Cisco FXOS CLI 配置指南 1.1(1)

首次发布日期: 2015 年 07 月 16 日

上次修改日期: 2015 年 10 月 12 日

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

文本部件号： 仅提供在线版本

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

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

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。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担保，包括（但不限于）适销性、特定用途适用性和无侵权担保，或者因买卖或使用以及商业惯例所引发的担保。

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：http://www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1110R)

目 录

第 1 章

Firepower 安全设备简介

关于 Firepower 安全设备

Cisco FXOS 机箱是下一代网络和内容安全解决方案平台。FXOS 机箱是思科以应用为中心的基础设施 (ACI) 安全解决方案的一部分，提供灵活、开放的安全平台，专为可扩展性、一致控制和简化管理而构建。

FXOS 机箱具有以下特性：

- 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。

第 2 章

命令行界面概述

受管对象

Firepower 可扩展操作系统使用受管对象模型，其中受管对象是可以管理的物理或逻辑实体的抽象表示。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 包含在命令模式的层次结构中，其中 EXEC 模式是该层次结构的最高级别模式。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至下一个较低级别模式，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	适用于 EXEC 模式的 **scope eth-server** 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	/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 #

模式名称	用于访问的命令	模式提示符
组织	适用于 EXEC 模式的 **scope org** 命令	/org #
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 #
服务配置文件	适用于 EXEC 模式的 **scope service-profile** 命令	/service-profile #
ssa	适用于 EXEC 模式的 **scope ssa** 命令	/ssa #
系统	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	/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，存在对应的 **delete***object* 和 **enter***object* 命令。

在用户实例化对象的管理中，这些命令的行为取决于对象是否存在，如下表中所述：

表 *2*：对象不存在时的命令行为

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

表 *3*：对象存在时的命令行为

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

完成命令

可以在任何模式下使用 Tab 键来完成命令。部分键入命令名称并按 Tab 键即可显示完整命令，或者显示达到必须选择其他关键字或必须输入参数值的程度。

命令历史记录

CLI 可存储当前会话中使用的所有命令。可以通过使用向上箭头键或向下箭头键逐条浏览先前使用的命令。向上箭头键浏览至历史记录中的上一个命令，向下箭头键浏览至历史记录中的下一个命令。如果到达历史记录的结尾，则按向下箭头键不起任何作用。

通过逐条浏览历史记录以重新调用所需命令并按Enter键，即可再次输入历史记录中的所有命令。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、放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 a **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 将多个命令一起提交不是基本操作。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？字符来显示在语法的当前状态下可用的选项。

如果尚未在提示符处键入任何内容，则键入？会列出您所处模式的所有可用命令。如果已部分键入某个命令，则键入？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

Firepower 可扩展操作系统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

入门

任务流

以下程序显示配置 FXOS 机箱时应当完成的基本任务。

过程

步骤 1 配置 FXOS 机箱硬件（请参阅Cisco 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 10 页）。
步骤 3 设置日期和时间（请参阅设置日期和时间， 第 41 页）。
步骤 4 配置 DNS 服务器（请参阅配置 DNS 服务器， 第 65 页）。
步骤 5 注册产品许可证（请参阅许可证管理， 第 15 页）。
步骤 6 配置用户（请参阅用户管理， 第 21 页）。
步骤 7 按需执行软件更新（请参阅映像管理， 第 33 页）。
步骤 8 配置其他平台设置（请参阅平台设置， 第 39 页）。
步骤 9 配置接口（请参阅接口管理， 第 67 页）。
步骤 10 创建逻辑设备（请参阅逻辑设备， 第 71 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 FXOS 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 FXOS 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 FXOS 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 Cisco 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 FXOS 机箱的电源。
在 FXOS 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 21 页）
- 管理员密码
- 系统名称
- 管理端口 IPv4 地址和子网掩码，或者 IPv6 地址和前缀
- 默认网关 IPv4 或 IPv6 地址

- 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。

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
  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
  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

您可以使用插入控制台端口的终端连接到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 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 连接，您需要知道 FXOS 机箱的主机名或 IP 地址。

使用下列语法示例之一，通过 SSH、Telnet 或 Putty 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，Telnet 处于禁用状态。有关启用 Telnet 的说明，请参阅配置 Telnet，第 45 页。

- **telnetucs-***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

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。

关于智能软件许可

本部分介绍智能软件许可的工作原理。

FXOS 机箱上的应用的智能软件许可

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

- FXOS 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。FXOS 机箱本身不需要任何许可证即可运行。
- 应用 - 在应用中配置所有许可证授权。

智能软件管理器和帐户

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这些许可证进行管理：

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，请点击链接设置新帐户。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。

按虚拟帐户管理的许可证和设备

仅当虚拟帐户的设备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 FXOS 机箱注册为设备，而机箱中的 应用会请求自己的许可证。例如，对于有 3 个安全模块的 Firepower 9300 机箱，机箱算作一台设备，但这些模块使用 3 个独立许可证。

设备注册和令牌

对于每个虚拟帐户，可以创建注册令牌。默认情况下，此令牌有效期为30天。当部署每台设备时，或者注册现有设备时，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。

注释 设备注册在 FXOS 机箱管理引擎中配置，而不是在 安全模块上配置。

在完成部署后或在现有设备上手动配置这些参数后启动时，设备会向思科许可证颁发机构进行注册。当设备向令牌注册时，许可证颁发机构会为设备与许可证颁发机构之间的通信颁发ID证书。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。

您可以选择配置 HTTP 代理。设备必须可以直接访问互联网，或者至少每 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，但是，如果您的设备具有宽限期，则会最多运行90天，而不会进行自动通报。您必须在 90 天截止前与许可证颁发机构联系。

注释 不支持离线许可。

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。

在 90 天重新授权尝试过后，设备将以某种方式受限，具体情况取决于应用。

Smart Call Home 基础设施

默认情况下，Smart Call Home 配置文件存在于配置中，指定许可授权机构的 URL。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 Cisco TAC 的指示，否则不应更改许可证颁发机构 URL。

无法针对智能软件许可禁用 Smart Call Home。

智能软件许可必备条件

- 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，请点击链接设置新帐户。通过智能软件管理器，您可以为组织创建一个主帐户。

- 从思科软件中心购买一个或多个许可证。
- 确保可从设备访问互联网或访问 HTTP 代理，以使设备能够联系许可颁发机构。不支持离线许可。
- 配置 DNS 服务器，以使设备能够解析许可颁发机构服务器的名称。请参阅配置 DNS 服务器，第 65 页。
- 设置设备时钟。请参阅设置日期和时间，第 41 页。

智能软件许可的默认设置

FXOS 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 FXOS 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 18 页。

步骤 2 向许可证颁发机构注册 Firepower 安全设备，第 19 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。

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*ip_address*

示例：

```
set http-proxy-server-url 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

向许可证颁发机构注册 Firepower 安全设备

当您注册 FXOS 机箱时，许可证颁发机构将签发一张 ID 证书用于 FXOS 机箱与许可证颁发机构之间的通信。它还会将 FXOS 机箱分配到相应的虚拟帐户。通常情况下，此程序是一次性实例。但是，如果 ID 证书由于通信问题等原因而过期，则稍后您可能需要重新注册 FXOS 机箱。

过程

步骤 1 在智能软件管理器中，为您希望将此 FXOS 机箱添加到的虚拟帐户请求并复制注册令牌。

步骤 2 在 FXOS 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：
注销

对 FXOS 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。您可能要注销以释放许可证用于新的 FXOS 机箱。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 licdebug renew

默认情况下，ID 证书每 6 个月自动续订一次，许可证授权每 30 天续订一次。如果您访问互联网的时间有限，或者在 Smart Software Manager 中进行了任何许可更改等操作，则您可能要为这些项目手动续订注册。

监控智能软件许可

请参阅以下命令，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 FXOS 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 FXOS 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。最多可以配置48个本地用户帐户。每个用户帐户必须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，不能修改或删除。此帐户是系统管理员或超级用户帐户，拥有完整权限。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。

管理员帐户始终为活动状态，不会过期。不能将管理员帐户配置为非活动状态。

本地身份验证用户帐户

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。如果您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）。

远程身份验证用户帐户

远程身份验证用户帐户是通过 LDAP、RADIUS 或 TACACS+ 进行身份验证的任意用户帐户。

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。

用户帐户过期

用户帐户可以配置为在预定义时间过期。到了过期时间，用户帐户将被禁用。

默认情况下，用户帐户不会过期。

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。

用户名准则

用户名也可用作 Firepower 机箱管理器和 FXOS CLI 的登录 ID。当您为用户帐户分配登录 ID 时，请考虑以下准则和限制：

- 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）

  .（圆点）

- 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。

密码准则

密码对于每个本地认证的用户帐户都是必需的。拥有管理员或AAA权限的用户可以将系统配置为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。

我们建议每个用户都使用强密码。如果对本地身份验证用户启用密码强度检查，Firepower可扩展操作系统将拒绝任何不符合以下要求的密码：

- 必须包含最少 8 个字符，最多 80 个字符。
- 必须包含至少以下三项：

  小写字母

  大写字母

  数字

  特殊字符

- 不得包含连续重复 3 次以上的字符，例如 aaabbb。
- 不得包含三个连续数字，例如 password123。
- 不得与用户名相同，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。
- 不得包含以下符号：$（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。

默认用户角色

系统包含下列默认用户角色：

管理员

对整个系统的完整读写访问权限。默认情况下，为默认管理员帐户分配此角色，不能更改。

只读

对系统配置的只读权限，无权修改系统状态。

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。您不能为每个本地身份验证用户指定不同的密码配置文件。

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。当配置此属性时，Firepower 机箱存储本地身份验证用户曾经使用的密码，最多存储 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。

如果需要，您可以清除本地身份验证用户的密码历史记录计数，启用重新使用以前的密码。

密码更改间隔

通过密码更改间隔，您可以限制本地身份验证用户在给定小时数内更改密码的次数。下表列出了密码更改间隔的两个配置选项。

间隔配置	说明	示例
不允许密码更改 (No password change allowed)	此选项不允许在密码更改之后的指定小时数内更改本地身份验证用户的密码。 您可以将无更改间隔指定为介于 1 和 745 小时之间。默认情况下，无更改间隔指定为 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： • 间隔内更改设置为禁用 • 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用户可以在预定义间隔内更改密码的最大次数。 您可以将更改间隔指定为介于 1 和 745 小时之间，密码更改最大次数介于 0 和 10 之间。默认情况下，允许本地身份验证用户在 48 小时间隔内最多执行 2 次密码更改。	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： • 间隔内更改设置为启用 • 更改计数设置为 1 • 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 60 和 172800 之间的整数。默认值为 600 秒。

如果超出此时间限制，Firepower 可扩展操作系统 则认为 Web 会话无效，但它不会终止会话。

步骤 6 （可选） 指定自上次刷新请求到 Firepower 可扩展操作系统 认为 Web 会话已结束之前的最长时间间隔：
Firepower-chassis /security/default-auth # **set session-timeout***seconds*

指定一个介于 60 和 172800 之间的整数。默认值为 7200 秒。

注释 如果为 RADIUS 或 TACACS+ 领域设置双因素身份验证，请考虑增加 **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 确认系统配置任务：
commit-buffer

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 7200 秒（2 小时），将会话超时期限设置为 28800 秒（8 小时），并且启用双因素身份验证。然后，确认任务。

```
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 7200
Firepower-chassis /security/default-auth* # set session-timeout 28800
Firepower-chassis /security/default-auth* # commit-buffer
Firepower-chassis /security/default-auth #
```

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。

这是默认行为。

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 确认系统配置任务：
Firepower-chassis /security # **commit-buffer**

以下示例为远程用户设置角色策略，确认任务：

```
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（请参阅密码准则，第 22 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**}

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 #
```

为更改间隔配置最大密码更改次数

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*

该值可以是介于 0 和 10 之间的任意值。

步骤 5 指定最大小时数，在该时间段内，密码更改次数为**更改计数 (Change Count)** 字段中所指定的值。
Firepower-chassis /security/password-profile # **set change-interval** *num-of-hours*

该值可以是介于 1 和 745 小时之间的任意值。

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 确认系统配置任务：
Firepower-chassis /security/password-profile # **commit-buffer**

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，并且确认任务：

```
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 #
```

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*

该值可以是介于 1 和 745 小时之间的任意值。

如果未将**间隔期间更改 (Change During Interval)** 属性设置为**禁用 (Disable)**，该时间间隔将被忽略。

步骤 5 确认系统配置任务：
Firepower-chassis /security/password-profile # **commit-buffer**

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，确认任务：

```
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*

该值可以是介于 0 和 15 之间的任意值。

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

步骤 4 确认系统配置任务：
Firepower-chassis /security/password-profile # **commit-buffer**

以下示例配置密码历史记录计数并且确认任务：

```
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*

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*

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） 指定用户电邮地址。
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 确认任务。
Firepower-chassis security/local-user # **commit-buffer**

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，并且确认任务：

```
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* # 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，并且确认任务。

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

```
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 确认系统配置任务：
Firepower-chassis /security #**commit-buffer**

以下示例删除 foo 用户帐户，并且确认任务：

```
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。

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 确认系统配置任务：
Firepower-chassis /security/local-user # **commit-buffer**

以下示例配置密码历史记录计数并且确认任务：

```
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

FXOS 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FXOS 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。版本 1.1.1 是适用于 ASA 的唯一可用应用映像。您可以将同一应用映像类型的多个不同版本存储在 Firepower 管理引擎上。

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

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/firepower9300-software。
FXOS 机箱的软件下载页面在浏览器中打开。

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 FXOS 机箱

您可以使用 FTP、SCP、SFTP 或 TFTP 将 FXOS 软件映像复制到 FXOS 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 # **scopefirmware**

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

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**

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)
```

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 34 页），然后将此映像下载到 FXOS 机箱（请参阅将逻辑设备软件映像下载到 FXOS 机箱，第 36 页）。

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI，第 12 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 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 6 要监控升级流程，请执行以下操作：

a) 输入 **scopefirmware**。
b) 输入 **scopeauto-install**。
c) 输入 **showfsmstatusexpand**。

将逻辑设备软件映像下载到 FXOS 机箱

您可以使用 FTP、SCP、SFTP 或 TFTP，将逻辑设备软件映像复制到 FXOS 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**

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

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 34 页），然后将映像下载到 FXOS 机箱（请参阅将逻辑设备软件映像下载到 FXOS 机箱，第 36 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 将入门版本设置为想要更新的版本：
Firepower-chassis /ssa/slot/app-instance # **setstartup-version***version_number*

步骤 5 确认配置：
commit-buffer

确认系统配置任务。应用映像已更新，应用重新启动。

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 #
```

第 7 章

平台设置

更改管理 IP 地址

开始之前

您可以从 FXOS CLI 更改 FXOS 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 12 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) 确认系统配置任务：
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) 确认系统配置任务：
Firepower-chassis /fabric-interconnect/ipv6-config* # **commit-buffer**

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 #
```

设置日期和时间

使用 下文描述的 CLI 命令手动设置日期和时间，或者配置 NTP 服务器。

注释 NTP 设置无法在 Firepower 机箱和任何安装在机箱上的应用之间同步。为确保正常运行，您必须在 Firepower 机箱中以及在机箱中运行的应用上配置相同的 NTP 设置。

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**

以下示例将时区配置为太平洋时区，确认任务，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#
```

添加 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 确认系统配置任务：
Firepower-chassis /system/services # **commit-buffer**

以下示例使用 IP 地址 192.168.200.101 配置 NTP 服务器并且确认任务：

```
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 服务器并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /system/services # **commit-buffer**

以下示例删除带有 IP 地址 192.168.200.101 的 NTP 服务器，并且确认任务：

```
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，并且确认任务：

```
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。无需确认缓冲区。

以下示例配置了系统时钟：

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

配置 SSH

以下程序介绍如何启用或禁用对 Firepower 机箱的 SSH 访问。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 确认系统配置任务：
Firepower /system/services # **commit-buffer**

以下示例启用对 Firepower 机箱的 SSH 访问，并且确认任务：

```
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，Telnet 处于禁用状态。

注释 目前，Telnet 配置只有在使用 CLI 时才可使用。

过程

步骤 1 进入系统模式：
Firepower-chassis #**scope system**

步骤 2 进入系统服务模式：

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

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

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

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

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

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

步骤 4 确认系统配置任务：
Firepower /system/services # **commit-buffer**

以下示例启用 Telnet 并且确认任务：

```
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 - 用于使用 SNMP 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，并按需向 SNMP 管理器报告数据。Firepower 机箱包括代理和一系列的 MIB。要启用 SNMP 代理并在管理器和代理之间创建关系，请在 Firepower 机箱管理器或 FXOS CLI 中启用和配置 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 的主要特性是能够从 SNMP 代理生成通知。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 机箱生成 SNMP 通知，作为陷阱或通告。陷阱不如通告可靠，因为 SNMP 管理器在接收陷阱时不会发送任何确认信息，而且 Firepower 机箱无法确定陷阱是否已收到。接收通告请求的 SNMP 管理器通过 SNMP 响应协议数据单元 (PDU) 确认消息。如果 Firepower 机箱没有收到 PDU，它可以再次发送通告请求。

SNMP 安全等级和权限

SNMPv1、SNMPv2c 和 SNMPv3 分别代表不同的安全模型。安全模型与选中的安全等级相结合，确定处理 SNMP 消息时应用的安全机制。

安全等级确定查看与 SNMP 陷阱关联的消息所需的权限。权限等级确定消息是否需要保护以防止泄露或进行身份验证。支持的安全等级取决于实施哪种安全模型。SNMP 安全等级支持下列一个或多个权限：

- 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承担的角色而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两者共同决定了处理 SNMP 数据包时使用的安全机制。

支持的 SNMP 安全模型和级别组合

下表列出了安全模型和级别组合的含义。

表 *4*: *SNMP* 安全模型和级别

模型	级别	身份验证	加密	发生的事件
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。除了基于密码块链 (CBC) DES (DES-56) 标准的身份验证，还提供数据加密标准 (DES) 56 位加密。

SNMPv3 安全功能

SNMPv3 通过将网络帧身份验证和加密结合在一起，提供对设备的安全访问。SNMPv3 仅授权已配置的用户执行管理操作，并加密 SNMP 消息。SNMPv3 基于用户的安全模型 (USM) 指的是 SNMP 消息级安全性，提供下列服务：

- 消息完整性 - 确保消息没有以未经授权的方式被更改或损坏，确保数据顺序的更改程度未超出非恶意性更改。
- 消息起源身份验证 - 确保已接收数据的起源用户的声明身份已得到确认。
- 消息保密性和加密 - 确保消息未被公布或披露给未经授权的个人、实体或进程。

SNMP 支持

Firepower 机箱为 SNMP 提供下列支持：

MIB 支持

Firepower 机箱支持对 MIB 的只读访问。

面向 SNMPv3 用户的身份验证协议

Firepower 机箱支持面向 SNMPv3 用户的 HMAC-SHA-96 (SHA) 身份验证协议。

面向 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 消息加密的一个隐私协议，并且符合 RFC 3826。

隐私密码或 priv 选项为 SNMP 安全加密提供 DES 或 128 位 AES 加密选项。如果您启用 AES-128 配置，并且包含 SNMPv3 用户的隐私密码，Firepower 机箱将使用此隐私密码生成 128 位 AES 密钥。AES 隐私密码至少有 8 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 确认系统配置任务：
Firepower-chassis /monitoring # **commit-buffer**

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，并且确认任务：

```
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 #
```

接下来的操作

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**

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 2 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 确认系统配置任务：
Firepower-chassis /monitoring # **commit-buffer**

以下示例删除位于 IP 地址 192.168.100.112 的 SNMP 陷阱，并且确认任务：

```
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**

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，并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /monitoring # **commit-buffer**

以下示例删除名为 snmp-user14 的 SNMPv3 用户，并且确认任务：

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

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 确认系统配置任务：
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。

以下示例将 HTTPS 端口号设置为 443 并且确认任务：

```
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 #
```

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、执行策略、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标识用户的方法，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 FXOS 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

授权是强制实施策略的过程：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。

记帐

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。身份验证用于标识用户。授权实现策略，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 机箱维护本地数据库，您可以在其中填入用户配置文件。您可以使用本地数据库代替 AAA 服务器来提供用户验证、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。此帐户应具有永不过期的密码。

过程

步骤 1 进入安全模式：
Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：
Firepower-chassis /security # **scope ldap**

步骤 3 仅限对包含指定属性的记录进行数据库搜索：
Firepower-chassis /security/ldap # **set attribute** *attribute*

步骤 4 仅限对包含指定区别名的记录进行数据库搜索：
Firepower-chassis /security/ldap # **set basedn** *distinguished-name*

步骤 5 仅限对包含指定过滤器的记录进行数据库搜索：
Firepower-chassis /security/ldap # **set filter** *filter*

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 确认系统配置任务：
Firepower-chassis /security/ldap # **commit-buffer**

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，并且确认任务：

```
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。

接下来的操作

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。此帐户应具有永不过期的密码。

过程

步骤 1 进入安全模式：
Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：
Firepower-chassis /security # **scope ldap**

步骤 3 创建 LDAP 服务器实例，进入安全 LDAP 服务器模式：
Firepower-chassis /security/ldap # **create server***server-name*

如果 SSL 已启用，*server-name*（通常为 IP 地址或 FQDN）必须精确匹配 LDAP 服务器安全认证中的通用名称 (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** - 要求加密。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 确认系统配置任务：
Firepower-chassis /security/ldap/server # **commit-buffer**

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，并且确认任务：

```
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，并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /security/ldap # **commit-buffer**

以下示例删除名为 ldap1 的 LDAP 服务器，并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /security/radius # **commit-buffer**

以下示例将 RADIUS 重试次数设置为 4，将超时间隔设置为 30 秒，并且确认任务：

```
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 #
```

接下来的操作

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**超时 (Timeout)** 值。

步骤 9 确认系统配置任务：
Firepower-chassis /security/radius/server # **commit-buffer**

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，将秘钥设置为 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，并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /security/radius # **commit-buffer**

以下示例删除名为 radius1 的 RADIUS 服务器，并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /security/tacacs # **commit-buffer**

以下示例将 TACACS+ 超时间隔设置为 45 秒，并且确认任务：

```
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 #
```

接下来的操作

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 确认系统配置任务：
Firepower-chassis /security/tacacs/server # **commit-buffer**

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，并且确认任务：

```
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 确认系统配置任务：
Firepower-chassis /security/tacacs # **commit-buffer**

以下示例删除名为 tacacs1 的 TACACS+ 服务器，并且确认任务：

```
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后台守护程序的服务器的方法。记录到中央系统日志服务器有助于汇聚日志和警报。系统日志服务接受消息并将其存储在文件中，或者根据简单配置文件将其打印。此形式的日志记录为日志提供受保护的长期存储。日志在例程故障排除和事件处理方面均有帮助。

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 确认任务：
Firepower-chassis /monitoring # **commit-buffer**

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确认任务：

```
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 确认系统配置任务：
Firepower /system/services # **commit-buffer**

以下示例配置具有 IPv4 地址 192.168.200.105 的 DNS 服务器并且确认任务：

```
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 服务器并且确认任务：

```
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 服务器并且确认任务：

```
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 8 章

接口管理

关于 Firepower 安全设备接口

FXOS 机箱支持单个接口以及 EtherChannel（端口通道）接口。EtherChannel 接口最多可包含 16 个相同类型的成员接口。

每个接口可以是以下类型之一：

- 数据 (Data)（默认设置）- 不能在逻辑设备之间共享数据接口。
- 管理 (Management) - 可以在逻辑设备之间共享管理接口。您只能为每个逻辑设备分配一个管理接口。
- 集群 (Cluster) - 用于集群逻辑设备的特殊接口类型。此类型自动分配给集群控制链路，用于实现设备间集群通信。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。

编辑接口属性

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 命令，将会收到一条错误消息，说明对象不存在。应先使用 enter interface 命令编辑接口，然后在将接口添加到端口通道。

步骤 3　（可选）设置接口类型：
setport-type {**data** | **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。

步骤 4　（可选）设置接口速度：
setspeed {**10gbps** | **1gbps**}

示例：

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

步骤 5　确认配置：
commit-buffer

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。

开始之前

FXOS 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 确认配置：
commit-buffer

配置分支线缆

以下程序介绍如何配置分支线缆以供FXOS机箱使用。您可以使用分支线缆提供4个10 Gbps端口，代替单个 40 Gbps 端口。

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_slotport*

示例：

```
Firepower /cabling/fabric/ # create breakout 2 1
```

c) 确认配置：
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_slotport*

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) 确认配置：
commit-buffer

第 9 章

逻辑设备

关于逻辑设备

当您创建逻辑设备时，FXOS 机箱管理引擎会部署逻辑设备，方法是下载指定软件版本，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，或者，如果是机箱内集群，则推送到安装在 Firepower 机箱内的所有安全模块。

您可以创建以下两类逻辑设备之一：

注释 在支持多个安全模块的FXOS机箱上，只能以独立或集群方式创建一类逻辑设备。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，使用剩余的两个逻辑设备创建集群。

- 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。集群具有单台设备的全部便捷性（管理、集成到一个网络中），同时还能提高吞吐量并实现多台设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。

创建独立的 ASA 逻辑设备

您可以为 FXOS 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。

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）。
- 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 34 页），然后将映像下载到 FXOS 机箱（请参阅将逻辑设备软件映像下载到 FXOS 机箱， 第 36 页）。
- 配置逻辑设备要使用的管理接口。

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

步骤 5 配置管理引导程序信息：

a) 创建引导程序对象：
Firepower /ssa/logical-device* # **createmgmt-bootstrapasa**

b) 创建启用密码：
Firepower /ssa/logical-device/mgmt-bootstrap* # **createbootstrap-key-secretPASSWORD**

c) 设置密码值：
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **setvalue**
值：*password*

d) 退出密码配置范围：
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # **exit**

e) 配置管理 IP 地址：
Firepower /ssa/logical-device/mgmt-bootstrap* # **createipv4***slot_id***default**

f) 设置网关地址：
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setgateway***gateway_address*

g) 设置 IP 地址和掩码：
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **setip***ip_address***mask***network_mask*

h) 退出管理 IP 配置范围：
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # **exit**

i) 退出管理引导程序配置范围：

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

步骤 6 确认配置：
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
```

部署集群

通过集群，您可以将多个安全模块组合成一个逻辑设备。集群具有单台设备的全部便捷性（管理、集成到一个网络中），同时还能提高吞吐量并实现多台设备的冗余性。Firepower 9300 等多模块设备支持机箱内集群。

注释 Firepower 9300 不支持跨多个机箱（机箱间）的集群；仅支持机箱内集群。

关于 FXOS 机箱上的集群

集群由多台设备组成，这些设备作为一个整体运行。当您在FXOS 机箱 上部署集群时，它执行以下操作：

- 为设备到设备通信创建集群控制链路（端口通道 48）。对于机箱内集群，此链路利用 Firepower 9300背板进行集群通信。
- 在应用内创建集群引导程序配置。

  部署集群时，FXOS 机箱 管理引擎向包含此集群名称、集群控制链路接口和其他集群设置的每台设备推送最低引导程序配置。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。

  注释 不支持单个接口，但管理接口除外。
- 向集群中的所有设备分配管理接口。

以下部分将更加详细地介绍集群概念和实施。

主设备和从设备角色

集群的一个成员是主设备。自动确定主设备。所有其他成员均为从设备。

您必须仅在主设备上执行所有配置；随后，配置将被复制到从设备。

集群控制链路

使用端口通道48接口自动创建集群控制链路。对于机箱内集群，此接口没有成员接口。此集群类型EtherChannel 利用 Firepower 9300 背板进行集群通信，实现机箱内集群。

集群控制链路流量包括控制流量和数据流量。

管理界面

您可以将管理类型接口分配给集群。与跨网络接口相比，此接口是一个特殊的独立接口。通过管理接口，可以直接连接每台设备。

对于ASA，主集群IP地址是集群的固定地址，始终属于当前的主设备。还要配置一个地址范围，以便包括当前主设备在内的每台设备都可以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，在故障排除时也非常有用。例如，您可以通过连接到主集群 IP 地址来管理集群，该地址始终属于当前的主设备。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台设备都使用本地 IP 地址连接到服务器。

集群准则

- 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 FXOS 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。

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 68 页或编辑接口属性，第 67 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。

步骤 2 添加“管理 (Management)”类型接口或 EtherChannel。请参阅创建端口通道，第 68 页或编辑接口属性，第 67 页。

步骤 3 端口通道 48 预留为集群控制链路。

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 "1,2,3" clustered**

示例：

```
Firepower /ssa # enter logical-device ASA1 asa "1,2,3" clustered
Firepower /ssa/logical-device* #
```

device_name 由 FXOS 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。

步骤 6 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 7 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* #
```

名称必须是长度介于 1 和 38 个字符之间的 ASCII 字符串。

步骤 8 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 9 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。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 10 设置机箱 ID：
set chassis-id*id*

示例：

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

步骤 11 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
Firepower /ssa/logical-device/cluster-bootstrap* #
```

系统将提示您输入共享密钥。

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

步骤 12 退出集群引导程序模式和逻辑设备模式：
exit

exit

步骤 13 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 14 确认配置：
commit-buffer

FXOS 机箱管理引擎通过下载默认安全模块软件版本以及向每个安全模块推送集群引导程序配置和管理接口设置来部署集群。

步骤 15 连接到主设备安全模块以自定义集群配置。

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

    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
```

集群历史记录

功能名称	平台版本	功能信息
对 Cisco 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**

连接到应用或修饰程序的控制台

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：
Firepower-module1>**connect asa**

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。
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，请键入 ~。
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#
```

索 引

字母

B

C

D

F

G

J

L

M

P

Q

R

S

T

X

Y

Z