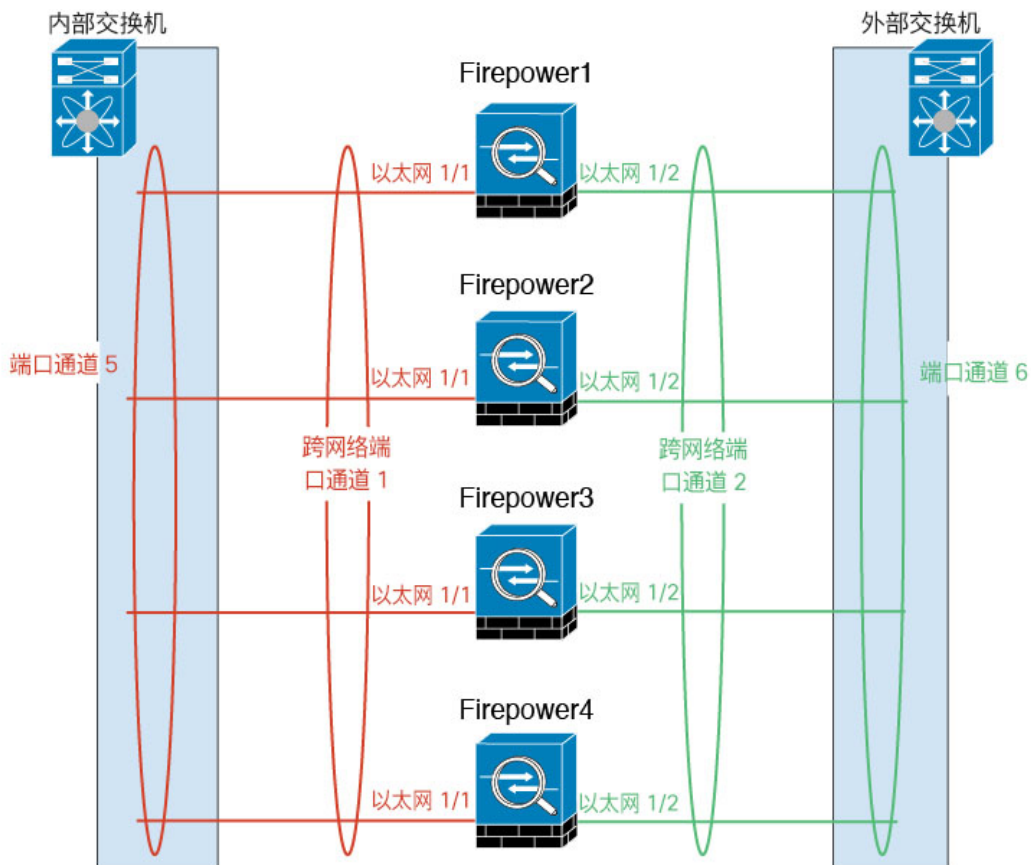
对于 ASA，主集群 IP 地址是始终属于当前主设备的集群的固定地址。您必须配置一个地址范围，使每个设备（包括当前主设备在内）都能使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问权限；当主设备更改时，主集群 IP 地址将转移给新的主设备，使集群管理可以无缝衔接。本地 IP 地址用于路由，在排除故障时也非常有用。例如，可以通过连接到主集群 IP 地址来管理集

群，该地址始终连接到当前主设备。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每个设备都使用本地 IP 地址来连接到服务器。

对于 Firepower 威胁防御，请向同一网络上的每个设备分配管理 IP 地址。将每个设备连接到 FMC 时，请使用这些 IP 地址。

跨网络 EtherChannel

您可以将每个机箱的一个或多个接口组成跨集群中所有机箱的 EtherChannel。EtherChannel 汇聚通道中所有可用活动接口上的流量。在路由模式和透明防火墙模式下均可配置跨网络 EtherChannel。在路由模式下，EtherChannel 配置为具有单个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。负载均衡属于 EtherChannel 固有的基本操作。



站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥集群的作用。

您可以将每个集群机箱配置为属于单独的站点 ID。

站点 ID 与站点特定的 MAC 地址和 IP 地址配合使用。集群发送的数据包使用站点特定的 MAC 地址和 IP 地址，而集群接收的数据包使用全局 MAC 地址和 IP 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。只有使用跨网络 EtherChannel 的路由模式支持站点特定的 MAC 地址和 IP 地址。

站点 ID 还用于使用 LISP 检查、导向器本地化来实现流量移动，以提高性能、减少数据中心的站点间集群的往返时间延迟以及连接的站点冗余，其中流量流的备用所有者始终位于与所有者不同的站点上。

有关站点间集群的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 - [集群要求和必备条件](#)，第 161 页
- 站点间准则 - [集群准则和限制](#)，第 165 页
- 站点间示例 - [站点间集群示例](#)，第 199 页

添加 ASA 集群

您可以将单个 Firepower 9300 机箱添加为机箱内集群，或添加多个机箱以实现机箱间集群。对于机箱间集群，您必须单独配置每个机箱。在一个机箱上添加集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署

创建 ASA 集群

在 Firepower 4100/9300 机箱上部署集群。

对于多情景模式，您必须先部署逻辑设备，然后在 ASA 应用中启用多情景模式。

您可以通过 Firepower 4100/9300 机箱部署一个路由或透明防火墙模式的 ASA。

开始之前

- 您必须启用对 Firepower 9300 机箱中全部 3 个模块插槽的启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
- 在 **接口 (Interfaces)** 选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的 **运行状态 (Operation State)** 将显示为 **失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

过程

步骤 1 部署集群之前，至少添加一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。

部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的 EtherChannel。在每个机箱上添加同一 EtherChannel。将所有集群设备上的成员接口合并到交换机上的单个 EtherChannel 中。有关机箱间集群 EtherChannel 的详细信息，请参阅 [集群准则和限制](#)，第 165 页。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。

对于机箱间集群，在各机箱上添加相同的管理接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口（并且该接口在 **接口选项卡** 的顶部显示为 **MGMT**）不同。

步骤 3 对于机箱间集群，向端口通道 48 添加成员接口，用作集群控制链路。

如果不包含成员接口，那么当您部署逻辑设备时，Firepower 机箱管理器 会认为此集群为机箱内集群，并且不显示**机箱 ID (Chassis ID)** 字段。在各机箱上添加相同的成员接口。 集群控制链路是每个机箱上的设备本地 EtherChannel。在交换机上对每个设备使用单独的 Etherchannel。有关机箱间集群 EtherChannel 的详细信息，请参阅[集群准则和限制](#)，第 165 页。

步骤 4 选择逻辑设备。

逻辑设备页面显示机箱上的逻辑设备列表。

步骤 5 点击 **Add Device**（添加设备）。

系统将显示 **Add Device** 对话框。

步骤 6 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

此名称由 Firepower 4100/9300 机箱 管理引擎用于配置管理设置和分配接口；它不是在 安全模块/引擎 配置中使用的设备名称。

步骤 7 对于**模板 (Template)**，请选择**思科自适应安全设备 (Cisco Adaptive Security Appliance)**。

步骤 8 选择 ASA 映像版本。

步骤 9 在**设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。

步骤 10 点击**新建集群 (Create New Cluster)** 单选按钮。

步骤 11 点击**确定 (OK)**。

如果您配置了任何独立设备，系统将提示您用新集群替代它们。屏幕将显示**调配 - 设备名称 (Provisioning - device name)** 窗口。

默认情况下，所有接口都会分配给集群。

步骤 12 点击屏幕中心的设备图标。

系统将显示 **ASA 配置**对话框，其中**集群信息**选项卡已选定。

步骤 13 在**机箱 ID (Chassis ID)** 字段中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。

步骤 14 对于**站点间集群**，在**站点 ID (Site ID)** 字段中输入此机箱的站点 ID（1 和 8 之间的整数）。

步骤 15 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。

共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 16 设置**集群组名 (Cluster Group Name)**，这是安全模块配置中的集群组名。

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

步骤 17 点击**管理接口 (Management Interface)**，选择您之前创建的管理接口。

步骤 18 （可选）将 **CCL 子网 IP** 设为 *a.b.0.0*。

默认情况下， 集群控制链路使用 127.2.0.0/16 网络。但是，某些网络部署不允许 127.2.0.0/16 流量通过。在这种情况下，请对集群指定唯一网络上的任意 /16 网络地址，环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外。如果将该值设置为 0.0.0.0，则会使用默认网络。

机箱会根据机箱 ID 和插槽 ID 自动生成每台设备的集群控制链路接口 IP 地址：*a.b.chassis_id.slot_id*。

步骤 19 选择管理接口的地址类型 (Address Type)。

此信息用于配置安全模块配置中的管理接口。

- a) 在**管理 IP 池 (Management IP Pool)** 字段中，配置本地 IP 地址池，其中一个地址将分配给接口的每个集群设备，方法是输入以连字符分隔的起始地址和结束地址。

至少包含与集群中的设备数量相同的地址。请注意，对于 Firepower 9300，每台机箱必须包括 3 个地址，即使未填满所有模块插槽。如果计划扩展集群，则应包含更多地址。属于当前主设备的虚拟 IP 地址（称作“主集群 IP 地址”）不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。

- b) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
- c) 输入**网络网关 (Network Gateway)**。
- d) 输入**虚拟 IP 地址 (Virtual IP address)**。

此 IP 地址必须与集群池地址属于同一个网络，但不在地址池中。

步骤 20 点击设置选项卡。

步骤 21 输入并确认管理员用户和启用密码的密码。

预配置的 ASA 管理员用户在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

步骤 22 选择防火墙模式：路由 或透明。

系统仅在初始部署时设置防火墙模式。如果您重新应用引导程序设置，则不会使用此设置。

步骤 23 点击确定 (OK)，可关闭“ASA 配置 (ASA Configuration)”对话框。

步骤 24 点击保存 (Save)。

Firepower 4100/9300 机箱管理引擎通过下载指定的软件版本并向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 25 对于机箱间集群，请将下一个机箱添加到集群。

请确保新机箱上的接口配置相同。您可以导出和导入 FXOS 机箱配置以简化此过程。

- a) 在第一个机箱 Firepower 机箱管理器上，点击右上角的**显示集群详细信息 (Show Cluster Details)** 图标；复制显示的集群配置。
- b) 连接到下一个机箱上的 Firepower 机箱管理器，然后按照此程序添加逻辑设备。
- c) 选择**加入现有集群 (Join an Existing Cluster)**。
- d) 点击**复制配置 (Copy config)** 复选框，然后点击**确定 (OK)**。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
- e) 在**复制集群详细信息 (Copy Cluster Details)** 对话框中，粘贴第一个机箱的集群配置，然后点击**确定 (OK)**。
- f) 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：
 - **机箱 ID (Chassis ID)** - 输入唯一的机箱 ID。

- **站点 ID (Site ID)** - 输入正确的站点 ID。
- **集群密钥 (Cluster Key)** - (未预填充) 输入相同的集群密钥。

点击**确定 (OK)**。

g) 点击**保存**。

步骤 26 连接到主设备 ASA 以自定义集群配置。

添加更多集群成员

添加或替换 ASA 集群成员。




注释

此程序仅适用于添加或替换机箱；如果将模块添加或替换到已启用集群的 Firepower 9300，则该模块将自动添加。

开始之前

- 确保现有集群在此新成员的管理 IP 地址池中有足够的 IP 地址。如果没有，您需要在每个机箱上编辑现有集群引导程序配置，然后才可添加此新成员。此更改将导致重新启动逻辑设备。
- 新机箱上的接口配置必须相同。您可以导出和导入 FXOS 机箱配置以简化此过程。
- 对于多情景模式，在第一个集群成员上的 ASA 应用中启用多情景模式；其他集群成员将自动继承多情景模式配置。

过程

- 步骤 1** 在现有集群机箱 Firepower 机箱管理器上，选择**逻辑设备**打开**逻辑设备**页面。
- 步骤 2** 点击右上角的显示配置图标 ()；复制显示的集群配置。
- 步骤 3** 连接到新机箱上的 Firepower 机箱管理器，然后点击**添加设备**。
- 步骤 4** 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。
- 步骤 5** 对于**模板 (Template)**，请选择**思科自适应安全设备 (Cisco Adaptive Security Appliance)**。
- 步骤 6** 对于**映像版本 (Image Version)**，请选择 ASA 软件版本。
- 步骤 7** 在**设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。
- 步骤 8** 选择**加入现有集群 (Join an Existing Cluster)**。
- 步骤 9** 点击**复制配置 (Copy config)** 复选框，然后点击**确定 (OK)**。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
- 步骤 10** 在**复制集群详细信息 (Copy Cluster Details)** 对话框中，粘贴第一个机箱的集群配置，然后点击**确定 (OK)**。

步骤 11 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：

- **机箱 ID (Chassis ID)** - 输入唯一的机箱 ID。
- **站点 ID (Site ID)** - 输入正确的站点 ID。
- **集群密钥 (Cluster Key)** - (未预填充) 输入相同的集群密钥。

点击确定 (OK)。

步骤 12 点击保存。

添加 Firepower 威胁防御集群

您可以将单个 Firepower 9300 机箱添加为机箱内集群，或添加多个机箱以实现机箱间集群。对于机箱间集群，您必须单独配置每个机箱。在一个机箱上添加集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署

创建 Firepower 威胁防御集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。对于机箱间集群，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

开始之前

- 您必须启用对 Firepower 9300 机箱中全部 3 个模块插槽的启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
- 在**接口 (Interfaces)** 选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

过程

步骤 1 部署集群之前，至少添加一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。

部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的跨网络 EtherChannel。在每个机箱上添加同一 EtherChannel。将所有集群设备上的成员接口合并到交换机上的单个 EtherChannel 中。有关机箱间集群 EtherChannel 的详细信息，请参阅[集群准则和限制](#)，第 165 页。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。

对于机箱间集群，在各机箱上添加相同的管理接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口（并且该接口在**接口**选项卡的顶部显示为 **MGMT**）不同。

步骤 3 对于机箱间集群，向端口通道 48 添加成员接口，用作集群控制链路。

如果不包含成员接口，那么当您部署逻辑设备时，Firepower 机箱管理器 会认为此集群为机箱内集群，并且不显示**机箱 ID (Chassis ID)** 字段。在各机箱上添加相同的成员接口。 集群控制链路是每个机箱上的设备本地 EtherChannel。在交换机上对每个设备使用单独的 Etherchannel。有关机箱间集群 EtherChannel 的详细信息，请参阅**集群准则和限制**，第 165 页。

步骤 4 （可选）添加 Firepower 事件接口。

此接口是 FTD 设备的辅助管理接口。要使用此接口，您必须在 FTD CLI 上配置其 IP 地址和其他参数。例如，您可以将管理流量从活动（例如网络活动）中分隔出来。请参阅 Firepower 威胁防御命令参考中的 **configure network** 命令。

对于机箱间集群，在各机箱上添加相同的事件接口。

步骤 5 选择逻辑设备。

逻辑设备页面显示机箱上的逻辑设备列表。

步骤 6 点击 **Add Device**（添加设备）。

系统将显示 **Add Device** 对话框。

步骤 7 对于**设备名称 (Device Name)**，请为逻辑设备提供一个名称。

此名称由 Firepower 4100/9300 机箱 管理引擎用于配置管理设置和分配接口；它不是在 安全模块/引擎 配置中使用的设备名称。

步骤 8 对于**模板 (Template)**，请选择思科 **Firepower 威胁防御 (Cisco Firepower Threat Defense)**。


步骤 9 选择 Firepower 威胁防御映像版本。

步骤 10 在**设备模式 (Device Mode)** 中，点击**集群 (Cluster)** 单选按钮。

步骤 11 点击**新建集群 (Create New Cluster)** 单选按钮。

步骤 12 点击**确定 (OK)**。

如果您配置了任何独立设备，系统将提示您用新集群替代它们。您会看到**调配-设备名称 (Provisioning - device name)** 窗口。

对于机箱间集群，默认情况下，所有接口都分配给集群。具有硬件绕行功能的端口使用以下图标显示：。如果您未同时分配一个硬件绕行对中的两个接口，则会收到一条警告消息，确认您是故意这样分配。您不需要使用硬件绕行功能，因此如果您愿意，可以分配单个接口。硬件旁路端口不支持机箱间集群，因系统不支持此类端口作为 EtherChannel 成员。机箱间集群不支持硬件旁路端口，因为不支持将其作为 EtherChannel 成员。

步骤 13 点击屏幕中心的设备图标。

此时将显示思科 **Firepower 威胁防御配置 (Cisco Firepower Threat Defense Configuration)** 对话框。

步骤 14 在**集群信息 (Cluster Information)** 选项卡上，填写以下字段：

- 在**机箱 ID (Chassis ID)** 字段中，输入机箱 ID。集群中的每个机箱都必须使用唯一 ID。
- 在**站点 ID** 字段中，对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。此功能仅可使用 Firepower 管理中心 FlexConfig 功能进行配置。

- c) 在**集群密钥 (Cluster Key)** 字段中，为集群控制链路上的控制流量配置身份验证密钥。
共享密钥是长度介于 1 和 63 个字符之间的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。
- d) 设置**集群组名称 (Cluster Group Name)**，即逻辑设备配置中的集群组名称。
名称必须是长度为 1 到 38 个字符的 ASCII 字符串。
- e) 从**管理接口 (Management Interface)** 下拉列表中选择逻辑设备要使用的管理接口。
如果您分配一个支持硬件绕行功能的接口作为管理接口，则会收到一条警告消息，确认您是故意这样分配。

步骤 15 在**设置 (Settings)** 选项卡上，完成下列操作：

- a) 在**注册密钥 (Registration Key)** 字段中，输入注册期间 Firepower 管理中心与集群成员之间要共享的密钥。
- b) 在**密码 (Password)** 字段中，输入集群中管理员用户的密码。
- c) 在**Firepower 管理中心 IP (Firepower Management Center IP)** 字段中，输入执行管理的 Firepower 管理中心的 IP 地址。
- d) 在**搜索域 (Search Domains)** 字段中，输入管理网络的搜索域逗号分隔列表。
- e) 从**防火墙模式 (Firewall Mode)** 下拉列表中选择**透明 (Transparent)** 或**路由 (Routed)**。
- f) 在**DNS 服务器 (DNS Servers)** 字段中，输入 FTD 设备应在管理网络中使用的 DNS 服务器逗号分隔列表。
- g) 在**完全限定主机名 (Fully Qualified Hostname)** 字段中，输入 FTD 设备的完全限定名称。
- h) 从**事件接口 (Eventing Interface)** 下拉列表中，选择发送 Firepower 事件时应当使用的接口。如果未指定，系统将使用管理接口。

要指定发送 Firepower 事件所用的独立接口，必须将接口配置为 *firepower-eventing* 接口。如果您分配一个支持硬件绕行功能的接口作为事件接口，则会收到一条警告消息，以确认您是故意这样分配的。

步骤 16 在**接口信息 (Interface Information)** 选项卡中，为集群中的每个安全模块配置一个管理 IP 地址。从**地址类型 (Address Type)** 下拉列表中选择地址类型，然后为每个安全模块填写以下字段。

注释 您必须为机箱中全部 3 个模块插槽设置 IP 地址，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。

- a) 在**管理 IP (Management IP)** 字段中，配置 IP 地址。
在同一网络上为每个模块指定 IP 地址。
- b) 输入**网络掩码 (Network Mask)** 或**前缀长度 (Prefix Length)**。
- c) 输入**网络网关 (Network Gateway)** 地址。


步骤 17 在**协议 (Agreement)** 选项卡上，阅读并接受最终用户许可协议 (EULA)。

步骤 18 点击**确定 (OK)** 以关闭思科 Firepower 威胁防御配置 (Cisco Firepower Threat Defense Configuration) 对话框。

步骤 19 点击**保存 (Save)**。

Firepower 4100/9300 机箱管理引擎通过下载指定的软件版本并向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 20 对于机箱间集群，将下一个机箱添加到集群中：

- a) 在第一个机箱 Firepower 机箱管理器上，点击右上角的显示配置图标 ()；复制显示的集群配置。
- b) 连接到下一个机箱上的 Firepower 机箱管理器，然后按照此程序添加逻辑设备。
- c) 选择加入现有集群 (**Join an Existing Cluster**)。
- d) 点击复制配置 (**Copy config**) 复选框，然后点击确定 (**OK**)。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
- e) 在复制集群详细信息 (**Copy Cluster Details**) 对话框中，粘贴第一个机箱的集群配置，然后点击确定 (**OK**)。
- f) 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：
 - 机箱 ID (**Chassis ID**) - 输入唯一的机箱 ID。
 - 站点 ID - 对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。此功能仅可使用 Firepower 管理中心 FlexConfig 功能进行配置。
 - 集群密钥 (**Cluster Key**) - （未预填充）输入相同的集群密钥。
 - 管理 IP (**Management IP**) - 将每个模块的管理地址更改为与其他集群成员位于同一网络中的唯一 IP 地址。
 - CCL 子网 IP - 默认情况下，集群控制链路使用 127.2.0.0/16 网络。但是，某些网络部署不允许 127.2.0.0/16 流量通过。在这种情况下，请对集群指定唯一网络上的任意 /16 网络地址，环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外。如果将该值设置为 0.0.0.0，则会使用默认网络。机箱会根据机箱 ID 和插槽 ID 自动生成每台设备的集群控制链路接口 IP 地址：
a.b.chassis_id.slot_id。

点击确定。

- g) 点击保存 (**Save**)。

步骤 21 使用管理 IP 地址将主设备添加到 Firepower 管理中心。

所有集群设备必须位于 FXOS 上成功建立的集群中，才能将它们添加到 Firepower 管理中心。

然后，Firepower 管理中心会自动检测从属设备。

添加更多集群成员

在现有集群中添加或替换 FTD 集群。在 FXOS 中添加新的集群成员时，Firepower 管理中心会自动添加该成员。



注释 此程序中的 FXOS 步骤仅适用于添加新机箱；如果将新模块添加或替换到已启用集群的 Firepower 9300，则该模块将自动添加。

开始之前

- 在替换的情况下，您必须从 Firepower 管理中心中删除旧的集群成员。当您将其替换为一台新设备时，它将被视为 Firepower 管理中心上的一个新设备。
- 新机箱上的接口配置必须相同。您可以导出和导入 FXOS 机箱配置以简化此过程。

过程

- 步骤 1** 在现有集群机箱 Firepower 机箱管理器上，选择逻辑设备打开逻辑设备页面。
- 步骤 2** 点击右上角的显示配置图标 ()；复制显示的集群配置。
- 步骤 3** 连接到新机箱上的 Firepower 机箱管理器，然后点击添加设备。
- 步骤 4** 对于设备名称 (**Device Name**)，请为逻辑设备提供一个名称。
- 步骤 5** 对于模板 (**Template**)，请选择思科 Firepower 威胁防御 (**Cisco Firepower Threat Defense**)。
- 步骤 6** 对于映像版本 (**Image Version**)，请选择 FTD 软件版本。
- 步骤 7** 在设备模式 (**Device Mode**) 中，点击集群 (**Cluster**) 单选按钮。
- 步骤 8** 选择加入现有集群 (**Join an Existing Cluster**)。
- 步骤 9** 点击复制配置 (**Copy config**) 复选框，然后点击确定 (**OK**)。如果取消选中此复选框，必须手动输入设置，以匹配第一个机箱配置。
- 步骤 10** 在复制集群详细信息 (**Copy Cluster Details**) 对话框中，粘贴第一个机箱的集群配置，然后点击确定 (**OK**)。
- 步骤 11** 点击屏幕中心的设备图标。集群信息通常已预填充，但您必须更改以下设置：
- 机箱 ID (**Chassis ID**) - 输入唯一的机箱 ID。
 - 站点 ID - 对于机箱间集群，输入此机箱的站点 ID（介于 1 和 8 之间）。此功能仅可使用 Firepower 管理中心 FlexConfig 功能进行配置。
 - 集群密钥 (**Cluster Key**) - （未预填充）输入相同的集群密钥。
 - 管理 IP (**Management IP**) - 将每个模块的管理地址更改为与其他集群成员位于同一网络中的唯一 IP 地址。
- 点击确定 (**OK**)。
- 步骤 12** 点击保存。
-

配置 Radware DefensePro

思科 Firepower 4100/9300 机箱可在单个刀片上支持多个服务（例如防火墙和第三方 DDoS 应用）。这些应用和服务可以链接在一起形成服务链。

关于 Radware DefensePro

在当前支持的服务链配置中，可以安装第三方 Radware DefensePro 虚拟平台以在 ASA 防火墙前面或在 Firepower 威胁防御前面运行。Radware DefensePro 是基于 KVM 的虚拟平台，可在 Firepower 4100/9300 机箱上提供分布式拒绝服务 (DDoS) 检测和缓解功能。当在 Firepower 4100/9300 机箱上启用服务链时，来自网络的流量必须先通过 DefensePro 虚拟平台，然后再到达主要 ASA 或 Firepower 威胁防御。



注释

- Radware DefensePro 虚拟平台可以称为 *Radware vDP*（虚拟 DefensePro），或者简称为 *vDP*。
- Radware DefensePro 虚拟平台有时可能是指链路修饰器。

Radware DefensePro 的必备条件

在 Firepower 4100/9300 机箱上部署 Radware DefensePro 之前，必须将 Firepower 4100/9300 机箱配置为使用 **etc/UTC** 时区的 NTP 服务器。有关设置 Firepower 4100/9300 机箱日期与时间的详细信息，请参阅[设置日期和时间](#)，第 80 页。

服务链准则

模式

- ASA - 以下型号的 ASA 支持 Radware DefensePro (vDP) 平台：
 - Firepower 9300
 - Firepower 4110
 - Firepower 4120
 - Firepower 4140
 - Firepower 4150
- Firepower 威胁防御 - 在以下型号上，支持 Radware DefensePro 平台用于 Firepower 威胁防御：
 - Firepower 9300

- Firepower 4110- 请注意，还必须同时部署修饰器与逻辑设备。在设备上配置了逻辑设备后，无法安装修饰器。
- Firepower 4120- 请注意，还必须同时部署修饰器与逻辑设备。在设备上配置了逻辑设备后，无法安装修饰器。
- Firepower 4140
- Firepower 4150

其他规定

- 服务链在机箱间集群配置中不受支持。但是，在机箱间集群场景中，可采用独立配置部署 Radware DefensePro (vDP) 应用。

在独立逻辑设备上配置 Radware DefensePro

以下程序显示如何在独立 ASA 或 Firepower 威胁防御逻辑设备前面的单个服务链中安装 Radware DefensePro。



注释 如果要在 Firepower 4120 或 4140 安全设备上的 ASA 前面安装 Radware vDP，则必须使用 FXOS CLI 部署修饰器。有关如何在 Firepower 4100 设备上在 ASA 前面的服务链中安装和配置 Radware DefensePro 的完整 CLI 说明，请参阅 FXOS CLI 配置指南。

开始之前

- 从 Cisco.com 下载 vDP 映像（请参阅[从 Cisco.com 下载映像](#)，第 38 页），然后将此映像上传到 Firepower 4100/9300 机箱（请参阅[将映像上传到 Firepower 安全设备](#)，第 38 页）。
- 您可以在机箱内集群的独立配置中部署 Radware DefensePro 应用；对于机箱内集群，请参阅[在机箱内集群上配置 Radware DefensePro](#)，第 189 页。

过程

- 步骤 1** 如果要将单独的管理接口用于 vDP，请启用该接口并根据[配置物理接口](#)，第 139 页将其设置为管理类型。否则，您可以共享应用管理接口。
- 步骤 2** 选择逻辑设备 (**Logical Devices**) 打开“逻辑设备” (Logical Devices) 页面。
“逻辑设备” (Logical Devices) 页面显示在机箱上配置的逻辑设备列表。如果尚未配置逻辑设备，系统将显示一条消息，要求您配置逻辑设备。
- 步骤 3** 创建独立 ASA 或 Firepower 威胁防御逻辑设备（请参阅[添加独立 ASA](#)，第 169 页或[添加独立的 Firepower 威胁防御](#)，第 170 页）。

- 步骤 4** 在修饰器 (**Decorators**) 区域中, 选择 vDP。系统将显示 “Radware: 虚拟 DefensePro - 配置 (Radware: Virtual DefensePro - Configuration)” 窗口。配置常规信息 (**General Information**) 选项卡下的以下字段。
- 步骤 5** 如果您已将多个 vDP 版本上传到 Firepower 4100/9300 机箱, 请在版本 (**Version**) 下拉列表中选择要使用的版本。
- 步骤 6** 如果您有一个资源可配置的 Radware DefensePro 应用, 则资源配置文件下拉列表下会显示支持的资源配置文件列表。选择要分配给设备的资源配置文件。如果未选择资源配置文件, 则使用默认设置。
- 步骤 7** 在管理接口 (**Management Interface**) 下拉列表下, 选择在此操作步骤的步骤 1 中创建的管理接口。
- 步骤 8** 选择默认地址类型 (**Address Type**): 仅 IPv4、仅 IPv6, 或者 IPv4 和 IPv6。
- 步骤 9** 根据在上一步中选择的地址类型 (**Address Type**), 配置以下字段。
- a) 在管理 IP (**Management IP**) 字段中, 配置本地 IP 地址。
 - b) 仅 IPv4: 输入网络掩码 (**Network Mask**)。
仅 IPv6: 输入前缀长度 (**Prefix Length**)。
 - c) 输入网络网关 (**Network Gateway**) 地址。
- 步骤 10** 点击您想要分配给设备的每个数据端口旁边的复选框。
- 步骤 11** 点击确定 (**OK**)。
- 步骤 12** 点击保存 (**Save**)。

Firepower 可扩展操作系统通过下载指定的软件版本, 并将引导程序配置和管理接口设置推送到指定安全模块来部署逻辑设备。

下一步做什么

为 DefensePro 应用设置密码。请注意, 在您完成密码设置之前, DefensePro 应用无法联网。有关更多信息, 请参阅 Cisco.com 上的《Radware DefensePro DDoS 攻击缓解用户指南》。

在机箱内集群上配置 Radware DefensePro

以下程序显示如何安装 Radware DefensePro 映像, 以及在 ASA 或 Firepower 威胁防御机箱内集群前面的服务链中配置此映像。



注释 服务链在机箱间集群配置中不受支持。但是, Radware DefensePro 应用可在机箱间集群情景的独立配置中进行部署。

开始之前

- 从 Cisco.com 下载 vDP 映像 (请参阅[从 Cisco.com 下载映像](#), 第 38 页), 然后将此映像上传到 Firepower 4100/9300 机箱 (请参阅[将映像上传到 Firepower 安全设备](#), 第 38 页)。

过程

- 步骤 1 如果要单独的管理接口用于 vDP，请启用该接口并根据[配置物理接口](#)，第 139 页将其设置为管理类型。否则，您可以共享应用管理接口。
- 步骤 2 配置 ASA 或 Firepower 威胁防御机箱内集群（请参阅[创建 ASA 集群](#)，第 178 页或[创建 Firepower 威胁防御集群](#)，第 182 页）。

请注意，在配置机箱内集群的程序结束时点击 **Save** 之前，必须首先按照以下步骤将 vDP 修饰器添加到集群。
- 步骤 3 在修饰器 (**Decorators**) 区域中，选择 vDP。系统将显示 **Radware: 虚拟 DefensePro - 配置 (Radware: Virtual DefensePro - Configuration)** 对话框。在**一般信息 (General Information)** 选项卡下配置以下字段。
- 步骤 4 如果已将多个 vDP 版本上传到 Firepower 4100/9300 机箱，请在**版本 (Version)** 下拉列表中选择要使用的 vDP 版本。
- 步骤 5 如果您有一个资源可配置的 Radware DefensePro 应用，则“资源配置文件”下拉列表下会显示支持的资源配置文件列表。选择要分配给设备的资源配置文件。如果未选择资源配置文件，则使用默认设置。
- 步骤 6 在**管理接口 (Management Interface)** 下拉列表下，选择管理接口。
- 步骤 7 点击您想分配给 vDP 修饰程序的每个数据端口旁边的复选框。
- 步骤 8 点击**接口信息 (Interface Information)** 选项卡。
- 步骤 9 选择要使用的**地址类型 (Address Type)**，仅 IPv4、仅 IPv6 或 IPv4 和 IPv6。
- 步骤 10 为每个安全模块配置以下字段。请注意，显示的字段取决于您在上一步中选择的**地址类型 (Address Type)**。
 - a) 在**管理 IP (Management IP)** 字段中，配置本地 IP 地址。
 - b) 仅 IPv4: 输入**网络掩码 (Network Mask)**。
仅 IPv6: 输入**前缀长度 (Prefix Length)**。
 - c) 输入**网络网关 (Network Gateway)** 地址。
- 步骤 11 点击**确定 (OK)**。
- 步骤 12 点击**保存 (Save)**。

Firepower 可扩展操作系统通过下载指定的软件版本，并将引导程序配置和管理接口设置推送到指定安全模块来部署逻辑设备。
- 步骤 13 选择**逻辑设备 (Logical Devices)** 打开“逻辑设备” (Logical Devices) 页面。
- 步骤 14 滚动已配置的逻辑设备列表至 vDP 条目。验证**管理 IP (Management IP)** 列中列出的属性。
 - 如果 **CLUSTER-ROLE** 元素针对 DefensePro 实例显示为 *unknown*，必须进入 DefensePro 应用，配置主 IP 地址，完成 vDP 集群创建。
 - 如果 **CLUSTER-ROLE** 元素针对 DefensePro 实例显示为 *primary* 或 *secondary*，则说明应用在线，并且已在集群中形成。

下一步做什么

为 DefensePro 应用设置密码。请注意，在您完成密码设置之前，DefensePro 应用无法联网。有关更多信息，请参阅 Cisco.com 上的《Radware DefensePro DDoS 攻击缓解用户指南》。

开放 UDP/TCP 端口和启用 vDP Web 服务

Radware APSolute Vision 管理器接口可使用各种 UDP/TCP 端口与 Radware vDP 应用进行通信。为使 vDP 应用与 APSolute Vision 管理器进行通信，您必须确保这些端口可访问及未被防火墙阻止。有关哪些特定接口可开放的详细信息，请参阅《APSolute Vision 用户指南》中的以下表格：

- APSolute Vision 服务器端口 - WBM 通信和操作系统
- 带 Radware 设备的 APSolute Vision 服务器的通信端口

为使 Radware APSolute Vision 管理部署在 FXOS 机箱上的虚拟 DefensePro 应用，您必须使用 FXOS CLI 启用 vDP Web 服务。

过程

步骤 1 从 FXOS CLI 连接到 vDP 应用实例。

```
connect module slot console
connect vdp
```

步骤 2 启用 vDP Web 服务。

```
manage secure-web status set enable
```

步骤 3 退出 vDP 应用控制台并返回 FXOS 模块 CLI。

```
Ctrl ]
```

管理逻辑设备

您可以删除逻辑设备、将 ASA 转换为透明模式、更改接口配置并在现有逻辑设备上执行其他任务。

连接到应用控制台

使用以下程序连接至应用的控制台。

过程

步骤 1 使用控制台连接或 Telnet 连接来连接至模块 CLI。

connect module slot_number {console | telnet}

要连接至不支持多个安全模块的设备的引擎，请使用 **1** 作为 *slot_number*。

使用 Telnet 连接的优点在于，您可以同时对模块开展多个会话，并且连接速度更快。

示例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

步骤 2 连接到应用控制台。为您的设备输入适当的命令。

connect asa

connect ftd name

connect vdp name

对于一种类型的应用，如果您有多个应用实例，则必须指定实例名称。要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

示例：

```
Firepower-module1> connect ftd
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

步骤 3 退出应用控制台到 FXOS 模块 CLI。

- ASA - 输入 **Ctrl-a, d**
- FTD - 输入退出
- vDP - 输入 **Ctrl-], .**

出于故障排除目的，您可能想使用 FXOS 模块 CLI。

步骤 4 返回 FXOS CLI 的管理引擎层。

退出控制台：

- a) 输入 ~
您将退出至 Telnet 应用。
- b) 要退出 Telnet 应用，请输入：
telnet>quit

退出 Telnet 会话：

- a) 输入 **Ctrl-],.**

示例

以下示例连接至安全模块 1 上的 ASA，然后退回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

删除逻辑设备

过程

- 步骤 1** 选择逻辑设备 (**Logical Devices**) 打开“逻辑设备” (**Logical Devices**) 页面。
“逻辑设备” (**Logical Devices**) 页面显示在机箱上配置的逻辑设备列表。如果尚未配置任何逻辑设备，则显示一条表明此情况的消息。
 - 步骤 2** 点击想要删除的逻辑设备所对应的删除 (**Delete**)。
 - 步骤 3** 点击是 (**Yes**) 确认想要删除此逻辑设备。
 - 步骤 4** 点击是 (**Yes**) 确认想要删除应用配置。
-

删除与逻辑设备不关联的应用实例

删除逻辑设备后，系统将提示您是否要删除逻辑设备的应用配置。如果不删除应用配置，则在删除该应用实例之前，将无法使用其他应用创建逻辑设备。当应用实例不再与逻辑设备关联时，可使用以下程序步骤从安全模块/引擎中删除应用实例。

过程

步骤 1 选择逻辑设备 (Logical Devices) 打开“逻辑设备” (Logical Devices) 页面。

“逻辑设备” (Logical Devices) 页面显示在机箱上配置的逻辑设备列表。如果尚未配置任何逻辑设备，则系统将显示一条表明此情况的消息。在逻辑设备列表下方，您可以看到与逻辑设备不关联的应用实例列表。

步骤 2 点击想要删除的应用实例所对应的删除 (Delete)。

步骤 3 点击是 (Yes) 确认想要删除应用实例。

更改 Firepower 威胁防御逻辑设备上的接口

可以在 Firepower 威胁防御逻辑设备上分配或取消分配接口，或者替换管理接口。然后，您可以在 Firepower 管理中心中同步接口配置。

开始之前

- 根据[配置物理接口](#)，第 139 页和[添加 EtherChannel（端口通道）](#)，第 139 页配置您的接口，并添加任何 EtherChannel。
- 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备或要求在 Firepower 管理中心上进行同步。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要将管理或 Firepower 事件接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。在 Firepower 威胁防御设备重新引导（管理接口更改导致重新引导），并且您在 Firepower 管理中心中同步配置后，还可以将（目前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在 Firepower 管理中心中同步配置。我们建议您先在从属/备用设备上更改接口，然后再在主/活动设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

过程

- 步骤 1 在 Firepower 机箱管理器中，选择**逻辑设备 (Logical Devices)**。
- 步骤 2 点击右上角的**编辑 (Edit)** 图标以编辑逻辑设备。
- 步骤 3 通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。
- 步骤 4 通过在**数据端口 (Data Ports)** 区域中选择新的数据接口来分配该接口。
- 步骤 5 替换管理或事件接口：

对于这些类型的接口，在您保存更改后，设备会重新启动。

- a) 点击页面中心的设备图标。
- b) 在**常规/集群信息 (General/Cluster Information)** 选项卡上，从下拉列表中选择新的**管理接口 (Management Interface)**。
- c) 在**设置 (Settings)** 选项卡上，从下拉列表中选择新的**事件接口 (Eventing Interface)**。
- d) 点击**确定 (OK)**。

如果更改管理接口的 IP 地址，则还必须更改 Firepower 管理中心中设备的 IP 地址：转到**设备 (Devices) > 设备管理 (Device Management) > 设备/集群 (Device/Cluster)**。在**管理 (Management)** 区域中，设置 IP 地址以匹配引导程序配置地址。

- 步骤 6 点击**保存 (Save)**。
- 步骤 7 登录至 Firepower 管理中心。
- 步骤 8 依次选择**设备 > 设备管理**，并点击 FTD 设备的编辑图标 (🔧)。系统会默认选择接口选项卡。
- 步骤 9 点击**接口 (Interfaces)** 选项卡左上方的**从设备同步接口 (Sync Interfaces from device)** 按钮。
- 步骤 10 点击**保存 (Save)**。

此时，可以点击**部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

更改 ASA 逻辑设备上的接口

可以在 ASA 逻辑设备上分配、取消分配或替换管理接口。ASDM 会自动发现新接口。

开始之前

- 根据[配置物理接口](#)，第 139 页和[添加 EtherChannel（端口通道）](#)，第 139 页配置您的接口，并添加任何 EtherChannel。
- 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。

- 如果在 FXOS 中移除一个分配的接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个分配的接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中移除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。
- 如果要将管理接口替换为管理 EtherChannel，则需要创建至少具有 1 个取消分配数据成员接口的 EtherChannel，然后将当前管理接口替换为 EtherChannel。在 ASA 重新加载（管理接口更改导致重新加载）后，您还可以将（当前取消分配的）管理接口添加到 EtherChannel。
- 对于集群或故障切换，请确保添加或移除所有设备上的接口。我们建议您先在从属/备用设备上更改接口，然后再在主/活动设备上更改接口。新的接口在管理性关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 在 Firepower 机箱管理器中，选择**逻辑设备 (Logical Devices)**。

步骤 2 点击右上角的**编辑 (Edit)** 图标以编辑逻辑设备。

步骤 3 通过在**数据端口 (Data Ports)** 区域中取消选择数据接口来取消分配该接口。

步骤 4 通过在**数据端口 (Data Ports)** 区域中选择新的数据接口来分配该接口。

步骤 5 替换管理接口：

对于此类型的接口，在您保存更改后，设备会重新加载。

- a) 点击页面中心的设备图标。
- b) 在**常规/集群信息 (General/Cluster Information)** 选项卡上，从下拉列表中选择新的**管理接口 (Management Interface)**。
- c) 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

修改或恢复逻辑设备的引导程序设置

您可以修改逻辑设备的引导程序设置。然后可以立即使用这些新设置重启应用实例，或者保存更改，稍后再使用这些新设置重启应用实例。

过程

步骤 1 在 Firepower 机箱管理器中，选择**逻辑设备 (Logical Devices)**。

步骤 2 点击右上角的**编辑 (Edit)** 图标以编辑逻辑设备。

步骤 3 点击页面中心的设备图标。

步骤 4 根据需要修改逻辑设备设置。

步骤 5 点击 **OK**。

步骤 6 点击**立即重启**，以保存更改并立即重启应用实例。点击**稍后重启**，以保存更改而不重启应用实例。

注释 如果您选择**稍后重启**，您可以在准备好时，通过点击“逻辑设备”页面中的**重启实例**来重启应用实例。

“逻辑设备 (Logical Devices)” 页面

使用 Firepower 机箱管理器的**逻辑设备**页面创建、编辑和删除逻辑设备。**逻辑设备**页面包含每个 Firepower 4100/9300 机箱 安全模块/引擎上安装的逻辑设备的信息区域。

每个逻辑设备区域的标头均提供以下信息：

- 逻辑设备的唯一名称。
- 逻辑设备模式，即“独立 (Standalone)”或“集群 (Clustered)”。
- 状态 - 显示逻辑设备的状态：
 - ok - 逻辑设备配置完成。
 - incomplete-configuration - 逻辑设备配置未完成。

每个逻辑设备区域均提供以下信息：

- 安全模块 - 显示安全模块。
- 端口 - 显示分配给应用实例的端口。
- 应用 - 显示安全模块上运行的应用。
- 版本 - 显示安全模块上运行的应用的软件版本号。



注释 对逻辑设备FTD进行的更新是通过Firepower管理中心完成的，而且所做的更新并未反映在Firepower 机箱管理器中的**逻辑设备编辑 (Logical Devices > Edit)**和**系统更新 (System > Updates)**页面上。这些页面中显示的版本是指创建 FTD逻辑设备所用的软件版本（CSP 映像）。

- 管理 IP - 显示分配作为逻辑设备管理 IP 的本地 IP 地址。
- 网关 - 显示分配给应用实例的网络网关地址。
- 管理端口 - 显示分配给应用实例的管理端口。
- 状态 - 显示应用实例的状态：
 - 在线 (Online) - 应用正在运行和工作。
 - 离线 (Offline) - 应用已停止并且不可操作。

- 正在安装 (Installing) - 应用安装正在进行。
- 未安装 (Not Installed) - 应用未安装。
- 安装失败 (Install Failed) - 应用安装失败。
- 正在启动 (Starting) - 应用正在启动。
- 启动失败 (Start Failed) - 应用启动失败。
- 已启动 (Started) - 应用成功启动，正在等待应用代理心跳。
- 正在停止 (Stopping) - 应用正在停止。
- 停止失败 (Stop Failed) - 应用无法进入离线状态。
- 未响应 (Not Responding) - 应用未响应。
- 正在更新 - 应用软件正在更新。
- 更新失败 - 应用软件更新失败。
- 更新成功 - 应用软件更新成功。
- 不支持 - 不支持安装的应用程序。

如果安全模块不存在或处于故障状态，该信息将显示在状态字段中。您可以将鼠标悬停在信息图标上，以查看故障的其他信息。有关安全模块故障的详细信息，请参阅[关于 FXOS 安全模块/安全引擎，第 207 页](#)。

- **属性** - 显示当前正在运行的应用实例的其他属性。



注释 如果修改了应用的引导程序设置而未立即重启应用实例，则在应用重启之前，属性字段将显示当前正在运行的应用的信息，而不会反映所做的更改。

- **集群操作状态** - 显示分配给应用实例的管理 URL。
- **管理 IP/Firepower 管理 IP** - 显示分配给应用实例的管理 IP 地址。
- **集群角色** - 显示应用实例的集群角色：主从。
- **HA 角色** - 显示应用实例的高可用性角色：主用或备用。
- **管理 URL** - 显示分配给应用实例的管理应用 URL。
- **UUID** - 显示应用实例的全局唯一标识符。

从 Firepower 机箱管理器的**逻辑设备**页面，可以在逻辑设备上执行以下功能：

- **刷新** - 刷新“逻辑设备”页面上的信息。
- **添加设备** - 允许您创建逻辑设备。

- **编辑** - 允许您编辑现有逻辑设备。
- **更新版本** - 允许您升级或降级逻辑设备上的软件。
- **删除** - 删除逻辑设备。
- **显示配置** - 打开对话框，以 JSON 格式显示逻辑设备或集群的配置信息。您可以复制配置信息，并在创建作为集群一部分的更多设备时使用此配置信息。
- **启用/禁用** - 启用或禁用应用实例。
- **升级/降级** - 允许您升级或降级应用实例。
- **重启实例** - 允许您重启应用实例。如果您已修改设备引导程序信息，但尚未重新启动应用实例，您可以点击“重新启动实例”，以清除现有的管理引导程序信息，并使用新的引导程序信息重新启动应用实例。
- **转到设备管理器** - 提供指向为应用实例所定义的 Firepower 管理中心或 ASDM 的链接。

站点间集群示例

以下示例显示支持的集群部署。

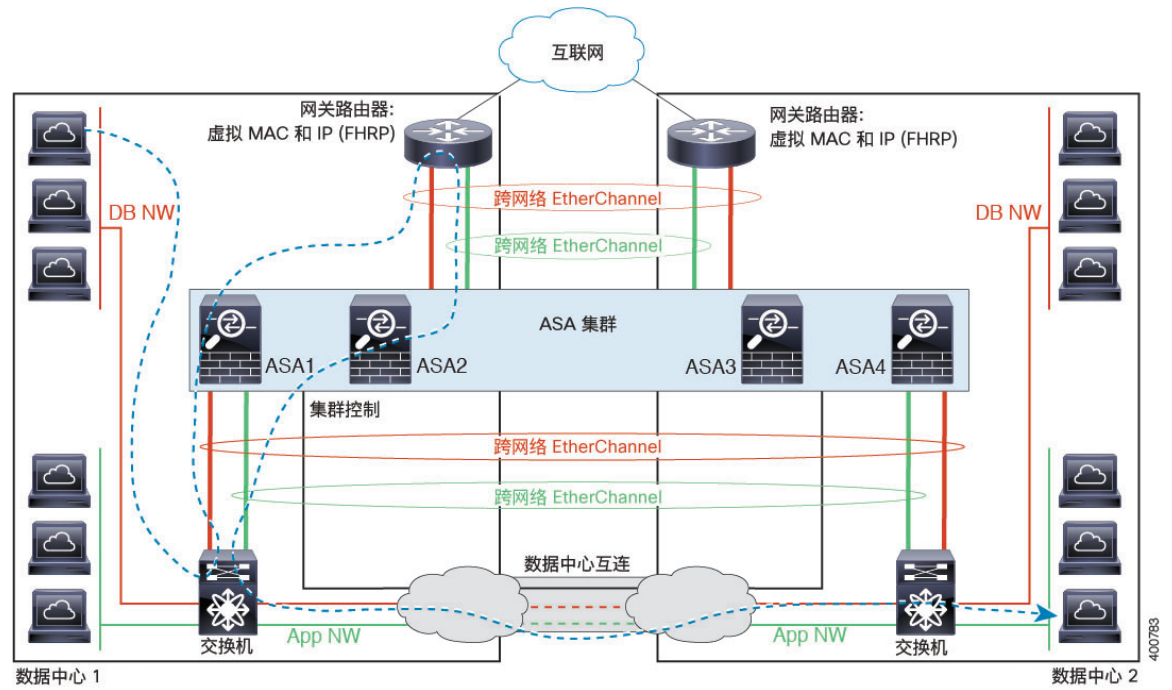
跨网络 EtherChannel 透明模式南北站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨网络 EtherChannel 连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

- **站点间 VSS/vPC** - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的集群设备只连接到本地交换机，而 VSS/vPC 流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您也可以选择将每台设备通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。
- **位于每个站点的本地 VSS/vPC** - 为了获得更高的交换机冗余能力，您可以在每个站点安装 2 对单独的 VSS/vPC。在此情况下，尽管集群设备仍然有一个跨网络 EtherChannel 将数据中心 1 的机箱仅连接到两本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨网络 EtherChannel 本质上是“分离的”。每个本地 VSS/vPC 都会将跨网络 EtherChannel 视作站点本地的 EtherChannel。



有关 vPC/VSS 选项的详细信息，请参阅[跨网络 EtherChannel 透明模式南北站点间集群示例](#)，第 199 页。

逻辑设备的历史记录

功能名称	平台版本	功能信息
Firepower 威胁防御的多实例功能	2.4.1	

功能名称	平台版本	功能信息
		<p>您现在可以在单个安全引擎/模块上部署多个逻辑设备，每台逻辑设备都设 Firepower 威胁防御容器实例。以前，您仅可部署单个本地应用实例。此外，仍支持本地实例。对于 Firepower 9300，可以在某些模块上使用本地实例，在其他模块上使用容器实例。</p> <p>要确保灵活使用物理接口，可以在 FXOS 中创建 VLAN 子接口，还可以在多个实例之间共享接口。部署容器实例时，必须指定分配的 CPU 核心数量；系统会根据核心数量动态分配 RAM，并将每个实例的磁盘空间设为 40 GB。此资源管理允许您自定义每个实例的性能。</p> <p>您可以在 2 个独立机箱上使用容器实例来实现高可用性；例如，如果您有 2 个机箱，每个机箱设 10 个实例，您可以创建 10 个高可用性对。不支持集群。</p> <p>注释 尽管实现方式不同，但多实例功能与 ASA 多情景模式类似。多情景模式下区分了单个应用实例，而多实例功能允许独立容器实例。容器实例允许硬资源分离、单独配置管理、单独重新加载、单独软件更新和完全 Firepower 威胁防御功能支持。由于共享资源，多情景模式支持给定平台上的更多情景。Firepower 威胁防御不支持多情景模式。</p> <p>注释 要求使用 6.3 或更高版本的 FTD。</p> <p>新增/修改的 Firepower 机箱管理器菜单项： 概述 > 设备 接口 > 所有接口 > 添加新下拉菜单 > 子接口 接口 > 所有接口 > 类型</p>

功能名称	平台版本	功能信息
		逻辑设备 > 添加设备 平台设置 > Mac 池 平台设置 > 资源配置文件 新增/修改的 Firepower 管理中心菜单项： 设备 > 设备管理 > 编辑图标 > 接口选项卡
支持 ASA 逻辑设备的透明模式部署	2.4.1	您现在可以在部署 ASA 时指定透明模式或路由模式。 新增/修改的 Firepower 机箱管理器菜单项： 逻辑设备 > 添加设备 > 设置 新增/修改的选项：防火墙模式下拉列表
集群控制链路可自定义 IP 地址	2.4.1	默认情况下， 集群控制链路使用 127.2.0.0/16 网络。现在，可以在 FXOS 中部署集群时设置网络。机箱根据机箱 ID 和插槽 ID 自动生成每个设备的集群控制链路接口 IP 地址： <code>127.2.chassis_id.slot_id</code> 。但是，某些网络部署不允许 127.2.0.0/16 流量通过。因此，您现在可以为 FXOS 中的集群控制链路设置一个自定义的 /16 子网（环回 (127.0.0.0/8) 和组播 (224.0.0.0/4) 地址除外）。 新增/修改的菜单项： 逻辑设备 > 添加设备 > 集群信息 > CCL 子网 IP 字段

功能名称	平台版本	功能信息
对于 FTD 引导程序配置，您现在可以在 FXOS CLI 中设置 FMC 的 NAT ID	2.4.1	<p>您现在可以在 FXOS CLI 中设置 FMC NAT ID。以前，您只能在 FTD CLI 内设置 NAT ID。通常，无论是出于路由目的还是为了进行身份验证，都需要两个 IP 地址（连同同一个注册密钥）：FMC 指定设备 IP 地址，设备指定 FMC IP 地址。但是，如果您只知道其中一个 IP 地址（这是实现路由目的的最低要求），您还必须在连接的两端指定唯一的 NAT ID，以建立对初始通信的信任，并查找正确的注册密钥。FMC 和设备使用注册密钥和 NAT ID（而不是 IP 地址）对初始注册进行身份验证和授权。</p> <p>新增/修改的命令：enter bootstrap-key NAT_ID</p>
ASA 的站点间集群改进	2.1.1	<p>现在，您可以在部署 ASA 集群时为每个 Firepower 4100/9300 机箱配置站点 ID。以前，您必须在 ASA 应用中配置站点 ID；此新功能简化了最初的部署。请注意，您不能再在 ASA 配置中设置站点 ID。此外，为了实现与站点间集群的最佳兼容性，我们建议您升级到 ASA 9.7(1) 和 FXOS 2.1.1，升级版包含对稳定性和性能的多项改进。</p> <p>我们修改了以下屏幕：逻辑设备 (Logical Devices) > 配置 (Configuration)</p>
对 6 个 FTD 模块进行机箱间集群	2.1.1	<p>现在，您可以对 FTD 启用机箱间集群。在最多 6 个机箱中最多可以包含 6 台设备。</p> <p>我们修改了以下屏幕：逻辑设备 (Logical Devices) > 配置 (Configuration)</p>
ASA 集群中，支持 16 个 Firepower 4100 机箱	2.0.1	在 ASA 集群中，最多可以集群 16 个机箱。
支持在 Firepower 4100 上执行 ASA 集群	1.1.4	在 ASA 集群中，最多可以集群 6 个机箱。

功能名称	平台版本	功能信息
支持在 Firepower 9300 上的 FTD 上执行机箱内集群	1.1.4	Firepower 9300 支持使用 FTD 应用执行机箱内集群。 我们修改了以下屏幕： 逻辑设备 (Logical Devices) > 配置 (Configuration)
Firepower 9300 上 16 个 ASA 模块的机箱内集群	1.1.3	现在，您可以对 ASA 启用机箱间集群。在最多 16 个机箱中最多可以包含 16 个模块。 我们修改了以下屏幕： 逻辑设备 (Logical Devices) > 配置 (Configuration)
Firepower 9300 上 ASA 的机箱内集群	1.1.1	您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建集群。 我们引入了以下屏幕： 逻辑设备 (Logical Devices) > 配置 (Configuration)



第 11 章

安全模块/引擎管理

- [关于 FXOS 安全模块/安全引擎，第 207 页](#)
- [停用/重新启用安全模块，第 209 页](#)
- [确认安全模块/引擎，第 209 页](#)
- [重置安全模块/引擎，第 210 页](#)
- [重新初始化安全模块/引擎，第 210 页](#)
- [使网络模块离线或在线，第 211 页](#)
- [关闭/开启安装的模块/引擎，第 212 页](#)

关于 FXOS 安全模块/安全引擎

在 Firepower 机箱管理器的“安全模块/安全引擎”页面上，您可以查看安全模块/引擎的状态，并在安全模块/引擎上执行各种功能：

安全模块/安全引擎 (Security Modules/Security Engine) 页面提供以下信息：

- 硬件状态 - 显示安全模块/引擎硬件的状态。
 - 启动 - 安全模块/引擎已成功启动，未显示任何硬件故障。
 - 正在启动 - 安全模块/引擎正在启动过程中。
 - 重启 - 安全模块/引擎正在重启过程中。
 - 关闭 - 安全模块/引擎的电源未打开或硬件故障阻止安全模块/引擎成功启动。
 - 未关联 - 安全模块/引擎没有与之关联的逻辑设备。
 - 不匹配 (Mismatch) - 安全模块已停用或插槽中安装了新的安全模块。使用“重新启用 (Recommission)”或“确认 (Acknowledge)”功能，使安全模块恢复正常运行状态。
 - 空 - 该插槽中未安装安全模块。
- 服务状态 - 显示安全模块/引擎上软件的状态：
 - 不可用 (Not-available) - 安全模块已从插槽中移除。重新安装安全模块，使之回到正常运行状态。

- 离线 - 安全模块/引擎已安装但已被停用、已关闭电源或仍在启动过程中。
- 在线 - 安全模块/引擎已安装并处于正常运行模式。
- 未响应 - 安全模块/引擎未响应。
- 令牌不匹配 (Token Mismatch) - 表示已安装到机箱插槽中的安全模块不是之前配置的安全模块。这也可能是软件安装错误引起的。使用“重新初始化 (Reinitialize)”功能使安全模块恢复正常运行状态。
- 故障 - 安全模块/引擎处于故障状态。查看系统故障列表，了解有关故障状态可能原因的详细信息。您也可以将鼠标悬停在故障对应的信息图标上，以查看更多信息。

安全模块故障

- 故障保护模式 - 安全模块处于故障保护模式。在此模式下，系统会阻止启动应用。要进行故障排除或禁用故障保护模式，请连接到安全模块。也可以删除应用实例。
- HDD 错误 - 安全模块磁盘驱动器出现错误。请确认安全模块有磁盘驱动器，并且如果故障未清除，则更换故障磁盘驱动器。
- 文件系统错误 - 安全模块上的磁盘分区不兼容。重启安全模块有可能会使其从故障中恢复。如果此故障仍然存在，请将数据备份到外部设备，然后对插槽进行重新初始化。
- 格式故障 - 安全模块磁盘驱动器上的自动格式功能出现故障。重新初始化安全模块以便重新格式化。
- 电源 - 显示安全模块/引擎的电源状态：
 - 开 (On) - 使用“电源关/开 (Power off/on)”功能切换安全模块/引擎的电源状态。
 - 关 (Off) - 使用“电源关/开 (Power off/on)”功能切换安全模块/引擎的电源状态。
- 应用 - 显示安全模块/引擎上安装的逻辑设备类型。

在 Firepower 机箱管理器的“安全模块/安全引擎”页面上，您可以在安全模块/引擎上执行以下功能：

- 停用/重新启用 (Decommission/Recommission) (仅限安全模块) - 停用安全模块后，安全模块将进入维护模式。您还可以先停用安全模块，然后重新启用安全模块，从而纠正某些故障状态。请参阅[停用/重新启用安全模块](#)，第 209 页。
- 确认 (Acknowledge) - 让新安装的安全模块上线。请参阅[确认安全模块/引擎](#)，第 209 页。
- 重启 - 重新启动安全模块/引擎。请参阅[重置安全模块/引擎](#)，第 210 页。
- 重新初始化 - 重新格式化安全模块/引擎硬盘，从安全模块/引擎上删除所有部署的应用和配置，然后重新启动系统。在重新初始化完成后，如果为安全模块/引擎配置了逻辑设备，Firepower 可扩展操作系统将重新安装应用软件，重新部署逻辑设备，并自动启动应用。请参阅[重新初始化安全模块/引擎](#)，第 210 页。



警告 在重新初始化期间，安全模块/引擎上的所有应用数据都将被删除。请在重新初始化安全模块/引擎之前备份所有应用数据。

- 电源关/开 - 切换安全模块/引擎的电源状态。请参阅[关闭/开启安装的模块/引擎](#)，第 212 页。

停用/重新启用安全模块

当您停用安全模块时，安全模块对象将从配置中删除，安全模块将变为非托管状态。安全模块上运行的任何逻辑设备或软件都将变为非活动状态。

如果要暂时停止使用安全模块，您可以停用安全模块。此外，如果重新启动安全模块无法纠正错误状态，您可以尝试停用然后重新启用安全模块，以查看是否能够纠正错误状态而不必重新初始化安全模块。

过程

步骤 1 选择安全模块 (**Security Modules**) 打开“安全模块 (Security Modules)”页面。

步骤 2 要停用安全模块，点击该安全模块所对应的下线 (**Decommission**)。

要重新启用安全模块，点击该安全模块所对应的**重新上线 (Recommission)**。

步骤 3 点击是 (**Yes**) 确认要停用或重新启用指定的安全模块。

确认安全模块/引擎

将新的安全模块安装到机箱时，或将现有模块替换为一个具有不同产品 ID (PID) 的模块时，必须确认安全模块，然后才能开始使用该模块。

如果安全模块显示“不匹配”或“令牌不匹配”状态，这表示安装在插槽中的安全模块上的数据与之前安装在该插槽中的模块不匹配。如果安全模块上已有数据并且您确定要在新的插槽中使用它（换句话说，安全模块并非无意中安装到错误插槽），您必须重新初始化该安全模块，然后才可以向它部署逻辑设备。

过程

步骤 1 选择安全模块/安全引擎 (**Security Modules/Security Engine**) 打开“安全模块/安全引擎 (Security Modules/Security Engine)”页面。

步骤 2 点击您想要确认的安全模块/引擎所对应的**确认 (Acknowledge)**。

步骤 3 点击是 (Yes) 确定您要确认指定的安全模块/引擎。

重置安全模块/引擎

按照以下步骤重启安全模块/引擎。

过程

步骤 1 选择安全模块/安全引擎 (Security Modules/Security Engine) 打开“安全模块/安全引擎 (Security Modules/Security Engine)”页面。

步骤 2 点击您想要重置的安全模块/引擎所对应的**重启 (Power Cycle)**。

步骤 3 执行以下操作之一：

- 点击**安全重启 (Safe Power Cycle)** 让系统等待最多五分钟，以便在系统重置指定的安全模块/引擎之前关闭安全模块/引擎上运行的应用。
 - 点击**立即重启 (Power Cycle Immediately)** 让系统立即重置指定的安全模块/引擎。
-

重新初始化安全模块/引擎

当安全模块/引擎重新初始化时，安全模块/引擎的硬盘将会格式化，所有安装的应用实例、配置和数据均会删除。在重新初始化完成后，如果为安全模块/引擎配置了逻辑设备，FXOS 将重新安装应用软件，重新部署逻辑设备，并自动启动应用。



注意 在重新初始化期间，安全模块/引擎上的所有应用数据都将被删除。请在重新初始化安全模块/引擎之前备份所有应用数据。

过程

步骤 1 选择安全模块/安全引擎 (Security Modules/Security Engine) 打开“安全模块/安全引擎 (Security Modules/Security Engine)”页面。

步骤 2 点击您想要重新初始化的安全模块/引擎所对应的**重新初始化 (Reinitialize)**。

步骤 3 点击是 (Yes) 确认您要重新初始化指定的安全模块/引擎。

安全模块/引擎会重启，安全模块上的所有数据均会删除。此过程可能需要数分钟。

使网络模块离线或在线

按照以下步骤以使用 CLI 命令使网络模块离线，或者使其重新恢复在线；在执行模块在线插入和删除 (OIR) 时用于示例。



注释 如果要删除或更换网络模块，请按照适用于设备的《安装指南》的“维护和升级”一章中的说明进行操作。请参阅<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>。

过程

步骤 1 对于要使其离线的模块，使用以下命令进入 `/fabric-interconnect` 模式，然后进入 `/card` 模式：

```
scope fabric-interconnect a
scope card ID
```

步骤 2 您可以使用 `show detail` 命令来查看关于此卡的信息，包括其当前状态。

步骤 3 要使模块离线，请输入：

```
set adminstate offline
```

步骤 4 输入 `commit-buffer` 命令，以保存配置更改。

您可以再次使用 `show detail` 命令确认该模块已离线。

步骤 5 要使网络模块重新恢复在线，请输入：

```
set adminstate online
commit-buffer
```

示例

```
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # scope card 2
FP9300-A /fabric-interconnect/card # show detail
```

```
Fabric Card:
  Id: 2
  Description: Firepower 4x40G QSFP NM
  Number of Ports: 16
  State: Online
  Vendor: Cisco Systems, Inc.
  Model: FPR-NM-4X40G
  HW Revision: 0
  Serial (SN): JAD191601DE
  Perf: N/A
  Admin State: Online
  Power State: Online
```

```

Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
FP9300-A /fabric-interconnect/card # set adminstate offline
FP9300-A /fabric-interconnect/card* # commit-buffer
FP9300-A /fabric-interconnect/card # show detail

Fabric Card:
Id: 2
Description: Firepower 4x40G QSFP NM
Number of Ports: 16
State: Offline
Vendor: Cisco Systems, Inc.
Model: FPR-NM-4X40G
HW Revision: 0
Serial (SN): JAD191601DE
Perf: N/A
Admin State: Offline
Power State: Off
Presence: Equipped
Thermal Status: N/A
Voltage Status: N/A
FP9300-A /fabric-interconnect/card #

```

关闭/开启安装的模块/引擎

按照以下步骤关闭或开启安全或网络模块。

过程

步骤 1 选择安全模块/安全引擎 (Security Modules/Security Engine) 打开“安全模块/安全引擎 (Security Modules/Security Engine)”页面。

步骤 2 要关闭安全模块/引擎电源：

- a) 点击该安全模块/引擎所对应的关机 (Power Off)。
- b) 执行以下操作之一：
 - 点击安全关机 (Safe Power Off) 让系统等待最多五分钟，以便在系统关闭指定的安全模块/引擎之前关闭安全模块/引擎上运行的应用。
 - 点击立即关机 (Power Off Immediately) 让系统立即关闭指定的安全模块/引擎。

步骤 3 要打开安全模块/引擎电源：

- a) 点击该安全模块/引擎所对应的开机 (Power on)。
- b) 点击是 (Yes) 确认您要打开指定的安全模块/引擎的电源。



第 12 章

配置导入/导出

- [关于配置导入/导出，第 213 页](#)
- [导出 FXOS 配置文件，第 214 页](#)
- [计划自动配置导出，第 214 页](#)
- [设置配置导出提醒，第 215 页](#)
- [导入配置文件，第 216 页](#)

关于配置导入/导出

使用配置导出功能将包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。之后，您便可以导入此配置文件，快速将配置设置应用于 Firepower 4100/9300 机箱，以返回到已知的正确配置，或从系统故障中恢复。

准则和限制

- 请勿修改配置文件的内容。如果配置文件被修改，使用该文件进行配置导入可能会失败。
- 特定应用的配置设置不包含在配置文件中。您必须使用应用提供的配置备份工具来管理特定应用的设置和配置。
- 将配置导入到 Firepower 4100/9300 机箱时，Firepower 4100/9300 机箱上的所有现有配置（包括任何逻辑设备）将被删除并完全替换为导入文件中包含的配置。
- 我们建议您只将配置文件导入当初从中导出该配置的同个 Firepower 4100/9300 机箱。
- 进行导入的 Firepower 4100/9300 机箱的平台软件版本应与执行导出时的版本相同。否则，导入操作将无法确保会成功。我们建议您在升级或降级 Firepower 4100/9300 机箱时导出备份配置。
- 进行导入的 Firepower 4100/9300 机箱必须在与执行导出时所用的相同插槽中安装相同的网络模块。
- 进行导入的 Firepower 4100/9300 机箱必须为您正在导入的导出文件中定义的任意逻辑设备安装了正确的软件应用映像。
- 如果导入的配置文件包含其应用具有最终用户许可协议 (EULA) 的逻辑设备，则在导入配置之前，必须在 Firepower 4100/9300 机箱上接受该应用的 EULA，否则操作将失败。

- 要避免覆盖现有的备份文件，请务必更改备份操作中的文件名或将现有文件复制到其他位置。

导出 FXOS 配置文件

使用配置导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。

请查看[关于配置导入/导出](#)，了解有关使用配置导出功能的重要信息。

过程

步骤 1 依次选择系统 (System) > 配置 (Configuration) > 导出 (Export)。

步骤 2 要将配置文件导出到本地计算机，请点击本地导出 (Export Locally)。

配置文件已创建，然后根据您的浏览器，该文件可能会自动下载到默认下载位置，或者系统会提示您保存文件。

步骤 3 要将配置文件导出到之前配置的远程服务器，请点击您要使用的远程配置的导出 (Export) 按钮。

配置文件已创建，并已被导出到指定位置。

步骤 4 要将配置文件导出到新的远程服务器：

- a) 在“按需导出 (On-Demand Export)”下面，点击添加按需配置 (Add On-Demand Configuration)。
- b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。
- c) 输入备份文件应存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

- d) 如果您使用非默认端口，请在端口 (Port) 字段中输入端口号。
- e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。
- f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。
- g) 在位置 (Location) 字段中，输入配置文件导出位置的完整路径，包括文件名。如果您省略了文件名，导出操作步骤将为该文件分配一个名称。
- h) 点击确定 (OK)。
“远程配置 (Remote Configuration)”将添加到按需导出 (On-Demand Export) 表。
- i) 点击您想使用的远程配置的导出 (Export) 按钮。
配置文件已创建，并已被导出到指定位置。

计划自动配置导出

使用计划的导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件自动导出到远程服务器或本地计算机。您可以计划每日、每周或每两周运行一次导出。配置导出将按计划

执行，计划基于计划的导出功能的启用时间。例如，如果您在星期三的晚上 10:00 启用每周一次的计划的导出，系统将在每个星期三的晚上 10:00 触发新的导出。

请查看[关于配置导入/导出](#)，了解有关使用配置导出功能的重要信息。

过程

-
- 步骤 1** 依次选择系统 (System) > 配置 (Configuration) > 导出 (Export)。
 - 步骤 2** 点击计划导出 (Schedule Export)。
您将看到配置计划的导出 (Configure Scheduled Export) 对话框。
 - 步骤 3** 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。
 - 步骤 4** 要启用计划的导出，请选中启用 (Enable) 复选框。

注释 之后，您可以使用此复选框启用或禁用计划的导出；但是，在启用或禁用计划的导出时，您将需要重新指定密码。
 - 步骤 5** 输入备份文件应存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。
 - 步骤 6** 如果您使用非默认端口，请在端口 (Port) 字段中输入端口号。
 - 步骤 7** 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。
 - 步骤 8** 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。
 - 步骤 9** 在位置 (Location) 字段中，输入配置文件导出位置的完整路径，包括文件名。如果您省略了文件名，导出操作步骤将为该文件分配一个名称。
 - 步骤 10** 选择您想要根据它自动导出配置的计划。它可以是以下计划之一：“每天 (Daily)”、“每周 (Weekly)”或“每两周 (BiWeekly)”。
 - 步骤 11** 点击 OK。
计划的导出已创建。如果启用了计划的导出，系统将按照您选择的计划自动将配置文件导出到指定位置。
-

设置配置导出提醒

使用导出提醒功能，让系统在一定天数内没有执行配置导出时报告错误。

过程

-
- 步骤 1** 依次选择系统 (System) > 配置 (Configuration) > 导出 (Export)。
 - 步骤 2** 要启用配置导出提醒，请选中导出触发提醒 (Reminder to trigger an export) 下的复选框。
 - 步骤 3** 输入在两次配置导出之间，系统在生成提醒错误前应等待的天数（1 和 365 之间的整数）。

步骤 4 点击保存提醒 (Save Reminder)。

导入配置文件

您可以使用配置导入功能应用之前已从 Firepower 4100/9300 机箱导出的配置设置。此功能允许您返回已知的良好配置或从系统故障中进行恢复。请查看[关于配置导入/导出](#)，了解有关使用配置导入功能的重要信息。

过程

步骤 1 依次选择系统 (System) > 配置 (Configuration) > 导入 (Import)。

步骤 2 要从本地配置文件导入：

- a) 点击**选择文件 (Choose File)**以导航到要导入的配置文件并将其选定。
- b) 点击**Import**。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。
- c) 点击**是 (Yes)**以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到 Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

步骤 3 要从之前配置的远程服务器导入配置文件：

- a) 在“Remote Import (远程导入)”表中，点击您想要使用的远程配置的**导入 (Import)**按钮。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。
- b) 点击**是 (Yes)**以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到 Firepower 4100/9300 机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。

步骤 4 要从新的远程服务器上的配置文件导入：

- a) 在“远程导入 (Remote Import)”下，点击**添加远程配置 (Add Remote Configuration)**。
- b) 选择与远程服务器通信时要使用的协议。它可以是以下协议之一：FTP、TFTP、SCP 或 SFTP。
- c) 如果您使用非默认端口，请在**端口 (Port)**字段中输入端口号。
- d) 输入备份文件存储位置的主机名或 IP 地址。这可以是 Firepower 4100/9300 机箱可通过网络访问的服务器、存储阵列、本地驱动器或任何读/写介质。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。
- e) 输入系统在登录远程服务器时应使用的用户名。如果协议是 TFTP，将无法应用该字段。
- f) 输入远程服务器用户名的密码。如果协议是 TFTP，将无法应用该字段。
- g) 在**文件路径 (File Path)**字段中，输入配置文件的完整路径，包括文件名。
- h) 点击**保存 (Save)**。
远程配置将添加到“远程导入 (Remote Import)”表。
- i) 点击您想使用的远程配置的**导入 (Import)**按钮。
系统将打开确认对话框，请求您确认是否要继续，并警告您可能需要重新启动机箱。

- j) 点击**是 (Yes)** 以确认要导入指定的配置文件。
现有配置被删除，导入文件中指定的配置应用到Firepower4100/9300机箱。在导入过程中，如果有分支端口配置更改，Firepower 4100/9300 机箱将需要重新启动。
-



第 13 章

故障排除

- [数据包捕获](#)，第 219 页
- [测试网络连接](#)，第 224 页
- [确定端口通道状态](#)，第 226 页
- [从软件故障中恢复](#)，第 228 页
- [从损坏的文件系统中恢复](#)，第 233 页
- [Firepower 威胁防御集群成员的灾难恢复](#)，第 242 页

数据包捕获

数据包捕获工具是一项宝贵资产，可用于调试连接和配置问题，了解通过 Firepower 4100/9300 机箱的流量。您可以使用数据包捕获工具记录通过 Firepower 4100/9300 机箱上面向特定接口的流量。

您还可以创建多个数据包捕获会话，每个会话都可以捕获多个接口上的流量。对于包含在数据包捕获会话中的每个接口，将创建单独的数据包捕获 (PCAP) 文件。

背板端口映射

Firepower 4100/9300 机箱对内部背板端口使用以下映射：

安全模块	端口映射	说明
安全模块 1/安全引擎	Ethernet1/9	内部数据 0/0
安全模块 1/安全引擎	Ethernet1/10	内部数据 0/1
安全模块 2	Ethernet1/11	内部数据 0/0
安全模块 2	Ethernet1/12	内部数据 0/1
安全模块 3	Ethernet1/13	内部数据 0/0
安全模块 3	Ethernet1/14	内部数据 0/1

数据包捕获准则和限制

数据包捕获工具存在以下限制：

- 捕获速度最多达到 100 Mbps。
- 即使没有足够的存储空间来运行数据包捕获会话，依然可以创建数据包捕获会话。在开始数据包捕获会话之前，您应验证您有足够的存储空间。
- 不支持多个活动数据包捕获会话。
- 仅在内部交换机的入口阶段进行捕获。
- 对于内部交换机无法理解的数据包（例如，安全组标记和网络服务报头数据包），过滤器不起作用。
- 即使您在一个或多个父接口上设有多个子接口，针对每个会话也只可捕获一个子接口的数据包。
- 无法捕获整个 EtherChannel 或 EtherChannel 子接口的数据包。然而，对于分配至逻辑设备的 EtherChannel，可以捕获 EtherChannel 每个成员接口上的数据包。如果分配子接口而不是父接口，则无法捕获成员接口上的数据包。
- 当捕获会话仍处于活动状态时，您无法复制或导出 PCAP 文件。
- 删除数据包捕获会话时，与此会话相关的所有数据包捕获文件也将被删除。

创建或编辑数据包捕获会话

过程

步骤 1 依次选择工具 (Tools) > 数据包捕获 (Packet Capture)。

捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 执行以下操作之一：

- 要创建数据包捕获会话，请点击**捕获会话 (Capture Session)** 按钮。
- 要编辑现有的数据包捕获会话，请点击该会话的**编辑 (Edit)** 按钮。

您可以在窗口左侧选择特定应用实例，然后该实例的表示形式便显示在窗口左侧。此表示用于选择您希望捕获数据包的接口。窗口右侧包含用于定义数据包捕获会话的字段。

步骤 3 从下拉菜单中**选择实例**。

步骤 4 点击要在其上捕获流量的接口。选定接口显示复选标记。

步骤 5 对于子接口，点击父接口左侧图标查看**子接口选择**列中的子接口。点击该列中的一个子接口；即使您在一个或多个父接口上设有多个子接口，针对每个捕获会话也只可捕获一个子接口的数据包。

对于多个子接口，则将图标标记为**子接口(n)**；对于单个子接口，则使用子接口 ID 标记该图标。如果系统也将父接口分配至实例，您可以选择父接口或子接口；您无法同时选择两者。如果系统未分配父接口，则父接口将显示为灰色。不支持 Etherchannel 的子接口。

步骤 6 要捕获从背板端口传出的逻辑设备的流量：

a) 点击代表应用实例的框。

捕获位置 (Capture On)、**应用端口 (Application Port)** 和**应用捕获方向 (Application Capture Direction)** 字段位于**配置数据包捕获会话 (Configure Packet Capture Session)** 窗口的右侧。

b) 选择您想要在其上捕捉流量的背板端口或从**捕捉端口 (Capture On)** 下拉列表中选择所有背板端口 (**All Backplane Ports**)。

步骤 7 请在**会话名称 (Session Name)** 字段中输入数据包捕获会话的名称。

步骤 8 可以通过以下两种方式指定要用于此数据包捕获会话的缓冲区大小：从**缓冲区大小 (Buffer Size)** 列表中选择预定义的值之一，或选择**自定义 (MB) (Custom in MB)**，然后输入所需的缓冲区大小。指定的缓冲区大小必须介于 1 和 2048 MB 之间。

步骤 9 在**Snap 长度 (Snap Length)** 字段中指定要捕获的数据包的长度。有效值范围为 64 至 9006 个字节。默认的 Snap 长度为 1518 个字节。

步骤 10 指定当执行此数据包捕获会话时，您是希望覆盖现有的 PCAP 文件还是将数据附加到 PCAP 文件。

步骤 11 要捕获应用实例与特定接口之间的流量：

a) 点击表示该逻辑设备的框。

b) 从**捕获位置**下拉列表中，选择应用类型（例如，**asa**）。

c) 选择您想要捕获流出或流入流量的**应用端口**。

d) 要仅捕获从逻辑设备流向指定接口的流量，请点击**应用捕获方向 (Application Capture Direction)** 旁边的**出口数据包 (Egress Packets)** 选项。

e) 要捕捉流出或流入指定接口的流量，请点击**应用捕捉方向 (Application Capture Direction)** 旁边的**所有数据包 (All Packets)** 选项。

步骤 12 要过滤捕获的流量：

a) 点击**捕获过滤器 (Capture Filter)** 字段的应用过滤器 (**Apply Filter**) 选项。

您将看到一组用于配置过滤器的字段。

b) 如果您需要创建过滤器，请点击**创建过滤器 (Create Filter)**。

您将看到**创建数据包过滤器 (Create Packet Filter)** 对话框。有关详细信息，请参阅[配置数据包捕获的过滤器](#)，第 222 页。

c) 从**应用 (Apply)** 下拉列表中选择要使用的过滤器。

d) 从**应用目标 (To)** 下拉列表中选择要应用过滤器的接口。

e) 要应用其他过滤器，请点击**应用其他过滤器 (Apply Another Filter)**，然后重复以上步骤应用其他过滤器。

步骤 13 执行以下操作之一：

- 要保存此数据包捕获会话并立刻运行该会话，请点击**保存并运行 (Save and Run)** 按钮。仅在当前未运行其他数据包捕获会话时，此选项才可用。

- 要保存此数据包捕获会话，以便在稍后运行，请点击**保存 (Save)** 按钮。

在**捕获会话 (Capture Session)** 选项卡中，您将看到列出了您的会话及之前创建的任何其他会话。如果选择**保存并运行 (Save and Run)**，数据包捕获会话将捕获数据包。要从会话下载 PCAP 文件，您需要先停止捕获。

配置数据包捕获的过滤器

您可以创建过滤器来限制数据包捕获会话中包含的流量。在创建数据包捕获会话时，您可以选择哪些接口应使用特定过滤器。



注释 如果您修改或删除已应用于当前正在运行的数据包捕获会话的过滤器，那么在您禁用并重新启用该会话后，更改才会生效。

过程

步骤 1 依次选择工具 (**Tools**) > **数据包捕获 (Packet Capture)**。

捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 执行以下操作之一：

- 要创建过滤器，请点击**添加过滤器 (Add Filter)** 按钮。
- 要编辑现有过滤器，请点击该过滤器的**编辑 (Edit)** 按钮。

您将看到**创建或编辑数据包过滤器 (Create or Edit Packet Filter)** 对话框。

步骤 3 请在**会话名称 (Session Name)** 字段中输入数据包捕获过滤器的名称。

步骤 4 要对特定协议进行过滤，请从**协议 (Protocol)** 列表中选择该协议，或选择**自定义 (Custom)**，然后输入所需的协议。自定义协议必须为 IANA 定义的协议，并采用十进制格式 (0 - 255)。

步骤 5 要对特定以太网类型进行过滤，请从**以太网类型 (EtherType)** 列表中选择该以太网类型，或选择**自定义 (Custom)**，然后输入所需的以太网类型。自定义以太网类型必须是 IANA 定义的以太网类型，并采用十进制格式（例如，IPv4 = 2048，IPv6 = 34525，ARP = 2054 和 SGT = 35081）。

步骤 6 要基于内部 VLAN（进入端口时的 VLAN ID）或外部 VLAN（Firepower 4100/9300 机箱添加的 VLAN ID）过滤流量，请在指定字段中输入 VLAN ID。

步骤 7 要过滤特定来源或目的流量，请在指定的来源或目的字段中输入 IP 地址和端口或输入 MAC 地址。

注释 您可以使用 IPv4 或 IPv6 地址过滤，但无法在同一数据包捕获会话中同时过滤这两类地址。

步骤 8 点击**保存 (Save)** 保存过滤器，

在过滤器列表 (Filter List) 选项卡中，您将看到列出了您的过滤器和已创建的任何其他过滤器。

启动和停止数据包捕获会话

过程

步骤 1 依次选择工具 (Tools) > 数据包捕获 (Packet Capture)。

捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 要启动数据包捕获会话，请点击该会话的启用会话 (Enable Session) 按钮，然后点击是 (Yes) 进行确认。

注释 您无法在另一个会话运行时启动数据包捕获会话。

会话中所包含接口的 PCAP 文件将开始收集流量。如果会话配置为覆盖会话数据，现有的 PCAP 数据将会擦除。如果不这样配置，数据将被附加到现有文件（如有）。

在数据包捕获会话运行时，单个 PCAP 文件的文件大小将随流量捕获而增加。一旦达到缓冲区大小限制，系统将开始丢弃数据包，您将会看到“丢弃计数 (Drop Count)”字段数值增加。

步骤 3 要停止数据包捕获会话，请点击该会话的禁用会话 (Disable Session) 按钮，然后点击是 (Yes) 进行确认。

在禁用会话后，您便可以下载 PCAP 文件（请参阅 [下载数据包捕获文件](#)，第 223 页）。

下载数据包捕获文件

您可将数据包捕获 (PCAP) 文件从会话下载到本地计算机，以便使用网络数据包分析器分析这些文件。

过程

步骤 1 依次选择工具 (Tools) > 数据包捕获 (Packet Capture)。

捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 要从数据包捕获会话下载特定接口的 PCAP 文件，请点击对应此接口的下载 (Download) 按钮。

注释 在数据包捕获会话运行时，无法下载 PCAP 文件。

根据您的浏览器，指定的PCAP文件要么会自动下载到默认下载位置，要么系统会提示您保存文件。

删除数据包捕获会话

如果单个数据包捕获会话当前未运行，则可将其删除，或者可以删除所有不活动的数据包捕获会话。

过程

步骤 1 依次选择工具 (Tools) > 数据包捕获 (Packet Capture)。

捕获会话 (Capture Session) 选项卡将会显示当前已配置的数据包捕获会话列表。如果当前未配置数据包捕获会话，将会显示说明此情况的消息。

步骤 2 要删除特定数据包捕获会话，请点击对应于该会话的删除 (Delete) 按钮。

步骤 3 要删除所有不活动的数据包捕获会话，请点击数据包捕获会话列表上方的删除所有会话 (Delete All Sessions) 按钮。

测试网络连接

开始之前

要使用主机名或 IPv4 地址 ping 网络中的另一设备，以此来测试基本网络连接，请使用 **ping** 命令。要使用主机名或 IPv6 地址 ping 网络上中的另一设备，请使用 **ping6** 命令。

要使用主机名或 IPv4 地址跟踪网络中另一设备的路由，请使用 **tracert** 命令。要使用主机名或 IPv6 地址跟踪网络中另一设备的路由，请使用 **tracert6** 命令。

- **ping** 和 **ping6** 命令可在 `local-mgmt` 模式下使用。
- **ping** 命令还可在 `module` 模式下使用。
- **tracert** 和 **tracert6** 命令可在 `local-mgmt` 模式下使用。
- **tracert** 命令还可在 `module` 模式下使用。

过程

步骤 1 通过输入以下命令之一连接到 `local-mgmt` 或 `module` 模式：

- **connect local-mgmt**
- **connect module *module-ID* {console | telnet}**

示例:

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

步骤 2 使用主机名或 IPv4 地址 ping 网络中的另一设备，以此来测试基本网络连接：

```
ping {hostname | IPv4_address} [count number_packets ] | [deadline seconds ] | [interval seconds ] | [packet-size bytes ]
```

示例:

此示例演示如何 ping 连接网络中的另一设备十二次：

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

步骤 3 使用主机名或 IPv4 地址跟踪网络中另一设备的路由：

```
traceroute {hostname | IPv4_address}
```

示例:

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1 198.51.100.57 (198.51.100.57) 0.640 ms 0.737 ms 0.686 ms
 2 net1-gw1-13.cisco.com (198.51.100.101) 2.050 ms 2.038 ms 2.028 ms
 3 net1-sec-gw2.cisco.com (198.51.100.201) 0.540 ms 0.591 ms 0.577 ms
 4 net1-fp9300-19.cisco.com (198.51.100.108) 0.336 ms 0.267 ms 0.289 ms

FP9300-A(local-mgmt)#
```

步骤 4 （可选）输入 **exit** 退出 local-mgmt 模式并返回到顶级模式。

确定端口通道状态

您可以按照以下步骤来确定当前定义的端口通道的状态。

过程

步骤 1 通过输入以下命令进入 `/eth-uplink/fabric` 模式：

- `scope eth-uplink`
- `scope fabric {a | b}`

示例：

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

步骤 2 输入 `show port-channel` 命令以显示当前的端口通道列表以及每个通道的管理状态和运行状态。

示例：

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
  Port Channel Id Name          Port Type      Admin
  State Oper State          State Reason
  -----
  10                    Port-channel10 Data            Enabl
ed    Failed                No operational members
  11                    Port-channel11 Data            Enabl
ed    Failed                No operational members
  12                    Port-channel12 Data            Disab
led   Admin Down             Administratively down
  48                    Port-channel48 Cluster          Enabl
ed    Up

FP9300-A /eth-uplink/fabric #
```

步骤 3 通过输入以下命令进入 `/port-channel` 模式，以显示各个端口通道和端口信息：

- `scope port-channel ID`

示例：

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.
```

The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license.

```
<--- remaining lines removed for brevity --->
```

```
FP9300-A(fxos)#
```

步骤 4 输入 **show** 命令以显示指定端口通道的状态信息。el.

示例:

```
FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
  Port Channel Id Name          Port Type          Admin
  State Oper State              State Reason
  -----
  10                          Port-channel10    Data              Enabl
ed      Failed                No operational members

FP9300-A /eth-uplink/fabric/port-channel #
```

步骤 5 输入 **show member-port** 命令以显示端口通道成员端口的状态信息。

示例:

```
FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
  Port Name          Membership          Oper State          State Reas
on
  -----
  --
  Ethernet2/3        Suspended           Failed              Suspended
  Ethernet2/4        Suspended           Failed              Suspended

FP9300-A /eth-uplink/fabric/port-channel #
```

除非已将端口通道分配到逻辑设备，否则不会显示相关信息。如果从逻辑设备中移除端口通道或逻辑设备被删除，该端口通道将恢复为“暂停”状态。

步骤 6 要查看其他端口通道和 LACP 信息，请通过输入以下命令退出 `/eth-uplink/fabric/port-channel` 模式并进入 `fxos` 模式:

- **top**
- **connect fxos**

示例:

步骤 7 输入 **show port-channel summary** 命令以显示当前端口通道的摘要信息。

示例:

```
FP9300-A(fxos)# show port-channel summary
Flags:  D - Down          P - Up in port-channel (members)
        I - Individual    H - Hot-standby (LACP only)
        s - Suspended     r - Module-removed
        S - Switched     R - Routed
        U - Up (port-channel)
        M - Not in use. Min-links not met
```

```

-----
-----
Group Port-          Type      Protocol  Member Ports
Channel
-----
-----
10    Po10 (SD)        Eth       LACP      Eth2/3 (s)  Eth2/4 (s)
11    Po11 (SD)        Eth       LACP      Eth2/1 (s)  Eth2/2 (s)
12    Po12 (SD)        Eth       LACP      Eth1/4 (D)  Eth1/5 (D)
48    Po48 (SU)        Eth       LACP      Eth1/1 (P)  Eth1/2 (P)

```

其他 **show port-channel** 和 **show lacp** 命令可在 `fxos` 模式下使用。您可以使用这些命令来显示各种端口通道和 LACP 信息，例如容量、流量、计数器和使用率。

下一步做什么

有关创建端口通道的信息，请参阅[添加 EtherChannel（端口通道）](#)，第 139 页。

从软件故障中恢复

开始之前

在阻止系统成功引导的软件故障情况下，您可以使用以下程序引导新的软件版本。要完成该过程，您需要 TFTP 来引导启动映像，下载新的系统和管理器映像，然后使用新映像进行引导。

特定 FXOS 版本的恢复映像可以从 Cisco.com 上的以下任一位置获取：

- Firepower 9300 -<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 系列 -<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

恢复映像包含三个单独的文件。例如，以下是 FXOS 2.1.1.64 的当前恢复映像。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

过程

步骤 1 访问 ROMMON:

- a) 连接到控制台端口。
- b) 重启系统。

系统将开始加载，并且在该过程中会显示一个倒计时计时器。

- c) 在倒计时期间按 **Escape** 键可进入 ROMMON 模式。

示例:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
```

```
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

步骤 2 TFTP 引导启动映像:

- a) 确认已正确设置管理 IP 地址、管理网络掩码和网关 IP 地址。您可以使用 **set** 命令查看其值。您可以使用 **ping** 命令测试与 TFTP 服务器的连接性。

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) 将启动映像复制到可从 Firepower 4100/9300 机箱访问的 TFTP 目录。

注释 该启动映像的版本号将与捆绑包版本号不匹配。显示 FXOS 版本与启动映像之间映射的信息可在 Cisco.com 软件下载页面找到。

- c) 使用引导命令从 ROMMON 引导映像:

```
boot tftp://<IP address>/<path to image>
```

注释 您还可以使用插入 Firepower 4100/9300 机箱前面板的 USB 插槽中的 USB 介质设备，从 ROMMON 引导启动映像。如果 USB 设备是在系统运行期间插入的，则您需要先重新启动系统，然后系统才会识别该 USB 设备。

系统将显示一系列 # 指示正在接收映像并且随后会加载启动映像。

示例:

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

步骤 3 下载与您刚刚加载到 Firepower 4100/9300 机箱的启动映像相匹配的恢复系统和管理器映像:

- a) 要下载恢复系统和管理器映像，您需要设置管理 IP 地址和网关。您无法通过 USB 下载这些映像。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

- b) 将恢复系统和管理器映像从远程服务器复制到 bootflash:

```
switch(boot)# copy URL bootflash:
```

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/path/image_name**

示例:

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
```

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

- c) 将映像成功复制到 Firepower 4100/9300 机箱后，创建一个自 nuova-sim-mgmt-nsg.0.1.0.001.bin 的管理器映像系统链接。此链接可向加载机制指明要加载的管理器映像。该系统链接的名称应始终为 nuova-sim-mgmt-nsg.0.1.0.001.bin，无论您尝试加载什么映像都是如此。

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

示例:

```
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway 10.0.0.1
switch(boot) (config)# exit
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

```
switch(boot)# copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...
```

```
switch boot> # copy bootflash:fxos-k9-manager.4.1.1.69.SPA
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch boot> #
```

步骤 4 加载您刚刚下载的系统映像:

```
switch boot> # load bootflash:<system-image>
```

示例:

```
switch boot> # load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful
...
System is coming up ... Please wait ...

Cisco FPR Series Security Appliance
FP9300-A login:
```

步骤 5 加载恢复映像后，输入以下命令以避免系统尝试加载旧映像:

注释 在加载恢复映像后应立即执行此步骤。

```
FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
FP9300-A /org/fw-platform-pack* # commit-buffer
```

步骤 6 下载并安装您要在 Firepower 4100/9300 机箱上使用的平台捆绑包映像。有关详细信息，请参阅[映像管理，第 37 页](#)。

示例:

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port      Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
           Tftp      192.168.1.2          0          Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```


从损坏的文件系统中恢复

开始之前

如果管理引擎的板载闪存损坏，并且系统无法再成功启动，您可以使用以下程序恢复系统。要完成该过程，您需要 TFTP 来引导启动映像，重新格式化闪存，下载新的系统和管理器映像，然后使用新映像进行引导。



注释 此程序包括重新格式化系统闪存。因此，您需要在系统恢复后对其进行完全重新配置。

特定 FXOS 版本的恢复映像可以从 Cisco.com 上的以下任一位置获取：

- Firepower 9300 -<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 系列 -<https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

恢复映像包含三个单独的文件。例如，以下是 FXOS 2.1.1.64 的恢复映像。

```
Recovery image (kickstart) for FX-OS 2.1.1.64.  
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA
```

```
Recovery image (manager) for FX-OS 2.1.1.64.  
fxos-k9-manager.4.1.1.63.SPA
```

```
Recovery image (system) for FX-OS 2.1.1.64.  
fxos-k9-system.5.0.3.N2.4.11.63.SPA
```

过程

步骤 1 访问 ROMMON:

- a) 连接到控制台端口。
- b) 重启系统。

系统将开始加载，并且在该过程中会显示一个倒计时计时器。

- c) 在倒计时期间按 **Escape** 键可进入 ROMMON 模式。

示例:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE  
Copyright (c) 1994-2015 by Cisco Systems, Inc.  
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0  
Last reset cause: LocalSoft  
DIMM Slot 0 : Present  
DIMM Slot 1 : Present  
No USB drive !!
```

```

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 >

```

步骤 2 TFTP 引导启动映像:

- a) 确认已正确设置管理 IP 地址、管理网络掩码和网关 IP 地址。您可以使用 **set** 命令查看其值。您可以使用 **ping** 命令测试与 TFTP 服务器的连接性。

```

rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>

```

- b) 将启动映像复制到可从 Firepower 4100/9300 机箱访问的 TFTP 目录。

注释 该启动映像的版本号将与捆绑包版本号不匹配。显示 FXOS 版本与启动映像之间映射的信息可在 Cisco.com 软件下载页面找到。

- c) 使用引导命令从 ROMMON 引导映像:

```
boot tftp://<IP address>/<path to image>
```

注释 您还可以使用插入 Firepower 4100/9300 机箱前面板的 USB 插槽中的 USB 介质设备，从 ROMMON 引导启动映像。如果 USB 设备是在系统运行期间插入的，则您需要先重新启动系统，然后系统才会识别该 USB 设备。

系统将显示一系列 # 指示正在接收映像并且随后会加载启动映像。

示例:

```

rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2

```

```

..!!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
      ADDRESS: 10.0.0.2
      NETMASK: 255.255.255.0
      GATEWAY: 10.0.0.1
      SERVER: 192.168.1.2
      IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

      TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....

Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.

```

步骤 3 加载 kickstart 映像后，使用 **init system** 命令重新格式化闪存。

init system 命令会擦除闪存内容，包括下载到系统的所有软件映像以及系统上的所有配置。完成该命令大概需要 20-30 分钟。

示例:

```

switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:.

Do you want to continue? (y/n) [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Sysdebug partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done

```

步骤 4 将恢复映像下载到 Firepower 4100/9300 机箱:

- a) 要下载恢复映像，您需要设置管理 IP 地址和网关。您无法通过 USB 下载这些映像。

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address <ip address> <netmask>
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway <gateway>
switch(boot)(config)# exit
```

- b) 将三个恢复映像从远程服务器复制到 bootflash:

```
switch(boot)# copy URL bootflash:
```

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/path/image_name**

示例:

```
switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:
```

```
switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
```

```
switch(boot)# copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
```

- c) 将映像成功复制到 Firepower 4100/9300 机箱后，创建一个自 `nuova-sim-mgmt-nsg.0.1.0.001.bin` 的管理器映像系统链接。此链接可向加载机制指明要加载的管理器映像。该系统链接的名称应始终为 `nuova-sim-mgmt-nsg.0.1.0.001.bin`，无论您尝试加载什么映像都是如此。

```
switch(boot)# copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

示例:

```
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.0.0.1
switch(boot)(config)# exit
switch(boot)# copy
```

```

tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy
tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.1.1.69.SPA
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot)#

```

步骤 5 重新加载交换机:

```
switch(boot)# reload
```

示例:

```
switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.
```

```
!! Rommon image verified successfully !!
```

```
Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb
```

```
autoboot: Can not find autoboot file 'menu.lst.local'
Or can not find correct boot string !!
```

```
rommon 1 >
```

步骤 6 从启动和系统映像引导:

```
rommon 1 > boot <kickstart-image> <system-image>
```

注释 在加载系统映像期间，您很可能会看到许可证管理器失败消息。可以安全忽略这些消息。

示例:

```
rommon 1 > dir
Directory of: bootflash:\

01/01/12 12:33a <DIR>          4,096  .
01/01/12 12:33a <DIR>          4,096  ..
01/01/12 12:16a <DIR>          16,384 lost+found
01/01/12 12:27a              34,333,696 fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
01/01/12 12:29a              330,646,465 fxos-k9-manager.4.1.1.69.SPA
01/01/12 12:31a              250,643,172 fxos-k9-system.5.0.3.N2.4.11.69.SPA
01/01/12 12:34a              330,646,465 nuova-sim-mgmt-nsg.0.1.0.001.bin
      4 File(s) 946,269,798 bytes
      3 Dir(s)
```

```
rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan 1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
```

the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

You have chosen to setup a new Security Appliance. Continue? (y/n):

步骤 7 加载映像后，系统将提示您进入初始配置设置。有关详细信息，请参阅[初始配置](#)，第 6 页。

步骤 8 下载您要在 Firepower 4100/9300 机箱上使用的平台捆绑包映像。有关详细信息，请参阅[映像管理](#)，第 37 页。

示例：

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
  File Name Protocol Server          Port    Userid      State
  -----
  fxos-k9.2.1.1.73.SPA
      Tftp      192.168.1.2          0
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

步骤 9 安装您在上一步中下载的平台捆绑包映像：

a) 进入自动安装模式：

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

b) 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 2.1(1.73)。

c) 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。

d) 输入 **yes** 确认您想要继续安装，或者输入 **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。

e) 要监控升级流程，请执行以下操作：

- 输入 **scope firmware**。

- 输入 **scope auto-install**。
- 输入 **show fsm status expand**。

步骤 10 如果您安装的平台捆绑包映像与用于恢复系统的映像一致，必须手动激活 **kickstart** 和系统映像，以便在将来加载系统时使用。安装映像与所使用的恢复映像一致的平台捆绑包时，系统不会自动激活。

a) 设置交换矩阵互联 a 的范围：

```
FP9300-A# scope fabric-interconnect a
```

b) 使用 **show version** 命令查看正在运行的内核版本和系统版本。您将使用这些字符串激活映像。

```
FP9300-A /fabric-interconnect # show version
```

注释 如果启动内核版本和启动系统版本已设置且与运行内核版本和运行系统版本相匹配，则无需激活映像，并且可以转至步骤 11。

c) 输入以下命令以激活映像：

```
FP9300-A /fabric-interconnect # activate firmware  
kernel-version <running_kernel_version> system-version <running_system_version>  
commit-buffer
```

注释 服务器状态可能更改为“Disk Failed”。您无需担心此消息，并可继续执行此程序。

d) 使用 **show version** 命令确认已正确设置启动版本并监控映像的激活状态。

重要事项 在状态从“Activating”更改为“Ready”之前，请勿继续进行下一步。

```
FP9300-A /fabric-interconnect # show version
```

示例：

```
FP9300-A /firmware # top  
FP9300-A# scope fabric-interconnect a  
FP9300-A /fabric-interconnect # show version  
Fabric Interconnect A:  
  Running-Kern-Vers: 5.0(3)N2(4.11.69)  
  Running-Sys-Vers: 5.0(3)N2(4.11.69)  
  Package-Vers: 2.1(1.73)  
  Startup-Kern-Vers:  
  Startup-Sys-Vers:  
  Act-Kern-Status: Ready  
  Act-Sys-Status: Ready  
  Bootloader-Vers:  
  
FP9300-A /fabric-interconnect # activate firmware kernel-version  
5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)  
Warning: When committed this command will reset the end-point  
FP9300-A /fabric-interconnect* # commit-buffer  
FP9300-A /fabric-interconnect # show version  
Fabric Interconnect A:  
  Running-Kern-Vers: 5.0(3)N2(4.11.69)  
  Running-Sys-Vers: 5.0(3)N2(4.11.69)  
  Package-Vers: 2.1(1.73)
```



```
Startup-Kern-Vers: 5.0(3)N2(4.11.69)
Startup-Sys-Vers: 5.0(3)N2(4.11.69)
Act-Kern-Status: Activating
Act-Sys-Status: Activating
Bootloader-Vers:
```

```
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:
```

步骤 11 重新启动系统:

示例:

```
FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #
```

系统在最终关闭之前会先关闭每个安全模块/引擎，然后才重启 Firepower 4100/9300 机箱。此过程大约需要 5-10 分钟。

步骤 12 监控系统状态。服务器状态应从“Discovery”转为“Config”，最后转为“Ok”。

示例:

```
FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Discovery In Progress
1/2 Equipped Discovery In Progress
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Config Complete
1/2 Equipped Config Complete
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Ok Complete
1/2 Equipped Ok Complete
1/3 Empty
```

当整体状态为“Ok”时，您的系统即已恢复。您仍必须重新配置安全设备（包括许可证配置），并重新创建所有逻辑设备。更多详情：

- Firepower 9300 快速入门指南 -<http://www.cisco.com/go/firepower9300-quick>

- Firepower 9300 配置指南 -<http://www.cisco.com/go/firepower9300-config>
- Firepower 4100 系列快速入门指南 -<http://www.cisco.com/go/firepower4100-quick>
- Firepower 4100 系列配置指南 -<http://www.cisco.com/go/firepower4100-config>

Firepower 威胁防御集群成员的灾难恢复

在灾难恢复场景之后，使用此程序和 Firepower 威胁防御，将 Firepower 4100/9300 集群成员恢复在线状态并加入一个集群。请注意，如果与集群设备关联的 Firepower 威胁防御应用版本不同步，您必须按照[更新逻辑设备的映像版本](#)，第 40 页中所述的步骤，使其同步为相同版本。

开始之前

使用配置导出功能将包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。有关详细信息，请参阅[关于配置导入/导出](#)，第 213 页。

过程

- 步骤 1** 从属设备正常运行后，恢复备份。有关如何导入配置的说明，请参阅[导入配置文件](#)，第 216 页。应用安装开始。
- 步骤 2** 接受许可协议。
- 步骤 3** 如有必要，设置应用的启动版本，以便集群中各个设备上的版本匹配。有关如何设置应用启动版本的说明，请参阅[更新逻辑设备的映像版本](#)，第 40 页。
- 步骤 4** 一旦更改应用启动版本，请重新初始化安全模块，以使 Firepower 威胁防御运行版本与启动版本相匹配。
- 导航到“安全模块/安全引擎”页面。
 - 点击 **Reinitialize Security Engine** 按钮。
 - 点击“是”，以确认更改。系统会重新格式化安全模块并重新安装应用启动版本。
- 应用将恢复在线状态并加入集群。

- 步骤 5** 确认应用的启动版本和运行版本相同。

- 在 FXOS CLI 中，进入安全服务模式：

```
Firepower scope ssa
```

- 显示应用实例：

```
firepower /ssa # show app-instance
```

示例：

```
firepower /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          6.2.3.1624      6.2.3.1624  
              In Cluster      Slave
```

步骤 6 在 Firepower 管理中心，删除从属设备成员。请参阅 Firepower 管理中心配置指南中的“删除从属设备成员”。

步骤 7 将恢复的 Firepower 9300/4100 从属设备重新添加到 Firepower 管理中心。请参阅 Firepower 管理中心配置指南中的“替换集群成员”。



索引

A

- 安全模块 [209, 210, 211, 212](#)
 - 打开电源 [212](#)
 - 断开 [212](#)
 - 离线 [211](#)
 - 确认 [209](#)
 - 停用 [209](#)
 - 在线 [211](#)
 - 重新初始化 [210](#)
 - 重置 [210](#)

B

- 本地身份验证的用户 [36](#)
 - 清除密码历史记录 [36](#)
- 本地身份验证用户 [26](#)
 - 密码配置文件 [26](#)

C

- 出厂默认配置 [70](#)
 - 恢复 [70](#)
- 初始配置 [6](#)
- 创建数据包捕获会话 [220](#)

D

- 打开/关闭安全模块电源 [212](#)
- 导出配置 [213](#)
- 导入配置 [213](#)
- 登录或注销 [8](#)
- 登录前横幅 [67, 68, 69](#)
 - 创建 [67](#)
 - 删除 [69](#)
 - 修改 [68](#)
- 端口通道 [139, 226](#)
 - 配置 [139](#)
 - status [226](#)

F

- 访问命令行界面 [9](#)
- 分支电缆 [143](#)
 - 配置 [143](#)
- 分支端口 [143](#)

G

- 高级任务列表 [5](#)
- 固件 [41](#)
 - 升级 [41](#)
- 故障排除 [226](#)
 - 端口通道状态 [226](#)
- 关闭 Firepower 机箱 [70](#)
- 管理 IP 地址 [62](#)
 - 不断变化的 [62](#)

H

- 恢复出厂默认配置 [70](#)
- 会话超时 [29, 30](#)

J

- 机箱 [2, 6](#)
 - 初始配置 [6](#)
 - 监控状态 [2](#)
- 机箱管理器 [1](#)
 - 用户界面概述 [1](#)
- 集群 [165, 166, 174, 175, 176, 178, 182](#)
 - 创建 [165, 178, 182](#)
 - 关于 [174](#)
 - 集群控制链路 [175](#)
 - redundancy [175](#)
 - size [175](#)
 - 设备本地 EtherChannel, 在交换机上配置 [166](#)
 - management [176](#)
 - 网络 [176](#)
 - spanning-tree portfast [165](#)
- 监控机箱状态 [2](#)

接口 [139](#)

配置 [139](#)

属性 [139](#)

K

控制台 [29, 30](#)

timeout [29, 30](#)

L

历史记录, 密码 [26](#)

连接到逻辑设备 [191](#)

逻辑设备 [40, 165, 169, 170, 178, 182, 191, 193, 194, 197](#)

创建独立 [169, 170](#)

创建集群 [165, 178, 182](#)

更新映像版本 [40](#)

了解 [197](#)

连接到 [191](#)

删除 [193](#)

删除应用实例 [194](#)

退出连接 [191](#)

M

密码 [23, 26, 27](#)

更改间隔 [27](#)

历史记录计数 [26](#)

强度检查 [27](#)

指导原则 [23](#)

密码配置文件 [26, 36](#)

关于 [26](#)

清除密码历史记录 [36](#)

密钥环 [94, 95, 96, 97, 99, 100, 104](#)

创建 [94](#)

导入证书 [100](#)

关于 [94](#)

删除 [104](#)

受信任点 [99](#)

证书请求 [96, 97](#)

重新生成 [95](#)

命令行界面 [9](#)

访问 [9](#)

P

配置 [94, 95, 96, 97, 99, 100](#)

HTTPS [94, 95, 96, 97, 99, 100](#)

配置导入/导出 [213](#)

限制 [213](#)

指导原则 [213](#)

配置文件 [26](#)

password [26](#)

平台捆绑包 [37, 38, 39](#)

从 Cisco.com 下载 [38](#)

关于 [37](#)

上传到 Firepower 安全设备 [38](#)

升级 [39](#)

验证完整性 [39](#)

Q

启用 [89](#)

SNMP [89](#)

确认安全模块 [209](#)

R

任务流 [5](#)

日期 [80, 82](#)

查看 [80](#)

手动设置 [82](#)

日期和时间 [80](#)

配置 [80](#)

软件故障 [228](#)

恢复 [228](#)

S

删除数据包捕获会话 [224](#)

设备名称 [66](#)

和不断变化的 [66](#)

社区, SNMP [89](#)

升级固件 [41](#)

时区 [81, 82](#)

setting [81, 82](#)

使安全模块离线或在线 [211](#)

受信任点 [94, 99, 104](#)

创建 [99](#)

关于 [94](#)

删除 [104](#)

数据包捕获 [219, 220, 222, 223, 224](#)

创建数据包捕获会话 [220](#)

启动数据包捕获会话 [223](#)

删除数据包捕获会话 [224](#)

停止数据包捕获会话 [223](#)

下载 PCAP 文件 [223](#)

filter [222](#)

思科安全包 [37, 38](#)

从 Cisco.com 下载 [38](#)

关于 [37](#)

上传到 Firepower 安全设备 [38](#)

损坏的文件系统 **233**
 恢复 **233**

T

停用安全模块 **209**
 通信服务 **89, 94, 95, 96, 97, 99, 100**
 HTTPS **94, 95, 96, 97, 99, 100**
 SNMP **89**
 通知 **87**
 关于 **87**
 退出逻辑设备连接 **191**

W

威胁防御 **165, 170, 182, 191, 193, 194**
 创建独立威胁防御逻辑设备 **170**
 创建集群 **165, 182**
 连接到 **191**
 删除逻辑设备 **193**
 删除应用实例 **194**
 退出连接 **191**
 系统恢复 **228, 233**
 系统日志 **114**
 配置本地目的 **114**
 配置本地源 **114**
 配置远程目的 **114**

X

下载数据包捕获文件 **223**
 陷阱 **87, 90, 91**
 创建 **90**
 关于 **87**
 删除 **91**
 许可证颁发机构 **16**

Y

映像 **37, 38, 39**
 从 Cisco.com 下载 **38**
 管理 **37**
 上传到 Firepower 安全设备 **38**
 升级 Firepower 可扩展操作系统平台捆绑包 **39**
 验证完整性 **39**
 映像版本 **40**
 更新 **40**
 用户 **21, 22, 23, 26, 27, 34, 35, 36, 91, 93**
 本地身份验证 **26, 36**
 创建 **34**
 管理 **21**

用户 (续)
 激活 **35**
 角色 **26**
 密码准则 **23**
 命名准则 **22**
 默认身份验证 **27**
 删除 **35**
 停用 **35**
 settings **27**
 SNMP **91, 93**
 用户界面 **1**
 概述 **1**
 用户账户 **26, 36**
 密码配置文件 **26, 36**

Z

账户 **26, 36**
 本地身份验证 **26, 36**
 重新初始化安全模块 **210**
 重新启动 **70**
 重置安全模块 **210**
 注册许可证 **16**
 自动注销 **61**
 AAA **107, 108, 110, 112, 113**
 LDAP 提供程序 **107, 108, 110**
 RADIUS 提供程序 **110, 112**
 TACACS+ 提供程序 **112, 113**
 asa **40, 165, 169, 178, 191, 193, 194**
 创建独立 asa 逻辑设备 **169**
 创建集群 **165, 178**
 更新映像版本 **40**
 连接到 **191**
 删除逻辑设备 **193**
 删除应用实例 **194**
 退出连接 **191**
 asa 映像 **37, 38**
 从 Cisco.com 下载 **38**
 关于 **37**
 上传到 Firepower 安全设备 **38**
 authentication **27**
 default **27**
 authNoPriv **87**
 authPriv **87**
 banner **67, 68, 69**
 pre-login **67, 68, 69**
 call home **15**
 配置 HTTP 代理 **15**
 certificate **94**
 关于 **94**
 CLI, 请参阅 命令行界面

- clustering **162**
 - 成员要求 **162**
 - 软件要求 **162**
 - 升级软件 **162**
- CSP, 请参阅 思科安全包
- DNS **117**
- Firepower 安全设备 **1**
 - 概述 **1**
- Firepower 机箱 **2, 6, 70**
 - 初始配置 **6**
 - 断开 **70**
 - 监控状态 **2**
 - 重新启动 **70**
- Firepower 机箱管理器 **1, 8, 61**
 - 登录或注销 **8**
 - 用户界面概述 **1**
 - 自动注销 **61**
- Firepower 可扩展操作系统 **39**
 - 升级平台捆绑包 **39**
- Firepower 平台捆绑包 **37, 38, 39**
 - 从 Cisco.com 下载 **38**
 - 关于 **37**
 - 上传到 Firepower 安全设备 **38**
 - 升级 **39**
 - 验证完整性 **39**
- Firepower 威胁防御, 请参阅 威胁防御
- fpga **41**
 - 升级 **41**
- ftd, 请参阅 威胁防御
- FXOS 机箱, 请参阅 Firepower 机箱
- HTTP 代理 **15**
 - 配置 **15**
- HTTPS **8, 29, 30, 94, 95, 96, 97, 99, 100, 102, 103, 105**
 - 创建密钥环 **94**
 - 导入证书 **100**
 - 登录或注销 **8**
 - 更改端口 **103**
 - 禁用 **105**
 - 配置 **102**
 - 受信任点 **99**
 - 证书请求 **96, 97**
 - 重新生成密钥环 **95**
 - timeout **29, 30**
- LDAP **107, 108, 110**
- LDAP 提供程序 **108, 110**
 - 创建 **108**
 - 删除 **110**
- license **16**
 - 注册 **16**
- noAuthNoPriv **87**
- NTP **80, 81, 82**
 - 配置 **80, 81**
 - 删除 **82**
 - 添加 **81**
- PCAP, 请参阅 数据包捕获
- PCAP 文件 **223**
 - 下载 **223**
- ping **224**
- PKI **94**
- RADIUS **110, 112**
 - RADIUS 提供程序 **110, 112**
 - 创建 **110**
 - 删除 **112**
- rommon **41**
 - 升级 **41**
- RSA **94**
- smart call home **15**
 - 配置 HTTP 代理 **15**
- SNMP **86, 87, 88, 89, 90, 91, 93**
 - 安全级别 **87**
 - 版本 3 安全功能 **88**
 - 关于 **86**
 - 启用 **89**
 - 权限 **87**
 - 通知 **87**
 - 陷阱 **90, 91**
 - 创建 **90**
 - 删除 **91**
 - 用户 **91, 93**
 - 创建 **91**
 - 删除 **93**
 - 支持 **86, 88**
 - community **89**
- SNMPv3 **88**
 - 安全功能 **88**
- SSH **29, 30, 83**
 - 配置 **83**
 - timeout **29, 30**
- system **6**
 - 初始配置 **6**
- TACACS+ **112, 113**
 - TACACS+ 提供程序 **112, 113**
 - 创建 **112**
 - 删除 **113**
- Telnet **29, 30, 85**
 - 配置 **85**
 - timeout **29, 30**
- time **80, 82**
 - 查看 **80**
 - 手动设置 **82**
- timeout **29, 30**
 - 控制台 **29, 30**

timeout (续)

HTTPS、SSH 和 Telnet [29, 30](#)

traceroute [224](#)

连接测试 [224](#)

