思科 FXOS CLI 配置指南 2.2(1)

首次发布日期: 2017 年 5 月 15 日

上次修改日期: 2018 年 2 月 13 日

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

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

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

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

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

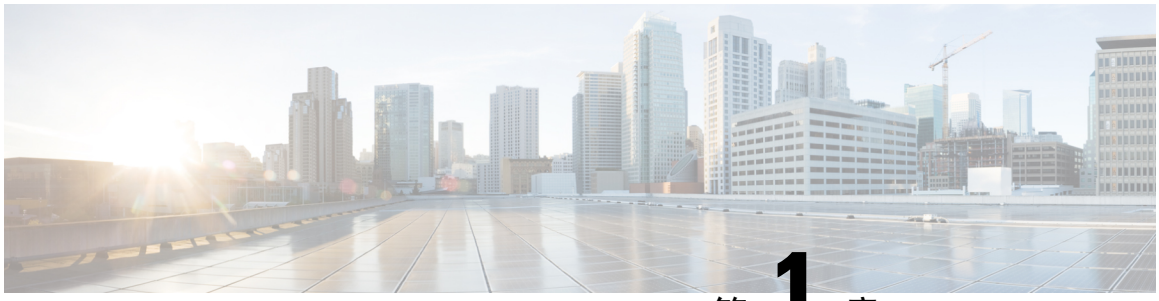
在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

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

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

© 2017 – 2018 Cisco Systems, Inc. 保留所有权利。

目录



第 1 章

Firepower 安全设备简介

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 机箱是思科应用中心基础设施 (ACI) 安全解决方案的一部分，并且提供为实现可扩展性、一致控制和简化管理而构建的灵活、开放、安全的平台。

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，简单、直观地显示当前机箱状态并提供简化的机箱功能配置。
- FXOS CLI - 提供基于命令的接口，用于配置功能，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。

监控机箱运行状况

您可使用 **show environment summary** 命令获取显示 Firepower 4100/9300 机箱整体运行状况的以下各条信息的视图：

- 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 14 页）。

步骤 2 进入机箱模式：

Firepower-chassis# **scopechassis1**

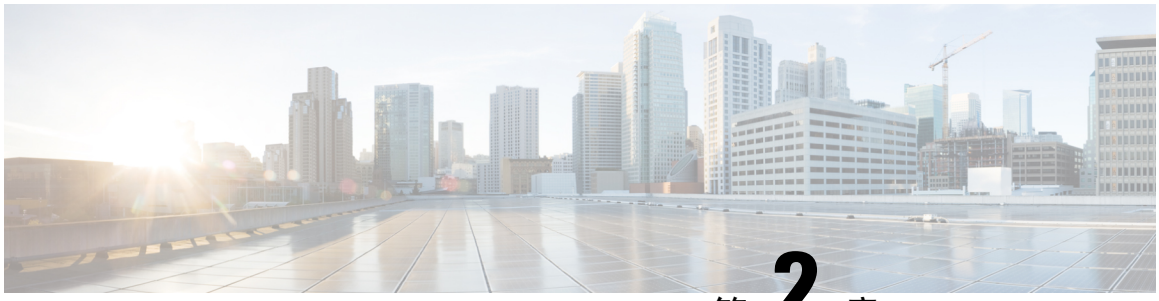
步骤 3 要查看机箱运行状况摘要，请输入以下命令：

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

Firepower 可扩展操作系统 (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 **exit** 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 #`

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）。

命令	行为
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 将多条命令一起提交不是单一操作。如果任何命令失败，则即便失败也会应用成功的命令。在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 #
```

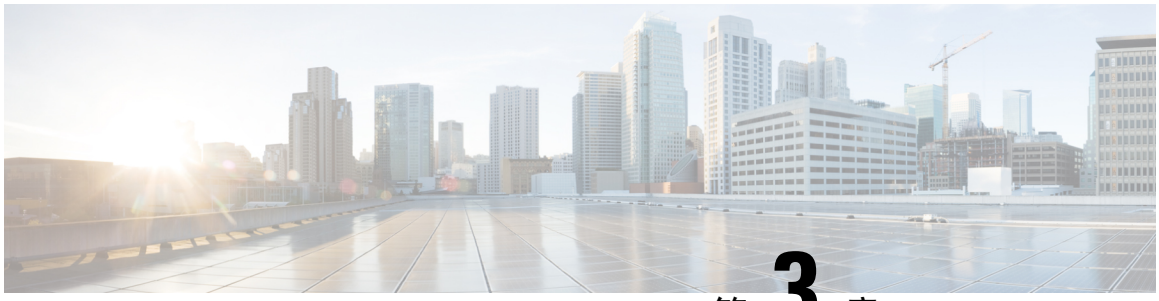
CLI 的在线帮助

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可用的关键字和参数。

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

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 101 页）。

步骤 4 配置 DNS 服务器（请参阅配置 DNS 服务器，第 141 页）。

步骤 5 注册产品许可证（请参阅ASA 的许可证管理，第 17 页）。

步骤 6 配置用户（请参阅用户管理，第 29 页）。

步骤 7 按需执行软件更新（请参阅映像管理，第 51 页）。

步骤 8 配置其他平台设置（请参阅平台设置，第 101 页）。

步骤 9 配置接口（请参阅接口管理，第 143 页）。

步骤 10 创建逻辑设备（请参阅逻辑设备，第 153 页）。

初始配置

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

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

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

开始之前

1. 在 Firepower 4100/9300 机箱上验证下列物理连接：
   - 控制台端口以物理方式连接到计算机终端或控制台服务器。
   - 1 Gbps 以太网管理端口连接到外部集线器、交换机或路由器。

   有关详细信息，请参阅思科 *Firepower* 安全设备硬件安装指南。
2. 验证连接到控制台端口的计算机终端（或控制台服务器）上的控制台端口参数是否如下所示：
   - 9600 波特率
   - 8 个数据位
   - 无奇偶校验
   - 1 个停止位

过程

步骤 1 连接到控制台端口。

步骤 2 打开 Firepower 4100/9300 机箱 的电源。

在 Firepower 4100/9300 机箱 启动时，您将看到开机自测消息。

步骤 3 当未配置的系统启动时，安装向导将提示您输入配置系统所需的下列信息：
- 设置模式（从完整系统备份或初始设置中恢复）
- 强密码执行策略（对于强密码准则，请参阅用户帐户 ， 第 29 页）
- 管理员密码
- 系统名称
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 默认网关 IPv4 或 IPv6 地址
- （可选）用于 SSH 访问的 IP 块地址
- （可选）用于 SSH 访问的 IPv4 或 IPv6 块子网掩码
- （可选）用于 HTTPS 访问的 IP 块地址

- （可选）用于 HTTPS 访问的 IPv4 或 IPv6 块子网掩码
- DNS 服务器 IPv4 或 IPv6 地址
- 默认域名

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

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

示例

以下示例使用 IPv4 管理地址设置配置：

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

以下示例使用 IPv6 管理地址设置配置：

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address :  2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
```

```
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
  Physical Switch Mgmt0 IPv6 Prefix=64
  Default Gateway=2001::1
  Ipv6 value=1
  SSH Access Configured=yes
      SSH IP Address=0.0.0.0
      SSH IP Netmask=0.0.0.0
  HTTPS Access Configured=yes
      HTTPS IP Address=0.0.0.0
      HTTPS IP Netmask=0.0.0.0
  DNS Server=2001::101
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

访问 FXOS CLI

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 来连接到 FXOS CLI。Firepower 可扩展操作系统最多支持 8 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：

- **sshucs-***auth-domain**username*@{*UCSM-ip-address* | *UCMS-ipv6-address*}

  ssh ucs-example\\jsmith@192.0.20.11

  ssh ucs-example\\jsmith@2001::1

- **ssh -lucs-***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*} **-lucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
ssh 2001::1 -l ucs-example\\jsmith
```

- **sshucs-***auth-domain**username*@{*UCSM-ip-address* | *UCSM-ipv6-address*}

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

使用 Telnet 从 Linux 终端登录：

注释 默认情况下，会禁用 Telnet。有关启用 Telnet 的说明，请参阅配置 Telnet，第 107 页。

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

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

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

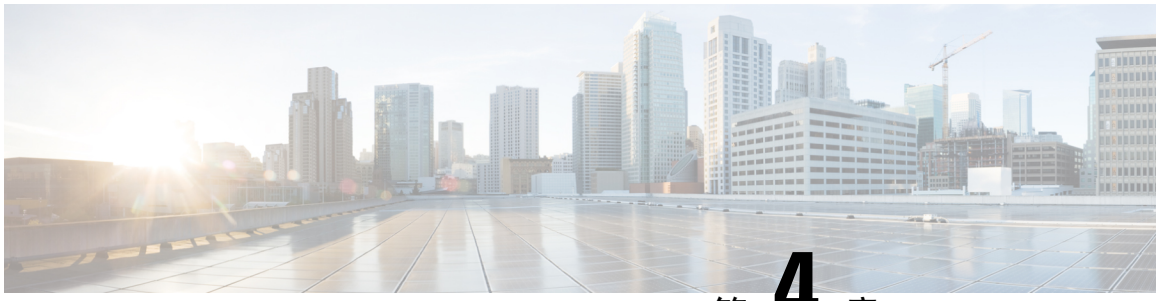
```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\blradmin
```

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 是本地帐户名称。



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

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

  注释 机箱间集群需要您在集群的每个机箱上启用相同的智能许可方法。

- ASA 应用 - 配置应用中的所有许可证授权。

智能软件管理器和帐户

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帐户。

注释 如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

默认情况下，许可证分配给主帐户下的默认虚拟帐户。作为帐户管理员，您可以选择创建其他虚拟帐户；例如，您可以为区域、部门或子公司创建帐户。通过多个虚拟帐户，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，请参阅智能帐户管理器卫星上的智能软件管理器卫星安装和配置指南。

按虚拟帐户管理的许可证和设备

仅当虚拟帐户可以使用分配给该帐户的许可证时，才能按虚拟帐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帐户传输未使用的许可证。您还可以在虚拟帐户之间迁移设备。

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

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

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

与许可证颁发机构的定期通信

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

您可以随意配置 HTTP 代理。

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

不合规状态

设备在以下情况下可能会处于不合规状态：

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

要验证您的帐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帐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。您无法删除此配置文件。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标地址 URL。除非获得思科 TAC 的指示，否则不应更改许可证颁发机构 URL。

智能软件许可必备条件

- 请注意，本章仅适用于 Firepower 4100/9300 机箱上的 ASA 逻辑设备。有关如何为 Firepower 威胁防御逻辑设备进行许可方面的详细信息，请参阅《Firepower 管理中心配置指南》。
- 在思科智能软件管理器上创建主帐户：

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

  如果您还没有帐户，请点击此链接以设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

- 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帐户。
- 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 故障转移和集群指南

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

智能软件许可的默认设置

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

```
scope monitoring
  scope callhome
    scope profile SLProf
      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帐户获得的注册令牌 ID。

过程

步骤 1 （可选）配置 HTTP 代理，第 22 页.

步骤 2 向许可证颁发机构注册 Firepower 安全设备，第 23 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 call-home
    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 *port*

示例：

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

步骤 4 确认缓冲区：

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 显示目标：
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 分配到相应的虚拟帐户。通常，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 机箱添加到的虚拟帐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》(http://www.cisco.com/web/software/286285517/138897/Smart_Software_Manager_satellite_4.1.0_User_Guide.pdf)。

步骤 2 在 Firepower 4100/9300 机箱中输入注册令牌：

scope license

register idtoken *id-token*

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

对 Firepower 4100/9300 机箱注销会从帐户中删除设备。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，或者在例如智能软件管理器中进行了任何许可更改，则可能要为其中任一项手动更新注册。

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 20 页中列出的所有必要条件。
- 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》。
- 如果您还没有证书链，请按照以下程序请求一个：
  - 创建密钥环 (创建密钥环，第 117 页)。
  - 为该密钥环创建一个证书请求 (使用基本选项创建密钥环的证书请求，第 118 页)。
  - 将此证书请求发送到信任锚或证书颁发机构，以便为密钥环获取证书链。

有关详细信息，请参阅证书、密钥环和受信任点，第 116 页。

过程

步骤 1 将卫星服务器设置为 Callhome 目标：

scopemonitoring

scopecall-home

scopeprofileSLProfile

scopedestinationSLDest

setaddresshttps://*ip_address***/Transportgateway/services/DeviceRequestHandler**

步骤 2 创建新信任点。

a) 进入安全模式：

scopesecurity

b) 创建并命名信任点：

createtrustpoint *trustpoint_name*

c) 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。

setcertchain *certchain*

对于 *certchain* 变量，请使用此程序的证书生成必备条件中获得的证书链信息。

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。

d) 提交配置：

commit-buffer

示例：

```
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 #
```

步骤 3 向证书颁发机构注册 Firepower 4100/9300 机箱（请查阅向许可证颁发机构注册 Firepower 安全设备，第 23 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。并非所有帐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，点击 **Licenses** 选项卡：

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

Licenses 选项卡显示与您的帐户相关的所有现有许可证（普通和永久）。

步骤 5 点击 **License Reservation**，并在框中键入生成的预留申请代码。

步骤 6 点击 **Reserve License**。

智能软件管理器将生成授权码。您可以下载该授权码或将其复制到剪贴板。根据智能软件管理器，许可证现已处于使用状态。

如果您未看到 **License Reservation** 按钮，则您的帐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 从 FXOS CLI 生成返还代码：

license smart reservation 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 2 在智能软件管理器中查看 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 3 访问“智能软件管理器库存 (Smart Software Manager Inventory)”屏幕，点击 **Product Instances** 选项卡：

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

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

步骤 5 选择 **Actions** > **Remove**，在框中键入生成的返还代码。

步骤 6 点击 **Remove Product Instance**。

永久许可证被返还到可用池。

步骤 7 重启系统。有关如何重新引导您的 Firepower 4100/9300 机箱的详细信息，请参阅重新启动 Firepower 4100/9300 机箱，第 91 页。

监控智能软件许可

请参阅以下命令来查看许可证状态：

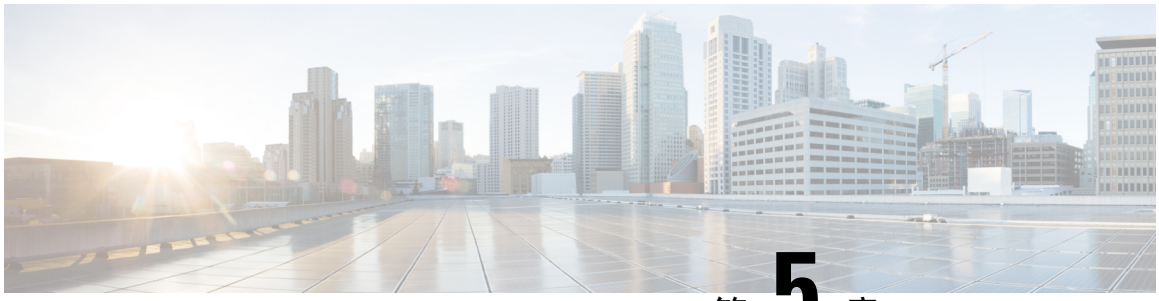
- **show license all**

  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
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。智能软件许可配置在 Firepower 4100/9300 机箱管理引擎和安全模块之间拆分。 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

用户帐户用于访问系统。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。

管理员帐户

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。管理员帐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帐户

本地身份验证用户帐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。一旦本地用户帐户被禁用，该用户将无法登录。已禁用本地用户帐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，此帐户将再次处于活动状态，且采用现有配置（包括用户名和密码）。

远程身份验证的用户帐户

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

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

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

- 远程身份验证指导原则，第 32 页
- 配置 LDAP 提供程序，第 129 页
- 配置 RADIUS 提供程序，第 134 页
- 配置 TACACS+ 提供程序，第 137 页

用户帐户的到期

您可以配置用户帐户在预定时间过期。当到达到期时间时，系统将会禁用用户帐户。

默认情况下，用户帐户不会到期。

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 分配到用户帐户时，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：
  - 任意字母字符
  - 任意数字

- _（下划线）
- -（短划线）
- .（点）

- 登录 ID 必须唯一。
- 登录 ID 必须以字母字符开头。它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。
- 不能创建全数字登录 ID。
- 创建用户帐户后，不能更改登录 ID。必须删除该用户帐户，创建新的用户帐户。

面向密码的指导原则

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

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

- 必须包含最少 8 个字符，最多 80 个字符。

注释 您可以选择在系统上配置 15 个字符（最小密码长度）的密码，以符合通用标准需求。有关详细信息，请参阅配置最小密码长度检查，第 43 页。

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

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，则必须创建用于该服务的提供程序，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帐户

用户帐户可能存在于 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帐户，则必须确保帐户包括用户在 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。根据角色策略，系统可能会禁止用户登录，或仅向其授予只读权限。

远程身份验证提供程序中的用户属性

对于 RADIUS 和 TACAS+ 配置，您必须在用户通过其登录到 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. 如果用户已通过验证，请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。	Cisco LDAP 实施需要 unicode 类型属性。 如果选择创建 CiscoAVPair 自定义属性，请使用以下属性 ID：1.3.6.1.4.1.9.287247.1 以下部分提供示例 OID。

身份验证提供程序	自定义属性	方案扩展	属性 ID 要求
RADIUS	可选	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。	Cisco 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。
TACAS	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。 以下语法示例说明，在创建 cisco-av-pair 属性时，如何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，为默认管理员帐户分配此角色，不能更改。

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	描述	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 # **scopedefault-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

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 # **scopedefault-auth**

步骤 3 设置 HTTPS、SSH 和 Telnet 会话的空闲超时：

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

步骤 4 （可选）设置控制台会话的空闲超时：

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

步骤 5 （可选）查看会话和绝对会话超时设置：

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

示例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 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 # **scopedefault-auth**

步骤 3 设置绝对会话超时：

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

步骤 4 （可选）设置单独的控制台绝对会话超时：

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

步骤 5 （可选）查看会话和绝对会话超时设置：

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

示例：

```
Default authentication:
 Admin Realm: Local
 Operational Realm: Local
 Web session refresh period(in secs): 600
 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 # **scopesecurity**

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

如果启用了密码强度检查，Firepower可扩展操作系统不允许用户选择不符合强密码准则的密码（请参阅面向密码的指导原则，第 31 页）。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scopesecurity**

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。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，配置最大登录尝试次数。

注释

- 在超过最大尝试登录次数后，所有类型的用户帐户（包括管理员帐户）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 41 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 63 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scopesystem

scopesecurity

步骤 2 设置最大尝试登录失败次数。

setmax-login-attempts

max_login

max_login 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）：

setuser-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 40 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scopesystem

scopesecurity

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 # **scopesecurity**

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*

该值可以是从 0 到 10 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，则必须最少使用指定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 63 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：

步骤 2 **scopesystem**

scopesecurity

步骤 3 指定最小密码长度：

setmin-password-length *min_length*

步骤 4 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 # **scopesecurity**

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 **Change During Interval** 属性设置为 **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 # **scopesecurity**

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，**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 #
```

创建本地用户帐户

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 创建用户帐户：

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

其中，*local-user-name* 是登录此帐户时要使用的帐户名称。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 30 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 指定本地用户帐户已启用还是已禁用：

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

步骤 4 设置用户帐户的密码：

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

输入密码：*password*

确认密码：*password*

如果启用密码强度检查，则用户的密码必须为强密码，Firepower 可扩展操作系统会拒绝任何不满足强度检查要求的密码（请参阅面向密码的指导原则，第 31 页）。

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）指定用户帐户到期日期：*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帐户的权限的角色（请参阅用户角色，第 34 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。如果在向用户帐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*

注释 所有用户均默认分配了 *read-only* 角色，并且此角色无法删除。

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 的用户帐户，启用用户帐户，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 的用户帐户，启用用户帐户，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+k8f4VcOelBxlsGk5luq5ls1oblVOIEwcKEL/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 的用户帐户，启用用户帐户，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 #
```

删除本地用户帐户

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 删除本地用户帐户：

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 用户帐户，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帐户

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帐户。

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 指定本地用户帐户是活动还是非活动状态：

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

注释 管理员用户帐户始终设置为活动。不能修改。

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/local-user # set account-status active
```

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 # **scopesecurity**

步骤 2 进入已指定用户帐户的本地用户安全模式：

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

步骤 3 清除已指定用户帐户的密码历史记录：

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

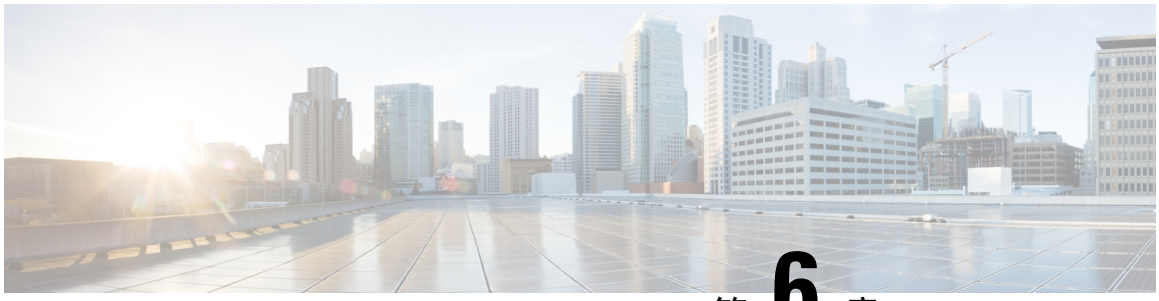
步骤 4 将任务提交到系统配置：

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

Firepower 4100/9300 机箱使用的映像分为两个基本类型：

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

- 平台捆绑包 (Platform Bundle) - Firepower 平台捆绑包是一系列运行在 Firepower 管理引擎和 Firepower 安全模块/引擎上的多个独立映像。平台捆绑包是 Firepower 可扩展操作系统软件包。
- 应用 (Application) - 应用是您想在安全模块/引擎的 Firepower 4100/9300 机箱上部署的软件映像。应用映像作为思科安全数据包文件 (CSP) 进行交付，在部署到安全模块/引擎之前，存储在管理引擎上，参与逻辑设备创建，或者为稍后的逻辑设备创建做准备。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 帐户。

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 可扩展操作系统软件映像下载到 Firepower 4100/9300 机箱

您可以使用 FTP、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

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*
- **scp**://*username@hostname*/*path*/*image_name*

- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*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)
```

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 14 页）。

步骤 2 进入固件模式：

Firepower-chassis# **scopefirmware**

步骤 3 列出映像：

Firepower-chassis /firmware # **showpackage**

步骤 4 验证映像：

Firepower-chassis /firmware # **verifyplatform-packversion** *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 # **showvalidate-task**

升级Firepower 可扩展操作系统平台捆绑包

开始之前

从 Cisco.com 下载平台捆绑包软件映像（请参阅从 Cisco.com 下载映像，第 52 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 55 页）。

注释 升级过程通常需要 20 到 30 分钟。

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

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

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 14 页）。

步骤 2 进入固件模式：

Firepower-chassis# **scopefirmware**

步骤 3 进入自动安装模式：

Firepower-chassis /firmware # **scopeauto-install**

步骤 4 安装 FXOS 平台捆绑包：

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

version_number 是您正在安装的 FXOS平台捆绑包的版本号，例如 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**，可确认您想要继续安装，或者输入 **no**，可取消安装。

Firepower 可扩展操作系统打开捆绑包，升级/重新加载组件。

步骤 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、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

过程

步骤 1 进入安全服务模式：

Firepower-chassis # **scopessa**

步骤 2 进入应用软件模式：

Firepower-chassis /ssa # **scopeapp-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*
- **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。

在初始创建 Firepower 威胁防御逻辑设备后，您将无法使用 Firepower 机箱管理器或 FXOS CLI升级 Firepower 威胁防御逻辑设备。要升级 Firepower 威胁防御逻辑设备，您必须使用 Firepower 管理中心。有关详细信息，请参阅《Firepower 系统版本说明》：http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html。

另请注意，Firepower 威胁防御逻辑设备的任何更新都不会反映在 Firepower 机箱管理器的 **Logical Devices** > **Edit** 和 **System** > **Updates** 页面上。在这些页面上，显示的版本表示用于创建 Firepower 威胁防御逻辑设备的软件版本（CSP 映像）。

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

ASA 高可用性 -

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

ASA 机箱间集群 -

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

开始之前

从 Cisco.com 下载要用于逻辑设备的应用映像（请参阅从 Cisco.com 下载映像，第 52 页），然后将映像下载到 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 55 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 # **scopessa**

步骤 2 将范围设置为您正在更新的安全模块：

Firepower-chassis /ssa # **scopeslot** *slot_number*

步骤 3 将范围设置为您正在更新的应用：

Firepower-chassis /ssa/slot # **scopeapp-instance** *app_template*

步骤 4 设置启动版本：

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

步骤 5 提交配置：

commit-buffer

确认系统配置任务。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

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

过程

步骤 1 使用网络浏览器导航至 http://www.cisco.com/go/firepower9300-software 或 http://www.cisco.com/go/firepower4100-software。
系统将在浏览器中打开 Firepower 4100/9300 机箱的软件下载页面：

步骤 2 从 Cisco.com 查找，然后将合适的固件包下载到您可从 Firepower 4100/9300 机箱访问的服务器。

步骤 3 在 Firepower 4100/9300 机箱上，进入固件模式：

Firepower-chassis # **scopefirmware**

步骤 4 将 FXOS 固件映像下载到 Firepower 4100/9300 机箱：

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

使用以下语法之一，为正在导入的文件指定 URL：

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

步骤 5 要监控下载过程，请执行以下操作：

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

步骤 6 下载完成后，可输入以下命令查看固件包的内容：

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

步骤 7 可输入以下命令查看固件包的版本号：

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

当安装固件包时，在以下步骤中使用此版本号：

步骤 8 要安装固件包：

a) 进入固件安装模式：

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

b) 安装固件包：

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

系统将验证固件包，并通知您验证过程可能需要几分钟才能完成。

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

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

步骤 9 要监控升级流程，请执行以下操作：

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

步骤 10 安装完成后，可输入以下命令查看当前固件版本：

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

Firepower-chassis # **scope chassis 1**

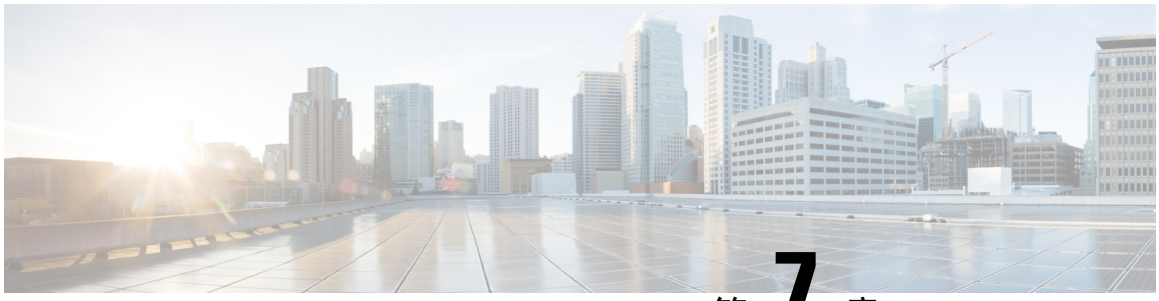
Firepower-chassis /firmware # **show sup version**

示例

下面的示例将固件升级到了版本 1.0.10：

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

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

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

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

Firepower-chassis /firmware # show package

Name                                       Version
```

```
------------------------------------------- -------
fxos-k9-fpr9k-firmware.1.0.10.SPA             1.0.10

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

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

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

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

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

Upgrading FXOS SUP firmware software package version 1.0.10

command executed
```



第 7 章

安全认证合规性

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 64 页
- 启用通用标准模式， 第 65 页
- 配置 IPSec 安全通道， 第 66 页
- 配置信任点静态 CRL， 第 71 页
- 关于证书吊销列表检查， 第 72 页
- 配置 CRL 定期下载， 第 76 页
- 启用 NTP 服务器身份验证， 第 78 页
- 设置 LDAP 密钥环证书， 第 79 页

- 配置 IP 访问列表， 第 79 页
- 启用客户端证书身份验证， 第 81 页
- 配置最小密码长度检查， 第 43 页
- 设置最大尝试登录次数， 第 40 页
- 用户角色， 第 34 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导致合规性自动传播到与之连接的任何逻辑设备。

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：

scopesystem

scopesecurity

步骤 2 启用 FIPS 模式：

enablefips-mode

步骤 3 提交配置：

commit-buffer

步骤 4 重新启动系统：

connectlocal-mgmt

reboot

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 65 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：

scopesystem

scopesecurity

步骤 2 启用通用标准模式：

enablecc-mode

步骤 3 提交配置：

commit-buffer

步骤 4 重新启动系统：

connectlocal-mgmt

reboot

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 65 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。

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 64 页或启用通用标准模式，第 65 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：

scopesystem

scopeservices

步骤 2 删除 SSH 主机密钥：

deletessh-serverhost-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：

setssh-serverhost-keyrsa 2048

步骤 5 提交配置：

commit-buffer

步骤 6 创建新的 SSH 主机密钥：

createssh-serverhost-key

commit-buffer

步骤 7 确认新的主机密钥长度：

showssh-serverhost-key

主机密钥长度：2048

配置 IPSec 安全通道

您可以在 Firepower 4100/9300 机箱上配置 IPSec，对通过公用网络的数据包提供端到端数据加密和身份验证服务。这是为实现系统的通用标准认证合规性提供的众多选项之一。有关详细信息，请参阅安全认证合规性，第 63 页。

注释 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。

执行这些步骤，以配置 IPSec 安全通道。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scopesystem

scopesecurity

步骤 2 创建密钥环：

enterkeyringssp

!createcertreqsubject-name *subject-name***ip** *ip*

步骤 3 输入关联的证书请求信息：

entercertreq

步骤 4 设置国家/地区：

setcountry *country*

步骤 5 设置 DNS：

setdns *dns*

步骤 6 设置邮件：

sete-mail *email*

步骤 7 设置 IP 信息：

setfi-a-ip *fi-a-ip*

setfi-a-ipv6 *fi-a-ipv6*

setfi-b-ip *fi-b-ip*

setfi-b-ipv6 *fi-b-ipv6*

setipv6 *ipv6*

步骤 8 设置位置：

setlocality *locality*

步骤 9 设置组织名称：

setorg-name *org-name*

步骤 10 设置组织单位名称：

setorg-unit-name *org-unit-name*

步骤 11 设置密码：

!setpassword

步骤 12 设置状态：

setstate *state*

步骤 13 设置 certreq 的主题名称：

setsubject-name *subject-name*

步骤 14 退出：

exit

步骤 15 设置模数：

setmodulus *modulus*

步骤 16 设置证书请求的重新生成：

setregenerate *{ yes | no }*

步骤 17 设置信任点：

settrustpointinterca

步骤 18 退出：

exit

步骤 19 输入新创建的信任点：

entertrustpointinterca

步骤 20 生成证书签名请求：

setcertchain

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+YRazaIT9xj9KH
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：

showcertreq

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：

scopeipsec

步骤 23 设置日志冗长级别：

setlog-level *log_level*

步骤 24 创建并输入一个 IPSec 连接：

enterconnection *connection_name*

步骤 25 将 IPSec 模式设置为隧道或传输：

setmode *tunnel_or_transport*

步骤 26 设置本地 IP 地址：

setlocal-addr *ip_address*

步骤 27 设置远程 IP 地址：

setremote-addr *ip_address*

步骤 28 如果使用隧道模式，则设置远程子网：

setremote-subnet *ip/mask*

步骤 29 （可选）设置远程身份：

setremote-ike-ident *remote_identity_name*

步骤 30 设置密钥环名称：

setkeyring-name *name*

步骤 31 （可选）设置密钥环密码：

setkeyring-passwd *passphrase*

步骤 32 （可选）设置 IKE-SA 生命周期（分钟）：

setike-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)：

setesp-rekey-time *minutes*

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：

setkeyringtries *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：

setrevoke-policy *{ relaxed | strict }*

步骤 36 启用连接：

setadmin-stateenable

步骤 37 重新加载所有连接：

reload-conns

步骤 38 （可选）将现有信任点名称添加至 IPsec：

createauthority *trustpoint_name*

步骤 39 配置执行 IKE 和 SA 连接间加密密钥强度的匹配：

setsa-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 63 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：

scopesecurity

步骤 2 进入信任点模式：

scopetrustpoint *trustname*

步骤 3 进入吊销模式：

scoperevoke

步骤 4 下载 CRL 文件：

importcrl *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：

showimport-taskdetail

步骤 6 将证书撤销方法设置为仅限于 CRL：

setcertrevokemethod{crl}

关于证书吊销列表检查

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

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

有关启用或禁用对安全 IPSec、LDAP 和 HTTPS 连接的证书吊销检查的具体步骤，请参阅配置 IPSec 安全通道，第 66 页、创建 LDAP 提供程序，第 130 页和配置 HTTPS，第 124 页。

注释

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

下表说明了连接结果，具体取决于证书吊销列表检查设置和证书验证。

表 *4:* 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
某个CDP缺少对等证书链	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息
某个CDP CRL在具有有效签名的对等证书链中为空	连接成功	连接成功	连接失败，系统显示系统日志消息
无法下载对等证书链中的任何 CDP	连接失败，系统显示系统日志消息	对等证书：连接失败，系统显示系统日志消息 中间 CA：连接失败	连接失败，系统显示系统日志消息

无本地静态 CRL	LDAP 连接	IPSec 连接	客户端证书身份验证
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 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 *5:* 具有本地静态 *CRL* 时将“证书撤销检查模式 *(Certificate Revocation Check Mode)*”设置为“严格 *(Strict)*”

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

表 *6:* 无本地静态 ***CRL*** 时将“证书撤销检查模式 ***(Certificate Revocation Check Mode)***”设置为“释放 ***(Relaxed)***”

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

表 *7:* 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

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

配置 CRL 定期下载

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

您可将以下协议和接口用于该功能：

- FTP
- SCP
- SFTP
- TFTP
- USB

注释

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

注释 您只能以一小时为间隔配置周期。

执行以下步骤，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 71 页。

过程

步骤 1 从 FXOS CLI 进入安全模式：

scopesecurity

步骤 2 进入信任点模式：

scopetrustpoint

步骤 3 进入吊销模式：

scoperevoke

步骤 4 编辑吊销配置：

shconfig

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
```

启用 NTP 服务器身份验证

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

注释

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

过程

步骤 1 下载 ntp 4.2.8p8。

步骤 2 在 **ntpd openssl** 启用时安装 NTP 服务器。

步骤 3 生成 NTP 密钥 ID 和密钥值：

ntp-keygen-M

使用这些生成的密钥执行以下步骤。

步骤 4 从 FXOS CLI 创建 NTP 服务器：

createntp-server *server_id*

步骤 5 输入 NTP 服务器：

scopentp-server *server_id*

步骤 6 设置 SHA1 密钥 ID：

setntp-sha1-key-id *key_id*

步骤 7 设置 SHA1 密钥字符串：

setntp-sha1-key-string *key_string*

步骤 8 启用 NTP 身份验证：

enablentp-authentication

设置 LDAP 密钥环证书

您可配置安全的 LDAP 客户端密钥环证书，以便支持 Firepower 4100/9300 机箱 上的 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 63 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。

如果为进入 LDAP 服务器启用 SSL，则系统在建立连接时会参考并检查密钥环信息。

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，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：

scopesecurity

步骤 2 进入 LDAP 模式：

scopeldap

步骤 3 进入 LDAP 服务器模式：

enterserver *{server_ip|server_dns}*

步骤 4 设置 LDAP 密钥环：

setkeyring *keyring_name*

步骤 5 提交配置：

commit-buffer

配置 IP 访问列表

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

IP 访问列表支持以下协议：

- HTTPS

- SNMP
- SSH

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

过程

步骤 1 从 FXOS CLI 进入服务模式：

scopesystem

scopeservices

步骤 2 为要启用访问权限的服务创建 IP 块：

IPv4：

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

IPv6：

createipv6-block *ip prefix [0-28]* [**http** | **snmp** | **ssh**]

示例

IPv4：

```
Firepower-chassis # scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # create ip-block 10.1.1.1 24 https
Firepower-chassis /system/services/ip-block* # com
Firepower-chassis /system/services/ip-block # up
Firepower-chassis /system/services # create ip-block 11.1.1.1 24 ssh
Firepower-chassis /system/services/ip-block* # com
Firepower-chassis /system/services/ip-block # up
Firepower-chassis /system/services # create ip-block 12.1.1.1 24 snmp
Firepower-chassis /system/services/ip-block* # com
Firepower-chassis /system/services/ip-block # up
Firepower-chassis /system/services # sh ip-block
Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    10.1.1.1        24            Https
    11.1.1.1        24            Ssh
    12.1.1.1        24            Snmp
```

IPv6：

```
Firepower-chassis /system/services # create ipv6-block 2014::10:76:78:107 64 ssh
Firepower-chassis /system/services/ipv6-block* # com
Firepower-chassis /system/services/ipv6-block # up
Firepower-chassis /system/services # create ipv6-block 2014::10:76:78:107 64 snmp
Firepower-chassis /system/services/ipv6-block* # com
Firepower-chassis /system/services/ipv6-block # up
```

```
Firepower-chassis /system/services # create ipv6-block 2014::10:76:78:107 64 https
Firepower-chassis /system/services/ipv6-block* # com
Firepower-chassis /system/services/ipv6-block # up
Firepower-chassis /system/services # sh ipv6-block
Permitted IPv6 Block:
    IPv6 Address Prefix Length Protocol
    ------------ ------------- --------
    2014::10:76:78:107   64      Https
    2014::10:76:78:107   64      Snmp
    2014::10:76:78:107   64      Ssh
```

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 签名。

过程

步骤 1 从 FXOS CLI 进入服务模式：

scopesystem

scopeservices

步骤 2 （可选）查看 HTTPS 身份验证选项：

sethttpsauth-type

示例：

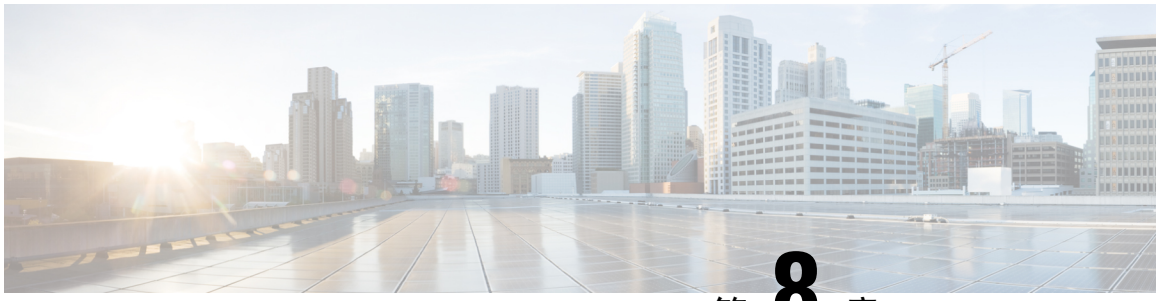
```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

步骤 3 将 HTTPS 身份验证设为基于客户端：

sethttpsauth-typecert-auth

步骤 4 提交配置：

commit-buffer



第 8 章

系统管理

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 14 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# **scopefabric-interconnecta**

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 # **setout-of-bandip** *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# **scopefabric-interconnecta**

b) 设置管理 IPv6 配置的范围：

Firepower-chassis /fabric-interconnect # **scopeipv6-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 # **setout-of-bandipv6** *ipv6_address***ipv6-prefix** *prefix_length***ipv6-gw** *gateway_address*

e) 将任务提交到系统配置：

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

示例

以下示例配置 IPv4 管理接口和网关：

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

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

以下示例配置 IPv6 管理接口和网关：

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

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

更改应用管理 IP

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

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

过程

步骤 1 连接到 FXOS CLI。（请参阅访问 FXOS CLI，第 14 页）。

步骤 2 将范围设置为逻辑设备：

scopessa

scopelogical-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：
scopemgmt-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：
setip *ipv4_address***mask** *network_mask*

d) （仅限 IPv6）设置新的 IP 地址：
setip *ipv6_address***prefix-length** *prefix_length_number*

e) 设置网关地址：
setgateway *gateway_ip_address*

f) 提交配置：

commit-buffer

对于 ASA 逻辑设备的集群配置：

a) 输入集群管理引导程序：
scopecluster-bootstrap *asa*

b) （仅限 IPv4）设置新的虚拟 IP：
setvirtualipv4 *ip_address***mask** *network_mask*

c) （仅限 IPv6）设置新的虚拟 IP：
setvirtualipv6 *ipv6_address***prefix-length** *prefix_length_number*

d) 设置新的 IP 池：
setippool *start_ip end_ip*

e) 设置网关地址：
setgateway *gateway_ip_address*

f) 提交配置：
commit-buffer

对于 Firepower 威胁防御的独立和集群配置：

a) 输入逻辑设备管理引导程序：
scopemgmt-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：
setip *ipv4_address***mask** *network_mask*

d) （仅限 IPv6）设置新的 IP 地址：
setip *ipv6_address***prefix-length** *prefix_length_number*

e) 设置网关地址：
setgateway *gateway_ip_address*

f) 提交配置：
commit-buffer

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

步骤 4 为每个应用清除管理引导程序信息：

a) 将范围设置为 ssa 模式：
scopessa

b) 将范围设置为插槽：

scopeslot *slot_number*

c) 将范围设置为应用实例：

scopeapp-instance *asa_or_ftd*

d) 清除管理引导程序信息：

clearmgmt-bootstrap

e) 提交配置：

commit-buffer

步骤 5 禁用应用：

disable

commit-buffer

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

步骤 6 当应用离线且插槽恢复在线时，重新启用应用。

a) 将范围重置为 ssa 模式：

scopessa

b) 将范围设置为插槽：

scopeslot *slot_number*

c) 将范围设置为应用实例：

scopeapp-instance *asa_or_ftd*

d) 启用应用：

enable

e) 提交配置：

commit-buffer

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

更改 Firepower 4100/9300 机箱 名称

开始之前

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 14 页）。

步骤 2 进入系统模式：

Firepower-chassis-A# **scopesystem**

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 # **setname** *device_name*

步骤 5 将任务提交到系统配置：

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

示例

以下示例将更改设备名称：

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

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

登录前横幅

如果配置了登录前横幅，当用户登录到Firepower机箱管理器时，系统将显示横幅文本，用户必须在消息屏幕上点击**确定(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 14 页）。

步骤 2 进入安全模式：

Firepower-chassis# **scopesecurity**

步骤 3 进入横幅安全模式：

Firepower-chassis /security # **scopebanner**

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 14 页）。

步骤 2 进入安全模式：

Firepower-chassis# **scopesecurity**

步骤 3 进入横幅安全模式：

Firepower-chassis /security # **scopebanner**

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 14 页）。

步骤 2 进入安全模式：

Firepower-chassis# **scopesecurity**

步骤 3 进入横幅安全模式：

Firepower-chassis /security # **scopebanner**

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 [*reason*] **[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 [*reason*] **[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** 命令前系统不会关闭。

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，您需要连接到 Firepower 4100/9300 机箱上的控制台端口，以使用设置向导重新配置系统（请参阅初始配置，第 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

对 Firepower 4100/9300 机箱注销会从帐户中删除设备。系统会删除设备上的所有许可证授权和证书。

步骤 2 连接到本地管理：

connect local-mgmt

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

erase configuration

系统将提示您确认，是否确定想要清除所有用户配置。

步骤 4 通过在命令提示符后输入 **yes**，确认您想要清除配置。
系统将从您的 Firepower 4100/9300 机箱中清除所有用户配置，然后重启系统。

安装受信任身份证书

在完成初始配置后，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 14 页）。

步骤 2 输入安全模块：

scopesecurity

步骤 3 创建密钥环：

createkeyring *keyring_name*

步骤 4 设置私钥的模数大小：

setmodulus *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。

createcertreqcertreq *subject_name*

password

setcountry *country*

setstate *state*

setlocality *locality*

setorg-name *organization_name*

setorg-unit-name *organization_unit_name*

setsubject-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：

showcertreq

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。

createtrustpoint *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。

setcertchain

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：

scopekeyring *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：

settrustpoint *trustpoint_name*

步骤 **18** 导入服务器的签名身份证书。

setcert

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
>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-----
>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：

scopesystem

步骤 **23** 进入服务模式：

scopeservices

步骤 24 配置 FXOS Web 服务以使用新证书：

sethttpskeyring *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：

showhttps

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**：

scopesecurity

showkeyring *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:
```

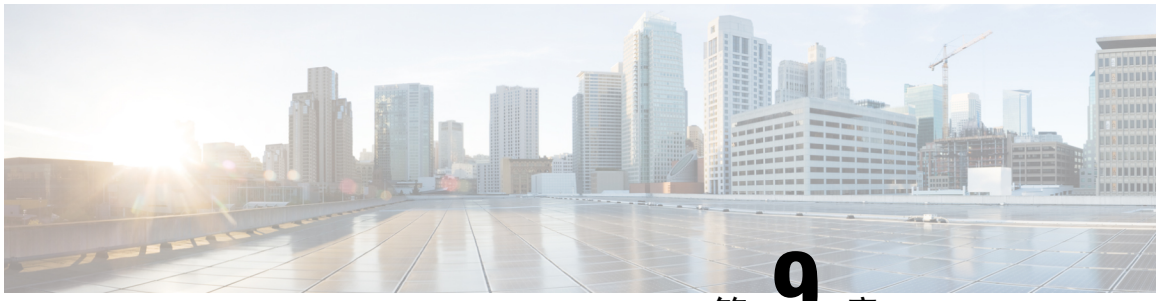
```
                    3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
                    a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
                    9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
                    20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
                    ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
                    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
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-----

    Zeroized: No
```

下一步做什么

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

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



第 9 章

平台设置

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。应对 Firepower 4100/9300 机箱和 Firepower 管理中心使用相同 NTP 服务器。

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

查看配置的日期和时间

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 14 页）。

步骤 2 要查看已配置的时区，请执行以下操作：

Firepower-chassis# **showtimezone**

步骤 3 查看配置的日期和时间：

Firepower-chassis# **showclock**

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# **scopesystem**

步骤 2 进入系统服务模式：

Firepower-chassis /system # **scopeservices**

步骤 3 设置时区：

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

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。

过程

步骤 1 进入系统模式：

Firepower-chassis# **scopesystem**

步骤 2 进入系统服务模式：

Firepower-chassis /system # **scopeservices**

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 # **createntp-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**

步骤 5 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 6 查看特定 NTP 服务器的同步状态：

Firepower-chassis /system/services # **scopentp-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# **scopesystem**

步骤 2 进入系统服务模式：

Firepower-chassis /system # **scopeservices**

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 # **deletentp-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。系统时钟修改立即生效。

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# **scopesystem**

步骤 2 进入系统服务模式：

Firepower-chassis /system # **scopeservices**

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。无需提交缓冲区。

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

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

过程

步骤 1 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 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 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，会禁用 Telnet。

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

本部分介绍如何在 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 提供了标准化的框架和通用语言，可用于监控和管理网络中的设备。

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)

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。

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等级。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。安全等级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 *8: SNMP* 安全模型和级别

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

SNMPv3 安全功能

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

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

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

针对 MIB 的支持

Firepower 机箱支持对 MIB 的只读访问。

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

适用于 SNMPv3 用户的身份验证协议

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

适用于 SNMPv3 用户的 AES 隐私协议

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

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

启用 SNMP 并配置 SNMP 属性

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

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

步骤 3 进入 snmp 社区模式：

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

输入 **set snmp community** 命令后，系统将提示您进入 SNMP 社区。

步骤 4 指定 SNMP 社区。使用社区名作为密码。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*

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

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：

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

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**}

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：

- **身份验证 (auth)** - 有身份验证，但没有加密
- **无身份验证 (noauth)** - 没有身份验证和加密
- **权限 (priv)** - 有身份验证和加密

步骤 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 创建指定的 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。

步骤 4 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，禁用 AES-128 加密。

步骤 5 指定用户隐私密码：

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

输入 **set priv-password** 命令后，系统将提示您输入并确认隐私密码。

步骤 6 确认系统配置任务：

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 #
```

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。

如果集群名称更改或证书过期，则必须手动重新生成默认密钥环证书。

证书

作为安全通信前的准备，两台设备首先会交换数字证书。证书是包含设备公钥以及设备身份相关签名信息的文件。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。远程用户连接至呈现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共密钥。

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 # **createkeyring** *keyring-name*

步骤 3 设置 SSL 密钥长度（以位为单位）：

Firepower-chassis # **setmodulus** {**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

为该密钥环创建证书请求。

重新生成默认密钥环

如果集群名称更改或证书过期，则必须手动重新生成默认密钥环证书。

过程

步骤 1 进入安全模式：

Firepower-chassis #**scope security**

步骤 2 进入默认密钥环的密钥环安全模式：

Firepower-chassis /security # **scopekeyring default**

步骤 3 重新生成默认密钥环：

Firepower-chassis /security/keyring # **setregenerate 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 # **createcertreq**

步骤 4 指定公司所在国家/地区的国家/地区代码：

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

步骤 5 指定与请求相关联的域名服务器 (DNS) 地址：

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

步骤 6 指定与证书请求相关联的邮件地址：

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

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

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

步骤 8 指定请求此证书的公司总部所在的城市或城镇：

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

步骤 9 指定请求证书的组织：

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

步骤 10 指定组织单位：

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

步骤 11 为证书请求指定可选密码：

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

步骤 12 指定请求此证书的公司总部所在的省、市或自治区：

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

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

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

步骤 14 提交任务：

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

步骤 15 显示您可以复制并发送至信任锚或证书颁发机构的证书请求：

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

示例

以下示例使用高级选项为密钥环创建并显示具有 IPv4 地址的证书请求：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* #  set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
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 # **createtrustpoint** *name*

步骤 3 为此受信任点指定证书信息：

Firepower-chassis /security/trustpoint # **setcertchain** [*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受信任点证书：

```
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。

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 # **scopekeyring** *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 # **settrustpoint** *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 # **setcert**

在提示符后，粘贴从信任锚或证书颁发机构接收的证书文本。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，一旦保存或提交事务，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：

setrevoke-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 # **sethttpsport** *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 #
```

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 # **deletekeyring** *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# **scopesecurity**

步骤 2 删除指定受信任点：

Firepower-chassis /security # **deletetrustpoint** *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、授权和记帐。有关详细信息，请参阅以下主题：

关于 AAA

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

身份验证

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

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

- HTTPS
- SSH
- 串行控制台

授权

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

会计

记帐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。记帐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、资源利用和容量规划活动。

身份验证、授权和记帐之间的交互

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。您可以单独使用记帐功能，也可以将其与身份验证和授权功能配合使用。

AAA 服务器

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

本地数据库支持

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

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，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户帐户以绑定 Firepower 可扩展操作系统。此帐户应具有非到期的密码。

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*

步骤 6 设置在注明 LDAP 服务器已关闭之前，系统应等待服务器发出响应的时间间隔：

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 userdn 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

Firepower 可扩展操作系统最多支持 16 个 LDAP 提供程序。

开始之前

如果使用 Active Directory 作为 LDAP 服务器，请在 Active Directory 服务器中创建用户帐户以绑定 Firepower 可扩展操作系统。此帐户应具有非到期的密码。

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 服务器安全认证中的通用名称 (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 的长度可以设置为最大长度 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 数据库帐户设置区别名 (DN)，该帐户对基础 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*

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 数据库帐户指定密码：

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

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。

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。

步骤 9 （可选） 指定 Firepower 可扩展操作系统 使用此提供程序对用户进行身份验证的顺序：

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 指定系统在超时之前，尝试连接 LDAP 数据库时应花费的时间（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，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

步骤 1 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 # **set retries** *retry-num*

步骤 4 （可选） 设置在注明服务器已关闭之前，系统应等待 RADIUS 服务器发出响应的时间间隔：

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

Firepower 可扩展操作系统最多支持 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。

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 指定在注明服务器已关闭之前，系统应等待 RADIUS 服务器作出响应的时间间隔。

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 **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，启用双因素身份验证，并且提交任务：

```
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。如果单个提供程序包括任何这些属性的设置，Firepower 可扩展操作系统将使用该设置并忽略默认设置。

过程

步骤 1 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） 设置在注明服务器已关闭之前，系统应等待 TACACS+ 服务器发出响应的时间间隔：

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

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

Firepower 可扩展操作系统最多支持 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。

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 指定在注明服务器已关闭之前，系统应等待 TACACS+ 服务器作出响应的时间间隔：

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 将事务提交到系统配置：

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 #
```

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守护程序的服务器的一种方法。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 (Critical)”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。如果远程目标已启用，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-chassis /monitoring # **set syslog remote-destination** {**server-1** | **server-2** | **server-3**} **hostname** *hostname*

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 # **createdns** *{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 # **deletedns** *{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 #
```

第 10 章

接口管理

关于 Firepower 安全设备接口

Firepower 4100/9300 机箱支持单一接口以及 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。

接口类型

每个接口可以是以下类型之一：

- 数据（默认设置）- 不能在逻辑设备之间共享数据接口。
- 管理 - 可以在逻辑设备之间共享管理接口。只能为每个逻辑设备分配一个管理接口。

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

  诊断逻辑接口可以连同管理中心**设备 (Devices)** > **设备管理 (Device Management)** > **接口 (Interfaces)** 屏幕上的其余数据接口一起进行配置。使用诊断接口是可选的。诊断接口只允许管理流量，而不允许通过流量。

- 机箱管理 - 此物理管理接口用于通过 SSH 或 Firepower 机箱管理器来管理 FXOS 机箱。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。

  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 # **connectlocal-mgmt**

Firepower(local-mgmt) # **showmgmt-port**

- Firepower 事件 - 此接口是 Firepower 威胁防御设备的辅助管理接口。要使用此接口，您必须在 Firepower 威胁防御 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。
- 集群 - 用于集群逻辑设备的特殊接口类型。此类型自动分配到集群控制链路以进行设备间集群通信。默认情况下，系统会在端口通道 48 上自动创建集群控制链路。

注释 您可以使用 Firepower 管理中心或 Firepower 威胁防御 CLI 将两个上行链路、分支或数据端口接口配置为内联对。一旦将两个端口配置为内联对，它们将相当于一个接口。然后，此配置被传播到FXOS机箱。

请注意内联对的以下限制：

- 两个端口接口必须是唯一的。端口一旦加入一个内联对，将无法加入其他内联对。
- 只有上行链路端口、数据端口或分支端口才可以配置为内联对。

有关详细信息，请参阅《Firepower 管理中心配置指南》中的“配置 IPS 专用接口的内联集”部分。

硬件旁路对

对于 Firepower 威胁防御，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。硬件旁路可在停电时确保流量在内联接口对之间继续流动。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 硬件旁路应用中进行配置。您不需要将这些接口用作 硬件旁路对；它们可用作 ASA 和 Firepower 威胁防御应用的常规接口。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。

对于以下型号上特定网络模块的接口对，Firepower 威胁防御支持硬件旁路：

- Firepower 9300
- Firepower 4100 系列

这些型号的受支持硬件旁路网络模块包括：

- 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 铜缆 FTW 单位宽网络模块 (FPR-NM-8X1G-F)

硬件旁路只能使用以下端口对：

- 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。

编辑接口属性

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。

scopeeth-uplink

scope fabric a

步骤 2 启用接口。

enterinterface *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。您应该先使用 **enter interface** 命令编辑接口，然后再将其添加到端口通道。

步骤 3 （可选）设置接口类型。

setport-type {**data** | **firepower-eventing** | **mgmt** | **cluster**}

示例：

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

data 关键字为默认类型。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。

setadmin-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。

setadmin-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 148 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 #
```

创建端口通道

EtherChannel（也称为端口通道）最多可以包含 16 个同一类型的成员接口。

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

- EtherChannel 添加为独立逻辑设备的数据或管理端口
- EtherChannel 被添加为属于集群一部分的逻辑设备的管理或 CCL 端口
- EtherChannel 被添加为属于集群一部分的逻辑设备的数据端口，并且至少有一个安全模块已加入该集群

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

开始之前

Firepower 4100/9300 机箱仅在有效链路汇聚控制协议 (LACP) 模式下支持 EtherChannel。我们建议将连接交换机端口设置为“活动 (Active)”模式，以实现最佳兼容性。

过程

步骤 1 进入接口模式：

scopeeth-uplink

scope fabric a

步骤 2 创建端口通道：

createport-channel *id*

enable

步骤 3 分配成员接口：

createmember-port *interface_id*

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：

setport-type {**data** | **mgmt** | **cluster**}

示例：

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

data 关键字为默认类型。请勿选择 **cluster** 关键字，除非要将此端口类型用作集群控制链路，而不是默认设置。

步骤 5 （可选）为端口通道的所有成员设置接口速度：

setspeed {**10gbps** | **1gbps**}

示例：

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

步骤 6 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。

scopeeth-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，请在“name”中输入 **default** 。

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 #
```

配置分支电缆

以下操作步骤介绍如何配置分支电缆以用于 Firepower 4100/9300 机箱。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

具有 硬件旁路功能的接口不可为分支端口配置。

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：

scopecabling

scope fabric a

b) 创建分支：

createbreakout *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：

scopeeth-uplink

scopefabrica

scopeaggr-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。您应该先使用 **enter interface** 命令编辑接口，然后再将其添加到端口通道。

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

查看已安装接口

请按照以下程序查看机箱上已安装接口的状态。

过程

步骤 1 进入接口模式：

scopeeth-uplink

scope fabric a

步骤 2 显示机箱上的已安装接口：

showinterface

注释　此列表中不包含在端口通道中充当端口的接口。

示例

```
Firepower /eth-uplink/fabric # show interface

Interface:
    Port Name       Port Type          Admin State Oper State       State Reason
```

```
   --------------- ------------------ ----------- ---------------- ------------
   Ethernet1/1     Mgmt               Enabled     Up
   Ethernet1/2     Data               Enabled     Link Down        Link failure
or not-connected
   Ethernet1/3     Data               Enabled     Up
   Ethernet1/4     Data               Enabled     Sfp Not Present  Unknown
   Ethernet1/6     Data               Enabled     Sfp Not Present  Unknown
   Ethernet1/7     Data               Enabled     Sfp Not Present  Unknown
   Ethernet1/8     Data               Disabled    Sfp Not Present  Unknown
   Ethernet2/1     Data               Enabled     Up
   Ethernet2/2     Data               Enabled     Up
   Ethernet2/4     Data               Enabled     Up
   Ethernet2/5     Data               Enabled     Up
   Ethernet2/6     Data               Enabled     Up
   Ethernet3/2     Data               Enabled     Up
   Ethernet3/4     Data               Enabled     Up
```

第 11 章

逻辑设备

关于逻辑设备

创建逻辑设备时，Firepower 4100/9300 机箱管理引擎通过下载指定的软件版本并将引导程序配置和管理接口设置推送到指定的安全模块/引擎，或在使用机箱内集群的情况下推送到 Firepower 机箱中安装的所有安全模块来部署逻辑设备。

您可以创建以下两类逻辑设备之一：

- 独立 (Standalone) - 您可以为安装在 Firepower 机箱中的每个安全模块/引擎创建独立逻辑设备。
- 集群 (Cluster) - 通过集群，您可以将多个安全模块组合成一个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。

注释 在具有多个安全模块的 Firepower 9300 设备上，只能创建一种类型的逻辑设备（独立或集群）。换句话说，如果您已安装三个安全模块，则不能在一个安全模块上创建独立逻辑设备，而使用剩余的两个安全模块创建集群。

注释 如果您正在配置独立逻辑设备，必须在机箱中的所有模块上安装同一类型软件；此时不支持不同的软件类型。请注意，模块可以运行特定设备类型的不同版本，但所有模块必须配置为同一类型的逻辑设备。

创建独立的逻辑设备

您可以为安装在 Firepower 机箱中的每个安全模块/引擎创建独立的逻辑设备。

创建独立的 ASA 逻辑设备

您可以为 Firepower 4100/9300 机箱中安装的每个 安全模块/引擎 创建独立逻辑设备。在 Firepower 9300 等多模块设备上，如果您已配置了集群，则无法创建独立逻辑设备。您需要删除集群，然后才能配置独立设备。

注释 或者，您可以安装第三方 Radware DefensePro 虚拟平台，作为位于安全模块上 ASA 防火墙前面的 DDoS 检测和迁移服务（请参阅关于服务链， 第 190 页）。

注释 您必须在机箱中的所有模块上安装同一类型软件；目前不支持使用其他类型的软件。请注意，模块可以运行特定设备类型的不同版本，但所有模块必须配置为同一类型的逻辑设备。

开始之前

- 如果您想用于逻辑设备的安全模块/引擎上已配置了逻辑设备，则必须首先删除现有的逻辑设备（请参阅删除逻辑设备， 第 199 页）。
- 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 52 页），然后将映像下载到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 55 页）。
- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口（在 FXOS 中，您可能会看到该接口显示为 MGMT、management0 或其他类似名称） 不同。
- 您可以通过 Firepower 4100/9300 机箱部署一个路由防火墙模式的 ASA。

过程

步骤 1 进入安全服务模式：

Firepower# **scopessa**

步骤 2 创建逻辑设备：

Firepower /ssa # **createlogical-device** *device_name***asa** *slot_id***standalone**

步骤 3 输入逻辑设备说明：

Firepower /ssa/logical-device* # **setdescription** *"logical device description"*

步骤 4 向逻辑设备分配管理和数据接口：

Firepower /ssa/logical-device* # **createexternal-port-link** *name interface_id***asa**

Firepower-chassis /ssa/logical-device/external-port-link* # **exit**

name 由 Firepower 4100/9300 机箱管理引擎使用；它不是在安全模块配置中使用的接口名称。对各个接口重复此步骤。

步骤 5 配置管理引导程序信息：

a) 创建引导程序对象：

Firepower /ssa/logical-device* # **createmgmt-bootstrapasa**

b) 创建 ASA 管理员用户密码：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-key-secretPASSWORD**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **setvalue**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **exit**

预配置的 ASA 管理员用户在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: happytuesday
Confirm the value: happytuesday
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) 配置管理 IP 地址：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createipv4** *slot_id***default**

d) 设置网关地址：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setgateway** *gateway_address*

e) 设置 IP 地址和掩码：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setip** *ip_address***mask** *network_mask*

f) 退出管理 IP 配置范围：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **exit**

g) 退出管理引导程序配置范围：

Firepower /ssa/logical-device/mgmt-bootstrap* # **exit**

步骤 6 提交配置：

commit-buffer

确认系统配置任务。

示例

```
Firepower# scope ssa
Firepower /ssa # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # set description "logical device description"
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* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Value: <password>
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 1.1.1.254
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 1.1.1.1 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* # show configuration pending
+enter logical-device MyDevice1 asa 1 standalone
+    enter external-port-link inside Ethernet1/1 asa
+        set decorator ""
+        set description "inside link"
+    exit
+    enter external-port-link management Ethernet1/7 asa
+        set decorator ""
+        set description "management link"
+    exit
+    enter external-port-link outside Ethernet1/2 asa
+        set decorator ""
+        set description "external link"
+    exit
+    enter mgmt-bootstrap asa
+        enter bootstrap-key-secret PASSWORD
+            set value
+        exit
+        enter ipv4 1 default
+            set gateway 1.1.1.254
+            set ip 1.1.1.1 mask 255.255.255.0
+        exit
+    exit
+    set description "logical device description"
+exit
Firepower /ssa/logical-device* # commit-buffer
```

创建独立威胁防御逻辑设备

您可以为 Firepower 4100/9300 机箱中安装的每个 安全模块/引擎 创建独立逻辑设备。在 Firepower 9300 等多模块设备上，如果您已配置了集群，则无法创建独立逻辑设备。您需要删除集群，然后才能配置独立设备。

注释 或者，您可以安装第三方 Radware DefensePro 虚拟平台，作为位于安全模块上 Firepower 威胁防御逻辑设备前面的 DDoS 检测和迁移服务（请参阅关于服务链，第 190 页）。

注释 您必须在机箱中的所有模块上安装同一类型软件；目前不支持使用其他类型的软件。请注意，模块可以运行特定设备类型的不同版本，但所有模块必须配置为同一类型的逻辑设备。

开始之前

- 如果您想用于逻辑设备的安全模块/引擎上已配置了逻辑设备，必须首先删除现有的逻辑设备（请参阅删除逻辑设备，第 199 页）。
- 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 52 页），然后将映像下载到 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 55 页）。
- 配置逻辑设备要使用的管理接口。管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口（在 FXOS 中，您可能会看到该接口显示为 MGMT、management0 或其他类似名称） 不同。您还必须至少配置一个数据类型的接口。或者，您也可以创建 Firepower 事件接口，传输所有事件流量（例如 Web 事件）。有关详细信息，请参阅接口类型，第 143 页。

过程

步骤 1 进入安全服务模式：

Firepower# **scopessa**

步骤 2 创建逻辑设备：

Firepower /ssa # **createlogical-device** *device_name***ftd** *slot_id***standalone**

device_name 由Firepower 4100/9300 机箱管理引擎用于配置管理设置以及分配接口；它不是在安全模块配置中使用的设备名称。

步骤 3 向逻辑设备分配管理和数据接口：

Firepower /ssa/logical-device* # **createexternal-port-link** *name interface_id***ftd**

Firepower-chassis /ssa/logical-device/external-port-link* # **exit**

name 由 Firepower 4100/9300 机箱管理引擎使用；它不是在安全模块配置中使用的接口名称。对各个接口重复此步骤。

步骤 4 配置管理引导程序参数：

a) 创建引导程序对象：

Firepower /ssa/logical-device* # **createmgmt-bootstrapftd**

b) 指定管理 Firepower 管理中心的 IP 地址：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-keyFIREPOWER_MANAGER_IP**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **set value** *IP_address*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **exit**

c) 指定逻辑设备的运行模式（路由或透明）：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-keyFIREWALL_MODE**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **set value** *firewall_mode*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **exit**

d) 指定设备和 Firepower 管理中心要共享的密钥：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-key-secretREGISTRATION_KEY**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **set value**

值：*registration_key*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **exit**

e) 指定用于逻辑设备的密码：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-key-secretPASSWORD**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **set value**

值：*password*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **exit**

f) 指定逻辑设备的完全限定主机名：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-keyFQDN**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **set value** *fqdn*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **exit**

g) 指定逻辑设备使用的 DNS 服务器列表（用逗号隔开）；

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-keyDNS_SERVERS**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **set value** *dns_servers*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **exit**

h) 指定逻辑设备的搜索域名（用逗号隔开）：

Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-keySEARCH_DOMAINS**

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **set value** *search_domains*

Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # **exit**

i) 配置管理接口设置：

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：

   Firepower /ssa/logical-device/mgmt-bootstrap* # **createipv4** *slot_id***firepower**

2. 设置网关地址：

   Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setgateway** *gateway_address*

3. 设置 IP 地址和掩码：

   Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setip** *ip_address***mask** *network_mask*

4. 退出管理 IP 配置范围：

   Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **exit**

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：

   Firepower /ssa/logical-device/mgmt-bootstrap* # **createipv6** *slot_id***firepower**

2. 设置网关地址：

   Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # **setgateway** *gateway_address*

3. 设置 IP 地址和前缀：

   Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # **set ip** *ip_address***prefix-length** *prefix*

4. 退出管理 IP 配置范围：

   Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # **exit**

j) 退出管理引导程序模式：

Firepower /ssa/logical-device/mgmt-bootstrap* #**exit**

步骤 5 接受最终用户许可协议：

a) Firepower /ssa/logical-device* # **exit**
b) Firepower /ssa* #**show app-instance**

显示 Firepower 威胁防御应用的版本。

c) Firepower /ssa* #**scope app ftd** *application_version*
d) Firepower /ssa/app* #**show license-agreement**
e) Firepower /ssa/app* #**accept-license-agreement**

f) Firepower /ssa/app* #**exit**

步骤 6 （可选） 安装 Radware DefensePro 实例：

Firepower /ssa* # **scope slot** *slot_id*

Firepower/ssa/slot* # **createapp-instance vdp**

执行此程序中的最后一步以确认逻辑设备配置后，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 服务链，第 191 页程序，从第 4 步开始。对于 Firepower 4110 和 4120，必须先创建应用实例，然后才能提交逻辑设备配置。

步骤 7 提交配置：

commit-buffer

确认系统配置任务。

示例

```
Firepower# scope ssa
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
Value:
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
Value:
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* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* # exit
Firepower /ssa* # scope app ftd 6.0.0.837
Firepower /ssa/app* # accept-license-agreement
Firepower /ssa/app* # commit-buffer
```

部署高可用性对

Firepower威胁防御或ASA高可用性（也称为故障转移）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。

过程

步骤 1 每个逻辑设备应位于单独的机箱上；不建议为 Firepower 9300 配置机箱内高可用性，而且可能不支持此功能。

步骤 2 将相同的接口分配给各个逻辑设备。

步骤 3 为故障转移和状态链路分配 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转移和状态链路。如果您有可用的接口，可以使用单独的故障转移和状态链路；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转移或状态链路。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转移接口。

步骤 4 根据《Firepower 威胁防御或 ASA 配置指南》，在逻辑设备上启用高可用性。

步骤 5 如果您在启用高可用性后需要更改接口，请先在备用设备上执行更改，然后再在活动设备上执行更改。

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 中手动删除旧的接口配置。

部署集群

通过集群，您可以将多台设备组合成单个逻辑设备。集群具有单个设备的全部便捷性（管理、集成到一个网络中），同时还能实现吞吐量增加和多个设备的冗余性。包含多个模块的 Firepower 9300 支持机箱内集群，您可以将单个机箱中的所有模块组合到一个集群中。您还可使用将多个机箱分组在一起的机箱间集群；机箱间集群是单模块设备（例如 Firepower 4100 系列）的唯一选择。

关于 Firepower 4100/9300 机箱上的集群

集群由充当单一逻辑单元的多个设备组成。在 Firepower 4100/9300 机箱 上部署集群时，它执行以下操作：

- 为设备间通信创建集群控制链路（默认情况下，使用端口通道 48）。对于机箱内集群（仅限 Firepower 9300），此链路利用 Firepower 9300背板进行集群通信。对于机箱间集群，需要手动将物理接口分配到此 EtherChannel 以进行机箱间通信。
- 在应用中创建集群引导程序配置。

  在部署集群时，Firepower 4100/9300 机箱 管理引擎将最低引导程序配置推送到包含集群名称、集群控制链路接口及其他集群设置的每个设备。如果您需要自定义集群环境，可以在应用内对引导程序配置的某些用户可配置部分进行配置。
- 将数据接口作为跨网络接口分配给集群。

  对于机箱内集群，跨网络接口不仅限于 EtherChannel，与机箱间集群类似。Firepower 9300 管理引擎在内部利用 EtherChannel 技术，将流量负载均衡到共享接口上的多个模块，使任何数据接口类型都可用于跨网络模式。对于机箱间集群，必须对所有数据接口使用跨网络 EtherChannel。

  注释 除管理接口以外，不支持单个接口。
- 向集群中的所有设备分配管理接口。

以下部分提供有关集群概念和实施的更多详细信息。

主设备角色和辅助设备角色

集群的一个成员是主设备。系统自动确定主设备。所有其他成员都是辅助设备。

您必须仅在主设备上执行所有配置；然后，配置将复制到辅助设备。

集群控制链接

集群控制链路使用端口通道48接口自动进行创建。对于机箱内集群，此接口没有成员接口。对于机箱间集群，必须将一个或多个接口添加到 EtherChannel。此集群类型 EtherChannel 利用 Firepower 9300 背板进行机箱内集群的集群通信。

对于包含 2 个成员的机箱间集群，请勿直接将集群控制链路从一个机箱连接到另一个机箱。如果直接连接两个接口，则当一台设备发生故障时，集群控制链路失效，会导致剩下的那台正常设备也发生故障。而如果通过交换机连接集群控制链路，则集群控制链路仍会对正常设备打开。

集群控制链路流量包括控制流量和数据流量。

设定机箱间集群的集群控制链路大小

如果可能，应将集群控制链路的大小设定为与每个机箱的预期吞吐量匹配，以使集群控制链路可以处理最坏情况。

集群控制链路流量主要由状态更新和转发的数据包组成。集群控制链路在任一给定时间的流量大小不尽相同。转发流量的大小取决于负载均衡的效率或是否存在大量用于集中功能的流量。例如：

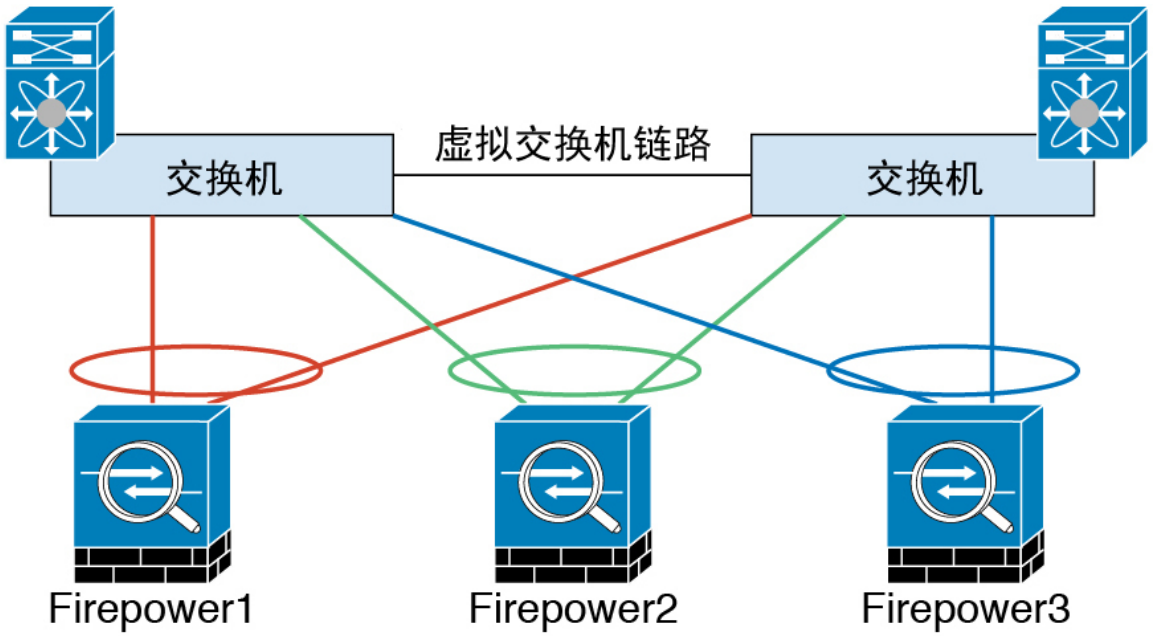
- NAT 会使连接的负载均衡不佳，需要对所有返回流量进行再均衡，将其转发到正确的设备。
- 当成员身份更改时，集群需要对大量连接进行再均衡，因此会暂时耗用大量集群控制链路带宽。

带宽较高的集群控制链路可以帮助集群在发生成员身份更改时更快地收敛，并防止出现吞吐量瓶颈。

注释 如果集群中存在大量非对称（再均衡）流量，应增加集群控制链路的吞吐量大小。

机箱间集群的集群控制链路冗余

下图显示了如何在虚拟交换系统 (VSS) 或虚拟端口通道 (vPC) 环境中使用 EtherChannel 作为集群控制链路。EtherChannel 中的所有链路都是活动链路。当交换机是 VSS 或 vPC 的一部分时，您可以将同一 EtherChannel 中的 Firepower 4100/9300 机箱接口连接到 VSS 或 vPC 中的单独交换机。交换机接口是同一个 EtherChannel 端口通道接口的成员，因为两台单独的交换机的行为就像一台交换机一样。请注意，此 EtherChannel 是设备本地的，而非跨网络 EtherChannel。



机箱间集群的集群控制链路可靠性

为了确保集群控制链路的功能，设备之间的往返时间 (RTT) 务必要小于 20 毫秒。此最大延迟能够增强与不同地理位置安装的集群成员的兼容性。要检查延迟，请在设备之间的集群控制链路上执行 ping 操作。

集群控制链路必须可靠，没有数据包无序或丢弃数据包的情况；例如，站点间部署应使用专用链路。

集群控制链路网络

Firepower 4100/9300 机箱会根据机箱 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：127.2.*chassis_id*.*slot_id*。在 FXOS 或应用中，均无法手动设置此 IP 地址。 集群控制链路网络不能包含设备之间的任何路由器；仅允许第 2 层交换。对于站点间流量，思科建议使用重叠传输虚拟化 (OTV)。

管理网络

我们建议将所有设备都连接到一个管理网络。此网络与集群控制链路分隔开来。

管理界面

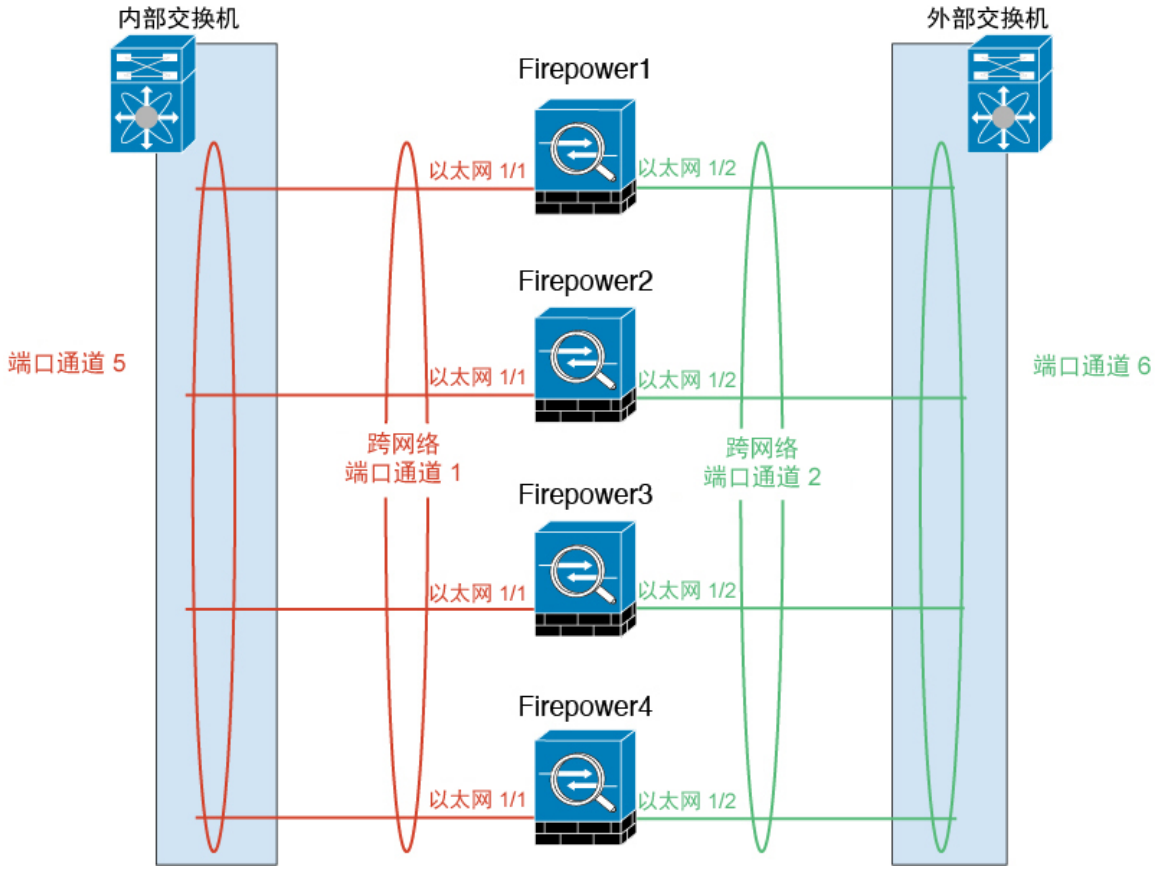
必须为集群分配管理类型的接口。此接口是相对于跨网络 (Spanned) 接口的特殊单独接口。通过管理接口，可以直接连接到每个设备。

对于ASA，主集群IP地址是始终属于当前主设备的集群的固定地址。您必须配置一个地址范围，使每个设备（包括当前主设备在内）都能使用该范围内的本地地址。主集群 IP 地址提供对地址的统一管理访问权限；当主设备更改时，主集群 IP 地址将转移给新的主设备，使集群管理可以无缝衔接。本地 IP 地址用于路由，在排除故障时也非常有用。例如，可以通过连接到主集群 IP 地址来管理集群，该地址始终连接到当前主设备。要管理单个成员，您可以连接到本地 IP 地址。对于 TFTP 或系统日志等出站管理流量，包括主设备在内的每个设备都使用本地 IP 地址来连接到服务器。

对于 Firepower 威胁防御，请向同一网络上的每个设备分配管理 IP 地址。将每个设备连接到 管理中心时，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都可以配置跨网络 EtherChannel。在路由模式下，EtherChannel 被配置为只有一个 IP 地址的路由接口。在透明模式下，IP 地址分配到 BVI 而非网桥组成员接口。负载均衡属于 EtherChannel 固有的基本操作。



站点间集群

对于站点间安装，您只要遵循建议的准则即可充分发挥集群的作用。

您可以将每个集群机箱配置为属于单独的站点 ID。

站点 ID 与站点特定的 MAC 地址和 IP 地址配合使用。集群发送的数据包使用站点特定的 MAC 地址和 IP 地址，而集群接收的数据包使用全局 MAC 地址和 IP 地址。此功能可防止交换机从两个不同端口上的两个站点获知相同全局 MAC 地址，导致 MAC 地址摆动；相反，它们仅获知站点 MAC 地址。只有使用跨网络 EtherChannel 的路由模式支持站点特定的 MAC 地址和 IP 地址。

站点 ID 还用于使用 LISP 检查、导向器本地化来实现流量移动，以提高性能、减少数据中心的站点间集群的往返时间延迟不同的站点上。

有关站点间集群的详细信息，请参阅以下各节：

- 确定数据中心互联的规格 -集群要求，第 166 页
- 站点间准则 -面向集群的指导原则，第 167 页
- 站点间示例 -站点间集群示例，第 186 页

集群要求

机箱间硬件和软件要求

集群中的所有机箱：

- 对于 Firepower 4100 系列：所有机箱必须为同一型号。对于 Firepower 9300：所有安全模块必须为同一类型。您可以在各机箱中安装不同数量的安全模块，但机箱中存在的所有模块（包括任何空插槽）必须属于集群。
- 除进行映像升级外，必须运行完全相同的 FXOS 软件。
- 对于分配给集群的接口，必须采用相同的接口配置，例如：相同的管理接口、EtherChannel、主用接口、速度和复用等。您可在机箱中使用不同的网络模块类型，但必须满足以下条件：对于相同接口 ID，容量必须匹配，且接口可成功捆绑于同一跨网络 EtherChannel 中。请注意，所有数据接口必须是机箱间集群中的 EtherChannel。如果您要在启用集群（例如，通过添加或删除接口模块，或配置 Etherchannel）后更改 FXOS 中的接口，则请对每个机箱执行相同更改，从从属设备开始，到主设备结束。
- 必须使用同一台 NTP 服务器。对于 Firepower 威胁防御，Firepower 管理中心也必须使用同一 NTP 服务器。请勿手动设置时间。
- ASA：每个 FXOS 机箱都必须注册到许可证颁发机构或卫星服务器。从属设备不会产生额外成本。对于预留永久许可证，必须为每个机箱购买单独的许可证。对于 Firepower 威胁防御，所有许可由 Firepower 管理中心处理。

机箱间集群交换机必备条件

- 请务必先完成交换机配置并将机箱中的所有 EtherChannel 成功连接至交换机后，再在 Firepower 4100/9300 机箱 上配置集群。
- 有关受支持的交换机列表，请参阅《思科 FXOS 兼容性》。

调整站点间集群的数据中心互联

您应在数据中心互联 (DCI) 上为集群控制链路流量保留等同于以下计算结果的带宽：

$$\frac{\text{每个站点的集群成员数量}}{2} \times \text{每个成员的集群控制链路大小}$$

如果各站点的成员数不同，请使用较大的数量进行计算。DCI 的最低带宽不得低于一个成员的集群控制链路的流量大小。

例如：

- 位于 4 个站点的 2 个成员：
  - 总共 4 个集群成员
  - 每个站点 2 个成员

- 每个成员 5 Gbps 集群控制链路

保留的 DCI 带宽 = 5 Gbps (2/2 x 5 Gbps)。

- 对位于 3 个站点的 6 个成员而言，规格加大：
  - 总共 6 个集群成员
  - 站点 1 有 3 个成员，站点 2 有 2 个成员，站点 3 有 1 个成员
  - 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 15 Gbps (3/2 x 10 Gbps)。

- 位于 2 个站点的 2 个成员：
  - 总共 2 个集群成员
  - 每个站点 1 个成员
  - 每个成员 10 Gbps 集群控制链路

保留的 DCI 带宽 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps；但最低带宽不得低于集群控制链路的流量大小 (10 Gbps)）。

面向集群的指导原则

模式

- Firepower 9300 上的 ASA - 支持机箱内、机箱间和站点间集群。
- Firepower 4100 系列 上的 ASA - 支持机箱间和站点间集群。
- Firepower 9300 上的 Firepower 威胁防御 - 支持机箱内和机箱间集群。
- Firepower 4100 系列 上的 Firepower 威胁防御 - 支持机箱间集群。
- Radware DefensePro - 对于包含 ASA 的机箱内集群受支持。
- Radware DefensePro - 对于包含 Firepower 威胁防御的机箱内集群受支持。

机箱间集群的交换机

- 对于 ASR 9006，如果要设置非默认 MTU，请将 ASR 接口 MTU 设置为高于集群设备 MTU 14 个字节。除非使用 **mtu-ignore** 选项，否则 OSPF 邻近对等尝试可能会失败。请注意，集群设备 MTU 应与 ASR *IPv4* MTU 匹配。
- 在用于集群控制链路接口的交换机上，您可以选择在连接到集群设备的交换机端口上启用生成树 PortFast 来加快新设备加入集群的过程。

- 当发现交换机上跨网络 EtherChannel 的绑定速度缓慢时，可以对交换机上的单个接口启用快速 LACP 速率。请注意，某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。
- 在交换机上，我们建议使用以下其中一种 EtherChannel 负载均衡算法：**source-dest-ip** 或 **source-dest-ip-port**（请参阅思科 Nexus OS 和思科 IOS **port-channel load-balance** 命令）。请勿在负载均衡算法中使用关键字 **vlan**，否则会导致传输到集群中的设备的流量分摊不均。
- 如果在交换机上更改 EtherChannel 的负载均衡算法，则交换机上的 EtherChannel 接口将暂时停止转发流量，生成树协议重新启动。在流量再次开始传输之前会存在延迟。
- 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-distributionfixed**

  请勿全局更改算法；您可能需要对 VSS 对等链路使用自适应算法。

机箱间集群的 EtherChannel

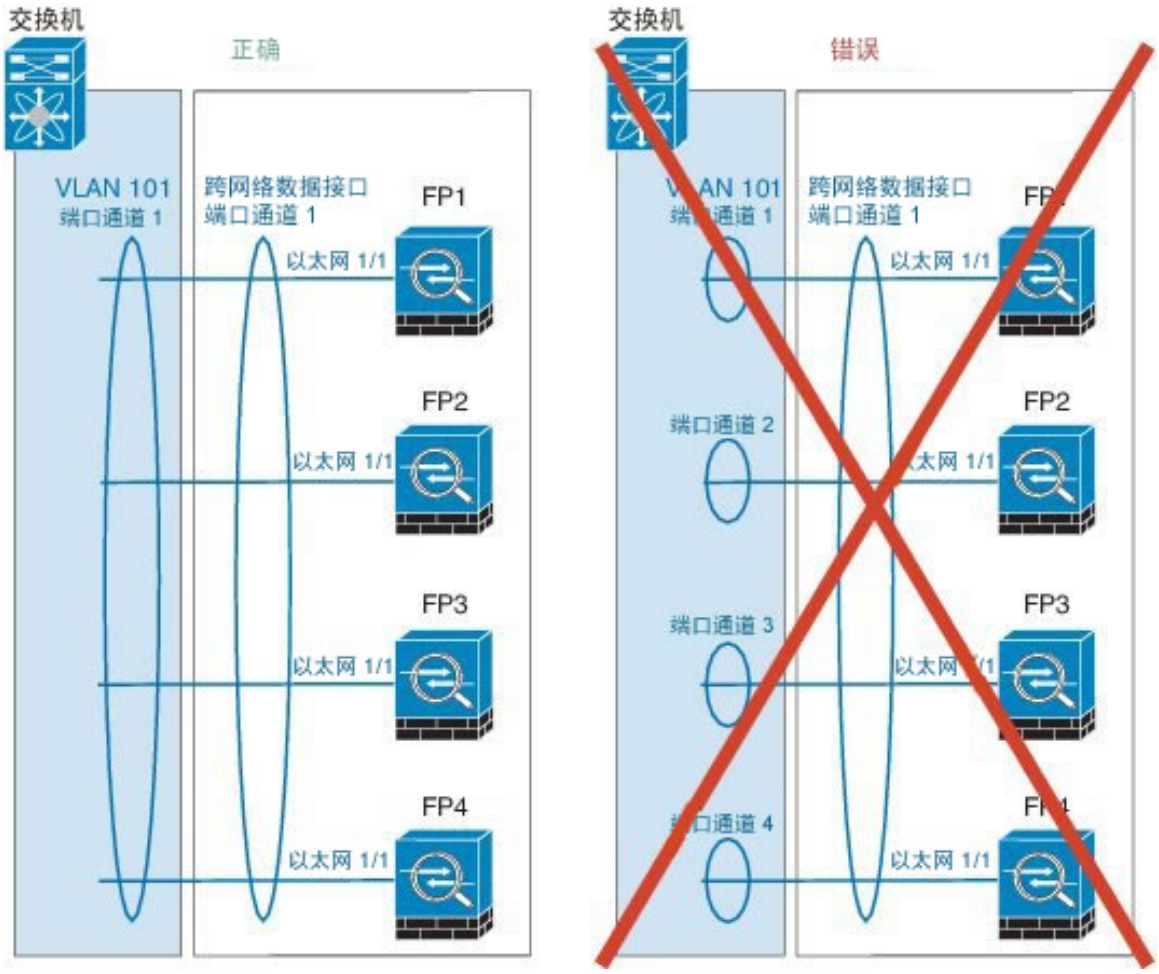
- 为了连接交换机，请将 EtherChannel 模式设置为 Active；Firepower 4100/9300 机箱 不支持 ON 模式，甚至对于集群控制链路也是如此。
- 默认情况下系统将 FXOS EtherChannel 的 LACP 速率设为正常。此设置可能使端口通道成员的捆绑时间超过 30 秒，从而导致集群接口运行状况检查失败，这会让设备从集群中删除。我们建议您将 LACP 速率更改为快速。以下示例修改了“默认”lacp 策略：

```
firepower# scope org
firepower /org # scope lacppolicy default
firepower /org/lacppolicy# set lacp-rate fast
firepower /org* # commit-buffer
```

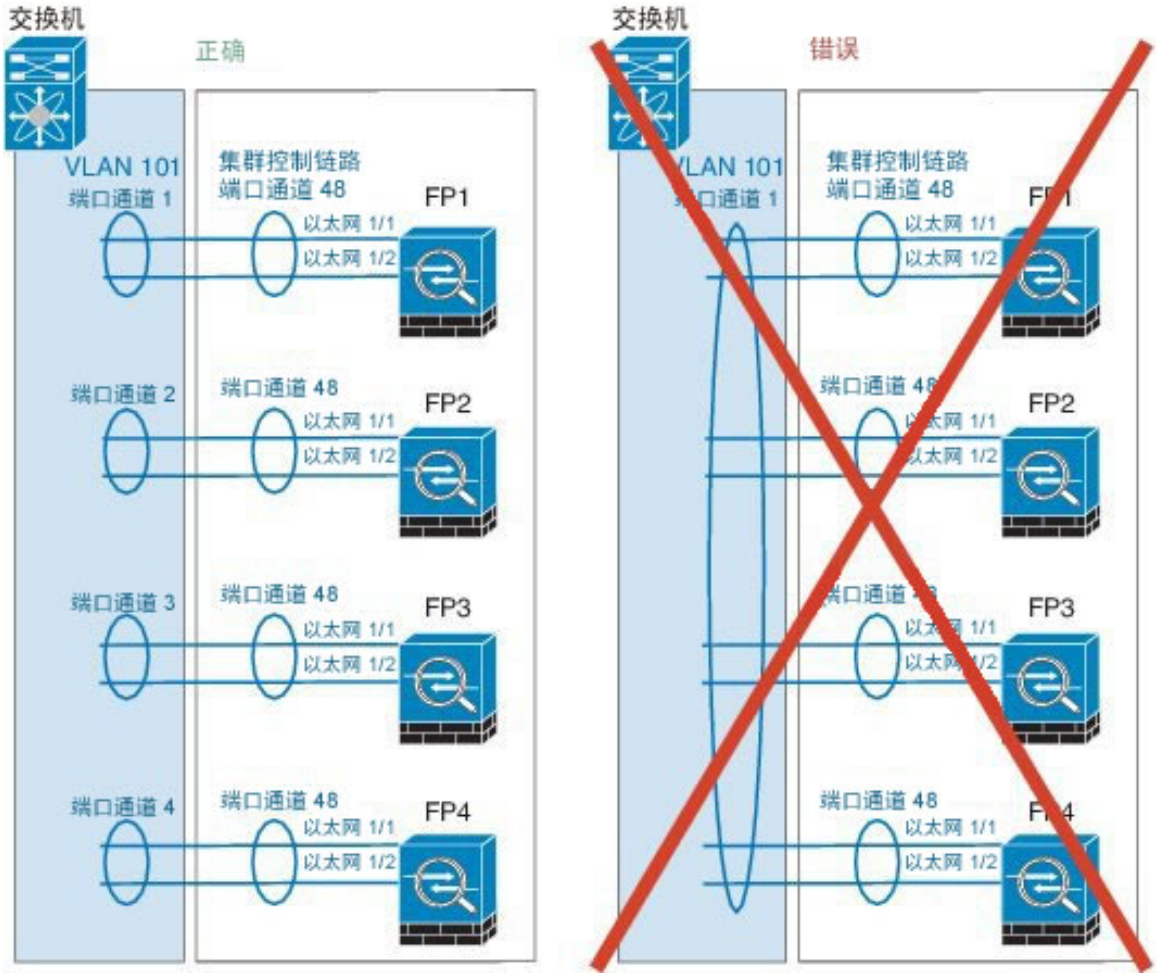
> **注释** 某些交换机（如 Nexus 系列）在执行服务中软件升级 (ISSU) 时不支持 LACP 速率“快速”，因此我们建议不要一起使用 ISSU 与集群。

- 在低于 15.1(1)S2 的 Catalyst 3750-X 思科 IOS 软件版本中，此集群设备不支持将 EtherChannel 连接到交换机堆叠。在默认交换机设置下，如果跨堆叠连接集群设备 EtherChannel，则当主交换机关闭时，连接到其余交换机的 EtherChannel 不会正常工作。要提高兼容性，请将 **stack-mac persistent timer** 命令设置为一个足够大的值，以考虑重新加载时间；例如，8 分钟或无限接近 0。或者，您可以升级到更加稳定的交换机软件版本，例如 15.1(1)S2。
- 跨网络与设备本地 EtherChannel 配置 - 请务必为跨网络 EtherChannel 和设备本地 EtherChannel 适当地配置交换机。

- 跨网络 EtherChannel - 对于跨越所有集群成员的集群设备跨网络 EtherChannel，所有接口在交换机上合并为一个 EtherChannel。请确保每个接口都属于交换机上的同一个通道组。



- 设备本地 EtherChannel - 对于集群设备本地 EtherChannels，包括为集群控制链路配置的任何 EtherChannel，请务必在交换机上配置分散的 EtherChannel；请勿在交换机上将多个集群设备 EtherChannel 合并为一个 EtherChannel。



其他规定

- 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。

集群默认设置

集群控制链路使用端口通道 48。

配置 ASA 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，在下一个机箱上输入基本相同的设置。

开始之前

- 您必须对 Firepower 9300 机箱中全部 3 个模块插槽启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
- 在**接口 (Interfaces)** 选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。
- 您可以通过 Firepower 4100/9300 机箱部署一个路由防火墙模式的 ASA。

过程

步骤 1 部署集群之前，至少配置一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。请参阅创建端口通道，第 147 页或编辑接口属性，第 145 页。

默认情况下，所有接口都会分配给集群。部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的 EtherChannel。在每个机箱上添加 EtherChannel。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。请参阅创建端口通道，第 147 页或编辑接口属性，第 145 页。

管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口不同（在 FXOS 中，您可能会看到机箱管理接口显示为 MGMT、management0 或其他类似名称）。

步骤 3 端口通道 48 预留为集群控制链路。对于机箱间集群，至少向端口通道 48 添加一个成员接口。

步骤 4 进入安全服务模式：

scopessa

示例：

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

步骤 5 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**。您必须对 Firepower 9300 机箱中全部 3 个模块插槽启用集群，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 6 创建管理引导程序对象。

entermgmt-bootstrapasa

示例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

步骤 7 指定管理员用户密码。

enterbootstrap-key-secretPASSWORD

setvalue

exit

exit

预配置的 ASA 管理员用户在进行密码恢复时非常有用；如果您有 FXOS 访问权限，在您忘记了管理员用户密码时，可以将其重置。

示例：

```
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: happytuesday
Confirm the value: happytuesday
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

步骤 8 配置集群参数：

enter cluster-bootstrap

示例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

步骤 9 在安全模块配置中设置集群组名称。

set service-type *cluster_name*

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

名称必须是长度为 1 到 38 个字符的 ASCII 字符串。

步骤 10 设置集群接口模式：

set mode spanned-etherchannel

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

跨网络 EtherChannel 模式是唯一支持的模式。

步骤 11 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。

a) 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。属于当前主设备的虚拟 IP 地址（称作“主集群 IP 地址”）不在此地址池中；请务必在同一个网络中为主集群 IP 地址保留一个 IP 地址。您可以使用 IPv4 和/或 IPv6 地址。

b) 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。

c) 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
```

步骤 12 设置机箱 ID：

set chassis-id *id*

集群中的每个机箱都需要唯一 ID。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

步骤 13 对于站点间集群，将站点 ID 设置为 1 和 8 之间的整数：

set site-id *number*。

示例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

步骤 14 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。

共享密钥是长度为 1 到 63 个字符的 ASCII 字符串。共享密钥用于生成密钥。此选项不影响数据路径流量，包括连接状态更新和转发的数据包，它们始终以明文发送。

步骤 15 退出集群引导程序模式和逻辑设备模式：

exit

exit

步骤 16 查看可用的软件版本，然后设置要使用的版本：

a) 显示可用版本：

show app

示例：

```
/ssa # show app

Application:
    Name       Version    Description Author     Deploy Type  CSP Type    Is Default App

    ---------- ---------- ----------- ---------- -----------  ----------- --------------

     asa        9.1.4.152  N/A         cisco      Native       Application Yes
     asa        9.4.2      N/A         cisco      Native       Application No
     asa        9.5.2.1    N/A         cisco      Native       Application No
```

b) 进入要使用的版本的应用模式：

scope app asa *version_number*

c) 将此版本设置为默认版本：

set-default

d) 退出应用模式：

exit

示例：

```
/ssa* # scope app asa 9.5.2.1
/ssa/app* # set-default
/ssa/app* # exit
/ssa* #
```

步骤 17 提交配置：

commit-buffer

Firepower 4100/9300 机箱管理引擎通过下载默认安全模块软件版本并将集群引导程序配置和管理接口设置推送到各安全模块来部署集群。

步骤 18 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，两个机箱将会使用同一配置。

步骤 19 连接到主设备 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
```

配置 Firepower 威胁防御集群

您可以从 Firepower 4100/9300 机箱管理引擎轻松部署集群。自动为每台设备生成所有初始配置。 对于机箱间集群，您必须单独配置每个机箱。在一个机箱上部署集群；然后，您可以将引导程序配置从第一个机箱复制到下一个机箱，实现轻松部署。

开始之前

- 您必须对 Firepower 9300 机箱中全部 3 个模块插槽启用集群，即使您没有安装模块。如果不配置全部 3 个模块，集群将不会正常工作。
- 在**接口 (Interfaces)** 选项卡上，如果不包括任何成员接口，则端口通道 48 集群类型接口的**运行状态 (Operation State)**将显示为**失败 (failed)**。对于机箱内集群，此 EtherChannel 无需任何成员接口，您可忽略此“运行状态 (Operational State)”。

过程

步骤 1 部署集群之前，至少配置一个“数据 (Data)”类型接口或 EtherChannel（也称为端口通道）。请参阅创建端口通道，第 147 页或编辑接口属性，第 145 页。

部署之后，您也可以将数据接口添加到集群。

对于机箱间集群，所有数据接口必须为至少带有一个成员接口的 EtherChannel。在每个机箱上添加 EtherChannel。

步骤 2 （可选）部署集群之前，配置 Firepower 事件类型接口。请参阅编辑接口属性，第 145 页。

此接口是 Firepower 威胁防御设备的二级管理接口。要使用此接口，您必须在 Firepower 威胁防御 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 管理中心命令参考中的 **configure network** 命令。

步骤 3 添加“管理 (Management)”类型接口或 EtherChannel。请参阅创建端口通道，第 147 页或编辑接口属性，第 145 页。

管理接口是必需的。请注意，此管理接口与仅用于机箱管理的机箱管理接口不同（在 FXOS 中，您可能会看到机箱管理接口显示为 MGMT、management0 或其他类似名称）。

步骤 4 端口通道 48 预留为集群控制链路。对于机箱间集群，至少向端口通道 48 添加一个成员接口。

步骤 5 进入安全服务模式：

scopessa

示例：

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

步骤 6 创建集群：

enter logical-device *device_name***ftd "1,2,3" clustered**

示例：

```
Firepower /ssa # enter logical-device FTD1 ftd "1,2,3" clustered
Firepower /ssa/logical-device* #
```

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。

注释 您必须启用对机箱中全部 3 个模块插槽的集群，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。

步骤 7 配置集群引导程序参数：

a) 创建集群引导程序对象：

enter 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，将站点 ID 设置为 1 和 8 之间的整数：

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) 在安全模块配置中设置集群密钥：

set key

系统将提示您输入共享密钥。

共享密钥是长度为 1 到 63 个字符的 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

跨网络 EtherChannel 模式是唯一支持的模式。

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。

g) 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 8 配置管理引导程序参数：

a) 创建管理引导程序对象：

entermgmt-bootstrapftd

b) 指定管理 Firepower 管理中心的 IP 地址：

enterbootstrap-keyFIREPOWER_MANAGER_IP

setvalue *IP_address*

exit

c) 指定逻辑设备的运行模式（路由或透明）：

enterbootstrap-keyFIREWALL_MODE

setvalue {**routed** | **transparent**}

exit

d) 指定设备和 Firepower 管理中心之间要共享的密钥：

enterbootstrap-key-secretREGISTRATION_KEY

setvalue

registration_key

exit

e) 指定用于逻辑设备的密码：

enterbootstrap-key-secretPASSWORD

setvalue

password

exit

f) 指定逻辑设备的完全限定主机名：

enterbootstrap-keyFQDN

setvalue *fqdn*

exit

g) 指定逻辑设备使用的 DNS 服务器列表（用逗号隔开）；

enterbootstrap-keyDNS_SERVERS

setvalue *dns_servers*

exit

h) 指定逻辑设备的搜索域名（用逗号隔开）：

enterbootstrap-keySEARCH_DOMAINS

setvalue *search_domains*

exit

i) 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：

   enteripv4 *slot_id***firepower**

2. 设置网关地址：

   setgateway *gateway_address*

3. 设置 IP 地址和掩码：

   setip *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：

   enteripv6 *slot_id***firepower**

2. 设置网关地址：

   setgateway *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。

j) 退出管理引导程序模式：

   exit

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 9 退出逻辑设备模式：

exit

步骤 10 查看可用的软件版本，然后设置要使用的版本：

a) 显示可用版本：

show app

示例：

```
/ssa # show app

Application:
    Name       Version    Description Author     Deploy Type CSP Type    Is Default App

    ---------- ---------- ----------- ---------- ----------- ----------- --------------

    ftd        6.0.1.37   N/A         cisco      Native      Application Yes
    ftd        6.1.0.11   N/A         cisco      Native      Application No
    ftd        6.1.0.21   N/A         cisco      Native      Application No
```

b) 进入要使用的版本的应用模式：

scope app ftd *version_number*

c) 将此版本设置为默认版本：

set-default

d) 接受此版本的最终用户许可协议：

accept-license-agreement

e) 退出应用模式：

exit

示例：

```
/ssa # scope app ftd 6.1.0.21
/ssa/app # set-default
/ssa/app* # accept-license-agreement
/ssa/app* # exit
/ssa* #
```

步骤 11 提交配置：

commit-buffer

Firepower 4100/9300 机箱管理引擎通过下载默认安全模块软件版本并将集群引导程序配置和管理接口设置推送到各安全模块来部署集群。

步骤 12 要向集群添加其他机箱，请重复此程序过程，但必须配置唯一的 **chassis-id** 和唯一的管理 IP 地址；否则，两个机箱会使用同一配置。

步骤 13 使用管理 IP 地址将每个安全模块添加到 Firepower 管理中心，然后在 Web 界面上将其组成集群。

所有集群设备必须在 FXOS 上已成功建立的集群中，然后才可将其添加到 Firepower 管理中心 中。

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
    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
 accept-license-agreement
 exit
commit-buffer
```

站点间集群示例

以下示例显示支持的集群部署。

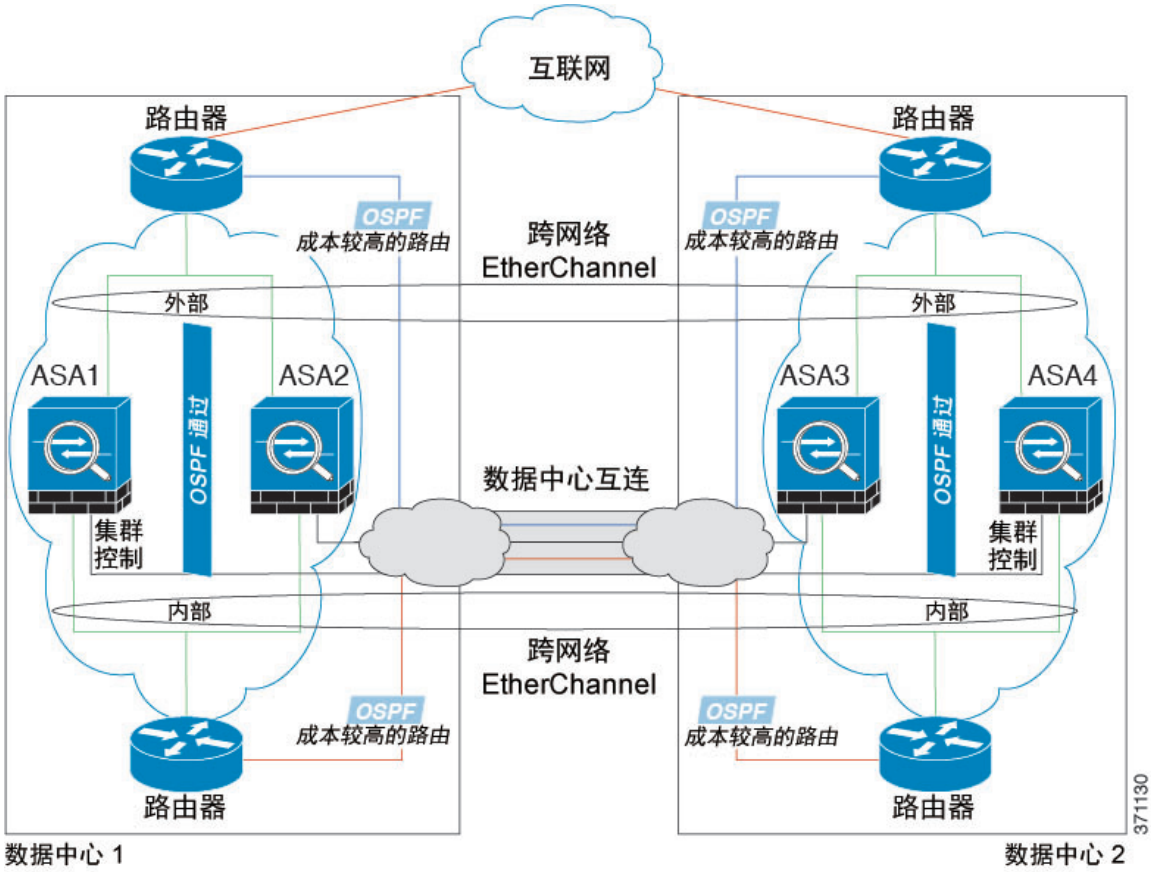
跨网络 EtherChannel 透明模式南北站点间集群示例

以下示例显示了 2 个集群成员，这两个集群成员分别位于 2 个部署在内部和外部路由器之间（南北插入）的数据中心。集群成员由集群控制链路通过 DCI 连接。位于每个站点的集群成员使用面向内部和外部的跨网络 EtherChannel 连接到本地交换机。每个 EtherChannel 跨越集群中的所有机箱。

位于每个数据中心的内部和外部路由器均使用 OSPF（可通过透明的 ASA）。与 MAC 地址不同，路由器 IP 地址在所有路由器上都是唯一的。通过指定 DCI 中开销较高的路由，可将流量保持在每个数据中心内，除非给定站点上的所有集群成员都中断连接。通过 ASA 的开销较低的路由必须经过位于每个站点的同一网桥组才能使集群维持非对称连接。如果位于一个站点的所有集群成员都发生故障，流量将从每台路由器通过 DCI 发往位于另一个站点的集群成员。

位于每个站点的交换机的实施可包括：

- 站点间 VSS/vPC - 在此情景中，一台交换机安装在数据中心 1，另一台交换机安装在数据中心 2。一个方案是将位于每个数据中心的集群设备只连接到本地交换机，而 VSS/vPC 流量通过 DCI 传输。在此情况下，连接多半会保持在每个数据中心本地。如果 DCI 可以处理额外的流量，您也可以选择将每台设备通过 DCI 连接到两台交换机。在此情况下，流量跨数据中心分摊，因此 DCI 必须非常强健稳定。
- 位于每个站点的本地 VSS/vPC - 为了获得更高的交换机冗余能力，您可以在每个站点安装 2 对单独的 VSS/vPC。在此情况下，尽管集群设备仍然有一个跨网络 EtherChannel 将数据中心 1 的机箱仅连接到两台本地交换机，将数据中心 2 的机箱连接到本地交换机，但跨网络 EtherChannel 本质上是“分离的”。每个本地 VSS/vPC 都会将跨网络 EtherChannel 视作站点本地的 EtherChannel。

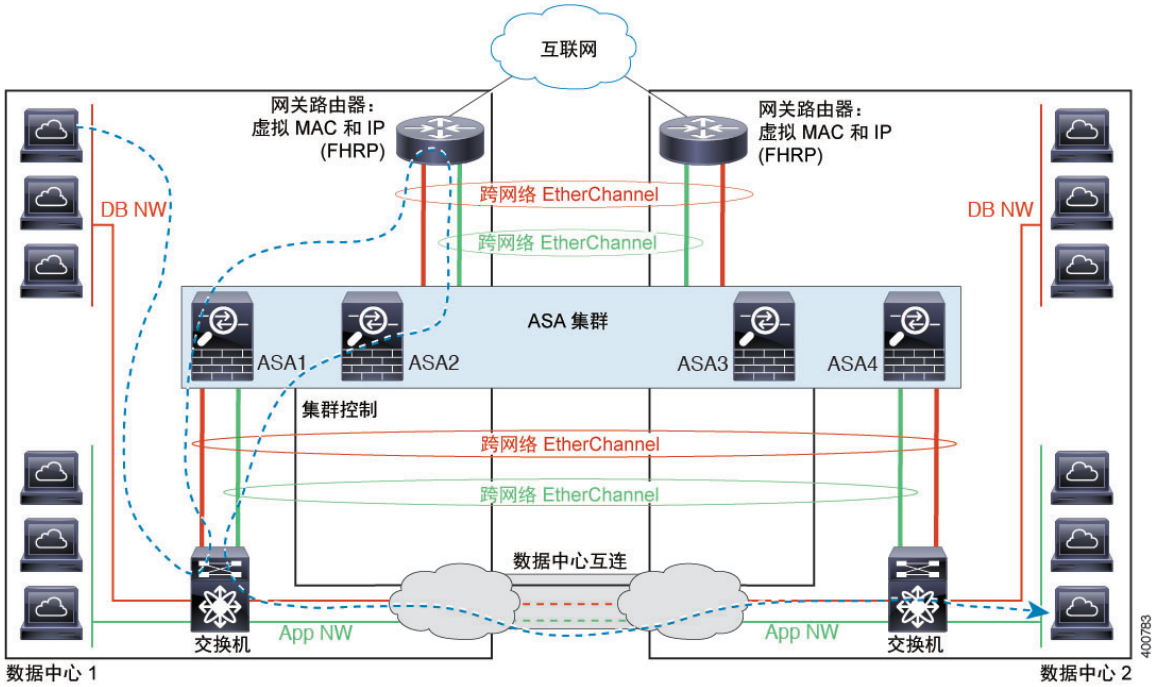


跨网络 EtherChannel 透明模式东西站点间集群示例

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网络EtherChannel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 **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集群示例，第 186 页。

集群历史记录

功能名称	平台版本	功能信息
对思科 ASA 进行机箱内集群	1.1.1	您可以对 Firepower 9300 机箱内的所有 ASA 安全模块创建集群。 我们引入了以下命令：**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**

功能名称	平台版本	功能信息
对 6 个 ASA 模块进行机箱间集群	1.1.3	现在，您可以对ASA启用机箱间集群。您最多可以在 6 个机箱中包含 6 个模块。
支持在 Firepower 9300 上的 Firepower 威胁防御 上执行机箱内集群	1.1.4	Firepower 9300 支持使用 Firepower 威胁防御 应用执行机箱内集群。 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 4100/9300 机箱上的 ASA 的站点间集群改进	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**
对 6 个 Firepower 威胁防御模块进行机箱间集群	2.1.1	现在，您可以对 Firepower 威胁防御启用机箱间集群。您最多可以在 6 个机箱中包含 6 个模块。

配置服务链

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。

关于服务链

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。

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。

服务链的先决条件

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 101 页。

服务链准则

模式

- 在以下安全设备上支持将 Radware DefensePro (vDP) 平台与 ASA 一同使用：
  - Firepower 9300
  - Firepower 4120 - 您必须使用 CLI 在此平台上部署 Radware DefensePro；Firepower 机箱管理器尚不支持此功能。
  - Firepower 4140 - 您必须使用 CLI 在此平台上部署 Radware DefensePro；Firepower 机箱管理器尚不支持此功能。
  - Firepower 4150
- 在以下安全设备上支持 Radware DefensePro 平台使用 Firepower 威胁防御：
  - Firepower 9300
  - Firepower 4110 - 请注意，还必须将修饰器与逻辑设备同时部署。在设备上配置了逻辑设备后，无法安装修饰器。
  - Firepower 4120 - 请注意，还必须将修饰器与逻辑设备同时部署。在设备上配置了逻辑设备后，无法安装修饰器。
  - Firepower 4140
  - Firepower 4150

其他规定

- 服务链在机箱间集群配置中不受支持。但是，在机箱间集群场景中，可采用独立配置部署Radware DefensePro (vDP) 应用。
- DefensePro 应用可以作为单独实例在最多三个安全模块上运行。

在独立逻辑设备上配置 Radware DefensePro 服务链

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 52 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 55 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 服务链，第 193 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编辑接口属性，第 145 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（请参阅创建独立的 ASA 逻辑设备，第 154 页或创建独立威胁防御逻辑设备，第 157 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# **scopessa**

步骤 4 创建 Radware vDP 实例：

Firepower /ssa # **scope slot** *slot_id*

Firepower /ssa/slot # **createapp-instance vdp**

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 vDP 应用处于在线状态后，访问逻辑设备：

Firepower /ssa # **scopelogical-device** *device_name*

步骤 8 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 # **enterexternal-port-link** *nameinterface_id***vdp**

Firepower /ssa/logical-device/external-port-link* # **exit**

步骤 9 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* #**createipv4** *slot_id***default**

c) 设置网关地址：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**setgateway** *gateway_address*

d) 设置 IP 地址和掩码：

Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* #**setip** *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 10 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* # **scopeexternal-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

步骤 11 向逻辑设备添加 vDP：

Firepower /ssa/logical-device/external-port-link* # **setdecorator vdp**

对要使用 vDP 的每个接口重复上述操作。

步骤 12 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
```

步骤 13 提交配置：

commit-buffer

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 服务链

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 52 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 55 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编辑接口属性，第 145 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（请参阅配置 ASA 集群，第 170 页）或 Firepower 威胁防御机箱内集群（请参阅配置 Firepower 威胁防御集群，第 177 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 **decoratorvdp**

set **description""**

exit

步骤 4 为逻辑设备分配外部管理接口：

enter **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：

enter **external-port-linkmgmt_vdp** *interface_name { asa | ftd }*

set **decorator""**

set **description""**

步骤 6 配置集群端口通道：

enter **external-port-link** port-channel48 Port-channel48 *{ asa | ftd }*

set **decorator""**

set **description""**

exit

步骤 7 为所有的三个 DefensePro 实例配置管理引导程序：

enter **mgmt-bootstrapvdp**

enter **ipv4** *slot_id***default**

setgateway *gateway_address*

setip *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 8 退出管理引导程序配置范围：

exit

步骤 9 进入主刀片上的 DefensePro 应用实例：

connectmodule *slot***console**

connectvdp

步骤 10 在主刀片上，设置管理 IP：

deviceclusteringmanagement-channelip

步骤 11 使用上一步中找到的 IP 设置主 IP：

deviceclusteringmasterset *management-channel ip*

步骤 12 启用集群：

deviceclusteringstatesetenable

步骤 13 退出应用控制台并返回到 FXOS 模块 CLI：

Ctrl]

步骤 14 重复步骤 10、12、13 和 14 以设置在步骤 11 中找到的主 IP，并为每个刀片应用实例启用集群。

步骤 15 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 16 验证所有 DefensePro 应用都已加入该集群：

deviceclustershow

步骤 17 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：

scopessa

scopeslot *slot_number*

scopeapp-instancevdp

showapp-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。

scopessa

scope *slot_number*

showapp-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，配置主 IP 地址，创建 vDP 集群。

如果 DefensePro 应用已联网并在集群中形成，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]

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，以及对现有逻辑设备执行其他任务。

连接到应用或修饰器的控制台

使用以下程序连接至应用或修饰程序的控制台。

注释 如果您在访问控制台时遇到任何问题，我们建议您尝试不同的SSH客户端，或者将SSH客户端升级到较新的版本。

过程

步骤 1 要连接至应用或修饰程序的控制台，请执行以下操作：

a) 从 FXOS CLI，连接至安全模块/引擎：

Firepower-chassis # **connectmodule** *slot_number***console**

注释 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*。

首次连接到安全模块时，您会进入 FXOS 模块 CLI。

b) 要连接到应用或修饰程序，请输入适用于您的设备的命令：

Firepower-module1>**connect asa**

Firepower-module1>**connect ftd**

Firepower-module1>**connect vdp**

从 FXOS CLI 的管理引擎层到安全模块/引擎的后续连接直接访问安全模块/引擎操作系统。

步骤 2 （可选） 键入 **Ctrl-A-D**，使应用控制台返回到 FXOS 模块 CLI。

键入 **Ctrl-]-**，使修饰程序控制台返回到 FXOS 模块 CLI。

出于故障排除目的，您可能想访问 FXOS 模块 CLI。

步骤 3 返回 FXOS CLI 的管理引擎层。

a) 要退出安全模块/引擎控制台，请输入 ~。

您将退出至 Telnet 应用。

b) 要退出 Telnet 应用，请输入：

telnet>**quit**

示例

以下示例连接至安全模块 1 上的 ASA，然后返回到 FXOS CLI 的管理引擎层。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

删除逻辑设备

过程

步骤 1 进入安全服务模式：

Firepower# **scopessa**

步骤 2 查看机箱上的逻辑设备的详细信息：

Firepower /ssa # **showlogical-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 # **deletelogical-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 # **showapp-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 # **scopeslot** *slot_number*
b) Firepower /ssa/slot # **deleteapp-instance** *application_name*
c) Firepower /ssa/slot # **exit**

步骤 6 提交配置：

commit-buffer

确认系统配置任务。

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# **scopessa**

步骤 2 查看已安装应用的详细信息：

Firepower /ssa # **showapp-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 # **scopeslot** *slot_number*
b) Firepower /ssa/slot # **deleteapp-instance** *application_name*
c) Firepower /ssa/slot # **exit**

步骤 4 提交配置：

commit-buffer

确认系统配置任务。

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 Firepower 威胁防御逻辑设备上分配或取消分配接口。然后，您可以在 Firepower 管理中心中同步接口配置。

开始之前

- 根据编辑接口属性，第 145 页和创建端口通道，第 147 页配置您的接口，并添加任何 EtherChannel。
- 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备或要求在 Firepower 管理中心上进行同步。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到 EtherChannel。对于新的 EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果要替换管理或 Firepower 事件接口，则必须使用 Firepower 机箱管理器；CLI 不支持此更改。
- 对于集群或高可用性，请确保在所有设备上添加或删除该接口，然后在 Firepower 管理中心中同步配置。我们建议您先在从属/备用设备上更改接口，然后再在主/活动设备上更改接口。请注意，新的接口在管理权限关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 进入安全服务模式：

Firepower# **scopessa**

步骤 2 编辑逻辑设备：

Firepower /ssa # **scopelogical-device** *device_name*

步骤 3 从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **deleteexternal-port-link** *name*

输入 **show external-port-link** 命令以查看接口名称。

步骤 4 将新的接口分配到逻辑设备：

Firepower /ssa/logical-device* # **createexternal-port-link** *name interface_id***ftd**

步骤 5 提交配置：

commit-buffer

确认系统配置任务。

步骤 6 登录至Firepower 管理中心。

步骤 7 依次选择**设备** > **设备管理** 并点击 Firepower 威胁防御 设备的编辑图标 ( )。系统会默认选择**接口**选项卡。

步骤 8 点击**接口 (Interfaces)** 选项卡左上方的**从设备同步接口 (Sync Interfaces from device)** 按钮。

步骤 9 点击**保存**。

此时，可以点击**部署** 并将策略部署到所分配的设备。在部署更改之后，更改才生效。

更改 ASA 逻辑设备上的接口

可以在 ASA 逻辑设备上分配、取消分配或替换管理接口。ASDM 会自动发现新接口。

开始之前

- 根据编辑接口属性， 第 145 页和创建端口通道， 第 147 页配置您的接口，并添加任何 EtherChannel。
- 您可以编辑已分配的 EtherChannel 的成员，而不影响逻辑设备。
- 如果您要将已分配的接口添加到 EtherChannel（例如，默认情况下将所有接口分配给集群），则需要先从逻辑设备取消分配接口，然后再将该接口添加到EtherChannel。对于新的EtherChannel，您可以随后将 EtherChannel 分配到设备。
- 如果在 FXOS 中移除一个分配的接口（例如，如果您移除网络模块，移除 EtherChannel，或将某个分配的接口重新分配到 EtherChannel），则 ASA 配置会保留原始命令，以便您可以进行任何必要的调整；从配置中移除接口会产生广泛的影响。您可以在 ASA OS 中手动移除旧的接口配置。

- 对于集群或故障转移，请确保添加或移除所有设备上的接口。我们建议您先在从属/备用设备上更改接口，然后再在主/活动设备上更改接口。新的接口在管理性关闭的状态下添加，因此，它们不会影响接口监控。

过程

步骤 1 进入安全服务模式：

Firepower# **scopessa**

步骤 2 编辑逻辑设备：

Firepower /ssa # **scopelogical-device** *device_name*

步骤 3 从逻辑设备取消分配接口：

Firepower /ssa/logical-device # **deleteexternal-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* # **createexternal-port-link** *name interface_id***asa**

步骤 5 提交配置：

commit-buffer

确认系统配置任务。

第 12 章

配置导入/导出

关于配置导入/导出

您可以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。之后，您便可以导入此配置文件，快速将配置设置应用于 Firepower 4100/9300 机箱，以返回到已知的正确配置，或从系统故障中恢复。

准则和限制

- 请勿修改配置文件的内容。如果配置文件被修改，使用该文件进行配置导入可能会失败。
- 特定应用的配置设置不包含在配置文件内。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）将被删除并完全替换为导入文件中包含的配置。
- 我们建议您只将配置文件导入当初从中导出配置的同一个 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，必须在 Firepower 4100/9300 机箱上接受该应用的 EULA，否则操作将失败。

- 要避免覆盖现有的备份文件，请务必更改备份操作中的文件名或将现有文件复制到其他位置。

导出 FXOS 配置文件

使用配置导出功能将包含 Firepower 4100/9300 机箱逻辑设备和平台配置设置的 XML 文件导出到远程服务器。

请查看关于配置导入/导出，了解有关使用配置导出功能的重要信息。

过程

步骤 1 要将配置文件导出到远程服务器：

scopesystem

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：

scopesystem

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：

scopesystem

show export-config

步骤 4 要修改某个现有导出任务，请执行以下操作：

scopesystem

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：

scopesystem

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：

scopeorg

scope cfg-export-policy default

b) 启用导出策略：

setadminstate 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。它可以是服务器、存储阵列、本地驱动器或 Firepower 4100/9300 机箱可通过网络访问的任何读/写媒体。

如果使用主机名而不使用 IP 地址，则必须配置 DNS 服务器。

sethostname *hostname*

e) 如果您使用的是非默认端口，请指定端口号：

setport *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：

setuser *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：

setpassword *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：

setremote-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)”。

setschedule {**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。

过程

要创建配置导出提醒，请执行以下操作：

scopeorg

scope cfg-export-reminder

set frequency *days*

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。请查看关于配置导入/导出，了解有关使用配置导入功能的重要信息。

过程

步骤 1 要从远程服务器导入配置文件，请执行以下操作：

scopesystem

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：

scopesystem

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：

scopesystem

show import-config

步骤 4 要修改现有导入任务，请执行以下操作：

scopesystem

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：

scopesystem

delete import-config *hostname*

commit-buffer

第 13 章

故障排除

数据包抓包

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 机箱上面向特定客户的端口或应用端口的流量。

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端口上的流量。对于包含在数据包捕获会话中的每个端口，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
Security Module 2	Ethernet1/11	内部数据 0/0
Security Module 2	Ethernet1/12	内部数据 0/1
Security Module 3	Ethernet1/13	内部数据 0/0
Security Module 3	Ethernet1/14	内部数据 0/1

规定和限制

数据包捕获工具存在以下限制：

- 捕获速度最多达到 100 Mbps。
- 即使没有足够的存储空间来运行数据包捕获会话，依然可以创建数据包捕获会话。在开始数据包捕获会话之前，您应验证您有足够的存储空间。
- 不支持多个活动数据包捕获会话。
- 仅在内部交换机的入口阶段进行捕获。
- 对于内部交换机无法理解的数据包（例如，安全组标记和网络服务报头数据包），过滤器不起作用。
- 不支持抽象（例如，端口通道和服务链）。

注释 尽管不支持在端口通道上捕获流量，但您可以包含在数据包捕获会话中组成端口通道的单个成员端口，数据包捕获工具将为每个成员端口创建单独的数据包捕获文件。

- 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 要创建新的数据包捕获会话：

Firepower-chassis /packet-capture # **create session** *session_name*

要编辑现有的数据包捕获会话：

Firepower-chassis /packet-capture # **enter session** *session_name*

步骤 3 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 4 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 5 指定此数据包捕获会话中应包含的端口。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面向客户的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) 要添加面向客户的端口：

Firepower-chassis /packet-capture/session* # **create** {**phy-port | phy-aggr-port**} *port_name*

对于 phy-port，*port_name* 语法为 **Ethernet**<*slot_id*>/<*port_id*> 或 **Port-Channel**<*number*>。对于分支电缆 (phy-aggr-port)， *port_name* 语法为 **Ethernet**<*slot_id*>/<*port_id*>/<*breakout_port_id*>。

b) 要添加应用端口：

Firepower-chassis /packet-capture/session* # **create app_port** *security_module_slot_id link_name interface_name app_name*

c) 根据需要重复上述步骤，添加所需的所有端口。

步骤 6 要过滤捕获的流量：

可以将过滤器应用于数据包捕获会话中包含的任何接口。有关创建过滤器的说明，请参阅配置数据包捕获的过滤器，第 216 页。

a) 输入要应用过滤器的接口范围。

Firepower-chassis /packet-capture/session* # **scope** {**phy-port | phy-aggr-port**} *port_name*

```
scope phy-port Ethernet<slot_id>/<port_id>
or
scope phy-aggr-port Ethernet<slot_id>/<port_id>/<breakout_port_id>
or
scope <security_module_slot_id> <link_name> <interface_name> <app_name>
```

b) 应用所需的过滤器：

Firepower-chassis /packet-capture/session/{phy-port|phy-aggr-port|app-port}* # **set** {**source-filter**} *filtername*

注释 要从端口删除过滤器，请使用 **set source-filter ""**。

c) 要应用其他过滤器，请根据需要重复以上步骤。

步骤 7 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 8 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* # 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 *9:* 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	目标 IP 地址 (IPv4)
srcipv6	源 IP 地址 (IPv6)
destipv6	目标 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	目标 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** 命令也可用于 `module` 模式。
- **traceroute** 和 **traceroute6** 命令可在 `local-mgmt` 模式下使用。
- **traceroute** 命令也可用于 `module` 模式。

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** 可退出 `local-mgmt` 模式并返回顶级模式。

确定端口通道状态

您可以按照以下步骤来确定当前定义的端口通道的状态。

过程

步骤 1 通过输入以下命令进入 `/eth-uplink/fabric` 模式：

- **scope eth-uplink**
- **scope fabric** {**a** | **b**}

示例：

```
FP9300-A# scope eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

步骤 2 输入 **show port-channel** 命令以显示当前的端口通道列表以及每个通道的管理状态和运行状态。

示例：

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
    Port Channel Id Name             Port Type          Admin
 State Oper State       State Reason
    --------------- ---------------- ------------------ -----
------ ---------------- ------------
    10              Port-channel10   Data               Enabl
ed     Failed           No operational members
    11              Port-channel11   Data               Enabl
ed     Failed           No operational members
    12              Port-channel12   Data               Disab
led    Admin Down       Administratively down
    48              Port-channel48   Cluster            Enabl
ed     Up

FP9300-A /eth-uplink/fabric #
```

步骤 3 通过输入以下命令进入 `/port-channel` 模式，以显示各个端口通道和端口信息：

- **scope port-channel** *ID*

示例：

```
FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

    <--- remaining lines removed for brevity --->

FP9300-A(fxos)#
```

步骤 4 输入 **show** 命令以显示指定端口通道的状态信息。

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)
```

在 `fxos` 模式下还可使用其他 **show port-channel** 和 **show lacp** 命令。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，请参阅创建端口通道 ， 第 147 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 kickstart 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 23:59:59:59.99 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 kickstart 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 kickstart 映像复制到可从 Firepower 4100/9300 机箱访问的 TFTP 目录。

注释 该 kickstart 映像的版本号将与捆绑包版本号不匹配。显示 FXOS 版本与 kickstart 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 kickstart。如果 USB 设备是在系统运行期间插入的，则您需要先重新引导系统，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 kickstart 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 kickstart 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 51 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 kickstart 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 23:59:59:59.99 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 kickstart 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 kickstart 映像复制到可从 Firepower 4100/9300 机箱访问的 TFTP 目录。

注释 该 kickstart 映像的版本号将与捆绑包版本号不匹配。显示 FXOS 版本与 kickstart 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 kickstart。如果 USB 设备是在系统运行期间插入的，则您需要先重新引导系统，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 kickstart 和系统映像引导：

```
rommon 1 > boot <kickstart-image> <system-image>
```

注释 在加载系统映像期间，您很可能会看到许可证管理器失败消息。可以安全忽略这些消息。

示例：

```
rommon 1 > dir
Directory of: bootflash:\

  01/01/12  12:33a <DIR>          4,096  .
  01/01/12  12:33a <DIR>          4,096  ..
  01/01/12  12:16a <DIR>         16,384  lost+found
  01/01/12  12:27a           34,333,696  fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  01/01/12  12:29a          330,646,465  fxos-k9-manager.4.1.1.69.SPA
  01/01/12  12:31a          250,643,172  fxos-k9-system.5.0.3.N2.4.11.69.SPA
  01/01/12  12:34a          330,646,465  nuova-sim-mgmt-nsg.0.1.0.001.bin
          4 File(s) 946,269,798 bytes
          3 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
  !!   Kickstart Image verified successfully   !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[    0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu
```

```
INIT: version 2.86 booting

POST INIT Starts at Sun Jan  1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA


Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

           ---- Basic System Configuration Dialog ----

  This setup utility will guide you through the basic configuration of
  the system. Only minimal configuration including IP connectivity to
  the Fabric interconnect and its clustering mode is performed through these steps.

  Type Ctrl-C at any time to abort configuration and reboot system.
  To back track or make modifications to already entered values,
  complete input till end of section and answer no when prompted
  to apply configuration.


  You have chosen to setup a new Security Appliance. Continue? (y/n):
```

步骤 7 加载映像后，系统将提示您进入初始配置设置。有关详细信息，请参阅初始配置，第 11 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。平台捆绑包映像版本应与您用于恢复系统的映像一致。有关详细信息，请参阅映像管理，第 51 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**，可确认您想要继续安装，或者输入 **no**，可取消安装。

Firepower 可扩展操作系统打开捆绑包，升级/重新加载组件。

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 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 11 监控系统状态。服务器状态应从“Discovery”转为“Config”，最后转为“Ok”。

示例：

```
FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Discovery             In Progress
1/2     Equipped                           Discovery             In Progress
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
```

```
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Config                Complete
1/2     Equipped                           Config                Complete
1/3     Empty

FP9300-A# show server status
Server  Slot Status                        Overall Status        Discovery
------- ---------------------------------- --------------------- ---------
1/1     Equipped                           Ok                    Complete
1/2     Equipped                           Ok                    Complete
1/3     Empty
```

当整体状态为“Ok”时，您的系统即已恢复。您仍必须重新配置安全设备（包括许可证配置），并重新创建所有逻辑设备。更多详情：

- Firepower 9300 快速入门指南 -http://www.cisco.com/go/firepower9300-quick
- Firepower 9300 配置指南 -http://www.cisco.com/go/firepower9300-config
- Firepower 4100 系列快速入门指南 -http://www.cisco.com/go/firepower4100-quick
- Firepower 4100 系列配置指南 -http://www.cisco.com/go/firepower4100-config

Firepower 威胁防御机箱间集群的灾难恢复

在灾难恢复场景之后，使用此程序和 Firepower 威胁防御，将 Firepower 4100/9300 机箱间集群恢复在线状态并加入一个集群。请注意，如果与集群设备关联的Firepower威胁防御应用版本不同步，您必须按照更新逻辑设备的映像版本，第 57 页中所述的步骤，使其同步为相同版本。

开始之前

使用配置导出功能将包含 Firepower 4100/9300 机箱的逻辑设备和平台配置设置的 XML 文件导出到远程服务器或本地计算机。有关详细信息，请参阅关于配置导入/导出，第 205 页。

过程

步骤 1 从属设备正常运行后，恢复备份。有关如何导入配置的说明，请参阅导入配置文件，第 210 页。应用安装开始。

步骤 2 接受许可协议。

步骤 3 如有必要，设置应用的启动版本，以便集群中各个设备上的版本匹配。有关如何设置应用启动版本的说明，请参阅更新逻辑设备的映像版本，第 57 页。此过程结束时，应用将恢复在线状态并加入集群。

步骤 4 确认应用的启动版本和运行版本相同。

a) 在 FXOS CLI 中，进入安全服务模式：

Firepower **scopessa**

b) 显示应用实例：

firepower /ssa # **showapp-instance**

示例：

```
firepower /ssa # show app-instance
App Name   Slot ID    Admin State Oper State      Running Version Startup Version Profile
 Name Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- ---------------
------------ --------------- ------------
ftd        1          Enabled     Online           6.2.3.1624      6.2.3.1624
         In Cluster      Slave
```

步骤 5 在Firepower管理中心，删除从属设备成员。有关如何删除从属设备成员的说明，请参阅《Firepower管理中心配置指南》中的“删除从属设备成员”主题。

步骤 6 将恢复的 9300/4100 从属设备注册为独立的 Firepower 设备。

步骤 7 在 Firepower 管理中心内，选择 **Devices > Add Cluster**，然后选择当前主设备。Firepower 管理中心将填充现有集群的名称，并将新的从属设备添加到现有集群。有关如何将集群添加到Firepower管理中心的说明，请参阅《Firepower 管理中心配置指南》中的“将集群添加到管理中心”主题。

索引

L

M

P

Q

R

S

T

W

X

Y

Z