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 FTD，则必须在 Firepower 4100/9300 机箱上配置 NTP，使智能许可正常工作并确保设备注册的时间戳正确。您应对 Firepower 4100/9300 机箱 和 FMC 使用相同的 NTP 服务器，但请注意，您不能使用 FMC 作为 Firepower 4100/9300 机箱 的 NTP 服务器。

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

查看配置的日期和时间

过程

步骤 1 连接到 FXOS CLI（请参阅访问 FXOS CLI）。

步骤 2 要查看已配置的时区，请执行以下操作：

Firepower-chassis# **show timezone**

步骤 3 查看配置的日期和时间：

Firepower-chassis# **show clock**

示例

以下示例显示如何显示配置的时区和当前系统日期及时间：

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

设置时区

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 设置时区：

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

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

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

步骤 4 要查看已配置的时区，请执行以下操作：

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

Firepower-chassis# **show timezone**

示例

以下示例将时区配置为太平洋时区，提交任务，并且显示已配置的时区：

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

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

The following information has been given:

        United States
        Pacific Time

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

使用 NTP 设置日期和时间

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

注释

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

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

开始之前

如果您要将主机名用于 NTP 服务器，则必须配置 DNS 服务器。请参阅 配置 DNS 服务器，第 54 页。

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 使用指定的主机名、IPv4 或 IPv6 地址配置系统，使其使用 NTP 服务器：

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

步骤 4 （可选） 配置 NTP 身份验证。

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

a) 设置 SHA1 密钥 ID。

set ntp-sha1-key-id *key_id*

b) 设置 SHA1 密钥字符串。

set ntp-sha1-key-string

系统会提示您输入密钥字符串。

c) 退出 ntp-server 模式。

exit

d) 启用 NTP 认证。

enable ntp-authentication

示例：

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

步骤 5 将任务提交到系统配置：

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

步骤 6 查看所有已配置的 NTP 服务器的同步状态：

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

步骤 7 查看特定 NTP 服务器的同步状态：

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

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

示例

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

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

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

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

删除 NTP 服务器

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 删除带有指定主机名、IPv4 或 IPv6 地址的 NTP 服务器：

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

步骤 4 将任务提交到系统配置：

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

示例

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

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

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

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

手动设置日期和时间

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

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

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 配置系统时钟：

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

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

系统时钟修改立即生效。无需确认缓冲区。

示例

以下示例配置了系统时钟：

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

配置 SSH

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

默认情况下，SSH 处于启用状态。

过程

步骤 1 进入系统模式：

Firepower-chassis # **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 要配置对机箱的 SSH 访问，请执行以下操作之一：

- 要允许对机箱进行 SSH 访问，请输入以下命令：

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

- 要禁止对机箱进行 SSH 访问，请输入以下命令：

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

步骤 4 配置服务器的加密算法：

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

示例：

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

示例：

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

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

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

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

示例：

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

DH密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

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

步骤 6 设置服务器 mac 算法：

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

示例：

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

步骤 7 对于服务器主机密钥，请输入 RSA 密钥对的模块大小。

模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

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

示例：

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

步骤 8 对于服务器密钥更新数量限制，请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。

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

示例：

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

步骤 9 对于服务器密钥更新时间限制，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

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

示例：

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

步骤 10 将任务提交到系统配置：

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

步骤 11 配置严格的主机密钥检查，以控制 SSH 主机密钥检查：

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

示例：

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

- **启用** - 如果 FXOS 已知的主机文件中未包含主机密钥，连接将被拒绝。您必须在 FXOS CLI 中使用系统/服务范围的 **enter ssh-host** 命令手动添加主机。
- **提示** - 对于机箱中未存储的主机密钥，系统会提示您接受或拒绝该主机密钥。
- **禁用** -（默认）机箱将自动接受以前未存储的主机密钥。

步骤 12 配置客户端的加密算法：

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

示例：

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

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

注释
- 通用标准中不支持 3des-cbc。如果在 FXOS 机箱上启用了通用标准模式，则不能使用 3des-cbc 作为加密算法。
- 以下加密算法默认不会启用：

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

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

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

示例：

```
Firepower /system/services # set ssh-client kex-algorithm
  curve25519-sha256               curve25519-sha256
  curve25519-sha256_libssh_org    curve25519-sha256@libssh.org
  diffie-hellman-group14-sha1     diffie-hellman-group14-sha1
  diffie-hellman-group14-sha256   diffie-hellman-group14-sha256
  ecdh-sha2-nistp256              ecdh-sha2-nistp256
  ecdh-sha2-nistp384              ecdh-sha2-nistp384
  ecdh-sha2-nistp521              ecdh-sha2-nistp521
```

DH密钥交换提供无法由任何一方单独确定的共享密钥。密钥交换与签名和主机密钥配合使用，以提供主机身份验证。此密钥交换方法提供显式服务器身份验证。有关使用 DH 密钥交换方法的详细信息，请参阅 RFC 4253。

步骤 14 设置客户端 mac 算法：

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

示例：

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

步骤 15 对于客户端主机密钥，请输入 RSA 密钥对的模块大小。

模数值（以位为单位）应为 8 的倍数，且介于 1024 到 2048 之间。指定的密钥模块大小越大，生成 RSA 密钥对所需的时间就越长。建议值为 2048。

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

示例：

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

步骤 16 对于客户端密钥更新数量限制，请设置 FXOS 断开会话连接之前连接上允许的流量（以 KB 为单位）。

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

示例：

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

步骤 17 对于客户端密钥更新时间限制，请设置 FXOS 断开会话连接之前允许的 SSH 会话空闲时间（以分钟为单位）。

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

示例：

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

步骤 18 将任务提交到系统配置：

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

示例

以下示例启用对机箱的 SSH 访问，并且提交任务：

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

配置 TLS

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

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

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

注释

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

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 查看您的系统中可用的 TLS 版本选项：

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

示例：

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

步骤 3 设置最低 TLS 版本：

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

示例：

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

步骤 4 提交配置：

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

步骤 5 显示在您的系统上配置的最低 TLS 版本：

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

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

示例：

```
Firepower-chassis /system/services # show
Name: ssh
    Admin State: Enabled
    Port: 22
Kex Algo: Diffie Hellman Group1 Sha1,Diffie Hellman Group14 Sha1
Mac Algo: Hmac Sha1,Hmac Sha1 96,Hmac Sha2 512,Hmac Sha2 256
Encrypt Algo: 3des Cbc,Aes256 Cbc,Aes128 Cbc,Aes192 Cbc,Aes256 Ctr,Aes128 Ctr,Ae
s192 Ctr
Auth Algo: Rsa
    Host Key Size: 2048
Volume: None Time: None
Name: telnet
    Admin State: Disabled
    Port: 23
Name: https
    Admin State: Enabled
    Port: 443
    Operational port: 443
    Key Ring: default
    Cipher suite mode: Medium Strength
    Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIU
M:+EXP:+eNULL
    Https authentication type: Cert Auth
    Crl mode: Relaxed
```

```
TLS:
    TLS version: v1.2
```

配置 Telnet

以下程序介绍如何启用或禁用对机箱的 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 要配置对机箱的 Telnet 访问，请执行以下操作之一：

- 要允许对机箱进行 Telnet 访问，请输入以下命令：

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

- 要禁止对机箱进行 Telnet 访问，请输入以下命令：

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

步骤 4 将任务提交到系统配置：

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

示例

以下示例启用 Telnet 并且提交任务：

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

配置 SNMP

本节介绍如何在机箱上配置简单网络管理协议 (SNMP)。有关详细信息，请参阅以下主题：

关于 SNMP

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

SNMP 框架由三个部分组成：

- SNMP 管理器 - 用于通过 SNMP 来控制和监控网络设备的活动的系统。
- SNMP 代理 - 机箱内的软件组件，用于维护机箱的数据并根据需要向 SNMP 管理器报告数据。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。

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

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

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

SNMP 通知

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

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。如果机箱不接收 PDU，则其可以再次发送通知请求。

但是，通知仅可配合 SNMPv2c 使用，这被认为不安全，因此不建议使用。

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

SNMP 安全级别和权限

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

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

- noAuthNoPriv - 无身份验证或加密
- authNoPriv - 身份验证，但无加密
- authPriv - 身份验证和加密

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

支持的 SNMP 安全模型和级别组合

下表确定安全模型和级别的组合含义。

表 *1: SNMP* 安全模型和级别

型号	级别	身份验证	加密	状况
v1	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。
v2c	noAuthNoPriv	社区字符串	否	使用社区字符串匹配进行身份验证。

型号	级别	身份验证	加密	状况
V3	noAuthNoPriv	用户名	否	使用用户名匹配进行身份验证。 注释 虽然可以配置，但 FXOS 不支持将 `noAuthNoPriv` 与 SNMP 第 3 版配合使用。
V3	authNoPriv	HMAC-SHA	否	提供基于 HMAC 安全散列算法 (SHA) 的身份验证。
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

机箱为 SNMP 提供下列支持：

针对 MIB 的支持

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

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

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，则机箱使用该隐私密码来生成 128 位 AES 密钥。AES 隐私密码至少可具有八个字符。如果口令用明文指定，您可以指定最多 64 个字符。

启用 SNMP 并配置 SNMP 属性

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

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

步骤 3 （可选）进入 SNMP 社区模式：

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

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

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

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

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

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

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

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

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

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

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

步骤 7 将任务提交到系统配置：

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

示例

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

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

下一步做什么

创建 SNMP 陷阱和用户。

创建 SNMP 陷阱

以下步骤介绍如何创建 SNMP 陷阱。

注释 最多可以定义八个 SNMP 陷阱。

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

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

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

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

步骤 4 指定用于 SNMP 陷阱的 SNMP 社区名或版本 3 用户名：

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

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

步骤 5 指定用于 SNMP 陷阱的端口：

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

步骤 6 指定用于陷阱的 SNMP 版本和型号：

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

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

步骤 7 （可选） 指定要发送的陷阱类型。

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

该字段可以是：

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

  注释　仅在您为版本选择 v2c 时，才可以发送通告通知。

步骤 8 （可选） 如果为版本选择 v3，请指定与陷阱相关的权限：

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

该字段可以是：

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

步骤 9 确认系统配置任务：

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

示例

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

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

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

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

删除 SNMP 陷阱

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 删除带有指定主机名或 IP 地址的 SNMP 陷阱：

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

步骤 3 将任务提交到系统配置：

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

示例

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

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

创建 SNMPv3 用户

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用 SNMP：

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

步骤 3 创建 SNMPv3 用户：

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

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

FXOS 拒绝任何不满足以下要求的密码：

- 必须包含最少 8 个字符，最多 80 个字符。
- 必须仅包含字母、数字和以下字符：

  ~`!@#%^&*()_-+{}[]|\:;"'<,>./

- 不得包含以下符号：$（美元符号）、?（问号）或 =（等号）。
- 必须包含至少 5 个不同的字符。
- 不得包含过多连续递增或递减数字或字母。例如，字符串“12345”包含四个此类字符，字符串“ZYXW”包含三个此类字符。如果此类字符的总数超过某个限值（通常约大于 4 至 6 个字符），则简单性检查将会失败。

  注释 在使用的非递增或递减字符数介于两者之间时，系统不会重置连续递增或递减字符计数。例如，abcd&!21 将致使密码检查失败，但 abcd&!25 不会。

步骤 4 指定 SHA 身份验证的使用情况：

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

步骤 5 启用或禁用 AES-128 加密的使用：

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

默认情况下会禁用 AES-128 加密。

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

注释 当启用带 Authpriv 的 SNMPv3（DES）时，您无法从某些 NMS 监控应用轮询 SNMPv3 FXOS 设备。如果从以前支持使用 DES 的版本升级设备，则必须使用 AES 重新创建用户以轮询 SNMPv3 FXOS 设备。

步骤 6 指定用户密码：

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

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

步骤 7 将任务提交到系统配置：

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

示例

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

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

删除 SNMPv3 用户

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 删除指定的 SNMPv3 用户：

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

步骤 3 将任务提交到系统配置：

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

示例

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

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

查看当前的 SNMP 设置

使用以下 CLI 命令显示当前的 SNMP 设置、用户和陷阱。

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

过程

步骤 1 进入监控模式：

firepower# **scope monitoring**

步骤 2 显示当前 SNMP 设置：

firepower/monitoring # **show snmp**

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

步骤 3 列出当前定义的 SNMPv3 用户：

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

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

步骤 4 列出当前定义的 SNMP 陷阱：

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

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

示例

此示例演示如何显示特定 SNMPv3 用户的相关详细信息：

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

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

配置 HTTPS

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

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

证书、密钥环和受信任点

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

加密密钥和密钥环

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

如果群集名称更改或证书过期，则必须手动重新生成默认密钥环证书。

证书

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

受信任点

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

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

创建密钥环

FXOS 最多支持 8 个密钥环，包括默认密钥环。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 创建并命名密钥环：

Firepower-chassis # **create keyring** *keyring-name*

步骤 3 设置 SSL 密钥长度（以位为单位）：

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

步骤 4 提交任务：

Firepower-chassis # **commit-buffer**

示例

以下示例创建密钥大小为 1024 位的密钥环：

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

下一步做什么

创建该密钥环证书请求。为该密钥环创建证书请求。

重新生成默认密钥环

如果群集名称更改或证书过期，则必须手动重新生成默认密钥环证书。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入默认密钥环的密钥环安全模式：

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

步骤 3 重新生成默认密钥环：

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

步骤 4 提交任务：

Firepower-chassis # **commit-buffer**

示例

以下示例重新生成默认密钥环：

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

创建密钥环的证书请求

使用基本选项创建密钥环证书请求使用基本选项创建密钥环的证书请求

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密钥环配置模式：

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

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

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

步骤 4 提交任务：

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

步骤 5 显示您可以复制并发送至信任锚或证书颁发机构的证书请求：

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

示例

以下示例使用基本选项为密钥环创建并显示具有 IPv4 地址的证书请求：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #
```

下一步做什么

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

使用高级选项创建密钥环的证书请求

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入密钥环配置模式：

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

步骤 3 创建证书请求：

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

步骤 4 指定公司所在国家/地区的国家/地区代码：

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

步骤 5 指定与请求相关联的域名服务器 (DNS) 地址：

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

步骤 6 指定与证书请求相关联的邮件地址：

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

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

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

步骤 8 指定请求此证书的公司总部所在的城市或城镇：

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

步骤 9 指定请求证书的组织：

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

步骤 10 指定组织单位：

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

步骤 11 为证书请求指定可选密码：

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

步骤 12 指定请求此证书的公司总部所在的省、市或自治区：

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

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

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

步骤 14 提交任务：

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

步骤 15 显示您可以复制并发送至信任锚或证书颁发机构的证书请求：

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

示例

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

以下示例使用高级选项为密钥环创建并显示具有 IPv4 地址的证书请求：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set "ip 192.168.200.123"
Firepower-chassis /security/keyring/certreq* #  set subject-name "sjc04"
Firepower-chassis /security/keyring/certreq* # set country "US"
Firepower-chassis /security/keyring/certreq* # set dns "bg1-samc-15A"
Firepower-chassis /security/keyring/certreq* # set email "test@cisco.com"
Firepower-chassis /security/keyring/certreq* # set locality "new york city"
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name "Testing"
Firepower-chassis /security/keyring/certreq* # set state "new york"
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKn1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF8OPhKbhghLA1YZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtX1WsylwUWV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNIcECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHUO03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWIcTWgHhH8BimOb/0OKuG8kwfIGGsEDlAv
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGxlDNqoN+odCXPc5kjoXD0lZTL09H
BA==
-----END CERTIFICATE REQUEST-----

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

下一步做什么

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

创建受信任点

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 创建受信任点：

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

步骤 3 为此受信任点指定证书信息：

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

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

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

步骤 4 提交任务：

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

示例

以下示例创建受信任点并提供为受信任点提供证书：

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMDCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl9O3O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3nO4MIGeBgNVHSMEgZYwgZOAFLlNjtcEMyZ+f7+3yh42
> 1ido3nO4oXikdjB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExFDASBgNVBAcT
> C1NhbnRhIENsYXJhMRswGQYDVQQKExJOdW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQ8wDQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQqXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8copP1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIZJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
```

```
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

下一步做什么

从信任锚或证书颁发机构获取密钥环证书并将其导入密钥环。

将证书导入密钥环

开始之前

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

注释 如果更改已在 HTTPS 上配置的密钥环中的证书，您必须重新启动 HTTPS 才能使新证书生效。有关详细信息，请参阅：重新启动 HTTPS，第 35 页。

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 进入将接收证书的密钥环的配置模式：

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

步骤 3 为从其中获取密钥环证书的信任锚或证书颁发机构指定受信任点：

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

步骤 4 启动用于输入和上传密钥环证书的对话框：

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

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

重要事项 证书必须采用 Base64 编码 X.509 (CER) 格式。

步骤 5 提交任务：

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

示例

以下示例指定信任点并将证书导入密钥环：

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
> BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

下一步做什么

使用密钥环配置 HTTPS 服务。

配置 HTTPS

⚠

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

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 启用 HTTPS 服务：

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

步骤 4 （可选） 指定要用于 HTTPS 连接的端口：

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

步骤 5 （可选） 指定创建用于 HTTPS 的密钥环名称：

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

步骤 6 （可选） 指定域使用的 Cipher Suite 安全级别：

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

cipher-suite-mode 可以是以下关键字之一：

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

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

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

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

例如，默认情况下，FXOS 使用的中强度规范字符串为：
ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

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

步骤 8 （可选） 启用或禁用证书吊销列表检查：

set revoke-policy *{ relaxed | strict }*

步骤 9 将任务提交到系统配置：

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

示例

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

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

更改 HTTPS 端口

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

过程

步骤 1 进入系统模式：

Firepower-chassis # **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 指定用于 HTTPS 连接的端口：

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

为 *port-number* 指定一个介于 1 和 65535 之间的整数。默认情况下，在端口 443 上启用 HTTPS。

步骤 4 将任务提交到系统配置：

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

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

https://*<chassis_mgmt_ip_address>*:*<chassis_mgmt_port>*

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

示例

以下示例将 HTTPS 端口号设置为 443 并且提交任务：

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

重新启动 HTTPS

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

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 将 HTTPS 密钥环恢复为其默认值：

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

步骤 4 将任务提交到系统配置：

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

步骤 5 等待五秒钟。

步骤 6 使用您创建的密钥环来设置 HTTPS：

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

步骤 7 将任务提交到系统配置：

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

删除密钥环

过程

步骤 1 进入安全模式：

Firepower-chassis # **scope security**

步骤 2 删除指定密钥环：

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

步骤 3 提交任务：

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

示例

以下示例删除密钥环：

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

删除受信任点

开始之前

确保密钥环未使用受信任点。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 删除指定受信任点：

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

步骤 3 提交任务：

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

示例

以下示例删除受信任点：

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

禁用 HTTPS

过程

步骤 1 进入系统模式：

Firepower-chassis# **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 禁用 HTTPS 服务：

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

步骤 4 将任务提交到系统配置：

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

示例

以下示例禁用 HTTPS 并提交任务：

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

配置 AAA

本部分介绍身份验证、授权和记账。有关详细信息，请参阅以下主题：

关于 AAA

验证、授权和记帐 (AAA) 是一组服务，用于控制对网络资源的访问、实施策略、评估使用情况并提供对服务进行计费所需的信息。身份验证用于识别用户。授权用于实施策略，这些策略确定经过身份验证的用户能够访问哪些资源和服务。记账对时间和数据资源进行追踪，这些资源用于计费和分析。这些过程对于高效进行网络管理和安全性而言至关重要。

身份验证

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

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

- HTTPS
- SSH
- 串行控制台

授权

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

会计

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

身份验证、授权和记账之间的交互

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

支持的身份验证类型

FXOS 支持以下类型的用户身份验证：

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

用户角色

FXOS 支持以用户角色分配的形式进行本地和远程授权。可以分配的角色包括：

- **管理员** - 完成对整个系统的读写访问。默认情况，下会向默认管理员账户分配此角色，并且不能对其进行更改。
- **AAA 管理员** - 对用户、角色和 AAA 配置进行读写访问。对系统其余部分的读取访问。
- **操作** - 对 NTP 配置、用于智能许可的 Smart Call Home 配置和系统日志（包括系统日志服务器和故障）进行读写访问。对系统其余部分的读取访问。
- **只读** - 对系统配置进行只读访问，但无权修改系统状态。

有关本地用户和角色分配的详细信息，请参阅用户管理。

设置 AAA

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

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

- 配置 LDAP 提供程序， 第 40 页
- 配置 RADIUS 提供程序， 第 45 页
- 配置 TACACS+ 提供程序， 第 48 页

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

2. 指定默认身份验证方法 - 这也是用户管理的一部分。

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

配置 LDAP 提供程序

配置 LDAP 提供程序的属性

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

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

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：

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

步骤 3 仅限对包含指定属性的记录进行数据库搜索：

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

步骤 4 仅限对包含指定区别名的记录进行数据库搜索：

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

步骤 5 仅限对包含指定过滤器的记录进行数据库搜索：

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

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

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

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

步骤 7 将任务提交到系统配置：

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

示例

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

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

注释 如果 LDAP 用户的 DN 超过 255 个字符，用户登录将失败。

下一步做什么

创建 LDAP 提供程序。

创建 LDAP 提供程序

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

注释 FXOS最多支持 16 个 LDAP 提供程序。

开始之前

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

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：

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

步骤 3 创建 LDAP 服务器实例，进入安全 LDAP 服务器模式：

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

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

步骤 4 （可选） 设置 LDAP 属性，用来存储用户角色和区域设置值：

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

此属性始终是一个名称值对。系统在用户记录中查询匹配此属性名称的值。

该值为必填项，除非已为 LDAP 提供程序设置了默认属性。

步骤 5 （可选） 在 LDAP 层级结构中设置特定的区别名，在此层次结构中，当远程用户登录并且系统尝试根据其用户名获取用户的 DN 时，服务器应当开始搜索：

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

基础 DN 的长度最大可以是 255 个字符减去 CN=username 长度，其中，用户名标识尝试使用 LDAP 身份验证访问 Firepower 机箱管理器或 FXOS CLI 的远程用户。

该值为必填项，除非已为 LDAP 提供程序设置了默认基础 DN。

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

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

支持的最大字符串长度为 255 个 ASCII 字符。

步骤 7 （可选） 将 LDAP 搜索限制为匹配已定义过滤器的用户名。

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

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

该值为必填项，除非已为 LDAP 提供程序设置了默认过滤器。

步骤 8 为已为绑定 DN 指定的 LDAP 数据库账户指定密码：

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

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

您可以输入任意标准 ASCII 字符，但空格、§（分节号）、？（问号）或 =（等号）除外。

步骤 9 （可选） 指定 FXOS使用此提供程序对用户进行身份验证的顺序：

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

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

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

步骤 11 与 LDAP 服务器通信时，启用或禁用加密使用：

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

选项如下：

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

LDAP 使用 STARTTLS。这允许使用端口 389 进行加密通信。

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

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

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

步骤 13 指定提供 LDAP 提供程序或服务器详细信息的供应商：

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

选项如下：

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

步骤 14 （可选）启用证书吊销列表检查：

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

注释 此配置仅在启用 SSL 连接后才生效。

步骤 15 将事务提交到系统配置：

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

示例

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

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

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

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

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

删除 LDAP 提供程序

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 LDAP 模式：

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

步骤 3 删除指定的服务器：

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

步骤 4 将任务提交到系统配置：

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

示例

以下示例删除名为 ldap1 的 LDAP 服务器，并且提交任务：

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

配置 RADIUS 提供程序

配置 RADIUS 提供程序的属性

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

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 RADIUS 模式：

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

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

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

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

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

步骤 5 将任务提交到系统配置：

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

示例

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

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

下一步做什么

创建 RADIUS 提供程序。

创建 RADIUS 提供程序

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

注释 FXOS最多支持 16 个 RADIUS 提供程序。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 RADIUS 模式：

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

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

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

步骤 4 （可选） 指定用于与 RADIUS 服务器通信的端口。

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

步骤 5 设置 RADIUS 服务器密钥：

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

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

您可以输入任意标准 ASCII 字符，但空格、§（分节号）、？（问号）或 =（等号）除外。

步骤 6 （可选） 指定尝试此服务器的顺序。

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

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

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

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

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

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

步骤 9 确认系统配置任务：

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

示例

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

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

删除 RADIUS 提供程序

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 RADIUS 模式：

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

步骤 3 删除指定的服务器：

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

步骤 4 将任务提交到系统配置：

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

示例

以下示例删除名为 radius1 的 RADIUS 服务器，并且提交任务：

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

配置 TACACS+ 提供程序

配置 TACACS+ 提供程序的属性

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

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

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 TACACS+ 模式：

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

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

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

请输入一个介于 1 到 60 秒的整数。默认值为 5 秒。

步骤 4 将任务提交到系统配置：

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

示例

以下示例将 TACACS+ 超时间隔设置为 45 秒，并且提交任务：

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

下一步做什么

创建 TACACS+ 提供程序。

创建 TACACS+ 提供程序

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

注释 FXOS最多支持 16 个 TACACS+ 提供程序。

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 TACACS+ 模式：

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

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

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

步骤 4 指定 TACACS+ 服务器密钥：

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

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

您可以输入任意标准 ASCII 字符，但空格、§（分节号）、？（问号）或 =（等号）除外。

步骤 5 （可选） 指定尝试此服务器的顺序。

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

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

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

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

步骤 7 （可选） 指定用于与 TACACS+ 服务器通信的端口：

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

步骤 8 将任务提交到系统配置：

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

示例

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

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

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

删除 TACACS+ 提供程序

过程

步骤 1 进入安全模式：

Firepower-chassis# **scope security**

步骤 2 进入安全 TACACS+ 模式：

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

步骤 3 删除指定的服务器：

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

步骤 4 将任务提交到系统配置：

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

示例

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

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

验证远程 AAA 服务器配置

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

确定当前的 FXOS 身份验证配置

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

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

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

确定当前的 LDAP 配置

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

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

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

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

确定当前的 RADIUS 配置

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

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

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

确定当前的 TACACS+ 配置

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

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

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

配置系统日志

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

过程

步骤 1 进入监控模式：

Firepower-chassis# **scope monitoring**

步骤 2 启用或禁用向控制台发送系统日志：

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

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

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

步骤 4 启用或禁用操作系统监控系统日志消息：

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

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

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

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

步骤 6 启用或禁用向系统日志文件写入系统日志消息：

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

步骤 7 指定记录消息的文件的名称。文件名中最多包含 16 个字符。

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

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

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

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

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

步骤 10 配置向最多三个外部系统日志服务器发送系统日志消息：

a) 启用或禁用向最多三个外部系统日志服务器发送系统日志消息：

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

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

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

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

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

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

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

步骤 11 配置本地来源。为您要启用或禁用的每个本地来源输入以下命令：

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

这可以是以下其中一项：

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

步骤 12 提交任务：

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

示例

以下示例介绍如何启用在本地文件中存储系统日志消息并且提交任务：

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

配置 DNS 服务器

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

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

过程

步骤 1 进入系统模式：

Firepower-chassis # **scope system**

步骤 2 进入系统服务模式：

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

步骤 3 要创建或删除 DNS 服务器，请输入相应的命令，如下所示：

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

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

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

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

步骤 4 将任务提交到系统配置：

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

示例

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

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

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

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

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

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

启用 FIPS 模式

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

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 启用 FIPS 模式：

enable fips-mode

步骤 3 提交配置：

commit-buffer

步骤 4 重新启动系统：

connect local-mgmt

reboot

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

下一步做什么

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

启用通用标准模式

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

过程

步骤 1 从 FXOS CLI 进入安全模式：

scope security

步骤 2 启用通用标准模式：

enable cc-mode

步骤 3 提交配置：

commit-buffer

步骤 4 重新启动系统：

connect local-mgmt

reboot

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

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

下一步做什么

在 FXOS 版本 2.0.1 之前，首次设置设备时创建的现有 SSH 主机密钥被硬编码为 1024 位。要符合 FIPS 和通用标准认证需求，您必须销毁此旧主机密钥，并使用生成 SSH 主机密钥中的详细操作步骤

生成新的主机密钥。如果不执行这些附加步骤，则在“通用标准 (Common Criteria)”模式启用的情况下，设备重新启动后，将无法使用 SSH 连接到管理引擎。如果您使用 FXOS 2.0.1 或更高版本执行初始设置，则无需生成新的主机密钥。

配置 IP 访问列表

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

IP 访问列表支持以下协议：

- HTTPS
- SNMP
- SSH

对于各 IP 地址块（v4 或 v6），可为各服务配置最多 100 个不同子网。子网 0 和前缀 0 允许无限制无限访问服务。

过程

步骤 1 从 FXOS CLI 进入服务模式：

scope system

scope services

步骤 2 为要启用访问权限的服务创建 IP 块：

IPv4：

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

IPv6：

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

示例

以下示例显示了如何创建、输入和验证 IPv4 地址块以提供 SSH 访问：

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

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

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

以下示例显示了如何创建、输入和验证 IPv6 地址块以提供 SSH 访问：

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

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

为容器实例接口添加 MAC 池前缀，并查看其 MAC 地址

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

A2*xx.yyzz.zzzz*

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

有关详细信息，请参阅容器实例接口的自动 MAC 地址。

此程序介绍如何查看 MAC 地址，以及如何选择性地定义生成所使用的前缀。

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

过程

步骤 1 先进入安全服务模式，然后进入自动 MAC 池模式。

scope ssa

scope auto-macpool

示例：

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

步骤 2 设置生成 MAC 地址所使用的 MAC 地址前缀。

set prefix 前缀

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

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

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

对于前缀 1009 (03F1)，MAC 地址为：

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

示例：

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

步骤 3 保存配置。

commit-buffer

示例：

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

步骤 4 查看 MAC 地址分配。

show mac-address

示例：

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

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

示例

以下示例将 MAC 前缀设为 33。

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

为容器实例添加资源配置文件

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

- 最小核心数量为 6。

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

- 您可以分配偶数（6、8、10、12、14 等）个核心，乃至最大值。
- 最大可用核心数取决于安全模块/机箱型号，请参阅容器实例的要求和必备条件。

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

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

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

过程

步骤 1 进入安全服务模式。

scope ssa

示例：

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

步骤 2 创建资源配置文件。

enter resource-profile *name*

- *name* - 设置介于 1 和 64 个字符之间的配置文件名称。请注意，此配置文件名称添加后无法更改。

示例：

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

步骤 3 输入说明。

set description *description*

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

示例：

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

步骤 4 设置 CPU 核心数。

set cpu-core-count *cores*

- *cores* - 设置介于 6 和最大值之间的配置文件核心数（偶数），具体取决于机箱。

示例：

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

步骤 5 保存配置。

commit-buffer

示例：

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

步骤 6 从安全服务模式查看资源配置文件分配情况。

show resource-profile user-defined

示例：

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

步骤 7 查看安全模块/引擎插槽的资源使用情况。

show monitor detail

示例：

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

步骤 8 查看应用实例的资源配置情况。

show resource detail

示例：

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

示例

以下示例添加了三个资源配置文件。

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

配置网络控制策略

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

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

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

注释

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

过程

步骤 1 输入组织范围。

scope org

示例：

```
Firepower # scope org
```

步骤 2 创建并启用网络控制策略。

create nw-ctrl-policy *nw-policy*

示例：

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

步骤 3 启用 LLDP。

enable lldp *{receive | transmit}*

示例：

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

步骤 4 提交配置：

commit-buffer

示例：

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

步骤 5 指定是否启用或禁用 LLDP 进行接收/传输。

enable lldp 接收/传输

commit-buffer

示例：

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

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

步骤 6 使用以下命令将网络控制策略应用到接口。

a) 输入接口：

scope eth-uplink

scope fabric a

scope interface *interface_id*

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

b) 设置　网络控制策略：

set nw-ctrl-policy *nw-policy*

commit-buffer

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

c) 查看更改：

show detail

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

d) 提交配置：

commit-buffer

示例：

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

配置机箱 URL

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

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

过程

步骤 1 进入系统模式：

scope system

示例：

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

步骤 2 要配置新的机箱名称：

set name *chassis_name*

- 机箱名称 - 设置介于 1 至 60 个字符之间的机箱名称。

示例：

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

步骤 3 要配置管理 URL：

set mgmt-url *management_url*

- *management_url* - 设置 FMC 应该用于连接到 Firepower 机箱管理器 中 FTD 实例的 URL。URL 必须以 https:// 开头。如果未指定机箱管理 URL，则使用机箱名称。

示例：

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

步骤 4 保存配置。

commit-buffer

示例：

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

步骤 5 查看配置设置。

show detail

示例：

```
Firepower_chassis /system # show detail

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

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