思科 Firepower 4100/9300 FXOS CLI 配置指南，2.10(1)

首次发布日期: 2021 年 5 月 26 日

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

目录

第 1 章

Firepower 安全设备简介 1

关于 Firepower 安全设备 1

逻辑设备如何与以下产品一起使用： Firepower 1

支持的应用 2

监控机箱运行状况 2

第 2 章

CLI 概述 5

受管对象 5

命令模式 5

FXOS CLI 连接图 7

对象命令 8

完成命令 9

命令历史记录 9

提交、丢弃和查看待处理命令 9

CLI 的内联帮助 10

CLI 会话限制 10

第 3 章

使用入门 11

任务流 11

初始配置 11

使用控制台端口的初始配置 12

使用管理端口的低接触调配 14

访问 FXOS CLI 18

第 4 章

ASA 的许可证管理 21
关于智能软件许可 21
适用于 ASA 的智能软件许可 21
智能软件管理器和账户 22
离线管理 22
永久许可证预留 22
卫星服务器 23
按虚拟账户管理的许可证和设备 23
评估许可证 23
智能软件管理器通信 23
设备注册和令牌 24
与许可证颁发机构的定期通信 24
不合规状态 24
Smart Call Home 基础设施 24
思科成功网络 25
思科成功网络遥测数据 25
智能软件许可必备条件 35
智能软件许可准则 35
智能软件许可的默认设置 36
配置定期智能软件许可 36
（可选）配置 HTTP 代理 36
（可选）删除 Call Home URL 37
向许可证颁发机构注册 Firepower 安全设备 38
更改 Cisco Success Network 注册 39
配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱 40
配置永久许可证预留 41
安装永久许可证 41
（可选）返还永久许可证 43
监控智能软件许可 43
智能软件许可历史记录 44

第 5 章 用户管理 47

用户帐户 47
面向用户名的指导原则 48
密码的指导原则 49
远程身份验证指导原则 50
用户角色 52
本地身份验证用户的密码配置文件 52
选择默认身份验证服务 53
配置会话超时 55
配置绝对会话超时 56
为远程用户配置角色策略 57
为本地身份验证的用户启用密码强度检查 57
设置最大尝试登录次数 58
查看和清除用户锁定状态 59
配置更改间隔的最大密码更改次数 60
配置最小密码长度检查 61
为密码配置无更改间隔 61
配置密码历史记录计数 62
创建本地用户账户 63
删除本地用户账户 65
激活或停用本地用户账户 66
清除本地身份验证的用户的密码历史记录 66

第 6 章 映像管理 69

关于映像管理 69
从 Cisco.com 下载映像 70
将Firepower eXtensible Operating System软件映像下载到 Firepower 4100/9300 机箱 70
验证映像的完整性 72
升级 Firepower eXtensible Operating System平台捆绑包 73
将逻辑设备软件映像下载到 Firepower 4100/9300 机箱 74

更新逻辑设备的映像版本 76
固件升级 78
手动降级到版本 2.0.1 或更低版本 78

第 7 章 安全认证合规性 81
安全认证合规性 81
生成 SSH 主机密钥 82
配置 IPSec 安全通道 83
配置信任点静态 CRL 89
关于证书撤销吊销列表检查 89
配置 CRL 定期下载 93
设置 LDAP 密钥环证书 95
启用客户端证书身份验证 96

第 8 章 系统管理 99
更改管理 IP 地址 99
更改应用管理 IP 101
更改 Firepower 4100/9300 机箱名称 104
安装受信任身份证书 104
登录前横幅 110
创建登录前横幅 110
修改登录前横幅 111
删除登录前横幅 112
重新启动 Firepower 4100/9300 机箱 113
关闭 Firepower 4100/9300 机箱电源 114
恢复出厂默认配置 114
安全地擦除系统组件 115

第 9 章 平台设置 117
设置日期和时间 117
查看配置的日期和时间 118

设置时区 118
使用 NTP 设置日期和时间 120
删除 NTP 服务器 122
手动设置日期和时间 123
配置 SSH 124
配置 TLS 128
配置 Telnet 130
配置 SNMP 130
关于 SNMP 131
SNMP 通知 131
SNMP 安全级别和权限 132
支持的 SNMP 安全模型和级别组合 132
SNMPv3 安全功能 133
SNMP 支持 133
启用 SNMP 并配置 SNMP 属性 134
创建 SNMP 陷阱 135
删除 SNMP 陷阱 137
创建 SNMPv3 用户 137
删除 SNMPv3 用户 139
查看当前的 SNMP 设置 139
配置 HTTPS 141
证书、密钥环和受信任点 141
创建密钥环 142
重新生成默认密钥环 142
创建密钥环的证书请求 143
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 143
使用高级选项创建密钥环的证书请求 144
创建受信任点 147
将证书导入密钥环 148
配置 HTTPS 149
更改 HTTPS 端口 151

重新启动 HTTPS 151
删除密钥环 152
删除受信任点 153
禁用 HTTPS 153
配置 AAA 154
关于 AAA 154
设置 AAA 155
配置 LDAP 提供程序 156
配置 RADIUS 提供程序 161
配置 TACACS+ 提供程序 164
验证远程 AAA 服务器配置 166
配置系统日志 168
配置 DNS 服务器 170
启用 FIPS 模式 171
启用通用标准模式 172
配置 IP 访问列表 173
为容器实例接口添加 MAC 池前缀，并查看其 MAC 地址 174
为容器实例添加资源配置文件 176
配置网络控制策略 179
配置机箱 URL 181

第 10 章 接口管理 185
关于 Firepower 接口 185
机箱管理接口 185
接口类型 186
FXOS 接口与应用接口 187
硬件旁路对 189
巨帧支持 190
共享接口可扩展性 190
共享接口最佳实践 191
共享接口使用示例 192

查看共享接口资源 202
Firepower 威胁防御的内联集链路状态传播 202
Firepower 接口的准则和限制 203
配置接口 205
配置物理接口 205
添加 EtherChannel（端口通道） 207
为容器实例添加 VLAN 子接口 210
配置分支电缆 212
配置流量控制策略 213
监控接口 215
排除接口故障 217
接口历史 223

第 11 章 逻辑设备 225
关于逻辑设备 225
独立和群集逻辑设备 225
逻辑设备应用程序实例：容器和本地 226
容器实例接口 226
机箱如何将数据包分类 226
分类示例 227
级联容器实例 230
典型多实例部署 231
容器实例接口的自动 MAC 地址 232
容器实例资源管理 233
多实例功能的性能扩展因素 233
容器实例与高可用性 233
容器实例和集群 233
逻辑设备的要求和必备条件 233
硬件和软件组合的要求与前提条件 233
群集要求和必备条件 235
高可用性的要求和前提条件 239

容器实例的要求和必备条件 240
逻辑设备的准则和限制 241
一般准则和限制 241
集群准则和限制 242
添加独立的逻辑设备 246
添加独立 ASA 246
为 FMC 添加独立的 Firepower 威胁防御 252
为 FDM 添加独立的 Firepower 威胁防御 264
添加高可用性对 273
添加群集 274
关于 Firepower 4100/9300 机箱上的群集 274
主设备角色和辅助设备角色 275
集群控制链接 275
管理网络 277
管理接口 277
跨网络 EtherChannel 277
站点间群集 278
添加 ASA 群集 279
创建 ASA 集群 279
添加更多群集成员 287
添加 Firepower 威胁防御群集 288
创建 Firepower 威胁防御集群 288
添加更多集群设备 308
配置 Radware DefensePro 309
关于 Radware DefensePro 309
Radware DefensePro 的必备条件 309
服务链准则 309
在独立逻辑设备上配置 Radware DefensePro 310
在机箱内集群上配置 Radware DefensePro 313
开放 UDP/TCP 端口和启用 vDP Web 服务 318
配置 TLS 加密加速 319

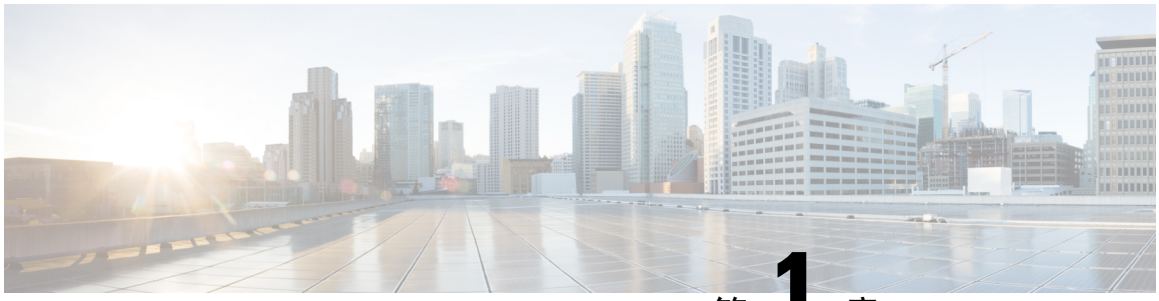
关于 TLS 加密加速 319
TLS 加密加速的准则和限制 319
启用容器实例的 TLS 加密加速 321
查看 TLS 加密加速的状态 321
管理逻辑设备 322
连接到应用控制台 322
删除逻辑设备 324
删除群集设备 325
删除与逻辑设备不关联的应用实例 326
更改 Firepower 威胁防御逻辑设备上的接口 327
更改 ASA 逻辑设备上的接口 331
监控逻辑设备 332
站点间群集示例 334
具有站点特定的 MAC 地址的跨网络 EtherChannel 路由模式示例 334
跨网络 EtherChannel 透明模式南北站点间群集示例 335
跨网络 EtherChannel 透明模式东西站点间集群示例 336
逻辑设备的历史记录 337

第 12 章 安全模块/引擎管理 343
关于 FXOS 安全模块/安全引擎 343
停用安全模块 344
确认安全模块/引擎 344
重启安全模块/引擎 345
重新初始化安全模块/引擎 346
使网络模块离线或在线 347

第 13 章 配置导入/导出 349
关于配置导入/导出 349
为配置导入/导出设置加密密钥 350
导出 FXOS 配置文件 351
计划自动配置导出 353

设置配置导出提醒 354
导入配置文件 355

第 14 章 故障排除 359
数据包捕获 359
背板端口映射 359
数据包捕获准则和限制 360
创建或编辑数据包捕获会话 360
配置数据包捕获的过滤器 364
启动和停止数据包捕获会话 365
下载数据包捕获文件 366
删除数据包捕获会话 366
测试网络连接 367
管理接口状态故障排除 369
确定端口通道状态 369
从软件故障中恢复 372
从损坏的文件系统中恢复 376
管理员密码未知时恢复出厂默认配置 386
生成故障排除日志文件 388
启用 Firepower 模块核心转储 390
查找序列号 Firepower 4100/9300 机箱 391
重建 RAID 虚拟驱动器 392
确定 SSD 的问题 393



第 1 章

Firepower 安全设备简介

- 关于 Firepower 安全设备， 第 1 页
- 监控机箱运行状况， 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。

逻辑设备如何与以下产品一起使用： Firepower

Firepower 在名为 Firepower 可扩展操作系统 (FXOS) 的管理引擎上运行其操作系统。即用型 Firepower 机箱管理器提供简单的基于 GUI 的管理功能。您可以使用 FXOS CLI 在管理引擎上配置硬件接口设置、智能许可（适用于 ASA）和其他基本运行参数。

逻辑设备允许您运行一个应用实例和一个可选的修饰器应用以形成服务链。部署逻辑设备时，管理引擎将下载您选择的应用映像，并创建默认配置。然后，您可以在应用操作系统中配置安全策略。

逻辑设备不能彼此形成服务链，也不能通过背板彼此通信。所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。对于容器实例，可以共享数据接口；只有在这种情况下，多个逻辑设备才能通过背板进行通信。

支持的应用

您可以使用以下应用类型在机箱上部署逻辑设备。

Firepower 威胁防御

FTD 提供各种下一代防火墙服务，包括状态防火墙、路由、下一代入侵防御系统 (NGIPS)、应用可视性与可控性 (AVC)、URL 过滤，以及高级恶意软件防护 (AMP)。

您可以使用以下管理器之一

- FMC- 位于单独服务器上的功能齐全的多设备管理器。
- Firepower 设备管理器 (FDM) - 设备上的一个简化的单设备管理器。
- 思科防御协调器 (CDO) — 一种基于云的多设备管理器。

ASA

ASA 在一台设备中提供高级状态防火墙和 VPN 集中器功能。您可以使用以下任一管理器管理 ASA：

- ASDM - 设备上的单设备管理器。
- CLI
- 思科防御协调器 (CDO) — 一种基于云的多设备管理器。
- 思科安全管理器 - 位于单独的服务器上的多设备管理器。

Radware DefensePro （修饰器）

您可以安装 Radware DefensePro (vDP) 以在 ASA 前面运行，或者安装 FTD 作为修饰器应用程序。vDP 是基于 KVM 的虚拟平台，可在 Firepower 上提供分布式拒绝服务 (DDoS) 检测和缓解功能。来自网络的流量必须先经过 vDP，然后才能到达 ASA 或 FTD。

监控机箱运行状况

您可使用 **show environment summary** 命令查看显示Firepower 4100/9300 机箱整体运行状况的以下各条信息：

- 总功耗 (Total Power Consumption) - 总功耗（以瓦为单位）。
- 入口温度 (Inlet Temperature) - 环境系统温度（以摄氏度为单位）。
- CPU 温度 (CPU Temperature) - 处理器温度（以摄氏度为单位）。
- 电源类型 (Power Supply Type) - 交流或直流。
- 电源入口进给状态 (Power Supply Input Feed Status) - 输入状态（“正常 [Ok]”、“故障 [Fault]”）。

- 电源输出状态 (Power Supply Output Status) - 12V 输出状态（“正常 [Ok]”、“故障 [Fault]”）。
- 电源整体状态 (Power Supply Overall Status) - PSU 的整体运行状况（“可运行 [Operable]”、“已取下 [Removed]”、“热问题 [Thermal problem]”）。
- 风扇速度 RPM (Fan Speed RPM) - 单个风扇托架中两个风扇的最高 RPM。
- 风扇速度状态 (Fan Speed Status) - 风扇速度（“缓慢 [Slow]”、“正常 [Ok]”、“高 [High]”、“重要 [Critical]”）。
- 风扇整体状态 (Fan Overall Status) - 风扇的整体运行状况（“可运行 [Operable]”、“已取下 [Removed]”、“热问题 [Thermal problem]”）。
- 刀片总功耗 (Blade Total Power Consumption) - 安全模块/引擎的总功耗（以瓦为单位）。
- 刀片处理器温度 (Blade Processor Temperature) - 安全模块/引擎上处理器的最高温度（以摄氏度为单位）。

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 18 页）。

步骤 2 进入机箱模式：

Firepower-chassis# **scope chassis 1**

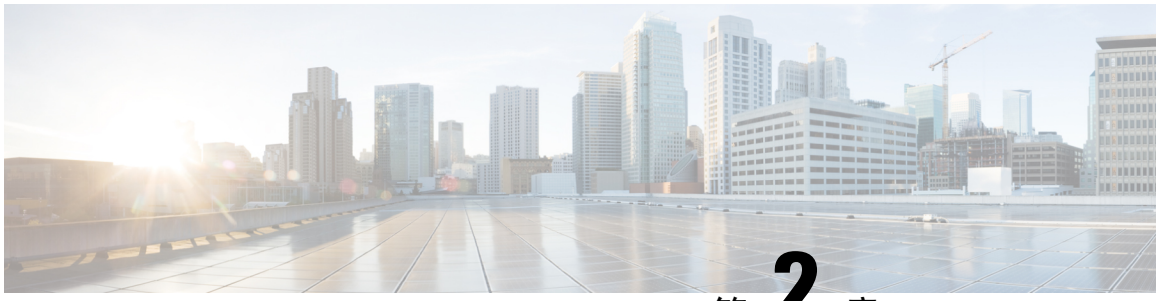
步骤 3 要查看机箱运行状况摘要，请输入以下命令：

Firepower-chassis /chassis # **show environment summary**

示例

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # show environment summary

Chassis INFO :

Total Power Consumption: 638.000000
Inlet Temperature (C): 32.000000
CPU Temperature (C): 47.000000
Last updated Time: 2017-01-05T23:34:39.115

PSU 1:
Type: AC
Input Feed Status: Ok
12v Output Status: Ok
Overall Status: Operable
PSU 2:
Type: AC
Input Feed Status: Ok
12v Output Status: Ok
Overall Status: Operable
```

```
FAN 1
Fan Speed RPM (RPM): 3168
Speed Status: Ok
Overall Status: Operable
FAN 2
Fan Speed RPM (RPM): 3388
Speed Status: Ok
Overall Status: Operable
FAN 3
Fan Speed RPM (RPM): 3168
Speed Status: Ok
Overall Status: Operable
FAN 4
Fan Speed RPM (RPM): 3212
Speed Status: Ok
Overall Status: Operable

BLADE 1:
Total Power Consumption: 216.000000
Processor Temperature (C): 58.000000
BLADE 2:
Total Power Consumption: 222.000000
Processor Temperature (C): 62.500000
```



第 2 章

CLI 概述

- 受管对象， 第 5 页
- 命令模式， 第 5 页
- FXOS CLI 连接图， 第 7 页
- 对象命令， 第 8 页
- 完成命令， 第 9 页
- 命令历史记录， 第 9 页
- 提交、丢弃和查看待处理命令， 第 9 页
- CLI 的内联帮助, on page 10
- CLI 会话限制， 第 10 页

受管对象

Firepower eXtensible Operating System (FXOS) 使用受管对象模型（受管对象为可管理的物理或逻辑实体的抽象表示形式）。例如，机箱、安全模块、网络模块、端口和处理器是表示为受管对象的物理实体，许可证、用户角色和平台策略是表示为受管对象的逻辑实体。

受管对象可能具有一个或多个可以配置的关联属性。

命令模式

CLI 组织为命令模式层次结构，该层次结构的最高级别模式为 EXEC 模式。较高级别模式划分为较低级别模式。使用 **create**、**enter** 和 **scope** 命令可从较高级别模式移到下一较低级别模式，而使用 **up** 命令可在模式层次结构中上移一个级别。您还可以使用 **top** 命令移至模式层次结构中的顶级。

注释 大多数命令模式与受管对象关联，因此必须先创建对象，然后才能访问与该对象关联的模式。使用 **create** 和 **enter** 命令可为受访问的模式创建受管对象。**scope** 命令不创建受管对象，并且只能访问已存在受管对象的模式。

每个模式均包含可在该模式下输入的命令集。每个模式中可用的大多数命令都与关联受管对象相关。

每个模式的 CLI 提示符可显示模式层次结构下的当前模式的完整路径。这可帮助您确定您在命令模式层次结构中的位置，并且在您需要浏览层次结构时会是一个宝贵的工具。

下表列出主要命令模式、用于访问各模式的命令以及与各模式关联的 CLI 提示符。

表 *1:* 主要命令模式和提示符

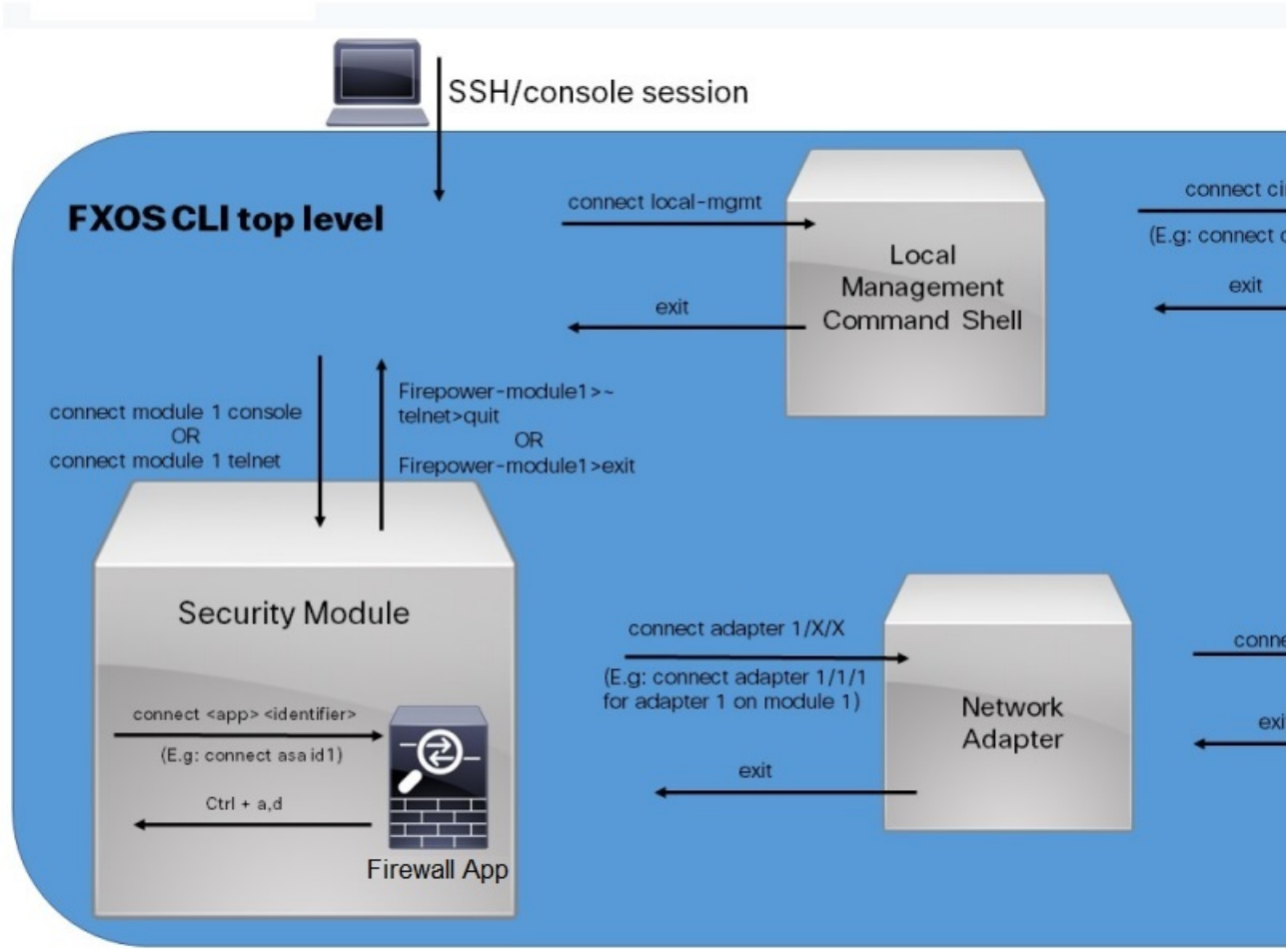
模式名称	用于访问的命令	模式提示符
EXEC	适用于任何模式的 **top** 命令	`#`
适配器	适用于 EXEC 模式的 **scope adapter** 命令	`/adapter #`
布线	适用于 EXEC 模式的 **scope cabling** 命令	`/cabling #`
机箱	适用于 EXEC 模式的 **scope chassis** 命令	`/chassis #`
以太网服务器域	适用于 EXEC 模式的 **scope eth-server** 命令；当前不支持此命令和所有子命令	`/eth-server #`
以太网上行链路	适用于 EXEC 模式的 **scope eth-uplink** 命令	`/eth-uplink #`
交换矩阵互联	适用于 EXEC 模式的 **scope fabric-interconnect** 命令	`/fabric-interconnect #`
固件	适用于 EXEC 模式的 **scope firmware** 命令	`/firmware #`
主机以太网接口	适用于 EXEC 模式的 **scope host-eth-if** 命令 **注释** 此级别不支持此命令和所有子命令；在 `/adapter #` 模式下可使用主机以太网接口命令。	`/host-eth-if #`
许可证	适用于 EXEC 模式的 **scope license** 命令	`/license #`
监控	适用于 EXEC 模式的 **scope monitoring** 命令	`/monitoring #`
Organization	适用于 EXEC 模式的 **scope org** 命令	`/org #`
数据包捕获	适用于 EXEC 模式的 **scope packet-capture** 命令	`/packet-capture #`
安全	适用于 EXEC 模式的 **scope security** 命令	`/security #`
服务器	适用于 EXEC 模式的 **scope server** 命令	`/server #`

模式名称	用于访问的命令	模式提示符
服务配置文件	适用于 EXEC 模式的 **scope service-profile** 命令 **注释** 不要更改或配置服务配置文件；换言之，不要使用 **create**、**set** 或 **delete** 子命令集。	`/service-profile #`
SSA	适用于 EXEC 模式的 **scope ssa** 命令	`/ssa #`
System	适用于 EXEC 模式的 **scope system** 命令	`/system #`
虚拟 HBA	适用于 EXEC 模式的 **scope vhba** 命令 **注释** 当前不支持此命令和所有子命令。	`/vhba #`
虚拟 NIC	适用于 EXEC 模式的 **scope vnic** 命令	`/vnic #`

FXOS CLI 连接图

下图概述了可从 FXOS CLI 顶层执行的各种命令，以便访问 FXOS 命令 shell、本地管理命令 shell、网络适配器、CIMC 和安全模块 CLI。

图 *1: Firepower 4100/9300 FXOS CLI* 连接图



对象命令

四个通用命令可用于对象管理：

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

可以将 **scope** 命令用于任何受管对象（无论是永久对象，还是用户实例化对象）。其他命令用于创建和管理用户实例化对象。对于每个 **create** *object* 命令，都存在一个对应的 **delete** *object* and **enter** *object* 命令。

在用户实例化对象的管理中，这些命令的行为取决于对象是否存在，如下表中所述：

表 *2:* 对象不存在时的命令行为

命令	行为
create *object*	创建对象并进入其配置模式（如果适用）。
delete *object*	生成错误消息。
enter *object*	创建对象并进入其配置模式（如果适用）。
scope *object*	生成错误消息。

表 *3:* 对象存在时的命令行为

命令	行为
create *object*	生成错误消息。
delete *object*	删除对象。
enter *object*	进入对象的配置模式（如果适用）。
scope *object*	进入对象的配置模式。

完成命令

可以在任何模式下使用 **Tab** 键来完成命令。键入部分命令名称并按 **Tab** 键，会使命令完全显示或转到必须输入其他关键字或参数值的位置。

命令历史记录

CLI 可存储当前会话中使用的所有命令。您可以使用向上箭头键或向下箭头键逐条浏览之前使用过的命令。向上箭头键将移至历史记录中的上一条命令，向下箭头键将移至历史记录中的下一条命令。当浏览至历史记录的末尾时，按向下箭头键将不起任何作用。

您可以通过逐条浏览历史记录以重新调用该命令，然后按**Enter**，从而输入历史记录中的任何命令。命令的输入就如同您手动键入一样。您也可以重新调用命令，并在按 **Enter** 键之前更改该命令。

提交、丢弃和查看待处理命令

当在 CLI 中输入配置命令时，将不会应用该命令，直至输入 **commit-buffer** 命令为止。直到提交后，配置命令才处于待处理状态，并可通过输入 **discard-buffer** 命令进行放弃。

可以累积多命令模式下的待处理更改，并将其与单个 **commit-buffer** 命令一起应用。可以通过在任意命令模式下输入 **show configuration pending** 命令来查看待处理命令。

注释 检查所有挂起的命令是否有效。但是，如果在提交期间排队中的任何命令失败，系统会应用其余命令；错误消息中会报告失败的命令。

当所有命令处于待处理状态时，在命令提示符之前会出现星号 (*)。输入 **commit-buffer** 命令时，星号会消失。

以下示例显示提示符在命令输入过程中如何更改：

```
Firepower# scope system
Firepower /system # scope services
Firepower /system/services # create ntp-server 192.168.200.101
Firepower /system/services* # show configuration pending
 scope services
+    create ntp-server 192.168.200.101
 exit
Firepower /system/services* # commit-buffer
Firepower /system/services #
```

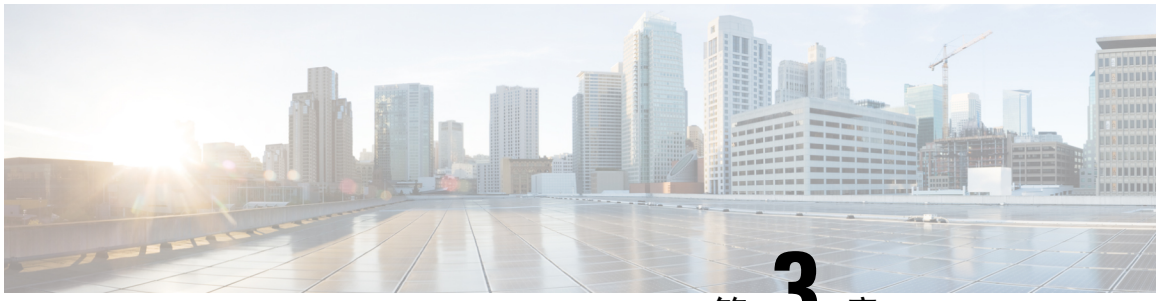
CLI 的内联帮助

您可以随时键入 **?** 字符来显示在命令语法的当前状态下可用的选项。

如果尚未在提示符处输入任何内容，则输入 **?** 会列出您所处模式的所有可用命令。对于已部分输入的命令，输入 **?** 会列出命令语法中当前位置提供的所有关键字和参数。

CLI 会话限制

FXOS 将一次可处于活动状态的 CLI 会话数限制为总共 32 个会话。该值不可配置。



第 3 章

使用入门

- 任务流，第 11 页
- 初始配置，第 11 页
- 访问 FXOS CLI，第 18 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 11 页）。

步骤 3 设置日期和时间（请参阅设置日期和时间，第 117 页）。

步骤 4 配置 DNS 服务器（请参阅配置 DNS 服务器，第 170 页）。

步骤 5 注册产品许可证（请参阅 ASA 的许可证管理，第 21 页）。

步骤 6 配置用户（请参阅用户管理，第 47 页）。

步骤 7 按需执行软件更新（请参阅映像管理，第 69 页）。

步骤 8 配置其他平台设置（请参阅平台设置，第 117 页）。

步骤 9 配置接口（请参阅接口管理，第 185 页）。

步骤 10 创建逻辑设备（请参阅逻辑设备，第 225 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，必须执行一些初始配置任务。您可以使用通过控制台端口访问的 FXOS CLI 或使用通过管理端口访问的 SSH、HTTPS 或 REST API 来执行初始配置（此程序也称为低接触调配）。

使用控制台端口的初始配置

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。

注释 要重复初始设置，您需要使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

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为如下所示：
   - 9600 波特率
   - 8 个数据位
   - 无奇偶校验
   - 1 个停止位
3. 收集以下信息以与设置脚本一起使用：
   - 新管理员密码
   - 管理 IP 地址和子网掩码
   - 网关 IP 地址
   - 要从中允许 HTTPS 和 SSH 访问的子网
   - 主机名和域名
   - DNS 服务器 IP 地址

过程

步骤 1 接通机箱电源。

步骤 2 使用终端仿真器连接到串行控制台端口。

Firepower 随附 RS-232 转 RJ-45 串行控制台电缆。可能需要使用第三方串口转 USB 电缆建立连接。使用以下串行参数：

- 9600 波特率
- 8 个数据位
- 无奇偶校验
- 1 个停止位

步骤 3 根据提示完成系统配置。

注释 您可以在初始配置期间随时进入调试菜单，以调试任何设置问题或中止配置并重新引导系统。要进入调试菜单，请按Ctrl-C。要退出调试菜单，请按两次Ctrl-D。请注意，您在第一次按下 Ctrl-D 与第二次按下 Ctrl-D 之间输入任何内容，都将在第二次按下后运行。

示例：

```
          ---- 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 FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or 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? (yes/no): y

Enforce strong password? (yes/no) [y]: n

Enter the password for "admin": Farscape&32
Confirm the password for "admin": Farscape&32
Enter the system name:  firepower-9300

Supervisor Mgmt IP address : 10.80.6.12

Supervisor Mgmt IPv4 netmask : 255.255.255.0

IPv4 address of the default gateway : 10.80.6.1

The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0
```

```
  SSH Mgmt Access IPv4 netmask: 255.0.0.0

  Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

  Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

  HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

  Configure the DNS Server IP address? (yes/no) [n]: y

    DNS IP address : 10.164.47.13

  Configure the default domain name? (yes/no) [n]: y

    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Cisco FPR Series Security Appliance
firepower-9300 login:  admin
Password: Farscape&32
Successful login attempts for user 'admin' : 1
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

[...]

firepower-chassis#
```

使用管理端口的低接触调配

当您的 Firepower 4100/9300 机箱 启动时，如果其找不到启动配置，设备将进入低接触调配模式，在该模式中，设备会寻找动态主机控制协议 (DHCP) 服务器，然后使用其管理接口 IP 地址自行启动。然后，您可以通过管理接口进行连接，以使用 SSH、HTTPS 或 FXOS REST API 配置系统。

注释 要重复初始设置，您需要使用以下命令清除任何现有配置：

```
Firepower-chassis# connect local-mgmt
firepower-chassis(local-mgmt)# erase configuration
```

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

收集以下信息以与设置脚本一起使用：

- 新管理员密码
- 管理 IP 地址和子网掩码
- 网关 IP 地址
- 要从中允许 HTTPS 和 SSH 访问的子网
- 主机名和域名
- DNS 服务器 IP 地址

过程

步骤 1 配置您的 DHCP 服务器以将 IP 地址分配到 Firepower 4100/9300 机箱 的管理端口。

来自 Firepower 4100/9300 机箱 的 DHCP 客户端请求将包含以下内容：

- 管理接口的 MAC 地址。
- DHCP 选项 60 (vendor-class-identifier) - 设置为“FPR9300”或“FPR4100”。
- DHCP 选项 61(dhcp-client-identifier) - 设置为 Firepower 4100/9300 机箱 序列号。此序列号可在机箱的拉出卡舌上找到。

步骤 2 打开 Firepower 4100/9300 机箱 的电源。
如果在机箱启动时找不到启动配置，设备将进入低接触调配模式。

步骤 3 要使用 HTTPS 配置系统：

a) 使用支持的浏览器，在地址栏中输入以下 URL：

https://<*ip_address*>/api

其中 <*ip_address*> 是您的 DHCP 服务器分配的 Firepower 4100/9300 机箱 上的管理端口 IP 地址。

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

b) 系统提示时，使用用户名 **install** 和密码 <*chassis_serial_number*> 登录。

检查机箱上的标签可获取 <*chassis_serial_number*> 。

c) 根据提示完成系统配置。

- 强密码执行策略（对于强密码准则，请参阅用户帐户 ， 第 47 页）
- 管理员帐户的密码。
- 系统名称
- 监控程序管理端口 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。
- 允许使用 SSH 访问的主机/网络地址和网络掩码/前缀。
- 允许使用 HTTPS 访问的主机/网络地址和网络掩码/前缀。
- DNS 服务器 IPv4 或 IPv6 地址。
- 默认域名。

d) 单击**提交**。

步骤 4 要使用 SSH 配置系统：

a) 使用以下命令连接到管理端口：

ssh install@*<ip_address>*

其中 <*ip_address*> 是您的 DHCP 服务器分配的 Firepower 4100/9300 机箱 上的管理端口 IP 地址。

b) 出现提示时，使用密码 **Admin123** 登录。

c) 根据提示完成系统配置。

注释 您可以在初始配置期间随时进入调试菜单，以调试任何设置问题或中止配置并重新引导系统。要进入调试菜单，请按 Ctrl-C。要退出调试菜单，请按两次 Ctrl-D。请注意，您在第一次按下 Ctrl-D 与第二次按下 Ctrl-D 之间输入任何内容，都将在第二次按下后运行。

示例：

```
          ---- 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 FXOS Supervisor is performed through these steps.

  Type Ctrl-C at any time for more options or 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? (yes/no): y

  Enforce strong password? (yes/no) [y]: n

  Enter the password for "admin": Farscape&32
  Confirm the password for "admin": Farscape&32
  Enter the system name:  firepower-9300

  Supervisor Mgmt IP address : 10.80.6.12

  Supervisor Mgmt IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 10.80.6.1

  The system cannot be accessed via SSH if SSH Mgmt Access is not configured.

  Do you want to configure SSH Mgmt Access? (yes/no) [y]: y

  SSH Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  SSH Mgmt Access IPv4 netmask: 255.0.0.0

  Firepower Chassis Manager cannot be accessed if HTTPS Mgmt Access is not configured.

  Do you want to configure HTTPS Mgmt Access? (yes/no) [y]: y

  HTTPS Mgmt Access host/network address (IPv4/IPv6): 10.0.0.0

  HTTPS Mgmt Access IPv4 netmask: 255.0.0.0

  Configure the DNS Server IP address? (yes/no) [n]: y

    DNS IP address : 10.164.47.13

  Configure the default domain name? (yes/no) [n]: y

    Default domain name : cisco.com

  Following configurations will be applied:

    Switch Fabric=A
    System Name=firepower-9300
    Enforced Strong Password=no
    Supervisor Mgmt IP Address=10.89.5.14
    Supervisor Mgmt IP Netmask=255.255.255.192
    Default Gateway=10.89.5.1
    SSH Access Configured=yes
        SSH IP Address=10.0.0.0
        SSH IP Netmask=255.0.0.0
    HTTPS Access Configured=yes
        HTTPS IP Address=10.0.0.0
        HTTPS IP Netmask=255.0.0.0
    DNS Server=72.163.47.11
    Domain Name=cisco.com

  Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y
  Applying configuration. Please wait...  Configuration file - Ok
.....

Initial Setup complete, Terminating sessions
.Connection to <ip_address> closed.
```

步骤 5 要使用 FXOS REST API 配置您的系统：

使用以下示例通过 REST API 配置系统。有关详细信息，请参阅https://developer.cisco.com/site/ssp/firepower/。

注释　属性 dn、domain_name、https_net、https_mask、ssh_net 和 ssh_mask 都为选填。REST API 配置的所有其他属性都为必填。

```
IPv4 REST API example:

{
    "fxosBootstrap": {
        "dns": "1.1.1.1",
        "domain_name": "cisco.com",
        "mgmt_gw": "192.168.0.1",
        "mgmt_ip": "192.168.93.3",
        "mgmt_mask": "255.255.0.0",
        "password1": "admin123",
        "password2": "admin123",
        "strong_password": "yes",
        "system_name": "firepower-9300",
        "https_mask": "2",
        "https_net": "::",
        "ssh_mask": "0",
        "ssh_net": "::"
    }
}


IPV6 REST API example

{
    "fxosBootstrap": {
        "dns": "2001::3434:4343",
        "domain_name": "cisco.com",
        "https_mask": "2",
        "https_net": "::",
        "mgmt_gw": "2001::1",
        "mgmt_ip": "2001::2001",
        "mgmt_mask": "64",
        "password1": "admin123",
        "password2": "admin123",
        "ssh_mask": "0",
        "ssh_net": "::",
        "strong_password": "yes",
        "system_name": "firepower-9300"
    }
}
```

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 eXtensible Operating System 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，Telnet 处于禁用状态。有关启用 Telnet 的说明，请参阅配置 Telnet，第 130 页。

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

```
telnet ucs-qa-10
login: ucs-ldap23\blradmin
```

- **telnet ucs-**{*UCSM-ip-address* | *UCSM-ipv6-address*}*ucs-auth-domain**username*

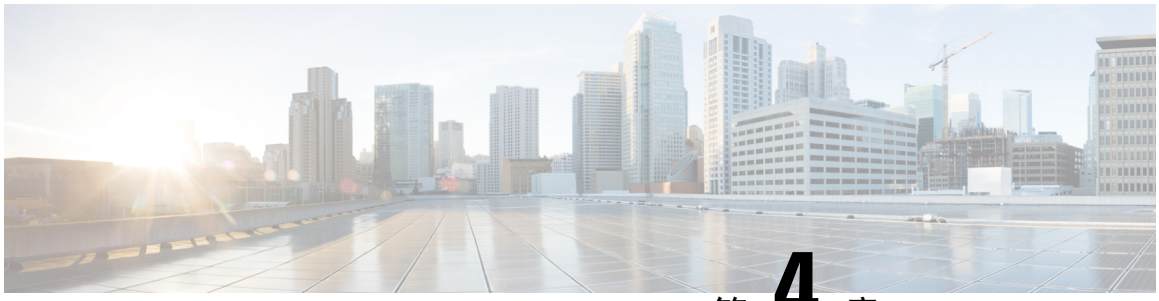
```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

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 4 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 21 页
- 智能软件许可必备条件， 第 35 页
- 智能软件许可准则， 第 35 页
- 智能软件许可的默认设置， 第 36 页
- 配置定期智能软件许可， 第 36 页
- 配置智能许可证卫星服务器用于 Firepower 4100/9300 机箱， 第 40 页
- 配置永久许可证预留， 第 41 页
- 监控智能软件许可， 第 43 页
- 智能软件许可历史记录， 第 44 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 机箱间群集需要您在群集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。

注释 Firepower 4100/9300 安全设备上不支持思科传输网关。

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，请单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。

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。

注释 如果您的设备在一年内无法与许可证颁发机构通信，则设备将进入未注册状态，但不会丧失任何以前启用的强加密功能。

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目的地址 URL。除非获得 Cisco TAC 的指示，否则不应更改许可证颁发机构 URL。

注释 Firepower 4100/9300 安全设备上不支持思科传输网关。

思科成功网络

思科成功网络是一项用户启用的云服务。启用思科成功网络时，Firepower 4100/9300 机箱与思科云之间会建立安全连接以传输使用情况信息和统计信息。流传输遥测数据可以提供一种机制，用于从 ASA 选择感兴趣的数据，并使用结构化格式将其传输到远程管理站，以便执行以下任务：

- 向您告知在网络中可用来改进产品效果的未使用功能。
- 向您告知可能适用于您的产品的其他技术支持服务和监控。
- 帮助思科改善我们的产品

将 Firepower 4100/9300注册到思科智能软件管理器时，可启用思科成功网络。请参阅向许可证颁发机构注册 Firepower 安全设备，第 38 页。

仅当满足以下所有条件时，才可以注册 Cisco Success Network：

- 已注册智能软件许可证。
- 已禁用智能许可证卫星模式。
- 已禁用永久许可证。

当您注册 Cisco Success Network 后，机箱总是会建立并维护安全的连接。您可以通过禁用思科成功网络随时关闭此连接，这样会将设备与思科成功网络云断开。

您可以在**系统 (System)** > **许可 (Licensing)** > **Cisco Success Network** 页面上查看当前的 Cisco Success Network 注册状态，还可以更改注册状态。请参阅更改 Cisco Success Network 注册，第 39 页。

思科成功网络遥测数据

Cisco Success Network 允许机箱每 24 小时向 Cisco Success Network 云端流传输一次配置和运行状态信息。收集和监控的数据包括：

- **注册设备信息** - Firepower 4100/9300 机箱 型号名称、产品标识符、序列号、UUID、系统正常运行时间和智能许可信息。请参阅已注册设备数据，第 26 页。
- **软件信息** - 在 Firepower 4100/9300 机箱 上运行的软件的类型和版本号。请参阅软件版本数据，第 26 页。
- **ASA 设备信息** - 与 Firepower 4100/9300 的 安全模块/引擎 上运行的 ASA 设备相关的信息。请注意，对于 Firepower 4100 系列，仅包含有关单个 ASA 设备的信息。ASA 设备信息包括每个设备的在用智能许可证、设备型号、序列号和软件版本。请参阅ASA 设备数据，第 27 页。
  - **性能信息** - ASA 设备的系统正常运行时间、CPU 使用率、内存使用率、磁盘空间使用情况和带宽使用信息。请参阅性能数据，第 27 页。

- **使用信息** - 功能状态、集群、故障切换和登录信息：
  - **功能状态** - 您已配置或默认启用的已启用 ASA 功能的列表。
  - **集群信息** - 如果 ASA 设备处于集群模式，则包括集群信息。如果 ASA 设备未处于集群模式，则不会显示此信息。集群信息包括ASA设备的集群组名称、集群接口模式、设备名称和状态。对于同一集群中的其他对等设备，这些信息包括名称、状态和序列号。
  - **故障切换信息** - 如果 ASA 处于故障切换模式，则包括故障切换信息。如果 ASA 未处于故障切换模式，则不会显示此信息。故障切换信息包括ASA的角色和状态，以及对等 ASA 设备的角色、状态和序列号。
  - **登录历史记录** - ASA 设备上的用户登录频率、登录时间和最近成功登录的日期戳。但是，登录历史记录不包括用户登录名、凭证或任何其他个人信息。

有关详细信息，请参阅使用数据，第 28 页。

已注册设备数据

在 Cisco Success Network 中注册 Firepower 4100/9300 机箱 后，选定的机箱相关遥测数据将流传输到思科云。下表说明所收集和监控的数据。

表 *4:* 已注册设备遥测数据

数据点	示例值
设备型号	思科 Firepower FP9300 安全设备
序列号	GMX1135L01K
智能许可证 PIID	752107e9-e473-4916-8566-e26d0c4a5bd9
智能许可证虚拟帐户名称	FXOS-general
系统运行时间	32115
UDI 产品标识符	FPR-C9300-AC

软件版本数据

Cisco Success Network 会收集与机箱相关的软件信息，包括类型和软件版本。下表说明所收集和监控的软件信息。

表 *5:* 软件版本遥测数据

数据点	示例值
类型	package_version
版本	2.7(1.52)

ASA 设备数据

Cisco Success Network 会收集上与 Firepower 4100/9300 的 安全模块/引擎 上运行的 ASA 设备相关的信息。下表说明所收集和监控的 ASA 设备相关信息。

表 *6: ASA* 设备遥测数据

数据点	示例值
ASA 设备 PID	FPR9K-SM-36
ASA 设备型号	思科自适应安全设备
ASA 设备序列号	XDQ311841WA
部署类型（本地或容器）	原生型
安全上下文模式（单或多）	单值

ASA 软件版本	{
	type: "asa_version",
	ersion: "9.13.1.5"
	}

设备管理器版本	{
	type: "device_mgr_version",
	version: "7.10.1"
	}

正在使用的已激活智能许可证	{
	"type": "Strong encryption",
	"tag":
	"regid.2016-05.com.cisco.ASA-GEN-STRONG-ENCRYPTION,
	5.7_982308k4-74w2-5f38-64na-707q99g10cce",
	"count": 1
	}

性能数据

Cisco Success Network 会收集 ASA 设备的性能特定信息。这些信息包括系统正常运行时间、CPU 使用率、内存使用率、磁盘空间使用情况和带宽使用信息。

- **CPU 使用率** - 过去五分钟的 CPU 使用信息
- **内存使用率** - 系统的可用、已用及总内存
- **磁盘使用情况** - 可用、已用及总磁盘空间信息
- **系统正常运行时间** - 系统正常运行时间信息
- **带宽使用** - 系统带宽使用情况；从所有 nameif 接口汇聚

  这会显示自系统启动时间以来已接收和传输的数据包（或字节）的统计信息。

下表说明所收集和监控的数据。

表 *7:* 性能遥测数据

数据点	示例值
过去五分钟的系统 CPU 使用率	{ “fiveSecondsPercentage”:0.2000000, “oneMinutePercentage”: 0, “fiveMinutesPercentage”: 0 }
系统内存使用率	{ “freeMemoryInBytes”:225854966384, “usedMemoryInBytes”: 17798281616, “totalMemoryInBytes”:243653248000 }
系统磁盘使用情况	{ "freeGB": 21.237285, "usedGB": 0.238805, "totalGB": 21.476090 }
系统运行时间	99700000
系统带宽使用情况	{ "receivedPktsPerSec": 3, "receivedBytesPerSec": 212, "transmittedPktsPerSec": 3, "transmittedBytesPerSec": 399 }

使用数据

Cisco Success Network 会收集机箱的 安全模块/引擎 上运行的 ASA 设备的功能状态、集群、故障切换和登录信息。下表说明所收集和监控的 ASA 设备使用数据。

表 *8:* 使用情况遥测数据

数据点	示例值
功能状态	[{ “name”: “cluster”, “status”: “enabled” }, { “name”: “webvpn”, “status”: “enabled” }, { “name”: “logging-buffered”, “status”: “debugging” }]

数据点	示例值

集群信息	<pre>{
	"clusterGroupName": "asa-cluster",
	"interfaceMode": "spanned",
	"unitName": "unit-3-3",
	"unitState": "SLAVE",
	"otherMembers": {
	"items": [
	{
	"memberName": "unit-2-1",
	"memberState": "MASTER",
	
	"memberSerialNum": "DAK391674E"
	}
	]
	}
	
	}</pre>

故障切换信息	<pre>{
	myRole: “Primary”,
	peerRole: “Secondary”,
	myState: “active”,
	peerState: “standby”,
	peerSerialNum:
	“DAK39162B”
	}</pre>

登录历史	<pre>{
	"loginTimes": "1 times in last 1 days",
	"lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
	}</pre>

遥测示例文件

Firepower 4100/9300 机箱 汇聚从已启用遥测的所有 ASA 设备接收的数据，并在将数据发送到思科云之前，与机箱特定信息和其他字段一起位于线上。如果没有具有遥测数据的应用程序，则仍将遥测与机箱信息一起发送到思科云。

以下是 Cisco Success Network 遥测文件的一个示例，其中包含发送到思科云的 Firepower 9300 上两台 ASA 设备的信息。


```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json",
    "msgID": "2227"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1560868270055,
    "FXOS": {
      "FXOSdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "HNY4475P01K",
        "smartLicenseProductInstanceIdentifier": "413509m0-f952-5822-7492-r62c0a5h4gf4",
```

```
    "smartLicenseVirtualAccountName": "FXOS-general",
    "systemUptime": 32115,
    "udiProductIdentifier": "FPR-C9300-AC"
  },
  "versions": {
    "items": [
      {
        "type": "package_version",
        "version": "2.7(1.52)"
      }
    ]
  }
},
"asaDevices": {
  "items": [
    {
      "CPUUsage": {
        "fiveMinutesPercentage": 0,
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0
      },
      "bandwidthUsage": {
        "receivedBytesPerSec": 1,
        "receivedPktsPerSec": 0,
        "transmittedBytesPerSec": 1,
        "transmittedPktsPerSec": 0
      },
      "deviceInfo": {
        "deploymentType": "Native",
        "deviceModel": "Cisco Adaptive Security Appliance",
        "securityContextMode": "Single",
        "serialNumber": "ADG2158508T",
        "systemUptime": 31084,
        "udiProductIdentifier": "FPR9K-SM-24"
      },
      "diskUsage": {
        "freeGB": 19.781810760498047,
        "totalGB": 20.0009765625,
        "usedGB": 0.21916580200195312
      },
      "featureStatus": {
        "items": [
          {
            "name": "aaa-proxy-limit",
            "status": "enabled"
          },
          {
            "name": "firewall_user_authentication",
            "status": "enabled"
          },
          {
            "name": "IKEv2 fragmentation",
            "status": "enabled"
          },
          {
            "name": "inspection-dns",
            "status": "enabled"
          },
          {
            "name": "inspection-esmtp",
            "status": "enabled"
          },
          {
            "name": "inspection-ftp",
```

```
    "status": "enabled"
  },
  {
    "name": "inspection-hs232",
    "status": "enabled"
  },
  {
    "name": "inspection-netbios",
    "status": "enabled"
  },
  {
    "name": "inspection-rsh",
    "status": "enabled"
  },
  {
    "name": "inspection-rtsp",
    "status": "enabled"
  },
  {
    "name": "inspection-sip",
    "status": "enabled"
  },
  {
    "name": "inspection-skinny",
    "status": "enabled"
  },
  {
    "name": "inspection-snmp",
    "status": "enabled"
  },
  {
    "name": "inspection-sqlnet",
    "status": "enabled"
  },
  {
    "name": "inspection-sunrpc",
    "status": "enabled"
  },
  {
    "name": "inspection-tftp",
    "status": "enabled"
  },
  {
    "name": "inspection-xdmcp",
    "status": "enabled"
  },
  {
    "name": "management-mode",
    "status": "normal"
  },
  {
    "name": "mobike",
    "status": "enabled"
  },
  {
    "name": "ntp",
    "status": "enabled"
  },
  {
    "name": "sctp-engine",
    "status": "enabled"
  },
  {
    "name": "smart-licensing",
```

```
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
  "licenseActivated": {
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:18 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226031548496,
    "totalMemoryInBytes": 241583656960,
    "usedMemoryInBytes": 15552108464
  },
  "versions": {
    "items": [
      {
        "type": "asa_version",
        "version": "9.13(1)248"
      },
      {
        "type": "device_mgr_version",
        "version": "7.13(1)31"
      }
    ]
  }
},
{
  "CPUUsage": {
    "fiveMinutesPercentage": 0,
    "fiveSecondsPercentage": 0,
    "oneMinutePercentage": 0
  },
  "bandwidthUsage": {
    "receivedBytesPerSec": 1,
    "receivedPktsPerSec": 0,
    "transmittedBytesPerSec": 1,
    "transmittedPktsPerSec": 0
  },
  "deviceInfo": {
    "deploymentType": "Native",
    "deviceModel": "Cisco Adaptive Security Appliance",
    "securityContextMode": "Single",
    "serialNumber": "RFL21764S1D",
    "systemUptime": 31083,
    "udiProductIdentifier": "FPR9K-SM-24"
  },
  "diskUsage": {
    "freeGB": 19.781543731689453,
    "totalGB": 20.0009765625,
```

```
  "usedGB": 0.21943283081054688
},
"featureStatus": {
  "items": [
    {
      "name": "aaa-proxy-limit",
      "status": "enabled"
    },
    {
      "name": "call-home",
      "status": "enabled"
    },
    {
      "name": "crypto-ca-trustpoint-id-usage-ssl-ipsec",
      "status": "enabled"
    },
    {
      "name": "firewall_user_authentication",
      "status": "enabled"
    },
    {
      "name": "IKEv2 fragmentation",
      "status": "enabled"
    },
    {
      "name": "inspection-dns",
      "status": "enabled"
    },
    {
      "name": "inspection-esmtp",
      "status": "enabled"
    },
    {
      "name": "inspection-ftp",
      "status": "enabled"
    },
    {
      "name": "inspection-hs232",
      "status": "enabled"
    },
    {
      "name": "inspection-netbios",
      "status": "enabled"
    },
    {
      "name": "inspection-rsh",
      "status": "enabled"
    },
    {
      "name": "inspection-rtsp",
      "status": "enabled"
    },
    {
      "name": "inspection-sip",
      "status": "enabled"
    },
    {
      "name": "inspection-skinny",
      "status": "enabled"
    },
    {
      "name": "inspection-snmp",
      "status": "enabled"
    },
```

```
      {
        "name": "inspection-sqlnet",
        "status": "enabled"
      },
      {
        "name": "inspection-sunrpc",
        "status": "enabled"
      },
      {
        "name": "inspection-tftp",
        "status": "enabled"
      },
      {
        "name": "inspection-xdmcp",
        "status": "enabled"
      },
      {
        "name": "management-mode",
        "status": "normal"
      },
      {
        "name": "mobike",
        "status": "enabled"
      },
      {
        "name": "ntp",
        "status": "enabled"
      },
      {
        "name": "sctp-engine",
        "status": "enabled"
      },
      {
        "name": "smart-licensing",
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
  "licenseActivated": {
    "items": []
  },
  "loginHistory": {
    "lastSuccessfulLogin": "05:53:16 UTC Jun 18 2019",
    "loginTimes": "1 times in last 1 days"
  },
  "memoryUsage": {
    "freeMemoryInBytes": 226028740080,
    "totalMemoryInBytes": 241581195264,
    "usedMemoryInBytes": 15552455184
  },
  "versions": {
    "items": [
```

```
            {
              "type": "asa_version",
              "version": "9.13(1)248"
            },
            {
              "type": "device_mgr_version",
              "version": "7.13(1)31"
            }
          ]
        }
      }
    ]
  }
 }
}
```


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，请单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 故障切换和群集指南

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“SLProfile”的 Smart Call Home 配置文件，该文件用于指定许可颁发机构的 URL。

```
scope monitoring
  scope callhome
    scope profile SLProfile
      scope destination SLDest
        set address https://tools.cisco.com/its/service/oddce/services/DDCEService
```

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 36 页。

步骤 2 （可选）删除 Call Home URL，第 37 页

步骤 3 向许可证颁发机构注册 Firepower 安全设备，第 38 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 启用 HTTP 代理：

scope monitoring scope callhome set http-proxy-server-enable on

示例：

```
scope monitoring
  scope callhome
```

```
set http-proxy-server-enable on
```

步骤 2 设置代理 URL：

set http-proxy-server-url *url*

其中 *url* 是代理服务器的 HTTP 或 HTTP 地址。

示例：

```
set http-proxy-server-url https://10.1.1.1
```

步骤 3 设置端口：

set http-proxy-server-port 端口

示例：

```
set http-proxy-server-port 443
```

步骤 4 提交缓冲区：

commit-buffer

（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 输入监控范围：

scope monitoring

步骤 2 输入 callhome 范围：

scope callhome

步骤 3 查找 SLProfile：

scope profile SLProfile

步骤 4 目的：

show destination

示例：

```
SLDest https https://tools.cisco.com/its/oddce/services/DDCEService
```

步骤 5 删除 URL：

delete destination SLDest

步骤 6 提交缓冲区：

commit-buffer

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 4100/9300 机箱 中输入注册令牌：

scope license

register idtoken *id-token*

（可选）启用 **force** 选项。如果由于设备与门户或卫星之间的通信失败导致设备注册失败，CTC 将等待 24 小时，然后再次尝试注册设备。使用 **force** 选项来强制注册：

register idtoken *id-token* **force**

示例：

```
scope license
  register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
V8N3R0dXM1Z0NjWkdpR214eFZhMldBOS9CVnNEYnVKM1
g3R3dvemRD%0AY29NQT0%3D%0A
```

步骤 3 要稍后取消注册设备，请输入：

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。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。

步骤 4 要续签 ID 证书和更新所有安全模块上的授权，请输入：

scope license

scope licdebug

renew

默认情况下，ID证书每6个月自动更新，许可证授权每30天更新。如果您访问互联网的时间有限，或者在智能软件管理器中进行了任何许可更改等操作，则可能要为这些项目手动续订注册。

更改 Cisco Success Network 注册

将 Firepower 4100/9300注册到思科智能软件管理器时，可启用思科成功网络。之后，可以使用以下程序查看或更改注册状态。

注释 思科成功网络在评估模式下无法工作。

过程

步骤 1 输入系统范围。

scope system

示例：

```
Firepower# scope system
Firepower /system #
```

步骤 2 输入服务范围。

scope services

示例：

```
Firepower /system # scope services
Firepower /system/services #
```

步骤 3 输入遥测范围。

scope telemetry

示例：

```
Firepower /system/services # scope telemetry
Firepower /system/services/telemetry #
```

步骤 4 启用或禁用 Cisco Success Network 功能。

{enable | disable}

示例：

```
Firepower /system/services/telemetry # enable
```

步骤 5 验证 Firepower 4100/9300 机箱 中的 Cisco Success Network 状态。

show detail

示例：

确认 **Admin State** 显示 Cisco Success Network 的正确状态。

```
Telemetry:
    Admin State: Enabled
    Oper State: Registering
    Error Message:
    Period: 86400
    Current Task: Registering the device for Telemetry
    (FSM-STAGE:sam:dme:CommTelemetryDataExchSeq:RegisterforTelemetry)
```

示例：

确认 **Oper State** 显示 **OK**，表示已发送遥测数据。

```
Telemetry:
    Admin State: Enabled
    Oper State: Ok
    Error Message:
    Period: 86400
    Current Task:
```

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 35 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 VMwareESXi 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 将卫星服务器设置为 Callhome 目的：

scope monitoring

scope callhome

scope profile SLProfile

scope destination SLDest

set address https://[卫星服务器的 *FQDN*]**/Transportgateway/services/DeviceRequestHandler**

步骤 2 向证书颁发机构注册Firepower 4100/9300 机箱（请参阅向许可证颁发机构注册 Firepower 安全设备，第 38 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 从 FXOS CLI 启用许可证预留：

scope license

enable reservation

步骤 2 将范围设置为许可证预留：

scope license

scope reservation

步骤 3 生成预留申请代码：

request universal

show license resvcode

步骤 4 转至思科智能软件管理器门户的“智能软件管理器库存”(Smart Software Manager Inventory) 屏幕，单击**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 5 单击**License Reservation**，并在框中键入生成的预留申请代码。

步骤 6 单击 **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 7 在 FXOS CLI 中，输入许可范围：

scope license

步骤 8 输入预留范围：

scope reservation

步骤 9 输入授权码：

install *code*

您的 Firepower 4100/9300 机箱现已完全获得 PLR 许可。

步骤 10 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 在 FXOS CLI 中，输入许可证范围：

scope license

步骤 2 输入预留范围：

scope reservation

步骤 3 返还永久许可证：

return

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

步骤 4 查看和复制返还预留代码：

show license resvcode

步骤 5 在智能软件管理器中查看和复制 FXOS 通用设备标识符 (UDI)，这样可以找到您的 FXOS 实例：

show license udi

步骤 6 访问“智能软件管理器库存”(Smart Software Manager Inventory) 屏幕，单击**Product Instances**选项卡：

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

步骤 7 使用通用设备标识符 (UDI) 搜索您的 Firepower 4100/9300 机箱。

步骤 8 选择 **Actions** > **Remove**，并在框中键入生成的返还预留代码。

步骤 9 单击 **Remove Product Instance**。

永久许可证被返还到可用池。

步骤 10 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 113 页。

监控智能软件许可

请参阅以下命令来查看许可证状态：

- **show license all**

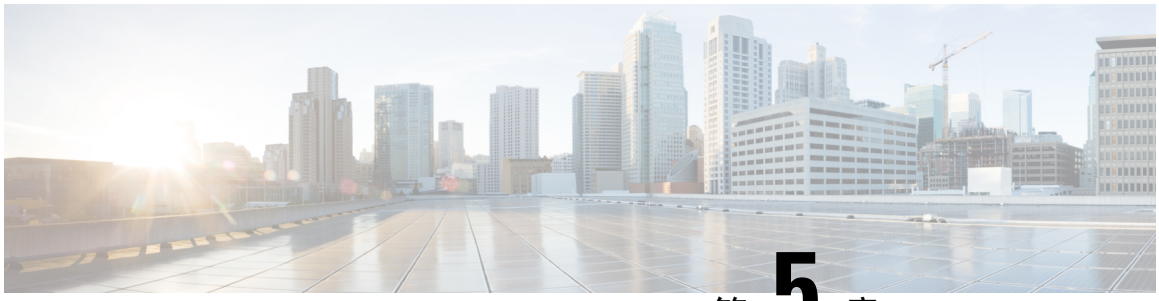
显示智能软件许可的状态、智能代理版本、UDI 信息、智能代理状态、全局合规状态、授权状态、许可证书信息和计划智能代理任务。

- **show license status**
- **show license techsupport**

智能软件许可历史记录

功能名称	平台版本	说明
思科成功网络	2.7.1	思科成功网络是一项用户启用的云服务。启用思科成功网络时，Firepower 4100/9300 机箱与思科云之间会建立安全连接以传输使用情况信息和统计信息。流传输遥测数据可以提供一种机制，用于从 ASA 选择感兴趣的数据，并使用结构化格式将其传输到远程管理站，以便执行以下任务： • 向您告知在网络中可用来改进产品效果的未使用功能。 • 向您告知可能适用于您的产品的其他技术支持服务和监控。 • 帮助思科改善我们的产品 当您注册 Cisco Success Network 后，机箱总是会建立并维护安全的连接。您可以通过禁用思科成功网络随时关闭此连接，这样会将设备与思科成功网络云断开。 引入了以下命令： **scope telemetry {enable | disable}** 引入了以下菜单项： **系统 > 许可 > Cisco Success Network**

功能名称	平台版本	说明
面向 Firepower 4100/9300 机箱的思科智能软件许可	1.1(1)	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。 我们引入了以下命令：**deregister**、**register idtoken**、**renew**、**scope callhome**、**scope destination**、**scope licdebug**、**scope license**、**scope monitoring**、**scope profile**、**set address**、**set http-proxy-server-enable on**、**set http-proxy-server-url**、**set http-proxy-server-port**、**show license all**、**show license status**、**show license techsupport**



第 5 章

用户管理

- 用户帐户， 第 47 页
- 面向用户名的指导原则， 第 48 页
- 密码的指导原则， 第 49 页
- 远程身份验证指导原则， 第 50 页
- 用户角色， 第 52 页
- 本地身份验证用户的密码配置文件， 第 52 页
- 选择默认身份验证服务， 第 53 页
- 配置会话超时， 第 55 页
- 配置绝对会话超时， 第 56 页
- 为远程用户配置角色策略， 第 57 页
- 为本地身份验证的用户启用密码强度检查， 第 57 页
- 设置最大尝试登录次数， 第 58 页
- 查看和清除用户锁定状态， 第 59 页
- 配置更改间隔的最大密码更改次数， 第 60 页
- 配置最小密码长度检查， 第 61 页
- 为密码配置无更改间隔， 第 61 页
- 配置密码历史记录计数， 第 62 页
- 创建本地用户账户， 第 63 页
- 删除本地用户账户， 第 65 页
- 激活或停用本地用户账户， 第 66 页
- 清除本地身份验证的用户的密码历史记录， 第 66 页

用户帐户

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

管理员账户

管理员帐户是默认用户帐户，并且无法修改或删除。此帐户是系统管理员或超级用户帐户并具有完整权限。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。

管理员帐户始终处于活动状态，并且不会到期。无法将管理员帐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帐户，此帐户将再次以现有配置变为活动状态。

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。默认情况下，所有远程用户最初都分配了**只读**角色。

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。

备用身份验证方法是使用本地数据库。该备用方法是不可配置的。

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 50 页
- 配置 LDAP 提供程序，第 156 页
- 配置 RADIUS 提供程序，第 161 页
- 配置 TACACS+ 提供程序，第 164 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。

在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐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。
- 创建用户帐户后，无法更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

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 eXtensible Operating System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 127 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 61 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。
- 不得包含空格。
- 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： • 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。
RADIUS	可选	您可以选择执行以下操作之一： • 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，cisco-avpair）创建自定义属性。	思科 RADIUS 实施的供应商 ID 为 009，属性的供应商 ID 为 001。 以下语法示例显示，如果选择创建 cisco-avpair 属性，如何指定多个用户角色和区域：`shell:roles="admin,aaa" shell:locales="L1,abc"`。使用逗号“,”作为分隔多个值的分隔符。
TACACS+	必要	必须扩展方案，并使用名称 cisco-av-pair 创建自定义属性。	cisco-av-pair 名称是为 TACACS+ 提供程序提供属性 ID 的字符串。 以下语法示例显示如何在创建 cisco-av-pair 属性时指定多个用户角色和区域：`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。在 cisco-av-pair 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。

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： • 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： • 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

选择默认身份验证服务

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 指定默认身份验证：

Firepower-chassis /security/default-auth # **set realm** *auth-type*

其中 *auth-type* 为以下关键字之一：

- **ldap**- 指定 LDAP 身份验证
- **local**- 指定本地身份验证
- **none**- 允许本地用户登录，无需指定密码
- **radius**- 指定 RADIUS 身份验证

- **tacacs**- 指定 TACACS+ 身份验证

注释　如果默认身份验证和控制台身份验证都设置为使用相同的远程身份验证协议（RADIUS、TACACS+ 或 LDAP），不更新这些用户设置就无法更改该服务器配置的某些方面（例如，删除该服务器或更改其分配顺序）。

步骤 4 （可选） 指定相关联的提供程序组，如果有：

Firepower-chassis /security/default-auth # **set auth-server-group** *auth-serv-group-name*

步骤 5 （可选） 为本域中的用户指定刷新请求的最大时间间隔：

Firepower-chassis /security/default-auth # **set refresh-period** *seconds*

指定一个介于 0 和 600 之间的整数。默认值为 600 秒。

如果超过此时间限制，则 FXOS 会认为 Web 会话处于非活动状态，但不终止此会话。

步骤 6 （可选） 指定自上次刷新请求后至 FXOS 认为 Web 会话已结束前的最长时间间隔：

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

指定一个介于 0 和 600 之间的整数。默认值为 600 秒。

注释　如果为 RADIUS 或 TACACS+ 领域设置双因素身份验证，请考虑延长 **session-refresh** 和 **session-timeout** 期限，避免远程用户太过频繁地重新进行身份验证。

步骤 7 （可选） 将领域的身份验证方式设置为双因素身份验证：

Firepower-chassis /security/default-auth # **set use-2-factor yes**

注释　双因素身份验证仅适用于 RADIUS 和 TACACS+ 领域。

步骤 8 将任务提交到系统配置：

commit-buffer

示例

以下示例将默认身份验证设置为 RADIUS，将默认身份验证提供程序组设置为 provider 1，启用双因素身份验证，将刷新期限设置为 300 秒（5 分钟），将会话超时期限设置为 540 秒（9 分钟），并且启用双因素身份验证。然后，提交任务。

```
Firepower-chassis# scope security
Firepower-chassis /security # scope default-auth
Firepower-chassis /security/default-auth # set realm radius
Firepower-chassis /security/default-auth* # set auth-server-group provider1
Firepower-chassis /security/default-auth* # set use-2-factor yes
Firepower-chassis /security/default-auth* # set refresh-period 300
Firepower-chassis /security/default-auth* # set session-timeout 540
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
```

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 将任务提交到系统配置：

Firepower-chassis /security/default-auth # **commit-buffer**

步骤 6 （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 将任务提交到系统配置：

Firepower-chassis /security/default-auth # **commit-buffer**

步骤 6 （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
```

为远程用户配置角色策略

默认情况下，向使用 LDAP、RADIUS 或 TACACS 协议从远程服务器登录 Firepower 机箱管理器或 FXOS CLI 的所有用户授予只读权限。出于安全原因，有必要限制匹配已建立的用户角色的那些用户的访问权限。

您可以通过以下方式为远程用户配置角色策略：

assign-default-role

当用户尝试登录并且远程身份验证提供程序不能为用户角色提供身份验证信息时，允许用户使用只读用户角色登录。

此为默认行为。

no-login

当用户尝试登录并且远程身份验证提供程序不为用户角色提供身份验证信息时，拒绝访问。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 指定是否应根据用户角色限制对 Firepower 机箱管理器 和 FXOS CLI 的用户访问：

Firepower-chassis /security # **set remote-user default-role** {**assign-default-role** | **no-login**}

步骤 3 将任务提交到系统配置：

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

示例

以下示例为远程用户设置角色策略，提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # set remote-user default-role no-login
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

为本地身份验证的用户启用密码强度检查

如果启用密码强度检查，则 Firepower eXtensible Operating System不允许用户选择不符合强密码准则的密码（请参阅密码的指导原则，第 49 页）。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 指定密码强度检查已启用还是已禁用：

Firepower-chassis /security # **set enforce-strong-password** {**yes** | **no**}

示例

以下示例启用密码强度检查：

```
Firepower-chassis# scope security
Firepower-chassis /security # set enforce-strong-password yes
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

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 59 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 81 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 58 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**

配置更改间隔的最大密码更改次数

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密码配置文件安全模式：

Firepower-chassis /security # **scope password-profile**

步骤 3 限制本地身份验证用户在给定小时数内更改密码的次数。

Firepower-chassis /security/password-profile # **set change-during-interval enable**

步骤 4 指定本地身份验证用户在更改间隔内可以更改其密码的最大次数：

Firepower-chassis /security/password-profile # **set change-count** *pass-change-num*

该值可以是介于 0 和 10 之间的任意值。

步骤 5 指定最大小时数，在该时间段内，密码更改次数为**更改计数 (Change Count)** 字段中所指定的值。

Firepower-chassis /security/password-profile # **set change-interval** *num-of-hours*

该值可以是 1 至 745（小时）的任意值。

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。

步骤 6 将任务提交到系统配置：

Firepower-chassis /security/password-profile # **commit-buffer**

示例

以下示例启用“间隔期间更改 (change during interval)”选项，将更改计数设置为 5，将更改间隔设置为 72 小时，并且提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval enable
Firepower-chassis /security/password-profile* # set change-count 5
Firepower-chassis /security/password-profile* # set change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

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 81 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

为密码配置无更改间隔

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密码配置文件安全模式：

Firepower-chassis /security # **scope password-profile**

步骤 3 禁用在间隔内更改功能：

Firepower-chassis /security/password-profile # **set change-during-interval disable**

步骤 4 指定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：

Firepower-chassis /security/password-profile # **set no-change-interval** *min-num-hours*

该值可以是 1 至 745（小时）的任意值。

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。

步骤 5 将任务提交到系统配置：

Firepower-chassis /security/password-profile # **commit-buffer**

示例

以下示例禁用“间隔期间更改 (change during interval)”选项，将无更改间隔设置为 72 小时，提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set change-during-interval disable
Firepower-chassis /security/password-profile* # set no-change-interval 72
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

配置密码历史记录计数

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密码配置文件安全模式：

Firepower-chassis /security # **scope password-profile**

步骤 3 指定本地身份验证用户必须创建的唯一密码数量，在此之前，用户可以重新使用以前用过的密码：

Firepower-chassis /security/password-profile # **set history-count** *num-of-passwords*

该值可以是从 0 至 15 的任意值。

默认情况下，**历史计数 (History Count)** 字段设置为 0，这表示禁用历史计数，使用户随时都能够重复使用之前已使用的密码。

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/password-profile # **commit-buffer**

示例

以下示例配置密码历史记录计数并且提交任务：

```
Firepower-chassis # scope security
Firepower-chassis /security # scope password-profile
Firepower-chassis /security/password-profile # set history-count 5
Firepower-chassis /security/password-profile* # commit-buffer
Firepower-chassis /security/password-profile #
```

创建本地用户账户

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 创建用户账户：

Firepower-chassis /security # **create local-user** *local-user-name*

其中，*local-user-name* 是登录此账户时要使用的账户名称。此名称必须唯一，并满足用户帐户名称的准则和限制（请参阅面向用户名的指导原则，第 48 页）。

创建用户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

步骤 3 指定本地用户账户已启用还是已禁用：

Firepower-chassis /security/local-user # **set account-status** {**active**| **inactive**}

步骤 4 设置用户账户的密码：

Firepower-chassis /security/local-user # **set password**

输入密码：*password*

确认密码：*password*

如果启用了密码强度检查，则用户的密码必须为强密码，Firepower eXtensible Operating System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 49 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。

步骤 5 （可选） 指定用户的名字：

Firepower-chassis /security/local-user # **set firstname** *first-name*

步骤 6 （可选） 指定用户的姓氏：

Firepower-chassis /security/local-user # **set lastname** *last-name*

步骤 7 （可选） 指定用户账户到期日期： *month* 参数是月份名称的前三个字母。

Firepower-chassis /security/local-user # **set expiration** *month* *day-of-month* *year*

注释 在为用户帐户配置过期日期后，无法将帐户重新配置为不过期。然而，您可以为帐户配置可用的最新过期日期。

步骤 8 （可选） 指定用户邮件地址。

Firepower-chassis /security/local-user # **set email** *email-addr*

步骤 9 （可选） 指定用户电话号码。

Firepower-chassis /security/local-user # **set phone** *phone-num*

步骤 10 （可选） 指定用于无密码访问的 SSH 密钥。

Firepower-chassis /security/local-user # **set sshkey** *ssh-key*

步骤 11 所有用户均默认分配了 *read-only* 角色，并且此角色无法删除。对于要指定给用户的每个额外角色：

Firepower-chassis /security/local-user # **create role** *role-name*

其中，*role-name* 是代表要分配给用户账户的权限的角色（请参阅用户角色，第 52 页）。

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。

步骤 12 从用户删除分配的角色：

Firepower-chassis /security/local-user # **delete role** *role-name*

所有用户均默认分配了 *read-only* 角色，并且此角色无法删除。

注释 删除用户角色时，系统会撤销该用户的当前会话 ID，这意味着用户的所有活动会话（包括 CLI 和 Web）都将立即终止。

步骤 13 提交任务。

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

示例

以下示例创建名为 kikipopo 的用户账户，启用用户账户，将密码设置为 foo12345，分配管理员用户角色，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user kikipopo
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* # set password
Enter a password:
Confirm the password:
Firepower-chassis /security/local-user* # create role admin
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

以下示例创建名为 lincey 的用户账户，启用用户账户，设置 OpenSSH 密钥以进行无密码访问，分配 aaa 和运营用户角色，并且提交任务。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user lincey
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
m8HPh2LOgyH7Ei1MI8="
```

```
Firepower-chassis /security/local-user* # create role aaa
Firepower-chassis /security/local-user* # create role operations
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

以下示例创建名为 jforlenz 的用户账户，启用用户账户，设置 Secure SSH 密钥以进行无密码访问，并且提交任务。

```
Firepower-chassis# scope security
Firepower-chassis /security # create local-user jforlenz
Firepower-chassis /security/local-user* # set account-status active
Firepower-chassis /security/local-user* #  set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```

删除本地用户账户

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 删除本地用户账户：

Firepower-chassis /security # **delete local-user** *local-user-name*

步骤 3 将任务提交到系统配置：

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

示例

以下示例删除 foo 用户账户，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # delete local-user foo
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

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 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 针对您要激活或停用的用户，进入本地用户安全模式：

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

步骤 3 指定本地用户账户是活动还是非活动状态：

Firepower-chassis /security/local-user # **set account-status** {**active** | **inactive**}

注释 管理员用户账户始终设置为活动。不能修改。

步骤 4 将任务提交到系统配置：

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

示例

以下示例启用一个名为 accounting 的本地用户帐户：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope local-user accounting
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

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**

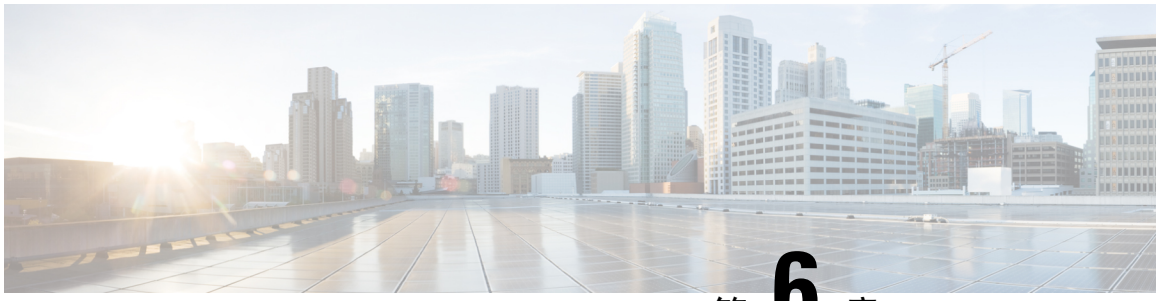
步骤 4 将任务提交到系统配置：

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 6 章

映像管理

- 关于映像管理， 第 69 页
- 从 Cisco.com 下载映像， 第 70 页
- 将Firepower eXtensible Operating System软件映像下载到 Firepower 4100/9300 机箱， 第 70 页
- 验证映像的完整性， 第 72 页
- 升级 Firepower eXtensible Operating System平台捆绑包， 第 73 页
- 将逻辑设备软件映像下载到 Firepower 4100/9300 机箱， 第 74 页
- 更新逻辑设备的映像版本， 第 76 页
- 固件升级， 第 78 页
- 手动降级到版本 2.0.1 或更低版本， 第 78 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 eXtensible Operating System 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，直至在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Firepower eXtensible Operating System软件映像下载到 Firepower 4100/9300 机箱

您可以使用 FTP、HTTP/HTTPS、SCP、SFTP 或 TFTP 将FXOS软件映像复制到 Firepower 4100/9300 机箱。

开始之前

收集将需要导入配置文件的以下信息：

- 您从其拷贝映像的服务器的 IP 地址和身份验证凭证
- FXOS映像文件的完全限定名称

注释 从 FXOS 2.8.1 开始，支持 HTTP/HTTPS 以下载固件和应用映像。

过程

步骤 1 进入固件模式：

Firepower-chassis # **scope firmware**

步骤 2 下载 FXOS 软件映像：

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*/*image_name*
- **http**://*username@hostname*/*path*/*image_name*
- **https**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname*:*port-num*/*path*/*image_name*
- **usbA**://*hostname*:*port-num*/*path*/*image_name*

步骤 3 要监控下载过程，请执行以下操作：

Firepower-chassis /firmware # **show package** *image_name* **detail**

示例

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
    File Name: fxos-k9.1.1.1.119.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 5120
    State: Downloading
    Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

以下示例使用 HTTP/HTTPS 协议复制映像：

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
https://user@192.168.1.1/images/fxos-k9.1.1.1.119.SPA
Firepower-chassis /firmware # show download task

Download task:
File Name    Protocol   Server  Port  Userid State
--------- -------- -------------- ---------- -------------- -----
fxos-k9.1.1.1.119.SPA
     Https  192.168.1.1  0   Downloaded
fxos-k9.1.1.1.119.SPA
     Http  sjc-ssp-artifac      0   Downloaded

-------------------------------------------------------------------------------------------
```

```
Firepower-chassis /firmware # show package fxos-k9.1.1.1.119.SPA detail
Download task:
    File Name: fxos-k9.1.1.1.119.SPA
    Protocol: https
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 5120
    State: Downloading
    Current Task: downloading image fxos-k9.1.1.1.119.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

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 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 18 页）。

步骤 2 进入固件模式：

Firepower-chassis# **scope firmware**

步骤 3 列出映像：

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

步骤 4 验证映像：

Firepower-chassis /firmware # **verify platform-pack version** *version_number*

version_number 是您正在验证的 FXOS 平台捆绑包的版本号，例如 1.1(2.51)。

步骤 5 系统将警告您验证可能需要几分钟。

输入**yes**，确认您想要继续验证。

步骤 6 要检查映像验证状态：

Firepower-chassis /firmware # **show validate-task**

升级 Firepower eXtensible Operating System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 70 页），然后将此映像下载到 Firepower 4100/9300 机箱（请参阅将逻辑设备软件映像下载到 Firepower 4100/9300 机箱，第 74 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群集的 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群集的 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，该群集中的其他设备仍然会通过流量。

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 18 页）。

步骤 2 进入固件模式：

Firepower-chassis# **scope firmware**

步骤 3 进入自动安装模式：

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

步骤 4 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 1.1(2.51)。

步骤 5 系统将首先验证想要安装的软件包。它会告知您当前已安装的应用与指定的 FXOS 平台软件包之间的所有不兼容。此外，它还会警告您，在升级过程中，任何现有会话都将终止，系统将需要重启。

输入 **yes**，确认您想要继续验证。

步骤 6 输入 **yes**确认您想要继续安装，或者输入 **no**取消安装。

Firepower eXtensible Operating System打开捆绑包，升级/重新加载组件。

步骤 7 要监控升级流程，请执行以下操作：

a) 输入 **scope firmware**。
b) 输入 **scope auto-install**。

c) 输入 **show fsm status expand**。

将逻辑设备软件映像下载到 Firepower 4100/9300 机箱

您可以使用 FTP、HTTP/HTTPS、SCP、SFTP 或 TFTP 将逻辑设备软件映像复制到 Firepower 4100/9300 机箱。

开始之前

收集将需要导入配置文件的以下信息：

- 您从其拷贝映像的服务器的 IP 地址和身份验证凭证
- 软件映像文件的完全限定名称

注释 FXOS 2.8.1 及更高版本支持用于固件和应用映像下载的 HTTP/HTTPS 协议。

过程

步骤 1 进入安全服务模式：

Firepower-chassis # **scope ssa**

步骤 2 进入应用软件模式：

Firepower-chassis /ssa # **scope app-software**

步骤 3 下载逻辑设备软件映像：

Firepower-chassis /ssa/app-software # **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*
- **http**://*username@hostname/path*
- **https**://*username@hostname/path*
- **scp**://*username@hostname/path*
- **sftp**://*username@hostname/path*
- **tftp**://*hostname*:*port-num*/*path*

步骤 4 要监控下载过程，请执行以下操作：

Firepower-chassis /ssa/app-software # **show download-task**

步骤 5 要查看已下载的应用，请执行以下操作：

Firepower-chassis /ssa/app-software # **up**

Firepower-chassis /ssa # **show app**

步骤 6 要查看特定应用的详细信息，请执行以下操作：

Firepower-chassis /ssa # **scope app** *application_type image_version*

Firepower-chassis /ssa/app # **show expand**

示例

以下示例使用 SCP 协议复制映像：

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
    File Name                     Protocol   Server               Userid          State
    ----------------------------- ---------- -------------------- --------------- -----
    cisco-asa.9.4.1.65.csp        Scp        192.168.1.1          user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App
    ---------- ---------- ----------- ---------- ----------- ----------- --------------
    asa        9.4.1.41   N/A                    Native      Application No
    asa        9.4.1.65   N/A                    Native      Application Yes

Firepower-chassis /ssa # scope app asa 9.4.1.65
Firepower-chassis /ssa/app # show expand

Application:
    Name: asa
    Version: 9.4.1.65
    Description: N/A
    Author:
    Deploy Type: Native
    CSP Type: Application
    Is Default App: Yes

    App Attribute Key for the Application:
        App Attribute Key Description
        ----------------- -----------
        cluster-role      This is the role of the blade in the cluster
        mgmt-ip           This is the IP for the management interface
        mgmt-url          This is the management URL for this application

    Net Mgmt Bootstrap Key for the Application:
```

```
        Bootstrap Key Key Data Type Is the Key Secret Description
        ------------- ------------- ----------------- -----------
        PASSWORD      String        Yes               The admin user password.

    Port Requirement for the Application:
        Port Type: Data
        Max Ports: 120
        Min Ports: 1

        Port Type: Mgmt
        Max Ports: 1
        Min Ports: 1

        Mgmt Port Sub Type for the Application:
            Management Sub Type
            -------------------
            Default

        Port Type: Cluster
        Max Ports: 1
        Min Ports: 0
Firepower-chassis /ssa/app #
```

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。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系统发行说明》：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**逻辑设备 (Logical Devices)** > **编辑 (Edit)** 和**系统 (System)** > **更新 (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 机箱间群集 -

1. 更改数据设备上的启动版本。

2. 将数据设备设置为控制设备。
3. 更改原始控制设备（现在的数据设备）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 70 页），然后将该映射下载到 Firepower 4100/9300 机箱（请参阅将逻辑设备软件映像下载到 Firepower 4100/9300 机箱，第 74 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 进入安全服务模式：

Firepower-chassis # **scope ssa**

步骤 2 将范围设置为您正在更新的安全模块：

Firepower-chassis /ssa # **scope slot** *slot_number*

步骤 3 将范围设置为您正在更新的应用：

Firepower-chassis /ssa/slot # **scope app-instance** *app_template*

步骤 4 设置启动版本：

Firepower-chassis /ssa/slot/app-instance # **set startup-version** *version_number*

如果您正在设置 Firepower 威胁防御逻辑设备上的应用启动版本，系统将显示以下警告消息：

13254: 警告: ftd 不支持 FXOS 升级。指定版本只有在需要重新安装 ftd 时才会使用。

示例：

```
firepower /ssa/slot/app-instance # set startup-version 6.2.2.81
13254:  Warning: FXOS upgrades are not supported for ftd. The specified version will be
used only if ftd needs to be reinstalled.
```

步骤 5 提交配置：

commit-buffer

提交系统配置任务。应用映像已更新，应用重新启动。

示例

以下示例更新正在安全模块 1 上运行的 ASA 软件映像。请注意，您可以使用 **show** 命令查看更新状态。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
```

```
Firepower-chassis /ssa/slot # scope app-instance asa
Firepower-chassis /ssa/slot/app-instance # set startup-version 9.4.1.65
Firepower-chassis /ssa/slot/app-instance* # show configuration pending
 enter app-instance asa
+    set startup-version 9.4.1.65
 exit
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance # show

Application Instance:
    Application Name Admin State Operational State Running Version Startup Version
    ---------------- ----------- ----------------- --------------- ---------------
    asa              Enabled     Updating          9.4.1.41        9.4.1.65
Firepower-chassis /ssa/slot/app-instance #
Firepower-chassis /ssa/slot/app-instance # show

Application Instance:
    Application Name Admin State Operational State Running Version Startup Version
    ---------------- ----------- ----------------- --------------- ---------------
    asa              Enabled     Online            9.4.1.65        9.4.1.65
Firepower-chassis /ssa/slot/app-instance #
```

固件升级

有关在您的 Firepower 4100/9300 机箱 上升级固件的信息，请参阅《思科 *Firepower 4100/9300 FXOS* 固件升级指南》。

手动降级到版本 2.0.1 或更低版本

按照以下 CLI 步骤，在安全模块上手动降级 CIMC 映像。

注释 此过程专门用于从版本 2.1.1 或更高版本降级到版本 2.0.1 或更低版本。

开始之前

确保要降级的应用程序映像已下载到 Firepower 4100/9300 机箱 （请参阅从 Cisco.com 下载映像， 第 70 页和将逻辑设备软件映像下载到 Firepower 4100/9300 机箱， 第 74 页）。

过程

步骤 1 在降级 CIMC 映像之前，请禁用映像版本比较。

按照本示例中的步骤清除默认平台映像版本：

示例：

```
firepower# scope org
firepower /org # scope fw-platform-pack default
```

```
firepower /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
firepower /org/fw-platform-pack* # commit-buffer
firepower /org/fw-platform-pack #
```

步骤 2 降级模块映像。

按照本示例中的步骤更改 CIMC 映像：

示例：

```
firepower# scope server 1/1
firepower /chassis/server # scope cimc
firepower /chassis/server/cimc # update firmware <version_num>
firepower /chassis/server/cimc* # activate firmware <version_num>
firepower /chassis/server/cimc* # commit-buffer
firepower /chassis/server/cimc #
```

根据需要重复此步骤，以更新其他模块。

步骤 3 安装新的固件捆绑包。

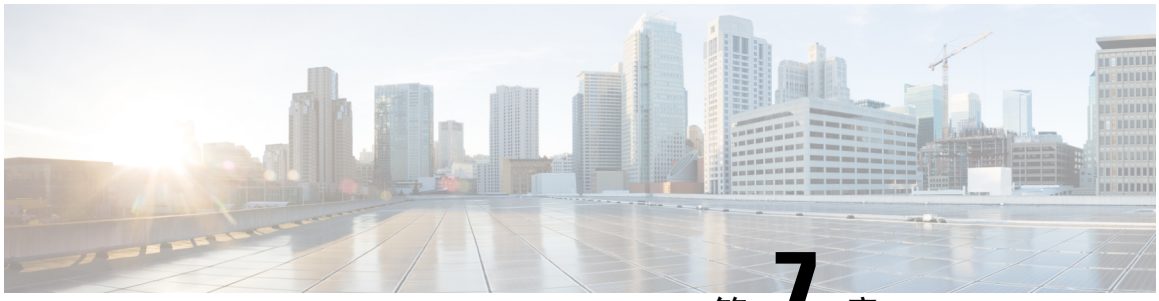
按照本示例中的步骤安装降级映像：

示例：

```
firepower# scope firmware
firepower /firmware # scope auto-install
firepower /firmware/auto-install # install platform platform-vers <version_num>
The currently installed FXOS platform software package is <version_num>

WARNING: If you proceed with the upgrade, the system will reboot.

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup
Do you want to proceed? (yes/no):
```

下一步做什么

您可以在固件/自动安装模式下使用 **show fsm status expand** 命令来监控安装过程。



第 7 章

安全认证合规性

- 安全认证合规性， 第 81 页
- 生成 SSH 主机密钥， 第 82 页
- 配置 IPSec 安全通道， 第 83 页
- 配置信任点静态 CRL， 第 89 页
- 关于证书撤销吊销列表检查， 第 89 页
- 配置 CRL 定期下载， 第 93 页
- 设置 LDAP 密钥环证书， 第 95 页
- 启用客户端证书身份验证， 第 96 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 171 页
- 启用通用标准模式， 第 172 页
- 配置 IPSec 安全通道， 第 83 页
- 配置信任点静态 CRL， 第 89 页
- 关于证书撤销吊销列表检查， 第 89 页
- 配置 CRL 定期下载， 第 93 页
- 配置 NTP 身份验证： 使用 NTP 设置日期和时间， 第 120 页
- 设置 LDAP 密钥环证书， 第 95 页
- 配置 IP 访问列表， 第 173 页
- 启用客户端证书身份验证， 第 96 页
- 配置最小密码长度检查， 第 61 页

- 设置最大尝试登录次数， 第 58 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 171 页或启用通用标准模式， 第 172 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

IPSec 是由互联网工程任务组 (IETF) 开发的一个开放标准框架。它可以在 IP 网络上创建安全、经过身份验证和可靠的通信。IPsec 安全服务提供：

- 无连接完整性 - 确保接收的流量未被修改。
- 数据源身份验证 - 确保流量是由合法方发送的。
- 保密性（加密）- 确保用户的流量不被非授权方检查。
- 访问控制 - 防止未经授权使用资源。

注释 IPSec 连接只能从 FXOS 启动。FXOS 不接受传入的 IPSec 连接请求。

IPsec 隧道是 FXOS 在对等体之间建立的 SA 集合。SA 指定适用于敏感数据的协议和算法并指定对等体使用的密钥内容。IPSec SA 控制用户流量的实际传输。SA 是单向的，但是通常成对建立（入站和出站）。

Firepower 机箱管理器上的 IPSec 有两种模式：

传输模式
IP 报头，IPSec 报头，TCP 报头，数据

隧道模式
新 IP 报头，IPSec 报头，原始 IP 报头，TCP 报头，数据

IPSec 的操作可分为五个主要步骤：

1. 流量选择 - 匹配 IPSec 策略的需要关注的流量会启动 IKE 进程。例如，可以使用 src/dst 主机 IP 或子网选择流量。或者，用户也可以通过 admin 命令来触发 IKE 进程。
2. IKE 第 1 阶段 - 对 IPSec 对等体进行身份验证，并设置安全通道以启用 IKE 交换
3. IKE 第 2 阶段 - 协商 SA 以设置 IPSec 隧道。SA 代表安全关联，它是 IPSec 终端之间的关系，描述了用于保护数据流量的安全服务。
4. 数据传输 - 使用 SA 中存储的参数和密钥将数据包加密并封装在 IPSec 报头中
5. IPSec 隧道终止 - IPSec SA 通过删除或超时终止。

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 81 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 ip *ip-address*

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
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMAsG
A1UECwwEU1RCVTELMAkGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWC3NzcEBzc3Au
bmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
```

Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690Vl8/mNPWdjCjDI+U/L9keYs/rbZdRSeXy9kMae42+4FlRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QIiGYSctlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoGNGwNTO85fK3kjgMOdWbdeMG3EihxEEOUPD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVl/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNSAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZlO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybDAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEAvI8ky2jiXc4wPiMuxIfY
W7DRmszPUWQ7edor7yxuCqzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhzYxVZ10DHKIzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpBQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJCggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+UkfP89hvJt/fluJ+s/VJSVZWK4tAWvR7wl
QngCKRJW6FYpzeyNBctiJ07wO+Wt4e3KhIjJDYvA9hFixWcVGDf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/0do512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2IaatyI
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBjN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAcMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJ1
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGludGVybTEtY2EubmV0MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZsegjhLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXl3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiancDVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguIEDL812ROejQvpmfqGUq11stkIIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLlI
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFpLCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXlolb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfhoIdPA28xlnfIB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKgJCjaujz55TGGd1
GjnxDMX9twwz7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLlZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AzvnzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAAaNBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSgIqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWOc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWyd79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NWpwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXaIcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIW3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvpuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCei6aROlGdP/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjxKlJlp1c3WbfCue/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-----
MIICwTCCAakCAQAwVTELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAkNBMQwwCgYDVQQH
DANTSkMxDjAMBgNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDq292Rq3t0laoxPbfE
p/lTKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjClK/tsIxsPkV0
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPlX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vwzRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZECP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAlBgkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUIcEwKgA
rjANBgkqhkiG9w0BAQsFAAOCAQEARtRBoInxXkBYNlVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZl03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMl9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
RJh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWNo6
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 重新加载连接：

reload-conns

系统会停止所有连接，然后重新加载它们。系统将尝试重新建立所有连接。

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 81 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 certrevokemethod {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”。

FXOS 从 X.509 证书的 CDP 信息中获取动态（非静态）CRL 信息，该信息指示动态 CRL 信息。系统管理人员会手动下载指示 FXOS 系统中的本地 CRL 信息的静态 CRL 信息。FXOS 根据证书链中当前正在处理的证书处理动态 CRL 信息。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、创建 LDAP 提供程序和配置 HTTPS。

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 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。当 FXOS 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，FXOS 会忽略对等证书中的 CDP。
- 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 *9:* 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
对等证书链中缺少一个 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

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
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 *10:* 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
对等证书链中缺少一个 CDP（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

具有本地静态 CRL	LDAP 连接	IPSec 连接
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 *11:* 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
对等证书链中缺少一个 CDP	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 *12:* 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
对等证书链中缺少一个CDP（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 89 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 81 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：

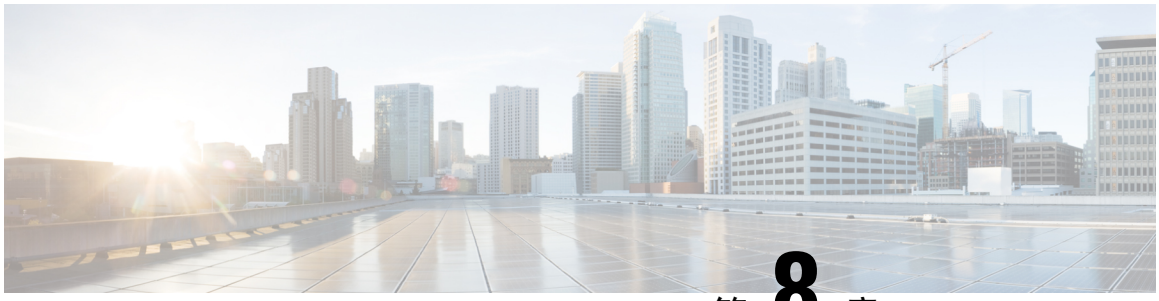
```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

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 8 章

系统管理

- 更改管理 IP 地址， 第 99 页
- 更改应用管理 IP， 第 101 页
- 更改 Firepower 4100/9300 机箱名称， 第 104 页
- 安装受信任身份证书， 第 104 页
- 登录前横幅， 第 110 页
- 重新启动 Firepower 4100/9300 机箱， 第 113 页
- 关闭 Firepower 4100/9300 机箱电源， 第 114 页
- 恢复出厂默认配置， 第 114 页
- 安全地擦除系统组件， 第 115 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 18 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*

注释 仅支持 IPv6 全局单播地址作为机箱的 IPv6 管理地址。

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 更改应用程序管理 IP 会导致服务中断。

过程

步骤 1 连接到 FXOS CLI。（请参阅访问 FXOS CLI，第 18 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 逻辑设备的群集配置：

a) 输入群集管理引导程序：
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 威胁防御的独立和群集配置：

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 对于群集配置，您必须为连接到 Firepower 4100/9300 机箱的每个应用设置新的 IP 地址。如果您有机箱间群集或 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 对于群集配置，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。如果您有机箱间群集或 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_ftd*

d) 启用应用：

enable

e) 提交配置：

commit-buffer

注释 对于群集配置，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。如果您有机箱间群集或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 18 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 #
```

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 18 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-----
MIIC6zCCAdMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEx
ETAPBgNVBAcMCFNhbiBKb3NlMRYwFAYDVQQKDA1DaXNjbyBTeXN0ZW1zMQwwCgYD
```

```
VQQLDANUQUMxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmxvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQA1mQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSLoShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTB1ZHaKV9bttYg3kf/UEUUgk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIIzOavU6d1tB9rnyxgGth5dPV0dhQIDAQABoC8wLQYJ
KoZIhvcNAQkOMSAwHjAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVDcL+tATu5xFE3LA310ck6GjlNv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ1OIkyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLfG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxB0gyaRdnea5RhiGjYQ2lDXYDjEXp7rCx9
+6bvDl1n70JCegHdCWtP75SaNyaBEPkO0365rTckbw==
-----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-----
>MIICDTCCAbOgAwIBAgIQYIutxPDPw6BOp3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAASvEA27V1Enq1gMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkm1xmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgkrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPrFwEEBcbxGSgQW7pOVIkwEAYJKwYB
>BAGCNxUBBAMCAQAwCgYIKoZIzj0EAwIDSAAwRQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsv1gCxsQVOw0xZVRugSdoOak6n7wCjTFX9jr
>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-----
>MIIE8DCCBJagAwIBAgITRQAAAArehlUWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3Rp
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
>aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
>bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
>MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
>BwdudS3sulXIwKGco48mMHCRQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
>yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
>AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
>dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
>Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
>AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
>IFew7NcJirEtFRvyxjkQ4/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/IsZAEZFghuYWF1c3Rp
bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTYwNDI4MTMw
OTU0WhcNMTgwNDI4MTMwOTU0WjB3MQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2Fs
aWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDDAKBgNVBAsTA1RBQzEaMBgGA1UEAxMRZnA0MTIwLnRlc3QubG9jYWwwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+LglUQA0b7tga
BwdudS3sulXIwKGco48mMHCRQwlADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
```

```
ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67YOyig9WrvqZObwHBg
yodskS/g+a5GNYTzzIS9XAfslMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
/cujcb0hNssvmAhhlVq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAa2Hl09XR2FAgMB
AAGjggJYMIICVDAcBgNVHREEFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
FgQU/1WpstiEYExs8DlZWcuHZwPtu5QwHwYDVR0jBBgwFoAUyInbDHPrFwEEBcbx
GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRp
b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGlz
dD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MIHMBggrBgEF
BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
QVVTVElOLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxD
Tj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
P2NBQ2VydGlmaWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
aG9yaXR5MCEGCSsGAQQBgjcUAgQUHhIAVwBlAGIAUwBlAHIAdgBlAHIwDgYDVR0P
AQH/BAQDAgWgMBMGA1UdJQQMMAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0gAMEUC
IFew7NcJirEtFRvyxjkQ4/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。

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单击**确定 (OK)**，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 18 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 18 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 18 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 进入机箱模式：

scope chassis 1

步骤 2 输入以下命令重新启动机箱：

reboot [原因] [**no-prompt**]

注释 如果您使用 [**no-prompt**] 关键字，则输入命令后机箱将立即重新启动。如果您不使用 [**no-prompt**] 关键字，则在您输入 **commit-buffer** 命令前系统不会重新启动。

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。

步骤 3 监控重新启动过程：

scope chassis 1

show fsm status

关闭 Firepower 4100/9300 机箱电源

过程

步骤 1 进入机箱模式：

scope chassis 1

步骤 2 输入以下命令关闭机箱：

shutdown [原因] [**no-prompt**]

注释 如果您使用 [**no-prompt**] 关键字，则输入命令后机箱将立即关闭。如果您不使用 [**no-prompt**] 关键字，则在您输入 **commit-buffer** 命令前系统不会重新启动。

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。此过程大约需要 15-20 分钟。在机箱成功关闭后，您可以拔掉机箱的电源插头。

步骤 3 监控关闭过程：

scope chassis 1

show fsm status

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，您需要重新配置系统（请参阅初始配置，第 11 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 连接到本地管理外壳：

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。

安全地擦除系统组件

您可以使用 FXOS CLI 清除并安全地擦除 Firepower 设备的组件。

如恢复出厂默认配置，第 114 页中所述，**erase configuration** 命令可删除机箱上的所有用户配置信息，将其恢复为原始出厂默认配置。

erase secure 命令会安全地擦除指定的设备组件。也就是说，并非仅删除数据，物理存储也会被“擦除”（完全清除）。这在运输或退回设备时非常重要，因为硬件存储组件不会保留残留数据或存根。

注释 设备会在安全清除期间重新引导，这意味着 SSH 连接会终止。因此，我们建议通过串行控制台端口连接执行安全擦除。

过程

步骤 1 连接到本地管理外壳：

connect local-mgmt

步骤 2 输入以下 **erase configuration** 命令之一，以安全地擦除指定的设备组件：

a) **erase configuration chassis**

系统会警告您，所有数据和映像都将丢失且无法恢复，并要求您确认是否要继续。如果您输入 **y**，整个 Firepower 机箱会被安全地擦除；首先清除安全模块，然后再清除管理引擎。

由于设备上的所有数据和软件都会被清除，因此只能从 ROM 监控器 (ROMMON) 恢复设备。

b) **erase configuration security_module** *module-ID*

系统会警告您，模块上的所有数据和映像都将丢失且无法恢复，并要求您确认是否要继续。如果输入 **y**，模块将被清除。

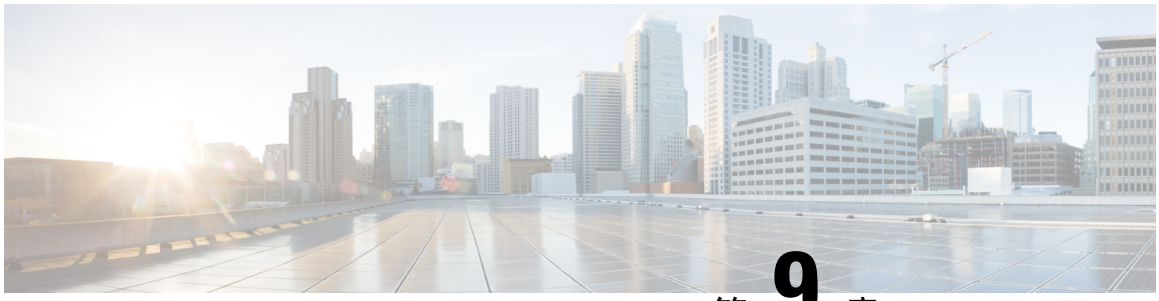
注释 **decommission-secure** 命令产生的结果与此命令基本相同。

清除安全模块后，它将保持关闭状态，直到被确认（类似于已停用的模块）。

c) **erase configuration supervisor**

系统会警告您，所有数据和映像都将丢失且无法恢复，并要求您确认是否要继续。如果您输入 **y**，Firepower 管理引擎会被安全地清除。

由于管理引擎上的所有数据和软件都会被清除，因此只能从ROM 监控器 (ROMMON) 恢复设备。



第 9 章

平台设置

- 设置日期和时间， 第 117 页
- 配置 SSH， 第 124 页
- 配置 TLS， 第 128 页
- 配置 Telnet， 第 130 页
- 配置 SNMP， 第 130 页
- 配置 HTTPS， 第 141 页
- 配置 AAA， 第 154 页
- 验证远程 AAA 服务器配置， 第 166 页
- 配置系统日志， 第 168 页
- 配置 DNS 服务器， 第 170 页
- 启用 FIPS 模式， 第 171 页
- 启用通用标准模式， 第 172 页
- 配置 IP 访问列表， 第 173 页
- 为容器实例接口添加 MAC 池前缀，并查看其 MAC 地址， 第 174 页
- 为容器实例添加资源配置文件， 第 176 页
- 配置网络控制策略， 第 179 页
- 配置机箱 URL， 第 181 页

设置日期和时间

使用 下文介绍的 CLI 命令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。您应对 Firepower 4100/9300 机箱和 Firepower 管理中心 使用相同的 NTP 服务器，但请注意，您不能使用 Firepower 管理中心作为的 Firepower 4100/9300 机箱 的 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 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 18 页）。

步骤 2 要查看已配置的时区，请执行以下操作：

Firepower-chassis# **show timezone**

步骤 3 查看配置的日期和时间：

Firepower-chassis# **show clock**

示例

以下示例显示如何显示配置的时区和当前系统日期及时间：

```
Firepower-chassis# show timezone
Timezone: America/Chicago
Firepower-chassis# show clock
Thu Jun  2 12:40:42 CDT 2016
Firepower-chassis#
```

设置时区

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 设置时区：

Firepower-chassis /system/services # **set timezone**

此时，系统将提示您输入与您所在的洲、国家/地区和时区区域对应的编号。在每个系统提示符处输入适当的信息。

当您完成指定位置信息时，系统将提示您确认已设置了正确的时区信息。输入 **1**（是）进行确认，或者输入 **2**（否）取消操作。

步骤 4 要查看已配置的时区，请执行以下操作：

Firepower-chassis /system/services # **top**

Firepower-chassis# **show timezone**

示例

以下示例将时区配置为太平洋时区，提交任务，并且显示已配置的时区：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 2
Please select a country.
 1) Anguilla                 28) Haiti
 2) Antigua & Barbuda        29) Honduras
 3) Argentina                30) Jamaica
 4) Aruba                    31) Martinique
 5) Bahamas                  32) Mexico
 6) Barbados                 33) Montserrat
 7) Belize                   34) Nicaragua
 8) Bolivia                  35) Panama
 9) Brazil                   36) Paraguay
10) Canada                   37) Peru
11) Caribbean Netherlands    38) Puerto Rico
12) Cayman Islands           39) St Barthelemy
13) Chile                    40) St Kitts & Nevis
14) Colombia                 41) St Lucia
15) Costa Rica               42) St Maarten (Dutch part)
16) Cuba                     43) St Martin (French part)
17) Curacao                  44) St Pierre & Miquelon
18) Dominica                 45) St Vincent
19) Dominican Republic       46) Suriname
20) Ecuador                  47) Trinidad & Tobago
21) El Salvador              48) Turks & Caicos Is
22) French Guiana            49) United States
23) Greenland                50) Uruguay
24) Grenada                  51) Venezuela
25) Guadeloupe               52) Virgin Islands (UK)
26) Guatemala                53) Virgin Islands (US)
27) Guyana
#? 49
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
 6) Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
 7) Eastern Time - Indiana - Pulaski County
```

```
 8) Eastern Time - Indiana - Crawford County
 9) Eastern Time - Indiana - Pike County
10) Eastern Time - Indiana - Switzerland County
11) Central Time
12) Central Time - Indiana - Perry County
13) Central Time - Indiana - Starke County
14) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties
15) Central Time - North Dakota - Oliver County
16) Central Time - North Dakota - Morton County (except Mandan area)
17) Central Time - North Dakota - Mercer County
18) Mountain Time
19) Mountain Time - south Idaho & east Oregon
20) Mountain Standard Time - Arizona (except Navajo)
21) Pacific Time
22) Pacific Standard Time - Annette Island, Alaska
23) Alaska Time
24) Alaska Time - Alaska panhandle
25) Alaska Time - southeast Alaska panhandle
26) Alaska Time - Alaska panhandle neck
27) Alaska Time - west Alaska
28) Aleutian Islands
29) Hawaii
#? 21

The following information has been given:

        United States
        Pacific Time

Therefore timezone 'America/Los_Angeles' will be set.
Local time is now:      Wed Jun 24 07:39:25 PDT 2015.
Universal Time is now:  Wed Jun 24 14:39:25 UTC 2015.
Is the above information OK?
1) Yes
2) No
#? 1
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services # top
Firepower-chassis# show timezone
Timezone: America/Los_Angeles (Pacific Time)
Firepower-chassis#
```

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 使用 NTP 版本 3。
- 如果外部 NTP 服务器的层值为13 或更大，则应用程序实例无法同步到 FXOS 机箱上的 NTP 服务器。每次 NTP 客户端同步到 NTP 服务器时，层值就会增加 1。

  如果您已设置自己的 NTP 服务器，则可以在服务器上的 /etc/ntp.conf 文件中找到它的层值。如果 NTP 服务器的层值大于或等于 13，则可以更改 ntp.conf 文件中的层值并重新启动服务器，或者使用其他 NTP 服务器（例如：pool.ntp.org）。

开始之前

如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器。请参阅 配置 DNS 服务器，第 170 页。

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 使用指定的主机名、IPv4 或 IPv6 地址配置系统，使其使用 NTP 服务器：

Firepower-chassis /system/services # **create ntp-server** *{hostname | ip-addr | ip6-addr}*

步骤 4 （可选） 配置 NTP 身份验证。

仅支持使用 SHA1 进行 NTP 服务器身份验证。从 NTP 服务器获取密钥 ID 和值。例如，要在安装了 OpenSSL 的 NTP 服务器 4.2.8p8 版或更高版本上生成 SHA1 密钥，请输入 **ntp-keygen -M** 命令，然后在 ntp.keys 文件中查看密钥 ID 和值。密钥用于告知客户端和服务器在计算消息摘要时要使用哪个值。

a) 设置 SHA1 密钥 ID。

set ntp-sha1-key-id *key_id*

b) 设置 SHA1 密钥字符串。

set ntp-sha1-key-string

系统会提示您输入密钥字符串。

c) 退出 ntp-server 模式。

exit

d) 启用 NTP 认证。

enable ntp-authentication

示例：

```
firepower /system/services/ntp-server* # set ntp-sha1-key-string 11
firepower /system/services/ntp-server* # set ntp-sha1-key-string
NTP SHA-1 key string: 7092334a7809ab9873124c08123df9097097fe72
firepower /system/services/ntp-server* # exit
firepower /system/services* # enable authentication
```

步骤 5 将任务提交到系统配置：

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

步骤 6 查看所有已配置的 NTP 服务器的同步状态：

Firepower-chassis /system/services # **show ntp-server**

步骤 7 查看特定 NTP 服务器的同步状态：

Firepower-chassis /system/services # **scope ntp-server** *{hostname | ip-addr | ip6-addr}*

Firepower-chassis /system/services/ntp-server # **show detail**

示例

以下示例使用 IP 地址 192.168.200.101 配置 NTP 服务器并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

以下示例使用 IPv6 地址 4001::6 配置 NTP 服务器并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

删除 NTP 服务器

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 删除带有指定主机名、IPv4 或 IPv6 地址的 NTP 服务器：

Firepower-chassis /system/services # **delete ntp-server** *{hostname | ip-addr | ip6-addr}*

步骤 4 将任务提交到系统配置：

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

示例

以下示例删除带有 IP 地址 192.168.200.101 的 NTP 服务器，并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 192.168.200.101
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

以下示例删除带有 IPv6 地址 4001::6 的 NTP 服务器，并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete ntp-server 4001::6
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

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。系统时钟修改会在机箱上立即生效。请注意，手动设置 Firepower 机箱日期和时间后，更改可能需要一些时间才能反映在已安装的逻辑设备中。

注释 如果系统时钟当前正在与 NTP 服务器同步，您将无法手动设置日期和时间。

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 配置系统时钟：

Firepower-chassis /system/services # **set clock** *month day year hour min sec*

对于月份，请使用当月的头三个数字。小时必须使用 24 小时格式输入，其中 7 pm 可以输入为 19。

系统时钟修改立即生效。无需确认缓冲区。

示例

以下示例配置了系统时钟：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set clock jun 24 2015 15 27 00
Firepower-chassis /system/services #
```

配置 SSH

以下程序介绍如何启用或禁用使用 SSH 访问 Firepower 机箱、如何将 FXOS 机箱作为 SSH 客户端启用，以及如何配置 SSH 用于 SSH 服务器和 SSH 客户端加密、密钥交换和消息身份验证的各种算法。

默认情况下，SSH 处于启用状态。

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 SSH 访问，请执行以下操作之一：

- 要允许对 Firepower 机箱进行 SSH 访问，请输入以下命令：

  Firepower-chassis /system/services # **enable ssh-server**

- 要禁止对 Firepower 机箱进行 SSH 访问，请输入以下命令：

  Firepower-chassis /system/services # **disable ssh-server**

步骤 4 配置服务器的加密算法：

Firepower-chassis /system/services # **set ssh-server encrypt-algorithm** *encrypt_algorithm*

示例：

```
Firepower /system/services # set ssh-server encrypt-algorithm ?
  3des-cbc    3des Cbc
  aes128-cbc  Aes128 Cbc
  aes128-ctr  Aes128 Ctr
  aes192-cbc  Aes192 Cbc
  aes192-ctr  Aes192 Ctr
  aes256-cbc  Aes256 Cbc
  aes256-ctr  Aes256 Ctr
```

示例：

注释
- 在通用标准模式下不支持以下加密算法：
  - 3des-cbc
  - chacha20-poly1305@openssh.com
- chacha20-poly1305@openssh.com 在 FIPS 中不受支持。如果在 FXOS 机箱上启用了 FIPS 模式，则不能使用 chacha20-poly1305@openssh.com 作为加密算法。
- 以下加密算法默认不会启用：

```
aes128-cbc
aes192-cbc
aes265-cbc
```

步骤 5 配置服务器 Diffie-hellman (DH) 密钥交换算法：

Firepower-chassis /system/services # **set ssh-server kex-algorithm**

示例：

```
Firepower /system/services # set ssh-server kex-algorithm
  diffie-hellman-group1-sha1   Diffie Hellman Group1 Sha1
  diffie-hellman-group14-sha1  Diffie Hellman Group14 Sha1
```

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。

注释
- 在通用标准模式下不支持以下密钥交换算法：
  - diffie-hellman-group14-sha256
  - curve25519-sha256
  - curve25519-sha256@libssh.org
- 在 FIPS 模式下不支持以下密钥交换算法：
  - curve25519-sha256
  - curve25519-sha256@libssh.org

步骤 6 设置服务器 mac 算法：

Firepower-chassis /system/services # **set ssh-server mac-algorithm**

示例：

```
Firepower /system/services # set ssh-server mac-algorithm
  hmac-sha1      Hmac Sha1
  hmac-sha1-160  Hmac Sha1 160
  hmac-sha1-96   Hmac Sha1 96
  hmac-sha2-256  Hmac Sha2 256
  hmac-sha2-512  Hmac Sha2 512
```

步骤 7 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。

Firepower-chassis /system/services # **set ssh-server host-key rsa** *modulus_value*

示例：

```
Firepower /system/services # set ssh-server host-key rsa ?
<1024-2048>  Enter number of bits (in multiples of 8)
Firepower /system/services # set ssh-server host-key rsa 2048
```

步骤 8 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）。

Firepower-chassis /system/services # **set ssh-server rekey-limit volume** *KB_of_Traffic*

示例：

```
Firepower /system/services # set /system/services # set ssh-server rekey-limit volume ?
  100-4194303  Max volume limit in KB
```

步骤 9 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）。

Firepower-chassis /system/services # **set ssh-server rekey-limit time** *minutes*

示例：

```
Firepower /system/services # set /system/services # set ssh-server rekey-limit time ?
   10-1440  Max time limit in Minutes
```

步骤 10 将任务提交到系统配置：

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

步骤 11 配置严格的主机密钥检查，以控制 SSH 主机密钥检查：

Firepower /system/services # **ssh-client stricthostkeycheck** *enable/disable/prompt*

示例：

```
Firepower /system/services # set ssh-client stricthostkeycheck enable
```

- **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 配置客户端的加密算法：

Firepower-chassis /system/services # **set ssh-client encrypt-algorithm** *encrypt_algorithm*

示例：

```
Firepower /system/services # set ssh-client encrypt-algorithm ?
  3des-cbc    3des Cbc
  aes128-cbc  Aes128 Cbc
  aes128-ctr  Aes128 Ctr
  aes192-cbc  Aes192 Cbc
```

```
aes192-ctr  Aes192 Ctr
aes256-cbc  Aes256 Cbc
aes256-ctr  Aes256 Ctr
```

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。
- 以下加密算法默认不会启用：

```
aes128-cbc
aes192-cbc
aes265-cbc
```

步骤 13 配置客户端 Diffie-hellman (DH) 密钥交换算法：

Firepower-chassis /system/services # **set ssh-client kex-algorithm**

示例：

```
Firepower /system/services # set ssh-client kex-algorithm
  diffie-hellman-group1-sha1   Diffie Hellman Group1 Sha1
  diffie-hellman-group14-sha1  Diffie Hellman Group14 Sha1
```

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 设置客户端 mac 算法：

Firepower-chassis /system/services # **set ssh-client mac-algorithm**

示例：

```
Firepower /system/services # set ssh-client mac-algorithm
  hmac-sha1      Hmac Sha1
  hmac-sha1-160  Hmac Sha1 160
  hmac-sha1-96   Hmac Sha1 96
  hmac-sha2-256  Hmac Sha2 256
  hmac-sha2-512  Hmac Sha2 512
```

步骤 15 对于客户端主机密钥，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。

Firepower-chassis /system/services # **set ssh-client host-key rsa** *modulus_value*

示例：

```
Firepower /system/services # set ssh-client host-key rsa ?
<1024-2048>  Enter number of bits (in multiples of 8)
Firepower /system/services # set ssh-client host-key rsa 2048
```

步骤 16 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）。

Firepower-chassis /system/services # **set ssh-client rekey-limit volume** *KB_of_Traffic*

示例：

```
Firepower /system/services # set /system/services # set ssh-client rekey-limit volume ?
  100-4194303  Max volume limit in KB
```

步骤 17 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）。

Firepower-chassis /system/services # **set ssh-client rekey-limit time** *minutes*

示例：

```
Firepower /system/services # set /system/services # set ssh-client rekey-limit time ?
   10-1440  Max time limit in Minutes
```

步骤 18 将任务提交到系统配置：

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

示例

以下示例启用对 Firepower 机箱的 SSH 访问，并且提交任务：

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

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,Ae
s192 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:+MEDIU
M:+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

本节介绍如何在 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 来控制和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)

注释 请注意，SNMP 版本 1 和 2c 具有严重的已知安全问题：它们以不加密的方式传输所有信息，包括社区字符串，该字符串充当这些版本中唯一的身份验证形式。

SNMP 通知

SNMP 的一个关键功能是能够生成来自 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 通知生成为陷阱或通知。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。

但是，通知仅可配合 SNMPv2c 使用，这被认为不安全，因此不建议使用。

注释 重新引导 FXOS 后，使用 SNMP 的接口上的 ifindex 顺序不会变化。但是，当您重新引导 FXOS 时，FXOS 磁盘使用 OID 上的索引号会发生变化。

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 *13: 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。 **注释** 虽然可以配置，但 FXOS 不支持将 `noAuthNoPriv` 与 SNMP 第 3 版配合使用。
V3	authNoPriv	HMAC-SHA	否	提供基于 HMAC 安全散列算法 (SHA) 的身份验证。

型号	级别	身份验证	加密	状况
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 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

Firepower-chassis /monitoring # **enable snmp**

步骤 3 （可选）进入 SNMP 社区模式：

Firepower-chassis /monitoring # **set snmp community**

输入 **set snmp community** 命令后，系统将提示您输入 SNMP 社区名称。

当您指定 SNMP 社区名称时，也会自动为来自 SNMP 远程管理器的轮询请求启用 SNMP 版本 1 和 2c。

注释 请注意，SNMP 版本 1 和 2c 具有严重的已知安全问题：它们以不加密的方式传输所有信息，包括社区字符串，该字符串充当这些版本中唯一的身份验证形式。

步骤 4 指定 SNMP 社区名称；此社区名称用作 SNMP 密码。社区名可以是任意字母数字字符串，最多 32 个字符。

Firepower-chassis /monitoring # **Enter a snmp community:** *community-name*

只能有一个社区名称；但是，您可以使用 **set snmp community** 覆盖现有名称。要删除现有社区名称（同时为来自 SNMP 远程管理器的轮询请求禁用 SNMP 版本 1 和 2c），请输入 **set snmp community**，但不键入社区字符串；也就是说，只需再次按 **Enter**。在您提交缓冲区后， **show snmp** 输出将包括以下行：是否设置社区：否。

步骤 5 指定负责 SNMP 的系统联系人。系统联系人姓名可以是任意字母数字字符串，最多 255 个字符，例如电邮地址或姓名和电话号码。

Firepower-chassis /monitoring # **set snmp syscontact** *system-contact-name*

步骤 6 指定 SNMP 代理（服务器）运行所在的主机的位置。系统位置名称可以是任意字母数字字符串，最多 512 个字符。

Firepower-chassis /monitoring # **set snmp syslocation** *system-location-name*

步骤 7 将任务提交到系统配置：

Firepower-chassis /monitoring # **commit-buffer**

示例

以下示例启用 SNMP，配置名为 SnmpCommSystem2 的 SNMP 社区，配置名为 contactperson 的系统联系人，配置名为 systemlocation 的联系人位置，并且提交任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # set snmp community
Enter a snmp community: SnmpCommSystem2
Firepower-chassis /monitoring* # set snmp syscontact contactperson1
Firepower-chassis /monitoring* # set snmp syslocation systemlocation
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

下一步做什么

创建 SNMP 陷阱和用户。

创建 SNMP 陷阱

以下步骤介绍如何创建 SNMP 陷阱。

注释 最多可以定义八个 SNMP 陷阱。

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

Firepower-chassis /monitoring # **enable snmp**

步骤 3 使用指定的主机名、IPv4 地址或 IPv6 地址创建 SNMP 陷阱。

Firepower-chassis /monitoring # **create snmp-trap** {*hostname* | *ip-addr* | *ip6-addr*}

步骤 4 指定用于 SNMP 陷阱的 SNMP 社区名或版本 3 用户名：

Firepower-chassis /monitoring/snmp-trap # **set community** *community-name*

指定 SNMPv1/v2c 社区字符串或 SNMPv3 用户名，以允许访问陷阱目标。输入此命令后，系统会向您查询社区名称。名称最多可包含 32 个字符，不含空格；键入时不显示名称。

步骤 5 指定用于 SNMP 陷阱的端口：

Firepower-chassis /monitoring/snmp-trap # **set port** *port-num*

步骤 6 指定用于陷阱的 SNMP 版本和型号：

Firepower-chassis /monitoring/snmp-trap # **set version** {**v1** | **v2c** | **v3**}

注释　请注意，SNMP 版本 1 和 2c 具有严重的已知安全问题：它们以不加密的方式传输所有信息，包括社区字符串，该字符串充当这些版本中唯一的身份验证形式。

步骤 7 （可选） 指定要发送的陷阱类型。

Firepower-chassis /monitoring/snmp-trap # **set notificationtype** {**traps** | **informs**}

该字段可以是：

- **陷阱 (traps)**，如果为版本选择 v2c 或 v3。
- **通告 (informs)**，如果为版本选择 v2c。

  注释　仅在您为版本选择 v2c 时，才可以发送通告通知。

步骤 8 （可选） 如果为版本选择 v3，请指定与陷阱相关的权限：

Firepower-chassis /monitoring/snmp-trap # **set v3privilege** {**auth** | **noauth** | **priv**}

该字段可以是：

- **auth** - 身份验证但不加密。
- **noauth** - 没有身份验证或加密。请注意，虽然可以指定，但 FXOS 不支持与 SNMPv3 配合使用此安全级别。
- **priv** - 身份验证和加密。

步骤 9 确认系统配置任务：

Firepower-chassis /monitoring/snmp-trap # **commit-buffer**

示例

以下示例启用 SNMP，使用 IPv4 地址创建 SNMP 陷阱，指定陷阱将在端口 3 上使用 SnmpCommSystem2 社区，将版本设置为 v3，将通知类型设置为陷阱，将 v3 权限设置为“权限 (priv)”，并且确认任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 192.168.100.112
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem2
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

以下示例启用 SNMP，使用 IPv6 地址创建 SNMP 陷阱，指定陷阱将在端口 2 上使用 SnmpCommSystem3 社区，将版本设置为 v3，将通知类型设置为陷阱，将 v3 权限设置为“权限 (priv)”，并且确认任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-trap 2001::1
Firepower-chassis /monitoring/snmp-trap* # set community SnmpCommSystem3
Firepower-chassis /monitoring/snmp-trap* # set port 2
Firepower-chassis /monitoring/snmp-trap* # set version v3
Firepower-chassis /monitoring/snmp-trap* # set notificationtype traps
Firepower-chassis /monitoring/snmp-trap* # set v3privilege priv
Firepower-chassis /monitoring/snmp-trap* # commit-buffer
Firepower-chassis /monitoring/snmp-trap #
```

删除 SNMP 陷阱

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 删除带有指定主机名或 IP 地址的 SNMP 陷阱：

Firepower-chassis /monitoring # **delete snmp-trap** {*hostname* | *ip-addr*}

步骤 3 将任务提交到系统配置：

Firepower-chassis /monitoring # **commit-buffer**

示例

以下示例删除位于 IP 地址 192.168.100.112 的 SNMP 陷阱，并且提交任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-trap 192.168.100.112
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

创建 SNMPv3 用户

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

Firepower-chassis /monitoring # **enable snmp**

步骤 3 创建 SNMPv3 用户：

Firepower-chassis /monitoring # **create snmp-user** *user-name*

输入 **create snmp-user** 命令后，系统将提示您输入密码。

Firepower eXtensible Operating System 拒绝任何不满足以下要求的密码：

- 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。

步骤 4 指定 SHA 身份验证的使用情况：

Firepower-chassis /monitoring/snmp-user # **set auth** [**sha** | **sha224** | **sha256** | **sha358**}

步骤 5 启用或禁用 AES-128 加密的使用：

Firepower-chassis /monitoring/snmp-user # **set aes-128** {**no** | **yes**}

默认情况下会禁用 AES-128 加密。

SNMPv3 不支持 DES。如果您让 AES-128 保持禁用，则不会进行隐私加密，任何配置的隐私密码都不会生效。

步骤 6 指定用户密码：

Firepower-chassis /monitoring/snmp-user # **set password**

输入 **set password** 命令后，系统将提示您输入并确认密码。

步骤 7 将任务提交到系统配置：

Firepower-chassis /monitoring/snmp-user # **commit-buffer**

示例

以下示例启用 SNMP，创建名为 snmp-user14 的 SNMPv3 用户，启用 AES-128 加密，设置密码和隐私密码，并且提交任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # enable snmp
Firepower-chassis /monitoring* # create snmp-user snmp-user14
Password:
Firepower-chassis /monitoring/snmp-user* # set aes-128 yes
Firepower-chassis /monitoring/snmp-user* # set priv-password
Enter a password:
Confirm the password:
Firepower-chassis /monitoring/snmp-user* # commit-buffer
Firepower-chassis /monitoring/snmp-user #
```

删除 SNMPv3 用户

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 删除指定的 SNMPv3 用户：

Firepower-chassis /monitoring # **delete snmp-user** *user-name*

步骤 3 将任务提交到系统配置：

Firepower-chassis /monitoring # **commit-buffer**

示例

以下示例删除名为 snmp-user14 的 SNMPv3 用户，并且提交任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # delete snmp-user snmp-user14
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

查看当前的 SNMP 设置

使用以下 CLI 命令显示当前的 SNMP 设置、用户和陷阱。

注释 重新启动 FXOS 后，使用 SNMP 的 FXOS 接口上的 ifIndex 顺序不会变化。

过程

步骤 1 进入监控模式：

firepower# **scope monitoring**

步骤 2 显示当前 SNMP 设置：

firepower/monitoring # **show snmp**

```
Name: snmp
    Admin State: Enabled
    Port: 161
    Is Community Set: Yes
    Sys Contact: R_Admin
    Sys Location:
```

步骤 3 列出当前定义的 SNMPv3 用户：

firepower/monitoring # **show snmp-user**

```
SNMPv3 User:
    Name                     Authentication type
    ------------------------ -------------------
    snmp-user1               Sha
    testuser                 Sha
    snmp-user2               Sha
```

步骤 4 列出当前定义的 SNMP 陷阱：

firepower/monitoring # **show snmp-trap**

```
SNMP Trap:
    SNMP Trap                Port     Community  Version V3 Privilege Notification Type
    ------------------------ -------- ---------- ------- ------------ -----------------
    trap1_informs            162      ****       V2c     Noauth       Informs
    192.168.10.100           162      ****       V3      Noauth       Traps
```

示例

此示例演示如何显示特定 SNMPv3 用户的相关详细信息：

```
firepower /monitoring # show snmp-user snmp-user1 detail

SNMPv3 User:
    Name: snmp-user1
    Authentication type: Sha
    Password: ****
    Privacy password: ****
    Use AES-128: Yes
firepower /monitoring #
```

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，秘钥长度越长，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。

如果群集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

如果群集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-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
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

注释 对于 2.7 之前的版本，我们建议不要使用不带 FQDN 的“set dns”或“ set subject-name”来提交缓冲区。如果您尝试使用非 FQDN 的 DNS 或使用者名称来创建认证要求，则会导致错误。

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-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
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

以下示例创建受信任点并提供为受信任点提供证书：

```
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
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 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。

注释 如果更改已在 HTTPS 上配置的密钥环中的证书，您必须重新启动 HTTPS 才能使新证书生效。有关详细信息，请参阅：重新启动 HTTPS，第 151 页。

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任点：

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/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> 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#sslciphersuite。

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 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 指定用于 HTTPS 连接的端口：

Firepower-chassis /system/services # **set https port** *port-number*

为 *port-number* 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 HTTPS。

步骤 4 将任务提交到系统配置：

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

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。

示例

以下示例将 HTTPS 端口号设置为 443 并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # set https port 444
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

重新启动 HTTPS

如果更改已在 HTTPS 上配置的密钥环中的证书，您必须重新启动 HTTPS 才能使新证书生效。使用以下程序重置具有更新密钥环的 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 将 HTTPS 密钥环恢复为其默认值：

Firepower-chassis /system/services # **set https keyring default**

步骤 4 将任务提交到系统配置：

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

步骤 5 等待五秒钟。

步骤 6 使用您创建的密钥环来设置 HTTPS：

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

步骤 7 将任务提交到系统配置：

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

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

以下示例删除受信任点：

```
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

验证、授权和记帐 (AAA) 是一组服务，用于控制对网络资源的访问、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。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。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每个用户的方法，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 服务器会将用户提供的凭证与数据库中存储的用户凭证进行比较。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：确定允许每个用户访问哪些类型的活动、资源或服务。进行身份验证后，可能会授权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帐功能配合使用。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。

支持的身份验证类型

FXOS 支持以下类型的用户身份验证：

- **远程** - 支持以下网络 AAA 服务：
  - LDAP
  - RADIUS
  - TACACS+
- **本地** – Firepower 机箱维护一个可用用户配置文件填充的本地数据库。您可以使用此本地数据库代替 AAA 服务器来提供用户身份验证、授权和记帐。

用户角色

FXOS 支持以用户角色分配的形式进行本地和远程授权。可以分配的角色包括：

- **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。
- **AAA 管理员** - 对用户、角色和 AAA 配置进行读写访问。对系统其余部分的读取访问。
- **操作** - 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。
- **只读** - 对系统配置进行只读访问，但无权修改系统状态。

有关本地用户和角色分配的详细信息，请参阅用户管理，第 47 页。

设置 AAA

这些步骤提供了在 Firepower 4100/9300 设备上设置身份验证、授权和记帐 (AAA) 的基本大纲。

1. 配置所需的用户身份验证类型：
   - **本地** - 用户定义和本地身份验证是用户管理，第 47 页的一部分。
   - **远程** - 配置远程 AAA 服务器访问是平台设置的一部分，特别是：

- 配置 LDAP 提供程序，第 156 页
- 配置 RADIUS 提供程序，第 161 页
- 配置 TACACS+ 提供程序，第 164 页

注释 如果您将使用远程AAA服务器，请务必在远程服务器上启用和配置 AAA 服务，然后在 Firepower 机箱上配置远程 AAA 服务器访问。

2. 指定默认身份验证方法 - 这也是用户管理，第 47 页的一部分。

注释 如果默认身份验证和控制台身份验证都设置为使用相同的远程身份验证协议（RADIUS、TACACS+ 或 LDAP），不更新这些用户设置就无法更改该服务器配置的某些方面（例如，删除该服务器或更改其分配顺序）。

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 eXtensible Operating System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 eXtensible Operating System。此账户应具有永不过期的密码。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：

Firepower-chassis /security # **scope ldap**

步骤 3 仅限对包含指定属性的记录进行数据库搜索：

Firepower-chassis /security/ldap # **set attribute** *attribute*

步骤 4 仅限对包含指定区别名的记录进行数据库搜索：

Firepower-chassis /security/ldap # **set basedn** *distinguished-name*

步骤 5 仅限对包含指定过滤器的记录进行数据库搜索：

Firepower-chassis /security/ldap # **set filter** *filter*

其中 *filter* 是要与 LDAP 服务器一起使用的过滤器属性，例如 *cn=$userid* 或 *sAMAccountName=$userid*。过滤器必须包含 *$userid*。

步骤 6 设置系统在注明 LDAP 服务器停机之前，将等待服务器发出响应的时间量：

Firepower-chassis /security/ldap # **set timeout** *seconds*

步骤 7 将任务提交到系统配置：

Firepower-chassis /security/ldap # **commit-buffer**

示例

以下示例将 LDAP 属性设置为 CiscoAvPair，将基础区别名设置为“DC=cisco-firepower-aaa3,DC=qalab,DC=com”，将过滤器设置为 sAMAccountName=$userid，将超时间隔设置为 5 秒，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # set attribute CiscoAvPair
Firepower-chassis /security/ldap* # set basedn "DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap* # set filter sAMAccountName=$userid
Firepower-chassis /security/ldap* # set timeout 5
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```

注释 如果 LDAP 用户的 DN 超过 255 个字符，用户登录将失败。

下一步做什么

创建 LDAP 提供程序。

创建 LDAP 提供程序

按照以下步骤定义和配置 LDAP 提供程序，即为此 Firepower 设备提供基于 LDAP 的 AAA 服务的特定远程服务器。

注释 Firepower eXtensible Operating System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 eXtensible Operating System。此账户应具有永不过期的密码。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：

Firepower-chassis /security # **scope ldap**

步骤 3 创建 LDAP 服务器实例，进入安全 LDAP 服务器模式：

Firepower-chassis /security/ldap # **create server** *server-name*

如果 SSL 已启用， *server-name*（通常为 IP 地址或 FQDN）必须精确匹配 LDAP 服务器安全证书中的通用名称 (CN)。除非指定了 IP 地址，否则必须配置 DNS 服务器。

步骤 4 （可选） 设置 LDAP 属性，用来存储用户角色和区域设置值：

Firepower-chassis /security/ldap/server # **set attribute** *attr-name*

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，除非已为 LDAP 提供程序设置了默认属性。

步骤 5 （可选） 在 LDAP 层级结构中设置特定的区别名，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：

Firepower-chassis /security/ldap/server # **set basedn** *basedn-name*

基础 DN 的长度最大可以是 255 个字符减去 CN=username 长度，其中，用户名标识尝试使用 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，除非已为 LDAP 提供程序设置了默认基础 DN。

步骤 6 （可选） 为 LDAP 数据库账户设置区别名 (DN)，该账户对基础 DN 下的所有对象拥有读取和搜索权限：

Firepower-chassis /security/ldap/server # **set binddn** *binddn-name*

支持的最大字符串长度为 255 个 ASCII 字符。

步骤 7 （可选） 将 LDAP 搜索限制为匹配已定义过滤器的用户名。

Firepower-chassis /security/ldap/server # **set filter** *filter-value*

其中 *filter-value* 是要与 LDAP 服务器一起使用的过滤器属性，例如 *cn=$userid* 或 *sAMAccountName=$userid*。过滤器必须包含 *$userid*。

该值为必填项，除非已为 LDAP 提供程序设置了默认过滤器。

步骤 8 为已为绑定 DN 指定的 LDAP 数据库账户指定密码：

Firepower-chassis /security/ldap/server # **set password**

要设置密码，请在键入 **set password** 命令后，按 **Enter** 键，并在提示符处输入密钥值。

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。

步骤 9 （可选） 指定 Firepower eXtensible Operating System使用此提供程序对用户进行身份验证的顺序：

Firepower-chassis /security/ldap/server # **set order** *order-num*

步骤 10 （可选） 指定用于与 LDAP 服务器通信的端口。标准端口号为 389。

Firepower-chassis /security/ldap/server # **set port** *port-num*

步骤 11 与 LDAP 服务器通信时，启用或禁用加密使用：

Firepower-chassis /security/ldap/server # **set ssl** {**yes** | **no**}

选项如下：

- **yes** - 必须加密。如果加密无法协商，连接将失败。
- **no** - 禁用加密。身份验证信息以明文发送。

LDAP 使用 STARTTLS。这允许使用端口 389 进行加密通信。

步骤 12 指定在系统超时之前，系统尝试连接 LDAP 数据库时将花费的时间长度（以秒为单位）：

Firepower-chassis /security/ldap/server # **set timeout** *timeout-num*

输入一个介于 1 和 60 秒之间的整数，或者输入 0（零），以使用为 LDAP 提供程序指定的全局超时值。默认值为 30 秒。

步骤 13 指定提供 LDAP 提供程序或服务器详细信息的供应商：

Firepower-chassis /security/ldap/server # **set vendor** *{ms-ad | openldap}*

选项如下：

- **ms-ad**—LDAP 提供程序是 Microsoft Active Directory。
- **openldap**—LDAP 提供程序不是 Microsoft Active Directory。

步骤 14 （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。

步骤 15 将事务提交到系统配置：

Firepower-chassis /security/ldap/server # **commit-buffer**

示例

以下示例创建名为 10.193.169.246 的 LDAP 服务器实例，配置绑定 DN、密码、顺序、端口、SSL 设置、供应商属性，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 10.193.169.246
Firepower-chassis /security/ldap/server* # set binddn
```

```
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 2
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 30
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

以下示例创建名为 12:31:71:1231:45b1:0011:011:900 的 LDAP 服务器实例，配置绑定 DN、密码、顺序、端口、SSL、设置、供应商属性，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap* # create server 12:31:71:1231:45b1:0011:011:900
Firepower-chassis /security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-firepower-aaa3,DC=qalab,DC=com"
Firepower-chassis /security/ldap/server* # set password
Enter the password:
Confirm the password:
Firepower-chassis /security/ldap/server* # set order 1
Firepower-chassis /security/ldap/server* # set port 389
Firepower-chassis /security/ldap/server* # set ssl yes
Firepower-chassis /security/ldap/server* # set timeout 45
Firepower-chassis /security/ldap/server* # set vendor ms-ad
Firepower-chassis /security/ldap/server* # commit-buffer
Firepower-chassis /security/ldap/server #
```

删除 LDAP 提供程序

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：

Firepower-chassis /security # **scope ldap**

步骤 3 删除指定的服务器：

Firepower-chassis /security/ldap # **delete server** *serv-name*

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/ldap # **commit-buffer**

示例

以下示例删除名为 ldap1 的 LDAP 服务器，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope ldap
Firepower-chassis /security/ldap # delete server ldap1
Firepower-chassis /security/ldap* # commit-buffer
Firepower-chassis /security/ldap #
```

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 eXtensible Operating System 将使用该设置并忽略默认设置。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 RADIUS 模式：

Firepower-chassis /security # **scope radius**

步骤 3 （可选） 指定在注明 RADIUS 服务器停机之前，重新尝试联系服务器的次数：

Firepower-chassis /security/radius # **set retries** *retry-num*

步骤 4 （可选） 设置系统在注明 RADIUS 服务器停机之前，将等待服务器发出响应的时间量：

Firepower-chassis /security/radius # **set timeout** *seconds*

步骤 5 将任务提交到系统配置：

Firepower-chassis /security/radius # **commit-buffer**

示例

以下示例将 RADIUS 重试次数设置为 4，将超时间隔设置为 30 秒，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # set retries 4
Firepower-chassis /security/radius* # set timeout 30
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

下一步做什么

创建 RADIUS 提供程序。

创建 RADIUS 提供程序

按照以下步骤定义和配置 RADIUS 提供程序，即为此 Firepower 设备提供基于 RADIUS 的 AAA 服务的特定远程服务器。

注释 Firepower eXtensible Operating System最多支持 16 个 RADIUS 提供程序。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 RADIUS 模式：

Firepower-chassis /security # **scope radius**

步骤 3 创建 RADIUS 服务器实例，进入安全 RADIUS 服务器模式：

Firepower-chassis /security/radius # **create server** *server-name*

步骤 4 （可选） 指定用于与 RADIUS 服务器通信的端口。

Firepower-chassis /security/radius/server # **set authport** *authport-num*

步骤 5 设置 RADIUS 服务器密钥：

Firepower-chassis /security/radius/server # **set key**

要设置密钥值，请在键入 **set key** 命令后，按 **Enter** 键，并在提示符处输入密钥值。

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。

步骤 6 （可选） 指定尝试此服务器的顺序。

Firepower-chassis /security/radius/server # **set order** *order-num*

步骤 7 （可选） 设置在注明服务器已关闭之前，重新尝试与 RADIUS 服务器进行通信的次数：

Firepower-chassis /security/radius/server # **set retries** *retry-num*

步骤 8 指定系统在注明 RADIUS 服务器停机之前，将等待服务器发出响应的时间量：

Firepower-chassis /security/radius/server # **set timeout** *seconds*

提示 如果您为 RADIUS 提供程序选择双因素身份验证，建议您配置较高的**超时 (Timeout)** 值。

步骤 9 确认系统配置任务：

Firepower-chassis /security/radius/server # **commit-buffer**

示例

以下示例创建一个名为 radiusserv7 的服务器实例，将身份验证端口设置为 5858，将密钥设置为 radiuskey321，将顺序设置为 2，将重试次数设置为 4，将超时设置为 30，并且提交事务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # create server radiusserv7
Firepower-chassis /security/radius/server* # set authport 5858
Firepower-chassis /security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
Firepower-chassis /security/radius/server* # set order 2
Firepower-chassis /security/radius/server* # set retries 4
Firepower-chassis /security/radius/server* # set timeout 30
Firepower-chassis /security/radius/server* # commit-buffer
Firepower-chassis /security/radius/server #
```

删除 RADIUS 提供程序

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 RADIUS 模式：

Firepower-chassis /security # **scope RADIUS**

步骤 3 删除指定的服务器：

Firepower-chassis /security/radius # **delete server** *serv-name*

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/radius # **commit-buffer**

示例

以下示例删除名为 radius1 的 RADIUS 服务器，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope radius
Firepower-chassis /security/radius # delete server radius1
Firepower-chassis /security/radius* # commit-buffer
Firepower-chassis /security/radius #
```

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。如果单个提供程序配置包括任何这些属性的设置，则 Firepower eXtensible Operating System 将使用该设置并忽略默认设置。

注释　FXOS 机箱不支持　终端访问控制器访问控制系统增强型 (TACACS+) 协议的命令审计。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 TACACS+ 模式：

Firepower-chassis /security # **scope tacacs**

步骤 3 （可选） 设置系统在注明 TACACS+ 服务器停机之前，将等待服务器发出响应的时间量：

Firepower-chassis /security/tacacs # **set timeout** *seconds*

请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/tacacs # **commit-buffer**

示例

以下示例将 TACACS+ 超时间隔设置为 45 秒，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # set timeout 45
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

下一步做什么

创建 TACACS+ 提供程序。

创建 TACACS+ 提供程序

按照以下步骤定义和配置 TACACS+ 提供程序，即为此 Firepower 设备提供基于 TACACS 的 AAA 服务的特定远程服务器。

注释 Firepower eXtensible Operating System最多支持 16 个 TACACS+ 提供程序。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 TACACS+ 模式：

Firepower-chassis /security # **scope tacacs**

步骤 3 创建 TACACS+ 服务器实例，进入安全 TACACS+ 服务器模式：

Firepower-chassis /security/tacacs # **create server** *server-name*

步骤 4 指定 TACACS+ 服务器密钥：

Firepower-chassis /security/tacacs/server # **set key**

要设置密钥值，请在键入 **set key** 命令后，按 **Enter** 键，并在提示符处输入密钥值。

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。

步骤 5 （可选） 指定尝试此服务器的顺序。

Firepower-chassis /security/tacacs/server # **set order** *order-num*

步骤 6 指定系统在注明 TACACS+ 服务器停机之前，将等待服务器发出响应的时间间隔：

Firepower-chassis /security/tacacs/server # **set timeout** *seconds*

提示 如果您为 TACACS+ 提供程序选择双因素身份验证，建议您配置较大的超时值。

步骤 7 （可选） 指定用于与 TACACS+ 服务器通信的端口：

Firepower-chassis /security/tacacs/server # **set port** *port-num*

步骤 8 将任务提交到系统配置：

Firepower-chassis /security/tacacs/server # **commit-buffer**

示例

以下示例创建名为 tacacsserv680 的服务器实例，将密钥设置为 tacacskey321，将顺序设置为 4，将身份验证端口设置为 5859，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # create server tacacsserv680
Firepower-chassis /security/tacacs/server* # set key
```

```
Enter the key: tacacskey321
Confirm the key: tacacskey321
Firepower-chassis /security/tacacs/server* # set order 4
Firepower-chassis /security/tacacs/server* # set port 5859
Firepower-chassis /security/tacacs/server* # commit-buffer
Firepower-chassis /security/tacacs/server #
```

删除 TACACS+ 提供程序

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 TACACS+ 模式：

Firepower-chassis /security # **scope tacacs**

步骤 3 删除指定的服务器：

Firepower-chassis /security/tacacs # **delete server** *serv-name*

步骤 4 将任务提交到系统配置：

Firepower-chassis /security/tacacs # **commit-buffer**

示例

以下示例删除名为 tacacs1 的 TACACS+ 服务器，并且提交任务：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope tacacs
Firepower-chassis /security/tacacs # delete server tacacs1
Firepower-chassis /security/tacacs* # commit-buffer
Firepower-chassis /security/tacacs #
```

验证远程 AAA 服务器配置

以下各节介绍如何使用 FXOS CLI 确定各种远程 AAA 服务器的当前配置。

确定当前的 FXOS 身份验证配置

以下示例显示如何使用 **show authentication** 命令确定当前的 FXOS 身份验证设置。在本示例中，LDAP 是默认的身份验证模式。

```
firepower# scope security
firepower /security # show authentication
Console authentication: Local
Operational Console authentication: Local
```

```
Default authentication: Ldap
Operational Default authentication: Ldap
Role Policy For Remote Users: Assign Default Role
firepower /security #
```

确定当前的 LDAP 配置

以下示例显示如何在 ldap 模式下使用 **show server detail** 命令来确定当前的 LDAP 配置设置。

```
firepower# scope security
firepower /security # scope ldap
firepower /security/ldap # show server detail

LDAP server:
    Hostname, FQDN or IP address: 10.48.53.132
    Descr:
    Order: 1
    DN to search and read: CN=cisco,CN=Users,DC=fxosldapuser,DC=lab
    Password:
    Port: 389
    SSL: No
    Key:
    Cipher Suite Mode: Medium Strength
    Cipher Suite:
ALL:!DHE-PSK-AES256-CBC-SHA:!EDH-RSA-DES-CBC3-SHA:!EDH-DSS-DES-CBC3-SHA:!DES-CBC3-SHA:!ADH:!3DES:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL

    CRL: Relaxed
    Basedn: CN=Users,DC=fxosldapuser,DC=lab
    User profile attribute: CiscoAVPair
    Filter: cn=$userid
    Timeout: 30
    Ldap Vendor: MS AD
firepower /security/ldap #
```

确定当前的 RADIUS 配置

以下示例显示如何在 radius 模式下使用 **show server detail** 命令来确定当前的 RADIUS 配置设置。

```
firepower# scope security
firepower /security # scope radius
firepower /security/radius # show server detail

RADIUS server:
    Hostname, FQDN or IP address: 10.48.17.199
    Descr:
    Order: 1
    Auth Port: 1812
    Key: ****
    Timeout: 5
    Retries: 1
firepower /security/radius #
```

确定当前的 TACACS+ 配置

以下示例显示如何在 tacacs 模式下使用 **show server detail** 命令来确定当前的 TACACS+ 配置设置。

```
firepower# scope security
firepower /security # scope tacacs
firepower /security/tacacs # show server detail
```

```
TACACS+ server:
    Hostname, FQDN or IP address: 10.48.17.199
    Descr:
    Order: 1
    Port: 49
    Key: ****
    Timeout: 5
firepower /security/tacacs #
```

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。将信息记录到中央系统日志服务器有助于汇聚日志和提醒。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 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用或禁用向控制台发送系统日志：

Firepower-chassis /monitoring # {**enable** | **disable**} **syslog console**

步骤 3 （可选）选择要显示的最低消息级别。如果系统日志已启用，系统将在控制台上显示此级别及以上消息。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

Firepower-chassis /monitoring # **set syslog console level** {**emergencies** | **alerts** | **critical**}

步骤 4 启用或禁用操作系统监控系统日志消息：

Firepower-chassis /monitoring # {**enable** | **disable**} **syslog monitor**

步骤 5 （可选）选择要显示的最低消息级别。如果监视器状态已启用，系统将显示此级别及以上消息。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

Firepower-chassis /monitoring # **set syslog monitor level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

注释 只有当您输入了 **terminal monitor** 命令之后，才在终端监视器上显示低于“严重”级别的消息。

步骤 6 启用或禁用向系统日志文件写入系统日志消息：

Firepower-chassis /monitoring # {**enable** | **disable**} **syslog file**

步骤 7 指定记录消息的文件的名称。文件名中最多包含 16 个字符。

Firepower-chassis /monitoring # **set syslog file name** *filename*

步骤 8 （可选） 选择要存储到文件中的最低消息级别。如果文件状态已启用，系统将在系统日志文件中存储此级别及以上消息。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

Firepower-chassis /monitoring # **set syslog file level** {**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

步骤 9 （可选） 在系统开始用最新消息覆写最旧消息之前，请指定最大文件大小（以字节为单位）。范围为 4096 到 4194304 字节。

Firepower-chassis /monitoring # **set syslog file size** *filesize*

步骤 10 配置向最多三个外部系统日志服务器发送系统日志消息：

a) 启用或禁用向最多三个外部系统日志服务器发送系统日志消息：

Firepower-chassis /monitoring # {**enable** | **disable**} **syslog remote-destination** {**server-1** | **server-2** | **server-3**}

b) （可选） 选择要存储到外部日志的最低消息级别。如果远程目的已启用，系统将向外部服务器发送此级别及以上消息。级别选项按紧急程度从高到低的顺序列出。默认级别为“严重 (Critical)”。

Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **level**{**emergencies** | **alerts** | **critical** | **errors** | **warnings** | **notifications** | **information** | **debugging**}

c) 指定已指定的远程系统日志服务器的主机名或 IP 地址。主机名中最多包含 256 个字符。

Firepower 机箱 /monitoring # **set syslog remote-destination** {**server-1** |**server-2** |**server-3**} **hostname** 主机名

d) （可选） 指定向已指定远程系统日志服务器发送的系统日志消息中包含的设备级别。

Firepower-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**}

步骤 11 配置本地来源。为您要启用或禁用的每个本地来源输入以下命令：

Firepower-chassis /monitoring # {**enable** | **disable**} **syslog source** {**audits** | **events** | **faults**}

这可以是以下其中一项：

- **审核 (audits)** - 启用或禁用所有审核事件的日志记录。
- **事件 (events)** - 启用或禁用所有系统事件的日志记录。
- **故障 (faults)** - 启用或禁用所有系统故障的日志记录。

步骤 12 提交任务：

Firepower-chassis /monitoring # **commit-buffer**

示例

以下示例介绍如何启用在本地文件中存储系统日志消息并且提交任务：

```
Firepower-chassis# scope monitoring
Firepower-chassis /monitoring # disable syslog console
Firepower-chassis /monitoring* # disable syslog monitor
Firepower-chassis /monitoring* # enable syslog file
Firepower-chassis /monitoring* # set syslog file name SysMsgsFirepower
Firepower-chassis /monitoring* # set syslog file level notifications
Firepower-chassis /monitoring* # set syslog file size 4194304
Firepower-chassis /monitoring* # disable syslog remote-destination server-1
Firepower-chassis /monitoring* # disable syslog remote-destination server-2
Firepower-chassis /monitoring* # disable syslog remote-destination server-3
Firepower-chassis /monitoring* # commit-buffer
Firepower-chassis /monitoring #
```

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 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 要创建或删除 DNS 服务器，请输入相应的命令，如下所示：

- 要配置系统以使用具有指定 IPv4 或 IPv6 地址的 DNS 服务器，请执行以下操作：

  Firepower-chassis /system/services # **create dns** *{ip-addr | ip6-addr}*

- 要删除具有指定 IPv4 或 IPv6 地址的 DNS 服务器，请执行以下操作：

  Firepower-chassis /system/services # **delete dns** *{ip-addr | ip6-addr}*

步骤 4 将任务提交到系统配置：

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

示例

以下示例配置具有 IPv4 地址 192.168.200.105 的 DNS 服务器并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

以下示例配置具备 IPv6 地址 2001:db8::22:F376:FF3B:AB3F 的 DNS 服务器并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create dns 2001:db8::22:F376:FF3B:AB3F
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

以下示例删除具有 IP 地址 192.168.200.105 的 DNS 服务器并且提交任务：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # delete dns 192.168.200.105
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

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 从 FXOS CLI 进入安全模式：

scope security

步骤 2 启用 FIPS 模式：

enable fips-mode

步骤 3 提交配置：

commit-buffer

步骤 4 重新启动系统：

connect local-mgmt

reboot

如果已启用 FIPS 模式，则会限制允许的密钥大小和算法。MIO 会使用 CiscoSSL 和 FIPS 对象模块 (FOM) 来满足其加密需求。与 ASA 的专有加密库实施和硬件加速相比，它会让 FIPS 验证变得更容易。

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 82 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 从 FXOS CLI 进入安全模式：

scope security

步骤 2 启用通用标准模式：

enable cc-mode

步骤 3 提交配置：

commit-buffer

步骤 4 重新启动系统：

connect local-mgmt

reboot

通用标准是计算机安全的国际标准。CC 侧重于证书、审核、日志记录、密码、TLS、SSH 等。它基本上假设达到 FIPS 合规性要求。与 FIPS 类似，思科与 NIST 认证的实验室供应商签订合同，以便执行测试并提交至 NIAP。

启用 CC 模式时，它会限制需要支持的算法、密码套件和功能的列表。根据网络设备协作保护配置文件 (NDcPP) 来评估 MIO。CiscoSSL 只能执行部分要求，其中大部分要求在《CC 合规性指南》中均有介绍。

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 82 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 100 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 从 FXOS CLI 进入服务模式：

scope system

scope services

步骤 2 为要启用访问权限的服务创建 IP 块：

IPv4：

create ip-block *ip prefix [0-32]* [**http** | **snmp** | **ssh**]

IPv6：

create ipv6-block *ip prefix [0-128]* [**http** | **snmp** | **ssh**]

示例

以下示例显示了如何创建、输入和验证 IPv4 地址块以提供 SSH 访问：

```
firepower # scope system
firepower /system # scope services
firepower /system/services # enter ip-block 192.168.200.101 32 ssh
firepower /system/services/ip-block* # commit-buffer
firepower /system/services/ip-block # up
firepower /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
```

```
    --------------- ------------- --------
    0.0.0.0                     0 https
    0.0.0.0                     0 snmp
    0.0.0.0                     0 ssh
    192.168.200.101            32 ssh
firepower /system/services #
```

以下示例显示了如何创建、输入和验证 IPv6 地址块以提供 SSH 访问：

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ipv6-block 2001:DB8:1::1 64 ssh
firepower /system/services/ipv6-block* # commit-buffer
firepower /system/services/ipv6-block # up
firepower /system/services # show ipv6-block

Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    ::                       0 https
    ::                       0 snmp
    ::                       0 ssh
    2001:DB8:1::1
                            64 ssh
firepower /system/services #
```

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：

A2*xx.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。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 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 232 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 先进入安全服务模式，然后进入自动 MAC 池模式。

scope ssa

scope auto-macpool

示例：

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool #
```

步骤 2 设置生成 MAC 地址所使用的 MAC 地址前缀。

set prefix 前缀

- 前缀 - 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：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.zzzz*

示例：

```
Firepower /ssa/auto-macpool # set prefix 65
Firepower /ssa/auto-macpool* #
```

步骤 3 保存配置。

commit-buffer

示例：

```
Firepower /ssa/auto-macpool* # commit-buffer
Firepower /ssa/auto-macpool #
```

步骤 4 查看 MAC 地址分配。

show mac-address

示例：

```
Firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
    Mac Address           Owner Profile            Owner Name
    -------------------- ------------------------ ----------
    A2:46:C4:00:00:1E    ftd13                    Port-channel14
    A2:46:C4:00:00:20    ftd14                    Port-channel15
    A2:46:C4:00:01:7B    ftd1                     Ethernet1/3
    A2:46:C4:00:01:7C    ftd12                    Port-channel11
    A2:46:C4:00:01:7D    ftd13                    Port-channel14
    A2:46:C4:00:01:7E    ftd14                    Port-channel15
    A2:46:C4:00:01:7F    ftd1                     Ethernet1/2
    A2:46:C4:00:01:80    ftd12                    Ethernet1/2
    A2:46:C4:00:01:81    ftd13                    Ethernet1/2
    A2:46:C4:00:01:82    ftd14                    Ethernet1/2
    A2:46:C4:00:01:83    ftd2                     Ethernet3/1/4
    A2:46:C4:00:01:84    ftd2                     Ethernet3/1/1
    A2:46:C4:00:01:85    ftd2                     Ethernet3/1/3
```

```
A2:46:C4:00:01:86    ftd2                    Ethernet3/1/2
A2:46:C4:00:01:87    ftd2                    Ethernet1/2
A2:46:C4:00:01:88    ftd1                    Port-channel21
A2:46:C4:00:01:89    ftd1                    Ethernet1/8
```

示例

以下示例将 MAC 前缀设为 33。

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool # set prefix 33
Firepower /ssa/auto-macpool* # commit-buffer
Firepower /ssa/auto-macpool #
```

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。

  注释 与具有较大内核数量的实例相比，具有较小核心数量的实例可能具有相对更高的CPU利用率。具有较小核心数量的实例对流量负载变化更敏感。如果出现流量丢弃情况，请尝试分配更多核心。

- 您可以分配偶数（6、8、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 240 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或集群中实例的大小，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 FMC **设备** > **设备管理** > **设备** > **系统** > **资产**对话框上更新每个设备的资产。

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 2 创建资源配置文件。

enter resource-profile *name*

- *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。

示例：

```
Firepower /ssa # enter resource-profile gold
Firepower /ssa/resource-profile* #
```

步骤 3 输入说明。

set description *description*

- *description* - 设置最多 510 个字符的配置文件说明。在含有空格的短语两侧使用引号 (")。

示例：

```
Firepower /ssa/resource-profile* # set description "highest level"
```

步骤 4 设置 CPU 核心数。

set cpu-core-count *cores*

- *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。

示例：

```
Firepower /ssa/resource-profile* # set cpu-core-count 14
```

步骤 5 保存配置。

commit-buffer

示例：

```
Firepower /ssa/resource-profile* # commit-buffer
Firepower /ssa/resource-profile #
```

步骤 6 从安全服务模式查看资源配置文件分配情况。

show resource-profile user-defined

示例：

```
Firepower /ssa # show resource-profile user-defined
Profile Name       Is In Use  CPU Logical Core Count Description
------------------ ---------- ---------------------- -----------
bronze               No               6             low end device
gold                 No               14            highest
silver               No               10             mid-level
```

步骤 7 查看安全模块/引擎插槽的资源使用情况。

show monitor detail

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # show monitor detail
Monitor:
    OS Version:
    CPU Total Load 1 min Avg: 18.959999
    CPU Total Load 5 min Avg: 19.080000
    CPU Total Load 15 min Avg: 19.059999
    Memory Total (MB): 252835
    Memory Free (MB): 200098
    Memory Used (MB): 52738
    CPU Cores Total: 72
    CPU Cores Available: 30
    Memory App Total (MB): 226897
    Memory App Available (MB): 97245
    Data Disk Total (MB): 1587858
    Data Disk Available (MB): 1391250
    Secondary Disk Total (MB): 0
    Secondary Disk Available (MB): 0
    Disk File System Count: 7
    Blade Uptime:
    Last Updated Timestamp: 2018-05-23T14:26:06.132
```

步骤 8 查看应用实例的资源配置情况。

show resource detail

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
    Allocated Core NR: 10
    Allocated RAM (MB): 32413
    Allocated Data Disk (MB): 49152
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0
```

示例

以下示例添加了三个资源配置文件。

```
Firepower# scope ssa
Firepower /ssa # enter resource-profile basic
Firepower /ssa/resource-profile* # set description "lowest level"
Firepower /ssa/resource-profile* # set cpu-core-count 6
Firepower /ssa/resource-profile* # exit
Firepower /ssa # enter resource-profile standard
Firepower /ssa/resource-profile* # set description "middle level"
Firepower /ssa/resource-profile* # set cpu-core-count 10
Firepower /ssa/resource-profile* # exit
Firepower /ssa # enter resource-profile advanced
Firepower /ssa/resource-profile* # set description "highest level"
Firepower /ssa/resource-profile* # set cpu-core-count 12
Firepower /ssa/resource-profile* # commit-buffer
Firepower /ssa/resource-profile #
```

配置网络控制策略

为允许发现非思科设备，FXOS 支持链路层发现协议 *(LLDP)*，这是一个独立于供应商的设备发现协议，在 IEEE 802.1ab 标准中定义。LLDP 允许网络设备将自身信息通告给网络中的其他设备。此协议在数据链路层上运行，它使运行不同网络的两个系统可以了解彼此。

LLDP是一种单向协议，它传输设备及其接口的功能和当前状态信息。LLDP设备使用该协议来仅从其他 LLDP 设备请求信息。

要在 FXOS 机箱上启用此功能，您可以配置网络控制策略，用于指定 LLDP 传输和接收行为。 网络控制策略创建后，需要分配至接口。您可以启用包括非模块化端口、EPM端口、端口通道和分支端口在内的任何前接口上的 LLDP。

注释

- 无法在专用管理端口上配置 LLDP。
- 连接到刀片的内部背板端口默认启用LLDP且未设禁用选项。所有其他端口均默认禁用LLDP。

过程

步骤 1 输入组织范围。

scope org

示例：

```
Firepower # scope org
```

步骤 2 创建并启用网络控制策略。

create nw-ctrl-policy *nw-policy*

示例：

```
Firepower /org #  create nw-ctrl-policy nw-policy
```

步骤 3 启用 LLDP。

enable lldp *{receive | transmit}*

示例：

```
Firepower /org/nw-ctrl-policy* # enable lldp receive
Firepower /org/nw-ctrl-policy* # disable lldp transmit
```

步骤 4 提交配置：

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

步骤 5 指定是否启用或禁用 LLDP 进行接收/传输。

enable lldp 接收/传输

commit-buffer

示例：

```
Firepower /org/nw-ctrl-policy* # enable lldp receive
Firepower /org/nw-ctrl-policy* # disable lldp transmit
Firepower /org/nw-ctrl-policy* # commit-buffer

Firepower /org/nw-ctrl-policy* # enable lldp receive
Firepower /org/nw-ctrl-policy* # disable lldp transmit
Firepower /org/nw-ctrl-policy* # commit-buffer
```

步骤 6 使用以下命令将网络控制策略应用到接口。

a) 输入接口：

scope eth-uplink

scope fabric a

scope interface *interface_id*

```
Firepower # scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface Ethernet3/1
```

b) 设置　网络控制策略：

set nw-ctrl-policy *nw-policy*

commit-buffer

```
Firepower /eth-uplink/fabric/interface # set nw-ctrl-policy nw-policy
Firepower /eth-uplink/fabric/interface* # commit-buffer
MIO-5 /eth-uplink/fabric/interface # show detail
```

c) 查看更改：

show detail

```
Firepower /eth-uplink/fabric/interface # show detail
Interface:
    Port Name: Ethernet3/1
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Sfp Not Present
    State Reason: Unknown
    flow control policy: default
    Auto negotiation: No
    Admin Speed: 100 Gbps
    Oper Speed: 100 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Allowed Vlan: All
    Network Control Policy: nw-policy
    Current Task:
```

d) 提交配置：

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

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 进入系统模式：

scope system

示例：

```
Firepower# scope system
Firepower /system #
```

步骤 2 要配置新的机箱名称：

set name *chassis_name*

- 机箱名称 - 设置介于 1 至 60 个字符之间的机箱名称。

示例：

```
Firepower /system # set name Firepower_chassis
```

步骤 3 要配置管理 URL：

set mgmt-url *management_url*

- *management_url* - 设置 FMC 应用来连接到 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。

示例：

```
Firepower /system # set mgmt-url https://192.168.1.55
```

步骤 4 保存配置。

commit-buffer

示例：

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

步骤 5 查看配置设置。

show detail

示例：

```
Firepower_chassis /system # show detail

Systems:
    Name: Firepower_chassis
    Mode: Stand Alone
    System IP Address: 192.168.1.10
```

```
System IPv6 Address: ::
System Owner:
System Site:
Description for System:
Chassis Mgmt URL: https://192.168.1.55
```

第 10 章

接口管理

- 关于 Firepower 接口， 第 185 页
- Firepower 接口的准则和限制， 第 203 页
- 配置接口， 第 205 页
- 监控接口， 第 215 页
- 排除接口故障， 第 217 页
- 接口历史， 第 223 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 99 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。

注释 机箱管理接口不支持巨型帧。

接口类型

每个接口可以是以下类型之一：

- 数据 - 用于常规数据。不能在逻辑设备之间共享数据接口，且逻辑设备无法通过背板与其他逻辑设备通信。对于数据接口上的流量，所有流量必须在一个接口上退出机箱，并在另一个接口上返回以到达另一个逻辑设备。
- 数据共享 - 用于常规数据。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使用FMC）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。共享接口不支持用于网桥组成员接口（在透明模式或路由模式下）、内联集、被动接口、集群或故障切换链路。
- 管理 - 用于管理应用程序实例。这些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。对于 ASA、FMC 以及 FTD：您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。

  注释 管理接口更改会导致逻辑设备重新启动，例如将管理接口从 e1/1 更改为 e1/2 会导致逻辑设备重新启动以应用新的管理接口。

- Firepower 事件 - 用作 FTD-using-FMC 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。有关详细信息，请参阅 FMC 配置指南。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。 如果稍后为管理配置数据接口，则无法使用单独的事件接口。
- 集群 - 用作集群逻辑设备的集群控制链路。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。“集群”类型仅在 EtherChannel 接口上受支持。 对于多实例集群，无法在设备之间共享集群类型接口。您可以将 VLAN 子接口添加到集群 EtherChannel，以便为每个集群提供单独的集群控制链路。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。FDM 不支持集群。

有关独立部署和集群部署中 FTD 和 ASA 应用的接口类型支持，请参阅下表。

表 *14:* 接口类型支持

应用		数据	数据：子接口	数据共享	数据共享：子接口	管理	Firepower 事件	集群（仅 EtherChannel）	集群：子接口
FTD	独立本地实例	支持	-	-	-	支持	支持	-	-
	独立容器实例	支持	支持	支持	支持	支持	支持	-	-
	集群本地实例	支持（EtherChannel 仅用于机箱间集群）	-	-	-	支持	支持	支持	-
	集群容器实例	支持（EtherChannel 仅用于机箱间集群）	-	-	-	支持	支持	支持	支持
ASA	独立本地实例	支持	-	-	-	支持	-	支持	-
	集群本地实例	支持（EtherChannel 仅用于机箱间集群）	-	-	-	支持	-	支持	—

FXOS 接口与应用接口

Firepower 4100/9300 管理物理接口、容器实例的 VLAN 子接口和 EtherChannel（端口通道）接口的基本以太网设置。在应用中，您可以配置更高级别的设置。例如，您只能在 FXOS 中创建 EtherChannel；但是，您可以为应用中的 EtherChannel 分配 IP 地址。

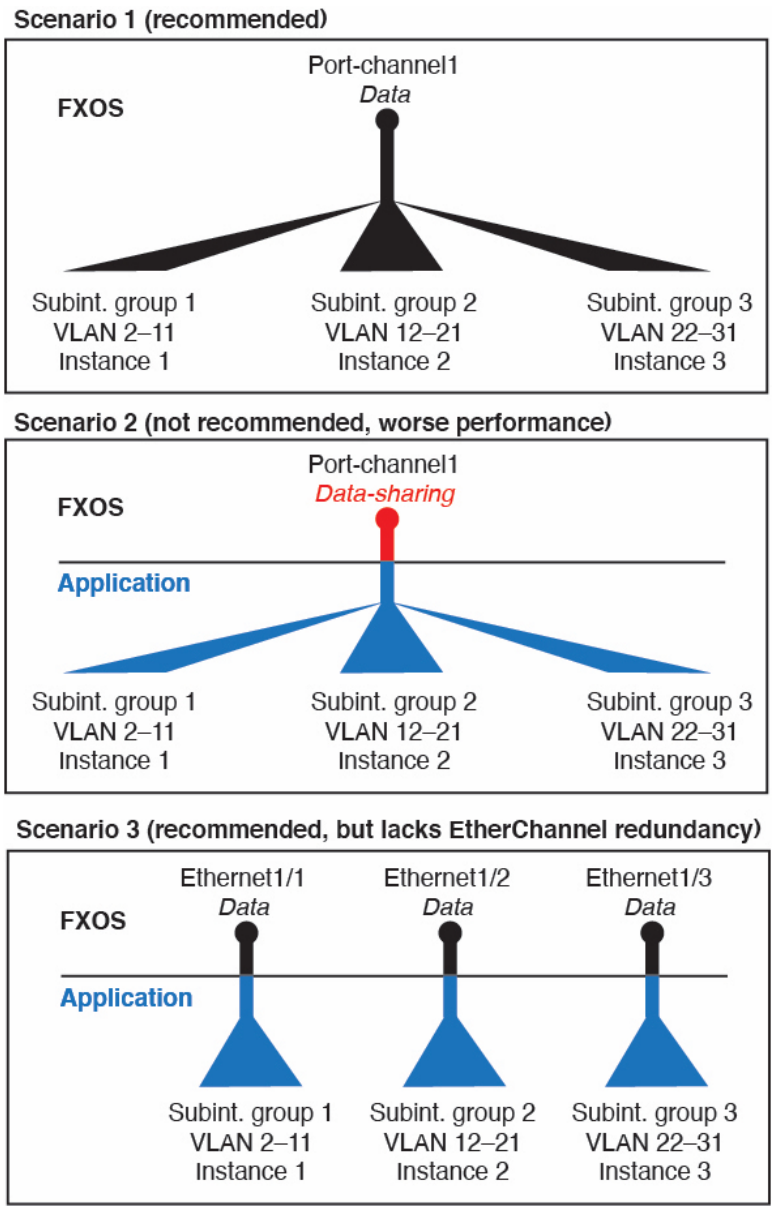
下文将介绍 FXOS 接口与应用接口之间的交互。

VLAN 子接口

对于所有逻辑设备，您可以在应用内创建 VLAN 子接口。

仅对于独立模式下的容器实例，您还可以在 FXOS 中创建 VLAN 子接口（在没有 FXOS 子接口的接口上）。除集群类型接口外，多实例集群不支持 FXOS 中的子接口。应用定义的子接口不受 FXOS 限值的约束。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：

图 *2: FXOS* 中的 *VLAN* 与容器实例的应用



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，但默认启用子接口。

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旁路功能。硬件旁路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。

硬件旁路功能在 FTD 应用中进行配置。您不需要将这些接口用作硬件旁路对；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旁路功能的接口。如果您想使用硬件旁路功能，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。

当在内联对上启用硬件旁路时，首先尝试交换机旁路。如果由于交换机错误而导致旁路配置失败，则会启用物理旁路。

注释 硬件旁路 (FTW) 在与第三方应用（例如 VDP/Radware）的服务链中安装的 FTD 上不受支持。

对于以下型号上特定网络模块的接口对，FTD 支持 硬件旁路：

- Firepower 9300
- Firepower 4100 系列

这些型号的受支持 硬件旁路 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)

硬件旁路 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。

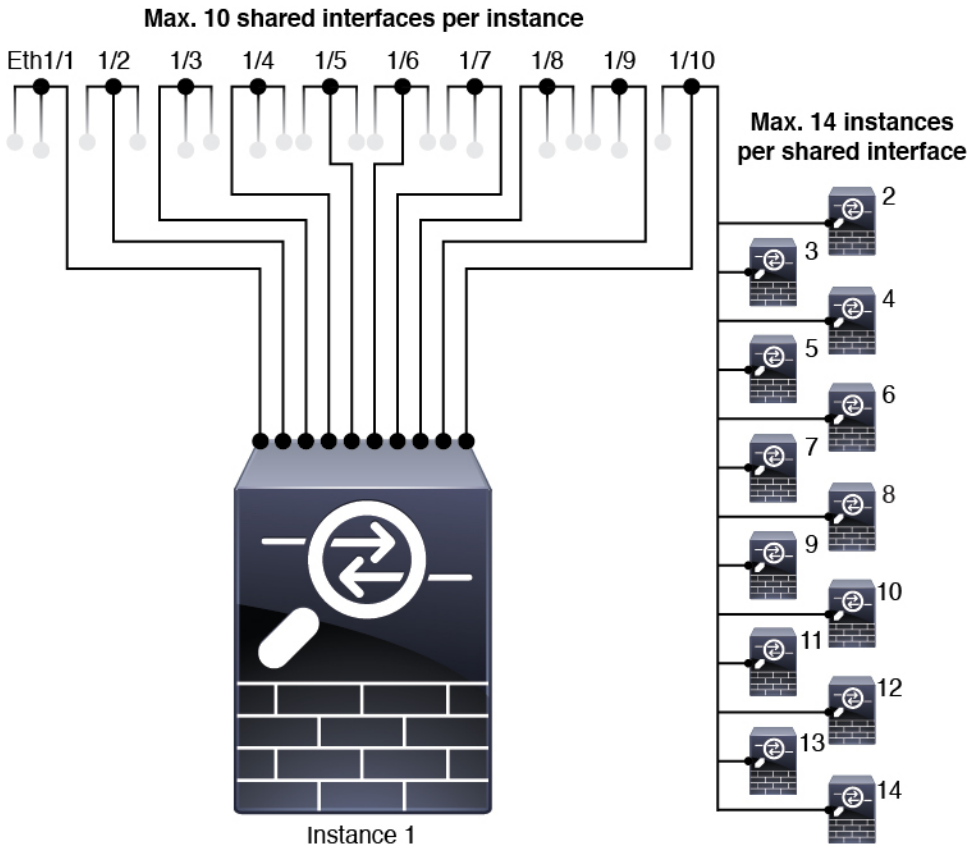
注释 机箱管理接口不支持巨型帧。

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。您最多可以创建 500 个 VLAN 子接口。

请参阅共享接口分配的以下限制：



共享接口最佳实践

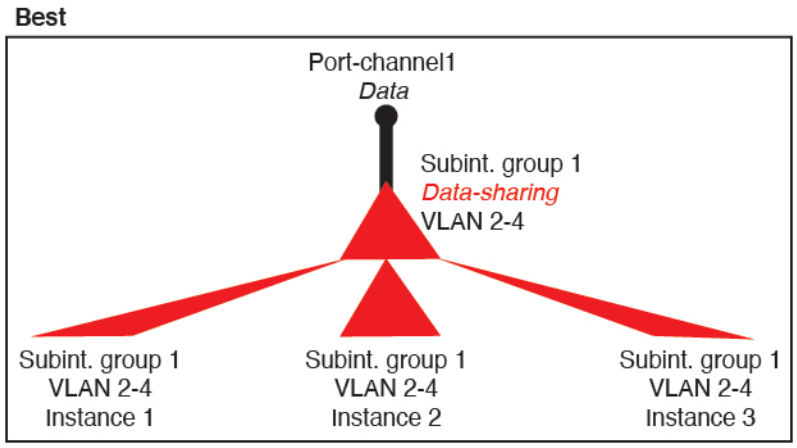
为确保转发表的最佳可扩展性，请共享尽可能少的接口。相反，您可以在一个或多个物理接口上创建最多 500 个 VLAN 子接口，然后在容器实例之间划分 VLAN。

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实例。

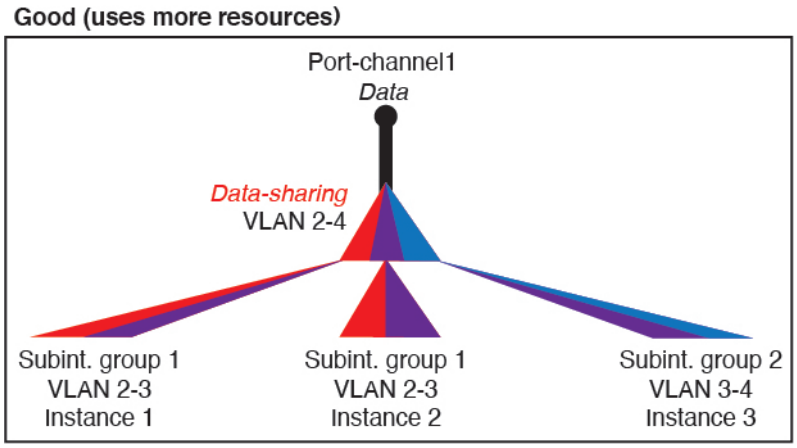
   例如，创建一个大型 EtherChannel 以将所有类似接口捆绑在一起，然后共享该 EtherChannel 的子接口：Port-Channel1.2, 3 和 4 而不是 Port-Channel2、Port-Channel3 和 Port-Channel4。与跨父项共享物理/EtherChannel 接口或子接口相比，当您共享单父项子接口时，VLAN 组表提供更高的转发表可扩展性。

   图 *3:* 最佳：一个父项上的共享子接口组



   如果未与一组实例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，与实例 1、2 和 3（一个 VLAN 组）共享 Port-Channel1.2, 3 和 4 而不是与实例 1 和 2 分享 Port-Channel1.2 和 3，同时与实例 3（两个 VLAN 组）共享 Port-Channel1.3 和 4。

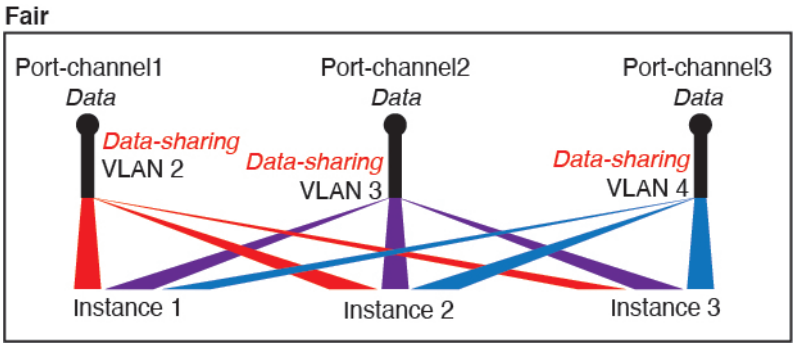
   图 *4:* 良好：一个父项上共享多个子接口组



2. 一般 - 跨父项共享子接口。

例如，共享 Port-Channel1.2、Port-Channel2.3 和 Port-Channel3.4 而不是 Port-Channel2、Port-Channel4 和 Port-Channel4。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。

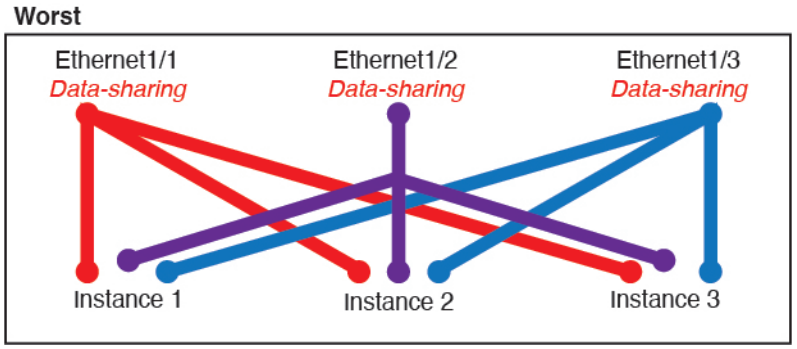
图 *5:* 一般：独立父项上的共享子接口



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。

图 *6:* 最差：共享父接口



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 15: Firepower 9300（设有三个 SM-44）上的物理/EtherChannel 接口和实例， 第 193 页
- 表 16: Firepower 9300（设有三个 SM-44）上的一个父接口的子接口和实例， 第 195 页
- 表 17: Firepower 9300（设有一个 SM-44）上的物理/EtherChannel 接口和实例， 第 198 页
- 表 18: Firepower 9300（设有一个 SM-44）上的一个父接口的子接口和实例， 第 200 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 *15: 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: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 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:** • 1 • 1 • 1	**33:** • 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: • *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:*** • *1* • *1* • *1*	***34:*** • 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: • 30（每个实例 1 个专用接口）	**1**	**6：** • 实例 1 实例 6	25%
30: • 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:** • 1 • 1 • 1	**6：** • 实例 1 至实例 2 • 实例 2 至实例 4 • 实例 5 至实例 6	23%
30: • 30（每个实例 6 个专用接口）	**2**	**5：** • 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: • 12（每个实例 6 个专用接口） • 18（每个实例 6 个专用接口）	**4:** • 2 • 2	**5:** • 实例 1 至实例 2 • 实例 2 至实例 5	26%
24: • 6 • 6 • 6 • 6	**7**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	44%
24: • 12（每个实例 6 个专用接口） • 12（每个实例 6 个专用接口）	**14:** • 7 • 7	**4:** • 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 ***16: 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: • 168（每个实例 4 个专用子接口）	**0**	**42:** • 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: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	27%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
33: • 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:** • 1 • 1 • 1	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
165: • 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:** • 1 • 1 • 1	**33:** • 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: • 70（每个实例 5 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
165: • 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:** • 2 • 2 • 2	**33:** • 实例 1 至实例 11 • 实例 12 至实例 22 • 实例 23 至实例 33	98%
70: • 70（每个实例 5 个专用子接口）	**10**	**14:** • 实例 1 至实例 14	46%
165: • *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:*** • *10* • *10* • *10*	***33:*** • 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 *17: 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: • 8 • 8 • 8 • 8	**0**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	16%
30: • 15 • 15	**0**	**2:** • 实例 1 • 实例 2	14%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
14: • 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:** • **1** • **1**	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
32: • 8 • 8 • 8 • 8	**1**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	21%

专用接口	共享接口	实例数	转发表使用百分比
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**2**	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	20%
32: • 8 • 8 • 8 • 8	**2**	**4:** • 实例 1 • 实例 2 • 实例 3 • 实例 4	25%
32: • 16（每个实例 8 个专用接口） • 16（每个实例 8 个专用接口）	**4:** • 2 • 2	**4:** • 实例 1 至实例 2 • 实例 3 至实例 4	24%
24: • 8 • 8 • 8	**8**	**3:** • 实例 1 • 实例 2 • 实例 3	37%
10: • 10（每个实例 2 个专用接口）	**10**	**5:** • 实例 1 至实例 5	69%

专用接口	共享接口	实例数	转发表使用百分比
10: • 6（每个实例2个专用接口） • 4（每个实例2个专用接口）	**20:** • 10 • 10	**5：** • 实例 1 至实例 3 • 实例 4 至实例 5	59%
14: • *12*（每个实例 *2* 个专用接口）	***10***	***7***： • 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 ***18: 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： • 112（每个实例 8 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
224: • 224（每个实例 16 个专用子接口）	**0**	**14:** • 实例 1 至实例 14	17%
14: • 14（每个实例 1 个专用子接口）	**1**	**14:** • 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
14: • 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:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**1**	**14:** • 实例 1 至实例 14	46%
112： • 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:** • 1 • 1	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
112： • 112（每个实例 8 个专用子接口）	**2**	**14:** • 实例 1 至实例 14	46%
112： • 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：** • 2 • 2	**14:** • 实例 1 至实例 7 • 实例 8 至实例 14	37%
140: • 140（每个实例 10 个专用子接口）	**10**	**14:** • 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
140: • 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:** • 10 • 10	**14:** • 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，在 **scope fabric-interconnect** 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

- 子接口（和父接口）仅可分配至容器实例。

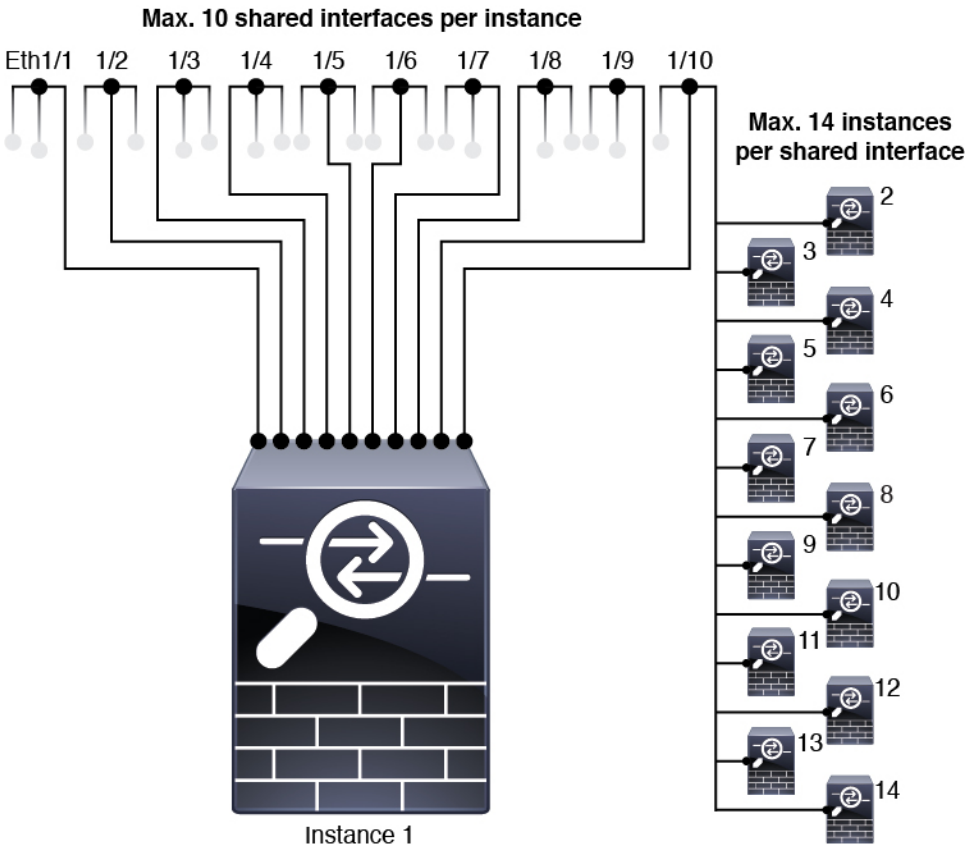
  注释 如果将父接口分配至容器实例，该接口将仅传递未标记（非 VLAN）流量。除非您想要传递未标记流量，否则不予分配父接口。 对于集群类型接口，不得使用父接口。

- 子接口在数据或数据共享型接口以及集群类型接口上受支持。如果向某个集群接口添加子接口，则不能将该接口用于本地集群。
- 对于多实例集群，数据接口上不支持子接口。但是，集群控制链路支持子接口，因此可以将专用 EtherChannel 或 EtherChannel 子接口用于集群控制链路。
- 最多可以创建 500 个 VLAN ID。
- 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

- 不得结合使用数据共享接口和本地实例。
- 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。



- 不得在集群中使用数据共享接口。
- 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 FTD

- 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。

硬件旁路

- 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 硬件旁路。
- 不可为分支端口配置具有硬件旁路功能的接口。

- 不得包含 EtherChannel 中的硬件旁路接口包含在并将它们用于硬件旁路；可以将它们用作 EtherChannel 中的常规接口。
- 硬件旁路不支持高可用性。

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。对于子接口，如果决定要手动配置 MAC 地址，请确保将唯一 MAC 地址用于同一父接口上的所有子接口，从而确保分类正确。请参阅容器实例接口的自动 MAC 地址，第 232 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。

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 进入接口模式。

scope eth-uplink

scope fabric a

步骤 2 启用接口。

enter interface *interface_id*

enable

示例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

注释 不能单独修改作为端口通道成员的接口。如果您在作为端口通道成员的接口上使用 **enter interface** 或 **scope interface** 命令，将会收到一条错误消息，说明对象不存在。应先使用 **enter interface** 命令编辑接口，然后在将接口添加到端口通道。

步骤 3 （可选）设置接口类型。

set port-type {**data** | **data-sharing** | **mgmt** | **firepower-eventing** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data 关键字为默认类型。容器实例仅支持**data-sharing**类型。请勿选择 **cluster** 关键字；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 4 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 5 设置接口速度。

set admin-speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

步骤 6 设置接口双工模式。

set admin-duplex {**fullduplex** |**halfduplex**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

步骤 7 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。请参阅配置流量控制策略，第 213 页。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 8 保存配置。

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

添加 EtherChannel（端口通道）

EtherChannel（也称为端口通道）最多可以包含 16 个同一介质类型和容量的成员接口，并且必须设置为相同的速度和双工模式。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的 SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 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。

注释 如果将其模式从打开更改为主用或从主用更改为打开状态，则可能需要多达三分钟的时间才能使 EtherChannel 进入运行状态。

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。

Firepower 4100/9300 机箱 创建 EtherChannel 时，EtherChannel 将处于**挂起**状态（对于主动 LACP 模式）或**关闭**状态（对于打开 LACP 模式），直到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**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**或**关闭**状态。

过程

步骤 1 进入接口模式：

scope eth-uplink

scope fabric a

步骤 2 创建端口通道：

create port-channel *id*

enable

步骤 3 分配成员接口：

create member-port *interface_id*

您最多可以添加相同介质类型和容量的16个成员接口。成员接口必须设置为相同的速度和双工，并且必须与您为此端口通道配置的速度和双工相匹配。介质类型可以是 RJ-45 或 SFP；可以混合使用不同类型（铜缆和光纤）的SFP。不能通过在大容量接口上将速度设置为较低值来混合接口容量（例如 1GB 和 10GB 接口）。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

步骤 4 （可选） 设置接口类型。

set port-type {**data** | **data-sharing** | **mgmt** | **firepower-eventing** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data 关键字为默认类型。容器实例仅支持**data-sharing**类型。请勿选择 **cluster** 关键字，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 5 为端口通道的成员设置所需的接口速度。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

如果添加未达到指定速度的成员接口，接口将无法成功加入端口通道。默认值为 **10gbps**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

步骤 6 （可选） 为端口通道的成员设置所需的双工。

set duplex {**fullduplex** | **halfduplex**}

如果添加以指定双工配置的成员接口，接口将无法成功加入端口通道。默认值为 **fullduplex**。

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

步骤 7 启用或禁用自动协商（如果您的接口支持）。

set auto-negotiation {**on** | **off**}

示例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

步骤 8 设置数据和数据共享接口的 LACP 端口通道模式。

对于非数据和数据共享接口，模式始终是主用模式。

set port-channel-mode {**active** | **on**}

示例：

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

步骤 9 如果您编辑了默认流量控制策略，则它已应用于接口。如果您创建了新策略，请将其应用于接口。请参阅配置流量控制策略，第 213 页。

set flow-control-policy *name*

示例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

步骤 10 提交配置：

commit-buffer

为容器实例添加 VLAN 子接口

您最多可以将 500 个子接口连接到您的机箱。

对于多实例集群，只能将子接口添加到集群类型接口；不支持数据接口上的子接口。

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。

您还可以在应用内添加子接口。

过程

步骤 1 进入交换矩阵模式。

scope eth-uplink

scope fabric a

示例：

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric #
```

步骤 2 输入要添加子接口的接口。

enter {**interface** | **port-channel**} *interface_id*

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。

子接口在数据或数据共享型接口以及集群类型接口上受支持。

示例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface #
```

步骤 3 创建子接口。

enter subinterface *id*

- *id* - 设置介于 1 和 4294967295 之间的 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。

示例：

```
Firepower /eth-uplink/fabric/interface # enter subinterface 100
Firepower /eth-uplink/fabric/interface/subinterface* #
```

步骤 4 设置 VLAN。

set vlan *id*

- *id* - 设置介于 1 和 4095 之间的 VLAN ID。

示例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 100
```

步骤 5 设置接口类型。

set port-type {**data** | **data-sharing** | **cluster**}

示例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data
```

对于数据和数据共享接口：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。默认类型为数据。

步骤 6 保存配置。

commit-buffer

示例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

示例

以下示例在以太网接口 1/1 上创建 3 个子接口，并将这些接口设置为数据共享接口。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface Ethernet1/1
Firepower /eth-uplink/fabric/interface # enter subinterface 10
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 11
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
```

```
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 12
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

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旁路功能的接口。

过程

步骤 1 要创建新分支，请使用以下命令：

a) 进入布线模式：

scope cabling

scope fabric a

b) 创建分支：

create breakout *network_module_slot port*

示例：

```
Firepower /cabling/fabric/ # create breakout 2 1
```

c) 提交配置：

commit-buffer

这将造成自动重启。配置多个分支时，应在发出 commit-buffer 命令之前创建所有分支。

步骤 2 要启用/配置分支端口，请使用以下命令：

a) 进入接口模式：

scope eth-uplink

scope fabric a

scope aggr-interface *network_module_slot port*

注释　不能单独修改作为端口通道成员的接口。如果您在作为端口通道成员的接口上使用 **enter interface** 或 **scope interface** 命令，将会收到一条错误消息，说明对象不存在。应先使用 **enter interface** 命令编辑接口，然后在将接口添加到端口通道。

b) 使用 **set** 命令配置接口速度和端口类型。

使用 **enable** 或 **disable** 命令设置接口的管理状态。

c) 提交配置：

commit-buffer

配置流量控制策略

流量控制策略确定当端口的接收缓冲区已满时，以太网端口是否发送和接收 IEEE 802.3x 暂停帧。这些暂停帧请求传输端口暂停发送数据几毫秒，直到缓冲区已清除。要使设备之间的流量控制正常工作，必须同时启用两个设备对应的接收和发送流量控制参数。

默认策略会禁用发送和接收控制，并将优先级设为自动协商。

过程

步骤 1 进入以太网上行链路，然后进入流量控制模式。

scope eth-uplink

scope flow-control

示例：

```
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control #
```

步骤 2 编辑或创建流量控制策略。

enter policy *name*

如果想要编辑默认策略，请输入 **default** 作为名称。

示例：

```
firepower-4110 /eth-uplink/flow-control # enter policy default
firepower-4110 /eth-uplink/flow-control/policy* #
```

步骤 3 设置优先级。

set prio {**auto** | **on**}

优先级设置是否协商或启用此链路的 PPP。

示例：

```
firepower-4110 /eth-uplink/flow-control/policy* # set prio on
```

步骤 4 启用或禁用流量控制接收暂停。

set receive {**on** | **off**}

- **启用** - 接受暂停请求，该上行链路端口上的所有流量都暂停，直到网络取消暂停请求为止。
- **禁用** - 忽略来自网络的暂停请求，流量继续正常传输。

示例：

```
firepower-4110 /eth-uplink/flow-control/policy* # set receive on
```

步骤 5 启用或禁用流量控制发送暂停。

set send {**on** | **off**}

- **启用** - 如果传入数据包速率太高，Firepower 4100/9300 会向网络发送暂停请求。暂停保持几毫秒，直至流量重置为正常水平。
- **禁用** - 端口上的流量正常传输，无论数据包负载如何。

示例：

```
firepower-4110 /eth-uplink/flow-control/policy* # set send on
```

步骤 6 保存配置。

commit-buffer

示例：

```
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer
firepower-4110 /eth-uplink/flow-control/policy #
```

示例

以下示例配置了流量控制策略。

```
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control # enter policy FlowControlPolicy23
firepower-4110 /eth-uplink/flow-control/policy* # set prio auto
firepower-4110 /eth-uplink/flow-control/policy* # set receive on
firepower-4110 /eth-uplink/flow-control/policy* # set send on
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer
firepower-4110 /eth-uplink/flow-control/policy #
```

监控接口

注释 由于 FTD/ASA 中的分段删除，FXOS 和 FTD/ASA 接口利用率之间可能存在差异。要查看分散性下降，请参阅 FTD/ASA **show asp drop** 和 **show fragment** 命令。

- **show interface**

  显示接口状态。

  注释 此列表中不包含在端口通道中充当端口的接口。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State
  Allowed Vlan State Reason
    --------------- ------------------ ----------- ----------------
 ------------ ------------
    Ethernet1/2     Data               Enabled     Up
  All
    Ethernet1/4     Mgmt               Enabled     Up
  All
    Ethernet1/5     Data               Enabled     Up
  Untagged
    Ethernet1/7     Firepower Eventing Enabled     Up
  All
    Ethernet1/8     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/1     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/2     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/3     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/4     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/5     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/6     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/7     Data               Disabled    Sfp Not Present
  All          Unknown
    Ethernet2/8     Data               Disabled    Sfp Not Present
  All          Unknown
```

- **show port-channel**

  显示端口通道状态。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin State Oper State
Port Channel Mode Allowed Vlan State Reason
    ---------------- ---------------- ------------------ ----------- ----------------
----------------- ------------ ------------
    1                Port-channel1    Data               Enabled     Up
Active            Untagged
    2                Port-channel2    Data               Enabled     Failed
Active            All          No operational members
    48               Port-channel48   Cluster            Enabled     Up
Active            All
```

- **show detail**

  查看共享接口的转发表和 VLAN 组使用情况。

```
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:
```

- **show subinterface**

  显示给定接口的子接口。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface ethernet1/8
Firepower /eth-uplink/fabric/interface # show subinterface
Sub Interface:
    Sub-If Id  Sub-Interface Name VLAN        Port Type
    ---------- ------------------ ----------- ---------
            10 Ethernet1/8.10     11          Data
            11 Ethernet1/8.11     12          Data
```

- **show mac-address**

  显示容器实例接口的 MAC 地址分配情况。

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
    Mac Address          Owner Profile            Owner Name
    -------------------- ------------------------ ----------
    A2:46:C4:00:00:1E    ftd13                    Port-channel14
    A2:46:C4:00:00:20    ftd14                    Port-channel15
    A2:46:C4:00:01:7B    ftd1                     Ethernet1/3
    A2:46:C4:00:01:7C    ftd12                    Port-channel11
    A2:46:C4:00:01:7D    ftd13                    Port-channel14
    A2:46:C4:00:01:7E    ftd14                    Port-channel15
    A2:46:C4:00:01:7F    ftd1                     Ethernet1/2
    A2:46:C4:00:01:80    ftd12                    Ethernet1/2
    A2:46:C4:00:01:81    ftd13                    Ethernet1/2
    A2:46:C4:00:01:82    ftd14                    Ethernet1/2
    A2:46:C4:00:01:83    ftd2                     Ethernet3/1/4
    A2:46:C4:00:01:84    ftd2                     Ethernet3/1/1
    A2:46:C4:00:01:85    ftd2                     Ethernet3/1/3
    A2:46:C4:00:01:86    ftd2                     Ethernet3/1/2
    A2:46:C4:00:01:87    ftd2                     Ethernet1/2
    A2:46:C4:00:01:88    ftd1                     Port-channel21
    A2:46:C4:00:01:89    ftd1                     Ethernet1/8
```

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  present
                                          200  present
                                          300  present
2048 512       configured
                                          0    present
2049 511       configured
                                          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                           Port or Port Channel Name Port Type          App Name
   Description
    ------------------------------ ------------------------- ------------------ ----------
 -----------
    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

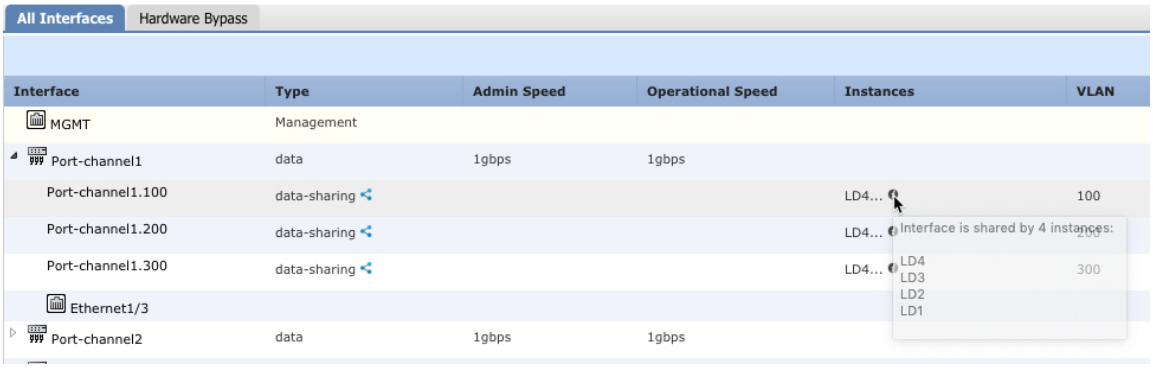
从 CLI 上组中的所有逻辑设备上删除子接口，然后保存配置以同步删除信息。例如：

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  present
                                             200  present
                                             300  present
2048 512       configured
                                             0    present
2049 511       configured
                                             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，并应与 **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 7: 每个共享接口的实例数



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-channel1.400
 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-channel1.400
 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-channel1.400
 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-channel1.400
 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
FTD 运行链路状态与物理链路状态之间的同步	2.9.1	机箱现在可以将 FTD 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 FTD 应用接口管理状态。如果没有从 FTD 同步，数据接口可能在 FTD 应用完全上线之前处于“Up”物理状态，或者在您启动 FTD 关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 FTD 可以处理流量之前开始向 FTD 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 FTD 不支持此功能。此外，ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备 > 启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail**
支持集群类型接口上的 VLAN 子接口（仅限多实例使用）	2.8.1	要与多实例集群配合使用，您现在可以在集群类型接口上创建 VLAN 子接口。由于每个集群都需要唯一的集群控制链路，因此 VLAN 子接口提供了一种可满足此要求的简单方法。您也可以为每个集群分配专用的 EtherChannel。现在允许多个集群类型接口。 新增/修改的命令：**set port-type cluster**
支持 500 个 VLAN，无意外事件	2.7.1	以前，设备支出 250 到 500 个 VLAN，具体取决于父接口的数量和其他部署决策。现在，您可以在所有情况下使用 500 个 VLAN。

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	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。 **注释** 要求使用 6.3 或更高版本的 FTD。 新增/修改的命令：**create subinterface, set vlan, show interface,show subinterface** 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
用于容器实例的数据共享接口	2.4.1	要确保灵活使用物理接口，可以在多个实例之间共享接口。 **注释** 要求使用 6.3 或更高版本的 FTD。 新增/修改的命令：**set port-type data-sharing**、**show interface**
支持保存模式下的数据 Etherchannel	2.4.1	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。 新增/修改的命令：**set port-channel-mode**
支持 FTD内联集中的 Etherchannel	2.1.1	现在可以使用 FTD 内联集中的 EtherChannel。
FTD 支持的内联集链路状态传播	2.0.1	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。 新增/修改的命令：**show fault |grep link-down**, **show interface detail**
FTD 支持的硬件绕行网络模块	2.0.1	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。 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**
用于 FTD 的 Firepower 事件类型接口	1.1.4	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。 新增/修改的 FXOS 命令：**set port-type firepower-eventing**、**show interface**

第 11 章

逻辑设备

- 关于逻辑设备， 第 225 页
- 逻辑设备的要求和必备条件， 第 233 页
- 逻辑设备的准则和限制， 第 241 页
- 添加独立的逻辑设备， 第 246 页
- 添加高可用性对， 第 273 页
- 添加群集， 第 274 页
- 配置 Radware DefensePro， 第 309 页
- 配置 TLS 加密加速， 第 319 页
- 管理逻辑设备， 第 322 页
- 监控逻辑设备， 第 332 页
- 站点间群集示例， 第 334 页
- 逻辑设备的历史记录， 第 337 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，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

独立和群集逻辑设备

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。

- 群集 - 群集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群集。对于 Firepower 9300，所有三个模块必须参与集群，同时适用于本地实例和容器实例。 FDM 不支持集群。

逻辑设备应用程序实例：容器和本地

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。仅使用 FMC 的 Firepower 威胁防御支持多实例功能；ASA 或使用 FDM 的 FTD 不支持。

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。 多实例集群不得使用 VLAN 子接口或共享接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。请参阅共享接口可扩展性，第 190 页和为容器实例添加 VLAN 子接口，第 210 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。

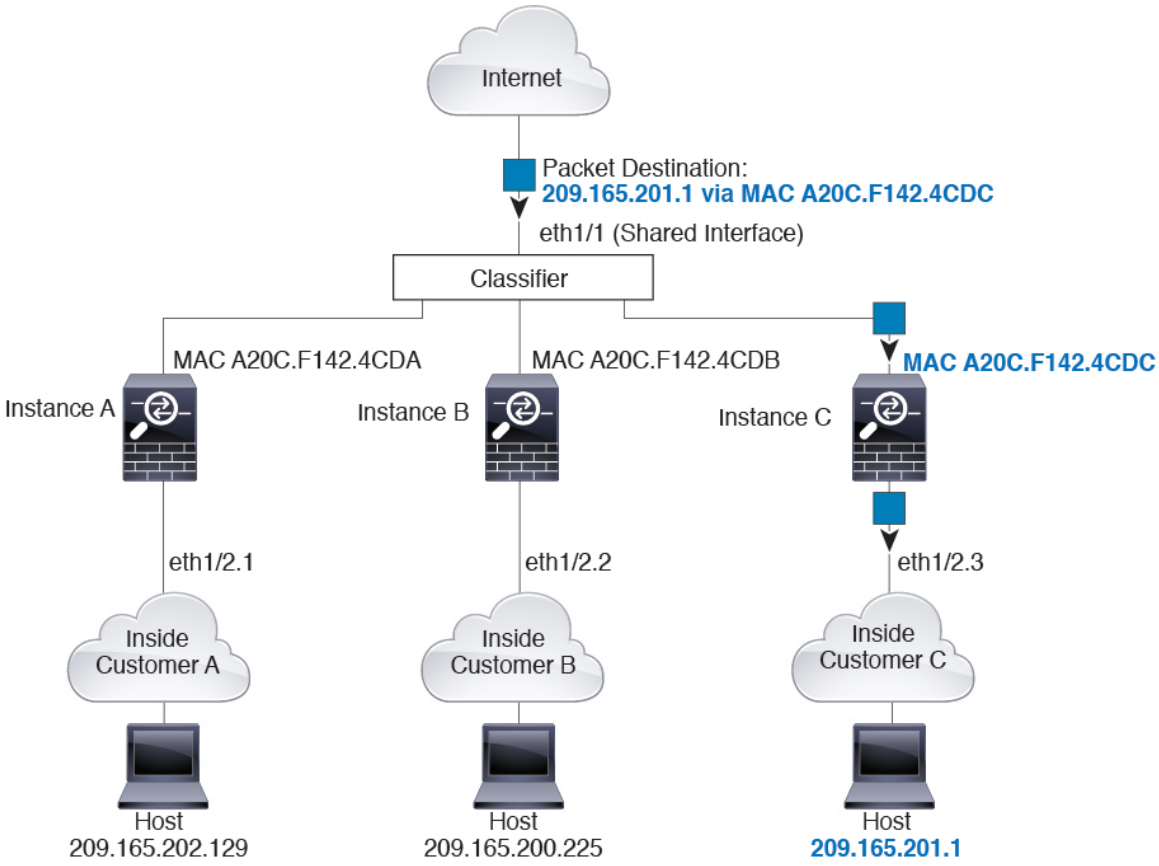
- 唯一接口 - 如果仅有一个实例与传入接口相关联，则机箱会将数据包分类至该实例。对于桥接组成员接口（在透明模式或路由模式下）、内联集或被动接口，此方法用于始终与数据包进行分类。
- 唯一 MAC 地址 - 机箱将自动生成包括共享接口在内的所有接口的唯一 MAC 地址。如果多个实例共享一个接口，则分类器在每个实例中使用分配给该接口的唯一 MAC 地址。上游路由器无法直接路由至不具有唯一MAC地址的实例。在应用内配置每个接口时，您也可以手动设置MAC地址。

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

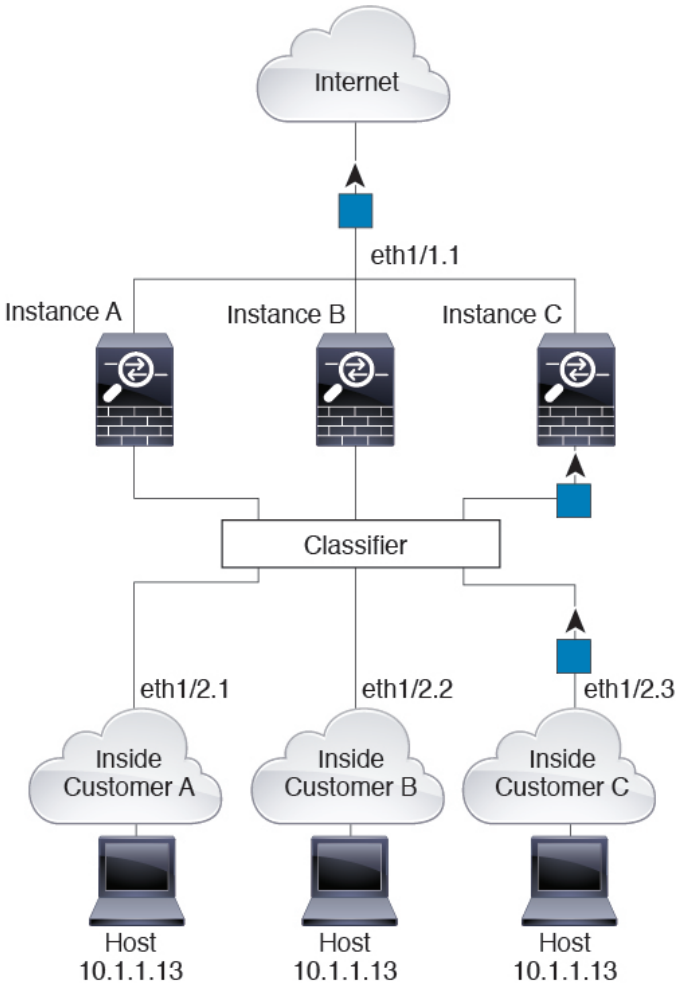
下图显示共享外部接口的多个实例。因为实例 C 包含路由器将数据包发送到的 MAC 地址，因此分类器会将该数据包分配至实例 C。

图 *8:* 使用 ***MAC*** 地址通过共享接口进行数据包分类



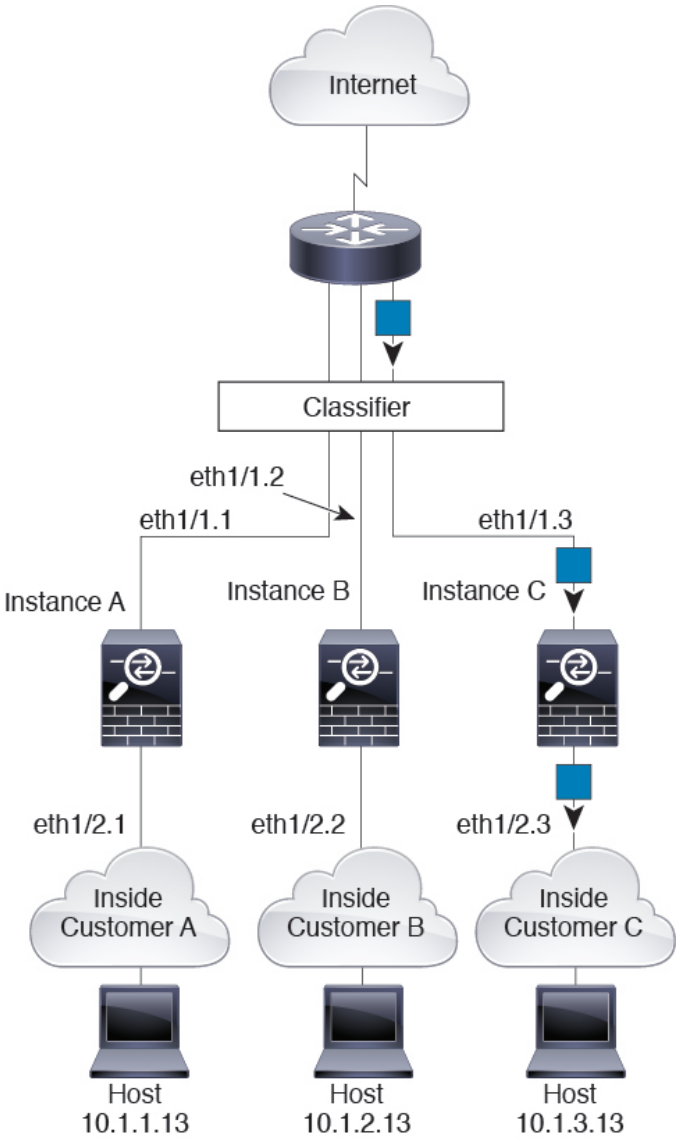
请注意，必须对所有新的传入流量加以分类，即使其来自内部网络。下图展示了实例 C 内部网络上的主机访问互联网。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

图 *9:* 来自内部网络的传入流量



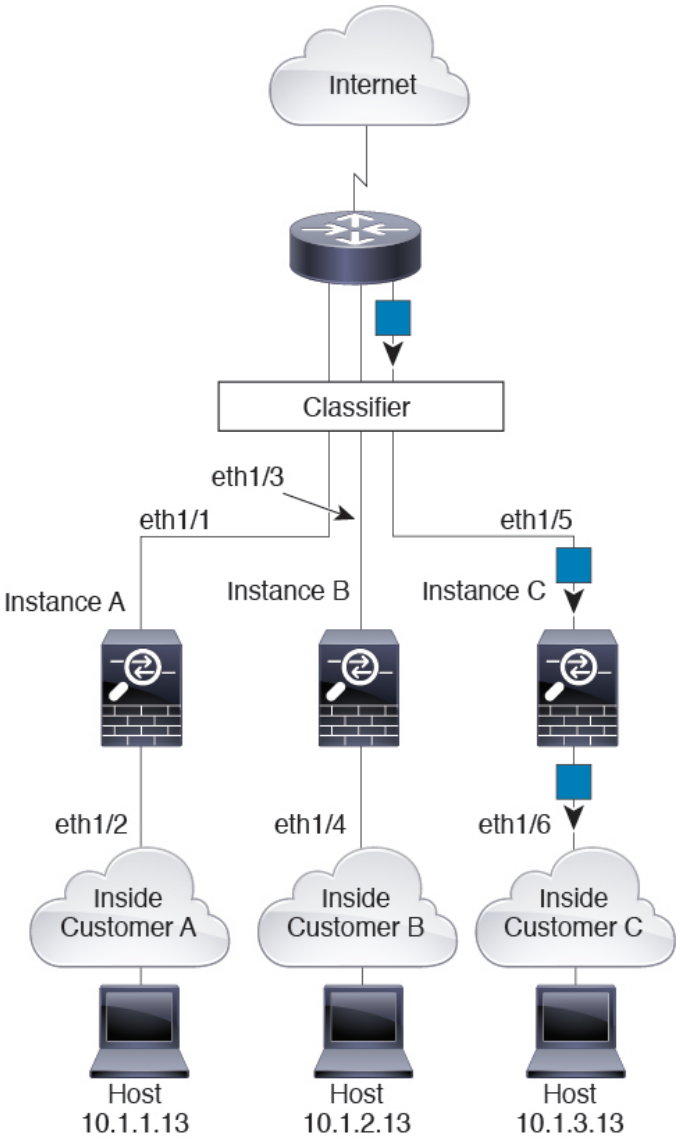
对于透明防火墙，您必须使用唯一接口。下图展示了来自互联网并以实例 C 内部网络上的主机为目标的数据包。由于传入接口是分配至实例 C 的以太网接口 1/2.3，因此分类器会将数据包分配至实例 C。

图 *10:* 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 *11: FTD* 的内联集

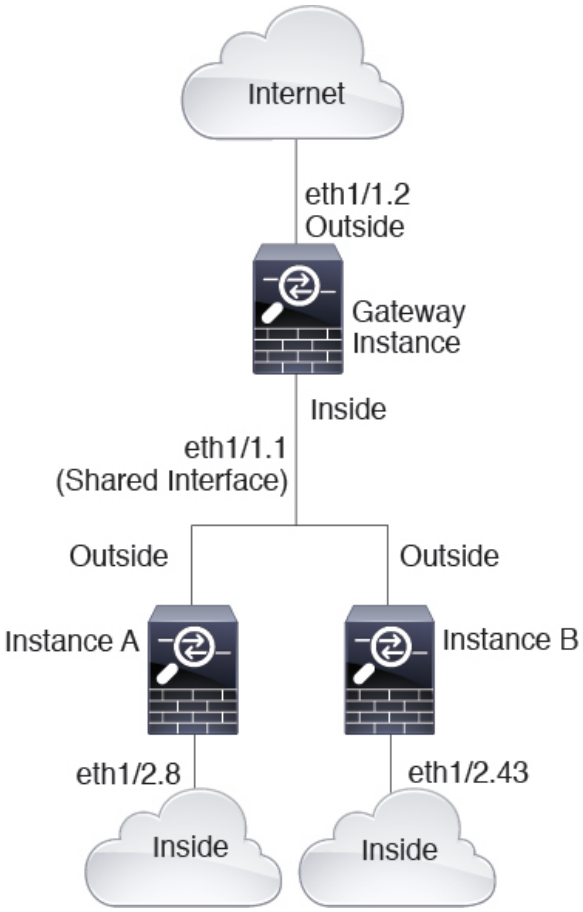


级联容器实例

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。

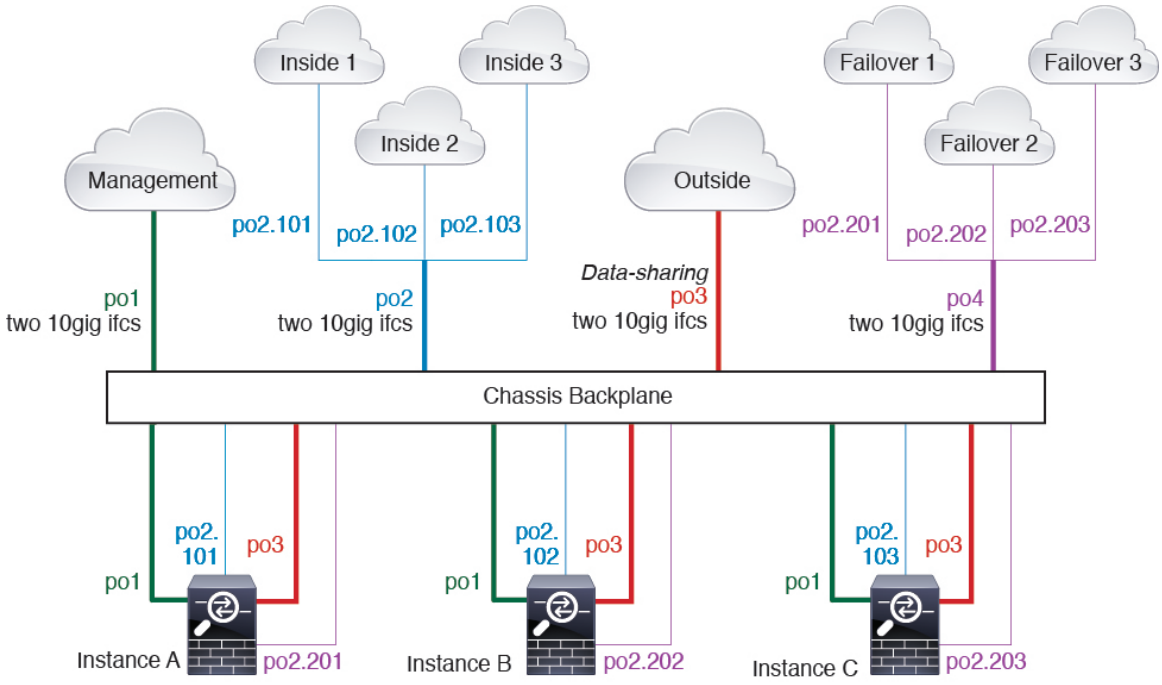
图 *12:* 级联容器实例



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，该接口都使用同一外部网络上的唯一 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 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。在极少数情况下，生成的 MAC 地址会与网络中的其他专用 MAC 地址冲突，我们建议您在应用中为接口手动设置 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。

FXOS 机箱使用以下格式生成 MAC 地址：

A2*xx.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。系统定义的前缀与已在 IDPROM 中编程的烧录 MAC 地址池中的第一个 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：

A2**4D.00***zz.zzzz*

对于前缀 1009 (03F1)，MAC 地址为：

A2**F1.03***zz.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 240 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 176 页。

多实例功能的性能扩展因素

计算平台的最大吞吐量（连接数、VPN 会话数和 TLS 代理会话数）是为了得出本地实例的内存和 CPU 使用情况（此值显示在 **show resource usage** 中）。如果使用多个实例，则需要根据分配给实例的 CPU 核心百分比来计算吞吐量。例如，如果使用具有 50% 核心的容器实例，则最初应计算 50% 的吞吐量。此外，尽管扩展可能会因为您的网络而更好或更差，但容器实例可用的吞吐量可能低于本地实例可用的吞吐量。

有关计算实例吞吐量的详细说明，请参阅https://www.cisco.com/c/en/us/products/collateral/security/firewalls/white-paper-c11-744750.html。

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。

有关详细要求，请参阅高可用性的要求和前提条件，第 239 页和添加高可用性对，第 273 页。

容器实例和集群

您可以每个安全模块/引擎各使用一个容器实例创建容器实例集群。有关详细要求，请参阅群集要求和必备条件，第 235 页。

逻辑设备的要求和必备条件

有关要求和必备条件，请参阅以下章节。

硬件和软件组合的要求与前提条件

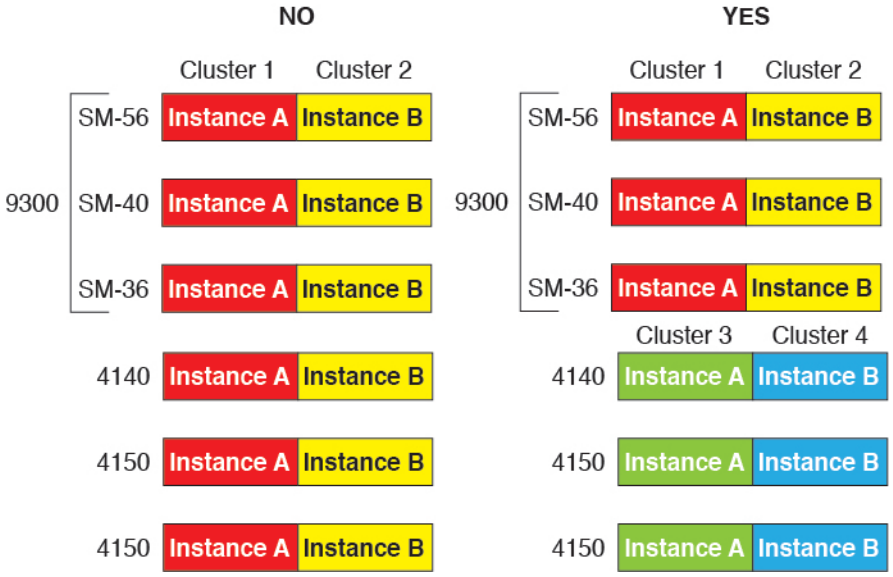
Firepower 4100/9300支持多种型号、安全模块、应用类型以及高可用性和可扩展性功能。请参阅以下要求，了解允许的组合。

Firepower 9300 的要求

Firepower 9300 包括 3 个安全模块插槽和多种类型的安全模块。请参阅以下要求：

- 安全模块类型 - 您可以在 Firepower 9300 中安装不同类型的模块。例如，您可以将 SM-36 作为模块 1、SM-40 作为模块 2、SM-44 作为模块 3 安装。

- 本地和容器实例 - 在安全模块上安装容器实例时，该模块只能支持其他容器实例。本地实例将使用模块的所有资源，因此只能在模块上安装一个本地实例。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。例如，您可以在模块 1 和模块 2 上安装本地实例，但在模块 3 上安装容器实例。
- 本地实例 集群 - 集群中的所有安全模块（无论是机箱内还是机箱间）都必须为同一类型。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。例如，您可以在机箱 1 中安装 2 个 SM-36，在机箱 2 中安装 3 个 SM-36。 如果在同一机箱中安装了 1 个 SM-24 和 2 个 SM-36，则无法使用集群。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，您可以使用 Firepower 9300 SM-56、SM-40 和 SM-36 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



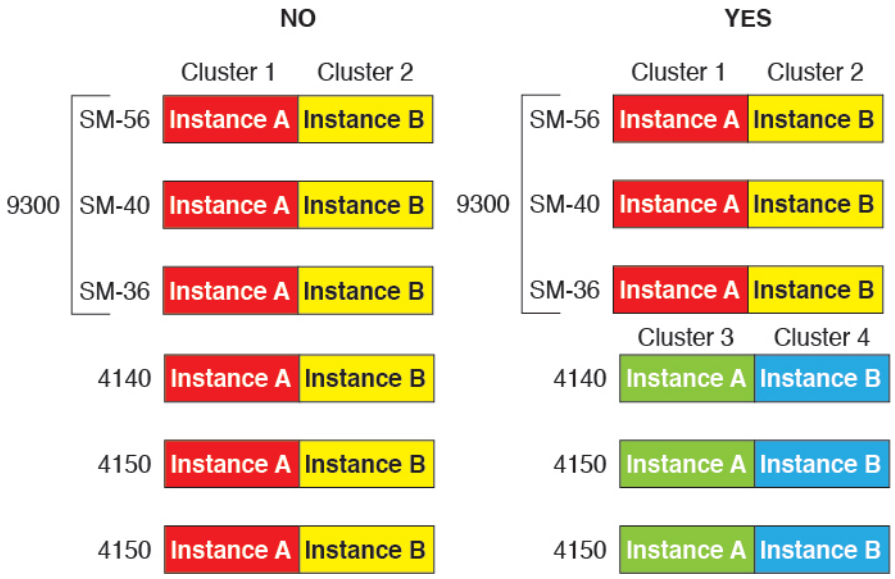
- 高可用性 - 仅在 Firepower 9300 上的同类模块间支持高可用性。 但是，这两个机箱可以包含混合模块。例如，每个机箱都设有 SM-36、SM-40 和 SM-44。可以在 SM-36 模块之间、SM-40 模块之间和 SM-44 模块之间创建高可用性对。
- ASA 和 FTD 应用类型 - 您可以在机箱中的独立模块上安装不同类型的应用。例如，您可以在模块 1 和模块 2 上安装 ASA，在模块 3 上安装 FTD。
- ASA 或 FTD 版本 - 您可以在单独的模块上运行不同版本的应用实例类型，或在同一模块上运行单独的容器实例。例如，您可以在模块 1 上安装 FTD 6.3，在模块 2 上安装 FTD 6.4，在模块 3 上安装 FTD 6.5。

Firepower 4100 的要求

Firepower 4100 有多个型号。请参阅以下要求：

- 本地和容器实例 - 在 Firepower 4100 上安装容器实例时，该设备只能支持其他容器实例。本地实例将使用设备的所有资源，因此只能在设备上安装一个本地实例。

- 本地实例 集群 - 集群内的所有机箱都必须为同一型号。
- 容器实例集群 - 您可以使用不同型号类型上的实例创建集群。例如，可以使用 Firepower 4140 和 4150 上的实例创建集群。但是，不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。



- 高可用性 - 仅在同类模块间支持高可用性。
- ASA 和 FTD 应用类型 - Firepower 4100 只能运行一种应用类型。
- FTD 容器实例版本 - 您可以在同一模块上将不同版本的 FTD 作为单独的容器实例运行。

群集要求和必备条件

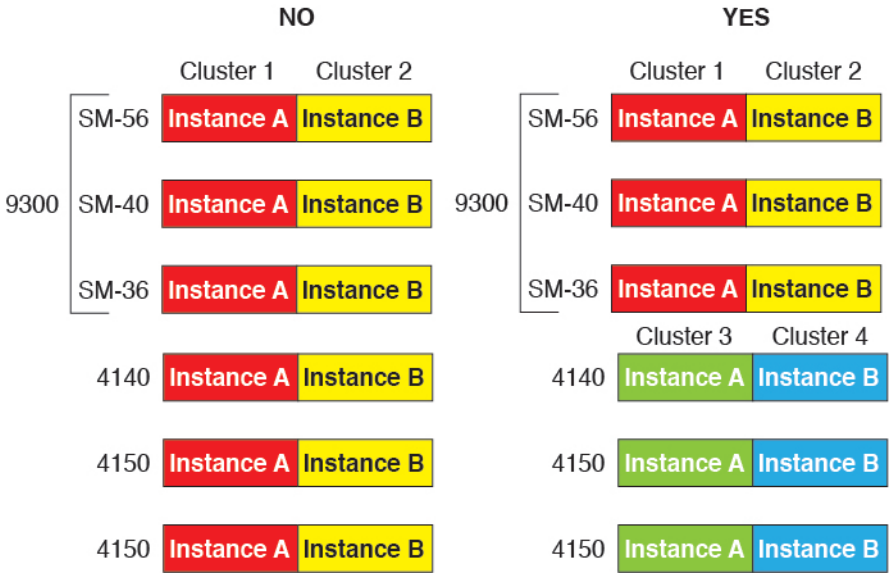
群集型号支持

- Firepower 9300 上的 ASA - 最多 16 个模块。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。请注意，机箱中的所有模块都必须属于该集群。支持机箱内、机箱间和站点间群集。
- Firepower 4100 系列 上的 ASA - 最多 16 个机箱。支持机箱间和站点间群集。
- FTD在使用 FMC 的 Firepower 9300 上 - 6 个模块。例如，您可以在 3 个机箱中使用 2 个模块，或者在 2 个机箱中使用 3 个模块，或者最多提供 6 个模块的任意组合。请注意，机箱中的所有模块都必须属于该集群。支持机箱内和机箱间群集。
- FTD在使用 FMC 的 Firepower 4100 系列 上 - 最多 6 个机箱。支持机箱间群集。
- Radware DefensePro - 对于包含 ASA 的机箱内群集受支持。
- Radware DefensePro - 支持包含 FTD的机箱内群集。 不支持多实例集群。

集群硬件和软件要求

集群中的所有机箱：

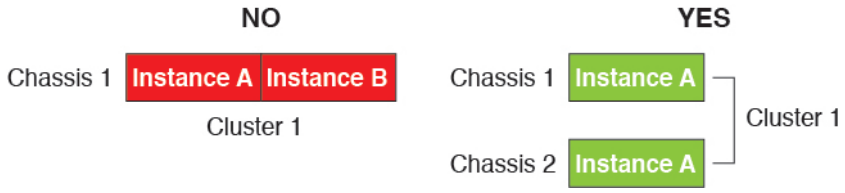
- 本地实例集群 - 对于 Firepower 4100 系列：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。例如，如果使用集群，则 Firepower 9300 中的所有模块都必须是 SM-40s。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 容器实例集群 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-40 和 SM-36 上的实例创建集群。或者，可以在 Firepower 4140 和 4150 上创建集群。



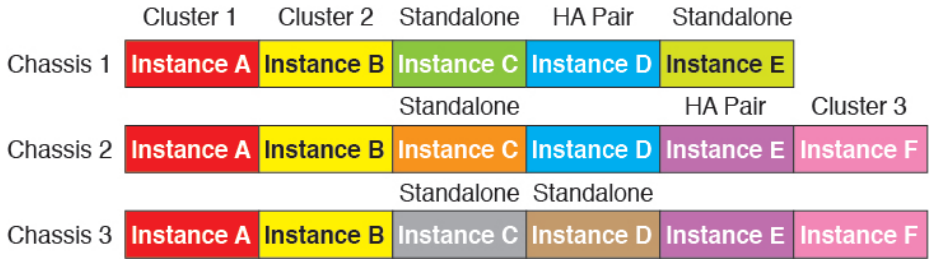
- 除进行映像升级外，必须运行完全相同的 FXOS 软件。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨区以太网通道中。请注意，所有数据接口必须是机箱间集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从数据节点开始，到控制节点结束。
- 必须使用同一台 NTP 服务器。 对于 Firepower 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。数据节点没有额外的成本。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。

多实例集群要求

- 无内部安全模块/引擎集群 - 对于给定集群，只能在每个安全模块/引擎中使用单个容器实例。如果 2 个容器实例在同一模块上运行，则不能将其添加到同一集群。



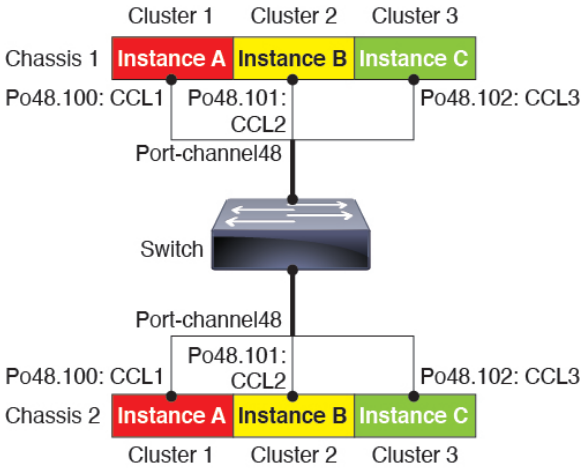
- 混合和匹配集群和独立实例 - 并非安全模块/引擎上的所有容器实例都需要属于集群。可以将某些实例用作独立节点或高可用性节点。还可以在同一安全模块/引擎上使用单独的实例来创建多个集群。



- Firepower 9300 中的所有 3 个模块都必须属于集群 - 对于 Firepower 9300，集群要求所有 3 个模块上都有一个容器实例。例如，不能使用模块 1 和 2 上的实例来创建集群，然后在模块 3 中使用本地实例。

- 匹配资源配置文件 - 建议集群中的每个节点都使用相同的资源配置文件属性；但是，在将集群节点更改为使用其他资源配置文件或使用不同型号时，允许使用不匹配的资源。

- 专用集群控制链路 - 对于机箱间集群，每个集群都需要专用的集群控制链路。例如，每个集群可以在同一集群类型 EtherChannel 上使用单独的子接口，也可以使用单独的 Etherchannel。



- 无共享接口 - 集群不支持共享类型接口。但是，多个集群可以使用相同的管理接口和事件接口。
- 无子接口 - 多实例集群无法使用 FXOS 定义的 VLAN 子接口。集群控制链路例外，它可以使用集群 EtherChannel 的子接口。
- 混合机箱型号 - 建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。例如，您可以使用 Firepower 9300 SM-56、SM-40 和 SM-36 上的实例创建集群。或者，可以在 Firepower 4140 和 4150 上创建集群。

- 最多 6 个节点 - 在一个集群中最多可以使用六个容器实例。

机箱间群集交换机必备条件

- 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的特性，请参阅思科 FXOS 兼容性。

调整站点间群集的数据中心互联

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：

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

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)）。

高可用性的要求和前提条件

- 高可用性故障切换配置中的两个设备必须：
  - 位于单独的机箱上；不支持 Firepower 9300 的机箱内高可用性。
  - 型号相同。

- 将同一接口分配至高可用性逻辑设备。
- 拥有相同数量和类型的接口。启用高可用性之前，所有接口必须在 FXOS 中进行相同的预配置。

- 仅 Firepower 9300 上同种类型模块之间支持高可用性；但是两个机箱可以包含混合模块。例如，每个机箱都设有 SM-36、SM-40 和 SM-44。可以在 SM-36 模块之间、SM-40 模块之间和 SM-44 模块之间创建高可用性对。
- 对于容器实例，每个单元必须使用相同的资源配置文件属性。
- 有关其他高可用性系统要求，请参阅“高可用性”的应用配置指南一章。

容器实例的要求和必备条件

受支持应用类型

- 使用 FMC 的 Firepower 威胁防御

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 *19:* 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 4112	3	22	78 GB	308 GB
Firepower 4115	7	46	162 GB	308 GB
Firepower 4120	3	46	101 GB	125.6 GB
Firepower 4125	10	62	162 GB	644 GB
Firepower 4140	7	70	222 GB	311.8 GB
Firepower 4145	14	86	344 GB	608 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-40 安全模块	13	78	334 GB	1359 GB

型号	最大容器实例数	可用 **CPU** 核心	可用 **RAM**	可用磁盘空间
Firepower 9300 SM-44 安全模块	14	86	218 GB	628.4 GB
Firepower 9300 SM-48 安全模块	15	94	334 GB	1341 GB
Firepower 9300 SM-56 安全模块	18	110	334 GB	1314 GB

Firepower 管理中心系统要求

对于在 Firepower 4100 机箱或 Firepower 9300 模块上的所有情况下，由于许可实施，您必须使用相同 Firepower 管理中心 (FMC)。

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。

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使用 FMC 的 FTD。
- 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。
- 您可以在最多 16 个容器实例上启用 TLS 加密加速。
- 对于 FTD 容器实例，不支持以下功能：
  - Radware DefensePro 链路修饰器
  - FMC UCAPL/CC 模式

- 到硬件的流负载分流

集群准则和限制

机箱间集群的交换机

- 确保连接的交换机与集群数据接口和集群控制链路接口的 MTU 匹配。您应将集群控制链路接口 MTU 配置为比数据接口 MTU 至少高 100 字节，因此请确保适当配置集群控制链路连接的交换机。由于集群控制链路流量包括数据包转发，因此集群控制链路需要能够容纳完整大小的数据包以及集群流量开销。
- 对于 Cisco IOS XR 系统，如果要设置非默认 MTU，请将 IOS 接口 MTU 设置为比集群设备 MTU 高 14 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 IOS *IPv4* MTU 匹配。Cisco Catalyst 和 Cisco Nexus 交换机不需要进行这种调整。
- 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。
- 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，使跨区以太网通道具有更高兼容性。
- 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：

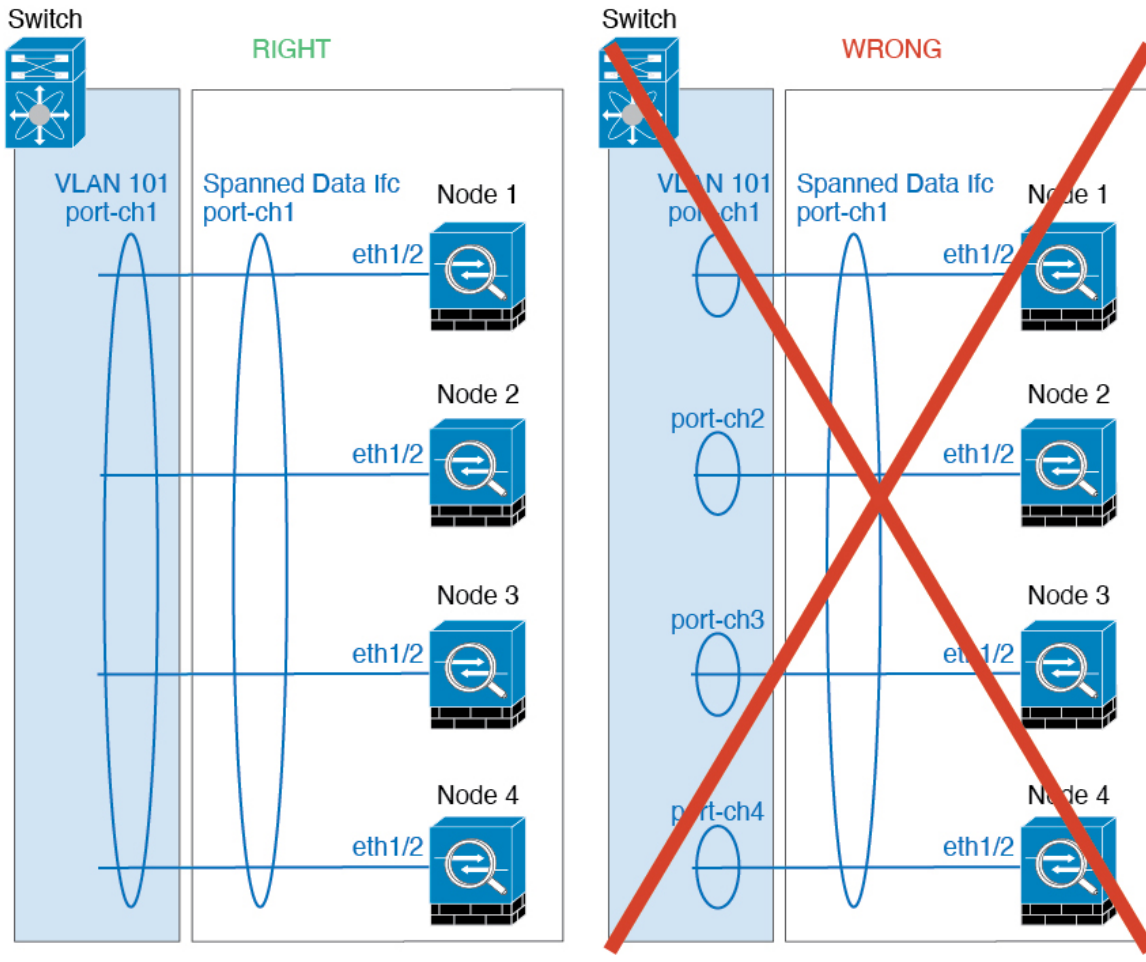
  router(config)# **port-channel** *id* **hash-distribution fixed**

  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。

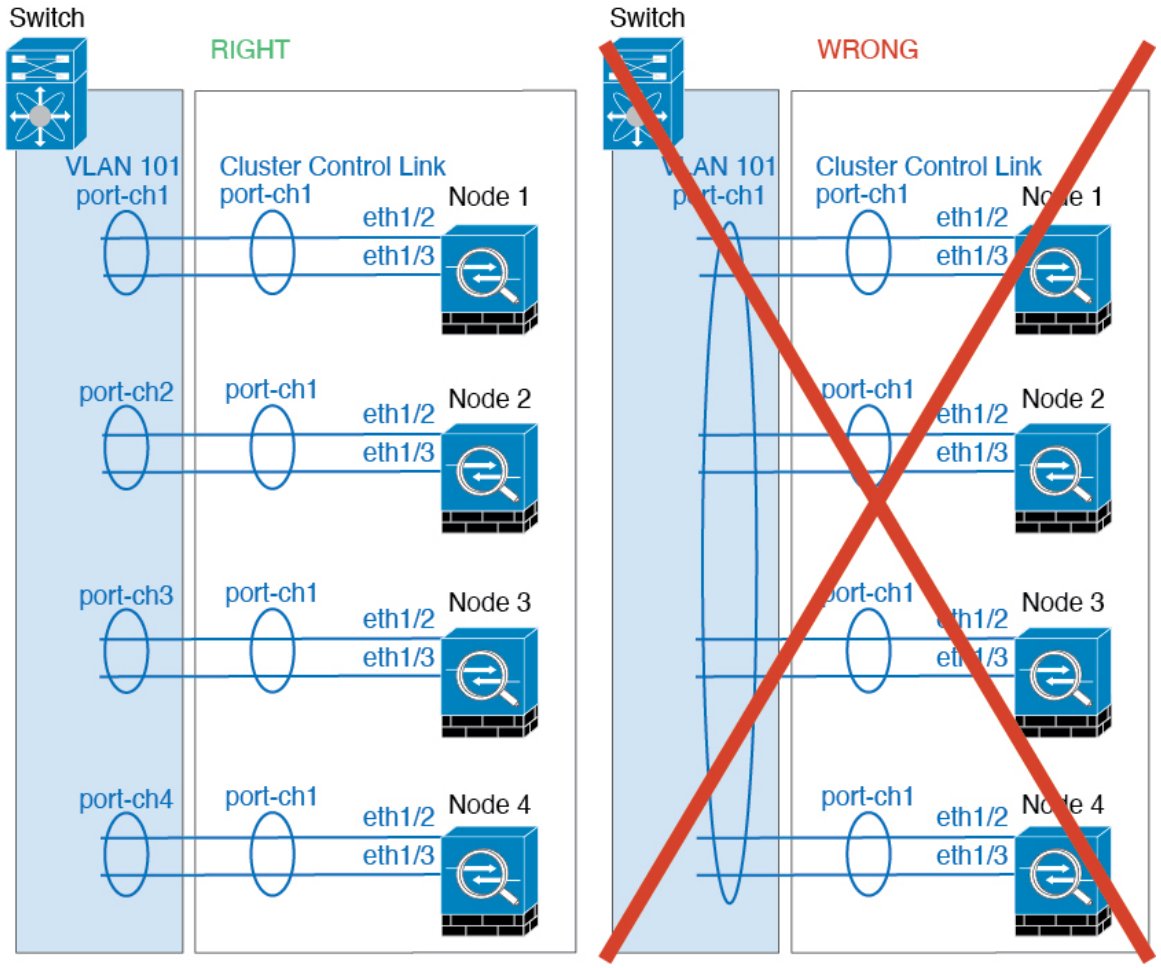
- Firepower 4100/9300 集群支持 LACP 正常融合。因此，，您可以在连接的思科 Nexus 交换机上启用 LACP 正常融合。
- 当发现交换机上跨区以太网通道的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为快速。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

机箱间集群的 EtherChannel

- 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，如果跨堆栈连接集群设备 EtherChannel，则当控制设备交换机关闭时，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 - 请务必为跨区以太网通道和设备本地 EtherChannel 适当地配置交换机。
  - 跨区以太网通道 - 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。
- ASA 不会加密集群控制链路上转发的数据流量，因为它是专用链接，即使在数据中心互连 (DCI) 上使用也是如此。如果您使用重叠传输虚拟化 (OTV) 或将集群控制链路扩展到本地管理域外部，可以在边界路由器（例如基于 OTV 的 802.1AE MacSec）上配置加密。
- 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，给定连接的连接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，则远程站点节点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，目标 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 地址目标。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。
- 对于透明模式，如果集群连接到 HSRP 路由器，则必须在 ASA。当邻接路由器使用 HSRP 时，发往 HSRP IP 地址的流量将发送到 HSRP MAC 地址，但返回流量将来自 HSRP 对中特定路由器接口的 MAC 地址。因此，ASA MAC 地址表通常仅在 HSRP IP 地址的 ASA ARP 表条目到期时更新，并且 ASA 发送 ARP 请求并接收应答。由于 ASA 的 ARP 表条目默认在 14400 秒后到期，但 MAC 地址表条目默认在 300 秒后到期，因此需要添加静态 MAC 地址条目来避免 MAC 地址表到期流量丢弃。
- 对于使用跨区以太网通道的路由模式，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节点。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。
- 如果使用连接到跨区以太网通道接口的 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。
- 对于解密的 TLS/SSL 连接，解密状态不同步，如果连接所有者失败，则解密的连接将重置。需要建立新连接以连通新设备。未解密的连接（它们匹配“不解密”规则）不受影响，并且可以正确复制。

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 273 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。在具有多个安全模块的 Firepower 9300 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，然后将映像下载到 Firepower 4100/9300 机箱。

  注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

- 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，此管理接口不同于仅用于机箱管理的机箱管理端口（在 FXOS 中，可能会看到该接口显示为 MGMT、management0 或其他类似名称）。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 2 设置应用实例映像版本。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id*始终为 1；对于 Firepower 9300，则始终为 1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) 创建应用实例。

enter app-instance asa *device_name*

device_name 可介于 1 至 64 个字符之间。在对此实例创建逻辑设备时，您将使用此设备名称。

示例：

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) 设置 ASA 映像版本。

set startup-version *version*

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 3 创建逻辑设备。

enter logical-device *device_name* **asa** *slot_id* **standalone**

使用与您之前添加的应用实例相同的 *device_name*。

示例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

步骤 4 向逻辑设备分配管理和数据接口。对各个接口重复此步骤。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name* - 由 Firepower 4100/9300 机箱管理引擎使用；它不是在 ASA 配置中使用的接口名称。
- *description* - 在含有空格的短语两侧使用引号 (")。

管理接口与机箱管理端口不同。稍后您需要在 ASA 上启用和配置数据接口，包括设置 IP 地址。

示例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

步骤 5 配置管理引导程序信息。

a) 创建引导程序对象。

create mgmt-bootstrap asa

示例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定管理员并启用密码。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 配置 IPv4 管理接口设置。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 配置 IPv6 管理接口设置。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 6 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
    Native                   Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
    Container   Default-Small Not Applicable  None
```

步骤 7 请参阅 ASA 配置指南，以开始配置安全策略。

示例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

为 FMC 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。在具有多个安全模块的 Firepower 9300 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，然后将映像下载到 Firepower 4100/9300 机箱。

  注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

- 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，此管理接口不同于仅用于机箱管理的机箱管理端口（在 FXOS 中，可能会看到该接口显示为 MGMT、management0 或其他类似名称）。
- 您可以稍后从数据接口启用管理；但必须将管理接口分配给逻辑设备，即使您不打算在启用数据管理后使用该接口。有关详细信息，请参阅 FTD 命令参考中的 **configure network management-data-interface** 命令。
- 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 186 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 176 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。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 346 页。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - FMC 您选择的 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址

- FTD 主机名和域名

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 2 接受想要使用的Firepower威胁防御版本的最终用户许可协议。如果尚未接受此版本的EULA，则只需执行此步骤即可。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 将范围设置为映像版本。

scope app ftd *application_version*

示例：

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) 接受许可协议。

accept-license-agreement

示例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
```

```
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

d) 保存配置。

commit-buffer

示例：

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

e) 退出到安全服务模式。

exit

示例：

```
Firepower /ssa/app # exit
Firepower /ssa #
```

步骤 3 设置应用实例参数，包括映像版本。

a) 对于容器实例，查看可用资源配置文件。要添加配置文件，请参阅为容器实例添加资源配置文件，第 176 页。

show resource-profile

请注意您想要使用的配置文件名称。

示例：

```
Firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
 Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
bronze             N/A        N/A          No         all
      6            N/A No              Custom       low end device
silver 1           N/A        N/A          No         all
      8            N/A No              Custom       mid-level
```

b) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id*始终为 1；对于 Firepower 9300，则始终为 1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) 创建应用实例。

enter app-instance ftd *device_name*

device_name 可介于 1 至 64 个字符之间。在对此实例创建逻辑设备时，您将使用此设备名称。

示例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

d) 对于容器实例，请将应用实例类型设置为容器。

set deploy-type container

容器实例使用部分安全模块/引擎资源，因此可以安装多个容器实例。本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此仅可安装一个本地实例。

保存配置后，无法更改实例类型。默认类型为**native**。

示例：

```
Firepower /ssa/slot/app-instance* # set deploy-type container
```

e) 对于容器实例，设置资源配置文件。

set resource-profile-name *name*

该配置文件名称必须已存在。

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。

示例：

```
Firepower /ssa/slot/app-instance* # set resource-profile-name bronze
```

f) 设置 Firepower 威胁防御映像版本。

set startup-version *version*

输入您接受 EULA 时在此程序中事先记录的版本号。

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

g) 对于容器实例，请启用或禁用 TLS 加密加速。

enter hw-crypto

set admin-state {**enabled** | **disabled**}

exit

此设置在硬件中启用TLS加密加速，并提高某些类型流量的性能。默认情况下启用此功能。您最多可以为每个安全模块的 16 个实例启用 TLS 加密加速。本地实例不支持此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。请注意，版本 2 指的是 FXOS 2.7 及更高版本中使用的 TLS 加密加速类型。

示例：

```
Firepower /ssa/slot/app-instance* # enter hw-crypto
Firepower /ssa/slot/app-instance/hw-crypto* # set admin-state enabled
Firepower /ssa/slot/app-instance/hw-crypto* # exit
Firepower /ssa/slot/app-instance* # commit-buffer
Firepower /ssa/slot/app-instance # show hw-crypto
Hardware Crypto:
    Admin State           Hardware Crypto Size       Hardware Crypto Version
    ----------            -------------------------- -------------------------------

    enabled                    40%                                 2
```

h) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

i) （可选） 创建适用于 Firepower 4110 或 4120 的 Radware DefensePro 实例，要求在创建逻辑设备之前创建应用实例（容器实例不支持 Radware DefensePro）。

enter app-instance vdp *device_name*

exit

设置 *device_name*以匹配 Firepower 威胁防御应用实例。完成逻辑设备配置后，您必须在具有 Firepower 威胁防御逻辑设备的服务链中继续配置 Radware DefensePro 修饰器。请参阅在独立逻辑设备上配置 Radware DefensePro，第 310 页，从步骤 4 开始。

示例：

```
Firepower /ssa/slot* # enter app-instance vdp FTD1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

j) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 4 创建逻辑设备。

enter logical-device *device_name* **ftd** *slot_id* **standalone**

使用与您之前添加的应用实例相同的 *device_name*。

示例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

步骤 5 向逻辑设备分配管理和数据接口。对各个接口重复此步骤。

create external-port-link *name interface_id* **ftd**

set description *description*

exit

- *name* - 由 Firepower 4100/9300 机箱管理引擎使用；它不是在 Firepower 威胁防御配置中使用的接口名称。
- *description* - 在含有空格的短语两侧使用引号 (")。

管理接口与机箱管理端口不同。稍后您需要在 FMC 中启用和配置数据接口，包括设置 IP 地址。

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。

示例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
```

```
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

步骤 6 启用链路状态同步。

set link state sync enabled

机箱现在可以将 FTD 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 FTD 应用接口管理状态。如果没有从 FTD 同步，数据接口可能在 FTD 应用完全上线之前处于“Up”物理状态，或者在您启动FTD关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 FTD 可以处理流量之前开始向 FTD 发送流量。

该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。此功能不会影响非数据接口（例如管理接口或集群接口）。

当您启用 FTD 链路状态同步时，FXOS 中接口的**服务状态**将与 FTD 中该接口的管理状态同步。例如，如果关闭 FTD 中的接口，“服务状态”将显示为“已禁用”。如果关闭 FTD 应用，所有接口将显示为“已禁用”。对于硬件旁路接口，以管理方式关闭FTD中的接口会将“服务状态”设置为“已禁用”；但关闭FTD应用或执行其他机箱级别的关闭（包括关闭电源）会使接口对保持“已启用”状态。

如果禁用 FTD 链路状态同步，则“服务状态”将始终显示为“已启用”。

注释 集群、容器实例或具有 Radware vDP 修饰器的 FTD 不支持此功能。此外，ASA 也不支持此功能。

要查看接口的当前服务状态以及上次关闭原因，请输入 **show interface expand detail** 命令。

示例：

```
Firepower /ssa/logical-device* # set link state sync enabled
Firepower /ssa/logical-device* # scope eth-uplink
Firepower /eth-uplink* # scope fabric a
Firepower /eth-uplink/fabric* # show interface expand detail
Interface:
    Port Name: Ethernet1/2
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: Yes
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Service State: Enabled
    Last Service State Down Reason: None
    Allowed Vlan: All
    Network Control Policy: default
```

```
    Current Task:
<...>
```

步骤 7 配置管理引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建引导程序对象。

create mgmt-bootstrap ftd

示例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 对于本地实例，请将管理器设置为 FMC。

enter bootstrap-key MANAGEMENT_TYPE

set value FMC

exit

本地实例还支持 FDM 作为管理器。部署逻辑设备后，无法更改管理器类型。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key MANAGEMENT_TYPE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value FMC
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定管理 Firepower 管理中心的 IP 地址或主机名或 NAT ID：

设置以下其中一项：

- **enter bootstrap-key FIREPOWER_MANAGER_IP**

  set value *IP_address*

  exit

- **enter bootstrap-key FQDN**

  set value *fmc_hostname*

  exit

- **enter bootstrap-key NAT_ID**

  set value *nat_id*

  exit

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。您可以将长度介于 1 到 37 个字符之间的任意文本字符串指定为 NAT ID。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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 指定设备和 Firepower 管理中心要共享的密钥。可以为此密钥选择介于 1 至 37 个字符之间的任何密码；添加 FTD 时，需要在 FMC 上输入相同的密钥。

create bootstrap-key-secret REGISTRATION_KEY

set value

输入值：*registration_key*

确认值：*registration_key*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 指定管理员密码。此密码供管理员用户用于 CLI 访问。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) 指定完全限定主机名。

create bootstrap-key FQDN

set value *fqdn*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd1.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 指定 DNS 服务器列表（用逗号隔开）。

create bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

例如，如果指定 FMC 主机名，则 FTD 使用 DNS。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) 指定搜索域列表（用逗号隔开）。

create bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

j) （可选）对于容器实例，允许 FTD SSH 会话专家模式。专家模式提供 FTD shell 访问权限以确保实现高级故障排除。

create bootstrap-key PERMIT_EXPERT_MODE

set value {**yes** | **no**}

exit

- **yes**- 拥有直接从 SSH 会话访问此容器实例的权限的用户可以输入专家模式。
- **no**- 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。

默认情况下，对于容器实例，只有从 FXOS CLI 访问 FTD CLI 的用户可以进入专家模式。此限制仅用于容器实例，以增强实例之间的隔离。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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

k) 配置 IPv4 管理接口设置。

create ipv4 *slot_id* **firepower**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

l) 配置 IPv6 管理接口设置。

create ipv6 *slot_id* **firepower**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

m) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 8 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                    9.12.1
    Native                    Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49        6.4.0.49
    Container   Default-Small Not Applicable  None
```

步骤 9 请参阅 FMC 配置指南，将 FTD 添加为受管设备，并开始配置安全策略。

示例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.3.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.3.0
```

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: juniorwindowpane
Confirm the value: juniorwindowpane
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

为 FDM 添加独立的 Firepower 威胁防御

可以将FDM与本地实例结合使用。不支持容器实例。独立逻辑设备可单独使用，也可在高可用性对中使用。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像下载到 Firepower 4100/9300 机箱。

注释 对于 Firepower 9300，可以在机箱中的独立模块上安装不同类型的应用（ASA 和 FTD）。还可以在独立模块上运行一种应用实例的不同版本。

- 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，此管理接口不同于仅用于机箱管理的机箱管理端口（在 FXOS 中，可能会看到该接口显示为 MGMT、management0 或其他类似名称）。
- 您还必须至少配置一个数据类型的接口。
- 收集以下信息：
  - 此设备的接口 ID
  - 管理接口 IP 地址和网络掩码
  - 网关 IP 地址
  - DNS 服务器 IP 地址
  - FTD 主机名和域名

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 2 接受想要使用的 Firepower 威胁防御版本的最终用户许可协议。如果尚未接受此版本的 EULA，则只需执行此步骤即可。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

```
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 将范围设置为映像版本。

scope app ftd *application_version*

示例：

```
Firepower /ssa # scope app ftd 6.5.0
Firepower /ssa/app #
```

c) 接受许可协议。

accept-license-agreement

示例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

d) 保存配置。

commit-buffer

示例：

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

e) 退出到安全服务模式。

exit

示例：

```
Firepower /ssa/app # exit
Firepower /ssa #
```

步骤 3 设置应用实例映像版本。

a) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id*始终为 1；对于 Firepower 9300，则始终为 1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

b) 创建应用实例。

enter app-instance ftd *device_name*

device_name 可介于 1 至 64 个字符之间。在对此实例创建逻辑设备时，您将使用此设备名称。

示例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

c) 设置 Firepower 威胁防御映像版本。

set startup-version *version*

输入您接受 EULA 时在此程序中事先记录的版本号。

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.5.0
```

d) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

e) （可选） 创建适用于 Firepower 4110 或 4120 的 Radware DefensePro实例，要求在创建逻辑设备之前创建应用实例。

enter app-instance vdp *device_name*

exit

设置 *device_name* 以匹配 Firepower 威胁防御应用实例。完成逻辑设备配置后，您必须在具有 Firepower 威胁防御逻辑设备的服务链中继续配置 Radware DefensePro 修饰器。请参阅在独立逻辑设备上配置 Radware DefensePro，第 310 页，从步骤 4 开始。

示例：

```
Firepower /ssa/slot* # enter app-instance vdp FTD1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 6.5.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 4 创建逻辑设备。

enter logical-device *device_name* **ftd** *slot_id* **standalone**

使用与您之前添加的应用实例相同的 *device_name*。

示例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* #
```

步骤 5 向逻辑设备分配管理和数据接口。对各个接口重复此步骤。

create external-port-link *name interface_id* **ftd**

set description *description*

exit

- *name* - 由 Firepower 4100/9300 机箱管理引擎使用；它不是在 Firepower 威胁防御配置中使用的接口名称。
- *description* - 在含有空格的短语两侧使用引号 (")。

管理接口与机箱管理端口不同。稍后需要在 FDM 中启用和配置数据接口，包括设置 IP 地址。

示例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

步骤 6 启用链路状态同步。

set link state sync enabled

机箱现在可以将 FTD 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 FTD 应用接口管理状态。如果没有从 FTD 同步，数据接口可能在 FTD 应用完全上线之前处于“Up”物理状态，或者在您启动FTD关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 FTD 可以处理流量之前开始向 FTD 发送流量。

该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。此功能不会影响非数据接口（例如管理接口或集群接口）。

当您启用 FTD 链路状态同步时，FXOS 中接口的**服务状态**将与 FTD 中此接口的管理状态同步。例如，如果关闭 FTD 中的接口，“服务状态”将显示为“已禁用”。如果关闭 FTD 应用，所有接口将显示为“已禁用”。对于硬件旁路接口，以管理方式关闭FTD中的接口会将“服务状态”设置为“已禁用”；但关闭FTD应用或执行其他机箱级别的关闭（包括关闭电源）会使接口对保持“已启用”状态。

如果禁用 FTD 链路状态同步，则“服务状态”将始终显示为“已启用”。

注释 集群、容器实例或具有 Radware vDP 修饰器的 FTD 不支持此功能。此外，ASA 也不支持此功能。

要查看接口的当前服务状态以及上次关闭原因，请输入 **show interface expand detail** 命令。

示例：

```
Firepower /ssa/logical-device* # set link state sync enabled
Firepower /ssa/logical-device* # scope eth-uplink
Firepower /eth-uplink* # scope fabric a
Firepower /eth-uplink/fabric* # show interface expand detail
Interface:
    Port Name: Ethernet1/2
    User Label:
    Port Type: Data
    Admin State: Enabled
    Oper State: Up
    State Reason:
    flow control policy: default
    Auto negotiation: Yes
    Admin Speed: 1 Gbps
    Oper Speed: 1 Gbps
    Admin Duplex: Full Duplex
    Oper Duplex: Full Duplex
```

```
    Ethernet Link Profile name: default
    Oper Ethernet Link Profile name: fabric/lan/eth-link-prof-default
    Udld Oper State: Admin Disabled
    Inline Pair Admin State: Enabled
    Inline Pair Peer Port Name:
    Service State: Enabled
    Last Service State Down Reason: None
    Allowed Vlan: All
    Network Control Policy: default
    Current Task:
<...>
```

步骤 7 配置管理引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建引导程序对象。

create mgmt-bootstrap ftd

示例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 对于本地实例，请将管理器设置为 FDM。

enter bootstrap-key MANAGEMENT_TYPE

set value LOCALLY_MANAGED

exit

本地实例还支持 FMC 作为管理器。部署逻辑设备后，无法更改管理器类型。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key MANAGEMENT_TYPE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定管理员密码。此密码供管理员用户用于 CLI 访问。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
```

```
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 指定完全限定主机名。

create bootstrap-key FQDN

set value *fqdn*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd1.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 指定 DNS 服务器列表（用逗号隔开）。

create bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 指定搜索域列表（用逗号隔开）。

create bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) 配置 IPv4 管理接口设置。

create ipv4 *slot_id* **firepower**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 配置 IPv6 管理接口设置。

create ipv6 *slot_id* **firepower**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 8 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                   9.12.1
    Native                   Not Applicable  None
ftd        ftd1       1          Enabled     Online           6.4.0.49       6.4.0.49
    Container   Default-Small Not Applicable  None
```

步骤 9 请参阅《 FDM 配置指南》，以开始配置安全策略。

示例

```
Firepower# scope ssa
Firepower /ssa* # scope app ftd 6.5.0
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app # exit
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd
Firepower /ssa/slot/app-instance* # set startup-version 6.5.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 ftd 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 ftd
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 ftd
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 ftd
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value ftd.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value search.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

添加高可用性对

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

请参阅高可用性的要求和前提条件，第 239 页。

过程

步骤 1 将相同的接口分配给各个逻辑设备。

步骤 2 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 3 在逻辑设备上启用高可用性。

步骤 4 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。

添加群集

通过群集，您可以将多台设备组合成单个逻辑设备。群集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 支持机箱内群集，在此，即您可以将单个机箱中的所有模块分组到一个群集中。您还可使用将多个机箱组合在一起的机箱间群集；机箱间群集是单模块设备（例如 Firepower 4100 系列）的唯一选择。

关于 Firepower 4100/9300 机箱上的群集

在 Firepower 4100/9300 机箱 上部署群集时，它执行以下操作：

- 对于本地实例群集：为设备间通信创建群集控制链路（默认情况下，使用端口通道 48）。

  对于多实例群集：您应该在一个或多个群集类型 Etherchannel 上预配置子接口；每个实例都需要自己的群集控制链路。

对于机箱内群集（仅限 Firepower 9300），此链路利用 Firepower 9300 背板进行群集通信。

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。

- 在应用中创建群集引导程序配置。

  在部署集群时，机箱管理引擎将最低引导程序配置推送到包含群集名称、群集控制链路接口及其他群集设置的每个设备。 如果您需要自定义群集环境，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 接口分配给群集。

  对于机箱内群集，跨网络接口不仅限于 EtherChannel，与机箱间群集类似。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。 对于机箱间群集，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。

- 向群集中的所有设备分配管理接口。

主设备角色和辅助设备角色

群集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

对于本地实例集群：使用端口通道 48 接口自动创建集群控制链路。

对于多实例群集：您应该在一个或多个群集类型 Etherchannel 上预配置子接口；每个实例都需要自己的群集控制链路。

对于机箱内群集，此接口未设任何成员接口。此群集类型 EtherChannel 利用 Firepower 9300 背板进行机箱内群集的群集通信。 对于机箱间群集，必须将一个或多个接口添加到 EtherChannel。

对于包含 2 个成员的机箱间群集，请勿直接将群集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，群集控制链路失效，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群集控制链路，则群集控制链路仍会对正常设备打开。

群集控制链路流量包括控制流量和数据流量。

设定机箱间群集的群集控制链路大小

如果可能，应将群集控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使群集控制链路可以处理最坏情况。

群集控制链路流量主要由状态更新和转发的数据包组成。群集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。

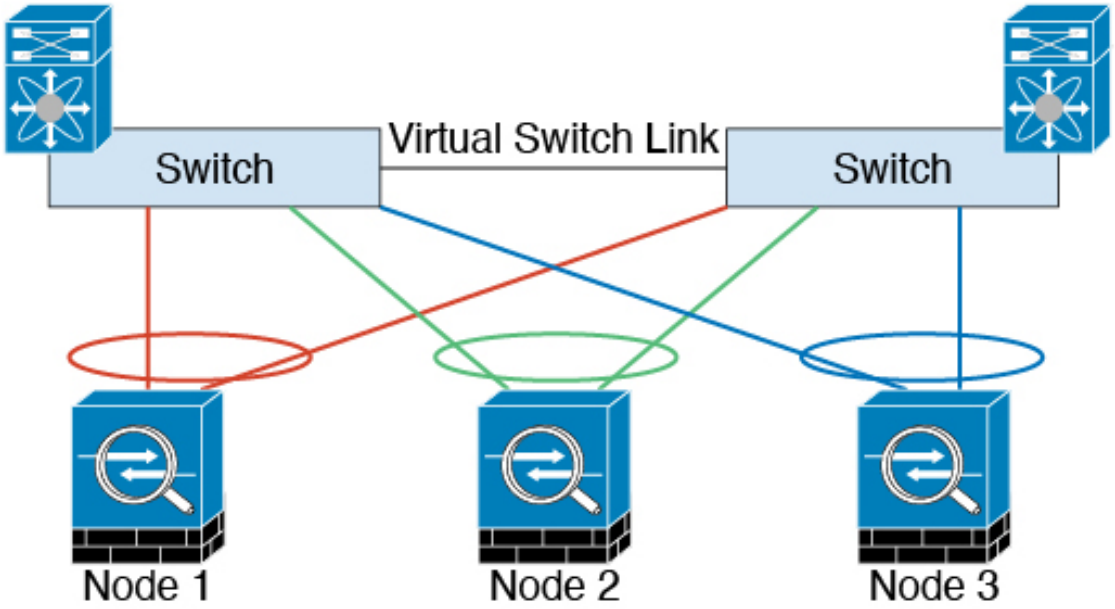
- 当成员身份更改时，群集需要对大量连接进行再均衡，因此会暂时耗用大量群集控制链路带宽。

带宽较高的群集控制链路可以帮助群集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 如果群集中存在大量不对称（再均衡）流量，应增加群集控制链路的吞吐量大小。

机箱间群集的群集控制链路冗余

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 作为群集控制链路。EtherChannel 中的所有链路都是活动链路。如果交换机是 VSS 或 vPC 的一部分，则您可以将同一个 EtherChannel 中的防火墙接口连接到 VSS 或 vPC 中单独的交换机。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。



机箱间群集的群集控制链路可靠性

为了确保群集控制链路的功能，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群集成员的兼容性。要检查延迟，请在设备之间的群集控制链路上执行 ping 操作。

群集控制链路必须可靠，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。

群集控制链路网络

Firepower 4100/9300 机箱基于机箱 ID 和插槽 ID 自动为每个设备生成群集控制链路接口 IP 地址：127.2.*chassis_id*.*slot_id*。 对于多实例集群（通常使用同一 EtherChannel 的不同 VLAN 子接口），由于 VLAN 分离，同一 IP 地址可用于不同的集群。当您部署群集时，您可以自定义此 IP 地址。群集

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。此网络与群集控制链路分隔开来。

管理接口

必须为群集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。

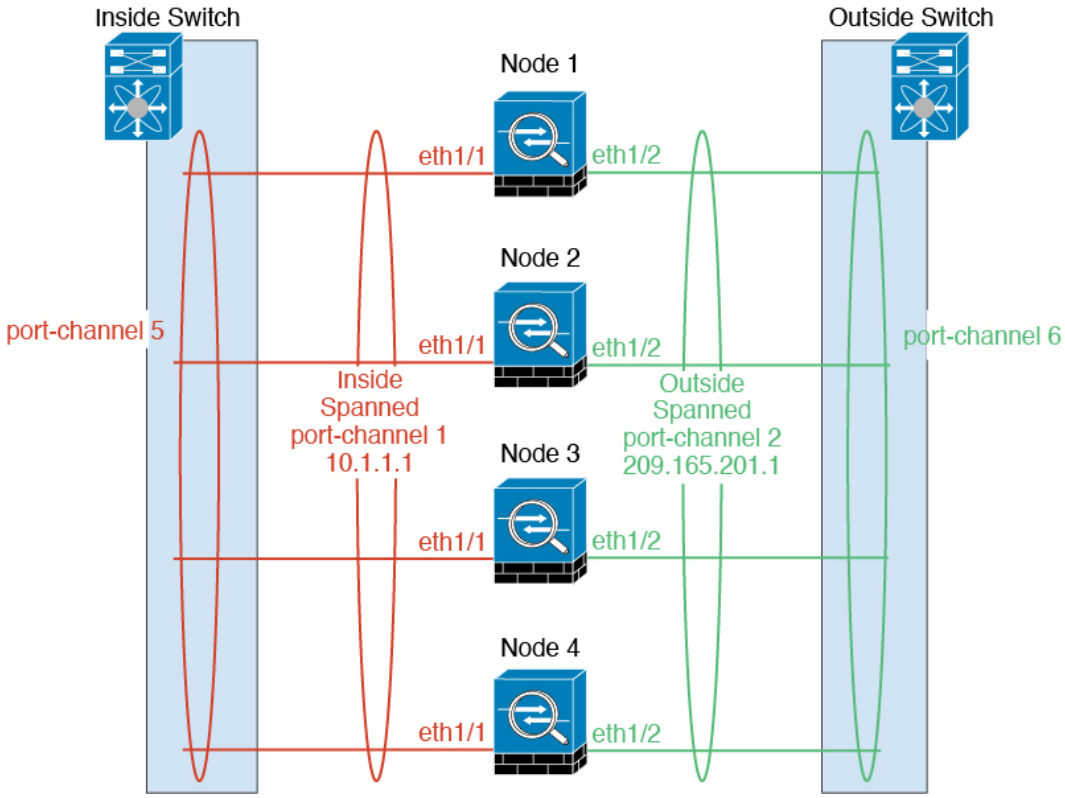
对于ASA，主群集IP地址是始终属于当前主设备的群集的固定地址。您必须配置一个地址范围，使每个设备（包括当前主设备在内）都能使用该范围内的本地地址。主群集IP地址提供对地址的统一管理访问权限；当主设备更改时，主群集IP地址将转移给新的主设备，使群集管理可以无缝衔接。本地 IP 地址用于路由，在排除故障时也非常有用。例如，可以通过连接到主群集 IP 地址来管理群集，该地址始终连接到当前主设备。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每个设备都使用本地 IP 地址来连接到服务器。

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区以太网通道。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。

对于多实例集群，每个集群都需要专用数据 Etherchannel，不能使用共享接口或 VLAN 子接口。



站点间群集

对于站点间安装，您只要遵循建议的准则即可充分发挥群集的作用。

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。集群发出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。只有使用跨区以太网通道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。

有关站点间群集的详细信息，请参阅以下各节：

- 调整数据中心互联的规模 -群集要求和必备条件， 第 235 页
- 站点间准则 -集群准则和限制， 第 242 页
- 站点间示例 -站点间群集示例， 第 334 页

添加 ASA 群集

您可以将单个 Firepower 9300 机箱添加为机箱内群集，或添加多个机箱以实现机箱间群集。 对于机箱间群集，您必须单独配置每个机箱。在一个机箱上添加群集；然后，您可以在下一个机箱上输入基本相同的设置。

创建 ASA 集群

将范围设置为映像版本。

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。

在 Firepower 9300 机箱中，必须对全部 3 个模块插槽或容器实例（每个插槽中有一个容器实例）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。

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，然后将映像上传至 Firepower 4100/9300 机箱。
- 收集以下信息：
  - 管理接口 ID、IP 地址和网络掩码
  - 网关 IP 地址

过程

步骤 1 配置接口。

步骤 2 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 3 设置应用实例参数，包括映像版本。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
```

```
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 将范围设置为映像版本。

scope app asa *application_version*

示例：

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) 将此版本设置为默认版本。

set-default

示例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

步骤 4 创建集群。

enter logical-device *device_name* **asa** *slots* **clustered**

- *Device_name* - 由 Firepower 4100/9300 机箱管理引擎用于配置集群设置以及分配接口；它不是在安全模块配置中使用的集群名称。必须指定全部三个安全模块，即使尚未安装硬件也是如此。
- *slots* - 将机箱模块分配给集群。对于 Firepower 4100，指定 **1**。对于 Firepower 9300，指定 **1,2,3**。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。

示例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

步骤 5 配置集群引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建集群引导程序对象。

enter cluster-bootstrap

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) 设置机箱 ID。

set chassis-id *id*

集群中的每个机箱都需要唯一 ID。

c) 对于站点间集群，请将站点 ID 设置为 1 到 8 之间的值。

set site-id *number*。

要删除站点 ID，请将值设为 **0**。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) 为集群控制链路上的控制流量配置身份验证密钥。

set key

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

系统将提示您输入共享密钥。

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。

e) 设置集群接口模式。

set mode spanned-etherchannel

跨区以太网通道模式是唯一支持的模式。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) 在安全模块配置中设置集群组名称。

set service-type *cluster_name*

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （可选） 设置　集群控制链路 IP 网络。

set cluster-control-link network *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，您可以对集群指定唯一网络上的 /16 地址。

- *a*.*b*.**0.0** - 指定任意 /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，则使用默认网络：127.2.0.0。

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*。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

h) 配置管理 IP 地址信息。

此信息用于配置安全模块配置中的管理接口。

1. 配置本地 IP 地址池，其中一个地址将被分配到接口的每个集群设备。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   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。属于当前控制设备的虚拟 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。

2. 为管理接口配置主集群 IP 地址。

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

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   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。

3. 输入网络网关地址。

set ipv4 gateway *ip_address*

set ipv6 gateway *ip_address*

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) 退出集群引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

步骤 6 配置管理引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建管理引导程序对象。

enter mgmt-bootstrap asa

示例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定管理员并启用密码。

create bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第2层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 7 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
```

```
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ ---------------- ------------
ftd         cluster1   1           Enabled     Online           6.4.0.49        6.4.0.49
    Native                    In Cluster      Slave
ftd         cluster1   2           Enabled     Online           6.4.0.49        6.4.0.49
    Native                    In Cluster      Master
ftd         cluster1   3           Disabled    Not Available                    6.4.0.49
    Native                    Not Applicable  None
```

步骤 8 要向集群添加其他机箱，请重复此程序，但必须配置唯一的 **chassis-id** 和正确的 **site-id**；否则，请对两个机箱使用同一配置。

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。

步骤 9 连接到控制设备 ASA 以自定义集群配置。

示例

对于机箱 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
```

```
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

对于机箱 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
```

```
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

添加更多群集成员

添加或替换 ASA 群集成员。

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群集的Firepower 9300，则该模块将自动添加。

开始之前

- 确保现有群集在此新成员的管理 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群集引导程序配置，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，在第一个群集成员上的ASA应用中启用多情景模式；其他群集成员将自动继承多情景模式配置。

过程

步骤 1 确定 (OK)。

步骤 2 要向集群添加其他机箱，请在创建 ASA 集群，第 279 页中重复此程序，但必须配置唯一的 **chassis-id** 和正确的 **site-id**； 否则，请对两个机箱使用同一配置。

添加 Firepower 威胁防御群集

在原生模式下： 您可以将单个 Firepower 9300 机箱添加为机箱内群集，或添加多个机箱以实现机箱间群集。

在多实例模式下：您可以在单个 Firepower 9300 机箱上添加一个或多个集群作为机箱内集群（必须在每个模块上包含一个实例），或者在多个机箱上添加一个或多个集群以用于机箱间集群。

对于机箱间集群，您必须单独配置每个机箱。在一个机箱上添加群集；然后，您可以在下一个机箱上输入基本相同的设置。

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。

在 Firepower 9300 机箱中，必须对全部 3 个模块插槽或容器实例（每个插槽中有一个容器实例）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。

开始之前

- 从 Cisco.com 下载要用于逻辑设备的应用映像，然后将映像上传至 Firepower 4100/9300 机箱。
- 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 176 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。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 346 页。
- 收集以下信息：
  - 管理接口 ID、IP 地址和网络掩码
  - 网关 IP 地址
  - FMC 您选择的 IP 地址和/或 NAT ID
  - DNS 服务器 IP 地址

- FTD 主机名和域名

过程

步骤 1 配置接口。

步骤 2 进入安全服务模式。

scope ssa

示例：

```
Firepower# scope ssa
Firepower /ssa #
```

步骤 3 接受想要使用的Firepower威胁防御版本的最终用户许可协议。如果尚未接受此版本的EULA，则只需执行此步骤即可。

a) 查看可用映像。请注意您想要使用的版本号。

show app

示例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 将范围设置为映像版本。

scope app ftd *application_version*

示例：

```
Firepower /ssa # scope app ftd 6.2.3
Firepower /ssa/app #
```

c) 接受许可协议。

accept-license-agreement

示例：

```
Firepower /ssa/app # accept-license-agreement

End User License Agreement: End User License Agreement

Effective: May 22, 2017
```

```
This is an agreement between You and Cisco Systems, Inc. or its affiliates
("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the
individual or legal entity licensing the Software under this EULA. "Use" or
"Using" means to download, install, activate, access or otherwise use the
Software. "Software" means the Cisco computer programs and any Upgrades made
available to You by an Approved Source and licensed to You by Cisco.
"Documentation" is the Cisco user or technical manuals, training materials,
specifications or other documentation applicable to the Software and made
available to You by an Approved Source. "Approved Source" means (i) Cisco or
(ii) the Cisco authorized reseller, distributor or systems integrator from whom
you acquired the Software. "Entitlement" means the license detail; including
license metric, duration, and quantity provided in a product ID (PID) published
on Cisco's price list, claim certificate or right to use notification.
"Upgrades" means all updates, upgrades, bug fixes, error corrections,
enhancements and other modifications to the Software and backup copies thereof.

[...]

Please "commit-buffer" if you accept the license agreement, otherwise "discard-buffer".

Firepower /ssa/app* #
```

d) 保存配置。

commit-buffer

示例：

```
Firepower /ssa/app* # commit-buffer
Firepower /ssa/app #
```

e) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope app ftd 6.3.0.21
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # exit
Firepower /ssa* #
```

步骤 4 设置应用实例参数，包括映像版本。

a) 对于容器实例，查看可用资源配置文件。要添加配置文件，请参阅为容器实例添加资源配置文件，第 176 页。

show resource-profile

请注意您想要使用的配置文件名称。

示例：

```
Firepower /ssa # show resource-profile

Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
 Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
bronze             N/A        N/A          No         all
      6            N/A No              Custom       low end device
silver 1           N/A        N/A          No         all
      8            N/A No              Custom       mid-level
```

b) 将范围设置为安全模块/引擎插槽。

scope slot *slot_id*

对于 Firepower 4100，*slot_id* 始终为 1；对于 Firepower 9300，则始终为 1、2 或 3。

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) 创建应用实例。

enter app-instance ftd *device_name*

device_name 可介于 1 至 64 个字符之间。在对此实例创建逻辑设备时，您将使用此设备名称。

示例：

```
Firepower /ssa/slot # enter app-instance ftd FTD1
Firepower /ssa/slot/app-instance* #
```

d) 对于容器实例，请将应用实例类型设置为容器。

set deploy-type container

容器实例使用部分安全模块/引擎资源，因此可以安装多个容器实例。本地实例使用安全模块/引擎的所有资源（CPU、RAM 和磁盘空间），因此仅可安装一个本地实例。

保存配置后，无法更改实例类型。默认类型为**native**。

示例：

```
Firepower /ssa/slot/app-instance* # set deploy-type container
```

e) 对于容器实例，设置资源配置文件。

set resource-profile-name *name*

该配置文件名称必须已存在。

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或集群，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。

示例：

```
Firepower /ssa/slot/app-instance* # set resource-profile-name bronze
```

f) 设置映像版本。

set startup-version *version*

输入您在此程序中之前记录的版本号。

示例：

```
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
```

g) （可选）对于容器实例，请启用或禁用 TLS 加密加速。

enter hw-crypto

set admin-state {**enabled** | **disabled**}

exit

此设置在硬件中启用TLS加密加速，并提高某些类型流量的性能。默认情况下启用此功能。您最多可以为每个安全模块的 16 个实例启用 TLS 加密加速。本地实例不支持此功能。要查看分配给该实例的硬件加密资源百分比，请输入 **show hw-crypto** 命令。请注意，版本 2 指的是 FXOS 2.7 及更高版本中使用的 TLS 加密加速类型。

示例：

```
Firepower /ssa/slot/app-instance* # enter hw-crypto
Firepower /ssa/slot/app-instance/hw-crypto* # set admin-state enabled
Firepower /ssa/slot/app-instance/hw-crypto* # exit
Firepower /ssa/slot/app-instance* # commit-buffer
Firepower /ssa/slot/app-instance # show hw-crypto
Hardware Crypto:
    Admin State           Hardware Crypto Size       Hardware Crypto Version
    ----------            -------------------------- --------------------------------

    enabled                   40%                                   2
```

h) 退出到插槽模式。

exit

示例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

i) 对于 Firepower 9300 上的容器实例，请重复这些步骤，以在每个安全模块上创建一个容器实例。

j) 退出到 ssa 模式。

exit

示例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

示例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa # scope slot 2
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa # scope slot 3
Firepower /ssa/slot # enter app-instance ftd MyDevice1
Firepower /ssa/slot/app-instance* # set deploy-type container
Firepower /ssa/slot/app-instance* # set resource-profile-name silver 1
Firepower /ssa/slot/app-instance* # set startup-version 6.6.0
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

步骤 5 创建集群：

enter logical-device *device_name* **ftd** *slots* **clustered**

- *device_name* - 使用与您之前添加的应用实例相同的 *device_name*。
- *slots* - 将机箱模块分配给集群。对于 Firepower 4100，指定 **1**。对于 Firepower 9300，指定 **1,2,3**。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。

示例：

```
Firepower /ssa # enter logical-device FTD1 ftd 1,2,3 clustered
Firepower /ssa/logical-device* #
```

步骤 6 配置集群引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建集群引导程序对象。

enter cluster-bootstrap

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
```

```
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) 设置机箱 ID。

set chassis-id *id*

集群中的每个机箱都需要唯一 ID。

c) 对于站点间集群，请将站点 ID 设置为 1 到 8 之间的值。

set site-id *number*。

要删除站点 ID，请将值设为 **0**。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) 为集群控制链路上的控制流量配置身份验证密钥。

set key

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

系统将提示您输入共享密钥。

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。

e) 设置集群接口模式。

set mode spanned-etherchannel

跨区以太网通道模式是唯一支持的模式。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) 在安全模块配置中设置集群组名称。

set service-type *cluster_name*

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （可选） 设置　集群控制链路 IP 网络。

set cluster-control-link network *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，您可以对集群指定唯一网络上的 /16 地址。

- ***a*.*b*.0.0** - 指定任意 /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，则使用默认网络：127.2.0.0。

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*。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
10.10.0.0
```

h) 退出集群引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

步骤 7 配置管理引导程序参数。

这些设置仅用于仅初始部署或灾难恢复。为了实现正常运行，稍后可以更改应用 CLI 配置中的大多数值。

a) 创建管理引导程序对象。

enter mgmt-bootstrap ftd

示例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) 指定管理 Firepower 管理中心 的 IP 地址或主机名或 NAT ID。

设置以下其中一项：

- **enter bootstrap-key FIREPOWER_MANAGER_IP**

  set value *IP_address*

  exit

- **enter bootstrap-key FQDN**

set value *fmc_hostname*

exit

- **enter bootstrap-key NAT_ID**

  set value *nat_id*

  exit

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。您可以将长度介于 1 到 37 个字符之间的任意文本字符串指定为 NAT ID。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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key NAT_ID
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value sc0rpius15
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 指定防火墙模式：路由或透明。

create bootstrap-key FIREWALL_MODE

set value {**routed** |**transparent**}

exit

在路由模式中，设备被视为网络中的路由器跃点。要在其间路由的每个接口都位于不同的子网上。另一方面，透明防火墙是一个第 2 层防火墙，充当“线缆中的块”或“隐蔽的防火墙”，不被视为是到所连接设备的路由器跃点。

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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 指定设备和 FMC之间要共享的密钥。

enter bootstrap-key-secret REGISTRATION_KEY

set value

输入值：*registration_key*

确认值：*registration_key*

exit

可以为此密钥选择介于 1 至 37 个字符之间的任何文本字符串；添加FTD时，需要在FMC上输入相同的密钥。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) 指定供 FTD 管理员用户用于 CLI 访问的密码。

enter bootstrap-key-secret PASSWORD

set value

输入值： 密码

确认值： 密码

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 指定完全限定主机名。

enter bootstrap-key FQDN

set value *fqdn*

exit

有效字符是从 a 到 z 的字母、从 0 到 9 的数字、点 (.) 和连字符(-)；最大字符数为 253。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
ftdcluster1.example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

g) 指定 DNS 服务器列表（用逗号隔开）。

enter bootstrap-key DNS_SERVERS

set value *dns_servers*

exit

例如，如果指定 FMC 主机名，则 FTD 使用 DNS。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

h) 指定搜索域列表（用逗号隔开）。

enter bootstrap-key SEARCH_DOMAINS

set value *search_domains*

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

i) （可选）对于容器实例，允许 FTD SSH 会话专家模式。专家模式提供 FTD shell 访问权限以确保实现高级故障排除。

create bootstrap-key PERMIT_EXPERT_MODE

set value {**yes** | **no**}

exit

- **yes**- 拥有直接从 SSH 会话访问此容器实例的权限的用户可以输入专家模式。
- **no**- 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。

默认情况下，对于容器实例，只有从 FXOS CLI 访问 FTD CLI 的用户可以进入专家模式。此限制仅用于容器实例，以增强实例之间的隔离。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。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

j) 为集群中的每个安全模块配置管理 IP 地址。

注释 对于 Firepower 9300，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。

要创建 IPv4 管理接口对象，请执行以下操作：

1. 创建管理接口对象。

   enter ipv4 *slot_id* **firepower**

2. 设置网关地址。

   set gateway *gateway_address*

3. 设置 IP 地址和掩码。

   set ip *ip_address* **mask** *network_mask*

4. 退出管理 IP 模式。

   exit

5. 对机箱中的其余模块重复此操作。

要创建 IPv6 管理接口对象，请执行以下操作：

1. 创建管理接口对象。

   enter ipv6 *slot_id* **firepower**

2. 设置网关地址。

   set gateway *gateway_address*

3. 设置 IP 地址和网络前缀。

   set ip *ip_address* **prefix-length** *prefix*

4. 退出管理 IP 模式。

   exit

5. 对机箱中的其余模块重复此操作。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.35 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.36 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 firepower
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3211
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3212
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

k) 退出管理引导程序模式。

exit

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

示例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.0.0.100
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
  Value: ziggy$tardust
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
  Value: $pidersfrommars
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FQDN
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.cisco.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 192.168.1.1
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 1 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 2 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.32 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # enter ipv4 3 firepower
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
```

```
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.33 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 8 保存配置。

commit-buffer

机箱通过下载指定软件版本，并将引导程序配置和管理接口设置推送至应用实例来部署逻辑设备。使用 **show app-instance** 命令检查部署状态。当**管理状态**为**已启用**且**运行状态**为**在线**时，应用实例正在运行且可供使用。

示例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State      Running Version Startup Version
 Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- --------------- ---------------
 ----------- ------------ --------------- ------------
ftd        cluster1   1          Enabled     Online           6.4.0.49        6.4.0.49
    Native                    In Cluster      Slave
ftd        cluster1   2          Enabled     Online           6.4.0.49        6.4.0.49
    Native                    In Cluster      Master
ftd        cluster1   3          Disabled    Not Available                    6.4.0.49
    Native                    Not Applicable  None
```

步骤 9 要将其他机箱添加到集群中，请重复此过程，但必须配置唯一的 **chassis-id** 和管理 IP 地址以及正确的**site-id**；否则，请对两个机箱使用相同的配置。

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。

步骤 10 使用管理 IP 地址将控制设备添加到 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 会自动检测数据设备。

本地集群示例

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
```

```
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type firepower-eventing
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      enter bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
      enter ipv4 1 firepower
```

```
      set gateway 10.0.0.1
      set ip 10.0.0.31 mask 255.255.255.0
      exit
    enter ipv4 2 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.32 mask 255.255.255.0
      exit
    enter ipv4 3 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.33 mask 255.255.255.0
      exit
    exit
  exit
 scope app ftd 6.0.0.837
  accept-license-agreement
  set-default
  exit
 commit-buffer
```

对于机箱 2：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type firepower-eventing
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
```

```
commit-buffer

scope ssa
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      enter bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
      enter ipv4 1 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.31 mask 255.255.255.0
        exit
      enter ipv4 2 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.32 mask 255.255.255.0
        exit
      enter ipv4 3 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.33 mask 255.255.255.0
        exit
      exit
    exit
  scope app ftd 6.0.0.837
    set-default
    accept-license-agreement
    exit
  commit-buffer
```

多实例集群示例

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
```

```
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter interface Ethernet1/8
      set port-type mgmt
      enable
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      enter subinterface 100
        set vlan 100
        set port-type cluster
      exit
    exit
  exit
commit-buffer

scope ssa
  scope slot 1
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
  scope slot 2
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      enter bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
```

```
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
        exit
      enter ipv4 1 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.31 mask 255.255.255.0
        exit
      enter ipv4 2 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.32 mask 255.255.255.0
        exit
      enter ipv4 3 firepower
        set gateway 10.0.0.1
        set ip 10.0.0.33 mask 255.255.255.0
        exit
      enter bootstrap-key PERMIT_EXPERT_MODE
        set value yes
        exit
      exit
    exit
  scope app ftd 6.6.0
    accept-license-agreement
    exit
  commit-buffer
```

对于机箱 2：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    enter interface Ethernet1/8
      set port-type mgmt
      enable
      exit
```

```
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      enter subinterface 100
        set vlan 100
        set port-type cluster
      exit
    exit
  exit
commit-buffer

scope ssa
  scope slot 1
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
  scope slot 2
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
    enter app-instance ftd FTD1
      set deploy-type container
      set resource-profile-name medium
      set startup-version 6.6.0
      exit
    exit
  enter logical-device FTD1 ftd "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set key cluster_key
      set mode spanned-etherchannel
      set service-type ftd-cluster
      exit
    enter mgmt-bootstrap ftd
      enter bootstrap-key FIREPOWER_MANAGER_IP
        set value 10.0.0.100
        exit
      enter bootstrap-key FIREWALL_MODE
        set value transparent
        exit
      enter bootstrap-key-secret REGISTRATION_KEY
        set value
          Value: alladinsane
        exit
      enter bootstrap-key-secret PASSWORD
        set value
          Value: widthofacircle
        exit
      enter bootstrap-key FQDN
        set value ftd.cisco.com
        exit
      enter bootstrap-key DNS_SERVERS
        set value 192.168.1.1
        exit
      enter bootstrap-key SEARCH_DOMAINS
        set value search.com
```

```
      exit
    enter ipv4 1 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.31 mask 255.255.255.0
      exit
    enter ipv4 2 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.32 mask 255.255.255.0
      exit
    enter ipv4 3 firepower
      set gateway 10.0.0.1
      set ip 10.0.0.33 mask 255.255.255.0
      exit
    enter bootstrap-key PERMIT_EXPERT_MODE
      set value yes
      exit
    exit
  exit
scope app ftd 6.6.0
  accept-license-agreement
  exit
commit-buffer
```

添加更多集群设备

在现有群集中添加或替换 FTD 集群设备。在 FXOS 中添加新的群集设备时，Firepower 管理中心会自动添加该设备。

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群集的 Firepower 9300，则该模块将自动添加。

开始之前

- 如果是替换，则必须从Firepower 管理中心中删除旧的集群设备。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

要向群集添加其他机箱，请在 创建 Firepower 威胁防御集群，第 288 页 中重复此程序，但必须将以下设置配置为唯一设置；否则，请对两个机箱使用同一配置。

- 机箱 ID
- 管理 IP 地址

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 117 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 4115
  - Firepower 4120
  - Firepower 4125
  - Firepower 4140
  - Firepower 4145
  - 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 4112
  - Firepower 4115
  - 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 4125
  - Firepower 4140
  - Firepower 4145
  - Firepower 4150

其他规定

- 服务链在机箱间群集配置中不受支持。但是，在机箱间群集场景中，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。

开始之前

- 从 Cisco.com 下载 vDP 映像（请参阅从 Cisco.com 下载映像，第 70 页），然后将此映像下载到 Firepower 4100/9300 机箱（请参阅将逻辑设备软件映像下载到 Firepower 4100/9300 机箱，第 74 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 313 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 205 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 在独立配置中创建 ASA 或 Firepower 威胁防御逻辑设备（请参阅添加独立 ASA，第 246 页或为 FMC 添加独立的 Firepower 威胁防御，第 252 页）。请注意，如果您在 Firepower 4110 或 4120 安全设备上安装映像，则必须在提交配置之前安装 vDP 以及 Firepower 威胁防御映像。

步骤 3 进入安全服务模式：

Firepower# **scope ssa**

步骤 4 创建 Radware vDP 实例：

Firepower /ssa # **scope slot** *slot_id*

Firepower /ssa/slot # **create app-instance vdp** *logical_device_identifier*

Firepower /ssa/slot/app-instance* # **exit**

Firepower /ssa/slot/* # **exit**

步骤 5 提交配置：

commit-buffer

步骤 6 验证 vDP 在安全模块上的安装和调配：

Firepower /ssa # **show app-instance**

示例：

```
Firepower /ssa # show app-instance
App Name    Slot ID    Admin State Oper State       Running Version Startup Version Cluster
 State    Cluster Role
---------- ---------- ----------- ---------------- --------------- ---------------
---------------- -------------
ftd         1          Enabled     Online           6.2.1.62        6.2.1.62        Not
Applicable  None
vdp         1          Disabled    Installing                       8.10.01.16-5    Not
Applicable  None
```

步骤 7 （可选）显示受支持的可用资源配置文件：

Firepower /ssa/app # **show resource-profile system**

示例：

```
Firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
 2           8192 No              System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
```

```
 4          16384 No              System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 8          32768 No              System
```

步骤 8 （可选）使用上一步中可用的配置文件之一设置资源配置文件：

a) 确定插槽 1 的范围：

Firepower /ssa*# **scope slot 1**

b) 输入 DefensePro 应用实例：

Firepower /ssa/slot* # **enter app-instance vdp**

c) 设置资源配置文件：

Firepower /ssa/slot/app-instance* # **set resource-profile-name** *resource_profile_name*

d) 提交配置：

Firepower /ssa/slot/app-instance* # **commit-buffer**

步骤 9 安装 vDP 应用后，访问逻辑设备：

Firepower /ssa # **scope logical-device** *device_name*

步骤 10 将管理接口分配给 vDP。您可以使用与逻辑设备相同的物理接口，也可以使用单独的接口。

Firepower /ssa/logical-device # **enter external-port-link** *name interface_id* **vdp**

Firepower /ssa/logical-device/external-port-link* # **exit**

步骤 11 为 vDP 配置外部管理接口设置：

a) 创建引导程序对象：

Firepower /ssa/logical-device* # **create mgmt-bootstrap vdp**

b) 配置管理 IP 地址：

Firepower /ssa/logical-device/mgmt-bootstrap* # **create ipv4** *slot_id* **default**

c) 设置网关地址：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**set gateway** *gateway_address*

d) 设置 IP 地址和掩码：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**set ip** *ip_address* **mask** *network_mask*

e) 退出管理 IP 配置范围：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**exit**

f) 退出管理引导程序配置范围：

Firepower /ssa/logical-device/mgmt-bootstrap* #**exit**

步骤 12 编辑要在其中将 vDP 置于 ASA 或 Firepower 威胁防御流前面的数据接口：

Firepower /ssa/logical-device* # **scope external-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

步骤 13 向逻辑设备添加 vDP：

Firepower /ssa/logical-device/external-port-link* # **set decorator vdp**

对要使用 vDP 的每个接口重复上述操作。

步骤 14 提交配置：

commit-buffer

步骤 15 验证并确保针对接口设置了第三方应用：

Firepower /ssa/logical-device/external-port-link* # **show detail**

示例：

```
Firepower /ssa/logical-device/external-port-link # show detail

External-Port Link:
    Name: Ethernet11_ftd
    Port or Port Channel Name: Ethernet1/1
    App Name: ftd
    Description:
    Link Decorator: vdp
```

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

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 70 页），然后将此映像下载到 Firepower 4100/9300 机箱（请参阅将逻辑设备软件映像下载到 Firepower 4100/9300 机箱，第 74 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 205 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 机箱内集群（请参阅创建 ASA 集群，第 279 页）或 Firepower 威胁防御机箱内集群（请参阅创建 Firepower 威胁防御集群，第 288 页）。

步骤 3 用 Radware DefensePro 修饰外部（面向客户端）端口：

enter external-port-link *name interface_name* { **asa** | **ftd** }

set **decorator vdp**

set **description** ""

exit

步骤 4 为逻辑设备分配外部管理接口：

输入 **external-port-link** *{ mgmt_asa | mgmt_ftd } interface_id { asa | ftd }*

set **decorator** ""

set **description** ""

exit

步骤 5 为 DefensePro 分配外部管理端口：

输入 **external-port-link mgmt_vdp** *interface_name { asa | ftd }*

set **decorator** ""

set **description** ""

步骤 6 （可选）显示受支持的可用资源配置文件：

show resource-profile system

示例：

```
Firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core Count
 RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- --------------- ----------------------
 -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
 4          16384 Yes             System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 6          24576 Yes             System
VDP-10-CORES       vdp        8.13.01.09-2 No        FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

10          40960 No              System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
 2           8192 No              System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
```

```
 4          16384 No              System
VDP-8-CORES        vdp       8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44, FPR9K-SM-36,
 FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

 8          32768 No              System
```

步骤 7 （可选）使用上一步中可用的配置文件之一设置资源配置文件：

注释 提交此更改后，FXOS 机箱将重新启动。

a) 确定插槽 1 的范围：

Firepower /ssa*# **scope slot 1**

b) 输入 DefensePro 应用实例：

Firepower /ssa/slot* # **enter app-instance vdp**

c) 设置资源配置文件：

Firepower /ssa/slot/app-instance* # **set resource-profile-name** *resource_profile_name*

d) 提交配置：

Firepower /ssa/slot/app-instance* # **commit-buffer**

步骤 8 配置集群端口通道：

输入 **external-port-link** port-channel48 Port-channel48 *{ asa | ftd }*

set **decorator** ''''

set **description** ''''

exit

步骤 9 为所有的三个 DefensePro 实例配置管理引导程序：

enter **mgmt-bootstrap vdp**

输入 **ipv4** *slot_id* **default**

set gateway *gateway_address*

set ip *ip_address* **mask** *network_mask*

exit

示例：

```
enter mgmt-bootstrap vdp
    enter ipv4 1 default
        set gateway 172.16.0.1
        set ip 172.16.4.219 mask 255.255.0.0
    exit

    enter ipv4 2 default
        set gateway 172.16.0.1
        set ip 172.16.4.220 mask 255.255.0.0
    exit

    enter ipv4 3 default
```

```
        set gateway 172.16.0.1
        set ip 172.16.4.221 mask 255.255.0.0
    exit
```

步骤 10 退出管理引导程序配置范围：

exit

步骤 11 进入控制刀片上的 DefensePro 应用实例：

connect module *slot* **console**

connect vdp

步骤 12 在控制刀片上，设置管理 IP：

device clustering management-channel ip

步骤 13 使用上一步中找到的 IP 设置控制 IP：

device clustering master set *management-channel ip*

步骤 14 启用集群：

device clustering state set enable

步骤 15 退出应用控制台并返回到 FXOS 模块 CLI：

Ctrl]

步骤 16 重复步骤 10、12、13 和 14 以设置在步骤 11 中找到的控制刀片 IP，并为每个刀片应用实例启用集群。

步骤 17 提交配置：

commit-buffer

注释 完成此程序后，必须验证是否已在集群中配置 DefensePro 实例。

步骤 18 验证所有 DefensePro 应用都已加入该集群：

device cluster show

步骤 19 使用以下方法之一，验证哪个 DefensePro 实例是主要的，哪个是次要的。

a) 确定 DefensePro 实例范围，仅显示 DefensePro 的应用属性：

scope ssa

scope slot *slot_number*

scope app-instance vdp

show app-attri

b) 确定插槽范围，显示 DefensePro 实例的详细信息。此方法显示插槽上的逻辑设备和 vDP 应用实例的相关信息。

scope ssa

scope *slot_number*

show app-instance expand detail

如果 DefensePro 应用在线，但尚未在集群中形成，CLI 将显示：

```
App Attribute:
    App Attribute Key: cluster-role
    Value: unknown
```

如果系统显示此“unknown”值，您必须进入 DefensePro 应用，配置控制刀片 IP 地址，创建 vDP 集群。

如果 DefensePro 应用在线，并且已在集群中形成，CLI 将显示：

```
App Attribute:
    App Attribute Key: cluster-role
    Value: primary/secondary
```

示例

```
scope ssa
  enter logical-device ld asa "1,2,3" clustered
     enter cluster-bootstrap
         set chassis-id 1
         set ipv4 gateway 172.16.0.1
         set ipv4 pool 172.16.4.216 172.16.4.218
         set ipv6 gateway 2010::2
         set ipv6 pool 2010::21 2010::26
         set key secret
         set mode spanned-etherchannel
         set name cisco
         set virtual ipv4 172.16.4.222 mask 255.255.0.0
         set virtual ipv6 2010::134 prefix-length 64
     exit
     enter external-port-link Ethernet1-2 Ethernet1/2 asa
         set decorator vdp
         set description ""
     exit
     enter external-port-link Ethernet1-3_asa Ethernet1/3 asa
         set decorator ""
         set description ""
     exit
     enter external-port-link mgmt_asa Ethernet1/1 asa
         set decorator ""
         set description ""
     exit
     enter external-port-link mgmt_vdp Ethernet1/1 vdp
         set decorator ""
         set description ""
     exit
     enter external-port-link port-channel48 Port-channel48 asa
         set decorator ""
         set description ""
     exit
     enter mgmt-bootstrap vdp
         enter ipv4 1 default
             set gateway 172.16.0.1
             set ip 172.16.4.219 mask 255.255.0.0
         exit
```

```
          enter ipv4 2 default
              set gateway 172.16.0.1
              set ip 172.16.4.220 mask 255.255.0.0
          exit

          enter ipv4 3 default
              set gateway 172.16.0.1
              set ip 172.16.4.221 mask 255.255.0.0
          exit
 exit
commit-buffer
scope ssa
   scope slot 1
   scope app-instance vdp
   show app-attri
    App Attribute:
        App Attribute Key: cluster-role
        Value: unknown
```

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]

配置 TLS 加密加速

以下主题讨论 TLS 加密加速、如何启用它，以及如何使用 Firepower 管理中心查看其状态。

下表会将 FTD 和 FXOS 版本与所需的 TSL 加密进行映射：

注释 当 FXOS 2.6.1 升级到 FXOS 2.7.x 及更高版本时，FTD 6.4 不会自动启用加密，因为 6.4 与 TLS 加密不兼容。

FTD	FXOS	加密
6.4	2.6	仅支持一个容器实例（第 1 阶段）
6.4	2.7 及更高版本	不适用
6.5 及更高版本	2.7 及更高版本	支持最多 16 个容器实例（第 2 阶段）

关于 TLS 加密加速

The Firepower 4100/9300 支持传输层安全加密加速，它在硬件中执行传输层安全/安全套接层 (TLS/SSL) 加密和解密，这极大地改进了以下方面的性能：

- TLS/SSL 加密和解密。
- VPN，包括TLS/SSL和 IPsec

TLS 加密加速功能在本地实例上自动启用，无法禁用。您还可以在每个安全引擎/模块上的 最多 16 个 FTD 容器实例 上启用 TLS 加密加速。

TLS 加密加速的准则和限制

如果 FTD 启用了 TLS 加密加速，请记住以下几点。

检测引擎故障

如果检测引擎配置为保留连接，并且检测引擎意外出现故障，则 TLS/SSL流量将被丢弃，直到引擎重启。

此行为由 FTD **configure snort preserve-connection {enable | disable}** 命令控制。

仅 HTTP 性能

在不解密流量的 FTD 容器实例 上使用 TLS 加密加速 可能会影响性能。我们建议TLS 加密加速 仅 在解密 TLS/SSL 流量的 FTD 容器实例 上启用。

联邦信息处理标准 (FIPS)

如果同时启用了 TLS 加密加速和联邦信息处理标准 (FIPS)，则与以下选项的连接会失败：

- 大小小于 2048 字节的 RSA 密钥
- Rivest 密码 4 (RC4)
- 单一数据加密标准（单一 DES）
- Merkle – Damgard 5 (MD5)
- SSL v3

当您将 Firepower 管理中心和 FTD 配置为以安全认证合规模式运行时，FIPS 会被启用。在这些模式下运行时，要允许连接，可以在 FTD 容器实例 上禁用 TLS 加密加速，或者可以配置 Web 浏览器以接受更为安全的选项。

更多详情：

- 通用标准。

高可用性 (HA) 和集群

如果有高可用性 (HA) 或集群 FTD，则必须分别在每个 FTD 上启用 TLS 加密加速。一个设备的 TLS 加密加速 配置不与 HA 对或集群中的其他设备共享。

TLS 心跳

某些应用使用 RFC6520 定义的传输层安全 (TLS) 和数据报传输层安全 (DTLS) 协议的 *TLS* 心跳扩展。SSL 心跳可用于确认连接是否仍处于活动状态 - 客户端或服务器发送指定字节数的数据，并请求另一方回送响应。如果此过程成功，则发送加密的数据。

当启用 TLS 加密加速 的受 FMC 管理的 FTD 遇到使用 TLS 心跳扩展的数据包时，该 FTD 将执行 SSL 策略的**无法解密的操作**中**解密错误** FMC 设置所指定的操作：

- 阻止
- 阻止并重置

要确定应用程序是否使用 TLS 心跳，请参阅《*Firepower* 管理中心配置指南》中有关 TLS/SSL 故障排除规则的章节。

如果在 FTD 容器实例 上禁用 TLS 加密加速，则可以在 FMC 中的网络分析策略 (NAP) 中配置**最大心跳长度**，以便确定如何处理 TLS 心跳。

有关 TLS 心跳的详细信息，请参阅《*Firepower* 管理中心配置指南》中有关 TLS/SSL 故障排除规则的章节。

TLS/SSL 超订用

TLS/SSL 超订用 指 FTD TLS/SSL 流量过载的状态。任何 FTD 都可能会遇到 TLS/SSL 超订用，但只有支持 TLS 加密加速 的 FTD 才提供可配置的方式对其进行处理。

当启用了 TLS 加密加速 的 FTD 发生超订用时，对于该 FTD 接收的任何数据包，都将根据 SSL 策略**无法解密的操作**中**握手错误**设置进行处理：

- 继承默认操作
- 不解密
- 阻止
- 阻止并重置

如果 SSL 策略**无法解密的操作**中**握手错误**的设置为**不解密**，且相关的访问控制策略配置为检查流量，则检查会发生；但是解密不会发生。

如果出现大量超订用，有以下选项可供选择：

- 升级到具有更多 TLS/SSL 处理能力的 FTD。
- 更改您的 SSL 策略，为不具有较高解密优先级的流量添加**不解密**规则。

有关 TLS 超订用的详细信息，请参阅《*Firepower* 管理中心配置指南》中有关 TLS/SSL 故障排除规则的章节。

不支持被动和内联轻触设置

启用 TLS 加密加速 后，无法在被动或内联轻触设置接口上解密 TLS/SSL 流量。

启用容器实例的 TLS 加密加速

当按照为 FMC 添加独立的 Firepower 威胁防御，第 252 页中所述部署逻辑实例时，将自动启用 TLS 加密加速。

TLS 加密加速 将在所有本地实例上自动启用，并且无法禁用。

查看 TLS 加密加速的状态

本主题讨论如何确定是否已启用 TLS 加密加速。

在 Firepower 管理中心执行以下任务。

过程

步骤 1 登录到 Firepower 管理中心。

步骤 2 单击**设备** > **设备管理**。

步骤 3 单击 **编辑**（  ） 以编辑受管设备。

步骤 4 单击**设备 (Device)**页面。TLS 加密加速 状态显示在“常规”(General) 部分中。

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安全引擎，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 *name*

connect ftd *name*

connect vdp *name*

要查看实例名称，请输入不含名称的命令。

示例：

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
```

```
asa>
```

示例：

```
Firepower-module1> connect ftd ftd1
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 **exit**
- vDP - 输入 **Ctrl-], .**

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 asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

删除逻辑设备

过程

步骤 1 进入安全服务模式：

Firepower# **scope ssa**

步骤 2 查看机箱上的逻辑设备的详细信息：

Firepower /ssa # **show logical-device**

步骤 3 对于想要删除的每个逻辑设备，请输入以下命令：

Firepower /ssa # **delete logical-device** *device_name*

步骤 4 查看逻辑设备上安装的应用的详细信息：

Firepower /ssa # **show app-instance**

步骤 5 对于想要删除的每个应用，请输入以下命令：

a) Firepower /ssa # **scope slot** *slot_number*
b) Firepower /ssa/slot # **delete app-instance** *application_name*
c) Firepower /ssa/slot # **exit**

步骤 6 提交配置：

commit-buffer

提交系统配置任务。

示例

```
Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
    Name       Description Slot ID    Mode       Operational State        Template Name
    ---------- ----------- ---------- ---------- ------------------------ -------------
    FTD                    1,2,3      Clustered  Ok                       ftd
Firepower /ssa # delete logical-device FTD
Firepower /ssa* # show app-instance
Application Name    Slot ID    Admin State    Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ----------- --------------- -------------------- ---------------
--------------- ------------------
ftd                            1 Disabled        Stopping             6.0.0.837
6.0.0.837       Not Applicable
ftd                            2 Disabled        Offline              6.0.0.837
6.0.0.837       Not Applicable
ftd                            3 Disabled        Not Available
6.0.0.837       Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
```

```
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

删除群集设备

以下部分介绍如何临时或永久删除群集中的设备。

临时删除

例如，出现硬件或网络故障时，群集设备会自动从群集中删除。此删除是临时的，故障消除后，它们可以重新加入群集。您也可以手动禁用群集。

要检查设备当前是否在群集中，在应用程序内使用 **show cluster info** 命令查看群集状态：

```
ciscoasa# show cluster info
Clustering is not enabled
```

对于使用 FMC 的 FTD，应该将设备留在 FMC 设备列表中，以便在重新启用群集后，它可以恢复全部功能。

- 在应用程序中禁用群集 - 您可以使用应用程序 CLI 禁用群集。输入 **cluster remove unit** *name* 命令删除除您登录的设备以外的所有设备。引导程序配置保持不变，从控制设备同步的最新配置也保持不变，因此您可于稍后重新添加该设备而不会丢失配置。如果在数据设备上输入此命令来删除控制设备，将会选举新的控制设备。

  当设备处于非主用状态时，所有数据接口关闭；只有管理接口可以发送和接收流量。要恢复流量流，请重新启用群集。管理接口将保持打开，使用设备从引导程序配置接收的 IP 地址。但如果您重新加载，而设备仍在群集中处于非主用状态，则管理接口将被禁用。

  要重新启用群集，请在 ASA 上输入 **cluster group** *name*，然后输入 **enable**。要重新启用群集，请在 FTD 上输入 **cluster enable**。

- 禁用应用程序实例 - 在 FXOS CLI 中，请参阅以下示例：

  ```
  Firepower-chassis# scope ssa
  Firepower-chassis /ssa # scope slot 1
  Firepower-chassis /ssa/slot # scope app-instance asa asa1
  Firepower-chassis /ssa/slot/app-instance # disable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

  要重新启用：

  ```
  Firepower-chassis /ssa/slot/app-instance # enable
  Firepower-chassis /ssa/slot/app-instance* # commit-buffer
  Firepower-chassis /ssa/slot/app-instance #
  ```

- 关闭 安全模块/引擎 - 在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

要接通电源：

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- 关闭机箱 - 在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

永久删除

您可以使用以下方法永久删除群集成员。

对于使用 FMC 的 FTD，确保在机箱上禁用群集后，从 FMC 设备列表删除设备。

- 删除逻辑设备 - 在 FXOS CLI 中，请参阅以下示例：

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- 从服务中删除机箱或安全模块 - 如果从服务中删除设备，则可以将替换硬件添加为群集的新成员。

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 进入安全服务模式：

Firepower# **scope ssa**

步骤 2 查看已安装应用的详细信息：

Firepower /ssa # **show app-instance**

步骤 3 对于想要删除的每个应用，请输入以下命令：

a) Firepower /ssa # **scope slot** *slot_number*
b) Firepower /ssa/slot # **delete app-instance** *application_name*
c) Firepower /ssa/slot # **exit**

步骤 4 提交配置：

commit-buffer

提交系统配置任务。

示例

```
Firepower# scope ssa
Firepower /ssa* # show app-instance
Application Name     Slot ID     Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ----------- --------------- -------------------- ---------------
--------------- ------------------
ftd                              1 Disabled        Stopping             6.0.0.837
6.0.0.837       Not Applicable
ftd                              2 Disabled        Offline              6.0.0.837
6.0.0.837       Not Applicable
ftd                              3 Disabled        Not Available
6.0.0.837       Not Applicable
Firepower /ssa* # scope slot 1
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 2
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # scope slot 3
Firepower /ssa/slot # delete app-instance ftd
Firepower /ssa/slot* # exit
Firepower /ssa* # commit-buffer
```

更改 Firepower 威胁防御逻辑设备上的接口

可以在 FTD 逻辑设备上分配或取消分配接口。然后，可以在 FMC 或 FDM 中同步接口配置。

添加新接口或删除未使用接口对FTD配置的影响最小。但是，删除安全策略中使用的接口会影响配置。可以直接在 FTD 配置中的很多位置引用接口，包括访问规则、NAT、SSL、身份规则、VPN、DHCP 服务器等。引用安全区域的策略不受影响。还可以编辑已分配的 EtherChannel 的成员关系，而不影响逻辑设备或要求在FMC或FDM上进行同步。

对于 FMC：删除接口将删除与该接口相关的任何配置。

对于 FDM：可以在删除旧接口前，将配置从一个接口迁移至另一个接口。

开始之前

- 根据配置物理接口，第 205 页和添加 EtherChannel（端口通道），第 207 页配置您的接口，并添加任何 EtherChannel。
- 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。
- 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FMC 或 FDM 中同步配置。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。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 进入安全服务模式：

Firepower# **scope ssa**

步骤 2 编辑逻辑设备：

Firepower /ssa # **scope logical-device** *device_name*

步骤 3 将新的接口分配到逻辑设备：

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **ftd**

请勿删除任何接口。

步骤 4 提交配置：

commit-buffer

提交系统配置任务。

步骤 5 同步中FMC的接口。

a) 登录至FMC。

b) 依次选择**设备 (Devices)** > **设备管理 (Device Management)**，并单击 FTD 设备的 **编辑**（  ）。系统默认选择**接口 (Interfaces)** 页面。

c) 单击**接口 (Interfaces)** 页面左上方的**同步设备 (Sync Device)** 按钮。

d) 检测到更改后，可以在**接口 (Interfaces)** 页面上看到红色横幅，表明接口配置已发生更改。单击**单击了解详情 (Click to know more)** 链接以查看接口更改。

e) 如果计划删除接口，请手动将任何接口配置从旧接口传输至新接口。

由于尚未删除任何接口，因此可以引用现有配置。在删除旧接口并重新运行验证后，将有额外的机会来修复配置。验证将显示仍在使用旧接口的所有位置。

f) 单击**验证更改 (Validate Changes)** 以确保策略在接口更改后仍有效。

如出现任何错误，则需要更改配置并重新运行验证。

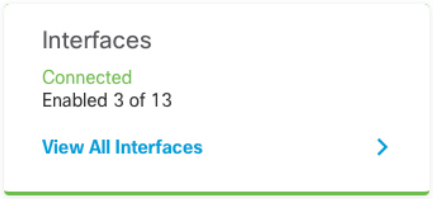
g) 单击**保存 (Save)**。

h) 选择设备然后单击**部署 (Deploy)**，以将策略部署到所分配的设备。在部署更改之后，更改才生效。

步骤 6 同步和迁移 FDM 中的接口。

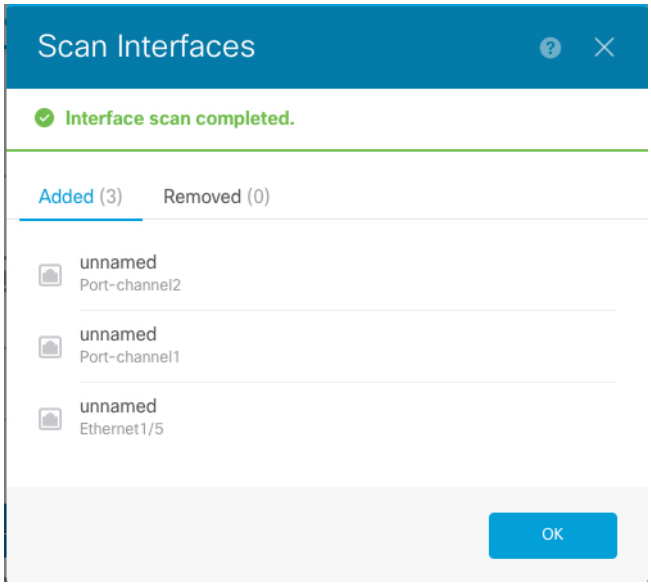
a) 登录至 FDM。

b) 单击**设备 (Device)**，然后单击**接口 (Interfaces)** 摘要中的**查看所有接口 (View All Interfaces)** 链路。



c) 单击**扫描接口 (Scan Interfaces)** 图标。

d) 等待接口扫描，然后单击**确定 (OK)**。



e) 使用名称、IP 地址等配置新接口。

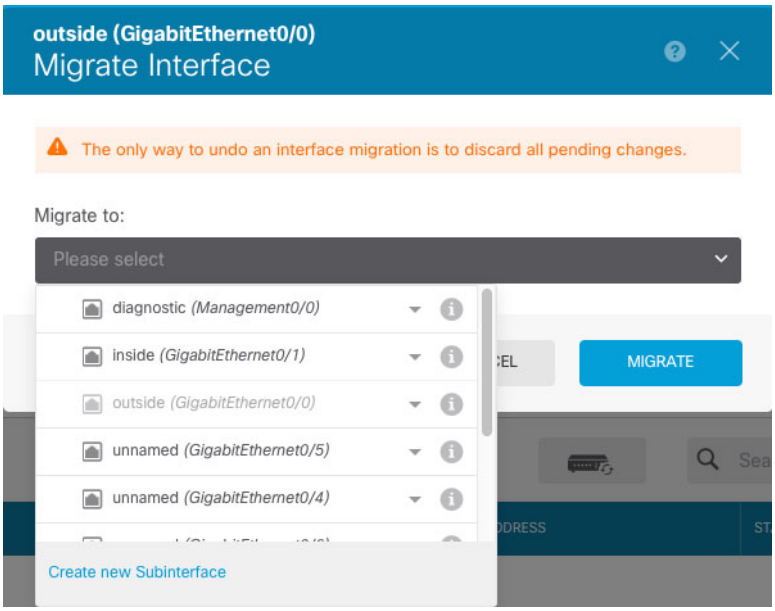
如果要使用待删除接口的现有 IP 地址和名称，则需要使用虚拟名称和 IP 地址重新配置旧接口，以便可以在新接口上使用这些设置。

f) 要将旧接口替换为新接口，请单击旧接口的“替换”(Replace) 图标。

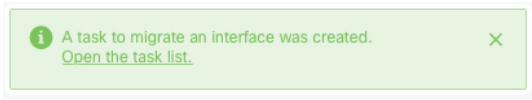
替换图标

此过程会将旧接口替换为引用该接口的所有配置设置中的新接口。

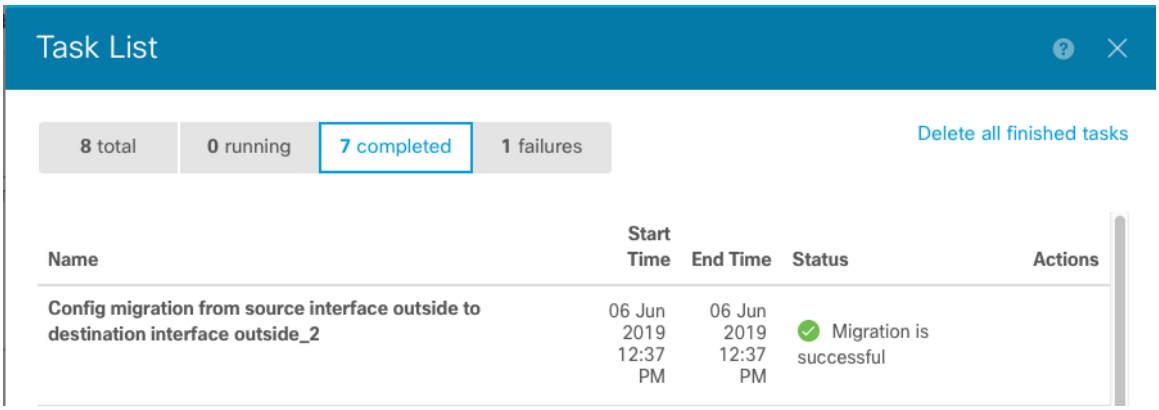
g) 从**替换接口 (Replacement Interface)** 下拉列表中选择新接口。



h) 一则消息将显示在**接口 (Interfaces)** 页面上。单击消息中的链接。



i) 检查**任务列表 (Task List)**，以确保迁移成功。



步骤 7 在 FXOS 中，从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **delete external-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

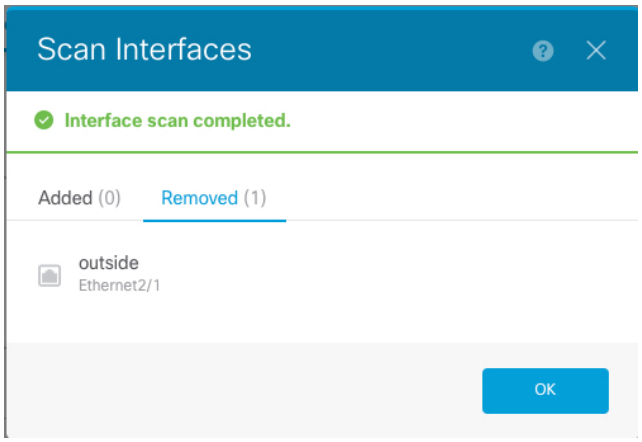
步骤 8 提交配置：

commit-buffer

提交系统配置任务。

步骤 9 再次在 FMC或 FDM 中同步接口。

图 *13: FDM* 扫描接口



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。

添加新接口或删除未使用的接口对 ASA 配置的影响很小。但是，如果在 FXOS 中删除已分配的接口（例如，如果删除网络模块、删除 EtherChannel，或将分配的接口重新分配给 EtherChannel），并且在安全策略中使用该接口，则删除操作会影响 ASA 配置。在这种情况下，ASA 配置会保留原始命令，以便您可以进行任何必要的调整。您可以在 ASA OS 中手动移除旧的接口配置。

注释 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。

开始之前

- 根据配置物理接口，第 205 页和添加 EtherChannel（端口通道），第 207 页配置您的接口，并添加任何 EtherChannel。
- 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。
- 对于群集或故障切换，请确保添加或移除所有设备上的接口。我们建议先在数据/备用设备上更改接口，然后再在控制/主用设备上更改接口。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 进入安全服务模式：

Firepower# **scope ssa**

步骤 2 编辑逻辑设备：

Firepower /ssa # **scope logical-device** *device_name*

步骤 3 从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **delete external-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

对于管理接口，请删除当前接口，然后在添加新的管理接口之前，使用 **commit-buffer** 命令确认更改。

步骤 4 将新的接口分配到逻辑设备：

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

步骤 5 提交配置：

commit-buffer

提交系统配置任务。

监控逻辑设备

- **show app**

  查看可用映像。

```
Firepower# scope ssa
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is Default
 App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    vdp        8.13.01.09-2    radware    Vm                     Application Yes
```

- **show app-instance**

  查看应用实例状态和信息。

```
firepower# scope ssa
firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- ----------- ------------ --------------- -------------
ftd        LD1        1          Enabled     Online          6.4.0.10353     6.4.0.10353
     Container   Default-Small Not Applicable  None
```

```
ftd        LD2        1          Enabled     Online          6.4.0.10353     6.4.0.10353
     Container   Default-Small Not Applicable  None
ftd        LD3        1          Enabled     Online          6.4.0.10353     6.4.0.10353
     Container   Default-Small Not Applicable  None
ftd        LD4        1          Enabled     Online          6.4.0.10353     6.4.0.1056
      Container   Default-Small Not Applicable  None
```

- **show logical-device**

  查看逻辑设备的详细信息。

```
Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
    Name       Description Slot ID    Mode       Oper State                Template Name

    ---------- ----------- ---------- ---------- ------------------------ -------------

    asa1                   1          Standalone Ok                        asa
```

- **show resource-profile system**

  显示 vDP 的资源配置文件。

```
Firepower# scope ssa
Firepower /ssa # show resource-profile system
Profile Name       App Name   App Version  Is In Use  Security Model  CPU Logical Core
 Count RAM Size (MB)  Default Profile Profile Type Description
------------------ ---------- ------------ ---------- ---------------
---------------------- -------------- --------------- ------------ -----------
DEFAULT-4110-RESOURCE
                   vdp        8.13.01.09-2 No         FPR4K-SM-12
     4          16384 Yes              System
DEFAULT-RESOURCE   vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

     6          24576 Yes              System
VDP-10-CORES       vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

    10          40960 No               System
VDP-2-CORES        vdp        8.13.01.09-2 No         all
     2           8192 No               System
VDP-4-CORES        vdp        8.13.01.09-2 No         all
     4          16384 No               System
VDP-8-CORES        vdp        8.13.01.09-2 No         FPR9K-SM-56, FPR9K-SM-44,
FPR9K-SM-36, FPR9K-SM-24, FPR4K-SM-44, FPR4K-SM-36, FPR4K-SM-24

     8          32768 No               System
```

- **show resource-profile user-defined**

  查看容器实例资源配置文件的分配情况。

```
Firepower# scope ssa
Firepower /ssa # show resource-profile user-defined
Profile Name       Is In Use  CPU Logical Core Count Description
------------------ ---------- ---------------------- -----------
bronze               No               6             low end device
```

```
gold                No              14              highest
silver              No              8               mid-level
```

- **show resource detail**

  查看应用实例的资源配置情况。

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance ftd ftd1
Firepower /ssa/slot/app-instance # show resource detail
Resource:
    Allocated Core NR: 10
    Allocated RAM (MB): 32413
    Allocated Data Disk (MB): 49152
    Allocated Binary Disk (MB): 3907
    Allocated Secondary Disk (MB): 0
```

站点间群集示例

以下示例显示支持的群集部署。

具有站点特定的 MAC 地址的跨网络 EtherChannel 路由模式示例

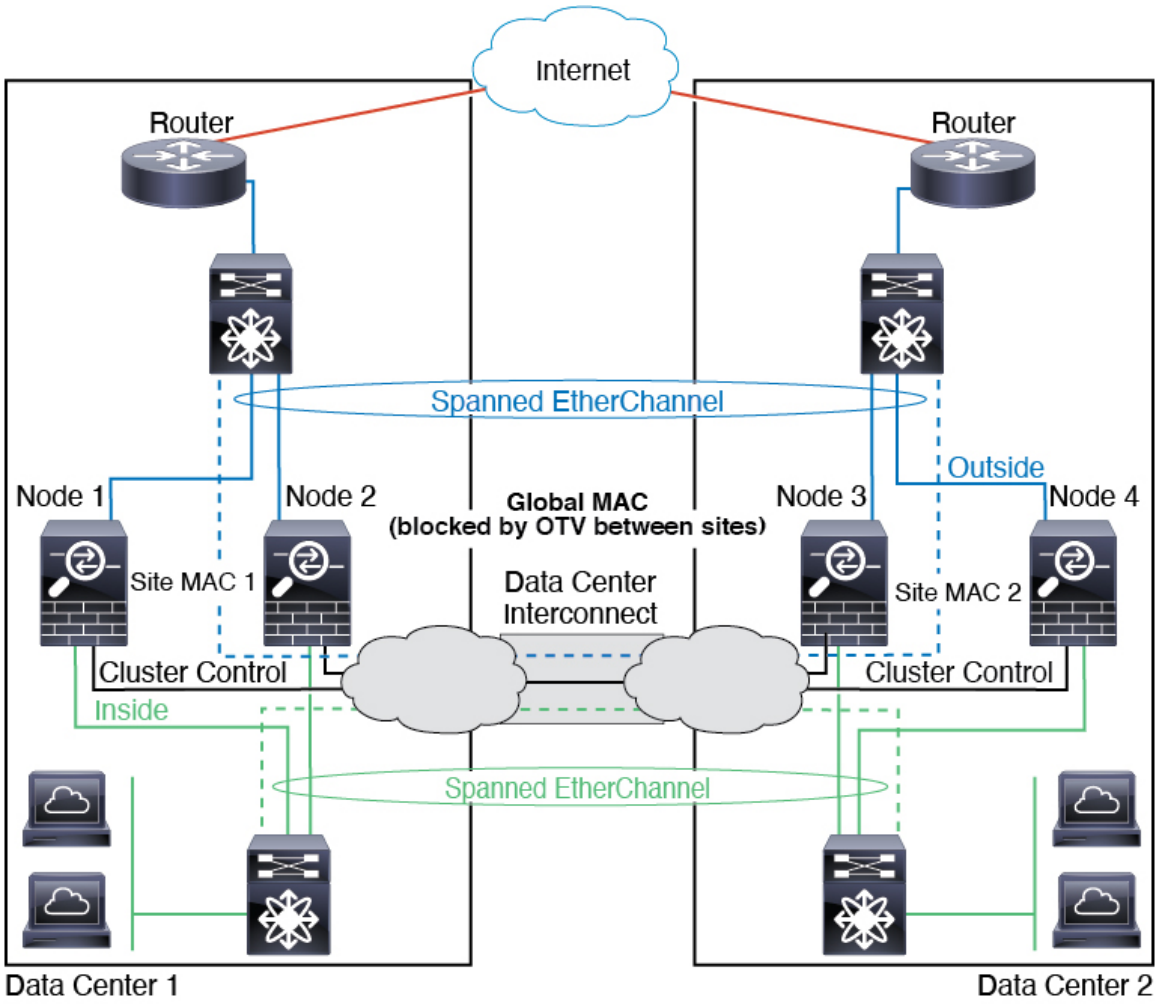
以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在每个站点上的网关路由器和内部网络之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加阻止全局 MAC 地址的过滤器，防止发往集群的流量通过 DCI 发送到另一站点。如果无法访问一个站点上的集群节点，则您必须删除过滤器，使流量能够发送到另一站点的集群节点。您应使用 VACL 来过滤全局 MAC 地址。务必禁用 ARP 检查。

集群相当于内部网络的网关。所有集群节点共享的全局虚拟 MAC 仅用于接收数据包。传出数据包使用来自每个DC集群的站点特定的MAC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。

在此场景中：

- 从集群发送的所有出口数据包使用站点 MAC 地址，并在数据中心进行本地化。
- 发送到集群的所有入口数据包使用全局MAC地址发送，因此可以被两个站点的任何节点接收；OTV 的过滤器将数据中心内的流量本地化。



跨网络 EtherChannel 透明模式南北站点间群集示例

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区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

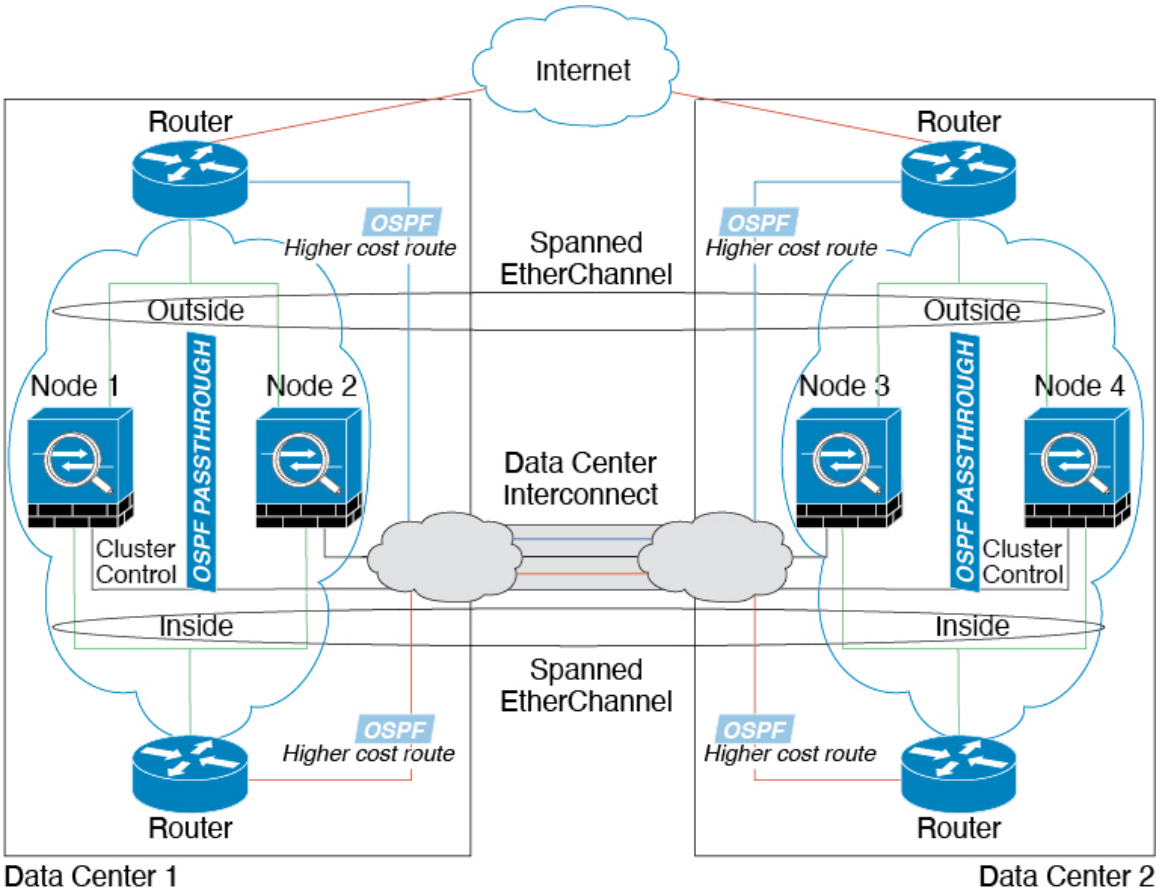
位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

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节点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

也可以选择将每个节点通过 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，尽管集群节点仍然有一个跨区以太网通道将数据中心 1 的机箱仅连接到两台本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨区以太网通道本质上是“分离的”。每个本地 VSS/vPC 都会将跨区以太网通道视作站点本地的 EtherChannel。

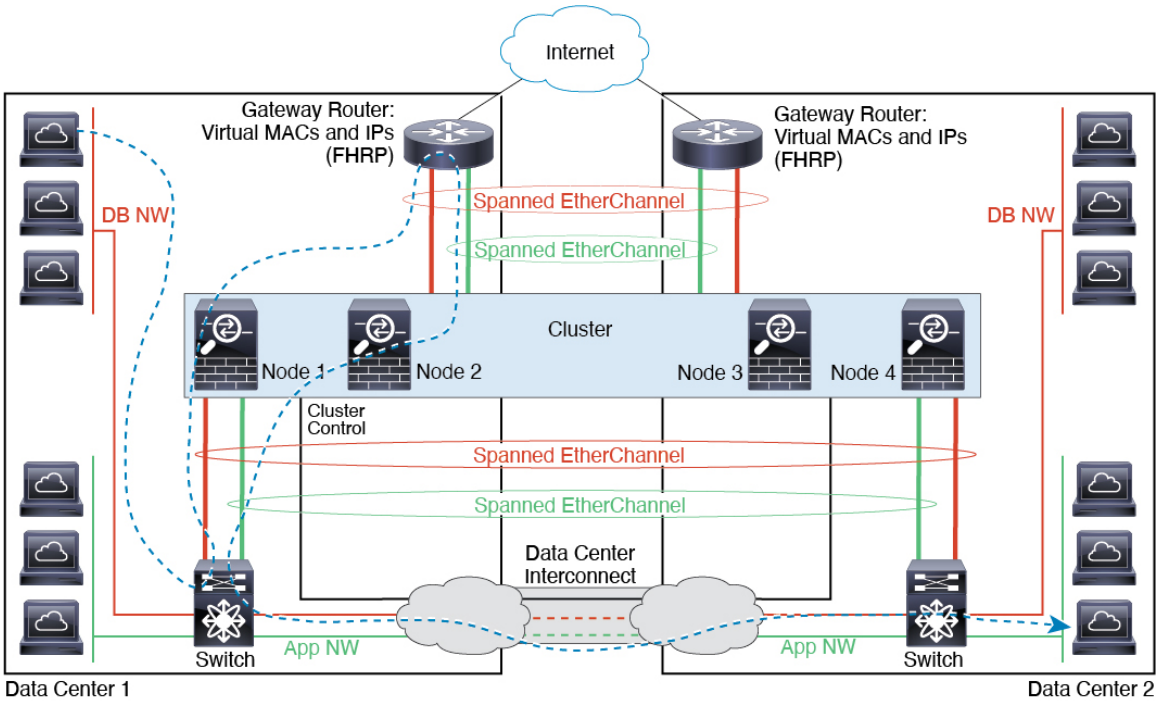


跨网络 EtherChannel 透明模式东西站点间集群示例

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 个部署在每个站点上的网关路由器和两个内部网络（应用网络和数据库网络）之间（东西插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。每个站点上的集群成员使用面向内部与外部应用网络和数据库网络的跨区以太网通道连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

每个站点上的网关路由器使用 FHRP（例如 HSRP）在每个站点上提供相同的目标虚拟 MAC 和 IP 地址。要避免 MAC 地址意外摆动，最好使用使用 **mac-address-table static** *outside_interface mac_address* 命令将网关路由器实际 MAC 地址静态添加到 ASA MAC 地址表。如果没有这些条目，当位于站点 1 的网关与位于站点 2 的网关通信时，流量可能通过 ASA 并尝试从内部接口到达站点 2，从而导致出现问题。数据 VLAN 使用重叠传输虚拟化 (OTV) 或类似技术在站点之间扩展。您必须添加过滤

器，阻止发往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，则您必须删除过滤器，使流量能够发送到另一站点的网关路由器。



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群集示例。

逻辑设备的历史记录

功能名称	平台版本	功能信息
FTD 运行链路状态与物理链路状态之间的同步	2.9.1	机箱现在可以将 FTD 运行链路状态与数据接口的物理链路状态同步。目前，只要 FXOS 管理状态为“运行”且物理链路状态为“运行”，接口将处于“运行”状态，而不考虑 FTD 应用接口管理状态。如果没有从 FTD 同步，数据接口可能在 FTD 应用完全上线之前处于“Up”物理状态，或者在您启动 FTD 关闭后的一段时间内保持“Up”状态。对于内联集，此状态不匹配可能会导致数据包丢失，因为外部路由器可能会在 FTD 可以处理流量之前开始向 FTD 发送流量。该功能默认为禁用状态并可在 FXOS 中按逻辑设备逐一启用。 **注释** 集群、容器实例或具有 Radware vDP 修饰器的 FTD 不支持此功能。此外，ASA 也不支持此功能。 新增/修改的 Firepower 机箱管理器屏幕：**逻辑设备 > 启用链路状态** 新增/修改的 FXOS 命令：**set link-state-sync enabled**、**show interface expand detail**

功能名称	平台版本	功能信息
对容器实例使用FMC的FTD配置备份和恢复	2.9.1	您现在可以在 FTD 容器实例上使用 FMC 备份/恢复工具。 新增/修改的 FMC 屏幕：**系统 (System) > 工具 (Tools) > 备份/恢复 (Backup/Restore) > 受管设备备份 (Managed Device Backup)** 新增/修改的 FTD CLI 命令： **restore** 支持的平台：Firepower 4100/9300 **注释** 需要使用 Firepower 6.7。
多实例群集	2.8.1	您现在可以使用容器实例来创建集群。在 Firepower 9300 上，必须在集群中的每个模块上包含一个容器实例。不能为每个安全引擎/模块向集群添加多个容器实例。我们建议您为每个集群实例使用相同的安全模块或机箱模型。但是，如果需要，您可以在同一集群中的不同 Firepower 9300 安全模块类型或 Firepower 4100 型号上混合和匹配容器实例。不能在同一个集群中混合使用 Firepower 9300 和 Firepower 4100。 新增/修改的命令：**set port-type cluster** **注释** 需要使用 Firepower 6.6 或更高版本。
支持使用Firepower设备管理器的FTD	2.7.1	现在，您可以部署本地 FTD 实例并指定 FDM 管理。不支持容器实例。 新增/修改的命令：**enter bootstrap-key MANAGEMENT_TYPE**、**set value LOCALLY_MANAGED**。 **注释** 需要 FTD 6.5 或更高版本。
多个容器实例的 TLS 加密加速	2.7.1	现在，在 Firepower 4100/9300 机箱上的多个容器实例（最多16个）上支持 TLS 加密加速。以前，每个模块/安全引擎只能为一个容器实例启用 TLS 加密加速。 新实例默认启用此功能。但是，升级不会在现有实例上启用加速。相反，请依次使用 **enter hw-crypto** 和 **set admin-state enabled** FXOS 命令。 新的 FXOS CLI 命令：**enter hw-crypto**、**set admin-state** 删除的 FXOS CLI 命令：**show hwCrypto**、**config hwCrypto** 删除的 FTD CLI 命令： **show crypto accelerator status** **注释** 需要 FTD 6.5 或更高版本。
Firepower 4115、4125 和 4145	2.6.1	我们推出了 Firepower 4115、4125 和 4145。 **注释** 要求 ASA 9.12(1)。Firepower 6.4.0 要求 FXOS 2.6.1.157。 未修改任何命令。

功能名称	平台版本	功能信息
Firepower 9300 SM-40、SM-48 和 SM-56 支持	2.6.1	引入了以下三个安全模块：SM-40、SM-48 和 SM-56。 注释 SM-40 和 SM-48 要求 ASA 9.12(1)。SM-56 要求 ASA 9.12(2) 和 FXOS 2.6.1.157。 所有模块都要求 FTD 6.4 和 FXOS 2.6.1.157。 未修改任何命令。
支持在同一个 Firepower 9300 上使用独立的 ASA 和 FTD 模块	2.6.1	您现在可以在同一个 Firepower 9300 上同时部署 ASA 和 FTD 逻辑设备。 注释 要求 ASA 9.12(1)。Firepower 6.4.0 要求 FXOS 2.6.1.157。 未修改任何命令。
对于 FTD 引导程序配置，您现在可以在 Firepower 机箱管理器中设置 FMC 的 NAT ID	2.6.1	您现在可以在 Firepower 机箱管理器中设置 FMC NAT ID。以前，您只能在 FXOS CLI 或 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。 新增/修改的屏幕： **逻辑设备** > **添加设备** > **设置** > **Firepower 管理中心 NAT ID**字段
支持将 SSL 硬件加速用于模块/安全引擎上的一个 FTD 容器实例	2.6.1	您现在可以启用用于模块/安全引擎上的一个容器实例的SSL硬件加速。SSL硬件加速禁用于其他容器实例，但启用于本地实例。有关详细信息，请参阅 Firepower 管理中心配置指南。 新增/修改的命令：**config hwCrypto enable**、**show hwCrypto**

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	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。 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40GB。此资源管理允许您自定义每个实例的性能。 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。 **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。 **注释** 要求使用 6.3 或更高版本的 FTD。 新增/修改的 FXOS 命令：**connect ftd** *name*、**connect module telnet**、**create bootstrap-key PERMIT_EXPERT_MODE**、**create resource-profile**、**create subinterface**、**scope auto-macpool**、**set cpu-core-count**、**set deploy-type**、**set port-type data-sharing**、**set prefix**、**set resource-profile-name**、**set vlan**、**scope app-instance ftd** *name*、**show cgroups container**、**show interface**、**show mac-address**、**show subinterface**、**show tech-support module app-instance**、**show version** 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/修改的命令：**enter bootstrap-key FIREWALL_MODE**、**set value routed** 和 **set value transparent**。
群集控制链路可自定义 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：127.2.*chassis_id*.*slot_id*。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/修改的命令：**set cluster-control-link network**

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	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。 新增/修改的命令：**enter bootstrap-key NAT_ID**
ASA 的站点间群集改进	2.1.1	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。 我们修改了以下命令：**set site-id**
Firepower 9300 上 6 个 FTD 模块的机箱内群集	2.1.1	现在，您可以对 Firepower 9300 上的 FTD 启用机箱间群集。最多可以包含 6 个模块。例如，您可以在 6 个机箱中使用 1 个模块，或者在 3 个机箱中使用 2 个模块，也可以使用最多提供 6 个模块的任意组合。
支持在 Firepower 4100 上执行 FTD 群集	2.1.1	在 FTD 群集中，最多可以群集 6 个机箱。
ASA 群集中，支持 16 个 Firepower 4100 机箱	2.0.1	在 ASA 群集中，最多可以群集 16 个机箱。
支持在 Firepower 4100 上执行 ASA 群集	1.1.4	在 ASA 群集中，最多可以群集 6 个机箱。
支持在 Firepower 9300 上的 FTD 上执行机箱内群集	1.1.4	Firepower 9300 支持使用 FTD 应用执行机箱内群集。 我们引入了以下命令：**enter mgmt-bootstrap ftd**、**enter bootstrap-key FIREPOWER_MANAGER_IP**、**enter bootstrap-key FIREWALL_MODE**、**enter bootstrap-key-secret REGISTRATION_KEY**、**enter bootstrap-key-secret PASSWORD**、**enter bootstrap-key FQDN**、**enter bootstrap-key DNS_SERVERS**、**enter bootstrap-key SEARCH_DOMAINS**、**enter ipv4 firepower**、**enter ipv6 firepower**、**set value**、**set gateway**、**set ip**、**accept-license-agreement**
Firepower 9300 上 16 个 ASA 模块的机箱内群集	1.1.3	现在，您可以对 ASA 启用机箱间群集。最多可以包含 16 个模块。例如，您可以在 16 个机箱中使用 1 个模块，或者在 8 个机箱中使用 2 个模块，也可以使用最多提供 16 个模块的任意组合。

功能名称	平台版本	功能信息
Firepower 9300 上 ASA 的机箱内群集	1.1.1	您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建群集。 我们引入了以下命令：**enter cluster-bootstrap**、**enter logical-device clustered**、**set chassis-id**、**set ipv4 gateway**、**set ipv4 pool**、**set ipv6 gateway**、**set ipv6 pool**、**set key**、**set mode spanned-etherchannel**、**set port-type cluster**、**set service-type**、**set virtual ipv4**、**set virtual ipv6**

第 12 章

安全模块/引擎管理

- 关于 FXOS 安全模块/安全引擎， 第 343 页
- 停用安全模块， 第 344 页
- 确认安全模块/引擎， 第 344 页
- 重启安全模块/引擎， 第 345 页
- 重新初始化安全模块/引擎， 第 346 页
- 使网络模块离线或在线， 第 347 页

关于 FXOS 安全模块/安全引擎

您可以使用FXOS CLI在安全模块/引擎上执行以下功能：

- 停用（仅限安全模块）- 停用安全模块后，安全模块将进入维护模式。您还可以先停用然后确认安全模块，从而纠正某些故障状态。请参阅停用安全模块， 第 344 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 344 页。
- 重启 - 重新启动 安全模块/引擎。请参阅重启安全模块/引擎， 第 345 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 eXtensible Operating System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 346 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。请参阅重启安全模块/引擎， 第 345 页。

停用安全模块

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。

注释 模块必须先停用，然后才能使用 **delete decommissioned** 命令将其删除。

过程

步骤 1 要停用模块，请输入 **decommission server** 命令：

decommission server {*ID* | *chassis-id/blade-id*}

根据承载待停用模块的设备类型，使用其模块ID（4100系列）或机箱编号和模块编号（9300设备）来标识设备。

示例：

```
FP9300-A# decommission server 1/2
FP9300-A* #
```

步骤 2 输入 **commit-buffer** 命令，以提交更改。

您可以使用 **show server decommissioned** 命令来查看已停用模块的列表。

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 进入机箱模式：

scope chassis

步骤 2 将不会替换的模块停用并以物理方式移除后，或将模块替换为另一个不同类型（即，具有不同的 PID）的模块后，输入 **acknowledge slot** 命令：

acknowledge slot

示例：

```
FP9300-A# scope chassis
FP9300-A /chassis # acknowledge slot 2
FP9300-A /chassis* #
```

步骤 3 确认配置：

commit-buffer

重启安全模块/引擎

按照以下步骤重启安全模块/引擎。

过程

步骤 1 进入 /service-profile 模式：

scope service-profile server {*chassis_id*>/*blade_id*}

示例：

```
FP9300-A # scope service-profile server 1/1
FP9300-A /org/service-profile #
```

步骤 2 输入以下 **cycle** 命令之一：

- **cycle cycle-immediate** - 立即重启模块。
- **cycle cycle-wait** - 系统等待最多五分钟以关闭模块上正在运行的应用，之后重启模块。

示例：

```
FP9300-A /org/service-profile # cycle cycle-wait
FP9300-A /org/service-profile* #
```

步骤 3 提交缓冲区，以重启模块：

commit-buffer

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 进入安全服务模式：

```
scope ssa
```

步骤 2 输入所需模块的插槽模式：

```
scope slot {slot_id}
```

示例：

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot #
```

步骤 3 输入 **reinitialize** 命令：

示例：

```
FP9300-A # scope ssa
FP9300-A /ssa # scope slot 2
FP9300-A /ssa/slot # reinitialize
Warning: Reinitializing blade takes a few minutes. All the application data on blade will
get lost. Please backup application running config files before commit-buffer.
FP9300-A /ssa/slot* #
```

步骤 4 如有必要，备份应用配置文件。

步骤 5 提交缓冲区，对模块进行重新初始化：

```
commit-buffer
```

模块重启，安全模块上的所有数据均被删除。此过程可能需要数分钟。

步骤 6 您可以使用 **show detail** 命令来查看重新格式化操作的进度、重新格式化的结果（成功或失败），以及操作失败时的错误代码。

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。
- 如果在 Firepower 8 端口 1G 铜缆 FTW 网络模块 (FPR-NM-8X1G-F FTW) 上执行网络模块在线插入和拆卸 (OIR)，请注意，网络模块 LED 将保持熄灭，直到您使用此程序使卡上线。LED 先闪烁琥珀色，然后在发现网络模块后将更改为绿色，并且应用程序上线。

注释 如果删除 FTW 网络模块并确认插槽，则系统会从 Firepower 威胁防御逻辑设备中删除网络模块端口。在这种情况下，必须先使用Firepower管理中心删除硬件旁路内联集配置，然后再重新插入网络模块。重新插入网络模块后，必须执行以下操作：

- 使用 Firepower 机箱管理器或 FXOS 命令行界面 (CLI) 将网络模块端口配置为管理在线状态。
- 将网络模块端口添加到 FTD 逻辑设备，并使用 Firepower 管理中心重新配置端口。

如果您在未确认插槽的情况下移除网络模块，则会保留内联集配置，并且端口在Firepower管理中心中显示为关闭。重新插入网络模块后，将恢复先前的配置。

有关内联集的硬件旁路的详细信息，请参阅硬件旁路对，第 189 页。

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 #
```

第 13 章

配置导入/导出

- 关于配置导入/导出，第 349 页
- 为配置导入/导出设置加密密钥，第 350 页
- 导出 FXOS 配置文件，第 351 页
- 计划自动配置导出，第 353 页
- 设置配置导出提醒，第 354 页
- 导入配置文件，第 355 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。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

- 从 FXOS 2.6.1 开始，可配置加密密钥。必须先设置加密密钥，才可导出配置。导入该配置时，必须在系统上设置相同的加密密钥。如果您修改了加密密钥确保其与导出期间使用的密钥不再匹配，导入操作将失败。请确保记录用于每个导出配置的加密密钥。
- 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内。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）会被删除并完全替换为导入文件中包含的配置。
- 除了在 RMA 场景中，我们建议您只将配置文件导入当初从中导出该配置的同一个 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，您必须在 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，请更改备份操作中的文件名或将现有文件复制到其他位置。

为配置导入/导出设置加密密钥

导出配置时，FXOS 将加密敏感数据，例如密码和密钥。

从 FXOS 2.6.1 开始，可配置加密密钥。必须先设置加密密钥，才可导出配置。导入该配置时，必须在系统上设置相同的加密密钥。如果您已修改加密密钥确保其与导出期间使用的密钥不再匹配，导入操作将失败。请确保记录用于每个导出配置的加密密钥。

如果要将从 2.6.1 以前版本 FXOS 导出的配置导入 FXOS 2.6.1 或更高版本，系统将不会检查加密密钥并将允许导入。

注释 如果要进行导入的平台软件版本与进行导出的版本不一致，则不能保证导入操作成功。我们建议您在升级或降级 Firepower 4100/9300 机箱时导出备份配置。

每当 FTD 逻辑设备升级到新软件时，使用“设置版本”(Set Version) 选项并导出备份配置，以便新的启动版本与升级版本的软件版本相匹配。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

示例：

```
Firepower# scope security
Firepower /security #
```

步骤 2 设置加密密钥：

set password-encryption-key

输入密钥：*encryption_key*

确认密钥：*encryption_key*

encryption_key 的长度必须介于 4 至 40 个字符之间。

示例：

```
Firepower /security #set password-encryption-key
Enter a key:
Confirm the key:
Firepower /security* #
```

步骤 3 提交配置：

commit-buffer

示例：

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

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。

开始之前

查看关于配置导入/导出。

过程

步骤 1 要将配置文件导出到远程服务器：

scope system

export-config *URL* **enabled commit-buffer**

使用以下语法之一，为正在导出的文件指定 URL：

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

注释　您必须指定完整路径，包括文件名。如果不指定文件名，系统将以指定的路径创建一个隐藏文件。

示例：

```
Firepower-chassis# scope system
Firepower-chassis /system # export-config scp://user1@192.168.1.2:/export/cfg-backup.xml
enabled
```

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

步骤 2 检查导出任务的状态：

scope system

scope export-config *hostname*

show fsm status

示例：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope export-config 192.168.1.2
Firepower-chassis /system/export-config # show fsm status

Hostname: 192.168.1.2

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Nop
        Previous Status: Backup Success
        Timestamp: 2016-01-03T15:32:08.636
        Try: 0
        Progress (%): 100
        Current Task:
```

步骤 3 要查看现有导出任务，请执行以下操作：

scope system

show export-config

步骤 4 要修改某个现有导出任务，请执行以下操作：

scope system

scope export-config *hostname*

使用以下命令修改导出任务：

- {**enable**|**disable**}
- **set description** <*description*>
- **set password** <*password*>
- **set port** <*port*>
- **set protocol** {**ftp**|**scp**|**sftp**|**tftp**}
- **set remote-file** *path_and_filename*
- **set user** <*user*>

步骤 5 要删除导出任务，请执行以下操作：

scope system

delete export-config *hostname*

commit-buffer

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。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

创建计划的导出任务：

a) 设置导出策略配置的范围：

scope org

scope cfg-export-policy default

b) 启用导出策略：

set adminstate enable

c) 指定与远程服务器通信时要使用的协议：

set protocol {**ftp**|**scp**|**sftp**|**tftp**}

d) 指定应存储备份文件的位置的主机名或 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。

set hostname *hostname*

e) 如果您使用的是非默认端口，请指定端口号：

set port *port*

f) 指定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：

set user *username*

g) 指定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：

set password *password*

h) 指定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，导出过程中将为该文件分配一个名称：

set remote-file *path_and_filename*

i) 指定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)”。

set schedule {**daily**|**weekly**|**bi-weekly**}

j) 将任务提交到系统配置：

commit-buffer

示例：

```
Firepower-chassis# scope org
Firepower-chassis /org # scope cfg-export-policy default
Firepower-chassis /org/cfg-export-policy # set adminstate enable
Firepower-chassis /org/cfg-export-policy* # set protocol scp
Firepower-chassis /org/cfg-export-policy* # set hostname 192.168.1.2
Firepower-chassis /org/cfg-export-policy* # set remote-file /export/cfg-backup.xml
Firepower-chassis /org/cfg-export-policy* # set user user1
Firepower-chassis /org/cfg-export-policy* # set password
Password:
Firepower-chassis /org/cfg-export-policy* # set schedule weekly
Firepower-chassis /org/cfg-export-policy* # commit-buffer
Firepower-chassis /org/cfg-export-policy #
Firepower-chassis /org/cfg-export-policy # show detail

Config Export policy:
    Name: default
    Description: Configuration Export Policy
    Admin State: Enable
    Protocol: Scp
    Hostname: 192.168.1.2
    User: user1
    Remote File: /export/cfg-backup.xml
    Schedule: Weekly
    Port: Default
    Current Task:
```

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。

默认情况下，导出提醒的启用频率为 30 天。

注释 如果提醒频率小于计划导出策略中的天数（每天、每周或每两周），您将收到导出提醒错误消息（“配置备份可能已过期(Config backup may be outdated)”）。例如，如果您的导出计划为每周且提醒频率为五天，若未在此时间内导出配置，则会每五天会发出此故障消息。

过程

要创建配置导出提醒，请执行以下操作：

scope org

scope cfg-export-reminder

set frequency 天

set adminstate {**enable**|**disable**}

commit-buffer

示例：

```
Firepower-chassis# scope org
Firepower-chassis /org # scope cfg-export-reminder
Firepower-chassis /org/cfg-export-reminder # set frequency 10
Firepower-chassis /org/cfg-export-reminder* # set adminstate enable
Firepower-chassis /org/cfg-export-reminder* # commit-buffer
Firepower-chassis /org/cfg-export-reminder # show detail

Config Export Reminder:
    Config Export Reminder (Days): 10
    AdminState: Enable
```

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。

开始之前

查看关于配置导入/导出。

过程

步骤 1 要从远程服务器导入配置文件，请执行以下操作：

scope system

import-config *URL* **enabled**

commit-buffer

使用以下语法之一，为正在导入的文件指定 URL：

- **ftp**://*username@hostname*/*path*/*image_name*

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

示例：

```
Firepower-chassis# scope system
Firepower-chassis /system # import-config scp://user1@192.168.1.2:/import/cfg-backup.xml
enabled
Warning: After configuration import any changes on the breakout port configuration will
  cause the system to reboot
Firepower-chassis /system/import-config # commit-buffer
```

步骤 2 要检查导入任务的状态，请执行以下操作：

scope system

scope import-config *hostname*

show fsm status

示例：

```
Firepower-chassis# scope system
Firepower-chassis /system # scope import-config 192.168.1.2
Firepower-chassis /system/import-config # show fsm status

Hostname: 192.168.1.2

    FSM 1:
        Remote Result: Not Applicable
        Remote Error Code: None
        Remote Error Description:
        Status: Import Wait For Switch
        Previous Status: Import Config Breakout
        Timestamp: 2016-01-03T15:45:03.963
        Try: 0
        Progress (%): 97
        Current Task: updating breakout port configuration(FSM-STAGE:sam:dme:
          MgmtImporterImport:configBreakout)
```

步骤 3 要查看现有导入任务，请执行以下操作：

scope system

show import-config

步骤 4 要修改现有导入任务，请执行以下操作：

scope system

scope import-config *hostname*

使用以下命令修改导入任务：

- {**enable**|**disable**}
- **set description** <*description*>

- **set password** <*password*>
- **set port** <*port*>
- **set protocol** {**ftp**|**scp**|**sftp**|**tftp**}
- **set remote-file** *path_and_filename*
- **set user** <*user*>

步骤 5 要删除导入任务，请执行以下操作：

scope system

delete import-config *hostname*

commit-buffer

第 14 章

故障排除

- 数据包捕获， 第 359 页
- 测试网络连接， 第 367 页
- 管理接口状态故障排除， 第 369 页
- 确定端口通道状态， 第 369 页
- 从软件故障中恢复， 第 372 页
- 从损坏的文件系统中恢复， 第 376 页
- 管理员密码未知时恢复出厂默认配置， 第 386 页
- 生成故障排除日志文件， 第 388 页
- 启用 Firepower 模块核心转储， 第 390 页
- 查找序列号 Firepower 4100/9300 机箱， 第 391 页
- 重建 RAID 虚拟驱动器， 第 392 页
- 确定 SSD 的问题， 第 393 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	端口映射	说明
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。
- 对于单宽 4x100Gbps 或 2x100Gbps 网络模块（部件号分别为 FPR-NM-4X100G 和 FPR-NM-2X100G）上的数据包捕获会话，如果模块管理状态被设为关 (off)，则捕获会话会自动禁用并出现“状态原因：未知错误。”(Oper State Reason: Unknown Error.)。您必须在管理状态被再次设为开 (on) 后重新启动捕获会话。

  对于所有其他网络模块，数据包捕获会话会在模块管理状态更改期间继续。
- 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 进入数据包捕获模式：

Firepower-chassis # **scope packet-capture**

步骤 2 创建过滤器；请参阅配置数据包捕获的过滤器，第 364 页。

可以将过滤器应用于数据包捕获会话中包含的任何接口。

步骤 3 要创建或编辑数据包捕获会话：

Firepower-chassis /packet-capture # **enter session** *session_name*

步骤 4 指定要用于此数据包捕获会话的缓冲区大小：

Firepower-chassis /packet-capture/session* # **set session-memory-usage** *session_size_in_megabytes*

指定的缓冲区大小必须介于 1 和 2048 MB 之间。

步骤 5 指定要为此数据包捕获会话捕获的数据包长度：

Firepower-chassis /packet-capture/session* # **set session-pcap-snaplength** *session_snap_length_in_bytes*

指定的 Snap 长度必须在 64 到 9006 个字节之间。如果未配置会话 Snap 长度，则默认的捕获长度为 1518 个字节。

步骤 6 指定此数据包捕获会话中应包含的物理源端口。

您可以从多个端口捕获，也可以在同一数据包捕获会话期间同时从物理端口和应用端口捕获。将为会话中包含的每个端口创建单独的数据包捕获文件。无法捕获整个 EtherChannel 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 EtherChannel，则无法捕获成员接口上的数据包。

注释 要从数据包捕获会话中删除端口，请使用 **delete** 代替下面所列命令中的 **create**。

a) 指定物理端口。

Firepower-chassis /packet-capture/session* # **create** {**phy-port | phy-aggr-port**} *port_id*

示例：

```
Firepower-chassis /packet-capture/session* # create phy-port Ethernet1/1
Firepower-chassis /packet-capture/session/phy-port* #
```

b) 捕获子接口上的数据包。

Firepower-chassis /packet-capture/session/phy-port* # **set subinterface** *id*

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。不支持 Etherchannel 的子接口。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。

示例：

```
Firepower-chassis /packet-capture/session/phy-port* # set subinterface 100
Firepower-chassis /packet-capture/session/phy-port* #
```

c) 对于容器实例，请指定容器实例名称。

Firepower-chassis /packet-capture/session/phy-port* # **set app-identifier** *instance_name*

示例：

```
Firepower-chassis /packet-capture/session/phy-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/phy-port* #
```

d) 指定应用类型。

Firepower-chassis /packet-capture/session/phy-port* # **set app** *name*

示例：

```
Firepower-chassis /packet-capture/session/phy-port* # set app ftd
Firepower-chassis /packet-capture/session/phy-port* #
```

e) （可选） 应用所需的过滤器。

Firepower-chassis /packet-capture/session/phy-port* # **set** {**source-filter**} *filtername*

注释 要从端口删除过滤器，请使用 **set source-filter ""**。

f) 根据需要重复上述步骤，添加所需的所有端口。

步骤 7 指定此数据包捕获会话中应包含的应用源端口。

您可以从多个端口捕获，也可以在同一数据包捕获会话期间同时从物理端口和应用端口捕获。将为会话中包含的每个端口创建单独的数据包捕获文件。

注释 要从数据包捕获会话中删除端口，请使用 **delete** 代替下面所列命令中的 **create**。

a) 指定应用端口。

Firepower-chassis /packet-capture/session* # **create app_port** *module_slot link_name interface_name app_name*

Syntax Description

module_slot	在其中安装了应用程序的安全模块。
link_name	引用接口的任何用户描述性名称，例如，link1、inside_port1 等。
interface_name	连接到需要捕获数据包的应用程序的接口，例如，Ethernet1/1、Ethernet2/2
app_name	安装在模块 -ftd、asa 上的应用程序

b) 对于容器实例，请指定容器实例名称。

Firepower-chassis /packet-capture/session/app-port* # **set app-identifier** *instance_name*

示例：

```
Firepower-chassis /packet-capture/session/app-port* # set app-identifier ftd-instance1
Firepower-chassis /packet-capture/session/app-port* #
```

Syntax Description

instance_name	需要数据包捕获的应用程序实例的名称，即本地或容器

c) （可选） 应用所需的过滤器。

Firepower-chassis /packet-capture/session/phy-port* # **set** {**source-filter**} *filtername*

Syntax Description

filtername	数据包捕获范围下“create filter”命令的过滤器名称

注释 要从端口删除过滤器，请使用 **set source-filter ""**。

d) 根据需要重复上述步骤，添加所需的所有应用端口。

步骤 8 如果想要现在开始数据包捕获会话：

Firepower-chassis /packet-capture/session* # **enable**

默认情况下，新建的数据包捕获会话处于禁用状态。提交更改后，明确启用会话会激活数据包捕获会话。如果有其他会话正处于活动状态，启用会话将生成错误。您必须禁用已处于活动状态的数据包捕获会话，才能启用此会话。

步骤 9 将任务提交到系统配置：

Firepower-chassis /packet-capture/session* # **commit-buffer**

如果已启用数据包捕获会话，系统将开始捕获数据包。要从会话下载 PCAP 文件，您需要先停止捕获。

示例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create session asa1inside
Firepower-chassis packet-capture/session # set session-memory-usage 256
Firepower-chassis packet-capture/session* # create phy-port Ethernet3/1
Firepower-chassis packet-capture/session* # create phy-aggr-port Ethernet2/1/1
Firepower-chassis packet-capture/session* # create app-port 1 link1 Ethernet 1/1 asa
Firepower-chassis packet-capture/session* # exit
Firepower-chassis packet-capture* # create filter interface1vlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcIP 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcPort 80
Firepower-chassis packet-capture/filter* # set destIP 10.10.10.10
Firepower-chassis packet-capture/filter* # set destPort 5050
Firepower-chassis packet-capture/filter* # exit
Firepower-chassis packet-capture/session* # scope phy-port Ethernet3/1
Firepower-chassis packet-capture/session/phy-port* # set src-filter interface1vlan100
Firepower-chassis packet-capture/session/phy-port* # exit
Firepower-chassis packet-capture/session* # scope app-port 1 link1 Ethernet1/1 asa
Firepower-chassis packet-capture/session/app-port* # set src-filter interface1vlan100
Firepower-chassis packet-capture/session/app-port* # exit
Firepower-chassis packet-capture/session* # enable
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

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 进入数据包捕获模式：

Firepower-chassis # **scope packet-capture**

步骤 2 要创建新的数据包捕获过滤器：

Firepower-chassis /packet-capture # **create filter** *filter_name*

要编辑现有的数据包捕获过滤器：

Firepower-chassis /packet-capture # **enter filter** *filter_name*

要删除现有的数据包捕获过滤器：

Firepower-chassis /packet-capture # **delete filter** *filter_name*

步骤 3 通过设置一个或多个过滤器属性，指定过滤器的详细信息：

Firepower-chassis /packet-capture/filter* # **set** <*filterprop filterprop_value*

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。

表 *20:* 支持的过滤器属性

ivlan	内部 VLAN ID （进入端口时的数据包 VLAN）
ovlan	外部 VLAN ID（Firepower 4100/9300 机箱添加的 VLAN）
srcip	源 IP 地址 (IPv4)
destip	目的 IP 地址 (IPv4)
srcipv6	源 IP 地址 (IPv6)
destipv6	目的 IP 地址 (IPv6)
srcport	源端口号
destport	目的端口号

protocol	IP 协议 [IANA 定义的协议值，采用十进制格式]
ethertype	以太网协议类型 [IANA 定义的以太网协议类型值，采用十进制格式。例如：IPv4＝2048，IPv6 = 34525，ARP = 2054，SGT = 35081]
srcmac	源 Mac 地址
destmac	目的 MAC 地址

示例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # create filter interface1vlan100
Firepower-chassis packet-capture/filter* # set ivlan 100
Firepower-chassis packet-capture/filter* # set srcip 6.6.6.6
Firepower-chassis packet-capture/filter* # set srcport 80
Firepower-chassis packet-capture/filter* # set destip 10.10.10.10
Firepower-chassis packet-capture/filter* # set destport 5050
Firepower-chassis packet-capture/filter* # commit-buffer
```

启动和停止数据包捕获会话

过程

步骤 1 进入数据包捕获模式：

Firepower-chassis # **scope packet-capture**

步骤 2 输入您要启动或停止数据包捕获会话的范围：

Firepower-chassis /packet-capture # **enter session** *session_name*

步骤 3 要启动数据包捕获会话：

Firepower-chassis /packet-capture/session* # **enable** [append | overwrite]

注释 您无法在另一个会话运行时启动数据包捕获会话。

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 4 要停止数据包捕获会话：

Firepower-chassis /packet-capture/session* # **disable**

步骤 5 将任务提交到系统配置：

Firepower-chassis /packet-capture/session* # **commit-buffer**

如果已启用数据包捕获会话，会话中所包含的接口的 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）。

示例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # scope session asa1inside
Firepower-chassis packet-capture/session # enable append
Firepower-chassis packet-capture/session* # commit-buffer
Firepower-chassis packet-capture/session #
```

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。

PCAP 文件将存储到 `workspace://packet-capture` 目录，并使用以下命名约定：

`workspace://packet-capture/session-<id>/<session-name>-<interface-name>.pcap`

过程

要从 Firepower 4100/9300 机箱复制 PCAP 文件：

注释 您应先停止数据包捕获会话，然后从该会话下载 PCAP 文件。

a) 连接到本地管理：

Firepower-chassis # **connect localmgmt**

b) 复制 PCAP 文件：

copy *pcap_file copy_destination*

示例

```
Firepower-chassis# connect localmgmt
# copy workspace:/packet-capture/session-1/test-ethernet-1-1-0.pcap
scp://user@10.10.10.1:/workspace/
```

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 进入数据包捕获模式：

Firepower-chassis # **scope packet-capture**

步骤 2 要删除特定的数据包捕获会话：

Firepower-chassis /packet-capture # **delete session** *session_name*

步骤 3 要删除所有不活动的数据包捕获会话：

Firepower-chassis /packet-capture # **delete-all-sessions**

步骤 4 将任务提交到系统配置：

Firepower-chassis /packet-capture* # **commit-buffer**

示例

```
Firepower-chassis# scope packet-capture
Firepower-chassis packet-capture # delete session asa1inside
Firepower-chassis packet-capture* # commit-buffer
Firepower-chassis packet-capture #
```

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 **traceroute** 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 **traceroute6** 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。
- **traceroute** 和 **traceroute6** 命令可在 `local-mgmt` 模式下使用。
- **traceroute** 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。

管理接口状态故障排除

在初始化和配置期间，如果您怀疑管理接口由于某种原因未打开（例如，无法访问机箱管理器），请使用 `local-mgmt` shell 中的 **show mgmt-port** 命令来确定管理接口的状态。

注释 请勿在 `fxos` shell 中使用 **show interface brief** 命令，因为它当前显示的信息不正确。

过程

步骤 1 通过输入以下命令连接到 `local-mgmt` 模式：

- **connect local-mgmt**

示例：

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

步骤 2 使用 **show mgmt-port** 命令确定管理接口的状态。

示例：

```
firepower(local-mgmt)# show mgmt-port
eth0      Link encap:Ethernet  HWaddr b0:aa:77:2f:f0:a9
          inet addr:10.89.5.14  Bcast:10.89.5.63  Mask:255.255.255.192
          inet6 addr: fe80::b2aa:77ff:fe2f:f0a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3210912 errors:0 dropped:0 overruns:0 frame:0
          TX packets:705434 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1648941394 (1.5 GiB)  TX bytes:138386379 (131.9 MiB)

firepower(local-mgmt)#
```

您还可以使用 **show mgmt-ip-debug** 命令；但它会生成大量的接口配置信息。

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 207 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 FAT32 格式的 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 69 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，请参阅使用控制台端口的初始配置，第 12 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 69 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 #
```

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 eXtensible Operating System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

管理员密码未知时恢复出厂默认配置

此程序可将 Firepower 4100/9300 机箱系统恢复为其默认配置设置，包括管理员密码。当管理员密码未知时，可遵照此程序重置设备上的配置。此程序也会清除所有已安装的逻辑设备。

注释 此程序需要控制台访问 Firepower 4100/9300 机箱。

过程

步骤 1 使用所提供的控制台电缆将 PC 连接到控制台端口，并使用已设置为 9600 波特、8 个数据位、无奇偶校验、1 个停止位、无流量控制功能的终端仿真器连接到控制台。有关控制台电缆的详细信息，请参阅《思科 Firepower 9300 硬件安装指南》。

步骤 2 启动设备。系统显示以下提示时，按 ESC 键停止启动。

示例：

```
!!  Rommon image verified successfully  !!

Cisco System ROMMON, Version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015  by Cisco Systems, Inc.

Current image running: Boot ROM0
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: 00:00:00:00:00:00

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
 bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
rommon 1 >
```

步骤 3 记下启动和系统映像名称：

示例：

```
bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

步骤 4 加载启动映像：

rommon 1 > **boot** *kickstart_image*

示例：

```
rommon 1 > boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.3.14.69.SPA
 !! Kickstart Image verified successfully !!
```

```
Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Tue Nov 24 12:10:28 PST 2015
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
INIT: POST INIT Starts at Wed Jun 1 13:46:33 UTC 2016
can't create lock file /var/lock/mtab~302: No such file or directory (use -n flag to override)
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2015, 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. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch(boot)#
```

步骤 5 输入配置终端模式：

switch(boot) # **config terminal**

示例：

```
switch(boot)#
switch(boot)# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

步骤 6 重置密码并确认更改：

switch(boot) (config) # **admin-password erase**

注释 此步骤会清除所有配置并将系统恢复为其默认配置设置。

示例：

```
switch(boot)(config)# admin-password erase
Your password and configuration will be erased!
Do you want to continue? (y/n)  [n] y
```

步骤 7 退出配置终端模式：

switch(boot) (config) # **exit**

步骤 8 加载此程序第 3 步中提到的系统映像，然后使用初始配置，第 11 页任务流从头配置您的系统。

switch(boot) # **load** *system_image*

示例：

```
switch(boot)# load bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA

Uncompressing system image: bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.3.14.69.SPA
```

生成故障排除日志文件

您可以生成日志文件来帮助进行故障排除，或在需要时发送至思科 TAC。

过程

步骤 1 连接到本地管理模式：

Firepower# connect local-mgmt

步骤 2 （可选）输入以下命令：

Firepower(local-mgmt)# show tech-support ?

命令输出中显示您可以为其生成故障排除文件的组件。

示例：

```
  chassis  Chassis
  fprm     Firepower Platform Management
  module   Security Module
```

步骤 3 运行以下命令以生成故障排除文件：

Firepower(local-mgmt)# show tech-support <component keyword>

请确保为要生成其故障排除文件的组件提供所需的关键字。例如， **module**关键字会为安全模块生成故障排除文件。

请确保为要生成其故障排除文件的组件提供所需的关键字。例如， **fprm**关键字会为 Firepower 平台管理生成故障排除文件。

表 *21:* 组件和命令示例

组件	命令示例
机箱	**Firepower (local-mgmt)# show tech-support chassis 1**
Firepower 平台管理	**fprm** 选项在 2.8(1) 版本中已被弃用，不能再使用。
安全模块	**Firepower (local-mgmt)# show tech-support module 1**

示例：

```
Firepower(local-mgmt)# show tech-support chassis 1 detail

The show tech support file will be located at
/workspace/techsupport/20191105041703_firepower-9300_BC1_all.tar

Initiating tech-support information task on FABRIC A ...
```

```
Initiating tech-support information task on Chassis 1 Fabric Extender 1 ...
Initiating tech-support information task on Chassis 1 CIMC 1 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/1 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/1 ...
Initiating tech-support information task on Chassis 1 CIMC 2 ...
Initiating tech-support information task on Adaptor 1 on Chassis/Server 1/2 ...
Initiating tech-support information task on Adaptor 2 on Chassis/Server 1/2 ...
Completed initiating tech-support subsystem tasks (Total: 8)
Waiting (Timeout: 900 Elapsed: 30) for completion of subsystem tasks (1/8).
Waiting (Timeout: 900 Elapsed: 50) for completion of subsystem tasks (2/8).
Waiting (Timeout: 900 Elapsed: 70) for completion of subsystem tasks (5/8).
Waiting (Timeout: 900 Elapsed: 90) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 110) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 130) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 150) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 170) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 190) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 210) for completion of subsystem tasks (6/8).
Waiting (Timeout: 900 Elapsed: 230) for completion of subsystem tasks (7/8).
--More--
The detailed tech-support information is located at workspace:///techsupport/201--More--
91105041703_firepower-9300_BC1_all.tar
```

同样，您也可以从安全模块生成故障排除文件。

在生成故障排除文件后，您可以在工作空间中找到该文件。

步骤 4 运行以下命令以确认文件是否生成：

dir workspace:/techsupport

示例：

```
1  34426880 Mar 05 13:10:05 2019 20190305130133_firepower-9300_FPRM.tar
1  56995840 Aug 27 05:30:37 2019 20190827052331_firepower-9300_FPRM.tar
1  56842240 Aug 27 12:42:42 2019 20190827123535_firepower-9300_FPRM.tar
1  87623680 Sep 17 06:27:57 2019 20190917062046_firepower-9300_FPRM.tar
1  87756800 Sep 17 10:22:38 2019 20190917101527_firepower-9300_FPRM.tar
1 152627200 Nov 05 04:30:10 2019 20191105041703_firepower-9300_BC1_all.tar

Usage for workspace://
3999125504 bytes total
476835840 bytes used
3317436416 bytes free
```

注释 如果您使用所有三个参数（fprm、机箱和模块）成功生成文件，则应在 **/techsupport** 目录中看到它们。

步骤 5 运行以下命令。

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> ?

输出结果中显示支持的协议，用于允许将故障排除文件从 FXOS 复制到您的本地计算机。您可以使用任何受支持的协议。

示例：

```
Firepower(local-mgmt)# copy workspace:/techsupport/
20191105041703_firepower-9300_BC1_all.tar ?
  ftp:        Dest File URI
  http:       Dest File URI
  https:      Dest File URI
  scp:        Dest File URI
```

```
sftp:       Dest File URI
tftp:       Dest File URI
usbdrive:   Dest File URI
volatile:   Dest File URI
workspace:  Dest File URI
```

在将文件从 FXOS 复制到计算机之前，请确保满足以下前提条件：

- 本地计算机上的防火墙接受任何必要端口上的传入连接。例如，如果通过安全外壳复制文件，则计算机必须允许来自任何相关端口（如端口 22）的连接。
- 您的计算机必须运行安全复制 (SCP) 服务或任何受支持的协议，以允许复制文件。您可以在互联网上找到各种 SSH 或 SCP 服务器软件。但是，思科不支持安装和配置任何特定 SCP 服务器。

步骤 6 运行以下命令以复制文件。

Firepower(local-mgmt)# copy workspace:/techsupport/<troubleshooting file name> <supported file transfer protocol>://<username>@<destination IP address>

示例：

```
firepower-9300(local-mgmt)# copy workspace:/techsupport/
20191105041703_firepower-9300_BC1_all.tar scp:/xyz@192.0.2.1
```

启用 Firepower 模块核心转储

在 Firepower 模块上启用核心转储有助于在系统崩溃时进行故障排除，或者应要求发送到思科 TAC。

过程

步骤 1 连接到所需的 Firepower 模块；例如：

Firepower# connect module 1 console

步骤 2 （可选）输入以下命令以查看当前的核心转储状态：

Firepower-module1> show coredump detail

命令输出会显示当前核心转储状态信息，包括是否启用核心转储压缩。

示例：

```
Firepower-module1>show coredump detail
Configured status: ENABLED.
ASA Coredump: ENABLED.
Bootup status: ENABLED.
Compress during crash: DISABLED.
```

注释 此命令仅在 Firepower 设备上运行 ASA 逻辑设备时可用，而在 Firepower 设备上运行 FTD 逻辑设备时不可用。

步骤 3 使用 **config coredump** 命令可启用或禁用核心转储，以及在崩溃期间启用或禁用核心转储压缩。

- 使用 **config coredump enable** 在崩溃期间创建核心转储。
- 使用 **config coredump disable** 在崩溃期间禁用核心转储创建。
- 使用 **config coredump compress enable** 来启用核心转储压缩。
- 使用 **config coredump compress disable** 来禁用核心转储压缩。

示例：

```
Firepower-module1>config coredump enable
Coredump enabled successfully.
ASA coredump enabled, do 'config coredump disableAsa' to disable
Firepower-module1>config coredump compress enable
WARNING: Enabling compression delays system reboot for several minutes after a system
failure.  Are you sure? (y/n):
y
Firepower-module1>
```

注释 核心转储文件会消耗磁盘空间，如果空间不足且未启用压缩，则即使启用了核心转储，也无法保存核心转储文件。

查找序列号 Firepower 4100/9300 机箱

您可以找到有关 Firepower 4100/9300 机箱 及其序列号的详细信息。请注意，Firepower 4100/9300 机箱 的序列号与逻辑设备的序列号不同。

过程

步骤 1 输入机箱范围：

scope chassis

示例：

```
Firepower# scope chassis
Firepower /chassis #
```

步骤 2 查看清单详细信息：

show inventory

示例：

```
Firepower /chassis # show inventory
```

输出中显示序列号和其他详细信息。

```
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-C9300-AC    Cisco Systems Inc JMX1950196H 0
```

重建 RAID 虚拟驱动器

RAID（独立磁盘冗余阵列）是多个独立物理驱动器的阵列或组，旨在提供高性能和容错能力。驱动器组是一组物理驱动器。这些驱动器在称为虚拟驱动器的分区中进行管理。

与单驱动器存储系统相比，RAID驱动器组可提高数据存储可靠性和容错能力。通过从剩余驱动器重建缺失数据，可以防止驱动器故障导致的数据丢失。RAID可提高I/O性能并提高存储子系统的可靠性。

如果一个 RAID 驱动器发生故障或离线，则 RAID 虚拟驱动器会被视为处于降级状态。使用此程序来验证 RAID 虚拟驱动器是否处于降级状态，并在必要时临时将本地磁盘配置保护策略设置为“否”(no) 以便重新构建它。

注释 当您将本地磁盘配置保护策略设置为“否”(no) 时，磁盘上的所有数据都会被销毁。

过程

步骤 1 检查 RAID 驱动器状态。

1. 进入机箱模式：

   scope chassis

2. 进入服务器模式：

   scope server 1

3. 进入 RAID 控制器：

   scope raid-controller 1 sas

4. 查看虚拟驱动器：

   show virtual-drive

   如果 RAID 虚拟驱动器被降级，则可操作性显示为 **Degraded**。例如：

```
Virtual Drive:
    ID: 0
    Block Size: 512
    Blocks: 3123046400
    Size (MB): 1524925
    Operability: Degraded
Presence: Equipped
```

步骤 2 将本地磁盘配置策略保护设置为“否”(no) 以重建 RAID 驱动器。注意 - 完成这一步后，磁盘上的所有数据都将被销毁。

1. 输入组织范围：

   scope org

2. 输入本地磁盘配置策略范围：

   scope local-disk-config-policy ssp-default

3. 将保护设为“否”(no)：

   set protect no

4. 提交配置：

   commit-buffer

步骤 3 等待 RAID 驱动器重建。检查 RAID 重建状态：

scope chassis 1

show server

当 RAID 驱动器重建成功时，插槽的总体状态会显示为 **Ok**。例如：

示例：

```
Server:
    Slot    Overall Status        Service Profile
    ------- --------------------- ---------------
          1 Ok                    ssp-sprof-1
```

步骤 4 RAID 驱动器重建成功后，将本地磁盘配置策略保护恢复为“是”(yes)。

1. 输入组织范围：

   scope org

2. 输入本地磁盘配置策略范围：

   scope local-disk-config-policy ssp-default

3. 将保护设为“否”(no)：

   set protect yes

4. 提交配置：

   commit-buffer

确定 SSD 的问题

使用以下程序来收集信息并确定设备上安装的 SSD 可能存在的问题。SSD 问题的一个示例症状是数据管理引擎 (DME) 进程无法启动。

如果以下日志记录文件的输出表明 SSD 存在问题，则需要对管理引擎模块执行 RMA（请参阅 https://www.cisco.com/c/en/us/buy/product-returns-replacements-rma.html）。

过程

步骤 1 连接到 FXOS 命令 shell：

connect fxos

步骤 2 显示 nvram 日志记录文件：

show logging nvram

错误输出示例：

```
2020 Oct 22 13:03:26 MDCNGIPSAPL02 %$ VDC-1 %$ Oct 22 13:03:25 %KERN-2-SYSTEM_MSG:
[28175880.598580] EXT3-fs error (device sda4): ext3_get_inode_loc: unable to read inode
block - inode=14, block=6
```

步骤 3 显示日志记录文件：

show logging logfile

错误输出示例：

```
   2020 Oct 21 21:11:25  (none) kernel: [28118744.718445] EXT3-fs error (device sda4):
ext3_get_inode_loc: unable to read inode block - inode=14, block=6
```

索引

A

安全模块 344–347
  确认 344
  停用 344
  重新初始化 346
  重置 345
  离线 347
  在线 347

B

本地身份验证的用户 52, 60–62, 66
  更改间隔 60
  清除密码历史记录 66
  无更改间隔 61
  密码历史记录计数 62
  密码配置文件 52

C

创建数据包捕获会话 360
出厂默认配置 114
  恢复 114
初始配置 11–12, 14
  使用控制台端口 12
  使用管理端口 14

D

导出配置 349
导入配置 349
低接触调配 14
  使用管理端口 14
对象命令 8
待处理命令 9
端口通道 207, 369
  配置 207
  status 369
登录前横幅 110–112
  创建 110
登录前横幅 (续)
  删除 112
  修改 111

F

访问命令行界面 18
分支电缆 212
  配置 212
分支端口 212

G

固件 78
  升级 78
高级任务列表 11
管理界面 369
  status 369
管理 IP 地址 99
  不断变化的 99
关闭 Firepower 机箱 114
故障排除 369, 388, 390
  generating coredumps 390
  生成日志文件 388
  管理界面 369
  端口通道状态 369

H

恢复出厂默认配置 114
会话超时 55–56

J

机箱 2, 11
  初始配置 11
  监控运行状况 2
集群 236, 242–243, 274–277, 279, 288
  创建 242, 279, 288
  关于 274

集群 *(续)*
群集控制链路 **275–276**
redundancy **276**
size **275**
设备本地 EtherChannel，在交换机上配置 **243**
management **277**
网络 **277**
成员要求 **236**
软件要求 **236**
spanning-tree portfast **242**
升级软件 **236**
加密密钥 **350**
接口 **179, 205**
配置 **179, 205**
属性 **179, 205**
监控机箱运行状况 **2**

K

控制台 **55–56**
timeout **55–56**

L

连接到逻辑设备 **322**
历史记录, 密码 **52**
逻辑设备 **76, 78, 242, 246, 252, 279, 288, 322, 324, 326**
手动降级映像版本 **78**
连接到 **322**
创建集群 **242, 279, 288**
创建独立 **246, 252**
删除应用实例 **326**
删除 **324**
退出连接 **322**
更新映像版本 **76**

M

命令行界面 **18**
访问 **18**
命令模式 **5**
命令 **9**
history **9**
密钥环 **141–144, 147–148, 152**
创建 **142**
关于 **141**
证书请求 **143–144**
删除 **152**
导入证书 **148**
重新生成 **142**
受信任点 **147**
密码配置文件 **52, 60–62, 66**
关于 **52**
更改间隔 **60**
清除密码历史记录 **66**
无更改间隔 **61**
密码历史记录计数 **62**
密码 **49, 52–53, 57**
更改间隔 **53**
指导原则 **49**
历史记录计数 **52**
强度检查 **57**

P

配置 **142–144, 147–148**
HTTPS **142–144, 147–148**
配置导入/导出 **349–350**
加密密钥 **350**
指导原则 **349**
限制 **349**
平台捆绑包 **69–70, 72–73**
关于 **69**
从 Cisco.com 下载 **70**
下载到 Firepower 安全设备 **70**
升级 **73**
验证完整性 **72**
配置文件 **52**
password **52**

Q

启用 **134**
SNMP **134**
确认安全模块 **344**

R

日期和时间 **117**
配置 **117**
日期 **118, 123**
手动设置 **123**
查看 **118**
日志文件 **388**
生成 **388**
软件故障 **372**
恢复 **372**
任务流 **11**

S

身份验证 53
  default 53
思科安全包 69–70, 74
  关于 69
  从 Cisco.com 下载 70
  下载到 Firepower 安全设备 74
社区，SNMP 134
损坏的文件系统 376
  恢复 376
删除数据包捕获会话 366
设备名称 104
  不断变化的 104
实施密码强度 57
受管对象 5
数据包捕获 359–360, 364–366
  创建数据包捕获会话 360
  删除数据包捕获会话 366
  下载 PCAP 文件 366
  filter 364
  启动数据包捕获会话 365
  停止数据包捕获会话 365
使安全模块离线或在线 347
时区 118, 120, 123
  setting 118, 120, 123
受信任点 141, 147, 153
  创建 147
  关于 141
  删除 153
升级固件 78

T

通信服务 134, 142–144, 147–148
  HTTPS 142–144, 147–148
  SNMP 134
停用安全模块 344
退出逻辑设备连接 322
通知 131
  关于 131

W

系统日志 168
  配置本地目的 168
  配置本地源 168
  配置远程目的 168
系统恢复 372, 376
威胁防御映像 74
  下载到 Firepower 安全设备 74
威胁防御 242, 252, 288, 322, 324, 326
  连接到 322
  创建集群 242, 288
  创建独立威胁防御逻辑设备 252
  删除逻辑设备 324
  删除应用实例 326
  退出连接 322

X

下载数据包捕获文件 366
许可证颁发机构 38
许可证 38
  注册 38
陷阱 131, 135, 137
  创建 135
  关于 131
  删除 137

Y

映像版本 76
  更新 76
映像 69–70, 72–74
  从 Cisco.com 下载 70
  下载到 Firepower 安全设备 70, 74
  管理 69
  升级 Firepower 可扩展操作系统平台捆绑包 73
  验证完整性 72
远程用户的角色策略 57
用户账户 52, 60–62, 66
  密码配置文件 52, 60–62, 66
用户 10, 47–49, 52–53, 57, 60–63, 65–66, 137, 139
  创建 63
  激活 66
  CLI 会话限制 10
  停用 66
  默认身份验证 53
  删除 65
  本地身份验证 52, 60–62, 66
  管理 47
  命名准则 48
  密码准则 49
  密码强度检查 57
  远程，角色策略 57
  角色 52
  SNMP 137, 139

Z

AAA 156–157, 160–164, 166
  LDAP 提供程序 156–157, 160
  RADIUS 提供程序 161–163
  TACACS+ 提供程序 164, 166
账户 52, 60–62, 66
  本地身份验证 52, 60–62, 66
asa 映像 69–70, 74
  关于 69
  从 Cisco.com 下载 70
  下载到 Firepower 安全设备 74
asa 76, 242, 246, 279, 322, 324, 326
  连接到 322
  创建集群 242, 279
  创建独立 asa 逻辑设备 246
  删除逻辑设备 324
  删除应用实例 326
  退出连接 322
  更新映像版本 76
authNoPriv 132
authPriv 132
banner 110–112
  pre-login 110–112
BMC 映像版本 78
  手动降级 78
call home 36
  配置 HTTP 代理 36
certificate 141
  关于 141
CLI 会话限制 10
CLI，请参阅 命令行界面
coredumps 390
  生成 390
CSP，请参阅 思科安全包
DNS 170
erase 115
  配置 115
  secure 115
Firepower 机箱 2, 11, 113–114
  初始配置 11
  监控运行状况 2
  断开 114
  重新启动 113
Firepower 可扩展操作系统 73
  升级平台捆绑包 73
Firepower 平台捆绑包 69–70, 72–73
  关于 69
  从 Cisco.com 下载 70
  下载到 Firepower 安全设备 70
  升级 73
Firepower 平台捆绑包 *(续)*
  验证完整性 72
Firepower 安全设备 1
  概述 1
Firepower 威胁防御，请参阅 威胁防御
fpga 78
  升级 78
ftd，请参阅 威胁防御
FXOS 机箱，请参阅 Firepower 机箱
HTTP 代理 36
  配置 36
HTTPS 55–56, 142–144, 147–149, 151, 153
  配置 149
  证书请求 143–144
  更改端口 151
  创建密钥环 142
  禁用 153
  导入证书 148
  重新生成密钥环 142
  timeout 55–56
  受信任点 147
LDAP 提供程序 157, 160
  创建 157
  删除 160
LDAP 156–157, 160
noAuthNoPriv 132
NTP 117, 120, 122
  配置 117, 120
  添加 120
  删除 122
PCAP 文件 366
  下载 366
PCAP，请参阅 数据包捕获
ping 367
PKI 141
RADIUS 提供程序 162–163
  创建 162
  删除 163
RADIUS 161–163
重新启动 113
注册许可证 38
重新初始化安全模块 346
重置安全模块 345
rommon 78
  升级 78
RSA 141
smart call home 36
  配置 HTTP 代理 36
SNMP 131–135, 137, 139
  启用 134
  关于 131

SNMP *(续)*
community 134
当前设置 139
通知 131
权限 132
安全级别 132
支持 131, 133
陷阱 135, 137
创建 135
删除 137
用户 137, 139
创建 137
删除 139
版本 3 安全功能 133
SNMPv3 133
安全功能 133
SSH 55–56, 124
配置 124
SSH *(续)*
timeout 55–56
system 11
初始配置 11
TACACS+ 提供程序 164, 166
创建 164
删除 166
TACACS+ 164, 166
Telnet 55–56, 130
配置 130
timeout 55–56
time 118, 123
手动设置 123
查看 118
timeout 55–56
控制台 55–56
HTTPS、SSH 和 Telnet 55–56
traceroute 367
连接测试 367